ACTA ARITHMETICA
LXXXVIII.2 (1999)

Corps de nombres engendrés par un nombre de Salem

par

Franck Lalande (Paris)

Introduction. Les nombres de Salem et plus généralement les entiers algébriques réciproques constituent une obstruction à la solution de la question de Lehmer (1933) [L] : Existe-t-il des polynômes unitaires, à coefficients entiers, irréductibles, dont la mesure de Mahler soit inférieure à 1,1762...?

La mesure de Mahler d'un entier algébrique α de polynôme minimal $P(X) = \prod_{i=1}^{n}(X - \alpha_i)$ est définie par

$$M(\alpha) = M(P) = \prod_{i=1}^{n} \max(1, |\alpha_i|).$$

Le nombre $\tau_0 = 1{,}1762\ldots$, appelé nombre de Lehmer, est le plus petit nombre de Salem connu. Sa mesure de Mahler 1,1762... est la plus petite mesure de Mahler actuellement connue, et le nombre τ_0 est racine du polynôme irréductible de degré 10

$$X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1$$

dont le groupe de Galois est T_{37} (cf. [Bu]), l'unique sous-groupe pair d'indice 2 du produit en couronne $\mathbb{Z}/2 \wr S_5$.

Bien que les nombres de Pisot et de Salem soient très liés (tout nombre de Pisot est limite d'une suite de nombres de Salem), les méthodes utilisées pour l'étude des nombres de Pisot n'ont jamais permis d'approcher les nombres de Salem. Ceci tient essentiellement au fait que les nombres de Salem sont des entiers algébriques réciproques.

En particulier, on ne sait toujours pas s'il existe un plus petit nombre de Salem ou si, au contraire, une suite infinie de nombres de Salem tend vers 1. Seules les tables de Boyd [Bo1–3] puis de Mossinghoff [M1–2] nous renseignent de façon complète sur les plus petites mesures de Mahler des entiers algébriques réciproques jusqu'au degré 24.

1991 *Mathematics Subject Classification*: Primary 11R06, 11R32; Secondary 11R27, 12F10.

Key words and phrases: nombres de Salem, théorie de Galois, polynômes réciproques.

On peut alors penser que les corps de nombres engendrés par un nombre de Salem ou plus généralement par un entier algébrique réciproque ont des propriétés remarquables, donnant en retour des renseignements sur les plus petits nombres de Salem.

Ainsi motivés, nous avons cherché à caractériser de tels corps de nombres. La répartition très caractéristique des racines d'un polynôme de Salem ou d'un polynôme réciproque nous a alors orienté vers une caractérisation en termes de groupes de Galois.

1. Rappels et notations. Commençons par rappeler quelques définitions.

Définition 1. Un *nombre de Pisot* est un entier algébrique réel supérieur à 1 dont tous les autres conjugués ont un module strictement inférieur à 1.

Définition 2. Un *nombre réciproque* est un entier algébrique dont le polynôme minimal P est réciproque, c'est-à-dire $P(z) = z^s P(1/z)$ pour tout $z \in \mathbb{C}^*$ où s désigne le degré de P.

Un nombre réciproque peut également être vu comme un entier algébrique α dont $1/\alpha$ est l'un des conjugués.

Définition 3. Un *nombre de Salem* est un entier algébrique réel τ strictement supérieur à 1, dont tous les autres conjugués ont un module inférieur ou égal à 1 avec au moins un conjugué de module 1.

On déduit de cette définition que le polynôme minimal d'un nombre de Salem τ est réciproque de degré pair au moins égal à 4 et que tous les conjugués de τ (excepté τ et $1/\tau$) sont complexes non réels et de module 1. On pourra consulter [Be] pour davantage de précisions.

Rappelons maintenant un résultat concernant les nombres de Pisot qui sera utile pour la suite.

Proposition 1. *Tout corps de nombres réel peut être engendré par une infinité de nombres de Pisot. Certains de ces nombres sont des unités du corps.*

Nous ne rappelons pas ici la démonstration de cette proposition. Elle est par exemple rédigée dans [Be] (Théorème 5.2.2).

Etant donné un polynôme irréductible P de $\mathbb{Q}[X]$ et L son corps de décomposition, une numérotation des racines $x_1, \ldots, x_n$ de P étant choisie, on identifiera dans la suite le groupe de Galois de l'extension $L/\mathbb{Q}$ à son image dans le groupe symétrique S_n par le morphisme

$$\varphi : \mathrm{Gal}(L/\mathbb{Q}) \to S_n, \quad \sigma \mapsto \widetilde{\sigma},$$

où $\widetilde{\sigma}$ est défini par $\sigma(x_i) = x_{\widetilde{\sigma}(i)}$ pour tout $i = 1, \ldots, n$.

