

SÉMINAIRE DUBREIL. ALGÈBRE ET THÉORIE DES NOMBRES

PIERRE SAMUEL

Éléments de la théorie des algèbres

Séminaire Dubreil. Algèbre et théorie des nombres, tome 1 (1947-1948), exp. n° 5, p. 1-15

<http://www.numdam.org/item?id=SD_1947-1948__1__A5_0>

© Séminaire Dubreil. Algèbre et théorie des nombres
(Secrétariat mathématique, Paris), 1947-1948, tous droits réservés.

L'accès aux archives de la collection « Séminaire Dubreil. Algèbre et théorie des nombres » 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/>

ÉLÉMENTS DE LA THÉORIE DES ALGÈBRES

par Pierre SAMUEL

1. Etude du radical d'un anneau.

Il ne s'agira dans cet exposé que d'anneaux commutatifs, et possédant un élément unité, noté 1 .

1° Idéal maximal. - Dans un anneau A , un idéal est maximal s'il n'est contenu que dans lui-même et dans l'idéal trivial A . L'application du théorème de Zorn montre que si un anneau contient un idéal non trivial, A , il existe un idéal maximal contenant A .

Pour qu'un idéal M soit maximal, il faut et il suffit que l'anneau quotient A/M soit un corps.

Si M est un idéal maximal, tout élément a qui n'est pas dans M a un inverse, mod M , si non l'ensemble des éléments :

$$a' = ax + m \quad (x \in A, m \in M)$$

ne contiendra pas 1, et constituera un idéal M' , différent de A et de M et contenant M .

Réciproquement, si A/M est un corps, tout idéal M' , contenant M et un élément a qui n'est pas dans M , contient tous les éléments a' construits ci-dessus et en particulier 1, puisque la classe $a + M$ a une inverse ; M' est donc égal à A .

2° Radical d'un anneau. - Le radical R d'un anneau A est l'intersection de tous ses idéaux maximaux. Un anneau est appelé semi-simple quand son radical est nul.

Propriété caractéristique. - Pour qu'un élément a d'un anneau appartienne au radical, il faut et il suffit que l'élément $1 - ax$ ait un inverse (ou soit inversible), quel que soit l'élément x de A .

Si a est contenu dans tout idéal maximal, $a' = 1 - ax$ a nécessairement

un inverse. Si non les éléments $a', \dots$ définiraient un idéal non trivial qui serait contenu dans un idéal maximal M , qui contiendrait à la fois :

$$a, \quad a' = 1 - ax, \quad \text{donc } 1;$$

ce qui est absurde.

Si $a' = 1 - ax$ a un inverse, quel que soit l'élément x de A , a est contenu dans tout idéal maximal M . Si non a n'étant pas contenu dans l'idéal maximal M , la classe $a, (\text{mod } M)$, aurait une inverse et il existerait x' dans A , tel que $ax' = 1$ soit contenu dans M ; ce qui est absurde, puisque $ax' = 1$ a un inverse et que M n'est pas l'idéal trivial A .

3° Éléments nilpotents. - Un élément est nilpotent si l'une de ses puissances est nulle :

$$a^n = 0 \quad (n \text{ entier positif}).$$

L'ensemble de tous les éléments nilpotents d'un anneau est un idéal contenu dans le radical.

L'ensemble N des éléments nilpotents est un idéal :

$$a^p = 0 \quad \text{et} \quad b^q = 0 \longrightarrow (xa + yb)^{p+q+1} = 0$$

pour tous éléments x, y de A , car tout monôme du développement du deuxième membre contient soit une puissance de a d'exposant supérieur à p , soit une puissance de b , d'exposant supérieur à q .

Si a^n est nul, $1 - ax$ a un inverse, car :

$$(1 - ax)(1 + ax + a^2 x^2 + \dots + a^{n-1} x^{n-1}) = 1 - a^n x^n = 1;$$

c'est la condition pour que a soit dans le radical.

En général il n'y a pas égalité entre le radical et l'ensemble des éléments nilpotents, ainsi que le montre l'exemple de l'anneau des entiers p -adiques ; le radical est alors l'idéal de valuation et le seul élément nilpotent est 0 .

Il y a toutefois égalité dans le cas important des anneaux d'Artin.

4° Anneaux d'Artin. - Un anneau est d'Artin si toute famille d'idéaux y possède un élément minimal. Il est équivalent de dire que toute suite "descendante" d'idéaux de A :

$$I_1 \supset I_2 \supset \dots \supset I_n \supset \dots$$

n'a qu'un nombre fini de termes différents.

