

SÉMINAIRE HENRI CARTAN

J-P. SERRE

**Applications algébriques de la cohomologie des groupes.
II : théorie des algèbres simples**

Séminaire Henri Cartan, tome 3 (1950-1951), exp. n° 7, p. 1-11

http://www.numdam.org/item?id=SHC_1950-1951__3__A7_0

© Séminaire Henri Cartan

(Secrétariat mathématique, Paris), 1950-1951, tous droits réservés.

L'accès aux archives de la collection « Séminaire Henri Cartan » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

Séminaire H. CARTAN,
E.N.S., 1950/51 . Topologie algébrique.

APPLICATIONS ALGÈBRIQUES DE LA COHOMOLOGIE DES GROUPES. II :

THÉORIE DES ALGÈBRES SIMPLES

(2ème exposé de J-P. SERRE, le 15.1.1951)

7.- Le théorème de Skolem-Noether.

Théorème 8.- Soit A une algèbre simple finie et centrale sur k ; soient f et g deux k -isomorphismes d'une algèbre simple B dans A . Il existe alors un élément inversible $x \in A$, tel que $f(b) = x.g(b).x^{-1}$ pour tout $b \in B$.

Si A est une algèbre de matrices sur k , le théorème précédent signifie que deux représentations matricielles de B de même degré sont isomorphes, ce qui a déjà été démontré (Cor.2 au théorème 2).

Dans le cas général, soit A° l'algèbre opposée de A ; formons $B \otimes A^\circ$ et $A \otimes A^\circ$, et prolongeons f et g en des isomorphismes f' et g' de la première algèbre dans la seconde, en posant :

$$f'(b \otimes a) = f(b) \otimes a \quad , \quad g'(b \otimes a) = g(b) \otimes a \quad (b \in B \quad , \quad a \in A^\circ) .$$

Comme $A \otimes A^\circ$ est une algèbre de matrices sur k (Cor.2 au théorème 4) , il existe, d'après la première partie de la démonstration, un $x \in A \otimes A^\circ$ tel que :

$$f'(b \otimes a) = x.g'(b \otimes a).x^{-1} .$$

Si l'on prend $b = 1$, on voit que x permute avec les éléments de la forme $1 \otimes a$ ($a \in A^\circ$) , donc appartient à $A \otimes 1$ (Lemme 4) , et on peut l'écrire $x \otimes 1$, avec $x \in A$. On a alors :

$$f(b) = x.g(b).x^{-1} \quad , \quad \text{c.q.f.d.}$$

Corollaire - Tout k -automorphisme d'une algèbre simple finie et centrale sur k est un automorphisme intérieur.

8.- La commutation dans les algèbres simples.

Théorème 9.- Soit A une algèbre simple, finie et centrale sur k . Soit B une sous-algèbre simple de A , C le commutant de B dans A . Alors C est simple, B est le commutant de C , $[B : k].[C : k] = [A : k]$.

Désignons par E l'algèbre B considérée comme k -espace vectoriel, et

soit $L(E)$ l'algèbre des k -endomorphismes de E . On peut faire opérer B sur E par les translations à gauche : cela revient à plonger B isomorphiquement dans $L(E)$. On sait que le commutant de B dans $L(E)$ n'est autre que l'algèbre des translations à droite de E , isomorphe à B° .

Ceci étant, considérons l'algèbre simple $A \otimes L(E)$. On peut y plonger B de deux façons : par $B \otimes 1$, et par $1 \otimes B$. Le commutant de $B \otimes 1$ est $C \otimes L(E)$, et celui de $1 \otimes B$ est $A \otimes B^\circ$ (lemme 4).

Mais d'après le théorème 8, il existe un automorphisme intérieur de $A \otimes L(E)$ qui transforme $B \otimes 1$ en $1 \otimes B$; cet automorphisme transforme donc aussi les commutants de ces deux algèbres l'un dans l'autre, et, en particulier, ces deux algèbres sont isomorphes.

