ANNALES DE L'INSTITUT FOURIER

MICHEL KERVAIRE

Corps quadratiques, $GL_2(\mathbf{Z})$ et polynômes de Dickson

Annales de l'institut Fourier, tome 46, n° 4 (1996), p. 951-969

<http://www.numdam.org/item?id=AIF_1996__46_4_951_0>

Ann. Inst. Fourier, Grenoble
46, 4 (1996), 951-969

CORPS QUADRATIQUES, $GL_2(\mathbf{Z})$ ET POLYNÔMES DE DICKSON

par Michel KERVAIRE

Soit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ un élément de $GL_2(\mathbf{Z})$ de trace $\tau = a + d$ et déterminant $\delta = ad - bc = \pm 1$. Les valeurs propres $\lambda, \lambda' = \dfrac{\tau \pm \sqrt{\tau^2 - 4\delta}}{2}$ de γ sont des unités de l'anneau $\mathcal{O}$ des entiers algébriques du corps $K = \mathbf{Q}(\sqrt{\tau^2 - 4\delta})$. Une question naturelle, portée à mon attention par Pierre de la Harpe, est de localiser λ, λ' dans le groupe des unités $\mathcal{O}^*$ de $\mathcal{O}$. Une réponse peut s'exprimer en termes des polynômes de Dickson de première espèce.

Une question voisine est celle de donner un critère pour décider si une matrice $\alpha \in GL_2(\mathbf{Z})$ est une puissance $\alpha = \beta^n$ avec $\beta \in GL_2(\mathbf{Z})$ et $n > 1$. Un tel critère, faisant intervenir les polynômes de Dickson de première et deuxième espèce, est fourni par la proposition 4.

Les énoncés de cette note sont très élémentaires et je me suis efforcé d'en donner une exposition aussi simple que possible. Les polynômes de Dickson sont une variante (avec paramètre) des polynômes de Tchebycheff qui apparaissent classiquement dans l'arithmétique des corps quadratiques réels. J'espère avoir mis en évidence le rôle du paramètre dans ces questions.

La rédaction a été très améliorée grâce aux suggestions de S. Eliahou et celles de T. Vust à qui je dois en particulier une meilleure version de la preuve de la formule (4).

Le cas intéressant est celui où $K = \mathbf{Q}(\sqrt{\tau^2 - 4\delta})$ est un corps quadratique réel ce qui équivaut à dire que $\tau^2 - 4\delta$ est positif et non-carré.

Pendant la préparation de cet article l'auteur était titulaire d'un contrat de recherche avec le Fonds National Suisse de la Recherche Scientifique.
Mots-clés : Corps quadratiques – Unités – Polynômes de Dickson.
Classification math. : 11R11 – 11R27.

Lorsque K est quadratique imaginaire, ou si $K = \mathbf{Q}$, les valeurs propres λ, λ' sont des racines de l'unité facilement identifiables. De plus, pour le premier problème du moins, on ne perd rien en supposant $\tau > 0$, quitte à changer les signes des valeurs propres.

On notera $\mathbf{N}$ l'ensemble des entiers positifs et il sera pratique de désigner par $\mathbf{P} \subset \mathbf{N} \times \{\pm 1\}$ l'ensemble des paires $(\tau, \delta) \in \mathbf{N} \times \{\pm 1\}$ telles que $\tau^2 - 4\delta$ est positif et non-carré, *i.e.*

$$\mathbf{P} = \{(\tau, \delta) \in \mathbf{N} \times \{\pm 1\} \mid \tau \geqslant 1 \text{ si } \delta = -1 \text{ et } \tau \geqslant 3 \text{ si } \delta = +1\}.$$

Les données τ, δ déterminent une décomposition

$$\tau^2 - 4\delta = f^2 D, \tag{1}$$

où f est entier (positif) et où D est un *discriminant fondamental*, *i.e.* ou bien $D = 4d$ avec d sans facteur carré et $d \equiv 2$ ou $3 \bmod 4$, ou bien $D = d$ sans facteur carré avec $d \equiv 1 \bmod 4$. Il est immédiat de vérifier que cette décomposition existe toujours et détermine univoquement f et D.

L'anneau $\mathcal{O}$ des entiers de $K = \mathbf{Q}(\sqrt{d})$, où $d \neq 1$ est sans facteur carré, admet pour $\mathbf{Z}$-base $\{1, \omega\}$ avec $\omega = \sqrt{d}$ si $d \equiv 2$ ou $3 \bmod 4$ et $\omega = \dfrac{1+\sqrt{d}}{2}$ si $d \equiv 1 \bmod 4$. Pour $d > 0$ on supposera $K \subset \mathbf{R}$ avec $\sqrt{d} > 0$. En particulier, pour $(\tau, \delta) \in \mathbf{P}$, on a $\lambda = \dfrac{\tau + \sqrt{\tau^2 - 4\delta}}{2}$ réel et $\lambda > 1$.

Le groupe $\mathcal{O}^*$ des éléments inversibles de $\mathcal{O}$ est produit direct de $\{\pm 1\}$ par un groupe infini cyclique. Si f est un entier positif, les éléments inversibles de $\mathcal{O}_f = \mathbf{Z} + \mathbf{Z} f\omega$ forment un sous-groupe $\mathcal{O}_f^*$ d'indice fini dans $\mathcal{O}^* = \mathcal{O}_1^*$. On notera ε_f l'unité fondamentale de $\mathcal{O}_f$. Par convention, ε_f est caractérisée, parmi les éléments de $\mathcal{O}_f^*$ dont la classe modulo $\{\pm 1\}$ engendre $\mathcal{O}_f^*/\{\pm 1\}$, par la condition $\varepsilon_f > 1$. On écrit ε pour ε_1. La plus petite puissance positive entière de ε qui appartient à $\mathcal{O}_f^*$ est l'unité fondamentale ε_f de $\mathcal{O}_f$.

PROPOSITION 1. — *Avec les notations introduites ci-dessus, supposons* $(\tau, \delta) \in \mathbf{P}$. *Alors, on a*

$$\lambda = \frac{\tau + \sqrt{\tau^2 - 4\delta}}{2} = \varepsilon_f,$$

sauf si $\tau = 3$, $\delta = +1$, *et dans ce cas* $\lambda = \varepsilon_f^2$.

Preuve. — On constate d'abord que $\lambda \in \mathcal{O}_f$. En effet, avec les notations de la décomposition (1), si $D \equiv 0 \bmod 4$, alors $\lambda = \frac{\tau}{2} + f\omega$, mais dans ce cas τ doit être pair. Si $D \equiv 1 \bmod 4$, alors $\lambda = \frac{\tau - f}{2} + f\omega$, et dans ce cas $\tau \equiv f \bmod 2$. On a donc bien $\lambda \in \mathbf{Z} + \mathbf{Z}f\omega = \mathcal{O}_f$.

De plus, dans les deux cas, le coefficient de $f\omega$ dans l'expression de $\lambda \in \mathbf{Z} + \mathbf{Z}f\omega$ est exactement 1.

Ceci est suffisant pour garantir $\lambda = \varepsilon_f$ avec l'exception citée. Rappelons brièvement cet argument classique et facile. (Cf. [BS], p. 133.)

Soit $\alpha \to \alpha'$ la conjugaison dans K (*i.e.* le générateur du groupe de Galois $\mathrm{Gal}(K/\mathbf{Q}) = C_2$).

Soit $\varepsilon_f = p + qf\omega \in \mathcal{O}_f^*$ l'unité fondamentale de $\mathcal{O}_f$. D'abord, $\varepsilon_f > 1$ entraîne que p et q sont tous les deux des entiers strictement positifs, sauf précisément dans le cas où $f = 1$ et $\omega = \frac{1+\sqrt{5}}{2}$ pour lequel $p = 0, q = 1$.

