ANNALES DE L'INSTITUT FOURIER

ALINE BONAMI

# Ensembles $\Lambda(p)$ dans le dual de $D^\infty$

*Annales de l'institut Fourier*, tome 18, nº 2 (1968), p. 193-204

<http://www.numdam.org/item?id=AIF_1968__18_2_193_0>

Ann. Inst. Fourier, Grenoble
**18**, 2 (1968), 193-204.

# ENSEMBLES $\Lambda(p)$ DANS LE DUAL DE $D^\infty$

**par Aline BONAMI**

---

$D^\infty$ est le groupe $\{-1,1\}^N$ muni de la topologie compacte produit des topologies discrètes sur $\{-1,1\}$. Le dual de $D^\infty$, que nous appellerons $\Gamma$, est isomorphe à la somme directe $\Sigma \mathbf{Z}_2$ munie de la topologie discrète. $\Gamma$ est un espace vectoriel sur le corps $\mathbf{Z}_2$, sa structure de groupe en tant qu'espace vectoriel étant celle dont il est muni en tant que dual de $D^\infty$. On notera par $e_1, e_2, \ldots, e_n, \ldots$ la base canonique de $\Gamma$, formée des éléments dont toutes les coordonnées sont nulles sauf une. Si $x_n$ est la n-ième coordonnée de $x$ dans $D^\infty$, $(x, e_n) = x_n$.

Suivant Rudin [1], E étant un ensemble dans $\Gamma$, une fonction $f$ de $L^1(D^\infty)$ est appelée E-fonction si $\hat{f}(\gamma) = 0$ pour tout $\gamma$ n'appartenant pas à E. Si $f$ est en même temps un polynôme trigonométrique, $f$ est appelée E-polynôme. Soit $p$ un nombre réel positif. On dit que E est un ensemble $\Lambda(p)$ s'il existe un nombre $p'$, $0 < p' < p$, et une constante $B_{p'}$ tels que pour tout E-polynôme $\|f\|_p \leqslant B_{p'} \|f\|_{p'}$. On peut alors à tout $q$ inférieur à $p$ faire correspondre $B_q$ tel que pour tout E-polynôme $\|f\|_p \leqslant B_q \|f\|_q$. En particulier si $p > 2$ on appellera $A(p, E)$ la plus petite constante B telle que $\|f\|_p \leqslant B\|f\|_2$ pour tout E-polynôme.

Cette étude, dont je dois le sujet à M. Yves Meyer que je tiens à remercier ici, a pour but d'adapter aux ensembles $\Lambda(p)$ dans $\Gamma$ certains des résultats de Rudin [1] sur les ensembles $\Lambda(p)$ dans $\mathbf{Z}$.

On trouve (théorèmes 1 et 2) des conditions nécessaires pour qu'un ensemble soit $\Lambda(p)$ analogues à celles de Rudin : les progressions arithmétiques dans $\mathbf{Z}$ sont remplacées par les sous-espaces vectoriels de $\Gamma$. Par contre nous ne savons pas si ces conditions nécessaires sont les meilleures possibles, et, si c'était le cas, si elles sont suffisantes ou non. La condition suffisante de Rudin pour qu'un ensemble soit $\Lambda(2s)$, $s$ étant un entier supérieur à 1, se transcrit également dans le cas de $\Gamma$ (théorème 6). Si la construction de Rudin d'un ensemble $\Lambda(2s)$ qui ne soit pas $\Lambda(2s+\varepsilon)$ n'a pas pu être adaptée dans $\Gamma$ (elle paraît trop attachée à des propriétés arithmétiques), par contre la structure algébrique de $\Gamma$ a permis de construire facilement des ensembles $\Lambda(p)$ pour tout $p$ tels que la fonction $A(p, E)$ soit arbitrairement croissante, ce qui dans le cas de $\mathbf{Z}$ nécessite une construction délicate reposant sur un résultat de Erdös. Les théorèmes 3 et 4 fournissent d'autres exemples d'ensembles $\Lambda(p)$ pout tout $p$, qui ne relèvent pas du théorème 6. Le théorème 4 en particulier permet d'affirmer le résultat précis suivant : quelle que soit la forme quadratique $Q(x) = \Sigma a_{mn}(x, e_m)(x, e_n)$ telle que $\Sigma|a_{mn}|^2$ soit fini, et quel que soit le réel positif $\lambda$, exp $(\lambda|Q|)$ appartient à $L^1$.

Toute cette étude pose le problème d'une caractérisation des ensembles $\Lambda(p)$ de $\Gamma$ par des propriétés algébriques, caractérisation qui existe dans le cas des ensembles de Sidon [3].

