ANNALES SCIENTIFIQUES DE L'É.N.S.

JEAN-MARC FONTAINE

Sur la décomposition des algèbres de groupes

Annales scientifiques de l'É.N.S. 4^e série, tome 4, n° 1 (1971), p. 121-180
<http://www.numdam.org/item?id=ASENS_1971_4_4_1_121_0>

Ann. scient. Éc. Norm. Sup.,
4e série, t. 4, 1971, p. 121 à 180.

SUR LA DÉCOMPOSITION DES ALGÈBRES DE GROUPES

PAR JEAN-MARC FONTAINE.

Introduction.

Soit p un nombre premier. Un groupe fini est dit *de type* R_p si c'est le produit semi-direct d'un sous-groupe cyclique d'ordre premier à p par un p-sous-groupe invariant. Les groupes de type R_p interviennent dans l'étude des extensions des corps locaux (si L est une extension finie galoisienne totalement ramifiée d'un corps local K, le groupe de Galois de l'extension est de type R_p, p étant la caractéristique du corps résiduel de K).

Le but de ce travail était primitivement l'étude de la décomposition des algèbres de groupes de type R_p. Witt a étudié dans [13] la décomposition des algèbres de groupes finis quelconques, mais par des techniques qui ne semblent pas très appropriées au cas particulier des groupes de type R_p. On a donc été conduit à développer d'autres méthodes. Il s'est avéré qu'elles pouvaient s'appliquer à des groupes beaucoup plus généraux que les groupes de type R_p (en particulier, aux groupes résolubles). C'est ce que l'on expose dans cet article.

Soit G un groupe fini et soit E un corps de caractéristique o. L'algèbre E[G] est semi-simple. Soit A un facteur simple de l'algèbre E[G]. L'algèbre A est une algèbre simple d'un type particulier, nommé « Kreisalgebra » par Witt (*loc. cit.*). L'ensemble des classes de « Kreisalgebren », de centre un corps donné E, forme un sous-groupe du groupe de Brauer de E, que nous appelons *le groupe de Brauer cyclotomique de* E. Le paragraphe 1 est une étude détaillée du groupe de Brauer cyclotomique de E, lorsque E est une extension finie de $\mathbf{Q}_p$.

Le paragraphe 2 rappelle un certain nombre de résultats sur les algèbres semi-simples et sur les caractères des groupes finis. Le paragraphe 3 déter-

mine la structure de l'algèbre simple centrale correspondant à un caractère absolument irréductible d'un groupe G fini, induit par un caractère d'un sous-groupe invariant de G.

Le paragraphe 4 applique les méthodes du paragraphe 3 aux groupes nilpotents. Le paragraphe 5 expose la structure des représentations des groupes résolubles. Les paragraphes 6 et 7 sont consacrés à l'étude des algèbres des groupes de type R_p : le paragraphe 6 se limite au cas de certains groupes de structure particulièrement simple, les groupes de type C_p, et le paragraphe 7 montre comment on peut se ramener à ce cas. Dans le paragraphe 8, enfin, on rappelle le résultat principal de l'article indiqué de Witt et on en donne quelques applications immédiates.

Dans un prochain article, on montrera comment les résultats des paragraphes 6 et 7 permettent de résoudre le problème de la rationalité des représentations d'Artin des extensions galoisiennes finies des corps locaux.

Définitions et notations.

Dans le paragraphe 1, on utilise abondamment certaines des méthodes exposées par Serre dans son livre sur les corps locaux ([9], cité CL).

On appelle *corps local* un corps muni d'une valuation discrète pour laquelle il est complet. Si K est un corps local, on appelle *valuation normalisée* de K la valuation v de K telle que $v(K^*) = \mathbf{Z}$.

Soit L une extension finie d'un corps local K. Si v' désigne la valuation normalisée de L, on note $e_{L/K}$ l'indice du groupe $v'(K^*)$ dans $\mathbf{Z}$.

On dit que l'extension L/K est :

— *non ramifiée* si $e_{L/K} = 1$ et si l'extension résiduelle est séparable;

— *totalement ramifiée* si le corps résiduel de L est le même que celui de K;

— *modérément ramifiée* si $e_{L/K}$ est premier à la caractéristique du corps résiduel et si l'extension résiduelle est séparable.

Soit L^{nr} l'extension maximale non ramifiée de K contenue dans L. Si l'extension L/K est galoisienne on appelle *groupe d'inertie* de l'extension le groupe de Galois de l'extension L/L^{nr}.

Dans tout cet article, les seuls corps locaux envisagés seront les extensions finies de $\mathbf{Q}_p$ de sorte que les extensions résiduelles seront toujours séparables.

Enfin, les notations et les définitions de cohomologie utilisées sont usuelles; en particulier, celles des homomorphismes Inf, Res et Cor (*cf.* CL, p. 124 et 127).

1. Le groupe de Brauer cyclotomique.

1.1. Définition. Premières propriétés. — Soit k un corps. Soit K une extension galoisienne de k et soit G le groupe de Galois de l'extension K/k. Le groupe multiplicatif K^* de K est un G-module. Comme il est d'usage, on écrit $H^q(K/k)$ au lieu de $H^q(G, K^*)$.

Soit k_s une clôture séparable de k. On note $Br(k) = H^2(k_s/k)$ le groupe de Brauer de k. C'est la limite inductive, pour K parcourant l'ensemble des extensions finies galoisiennes de k contenues dans k_s, de $H^2(K/k)$.

Pour tout corps k, on note $\mu(k)$ le groupe des racines de l'unité contenues dans k. Si K est une extension galoisienne de k et si G est le groupe de Galois de l'extension, il est clair que $\mu(K)$ est un sous-G-module de K^*. Pour tout entier positif q, on écrit $H^q(K/k, \mu)$ au lieu de $H^q(G, \mu(K))$. On a un homomorphisme canonique de $H^q(K/k, \mu)$ dans $H^q(K/k)$. Nous notons $H^q_\mu(K/k)$ l'image de $H^q(K/k, \mu)$ par cet homomorphisme.

Soit L une extension galoisienne de k contenant K. Il est clair que l'image par inflation de $H^q_\mu(K/k)$ est contenue dans $H^q_\mu(L/k)$. Soient K_1 et K_2 deux extensions finies cyclotomiques de k. Soit K′ le corps engendré sur k par K_1 et K_2. L'extension K'/k est encore cyclotomique. On peut donc parler de la limite inductive de $H^2_\mu(K/k)$ pour K parcourant l'ensemble des extensions finies cyclotomiques de k contenues dans k_s. C'est un sous-groupe de $Br(k)$ que nous notons $Br_\mu(k)$ et que nous appelons *le groupe de Brauer cyclotomique de k*. Si k_c désigne l'extension cyclotomique maximale de k contenue dans k_s, on voit que $Br_\mu(k) = H^2_\mu(k_c/k)$.

Soit K un corps et soit $\bar{\varepsilon}$ un élément de $Br_\mu(K)$. Il est clair que l'on peut choisir une extension L de K et une racine de l'unité ν contenue dans L telles que les conditions suivantes soient satisfaites :

(i) on a $L = K(\nu)$;

(ii) l'élément $\bar{\varepsilon}$ appartient à $H^2_\mu(L/K)$ et admet un représentant ε à valeurs dans le groupe cyclique engendré par ν.

Soit k le sous-corps premier de K, soit $k' = k(\nu)$ et soit $k_1 = k' \cap K$. L'élément $\bar{\varepsilon}$ de $Br_\mu(K)$ est la restriction d'un élément de $H^2_\mu(k'/k_1)$ qui est contenu dans $Br_\mu(k_1)$. On peut donc, en un certain sens, se contenter d'étudier $Br_\mu(K)$ lorsque K est une extension finie cyclotomique d'un corps premier.

En particulier, si la caractéristique de K est différente de zéro, toute extension finie de son corps premier est un corps fini k_1. On a donc $Br_\mu(k_1) = 1$, puisque $Br(k_1) = 1$. Par conséquent, $Br_\mu(K) = 1$. On a établi le résultat suivant :

PROPOSITION 1.1. — *Pour tout corps* K *de caractéristique non nulle*, $\mathrm{Br}_\mu(K) = 1$.

Si K est de caractéristique nulle, toute extension finie de son sous-corps premier est un corps de nombres. Si K est un corps de nombres, la connaissance d'un élément de Br(K) est équivalente à la connaissance de la restriction de cet élément à chacun des complétés $K_\mathfrak{p}$ de K. La restriction à $K_\mathfrak{p}$ de $\mathrm{Br}_\mu(K)$ est évidemment contenue dans $\mathrm{Br}_\mu(K_\mathfrak{p})$.

Si $K_\mathfrak{p} \simeq \mathbf{C}$, on a, trivialement : $\mathrm{Br}_\mu(\mathbf{C}) = \mathrm{Br}(\mathbf{C}) = 1$.

Si $K_\mathfrak{p} \simeq \mathbf{R}$, $\mathrm{Br}(\mathbf{R})$ est un groupe cyclique d'ordre 2 et on vérifie immédiatement que $\mathrm{Br}_\mu(\mathbf{R}) = \mathrm{Br}(\mathbf{R})$.

Dans les autres cas, $K_\mathfrak{p}$ est un corps local de caractéristique nulle, à corps résiduel fini. Il est donc isomorphe à une extension finie de $\mathbf{Q}_p$. Le reste du paragraphe 1 est consacré à l'étude de $\mathrm{Br}_\mu(K)$ lorsque K est une extension finie de $\mathbf{Q}_p$.

1.2. ÉTUDE DU GROUPE $H^2_\mu(L/K)$. — Dans toute la suite du paragraphe 1, sauf mention explicite du contraire, on désigne par p un nombre premier, par K un corps de caractéristique nulle et par $\overline{K}$ une clôture algébrique de K. Pour tout entier m strictement positif, K_m désigne le sous-corps de $\overline{K}$ engendré sur K par les racines $m^{\text{ièmes}}$ de l'unité. On note K'_∞ la limite inductive des K_m, pour m premier à p (la relation d'ordre sur les entiers m étant évidemment la divisibilité), et K''_∞ la limite inductive des K_m, pour m puissance de p.

Soit L une extension finie galoisienne de K contenue dans $\overline{K}$. Pour tout entier m strictement positif, on pose $L^{(m)} = L \cap K_m$, $L' = L \cap K'_\infty$, $L'' = L \cap K''_\infty$. On désigne par $\mu'(L)$ [resp. $\mu''(L)$] le groupe des racines de l'unité d'ordre premier à p (resp. d'ordre une puissance de p) contenues dans L. Si G désigne le groupe de Galois de l'extension L/K, $\mu(L)$ est le produit direct des G-modules $\mu'(L)$ et $\mu''(L)$. On écrit $H^q(L/K, \mu')$ au lieu de $H^q(G, \mu'(L))$ et $H^q(L/K, \mu'')$ au lieu de $H^q(G, \mu''(L))$.

On désigne par $H^q_{\mu'}(L/K)$ [resp. $H^q_{\mu''}(L/K)$] l'image canonique de $H^q(L/K, \mu')$ [resp. $H^q(L/K, \mu'')$] dans $H^q(L/K)$. On voit que les groupes $H^q_{\mu'}(L/K)$ et $H^q_{\mu''}(L/K)$ sont d'ordres premiers entre eux et on en déduit que $H^q_\mu(L/K)$ est égal à leur produit direct.

Si K est un corps local, on désigne par L^{nr} (resp. L^{mr}) l'extension maximale non ramifiée (resp. modérément ramifiée) de K contenue dans L. Si K est une extension finie de $\mathbf{Q}_p$, il est clair que $L^{nr} = L'$ et que, si l'extension L/K est cyclotomique, $L^{mr} = L \cap (K'_\infty)_p$.

THÉORÈME 1. — *Soit* K *une extension finie de* $\mathbf{Q}_p$ *et soit* L *une extension finie cyclotomique de* K (*si* $p = 2$, *on suppose de plus que* K *contient les racines quatrièmes de l'unité*). *Alors*

$$H^2_\mu(L/K) = H^2_\mu(L^{(p)}/K).$$

Nous allons décomposer la démonstration de ce théorème en cinq parties.

1.2.1. *Le groupe* $H^2_\mu(L/K)$ *d'une extension cyclique.*

Soit K un corps quelconque et soit L une extension galoisienne de K. Soit G le groupe de Galois de l'extension L/K. Soit χ un caractère de degré 1 de G à valeurs dans $\mathbf{Q}/\mathbf{Z}$. C'est un élément de $H^1(G, \mathbf{Q}/\mathbf{Z})$. Soit δ le cobord de la suite exacte

$$0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0.$$

L'élément $\delta\chi$ est dans $H^2(G, \mathbf{Z})$. Si b est un élément non nul de K, c'est-à-dire un élément de $H^0(L/K)$, le cup-produit $b.\delta\chi$ est un élément de $H^2(L/K)$ qu'il est d'usage de désigner par le symbole (χ, b). On sait (*cf.* CL, prop. 1, p. 211) que $(\chi, b)(\chi, b') = (\chi, bb')$.

Supposons l'extension L/K cyclique. Soit d son degré et soit s un générateur de G. Soit φ_s le caractère de G défini par $\varphi_s(s) = 1/d$. On sait (*cf.* CL, cor. 1 et 2 à la prop. 2, p. 211) que tout élément de $H^2(L/K)$ est de la forme $\bar{\varepsilon} = (\varphi_s, b)$, avec $b \in K^*$, et qu'un élément de cette forme est égal à 1 si et seulement si b est une norme dans l'extension L/K. Il est immédiat que, si $\bar{\varepsilon} = (\varphi_s, b)$, le cocycle ε défini par

$$\varepsilon_{s^k, s^{k'}} = \begin{cases} 1 & \text{si } k + k' < d \\ b & \text{si } k + k' \geq d \end{cases} \qquad \text{pour} \quad 0 \leq k, k' \leq d - 1,$$

est un représentant de $\bar{\varepsilon}$. Il est alors clair que $\bar{\varepsilon}$ est un élément de $H^2_\mu(L/K)$ si et seulement si il existe une racine de l'unité ν dans K telle que $(\varphi_s, b) = (\varphi_s, \nu)$. Ceci revient à dire que b est le produit d'une racine de l'unité contenue dans K par la norme de L à K d'un élément de L.

Supposons maintenant que K est une extension finie de $\mathbf{Q}_p$. Soit $s_b = (b, L/K)$ l'élément de G défini par l'application de réciprocité. L'invariant de $\bar{\varepsilon} = (\varphi_s, b)$ est (*cf.* CL, prop. 3, p. 212) :

$$\text{inv}(\bar{\varepsilon}) = \varphi_s(s_b). \tag{1}$$

PROPOSITION 1.2. — *Soit* K *une extension finie de* $\mathbf{Q}_p$ *et soit* L *une extension finie non ramifiée de* K. *Alors* $H^2_\mu(L/K) = 1$.

Démonstration. — Tout élément de $H^2_\mu(L/K)$ est de la forme (φ_s, ν) où ν est un élément de $\mu(K)$, donc une unité de K, et on sait que dans une extension non ramifiée toute unité est norme (*cf.* CL, cor. à la prop. 3, p. 90).

C. Q. F. D.

1.2.2. *Un lemme.*

Lemme 1. — *Soit* G *un groupe et soit* A *un* G*-module fini. Soit* H *un sous-groupe invariant de* G. *Supposons* H *fini et cyclique. Posons* $N = \sum_{h \in H} h$. *Alors, si* $NA = A^H$, *pour tout entier* q *strictement positif, on a*

$$H^q(G, A) = H^q(G/H, A^H).$$

Démonstration. — Comme H est un groupe cyclique fini, $H^q(H, A)$ ne dépend que de la parité de q et $H^q(H, A) = A^H/NA$ si q est pair (*cf.* CL, cor. à la prop. 6, p. 141). Comme A est fini, $H^q(H, A)$ et $H^{q+1}(H, A)$ ont le même nombre d'éléments (*cf.* CL, prop. 8, p. 142). Si $NA = A^H$, on a donc $H^q(H, A) = 0$, pour tout entier q strictement positif.

Or, on sait (*cf.* CL, prop. 5, p. 126) que si $H^i(H, A) = 0$, pour $1 \leq i \leq q-1$, la suite

$$0 \to H^q(G/H, A^H) \xrightarrow{\text{Inf}} H^q(G, A) \xrightarrow{\text{Res}} H^q(H, A)$$

est exacte. Comme $H^q(H, A) = 0$, on en déduit que l'homomorphisme d'inflation est un isomorphisme de $H^q(G/H, A^H)$ sur $H^q(G, A)$ et on peut identifier ces deux groupes. C. Q. F. D.

1.2.3. *Le groupe* $H^2(L/K, \mu')$.

Lemme 2. — *Soit* K *une extension finie de* $\mathbf{Q}_p$ *et soit* L *une extension finie non ramifiée de* K. *Soit* H *le groupe de Galois de l'extension. Alors*

$$\mu'(K) = (\mu'(L))^H = N_{L/K}(\mu'(L)).$$

Démonstration. — L'ensemble $\mu'(L) \cup \{0\}$ (resp. $\mu'(K) \cup \{0\}$) n'est autre que le système de représentants multiplicatifs du corps résiduel $\tilde{L}$ de L (resp. $\tilde{K}$ de K) dans L (resp. K) et l'assertion résulte de la surjectivité bien connue de la norme dans une extension finie d'un corps fini.

C. Q. F. D.

Proposition 1.3. — *Soit* K *une extension finie de* $\mathbf{Q}_p$ *et soit* L *une extension finie cyclotomique de* K. *Alors*

$$H^2(L/K, \mu') = H^2(L^{(p)}/K, \mu').$$

Démonstration. — Comme l'extension L/K est cyclotomique, il existe un entier n tel que L est contenu dans $K(\sqrt[n]{1})$. Si $n = n_0 p^r$, avec $(n_0, p) = 1$, le corps L est contenu dans $L''(\sqrt[n]{1})$ et l'extension L/L'' est non ramifiée, donc cyclique. Soit H le groupe de Galois de l'extension L/L''. D'après le lemme 2, $N_{L/L''}(\mu'(L)) = (\mu'(L))^H$. Donc, d'après le lemme 1,

$$H^2(L/K, \mu') = H^2(L''/K, \mu').$$

L'extension $L''/L^{(p)}$ est une p-extension totalement ramifiée et $\mu'(L'') = \mu'(L^{(p)})$.

— Si $p \neq 2$, l'extension $L''/L^{(p)}$ est cyclique. Soit p^a son degré. On a

$$N_{L''/L^{(p)}}(\mu'(L'')) = (\mu'(L^{(p)}))^{p^a} = \mu'(L^{(p)}).$$

Donc, d'après le lemme 1, $H^2(L''/K, \mu') = H^2(L^{(p)}/K, \mu')$.

— Si $p = 2$, l'extension $L''/L^{(2)}$ peut se décomposer en une suite de deux extensions cycliques. Pour chacune d'elles, on peut faire le même raisonnement.

C. Q. F. D.

1.2.4. *Le groupe* $H^2(L/K, \mu'')$.

Lemme 3. — *Soit* L *une extension finie galoisienne de* K. *Supposons que* $L = L''$ *et que* $K = L^{(p)}$. *Si* $p = 2$, *supposons de plus que* $\sqrt{-1} \in K$. *Soit* H *le groupe de Galois de l'extension. Alors*

$$\mu''(K) = (\mu''(L))^H = N_{L/K}(\mu''(L)).$$

Démonstration. — Si K ne contient pas les racines $p^{\text{ièmes}}$ de l'unité, on a $\mu''(K) = \{1\}$, et l'assertion est triviale.

Si K contient les racines $p^{\text{ièmes}}$ de l'unité, désignons par a le plus grand entier tel que $L^{(p^a)} = K$ et par b le plus petit entier tel que $L^{(p^b)} = L$. On a $a \geqq 1$, et, par hypothèse, si $p = 2$, $a \geqq 2$. Le groupe $\mu''(K)$ [resp. $\mu''(L)$] est le groupe des racines $(p^a)^{\text{ièmes}}$ de l'unité [resp. $(p^b)^{\text{ièmes}}$ de l'unité] et l'extension L/K est cyclique de degré p^{b-a}. Si ν désigne une racine primitive $(p^b)^{\text{ième}}$ de l'unité, on vérifie immédiatement que l'application $\nu \mapsto \nu^c$, avec $c = 1 + p^a$, définit un générateur du groupe de Galois de l'extension L/K.

On a donc $N_{L/K}(\nu) = \nu^d$, avec

$$d = 1 + c + \ldots + c^{p^{b-a}-1} = (c^{p^{b-a}} - 1)/(c-1) = ((1+p^a)^{p^{b-a}} - 1)/p^a$$
$$= \sum_{j=1}^{p^{b-a}} \binom{p^{b-a}}{j} \cdot p^{(j-1)a} \equiv p^{b-a} \pmod{p^{b-a+1}}.$$

Comme $p^{b-(b-a)} = p^a$, on voit que $N_{L/K}(\nu)$ est une racine primitive $(p^a)^{\text{ième}}$ de l'unité et engendre le groupe $\mu''(K)$. C. Q. F. D.

PROPOSITION 1.4. — *Soit* L *une extension finie cyclotomique de* K. *Alors :*

(i) *si* $p \neq 2$, *ou si* $p = 2$ *et* $\sqrt{-1} \in K$, *on a*

$$H^2(L/K, \mu'') = H^2(L'/K, \mu'');$$

(ii) *si* $p = 2$ *et si* $\sqrt{-1} \in L$, *on a*

$$H^2(L/K, \mu'') = H^2(L'(\sqrt{-1})/K, \mu'').$$

Démonstration. — Posons $M = L \cap K'(\sqrt[p]{1})$. Dans le cas (i), il est clair que l'extension L/M est cyclique et vérifie les hypothèses du lemme 3. Si H désigne le groupe de Galois de l'extension L/M, on a donc

$$(\mu''(L))^H = N_{L/M}(\mu''(L)).$$

Par conséquent, d'après le lemme 1, on a $H^2(L/K, \mu'') = H^2(M/K, \mu'')$.

Si $M = L'$, le résultat est établi. Sinon, on a $\mu''(L') = \{1\}$. L'extension M/L' est cyclique et, si J désigne son groupe de Galois, on a

$$\{1\} = (\mu''(M))^J = N_{M/L'}(\mu''(M)).$$

D'après le lemme 1, on a donc $H^2(M/K, \mu'') = H^2(L'/K, \mu'')$.

Dans le cas (ii), il suffit de remplacer, dans la démonstration qui précède, M par $M(\sqrt{-1})$ et L' par $L'(\sqrt{-1})$. C. Q. F. D.

1.2.5. *Fin de la démonstration du théorème* 1. — Supposons de nouveau que K est une extension finie de $\mathbf{Q}_p$. La proposition 1.4 montre que, dans le cas (i), $H^2_{\mu''}(L/K) = H^2_{\mu''}(L^{nr}/K)$. Comme, d'après la proposition 1.2, $H^2_{\mu}(L^{nr}/K) = 1$, on a, en particulier, $H^2_{\mu''}(L^{nr}/K) = 1$. On a donc établi le résultat suivant :

PROPOSITION 1.5. — *Soit* K *une extension finie de* $\mathbf{Q}_p$ *et soit* L *une extension finie cyclotomique de* K (*si* $p = 2$, *on suppose que* $\sqrt{-1} \in K$). *Alors,* $H^2_{\mu''}(L/K) = 1$.

On a donc $H^2_{\mu}(L/K) = H^2_{\mu'}(L/K)$ et le théorème 1 résulte de la proposition 1.3.

1.3. LE GROUPE DE BRAUER CYCLOTOMIQUE. — Dans tout le n° 1.3, on désigne par K une extension finie de $\mathbf{Q}_p$ et par $\tilde{K}$ son corps résiduel. Le groupe $\mu(\tilde{K})$ s'identifie canoniquement à $\mu'(K)$.

1.3.1. *Le symbole local* $(a, b)_v$. — Soit d un entier positif fixé qui divise l'ordre de $\mu(K)$. Si a et b sont des éléments de K^*, on peut définir le symbole local $(a, b)_v$ de la manière suivante (*cf.* CL, prop. 6, p. 215) :

— on pose $s_b = (b, K(a^{1/d})/K)$;
— si $\alpha = a^{1/d}$, on pose $(a, b)_v = s_b(\alpha)/\alpha$.

