

Polynômes ter (version chantier)

Marc SAGE

<2015

Table des matières

1	Cosinus et rationnels	2
2	Ordres dans $GL_2(\mathbf{Z})$	2
3	Similtude et équivalence	3
4	un équivalent	3
5	Chevalley Warning	4
6	Nombre de polynômes irréductibles (unitaires) dans un corps fini	4
7	Tout sev de M_n disjoint de GL_n est de $\text{codim} \geq n$	5
8	Une somme trigo	7
9	Trouver des racines	8
10	Un peu de cyclotomie	8
11	signe d'un somme de cosinus	8
12	Exo d'anneaux	8

1 Cosinus et rationnels

Trouver tous les rationnels $r \in \mathbf{Q}$ tels que $\cos r\pi$ soit rationnel.

Solution proposée.

On connaît des candidats : 1, $\frac{1}{2}$ ou $\frac{1}{3}$. En se rappelant que pour chaque entier $n \geq 1$ on a $\cos nr = T_n(\cos r)$ où T_n est un polynôme à coefficients entiers¹, on voit que chaque rationnel de dénominateur 1, 2 ou 3 convient. Nous allons voir ce que ce sont les seuls – une fois mis sous forme irréductible.

Cet exercice se traite beaucoup plus vite à l'aide des polynômes cyclotomiques. Étant donnée une fraction $\frac{a}{b}$ sous forme irréductible, les racines du polynôme $X^2 - 2\cos\left(2\pi\frac{a}{b}\right)X + 1$ sont des racines b -ièmes primitives de l'unité, donc ce polynôme doit diviser le b -ième polynôme cyclotomique Φ_b . Lorsque $\cos\left(2\pi\frac{a}{b}\right)$ est rationnel, cette divisibilité s'exprime dans $\mathbf{Q}[X]$ où Φ_b est irréductible, ce qui force l'égalité des polynômes, d'où l'égalité des degrés $\varphi(b) = 2$, ce qui conduit à $b \in \{1, 2, 3, 6\}$. On se ramène à $a = 1$ grâce à Bézout.

Variante : déterminer les rationnels r tels que $\tan(\alpha\pi)$ soit rationnels.

2 Ordres dans $GL_2(\mathbf{Z})$

Quels sont les ordres (finis) possibles d'une matrice de $GL_2(\mathbf{Z})$? Exhiber des éléments ayant ces ordres.

Solution proposée.

Soit $A \in GL_2(\mathbf{Z})$ d'ordre fini ω . Son polynôme caractéristique $\chi_A \in \mathbf{Z}[X]$ s'écrit $X^2 - (\text{tr } A)X + \det A$ et se scinde sur $\mathbf{C}$ en $(X - \lambda)(X - \bar{\lambda})$. Puisque $A^\omega = 1$, la valeur propre λ est racine ω -ième de l'unité, ce qui s'écrit $\lambda = e^{2\pi i \frac{u}{\omega}}$ pour un $u \in \mathbf{Z}$. Alors la somme $\lambda + \bar{\lambda} = \text{tr } A$ vaut un entier $2\cos\frac{2u\pi}{\omega}$, ce qui montre que $\cos\left(\frac{2u}{\omega}\pi\right)$ est rationnel. D'après la question précédente, $\frac{2u}{\omega}$ est de la forme $v, \frac{v}{2}$ ou $\frac{v}{3}$ avec $v \in \mathbf{Z}$.

Tout ce qui suit n'est que discussion de cas. Quitte à restreindre le choix de u dans $[0, \omega[$, on pourra prendre le quotient $\frac{2u}{\omega}$ dans $[0, 2[$.

1. Cas $\frac{2u}{\omega} \in \mathbf{Z}$. Le quotient $\frac{2u}{\omega}$ est un entier de $[0, 2[$, donc vaut 0 ou 1. S'il est nul, u vaut 0, i. e. $\lambda = 1$, donc $\text{Sp } A = \{1\}$; puisque A est diagonalisable (car annulé par $X^\omega - 1$), elle vaut l'identité. Le cas $u = \frac{\omega}{2}$ donne de même $\lambda = -1$ puis $A = -1$.
2. Cas $\frac{2u}{\omega} \in \frac{1}{2}\mathbf{Z}$. Le rapport $\frac{4u}{\omega}$ est un entier de $]-2, 2[$. Le cas 0 venant d'être traité, u ne peut valoir que $\pm\frac{\omega}{4}$ ou $\frac{\omega}{2}$. Le cas médian $u = \frac{\omega}{2}$ équivaut à $\frac{2u}{\omega} = 1$, cas déjà traité. Les cas $u = \pm\frac{\omega}{4}$ donnent tous deux $\text{Sp } A = \{\pm i\}$.

