JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Franck LALANDE

La relation linéaire $a = b + c + \cdots + t$ entre les racines d'un polynôme

Tome 19, n° 2 (2007), p. 473-484.

<http://jtnb.cedram.org/item?id=JTNB_2007__19_2_473_0>

Journal de Théorie des Nombres
de Bordeaux **19** (2007), 473-484

La relation linéaire $a = b + c + \cdots + t$ entre les racines d'un polynôme

par Franck LALANDE

Résumé. Nous nous intéressons à la question suivante: À quelles conditions un groupe G est-il le groupe de Galois (principalement sur le corps des rationnels) d'un polynôme irréductible dont certaines racines distinctes vérifient une relation linéaire du type $a = b + c + \cdots + t$? Nous montrons que la relation $a = b + c$ est possible dès que G contient un sous-groupe d'ordre 6, nous décrivons les groupes abéliens pour lesquels la relation $a = b+c+d$ est satisfaite et construisons une famille de relations $a = b+c+\cdots+t$ de longueur $1 + (m-2)(m-3)/2$ pour le groupe alterné A_m. Chaque partie est accompagnée d'exemples.

Abstract. We are going to deal with the following question: Which groups can be the Galois group of an irreducible polynomial with rational coefficients whose distinct roots satisfy a linear relation $a = b + c + \cdots + t$? We are going to show that the relation $a = b + c$ is possible when G contains a subgroup of order 6, describe the abelian groups for which the relation $a = b + c + d$ is possible and construct a family of relations $a = b + c + \cdots + t$ of length $1 + (m-2)(m-3)/2$ for the alternating group A_m.

1. Introduction

Nous nous demandons dans la suite dans quelle mesure des racines distinctes d'un polynôme irréductible à coefficients dans un corps k de caractéristique 0, peuvent vérifier une relation linéaire simple du type $a = b + c + \cdots + t$ en nous attardant sur les relations $a = b + c$ et $a = b + c + d$. Ce problème ne dépend que du groupe de Galois, en ce sens que si une relation est vérifiée par les racines d'un polynôme de groupe G, toute extension de groupe G est alors corps de décomposition d'un polynôme dont les racines vérifient cette relation. On peut alors reformuler le problème de la manière suivante : Pour quelles paires (G, H) de groupe finis $(H \subset G)$, existe-t-il une extension L/k galoisienne de groupe G et un élément x de L

Manuscrit reçu le 18 mai 2006.

qui engendre L^H et dont les conjugués sur k vérifient une relation linéaire du type $a = b+c+\cdots+t$? L'étude de cette problématique remonte je crois à une question de J. Browkin [3] : Existe-t-il un polynôme irréductible sur $\mathbb{Q}$ et non cyclotomique dont trois racines a, b, c vérifient la relation multiplicative $a = bc$? Question à laquelle a répondu positivement A. Schinzel en exhibant le polynôme $P(X) = X^6 - 2X^4 - 6X^3 - 2X^2 + 1$ de groupe de Galois le groupe diédral D_{12} à 12 éléments. Cette relation multiplicative ou de manière équivalente [5], la relation linéaire $a = b + c$, a été étudiée par plusieurs auteurs depuis et dans le cas abélien, des théorèmes de [1], [3] et [5] affirment que pour que la relation $a = b + c$ ait lieu, il faut et il suffit que l'ordre de G soit un multiple de 6. La situation est moins claire dans le cas non abélien. Nous montrons que dans le cas régulier ($H = 1$), elle est possible dès que G possède un sous-groupe d'ordre 6 et dans un récent travail, Girstmair [6] vient de prouver que plus généralement, si elle est possible dans le cas régulier pour un groupe G' elle l'est également pour tout groupe G contenant G'.

Dans la section 2, nous rappelons le cadre naturel, introduit par Kurt Girstmair [4] au début des années 80, dans lequel se placer pour étudier ces relations linéaires ainsi que des résultats de [5] utiles pour la suite. Dans la section 3, nous donnons des exemples de relations linéaires du type $a = b+c$ pour différents groupes de Galois et montrons que cette dernière est possible pour tout groupe contenant un sous-groupe d'ordre 6. Nous donnons dans la section 4 les conditions pour que la relation $a = b + c + d$ ait lieu dans le cas abélien avec cependant un doute pour les groupes du type $C_{2^k} \times C_{p^l}$ où p est un nombre premier impair. Enfin nous construisons section 5 une famille de relations du type $a = b+c+\cdots+t$ et de longueur $1+(m-2)(m-3)/2$ pour la paire primitive (A_m, S_{m-2}). La relation $a = b + c + d$ est donc également possible pour A_5 dans le cas primitif.