On voit que $(a, b)_v$ est une racine $d^{\text{ième}}$ de l'unité qui ne dépend pas du choix de α. On sait d'autre part que (*cf.* CL, prop. 7, p. 215) :

$$(2)\quad \begin{cases} \text{(i)} & (aa', b)_v = (a, b)_v.(a', b)_v; \\ \text{(ii)} & (a, bb')_v = (a, b)_v.(a, b')_v; \\ \text{(iii)} & \text{pour que } (a, b)_v = 1, \text{ il faut et il suffit que } b \text{ soit une norme dans l'extension } K(a^{1/d})/K; \\ \text{(iv)} & (a, b)_v.(b, a)_v = 1. \end{cases}$$

1.3.2. *Le calcul de* $(b, L/K)$ *dans un cas particulier.* — Soit L une extension finie galoisienne modérément ramifiée de K. Soit π une uniformisante de L. Soit G_0 le groupe d'inertie de l'extension, soit e son indice de ramification et soit μ_e le groupe des racines $e^{\text{ièmes}}$ de l'unité. Le groupe μ_e peut être identifié à un sous-groupe de $\mu(\tilde{K})$ donc de $\mu(K)$. Pour tout s dans G_0, désignons par $\theta_0(s)$ l'image de $s(\pi)/\pi$ dans K. Alors, $\theta_0(s)$ est un élément de μ_e indépendant du choix de π et θ_0 est un isomorphisme de G_0 sur le sous-groupe μ_e de $\mu(K)$ (*cf.* CL, cor. 1 à la prop. 7, p. 75).

Proposition 1.6. — *Soit* K *une extension finie de* $\mathbf{Q}_p$ *et soit* q *le nombre d'éléments de son corps résiduel. Soit* L *une extension cyclique de* K *dont le degré* d *divise* $q - 1$. *Soit* e *l'indice de ramification de l'extension. Alors l'image par l'application de réciprocité du groupe* $\mu'(K)$ *est le groupe d'inertie* G_0 *de l'extension. Pour tout* b *dans* $\mu'(K)$, $(b, L/K) = s_b$ *est défini par*

$$\theta_0(s_b) = b^{-(q^{d/e}-1)/d}.$$

Démonstration. — Soit v (resp. v') la valuation normalisée de K (resp. L). Le corps K contient les racines $d^{\text{ièmes}}$ de l'unité. Il existe donc un élément α de L tel que $L = K(\alpha)$ et $\alpha^d = a \in K$. L'ensemble A des éléments a' de K tels que $L = K(a'^{1/d})$ est alors l'ensemble des a' de la forme $a' = c^d a^k$, avec $c \in K^*$ et $(k, d) = 1$. On peut donc choisir a pour que $v(a) \geqq 0$ et pour que, de plus, pour tout a' dans A avec $v(a') \geqq 0$, on ait $v(a') \geqq v(a)$. Supposons ce choix fait, et posons $v(a) = d_0$. On voit que d_0 divise d. Il est immédiat que l'extension $K(a^{1/d_0})/K$ est non ramifiée et que l'extension $K(a^{1/d})/K(a^{1/d_0})$ est totalement et modérément ramifiée. On a donc $d_0 = d/e$. Comme $v'(\alpha) = e.(1/d).v(a) = ed_0/d = 1$, on voit que α est une uniformisante de L.

Soit b une racine de l'unité contenue dans K. L'élément b est une unité et est donc une norme dans l'extension L^{nr}/K. Par conséquent, $(b, L^{nr}/K) = 1$, et il est clair que ceci entraîne que $s_b = (b, L/K)$ appartient à G_0. Comme α est une uniformisante de L, on a alors $\theta_0(s_b) = (a, b)_v$.

D'après (2) (iv), $(a, b)_v = 1/(b, a)_v$. Soit $L_b = K(b^{1/d})$. Si b appartient à $\mu'(K)$, b est une racine $(q-1)^{\text{ième}}$ de l'unité. L'extension L_b/K est donc non ramifiée. Soit F le générateur de Frobenius du groupe de Galois de l'extension L_b/K. On a (*cf.* CL, prop. 13, p. 205) $(a, L_b/K) = F^{v(a)}$. On a donc $(a, L_b/K) = s_a = F^{d_0}$.

Soit β un élément de L' tel que $\beta^d = b$. On a $F(\beta) = \beta^q$; donc

$$(b, a)_v = s_a(\beta)/\beta = \beta^{q^{d/e}-1} = b^{(q^{d/e}-1)/d}.$$

Finalement, on a

$$\theta_0(s_b) = b^{-(q^{d/e}-1)/d}.$$

Pour achever la démonstration de la proposition, il suffit de montrer que si b est une racine primitive $(q-1)^{\text{ième}}$ de l'unité, alors $b^{-(q^{d/e}-1)/d}$ est une racine primitive $e^{\text{ième}}$ de l'unité; ou encore que $(q-1, (q^{d/e}-1)/d) = (q-1)/e$. Or

$$q^{d/e} - 1 = ((q-1)+1)^{d/e} - 1 = \sum_{j=1}^{d/e} \binom{d/e}{j} \cdot (q-1)^j.$$

Par conséquent,

$$(q^{d/e}-1)/d = (d/e) \cdot (q-1)/d + \lambda(q-1) = (q-1)/e + \lambda(q-1),$$

avec $\lambda \in \mathbf{Z}$. On a donc

$$(q-1, (q^{d/e}-1)/d) = (q-1, (q-1)/e + \lambda(q-1)) = (q-1)/e.$$

C. Q. F. D.

1.3.3. *Le groupe* $H^2_\mu(L/K)$.

THÉORÈME 2. — *Soit* K *une extension finie de* $\mathbf{Q}_p$ *et soit* L *une extension finie cyclotomique de* K (*si* $p = 2$, *on suppose de plus que* K *contient les racines quatrièmes de l'unité*). *Soit* $e = e_0 p^r$, *avec* $(e_0, p) = 1$, *l'indice de ramification de l'extension. Alors* $H^2_\mu(L/K)$ *est le sous-groupe de* Br(K) *d'ordre* e_0.

Démonstration. — D'après le théorème 1, on a $H^2_\mu(L/K) = H^2_{\mu'}(L^{(p)}/K)$. L'extension $L^{(p)}/K$ est cyclique et son degré divise $p-1$. Elle satisfait donc les hypothèses de la proposition 1.6, avec e_0 comme indice de ramification. Soit s un générateur du groupe de Galois de l'extension $L^{(p)}/K$. Avec les

notations du n° 1.2.1, on voit que tout élément de $H^2_{\mu'}(L^{(p)}/K)$ est de la forme $\bar{\varepsilon} = (\varphi_s, b)$, avec b racine $(q-1)^{\text{ième}}$ de l'unité. D'après la formule (1) du n° 1.2.1, l'invariant de $\bar{\varepsilon}$ est alors $\varphi_s(s_b)$.

Il est clair que s^{d/e_0} est un générateur du groupe de Galois de $L^{(p)}/(L^{(p)})^{nr}$ et que, par conséquent, $\theta_0(s^{d/e_0}) = \nu$ est une racine primitive $(e_0)^{\text{ième}}$ de l'unité. Si $b^{-(q^{d/e_0}-1)/d} = \nu^k$, on a $\theta_0(s_b) = \theta_0(s^{dk/e_0})$. L'invariant de $\bar{\varepsilon}$ est donc $(dk/e_0).(1/d)$, ou encore

$$\text{inv}(\bar{\varepsilon}) = k/e_0. \tag{3}$$

Il résulte alors de la proposition 1.6 que, lorsque b décrit le groupe des racines $(q-1)^{\text{ièmes}}$ de l'unité, k/e_0 décrit le sous-groupe $\frac{1}{e_0}\mathbf{Z}/\mathbf{Z}$ de $\mathbf{Q}/\mathbf{Z}$.

C. Q. F. D.

Corollaire 1. — *Soit* K *une extension finie de* $\mathbf{Q}_p$ *(si* $p = 2$, *on suppose que* K *contient les racines quatrièmes de l'unité). Soit* E *l'indice de ramification absolu de* K. *Soit* $e = (p-1)/(p-1, E)$. *Alors* $\text{Br}_\mu(K)$ *est le sous-groupe de* $\text{Br}(K)$ *d'ordre* e.

En particulier, pour que $\text{Br}_\mu(K) = 1$, *il faut et il suffit que* $p-1$ *divise* E.

En effet, il résulte du théorème 1 que $\text{Br}_\mu(K) = H^2_\mu(K(\sqrt[p]{1})/K)$. L'extension $K(\sqrt[p]{1})/K$ est modérément ramifiée. Si e est son indice de ramification, il résulte donc du théorème 2 que $\text{Br}_\mu(K)$ est le sous-groupe de $\text{Br}(K)$ d'ordre e.

Soit $\overline{K}$ une clôture algébrique de K et soit K_{nr} l'extension maximale non ramifiée de K contenue dans $\overline{K}$. Il est clair que e est égal au degré de l'extension $K_{nr}(\sqrt[p]{1})/K_{nr}$. L'assertion résulte alors du fait qu'un corps local à corps résiduel algébriquement clos contient les racines $p^{\text{ièmes}}$ de l'unité si et seulement si son indice de ramification absolu est divisible par $p-1$ (*cf.* [10], cor. 2 à la prop. 6, p. 114).

Remarques :

(*a*) On voit en particulier que, si K est une extension finie de $\mathbf{Q}_p$ qui contient les racines $p^{\text{ièmes}}$ de l'unité (pour $p = 2$, les racines quatrièmes de l'unité), alors $\text{Br}_\mu(K) = 1$. Ce résultat avait déjà été obtenu par Witt ([13], Satz 12).

(*b*) Il est clair que le corollaire peut encore s'écrire sous la forme suivante :

Corollaire 2. — *Soit* K *une extension finie de* $\mathbf{Q}_p$ *(si* $p = 2$, *on suppose que* K *contient les racines quatrièmes de l'unité). Soit* K_0 *l'extension maximale non*

ramifiée de $\mathbf{Q}_p$ *contenue dans* K. *Alors* $\mathrm{Br}_\mu(K_0)$ *est le sous-groupe de* $\mathrm{Br}(K_0)$ *d'ordre* $p-1$ *et* $\mathrm{Br}_\mu(K)$ *est la restriction à* K *de* $\mathrm{Br}_\mu(K_0)$.

1.3.4. *Calcul explicite de l'invariant, pour* $p \neq 2$. — Soit $\bar{\varepsilon}$ un élément de $\mathrm{Br}_\mu(K)$ défini par un cocycle ε à valeurs dans le groupe des racines de l'unité d'une extension finie cyclotomique de K. Nous nous proposons de donner une formule explicite de l'invariant de $\bar{\varepsilon}$.

Soit $q = p^a$ le nombre d'éléments du corps résiduel de K (on suppose $p \neq 2$). Soit L une extension finie cyclotomique de K. Soit d (resp. e) le degré (resp. l'indice de ramification) de l'extension $L^{(p)}/K$. Soit $d_0 = d/e$. Posons $h = (q^{d_0}-1)/d_0(q-1)$. On a

$$h = 1 + \sum_{j=2}^{d_0} \binom{d_0}{j} \cdot (q-1)^{j-1}/d_0 = 1 + ((q-1)/d_0) \cdot \sum_{j=2}^{d_0} \binom{d_0}{j} \cdot (q-1)^{j-2},$$

et h est un entier car d_0 divise $q-1$.

Le groupe d'inertie G_0 de l'extension L/K est le produit direct d'un p-groupe G_{sr} par un groupe cyclique G_{mr} d'ordre e. Soit μ_e le groupe des racines $e^{\text{ièmes}}$ de l'unité contenues dans K. Le groupe G_{mr} opère trivialement sur μ_e et $H^1(G_{mr}, \mu_e)$ s'identifie au groupe des caractères de degré 1 de G_{mr} à valeurs dans μ_e.

Soit $\overline{G}_0$ le groupe d'inertie de l'extension $L^{(p)}/K$ et soit θ_0 le caractère de $\overline{G}_0$ défini au n° 1.3.2. Il est clair que le groupe $\overline{G}_0$ est canoniquement isomorphe à G_{mr} et θ_0 peut être considéré comme un générateur de $H^1(G_{mr}, \mu_e)$.

Soit φ un élément du groupe de Galois G de L/K dont l'image canonique dans G/G_0 est le générateur de Frobenius F du groupe de Galois de L^{nr}/K.

Soit ε un représentant, à valeurs dans $\mu(L)$, d'un élément $\bar{\varepsilon}$ de $H^2_\mu(L/K)$. Il s'écrit, d'une manière et d'une seule, sous la forme $\varepsilon = \varepsilon'\varepsilon''$, où ε' (resp. ε'') est un 2-cocycle de G à valeurs dans $\mu'(L)$ [resp. $\mu''(L)$].

Pour tout t dans G_{mr}, posons

$$\lambda_\varepsilon(t) = \varepsilon'^{-h}_{t,\varphi}\, \varepsilon'^{h}_{\varphi,t} \cdot \Big(\prod_{u \in G_{mr}} \varepsilon'_{t,u} \Big)^{-(q^{d/e}-1)/d}. \tag{4}$$

Proposition 1.7. — *Soit* ε *un représentant, à valeurs dans* $\mu(L)$, *d'un élément* $\bar{\varepsilon}$ *de* $H^2_\mu(L/K)$. *Alors* λ_ε *est un caractère de* G_{mr} *à valeurs dans* μ_e. *Si* $\lambda_\varepsilon = \theta_0^k$, *l'invariant de* $\bar{\varepsilon}$ *est* k/e.

Démonstration. — D'après la proposition 1.5, ε est cohomologue à ε' et on peut supposer que $\varepsilon = \varepsilon'$.

D'après la proposition 1.3, ε est alors cohomologue dans $\mu'(L)$ à un élément de $H^2(L^{(p)}/K, \mu')$. Soit s un générateur du groupe de Galois $\overline{G}$ de l'extension $L^{(p)}/K$. On a vu au n° 1.2.1 que tout 2-cocycle de $\overline{G}$ à valeurs dans $\mu'(L^{(p)})$ est cohomologue, dans $\mu'(L^{(p)})$, à un 2-cocycle ε^0 de la forme

$$\varepsilon^0_{s^k, s^{k'}} = \begin{cases} 1 & \text{si } k+k' < d \\ b & \text{si } k+k' \geq d \end{cases} \qquad \text{pour} \quad 0 \leq k, k' \leq d-1,$$

b étant un élément de $\mu'(K)$. Il existe donc une application m de G dans $\mu'(L)$ et un 2-cocycle ε^1 tels que :

— d'une part, pour σ, τ dans G, on ait $\varepsilon_{\sigma,\tau} = (\sigma(m_\tau)\, m_\sigma / m_{\sigma\tau}).\varepsilon^1_{\sigma,\tau}$;

— d'autre part, si $\bar{\sigma}$ désigne l'image canonique de σ dans $\overline{G}$, pour σ, τ dans G, on ait $\varepsilon^1_{\sigma,\tau} = \varepsilon^0_{\bar{\sigma},\bar{\tau}}$.

Il est clair que l'on peut choisir un générateur t_0 de G_{mr} pour que $\bar{t}_0 = s^{d/e}$.

Supposons d'abord que $\varepsilon = \varepsilon^1$. Pour tout entier j compris entre 0 et $e-1$, on a $\varepsilon_{t_0^j, \varphi} = \varepsilon_{\varphi, t_0^j}$; d'autre part, on voit que

$$\varepsilon_{t_0^i, t_0^j} = \varepsilon^0_{s^{di/e}, s^{dj/e}} = \begin{cases} 1 & \text{si } i+j < e \\ b & \text{si } i+j \geq e \end{cases} \qquad \text{pour} \quad 0 \leq i, j \leq e-1.$$

On a donc $\prod_{u \in G_{mr}} \varepsilon_{t_0^i, u} = \prod_{j=0}^{e-1} \varepsilon_{t_0^i, t_0^j} = b^i$. Par conséquent $\lambda_\varepsilon(t_0^i) = (b^{-(q^{d/e}-1)/d})^i$. On voit que λ_ε est bien un caractère de G_{mr} à valeurs dans μ_e. Si $\theta_0(s^{d/e}) = \nu$ et si $b^{-(q^{d/e}-1)/d} = \nu^k$, alors, d'après la formule (3), l'invariant de $\bar{\varepsilon}$ est k/e. Il est clair que cette condition revient bien à affirmer que $\lambda_\varepsilon = \theta_0^k$.

Revenons au cas général. Pour tout couple s, t d'éléments de G, posons $\gamma_{s,t} = \varepsilon_{s,t}/\varepsilon^1_{s,t}$. Pour tout t dans G_{mr}, on a $\gamma_{t,\varphi} = t(m_\varphi)\, m_t / m_{t\varphi} = m_\varphi m_t / m_{t\varphi}$, puisque m_φ est un élément de $\mu'(L)$, groupe sur lequel G_{mr} opère trivialement. De même, $\gamma_{\varphi,t} = \varphi(m_t)\, m_\varphi / m_{\varphi t} = m_t^q m_\varphi / m_{t\varphi}$, puisque le groupe G est abélien et puisque l'action de φ sur tout élément de $\mu'(L)$ est la même que celle de l'automorphisme F de Frobenius. On a donc $\gamma^{-h}_{t,\varphi} \varphi^h_{\varphi,t} = m_t^{h(q-1)}$.

Pour tout couple t, u d'éléments de G_{mr}, on a

$$\gamma_{t,u} = t(m_u)\, m_t / m_{tu} = (m_u / m_{tu}).m_t,$$

puisque m_u est un élément de $\mu'(L)$ sur lequel G_{mr} opère trivialement. On a donc

$$\prod_{u \in G_{mr}} \gamma_{t,u} = \prod_{u \in G_{mr}} ((m_u / m_{tu}).m_t) = m_t^e.$$

Par conséquent, $\lambda_\gamma(t) = m_t^{h(q-1)-e(q^{d/e}-1)/d} = 1$, puisque

$$h(q-1) = e(q^{d/e}-1)/d.$$

Donc, $\lambda_\varepsilon(t) = \lambda_\gamma(t).\lambda_{\varepsilon^t}(t) = \lambda_{\varepsilon^t}(t)$ et $\lambda_\varepsilon = \lambda_{\varepsilon^t}$. En particulier, si $\lambda_\varepsilon = \theta_0^k$, l'invariant de $\bar{\varepsilon}$ est bien k/e. C. Q. F. D.

COROLLAIRE. — *Le caractère* λ_ε *ne dépend pas du choix du représentant* ε, *à valeurs dans* L, *de* $\bar{\varepsilon}$.

En effet, pour tout entier k il existe un caractère λ de G_{mr} à valeurs dans μ_e et un seul tel que $\lambda = \theta_0^k$.

Remarque. — On comparera la formule (4) et la proposition 1.7 avec le calcul de l'invariant fait par Witt dans le cas où $K = \mathbf{Q}_p$ ([13], Satz 10).

1.4. LE CAS $p = 2$ AVEC $\sqrt{-1} \notin K$.

1.4.1. *Le groupe* $H^2(L/K, \mu)$. — Soit K une extension finie de $\mathbf{Q}_2$ ne contenant pas les racines quatrièmes de l'unité.

Soit L une extension de K de degré 2. Soit $H = \{1, h\}$ le groupe de Galois de l'extension. Soit ε^L l'application de $H \times H$ dans $\mu(L)$ définie par

$$\varepsilon^L_{1,1} = \varepsilon^L_{1,h} = \varepsilon^L_{h,1} = 1, \qquad \varepsilon^L_{h,h} = -1. \tag{5}$$

Il est immédiat que ε^L est un 2-cocycle de H. On note $\bar{\varepsilon}^L$ son image dans $H^2(L/K, \mu'')$.

Soit K′ l'unique extension non ramifiée de K de degré 2 et soit $\hat{K} = K'(\sqrt{-1})$. Soit s (resp. t) l'élément différent de l'unité du groupe de Galois de $\hat{K}/K'$ [resp. $\hat{K}/K(\sqrt{-1})$]. Posons $r = st$. On voit que le groupe de Galois J de l'extension $\hat{K}/K$ est abélien de type (2, 2) et que ses trois éléments d'ordre 2 sont r, s et t. Soit ν un générateur de $\mu''(K(\sqrt{-1}))$. Considérons l'application η_1 de $J \times J$ dans $\mu''(\hat{K})$ définie par

$$\eta_{r^i s^j, r^{i'} s^{j'}} = \begin{cases} \nu^{(-1)^i} & \text{si } j = i' = 1 \\ 1 & \text{sinon} \end{cases} \qquad \text{pour } i, j, i', j' \text{ dans } \{0, 1\}. \tag{6}$$

On vérifie, par un calcul sans difficulté, que η_1 est un 2-cocycle de J. Considérons l'application a de J dans $\mu''(\hat{K})$ définie par

$$a_{r^i s^j} = \begin{cases} 1 & \text{si } i = 0 \\ \nu^{-1} & \text{si } i = 1 \end{cases} \qquad \text{pour } j = 0, 1.$$

On vérifie immédiatement que son cobord est η_1^2. On en déduit que l'image $\bar{\eta}_1$ de η_1 dans $H^2(L/K, \mu'')$ ne dépend pas du choix de la racine primitive ν.

THÉORÈME 1′. — *Soit* K *une extension finie de* $\mathbf{Q}_2$ *ne contenant pas les racines quatrièmes de l'unité. Soit* L *une extension finie cyclotomique de* K *contenant les racines quatrièmes de l'unité. Soit* m *le degré de l'extension maximale non ramifiée de* K *contenue dans* L. *Alors :*

(i) *si* m *est impair,* $H^2(L/K, \mu) = H^2(K(\sqrt{-1})/K, \mu'')$;

(ii) *si* m *est pair,* $H^2(L/K, \mu) = H^2(\hat{K}/K, \mu'')$.

Nous allons, en fait, établir la proposition suivante, plus précise :

PROPOSITION 1.8. — *Avec les notations et les hypothèses du théorème* 1′ :

(i) *si* m *est impair,* $H^2(L/K, \mu)$ *est un groupe cyclique d'ordre* 2. *L'élément non trivial de ce groupe est* $\bar{\varepsilon}^{K(\sqrt{-1})}$;

(ii) *si* m *est pair,* $H^2(L/K, \mu)$ *est un groupe abélien de type* (2, 2, 2). *Les éléments* $\bar{\varepsilon}^{K(\sqrt{-1})}$, $\bar{\varepsilon}^{K'}$, $\bar{\gamma}_1$ *engendrent le groupe.*

Démonstration. — Comme $L^{(2)} = K$, il résulte de la proposition 1.3 que $H^2(L/K, \mu') = 1$. On a donc $H^2(L/K, \mu) = H^2(L/K, \mu'')$ et il suffit de démontrer la proposition 1.8 en remplaçant μ par μ''. D'après la proposition 1.4, on a $H^2(L/K, \mu'') = H^2(L^{nr}(\sqrt{-1})/K, \mu'')$ et on peut supposer que $L = L^{nr}(\sqrt{-1})$.

Soit M la 2-extension maximale de K contenue dans L. L'extension L/M est cyclique d'ordre m_1 impair. Soit H son groupe de Galois. On a

$$\mu''(M) = \mu''(L) \qquad \text{et} \qquad N_{L/M}(\mu''(L)) = (\mu''(L))^{m_1} = \mu''(L) = \mu''(M).$$

D'après le lemme 1, on a donc

$$H^2(L/K, \mu'') = H^2(M/K, \mu'').$$

Si m est impair, on a alors $H^2(L/K, \mu) = H^2(K(\sqrt{-1})/K, \mu'')$ et on vérifie immédiatement que ce groupe est engendré par $\bar{\varepsilon}^{K(\sqrt{-1})}$ et que cet élément est d'ordre 2.

Si m est pair, on voit que l'on peut se ramener au cas où $m = 2^a$, avec $a \geqq 1$. Soit s (resp. t) un générateur du groupe de Galois de l'extension L/L^{nr} [resp. $L/K(\sqrt{-1})$]. Posons $r = st$. Le groupe de Galois J de l'extension L/K est le produit direct du groupe cyclique engendré par r, qui est d'ordre 2^a, par le groupe cyclique engendré par s, qui est d'ordre 2.

Comme l'extension $L/K(\sqrt{-1})$ est non ramifiée, on a $\mu''(L) = \mu''(K(\sqrt{-1}))$ et, par conséquent, t opère trivialement sur $\mu''(L)$. Soit 2^b, avec $b \geqq 2$, l'ordre de $\mu''(L)$, et soit ν un générateur de $\mu''(L)$. On voit que l'action de J sur $\mu''(L)$ est définie par $r(\nu) = \nu^{-1}$ et $s(\nu) = \nu^{-1}$. Le groupe $H^2(L/K, \mu'')$ s'identifie alors au groupe des extensions de J par le J-module $\mu''(L)$.

Soit Γ une extension de J par $\mu''(L)$ et soit ρ (resp. σ) un élément de Γ dont l'image canonique dans J est r (resp. s). On a

$$\rho\nu\rho^{-1}=\nu^{-1} \qquad \text{et} \qquad \sigma\nu\sigma^{-1}=\nu^{-1}.$$

Il est clair que Γ est entièrement déterminé par la donnée de ρ^{2^a}, σ^2 et $\sigma\rho\sigma^{-1}\rho^{-1}$. Comme $\rho^{2^a}=\rho(\rho^{2^a})\rho^{-1}=\rho^{-2^a}$, l'élément ρ^{2^a} doit appartenir à $\{1,-1\}$. De la même manière, σ^2 doit appartenir à $\{1,-1\}$.

