

## Une caractérisation de certaines classes d'entiers algébriques généralisant les nombres de Salem

par

MOHAMED KERADA (Jijel)

**Introduction.** En 1933, D. H. Lehmer [7] posa la question suivante : existe-t-il une constante  $\varepsilon_0$ ,  $\varepsilon_0 > 0$ , telle que tout polynôme  $P$  unitaire, à coefficients entiers rationnels vérifiant

$$M(P) < 1 + \varepsilon_0,$$

ne possède que des racines de l'unité?

La quantité  $M(P)$ , appelée *mesure de Mahler de  $P$* , est définie pour un tel polynôme par

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

où  $\theta_1, \dots, \theta_n$  désignent les racines de  $P$ .

Lehmer donna également un polynôme de degré 10, de mesure de Mahler 1,17628..., appelé "polynôme de Lehmer" :

$$P(z) = z^{10} + z^9 - z^7 - z^6 - z^5 - z^4 - z^3 + z + 1.$$

La mesure de Mahler de ce polynôme est encore la plus petite mesure de Mahler connue. On remarque que ce polynôme est unitaire, irréductible, réciproque et possède une seule racine  $\tau$  positive de module strictement supérieur à 1 et au moins une racine de module 1. Un tel polynôme est appelé "polynôme de Salem" et sa racine de module supérieur à 1 "nombre de Salem".

Smyth [10] prouva en 1971 l'inégalité

$$M(P) \geq \theta_0 = 1,3247\dots,$$

pour  $P$  unitaire, à coefficients entiers rationnels, non réciproque,  $\theta_0$  désignant le plus petit "nombre de Pisot", racine supérieure à 1 de l'équation  $z^3 - z - 1 = 0$ . Rappelons qu'un entier algébrique  $\theta$ ,  $\theta > 1$ , est un "nombre de Pisot" si les autres conjugués ont un module strictement inférieur à 1.

Ce résultat de Smyth souligne l'importance de l'étude des polynômes unitaires, irréductibles, réciproques, en particulier des "polynômes de Salem", dans la résolution de la question de Lehmer.

Malheureusement, l'ensemble  $T$  des "nombres de Salem" est mal connu. On ignore la répartition des "nombres de Salem" dans  $\mathbb{R}$  et l'on ne sait si  $\inf(T) > 1$ . On remarque toutefois qu'une réponse positive à la question de Lehmer entraînerait  $\inf(T) > 1$ .

En 1944, Salem [8] a prouvé l'inclusion  $S \subset T'$ , où  $S$  désigne l'ensemble des "nombres de Pisot" et  $T'$  l'ensemble dérivé de l'ensemble  $T$ . Ce résultat découle de la construction suivante connue sous le nom de construction de Salem. Si  $\theta$  est un "nombre de Pisot", de polynôme minimal  $P$ , et  $\varepsilon$  le nombre  $+1$  ou  $-1$ , on définit le polynôme  $Q_n^\varepsilon$  par

$$Q_n^\varepsilon(z) = z^n P(z) + \varepsilon P^*(z),$$

où  $n$  est un entier rationnel,  $n \geq 1$  et  $P^*$  le polynôme réciproque de  $P$  ( $P^*(z) = z^s P(1/z)$ ,  $s$  désignant le degré de  $P$ ).

Salem [9] a alors montré que pour  $n \geq n_0$ , l'équation  $Q_n^\varepsilon(z) = 0$  a pour zéro un "nombre de Salem"  $\tau_n^\varepsilon$  tendant vers  $\theta$  lorsque  $n$  tend vers l'infini.

En 1977, D. W. Boyd [5] prouvait que tout "nombre de Salem" pouvait s'obtenir par la construction de Salem. Bien plus, il montrait que tout "nombre de Salem" est racine d'un polynôme  $Q_\varepsilon(z) = zP(z) + \varepsilon P^*(z)$ , où  $P$  est un polynôme unitaire, à coefficients entiers rationnels, ayant toutes ses racines de module strictement supérieur à 1.

Ce dernier résultat est d'ailleurs en relation avec les ensembles  $\mathcal{T}_q$  définis par M. J. Bertin [1].

En 1986, M. J. Bertin et D. W. Boyd ([2], [3]) ont défini des classes  $A_q$  et  $B_q$  de "nombres de Salem" telles que  $T = \bigcup_{q \geq 2} A_q = \bigcup_{q \geq 0} B_q$  et montré que tous les petits "nombres de Salem" connus, à quelques exceptions près, ont leurs conjugués séparés par des racines de l'unité.

Nous nous proposons ici d'étendre ce résultat à des polynômes unitaires, réciproques, de petite mesure, possédant  $j$  racines ( $j \geq 2$ ) de module strictement supérieur à 1 et au moins une racine de module 1 ( $j$ -Salem) dont la liste est donnée par D. W. Boyd dans [5]. L'intérêt de ces résultats est une meilleure connaissance de la répartition sur le disque unité des racines des polynômes réciproques de petite mesure. La généralisation est basée sur l'idée d'ajouter aux racines de module 1 d'un  $j$ -Salem des racines  $j$ ième de l'unité, ce qui était évidemment occulté dans le cas  $j = 1$ .

