Corps des fractions rationnelles à une indéterminée sur un corps commutatif. Applications

prérequis : corps des fractions d'un anneau intègre, zéros des polynômes, extension de corps, courbes paramétrées.

Il faut présenter dans un premiers paragraphe le théorème principal de la leçon, i.e. la décomposition en éléments simples d'une fraction rationnelle et donner à travers divers exemples des méthodes pratiques (division suivant les puissances croissantes, utilisation d'extension de corps, automorphismes de corps, équivalent, dérivée logarithmique...). Les autres thèmes principaux sont :

- l'étude des sous-corps de $k(t)$, ses automorphismes et l'étude d'équations diophantiennes ;
- de la géométrie : les courbes unicursales, la sphère de Riemann ;
- étude des zéros des fractions rationnelles ;
- séries génératrices et problèmes combinatoires.

Comme l'intitulé le demande, on doit se limiter au cas d'une variable même s'il n'est pas interdit de signaler quelques résultats dans le cas général, comme par exemple le théorème de Luroth, la combinatoire ou encore le 17-ème problème de Hilbert.

Table des matières

1. Définitions et premières propriétés

Dans la suite K désigne un corps commutatif.

1.1. Définition. — Le corps des fractions rationnelles est le corps des fractions de l'anneau des polynômes de $K[t]$. Un élément $F \in K(t)$ possède un unique représentant sous la forme $\frac{P}{Q}$ où $P, Q \in K[t]$ sont premiers entre eux et Q est unitaire : P/Q s'appelle la représentation normale de F.
Remarque : toute représentation de F s'obtient à partir de sa représentation normale P/Q par multiplication par un élément $D \in K[t]$, i.e. $F = \frac{DP}{DQ}$.

Les zéros de P (resp. de Q) s'appellent les zéros (resp. les pôles) de F.

Définition 1.1. — Le degré de F est défini par $\deg(F) = deg(P) - deg(Q)$ où $F = P/Q$ est une représentation quelconque.

Pour toutes fractions F et F', on a $\deg(F + F') = \sup\{\deg(F), \deg(F')\}$ et $\deg(FF') = \deg(F) + \deg(F')$.

1.2. Décomposition en éléments simples. — Toute fraction rationnelle F peut s'écrire de manière unique sous la forme $E + G$ où $E \in K[T]$ s'appelle la partie entière de F et $\deg G < 0$. Concrètement à partir d'une représentation P/Q, on effectue la division euclidienne de P par Q : $P = EQ + R$ avec $G = R/Q$.
Remarque : la partie entière de $F + G$ est la somme de celle de F par celle de G.

Théorème 1.2. — *Soit $F = P/Q$ écrite sous forme normale avec $Q = \prod_i Q_i^{\alpha_i}$ où les Q_i sont les facteurs irréductibles de Q. Il existe alors pour tout i et $1 \leq j \leq \alpha_i$ des polynômes $f_{i,j}$ de degré $< \deg Q_i$ tels que*

$$F = E + \sum_i \sum_{j=1}^{\alpha_i} \frac{f_{i,j}}{Q_i^j}.$$

Cette écriture est par ailleurs unique.

Remarque : l'énoncé précédent peut s'interpréter comme la donnée d'une base de $K(t)$ en tant que K-espace vectoriel.

Méthodes pratiques :
- pour les pôles simples, i.e. $\deg Q_i = 1$, le plus simple est d'effectuer la division suivant les puissances croissantes ; le coefficient f_{i,α_i} peut aussi se calculer directement en évaluant $FQ_i^{\alpha_i}$ en la racine de Q_i.
- pour les pôles multiples $\deg Q_i > 1$, on effectue les calculs dans la base $1, \beta, \cdots, \beta^{\alpha_i - 1}$ où β est une racine de Q_i dans une extension de K.
- dans le cas où on cherche à décomposer F dans une extension galoisienne L de K, on utilisera le groupe de Galois pour propager les calculs : typiquement pour $K = \mathbb{R}$ et $L = \mathbb{C}$, utiliser la conjugaison complexe.
- utiliser des équivalents, la dérivée logarithmique...

Exemples : $\frac{X^2+2X+3}{X^2(X-1)^4(X^2+X+1)^3}$.

1.3. Localisation des zéros de P'/P. — En utilisant la dérivée logarithmique, pour $P = \prod_i (X - \alpha_i)^{n_i}$, la fraction rationnelle P'/P s'écrit sous la forme $\sum_i \frac{n_i}{x-\alpha_i}$).

Définition 1.3. — Pour $P \in \mathbb{R}[z]$, pour toute paire $(z, \bar{z})$ de racines conjuguées de f, le disque de Jensen est le disque fermé de diamètre les points d'affixe z et $\bar{z}$.

Théorème 1.4. — *(Jensen) Toute racine non réelle de f' appartient à un des disques de Jensen.*

Exemple : soit $f(z) = (z^2 - 1)(z - i\sqrt{3})$ dont les racines sont les sommets du triangle isocèle $\pm 1, i\sqrt{3}$; on a $f'(z) = 3(z - \frac{i}{\sqrt{3}})^2$ a une racine double en $i/\sqrt{3}$ un point intérieur à ce triangle. Le phénomène est général comme le prouve le résultat suivant.

Théorème 1.5. — *(Gauss-Lucas) Les racines de P' appartiennent à l'enveloppe convexe des racines de P.*

Remarque : en particulier si toutes les racines de P sont dans un disque D alors il en est de même des racines de P'. La généralisation naturelle est de considérer plusieurs disques contenant les racines de P et d'obtenir des précisions sur la localisation des racines de P'. Cette question a été étudiée en particulier par Walsh dont nous citons le résultat le plus simple.

Théorème 1.6. — *(Walsh) Supposons que les racines de f_1 et f_2 appartiennent respectivement au disque D_i pour $i = 1, 2$ de centre c_i et de rayon r_i, alors les racines de $(f_1 f_2)'$ appartiennent soit à D_1, D_2 soit au disque D de centre $\frac{n_2 c_1 + n_1 c_2}{n_1 + n_2}$ et de rayon $\frac{n_2 r_1 + n_1 r_2}{n_1 + n_2}$, où $n_i = \deg f_i$.*

Remarque : en revenant au cas d'une fonction réelle, on obtient un supplément au théorème de Rolle : soit P un polynôme réel de degré n tek que m_1 de ses racines appartiennent à l'intervalle réel $I_1 = [a_1, b_1]$ et les $m_2 = n - m_1$ autres sont dans $I_2 = [a_2, b_2]$ avec $a_2 > b_1$. Alors les racines de P' qui n'appartiennent pas à $I_2 \cup I_2$ appartiennent à l'intervalle $I = [a, b]$ avec $a = \frac{m_2 a_1 + m_1 a_2}{n}$ et $b = \frac{m_2 b_1 + m_1 b_2}{n}$.
Remarque : on notera que les preuves ne nécessite pas le fait que les n_i soient entiers. En ce sens une généralisation du théorème de Lucas est donnée par le théorème suivant.