Enfin, considérons le polynôme

$$P_n(x_1, \ldots, x_{2n}) = x_1x_2 + x_3x_4 + \ldots + x_{2n-1}x_{2n}.$$

Le groupe symétrique S_{2n} agit de manière naturelle sur P_n en posant pour tout $\sigma \in S_{2n}$,

$$\sigma(P_n(x_1, \ldots, x_{2n})) = P_n(x_{\sigma(1)}, \ldots, x_{\sigma(2n)}).$$

Pour cette action, le sous-groupe de S_{2n} qui stabilise P_n est le produit semi-direct de $(\mathbb{Z}/2)^n$ par S_n pour l'action

$$S_n \times (\mathbb{Z}/2)^n \to (\mathbb{Z}/2)^n, \quad (h, (\sigma_1, \ldots, \sigma_n)) \mapsto (\sigma_{h^{-1}(1)}, \ldots, \sigma_{h^{-1}(n)}).$$

Ce produit semi-direct est appelé *produit en couronne* de $\mathbb{Z}/2$ par S_n et noté $\mathbb{Z}/2 \wr S_n$. On définit de même le produit en couronne $\mathbb{Z}/2 \wr H$ pour tout sous-groupe H de S_n.

Ce produit en couronne $\mathbb{Z}/2 \wr S_n$ est bien connu des géomètres. C'est le groupe des symétries du repère cartésien orthonormal de dimension n. Il est appelé *groupe hyper-octaédral* et noté B_n ou $[3^{n-2}, 4]$. On pourra consulter [CM] pour davantage de précisions.

2. Corps de nombres engendrés par un nombre de Salem. Soit K un corps de nombres réel. Le premier problème est de déterminer sous quelles conditions K peut être engendré par un nombre de Salem.

Par définition des nombres de Salem, K doit nécessairement être une extension de $\mathbb{Q}$ de degré pair égal à $2n$ supérieur ou égal à 4 et admettre $2n-2$ corps conjugués complexes.

Nous allons prouver le résultat suivant :

THÉORÈME 1. *Soit K un corps de nombres réel de degré $2n$, dont le groupe des unités est de rang n et de clôture galoisienne L. Notons θ_1 un générateur de K et $\theta_1, \ldots, \theta_{2n}$ les conjugués de θ_1 ($\theta_1, \theta_2 \in \mathbb{R}$, $\theta_i \in \mathbb{C} \setminus \mathbb{R}$ pour $i = 3, 4, \ldots, 2n$). Le corps de nombres K est engendré par un nombre de Salem si et seulement si, en ordonnant les conjugués de la manière suivante* :

$$x_1 = \theta_1,\ x_2 = \theta_2,\ x_3 = \theta_3,\ x_4 = \overline{\theta}_3,\ \ldots,\ x_{2n-1} = \theta_{2n-1},\ x_{2n} = \overline{\theta}_{2n-1},$$

le groupe de Galois $\mathrm{Gal}(L/\mathbb{Q})$ *est inclus dans* $\mathbb{Z}/2 \wr S_n$.

P r e u v e. Montrons tout d'abord que si K est engendré par un nombre de Salem alors $\mathrm{Gal}(L/\mathbb{Q}) \subset \mathbb{Z}/2 \wr S_n$.

Fixons les notations. Notons τ un nombre de Salem engendrant K et $\tau_1 = \tau, \tau_2, \ldots, \tau_{2n}$ ses conjugués tels que $\tau_2 = 1/\tau$, $\tau_{2i-1} \in \mathbb{C} \setminus \mathbb{R}$ et $\tau_{2i} = \overline{\tau}_{2i-1} = 1/\tau_{2i-1}$ pour tout $i = 2, 3, \ldots, n$. Considérons alors $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Pour tout $i = 1, \ldots, n$,

$$\sigma(\tau_{2i-1})\sigma(\tau_{2i}) = \sigma(\tau_{2i-1}\tau_{2i}) = \sigma(1) = 1.$$

Ainsi, si $\sigma(\tau_{2i-1}) = \tau_{2k-1}$ ($k \in \{1,\dots,n\}$), $\sigma(\tau_{2i}) = 1/\tau_{2k-1} = \tau_{2k}$ et si $\sigma(\tau_{2i-1}) = \tau_{2k}$, $\sigma(\tau_{2i}) = \tau_{2k-1}$. Par suite, $\sigma \in \mathrm{Stab}_{S_{2n}}(P_n) = \mathbb{Z}/2 \wr S_n$ et donc $\mathrm{Gal}(L/\mathbb{Q}) \subset \mathbb{Z}/2 \wr S_n$.

Montrons maintenant la réciproque. Elle utilise le lemme suivant.

