Séminaire Dubreil.
Algèbre et théorie
des nombres

Ellis R. Kolchin

Le théorème de la base finie pour les polynômes différentiels

Séminaire Dubreil. Algèbre et théorie des nombres, tome 14, n° 1 (1960-1961), exp. n° 7, p. 1-15

<http://www.numdam.org/item?id=SD_1960-1961__14_1_A7_0>

Séminaire DUBREIL-PISOT
(Algèbre et Théorie des nombres)
14e année, 1960/61, n° 7

9 janvier 1961

LE THÉORÈME DE LA BASE FINIE POUR LES POLYNÔMES DIFFÉRENTIELS

par Ellis R. KOLCHIN

Introduction. - Le théorème de la base finie de Hilbert est un outil précieux dans l'étude des équations algébriques, et il serait bien agréable d'avoir un théorème semblable dans la théorie des équations différentielles algébriques. Malheureusement, l'énoncé tout à fait analogue dans cette dernière théorie est inexact. Mais RITT a démontré (voir [2]) l'analogue du théorème plus faible dans lequel on affirme le principe des "chaînes ascendantes" pour l'ensemble des idéaux parfaits au lieu de l'ensemble de tous les idéaux (un idéal est dit "parfait" lorsqu'il contient un élément toutes les fois qu'il contient une puissance de cet élément) ; on sait que, pour beaucoup d'applications, le théorème affaibli suffit. Or, le théorème de Ritt a été démontré dans le cas où les coefficients forment un "corps différentiel" de caractéristique 0 . J'ai démontré [1] le théorème sous une hypothèse plus générale mais encore assez restrictive, donnant en même temps un contre-exemple pour quelques corps différentiels de caractéristique $\neq 0$. SEIDENBERG a repris la question et a démontré [3] que le théorème reste vrai pour un corps différentiel quelconque si on se borne à une classe d'idéaux plus étroite.

Dans ce qui suit, j'aborde le théorème dans une formulation plus large, et j'obtiens un résultat qui contient tous les résultats connus, et même un peu plus.

Avant de pouvoir le formuler, il faut préciser certaines définitions et développer certains résultats préliminaires.

1. Anneaux différentiels.

Un anneau (resp. corps) différentiel est un anneau (resp. corps) R muni d'un ensemble fini d'opérateurs Δ tel que

$$\delta(a + b) = \delta a + \delta b \quad ,$$

$$\delta(ab) = (\delta a)b + a(\delta b) \quad ,$$

$$(\delta\delta')a = \delta(\delta' a)$$

pour tous $a \in R$, $b \in R$, $\delta \in \Delta$, $\delta' \in \Delta$; l'ensemble Δ s'appelle l'ensemble

d'opérateurs de dérivation de R. Nous ne considérerons que des anneaux et des corps commutatifs.

Soient R un anneau différentiel, Δ son ensemble d'opérateurs de dérivations. Notons Θ le monoïde commutatif libre engendré par Δ ; si les éléments de Δ sont notés δ_1 , ..., δ_m , alors les éléments de Θ sont les produits $\delta_1^{i_1} \dots \delta_m^{i_m}$, chaque i_μ étant un entier naturel. On peut définir d'une façon unique une opération de Θ sur R prolongeant l'opération de Δ sur R telle que $(\theta\theta')\, a = \theta(\theta'\, a)$ pour $\theta \in \Theta$, $\theta' \in \Theta$, $a \in R$ et que $1a = a$ pour $a \in R$ (1 désignant l'élément-unité de Θ) ; Θ s'appelle l'ensemble d'opérateurs dérivés de R. Si

$$\theta = \delta_1^{i_1} \dots \delta_m^{i_m} \in \Theta \quad ,$$

l'entier $r = \sum i_\mu$ s'appelle l'ordre de θ , et se note ord θ ; et, pour chaque $a \in R$, θa s'appelle un dérivé de a d'ordre r .

Un élément $c \in R$, tel que $\delta c = 0$ pour chaque $\delta \in \Delta$, s'appelle une constante. L'ensemble des constantes de R est un sous-anneau différentiel de R (et dans le cas où R est un corps différentiel, un sous-corps différentiel de R) ; on l'appelle l'anneau (ou, selon le cas, le corps) des constantes de R. Si R est un corps de caractéristique $p \neq 0$, alors R^p est un sous-corps du corps des constantes de R.

Si R' est aussi un anneau différentiel, ayant le même ensemble d'opérateurs de dérivation Δ , une application $f : R \to R'$ s'appelle homomorphisme de R dans R' , si elle est un homomorphisme d'anneaux et si, de plus, $f(\delta a) = \delta f(a)$ pour chaque $a \in R$ et chaque $\delta \in \Delta$. L'image $f(R)$ d'un homomorphisme $f : R \to R'$ est un sous-anneau différentiel de R' . Le noyau k de f est un idéal de R ayant la propriété $\delta k \subset k$ pour chaque $\delta \in \Delta$. Un idéal de R ayant cette propriété s'appelle un idéal différentiel.

Si k est un idéal différentiel quelconque de R , et si $\delta \in \Delta$, deux éléments a , b d'une même classe de restes de R suivant k ont toujours leurs dérivés δa , δb dans une même classe de restes, de sorte que l'on peut définir sur l'anneau de restes R/k une structure d'anneau différentiel unique telle que l'homomorphisme canonique d'anneaux $g : R \to R/k$ est un homomorphisme d'anneaux différentiels. On appelle R/k l'anneau différentiel de restes de R suivant k. L'application bijective $\alpha \to g(\alpha)$ de l'ensemble d'idéaux α de R avec $\alpha \supset k$ sur l'ensemble de tous les idéaux de R/k (dont l'application réciproque est donnée par $\alpha' \to g^{-1}(\alpha')$) a la propriété :

α est différentiel si et seulement si $g(\alpha)$ l'est.