Théorème 1.7. — *(cf. [4] p.30) Soit $F(z) = \sum_{j=1}^{n} m_j f_j(z)$ où*

$$f_j(z) = \frac{(z - a_{j,1}) \cdots (z - a_{j,p})}{(z - b_{j,1}) \cdots (z - b_{j,q})}$$

et où les $m_j \in \mathbb{C}$ sont tels que

$$\mu \leq \arg m_j \leq \mu + \gamma < \mu + \pi \qquad j = 1, \cdots, n.$$

Si K est partie convexe de $\mathbb{C}$ qui contient tous les $a_{j,k}, b_{j,k}$ alors $F(\zeta) \neq 0$ en tout point $\zeta \in \mathbb{C}$ qui voit K sous un angle inférieur à $\Psi = \frac{\pi - \gamma}{p+q}$.

1.4. Fractions rationnelles à valeurs entières sur $\mathbb{Z}$. — Commençons tout d'abord par les polynômes.

Proposition 1.8. — *Soient n un entier quelconque et p_k un polynôme de degré k prenant des valeurs entières en $x = n, n+1, \cdots, n+k$. Il existe alors des entiers $c_0, \cdots, c_k$ tels que*

$$p_k(x) = c_0\tbinom{x}{k} + c_1\tbinom{x}{k-1} + c_2\tbinom{x}{k-2} + \cdots + c_k$$

où $\tbinom{x}{i} = \frac{x(x-1)\cdots(x-i+1)}{i!}$.

Preuve : Notons tout d'abord que les fonctions $\tbinom{x}{i}$ sont à valeurs entières, i.e. $\tbinom{x}{i} \in \mathbb{Z}$ pour tout $x \in \mathbb{Z}$: le cas $i = 1$ est évident. On raisonne alors par récurrence ; supposons le résultat acquis jusqu'au rang k. Les égalités

$$\tbinom{x+1}{k+1} - \tbinom{x}{k+1} = \tbinom{x}{k} \qquad \tbinom{0}{i} = 0$$

permettent alors de conclure. Comme $\tbinom{x}{i}$ pour $i = 0, \cdots, k$ est une famille étagée de $\mathbb{Q}[x]_k$ elle en est une base ce qui montre l'existence des nombres $c_0, \cdots, c_k$; il ne reste alors plus qu'à montrer que les c_i sont entiers. On raisonne par récurrence sur k ; pour $k = 0$ le polynôme $p_0(x) = c_0$ prend une valeur entière en $x = n$ et donc $c_0 \in \mathbb{Z}$. Supposons alors le résultat acquis jusqu'au rang k et traitons le cas de $k+1$. Pour $p_{k+1}(x) = c_0\tbinom{x}{k+1} + \cdots + c_{k+1}$ soit

$$\Delta p_{k+1}(x) = p_{k+1}(x+1) - p_{k+1}(x) = c_0\tbinom{x}{k} + \cdots + c_k$$

qui prend des valeurs entières en $x = n, n+1, \cdots, n+k+1$ de sorte que $c_0, \cdots, c_k$ sont entiers et donc comme

$$c_{k+1} = p_{k+1}(n) - c_0\tbinom{n}{k+1} - \cdots - c_k\tbinom{n}{1} \in \mathbb{Z}.$$

□

Corollaire 1.9. — *Soit $R(x)$ une fraction rationnelle qui prend des valeurs entières sur $\mathbb{Z}$ alors $R(x)$ est un polynôme.*

Preuve : On écrit $R(x) = \frac{f(x)}{g(x)}$ où f et g sont des polynômes premiers entre eux. En effectuant la division euclidienne $f = p_k g + r$ on a $R(x) = p_k(x) + r(x)$ avec $r(x) \to 0$ pour $x \to \infty$. Ainsi si n est grand $p_k(n)$ est proche d'un entier ; montrons que $p_k(x)$ est à valeurs entières sur $\mathbb{Z}$. On écrit

$$p_k(x) = c_0\tbinom{x}{k} + \cdots + c_k.$$

Si $k = 0$ alors c_0 est arbitrairement proche d'un entier et donc $c_0 \in \mathbb{Z}$. Le polynôme

$$\Delta p_k(x) = p_{k+1}(x+1) - p_{k+1}(x) = c_0\tbinom{x}{k} + \cdots + c_{k-1}$$

prend lui-aussi des valeurs presque entières pour tout $x \in \mathbb{Z}$ assez grand. Par hypothèse de récurrence, $c_0, \cdots, c_{k-1}$ sont entiers et donc $c_k = p_k(n) - c_0\tbinom{n}{k} - \cdots - c_{k-1}\tbinom{n}{1}$ aussi. On en déduit alors que $r(n)$ est nul pour tout n assez grand et donc $r(x)$ est nulle d'où le résultat. □

Corollaire 1.10. — *Soient f, g des polynômes de $\mathbb{Z}[x]$ tels que $g(n)|f(n)$ pour tout $n \in \mathbb{Z}$; il existe alors des entiers tels que*

$$f(x) = \Big(\sum_{k=0}^{m} c_k\tbinom{x}{k}\Big) g(x).$$

Remarque : Polya a par ailleurs montré que si $f(z)$ est une fonction analytique à valeurs entières sur $\mathbb{Z}$ telle que $|f(z)| < Ce^k|z|$ où $k < \ln(\frac{3+\sqrt{5}}{2})$ alors $f(z)$ est polynomiale. L'exemple de 2^z montre qu'une hypothèse de croissance à l'infini est nécessaire ; en outre l'exemple de

$$\frac{1}{\sqrt{5}}\Big((\frac{3+\sqrt{5}}{2})^z - (\frac{3-\sqrt{5}}{2})^z\Big)$$

montre que la majoration est optimale.

2. Le corps $K(t)$

Dans ce paragraphe on s'intéresse à la structure du corps des fractions rationnelles à la sauce théorie de Galois.

2.1. Sous-corps. —

Lemme 2.1. — *Soit $F = P/Q$ écrit sous forme normale alors le degré de $K(t)$ sur $K(F)$ est égal à* $\max\{\deg p, \deg q\}$.

