Polynômes

Vincent Pilaud

2007

Dans tout ce texte, A désigne un anneau factoriel, k un corps (commutatif), et $A[X]$ (resp. $k[X]$) l'algèbre des polynômes à une indéterminée sur A (resp. k).

1 Racines

1.1 Définitions élémentaires

Définition 1. *Soit $P \in k[X]$ et $a \in k$. On dit que a est une* racine *de P si $P(a) = 0$, ou de manière équivalente si $X - a$ divise P. On appelle* multiplicité *de a le plus grand entier μ tel que $(X-a)^\mu$ divise P.*

Proposition 1. *Si $P \in k[X]$ admet $a_1, \dots, a_\ell$ pour racines, de multiplicités respectives $\mu_1, \dots, \mu_\ell$, alors il existe $Q \in k[X]$ tel que $P = Q \prod^\ell (X - a_i)^{\mu_i}$.*

En particulier, seul le polynôme nul admet strictement plus de racines que son degré.

Définition 2. *On dit qu'un polynôme P est scindé si on peut écrire $P = \lambda \prod^\ell (X - a_i)^{\mu_i}$, avec $\ell, \mu_1, \dots, \mu_\ell \in \mathbb{N}$ et $\lambda, a_1, \dots, a_\ell \in k$.*

1.2 Quelques exemples

Les polynômes du second degré. Soient a, b et c trois réels, avec $a \neq 0$. Alors le polynôme

$$P = aX^2 + bX + c = a(X + \frac{b}{2a})^2 - \frac{b^2 - 4ac}{4a^2}$$

admet deux racines réelles $\frac{-b+\sqrt{b^2-4ac}}{2a}$ et $\frac{-b-\sqrt{b^2-4ac}}{2a}$ (resp. une racine double $\frac{-b}{2a}$, resp. aucune racine réelle) lorsque $b^2 - 4ac > 0$ (resp. $b^2 - 4ac = 0$, resp. $b^2 - 4ac < 0$).

Le déterminant. Le déterminant d'une matrice $M = [m_{i,j}]_{1 \leq i,j \leq n}$ est un polynôme (à plusieurs indéterminées) en les coefficients de M, donné par la formule

$$\det(M) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} m_{i,\sigma(i)}.$$

Les deux exemples suivants montrent des utilisations du caractère polynomial du déterminant :

Proposition 2. *Soient $a_0, \dots, a_n \in k$. Le* déterminant de Vandermonde *de $a_0, \dots, a_n$ est donné par*

$$V(a_0, \dots, a_n) = \det \begin{pmatrix} 1 & a_0 & \dots & a_0^n \\ 1 & a_1 & \dots & a_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \dots & a_n^n \end{pmatrix} = \prod_{1 \leq i < j \leq n} a_j - a_i.$$

On montre ce résultat par récurrence sur n. Il est évident pour $n = 1$. Supposons maintenant le résultat vrai au rang n. On considère le déterminant $V(a_0, \dots, a_n, X)$. Un développement par rapport à la première colonne assure que $V(a_0, \dots, a_n, X)$ est un polynôme en X, de degré $n+1$ dont le coefficient dominant est $V(a_0, \dots, a_n)$. Par ailleurs, il s'annule en tous les a_i. Par conséquent, $V(a_0, \dots, a_n, X) = V(a_0, \dots, a_n) \prod_{i=0}^{n} (X - a_i)$, ce qui donne le résultat grâce à l'hypothèse de récurrence.

Définition 3. *On appelle* polynôme caractéristique *d'une matrice $M \in M_n(k)$ le polynôme $\chi_M(X) = \det(M - X\mathrm{I}_n)$. Ses racines sont exactement les* valeurs propres *de M, ie. les scalaires $\alpha \in k$ tels qu'il existe un* vecteur propre *$x \in k^n \setminus \{0\}$ tel que $Mx = \lambda x$.*

Exemple.

1. L'ensemble des matrices inversibles de $M_n(\mathbb{R})$ est dense dans $M_n(\mathbb{R})$
2. Soient $A, B \in M_n(\mathbb{R}) \subset M_n(\mathbb{C})$. A et B sont semblables dans $\mathbb{R}$ si et seulement si elles sont semblables dans $\mathbb{C}$.

Les suites récurrentes linéaires.

Définition 4. *On dit qu'une suite $(u_n)_{n\in\mathbb{N}} \in k^{\mathbb{N}}$ est* récurrente linéaire *s'il existe $p \in \mathbb{N}^*$ et $v_0, \dots, v_p \in k$ tels que pour tout $i \in \mathbb{N}$,*

$$u_{i+p+1} = \sum_{j=0}^{p} v_j u_{i+j}.$$

Le polynôme $X^{p+1} - \sum_{j=0}^{p} v_j X^j$ est appelé polynôme générateur *de la suite $(u_n)_{n\in\mathbb{N}}$.*

Proposition 3. *Soit $P = \prod^{\ell}(X - a_i)_i^{\mu}$ un polynôme générateur scindé d'une suite récurrente linéaire $(u_n)_{n\in\mathbb{N}}$. Alors il existe $\lambda_{1,1}, \dots, \lambda_{\ell,\alpha_\ell} \in k$, dépendant des conditions initiales, tels que pour tout $n \in \mathbb{N}$,*

$$u_n = \sum_{i=1}^{\ell} \sum_{j=1}^{\mu_i} \lambda_{i,j} n^{j-1} a_i^n.$$

Exemple. La *suite de Fibonacci* définie par $u_0 = u_1 = 1$ et $u_{n+2} = u_{n+1} + u_n$ est donnée par

$$u_n = \lambda \left(\frac{1+\sqrt{5}}{2}\right) + \mu \left(\frac{1-\sqrt{5}}{2}\right), \quad \text{avec} \quad \lambda = \frac{1}{2} + \frac{1}{2\sqrt{5}} \text{ et } \mu = \frac{1}{2} - \frac{1}{2\sqrt{5}}.$$

Les polynômes interpollateurs de Lagrange.

Proposition 4. *Soient $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in k$ avec $\alpha_i \neq \alpha_j$ pour tout $i \neq j$. Le polynôme*

$$L(X) = \sum_{i=1}^{n} \beta_i \prod_{j\neq i} \frac{X - \alpha_j}{\alpha_i - \alpha_j}$$

est l'unique polynôme de degré strictement inférieur à n tel que $L(\alpha_i) = \beta_i$ pour tout $1 \leq i \leq n$.

Les polynômes de Tchebychev.

