15 '24

K/ 02

THEOREME DE KRONECKER

X-ENS Al 1 p213
Szpirglas, algèbre pour la L3 p573.

Pas de réf pour corollaire

Prérequis
- fonctions symétriques élémentaires, relation coefficients-racines.
  ↔ thm de structure des polynômes symétriques.
- $X^n - 1 = \prod_{d|n} \Phi_d$

Théorème : Si $P \in \mathbb{Z}[X]$ unitaire dont les racines sont de module ≤ 1. On suppose $P(0) \neq 0$. Alors les racines de P sont des racines de l'unité.

Dém : $\Omega_n = \{P \in \mathbb{Z}[X]$ unitaire de deg n et $z \in Z(P) \Rightarrow 0 < |z| \leq 1\}$, pour $n \in \mathbb{N}^*$

Etape 1 : Ω_n est fini

Soit $P \in \Omega_n$, on note $z_1, \dots, z_n$ ses racines et $\sigma_1, \dots, \sigma_n$ les fonctions symétriques élémentaires de évaluées en $(z_1, \dots, z_n)$: $\sigma_p = \sum_{1 \leq i_1 < \dots < i_p \leq n} z_{i_1} \cdots z_{i_p}$

On note $P = X^n + a_1 X^{n-1} + \dots + a_{n-1} X + a_n = (X - z_1) \cdots (X - z_n)$

~~Comme $P(0) \neq 0$, $a_n \neq 0$.~~

Par relation coefficients racines, $a_p = (-1)^p \sigma_p$

d'où $P = X^n - \sigma_1 X^{n-1} + \dots + (-1)^n \sigma_n$.

Comme $P \in \mathbb{Z}[X]$, $\sigma_i \in \mathbb{Z}$ pour $i \in [\![1, n]\!]$.

Comme $|z_i| \leq 1$, $|\sigma_p| = \left| \sum_{1 \leq i_1 < \dots < i_p \leq n} z_{i_1} \cdots z_{i_p} \right| \leq \sum_{1 \leq i_1 < \dots < i_p \leq n} 1 = \binom{n}{p}$ parties à p élts de $[\![1, n]\!]$.

Or $\sigma_p \in \mathbb{N}$ d'où $\sigma_p \in$ ~~$\{\pm \binom{n}{p}\}$~~. Ainsi Ω_n est fini, pour $n \in \mathbb{N}^*$.
?? $\sigma_p \in [\![-\binom{n}{p}, \binom{n}{p}]\!]$

Etape 2 : $P_k = \prod_{i=1}^n (X - z_i^k) \in \Omega_n$. pour $k \in \mathbb{N}^*$ où les z_i sont les racines de P. ($P_1 = P$)

On a $\deg P_k = n$, P_k est unitaire et, comme $0 < |z_i| \leq 1$, $0 < |z_i^k| \leq 1$.
Il reste à montrer que $P_k \in \mathbb{Z}[X]$.

Le coefficient de X^{n-r} dans P_k est $(-1)^r \sigma_r \cdot (z_1^k, \dots, z_n^k)$ par relations coefficients racines

Or $\sigma_r(X_1^k, \dots, X_n^k)$ est un polynome symétrique à coefficients dans $\mathbb{Z}$, donc par théorème de structure des polynomes symétriques, il existe $Q_r \in \mathbb{Z}[X_1, \dots, X_n]$

tq $\sigma_r(X_1^k, \dots, X_n^k) = Q_r(\sigma_1(X_1, \dots, X_n), \dots, \sigma_n(X_1, \dots, X_n))$

d'où $\sigma_r(z_1^k, \dots, z_n^k) = \underbrace{Q_r}_{\in \mathbb{Z}[X_1, \dots, X_n]}(\underbrace{\sigma_1(z_1, \dots, z_n)}_{\in \mathbb{Z}}, \dots, \underbrace{\sigma_n(z_1, \dots, z_n)}_{\in \mathbb{Z}}) \in \mathbb{Z}$.

$P \in \mathbb{Z}[X]$

donc $P_k \in \Omega_n$.

Etape 3 : conclusion.

Notons Z_n l'ensemble des racines des éléments de Ω_n. D'après l'étape 1, Ω_n est fini d'où Z_n est fini. D'après l'étape 2, si $z_i \in Z_n$ alors $z_i^k \in Z_n$ pour $k \in \mathbb{N}^*$.