Soit $\rho'=\nu^c\rho$ et $\sigma'=\nu^d\sigma$ d'autres représentants de r et s dans Γ. On voit que $\rho'^2=\nu^c\rho\nu^c\rho=\rho^2$, donc que $\rho'^{2^a}=\rho^{2^a}$. De même, $\sigma'^2=\sigma^2$. Enfin, on a

$$\sigma'\rho'\sigma'^{-1}\rho'^{-1}=\nu^d\sigma\nu^c\rho\sigma^{-1}\nu^{-d}\rho^{-1}\nu^{-c}=\nu^d\nu^{-c}\sigma\rho\sigma^{-1}\rho^{-1}\nu^d\nu^{-c}=\nu^{2(d-c)}\sigma\rho\sigma^{-1}\rho^{-1}.$$

On peut donc choisir σ et ρ pour que $\sigma\rho\sigma^{-1}\rho^{-1}$ soit égal à ν ou à 1. En revanche, les éléments ρ^{2^a} et σ^2 sont indépendants du choix de ρ et σ. Il est immédiat que :

(i) si $\rho^2=1$, $\sigma^2=-1$, $\sigma\rho\sigma^{-1}\rho^{-1}=1$, alors la classe définie par Γ est $\bar{\varepsilon}^{K(\sqrt{-1})}$;

(ii) si $\rho^2=-1$, $\sigma^2=-1$, $\sigma\rho\sigma^{-1}\rho^{-1}=1$, alors la classe définie par Γ est $\bar{\varepsilon}^{K'}$;

(iii) si $\rho^2=1$, $\sigma^2=1$, $\sigma\rho\sigma^{-1}\rho^{-1}=\nu$, alors la classe définie par Γ est $\bar{\eta}$; et que, pour toute extension Γ de J par $\mu''(L)$, la classe définie par Γ est le produit de certaines de ces trois classes. C. Q. F. D.

1.4.2. *Le groupe* $H^2_\mu(L/K)$.

THÉORÈME 2'. — *Avec les notations et les hypothèses du théorème* 1', *on a :*

(*a*) *si m est impair :*

(*a*.i) *si le degré de l'extension* $K/\mathbf{Q}_2$ *est pair,* $H^2_\mu(L/K)=1$;

(*a*.ii) *si le degré de l'extension* $K/\mathbf{Q}_2$ *est impair,* $H^2_\mu(L/K)$ *est le sous-groupe de* $Br(K)$ *d'ordre* 2;

(*b*) *si m est pair, soit* K_c *l'extension cyclotomique maximale de* $\mathbf{Q}_2$ *contenue dans* K;

(*b*.i) *si le degré de l'extension* K/K_c *est pair,* $H^2_\mu(L/K)=1$;

(*b*.ii) *si le degré de l'extension* K/K_c *est impair,* $H^2_\mu(L/K)$ *est le sous-groupe de* $Br(K)$ *d'ordre* 2.

Démonstration. — Comme -1 n'est pas norme dans l'extension $\mathbf{Q}_2(\sqrt{-1})/\mathbf{Q}_2$, il est clair que l'invariant de l'image de $\bar{\varepsilon}^{\mathbf{Q}_2(\sqrt{-1})}$ dans $H^2(\mathbf{Q}_2(\sqrt{-1})/\mathbf{Q}_2)$ est 1/2. Comme l'image de $\bar{\varepsilon}^{K(\sqrt{-1})}$ dans $H^2(K(\sqrt{-1})/K)$ n'est autre que la restriction de l'image de $\bar{\varepsilon}^{\mathbf{Q}_2(\sqrt{-1})}$ dans $H^2(\mathbf{Q}_2(\sqrt{-1})/\mathbf{Q}_2)$,

son invariant est $m/2$ et l'assertion (a) résulte du (i) de la proposition 1.8.

Comme l'extension K′/K est non ramifiée, il résulte de la proposition 1.2 que l'image de $\bar{\varepsilon}^{K'}$ dans $H^2(K'/K)$ est égale à 1.

LEMME 4. — *L'invariant de l'image de* $\bar{\eta}$ *dans* $H^2(\hat{K}/K)$ *est* 0 *ou* $1/2$ *suivant que le degré de l'extension* K/K_c *est pair ou impair.*

Démonstration du lemme. — Soit $\bar{\eta}_c$ l'élément de $H^2(\hat{K}_c/K_c, \mu)$ obtenu en remplaçant, dans la définition de η, le corps K par le corps K_c. Il est clair que l'image de $\bar{\eta}$ dans $H^2(\hat{K}/K)$ n'est autre que la restriction de l'image de $\bar{\eta}_c$ dans $H^2(\hat{K}_c/K_c)$. L'invariant de l'image de $\bar{\eta}$ est donc le produit de l'invariant de l'image de $\bar{\eta}_c$ par le degré de l'extension K/K_c. Il suffit donc de montrer que, lorsque K est une extension finie cyclotomique de $\mathbf{Q}_2$, l'invariant de l'image de $\bar{\eta}$ est $1/2$.

Le groupe de Galois de l'extension $\hat{K}/K$ est $J = \{1, r, s, t\}$. Posons $a_1 = 1$, $a_r = 1$, $a_s = 1 + \nu^{-1}$, $a_t = 1 + \nu$. Considérons le 2-cocycle η' de J à valeurs dans $\hat{K}$ défini par

$$\eta'_{\sigma,\tau} = (\sigma(a_\tau)\, a_\sigma / a_{\sigma\tau})\, \eta_{\sigma,\tau} \quad \text{pour } \sigma, \tau \text{ dans J.}$$

Les 2-cocycles η' et η sont cohomologues dans $\hat{K}$. Un calcul, sans difficultés, montre que, pour i, j, i', j' appartenant à $\{0, 1\}$,

$$\eta'_{r^i s^j, r^{i'} s^{j'}} = \begin{cases} 1 & \text{si } j = 0 \quad \text{ou si } j' = 0; \\ \nu(1 + \nu^{-1})^2 & \text{si } j = j' = 1. \end{cases}$$

Posons $b = \nu(1 + \nu^{-1})^2$. Soit $\tilde{K}$ le corps fixe du groupe cyclique engendré par r, et soit u l'élément non nul du groupe de Galois de l'extension $\tilde{K}/K$. Le 2-cocycle η' est l'image par inflation du 2-cocycle $\tilde{\eta}$ de $\{1, u\}$:

$$\tilde{\eta}_{1,1} = \tilde{\eta}_{1,u} = \tilde{\eta}_{u,1} = 1, \qquad \tilde{\eta}_{u,u} = b.$$

Il est alors clair que l'invariant de l'image de $\bar{\eta}$ est 0 ou $1/2$ suivant que b est ou n'est pas norme dans l'extension $\tilde{K}/K$.

Comme $b = (1 + \nu)(1 + \nu^{-1})$, on voit que b est norme dans l'extension $K(\sqrt{-1})/K$. On en déduit que, pour achever la démonstration du lemme, il suffit de montrer que b n'est pas norme dans l'extension K′/K. Comme l'extension K′/K est non ramifiée, cela revient à montrer que la valuation normalisée de b dans K est un entier impair (*cf.* CL, prop. 13, p. 105).

Or on a $b = \nu^{-1}(1 + \nu)^2$. Désignons par v (resp. v_1) la valuation normalisée de K [resp. $K(\sqrt{-1})$]. On a évidemment $v(b) = v_1(b)/2$ et

$v_1(b) = v_1(\nu^{-1}) + 2\,v_1(1+\nu) = 2\,v_1(1+\nu)$. Donc $v(b) = v_1(1+\nu)$. Comme l'extension $K/\mathbf{Q}_2$ est cyclotomique, l'extension $K(\sqrt{-1})/\mathbf{Q}_2(\nu)$ est non ramifiée et, si on désigne par v'_1 la valuation normalisée de $\mathbf{Q}_2(\nu)$, on a $v'_1(1+\nu) = v_1(1+\nu)$. Posons $\pi = \nu - 1$. On sait (*cf.* CL, prop. 17, p. 85) que π est une uniformisante de $\mathbf{Q}_2(\nu)$. On a donc

$$v'_1(1+\nu) = v'_1(1+1+\pi) = v'_1(\pi+2) = 1.$$

On a bien $v(b) = 1$. C. Q. F. D.

Fin de la démonstration du théorème 2'. — Il suffit d'appliquer la partie (ii) de la proposition 1.8.

Si le degré de l'extension K/K_c est pair, on vérifie immédiatement que les images de $\bar{\varepsilon}^{K(\sqrt{-1})}$, $\bar{\varepsilon}^{K'}$, $\bar{\eta}$ dans $H^2(\hat{K}/K)$ sont toutes égales à 1.

Si le degré de l'extension K/K_c est impair, on voit que l'image de $\bar{\varepsilon}^{K'}$ dans $H^2(\hat{K}/K)$ est égale à 1, que celle de $\bar{\varepsilon}^{K(\sqrt{-1})}$ est égale à 1 ou d'ordre 2 suivant les cas et que celle de $\bar{\eta}$ est d'ordre 2. C. Q. F. D.

Corollaire 1'. — *Soit* K *une extension finie de* $\mathbf{Q}_2$ *et soit* K_c *l'extension cyclotomique maximale de* $\mathbf{Q}_2$ *contenue dans* K. *Alors :*

(i) *si* $\sqrt{-1} \in K$, *on a* $\mathrm{Br}_\mu(K) = 1$;

(ii) *si* $\sqrt{-1} \notin K$, *et si le degré de* K/K_c *est pair, on a* $\mathrm{Br}_\mu(K) = 1$;

(iii) *si* $\sqrt{-1} \notin K$, *et si le degré de* K/K_c *est impair,* $\mathrm{Br}_\mu(K)$ *est le sous-groupe de* $\mathrm{Br}(K)$ *d'ordre* 2.

C'est clair.

Remarque. — Il est immédiat que le corollaire 1' peut encore s'écrire de la manière suivante :

Corollaire 2'. — *Soit* K *une extension finie de* $\mathbf{Q}_2$ *et soit* K_c *l'extension maximale cyclotomique de* $\mathbf{Q}_2$ *contenue dans* K. *Alors* $\mathrm{Br}_\mu(K_c)$ *est le sous-groupe de* $\mathrm{Br}(K_c)$ *d'ordre* 1 *ou* 2 *suivant que* K *contient ou non les racines quatrièmes de l'unité et* $\mathrm{Br}_\mu(K)$ *est la restriction à* K *de* $\mathrm{Br}_\mu(K_c)$.

1.4.3. *Calcul explicite de l'invariant.* — Soit K une extension finie de $\mathbf{Q}_2$. Soit L une extension finie cyclotomique de K et soit G le groupe de Galois de l'extension. Soit ε un 2-cocycle de G à valeurs dans $\mu(L)$. Nous nous proposons de donner une formule explicite de l'invariant, $\mathrm{inv}(\varepsilon)$, de l'image de ε dans $\mathrm{Br}(K)$. Il résulte du corollaire précédent que l'on peut se contenter de le faire lorsque $\sqrt{-1} \notin K$. Par inflation, on peut toujours supposer que $\sqrt{-1}$ appartient à L.

Soit 2^a (resp. 2^b) l'ordre de $\mu''(K(\sqrt{-1}))$ [resp. $\mu''(L)$]. Soit ν une racine primitive $(2^b)^{\text{ième}}$ de l'unité. Il est clair que le groupe d'inertie de l'extension L/K est le produit direct de deux sous-groupes cycliques :

— un groupe cyclique d'ordre 2 engendré par l'élément s défini par $s(\nu) = \nu^{-1}$;

— un groupe cyclique d'ordre 2^{b-a} engendré par l'élément u défini par $u(\nu) = \nu^{1+2^a}$.

L'extension $L/K(\nu)$ est cyclique et non ramifiée. Soit t un générateur de son groupe de Galois. Tout 2-cocycle ε de G à valeurs dans $\mu(L)$ se décompose de manière unique sous la forme $\varepsilon = \varepsilon'\varepsilon''$ où ε' (resp. ε'') est un 2-cocycle de G à valeurs dans $\mu'(L)$ [resp. $\mu''(L)$]. Posons

$$(7) \qquad \begin{cases} \lambda_1(\varepsilon) = \varepsilon''_{1,s}\,\varepsilon''_{s,s}, \\ \lambda_2(\varepsilon) = \varepsilon''_{u,t}\,\varepsilon''^{-1}_{t,u}\,(\varepsilon''_{s,t}\,\varepsilon''^{-1}_{t,s})^{2^{a-1}}, \\ \lambda_3(\varepsilon) = \lambda_1(\varepsilon)\,\lambda_2(\varepsilon). \end{cases}$$

Pour $i = 1, 2, 3$, posons

$$(8) \qquad \theta_i(\varepsilon) = \begin{cases} 0 & \text{si } \lambda_i(\varepsilon) = 1, \\ 1/2 & \text{sinon.} \end{cases}$$

Désignons encore par K_c l'extension cyclotomique maximale de $\mathbf{Q}_2$ contenue dans K.

PROPOSITION 1.9. — *Avec les hypothèses et les notations qui précèdent, les* $\lambda_i(\varepsilon)$ *sont à valeurs dans* $\mu''(K) = \{1, -1\}$. *De plus,*

(i) *si les extensions* $K/\mathbf{Q}_2$ *et* L^{nr}/K *sont toutes deux de degré impair,* $\mathrm{inv}(\varepsilon) = \theta_1(\varepsilon)$;

(ii) *si les extensions* $K/\mathbf{Q}_2$ *et* L^{nr}/K *sont de degré pair et si l'extension* K/K_c *est de degré impair,* $\mathrm{inv}(\varepsilon) = \theta_2(\varepsilon)$;

(iii) *si l'extension* $K/\mathbf{Q}_2$ *est de degré impair et si l'extension* L^{nr}/K *est de degré pair,* $\mathrm{inv}(\varepsilon) = \theta_3(\varepsilon)$;

(iv) *dans tous les autres cas,* $\mathrm{inv}(\varepsilon) = 0$.

Démonstration. — Il résulte de la proposition 1.3 que $H^2(L/K, \mu') = 1$. On a donc $\mathrm{inv}(\varepsilon) = \mathrm{inv}(\varepsilon'')$ et on peut supposer que $\varepsilon = \varepsilon''$.

LEMME 5. — *Si* $\tilde{\varepsilon}$ *et* ε *sont des 2-cocycles de* G *à valeurs dans* $\mu''(L)$, *cohomologues dans* $\mu''(L)$, *alors, pour* $i = 1, 2, 3$, *on a* $\lambda_i(\tilde{\varepsilon}) = \lambda_i(\varepsilon)$.

Démonstration du lemme. — Soit a une application de G dans $\mu''(L)$. Supposons que, pour tout couple σ, τ d'éléments de G, $\tilde{\varepsilon}_{\sigma,\tau} = \sigma(a_\tau) a_\sigma a_{\sigma\tau}^{-1} \varepsilon_{\sigma,\tau}$. Alors :

(*a*) On a

$$\lambda_1(\tilde{\varepsilon}) = a_s a_1 a_s^{-1} . s(a_s) a_s a_1^{-1} . \lambda_1(\varepsilon) = \lambda_1(\varepsilon),$$

car

$$s(a_s) = a_s^{-1}.$$

(*b*) On a

$$\tilde{\varepsilon}_{u,t} \tilde{\varepsilon}_{t,u}^{-1} = u(a_t) a_u a_{ut}^{-1} . (t(a_u) a_t a_{tu}^{-1})^{-1} . \varepsilon_{u,t} \varepsilon_{t,u}^{-1} = a_t^{2^a} \varepsilon_{u,t} \varepsilon_{t,u}^{-1}$$

car

$$u(a_t) = a_t^{1+2^a}, \qquad a_{ut} = a_{tu} \qquad \text{et} \qquad t(a_u) = a_u.$$

D'autre part,

$$\tilde{\varepsilon}_{s,t} \tilde{\varepsilon}_{t,s}^{-1} = s(a_t) a_s a_{st}^{-1} . (t(a_s) a_t a_{ts}^{-1})^{-1} . \varepsilon_{s,t} \varepsilon_{t,s}^{-1} = a_t^{-2} . \varepsilon_{s,t} \varepsilon_{t,s}^{-1},$$

car

$$s(a_t) = a_t^{-1}, \qquad t(a_s) = a_s \qquad \text{et} \qquad a_{st} = a_{ts}.$$

Finalement,

$$\lambda_2(\tilde{\varepsilon}) = a_t^{2^a} a_t^{-2 \times 2^{a-1}} . \lambda_2(\varepsilon) = \lambda_2(\varepsilon).$$

(*c*) Enfin, l'assertion pour $i = 3$ résulte trivialement de l'assertion pour $i = 1$ et 2. C. Q. F. D.

Fin de la démonstration de la proposition 1.9. — Compte tenu du lemme précédent, il suffit de vérifier la proposition 1.9 pour un représentant de chaque élément d'un système de générateurs du groupe $H^2(L/K, \mu'')$. On peut prendre les générateurs indiqués dans la proposition 1.8 et appliquer le lemme 4 et le théorème 2'. Le calcul ne présente aucune difficulté.

C. Q. F. D.

2. Algèbres de groupes (rappel de résultats).

Dans tout ce paragraphe, on désigne par E un corps et par $\overline{E}$ une clôture algébrique de E.

2.1. Le groupe de Brauer classique. — Soit D un anneau. Nous notons $M_n(D)$ l'algèbre des matrices (n, n) à coefficients dans D.

Soit A une E-algèbre de dimension finie. L'algèbre A est appelée une *algèbre simple centrale sur* E si elle n'a pas d'idéal bilatère non trivial et si son centre est E. On sait (théorème de Wedderburn, *cf.* par exemple CL, prop. 7, p. 165) qu'il existe alors un corps gauche D de centre E et un entier strictement positif n tels que A est E-isomorphe à $M_n(D)$.

Deux algèbres simples A et A′ centrales sur E sont dites équivalentes s'il existe un corps gauche D de centre E et deux entiers strictement positifs n et n' tels que A (resp. A′) soit E-isomorphe à $M_n(D)$ [resp. $M_{n'}(D)$]. Soit A(E) l'ensemble des classes d'algèbres simples centrales sur E pour cette relation d'équivalence. Le produit tensoriel au-dessus de E définit, par passage au quotient, une structure de groupe abélien sur A(E). C'est ce groupe que l'on appelle classiquement *le groupe de Brauer de* E.

Soit $\bar{\varepsilon}$ un élément de Br(E). Soit F une extension finie galoisienne de E qui décompose $\bar{\varepsilon}$. Alors, $\bar{\varepsilon}$ s'identifie à un élément de $H^2(F/E)$. Soit J le groupe de Galois de l'extension et soit d son ordre. Soit ε un représentant de $\bar{\varepsilon}$ dans les 2-cocycles de J. Considérons l'espace vectoriel de dimension d sur F,

$$A = \sum_{\sigma \in J} F u_\sigma.$$

On le munit d'une structure d'algèbre en posant

$$u_\sigma a = \sigma(a) u_\sigma \quad \text{pour} \quad \sigma \in J \quad \text{et} \quad a \in F;$$
$$u_\sigma u_\tau = \varepsilon_{\sigma,\tau} u_{\sigma\tau} \quad \text{pour} \quad \sigma, \tau \in J.$$

On vérifie (*cf.* [8], exp. 7, th. 13) qu'on obtient ainsi une algèbre simple centrale sur E et que sa classe ne dépend pas du choix du représentant ε de $\bar{\varepsilon}$. On a donc ainsi défini une application de Br(E) dans A(E) et on montre (*ibid.*, th. 14) que cette application est, en fait, un isomorphisme. Dans toute la suite de cet article, nous identifierons Br(E) et A(E). Pour toute algèbre simple centrale A sur E, nous noterons $\bar{\varepsilon}_E(A)$ sa classe.

Remarque. — Dans « CL » (chap. X, § 5), Serre donne une autre façon d'identifier Br(E) et A(E). On obtient ainsi l'identification opposée à celle que nous utilisons (*cf.* CL, exerc. 2, p. 167).

Dans chaque classe $\bar{\varepsilon}$, il y a, à un E-isomorphisme près, un et un seul corps gauche $D_{\bar{\varepsilon}}$. Sa dimension sur E est le carré d'un nombre entier strictement positif que l'on appelle l'*indice de Schur de* $\bar{\varepsilon}$ et que l'on note $m_E(\bar{\varepsilon})$. Si A est une algèbre simple centrale sur E, on appelle *indice de Schur de* A, et on note $m_E(A)$, l'indice de Schur de sa classe. Toute algèbre simple centrale A sur E est définie, à un E-isomorphisme près, par la donnée de sa classe $\bar{\varepsilon}$ et de l'entier n strictement positif tels que A soit isomorphe à $M_n(D_{\bar{\varepsilon}})$. L'algèbre A est alors de dimension $(n \times m_E(A))^2$ sur E.

L'ordre de $\bar{\varepsilon}$ divise $m_E(\bar{\varepsilon})$ et, dans le cas où E est un corps de nombres ou une complétion d'un corps de nombres, l'ordre de $\bar{\varepsilon}$ est égal à $m_E(\bar{\varepsilon})$.

Si A est une algèbre simple centrale sur E et si F est une extension de E, l'algèbre $A \otimes_E F$ est une algèbre simple centrale sur F que l'on note encore A.

Sa classe, $\bar{\varepsilon}_F(A)$ est la restriction à $Br(F)$ de $\bar{\varepsilon}_E(A)$. On en déduit que $m_F(A)$ divise $m_E(A)$. Si $\bar{\varepsilon}$ est décomposé sur F, on dit que A est *décomposée sur* F. On peut montrer que $m_E(A)$ est le pgcd des degrés des extensions finies de E sur lesquelles A est décomposée.

Si E est un corps de nombres, $Br(E)$ s'envoie dans la somme directe des $Br(E_\mathfrak{p})$, pour tous les complétés $E_\mathfrak{p}$ de E. On a la suite exacte (*cf.* CL, p. 171)

$$1 \to Br(E) \to \bigoplus Br(E_\mathfrak{p}) \xrightarrow{\sigma} \mathbf{Q}/\mathbf{Z} \to 0$$

[on a noté $Br(E)$ multiplicativement, et $\mathbf{Q}/\mathbf{Z}$ additivement], l'application σ faisant correspondre à chaque élément de $\bigoplus Br(E_\mathfrak{p})$ la somme des invariants. Ceci montre que toute algèbre simple centrale A sur E est complètement déterminée par ses restrictions dans les complétés de E. En particulier, $m_E(A)$ est le ppcm des $m_{E_\mathfrak{p}}(A)$.

2.2. Algèbres semi-simples. — Soit A une E-algèbre semi-simple de dimension finie sur E. L'algèbre A est une somme directe d'algèbres simples

$$A = \bigoplus_{i=1}^{n} A_i.$$

Pour chaque i, le centre de A_i est E-isomorphe à une extension finie E_i de E et A_i est une algèbre simple centrale sur E_i. On peut définir $\bar{\varepsilon}_{E_i}(A_i)$ et $m_{E_i}(A_i)$. L'entier $m_{E_i}(A_i)$ s'appelle aussi l'*indice de Schur de* A_i *sur* E et se note $m_E(A_i)$.

Une algèbre semi-simple est dite *décomposée sur* E si c'est un produit fini d'algèbres de matrices sur des corps commutatifs. Pour l'algèbre A, on voit que cela revient à dire que, pour tout entier i, A_i est décomposée sur E_i. L'algèbre A est donc décomposée si et seulement si tous les indices de Schur $m_E(A_i)$ sont égaux à 1.

2.3. L'algèbre d'un groupe fini. — Supposons maintenant le corps E de caractéristique 0.

Soit G un groupe fini et soit χ une fonction centrale sur G à valeurs dans $\overline{E}$. On dit que χ est un *caractère* de G (on dit parfois que χ est un *caractère propre*) s'il existe une représentation α de G par des matrices à coefficients dans $\overline{E}$ dont la trace est χ.

La représentation α ainsi associée à χ est alors définie à un isomorphisme près. On appelle noyau de χ, et on note $\mathrm{Ker}\chi$, le noyau de la représentation α. On dit que χ est *absolument irréductible* (resp. *fidèle*) si la repré-

sentation α est absolument irréductible (resp. fidèle). Si H est un sous-groupe de G et si ξ est un caractère de H, on dit que χ est *induit par* ξ s'il existe une représentation α de G, dont le caractère est χ, induite par une représentation β de H dont le caractère est ξ.

