Canad. Math. Bull. Vol. **32** (4), 1989

GÉNÉRALISATION D'UN LEMME DE KUMMER*

PAR
KLAUS HOECHSMANN

A la mémoire de mon ami Jean-Claude

ABSTRACT. If A is a finite abelian group and $\mathbf{Z}A$ its integral group ring, consider units $u \in \mathbf{Z}A$ which have coefficient sum $= 1$ and are fixed under the involution $a \longrightarrow a^{-1}$, $a \in A$. For an odd regular prime p and a p-group A, it is shown that $u \equiv 1 \bmod p$ if only if $u = \pi(v)v^{-p}$, where v is the same kind of unit, and π is the ring endomorphism given by $a \longrightarrow a^p$, $a \in A$.

Soit p un nombre premier impair, ζ une racine primitive p-ième de l'unité. En réduisant modulo p l'anneau $\mathbf{Z}[\zeta]$ des entiers cyclotomiques, on obtient un anneau local artinien $\mathbf{F}_p[\xi]$ dont l'idéal maximal est engendré par $(\xi - 1)$, avec $(\xi - 1)^{p-1} = 0$. Dans sa démonstration du théorème de Fermat pour les nombres premiers *réguliers*, Kummer se sert du lemme suivant:

Si u est une unité (élément inversible) de $\mathbf{Z}[\zeta]$ dont l'image dans $\mathbf{F}_p[\xi]$ est de la forme $a \in \mathbf{F}_p$, sans terme en $(\xi - 1)$, alors $u = v^p$ avec $v \in \mathbf{Z}[\zeta]$. (Voir la fin de son article [4].)

Réduisons d'abord ce lemme à son essentiel. Comme $a^{p-1} = 1$, et $(p - 1)$ est inversible modulo p, on ne perd rien en supposant $a = 1$. Il s'agit donc du noyau de l'homomorphisme de réduction

$$\rho : U\mathbf{Z}[\zeta] \longrightarrow U\mathbf{F}_p[\xi]$$

entre les groupes d'unités. Or, d'après Dirichlet, on sait que $U\mathbf{Z}[\zeta]$ est de la forme $W \times L$, ou W est un groupe d'ordre p, et L est un $\mathbf{Z}$-module libre de rang $(p - 3)/2$. De façon plus précise, ce dernier consiste des unités $U_*\mathbf{Z}[\zeta]$ qui sont stables sous l'involution $\zeta \longrightarrow \zeta^{-1}$ et $\equiv 1 \bmod (\zeta - 1)$. W est simplement le groupe engendré par ζ; il n'a rien à faire avec le noyau de ρ. Par contre, toutes les puissances p-ièmes de $U_*\mathbf{Z}[\zeta]$ y sont, car du coté de $\mathbf{F}_p[\xi]$ tout élément $\equiv 1 \bmod (\xi - 1)$ est d'ordre p ou 1, puisque $(\xi - 1)^p = 0$. Le lemme de Kummer affirme que, dans le cas où p est régulier, le noyau de ρ ne contient pas d'autres éléments.

Reçu par la rédaction le 22 avril 1988 et, sous une forme révisée, le 21 juillet 1988.
*Travail subventionné par le CRSNG du Canada.
AMS Classification (1980): 20C05, 16A25, 16A18.

Soit C un groupe d'ordre p, et $U_*\mathbf{Z}C$ le groupe des unités, dans l'anneau de groupe $\mathbf{Z}C$, qui sont stables sous l'involution $x \longrightarrow x^{-1} (x \in C)$ et $\equiv 1$ modulo l'idéal engendré par les $(x - 1)$. On voit facilement que l'application d'un générateur de C sur ζ donne un isomorphise $U_*\mathbf{Z}C \simeq U_*\mathbf{Z}[\zeta]$. Le lemme de Kummer est donc équivalent à l'affirmation que la réduciton $\rho : U_*\mathbf{Z}C \longrightarrow U_*\mathbf{F}_pC$ ne trivialise que les puissances p-ièmes, toujours supposant que p soit régulier. Nous nous proposons de généraliser ce résultat aux p-groupes abeliens finis quelconques. Il est évident, pour un tel groupe A, que ker ρ contient tous les éléments de la forme $\pi(u)u^{-p}$, où π est l'endomorphisme de $\mathbf{Z}A$ induit par l'homomorphisme de groupes $A \longrightarrow A^p$ donné par $a \longrightarrow a^p$. En effet, $\pi(u)$ et u^p coïncident dans $\mathbf{F}_pA$. Il sera commode de considérer l'endomorphisme ψ de $U_*\mathbf{Z}A$ défini par $\psi(u) = \pi(u)u^{-p}$. Montrons d'abord qu'il est injectif. Si l'on avait $\pi(u) = u^p$, on obtiendrait par induction que $\pi^r(u) = u^{p^r}$ pour tout r. Or, pour r assez grand, on a $\pi^r(u) = 1$, donc u serait d'ordre fini. Mais il n'y a pas de torsion dans $U_*\mathbf{Z}A$, qui s'identifie, par la décomposition de Wedderburn, à un sous-groupe d'unités dans un produit direct de corps de nombres réels. On arrive à la même conclusion quand on remplace l'anneau $\mathbf{Z}$ de coefficients par celui des entiers p-adiques $\mathbf{Z}_p$ (complété). Dans ce cas, il faut se rappeler que le groupe $U_*\mathbf{Z}_p[\zeta]$ est un $\mathbf{Z}_p$-module libre de rang $p^{r-1} \cdot (p - 1)/2$, si ζ est une racine primitive p^r-ième de 1 (voir [1], 15.5).