Pour chaque partie $\Sigma \subset R$, l'intersection de tous les idéaux différentiels de R contenant Σ est un idéal différentiel contenant Σ ; il s'appelle l'idéal différentiel de R engendré par Σ et se note $[\Sigma]$. Evidemment, $[\Sigma]$ est égal à l'idéal $(\Theta\Sigma)$ engendré par l'ensemble des dérivés θs $(\theta \in \Theta,\ s \in \Sigma)$.

Si Σ est une partie non vide multiplicative de R, et si $\delta \in \Delta$, deux éléments a/s, b/t de l'anneau de fractions $\Sigma^{-1} R$ avec $a/s = b/t$ ont toujours la propriété :

$$(s\,\delta a - a\,\delta s)/s^2 = (t\,\delta b - b\,\delta t)/t^2 \quad ;$$

on peut donc définir sur $\Sigma^{-1} R$, de façon évidente, une structure d'anneau différentiel, et alors l'homomorphisme canonique d'anneaux $h : R \to \Sigma^{-1} R$ devient un homomorphisme d'anneaux différentiels. On appelle $\Sigma^{-1} R$ l'anneau différentiel de fractions de R sur Σ. En appelant Σ-premier chaque idéal k de R tel que $k:s = k$ pour chaque $s \in \Sigma$, on a une application biunivoque $k \to (\Sigma^{-1} R)\, h(k) = \Sigma^{-1} k$ de l'ensemble des idéaux Σ-premiers de R sur l'ensemble des idéaux de $\Sigma^{-1} R$, dont l'application réciproque est donnée par $\alpha' \to h^{-1}(\alpha')$; α est différentiel si et seulement si $\Sigma^{-1} \alpha'$ l'est.

2. Polynômes différentiels.

Soit R un anneau différentiel admettant l'ensemble d'opérateurs de dérivation Δ et l'ensemble d'opérateurs dérivés Θ ; désignons par $\delta_1, \ldots, \delta_m$ les éléments de Δ.

Considérons une famille $(u_i)_{i\in I}$ d'éléments d'un sur-anneau différentiel S de R. Le sous-anneau de S engendré par les éléments de R et tous les dérivés θu_i $(\theta \in \Theta,\ i \in I)$ est un sous-anneau différentiel de S, que l'on note $R\{(u_i)_{i\in I}\}$. Si la famille $(\theta u_i)_{\theta\in\Theta, i\in I}$ est algébriquement liée sur R, on dit que la famille $(u_i)_{i\in I}$ est différentiellement algébriquement liée sur R ; sinon, on dit que $(u_i)_{i\in I}$ est différentiellement algébriquement libre sur R, ou bien que $(u_i)_{i\in I}$ est une famille d'indéterminées différentielles (sur R). On voit sans difficulté que, pour chaque ensemble I d'indices, il existe une famille $(y_i)_{i\in I}$ d'indéterminées différentielles.

Soit $(y_i)_{i\in I}$ une famille d'indéterminées différentielles sur R. Les éléments de $R\{(y_i)_{i\in I}\}$ s'appellent polynômes différentiels en $(y_i)_{i\in I}$, à coefficients dans R (ou sur R). Si $(u_i)_{i\in I}$ est une famille quelconque d'éléments d'un sur-anneau différentiel de R, ayant le même ensemble d'indices I, il existe un homomorphisme unique $R\{(y_i)_{i\in I}\} \to R\{(u_i)_{i\in I}\}$ laissant fixe chaque élément de R et envoyant y_i sur u_i pour chaque $i \in I$.

On l'appelle l'homomorphisme de substitution de (u_i) à (y_i) ; si $A \in R\{(y_i)_{i\in I}\}$, on désigne l'image de A par cet homomorphisme par $A((u_i)_{i\in I})$.

3. Rangements. Réduction.

Avec la même notation que dans le § 2, soit $S = R\{y_1, \dots, y_n\}$ l'anneau différentiel des polynômes différentiels sur R en une famille finie $(y_1, \dots, y_n)$ d'indéterminées différentielles.

Pour faciliter l'étude systématique de S, il est commode d'introduire un type d'ordre sur l'ensemble des dérivés θy_j $(\theta \in \Theta,\ 1 \leq j \leq n)$. Un ordre sur cet ensemble s'appelle un rangement de $(y_1, \dots, y_n)$ si cet ordre est total et si les deux conditions suivantes sont remplies :

$$u < \delta u \quad ,$$

$$u < v \implies \delta u < \delta v \quad ,$$

pour tous les dérivés u et v et chaque $\delta \in \Delta$. On voit sans peine qu'un rangement est toujours un bon ordre, c'est-à-dire un ordre par rapport auquel l'ensemble des dérivés θy_j est bien ordonné. Si $u < v$ on dit alors que u est de rang inférieur à v, etc. Un rangement s'appelle séquentiel si son ensemble ordonné est isomorphe à l'ensemble ordonné $\underline{N}$ des entiers naturels, c'est-à-dire si, pour chaque dérivé v, le nombre de dérivés u avec $u < v$ est fini. Par exemple, on obtient un rangement séquentiel en ordonnant l'ensemble des dérivés $\delta_1^{i_1}, \dots, \delta_m^{i_m} y_j$ lexicographiquement par rapport à $(\Sigma i_\mu, i_1, \dots, i_m, j)$.

