Constructions polynomiales et théorie de Galois

JEAN-FRANÇOIS MESTRE

UFR de Math.
Université Paris 7
2 place Jussieu, F-75251 Paris Cedex 05, France

1. Introduction

Soit G un groupe fini. Existe-t-il une extension de $\mathbf{Q}$ (ou plus généralement une infinité d'extensions de $\mathbf{Q}$, ou plus généralement encore une extension régulière de $\mathbf{Q}(t)$) galoisienne de groupe de Galois G?

Lorsque G est extension centrale d'un groupe H par $\mathbf{Z}/2\mathbf{Z}$, et que l'on connaît une extension régulière K de $\mathbf{Q}(t)$ de groupe de Galois H, l'existence d'une extension quadratique M de K telle que $M/\mathbf{Q}(t)$ soit galoisienne de groupe de Galois G est reliée au fait qu'un certain élément α_K de $\mathrm{Br}_2(\mathbf{Q}(t))$ associé à l'extension K est nul [1].

Dans la section 1, nous considérons le cas où H est le groupe alterné A_n ($n \geq 4$), et $G = \tilde{A}_n$ l'unique extension centrale non triviale de A_n par $\mathbf{Z}/2\mathbf{Z}$. Pour n impair, nous construisons des extensions K de $\mathbf{Q}(t)$ de groupe de Galois A_n, dont les ordres des groupes d'inertie sont impairs (en fait égaux à 3). L'invariant α_K est alors constant. Comme, pour $t = \infty$, ces extensions se spécialisent en des algèbres étales scindées $\mathbf{Q}^n$, l'invariant α_K est nul, et le groupe $\tilde{A}_n$ est groupe de Galois d'une extension régulière de $\mathbf{Q}(t)$. Il est facile de voir que le cas n pair se déduit du cas n impair, d'où le théorème:

THÉORÈME 1 *Si n est un entier ≥ 4, le groupe $\tilde{A}_n$ est groupe de Galois d'une extension régulière de $\mathbf{Q}(t)$.*

Dans la section 2, nous traitons le cas où $H = \mathrm{PSL}_2(F_7)$ et $G = \mathrm{SL}_2(\mathbf{F}_7)$. Dans ce cas, LaMacchia a construit des extensions régulières de $\mathbf{Q}(x)$ de groupe de Galois $\mathrm{PSL}_2(\mathbf{F}_7)$ telles que l'invariant $w \in \mathrm{Br}_2(\mathbf{Q}(x))$ associé a 4 points de ramification d'indice pair, et qui, pour certaines valeurs de t, s'annule.

Le théorème

THÉORÈME 2 *Le groupe $\mathrm{SL}_2(\mathbf{F}_7)$ est groupe de Galois d'une extension régulière de $\mathbf{Q}(t)$*

apparaît alors comme un corollaire du théorème suivant:

[1] Plus précisément, si β est l'élément de $H^2(H, \mathbf{Z}/2\mathbf{Z})$ associé à G, et $\rho : \mathrm{Gal}(\overline{\mathbf{Q}(t)}/\mathbf{Q}(t)) \to H$ le morphisme associé à l'extension K, on a $\alpha_K = \rho^*(\beta)$.

Proceedings of the International Congress
of Mathematicians, Zürich, Switzerland 1994
© Birkhäuser Verlag, Basel, Switzerland 1995

THÉORÈME 3 *Soit k un corps de caractéristique différente de 2, et α un élément de $\mathrm{Br}_2(k(x))$, tel que l'élément $\alpha(\infty) \in \mathrm{Br}_2(k)$ obtenu par spécialisation de x en l'infini est nul, et dont la somme des degrés des pôles est ≤ 4. Il existe alors une fraction rationnelle $x = f(t)$ non constante, telle que $f(\infty) = \infty$, et telle que l'élément $f^*(\alpha)$ de $\mathrm{Br}_2(k(t))$ est nul.*

Ce théorème (ainsi que le théorème analogue lorsque la somme des degrés des pôles est ≤ 5) résulte de constructions polynomiales élémentaires.

Dans la section 3, nous montrons comment ces mêmes constructions permettent de construire une courbe elliptique sur $\mathbf{Q}(t)$ de rang 12 (et donc une infinité de courbes elliptiques sur $\mathbf{Q}$ de rang 12).

