ACTA ARITHMETICA
127.2 (2007)

Trinômes irréductibles résolubles sur un corps de nombres

par

Julien Angeli (Limoges)

1. Introduction. Le problème de la détermination des trinômes $X^n - aX^m + b$ à coefficients dans un corps de nombres k, avec n et m premiers entre eux, et dont le groupe de Galois est un sous-groupe G de S_n donné, se ramène à la recherche de points k-rationnels sur une certaine courbe algébrique, dépendant de G, n et m. Le calcul du genre de cette courbe présente alors un intérêt important : on sait que l'on a trois comportements très différents lorsque $g = 0$, $g = 1$ ou $g \geq 2$. Dans ce dernier cas, la conjecture de Mordell, démontrée par Faltings [6], affirme qu'il n'existe qu'un nombre fini de points rationnels sur la courbe. À homothétie des racines près, il n'existera alors qu'un nombre fini de tels trinômes.

Pour tout entier n premier, on se propose de déterminer le genre de la courbe correspondant au groupe $G = \mathrm{AGL}(1, n)$ des transformations affines sur le corps à n éléments, vu comme un sous-groupe de S_n. On recherche de cette façon les trinômes irréductibles et résolubles : c'est une propriété bien connue que tout polynôme irréductible et résoluble de degré n a son groupe de Galois inclus dans le groupe affine $\mathrm{AGL}(1, n)$ (cf. [1]). Le cas $n = 5$ est déjà connu dans la littérature [9]. Pour $m = 1$, le genre de la courbe vaut 0 et on a une famille paramétrée de trinômes résolubles : les $(4u^2 + 16)x^5 + (5u^2 - 5)x + (4u^2 + 10u + 6)$ (cf. [11]). Pour $m = 2$, le genre vaut 1. La courbe est une courbe elliptique de rang 0 dont les points $\mathbb{Q}$-rationnels donnent exactement 5 trinômes de $\mathbb{Q}[t]$ résolubles (à équivalence près) : $5x^5 - 10x^2 - 1$, $x^5 - 100x^2 - 1000$, $x^5 - 5x^2 - 3$, $x^5 - 5x^2 + 15$, $x^5 - 25x^2 - 300$. On montre ici que pour tout $n > 5$ premier, le genre cherché est toujours supérieur à 2 et qu'il n'existe donc qu'un nombre fini, à équivalence près, de trinômes irréductibles résolubles de degré n sur tout corps de nombres k.

Quelques exemples similaires de calculs du genre sont déjà connus. L'article de A. Schinzel [8] traite le cas où G est non transitif. Une expression

2000 *Mathematics Subject Classification*: 11R32, 11S15, 12F12.

générale du genre est donnée lorsque $G = S_p \times S_{n-p}$. Il est ensuite possible de déterminer quels sont les triplets (n, m, p) pour lesquels le genre est nul, d'en déduire quels sont les trinômes $X^n - aX^m + b$, avec $b^{n-m}a^{-n} \notin \mathbb{Q}$ à coefficients dans $\mathbb{Q}(t)$, qui se factorisent en deux facteurs de degré p et $n-p$, et enfin de donner leur factorisation explicite. En dehors des cas $p = 1$, $p = 2$ et des triplets $(2p, p, p)$, on obtient une liste finie de 12 factorisations possibles.

Dans l'article de N. Bruin et N. D. Elkies [2], on donne le genre, égal à 2, puis l'équation, de la courbe correspondant au groupe $G = \mathrm{PSL}(3, 2)$, pour $n = 7$ et $m = 1$. La courbe n'a qu'un nombre fini de points $\mathbb{Q}$-rationnels, et une recherche informatique permet de les déterminer tous. On retrouve ainsi les trinômes déjà connus de Trinks–Matzat ($X^7 - 7X + 3$, cf. [10]) et de Erbach–Fischer–McKay ($X^7 - 154X + 99$, cf. [5]), auxquels viennent s'ajouter deux nouveaux trinômes. Un travail similaire est effectué pour $n = 8$, $m = 1$, et $G = \mathrm{AGL}(3, 2)$, le groupe des transformations affines de $(\mathbb{F}_2)^3$. La courbe correspondante est elle aussi de genre 2, et la recherche (non exhaustive) de points rationnels donne quatre trinômes exceptionnels jusque là inconnus.

