J-P. Serre

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

Séminaire Henri Cartan, tome 3 (1950-1951), exp. n° 6, p. 1-9
<http://www.numdam.org/item?id=SHC_1950-1951__3__A6_0>

Séminaire H. CARTAN

E.N.S., 1950/51 . Topologie algébrique.

APPLICATIONS ALGÉBRIQUES DE LA COHOMOLOGIE DES GROUPES. II : THÉORIE DES ALGÈBRES SIMPLES.

(1er exposé de J-P. SERRE, le 8.1.1951).

BIBLIOGRAPHIE :

DEURING - Algebren (Ergebnisse der Mathematik IV-1). - Berlin, Springer, 1935.

ARTIN-NESBITT-THRALL - Rings with minimum condition. - Ann Arbor, Univ. of Michigan Press, 1948.

Notations. Toutes les algèbres considérées par la suite auront un élément unité, noté 1. Le corps de base sera identifié aux multiples de cet élément unité. Si E est un espace de représentation de l'algèbre A (sur le corps k), E sera supposé de dimension finie sur k, et l'élément $1 \in A$ définira l'automorphisme identique de E. E sera dit représentation irréductible de A, si $E \neq 0$, et si tout sous-espace stable de E est identique à 0 ou E ; E sera dit complètement réductible s'il est somme directe de sous-espaces stables pour A et irréductibles. Un tel espace peut être considéré comme un groupe semi-simple (à opérateurs) et on peut, par exemple, utiliser les résultats démontrés dans Bourbaki, Alg.I, paragraphe 6, numéro 15 .

1.- Le théorème de Wedderburn.

Rappelons qu'une algèbre est dite simple si elle n'a pas d'autres idéaux bilatères qu'elle même et 0.

Théorème 1.- *Soit* A *une algèbre de dimension finie sur un corps commutatif* k, *simple, et possédant un élément unité. Alors* A *est isomorphe à une algèbre de matrices sur un corps gauche qui contient* k *dans son centre, et est fini sur* k.

Soit E une représentation irréductible de A ; une telle représentation existe : il n'y a qu'à prendre un idéal minimal à gauche de A, par exemple. Soit $L(E)$ l'algèbre des endomorphismes du k-espace vectoriel E, et soit K l'ensemble des endomorphismes $\in L(E)$ qui commutent avec les opérateurs de A. On a :

Lemme 1 - K *est un corps gauche*.

Soit en effet $u \neq o$, $u \in K$. Posons $V = u^{-1}(o)$; si $x \in V$, on a : $o = au.x = ua.x$ pour tout $a \in A$, ce qui montre que V est stable pour A , et, comme on a supposé que $u \neq o$, $V = 0$, d'où le fait que u est inversible dans $L(E)$; il est alors évident que son inverse est dans K .

Ceci démontré, reparquons d'abord que la représentation E est <u>fidèle</u> : en effet, le noyau de cette représentation est un idéal bilatère de A qui ne contient pas 1 , donc qui est réduit à 0 .

Soit alors B le commutant de K dans $L(E)$, c'est-à-dire l'ensemble des $b \in L(E)$ tels que $b.u = u.b$ pour tout $u \in K$. Il est évident que $A \subset B$; en fait nous allons montrer que $A = B$. Quand ceci sera fait, on pourra dire que A n'est autre que l'ensemble des K-<u>endomorphismes</u> de E (considéré comme espace vectoriel à gauche sur le corps K) , et il en résultera que A est isomorphe à une algèbre de matrices à coefficients dans le corps K^o opposé de K .

Reste donc à voir que $A = B$. C'est l'objet du lemme plus général suivant :

<u>Lemme 2</u> - <u>Soit</u> E <u>une représentation complètement réductible et fidèle d'une algèbre</u> A ; <u>soit</u> K <u>le commutant de</u> A <u>dans</u> $L(E)$, B <u>le commutant de</u> K <u>dans</u> $L(E)$. <u>On a</u> : $A = B$.

Soit d'abord $x \in E$ et $b \in B$. Nous allons montrer qu'il existe $a \in A$ tel que $ax = bx$.