Théorème 2.2. — *(Luroth) Soit $K \subset L \subset K(t)$; il existe alors $F \in K(t)$ tel que $L = K(F)$.*

2.2. Equations diophantiennes sur $K(t)$. — L'anneau $K[t]$ étant euclidien, on a les mêmes notions et propriétés que sur $\mathbb{Z}$; en outre en utilisant les notions de degré, racines et la dérivation, la résolution des énoncés d'arithmétique est généralement largement plus aisé que dans le cas de $\mathbb{Z}$. Historiquement $K[t]$ est une source d'inspiration pour formuler des conjectures sur $\mathbb{Z}$ et parfois suggère des techniques.

Théorème 2.3. — ***(Mason)*** *(cf.* [**5**] *§4.3) Soient $a(x)$, $b(x)$ et $c(x)$ des polynômes premiers entre eux deux à deux tels que $a + b + c = 0$, alors*

$$\max\{\deg a, \deg b, \deg c\} \leq n_0(abc) - 1$$

où $n_0(P)$ est le nombre de racines distinctes du polynôme P.

Preuve : Soient $f = \frac{a}{c}$ et $g = \frac{b}{c}$ de sorte que f et g sont des fractions rationnelles qui satisfont l'équation $f + g + 1 = 0$ ce qui donne $f' = -g'$ et donc

$$\frac{b}{a} = \frac{g}{f} = -\frac{f'/f}{g'/g}.$$

Rappelons que pour $R(x) = \prod_i (x - \rho_i)^{r_i}$, on a $\frac{R'}{R} = \sum_i \frac{r_i}{x-\rho_i}$. Posons

$$a(x) = \prod_i (x - \alpha_i)^{a_i}, \quad b(x) = \prod_j (x - \beta_j)^{b_j}, \quad c(x) = \prod_k (x - \gamma_k)^{c_k},$$

de sorte que

$$\frac{f'}{f} = \sum_i \frac{a_i}{x - \alpha_i} - \sum_k \frac{c_k}{x - \gamma_k}, \qquad \frac{g'}{g} = \sum_j \frac{\beta_j}{x - \beta_j} - \sum_k \frac{c_k}{x - \gamma_k}.$$

Pour N_0 le ppcm des $(x - \alpha_i)$, $(x - \beta_j)$, $(x - \gamma_k)$ qui est donc de degré $n_0(abc)$, on a

$$\frac{b}{a} = -\frac{N_0 f'/f}{N_0 g'/g}$$

où $N_0 f'/f$ et $N_0 g'/g$ sont des polynômes de degré inférieurs ou égaux à $n_0(abc) - 1$. Or comme a et b sont premiers entre eux on en déduit que leur degré est aussi inférieur ou égal à $n_0(abc) - 1$. Pour $c(x)$ la preuve est similaire. □

Corollaire 2.4. — *Soient f, g, h des polynômes premiers entre eux dont un au moins n'est pas constant alors l'égalité $f^n + g^n = h^n$ est impossible pour $n \geq 3$.*

Preuve : Supposons $f^n + g^n = h^n$ de sorte que d'après le théorème précédent on a

$$n \max\{\deg f, \deg g, \deg h\} \leq \deg f + \deg g + \deg h - 1.$$

En ajoutant ces trois inégalités on obtient alors

$$n(\deg f + \deg g + \deg h) \leq 3(\deg f + \deg g + \deg h - 1)$$

et donc $n < 3$. □

Remarque : selon le même procédé, on peut montrer que pour α, β, γ des entiers tels que $2 \leq \alpha \leq \beta \leq \gamma$ alors l'équation $f^\alpha + g^\beta = h^\gamma$ n'a pas de solutions premières entre elles sauf pour (α, β, γ) égal à

$$(2, 2, \gamma), \quad (2, 3, 3), \quad (2, 3, 4), \quad (2, 3, 5).$$

Corollaire 2.5. — *(Equation de Catalan) Pour $m, n \geq 2$, si l'équation $x^n - y^m = 1$ possède des solutions dans $\mathbb{C}(x)$ alors $m = n = 2$.*

Preuve : Soient $x = f/g$ et $y = h/k$ écrits sous forme irréductible une solution de $x^n - y^m = 1$ de sorte que

$$f^m k^n - h^n g^m = g^m k^m.$$

Comme f et g sont premiers entre eux, on obtient que si $g(\alpha) = 0$ alors $k(\alpha) = 0$; de même si $k(\alpha) = 0$ alors $g(\alpha) = 0$ de sorte que $g(t) = \prod_i (t - \alpha_i)^{a_i}$ et $k(t) = \prod_i (t - \alpha_i)^{b_i}$ avec $a_i, b_i \geq 1$. Ainsi la multiplicité de α_i comme racine des polynômes $f^m k^n$, $h^n g^m$ et $g^m k^n$ est respectivement égale à nb_i, ma_i et $nb_i + ma_i$. Si $nb_i \neq ma_i$ alors la multiplicité de α_i dans $f^m k^n - h^n g^m$ est strictement inférieure à $nb_i + ma_i$ d'où la contradiction. Ainsi $nb_i = ma_i$ i.e. $k^n = g^m$. Après division par $k^n = g^m$, l'équation devient $f^m - h^n = g^m$ qui d'après le corollaire précédent n'a des solutions que pour $\{m, n\} = \{2, 2\}$ ou $\{2, 3\}$. Dans le second cas, on a $k^n = g^m = l^6$ où l est un polynôme alors que l'équation $f^3 - h^2 = l^6$ n'a pas de solutions, d'où le résultat. □

Remarque : inspirés par la preuve de Fermat via le théorème de Mason, Oesterlé et Masser ont en 1985, proposé une version sur $\mathbb{Z}$ du théorème de Mason que l'on appelle la **conjecture abc**, on renvoie à l'exercice 7.6

2.3. Groupe de Galois. — automorphisme de $K(t)/K$: l'application $PGL_2(K) \longrightarrow \mathrm{aut}_K(K(T))$ qui à $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ associe $T \mapsto \frac{aT+b}{cT+d}$ est un isomorphisme de groupes.

2.4. Dix-septième problème de Hilbert. — (prouvé par Artin) : si $r(x_1, \cdots, r_n) \in \mathbb{R}(x_1, \cdots, x_n)$ est une fraction rationnelle réelle à valeurs positives alors elle peut s'écrire comme une somme de carrés de fractions rationnelles à coefficients réels. Le résultat n'est pas valable pour les polynômes sauf pour $n = 1$ (théorème d'Artin-Cassels-Pfister).

la situation est particulièrement simple comme le montre les deux résultats suivants.