Proposition 5. *Pour tout entier n, il existe un unique polynôme $T_n \in \mathbb{R}[X]$ de degré n, appelé* n-ième polynôme de Tchebychev*, qui vérifie $T_n(\cos\theta) = \cos(n\theta)$, pour tout $\theta \in \mathbb{R}$.*

Ces polynômes vérifient la formule de récurrence suivante :

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

1.3 Relations entre les coefficients et les racines d'un polynôme

1.3.1 Polynômes symétriques élémentaires

Définition 5. *Soient $p \leq n$ deux entiers. On appelle* p-ième polynôme symétrique élémentaire de $A[X_1, \dots, X_n]$ *le polynôme*

$$\Sigma_{p,n} = \sum_{1\leq i_1 < \dots < i_p \leq n} X_{i_1} \dots X_{i_p}.$$

Par exemple, $\Sigma_{1,1} = X_1$, $\Sigma_{1,2} = X_1 + X_2$, $\Sigma_{2,2} = X_1X_2$, $\Sigma_{1,3} = X_1 + X_2 + X_3$, $\Sigma_{2,3} = X_1X_2 + X_1X_3 + X_2X_3$, $\Sigma_{3,3} = X_1X_2X_3$, etc.

Théorème 1 (Relations racines-coefficients)**.** *Soit $P = c_nX^n + \dots + c_1X + c_0 = c_n \prod_{i=1}^{n}(X - a_i)$ un polynôme scindé (avec $c_n \neq 0$). Alors pour tout $1 \leq p \leq n$, le $(n-p)$-ième coefficient de P est donné par*

$$c_{n-p} = (-1)^p c_n \Sigma_{p,n}(a_1, \dots, a_n).$$

Exemple. Soient σ et π deux réels. Les deux racines du polynôme $X^2 - \sigma X + \pi$, lorsqu'elles existent, forment l'unique couple de réels dont la somme vaut σ et le produit π.

1.3.2 Localisation de racines

Théorème 2. *Soit $P = X^n + c_{n-1}X^{n-1} + \ldots + c_1X + c_0$ un polynôme unitaire de $\mathbb{C}[X]$ de racines $a_1, \ldots, a_n \in \mathbb{C}$. On note $M = \max\{|a_i| \mid 1 \leq i \leq n\}$. Si $\delta \in \mathbb{R}^+$ vérifie $\delta^n \geq |c_{n-1}|\delta^{n-1} + \ldots + |c_1|\delta + |c_0|$, alors $M \leq \delta$.*

En effet, soient $\delta \in \mathbb{R}^+$ vérifiant $\delta^n \geq |c_{n-1}|\delta^{n-1} + \ldots + |c_1|\delta + |c_0|$ et $z \in \mathbb{C}$ avec $|z| > \delta$. Alors

$$|P(z)| = |z^n + \sum_{i=0}^{n-1} c_i z^i| \geq |z|^n - \left|\sum_{i=0}^{n-1} c_i z^i\right| \geq |z|^n - \sum_{i=0}^{n-1} |c_i||z|^i = \left(\frac{|z|}{\delta}\right)^n \left(\delta^n - \sum_{i=0}^{n-1} |c_i|\delta^i \left(\frac{\delta}{|z|}\right)^{n-i}\right) > 0$$

Ainsi, toute racine de P a un module inférieur ou égal à δ.

Exemple. On obtient en particulier les inégalités suivantes :

(i) $M \leq \max(1, \sum_{i=0}^{n-1} |c_i|)$,

(ii) $M \leq 1 + \max\{|c_i| \mid 0 \leq i \leq n-1\}$,

(iii) $M \leq |1 - c_{n-1}| + |c_{n-1} - c_{n-2}| + \ldots + |c_1 - c_0| + |c_0|$,

(iv) Si tous les c_i sont non nuls, alors $M \leq \max\left\{2|c_{n-1}|, 2\frac{|c_{n-2}|}{|c_{n-1}|}, \ldots, 2\frac{|c_0|}{|c_1|}\right\}$.

1.3.3 Continuité des racines

Théorème 3 (Continuité des racines d'un polynôme complexe)**.** *Soit U_n l'ensemble des polynômes de $\mathbb{C}[X]$ de degré exactement n (c'est un ouvert de $\mathbb{C}_n[X]$ que l'on munit de la topologie induite). Soit V_n le quotient de $\mathbb{C}^n$ par le groupe symétrique $\mathfrak{S}_n$, munit de la topologie quotient. Alors l'application $\phi : U_n \to V_n$, qui a un polynôme associe (la classe de) ses racines, est continue.*

Remarque. La topologie de V_n est métrisée par la distance définie par :

$$d(A, B) = \min_{\sigma \in \mathfrak{S}_n} \{ \max_{i=1,\ldots,n} |a_i - b_{\sigma(i)}| \},$$

où $(a_1, \ldots, a_n)$ (resp. $(b_1, \ldots, b_n)$) désigne un représentant quelconque de la classe d'équivalence A (resp. B).

2 Polynômes irréductibles

2.1 Définitions

Définition 6. *On dit qu'un polynôme $P \in A[X]$ est* irréductible *si*

(i) $P \notin A[X]^* = A^*$,

(ii) $\forall Q, R \in A[X]$ *tels que* $P = QR$, *on a* $Q \in A^*$ *ou* $R \in A^*$.

Remarque. L'hypothèse de factorialité de l'anneau A implique que $A[X]$ est factoriel. Par ailleurs, lorsque k est un corps, $k[X]$ est euclidien, donc factoriel. Ainsi, on se place toujours dans un cadre qui assure l'existence et l'unicité de la décomposition d'un polynôme en produits de facteurs irréductibles.

Exemple.

(a) Sur un corps algébriquement clos, les seuls polynômes irréductibles sont les polynômes de degré 1.

(b) Sur $\mathbb{R}$, les polynômes irréductibles sont les polynômes de degré 1 et les polynômes de degré 2 de la forme $aX^2 + bX + c$, avec $a \neq 0$ et $b^2 - 4ac < 0$.

(c) Nous verrons plus loin que sur $\mathbb{Q}$ ou sur un corps fini, il existe des polynômes irréductibles de n'importe quel degré.

2.2 Relation entre irréductibilité dans A et dans $\mathrm{frac}(A)$

Définition 7. *Soit $P \in A[X]$. On appelle* contenu *de P le* pgcd *de ses coefficients. On le note $c(P)$. On dit que P est* primitif *lorsque $c(P) = 1$.*

Lemme 1 (Gauss)**.** *Pour tous $P, Q \in A[X]$, on a $c(PQ) = c(P)c(Q)$.*

Proposition 6. *Soit A un anneau factoriel et $\mathrm{frac}(A)$ son corps des fractions. Les polynômes irréductibles de $A[X]$ sont :*

- *les constantes irréductibles dans A,*

– *les polynômes non constants primitifs et irréductibles dans* $\mathrm{frac}(A)$.

Remarque. Le polynôme $2X$ et irréductible sur $\mathbb{Q}$ mais pas sur $\mathbb{Z}$.

