# UN THÉORÈME DE TRANSFERT D'UN ANNEAU ABSTRAIT À L'ANNEAU DES POLYNOMES

LÉONCE LESIEUR

CERTAINS théorèmes démontrent pour l'anneau des polynomes $A[x_1, \ldots, x_n]$ une propriété supposée valable dans l'anneau $A$, par exemple le théorème de la base finie de Hilbert pour tout idéal d'un anneau commutatif qui possède un élément unité. (Voir P. Dubreil [2] p. 210, ou B. L. Van der Waerden [7] §80, ou le mémoire original de Hilbert [3], p. 473.) E. Lasker [5] a montré que tout idéal de l'anneau $K[x_1, x_2, \ldots, x_n]$ des polynomes à $n$ variables à coefficients dans un corps $K$ commutatif est l'intersection d'un nombre fini d'idéaux primaires. Sa démonstration repose sur la théorie de l'élimination. E. Noether ([7] §83) a établi plus généralement le décomposition en un nombre fini d'idéaux primaires pour tout idéal d'un anneau satisfaisant le théorème de la base finie (anneau noetherien).

Le présent travail apporte d'abord, aux paragraphes 1 et 2, un nouveau théorème de transfert d'un anneau $A$ à l'anneau $A[x_1, \ldots, x_n]$ des polynomes à $n$ variables. Je suppose la propriété suivante valables dans $A$ (commutatif et possédant un élément unité).

PROPRIÉTÉ 1. Tout idéal $\mathfrak{i}$, différent de l'idéal unité $A$, admet au moins un diviseur premier $\mathfrak{p}$, différent de $A$, tel que pour tout élément $p$ de $\mathfrak{p}$ il existe au moins un entier $\rho$, et un élément $l$ associé, vérifiant:

$$p^\rho \,.\, l \equiv 0(\mathfrak{i}), \text{ avec } l \not\equiv 0\ (\mathfrak{p}).$$

Cette propriété se conserve alors pour l'anneau $A[x_1, \ldots, x_n]$. (théorème 1).

Je donne ensuite, au paragraphe 3, une application au théorème des zéros de Hilbert (Nullstellensatz) et au théorème exprimant qu'un idéal premier dans $K[x_1, \ldots, x_n]$ est l'idéal associé à sa variété (théorème 6); au paragraphe 4, je présente au moyen d'une démonstration élémentaire la décomposition d'un idéal dans $K[x_1, \ldots, x_n]$ en un nombre fini d'idéaux primaires.

**1. Remarques préliminaires.** $A$ est un anneau commutatif avec élément unité $e$. Soit $\mathfrak{J}$ un idéal dans l'anneau $A[x]$ des polynomes à une variable. L'ensemble des polynomes de l'idéal $\mathfrak{J}$ qui se réduisent à des éléments de l'anneau $A$ des coefficients constitue un idéal dans $A$:

$$\mathfrak{i} = \mathfrak{J} \cap A.$$

C'est l'intersection de $\mathfrak{J}$ avec $A$, que nous appellerons aussi la *projection*[1] de l'idéal $\mathfrak{J}$ dans $A$. Lorsque l'idéal $\mathfrak{J}$ n'est pas l'idéal unité $\mathfrak{R} = A[x]$, sa projection $\mathfrak{i}$ n'est pas l'idéal unité $A$; sinon, l'idéal $\mathfrak{i}$ admettrait $e$ comme

Reçu le 24 Janvier, 1949.

[1]On pourrait encore dire, d'après Krull [4], "restriction".



https://doi.org/10.4153/CJM-1950-006-9 Published online by Cambridge University Press

élément, et de même $\mathfrak{J}$ qui serait confondu avec $\mathfrak{R}$. Quand l'idéal $\mathfrak{J}$ est un idéal premier $\mathfrak{P}$ dans $A[x]$, sa projection $\mathfrak{i}$ est un idéal premier $\mathfrak{p}$ dans $A$.

