144 — Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.

$\mathbb{K}$ corps commutatif

I / Racines d'un polynôme

1) Définitions et premières propriétés (GOU)

Déf 1 Soit $P \in \mathbb{K}[X]$. On dit que $\alpha \in \mathbb{K}$ est une racine de P si $P(\alpha) = 0$

Ex 2 Les racines complexes de $X^n - 1$ sont les racines $n^{ième}$ de l'unité.

Prop 3 $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$.
(α racine de P) $\iff$ ($X - \alpha \mid P$).

Déf 4 Soit $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$, $k \in \mathbb{N}^*$. On dit que α est racine d'ordre k si $(X-\alpha)^k \mid P$ et $(X-\alpha)^{k+1} \nmid P$.

Rq 5 Si $P \in \mathbb{K}[X]$ est de degré ≥ 1, alors P a au plus n racines (avec multiplicité).

⚠ Cette remarque est fausse dans le cas d'un anneau.
$P(X) = 4X \in \mathbb{Z}/8\mathbb{Z}[X]$ a 3 racines 0, 2 et 4.

Prop 6 Soit $P \in \mathbb{K}[X]$ tel que $\forall x \in \mathbb{K}$, $P(x) = 0$.
Si $\mathbb{K}$ est infini, on a $P = 0$

Cex 7 Si $\mathbb{K} = \{a_1, \dots, a_n\}$, $P(X) := (X-a_1)\dots(X-a_n)$ est non nul pourtant $\forall x \in \mathbb{K}$, $P(x) = 0$.

Cor 8 Soient $a_0, \dots, a_n$ $n+1$ réels distincts.

$$\phi : \mathbb{R}_n[X] \longrightarrow \mathbb{R}^{n+1}, \quad P \longmapsto (P(a_0), \dots, P(a_n))$$ est un isomorphisme.

(polynômes interpolateurs)

App 9 Calcul du déterminant de Van Der Monde

$$\begin{vmatrix} 1 & \alpha_1 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \dots & \alpha_2^{n-1} \\ \vdots & & & \\ 1 & \alpha_n & \dots & \alpha_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i).$$

Déf 10 $P \in \mathbb{K}[X]$ est irréductible dans $\mathbb{K}[X]$ si P n'est pas constant et si ses seuls diviseurs dans $\mathbb{K}[X]$ sont les constantes non nulles et les polynômes associés à P.

Déf 11 $P \in \mathbb{K}[X]$ est scindé sur $\mathbb{K}$ si $P = \lambda \prod_{i=1}^{r} (X - \alpha_i)^{m_i}$
$\lambda \in \mathbb{K}$, $m_i \in \mathbb{N}^*$, $\alpha_i \in \mathbb{K}$

Th 12 (d'Alembert - Gauss) Soit $P \in \mathbb{C}[X]$ non constant.
$\exists z_0 \in \mathbb{C}$, $P(z_0) = 0$.

Cor 13 Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1

Prop 14 Les irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatif

2) Adjonction de racines (PER)

Déf 15 Soit $P \in \mathbb{K}[X]$ irréductible
Une extension $K \hookrightarrow L$ est appelée un corps de rupture de P si $L = \mathbb{K}(\alpha)$ avec $P(\alpha) = 0$.

Th 16 Soit $P \in \mathbb{K}[X]$ irréductible.
Il existe un corps de rupture de P sur $\mathbb{K}$, unique à isomorphisme près.

Ex 17
- $\mathbb{C}$ est le corps de rupture de X^2+1 sur $\mathbb{R}$
- $\mathbb{F}_4$ ______ de X^2+X+1 sur $\mathbb{F}_2$

Déf 18 Soit $P \in \mathbb{K}[X]$. On appelle corps de décomposition de P sur $\mathbb{K}$ une extension L de $\mathbb{K}$ telle que
- dans $L[X]$, P est produit de facteurs de degré 1
- les racines de P engendrent L (i.e. L est minimal)

Th 19 Soit $P \in \mathbb{K}[X]$. Il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près. On le note $D_{\mathbb{K}}(P)$.

