Séminaire Dubreil.
Algèbre et théorie
des nombres

Leo Kaloujnine

Généralisation de la théorie de Galois

Séminaire Dubreil. Algèbre et théorie des nombres, tome 1 (1947-1948), exp. n° 6, p. 1-16
<http://www.numdam.org/item?id=SD_1947-1948__1__A6_0>

Faculté des Sciences de Paris
-:-:-:-
Séminaire A. CHÂTELET et P. DUBREIL
(ALGÈBRE et THÉORIE DES NOMBRES)
Année 1947/48
-:-:-:-

Exposé n° 6

GÉNÉRALISATION DE LA THÉORIE DE GALOIS

par Leo KALOUJNINE

Les notations sont celles de l'exposé de M. LAZARD [2] ; il ne s'agit encore que de corps commutatifs L , H , K , ... Les éléments des corps sont désignés par des lettres minuscules α , β , ... , a , b , x , les lettres latines étant, en principe, réservées au corps de base (ou corps des invariants) K , dans le cas d'une extension $L|K$.

1. Définitions matricielles.

1. Hypermorphismes.

Un hypermorphisme, de dimension k , d'un corps (commutatif) L , est un isomorphisme de L avec un sous-corps $\bar{L}$, de l'anneau des matrices carrées, d'ordre k , à termes dans L :

$$\alpha \longrightarrow \varphi(\alpha) \quad \text{ou} \quad \alpha.\varphi$$

$$(i , j \text{ de } 1 \text{ à } k , \alpha_{ij} \in L)$$

$$\varphi(\alpha) \quad \text{ou} \quad \alpha.\varphi = ||\alpha_{ij}||$$

L'opérateur φ de l'isomorphisme peut être noté en signe de fonction, ou en signe de multiplicateur.

Les matrices $||\alpha_{ij}||$ du corps $\bar{L}$, sont permutables entre elles ; sauf la matrice nulle, chacune a une inverse dans le corps ; la matrice correspondant à 1 ($\varphi(1)$ ou $1.\varphi$) est la matrice scalaire unité.

On peut considérer que l'hypermorphisme a lieu entre les matrices scalaires $\{\alpha\}$, d'ordre k , et les matrices carrées $||\alpha_{ij}||$; c'est alors un automorphisme entre sous-corps de l'anneau des matrices carrées, d'ordre k , dans L .

Un hypermorphisme de L , l'est aussi de l'extension $L|K$, s'il fait correspondre à tout élément a , de K , la matrice scalaire $\{a\}$, (ou bien encore s'il laisse invariante cette matrice scalaire).

Réciproquement, l'ensemble des éléments a , invariants dans L , pour un

hypermorphisme φ (ou, plus exactement, transformés en les matrices scalaires $\{a\}$), constituent un sous-corps K, de L, qui peut être appelé <u>le sous-corps des invariants de</u> φ ; (de sorte que φ est hypermorphisme de $L|K$). Ces deux définitions s'étendent à un ensemble d'hypermorphismes φ_i $(i \in I)$.

Un hypermorphisme de dimension 1 est un automorphisme, soit de L, soit de $L|K$.

2. <u>Addition</u>.

La <u>somme</u> de deux hypermorphismes, φ, de dimension k, et ψ, de dimension ℓ, est définie par la correspondance :

$$\alpha.(\varphi+\psi) = \left\| \begin{matrix} \alpha.\varphi & 0 \\ 0 & \alpha.\psi \end{matrix} \right\| \quad \text{(matrice composée).}$$

C'est un hypermorphisme de dimension $k + \ell$, dont le corps des invariants est l'intersection des corps des invariants de φ et ψ.

Cette addition est associative, a priori non commutative, il n'y a pas de soustraction. On peut noter $m\varphi$ (m entier positif), la somme de m hypermorphismes égaux à φ (itération ou puissance).

3. <u>Multiplication</u>.

Le <u>produit</u> de deux hypermorphismes (d'un corps L) est défini par leur <u>succession</u> :

$$\alpha.\varphi = ||\alpha_{ij}|| \ , \ \alpha_{ij}.\psi = ||(\alpha_{ij})_{i'j'}||$$

(i, j de 1 à k ; puis, pour chaque couple i, j : i', j' de 1 à ℓ) ;

$$\psi(\varphi(\alpha)) \quad \text{ou} \quad \alpha.(\varphi\times\psi) = ||(\alpha_{ij})_{i'j'}|| \ ;$$

le dernier terme est une matrice composée, d'ordre ℓ dans l'anneau des matrices d'ordre k, donc d'ordre $k\ell$ dans L.

