QE pour $\mathbb{Q}_p$

$\{(x,y) \mid ord(x) < ord(y)\}$ est définissable ?

$|y| < |x|$

$\subset \mathbb{Q}_p^2$

$p > 2$

$\{(x,y) \mid \exists z \; (z^2 = x^2 + py^2)\}$

ordre pair dans $\mathbb{Z}$

$ord(y) \leq ord(x)$

ordre impair

$ord(y) > ord(x)$

pair

Hensel [inconnu z exercice.

$\underline{ord(x) \leq ord(y)}$ suffisante pour QE ? Non.

$p = 2 \quad \{(x,y) \in \mathbb{Q}_2^2 \mid \exists z \quad z^3 = x^3 + py^3\}$

$= \{(x,y) \mid ord(x) \leq ord(y)\}$.

$\mathbb{R} \longrightarrow \mathbb{R}_{\geq 0} \quad \mathcal{L}_{anneaux}$

carrés dans $\mathbb{R}$

$\mathbb{Q}_p \longrightarrow P_2 \subset \mathbb{Q}_p$ carrés dans $\mathbb{Q}_p$

pas déf dans $\mathcal{L}_{rings}$ $\cup \{ord \ldots \leq ord \ldots\}$

P_3 les cubes dans $\mathbb{Q}_p$

P_n les puissance n-ième dans $\mathbb{Q}_p$

$\{x \in \mathbb{Q}_p^n \mid \exists y \in \mathbb{Q}_p \; y^n = x\}$.

$x \in P_n$

[$ord(x)$ est multiple de n, dans $n\mathbb{Z}$

$p(x) \overset{=0}{\neq 0}$, $ord(p(x)) \leq ord(q(x))$

$x \in P_n$ ssi $\mathrm{ordre}(x) \in n\mathbb{Z}$ et $x = 0$ ou

$x = \sum_{l \geq j} a_l p^l$ $\quad a_j \neq 0 \quad a_j \in \{0, \dots, p-1\}$

a_j est puissance n-ième dans $\mathbb{F}_p$

(si $p > n$)

$(p, n) = 1$

$\mathrm{ord}(n)$

$p \mid n$

a_j, a_{j+1}, a_{j+2}

$a_j + p a_{j+1} + a_{j+2} p^2 \in \mathbb{Z}/p^3$

puissance n-ième dans "

$\mathbb{Q}_2$ $\quad (a_0 + 2a_1 + 4a_2 + \dots)^2$ $\quad a_i \in \{0,1\}$

$\| \qquad a_0 \neq 0$

$a_0^2 + 2 \cdot a_0 2a_1 + 4a_1^2 + \dots$

$4 a_0 a_1$

$= 1 + 0 \cdot 2 + b_2 2^2 + b_3 2^3 + \dots$ général

Thm QE. Macintyre

$\mathbb{Q}_p$ admet Q.E. dans le langage

$+, -, \cdot, 0, 1, P_2, P_3, P_4, \dots P_n, \dots$

avec $P_n = \{x \in \mathbb{Q}_p \mid \exists y\ y^n = x\}$.

chaque ensemble déf comb Booléenne

$U_n \{ x \in \mathbb{Q}_p^n \mid \ldots p_{\ldots}(x) \in P_m \}$

$\notin$, $= 0$, $\neq 0$

géométrie

topologie

$\underbrace{\mathrm{ord}(p(x)) \leq \mathrm{ord}(q(x))}$

$\mathrm{ord}(x) > N$

polynôme

déf — P_2 $\quad p > 2$

$\underbrace{p(x) + p \cdot q(x) \in P_2}$ $\quad P_3$ $\quad p = 2$

premier

$\mathbb{F}_p((t)) \to$ ~~résolution de sing~~ $\to$?

$\to$ ~~QE~~ ?

$\to$ ~~Bernstein–Sato~~

candidat pour langage ?