Un panorama très complet sur les trinômes peut être trouvé sur le site de N. D. Elkies [4].

2. La courbe $C(\overline{k})$

2.1. *Notations.* Dans la suite, k sera un corps de nombres, et $\overline{k}$ sa clôture algébrique. On se donne deux entiers premiers entre eux n et m, avec $0 < m < n$, et G un sous-groupe quelconque de S_n. On définit l'ensemble des trinômes (n, m) sur $\overline{k}$:

$$\mathcal{T}_{n,m}(\overline{k}) = \{X^n - aX^m + b : a, b \in \overline{k}^\times\}.$$

On rappelle que le groupe $\overline{k}^\times$ agit sur $\overline{k}[X]$ et $\mathcal{T}_{n,m}(\overline{k})$ par $\mu.P(X) = \mu^{-n}P(\mu X)$. Cette action laisse le groupe de Galois invariant. Si on se fixe deux entiers r et s tels que $s(n-m) - rn = 1$, alors chaque trinôme $X^n - aX^m + b$ est équivalent à un unique *trinôme réduit* $X^n - t^rX^m + t^s$. On appelle *paramètre* du trinôme la quantité t, qui est égale à $b^{n-m}a^{-n}$.

On définit le trinôme générique $T(X) = X^n - t^rX^m + t^s \in \overline{k}(t)[X]$. On note N (respectivement N_0) son corps des racines sur $\overline{k}(t)$ (respectivement $k(t)$). Le groupe de Galois des extensions $N/\overline{k}(t)$ et $N_0/k(t)$ est S_n (cf. [8]). Comme G est un sous-groupe de S_n, il agit naturellement sur N (respectivement N_0), et on peut introduire le corps N^G (respectivement N_0^G) fixé par G.

2.2. *La courbe $C(\overline{k})$.* Les corps N et N^G sont des extensions de $\overline{k}$ de degré de transcendance 1. Or, la catégorie des extensions de degré de transcendance 1 sur $\overline{k}$, dont les flèches sont les $\overline{k}$-morphismes, est équivalente à la

catégorie des courbes quasi-projectives, dont les flèches sont les morphismes rationnels dominants [7]. Cela nous permet d'introduire les courbes $C(\overline{k})$, $C_G(\overline{k})$ et $\mathbb{P}^1(\overline{k})$, dont les corps de fonctions respectifs sont N, N^G et $\overline{k}(t)$:

$$\begin{array}{cc} N & C(\overline{k}) \\ | & \downarrow \\ N^G & C_G(\overline{k}) \\ | & \downarrow \\ \overline{k}(t) & \mathbb{P}^1(\overline{k}) \end{array}$$

De $C(\overline{k})$, on peut donner un modèle explicite : À tout point $(\lambda_0 : \ldots : \lambda_{n-1})$ de $\mathbb{P}^{n-1}(\overline{k})$, on associe la classe d'équivalence du polynôme

$$\prod_{i=0}^{n-1}(X-\lambda_i) = X^n - \sigma_1 X^{n-1} + \cdots + (-1)^{n-1}\sigma_{n-1}X + (-1)^n\sigma_n$$

où σ_i est la fonction symétrique élémentaire de degré i des coordonnées $\lambda_0, \ldots, \lambda_{n-1}$.

On prend pour $C(\overline{k})$ l'ensemble des points de $\mathbb{P}^{n-1}(\overline{k})$ associés aux trinômes de $\mathcal{T}_{n,m}(\overline{k})$, c'est-à-dire la variété algébrique définie par les équations homogènes $\sigma_i = 0$, pour $1 \leq i < n-m$, $n-m < i < n$.

