ACTA ARITHMETICA
XXXIX (1981)

Remarques sur la structure galoisienne des unités des corps de nombres

par

JEAN-JACQUES PAYAN (St. Martin d'Hères)

Soit K une extension galoisienne de $\boldsymbol{Q}$ de groupe de Galois G. On note U (resp. T) le groupe des unités (resp. des racines de l'unité) de K et on pose $E = U/T$. Si ε est dans U, on note $\bar{\varepsilon}$ son image dans U/T. On dira que ε est une unité de Minkowski de K si et seulement si $\lambda \in \boldsymbol{Z}[G] \to \overline{\lambda\varepsilon}$ de $\boldsymbol{Z}[G]$ dans E est surjective.

Pour tout sous-groupe H de G, on note 1_H^G le caractère de G induit par le caractère trivial de H, et $\tilde{H}$ la somme des éléments de H. Si K est non réel, on note γ la restriction à K de la conjugaison complexe et $C = \{1, \gamma\}$. On sait que tout sous-G-module d'indice fini de E admet $1_1^G - 1_G^G$ comme caractère si K est réel et $1_C^G - 1_G^G$ si K est non réel et que tout $\boldsymbol{Z}[G]$-module sans $\boldsymbol{Z}$-torsion associé à un tel caractère s'injecte sur un sous-module d'indice fini de E.

R. Brauer [1] et C. D. Walter [5] ont utilisé comme $\boldsymbol{Z}[G]$-modules témoins d'une part le module $\mathscr{L} = \boldsymbol{Z}[G]/\boldsymbol{Z}\tilde{G}$ (resp. $\boldsymbol{Z}[G]\tilde{C}/\boldsymbol{Z}\tilde{G}$) de l'autre le module dual $\mathscr{L}^*$ défini par la suite exacte

$$0 \to \mathscr{L}^* \to \boldsymbol{Z}[G] \to \boldsymbol{Z} \to 0 \quad (\text{resp. } 0 \to \mathscr{L}^* \to \boldsymbol{Z}[G]\tilde{C} \to \boldsymbol{Z} \to 0).$$

N. Moser [3] a montré que si K est réel, il admet une unité de Minkowski si et seulement si $E \simeq \mathscr{L}$ et que si K est imaginaire et G diédral d'ordre $2p$, il peut exister des unités de Minkowski même si E n'est pas isomorphe à $\mathscr{L}$.

Le travail qui suit a pour objet de répondre aux deux questions suivantes:

1. Pour quels G, $\mathscr{L}$ et $\mathscr{L}^*$ sont-ils $\boldsymbol{Z}[G]$-isomorphes?

2. Pour quels G la situation décrite par Nicole Moser (existence d'une unité de Minkowski de norme 1 sur le sous-corps réel maximal) peut-elle se produire?

I. Isomorphie de $\mathscr{L}$ et $\mathscr{L}^*$. Rappelons d'abord le résultat suivant:

THÉORÈME (Walter [5]). *Soient M et N deux $\boldsymbol{Z}[G]$-modules de type*

fini sans $\mathbf{Z}$*-torsion de même caractère (on peut donc supposer* $\mathbf{Q}\otimes_{\mathbf{Z}}M = \mathbf{Q}\otimes_{\mathbf{Z}}N$*).*

On note $\mathscr{H}$ *un ensemble de sous-groupes de* G *et pour tout* H *de* $\mathscr{H}$ *on note* M^H *(resp.* N^H*) l'ensemble des éléments de* M *(resp.* N*) invariants par l'action de* H*.*

On se donne une relation de dépendance $\mathbf{Z}$ *linéaire non triviale*

$$\sum_{H\in\mathscr{H}} a_H 1_H^G = 0. \tag{1}$$

Si M *et* N *sont* $\mathbf{Z}[G]$*-isomorphes alors:*

$$\prod_{H\in\mathscr{H}} [M^H : N^H]^{a_H} = 1.$$

On peut le compléter par la:

Remarque I.1. Si on suppose simplement, sous les hypothèses du théorème, que M et N sont dans le même genre, c'est-à-dire sont $\mathbf{Z}_p[G]$-isomorphes pour tout p premier, alors $\prod_{H\in\mathscr{H}} [M^H : N^H]^{a_H} = 1$.

