THEORIE DES NOMBRES
BESANCON

Années 1989/90-1990/91

CONSTRUCTION EXPLICITE DE 2-GROUPES EXTRA-SPECIAUX COMME GROUPES DE GALOIS SUR $\mathbb{Q}(T)$

Leila SCHNEPS

Construction explicite de 2-groupes extra-spéciaux comme groupes de Galois sur $\mathbf{Q}(T)$

Leila Schneps

Soit C_2 le groupe cyclique d'ordre 2. Dans cet article nous construisons explicitement en tant que groupes de Galois sur le corps $\mathbf{Q}(T)$ tous les 2-groupes G vérifiant une suite exacte:

$$1 \to C_2 \to G \to C_2^n \to 1$$

pour tout entier $n \geq 1$. Les 2-groupes dits 'extra-spéciaux' sont ceux de ces groupes ayant centre et sous-groupe commutateur isomorphe à C_2; la structure de ces groupes a été examinée de près par Lam et Smith dans l'article [L-S]. J'aimerais remercier Jack Sonn pour m'avoir montré cet article au cours d'une des discussions intéressantes que j'ai eues avec lui à ce sujet.

Si G et H sont deux groupes avec involution centrale distinguée, soit $H \times G$ leur produit et HG leur produit 'central', c'est-à-dire le quotient du produit de ces groupes modulo l'identification de leurs involutions centrales. Nous écrivons G^n pour le produit de n copies de G et $G^{(n)}$ pour leur produit central (remarquons que ce produit est associatif). Notons D le groupe diédral d'ordre 8, Q le groupe des quaternions d'ordre 8 et C le groupe cyclique d'ordre 4. Soit K le corps $\mathbf{Q}(T)$. Notre théorème principal est le suivant:

Théorème 1: *(i) Il existe des éléments $d_1, \ldots, d_n$ de K, indépendants dans $K^*/(K^*)^2$ et tels que les algèbres de quaternions (d_1, d_1), (d_2, d_2) et (d_i, d_{i+1}) pour $1 \leq i \leq n$ sont toutes décomposées sur K.*

(ii) Soient $d_1, \ldots, d_n$ comme dans le (i) et posons $L = K(\sqrt{d_1}, \ldots, \sqrt{d_n})$. Alors pour tout extension G de C_2^n par C_2 on peut trouver de façon explicite un élément γ_G dans L tel que $L(\sqrt{\gamma_G})$ soit galoisien sur K de groupe de Galois G.

Avant de démontrer le théorème, rappelons la classification de toutes les extensions de C_2^n par C_2.

Proposition 2: *(i) Chaque extension de C_2^n par C_2 est isomorphe à l'un des groupes*

suivants, qui sont mutuellement non-isomorphes:

$$D^{(i)} \times C_2^j \quad \text{ou} \quad QD^{(i-1)} \times C_2^j \quad \text{avec} \quad 2i+j=n \quad \text{ou} \quad CD^{(i)} \times C_2^j \quad \text{avec} \quad 2i+j+1=n.$$

(ii) Si n est pair, il y a $(3n+2)/2$ extensions possibles de C_2^n par C_2 à isomorphisme près; si n est impair il y en a $(3n+1)/2$. De plus, il y a exactement deux 2-groupes extra-spéciaux d'ordre 2^{n+1} si n est pair et aucun si n est impair.

Démonstration: On commence par remarquer que les groupes donnés dans le (i) sont tous extensions de C_2^n par C_2 et qu'ils sont bien non-isomorphes, ce qui se démontre en comparant le nombre de leurs éléments d'ordre 2 et l'ordre de leurs centres. Il reste donc à démontrer qu'on a bien toutes les extensions de C_2^n par C_2 possibles. Nous allons utiliser les liens entre les extensions de C_2^n par C_2 et les formes quadratiques en n variables sur $\mathbf{Z}/2\mathbf{Z}$. Les deux lemmes suivants sont bien connus:

Lemme 3: *Il y a bijection entre les classes d'isomorphisme des extensions de C_2^n par C_2 et les classes d'équivalence des formes quadratiques en n variables sur $\mathbf{Z}/2\mathbf{Z}$.*