Il en résulte d'abord que $C \otimes L(E)$ est simple puisque $A \otimes B^\circ$ l'est, donc C est simple.

D'autre part : $[C \otimes L(E) : k] = [C : k][B : k]^2$ et :

$$[A \otimes B^\circ : k] = [A : k][B : k] .$$

D'où : $[A : k] = [B : k][C : k]$.

Si B' désigne le commutant de C dans A , on a $B' \supset B$. Mais d'après ce qui vient d'être démontré : $[A : k] = [C : k][B' : k]$, d'où $[B : k] = [B' : k]$ et $B' = B$.

Corollaire 1 - Si B est centrale sur k , B et C sont linéairement disjoints sur k , et $A = B \otimes C$.

Les centres de B et de C sont égaux à $B \cap C$, donc sont réduits à k . L'algèbre $B \otimes C$ est donc simple et centrale sur k , et l'homomorphisme canonique de cette algèbre sur le produit de B et de C dans A est un isomorphisme. Comme $B \otimes C$ et A ont même dimension, cet isomorphisme applique $B \otimes C$ sur A .

Corollaire 2 - Soit L un sous-corps commutatif d'une algèbre A simple, finie et centrale sur k . Pour que L soit son propre commutant dans A il faut et il suffit que $[A : k] = [L : k]^2$ ou que L soit sous-anneau commutatif maximal de A .

Soit L' le commutant de L dans A ; puisque L est commutatif, $L' \supset L$. D'après le théorème 9, il est clair que $L' = L$ équivaut à :

$$[L : k]^2 = [A : k] .$$

D'autre part, si $L' = L$, tous sous-anneau commutatif de A contenant L est dans L' , donc est confondu avec L , et L est sous-anneau commutatif maximal de A . Réciproquement s'il en est ainsi, tout élément commutant avec L est dans L , et $L' = L$.

Corollaire 3 - Tout sous-corps commutatif maximal L d'un corps gauche D est tel que $[L : k]^2 = [D : k]$.

Résulte du corollaire précédent et du fait que tout sous-anneau de D est un sous-corps.

9.- Le critère de décomposition.

Soit k un corps commutatif, G_k le groupe de Brauer de k , W un élément de G_k , c'est-à-dire une classe d'algèbres simples, finies et centrales sur k . Si L est une extension de k , rappelons que L est dit corps de décomposition de W si l'image canonique de W dans G_L est o .

Théorème 10.- Les deux conditions suivantes sont équivalentes :

- a) L est un corps de décomposition de W ;
- b) Il existe $A \in W$, avec $L \subset A$ et $[A : k] = [L : k]^2$.

a) $\Rightarrow$ b) - Soit $B \in W$; puisque L est corps de décomposition de B , il l'est aussi de B° et $B^\circ \otimes L$ est une algèbre de matrices sur L , ou encore l'algèbre $L(E_L)$ des endomorphismes d'un L -espace vectoriel E_L . Soit $L(E)$ l'algèbre des k -endomorphismes de E_L . L'algèbre $B^\circ \otimes L$ se trouve donc plongée dans $L(E)$, et son algèbre commutante est L (c'est ce qui exprime le fait que $B^\circ \otimes L$ est l'algèbre des L -endomorphismes de E_L). Soit A l'algèbre commutante de B° dans $L(E)$. Je dis que A répond aux conditions imposées.

Tout d'abord, il est clair que A contient L , et que A est une algèbre simple. En outre $[B : k].[A : k] = [L(E) : k] = [B^\circ \otimes L : k].[L : k]$, d'où

$$[A : k] = [L : k]^2.$$

Enfin, d'après le corollaire 1 au théorème 9, A est centrale sur k et $B^\circ \otimes A = L(E)$; ceci montre que la classe de A est l'opposée de celle de B° , donc est W .

b) $\Rightarrow$ a) - Il suffit de montrer que A est décomposée par L . Pour cela, remarquons que, d'après le corollaire 2 au théorème 4, $A \otimes A^\circ = L(E)$, algèbre des k -endomorphismes de l'espace vectoriel E . Plongeons L dans A° ; son commutant dans $L(E)$ est alors $A \otimes L$. Mais ceci signifie que $A \otimes L$

est l'algèbre des L -endomorphismes de E , et W est bien décomposée par L .