En effet, soit $\varepsilon'_f = \pm\varepsilon_f^{-1}$ le conjugué de ε_f. Comme $\varepsilon_f > 1$, on a $|\varepsilon'_f| < 1$. Donc, $\varepsilon_f - \varepsilon'_f = qf(\omega - \omega') > 0$. Or $\omega - \omega' > 0$ et par suite $q > 0$. De plus, $-f\omega' = f\sqrt{d}$, ou $-f\omega' = f\frac{\sqrt{d}-1}{2}$, selon que $d \equiv 2$ ou $3 \bmod 4$, ou que $d \equiv 1 \bmod 4$. On a donc $-f\omega' > 1$ excepté si $f = 1$ et $\omega = \frac{1+\sqrt{5}}{2}$. Il s'ensuit que $p = -qf\omega' + \varepsilon'_f > q - |\varepsilon'_f| > 0$.

Lorsque l'on forme les puissances positives successives de ε_f, *i.e.* $\varepsilon_f^n = p_n + q_n f\omega$, le coefficient q_n est une fonction strictement croissante de n. Une égalité de la forme $\lambda = u + f\omega = \varepsilon_f^n$ avec n positif (et $u \in \mathbf{Z}$) n'est donc possible que si $n = 1$ et alors $\lambda = \varepsilon_f$.

Si $\tau = 3$, $\delta = 1$, on a $f = 1$, $d = 5$, donc $\varepsilon_f = \varepsilon = \frac{1+\sqrt{5}}{2}$ et $\lambda = \varepsilon_f^2$. □

Revenons au problème original de localiser λ dans le groupe des unités $\mathcal{O}^*$ de $\mathbf{Q}(\lambda)$. Il reste à comparer λ (ou ε_f) avec ε. On a $\lambda = \varepsilon^m$ pour un certain entier positif m.

Si $f = 1$ dans la décomposition (1), *i.e.* si $\tau^2 - 4\delta = D$ est un discriminant fondamental, alors $\mathcal{O}_f = \mathcal{O}$ et, en supposant que $\tau \geqslant 4$ si $\delta = +1$, il résulte de la proposition 1 que $\lambda = \varepsilon_f = \varepsilon$ est l'unité fondamentale de l'anneau des entiers de $\mathbf{Q}(\sqrt{\tau^2 - 4\delta})$. On a aussi en particulier $N(\varepsilon) = \delta$.

Cependant, l'égalité $\varepsilon_f = \varepsilon$ peut avoir lieu même lorsque $f > 1$. Par exemple, avec $\tau = 10$ et $\delta = +1$, on a $f = 2$, $D = 24$. Dans ce cas, on voit que $\lambda = \varepsilon_f = \varepsilon = 5 + 2\omega$.

L'entier positif m tel que $\lambda = \varepsilon^m$ est le maximum des entiers positifs n tels que $\lambda \in K^n$, c'est-à-dire tels qu'il existe $\mu \in K$ satisfaisant $\lambda = \mu^n$. En effet, si $\lambda = \mu^n$, l'élément $\mu \in K$ est nécessairement lui-même une unité, et on peut supposer $\mu > 1$.

1. Puissances dans un corps quadratique.

Si on se donne un élément α dans un corps K quadratique sur $\mathbf{Q}$, un critère pour décider si $\alpha \in K^n$ peut s'exprimer à l'aide des polynômes de Dickson.

Rappelons que les polynômes de Dickson $D_n(x, a)$ de première espèce à une variable x et un paramètre a sont définis récursivement par

$$D_0(x, a) = 2\ , \quad D_1(x, a) = x\ , \quad \text{et}$$

$$D_{n+1}(x, a) \ = \ xD_n(x, a) \ - \ aD_{n-1}(x, a).$$

On a également une formule explicite

$$D_n(x, a) = x^n + \sum_{i=1}^{[\frac{n}{2}]} (-1)^i \frac{n}{n-i} \binom{n-i}{i} a^i x^{n-2i},$$

avec des coefficients $\dfrac{n}{n-i}\binom{n-i}{i}$ entiers. (Voir [LMT].)

On a le critère suivant.

PROPOSITION 2. — *Soient K un corps quadratique sur $\mathbf{Q}$ et $\alpha \in K$, $\alpha \notin \mathbf{Q}$, un élément de trace $\tau = \mathrm{Tr}(\alpha)$ et norme $\delta = \mathrm{N}(\alpha)$. Soit n un entier positif.*

Il existe $\beta \in K$ tel que $\alpha = \beta^n$ si et seulement si il existe des nombres rationnels σ et ν tels que

$$\tau = D_n(\sigma, \nu) \text{ et } \delta = \nu^n.$$

Preuve. — Les polynômes de Dickson satisfont la formule

$$D_n\left(z + \frac{a}{z}, a\right) = z^n + \left(\frac{a}{z}\right)^n \tag{2}$$

qui se démontre aisément par récurrence sur n.

S'il existe $\beta \in K$ avec $\alpha = \beta^n$, soient $\sigma = \mathrm{Tr}(\beta) = \beta + \beta'$ et $\nu = \mathrm{N}(\beta) = \beta\beta'$ la trace et la norme de β respectivement. On a $\delta = \mathrm{N}(\alpha) = \nu^n$ et

$$\tau = \mathrm{Tr}(\alpha) = \alpha + \alpha' = \beta^n + \beta'^n = \beta^n + \left(\frac{\nu}{\beta}\right)^n = D_n(\sigma, \nu).$$

Réciproquement, supposons $\tau = D_n(\sigma, \nu)$ avec σ, ν rationnels et $\delta = \nu^n$. Soient β et $\beta' = \dfrac{\nu}{\beta} \in \mathbf{C}$ les racines du polynôme $X^2 - \sigma X + \nu$.

Comme $\beta^n + \beta'^n = \beta^n + \left(\dfrac{\nu}{\beta}\right)^n = D_n\left(\beta + \dfrac{\nu}{\beta}, \nu\right) = \tau$ et $\beta^n \beta'^n = \nu^n = \delta$ par hypothèse, on voit que $\{\alpha, \alpha'\}$ et $\{\beta^n, \beta'^n\}$ sont tous les deux le couple des racines du même polynôme $X^2 - \tau X + \delta$.

On en conclut que $\alpha = \beta^n$, quitte à intervertir β et β' si nécessaire. En outre, $\mathbf{Q}(\alpha) \subset \mathbf{Q}(\beta)$, et comme $\alpha \notin \mathbf{Q}$, on a $[\mathbf{Q}(\beta) : \mathbf{Q}] \leqslant 2 = [\mathbf{Q}(\alpha) : \mathbf{Q}]$, et il s'ensuit $K = \mathbf{Q}(\alpha) = \mathbf{Q}(\beta)$ et donc $\beta \in K$. □

Si α est une unité et si $\alpha = \beta^n$, alors $\sigma = \mathrm{Tr}(\beta)$ et $\nu = \mathrm{N}(\beta)$ doivent être des entiers rationnels (car β est alors également une unité). On doit avoir en outre $\nu = \pm 1$ et la recherche de solutions en n, σ, ν de l'équation $\mathrm{Tr}(\alpha) = D_n(\sigma, \nu)$ avec $\mathrm{N}(\alpha) = \nu^n$ est limitée à un nombre fini contrôlable de cas.