Réciproquement, pour trouver une matrice A telle que $\chi_A = X^2 + 1$ (qui sera alors diagonalisable et d'ordre 4), on cherche à réaliser $\begin{cases} \text{tr } A = 0 \\ \det A = 1 \end{cases}$, par exemple $\begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}$.

3. Cas $\frac{2u}{\omega} \in \frac{1}{3}\mathbf{Z}$. Le rapport $\frac{6u}{\omega}$ est un entier non nul de $]-3, 3[$ donc u ne peut valoir que $\pm\frac{\omega}{6}, \pm\frac{\omega}{3}$ ou $\frac{\omega}{2}$. Le cas $\frac{\omega}{2}$ a déjà été traité.

Les cas $u = \pm\frac{\omega}{3}$ donnent $\text{Sp } A = \{j, \bar{j}\}$. Pour avoir $\chi_A = X^2 + X + 1$, on regarde $\begin{cases} \text{tr } A = -1 \\ \det A = 1 \end{cases}$, ce qui est réalisé pour $\begin{pmatrix} 1 & -1 \\ 3 & -2 \end{pmatrix}$.

Les cas $u = \pm\frac{\omega}{6}$ donnent $\text{Sp } A = \{-j, -\bar{j}\}$, de polynôme caractéristique $\chi_A = X^2 - X + 1$ dont un représentant est $\begin{pmatrix} 2 & -1 \\ 3 & -1 \end{pmatrix}$.

¹Les polynômes de Tchebycheff T_n peuvent être définis par la récurrence

$$(T_0, T_1) = (1, X) \text{ et } T_n = \frac{T_{n-1} + T_{n+1}}{2X}.$$

Conclusion : les ordres possibles sont (on donne un représentant pour chaque)

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \quad \begin{pmatrix} 2 & & & \\ & -1 & & \\ & & -1 & \\ & & & -1 \end{pmatrix} \quad \begin{pmatrix} 3 & & & \\ & 1 & -1 & \\ & & 3 & -2 \\ & & & -1 \end{pmatrix} \quad \begin{pmatrix} 6 & & & \\ & 2 & -1 & \\ & & 3 & -1 \\ & & & -1 \end{pmatrix}.$$

Remarque. Si l'on avait restreint la recherche aux ordres $\omega = p$ premiers, on pouvait aller beaucoup plus vite à l'aide des polynôme cyclotomiques Φ_n . En effet, le polynôme minimal μ_A divise le polynôme annulateur

$$X^p - 1 = \prod_{d|p} \Phi_d = \Phi_1 \Phi_p = (X - 1) \Phi_p,$$

donc (par irréductibilité de μ_A et Φ_p) égale $X - 1$ ou Φ_p . Le premier cas donne de suite $A = 1$. Dans le second, prendre les degrés donne $p - 1 = \varphi(p) \in \{1, 2\}$, d'où $p \in \{2, 3\}$.

3 Similtude et équivalence

Soit A et B deux matrices dans $M_n(K)$.

Montrer qu'elle sont semblables ssi $X - A$ et $X - B$ sont équivalentes dans $M_n(K[X])$.

Sens facile : si $A = PBP^{-1}$, alors $X - A = P(X - B)P^{-1}$.

Supposons $P(X - A) = (X - B)Q$. Une division euclidienne coefficient par coefficient donne

$$\begin{aligned} P &= (X - B)P_1 + R_1 \\ Q &= Q_1(X - A) + S_1 \end{aligned} \quad \text{où } R_1, S_1 \in M_n(K).$$

On calcule alors

$$\begin{aligned} (X - B)(P_1 - Q_1)(X - A) &= \underline{(X - B)P_1(X - A)} - (X - B)\underline{Q_1(X - A)} \\ &= (P - R_1)(X - A) - (X - B)(Q - S_1) \\ &= -R_1(X - A) - (X - B)(-S_1) \text{ par hypothèse} \\ &= X(S_1 - R_1) + R_1A - BS_1. \end{aligned}$$

À droite le degré est ≤ 1 , à gauche il est ≥ 2 (si $P_1 \neq Q_1$), donc tout est nul : $P_1 = Q_1$, $S_1 = R_1$ et $R_1A = BR_1$.

Montrons que R_1 est inversible. Une division euclidienne donne $P^{-1} = (X - A)P_2 + R_2$, d'où

$$\begin{aligned} 1 &= \underline{P(X - A)P_2} + \underline{PR_2} \\ &= (X - B)QP_2 + (X - B)P_1R_2 + R_1R_2 \\ &= (X - B)(Q + P_1)P_2 + R_1R_2. \end{aligned}$$

Prenant les degrés, ne reste à droite que $R_1R_2 = 1$, ce qui conclut.