THÉORÈME. *Soit p un nombre premier impair, A un p-groupe abélien fini, K l'anneau des entiers ou rationnels ($K = \mathbf{Z}$) ou p-adiques ($K = \mathbf{Z}_P$). Considérons la suite*

$$1 \longrightarrow U_*KA \xrightarrow{\psi} U_*KA \xrightarrow{\rho} U_*\mathbf{F}_pA,$$

où ψ et ρ sont définis comme ci-dessus. Alors cette suite est exacte, pourvu que p soit régulier au cas $K = \mathbf{Z}$.

La démonstration se fera par induction sur le nombre m minimal tel que $\pi^m(A) = \{1\}$. Pour $m = 0$, il n'y a rien à prouver. Comme instrument de décalage on se servira d'un morphisme de suites que voici:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & U_*K(A,A_p) & \longrightarrow & U_*KA & \xrightarrow{\pi} & U_*KA^p & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle \rho} & & \downarrow & & \\
1 & \longrightarrow & U_*\mathbf{F}_p(A,A_p) & \longrightarrow & U_*\mathbf{F}_pA & \longrightarrow & U_*\mathbf{F}_pA^p & \longrightarrow & 1
\end{array}$$

$U_*K(A, A_p)$ est simplement le noyau de π. La notation vient du fait que l'idéal annullé par $\pi : KA \longrightarrow KA^p$ est normalement désigné par $\Delta K(A, A_p)$; il est engendré par les éléments $(a - 1)$ où $a \in A_p = \ker(A \xrightarrow{\pi} A^p)$.

Il est clair que la deuxième suite est exacte. Dans le cas $K = \mathbf{Z}_p$ l'exactitude à droite de la première est aussi évidente; pour $K = \mathbf{Z}$ et p régulier, elle résulte de [2], Théorème 3.

Soit maintenant $u \in U_*KA$ avec $\rho(u) = 1$. Par hypothèse d'induction, on trouve un $w \in U_*KA$ tel que $\pi(u) = \psi(\pi(w)) = \pi\psi(w)$. Donc $u_1 = u\psi(w)^{-1}$ est dans $U_*K(A, A_p)$ et $\rho(u_1) = 1$. On montrera que $u_1 = v^p$, pour un $v \in U_*K(A, A_p)$, ce qui achèvera la démonstration puisque $v^p = \psi(v^{-1})$.

Voici qu'il faut distinguer les deux cas. Si $K = \mathbf{Z}_p$, le groupe $U_*\mathbf{Z}_p(A, A_p)$ consiste de tous les éléments de $1 + \Delta_*\mathbf{Z}_p(A, A_p)$, l'astérisque désignant toujours la stabilité par rapport à l'involution $a \longrightarrow a^{-1}$. Or, on sait que le logarithme donne un isomorphisme $U_*\mathbf{Z}_p(A, A_p) \simeq \Delta_*\mathbf{Z}_p(A, A_p)$, ce qui serait faux sans l'astérisque d'ailleurs (voir [3], Theorem 1). Alors $\rho(u_1) = 1$ signifie que $u_1 = 1 + p\delta$ avec $\delta \in \Delta_*\mathbf{Z}_p(A, A_p)$. En conséquence, $\log u_1 \in p\Delta_*\mathbf{Z}_p(A, A_p)$, et u_1 est une p-ième puissance.

Le cas $K = \mathbf{Z}$, p régulier, est plus délicat. Abrégeons U/U^p par $\bar{U}$, et notons que nous savons déjà l'injectivité de la deuxième flèche dans

$$\bar{U}\,\mathbf{Z}(A, A_p) \longrightarrow \bar{U}\,\mathbf{Z}_p(A, A_p) \xrightarrow{\rho} U_*\mathbf{F}_p(A, A_p).$$

Tout revient à établir celle de la première.