Proposition 2.6. — *Soit $p(X) \in \mathbb{R}[X]$ tel que pour tout $x \in \mathbb{R}$ on a $p(x) \geq 0$. Il existe alors $f_1, f_2 \in \mathbb{R}[X]$ tels que $p = f_1^2 + f_2^2$.*

Preuve : On factorise p en séparant ses racines réelles de ses racines complexes :

$$p(x) = a\prod_{i=1}^{s}(x-z_i)(x-\bar{z}_i)\prod_{k=1}^{t}(x-\alpha_k)^{m_k}.$$

Comme $p(x) \geq 0$ pour tout $x \in \mathbb{R}$, alors $a \geq 0$ et toutes les multiplicités m_k sont paires de sorte que l'on peut aussi séparer ses racines réelles en deux soit

$$p(x) = \Big(\sqrt{a}\prod_{j=1}^{l}(x-z_j)\Big)\Big(\sqrt{a}\prod_{j=1}^{l}(x-\bar{z}_j)\Big),$$

où cette fois-ci les z_j peuvent être réelles. On écrit alors $\sqrt{a}\prod_{j=1}^{l}(x-z_j) = q(x)+ir(x)$ où $q, r \in \mathbb{R}[X]$ de sorte que $\sqrt{a}\prod_{j=1}^{l}(x-\bar{z}_j) = q(x)-ir(x)$ et donc $p(x) = q(x)^2 + r(x)^2$. □

Théorème 2.7. — ***(Artin-Cassels-Pfister)*** *Soient K un corps de caractéristique différente de 2 et $f \in K[X]$. On suppose que*

$$f(x) = \sum_{i=1}^{n}\alpha_i r_i(x)^2 \qquad \alpha_i \in K,\ r_i \in K(X)\forall i = 1,\cdots,n$$

alors il existe des polynômes $p_i \in K[X]$ pour $i = 1,\cdots,n$ tels que

$$f(x) = \sum_{i=1}^{n}\alpha_i p_i(x)^2.$$

Preuve : Pour $n = 1$ le résultat est évident, supposons donc $n > 1$ et $\alpha_i \neq 0$ pour tout i. On introduit la forme quadratique $\phi(u,v) = \sum_i \alpha_i u_i v_i$ définie sur $K(x)^n$; il s'agit alors de prouver que si $f \in K[x]$ est tel que $f = \phi(u,u)$ avec $u \in K(x)^n$ alors il existe $w \in K[x]^n$ tel que $f = \phi(w,w)$.

Cas où ϕ est isotrope : nous allons en fait montrer que pour tout $f \in K[x]$ il existe $w \in K[x]^n$ tel que $\phi(w,w) = f$ (on n'utilise par l'hypothèse $f = \phi(u,u)$). Soit $u = (u_1,\cdots,u_n) \in K[x]^n$ un vecteur isotrope, i.e. $\phi(u,u) = 0$ avec $u_1\wedge\cdots\wedge u_n = 1$. Soit alors $u_1v_1+\cdots+u_nv_n = 1$ une relation de Bezout. On pose alors $w_i' = \frac{v_i}{2\alpha_i}$ de sorte que $\phi(u,w') = 1/2$. Des égalités

$$\phi(u, w'+\lambda u) = \phi(u,w') \qquad \phi(u+\lambda w', w'+\lambda u) = \phi(w',w') + \lambda$$

en remplaçant w' par $w' - \phi(w',w')u$, on peut supposer que $\phi(w',w') = 0$ de sorte que pour tout $f \in K[x]$ on a

$$\phi(fu+w', fu+w') = f^2\phi(u,u) + 2f\phi(u,w') + \phi(w',w') = f$$

ce qui donne le résultat en posant $w = fu + w'$.

Cas où ϕ est anisotrope : on multiplie l'égalité $f = \phi(u,u)$ par le ppcm des dénominateurs des u_i ce qui donne une égalité polynomiales $\alpha_1u_1^2 + \cdots + \alpha_nu_n^2 = fu_0^2$. Parmi toutes les égalités de cette forme, on en considère une telle que $r = \deg u_0$ est minimal ; il s'agit alors de montrer que $r = 0$. Supposons $r > 0$ et on effectue la division euclidienne des u_i par u_0, i.e. $\deg(u_i - u_0v_i) \leq r-1$. Soient alors les vecteurs $u = (u_1,\cdots,u_n)$, $v = (v_1,\cdots,v_n)$ ainsi que $\tilde{u} = (u_0,\cdots,u_n)$ et $\tilde{v} = (v_0,\cdots,v_n)$ avec $v_0 = 1$. On note aussi

$$\tilde{\phi}(\tilde{x},\tilde{y}) = \phi(x,y) - fx_0y_0$$

la forme sur $K(x)^{n+1}$ avec des notations évidentes. Par hypothèse on a $\tilde{\phi}(\tilde{u},\tilde{u}) = \phi(u,u) - fu_0^2 = 0$ et $\tilde{\phi}(\tilde{v},\tilde{v}) = \phi(v,v) - f \neq 0$ par minimalité de $r > 0$. En particulier $\tilde{u}$ et $\tilde{v}$ ne sont pas proportionnels et donc

$$\tilde{w} = \tilde{\phi}(\tilde{v},\tilde{v})\tilde{u} - 2\tilde{\phi}(\tilde{u},\tilde{v})\tilde{v} \neq 0$$

avec $\tilde{\phi}(\tilde{w},\tilde{w}) = 0$ comme le montre un calcul simple, i.e. $\phi(w,w) = fw_0^2$. Pour aboutir à une contradiction il s'agit alors de montrer que $\deg w_0 < r$. Comme $v_0 = 1$ on a

$$\begin{aligned}\tilde{w}_0 &= \tilde{\phi}(\tilde{v},\tilde{v})u_0 - 2\tilde{\phi}(\tilde{u},\tilde{v})v_0 = \Big(\textstyle\sum_{i=1}^n \alpha_i v_i^2 - f\Big)u_0 - 2\Big(\sum_{i=1}^n \alpha_i u_i v_i - fu_0\Big) \\ &= \textstyle\sum_{i=1}^n \alpha_i\Big(v_i^2 u_0 - 2u_i v_i + \frac{u_i^2}{u_0}\Big) - \sum_{i=1}^n \frac{\alpha_i u_i^2}{u_0} + fu_0 = \frac{1}{u_0}\sum_{i=1}^n n\alpha_i(u_i - u_0 v_i)^2\end{aligned}$$

car $\sum_{i=1}^n \alpha_i u_i^2 = fu_0^2$. Or on a $\deg(u_i - u_0 v_i) \leq r-1$ et donc

$$\deg w_0 = \deg\Big(\sum_{i=1}^n \alpha_i(u_i - u_0 v_i)^2\Big) - \deg u_0 \leq 2(r-1) - r = r - 2.$$