Lemme 1. *En conservant les notations du théorème* 1, *si* $\mathrm{Gal}(L/\mathbb{Q})$ *est inclus dans* $\mathbb{Z}/2 \wr S_n$ *alors* $\mathbb{Q}(\theta_{2k-1}) = \mathbb{Q}(\theta_{2k})$ *pour tout* $k \in \{1,\dots,n\}$.

Preuve. Soit k un entier appartenant à $\{1,\dots,n\}$. Notons $G = \mathrm{Gal}(L/\mathbb{Q}) \subset \mathbb{Z}/2 \wr S_n$ et H le sous-groupe de G qui fixe le sous-corps $\mathbb{Q}(\theta_{2k-1}, \theta_{2k})$ de L. Comme G est un sous-groupe transitif de S_{2n} puisque le polynôme minimal de θ_1 sur $\mathbb{Q}$ est irréductible, il existe $2n$ éléments distincts de G, $\sigma_1,\dots,\sigma_{2n}$, tels que $\sigma_i(\theta_{2k-1}) = \theta_i$ pour tout $i = 1,\dots,2n$. Ces $2n$ éléments de G constituent un système de représentants de G/H.

En effet, si $\sigma_i^{-1}\sigma_j \in H$ pour $i \neq j$ alors $\sigma_i^{-1}\sigma_j(\theta_{2k-1}) = \theta_{2k-1}$ soit $\sigma_i(\theta_{2k-1}) = \sigma_j(\theta_{2k-1})$ ou encore $\theta_i = \theta_j$, d'où la contradiction puisque les θ_i sont les conjugués de θ_1. Ainsi, les classes des σ_i dans G/H sont toutes distinctes.

De plus, $\mathrm{Card}(G/H) \leq 2n$. En effet, dans le cas contraire, il existerait deux éléments $\widetilde{\sigma}$ et $\widetilde{\sigma}'$ de G/H dont les représentants σ et σ' vérifieraient $\sigma(\theta_{2k-1}) = \sigma'(\theta_{2k-1})$. Mais comme σ et σ' appartiennent à $G \subset \mathbb{Z}/2 \wr S_n$, on aurait également $\sigma(\theta_{2k}) = \sigma'(\theta_{2k})$ et ainsi $\sigma^{-1}\sigma'$ serait dans H, d'où la contradiction.

Ainsi, $[\mathbb{Q}(\theta_{2k-1}, \theta_{2k}) : \mathbb{Q}] = 2n$ et comme $[\mathbb{Q}(\theta_{2k-1}) : \mathbb{Q}] = [\mathbb{Q}(\theta_{2k}) : \mathbb{Q}] = 2n$, on en déduit $\mathbb{Q}(\theta_{2k-1}, \theta_{2k}) = \mathbb{Q}(\theta_{2k-1}) = \mathbb{Q}(\theta_{2k})$.

Ceci achève la démonstration du lemme 1.

Revenons maintenant à la démonstration du théorème 1. Désormais, si F est un corps de nombres, on notera U_F le groupe des unités de F, $\mathrm{rg}(U_F)$ son rang et E_F le groupe des racines de l'unité de F.

D'après le lemme 1, $K = \mathbb{Q}(\theta_1) = \mathbb{Q}(\theta_2)$, ainsi le corps $K_0 = \mathbb{Q}(\theta_1 + \theta_2, \theta_1\theta_2)$ est un sous-corps de K. D'une part, $\theta_1 \notin K_0$ car sinon θ_1 s'écrirait sous la forme $R(\theta_1 + \theta_2, \theta_1\theta_2)$ ($R \in \mathbb{Q}[X,Y]$) et n'aurait donc qu'au plus n conjugués distincts, et d'autre part, comme θ_1 est une racine de $P(X) = X^2 - (\theta_1+\theta_2)X + \theta_1\theta_2$ appartenant à $K_0[X]$, K est une extension quadratique de K_0 et par suite, $[K_0 : \mathbb{Q}] = n$. Le groupe des unités U_{K_0} de K_0 est donc de rang $< n$. Plus précisement, comme les corps conjugués $K_0^{(i)} = \mathbb{Q}(\theta_{2i-1} + \theta_{2i}, \theta_{2i-1}\theta_{2i})$ ($i = 1,\dots,n$) de K_0 sont réels, K_0 est totalement réel et $\mathrm{rg}(U_{K_0}) = n - 1$.