Rappelons enfin l'importance du choix de la représentation de permutation du groupe G, c'est à dire du choix de H. Aucune relation non triviale n'est possible pour une paire (G, H) 2-transitive telle la paire (S_n, S_{n-1}) alors que la relation $a = b+c$ est toujours possible pour la paire $(S_n, 1)$. La paire (G, H) est dite *régulière* lorsque $H = 1$ et *primitive* lorsque H est un sous-groupe maximal de G. On supposera toujours dans la suite cette représentation de permutation fidèle, ce qui revient à dire que L est la clôture normale de L^H.

2. Le cadre naturel

Supposons l'existence d'un polynôme irréductible à coefficients dans un corps k de caractéristique nulle dont les racines $x_1, \ldots, x_n$ vérifient la relation linéaire

$$\sum_{i=1}^{n} a_i x_i = 0, \quad a_i \in k \ . \tag{2.1}$$

Notons G le groupe de Galois de l'extension $L/k = k(x_1, \ldots, x_n)/k$, H le fixateur d'une racine x et $s_1, \ldots, s_n$ un système de représentants des classes à gauche de G modulo H. On pose alors $e_H = \frac{1}{|H|} \sum_{h \in H} h$. C'est un élément idempotent de $k[G]$ et pour $g \in G$, $ge_H = e_H$ si et seulement si g appartient à H. Les éléments du $k[G]$-module $k[G]e_H$ s'écrivent de manière unique sous la forme $\sum b_i s_i e_H$ $(b_i \in k)$. Ces éléments agissent de manière naturelle sur L^H et la relation 2.1 s'écrit $ax = 0$ où $a = \sum a_i s_i e_H$. Dans la terminologie introduite par Girstmair, on dit que l'élément a est *admissible* pour la paire (G, H) s'il existe un générateur x de L^H tel que $ax = 0$. Cette notion d'admissibilité est indépendante de l'extension L/k. C'est là un résultat de Girstmair [5] qu'il semble important de rappeler.

Proposition 1. *Pour qu'un élément a de $k[G]e_H$ soit admissible pour la paire (G, H) il faut et il suffit qu'il existe un élément b de $k[G]$ tel que $ab = 0$ et dont le fixateur sous l'action de G soit $G_b = H$.*

Démonstration. C'est une conséquence directe du théorème de la base normale qui affirme que si L/k est une extension galoisienne de groupe G, on peut trouver une base du k-espace vectoriel L de la forme $(s(z))_{s \in G}$. Cela fournit en outre un $k[G]$-isomorphisme $k[G] \longrightarrow L$ qui à $u \in k[G]$ associe $u(z)$.

Si a est admissible pour la paire (G, H), il existe une extension galoisienne L/k de groupe G et un générateur x de L^H tel que $ax = 0$. Considérons alors une base normale $(s(z))_{s \in G}$ de L/k. Il existe un unique $b \in k[G]$ tel que $x = bz$. On a alors $abz = 0$ et comme x engendre L^H, pour $g \in G$, $gx = x$ si et seulement si $g \in H$. D'après le théorème de la base normale $ab = 0$ et $G_b = H$.

Réciproquement, s'il existe $b \in k[G]$ tel que $ab = 0$ et $G_b = H$ et si $(s(z'))_{s \in G}$ est une base normale d'une extension L'/k galoisienne de groupe G, $y = bz'$ est un générateur de L'^H dont les conjugués sur k vérifient la relation $ay = 0$. □

Si le groupe G est abélien, la représentation de permutation induite par H n'est fidèle que pour $H = 1$. Girstmair [5] caractérise les éléments admissibles pour la paire $(G, 1)$ de la manière suivante :

Proposition 2. *Si G est abélien, un élément de $k[G]$ est admissible s'il est annulé par des caractères de G qui engendrent le groupe $\widehat{G}$ des caractères irréductibles de G.*

Enfin suivant [9], si on note A l'anneau $e_H k[G]e_H$ et L/k une extension de groupe G, le théorème de la base normale permet également de vérifier que le morphisme d'algèbre

$$\varphi : A \longrightarrow \mathrm{End}_k(L^H)$$

qui à $a \in A$ associe l'endomorphisme $\varphi_a : x \mapsto ax$, est injectif. Ainsi, à un élément non inversible de A correspond une application φ_a non injective dont les éléments du noyau vérifient la relation linéaire $ax = 0$. Si de plus la paire (G, H) est primitive et si a est de poids non nul (le *poids* de $a = \sum a_g g$ est $p(a) = \sum a_g$), un élément x de ce noyau est un générateur de L^H et a est un élément admissible de A. Nous construisons ainsi dans la section 5 une famille de relations de la forme $x = \sum x_i$ pour la paire (A_m, S_{m-2}).

3. La relation $a = b + c$

Cette section est consacrée à la recherche d'exemples de relations du type $a = b + c$ dans le cas régulier. Autrement dit, on recherche des paires $(G, 1)$ pour lesquelles on puisse trouver un élément admissible de $k[G]$ de la forme $\alpha = 1 - g - g'$. C'est un élément non inversible de $k[G]$ et d'après la proposition 1, il s'agit de trouver un élément β de l'annulateur (à droite) de α et dont le fixateur G_β est réduit à 1. C'est toujours possible par exemple lorsque le groupe G admet un sous-groupe d'ordre 6.

