SÉMINAIRE DE MATHÉMATIQUES

CLAUDE CHEVALLEY

Invariants d'une algèbre. Loi de réciprocité

Séminaire de Mathématiques (Julia), tome 1 (1933-1934), exp. n° 12, p. 1-10

<http://www.numdam.org/item?id=SMJ_1933-1934__1__A12_0>

Exemplaire n° 4
Institut Henri Poincaré
(Ne peut quitter la salle de travail)

SEMINAIRE DE MATHEMATIQUES

Année 1933-1934

Théorie des Groupes et des Algèbres

I.- INVARIANTS D'UNE ALGEBRE
LOI DE RECIPROCITE

Exposé fait par M. Claude CHEVALLEY, le 28 Mai 1934

A.- Caractérisation d'une algèbre par ses invariants .

Soient k un corps de nombres algébriques, et γ une algèbre simple de centre k . Rappelons qu'il est usuel en théorie du corps de classes d'introduire r symboles $\mathfrak{p}_{\infty,1}, \mathfrak{p}_{\infty,2}$ .... $\mathfrak{p}_{\infty,r}$, en correspondance univoque avec les conjugués réels $k^{(1)}$, $k^{(2)}$, ... $k^{(r)}$ de k et qui s'appellent les idéaux premiers à l'infini de k . A chacun de ces idéaux, correspond une "valeur absolue" de k qui s'obtient en associant à un nombre de k le nombre réel $|\beta^{(i)}|$ conjugué de β dans $k^{(i)}$.La fermeture de k relativement à cette valeur absolue (c'est à dire le corps des suites convergentes suivant cette valeur absolue) est un corps $k_{\mathfrak{p}_{\infty,i}}$ isomorphe au corps des nombres réels . On pose $\gamma_{\mathfrak{p}_{\infty,i}} = k_{\mathfrak{p}_{\infty,i}} \gamma$.

Ceci posé, à chaque classe $\{\gamma\}$ d'algèbres simples de centre k correspond pour chaque idéal premier $\mathfrak{p}$ fini ou infini une classe $\{\gamma_{\mathfrak{p}}\}$ d'algèbres de centre $k_{\mathfrak{p}}$, et cette correspondance est une homomorphie appliquant le groupe des classes de centre k sur un sous-groupe du groupe des classes de centre $k_{\mathfrak{p}}$. Soit $\sigma_{\mathfrak{p}}$ ce dernier groupe . De plus, pour $\{\gamma\}$ donné, la classe $\{\gamma_{\mathfrak{p}}\}$ ne peut être dans le corps gauche contenu dans la classe $\{\gamma\}$, donc en tous cas, pour un nombre fini d'idéaux premiers. Nous pou-

vons donc encore dire que nous avons une homomorphie du groupe des classes $\{\gamma\}$ sur un sous-groupe du produit direct de tous les $\gamma_\mathfrak{p}$.

D'autre part, il résulte de l'exposé précédent que si $\{\gamma_\mathfrak{p}\} = 1$ quel que soit $\mathfrak{p}$, on a $\{\gamma\} = 1$. L'homomorphie précédente est donc une isomorphie et la classe $\{\gamma\}$ est bien déterminée quand on connait tous les $\{\gamma_\mathfrak{p}\}$. Pour caractériser $\{\gamma\}$ par des invariants numériques, il suffira donc de caractériser les $\{\gamma_\mathfrak{p}\}$.

