Can. J. Math., Vol. XXXII, No. 1, 1980, pp. 165–184

ALGEBRES SIMPLES DE GROUPES A GAUCHE

DAVID HANDELMAN

Soit R un anneau et soit G^{op} un sous groupe de Aut (R). Formons l'anneau de groupe à gauche ("skew group ring") R_sG, en imposant, sur le module libre à gauche avec une base G, la multiplication $rg = gr^g$. (On écrit G^{op} au lieu de G car, si $G <$ Inn (R) = le groupe d'automorphismes intérieurs, la condition $g^{-1}rg = r^g$ implique que le homomorphisme naturel $r_g \mapsto g$, où $g \equiv r_g - r_g{}^{-1}$, est vraiment un anti-homomorphisme).

Nous considérons le cas où $R = M_nF$, F un corps, M_nF l'anneau de matrices, d'ordre n, et G^{op} un sous-groupe (généralement) fini, de $PGL(n, F) =$ Inn (R). Ce travail est consacré à l'étude de la simplicité de R_sG.

Si R_sG est simple et si G est intérieur, on en déduit dans le chapitre I, que G est fini, et en particulier que $|G| \mid n^2$. Dans le deuxième chapitre on montre que R_sG est simple si, et seulement si, pour tout sous-groupe de Sylow G_p de G, R_sG_p est simple. De plus, on a $R_sG \simeq \otimes R_sG_p$ (quand R_sG est simple) mais l'isomorphisme n'est pas naturel.

Le troisième chapitre est composé de résultats concernant le centre de R_sG. Si $K = Z(R_sG)$ et $[K: F] = |G|$, on peut effectivement d'écrire précisément le groupe G, son action sur R, et le centre K. Si $K = F$, il y a une réduction du problème aux groupes de type central ("groups of central type," "Z-gruppen") qui sont plongeables dans $PGL(n, F)$ d'une façon particulière. Des autres cas sont étudiés, et nous démontrons que, si $K \neq F$, il existe un p-groupe invariant dans G. Si G est abélien, des conditions nécessaires et suffisantes sont obtenues pour que R_sG soit simple.

Le quatrième chapitre étudie les corps tels qu'il n'existe pas de groupes $G \neq \{1\}$ avec R_sG simple; des classes de groupes finis sont trouvées telles que pour ces groupes R_sG n'est jamais simple, quelque soit le corps et l'ordre n.

S'il y a une application $\gamma: G \times G \to R^* =$ {éléments inversibles de R}, tels que

$$\gamma(x, y)\gamma(xy, z) = \gamma(y, z)\gamma(x, yz) \quad x, y, z \in G;$$

on peut former *l'anneau* de *groupe tordu*, ("twisted group ring") en imposant la multiplication aux éléments $\{t_g\}_{g \in G}$,

$$rt_g = t_g r \text{ et } t_g t_h = \gamma(g, h)t_{gh}.$$

Si de plus, il existe une action de G sur R (c'est à dire, $G^{\text{op}} \to$ Aut (R)), on peut former le *produit croisé*, R_cG,

$$rt_g = t_g r^g \text{ et } t_g t_h = \gamma(g, h)t_{gh}.$$

Reçu le 17 mai, 1978 et sous forme revisée, le 19 décembre, 1978.

Si $H \lhd G$, on a $R_cG \simeq (R_cH)_dG/H$ pour l'action induite et le cocyle γ approprié.

Je voudrais remarquer que je regrette qu'il faille employer le mot "gauche" pour indiquer quelquechose d'anormal.

On suppose toujours que car $F = 0$, mais cela n'est pas nécessaire en général; d'habitude, il suffit que car F ne divise pas $|G|$, et quelquefois même cette condition n'est pas nécessaire.

1. Résultats préliminaires. Soit F un corps, $R = M_nF$, et G^{op} un sous groupe (fini) de Aut (R), d'habitude de $PGL(n, F)$. Dans ce chapitre nous étudions quelques propriétés du groupe G en supposant que R_sG soit simple. Par exemple, si $G^{\text{op}} < PGL(n, F)$ et si R_sG est simple, alors $|G| \mid n^2$; un résultat plus précis sera obtenu.

Fisher et Osterburg [**2**] ont noté qu'one peut considérer R comme un R_sG-module à droite, R_{R_sG} avec l'action,

$$(r)(\sum g_i r_i) = \sum r^{g_i} r_i.$$

De plus, ce n'est pas difficile à voir que R^G, la sous-algébre fixe de G, est isomorphe à End R_{R_sG}. On voit que R a la structure d'un $R^G - R_sG$ bimodule, et qu'il y a un homomorphisme naturel $R_sG \to \text{End}\ {}_{R^G}R$. Quand R_sG est simple, naturellement cet homomorphisme est une immersion, et nous démontrons que c'est en fait un isomorphisme et que ${}_{R^G}R_{R_sG}$ établit un équivalence de Morita entre R^G et R_sG.

LEMME 1.1. *Soit T un anneau, et P un module à droite tel que $mP \simeq T$ (comme modules à droite) pour $m \in \mathbf{N}$. Formons $S = \text{End}\ P$; alors ${}_SP$ est un module libre de rang m, et* End ${}_SP \simeq T$.

Démonstration. On a $T \simeq M_m\ (\text{End}\ P) = M_mS$, et sous cet isomorphisme, P_T devient une ligne de M_mS, et ${}_SP$ est donc libre de rang m, et End ${}_SP \simeq T$.

THÉORÈME 1.2. *Si R_sG est simple, et $|G| = m$, alors*

(i) ${}_RG^R$ *est libre de rang m;*

(ii) ${}_RG^R{}_{R_sG}$ *est un bimodule qui établit un équivalence de Morita entre R^G et R_sG;*

(iii) $R_sG \simeq M_m(R^G)$.

Démonstration. Posons $T = R_sG$; comme R_sG est un anneau simple et artinien, et dim ${}_FR_sG = m$ dim ${}_FR$, $P = R_{R_sG}$, on a $mP_T \simeq T_T$. Comme $R^G \simeq \text{End}\ (R_{R_sG})$, on peut appliquer le lemme précédent.

COROLLAIRE 1.3. *Si G est un groupe fini d'automorphismes intérieurs de R tel que R_sG est simple, alors*

$$|G| \mid n^2/[K:F],$$

où K est le centre de R_sG.

https://doi.org/10.4153/CJM-1980-013-2 Published online by Cambridge University Press

Démonstration. Comme G est intérieur, $F \subset K$ et $F \subset R^G$; selon 1.2 (i, iii) $n^2 = |G| \dim R^G$. Comme $K \subset R^G$ et K est un corps, $\dim K$ divise $\dim R^G$, d'où le résultat.

Par exemple, si n est un nombre premier, il faut que G soit abélien, cyclique d'ordre n^2 ou d'ordre n, ou de type (n, n).

Bien que le résultat suivant ne soit pas nécessaire pour ce qui suit, cela justifie notre restriction au cas où G est fini.

THÉORÈME 1.4. *Soit* $G^{\mathrm{op}} \subset \mathrm{Aut}\,(R)$ (*non nécessairement fini*) *tel que* $R_{R_s G}$ *soit un module fidèle, et* $[F\colon F^G] < \infty$. *Alors G est fini, en fait* $|G| \leqq n^2[F\colon F^G]$.

Démonstration. Le module $R_{R_s G}$ étant fidèle, il existe un monomorphisme (de F^G-algèbres),

$$R_s G \longrightarrow \mathrm{End}\,(R_{R_s G}) \subset \mathrm{End}\, R_{F^G} = M_{n^2[F,F^G]} F^G.$$

La F^G–dimension de $R_s G$ étant $|G| \cdot n^2[F\colon F^G]$, nous obtenons que

$$|G| n^2[F\colon F^G] \leqq n^4[F\colon F^G]^2,$$

d'où $|G| \leqq n^2[F\colon F^G]$.

COROLLAIRE 1.5. *Si G est intérieur et si* $R_s G$ *est simple, alors G est fini* (*même si* $[G\colon \mathrm{Inn}\, G] < \infty$, *et* $R_s G$ *est simple, G est fini*).