Démontrons alors la

Propriété I. *Si* K *est réel,* $\mathscr{L}$ *et* $\mathscr{L}^*$ *sont isomorphes si et seulement si* G *est cyclique.*

Démonstration. Si G est cyclique et engendré par σ, $\mathscr{L}^* = \mathbf{Z}[G](\sigma-1)$ et d'après [3], proposition I.3, $\mathscr{L}^*$ est $\mathbf{Z}[G]$-isomorphe à $\mathbf{Z}[G]/\mathbf{Z}\tilde{G}$. Supposons alors G non cyclique, nous allons exhiber une relation du type (1) pour laquelle

$$\prod_H [\mathscr{L}^{*H} : (\mathbf{Z}[G]/\mathbf{Z}\tilde{G})^H]^{a_H} \neq 1$$

on aura prouvé que $\mathscr{L}^*$ et $\mathbf{Z}[G]/\mathbf{Z}\tilde{G}$ sont non-$\mathbf{Z}[G]$-isomorphes et même qu'ils ne sont pas dans le même genre. Pour un tel G ou bien il existe p tel que les p-groupes de Sylow soient non cycliques, ou bien pour tout p les p-groupes de Sylow de G sont cycliques. Ces derniers groupes sont décrits dans [2], p. 111. Ils sont engendrés par deux éléments a, b avec les relations $a^m = b^n = 1$, $b^{-1}ab = a^s$ où m, n, s sont les entiers naturels plus grands que 1 vérifiant $(s-1)n$ et m sont premiers entre eux.

Premier cas: tous les p-groupes de Sylow sont cycliques. Un calcul facile utilisant les formules données dans [1] montre que

$$1_G^G = \frac{1}{m}\sum_{i=0}^{m-1} 1_{g_i}^G + \frac{1}{n}1_H^G - \frac{1}{n}1_1^G$$

où les g_i, $i = 0, \ldots, m-1$ sont les sous-groupes conjugués de $g_0 = \langle b\rangle$ et où H désigne le sous-groupe dérivé de G.

La relation s'écrit alors:

$$mn1_G^G - n\sum_{i=0}^{m-1} 1_{g_i}^G - m1_H^G + m1_1^G = 0. \tag{1'}$$

Deuxième cas: G admet un p-sous-groupe de Sylow non cyclique S. S étant non cyclique, il existe T distingué dans S tel que $S/T \simeq \mathbf{Z}/p\mathbf{Z}\times\ \times\mathbf{Z}/p\mathbf{Z}$. Ecrivons la relation de Brauer de dépendance des caractères de S/T. On obtient, en notant H_i, $i = 1, \ldots, p+1$ les sous-groupes d'ordre p de S/T:

$$1_{S/T}^{S/T} = \frac{1}{p}\sum_{i=1}^{p+1} 1_{H_i}^{S/T} - \frac{1}{p}1_1^{S/T}$$

et on a la relation de dépendance $\mathbf{Z}$-linéaire

$$p1_{S/T}^{S/T} - \sum_{i=1}^{p+1} 1_{H_i}^{S/T} + 1_1^{S/T} = 0.$$

Comme l'a indiqué C. D. Walter dans [5] démonstration du théorème 4.1, cette relation implique la relation suivante obtenue en prenant les images réciproques par la projection canonique de S sur S/T des sous-groupes de S/T qui interviennent:

$$p1_S^S - \sum_{i=1}^{p+1} 1_{H_i'}^S + 1_T^S = 0$$

où les H_i' sont les images réciproques des H_i. En prenant les caractères induits à G tout entier on a enfin

$$p1_S^G - \sum_{i=1}^{p+1} 1_{H_i'}^G + 1_T^G = 0. \tag{1''}$$

Remarquons alors que les formules de nombres de classes de Brauer [1] et Walter [5] associées à la formule de dépendance $\mathbf{Z}$-linéaire $\sum_{H\in\mathscr{H}} a_H 1_H^G = 0$ entraînent:

$$\prod_H [\mathscr{L}^{*H} : \mathscr{L}^H]^{a_H} = \prod_H \left(\frac{\delta(H)}{[G:H]}\right)^{a_H}$$

dans le cas envisagé ici $\mathscr{L} = \mathbf{Z}[G]/\mathbf{Z}\tilde{G}$, $\delta(H) = 1$, pour tout H, d'autre part $\sum_{H\in\mathscr{H}} a_H = 0$ entraîne

$$\prod_{H\in\mathscr{H}} \frac{1}{|G|^{a_H}} = 1$$

d'où

$$\prod_{H\in\mathscr{H}}[\mathscr{L}^{*H}:\mathscr{L}^{H}]=\prod_{H\in\mathscr{H}}|H|^{a_H}.$$