Dans le premier paragraphe, on rappelle certaines définitions et propriétés de courbes algébriques. Dans le deuxième on généralise la construction de Boyd. On introduit au paragraphe 3 les ensembles  $A_q(j)$  et  $B_q(j)$ , prouvant certaines relations d'inclusion entre ces ensembles, pour caractériser au paragraphe 4 des sous-ensembles des  $A_q(j)$  et  $B_q(j)$ .

**I. Rappels.** Dans la suite,  $\varepsilon$  désignera le nombre  $+1$  ou  $-1$  et  $j$  un entier strictement positif. Soit  $P$  un polynôme à coefficients réels de degré  $s$ . On note  $P^*$  le polynôme réciproque de  $P$  défini par  $P^*(z) = z^s P(1/z)$ .

On suppose  $P$  et  $P^*$  premiers entre eux. Comme dans [5], on associe au polynôme  $Q_j^\varepsilon$  défini par

$$Q_j^\varepsilon(z) = z^j P(z) + \varepsilon P^*(z),$$

l'équation algébrique  $Q_j^\varepsilon(z, t) = z^j P(z) + \varepsilon t P^*(z) = 0$ ,  $0 \leq t \leq 1$ . Cette équation définit une courbe algébrique  $C$ ,  $z = Z(t)$ , possédant  $j + s$  branches, notées  $z_k(t)$ , orientées dans le sens des  $t$  croissant, ayant les propriétés suivantes :

(a)  $z_k([0, 1]) \subset D(0, 1)$  ou bien  $z_k([0, 1]) \subset \mathbb{C} - \overline{D(0, 1)}$ ,  $D(0, 1)$  (resp.  $\overline{D(0, 1)}$ ) désignant le disque unité ouvert (resp. fermé);

(b)  $z_k(1)$  est racine du polynôme  $Q_j^\varepsilon$ ;

(c) si  $\alpha$  est une racine de module 1 de  $Q_j^\varepsilon$ , il existe au moins une branche  $z_k$  telle que  $z_k(1) = \alpha$ ;

(d)  $z_k(0)$  est racine du polynôme  $z^j P$ .

**DÉFINITION 1.1.** Soit  $\alpha$  une racine de module 1 de  $Q_j^\varepsilon$  et  $z_k$  une branche de  $C$  passant par  $\alpha$  (i.e.  $z_k(1) = \alpha$ ). On dit que  $\alpha$  est une *sortie* (resp. *entrée*) si  $|z_k(0)| < 1$  (resp.  $|z_k(0)| > 1$ ). On dit également que la branche *sort* (resp. *entre*) en  $\alpha$ .

On rappelle également le lemme suivant dû à Boyd [5].

**LEMME 1.1.** Soit  $\alpha$  une racine de module 1 de  $Q_j^\varepsilon$ .

(1) On suppose  $\alpha$  racine simple. Alors  $\alpha$  est une entrée (resp. sortie) si et seulement si

$$\varepsilon \alpha^{1-s} P(\alpha) (Q_j^\varepsilon)'(\alpha) > 0 \quad (\text{resp. } < 0).$$

(2) On suppose  $\alpha$  racine multiple d'ordre  $k$ ,  $k \geq 2$ . Alors il existe  $k_1$  branches entrant en  $\alpha$  et  $k_2$  branches sortant en  $\alpha$ , avec  $k_1 + k_2 = k$ ,  $k_1 \geq [k/2]$ ,  $k_2 \geq [k/2]$  ( $[x]$  désignant la partie entière du réel  $x$ ).

On utilisera aussi les lemmes suivants (cf. [4]).

**LEMME 1.2.** Soit  $Q$  un polynôme réciproque à coefficients réels, de degré  $2m$  et  $\alpha$  une racine de module 1 de  $Q$ . Alors  $Q'(\alpha)/\alpha^{m-1}$  est nul ou imaginaire pur.

**LEMME 1.3.** Soit  $Q$  le polynôme réciproque à coefficients réels  $Q(z) = d_0 + \dots + d_m z^m + \dots + d_0 z^{2m}$ . Soit  $\alpha$  une racine de module 1 de  $Q$ . Alors  $d_m/2 + d_{m-1}\alpha + \dots + d_0\alpha^m$  est nul ou imaginaire pur.

## II. Généralisation de la construction de Boyd

**DÉFINITION 2.1.** Soit  $\tau$  un entier algébrique tel que  $|\tau| > 1$ . On dit que  $\tau$  est un  $j$ -Salem (resp.  $j$ -Pisot) si son polynôme minimal possède exactement  $j - 1$  racines différentes de  $\tau$  dans  $|z| > 1$  et au moins une (resp. aucune) racine sur  $|z| = 1$ . On note  $T(j)$  (resp.  $S(j)$ ) l'ensemble des  $j$ -Salem (resp.  $j$ -Pisot).