Soit $\mathfrak{p}$ un idéal premier différent de $A$. L'anneau $A/\mathfrak{p}$ est un domaine d'intégrité dont le corps des quotients $k$ est constitué par les éléments

$$\frac{\bar{u}}{\bar{w}}$$

où $\bar{u}$ et $\bar{w}$ sont les classes de $u$ et $w$ modulo $\mathfrak{p}$, avec $w \not\equiv 0(\mathfrak{p})$.

A chaque polynome

$$F(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in A[x]$$

on peut faire correspondre le polynome

$$\overline{F(x)} = \bar{a}_n x^n + \bar{a}_{n-1}x^{n-1} + \ldots + \bar{a}_0 \in k[x].$$

Cette correspondance est un homomorphisme $\lambda$ de $A[x]$ dans $k[x]$.

Quand $F(x)$ décrit l'idéal $\mathfrak{J}$ dans $A[x]$, les polynomes de la forme

$$\frac{\lambda F(x)}{\bar{w}}, \text{ où } w \not\equiv 0(\mathfrak{p}) \text{ dans } A$$

constituent un idéal $\bar{\mathfrak{J}}$ dans $k[x]$. Posons

$$\bar{\mathfrak{J}} = \bar{\lambda}(\mathfrak{J}).$$

La correspondance $\bar{\lambda}$ ramène l'étude de certaines propriétés des idéaux dans $A[x]$ à des propriétés simples des idéaux bien connus dans $k[x]$. Elle respecte évidemment l'inclusion des idéaux dans $A[x]$, c'est à dire:

$$\mathfrak{J} \subseteq \mathfrak{F} \text{ entraine } \bar{\mathfrak{J}} \subseteq \bar{\mathfrak{F}}.$$

De plus, elle a les propriétés du lemme suivant, qui nous sera utile:

Lemme 1. *Lorsque $\mathfrak{P}$ est un idéal premier différent de $\mathfrak{R} = A[x]$, tel que $\mathfrak{P} \cap A = \mathfrak{p}$, l'idéal $\bar{\mathfrak{P}} = \bar{\lambda}(\mathfrak{P})$ est un idéal premier dans $k[x]$, différent de l'anneau $k[x]$.*

*Inversement, $\bar{\mathfrak{P}}$ étant un idéal premier différent de l'anneau $k[x]$, il n'existe qu'un idéal premier $\mathfrak{P}$ dans $A[x]$, vérifiant*

$$\mathfrak{P} \cap A = \mathfrak{p} \text{ et } \bar{\lambda}(\mathfrak{P}) = \bar{\mathfrak{P}}.$$

*Cet idéal, différent de $\mathfrak{R}$, est constitué par les polynomes $F(x)$ tels que*

$$\lambda F(x) \in \bar{\mathfrak{P}}.$$

*Démonstration*: soit $\mathfrak{P}$ un idéal premier, différent de $\mathfrak{R}$, qui se projette dans $A$ suivant $\mathfrak{p}$. Montrons que $\bar{\mathfrak{P}}$ est premier. Supposons

$$K_1(x).\, K_2(x) \equiv 0 \quad (\bar{\mathfrak{P}}).$$

Les polynomes $K_1(x)$ et $K_2(x)$ peuvent s'écrire

$$K_1(x) = \frac{\lambda A_1(x)}{\bar{w}_1};\; K_2(x) = \frac{\lambda A_2(x)}{\bar{w}_2}$$

avec $A_1(x)$ et $A_2(x) \in A[x]$.

https://doi.org/10.4153/CJM-1950-006-9 Published online by Cambridge University Press

D'où, d'après la définition de $\overline{\mathfrak{P}}$

$$\frac{\lambda A_1(x)}{\bar{w}_1} \cdot \frac{\lambda A_2(x)}{\bar{w}_2} = \frac{\lambda P(x)}{\bar{w}} \quad \text{avec } P(x) \epsilon \mathfrak{P}.$$

