Séminaire Dubreil.
Algèbre et théorie
des nombres

Maurice Crestey

Travaux récents sur les algèbres universelles

Séminaire Dubreil. Algèbre et théorie des nombres, tome 19, n° 1 (1965-1966), exp. n° 4, p. 1-9

<http://www.numdam.org/item?id=SD_1965-1966__19_1_A3_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
19e année, 1965/66, n° 4

6 décembre 1965

TRAVAUX RÉCENTS SUR LES ALGÈBRES UNIVERSELLES

par Maurice CRESTEY

[d'après E. MARCZEWSKI, W. NARKIEWICZ, K. URBANIK, etc.]

1. Rappel de résultats classiques concernant les bases des modules libres.

On sait que la théorie des bases des modules sur un anneau A ne conduit pas à des résultats aussi remarquables que la théorie analogue des bases des espaces vectoriels. C'est ainsi qu'un A-module n'admet pas toujours de base, et que, pour certains anneaux A , il peut exister des A-modules libres ayant des bases finies de cardinaux différents ([2], § 1, exercice 16).

Cependant, on a pu établir les théorèmes suivants, qui rappellent certaines propriétés des bases des espaces vectoriels :

THÉORÈME 1.1 ([2], § 1, n° 12). - Si A est un anneau unitaire, et E un A-module unitaire admettant une base infinie B , toute autre base B' de E a le même cardinal que B .

THÉORÈME 1.2 ([2], § 7, n° 2). - Si A est un anneau unitaire, et E un A-module unitaire libre, il suffit qu'il existe un homomorphisme de l'anneau A dans un corps D pour que deux bases quelconques de E aient le même cardinal.

THÉORÈME 1.3 ([3], § 5, n° 6). - Si E est un anneau unitaire, et A un sous-anneau simple de E ayant même élément unité, E est un A-module libre et deux bases quelconques de E ont le même cardinal.

Remarques.

1. La suite de cet exposé montrera que l'on peut sans inconvénient supprimer le mot "unitaire" dans l'énoncé du théorème 1.1.

2. Les conditions du théorème 1.2 sont remplies dans les cas particuliers :

(a) L'anneau A est un corps.

(b) L'anneau A est unitaire, commutatif, non réduit à l'élément 0 .

3. Dans l'énoncé du théorème 1.3, A est un anneau simple au sens de [3],

c'est-à-dire non réduit à l'élément 0 , artinien à gauche, et sans idéaux bilatères propres.

4. Le théorème 1.3 permet de s'assurer que la condition suffisante fournie par le théorème 1.2 n'est nullement nécessaire.

Les notions d'indépendance et de base ont été définies pour des structures algébriques plus générales que la structure de module sur un anneau. Il est naturel de se demander si certaines des propriétés classiques subsistent lorsqu'on envisage ces structures plus générales. La suite de cet exposé est consacrée à un résumé des travaux effectués depuis quelques années par les algébristes Polonais de l'Université de Wroclaw. On pourra se reporter pour certaines démonstrations (malheureusement très longues) aux mémoires originaux, tous rédigés en langue anglaise.

2. Algèbres universelles. Opérations.

Considérons un ensemble non vide A , et pour chaque entier $n \geqslant 0$, une famille $\mathfrak{F}_n$ (éventuellement vide) d'applications du produit cartésien A^n dans A . Chaque $f \in \mathfrak{F}_n$ sera appelée opération à n variables. Une opération à 0 variable consiste à désigner un élément de A .

Nous poserons $\mathfrak{F} = \bigcup_{n \geqslant 0} \mathfrak{F}_n$, et nous appellerons algèbre universelle le couple $(A , \mathfrak{F})$. A est le support et $\mathfrak{F}$ la famille des opérations fondamentales de cette algèbre universelle ([1], [5], [6], [9], [10]).