Tous les résultats ici restent valables si on remplace $R_s G$ par un produit croisé $R_c G$, pourvu que l'action de G reste fidèle.

2. Sous-groupes de Sylow. Nous démontrons que, si $R_c G$ est simple alors $R_c H$ l'est aussi, où H est un sous-groupe de Hall; en particulier, ceci est vrai pour les sous groupes de Sylow.

LEMME 2.1. *Soit p un nombre premier et soit*

$$\{a_i\}_{i=1}^{t},\ \{b_i\}_{i=1}^{t},\ \{m_i\}_{i=1}^{t},\ \{d_i\}_{i=1}^{t},\ c,\ r$$

des nombres positifs, tels que

(i) $b_i | d_i^2 c$ *pour tout i;*

(ii) $\sum_i a_i^2 b_i = p^r \| (\sum m_i a_i d_i)^2 c$;

(iii) $m_i d_i / a_i b_i = m_1 d_1 / a_1 b_1$ *pour tout i.*

Alors $t = 1$ *et* $(p, m_1) = 1$.

Démonstration. Si $p^k | a_i$ pour tout i, remplaçant a_i par a_i / p^k ceci ne change pas les hypothéses; nous pouvons donc supposer qu'il existe un indice i_0 tel que $p \nmid a_{i_0}$, et que $i_0 = 1$. Posons $n = \sum m_i a_i d_i$.

De (iii), nous déduisons

$$a_i^2 b_i = (m_i a_i d_i) a_1 b_1 / m_1 d_1;$$

faisant la somme et employant (ii):

(1) $\quad n a_1 b_1 / m_1 d_1 = p^r \| n^2 c.$

https://doi.org/10.4153/CJM-1980-013-2 Published online by Cambridge University Press

Soit $v(u)$ la puissance la plus grande telle que $p^{v(u)}|u$. On a $v(a_1) = 0$. De (1),

(2) $\quad r = v(n) + v(b_1) - v(m_1) - v(d_1) = 2v(n) + v(c).$

De (i), $v(b_1) - 2v(d_1) \leqq v(c)$. Donc

$$v(n) + v(b_1) - v(m_1) - v(d_1) \geqq 2v(n) + v(b_1) - 2v(d_1);$$

alors,

(3) $\quad v(d_1) \geqq v(n) + v(m_1).$

Mettant (3) dans (2) (gauche),

$$r + v(n) + v(m_1) \leqq v(n) + v(b_1) - v(m_1); \text{ donc}$$
$$r + 2v(m_1) \leqq v(b_1).$$

Alors, p^r/b_1. De (ii), on obtient $t = 1$ (et $a_1 = 1$), donc $b_1 = p^r$, et $(p, m_1) = 1$. (Rappelons-nous que nous avons déjà fait une réduction.)

THÉORÈME 2.2. *Soit A, B deux algèbres semisimples et de dimensions finies sur un anneau de division F tel que tous les anneaux de division des composantes de A, B contiennent une copie naturelle de F. Supposons aussi que A soit une sous-algèbre (avec unité) de B et que*

(a) $\dim {}_FA = p^r \| \dim {}_FB$ *(p nombre premier)*

(b) ${}_AB$ *est un module libre.*

Alors, si B est simple, A est simple.

Démonstration. Selon le théorème de Wedderburn, il existe une (F) algèbre de division D telle que $M_nD = B$. Ecrivons $A_i = e_iA$, où $\{e_i\}_{i=1}^t$ est l'ensemble des dempotents centraux et minimaux. Comme éléments de B, nous pouvons considérer les matrices diagonales idempotentes e_i. Il existe des monomorphismes naturels $A_i \subset e_iBe_i$ induits par $A \subset B$. Ecrivons $A_i = M_{a_i}F_i$, où les F_i sont des algèbres de division sur F. Les inclusions $A_i \subset e_iBe_i$ induisent les monomorphismes $F_i \to M_{m_id_i}D$ (m_i, d_i à être déterminés). A chacun de ces monomorphismes est associé une multiplicité: F_i est plongeable irréductiblement dans $M_{d_i}D$ et F_i est donc appliqué diagonalement sur:

$$\begin{bmatrix} [F_i]_{d_1} & & & \\ & [F_i]_{d_1} & & \\ & & \cdot & \\ & & & \cdot \\ & & & & \cdot \end{bmatrix}_{m_id_i}$$

(m_i copies de $M_{d_i}F_i$). Donc $e_iBe_i = M_{m_ia_id_i}D$. Alors,

$$\text{rang}_D\, e_i = m_ia_id_i.$$

https://doi.org/10.4153/CJM-1980-013-2 Published online by Cambridge University Press

Comme e_iB est un module libre sur A_i (de rang qui est indépendant de i), et que e_iA s'est composé de $m_ia_id_i$ rangées de M_nD, alors,

(1) $\dim {}_Fe_iA = nm_ia_id_i[D:F]$.

Nous avons $n = \sum m_ia_id_i$. Les rangs de e_iB sur A_i étant tous égaux ($=\text{rang}_A B$), on en deduit

$$nm_ia_id_i[D:F]/a_i^2[F_i:F] = na_1m_1d_1[D:F]/a_1^2[F_1:F].$$

Donc

(2) $m_id_i/a_i[F_i:F] = m_1d_1/a_1[F_1:F]$ pour tout i.

L'anneau de division F_i se plonge dans $M_{d_i}D$; donc

(3) $[F_1:F]|d_i^2[D:F]$.

Posons $b_i = [F_i:F]$, $c = [D:F]$; compte-tenu du lemme précédent, on a $t = 1$ et A est simple.

PROPOSITION 2.3. *Soit B une algèbre de dimension finie sur un anneau de division F. Supposons que pour chaque nombre premier p qui divise* $\dim {}_FB$, *il existe une sous-algèbre A_p (avec unité) simple tel que l'anneau de division de A_p contienne naturellement une copie de F, et que*

$$\dim A_p = p^r \| \dim {}_FB.$$

Alors B est simple.

Démonstration. Soit I un idéal bilatère, non nul, de B. Ecrivons $A_p = M_{n(p)}D_p$, D_p une F-algèbre de division. Comme $A_p \subset B$, il existe une sous-algèbre R_p contenant D_p telle que

$$B = M_{n(p)}R_p, \text{ et } I = M_{n(p)}I_p,\ I_p \lhd R_p.$$

Comme $I \neq 0$, $I_p \neq 0$, et alors $[D_p:F]|I_p$, d'où $\dim A_p|\dim I$. Alors,

$$\pi_p \dim A_p = \dim I,$$

d'où $B = I$.

THÉORÈME 2.4. *Supposons qu'un groupe G ait une action intérieure sur R, et qu'on puisse former un produit croisé, R_cG.*

(a) *Si R_cG est simple, alors R_cH l'est aussi pour tout sous-groupe de Hall, H, de G.*

(b) *R_cG est simple si et seulement si R_cG_p est simple pour tous les sous-groupes de Sylow, G_p, de G.*

Démonstration. Supposons que R_cG soit simple; on voit que $R_cG_p \subset R_cG$ et on peut écrire $R_cG_p = M_n(T_p)$, $R_cG = M_nT$, où $T_p \subset T$. On voit que $F \subset Z(T_p)$, $Z(T)$ car G est intérieur, et que R_cG est libre sur R_cG_p, donc ${}_{T_p}T$ est

https://doi.org/10.4153/CJM-1980-013-2 Published online by Cambridge University Press

libre, et il est facile de voir que $\dim {}_F T_p = p^r \| \dim {}_F T$, d'où T_p est simple (Théorème 2.2).

Soit $H < G$ un sous-groupe de Hall. Si H_p est un sous-groupe de Sylow de H, il est aussi un sous-groupe de Sylow de G; donc $R_c H_p$ est simple. Notons que comme dans le premier paragraphe, on peut "dématriser" $R_c H_p$, $R_c H$, on peut appliquer 2.3 pour obtenir que $R_s H$ est simple aussi. La méthode s'applique aussi au cas où $H = G$, ce qui complète la démonstration.

Ce résultat peut être considéré comme une généralisation de [**6**; Satz 1].