Elle est obtenue en remplaçant, dans la matrice $||\alpha_{ij}||$, correspondante de α dans φ, chaque terme α_{ij} par la matrice correspondante dans ψ.

On peut vérifier qu'on obtient ainsi un hypermorphisme, de dimension $k\ell$, dont le corps des invariants est l'intersection des corps des invariants de φ et ψ.

En particulier, le déterminant de la matrice composée est obtenu en calculant

son déterminant dans le corps des matrices commutatives (d'ordre ℓ) $\alpha_{ij} . \varphi$, ce qui donne une matrice, d'ordre ℓ, non nulle (si $\alpha \neq 0$), puis de calculer le déterminant de cette matrice qui est aussi non nul.

La multiplication, ainsi définie, est associative ; il y a un élément neutre qui est l'hypermorphisme identique (ou automorphisme). La multiplication des hypermorphismes de dimension 1 est équivalente à celle des automorphismes correspondants.

4. Transposé (ou symétrique) d'un hypermorphisme.

A un hypermorphisme φ, de dimension k, on peut associer l'hypermorphisme transposé, ou symétrique φ^* :

$$\alpha . \varphi = ||\alpha_{ij}|| \qquad \alpha . \varphi^* = ||\alpha_{ji}|| \ ;$$

obtenu en permutant les lignes et les colonnes dans chaque matrice image.

Il est visible que c'est encore un hypermorphisme : la somme des transposés de deux matrices est la transposée de la somme, et de même pour le produit, en tenant compte de sa commutativité.

5. Equivalence (ou congruence) des hypermorphismes.

S étant une matrice carrée, d'ordre k, régulière, à termes dans le corps L, la correspondance φ', définie par :

$$\alpha . \varphi' = S \times (\alpha . \varphi) \times S^{-1} \qquad (\text{ou } \varphi'(\alpha) = S \times \varphi(\alpha) \times S^{-1})$$

obtenue en effectuant la transmutation, d'opérateur S, sur toutes les matrices images de l'hypermorphisme φ est encore un hypermorphisme φ' et φ est deduit de φ' par la transmutation d'opérateur S^{-1}.

On convient de définir équivalents, ou congrus, des hypermorphismes déduits les uns des autres par des transmutations.

On peut vérifier directement que :

1° cette équivalence, ou congruence, a les qualités d'une égalité et qu'elle est compatible avec (ou laisse déterminées) l'addition et la multiplication définies ci-dessus ;

2° dans l'ensemble des hypermorphismes, définis à une équivalence, ou congruence près, l'addition est commutative; la multiplication est distributive des deux

côtés, par rapport à l'addition.

Ces propriétés sont peut-être rendues plus évidentes par l'emploi des modules de représentation, ou bimodules, ce qui va faire l'objet du paragraphe suivant.

2. Bimodules.

6. Définition générale.

Un bimodule, sur un corps L, commutatif, est un ensemble d'éléments, X, Y, Z, ..., appelés vecteurs, tels que

1° l'ensemble est un module Γ, ou groupe abélien additif (signes + et -) ;

2° il existe deux multiplications, ou lois de composition externes, par les éléments de L : à droite $X\beta$ et à gauche αX :

$$X\beta \ , \ \alpha X \in \Gamma \text{ (pour tous } \alpha, \beta \in L) \ .$$

3° les deux multiplications sont permutables entre elles, c'est-à-dire que :

$$(\alpha X)\beta = \alpha(X\beta) \ .$$

7. Dimension d'un bimodule.

Pour un bimodule Γ (ou pour une famille de bimodules) sur L, les éléments a de L, tels que :

$$aX = Xa \quad \text{(pour tout } X \in \Gamma) \ ,$$

constituent un sous-corps K de L, appelé corps des invariants de Γ (ou de la famille).

Si Γ, considéré comme espace vectoriel à droite sur L, est de dimension finie : $(\Gamma : L) = k$, et si L est extension de degré fini sur K, le bimodule Γ, considéré comme espace vectoriel, à gauche, sur L, est de la même dimension (finie) k. Ceci, en raison de l'égalité, valable des deux côtés :

$$(\Gamma : K) = (\Gamma : L).(L : K) \ ,$$

et du fait que le premier membre, en raison de la définition de K, a la même valeur des deux côtés, k est appelé la dimension de Γ.