Dans un anneau d'Artin, tout élément a du radical R est nilpotent ; (R est un nilidéal et contient tout nilidéal).

Formons la suite descendante des idéaux principaux :

$$(a) \supset (a^2) \supset \dots \supset (a^n) \supset \dots ;$$

puisque'elle n'a qu'un nombre fini de termes, différents, il existe nécessairement un exposant n tel que :

$$(a^{n+1}) = (a^n) ;$$

et, par suite

$$(a^{n+i}) = (a^n) \quad (\text{pour tout } i)$$

Il en résulte :

$$a^n = x \cdot a^{n+1}, \quad x \in A, \quad \text{ou} \quad a^n(1 - xa) = 0$$

Comme $1 - xa$ a un inverse, cette égalité entraîne l'annulation de a^n ; de sorte que a est bien nilpotent.

Sous le nom de théorème de Hopkins, on démontre la propriété suivante :

Dans un anneau d'Artin, tout nilidéal I (idéal dont tous les éléments sont nilpotents : il en est ainsi par exemple pour le radical R) est un idéal nilpotent (c'est-à-dire qu'une puissance I^s de l'idéal est zéro). En particulier, le produit de s éléments de I est nul.

Il suffit de démontrer cette propriété pour l'idéal N , constitué par tous les éléments nilpotents ; elle restera vraie pour tout sous-idéal de N .

La suite descendante des puissances N^i n'ayant qu'un nombre fini de termes différents, il existe s tel que $N^s = N^{s+1}$.

Soit alors d un élément de N^s , on peut trouver :

$$d_1' \in N^s, \quad a_1 \in N, \quad \text{tels que} \quad d = a_1 d_1'$$

On peut répéter le même raisonnement sur d_1' , en formant a_2 et d_2' , puis sur d_2' et ainsi de suite ; on constitue une suite d'éléments a_i de N , tels que :

$$d = a_1 a_2 \dots a_n d_n' \quad d_n' \in N^s$$

Mais la suite descendante des idéaux principaux :

$$(a_1) \supset (a_1 a_2) \supset \dots \supset (a_1 a_2 \dots a_h) \supset \dots$$

n'a qu'un nombre fini de termes différents ; il existe donc un indice k , tel que :

$$a_1 a_2 \dots a_k = a_1 a_2 \dots a_k a_{k+1} x, \text{ ou } (a_1 a_2 \dots a_k)(1 - a_{k+1} x) = 0$$

ce qui entraîne l'annulation de $(a_1 a_2 \dots a_k)$ et par suite de d qui est élément quelconque de N^S .

5° Anneau local. - Un anneau A est appelé local, s'il existe dans A un idéal P , tel que tout élément de A , qui n'est pas dans P , ait un inverse (soit inversible, ou diviseur de 1).

Un tel anneau n'a qu'un idéal maximal qui est P , lequel est par suite le radical de A .

En effet tout idéal de A , ou bien est contenu dans P , ou bien contient un diviseur de 1, donc est égal à l'idéal trivial A . L'idéal P n'est donc contenu que dans A , et aucun autre idéal n'est maximal, puisque contenu dans P , ou égal à A .

Un anneau de valuation, un anneau de série formelles constituent des exemples d'anneaux locaux.

Dans un anneau local, il n'y a d'autres éléments idempotents que 0 et 1.

Effectivement si c est idempotent, il en est de même de $1 - c$:

$$c^2 = c \rightarrow (1 - c)^2 = 1 - 2c + c^2 = 1 - c.$$

Si aucun de ces deux éléments, c et $1 - c$ n'est diviseur de 1, ils appartiennent tous deux à l'idéal maximal P , ce qui est absurde, puisqu'il contiendrait 1.

2. Structure des algèbres finies.

1° Algèbre finie. - Une algèbre sur un corps K est un espace vectoriel A , dans lequel existe une multiplication associative, distributive par rapport à l'addition.