Supposons d'abord $\mathfrak{p}$ fini. Le corps gauche $\tilde{K}_\mathfrak{p}$ contenu dans $\{\gamma_\mathfrak{p}\}$ admet pour sous-corps commutatif maximum le sous-corps relativement cyclique non ramifié $k_\mathfrak{p}$ de $k_\mathfrak{p}$ de degré relatif $n_\mathfrak{p}$ égal au degré de $\tilde{K}_\mathfrak{p}$ et par suite $\tilde{K}_\mathfrak{p}$ se représente comme produit croisé sous la forme

$$\tilde{K}_\mathfrak{p} = \{\alpha, k_\mathfrak{p}, s\}$$

où s est une substitution engendrant le groupe de Galois de $k_\mathfrak{p} / k_\mathfrak{p}$. α se met sous la forme $\varepsilon \pi^m$, où ε est une unité de $k_\mathfrak{p}$ et π un nombre divisible exactement par la première puissance de $\mathfrak{p}$. Quand on se donne s, $\tilde{K}_\mathfrak{p}$ est déterminé par la classe de restes à laquelle appartient m modulo $n_\mathfrak{p}$. En effet, α est déterminé à une norme près d'un nombre de $k_\mathfrak{p}$. Or une unité ou un nombre de la forme $\pi^{an_\mathfrak{p}}$ sont des normes de $k_\mathfrak{p}$. D'ailleurs m est premier à $n_\mathfrak{p}$.

D'autre part, on peut choisir s d'une manière invarian-

te $\mathfrak{p}$. En effet, on démontre en théorie des corps (Voir (1)) l'existence d'une opération A bien déterminée telle que, pour tout entier A de $k_\mathfrak{p}$, on ait :

$$s\,A \equiv A^{N\mathfrak{p}} \pmod{\mathfrak{P}}$$

Cette substitution engendre le groupe de k / k et est appelée Substitution de Frobenius .

En supposant s égale à la substitution de Frobenius, $\{\gamma_\mathfrak{p}\}$ est donc déterminé par $k_\mathfrak{p}$ et par la valeur de m modulo $n_\mathfrak{p}$, ou encore par le quotient $\frac{m}{n_\mathfrak{p}}$ pris mod. 1 . C'est ce nombre que Hasse appelle invariant $P_\mathfrak{p}$ de $\{\gamma_\mathfrak{p}\}$ ou de $\{\gamma\}$ pour $\mathfrak{p}$. D'ailleurs, si une algèbre quelconque $\gamma_\mathfrak{p}$ de la classe $\{\gamma_\mathfrak{p}\}$ se représente sous la forme d'un produit croisé $\{\pi^{m'}, k'_\mathfrak{p}, s'\}$ où $k'_\mathfrak{p}$ est une extension cyclique non ramifiée de $k_\mathfrak{p}$ de degré $n'_\mathfrak{p}$, on a

$$\frac{m'}{n'_\mathfrak{p}} \equiv \frac{m}{n_\mathfrak{p}} \pmod{1}$$

Si $\mathfrak{p}$ est infini , $k_\mathfrak{p}$ est isomorphe au corps des nombres réels . Donc, $\{\gamma_\mathfrak{p}\}$ est la classe des algèbres de matrices à coefficients , ou bien réels, ou bien contenus dans le corps des quaternions . Dans le premier cas, on posera : $P_\mathfrak{p}\{\gamma\} \equiv 0 \pmod{1}$, dans le second : $P_\mathfrak{p}\{\gamma\} \equiv \frac{1}{2} \pmod{1}$.

Si $\{\gamma\}$, $\{\gamma'\}$, sont deux classes de centre k , on vérifie tout de suite que pour chaque $\mathfrak{p}$:

$$p_g\{\gamma\gamma'\} \equiv p_g\{\gamma\} + p_g\{\gamma'\} \pmod{1}$$

On peut donc dire que $p_g\{\gamma\}$ est un caractère additif du groupe des classes d'algèbres .

Pour que $\{\gamma_g\} = 1$, il faut et il suffit que $p_g \equiv 0 \pmod{1}$. Il résulte de là que le groupe des classes d'algèbres simples de centre k_g est isomorphe au groupe additif des nombres rationnels (mod.1) .

Nous avons donc caractérisé chaque classe d'algèbres par un système d'une infinité d'invariants attachés aux divers idéaux premiers du centre .

