Math. Z. 119, 345–348 (1971)

Deux groupes finis distincts ayant la même algèbre de groupe sur tout corps

EVERETT C. DADE

Nous construirons deux groupes finis G_1 et G_2 ayant les propriétés suivantes:

(1a) *Le groupe G_1 n'est pas isomorphe au groupe G_2.*

(1b) *Pour tout corps k, l'algèbre de groupe kG_1 de G_1 sur k est isomorphe à l'algèbre de groupe kG_2.*

Ces groupes forment un contre-exemple à une conjecture bien connue (voir le problème 2* à la p. 144 de [1]), qui niait justement la possibilité de l'existence de tels groupes.

Les groupes G_1 et G_2 étant metabéliens, on sait, d'après un théorème non-publié de Whitcomb, que leurs algèbres de groupe ZG_1 et ZG_2 sur l'anneau Z des entiers ne peuvent pas être isomorphes. Donc la conjecture qu'un groupe fini G est déterminé par son algèbre ZG reste toujours ouverte.

On commence avec deux entiers premiers p et q tels que:

$$q \equiv 1 \pmod{p^2}. \tag{2}$$

Evidemment l'entier premier q est impair. Donc les deux groupes non-commutatifs d'ordre q^3 ont les présentations:

$$Q_1 = \langle \rho_1, \sigma_1, \tau_1 | \rho_1^q = \sigma_1^q = \tau_1^q = 1, [\rho_1, \sigma_1] = \tau_1, [\rho_1, \tau_1] = [\sigma_1, \tau_1] = 1 \rangle, \tag{3a}$$

$$Q_2 = \langle \rho_2, \sigma_2, \tau_2 | \rho_2^q = \tau_2^q = 1, \sigma_2^q = \tau_2, [\rho_2, \sigma_2] = \tau_2, [\rho_2, \tau_2] = [\sigma_2, \tau_2] = 1 \rangle, \tag{3b}$$

où, comme d'habitude, $[\alpha, \beta]$ est le commutateur $\alpha^{-1}\beta^{-1}\alpha\beta$, pour tout α, β.

Soient $\langle \pi_1 \rangle, \langle \pi_2 \rangle$ des groupes cycliques d'ordres p^2 et p, respectivement. La condition (2) implique l'existence d'un entier w tel que:

$$w \not\equiv 1, \quad w^p \equiv 1 \pmod{q^2}. \tag{4}$$

Pour tout $i, j = 1, 2$, on définit une opération du groupe $\langle \pi_i \rangle$ comme automorphismes du groupe Q_j par:

$$\rho_j^{\pi_i} = \rho_j, \quad \sigma_j^{\pi_i} = \sigma_j^w, \quad \tau_j^{\pi_i} = \tau_j^w. \tag{5}$$

On obtient ainsi quatre produits semi-directs $\langle\pi_i\rangle Q_j$. Les groupes G_1 et G_2 sont les produits directs:

$$G_1=\langle\pi_1\rangle Q_1\times\langle\pi_2\rangle Q_2, \quad G_2=\langle\pi_1\rangle Q_2\times\langle\pi_2\rangle Q_1 \tag{6}$$

de ces produits semi-directs.

Il reste à démontrer que G_1 et G_2 ont les propriétés (1).

Démonstration de (1a). De (3) et (5) on déduit que le groupe dérivé G_i' est égal à $\langle\sigma_1,\tau_1\rangle\times\langle\sigma_2,\tau_2\rangle$, pour tout $i=1,2$. Mais $\langle\sigma_1,\tau_1\rangle$ est élémentaire, tandis que $\langle\sigma_2,\tau_2\rangle=\langle\sigma_2\rangle$ est cyclique d'ordre q^2. Donc le sous-groupe $(G_i')^q$ des puissances q-ièmes des éléments de G_i' est toujours $\langle\sigma_2^q\rangle=\langle\tau_2\rangle$. De par (5) et (6) le centralisateur $C_{G_i}((G_i')^q)$ de $(G_i')^q=\langle\tau_2\rangle$ dans G_i a $\langle\pi_1\rangle$ comme p-sous-groupe de Sylow, si $i=1$, et $\langle\pi_1^p\rangle\times\langle\pi_2\rangle$, si $i=2$. Ces deux p-groupes n'étant pas isomorphes, les deux groupes G_1 et G_2 ne peuvent pas l'être. Donc (1a) est vrai.