On désigne par $E(\chi)$ le sous-corps de $\overline{E}$ engendré sur E par les valeurs de χ.

L'algèbre E[G] est semi-simple, et on peut lui appliquer les considérations du n° 2.2. On a

$$E[G] = \bigoplus_{i=1}^{n} A_i,$$

les A_i étant des algèbres simples de dimension finie sur E.

Soit χ un caractère absolument irréductible de G. Le caractère χ se prolonge d'une manière et d'une seule en un E-homomorphisme du groupe additif de E[G] dans le groupe additif de $E(\chi)$. Il existe alors une algèbre A_i et une seule telle que $\chi(A_i) \neq 0$. On l'appelle le *facteur simple de* E[G] *associé à* χ, et on la désigne par $A_E(\chi)$. Si χ et χ' sont deux caractères absolument irréductibles de G, pour que $A_E(\chi) = A_E(\chi')$, il faut et il suffit que χ et χ' soient conjugués sur E [ceci signifiant qu'il existe un E-automorphisme σ de $\overline{E}$, tel que, pour tout s dans G, on ait $\chi'(s) = \sigma(\chi(s))$]. Pour toute algèbre A_i, il existe un caractère absolument irréductible χ de G tel que $A_i = A_E(\chi)$.

Soit χ un caractère absolument irréductible de G. On appelle *indice de Schur de* χ *sur* E, et on note $m_E(\chi)$, l'indice de Schur de $A_E(\chi)$. Le centre E_i de $A_i = A_E(\chi)$ est isomorphe à $E(\chi)$. La classe de $A_E(\chi)$ dans $Br(E(\chi))$ s'appelle *la classe de* χ *sur* $E(\chi)$, et se note $\bar{\varepsilon}_{E(\chi)}(\chi)$.

Soit d_χ le degré de χ. L'algèbre $A_E(\chi)$ est un espace vectoriel de dimensions d_χ^2 sur $E(\chi)$. En particulier, on voit que $m_E(\chi)$ divise le degré de χ. Soit $n_\chi = d_\chi / m_E(\chi)$. Posons $\bar{\varepsilon} = \varepsilon_{E(\chi)}(\chi)$. Il existe un E-épimorphisme α_χ de E[G] sur $M_{n_\chi}(D_{\bar{\varepsilon}})$ dont la trace est $m_E(\chi).\chi$. On dit que α_χ est un E-*épimorphisme associé à* χ. Réciproquement, soit α un E-épimorphisme de E[G] sur une algèbre simple centrale $M_n(D)$. Soit E' le centre de cette algèbre, soit $\bar{\varepsilon}$ sa classe sur E' et soit m son indice de Schur. Le corps E' s'identifie à une extension finie de E contenue dans $\overline{E}$. Soit $Tr(\alpha)$ la trace de α et soit $\chi = Tr(\alpha)/m$ (on dit que χ est la *trace réduite de* α). Alors χ est un caractère absolument irréductible de G et α est un E-épimorphisme associé à χ. En particulier, $A_E(\chi)$ est E-isomorphe à $M_n(D)$.

Si φ est un caractère de G, on dit que φ est *rationnel sur* E s'il existe une représentation de G par des matrices à coefficients dans E dont le carac-

tère est φ (par abus de langage, on dit aussi que *la représentation dont le caractère est φ est rationnelle sur* E).

Soit χ un caractère absolument irréductible de G. On voit que χ est rationnel sur $E(\chi)$ si et seulement si $m_E(\chi) = 1$. L'entier $m_E(\chi)$ peut s'interpréter comme le plus petit entier strictement positif m tel que $m\chi$ soit rationnel sur $E(\chi)$. On a le résultat suivant (*cf.* [11], § 2) :

PROPOSITION 2.1. — *Soit φ un caractère de* G. *Pour que φ soit rationnel sur* E, *il faut et il suffit que les conditions suivantes soient réalisées :*

(i) *le caractère φ est à valeurs dans* E;

(ii) *pour tout caractère absolument irréductible χ de* G, $m_E(\chi)$ *divise le produit scalaire* (χ, φ).

En particulier, on voit que, pour que tout caractère de G à valeurs dans E soit rationnel sur E, il faut et il suffit que l'algèbre E[G] soit décomposée.

Pour tout caractère φ à valeurs dans E, on appelle *indice de Schur de φ*, et on note $m_E(\varphi)$ le plus petit entier m strictement positif tel que $m\varphi$ soit rationnel sur E. On voit que, si φ est absolument irréductible, $m_E(\varphi)$ est l'indice de Schur au sens usuel. Dans le cas général, il résulte de la proposition 2.1 que $m_E(\varphi)$ est le ppcm des $m_E(\chi)/(m_E(\chi), (\chi, \varphi))$ pour tous les caractères absolument irréductibles χ de G. Il est alors clair que $m_E(\varphi)$ est le pgcd des entiers m strictement positifs tels que $m\varphi$ est rationnel sur E, et que, si F est une extension de E, $m_F(\varphi)$ divise $m_E(\varphi)$.

3. Caractères E-opposés et représentations induites.

Dans tout ce paragraphe, on désigne par E un corps de caractéristique o, par $\overline{E}$ une clôture algébrique de E, et par G un groupe fini.

3.1. CARACTÈRES E-OPPOSÉS. — Soit G′ un groupe fini. Soit χ (resp. χ') un caractère absolument irréductible de G (resp. G′) à valeurs dans E. Le caractère $\chi \otimes \chi'$ est un caractère absolument irréductible à valeurs dans E du produit direct $G \times G'$. Nous disons que χ et χ' sont E-*opposés* si $\chi \otimes \chi'$ est rationnel sur E. Comme $\bar{\varepsilon}_E(\chi \otimes \chi') = \bar{\varepsilon}_E(\chi).\bar{\varepsilon}_E(\chi')$, cela revient à dire que les classes de χ et χ' dans E sont opposées.

Soit χ un caractère absolument irréductible de G à valeurs dans E. Soit m un entier strictement positif et soit G′ le produit direct de m copies de G. Soit χ' le caractère de la représentation obtenue par produit tensoriel de m représentations de caractère χ. Il est clair que χ' peut être considéré

comme un caractère absolument irréductible de G′ à valeurs dans E et que $\bar{\varepsilon}_E(\chi') = (\bar{\varepsilon}_E(\chi))^m$. En particulier, si $\bar{\varepsilon}_E(\chi)$ est d'ordre $m+1$, χ et χ' sont E-opposés. On en déduit que, pour tout caractère absolument irréductible χ de G, à valeurs dans E, il existe un groupe fini G′ et un caractère absolument irréductible χ' de G′ à valeurs dans E tels que χ et χ' sont E-opposés.

PROPOSITION 3.1. — *Soit χ un caractère absolument irréductible de* G *à valeurs dans* E. *Soit* H *un sous-groupe de* G *et soit ξ un caractère absolument irréductible de* H *à valeurs dans* E *tel que* $(\mathrm{Res}_H(\chi), \xi) = n \neq 0$. *Alors, pour tout nombre premier p ne divisant pas n, les p-composantes de $\bar{\varepsilon}_E(\chi)$ et de $\bar{\varepsilon}_E(\xi)$ sont égales.*

Démonstration. — Il est clair que l'on peut construire une extension finie E′ de E de degré premier à p sur laquelle $\bar{\varepsilon}_{E'}(\chi)$ et $\bar{\varepsilon}_{E'}(\xi)$ sont tous deux d'ordre une puissance de p. La p-composante de $\bar{\varepsilon}_E(\chi)$ [resp. $\bar{\varepsilon}_E(\xi)$] est entièrement déterminée par $\bar{\varepsilon}_{E'}(\chi)$ [resp. $\bar{\varepsilon}_{E'}(\xi)$]. Il suffit donc de démontrer la proposition lorsque les ordres de $\bar{\varepsilon}_E(\chi)$ et de $\bar{\varepsilon}_E(\xi)$ sont des puissances de p.

Soit χ' un caractère absolument irréductible à valeurs dans E d'un groupe fini G′ tel que χ et χ' soient E-opposés. Le caractère $\chi \otimes \chi'$ de $G \times G'$ est rationnel sur E donc aussi sa restriction à $H \times G'$ qui n'est autre que $\mathrm{Res}_H(\chi) \otimes \chi'$. Le caractère $\xi \otimes \chi'$ est un caractère absolument irréductible de $H \times G'$ à valeurs dans E et on a

$$(\mathrm{Res}_H(\chi) \otimes \chi', \xi \otimes \chi') = (\mathrm{Res}_H(\chi), \xi).(\chi', \chi') = n \times 1 = n.$$

Comme $\xi \otimes \chi'$ est à valeurs dans E, on en déduit que $n.\xi \otimes \chi'$ est aussi rationnel sur E. Comme $\bar{\varepsilon}_E(\xi \otimes \chi') = \bar{\varepsilon}_E(\xi).\bar{\varepsilon}_E(\chi')$, on voit que, si les ordres de $\bar{\varepsilon}_E(\xi)$ et $\bar{\varepsilon}_E(\chi')$ sont des puissances de p, il en est de même de l'ordre de $\bar{\varepsilon}_E(\xi \otimes \chi')$. Si n est premier à p, on en déduit que $\xi \otimes \chi'$ est aussi rationnel sur E, donc que ξ et χ' sont E-opposés. Par conséquent, $\bar{\varepsilon}_E(\xi) = \bar{\varepsilon}_E(\chi)$. C. Q. F. D.

Remarque. — Ce résultat avait déjà été obtenu par Witt (*cf.* [13], Satz 8). Il admet comme corollaire le résultat suivant déjà obtenu par Yamada (*cf.* [16], th. 1) :

COROLLAIRE. — *Soit χ un caractère absolument irréductible de* G *à valeurs dans* E. *Soit* H *un sous-groupe de* G *et soit ξ un caractère absolument irréductible de* H *à valeurs dans* E *tel que χ soit induit par ξ. Alors,* $\bar{\varepsilon}_E(\chi) = \bar{\varepsilon}_E(\xi)$.

En effet, on a $(\mathrm{Res}_{\mathrm{H}}(\chi), \xi) = (\chi, \xi^*) = 1$, et, pour tout nombre premier p les p-composantes de $\bar{\varepsilon}_{\mathrm{E}}(\chi)$ et $\bar{\varepsilon}_{\mathrm{E}}(\xi)$ sont les mêmes.

3.2. Caractère induit par un caractère rationnel sur E. — Soit χ un caractère absolument irréductible de G à valeurs dans E. Soit A un sous-groupe invariant de G et soit ξ un caractère absolument irréductible de A tel que χ soit induit par ξ.

3.2.1. Soit X l'espace des fonctions sur A à valeurs dans $\mathrm{E}(\xi)$. Le groupe G opère sur X par

$$\forall\, \eta \in \mathrm{X}, \quad \forall\, g \in \mathrm{G}, \quad \forall\, h \in \mathrm{A} : \quad \eta_g(h) = \eta(ghg^{-1}).$$

Avec ces notations, pour tout h dans G, on a alors

$$\chi(h) = \begin{cases} \sum_{g \in \mathrm{G/A}} \xi_g(h) & \text{si } h \in \mathrm{A}; \\ 0 & \text{si } h \notin \mathrm{A}. \end{cases}$$

Soit n l'exposant de G. Le corps $\mathrm{E}(\xi)$ est contenu dans le corps des racines $n^{\text{ièmes}}$ de l'unité sur E; l'extension $\mathrm{E}(\xi)/\mathrm{E}$ est donc cyclotomique. Soit J son groupe de Galois. Le groupe J opère sur X par

$$\forall\, \eta \in \mathrm{X}, \quad \forall\, \sigma \in \mathrm{J}, \quad \forall\, h \in \mathrm{A} : \quad (\sigma.\eta)(h) = \sigma(\eta(h)).$$

Soit G_ξ l'ensemble des éléments g de G tels que ξ_g et ξ sont conjugués sur E; c'est un sous-groupe de G contenant A. Pour tout g dans G_ξ, il existe un élément σ_g de J et un seul tel que $\xi_g = \sigma_g.\xi$. Soit ψ l'application de G_ξ dans J qui, à g, fait correspondre σ_g. On vérifie immédiatement que c'est un homomorphisme. Pour tout σ dans J, il est clair que le caractère de G induit par $\sigma.\xi$ est χ. On a donc $(\mathrm{Res}_{\mathrm{A}}(\chi), \sigma.\xi) = 1$. Comme la décomposition de $\mathrm{Res}_{\mathrm{A}}(\chi)$ en somme de caractères absolument irréductibles est de la forme $\mathrm{Res}_{\mathrm{A}}(\chi) = \sum_{g \in \mathrm{G/A}} \xi_g$, on en déduit qu'il existe un élément g de G tel que $\sigma.\xi = \xi_g$. Donc $g \in \mathrm{G}_\xi$ et $\psi(g) = \sigma$. Par conséquent, ψ est un épimorphisme.

Comme, pour tout g dans A, $\xi_g = \xi$, le noyau de ψ contient A. S'il existait un élément g de G_ξ non contenu dans A tel que $\xi_g = \xi$, le caractère induit ne serait pas irréductible. On a donc la suite exacte

$$1 \to \mathrm{A} \to \mathrm{G}_\xi \xrightarrow{\psi} \mathrm{J} \to 1.$$

Soit s une section de J dans G_ξ et soit ε l'application de $\mathrm{J} \times \mathrm{J}$ dans A définie par

$$\forall\, \sigma, \tau \in \mathrm{J} : \quad s_\sigma s_\tau = \varepsilon_{\sigma,\tau} s_{\sigma\tau}.$$

Supposons ξ rationnel sur $E(\xi)$ et soit q le degré de ξ. Le facteur simple $A_E(\xi)$ de l'algèbre $E[A]$ associé à ξ est isomorphe à $M_q(E(\xi))$. Soit β un E-épimorphisme associé à ξ de $E[A]$ sur $M_q(E(\xi))$.

Pour tout λ dans $M_q(E(\xi))$, on note $\det(\lambda)$ son déterminant et $\mathrm{tr}(\lambda)$ sa trace. Ce sont des éléments de $E(\xi)$.

THÉORÈME 3. — *Si ξ est rationnel sur $E(\xi)$, alors $(\bar{\varepsilon}_E(\chi))^q$ est un élément de $H^2_\mu(E(\xi)/E)$. L'application ε' de $J\times J$ dans $E(\xi)$ définie par*

$$\varepsilon'_{\sigma,\tau} = \det(\beta(\varepsilon_{\sigma,\tau})), \qquad \textit{pour} \quad \sigma, \tau \in J,$$

est un 2-cocycle de J à valeurs dans $\mu(E(\xi))$ dont la classe, dans $\mathrm{Br}(E)$, est $(\bar{\varepsilon}_E(\chi))^q$.

Démonstration. — Le corollaire de la proposition 3.1 ramène la démonstration au cas où $G = G_\xi$, ce que nous supposerons dans la suite.

Posons $E' = E(\xi)$. Le groupe G opère sur $E[A]$ par les automorphismes intérieurs :

$$\forall g \in G, \quad \forall a \in E[A] : \quad g(a) = gag^{-1} = a^{g^{-1}}.$$

Pour tout g dans G, ξ_g et ξ sont conjugués sur E. Par conséquent, le facteur simple de l'algèbre $E[A]$ associé à ξ_g n'est autre que $A_E(\xi)$. On en déduit que, pour tout a dans $E[A]$, $\beta(a)$ est nul si et seulement si $\beta(g(a))$ l'est. Le groupe G opère donc aussi sur $M_q(E')$: à tout élément g de G on peut associer un E-automorphisme φ_g de $M_q(E')$ défini par

$$\forall a \in E[A] : \varphi_g(\beta(a)) = \beta(gag^{-1}).$$

Soit d l'ordre de J. Considérons l'algèbre de rang d sur $M_q(E')$ définie par

$$U = \sum_{\sigma \in J} M_q(E')\, u_\sigma,$$

la multiplication étant définie par

$$\begin{cases} u_\sigma a = \varphi_{s_\sigma}(a)\, u_\sigma, \\ u_\sigma u_\tau = \beta(\varepsilon_{\sigma,\tau})\, u_{\sigma\tau}. \end{cases}$$

L'application α de $E[G]$ dans U définie par

$$\alpha(as_\sigma) = \beta(a)\, u_\sigma$$

est un épimorphisme d'algèbres. Il est clair que U est isomorphe au facteur simple de $E[G]$ associé à χ. C'est donc une algèbre simple centrale, de centre E, et nous nous proposons de l'écrire sous la forme d'un produit croisé ordinaire.

3.2.2. Pour tout g dans G, l'application $\beta.g$ est un E-épimorphisme de E[A] sur $M_q(E')$. Comme, pour tout h dans A,

$$\mathrm{tr}(\beta(ghg^{-1})) = \xi(ghg^{-1}) = \xi_g(h),$$

on voit que $\beta.g$ est associé à ξ_g.

Le groupe J opère de façon naturelle sur $M_q(E')$:

$\sigma((a_{i,j})) = (\sigma(a_{i,j}))$, pour toute matrice $(a_{i,j})$ à coefficients dans E'. Pour tout σ dans J, il est clair que l'application $\sigma.\beta$ est un E-épimorphisme de E[A] sur $M_q(E')$. Comme, pour tout h dans A,

$$\mathrm{tr}(\sigma.\beta(h)) = \sigma(\mathrm{tr}(\beta(h))) = \sigma.\xi(h),$$

on voit que $\sigma.\beta$ est associé à $\sigma.\xi$.

Pour tout σ dans J, l'application $\sigma^{-1}.\beta.s_\sigma$ est donc un E-épimorphisme de E[A] sur $M_q(E')$ dont le caractère associé est ξ. On en déduit que $\sigma^{-1}.\varphi_{s_\sigma}$ est un E'-automorphisme de $M_q(E')$. Il existe donc une matrice m'_σ de $M_q(E')$ telle que, pour tout a dans $M_q(E')$, $\sigma^{-1}.\varphi_{s_\sigma}(a) = m'^{-1}_\sigma a m'_\sigma$; ou encore, en posant $\sigma(m'_\sigma) = m_\sigma$, il existe une matrice m_σ telle que

$$\forall\, a \in M_q(E') : \quad \varphi_{s_\sigma}(a) = m_\sigma^{-1}\sigma(a)\, m_\sigma.$$

Posons $v_\sigma = m_\sigma u_\sigma$.

Pour tout a dans $M_q(E')$, on a

$$v_\sigma a = m_\sigma u_\sigma a = m_\sigma \varphi_{s_\sigma}(a)\, u_\sigma = \sigma(a)\, v_\sigma.$$

Pour σ, τ dans J,

$$v_\sigma v_\tau = m_\sigma u_\sigma m_\tau u_\tau = m_\sigma \varphi_{s_\sigma}(m_\tau)\, u_\sigma u_\tau = m_\sigma m_\sigma^{-1}\sigma(m_\tau)\, m_\sigma \beta(\varepsilon_{\sigma,\tau})\, u_{\sigma\tau} = \tilde{\varepsilon}_{\sigma,\tau}\, v_{\sigma\tau},$$

en posant

$$\tilde{\varepsilon}_{\sigma,\tau} = \sigma(m_\tau)\, m_\sigma \beta(\varepsilon_{\sigma,\tau})\, m_{\sigma\tau}^{-1}. \tag{9}$$

Lemme 1. — *Pour tout couple σ, τ d'éléments de* J, $\tilde{\varepsilon}_{\sigma,\tau}$ *est un élément de* E' [E' *étant identifié au centre de* $M_q(E')$].

Démonstration du lemme. — Il suffit de montrer que $\forall\, \lambda \in M_q(E')$, $\tilde{\varepsilon}_{\sigma,\tau}\lambda = \lambda\tilde{\varepsilon}_{\sigma,\tau}$. Pour tout μ dans $M_q(E')$ et pour tout h dans A,

$$\varphi_h(\mu) = \beta(h)\,\mu\beta(h)^{-1}.$$

L'égalité $\varphi_{s_\sigma}\varphi_{s_\tau} = \varphi_{\varepsilon_{\sigma,\tau}}\varphi_{s_{\sigma\tau}}$ appliquée à μ s'écrit donc :

$$m_\sigma^{-1}\sigma(m_\tau^{-1}\tau(\mu)\, m_\tau)\, m_\sigma = \beta(\varepsilon_{\sigma,\tau})\, m_{\sigma\tau}^{-1}\sigma\tau(\mu)\, m_{\sigma\tau}\beta(\varepsilon_{\sigma,\tau})^{-1}$$

ou

$$m_\sigma^{-1}\sigma(m_\tau^{-1})\,\sigma\tau(\mu)\,\sigma(m_\tau)\,m_\sigma=\beta(\varepsilon_{\sigma,\tau})\,m_{\sigma\tau}^{-1}\sigma\tau(\mu)\,m_{\sigma\tau}\beta(\varepsilon_{\sigma,\tau})^{-1},$$

ou encore

$$\sigma\tau(\mu)\,\tilde{\varepsilon}_{\sigma,\tau}=\tilde{\varepsilon}_{\sigma,\tau}\sigma\tau(\mu)\,;$$

d'où le résultat, en choisissant $\mu=(\sigma\tau)^{-1}(\lambda)$. C. Q. F. D.

3.2.3. *Fin de la démonstration du théorème* 3. — Il résulte de l'associativité du produit des ρ_σ que $\tilde{\varepsilon}$ est un 2-cocycle de J à valeurs dans E′. Soit $\bar{\tilde{\varepsilon}}$ sa classe dans Br(E). Soit V le sous-ensemble de U défini par $V=\sum_{\sigma\in J}E'\rho_\sigma$. Il est clair que c'est une sous-algèbre de U et on voit que c'est une algèbre simple centrale sur E de rang d^2 sur E dont la classe est $\bar{\tilde{\varepsilon}}$. L'algèbre $M_q(E)$ est contenue dans U et est de rang q^2 sur E. Les algèbres V et $M_q(E)$ sont linéairement disjointes sur E et U est de rang q^2d^2 sur E. On en déduit que U est isomorphe à $M_q(E)\otimes_E V$. On a donc établi le résultat suivant :

PROPOSITION 3.2. — *On a* $\bar{\varepsilon}_E(\chi)=\bar{\tilde{\varepsilon}}$.

Soit γ l'application de J dans E′ définie par $\gamma_\sigma=\det(m_\sigma)$, pour tout σ dans J. D'après la formule (9), comme $\det(\sigma(m_\tau))=\sigma(\det(m_\tau))$, on a

$$\tilde{\varepsilon}'_{\sigma,\tau}=\det(\tilde{\varepsilon}_{\sigma,\tau})=\sigma(\gamma_\tau)\,\gamma_\sigma\det(\beta(\varepsilon_{\sigma,\tau}))\,\gamma_{\sigma\tau}^{-1}\,;$$

ou encore

$$\tilde{\varepsilon}'_{\sigma,\tau}=\det(\beta(\varepsilon_{\sigma,\tau}))\,.\,\sigma(\gamma_\tau)\,\gamma_\sigma\gamma_{\sigma\tau}^{-1}.$$

On voit donc que, si ε' est défini par $\varepsilon'_{\sigma,\tau}=\det(\beta(\varepsilon_{\sigma,\tau}))$, pour $\sigma,\tau\in J$, alors $\tilde{\varepsilon}'$ est équivalent à ε'. Comme $\beta(\varepsilon_{\sigma,\tau})$ est une matrice d'ordre fini, on voit que ε' est à valeurs dans $\mu(E')$, ce qui achève la démonstration du théorème. C. Q. F. D.

3.2.4. *Remarques.*

(*a*) La proposition 3.2 permet, en un certain sens, de déterminer complètement $\bar{\varepsilon}_E(\chi)$, même lorsque $\bar{\varepsilon}_{E(\xi)}(\xi)\neq 1$. En effet, soit Γ un groupe fini admettant un caractère absolument irréductible φ à valeurs dans E tel que $\bar{\varepsilon}_{E(\xi)}(\varphi)=(\bar{\varepsilon}_{E(\xi)}(\varphi))^{-1}$ [un tel couple (Γ,φ) existe toujours : on peut prendre, par exemple, pour φ un caractère E-opposé à χ; dans le cas où E est un corps local, nous verrons plus loin (*cf.* prop. 6.8 et prop. 8.1) comment on peut construire un groupe Γ très simple admettant un tel caractère]. Le caractère $\chi\otimes\varphi$ est un caractère absolument irréductible

à valeurs dans E de $G \times \Gamma$. Il est induit par le caractère $\xi \otimes \varphi$ de $A \times \Gamma$ qui est, par construction, rationnel sur $E(\xi) = E(\xi \otimes \varphi)$ et on peut appliquer la proposition 3.2. On a alors

$$\bar{\varepsilon}_E(\chi) = \bar{\varepsilon}_E(\chi \otimes \varphi) \cdot (\bar{\varepsilon}_E(\varphi))^{-1}.$$

(*b*) Soit q le degré de ξ et soit d le degré de l'extension $E(\xi)/E$. Soit E_1 une extension de E, de degré $m_E(\xi)$, telle que ξ soit rationnel sur $E_1(\xi)$. La proposition 3.2 détermine la restriction de $\bar{\varepsilon}_E(\chi)$ à E_1. Le corollaire à la proposition 3.1 détermine la restriction de $\bar{\varepsilon}_E(\chi)$ à $E(\xi)$. Supposons $m_E(\xi)$ et d premiers entre eux. Cela signifie que les extensions E_1/E et $E(\xi)/E$ sont de degrés premiers entre eux, et l'élément $\bar{\varepsilon}_E(\chi)$ est entièrement déterminé par ces restrictions.

