

SÉMINAIRE DUBREIL. ALGÈBRE ET THÉORIE DES NOMBRES

EMIL GROSSWALD

Les groupes de Galois des polynômes de Bessel

Séminaire Dubreil. Algèbre et théorie des nombres, tome 18, n° 1 (1964-1965), exp. n° 17, p. 1-12

http://www.numdam.org/item?id=SD_1964-1965__18_1_A14_0

© Séminaire Dubreil. Algèbre et théorie des nombres
(Secrétariat mathématique, Paris), 1964-1965, tous droits réservés.

L'accès aux archives de la collection « Séminaire Dubreil. Algèbre et théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

LES GROUPES DE GALOIS DES POLYNÔMES DE BESSEL

par Emil GROSSWALD

1. Introduction.

L'équation des ondes en trois dimensions spatiales s'écrit $\nabla^2 u = \frac{1}{c^2} \frac{\partial^2 u}{\partial t^2}$. Si l'on exprime le Laplacien $\nabla^2 u$ en coordonnées sphériques et l'on sépare les variables, on obtient (après un changement d'échelle) :

$$r^2 f'' + 2rf' + r^2 f = \mu f ,$$

où $\mu = n(n+1)$ est une valeur propre imposée par une des autres équations différentielles. En général, on pose $f = r^{-1/2} y$, et on obtient l'équation de Bessel :

$$r^2 y'' + ry' + (r^2 - (n + \frac{1}{2})^2)y = 0$$

d'ordre semi-entier, donc avec des solutions élémentaires. Si l'on pose

$$f = r^{-1} w(r) ,$$

on obtient

$$r^2 (w'' + w) = n(n+1)w ,$$

équation d'ondes stationnaires. Enfin, le changement de variable $x = \frac{1}{ir}$ donne

$$x^2 y'' + (2x + 2)y' - n(n+1)y = 0 ,$$

équation qui a des solutions polynomiales, et qu'il convient de comparer à l'équation

$$x^2 y'' + (2x + 2)y' - n(n+1)y = y'' + 2y'$$

des polynômes de Legendre.

D'une manière un peu plus générale, on peut considérer avec KRALL et FRINK [18] l'équation $x^2 y'' + (ax + b)y' - n(n+a-1)y = 0$. Le paramètre b est sans importance car, en posant $x = bz$, l'équation se réduit à $z^2 y'' + (az+1)y' - n(n+a-1)y = 0$; mais a est un paramètre effectif.

Les solutions polynomiales :

$$(1) \quad y_n = \sum_{k=0}^n \frac{(n+k)!}{(n-k)! k!} \left(\frac{x}{2}\right)^k$$

$$= 1 + \frac{n(n+1)}{2} x + \dots + \frac{(2n-1)!}{(n-1)!} \left(\frac{x}{2}\right)^{n-1} + \frac{(2n)!}{n!} \left(\frac{x}{2}\right)^n$$

ont été étudiées par KRALL et FRINK [18] en 1949, et ces polynômes avaient déjà été rencontrés par KRALL en 1941 [17]. En fait, ils avaient déjà été utilisés par HAHN en 1935 [12] et BOCHNER (1929 ; voir [4]), et ne diffèrent que par leur normalisation des polynômes employés par HERMITE [13] pour prouver la transcendance de e .

Depuis 1949, ces polynômes, appelés par KRALL et FRINK polynômes de Bessel (nous utiliserons ici pour les désigner l'abréviation P. B.), ont été beaucoup étudiés (BURCHNALL (1951) [6], AGARWAL (1954) [1], NASSIF (1954) [19], CARLITZ (1957) [8], AL-SALAM (1957) [2], [3], GROSSWALD [11], et d'autres). On a étudié leurs propriétés d'orthogonalité, représentations de certaines classes de fonctions en séries de P. B., fonctions génératrices, etc.

2. Propriétés générales des P. B.

(a) Relations de récurrences.

$$(2) \quad y_{n+1} = (2n+1)xy_n + y_{n-1}.$$

$$(3) \quad x^2 y'_n = (nx-1)y_n + y_{n-1}.$$

$$(4) \quad x^2 y'_{n-1} = y_n - (nx+1)y_{n-1}.$$

(b) Orthogonalité.

$$\frac{1}{2\pi i} \int_{|z|=1} y_m(z) \overline{y_n(z)} e^{-2/z} dz = \begin{cases} 0 & m \neq n \\ (-1)^n \frac{2}{2n+1} & m = n \end{cases}.$$

Remarques.