Lemme 2. *Soient $P, Q \in A[X]$ tel que P soit unitaire et PQ soit unitaire et à coefficients entiers. Alors Q est unitaire et P et Q sont à coefficients entiers.*

Le fait que Q est unitaire est évident. Écrivons maintenant $P = X^\alpha + \frac{1}{\mu}\sum_{i=0}^{\alpha-1} p_i X^i$, où les entiers $\mu, p_0, \ldots, p_{\alpha-1}$ sont premiers entre eux dans leur ensemble (pour celà, il suffit de choisir pour μ le ppcm des dénominateurs des coefficients de P). On écrit de même $Q = X^\beta + \frac{1}{\nu}\sum_{i=0}^{\beta-1} q_i X^i$, avec $\nu, q_0, \ldots, q_\nu$ premiers entre eux dans leur ensemble. On sait alors que les polynômes μP et νQ sont à coefficients entiers et de contenu 1. On a donc $1 = c(\mu P)c(\nu Q) = c(\mu P.\nu Q) = \mu\nu.c(PQ) = \mu\nu$, ce qui implique que $\mu = \nu = 1$, i.e. que P et Q sont à coefficients entiers.

2.3 Exemple : polynômes cyclotomiques

Soit $m \in \mathbb{N}^*$. On note $\mathbb{U}_m = \{z \in \mathbb{C} \mid z^m = 1\}$ l'ensemble des *racines m-ièmes de l'unité* dans $\mathbb{C}$. On rappelle que $\mathbb{U}_m$ est un groupe cyclique, et on appelle *racine primitive m-ième de l'unité* tout générateur de $\mathbb{U}_m$. On note $\mathbb{P}_m$ l'ensemble des racines primitives m-ième de l'unité.

Définition 8. *On appelle* m-ième polynôme cyclotomique *le polynôme*

$$\Phi_m = \prod_{z \in \mathbb{P}_m} (X - z).$$

Proposition 7. *(i) Le polynôme Φ_m est unitaire de degré $\phi(m)$.*
(ii) $X^m - 1 = \prod_{d|m} \Phi_d$.
(iii) Φ_m est à coefficients dans $\mathbb{Z}$.

Les points (i) et (ii) découlent directement des propriétés de structure de $\mathbb{Z}/m\mathbb{Z}$. Montrons le point (iii) par récurrence :
– le résultat est immédiat pour $m = 1$ puisque $\Phi_1 = X - 1$.
– en supposant le résultat vrai pour tous les entiers inférieurs à m, on obtient que $U = \prod_{d|m, d\neq m} \Phi_d$ est un polynôme unitaire à coefficients dans $\mathbb{Z}$. On peut donc effectuer dans $\mathbb{Z}[X]$ la division euclidienne de $X^m - 1$ par U : il existe $Q, R \in \mathbb{Z}[X]$ tels que $X^m - 1 = UQ + R$ et $deg(R) < deg(U)$. L'unicité de la division euclidienne dans $\mathbb{C}[X]$ permet de conclure que $Q = \Phi_m$ et $R = 0$, ce qui implique que Φ_m est bien à coefficients entiers.

Théorème 4. *Le polynôme Φ_m est irréductible dans $\mathbb{Q}[X]$.*

Pour montrer ce théorème, il suffit de montrer que Φ_m est le polynôme minimal de l'une de ses racines. Soit $z \in \mathbb{P}_m$ et $\pi \in \mathbb{Q}[X]$ son polynôme minimal (unitaire). On va montrer que π s'annule sur toutes les racines primitives m-ièmes de l'unité, ce qui impliquera que $\Phi_m = \pi$.

Commençons par remarquer que comme $X^m - 1$ s'annule en z, π le divise, donc il existe $R \in \mathbb{Q}[X]$ tel que $\pi R = X^m - 1$. Le lemme 2 affirme alors que π et R sont à coefficients entiers.

Considérons maintenant une racine ω de π et un nombre premier p ne divisant pas m, et supposons que ω^p n'est pas une racine de π. Tout d'abord, comme π divise $X^m - 1$, on sait que $\omega \in \mathbb{U}_m$, et donc que $\omega^p \in \mathbb{U}_m$. On a donc $0 = (\omega^p)^m - 1 = \pi(\omega^p)R(\omega^p)$. Comme on a supposé que ω^p n'est pas une racine de π, on obtient $R(\omega^p) = 0$. Le polynôme π étant irréductible, unitaire et s'annulant en ω, c'est le polynôme minimal de ω, donc il divise $R(X^p)$. Soit $S \in \mathbb{Q}[X]$ tel que $R(X^p) = \pi(X)S(X)$. À nouveau d'après le lemme 2, S est unitaire et à coefficients entiers.

Ainsi, l'égalité $R(X^p) = \pi(X)S(X)$ est une égalité dans $\mathbb{Z}[X]$, et on peut la passer modulo p : $\bar{R}(X)^p = \overline{R(X^p)} = \bar{\pi}(X)\bar{S}(X)$. Cette égalité nous assure que si T est un facteur irréductible de $\bar{\pi}$, alors T divise $\bar{R}(X)^p$, donc $\bar{R}(X)$. Par conséquent, T^2 divise $\bar{R}\bar{\pi} = \overline{X^m - 1} = X^m - 1$. Ceci est impossible car $X^m - 1$ et sa dérivée mX^{m-1} sont premiers entre eux : en effet, comme m est premier avec p, on peut l'inverser dans $\mathbb{Z}/p\mathbb{Z}$ et $\left(\frac{1}{m}X\right) mX^{m-1} - (X^m - 1) = 1$.

On obtient ainsi une contradiction ce qui montre que si ω est une racine de π et p un nombre premier ne divisant pas m, alors ω^p est aussi une racine de π.

Considérons maintenant une racine primitive m-ième de l'unité z'. On sait qu'il existe un entier n premier avec m et tel que $z' = z^n$. On écrit $n = p_1^{\alpha_1} \ldots p_\ell^{\alpha_\ell}$ où les p_i sont des entiers premiers ne divisant pas m. D'après la discussion précédente, et comme z est une racine de π, il est facile de montrer que z' est aussi une racine de π, ce qui termine la preuve du théorème.

Proposition 8 (Un cas particulier du théorème de Dirichlet)**.** *Soit m un entier non nul.*

1. *Soient $a \in \mathbb{N}$ et p un entier premier. Si p divise $\Phi_m(a)$ mais pas $\Phi_d(a)$ pour tout diviseur strict d de m, alors $p \equiv 1 [\text{mod } m]$.*
2. *Il existe une infinité de nombres premiers de la forme $\lambda m + 1$ (avec $\lambda \in \mathbb{N}$).*

Pour montrer le premier point, il suffit d'étudier l'ordre de a dans le groupe $(\mathbb{Z}/p\mathbb{Z})^*$. On sait que p divise $\Phi_m(a)$, donc aussi $a^m - 1$. Ainsi, $a^m \equiv 1 \ [\text{mod } p]$ et l'ordre de a est un diviseur de m. Par un raisonnement similaire, le fait que p ne divise $\Phi_d(a)$ pour aucun diviseur strict de m assure que a est en fait exactement d'ordre m. Par conséquent, m divise l'ordre du groupe $(\mathbb{Z}/p\mathbb{Z})^*$, c'est à dire $p-1$, donc $p \equiv 1 \ [\text{mod } m]$.