Soit en effet V le sous-espace stable de E défini par $V = Ax$. V admet un supplémentaire stable (Bourbaki, <u>loc. cit</u>.), soit p un projecteur de E sur V . Le projecteur p , étant A-linéaire, est $\in K$. On en conclut : $pbx = bpx = bx$, d'où $bx \in V$, c.q.f.d.

Ce résultat partiel établi, nous allons pouvoir démontrer le lemme 2 . Il résultera tout de suite du suivant :

<u>Lemme 3</u> - <u>Dans les conditions du lemme</u> 2 , <u>soient</u> $x_1 , \ldots , x_n \in E$ <u>et</u> $b \in B$. <u>Il existe</u> $a \in A$ <u>tel que</u> $ax_1 = bx_1 , \ldots , ax_n = bx_n$.

Soit F l'espace somme directe de n fois la représentation E . On peut considérer F comme formé des éléments $(y_1 , \ldots , y_n)$ $(y_i \in E)$ sur lesquels A opère par la formule : $a.(y_1 , \ldots , y_n) = (ay_1 , \ldots , ay_n)$.

La représentation F est encore complètement réductible. Le commutant de A dans $L(F)$ est formé des matrices (u_{ij}) , $u_{ij} \in K$, et il en résulte que, si l'on fait opérer B sur F par la formule :

$$b.(y_1 , \dots , y_n) = (by_1 , \dots , by_n) \quad ,$$

les éléments de $L(F)$ ainsi définis seront encore dans le commutant du commutant de A (le "bicommutant"). En appliquant alors au point $x = (x_1 , \dots , x_n) \in F$, et à $b \in B$ le résultat démontré après l'énoncé du lemme 2 , on obtient bien le lemme 3, ce qui achève la démonstration.

Nous écrirons K_n l'algèbre des matrices à n lignes et n colonnes sur le corps K . Si K contient k dans son centre, on a : $K_n = k_n \otimes K$, comme on le voit aisément.

2.- Représentations des algèbres simples.

Soit A une algèbre et faisons opérer A sur elle-même par les translations à gauche. On obtient ainsi une représentation linéaire de A qui est dite représentation régulière gauche. Si A est une algèbre de matrices K_n de base canonique (e_{ij}) , les éléments e_{ij} où j est fixé, engendrent un sous-espace vectoriel N_j de A ; on vérifie aisément que N_j est un idéal à gauche minimal, et que les représentations linéaires de A fournies par les différents N_j sont toutes isomorphes. En d'autres termes : la représentation régulière gauche de K_n est la somme de n représentations irréductibles isomorphes. Plus généralement :

Théorème 2.- Toute représentation d'une algèbre simple A est isomorphe à une somme directe de représentations irréductibles toutes isomorphes.

Soit E une représentation linéaire de A , (e_i) un système fini de générateurs de E $(1 \leq i \leq p)$. Considérons l'application de A^p sur E définie par :

$$(a_1 , \dots , a_p) \longrightarrow a_1e_1 + a_2e_2 + \dots + a_pe_p \quad .$$

Cette application permet d'identifier E à un quotient de A^p (A^p étant considéré comme la somme directe de p fois la représentation régulière gauche de A). Comme le théorème 2 a été vérifié pour A^p , il est donc démontré pour E (Bourbaki, loc. cit.).

Corollaire 1 - Toute représentation de A est complètement réductible.

Corollaire 2 - Deux représentations de A qui ont même dimension sur k sont isomorphes.

3.- Produits tensoriels d'algèbres simples.

Donnons d'abord un lemme :

Lemme 4 - Soient A et A' deux algèbres sur k, ayant un élément unité. Soient B et B' des sous-algèbres de A et A' respectivement, C et C' leurs commutants dans A et A'. Alors le commutant de $B \otimes B'$ dans $A \otimes A'$ est identique à $C \otimes C'$.

Cherchons d'abord le commutant de $B \otimes 1$. Pour cela, soit a_i' une base de A'. Tout $x \in A \otimes A'$ s'écrit d'une seule façon sous la forme :

$$x = \sum_i a_i \otimes a_i' \qquad , \qquad a_i \in A \ .$$

Si l'on écrit que x commute avec $b \otimes 1$, on obtient : $a_i b = ba_i$, c'est-à-dire $a_i \in C$ pour tout i. On voit ainsi que le commutant de $B \otimes 1$ n'est autre que $C \otimes A'$. De même, celui de $1 \otimes B'$ est $A \otimes C'$. Il en résulte que le commutant de $B \otimes B'$ est égal à l'intersection des commutants de $B \otimes 1$ et $1 \otimes B'$, c'est-à-dire à $(C \otimes A') \cap (A \otimes C') = C \otimes C'$, c.q.f.d.