Soit donné un rangement de $(y_1, \dots, y_n)$. Si $A \in S$ et $A \notin R$, on appelle leader de A et on note u_A le dérivé du plus haut rang figurant dans A. On peut alors écrire

$$A = A_0 + A_1 u_A + \dots + A_d u_A^d \quad , \qquad A_d \neq 0 \quad ,$$

où les A_i sont dans S et ne contiennent que des dérivés de rang inférieur à u_A ; on appelle initial de A et on note I_A le polynôme différentiel A_d. Le polynôme différentiel $\partial A/\partial u_A = A_1 + \dots + d.A_d\, u^{d-1}$ s'appelle le séparant de A et se note S_A.

On étend la notion de rang comparatif à l'ensemble S tout entier en convenant que $A \leq B$ si :

a. $A = 0$; ou

b. $A \in R$, $A \neq 0$, $B \neq 0$; ou

c. $A \notin \mathcal{R}$, $B \notin \mathcal{R}$, et ou bien $u_A < u_B$, ou bien $u_A = u_B$ et $\deg_{u_A} A \leqslant \deg_{u_B} B$.

On n'obtient pas ainsi une relation d'ordre sur $\mathcal{S}$, mais seulement une relation de pré-ordre, puisqu'on peut avoir $A \leqslant B$ et $B \leqslant A$ sans $A = B$. Mais ce pré-ordre est bon.

Si $A \in \mathcal{S}$, $A \notin \mathcal{R}$, alors $\delta A - S_A \, \delta u_A < \delta u_A$ pour chaque $\delta \in \Delta$. On voit par récurrence que, pour chaque $\theta \in \Theta$ avec $\operatorname{ord}\theta > 0$, il existe un $T_\theta \in \mathcal{S}$ avec $T_\theta < \theta u_A$ tel que $\theta A = S_A \, \theta u_A - T_\theta$. Ce fait nous permettra de démontrer un lemme pour les polynômes différentiels un peu analogue (bien que beaucoup plus compliqué) au théorème de division euclidienne.

Si $A \in \mathcal{S}$, $A \notin \mathcal{R}$, un élément $B \in \mathcal{S}$ s'appelle réduit par rapport à A si B ne contient aucun dérivé de u_A d'ordre > 0 et, de plus, $\deg_{u_A} B < \deg_{u_A} A$.

Un ensemble $\mathfrak{A} \subset \mathcal{S}$ s'appelle autoréduit si $\mathfrak{A}$ ne contient aucun élément de $\mathcal{R}$ et chaque élément de $\mathfrak{A}$ est réduit par rapport à chaque autre élément de $\mathfrak{A}$. Deux éléments distincts d'un ensemble autoréduit ont leurs leaders distincts. On en conclut que chaque ensemble autoréduit est fini. On dit que B est réduit par rapport à $\mathfrak{A}$, si B est réduit par rapport à chaque élément de $\mathfrak{A}$.

LEMME de réduction. - Soit $\mathfrak{A}$ un ensemble autoréduit dans $\mathcal{S}$, et soit $B_i \in \mathcal{S}$ $(1 \leqslant i \leqslant r)$. Il existe des entiers naturels $s(A)$, $t(A)$ $(A \in \mathfrak{A})$ et des éléments $B_i^* \in \mathcal{S}$ $(1 \leqslant i \leqslant r)$ tels que

$$\left.\begin{array}{l} B_i^* \text{ est réduit par rapport à } \mathfrak{A}, \\ \prod\limits_{A \in \mathfrak{A}} S_A^{s(A)} \, I_A^{t(A)} \cdot B_i \equiv B_i^* \pmod{[\mathfrak{A}]} \end{array}\right\} \quad (1 \leqslant i \leqslant r) \quad .$$

Si chaque B_i est réduit par rapport à $\mathfrak{A}$, le résultat est évident ; sinon, on procède (en utilisant le fait signalé ci-dessus) par récurrence sur le plus grand rang des dérivés v tels que

ou bien v est un dérivé d'ordre > 0 d'un leader u_A avec $A \in \mathfrak{A}$ et v se trouve dans un B_i au moins,

ou bien $v = u_A$ pour un $A \in \mathfrak{A}$ et $\deg_v B_i \geqslant \deg_{u_A} A$ pour un i au moins.

Remarquons que l'on peut définir la notion de rang comparatif sur l'ensemble des parties autoréduites de $\mathcal{S}$. A savoir, si $\mathfrak{A}$ et $\mathfrak{B}$ sont deux ensembles autoréduits dont les éléments (dans l'ordre des rangs croissants) sont $A_1, \ldots, A_r$ et $B_1, \ldots, B_s$, respectivement ; on pose $\mathfrak{A} \leqslant \mathfrak{B}$ si

ou bien, il existe un entier k avec $1 \leqslant k \leqslant r$ et $1 \leqslant k \leqslant s$ tel que A_i et B_i soient du même rang $(1 \leqslant i < k)$ et A_k soit de rang inférieur à B_k,

ou bien $r \geqslant s$ et A_i et B_i sont du même rang $(1 \leqslant i \leqslant s)$.

On définit ainsi une relation de bon pré-ordre sur l'ensemble de toutes les parties autoréduites de $\mathfrak{S}$.

4. Extensions séparables et extensions quasi-séparables.

Soit L une extension d'un corps K de caractéristique p. Rappelons que L est dite séparable sur K si :

ou bien $p = 0$,

ou bien $p \neq 0$ et les corps L^p et K sont linéairement disjoints sur K^p.

Nous allons introduire, pour une extension de corps, une propriété moins forte que la propriété d'être séparable.