C'est en particulier le cas lorsque $(q, d) = 1$, parce que $m_E(\xi)$ divise q. On voit qu'alors le corollaire à la proposition 3.1 et le théorème 3 déterminent entièrement $\bar{\varepsilon}_E(\chi)$ car le théorème 3 détermine la puissance $q^{\text{ième}}$ de la restriction à E_1 de $\bar{\varepsilon}_E(\chi)$ qui est un élément d'ordre divisant d donc premier à q.

Lorsque $q = 1$, ξ est rationnel sur $E(\xi)$ et la formule du théorème 3 s'écrit simplement

$$\varepsilon'_{\sigma,\tau} = \xi(\varepsilon_{\sigma,\tau}). \tag{10}$$

On retrouve ainsi un résultat obtenu par Yamada ([16], th. 2).

3.3. Représentations E-métabéliennes. — Soit χ un caractère absolument irréductible de G à valeurs dans E. Nous disons que χ est E-*métabélien* s'il est induit par un caractère ξ de degré 1 d'un sous-groupe invariant A de G et si le degré de l'extension $E(\xi)/E$ est égal à l'indice de A dans G.

On a vu que le groupe G contient un sous-groupe G_ξ contenant A tel que le quotient G_ξ/A est isomorphe au groupe de Galois J de l'extension $E(\xi)/E$. Dans la définition d'un caractère E-métabélien, la deuxième condition revient donc à dire que $G_\xi = G$. Le groupe A est donc invariant dans G et on a la suite exacte

$$1 \to A \to G \to J \to 1.$$

Soit ε l'élément de $H^2(J, A)$ correspondant. Il est clair que le théorème 3 s'énonce, dans ce cas :

Proposition 3.3. — *L'élément* $\bar{\varepsilon}_E(\chi)$ *est la classe, dans* $\mathrm{Br}(E)$, *de l'image par* ξ *de* ε.

Par abus de langage, on écrit

$$\bar{\varepsilon}_E(\chi) = \xi(\varepsilon). \tag{10'}$$

Nous disons qu'un groupe fini G est E-*métabélien* s'il admet un caractère absolument irréductible et fidèle χ, à valeurs dans E, qui est E-métabélien. Il est clair que le noyau de χ est le même que celui de ξ et que, par conséquent, G admet un sous-groupe cyclique invariant A tel que le quotient G/A est un groupe abélien isomorphe à un sous-groupe du groupe des automorphismes de A.

Nous disons qu'un groupe fini G a *la propriété* (W) s'il existe une suite

$$\{1\} \subset G_0 \subset G_1 \subset \ldots \subset G_k = G$$

de sous-groupes invariants de G tels que G_0 est abélien et que, pour $i = 1, 2, \ldots, k$, G_i/G_{i-1} est cyclique. En particulier, on voit qu'un groupe hyperrésoluble a la propriété (W).

Si un caractère χ absolument irréductible d'un groupe fini G est à valeurs dans E et est induit par un caractère ξ E-métabélien d'un sous-groupe de G, il résulte du corollaire à la proposition 3.1 que $\bar{\varepsilon}_E(\chi) = \bar{\varepsilon}_E(\xi)$. D'où l'intérêt de la proposition suivante :

PROPOSITION 3.4. — *Soit* G *un groupe fini ayant la propriété* W *et soit* χ *un caractère absolument irréductible de* G *à valeurs dans* E. *Alors* χ *est induit par un caractère* E-*métabélien d'un sous-groupe de* G.

Démonstration. — Nous allons d'abord donner deux définitions et établir trois lemmes.

Nous disons qu'un caractère d'un groupe fini G, à valeurs dans E, est E-*primitif* s'il n'existe pas de sous-groupe H de G, distinct de G, tel qu'il soit induit par un caractère de H à valeurs dans E.

Nous disons qu'un caractère χ de G est E-*irréductible* si c'est la trace réduite d'une représentation de G par des matrices à coefficients dans E qui est irréductible. Cela revient à dire qu'il existe un caractère ξ absolument irréductible de G tel que, si J désigne le groupe de Galois de l'extension $E(\varepsilon)/E$, on ait $\chi = \sum_{\sigma \in J} \sigma.\xi$.

LEMME 1. — *Soit* χ *un caractère à valeurs dans* E, *absolument irréductible et* E-*primitif d'un groupe fini* G. *Soit* A *un sous-groupe invariant de* G. *Alors la restriction de* χ *à* A *est un multiple entier d'un caractère* E-*irréductible.*

Démonstration. — Supposons d'abord χ rationnel sur E. Soit M un E[G]-module qui définit une représentation de G dont le caractère est χ. Soit $M = \sum M_i$ la décomposition de M en somme directe de E[A]-modules isotypiques non nuls. Comme χ est absolument irréductible, M est un E[G]-module simple et G opère transitivement sur les M_i. Soit M_1 l'un d'entre eux et soit H le sous-groupe d'isotropie de M_1. Il est clair que M_1 est un E[H]-module et que M est induit par M_1. Si ξ désigne le caractère de la représentation de H définie par M_1, on en déduit que ξ est un caractère à valeurs dans E et que χ est induit par ξ. Comme χ est E-primitif, on a $H = G$ et $M = M_1$. Comme M_1 est un E[A]-module isotypique, le caractère de la représentation qu'il définit, qui n'est autre que $\mathrm{Res}_A(\chi)$, est multiple d'un caractère E-irréductible.

Si χ n'est pas rationnel sur E, soit G' un groupe fini admettant un caractère absolument irréductible χ' à valeurs dans E tel que χ et χ' soient E-opposés. Le caractère $\chi \otimes \chi'$ est un caractère absolument irréductible de $G \times G'$ qui est rationnel sur E. Il est clair que l'on peut choisir G' et χ' pour que χ' soit E-primitif et qu'alors $\chi \otimes \chi'$ l'est aussi. Si A est un sous-groupe invariant de G, $A \times G'$ est un sous-groupe invariant de $G \times G'$ et, par conséquent, $\mathrm{Res}_{A \times G'}(\chi \otimes \chi')$ est multiple d'un caractère E-irréductible. Supposons que $\mathrm{Res}_A(\chi)$ ne soit pas multiple d'un caractère E-irréductible. On pourrait écrire $\mathrm{Res}_A(\chi)$ sous la forme $\sum c_i \eta_i$ où les η_i seraient des caractères E-irréductibles distincts et où deux entiers c_i au moins seraient différents de o. On aurait

$$\mathrm{Res}_{A \times G'}(\chi \otimes \chi') = (\mathrm{Res}_A(\chi)) \otimes \chi' = \sum c_i \eta_i \otimes \chi'$$

et $\mathrm{Res}_{A \times G'}(\chi \otimes \chi')$ ne serait pas multiple d'un caractère E-irréductible. Donc, $\mathrm{Res}_A(\chi)$ est multiple d'un caractère E-irréductible.

C. Q. F. D.

LEMME 2. — *Soit* G *un groupe admettant un caractère* χ *à valeurs dans* E, *absolument irréductible,* E*-primitif et fidèle. Alors, tout sous-groupe abélien invariant de* G *est cyclique.*

Démonstration. — Soit $\overline{E}$ une clôture algébrique de E et soit ρ une représentation de G par des matrices à coefficients dans $\overline{E}$, dont le caractère est χ. Soit A un sous-groupe de G. Comme χ est fidèle, le noyau de ρ est réduit à l'élément neutre, donc aussi celui de la restriction de ρ à A. Si A est invariant, comme χ est E-primitif, il résulte du lemme 1 que la restriction de ρ à A est somme directe de représentations isotypiques qui sont conju-

guées sur E; elles ont donc le même noyau, et c'est encore le même que celui de la restriction de ρ à A qui est l'élément neutre. Donc, A admet une représentation absolument irréductible et fidèle. Si A est abélien, ceci entraîne que A est cyclique. C. Q. F. D.

LEMME 3. — *Soit* G *un groupe hyperrésoluble tel que tout sous-groupe abélien invariant est cyclique. Alors, il existe un sous-groupe cyclique invariant* A *de* G *tel que le quotient* G/A *est abélien et canoniquement isomorphe à un sous-groupe du groupe des automorphismes de* A.

Démonstration. — Soit A un sous-groupe abélien invariant de G qui est maximal. Par hypothèse, A est cyclique. On en déduit que le groupe J_A des automorphismes de A est abélien. Pour tout σ dans G, l'application $a \mapsto \sigma a \sigma^{-1}$ définit un automorphisme $\Phi(\sigma)$ de A. On voit immédiatement que Φ est un homomorphisme de G dans J_A, dont le noyau N contient A. Le groupe N est invariant dans G et si N était différent de A, le groupe N/A serait un sous-groupe invariant non trivial du groupe hyperrésoluble G/A. Il existerait donc un sous-groupe cyclique invariant $\overline{T}$ de G/A, non trivial, qui serait contenu dans N/A. Le relèvement T de $\overline{T}$ dans G serait alors un sous-groupe abélien invariant de G contenant strictement A, contrairement à l'hypothèse de maximalité de A. Donc, N = A et G/A est canoniquement isomorphe à un sous-groupe de J_A.

C. Q. F. D.

Fin de la démonstration de la proposition 3.4. — Comme un sous-groupe, ou un groupe quotient d'un groupe ayant la propriété (W) a encore la propriété (W), on peut supposer que χ est E-primitif et fidèle. Il résulte du lemme 2 que G satisfait les hypothèses du lemme 3. Soit A un sous-groupe de G qui a les propriétés énoncées dans le lemme 3. Soit ξ un caractère absolument irréductible de A intervenant dans la décomposition de la restriction de χ à A, et soit J le groupe de Galois de l'extension $E(\xi)/E$. Il résulte du lemme 1 qu'il existe un entier strictement positif c tel que $\mathrm{Res}_A(\chi) = c\sum_{\sigma \in J} \sigma.\xi$. On a vu, dans la démonstration du lemme 2, que ξ est le caractère d'une représentation fidèle; donc, ξ est fidèle. Comme G/A est isomorphe à un sous-groupe du groupe des automorphismes de A, on en déduit que le caractère χ' de G induit par ξ est absolument irréductible. Or, on a $(\chi, \chi') = (\mathrm{Res}_A(\chi), \xi) = c$; par conséquent, $c = 1$ et $\chi = \chi'$. Comme $\mathrm{Res}_A(\chi) = \sum_{\sigma \in G/A} \sigma.\xi$, on voit que les groupes G/A et J s'identifient. Le caractère χ est donc E-métabélien. C. Q. F. D.

Remarque. — La proposition 3.4 est l'analogue, en termes de caractères, d'un résultat de Witt (*cf.* [13], Satz 1) énoncé en termes de représentations réalisables par des matrices à coefficients dans un corps gauche.

4. L'algèbre d'un groupe nilpotent.

Soit E un corps de caractéristique o et soit $\overline{E}$ une clôture algébrique de E. Soit G un groupe fini nilpotent. On sait que G est le produit direct de ses p-sous-groupes de Sylow. La structure de l'algèbre E[G] peut donc s'obtenir aisément à partir de celles des p-sous-groupes de Sylow de G.

4.1. Le cas « général ».

Proposition 4.1. — *Soit p un nombre premier et soit* G *un p-groupe. Si $p = 2$, on suppose que* E *contient les racines quatrièmes de l'unité. L'algèbre* E[G] *est décomposée.*

Démonstration. — Soit χ un caractère absolument irréductible de G. Posons $E_1 = E(\chi)$. Comme un p-groupe est hyperrésoluble, G a la propriété (W). D'après la proposition 3.4, le caractère χ est induit par un caractère η E_1-métabélien d'un sous-groupe G_1 de G. D'après le corollaire à la proposition 3.1, on a $\bar{\varepsilon}_{E_1}(\chi) = \bar{\varepsilon}_{E_1}(\eta)$.

Si η est induit par un caractère ξ de degré 1 d'un sous-groupe invariant A de G_1, on voit qu'il existe un entier positif a tel que $E_1(\xi)$ soit contenu dans $E_1(\sqrt[p^a]{1})$. Il résulte de la proposition 3.3 que $\bar{\varepsilon}_{E_1}(\eta)$ est l'image dans $\mathrm{Br}(E_1)$ d'un élément de $H^2(E_1(\sqrt[p^a]{1})/E_1, \mu'')$. D'après la proposition 1.4, ce dernier groupe est réduit à l'élément neutre. Par conséquent, η et χ sont rationnels sur E_1. C. Q. F. D.

Remarque. — Ce résultat est classique (*cf.* [7] et [12], cor. au th. 5).

4.2. Le cas $p = 2$. — Pour tout entier positif n, désignons par I_n un groupe cyclique d'ordre 2^n. Supposons $n \geq 2$ et soit $J = \{1, s\}$ un groupe cyclique d'ordre 2. Soit G une extension de J par I_n.

— On pose $G = D_n$ si, pour tout a dans I_n, on a $s(a) = a^{-1}$ et si G s'identifie au produit semi-direct de J par I_n (le groupe D_n est isomorphe au groupe diédral d'ordre 2^{n+1}).

— On pose $G = H_n$ si, pour tout a dans I_n, on a $s(a) = a^{-1}$ et s'il n'existe pas de relèvement de s dans G qui soit d'ordre 2 (le groupe H_n est isomorphe au groupe des quaternions généralisés d'ordre 2^{n+1}).

— Si $n \geq 3$, on pose $G = M_n$ si, pour tout a dans I_n, on a $s(a) = a^{1+2^{n-1}}$ et si G s'identifie au produit semi-direct de J par I_n.

Les groupes I_n, D_n, H_n, M_n sont définis à un isomorphisme près.

Soit G un 2-groupe et soit χ un caractère absolument irréductible de G. D'après la proposition 3.4, il existe un sous-groupe H de G et un caractère η de H qui est $\mathbf{Q}(\chi)$-métabélien tels que χ soit induit par η. Pour $P = I, D, H, M$, nous disons que χ est de type P_n si l'on peut choisir H et η de telle sorte que le quotient de H par le noyau de η soit isomorphe au groupe P_n.

Soit $\overline{\mathbf{Q}}$ une clôture algébrique de $\mathbf{Q}$ et soit ρ un plongement de $\overline{\mathbf{Q}}$ dans $\overline{E}$. Pour tout entier n positif, soit ν une racine $(2^n)^{\text{ième}}$ de l'unité contenue dans $\overline{\mathbf{Q}}$. Posons $\mathbf{Q}_{(n)} = \mathbf{Q}(\nu)$ et désignons par $\mathbf{Q}'_{(n)}$ (resp. $\mathbf{Q}''_{(n)}$) le corps fixe de l'automorphisme σ de $\mathbf{Q}_{(n)}$ défini par $\sigma(\nu) = \nu^{-1}$ [resp. $\sigma(\nu) = \nu^{1+2^{n-1}}$]. Désignons par $E_{(n)}$ (resp. $E'_{(n)}$, $E''_{(n)}$) l'intersection de $\rho(\mathbf{Q}_{(n)})$ [resp. $\rho(\mathbf{Q}'_{(n)})$, $\rho(\mathbf{Q}''_{(n)})$] avec $\overline{E}$. Pour $i = 0, 1, 2$, on a $E = E_{(0)} = E_{(1)} = E'_{(i)} = E''_{(i)}$. S'il existe un entier n tel que le corps $\mathbf{H}$ des quaternions usuels sur $\mathbf{Q}$ soit décomposé sur $E'_{(n)}$, il est clair que $\mathbf{H}$ est aussi décomposé sur $E'_{(n')}$, pour tout entier n' supérieur à n. Nous désignons par $\mathfrak{r}(E)$ le plus petit entier supérieur ou égal à 2 satisfaisant à cette propriété. Si, pour tout entier positif n, $\mathbf{H}$ n'est pas décomposé sur $E'_{(n)}$, nous posons $\mathfrak{r}(E) = +\infty$.

Exemples :

(*a*) On a $\mathfrak{r}(\mathbf{Q}(\sqrt{-1})) = 2$.

(*b*) On a $\mathfrak{r}(E) = +\infty$, si E est un corps de nombres réels (en effet, pour tout entier n positif, $E'_{(n)}$ peut être plongé dans $\mathbf{R}$. Comme $\mathbf{H} \otimes_{\mathbf{Q}} \mathbf{R}$ est le corps des quaternions sur $\mathbf{R}$, $\mathbf{H} \otimes_{\mathbf{Q}} E'_{(n)}$ ne peut pas être une algèbre de matrices).

(*c*) Soit E une extension finie de $\mathbf{Q}_2$. On a $\mathfrak{r}(E) = 3$ si le degré de l'extension $E/\mathbf{Q}_2$ est impair et $\mathfrak{r}(E) = 2$, sinon [en effet, -1 n'est pas norme dans l'extension $\mathbf{Q}_2(\sqrt{-1})/\mathbf{Q}_2$. On en déduit que la classe de $\mathbf{H} \otimes_{\mathbf{Q}} \mathbf{Q}_2$ est l'élément de $\mathrm{Br}(\mathbf{Q}_2)$ dont l'invariant est égal à $1/2$. L'invariant de sa restriction à E est donc 0 si et seulement si l'extension $E/\mathbf{Q}_2$ est de degré pair. Comme, pour $n \geq 3$, l'extension $\mathbf{Q}_2(\nu + \nu^{-1})/\mathbf{Q}_2$ est de degré pair, l'invariant de l'élément correspondant de $\mathrm{Br}(\mathbf{Q}_2(\nu + \nu^{-1}))$ est nul. *A fortiori*, celui de $\mathrm{Br}(E(\nu + \nu^{-1}))$ l'est aussi].

(*d*) Pour $p \neq 2$, on a $\mathfrak{r}(\mathbf{Q}_p) = 2$ [en effet, comme -1 est une unité et comme l'extension $\mathbf{Q}_p(\sqrt{-1})/\mathbf{Q}_p$ est non ramifiée, -1 est norme dans l'extension].

PROPOSITION 4.2. — *Soit* G *un* 2*-groupe et soit* χ *un caractère absolument irréductible de* G. *On est dans l'un des cas suivants :*

(i) *il existe un entier* $n \geq 0$ (*resp.* $\geq 2, \geq 3$) *tel que* χ *est de type* I_n (*resp.* D_n, M_n); *on a alors* $E(\chi) = E_{(n)}$ (*resp.* $E'_{(n)}, E''_{(n)}$) *et* χ *est rationnel sur* $E(\chi)$;

(ii) *il existe un entier* $n \geq 2$ *tel que* χ *est de type* H_n; *on a alors :*

(*a*) *si* $n \geq \mathfrak{r}(E)$, χ *est rationnel sur* $E(\chi)$;

(*b*) *si* $n < \mathfrak{r}(E)$, $\bar{\varepsilon}_{E(\chi)}(\chi)$ *est la classe du corps des quaternions usuels sur* $E(\chi)$.

Démonstration. — Il est clair qu'il suffit de démontrer la proposition lorsque $E = \mathbf{Q}$. Le corollaire à la proposition 3.1 et la proposition 3.4 ramènent la démonstration au cas où χ est $\mathbf{Q}(\chi)$-métabélien. Quitte à passer au quotient, on peut supposer χ fidèle et le groupe G est alors $\mathbf{Q}(\chi)$-métabélien.

Le caractère χ est alors induit par un caractère ξ d'un sous-groupe cyclique invariant A de G. Posons $K = \mathbf{Q}(\chi)$, $L = \mathbf{Q}(\xi)$ et désignons par J le groupe de Galois de l'extension L/K. On a la suite exacte

$$1 \to A \to G \to J \to 1.$$

Soit 2^m l'ordre de A et soit a un générateur de A. Posons $\xi(a) = \nu$. L'élément ν est une racine primitive $(2^m)^{\text{ième}}$ de l'unité et $L = \mathbf{Q}(\nu)$.

Si $m = 0$ ou 1, on a $L = \mathbf{Q}(\nu) = \mathbf{Q}$, et par conséquent $K = L$ et $J = \{1\}$. On est dans le cas (i) avec $n = m$ et χ de type I_n.

Supposons $m \geq 2$. On voit que $\mu''(L)$ est le groupe cyclique engendré par ν et il est clair que ξ définit un isomorphisme de $H^2(J, A)$ sur $H^2(L/K, \mu'')$. Soit ε l'élément de $H^2(J, A)$ qui définit G. On a vu (*cf.* prop. 3.3) que $\bar{\varepsilon}_K(\chi)$ est l'image de ε dans $\mathrm{Br}(K)$. Comme $m \geq 2$, L contient $\sqrt{-1}$ et il résulte de la proposition 1.4 que

$$H^2(L/K, \mu'') = H^2(K(\sqrt{-1})/K, \mu''). \tag{11}$$

Il est clair qu'il existe un entier n vérifiant $1 \leq n \leq m$ tel que $K(\sqrt{-1}) = \mathbf{Q}_{(n)}$. Soit J' le groupe de Galois de l'extension $L/K(\sqrt{-1})$ et soit A' le sous-groupe de A d'ordre 2^n. Il est clair que J' est un sous-groupe de J d'indice 1 ou 2 suivant que $\sqrt{-1}$ appartient ou non à K. La restriction de ξ à A' est un isomorphisme de A' sur $\mu''(K(\sqrt{-1}))$. La formule (11) montre donc que :

— si $J = J'$, alors $\varepsilon = 1$;

— si $J \neq J'$, et si σ désigne un élément de J qui n'appartient pas à J', alors il existe un élément c de A' tel que ε admette un représentant dans les cocycles vérifiant $\varepsilon_{s,s'} = \varepsilon_{s,\sigma s'} = \varepsilon_{\sigma s,s'} = 1$ et $\varepsilon_{\sigma s,\sigma s'} = c$, $\forall\, s, s' \in J'$.

Il existe donc, dans les deux cas, un sous-groupe G' de G qui relève J et dont l'intersection avec A est réduite à A'; le groupe J' s'identifie à un sous-groupe de G'.

Comme l'image par ξ de A' est contenue dans $K(\sqrt{-1})$, le groupe J' opère trivialement sur A'. Donc le groupe J' est un sous-groupe invariant de G' et le groupe A'J' est un sous-groupe abélien de G'. Il est immédiat que le caractère φ de A'J' défini par

$$\varphi(at) = \xi(a), \quad \forall\, a \in A', \quad t \in J'.$$

est un caractère de degré 1 de A'J', à valeurs dans $K(\sqrt{-1})$, et que le caractère ψ de G' induit par φ est un caractère à valeurs dans K dont le noyau est J'. On vérifie sur les valeurs des caractères que χ est induit par ψ.

Posons $\overline{G} = G'/J'$ et $\overline{J} = J/J'$. On a la suite exacte

$$1 \to A' \to \overline{G} \to \overline{J} \to 1.$$

Il est clair que K est égal soit à $\mathbf{Q}_{(n)}$, soit à $\mathbf{Q}'_{(n)}$, soit à $\mathbf{Q}''_{(n)}$ avec $n \geqq 3$ (car $\mathbf{Q}''_{(2)} = \mathbf{Q}'_{(2)}$).

Si $K = \mathbf{Q}_{(n)}$, on a $J = J'$, donc $\overline{J} = 1$ et $\overline{G}$ est cyclique d'ordre 2^n. Le caractère χ est donc de type I_n et est évidemment rationnel sur $\mathbf{Q}(\chi)$.

Si $K = \mathbf{Q}'_{(n)}$, on a $\sigma(a) = a^{-1}$, pour tout a dans A'. Si $\varepsilon_{\sigma,\sigma} = 1$, on voit que le groupe $\overline{G}$ est isomorphe à D_n. Le caractère χ est donc de type D_n et est rationnel sur $\mathbf{Q}(\chi)$, puisque $\xi(\varepsilon) = 1$. Si $\varepsilon_{\sigma,\sigma} = c$, avec $c \in A' - \{1\}$, on voit que $\xi(c)$ doit appartenir à $\mu''(K)$ et doit donc être égal à -1. On en déduit que le groupe $\overline{G}$ est isomorphe à H_n, donc que χ est de type H_n, et que $\xi(\varepsilon)$ est la classe du corps des quaternions usuels sur $\mathbf{Q}(\chi)$.