Ex 20
- Pour $\mathbb{K} = \mathbb{Q}$, $P(X) = X^3 - 2$, $D_{\mathbb{Q}}(P) = \mathbb{Q}(\sqrt[3]{2}, j)$
- Pour $\mathbb{K} = \mathbb{Q}$, $P(X) = X^4 - 2$, $D_{\mathbb{Q}}(P) = \mathbb{Q}(\sqrt[4]{2}, i)$

Déf 21 Une extension $\overline{\mathbb{K}}$ de $\mathbb{K}$ est appelée une clôture algébrique de $\mathbb{K}$ si $\overline{\mathbb{K}}$ est algébriquement clos et $\overline{\mathbb{K}}$ algébrique sur $\mathbb{K}$.

Ex 22 $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$

App 23 Construction des corps finis
Soit $p \in \mathbb{P}$ et $n \in \mathbb{N}^*$. Soit $q = p^n$.
Il existe un corps $\mathbb{K}$ à q éléments, c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. Il est unique à isomorphisme près, on le note $\mathbb{F}_q$.

Rq 24 Un corps fini n'est jamais algébriquement clos

3) Fonctions symétriques élémentaires [Gou, TEST, RDO]

• Relations entre coefficients et racines

Soit $P = a_0X^n + a_1X^{n-1} + \dots + a_{n-1}X + a_n \in \mathbb{K}[X]$, $a_0 \neq 0$ scindé sur $\mathbb{K}$. $P = a_0(X - x_1)\cdots(X - x_n)$

Alors $\forall p \in \{1, \dots, n\}$, $\sigma_p = \sum_{1 \leq i_1 < \dots < i_p \leq n} x_{i_1} \cdots x_{i_p} = (-1)^p \frac{a_p}{a_0}$

En particulier, $\sigma_1 = \sum_{i=1}^n x_i = -\frac{a_1}{a_0}$, $\sigma_2 = \sum_{1 \leq i < j \leq n} x_i x_j = \frac{a_2}{a_0}$, $\sigma_n = \prod_{i=1}^n x_i = (-1)^n \frac{a_n}{a_0}$

App 25. Résolution du système :

$$\begin{cases} x + y + z = 1 \\ x^2 + y^2 + z^2 = 21 \\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1 \end{cases}$$

• Polynômes symétriques
$\mathfrak{S}_n$ agit sur $\mathbb{K}[X_1, \dots, X_n]$ de la façon suivante :
Pour $\sigma \in \mathfrak{S}_n$, $(\sigma.P)(X_1, \dots, X_n) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$.

Déf 26 Les polynômes symétriques sont les polynômes $P \in \mathbb{K}[X]$ tels que $\forall \sigma \in \mathfrak{S}_n$, $\sigma.P = P$.

Rq 27 P est un polynôme symétrique ssi pour toute transposition τ, $\tau.P = P$.

Ex 28 • $P(X_1, X_2) = X_1 + X_2$
• $P(X_1, X_2, X_3) = X_1^2X_2 + X_1^2X_3 + X_1X_2^2 + X_1X_3^2 + X_2^2X_3 + X_2X_3^2$
sont des polynômes symétriques.

Prop / Déf 29 Dans $\mathbb{K}[X_1 \dots X_n]$ les n polynômes Σ_p, $1 \leq p \leq n$ définis par $\Sigma_p = \sum_{1 \leq i_1 < \dots < i_p \leq n} X_{i_1} \cdots X_{i_p}$ sont symétriques et sont appelés polynômes symétriques élémentaires

Déf 30 On appelle poids du monôme $Y_1^{i_1} \cdots Y_n^{i_n}$ l'entier $\sum_{k=1}^n k i_k$
Si $P = \sum_{i \in \mathbb{N}^n} a_i Y_1^{i_1} \cdots Y_n^{i_n}$ est non nul, le poids du polynôme P est $\pi(P) := \max\{m \in \mathbb{N} \mid \exists i \in \mathbb{N}^n, a_i \neq 0 \text{ et } \sum_{k=1}^n k i_k = m\}$.
Si $P = 0$, $\pi(P) := -\infty$.

