6. DÉMONSTRATION DU CAS GLOBAL

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **47 (2001)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **10.08.2024**

$$\# \hat{c}(\mathbf{F}_p) > p + 1 - 2\sqrt{p} \geq (\sqrt{19} - 1)^2 > 11 .$$

La contraction sur $\widehat{C}$ peut écraser 10 de nos points lisses, mais il reste au moins un point lisse sur $\widehat{C}(\mathbf{F}_p)$

Si $\widehat{C}/\mathbf{F}_p$ est de genre 0, ou si elle se décompose sur $\overline{\mathbf{F}}_p$ en ayant une composante simple définie sur $\mathbf{F}_p$, le même argument montre qu'elle a toujours suffisamment de points pour en avoir qui soient lisses. Le seul cas où il faut s'inquiéter c'est quand elle se décompose sur $\overline{\mathbf{F}}_p$ en cinq droites. Mais ce cas est exclu par notre hypothèse, car cela voudrait dire que chaque point de $\widehat{C}$ serait un point d'inflexion, et se trouverait donc sur la Hessienne H. $\square$

Pour terminer la démonstration de la proposition, il suffit donc de calculer la résultante de H avec $\widehat{C}$, en éliminant z, ce qui donne la réduction de

$$2^{44} \cdot (4x^5 - 12x^4y + 10x^3y^2 - 7xy^4 + 4y^5)^6 \cdot q(x:y),$$

où $q(x:y)$ est un polynôme homogène, primitif, de degré 15. Ce n'est jamais 0 modulo un premier $p > 2$. $\square$

6. Démonstration du cas global

Proposition 6.1. *La courbe C donnée par* (1.1) *n'a pas de point rationnel.*

Preuve. On suppose que $(x:y:z)$ est une solution rationnelle de (1.1). On peut supposer que x, y et z sont des entiers et qu'ils n'ont pas de facteur en commun.

Soit p un premier rationnel différent de 2 et de 11, avec $p \not\equiv \pm 1 \pmod{11}$. Alors p ne divise pas r dans la formule (4.1): sinon $x - \varepsilon y = x + y - 4\theta y + \theta^2 y$ serait dans $p\mathcal{O}_K$. Le fait que $\{1, \theta, \theta^2, \theta^3, \theta^4\}$ est une $\mathbf{Z}$-base de $\mathcal{O}_K$ montre alors que p diviserait y et $x+y$. Puisque p ne peut pas être facteur des trois coordonnées, on aurait donc $p \nmid z$, d'où $p \mid f$. Mais $f \equiv 16z^4 \not\equiv 0 \pmod{p}$.

De la même manière, on montre que p ne divise pas s. Donc r et s sont composés de facteurs premiers 2, 11 et de premiers de la forme $p \equiv \pm 1 \pmod{11}$. La même conclusion est vraie pour leurs facteurs y, z, f et g. Considérons $p = 2$ de plus près: rappelons-nous que $2\mathcal{O}_K$ est un idéal premier. On dénote par β la valuation de y en $2\mathbf{Z}$, et par γ celle de z.

On suppose dans un premier temps que β, $\gamma > 0$. Alors $2 \nmid x$, ce qui dit que $x - \varepsilon y \notin 2\mathcal{O}_K$. Ceci implique que $2^4 \parallel r$, autrement dit que $0 < \gamma \leq 4$ et que $2^{4-\gamma} \parallel f$. (On a utilisé la notation $\parallel$ pour dire «divise exactement»). Calculons f modulo 16:

$$f \equiv 4y^2 \cdot 3x^2 + 4y^3 \cdot x + 2y^4 \cdot 5 + 4yz \cdot x^2 + 2y^2z \cdot 5x + y^2z^2 + 8yz^3 \pmod{16}.$$

Par hypothèse, y et z sont au moins une fois divisibles par 2, le terme à droite est donc égal à 0 modulo 16, ce qui n'est pas possible car $16 \nmid f$.

Occupons-nous à présent du cas $\beta = 0$ et $\gamma > 0$: on a $x - \varepsilon y = x + y - 4\theta y + \theta^2 y \notin 2\mathcal{O}_K$, alors comme avant $2^{4-\gamma} \parallel f$. Cette fois-ci on regarde f modulo 4:

$$f \equiv 2 \cdot y^4 + 2xz \cdot y^2 + z^2 \cdot y^2 \equiv 2 \pmod 4,$$

puisque $2 \nmid y$. Cela veut dire que $2 \parallel f$ et donc $\gamma = 3$. (On a vu dans 5.1 que derrière cela «se cache» une solution 2-adique. On ne pourrait pas l'éliminer en considérant $p = 2$.)