L'hypothèse de A espace vectoriel comporte l'existence, dans A : d'une addition (de signe $+$, associative et commutative) ; de l'opération inverse, ou soustraction (de signe $-$) ; de la multiplication par les éléments de K ,

appelés scalaires, (associative relativement aux scalaires et doublement distributive). L'existence de ces opérations peut être exprimée par la condition d'appartenance :

$$\alpha, \beta \in A \text{ et } x, y \in K \longrightarrow \alpha x + \beta y \in A.$$

En raison de l'existence d'une multiplication cette algèbre est un anneau ; conformément aux conventions restrictives faites ci-dessus, nous supposons que cette algèbre, ou cet anneau, contient un élément unité et que la multiplication est commutative. Il en résulte qu'elle contient un sous-anneau, isomorphe de K , constitué par les produits de l'élément unité par les scalaires (éléments de K) ; c'est une "extension" de K , considéré comme anneau.

Une algèbre est finie, et de dimension h , quand elle est définie par un espace vectoriel fini, de dimension h , c'est-à-dire si ses éléments se déduisent (par multiplication par des scalaires et addition) d'une "base" de h éléments α_i , indépendants dans K :

$$\alpha \in A \implies \alpha = \sum x_i \alpha_i \quad (x_i \in K) \quad (i \text{ de } 1 \text{ à } h).$$

$$\sum x_i \alpha_i = 0 \implies x_i = 0$$

La multiplication dans A est alors définie par une table de multiplication des éléments de la base :

$$\alpha_i \cdot \alpha_j = \sum a_{ijk} \alpha_k \quad (i, j, k \text{ de } 1 \text{ à } h).$$

Entre les h^3 coefficients scalaires a_{ijk} existent des relations telles que la multiplication des h éléments α_i soit commutative ($a_{ijk} = a_{jik}$), associative, et qu'il existe un élément 1 . (Si on le suppose égal à α_1 , ces dernières relations sont :

$$j \neq k \longrightarrow a_{1jk} = a_{j1k} = 0, \quad (a_{1jj} = a_{j1j} = 1).$$

On peut représenter un élément α de l'algèbre A par la matrice carrée $\bar{A}$ des coefficients de la table de multiplication de α par les éléments α_i , d'après la relation matricielle :

$$\alpha \cdot ||\alpha_1 \alpha_2 \dots \alpha_h|| = ||\alpha_1 \alpha_2 \dots \alpha_h|| \times \bar{A};$$

A l'élément α_i correspond la matrice $\bar{A}_i = ||a_{ijk}||$ (k ligne, j colonne).

Cette représentation conserve les opérations : addition, produit par un scalaire, multiplication.

EXEMPLES. - Une extension d'un corps est une algèbre qui est un corps.

Une somme directe d'algèbres : A d'éléments α , B d'éléments β , ..., est encore une algèbre.

La somme directe de A et B est l'ensemble des couples

$$\gamma = ||\alpha \quad \beta||$$

les opérations étant définies par les conjonctions des opérations sur les coordonnées :

$$x_1 ||\alpha_1 \quad \beta_1|| + x_2 ||\alpha_2 \quad \beta_2|| = ||x_1 \alpha_1 + x_2 \alpha_2 \quad x_1 \beta_1 + x_2 \beta_2||$$

$$||\alpha_1 \quad \beta_1|| \times ||\alpha_2 \quad \beta_2|| = ||\alpha_1 \alpha_2 \quad \beta_1 \beta_2|| .$$

Une somme directe d'extensions de corps (qui sont des corps) est une algèbre qui a des diviseurs de zéro.

PROPRIÉTÉS. - Si une algèbre finie est construite sur un corps de base K, on en définit une extension sur un sur-corps L de K, en formant les éléments :

$$\sum z_i \alpha_i \quad (\alpha_i \text{ éléments de base de A sur K, } z_i \in L) .$$

C'est encore une algèbre sur L, car la multiplication définie dans A par les coefficients a_{ijk} (de K), reste ainsi définie dans l'extension formée et conserve ses propriétés.

Une algèbre finie, de dimension h, est un anneau d'Artin, car un idéal est un sous-espace vectoriel, et toute suite descendante d'idéaux ne peut avoir que h + 1 termes au plus (y compris 0) .

2° Algèbre locale. - Une algèbre A, sur un corps K est locale, ou primaire, si l'anneau sous-jacent est local. Le radical de A est l'idéal maximal P' .

Tout élément de A qui n'est pas diviseur de 1, ou qui est diviseur de 0, est nilpotent : il appartient en effet à P' qui est lui-même nilpotent.

Dans une algèbre A, sur un corps K, l'anneau quotient $A|Q$, de A par

un idéal Q , est encore une algèbre sur K , a fortiori finie, si K est finie.