LEMME 2.4A. *Soit A, B deux algèbres simples de dimension finies sur un corps F, telles que $F \subset Z(A)$, $Z(B)$. Supposons que $A \subset B$, et que*

$$\left(\dim_F A, \frac{\dim_F B}{\dim_F A}\right) = 1.$$

Alors, $Z(A) = Z(B) \cap A$.

Démonstration. En considérant $eAe \subset eBe$ pour un certain idempotent e de A, on peut supposer que A est une algèbre de division (d'où $\dim_F A$ divise $\dim_F B$). Soit $K = Z(B)$, et $L = K \cap A$; on remarque que $L \subset Z(A)$ et

$$\left(\dim_L A, \frac{\dim_L B}{\dim_L A}\right) = 1.$$

Comme $A \cap K = L$, l'algébre C, engendrée par A et K, est isomorphe à $A \otimes_L K$; comme les dimensions sont premieres entre elles, $A \otimes_L K$ est une algèbre de division (un idéal à droite de $A \otimes_L K$ est un espace vectoriel sur A et sur K, et $(\dim_L A, \dim_L K) = 1$). On déduit encore une fois, que

$$(1) \quad \left(\dim_K C, \frac{\dim_K B}{\dim_K C}\right) = 1.$$

Selon le Lemme A-II (voir l'Appendice 2),

$$(2) \quad (\dim_K C) \cdot (\dim_K C_B(C)) = \dim_K B$$

d'où

$$(3) \quad (\dim_K C_B(C), \dim_K C) = 1.$$

Mais, $Z(C) = C_B(C) \cap C$, et comme $Z(C)$ est un corps, $\dim_K Z(C)$ divise $\dim_K C_B(C)$ et $\dim_K C$. On déduit de (3), que $Z(C) = K$. Comme $A \otimes_L K \simeq C$, il s'en suit que $Z(A) = L$, d'où $Z(A) = A \cap K = A \cap Z(B)$.

Maintenant supposons que $R_s G$ est simple et que H est un sous-groupe de Hall du groupe G. En choisisant l'idempotent $e = e_{11}$ de $R = M_n F$, on obtient $eR_s He \subset eR_s Ge$ et

$$\dim_F eR_s He = |H| \text{ et } \dim_F eR_s Ge = |G|.$$

Comme H est un sous-groupe de Hall, de 2.4 et de 2.4A, on conclut que

$Z(eR_sHe) = Z(eR_sGe) \cap eR_sHe$. Donc, en formant les anneaux de matrices n par n,

$$Z(R_sH) = Z(R_sG) \cap R_sH.$$

Nous allons employer ce résultat plusieurs fois dans ce qui suit.

LEMME 2.5. *Soit* $\{A_i\}_{i=1}^m$, $\{B_i\}_{i=1}^n$ *deux familles d'algèbres simples centrales de dimension finie sur un corps* F. *Supposons que:*

(a) $\bigotimes_i{}^m A_i \simeq \bigotimes_i{}^m B$;

(b) $\dim A_i = \dim B_i$ *pour tout* i;

(c) *pour tout* $i \neq j$, $(\dim A_i, \dim A_j) = 1$.

Alors $A_i \simeq B_i$ *pour tout* i.

Démonstration. Par recurrence, on peut supposer que $m = 2$. Soit $[A_i]$, $[B_i]$ les images de A_i, B_i dans le groupe de Brauer de F, et posons $n_i{}^2 = \dim A_i$. On a

$$[A_1][A_2] = [B_1][B_2]. \tag{1}$$

De (b) et [**5**, p. 119], $[A_i]^{n_i} = [B_i]^{n_i} = [F]$; donc

$$[A_1]^{n_2} = [B_1]^{n_2} \quad \text{(de (1))}.$$

Il existe $c, d \in \mathbf{Z}$, tel que $cn_1 + dn_2 = 1$; alors

$$[A_1] = [A_1]^{cn_1+dn_2} = [A_1]^{cn_1}([A_1]^{n_2})^d = ([A_1]^{n_2})^d = (B_1)^{n_2 d} = [B_1]^{cn_1+dn_2} = [B_1];$$

d'où $[A_1] = [B_1]$. Mais $\dim A_1 = \dim B_1$, donc $A_1 \simeq B_1$.

PROPOSITION 2.6. *Soit* $\{A_p\}$ *une famille de sous-algèbres (avec unité) simples d'une algèbre simple* B, *de dimension finie sur un corps central* F. *Supposons que:*

(a) $\dim {}_F A_p = p^{r(p)} \| \dim {}_F B$ (p *nombre premier*) *pour tout* A_p;

(b) $\dim {}_F B = \pi \dim {}_F A_p$;

(c) $Z(A_p) = Z(B) \cap A_p$.

Alors $B \simeq \bigotimes_F A_p$.

Démonstration. Posons $K = Z(B)$, $K_p = Z(A_p)$. Notons d'abord que le centre de $A_p \otimes_{K_p} K$ est précisément K ($K_p \subset K$ à cause de (c)); cela implique que les algèbres $B_p = A_p \otimes_{K_p} K$ sont toutes simples et centrales sur K. Il y a un homomorphisme naturel

$$B_p \to \langle A_p, K \rangle \subset B;$$

comme B_p est simple c'est un isomorphisme de K-algèbres, et nous identifierons B_p avec son image $\langle A_p, K \rangle$ dans B.

Selon [**5**, 4.4.2], on peut écrire $B = B_p \otimes_K B_p'$ ('indique le commutant); selon [**5**; 4.4.6], on peut écrire $B = \bigotimes_K C_q$, où $\{C_q\}$ sont des algèbres simples et centrales de K-dimension $q^{r(q)} \| \dim B$. Pour p fixe, 2.5 nous assure que $B_p \simeq C_p$. Donc,

$$B \simeq \bigotimes_{p \neq K} B_p \simeq \bigotimes_K (A_p \otimes_{K_p} K).$$

https://doi.org/10.4153/CJM-1980-013-2 Published online by Cambridge University Press

Pour $p \neq q$, formons $K_{pq} = K_pK_q$, et remarquons qu'il existe un isomorphisme naturel

$$A_p \otimes_F A_q \simeq (A_p \otimes_{K_p} K_q) \otimes_{K_q} (A_q \otimes_{K_q} \otimes K_p).$$

Par induction $\otimes_F A_p \simeq \otimes_K (A_p \otimes K) \simeq B$.

Seulement pour le theorème suivant, on note par $\bar{S}$ un anneau tel que l'anneau S est isomorphe à $M_n\bar{S}$; par example, soit e unidempotent minimal de R; on peut choisi pour $\overline{R_sG}$ l'anneau eR_sGe.

THÉORÈME 2.7. *Si G est intérieur et R_sG est simple, alors*

$$\overline{R_sG} \simeq \otimes_p {}_F\overline{R_sG_p}$$

où $\{G_p\}$ est une sélection de sous-groupes de Sylow de G, un pour chaque $p \| |G|$.

Démonstration. C'est une conséquence immédiate des deux résultats précédents et de la remarque précédente.

On remarque que le théorème reste valable si on a un produit croisé et si action de G est intérieure; mais si G est par exemple extérieur (tous les éléments non nuls sont extérieurs), $\overline{R_cG} \simeq \otimes\ \overline{R_cG_p}$ si, et seulement si, G est résoluble.

3. Cas spécifiques. Quand R_sG est simple, le centre, K, est un corps. Nous considérons tous les cas possibles:

(i) $[K:F] = |G|$
(ii) $K = F$
(iii) $K \neq F$ mais $[K:F] \neq |G|$,

suivi de certains résultats plus spécifiques; par exemple, dans le cas où $[K:F]$ est maximal. Si G est abélien, nous obtenons des conditions nécessaires et suffisantes pour que R_sG soit simple.

Soit $p: GL(n, F) \to PGL(n, F)$ l'homomorphisme naturel. Selon notre définition de l'action de G sur R, c'est G^{op} qui peut être considéré comme un sous-groupe de $PGL(n, F)$. Posons $H = p^{-1}G^{\text{op}}$.