On peut donc définir $\begin{array}{ccc} \mathbb{N}^* & \longrightarrow & Z_n \\ k & \longmapsto & z_i^k \end{array}$. Cette application n'est pas injective car $\#E_n < \infty$. d'où il existe k, ℓ $\underset{\text{ou } k > \ell}{k \neq \ell}$ tq $z_i^k = z_i^\ell$. or $z_i \neq 0$ par hypothèse ($P(0) \neq 0$)

d'où $z_i^{k-\ell} = 1$ d'où z_i est une racine de l'unité. On fait cela pour $i \in [\![1, n]\!]$, ce qui donne le résultat.

10'55

Corollaire: Soit $P \in \mathbb{Z}[X]$ unitaire irréductible dans $\mathbb{Z}$ (mais aussi ds $\mathbb{Q}$) à racines de modules ≤ 1.
Alors $P = X$ ou P est un polynôme cyclotomique.

Dém: Supposons $P \neq X$, comme P est irréductible, $P(0) \neq 0$. donc d'après le théorème de

Kronecker, les racines de P sont des racines de l'unité : $\exists N \in \mathbb{N}^* \ \forall z \in Z(P) \ z^N - 1 = 0$
$N = $ ppcm de n_i tq $z_i^{n_i} = 1$

Ne pas oublier !!!

Si P n'était pas à racines simples, $P \wedge P'$* serait un polynôme non constant divisant P strictement. Or P est irréductible
Donc P est à racines simples.
Donc $P \mid X^N - 1$.
Or $X^N - 1 = \prod_{d \mid N} \Phi_d$ décomposition en facteurs irréductibles de $X^N - 1$ dans $\mathbb{Z}[X]$
où Φ_d est le d^e polynome cyclotomique.
et P irréductible (avec $P \neq 1$) d'où $P = \Phi_d$ pour un $d \mid N$.

Corollaire - Soit $P \in \mathbb{Z}[X]$ unitaire à racines de modules ≤ 1. alors P est un produit de puissances de X et de polynômes cyclotomiques.

Dém: Soit Q un facteur irréductible de P dans $\mathbb{Z}[X]$ qui est factoriel. alors il vérifie le corollaire précédent d'où $Q = X$ ou Q est un polynôme cyclotomique.

* $\mathbb{K}$ un sous corps de $\mathbb{C}$, $P \in \mathbb{K}[X]$ a une racine multiple dans $\mathbb{C}$ ssi $D = \mathrm{pgcd}(P, P')$ est non cst.

- si P a une racine multiple, $X - a \mid P$ et P' d'où $X - a \mid D$.
  ($P = (X-a)^m P_1$ $\quad P_1(a) \neq 0$ $\quad P' = (X-a)^m P_1' + (X-a)^{m-1} m P_1$)
- si D non cst, par d'Alembert, $\exists a \in \mathbb{C}$ tq $D(a) = 0$. d'où $X - a \mid D$
  d'où $X - a \mid P$ et P' d'où a de multiplicité ≥ 2.

si $D = P$ alors $P \mid P'$ ↯ par degré

~~**: $P = QR$, $P \in \mathbb{Z}[X]$ unitaire alors $Q, R \in \mathbb{Z}[X]$ unitaires~~ ~~$Q, R \in \mathbb{Q}[X]$ Q unitaire~~ en reprenant le lemme ~~irréduct des poly cyclo~~

$\mathrm{Pgcd}(P, P') \in \mathbb{Q}[X]$ car P' n'est pas à coefficients dominant inversible donc on peut pas faire dans $\mathbb{Z}$.

On a $P = \mathrm{Pgcd}(P, P) \times Q$ où $Q \in \mathbb{Q}[X]$ et on applique **
donc $\mathrm{Pgcd}(P, P') \in \mathbb{Z}[X]$

ou $P \wedge P' \in \mathbb{Q}[X]$ non constant si y a une racine double or $P \wedge P' \mid P$ dans $\mathbb{Q}[X]$ on a donc trouvé une décomposition de P dans $\mathbb{Q}[X]$ qui n'est pas en polynômes cst donc absurde car P irréd sur $\mathbb{Q}$