De ce lemme résulte par exemple que le centre d'un produit tensoriel est le produit tensoriel des centres. En appliquant ceci à une algèbre simple (de rang fini) : $A = k_n \otimes K$, on voit que le centre de A est $k \otimes C$, C désignant le centre de K :

Corollaire - Le centre d'une algèbre simple, finie sur k, est un corps (commutatif).

On s'intéressera particulièrement par la suite aux algèbres de centre k. Une telle algèbre sera dite centrale.

Théorème 3.- Soient A, A' deux algèbres simples, finies sur k, dont l'une est centrale. Alors, le produit tensoriel $A \otimes A'$ est une algèbre simple.

Supposons que $A' = k_n \otimes K'$ soit centrale, autrement dit que le centre du corps gauche K' soit réduit à k. Il suffira de voir que $A \otimes K'$ est une algèbre simple. En effet, si ceci est démontré, $A \otimes K' = k_m \otimes K''$, et $A \otimes A' = k_m \otimes k_n \otimes K'' = k_{mn} \otimes K'' = K''_{mn}$. L'algèbre $A \otimes A'$ sera donc isomorphe à une algèbre de matrices pour laquelle la simplicité se vérifie immédiatement. Reste donc à voir que $A \otimes K'$ est simple. Cela résulte du théorème suivant :

Théorème 4.- Soit A une algèbre sur k, ayant un élément unité, et K' un corps gauche de centre k. Tout idéal bilatère N de $A \otimes K'$ est engendré (en tant qu'espace vectoriel à gauche sur K') , <u>par son intersection avec</u> $A \otimes 1$. (Ni A ni K' ne sont supposés finis sur k) .

On notera d'abord que l'on peut faire opérer K' à gauche sur $A \otimes K'$ par :

$$k'(a \otimes k'') = a \otimes k'k'' \quad .$$

Si N est un idéal de l'algèbre $A \otimes K'$, c'est en particulier un <u>K'-sous-espace vectoriel à gauche de</u> $A \otimes K'$.

Soit a_i une base de A sur k ; les éléments $a_i \otimes 1$ forment également une base du K'-espace vectoriel $A \otimes K'$. Soit x un élément <u>primordial</u> de N par rapport à cette base (Bourbaki, Alg.II, paragraphe 5) :

$$x = \sum_i a_i \otimes k'_i \quad .$$

Considérons l'élément xm ($m \in K'$) ; on a $x.m \in N$ (N est un idéal bilatère), et d'autre part :

$$x.m = \sum_i a_i \otimes k'_i m \quad .$$

Il résulte alors des propriétés des éléments primordiaux que l'on a :

$$k'_i m = nk'_i \quad \text{pour tout } i \qquad (n \in K') \quad .$$

Comme l'un des k'_i est égal à 1 , on a $m = n$, et l'égalité précédente signifie simplement que k'_i commute avec tout $m \in K'$, i.e. que $k'_i \in k$. On peut alors écrire : $x = a \otimes 1$, en posant : $a = \sum_i k'_i a_i$. On a donc montré que <u>tout élément primordial</u> x <u>est dans</u> $A \otimes 1$; le théorème en résulte aussitôt puisque tout espace vectoriel est engendré par ses éléments primordiaux.

<u>Corollaire 1</u> - <u>Le produit tensoriel de deux algèbres simples, centrales et finies sur</u> k <u>est du même type</u>.