Appelons $x = (x_i)_{i \in I}$ une famille d'éléments de L séparablement liée sur K s'il existe un polynôme $f \in K[X] = K[(X_i)_{i \in I}]$ tel que $f(x) = 0$ et $\frac{\partial f}{\partial X_i}(x) \neq 0$ pour un indice i au moins, et séparablement libre sur K dans le cas contraire. Dire que x est séparablement liée sur K équivaut à dire qu'une coordonnée x_i de x est séparablement algébrique sur l'extension du corps K engendrée par les autres coordonnées.

D'autre part, si J est une partie de I telle que la sous-famille $(x_i)_{i \in J}$ soit une base de transcendance de l'extension $K(x)$ de K, et si $I - J$ est fini, alors $\mathrm{card}(I - J)$ est indépendant du choix de J ; nous disons alors que la famille x est de codimension algébrique finie sur K et que l'entier naturel $\mathrm{card}(I - J)$ est sa codimension algébrique sur K.

Cela dit, on a le critère suivant de séparabilité d'une extension L du corps K :

pour que L soit séparable sur K, il faut et il suffit que chaque famille d'éléments de L qui est séparablement libre sur K soit de codimension algébrique 0 sur K (i. e. soit algébriquement libre sur K).

Nous dirons que L est quasi-séparable sur K si chaque famille d'éléments de L qui est séparablement libre sur K est de codimension algébrique finie sur K.

Evidemment, si L est séparable sur K, L est quasi-séparable. On peut démontrer que, si L est de type fini (en qualité d'extension du corps K), alors L est quasi-séparable sur K.

Ces notions s'appliquent, naturellement, aux corps différentiels.

Soit $\mathfrak{F}$ un corps différentiel de caractéristique p ; désignons par $\mathfrak{C}$ le corps de constantes de $\mathfrak{F}$. Nous dirons que $\mathfrak{F}$ est différentiellement parfait (resp. différentiellement quasi-parfait) si chaque sur-corps différentiel de $\mathfrak{F}$ est séparable (resp. quasi-séparable) sur $\mathfrak{F}$.

Si $p = 0$, évidemment $\mathfrak{F}$ est différentiellement parfait, donc différentiellement quasi-parfait.

Si $p \neq 0$, on voit aisément que $\mathfrak{F}$ est différentiellement parfait si et seulement si $\mathfrak{C} = \mathfrak{F}^p$.

Plus difficile à démontrer, mais également vrai, est le critère de quasi-perfection différentielle. $\mathfrak{F}$ (de caractéristique $p \neq 0$) est différentiellement quasi-parfait si et seulement si le degré $[\mathfrak{C} : \mathfrak{F}^p]$ est fini. Nous omettrons la démonstration.

5. Idéaux séparables et idéaux quasi-séparables.

Soit R un anneau commutatif et soit R_0 un sous-anneau de R.

Si p est un idéal premier de R et si $f : R \to R/p$ désigne l'homomorphisme canonique, le corps de fractions de $f(R)$ est une extension du corps de fractions de $f(R_0)$; nous dirons que p est séparable (resp. quasi-séparable) sur R_0 si cette extension est séparable (resp. quasi-séparable).

Cette notion de séparabilité peut être généralisée. Remarquons que p est séparable sur R_0 si et seulement si

ou bien la caractéristique p de $f(R_0)$ est 0,

ou bien $p \neq 0$, et $f(R)^p$ et $f(R_0)$ sont linéairement disjoints sur $f(R_0)^p$.

Considérons un idéal $\mathfrak{k}$ quelconque de R, et notons encore $f : R \to R/\mathfrak{k}$ l'homomorphisme canonique. Nous dirons que $\mathfrak{k}$ est séparable sur R_0 si $\mathfrak{k} = R$, ou si $\mathfrak{k} \neq R$ et les deux conditions suivantes sont remplies.

(i) $a \in R_0$, $a \notin \mathfrak{k}$, $b \in R$, $b \notin \mathfrak{k} \Rightarrow ab \notin \mathfrak{k}$ (de sorte que $\mathfrak{k} \cap R_0$ est un idéal premier de R_0 et $f(R_0)$ est intègre).

(ii) Ou bien la caractéristique p de $f(R_0)$ est 0 ou bien $p \neq 0$ et $f(R)^p$ et $f(R_0)$ sont linéairement disjoints sur $f(R_0)^p$.

Il est évident que, si $g : R \to R'$ est un épimorphisme d'anneaux avec $\ker g \subset \mathfrak{k}$, alors $\mathfrak{k}$ est un idéal de R séparable sur R_0 (resp. un idéal premier de R quasi-séparable sur R_0) si et seulement si $g(\mathfrak{k})$ est un idéal

de R' séparable sur $g(R_0)$ (resp. un idéal premier de R' quasi-séparable sur $g(R_0)$).

6. Systèmes conservatifs.

Soit R un anneau.

Considérons un ensemble $\mathfrak{C}$ d'idéaux de R tel que les trois conditions suivantes soient satisfaites.

(i) L'intersection d'un ensemble quelconque d'éléments de $\mathfrak{C}$ est elle-même un élément de $\mathfrak{C}$.

(ii) La réunion d'un ensemble non vide d'éléments de $\mathfrak{C}$ qui est totalement ordonné (par inclusion) est toujours un élément de $\mathfrak{C}$.

(iii) Si $c \in \mathfrak{C}$ et $s \in R$, alors $c:s^\infty \in \mathfrak{C}$ (où $c:s^\infty = \bigcup (c : s^n)$).

Nous appellerons un tel ensemble $\mathfrak{C}$ un système conservatif de R.