8. Hypermorphisme et bimodule.

Un hypermorphisme, de dimension k d'un corps (commutatif) L, défini à une équivalence, ou congruence, près, est équivalent à la construction d'un bimodule Γ,

de dimension k sur L, et le sous-corps K des invariants est le même pour l'hypermorphisme et le bimodule.

Considérons un bimodule Γ, de dimension k sur le corps L, et choisissons en une base à droite de k éléments (indépendants) ; X_i.

Pour tout élément α de L, les k éléments αX_i (de Γ) sont des expressions linéaires, à droite, des X_j :

$$\alpha . X_i = \sum X_j . \alpha_{ij} : \quad (j \text{ de } 1 \text{ à } k, \text{ pour chaque } i)$$

ou

$$\alpha . ||X_1 \dots X_k|| = ||X_1 \dots X_k|| \times ||\alpha_{ij}|| .$$

Il est visible que la correspondance ainsi réalisée :

$$\alpha \longrightarrow ||\alpha_{ij}|| \quad \text{ou} \quad \alpha . \varphi = ||\alpha_{ij}|| ;$$

entre tout élément α et une matrice carrée, d'ordre k de L, est un hypermorphisme ; (on calcule immédiatement la somme et le produit de deux éléments et il leur correspond la somme et le produit des matrices).

Tout changement de base, dans Γ, défini par une matrice carrée, régulière, d'ordre k, S, est équivalent à une transmutation de φ, d'opérateur S, et, par suite, le remplace par un hypermorphisme équivalent.

Réciproquement, considérons un hypermorphisme φ d'un corps L. Pour construire un bimodule prenons k vecteurs X_i, et formons l'espace vectoriel à droite

$$X = \sum X_i . \alpha_i$$

isomorphe à la puissance directe L^k, ou à l'ensemble de k-uples :

$$||\alpha_1 \dots \alpha_k|| ;$$

tant au point de vue de l'addition que de la multiplication à droite, par un élément α, de L.

On définit ensuite la multiplication à gauche par un élément α de L, pour les k vecteurs X_i, et, par suite pour tout vecteur X,

$$\alpha . \varphi = ||\alpha_{ij}|| , \qquad \alpha . X_i = \sum X_j . \alpha_{ij} \quad (j \text{ de } 1 \text{ à } k)$$

et

$$\alpha . \sum X_i . \lambda_i = \sum X_j . \lambda_i \alpha_{ij} \quad (i \text{ et } j \text{ de } 1 \text{ à } k)$$

On obtient bien un bimodule auquel est associé l'hypermorphisme considéré.

Il est visible qu'une équivalence, ou transmutation, de φ est équivalente à un changement de base du bimodule associé :

$$\alpha . (||X_1 \dots X_k|| \times S^{-1}) = ||X_1 \dots X_k|| \times S^{-1} \times (S \times ||\alpha_{ij}|| \times S^{-1})$$

En outre les éléments invariants a du corps K sont caractérisés pour l'hypermorphisme, comme pour le bimodule par les conditions équivalentes :

$$a . \varphi = \{a\}, \quad a\,||X_1 \dots X_k|| = ||X_1 \dots X_k|| \times \{a\} .$$

9. Addition des bimodules.

Γ et Δ étant des bimodules sur L, de dimension k et ℓ, et de vecteurs respectifs X et Y, on les additionne en formant leur somme directe. C'est l'ensemble $\sum$ des couples $||X \quad Y||$, pour lesquels les 3 opérations sont définies par

$$||X \quad Y|| + ||X' \quad Y'|| = ||(X + X') \quad (Y + Y')||$$

$$\alpha . ||X \quad Y|| = ||\alpha . X \quad \alpha . Y|| \qquad ||X \quad Y|| . \beta = ||X . \beta \quad Y . \beta||$$

$\sum$ est manifestement un bimodule de dimension $k+\ell$ sur L, et cette addition est associative et commutative, si l'on ne distingue pas des bimodules isomorphes.

Pour construire des hypermorphismes associés choisissons des bases :

$$X_1, \dots, X_k ; \quad Y_1, \dots, Y_\ell ; \quad X_1, \dots, X_k, Y_1, \dots, Y_\ell ,$$

l'hypermorphisme associé à $\sum$ est manifestement la somme, au sens défini ci-dessus des hypermorphismes associés à Γ et Δ.