Pour se représenter $C_G(\overline{k})$, rappelons que $C(\overline{k})$, $C(k)$, $C_G(\overline{k})$ et $C_G(k)$ s'identifient respectivement à l'ensemble des places de degré 1 de N, N_0, N^G et N_0^G. Il y a alors une bijection naturelle entre $C_G(\overline{k})$ et l'ensemble des G-orbites des points de $C(\overline{k})$ (cf. [3], notamment le théorème 2 du chapitre IV).

2.3. *Inertie de l'extension $N/\overline{k}(t)$.* On aura besoin de connaître l'inertie de $N/\overline{k}(t)$. C'est un résultat déjà connu ([8]), que l'on se contente de rappeler :

PROPOSITION 1. *Soit $t_0 = m^m(n-m)^{n-m}n^{-n}$. Un trinôme de $\mathcal{T}_{n,m}(\overline{k})$ est inséparable si, et seulement si, son paramètre est égal à t_0.*

On note respectivement v_0, v_{t_0} et v_∞ les places (t)-adique, $(t-t_0)$-adique et $(1/t)$-adique de $\overline{k}(t)$.

Alors v_0, v_{t_0} et v_∞ sont les seules places de $\overline{k}(t)$ qui se ramifient dans N.

- *Si w est une place de N au-dessus de v_0, alors le groupe d'inertie $I(w \mid v_0)$ est engendré par le produit disjoint d'un m-cycle et d'un $(n-m)$-cycle.*
- *Si w est une place de N au-dessus de v_{t_0}, alors $I(w \mid v_{t_0})$ est engendré par une transposition.*
- *Si w est une place de N au-dessus de v_∞, alors $I(w \mid v_\infty)$ est engendré par un n-cycle.*

2.4. *Paramétrisation des trinômes de groupe de Galois inclus dans G.* Il existe sur $C(\overline{k})$ une fonction rationnelle $\tau : C(\overline{k}) \to \mathbb{P}^1(\overline{k})$ qui à tout point de la courbe associe le paramètre du trinôme correspondant ; sa valeur est $(-1)^n \sigma_n^{n-m} \sigma_{n-m}^{-n}$.

La fonction τ est invariante sous l'action de S_n, on dispose donc sur $C_G(\overline{k})$ ou $\mathbb{P}^1(\overline{k})$ de la fonction image de τ, qu'on notera encore τ.

Il est clair que l'image par τ d'un point k-rationnel $(\lambda_0 : \ldots : \lambda_{n-1})$ de $C(\overline{k})$ est le paramètre d'un trinôme $\prod_{i=0}^{n-1}(X - \lambda_i)$ scindé sur k, c'est-à-dire de groupe de Galois trivial. Plus généralement, on a la propriété suivante :

Proposition 2. *Les paramètres des k-trinômes séparables, dont le groupe de Galois est inclus dans G, sont exactement les $\tau(P)$ différents de 0, t_0 et ∞, pour $P \in C_G(k)$.*

On utilise le lemme suivant :

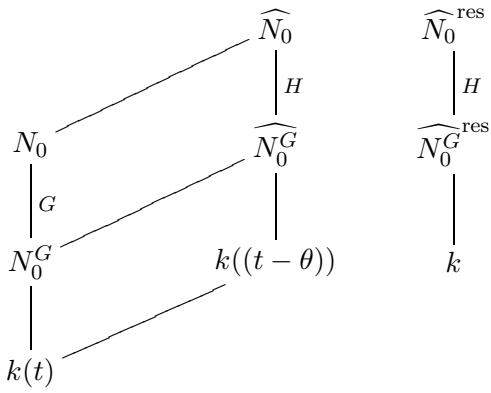
Lemme 1. *Soit $P \in k(t)[X]$ et $\theta \in k$. Soit N le corps des racines de P sur $k(t)$, v une place de N au-dessus de la place $(t-\theta)$-adique de $k(t)$, et $\widehat{N}$ le complété de N pour la place v. On suppose que la réduction P^{res} de P modulo v est un polynôme séparable de $k(t)$. Alors le corps résiduel $\widehat{N}^{\mathrm{res}}$ est le corps des racines de P^{res} sur k.*

Preuve. Le polynôme P est lui aussi séparable, on note $L_0, \ldots, L_{n-1}$ ses racines distinctes dans N. Il est clair que leurs réductions $\lambda_0, \ldots, \lambda_{n-1}$ dans $\widehat{N}^{\mathrm{res}}$ sont des racines de P^{res}. D'après le lemme de Hensel, on peut relever chaque λ_i en une unique racine de P, donc les λ_i sont distincts, et $\widehat{N}^{\mathrm{res}}$ contient toutes les racines de P^{res}.