Montrons à présent cette version faible du théorème de Dirichlet. Soit $N \in \mathbb{N}$. On pose $a = 3N!$. Soit p un diviseur premier de $\Phi_m(a)$. Alors

(i) p est strictement plus grand que N. En effet, si $p \leq N$, alors p divise a. Comme Φ_m est à coefficients entiers, on en déduit que p divise $\Phi_m(a) - \Phi_m(0)$, donc il divise $\Phi_m(0) = \pm 1$. On obtient une absurdité.

(ii) $p \equiv 1 \ [\text{mod } m]$. En effet, s'il existe un diviseur strict d de m tel que p divise $\Phi_d(a)$, alors a est une racine double de $X^m - 1 = \prod_{d|m} \Phi_d(X)$ dans $\mathbb{Z}/p\mathbb{Z}$, ce qui encore une fois est impossible puisque $X^m - 1$ et sa dérivée sont premier entre eux.

On a donc trouvé une infinité de nombres premiers congrus à 1 modulo m.

Le théorème suivant, du à Kronecker, donne une caractérisation intéressante des polynômes cyclotomiques par les modules de leurs racines :

Théorème 5 (Kronecker)**.** *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire irréductible dans $\mathbb{Q}[X]$ de degré supérieur ou égal à 1. On suppose que toutes ses racines sont de module inférieur ou égal à 1. Alors $P = X$ ou P est un polynôme cyclotomique.*

Soient $a_1, \ldots, a_n$ les racines de P et p_0 son terme constant. D'après les relations racines-coefficients, $p_o = \prod a_i$. On a alors deux cas :

(i) soit l'une des racines est de module strictement inférieur à 1. Alors $|p_0| = \prod |a_i| < 1$, donc $p_0 = 0$. L'irréductibilité de P entraine donc que $P = X$.

(ii) soit toutes les racines de P sont de module 1. Pour tout entier k, on pose $\mu_k = \prod_{i=1}^n (a_i^k - 1)$. C'est un polynôme symétrique en les racines de P, donc μ_k s'exprime comme un polynôme en les $\Sigma_{i,n}(a_1, \ldots, a_n)$, i.e. en les coefficients de P. Par conséquent, μ_k est un entier pour tout k.

Supposons maintenant que pour tout k, μ_k soit non nul. Alors

$$|a_1^k - 1| = \frac{\mu_k}{\prod_{i \neq 1} |\alpha_i - 1|} \geq \frac{1}{\prod_{i \neq 1} |a_i|^k + 1} = \frac{1}{2^{n-1}},$$

donc le sous-groupe de $\mathbb{U}$ engendré par a_1 n'est pas dense. Il existe donc un rationel p/q tel que $a_1 = e^{2ip\pi/q}$. Mais alors $a_1^q = 1$ et $\mu_q = 0$, ce qui contredit notre hypothèse.

On en déduit donc que μ_k s'annule pour un certain k, et donc qu'il existe i tel que $a_i^k = 0$. Comme P est le polynôme minimal de a_i, on en déduit qu'il divise $X^k - 1$, donc c'est un polynôme cyclotomique.

2.4 Critères d'irréductibilité

2.4.1 Irréductibilité et racines

Pour qu'un polynôme de degré supérieur ou égal à 2 soit irréductible sur un corps k, il faut évidemment qu'il n'ait pas de racines dans k. Cette condition nécessaire est aussi suffisante si le polynôme est de degré 2 ou 3. La proposition suivante généralise ce fait aux degrés plus grands :

Proposition 9. *Soit P un polynôme de $k[X]$ de degré α. Alors P est irréductible si et seulement s'il n'admet de racine dans aucune extension K de k telle que $[K : k] \leq \alpha/2$.*

Exemple. Le polynôme $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

2.4.2 Critère de Dumas, d'Eisenstein, ...

Définition 9. *Soit A un anneau factoriel et* frac(A) *son corps des fractions. Soit p un irréductible de A. On appelle* valuation p-adique *d'un élément a de A l'entier $v_p(a) = \max\{\ell \in \mathbb{N} \mid p^\ell \text{ divise } a\}$. On appelle* valuation p-adique *d'un élément $\frac{a}{b}$ de* frac(A) *l'entier $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$.*

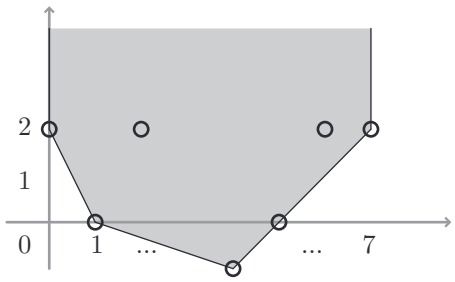

FIG. 1 – Le 2-polygone de Newton du polynôme $12 + \frac{1}{5}X + 4X^2 + \frac{1}{2}X^4 + X^5 + \frac{4}{7}X^6 + 4X^7$

Définition 10. *Soit $P = \sum_{i=0}^{n} c_i X^i \in \mathrm{frac}(A)[X]$ et p un nombre premier. On appelle* p-polygone de Newton de P *l'enveloppe convexe inférieure $\mathcal{N}_p(P)$ de l'ensemble $\{(i, v_p(c_i)) \mid 0 \leq i \leq n\}$.*

Exemple. Sur la figure 1, on a grisé le 2-polygone de Newton du polynôme $12 + \frac{1}{5}X + 4X^2 + \frac{1}{2}X^4 + X^5 + \frac{4}{7}X^6 + 4X^7$.

Proposition 10. *Soient P et Q deux polynômes de* $\mathrm{frac}(A)[X]$ *et p un irréductible de A. Alors*

$$\mathcal{N}_p(PQ) = \mathcal{N}_p(P) + \mathcal{N}_p(Q) = \{u \in \mathbb{R}^2 \mid \exists v \in \mathcal{N}_p(P), w \in \mathcal{N}_p(Q), \text{tels que } u = v + w\}.$$

Pour montrer cette proposition, on note

$$P = \sum_{i \in \mathbb{N}} \alpha_i p^{\beta_i} X^i \quad \text{et} \quad Q = \sum_{i \in \mathbb{N}} \gamma_i p^{\delta_i} X^i$$

où $(\alpha_i)_{i\in\mathbb{N}}$ (resp. $(\gamma_i)_{i\in\mathbb{N}}$) est une suite presque nulle d'éléments de $\mathrm{frac}(A)$ de valuation p-adique nulle et $(\beta_i)_{i\in\mathbb{N}}$ (resp. $(\delta_i)_{i\in\mathbb{N}}$) est une suite d'entiers avec $\beta_i = +\infty$ lorsque $\alpha_i = 0$ (resp. $\delta_i = +\infty$ lorsque $\gamma_i = 0$). Avec ces notations, le polygone de Newton $\mathcal{N}_p(P)$ (resp. $\mathcal{N}_p(Q)$) est l'enveloppe convexe inférieure de l'ensemble $\{(i, \beta_i) \mid i \in \mathbb{N}\}$ (resp. $\{(i, \delta_i) \mid i \in \mathbb{N}\}$).