Nous calculons le centre de R_sG. On voit aussitôt que chacune des classes de conjugais on contribue soit une soit zéro dimension au centre, et que les classes qui en donnent une, contribuent à une *base* du centre. Explicitement, si α est un classe de conjugaison de G, pour que

$$z = \sum_\alpha gr_g$$

commute avec tous les éléments de R, il faut et il suffit que r_g induise l'automorphisme intérieur g, c'est à dire $g \equiv r_g - r_g^{-1}$. Pour que de tels éléments commutent avec tous les éléments de G aussi, il faut et suffit que

$$r_{g^h} = (r_g)^h (g^h = hgh^{-1}) \text{ pour tout } h \in G.$$

On peut exprimer cela d'une manière plus compacte:

Si α est engendré par g, et $h \in G$ commute avec g, alors

$$r_g r_h = r_h r_g.$$

(Généralement, on ne peut que dire $r_g r_h = \lambda r_h r_g$, pour $\lambda \in F^*$.)

Supposons que toutes les dimensions de G soient absorbées par le centre, c'est à dire, $[K:F] = |G|$. En ce cas le groupe G a $|G|$ classes de conjugation—G est abélien. De plus, comme chaque classe contribue au centre, $p^{-1}G^{\mathrm{op}} = H$ est abélien.

PROPOSITION 3.1. *Si R_sG est simple et si $K = Z(R_sG)$ est de dimension $|G|$ sur F, alors*

(a) *$|G|$ divise n;*

(b) *$p^{-1}G^{\mathrm{op}}$ est abélien.*

Démonstration. (a) Cela résulte de 1.3.

(b) Voir la discussion précédente.

Quand G est abélien, des conditions sous lesquelles R_sG est simple ont été obtenues pour un anneau simple R quelconque. Si l'on definit l'ensemble:

$$L = \{g \in G | \text{ il existe } r \in R^G \text{ tel que } g \equiv r - r^{-1}\},$$

on voit aisément que $L = p(Z(p^{-1}G))$, donc L est un sous-groupe intéressant de $Z(G)$, même si G n'est pas abélien.

THÉORÈME 3.2. [**4**, Theorem 1.7] *Soit R un anneau simple quelconque, et G un groupe abélien d'automorphismes de R. Alors R_sG est simple si, et seulement si, les conditions suivantes sont staisfaites:*

(i) *L est un groupe de torsion;*

(ii) *pour $g \in L$, si $o(g) = n$, alors il n'existe pas de $r \in R^G$ tel que $r^n = 1$ et $g \equiv r - r^{-1}$;*

(iii) *pour $g \in L$, si $o(g) = 4$, il n'existe pas de $r \in R^G$ tel que $r^4 = -4$ et $g \equiv r - r^{-1}$.*

Quand les conditions sont vérifiées, alors le centre de R_sG est précisément l'algèbre tordue k^tL, où k est le sous-corps fixe du centre de R.

Dans le cas qui nous interresse, L est fini, et il résulte de [**4**, Theorem 1.6], que le centre a la forme

$$F[x_1, x_2, \ldots x_t]/\sum_i (x_i{}^{s(i)} - a_i) \quad a_i \in F;$$

en fait $L = \oplus\, \mathbf{Z}/s_i\mathbf{Z}$ et on peut écrire L (à conjugaison près dans $PGL(n, F)$). Soit $g_i \in M_{s(i)}F$ la matrice

$$g_i = \begin{bmatrix} 0 & a_i & & & & \\ & 0 & 1 & & & \\ & & 0 & 1 & & \\ & & & \cdot & \cdot & \\ & & & & \cdot\ \cdot & \\ & & & & & 1 \\ 1 & & & & & 0 \end{bmatrix}$$

https://doi.org/10.4153/CJM-1980-013-2 Published online by Cambridge University Press

et posons $h_i \in GL(n, F)$,

$$h_i = (I_{s(1)} \otimes I_{s(2)} \otimes \ldots g_i \otimes I_{s(i+1)} \otimes \ldots) \otimes I_t$$

où $t\pi s(i) = n$. Alors l'image de $\langle h_i \rangle$ dans $PGL(n, F)$ est $G_0 = \oplus \langle \bar{h}_i \rangle$, où $\bar{h}_i^{s(i)} = 1$, et l'algèbre tordue F^tG_0 est précisément $F[x_i]/\sum(x_i^{s(i)} - a_i)$. Ce sera un corps si les conditions de [**4**, I.5] sont satisfaites. On voit sans peine que si R_sL est simple, alors L peut être conjugué à G_0 dans $PGL(n, F)$.

Nous reviendrons au cas où G est abélien (et $L \neq G$). Il faut d'abord examiner un autre cas extrême, le cas $Z(R_sG) = F$.

LEMME 3.3. *Si la classe de conjugaison de l'élément $g \in G$ ne contribue pas au centre de R_sG, et $o(g) = p^s$ (p premier), alors il existe dans F une racine primitive p-ième de l'unité.*

Démonstration. Selon la discussion précédente, il existe r_g, r_h tels que $g \equiv r_g - r_g^{-1}$ et $\lambda \in F^* - \{1\}$ avec

$$r_g r_h = \lambda r_h r_g;$$

c'est à dire,

$$r_g = \lambda r_h r_g r_h^{-1}.$$

Comme $g^{p^s} = 1$, $(r_g)^{p^s} \in F^*$; donc, $\lambda^{p^s} = 1$, d'où le résultat.

Maintenant, considérons le cas où $Z(R_sG) = F$. Si $\bar{F}$ est la fermeture algébrique de F, $Z((R \otimes \bar{F})_sG) = \bar{F}$, donc $\bar{R}_sG$ est simple. Posons $H_1 = p^{-1}G^{\mathrm{op}}$ (p: $GL(n, \bar{F}) \to PGL(n, \bar{F})$). Soit

$$H_2 = H_1 \cap SL(n, \bar{F}).$$

Comme $\bar{F}$ est algébriquement clos, $p(H_2) = G$; si $\lambda \in F^*$ et $\det \lambda = 1$, alors $\lambda^n = 1$. On a donc la suite exacte

$$1 \to \{\lambda \in F^* | \lambda^n = 1\} \to H_2 \xrightarrow{p} G \to 1,$$

d'où H_2 est fini. Si $h \in H_2 - F^*$, il existe $h_0 \in H$, $\lambda \in F^* - 1$, tel que $hh_0h^{-1}h_0^{-1} = \lambda$ (comme $Z(\bar{R}_sG) = \bar{F}$, la classe de conjugaison de $p(h)$ dans G ne contribue pas au centre); donc $\mathrm{tr}(h) = 0$. Il s'en suit que $Z(H) = \ker p \cap H_2 = \{\text{racines } n\text{-ième de l'unité de } F^*\}$.

Un groupe J est de *type central* si J a une représentation irréductible de degré $[J: Z(J)]^{1/2}$.

LEMME 3.4. [**1**, Lemma 1, Corollary 1] *Un groupe fini est de type central si, et seulement si, pour tout $g \in J - Z(J)$, il existe $h \in J$ tel que $[g, h] \in Z(J) - \{1\}$.*

Donc notre groupe H_2 est de type central.

Un sous-groupe J de $GL(n, \bar{F})$ est *centralement immersible* dans $GL(n, \bar{F})$ si $Z(J)$ se compose d'éléments de $\bar{F}^*$.

https://doi.org/10.4153/CJM-1980-013-2 Published online by Cambridge University Press

PROPOSITION 3.5. *Soit G^{op} un sous-groupe fini de $PGL(n, \bar{F})$. Alors, le centre de $\bar{R}_sG$ est $\bar{F}$ si et seulement si, pour $H_2 = p^{-1}G \cap SL(n, \bar{F})$, H_2 est de type central et centralement immersible dans $GL(n, \bar{F})$. En ce cas, $H/Z(H) = G$.*

Démonstration. On a obtenu ci-dessus qu'un tel H_2 est de type central et centralement immersible. D'autre part, on voit que pour tout $g \in G^{op}$ il existe $r_g \in H$, $r_h \in H$, tel que $r_g \to g$, et $r_g r_h = \lambda r_h r_g$, $\lambda \in \bar{F}^* - \{1\}$. Alors le classe de conjugaison de g ne contribue pas au centre, donc $Z(R_sG) = \bar{F}$.

Comme on a car $(F) = 0$, R_sG est simple si, et seulement si, $Z(R_sG)$ est un corps, parce que R_sG est toujours semisimple.

