ALGÈBRE DES POLYNOMES

Autor(en): **Zamansky, Marc**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **2 (1956)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **19.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-32901

ALGÈBRE DES POLYNOMES

PAR

Marc ZAMANSKY, Paris

INTRODUCTION

L'objet de cet article est de présenter les propriétés algébriques fondamentales des êtres qu'on appelle polynômes à une indéterminée ou improprement, polynômes à une variable.

On n'y trouvera que des résultats élémentaires bien connus (sauf peut-être celui qui concerne le lien entre les deux divisions) mais tout ce qui pourrait rappeler l'analyse a été banni de la présentation car la confusion de notations entraîne souvent chez les jeunes étudiants la confusion des concepts et des propriétés.

PREMIÈRES DÉFINITIONS. NOTATIONS.

Définition d'un polynôme

On appelle polynôme un ensemble ordonné d'une infinité dénombrable de nombres (réels ou complexes) tous nuls à partir d'un certain rang.

Nous représenterons au début un polynôme par $(a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$. Les nombres a_k sont appelés *coefficients* et dans cette écriture l'entier k repère le rang d'ordre du coefficient (a_k est le $(k+1)^{\underline{e}}$ coefficient).

Nous désignons aussi un polynôme par une seule lettre et écrirons:

$$A = (a_0, a_1, \ldots, a_n, 0, 0, \ldots) .$$

Egalité de deux polynômes

Deux polynômes $A = (a_0, a_1, ..., a_n, 0, 0, ...)$ et $B = (b_0, b_1, ..., b_m, 0, ...)$ seront dits égaux si quel que soit k: $a_k = b_k$, $(k \geqslant 0)$. Cette définition entraîne qu'à partir du même rang a_k et b_k sont nuls.

On écrira $A = B$, le symbole $=$ pouvant alors être employé de nouveau.

Lois algébriques sur l'ensemble des polynomes

Lois internes

Les conventions suivantes construisent des polynômes à partir de polynômes; elles définissent ce qu'on appelle des *lois internes*. Ce seront l'*addition* et la *multiplication*. Leur définition entraîne des propriétés qui feront de l'ensemble des polynômes muni de ces deux lois, un *anneau commutatif unitaire*.

1° *Addition.*

Soit $A = (a_0, a_1, ...)$, $B = (b_0, b_1, ...)$, deux polynômes. Par définition le polynôme $(a_0 + b_0, a_1 + b_1, ..., a_k + b_k, ...)$ est appelé *somme* de A et B et on écrit:

$$A + B = (a_0 + b_0, a_1 + b_1, ..., a_k + b_k, ...) .$$

Les propriétés des nombres complexes montrent que cette addition est *associative*, c'est-à-dire que $(A + B) + C = A + (B + C)$ et *commutative*, c'est-à-dire que $A + B = B + A$, quels que soient A, B, C.

Désignons par Θ le polynôme dont tous les coefficients sont nuls: $a_k = 0$ pour $k = 0, 1, 2, ...$ On a alors quel que soit le polynôme A:

$$A + \Theta = \Theta + A = A$$

Θ est donc l'*élément neutre* pour l'addition.

Désignons par $(- A)$ le polynôme $(- a_0, - a_1, ..., - a_k, ...)$. On a alors: $A + (- A) = \Theta$. Donc tout polynôme A a un *symétrique* $(- A)$ pour l'addition.

Ces propriétés de l'addition signifient que l'ensemble des polynômes muni de l'addition est un *groupe commutatif* ou *groupe abélien.*

2° *Multiplication.*

Soit A = $(a_0, a_1, ...)$, B = $(b_0, b_1, ...)$ deux polynômes. Par définition le polynôme $(a_0 b_0, a_0 b_1 + a_1 b_0, ..., a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + ... + a_k b_0, ...)$ est appelé produit de A par B et on écrit:

$$AB = (a_0 b_0, a_0 b_1 + a_1 b_0, ...) .$$

Cette multiplication est évidemment *associative* et *commutative*, c'est-à-dire que quels que soient A, B, C: (AB) C = A (BC) et AB = BA.