Par ailleurs,

$$PQ = \sum_{i \in \mathbb{N}} \left(\sum_{j+k=i} \alpha_j \gamma_k p^{\beta_j + \delta_k} \right) X^i,$$

donc $\mathcal{N}_p(PQ)$ est l'enveloppe convexe inférieure de l'ensemble $\left\{ \left(i, v_p \left(\sum_{j+k=i} \alpha_j \gamma_k p^{\beta_j+\delta_k} \right) \right) \mid i \in \mathbb{N} \right\}$.

Or

$$v_p \left(\sum_{j+k=i} \alpha_j \gamma_k p^{\beta_j + \delta_k} \right) \geq \min\{\beta_j + \delta_k \mid j + k = i\}, \tag{1}$$

donc on a déjà l'inclusion $\mathcal{N}_p(PQ) \subset \mathcal{N}_p(P) + \mathcal{N}_p(Q)$, et tout revient à montrer l'égalité dans l'inéquation 1.

Pour cela, considérons un sommet u de $\mathcal{N}_p(P) + \mathcal{N}_p(Q)$. Par définition, il existe $(v, w) \in \mathcal{N}_p(P) \times \mathcal{N}_p(Q)$ tel que $u = v + w$. Montrons que ce couple est unique : supposons qu'il existe un autre couple $(\tilde{v}, \tilde{w}) \in \mathcal{N}_p(P) \times \mathcal{N}_p(Q)$ tel que $u = \tilde{v} + \tilde{w}$. On a alors $u = \frac{1}{2}(v + w + \tilde{v} + \tilde{w}) = \frac{1}{2}((v + \tilde{w}) + (\tilde{v} + w))$ et $v + \tilde{w},\ \tilde{v} + w \in \mathcal{N}_p(P) + \mathcal{N}_p(Q)$. Comme u est extremal, on obtient donc $v + \tilde{w} = \tilde{v} + w$. En combinant avec l'égalité $v + w = \tilde{v} + \tilde{w}$, on obtient $v = \tilde{v}$ et $w = \tilde{w}$.

Ainsi, pour tout sommet $u = (x, y)$ de $\mathcal{N}_p(P) + \mathcal{N}_p(Q)$, il existe un unique couple d'entiers (j, k) tel que $x = j + k$ et $y = \beta_j + \delta_k$. On a donc bien égalité dans l'inéquation 1, et donc le résultat.

Nous pouvons maintenant appliquer directement cette proposition pour donner un critère géométrique d'irréductibilité d'un polynôme :

Théorème 6 (Critère de Dumas)**.** *Soit $P \in \mathrm{frac}(A)[X]$ de coefficient constant non nul. S'il existe un irréductible p tel que le p-polygone de Newton de P soit l'enveloppe convexe inférieure d'un segment ne rencontrant $\mathbb{Z}^2$ qu'en ses extremités, alors P est irréductible dans* $\mathrm{frac}(A)[X]$.

Exemple. Le critère d'Eisenstein est un cas particulier de ce critère : soit $P = c_n X^n + \ldots + c_1 X + c_0 \in A[X]$ et $p \in A$ irréductible et tel que

$$\text{(i) } p \nmid c_n \quad \text{(ii) } \forall 0 \leq j \leq n,\ p | a_j \quad \text{(iii) } p^2 \nmid c_0.$$

Alors P est irréductible dans $\mathrm{frac}(A)[X]$.

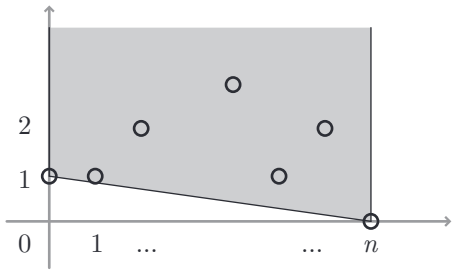

FIG. 2 – Le critère d'Eisenstein

2.4.3 Réduction modulo p

Théorème 7. *Soit A un anneau factoriel et* frac(A) *son corps des fractions. Soit I un idéal premier de A et B le quotient de A par I. Soit $P = c_nX^n + \ldots + c_1X + c_0$ un polynôme de $A[X]$ et $\tilde{P} = \tilde{c_n}X^n + \ldots + \tilde{c_1}X + \tilde{c_0} \in B[X]$ sa réduction modulo I ($\tilde{c_i}$ désigne la classe de c_i dans B). Si $\tilde{c_n} \neq 0$ et $\tilde{P}$ est irréductible sur B (ou* frac(B)*), alors P est irréductible sur* frac(A) *(et donc sur A s'il est primitif).*

Exemple.

(i) Le polynôme $5X^3 + 4X^2 + 3X + 1$ se réduit modulo 2 en $X^3 + X + 1$ qui est irréductible sur $\mathbb{F}_2$ (il est de degré 3 et n'a pas de racines).

(ii) Même lorsqu'une réduction ne donne pas directement un critère d'irréductibilité, elle fournit des informations sur les possibles décomposition du polynôme de départ. Par exemple, le polynôme $P = X^5 + X^2 + X + 2$ se réduit modulo 2 en $X(X^4 + X + 1)$. Le polynôme $X^4 + X + 1$ étant irréductible dans $\mathbb{F}_2$, il y a deux possibilités : soit P est irréductible, soit P se décompose en deux polynômes, l'un de degré 1 et l'autre de degré 4. Or la réduction de P modulo 3 n'a pas de racine, donc la deuxième solution est écartée. P est donc irréductible.

(iii) Il existe des polynômes irréductibles sur $\mathbb{Z}$ dont la réduction modulo n'importe quel nombre premier est réductible : c'est le cas du polynôme cyclotomique $X^4 + 1$.

3 Extensions de corps

3.1 Rappels sur les extensions de corps, nombres algébriques et transcendants

Définition 11. *Soient k et K deux corps tels que $k \subset K$. On dit alors que K est une* extension *(de corps) de k, et on note K/k cette extension.*

Si K est une extension de k, alors K peut être vu comme un k-espace vectoriel avec la loi externe : $\forall a \in k, \forall b \in K, a.b = ab$ (multiplication dans le corps K). Si K est de dimension finie sur k, on dit que l'extension est *finie* et la dimension de K sur k est appelée *degré de l'extension* et est notée $[K : k]$.