Il suffit alors de montrer que $\widehat{N}^{\mathrm{res}}$ est engendré par les λ_i. On peut introduire un élément primitif u de $\widehat{N}$ tel que $u \in k[L_0, \ldots, L_{n-1}]$. Sa réduction u^{res} modulo v appartient alors à $k[\lambda_0, \ldots, \lambda_{n-1}]$. Choisissons un élément a^{res} de $\widehat{N}^{\mathrm{res}}$; il se relève en $a = \sum f_i(t-\theta)u^i \in \widehat{N}$. Les séries f_i sont entières ; sinon, en multipliant par $(t-\theta)^j$, où j est le plus grand ordre des pôles des f_i, et en réduisant modulo v, on aboutit à une contradiction. Par conséquent, $a^{\mathrm{res}} = \sum f_i(0)(u^{\mathrm{res}})^i \in k[\lambda_0, \ldots, \lambda_{n-1}]$, ce qui démontre le lemme. ∎

Preuve de la proposition 2. Supposons d'abord que P soit un point de $C_G(k)$ tel que la quantité $\theta = \tau(P)$ soit différente de 0, t_0 et ∞.

Au point P correspond une place v_P de N_0^G ; on note $\widehat{N_0^G}$ le complété de N_0^G pour v_P. La place v_P est au-dessus d'une place v_θ de $k(t)$, et on complète ce dernier pour obtenir le corps $k((t-\theta))$. Enfin, on choisit une place v de N_0 au-dessus de v_P, et on complète N_0 en le corps $\widehat{N_0}$. On obtient ainsi une tour de corps complétés :



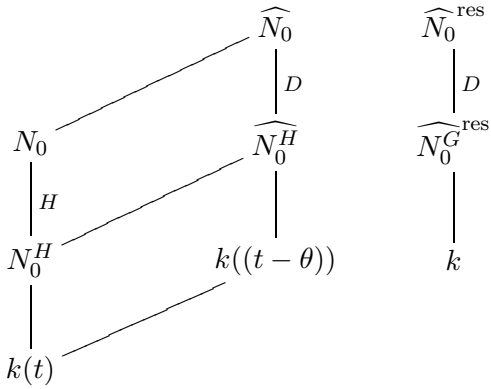
Le groupe de Galois H de l'extension $\widehat{N_0}/\widehat{N_0^G}$ est le sous-groupe de décomposition du groupe de Galois G de N_0/N_0^G, pour la place v de N_0 choisie.

Le groupe de Galois entre les corps résiduels $\widehat{N_0}^{\mathrm{res}}$ et $\widehat{N_0^G}^{\mathrm{res}}$ est le quotient du groupe de décomposition H par le sous-groupe d'inertie ; comme θ est différent de 0, t_0, ∞, l'extension $\widehat{N_0}/\widehat{N_0^G}$ est non ramifiée, et $\mathrm{Gal}(\widehat{N_0}^{\mathrm{res}}/\widehat{N_0^G}^{\mathrm{res}})$ s'identifie à $\mathrm{Gal}(\widehat{N_0}/\widehat{N_0^G}) = H$.

Le corps résiduel de $\widehat{N_0^G}$ est égal à k car P est k-rationnel, et $\widehat{N_0}^{\mathrm{res}}$ est le corps des racines de $X^n - \theta^r X^m + \theta^s$ sur k.

Ceci démontre un sens de l'équivalence.