La congruence, mod Q , respecte en effet les diverses opérations :

$$\alpha \equiv \alpha' \quad \text{et} \quad \beta \equiv \beta' \quad (\text{mod } Q)$$

$$\longrightarrow (x\alpha + y\beta) \equiv (x\alpha' + y\beta') ; \quad \alpha\beta \equiv \alpha'\beta' \quad (\text{mod } Q)$$

ce qui est d'une vérification immédiate.

En outre Q ne renfermant aucun scalaire (élément de K) les scalaires restent distincts dans A/Q .

Si dans une algèbre A , un idéal P' est contenu dans un idéal maximal P et en contient une puissance P^S :

$$P^S \subset P' \subset P$$

l'algèbre A/P' est locale et son idéal maximal est formé des éléments de P , définis mod P' .

D'une part toute classe, mod P' , dont un élément α est dans P est nilpotente, car :

$$\alpha^S \in P^S \subset P' \longrightarrow \alpha^S = 0 \quad (\text{mod } P')$$

D'autre part toute classe, de représentant ζ , qui n'a pas d'élément commun avec P a une inverse. En effet ζ a un inverse, mod P (dans A), ou dans A/P qui est un corps) :

$$\zeta\zeta' = 1 - \alpha \quad (\alpha \in P) .$$

Il suffit alors de construire ζ'' :

$$\zeta'' = \zeta'(1 + \alpha + \alpha^2 + \dots + \alpha^{S-1}) ;$$

et :

$$\zeta\zeta'' = 1 - \alpha^S \equiv 1 \quad (\text{mod } P') .$$

THEOREME de Wedderburn. - La propriété de structure est alors exprimée par l'énoncé :

Toute algèbre finie, sur un corps K , est une somme directe d'algèbres locales (en nombre fini).

La démonstration comporte diverses étapes : décomposition du radical comme

intersection d'idéaux maximaux ;

- construction d'un système d'éléments "orthogonaux" ;
- formation des algèbres locales.

3° Décomposition du radical. - Dans une algèbre finie A , le radical R est l'intersection d'un certain nombre n (fini) d'idéaux maximaux :

$$R = [P_1, P_2, \dots, P_n] \text{ ou } R = P_1 \cap P_2 \cap \dots \cap P_n$$

Il suffit de construire une suite d'idéaux maximaux P_i , de façon que la suite descendante des intersections :

$$Q_1 = P_1 \quad Q_2 = [P_1, P_2] \quad \dots \quad Q_i = [P_1, P_2, \dots, P_i] \quad \dots$$

soit propre, c'est-à-dire ne contienne que des idéaux distincts.

On prend pour cela l'idéal P_i , s'il en existe, maximal et ne contenant pas l'intersection Q_{i-1} .

La suite est nécessairement limitée, puisque l'algèbre étant finie est un anneau d'Artin. Le dernier terme est le radical dont on a ainsi établi la décomposition.

On peut appliquer à cette décomposition le théorème de Jordan : le nombre n d'idéaux maximaux (longueur de la suite de décomposition) est indépendant du mode de décomposition.

Les idéaux de l'algèbre A constituent en effet un treillis (ou lattice, ou structure de ORE) au point de vue de l'inclusion.

Le plus grand sous-idéal commun de deux idéaux I_1 et I_2 est leur intersection $[I_1, I_2]$; le plus petit sur-idéal commun est la "réunion complétée" (I_1, I_2) , idéal ayant pour générateurs les éléments de I_1 et I_2 (ou seulement leurs générateurs respectifs).

Ce treillis est normal, ou vérifie la condition de Dedekind :

$$I_1 \subset I_2 \rightarrow (\overline{I_1}, [I_2, J]) = [I_2, (\overline{I_1}, J)] ;$$

les idéaux sont en effet des "sous-groupes invariants" de A , considéré comme groupe additif.

Je rappelle sommairement la démonstration ; le premier membre de l'égalité est un idéal manifestement contenu dans le deuxième membre.

D'autre part un élément α du deuxième membre, étant dans $(\overline{I_1}, J)$ est de la forme :

$$\alpha = \alpha_1 + \beta \quad (\alpha_1 \in I, \quad \beta \in J)$$

comme α_1 est a fortiori dans I_2 , pour que α soit aussi dans I_2 il faut que β soit dans I_2 , donc dans l'intersection $[I_2, J]$; il en résulte bien que α est dans la réunion complétée du premier membre.