## 1. Conditions nécessaires pour qu'un ensemble soit $\Lambda(p)$.

Théorème 1. — *Soit* E *un ensemble* $\Lambda(p)$, $p > 2$, *tel que pour tout* E-*polynôme* $\|f\|_p \leqslant B\|f\|_2$ ; *quel que soit le sous-espace vectoriel* V *de dimension finie dans* $\Gamma$, *on a alors :*

$$\text{card}\,(E \cap V) \leqslant B^2 2^{2/p \dim V}.$$

Démontrons-le tout d'abord dans le cas particulier où V est engendré par des éléments de la base canonique : $V = \left\{\sum_{i=1}^{k} \varepsilon_i e_{n_i} | \varepsilon_i \in \{0,1\}\right\}$. On considère le produit de Riesz $P_k(x) = \prod_{i=1}^{k}(1 + (x, e_{n_i})) = \sum_{\gamma\in V}(x, \gamma)$. La mesure de Haar sur $D^\infty$ étant la mesure produit des mesures de Haar sur $\{-1,1\}$, $\int |P_k(x)|^p\,dx = \int (P_k(x))^p\,dx = \prod_{i=1}^{k}\int(1 + (x, e_{n_i}))^p\,dx$. Comme $\int(1 + (x, e_{n_i}))^p\,dx = 2^{p-1}$, $\|P_k\|_p = 2^{k(1-1/p)}$.

Posons $f(x) = \sum\limits_{\gamma \in V \cap E} (x, \gamma)$; on a $\|f\|_2^2 = \text{card}(E \cap V)$ et $\|f\|_2^2 = \int f P_k\, dx \leqslant \|f\|_p \|P\|_{p'} \left(\frac{1}{p} + \frac{1}{p'} = 1\right)$. Mais par hypothèse $\|f\|_p \leqslant B\|f\|_2$. Donc

$$\text{card}(E \cap V) \leqslant B[\text{card}(E \cap V)]^{1/2}\, 2^{k/p},$$

d'où l'on déduit le résultat dans ce cas particulier.

Le résultat dans le cas général s'appuie sur le lemme suivant :

Lemme 1. — *Soit* $\alpha$ *un automorphisme de* $\Gamma$. *L'application* T *définie par* $\widehat{Tf}(\gamma) = \hat{f}(\alpha(\gamma))$ *est une isométrie de* $L^p(D^\infty)$ *pour tout* $p$.

On montre en effet (voir Rudin [2], p. 79) que $Tf(x) = f[\beta^{-1}(x)]$, où $\beta$ est un isomorphisme bicontinu de $D^\infty$ dans lui-même, défini par $(\beta(x), \gamma) = (x, \alpha(\gamma))$ pour tout $\gamma$.

Soit alors V un sous-espace vectoriel quelconque de $\Gamma$. On prend pour $\alpha$ une des applications linéaires bijectives de $\Gamma$ dans lui-même qui envoie une base de V sur une partie de la base canonique de $\Gamma$ : V est alors envoyé sur un sous-espace vectoriel $V'$ engendré par des éléments de la base canonique, E sur un sous-ensemble $E'$ de $\Gamma$. T et $T^{-1}$ faisant se correspondre les E-fonctions et les $E'$-fonctions avec conservation des normes, $E'$ est un ensemble $\Lambda(p)$ avec même constante $A(p, E)$, et $\text{card}(E' \cap V') \leqslant B^2 2^{2/p \dim V'}$. Comme $\text{card}(E' \cap V') = \text{card}(E \cap V)$, $\dim V' = \dim V$, $\text{card}(E \cap V) \leqslant B^2 2^{2/p \dim V}$.

Théorème 2. — *Soit* E *un ensemble* $\Lambda(p)$, $p > 0$ : E *ne contient pas de sous-espace vectoriel de dimension arbitrairement grande.*

(Si $p > 2$ c'est un corollaire du théorème 1).

Nous ne le montrerons que pour les sous-espaces vectoriels engendrés par des éléments de la base, le résultat général s'en déduisant encore grâce au lemme 1.

On considère à nouveau les produits de Riesz $P_k$; si le sous-espace vectoriel V de dimension $k$ est contenu dans E : $\|P_k\|_p \leqslant B_{p'} \|P_k\|_{p'}$ si $p' < p$, c'est-à-dire $2^{k(1-1/p)} \leqslant B_{p'} 2^{k(1-1/p')}$, $k \leqslant \frac{pp'}{p - p'} \log_2 B_{p'}$.