Désignons par I le polynôme dont tous les coefficients sont nuls sauf le premier a_0 qui vaut 1:I = (1, 0, 0, ...). On a quel que soit A:

$$IA = AI .$$

I est donc l'*élément neutre* pour la multiplication.

En général A n'a pas de symétrique pour la multiplication. Car s'il existe B, tel que AB = I, on doit avoir $a_0 b_0 = 1$ ce qui exige $a_0 \neq 0$, $b_0 \neq 0$.

3° *Propriété de la multiplication par rapport à l'addition.*

De la distributivité de la multiplication par rapport à l'addition dans le corps des nombres complexes résulte que quels que soient les polynômes A, B, C:

$$A (B + C) = (B + C) A = AB + AC .$$

La multiplication des polynômes est donc *distributive* (doublement) par rapport à l'addition.

4° *L'anneau des polynômes.*

Les propriétés de l'addition jointes à l'associativité et la distributivité (par rapport à l'addition) de la multiplication font de l'ensemble des polynômes un *anneau.*

Si on y ajoute la *commutativité* de la multiplication, cet ensemble prend le nom d'*anneau commutatif.*

Si on y ajoute encore l'existence de l'élément neutre I, cet ensemble prend le nom d'*anneau commutatif unitaire.*

II. *Loi externe*

On peut définir une opération qui construira un polynôme à partir de deux êtres qui seront l'un un polynôme, l'autre un nombre du corps des complexes. A tout polynôme A et tout nombre α, on fait correspondre le polynôme $(\alpha a_0, \alpha a_1, \ldots, \alpha a_k, \ldots)$ qu'on désigne par α A et qu'on appelle *produit de A par* α.

Les propriétés suivantes, vraies quels que soient les polynômes A, B, C et les nombres α, β, ... découlent immédiatement des définitions et propriétés qui précèdent:

1) $\alpha(A + B) = \alpha A + \alpha B$
2) $\alpha(\beta A) = (\alpha\beta) A$
3) $1 . A = A$
4) $(\alpha + \beta) A = \alpha A + \beta A$
5) $\alpha(AB) = (\alpha A) B = A(\alpha B)$.

De ces propriétés, résulte que quel que soit A, $OA = \Theta$. Désormais nous remplaçons Θ par O. D'autre part comme $1.A = A$ et $I.A = A$, nous remplacerons I par 1 et de façon générale, le polynôme $(a_0, 0, 0, \ldots)$ pouvant être considéré comme le produit de $(1, 0, 0, \ldots)$ par a_0 nous identifions le polynôme $(a_0, 0, 0, \ldots)$ où $a_k = 0$ si $k \geqslant 1$ et le nombre a_0. Un tel polynôme s'appelle parfois une constante.

Enfin $(-A)$, symétrique de A pour l'addition, est aussi le polynôme $(-1) A$ obtenu en multipliant A par (-1). Nous ne les distinguerons donc pas.

III. *Espace vectoriel*

Si on considère l'ensemble des polynômes muni de l'addition et de la précédente loi externe, les propriétés de l'addition et les quatre premières propriétés de la loi externe font de cet ensemble un *espace vectoriel sur le corps des nombres complexes.* Mais comme on le verra ci-dessous cet espace n'est pas de dimension finie.

Base de l'espace vectoriel des polynomes

Les propriétés de l'espace vectoriel des polynômes permettent d'écrire tout polynôme A sous la forme:

$$A = a_0 (1, 0, 0, ...) + a_1 (0, 1, 0, ...) + ... + a_n (0, 0, ..., 1, 0, ...)$$

c'est-à-dire, en désignant par e_k le polynôme dont tous les coefficients sont nuls sauf celui de rang $k + 1$ qui vaut 1,

$$A = a_0 e_0 + a_1 e_1 + ... + a_n e_n .$$

L'ensemble des polynômes e_k *s'appelle base* et l'écriture précédente réalise ce qu'on appelle la *décomposition de A sur la base.* $a_p e_p$ s'appelle terme de degré p.