Théorème 1. *Si G admet un sous-groupe d'ordre 6 alors il existe dans $k[G]$ un élément admissible de la forme $1 - g - g'$ où g et g' sont distincts et distincts de 1.*

Démonstration. Les groupes d'ordre 6 sont isomorphes au groupe cyclique C_6 ou au groupe symétrique S_3.

Si G contient un sous-groupe isomorphe à C_6 il contient un élément r d'ordre 6. En posant $\alpha = 1 - r - r^{-1}$ et $\beta = 1 + r - r^3 - r^4$, $\alpha\beta = 0$, $G_\beta = 1$ et α est admissible.

Dans le cas où G contient un sous-groupe isomorphe à S_3 il contient deux éléments r et s d'ordres respectifs 3 et 2 et tels que $rs = sr^{-1}$. En posant cette fois $\alpha = 1 - s - rs$ et $\beta = -r + r^2 - s + rs$, $\alpha\beta = 0$, $G_\beta = 1$ et α est admissible. □

Remarque. Girstmair vient de démontrer dans [6] que plus généralement si G' est un sous-groupe de G, un élément admissible de $k[G']$ le reste dans $k[G]$. Sa démonstration, effectuée dans le cas régulier ($H = 1$), reste valable dans le cas général. Ainsi, si $H \subset G' \subset G$ et si un élément α est admissible dans $k[G']e_H$ alors α est admissible dans $k[G]e_H$.

Exemples. 1) Pour $G = C_6 =< r >$, $\alpha = 1 - r - r^5$ est admissible. Il est annulé par $\beta = 1 + r - r^3 - r^4$ et $G_\beta = 1$. En posant $x = \mathrm{e}^{\frac{2i\pi}{7}}$, βx engendre

une extension galoisienne de groupe C_6 et ses conjugués vérifient la relation $a = b + c$. Le polynôme minimal de βx sur $\mathbb{Q}$ est $X^6 + 14X^4 + 49X^2 + 7$.
2) Pour $G = D_6 = \{r, s/r^3 = s^2 = 1, rsr = s\} = S_3$, $\alpha = 1 - s - rs$ est admissible. Il est annulé par $\beta = -r + r^2 - s + rs$ et $G_\beta = 1$. En posant $x = 2^{1/3} + i\sqrt{3}$ et $j = \mathrm{e}^{\frac{2i\pi}{3}}$, $\beta x = (j^2 - 1)2^{1/3}$ admet pour polynôme minimal $X^6 + 108$ de groupe de Galois D_6 et dont trois racines vérifient la relation $a = b + c$.

En partant de $P(X) = X^3 + X + 1 = \prod(X - x_i)$ de groupe S_3, en prenant $\beta = 1 + r^2 s - s - r = 1 + (13) - (23) - (123)$ et en posant $u = x_1 x_2$, $\beta u = x_1(x_2 - x_3)$ est un générateur du corps de décomposition de P et son polynôme minimal $X^6 - 2X^4 + X^2 + 31$ admet des racines qui vérifient $a = b + c$.
3) Pour $G = D_{12} =< r, s/r^6 = s^2 = (rs)^2 = 1 >$, $\alpha = 1 - r - r^{-1}$ est admissible. Son annulateur (à droite) dans $\mathbb{Q}[G]$ est un $\mathbb{Q}$-espace vectoriel de dimension 4 et de base $(\beta = 1 - r^2 - r^3 + r^5, r\beta, s\beta, rs\beta)$ et $G_\beta = 1$. En prenant $x = 2^{1/6}(5 + i\sqrt{3})$, on obtient $\beta x = 2^{1/6}(10 + 2j^2)$ de polynôme minimal $X^{12} - 988416X^6 + 1405192126464$.

Remarque. Si on note H le groupe d'ordre 2 engendré par s, l'élément $\widetilde{\alpha} = (1 - r - r^{-1})e_H$ est admissible pour la paire (D_{12}, H). En effet, en posant $\widetilde{\beta} = e_H\beta$, $\widetilde{\alpha}\widetilde{\beta} = 0$ et $G_{\widetilde{\beta}} = H$. C'est ainsi par exemple qu'on obtient la relation classique $a = b + c$ vérifiée par les racines de $X^6 - 2$ et directement issue de $1 + j + j^2 = 0$.