La démonstration de (1b) varie suivant la caractéristique du corps k. Pour la plupart des caractéristiques, elle est donnée par le

(7) **Lemme.** *Si R est un anneau commutatif avec 1 dans lequel (l'image de) l'entier premier q est inversible, alors les deux R-algèbres de groupe RG_1 et RG_2 sont isomorphes.*

Démonstration. De par (6) la R-algèbre RG_1 est le produit tensoriel (sur R) de ses sous-algèbres $R\langle\pi_1\rangle Q_1$ et $R\langle\pi_2\rangle Q_2$, tandis que RG_2 est le produit tensoriel de $R\langle\pi_1\rangle Q_2$ et $R\langle\pi_2\rangle Q_1$. Donc le lemme sera une conséquence immédiate des isomorphismes d'algèbres:

$$R\langle\pi_i\rangle Q_1\simeq R\langle\pi_i\rangle Q_2, \quad \textit{pour } i=1,2. \tag{8}$$

Pour établir (8), on note que l'inversibilité de q dans R implique l'existence d'un idempotent:

$$e_j=\frac{1}{q}\sum_{h=1}^{q}(\tau_j)^h$$

dans $R\langle\tau_j\rangle\subseteq R\langle\pi_i\rangle Q_j$, pour $j=1,2$. Cet idempotent est clairement central dans $R\langle\pi_i\rangle Q_j$, et donc définit une décomposition de celle-ci en somme directe de sous-algèbres:

$$R\langle\pi_i\rangle Q_j=e_jR\langle\pi_i\rangle Q_j\oplus(1-e_j)R\langle\pi_i\rangle Q_j, \quad \textit{pour } i,j=1,2.$$

La sous-algèbre $e_jR\langle\pi_i\rangle Q_j$ est naturellement isomorphe à l'algèbre de groupe $R[\langle\pi_i\rangle Q_j/\langle\tau_j\rangle]$ du groupe quotient $\langle\pi_i\rangle Q_j/\langle\tau_j\rangle$. Mais ce groupe quotient est indépendant de j (la seule différence entre (3a) et (3b) est que $\sigma_1^q=1$ tandis que $\sigma_2^q=\tau_2$, une différence qui disparaît dans les groupes quotients). Donc l'algèbre $e_1R\langle\pi_i\rangle Q_1$ est isomorphe à $e_2R\langle\pi_i\rangle Q_2$ et la démonstration de l'isomorphisme (8) se ramène à celle de

$$(1-e_1)R\langle\pi_i\rangle Q_1\simeq(1-e_2)R\langle\pi_i\rangle Q_2, \quad \textit{pour } i=1,2. \tag{9}$$

Pour tout $j=1,2$, le sous-groupe $\langle\rho_j,\tau_j\rangle=\langle\rho_j\rangle\times\langle\tau_j\rangle$ est élémentaire d'ordre q^2. Ses sous-groupes d'ordre q autres que $\langle\tau_j\rangle$ sont les $\langle\rho_j\tau_j^k\rangle$, pour $k=1,\ldots,q$. Les idempotents correspondants dans $R\langle\rho_j,\tau_j\rangle$ sont les

$$f_{jk}=\frac{1}{q}\sum_{h=1}^{q}(\rho_j\tau_j^k)^h, \quad \textit{pour } k=1,\ldots,q.$$

On calcule facilement que:

$$(10a)\qquad (1-e_j)f_{jk}(1-e_j)f_{jl}=\begin{cases}(1-e_j)f_{jk}, & \textit{si } k=l=1,\ldots,q,\\ 0, & \textit{si } k,l=1,\ldots,q \textit{ et } k\neq l,\end{cases}$$

$$(10b)\qquad 1-e_j=\sum_{k=1}^{q}(1-e_j)f_{jk}.$$

De (3) on déduit que:

$$(11)\qquad \sigma_j^{-k}[(1-e_j)f_{jq}]\,\sigma_j^k=(1-e_j)f_{jk}, \quad \textit{pour } k=1,\ldots,q.$$

Donc (10b) est une décomposition de l'identité $1-e_j$ de $(1-e_j)R\langle\pi_i\rangle Q_j$ en somme orthogonale d'idempotents de cette algèbre qui y sont tous conjugués. Il s'ensuit que $(1-e_j)R\langle\pi_i\rangle Q_j$ est isomorphe à l'algèbre de toutes les $q\times q$ matrices à éléments dans sa sous-algèbre $(1-e_j)f_{jq}R\langle\pi_i\rangle Q_j(1-e_j)f_{jq}$. Donc la démonstration de (9) se ramène à celle des isomorphismes:

$$(12)\qquad \begin{aligned}&(1-e_1)f_{1q}R\langle\pi_i\rangle Q_1(1-e_1)f_{1q}\\ &\quad\simeq(1-e_2)f_{2q}R\langle\pi_i\rangle Q_2(1-e_2)f_{2q}, \quad \textit{pour } i=1,2.\end{aligned}$$