La définition de l'égalité de deux polynômes entraîne que cette décomposition est *unique.*

Appliquons la définition du produit de deux polynômes à deux polynômes e_p, e_q. On a $e_p = (\alpha_0, \alpha_1, ..., \alpha_p, \alpha_{p+1}, ...)$ où $\alpha_k = 0$ si $k \neq p$ et $\alpha_p = 1$; $e_q = (\beta_0, \beta_1, ..., \beta_q, \beta_{q+1}, ...)$ où $\beta_k = 0$ si $k \neq q$ et $\beta_q = 1$.

Le $(k + 1)^{\underline{e}}$ coefficient de $e_p e_q$ est $\alpha_k \beta_0 + \alpha_{k-1} \beta_1 + ... + \alpha_0 \beta_k$. Ce coefficient ne peut être différent de zéro que s'il contient $\alpha_p \beta_p$. Or le $(k + 1)^{\underline{e}}$ coefficient de $e_p e_q$ est une somme de termes tels que la somme des indices de chaque terme $\alpha_{k-m} \beta_m$ est k; on ne trouvera donc $\alpha_p \beta_p$ que dans le $(p + q + 1)^{\underline{e}}$ coefficient ce qui entraîne que seul le $(p + q + 1)^{\underline{e}}$ coefficient de $e_p e_q$ n'est pas nul. Ce dernier coefficient est par définition:

$$\alpha_{p+q} \beta_0 + \alpha_{p+q-1} \beta_1 + ... + \alpha_p \beta_q + ... + \alpha_0 \beta_{p+q} = \alpha_p \beta_q = 1 .$$

Donc:

$$e_p e_q = e_q e_p = e_{p+q} .$$

Les propriétés suivantes:

$$\begin{aligned}
&\alpha (A + B) = \alpha A + \alpha B \\
&(\alpha + \beta) A = \alpha A + \beta A \\
&\alpha (\beta A) = \alpha\beta A \\
&A (B + C) = AB + AC \\
&e_p e_q = e_{p+q} .
\end{aligned}$$

permettent alors de calculer plus aisément que ne l'indiquaient les définitions, la somme et le produit de polynômes.

Ainsi:

$$\begin{aligned} \mathrm{AB} &= (a_0 e_0 + a_1 e_1 + a_2 e_2)(b_0 e_0 + b_1 e_1) \\ &= a_0 b_0 e_0 + (a_0 b_1 + a_1 b_0) e_1 + (a_1 b_1 + a_2 b_0) e_2 . \end{aligned}$$

On retrouve les règles de calcul élémentaires.

Enfin la règle de calcul $e_p e_q = e_{p+q}$ pour le produit de deux polynômes de la base permet de montrer facilement que si A et B sont deux polynômes tels que $\mathrm{AB} = 0$, l'un au moins des polynômes est nul. Supposons en effet que ni A, ni B ne sont nuls; alors soit parmi les termes $a_k e_k$ de A celui d'indice le plus élevé $a_p e_p$ tel que $a_p \neq 0$ et de même $b_q e_q$ dans B. Dans AB figure $a_p b_q e_{p+q}$ et comme $a_p \neq 0$, $b_q \neq 0$, $\mathrm{AB} \neq 0$.

Ainsi $\mathrm{AB} = 0$ entraîne $\mathrm{A} = 0$ ou $\mathrm{B} = 0$. Il en résulte que si $\mathrm{A} \neq 0$ et si $\mathrm{AB} = 0$, alors $\mathrm{B} = 0$. Il en résulte encore que si $\mathrm{A} \neq 0$ et si $\mathrm{AB} = \mathrm{AC}$, on a $\mathrm{A}(\mathrm{B} - \mathrm{C}) = 0$, donc $\mathrm{B} - \mathrm{C} = 0$, donc $\mathrm{B} = \mathrm{C}$. En d'autres termes cela signifie que *tout polynôme différent de* 0 *est régulier pour la multiplication.*

Degré, valuation d'un polynome

Définition. — Soit $\mathrm{A} = (a_0, a_1, \ldots, a_n, 0, \ldots)$ un polynôme. Nous appellerons *degré de A* et nous le désignerons par *degA*, le plus grand entier $n \geqslant 0$ tel que $a_n \neq 0$:

$$n = \deg \mathrm{A}$$

Cela signifie que si $k \leqslant n$, il y a au moins un $a_k \neq 0$ et que $a_k = 0$ quel que soit $k > n$.