Plus précisément, d'une part les zéros du polynôme $D_n(x, 1)$ et de sa dérivée sont tous réels et contenus dans l'intervalle $[-2, +2]$. Bien entendu $D_n(x, -1)$ est positif et strictement croissant pour $x \geqslant 1$. Les polynômes $D_n(x, \nu)$ sont donc strictement croissants (en x) pour $x \geqslant 3$ si $\nu = +1$ et $x \geqslant 1$ si $\nu = -1$. Si $(\tau, \delta) \in \mathbf{N} \times \{\pm 1\}$ est une paire d'entiers tels que $\tau^2 - 4\delta$ est positif et non-carré, c'est-à-dire $(\tau, \delta) \in \mathbf{P}$, on observe que les égalités $\tau = D_n(\sigma, \nu)$, $\delta = \nu^n$, où $(\sigma, \nu) \in \mathbf{N} \times \{\pm 1\}$ ne sont possibles qu'avec $(\sigma, \nu) \in \mathbf{P}$ car $D_n(1, 1) \leqslant 2$ et $D_n(2, 1) = 2$. D'autre part les valeurs minimales $D_n(3, 1)$ et $D_n(1, -1)$ sont elles-mêmes strictement croissantes en n. Il est donc suffisant de chercher les premières valeurs de n, soient n_0, n_1 pour lesquelles $D_{n_0}(3, 1)$ et $D_{n_1}(1, -1)$ dépassent τ. Ensuite, pour chaque n dans l'intervalle $0 < n < n_i$, $i = 0$ ou 1, on a un intervalle fini de valeurs de x qui entrent en question pour satisfaire l'une ou l'autre des équations $\tau = D_n(x, \pm 1)$.

Pour $(\tau, \delta) \in \mathbf{P}$, soit $m(\tau, \delta)$ le plus grand entier positif n pour lequel il existe $(\sigma, \nu) \in \mathbf{P}$ tels que $\tau = D_n(\sigma, \nu)$ et $\delta = \nu^n$.

En formule,

$$m(\tau, \delta) = \max \{n \mid \exists\ (\sigma, \nu) \in \mathbf{P} \text{ tels que } \tau = D_n(\sigma, \nu) \text{ et } \delta = \nu^n\}.$$

Il résulte de la description sommaire ci-dessus du comportement des polynômes $D_n(x, \pm 1)$ et de l'identité $D_1(x, a) = x$ que $m(\tau, \delta)$ est bien défini pour tout $(\tau, \delta) \in \mathbf{P}$.

Bien entendu, $m(\tau, \delta)$ dépend réellement de δ et la condition $\delta = \nu^n$ dans la définition de $m(\tau, \delta)$ est indispensable. Par exemple, $m(11, 1) = 2$ car $D_2(3, -1) = 11$. Mais on a aussi $11 = D_5(1, -1)$ et $m(11, -1) = 5$.

La proposition 2 a pour corollaire l'énoncé suivant.

PROPOSITION 3. — *Soient τ un entier positif et $\delta = \pm 1$ tels que $\tau^2 - 4\delta$ soit positif et non-carré. Soient $\lambda = \dfrac{\tau + \sqrt{\tau^2 - 4\delta}}{2}$ et ε l'unité fondamentale du corps $K = \mathbf{Q}(\sqrt{\tau^2 - 4\delta})$. On a la formule*

$$\lambda = \varepsilon^{m(\tau, \delta)}.$$

En effet, si $\lambda = \varepsilon^m$, on a $\tau = \mathrm{Tr}(\lambda) = D_m(\sigma, \nu)$ et $\delta = \nu^m$ avec $\sigma = \mathrm{Tr}(\varepsilon)$ et $\nu = \mathrm{N}(\varepsilon)$ par la proposition 2. Donc, $m \leqslant m(\tau, \delta)$. Réciproquement, toujours par la proposition 2, λ est puissance $m(\tau, \delta)$-ième d'un élément μ de K. On peut supposer $\mu > 1$, et μ est alors lui-même une puissance positive de ε, et donc m est un multiple de $m(\tau, \delta)$. Donc, $m = m(\tau, \delta)$.

Noter que dans la formulation donnée, le cas $\tau = 3, \delta = 1$ n'est pas exceptionnel. En effet, on a $m(3, 1) = 2$, car $D_2(1, -1) = 3$.

Remarque. — Le maximum dans la définition de $m(\tau, \delta)$ est aussi un plus petit commun multiple. Ceci résulte immédiatement de la proposition 2 et pourrait également être obtenu directement à partir de l'identité

$$D_p(D_q(x, a), a^q) = D_{pq}(x, a)$$

qu'il est facile de démontrer en utilisant la formule (2).

Pour vérifier qu'une unité dans $\mathcal{O}^*$ de trace τ et norme δ est l'unité fondamentale, c'est-à-dire qu'il n'existe pas d'entier $n > 1$ et de couple $(x, a) \in \mathbf{P}$ tels que $\tau = D_n(x, a)$ et $\delta = a^n$, il suffit de faire cette vérification pour n premier. Pour $\delta = -1$ on peut même se borner à ne considérer que les polynômes $D_\ell(x, -1)$ avec ℓ premier impair. Pour $\delta = +1$ il faut prendre en compte $D_2(x, -1)$, $D_2(x, 1)$ et $D_\ell(x, 1)$ pour ℓ premier impair.

Il est facile et rapide d'engendrer la liste des valeurs à éviter pour τ si l'on veut vérifier qu'une unité de trace τ est l'unité fondamentale. Ces valeurs deviennent d'ailleurs vite assez espacées. Cette méthode sera illustrée au paragraphe 3.

2. Puissances dans $\mathrm{GL}_2(\mathbf{Z})$.

Soit $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{Z})$. Un critère pour que α soit une puissance n-ième dans $GL_2(\mathbf{Z})$ peut s'exprimer en faisant intervenir une condition de divisibilité des coefficients $a-d, b, c$.

Il n'est pas indispensable mais il est commode d'introduire la correspondance $\varphi : GL_2(\mathbf{Z})_{\tau,\delta} \to \mathcal{F}_\Delta$ entre l'ensemble $GL_2(\mathbf{Z})_{\tau,\delta}$ des matrices de $GL_2(\mathbf{Z})$ ayant trace τ et déterminant δ d'une part et l'ensemble $\mathcal{F}_\Delta$ des formes quadratiques binaires $F(X,Y) = AX^2+BXY+CY^2$ (à coefficients entiers) de discriminant $\Delta = B^2 - 4AC = \tau^2 - 4\delta$ d'autre part.

La flèche φ associe à $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{Z})$ la forme $F = \varphi(\alpha)$ donnée par $F(X,Y) = cX^2 - (a-d)XY - bY^2$.

On note que le discriminant de F est bien

$$(a-d)^2 + 4bc \;=\; (a+d)^2 - 4(ad-bc) \;=\; \tau^2 - 4\delta.$$

Pour τ et δ fixés (ce qui fixe Δ), la correspondance φ est une bijection.

En effet, si F est une forme, $F(X,Y) = AX^2 + BXY + CY^2$, avec discriminant $B^2 - 4AC = \Delta = \tau^2 - 4\delta$, la matrice $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{Z})_{\tau,\delta}$ telle que $\varphi(\alpha) = F$ est donnée par

$$a = \frac{\tau - B}{2}\ ,\ \ b = -C\ ,\ \ c = A\ ,\ \ d = \frac{\tau + B}{2},$$

avec a, d entiers car $B^2 - 4AC = \tau^2 - 4\delta$ implique $B \equiv \tau \bmod 2$.