Considérons alors le morphisme de groupes

$$N_{K/K_0} : U_K \to U_{K_0}, \qquad \varepsilon \mapsto \varepsilon\varepsilon',$$

où ε et ε' sont les conjugués de ε sur K_0. Cette application induit par passage

au quotient le morphisme

$$\widetilde{N}_{K/K_0} : U_K/E_K \to U_{K_0}/E_{K_0}.$$

En effet, $N_{K/K_0}(E_K)$ est inclus dans E_{K_0}. On a alors la suite exacte de $\mathbb{Z}$-modules libres suivante :

$$0 \to \operatorname{Ker} \widetilde{N}_{K/K_0} \to U_K/E_K \to \widetilde{N}_{K/K_0}(U_K/E_K) \to 0.$$

Ainsi $\operatorname{rg}(\operatorname{Ker} \widetilde{N}_{K/K_0}) = \operatorname{rg}(U_K/E_K) - \operatorname{rg}(\widetilde{N}_{K/K_0}(U_K/E_K)) \geq n-(n-1) = 1$. Par suite, il existe une unité ε_1 de K n'appartenant pas à E_K telle que $N_{K/K_0}(\varepsilon_1) = \varepsilon_1\varepsilon_2 = \pm 1$ (les seules racines de l'unité de K_0 sont ± 1 puisque K_0 est réel). En fait, $N_{K/K_0}(\varepsilon_1) = 1$. En effet, soit $\sigma \in G = \operatorname{Gal}(L/\mathbb{Q})$ tel que $\sigma(\theta_1) = \theta_3$. Comme $G \subset \mathbb{Z}/2 \wr S_n$, $\sigma(\theta_2) = \theta_4 = \overline{\theta}_3$ et donc $\sigma(N_{K/K_0}(\varepsilon_1)) = \sigma(\varepsilon_1)\sigma(\varepsilon_2) = \sigma(\varepsilon_1)\overline{\sigma(\varepsilon_1)} > 0$. Par conséquent, comme $\sigma(N_{K/K_0}(\varepsilon_1)) = \pm 1$, $\sigma(N_{K/K_0}(\varepsilon_1)) = 1$ et donc $N_{K/K_0}(\varepsilon_1) = 1$.

Considérons alors le polynôme $r \in \mathbb{Q}[X]$ tel que $\varepsilon_1 = r(\theta_1)$. Les conjugués de ε_1 sur $\mathbb{Q}$ sont alors $r(\theta_1), \ldots, r(\theta_{2n})$.

Nous allons maintenant voir que $\pm r(\theta_1)$ ou $\pm 1/r(\theta_1)$ est un nombre de Salem qui engendre K.

Puisque G est un sous-groupe transitif de S_{2n}, il existe $\sigma_i \in G$ tel que $\sigma_i(\theta_1) = \theta_{2i-1}$ pour tout $i \in \{1, \ldots, n\}$. Comme de plus, σ_i appartient à $\mathbb{Z}/2 \wr S_n$, $\sigma_i(\theta_2) = \theta_{2i}$. On a alors

$$\sigma_i(\varepsilon_1\varepsilon_2) = \sigma_i(1) = 1 = \sigma_i(r(\theta_1)r(\theta_2)) = r(\theta_{2i-1})r(\theta_{2i}).$$

De plus, comme $r(\theta_{2i}) = \overline{r(\theta_{2i-1})}$ pour $i = 2, 3, \ldots, n$, $r(\theta_i)$ est un nombre complexe non réel de module 1 pour tout $i = 3, 4, \ldots, 2n$. Enfin, les conjugués de $r(\theta_1)$ sont tous distincts. En effet, si deux conjugués étaient égaux, comme $r(\theta_i) \in \mathbb{C} \setminus \mathbb{R}$ pour tout $i = 3, 4, \ldots, 2n$, on aurait nécessairement $r(\theta_1) = r(\theta_2)$ et donc $\varepsilon_1 = \varepsilon_2$, d'où la contradiction.

Finalement, $r(\theta_1)$ est un entier algébrique réel admettant pour conjugués $r(\theta_2) = 1/r(\theta_1)$ et $2n-2$ conjugués complexes non réels tous distincts de module 1. Ainsi, $\pm r(\theta_1)$ ou $\pm 1/r(\theta_1)$ est un nombre de Salem qui engendre K. Ceci achève le démonstration du théorème 1.

Remarque 1. On peut déterminer de manière relativement explicite un nombre de Salem qui engendre K. En effet, on montre avec les mêmes arguments que ceux utilisés ci-dessus que $\mathbb{Q}(\theta_3)$ contient une unité qui n'est ni réelle ni imaginaire pure (un élément du noyau du morphisme $N : U_{\mathbb{Q}(\theta_3)} \to U_{\mathbb{Q}(\theta_3)\cap\mathbb{R}}$ convient). Notons u une telle unité et $u_1, u_2, u_3 = u, \ldots, u_{2n}$ ses conjugués. Comme u n'est ni réelle ni imaginaire pure, $u/\overline{u} = u_3/u_4$ est différent de ± 1, son conjugué u_1/u_2 est donc lui aussi différent de ± 1 et vérifie $N_{K/K_0}(u_1/u_2) = (u_1/u_2)(u_2/u_1) = 1$. Comme on vient de le voir, $\pm u_1/u_2$ ou $\pm u_2/u_1$ est alors un nombre de Salem qui engendre K.