$\deg \mathrm{A} = 0$ signifie que A est une constante, mais ne signifie pas nécessairement que $\mathrm{A} = 0$.

Le degré de 0 n'est pas défini.

Le degré et les deux lois algébriques.

D'après la définition du degré, on a les propriétés suivantes:

1° Si $\deg \mathrm{A} > \deg \mathrm{B}$, alors $\deg(\mathrm{A} + \mathrm{B}) = \deg \mathrm{A}$
Si $\deg \mathrm{A} = \deg \mathrm{B} = n$ et si $a_n + b_n \neq 0$, alors $\deg(\mathrm{A} + \mathrm{B}) = \deg \mathrm{A} = \deg \mathrm{B}$.

Dans le cas général:

$\deg(A + B) \leqslant \max(\deg A, \deg B)$, c'est-à-dire est inférieur ou égal au plus grand des entiers deg A, deg B.

2° Si $AB \neq 0$, $\deg AB = \deg A + \deg B$.

Définition. — Soit $A = (a_0, ..., a_n, 0, ...)$ un polynôme. Nous appellerons *valuation de A* et nous la désignerons par $\varphi(A)$, le plus petit entier $m \geqslant 0$ tel que $a_m \neq 0$.

Cela entraîne que si $m \geqslant 1$ on a $a_k = 0$ pour $0 \leqslant k \leqslant m-1$. La valuation de 0 n'est pas définie.

On remarquera que quel que soit A: $\varphi(A) \leqslant \deg A$.

La valuation et les deux lois algébriques.

D'après la définition, on a les propriétés suivantes:

1° Si $\varphi(A) > \varphi(B)$, alors $\varphi(A + B) = \varphi(B)$.
Si $\varphi(A) = \varphi(B) = m$ *et* si $a_m + b_m \neq 0$,
alors $\varphi(A + B) = \varphi(A) = \varphi(B)$.

Dans le cas général: $\varphi(A + B) \geqslant \min(\varphi(A), \varphi(B))$, c'est-à-dire supérieure ou égale au plus petit des entiers $\varphi(A)$, $\varphi(B)$.

2° Si $AB \neq 0$, alors $\varphi(AB) = \varphi(A) + \varphi(B)$.

Remarque. — Une condition *nécessaire* (seulement) pour que $A = B$ est que $\deg A = \deg B$ *et* $\varphi(A) = \varphi(B)$. La négation de cette proposition signifie que si l'une des conditions $\deg A = \deg B$ ou $\varphi(A) = \varphi(B)$ n'est pas réalisée, alors $A \neq B$.

Le problème de la division des polynomes

L'ensemble $\mathfrak{P}$ des polynômes est un anneau commutatif unitaire, mais n'est pas un corps, c'est-à-dire que la division n'est pas en général possible, c'est-à-dire encore, que deux polynômes A et B étant donnés il n'existe pas en général de polynômes X tel que $A = BX$.

Définition. — On dit que A est divisible par $B \neq 0$, s'il existe Q tel que $A = BQ$. On dit aussi que A est multiple de B ou que B divise A ou est diviseur de A. Alors A est aussi multiple de Q.

Si Q existe, il est unique car s'il existait encore Q′ tel que $A = BQ'$ on aurait $BQ = BQ'$ et comme $B \neq 0$, $Q = Q'$.

On peut alors présenter cette définition de la façon suivante:

Soit A et B $\neq 0$ deux polynômes; considérons tous les polynômes $A - BX$ où X parcourt $\mathfrak{P}$ (c'est-à-dire où X est un polynôme quelconque); dire que A est divisible par B c'est dire qu'il existe $Q \in \mathfrak{P}$ tel que $A - BQ = 0$; Q est alors unique.