□

3. Applications à la géométrie

3.1. Courbes unicursales. — ce qui signifie étymologiquement qu'on peut les tracer d'un seul coup de crayon ; ceci n'est vraiment exact dans le plan affine que lorsque le polynôme R n'a pas de racine réelle. Sinon, c'est dans le plan projectif, qu'il faut se placer pour imaginer qu'on ne lève pas le crayon. La réciproque est fausse : la parabole divergente $y^2 = x^3 - 1$ est probablement la courbe non rationnelle dont l'équation cartésienne est la plus simple, se trace d'un coup de crayon ; une telle courbe est dite unipartite. Une *paramétrisation propre* est une une paramétrisation (à l'exception éventuelle de quelques points) $(x_1,\cdots,x_n) = (f_1(t),\cdots,f_n(t))$ avec f_i des fractions rationnelles de $K(t)$ (en projectif $[x_1,\cdots,x_{n+1}] = [p_1(t),\cdots,p_{n+1}(t)]$ avec p_i des polynômes). La paramétrisation est dite propre si $K(t) = K(f_1,\cdots,f_n)$, i.e. s'il existe une fraction rationnelle H en n variables telle que $t = H(f_1,\cdots,f_n)$ (c'est l'analogue formel de l'injectivité d'une paramétrisation). Soit $(f_1,\cdots,f_n)$ une paramétrisation rationnelle et supposons qu'au moins une des fractions rationnelles f_i est non constante. D'après le théorème de Luroth, il existe une fraction rationnelle U de $K(t)$ telle que $K(f_1,\cdots,f_n) = K(U)$ et, nécessairement, U n'est pas constante. On fait alors un "changement de variable" : chaque f_i est de la forme $g_i \circ U$ où g_i est une fraction rationnelle. On a ainsi associée, grâce au théorème de Luroth, une paramétrisation propre $(g_1,\cdots,g_n)$ à la paramétrisation initiale $(f_1,\cdots,f_n)$. Les courbes rationnelles sont les courbes de genre nul.
Exemples : toute conique de $\mathbb{P}^2(\mathbb{C})$ est unicursale (application à la recherche des points rationnels d'une conique...)

3.2. La sphère de Riemann. — la droite projective complexe $\mathbb{P}^1(\mathbb{C})$, dit encore la sphère de Riemann S : ses fonctions méromorphes ($f(z)$ et $f(1/z)$ sont méromorphes) sont exactement les éléments de $\mathbb{C}(t)$. On interprète alors $PGL_2(\mathbb{C})$, le groupe des homographies, comme l'ensemble des automorphismes holomorphes de S ;

la projection stéréographique transforme $\mathbb{C} \cup \{\infty\}$ en $\mathbb{S}^2 \subset \mathbb{R}^3$. On peut alors montrer que toute rotation de $\mathbb{S}^2$ est représentée par une homographie ce qui fournit un isomorphisme $PSU_2(\mathbb{C}) \simeq SO_3(\mathbb{R})$.

4. Séries formelles

4.1. Définition. — On peut voir l'anneau des séries formelles $K[[X]]$ comme le complété du localisé de $K[X]$ en l'idéal (X) : le corps des fractions associé est alors l'anneau des séries de Laurent $K((X))$. Une fraction rationnelle écrite sous forme irréductible P/Q, vue dans $K((X))$ est une série formelle, i.e. un élément de $K[[X]]$ si et seulement si $Q(0) \neq 0$. Une question naturelle est de savoir reconnaître les séries formelles qui sont des fractions rationnelles, i.e. $K[[X]] \cap K(X) \subset K((X))$. Le résultat est le suivant :

Proposition Soit $S(X) = \sum_{k=0}^{\infty} a_k X^k$ une série formelle ; les points suivants sont alors équivalents :

- S appartient à $K(X)$;
- il existe des entiers n et k_0 ainsi que des nombres $c_1, \cdots, c_n$ fixés avec $c_n \neq 0$ tels que pour tout $k \geq k_0$, on ait la relation de récurrence
$$a_k = c_1 a_{k-1} + c_2 a_{k-2} + \cdots + c_n a_{k-n};$$
- il existe des polynômes $P_1, \cdots, P_n$ et des nombres $\lambda_1, \cdots, \lambda_n$ tels que pour tout k assez grand,
$$a_k = P_1(k)\lambda_1^k + P_2(k)\lambda_2^k + \cdots + P_n(k)\lambda_n^k$$

Remarque : Par ailleurs on a $S = P/Q$ avec $\deg Q = n$ et $\deg P \leq k_0$.

Applications : les problèmes de dénombrement (par exemple les nombres de Catalan, le nombre de chemin de Dick...), sommes de Newton

4.2. Relations de Newton et de Waring. — notons $s_d = X_1^d + \cdots + X_n^d$ et soit dans $\mathbb{Z}[X_1, \cdots, X_n, T]$, $F(T) = \prod_{i=1}^n (1 - TX_i) = 1 - \sigma_1 T + \sigma_2 T^2 - \cdots + (-1)^n \sigma_n T^n$. On a
$$\frac{-TF'(T)}{F(T)} = \frac{TX_1}{1-TX_1} + \cdots + \frac{TX_n}{1-TX_n} = \sum_{m \geq 1} T^m s_m$$
où la dernière égalité découle du développement en série formelle $(1-Z)^{-1} = \sum_{m \geq 0} Z^m$ pour $Z = TX_i$. Après simplification par T, on obtient la relation de Newton
$$F(T)\Big(\sum_{m \geq 1} T^{m-1} s_m\Big) + F'(T) = 0$$
qui est une égalité dans $\mathbb{Z}[X_1, \cdots, X_n][[T]]$. En considérant le coefficient de T^k, on trouve :

$$k \geq n : \ s_k - \sigma_1 s_{k-1} + \cdots + (-1)^n \sigma_n s_{k-n} = 0 \qquad 1 \leq k \leq n : \ s_k - \sigma_1 s_{k-1} + \cdots + (-1)^{k-1} \sigma_{k-1} s_1 + (-1)^k k s_k = 0.$$

Dans $\mathbb{Q}[X_1, \cdots, X_n][[T]]$, la relation de Newton s'écrit $\frac{F'(T)}{F(T)} = -P'(T)$, où $P(T) = \sum_{m \geq 1} \frac{s_m}{m} T^m$. Par « intégration » on obtient
$$F(T) = \exp\Big(-P(T)\Big) = 1 - P(T) + \frac{1}{2}P(T)^2 - \frac{1}{3!}P(T)^3 + \cdots$$
ce qui a bien un sens puisque $P(T)$ commence par T et donc $P(T)^k$ par T^k de sorte que le coefficient de T^k ne fait intervenir que les $P(T)^j$ pour $j \leq k$ et est donc fini. En particulier, on note que cette expression permet de calculer le polynôme G_k tel que $\sigma_k = G_k(s_1, \cdots, s_n)$.