Les résultats ci-dessus étant soit parus, soit à paraître prochainement, nous avons choisi ici d'insister sur la description des constructions polynomiales qui ont permis de les démontrer.

2. Le groupe $\tilde{A}_n$ est groupe de Galois d'une extension régulière de $\mathbf{Q}(t)$

Le point crucial de la démonstration (*cf.* [2]) est la construction suivante:

Soit n un entier impair. Il existe un polynôme $H \in \mathbf{Q}[X_1, \ldots, X_n]$ tel que tout élément $P = x^n + a_1 x^{n-1} + \ldots + a_n$ de $\mathbf{Q}[x]$ avec $H(a_1, \ldots, a_n) \neq 0$ vérifie les propriétés suivantes:

1) Il existe deux polynômes Q et R de degré $\leq n-1$, premiers avec P, vérifiant

$$P'Q - PQ' = R^2.$$

2) Le polynôme R a ses racines distinctes.
3) Soit t une nouvelle indéterminée. Le discriminant (par rapport à la variable x) du polynôme $F_t = P - tQ$ est égal à $S(t)^2 D$, où D est le discriminant de P et où S est un polynôme en t de degré $n-1$ ayant ses racines distinctes.
4) Si a est une racine de S, le polynôme F_a a une racine triple et $n-3$ racines simples.

L'existence de Q et R vérifiant $P'Q - PQ' = R^2$ résulte du fait que cette égalité est équivalente à un système de n équations linéaires à n inconnues, dont la matrice associée est antisymétrique (et a donc un noyau non nul pour n impair) ([2], p. 485). Les points 2), 3), 4) sont techniques, et en fait résultent de ce qu'ils sont vérifiés dans le cas particulier où $P(x) = x^n - x$ ([2], p. 486).

Soit à présent un polynôme $P \in \mathbf{Q}[x]$ de degré n impair dont les coefficients n'annulent pas H, et dont les racines sont simples et appartiennent à $\mathbf{Q}$. Soit K l'extension de $\mathbf{Q}(t)$ engendrée par les racines du polynôme F_t. Il n'est pas difficile de montrer que son groupe de Galois est le groupe alterné A_n, que les valeurs de ramification sont les $n-1$ racines t_i du polynôme S, et que les groupes d'inertie sont des 3-cycles, donc d'ordre impair. Par suite, l'obstruction $\alpha \in \mathrm{Br}_2(k(t))$ est constante. Pour $t = \infty$, l'extension K se spécialise en l'algèbre étale $\mathbf{Q}^n$, dont l'invariant α associé est nul. Donc $\alpha = 0$, et il existe une extension quadratique M de K dont le groupe de Galois est $\tilde{A}_n$.

REMARQUE 1. La méthode ci-dessus permet également de construire, pour n impair, une infinité d'extensions de $\mathbf{Q}$ totalement réelles de groupe de Galois $\tilde{A}_n$: en effet, la forme $\mathrm{Tr}(x^2)$ de l'extension $K/\mathbf{Q}(t)$ est indépendante de t, et est donc équivalente à la forme $\mathrm{Tr}(x^2)$ de l'algèbre $\mathbf{Q}[x]/(P)$. Si P est scindé sur $\mathbf{Q}$, cette forme est définie positive, d'où le résultat.

REMARQUE 2. Par des constructions analogues, on peut prouver que les groupes $6A_6$ et $6A_7$ (dans les notations de l'Atlas de Conway) sont groupes de Galois d'une extension régulière de $\mathbf{Q}(t)$.

3. Le groupe $\mathrm{SL}_2(\mathbf{F}_7)$ est groupe de Galois d'une extension régulière de $\mathbf{Q}(t)$

Dans [1], LaMacchia a construit des familles d'extensions $K_{a,b}$ régulières de $\mathbf{Q}(a,b)$ de groupe de Galois $\mathrm{PSL}_2(\mathbf{F}_7)$, où a et b sont deux indéterminées.

Lorsque $a = 4$ et $b = 1$, Malle a prouvé que l'extension de $\mathbf{Q}$ obtenue par spécialisation admet une extension quadratique galoisienne sur $\mathbf{Q}$ de groupe de Galois $\mathrm{SL}_2(\mathbf{F}_7)$. Considérons donc l'extension $K_{4,b}$ de $\mathbf{Q}(b)$. On peut montrer qu'elle est ramifiée de type $(3,3)$ en l'infini, et ramifiée d'ordre 2 en 4 autres points. L'invariant $\alpha \in Br_2(\mathbf{Q}(b))$ est donc tel que sa spécialisation en $b = 1$ est nulle, et que la somme des degrés de ses pôles est égale à 4. Le théorème 2 est donc conséquence du théorème 3 ci-dessus.