On en déduit dans $A[x]$:

$$wA_1A_2 = w_1w_2P + \Pi(x),$$

$\Pi(x)$ étant un polynome à coefficients dans $\mathfrak{p}$. Le deuxième membre appartient à $\mathfrak{P}$ puisque $\mathfrak{p} \subset \mathfrak{P}$. La condition $w \not\equiv 0(\mathfrak{p})$ entraine $w \not\equiv 0(\mathfrak{P})$ puisque $\mathfrak{P} \cap A = \mathfrak{p}$. Comme $\mathfrak{P}$ est premier, l'un des polynomes $A_1(x)$ ou $A_2(x)$ appartient à $\mathfrak{P}$. Donc l'un des polynomes $K_1(x)$ ou $K_2(x)$ appartient à $\overline{\mathfrak{P}}$, qui est bien un idéal premier. Démontrons que $\overline{\mathfrak{P}}$ est différent de $k[x]$. Si l'idéal $\overline{\mathfrak{P}}$ remplissait $k[x]$, il contiendrait une constante non nulle de $k$, soit

$$\frac{\bar{u}'}{\bar{w}'} = \frac{\lambda F_0(x)}{\bar{w}}$$

avec

$$F_0(x) = a_nx^n + \ldots + a_0 \epsilon \mathfrak{P}$$

et

$$\bar{a}_n = 0, \ldots, \bar{a}_1 = 0; \bar{a}_0 \neq 0$$

ou

$$a_n \equiv \ldots \equiv a_1 \equiv 0(\mathfrak{p}); a_0 \not\equiv 0(\mathfrak{p}).$$

Mais on tire de l'égalité

$$a_0 = F_0(x) - a_nx^n - \ldots - a_1x,$$

$a_0 \epsilon \mathfrak{P}$ donc $a_0 \epsilon \mathfrak{p}$, ce qui est impossible.

Inversement, donnons nous un idéal $\overline{\mathfrak{P}}$ dans $k[x]$, premier, et différent de l'anneau $k[x]$. Nous voulons trouver $\mathfrak{P}$, premier dans $A[x]$, tel que

$$\mathfrak{P} \cap A = \mathfrak{p} \qquad \text{et} \qquad \overline{\mathfrak{P}} = \bar{\lambda}(\mathfrak{P}).$$

L'ensemble $\mathfrak{P}$ des polynomes $F(x)$ qui vérifient

$$\lambda F(x) \epsilon \overline{\mathfrak{P}}$$

est un idéal premier; il satisfait $\mathfrak{P} \cap A = \mathfrak{p}$, car

$$\overline{\mathfrak{P}} \neq k[x];$$

il est différent de $A[x]$ puisque $\mathfrak{p}$ est différent de $A$. De plus $\bar{\lambda}(\mathfrak{P})$ décrit $\overline{\mathfrak{P}}$, tout polynome de $\overline{\mathfrak{P}}$ pouvant s'écrire

$$\frac{\lambda F(x)}{\bar{w}} \quad \text{avec } F(x) \epsilon A[x].$$

La solution $\mathfrak{P}$ ainsi trouvée est unique; soit $\mathfrak{P}'$ un autre idéal premier tel que

$$\mathfrak{P}' \cap A = \mathfrak{p} \quad \text{et} \quad \bar{\lambda}(\mathfrak{P}') = \overline{\mathfrak{P}}.$$

$F'(x) \epsilon \mathfrak{P}'$ entraine par définition $\dfrac{\lambda F'(x)}{\bar{w}} \epsilon \overline{\mathfrak{P}}$, ou $\lambda F'(x) \epsilon \overline{\mathfrak{P}}$, ce qui prouve

$$\mathfrak{P}' \subseteq \mathfrak{P}.$$

Supposons maintenant $F(x)\epsilon\mathfrak{P}$, donc $\lambda F(x)\epsilon\overline{\mathfrak{P}}$. L'idéal $\overline{\mathfrak{P}}$ est principal dans $k[x]$; on peut prendre sa base sous la forme $\lambda\varphi(x)$, irréductible dans $k[x]$, avec $\varphi(x)\epsilon A[x]$. Il existe donc $P'_0(x)\epsilon\mathfrak{P}'$ et $w'_0 \not\equiv 0(\mathfrak{p})$ tels que

$$\overline{\varphi(x)} = \lambda\varphi(x) = \frac{\lambda P'_0(x)}{\overline{w}'_0}.$$

