La démonstration par Artin-Tate du théorème de l'idéal principal

Daniel Ferrand
Janvier 2011

Le théorème en question affirme que pour un groupe, disons fini, G, le transfert dans le groupe $D(G)$ des commutateurs, $V : G/D(G) \longrightarrow D(G)/DD(G)$ est l'homomorphisme trivial. La démonstration *linéarise* la situation en passant aux algèbres de groups $\mathbf{Z}G$, ce qui permet de ramener le transfert à une trace ordinaire. Cette démonstration suit d'assez près la méthode exposée par Artin et Tate [1], aux pages 189 à 196 ; la principale différence réside dans la définition du "splitting module" qui apparaît ici comme un banal produit tensoriel au lieu d'être, auparavant, laborieusement construit à partir d'un 2-cocycle ; d'ailleurs aucun 2-cocycle n'est plus utilisé dans cette note.

1. *Soient G un groupe et $\varepsilon : \mathbf{Z}G \to \mathbf{Z}$ le morphisme tel que $\varepsilon(g) = 1$ pour tout $g \in G$; notons $I(G)$ l'idéal bilatère noyau de ce morphisme ; il est librement engrendré, comme $\mathbf{Z}$-module, par les $g-1$. L'application $c_G : G \longrightarrow I(G),\ g \mapsto g-1$ est le* 1-cocycle universel *; il induit un isomorphisme de groupes, noté $\tilde{c}_G$,*

$$G^{\mathrm{ab}} = G/D(G) \xrightarrow{\sim} I(G)/I(G)^2.$$

Enfin, si on pose $S = \sum_{g\in G} g$, alors $\mathrm{Ann}_{\mathbf{Z}G}(I(G))$ est le groupe engendré par S.

Pour g et h dans G, la relation dans $\mathbf{Z}G$,

$$gh - 1 = g - 1 + g(h-1)$$

montre que c_G est un 1-cocycle. Par ailleurs, soit $c : G \to E$ un 1-cocycle à valeurs dans un G-module E. Comme $I(G)$ est $\mathbf{Z}$-libre, de base les $g-1$, l'application c se prolonge en un morphisme de groupes additifs $I(G) \to E$ en envoyant $g-1$ sur $c(g)$; c'est un morphisme de G-modules puisque l'image de $h(g-1) = (hg-1) - (h-1)$ est $c(hg) - c(h) = hc(g)$.
Notons $I = I(G)$. La relation $gh-1 = (g-1)+(h-1)+(g-1)(h-1)$ montre que c_G induit un morphisme de groupes $G \to I/I^2$, visiblement surjectif.
Dans l'autre sens, considérons l'application $I \to G^{\mathrm{ab}}$ définie sur les éléments de la base par $g-1 \mapsto g^{\mathrm{ab}} = g$ mod.$D(G)$; elle est nulle sur I^2 puisque l'image de $(g-1)(h-1) = (gh-1) - (g-1) - (h-1)$ est $(gh)^{\mathrm{ab}}(g^{\mathrm{ab}})^{-1}(h^{\mathrm{ab}})^{-1} = 1$.
Il est enfin, clair que les deux applications ainsi définies sont inverses l'une de l'autre.□

Le second ingrédient est un résultat d'algèbre commutative, genre lemme de Nakayama. Le choix des notations est lié à celles de Artin-Tate.
2. *Soit G un groupe abélien fini d'ordre n ; on note $S = \sum_{g\in G} g \in \mathbf{Z}G$. Soit B un $\mathbf{Z}G$-module de type fini, muni d'une application $\mathbf{Z}G$-linéaire* surjective

$$B \longrightarrow I(G).$$

On suppose que le groupe $B/I(G)B$ est fini d'ordre N. Alors n divise N, soit $N = en$, et on a $eSB = 0$.