Théorème 8 (de la base télescopique et de la multiplication du degré)**.** *Soient K, L et M des corps tels que $K \subset L \subset M$. Soient $(e_i)_{i\in I}$ et $(f_j)_{j\in J}$ des bases respectives du K-espace vectoriel L et du L-espace vectoriel M. Alors $(e_if_j)_{i\in I, j\in J}$ est une base du K-espace vectoriel M. En particulier, si les extensions L/K et M/L sont finies de degrés respectifs $[L : K]$ et $[M : L]$, alors l'extension M/K est finie de degré $[M : K] = [M : L][L : K]$.*

Soit K/k une extension de corps et A une partie de K. On note $k(A)$ (resp. $k[A]$) le plus petit sous-corps (resp. sous-anneau) de K contenant k et A. On a bien sûr $k[A] \subset k(A)$. Si $A = \{a_1, \ldots, a_n\}$ est fini, on note aussi $k(A) = k(a_1, \ldots, a_n)$ (resp. $k[A] = k[a_1, \ldots, a_n]$). Si $K = k(a)$, on dit que l'extension est *monogène*.

Pour $a \in K$, on a

$$k[a] = \{P(a) \mid P \in k[X]\} \quad \text{et} \quad k(a) = \left\{ \frac{P(a)}{Q(a)} \mid P, Q \in k[X], Q(a) \neq 0 \right\}.$$

Il est important de noter que $k[a]$ (resp. $k(a)$) n'est en général pas isomorphe à $k[X]$ (resp. à $k(X)$) puisqu'il peut arriver que $P(a) = 0$ avec $P \neq 0$. Plus précisément, il y a deux situations possibles :

Définition 12. *Soit K/k une extension de corps et $a \in L$. Soit $\phi : k[X] \longrightarrow K$ le morphisme défini par $\phi(P) = P(a)$.*

(i) Si ϕ est injective, on dit que a est transcendant.

(ii) sinon, on dit que a est algébrique. *Dans ce cas, l'idéal $I = \mathrm{Ker}\ \phi$ est principal non nul, donc il est engendré par un unique polynôme π unitaire, appelé* polynôme minimal de a sur k.

Proposition 11. *(i) Si a est transcendant, $k[a] \simeq k[X]$ et $k(a) \simeq k(X)$.*

(ii) Si a est algébrique, $k[a] \simeq k(a) \simeq k[X]/(\pi)$.

Exemple.
- i et $\sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$,
- e et π sont transcendants sur $\mathbb{Q}$,
- le nombre de Liouville $\sum \frac{1}{10^{n!}}$ est transcendant.

Autant il est difficile de montrer que e et π sont transcendants, autant le fait que $\sum \frac{1}{10^{n!}}$ soit transcendant découle directement du lemme suivant :

Lemme 3. *Soit α un nombre algébrique. Alors il existe $n \in \mathbb{N}^*$ et $\lambda \in \mathbb{R}^*$ tels que $\forall (p,q) \in \mathbb{Z} \times \mathbb{Z}^*$, $|\alpha - \frac{p}{q}| \geq \frac{\lambda}{q^n}$.*

En effet, soit P tel que $P(\alpha) = 0$. On note n le degré de P et $\lambda = 1/\sup_{[\alpha-1;\alpha+1]} |P'|$. Alors pour tout $\frac{p}{q} \in [\alpha - 1; \alpha + 1]$, on a $|P(\frac{p}{q})| \leq \frac{1}{\lambda}|\frac{p}{q} - \alpha|$. Mais $P(\frac{p}{q}) \geq \frac{1}{q^n}$, et donc $|\alpha - \frac{p}{q}| \geq \frac{\lambda}{q^n}$.

Proposition 12. *Soit K/k une extension et $\kappa = \{x \in K \mid x$ algébrique sur $k\}$. Alors κ est un corps (on parle d'*extension intermédiaire*).*

Définition 13. *On dit qu'un corps k est* algébriquement clos *s'il satisfait les conditions équivalentes suivantes :*

(i) tout polynôme non constant de $k[X]$ admet une racine dans k,

(ii) les seuls polynômes irréductibles de $k[X]$ sont les polynômes de degré 1,

(iii) tout élément algébrique d'une extension K/k est contenu dans k,

(iv) il n'existe pas d'extension algébrique de k (autre que k).

3.2 Corps de rupture, corps de décomposition

Définition 14. *Soit k un corps et $P \in k[X]$ irréductible. Une extension K de k est un* corps de rupture *de P sur k si K est une extension monogène $K = k(a)$ avec $P(a) = 0$.*

Remarque.

(i) Par exemple, $\mathbb{C} = \mathbb{R}[i]$ est le corps de rupture de $X^2 + 1$ sur $\mathbb{R}$, $\mathbb{Q}[\sqrt[3]{2}]$ est celui de $X^3 - 2$ sur $\mathbb{Q}$.

(ii) La dimension $[K : k]$ est le degré de P.

Proposition 13. *Il existe un unique corps de rupture de P sur k à isomorphisme près. On le note $R_k(P)$.*

Définition 15. *Soit k un corps et $P \in k[X]$. Une extension K de k est un* corps de décomposition *de P sur k si :*
- *P est scindé sur K,*
- *les racines de P dans K engendrent K.*

Remarque.

(i) Par exemple, $\mathbb{Q}[\sqrt[3]{2}, j]$ est le corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$.

(ii) La dimension $[K : k]$ divise la factorielle du degré de P.

Proposition 14. *Il existe un unique corps de décomposition de P sur k à isomorphisme près. On le note $D_k(P)$.*

Définition 16. *On appelle* cloture algébrique *d'un corps k toute extension de k qui est à la fois algébriquement close et algébrique sur k.*

Proposition 15. *Il existe une unique cloture algébrique de k à isomorphisme près. On le note $\bar{k}$.*

4 Application : corps finis

4.1 Généralités

4.1.1 Caractéristique, cardinal

Définition 17. *Soit k un corps. On appelle* sous-corps premiers *de k le plus petit sous-corps de k contenant* 1. *On appelle* caractéristique *de k le générateur* $\mathrm{car}(k)$ *du noyau du morphisme de $\mathbb{Z}$ dans k défini par $n \mapsto n = 1+1+\ldots+1$.*

On a alors :

1. soit la caractéristique de k est nulle, et son sous-corps premier est $\mathbb{Q}$. k est donc infini.
2. soit a caractéristique de k est un nombre premier p et le sous-corps premier de k est $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Proposition 16. *Si un corps est fini, alors son cardinal est une puissance de sa caractéristique, qui est un nombre premier.*

Proposition 17. *Soit k un corps de caractéristique p. Alors l'application $x \mapsto x^p$ définit un automorphisme du corps k, appelé* automorphisme de Frobénius.

4.1.2 Existence et unicité

Théorème 9. *Soit p un nombre premier, $m \in \mathbb{N}^*$ et $q = p^m$. À isomorphisme près, il existe un unique corps $\mathbb{F}_q$ à q éléments : c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.*

4.1.3 Sous-corps et cloture algébrique d'un corps fini

Proposition 18. *Soit p un nombre premier, $m \in \mathbb{N}^*$ et $q = p^m$. On a une bijection*

$$\begin{aligned} \{\text{diviseurs de } m\} &\longleftrightarrow \{\text{sous} - \text{corps de } \mathbb{F}_q\} \\ d &\longmapsto \{x \in \mathbb{F}_q \mid x^{p^d} - x = 0\} \\ |F| &\longleftarrow\!\shortmid F \end{aligned}$$

Exemple. Soit p un nombre premier et $x \in \mathbb{F}_{p^2}$. Alors x est dans $\mathbb{F}_p$ si et seulement si $x^p = x$.