Réciproquement, soit $\theta \in k$ tel que le trinôme $X^n - \theta^r X^m + \theta^s$ soit séparable, de groupe de Galois sur k inclus dans G. On a alors θ différent de 0, t_0 et ∞. Notons $\lambda_0, \ldots, \lambda_{n-1}$ les racines de $X^n - \theta^r X^m + \theta^s$. Comme précédemment, on introduit les corps complétés. Le point $(\lambda_0 : \ldots : \lambda_{n-1})$ de $C(\overline{k})$ est associé à une place v de N_0. On appelle $k((t-\theta))$, $\widehat{N_0^H}$ et $\widehat{N_0}$ les complétés par rapport à v :



Le corps résiduel $\widehat{N_0}^{\mathrm{res}}$ est le corps des racines sur k du trinôme $X^n - \theta^r X^m + \theta^s$.

Le groupe de Galois entre $\widehat{N_0}^{\mathrm{res}}$ et $\widehat{N_0^G}^{\mathrm{res}}$ est aussi le groupe de décomposition $D = \mathrm{Gal}(\widehat{N_0}/\widehat{N_0^H})$; c'est un sous-groupe de $H = \mathrm{Gal}(\widehat{N_0}^{\mathrm{res}}/k)$. On en déduit que $\widehat{N_0^G}^{\mathrm{res}} = k$.

Par conséquent, la restriction de la place v est de degré 1 sur N_0^H, elle est donc *a fortiori* de degré 1 sur le corps N_0^G, qui est inclus dans N_0^H. Par conséquent, le point P de $C_G(\overline{k})$, image de $(\lambda_0, \ldots, \lambda_{n-1})$, est k-rationnel. Comme $\theta = \tau((\lambda_0 : \ldots : \lambda_{n-1})) = \tau(P)$, cela conclut la démonstration. ∎

3. Calcul et minoration du genre. Désormais n est un nombre premier, et G est le groupe affine $\mathrm{AGL}(1, n)$ sur le corps $\mathbb{F}_n$. Remarquons qu'il existe plusieurs choix possibles d'un plongement de G dans S_n, qui correspondent à des numérotations différentes des racines. Dans la suite, on suppose que ce choix a été fait une fois pour toutes.

Dans cette section, on calcule le genre du corps N^G, et donc de la courbe $C_G(\overline{k})$. Pour cela, on calcule les groupes d'inertie de l'extension $N^G/\overline{k}(t)$, on obtient les indices de ramifications comme cardinaux de ces groupes, et on utilise la formule de Riemann–Hurwitz.

3.1. *Structure de G.* Le groupe G des transformations affines sur $\mathbb{F}_n$ est un groupe d'ordre $n(n-1)$. Il est la réunion des sous-groupes d'intersections triviales suivants :

(i) le groupe cyclique d'ordre n des translations,
(ii) les n groupes cycliques d'ordre $n-1$ des transformations affines fixant un point $a \in \mathbb{F}_n$ (c'est-à-dire des homothéties de centre a).

Dans la suite, v est la place v_0, v_{t_0} ou v_∞ de $\overline{k}(t)$, w est une place de N^G au-dessus de v, et u une place de N au-dessus de w. On a

$$\begin{array}{ll} u & N \\ & \big\downarrow {\scriptstyle n(n-1)} \\ w & N^G \\ & \big\downarrow {\scriptstyle (n-2)!} \\ v & \overline{k}(t) \end{array}$$

3.2. *Nombre de branchement au-dessus de v_∞.* Il y a $(n-1)!$ places u de N au-dessus de v_∞, et leurs groupes d'inertie $I(u \,|\, v_\infty)$ sont des groupes cycliques d'ordre n. De plus, $I(u \,|\, w) = I(u \,|\, v_\infty) \cap G$.

Il y a $(n-2)!$ groupes cycliques d'ordre n dans S_n. Chacun d'entre eux est le groupe d'inertie I de $n-1$ places. En effet, si I est le groupe d'inertie de $u_1, \ldots, u_k$, et si $\sigma \in \mathrm{Gal}(N/L) = G$, alors $\sigma^{-1} I \sigma$ est le groupe d'inertie

de $u_1 \circ \sigma, \ldots, u_k \circ \sigma$, et l'action du groupe de Galois sur les places au-dessus de v_∞ est transitive.