Exemples.

1° L'ensemble de tous les idéaux de R.

2° L'ensemble réduit au seul élément R.

3° L'ensemble formé par R et tous les idéaux de R séparables sur R_0 et ayant avec R_0 une intersection donnée.

4° L'ensemble de tous les idéaux parfaits de R. Un idéal α de R s'appelle parfait si

$$(x \in R \text{ et } x^2 \in \alpha) \implies (x \in \alpha) \quad .$$

5° L'ensemble de tous les idéaux différentiels d'un anneau différentiel.

6° L'intersection d'un ensemble non vide quelconque de systèmes conservatifs de R.

Un système conservatif dont tous les éléments sont parfaits (resp. séparables sur R_0, resp. différentiels) s'appellera parfait (resp. séparable sur R_0, resp. différentiel).

Soit $F : \mathfrak{C} \to \mathfrak{C}'$ une application de $\mathfrak{C}$ dans un système conservatif d'un anneau R', et supposons que $F(\bigcap_{c \in M} c) = \bigcap_{c \in M} F(c)$ pour tous les ensembles $M \subset \mathfrak{C}$. Alors F est une application croissante :

$$a \subset b \Rightarrow F(a) \subset F(b) \quad .$$

Si, de plus,

$$F(\bigcup_{c\in T} c) = \bigcup_{c\in T} F(c)$$

pour chaque ensemble $T \subset \mathfrak{C}$ totalement ordonné, et si, pour chaque $c \in \mathfrak{C}$ et chaque $s' \in R'$, il existe un $c_0 \in \mathfrak{C}$ tel que $F(c) : s'^{\infty} = F(c_0)$, alors on dit que F est une application conservative, ou un homomorphisme, de $\mathfrak{C}$ dans $\mathfrak{C}'$. Si F est un homomorphisme bijectif, alors F^{-1} est un homomorphisme de $\mathfrak{C}'$ dans $\mathfrak{C}$; on dit alors que F est un isomorphisme. On peut voir, dans le cas général, que l'image $F(\mathfrak{C})$ est un système conservatif.

Exemples.

1° Soit R_0 un sous-anneau de R. L'application $c \to c \cap R_0$ $(c \in \mathfrak{C})$ est conservative. Désignons l'image (système conservatif de R_0) par $\mathfrak{C}|R_0$.

2° Soit $f : R \to R'$ un épimorphisme. L'ensemble de tous les $c \in \mathfrak{C}$ avec $c \supset \ker f$ est un système conservatif de R, et $c \to f(c)$ en est un isomorphisme sur un système conservatif de R', que nous notons $f(\mathfrak{C})$. Quand f est l'homomorphisme canonique $R \to R/\mathfrak{k}$ nous désignons $f(\mathfrak{C})$ par $\mathfrak{C}/\mathfrak{k}$.

3° Soit Σ une partie non vide multiplicative de R. L'ensemble de tous les $c \in \mathfrak{C}$ qui sont Σ-premiers est un système conservatif de R, et $c \to \Sigma^{-1} c$ en est un isomorphisme sur un système conservatif de $\Sigma^{-1} R$ que nous notons $\Sigma^{-1} \mathfrak{C}$.

Une application conservative $F : \mathfrak{C} \to \mathfrak{C}'$ s'appelle parfaite si $F(c)$ est parfait chaque fois que c l'est. Les applications conservatives des exemples ci-dessus sont parfaites, et (dans les deux derniers exemples) leurs inverses également.

Soit $\mathfrak{C}$ un système conservatif de R. Si Σ est une partie de R, on note $(\Sigma)_{\mathfrak{C}}$ l'intersection de tous les éléments de $\mathfrak{C}$ contenant Σ, c'est-à-dire le plus petit élément de $\mathfrak{C}$ qui contient Σ. Si $c \in \mathfrak{C}$, $c = (\Sigma)_{\mathfrak{C}}$, et Σ est finie, on dit que Σ est une $\mathfrak{C}$-base de c.

Pour un Σ quelconque, on appelle $\mathfrak{C}$-composant de Σ chaque élément minimal de l'ensemble des éléments de $\mathfrak{C}$ qui sont premiers et qui contiennent Σ. Chaque élément premier de $\mathfrak{C}$ qui contient Σ contient un $\mathfrak{C}$-composant de Σ.

LEMME 1. - Si $a \in (\Sigma)_{\mathfrak{C}}$, il existe alors une partie finie Φ de Σ avec $a \in (\Phi)_{\mathfrak{C}}$.

Démonstration par récurrence sur $\mathrm{card}(\Sigma)$.

LEMME 2. - Soit $\mathfrak{C}$ un système conservatif parfait de R ; soient Σ et T des parties de R . Alors

$$(\Sigma T)_{\mathfrak{C}} = (\Sigma)_{\mathfrak{C}} \cap (T)_{\mathfrak{C}} \quad .$$

$$(\Sigma T)_{\mathfrak{C}} : \Sigma = \bigcap_{s\in\Sigma} (\Sigma T)_{\mathfrak{C}} : s = \bigcap_{s\in\Sigma} (\Sigma T)_{\mathfrak{C}} : s^{\infty}$$

est un élément de $\mathfrak{C}$ contenant T , donc contenant $(T)_{\mathfrak{C}}$; il en résulte que $(\Sigma T)_{\mathfrak{C}} : (T)_{\mathfrak{C}}$ est un élément de $\mathfrak{C}$ contenant Σ , donc contenant $(\Sigma)_{\mathfrak{C}}$; ainsi $(\Sigma)_{\mathfrak{C}} (T)_{\mathfrak{C}} \subset (\Sigma T)_{\mathfrak{C}}$. Puisque l'idéal $(\Sigma T)_{\mathfrak{C}}$ est parfait, le résultat en découle.