Démonstration: A chaque forme quadratique $Q(x)$ en n variables sur $\mathbf{Z}/2\mathbf{Z}$ on associe un groupe G de la façon suivante. Soit $Q'(x,y) = Q(x+y) - Q(x) - Q(y)$ la forme bilinéaire associée à $Q(x)$. Soit $e_1, \ldots, e_n$ une base de C_2^n en tant que C_2-module et identifions l'élément non-trivial de C_2 avec -1. Alors le groupe G est engendré par des éléments $e_0, \tilde{e}_1, \tilde{e}_2, \ldots, \tilde{e}_n$ vérifiant les relations suivantes: $e_0^2 = 1$ et cet élément est central dans G (on l'identifie aussi avec -1), $\tilde{e}_i^2 = e_0^{Q(e_i)}$ pour $i = 1, \ldots, n$ et $e_i e_j e_i^{-1} e_j^{-1} = e_0^{Q'(e_i,e_j)}$. Il est facile de vérifier à partir de cette définition que si on construit les deux groupes associés à deux formes quadratiques équivalentes, les groupes seront isomorphes. De plus, étant donné une extension de C_2^n par C_2 par les relations vérifées par ses générateurs, on retrouve la forme quadratique associée.

Lemme 4: *Toute forme quadratique en n variables sur $\mathbf{Z}/2\mathbf{Z}$ est équivalente à une forme quadratique d'une des formes suivantes, qui sont deux à deux non-équivalentes:*

$$\textit{Si } n \textit{ est pair} \begin{cases} \sum_{k=1}^{n/2} e_k x_{2k-1} x_{2k} \\ \quad \textit{ou} \\ x_1^2 + \sum_{k=1}^{n/2-1} e_k x_{2k} x_{2k+1} \\ \quad \textit{ou} \\ x_1^2 + x_1 x_2 + x_2^2 + \sum_{k=2}^{n/2} e_k x_{2k-1} x_{2k}; \end{cases}$$

$$\textit{Si } n \textit{ est impair} \begin{cases} \sum_{k=1}^{(n-1)/2} e_k x_{2k-1} x_{2k} \\ \quad \textit{ou} \\ x_1^2 + \sum_{k=1}^{(n-1)/2} e_k x_{2k} x_{2k+1} \\ \quad \textit{ou} \\ x_1^2 + x_1 x_2 + x_2^2 + \sum_{k=1}^{(n-1)/2} e_k x_{2k-1} x_{2k}, \end{cases}$$

où les nombres e_k valent 1 pour $1 \leq k \leq i$ et 0 pour $i < k \leq n/2$ si n est pair et pour $i < k \leq (n-1)/2$ si n est impair, et i varie entre les deux limites de la somme.

Démonstration: La première assertion se démontre par récurrence. Pour voir que les formes quadratiques données sont deux-à-deux non-équivalentes, il suffit d'après le lemme 3 de calculer leurs groupes associés et de constater que ces groupes sont deux-à-deux non-isomorphes. En l'ordre, elles correspondent aux groupes $D^{(i)} \times C_2^j$, $CD^{(i)} \times C_2^j$, $QD^{(i-1)} \times C_2^j$ (pour n pair et impair); on a constaté au début de la démonstration que ces groupes sont non-isomorphes.

On compte selon le lemme 4 exactement $(3n+1)/2$ ou $(3n+2)/2$ classes d'isomorphisme de formes quadratiques sur $\mathbf{Z}/2\mathbf{Z}$ selon la parité de n, et exactement le même nombre de groupes décrits dans le (i), ce qui permet de conclure qu'on a bien décrit toutes les extensions de C_2^n par C_2. Pour terminer la démonstration de la proposition 2, nous déterminons quels sont les groupes extra-spéciaux, c'est-à-dire ayant centre d'ordre 2. Dans chaque cas il faut $j = 0$, ce qui donne les trois possibilités $D^{(n/2)}$ ou $QD^{(\frac{n-2}{2})}$ pour n pair, et $CD^{(\frac{n-1}{2})}$ pour n impair. Ce dernier ayant un centre d'ordre 4, nous obtenons le résultat énoncé. Ce résultat (et bien plus) a été démontré par Lam et Smith dans l'article [L-S].

Passons maintenant à la démonstration du théorème 1. Le lemme suivant suffit pour démontrer le (i).

Lemme 5: *Il existe $d_1, \ldots, d_n$ dans K tels que $\mathrm{Gal}\big(K(\sqrt{d_1}, \ldots, \sqrt{d_n})/K\big) \simeq C_2^n$ et les conditions suivantes sont vérifiées: les algèbres de quaternions (d_1, d_1), (d_2, d_2) et (d_i, d_{i+1}) pour $i \geq 1$ sont toutes décomposées sur K.*

