Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 47 (2001)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: UNE QUINTIQUE DE GENRE 1 QUI CONTREDIT LE PRINCIPE DE HASSE
Autor: WUTHRICH, Christian
Kapitel: 3. Un corps de nombres
DOI: https://doi.org/10.5169/seals-65433

REMARQUE. D'après le théorème de Riemann-Roch, tout diviseur de degré 1 est linéairement équivalent à un diviseur effectif, c-à-d. à un point rationnel. Pour éviter d'avoir de tels points sur notre courbe, il faut que l'application deg: $\mathrm{Div}(C/\mathbf{Q}) \to \mathbf{Z}$ ait $5\mathbf{Z}$ comme image.

Nous avons utilisé cela pour tamiser une certaine famille de quintiques pour trouver notre exemple: on prend une quintique dont on a vérifié qu'elle a des points locaux. On choisit quelques droites au hasard. L'intersection de la quintique avec chacune des droites doit être un diviseur irréductible sur $\mathbf{Q}$. Sinon la quintique possède des points rationnels. Pour la courbe

$$324x^5 - 36x^4y + x^3y^2 + 45x^2yz^2 - x^2z^3 - xy^2z^2 - 9y^5 + z^5 = 0,$$

par exemple, on ne trouve pas tout de suite un point rationnel. Mais quand on coupe par la droite $3x - y + z = 0$, on trouve un polynôme qui se factorise:

$$9(2y^2 + 3yz - 3z^2)(109y^3 - 96y^2z + 99yz^2 - 4z^3),$$

ce qui montre qu'il y a un point rationnel quelque part.

3. UN CORPS DE NOMBRES

Soit ζ une racine primitive $11^{\text{ème}}$ de l'unité. On considère le corps cyclotomique $\mathbf{Q}(\zeta)$. Pour tous les résultats de ce paragraphe, je me réfère à [CF], chap. 3. L'anneau des entiers $\mathcal{O}_{\mathbf{Q}(\zeta)}$ est égal à $\mathbf{Z}[\zeta]$ et le discriminant vaut $\mathrm{disc}(\mathbf{Q}(\zeta)) = -11^9$. Le premier 11 est totalement ramifié: $11\mathcal{O}_{\mathbf{Q}(\zeta)} = (1-\zeta)^{10}$. Un premier rationnel $p \neq 11$ se décompose en dix idéaux premiers si $p \equiv 1 \pmod{11}$, en cinq si $p \equiv -1 \pmod{11}$; autrement il reste premier si $p^5 \equiv -1 \pmod{11}$ et dans les autres cas il se factorise en deux idéaux premiers.

Dans $\mathbf{Q}(\zeta)$ il y a un sous-corps réel de degré 5, $K = \mathbf{Q}(\zeta + \bar{\zeta})$, qui est le corps fixe sous l'action de l'élément σ d'ordre 2 dans $\mathrm{Gal}(\mathbf{Q}(\zeta):\mathbf{Q})$. Comme l'extension $\mathbf{Q}(\zeta):\mathbf{Q}$ est abélienne, $K:\mathbf{Q}$ est galoisienne. Le discriminant $\mathrm{disc}(K)$ doit diviser celui de $\mathbf{Q}(\zeta)$, ce qui entraîne que 11 est le seul premier ramifié dans K; il est aussi totalement ramifié. On trouve un générateur de l'idéal au-dessus de $11\mathbf{Z}$ en prenant $\theta = N_{\mathbf{Q}(\zeta):K}(1-\zeta) = 2 - \zeta - \bar{\zeta} \in \mathcal{O}_K$. Il est facile de calculer le polynôme minimal de θ:

$$\theta^5 - 11\theta^4 + 44\theta^3 - 77\theta^2 + 55\theta - 11 = 0.$$

De plus, l'anneau des entiers $\mathcal{O}_K$ de K est égal à $\mathbf{Z}[\theta]$. Il est principal; un fait que nous n'utiliserons pas. On a $11\mathcal{O}_K = (\theta)^5$. On peut déduire de l'action de σ sur les idéaux que les premiers rationnels $p \equiv \pm 1 \pmod{11}$ se factorisent

en cinq idéaux premiers distincts dans $\mathcal{O}_K$ tandis que les $p \not\equiv \pm 1 \pmod{11}$ différents de 11 restent premiers. *PARI-GP®* trouve une base des unités modulo torsion, à savoir: $\{\theta - 2,\ \theta - 3,\ \theta^2 - 5\theta + 5,\ \theta^4 - 8\theta^3 + 21\theta^2 - 20\theta + 5\}$.

PROPOSITION 3.1. *Pour tout $\xi \in \mathcal{O}_K$ avec $\xi \notin (\theta)$ on a*

$$N(\xi) = N_{K:\mathbf{Q}}(\xi) \equiv \pm 1 \pmod{11}.$$

Preuve. Puisque $|N(\xi)| = N((\xi))$ et que (ξ) se factorise en idéaux premiers, il suffit de montrer que $N(\mathfrak{p}) \equiv \pm 1 \pmod{11}$ pour tout idéal premier $\mathfrak{p} \neq (\theta)$. Soit $\mathfrak{p}$ est au-dessus d'un premier rationnel $p \equiv \pm 1 \pmod{11}$ et alors sa norme est égal à $\pm p$, soit $\mathfrak{p}$ est de la forme $p\mathcal{O}_K$ et dans ce cas $N(\mathfrak{p}) = p^5 \equiv \pm 1 \pmod{11}$. □

REMARQUE. Dans l'appendice de [Co], Daniel Coray utilise cette extension $K:\mathbf{Q}$ pour construire une quintique qui contredit le principe de Hasse. Mais elle est lisse et donc de genre 6. L'équation s'écrit

$$N(x + \theta y) = z(z^2 + xz + x^2)(2z^2 + xz + x^2).$$

Par ailleurs, le premier contre-exemple qui est une courbe plane lisse de degré 5 a été construit par Fujiwara dans [Fu].

4. CHOIX DE LA COURBE

La quintique C qui nous servira de contre-exemple au principe de Hasse sera une combinaison linéaire

$$C = C_7 + \lambda_0 C_0 + \lambda_1 C_1 + \lambda_2 C_2 + \lambda_3 C_3 + \lambda_4 C_4.$$

On choisit les coefficients g_i et λ_i tels que les termes sans z s'écrivent comme $N(x - \varepsilon y) = N_{K:\mathbf{Q}}(x - \varepsilon y)$ et que les termes sans y s'écrivent comme $N(x - \eta z)$ pour certains ε et $\eta \in K$. J'ai essayé avec un millier de choix différents de (ε, η) pour lesquels il existe des coefficients g_i et λ_i. Parmi ceux auxquels ma méthode de démonstration s'applique, j'ai choisi le plus simple:

$$\varepsilon = -1 + 4\theta - \theta^2 \in \mathcal{O}_K^* \quad \text{et} \quad \eta = -3 + \theta \in \mathcal{O}_K^*,$$

dont les normes sont

$$N(x - \varepsilon y) = x^5 - 6x^4 y + 10x^3 y^2 - x^2 y^3 - 6xy^4 + y^5$$

$$N(x - \eta z) = x^5 + 4x^4 z + 2x^3 z^2 - 5x^2 z^3 - 2xz^4 + z^5,$$