Si $K = \mathbf{Q}''_{(n)}$, avec $n \geqq 3$, on a $\sigma(a) = a^{1+2^{n-1}}$. Pour la même raison que dans le cas précédent, on voit que $\xi(\varepsilon_{\sigma,\sigma})$ doit être égal à 1 ou à -1. Si ν_1 est une racine primitive huitième de l'unité [appartenant à $K(\sqrt{-1})$, puisque $n \geqq 3$], on voit que $\nu_1 \sigma(\nu_1) = -1$. On en déduit que l'on peut choisir le représentant de ε pour que $\varepsilon_{\sigma,\sigma} = 1$. Le groupe $\overline{G}$ est donc isomorphe à M_n et χ est de type M_n. Enfin, χ est rationnel sur $\mathbf{Q}(\chi)$ puisque $\xi(\varepsilon) = 1$. C. Q. F. D.

Remarque. — Si G est un p-groupe, avec p nombre premier différent de 2, la même démonstration montre que tout caractère absolument irréductible χ de G est induit par un caractère de degré 1, *à valeurs dans* $\mathbf{Q}(\chi)$, d'un sous-groupe de G.

5. Représentations des groupes résolubles.

Dans tout ce paragraphe, on désigne par G un groupe fini et par P un sous-groupe invariant de G tel que le quotient G/P soit cyclique. Nous nous proposons de déterminer la structure des représentations de G à partir de celles de P. On voit que ceci permet, en particulier, de déterminer la structure des représentations des groupes résolubles.

5.1. Caractères. — Soit X l'ensemble des caractères absolument irréductibles de P. Le groupe G opère sur X par

$$\forall\, g\in G,\ \forall\, \rho\in X,\quad \forall\, s\in P:\quad \rho_g(s)=\rho(gsg^{-1}).$$

Pour tout g dans P et pour tout ρ dans X, on a $\rho_g=\rho$; par passage au quotient, on peut donc faire opérer le groupe $H=G/P$ sur X.

Soit $(\rho_i)_{i\in X/H}$ un système de représentants des orbites de H dans X. Pour tout i, soit G_i' le groupe d'isotropie de ρ_i [par définition, $G_i'=\{g\in G,\ (\rho_i)_g=\rho_i\}$]. Soit H_i' l'image canonique de G_i' dans H. Soit q_i le degré de ρ_i, soit m_i l'ordre de H_i' et soit d_i l'indice de H_i' dans H. Soit n l'ordre de H; on a $n=m_id_i$ pour tout i.

Soit E un corps algébriquement clos de caractéristique o. Soit α_i une représentation de P par des matrices à coefficients dans E dont le caractère est ρ_i, c'est-à-dire un E-épimorphisme de E[P] sur $M_{q_i}(E)$ associé à ρ_i.

Soit $\overline{h}_i'$ un générateur de H_i' et soit h_i' un relèvement de $\overline{h}_i'$ dans G. Comme $(\rho_i)_{h_i'}=\rho_i$, l'application qui, pour tout s dans P, fait correspondre à $\alpha_i(s)$ l'élément $\alpha_i(h_i'sh_i'^{-1})$, se prolonge de manière unique en un E-automorphisme de $M_{q_i}(E)$. Il existe donc une matrice ν_i de $M_{q_i}(E)$ telle que

$$\forall\, \lambda\in E[P]:\quad \alpha_i(h_i'\,\lambda\, h_i'^{-1})=\nu_i\alpha_i(\lambda)\,\nu_i^{-1}.$$

On en déduit que

$$\forall\, k\in\mathbf{N},\ \forall\, \lambda\in E[P]:\quad \alpha_i(h_i'^{k}\lambda\, h_i'^{-k})=\nu_i^{k}\alpha_i(\lambda)\,\nu_i^{-k}.$$

En particulier, on a

$$\nu_i^{m_i}\alpha_i(\lambda)\,\nu_i^{-m_i}=\alpha_i(h_i'^{m_i}\lambda\, h_i'^{-m_i})=\alpha_i(h_i'^{m_i})\,\alpha_i(\lambda)\,(\alpha_i(h_i'^{m_i}))^{-1}.$$

Comme α_i est surjectif, on a

$$\forall\, \mu \in \mathrm{M}_{q_i}(\mathrm{E}) : \quad (\alpha_i(h_i'^{m_i}))^{-1}\, \nu_i^{m_i} \mu = \mu\, (\alpha_i(h_i'^{m_i}))^{-1}\, \nu_i^{m_i}.$$

Il existe donc un élément c_i de E tel que $\nu_i^{m_i} = c_i \alpha_i(h_i'^{m_i})$. Soit c_i' un élément de E tel que $c_i'^{m_i} = c_i$. Si l'on remplace ν_i par $c_i'^{-1}\nu_i$, on voit qu'alors $\nu_i^{m_i} = \alpha_i(h_i^{m_i})$. Il est immédiat que l'application $\tilde{\alpha}_i$ de G_i' dans $\mathrm{M}_{q_i}(\mathrm{E})$ définie par

$$\tilde{\alpha}_i(h_i'^k s) = \nu_i^k \alpha_i(s), \qquad \text{pour} \quad k \in \{0, 1, \ldots, m_i - 1\} \quad \text{et} \quad s \in \mathrm{P},$$

est une représentation de G_i' de degré q_i absolument irréductible. Soit $\tilde{\rho}_i$ le caractère de cette représentation.

Soient $(\xi_j)_{j=0,1,\ldots,m_i-1}$ les caractères absolument irréductibles de $\mathrm{G}_i'/\mathrm{P} = \mathrm{H}_i'$. Pour tout j, soit $\eta_{i,j} = \xi_j \tilde{\rho}_i$. Soit $\chi_{i,j}$ le caractère de G induit par $\eta_{i,j}$.

PROPOSITION 5.1. — *Les caractères $\chi_{i,j}$ sont absolument irréductibles, deux à deux distincts, et tout caractère absolument irréductible de* G *est égal à l'un d'entre eux.*

Démonstration :

(*a*) *Le caractère $\chi_{i,j}$ est absolument irréductible.*

Soit h un élément de G n'appartenant pas à G_i'. On a $(\rho_i)_h \neq \rho_i$. Comme la restriction de $(\eta_{i,j})_h$ à P est $(\rho_i)_h$, on en déduit que $(\eta_{i,j})_h$ est différent de $\eta_{i,j}$. Par conséquent, $\chi_{i,j}$ est irréductible.

(*b*) *Les $\chi_{i,j}$ sont deux à deux distincts.*

Montrons tout d'abord le lemme suivant :

LEMME. — *Pour $j \neq j'$, on a $\eta_{i,j} \neq \eta_{i,j'}$.*

Démonstration. — Soit ρ_i' le caractère de G_i' induit par ρ_i. Comme P est invariant dans G_i' et comme, pour tout s dans P et pour tout h dans G_i', on a $\rho_i(hsh^{-1}) = \rho_i(s)$, on voit que

$$\rho_i'(\sigma) = \begin{cases} 0 & \text{pour} \quad \sigma \notin \mathrm{P}; \\ m_i \rho_i(\sigma) & \text{pour} \quad \sigma \in \mathrm{P}. \end{cases}$$

Soit $\rho_i'' = \sum_{j=0}^{m_i-1} \eta_{i,j}$. On a

$$\rho_i''(\sigma) = \sum_j \xi_j(\sigma)\, \eta_{i,0}(\sigma) = \eta_{i,0}(\sigma) \sum_j \xi_j(\sigma).$$

Or, $\sum \xi_j$ n'est autre que la représentation régulière de G'_i/P. On a donc

$$\sum \xi_j(\sigma) = \begin{cases} 0 & \text{pour } \sigma \notin P; \\ m_i & \text{pour } \sigma \in P. \end{cases}$$

Comme la restriction de $\eta_{i,0}$ à P est ρ_i, on en déduit que $\rho'_i = \rho''_i$. Comme la restriction de $\eta_{i,j}$ à P est ρ_i, il résulte de la formule de réciprocité de Frobenius que $(\rho'_i, \eta_{i,j}) = (\rho_i, \rho_i) = 1$. Comme $\rho'_i = \sum \eta_{i,j}$, on en déduit que tous les $\eta_{i,j}$ sont distincts. C. Q. F. D.

Suite de la démonstration de la proposition 6.1. — Si les caractères $\chi_{i,j}$ et $\chi_{i',j'}$ sont égaux, ils ont la même restriction à P; donc ρ_i et $\rho_{i'}$ sont dans la même orbite, donc $i = i'$.

La restriction de $\chi_{i,j}$ à G'_i est $\sum_{h \in G/G'_i} (\eta_{i,j})_h$. On a donc, d'après la formule de réciprocité de Frobenius :

$$(\chi_{i,j'}, \chi_{i,j}) = \left(\eta_{i,j'}, \sum_{h \in G/G'_i} (\eta_{i,j})_h\right) = \sum_{h \in G/G'_i} (\eta_{i,j'}, (\eta_{i,j})_h).$$

Les $(\eta_{i,j})_h$ et $\eta_{i,j'}$ sont des caractères absolument irréductibles de G'_i. La restriction de $\eta_{i,j'}$ à P est ρ_i, celle de $(\eta_{i,j})_h$ est $(\rho_i)_h$. On a donc $(\eta_{i,j})_h \neq \eta_{i,j'}$, pour $h \notin G'_i$. Si $h \in G'_i$, on a $(\eta_{i,j})_h = \eta_{i,j}$. Il résulte alors du lemme que

$$(\chi_{i,j'}, \chi_{i,j}) = \begin{cases} 0 & \text{si } j \neq j'; \\ 1 & \text{si } j = j'. \end{cases}$$

Les $\chi_{i,j}$ sont donc bien deux à deux distincts.

(*c*) *Tout caractère absolument irréductible est de ce type.*

Soit q l'ordre de P. Soit q_i le degré de ρ_i. L'orbite de ρ_i par H a exactement d_i éléments, chacun de degré q_i. On en déduit que $\sum_i d_i q_i^2 = q$. Pour i fixé, on a m_i caractères distincts $\chi_{i,j}$, chacun de degré $d_i q_i$. On a alors

$$\sum_i m_i (d_i q_i)^2 = n \sum_i d_i q_i^2 = nq = (G : 1).$$

La somme $\sum \chi_{i,j}(1).\chi_{i,j}$ est donc le caractère de la représentation régulière de G. Les $\chi_{i,j}$ sont bien tous les caractères absolument irréductibles de G. C. Q. F. D.

5.2. Les facteurs simples de l'algèbre du groupe. — Soit E un corps de caractéristique o (que l'on ne suppose plus algébriquement clos). Soit $\chi = \chi_{i,j}$ un caractère absolument irréductible de G à valeurs dans E. Posons $\eta = \eta_{i,j}$ et $\rho = \rho_i$. Posons $E' = E(\eta)$. Les méthodes du paragraphe 3 permettent de déterminer la structure du facteur simple de l'algèbre E[G] associé à χ à partir de la structure du facteur simple de l'algèbre $E[G'_i]$ associé à η. Quant à $\bar{\varepsilon}_{E'}(\eta)$, il est déterminé par la proposition suivante :

Proposition 5.2. — *On a* $\bar{\varepsilon}_{E'}(\eta) = \bar{\varepsilon}_{E'}(\rho)$.

Démonstration. — Comme la restriction de η à P est ρ, on voit que $(\mathrm{Res}_P(\eta), \rho) = 1$. Donc, d'après la proposition 3.1, pour tout nombre premier p, les p-composantes de $\bar{\varepsilon}_{E'}(\eta)$ et $\bar{\varepsilon}_{E'}(\rho)$ sont les mêmes.

C. Q. F. D.

6. Représentations des groupes de type C_p.

6.1. Définitions.

6.1.1. Soit p un nombre premier et soit G un groupe fini. Nous disons que G est *un groupe de type* C_p si c'est le produit semi-direct d'un sous-groupe invariant P abélien p-élémentaire [c'est-à-dire de type $(p, p, \ldots, p)$] par un groupe cyclique H d'ordre premier à p et si P, considéré comme $\mathbf{F}_p[H]$-module, est isotypique.

Dans toute la suite de cet article, si G est un groupe de type C_p, on désigne par P son p-sous-groupe de Sylow et par H un groupe cyclique quelconque d'ordre premier à p tel que $G = H.P$. On désigne par H′ le noyau de la représentation canonique de H dans P et par G′ le produit direct $H' \times P$ (on voit que le groupe G′ est le centraliseur de P dans G). On pose

$$n(G) = n = (H : 1), \qquad m(G) = m = (H' : 1), \qquad d(G) = d = (H : H').$$

On a donc $n = md$.

Si P est réduit à l'élément neutre, le groupe G est tout simplement un groupe cyclique d'ordre premier à p et l'étude de ses représentations est entièrement triviale. Dans toute la suite du paragraphe, sauf mention explicite du contraire, nous désignons par G un groupe de type C_p et nous supposons P non réduit à l'élément neutre.

6.1.2. Nous disons que G est *un groupe de type* CS_p, si P est un $\mathbf{F}_p[H]$-module simple.

Soit G un groupe de type CS_p. Soit $\mathbf{F}_q$ la plus petite extension de $\mathbf{F}_p$ contenant les racines $d^{\text{ièmes}}$ de l'unité. Le corps $\mathbf{F}_q$ est donc le corps à $q = p^r$ éléments, en désignant par r le plus petit entier strictement positif tel que d divise $p^r - 1$. On voit que le groupe G est isomorphe au produit semi-direct du groupe cyclique $\mathbf{Z}/n\mathbf{Z}$ par le groupe additif de $\mathbf{F}_q$, l'action de $\mathbf{Z}/n\mathbf{Z}$ sur $\mathbf{F}_q$ se faisant par

$$x \mapsto \omega . x,$$

en désignant par ω une racine primitive $d^{\text{ième}}$ de l'unité. Un groupe de type CS_p est donc déterminé, à un isomorphisme près, par la donnée des entiers m et d, strictement positifs et premiers à p.

Pour tout groupe G de type C_p, nous désignons par $l(G) = l$ le nombre de facteurs intervenant dans la décomposition de P en $\mathbf{F}_p[H]$-modules simples. Le groupe G est de la forme

$$G = H.(P_1 \times P_2 \times \ldots \times P_l),$$

où les P_i sont des $\mathbf{F}_p[H]$-modules simples isomorphes. Le groupe $H.P_1$ est de type CS_p. Il est défini à un isomorphisme près et on l'appelle *le groupe de type* CS_p *associé à* G. On le note G_S.

Un groupe de type C_p est déterminé, à un isomorphisme près, par la donnée des entiers m, d et l.

6.1.3. Si P est cyclique d'ordre p, nous disons que G est *un groupe de type* CC_p. Il est clair qu'un groupe de type CC_p est de type CS_p et qu'un groupe de type CS_p est de type CC_p si et seulement si d divise $p - 1$.

Si G est un groupe de type C_p et si $d = d_C d'$, avec $d_C = (d, p - 1)$, nous notons H_C le sous-groupe de H d'ordre md_C. Si P_C est un sous-groupe cyclique d'ordre p de P, le groupe $H_C.P_C$ est un sous-groupe de type CC_p de G. Il est défini à un isomorphisme près et on l'appelle *le groupe de type* CC_p *associé à* G. On le note G_C. Il est clair que $G_C = (G_S)_C$.

6.2. Caractères.

Proposition 6.1. — *Les caractères absolument irréductibles de* G *sont :*

(i) *d'une part, n caractères de degré* 1 *: ce sont les caractères de degré* 1 *du groupe cyclique* G/P *qui est d'ordre n*;

(ii) *d'autre part,* $m(p^{rl} - 1)/d$ *caractères de degré d : ce sont les caractères induits par les caractères de degré* 1 *de* G′ *dont la restriction à* P *est différente du caractère* 1_P *de la représentation unité.*

Démonstration. — Comme P est abélien, l'ensemble X des caractères absolument irréductibles de P n'est autre que l'ensemble des $(P : 1) = p^{rl}$ caractères de degré 1 de P.

Soit $\rho \in X$. Si ρ est égal à 1_P, on voit que le sous-groupe d'isotropie de ρ est G tout entier et que, par conséquent, l'orbite de ρ est réduite à ρ.

Si ρ est différent de 1_P, on voit que le sous-groupe d'isotropie de ρ contient G'. Le noyau A de ρ est un sous-groupe de P d'ordre p^{rl-1}. Soit h un élément de H et soit H_h le sous-groupe de H engendré par h. Il est clair que P est un $\mathbf{F}_p[H_h]$-module semi-simple. Si $\rho_h = \rho$, on doit avoir $A^h = A$ et A est un sous-$\mathbf{F}_p[H_h]$-module de P. Il existe donc un sous-groupe cyclique S de P qui est un sous-$\mathbf{F}_p[H_h]$-module et qui est tel que la restriction de ρ à S est fidèle. Si s est un élément de S différent de 1, l'égalité $\rho_h = \rho$ entraîne $hsh^{-1} = s$. Par conséquent, $h \in H'$. On en déduit que le sous-groupe d'isotropie de ρ est G' et que l'orbite de ρ a d éléments.

L'assertion résulte alors de la proposition 5.1. C. Q. F. D.

Remarque : Valeurs des caractères. — Soit χ_0 (resp. ξ) un caractère fidèle de degré 1 de H (resp. H') et soit $(\rho_i)_{i=0,1,\ldots,(p^{rl}-1)/d}$ un système de représentants des orbites de X modulo H, avec $\rho_0 = 1_P$. On vérifie facilement que les caractères absolument irréductibles de G sont :

(i) d'une part n caractères de degré 1, $\chi_{0,j}$, pour $j = 0, 1, \ldots, n-1$, définis par

$$\chi_{0,j}(sg) = \chi_0^j(s), \quad \text{pour tout } s \text{ dans H et tout } g \text{ dans P};$$

(ii) d'autre part, $m(p^{rl}-1)/d$ caractères de degré d, $\chi_{i,j}$, pour $i = 1, 2, \ldots, (p^{rl}-1)/d$ et $j = 0, 1, \ldots, m-1$, définis par

$$\chi_{i,j}(sg) = \left\{ \begin{array}{c} 0 \text{ si } s \notin H' \\ \xi^j(s) \sum_{h \in H/H'} \rho_i(hgh^{-1}) \text{ si } s \in H' \end{array} \right\} \text{ pour tout } s \text{ dans H et tout } g \text{ dans P.}$$

Proposition 6.2. — *Soit χ un caractère absolument irréductible de* G *dont le noyau ne contient pas* P. *Alors le quotient de* G *par l'intersection de* P *et du noyau de χ est isomorphe au groupe de type* CS_p *associé à* G.

Démonstration. — Il est clair que $P \cap \mathrm{Ker}\chi$ est un sous-$\mathbf{F}_p[H]$-module de P. Il existe donc un $\mathbf{F}_p[H]$-module S tel que $P = S \times \mathrm{Ker}\chi$. On voit que la restriction χ_S de χ à S est un caractère fidèle. Si s est un élément de S différent de 1, on en déduit que S est le $\mathbf{F}_p[H]$-module engendré par s. Par conséquent, S est un $\mathbf{F}_p[H]$-module simple et l'assertion résulte de l'isomorphisme évident entre $G/P \cap \mathrm{Ker}\chi$ et H.S. C. Q. F. D.

COROLLAIRE. — *Soit* E *un corps de caractéristique* o. *Les assertions suivantes sont équivalentes :*

(i) *l'algèbre* E[G] *est décomposée;*

(ii) *l'algèbre* $E[G_S]$ *est décomposée.*

En effet, posons, comme au n° 6.1.2, $G = H.(P_1 \times P_2 \times \ldots \times P_l)$. Il est clair que toute représentation de $H.P_1$ définit, de manière canonique, une représentation de G dont le noyau contient $P_2 \times \ldots \times P_l$. Par conséquent, (i) entraîne (ii). L'assertion inverse résulte de la proposition 6.2.

Nous notons θ_G le caractère de G qui est la somme des caractères absolument irréductibles distincts de G dont le noyau ne contient pas P.

PROPOSITION 6.3. — *Soit* r_G (*resp.* $r_{G/P}$) *le caractère de la représentation régulière de* G (*resp.* G/P). *On a*

$$d\theta_G = r_G - r_{G/P}$$

et les valeurs de θ_G *sont*

$$\theta_G(s) = \begin{cases} 0 & si \quad s \notin P; \\ -m & si \quad s \in P - \{1\}; \\ m(p^{rl}-1) & si \quad s = 1. \end{cases}$$

Démonstration. — Soit X_1 (resp. X_2) l'ensemble des caractères absolument irréductibles de G dont le noyau contient P (resp. ne contient pas P). Il résulte de la proposition 6.1 que les caractères de X_1 (resp. X_2) sont tous de degré 1 (resp. d). On a donc $r_G = \sum_{\chi \in X_1} \chi + \sum_{\chi \in X_2} d\chi$ et $r_{G/P} = \sum_{\chi \in X_1} \chi$. Par conséquent, $r_G - r_{G/P} = \sum_{\chi \in X_2} d\chi = d\theta_G$. Les valeurs de θ_G se déduisent immédiatement de cette formule. C. Q. F. D.

PROPOSITION 6.4. — *Soit* E *un corps de caractéristique* o. *Les assertions suivantes sont équivalentes :*

(i) *l'algèbre* E[G] *est décomposée;*

(ii) *le caractère* θ_G *est rationnel sur* E.

Démonstration. — Il résulte de la proposition précédente que le caractère θ_G est à valeurs dans $\mathbf{Z}$ donc dans E. Si G est abélien, c'est-à-dire si $d = 1$, l'assertion est triviale. Sinon, on voit que θ_G est la somme de tous les caractères absolument irréductibles distincts de G qui ne sont pas de degré 1. Comme, pour tout caractère χ de degré 1, on a $m_E(\chi) = 1$,

il en résulte que $m_E(\theta_G)$ est le ppcm des $m_E(\chi)$, pour χ caractère absolument irréductible de G. La proposition 6.4 est alors évidente.

C. Q. F. D.

6.3. Décomposition de l'algèbre E[G]. — Dans toute la suite du paragraphe, on désigne par E un corps de caractéristique o.

6.3.1. *Réduction aux groupes de type* CC_p.

Proposition 6.5. — *Soit* χ *un caractère absolument irréductible de* G *induit par un caractère* η *de degré* 1 *de* G'. *Soit* H_c *le sous-groupe de* H *d'ordre* md_c, *avec* $d_c = (d, p-1)$. *Soit* χ_c *le caractère de* $H_c.P$ *induit par* η. *Alors* χ *est induit par* χ_c, *on a* $\mathbf{Q}(\chi_c) = \mathbf{Q}(\chi)$ *et le quotient de* $H_c.P$ *par l'intersection de* P *avec le noyau de* χ_c *est isomorphe au groupe de type* CC_p *associé à* G.

Démonstration. — Il est clair que χ est induit par χ_c. Soit, comme au n° 3.2.1, G_η l'ensemble des éléments g de G tels que η et η_g soient conjugués sur $\mathbf{Q}$. Comme χ est absolument irréductible, la restriction de η à P est différente du caractère 1_P de la représentation unité. On vérifie immédiatement que ceci entraîne $G_\eta = H_c.P$. On en déduit que H_c/H' est canoniquement isomorphe au groupe de Galois de l'extension $\mathbf{Q}(\eta)/\mathbf{Q}(\chi)$ et que, par conséquent, $\mathbf{Q}(\chi) = \mathbf{Q}(\chi_c)$. Enfin, la dernière assertion résulte de la proposition 6.2 appliquée à $H_c.P$. C. Q. F. D.

Proposition 6.6. — *Les assertions suivantes sont équivalentes :*

(i) *l'algèbre* E[G] *est décomposée;*

(ii) *l'algèbre* $E[G_c]$ *est décomposée.*

Démonstration. — Soit A un sous-groupe de P d'indice p dans P. Il est clair que A est invariant dans $H_c.P$ et que le groupe quotient $H_c.P/A$ est isomorphe à G_c. Tout caractère absolument irréductible χ_c de G_c peut donc être considéré comme un caractère absolument irréductible de $H_c.P$ dont le noyau contient A. Si χ_c n'est pas de degré 1, on voit que le caractère χ de G induit par χ_c est absolument irréductible et que $\mathbf{Q}(\chi) = \mathbf{Q}(\chi_c)$. D'après le corollaire à la proposition 3.1, χ_c est donc rationnel sur $\mathbf{Q}(\chi)$ si et seulement si χ l'est. Et (i) implique (ii). L'implication inverse résulte du corollaire à la proposition 3.1 et de la proposition 6.5. C. Q. F. D.

Corollaire. — *Soit* χ *un caractère absolument irréductible de* G. *Alors* $m_Q(\chi)$ *divise* $(p-1, d)$.

En effet, il existe un caractère χ_C de G_C tel que $m_Q(\chi_C) = m_Q(\chi)$ et $m_Q(\chi_C)$ divise le degré de χ_C qui est 1 ou $d_C = (p-1, d)$.