Proposition 19. *Soit p premier. Alors $K_p = \bigcup_{n\in\mathbb{N}^*} \mathbb{F}_{p^{n!}}$ est la cloture algébrique de $\mathbb{F}_p$.*

4.2 Polynômes irréductibles sur un corps fini

Proposition 20. *Le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique.*

En particulier, si a est un générateur de $\mathbb{F}_q^*$, alors $\mathbb{F}_q = \mathbb{F}_p[a]$. On en déduit :

Proposition 21. *Il existe donc au moins un polynôme irréductible de degré m sur $\mathbb{F}_p$.*

Un tel polynôme permet de représenter $\mathbb{F}_q$ sous la forme $\mathbb{F}_p[X]/(\pi)$. C'est cette représentation que l'on utilise en pratique pour les corps finis non premiers.

Théorème 10. *Soit p un nombre premier, $m \in \mathbb{N}^*$ et $q = p^m$. Pour tout $d \in \mathbb{N}$, on note $A(q,d)$ l'ensemble des polynômes irréductibles unitaires de degré d sur $\mathbb{F}_q$. Alors pour tout $\ell \in \mathbb{N}$,*

$$X^{q^\ell} - X = \prod_{d|\ell} \prod_{P\in A(q,d)} P.$$

Considérons en effet un entier d divisant ℓ et un polynôme P de $A(q,d)$. Soit $\kappa = R_{\mathbb{F}_q}(P)$ le corps de rupture de P sur $\mathbb{F}_q$. L'extension $\kappa/\mathbb{F}_q$ est de degré d, donc $\kappa \simeq \mathbb{F}_{q^d} = \{\text{racines de } X^{q^d} - X\}$. On en déduit que P divise $X^{q^d} - X$, qui divise $X^{q^\ell} - X$ (car $X^{q^\ell} - X = (X^{q^d} - X)(X^{q^{\ell-d}} + X^{q^{\ell-2d}} + \ldots + 1)$). Le polynôme P est donc bien un diviseur de $X^{q^\ell} - X$.

Réciproquement, soit P est un facteur irréductible unitaire de degré d de $X^{q^\ell} - X$ et soit x est une racine de P dans $\mathbb{F}_{q^m}$. Alors par multiplicativité des degrés, on a

$$[\mathbb{F}_{q^\ell} : \mathbb{F}_q(x)].d = [\mathbb{F}_{q^\ell} : \mathbb{F}_q(x)][\mathbb{F}_q(x) : \mathbb{F}_q] = [\mathbb{F}_{q^\ell} : \mathbb{F}_q] = \ell.$$

Donc d divise ℓ et $P \in A(q,d)$.

Enfin, les racines de $X^{q^\ell} - X$ dans $\mathbb{F}_{q^\ell}$ étant des racines simples, tout facteur irréductible de $X^{q^\ell} - X$ apparaît avec multiplicité 1. On a donc bien l'égalité

$$X^{q^\ell} - X = \prod_{d|\ell} \prod_{P \in A(q,d)} P.$$

Définition 18. *On appelle* fonction de Möbius *la fonction définie par* $\mu(1) = 1$, $\mu(n) = 0$ *si* n *contient un facteur carré et* $\mu(p_1 \dots p_r) = (-1)^r$ *si les* p_i *sont des nombres premiers distincts.*

Lemme 4. *(i) Pour tout entier* n, $\sum_{d|n} \mu(d) = \delta_{1,n}$.

(ii) Soit $f : \mathbb{N}^* \to \mathbb{N}$ *et* $g : \mathbb{N}^* \to \mathbb{N}$ *définie par* $g(n) = \sum_{d|n} f(d)$. *Alors pour tout* $n \in \mathbb{N}^*$,

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d).$$

Le premier point est clair pour $n = 1$. Maintenant, si p est un nombre premier divisant n, alors $n = mp$ (avec $m \in \mathbb{N}$) et

$$\sum_{d|n} \mu(d) = \sum_{d|mp} \mu(d) = \sum_{p \not| d|m} \mu(d) + \mu(dp) + \sum_{p|d|m} \mu(dp) = 0.$$

Pour le second point, on écrit

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{e|d} f(e) = \sum_{\frac{n}{d}|n} \mu\left(\frac{n}{d}\right) \sum_{\frac{n}{d}|\frac{n}{e}} f(e) = \sum_{\frac{n}{e}|n} f(e) \sum_{\frac{n}{d}|\frac{n}{e}} \mu\left(\frac{n}{d}\right) = \sum_{\frac{n}{e}|n} f(e)\delta_{1,\frac{n}{e}} = f(n).$$

Proposition 22. *Pour tout puissance d'un nombre premier* $q = p^m$ *et tout entier* ℓ, *on a*

$$|A(q,\ell)| = \frac{1}{\ell} \sum_{d|\ell} \mu\left(\frac{\ell}{d}\right) q^d \sim_{\ell \to \infty} \frac{q^\ell}{\ell}.$$

Le theorème 10 donne l'égalité $q^\ell = \sum_{d|\ell} d|A(q,d)|$, ce qui donne la première égalité par la formule d'inversion. Pour obtenir l'équivalent, il ne reste plus qu'à majorer la différence :

$$\left| \sum_{\substack{d|\ell \\ d \neq \ell}} \mu\left(\frac{\ell}{d}\right) q^d \right| < \sum_{d=1}^{\lfloor \frac{\ell}{2} \rfloor} q^d = q \frac{q^{\lfloor \frac{\ell}{2} \rfloor} - 1}{q-1} = o\left(\frac{q^\ell}{\ell}\right).$$

4.3 Carrés dans un corps fini

4.3.1 L'ensemble $\mathbb{F}_q^2$

Soit p un nombre premier, $m \in \mathbb{N}^*$ et $q = p^m$. Dans toute la fin de ce texte, on note $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q, x = y^2\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \setminus \{0\}$.

Proposition 23. *1. Si* $p = 2$, *alors* $\mathbb{F}_q^2 = \mathbb{F}_q$.

2. Si $p > 2$, *alors* $\left|\mathbb{F}_q^2\right| = \frac{q+1}{2}$.

Dans toute la suite, p est supposé différent de 2.

Proposition 24. *Soit* $x \in \mathbb{F}_q^*$. *Alors* $x \in \mathbb{F}_q^2$ *si et seulement si* $x^{\frac{q-1}{2}} = 1$.

Exemple. -1 est un carré de $\mathbb{F}_q$ si et seulement si $q \equiv 1$ [mod 4].