Nous allons nous servir de ces invariants pour résoudre le problème suivant : à quelle condition, une classe d'algèbres γ admet-elle pour corps de décomposition un sur-corps donné k de k ? Pour cela, il faut et il suffit que pour chaque idéal premier $\mathfrak{P}$ de $\mathfrak{k}$, $k_{\mathfrak{P}}$ soit corps de décomposition de $\{\gamma_g\}$, g étant l'idéal premier de k divisible par $\mathfrak{P}$. En effet, on vérifie tout de suite que $\{k\gamma\}_{\mathfrak{P}} = k_{\mathfrak{P}}\gamma_g$. Soit $N_{\mathfrak{P}} = (k_{\mathfrak{P}} : k_g)$. On sait que (Voir (2)) pour que $k_{\mathfrak{P}}$ soit corps de décomposition de $\{\gamma_g\}$, il faut et il suffit que $N_{\mathfrak{P}}$ soit divisible par le degré u_g du corps gauche contenu dans $\{\gamma_g\}$ ce qui s'exprime par les congruences $N_{\mathfrak{P}} p_g \equiv 0 \pmod{1}$. Ces congruences représentent donc la condition nécessaire et suffisante cherchée .

B.- Relation entre les invariants

On peut se demander si les invariants d'une algèbre sont des nombres arbitraires ou s'ils sont liés par des relations nécessaires . Nous allons montrer que c'est la seconde hypothèse qui est vraie .

Entre les invariants d'une classe quelconque existe la relation $\Sigma \rho_{\mathfrak{g}} \equiv 0 \pmod 1$. Nous esquisserons la marche de la démonstration en supposant, pour simplifier un peu, que tous les conjugués de k sont imaginaires, c'est à dire que k n'ait pas d'idéaux premiers infinis .

Lemme : Une algèbre γ de centre k admet un corps de décomposition K jouissant des propriétés suivantes :

1°- K est cyclique par rapport à k ;

2°- K est circulaire par rapport à k , c'est à dire contenu dans un corps $k(\zeta)$ où ζ est une racine N ième de l'unité ;

3°- N n'est divisible par aucun des idéaux premiers de k pour lesquels $\rho_{\mathfrak{g}}\{\gamma\} \not\equiv 0 \pmod 1$.

En effet, considérons les idéaux premiers pour lesquels $\rho_{\mathfrak{g}} \not\equiv 0$. Soit pour l'un de ces idéaux, $n_{\mathfrak{g}}$ le discriminateur réduit de $\rho_{\mathfrak{g}}$. Si $\mathfrak{P}$ est un diviseur premier de $\mathfrak{g}$ dans k , $N_{\mathfrak{P}} = (k_{\mathfrak{P}} : k_{\mathfrak{g}})$ est égal au degré relatif de $\mathfrak{P}$.

Il suffira donc de trouver un entier N, premier à certains idéaux $\mathfrak{g}$, tel que, en désignant par ζ une racine

primitive N ième de l'unité , par k le corps $k(\zeta)$, un certain nombre d'idéaux premiers de k se décomposent dans k en idéaux premiers de degrés relatifs divisibles par certain nombres donnés A l'avance . On démontre de diverses manières que de tels nombres existent (Voir (3)) .

Ceci posé, désignons par K un sur-corps relativement abélien de k . Soit $\mathfrak{p}$ un idéal premier de k non ramifié dans K . On démontre (Voir (1)) l'existence d'un élément s du groupe de Galois de K / k tel que pour tout entier A de k , on ait :

$$s\,A \equiv A^N \pmod{\mathfrak{p}}$$

s s'appelle substitution de Frobenius de $\mathfrak{p}$, et se désigne par $\left(\frac{K/k}{\mathfrak{p}}\right)$ ou $\left(\frac{K}{\mathfrak{p}}\right)$. Si $\mathfrak{P}$ est un facteur premier de $\mathfrak{p}$ dans K , on a