Il est évident que $\mathrm{trace}(\alpha) = \tau$. D'autre part,

$$\det(\alpha) = ad - bc = \frac{\tau^2 - B^2}{4} + AC = \frac{4\delta - 4AC}{4} + AC = \delta.$$

Pour la proposition 4 ci-dessous nous aurons besoin des polynômes de Dickson de *deuxième* espèce $E_n(x,a)$ à une variable x et paramètre a qui sont définis inductivement par les formules

$$E_0(x,a) = 1\ ,\ \ E_1(x,a) = x\ ,\ \text{ et}$$

$$E_{n+1}(x,a) \;=\; xE_n(x,a) \;-\; aE_{n-1}(x,a).$$

On a ainsi

$$E_2(x,a) = x^2 - a,\ E_3(x,a) = x^3 - 2ax,\ E_4(x,a) = x^4 - 3ax^2 + a^2,$$

et en général

$$E_n(x,a) = x^n + \sum_{i=1}^{\left[\frac{n}{2}\right]} (-1)^i \binom{n-i}{i} a^i x^{n-2i},$$

ce qui se démontre aisément à l'aide de la formule de récurrence ci-dessus.

En analogie avec la formule (2) ces polynômes satisfont l'identité

$$E_{n-1}\left(z + \frac{a}{z}, a\right) = \frac{z^n - \left(\frac{a}{z}\right)^n}{z - \frac{a}{z}},$$

comme on peut voir par récurrence sur n.

Les polynômes $E_n(x,a)$ interviennent dans le problème de caractériser les puissances dans $GL_2(\mathbf{Z})$ via la formule

$$\varphi(\beta^n) = E_{n-1}(\sigma,\nu)\cdot\varphi(\beta) \tag{4}$$

où $\beta \in \mathrm{GL}_2(\mathbf{Z})$, $\sigma = \mathrm{trace}(\beta)$, $\nu = \mathrm{dét}(\beta)$.

Preuve de (4). — On va d'abord démontrer

$$\beta^n = E_{n-1}(\sigma,\nu)\cdot\beta - E_{n-2}(\sigma,\nu)\cdot\nu \tag{5}$$

pour $n \geqslant 2$ par récurrence sur n. Cette formule remonte essentiellement à [R] et [T], où elle est exprimée en termes de polynômes de Tchebycheff.

Pour $n = 2$, on a bien

$$\beta^2 = \sigma\beta - \nu = E_1(\sigma,\nu)\cdot\beta - E_0(\sigma,\nu)\cdot\nu$$

par calcul direct, un cas particulièrement simple du théorème de Hamilton-Cayley. Ensuite, si $\beta^n = E_{n-1}(\sigma,\nu)\cdot\beta - E_{n-2}(\sigma,\nu)\cdot\nu$, on a

$$\begin{aligned}\beta^{n+1} &= E_{n-1}(\sigma,\nu)\cdot(\sigma\beta - \nu) - E_{n-2}(\sigma,\nu)\cdot\nu\beta \\ &= \{\sigma E_{n-1}(\sigma,\nu) - \nu E_{n-2}(\sigma,\nu)\}\cdot\beta - E_{n-1}(\sigma,\nu)\cdot\nu \\ &= E_n(\sigma,\nu)\cdot\beta - E_{n-1}(\sigma,\nu)\cdot\nu,\end{aligned}$$

par la formule de récurrence définissant les polynômes $E_n(x,a)$.

On applique maintenant φ en observant que φ est linéaire et associe la forme identiquement nulle à une matrice scalaire. Il vient

$$\varphi(\beta^n) = \varphi(E_{n-1}(\sigma,\nu)\cdot\beta) = E_{n-1}(\sigma,\nu)\cdot\varphi(\beta),$$

comme voulu. □

Soient τ et δ la trace et le déterminant de $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{Z})$.

PROPOSITION 4. — *Avec les notations ci-dessus, la matrice α est une puissance n-ième d'une matrice de $GL_2(\mathbf{Z})$ si et seulement si il existe un entier σ et un choix de $\nu = \pm 1$ tels que l'on ait simultanément*

(i) *$E_{n-1}(\sigma,\nu)$ divise les coefficients $c, -(a-d), -b$ de la forme $\varphi(\alpha)$, et*

(ii) *$\tau = D_n(\sigma,\nu)$ et $\delta = \nu^n$.*

Preuve. — Si $\alpha = \beta^n$ avec $\beta \in GL_2(\mathbf{Z})$, on pose $\sigma = \text{trace}(\beta)$, $\nu = \text{dét}(\beta)$ et la formule (4) montre que la forme $\varphi(\alpha)$ est divisible par $E_{n-1}(\sigma,\nu)$.

Si $\mu, \mu' = \dfrac{\nu}{\mu}$ sont les valeurs propres de β, alors $\lambda = \mu^n$, $\lambda' = \mu'^n$ sont celles de α et on a $\tau = \mu^n + \mu'^n = \mu^n + \left(\dfrac{\nu}{\mu}\right)^n = D_n\left(\mu + \dfrac{\nu}{\mu}, \nu\right) = D_n(\sigma,\nu)$, et $\delta = \lambda\lambda' = (\mu\mu')^n = \nu^n$.

Réciproquement, supposons que $\varphi(\alpha) = [c, -(a-d), -b]$ soit divisible par $E_{n-1}(\sigma,\nu)$ avec σ entier et $\nu = \pm 1$. Posons $E = E_{n-1}(\sigma,\nu)$ pour simplifier l'écriture et

$$r = \frac{1}{2}\left(\sigma + \frac{a-d}{E}\right),\ s = \frac{b}{E},\ t = \frac{c}{E},\ u = \frac{1}{2}\left(\sigma - \frac{a-d}{E}\right).$$

On va voir que si l'on pose $\beta = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$, on a $\alpha = \beta^n$. Soient $\mu, \mu' = \dfrac{\nu}{\mu}$ les racines du polynôme $X^2 - \sigma X + \nu$. On a

$$\tau = D_n(\sigma,\nu) = D_n\left(\mu + \frac{\nu}{\mu}, \nu\right) = \mu^n + \left(\frac{\nu}{\mu}\right)^n,$$

et

$$\tau^2 - 4\delta = \left(\mu^n + \left(\frac{\nu}{\mu}\right)^n\right)^2 - 4\delta = \left(\mu^n - \left(\frac{\nu}{\mu}\right)^n\right)^2 = E^2\cdot(\sigma^2 - 4\nu),$$

avec $E = E_{n-1}(\sigma, \nu)$ et en utilisant la formule (3).

On a donc

$$ru - st = \frac{1}{4}(\sigma^2 - \frac{(a-d)^2}{E^2}) - \frac{bc}{E^2} = \frac{1}{4}(\sigma^2 - \frac{\tau^2 - 4\delta - 4bc}{E^2}) - \frac{bc}{E^2}$$
$$= \frac{1}{4}(\sigma^2 - (\sigma^2 - 4\nu)) = \nu.$$

Ceci montre d'une part que r et u sont entiers (sinon ru conserverait le dénominateur 4, puisque $r+u \in \mathbf{Z}$). D'autre part, la matrice $\beta = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ a pour déterminant $\nu = \pm 1$ et appartient donc à $GL_2(\mathbf{Z})$.

En outre, on a

$$\varphi(\beta^n) = E_{n-1}(\sigma, \nu)\varphi(\beta) = [c, -(a-d), -b] = \varphi(\alpha).$$

Pour en conclure $\alpha = \beta^n$ il suffit de savoir que α et β^n ont même trace et même déterminant. C'est précisément le contenu des conditions $\tau = D_n(\sigma, \nu)$ et $\delta = \nu^n$. □

Remarques. — La condition (ii) est équivalente à demander que les valeurs propres λ, λ' de α soient des puissances n-ièmes dans $\mathbf{Q}(\lambda)$.