Déf 31 Soit P un polynôme symétrique de $\mathbb{K}[X_1, \dots, X_n]$. Il a même degré partiel par rapport à chaque indéterminée, on l'appelle ordre de P, et on le note $\omega(P)$.

Prop 32 Soit P un polynôme symétrique de $\mathbb{K}[X_1, \dots, X_n]$ de degré p et d'ordre ω. Il existe un unique polynôme Q de $\mathbb{K}[Y_1, \dots, Y_n]$ tel que $P(X_1, \dots, X_n) = Q(\Sigma_1, \dots, \Sigma_n)$. Q est de poids p et de degré ω.

Ex 33 $P = \sum_{i \neq j} X_i^2 X_j$ dans $\mathbb{K}[X_1, X_2, X_3]$. On a $P = \Sigma_1\Sigma_2 - 3\Sigma_3$

App 34 Théorème de Kronecker (DVP T 1)
Soit $P \in \mathbb{Z}[X]$ unitaire tel que $P(0) \neq 0$, $\deg P = n$
Si les racines complexes $\alpha_1, \dots, \alpha_n$ sont de module ≤ 1 alors $\alpha_1, \dots, \alpha_n$ sont des racines de l'unité.

II / Localisation et comptage de racines

1) Recherche algébrique

- On veut obtenir les racines rationnelles d'un polynôme à coefficients entiers.

Prop 35 Soit $P \in \mathbb{Z}[X]$, $P(X) = a_n X^n + \dots + a_1 X + a_0$.
Soit $\frac{p}{q} \in \mathbb{Q}$, $p \wedge q = 1$.
Si $\frac{p}{q}$ est racine de P, alors $p \mid a_0$ et $q \mid a_n$.

Rq 36 On obtient une liste finie de racines à tester.

Ex 37 $P(X) = X^4 + 3X^2 + X + 2$.
Si $\frac{p}{q}$ est racine rationnelle de P, $\frac{p}{q} \in \{\pm 1, \pm 2\}$ et on voit alors que P n'a aucune racine rationnelle.

- Soit $P \in \mathbb{R}_m[X]$, $x_1, \dots, x_t$ ses racines de multiplicités $m_1, \dots, m_t$.
On pose $S_k = \sum_{i=1}^{t} m_i x_i^k$ et $S_0 = m$ (sommes de Newton).

Th 38 $S(X_0, \dots, X_{n-1}) = \sum_{0 \leq i,j \leq n-1} S_{i+j} X_i X_j$ est une forme quadratique réelle.
Si on note (p, q) sa signature, alors le nombre de racines distinctes de P est $p+q$ et le nombre de racines réelles distinctes de P est $p-q$. (DVP 2)

2) Recherche complexe [GOU, TEST]

On peut localiser les racines de P :

Prop 39 Soit $P = X^n + a_1 X^{n-1} + \dots + a_{n-1} X + a_n \in \mathbb{C}[X]$.
Soit $\rho \geq 0$ le plus grand des modules des racines de P. Alors :
- $\rho \leq \sup\{1, \sum_{i=1}^{n} |a_i|\}$
- $\rho \leq 1 + \sup_{1 \leq i \leq n} |a_i|$

Th 40 Soit $z_0 \in \mathbb{C}$, $r > 0$.
On note $C(z_0, r) = \{z \in \mathbb{C} \mid |z - z_0| = r\}$
$D(z_0, r) = \{z \in \mathbb{C} \mid |z - z_0| < r\}$
On suppose que $P \in \mathbb{C}[X]$ ne s'annule en aucun point de $C(z_0, r)$.
Alors $\frac{1}{2i\pi} \int_{C(z_0,r)} \frac{P'(z)}{P(z)} dz$ est égale au nombre des racines de P contenues dans $D(z_0, r)$, comptées avec multiplicité.