4 un équivalent

équival de $\left[(1 + X + X^2)^n\right]_n$? il vaut $\int_0^\pi (1 + 2\cos)^n$ (eq intégrale des coeffe) puis le résultat $\frac{3^{n+\frac{1}{2}}}{2\sqrt{\pi n}}$

5 Chevalley Warning

Soit $q = p^\alpha$ ($\alpha \geq 1$) et $P \in \mathbf{F}_q[X_0, \dots, X_n]$ de degré $1 \leq d \leq n$ sans terme constant.

Montrer que P admet un zéro non trivial.

Généraliser : si une famille (P_i) de $\mathbf{F}_q[X_0, \dots, X_n]$ est telle que $\sum \deg P_i \leq n$, alors il y a un zéro commun à tous les P_i .

Rq : pour $x \in \mathbf{F}_q^{n+1}$, on a $P(x)^{q-1} = 0$ ou 1 , donc $\sum_x [1 - P(x)^{q-1}] = |Z(P)|$.

Lemme 1 : pour $k \geq 1$, on a $\sum_{\lambda \in \mathbf{F}_q} \lambda^k = \begin{cases} -1 & \text{si } q-1 \mid k \\ 0 & \text{si } q-1 \nmid k \end{cases}$. (prendre les série gén., cf. feuille arithmétique).

En corollaire : pour $0 \leq k < q-1$, cette somme est nulle (traiter le cas $k=0$ à part).

Lemme 2 : si $Q \in \mathbf{F}_q[X_0, \dots, X_n]$ est de degré $\leq n(q-1)$, alors $\sum_{x \in \mathbf{F}_q^{n+1}} Q(x) = 0$.

Raisonnons sur un monôme $Q(x) = x_0^{\alpha_0} \cdots x_n^{\alpha_n}$ de degré $\leq \deg Q$. On a $\sum_x Q(x) = (\sum_{x_0} x_0^{\alpha_0}) \cdots (\sum_{x_n} x_n^{\alpha_n})$. L'un des α_i est $< q-1$, sinon le degré de Q est $\sum \alpha_i \geq nq > n(q-1)$ car $n \geq 1$, d'où la nullité de la somme $\sum_{x_i} x_i^{\alpha_i}$ correspondante.

Conclusion : on écrit $\sum_x [1 - P(x)^{q-1}] = 0 - \sum_x P(x)^{q-1}$ avec $\deg P^{q-1} \leq n(q-1)$, donc $|Z(P)|$ est nul modulo q . Comme 0 est déjà zéro, $|Z(P)|$ est $\geq q$, CQFD.

Pour la généralisation, on part de l'identité $\sum_x \prod_i (1 - P_i(x)^{q-1}) = |\bigcap Z(P_i)|$ et on raisonne pareil.

6 Nombre de polynômes irréductibles (unitaires) dans un corps fini

Soit $q := p^\alpha$ où p est premier et $\alpha \geq 1$ un entier. Montrer que le nombre I_q^n de polynômes irréductibles unitaires de degré n sur $\mathbf{F}_q$ vaut

$$I_q^n = \frac{1}{n} \sum_{d \mid n} \mu(d) q^d$$

et en donner un équivalent à n fixé.

Solution proposée.

On veut $nI_q^n = \sum_{d \mid n} \mu(d) q^d$. Par la formule d'inversion de Möbius, il suffit de montrer que $q^n = \sum_{d \mid n} dI_n^d$ pour chaque $n \geq 1$. Pour cela, il suffit de montrer que $X^{q^n} - X$ est le produit de tous les polynômes irréductibles unitaires de degré divisant n (prendre alors le degré)

Nous proposons deux méthodes.

Soit P irréductible unitaire de degré $d \mid n$. Soit ξ une racine de P dans un corps de rupture $\mathbf{F}_q(\xi)$. L'extension $\mathbf{F}_q \hookrightarrow \mathbf{F}_q(\xi)$ est de degré $\deg P = d$, d'où $|\mathbf{F}_q(\xi)| = |\mathbf{F}_q|^d = q^d$ et $\xi^{q^d} = \xi$ (c'est Lagrange au groupe K^* pour K corps). Par itération, $\xi^{q^{kd}} = \xi$ pour chaque $k \geq 1$, en particulier pour $k = \frac{n}{d}$, d'où $\xi^{q^n} = \xi$, ce qui montre que $X^{q^n} - X$ est un polynôme annulateur de ξ , donc multiple de P , CQFD.