Le sous-groupe $\langle\rho_j\rangle$ étant centralisé par $\langle\pi_i\rangle$, l'idempotent f_{jq} est central dans la sous-algèbre $R\langle\pi_i,\rho_j,\tau_j\rangle$, pour $j=1,2$. Ceci et les identités (10a) et (11) impliquent que:

$$\begin{aligned}(1-e_j)f_{jq}R\langle\pi_i,\rho_j,\tau_j\rangle\,\sigma_j^k(1-e_j)f_{jq}&=R\langle\pi_i,\rho_j,\tau_j\rangle\,\sigma_j^k(1-e_j)f_{jk}(1-e_j)f_{jq}\\ &=0, \quad \textit{pour } k=1,\ldots,q-1.\end{aligned}$$

Comme l'algèbre $R\langle\pi_i\rangle Q_j$ est la somme directe de ses R-sous-modules $R\langle\pi_i,\rho_j,\tau_j\rangle\,\sigma_j^k$, pour $k=0,1,\ldots,q-1$, on déduit que:

$$(13)\qquad (1-e_j)f_{jq}R\langle\pi_i\rangle Q_j(1-e_j)f_{jq}=(1-e_j)f_{jq}R\langle\pi_i,\rho_j,\tau_j\rangle, \quad \textit{pour } i,j=1,2.$$

Mais il y a un isomorphisme φ du groupe $\langle\pi_i,\rho_1,\tau_1\rangle$ sur le groupe $\langle\pi_i,\rho_2,\tau_2\rangle$, pour $i=1,2$, envoyant π_i sur π_i, ρ_1 sur ρ_2, et τ_1 sur τ_2. Evidemment φ induit un isomorphisme ψ de l'algèbre $R\langle\pi_i,\rho_1,\tau_1\rangle$ sur l'algèbre $R\langle\pi_i,\rho_2,\tau_2\rangle$ envoyant e_1 sur e_2 et f_{1q} sur f_{2q}. Donc la restriction de ψ est un isomorphisme de la sous-algèbre $(1-e_1)f_{1q}R\langle\pi_i,\rho_1,\tau_1\rangle$ sur $(1-e_2)f_{2q}R\langle\pi_i,\rho_2,\tau_2\rangle$. Ceci et (13) démontrent les isomorphismes (12), ce qui complète la démonstration du lemme.

Pour les corps de caractéristique q on démontrera (1b) à l'aide du

(14) **Lemme.** *Si R est un anneau intègre dans lequel (l'image de) l'entier premier p est inversible, et si R contient une racine primitive p^2-ième de l'unité ζ, alors les deux R-algèbres de groupe RG_1 et RG_2 sont isomorphes.*

Démonstration. A cause de (4) et (5), le sous-groupe $\langle \pi_1^p \rangle$ d'ordre p est central dans G_i, pour $i=1,2$. Donc l'identité 1 est la somme orthogonale des idempotents centraux:

$$f_k = \frac{1}{p} \sum_{h=1}^{p} \zeta^{-pkh} \pi_1^{ph}, \qquad \textit{pour } k=1, \ldots, p,$$

dans RG_i. Il s'ensuit que RG_i est la somme directe de ses sous-algèbres:

$$RG_i = f_1 RG_i \oplus \cdots \oplus f_p RG_i.$$

Il est clair que l'algèbre RG_i a un R-automorphisme α fixant tous les éléments de $\langle \pi_2 \rangle$ et de $Q_1 \times Q_2$, et envoyant π_1 sur $\zeta \pi_1$. Evidemment l'automorphisme α permute cycliquement les idempotents $f_1, \ldots, f_p$. Donc les sous-algèbres $f_1 RG_i, \ldots, f_p RG_i$ sont deux-à-deux isomorphes, et l'algèbre RG_i est isomorphe à la somme directe de p exemplaires de $f_p RG_i$. Mais $f_p RG_i$ est isomorphe à l'algèbre de groupe $R[G_i/\langle \pi_1^p \rangle]$ du groupe quotient $G_i/\langle \pi_1^p \rangle$, et ce groupe quotient est indépendant du choix de i (la seule différence entre π_1 et π_2 était que $\pi_1^p \neq 1$ tandis que $\pi_2^p = 1$, une différence qui disparaît dans les groupes quotients). Donc l'algèbre RG_i est indépendante du choix de i à un isomorphisme près, ce qui est le lemme.

Démonstration de (1b). Si la caractéristique du corps k est différente de q, la propriété (1b) est une conséquence du lemme (7). Si q est la caractéristique de k, la condition (2) garantit l'existence d'une racine primitive p^2-ième de l'unité ζ dans k. Donc (1b) est une conséquence du lemme (14) dans ce cas.

Reference

1. Brauer, R.: Representations of finite groups. Dans «Lectures on modern mathematics I» (T.L. Saaty, Ed.). New York-London: John Wiley & Sons, Inc. 1963.

Prof. E.C. Dade
Institut de Recherche Mathématique Avancée
Université de Strasbourg
67-Strasbourg
France

(Reçu le 2 novembre 1970)