Ceci montre que la somme des hypermorphismes reste déterminée pour l'équivalence ou congruence, ou transmutation, et qu'elle est commutative.

10. Multiplication des bimodules.

Le produit des bimodules Γ et Δ est l'ensemble des couples (X , Y), entre lesquels les opérations sont définies par les conditions :

$$(X\ ,\ Y) + (X\ ,\ Y') = (X\ ,\ Y + Y')\ ;\quad (X\ ,\ Y) + (X'\ ,\ Y) = (X + X'\ ,\ Y)\ ;$$

$$(X\ ,\ Y).\beta = (X\ ,\ Y.\beta)\ ;\quad (X.\beta,\ Y) = (X\ ,\beta.Y)\ ;\ \alpha.(X\ ,\ Y) = (\alpha.X\ ,\ Y)\ .$$

On obtient ainsi un bimodule, noté :

$\Gamma \times \Delta$ (ordre de succession) , ou $\Delta_0\ \Gamma$ (ordre des fonctions) dont une base est constituée par les $k\ell$ couples :

$$(X_i\ ,\ Y_{i'}) \qquad (X_i \text{ base de } \Gamma\ ,\ Y_{i'} \text{ base de } \Delta\ )$$

A ce produit est bien associé le produit des hypermorphismes car :

$$\alpha.(X_i\ ,\ Y_{i'}) = (\alpha.X_i\ ,\ Y_{i'}) = (\sum X_j.\alpha_{ij},\ Y_{i'}) = \sum (X_j.\alpha_{ij},\ Y_{i'})$$

$$= \sum (X_j\ ,\alpha_{ij}.Y_{i'}) = \sum (X_{j'}\ (\sum Y_{j'}\ .(\alpha_{ij})_{i'j'}))$$

$$= \sum\sum (X_j\ ,\ Y_{j'}).(\alpha_{ij})_{i'j'}\ ,$$

les sommes sont étendues à j de 1 à k , puis j' de 1 à ℓ .

On obtient bien la matrice composee, construite précedemment.

Ceci montre que le produit des hypermorphismes reste determiné pour l'équivalence, ou congruence, ou transmutation, et qu'il est associatif. On constate en outre qu'il est distributif pour l'addition (les bimodules étant définis à un isomorphisme près).

11. Bimodules de diemnsion 1.

Un bimodule, de dimension 1 . est associé à un automorphisme (de L) :

$$\alpha\ .\ \omega = \alpha' \in L\ ,\ \alpha'.\omega^{-1} = \alpha\ .$$

Il est monogène, c'est-à-dire est engendré par un seul vecteur X_0 , et formé des éléments $X_0.\beta$, avec la loi de multiplication :

$$\alpha\ .X_0 = X_0.(\alpha.\omega)\ .$$

Le produit de deux bimodules, de dimension 1 , caractérisés par les automorphismes ω et ω' est l'ensemble des couples :

$$(X_0.\alpha,\ X_0.\beta) = (X_0, \alpha.X_0.\beta) = (X_0\ ,\ X_0.(\alpha.\omega' \times \beta)) = (X_0\ ,\ X_0\ \gamma).$$

Il est isomorphe au bimodule $X_0 . \gamma$ associée à l'automorphisme $\omega \times \omega'$, car :

$$(X_0 , X_0.\gamma) + (X_0 , X_0.\gamma') = (X_0 , X_0.(\gamma+\gamma')) ;$$

$$(X_0 , X_0.\gamma).\beta = (X_0 , X_0.(\gamma\beta))$$

$$\alpha.(X_0 , X_0.\gamma) = (\alpha.X_0 , X_0.\gamma) = (X_0.(\alpha.\omega) , X_0.\gamma) = (X_0 , (\alpha.\omega).X_0.\gamma)$$

$$= (X_0 , X_0.(\alpha.(\omega\times\omega')\gamma))$$

12. Bimodules transposés.

Un bimodule Γ étant associé à un hypermorphisme φ , et défini à un isomorphisme près, on appelle bimodule transposé, ou symétrique, et on note Γ^* , le bimodule associé à l'hypermorphisme transposé, ou symétrique, φ^* et isomorphe de Γ , au point de vue de l'addition. Si le correspondant du vecteur X est noté X^* , il y a correspondance des vecteurs de base et :

$$(\sum X_i.\lambda_i)^* = \sum X_i^*.\lambda_i \qquad (i \text{ de } 1 \text{ à } k) ;$$

mais les produits à gauche sont définis respectivement par :

$$\alpha.X_i = \sum X_j.\alpha_{ij} , \quad \alpha.X_i^* = \sum X_j^*.\alpha_{ji} \qquad (j \text{ de } 1 \text{ à } k) .$$

La transposition est manifestement réciproque. Deux bimodules transposés ont le même corps d'invariants K . Si L est une extension séparable sur K , on démontrera que les bimodules transposés sont isomorphes, il ne semble pas qu'on puisse l'affirmer dans le cas général.