On termine cette section par un exemple de polynôme dont les racines vérifient simultanément les relations $a = b + c$ et $a = b' + c' + d'$. Il est assez naturel que ces relations puissent avoir lieu simultanément car si $a = b + c$ et si σ envoie a sur b alors $b = \sigma(a) = \sigma(b) + \sigma(c)$ et $a = \sigma(b) + \sigma(c) + c$. Plus précisément si $\alpha = 1 - g - g'$ est admissible et si $\alpha\beta = 0$ avec $G_\beta = 1$ alors $g\alpha\beta = (g - g^2 - gg')\beta = 0$ et $(1 - g' - g^2 - gg')\beta = 0$. L'élément $\alpha' = 1 - g' - g^2 - gg'$ est donc admissible et si 1, g', g^2 et gg' sont distincts, les conjugués de βx vérifient les deux relations. Cela se produit par exemple pour le groupe alterné A_4.

Proposition 3. *Toute extension galoisienne L/k de groupe de Galois A_4 est le corps de décomposition d'un polynôme de $k[X]$, irréductible de degré 12 et dont les racines vérifient les deux relations linéaires $a = b + c$ et $a = b' + c' + d'$.*

Démonstration. L'élément $\alpha = 1 - g - g' = 1 - (123) - (124)$ est admissible pour la paire $(A_4, 1)$. Il est non inversible dans $k[A_4]$, son annulateur (à droite) est un k-espace vectoriel de dimension 3 et par exemple, $\beta = -(13)(24) + (14)(23) - (132) + (142) - (134) + (143)$ est un annulateur dont le fixateur sous l'action de A_4 est 1. On a de plus $\alpha'\beta = 0$ pour

$\alpha' = 1 - g' - g^2 - gg' = 1 - (124) - (132) - (13)(24)$. Les deux éléments α et α' sont donc admissibles et annulent le même générateur βx de L où $(s(x))_{s\in A_4}$ est une base normale de L. □

Exemple. D'après Schur, le polynôme $P(X) = X^4+4X^3+12X^2+24X+24$ est irréductible sur $\mathbb{Q}$ et de groupe de Galois A_4. En notant x_1, x_2, x_3, x_4 les racines de P et en posant $u = x_1x_2$, on obtient $\beta u = (x_1+x_2)(x_4-x_3)$. C'est un générateur du corps de décomposition de P dont le polynôme minimal $X^{12}+576X^{10}+115200X^8+11575296X^6+599851008X^4+13759414272X^2+12230590464$ a des racines qui vérifient les relations $a = b + c$ et $a = b' + c' + d'$.

Il est naturel à ce point de demander si la relation $a = b + c$ est possible dans le cas régulier pour tous les groupes dont l'ordre est un multiple de 6. La condition 6 divise $|G|$ n'est par contre pas nécessaire car d'après [6], A. Dubickas a démontré en 2001 que cette relation est possible pour les groupes affines $\mathrm{AGL}(1, p)$, p premier ≥ 5.

4. La relation $a = b + c + d$

Elle est donc possible pour le groupe alterné A_4 dans le cas régulier. On l'obtient également pour la paire (A_5, S_3) dans la section 5. Dans le cas abélien, elle est fréquente et lorsque le corps k est le corps $\mathbb{Q}$ des rationnels, de la proposition 2, on déduit le résultat suivant :

Proposition 4. *Soit G un groupe abélien.*
i) Si la relation $a = b+c+d$ est vraie pour le groupe G alors son ordre $|G|$ est pair.
ii) Si G est d'ordre pair et si G n'est pas de la forme $C_2 \times C_2$ ou $C_{2^k} \times C_{p^l}$ (p premier impair, $l \geq 0$) alors la relation $a = b + c + d$ est vraie pour le groupe G.

Démonstration. i) On suppose donc qu'il existe un élément admissible dans $\mathbb{Q}[G]$ de la forme $\alpha = 1 - s - t - u$. D'après la proposition 2, il existe un sous-ensemble I du groupe $\widehat{G}$ des caractères irréductibles de G qui engendre $\widehat{G}$ et qui annule α. Pour $\chi \in I$, la relation $\chi(\alpha) = 0$ s'écrit $1 = \xi + \xi' + \xi''$ où ξ, ξ', ξ'' sont des racines $|G|$-ièmes de l'unité. Il est connu [10] que seule une relation du type $1 = 1 + \xi + (-\xi)$ convient. L'ordre de G est donc pair puisque deux racines $|G|$-ièmes de l'unité sont opposées.

ii) Ce point repose sur la simple observation que si la relation est vraie pour un groupe G, elle l'est pour $G \times G'$. En effet, si $\chi_1, \ldots, \chi_k$ engendrent $\widehat{G}$ et annulent l'élément $\alpha = 1 - s - t - u$ de $\mathbb{Q}[G]$ alors en notant $\mu_1, \ldots, \mu_l$ des caractères qui engendrent $\widehat{G'}$ et en les étendant à $G \times G'$ en leur donnant la valeur 1 sur G, les caractères $\chi_1, \ldots, \chi_k, \chi_1\mu_1, \ldots, \chi_1\mu_l$ engendrent le

groupe des caractères irréductibles de $G \times G'$ et annulent $\alpha' = 1 - \bar{s} - \bar{t} - \bar{u}$ où pour $g \in G$, $\bar{g} = (g, 1) \in G \times G'$. Il ne reste donc qu'à vérifier la relation pour quelques groupes peu nombreux.