Une sous-algèbre $(B , \mathfrak{F})$ est un couple pour lequel B est une partie non vide de A , stable par toutes les $f \in \mathfrak{F}$. On montre sans difficulté que, pour toute partie non vide S de A , il existe une plus petite partie $\overline{S}$ contenant S et stable par toutes les $f \in \mathfrak{F}$. $(\overline{S} , \mathfrak{F})$ est appelée sous-algèbre engendrée par S .

Une congruence $\mathcal{C}$ de l'algèbre $(A , \mathfrak{F})$ est une relation d'équivalence définie sur A telle que, pour tout $n \geqslant 0$, pour tout $f \in \mathfrak{F}_n$, pour tout système $\{x_1 , x_2 , \dots , x_n ; y_1 , y_2 , \dots , y_n\}$ de $2n$ éléments de A , l'hypothèse $x_i \equiv y_i \ (\mathcal{C})$, $i = 1 , 2 , \dots , n$, entraîne

$$f(x_1 , x_2 , \dots , x_n) \equiv f(y_1 , y_2 , \dots , y_n) \ (\mathcal{C}) \ .$$

Si $(A , \mathfrak{F})$ et $(A' , \mathfrak{F}')$ sont deux algèbres telles qu'il existe une bijection β de $\mathfrak{F}$ sur $\mathfrak{F}'$ dans laquelle $\beta(\mathfrak{F}_n) = \mathfrak{F}'_n$, un homomorphisme de $(A , \mathfrak{F})$ dans $(A' , \mathfrak{F}')$ est une application φ de A dans A' telle que, pour tout entier $n \geqslant 0$, toute opération fondamentale $f \in \mathfrak{F}_n$ et tout choix de $x_1 , x_2 , \dots , x_n$ dans A , on ait

$$\varphi[f(x_1 , x_2 , \dots , x_n)] = f'[\varphi(x_1) , \varphi(x_2) , \dots , \varphi(x_n)] , \qquad f' = \beta(f) .$$

Soit $\mathcal{O}_n$ l'ensemble de toutes les applications de A^n dans A. Si $f \in \mathfrak{F}_p$, on peut définir une application $\hat{f}$ de $(\mathcal{O}_n)^p$ dans $\mathcal{O}_n$ en posant

$$\psi = \hat{f}(\varphi_1 , \varphi_2 , \dots , \varphi_p)$$

si et seulement si ($\forall\, x_1 , x_2 , \dots , x_n \in A$)

$$\psi(x_1,x_2,\dots,x_n) = f[\varphi_1(x_1,\dots,x_n) , \varphi_2(x_1,\dots,x_n) , \dots , \varphi_p(x_1,\dots,x_n)] .$$

Chaque $\mathcal{O}_n$ apparaît ainsi comme le support d'une algèbre $(\mathcal{O}_n , \hat{\mathfrak{F}})$.

On appelle <u>opérations triviales à n variables</u> les $e_n^j \in \mathcal{O}_n$ ($j = 1 , 2 , \dots , n$) définies par ($\forall\, x_1 , \dots , x_n \in A$) $e_n^j(x_1 , x_2 , \dots , x_n) = x_j$. L'ensemble $\{e_n^1 , e_n^2 , \dots , e_n^n\}$ engendre dans $(\mathcal{O}_n , \hat{\mathfrak{F}})$ une sous-algèbre $(\mathcal{G}_n , \hat{\mathfrak{F}})$. L'égalité à peu près évidente $f = \hat{f}(e_n^1 , e_n^2 , \dots , e_n^n)$ (pour $f \in \mathfrak{F}_n$) montre, d'une part que $\mathfrak{F}_n \subseteq \mathcal{G}_n$, d'autre part qu'il existe une bijection entre $\mathfrak{F}$ et $\hat{\mathfrak{F}}$, dans laquelle se correspondent f et $\hat{f}$.

On dira que les éléments g de $\mathcal{G} = \bigcup_{n \geqslant 0} \mathcal{G}_n$ sont les <u>opérations composées</u> de l'algèbre $(A , \mathfrak{F})$. On vérifie sans difficulté que les algèbres $(A , \mathfrak{F})$ et $(A , \mathcal{G})$ ont non seulement même support, mais qu'elles ont les mêmes congruences, les mêmes supports de sous-algèbres, les mêmes homomorphismes.