D'autre part la suite de composition des Q_i est maximale (on ne peut intercaler de terme sans la rendre impropre).

En effet l'idéal Q_{i+1} est maximal dans l'idéal Q_i , pris comme anneau, car l'anneau quotient Q_i/Q_{i+1} , isomorphe à A/P_{i+1} est un corps. On se trouve bien dans les conditions d'application du théorème de Jordan-Hölder.

4° Construction d'éléments orthogonaux. - On peut caractériser un système d'idéaux maximaux P_i par la condition qu'aucun des P_i ne contienne le produit des autres que je noterai :

$$Q'_i = \prod_{j \neq i} P_j, \quad (i' \text{ de } 1 \text{ à } n, \text{ sauf } i)$$

Cette condition entraîne manifestement celle qui a servi à la formation du système car P_i ne peut alors contenir $Q_i - 1 \supset Q'_i$.

Je vais établir la réciproque en établissant la propriété plus précise : on peut construire un élément δ_i , tel que ;

$$\delta_i \equiv 1 \pmod{P_i}, \quad \delta_i \equiv 0 \pmod{Q'_i}$$

(δ_i n'étant pas dans P_i , il en sera de même, a fortiori, de Q'_i)

D'une part deux idéaux de la suite sont différents, car si $P_i = P_j$ et par exemple $i < j$, comme P_i contient $[P_1, \dots, P_{i-1}, P_i]$, P_j contiendrait $[P_1, \dots, P_{j-1}]$, ce qui est contraire à l'hypothèse.

La réunion complétée $(\overline{P_i}, P_j)$ ne peut être que l'idéal trivial A , puisqu'elle contient P_i et ne lui est pas égale. Il existe donc un élément α_{ij} tel que :

$$\alpha_{ij} \equiv 1 \pmod{P_i}, \quad \alpha_{ij} \equiv 0 \pmod{P_j}$$

L'élément :

$$\delta_i = \prod_{j \neq i} \alpha_{ij} \quad (j \text{ de } 1 \text{ à } n, \text{ } i \text{ exclus})$$

vérifie la condition annoncée.

Le radical R de l'algèbre étant nilpotent, d'exposant s ($R^s = 0$), je construis les n éléments :

$$\theta_i = 1 - (1 - \zeta_i^s)^s ;$$

ils vérifient les conditions d'orthogonalité :

$$i \neq j \longrightarrow \theta_i \theta_j = 0, \quad \theta_i^2 = \theta_i, \quad \sum \theta_i = 1 \quad (i \text{ de } 1 \text{ à } n)$$

D'une part, de la construction des θ_i , il résulte :

$$\begin{aligned} \zeta_i^s &\equiv 0 \pmod{Q_i'} ; & (1 - \zeta_i^s)^s &\equiv 1 \pmod{(Q_i')^s} ; & \theta_i &\equiv 0 \pmod{(Q_i')^s} \\ (1 - \zeta_i^s) &\equiv 0 \pmod{P_i} ; & (1 - \zeta_i^s)^s &\equiv 0 \pmod{(P_i)^s} ; & \theta_i &\equiv 1 \pmod{(P_i)^s} \end{aligned}$$

D'autre part, en tenant compte des inclusions :

$$Q_i' Q_j' \subset [\dots P_i \dots] = R ; \quad P_i Q_i' \subset [\dots P_i \dots] = R ; \quad \prod P_i \subset [\dots P_i \dots] = R$$

et de la nilpotence de R , on obtient :

$$\begin{aligned} i \neq j &\longrightarrow \theta_i \theta_j \equiv 0 \pmod{(Q_i')^s} \quad (Q_j')^s \subset R^s = 0 \longrightarrow \theta_i \theta_j = 0 \\ \theta_i (1 - \theta_i) &\equiv 0 \pmod{(Q_i')^s} \quad (P_i)^s \subset R^s = 0 \longrightarrow \theta_i (1 - \theta_i) = 0 \\ \prod (1 - \theta_i) &\equiv 0 \pmod{(P_i)^s} \subset R^s = 0 \longrightarrow \prod (1 - \theta_i) = 0 ; \end{aligned}$$

et

$$0 = \prod (1 - \theta_i) = 1 - \sum \theta_i + \sum \theta_i \theta_j - \dots = 1 - \sum \theta_i$$