Corollaire 1 - Tout sous-corps commutatif maximal d'un corps gauche D est corps de décomposition de D .

Résulte immédiatement du Corollaire 3 au théorème 9.

Corollaire 2 - Soit D un corps gauche, et posons $[D : k] = r^2$. Pour tout corps de décomposition L de D , $[L : k]$ est un multiple de r .

L'algèbre A du théorème précédent est une algèbre de matrices d'ordre n sur D . On a donc : $[A : k] = n^2 r^2$, d'où $[L : k] = nr$.

Remarque : Il ne faudrait cependant pas croire que tout corps de décomposition de D contient un sous-corps commutatif maximal de D , ni que les sous-corps commutatifs maximaux de D sont isomorphes.

10.- Existence de corps de décomposition galoisiens.

Lemme - Soit D un corps gauche fini sur son centre k , et distinct de k . Il existe un sous-corps commutatif M de D , contenant k , séparable sur k , et distinct de k .

Sinon tout élément de D serait radiciel sur k , c'est-à-dire vérifierait la condition :

$$x^{(p^e)} \in k \quad \text{pour au moins un } e.$$

D étant fini sur k , on voit tout de suite qu'il existe un entier e tel que l'équation précédente ait lieu pour tout $x \in D$.

Soit alors e_i une base de D sur k , telle que $e_1 = 1$. Si l'on écrit un élément $x \in D$ sous la forme : $x = \sum_i x_i e_i$, l'élément : $x^{(p^e)}$ s'écrit sous la forme :

$$x^{(p^e)} = \sum_j P_j(x_i) e_j.$$

où les P_j sont

des polynômes par rapport aux x_i dont les coefficients s'expriment au moyen des éléments de la table de multiplication de D . Par hypothèse, on a $P_j(x_i) = 0$ ($j \neq 1$) pour tout système de valeurs des x_i . Comme on peut supposer que k est infini (puisque toute extension finie d'un corps fini est séparable), ceci montre que les P_j ($j \neq 1$) sont tous identiquement nuls.

Mais alors, on aura encore la même condition : $x^{(p^e)} \in k$ lorsqu'on étendra le corps de base. En particulier, étendons-le à une clôture algébrique de k , on obtiendra une algèbre de matrices qui contient des idempotents

x , qui mettent en défaut le résultat précédent. Ceci achève la démonstration.

Théorème 11.- Tout corps gauche D , fini sur son centre k , contient un sous-corps commutatif maximal qui est séparable sur k .

Soit L un sous-corps séparable maximal de D . Montrons que L est un sous-corps commutatif maximal de D ; pour cela, soit D' le commutant de L dans D . D' est un corps gauche, de centre L . S'il n'était pas confondu avec L , il y aurait, d'après le lemme, un corps L' , avec $L \subset L' \subset D'$, $L' \neq L$, et L' séparable sur L . Mais alors L' serait séparable sur k , ce qui est contraire au caractère maximal de L . Il en résulte que $D' = L$, et L est bien sous-corps commutatif maximal de D .

Corollaire - Tout $W \in G_k$ admet un corps de décomposition qui est galoisien sur k .

Il suffit de le voir pour un corps gauche D . Or, d'après le théorème 11 et le Corollaire au théorème 10, D admet un corps de décomposition L qui est séparable sur k . Si L' désigne une extension galoisienne quelconque de k qui contienne L (et il y en a) , L' est a fortiori corps de décomposition de D .

11.- Correspondance entre algèbres simples et extensions de groupes.

Soit k un corps, L une extension galoisienne et finie de k ; nous allons étudier le sous-groupe $H_{k,L}$ de G_k formé des classes d'algèbres simples centrales et finies sur k qui admettent L pour corps de décomposition.