(i) C'est bien le produit des polynômes et non $y_m(z) \overline{y_n(z)}$ qui apparaît sous le signe d'intégration.

(ii) Ces formules ressemblent beaucoup à celles relatives aux polynômes de Legendre.

(c) Fonction génératrice.

$$\sum_{n=0}^{\infty} y_{n-1}(x) \frac{t^n}{n!} = \exp\left\{\frac{1 - \sqrt{1 - 2tx}}{x}\right\} \quad (y_0 = y_{-1} = 1).$$

(d) Formule "de Rodrigues".

$$y_n(x) = 2^{-n} e^{2/x} \frac{d^n}{dx^n} (x^{2n} e^{-2/x}) .$$

Ces propriétés (ainsi que bien d'autres) se trouvent toutes démontrées en [18]. Nous utiliserons les relations de récurrence, qui se démontrent par directe substitution de (1).

(e) Zéros.

(i) Tous les zéros sont simples.

Démonstration. - Si $y_n(x_0) = y'_n(x_0) = 0$, alors (3) $\Rightarrow y_{n-1}(x_0) = 0$; ceci et (4) $\Rightarrow y'_{n-1}(x_0) = 0$ (car $x_0 \neq 0$). Donc, x_0 est zéro multiple de $y_{n-1}(x)$ et ainsi, par induction, de $y_1(x) (= 1 + x)$, ce qui est faux.

(ii) A l'exception de $y_1(x) = 1 + x$, tous les zéros des P. B. sont intérieurs au cercle $|x| < 1$.

Démonstration. - Le théorème de KAKEYA [16] affirme que, si $a_0 \geq a_1 \geq \dots \geq a_n \geq 0$, alors tous les zéros z_m de $\sum_{v=0}^n a_v x^{n-v}$ satisfont $|z_m| \leq 1$, et un théorème de Hurwitz donne une condition nécessaire (et suffisante) pour avoir $|z_m| = 1$. Tous les P. B. satisfont la condition de Kakeya, et aucun ne vérifie celle de Hurwitz, à l'exception de $y_1(x)$. (NASSIF montre que les racines de $y_n(x)$ se trouvent dans le cercle $|x| \leq \sqrt{\frac{n-1}{2n-1}}$.)

(iii) $y_{2n}(x)$ n'a pas de zéros réels. (La démonstration directe est compliquée; la propriété est un corollaire facile de certains résultats généraux de BURCHNALL [6].)

(iv) $y_{2n+1}(x) = 0$ a exactement une racine réelle.

Démonstration. - Si $x_1 < x_2$ sont deux racines réelles consécutives,

$$y'_{2n+1}(x_1) y'_{2n+1}(x_2) < 0 .$$

Il résulte donc de (3) que

$$0 > x_1^2 x_2^2 y'_{2n+1}(x_1) y'_{2n+1}(x_2) = y_{2n}(x_1) y_{2n}(x_2) ;$$

donc, $y_{2n}(x) = 0$ pour un x avec $x_1 < x < x_2$, ce qui est impossible d'après (iii).

3. Irréductibilité des P. B. sur $\mathbb{Q}$.

(a) Soit p un nombre premier, et

$$f(x) = \sum_{v=0}^n a_v p^{e_v} x^{n-v}, \quad p \nmid a_v.$$

On considère les points de coordonnées $(n - v, e_v)$, et on construit le "polygone de Newton" correspondant (polygone convexe d'ordonnées maximales, ne laissant aucun point $(n - v, e_v)$ au-dessous). En observant que $f(x)$ est sûrement irréductible sur $\mathbb{Q}$ s'il l'est dans une extension p -adique (mais pas réciproquement) et que, à chaque côté du polygone de Newton, correspond un facteur de $f(x)$ dans $\mathbb{Q}_p$, on obtient le résultat suivant (DUMAS, [10]) :

Supposons que le polygone de Newton a m côtés et que le côté r -ième ait la projection horizontale ℓ_r et verticale k_r , avec $(\ell_r, k_r) = \lambda_r$, de sorte que $\ell_r = \lambda_r s_r$; alors, tout facteur irréductible de $f(x)$ a un degré de la forme

$$\sum_{r=1}^m \mu_r s_r \quad (0 \leq \mu_r \leq \lambda_r).$$

Les critères d'irréductibilités bien connus de EISENSTEIN, PERRON, etc. en sont des cas particuliers.