13. Bimodules opposés.

Avec les mêmes notations et Γ étant de dimension finie k sur L , on appelle bimodule opposé, et on note Γ^0 , un module d'éléments X^0 , correspondant aux vecteurs X , avec conservation de la somme, mais les multiplications par les éléments de L étant définies par :

$$X^0.\beta = (\beta.X)^0 , \quad \alpha.X^0 = (X.\alpha)^0 .$$

C'est bien encore un bimodule, de même dimension k et de même corps d'invariants K . Les lois de composition des éléments de base sont définies respectivement dans les deux modules opposés par :

$$\alpha . X_i = \sum X_j . \alpha_{ij} \quad , \quad X_i^0 . \alpha = \sum (\alpha_{ij} . X_j) \qquad (j \text{ de } 1 \text{ à } k)$$

14. Bimodules inverses.

Les bimodules $(\Gamma^*)^0$ et $(\Gamma^0)^*$ seront dits inverses de Γ ; suivant la notation du produit, ils seront l'un à droite, l'autre à gauche (l'ordre est indifférent si les modules transposés sont isomorphes). Dans tous les cas les deux produits :

$$\Gamma \times (\Gamma^*)^0 \qquad \text{et} \qquad (\Gamma^0)^* \times \Gamma$$

contiennent un bimodule unité.

On peut choisir k vecteurs X_i de Γ, qui constituent une base, tant à droite qu'à gauche. Leur construction peut se prouver par récurrence.

Choisissons la base correspondante X^{*0} dans le bimodule inverse $(\Gamma^*)^0$; elle est aussi base des deux côtés. Dans le produit $\Gamma \times (\Gamma^*)^0$, formons le vecteur :

$$X_0 = \sum (X_i \ , \ (X_i^*)^0) \qquad (i \text{ de } 1 \text{ à } k)$$

il engendre un bimodule unité.

En effet :

$$\alpha . X_0 = \sum (\alpha . X_i \ , \ (X_i^*)^0) = \sum (\sum X_j . \alpha_{ij}) \ , \ (X_i^*)^0))$$

$$= \sum \sum (X_j \ , \alpha_{ij} . (X_i^*)^0) = \sum \sum (X_j \ , (X_i^* . \alpha_{ij})^0) = \sum (X_j \ , \alpha . X_j^{*0}))$$

$$= (\sum (X_j \ , \ X_j^{*0})) . \alpha \ = X_0 . \alpha$$

Les sommes sont étendues à i de 1 à k , puis à i et j , puis à j .

On opérerait de même pour l'autre produit.

15. Semi-algèbre.

Dans une extension finie $L|K$, (ou dans L , sur-corps de dimension finie sur K) , considérons l'ensemble S_K^L des bimodules Δ de L , dont le corps des invariants contient K :

$$\Delta \in S_K^L \qquad (\text{corps des invariants de } \Delta \supset K) .$$

Cet ensemble est appelé semi-algèbre ; il est caractérisé par les conditions

de structure suivantes :

1° A tout Δ , de l'ensemble, est associée sa dimension, (entier positif, noté : $\dim(\Delta)$.

2° Il y a deux relations d'ordre :

$$\Delta_1 \subset \Delta_2 : \Delta_1 \text{ sous-bimodule de } \Delta_2 ;$$

$$\Delta_1 \subset \Delta_2 : \Delta_1 \text{ homomorphe à } \Delta_2 .$$

Chacune d'elles entraîne :

$$\dim(\Delta_1) \leqslant \dim(\Delta_2) .$$

La conjonction de deux relations d'ordre converses est équivalente à l'égalité :

$$\Delta \simeq \Delta' \quad \text{et} \quad \Delta' \simeq \Delta \iff \Delta = \Delta' ,$$

$$\Delta \subset \Delta' \quad \text{et} \quad \Delta' \subset \Delta \iff \Delta = \Delta' .$$

On pourrait aussi définir des relations d'ordre strictes, (égalité exclue), qui entraîneraient des inégalités strictes des dimensions.