Soit G le groupe de Galois de L/k , L^* le groupe multiplicatif des éléments non nuls de L . Le groupe G opère sur L^* , et on peut définir le groupe $Q(G, L^*)$ des extensions de L^* par G (Voir Exposé 5) .

Théorème 12.- Les groupes $H_{k,L}$ et $Q(G, L^*)$ sont isomorphes.

Ce théorème sera démontré dans ce numéro et le suivant.

Nous allons commencer par définir une application $u : H_{k,L} \longrightarrow Q(G, L^*)$. Si $W \in H_{k,L}$, il existe d'après le théorème 10 une algèbre $A \in W$ contenant L et telle que $[A : k] = [L : k]^2$. Cette algèbre est donc bien déterminée, à un k -isomorphisme près. Plongeons L dans A , ce que nous savons être possible, et soit E l'ensemble des éléments inversibles de A qui définissent des automorphismes intérieurs laissant stable L . Autrement

dit, $x \in E$ signifie que $x.L.x^{-1} = L$.

Un tel élément définit un automorphisme de L/k , c'est-à-dire un élément $g \in G$. Je dis que la suite :

$$1 \longrightarrow L^* \longrightarrow E \longrightarrow G \longrightarrow 1$$

est exacte (les deux homomorphismes étant, le premier, l'injection de L^* dans E , et le second, celui qui vient d'être défini). Il y a deux choses à vérifier :

a) que $E \longrightarrow G$ est sur. Ceci signifie que tout k -automorphisme de L peut être prolongé en un automorphisme intérieur de A , ce qui résulte du théorème 8.

b) que le noyau de $E \longrightarrow G$ n'est autre que L^* . Ceci signifie que les seuls éléments de E qui commutent avec L^* sont les éléments de L^* , ce qui résulte du Corollaire² au théorème 9.

Le groupe E définit donc bien un élément $u(W) \in Q(G, L^*)$. Il faut encore vérifier que cet élément ne dépend pas de la façon dont on a plongé L dans A , ce qui résulte tout de suite du théorème 8.

Lemme - L'application $u : H_{k,L} \longrightarrow Q(G, L^*)$ est un homomorphisme.

(Nous utiliserons la définition de la multiplication dans $Q(G, L^*)$ qui a été donnée par Baer - Voir Appendice).

Soient $W, W', W'' = W + W' \in H_{k,L}$, et soient $B \in W, B' \in W'$, et $B \otimes B' \in W''$.

Les algèbres $B^0 \otimes L$ et $B'^0 \otimes L$ sont isomorphes aux algèbres des L -endomorphismes des espaces vectoriels sur L, V et V' . Il en résulte que $B^0 \otimes B'^0 \otimes L$ est isomorphe à l'algèbre des L -endomorphismes de $V \otimes V' = V''$.

Cherchons les algèbres A, A', A'' , telles que $A \in W, A' \in W', A'' \in W''$ et que $[A : k] = [A' : k] = [A'' : k] = [L : k]^2$. D'après la démonstration du théorème 10, on peut les obtenir en prenant les k -endomorphismes de V, V' et V'' qui commutent avec $B^0, B'^0, B^0 \otimes B'^0$ respectivement.

Désignons par E, E', E'' les éléments inversibles de A, A', A'' qui définissent des automorphismes intérieurs respectant L . Soit $u \in E, \lambda \in L, x \in V$, et notons λ^E le transformé de λ par l'image de u dans G , groupe de Galois de L/k . Par définition on a :

$$u \lambda u^{-1} = \lambda^g .$$

En appliquant ceci au vecteur $u(x)$, on obtient : $u(\lambda x) = \lambda^g u(x)$, ce qui exprime que u est semi-linéaire relativement à g . On peut donc donner une autre caractérisation de E : E est formé des automorphismes semi-linéaires de V qui permutent avec B^0 . Idem pour E' et E'' .