5° Formation des algèbres locales. - En raison de la 3e relation tout élément α de A peut être mis sous forme d'une somme :

$$\alpha = \sum \alpha \theta_i \quad \text{ou} \quad A = \sum A \cdot \theta_i \quad (i \text{ de } 1 \text{ à } n) .$$

En raison des deux premières conditions d'orthogonalité, cette expression se comporte comme une somme directe :

$$x\alpha + y\beta = \sum (x\alpha + y\beta) \theta_i ; \quad \alpha\beta = \sum (\alpha \theta_i) (\beta \theta_i) \quad (i \text{ de } 1 \text{ à } n) .$$

Les éléments $\alpha \theta_i$ (de $A \cdot \theta_i$) constituent un anneau isomorphe de l'anneau quotient A/P_i^s .

En effet, d'une part les éléments nuls $\omega \theta_i$ y sont bien définis par $\omega \in P_i^s$, car :

$$\omega \theta_i = 0 \longrightarrow 0 \equiv \omega \theta_i \equiv \omega \pmod{P_i^s} ;$$

et

$$\omega \in P_i^s \longrightarrow \omega \theta_i \in P_i^s \theta_i^s \subset R^s = 0 .$$

D'autre part, il y a bien conservation des opérations.

L'anneau considéré est donc bien une algèbre locale sur K ($P_i^s = P' \subset P_i$), ce qui établit la propriété de Wedderburn.

Cas particulier. - Si une algèbre (finie et commutative) est semi-simple, son radical R est nul, ou nilpotent d'exposant $s = 1$; les algèbres locales construites sont isomorphes aux corps quotients $A|P_i$, de sorte que :

Une algèbre (commutative, finie) semi-simple est une somme directe de corps.

3. Séparabilité et semi-simplicité.

1° Dérivation. - Pour une algèbre A , définie sur un corps K , on appelle dérivation de A une transformation ou application, de A dans A , représentée par le signe fonctionnel $D(\dots)$

$$\alpha \longrightarrow D(\alpha) \in A ,$$

telle que :

$$a \in K \longrightarrow D(a) = 0 ; \quad D(\alpha + \beta) = D(\alpha) + D(\beta) ;$$

$$D(\alpha \beta) = \alpha D(\beta) + D(\alpha) \beta .$$

Il en résulte, plus généralement :

$$D(x \alpha + y \beta) = x D(\alpha) + y D(\beta) ,$$

et, si l'algèbre est finie :

$$D\left(\sum x_i \alpha_i\right) = \sum x_i D(\alpha_i) \quad (i \text{ de } 1 \text{ à } n) .$$

La transformation, conservant la structure d'espace linéaire peut être appelée linéaire.

2° Séparabilité. - Une algèbre finie est séparable si elle ne possède que la seule dérivation (identiquement) nulle ($D(\alpha) = 0$ (pour tout α)).

Cette définition comprend comme cas particulier la notion de séparabilité d'une extension $K(\alpha)$, d'un corps K , définie par l'adjonction au corps K d'un élément α , zéro d'un polynôme

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_0$$

irréductible dans K .

Cette extension a pour éléments de base les puissances :

$$\alpha^i \quad (i \text{ de } 0 \text{ à } n-1)$$

d'après les règles de dérivation, on doit avoir :

$$0 = D(f(\alpha)) = (n\alpha^{n-1} + a_1(n-1)\alpha^{n-2} + \dots)D(\alpha) .$$

La condition ordinaire de séparabilité est que le polynôme entre crochets ne soit pas nul ($f(x)$ sans zéro, double dans l'extension $K(\alpha)$). Elle est donc équivalente à ce que la seule dérivation possible soit $D(\alpha) = 0$, par suite $D(\alpha^i) = 0$ et par suite la dérivation de tout élément $D(h(\alpha)) = 0$.