Corollaire 1. *En conservant les notations du théorème* 1 *et en notant* $\pi_1, \ldots, \pi_k$ *un système de représentants de* $S_{2n}/(\mathbb{Z}/2 \wr S_n)$, *si* $\theta_1\theta_2 + \theta_3\theta_4 + \ldots + \theta_{2n-1}\theta_{2n}$ *appartient à* $\mathbb{Z}$ *et n'est pas une racine multiple du polynôme*

$$Q_{(S_{2n},\mathbb{Z}/2\wr S_n)}(X) = \prod_{i=1}^{k}(X - \pi_i(P_n(\theta_1, \ldots, \theta_{2n})))$$

alors $\mathrm{Gal}(L/\mathbb{Q}) \subset \mathbb{Z}/2 \wr S_n$ *et* $K = \mathbb{Q}(\theta_1)$ *est engendré par un nombre de Salem.*

P r e u v e. On raisonne comme Stauduhar [S]. Si $P_n(\theta_1, \ldots, \theta_{2n})$ appartient à $\mathbb{Z}$ alors $P_n(\theta_1, \ldots, \theta_{2n})$ est fixé par tous les éléments de $\mathrm{Gal}(L/\mathbb{Q})$. Si de plus $P_n(\theta_1, \ldots, \theta_{2n})$ n'est pas une racine multiple de $Q_{(S_{2n},\mathbb{Z}/2\wr S_n)}$ alors seuls les éléments de $\mathbb{Z}/2 \wr S_n$ fixent $P_n(\theta_1, \ldots, \theta_{2n})$ et donc $\mathrm{Gal}(L/\mathbb{Q})$ est inclus dans $\mathbb{Z}/2 \wr S_n$. Par suite, d'après le théorème 1, K est engendré par un nombre de Salem.

Remarque 2. Si $P_n(\theta_1, \ldots, \theta_{2n})$ est une racine multiple de $Q_{(S_{2n},\mathbb{Z}/2\wr S_n)}$, on peut effectuer une transformation de Tschirnhaus. Plus précisément, on considère un polynôme $h \in \mathbb{Z}[X]$ tel que

$$\mathbb{Q}(\theta_1, \ldots, \theta_{2n}) = \mathbb{Q}(h(\theta_1), \ldots, h(\theta_{2n}))$$

et tel que le polynôme

$$R_{(S_{2n},\mathbb{Z}/2\wr S_n)}(X) = \prod_{i=1}^{k}(X - \pi_i(P_n(h(\theta_1)), \ldots, P_n(h(\theta_{2n}))))$$

n'ait pas de racines multiples. Un tel polynôme existe (voir [G]), la plupart des polynômes vérifient ces conditions.

Dans ce cas, si $h(\theta_1)h(\theta_2)+\ldots+h(\theta_{2n-1})h(\theta_{2n})$ appartient à $\mathbb{Z}$, $\mathrm{Gal}(L/\mathbb{Q})$ est inclus dans $\mathbb{Z}/2 \wr S_n$ et K est engendré par un nombre de Salem, sinon $\mathrm{Gal}(L/\mathbb{Q})$ n'est pas inclus dans $\mathbb{Z}/2 \wr S_n$.

Corollaire 2. *Soit* K *un corps de nombres réel de degré* 4 *dont le groupe des unités est de rang* 2. *Notons* θ *un générateur de* K *et* $\theta_1 = \theta, \theta_2, \theta_3, \theta_4 = \overline{\theta}_3$ *ses conjugués. Le corps de nombres* K *est engendré par un nombre de Salem si et seulement si* $\theta_1\theta_2 + \theta_3\theta_4 \in \mathbb{Z}$.

P r e u v e. Notons L la clôture galoisienne de K. D'après le corollaire 1, si $\theta_1\theta_2 + \theta_3\theta_4 \in \mathbb{Z}$ et n'est pas une racine multiple du polynôme

$$Q_{(S_4,\mathbb{Z}/2\wr S_2)}(X) = (X - (\theta_1\theta_2 + \theta_3\theta_4))(X - (\theta_1\theta_3 + \theta_2\theta_4))(X - (\theta_1\theta_4 + \theta_2\theta_4))$$

alors $\mathrm{Gal}(L/\mathbb{Q}) \subset \mathbb{Z}/2 \wr S_2$ et K est engendré par un nombre de Salem.