Si l'ordre de G admet plus de trois diviseurs premiers distincts, G possède un facteur H de la forme $C_{2^k} \times C_{p^l} \times C_{q^m}$. On note $a^i b^j c^f$ un élément de H où $a^{2^k} = b^{p^l} = c^{q^m} = 1$ et χ_1, χ_2, χ_3 les caractères de H qui envoient respectivement le triplet (a, b, c) sur $(\xi_1, 1, 1)$, $(1, \xi_2, 1)$ et $(1, 1, \xi_3)$ où $\xi_1^{2^k} = \xi_2^{p^l} = \xi_3^{q^m} = 1$. Les caractères χ_1, $\chi_1\chi_2$ et $\chi_1\chi_3$ engendrent $\widehat{H}$ et annulent $\alpha = 1 - b - c - bca^{2^{k-1}}$. La relation est donc vraie pour H et donc pour G.

Si l'ordre de G n'admet que deux diviseurs premiers distincts, G contient un facteur du type $C_{2^k} \times C_{p^l} \times C_{p^{l'}}$ ou $C_{2^k} \times C_{2^{k'}} \times C_{p^l}$ ou bien est de la forme $C_{2^k} \times C_{p^l}$. La même explication que dans le cas où $|G|$ admet trois diviseurs montre que la relation est vraie pour les groupes $C_{2^k} \times C_{p^l} \times C_{p^{l'}}$ et $C_{2^k} \times C_{2^{k'}} \times C_{p^l}$.

Si $|G|$ n'admet que 2 pour diviseur premier alors la relation est vraie pour $C_{2^k} \times C_{2^{k'}}$ $(k \geq 1,\ k' \geq 2)$ et par conséquent pour tout 2-groupe abélien différent de $C_2 \times C_2$ et C_{2^k}. En effet, notons $a^i b^j$ les éléments de $C_{2^k} \times C_{2^{k'}}$ $(a^{2^k} = b^{2^{k'}} = 1)$ et χ_1, χ_2 ses caractères qui envoient le couple (a, b) sur $(\xi_1, 1)$ et $(1, \xi_2)$ où $\xi_1^{2^k} = \xi_2^{2^{k'}} = 1$. Les caractères χ_1 et $\chi_1\chi_2$ engendrent $\widehat{G}$ et annulent $\alpha = 1 - b - b^{2^{k'-1}+1} - a^{2^{k-1}} b^{2^{k'-1}}$. □

Remarque. La relation $a = b + c + d$ n'a pas lieu pour les groupes $C_2 \times C_2$ et C_{2^k}. D'après l'étude de quelques exemples, elle ne semble pas avoir lieu non plus pour les groupes de la forme $C_{2^k} \times C_{p^l}$ où p est premier impair. Connaître ce dernier point réglerait totalement la question.

Exemples. 1) Pour $G = C_2 \times C_4 =< s, t, s^2 = t^4 = 1 >$, les caractères χ_1 et χ_2 qui envoient respectivement s et t sur les couples $(-1, 1)$ et $(1, i)$ engendrent le groupe $\hat{G}$ et annulent $\alpha = 1 + t^2 + st - t$. Ce dernier est donc admissible et $\alpha\beta = 0$ pour $\beta = -t^2 - t^3 + s + st$. Le groupe G est par exemple le groupe de Galois de l'extension galoisienne $L = \mathbb{Q}(\sqrt{2}, \mathrm{e}^{\frac{2i\pi}{5}})$. En posant $x = \sqrt{2} + \mathrm{e}^{\frac{2i\pi}{5}}$, βx est un générateur de L dont les conjugués vérifient la relation $a = b + c + d$. Le polynôme minimal de βx est $X^8 - 108X^6 + 5614X^4 - 155932X^2 + 1819801$.

2) Pour $G = C_2 \times C_6 =< s, t, s^2 = t^6 = 1 >$, $\alpha = t^4 + t + s - 1$ est admissible et $\beta = -2 - 2t - t^2 + t^3 + t^4 - s - st + 2st^3 + 2st^4 + st^5$ est un annulateur de α dans $\mathbb{Q}[G]$. L'extension $L = \mathbb{Q}(i, \mathrm{e}^{\frac{2i\pi}{7}})$ est galoisienne de groupe G et en posant $x = i + \mathrm{e}^{\frac{2i\pi}{7}}$, βx est un générateur de L dont les conjugués vérifient la relation $a = b + c + d$. Le polynôme minimal de βx est $X^{12} + 482X^{10} + 73991X^8 + 4081020X^6 + 87713151X^4 + 590948098X^2 + 414407449$.