PROPOSITION 3.6. *Quand H est un groupe fini, de type central et centralement immersible dans $GL(n, \bar{F})$, alors*

$$|{}^{H}/_{Z(H)}| \mid n^2 \text{ et } \operatorname{Exp}({}^{H}/_{Z(H)}) \mid n.$$

Démonstration. Nous savons déjà que $|G| \mid n^2$, d'où $|{}^{H}/_{Z(H)}| \mid n^2$. Pour démontrer que $\operatorname{Exp} G \mid n$, il suffit de démontrer que $\operatorname{Exp} G_p \mid n$ pour chacun de sous-groupes de Sylow, G_p. Comme $\bar{R}_sG$ est simple, $\bar{R}_sG_p$ l'est aussi, et $Z(\bar{R}_sG) = \bar{F}$, d'où

$$H_p = p^{-1}G_p^{op} \cap SL(n, \bar{F})$$

est de type central et centralement immersible.

Supposons que $p^r \| n$, et qu'il existe $h \in H_p$ tel que $h^{p^r} \notin Z(H_p)$. Alors $\{h, h^2 \ldots, h^{n-1}, h^n, h^{n+1}\}$ est disjoint de $Z(H_p)$ $(p^r \| n)$. Donc $\operatorname{tr}(h^i) = 0$ pour $1 \leqq i \leqq n + 1$, c'est-à-dire pour n puissances consécutives. Comme car $\bar{F} = 0$, cela implique $h = 0$, ce qui est absurde.

PROPOSITION 3.7. *Supposons que le groupe fini H soit de type central et centralement immersible dans $GL(n, \bar{F})$. Alors, la représentation $H < GL(n, F)$ contient une seule classe de représentation irréductible, et leur charactère ψ est fidèle et satisfait*

$$\psi(1)^2 = [H: Z(H)].$$

Démonstration. Appelons χ le charactère de $H < GL(n, \bar{F})$. Alors $\chi(h) = 0$ pour tout $h \in H - Z(H)$, et $\chi(z) = z$ pour $nz \in Z(H) \subset \bar{F}^*$. Soit m l'ordre du centre de H; notons qu'il faut que $Z(H)$ soit cyclique (la représentation est fidèle), choisissons z tel que $\langle z \rangle = Z(H)$. Soit τ un charactère irréductible quelconque. Donc,

$$\begin{aligned}(\chi, \tau) &= \frac{1}{|H|} \sum_h \chi(h)\, \tau(h^{-1}) \\ &= \frac{n^2}{|H|} \sum_i z^i \tau(z^{-i}) \\ &= \frac{n^2 \tau(1)}{|H|} \sum_i z^{i(1-t)} \text{ où } \tau(z) = z^t \tau(1).\end{aligned}$$

https://doi.org/10.4153/CJM-1980-013-2 Published online by Cambridge University Press

Si $t \not\equiv 1(m)$, $(\chi, \tau) = 0$. Si $t \equiv 1(m)$, choisissons τ_2 un autre charactère irréductible tel que $\tau_2(z) = z^t\tau_2(1)$. Comme $z^m = 1$ et $(m, t) = 1$, alors τ_2 est fidèle sur le centre de H. Selon [**6**, Corollary, p. 33], il faut que τ_2 soit fidèle, et donc que τ soit lui-même fidèle. Comme $\tau_1(h) = \tau_2(h) = 0$, pour tout $h \in H - z(H)$, $(\tau, \tau_2) \neq 0$; donc, $\tau = \tau_2$, c'est-à-dire, il n'existe qu'un charactère irréductible dans le support de $\chi = n^2m/|H|\tau$.

Quelquefois on peut réduire le cas général (R_sG simple) aux deux cas discutés ci-dessus ($[Z(R_sG):F] = |G|$ ou $Z(R_sG) = F$).

LEMME 3.8. *Soit* $L \lhd G \subset PGL(n, F)^{op}$ *tels que les deux algèbres* R_sL *et* R_sG *soient simples, et* $Z(R_sL) = Z(R_sG)$. *Alors* $G_{/L}$ *est "projectivement de type central", c'est-à-dire, qu'il existe un groupe fini* $H < GL(n, \bar{F})$ *tel que* H *est de type central, centralement immersible et* $H/Z(H)$ *est isomorphe naturellement à* G/L.

Démonstration. Voir l'Appendice II, A–V et A–$VI\rangle$.

THÉORÈME 3.9. *Si* G *est abélien et* R_sG *est simple, alors il y a une correspondance biunivoque entre les éléments de* L *et les éléments d'une base convenablement choisie du centre. De plus,* G/L *est projectivement de type central, et* $G/L \simeq M \times M$ *pour un groupe* M.

Démonstration. Appliquer 3.2, 3.8, et [**1**, p. 150].

On peut remarquer qu'il ne faut pas que L ait un complément dans G (voir l'Appendice I, à la fin.)

Pour le cas plus général (non-abélien), où $Z(R_sG)$ est un corps tel que ni $Z(R_sG) = F$ ni $[Z(R_sG):F] = |G|$ reste valable, on peut trouver quelques sous-groupes invariants dont l'ordre est p^r.

THÉORÈME 3.10. *Si* R_sG *est simple, et si* $p|[Z(R_sG):F]$, *alors il existe un* p*-sous-groupe normal non nul de* G.

Démonstration. Comme $R_sG \simeq \otimes R_sG_q$, et $Z(A) \otimes Z(B) = Z(A \otimes B)$, $Z(R_sG) \simeq \otimes Z(R_sG_q)$. Comme $p|[Z(R_sG):F]$, il faut que $Z(R_sG_p) \neq F$. Choisissons $g \in G_p$ tel que la classe de conjugaison de g dans G_p, α contribue une dimension au centre. Suivant les méthodes de § 2, on voit que l'élément $\sum_\alpha gr_g$ reste central dans R_sG, où α reste une classe de conjugaison de G. Soit $E = \langle\alpha\rangle$. Comme $\alpha \subset G_p$, $E < G_p$, d'où E est un p-groupe. Comme $\alpha^G = \alpha$, $E \lhd G$.

Il existe un cas extremal, qui prolonge les cas abéliens. Supposons que chacune des classes de conjugaison contribue au centre de R_sG. Il résulte facilement de la démonstration de 3.10 que tous les sous-groupes de Sylow sont invariants, c'est-à-dire, $G = \pi G_p$, et G est nilpotent. Donc, tous les R_sG_p satisfont la même condition. Comme dim $Z(R_sG_p)$ doit diviser $|G_p|$, on voir que t, le nombre de classes de conjugaison de G_p est un puissance de p, et le quotient est un carré. Si $p = 2$, et G_2 est non-abélien, $|G_2| = 2^r$, il faut que $r \geqq 6$; il existe des groupes d'ordre 2^6 avec $t = 16$ (voir [**3**]; je remercie les professeurs Dixon et Poland de l'Université Carleton qui m'en informent).

Pour $p > 2$, $|G_p| = p^r$, il faut que $r \geqq 11$ (comme des calculs élémentaires mais ennuyeux l'indiquent). Si $r = 11$ est possible, $p = 3$; si $p = 5$, il semble que $r \geqq 28$, et en général $r(p)$ semble s'augmenter très rapidement.

THÉORÈME 3.11. *Si R_sG est simple et si toutes les classes de conjugaison contribuent au centre, alors G est nilpotent. Si de plus, ni 2^6 ni p^{11} $(p > 2)$ ne divise l'ordre de G, alors G est abélien.*

Je remarque qu'il serait difficile de construire un groupe G d'ordre 2^6 (le plus petit possible), non-abélien et une immersion $G < PGL(n, F)$ pour un certain F, tel que la dimension du centre de R_sG soit $t = 16$, et que R_sG soit simple. Selon 1.3 il faut que $32|n$ (!).

4. Corps et groupes spéciaux. Pour certaines valeurs de n et certains corps, il n'existe pas de groupe $G < PGL(n, F)$ tel que R_sG est simple (sauf $G = \{1\}$). Par exemple, si n est impair et $F = \mathbf{R}$; pour un corps F de caractéristique 2 tel que tous les éléments possèdent une racine n-ième et tel que la fermeture algébrique relative de Z_2 dans F est Z_2 lui-même, et ceci pour n quelconque. D'autre part, il existe beaucoup de groupes finis tels que R_sG n'est pas simple, quelque soit n, F — par exemple les groupes dihédraux (sauf ceux d'ordre 2^n).