COROLLAIRE. - Si $\mathfrak{C}$ est un système conservatif parfait, alors chaque élément de $\mathfrak{C}$ est l'intersection de ses $\mathfrak{C}$-composants.

Soit $c \in \mathfrak{C}$. Si $x \notin c$, il existe un élément de $\mathfrak{C}$ contenant c mais ne contenant pas x , donc il existe un tel élément maximal m_x ; en utilisant le lemme 2, on voit que m_x est premier, donc que m_x contient un $\mathfrak{C}$-composant p_x de c . Evidemment $\bigcap_{x\notin c} p_x = p$.

7. Systèmes conservatifs rittiens.

Pour un système conservatif $\mathfrak{C}$ les deux conditions suivantes sont équivalentes.

(i) Chaque élément possède une $\mathfrak{C}$-base.

(ii) Chaque partie non vide de $\mathfrak{C}$ possède un élément maximal. Si $\mathfrak{C}$ satisfait ces conditions, et si, de plus, $\mathfrak{C}$ est parfait, on dit que $\mathfrak{C}$ est rittien.

Pour les systèmes conservatifs rittiens, le corollaire ci-dessus peut être beaucoup précisé.

THÉORÈME 1. - Si $\mathfrak{C}$ est un système conservatif rittien, chaque $c \in \mathfrak{C}$ est l'intersection d'un ensemble fini d'idéaux premiers dans $\mathfrak{C}$ dont aucun ne contient un autre ; cet ensemble fini est unique, étant l'ensemble de tous les composants de c .

L'existence se démontre par récurrence sur c (en munissant $\mathfrak{C}$ de l'ordre opposé à l'inclusion). L'unicité ne présente aucune difficulté.

PROPOSITION 1. - Soit $\mathfrak{C}$ un système conservatif rittien.

a. Chaque système conservatif contenu dans $\mathfrak{C}$ est rittien.

b. Chaque image d'un homomorphisme parfait de $\mathfrak{C}$ est rittien.

(a) est évident. Quant à (b), remarquons que, si (c_i') ... est une suite strictement croissante dans $F(\mathfrak{C})$, et si l'on note c_i l'intersection de tous les $c \in \mathfrak{C}$ avec $F(c) = c_i'$, alors (c_i) est une suite strictement croissante dans $\mathfrak{C}$.

LEMME 3. - Si le système conservatif parfait $\mathfrak{C}$ de R n'est pas rittien, l'ensemble des éléments de $\mathfrak{C}$ qui ne possèdent pas une $\mathfrak{C}$-base a un élément maximal. Un tel élément maximal est toujours premier.

L'existence d'un élément maximal résulte du lemme de Zorn ; que cet élément soit premier est une conséquence du lemme 2.

PROPOSITION 2. - Soient R_0 et R_1 deux sous-anneaux de R, R_1 étant un sur-anneau de R_0 de type fini, et soit $\mathfrak{C}$ un système conservatif parfait de R. Si $\mathfrak{C}|R_0$ est rittien alors $\mathfrak{C}|R_1$ est rittien.

On peut supposer que $R_1 = R_0[v]$, v étant un élément de R. Supposons la proposition fausse. Il existe alors (lemme 3) dans l'ensemble des éléments de $\mathfrak{C}|R_1$ sans $\mathfrak{C}|R_1$-base un élément maximal m, et m est premier. $\mathfrak{C}|R_0$ étant rittien, $m \cap R_0$ a une $\mathfrak{C}|R_0$-base Ψ_1 ; évidemment

$$(m \cap R_0)_{\mathfrak{C}|R_1} = (\Psi_1)_{\mathfrak{C}|R_1} \quad ,$$

d'où

$$m \neq (m \cap R_0)_{\mathfrak{C}|R_1} \quad ,$$

et il existe donc un polynôme $f = a_0 X^n + \ldots + a_n \in R_0[X]$ avec $f(v) \in m$ et $f(v) \notin (m \cap R_0)_{\mathfrak{C}|R_1}$. En choisissant n aussi petit que possible, on a $n > 0$ et $a_0 \notin m$. A cause de la maximalité de m, $(a_0, m)_{\mathfrak{C}|R_1}$ a une $\mathfrak{C}|R_1$-base et (lemme 1) même une $\mathfrak{C}|R_1$-base de la forme $\{a_0\} \cup \Psi_2$ avec $\Psi_2 \subset m$.

Or, pour chaque $w \in m$, on peut écrire $w = g(v)$, où $g \in R_0[X]$; en divisant g par f, on a $a_0^k g = qf + r$ avec $\deg r < n$, donc

$$r(v) \in (m \cap R_0)_{\mathfrak{C}|R_1} = (\Psi_1)_{\mathfrak{C}|R_1} \quad ,$$

d'où

$$a_0^k w \in (f(v), \Psi_1)_{\mathfrak{C}|R_1} \quad .$$

Ainsi,

$$a_0 m \subset (f(v), \Psi_1)_{\mathfrak{C}|R_1} \quad ,$$

d'où (voir le lemme 2)

$$\mathfrak{m} = \mathfrak{m} \cap (a_0 , \mathfrak{m})_{\mathfrak{C}|R_1} = \mathfrak{m} \cap (a_0 , \Psi_2)_{\mathfrak{C}|R_1} = (a_0 \mathfrak{m} , \Psi_2)_{\mathfrak{C}|R_1} = (f(v) , \Psi_1 , \Psi_2)_{\mathfrak{C}|R_1} ,$$

et ceci contredit le fait que $\mathfrak{m}$ n'a pas une $\mathfrak{C}|R_1$-base.