3° Il y a addition (définie ci-dessus).

Ses relations avec la dimension et les relations d'ordre sont :

$$\dim(\Delta_1 + \Delta_2) = \dim(\Delta_1) + \dim(\Delta_2) ,$$

$$\Delta_1 \subset \Delta_2 + \Delta_1 , \quad \Delta_1 \subset \Delta_1 + \Delta_2$$

Relativement à l'addition, la semi-algèbre a une structure de semi-groupe additif libre (il n'y a ni zéro, ni opposé). Elle est engendrée par les sommes des bimodules indécomposables qui contituent une base déterminée.

Les relations d'ordre sont conservées par addition.

4° Il y a une multiplication (définie ci-dessus) , associative, distributive par rapport à l'addition, et possédant un élément neutre.

La multiplication conserve les relations d'ordre.

Il y a produit des dimensions :

$$\dim(\Delta_1 \times \Delta_2) = \dim(\Delta_1) \times \dim(\Delta_2) .$$

La multiplication est déterminée par celle des éléments de la base.

5° Il y a des éléments qualifiés 'inverses", pour tout Δ , à droite et à gauche.

$$\Delta \times \Delta^{-1} \subset E \ , \qquad {}^{-1}\Delta \times \Delta \subset E \ :$$

Leurs dimensions sont égales à celle de Δ .

Si les éléments de la base (bimodules indécomposables) sont tous de dimension 1 , la base est un groupe, relativement à la multiplication.

Ce cas se présente si $L|K$ est une extension galoisienne (ou normale) ; et le groupe de la base est son groupe de Galois.

Dans le cas général, le produit de deux éléments de base étant une somme de certains des éléments de cette base, en définit ainsi une structure d'hypergroupe.

16. Correspondance.

1° A tout sous-corps K , d'un corps L , ($L|K$ étant de dimension finie), correspond biunivoquement une semi-algèbre S_K^L .

La biunivocité résulte de ce que, dans la semi-algèbre S_K^L , il y a nécessairement un bimodule Γ , dont le corps des invariants est effectivement K .
Il est constitué par une représentation régulière de L sur K .

2° A tout corps M , intermédiaire entre K et L , correspond une sous-algèbre S_M^L , de S_K^L :

$$K \supset M \supset L \ \dashrightarrow \ S_M^L \subset S_K^L \ .$$

17. Représentation régulière.

On appelle représentation régulière, ou bimodule régulier, ou hypermorphisme régulier P , d'une extension finie $L|K$ (de dimension n) , la correspondance entre éléments α de L , et les matrices (carrées d'ordre n) $||a_{ij}||$, à termes dans K , définie, en partant d'une base $\omega_1 , \dots , \omega_n$ de L sur K , par les n relations (j de 1 à n) :

$$\alpha . \omega_j = \sum \omega_i . a_{ij} \qquad (i \text{ de } 1 \text{ à } n)$$

équivalentes à la relation matricielle :

$$\alpha . ||\omega_1 \dots \omega_n|| = ||\omega_1 \dots \omega_n|| \times ||a_{ij}|| \ .$$

Il est visible que cette correspondance, qui est un cas particulier de la définition générale d'un bimodule (paragraphe 8) est un isomorphisme ; les éléments ω_i jouent le rôle de vecteurs de base.

Le corps des invariants est évidemment K .

Un changement de base est une équivalence, ou congruence (paragraphe 8) .

Dans une extension $L|K$, le bimodule régulier est unique, à une équivalence, ou changement de base, près.

THÉORÈME 1. - Dans un corps L , tout bimodule Δ , qui possède une base à droite X_J (J de 1 à N) , telle que l'hypermorphisme, défini par Δ et correspondant à cette base :

$$\alpha . ||X_1 \dots X_N|| = ||X_1 \dots X_N|| \times ||a'_{IJ}|| \ ,$$

ait ses coefficients dans $\text{inv}(\Delta) = K$ est un multiple de l'hypermorphisme régulier P :

$$\Delta = mP = P + \dots + P \ .$$

1° On établit d'abord qu'un bimodule Δ , dont la dimension N est minimum, est nécessairement régulier, (de dimension n) .