**PROPOSITION 2.1.** Soit  $P$  un polynôme unitaire à coefficients entiers sans racine sur  $|z| = 1$  et possédant exactement  $j$  racines dans  $|z| > 1$ . Soit  $Q^\varepsilon$  le polynôme défini par  $Q^\varepsilon(z) = z^j P(z) + \varepsilon P^*(z)$ . Si  $Q^\varepsilon$  possède exactement  $j$  racines dans  $|z| > 1$ , alors toutes ses racines de module 1 sont simples.

*Preuve.* Supposons que  $\alpha$  soit une racine de module 1 de  $Q^\varepsilon$  d'ordre  $r$ ,  $r \geq 2$ . Considérons la courbe algébrique  $C$  définie par  $Q^\varepsilon(z, t) = z^j P(z) + \varepsilon t P^*(z) = 0$ ,  $0 \leq t \leq 1$ . D'après le lemme 1.1,  $C$  possède au moins  $\lceil r/2 \rceil \geq 1$  branches rentrant en  $\alpha$ . Par suite,  $P$  possède au moins  $j + 1$  racines dans  $|z| > 1$  qui sont respectivement début des  $j$  branches finissant en les  $j$  racines de module supérieur à 1 de  $Q^\varepsilon$  et de la branche rentrant en  $\alpha$ ; d'où la contradiction.

**PROPOSITION 2.2.** Soit  $P$  un polynôme unitaire à coefficients entiers, sans racines dans  $|z| \leq 1$  et  $Q^\varepsilon$  le polynôme défini comme précédemment. Si  $Q^\varepsilon$  possède exactement  $j$  racines dans  $|z| > 1$ , alors toutes ses racines de module 1 sont simples.

*Preuve.* On définit comme dans la proposition 2.1 la courbe algébrique  $C$ . Si  $\alpha$  était racine multiple de module 1 de  $Q^\varepsilon$ , alors il y aurait au moins une branche de  $C$  sortant en  $\alpha$ ; d'où  $j + 1$  branches commençant en des zéros de  $z^j P$ , à savoir les  $j$  branches finissant en les  $j$  racines de  $Q^\varepsilon$  situées dans  $|z| < 1$  et la branche sortant en  $\alpha$ . Par suite,  $P$  posséderait au moins un zéro dans  $|z| < 1$ ; d'où la contradiction.

**THÉORÈME 2.1.** Soit  $P$  un polynôme de degré  $s$  à coefficients réels. On définit le polynôme  $Q^\varepsilon$  comme précédemment et l'on suppose que :

- (a) toutes les racines de  $Q^\varepsilon$  sont simples;
- (b)  $Q^\varepsilon$  possède exactement  $j$  racines dans  $|z| < 1$ ;
- (c)  $\varepsilon \alpha^{1-s} P(\alpha) (Q^\varepsilon)'(\alpha) < 0$  pour tout  $\alpha$  racine de module 1 de  $Q^\varepsilon$ .

Alors  $P$  possède  $j$  racines dans  $|z| > 1$  et  $s - j$  racines dans  $|z| < 1$ .

*Preuve.* Soit  $k$  le nombre de zéros de  $P$  dans  $|z| < 1$ . Définissons comme précédemment la courbe algébrique  $C$ . Les hypothèses (a) et (c) entraînent grâce au lemme 1.1 que les  $s - j$  racines de module 1 de  $Q^\varepsilon$  sont des sorties correspondant à des branches qui commencent en  $s - j$  racines de  $z^j P$  situées dans  $|z| < 1$ . En outre, les  $j$  racines de module inférieur à 1 de  $Q^\varepsilon$  sont des fins de branches commençant en des racines de  $z^j P$  situées dans  $|z| < 1$ . Par

suite,  $z^j P$  possède exactement  $s$  racines dans  $|z| < 1$ . On en déduit donc  $k = s - j$ .

THÉOREME 2.2. Soient  $P$  et  $Q^\varepsilon$  des polynômes définis comme dans le théorème 2.1. On suppose que :

- (a) toutes les racines de  $Q^\varepsilon$  sont simples;
- (b)  $Q^\varepsilon$  possède exactement  $j$  racines dans  $|z| > 1$ ;
- (c)  $\varepsilon \alpha^{1-s} P(\alpha)(Q^\varepsilon)'(\alpha) > 0$  pour toute racine  $\alpha$  de module 1 de  $Q^\varepsilon$ .

Alors  $P$  possède toutes ses racines dans  $|z| > 1$ .

Preuve. La raisonnement est semblable au précédent. Soit  $k$  le nombre des racines de  $P$  dans  $|z| > 1$ . Les hypothèses (a) et (c) entraînent grâce au lemme 1.1 que la courbe algébrique  $C$  possède  $s - j$  entrées qui proviennent donc de  $s - j$  racines de  $z^j P$  de module strictement supérieur à 1. Comme les racines de  $Q^\varepsilon$  de module strictement supérieur à 1 sont des fins de branches commençant dans  $|z| > 1$  en des zéros de  $z^j P$ , on en déduit que  $k = s - j + j = s$ .