## 2. Constructions d'ensembles $\Lambda(p)$.

On sait qu'un ensemble indépendant (c'est-à-dire linéairement indépendant sur $\mathbf{Z}_2$) dans $\Gamma$ est un ensemble de Sidon [3]. On peut alors se poser la question : si E et F sont indépendants $E + F$ est-il $\Lambda(p)$ pour tout $p$? Le théorème 3 montre qu'il en est ainsi si $F = E + \cdots + E$, le théorème 5 donne un exemple de deux ensembles E, F indépendants tels que $E + F$ ne soit $\Lambda(p)$ pour aucun $p$.

On appellera $k\mathrm{E}$ l'ensemble $E + \cdots + E$ où E a été pris $k$ fois.

THÉORÈME 3. — *Soit* E *un ensemble indépendant dans* $\Gamma$ : *l'ensemble* $k\mathrm{E}$ *est un ensemble* $\Lambda(p)$ *pour tout* $p$.

Il suffit de le montrer dans le cas où E est la base canonique $(e_n)$. Sinon on utilise le lemme 1 en prenant pour $\alpha$ l'une des applications linéaires bijectives de $\Gamma$ dans lui-même qui envoie E sur une partie de $(e_n)$; $\alpha(k\mathrm{E})$ étant contenu dans $k(e_n)$, si ce dernier ensemble est $\Lambda(p)$ pout tout $p$ il en est de même de $k\mathrm{E}$.

D'autre part, une réunion finie d'ensembles $\Lambda(p)$ étant $\Lambda(p)$ (si $p > 2$) (voir [1]) il suffit même de montrer que l'ensemble $\mathrm{F}_k$ des éléments qui peuvent s'écrire comme somme de $k$ éléments distincts de la base canonique est $\Lambda(p)$ pour tout $p$.

$$\mathrm{F}_k = \{e_{n_1} + e_{n_2} + \cdots + e_{n_k} | n_1 < n_2 < \cdots < n_k\}.$$

Un $\mathrm{F}_k$-polynôme peut s'écrire

$$f(x) = \sum_{n_1 < n_2 \cdots < n_k} a_{n_1 \ldots n_k}(e_{n_1} + e_{n_2} + \cdots + e_{n_k}, x).$$

On peut, pour cette démonstration, utiliser le théorème suivant dû à Paley [4] : si $f$ est une fonction de $L^p(D^\infty)$, $p > 1$, et si $f_n$ a été défini par $\hat{f}_n(\gamma) = \hat{f}(\gamma)\chi_n(\gamma + e_n)$, où $\chi_n$ est la fonction caractéristique du sous-espace vectoriel engendré par $e_1, e_2, \ldots, e_{n-1}$, alors :

$$\|f\|_p \leqslant C_p \|(\Sigma |f_n|^2)^{1/2}\|_p.$$

On en déduit, en appliquant à $\Sigma|f_n|^2$ l'inégalité de Minkowski généralisée pour l'exposant $\frac{p}{2}$, le corollaire suivant : $\|f\|_p \leqslant C_p(\Sigma\|f_n\|_p^2)^{1/2}$. On démontre alors facilement le théorème par récurrence en appliquant ce résultat au $F_k$-polynôme considéré. On obtient finalement

$$\|f\|_p \leqslant (C_p)^k\|f\|_2.$$

Mais cette démonstration donne une très mauvaise majoration de la constante $A(p, F_k)$, la constante $C_p$ du théorème de Paley croissant plus vite que $2^p$ avec $p$. Il vaut mieux, pour obtenir une bonne majoration, faire une démonstration combinatoire qui permet d'énoncer le théorème suivant :

THÉORÈME 4. — *Il existe une constante* $B_k$ *dépendant de* $k$ *seulement telle que pour tout* $F_k$*-polynôme* $f$, *et pour tout* $p > 2$ : $\|f\|_p \leqslant B_k p^{k/2}\|f\|_2$. *Si* $p$ *est un entier pair on peut prendre* $B_k = 1$.

On fera la démonstration dans le cas où $k = 2$.

Il suffit de considérer le cas où $p$ est un entier pair, et $f$ un $F_2$-polynôme réel, qu'on peut écrire sous la forme :

$$f(x) = \sum_{m,\, n} a_{mn}(x,\ e_m + e_n), \qquad \text{avec} \qquad a_{mn} = a_{nm} \qquad \text{et} \qquad a_{nn} = 0.$$

Alors

$$f^p(x) = \sum_{(n_1,\, n_2,\, \ldots,\, n_{2p}) \in \mathrm{N}^{2p}} a_{n_1n_2}a_{n_3n_4} \ldots a_{n_{2p-1}n_{2p}}(x,\ e_{n_1} + e_{n_2} \ldots + e_{n_{2p}}).$$

Comme $\int(x, \gamma)dx = 0$ si $\gamma$ n'est pas nul,

$$\int f^p\, dx = \Sigma\, a_{n_1n_2}a_{n_3n_4} \ldots a_{n_{2p-1}n_{2p}},$$

la sommation étant prise sur le sous-ensemble de $\mathrm{N}^{2p}$ formé des suites $(n_1, \ldots, n_{2p})$ telles que les $n_i$ soient deux à deux égaux. Appelons W ce sous-ensemble.