La seule condition (i) est bien entendu insuffisante pour conclure que α est une puissance n-ième dans $GL_2(\mathbf{Z})$. Même la condition

$$\text{(ii}\prime\text{)} \qquad \tau^2 - 4\delta = E_{n-1}^2(\sigma, \nu) \cdot (\sigma^2 - 4\nu)$$

jumelée avec (i) ne serait pas suffisante pour remplacer (ii) dans l'argument ci-dessus et entraîner $\alpha = \beta^n$. Par exemple, la matrice $\alpha = \begin{pmatrix} -5 & 3 \\ 3 & -2 \end{pmatrix}$ n'est pas un carré bien que $\varphi(\alpha) = [3, 3, -3]$ ait ses coefficients divisibles par $E_1(3,1) = 3$ et que, avec $n = 2$, $\sigma = 3$, $\nu = 1$, la condition (ii′) soit satisfaite.

Cependant, si n est impair, alors quitte à interchanger r et u avec changement de signe, on ne modifie pas $\varphi(\beta)$ et on change le signe de trace(β^n). Dans ce cas la condition (ii′) (plus faible que la condition (ii)) est donc suffisante pour garantir que α est une puissance n-ième dans $GL_2(\mathbf{Z})$.

Signalons enfin que la correspondance $\varphi : GL_2(\mathbf{Z})_{\tau,\delta} \to \mathcal{F}_\Delta$ satisfait la formule

$$\varphi(\xi^{-1}\gamma\xi) = \frac{1}{\det(\xi)}\, \varphi(\gamma)^\xi \tag{6}$$

pour tout $\gamma = GL_2(\mathbf{Z})_{\tau,\delta}$ et tout $\xi \in GL_2(\mathbf{Z})$, et où l'action (à droite) de $\xi = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathbf{Z})$ sur une forme F est donnée par $F^{\xi} = F'$ avec

$$F'(X,Y) = F(rX + sY, tX + uY).$$

La formule (6) se vérifie sans difficulté par calcul direct.

Ainsi les classes de conjugaison par $SL_2(\mathbf{Z})$ correspondent par φ aux classes d'équivalence propre des formes quadratiques binaires.

3. L'indice $[\mathcal{O}^* : \mathcal{O}_f^*]$.

Soient toujours K un corps quadratique réel sur $\mathbf{Q}$, de discriminant D, et $\mathcal{O}$ l'anneau des entiers de K.

Pour un entier positif donné f, on peut étudier l'indice $I(f) = [\mathcal{O}^* : \mathcal{O}_f^*]$ en utilisant les polynômes de Dickson de deuxième espèce $E_n(x,a)$. Dans ce paragraphe nous nous proposons de caractériser les indices $I(p)$ possibles, du moins lorsque p est un nombre premier impair.

Soit $\varepsilon = u + v\omega$ l'unité fondamentale de K. On notera $\sigma = \varepsilon + \varepsilon'$ la trace et $\nu = \varepsilon \cdot \varepsilon'$ la norme de ε. On a la formule

$$\varepsilon^n = E_{n-1}(\sigma,\nu)\varepsilon - E_{n-2}(\sigma,\nu)\nu, \tag{7}$$

analogue de (5) et qui se démontre de manière similaire, par récurrence en partant de $\varepsilon^2 = \sigma\varepsilon - \nu$.

La formule (7) *montre que* $I(f) = [\mathcal{O}^* : \mathcal{O}_f^*]$ *est le plus petit entier positif* n *pour lequel* $v \cdot E_{n-1}(\sigma,\nu)$, *le coefficient de* ω *dans* ε^n, *est divisible par* f.

Pour déterminer $I(f)$, il est suffisant d'étudier $I(p^r)$ avec p premier. En effet, si f_1 et f_2 sont premiers entre eux, on a $\mathcal{O}_{f_1 f_2}^* = \mathcal{O}_{f_1}^* \cap \mathcal{O}_{f_2}^*$. Par suite,

$$I(f_1 f_2) = \text{ppcm}\,\{I(f_1), I(f_2)\}\,, \text{ si pgcd}\,(f_1, f_2) = 1.$$

On va s'occuper d'abord de $I(p)$.

Bien entendu, $I(p) = 1$ si et seulement si p divise v.

Si p ne divise pas v, il y a deux cas selon que p divise ou non le discriminant D de K. On note que $\sigma^2 - 4\nu = (\varepsilon - \varepsilon')^2 = v^2(\omega - \omega')^2 = v^2 D$.

(1) *Cas ramifié.* Si p divise D, le polynôme $X^2 - \sigma X + \nu$ réduit modulo p a un discriminant nul et donc possède une racine double $a \in \mathbf{F}_p^*$. Soit $\wp$ l'idéal premier de $\mathcal{O}$ contenant p. (Rappelons que dans ce cas $p\mathcal{O} = \wp^2$.) Soit $\rho : \mathcal{O} \to \mathcal{O}/\wp = \mathbf{F}_p$ la réduction modulo $\wp$.

Avec ces notations, on a $\rho(\varepsilon) = \rho\left(\frac{\nu}{\varepsilon}\right) = a \in \mathbf{F}_p^*$ et

$$\rho(E_{p-1}(\sigma,\nu)) = \rho\left(\frac{\varepsilon^p - \left(\frac{\nu}{\varepsilon}\right)^p}{\varepsilon - \frac{\nu}{\varepsilon}}\right) = \rho\left(\sum_{i=1}^{p} \varepsilon^{p-i}\left(\frac{\nu}{\varepsilon}\right)^{i-1}\right)$$
$$= \sum_{i=1}^{p} a^{p-1} = p = 0 \in \mathbf{F}_p.$$

Donc, si p divise D, alors $I(p)$ divise p, et si $v \not\equiv 0 \bmod p$, on a $I(p) \neq 1$ et $I(p) = p$.

(2) *Cas non-ramifié.* Si p ne divise pas D, soit $\mathbf{F}_q$ le corps des racines sur $\mathbf{F}_p$ du polynôme $X^2 - \sigma X + \nu$. Soit $\alpha \in \mathbf{F}_q$ l'une de ces racines.

Dans ce cas, $vD \not\equiv 0 \bmod p$, l'indice $I(p)$ est déterminé par

$$I(p) = \text{Ordre de } \nu\alpha^2 \text{ dans } \mathbf{F}_q^*. \tag{8}$$

Par exemple, pour $p = 2$, ou bien le coefficient v est pair dans $\varepsilon = u + v\omega$ auquel cas $I(2) = 1$, ou bien v est impair et $I(2)$ doit être un diviseur > 1 de 3, autrement dit $I(2) = 3$. Ce cas particulier peut d'ailleurs facilement se vérifier par calcul direct des puissances successives ε, ε^2, ε^3.

Preuve de (8). — Soit $\wp$ un idéal premier de $\mathcal{O}$ divisant p. On a $\mathcal{O}/\wp = \mathbf{F}_q$. Les deux racines distinctes α, β de $X^2 - \sigma X + \nu \in \mathbf{F}_p[X]$ appartiennent au corps $\mathbf{F}_q$ et satisfont $\alpha\beta = \nu = \pm 1$.

On note encore ρ la réduction $\rho : \mathcal{O} \to \mathcal{O}/\wp$. On a

$$\rho(E_{m-1}(\sigma,\nu)) = \rho\left(\frac{\varepsilon^m - \left(\frac{\nu}{\varepsilon}\right)^m}{\varepsilon - \frac{\nu}{\varepsilon}}\right) = \frac{\alpha^m - \beta^m}{\alpha - \beta}.$$

Comme $\rho_{|\mathbf{Z}}$ se factorise par $\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z} \hookrightarrow \mathcal{O}/\wp$, on constate donc que $E_{m-1}(\sigma,\nu) \equiv 0 \bmod p$ si et seulement si $(\nu\alpha^2)^m = \left(\dfrac{\alpha}{\beta}\right)^m = 1$ dans $\mathbf{F}_q$. □

Pour le calcul de $I(p^r)$ avec $r > 1$, il faut distinguer les cas p premier impair et le cas $p = 2$.