Soit  $T$  le polynôme minimal d'un  $j$ -Salem de degré  $2m$ . Si  $U$  est un polynôme dont toutes les racines sont simples et racines de l'unité, alors le polynôme  $Q = UT$  est réciproque ou antiréciproque et possède  $s - 2j$  racines simples de module 1,  $s$  désignant le degré de  $Q$ .

THÉOREME 2.3. Soit  $Q = UT$  défini comme ci-dessus. En choisissant  $U$  convenablement on peut en outre supposer dans le cas  $\varepsilon = 1$  et  $s$  pair que le coefficient du monôme de degré  $s/2 - j$  de  $Q$  est pair. Alors pour  $\varepsilon$  valant  $+1$  ou  $-1$ , il existe une infinité de polynômes unitaires à coefficients entiers  $P$ , de degré  $s - j$ , ayant toutes leurs racines de module strictement supérieur à 1 tels que

$$Q(z) = z^j P(z) + \varepsilon P^*(z).$$

Preuve. Comme  $Q$  possède exactement  $s - 2j$  racines simples de module 1, les conditions (a) et (b) du théorème 2.2 sont vérifiées. On va alors déterminer  $P$  grâce au théorème 2.2. Supposons d'abord  $j$  impair,  $\varepsilon = 1$  et  $s$  pair. Dans ce cas,  $1$  et  $-1$  ne sont pas racines de  $Q$ . Posons  $s = 2l = j + n$  où  $n$  désigne le degré de  $P$ . On a donc

$$Q(z) = z^{2l} + d_1 z^{2l-1} + \dots + 2d_l z^l + \dots + d_1 z + 1.$$

Posons

$$P(z) = z^{2l-j} + d_1 z^{2l-j-1} + \dots + (d_j - c_1) z^{2l-2j} + \dots + (d_{l-1} - c_{l-j}) z^{l-j+1} + d_l z^{l-j} + c_{l-j} z^{l-j-1} + \dots + c_2 z + c_1.$$

Alors  $P$  vérifie  $Q = z^j P + P^*$ .

Pour obtenir un polynôme  $P$  dont toutes les racines sont de module strictement supérieur à 1, il suffit donc d'après le théorème 2.2 de déterminer

des entiers  $c_1, \dots, c_{l-j}$  ( $c_1 \neq 0$ ) vérifiant

$$(1) \quad \alpha^{1-2l+j} P(\alpha) Q'(\alpha) > 0$$

pour  $\alpha$  valant successivement  $\alpha_1, \dots, \alpha_{l-j}$  si l'on note  $\alpha_1, \bar{\alpha}_1, \dots, \alpha_{l-j}, \bar{\alpha}_{l-j}$  les racines de module 1 de  $Q$ .

On a donc un système de  $l-j$  inéquations pour déterminer  $l-j$  entiers. Ecrivons

$$\alpha^{1-2l+j} P(\alpha) Q'(\alpha) = (P(\alpha)/\alpha^{l-j})(Q'(\alpha)/\alpha^{l-j}).$$

On a donc

$$\begin{aligned} & P(\alpha)/\alpha^{l-j} \\ &= \alpha^l + d_1 \alpha^{l-j} + \dots + d_{l-1} \alpha + d_l - c_{l-j}(\alpha + \alpha^{-1}) - \dots - c_1(\alpha^{l-j} - \alpha^{-(l-j)}). \end{aligned}$$

D'après le lemme 1.3, on peut écrire

$$P(\alpha)/\alpha^{l-j} = i\delta - c_{l-j}(\alpha - \alpha^{-1}) - \dots - c_1(\alpha^{l-j} - \alpha^{-(l-j)}),$$

avec  $\delta \in \mathbb{R}$  et d'après le lemme 1.2,  $Q'(\alpha)/\alpha^{l-1} = i\rho$  avec  $\rho \in \mathbb{R}^*$ . Posant  $\alpha = e^{i\varphi}$ , on a donc

$$\alpha^{1-2l+j} P(\alpha) Q'(\alpha) = \rho(2c_1 \sin(l-j)\varphi + \dots + 2c_{l-j} \sin \varphi - \delta).$$

Par suite les  $l-j$  inéquations (1) sont équivalentes aux  $l-j$  inéquations (1') de la forme

$$c_1 \sin(l-j)\varphi + \dots + c_{l-j} \sin \varphi > \delta/2 \quad \text{si } \rho > 0$$

ou de la forme

$$c_1 \sin(l-j)\varphi + \dots + c_{l-j} \sin \varphi < \delta/2 \quad \text{si } \rho < 0.$$

Or la matrice  $\mathbb{A} = (a_{kh})$  où  $a_{kh} = \sin(l-j-h+1)\varphi$ , pour  $1 \leq h \leq l-j$  et où  $\varphi$  prend les valeurs successives  $\varphi_1, \dots, \varphi_{l-j}$ , a un déterminant non nul.