On vérifie, pour cela que les éléments :

$$\omega_i . X_1 \quad (\omega_i \text{ base de } L \text{ sur } \text{inv}(\Delta) = K) \ ,$$

sont indépendants à droite dans L . Par suite ces n éléments constituent une base d'un bimodule P , contenu dans Δ , donc égal à Δ , dont la dimension est supposée minimum.

Mais P est bimodule régulier (et monogène, engendré par le seul vecteur X_1) , ce qui démontre l'affirmation.

2° On considère ensuite un bimodule Δ , de dimension quelconque, de base X_J . On forme de même les n éléments $\omega_i . X_k$, pour une certaine valeur de k . Ils forment une base d'un bimodule régulier P_k , inclus dans Δ (en tenant compte, bien entendu de l'hypothèse des a'_{ij} dans $\text{inv}(\Delta) = K$.

On montre alors que :

$$\Delta = P_k + \Delta_k$$

et que cette somme est directe. La propriété est alors établie par récurrence.

THÉORÈME 2 (a). - Tout bimodule monogène Θ de L, tel que $\mathrm{inv}(\Theta) = K$, est homomorphe au bimodule régulier P de $L|K$.

Si Θ est engendré par un élément Y, les éléments $\omega_i.Y$, qui ne sont pas nécessairement indépendants, définissent un bimodule, manifestement homomorphe au bimodule régulier, défini par les éléments indépendants $\omega_i.X_1$ (ou simplement ω_i).

THÉORÈME 2 (b). - Tout bimodule Θ de L, tel que $\mathrm{inv}(\Theta)$ soit égal à K, est homomorphe à un multiple mP du bimodule régulier P de l'extension $L|K$.

Ce théorème, qui comprend le précédent, se vérifie de façon analogue, en suivant la démonstration du théorème 1.

18. Extensions séparables.

On sait qu'une extension $L|K$ est séparable si tout polynôme irréductible dans K, n'a pas de zéro multiple dans L. Si K est de caractéristique nulle, toute extension en est séparable.

Si un corps K (et, par suite, tout sur-corps L) est de caractéristique p (non nulle), une extension $L|K$ est appelée quasi-séparable si :

$$\alpha \in L \text{ et } \alpha^p \in K \longrightarrow \alpha \in K .$$

Si une extension est séparable, elle est, a fortiori, quasi-séparable, car le polynôme :

$$x^p - \alpha^p = (x - \alpha)^p$$

qui est dans K (et a une dérivée nulle) a un zéro multiple dans L, Il est donc décomposable dans K, ce qui exige que α soit dans K.

La réciproque n'est pas exacte, mais si pour tout corps intermédiaire M $(K \subset M \subset L)$, l'extension $M|K$ est quasi-séparable, $L|K$ est séparable. (Propriété connue et facile à établir).

LEMME 1. - Dans un corps L, de caractéristique p (non nulle), si un vecteur X engendre un bimodule monogène Θ, il vérifie l'implication :

$$\sum \alpha.X.\beta = 0 \longrightarrow \sum \alpha^p.X.\beta^p = 0$$

(la somme étant étendue à des couples d'éléments α, β, de L).

En effet, la base à droite du bimodule Θ étant formée de vecteurs $\gamma_j X$ (j de

1 à k) , a tout α correspond une matrice (carrée, d'ordre k) $||\alpha_{ij}||$, telle que :

$$\alpha . \; || \ldots \gamma_j X \ldots || = || \ldots \gamma_j X \ldots || \times ||\alpha_{ij}||$$

on en conclut les équivalences :

$$\sum \alpha . X . \beta = 0 \iff \sum \alpha . \; || \ldots \gamma_j X \ldots || \beta = 0$$

$$\iff \sum ||\alpha_{ij}|| \beta = 0$$

Il en résulte, par des égalités évidentes, dans un corps de caractéristique p) :

$$\sum ||\alpha_{ij}|| . \beta = 0 \longrightarrow \sum ||\alpha_{ij}||^p . \beta^p = 0 \longrightarrow \sum \alpha^p . X . \beta^p = 0$$

LEMME 2. - Si dans un corps L, de caractéristique p , il existe un bimodule Θ simple (sans autre sous-bimodule que lui-même et 0) dont le corps d'invariants est $inv(\Theta) = K$, l'extension $L|K$ est quasi-séparable.