Si $e_0 = 0$, $e_v \geq \frac{ve}{n}$, alors $m = 1$ et tout facteur irréductible a un degré $= \mu_r n / \lambda$ avec $\lambda = (n, e_n)$ et $\mu_r \leq \lambda$. Si en plus $(n, e_n) = 1$, alors $f(x)$ est irréductible.

(b) Pour étudier le groupe de Galois des P. B. (y inclus sa transitivité, c'est-à-dire l'irréductibilité des polynômes), il est plus convenable de considérer les polynômes réciproques $z_n(x) = x^n y_n(\frac{1}{x})$, soit

$$(5) \quad z_n(x) = \sum_{v=0}^n \frac{(n+v)!}{(n-v)! v! 2^v} x^{n-v};$$

ceux-ci ont les mêmes discriminants et mêmes groupes de Galois que les $y_n(x)$.

Soient $p_1 < p_2$ des nombres premiers consécutifs, $p_1 \leq n < p_2$, et posons

$$k_1 = n - p_1, \quad k_2 = p_2 - n - 1.$$

Alors (5) montre que, si $p = p_1$, $e_v = 0$ pour $0 \leq v \leq k_1$, et $e_v = 1$ pour $k_1 + 1 \leq v \leq n$; du polygone de Newton, il résulte qu'il y a un facteur irréductible de degré au moins $n - k_1$. De même, en prenant $p = p_2$, on montre l'existence d'un facteur irréductible de degré au moins $n - k_2$. En particulier, si $n = p$ ou $n = p - 1$, le P. B. est irréductible. Si $k = \min(k_1, k_2)$, le P. B. a un

facteur irréductible de degré $\geq n - k$.

On sait que, si $\varepsilon > 0$,

$$\exists N(\varepsilon) \text{ tel que } x \geq N(\varepsilon) \implies \{\exists p \text{ tel que } x < p \leq (1 + \varepsilon)x\}.$$

La fonction $N = N(\varepsilon)$ n'est pas connue en général, mais on sait, par exemple (voir [5]), que $N(\frac{1}{8}) = 48$. Pour $n \geq N(\varepsilon)$, $k \leq \frac{n}{2/\varepsilon + 1} < \frac{n\varepsilon}{2}$, de sorte que $z_n(x)$ contient un facteur irréductible de degré $\geq n - k > n(1 - \varepsilon/2)$. Avec $\varepsilon = 1/8$, $k \leq \frac{n}{2.8 + 1} = \frac{n}{17}$, $n - k \geq \frac{16}{17}n$ pour $n \geq 48$. Comme une étude directe montre que tous les P. B., avec $n < 50$, sont irréductibles, il en résulte :

(i) Les facteurs irréductibles des P. B. ne peuvent pas avoir des degrés d avec $k < d < n - k$.

(ii) Chaque P. B. a un facteur irréductible de degré $\geq An$ avec $A \geq \frac{16}{17}$ et $A \rightarrow 1$ lorsque $n \rightarrow \infty$.

(iii) Si $n = p^m$,

$$e_0 = 0, \quad e_\nu \geq \frac{\nu}{p-1} \quad (1 \leq \nu \leq n-1), \quad e_n = \frac{n-1}{p-1};$$

donc $e_\nu \geq \frac{\nu e_n}{n}$, et comme on a aussi $(e_n, n) = 1$, $z_n(x)$ est irréductible.

(iv) Si $n = q.p - 1$ (q peut ne pas être premier) avec $q < p$, alors

$$e_0 = 0, \quad e_\nu = \left[\frac{\nu-1}{p} \right] + 1 \quad (1 \leq \nu \leq n);$$

en particulier, $e_n = q$, $m = 1$, et $(e_n, n) = (q, qp - 1) = 1$, donc $z_n(x)$ est irréductible.

(V) $n = qp$, $q < p$. La situation est pareille à (iv), à l'exception du fait que $(e_n, n) = q$. Donc, on peut avoir des facteurs de degrés $\ell \frac{n}{q} = \ell p$ ($1 \leq \ell \leq q$). Si $q \leq 17$, $\frac{n}{17} < p \leq d = \ell p < n - \frac{n}{17}$, ce qui est impossible, d'après (i). Même si $q > 17$, mais $p > k$, on obtient l'irréductibilité, et c'est le cas de tous les $n = pq < 50$ (lorsque les P. B. correspondants ne sont pas déjà irréductibles en vertu des critères précédents).