Sinon il existerait  $l-j$  entiers  $c_1, \dots, c_{l-j}$  non tous nuls vérifiant

$$c_1(\alpha^{l-j} - \alpha^{-(l-j)}) + \dots + c_{l-j}(\alpha - \alpha^{-1}) = 0$$

pour  $\alpha$  valant successivement  $\alpha_1, \dots, \alpha_{l-j}$ . Par suite, le polynôme  $X$ , non identiquement nul, de degré inférieur ou égal à  $2l-2j$ ,

$$X(z) = c_1 z^{2l-2j} + \dots + c_{l-j} z^{l-j+1} - c_{l-j} z^{l-j-1} - \dots - c_2 z - c_1,$$

aurait  $2l-2j+1$  racines, à savoir  $1, \alpha_1, \bar{\alpha}_1, \dots, \alpha_{l-j}, \bar{\alpha}_{l-j}$ , ce qui est impossible.

Par suite, les  $l-j$  inéquations (1') définissent un cône de  $\mathbb{R}^{l-j}$  contenant une infinité de points à coordonnées entières  $(c_1, \dots, c_{l-j})$  avec  $c_1 \neq 0$ . Il existe donc une infinité de polynômes vérifiant les conditions du théorème.

Les cas  $\varepsilon = 1$ ,  $s$  impair, puis  $\varepsilon = -1$ ,  $s$  pair ou impair, se traitent de la même façon. Dans le premier cas,  $-1$  est racine de  $Q$ ,  $s = 2l+1 = n+j$  et l'on a  $l-j+1$  inéquations du type (1). Dans le dernier cas enfin  $\varepsilon = -1$ ,  $s = 2l+1$ ,  $1$  est racine de  $Q$  et l'on a  $l-j+1$  inéquations.

Un raisonnement analogue peut être fait pour  $j$  pair. Il est laissé au lecteur.

**THÉORÈME 2.4.** *Sous les hypothèses du théorème 2.3, pour  $\varepsilon \in \{-1, 1\}$ , il existe une infinité de polynômes unitaires, à coefficients entiers  $P$  de degré  $s - j$ , sans racine de module 1 et possédant exactement  $j$  racines de module supérieur à 1, vérifiant*

$$Q(z) = z^j P(z) + \varepsilon P^*(z).$$

*Preuve.* Comme  $Q$  possède exactement  $s - 2j$  racines simples de module 1, il vérifie les conditions (a) et (b) du théorème 2.1. On détermine alors  $P$  comme dans le théorème précédent mais grâce au théorème 2.1.

### III. Ensembles $A_q(j)$ et $B_q(j)$

**DÉFINITION 3.1.** On appelle  $A_q(j)$  (resp.  $B_q(j)$ ),  $q$  étant un entier supérieur ou égal à 2 (resp. 0), l'ensemble des  $j$ -Salem de polynôme minimal  $T$  pour lesquels il existe au moins un polynôme  $P$  vérifiant les conditions du théorème 2.3 (resp. 2.4) tel que  $|P(0)| = q$  et  $U$  multiple d'un facteur non trivial de  $z^j - 1$ .

*Remarque.* Si l'on désigne comme dans II par  $T(j)$  l'ensemble des  $j$ -Salem, le théorème 2.3 (resp. 2.4) entraîne les égalités

$$T(j) = \bigcup_{q \geq 2} A_q(j) \quad (\text{resp. } T(j) = \bigcup_{q \geq 0} B_q(j)).$$

**PROPOSITION 3.1.** *Pour  $q \geq 2$  et  $k \geq 1$ , on a les inclusions :*

- (a)  $A_q(j) \subset B_{q-2}(j) \cup B_{q+2}(j)$ ,
- (b)  $A_q(j) \subset A_{kq-k+1}(j) \cup A_{kq+k-1}(j)$ .

*Preuve.* (a) Soit  $\tau$  un élément de  $A_q(j)$  racine du polynôme  $Q$  tel que

$$Q(z) = U(z)T(z) = z^j P(z) - P^*(z),$$

$|P(0)| = q$ ,  $P$  sans racine dans  $|z| \leq 1$ ,  $U = MM_j$  où  $M_j$  est un facteur de  $z^j - 1$  vérifiant  $M_j = -M_j^*$ . Considérons le polynôme  $H = (z^j + 1)P - 2P^*$ . Il vérifie  $H(0) = \pm q - 2$  et  $z^j H + H^* = (z^j + 1)Q$ . En outre pour toute racine  $j$ ième de l'unité  $\alpha$  telle que  $Q(\alpha) = 0$ , on a  $H(\alpha) = 0$ . Soit donc  $M_j R_j$  le plus grand facteur cyclotomique divisant  $H$  tel que  $S_j R_j = z^j - 1$ . Posons  $P_2 = H/M_j R_j$ . Alors  $P_2(0) = -H(0)/R_j(0)$ .

Si  $R_j(0) = 1$  alors  $P_2(0) = -H(0) = -(\pm q - 2)$  et  $z^j P_2 - P_2^* = S_j M T$ .