Il vient alors

$$\lambda F(x) = K_1(x)\frac{\lambda P'_0(x)}{\overline{w}'_0} = \frac{\lambda A_1(x)}{\overline{w}}\frac{\lambda P'_0(x)}{\overline{w}'_0}.$$

On en déduit dans $A[x]$:

$$w \,.\, w'_0 \,.\, F(x) = A_1(x)P'_0(x) + \Pi(x)$$

le polynome $\Pi(x)$ étant à coefficients dans $\mathfrak{p}$. Le deuxième membre appartient à $\mathfrak{P}'$, donc le premier. On a

$$w \,.\, w'_0 \not\equiv 0\ (\mathfrak{p}), \text{ donc } w \,.\, w'_0 \not\equiv 0(\mathfrak{P}'),$$

et, comme $\mathfrak{P}'$ est premier

$$F(x)\epsilon\mathfrak{P}'$$

ce qui démontre

$$\mathfrak{P} \subseteq \mathfrak{P}'.$$

Il en résulte:

$$\mathfrak{P}' = \mathfrak{P}.$$

**2. Le théorème de transfert de $A$ à $A\ [x_1, x_2, \ldots x_n]$.** Pour démontrer qu'une propriété de l'anneau $A$ se conserve pour l'anneau $A[x_1, x_2, \ldots, x_n]$ des polynomes à $n$ variables, il suffit de montrer qu'elle s'étend à l'anneau des polynomes à une variable $A[x]$.

Nous allons supposer pour $A$ la

PROPRIÉTÉ 1. *Tout idéal $\mathfrak{i}$, différent de l'anneau $A$, admet au moins un diviseur premier $\mathfrak{p}$, différent de $A$, tel que pour tout élément $p$ de $\mathfrak{p}$, il existe au moins un entier $\rho$ et un élément $l$ associés, vérifiant*

$$p^\rho \,.\, l \equiv 0(\mathfrak{i}) \quad \text{avec} \quad l \not\equiv 0(\mathfrak{p}).$$

Indiquons d'abord deux conséquences de cette propriété.

CONSÉQUENCE 1. *Les éléments $q$ tels qu'il existe $l$ vérifiant*

$$q \,.\, l \equiv 0(\mathfrak{i}) \quad \text{avec} \quad l \not\equiv 0(\mathfrak{p})$$

*forment un idéal primaire $\mathfrak{q}$ admettant $\mathfrak{p}$ pour idéal premier associé.*

On a en effet les trois propriétés suivantes:

(1) $$\mathfrak{i} \subseteq \mathfrak{q} \subseteq \mathfrak{p}$$

(2) $$a \,.\, b \equiv 0(\mathfrak{q}) \text{ et } a \not\equiv 0(\mathfrak{q}) \text{ entrainent } b \equiv 0(\mathfrak{p}).$$

(3) Si $b \equiv 0(\mathfrak{p})$, il existe un entier $\rho$ tel que $b^\rho \equiv 0(\mathfrak{q})$.

Les deux premières s'établissent immédiatement, et la dernière est une conséquence de la propriété 1. Or ce sont là des conditions caractéristiques pour que $\mathfrak{q}$ soit primaire, avec $\mathfrak{p}$ pour idéal premier associé. ([2], p. 129, ou [7], §82, p. 33.)

CONSÉQUENCE 2. *L'idéal $\mathfrak{p}$ qui intervient dans la propriété 1 est un diviseur premier minimal pour $\mathfrak{i}$, c'est à dire*

$$\mathfrak{i} \subseteq \mathfrak{p}' \subseteq \mathfrak{p} \quad \textit{entrainent} \quad \mathfrak{p}' = \mathfrak{p}$$

*lorsque $\mathfrak{p}'$ est premier.*

En effet, supposons

$$p \equiv 0(\mathfrak{p}) \quad \text{et} \quad p \not\equiv 0(\mathfrak{p}').$$

On a

$$p^\rho . l \equiv 0(\mathfrak{i}) \quad \text{avec} \quad l \not\equiv 0(\mathfrak{p}),$$

d'où

$$p^\rho . l \equiv 0(\mathfrak{p}'),$$

et, puisque $\mathfrak{p}'$ est premier et $p \not\equiv 0(\mathfrak{p}')$,

$$l \equiv 0(\mathfrak{p}'),$$

donc

$$l \equiv 0(\mathfrak{p}),$$

ce qui est contraire à l'hypothèse.