On appelle <u>constantes algébriques</u> les résultats d'opérations constantes, ou, ce qui revient au même, les résultats d'opérations constantes à une variable. Les constantes algébriques constituent le support d'une sous-algèbre $(\Omega , \mathfrak{F})$ de $(A , \mathfrak{F})$ contenue dans toute autre sous-algèbre.

Nous écarterons de notre étude les algèbres $(A , \mathfrak{F})$ telles que tout élément $a \in A$ soit une constante algébrique.

Les opérations composées permettent de définir le support $\overline{S}$ de la sous-algèbre $(\overline{S} , \mathfrak{F})$ engendrée par S comme étant l'ensemble des $g(x_1 , \dots , x_n)$ où n décrit l'ensemble $\underset{\sim}{N}$ des entiers naturels, $g \in \mathcal{G}_n$, et $x_1 , \dots , x_n$ sont des éléments quelconques de S.

Lorsque $\overline{S} = A$, on dit que S est un <u>système générateur</u> de $(A , \mathfrak{F})$.

THÉORÈME 2.1 ([12]). - <u>Si l'algèbre $(A , \mathfrak{F})$ admet un système générateur minimal infini, deux systèmes générateurs minimaux ont le même cardinal</u>.

Démonstration. - Soient S , S' deux systèmes générateurs minimaux, S étant infini. Pour tout $a \in S'$, il existe une partie finie T_a de S , telle que $a \in \overline{T}_a$.

La réunion $\bigcup_{a \in S'} T_a$ est un système générateur de $(A , \mathfrak{F})$ contenu dans S , donc égal à S . Par suite, Card $S \leqslant$ Card S' , et S' est infini.

On a alors de même Card $S' \leqslant$ Card S , d'où l'égalité.

3. Indépendance.

Soit I une partie quelconque du support A d'une algèbre $(A , \mathfrak{F})$.

DÉFINITION 3.1. - On dit que I est un système libre (ou un système d'éléments indépendants) si toute application σ de I dans A peut être prolongée par un homomorphisme h de la sous-algèbre $(\overline{I} , \mathfrak{F})$ dans $(A , \mathfrak{F})$.

On peut démontrer l'équivalence (voir [12]) de cette définition et de la suivante :

DÉFINITION 3.2.

(a) Si I est fini : $I = \{a_1 , a_2 , \dots , a_n\}$, il est dit libre si, pour tout choix de f et g dans $\mathfrak{S}_n$, l'égalité $f(a_1 , a_2 , \dots , a_n) = g(a_1 , a_2 , \dots , a_n)$ entraîne $f = g$.

(b) Si I est infini, il est dit libre si toute partie finie de I est libre.

Remarques.

1. ϕ est un système libre, qui engendre la sous-algèbre $(\Omega , \mathfrak{F})$.

2. La famille des systèmes libres est $\cup$-inductive. Il existe donc des systèmes libres maximaux.

3. On montre facilement que l'homomorphisme h de la définition 3.1 est unique, pour une application σ donnée.

LEMME 3.3. - Si $I = I_1 \cup J$ $(I_1 \cap J = \phi)$ est un système libre, si h_1 est un homomorphisme de $(\overline{I}_1 , \mathfrak{F})$ dans $(A , \mathfrak{F})$ et si σ est une application de J dans A , il existe un homomorphisme de $(\overline{I} , \mathfrak{F})$ dans $(A , \mathfrak{F})$ qui prolonge à la fois h_1 et σ .

En effet, la restriction de h_1 à I_1 et σ définissent une application g de I dans A , et, puisque I est libre, cette application peut être prolongée par un homomorphisme h de $(\overline{I} , \mathfrak{F})$ dans $(A , \mathfrak{F})$.