$$\left(\frac{K_z}{\mathfrak{p}}\right) = \left(\frac{k}{\mathfrak{p}}\right)$$

$\mathfrak{m}$ étant un idéal quelconque de k premier au discriminant relatif de K , on peut décomposer $\mathfrak{m}$ en idéaux premiers : $\mathfrak{m} = \pi \mathfrak{p}_i^{a_i}$. On appelle <u>symbole de Artin</u> $\left(\frac{k}{\mathfrak{m}}\right)$ la substitution :

$$\left(\frac{K}{\mathfrak{m}}\right) = \pi \left(\frac{K}{\mathfrak{p}_i}\right)^{a_i}$$

du groupe de K / k . On constate que $\left(\frac{K}{\mathfrak{m}}\right)$ ne change pas si on multiplie $\mathfrak{m}$ par la norme relative d'un idéal de K premier au discriminant de K / k .

D'autre part, on démontre (Voir (1)) qu'il existe pour

chaque idéal premier $\mathfrak{p}$ de k ramifié dans K un idéal $f_{\mathfrak{p}}$ qui est puissance de $\mathfrak{p}$ tel que, $\mathfrak{P}$ désignant un facteur premier de $\mathfrak{p}$ dans K, pour qu'un nombre α de k soit norme par rapport à $k_{\mathfrak{p}}$ d'un nombre de $K_{\mathfrak{P}}$, il faille et il suffise que α soit reste normique de K mod. $f_{\mathfrak{p}}$, c'est à dire congru mod. $f_{\mathfrak{p}}$ à la norme d'un nombre de K. $f_{\mathfrak{p}}$ s'appelle le $\mathfrak{p}$-conducteur de K, et le produit des $\mathfrak{p}$-conducteurs de tous les idéaux premiers ramifiés dans K s'appelle le conducteur de K.

Ceci posé, supposons K cyclique par rapport à k, et soit $\{\gamma\}$ une classe d'algèbres de centre k, admettant K comme corps de décomposition. Donc une algèbre de la classe se mettra sous la forme (α, k, s), où s est une opération engendrant le groupe de K/k et α un élément de k. Supposons que $p_{\mathfrak{p}}\{\gamma\} \equiv 0 \pmod 1$ pour tous les idéaux premiers de k ramifiés dans K. Cela veut dire que pour un idéal premier $\mathfrak{p}$ de k ramifié dans k, et divisible par l'idéal premier $\mathfrak{P}$ de K, α est norme par rapport à $k_{\mathfrak{p}}$ d'un nombre de $K_{\mathfrak{P}}$, donc que α est reste normique mod. $f_{\mathfrak{p}}$. Comme on peut sans changer γ, multiplier α par la norme d'un nombre de K, on peut supposer $\alpha \equiv 1 \pmod{f_{\mathfrak{p}}}$ pour les idéaux premiers $\mathfrak{p}$ finis ramifiés dans K. Soit $\mathfrak{v}$ un idéal premier fini de k non ramifié dans K et π un nombre divisible par $\mathfrak{v}$, non par $\mathfrak{v}^2$. Soit $\mathfrak{v}^{s_{\mathfrak{v}}}$ la plus haute puissance de $\mathfrak{v}$ qui divise α. Soit d'autre part :

$$\left(\frac{k}{\mathfrak{p}}\right) = s^{b_{\mathfrak{p}}}$$

On démontre facilement que $\rho_{\mathfrak{p}}\{r\} \equiv \frac{a_{\mathfrak{p}}\, b_{\mathfrak{p}}}{n}$ où n est le degré de k par rapport à k . On a donc :

$$\sum_{\mathfrak{p}} \rho_{\mathfrak{p}} \equiv \frac{1}{n} \sum a_{\mathfrak{p}}\, b_{\mathfrak{p}}$$

D'autre part :

$$\left(\frac{k}{(\alpha)}\right) = s^{\sum a_{\mathfrak{p}}\, b_{\mathfrak{p}}}$$

Supposons maintenant de plus que k soit contenu dans un corps $k(\zeta)$ où ζ est une racine primitive Nième de l'unité , N étant un entier premier aux idéaux $\mathfrak{f}$ ramifiés dans k .