Comme dernière possibilité, on considère $\beta \geq 0$ et $\gamma = 0$: on voit que $x - \eta z = x + 3z - \theta z \notin 2\mathcal{O}_K$ (car $2 \nmid z$), alors $2^{4-\beta} \parallel g$ et $0 \leq \beta \leq 4$. On a

$$g \equiv 12x^2yz + 4xy^2z + 10y^3z + 4x^2z^2 + 10xyz^2 + yz^3 + 8z^4 \pmod{16}.$$

Si $\beta < 2$, alors

$$\frac{1}{4} > \frac{1}{2^{4-\beta}} = |g|_2 = |yz^3|_2 = \frac{1}{2^\beta} > \frac{1}{4}.$$

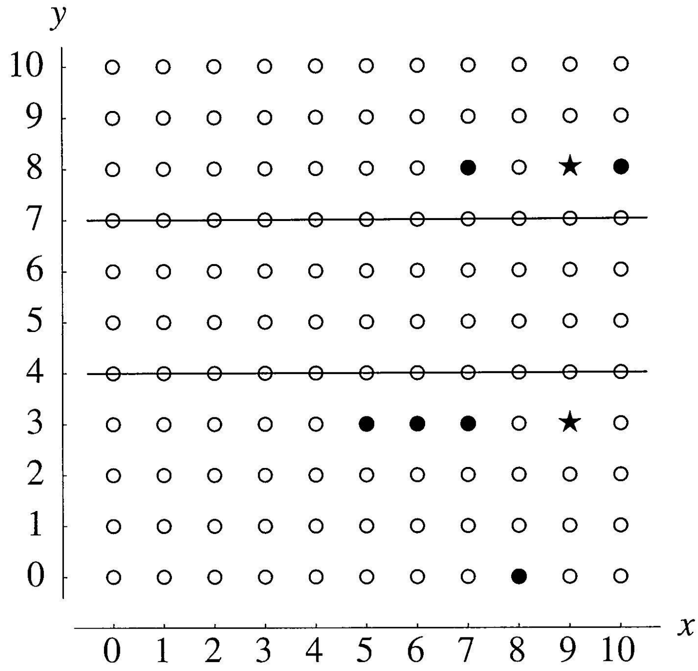
Si $\beta > 2$, alors $4 \mid g$, c-à-d.

$$\frac{1}{4} < \frac{1}{2^{4-\beta}} = |g|_2 \leq \frac{1}{4}.$$

Autrement dit, $\beta = 2$.

En résumé, il y a deux cas possibles pour (β, γ): soit $(0,3)$ soit $(2,0)$. Pour la fin de la démonstration, on se penche sur le premier $p = 11$:

Premier cas: *y et z ne sont pas divisibles par* 11. On sait qu'ils sont composés de facteurs 2 et $p \equiv \pm 1 \pmod{11}$. Si $(\beta, \gamma) = (0,3)$, alors $y \equiv \pm 1 \pmod{11}$ et $z \equiv \pm 2^3 \equiv \pm 8 \pmod{11}$. Leurs réductions se trouvent sur une des deux droites $l_1\colon y = 4z$ ou $l_2\colon y = 7z$ définies sur $\mathbf{F}_{11}$. Si $(\beta, \gamma) = (2,0)$, on a $y \equiv \pm 4 \pmod{11}$ et $z \equiv \pm 1 \pmod{11}$. Leurs réductions se trouvent sur les même droites. Mais ces deux droites ne coupent la courbe $\widehat{C}/\mathbf{F}_{11}$ en



FIGURE

La réduction de la courbe C dans le plan affine $z = 1$ sur $\mathbf{F}_{11}$

aucun point rationnel sur $\mathbf{F}_{11}$. La figure ci-dessus présente une « image » de la courbe dans la carte affine $z = 1$ sur $\mathbf{F}_{11}$. Les points noirs sont des points lisses et les étoiles des points singuliers de $\widehat{C}$.