On peut en déduire alors,

Th 41 (théorème de Rouché)
Soit $z_0 \in \mathbb{C}$, $r > 0$: $P, Q \in \mathbb{C}[X]$ tq $|Q(z)| < |P(z)|$ $\forall z \in C(z_0, r)$.
Alors P et $P + Q$ possèdent le même nombre de zéros dans le disque ouvert $D(z_0, r)$.

Ex 42 Soit N_P le nombre de racines de $P(z) = z^8 - 5z^3 + z - 2$ dans $D(0,1)$.
On a alors $N_P = 3$

On peut aussi localiser les racines de P' en fonction de celle de P :

Th 43 (Gauss Lucas)
Soit $P \in \mathbb{C}[X]$ non constant. Alors tout zéro de P' appartient à l'enveloppe convexe de l'ensemble des zéros de P.

3) Recherche réelle [TEST]

Th 44 Soit $P(X) = a_0 + a_1 X + \dots + a_n X^n \in \mathbb{R}[X]$.
Le nombre $N_+(P)$ (resp $N_-(P)$) de racines réelles positives (resp négatives) de P est majoré par le nombre de changements de signes de la suite $(a_0, \dots, a_n)$ (resp $(a_0, -a_1, \dots, (-1)^n a_n)$).

Ex 45 $P(X) = 1 + 3X - X^2 - 4X^3 - 2X^5 + X^6 + X^7$ a au plus 2 racines réelles positives et 3 racines réelles négatives.

Th 46 Soit $P_0 \in \mathbb{R}[X]$ et x_0 racine simple de P_0. Alors la racine dépend localement du polynôme de manière C^∞. Autrement dit : $\exists \varphi \in C^\infty(U, V)$, U voisinage de P_0 dans $\mathbb{R}_n[X]$, V voisinage de x_0 dans $\mathbb{R}$ telle que $\forall P \in U$, $\forall x \in V$, $\varphi(P) = x \Leftrightarrow P(x) = 0$.

<u>Références</u> :

- Objectif Agrégation
- Gourdon, Algèbre
- Testard, Analyse mathématiques
- Perrin, Algèbre
- Ramis Deschamps, Odoux, Cours de mathématiques, Algèbre 1

développement : formes de Hankel.

Ref : Caldero - Germoni, Histoires hédonistes de groupes et de géométrie (référence D.21 page 197)

But : Construire une forme quadratique réelle s associée à un polynôme réel P et telle que la signature de s permette de calculer le nombre de racines distinctes et le nombre de racines réelles distinctes de P.

Soit $P \in \mathbb{R}_n[X]$, $x_1, \dots, x_t$ ses racines et m_i = multiplicité de x_i.

On pose :
$S_k = m_1 x_1^k + \dots + m_t x_t^k$ (pour $k \geq 1$) et $S_0 = n$
(on les appelle souvent sommes de Newton).

Théorème : $S(X_0, \dots, X_{n-1}) = \sum_{0 \leq i,j \leq n-1} s_{i+j} X_i X_j$ est une forme quadratique réelle.
Si on note sa signature (p, q) alors le nombre de racines distinctes de P est $p+q$ et le nombre de racines réelles distinctes de P est $p-q$.

Dém :
- S est clairement une forme quadratique sur $\mathbb{C}^n$ (il suffit de l'écrire $S(X_0, \dots X_{n-1}) = b((X_0, \dots X_{n-1}), (X_0, \dots X_{n-1}))$
avec $b(X, Y) = \sum_{i=0}^{n-1} s_{2i} X_i Y_i + \frac{1}{2} \sum_{i \neq j} s_{i+j} X_i Y_j$

où $X = (X_0, \dots X_{n-1})$ et $Y = (Y_0, \dots Y_{n-1})$.
On vérifie que b est bilinéaire symétrique.