THÉORÈME 3.4 (théorème de l'échange). - Soit $I = I_0 \cup J$ ($I_0 \cap J = \emptyset$) un système libre. Si I_1 est un système libre tel que $\bar{I}_1 = \bar{I}_0$, le système $I' = I_1 \cup J$ est aussi libre, et $\bar{I} = \bar{I}'$.

Remarquons tout d'abord que $I_1 \subseteq \bar{I}_0$, d'où $\overline{I_1 \cup J} \subseteq \overline{I_0 \cup J}$. L'inclusion opposée s'obtient de la même façon, d'où l'égalité $\bar{I} = \bar{I}'$.

Soit σ une application de $I_1 \cup J$ dans A . Il existe alors un homomorphisme h_1 de $(\bar{I}_1 , \mathfrak{F})$ dans $(A , \mathfrak{F})$ tel que h_1 et σ aient la même restriction à I_1 .

D'après le lemme 3.3, il existe alors un homomorphisme de $(\bar{I}' , \mathfrak{F}) = (\bar{I} , \mathfrak{F})$ qui prolonge à la fois les restrictions de h_1 à I_1 et de σ à J , donc qui prolonge σ .

THÉORÈME 3.5. - Si I et J sont deux systèmes libres de même cardinal, les sous-algèbres $(\bar{I} , \mathfrak{F})$ et $(\bar{J} , \mathfrak{F})$ sont isomorphes.

Si σ est une bijection de I sur J , on voit facilement que les homomorphismes

$$h : (\bar{I} , \mathfrak{F}) \longrightarrow (A , \mathfrak{F}) \qquad \text{et} \qquad h' : (\bar{J} , \mathfrak{F}) \longrightarrow (A , \mathfrak{F})$$

qui prolongent σ et σ^{-1} respectivement sont tels que $h(\bar{I}) = \bar{J}$ et $h'(\bar{J}) = \bar{I}$. Pour tout $x \in I$, $h'[h(x)] = x$, et cette égalité s'étend à tout $x \in \bar{I}$. De même $h[h'(y)] = y$ pour tout $y \in \bar{J}$, ce qui achève la démonstration.

THÉORÈME 3.6. - Si l'algèbre $(A , \mathfrak{F})$ est image homomorphe d'une de ses sous-algèbres $(B , \mathfrak{F})$, tout système libre dans $(B , \mathfrak{F})$ est libre dans $(A , \mathfrak{F})$.

Soient φ un homomorphisme surjectif $(B , \mathfrak{F}) \to (A , \mathfrak{F})$, I un système libre dans $(B , \mathfrak{F})$, σ une application de I dans A . Pour tout $x \in I$, choisissons un $x' \in B$ tel que $\varphi(x') = \sigma(x)$, et posons $\tau(x) = x'$. L'application τ de I dans B peut être prolongée par un homomorphisme ψ de $(\bar{I} , \mathfrak{F})$ dans $(B , \mathfrak{F})$. Il est clair que $\varphi \circ \psi$ est un homomorphisme de $(\bar{I} , \mathfrak{F})$ dans $(A , \mathfrak{F})$ qui prolonge σ .

4. Bases.

Soit B une partie non vide du support A du support A d'une algèbre $(A , \mathfrak{F})$.

DÉFINITION 4.1. - On dit que B est une base de cette algèbre si B est à la fois un système libre et un système générateur de $(A , \mathfrak{F})$.

La théorie des modules sur un anneau fournit des exemples d'algèbres ayant des bases et des exemples d'algèbres n'ayant pas de bases.

DÉFINITION 4.2. - Une algèbre $(A , \mathfrak{F})$ qui possède au moins une base est dite libre.

Remarques.

1. Toute base est un système générateur minimal. En effet, si B est une base, et si $b_0 \in B$, on ne peut avoir $b_0 \in \overline{B \setminus \{b_0\}}$, sinon il existerait un entier n , une opération composée $g \in \mathfrak{S}_n$, et n éléments b_i de $B \setminus \{b_0\}$ tels que $b_0 = g(b_1 , b_2 , \ldots , b_n)$, ce qui contredit l'indépendance des éléments de toute partie finie de B .