Démonstration: Il suffit de montrer qu'on peut trouver d_1 et d_2 satisfaisant simultanément les conditions (d_1, d_1), (d_2, d_2) et (d_1, d_2) décomposées car ensuite les autres conditions sont satisfaites en choisissant successivement de nouveaux d_i non-carrés et indépendants des précédents, tels que (d_{i-1}, d_i) soit décomposée. Ceci est toujours possible puisqu'il suffit de prendre d_i de la forme $\frac{1-x^2 d_{i-1}}{y^2}$ pour x et y dans K. La condition (d_i, d_i) décomposée équivaut au fait que d_i est somme de deux carrés dans K. Il suffit donc de montrer qu'on peut toujours trouver d_1 et d_2 sommes de deux carrés tels que (d_1, d_2) soit décomposée et que le corps $K(\sqrt{d_1}, \sqrt{d_2})$ soit biquadratique sur K. Mais de tels d_1 et d_2 sont paramétrés par les équations:

$$d_1 = (-1 + u^2 + v^2 + w^2)^2 + 4u^2$$

$$d_2 = 4v^2 + 4w^2.$$

Comme alors $d_1 + d_2 = (1 + u^2 + v^2 + w^2)^2$, c'est un carré et donc (d_1, d_2) est décomposée.

Passons maintenant au (ii). On pose $L = K(\sqrt{d_1}, \ldots, \sqrt{d_n})$ pour $d_1, \ldots, d_n$ comme dans le lemme 5. Pour chaque extension G de C_2^n par C_2, soit $\tilde{G}$ le produit (usuel) de tous les groupes apparaîssant dans le produit définissant G, par exemple si $G = QD^{(i-1)} \times C_2^j$, alors $\tilde{G} = Q \times G^{i-1} \times C_2^j$. Evidemment, G est un quotient de $\tilde{G}$. Donc si L admet une extension qui est galoisienne sur K de groupe de Galois $\tilde{G}$, il admet aussi une extension quadratique galoisienne sur K de groupe de Galois G. Nous allons montrer que c'est le cas en construisant explicitement des $\tilde{G}$-extensions de K contenant L, et ensuite construire les G-extensions en donnant explicitement les éléments γ_G annoncés dans le théorème.

Nous commençons par le cas $\tilde{G} = D^i \times C_2^j$ et nous procédons de la façon suivante: nous allons plonger chacune des i extensions biquadratiques $K(\sqrt{d_{2k-1}}, \sqrt{d_{2k}})$ pour $1 \leq k \leq i$ dans des corps galoisiens su K ayant groupe de galois D. On sait que ceci peut se faire si et seulement si les i algèbres (d_{2k-1}, d_{2k}) sont toutes décomposées car ce sont les obstructions aux problèmes de plongement associés à ces extensions, et on sait que ces algèbres sont bien décomposées par le lemme 5. Ceci implique que pour chaque k, il existe des nombres x_k et y_k dans K tels que $d_{2k-1}x_k^2 + d_{2k}y_k^2 = 1$. Posons $\delta_k = \frac{-1}{2x_k} + \frac{\sqrt{d_{2k-1}}}{2}$. Alors on constate facilement que $K(\sqrt{\delta_k}, \sqrt{d_{2k}})$ est galoisien sur K de groupe de Galois D (le polynôme ayant ce corps comme corps de décomposition est $X^4 + \frac{1}{x_k}X^2 + \frac{d_{2k}y_k^2}{4x_k^2}$). Le corps $L(\sqrt{\delta_1}, \ldots, \sqrt{\delta_i})$ est bien de groupe de Galois $\tilde{G}$ sur K.

Le cas où $\tilde{G} = Q \times D^{i-1} \times C_2^j$ est identique sauf pour la construction de $\delta_1 \in K(\sqrt{d_1}, \sqrt{d_2})$, qui devra donner une extension de groupe de Galois Q sur K. Pour qu'un tel δ_1 existe, il faut que l'obstruction au problème de plongement soit décomposée: or cette obstruction est donnée par $(d_1, d_1)(d_2, d_2)(d_1, d_2)$ ce qui est décomposée par le lemme 5. Pour la construction explicite de δ_1, voir [W] ou [S].

Passons au cas $\tilde{G} = C \times D^i \times C_2^j$. On commence par construire une extension quadratique de $K(\sqrt{d_1})$ ayant groupe de Galois C sur K; ceci est possible car l'obstruction est donnée par (d_1, d_1). Puisque cette algèbre est décomposée, il existe x_0 et y_0 dans K tels que $-x_0^2 + d_1y_0^2 = 1$. Posons $\delta_0 = x_0d_1 + y_0\sqrt{d_1}$. Le corps $K(\sqrt{\delta_0})$ est galoisien sur K de groupe de Galois C. Ensuite on construit des D-extensions des corps biquadratiques $K(\sqrt{d_{2k}}, \sqrt{d_{2k+1}})$ pour $1 \leq k \leq i$ en posant $\delta_k = \frac{-1}{2x_k} + \frac{\sqrt{d_{2k}}}{2}$ pour x_k (et y_k) vérifiant $d_{2k}x_k^2 + d_{2k+1}y_k^2 = 1$, et on rajoute $\sqrt{\delta_0}, \ldots, \sqrt{\delta_i}$ au corps L pour obtenir une extension galoisienne de K de groupe de Galois $\tilde{G}$.