Soit donc α un élément de $\mathrm{Br}_2(k(x))$, où k est un corps de caractéristique différente de 2, dont la spécialisation en $+\infty$ est nulle. À un tel élément sont associés le polynôme unitaire p produit des pôles de α et le "résidu" de α, qui est un élément $r \in A^*/A^{*2}$, où $A = k[x]/(p)$ (*cf.* [5]).

On va voir que le théorème 3 est une conséquence facile du lemme élémentaire suivant:

LEMME. *Soit p un élément de $k[x]$ de degré $2n$, où n est un entier ≥ 1, et a le coefficient de son terme de degré $2n$. Il existe un unique polynôme $g \in k[x]$ de degré n et de terme dominant a tel que $ap - g^2$ soit de degré $\leq n-1$.*

Il suffit de prendre pour g la partie polynomiale du développement asymptotique de $(ap)^{1/2}$.

La démonstration du théorème 3 est alors immédiate: si t est une nouvelle indéterminée, et si R est un représentant de degré 3 de r (il en existe toujours), d'après le lemme, le polynôme $p + t^2R = g^2 + A(t)x - B(t)$, où A et B sont des éléments de $k(t)$. On peut montrer que B est de degré 8 et A est non nul de degré ≤ 6; le changement de variable $x = B(t)/A(t)$ répond alors à la question: il est tel que $f^*(\alpha) = 0$ et $f(\infty) = \infty$).

Le lemme précédent permet de prouver facilement des assertions voisines, par exemple:

THÉORÈME 4 *Soit k un corps de caractéristique distincte de 2, $p \in k[x]$ un polynôme unitaire de degré 8, $c \in k$, et α l'élément de $\mathrm{Br}_2(k(x))$ égal à (p,c). Il existe un changement de variable non constant $x = f(t)$, où $f \in k(t)$ vérifie $f(\infty) = \infty$, tel que $f^*(\alpha) = 0$.*

La démonstration complète de ce résultat fera l'objet d'un article ultérieur. Nous donnons ici la preuve du théorème ci-dessus lorsque le coefficient de degré 7 de p est nul (ce à quoi on peut toujours se ramener) et lorsque p n'est pas pair (i.e. $p(-x) \neq p(x)$).

Dans ce cas, d'après le lemme, il existe g de degré 4 et r de degré ≤ 3 tels que $p = g^2 + r$; si t est une nouvelle indéterminée, et si $G = g + ct^2/2$, on a donc $p = G^2 - cu^2G + r + c^2u^4/4$. Si l'on applique à présent le lemme au polynôme $cu^2G - r - c^2u^4/4$, on voit que $cu^2G - r - c^2u^4/4 = cH^2 + A(t)x - B(t)$; puisque p n'est pas pair, le polynôme A n'est pas nul. La fraction rationnelle $f = B/A$ répond alors à la question (Et on a même une solution explicite de l'équation $X^2p(f(t)) + Y^2c = Z^2$, avec $(X, Y, Z) = (1, H(f(t)), G(f(t)))$.)

Par une méthode légèrement différente (qui pourrait se ramener à l'application du lemme ci-dessus, mais ce serait artificiel), on peut également montrer le théorème suivant:

THÉORÈME 5 *Soit k un corps de caractéristique différente de 2, et α un élément de $\mathrm{Br}_2(k(x))$ dont la somme des degrés des pôles est ≤ 5, et dont la spécialisation en ∞ est nulle. Il existe une fraction rationnelle $x = f(t)$, de degré ≤ 16, telle que $f(\infty) = \infty$ et $f^*(\alpha) = 0$.*

Nous donnons ici les points principaux permettant de démontrer ce théorème, la démonstration détaillée faisant l'objet d'une publication ultérieure.