Soit P diviseur irréductible unitaire de $X^{q^n} - X$ de degré d . On sait que $X^{q^n} - X = \prod_{\lambda \in \mathbf{F}_{q^n}} (X - \lambda)$, donc P a une racine ξ dans $\mathbf{F}_{q^n}$, d'où une extension $\mathbf{F}_q(\xi) \hookrightarrow \mathbf{F}_{q^n}$. Or, $|\mathbf{F}_q(\xi)| = q^{\deg P} = q^d$, d'où une extension $\mathbf{F}_{q^d} \hookrightarrow \mathbf{F}_{q^n}$, ce qui force $d \mid n$, CQFD.

Enfin, $X^{q^n} - X$ n'admet aucun facteur irréductible multiple, sinon il aurait une racine multiple dans $\mathbf{F}_{q^n}$, donc annulerait sa dérivée -1 , ce qui est absurde.

Posons $\zeta_q(s) := \sum \frac{1}{|P|^s}$ où $|P| := q^{\deg P}$, la somme portant sur tous les polynômes unitaires de $\mathbf{F}_q[X]$. En sommant selon le degré de P , on obtient $\sum_{d \geq 0} q^d \frac{1}{q^{ds}}$ qui converge pour $\operatorname{Re} s > 1$ vers $\frac{1}{1 - \frac{1}{q^s - 1}}$. Comme pour la série harmonique, on a un produit Eulérien

$$\sum \frac{1}{|P|^s} = \prod_{\substack{P \text{ unitaire} \\ \text{irréductible}}} \frac{1}{1 - \frac{1}{|P|^s}} = \prod_{d \geq 1} \frac{1}{\left(1 - \frac{1}{q^{ds}}\right)^{I_q^d}}.$$

Posant $u := q^{-s}$ (on a les eq $\operatorname{Re} s > 1$ ssi $|u| < 1$), on en déduit

$$\frac{1}{1-qu} = \zeta_q(s) = \prod_{d \geq 1} \frac{1}{(1-u^d)^{I_q^d}},$$

d'où en prenant la dérivée logarithmique et en multipliant par u

$$\begin{aligned} \frac{qu}{1-qu} &= \sum_{d \geq 1} \frac{dI_q^d u^d}{1-u^d} \\ \sum_{n \geq 1} q^n u^n &= \sum_{d, \delta \geq 1} dI_q^d u^{d\delta} = \sum_{n \geq 1} \left(\sum_{dd'=1} dI_q^d \right) u^n. \end{aligned}$$

Pour l'équivalent, on ne regarde que le dernier terme $\frac{q^n}{n}$: en effet, le reste est négligeable :

$$\sum_{dd' < n} \mu(d) q^{d'} \leq \sum_{d'=1}^{\lfloor \frac{n}{2} \rfloor} q^{d'} = \frac{q^{\lfloor \frac{n}{2} \rfloor + 1} - q}{q-1} \leq \frac{q^{\frac{n}{2}}}{q-1} = o(q^n).$$

7 Tout sev de M_n disjoint de GL_n est de $\operatorname{codim} \geq n$

Soit $n \geq 1$ un entier.

On montre que le polynôme $T^n + X$ de $k(X)[T]$ est irréductible et on utilise ce résultat pour montrer qu'un sev de M_n disjoint de GL_n est de dimension $\leq n^2 - n$.

Lemme.

1. Montrer que $T^n + X$ est irréductible dans $k[X][T]$.
2. On définit le contenu d'un polynôme $A = \sum a_i T^i$ de $k[X][T]$ par

$$c(A) := \operatorname{pgcd}\{a_i\}.$$

Si $c(A) = 1 = c(B)$, montrer que $c(AB) = 1$.

3. Conclure.

Théorème.

Soit V un sev de M_n disjoint de GL_n .

1. Montrer qu'il suffit d'exhiber une sous-algèbre de $M_n(K)$ de dimension n qui est un corps.
2. Soit P un polynôme irréductible de degré n . Conclure en considérant l'algèbre engendrée par la matrice compagnon de P .
3. Conclure lorsque K est fini.
4. Conclure lorsque K est de la forme $k(X)$ où k est un corps infini.
5. Conclure.

Solution proposée (lemme).

1. Supposons que $T^n + X$ se factorise en un produit $\sum_{i=0}^p a_i T^i \sum_{j=0}^q b_j T^j$ où les a_i, b_j sont dans $k[X]$. Il vient en développant

$$T^n + X = a_0 b_0 + (a_0 b_1 + a_1 b_0) T + (a_0 b_2 + a_1 b_1 + a_2 b_0) T^2 + \cdots + a_p b_q T^{p+q}.$$

Quitte à diviser par $\frac{a_0 b_0}{X} = 1$ en répartissant le a_0 dans $\sum_{i=0}^p a_i T^i$ et le $\frac{b_0}{X}$ dans $\sum_{j=0}^q b_j T^j$, on peut supposer $(a_0, b_0) = (1, X)$. Le terme en T nous dit alors que b_1 est multiple de X , puis le terme en T^2 que b_2 aussi... ainsi de suite jusqu'au coefficient $a_0 b_q + \cdots + a_q b_0$ de T^q qui nous donne $X \mid b_q$. Il en résulte que X divise $\sum_{j=0}^q b_j T^j$, donc $T^n + X$, d'où en spécialisant X en 0 l'égalité $T^n = 0$, ce qui est impossible.