8. Un lemme.

Soit $\mathfrak{S} = \mathfrak{R}\{y_1 , \ldots , y_n\}$ l'anneau différentiel des polynômes différentiels en une famille finie d'indéterminées différentielles sur l'anneau différentiel $\mathfrak{R}$.

LEMME 4. - Soit $\mathfrak{p}$ un idéal différentiel premier de $\mathfrak{S}$, quasi-séparable sur $\mathfrak{R}$; soit donné un rangement séquentiel de $(y_1 , \ldots , y_n)$; soit $\mathfrak{A}$ une partie autoréduite de $\mathfrak{p}$ telle que $S_A \notin \mathfrak{p}$ pour chaque $A \in \mathfrak{A}$, de rang minimal. Notons V l'ensemble des dérivés des y_i qui ne sont dérivés d'ordre > 0 d'aucun leader u_A avec $A \in \mathfrak{A}$. Il existe alors une partie finie Y de V telle que chaque élément de $\mathfrak{p}$ qui est réduit par rapport à $\mathfrak{A}$ est dans l'idéal $(\mathfrak{p} \cap \mathfrak{R}[Y])$ de $\mathfrak{S}$.

Soit W l'ensemble des éléments $w \in V$ tels que seulement un nombre fini des dérivés de w soient dans V. On voit que, si $v \in V - W$, alors il existe un opérateur de dérivation δ tel que $\delta v \in V - W$. On peut démontrer que l'ensemble W est fini.

Remarquons ensuite que, si un élément $P \in \mathfrak{p}$ est réduit par rapport à $\mathfrak{A}$ et $P \notin \mathfrak{R}$, alors $S_p \in \mathfrak{p}$; c'est une conséquence de la minimalité du rang de $\mathfrak{A}$. Or, si $P \in \mathfrak{p} \cap \mathfrak{R}[V - W]$, alors P est réduit par rapport à $\mathfrak{A}$. En utilisant le fait que le rangement est séquentiel, et le lemme de réduction (§ 3), on peut démontrer alors que, pour chaque $P \in \mathfrak{p} \cap \mathfrak{R}[V - W]$,

$$\partial P/\partial v \in \mathfrak{p} \qquad (v \in V - W) \quad .$$

Notons $f : s \to s/\mathfrak{p}$ l'homomorphisme canonique. Ce que nous venons de dire montre que, si T est une partie de $V - W$, alors la famille $(f(v))_{v \in T}$ est séparablement libre sur $f(\mathfrak{R})$ (c'est-à-dire, sur le corps de fractions de $f(\mathfrak{R})$).

Supposons le lemme faux. Notons V_i l'ensemble des éléments de V d'ordre $< i$, et posons $q_i = \mathrm{card}(V_i)$; on voit alors que, pour chaque $i \in \mathbb{N}$, il existe un entier $i' > i$ tel que $\mathfrak{p} \cap \mathfrak{R}[V_{i'}]$ contienne un élément qui n'est pas dans $(\mathfrak{p} \cap \mathfrak{R}[V_i])$. Cela entraîne que le degré de transcendance de $f(\mathfrak{R}[V_{i'}])$ sur $f(\mathfrak{R}[V_i])$ est $< q_{i'} - q_i$. En posant

$$i^{(0)} = i \ , \quad i^{(\nu+1)} = i^{(\nu)'} \ (\nu \in \underset{\sim}{N}) \ ,$$

on voit que le degré de transcendance de $f(R[V_i(h)])$ sur $f(R)$ est

$$\leqslant q_i + \sum_{0 \leqslant \nu < h} (q_{i(\nu+1)} - q_{i(\nu)} - 1) = q_{i(h)} - h \ .$$

Donc, pour chaque i, il existe un $i^* > i$ tel que le degré de transcendance de $f(R[V_{i^*}])$ sur $f(R)$ soit $< q_{i^*} - q_i$.

Choisissons $i(0) \in \underset{\sim}{N}$ assez grand pour que $W \subset V_{i(0)}$, et posons

$$i(\nu + 1) = i(\nu)^* \ (\nu \in \underset{\sim}{N}) \ .$$

Le degré de transcendance de $f(R[V_{i(\nu+1)}])$ sur $f(R)$ est $< q_{i(\nu+1)} - q_{i(\nu)}$, donc la famille $(f(v))_{v \in V_{i(\nu+1)} - V_{i(\nu)}}$ est algébriquement liée sur $f(R)$. Cela étant ainsi pour chaque ν, on voit, en posant

$$V' = \bigcup_{\nu \in \underset{\sim}{N}} (V_{i(\nu+1)} - V_{i(\nu)}) = V - V_{i(0)} \subset V - W \ ,$$

que la famille $(f(v))_{v \in V'}$ est de codimension algébrique infinie sur $f(R)$. Mais cette famille est séparablement libre sur $f(R)$. Donc p n'est pas quasi-séparable sur R.