Soit p le polynôme unitaire produit des pôles de α, et r un polynôme de degré ≤ 4 représentant le résidu de α. Posons $U = r + ax + b$, $V = v0 + v1x + tx^2$, et $R = R_4x^4 + \ldots + R_0$ le reste de $U^2 - rV^2 \bmod p$. Il est clair que le système $R_4 = R_3 = 0$ est linéaire en a et b; lorsqu'on le résout, on voit que a est de degré 1 en v_0, et que le coefficient de degré 1 de a par rapport à v_0 est linéaire en v_1. On l'annule, et a et v_1 sont donc à présent des éléments de $k(t)$. On remarque alors que R_2 est un polynôme de degré 1 en v_0 (à coefficients dans $k(t)$). On résout donc $R_2 = 0$ par rapport à v_0; par suite, a, b, v_0, v_1 sont à présent des éléments de $k(t)$, et $R = R_1(t)x + R_0(t)$, où R_0 (resp. R_1) est de degré 16 (resp. 14) en t. Par suite, $U^2 - rV^2 \equiv R_1(t)x + R_0(t) \bmod p$, et le lemme 1.2 de [5] permet de conclure: la fraction rationnelle non constante $x = f(t) = -R_0/R_1$ est telle que $f(\infty) = \infty$ et l'on a $f^*(\alpha) = 0$.

4. Courbes elliptiques de rang élevé

Le lemme de la section précédente permet également de construire des courbes elliptiques de rang élevé: soit p un élément de $\mathbf{Q}(t)$ unitaire de degré 12, dont les racines sont distinctes et appartiennent à $\mathbf{Q}$. D'après le lemme, il existe g de degré 6 et r de degré ≤ 5 tels que $p = g^2 - r$. Supposons que r soit de degré 4; la courbe de genre 1 d'équation $y^2 = r(x)$ possède alors les 12 points rationnels $P_i = (x_i, g(x_i))$, où les x_i sont les racines de p.

Une méthode efficace pour trouver de tels polynômes p (tels que r soit de degré 4) est la suivante: soit $q = (x - a_1)\ldots(x - a_6)$ un polynôme de degré 6 scindé sur $\mathbf{Q}$, soit t une indéterminée, et soit $p(x) = q(x - t)q(x + t)$. Le polynôme

r est alors divisible par t^2, et si $R = r/t^2$, le coefficient de degré 5 de R est un polynôme $s(a_1, \ldots, a_6)$ en les a_i indépendant de t.

Par suite, si $s(a_1, \ldots, a_6) = 0$, on obtient une courbe de genre 1 sur $\mathbf{Q}(t)$, d'équation $y^2 = R(x)$, et possédant 12 points rationnels. On en choisit un comme origine, et la courbe elliptique ainsi obtenue est en général de rang 11 sur $\mathbf{Q}(t)$.

Pour obtenir des courbes de rang 12, on remarque que le coefficient de degré 4 de R est de la forme $Pt^2 + Q$, où P et Q sont des polynômes en les a_i. Si, pour certains choix de $(a_1, \ldots, a_6)$ annulant s, la conique (en (t, z)) $Pt^2 + Q = z^2$ a des points, on la paramétrise par $t = f(w)$: les points à l'infini de la courbe $y^2 = R(x)$, définie sur $\mathbf{Q}(w)$, sont alors rationnels sur $\mathbf{Q}(w)$, et l'on obtient ainsi en général une courbe de rang 12 sur $\mathbf{Q}(w)$ ([3]). Comme l'invariant modulaire de cette courbe est non constant, on obtient par spécialisation du paramètre w une infinité de courbes elliptiques sur $\mathbf{Q}$ de rang 12, deux à deux non isomorphes.

On peut donc espérer que par spécialisation on obtienne des courbes elliptiques sur $\mathbf{Q}$ de rang > 12. C'est ce qu'ont fait notamment Fermigier (qui a obtenu des courbes de rang ≥ 19) et Nagao (qui a obtenu une courbe de rang ≥ 21).

De façon plus surprenante, Nagao a remarqué ([6]) qu'en considérant la courbe obtenue en prenant $(a_1, a_2, a_3, a_4, a_5, a_6) = (148, 116, 104, 57, 25, 0)$, on obtient un treizième point rationnel sur $\mathbf{Q}(t)$, d'abscisse $(t + 103)/15$, et indépendant des précédents. De plus, la conique $Pt^2 + Q = z^2$ a un point (car ici $P = 1$), donc il obtient une courbe elliptique sur $\mathbf{Q}(w)$ (d'invariant non constant) de rang ≥ 13 (et donc une infinité de courbes elliptiques deux à deux non isomorphes, définies sur $\mathbf{Q}$, et de rang ≥ 13).