Dans le premier cas, la relation (1') donne $\prod_{H\in\mathscr{H}}[\mathscr{L}^{*H}:\mathscr{L}^{H}]=m^{m(n-1)}$ qui diffère de 1. Dans le deuxième cas, la relation (1'') donne

$$\prod_{H\in\mathscr{H}}[\mathscr{L}^{*H}:\mathscr{L}^{H}]^{a_H}=p^{p-1}\neq 1.$$

Le cas imaginaire est plus compliqué. Nous nous bornerons à la remarque suivante où $\mathscr{I}_G$ (resp. $\mathscr{I}_H$) désigne l'idéal d'augmentation de G (resp. H).

Remarque I.2. Si $G=CH$ avec H distingué, alors $\mathscr{L}^*=\mathscr{I}_G\tilde{C}=\mathscr{I}_H\tilde{C}$ et $\mathscr{L}^*$ est monogène si et seulement si $\mathscr{I}_H\tilde{C}$ est $\boldsymbol{Z}[G]$-monogène. Si $\mathscr{I}_H$ est $\boldsymbol{Z}[H]$-monogène, ce qui équivaut, on vient de le voir, à H cyclique, alors $\mathscr{L}^*$ est $\boldsymbol{Z}[G]$-monogène. Mais $\mathscr{I}_H\tilde{C}$ peut être $\boldsymbol{Z}[G]$-monogène sans que $\mathscr{I}_H$ soit $\boldsymbol{Z}[H]$-monogène. On le voit sur le groupe G produit semi-direct de H par C où H est défini par les générateurs σ et τ et les relations $\sigma^p=\tau^p=1$, $\sigma\tau=\tau\sigma$ et l'opération de γ sur H étant définie par $\gamma\sigma\gamma^{-1}=\tau$. $\mathscr{I}_H\tilde{C}$ est engendré par $(\sigma-1)\tilde{C}$ et $(\tau-1)\tilde{C}$, mais $\gamma(\sigma-1)\tilde{C}=(\tau-1)\tilde{C}$ donc $\mathscr{I}_H\tilde{C}$ admet comme $\boldsymbol{Z}[G]$-générateur $(\sigma-1)\tilde{C}$.

II. Unités de Minkowski de norme 1 sur le sous-corps réel maximal. Dans le cas imaginaire, la deuxième question posée au début de ce travail se traduit par:

G admettant un sous-groupe C d'ordre 2, existe-t-il un idéal à gauche $\mathfrak{a}$ de $\boldsymbol{Z}[G]$ contenant $\tilde{C}$ tel que $\boldsymbol{Z}[G]/\mathfrak{a}$ ait pour caractère $1_C^G-1_G^G$?

Propriété II. *Pour qu'il existe $\mathfrak{a}$ idéal à gauche de $\boldsymbol{Z}[G]$ avec $\tilde{C}\in\mathfrak{a}$ et $\boldsymbol{Z}[G]/\mathfrak{a}$ a pour caractère $1_C^G-1_G^G$, il faut et il suffit que $G=CH$ avec H abélien distingué d'ordre impair sur lequel γ opère par $\gamma\sigma\gamma=\sigma^{-1}$ pour tout σ de H.*