Si p est premier impair, soit p^s la puissance exacte de p divisant le coefficient de ω dans $\varepsilon^{I(p)}$. On pose $\varepsilon^{I(p)} = u_1 + p^s v_1 \omega$ avec u_1 et v_1 premiers à p. On a $s \geqslant 1$ et on voit facilement par récurrence sur k que

$$\varepsilon^{p^k I(p)} \equiv u_1^{p^k} + p^{s+k} v_1 \omega \bmod p^{s+k+1}\mathcal{O} \text{ pour } k \geqslant 0.$$

Il en résulte que $I(p^r)$ est de la forme $p^k I(p)$. En effet, $\mathcal{O}^*/\mathcal{O}_p^*$ est un quotient de $\mathcal{O}^*/\mathcal{O}_{p^r}^*$ donc $I(p)$ divise $I(p^r)$ et plus précisément

$$I(p^r) = \begin{cases} I(p) & \text{si } 1 \leqslant r \leqslant s, \\ p^{r-s} I(p) & \text{si } s \leqslant r, \end{cases}$$

ou si l'on préfère, $I(p^r) = p^{\max\{0, r-s\}} I(p)$.

Pour un discriminant fixé, l'entier positif s ($= s_p$, fonction de p) est difficile à cerner.

Par exemple, pour $d = 5$, on a $\varepsilon^n = F_{n-1} + F_n\omega$, où $\{F_n\}$ est la suite de Fibonacci ($F_0 = 0, F_1 = 1, F_{n+1} = F_n + F_{n-1}$). Dans ce cas, p^s est la puissance exacte de p divisant le plus petit F_m positif divisible par p. On sait que $m = I(p)$ divise $p - 1$ pour $p \equiv \pm 1 \bmod 5$ et divise $p + 1$ pour $p \equiv \pm 2 \bmod 5$. Je dois à Shalom Eliahou de m'avoir signalé que le problème de déterminer s_p dans ce cas est un problème non-résolu bien connu. Dans [M], Peter Montgomery annonce que $s_p = 1$ pour $p < 2^{32}$. On ne connaît pas de valeur de p pour laquelle $s_p \geqslant 2$ (avec $d = 5$).

Pour d'autres valeurs de d, on constate que si s_p vaut souvent 1, on trouve plusieurs exemples dispersés avec $s_p \geqslant 2$, *e.g.* pour $d = 2$ déjà, on a $s_7 = 2$, $s_{31} = 2$, pour $d = 29$ on a $s_3 = 3$, $s_{11} = 2$.

Notons cependant que dans le cas ramifié, avec p premier $p \geqslant 5$, p divisant D et si $I(p) = p$, alors on a toujours $s_p = 1$. En effet, pour le voir, il suffit d'écrire $\varepsilon = \dfrac{a + b\sqrt{D}}{2}$ avec a et b entiers premiers à p et de calculer le coefficient de $\sqrt{D}$ dans $\varepsilon^p \bmod p^2$. On trouve $\varepsilon^p \equiv \dfrac{1}{2^p}(a^p + pa^{p-1}b\sqrt{D}) \bmod p^2$, dès que $\dfrac{p-1}{2} \geqslant 2$. Pour $p = 3$, p divisant D et $I(3) = 3$, on a

encore $s_3 = 1$ si $D \equiv 3 \bmod 9$, mais $s_3 \geqslant 2$ si $D \equiv 6 \bmod 9$, comme on le voit par calcul direct.

Par contre, si p divise D mais $I(p) = 1$, on peut avoir $s_p \geqslant 2$ même pour $p \geqslant 5$. Par exemple, pour $d = 295$, $I(5) = 1$ et $s_5 = 2$. (L'unité fondamentale pour $d = 295$ est $\varepsilon = 2024999 + 117900 \cdot \sqrt{295}$.)

Passons maintenant au cas $p = 2$. Soit 2^s la puissance exacte de 2 divisant le coefficient de ω dans $\varepsilon^{I(2)}$. On pose $\varepsilon^{I(2)} = u_0 + 2^s v_0 \omega$ avec u_0, v_0 impairs (et $s \geqslant 1$). Soit de plus 2^t la puissance exacte de 2 telle que $\varepsilon^{2I(2)} = u_1 + 2^t v_1 \omega$ avec u_1, v_1 impairs. On a $t \geqslant s+1 \geqslant 1$ donc $t \geqslant 2$ et par récurrence sur k,

$$\varepsilon^{2^{k+1}I(2)} \equiv u_1^{2^k} + 2^{t+k} v_1 \omega \bmod 2^{t+k+1}\mathcal{O} \text{ pour } k \geqslant 0.$$

Le résultat dans ce cas prend la forme

$$I(2^r) = \begin{cases} I(2) & \text{si } 1 \leqslant r \leqslant s, \\ 2I(2) & \text{si } s+1 \leqslant r \leqslant t, \\ 2^{r-t+1} I(2) & \text{si } t \leqslant r. \end{cases}$$

Dans ces dernières formules, si $s \geqslant 2$, alors $t = s+1$ et, comme pour le cas p impair, $I(2^r)$ peut s'écrire plus simplement $I(2^r) = 2^{\max\{0, r-s\}} I(2)$.

Il est donc intéressant de savoir séparer les cas où $s = 1$ et $s \geqslant 2$.

Pour $D = 4d$, on peut résumer quelques remarques faciles donnant une information partielle sur $s = s_2$ dans le tableau suivant :

I(2)	1		2	
$d \bmod 4$	2	3	2	3
s	?	$s \geqslant 2$	$s = 1$	$s \geqslant 2$
exemples	$s = 1$ pour $d = 6$ $s = 2$ pour $d = 14$	$s = 2$ pour $d = 39$ $s = 3$ pour $d = 147$ $s = 4$ pour $d = 579$	$d = 2$	$s = 2$ ssi $d \equiv 3$ (8) $s = 3$ pour $d = 15$ $s = 4$ pour $d = 7$

D'autre part, pour $D = 4d$, on a toujours $t = s+1$, comme le montre le calcul direct de $\varepsilon^{2I(2)} = (u_0^2 + 2^s v_0^2 d) + 2^{s+1} u_0 v_0 \omega$.

Pour $D = d \equiv 1 \bmod 4$, il est facile de voir que $s = 1$ si et seulement si $\mathrm{N}(\varepsilon) = -1$. De plus, si $\mathrm{N}(\varepsilon) = +1$, alors $s \geqslant 3$. En effet, si $\varepsilon = u + v\omega$ avec v pair, la formule $\mathrm{N}(\varepsilon) = u^2 + uv - \dfrac{d-1}{4} v^2 = \pm 1$ montre que v est divisible par 4 si et seulement si $\mathrm{N}(\varepsilon) = 1$. Si v est impair, on a $I(2) = 3$

et le coefficient de ω dans ε^3 est $v_3 = 3u^2v + 3uv^2 + v^3\left(\frac{d-1}{4}\right) + v^3$. La réduction modulo 4 et la formule pour la norme donnent $v_3 \equiv 1 - \mathrm{N}(\varepsilon) \bmod 4$. Donc, $s = 1$ si et seulement si $\mathrm{N}(\varepsilon) = -1$. En fait, si $\mathrm{N}(\varepsilon) = 1$ et v est pair, alors $v \equiv 0 \bmod 2^3$. Pour v impair, $\frac{d-1}{4}$ doit être impair et $v_3 = 3\mathrm{N}(\varepsilon)v + 4v^3\frac{d-1}{4} + v^3 \equiv 0 \bmod 2^3$. Pour $\mathrm{N}(\varepsilon) = +1$ on a donc $s \geqslant 3$.