(vi) $n = p^m - 1$, $e_0 = 0$, $e_n = \frac{n}{p-1}$, $e_\nu \geq \frac{\nu e_n}{n}$ (calcul non trivial); donc, $(n, e_n) = \frac{n}{p-1}$, et les degrés des facteurs sont de la forme $\ell(p-1)$. Si $k < p-1$, $z_n(x)$ est irréductible.

On peut prouver d'autres critères, mais ils ne sont pas suffisants pour démontrer l'irréductibilité de tous les P. B. Pour $n \leq 400$, les critères énoncés suffisent dans tous les cas, sauf 19; ces 19 polynômes sont aussi irréductibles, comme on le prouve à l'aide de (i).

4. Le groupe de Galois G_n de $z_n(x)$.

(a) THÉOREME. - Si G_n est transitif, alors $G_n = S_n$, le groupe symétrique sur
n symboles, avec l'exception possible des cas $n = 11$ et $n = 12$.

Dans la démonstration de ce théorème, on fera usage de plusieurs théorèmes connus, ainsi que de certains résultats classiques concernant les groupes finis de petits degrés. On écrira $o(G)$ pour désigner l'ordre du groupe G .

THÉOREME A (I. SCHUR, [20]). - Soit $f(x) = \sum_{i=0}^n a_i x^{n-i}$ un polynôme irréducti-
ble sur $\mathbb{Q}$, de discriminant Δ , et ayant le groupe de Galois G_n . Supposons que

(a) $\exists p, m$ tels que $m \geq n$, $p^m | \Delta$, $p | a_n$, $p^2 \nmid a_n$; et

(b) $f(x) \equiv x^k y(x) \pmod{p}$, avec $\delta = \text{discriminant de } y(x)$ et $p \nmid \delta$.

Alors, $p | o(G_n)$.

THÉOREME B (C. JORDAN, [14], Note C). - Si le groupe G de permutations sur n symboles est primitif et contient une substitution circulaire d'ordre premier p , il est au moins $\ell = n - p + 1$ fois transitif.

THÉOREME C (C. JORDAN, [15], Théorème I). - Un groupe de degré $n = p + k$ (p premier, $k > 2$) ne peut être plus de k fois transitif, à moins de contenir le
groupe alterné.

THÉOREME D (R. DEDEKIND ; voir [20], p. 449, où le théorème est cité sans références bibliographiques. Il semble être équivalent à un résultat contenu dans [9], § 3 et 4). - Soit $f(x) \equiv f_1(x).f_2(x)...f_r(x) \pmod{p}$, $f_j(x)$ ($1 \leq j \leq r$) irré-
ductibles et distinctes $\pmod{p}$; alors, le groupe de Galois de $f(x)$ contient
au moins une permutation de r cycles, chacun correspondant à un facteur $f_j(x)$ et de même ordre que le degré du polynôme $f_j(x)$ auquel il correspond.

THÉOREME E (voir e. g. [7], p. 207, démonstration du corollaire). - Soit G un
groupe primitif de permutations sur n symboles, et soit $p < 2n/3$ un nombre
premier tel que $p^e | n!$, $p^{e+1} \nmid n!$; alors $p^e \nmid o(G)$, à moins que $G \supset A_n$ ($A_n =$
groupe alterné sur n symboles).

THÉOREME F (I. SCHUR [20]). - Si p satisfait aux conditions du théorème A et
en outre $\frac{n}{2} < p < n - 2$, alors $G_n = A_n$ si $\sqrt{n} \in \mathbb{Z}$, $G_n = S_n$ si $\sqrt{n} \notin \mathbb{Z}$.

Comme la justification de ce théorème en [20] est très brève, en voici une plus complète.