QE sur $\mathbb{Q}_p$ $\longrightarrow$ généraliser la rationalité de $Z_f(s)$.

__Excursion__

Est-ce que la rationalité de $Z_f(s)$ est surprenante ?

cas spécial de $Z_f(s) \in \mathbb{Q}(p^{-s})$, $s = 1$

$\underbrace{Z_f(1) \in \mathbb{Q}}$ $= \int_{\mathbb{Z}_p^n} |f(x)| \cdot |dx|$

||

$\mathbb{R}$ — $\int_{\substack{(x,y)\in\mathbb{R}^2 \\ x^2+y^2\leq 1}} 1\, dx\,dy = \pi$

π irrationnel, transcendant.

anneaux — $\mathcal{P}_{\mathbb{R}}$: périodes réelles.

$\pi + \zeta + \dots = \dots$ — $\mathcal{P} : \mathcal{P}_{\mathbb{R}} + i\,\mathcal{P}_{\mathbb{R}}$

$\neq$

intégral — intégrales

manipuler < c.v. ; par partie ; additivité

Kontsevich – Zagier 2000

$\mathbb{Q}_p$ — $\mathbb{Q}$ — — oui

Classiquement (Igusa)

$$\underline{N_m} := \#\{x \in (\mathbb{Z}/p^m)^n \mid \underline{f(x)=0}\}$$

maintenant, variante Serre — dans $\mathbb{Z}/p^m$ q-adelisation

$$\widetilde{N}_m := \#\{x \in (\mathbb{Z}/p^m)^n \mid \exists y_1 \in \mathbb{Q}_p \dots \exists y_n \in \mathbb{Q}_p \; \underline{f(y)=0} \text{ en } \mathbb{Q}_p \text{ et } y \equiv x \bmod p^m\}$$

$$P_f(t) = \sum_{m\geq 0} \widetilde{N}_m t^m$$

rationnelle en t ? → oui
intégrale ? → oui

$y_i \equiv x_i \mod p^n$, $y_i \in \mathbb{Z}_p$, $i = 1, \dots, n$

$$I(s) = \int_{(x,w) \in D \subset \mathbb{Z}_p^{n+1}} |w|^s \, |dx| \cdot |dw|$$

$I(s) \sim \tilde{P}(t)$ (pareil comme avant)

$$D = \{ (x,w) \in \mathbb{Z}_p^{n+1} \mid \exists y \in \mathbb{Q}_p^n \; f(y) = 0 \wedge |y - x| \leq |w| \}$$

déf.

formule dans $\mathcal{L}_{Mac}$: $+, -, \cdot, 0, 1, P_2, \dots, P_n, \dots$

Denef Mac. → $D = \{ (x,w) \in \mathbb{Z}_p^{n+1} \mid \underline{\vee} \wedge \varphi_1(x,w) \in P_n \}$, $\neq 0$, $= 0$, $\notin$

$$\int_D |w|^s |dx| |dw|$$

Serre $\tilde{P}(t)$ est rationnelle ?

oui : th. modèle (plus tard).
résolution de sing.

⇓

Cas de monômes (généralisé)

Plus généralement

Thm Denef. Soit $S \subset \mathbb{Z}_p^n$ et $g : S \to \mathbb{Z}_p$ définissable dans $\mathcal{L}_{Mac}$.

$$Z(s) = \int_{x \in S} |g(x)|^s |dx|$$

Alors $Z(s)$ est rationelle en $t = p^{-s}$.

preuve. I g est polynôme.

$S \longrightarrow$ # fini de polynômes $f_i(x)$ apparaissent dans la formule sans quantificateurs

$$f(x) := g(x) \cdot \prod_i f_i(x)$$

résolution de sing pour f

$y \in \mathbb{Z}_p^n$

$$u(y) \cdot y^a = v(y) \cdot y_1^{a_1} \cdots y_n^{a_n}.$$

Mac $\sim v(y) \cdot y^b$.