5. Les relations obtenues avec l'anneau de Schur A

Nous revenons dans cette partie sur les relations que l'on peut obtenir avec l'anneau $A = e_H k[G] e_H$. Des détails sur cette approche sont présents dans [9]. Si on note $(s_1, s_2, \ldots, s_n)$ un système de représentants des classes à gauche de G modulo H et $I_1, I_2, \ldots, I_r$ les différentes orbites de G/H sous l'action de H (l'entier r s'appelle le *rang* de la paire (G, H), l'orbite I_1 est celle de $\{H\}$ et réduite à $\{H\}$), la k-algèbre A est de dimension r et les

$$f_i = e_H s_{i'} e_H = \frac{1}{d_i} \sum_{s \in I_i} s e_H$$

où $s_{i'}$ est un élément quelconque de l'orbite I_i et d_i son ordre, en forment une base. Cette algèbre est commutative pour $r \leq 3$ et admet $f_1 = e_H$ pour élément unité. On étudie dans la suite cette algèbre pour la paire $(G, H) = (A_m, S_{m-2})$ et $m \geq 5$.

Le groupe alterné A_m agit sur les couples de $\{1, 2, \ldots, m\}$ et les éléments du fixateur H de $\{m-1, m\}$ sont ceux de S_{m-2} couplés ou non à la transposition $(m-1, m)$. La paire (A_m, S_{m-2}) est primitive de degré $d = m(m-1)/2$ et de rang 3. Elle figure dans les tables de [2]. Les calculs dans A se font de la manière suivante.

Proposition 5. *i) Les sous-degrés de la paire (A_m, S_{m-2}), c'est à dire les longueurs des orbites I_1, I_2 et I_3 sont $n_1 = 1$, $n_2 = 2(m-2)$ et $n_3 = (m-2)(m-3)/2$.*
ii) Les vecteurs de base f_i associés aux trois orbites I_1, I_2 et I_3 vérifient :

$$f_2^2 = \frac{1}{2(m-2)} \Big(f_1 + (m-2) f_2 + (m-3) f_3 \Big)$$

$$f_3^2 = \frac{2}{(m-2)(m-3)} \Big(f_1 + 2(m-4) f_2 + \frac{(m-5)(m-4)}{2} f_3 \Big)$$

$$f_2 f_3 = \frac{1}{2(m-2)} \Big(4 f_2 + 2(m-4) f_3 \Big) \ .$$

Démonstration. Pour $i = 1, 2, \ldots, m-2$, on considère des éléments d'ordre 2 $(i, m-1)(k, l)$ et $(i, m)(k', l')$ où k, l, k', l' appartiennent à $\{1, 2, \ldots, m-2\}$ et sont choisis de telle sorte que ces produits de transpositions soient des produits disjoints. On note s_i $(i = 1, 2, \ldots, 2(m-2))$ ces $2(m-2)$ éléments. On considère d'autre part les éléments $t_{i,j} = (i, m-1)(j, m)$ pour $1 \leq i < j \leq m-2$. Ils sont au nombre de $(m-2)(m-3)/2$. On vérifie alors aisément que les s_i et les $t_{i,j}$ forment un système de représentants de A_m/S_{m-2} et que ces deux ensembles constituent les deux orbites non triviales de A_m/S_{m-2} sous l'action de S_{m-2}. Ce qui prouve i).

On a alors $f_2 = e_H s_1 e_H$ où $s_1 = (1, m-1)(2,3)$ et $f_3 = e_H t_{1,1} e_H$. Ainsi

$$f_2^2 = e_H s_1 e_H s_1 e_H = \frac{1}{2(m-2)} e_H s_1 (s_1 + s_2 + \cdots + s_{2(m-2)}) e_H$$

et on vérifie sans difficulté le résultat annoncé. Il en va de même pour les calculs de f_3^2 et $f_2 f_3$. □

La connaissance de ces lois permet d'annoncer le résultat suivant.

Théorème 2. *L'élément* $f_1 - \dfrac{(m-2)(m-3)}{2} f_3$ *est admissible. Autrement dit, la relation* $x_1 = \sum_{i \in I_3} x_i$ *est une relation pour la paire primitive* (A_m, S_{m-2}).

Démonstration. Cela résulte du lemme suivant :

Lemme 1. *Dans le cas de la paire* $(G, H) = (A_m, S_{m-2})$*, pour qu'un élément* $\alpha = af_1 + bf_2 + cf_3$ *soit inversible dans* A *il faut et il suffit qu'il soit de poids non nul et que* $(b - 2a(m-2))(m-4)(4c - b(m-3))$ *et* $((2a-b)(m-2) + 4c)(2c - a(m-2)(m-3))$ *soient distincts.*

Ceci exprime simplement la non nullité du déterminant de la multiplication dans A par l'élément α.