9. Le théorème de la base.

THÉORÈME 2. - *Soient R un anneau différentiel, S un sur-anneau différentiel de R de type fini, et $\mathfrak{C}$ un système conservatif parfait différentiel de S. Si $\mathfrak{C}|R$ est rittien et si chaque élément premier de $\mathfrak{C}$ est quasi-séparable sur R, alors $\mathfrak{C}$ est rittien.*

Il existe un R-épimorphisme d'un anneau différentiel de polynômes différentiels $R\{y_1, \dots, y_n\}$ sur S ; on peut donc supposer qua même $S = R\{y_1, \dots, y_n\}$. Supposons le théorème faux. Alors (lemme 3) il existe dans l'ensemble des éléments de $\mathfrak{C}$ sans $\mathfrak{C}$-base, un élément maximal p, et p est premier. En adoptant la notation du lemme 4 de la proposition 2, on voit qu'il existe une partie finie Ψ de $p \cap R[Y]$ telle que

$$p \cap R[Y] = (\Psi)_{\mathfrak{C}|R[Y]} \ ,$$

d'où

$$(p \cap R[Y]) \subset (\Psi)_{\mathfrak{C}} \ .$$

Si $B \in \mathfrak{p}$, alors (lemme de réduction) on peut écrire

$$\prod_{A \in \mathfrak{A}} S_A^{s(A)} I_A^{t(A)} . B \equiv B^* \pmod{[\mathfrak{A}]} \quad ,$$

où B^* est réduit par rapport à $\mathfrak{A}$. En posant $H = \prod_{A \in \mathfrak{A}} S_A I_A$, on en conclut que

$$H\mathfrak{p} \subset (\mathfrak{A} , \Psi)_{\mathfrak{C}} \quad .$$

D'autre part, on voit sans peine que $I_A \notin \mathfrak{p}$ $(A \in \mathfrak{A})$, de sorte que $H \notin \mathfrak{p}$; donc $(H , \mathfrak{p})_{\mathfrak{C}}$ a une $\mathfrak{C}$-base, et même (lemme 1) une $\mathfrak{C}$-base de la forme $\{H\} \cup \Phi$, où $\Phi \subset \mathfrak{p}$. Donc, grâce au lemme 2,

$$\mathfrak{p} = \mathfrak{p} \cap (H , \mathfrak{p})_{\mathfrak{C}} = \mathfrak{p} \cap (H , \Phi)_{\mathfrak{C}} = (H\mathfrak{p} , \Phi)_{\mathfrak{C}} = (\mathfrak{A} , \Psi , \Phi)_{\mathfrak{C}} \quad ,$$

de sorte que $\mathfrak{A} \cup \Psi \cup \Phi$ est une $\mathfrak{C}$-base de $\mathfrak{p}$.

Un anneau différentiel, dans lequel l'ensemble de tous les idéaux différentiels parfaits est un système conservatif rittien, s'appelle rittien.

COROLLAIRE 1. - L'anneau de polynômes différentiels $\mathfrak{R}\{y_1 , \cdots , y_n\}$ est rittien si et seulement si $\mathfrak{R}$ est rittien et, pour chaque idéal différentiel premier $\mathfrak{p}_0$ de $\mathfrak{R}$, le corps différentiel de fractions de $\mathfrak{R}/\mathfrak{p}_0$ est différentiellement quasi-parfait.

Le seul point qui n'est pas conséquence du théorème est le fait que si $\mathfrak{R}\{y_1 , \cdots , y_n\}$ est rittien et si $\mathfrak{p}_0$ est un idéal différentiel premier de $\mathfrak{R}$, alors le corps différentiel de fractions de $\mathfrak{R}/\mathfrak{p}_0$ (corps que nous notons $\mathfrak{F}$) est différentiellement quasi-parfait. Or, on voit aisément que si $\mathfrak{R}\{y_1 , \cdots , y_n\}$ est rittien, alors $(\mathfrak{R}/\mathfrak{p}_0)\{y_1 , \cdots , y_n\}$ est rittien, donc $\mathfrak{F}\{y_1 , \cdots , y_n\}$ aussi. Si $\mathfrak{F}$ n'était pas différentiellement quasi-parfait, il y aurait (voir critère de quasi-perfection différentielle) une suite infinie (γ_i) de constantes dans $\mathfrak{F}$ telle que $\gamma_i \notin \mathfrak{F}^p$ $(\gamma_0 , \gamma_1 , \cdots , \gamma_{i-1})$ pour chaque i ; les idéaux $\mathfrak{p}_i = (y_1^p - \gamma_0 , (\delta y_1)^p - \gamma_1 , \cdots , (\delta^i y_1)^p - \gamma_i)$ de $\mathfrak{F}\{y_1 , \cdots , y_n\}$ seraient différentiels et premiers (a fortiori parfaits), et formeraient une suite infinie strictement croissante ; donc $\mathfrak{F}\{y_1 , \cdots , y_n\}$ ne serait pas rittien.

COROLLAIRE 2. - Si $\mathfrak{F}$ est un corps différentiel, l'anneau de polynômes différentiels $\mathfrak{F}\{y_1 , \cdots , y_n\}$ est rittien si et seulement si $\mathfrak{F}$ est différentiellement quasi-parfait.

COROLLAIRE 3. - Si $\mathfrak{F}$ est un corps différentiel, le système conservatif de tous les idéaux différentiels parfaits de $\mathfrak{F}\{y_1 , \cdots , y_n\}$ qui sont séparables sur $\mathfrak{F}$

est rittien.

Ce dernier corollaire est le théorème de Seidenberg.

BIBLIOGRAPHIE

[1] KOLCHIN (Ellis R.). - On the basis theorem for differential systems, Trans. Amer. math. Soc., t. 52, 1942, p. 115-127.

[2] RITT (Joseph Fels). - Differential algebra. - New York, American mathematical Society, 1950 (Amer. math. Soc. Coll. Publ., 33).

[3] SEIDENBERG (A.). - Some basis theorems in differential algebra (caracteristic b , arbitrary), Trans. Amer. math. Soc., t. 73, 1952, p. 174-190.