Rappellons nous que notre choix d'action est précisément le contraire du choix normal, c'est-à-dire nous considérons $G^{op} < PGL(n, F)$ au lieu de G (bien entendu $R_sG \simeq R_rG^{op}$, car R a une involution naturelle), et ce fait explique le lemme suivant.

LEMME 4.1. [**4**, Lemma 2.1] *Soit s: $G^{op} \to \mathrm{Inn}\,(R)$ un homomorphisme, et supposons qu'il existe un homomorphisme à gauche t:$G \to GL(1, R)$ tel que $pt = s$, ou p: $GL(1, R) \to \mathrm{Inn}\,(R)$ est l'homomorphisme naturel. Alors $R_sG \simeq RG^{op}$, (l'anneau de groupe usuel).*

Dans le cas particulier, où p:$GL(n, F) \to PGL(n, F)$ est scindé: alors $R = M_nF$ ne possède aucun groupe intérieur tel que R_sG soit simple. Le réciproque est aussi vraie.

THÉORÈME 4.2. *Pour le corps F et n fixe, les propriétés suivantes sont équivalentes:*

(i) *F^* est n-divisible d'une manière unique: tous les éléments de F^* possèdent une racine n-ième, mais il n'existe qu'une seule racine n-ième de l'unité.*

(ii) *$1 \to F^* \to GL(n, F)$ (immersion centrale de F^*) est scindée.*

(iii) *$GL(n, F) = F^* \times SL(n, F)$, et $PGL(n, F)$ est isomorphe naturellment à $SL(n, F)$.*

(iv) *$GL(n, F) \to PGL(n, F)$ est scindée.*

(v) *Chaque sous-groupe abélien fini et 2-engendré de $PGL(n, F)$ peut être relévé à un sous-groupe de $GL(n, F)$ tel que la restriction de p est un isomorphisme.*

(vi) *$R = M_nF$ ne possède aucun groupe intérieur tel que R_sG soit simple, sauf $G = \{1\}$.*

https://doi.org/10.4153/CJM-1980-013-2 Published online by Cambridge University Press

Démonstration. (i) $\Rightarrow$ (ii). L'application $h \to \sqrt[n]{\det h}$ est bien définie et est donc un homomorphisme $GL(n, F) \to F^*$ avec la propriété voulue.

(ii) $\Rightarrow$ (iii). Pour une suite exacte de groupes, se scindant à gauche, ceci implique que le groupe un produit direct.

(iii) $\Rightarrow$ (iv), (iv) $\Rightarrow$ (v), (iv) $\Rightarrow$ (vi). Les implications sont évidentes.

(iv) $\Rightarrow$ (i). Supposons $z^n = 1$ pour $z \in F$. Considérons les matrices A, B de $GL(n, F)$,

$$A = \begin{bmatrix} 0 & 1 & & & & \\ & 0 & 1 & & & \\ & & 0 & 1 & & \\ & & & \ddots & \ddots & \\ & & & & \ddots & 1 \\ 1 & & & & & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & & & & \\ & z & & & \\ & & z^2 & & \\ & & & \ddots & \\ & & & & z^{n-1} \end{bmatrix}.$$

Alors $A^n = B^n = I$ et $A^{-1}B^{-1}AB = zI$. Donc le groupe engendré dans $PGL(n, F)$ par les images de A, B, appelons-les X, Y, est abélien et 2-engendré. Si $\langle X, Y \rangle$ peut être rélevé, il faut envoyer X, Y à A', B' où $[A', B'] = I$; mais $A^{-1}A', B^{-1}B'$ doivent s'appartenir à F^*; c'est évidemment impossible à moins que z ne soit 1.

Maintenant choisissons $a \in F^*$. La matrice C de $GL(n, F)$ définie par

$$C = \begin{bmatrix} 0 & x & & & & \\ & 0 & 1 & & & \\ & & 0 & 1 & & \\ & & & \ddots & \ddots & \\ & & & & \ddots & 1 \\ 1 & & & & & 0 \end{bmatrix} \text{ où } x = (-1)^n a$$

satisfait $C^n = (-1)^n a I$, mais $C^t \notin F^*$ pour $1 \leqq t < n$. Alors le groupe engendré par l'image de C dans $PGL(n, F)$ est cyclique d'ordre n. Comme de tels groupes peuvent être relevés par hypothèse, il existe $D \in GL(n, F)$ tel que $D^n = 1$ et $CD^{-1} = bI$ pour $b \in F^*$. Comme $(\det (D))^n = 1$, $\det D = 1$ (nous savons maintenant que 1 est la seule racine n-ième de l'unité de F). Comme $\det C = a$, on voit que $CD^{-1} = bI$ implique $a = b^n$.

(vi) $\Rightarrow$ (i). Supposons que $z^n = 1$, $z \neq 1$ pour un certain $z \in F$. Il existe donc un nombre premier $p|n$, et une racine primitive d'unité d'ordre p, w, dans F^*. On forme les deux matrices $A_p, B_p \in GL(p, F)$

$$A_p = \begin{bmatrix} 0 & 1 & & & & \\ & 0 & 1 & & & \\ & & 0 & & & \\ & & & \ddots & & \\ & & & & \ddots & 1 \\ 1 & & & & & 0 \end{bmatrix} \quad B_p = \begin{bmatrix} 1 & & & & & \\ & w & & & & \\ & & w^2 & & & \\ & & & \ddots & & \\ & & & & \ddots & \\ & & & & & w^{p-1} \end{bmatrix}.$$

https://doi.org/10.4153/CJM-1980-013-2 Published online by Cambridge University Press

Posons $t = n/p$, et $E = A_p \otimes I_t$, $B_p \otimes I_t$. Comme le groupe d'automorphismes engendré dans $PGL(n, F)$ par l'image de $\langle E, M \rangle$ est $C_p \times C_p$, il est facile de voir que $\langle E, M \rangle$ est un groupe de type central, centralement immersible, et alors il existe un groupe tel que R_sG est simple. Donc il faut que $z = 1$.

Finalement, supposons qu'il existe un élément $a \in F^*$ qui n'ait pas de racine n-ième dans F. Alors il existe un nombre premier $p|n$, et un élément $C \in F^*$ n'ayant pas de racine p-ième. Comme dans les deux paragraphes précédents, on peut construire un groupe G d'ordre p tel que R_sG est simple.

On peut remarquer que les deux sortes d'obstructions obtenues en (iv) $\Rightarrow$ (i), du problème de la relevation de sous-groupes, ont de la signification cohomologique. Le manque de racines n-ièmes est mesuré par $F^*/F^{*n} = H^1(PGL(n, F), \mathbf{Z})$. Ce dernier détermine si les automorphismes individuels d'ordres finis peuvent être relevés. D'autre part, l'ensemble de racines de l'unité d'ordre n est précisément l'image de $H^2(GL(n, F), \mathbf{Z})$ dans $F^* = H^1(F^*, \mathbf{Z})$ obtenue en appliquant la cohomologie à

$$1 \to F^* \to GL(n, F) \to PGL(n, F) \to 1.$$

Alors l'obstruction complète est

$$F^*/F^{*n} \oplus \{z \in F | z^n = 1\}.$$

COROLLAIRE 4.3. *Si n est impair et F un corps réellement fermé, alors $R_sG \simeq RG^{op}$ pour tout $G <$ Aut (R).*

Démonstration. On note simplement que selon le théorème de Noether-Skolem, Aut $(R) = PGL(n, F)$; et $PGL(n, F)$ peut être relevé, d'où le résultat.