Démonstration. Supposons que $\mathfrak{a}$ existe avec les propriétés $\tilde{C}\in\mathfrak{a}$ et $\boldsymbol{Z}[G]/\mathfrak{a}$ de caractère $1_C^G-1_G^G$. De $\boldsymbol{Q}[G]=\boldsymbol{Q}[G](1+\gamma)+\boldsymbol{Q}[G](1-\gamma)$ résulte $\boldsymbol{Q}[G]\tilde{C}\subset\boldsymbol{Q}\otimes_{\boldsymbol{Z}}\mathfrak{a}$. On pose $|G|=2m$, l'assertion sur le caractère de $\boldsymbol{Z}[G]/\mathfrak{a}$ montre que $\dim_{\boldsymbol{Q}}\boldsymbol{Q}\otimes_{\boldsymbol{Z}}\mathfrak{a}=m+1$. Comme $\boldsymbol{Q}[G]$ est semi-simple, on en déduit que le caractère de $\mathfrak{a}$ est égal à la somme du caractère de $\boldsymbol{Q}[G]\tilde{C}$, c'est-à-dire 1_G^G, et d'un caractère de degré 1 qu'on note η. $\boldsymbol{Z}[G]/\mathfrak{a}$ a donc comme caractère le caractère de $\boldsymbol{Z}[G]$ moins celui de $\mathfrak{a}$ soit: $1_1^G-1_C^G-\eta$ d'où la condition nécessaire:

$$1_1^G=2(1_C^G-1_G^G)+\eta+1_G^G$$

au premier membre figure le caractère de la représentation régulière et au second une somme de „vrais" caractères. Le caractère de la représentation régulière s'écrit classiquement $\sum d_i\psi_i$ où les ψ_i sont les caractères absolument irréductibles de G et d_i le degré de ψ_i. $1_C^G-1_G^G$ étant le caractère d'une représentation est somme à coefficients entiers positifs ou nuls des ψ_i, soit $1_C^G-1_G^G=\sum\lambda_i\psi_i$. L'unicité de la décomposition en somme de caractères absolument irréductibles entraîne que G admet deux caractères absolument irréductibles de degré 1 et que les autres sont de degré pair. Le groupe G' dérivé de G est donc d'indice 2 et en égalant les degrés des deux membres on obtient:

$$2m=1+1+\sum d_{i'}^2,$$

les $d_{i'}$ étant pairs, m est nécessairement impair, c'est l'ordre de G'.

Soit alors $x\in G-G'$, η étant non trivial, $\eta(x)=-1$, d'autre part $1_G^G(x)=1$ et $1_1^G(x)=0$ l'égalité entre caractères entraîne $1_C^G(x)=1$. Revenons à la définition de 1_C^G, soit h_i un système complet de représentants des classes à gauche de G/C, on sait (c'est la définition d'un caractère induit) que

$$1_C^G(x)=\sum_{h_i^{-1}xh_i\in C}1_C^C(h_i^{-1}xh_i),$$

il existe donc un h_i et un seul tel que $h_i^{-1}xh_i\in C$, en outre $h_i^{-1}xh_i\neq 1$ sinon x serait l'élément unité. Pour ce h_i on a donc $h_i^{-1}xh_i=\gamma$. Cela signifie que γ et les éléments de $G-G'$ sont dans la même classe de conjugaison de G, le cardinal de celle-ci est donc au moins égal à m, comme c'est un diviseur strict de $|G|$ on en déduit que $G-G'$ est une classe de conjugaison contenant γ. Il en résulte $G=CG'$. Un élément de $G-G'$ s'écrit γh avec h dans G', étant conjugué de γ, il est d'ordre 2 d'où $\gamma h\gamma=h^{-1}$. Comme $h\to\gamma h\gamma$ est un automorphisme de G', ce groupe est nécessairement abélien.

Supposons réciproquement $G=CH$ avec H abélien d'ordre impair et $\gamma\sigma\gamma=\sigma^{-1}$ pour tout σ de H. On voit que $\mathfrak{a}=\boldsymbol{Z}[G]\tilde{C}+\boldsymbol{Z}[G]\tilde{H}$ est un idéal à gauche de $\boldsymbol{Z}[G]$ de caractère $1_G^G+\eta$ où η est le caractère de degré 1 autre que 1_G^G. Notons encore η le caractère irréductible de degré 1 non trivial sur $G-H$. Vérifions l'égalité $1_1^G=2(1_C^G-1_G^G)+\eta+1_G^G$, on compare les valeurs des deux membres:

si $x=e$,	$1_1^G(e)=2m$,	$1_C^G(e)=m$,	$1_G^G(e)=\eta(e)=1$,
si $x\in G'-e$,	$1_1^G(x)=0$,	$1_C^G(x)=0$,	$1_G^G(x)=1=\eta(x)$,
si $x\in G-G'$,	$1_1^G(x)=0$,	$1_C^G(x)=1$,	$1_G^G(x)=1$ et $\eta(x)=-1$.