Si  $R_j(0) = -1$  alors  $P_2(0) = H(0) = \pm q - 2$  et  $z^j P_2 + P_2^* = S_j M T$ .

En appliquant le théorème de Rouché pour  $0 \leq t < 1$  au polynôme  $H_t = 2P^* - t(z^j + 1)P$ , on montre que  $H$  possède  $n$  racines dans  $\{z : |z| < 1\} \cup \{z : z^j = 1\}$ ,  $n$  désignant le degré de  $P$ . Donc  $P_2$  possède  $j$  racines

dans  $|z| > 1$  et aucune racine de module 1. On en déduit alors que  $\tau$  appartient à  $B_{q-2}(j) \cup B_{q+2}(j)$ .

Si  $\tau$  élément de  $A_q(j)$  est racine du polynôme  $Q$  tel que

$$Q(z) = U(z)T(z) = z^j P(z) + P^*(z),$$

on considère le polynôme  $H = (z^j + 1)P + 2P^*$  et l'on raisonne comme précédemment.

(b) La démonstration est semblable à celle de (a) en prenant  $H = (z^j - k)P + (k-1)P^*$  si  $Q = z^j P - P^*$  et  $H = (z^j + k)P + (1-k)P^*$  si  $Q = z^j P + P^*$ .

#### IV. Caractérisation de certains sous-ensembles de $A_q(j)$ et $B_q(j)$ .

Dans ce paragraphe on désignera sous le nom de polynôme cyclotomique un polynôme non nécessairement irréductible dont les racines sont simples et racines de l'unité.

DÉFINITION 4.1. On note  $A_q^*(j)$  (resp.  $B_q^*(j)$ ) le sous-ensemble de  $A_q(j)$  (resp.  $B_q(j)$ ) pour lequel  $U = (z^j - 1)M$  si  $\varepsilon = -1$  et  $U = (z^j - 1)M/(z - 1)$  si  $\varepsilon = 1$ .

On peut alors montrer le théorème suivant.

THÉORÈME 4.1. *Soit  $\tau$  un  $j$ -Salem de polynôme minimal  $T$  ayant un nombre impair de conjugués réels dans  $]-\infty, -1[$  ou dans  $]1, \infty[$  (en changeant au besoin  $z$  en  $-z$  on peut donc toujours se ramener à l'hypothèse  $T(1) < 0$ ). Le  $j$ -Salem  $\tau$  appartient à  $A_q^*(j)$  si et seulement si il existe un polynôme cyclotomique  $K$  premier à  $z^j - 1$  et un polynôme réciproque  $L$  tel que*

(a)  $L(0) = q - 1,$

(b)  $\deg L = \deg KT - j,$

(c)  $L(1) \geq -K(1)T(1),$

(d)  $L$  possède toutes ses racines sur  $|z| = 1$ , simples et séparant les racines de module 1 de  $Q = (z^j - 1)KT$  ou  $Q = (z^j - 1)KT/(z - 1)$ .

Preuve. Par définition  $\tau \in A_q^*(j)$  si et seulement si il existe un polynôme  $P$  ayant tous ses zéros dans  $|z| > 1$  tel que  $|P(0)| = q$ ,  $Q = z^j P - P^* = (z^j - 1)MT$  ou  $Q = z^j P + P^* = (z^j - 1)MT/(z - 1)$ . Faisons la démonstration dans le cas  $j$  pair, celle dans le cas  $j$  impair est tout à fait semblable.

Considérons donc le premier cas,  $Q = z^j P - P^* = (z^j - 1)MT$ . On a alors  $n = \deg MT$  pair. On en déduit que 1 et  $-1$  sont racines de  $Q$ . Comme  $z^j P$  possède exactement  $j$  racines dans  $|z| \leq 1$ , ces racines sont les débuts de branches finissant en les  $j$  racines de module strictement inférieur à 1 de  $Q$ . Par suite, toutes les racines de module 1 de  $Q$  (qui sont par ailleurs simples d'après la proposition 2.2) sont des entrées. En particulier, 1 étant une entrée, on a d'après le lemme 1.1,  $-P(1)Q'(1) > 0$ . Or  $Q'(1) =$



$jM(1)T(1) < 0$  d'après l'hypothèse. Par suite,  $P(1) > 0$ , ce qui implique  $P(0) = q$  car  $P$  est sans racine dans  $|z| \leq 1$ . Prenons alors  $K = M$  et posons  $L = P - KT$ . On a  $L(0) = q - 1$ , c'est-à-dire (a).

La relation  $z^j L - z^n L(z^{-1}) = 0$  prouve que  $L$  est réciproque et que  $\deg L = \deg KT - j = n - j$ ; c'est la condition (b).

La relation  $L(1) = P(1) - K(1)T(1)$  entraîne, puisque  $P(1)$  est positif,  $L(1) > -K(1)T(1)$ ; c'est la condition (c).