2. Par l'absurde, supposons que P soit un diviseur irréductible de tous les coefficients de AB . En explicitant $A = \sum a_i X^i$ et $B = \sum b_i X^i$, on peut considérer un plus petit entier $\alpha \leq \deg A$ tel que P ne divise pas a_α (il existe sinon P diviserait $c(A) = 1$) et de même $\beta \leq \deg B$ minimal pour la propriété $P \mid b_\beta$. Le coefficient en $T^{\alpha+\beta}$ de AB s'écrit alors $a_\alpha b_\beta + \sum_{i+j=\alpha+\beta}^{i<\alpha \text{ ou } j<\beta} a_i b_j$, donc vaut $a_\alpha b_\beta$ modulo P , donc ce dernier divise $a_\alpha b_\beta$; comme il est irréductible, il divise a_α ou b_β , contredisant les définitions de α et β .
3. Supposons à présent $T^n + X = AB$ avec A, B à coefficients dans $K = k(X)$. Factorisant par un ppcm des dénominateurs (en X) des coefficients de A , puis par un pgcd des numérateurs restants, et en simplifiant éventuellement la fraction factorisée, on peut écrire $A = \frac{a}{\alpha} A^*$ où a et α sont premiers entre eux et où A est un polynôme à coefficients dans $k[X]$ tel que $c(A) = 1$. On écrit de même $B = \frac{b}{\beta} B^*$. On a donc $\alpha\beta(T^n + X) = abA^*B^*$. Prenant le contenu, il vient

$$\alpha\beta = \alpha\beta \cdot c(T^n + X) = c[\alpha\beta(T^n + X)] = c[abA^*B^*] = ab \cdot c(A^*B^*) \stackrel{\text{question précédente}}{=} ab.$$

On retombe ainsi sur une factorisation $T^n + X = A^*B^*$ dans $k[X][T]$ et la première question conclut.

Solution proposée (théorème).

1. Soit A une telle algèbre. Les éléments non nuls de cette algèbre étant inversibles, aucun d'eux ne peut se trouver dans V , de sorte que $V \cap A = \{0\}$. En prenant les dimensions, on trouve

$$\dim V = \dim(V + A) - \dim A \leq n^2 - \dim A = n^2 - n, \text{ CQFD.}$$

2. Notons C la matrice compagnon de P . À l'aide d'une division euclidienne par P (lequel annule C), on voit que l'algèbre $K[C] = \text{Vect}\{1, C, C^2, \dots, C^{n-1}\}$ est de dimension $\leq n$. Par ailleurs, en notant $(e_0, \dots, e_{n-1})$ la base canonique de K^n , on lit dans la k -ième colonne de C la relation $C^k e_0 = e_k$ pour chaque $k < n$; par conséquent, partant d'une relation de liaison $\sum_{0 \leq k < n} \lambda_k C^k = 0$, évaluer en e_0 donne $\sum_{0 \leq k < n} \lambda_k e_k = 0$, d'où $\vec{\lambda} = 0$. Finalement, l'algèbre $K[C]$ est de dimension n et il suffit (d'après la question précédente) de montrer qu'elle est un corps.

Soit $A(C)$ non nul dedans avec $A \in K_{n-1}[X]$. Puisque P est irréductible et $A \neq 0$ (sinon $A(C) = 0$), les polynômes A et P sont premiers entre eux, d'où par Bézout une écriture $AU + PV = 1$; évaluer en C donne $A(C)U(C) = 1$, d'où le caractère inversible de $A(C)$, CQFD.

3. Il suffit d'exhiber un polynôme irréductible de degré n arbitraire. Or, $\mathbf{F}_{q^n}^*$ est cyclique, d'où $\mathbf{F}_q[\alpha] = \mathbf{F}_{q^n}^* \cup \{0\} = \mathbf{F}_{q^n}$, de sorte que α est algébrique de degré n sur $\mathbf{F}_q$, donc de poly min répondant à la question.
4. Il suffit d'exhiber un polynôme irréductible de degré arbitraire : on nous donne $T^n + X$ pour chaque $n \geq 1$.
5. On peut toujours plonger un corps K dans le corps des fractions $K(X)$. Pour conclure, il suffit donc de montrer que, pour $d \geq 0$ donné, la propriété « être un sev de M_n de dimension d disjoint de GL_n » est invariante par extension des scalaires (sur un corps déjà infini).