<u>Corollaire 2</u> - <u>Soit</u> A <u>une algèbre simple, de centre</u> k , <u>et telle que</u> $[A : k] = n$. <u>Si</u> A^o <u>désigne l'algèbre opposée, on a</u> :

$$A \otimes A^o = k_{n^2} \quad .$$ (algèbre des matrices à n^2 lignes et n^2 colonnes, sur le corps k)

Désignons par E l'algèbre A considérée comme espace vectoriel sur k . On peut faire opérer A sur E par les translations à gauche ou par les translations à droite. Cela revient à identifier A et A^o à des sous-algèbres de l'algèbre $L(E)$ des k-endomorphismes de E . Comme les algèbres A et

A^o commutent dans $L(E)$, on peut définir un homomorphisme canonique de $A \otimes A^o$ dans $L(E)$ qui prolonge les isomorphismes : $A \longrightarrow L(E)$ et $A^o \longrightarrow L(E)$. L'algèbre $A \otimes A^o$ étant simple (th.3), cet homomorphisme est un isomorphisme; comme en outre :

$$[A \otimes A^o : k] = [A : k]^2 = n^2 = [L(E) : k] \quad ,$$

cet isomorphisme applique $A \otimes A^o$ <u>sur</u> $L(E) = k_{n^2}$, c.q.f.d.

<u>Remarque</u> : Si aucune des deux algèbres A et A' du théorème 3 n'est centrale, l'algèbre $A \otimes A'$ n'est pas simple en général. Toutefois, si le centre de A , par exemple, est une extension <u>galoisienne</u> de k , on montre que $A \otimes A'$ est un produit direct d'algèbres simples.

4.- <u>Groupe de Brauer. Définition</u>.

Soit A une algèbre simple sur k , centrale et finie sur k . D'après le théorème de Wedderburn, on a : $A = k_n \otimes K$, où K est un corps gauche de centre k , fini sur k . <u>Le corps gauche</u> K <u>est bien déterminé par</u> A , à un k-isomorphisme près. En effet, on peut le caractériser comme l'opposé du commutant de A dans une représentation irréductible quelconque de A (et on sait que deux telles représentations sont semblables). Nous pouvons donc parler <u>du</u> corps gauche associé à une algèbre A .

Nous dirons que deux algèbres centrales sur k , A et A' , sont <u>semblables</u> lorsque les corps gauches associés à A et A' sont les mêmes (à un k-isomorphisme près). Cette relation de similitude partage les algèbres centrales sur k en <u>classes</u>, qui correspondent biunivoquement aux corps gauches de centre k et finis sur k .

Nous allons munir cet ensemble de classes d'une loi de <u>groupe</u> :
Si B et B' sont deux classes, et A , A' des éléments de ces classes, on voit tout de suite que les algèbres $A \otimes A'$ sont toutes contenues dans une même classe, que nous appelerons le <u>produit</u> des classes B et B' .

La classe qui contient l'algèbre $A = k$ est évidemment l'élément neutre de cette loi de produit ; c'est la classe formée de toutes les algèbres de matrices sur k .

Le produit des classes est <u>commutatif</u>, puisque $A \otimes A'$ est k-isomorphe à $A' \otimes A$; on montre de même qu'il est <u>associatif</u>.

Si A parcourt une classe B , les algèbres opposées A^o parcourent une classe B^o qui n'est autre que l'inverse de B (Cor. 2 au th. 4). En résumé :

Théorème 5.- Les classes d'algèbres simples, centrales et finies sur k, munies de la loi de composition du produit tensoriel, forment un groupe abélien. Ce groupe est appelé groupe de Brauer de k, et nous le noterons G_k.

5.- Groupe de Brauer. Exemples.

a.- k est algébriquement clos. Alors $G_k = 0$.

Soit en effet K un corps gauche de centre k, fini sur k ; nous devons montrer que $K = k$. Sinon, il existerait $x \in K$, $x \notin k$. Soit C le corps engendré par x et k. C est un corps commutatif (puisque k et x commutent), extension finie de k ; donc $C = k$, ce qui est absurde.

b.- $k = R$, corps des réels. Alors $G_R = Z_2$.