Lorsque A n'est pas divisible par B, il est alors naturel d'étudier les polynômes $A - BX$ où X parcourt $\mathfrak{P}$ et de tenter de trouver X de façon que $A - BX$ possède quelque propriété vraie lorsque $A = BQ$. Or si $A = BQ$, *nécessairement* $\deg A = \deg BQ$ et $\nu(A) = \nu(BQ)$; si $A \neq 0$ ($A = 0$ n'offre pas d'intérêt) on *doit* avoir $\deg A = \deg B + \deg Q$ et $\nu(A) = \nu(B) + \nu(Q)$.

On peut être tenté de chercher pour deux polynômes A et B, un polynôme X tel que simultanément $\deg A = \deg B + \deg X$ *et* $\nu(A) = \nu(B) + \nu(X)$. Il est facile de voir par un exemple que c'est en général impossible.

On peut alors chercher à sauvegarder l'une des deux propriétés précédentes pour *tout* couple A, B; en d'autres termes la propriété cherchée doit être vraie *quels que soient* les polynômes A et B. Mais si alors on cherche X en lui imposant la seule condition $\deg A = \deg B + \deg X$, on peut satisfaire à cette condition d'une infinité de manières; nous sommes donc amenés à chercher parmi tous les X possibles, ceux qui possèdent une autre propriété. Cette discussion motive le point de vue qui suit.

Considérons une famille quelconque de polynômes non nuls. Comme les degrés sont des entiers $\geqslant 0$, il existe dans cette famille, au moins un polynôme dont le degré est inférieur ou égal à tous les degrés des polynômes de cette famille. Considérons alors la famille de tous les polynômes $A - BX$ où $X \in \mathfrak{P}$. Si à cette famille on applique la remarque qui vient d'être faite on en conclut qu'il existe au moins un polynôme Q tel que $\deg(A - BQ) \leqslant \deg(A - BX)$ quel que soit $X \in \mathfrak{P}$. Nous verrons alors que nécessairement $\deg(A - BQ) < \deg B$ et que pour tout couple A, B, le polynôme Q tel que $\deg(A - BQ) < \deg B$ est unique. Ce sera *la division euclidienne de* A *par* B *ou division suivant les puissances décroissantes.*

L'idée de la division suivant les puissances croissantes sera

déduite de la précédente division, puis nous montrerons que les deux divisions peuvent être ramenées l'une à l'autre.

La division euclidienne

Soit A et B deux polynômes. Soit $B \neq 0$. Si $A = 0$, on a $A = BO$ donc A est divisible par B. Supposons $A \neq 0$ et parmi tous les polynômes $A - BX$ soit $A - BQ$ tel que $\deg (A - BQ) \leqslant \deg (A - BX)$ quel que soit X, lorsque A n'est pas divisible par B.

Montrons que 1°: $\deg (A - BQ) < \deg B$; 2° Q est unique.

1° Soit en effet:

$$B = b_0 e_0 + \ldots + b_p e_p \; (b_p \neq 0)$$
$$A - BQ = c_0 e_0 + \ldots + c_p e_p + \ldots + c_m e_m$$

et supposons $m > p$ et $c_m \neq 0$, m étant le plus petit degré possible de tous les polynômes $A - BX$.

On a alors:

$$e_{m-p} B = b_0 e_{m-p} + \ldots + b_p e_m$$
$$\frac{c_m}{b_p} e_{m-p} B = \frac{b_0 c_m}{b_p} e_{m-p} + \ldots + \frac{c_m}{b_p} b_{p-1} e_{m-1} + c_m e_m .$$

D'où

$$A - BQ - \frac{c_m}{b_p} e_{m-p} B = A - B \left(Q + \frac{c_m}{b_p} e_{m-p} \right) =$$
$$= c_0 e_0 + \ldots + \left(c_{m-1} - \frac{c_m}{b_p} b_{p-1} \right) e_{m-1} .$$

Q′ désignant le polynôme $Q + \frac{c_m}{b_p} e_{m-p}$, $A - BQ'$ serait de degré $< m$ ce qui est en contradiction avec l'hypothèse faite sur m. L'hypothèse $m \geqslant p$ est donc incompatible avec "m est le plus petit degré possible de tous les $A - BX$". On a donc $m < p$, c'est-à-dire $\deg (A - BQ) < \deg B$.

