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: 2. Quintiques planes de genre 1

DOI: https://doi.org/10.5169/seals-65433

mais il doit apparemment se restreindre à des courbes elliptiques avec 5-torsion sur $\mathbf{Q}$.

La première partie de cet article décrit la méthode pour construire les courbes qui satisfont la condition géométrique, en utilisant des surfaces de Del Pezzo de degré 4. Après la construction du contre-exemple, la démonstration du théorème est expliquée en détail. J'aimerais attirer l'attention sur la démonstration du cas global qui contient des éléments originaux, comme l'examen simultané – *pour une même équation* – de deux éléments qui sont des normes: voir (4.1) et (4.2). Entièrement programmée sur ordinateur, elle a été appliquée à des familles de courbes pour tamiser un contre-exemple. La fin de l'article est réservée au calcul de la jacobienne E associée à cette quintique qui nous sert de contre-exemple. La normalisée de C représente alors un élément d'ordre 5 dans le groupe de Tate-Shafarevich $\text{Ш}(E/\mathbf{Q})$.

2. Quintiques planes de genre 1

Soit ω un nombre algébrique de polynôme minimal

$$p(X) = g_0 + g_1 X + g_2 X^2 + g_3 X^3 + g_4 X^4 + X^5$$

sur $\mathbf{Q}$. Soit $P_1 = (1 : \omega : \omega^2) \in \mathbf{P}^2(\mathbf{Q}(\omega))$ et soient P_2, P_3, P_4 et P_5 ses conjugués sur $\mathbf{Q}$. On introduit la notation B pour la conique $xz - y^2 = 0$ qui est définie par les P_i. Nous allons chercher toutes les quintiques $C/\mathbf{Q}$ du plan ayant des points doubles en P_1, P_2, P_3, P_4, P_5. Pour cela nous considérons le système linéaire complet des cubiques passant par les points P_i. Prenons comme base les cubiques $A_i/\mathbf{Q}$ suivantes:

$$A_0: \ x(xz - y^2) = 0\,, \qquad A_1: \ y(xz - y^2) = 0\,, \qquad A_2: \ z(xz - y^2) = 0\,,$$
$$A_3: \ g_0 x^3 + g_1 x^2 y + g_2 x^2 z + g_3 xyz + g_4 xz^2 + yz^2 = 0\,,$$
$$A_4: \ g_0 x^2 y + g_1 x^2 z + g_2 xyz + g_3 xz^2 + g_4 yz^2 + z^3 = 0\,.$$

Ceci donne une application birationnelle j de $\mathbf{P}^2_{\mathbf{Q}}$ dans une surface S de Del Pezzo de degré 4 dans $\mathbf{P}^4_{\mathbf{Q}}$, isomorphe au plan éclaté en les cinq points P_i, voir [Be].

Un petit calcul de syzygies montre que S est égale à l'intersection complète des deux quadriques

$$\mathcal{Q}_0: \ x_0 x_4 - x_1 x_3 = g_1 x_0^2 + g_3 x_0 x_2 + x_2^2$$
$$\mathcal{Q}_1: \ x_2 x_3 - x_1 x_4 = g_0 x_0^2 + g_2 x_0 x_2 + g_4 x_2^2$$

définies sur $\mathbf{Q}$.

L'intersection de S avec une quadrique $\mathcal{Q}$ qui ne contient pas la surface se contracte sur $\mathbf{P}^2$ en une sextique ayant des points doubles dans les cinq points P_i. On prend une droite du plan, par exemple $x = 0$, paramétrée par $(s : t) \mapsto (0 : s : t)$. Son image sur la surface S est une cubique gauche h paramétrée par

$$(s : t) \mapsto (0 : -s^3 : -s^2t : st^2 : g_4st^2 + t^3)\,.$$

On cherche toutes les quadriques de $\mathbf{P}^4$ qui contiennent cette cubique gauche h sans contenir toute la surface S. Une telle quadrique coupe la surface le long de h et d'une courbe dont la contraction sur le plan est une quintique ayant un point double en chacun des points P_i. On n'a pas de peine à trouver déjà cinq quadriques dégénérées de la forme $x_0x_i = 0$ pour $0 \leq i \leq 4$. Les quintiques correspondantes s'écrivent comme

$$C_i = A_i + B \qquad \text{pour} \quad 0 \leq i \leq 4\,.$$

De plus, on trouve trois cônes quadratiques de sommet $(1 : 0 : 0 : 0 : 0)$, au-dessus de trois quadriques dans l'hyperplan donné par l'équation $x_0 = 0$:

$$x_1x_3 + x_2^2 = 0\,, \quad x_1x_4 - x_2x_3 - g_4\,x_1x_3 = 0\,, \quad x_2x_4 + x_3^2 - g_4\,x_2x_3 = 0\,.$$

Voici les quintiques associées :

$$C_5\colon\ (xz - y^2)(g_0\,x^2y + g_1\,xy^2 + g_2\,xyz + g_3\,y^2z + g_4\,yz^2 + z^3) = 0\,,$$

$$\begin{aligned} C_6\colon\ &(xz - y^2)(-g_0g_4x^2y - g_0\,x^2z + (g_0 - g_1g_4)\,xy^2 - g_2g_4\ xyz \\ &- g_2\,xz^2 + (g_2 - g_3g_4)\,y^2z - g_4^2\,yz^2 - g_4\,z^3) = 0\,, \end{aligned}$$

$$\begin{aligned} C_7\colon\ &g_0^2\,x^5 + 2g_0g_1\,x^4y + 2g_0g_2\,x^4z + g_1^2\,x^3y^2 + 2(g_1g_2 + g_0g_3)\,x^3yz \\ &+ (g_2^2 + g_0g_4)\,x^3z^2 + (2g_1g_3 + g_0g_4)\,x^2y^2z \\ &+ (3g_0 + 2g_2g_3 + g_1g_4)\,x^2yz^2 + (g_1 + g_2g_4)\,x^2z^3 + (-g_0 + g_1g_4)\,xy^3z \\ &+ (g_1 + g_3^2 + g_2g_4)\,xy^2z^2 + (3g_2 + g_3g_4)\,xyz^3 + g_3\,xz^4 \\ &+ (-g_2 + g_3g_4)\,y^3z^2 + (g_3 + g_4^2)y^2z^3 + 2g_4\,yz^4 + z^5 = 0\,. \end{aligned}$$

On voit que les équations de C_5 et C_6 sont des combinaisons linéaires des équations de C_0, C_2 et C_4. Les quintiques $\{C_0, C_1, C_2, C_3, C_4, C_7\}$ forment une base du système des quintiques du plan ayant des points doubles en $P_1, \ldots, P_5$; on vérifie qu'elles sont indépendantes et que la dimension du système est égale à $\binom{5+2}{2} - 3 \cdot 5 = 6$, car les conditions imposées par les points P_i sont indépendantes.

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

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

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 :

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

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 $\mathrm{Gal}(\mathbf{Q}(\zeta)\colon\mathbf{Q})$. Comme l'extension $\mathbf{Q}(\zeta)\colon\mathbf{Q}$ est abélienne, $K\colon\mathbf{Q}$ 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