DEUXIÈME CAS : *z est divisible par* 11. Alors $11 \mid zf = -16N(x - \varepsilon y)$, autrement dit, $x - \varepsilon y = x + y - 4\theta y + \theta^2 y \in (\theta)$. Pour cela il faut que $x + y \in 11\mathbf{Z}$, c-à-d. $x \equiv -y \not\equiv 0 \pmod{11}$. On calcule f modulo 11, sachant que $z \equiv 0 \pmod{11}$:

$$f \equiv 64x^4 - 224x^3y + 108x^2y^2 + 116xy^3 + 10y^4 \equiv 4y^4 \pmod{11}.$$

Dans le cas $(\beta, \gamma) = (0, 3)$, il faut que $y \equiv \pm 1 \pmod{11}$ puisqu'il n'est pas divisible par 11. D'autre part, $f \equiv 4 \pmod{11}$ devrait être le produit de $2^1 \equiv 2 \pmod{11}$ et de facteurs $p \equiv \pm 1 \pmod{11}$. Dans le cas $(\beta, \gamma) = (2, 0)$, on a aussi une contradiction : $y \equiv \pm 4$, $f \equiv 4 \cdot 4^4 \equiv 1 \pmod{11}$ et $f \equiv 2^4 \cdot (\pm 1) \equiv \pm 5 \pmod{11}$.

TROISIÈME CAS : *y est divisible par* 11. Alors $11 \mid yg = -16N(x - \eta z)$. Pour cela il faut que $x + 3z \in 11\mathbf{Z}$. Cette fois-ci on considère g modulo 11, sachant que $y \equiv 0 \pmod{11}$ et $x \equiv -3z \pmod{11}$:

$$g \equiv -96x^4 - 224x^3z + 68x^2z^2 + 160xz^3 - 56z^4 \equiv 9z^4 \pmod{11}.$$

Comme avant, dans le cas $(\beta, \gamma) = (0,3)$: $z \equiv \pm 8$ et $g \equiv 2^4 \cdot (\pm 1) \equiv \pm 5 \not\equiv 9 \cdot 8^4 \equiv 3 \pmod{11}$. Et dans le cas $(\beta, \gamma) = (2,0)$: $z \equiv \pm 1$ et $g \equiv 2^2 \cdot (\pm 1) \not\equiv 9 \pmod{11}$. $\square$

7. La jacobienne de C

Il est certainement intéressant de connaître la jacobienne associée à la courbe. Nous allons construire une application birationnelle

$$\vartheta \colon C \dashrightarrow \mathrm{Jac}(C) = E$$

définie sur $\mathbf{Q}(\omega)$ à l'aide d'une transformation de Cremona de degré 3 du plan.

L'image de la conique B par l'application j est la droite

$$b = \overline{j(B)} = \{x_0 = x_1 = x_2 = 0\} \subset S \subset \mathbf{P}^4_{\mathbf{Q}}\,.$$

Prenons le point $R = (0:0:0:1:\omega) \in b(\mathbf{Q}(\omega))$ et calculons le plan tangent à S en R :

$$T_R S = T_R \mathcal{Q}_0 \cap T_R \mathcal{Q}_1 \colon \ \{-\omega x_0 + x_1 = 0\,, \quad \omega x_1 - x_2 = 0\}\,.$$

L'intersection de S avec $T_R S$ se décompose en deux droites b et e_1, où la seconde, qui correspond au diviseur exceptionnel de j au-dessus du point P_1, est décrite par les équations suivantes :

$$x_1 - \omega x_0 = 0\,, \qquad x_2 - \omega x_1 = 0\,, \qquad x_4 - \omega x_3 - (g_1 + g_3\omega^2 + \omega^4)x_0 = 0\,.$$

A ces trois équations correspondent trois cubiques du plan, passant par les point P_i et ayant un point double en P_1 :

$$\begin{aligned}
&A_0' \colon (y - \omega x)(xz - y^2) = 0\,, \qquad A_1' \colon (z - \omega y)(xz - y^2) = 0\,,\\
&A_2' \colon \ -g_0\omega x^3 + (g_0 - g_1\omega)x^2y + (-g_2\omega - g_3\omega^2 - \omega^4)x^2z\\
&\qquad + (g_1 + g_3\omega^2 + \omega^4)xy^2 + (g_2 - g_3\omega)xyz\\
&\qquad + (g_3 - g_4\omega)xz^2 + (g_4 - \omega)yz^2 + z^3 = 0\,.
\end{aligned}$$

Les trois cubiques $\{A_0', A_1', A_2'\}$ constituent une base du système linéaire de telles cubiques définies sur $\mathbf{Q}(\omega)$. On peut constater que l'application associée $\vartheta' \colon \mathbf{P}^2_{\mathbf{Q}(\omega)} \dashrightarrow \mathbf{P}^2_{\mathbf{Q}(\omega)}$ est birationnelle car deux telles cubiques n'ont qu'un point d'intersection hors des points P_i. Elle contracte les quatre droites P_1P_j en des points $Q_j \in \mathbf{P}^2(\mathbf{Q}(\omega))$ et elle contracte la conique B en un point $Q_1 = (0:0:1)$. D'autre part, elle éclate les points P_i. Le diviseur