2° Si existait $Q' \neq Q$ tel que $\deg (A - BQ') \leqslant \deg (A - BX)$ quel que soit X, on aurait $\deg (A - BQ') < \deg B$ d'après ce qui précède. Donc

$$\deg (A - BQ - (A - BQ')) = \deg B \, (Q' - Q) < \deg B .$$

Or si on suppose $Q' \neq Q$, on a $\deg (Q' - Q) \geqslant 0$, donc $\deg B (Q' - Q) \geqslant \deg B$ ce qui contredit $\deg B (Q' - Q) < \deg B$. Nécessairement $Q' = Q$.

D'où:

THÉORÈME. — *Etant donnés deux polynômes* A *et* B, $B \neq 0$ *il existe un polynôme* Q *et un seul tel que* $A - BQ = 0$ *ou bien tel que* $\deg (A - BQ) \leqslant \deg (A - BX)$ *quel que soit le polynôme* X *; de plus dans le second cas* $\deg (A - BQ) < \deg B$.

Ce résultat peut alors être écrit:

$$A = BQ + R , \qquad \deg R < \deg B$$

où le couple Q, R est unique. Q est le *quotient*, R *le reste.*

On notera que la première partie de la démonstration fournit la méthode pratique bien connue.

LA DIVISION SUIVANT LES PUISSANCES CROISSANTES

Soit $A = a_0 e_0 + \ldots + a_n e_n$ un polynôme non nul, de degré n ($a_n \neq 0$). Appelons polynôme *transposé* de A le polynôme $\overline{A} = a_n e_0 + a_{n-1} e_1 + \ldots + a_0 e_n$. Quel que soit $A \neq 0$, $\nu (\overline{A}) = 0$ et $\deg \overline{A} = \deg A - \nu (A)$; on a donc $\deg \overline{A} \leqslant \deg A$.

Cherchons les propriétés de l'opération qui à A associe $\overline{A}$ relativement au produit de A par une croissante α, à la somme $A + B$, au produit AB.

1° Si $\alpha \neq 0$, on a $\overline{(\alpha A)} = \alpha \overline{A}$.

2° Soit $A = a_0 e_0 + \ldots + a_n e_n$ ($a_n \neq 0$) et $B = b_0 e_0 + \ldots + b_p e_p$ ($b_p \neq 0$) et supposons par exemple $\deg A = n \geqslant \deg B = p$.

Remarquons que quel que soit h, $\overline{(e_h A)} = \overline{A} e_0$

a) Si $\deg A = n > p = \deg B$, on a:

$$\overline{(A + B)} = \overline{A} + e_{n-p} \overline{B}$$

b) Si $\deg A = n = p = \deg B$ et si $\deg (A + B) = \deg A$ (c'est-à-dire si $a_n + b_n \neq 0$), on a:

$$\overline{A + B} = \overline{A} + \overline{B}$$

c) Si $\deg A = \deg B$ et si $\deg (A + B) < \deg A$ (c'est-à-dire si $a_n + b_n \neq 0$), soit alors $m = \deg (A + B) < n$.

On a:

$$\overline{A + B} = (a_m + b_m)\, e_0 + \ldots + (a_0 + b_0)\, e_m$$

$$\overline{A} + \overline{B} = (a_m + b_m)\, e_{n-m} + \ldots + (a_0 + b_0)\, e_n = e_{n-m}\, \overline{(A + B)} .$$

Donc $\overline{A} + \overline{B} = e_{n-m}\, (\overline{A + B})$.