Montrons que $S_{|\mathbb{R}}$ définit une forme quadratique sur $\mathbb{R}^n$.
Il suffit de montrer que $s_k \in \mathbb{R}$ $\forall k$.

$$s_k = m_1 x_1^k + \dots + m_t x_t^k$$
$$= \underbrace{\sum m_i x_i^k}_{\text{racines réelles}} + \sum \underbrace{m_j x_j^k + m_j \overline{x_j^k}}_{\text{racines complexes conjuguées}} = \underbrace{\sum m_i x_i^k + \sum 2 m_j \operatorname{Re}(x_j^k)}_{\in \mathbb{R}}.$$

...note dorénavant (p,q) la signature de $J'_{\mathbb{R}}$ ← simplifier les notations..

$e(x_0 - x_{n-1}) = x_0 + x_e x_1 + \dots + x_e^{n-1} x_{n-1}$

1q : $(e_1, \dots, e_t)$ est une famille libre de $(\mathbb{C}^n)^*$.

~~Pour cela, on considère la base canonique de $\mathbb{C}^n$ qu'on note exceptionnellement $(e_0, \dots, e_{n-1})$ ($e_i = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \leftarrow (i+1)^{\text{ème}}$ position) et sa base duale $(e_0^*, \dots, e_{n-1}^*)$.~~
~~Si on écrit la matrice constituée des e_e dans la base duale on obtient :~~

$$\cancel{\left(e_1 \middle| e_2 \middle| \dots \middle| e_t \right) = \begin{pmatrix} 1 & 1 & & 1 \\ x_1 & x_2 & & x_t \\ \vdots & \vdots & \dots & \vdots \\ x_1^{n-1} & x_2^{n-1} & & x_t^{n-1} \end{pmatrix}}$$

~~Ce qui est une matrice de Vandermonde.~~
~~Les x_e sont distincts.~~
~~Donc la matrice est inversible (son déterminant est $\prod_{1 \le i < j \le t} (x_j - x_i)$)~~

Soit $(\lambda_1 \dots \lambda_t) \in \mathbb{C}^t$ tel que : $\lambda_1 e_1 + \dots + \lambda_t e_t = 0$
Notons exceptionnellement $(e_1, \dots, e_n)$ la base canonique de $\mathbb{C}^n$.
$\sum_{e=1}^{t} \lambda_e e_e(e_i) = 0$ donc $\sum_{e=1}^{t} \lambda_e x_e^{i-1} = 0 \quad \forall i \in [\![1; n]\!]$

Donc :
$$\underbrace{\begin{pmatrix} 1 & \dots & 1 \\ x_1 & & x_t \\ x_1^2 & & x_t^2 \\ x_1^{t-1} & & x_t^{t-1} \end{pmatrix}}_{\text{matrice de Vandermonde}} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_t \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$
(on a particularisé la précédente relation pour $i \in [\![1; t]\!]$) $\underline{t \le n}$

Son déterminant est $\prod_{1 \le i < j \le t} (x_j - x_i) \neq 0$ (les x_i sont $\neq$)

Donc $\lambda_1 = \dots = \lambda_t = 0$

D'où : $(e_1, \dots, e_t)$ est une famille libre de $(\mathbb{C}^n)^*$.

[illegible]

$$S = \sum_{h=1}^{t} m_h \alpha_h^2 .$$

$$\sum_{h=1}^{t} m_h \alpha_h^2 = \sum_{h=1}^{t} m_h \left(\sum_{i=0}^{n-1} x_h^i X_i \right)^2$$

$$= \sum_{h=1}^{t} m_h \sum_{0 \le i,j \le n-1} x_h^i x_h^j X_i X_j$$

$$= \sum_{0 \le i,j \le n-1} \left(\sum_{h=1}^{t} m_h x_h^{i+j} \right) X_i X_j$$

$$= \sum_{0 \le i,j \le n-1} s_{i+j} X_i X_j$$

$$= S$$

Ainsi le rang de S vu comme forme quadratique sur $\mathbb{C}^n$ est égal à t car les α_h sont linéairement indépendantes. Modulo un changement de base, S s'écrit matriciellement :

$$\begin{pmatrix} m_1 & & & & & \\ & m_2 & & & & \\ & & \ddots & & & \\ & & & m_t & & \\ & & & & 0 & \\ & & & & & \ddots \; 0 \end{pmatrix}$$

D'autre part, $rg(S) = p+q$ (vu comme forme quadratique sur $\mathbb{R}^n$)

Donc : $t = p+q$

D'où le nombre de racines distinctes de P est $p+q$.