Soit $V \subset M_n(K)$ un tel sev et $K \hookrightarrow L$ une extension de corps. Pour obtenir un L -sev de $M_n(L)$, il faut remplacer V par $LV := \text{Vect}\{\lambda v\}_{v \in V}^{\lambda \in L}$. Pour conserver la dimension, on observe qu'une K -base $(v_1, \dots, v_d)$ de V est aussi une L -base² de LV , d'où $\dim_L LV = \dim_K V$. Par ailleurs, le polynôme $\det\left(\sum_{i=1}^d X_i v_i\right)$ est nul sur K^d par hypothèse sur V , donc est le polynôme nul (car K est infini), donc s'annule sur L^d , de sorte qu'aucune matrice de LV n'est inversible, ce qui conclut.

Un autre argument, spécifique à l'extension $K \hookrightarrow K(X)$ avec K infini est le suivant. Soit $\sum F_i v_i \in \text{Vect } K(X)V$ dans $GL_n(K(X))$, mettons $\sum F_i v_i \times (G_{k,l}) = 1$. Il suffit d'évaluer pour obtenir un élément de V dans $GL_n(K)$, contradiction. Puisque K est infini, on peut choisir un point autre que les pôles des F_i et des $G_{k,l}$, ce qui conclut.

² Il est clair que

$$\text{Vect}_L\{v_1, \dots, v_d\} = LV.$$

Il reste à montrer la L -liberté des v_i . Considérons une K -base (e_j) de L . Une relation de L -liaison $\sum \lambda_i v_i = 0$ se réécrit

$$0 = \sum_i \sum_j \lambda_j^i e_j v_i = \sum_j e_j \left(\sum_i \lambda_j^i v_i \right)$$

où les λ_j^i sont dans K . Par K -liberté des e_j , on a $\sum_i \lambda_j^i v_i = 0$ pour tout j , d'où par K -liberté des v_i la nullité de tous des λ_j^i , donc des λ_i , CQFD.

Remarque. L'irréductibilité de $T^n + X$ est un cas particulier du critère d'Eisenstein suivant : si $P = a_n X^n + \dots + a_1 X + a_0$ est un polynôme à coefficients dans un anneau intègre A , si $\mathfrak{p}$ est un idéal premier de A contenant $a_0, a_1, \dots, a_{n-1}$ mais pas a_n et tel que a_0 ne s'écrit pas comme produit de deux éléments de $\mathfrak{p}$, alors P est irréductible en tant que polynôme à coefficients dans le corps des fractions de A . Voir le cours d'algèbre de D. Perrin pour plus de détails³.

8 Une somme trigo

EXO DUR : fixons $l \notin \frac{n}{2}\mathbb{Z}$. Calculer $S = \sum_{\substack{0 \leq k < n \\ k \pm l \not\equiv 0 \pmod{n}}} \frac{1}{\sin\left(\frac{k+l}{n}\pi\right) \sin\left(\frac{k-l}{n}\pi\right)}$.

DEM : On linéarise $\sin\left(\frac{k+l}{n}\pi\right) \sin\left(\frac{k-l}{n}\pi\right) = \frac{1}{2} \left(\cos\theta - \cos\frac{2k\pi}{n}\right)$ où $\theta := \frac{2\pi l}{n}$, d'où

$$S = \sum_{\substack{0 \leq k < n \\ k \neq l, n-l}} \frac{2}{\cos\theta - \cos\frac{2k\pi}{n}}$$

On reconnaît $\sum_{P(\lambda)=0} \frac{1}{(\cos\theta)-\lambda} = \frac{P'}{P}(\cos\theta)$ où $P = \prod_{\substack{0 \leq k < n \\ k \neq 0, n-l}} \left(X - \cos\frac{2k\pi}{n}\right) = \frac{\cos(n \arcs X) - 1}{(X - \cos\theta)^2}$ ($\cos nx - 1$ est polynôme en $\cos x$ s'annulant en $x = \theta$ et dont la dérivée s'annule aussi (car $\sin\theta \neq 0$) en $x = \theta$, donc θ racine double, donc $\frac{\cos(n \arcs X) - 1}{(X - \cos\theta)^2}$ est bien le polynôme P). Notons DL la dérivée log. Alors

$$\begin{aligned} \frac{P'}{P}(\cos x) &= \frac{P'(\cos x)(-\sin x)}{P(\cos x)(-\sin x)} = \frac{1}{-\sin x} \frac{\frac{\partial}{\partial x} P(\cos x)}{P(\cos x)} = \frac{1}{-\sin x} DL(P(\cos x)) \\ &= \frac{1}{-\sin x} (DL(\cos(nx) - 1) - 2DL(\cos x - \cos\theta)) \\ &= \frac{1}{-\sin x} \left(\frac{-n \sin nx}{\cos(nx) - 1} - 2 \frac{-\sin x}{\cos x - \cos\theta} \right) \end{aligned}$$