Mais comme $\theta_1\theta_3 + \theta_2\theta_4 = \overline{\theta_1\theta_4 + \theta_2\theta_3}$ et comme $\theta_1\theta_2 + \theta_3\theta_4$ est réel, si $\theta_1\theta_2 + \theta_3\theta_4$ était une racine multiple de $Q_{(S_4,\mathbb{Z}/2\wr S_2)}$, on aurait $\theta_1\theta_3 + \theta_2\theta_4 = \theta_1\theta_4 + \theta_2\theta_3$. Mais ceci equivaut à $(\theta_1 - \theta_2)(\theta_3 - \theta_4) = 0$, d'où la

contradiction puisque les θ_i sont tous distincts. Ceci achève la démonstration du corollaire 2.

EXEMPLES. Dans les exemples qui suivent, on considère un corps de nombres réel $K = \mathbb{Q}(\theta)$ de degré $2n$, dont le groupe des unités est de rang n et de clôture galoisienne L vérifiant $\mathrm{Gal}(L/\mathbb{Q}) \subset \mathbb{Z}/2 \wr S_n$. D'après le théorème 1, K est engendré par un nombre de Salem.

On note θ' l'un des conjugués non réels de θ et dans chacun des exemples suivants, on donne :

1. Le polynôme minimal P de θ.
2. Le groupe de Galois $\mathrm{Gal}(L/\mathbb{Q})$.
3. Une unité u de $\mathbb{Q}(\theta')$ ni réelle ni imaginaire pure.
4. Le polynôme minimal S d'un nombre de Salem engendrant K. Il est obtenu en considérant le polynôme $S_1(X) = \prod_{i=1}^{n}(X - u_{2i-1}/u_{2i})(X - u_{2i}/u_{2i-1})$ (où les u_i sont les conjugués de u sur $\mathbb{Q}$) (ou $S_1(-X)$ dans le cas où S_1 est le polynôme minimal de l'opposé d'un nombre de Salem) ou plus simplement en considérant le polynôme $S_2(X) = \prod_{i=1}^{2n}(X - u_i)$ (ou $S_2(-X)$ pour les mêmes raisons que ci-dessus) dans le cas où u est déjà de norme complexe égale à 1.
5. Une valeur approchée du nombre de Salem τ qui engendre K.

REMARQUE 3. Les calculs sont effectués avec Pari [P] et les polynômes considérés sont ou bien présents dans la littérature (cf. [O]) ou bien construits à l'aide d'une méthode qu'on exposera dans un prochain article. D'autre part, les notations utilisées pour les groupes sont celles de Butler et McKay [Bu].

$P(X) = X^6 - 3X^5 + 5X^4 - 5X^3 + X^2 + X - 1$
$\mathrm{Gal}(L/\mathbb{Q}) = T_6$
$u = \theta'$
$S(X) = X^6 - 5X^5 + 9X^4 - 11X^3 + 9X^2 - 5X + 1$
$\tau = 2{,}9024421609$

$P(X) = X^6 - 3X^5 + 3X^4 + X^3 - 3X^2 + 3X - 1$
$\mathrm{Gal}(L/\mathbb{Q}) = T_6$
$u = \theta'$
$S(X) = X^6 - 3X^5 + 3X^4 - 3X^3 + 3X^2 - 3X + 1$
$\tau = 2{,}0424905339$

$P(X) = X^6 - 3X^5 + 7X^4 - 9X^3 + 7X^2 - 3X - 1$
$\mathrm{Gal}(L/\mathbb{Q}) = T_6$
$u = \theta'$
$S(X) = X^6 - 9X^5 + 23X^4 - 31X^3 + 23X^2 - 9X + 1$
$\tau = 5{,}8788150324$

$P(X) = X^6 - 3X^2 - 1$
$\mathrm{Gal}(L/\mathbb{Q}) = T_4$
$u = \theta'^4 - \theta'^3 + \theta'^2 - 2\theta'$

$S(X) = X^6 - 12X^5 + 15X^4 - 16X^3 + 15X^2 - 12X + 1$
$\tau = 10{,}7297494343$

$P(X) = X^6 - 3X^5 + 6X^4 - 7X^3 + 2X^2 + X - 4$
$\mathrm{Gal}(L/\mathbb{Q}) = T_8$
$u = \theta'^3 + \theta' + 1$
$S(X) = X^6 - 219X^5 - 214X^4 - 52X^3 - 214X^2 - 219X + 1$
$\tau = 219{,}9739373551$