2. Toute base est un système libre maximal. En effet, si B est une base et si $a \in A \setminus B$, il existe un entier n , une opération composée $g \in \mathfrak{S}_n$, et n éléments b_i de B tels que $a = g(b_1 , b_2 , \ldots , b_n)$, et le système $B \cup \{a\}$ ne peut être libre.

3. Un système générateur minimal, un système libre maximal ne sont pas en général des bases. Dans le groupe additif $\underset{\sim}{Z}/(6)$, considéré comme un $\underset{\sim}{Z}$-module, il n'existe pas de système libre $\neq \emptyset$, et $\{\dot{2} , \dot{3}\}$ est un système générateur minimal. Dans le corps $\underset{\sim}{Q}$ des rationnels, considéré comme un $\underset{\sim}{Z}$-module, tout système réduit à un élément non nul est un système libre maximal et il n'existe pas de base.

THÉORÈME 4.3. - Si une algèbre libre $(A , \mathfrak{F})$ admet des bases B' , B'' de cardinaux différents, ces bases sont finies et les cardinaux des diverses bases de l'algèbre constituent une progression arithmétique.

Toute base de $(A , \mathfrak{F})$ est finie en vertu du théorème 2.1.

Supposons qu'il existe une base B' de n' éléments, une base B'' de n'' éléments, et soit $B_1 \cup B_2$ une base de $(n' + k)$ éléments,

$$(B_1 \cap B_2 = \emptyset , \quad \text{Card } B_1 = n' , \quad \text{Card } B_2 = k) .$$

Alors l'algèbre $(A , \mathfrak{F})$ est isomorphe à sa sous-algèbre $(\overline{B_1} , \mathfrak{F})$, d'après le théorème 3.5. $(\overline{B_1} , \mathfrak{F})$ a donc une base B_1^* de n'' éléments. Les éléments de B_1^* , indépendants dans $(\overline{B_1} , \mathfrak{F})$, le sont dans $(A , \mathfrak{F})$ (théorème 3.6) et, puisque $\overline{B_1} = \overline{B_1^*}$, on peut appliquer le théorème de l'échange (3.4) : $B_1^* \cup B_2$ est un système libre qui engendre la même sous-algèbre que $B_1 \cup B_2$, donc une base comportant $(n'' + k)$ éléments. De là on déduit facilement que la différence entre

deux éléments consécutifs de l'ensemble des cardinaux des différentes bases de l'algèbre est constante, ce qui achève la démonstration.

On trouvera une autre démonstration de ce théorème dans [7], la précédente étant empruntée à [12].

On peut se demander si les progressions arithmétiques ainsi obtenues sont quelconques. La réponse est affirmative : pour tout couple d'entiers naturels donnés (a , b) , on peut définir une algèbre $(A , \mathfrak{F})$ admettant pour tout entier naturel n une base de cardinal $a + bn$ ([7], [17]).

5. Une classe remarquable d'algèbres : les v*-algèbres.

On a vu que si I est un système libre d'une algèbre $(A , \mathfrak{F})$, la condition (C) suivante est vérifiée :

(C) $$(\forall\, a \in I) \qquad a \notin \overline{I \setminus \{a\}} \ .$$

Cette condition (C) ne caractérise nullement les systèmes libres, comme on le voit en considérant le $\mathbb{Z}$-module $\mathbb{Z}/(6)$ et le système $\{\dot{2} , \dot{3}\}$.

DÉFINITION 5.1 ([15]). - On appelle v**-algèbre toute algèbre dans laquelle la condition (C) caractérise les systèmes libres.

Une v**-algèbre n'est pas nécessairement libre, mais pour toute v**-algèbre libre, deux bases quelconques ont même cardinal.

DÉFINITION 5.2 ([13]). - On appelle v*-algèbre toute algèbre dans laquelle :

(α) Si $a \notin \Omega$, le système $\{a\}$ est libre.