Démonstration. - Si p satisfait aux conditions du théorème A, $p \mid o(G_n)$. Comme $p > n/2$, il résulte en plus que G_n contient un élément P , générateur d'un groupe cyclique d'ordre p ; donc, G_n est primitif. Il résulte ainsi du théorème B que G_n est au moins $\ell = n - p + 1$ (> 3) fois transitif. Alors, en écrivant $n = p + k$, $k = n - p = \ell - 1 > 2$, et il résulte du théorème C que $G_n \supset A_n$ (car $\ell = k + 1 > k$ et $k > 2$) et $G_n = A_n$ ou $G_n = S_n$, selon que $D_n^{1/2} \in \mathbb{Z}$ ou $D_n^{1/2} \notin \mathbb{Z}$.

(b) Pour appliquer ces théorèmes, il faut d'abord calculer le discriminant D_n de $z_n(x)$, le même que celui de $y_n(x)$. Si

$$y_n(x) = \sum_{m=0}^n a_{n-m} x^m,$$

il résulte de (1) que $a_0 = \frac{(2n)!}{n! 2^n}$, $a_n = 1$, et la résultante $R_n = R(y_{n-1}, y_n)$ se calcule, à l'aide de (2), comme suit : Si $x = x_\nu$ parcourt les zéros de $y_n(x)$, alors $y_{n+1}(x_\nu) = y_{n-1}(x_\nu)$, et en faisant le produit pour $\nu = 1, 2, \dots, n$,

$$a_0^{-n-1} R_{n+1} = a_0^{-n+1} R_n;$$

donc

$$R_{n+1} = a_0^2 R_n = \left(\frac{(2n)!}{n! 2^n} \right)^2 R_n,$$

et, par induction,

$$R_n = 2^{-(n-1)n} \left\{ \prod_{k=1}^{n-1} \frac{(2k)!}{k!} \right\}^2.$$

De même, la substitution de x_ν pour x en (3) donne

$$x_\nu^2 y'_n(x_\nu) = y_{n-1}(x_\nu),$$

et, en faisant le produit sur ν ,

$$\left(\prod_{\nu=1}^n x_\nu \right)^2 \left(\prod_{\nu=1}^n y'_n(x_\nu) \right) = \prod_{\nu=1}^n y_{n-1}(x_\nu),$$

d'où l'on obtient

$$a_0^{-2} (a_0^{-n+1} R(y_n, y'_n)) = a_0^{-n+1} R_n.$$

En observant que $a_0 D_n = R(y_n, y'_n)$, une simplification évidente donne

$$D_n = \frac{(2n)!}{2^n \cdot n!} \left(\prod_{k=1}^{n-1} \frac{(2k)!}{k!} \right) 2^{-n(n-1)},$$

ou

$$(6) \quad D_n = \prod_{k=0}^{n-1} (2n - 2k - 1)^{2k+1}.$$

Nous faisons les remarques suivantes :

- (i) Si $n > 1$, $\sqrt{D_n} \notin \mathbb{Z}$; donc, $G_n \supset A_n \Rightarrow G_n = S_n$; et
- (ii) Pour tout entier impair $m < n$, $m^k \nmid D_n$ à une puissance $k > n$.

(c) Essayons d'abord d'appliquer le théorème F; pour cela, comme nous le verrons, il nous faut trouver un nombre premier p tel que

$$(7) \quad \frac{2n-1}{3} < p < n-2.$$

Nous savons déjà de [5] que, pour $x \geq 48$, il y a un p tel que $x < p \leq \frac{9}{8}x$, et il résulte aisément (en posant $\frac{9}{8}x = n-3$) que, pour $n = 57$, il y a toujours un p dans l'intervalle désiré. Une vérification directe montre que de tels nombres premiers existent en fait pour tout $n \geq 14$, ainsi que pour $n = 10$.

Vérifions maintenant que les conditions du théorème A sont en fait satisfaites par un tel p .

Pour (a) : En écrivant

$$z_n(x) = \sum_{m=0}^n a_m z^{n-m},$$

$a_n = \frac{(2n)!}{2^n n!}$, d'après (5); donc p divise a_n exactement à la première puissance (car $p \mid (2n)!$, $2p \nmid (2n)!$, mais, d'après (7), $p \geq \frac{2n+1}{3}$ et $3p \nmid (2n)!$; aussi $p \mid n!$, mais $2p > \frac{4n}{3}$ et $p^2 \nmid n!$). Si $p = 2n - 2k - 1$, alors

$$m = 2k + 1 = 2n - p \geq 2n - (n - 3) = n + 3 > n$$

et $p^m \nmid D_n$ d'après (6).