On établit tout d'abord le lemme suivant :

LEMME 2. — *Soit* $E_p$ *l'ensemble des applications* $\alpha$ *de* $\{1, 2, \ldots, 2p\}$ *dans* $\{1, 2, \ldots, p\}$ *telles que* card $\alpha^{-1}(k) = 2$ *pour* $k=1, 2, \ldots$, p. *Pour tout* $F_2$*-polynôme* $f(x)=\Sigma a_{mn}(x, e_m+e_n)$

*et pour tout entier* $p$ :

$$(1) \quad \left|\int f^p\, dx\right| \leqslant \frac{1}{p\,!} \sum_{\substack{(r_1, r_2, \ldots, r_p) \in \mathrm{N}^p \\ \alpha \in \mathrm{E}_p}} |a_{r_{\alpha(1)} r_{\alpha(2)}} \cdots a_{r_{\alpha(2p-1)} r_{\alpha(2p)}}|.$$

Considérons en effet l'application $\varphi$ de $\mathrm{N}^p \times \mathrm{E}^p$ dans W, définie par : $\varphi[(r_1, r_2, \ldots, r_p), \alpha] = (r_{\alpha(1)}, r_{\alpha(2)}, \ldots, r_{\alpha(2p)})$.

Cette application est surjective. Choisissant

$$\nu = (n_1, n_2, \ldots, n_{2p})$$

dans W, calculons card $\varphi^{-1}(\nu)$ en supposant que les $n_i$ prennent $k$ valeurs distinctes $s_1, s_2, \ldots, s_k$, chacune un nombre de fois respectivement égal à $2\beta_1, 2\beta_2, \ldots, 2\beta_k$. La projection sur $\mathrm{N}^p$ de $\varphi^{-1}(\nu)$ est alors formée des suites $(r_1, r_2, \ldots, r_p)$ telles que les $r_i$ prennent les valeurs $s_1, s_2, \ldots, s_k$, chacune un nombre de fois respectivement égal à $\beta_1, \beta_2, \ldots \beta_k$. Le nombre de ces suites est $\dfrac{p\,!}{\beta_1\,!\ \beta_2\,!\ \ldots\ \beta_k\,!}$.

Ayant choisi une telle suite $(r_1, \ldots, r_p)$, il nous reste à compter le nombre des applications $\alpha \in \mathrm{E}_p$ telles que, pour tout $i$, $r_{\alpha(i)} = n_i$. Soit $\mathrm{N}_i$ l'ensemble $\{j\,;\ n_j = s_i\}$, $\mathrm{R}_i$ l'ensemble $\{l;\ r_l = s_i\}$ : les applications cherchées sont toutes les applications $\alpha \in \mathrm{E}_p$ telles que pour tout $i = 1, 2, \ldots, k$ $\alpha(\mathrm{N}_i) = \mathrm{R}_i$. Leur nombre est égal à

$$\text{card } \mathrm{E}_{\beta_1} \times \text{card } \mathrm{E}_{\beta_2} \times \cdots \times \text{card } \mathrm{E}_{\beta_k}.$$

On voit facilement que card $\mathrm{E}_\beta = 2^{-\beta}.(2\beta)\,!$. Finalement :

$$\text{card } \varphi^{-1}(\nu) = p\,! \frac{(2\beta_1)\,!}{2^{\beta_1}.\beta_1\,!} \cdots \frac{(2\beta_k)\,!}{2^{\beta_k}.\beta_k\,!}.$$

Par conséquent, quel que soit $\nu$, card $\varphi^{-1}(\nu) \geqslant p\,!$. Le lemme 2 s'en déduit aisément.