La dérivation peut être déterminée par les expressions des dérivés des éléments d'une base :

$$D(\alpha_i) = \sum d_{i\ell} \alpha_\ell ; \quad (\ell \text{ de } 1 \text{ à } n, \text{ pour chaque } i)$$

Les coefficients scalaires $d_{i\ell}$ sont liés aux coefficients scalaires a_{ijk} , de la table de multiplication de l'algèbre, par des relations linéaires :

$$\sum (a_{ik\ell} d_{jk} + a_{jkl} d_{ik}) = \sum a_{ijk} d_{k\ell} \quad (k \text{ de } 1 \text{ à } n, \text{ pour tous } i, j, \ell)$$

Il suffit pour cela de calculer de deux façons la dérivée du produit $\alpha_i \alpha_j$; d'une part par application de la distributivité :

$$D(\alpha_i \alpha_j) = \sum a_{ijk} D(\alpha_k) = \sum (\sum a_{ijk} d_{k\ell}) \alpha_\ell \quad (\text{indices } k, \ell)$$

d'autre part par application de la formule de dérivation d'un produit :

$$\begin{aligned} D(\alpha_i \alpha_j) &= \alpha_i D(\alpha_j) + D(\alpha_i) \alpha_j = \alpha_i \sum (d_{jk} \alpha_k) + \sum (d_{ik} \alpha_k) \alpha_j \\ &= \sum (\sum a_{ik\ell} d_{jk} + a_{jkl} d_{ik}) \alpha_\ell \quad (\text{indices } k, \ell) \end{aligned}$$

L'égalité exprime d'ailleurs la relation entre les matrices A_i et $D(A_i)$,

représentatives des éléments α_i et $D(\alpha_i)$:

$$A_i \cdot D(A_j) + D(A_i) \cdot A_j = \sum a_{ijk} D(A_k) ,$$

une algèbre finie inséparable, le reste dans toute extension du corps de base.

En effet si une algèbre A , finie sur un corps K , admet une dérivation (non nulle) caractérisée par des coefficients (dans K), cette dérivation subsiste dans une extension L de K , à condition de conserver les mêmes coefficients de multiplication a_{ijk} et de dérivation d_{ik} , puisqu'ils vérifient les mêmes relations linéaires (dans K , et, a fortiori, dans L).

PROPRIÉTÉ caractéristique. - Les algèbres finies séparables sont celles qui restent semi-simples, dans toute extension du corps de base.

Cette équivalence peut être exprimée schématiquement par la double implication :
semi-simple dans tout $L \supset K \iff$ séparable dans tout K .

On démontre en réalité la contraposée de l'implication droite, gauche, et l'implication gauche.droite elle-même, soient les deux implications :

non semi-simple dans un $L \rightarrow$ inséparable dans un K (égal à L)
semi-simple dans tout $L \supset K \rightarrow$ séparable dans tout K .

3° Semi-simplicité. - Je considère une algèbre A , dans un corps K , qui n'est pas (ou ne reste pas) semi-simple dans l'extension L , algébriquement fermée du corps K ; je vais démontrer qu'elle est inséparable dans ce même corps L , c'est-à-dire y admet une dérivation non nulle.

Il suffit de le faire pour une algèbre locale A_0 , dans L , dont le radical, ou idéal maximal unique, R_0 n'est pas nul.

Il suffira, en effet, ensuite de décomposer l'algèbre A , finie et non semi-simple sur L , en une somme directe d'algèbres locales $A\theta_i$. Pour l'une d'elles, au moins, notée $A\theta_0 = A_0$, le radical $R_0 = P_0$ n'est pas nul.

On prendra alors pour dérivation $D(A)$, une transformation égale à $D(A_0)$, pour tout élément de A_0 et nulle pour tous les éléments des autres algèbres $A\theta_i$.

Le radical R_0 de A_0 étant nilpotent d'exposant $s > 1$, il existe un élément ω (peut-être égal à 1) tel que :

$$\omega \cdot R_0^2 = 0 , \quad \omega \cdot R_0 \neq 0$$

Comme $R_0^{s-1} = R_0^{s-2} \cdot R_0 \neq 0$, il existe au moins un élément ω , dans R_0^{s-2} (peut-être réduit à 1), tel que $\omega \cdot R_0 \subset R_0^{s-1}$ ne soit pas nul. Il vérifie bien en outre $\omega \cdot R_0^2 \subset R_0^{s-2} \cdot R_0^2 = R_0^s = 0$.

La dérivée de $\lambda \in A_0$ sera alors définie par les conditions :

$$\lambda = \ell(\lambda) + \omega(\lambda), \quad \ell(\lambda) \in L, \quad \psi(\lambda) \in R_0, \quad D(\lambda) = \omega \cdot \psi(\lambda).$$

Le corps quotient A_0/R_0 étant une extension finie de L , qui est algébriquement fermé, est nécessairement isomorphe à L lui-même ; comme d'autre part R_0 ne contient aucun scalaire (de L), la décomposition indiquée de λ n'est possible que d'une seule façon.