(β) Si $S = \{a_1 , a_2 , \dots , a_n\}$ est libre et si $S \cup \{a_{n+1}\}$ ne l'est pas, on a $a_{n+1} \in \overline{S}$.

Il est facile de voir que toute v*-algèbre est une v**-algèbre.

On démontre ([13]) que dans une v*-algèbre, il y a équivalence entre :

(α) B est une base,

(β) B est un système générateur minimal,

(γ) B est un système libre maximal.

On en déduit que toute v*-algèbre est libre et que deux bases quelconques ont même cardinal, ce qui permet de définir la dimension.

L'analogie constatée entre cette théorie et celle des espaces vectoriels est en partie expliquée par le théorème suivant, dans lequel $\mathfrak{S}_{3,1}$ représente l'ensemble des $g \in \mathfrak{S}_3$ qui ne dépendent effectivement que d'une variable au plus.

THÉORÈME 5.3 ([19]). - Soit $(A , \mathfrak{F})$ une v*-algèbre de dimension $\geqslant 3$.

(α) Si $\mathfrak{S}_0 \neq \emptyset$ et si $\mathfrak{S}_3 \neq \mathfrak{S}_{3,1}$, il existe un corps K tel que A soit un K-espace vectoriel et un K-sous-espace A_0 de A , tels que $\mathfrak{S}$ soit l'ensemble des opérations g définies par

$$g(x_1 , x_2 , \dots , x_n) = \sum_{j=1}^{n} \lambda_j x_j + a \qquad (a \in A_0 , \ \lambda_j \in K) .$$

(β) Si $\mathfrak{S}_0 = \emptyset$ et $\mathfrak{S}_3 \neq \mathfrak{S}_{3,1}$, même énoncé en ajoutant la condition

$$\sum_{j=1}^{n} \lambda_j x_j = 1_K \quad \text{(élément-unité de K)} .$$

(γ) Si $\mathfrak{S}_3 = \mathfrak{S}_{3,1}$, il existe un groupe Γ de bijections de A sur lui-même et un sous-ensemble A_0 de A , stable par Γ et contenant les points fixes des bijections non identiques $\gamma \in \Gamma$, tels que $\mathfrak{S}$ soit l'ensemble des opérations g définies par

$$g(x_1 , x_2 , \dots , x_n) = \gamma(x_j) \qquad (\gamma \in \Gamma) ,$$

ou

$$g(x_1 , x_2 , \dots , x_n) = a \qquad (a \in A_0) .$$

On trouvera dans [20] et [21] la description complète des v*-algèbres de dimension 2 et 1 .

BIBLIOGRAPHIE

[1] BIRKHOFF (Garrett). - Universal algebra, Proceedings of the first Canadian mathematical Congress [1945, Montreal], p. 310-326. - Toronto, The University of Toronto Press, 1946.

[2] BOURBAKI (Nicolas). - Algèbre, chapitre 2 : Algèbre linéaire, 3e édition. - Paris, Hermann, 1962 (Act. scient. et ind., 1236 ; Bourbaki, 6).

[3] BOURBAKI (Nicolas). - Algèbre, chapitre 8 : Modules et anneaux semi-simples. - Paris, Hermann, 1958 (Act. scient. et ind., 1261 ; Bourbaki, 23).

[4] DUBREIL (Paul). - Lectures on the algebraic theory of semigroups. - New Orleans, Tulane University, 1962.

[5] DUBREIL (Paul). - Cours de la Faculté des Sciences de Paris, 1964/65 (non publié).

[6] DUBREIL (Paul). - Endomorphismes, Séminaire Dubreil-Pisot : Algèbre et Théorie des Nombres, t. 18, 1964/65, n° 23, 20 p.

[7] GOETZ (A.) et RYLL-NARDZEWSKI (C.). - On bases of abstract algebras, Bull. Acad. pol. Sc., Série math., astr. et phys., t. 8, 1960, p. 157-161.