Donc si $\mathfrak{l}$ est un facteur premier de N dans k , et $\mathfrak{L}$ un diviseur premier de $\mathfrak{l}$ dans k , α est norme de $k_{\mathfrak{L}}$ à $k_{\mathfrak{l}}$ d'un nombre de $k_{\mathfrak{L}}$. Donc il est reste normique de k modulo toute puissance de $k_{\mathfrak{L}}$. Ceci étant vrai pour tous les facteurs premiers $\mathfrak{l}$ de N , α est reste normique mod.N et on peut supposer sans restriction $\alpha \equiv 1 \pmod{N}$.

D'autre part, si $\mathfrak{v}$ est premier à N, on démontre facilement que

$$\left(\frac{k}{\mathfrak{v}}\right)\zeta = \zeta^{N\mathfrak{v}}$$

d'où $$\left(\frac{k}{(\alpha)}\right)\zeta = \zeta^{|N(\alpha)|}$$

Tous les conjugués de k étant imaginaires , on a $N(\alpha) \neq 0$; d'où $|N(\alpha)| = N(\alpha) \equiv 1 \pmod{N}$, et $\left(\frac{k}{(\alpha)}\right) = 1$.

On en déduit : $\sum a_{\sigma\tau} b_{\sigma\tau} \equiv 0 \pmod{n}$ et

(1) $$\boxed{\sum \rho_{\sigma\tau} \equiv 0 \pmod{1}}$$

Toute algèbre simple ayant, en vertu du lemme énoncé plus haut, un corps de décomposition cyclique circulaire satisfaisant aux conditions imposées à K, les invariants de toute algèbre simple de centre k satisfont à la relation précédente.

Soit maintenant K un corps de décomposition cyclique quelconque de γ et supposons $\alpha \equiv 1 \pmod{f}$ où f est le conducteur de k ; Alors de la relation $\sum \rho_{\sigma\tau} \equiv 0 \pmod{1}$ on déduit inversement que

$$\left(\frac{K}{(\alpha)}\right) = 1$$

Nous avons donc démontré que : si K est un sur-corps relativement cyclique de k, de conducteur f, $\left(\frac{K}{\sigma}\right)$ ne dépend que de la classe (mod.f) à laquelle appartient σ ; c'est à dire $\left(\frac{K}{\sigma}\right)$ ne change pas si on multiplie σ par un nombre $\equiv 1 \pmod{f}$.

Cet énoncé est connu sous le nom de loi de réciprocité de Artin. Il est équivalent à la relation (1). D'autre part, cette relation se déduit par des moyens purement arithmétiques du lemme précédent.

D'autre part, on constate que la loi de réciprocité permet de construire d'une manière purement arithmétique la

théorie des corps de classes , et par suite de démontrer le théorème fondamental sur les algèbres .

BIBLIOGRAPHIE

(1) Voir HASSE : Berlcht über neueue Untersuchungen J.de D.M.V. ou CHEVALLEY, Thèse, Journ? of Coll. of Sc. Tokyo

(2) BRAUER, HASSE, NOETHER, Beweis eines Hauptsatzes in der Theorie der Algebren Crelle, I67

(3) Van der WERDEN, Crelle 1934 .

Voir pour l'ensemble de l'exposé : Hasse, Theory of Cyclic algebras ower an algebraic number field , Trans. Amm. Mat. Soc. 34 , et HASSE , Die Struktur der R.Brauer-schen Algebrenklassengruppe .... M.A. I07 .