Pour (b) : D'après (5), p divise les coefficients de z^ν ($0 \leq \nu \leq p$); donc,

$$z_n(x) \equiv x^p \sum_{j=0}^{n-p} \frac{(n+j)!}{(n-j)! j! 2^j} x^{n-p-j} \pmod{p}.$$

Mais

$$\begin{aligned} \frac{(n+j)!}{(n-j)! j! 2^j} &= \frac{(n-j+1)(n-j+2)\dots(n+j)}{2^j j!} \\ &\equiv \frac{(n-p-j+1)\dots(n-p+j)}{2^j j!} = \frac{(n-p+j)!}{(n-p-j)! j! 2^j} \pmod{p}, \end{aligned}$$

de sorte que

$$z_n(x) \equiv x^p z_{n-p}(x) \pmod{p}.$$

Enfin, d'après (6), D_{n-p} ne contient que des facteurs plus petits que $2n-2p-1 < 2n - \frac{4n-2}{3} - 1 = \frac{2n-1}{3} < p$; donc, $p \nmid D_{n-p}$, et toutes les conditions du théorème A se trouvent vérifiées.

Enfin, pour $n > 1$, $\frac{2n-1}{3} \geq \frac{n}{2}$; donc le théorème F est applicable et, puisque $D_n^{1/2} \notin \mathbb{Z}$ pour tout $n > 1$, tous les P. B. irréductibles de degrés $n \geq 14$, ainsi que le P. B. de degré $n = 10$, ont comme groupe de Galois G_n le groupe symétrique S_n .

(d) Pour les autres valeurs de n ($1 \leq n \leq 13$, $n \neq 10$), nous sommes obligés d'étudier presque chaque cas séparément. Le cas $n = 1$ est trivial ; mais aussi $n = 2$ (car S_2 et A_2 sont les seules possibilités, et $G_2 \neq A_2$) et $n = 3$ (car il n'y a que les trois possibilités $G_3 = \{e\}$, A_3 ou S_3 , et les deux premières s'éliminent trivialement).

Pour $4 \leq n \leq 13$ ($n \neq 10$), nous essayons d'utiliser au moins le théorème A. Pour cela, il nous faut trouver, pour chaque n , un nombre premier $p = p_n$, tel que $\frac{2n-1}{3} < p_n < n$. Nous trouvons en effet de tels p_n , sauf pour $n = 5$ et $n = 11$, à savoir

$$p_4 = 3, \quad p_6 = p_7 = 5, \quad p_8 = p_9 = 7, \quad p_{12} = p_{13} = 11.$$

Les polynômes correspondants sont irréductibles, de sorte que leurs G_n sont transitifs. Donc, le théorème A s'applique, et $p_n \mid o(G_n)$. Comme on a encore dans tous ces cas $p_n > n/2$, il résulte que les G_n sont primitifs et le théorème B est applicable. Il en résulte que chacun de ces groupes G_n est transitif, d'ordre $\ell_n \geq n - p_n + 1$.

En particulier, pour $n = 4$, les seuls groupes de permutations primitifs de degré 4 sont A_4 et S_4 (voir [7], § 166 (ii), p. 214) ; donc, $G_4 \neq A_4 \Rightarrow G_4 = S_4$. Pour $n = 7$, $\ell_7 \geq 7 - 5 + 1 = 3$, et les seuls groupes de permutations de degré 7, triplement transitifs, sont A_7 et S_7 ([7], § 166 (V), p. 216), ainsi que $G_7 = S_7$. Pour $n = 13$, nous rappelons le fait (voir par exemple [7], § 165, p. 214, Ex. ; mais ce résultat fut connu par JORDAN) que, si $p_1 > 3$ et $p_2 = 2p_1 + 1$ sont des nombres premiers, alors tout groupe triplement transitif de degré $n = 2p_1 + 3$ contient A_n . En particulier, $\ell_{13} \geq 13 - 11 + 1 = 3$; donc, G_{13} est triplement transitif. On a aussi $n = 13 = 2.5 + 3$ avec $p_1 = 5 > 3$ et $2p_1 + 1 = 2.5 + 1 = 11 = p_2$ nombres premiers. Par conséquent, $G_{13} \supset A_{13}$, et

comme $D_{13}^{1/2} \notin \mathbb{Z} \Rightarrow G_{13} \neq A_{13}$, il s'ensuit que $G_{13} = S_{13}$.