En fait, on peut trouver une famille à deux paramètres (u, v) de telles courbes: Soit $(a_1, a_2, a_3, a_4, a_5, a_6) =$

$$(u^3v^2 - 2u^2v^3 + uv^4 - u^4 - 2u^2v^2 - 2uv^3 + v^4 + u^2v + uv^2 - v^3 + u^2 + 2uv + v^2 - v,$$

$$u^4v - 2u^3v^2 + u^2v^3 + u^4 - 2u^3v - 2u^2v^2 - v^4 - u^3 + u^2v + uv^2 + u^2 + 2uv + v^2 - u,$$

$$u^4 + u^4v - u^3v^2 - 2u^3v - 2u^3 + u^2v^3 + u^2v^2 + u^2 - 2u^2v + 2uv^3 - uv^4 + uv^2 + v^3 - v,$$

$$u^3 - u^4v - 2u^2v + u^2v^2 + u^2v^3 - 2u^2 - 2uv + uv^2 + 2uv^3 + u - v^2 + v^3 - v^4 + v,$$

$$u^3v^2 - u^4v + 2u^3v + u^3 + u^2v^2 - u^2v^3 + u^2v - 2uv^3 - 2uv^2 - u + uv^4 - 2v^3 + v^2 + v^4,$$

$$-a_1 - a_2 - a_3 - a_4 - a_5).$$

On a alors $s(a_1, \ldots, a_6) = 0$, et la courbe elliptique $y^2 = R(x)$, définie sur $\mathbf{Q}(u, v)(t)$, contient un treizième point rationnel sur $\mathbf{Q}(u, v)(t)$, indépendant des précédents, à savoir le point d'abscisse $(A + Bt)/(u^2 + v^2 + 1)$, où

$$A = 3u^3v^2 + 2u^4v + uv - 4v^3u - 3v^2u^2 + 3v^3u^2 - 4u^3v + u + v - u^6 + v^3 - 3v^4$$

$$+2v^5 - v^6 + 3u^2v + 3v^2u + 2v^4u - 3u^4 + u^3 + 2u^5 + u^5v^2 + u^5v - u^4v^3 - 2u^4v^2$$

$$-u^3v^4 - 4u^3v^3 + u^2v^5 - 2u^2v^4 + uv^5$$

et

$$B = -u^2 - v^2 + 2u + 2v + 1.$$

De plus, le terme de degré 4 de R est de la forme $R_4 = C(u,v)^2t^2 + D(u,v)$, où $C(u,v)$ et $D(u,v)$ sont des éléments de $\mathbf{Q}[u,v]$. donc en paramétrant la conique (en (t,z)) $R_4 = z^2$ par $t = f(w)$, on obtient une famille à deux paramètres (u,v) de courbes elliptiques sur $\mathbf{Q}(w)$ de rang ≥ 13. On retrouve la courbe de Nagao en prenant $(u,v) = (2,5)$.

REMARQUE. Le même type de constructions permet de construire une infinité de courbes elliptiques sur $\mathbf{Q}$, non deux à deux $\mathbf{Q}$-isomorphes, d'invariant modulaire égal à 0 (resp. 1728), et dont le rang est ≥ 6 (resp. ≥ 4) ([4]).

References

[1] M. E. LaMacchia, *Polynomials with Galois group $PSL(2,7)$*, Commun. Alg. **8** (1980), 983–992.

[2] J.-F. Mestre, *Extensions régulières de $\mathbf{Q}(t)$ de groupe de Galois $\tilde{A}_n$*, J. of Alg. **131** (1990), 483–495.

[3] ———, *Courbes elliptiques de rang 12 sur $\mathbf{Q}(t)$*, C. R. Acad. Sci. Paris **313** (1991), 171–174.

[4] ———, *Rang de courbes elliptiques d'invariant donné*, C. R. Acad. Sci. Paris **314** (1992), 919–922.

[5] ———, *Annulation, par changement de variable, d'éléments de* $\mathrm{Br}_2(k(x))$ *ayant quatre pôles*, C. R. Acad. Sci. Paris **319** (1994), 529–532.

[6] K. Nagao, *An example of Elliptic Curve over $\mathbf{Q}(T)$ with Rank ≥ 13*, Proc. of the Japan Acad. **70** (1994), 152–153.