Soit  $\alpha$  une racine simple de module 1 de  $\mathbb{Q}$ ,  $\alpha \neq \pm 1$ . D'après le raisonnement précédent,  $\alpha$  est une entrée et d'après le lemme 1.1,

$$(1) \quad \alpha^{1-n} P(\alpha) Q'(\alpha) < 0.$$

Comme  $L(\alpha) = P(\alpha) - K(\alpha)T(\alpha)$ , on en déduit

$$(2) \quad \alpha^{1-n} L(\alpha) Q'(\alpha) + \alpha^{1-n} K(\alpha) T(\alpha) Q'(\alpha) < 0.$$

Comme  $L$  est un polynôme de degré  $n - j$  pair on peut écrire

$$L = z^{(n-j)/2} B(z + z^{-1}) \quad \text{et} \quad Q = (z^2 - 1) z^{(n+j-2)/2} A(z + z^{-1}).$$

D'où

$$LQ = (z^2 - 1) z^n B(z + z^{-1}) A(z + z^{-1}).$$

De l'égalité  $Q = (z^j - 1)KT$  on déduit

$$(3) \quad Q'(\alpha) = j\alpha^{j-1} K(\alpha)T(\alpha) + (\alpha^j - 1)(KT)'(\alpha).$$

Si  $\alpha$  est une racine  $j$ ième de l'unité, (3) devient  $Q'(\alpha) = j\alpha^{j-1} K(\alpha)T(\alpha)$  et en reportant dans (2), on obtient

$$(4) \quad \alpha^{1-n} L(\alpha) Q'(\alpha) + (Q'(\alpha))^2 / (j\alpha^{n+j-2}) < 0.$$

En reportant dans (4) les relations

$$L(\alpha) Q'(\alpha) = (\alpha - \alpha^{-1})^2 \alpha^{n-1} B(\alpha + \alpha^{-1}) A'(\alpha + \alpha^{-1})$$

et

$$(Q'(\alpha))^2 / (j\alpha^{n+j-2}) = (\alpha - \alpha^{-1})^4 (A'(\alpha + \alpha^{-1}))^2 / j,$$

on obtient alors si  $\alpha = e^{i\varphi}$ ,

$$(5) \quad 4 \sin^2 \varphi B(\alpha + \alpha^{-1}) A'(\alpha + \alpha^{-1}) > 0.$$

Si  $\alpha$  n'est pas racine  $j$ ième de l'unité alors  $K(\alpha)T(\alpha) = 0$ , d'où  $L(\alpha) = P(\alpha)$  et l'on obtient encore l'inégalité (5). Enfin, comme  $\varphi \neq 0$  et  $\varphi \neq \pi$ , il vient

$$(6) \quad B(\alpha + \alpha^{-1}) A'(\alpha + \alpha^{-1}) > 0.$$

Désignons par  $\alpha_k = e^{i\varphi_k}$  (resp.  $\beta_k = e^{i\psi_k}$ ) les racines de  $(z^j - 1)KT$  (resp.  $L$ ) de module 1 et de partie imaginaire positive ou nulle, rangées par argument croissant,  $0 \leq k \leq (n - j)/2$ . Posons  $\varrho_k = \alpha_k + \alpha_k^{-1}$ .

Comme  $Q$  possède un nombre impair de racines réelles dans  $]1, \infty[$ , on a  $\text{sgn } A'(\varrho_k) = (-1)^k$  et d'après (6),  $(-1)^k B(\varrho_k) > 0$ ,  $1 \leq k \leq (n - j)/2 - 1$ .

Les conditions  $P(1) > 0$ ,  $T(1) < 0$  entraînent  $B(\varrho_0) > 0$ . Les conditions  $P(-1) > 0$  (car  $P$  est sans racine dans  $|z| \leq 1$  et  $P(1) > 0$ ),  $Q'(-1) > 0$  (car  $P(-1)Q'(-1) > 0$  puisque  $-1$  est une entrée) et  $P(-1) = (-1)^{(n-j)/2}B(-2) + Q'(-1)/j(-1)^{j-1}$  entraînent, comme  $j$  est pair,  $(-1)^{(n-j)/2}B(-2) > 0$ . Par suite,  $(-1)^k B(\varrho_k) > 0$  pour  $0 \leq k \leq (n-j)/2$  et  $B$  possède  $(n-j)/2$  racines dans  $] -2, 2[$ , notées  $2 \cos \psi_1, \dots, 2 \cos \psi_{(n-j)/2}$ , telles que

$$0 < \psi_1 < \varphi_1 < \dots < \varphi_{(n-j)/2-1} < \psi_{(n-j)/2} < \pi.$$

On en déduit (d).

Le cas  $Q = (z^{j-1} + \dots + 1)MT = z^j P + P^*$  se traite de façon analogue en remarquant que  $Q(1) = 2P(1) < 0$  entraîne  $P(0) = -q$ .

Réciproquement, supposons que les polynômes  $K$  et  $L$  satisfassent les conditions (a), (b), (c) et (d).