Il nous reste à considérer les cas $n = 5, 6, 8, 9, 11$ et 12 . Pour les étudier, nous utiliserons le théorème D, en vue d'établir l'existence d'un élément d'ordre $p'_n < \frac{2n}{3}$, tel que $p'_n | n!$, $(p'_n)^2 \nmid n!$. Le théorème E (avec $e = 1$) affirme que $p'_n \nmid o(G_n)$, à moins que $G_n \supset A_n$; mais ayant établi l'existence d'un élément de G_n d'ordre p' , $p'_n | o(G_n)$ et $G_n \supset A_n$, de sorte que $G_n = S_n$, comme avant.

Pour $n = 5$,

$$z_5(x) = x^5 + 15x^4 + 105x^3 + 420x^2 + 945x + 945 \\ \equiv (x^3 + x^2 + 4x + 5)(x - 2)(x - 1) \pmod{17},$$

avec $x^3 + x^2 + 4x + 5$ irréductible $\pmod{17}$. Donc, d'après le théorème D, G_5 contient un cycle d'ordre 3 et $3 | o(G_5)$. Mais les seuls groupes de degré 5, dont l'ordre soit divisible par 3, sont A_5 et S_5 ; ainsi, une fois de plus, $G_5 = S_5$.

De même,

$$z_6(x) \equiv (x + 3)(x^2 + x - 1)(x^3 + 4x^2 - 3x + 6) \pmod{13},$$

tous les facteurs étant irréductibles $\pmod{13}$. D'après le théorème D,

$$\exists P \in G_6, \quad P = (a, b)(c, d, e)(f);$$

alors $(a, b) = P^3 \in G_6$ aussi, et comme le groupe primitif G_6 contient une transposition, $G_6 = S_6$ (comme $2^4 | 6!$, il serait bien malaisé d'appliquer directement le théorème E).

Pour $n = 8$,

$$z_8(x) \equiv (x + 6)(x^2 + 2x + 2)(x^5 + 9x^4 - 7x^3 + 8x^2 - 7x + 4) \pmod{19},$$

avec des facteurs irréductibles $\pmod{19}$. Donc, d'après le théorème D,

$$\exists P \in G_8, \quad P = (a, b)(c, d, e, f, g)(h),$$

de sorte que $P^2 \in G_8$, $P^2 = (c, e, g, d, f)$ étant d'ordre 5. Comme $5 | 8!$, $5^2 \nmid 8!$ et $5 < 2.8/3$, le théorème E montre que $G_8 \supset A_8$; donc, $G_8 = S_8$.

Il nous reste à considérer seulement les trois valeurs $n = 9, 11$, et 12 . Tous les calculs précédents se font aisément à la main; mais déjà les calculs nécessaires pour obtenir la décomposition

$$z_9(x) \equiv (x + 3)(x^3 + 12x^2 - 13x + 3)(x^5 + x^4 - 5x^3 - x^2 + 7x + 13) \pmod{29}$$

seraient pénibles sans l'aide d'une calculatrice. Cette factorisation (en facteurs irréductibles mod 29) indique, d'après le théorème D, l'existence d'une permutation $P \in G_9$, de la forme

$$P = (a, b, c)(d, e, f, g, h)(i).$$

Donc, aussi $P^3 \in G_9$ et $P_3 = (d, g, e, h, f)$ est d'ordre 5. Par conséquent, $5 \mid o(G_9)$; mais, ayant aussi $5 \nmid 9!$, $5^2 \nmid 9!$, et $5 < \frac{2}{3} \cdot 9 = 6$, le théorème E montre que $G_9 \supset A_9$, ainsi que $G_9 = S_9$.

Pour les deux cas qui restent, $n = 11$ et $n = 12$, tous les efforts de mettre en évidence des éléments d'ordre 7 dans G_{11} et G_{12} ont échoué, bien que l'on soit allé jusqu'à des congruences mod 61 (pour $z_{11}(x)$) et mod 47 (pour $z_{12}(x)$). (Il est clair que, si $P \in G_n$, $o(P) = 7$; alors, $7 \mid n!$, $7^2 \nmid n!$, $7 < \frac{2n}{3}$, pour $n = 11$ et $n = 12$, et l'on obtiendrait, comme avant, $G_n = S_n$ dans ces deux cas.) Aussi, d'autres manières d'approcher le problème ont été essayées en vain, par exemple l'étude de leurs multiples transitivités, à l'aide des théorèmes classiques de JORDAN ou BURNSIDE, ou des résultats récents de M. HALL, WIELANDT et Ph. HALL. Ces échecs répétés nous amènent à considérer la possibilité que $G_n \neq S_n$ pour $n = 11$ et $n = 12$, et pour ces valeurs seulement !