3° Soit $a_n \neq 0$, $b_p \neq 0$.

$$AB = A\, b_p\, e_p + A\, b_{p-1}\, e_{p-1} + \ldots + A b_0\, e_0 .$$

En appliquant le résultat du 2° *a*) précédent on a:

$$\overline{AB} = \overline{A}\, b_0\, e_0 + e_{n+p-(n+p-1)}\, \overline{(A\, b_{p-1}\, e_{p-1} + \ldots)} =$$

$$= \overline{A}\, b_p\, e_0 + e_1\, \overline{A}\, b_{p-1} + \ldots .$$

D'où $\overline{AB} = \overline{A}\, \overline{B}$.

Ces règles étant établies, soient A et B non nuls et supposons deg A $\geqslant$ deg B. Soient Q et R les quotient et reste de la division euclidienne de A par B:

$$A = BQ + R , \qquad \deg R < \deg B .$$

Soit $n = \deg A$, $p = \deg B$, $r = \deg R < p$
On a alors:

$$\overline{A} = \overline{B}\, \overline{Q} + e_{n-r}\, \overline{R} = \overline{B}\, \overline{Q} + e_{\deg A - \deg (A - BQ)}\, \overline{R} .$$

Comme $\deg Q = n - p$, $\deg \overline{Q} < n - p$ et comme $r < p$, $n - p < \nu\,(e_{n-r}\, \overline{R}) = \nu\,(\overline{A} - \overline{B}\, \overline{Q})$.

Ainsi aux polynômes $\overline{A}$, $\overline{B}$, transposés de A et B est associé un polynôme $\overline{Q}$ tel que $\deg \overline{Q} < \nu\,(\overline{A} - \overline{B}\, \overline{Q})$. [On notera que $\nu\,(\overline{A}) = \nu\,(\overline{B}) = 0$].

Donc dans certains cas (jusqu'à présent), à deux polynômes A, B on peut associer un polynôme Q tel que $\deg Q < \nu\,(A - BQ)$.

C'est l'origine du théorème suivant:

THÉORÈME. — *Etant donnés deux polynômes* A, B *tels que* $\nu(B) = 0$ et un entier $k \geqslant 0$, *il existe un polynôme* Q *et un seul tel que*

$$\deg Q \leqslant k < \nu\ (A - DQ)$$

à moins que $A - BQ = 0$.

Existence. — Considérons tous les polynômes X tels que $\deg X \leqslant k$. Tous les polynômes $A - BX$ ont une valuation bornée car

$$\nu (A - BX) \leqslant \deg (A - BX) < \max (\deg A, k + \deg B) .$$

Il existe donc au moins un polynôme Q ($\deg Q \leqslant k$) pour lequel $\nu (A - BX) \leqslant \nu(A - BQ)$ quel que soit X. Je dis que pour ce polynôme Q, on a $\nu (A - BQ) > k$. En effet supposons que Q donne à $A - BQ$ la plus grande valuation possible et que cette valuation soit $m \leqslant k$.

On aurait alors

$$A - BQ = c_m e_m + \ldots + c_k e_k + \ldots + c_N e_N$$

$$B = b_0 e_0 + \ldots + b_p e_p$$

$$A - BQ - \frac{c_m}{b_0} e_m B = \lambda e_{m+1} + \ldots .$$

Donc $A - B \left(Q + \frac{c_m}{b_0} e_m\right)$ aurait une valuation $> m$ et $Q + \frac{c_m}{b_0} e_m$ serait de degré $\leqslant k$, ce qui contredit l'hypothèse faite sur Q.

Unicité. — Si existait $Q' \neq Q$ tel que $\deg Q' \leqslant k$ et $k < \nu (A - BQ')$ on aurait:

$$k < \nu (A - BQ - A + BQ') = \nu (B (Q' - Q)) = \nu (B) + \nu (Q' - Q) =$$

$$\nu (Q' - Q) \leqslant \deg (Q' - Q) \leqslant k$$

ce qui est impossible.