Si inversement on cherche à exprimer les s_i en fonction des $\sigma_1, \cdots, \sigma_n$, on utilise l'expression $P(T) = -\log\Big(F(T)\Big)$ où $F(T) = 1 - TG(T)$ avec $G(T) = \sigma_1 - \sigma_2 T + \sigma_3 T^2 + \cdots$ et donc
$$P(T) = TG + \frac{T^2 G^2}{2} + \frac{T^3 G^3}{3} + \cdots$$

Corollaire 4.1. — *Si K est de caractéristique nulle alors la famille $(s_1, \cdots, s_n)$ de $K[X_1, \cdots, X_n]$ est algébriquement libre sur K et engendre l'algèbre $K[X_1, \cdots, X_n]^{\Sigma_n}$.*

4.3. Fonction zeta. — Soit $f(y) \in \mathbb{F}_p[y_0, \cdots, y_n]$ un polynôme homogène, pour tout $s \geq 1$, on note N_s le nombre de zéros de f dans $\mathbb{P}^n(\mathbb{F}_{p^s})$.

Définition 4.2. — La fonction zeta de l'hypersurface projective définie par f est la série formelle

$$Z_f(u) = \exp\Big(\sum_{s=1}^{\infty} \frac{N_s u^s}{s}\Big).$$

Remarque : la série formelle $\sum_{s=1}^{\infty} \frac{N_s u^s}{s}$ étant de valuation 1, la série $Z_f(u)$ est bien définie. Plus généralement pour toute variété algébrique V, on notera $Z_V(u)$ sa fonction de zeta.
Exemples de l'hyperplan à l'infini : $H_0 = \{[a_0, \cdots, a_n] \in \mathbb{P}^n(\mathbb{F}_q) : \ a_0 = 0\}$. On a $H_0(\mathbb{F}_q) \simeq \mathbb{P}^{n-1}(\mathbb{F}_q)$ et donc

$$N_s = q^{s(n-1)} + q^{s(n-2)} + \cdots + q^s + 1$$

on utilise que $\mathbb{P}^n(\mathbb{F}_q) = \mathbb{A}_n(\mathbb{F}_q) \coprod \mathbb{P}^{n-1}(F)$ avec $|\mathbb{A}^n(\mathbb{F}_q)| = q^n$. On a alors

$$\sum_{s=1}^{\infty} \frac{N_s u^s}{s} = \sum_{m=0}^{n-1} \Big(\sum_{s=1}^{\infty} \frac{(q^m u)^s}{s}\Big) = -\sum_{m=0}^{n-1} \ln(1 - q^m u)$$

et donc $Z_{H_0}(u) = (1 - q^{n-1}u)^{-1}(1 - q^{n-2}u)^{-1} \cdots (1 - qu)^{-1}(1 - u)^{-1}$.

Weil a montré que pour tout $f(x_0, x_1, x_2) \in \mathbb{F}_q[x_0, x_1, x_2]$ homogène de degré d non singulière sur $\overline{\mathbb{F}}_p$, la fonction zeta était une fraction rationnelle et plus précisément $Z_f(u) = \frac{P(u)}{(1-u)(1-qu)}$ où $P(u)$ est un polynôme de $\mathbb{F}_q[u]$ de degré $(d-1)(d-2)$ dont les racines sont de module $q^{-1/2}$: ce dernier résultat est appelé l'hypothèse de Riemann pour les courbes. Il a alors conjecturé que la rationnalité de la fonction zeta de toute variété algébrique, dont Dwork a donné une preuve en 1959, ainsi que l'hypothèses de Riemann, dont une preuve a été donnée par Deligne en suivant le programme de Grothendieck.

Proposition 4.3. — *La fonction zeta $Z_f(u)$ est rationnelle si et seulement s'il existe des nombres complexes α_i, β_j tels que*

$$N_s = \sum_j \beta_j^s - \sum_i \alpha_i^s.$$

Preuve : En reprenant la même technique que dans les exemples précédents, on montre que si N_s est de la forme $\sum_j \beta_j^s - \sum_i \alpha_i^s$ alors $Z_f(u) = \frac{\prod_i (1-\alpha_i u)}{\prod_j (1-\beta_j u)}$.

Réciproquement supposons la fonction zeta rationnelle, alors comme sont terme constant est visiblement égal à 1, on peut supposer qu'elle s'écrit sous la forme $P(u)/Q(u)$ avec $P(0) = Q(0) = 1$:

$$Z_f(u) = \frac{\prod_i (1 - \alpha_i u)}{\prod_j (1 - \beta_j u)}$$

avec $\alpha_i, \beta_j \in \mathbb{C}$. La dérivée logarithmique donne

$$\frac{Z_f'(u)}{Z_f(u)} = \sum_i \frac{-\alpha_i}{1 - \alpha_i u} - \sum_j \frac{-\beta_j}{1 - \beta_j u}.$$

En développant en séries formelles, on obtient alors

$$\frac{uZ'_f(u)}{Z_f(u)} = \sum_{s=1}^{\infty} \Big(\sum_j \beta_j^s - \sum_i \alpha_i^s \Big) u^s.$$

Or le membre de droite est égal à $\sum_{s=1}^{\infty} N_s u^s$ et donc $N_s = \sum_j \beta_j^s - \sum_i \alpha_i^s$. □

4.4. Combinatoire. —

5. Applications à l'analyse

5.1. Intégration des fractions rationnelles. —

5.2. Formule de Plouffe. —

5.3. Théorème de Muntz. — via les déterminants de Cauchy ;

5.4. Le théorème de Runge. — Si f est une fonction holomorphe définie sur un ouvert Ω, si Z est un ensemble contenant au moins un point dans chaque composante connexe du complémentaire de Ω dans le plan complété $\hat{\mathbb{C}}$, alors f est dans l'adhérence de l'ensemble des fractions rationnelles à pôles dans Z pour la topologie de la convergence uniforme sur tout compact. En particulier si f est une fonction holomorphe définie sur un ouvert simplement connexe Ω, alors il existe une suite de polynômes convergeant uniformément vers sur tout compact ;

5.5. Formule des résidus. — Applications de la formule des résidus au calcul d'une intégrale par exemple $\int_0^\infty \frac{dt}{1+t^6}$...