Soit G le groupe multiplicatif $U(\mathbf{Z}/p^m\mathbf{Z})$ qui opère de manière naturelle sur tous les groupes d'unités en question. Il opère également, de façon galoisienne, sur toutes les composantes simples de l'algèbre $\mathbf{Q}A$. Ceci implique que la norme N_G est égale à 1 pour tout élément $u \in U_*\mathbf{Z}A$. En effet, puisque $u \equiv 1$ modulo l'idéal $(x-1)\,\mathbf{Z}A$, son image dans chaque composante $\mathbf{Q}[\zeta]$ de Wedderburn est une unité de $\mathbf{Z}[\zeta]$ congruente à 1 modulo l'idéal $(\zeta - 1)\,\mathbf{Z}[\zeta]$, qui est l'unique idéal premier au dessus de $p\mathbf{Z}$. Il en est de même pour tous les conjugués galoisiens et pour la norme galoisienne. Celle-ci est donc une unité de $\mathbf{Z}$, congruente à 1 modulo p, c'est-à-dire égale à 1, parce que p est impair. Les images de $N_G u$ dans les composantes $\mathbf{Q}[\zeta]$ sont des puissances de ces normes galoisiennes, donc toutes réduites à 1, d'où $N_G u = 1$. L'extension de scalaires $\mathbf{Z} \longrightarrow \mathbf{Z}_p$ applique alors $U_*\mathbf{Z}A$ dans le sous-groupe $U'_*\mathbf{Z}_pA$ d'éléments de norme 1. Or, on sait que l'image de $U_*\mathbf{Z}A$ dans $U'_*\mathbf{Z}_pA$ est dense, si p est régulier (voir [2], Theorem 1). Autrement dit, l'inclusion $\mathbf{Z}A \longrightarrow \mathbf{Z}_pA$ induit un isomorphisme $\hat{\imath} : \hat{U}_*\mathbf{Z}A \simeq U'_*\mathbf{Z}_pA$, où, pour un $\mathbf{Z}$-module libre X de rang fini, $\hat{X}$ désigne la complétion p-adique $X \otimes \mathbf{Z}_p$. Comme on a toujours $\bar{X} = X \otimes \mathbf{F}_p = \hat{X} \otimes_p \mathbf{F}_p$, $\otimes_p$ étant le produit tensoriel par rapport à $\mathbf{Z}_p$, il s'ensuit que $\hat{\imath} \otimes_p \mathbf{F}_p$ donne un isomorphisme $\bar{\imath} : \bar{U}_*\mathbf{Z}A \simeq \bar{U}'_*\mathbf{Z}_pA$.

Revenons à l'élément $u_1 \in U_*\mathbf{Z}(A, A_p)$ et supposons que, dans $U_*\mathbf{Z}_p(A, A_p)$, on ait $u_1 = v_1^p$. Comme $N_G u_1 = 1$, on aura $(N_G v_1)^p = 1$, donc $v_1 \in U'_*\mathbf{Z}_pA$ puisqu'il n'y a pas de torsion. Grâce à l'isomorphisme cité plus haut, on trouve un $v \in U_*\mathbf{Z}A$, tel que $u_1 = v^p$. Mais $1 = \pi(u_1) = \pi(v)^p$ entraîne $\pi(v) = 1$, encore faute de torsion. C'est-à-dire, $u_1 = v^p$ avec $v \in U_*\mathbf{Z}(A, A_p)$, comme prévu.

Remarque. Dans le cas $K = \mathbf{Z}$ la restriction aux éléments stables sous l'involution $a \longrightarrow a^{-1}$ ne fait qu'éliminer la torsion, mais dans le cas p-adique elle est importante. Si on essaye d'étendre le théorème au groupe $U_1\mathbf{Z}_pA = \ker \pi^m$, on trouvera qu'il est faux. Par example, si $A = C$ est d'ordre p, les dimensions sur $\mathbf{F}_p$ de $\bar{U}_1\mathbf{Z}_pC$ et $U_1\mathbf{F}_pC$ sont p et $p-1$, respectivement. Signalons enfin que le théorème reste valable si on

le restreint au noyau de la G-norme $U'_*\mathbf{Z}_pA \subset U_*\mathbf{Z}_pA : u = \psi(v)$, $N_G u = 1$ entraîne $\psi(N_G v) = 1$, d'où $N_G v = 1$.

Bibliographie

1. H. Hasse, *Zahlentheorie*, Akademie-Verlag, Berlin (1963).

2. K. Hoechsmann and S. K. Sehgal, *Units in regular abelian p-groups rings*, J. of Number Theory **30**, 375–381 (1988).

3. K. Hoechsmann and J. Ritter, *Logarithms and units in p-adic p-group rings*, Arch. d. Math., **49**, 23–28 (1987).

4. E. Kummer, *Beweis des Fermat'schen Satzes der Unmöglichkeit von* $x^\lambda + y^\lambda = z^\lambda$ *für eine unendliche Anzahl Primzahlen* λ, Monatsber. Akad. Wiss. Berlin, 1847, 305–319; Collected Papers I, p. 297.

University of British Columbia
Vancouver, Canada