On connaît un corps gauche de centre R, non réduit à R : le corps K des quaternions. Nous verrons dans l'exposé suivant que c'est le seul. Il en résultera bien $G_R = Z_2$.

c.- k est un corps fini. Alors $G_k = 0$. (Voir 2eme exposé).

d.- k est un corps p-adique Q_p. Alors $G_k = Q/Z$ ("rationnels mod 1").
Voir Deuring (Algebren - Chap. VII - paragraphe 2).

e.- $k = Q$, corps des rationnels. Alors G_Q est un certain sous-groupe de la somme directe : $Z_2 + Q/Z + Q/Z + \dots + Q/Z + \dots$

Voir Deuring, loc. cit. paragraphe 5 ainsi que S.Wang, Annals 1950. Les deux derniers exemples montrent que le groupe de Brauer d'un corps k peut être assez compliqué ; mais dans les deux cas, on peut remarquer qu'il est limite inductive de sous-groupes bien plus simples (par exemple, dans le cas d.- , de sous-groupes cycliques). Ce sont ces sous-groupes que nous allons étudier dans la suite, et ramener à des groupes de cohomologie.

6.- Extension du corps de base.

Théorème 6.- Soit A une algèbre simple, centrale et finie sur k, L un corps commutatif, extension de k (finie ou infinie). L'algèbre $A \otimes L$ est simple.

Si A est un corps gauche, on peut appliquer le théorème 4 : tout idéal bilatère de $A \otimes L$ est engendré par son intersection avec L qui est (0) ou L, et $A \otimes L$ est bien simple.

Si A est quelconque, on peut écrire $A = k_n \otimes K$, d'où :

$$A \otimes L = k_n \otimes (K \otimes L) = k_n \otimes K'_m \quad , \; K' \text{ étant un autre corps gauche.}$$

Il en résulte :

$$A \otimes L = K'_{nm} \quad ,$$

d'où le théorème.

Corollaire - Soit A une algèbre simple, centrale et finie sur k . Alors $[A : k]$ est un carré parfait.

Prenons pour L une extension algébriquement close de k . L'algèbre $A \otimes L$ peut être munie d'une structure d'algèbre sur L , et l'on a :

$$[A \otimes L : L] = [A : k] \quad .$$

Mais $A \otimes L$ est une algèbre simple, centrale sur L , et finie sur L . Il résulte alors de (5-a-) que c'est une algèbre de matrices sur L , et $[A \otimes L : L]$ est bien un carré parfait.

A toute algèbre centrale, simple et finie sur k , soit A , faisons correspondre son produit tensoriel avec L , considéré comme algèbre centrale, simple et finie sur L . Autrement dit : étendons le corps de bases de A de k à L . Il est clair que deux algèbres semblables resteront semblables : on obtient ainsi une application canonique $\varphi_{k,L}$ du groupe de Brauer sur k , G_k , dans le groupe de Brauer sur L , G_L . Je dis que $\varphi_{k,L}$ est un homomorphisme. Cela résulte tout de suite de la formule :

$$(A \otimes_k L) \otimes_L (A' \otimes_k L) = (A \otimes_k A') \otimes_k L \quad ,$$

où $\otimes_k$ et $\otimes_L$ désignent des produits tensoriels pris sur k et L respectivement. Nous désignerons le noyau de $\varphi_{k,L}$ par $H_{k,L}$. C'est un sous-groupe du groupe de Brauer G_k , le sous-groupe formé des classes d'algèbres qui deviennent des algèbres de matrices quand on étend le corps de base à L . On dit aussi que ce sont les algèbres qui admettent L comme corps de décomposition.

Toute algèbre A admet L pour corps de décomposition si L est algébriquement clos, puisqu'alors $G_L = (0)$. En fait, des extensions finies suffisent :

Théorème 7.- Le groupe G_k est réunion des sous-groupes $H_{k,L}$ où L parcourt l'ensemble des extensions finies de k .

Soit A une algèbre de base (e_i) , de table de multiplication (c_{ijk}) ; nous devons montrer qu'il existe une extension finie L de k , telle que $A \otimes L$ soit une algèbre de matrices sur L . On sait que ceci est réalisé si on prend pour corps une extension algébriquement close M de k . Ceci signifie qu'il existe des $m_{ij} \in M$ tels que les $\sum_j m_{ij} e_j = E_i$ aient pour table de multiplication la table bien connue dans les algèbres de matrices. Soit $L = (k, m_{ij})$ le corps obtenu en adjoignant à k les m_{ij}, il est clair que L répond à la question.

<u>Remarque</u> : On peut montrer qu'il suffit de considérer les extensions L qui sont <u>galoisiennes</u> sur k .