Effectuons la sommation du second membre de l'inégalité (1) d'abord par rapport à $r_1, \ldots, r_p$, $\alpha$ étant fixé, et posons :

$$\mathrm{S}_p(\alpha) = \sum_{(r_1, \ldots, r_p) \in \mathrm{N}^p} |a_{r_{\alpha(1)} r_{\alpha(2)}} \cdots a_{r_{\alpha(2p-1)} r_{\alpha(2p)}}|.$$

Nous allons montrer l'inégalité :

$$(2) \qquad \mathrm{S}_p(\alpha) \leqslant \Big(\sum_{m,\,n} |a_{mn}|^2\Big)^{p/2}$$

par récurrence sur $p$ : si $p = 2$ il est facile de voir que (2) est vérifiée pour tout $\alpha \in E_2$. Supposons donc qu'elle est vérifiée pour tout $p' < p$ et $\alpha \in E_{p'}$. Deux cas peuvent se présenter :

*Premier cas.* — $\alpha$ satisfait à l'hypothèse suivante : il existe une partition de $\{1, 2, \ldots, 2p\}$ en $N_1 \cup N_2$ telle que pour tout $i$, $2i$ appartienne à $N_1$ si et seulement si $2i$-1 lui appartient, et telle que $\alpha(N_1)$ et $\alpha(N_2)$ soient disjoints. Supposant que $N_1$ possède $2k$ éléments, on peut écrire $S_p(\alpha)$ sous la forme

$$S_p(\alpha) = \Big(\sum_{(r_1, \ldots, r_k)} |a_{r_{\alpha'(1)}r_{\alpha'(2)}} \cdots a_{r_{\alpha'(2k-1)}r_{\alpha'(2k)}}|\Big) \Big(\sum_{(r_1, \ldots, r_{p-k})} |a_{r_{\alpha''(1)}r_{\alpha''(2)}} \cdots a_{r_{\alpha''(2p-2k-1)}r_{\alpha''(2p-2k)}}|\Big)$$

où $\alpha'$ et $\alpha''$ sont des applications de $E_k$ et $E_{p-k}$ respectivement, induites par $\alpha$. Ainsi $S_p(\alpha) = S_k(\alpha')S_{p-k}(\alpha'')$, $S_p(\alpha)$ vérifie donc (2) grâce à l'hypothèse de récurrence.

*Deuxième cas.* — $\alpha$ ne satisfait pas à l'hypothèse précédente : il existe alors une permutation $\beta$ de $\{1, 2, \ldots, p\}$ telle que pour tout $(r_1, \ldots, r_p)$ :

$$(3) \quad a_{r_{\alpha(1)}r_{\alpha(2)}} \cdots a_{r_{\alpha(2p-1)}r_{\alpha(2p)}} = a_{r_{\beta(1)}r_{\beta(2)}}a_{r_{\beta(3)}r_{\beta(4)}} \cdots a_{r_{\beta(p-1)}r_{\beta(p)}}a_{r_{\beta(p)}r_{\beta(1)}}.$$

La permutation $\beta$ est obtenue de la manière suivante : on définit $\beta(1) = 1$. Il existe deux facteurs dans le premier membre de (3) qui dépendent de la variable $r_1$ : appelons-les $a_{r_1 r_i}$ et $a_{r_1 r_j}$ : on définit $\beta(2) = i$, $\beta(p) = j$. Ayant défini $\beta(1), \ldots, \beta(k-1)$, on définit $\beta(k)$ par : $\beta(k)$ est différent de $\beta(k-2)$ et le premier membre de (3) contient le facteur $a_{r_{\beta(k-1)}r_{\beta(k)}}$. D'après l'hypothèse, quel que soit $i < k, \beta(i) \neq \beta(k)$. Donc

$$S_p(\alpha) = \sum_{(r_1, r_2, \ldots, r_p)} |a_{r_1 r_2}a_{r_2 r_3} \cdots a_{r_{p-1}r_p}a_{r_p r_1}|.$$

On obtient facilement l'inégalité (2) en sommant successivement par rapport à $r_1, r_2, \ldots, r_p$ et en utilisant l'inégalité de Schwarz à chaque étape. Finalement, grâce à (1) et (2) :

$$\int f^p \, dx \leqslant \frac{1}{p!} \operatorname{card} E_p \Big(\sum_{m, n} |a_{mn}|^2\Big)^{p/2}.$$

Or
$$\sum_{m,n} |a_{mn}|^2 = 2 \sum_{m<n} |a_{mn}|^2 = \frac{1}{2} \|f\|_2^2.$$

Donc :
$$\|f\|_p^p \leqslant \frac{(2p)!}{p!\, 2^p} \cdot 2^{-p/2} \|f\|_2^p.$$

Si $p$ est un entier pair, $p = 2q$, $\dfrac{(2p)!}{p!\, 2^p} \cdot 2^{-p/2} \leqslant (2q)!\, 2^{-q} \leqslant (2q)^q$.

$$\|f\|_{2q} \leqslant 2q \|f\|_2.$$

Cette démonstration s'applique sans grande modification au cas où $k$ est plus grand que 2 : se limitant encore au cas où $p$ est un entier pair, $p = 2q$, on considère, comme au lemme 2, les applications de $E_{kq}$, et on se ramène à une sommation par rapport à $kq$ variables $r_1, r_2, \ldots, r_{kq}$. On obtient finalement que pour tout $F_k$-polynôme :

$$\|f\|_{2q} \leqslant (2q)^{k/2} \|f\|_2.$$

Ceci achève la démonstration du théorème 4.