Si x_h est racine complexe de P alors $\alpha_h^2 + \bar{\alpha}_h^2 = 2\mathrm{Re}(\alpha_h) - 2\mathrm{Im}(\alpha_h)$

Donc : $\mathrm{sign}(\alpha_h^2 + \bar{\alpha}_h^2) = (1,1)$

Notons r le nombre de racines réelles distinctes

$$S = \underbrace{\sum m_h \alpha_h^2}_{\substack{\text{associées}\\ \text{aux racines}\\ \text{réelles de } P}} + \underbrace{\sum m_h \alpha_h^2 + \bar{\alpha}_h^2}_{\substack{\text{associées}\\ \text{aux racines}\\ \text{complexes et conjuguées}\\ \text{de } P}}$$

$$(p,q) = (r, 0) + \left(\frac{t-r}{2}, \frac{t-r}{2} \right) = \left(r + \frac{t-r}{2}, \frac{t-r}{2} \right)$$

Donc : $p - q = r$ d'où le résultat.

iques importantes, le résultat pourrait être complètement ~~xxx~~ anecdotique si on ne savait pas calculer des s_k (sommes de Newton) sans connaître les racines.

Rappel : $s_k = \sum m_i x_i^k$
racine

lors elles sont en fait calculables par récurrence via les formules de Newton (cf [Gou, Alg ; p. 34])

Une fois qu'on a la matrice de notre forme quadratique, il faut disposer d'un algo efficace pour calculer sa signature ~~xxx~~.

$\text{sign } \xi = (n_+, n_-)$

nbre de valeurs propres >0 ; nbre de valeurs propres <0

inutilisable en pratique car le calcul des valeurs propres est difficile sauf pour certaines matrices

sign déterminée par réduction de Gauss : mise sous forme de carrés ; on peut procéder ainsi :

. Mais ce qui semble peut être le plus efficace, c'est d'utiliser les mineurs principaux de notre matrice et regarder les changements de signe (ce sont juste des calculs de déterminant) qui nous permettent d'avoir accès à la signature. (Michel Coste, site de la prépa agreg, comptage de racines).

Théorème de Kronecker

RIFFAUT Antonin

2013-2014

Théorème 1 (Kronecker). *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire, de degré $n \geq 1$. On suppose que les racines de P dans $\mathbb{C}$ sont de module inférieur ou égal à 1, et que 0 n'est pas racine. Alors les racines de P sont des racines de l'unité.*

Démonstration. Notons Ω_n l'ensemble des polynômes unitaires de $\mathbb{Z}[X]$, de degré n, et dont toutes les racines dans $\mathbb{C}$ sont de module inférieur ou égal à 1, et distinctes de 0. Bien entendu, $P \in \Omega_n$. Démontrons que Ω_n est un ensemble fini : soit $F \in \Omega_n$,

$$F = X^n + \sum_{i=1}^{n} f_i X^{n-i},$$

et notons $\beta_1, \ldots, \beta_n$ les racines de F dans $\mathbb{C}$ (non nécessairement distinctes). Par les relations coefficients-racines, pour tout $p \in \{1, \ldots, n\}$,

$$|f_p| = \left| \sum_{1 \leq i_1 < \cdots < i_p \leq n} \prod_{j=1}^{p} \beta_{i_j} \right| \leq \sum_{1 \leq i_1 < \cdots < i_p \leq n} \underbrace{\prod_{j=1}^{p} |\beta_{i_j}|}_{\leq 1} \leq \binom{n}{p}.$$

Comme les coefficients de F sont entiers, alors chacun d'entre eux ne peut prendre qu'un nombre fini de valeurs (indépendamment de F), ce qui impose à l'ensemble Ω_n d'être fini, le degré des éléments de Ω_n étant fixé égal à n.