S'il y a égalité en (c) posons  $Q = (z^{j-1} + \dots + 1)KT$  et définissons  $P$  par la relation  $L = (z-1)P - KT$ . Sinon posons  $Q = (z^j - 1)KT$  et définissons  $P$  par la relation  $L = P - KT$ . L'égalité correspond donc à  $P(0) = -q$  et  $Q = (z^{j-1} + \dots + 1)KT = z^j P + P^*$  tandis que l'inégalité stricte correspond à  $P(0) = q$  et  $Q = (z^j - 1)KT = z^j P - P^*$ .

La propriété (d) se traduit dans tous les cas par  $\varepsilon \alpha^{1-n} P(\alpha) Q'(\alpha) > 0$ ,  $\varepsilon = \pm 1$ , d'où l'on déduit grâce au lemme 1.1 que toutes les racines de module 1 de  $Q$  sont des entrées; ceci entraîne grâce au théorème 2.2 que  $P$  a toutes ses racines dans  $|z| > 1$ .

**THÉORÈME 4.2.** *Soit  $\tau$  un  $j$ -Salem de polynôme minimal  $T$  ayant un nombre pair de conjugués de module supérieur à 1 vérifiant  $T(1) > 0$  et  $T(-1) > 0$ . Alors  $\tau$  appartient à  $A_q^*(j)$  si et seulement si il existe un polynôme cyclotomique  $K$  premier à  $z^j - 1$  et un polynôme réciproque  $L$  tel que*

- (a)  $L(0) = -q - 1$ ,
- (b)  $\deg L = \deg KT - j$ ,
- (c)  $L(1) \leq -K(1)T(1)$ ,

(d) *les racines de  $L$  sont simples et de module 1 et séparent les racines de module 1 de  $Q = (z^j - 1)KT$  ou de  $Q = (z^j - 1)KT/(z - 1)$ .*

La preuve est analogue à celle du théorème 4.1, en remarquant que les hypothèses entraînent  $j$  pair.

**THÉORÈME 4.3.** *Soit  $\tau$  un  $j$ -Salem de polynôme minimal  $T$  vérifiant  $T(1) > 0$  et  $T(-1) > 0$ . Alors  $\tau$  appartient à  $B_q^*(j)$  si et seulement si il existe un polynôme cyclotomique  $K$  premier à  $z^j - 1$  et un polynôme réciproque  $L$  tel que*

- (a) ou bien  $L(0) = q + 1$  ou bien  $L(0) = 1 - q$ ,
- (b)  $\deg L = \deg KT - j$ ,
- (c)  $L(1) = K(1)T(1)$ ,
- (d)(i) ou bien  $L$  a ses racines comme dans le théorème 4.2,  
 (ii) ou bien  $L$  possède une unique racine dans  $|z| > 1$  et ses autres racines de module 1 sont simples et séparent les racines de module 1 de  $Q = (z^{j-1} + \dots + 1)KT$ .

La démonstration est analogue à celle des théorèmes 4.1 et 4.2, utilise toutefois la proposition 2.1 et le théorème 2.1.

Remarque. S'il existe un polynôme cyclotomique  $L$  de degré égal à  $\deg KT - j$  vérifiant  $L(1) \leq K(1)T(1)$  si  $T(-1) > 0$  et  $T(1) > 0$  ou  $L(1) \geq K(1)T(1)$  si  $T(1) < 0$ , dont les zéros séparent ceux de  $(z^j - 1)KT$  alors on peut montrer que  $\tau \in B_0^*(j)$ .

En utilisant les théorèmes et la remarque précédente on vérifie facilement en exhibant un couple de polynômes cyclotomiques  $K$  et  $L$  que presque tous les polynômes réciproques de petite mesure de degré inférieur à 12 donnés par Boyd [6] appartiennent à  $A_2^*(j)$  ou  $B_0^*(j)$ .

### Bibliographie

- [1] M. J. Bertin, *Familles fermées de nombres algébriques*, Acta Arith. 39 (1981), 207–240.
- [2] M. J. Bertin et D. W. Boyd, *Une caractérisation de certaines classes de nombres de Salem*, C. R. Acad. Sci. Paris Sér. I 303 (1986), 837–839.
- [3] —, —, *A characterization of two related classes of Salem numbers*, J. Number Theory, à paraître.
- [4] M. J. Bertin et M. Pathiaux, *Conjecture de Lehmer et petits nombres de Salem*, Queen's Papers in Pure and Appl. Math. 81 (1989).
- [5] D. W. Boyd, *Small Salem numbers*, Duke Math. J. 44 (1977), 315–328.
- [6] —, *Reciprocal polynomials having small measure*, Math. Comp. 35 (1980), 1361–1377.
- [7] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. 34 (1933), 461–479.
- [8] R. Salem, *Power series with integral coefficients*, Duke Math. J. 12 (1945), 135–172.
- [9] —, *Algebraic Number and Fourier Analysis*, Heath and Co., Boston, 1963.
- [10] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. 3 (1971), 169–175.

DÉPARTEMENT DE MATHÉMATIQUE  
 ÉCOLE NORMALE SUPÉRIEURE DE JIJEL  
 BP 98, OULED AISSA 18000, ALGÉRIE

Reçu le 6.12.1993

(2536)