Pour tout x dans G les deux membres sont égaux, il y a donc bien égalité des caractères. Le caractère de $\boldsymbol{Z}[G]/\mathfrak{a}$ étant $1_1^G-1_C^G-\eta$ l'égalité précédente montre que $\boldsymbol{Z}[G]/\mathfrak{a}$ a pour caractère $1_C^G-1_G^G$ d'où la propriété.

Je tiens à remercier J. M. Fontaine pour les fructueuses conversations que nous avons eues sur ce sujet.

Bibliographie

[1] R. Brauer, *Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers*, Math. Nachr. 4 (1951), p. 158–174.

[2] W. Feit, *Characters of finite groups*, Benjamin, Inc., New–York, Amsterdam 1967.

[3] N. Moser, *Unités et nombre de classes d'une extension galoisienne diédrale de* Q, Sém. Th. des Nombres, Univ. de Grenoble 1974, et Math. Sem. der Univ. Hamburg 48 (1979), p. 54–75.

[4] J. J. Payan, *Sur le théorème des indices de Brauer–Walter*, Sém. Th. des Nombres, Univ. de Grenoble 1975–1977.

[5] C. D. Walter, *Brauer's class number relation*, Acta Arith. 35 (1979), p. 33–40.

LABORATOIRE DE MATHÉMATIQUES PURES-INSTITUT FOURIER
UNIVERSITÉ SCIENTIFIQUE ET MÉDICALE DE GRENOBLE
38402 St. Martin d'Hères, France

Reçu le 8. 6. 1978 (1079)

ACTA ARITHMETICA
XXXIX (1981)

Limit theorems for uniformly distributed p-adic sequences*

by

JEFFREY D. VAALER (Austin, Tex.)

1. Introduction. Let Q_p and $\mathbf{Z}_p$ denote the locally compact field of p-adic numbers and the compact ring of p-adic integers respectively, where p is a fixed prime. We suppose that μ is Haar measure on Q_p normalized so that $\mu(\mathbf{Z}_p) = 1$ and that $|\ |_p$ is the p-adic absolute value normalized so that $|p|_p = p^{-1}$. For $J = 1, 2, 3, \ldots$ and $j = 0, 1, 2, \ldots, p^J - 1$ we define

$$\varphi(j, J, y) = \begin{cases} 1 & \text{if} \quad |y - j|_p \leqslant p^{-J}, \\ 0 & \text{if} \quad |y - j|_p > p^{-J}. \end{cases}$$

Thus $\varphi(j, J, y)$ is the characteristic function of the sphere $S_j^{(J)}$ centered at j and having radius p^{-J}. A sequence $\{x_n\}$, $n = 1, 2, 3, \ldots$, of p-adic integers is said to be *uniformly distributed* in $\mathbf{Z}_p$ if

$$\lim_{N \to \infty} N^{-1} \sum_{n=1}^{N} \varphi(j, J, x_n) = p^{-J}$$

for each J and j. We define the *p-adic discrepancy* of $\{x_n\}$, $n = 1, 2, \ldots, N$, by

$$\Delta_N = \sup \left| \sum_{n=1}^{N} \varphi(j, J, x_n) - N p^{-J} \right|$$

where the supremum is taken over all $J \geqslant 1$ and j, $0 \leqslant j \leqslant p^J - 1$. It is well known (see [3] or [4]) that $N^{-1}\Delta_N \to 0$ as $N \to \infty$ if and only if the sequence $\{x_n\}$ is uniformly distributed.

Let $\omega \in Q_p$ and let

$$\omega = \sum_{m=l}^{\infty} a_m p^m = \sum_{m=l}^{-1} a_m p^m + \sum_{m=0}^{\infty} a_m p^m$$

* This research was supported in part by the National Science Foundation, grant MCS77-01830.