THÉORÈME 4.4. *Soit G un sous-groupe de $PGL(n, F)$ et supposons que G soit de torsion. Donc G est localement fini. Si de plus, les ordres de ses éléments sont tous relativement premiers à n, alors il existe un sous-groupe H de $GL(n, F)$ tel que $p(H) = G$ et $H \cap F^* = \{1\}$. (C'est-à-dire, G peut être relevé.)*

Démonstration. Pour demontrer que G est localement fini, on peut supposer que F soit algébriquement clos. Soit $H_0 = p^{-1}G \cap SL(n, F)$. On voit que $p(H_0) = G$ (car $F = \bar{F}$ pour l'instant), et $H_0 \cap \ker p$ est cyclique d'ordre n: H_0 est donc de torsion. Le theorème de Burnside implique que H_0 est localement fini, donc G l'est aussi.

Maintenant, on ne suppose pas que F soit algébriquement clos. On peut considérer G comme une limite directe de groupes finis, $G = \lim G_i$. On pose $J_i = p^{-1}G_i$, un sous-groupe de $GL(n, F)$, et pour i fixe, on suppose que l'ordre de G_i soit m; donc $(m, n) = 1$.

Il existe un homomorphisme, le *transfert*, σ_i: $J_i \to F^*$ [**7**, pp. 60–63]. Comme F^* est contenu dans le centre de J_i, $\sigma_i(x) = x^m$ pour tout $x \in J_i$. On forme

$H_i = \ker \sigma_i \cap SL(n, F)$, et on voit immédiatement que $H_i \cap F^* = \{1\}$ ($(m, n) = 1$). Nous allons maintenant demontrer que $p(H_i) = G_i$.

On choisit $g \in G_i$, et suppose que l'ordre de g soit d; alors $(d, n) = 1$. Il existe $y \in p^{-1}G_i$ tel que $p(y) = g$ et $y^d = aI$, où $a \in F^*$. Donc, $(\det y)^d = a^n$. Comme $(d, n) = 1$, il existe $b \in F^*$ tel que $b^d = a$. On forme $h = b^{-1}y$; alors $p(h) = g$ et $h^d = I$, d'où $\det h$ est une racine d-ième de l'unité. Comme $(n, d) = 1$, toutes les racines d-ièmes de l'unité possèdent elles-mêmes une racine n-ième de l'unité; il existe donc $c \in F^*$ tel que $c^n = \det h$. On forme $h_1 = c^{-1}h$. On voit que $(h_1)^d = c^{-d}h^d = I$, donc $(h_1)^m = I$, $\det h_1 = 1$, et $p(h_1) = g$, d'où $h_1 \in H_i$, donc $p(H_i) = G_i$.

Il est maintenant facile de voir que la famille $\{H_i\}$ correspondante à la famille $\{G_i\}$ est ainsi dirigée: si $G_i \leqq G_k$, alors $i \leqq k$, donc $J_i \leqq J_k$, d'où $m(i) \leqq m(k)$, de sorte que $\ker \sigma_i \subset \ker \sigma_k$, donc $H_i < H_k$. Le groupe $\cup H_i$ est le groupe voulu.

On considère le problème analogue pour les groupes: Etant donné un groupe fini G, est-ce qu'il existe un corps F, un entier n, et une immersion G^{op} dans $PGL(n, F)$, tel que R_sG soit simple? Ce n'est pas difficile de le vérifier si G est abélien, mais si $G = S_n$ où D_n ($n \neq 2^m$), nous verrons que R_sG n'est jamais simple, quelque soit le corps, ou l'entier n.

LEMME 4.5. *Si $G < PGL(n, F)$ est cyclique et si R_sG est simple, alors $[Z(R_sG):F] = |G|$.*

Démonstration. Choisissons $g \in G$ tel que $G = \langle g \rangle$. Soit $h \in p^{-1}(g)$; alors $p^{-1}G = \langle h, F^* \rangle$, donc $p^{-1}G$ est abélien, donc tous les éléments de G contribuent au centre.

PROPOSITION 4.6. *Supposons que R_sG soit simple, $G^{op} < PGL(n, F)$. Si G_p, un sous-groupe de Sylow de G, est cyclique, alors G_p est contenu dans le centre de G.*

Démonstration. Comme G_p est cyclique, chacun des éléments de G_p contribuent au centre de R_sG_p, et suivant § 2, au centre de R_sG, d'où leurs classes de conjugaison dans G ne se composent que d'un seul élément.

THÉORÈME 4.7. *Si G est d'une formes indiquées au-dessous,*

(a) *G est simple (non-abélien) de type connu;*

(b) *$G = S_n$ ($n \geqq 3$);*

(c) *$G = D_n$ ($n \neq 2^m$);*

alors quelque soit le corps F ou l'entier n, il n'existe pas d'immersion $G < PGL(n, F)$ telle que R_sG soit simple.

Démonstration. (a) Pour chacun de groupes simples connus il existe un nombre premier p tel que $p \| |G|$; appliquer 4.6.

(b) Selon le postulat de Bertrand, il existe un nombre premier p tel que $n/2 \leqq p \leqq n$, et alors $p \| n!$

(c) Tous les sous-groupes de Sylow d'ordre impair sont cycliques mais ne sont pas centraux.

https://doi.org/10.4153/CJM-1980-013-2 Published online by Cambridge University Press

Appendice 1. Réduction incomplète au cas intérieur. Sil'on n'exclut pas les automorphismes extérieurs, quelquechose de différent se passe. Si R_sG_{inn} est simple, utilisant

$$R_sG \simeq (R_sG_{\text{inn}})_c{}^G/_{G_{\text{inn}}}$$

et le fait que les automorphismes induits de G/G_{inn} restent extérieurs (voir par exemple, la théorème de Noether-Skolem), une application de la méthode classique "shortening proof" de Jacobson nous permet de conclure que R_sG est simple.

PROPOSITION *A-I. Si* G^{op} *est un sous-groupe de* Aut (R), *tel que* R_sG_{inn} *soit simple, alors* R_sG *est simple.*

D'autre part, même si G est un produit direct de G_{inn} et G/G_{inn} (et G_{inn} est cyclique), la simplicité de R_sG n'implique pas celle de R_sG_{inn}. Voici un exemple.

Soit $n = 4$, et $F = Q[\sqrt{b}]$, où $b > 0$. Considérons les matrices $A, B \in GL(4, F)$,

$$A = \begin{bmatrix} 0 & -4 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix}.$$

Soit g l'automorphisme obtenu de A, et h celui obtenu à partir de B suivi de l'automorphisme extérieur induit par $\sqrt{b} \mapsto -\sqrt{b}$. Comme $BAB^{-1} = -A$, $gh = hg$. Soit $G = \langle g \rangle \times \langle h \rangle$. On voit que $g^4 = 1$, $g^2 \neq 1$, $h^2 = 1$, et que les éléments h, gh, g^2h, g^3h sont tous extérieurs. En calculant le centre de $R_sG(R = M_4F)$, on obtient $Q[\sqrt{b}Ag]$ (car, par exemple, $(\sqrt{b}A)^h = \sqrt{b}A$). Comme $x^4 - 4b^2$ est irreductible (l'élément b n'est pas un carré dans Q), et comme $(\sqrt{b}Ag)^4 = 4b^2$, le centre de R_sG est un corps, d'où R_sG est une algèbre simple.

D'autre part, $G_{\text{inn}} = \langle g \rangle$, mais $R_s\langle g \rangle$ n'est pas simple. Son centre est $Q[\sqrt{b}][Ag]$; comme gA satisfait $x^4 = -4$, et la dimension du centre est 4, le centre ne peut pas être un corps, car $x^4 + 4$ n'est pas irreductible.

Si l'on remplace h par l'automorphisme induit par B, on obtient un groupe abélien $G < PGL(4)$ tel que R_sG soit simple (le centre est engendré par A^2g^2 et le centre de R), mais $L = \langle g^2 \rangle$ (voir § 3) n'est pas un facteur direct.

Appendice 2. La sous-algèbre fixe. Supposons que $G^{\text{op}} < PGL(n, F)$, et que R_sG soit simple. On forme $H = p^{-1}G^{\text{op}}$, et on considère $\langle H \rangle$, l'algèbre engendrée par H. Si $\{r_g\}$ est un système complet de représentatifs de H par rapport à F^*, alors,

$$\langle H \rangle = \{\sum r_g\lambda_g | \ \lambda_g \in F^*\},$$

et il y a un isomorphisme naturel $\langle H \rangle \to F^tG$, avec le cocycle approprié. Si on considère $H' = \{r \in R | rh = hr \text{ pour tout } h \in H\}$, H' est egal à R^G, et comme

https://doi.org/10.4153/CJM-1980-013-2 Published online by Cambridge University Press

$H' = \langle H \rangle'$, $\langle H \rangle \subset (R^G)'$. Comme R^G est simple, son centre est donc un corps-alors le centre de $\langle H \rangle$ est un corps contenant F. Comme F^tG est semi-simple, alors $\langle H \rangle$ est simple, d'où $\langle H \rangle = (R^G)'$.