On a deux formes indéterminées. Levons la première : notant $X := x - \theta$

$$\begin{aligned} \sin nx &= \sin nx - \sin n\theta = nX + o(X^2) \\ \cos nx - 1 &= \frac{-n^2}{2} X^2 + o(X^3), \text{ d'où} \\ \frac{-n \sin nx}{\cos(nx) - 1} &= \frac{n^2 X + o(X^2)}{\frac{n^2}{2} X^2 + o(X^3)} = \frac{2}{X} \frac{1 + o(X)}{1 + o(X)} = \frac{2}{X} + o(1). \end{aligned}$$

La seconde donne

$$\begin{aligned} \frac{-2 \sin x}{\cos x - \cos\theta} &= 2 \frac{-\sin\theta + o(1)}{-X \sin\theta - X^2 \frac{\cos\theta}{2} + o(X^2)} = \frac{2}{X} \frac{1 + o(1)}{1 + X \frac{\cos\theta}{2 \sin\theta} + o(X)} \\ &= \frac{2}{X} \left(1 - X \frac{\cos\theta}{2 \sin\theta} + o(X) \right) = \frac{2}{X} - \frac{\cos\theta}{\sin\theta} + o(1). \end{aligned}$$

Ainsi, on peut conclure

$$\frac{P'}{P}(\cos x) = \frac{1}{-\sin x} \left(\frac{2}{X} + o(1) - \left(\frac{2}{X} - \frac{\cos\theta}{\sin\theta} + o(1) \right) \right) \longrightarrow -\frac{\cos\theta}{\sin^2\theta}$$

et la somme cherchée est le double $-\frac{2 \cos\theta}{\sin^2\theta}$
PB signe ? ? ? ?

³ Par exemple, $X^2 - 7X + 14$ vérifie les conditions pour l'idéal premier (7) de l'anneau intègre $\mathbf{Z}$, donc est irréductible sur $\mathbf{Q}[X]$ (on le savait : il est de degré ≤ 3 et n'a pas de racines sur $\mathbf{Q}$). Autre exemple : pour tout p premier, le polynôme cyclotomique

$$\Phi_p := 1 + X + X^2 + \dots + X^{p-1}$$

est irréductible : appliquer le critère d'Eisenstein à $\Phi_p(X+1)$.

9 Trouver des racines

Soit un polynôme réel $X^n + nX^{n-1} + \dots$ dont les racines vérifient $\sum \lambda_i^{6584720} = n$. Trouver les autres coeff.
 dem : $\frac{\sum |\lambda_i|^{380}}{n} = 1 = \left| \frac{\sum \lambda_i}{n} \right|^{27090} \leq \left(\frac{\sum |\lambda_i|}{n} \right)^{730}$, donc égal partout ; comme $\sum \lambda_i = -n$, tous les λ_i sont -1 ,
 d'où $P = (X + 1)^n$.

10 Un peu de cyclotomie

On fixe $n \geq 1$ un entier. Dans les trois premières questions, a désigne un entier relatif et p un premier.

1. On note ω l'ordre de a modulo p . Montrer que $p \mid \Phi_\omega(a)$.
2. On suppose $p \nmid n$. Montrer que $p \mid \Phi_n(a)$ ssi a est d'ordre n dans $\mathbf{F}_p^*$.
3. Montrer que $\mathbf{F}_p^*$ possède un élément d'ordre n ssi $p = 1 \pmod{n}$.
4. En déduire qu'il y a une infinité de premiers $p = 1 \pmod{n}$.

Solution proposée.

1. Par définition de ω , le premier p divise $a^\omega - 1 = \prod_{d \mid \omega} \Phi_d(a)$, donc p divise un certain $\Phi_{d_0}(a)$, d'où la nullité du produit $\prod_{d \mid d_0} \Phi_d(a) = a^{d_0} - 1$, d'où par minimalité de ω l'égalité $d_0 = \omega$, CQFD.
2. Le sens $\Leftarrow$ découle de la question 1.
 Partant de $p \mid \Phi_n(a)$, il vient de même $a^n = 1$ dans $\mathbf{F}_p^*$, d'où $\omega \mid n$; si la divisibilité était stricte, les polynômes Φ_n et Φ_ω seraient distincts et a serait alors racine multiple de $X^n - 1 = \Phi_n \Phi_\omega \dots$ dans $\mathbf{F}_p[X]$, ce qui est impossible vu que $X^n - 1$ est premier avec sa dérivée (c'est là qu'intervient l'hypothèse $p \nmid n$).
3. On a les implications $p = 1 \pmod{n} \implies n \mid p - 1 = |\mathbf{F}_p^*|$ cyclique $\implies$ il y a sg d'ordre $n \implies \exists a$ d'ordre n . Réciproquement, a d'ordre $n \implies n \mid p - 1$ (PTF) $\iff p = 1 \pmod{n}$.
4. Soient par l'absurde $p_1, \dots, p_r$ les premiers $p = 1 \pmod{n}$. On forme l'entier $N := np_1 \dots p_r$. Pour a assez grand, $\Phi_N(a)$ est grand en valeur absolue donc admet un diviseur premier p , qui doit être $p = 1 \pmod{N}$, *a fortiori* $p = 1 \pmod{n}$, donc p est l'un des p_i , d'où $p_i = 0 \pmod{N}$ et contradiction.