6. Développements

- la décomposition en éléments simples (présenter un algorithme)
- Nullstellensatz en utilisant le fait que les $(\frac{1}{X-a})_{a\in K}$, K algébriquement clos non dénombrable, est une partie libre non dénombrable de $K(X)$ [**2**]
- déterminants de Hankel [**?**]
- équivalent asymptotique du nombre de solutions d'une équation diophantienne de degré 1 [**3**] [**?**]
- Luroth et paramétrage propre des courbes unicursales
- théorème de Mason et application à l'analogue de la conjecture de Catalan ;
- combinatoire
- les automorphismes de $K(T)$ [**1**]
- déterminant de Cauchy et théorème de Muntz
- 17-ème problème de Hilbert
- Lucas et une généralisation

7. Questions

Exercice 7.1. — *Quelles sont les fractions rationnelles réelles paires ?*

Exercice 7.2. — *Soit* $A = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ *; donnez toutes les fractions rationnelles invariantes par* A.

Exercice 7.3. — *On considère la courbe paramétrée* $x(t) = t^2 + t + 1$, $y = \frac{t^2-1}{t^2+1}$. *En donner une équation algébrique.*

Exercice 7.4. — *Soient* $a_1, \cdots, a_l$ *des entiers positifs premiers entre eux dans leur ensemble. Soit* A_n *le nombre de solutions entières positives de*

$$a_1x_1 + a_2x_2 + \cdots + a_lx_l = n$$

(1) Montrez que

$$\lim_{n\to\infty} \frac{A_n}{n^{l-1}} = \frac{1}{a_1 \cdots a_l (l-1)!}.$$

(2) On suppose en outre que les a_i *sont premiers entre eux deux à deux ; montrez alors que*

$$A_n = P(n) + Q_n$$

où $P(x)$ *est un polynôme à coefficients rationnels de degré* $l-1$ *et où la suite* Q_n *est périodique de période* $a_1 \cdots a_l$.

(3) Dans le cas $l = 2$ *où* $a_1 = a$ *et* $a_2 = b$ *sont premiers entre eux, montrez que*

$$A_n \leq 1 \text{ quand } n > ab,$$
$$A_n \geq 1 \text{ quand } n > ab - a - b,$$

avec :

- $A_{ab} = 2$,
- $A_{ab-a-b} = 0$,
- $A_{n+ab} = A_n + 1$,
- A_n *est égal à* $\lfloor \frac{n}{ab} \rfloor$ *ou* $\lfloor \frac{n}{ab} \rfloor + 1$.

Exercice 7.5. — *Soient* $n > 2$ *et* x, y, z *trois polynômes de* $\mathbb{C}[X]$ *premiers entre eux ; montrez sans utiliser la dérivation que* $x^n + y^n = z^n$ *implique que les trois polynômes sont des constantes.*

Exercice 7.6. — *La conjecture abc est la suivante : soit* $\epsilon > 0$ *il existe alors une constante* K_ϵ *telle que pour tous* a, b, c *entiers relatifs premiers entre eux vérifiant* $a + b = c$, *on ait*

$$\max\{|a|, |b|, |c|\} \leq K_\epsilon N_0(abc)^{1+\epsilon}$$

où $N_0(n)$ *est le produit des nombres premiers divisant* n.

Montrez, en supposant la conjecture abc vérifée, qu'il existe N *qui dépend explicitement de* K_ϵ *tels que pour tout* $n \geq N$, *l'équation* $x^n + y^n = z^n$ *n'a pas de solutions entières.*
Remarque : la conjecture abc implique plusieurs résultats très importants comme la conjecture de Spiro, le théorème de Faltings, l'existence pour $a \geq 2$ *fixé, d'une infinité de premiers* p *tel* $a^{p-1} \not\equiv 1 \mod p^2$, *la conjecture d'Erdos-Woods (i.e. il existe une constante* $k > 0$ *telle que pour tous* x, y *positifs si* $N_0(x+i) = N_0(y+i)$ *pour tout* $i = 1, 2, \cdots, k$ *alors* $x = y$*).*

8. Solutions

7.1

7.2 Le polynôme caractéristique de A est $x^2 - x + 1$ i.e. $\Phi_6(x)$ de sorte que A est d'ordre 6 dans $GL_2(\mathbb{C})$ et d'ordre 3 dans $PGL_2(\mathbb{C})$. Pour construire une fraction rationnelle invariante par A on moyenne les éléments de l'orbite de X sous l'action du groupe engendré par A :

$$F(X) = \sum_{k=0}^{2} A^k.X = \Big(X + (1 - \frac{1}{X}) + \frac{-1}{X-1}\Big) = \frac{X^3 - 3X + 1}{X(X-1)}.$$

On a alors $K(F) \subset K(X)^{<A>} \subset K(X)$ avec $[K(X) : K(F)] = 3$. Or comme $K(X)^{<A>} \neq K(X)$ on en déduit par la multiplicativité des degrés que $K(X)^{<A>} = K(F)$.
Remarque : on aurait aussi pu argumenter que $< A >$ est contenu dans $\text{aut}_{K(X)^{<A>}} K(X)$ qui est de cardinal inférieur ou égal à $[K(X) : K(X)^{<A>}]$ autrement dit ce degré est supérieur ou égal à l'ordre de A dans $PGL_2(\mathbb{C})$.