6.3.2. *Représentations fidèles des groupes de type* CC_p. — Soit G un groupe de type CC_p et soit χ un caractère absolument irréductible et fidèle de G. Le noyau de χ ne contenant pas P, χ est induit par un caractère η de degré 1 de G'. Le sous-groupe G' est cyclique d'ordre mp et invariant dans G. On en déduit que tout sous-groupe de G' est invariant dans G et que, par conséquent, η est fidèle.

Si $J = G/G' = H/H'$, on a la suite exacte

$$1 \to G' \to G \to J \to 1.$$

On voit que $\mathbf{Q}(\eta) = (\mathbf{Q}(\chi))(\sqrt[p]{1})$ et que J est canoniquement isomorphe au groupe de Galois de l'extension $\mathbf{Q}(\eta)/\mathbf{Q}(\chi)$. Le caractère χ et le groupe G sont donc $\mathbf{Q}(\chi)$-métabéliens. Soit ε l'élément de $H^2(J, G')$ qui définit G. Il résulte de la proposition 3.3 que $\bar{\varepsilon}_{\mathbf{Q}(\chi)}(\chi)$ est l'image de $\eta(\varepsilon)$ dans $H^2(\mathbf{Q}(\eta)/\mathbf{Q}(\chi))$.

Posons $\mathbf{Q}' = \mathbf{Q}(\sqrt[p]{1})$ et désignons par $\mathbf{Q}''$ l'unique extension de $\mathbf{Q}$ de degré $(p-1)/d$ contenue dans $\mathbf{Q}'$. Soit h un générateur de H. Posons $h^d = h'$. Alors h' est un générateur de H'. Posons $\eta(h') = b$. Comme η est fidèle, b est une racine primitive $m^{\text{ième}}$ de l'unité et on voit que $\mathbf{Q}(\eta) = \mathbf{Q}'(b)$ et $\mathbf{Q}(\chi) = \mathbf{Q}''(b)$. Si $\bar{h}$ désigne l'image canonique de h dans J et si φ_h désigne le caractère de J défini par $\varphi_h(\bar{h}) = 1/d$, alors (*cf.* n° 1.2.1) on a $\bar{\varepsilon}_{\mathbf{Q}(\chi)}(\chi) = (\varphi_h, b)$. On a donc établi le résultat suivant :

PROPOSITION 6.7. — *Avec les notations qui précèdent, on a*

$$\bar{\varepsilon}_{\mathbf{Q}(\chi)}(\chi) = (\varphi_h, b).$$

COROLLAIRE 1. — *Supposons χ à valeurs dans* E. *Pour que χ soit rationnel sur* E, *il faut et il suffit que les racines $m^{\text{ièmes}}$ de l'unité soient normes dans l'extension* $E(\sqrt[p]{1})/E$.

En effet, $\bar{\varepsilon}_E(\chi)$ est la restriction à E de (φ_h, b) et est égal à 1 si et seulement si b est norme dans l'extension $E(\sqrt[p]{1})/E$. Un cas particulier du corollaire 1 est le suivant :

COROLLAIRE 2. — *Si $m = 1$, alors χ est rationnel sur $\mathbf{Q}(\chi)$.*

Remarques :

(*a*) L'élément $\bar{\varepsilon}_{\mathbf{Q}(\chi)}(\chi)$ est complètement déterminé par sa restriction à tous les complétés K_p de $\mathbf{Q}(\chi)$. Pour chacun d'entre eux, on peut en

calculer l'invariant. Si $m = 1$, tous les invariants sont nuls. Supposons donc $m > 1$. Un groupe de type CC_2 étant abélien, puisque d divise $2 - 1 = 1$, on peut aussi supposer $p \neq 2$.

(i) Si $m > 2$ ou si d est impair, on voit que $\mathbf{Q}(\chi)$ n'a pas de plongement réel. Si $m = 2$ et si d est pair, on voit que $\mathbf{R}(\chi) = \mathbf{R}$ et $\mathbf{R}(\eta) = \mathbf{C}$. Comme -1 n'est pas norme dans l'extension $\mathbf{C}/\mathbf{R}$, $\bar{\varepsilon}_{\mathbf{R}}(\chi)$ est l'unique élément non trivial de $\mathrm{Br}(\mathbf{R})$ et son invariant est $1/2$.

(ii) Soit λ un nombre premier différent de p. L'extension $\mathbf{Q}_\lambda(\eta)/\mathbf{Q}_\lambda(\chi)$ est non ramifiée. Comme b est une unité, b est une norme dans l'extension et χ est rationnel sur $\mathbf{Q}_\lambda(\chi)$. Donc, pour toute place au-dessus d'un nombre premier λ différent de p, l'invariant est nul.

(iii) Sur $\mathbf{Q}_p(\chi)$, l'invariant est donné par la proposition 1.7. Soit ν la racine primitive $d^{\text{ième}}$ de l'unité définie par $\theta_0(\bar{h}) = \nu$. Soit q la plus petite puissance de p telle que m divise $q - 1$. Soit k l'unique entier, modulo d, tel que $b^{-(q-1)/d} = \nu^k$. Alors l'invariant de $\bar{\varepsilon}_{\mathbf{Q}_p(\chi)}(\chi)$ est k/d.

De plus, si on pose $c = m/((q-1)/d, m)$, on voit que $b^{-(q-1)/d}$ est une racine primitive $c^{\text{ième}}$ de l'unité. L'indice de Schur de χ sur $\mathbf{Q}_p$ est le dénominateur de la fraction réduite égale à k/d, c'est-à-dire c. On vérifie immédiatement que $m/((q-1)/d, m) = d/((q-1)m, d)$. L'indice de Schur de χ sur $\mathbf{Q}$ est le ppcm des indices de Schur locaux. On a donc

$$m_{\mathbf{Q}}(\chi) = \begin{cases} d/((q-1)/m, d) & \text{si } m > 2 \text{ ou si } d \text{ est impair;} \\ \text{ppcm de 2 et } d/((p-1)/2, d) & \text{si } m = 2 \text{ et } d \text{ est pair.} \end{cases}$$

(*b*) On a le résultat suivant :

PROPOSITION 6.8. — *Soit p un nombre premier différent de 2 et soit* K *une extension finie de* $\mathbf{Q}_p$. *Soit* $\bar{\varepsilon}$ *un élément de* $\mathrm{Br}_\mu(\mathrm{K})$. *Alors il existe un groupe* G *de type* CC_p *et un caractère absolument irréductible* χ *de* G *à valeurs dans* K *tel que* $\bar{\varepsilon}_{\mathrm{K}}(\chi) = \bar{\varepsilon}$.

Démonstration. — Soit K_c l'extension cyclotomique maximale de $\mathbf{Q}_p$ contenue dans K. Le corps K_c contient l'extension maximale non ramifiée de $\mathbf{Q}_p$ contenue dans K et il résulte du corollaire 2 au théorème 2 que $\mathrm{Br}_\mu(\mathrm{K})$ est la restriction à K de $\mathrm{Br}_\mu(\mathrm{K}_c)$. Un caractère d'un groupe fini est à valeurs dans K si et seulement si il est à valeurs dans K_c; il suffit donc de démontrer l'assertion dans le cas où $\mathrm{K} = \mathrm{K}_c$.

Soit alors d le degré de l'extension $\mathrm{K}(\sqrt[p]{1})/\mathrm{K}$. Si $\mathrm{K} = \mathrm{K}_c$, l'extension $\mathrm{K}(\sqrt[p]{1})/\mathrm{K}$ est totalement ramifiée et $\mathrm{Br}_\mu(\mathrm{K})$ est le sous-groupe de $\mathrm{Br}(\mathrm{K})$ d'ordre d. Soit q le nombre d'éléments du corps résiduel de K. Il est clair

que, lorsque b décrit l'ensemble des racines $(q-1)^{\text{ièmes}}$ de l'unité, $b^{-(q-1)/d}$ décrit l'ensemble des racines $d^{\text{ièmes}}$ de l'unité. La proposition résulte alors immédiatement du (iii) de la remarque (a). C. Q. F. D.

6.3.3. *Décomposition de l'algèbre* E[G].

THÉORÈME 4. — *Soit* G *un groupe de type* C_p *et soit* E *un corps de caractéristique* 0. *Soit* F′ (*resp.* $\mathbf{Q}'$) *le corps des racines* $p^{\text{ièmes}}$ *de l'unité sur* E(*resp.* $\mathbf{Q}$). *Le corps* $\mathbf{Q}'$ *peut s'identifier à un sous-corps de* F′. *Soit* $\mathbf{Q}''$ *l'unique extension de* $\mathbf{Q}$ *de degré* $(p-1)/(p-1, d(G))$ *contenue dans* $\mathbf{Q}'$ *et soit* F *le corps engendré sur* E *par* $\mathbf{Q}''$. *Alors, pour que l'algèbre* E[G] *soit décomposée, il faut et il suffit que, pour toute racine* $m(G)^{\text{ième}}$ *de l'unité* b, b *soit norme dans l'extension* $F'(b)/F(b)$.

Démonstration. — D'après la proposition 6.6, l'algèbre E[G] est décomposée si et seulement si l'algèbre $E[G_C]$ l'est. On a $d(G_C) = (p-1, d(G))$ et $m(G_C) = m(G)$. On voit donc qu'il suffit de démontrer le théorème lorsque G est de type CC_p. S'il en est ainsi, il est clair que les caractères absolument irréductibles de G qui ne sont pas de degré 1 correspondent exactement, lorsque G n'est pas abélien, aux caractères absolument irréductibles et fidèles des groupes G_1 de type CC_p satisfaisant $d(G_1) = d(G)$ et $m(G_1)$ divise $m(G)$. Le théorème résulte alors du corollaire 1 à la proposition 6.7. C. Q. F. D.

COROLLAIRE 1. — *Soit* λ *un nombre premier différent de* p. *L'algèbre* $\mathbf{Q}_\lambda[G]$ *est décomposée.*

C'est une conséquence triviale du (ii) de la remarque (a) du numéro précédent.

COROLLAIRE 2. — *Pour que l'algèbre* $\mathbf{R}[G]$ *soit décomposée, il faut et il suffit que* $(m, d, p-1)$ *soit impair.*

En effet, il résulte du (i) de la remarque (a) du numéro précédent que $\mathbf{R}[G]$ est décomposée si et seulement si ou bien tout diviseur de m est différent de 2, ou bien $(d, p-1)$ est impair.

COROLLAIRE 3. — *Si* E *contient les racines* $p^{\text{ièmes}}$ *de l'unité, l'algèbre* E[G] *est décomposée.*

En effet, pour tout b, on a $F'(b) = F(b)$, et, par conséquent, b est norme dans l'extension $F'(b)/F(b)$.

COROLLAIRE 4. — *Si* $(m, d, p-1) = 1$, *l'algèbre* $\mathbf{Q}[G]$ *est décomposée.*

En effet, l'extension F'/F est de degré $(d, p-1)$ et b est une racine de l'unité d'ordre premier à $(d, p-1)$. Donc, b est norme dans l'extension $F'(b)/F(b)$.

COROLLAIRE 5. — *Soit d_m la m-composante de d. Si* E *contient les racines $(d_m m)^{\text{ièmes}}$ de l'unité (en particulier, si* E *contient les racines $n^{\text{ièmes}}$ de l'unité), l'algèbre* E[G] *est décomposée.*

En effet, on a alors $F'(b) = F'$ et $F(b) = F$. Soit a une racine primitive $(d_m m)^{\text{ième}}$ de l'unité contenue dans F. La norme de F' à F de a est a^d et on vérifie immédiatement que c'est une racine primitive $m^{\text{ième}}$ de l'unité.

6.4. CONSTRUCTION DE LA REPRÉSENTATION DÉFINIE PAR θ_G. — Pour achever ce paragraphe, nous allons retrouver par des méthodes entièrement élémentaires certains résultats du n° 6.3 et donner, dans certains cas, une construction explicite de la représentation définie par θ_G.

6.4.1. *Relations entre θ_G, θ_{G_s} et θ_{G_c}.* — Les deux propositions suivantes se vérifient immédiatement sur les valeurs des caractères :

PROPOSITION 6.9. — *Soit P_1 un sous-$\mathbf{F}_p$[H]-module simple non trivial de* P. *On a :*

(i) $\theta_{HP_1} = \mathrm{Res}_{HP_1}(\theta_G) - (p^{rl} - p^r)\, d^{-1} p^{-r} r_{HP_1}$, *en désignant par r_{HP_1} la représentation régulière de HP_1;*

(ii) $\theta_G = \theta_{G/P_1} + \theta^*_{HP_1}$, *en désignant par $\theta^*_{HP_1}$ le caractère de* G *induit par θ_{HP_1}.*

PROPOSITION 6.10. — *Supposons* G *de type CS_p. Soit H_C le sous-groupe de* H *d'ordre md_C, avec $d_C = (d, p-1)$. Pour tout élément s de $P - \{1\}$, soit P_s le groupe cyclique engendré par s et soit J_s la réunion des orbites des éléments de $P_s - \{1\}$ (pour l'action de* H *sur* P). *Les J_s constituent une partition $\mathfrak{T}$ de $P - \{1\}$. Dans chaque élément J de $\mathfrak{T}$, choisissons un élément s_J. On a :*

(i) *pour tout s appartenant à $P - \{1\}$,*

$$\theta_{H_C P_s} = \mathrm{Res}_{H_C P_s}(\theta_G) - (p^{r-1} - 1)\, d_C^{-1} r_{H_C P_s},$$

en désignant par $r_{H_C P_s}$ la représentation régulière de $H_C P_s$;

(ii) $p^{r-1}\theta_G = \sum_{J \in \mathfrak{T}} \theta^*_{H_C P_{s_J}}$, *en désignant par $\theta^*_{H_C P_{s_J}}$ le caractère de* G *induit par $\theta_{H_C P_{s_J}}$.*

Comme d divise $p^r - 1$ et comme d_C divise $p - 1$, on voit que les assertions (i) de ces propositions permettent, compte tenu de la proposition 6.4, de montrer que, si l'algèbre $E[G]$ est décomposée, alors l'algèbre $E[G_C]$ l'est aussi. De même les assertions (ii) permettent de montrer que si l'algèbre $E[G_C]$ est décomposée, $p^{r-1}\theta_G$ est rationnel sur E. Comme le degré de chaque caractère absolument irréductible qui divise θ_G est premier à p, on voit que $m_E(\theta_G)$ est premier à p. Donc θ_G est rationnel sur E et l'algèbre $E[G]$ est décomposée.

On retrouve ainsi la proposition 6.6.

6.4.2. *Construction de θ_G lorsque* E *contient les racines $p^{\text{ièmes}}$ de l'unité.*

PROPOSITION 6.11. — *Soit* X *l'ensemble des caractères absolument irréductibles de* P. *Soit 1_P le caractère de la représentation unité de* P *et soit (ρ_i) un système de représentants des orbites de $X - \{1_P\}$ pour l'action de* H. *Soit $r_{H'}$ le caractère de la représentation régulière de* H'. *Alors θ_G est le caractère de* G *induit par le caractère $r_{H'} \otimes \sum \rho_i$ de* G'.

Démonstration. — Le caractère θ_G est la somme de tous les caractères distincts induits par les caractères de degré 1 de G' dont la restriction à P n'est pas 1_P. On obtient chacun d'entre eux une fois et une fois seulement en prenant tous les caractères de la forme $\eta \otimes \rho_i$, avec η caractère de degré 1 de H', d'où le résultat. C. Q. F. D.

Le caractère $\sum \rho_i$ est une somme de caractères de degrés 1. Lorsque E contient les racines $p^{\text{ièmes}}$ de l'unité, chacun d'entre eux est à valeurs dans E et on peut donc construire une représentation de P sur E dont le caractère est $\sum \rho_i$. En tensorisant avec la représentation régulière de H' et en prenant la représentation de G induite, on obtient une construction effective de θ_G sur E. En particulier, on retrouve le corollaire 3 du théorème 4.

6.4.3. *Construction de θ_G sur* **Q** *lorsque* $(m, d) = 1$. — On a vu (cor. 4 au théorème 4) que, lorsque $(m, d) = 1$, l'algèbre $\mathbf{Q}[G]$ est décomposée. Nous allons retrouver ce résultat en donnant une construction de la représentation définie par θ_G dans ce cas.

Si $(m, d) = 1$, le groupe G est le produit direct d'un groupe cyclique A d'ordre m par un groupe G_1 de type C_p vérifiant $m(G_1) = 1$. On vérifie immédiatement que la représentation de G définie par θ_G peut s'obtenir comme produit tensoriel de la représentation régulière de A par la repré-

sentation de G_1 définie par θ_{G_1}. Il suffit donc de construire une représentation de caractère θ_G sur $\mathbf{Q}$ lorsque $m = 1$.

Le groupe G opère alors sur P de la manière suivante :

(*a*) P opère sur lui-même par les translations : $s : \sigma \mapsto s\sigma$;

(*b*) H opère sur P par les automorphismes intérieurs $h : \sigma \mapsto h\sigma h^{-1}$.

On en déduit une représentation de G sur l'espace vectoriel des fonctions sur P à valeurs dans $\mathbf{Q}$. Soit φ le caractère de cette représentation. Pour tout t dans G de la forme $t = hs$, avec h dans H et s dans P, $\varphi(hs)$ est égal au nombre de solutions dans P de l'équation en σ : $hs\sigma h^{-1} = \sigma$ ou $\sigma^{h-1} = s$. On vérifie immédiatement que, pour tout h différent de 1 appartenant à H, l'application $\sigma \mapsto \sigma^{h-1}$ est un automorphisme de P. On a donc

$$\varphi(t) = \begin{cases} 1 & \text{pour } t \notin P; \\ 0 & \text{pour } t \in P - \{1\}; \\ p^{rl} & \text{pour } t = 1. \end{cases}$$

Si 1_G désigne le caractère de la représentation unité de G, on voit que $\theta_G = \varphi - 1_G$. Par conséquent, θ_G est le caractère du quotient de la représentation définie par φ par la représentation unité.

6.4.4. *Construction de θ_G lorsque* E *contient les racines $n^{\text{ièmes}}$ de l'unité.* — Soit $\tilde{H} = G/P$ et soit ξ_1 un caractère de degré 1 de $\tilde{H}$ qui est fidèle. Posons $\xi_j = \xi_1^j$ et soit $\xi = \sum_{j=0}^{m-1} \xi_j$. Si le corps E contient les racines $n^{\text{ièmes}}$ de l'unité, le caractère ξ est une somme de caractères de degré 1 à valeurs dans E et est rationnel sur E. Il est clair que sa restriction à $\tilde{H}' = G'/P$ n'est autre que le caractère de la représentation régulière de $\tilde{H}'$. Si $\overline{G} = G/H'$, on vient de voir comment on peut construire une représentation de $\overline{G}$ de caractère $\theta_{\overline{G}}$ sur $\mathbf{Q}$ donc aussi sur E. On vérifie immédiatement sur les valeurs des caractères que le caractère $\xi \otimes \theta_{\overline{G}}$ du produit tensoriel des représentations définies par ξ et $\theta_{\overline{G}}$ est égal à θ_G. On obtient donc ainsi un moyen de construire θ_G sur E et on retrouve, en particulier, que si E contient les racines $n^{\text{ièmes}}$ de l'unité, l'algèbre E[G] est décomposée.

7. Représentations des groupes de type R_p.

7.1. Définitions. — Soit p un nombre premier et soit G un groupe fini. On dit que G est *de type* R_p si c'est le produit semi-direct d'un p-sous-groupe invariant par un groupe cyclique d'ordre premier à p.

Dans tout ce paragraphe, on désigne par G un groupe de type R_p, par P son p-sous-groupe de Sylow et par H un groupe cyclique d'ordre premier à p tel que $G = H.P$. On note $n(G) = n$ l'ordre de H.

Soit λ un entier naturel strictement positif, et soit

$$G = \Gamma_0 \supset \Gamma_1 \supset \ldots \supset \Gamma_\lambda \supset \Gamma_{\lambda+1} = \{1\}$$

une suite de sous-groupes invariants de G vérifiant $\Gamma_j \neq \Gamma_{j+1}$, pour $j = 1, 2, \ldots, \lambda$. On dit que c'est *une* C_p*-suite associée à* G si les conditions suivantes sont satisfaites :

(i) Γ_0/Γ_1 est un groupe cyclique d'ordre premier à p;

(ii) pour $j = 1, 2, \ldots, \lambda$, Γ_j/Γ_{j+1} est un groupe abélien de type $(p, p, \ldots, p)$ contenu dans le centre de Γ_1/Γ_{j+1} qui, en tant que $\mathbf{F}_p[\Gamma_0/\Gamma_1]$-module, est isotypique.

Dans ces conditions, on voit que $\Gamma_1 = P$ et que Γ_0/Γ_1 est canoniquement isomorphe à H. Par abus d'écriture, pour tout j non nul, nous notons encore H l'image de H dans G/Γ_{j+1}.

Il est clair que, pour tout j non nul, $H.\Gamma_j/\Gamma_{j+1}$ est un groupe de type C_p. On dit que la famille des $H.\Gamma_j/\Gamma_{j+1}$ est *la famille des groupes de type* C_p *correspondant à la* C_p*-suite* et que $H.\Gamma_j/\Gamma_{j+1}$ est le $j^{\text{ième}}$ *terme de la famille.* On voit qu'il est défini (par le choix de H) à un isomorphisme près. Une famille de groupes de type C_p correspondant à une suite associée à G est appelée *un système complet de groupes de type* C_p *associé à* G.

Il est immédiat que tout groupe de type R_p admet au moins une C_p-suite associée. On peut même la choisir de manière que tous les groupes de type C_p correspondants soient de type CS_p. Il suffit de choisir un élément s d'ordre p contenu dans le centre de P et de prendre pour Γ_λ le $\mathbf{F}_p[H]$-module engendré par s. On fait ensuite le quotient par Γ_λ, on recommence la même opération sur le groupe G/Γ_λ, et ainsi de suite, jusqu'à ce qu'on arrive à un quotient d'ordre premier à p.

7.2. Caractères. — On a vu (§ 5) comment on peut obtenir les caractères absolument irréductibles de G à partir de ceux de P.

Supposons G muni d'une C_p-suite associée. Soit χ un caractère absolument irréductible de G. Si le noyau de χ contient $\Gamma_1 = P$, χ peut être considéré comme un caractère absolument irréductible du groupe cyclique G/P. Il est donc de degré 1. En particulier, χ est rationnel sur $\mathbf{Q}(\chi)$.

Proposition 7.1. — *Soit* E *un corps de caractéristique* 0. *Si* $p = 2$, *on suppose l'algèbre* E[P] *décomposée. Soit* χ *un caractère absolument irréductible de* G *à valeurs dans* E. *Soit* j *le plus petit entier tel que le noyau de* χ *soit contenu dans* Γ_{j+1}. *Posons* $A_j = H.\Gamma_j/\Gamma_{j+1}$. *Alors, il existe un*

caractère absolument irréductible $\overline{\chi}'$ *d'un sous-groupe de* A_j *qui est à valeurs dans* E *et qui est tel que* $\overline{\varepsilon}_E(\chi) = \overline{\varepsilon}_E(\chi')$.

Démonstration. — Pour tout caractère absolument irréductible ρ de P, soit G'_ρ le sous-groupe d'isotropie de ρ (pour l'action de G).

7.2.1. *Calcul de* $\overline{\varepsilon}_E(\chi)$. — On sait (*cf.* prop. 5.1) qu'il existe un caractère absolument irréductible ρ de P et un caractère absolument irréductible η de G'_ρ tels que les conditions suivantes soient réalisées :

(i) la restriction de η à P est égale à ρ;

(ii) le caractère χ est induit par η.

Si p est différent de 2, d'après la proposition 4.1, ρ est rationnel sur $E(\rho)$; si $p = 2$, il en est de même par hypothèse. D'après la proposition 5.2, η est donc rationnel sur $E(\eta)$ et on peut appliquer le théorème 3.

Soit q le degré de η et soit β un E-épimorphisme de $E[G'_\rho]$ sur $M_q(E(\eta))$ correspondant à η. Soit G_η le sous-groupe de G formé de l'ensemble des g tels que $\eta_{|g}$ et η sont conjugués sur $E(\eta)$. On sait que G'_ρ est un sous-groupe invariant de G_η et que le quotient G_η/G'_ρ est canoniquement isomorphe au groupe de Galois J de l'extension $E(\eta)/E$. Soit ε un système de représentants de l'élément de $H^2(J, G')$ définissant l'extension

$$1 \to G'_\rho \to G_\eta \to J \to 1.$$

Alors, le théorème 3 dit que $(\overline{\varepsilon}_E(\chi))^q$ est la classe, dans Br(E), de l'image par β de dét(ε).