À présent, notons $\alpha_1, \ldots, \alpha_n$ les racines de P dans $\mathbb{C}$, et définissons, pour tout $k \geq 1$, $P_k = \prod_{i=1}^{n}(X - \alpha_i^k) \in \mathbb{C}[X]$, ainsi que $Q_k = X^k - Y \in \mathbb{Z}[X, Y]$. Commençons par montrer que $P_k \in \mathbb{Z}[X]$, puis que $P_k \in \Omega_n$. Pour ce faire, posons $R_k(Y) = \mathrm{Res}_X(P(X), Q_k(X, Y))$; R_k est un polynôme de $\mathbb{Z}[Y]$, puisque $P(X)$ et $Q_k(X, Y)$ sont tous les deux des polynômes de $\mathbb{Z}[X, Y]$. De plus,

$$R_k(Y) = \prod_{i=1}^{n} Q_k(\alpha_i, Y) = \prod_{i=1}^{n} (\alpha_i^k - Y) = (-1)^n P_k(Y),$$

ce qui prouve que $P_k \in \mathbb{Z}[X]$. On vérifie immédiatement que P_k est unitaire, et que ses racines sont toutes de module inférieur ou égal à 1, et distinctes de 0, autrement dit que $P_k \in \Omega_n$.

Remarquons que, puisque Ω_n est un ensemble fini, l'ensemble Z_n de toutes les racines des polynômes de Ω_n est également un ensemble fini. Soit α une racine de $P = P_1$. Pour tout $k \geq 1$, α^k est une racine de P_k, de sorte que l'application $k \longmapsto \alpha^k$ définit bien une application de $\mathbb{N}^*$ dans Z_n. Cette application est nécessairement non injective, d'où l'existence de deux entiers $1 \leq r < s$ tels que $\alpha^r = \alpha^s$. Finalement, $\alpha^{s-r} = 1$, et donc α est bien une racine de l'unité. ■

Corollaire 2. *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire. On suppose que P est irréductible et que les racines de P dans $\mathbb{C}$ sont de module inférieur ou égal à 1. Alors $P = X$ ou P est un polynôme cyclotomique.*

Démonstration. Supposons que $P \neq X$. Comme P est irréductible, alors 0 n'est pas racine de P, donc d'après le théorème de Kronecker, les racines de P sont des racines de l'unité. On en déduit qu'il existe un entier $N \in \mathbb{N}^*$ tel que pour toute racine α de P, $\alpha^N = 1$, de sorte que $P | X^N - 1$. Or la factorisation en irréductibles de $X^N - 1$ dans $\mathbb{Z}[X]$ étant

$$X^N - 1 = \prod_{d|N} \Phi_d,$$

par irréductibilité des polynômes cyclotomiques Φ_d, on en conclut que P est l'un des Φ_d pour $d|N$. ∎

Remarque. Dans la démonstration du théorème de Kronecker, voici une autre manière de démontrer que $P_k \in \mathbb{Z}[X]$: pour $l \in \{1, \dots, n\}$, le coefficient en X^{n-l} de P_k est égal à $(-1)^l \sigma_l(\alpha_1^k, \dots, \alpha_n^k)$. Or $\sigma_l(X_1^k, \dots, X_n^k) \in \mathbb{Z}[X_1, \dots, X_n]$ est un polynôme symétrique, donc il existe $S_l \in \mathbb{Z}[X_1, \dots, X_n]$ tel que

$$\sigma_l(X_1^k, \dots, X_n^k) = S_l(\sigma_1(X_1, \dots, X_n), \dots, \sigma_n(X_1, \dots, X_n)).$$

Comme $\sigma_j(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$, pour tout $j \in \{1, \dots, n\}$, on en déduit que $\sigma_l(\alpha_1^k, \dots, \alpha_n^k) \in \mathbb{Z}$.

Références

[Szp] Aviva Szpirglas, *Mathématiques L3*.