Enfin, toujours avec $d \equiv 1 \bmod 4$, si $s = 1$ on a $t \geqslant 3$, car dans ce cas $\omega^2 = \frac{d-1}{4} + \omega$ et $\varepsilon^{2I(2)} = \left(u_0^2 + 2^2v_0^2\frac{d-1}{4}\right) + 2^2v_0(u_0 + v_0)\omega$, où $u_0 + v_0$ est pair. On constate en calculant $\varepsilon^6 = u_6 + v_6\omega$ que pour $I(2) = 3$ on a $t = 3$ exactement. Par contre pour $I(2) = 1$ on peut avoir $t > 3$. Par exemple, pour $d = 41$, on a $\varepsilon = 27 + 10\omega$ et $s = 1$, $t = 7$.

Revenons maintenant à l'étude de $I(p)$.

Caractérisation de l'indice $I(p) = [\mathcal{O}^* : \mathcal{O}_p^*]$ pour p premier impair.

Tout d'abord, pour p premier impair, on ne peut avoir $I(p) = 1$ ou $I(p) = p$ que si ν est un carré mod p.

En effet, $I(p) \in \{1, p\}$ est équivalent à demander que p divise vD pour l'unité fondamentale $\varepsilon = u + v\omega$. L'assertion résulte donc de la formule pour la norme, $4\mathrm{N}(\varepsilon) = \sigma^2 - v^2D = 4\nu$, où $\sigma = \mathrm{Tr}(\varepsilon)$.

Dans les cas non-ramifiés, si $q = p$ dans la formule (8), *i.e.* si $X^2 - \sigma X + \nu$ a deux racines distinctes α, β dans $\mathbf{F}_p$, alors $I(p)$ est évidemment un diviseur de $p - 1$. C'est même un diviseur de $\frac{p-1}{2}$ si ν est un carré modulo p, ce qui a lieu si $\nu = 1$, ou $\nu = -1$ et $p \equiv 1 \bmod 4$. Par contre, si ν est non-carré mod p, alors $\nu = -1$ et $I(p)$ est un diviseur pair de $p - 1$, et donc le quotient $\frac{p-1}{I(p)}$ est impair.

D'autre part, si $q = p^2$, *i.e.* si $X^2 - \sigma X + \nu$ est irréductible sur $\mathbf{F}_p$, on a $\beta = \alpha^p$ et on voit donc que l'ordre de $(\nu\alpha^2)^{-1} = \frac{\beta}{\alpha} = \alpha^{p-1}$ dans $\mathbf{F}_q^*$ est un diviseur de $p + 1$. Là encore, si ν est un carré dans $\mathbf{F}_p$, $\nu = e^2$ avec $e \in \mathbf{F}_p$, alors $e\alpha$ est de norme 1, donc il existe un élément $\xi \in \mathbf{F}_q$ tel que $e\alpha = \xi^{p-1}$. Dans ce cas, l'ordre de $\nu\alpha^2 = \xi^{2(p-1)}$ est un diviseur de $\frac{p+1}{2}$. Si ν est non-carré dans $\mathbf{F}_p$, le quotient $\frac{p+1}{I(p)}$ doit être impair. En effet, α^{p-1} d'ordre $I(p)$ est de la forme $\alpha^{p-1} = \gamma^{\frac{p^2-1}{I(p)}}$ pour un générateur γ de

$\mathbf{F}_q^*$. On a donc $\alpha = a\gamma^{\frac{p+1}{I(p)}}$ avec $a \in \mathbf{F}_p^*$. En prenant la norme, il vient $\nu = a^2 \mathrm{N}(\gamma)^{\frac{p+1}{I(p)}}$, et l'exposant $\dfrac{p+1}{I(p)}$ doit donc être impair si ν est non-carré.

Réciproquement, on va voir que pour p donné, les ordres compatibles avec les remarques qui précèdent sont tous réalisables pour un discriminant convenable.

Plus précisément, on a l'énoncé suivant.

PROPOSITION 5. — *Soit p un nombre premier impair. Soient I un entier positif et $\nu = \pm 1$ satisfaisant l'une des conditions suivantes :*

(1) *ν est un non-carré mod p et I est un diviseur pair de $p-1$ ou un diviseur de $p+1$ avec $\dfrac{p+1}{I}$ impair;*

(2) *ν est un carré mod p et I est un diviseur $\neq 1$ de $\dfrac{p-1}{2}$ ou de $\dfrac{p+1}{2}$;*

(3) *ν est un carré mod p et $I = 1$ ou $I = p$.*

Il existe alors un corps quadratique $K = \mathbf{Q}(\sqrt{D})$ pour lequel l'unité fondamentale a norme ν et $[\mathcal{O}^* : \mathcal{O}_p^*] = I$.

Dans la situation des conditions (1) et (2), il est facile de trouver $\rho \in \mathbf{F}_p$ tel que le quotient des racines du polynôme $X^2 - \rho X + \nu \in \mathbf{F}_p[X]$ ait l'ordre souhaité I dans $\mathbf{F}_q^*$, où $\mathbf{F}_q$ est le corps des racines du polynôme $X^2 - \rho X + \nu$.

Il suffit alors de trouver un entier positif $\sigma \equiv \rho \bmod p$, tel que la racine $\lambda = \dfrac{\sigma + \sqrt{\sigma^2 - 4\nu}}{2}$ du polynôme $X^2 - \sigma X + \nu$ soit l'unité fondamentale $\varepsilon = u + v\omega$ de $\mathbf{Q}(\sqrt{\sigma^2 - 4\nu})$. L'indice $I(p) = [\mathcal{O}^* : \mathcal{O}_p^*]$ pour le corps $\mathbf{Q}(\sqrt{D})$ de discriminant D, où $\sigma^2 - 4\nu = v^2 D$, aura alors, d'après (8), la valeur I prescrite.

D'après la proposition 2, pour vérifier que $\varepsilon = \dfrac{\sigma + \sqrt{\sigma^2 - 4\nu}}{2}$ est l'unité fondamentale de $\mathbf{Q}(\sqrt{\sigma^2 - 4\nu})$ il suffira de vérifier que σ n'est pas une valeur des polynômes de Dickson $D_n(x, a)$ avec $\nu = a^n$ et $n > 1$. D'après la remarque qui suit la proposition 3, il est même suffisant de faire cette vérification pour $n = 2$ et $n = \ell$ premier impair.

Trouver σ avec ces spécifications est facile pour $\rho \neq 0 \in \mathbf{F}_p$. Il est suffisant de choisir (par le théorème de Dirichlet) un nombre premier σ satisfaisant les congruences

$$\sigma \equiv \rho \bmod p,\ \sigma \equiv 1 \bmod 4, \text{ et } \sigma \equiv 2 \text{ ou } 3 \bmod 5.$$

(Pour $p = 5$, on procède par observation directe.)

En effet, $D_2(x, \pm 1) = x^2 \pm 2$ est soit pair, soit $D_2(x, \pm 1) \equiv -1 \bmod 4$. Donc $\sigma \neq D_2(x, \pm 1)$. De plus, pour ℓ impair, $D_\ell(x, \pm 1)$ est un polynôme impair, donc de la forme $xP(x^2)$ et ses valeurs ne peuvent être des nombres premiers impairs que si $x = 1$ et $\nu = -1$.

On constate cependant que $D_n(1, -1) \equiv \pm 1 \bmod 5$ pour n impair.