4.3.2 Réciprocité quadratique

Définition 19. *Soit p un nombre premier différent de 2 et $x \in \mathbb{F}_p$. On note $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$ le* symbole de Legendre *de x. On l'étend pour $y \in \mathbb{Z}$ par $\left(\frac{y}{p}\right) = \left(\frac{\bar{y}}{p}\right)$.*

Proposition 25. *On a*

$$\left(\frac{1}{p}\right) = 1, \qquad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad \text{et} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Théorème 11 (de réciprocité quadratique de Gauss)**.** *Pour tous nombres premiers p et q distincts et différents de 2, on a*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Pour prouver ce résultat, on considère une racine primitive q-ième de l'unité ω dans une cloture algébrique de $\mathbb{F}_p$. On peut alors définir ω^x pour $x \in \mathbb{F}_q$ puisque $\omega^q = 1$. On definit donc la *somme de Gauss* :

$$S = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \omega^x.$$

On procède alors en deux étapes :

(i) On a

$$S^2 = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \omega^x \sum_{y \in \mathbb{F}_q} \left(\frac{y}{q}\right) \omega^y = \sum_{z \in \mathbb{F}_q} \left[\sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right)\left(\frac{z-x}{q}\right)\right] \omega^z.$$

Or si $x \neq 0$, on a

$$\left(\frac{x}{q}\right)\left(\frac{z-x}{q}\right) = \left(\frac{x(z-x)}{q}\right) = \left(\frac{-x^2}{q}\right)\left(\frac{1-zx^{-1}}{q}\right) = (-1)^{\frac{q-1}{2}}\left(\frac{1-zx^{-1}}{q}\right).$$

d'où

$$(-1)^{\frac{q-1}{2}} S^2 = \sum_{z \in \mathbb{F}_q} \left[\sum_{x \in \mathbb{F}_q^*} \left(\frac{1-zx^{-1}}{q}\right)\right] \omega^z = (q-1) + \sum_{z \in \mathbb{F}_q^*} \left[\sum_{x \in \mathbb{F}_q^*} \left(\frac{1-zx^{-1}}{q}\right)\right] \omega^z = (q-1) - \sum_{z \in \mathbb{F}_q^*} \omega^z = q,$$

car lorsque $z \neq 0$, l'application $x \mapsto 1 - zx^{-1}$ définit une bijection de $\mathbb{F}_q^*$ dans $\mathbb{F}_q \smallsetminus \{1\}$ et $\sum_{y \neq 1} \left(\frac{y}{q}\right) = -1$.
On a donc montré que

$$S^2 = (-1)^{\frac{q-1}{2}} q.$$

(ii) Par ailleurs

$$S^p = \left[\sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \omega^x\right]^p = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \omega^{xp} = \sum_{x \in \mathbb{F}_q} \left(\frac{xp^{-1}}{q}\right) \omega^x = \left(\frac{x}{q}\right) S.$$

On a alors tous les éléments pour terminer la preuve :

$$\left(\frac{p}{q}\right) = S^{p-1} = \left(S^2\right)^{\frac{p-1}{2}} = \left((-1)^{\frac{q-1}{2}} q\right)^{\frac{p-1}{2}} = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right).$$

5 Questions et remarques

5.1 Questions

On pourra traiter les problèmes suivants :

1. sur les exemples du paragraphe 1.2 :
   (a) montrer les propositions 3, 4 et 5.
   (b) montrer les deux assertions de l'exemple 1.2.

(c) donner l'inverse d'une matrice de Vandermonde (on pourra soit utiliser la formule de la comatrice, soit utiliser des polynômes interpollateurs de Lagrange).

(d) soient $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n, \gamma_1, \ldots, \gamma_n \in \mathbb{R}$. Montrer qu'il existe un unique polynôme P de degré strictement inférieur à $2n$ tel que pour tout $1 \leq i \leq n$, on ait $P(\alpha_i) = \beta_i$ et $P'(\alpha_i) = \gamma_i$.

(e) montrer que les polynômes de Tchebytchev vérifient la formule de dérivation suivante :

$$(1 - X^2)T_n''(X) - XT_n'(X) + n^2 T_n(X) = 0.$$

2. sur la localisation des racines :

(a) montrer les 4 inégalités de l'exemple 1.3.2 (pour le (iii), on considèrera le polynôme $R(X) = (X-1)P(X)$ auquel on appliquera le résultat du (i)).

(b) soit $P \in \mathbb{C}[X]$. Montrer que les racines de P' sont situées dans l'enveloppe convexe des racines de P.

3. sur les critères d'irréductibilité :

(a) donner d'autres exemples de critères d'irréductibilité que l'on peut obtenir à partir du critère de Dumas.

(b) montrer que même si le critère de Dumas ne révèle pas l'irréductibilité d'un polynôme P, il peut donner des informations sur les éventuels diviseurs de P. Montrer par exemple que le polynôme $P = 6X^4+3X^3+2X^2+6$ est irréductible en utilisant les diagrammes $\mathcal{N}_2(P)$ et $\mathcal{N}_3(P)$.

(c) appliquer le critère d'Eisenstein à $X^n + 2$ et $X^{p-1} + \ldots + X + 1$ (faire la transformation $Y + 1 = X$).

(d) montrer que le polynôme $X^4 + 1$ est réductible dans $\mathbb{F}_p$ pour tout premier p (on pourra d'abord montrer que $p^2 - 1$ est divisible par 8 pour tout nombre premier impair p, et en déduire l'existence d'une racine de $X^4 + 1$ dans $\mathbb{F}_{p^2}$). Pourquoi est-il irréductible dans $\mathbb{Z}$?

(e) montrer que pour tout p premier, $X^p - X - 1$ est irréductible dans $\mathbb{F}_p$.

4. sur les corps finis :

(a) représenter et faire des calculs dans un corps fini sous maple (la question ne se limite évidemment pas aux corps premiers).

(b) comment fait-on pour trouver un polynôme irréductible unitaire de degré ℓ sur $\mathbb{F}_q$?

(c) donner une preuve de la loi de réciprocité quadratique sans passer par les corps finis (c'est-à-dire en prenant pour ω une racine primitive q-ième de l'unité dans $\mathbb{C}$).

(d) calculer $\left(\frac{-3}{p}\right)$ en fonction du reste de p modulo 3.

5. autres questions :

(a) montrer que $\Phi_m(0) = \pm 1$.

(b) montrer qu'il existe une infinité indénombrable de nombres transcendants.

(c) montrer (directement) qu'il existe une infinité de nombres premiers congrus à 1 (resp. 3) modulo 4.

5.2 Remarques et références

Pour ce texte, j'ai utilisé essentiellement le *Cours d'algèbre* de D. Perrin, le livre de *Théorie de Galois* de Y. Gozard, le tome d'algèbre des *Maths en tête* de X. Gourdon et les *Exercices pour l'agrégation* (Tome 1 d'algèbre) de S. Francinou & H. Gianella.

Il va sans dire que tout ou partie de ce texte peut être présenté dans les leçons d'agrégation portant sur les polynômes. Pourtant, il me semble important dans ces leçons de bien réfléchir aux différences de point de vue que leur titre suggère. Il faudra donc rester prudent dans l'utilisation de ce texte.