L'un de ces $(n-2)!$ groupes est inclus dans le groupe affine G (il s'agit du sous-groupe des translations), tous les autres intersectent G trivialement.

Donc $n-1$ places u sont ramifiées au-dessus de w, d'indice $e(u \mid w) = n$, et les $(n-1)((n-2)!-1)$ places u restantes sont non ramifiées au-dessus de w.

Par conséquent, si on examine la ramification entre N^G et $k(t)$, on voit qu'il y a une place w non ramifiée au-dessus de $k(t)$, et $((n-2)!-1)/n$ places w ramifiées, avec un indice $e(w \mid v_\infty) = n$.

On en déduit le nombre de branchement :

$$B_\infty = \frac{1}{2}\sum_w (e-1) = \frac{1}{2}\,\frac{(n-2)!-1}{n}\,(n-1).$$

3.3. *Nombre de branchement au-dessus de v_{t_0}.* Cette fois, les groupes d'inertie I sont d'ordre 2. Le groupe G ne contenant pas de transposition, l'intersection $I(u \mid v_{t_0}) \cap G$ est toujours triviale. Donc il n'y a pas de ramification entre N et N^G, toute la ramification se situe entre les corps N^G et $k(t)$. On en déduit qu'il y a $(n-2)!/2$ places w ramifiés au-dessus de v_{t_0}, d'indice $e(w \mid v_{t_0}) = 2$, ce qui donne le nombre de branchement

$$B_{t_0} = \frac{(n-2)!}{4}.$$

3.4. *Nombre de branchement au-dessus de v_0, quand $m > 1$.* On distingue deux cas pour le calcul de B_0. Le cas simple est celui où $m > 1$. En effet, les groupes d'inerties sont alors engendrés par le produit disjoint d'un m-cycle et d'un $(n-m)$-cycle. Comme la seule transformation affine fixant deux points est l'identité, l'intersection de G et d'un tel groupe d'inertie est toujours triviale.

Comme il y a $n!/m(n-m)$ places u de N au-dessus de v_0, et comme toute la ramification se situe entre N^G et $k(t)$, il y a $(n-2)!/m(n-m)$ places w au-dessus de v_0, d'indice $e(w \mid v_0) = m(n-m)$. On obtient donc

$$B_0 = \frac{(n-2)!}{2m(n-m)}\,(m(n-m)-1).$$

3.5. *Nombre de branchement au-dessus de v_0, quand $m = 1$.* Cette fois, les groupes d'inertie sont des groupes cycliques d'ordre $n-1$, et leur intersection avec G n'est pas toujours triviale. Pour tout d divisant $n-1$, on veut dénombrer les groupes d'inertie I dont l'intersection avec G est d'ordre d. Notons α_d leur nombre.

Soit H un sous-groupe cyclique de G engendré par une permutation σ, produit de $(n-1)/d$ d-cycles disjoints.

- Le groupe H contient $\phi(d)$ générateurs.

- Chacun de ces générateurs a $\prod_{k=1}^{(n-1)/d-1}(n-1-kd)$ racines $(n-1)/d$-ièmes (qui sont des $(n-1)$-cycles).
- Chaque groupe I contient $\phi(n-1)$ générateurs, qui sont ces $(n-1)$-cycles.