Soient alors $u \in E$, $u' \in E'$, définissant le même élément $g \in G$. On peut définir l'opérateur $u \otimes u'$ sur $V \otimes V'$ par la formule :

$$(u \otimes u')(x \otimes x') = u(x) \otimes u'(x') .$$

Soit (E, E') le sous-groupe de $E \times E'$ formé des éléments ayant même projection sur G . La correspondance $(u, u') \longrightarrow u \otimes u'$ définit un homomorphisme de (E, E') dans E'' , car on voit tout de suite que les automorphismes $u \otimes u'$ sont semi-linéaires relativement au même g , et commutent avec $B^0 \otimes B'^0$. Soit E_1 l'image de (E, E') par cette application. E_1 contient évidemment les homothéties par les éléments de L^* , et, pour tout $g \in G$, contient des éléments g -semi-linéaires. Il en résulte que $E_1 = E''$. D'autre part, le noyau de $(E, E') \longrightarrow E''$ contient les couples (λ, λ^{-1}) , $\lambda \in L^*$, et rien d'autre comme on le voit immédiatement. Il s'ensuit que E'' est obtenu à partir de E et E' par le procédé de Baer, ce qui achève la démonstration.

12.- Construction d'un produit croisé.

Nous allons maintenant procéder en sens inverse et définir une application $v : Q(G, L^*) \longrightarrow H_{k,L}$.

Pour cela, soit donnée une suite exacte :

$$1 \longrightarrow L \longrightarrow E \longrightarrow G \longrightarrow 1 .$$

Nous allons construire à partir de là une algèbre A , dite produit croisé de L/k par E .

Construction - Soit $Z(E)$ l'algèbre de E sur l'anneau Z des entiers ; Tout élément $z \in Z(E)$ peut s'écrire d'une et d'une seule façon sous la forme :

$$z = \sum_x n_x X_x , n_x \in Z , x \in E .$$

En particulier, les éléments X_λ sont définis si $\lambda \in L^*$.
Considérons l'idéal bilatère u engendré par :

$$(1) \quad \begin{cases} X_\lambda + X_\mu - X_{\lambda+\mu} & \lambda, \mu, \lambda+\mu \in L^* \\ X_\lambda + X_{-\lambda} & \lambda \in L^* \end{cases}$$

Théorème 13. - L'anneau quotient $A = Z(E)/\mathcal{A}$ contient L et a pour centre k ; en outre c'est une algèbre simple sur k , vérifiant la condition : $[A : k] = [L : k]^2$.

Nous remarquerons d'abord que $\mathcal{A}$ est identique à l'idéal à gauche engendré par les éléments de la forme (1). En effet, on a :

$$(X_\lambda + X_{-\lambda}) X_x = X_x \cdot (X_{x^{-1}\lambda x} + X_{-x^{-1}\lambda x}) \quad \text{et}$$

$$(X_\lambda + X_\mu - X_{\lambda+\mu}) \cdot X_x = X_x \cdot (X_{x^{-1}\lambda x} + X_{x^{-1}\mu x} + X_{x^{-1}(\lambda+\mu)x}) .$$

Maintenant, soit $g \in G$, et notons I_g l'ensemble des $x \in E$ se projetant sur g , M_g le sous-groupe de $Z(G)$ engendré par les éléments de I_g , N_g l'image de M_g dans $A = Z(E)/\mathcal{A}$.

$Z(E)$ est somme directe des M_g , $g \in G$. Je dis que $\mathcal{A}$ est aussi somme directe des $\mathcal{A} \cap M_g$. Il suffit de voir que $\mathcal{A}$ est engendré par les $\mathcal{A} \cap M_g$. Or $\mathcal{A}$ est engendré par les produits des X_x et des éléments de la forme (1) ; comme chacun de ces produits est contenu dans un M_g , il en résulte que $\mathcal{A}$ est bien engendré (en tant que groupe abélien) par ceux de ses éléments qui sont dans l'un des M_g . Il en résulte que A est somme directe des N_g , $g \in G$. Nous allons déterminer ces N_g .