11 signe d'une somme de cosinus

signe de $\sum a_i \cos \pi r_i$ où $a_i \in \mathbf{Z}$ et $r_i \in \mathbf{Q}$?

on écrit $r_i = \frac{2n_i}{d}$ avec le même dénom, d'où $\cos \pi r_i = \cos \left(n_i \frac{2\pi}{d} \right) = T_{n_i} \left(\cos \left(\frac{2\pi}{d} \right) \right)$.

On calcule ensuite le poly min μ de $\cos \left(\frac{2\pi}{d} \right)$ l'aide des Φ_d .

Puis $\sum a_i T_{n_i} = Q\mu + R$

12 Exo d'anneaux

Soit A anneau unitaire. Soit deux éléments non nilpotents de somme 1 dont le produit, commutatif, est nilpotent Mq qu'il y a un idempotent non trivial. Que se passe si l'un des éléments est nilpotent ?

on écrit $a + b = 1$ avec $0 = (ab)^n = (a^2 - a)^n$. Si $n = 1$, a fonctionne (a est autre que 0 ou 1 sinon a ou b est nul). Supposons $n \geq 2$.

on cherche cet idempotent à partir de a : le calcul annelé étant les polynômes à coefficients dans Z , on cherche un $i := P(a)$ tel que $P(a)(P(a) - 1) = 0$.

Ce sera le cas si $P(a)$ contient du a^n et $P(a) - 1$ du $(a - 1)^n$. Ce sera réalisé si $P = X^n Q$ et $P - 1 = (X - 1)^n R$, d'où $(X + 1)^n Q(X + 1) = P(X + 1) = X^n R(*) + 1$.

Synthèse : On prend donc Q tq $(X+1)^n Q = O(X^n)$ et on pose $P = X^n Q (X-1)$.

Pour éviter les cas triviaux $i = 0$ ou 1 , on montre que $i - a$ est nilpotent. Il suffit de mq $a(a-1)$ le divise, donc de mq X et $X-1$ divisent $P-X$. Or $P-X = O(X^n) - X$ multiple de X , et $P-X = 1 + O(X-1)^n + 1$ multiple de $X-1$, CQFD.

Si a est nilpotent, on a un ceg. Dans $A = K[X]/X^2$ les éléments X et $1-X$ vérifient les conditions sauf que X est nilpotent, mais il n'y a pas d'idempotent non trivial (si $(aX+b)^2 = aX+b$, alors $2ab = a$ et $b^2 = b$, d'où $b = 1$ ou 0 et $a = 0$)

Soit $f, g \in A$ engendrant pour idéal tout A . Alors le morphisme $A \left[\frac{1}{f} \right] \times A \left[\frac{1}{g} \right] \longrightarrow A \left[\frac{1}{fg} \right]$ est de noyau A . Appliquons à $f+g=1$ et fg nilpotent. Alors $A \left[\frac{1}{fg} \right]$ est nul, donc $A \simeq A \left[\frac{1}{f} \right] \times A \left[\frac{1}{g} \right]$ est décomposable, d'où $\lambda := (1, 0)$ idempotent non trivial.

Montrons que $\lambda - a$ est nilpotent. Pour cela, il suffit de voir que l'image de $\lambda - a$ dans $A \left[\frac{1}{a} \right]$ (resp. $A \left[\frac{1}{1-a} \right]$) est nilpotente.

En effet, dans $A \left[\frac{1}{a} \right]$, $\lambda - a$ devient $1 - a$ qui est nilpotent si et seulement si $a(1-a)$ l'est vu que a est inversible (dans $A \left[\frac{1}{a} \right]$!); de même, dans $A \left[\frac{1}{1-a} \right]$ $\lambda - a$ devient $0 - a$ qui est nilpotent si et seulement si $(1-a)(-a)$ l'est vu que $1-a$ est inversible.