Par conséquent, H est inclus dans

$$\frac{\phi(d)}{\phi(n-1)} \prod_{k=1}^{(n-1)/d-1} (n-1-kd)$$

groupes I, quantité égale après simplification à

$$\frac{\phi(d)}{\phi(n-1)}\, d^{(n-1)/d-1}\left(\frac{n-1}{d}-1\right)!.$$

Comme il existe n tels groupes H dans G, on en déduit l'égalité

$$\sum_{d|e|n-1} \alpha_e = n\,\frac{\phi(d)}{\phi(n-1)}\, d^{(n-1)/d-1}\left(\frac{n-1}{d}-1\right)!.$$

On applique la formule d'inversion de Möbius pour obtenir

$$\alpha_d = \sum_{d|e|n-1} n\,\frac{\phi(e)}{\phi(n-1)}\, e^{(n-1)/e-1}\left(\frac{n-1}{e}-1\right)!\,\mu\left(\frac{e}{d}\right).$$

Chaque groupe I est le groupe d'inertie de $\phi(n-1)$ places u de N, ramifiées au-dessus de w, d'indice $e(u\,|\,w) = |I \cap G|$.

Il y a donc $\alpha_d\phi(n-1)$ places de N d'indice $e = d$ au-dessus de N^G.

À ces places correspondent $\alpha_d\phi(n-1)d/n(n-1)$ places w de N^G, d'indice de ramification $(n-1)/d$ au-dessus de v_0, et on peut calculer le nombre de branchement correspondant à la place v_0 :

$$\begin{aligned} B_0 &= \frac{1}{2}\sum_{d|n-1} \alpha_d\phi(n-1)\,\frac{d}{n(n-1)}\left(\frac{n-1}{d}-1\right) \\ &= \frac{1}{2}\sum_{d|e|n-1} \phi(e)e^{(n-1)/e-1}\left(\frac{n-1}{e}-1\right)!\,\mu\left(\frac{e}{d}\right)\left(1-\frac{d}{n-1}\right) \\ &= \frac{1}{2}\sum_{e|n-1} \phi(e)e^{(n-1)/e-1}\left(\frac{n-1}{e}-1\right)!\sum_{d|e}\mu\left(\frac{e}{d}\right)\left(1-\frac{d}{n-1}\right). \end{aligned}$$

En posant $f = e/d$, la somme $\sum_{d|e}\mu(e/d)(1-d/(n-1))$ s'écrit

$$\sum_{f|e}\mu(f) - \frac{e}{n-1}\sum_{f|e}\frac{\mu(f)}{f}.$$

Le terme $\sum_{f|e}\mu(f)$ vaut 1 si $e = 1$, et 0 sinon. Le terme $U(e) := \sum_{f|e}\mu(f)/f$ est égal à $\phi(e)/e$. En effet, U est une fonction multiplicative, et $U(p^k) =$

$1 - 1/p = \phi(p^k)/p^k$. On aboutit à l'expression suivante de B_0 :

$$B_0 = \frac{1}{2}\,(n-2)! - \frac{1}{2(n-1)} \sum_{e|n-1} \phi(e)^2 e^{(n-1)/e-1} \left(\frac{n-1}{e} - 1\right)!.$$

3.6. *Genre de la courbe et minoration*

Proposition 3. *Si $m = 1$, alors le genre g de la courbe est égal à*

$$g = \frac{1}{2} + \frac{1}{2n} + (n-2)!\left(\frac{1}{4} - \frac{1}{2n}\right) - \frac{1}{2(n-1)} \sum_{e|n-1} \phi(e)^2 e^{\frac{n-1}{e}-1} \left(\frac{n-1}{e} - 1\right)!.$$

Si $m > 1$, alors le genre g vaut

$$g = \frac{1}{2} + \frac{1}{2n} + (n-2)!\left(\frac{1}{4} - \frac{1}{2n} - \frac{1}{2m(n-m)}\right).$$

Dans tous les cas, on a $g > 1$ pour tout premier $n > 5$.

Preuve. L'expression du genre s'obtient à partir de la formule de Riemann–Hurwitz :

$$g = 1 - [S_n : G] + B_\infty + B_{t_0} + B_0.$$

La minoration de g dans le cas $m > 1$ s'obtient simplement : On a $2n \geq 12$, $2m(n-m) \geq 10$ et $(n-2)! \geq 24$, donc

$$g > \frac{1}{2} + 24\left(\frac{1}{4} - \frac{1}{12} - \frac{1}{10}\right) > 1.$$