La propriété 1 est satisfaite dans les deux exemples suivants:

EXEMPLE 1. *L'anneau $A$ est l'anneau $K[x]$ des polynomes à une variable à coefficients dans un corps $K$.*

Quand l'idéal $\mathfrak{i}$ est nul, la solution unique est $\mathfrak{p} = 0$. Quand $\mathfrak{i} \neq 0$, il n'admet qu'un nombre fini de diviseurs premiers qui vérifient tous la propriété 1.

EXEMPLE 2. *L'anneau $A$ est intersection d'un nombre fini d'idéaux primaires.*[2] Prenons

$$\mathfrak{i} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r:$$

décomposition qu'on peut supposer "normée" au sens de Krull ([4], p. 6), c'est à dire dans laquelle aucun des $\mathfrak{q}_j$ $(j = 1, 2, \ldots, r)$ n'est superflu, tandis que les idéaux premiers associés $\mathfrak{p}_j$ sont distincts, et différents de l'anneau $A$. Parmi ces $\mathfrak{p}_j$, en nombre fini, il existe au moins un idéal minimal $\mathfrak{p} = \mathfrak{p}_1$. Aucun des $\mathfrak{q}_j$ $(j \neq 1)$ n'admet $\mathfrak{p}$ pour idéal premier associé. Pour établir la propriété 1 il suffit alors d'utiliser un raisonnement classique ([7], §83, p. 38).

Soit

$$p \equiv 0(\mathfrak{p}).$$

Il existe un entier $\rho$ tel que

$$p^\rho \equiv 0(\mathfrak{q}_1).$$

$\mathfrak{p}$ étant minimal parmi les $\mathfrak{p}_j$, on peut trouver dans chaque $\mathfrak{p}_j$ $(j \neq 1)$ un élément $l_j \not\equiv 0(\mathfrak{p})$; il vérifie

$$l_j^{\rho_j} \equiv 0(\mathfrak{q}_j).$$

[2]En particulier, moyennant l'axiome du choix, quand $A$ est un anneau noetherien ([7] § 83).

Posons

$$l = \prod_{j \neq 1} l_j^{\rho_j} \not\equiv 0(\mathfrak{p}).$$

Il vient alors

$$p^{\rho} \,.\, l \equiv 0(\mathfrak{i}) \quad \text{avec} \quad l \not\equiv 0(\mathfrak{p}),$$

ce qui vérifie la propriété 1 dans l'exemple 2. Cette propriété est d'ailleurs vérifiée pour *tout* idéal $\mathfrak{p}'$ diviseur premier minimal pour $\mathfrak{i}$, car $\mathfrak{p}'$ est diviseur d'un $\mathfrak{q}_j$, soit $\mathfrak{q}$, donc d'un $\mathfrak{p}_j$, soit $\mathfrak{p}$; comme il est minimal pour $\mathfrak{i}$, on a $\mathfrak{p}' = \mathfrak{p}$, et $\mathfrak{p}$ est nécessairement minimal parmi les $\mathfrak{p}_j$. On termine alors comme plus haut.

Nous avons en vue le transfert de la propriété 1, supposée valable pour l'anneau $A$, à l'anneau $A[x]$ des polynomes à une variable. Soit $\mathfrak{J}$ un idéal dans $A[x]$, différent de $\mathfrak{R} = A[x]$. Considérons, comme au paragraphe 1, la projection

$$\mathfrak{i} = \mathfrak{J} \cap A$$

de $\mathfrak{J}$ dans l'anneau $A$. C'est un idéal $\mathfrak{i}$, différent de $A$. Par hypothèse l'idéal $\mathfrak{i}$ possède un diviseur premier $\mathfrak{p}$ qui vérifie la propriété 1. La recherche d'un diviseur premier $\mathfrak{P}$ pour $\mathfrak{J}$ est alors liée au problème suivant:

*Problème d'extension.* $\mathfrak{i}$ *et* $\mathfrak{p}$ *étant des idéaux dans* $A$ *qui satisfont la propriété* 1, $\mathfrak{J}$ *un idéal dans* $A[x]$ *qui se projette suivant* $\mathfrak{i}$ *dans* $A$, *trouver un diviseur premier* $\mathfrak{P}$ *de* $\mathfrak{J}$, *qui se projette suivant* $\mathfrak{p}$ *dans* $A$.

Les données sont $\mathfrak{J}$, $\mathfrak{i} = \mathfrak{J} \cap A$ et $\mathfrak{p}$ avec la propriété 1 pour $\mathfrak{i}$. Il faut trouver un diviseur premier $\mathfrak{P}$ de $\mathfrak{J}$ tel que $\mathfrak{P} \cap A = \mathfrak{p}$. La solution de ce problème n'est pas sans analogie avec celle de l'extension d'une spécialisation, donnée par A. Weil ([8], p. 30).

Considérons comme au paragraphe 1, l'idéal $\bar{\mathfrak{J}} = \bar{\lambda}(\mathfrak{J})$. *L'idéal* $\bar{\mathfrak{J}} = \bar{\lambda}(\mathfrak{J})$ *n'est pas l'idéal unité dans* $k[x]$. S'il était l'idéal unité, une constante non nulle serait dans $\bar{\mathfrak{J}}$ soit

$$\frac{\bar{u}'}{\bar{w}'} = \frac{\lambda F_0(x)}{\bar{w}}$$

avec

$$F_0(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathfrak{J}$$

et, puisque $\dfrac{\lambda F_0(x)}{\bar{w}}$ est une constante non nulle de $k[x]$,

$$\bar{a}_n = 0, \ldots, \bar{a}_1 = 0; \; \bar{a}_0 \neq 0$$

ou

$$a_n \equiv \ldots \equiv a_1 \equiv 0 \; (\mathfrak{p}); \; a_0 \not\equiv 0 \; (\mathfrak{p}).$$

D'après la propriété 1 appliquée à $\mathfrak{i}$ et $\mathfrak{p}$, on peut trouver des entiers $\rho_j$ et des éléments $l_j \not\equiv 0(\mathfrak{p})$, tels que

$$a_j^{\rho_j} \,.\, l_j \equiv 0(\mathfrak{i}); \; l_j \not\equiv 0(\mathfrak{p}); \; j = n, \ldots, 1.$$

https://doi.org/10.4153/CJM-1950-006-9 Published online by Cambridge University Press

Posons

$$\rho = 1 + \sum_{j=n}^{j=1} (\rho_j - 1); \ l = \prod_j l_j \not\equiv 0(\mathfrak{p}).$$

De la relation

$$a_0 = F_0(x) - a_n x^n - \ldots - a_1 x$$

on tire

$$a_0{}^\rho . l \equiv 0(\mathfrak{i}), \ l \not\equiv 0(\mathfrak{p}),$$

ce qui prouve

$$a_0 \epsilon \mathfrak{p}$$

contrairement à l'hypothèse.

Il ne reste plus pour l'idéal que deux possibilités:

$1^0$ cas. *L'idéal* $\bar{\mathfrak{J}}$ *est l'idéal nul,* c'est à dire pour tout

$$F(x) = a_n x^n + \ldots + a_0 \epsilon \mathfrak{J}$$

on a

$$\lambda F(x) = 0, \quad \text{ou} \quad \bar{a}_n = \ldots = \bar{a}_0 = 0$$

ce qui signifie

$$a_n \equiv \ldots \equiv a_0 \equiv 0(\mathfrak{p}).$$

L'idéal $\mathfrak{J}$ est donc contenu dans l'idéal $\Pi$ des polynomes de $A[x]$ qui ont leurs coefficients dans $\mathfrak{p}$.