L'expression $D(\lambda)$ est bien une dérivation non nulle.

Le choix de ω montre qu'il existe dans $\omega \cdot R_0$ un élément $\omega \lambda_0$ non nul, et

$$\lambda_0 = \psi(\lambda_0) \in R_0, \quad D(\lambda_0) = \omega \lambda_0 \neq 0.$$

Cette transformation $D(\lambda)$ est manifestement linéaire, car

$$\ell_1 \lambda_1 + \ell_2 \lambda_2 = \ell_1 \cdot \ell(\lambda_1) + \ell_2 \cdot \ell(\lambda_2) + \ell_1 \psi(\lambda_1) + \ell_2 \psi(\lambda_2) \quad (\ell_i, \ell(\lambda_i) \in L)$$

et :

$$D(\ell_1 \lambda_1 + \ell_2 \lambda_2) = \ell_1 (\omega \psi(\lambda_1)) + \ell_2 (\omega \psi(\lambda_2))$$

Par ailleurs le produit par ω a pour conséquence de déterminer $D(\lambda)$, pour λ défini au module R_0^2 près, car :

$$\begin{aligned} \lambda \equiv \lambda' \pmod{R_0^2} &\longrightarrow \psi(\lambda) \equiv \psi(\lambda') \pmod{R_0^2} ; \\ &\longrightarrow \omega \cdot \psi(\lambda) \equiv \omega \cdot \psi(\lambda'), \pmod{R_0^s = 0} \longrightarrow D(\lambda) = D(\lambda'). \end{aligned}$$

Il en résulte la règle de dérivation du produit :

$$\lambda_1 \lambda_2 \equiv \ell(\lambda_1) + \ell(\lambda_2) + \lambda_1 \cdot \psi(\lambda_2) + \psi(\lambda_1) \cdot \lambda_2 \pmod{R_0^2}$$

et

$$D(\lambda_1 \lambda_2) = \lambda_1 D(\lambda_2) + D(\lambda_1) \cdot \lambda_2.$$

EXEMPLE. - Un exemple de construction de dérivation dans une algèbre non simple est fourni par l'ensemble des éléments :

$$x + y\theta ; \theta^2 = 0 ; x, y \in K ;$$

(qui définissent par exemple un calcul d'approximations). Il suffit de prendre pour dérivée :

$$D(x + y\theta) = y\theta .$$

Une représentation par des matrices serait :

$$x \cdot \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} + y \cdot \begin{vmatrix} 1 & 1 \\ -1 & -1 \end{vmatrix} = \begin{vmatrix} x+y & y \\ -y & x-y \end{vmatrix}$$

4° Séparabilité (suite). - Considérons une algèbre A , sur un corps K , semi-simple dans toute extension, et, notamment, dans l'extension L , algébriquement fermée de K . Une dérivation dans K subsiste dans L , (d'après la remarque sur les valeurs des coefficients) ; elle y est nécessairement nulle, de sorte que A est séparable sur K .

En effet A , considéré dans l'extension L , est somme directe de corps, qui d'après la remarque de la démonstration précédente sont tous isomorphes à L :

$$A = \sum L \cdot \theta_i , \quad \theta_i = \theta_i^2 = \theta_i^3 = \dots$$

Pour toute dérivation, on doit donc avoir :

$$\begin{aligned} D(\theta_i) &= D(\theta_i^2) = 2\theta_i \cdot D(\theta_i) \\ &= D(\theta_i^3) = 3\theta_i^2 \cdot D(\theta_i) = 3\theta_i \cdot D(\theta_i) \end{aligned}$$

d'où par différence :

$$0 = \theta_i \cdot D(\theta_i) = 2\theta_i \cdot D(\theta_i) = D(\theta_i) = 0$$

BIBLIOGRAPHIE

- [1] CHEVALLEY (Claude). - On the theory of local rings, *Annals of Math.*, t. 44, 1943, p. 690-708.
- [2] HOCHSCHILD (G.). - On the cohomology groups of an associative algebra, *Annals of Math.*, t. 46, 1945, p. 58-67.
- [3] JACOBSON (Nathan). - The theory of rings. - New-York, American mathematical Society, 1943 (*Mathematical Surveys*, 2).
- [4] JACOBSON (Nathan). - The radical and semi-simplicity for arbitrary rings, *Amer. J. of Math.*, t. 67, 1945, p. 300-320.