Dans le cas $m = 1$, on majore le terme $\phi(e)^2 e^{(n-1)/e-1}\big(\frac{n-1}{e} - 1\big)!$ pour $e > 1$:

$$\phi(e)^2 e^{(n-1)/e-1} \left(\frac{n-1}{e} - 1\right)! < e(e^{1/e})^{n-1} \left(\frac{n-1}{2} - 1\right)!.$$

Une étude élémentaire de la fonction $x \mapsto x^{1/x}$ montre que $e^{1/e} \leq 3^{1/3}$. Donc

$$\phi(e)^2 e^{(n-1)/e-1} \left(\frac{n-1}{e} - 1\right)! < \left(\frac{n-1}{2} - 1\right)! \, 3^{(n-1)/3}(n-1).$$

Quand $n \geq 13$, ce produit est inférieur (terme à terme) à $2(n-3)!$. Alors

$$g \geq \frac{1}{2} + \frac{1}{2n} + (n-2)!\left(\frac{1}{4} - \frac{1}{2n}\right) - \frac{1}{2(n-1)} \left((n-2)! + \frac{n-2}{2} \cdot 2(n-3)!\right)$$

et

$$g > (n-2)!\left(\frac{1}{4} - \frac{1}{2n} - \frac{1}{n-1}\right) \geq 2.$$

Pour conclure la démonstration, il ne reste qu'à vérifier la valeur de g pour les petites valeurs de n :

n	g
5	0
7	10
11	56058

■

On peut donner finalement le résultat :

THÉORÈME 1. *Pour tout entier premier $n > 5$, pour tout corps de nombres k, il n'existe qu'un nombre fini, à équivalence près, de k-trinômes de degré n irréductibles et résolubles sur k.*

Preuve. D'après le théorème de Faltings [6], la courbe $C_G(\overline{k})$, de genre strictement supérieur à 1, n'admet qu'un nombre fini de points k-rationnels. Donc il n'existe qu'un nombre fini de k-trinômes $X^n - aX^m + b$ de groupe de Galois inclus dans le groupe affine. Comme il n'y a qu'un nombre fini de m possibles, le résultat s'en déduit. ■

Références

[1] E. Artin, *Galois Theory*, Dover, Mineola, NY, 1998.

[2] N. Bruin and N. D. Elkies, *Trinomials $ax^7 + bx + c$ and $ax^8 + bx + c$ with Galois groups of order* 168 *and* $8 \cdot 168$, in: Lecture Notes in Comput. Sci. 2369, Springer, Berlin, 2002, 172–188.

[3] C. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable*, Amer. Math. Soc., New York, 1951.

[4] N. D. Elkies, *Trinomials $ax^n + bx + c$ with interesting Galois groups*, http://www.math.harvard.edu/~elkies/trinomial.html.

[5] D. W. Erbach, J. Fischer and J. McKay, *Polynomials with* $\mathrm{PSL}(2,7)$ *as Galois group*, J. Number Theory 11 (1979), 69–75.

[6] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366.

[7] R. Hartshorne, *Algebraic Geometry*, Grad. Texts in Math. 52, Springer, New York, 1977.

[8] A. Schinzel, *On reducible trinomials*, Dissertationes Math. 329 (1993); Errata, Acta Arith. 73 (1995), 399–400.

[9] B. K. Spearman and K. S. Williams, *On solvable quintics x^5+ax+b and x^5+ax^2+b*, Rocky Mountain J. Math. 26 (1996), 753–772.

[10] W. Trinks, *Ein Beispiel eines Zahlkörpers mit der Galoisgruppe* $\mathrm{PSL}(3,2)$ *über* $\mathbb{Q}$, manuscrit, Univ. Karlsruhe, 1968.

[11] H. Weber, *Lehrbuch der Algebra*, Vieweg, Braunschweig, 1895–1896.

Département de Mathématiques et Informatique
XLIM (UMR CNRS 6172)
Université de Limoges
123 avenue Albert Thomas
87060 Limoges Cedex, France
E-mail: julien.angeli@xlim.fr

Reçu le 27.7.2006
et révisé le 16.10.2006 (5250)