7.3 Considérons les polynômes $t^2 + t + (1 - X)$ et $(Y - 1)t^2 + (Y + 1)$ de $\mathbb{R}[X, Y][t]$. Or ces deux polynômes ont un zéro commun, si et seulement si leur résultant est nul soit

$$\begin{vmatrix} 1 & 1 & (1-X) & 0 \\ 0 & 1 & 1 & (1-X) \\ (Y-1) & 0 & Y+1 & 0 \\ 0 & (Y-1) & 0 & Y+1 \end{vmatrix} = \dots$$

7.4 (1) De l'égalité

$$\sum_{n=0}^{\infty} A_n z^n = \frac{1}{(1 - z^{a_1}) \cdots (1 - z^{a_l})} = \frac{1}{a_1 \cdots a_l} \frac{1}{(1-z)^l} + F(z)$$

où $F(z)$ se décompose comme une somme de termes de la forme $\lambda \frac{1}{(1-\omega z)^k}$ où $\lambda \in \mathbb{Q}$, ω est une racine $a_1 \cdots a_l$-ème de l'unité distincte de 1 et, comme $a_1, \cdots, a_l$ n'ont pas de facteurs communs, $k \leq l - 1$. Le résultat découle alors de l'écriture

$$\frac{(k-1)!}{(1-\omega z)^k} = \sum_{n=0}^{\infty} (n + k - 1) \cdots (n + 1) z^n.$$

(2) Comme les a_i sont premiers entre eux deux à deux, on peut écrire $\prod_{i=1}^{l} (1 - z^{a_i})$ sous la forme $(1 - z)^l Q(z)$ où $Q(z)$ divise $1 - z^{a_1 \cdots a_l}$. En décomposant en éléments simples le pôle 1, on obtient une égalité du genre

$$\frac{1}{(1 - z^{a_1}) \cdots (1 - z^{a_l})} = R\Big(\frac{1}{1-z}\Big) + \frac{S(z)}{1 - z^{a_1 \cdots a_l}}$$

où $R(z)$ et $S(z)$ sont des polynômes de degré respectivement égal à l et plus petit que $a_1 \cdots a_l$. Le résultat découle alors de l'écriture

$$R\Big(\frac{1}{1-z}\Big) = \sum_{n=0}^{\infty} P(n) z^n, \qquad \frac{S(z)}{1 - z^{a_1 \cdots a_l}} = \sum_{n=0}^{\infty} Q_n z^n.$$

(3) Soient pour $n < ab$, $ax' + by' = n$ et $ax" + by" = n$; on a donc $0 \leq x', x" < b$ et comme l'égalité $a(x' - x") = -b(y' - y")$ avec $a \wedge b = 1$, $-b < x' - x" < b$ est divisible par b et donc nul. En résumé on a $A_n < 2$. Pour $n = ab$, le même raisonnement donne $A_{ab} \leq 2$ et comme $ab + b.0 = ab = a.0 + ba$ on a bien $A_{ab} = 2$.

Comme $a \wedge b = 1$,

$$T(z) = \frac{(1-z^{ab})(1-z)}{(1-z^a)(1-z^b)} = \Phi_1(z) \prod_{\substack{1 \neq d_1 | a \\ 1 \neq d_2 | b}} \Phi_{d_1 d_2}(z)$$

est un polynôme de la forme $z^{ab-a-b+1} + \cdots + 1$ avec $T(1) = \frac{ab}{ab} = 1$. On en déduit alors que

$$\frac{T(z) - T(1)}{1-z} = -z^{ab-a-b} + \cdots$$

est aussi un polynôme. On a alors

$$\begin{aligned} \textstyle\sum_{n=0}^{\infty}(A_n - A_{n-ab})z^n &= (1-z^{ab}) \textstyle\sum_{n=0}^{\infty} A_n z^n \\ &= \tfrac{T(z)}{1-z} \\ &= \tfrac{T(z)-T(1)}{1-z} + \tfrac{1}{1-z} \\ &= \cdots - z^{ab-a-b} + \textstyle\sum_{n=0}^{\infty} z^n \end{aligned}$$

et donc $A_{ab-a-b} = 0$ et $A_n = A_{n-ab} + 1$ pour tout $n > ab - a - b$. Ainsi on a

$$A_n = A_{n - \lfloor \frac{n}{ab} \rfloor ab} + \lfloor \frac{n}{ab} \rfloor$$

et comme $n - \lfloor \frac{n}{ab} \rfloor ab < n - (\frac{n}{ab} - 1)ab = ab$, on en déduit que, comme $A_{n-\lfloor \frac{n}{ab} \rfloor ab} = 0$ ou 1 que A_n est égal à $\lfloor \frac{n}{ab} \rfloor$ ou $\lfloor \frac{n}{ab} \rfloor + 1$.

7.5 Supposons qu'il existe (x, y, z) premiers entre eux satisfaisant $x^n + y^n = z^n$ tels que le maximum des trois degrés soit $D > 0$. On les choisit tels que D soit minimal. Pour $\xi = e^{2i\pi/n}$, on a

$$z^n = (x+y)(x+\xi y)(x+\xi^2 y) \cdots (x+\xi^{n-1} y).$$

Deux facteurs quelconques du produit n'ont pas de diviseur commun puisqu'un tel facteur diviserait x et y. Leur produit étant une puissance n-ème, ces facteurs sont de la forme βu^n avec $\beta \in \mathbb{C}^\times$ qui lui-même est une puissance n-ème. Ainsi comme $n - 1 \geq 2$ il existe des polynômes u, v, w tels que

$$x + y = u^n, \quad x + \xi y = v^n, x + \xi^2 y = w^n$$

qui sont donc premiers entre eux. En éliminant x et y de ces équations, on trouve $w^n + \xi u^n = (1 = \xi)v^n$. On pose alors $x' = w$, $y' = \xi^{1/n} u$, $z' = (1 = \xi)^{1/n} v$ de sorte que (x', y', z') constitue une solution de l'équation avec x', y', z' premiers entre eux ($\xi + 1 = 0$ implique $n = 2$) et de degré maximal D' satisfaisant $0 < D' \leq D/n < D$, d'où la contradiction.

7.6 Soient x, y, z premiers entre eux solutions de l'équation de Fermat pour n ; sous la conjecture abc, on a

$$|x|^n \leq \max\{|x|^n, |y|^n, |z|^n\} \leq K_\epsilon N_0((xyz)^n)^{1=\epsilon}.$$

Or comme $N_0((xyz)^n) = N_0(xyz)$, en écrivant la relation précédente pour $|y|^n$ et $|z|^n$ et en les multipliant toutes les trois on obtient

$$|xyz|^n \leq K_\epsilon^3 N_0(xyz)^{3(1+\epsilon)}$$

ce qui en utilisant que $N_0(xyz) \leq |xyz$ implique $|xyz|^{n-3(1+\epsilon)} \leq K_\epsilon^3$. De la minoration $|xyz| \geq 2$, on en déduit $2^{n-3(1+\epsilon)} \leq K_\epsilon^3$ et donc le résultat.

Références

[1] S. Francinou and Gianella H. *Exercices de mathématiques pour l'agrégation algèbre 1*. Masson, 1994.

[2] R. Goblot. *Algèbre commutative*. Masson, 1996.

[3] Gourdon. *Les maths en têtes : algèbre*. Ellipses, 1996.

[4] M. Marden. *Geometry of polynomials*. American Mathematical Society, 1966.

[5] V. Prasolov. *Polynomials*. Springer, 2004.