Θ étant simple est monogène, et tout vecteur peut se mettre (en général de plusieurs façons) sous la forme

$$Y = \sum \alpha . X . \beta$$

La transformation, d'opérateur φ , définie par :

$$Y . \varphi = (\sum \alpha . X . \beta) . \varphi = \sum \alpha^p . X . \beta^p \quad ;$$

est un endomorphisme pour l'addition, et elle est univoquement determinée, car, d'après le lemme précédent :

$$\alpha . X . \beta = \alpha' . X . \beta' \longrightarrow \alpha^p . X . \beta^p = \alpha'^p . X . \beta'^p \; .$$

L'ensemble des éléments Y de Θ , dont l'image par φ est nulle est un sous-bimodule de Θ , qui, d'après l'hypothèse, ne peut être que 0 , ou Θ lui-même (suivant ces deux circonstances, l'endomorphisme φ est un automorphisme, ou est nul). Or c'est le premier cas qui se produit, puisque :

$$X . \varphi = X \neq 0 \; .$$

Il y a donc automorphisme et :

$$\sum \alpha^p . X . \beta^p = 0 \longrightarrow \sum \alpha . X . \beta = 0 \; .$$

Ceci établi considérons un élément α de L, tel que

$$\alpha \in L \text{ et } \alpha^p \in K \ ;$$

on en conclut :

$$\alpha^p.X - X.\alpha^p = 0 \longrightarrow \alpha.X - X.\alpha = 0$$
$$\longrightarrow \alpha.X = X.\alpha \longrightarrow \alpha \in \text{inv}(\theta) = K$$

19. Semi-algèbre d'une extension finie séparable.

THÉORÈME 3. - Pour qu'une extension $L|K$, finie, soit séparable, il faut et il suffit que la base de la semi-algèbre S_K^L se compose d'un nombre fini de bimodules simples Δ_i.

La condition est suffisante. - Si S_K^L vérifie la propriété, il en est de même de S_M^L, semi-algèbre de toute extension intermédiaire $(K \subset M \subset L)$.

Le corps M est une intersection des corps des invariants de certains Δ_i. Mais L, $\text{Inv}(\Delta_i)$, est semi-séparable (Lemme 2) ; il en est de même de toute extension $L|M$; par suite $L|K$ est séparable.

La condition est nécessaire : Si $L|K$ est fini et séparable, c'est une extension simple, c'est-à-dire qu'elle est engendrée par un seul élément ω (ceci peut se démontrer sans utiliser de surextension normale de $L|K$).

Tout hypermorphisme est univoquement déterminé par la matrice $||\omega_{ij}||$; qui correspond à l'élément primitif ω.

Pour obtenir les bimodules réguliers simples, il suffit de décomposer, dans L, le polynôme fondamental $f(x)$ de ω dans K.

A chaque facteur irréductible, dont l'un est $x - \omega$, correspond un bimodule régulier simple dans L, et tout autre bimodule régulier est somme directe de ceux-là.

Il en résulte (théorème 2) que tout bimodule de S_K^L étant homomorphe à un multiple des précédents est aussi une somme directe de bimodules simples.

THÉORÈME réciproque. - On a ainsi établi qu'à toute extension finie et séparable $L|K$, correspond une semi-algèbre déterminée, (qui sera appelée algèbre de Galois), engendrée par une base de bimodules simples. Reste à établir la réciproque qu'on peut énoncer comme suit.

THÉORÈME. - Toute semi-algèbre S, de bimodules d'un corps L, engendrée par

une base de bimodules simples, est une semi-algèbre S_K^L d'une extension finie $L|K$ (de L relativement à un sous-corps).

La demonstration se fait en formant le corps K, des invariants de l'algèbre S, engendrée par les bimodules simples Δ_i, puis le bimodule régulier P_K^L de L sur K, qui contient le bimodule $P = \sum \Delta_i$.

On forme ensuite un certain anneau d'endomorphismes $\hat{P}$, en lui appliquant un théorème de Jacobson-Bourbaki [1], Ch. 11, paragraphe 5, p. 71, Théorème 3 b), on prouve que les dimensions de P et P_K^L sont égales, ce qui démontre l'équivalence de ces bimodules.

BIBLIOGRAPHIE

[1] BOURBAKI (Nicolas). - Algèbre, Chapitre 2 : algèbre linéaire, 2e éd. - Paris, Hermann, 1955 (Act. scient. et ind., 1032-1236; Eléments de Mathématique, 6).

[2] LAZARD (Michel). - Théorie de Galois : Extensions séparables normales des corps commutatifs, Séminaire Châtelet-Dubreil, t. 1, 1947/48, n° 3.