$P(X) = X^8 + 4X^6 + 2X^4 - 3X^2 - 1$
$\mathrm{Gal}(L/\mathbb{Q}) = T_{44} = \mathbb{Z}/2 \wr S_4$
$u = 8\theta'^7 - 7\theta'^6 + 38\theta'^5 - 33\theta'^4 + 45\theta'^3 - 39\theta'^2 + 11\theta' - 10$
$S(X) = X^8 - 126X^7 + 204X^6 + 86X^5 - 346X^4 + 86X^3 + 204X^2 - 126X + 1$
$\tau = 124{,}3541421240$

$P(X) = X^8 + 5X^6 + 5X^4 - 5X^2 - 5$
$\mathrm{Gal}(L/\mathbb{Q}) = T_{27} = \mathbb{Z}/2 \wr \mathbb{Z}/4$
$u = \theta'^5 + \theta'^4 + 3\theta'^3 + 3\theta'^2 + \theta' + 1$
$S(X) = X^8 - 8X^7 - 12X^6 - 16X^5 - 10X^4 - 16X^3 - 12X^2 - 8X + 1$
$\tau = 9{,}4610760104$

$P(X) = X^{10} + 6X^8 + 10X^6 + X^4 - 6X^2 - 1$
$\mathrm{Gal}(L/\mathbb{Q}) = T_8 \subset \mathbb{Z}/2 \wr \mathbb{Z}/5$
$u = \theta'^9 + 6\theta'^7 - \theta'^6 + 11\theta'^5 - 5\theta'^4 + 6\theta'^3 - 7\theta'^2 - 2$
$S(X) = X^{10} - 18X^9 - 15X^8 + 14X^6 + 4X^5 + 14X^4 - 15X^2 - 18X + 1$
$\tau = 18{,}7959000528$

$P(X) = X^{12} + 6X^{10} + 7X^8 - 12X^6 - 21X^4 - 9X^2 - 1$
$\mathrm{Gal}(L/\mathbb{Q}) = \mathbb{Z}/2 \wr T_6$
$u = \theta'^{10} + 5\theta'^8 + 2\theta'^6 + \theta'^5 - 16\theta'^4 + 4\theta'^3 - 13\theta'^2 + 3\theta' - 2$
$S(X) = X^{12} - 30X^{11} + 22X^{10} - 6X^9 - 17X^8 + 4X^7 - 12X^6 + 4X^5 - 17X^4 - 6X^3 + 22X^2 - 30X + 1$
$\tau = 29{,}2556933446$

$P(X) = X^{14} + 15X^{12} + 90X^{10} + 275X^8 + 448X^6 + 365X^4 + 114X^2 - 1$
$\mathrm{Gal}(L/\mathbb{Q}) = \mathbb{Z}/2 \wr S_7$
$u = 43\theta'^{13} - 4\theta'^{12} + 647\theta'^{11} - 60\theta'^{10} + 3896\theta'^9 - 360\theta'^8 + 11955\theta'^7 - 1101\theta'^6 + 19579\theta'^5 - 1800\theta'^4 + 16078\theta'^3 - 1480\theta'^2 + 5119\theta' - 473$
$S(X) = X^{14} - 970X^{13} - 1485X^{12} - 1148X^{11} - 559X^{10} + 714X^9 + 2043X^8 + 2680X^7 + 2043X^6 + 714X^5 - 559X^4 - 1148X^3 - 1485X^2 - 970X + 1$
$\tau = 971{,}5297341716$

3. Corps de nombres engendrés par un nombre réciproque. Plus généralement, on peut se demander à quelles conditions un corps de nombres peut être engendré par un nombre réciproque. Nous donnons ici une réponse à cette question dans le cas des corps de nombres non totalement complexes.

THÉORÈME 2. *Soit K un corps de nombres de degré $2n$, de clôture galoisienne L et dont le groupe des unités a un rang $\geq n$. Le corps de nombres K est engendré par un nombre réciproque si et seulement si* $\mathrm{Gal}(L/\mathbb{Q}) \subset \mathbb{Z}/2 \wr S_n$.

P r e u v e. On montre comme dans le cas des nombres de Salem que si K est engendré par un nombre réciproque alors $\mathrm{Gal}(L/\mathbb{Q}) \subset \mathbb{Z}/2 \wr S_n$.

On suppose maintenant que $\mathrm{Gal}(L/\mathbb{Q}) \subset \mathbb{Z}/2 \wr S_n$. Notons θ_1 un générateur de K, $\theta_1, \ldots, \theta_{2n}$ ses conjugués (ordonnés de telle sorte que pour cet ordre $\mathrm{Gal}(L/\mathbb{Q}) \subset \mathbb{Z}/2 \wr S_n$) et supposons d'abord K réel.