Notons $I = I(G)$. L'application $\mathbf{Z}G$-linéaire donnée $B \to I$ induit une application surjective $B/IB \to I/I^2$; comme G est abélien, l'application $G \to I/I^2$ est un isomorphisme, donc le groupe I/I^2 est fini d'ordre n ; ainsi, n divise N.
Le groupe abélien fini B/IB est somme directe de groupes cycliques d'ordre $e_1, \dots, e_m$; en relevant des générateurs de ces groupes on trouve des éléments $b_1, \dots, b_m$ dans B tels que $e_i b_i \in IB$. Choisissons un système $b_{m+1}, \dots, b_s$ générateur du groupe IB (Il est de type fini, tout comme B et I), et posons $e_{m+1} = \cdots = e_s = 1$. On a donc les propriétés suivantes :
1) Les éléments $b_1, \dots, b_s$ engendrent B.
2) Pour $i = 1, \dots, s$, on a $e_i b_i \in IB$.
3)$\prod_{i=1}^{s} e_i = N$.

1. E. Artin and J. Tate, *Class Field Theory*, Cours donné à Princeton en 1951-52, Publié par Harvard Univ. Press (1961) ; le passage en question est recopié fidèlement dans E. Weiss, *Cohomology of Groups*, Acad. Press, (1969)

D'après 1) et 2), on peut écrire, pour chaque i, $e_i b_i = \sum_{j=1}^{s} \theta_{ij} b_j$, avec $\theta_{ij} \in I$. Comme l'anneau $\mathbf{Z}G$ est commutatif, le déterminant de matrices à coefficients dans $\mathbf{Z}G$ est bien défini. Posons $\gamma = \det(e_i\delta_{ij} - \theta_{ij})$; on a $\gamma B = 0$, donc aussi $\gamma I = 0$ puisque I est un quotient de B ; donc il existe un entier t tel que $\gamma = tS$. En utilisant l' morphisme $\varepsilon : \mathbf{Z}G \longrightarrow \mathbf{Z}$, qui est nul sur I, on voit, d'une part que $\varepsilon(\gamma) = tn$, et d'autre part que

$$\varepsilon(\gamma) = \det(\varepsilon(e_i\delta_{ij} - \theta_{ij})) = \prod e_i = N = en.$$

Par suite, $t = e$, et on a bien $eSB = 0$. □

3. *Soit U un groupe tel que $D(U)$ soit de type fini et que $U^{\mathrm{ab}} = U/D(U)$ soit fini. Alors le transfert $U^{\mathrm{ab}} \longrightarrow D(U)^{\mathrm{ab}}$ est l'homomorphisme trivial.*

En passant aux quotients par $DD(U)$, on se ramène au cas où ce dernier groupe est trivial. Posons $A = D(U)$ et $G = U^{\mathrm{ab}} = U/A$, de sorte que A est un groupe abélien de type fini, et G un groupe fini. Notons que la suite exacte

$$(\star) \qquad 1 \longrightarrow A \longrightarrow U \xrightarrow{q} G \longrightarrow 1$$

montre que la conjugaison $a \mapsto uau^{-1}$, par un élément $u \in U$, définit un automorphisme de A qui ne dépend que de l'image de u dans G ; A est donc muni d'une structure de G-module, ce qui manque à U. Pour la démonstration on "remplace" cette suite exacte par une suite exacte de G-modules

$$1 \longrightarrow A \xrightarrow{j} B \xrightarrow{q'} I(G) \longrightarrow 0$$

où B est ce que Artin et Tate nomment le "splitting module" associé à la suite $(\star)$; leur définition, peut aujourd'hui être simplifiée en

$$B = I(U) \otimes_{\mathbf{Z}U} \mathbf{Z}G$$

L'homomorphisme $q : U \to G$ induit un homomorphisme de U-modules $I(q) : I(U) \longrightarrow I(G)$, d'où un homomorphisme de G-modules