*Remarque.* — Le théorème 1 permet de montrer l'existence d'une constante $C_k$ telle que $A(p, F_k) \geqslant C_k p^{k/2}$ : on prend pour sous-espace vectoriel $V$ le sous-espace vectoriel engendré par $e_1, e_2, \ldots, e_n$. Pour tout $p$ :

$$C_n^k = \operatorname{card}(V \cap F_k) \leqslant [A(p, F_k)]^2 2^{2n/p}.$$

Prenant $p = n$, on obtient :

$$A(p, F_k) \geqslant \left(\frac{p(p-1)\ldots(p-k+1)}{4k!}\right)^{1/2} \geqslant C_k p^{k/2}.$$

Le théorème 4 donne donc, à une constante près, la meilleure majoration possible pour $A(p, F_k)$.

Le théorème 4 admet le corollaire suivant, dont la démonstration est analogue à celle de [5] (page 214) correspondant au cas $k = 1$ :

Corollaire. — *Soit $f$ une $F_k$-fonction appartenant à $L^2(D^\infty)$. Alors, quel que soit $\lambda > 0$, $\exp(\lambda |f|^{2/k})$ appartient à $L^1$.*

Théorème 5. — *Il existe un ensemble indépendant $E$ tel que, quel que soit $p$, $E + \{e_1, e_2, \ldots, e_n, \ldots\}$ ne soit pas $\Lambda(p)$.*

On cherche un ensemble E tel que $\mathrm{E} + \{e_1, e_2, \ldots\}$ contienne des sous-espaces vectoriels de dimension arbitrairement grande. Considérons le sous-espace vectoriel engendré par $e_1, e_2, \ldots, e_k$. Il contient $2^k$ éléments qu'on peut ranger dans un certain ordre. On appellera $f_{k,n}$ ces éléments, où $0 \leqslant n \leqslant 2^k - 1$. Le problème sera résolu si on peut trouver une suite $p(k)$ telle que l'ensemble $\mathrm{E} = \{e_{p(k)+n} + f_{k,n}\}_{0 \leqslant n \leqslant 2^k-1}$ soit indépendant, car alors $\mathrm{E} + \{e_1, e_2, \ldots\}$ contiendra des sous-espaces vectoriels $\{f_{k,n}\}$ de dimension arbitraire. Pour que E soit indépendant il suffit que E soit formé d'éléments dont l'indice de la première coordonnée non nulle est strictement croissant, ce qui est réalisé si $p(k) = 2^k$.

On cherche maintenant une condition analogue à la condition suffisante de Rudin dans le cas d'un ensemble d'entiers positifs, condition qui fait intervenir le nombre de décompositions possibles d'un entier quelconque en somme d'entiers de l'ensemble considéré.

Par analogie appelons $r_s(\mathrm{E}, \gamma)$ le nombre de décompositions de $\gamma$ en somme d'au plus $s$ éléments distincts de E.

Théorème 6. — *S'il existe un entier* N *tel que, quel que soit* $\gamma$, $r_s(\mathrm{E}, \gamma)$ *soit majoré par* N, *l'ensemble* E est $\Lambda(2s)$.

Soit $f$ un E-polynôme : $f(x) = \sum_{\gamma \in \mathrm{E}} a(\gamma)(x, \gamma)$

$$f^s(x) = \sum_{\gamma_i \in \mathrm{E}} a(\gamma_1) \ldots a(\gamma_s)(x, \gamma_1 + \gamma_2 + \cdots + \gamma_s),$$

ou encore $f^s(x) = \Sigma b(\gamma)(x, \gamma)$, où $b(\gamma) = 0$ si $\gamma$ ne peut pas s'écrire comme somme de $s$ éléments de E et sinon

$$b(\gamma) = \sum_{\gamma_1+\gamma_2+\cdots+\gamma_s=\gamma} a(\gamma_1)a(\gamma_2) \ldots a(\gamma_s).$$