Tout élément de M_g est congru modulo $\mathcal{A}$ à 0 ou à un X_x , $x \in I_g$. Il suffit de le voir pour $X_x + \varepsilon X_y$, avec $\varepsilon = \pm 1$. Or $y = \lambda x$, $\lambda \in L^*$, et on a donc :

$$X_x + \varepsilon X_y \equiv X_{(1+\varepsilon\lambda)x} \quad \text{mod. } \mathcal{A} \quad \text{si } 1 + \varepsilon\lambda \neq 0 , \text{ et}$$

$$X_x + \varepsilon X_y \equiv 0 \quad \text{mod. } \mathcal{A} \quad \text{si } 1 + \varepsilon\lambda = 0 .$$

Montrons qu'une telle représentation est unique : soit $x_0 \in I_g$ et écrivons tout $y \in I_g$ sous la forme : $y = \lambda_y \cdot x_0$, $\lambda_y \in L^*$. A tout $z \in M_g$ faisons correspondre un élément $u(z) \in L$, en prolongeant par linéarité l'application : $U_y \rightarrow \lambda_y$. Un calcul immédiat montre que $u(z)$ est nul pour tout $z \in \mathcal{A} \cap M_g$. Il en résulte que $u(z)$ prend la même valeur pour deux éléments z , z' congrus modulo $\mathcal{A}$. En appliquant cela à U_x et $U_{x'}$, $x \neq x'$, on voit que x et x' ne sont pas congrus mod. $\mathcal{A}$, et ne sont

pas non plus congrus à 0 . D'où l'unicité cherchée. Nous avons donc démontré ceci :

A est somme directe des N_g ; chaque N_g peut être considéré comme la réunion de I_g et d'un élément noté 0 . L'addition est définie dans N_g par transport par translation à partir de l'addition de L . La multiplication est celle de E .

(On aurait pu prendre ce qui précède pour définition de A) .

En particulier, les éléments de N_1 forment un sous-anneau de A isomorphe à L , et on a : $[A : k] = [L : k] \cdot (\text{ordre de } G) = [L : k]^2$.

L est son propre commutant dans A , et k est le centre de A .

Reste à voir que A est simple. Pour cela, soit u_g ($g \in G$) un élément quelconque $\neq 0$ de N_g . Les u_g forment une base de A considéré comme L -espace vectoriel à gauche. Si m est un idéal bilatère de A , soit $x = \sum_g \lambda_g u_g$ un élément primordial de m par rapport aux u_g . Soit $\mu \in L$, et formons $x \cdot \mu \in m$. On a :

$$x \cdot \mu = \sum_g \lambda_g \cdot u_g \cdot \mu = \sum_g \lambda_g \cdot \mu^g \cdot u_g .$$

D'après les propriétés des éléments primordiaux, il en résulte que μ^g ne dépend pas de g , lorsque g est tel que $\lambda_g \neq 0$. Ceci exige qu'il n'y ait qu'un seul g jouissant de cette propriété, et l'élément u_g correspondant est alors dans m . Comme u_g est inversible, $m = A$, c.q.f.d.

Le théorème précédent nous permet de définir une application canonique : $v : Q(G, L^*) \rightarrow H_{k,L}$.

On a : $u \circ v = 1$.

Ceci signifie que lorsqu'on fait la construction précédente, et que l'on prend dans A l'ensemble des éléments définissant des automorphismes intérieurs respectant L , on retrouve la suite exacte dont on était parti. C'est bien évident.

On a : $v \circ u = 1$.

Soit A une algèbre simple et centrale sur k , contenant L , et telle que $[A : k] = [L : k]^2$. Elle définit une suite exacte, à partir de laquelle on définit une algèbre A' . Il faut montrer que A' est isomorphe à A .

En effet, l'application canonique de E dans A définit un homomorphisme canonique : $Z(E) \rightarrow A$. Dans cet homomorphisme les éléments du type

(1) donnent 0, donc on définit par passage au quotient un homomorphisme : $A' \rightarrow A$, qui prolonge $E \rightarrow A$. Comme A' est simple, cet homomorphisme est un isomorphisme, et, comme A et A' ont même dimension sur k , l'image de cet isomorphisme est A .