D'après la proposition 1, K est alors engendré par un nombre de Pisot que l'on peut choisir unité de K. Notons u cette unité et $u_1 = u, u_2, \ldots, u_{2n}$ ses conjugués sur $\mathbb{Q}$. D'après le lemme 1, $\mathbb{Q}(\theta_1) = \mathbb{Q}(\theta_2)$, u_2 est donc une unité de $\mathbb{Q}(\theta_1)$ et ainsi u_1/u_2 est un entier algébrique appartenant à K. D'autre part, $\mathrm{Gal}(L/\mathbb{Q})$ étant inclus dans $\mathbb{Z}/2 \wr S_n$, les conjugués de u_1/u_2 sont $u_1/u_2, u_2/u_1, u_3/u_4, \ldots, u_{2n-1}/u_{2n}, u_{2n}/u_{2n-1}$.

Il nous reste donc à voir que u_1/u_2 engendre K et ainsi K sera engendré par un nombre réciproque. Pour cela, montrons que les conjugués de u_1/u_2 sont tous distincts. Supposons que u_1/u_2 n'engendre pas K. Il existe alors 2 entiers j et k ($j = k \pm 1$) tels que $u_1/u_2 = u_j/u_k$ et donc tels que $u_1 u_k = u_2 u_j$. Considérons alors le polynôme

$$S(X) = \prod_{1 \le i < j \le 2n} (X - u_i u_j)$$

et appelons R le *polynôme minimal* de $u_1 u_k$. Comme $u_1 u_k = u_2 u_j$, $u_1 u_k$ est une racine double de S et donc R^2 divise S. D'autre part, R admet au moins une racine de module supérieur ou égal à 1, donc S admet une racine de module supérieur ou égal à 1 qui est double. Mais comme u_1 est un nombre de Pisot, les racines de S de module supérieur ou égal à 1 sont nécessairement de la forme $u_1 u_j$ avec $j \in \{2, 3, \ldots, 2n\}$. Il existe donc deux entiers j et j' distincts tels que $u_1 u_j = u_1 u_{j'}$ et donc tels que $u_j = u_{j'}$. D'où la contradiction et donc les conjugués de u_1/u_2 sur K sont tous distincts. Finalement, u_1/u_2 engendre K et par suite, si K est réel, K est engendré par un nombre réciproque.

Si K n'est pas réel, comme K n'est pas totalement complexe, l'un des corps conjugués K_i de K est réel. On montre alors comme on vient de le faire que K_i est engendré par un nombre réciproque et par suite K est également engendré par un nombre réciproque. Ceci achève la démonstration du théorème 2.

Je remercie très chaleureusement Mesdames Marie-José Bertin et Odile Lecacheux pour leur précieuse collaboration.

Bibliographie

[Be] M. J. Bertin, A. Decomps-Guilloux, M. Grandet-Hugo, M. Pathiaux-Delefosse and J. P. Schreiber, *Pisot and Salem Numbers*, Birkhäuser, Basel, 1992.

[Bo1] D. W. Boyd, *Small Salem numbers*, Duke Math. J. 44 (1977), 315–327.
[Bo2] —, *Reciprocal polynomials having small measure*, Math. Comp. 35 (1980), 1361–1377.
[Bo3] —, *Reciprocal polynomials having small measure 2*, ibid. 53 (1989), 355–357, S1–S5.
[Bu] G. Butler and J. McKay, *The transitive groups of degree up to eleven*, Comm. Algebra 11 (1983), 863–911.
[CM] H. S. M. Coxeter and W. O. J. Moser, *Generators and Relations for Discrete Groups*, 2nd ed., Springer, 1965.
[G] K. Girstmair, *On the computation of resolvents and Galois groups*, Manuscripta Math. 43 (1983), 289–307.
[L] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. 34 (1933), 461–479.
[M1] M. J. Mossinghoff, *Polynomials with small Mahler measure*, Math. Comp. 67 (1998), 1697–1705.
[M2] —, *Algorithms for the determination of polynomials with small Mahler measure*, Ph.D. thesis, University of Texas at Austin, 1995.
[O] M. Olivier, *Corps sextiques primitifs. 4*, Sém. Théor. Nombres Bordeaux (2) 3 (1991), no. 2, 381–404.
[P] C. Batut, D. Bernardi, H. Cohen and M. Olivier, *User's Guide to PARI-GP*, Version 1.39, 1995.
[S] R. P. Stauduhar, *The determination of Galois groups*, Math. Comp. 27 (1973), 981–996.

Equipe d'Arithmétique
Université P. et M. Curie (Paris 6)
Tour 46-56, 5ème étage, Boîte 247
4 place Jussieu
75252 Paris Cedex 05, France
E-mail: lalande@math.jussieu.fr

Reçu le 1.7.1998
et révisé le 21.9.1998 (3415)