Ainsi, d'après le lemme 1, $f_1 - \dfrac{(m-2)(m-3)}{2} f_3$ est non inversible dans A. Comme il est de poids non nul et que la paire (G, H) est primitive, c'est un élément admissible de A. □

Remarque. L'élément $f_1 - 2(m-2)f_2$ à qui il correspondrait la relation $x_1 = \sum_{i \in I_2} x_i$ n'est admissible que pour $m = 5$.

Exemple. Pour $m = 5$, les sous-degrés sont 1, 6 et 3. Si $s_1, s_2, \ldots, s_{10}$ constituent un système de représentants des classes à gauche de A_5 modulo S_3 telles que les trois orbites sous l'action de S_3 soient $\{s_1\}$, $\{s_2, s_3, s_4\}$ et $\{s_5, \ldots, s_{10}\}$, l'élément $\alpha = (s_1 - s_2 - s_3 - s_4)e_H$ est un élément admissible de A. Un annulateur de α dans A est $\beta = (3s_1 + (s_2 + s_3 + s_4) - (s_5 + s_6 + \cdots + s_{10}))e_H$. Alors si $P(X) = \prod_1^5 (X - x_i)$ est de groupe de Galois A_5, $x = x_1x_2x_3$ appartient à L^H puisque $H = S_3 =< (12)(45), (123) >$ et $\beta x = 3x_1x_2x_3 + x_4x_5(x_1 + x_2 + x_3) - (x_4 + x_5)(x_1x_2 + x_1x_3 + x_2x_3)$ est non nul. C'est donc un générateur de L^H puisque H est maximal. En partant du polynôme $P(X) = X^5 - 9X^4 + 44X^3 - 157X^2 + 307X - 465$ de groupe A_5, le polynôme minimal de βx est

$$\begin{gathered} X^{10} - 148749X^8 + 15725624X^7 + 5649336882X^6 \\ -1346967621352X^5 + 127922759167534X^4 \\ -9311396069853400X^3 + 416397211097230909X^2 \\ +2353276107262971784X + 40672746688427709399. \end{gathered}$$

C'est un polynôme de groupe A_5 dont quatre racines vérifient la relation $a = b + c + d$.

Ce type de relations simples n'est pas systématique pour les paires primitives de rang 3. La connaissance des lois de multiplication dans l'anneau A pour de nombreuses paires (G, H) de rang 3 montre que ces relations semblent peu fréquentes. On donne dans la suite ces lois de multiplication.

On note $1, n_2, n_3$ les longueurs des trois orbites I_i et pour $g \in G$, on pose $I_i^g = \{gs,\ s \in I_i\}$. Ainsi si on note $I_2 = \{s_1, \ldots, s_{n_2}\}$, dans l'expression

$$f_2^2 = (e_H s_1 e_H)^2 = \frac{1}{n_2} e_H s_1 (s_1 + \cdots + s_{n_2}) e_H = \frac{1}{n_2}(\alpha f_1 + \beta f_2 + \gamma f_3),$$

$\beta = |I_2 \cap I_2^g|$ pour $g \in I_2$.

On introduit alors les quatre constantes λ_2, λ_3, μ_2 et μ_3 définies comme suit : $|I_2 \cap I_2^g| = \lambda_2$ si $g \in I_2$ et μ_2 si $g \in I_3$ et de même $|I_3 \cap I_3^g| = \lambda_3$ si $g \in I_3$ et μ_3 si $g \in I_2$. Ces quatre constantes sont clairement définies et indépendantes de l'élément choisi dans une orbite. Elles sont introduites dans [7], premier d'une série d'articles où Higman classifie certains groupes de rang 3 par leurs sous-degrés n_2 et n_3. Higman montre dans [7] et [8] que ces constantes vérifient $\lambda_3 = n_3 - n_2 + \mu_2 - 1$ et $\mu_3 = n_3 - n_2 + \lambda_2 + 1$ lorsque $|G|$ est pair et $\lambda_2 = \lambda_3 = \mu_2 = \mu_3$ lorsque $|G|$ est impair. Sous ces notations, on a

$$f_2^2 = \frac{1}{n_2}(*f_1 + \lambda_2 f_2 + *f_3), \quad f_3^2 = \frac{1}{n_3}(*f_1 + *f_2 + \lambda_3 f_3)$$

et

$$f_2 f_3 = \frac{1}{n_2}(*f_1 + \mu_2 f_2 + *f_3) = \frac{1}{n_3}(*f_1 + *f_2 + \mu_3 f_3)$$

où chaque * désigne un nombre entier. On peut donner les composantes sur f_1 dans ces calculs. Dans ces trois calculs, par exemple dans celui de

$$f_2^2 = (e_H s_1 e_H)^2 = \frac{1}{n_2} e_H s_1 (s_1 + \cdots + s_{n_2}) e_H\ ,$$