Pour étrange que cela puisse paraître, cela n'est peut-être pas plus étrange que l'existence, précisément pour ces degrés, de groupes de hautes transitivités, ne contenant pas A_n , à savoir les groupes de Mathieu. Il paraît désirable de déterminer la structure de G_{11} et G_{12} , pour clore ainsi définitivement le problème des groupes de Galois transitifs des polynômes de Bessel.

BIBLIOGRAPHIE

- [1] AGARWAL (Ratan Prakash). - On Bessel polynomials, Canadian J. of Math., t. 6, 1954, p. 410-414.
- [2] AL-SALAM (Waleed A.). - The Bessel polynomials, Duke math. J., t. 24, 1957, p. 529-545.
- [3] AL-SALAM (Waleed A.). - On the Bessel polynomials, Boll. Unione mat. Italiana, Série 3, t. 12, 1957, p. 227-229.
- [4] BOCHNER (Salomon). - Über Sturm-Liouvillesche Polynomsysteme, Math. Z., t. 29, 1929, p. 730-736.
- [5] BREUSCH (Robert). - Zur Verallgemeinerung des Bertrandschen Postulates, dass zwischen x und $2x$ stets Primzahlen liegen, Math. Z., t. 34, 1932, p. 505-526.
- [6] BURCHNALL (J. L.). - The Bessel polynomials, Canadian J. of Math., t. 3, 1951, p. 62-68.

- [7] BURNSIDE (William). - Theory of groups of finite order. 2nd edition. - Dover Publications, 1955.
 - [8] CARLITZ (Leonard). - A note on the Bessel polynomials, Duke math. J., t. 24, 1957, p. 151-162.
 - [9] DEDEKIND (Richard). - Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen, Abh. Königl. Ges. Wiss. Göttingen, t. 23, 1878, p. 1-23 ; Gesammelte mathematische Werke, t. 1, p. 202-232. - Braunschweig, F. Vieweg und Sohn, 1930.
 - [10] DUMAS (Gustave). - Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels, J. Math. pures et appl., 6e série, t. 2, 1906, p. 191-258.
 - [11] GROSSWALD (Emil). - On some algebraic properties of the Bessel polynomials, Trans. Amer. math. Soc., t. 71, 1951, p. 197-210.
 - [12] HAHN (Wolfgang). - Über die Jacobischen Polynome und zwei verwandte Polynomklassen, t. 39, 1935, p. 634-638.
 - [13] HERMITE (Charles). - Sur la fonction exponentielle, C. R. Acad. Sc. Paris, t. 77, 1875, p. 18-24, 74-79, 226-233, 285-293 ; Oeuvres, t. 3, p. 150-181. - Paris, Gauthier-Villars, 1912.
 - [14] JORDAN (Camille). - Traité des substitutions et des équations algébriques, Nouveau tirage de l'édition de 1870. - Paris, Gauthier-Villars, A. Blanchard, 1957.
 - [15] JORDAN (Camille). - Sur la limite de transitivité des groupes non alternés, Bull. Soc. math. France, t. 1, 1872-73, p. 40-71.
 - [16] KAKEYA (Sôichi). - On the limits of the roots of an algebraic equation with positive coefficients, Tôhoku math. J., t. 2, 1912, p. 140-142.
 - [17] KRALL (H. L.). - On derivatives of orthogonal polynomials, Bull. Amer. math. Soc., t. 47, 1941, p. 261-264.
 - [18] KRALL (H. L.) and FRINK (Orrin). - A new class of orthogonal polynomials : The Bessel polynomials, Trans. Amer. math. Soc., t. 65, 1949, p. 100-115.
 - [19] NASSIF (M.). - Note on the Bessel polynomials, Trans. Amer. math. Soc., t. 77, 1954, p. 408-412.
 - [20] SCHUR (Issai). - Gleichungen ohne Affekt, Sitz. Preuss. Akad. Wiss. Berlin, 1930, p. 443-449.
-