Si $\sigma \equiv 2$ ou $3 \bmod 5$, on a donc $\sigma \neq D_\ell(x, \pm 1)$ pour tout premier impair ℓ, et tout x, quel que soit le choix de $\nu = \pm 1$.

Pour $\rho = 0 \in \mathbf{F}_p$, ce qui signifie que $I = 2$, on cherche un entier σ de la forme $\sigma = pp_1$ qui ne soit pas une valeur de $D_n(x, \pm 1)$. On distingue les deux cas $\nu = 1$ et $\nu = -1$.

Pour $\nu = 1$ on prend $\sigma = p^2$. On a encore $\sigma \neq D_2(x, 1)$ car pour x impair, $D_2(x, \pm 1) \equiv -1 \bmod 4$ comme noté précédemment. Ensuite, pour ℓ impair, on ne pourrait avoir $p^2 = D_\ell(x, a)$, $a^\ell = 1$ que si $a = 1$. De plus, $D_\ell(x, 1)$ étant divisible par x, on devrait avoir $x = 1, p$ ou p^2. Comme $|D_\ell(1, 1)| \leqslant 2$ et $p^2 < D_\ell(p, 1)$, il n'y a pas de solution à $\sigma = p^2 = D_\ell(x, 1)$.

La question est plus délicate pour $\nu = -1$. Dans ce cas il est inutile de considérer $D_2(x, \pm 1)$. Si on impose $\sigma = pp_1$, avec p_1 premier satisfaisant les inégalités $p \leqslant p_1 < p^2$, on garantit σ différent de $D_\ell(p, -1)$, $D_\ell(p_1, -1)$, et de $D_\ell(pp_1, -1)$ car pour $\ell \geqslant 3$, on a $x^3 < D_\ell(x, -1)$.

Il est donc suffisant de trouver p_1 premier, tel que $p \leqslant p_1 < p^2$ et $pp_1 \neq D_\ell(1, -1)$ pour tout ℓ impair $\geqslant 3$.

Une manière de résoudre ce problème est de prendre $\sigma = p^2$ et d'utiliser le fait que la suite des nombres $L_n = D_n(1, -1)$, appelés habituellement nombres de Lucas, ne contient pas d'autres carrés que $L_1 = 1$ et $L_3 = 4$. (Voir [C].)

On peut aussi montrer l'existence de nombres premiers p_1 répondant à la question (dans l'intervalle $p < p_1 < p^2$ et tels que $\sigma = pp_1$ ne soit pas une valeur de $D_\ell(1, -1)$) en comparant le nombre de premiers dans l'intervalle $[p, p^2]$ avec le nombre de valeurs de $D_n(1, -1)$ entre p^2 et p^3.

Pour cela, soit $\pi(x)$ le nombre de premiers $\leqslant x$. Une forme particulièrement simple du théorème de Tchebycheff donne les estimations

$$\frac{\log 2}{4}\,\frac{x}{\log x} < \pi(x) < 6(\log 2)\,\frac{x}{\log x}$$

dont une démonstration très simple est donnée dans [F], p. 19.

Le nombre M de nombres premiers p_1 tels que $p < p_1 < p^2$ est donc minoré par

$$M > \frac{\log 2}{\log p}\left(\frac{p^2 - 48p}{8}\right).$$

D'autre part, pour $n \geqslant 5$, le nombre m de valeurs des $D_n(1,-1)$ que l'on peut intercaler entre p^2 et p^3 est majoré par

$$m < \frac{\log p}{\log c} \;+\; 1,$$

avec $c = 1{,}61 < 29/18$, car $D_{k+1}(1,-1) > c\,D_k(1,-1)$ pour $k \geqslant 5$ comme on voit facilement par récurrence.

Ces estimations montrent que $M > m$ dès que $p \geqslant 59$ et donc il existe un choix de p_1 premier dans l'intervalle $p < p_1 < p^2$ tel que pp_1 est différent de $D_\ell(1,-1)$ pour tout ℓ. Il suffit alors de traiter individuellement les cas où $p < 59$.

Pour

$$p = 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,\ 53,$$

on a $I(p) = 2$ pour les corps $\mathbf{Q}(\sqrt{d})$ avec, respectivement,

$$d = 13,\ 11,\ 34,\ 30,\ 42,\ 19,\ 31,\ 33,\ 71,\ 46,\ 38,\ 83,\ 74,\ 103,\ 59.$$

Ces valeurs sont les plus petites valeurs de d pour lesquelles $I(p) = 2$. On en trouve d'autres avec $\sigma = pp_1$ comme ci-dessus.

Enfin, dans la situation de la condition (3) de la proposition, on note que ν est un carré mod p^2. Si $I = 1$, on peut fabriquer une infinité de discriminants d pour lesquels $\mathcal{O}_p = \mathcal{O}$ en prenant pour σ un nombre premier satisfaisant $\sigma \equiv 2e \bmod p^2$, où $\nu \equiv e^2 \bmod p^2$, $\sigma \equiv 1 \bmod 4$, et $\sigma \equiv 2$ ou $3 \bmod 5$. (De nouveau ceci exige d'examiner séparément le cas $p = 5$. On a $I(5) = 1$ par exemple pour $d = 23$ et pour $d = 185$.) Avec v et le discriminant D donnés par $\sigma^2 - 4\nu = v^2 D$, on a alors $v \equiv 0 \bmod p$.

Si $I = p$, on prend σ premier satisfaisant $\sigma \equiv 2e + p \bmod p^2$, et encore $\sigma \equiv 1 \bmod 4$ et $\sigma \equiv 2$ ou $3 \bmod 5$. Avec $\sigma^2 - 4\nu = v^2 D$, on a nécessairement $v \not\equiv 0 \bmod p$ et p divise D.

Dans les deux cas, le nombre premier σ n'est valeur d'aucun polynôme de Dickson $D_2(x, \pm 1)$, ni $D_\ell(x, \pm 1)$ avec $(x, \pm 1) \in \mathbf{P}$ et donc $\dfrac{\sigma + \sqrt{\sigma^2 - 4\nu}}{2}$ est l'unité fondamentale de $\mathbf{Q}(\sqrt{D})$. Il en résulte que $I(p)$ prend la valeur prescrite.

BIBLIOGRAPHIE

[BS] Z. I. BOREVICH, I. R. SHAFAREVICH, Number Theory, Academic Press, 1966.

[C] J.H.E. COHN, Square Fibonacci numbers, etc., The Fibonacci Quarterly, 2 (1964), 109-113.

[F] D. FLATH, Introduction to Number Theory, John Wiley & Sons, 1989.

[LMT] R. LIDL, G.L. MULLEN, G. TURNWALD, Dickson polynomials, Pitman Monographs and Surveys in Pure and Applied Mathematics, 65. Longman Scientific & Technical, 1993.

[M] P. L. MONTGOMERY, New solutions of $a^{p-1} \equiv 1 \pmod{p^2}$, Math. of Computation, 61 (1993), 361-363.

[R] P. E. RICCI, Alcuni osservazioni sulle potenze delle matrici del secondo ordine e sui polinomi di Tchebycheff di seconda specie. Atti Accad. Sci. Torino, Cl. Sci. Fis. Mat. Natur., 109 (1975), 405-410.

[T] F. G. TRICOMI, Sulle potenze di una matrici del secondo ordine. Dans le volume "Omagio a Carlo Ferrari", Libreria Editrice Universitaria Levrotto & Bella, Torino, Dicembre 1974, pp. 675-677.

Manuscrit reçu le 19 septembre 1995,
accepté le 22 janvier 1996.

Michel KERVAIRE,
Université de Genève
Département de Mathématiques
2, rue du Lièvre
C.P. 240
1211 Genève 24 (Suisse).