il apparait une composante sur f_1 lorsque $s_1 s_i \in H$. Il ne peut donc y avoir au plus qu'une composante sur f_1 puisque sinon $s_1 s_i$, $s_1 s_j$ et par suite $s_i^{-1} s_j$ seraient dans H pour $i \neq j$. Ainsi dans les calculs ci-dessus, la composante sur f_1 est 0 ou 1. Par ailleurs, de l'égalité $f_1 + n_2 f_2 + n_3 f_3 = n e_G$ on tire $f_2 + n_2 f_2^2 + n_3 f_2 f_3 = n e_G$ et $f_3 + n_2 f_2 f_3 + n_3 f_3^2 = n e_G$. La composante sur f_1 est donc ou bien dans f_2^2 et f_3^2 ou bien dans $f_2 f_3$. Les relations de Higman rappelées ci-dessus assurent que la composante en f_1 est dans f_2^2 et f_3^2 lorsque $|G|$ est pair et dans $f_2 f_3$ lorsque $|G|$ est impair. Comme enfin f_2 et f_3 sont de poids 1, on obtient les règles de calcul suivantes.

Proposition 6. *Les vecteurs de base f_i associés aux trois orbites I_1, I_2 et I_3 vérifient les relations*

$$f_2^2 = \frac{1}{n_2}\big(f_1+\lambda_2 f_2+(n_2-\lambda_2-1)f_3\big), \quad f_3^2 = \frac{1}{n_3}\Big(f_1+(n_3-\lambda_3-1)f_2+\lambda_3 f_3\Big)$$

et

$$f_2 f_3 = \frac{1}{n_2}\Big(\mu_2 f_2 + (n_2-\mu_2)f_3\Big) = \frac{1}{n_3}\Big((n_3-\mu_3)f_2+\mu_3 f_3\Big)$$

lorsque $|G|$ est pair et

$$f_2^2 = \frac{1}{n_2}\big(\frac{n_2-1}{2}f_2 + \frac{n_2+1}{2}f_3\big), \quad f_3^2 = \frac{1}{n_2}\Big(\frac{n_2+1}{2}f_2 + \frac{n_2-1}{2}f_3\Big)$$

et

$$f_2 f_3 = \frac{1}{n_2}\Big(f_1 + \frac{n_2-1}{2}f_2 + \frac{n_2-1}{2}f_3\Big)$$

lorsque $|G|$ est impair.

En effet, d'après [7] et [8], lorsque $|G|$ est impair, $n_2 = n_3$ et $\lambda_2 = \lambda_3 = \mu_2 = \mu_3 = \dfrac{n_2-1}{2}$.

La connaissance des constantes λ_2, λ_3, μ_2 et μ_3 permet donc de connaitre les éléments inversibles de l'anneau A et dans le cas primitif de connaitre les éléments admissibles de A. Higman donne ces constantes pour certains groupes classiques. Les relations simples $a = b + c + \cdots + t$ obtenues pour la paire (A_m, S_{m-2}) semblent rares. Par exemple, pour $PSL_4(3)$ qui admet une représentation primitive de rang 3 en degré 130 [2], les sous-degré sont $1, 48, 81$ et aucun des deux éléments f_1-48f_2 et f_1-81f_3 n'est admissible. Il en est de même pour $U_3(5)$ qui admet une représentation primitive de rang 3 en degré 50. On peut se demander quelles paires de rang 3 fournissent de telles relations.

Références

[1] J. D. Dixon, *Polynomials with relations between their roots.* Acta Arithmetica **82.3** (1997), 293–302.

[2] J. D. Dixon and B. Mortimer, *Permutation Groups.* Springer, New York, 1996.

[3] M. Drmota and M. Skalba, *Relations between polynomial roots.* Acta Arithmetica **71.1** (1995), 65-77.

[4] K. Girstmair, *Linear dependence of zeros of polynomials and construction of primitive elements.* Manuscripta Math. **39** (1982), 81–97.

[5] K. Girstmair, *Linear relations between roots of polynomials.* Acta Arithmetica **89.1** (1999), 53–96.

[6] K. Girstmair, *The Galois relation $x_1 = x_2 + x_3$ and Fermat over finite fields.* Acta Arithmetica **124.4** (2006), 357–370.

[7] D. G. Higman, *Finite permutation groups of rank* 3. Math. Zeitschr. **86** (1964), 145–156.

[8] D. G. Higman, *Primitive rank* 3 *groups with a prime subdegree.* Math. Zeitschr. **91** (1966), 70–86.

[9] F. Lalande, *Relations linéaires entre les racines d'un polynôme et anneaux de Schur*. Ann. Sci. Math. Québec **27.2** (2003), 169–175.

[10] H. B. Mann, *On linear relations between roots of unity*. Mathematika **12** (1965), 107–117.

Franck Lalande
38, grande rue
89140 Gisy les nobles, France
E-mail: lalande072@orange.fr