Puisque $r_s(\mathrm{E}, \gamma) \leqslant \mathrm{N}$, il existe au plus N décompositions de $\gamma$ en somme de $s, s-2, \ldots, s-2p, \ldots$ éléments distincts de E. Soit $\gamma = \gamma_{i_1} + \cdots + \gamma_{i_{s-2p}}$ une telle décomposition de $\gamma$ : c'est dire que quels que soient $\delta_1, \delta_2, \ldots, \delta_p$ dans E, $\gamma = \gamma_{i_1} + \cdots + \gamma_{i_{s-2p}} + \delta_1 + \delta_1 + \cdots + \delta_p + \delta_p$. Faisant la somme des termes de $b(\gamma)$ correspondant à ces décompositions on obtient :

$$s(s-1) \ldots (2p+1)\, a(\gamma_{i_1}) \ldots a(\gamma_{i_{s-2p}}) \sum_{\delta_i \in \mathrm{E}} [a(\delta_1)]^2 \ldots [a(\delta_p)]^2,$$

$s(s-1)\dots(2p+1)$ étant le nombre de manières de choisir $a(\gamma_{i_1})\dots a(\gamma_{i_{s-2p}})$ parmi les différents facteurs de $f^s$.

On reconnaît dans $\sum_{\delta_i \in E} |a(\delta_1)|^2 \dots |a(\delta_p)|^2$ la puissance p-ième de $\|f\|_2^2$.

Appelons $D_n(\gamma)$ l'ensemble $\{(\gamma_1, \dots, \gamma_n) \in \Gamma^n ;\ \gamma_i \neq \gamma_j$ si $i \neq j,\ \gamma = \gamma_1 + \gamma_2 + \dots + \gamma_n\}$, deux éléments de $D_n(\gamma)$ étant supposés semblables s'ils ne diffèrent que d'une permutation sur $1, 2, \dots, n$. Par hypothèse $\operatorname{card} \bigcup_{n=0}^{s} D_n(\gamma) \leqslant N$. D'autre part

$$b(\gamma) = \sum_{0 \leqslant 2p \leqslant s} \ \sum_{(\gamma_1, \dots, \gamma_{s-2p}) \in D_{s-2p}} s(s-1)\dots(2p+1) a(\gamma_1)\dots a(\gamma_{s-2p})$$
$$\sum_{\delta_i \in E} [a(\delta_1)]^2 \dots [a(\delta_p)]^2$$

$$|b(\gamma)| \leqslant \sum_{n=0}^{s} (s-1)\dots(s-n+1) \sum_{(\gamma_1, \dots, \gamma_n) \in D_n} |a(\gamma_1)\dots a(\gamma_n)| \|f\|_2^{s-n}.$$

Le nombre de termes de cette somme est au plus égal à $s!\,N$, et grâce à l'inégalité de Schwarz

$$|b(\gamma)|^2 \leqslant s!\,N \sum_{n=1}^{s} s(s-1)\dots(s-n+1)$$
$$\sum_{(\gamma_1, \dots, \gamma_n) \in D_n} |a(\gamma_1)\dots a(\gamma_n)|^2 \|f\|_2^{2s-2n}.$$

Formons $\sum_{\gamma \in \Gamma} |b(\gamma)|^2$ : les ensembles $D_n(\gamma)$, si $n$ est fixé, étant deux à deux disjoints,

$$\sum_{\gamma \in \Gamma} \ \sum_{(\gamma_1, \dots, \gamma_n) \in D_n(\gamma)} |a(\gamma_1)\dots a(\gamma_n)|^2 \leqslant \frac{1}{n!} \|f\|_2^{2n}$$

puisque chaque terme $|a(\gamma_1)\dots a(\gamma_n)|$ se trouve $n!$ fois dans le développement de $\|f\|_2^{2n}$.

Donc $\sum_{\gamma \in \Gamma} |b(\gamma)|^2 \leqslant s!\,N \sum_{n=0}^{s} C_s^n \|f\|_2^{2s} = s!\,N\,2^s \|f\|_2^{2s})$.

Or $\sum_{\gamma \in \Gamma} |b(\gamma)|^2 = \|f\|_{2s}^{2s}$

$$\|f\|_{2s} \leqslant A(s!\,N)^{1/2s} \|f\|_2.$$

Le lemme suivant montre qu'il est possible de construire des ensembles $\Lambda(2s)$ en utilisant la condition suffisante du théorème 6 :

Lemme 3. — *Soit $s$ un entier et $V$ un sous-espace vectoriel de $\Gamma$ de dimension finie $k$, $k$ étant un multiple de $2s$. Il* *existe un sous-ensemble* E *de* $V - \{0\}$ *possédant* $2^{k/2s}$ *éléments, tel que* $r_s(E, \gamma) \leqslant 1$ *pour tout* $\gamma$.