Ainsi à tout couple de polynôme A, B ($\nu (B) = 0$) et un entier $k \geqslant 0$ correspond un couple unique de polynômes Q, R tels que

$$A = BQ + e_{k+1} R \qquad \text{et} \qquad \deg Q \leqslant k .$$

Cette opération s'appelle division suivant les *puissances croissantes à l'ordre* k.

Relations entre les deux divisions

Nous avons introduit la seconde division en écrivant l'égalité déduite de $A = BQ + R$, $\deg R < \deg B$, pour les polynômes transposés:

$$\overline{A} = \overline{B}\,\overline{Q} + e_{n-r}\,\overline{R}$$

où $n = \deg A$, $r = \deg R$.

Il est évident que dans ce cas les coefficients de $\overline{Q}$ et $\overline{R}$ dans la division suivant les puissances croissantes sont les mêmes que ceux de Q et R, écrits dans l'ordre inverse.

Nous montrerons maintenant qu'on obtient la même propriété en partant de la division suivant les puissances croissantes.

Soit $A = BQ + e_{k+1}\,R$ avec $v(B) = 0$, $\deg Q \leqslant k$.

Posons $\deg A = n$, $\deg B = p$, $\deg Q = q \leqslant k$. Comme $v(B) = O$, on a: $\deg \overline{B} = \deg B = p$. Ecrivons $\overline{R} = \overline{A - BQ}$ et distinguons les quatre cas possibles suivants:

1er cas. Si $\deg A > \deg BQ$, on a: $\overline{A} - e_{n-p-q}\,\overline{B}\,\overline{Q} = \overline{R}$.

2e cas. Si $\deg A = \deg BQ$ et $\deg (A - BQ) = \deg A$, on a: $\overline{A} - \overline{B}\,\overline{Q} = \overline{R}$.

3e cas. Si $\deg A = \deg BQ$ et si $m = \deg (A - BQ) < \deg A$, on a $\overline{A} - \overline{B}\,\overline{Q} = e_{n-m}\,\overline{R}$.

4e cas. Si $\deg A < \deg BQ$, on a: $e_{p+q-n}\,\overline{A} - \overline{B}\,\overline{Q} = \overline{R}$.

Je dis que dans tous ces cas on a l'égalité d'une division euclidienne.

Remarquons qu'on a toujours $\deg \overline{R} \leqslant \deg R = \deg (A - BQ) - k - 1 < \deg (A - BQ) - q$.

Examinons les quatre cas:

1er *cas.* — On a $\deg \overline{R} < \deg (A - BQ) - q = n - q = \deg (e_{n-p-q}\,\overline{B})$ puisque $\deg \overline{B} = p$.

Donc $\overline{Q}$ et $\overline{R}$ sont les quotient et reste de la division euclidienne de $\overline{A}$ par $e_{n-p-q}\,\overline{B}$.

2e *cas.* — On a $\deg \overline{R} < p + q - q = p = \deg \overline{B}$.

Donc $\overline{Q}$ et $\overline{R}$ sont les quotient et reste de la division euclidienne de $\overline{A}$ par $\overline{B}$.

3e *cas.* — On a $\deg \overline{R} < m - q$, donc $\deg (e_{n-m}\, \overline{R}) < n - m + m - q = n - q = \deg B = \deg \overline{B}$.

Donc $\overline{Q}$ et $e_{n-m}\, \overline{R}$ sont les quotient et reste de la division euclidienne de $\overline{A}$ par $\overline{B}$.

4e *cas.* — On a $\deg \overline{R} < p + q - q = p = \deg \overline{B}$. Donc $\overline{Q}$ et $\overline{R}$ sont les quotient et reste de la division euclidienne de $e_{p+q-n}\, \overline{A}$ par $\overline{B}$.

Conclusion

Dans tous les cas on peut obtenir les coefficients des quotient Q et reste R de la division de A par B suivant les puissances croissantes à un ordre k, en effectuant la division euclidienne des transposés $\overline{A}$, $\overline{B}$ de A, B multipliés éventuellement par un e_h et en prenant les coefficients des transposés des quotient et reste de cette division euclidienne.