Posons $H_\eta = G_\eta \cap H$ et $H'_\rho = G'_\rho \cap H$. Soit h un générateur de H_η et soit d_E l'ordre de J. Soit $h' = h^{d_E}$. Il est clair que h' est un générateur de H'_ρ. Soit m l'ordre de H'_ρ et soit $\overline{h}$ l'image de h dans J. Il est immédiat que l'on peut choisir ε pour que

$$\varepsilon_{\overline{h}^k, \overline{h}^l} = \begin{cases} 1 & \text{si } k+l < d_E \\ h' & \text{si } k+l \geq d_E \end{cases} \qquad \text{pour } 0 \leq k, l < d_E.$$

Posons $b = \text{dét}(\beta(h'))$. Soit I la matrice unité de $M_q(E(\eta))$. Comme $(\beta(h'))^m = \beta(h'^m) = \beta(1) = I$, on voit que b est une racine $m^{\text{ième}}$ de l'unité. Soit $\varphi_{\overline{h}}$ le caractère de J à valeurs dans $\mathbf{Q}/\mathbf{Z}$ défini par $\varphi_{\overline{h}}(\overline{h}) = 1/d_E$. Alors, b appartient à E et (*cf.* n° 1.2.1), on a $(\overline{\varepsilon}_E(\chi))^q = (\varphi_{\overline{h}}, b)$.

Le degré q de η est égal au degré de ρ qui est un caractère absolument irréductible d'un p-groupe. Donc q est une puissance de p. Comme m divise n qui est premier à p, il existe une racine $m^{\text{ième}}$ de l'unité b' contenue

dans E et une seule telle que $b'^q = b$. Le groupe J est un groupe cyclique dont l'ordre, d_E, divise n. Le caractère χ étant induit par η est rationnel sur $E(\eta)$. Donc l'ordre de $\bar{\varepsilon}_E(\chi)$ divise le degré d_E de l'extension $E(\eta)/E$ et est premier à p. On en déduit que

$$\bar{\varepsilon}_E(\chi) = (\varphi_{\bar{h}}, b').$$

7.2.2. Comme, par hypothèse, le noyau de χ contient Γ_{j+1}, on peut, quitte à passer au quotient, supposer que $\Gamma_{j+1} = \{1\}$. Posons $\Gamma = \Gamma_j$.

LEMME 1. — *Il existe un caractère ρ' de degré 1 de Γ, différent du caractère 1_Γ de la représentation unité, tel que*

$$\mathrm{Res}_\Gamma(\eta) = q\rho'.$$

Démonstration du lemme. — Le caractère ρ est induit par un caractère $\tilde{\rho}$ de degré 1 d'un sous-groupe B de P. Pour tout s dans le centre de P, on a $\tilde{\rho}_s = \tilde{\rho}$. Comme ρ est absolument irréductible, on en déduit que B contient le centre de P. Comme Γ est contenu dans le centre de P, Γ est donc contenu dans B. Soit ρ' la restriction de $\tilde{\rho}$ à Γ. Il est clair que la restriction de ρ à Γ est $q\rho'$. Comme la restriction de η à P est ρ, on a donc

$$\mathrm{Res}_\Gamma(\eta) = q\rho'.$$

Si ρ' était égal à 1_Γ, le noyau de η contiendrait Γ. Comme Γ est invariant dans G, et comme χ est induit par η, le noyau de χ contiendrait aussi Γ, ce qui est contraire à l'hypothèse.

C. Q. F. D.

7.2.3. *Fin de la démonstration.* — Posons $A_\eta = H_\eta.\Gamma$. Il est clair que A_η est un sous-groupe de type C_p de A_j, que son p-sous-groupe de Sylow est Γ et que le centraliseur A'_η de P dans A est $H'_\rho.\Gamma$. Soit η' le caractère de degré 1 de A'_η défini par

$$\eta'(h') = b' \qquad \text{et} \qquad \mathrm{Res}_\Gamma(\eta') = \rho'.$$

On a vu que b' est un élément de E. Donc η' est à valeurs dans $E(\sqrt[p]{1})$. Soit χ' le caractère de A_η induit par η'. On vérifie immédiatement, à partir de la relation $\mathrm{Res}_\Gamma(\eta) = q\rho'$, que χ' est un caractère absolument irréductible de A à valeurs dans E. La proposition 6.7 montre que $\bar{\varepsilon}_E(\chi') = (\varphi_{\bar{h}}, b')$. On a donc $\bar{\varepsilon}_E(\chi) = \bar{\varepsilon}_E(\chi')$.

C. Q. F. D.

7.3. Décomposition de l'algèbre.

Théorème 5. — *Soit* G *un groupe de type* R_p *et soit* E *un corps de caractéristique* o. *Si* $p = 2$, *on suppose l'algèbre* E[P] *décomposée. Soit* $(A_j)_{j=1, 2, \ldots, \lambda}$ *un système complet de* C_p*-groupes associé à* G. *Les assertions suivantes sont équivalentes :*

(i) *l'algèbre* E[G] *est décomposée;*

(ii) *les algèbres* $E[A_j]$, *pour* $j = 1, 2, \ldots, \lambda$, *sont toutes décomposées.*

Démonstration. — Soit

$$G = \Gamma_0 \supset \Gamma_1 \supset \ldots \Gamma_\lambda \supset \Gamma_{\lambda+1} = \{1\}$$

une C_p-suite associée à G telle que, pour tout j, A_j soit le $j^{\text{ième}}$ terme de la famille de groupes de type C_p correspondants. On peut donc identifier A_j et $H.\Gamma_j/\Gamma_{j+1}$.

Pour tout caractère absolument irréductible χ de G, nous notons $j(\chi)$ le plus petit entier j tel que le noyau de χ soit contenu dans Γ_{j+1}.

7.3.1. *L'implication* (ii) $\Longrightarrow$ (i).

Lemme 2. — *Soient* G_1 *et* G_2 *deux groupes de type* C_p. *Supposons que* $m(G_1)$ *divise* $m(G_2)$ *et que* $d(G_1)$ *divise* $d(G_2)$. *Soit* E *un corps de caractéristique* o *et soit* χ_1 *un caractère absolument irréductible de* G_1 *à valeurs dans* E. *Alors, il existe un caractère absolument irréductible* χ_2 *de* G_2 *à valeurs dans* E *tel que* $\bar{\varepsilon}_E(\chi_2) = \bar{\varepsilon}_E(\chi_1)$.

Démonstration du lemme. — Si $d(G_1)$ divise $d(G_2)$, $(d(G_1), p - 1)$ divise $(d(G_2), p - 1)$ et il résulte de la proposition 6.5 que l'on peut supposer que G_1 et G_2 sont de type CC_p.

(*a*) Si $m(G_2) = m(G_1)$, on peut toujours considérer G_1 comme un sous-groupe de G_2. Soit χ_2 le caractère de G_2 induit par χ_1. Il résulte de la proposition 6.1 que χ_2 est absolument irréductible. Étant induit par χ_1, il est à valeurs dans E et le lemme résulte du corollaire à la proposition 3.1.

(*b*) Si $m(G_2) \neq m(G_1)$, désignons par H'' le sous-groupe cyclique de G_2 d'ordre $m(G_2)/m(G_1)$. Le groupe H'' est invariant dans G_2 et le groupe $\overline{G}_2 = G_2/H''$ est un groupe de type CC_p vérifiant $d(\overline{G}_2) = d(G_2)$ et $m(\overline{G}_2) = m(G_1)$. Il existe donc un caractère absolument irréductible χ_2 de $\overline{G}_2$ à valeurs dans E tel que $\bar{\varepsilon}_E(\chi_2) = \bar{\varepsilon}_E(\chi_1)$. Le lemme résulte alors de ce que ce caractère peut toujours être considéré comme le caractère d'une représentation de G_2 dont le noyau contient H''.

C. Q. F. D.

Soit alors χ un caractère absolument irréductible de G. Posons $j = j(\chi)$ et $E' = E(\chi)$. Si j n'est pas strictement positif, χ est de degré 1 et est rationnel sur E'. Supposons donc $j \geq 1$. D'après la proposition 7.1, il existe un caractère χ' d'un sous-groupe A de A_j, à valeurs dans E', tel que $\bar{\varepsilon}_{E'}(\chi) = \bar{\varepsilon}_{E'}(\chi')$. Comme A est un sous-groupe de A_j, on voit que $d(A)$ divise $d(A_j)$ et que $m(A)$ divise $m(A_j)$. D'après le lemme 2, il existe donc un caractère absolument irréductible χ_j de A_j, à valeurs dans E', tel que $\bar{\varepsilon}_{E'}(\chi_j) = \bar{\varepsilon}_{E'}(\chi')$. Si l'algèbre $E[A_j]$ est décomposée, on en déduit que χ est rationnel sur E', et (ii) implique (i).

7.3.2. *L'implication* (i) $\Rightarrow$ (ii). — Soit j un entier compris entre 1 et λ. Nous voulons montrer que si $E[G]$ est décomposée, $E[A_j]$ l'est aussi. Si $E[G]$ est décomposée, $E[G/\Gamma_{j+1}]$ l'est aussi. On peut donc, quitte à passer au quotient, supposer que $\Gamma_{j+1} = \{1\}$. Posons $d(A_j) = d$ et $m(A_j) = m$.

Lemme 3. — *Soit χ un caractère absolument irréductible de* G *tel que $j(\chi) = j$. Alors le degré de χ est divisible par d.*

Démonstration du lemme. — Reprenons les notations du n° 7.2, et soit H' le centraliseur de Γ dans A_j.

Si t est un élément de H qui n'appartient pas à H', ρ'_t est différent de ρ'. Comme la restriction à Γ de η est $q\rho'$, on voit que η_t est différent de η. Donc, t n'appartient pas à H'_ρ. Par conséquent, H'_ρ est contenu dans H'. Il en résulte que $(H : H')$ divise $(H : H'_\rho)$, d'où le lemme, puisque $d = (H : H')$ et puisque le degré de χ est $q\,(H : H'_\rho)$. C. Q. F. D.

Posons alors $\overline{G} = G/\Gamma$ et soit r (resp. $\bar{r}$) le caractère de la représentation régulière de G (resp. $\overline{G}$). Il est clair que $r - \bar{r}$ est un caractère de G. Soit e (resp. $\bar{e}$) l'ordre de G (resp. $\overline{G}$). Pour tout s dans G, on a

$$(r - \bar{r})(s) = \begin{cases} 0 & \text{si } s \notin \Gamma; \\ -\bar{e} & \text{si } s \in \Gamma - \{1\}; \\ e - \bar{e} & \text{si } s = 1. \end{cases}$$

Pour tout caractère absolument irréductible χ de G, soit d_χ son degré. Soit Y l'ensemble des caractères absolument irréductibles de G dont le noyau ne contient pas Γ. Il est clair que

$$r - \bar{r} = \sum_{\chi \in Y} d_\chi \chi.$$

Posons $\bar{e} = n\bar{e}'$ et $e = ne'$ (n désigne toujours l'indice de P dans G). Les entiers $\bar{e}'$ et e' sont des puissances de p. D'après le lemme 3, pour tout χ dans Y, d_χ est divisible par d. On en déduit que la fonction centrale $\Phi = (r - \bar{r})/d$ est un caractère de G. Ses valeurs sont

$$\Phi(s) = \begin{cases} 0 & \text{si } s \notin \Gamma; \\ -m\bar{e}' & \text{si } s \in \Gamma - \{1\}; \\ m\bar{e}'(e'/\bar{e}' - 1) & \text{si } s = 1. \end{cases}$$

Les valeurs du caractère θ_{A_j} de A_j défini au n° 6.2, sont

$$\theta_{A_j}(s) = \begin{cases} 0 & \text{si } s \notin \Gamma; \\ -m & \text{si } s \in \Gamma - \{1\}; \\ m(e'/\bar{e}' - 1) & \text{si } s = 1. \end{cases}$$

On en déduit que $\mathrm{Res}_{A_j}(\Phi) = \bar{e}'.\theta_{A_j}$. Comme Φ est à valeurs dans $\mathbf{Q}$, si l'algèbre E[G] est décomposée, Φ est rationnel sur E, donc aussi sa restriction à A_j. Comme $\bar{e}'$ est une puissance de p et comme l'indice de Schur sur E de chacun des caractères absolument irréductibles de A_j qui divise θ_{A_j} est premier à p, on en déduit que θ_{A_j} est rationnel sur E. D'après la proposition 6.4, ceci entraîne que l'algèbre E[A_j] est décomposée. Donc, (i) implique (ii). C. Q. F. D.

7.4. Les groupes de type R_2.

Théorème 5′. — *Soit* G *un groupe de type* R_2 *et soit* P *son 2-sous-groupe de Sylow. Soit* E *un corps de caractéristique* 0. *Les assertions suivantes sont équivalentes :*

(i) *l'algèbre* E[G] *est décomposée;*

(ii) *l'algèbre* E[P] *est décomposée.*

Démonstration. — Si A est un groupe de type C_2, l'algèbre E[A] est décomposée. Le théorème 5 montre donc que (ii) implique (i).

Soit $n = (G : P)$ et soit ρ un caractère absolument irréductible de P. Soit G'_ρ le sous-groupe d'isotropie de ρ (pour l'action naturelle de G sur l'ensemble des caractères de P). Soit $m = (G' : P)$. L'entier m divise n et est donc impair.

Soit $E' = E(\rho)$ et soit ρ^* le caractère de G induit par ρ. Le caractère ρ^* est un caractère de G à valeurs dans E′. Si l'algèbre E[G] est décomposée, il est donc rationnel sur E′. Il est clair que $(\mathrm{Res}_P(\rho^*), \rho) = m$. Comme ρ est à valeurs dans E′, on en déduit que $m\rho$ est rationnel sur E′. Comme l'indice de Schur de ρ est 1 ou 2, et comme m est impair, on voit que ρ est rationnel sur E′. C. Q. F. D.

8. Appendice : Théorème de Witt et applications.

8.1. Théorème de Witt. — Soit n un entier strictement positif et soit E un corps de caractéristique o. Soit ν une racine primitive $n^{\text{ième}}$ de l'unité. Soit $I_E(n)$ le groupe multiplicatif des entiers i modulo n tels que l'application $\nu \mapsto \nu^i$ définisse un automorphisme de $\mathbf{Q}(\nu)$ qui laisse fixe $\mathbf{Q}(\nu) \cap E$. Le groupe $I_E(n)$ est canoniquement isomorphe au groupe de Galois de l'extension $E(\nu)/E$.

Soit G un groupe fini et soit a un élément d'ordre n de G. On pose

$$N_E(a) = \{ g \in G \mid \exists\, i \in I_E(a) : gag^{-1} = a^i \}.$$

Le groupe G est dit E-*élémentaire, relativement au nombre premier* p, si c'est le produit semi-direct d'un p-groupe P par un groupe cyclique invariant $A = \langle a \rangle$ dont l'ordre n est premier à p et si $G = N_E(a)$.

Witt a obtenu le résultat suivant (*cf.* [13], Satz 9) :

Théorème de Witt. — *Soit* G *un groupe fini d'exposant* n. *Soit* p *un nombre premier et soit* E *un corps de nombres tel que le degré de l'extension* $E(\sqrt[n]{1})/E$ *soit une puissance de* p. *Soit* χ *un caractère absolument irréductible de* G *à valeurs dans* E. *Alors*

(i) *il existe un sous-groupe* H *de* G *qui est* E-*élémentaire relativement à* p *et un caractère absolument irréductible* ξ *de* H *à valeurs dans* E, *tels que* $(\mathrm{Res}_H(\chi), \xi) \not\equiv 0 \pmod{p}$;

(ii) *pour tout sous-groupe* H *de* G *et pour tout caractère absolument irréductible* ξ *de* H *à valeurs dans* E *tels que* $(\mathrm{Res}_H(\chi), \xi) \not\equiv 0 \pmod{p}$, *on a* $\bar{\varepsilon}_E(\chi) = \bar{\varepsilon}_E(\xi)$.

Remarque. — En fait, Witt énonce ce théorème sous une forme moins précise, mais c'est ce qu'il démontre. On trouvera une autre démonstration de l'assertion (i) dans un article de Solomon ([12], lemma 6, p. 154). Comme χ et ξ sont rationnels sur $E(\sqrt[n]{1})$ et comme $E(\sqrt{1})/E$ est une p-extension, les ordres de $\bar{\varepsilon}_E(\chi)$ et de $\bar{\varepsilon}_E(\xi)$ sont des puissances de p. On voit que l'assertion (ii) n'est qu'un cas particulier de la proposition 3.1.

8.2. Applications. — Supposons que l'on sache calculer $\bar{\varepsilon}_E(\chi)$ lorsque E est un corps de nombres contenant les valeurs de χ. Si E est un corps quelconque de caractéristique o contenant les valeurs de χ, E peut être considéré comme une extension de $\mathbf{Q}(\chi)$ et il est clair que $\bar{\varepsilon}_E(\chi)$ est la restriction à E de $\bar{\varepsilon}_{\mathbf{Q}(\chi)}(\chi)$.

Soit E un corps de nombres contenant les valeurs de χ. Comme un groupe E-élémentaire est hyper-résoluble, il résulte de la proposition 3.4 que tout caractère absolument irréductible, à valeurs dans E, d'un groupe E-élémentaire, est induit par un caractère E-métabélien. Le théorème de Witt fournit donc un moyen de calculer $\bar{\varepsilon}_E(\chi)$ lorsque $E(\sqrt[n]{1})/E$ est une p-extension.

Si E est un corps de nombres quelconque, pour tout nombre premier p, on peut construire une extension E′ de E contenue dans $E(\sqrt[n]{1})$ de degré m premier à p, telle que $E(\sqrt[n]{1})/E'$ soit une p-extension. Soit p^r le degré de l'extension $E(\sqrt[n]{1})/E'$ et soit m' un entier tel que $mm' \equiv 1 \pmod{p^r}$. Il est clair que la p-composante de $\bar{\varepsilon}_E(\chi)$ est $(\mathrm{Cor}_E(\bar{\varepsilon}_{E'}(\chi)))^{m'}$, en désignant par Cor_E l'application de correstriction de E′ à E. Le théorème résout donc le problème de la détermination de $\bar{\varepsilon}_E(\chi)$ dans tous les cas.

De plus, il résulte du théorème 3 que $\bar{\varepsilon}_{E'}(\chi)$ est un élément de $H^2_\mu(E(\sqrt[n]{1})/E')$. Il provient d'un élément de $H^2(E(\sqrt[n]{1})/E', \mu)$. Sa correstriction provient donc d'un élément de $H^2(E(\sqrt[n]{1})/E, \mu)$ et est, par conséquent, un élément de $H^2_\mu(E(\sqrt[n]{1})/E)$. Il en est évidemment de même de sa puissance $(m')^{\text{ième}}$. On voit que chaque p-composante de $\bar{\varepsilon}_E(\chi)$ est un élément de $H^2_\mu(E(\sqrt[n]{1})/E)$, donc $\bar{\varepsilon}_E(\chi)$ aussi. Il est clair (par restriction) que ce résultat reste vrai lorsque E est un corps de caractéristique o contenant les valeurs de χ, quelconque. On a donc démontré le résultat suivant :

PROPOSITION 8.1. — *Soit* G *un groupe fini d'exposant n et soit* E *un corps de caractéristique* o. *Soit* χ *un caractère absolument irréductible de* G *à valeurs dans* E. *Alors* $\bar{\varepsilon}_E(\chi)$ *est un élément de* $H^2_\mu(E(\sqrt[n]{1})/E)$ (*en particulier, on voit que c'est un élément du groupe de Brauer cyclotomique de* E).

COROLLAIRE 1. — *Soit* G *un groupe fini d'ordre premier à p. L'algèbre* $\mathbf{Q}_p[G]$ *est décomposée.*

En effet, l'extension $\mathbf{Q}_p(\sqrt[n]{1})/\mathbf{Q}_p(\chi)$ est non ramifiée et, d'après la proposition 1.2, $H^2_\mu(\mathbf{Q}_p(\sqrt[n]{1})/Q_p(\chi)) = 1$.

COROLLAIRE 2. — *Soit* G *un groupe fini et soit* χ *un caractère absolument irréductible de* G. *Alors :*

(i) *pour* $p \neq 2$, $m_{\mathbf{Q}_p}(\chi)$ *divise le degré de l'extension* $\mathbf{Q}_p(\sqrt[p]{1}, \chi)/\mathbf{Q}_p(\chi)$; *en particulier,* $m_{\mathbf{Q}_p}(\chi)$ *divise* $p - 1$.

(ii) *Pour* $p = 2$, $m_{\mathbf{Q}_2}(\chi)$ *divise le degré de l'extension* $\mathbf{Q}_2(\sqrt{-1}, \chi)/\mathbf{Q}_2(\chi)$; *en particulier,* $m_{\mathbf{Q}_2}(\chi)$ *divise* 2.

Ces assertions résultent, trivialement, des théorèmes 1 et 1′.

COROLLAIRE 3. — *Soit* G *un groupe fini et soit* χ *un caractère absolument irréductible de* G. *Alors :*

(i) *Si* G *est un 2-groupe,* $m_{\mathbf{Q}}(\chi)$ *divise* 2;

(ii) *Si* G *n'est pas un 2-groupe,* $m_{\mathbf{Q}}(\chi)$ *divise le* ppcm *des entiers* $p-1$, *pour* p *premier divisant l'ordre de* G.

En effet, soit $E = \mathbf{Q}(\chi)$. L'entier $m_{\mathbf{Q}}(\chi)$ est le ppcm de tous les $m_{E_\mathfrak{p}}(\chi)$ pour tous les complétés $E_\mathfrak{p}$ de E. Si $\mathfrak{p}$ est une place infinie ou au-dessus de 2, $m_{E_\mathfrak{p}}(\chi)$ divise 2. Si $\mathfrak{p}$ est une place au-dessus d'un nombre premier p différent de 2, $m_{E_\mathfrak{p}}(\chi)$ divise $p-1$ d'après le corollaire 2; il est égal à 1 si p est premier à l'ordre de G, d'après le corollaire 1. Le corollaire 3 est alors évident.

BIBLIOGRAPHIE.

[1] E. ARTIN et J. TATE, *Class field theory*, New York, Benjamin, 1967.

[2] R. BRAUER, *On the algebraic structure of group rings* (*J. Math. Soc. Japan*, t. 3, 1951, p. 237-251).

[3] A. H. CLIFFORD, *Representations induced in an invariant subgroup* (*Ann. of Math.*, t. 38, 1937, p. 533-550).

[4] M. DEURING, *Algebren*; zweite, korrigierte Auflage, Berlin, Springer, 1968.

[5] W. FEIT, *Characters of finite groups*, New York, Benjamin, 1967.

[6] J.-M. FONTAINE, *Rationalité des représentations d'Artin et de Swan* (*C. R. Acad. Sc.*, t. 270, série A, 1970, p. 93-95).

[7] P. ROQUETTE, *Realisierung von Darstellungen endlicher nilpotenter Gruppen* (*Arch. Math.*, t. 9, 1958, p. 241-250).

[8] J.-P. SERRE, *Applications algébriques de la cohomologie des groupes.* II : *Théorie des algèbres simples* (*Séminaire H. Cartan*, 3e année, 1950-1951, exp. 6 et 7).

[9] J.-P. SERRE, *Corps locaux*, Paris, Hermann, 1968 (cité CL).

[10] J.-P. SERRE, *Sur les corps locaux à corps résiduel algébriquement clos* (*Bull. Soc. math. Fr.*, t. 89, 1961, p. 105-154).

[11] J.-P. SERRE, *Sur la rationalité des représentations d'Artin* (*Annals of Math.*, t. 72, 1960, p. 405-420).

[12] L. SOLOMON, *The representation of finite groups in algebraic number fields* (*J. Math. Soc. Japan*, t. 13, 1961, p. 144-164).

[13] E. WITT, *Die algebraische Struktur des Gruppenringes einer endlichen Gruppe über einem Zahlkörper* (*J. reine ang. Math.*, t. 190, 1952, p. 231-245).

[14] T. YAMADA, *On the group algebras of metacyclic groups over algebraic number fields* (*J. fac. Sci. Univ. Tokyo*, t. 15, 1968, p. 179-198).

[15] T. YAMADA, *On the group algebras of metabelian groups over algebraic number fields* (I : *Osaka J. Math.*, t. 6, 1969, p. 211-228 et II : *J. fac. Sci. Univ. Tokyo*, t. 16, 1969, p. 83-90).

[16] T. YAMADA, *On the Schur index of a monomial representation* (*Proc. Jap. Ac.*, t. 45, n° 7, 1969, p. 522-525).

(Manuscrit reçu le 19 janvier 1971.)

Jean-Marc FONTAINE,
27, avenue Émile-Zola,
75-Paris, 15e.