$$q' : B = I(U) \otimes_{\mathbf{Z}U} \mathbf{Z}G \longrightarrow I(G).$$

Il reste à définir l'application G-linéaire $j : A \to B$, et à vérifier que son image est égale au noyau de q'. Le noyau du morphisme d'anneaux $\mathbf{Z}(q) : \mathbf{Z}U \longrightarrow \mathbf{Z}G$ est le groupe engendré par les éléments de la forme $u(a-1)$, avec $u \in U$ et $a \in A$; en effet, un élément du noyau est somme d'éléments du noyau de la forme $\sum n_x x$ où les x parcourent une orbite $uA \subset U$; comme on a $\sum_{x \in uA} n_x = 0$, cet élément s'écrit aussi $u(\sum_{a \in A} n_{ua} a) = u(\sum_{a \in A, a \neq 1} n_{ua}(a-1))$.
On peut donc écrire

$$(\star\star) \qquad B = I(U) \otimes_{\mathbf{Z}U} \mathbf{Z}G = I(U)/I(U)I(A) = I(U) \otimes_{\mathbf{Z}A} \mathbf{Z}.$$

Ce noyau est aussi celui de $I(q) : I(U) \longrightarrow I(G)$; c'est l'idéal à gauche de $\mathbf{Z}U$ engendré par l'image de l'application $I(A) \longrightarrow I(U)$.
Montrons que l'application $I(A) \otimes_{\mathbf{Z}A} \mathbf{Z} \longrightarrow I(U) \otimes_{\mathbf{Z}A} \mathbf{Z}$ est injective : on dispose d'une suite exacte de $\mathbf{Z}A$-modules

$$0 \longrightarrow I(A) \longrightarrow \mathbf{Z}A \times I(U) \longrightarrow \mathbf{Z}U \longrightarrow 0$$

Puisque A opère librement par multiplication à droite sur U, le $\mathbf{Z}A$-module $\mathbf{Z}U$ est libre ; la suite exacte précédente est donc scindée ; elle le reste par tensorisation par le $\mathbf{Z}A$-module $\mathbf{Z}$; cela montre l'injectivité annoncée. Bref, en tenant compte de $(\star\star)$, on a donc une suite exacte

$$0 \longrightarrow I(A)/I(A)^2 \longrightarrow B \xrightarrow{q'} I(G) \longrightarrow 0$$

Notons la commutativité du carré suivant, où par abus de notation, on a écrit c_U pour désigner le composé $U \xrightarrow{c_U} I(U) \longrightarrow I(U)/I(U)I(A) = B$, et où $\tilde{c}_A$ est un isomorphisme puisque A est abélien

$$\begin{array}{ccc} A & \longrightarrow & U \\ \downarrow{\scriptstyle \tilde{c}_A} & & \downarrow{\scriptstyle c_U} \\ I(A)/I(A)^2 & \longrightarrow & B \end{array}$$

L'application cherchée $j : A \longrightarrow B$ est la diagonale de ce carré. La G-linéarité de j mérite d'être précisée : la structure de G-module sur $B = I(U) \otimes_{\mathbf{Z}U} \mathbf{Z}G$ provient du produit à droite dans $I(U)$; soit $g \in G$, et soit $u \in U$ un relèvement de g ; pour $a \in A$, il faut donc vérifier que $j(a^g) = j(u^{-1}au)$ est égal à $j(a)g$, c'est-à-dire à la classe dans B de $(a-1)u$; or, comme $u^{-1}au$ est dans A, on a, dans $I(U)$,

$$(a-1)u - (u^{-1}au - 1) = (u-1)(u^{-1}au - 1) \in I(U)I(A);$$

d'où le résultat.

Notons les isomorphismes évidents : $B/I(G)B = B \otimes_{\mathbf{Z}G} \mathbf{Z} = I(U) \otimes_{\mathbf{Z}U} \mathbf{Z} = I(U)/I(U)^2$; on en déduit que le cardinal de $B/I(G)B$ est égal à celui de $U/D(U)$, c'est-à-dire à celui de G. On peut appliquer le §2 à l'application $q'B \to I(G)$, et avec $e = 1$, de sorte que l'on en déduit la relation $SB = 0$.