On peut dire que parmi les sous-groupes G de $PGL(n, F)$ tels que R^G soit simple, ceux pour lesquels R_sG est simple sont ceux qui donnent R^G d'une manière la plus efficace, c'est-à-dire tel que $[R:R^G]_F = |G|$.

La démonstration du lemme suivant est due à Michel Racine.

LEMME A-II. *Soit D une sous-algèbre (avec unité) simple, sur un corps F, d'une algèbre simple centrale et de dimension finie, A. Si $F \subset Z(D)$, alors*

$$\dim_F D \cdot \dim_F C_A(D) = \dim_F A.$$

($C_A(D)$ est le centralisateur de D dans A.)

Démonstration. Soit $K = Z(D)$. Soit n^2 la dimension (sur F) de A, et $t = [K:F]$. Alors t divise n; $n = rt$. Posons $E = C_A(D)$, et remarquons qu'il y a un isomorphisme (surjectif):

$$D \otimes_K E \to C_A(K)$$

car E, D et $D \otimes_K E$ sont K-algebres simples centrales. Maintenant, $\dim_K C_A(D) = r^2$, donc

(1) $\dim_K D \cdot \dim_K E = r^2$.

Mais, $t\dim_K D = \dim_F D$, et $t\dim_K E = \dim_F E$, et aussi $n^2 = r^2t^2$; le résultat est une conséquence de (1).

THÉORÈME A-III. *Pour G un sous-groupe fini de $PGL(n, D)$ (D etant une algèbre de division de dimension finie sur son centre), les conditions suivantes sont équivalentes:*

(a) *R_sG^{op} est simple (où $R = M_nD$);*

(b) *R^G est simple et $[R:R^G] = |G|$;*

(c) *$\dim_F \langle p^{-1}G \rangle = |G|$, (où $F = Z(D)$) et $\langle p^{-1}G \rangle$ est simple.*

Démonstration. (a) $\Rightarrow$ (b). Les mêmes idees utilisées au § 1.

(b) $\Rightarrow$ (c). Formons $A = \langle p^{-1}G \rangle$. Alors, pour un ensemble fixe d'éléments r_g (un pour chaque g dans G) avec r_g dans $p^{-1}(g)$,

$$A = \{\sum r_g\lambda_g |\ \lambda_g \in F, g \in G\}.$$

Le centralisateur de A dans R est précisément R^G, donc le centre de A doit être un corps.

Soit B le centralisateur de R dans R_sG^{op} (alors, $R_sG^{op} = M_nB$). Il est facile de voir que $B = \{\sum gr_g\lambda_g |\ \lambda_g \in F, g \in G\}$, d'où on en deduit que B est une algèbre de groupe tordue de F, $B = F^tG$. Il existe une application linéare $B \to A$, engendrée par $gr_g \mapsto r_g$. Nous vérifions que cette application est un

https://doi.org/10.4153/CJM-1980-013-2 Published online by Cambridge University Press

homomorphisme à gauche:

$$gr_g hr_g = hgr_h r_g \text{ (dans } R_s G^{\mathrm{op}})$$
$$= hgr_{hg}(r_{hg}^{-1} r_h r_g).$$

Mais $r_h r_g = r_{hg}(r_{hg}^{-1} r_h r_g)$, et $r_{hg}^{-1} r_h r_g \in F^*$.

Comme B est une algèbre de groupe tordue de dimension finie, B et donc A est semisimple. Comme $Z(A)$ est un corps, A est simple; par le théorème du deuxième centralisateur, $C_R(A) = R^G$. Le lemme précédent nous assure que

$$\dim_F R^G \cdot \dim_F A = \dim_F R.$$

Donc $\dim A = |G|$, d'où l'homomorphisme à gauche est un isomorphisme à gauche, donc B est simple. Comme $R_s G^{\mathrm{op}} = M_n B$, la démonstration de (c) $\Rightarrow$ (a) est claire.

LEMME A-IV. *Si $H < G < PGL(n, F)$, R^G, R^H sont simples, et $[R:R^G] = |G|$, alors $[R:R^H] = |H|$.*

Démonstration. (Suit la démonstration du théorème ci-dessus). La restriction de l'homomorphisme à gauche $B \to A$ induit un isomorphisme à gauche

$$R'^{R_s H} \to p^{-1}H.$$

Donc $|H| = \dim_F p^{-1}H$. Comme R et $R_s H$ sont semisimples, $\langle p^{-1}H \rangle$ est semisimple; mais son centralisateur est l'algèbre simple R^H, et comme ci-dessus on en déduit que $\langle p^{-1}H \rangle$ est simple. Par le théorème du deuxième centralisateur

$$\langle p^{-1}H \rangle = (R^H)'^R,$$

donc $\dim R^H \cdot \dim p^{-1}H = \dim R$, d'où $\dim R^H = (\dim R)/|H|$.

COROLLAIRE A-V. *Supposons $G < PGL(n, F)$, et que $R_s G$ soit simple. Soit H un sous-groupe de G. Alors,*

(a) *$R_s H$ est simple si, et seulement si, R^H est simple;*

(b) *Si H est un sous-groupe normal de G, et si $S = R^H$ est simple, alors, $G_1 = G/H$ est un groupe d'automorphismes (au sens naturel) de S, S^{G_1} est simple, et $[S:S^{G_1}] = |G_1|$, d'où $S_s G_1$ est simple.*

On a suggeré ([**1**], par exemple) que les groupes de type central sont résolubles. Nous présentons un résultat qui pourrait peur-être aider à le demontrer.

Un groupe fini D est *projectivement de type central*, s'il existe un groupe de type central P tel que $P/Z(P)$ est isomorphe à G.

PROPOSITION A-VI. *Si G est un groupe projectivement de type central, et si H est un sous-groupe normal de G, et si de plus H est projectivement de type central, alors G/H est projectivement de type central.*

Démonstration. Il existe un corps algébriquement clos, F, tel que $G < PGL(n, F)$, et tel que $p^{-1}G \cap SL(n, F) = G_2$ est centralement immersible

https://doi.org/10.4153/CJM-1980-013-2 Published online by Cambridge University Press

dans $GL(n, F)$ (3.5). Formons $H_2 = p^{-1}H \cap SL(n, F)$; alors, $Z(H_2) = Z(G_2) \subset F^*$, d'où H_2 est centralement immersible dans $GL(n, F)$. Les deux algèbres, R_sG, R_sH, sont donc simples (3.5), et A-V nous assure que $G_1 = G/H = G_2/H_2$ est projectivement de type central (3.5).

Je voudrais remercier Bill Scott, qui m'a considerablement aidé lorsque j'ai commencé les recherches présentées ici.

Bibliographie

1. F. R. DeMeyer and G. J. Janusz, *Finite groups with an irreducible representation of large degree,* Math. Zeit. *108* (1969), 145–153.
2. J. Fisher and J. Osterburg, *Some results on rings with finite group actions*, Proc. Ohio U. Ring Theory Conf. (to appear).
3. M. Hall Jr. and J. K. Senior, *The Groups of order* $2^n (n \leqq 6)$, (Macmillan, London, 1964).
4. D. Handelman, J. Lawrence and W. Schelter, *Skew group rings*, Houston J. Math. *4* (1978), 175–198.
5. I. N. Herstein, *Noncommutative rings*, Carus Mathematical Series *15* (1968).
6. H. Pahlings, *Gruppen mit irreduziblen darstellungen höhen grades*, Mitteil. Math. Sem. Giessen Heft *85* (1970), 27–44.
7. W. Scott, *Group theory* (Prentice Hall, New Jersey, 1964).

Université d'Ottawa,
Ottawa, Ontario