La démonstration du théorème 12 est donc achevée.

13.- Exemples.

On a montré dans l'exposé 5 que $Q(G, L^*) = H^2(G, L^*)$. On a donc :

Théorème 14.- Le groupe $H_{k,L}$ est isomorphe au second groupe de cohomologie $H^2(G, L^*)$ de G à valeurs dans le groupe multiplicatif de L .

Corollaire - Tout élément de G_k est d'ordre fini.

En effet, il suffit de montrer que tout élément de $H_{k,L}$ est d'ordre fini si L est une extension galoisienne de L . Or, on a vu dans l'exposé 5 que tout élément de $H^1(G, A)$ était d'ordre inférieur à n , nombre d'éléments de G .

Remarque : En fait, on peut, au moyen des systèmes de facteurs de Brauer, donner un résultat plus précis : si $W \in G$, et si D est le corps gauche contenu dans W , on a : $r.W = 0$, en désignant par r l'entier tel que $[D : k] = r^2$.

Examinons plus particulièrement le cas où G est cyclique. On sait que, si A est un groupe sur lequel opère G , on a :

$$H^2(G, A) = A'/A'',$$

où A' désigne le sous-groupe de A formé des $a \in A$ tels que $g.a = a$ pour tout $g \in G$, et où A'' désigne le sous-groupe de A formé des $\sum_{g \in G} g.a$.

Dans le cas qui nous intéresse ici, c'est-à-dire $A = L^*$; on a $A' = k^*$, et $A'' = N_{L/k}(L^*)$, groupe multiplicatif des normes des éléments de L^* . On a donc :

Théorème 15.- Si le groupe de Galois de G/k est cyclique, on a :

$$H_{k,L} = k^*/N_{L/k}(L^*)$$

Corollaire 1 - Tout corps fini est commutatif.

Ceci veut dire que $G_k = 0$ si k est fini ; il suffit de voir que $H_{k,L} = 0$ pour toute extension finie de k . Mais L est alors cyclique sur k , et tout élément de k^* est norme d'un élément de L^* (Bourbaki, Alg.V, paragraphe 11). Le corollaire en résulte immédiatement.

Corollaire 2 - $G_R = Z_2$.

En effet, la seule extension galoisienne du corps des réels est $\mathbb{C}$, et l'on a $N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}) = \mathbb{R}_+$. Comme $\mathbb{R}^*/\mathbb{R}_+^* = \mathbb{Z}_2$, ceci démontre le corollaire.

Corollaire 3 - Tout corps gauche sur les réels est isomorphe au corps des quaternions.

Résulte immédiatement du Corollaire 2.

APPENDICE - Multiplication de Baer.

Ceci est un complément à l'exposé 5, numéro 3.

Soient E, E' deux extensions d'un même groupe abélien A par un même groupe G ; on suppose en outre que G opère de la même façon sur A dans les deux cas. On va construire une extension E'' , produit de E par E' . Pour cela, soit $E \times E'$, et considérons le sous-groupe (E, E') de $E \times E'$ formé des couples (e, e') ayant la même projection sur G . On peut définir de façon évidente un homomorphisme de (E, E') sur G , dont le noyau est l'ensemble des (a, a') , a et $a' \in A$. Soit Q le sous-groupe de ce noyau formé des $(a, -a)$. Posons $E'' = (E, E')/Q$; on vérifie immédiatement que E'' est une extension de A par G correspondant aux opérateurs fixés sur A .

Reste à voir que cette multiplication est la même que celle que l'on définit par l'addition des cocycles. Soient k, k' des sections de E, E' . L'application (k, k') définit une section de E'' (par passage au quotient) et si u et u' sont les cocycles correspondant à k et k' , le cocycle correspondant à (k, k') est $u + u'$. Ceci achève la démonstration.

Bibliographie supplémentaire (pour les produits croisés, en particulier) :

J. DIEUDONNÉ, La Th. de Galois ... , Comm. math. helvetici, 21, 1948,
p. 154-184.