V possède $2^k - 1$ éléments non nuls. On construit E par récurrence : ayant déjà choisi $f_1, \ldots, f_n$, on choisit $f_{n+1}$ de manière que $f_{n+1} + \sum_{i=1}^{p} f_{r_i}$ soit différent de 0 quels que soient $p < 2s$ et les entiers $r_i$ deux à deux distincts et inférieurs ou égaux à $n$, c'est-à-dire $f_{n+1} \neq \sum_{i=1}^{p} f_{r_i}$. Il y a au plus $C_n^1 + C_n^2 + \cdots + C_n^{2s-1}$ éléments de V de cette forme, on pourra donc trouver $f_{n+1}$ tant que

$$C_n^1 + C_n^2 + \cdots + C_n^{2s-1} < 2^k - 1.$$

Comme $\sum_{p=1}^{2s-1} C_{2^{k/2s}}^p < (2s-1)\dfrac{2^k}{(2s-1)\,!} < 2^k - 1$ on peut choisir $2^{k/2s}$ éléments ayant la propriété cherchée.

Cette construction remplace ici la construction de Erdös qu'utilise Rudin [1], qui permet, dans le cas des entiers positifs, d'obtenir dans une progression arithmétique de longueur $s^{s-1}p^s$, où $p$ est un nombre premier supérieur à $s$, un ensemble E contenant $p$ termes et tel que $r_s(E, n) \leqslant 1$ pour tout $n$. Ce résultat est évidemment meilleur que celui du lemme 3 car c'est le meilleur possible d'après les conditions nécessaires de Rudin.

THÉORÈME 7. — *Quelle que soit la fonction* $\varphi(p)$ *croissante dans* $[8, +\infty[$, *il existe un ensemble* E *qui est* $\Lambda(p)$ *pour tout* $p$, *et tel que* $A(p, E) \geqslant \varphi(p)$ *pour tout* $p \geqslant 8$.

Soit $N = N_1 \cup N_2 \cup \cdots \cup N_k \cup \ldots$ une partition des entiers telle que $N_k$ possède exactement $n(k)$ éléments, $n(k)$ étant une suite croissante d'entiers tels que $n(k)$ soit divisible par $2k$. Soit $V_k$ l'ensemble des éléments non nuls du sous-espace vectoriel de $\Gamma$ engendré par les éléments $e_n$ de la base canonique tels que $n$ appartienne à $N_k$. On appelle $E_k$ le sous-ensemble de $V_k$ construit comme au lemme 3 avec $s = k$. Montrons que $E = \cup E_k$ est $\Lambda(2k)$ pour tout $k$. Soit en effet $E'_k = \bigcup_{n \geqslant k} E_n$. Pour tout $\gamma$ et pour tout $n$, $n \geqslant k$, $r_k(E_n, \gamma) \leqslant 1$. Soit $\gamma$ quelconque : $\gamma$ s'écrit d'une manière et d'une seule sous la forme $\gamma = \gamma_{n_1} + \cdots + \gamma_{n_p}$, où $\gamma_{n_i} \in V_{n_i} \cdot \gamma_{n_i}$, si $n_i \geqslant k$, s'écrivant d'au plus une manière sous forme de somme d'au plus $k$ éléments de $E_{n_i}$, $\gamma$ s'écrit d'au plus une manière sous forme de somme d'au plus $k$ éléments de $E'_k$. $E'_k$ est donc un ensemble $\Lambda(2k)$, $E - E'_k$ est également $\Lambda(2k)$ puisque c'est un ensemble fini, et par conséquent leur réunion $E$ est $\Lambda(2k)$.

E est donc $\Lambda(p)$ pour tout $p$. Cherchons une minoration de $A(p, E)$ : on utilise le théorème 1.

$2^{n(k)/2k} = \text{Card}\,(E \cap V_k) \leqslant [A(p, E)]^2 2^{2n(k)/p}$ quels que soient $k$ et $p$.

En particulier, si $p = 8k$, $A(8k, E) \geqslant 2^{n(k)/8k}$. La fonction $A(p, E)$ étant croissante et $n(k)$ arbitraire, on en déduit le résultat.

## BIBLIOGRAPHIE

[1] W. Rudin, Trigonometric series with gaps, *J. of Math. and Mech.*, 9 (1960).
[2] W. Rudin, Fourier analysis on groups, Interscience Publishers.
[3] M. et Mme Malliavin, Caractérisation arithmétique d'une classe d'ensembles de Helson, *C.R.A.S.*, 264, p. 192.
[4] Paley, A remarkable system of orthogonal functions, *PLMS*, 34 (1932).
[5] A. Zygmund, Trigonometric Series (tome 1), Cambridge University Press.

Manuscrit reçu le 20 avril 1968.

Mme A. Bonami,
Département de Mathématique,
Faculté des Sciences, Orsay (Essonne)