Lemme 6: *Posons*

$$\gamma_G = \begin{cases} \delta_0 \cdots \delta_i & si\ G = CD^{(i)} \times C_2^j \\ \delta_1 \cdots \delta_i & si\ G = D^{(i)} \times C_2^j\ ou\ QD^{(i-1)} \times C_2^j. \end{cases}$$

Alors $L(\sqrt{\gamma_G})$ est galoisien sur K de groupe de Galois G.

Démonstration: Il est clair qu'on obtient ainsi le bon quotient de $\tilde{G}$.

Si l'on veut démontrer que les 2-groupes extra-spéciaux se réalisent comme groupes de Galois d'extensions régulières sur $\mathbf{Q}(T)$ sans demander une construction explicite de ces extensions, on peut le faire d'une façon complètement différente: ça découle en effet d'un théorème beaucoup plus général qui est connu mais ne se trouve pas, à notre connaissance, dans la littérature.

Théorème 7: *Tout groupe G qui est une extension centrale d'un groupe abélien B par un groupe abélien A se réalise comme groupe de Galois d'une extension régulière de $\mathbf{Q}(T)$.*

Démonstration: Nous allons démontrer le résultat par récurrence sur l'ordre du groupe G. L'énoncé est clair quand $G = \{1\}$. Soit M un sous-groupe maximal de G et x un élément de G tel que G est engendré par M et x. Soit C le sous-groupe de G engendré par A et x. Alors C est un sous-groupe abélien de G puisque A est central, et en plus, ce sous-groupe est distingué puisqu'il est l'image inverse d'un sous-groupe distingué de B (forcément distingué puisque B est abélien). Donc G est un quotient du produit semi-direct $C \rtimes M$. Soit $B' \subset B$ l'image de M dans B. Le noyau de l'application $M \to B'$ est égal à $A \cap M$; c'est donc un groupe abélien et M vérifie la suite centrale

$$1 \to A \cap M \to M \to B' \to 1.$$

Donc par l'hypothèse de récurrence, M est réalisable comme groupe de Galois d'une extension régulière de $\mathbf{Q}(T)$, ce qui implique que G l'est (voir [M], Satz 2, p. 230).

Ce théorème démontre l'existence d'éléments $d_1, \ldots, d_n$ de $\mathbf{Q}(T)$ tels que (d_i, d_j) soit décomposée pour $1 \leq i, j \leq n$: c'est bien plus fort que les conditions décrites dans le théorème 1. Il semble difficile de trouver explicitement de tels d_i. L'algèbre (d_i, d_i) est décomposée si et seulement si d_i est somme de deux carrés, et c'est un problème ouvert de savoir si on peut choisir tous les d_i de la forme $T^2 + a_i^2$ pour $a_i \in \mathbf{Q}$. Ce problème est équivalent au problème de trouver des $a_i \in \mathbf{Q}$ tels que $a_i^2 - a_j^2$ soit toujours un carré quand $a_i^2 > a_j^2$ (voir [G], p. 99-103). On sait depuis Euler qu'il existe des solutions pour $n = 3$, par exemple on pose $a_1 = 697$, $a_2 = 185$ et $a_3 = 153$ et on trouve $a_1^2 - a_2^2 = 672^2$, $a_1^2 - a_3^2 = 680^2$ et $a_2^2 - a_3^2 = 104^2$ (voir [E], Chap. XIV, n° 236-7, pp. 439-441).

Références

[E] Euler, L. Elements of Algebra (Rev. J. Hewlett, trans.) Springer-Verlag (1984).

[G] Guy, R.K. Unsolved Problems in Number Theory, Springer-Verlag 1981.

[L-S] Lam, T.Y. et Smith, T. On the Clifford-Littlewood-Eckmann Groups: a new look at periodicity mod 8. *Rocky Mtn. Jour. Math.* **19**, N. 3 (1989), p. 749-786.

[M] Matzat, B. H. *Konstruktive Galoistheorie*, LNM 1284, Springer-Verlag.

[S] Schneps, L. $\tilde{D}_4$ et $\hat{D}_4$ comme groupes de Galois. *C. R. Acad. Sci. Paris*, t. **308**, Série I (1989), p. 33-36.

[W] Witt, E. Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f. *J. reine angew. math.* **174**, 1935, p. 237-245.

A partir de Octobre 1991

Faculté des Sciences
Laboratoire de Mathématiques
URA CNRS 741
25030 Besançon Cédex