Cet idéal $\Pi$, formé par les polynomes $F(x)$ tels que

$$\lambda F(x) = 0$$

est d'après le lemme 1, l'idéal premier unique, différent de $A[x]$, vérifiant

$$\Pi \cap A = \mathfrak{p} \quad \text{et} \quad \bar{\lambda}(\Pi) = 0.$$

C'est donc un diviseur premier de $\mathfrak{J}$, solution du problème d'extension. D'ailleurs, toute solution du problème d'extension contient $\mathfrak{p}$ donc $\Pi$.

*L'idéal* $\Pi$ *est donc la solution unique minimale du problème d'extension.*

$2^0$ cas. *L'idéal* $\bar{\mathfrak{J}}$ *n'est pas l'idéal nul.* Soit $\mathfrak{P}$ une solution du problème d'extension. L'idéal $\bar{\mathfrak{P}} = \bar{\lambda}(\mathfrak{P})$ est un diviseur premier de $\bar{\mathfrak{J}} \neq 0$. Or ces diviseurs sont en nombre fini; ils ont pour base l'un des facteurs irréductibles $\overline{\varphi_j(x)}$ de la décomposition de la base $\overline{\varphi(x)}$ de $\bar{\mathfrak{J}}$ dans $k[x]$. $(j = 1, 2, \ldots, r)$. Chacun d'eux, $\bar{\mathfrak{P}}_j$, ne correspond d'après le lemme 1 qu'à un seul idéal premier $\mathfrak{P}_j$ tel que

$$\mathfrak{P}_j \cap A = \mathfrak{p} \quad \text{et} \quad \bar{\lambda}(\mathfrak{P}_j) = \bar{\mathfrak{P}}_j.$$

$\mathfrak{P}_j$ est différent de $\mathfrak{R} = A[x]$, et il est constitué par tous les polynomes $F(x)$ tels que

$$\lambda F(x) \epsilon \bar{\mathfrak{P}}_j.$$

C'est aussi un diviseur premier de $\mathfrak{J}$, car pour tout $F(x) \epsilon \mathfrak{J}$ on a par définition

$$\lambda F(x) \epsilon \bar{\mathfrak{J}}, \ \text{donc} \ \lambda F(x) \epsilon \bar{\mathfrak{P}}_j.$$

Le problème d'extension admet, dans ce deuxième cas, $r$ *solutions* constituées par les $r$ idéaux $\mathfrak{P}_j$.

En résumé, le problème d' extension peut présenter deux cas:
$1^0$ cas. *Il existe une solution* $\Pi$ *et toute solution est un diviseur de* $\Pi$.
$2^0$ cas. *Il n'y a qu'un nombre fini de solutions constituées par les r idéaux* $\mathfrak{P}_j$.
Nous allons voir que la solution unique minimale $\Pi$ du premier cas, et chacune des solutions $\mathfrak{P}_j$ du $2^0$ cas vérifient la propriété 1 pour l'idéal $\mathfrak{J}$ dans $A[x]$.
*Dans le* $1^0$ *cas*: $\Pi$ est un diviseur premier de $\mathfrak{J}$ distinct de l'idéal unité $\mathfrak{R} = A[x]$.

Soit

$$F(x) = a_n x^n + \ldots + a_0 \equiv 0(\Pi)$$

On a donc

$$a_n \equiv \ldots \equiv a_0 \equiv 0(\mathfrak{p})$$

d'où, d'après la propriété 1 appliquée à $\mathfrak{i}$ et $\mathfrak{p}$,

$$a_j^{\rho_j} \equiv 0(\mathfrak{i}), \ l_j \not\equiv 0(\mathfrak{p}),$$

ce qui s'écrit encore

$$a_j^{\rho_j} l_j \equiv 0(\mathfrak{J}), \ l_j \not\equiv 0(\Pi).$$

En posant

$$\rho = 1 + \sum_{j=n}^{j=0} (\rho_j - 1), \ l = \prod_j l_j,$$

on obtient

$$F^\rho \, . \, l \equiv 0(\mathfrak{J}), \ l \not\equiv 0(\Pi).$$

La propriété 1 est bien vérifiée pour $\mathfrak{J}$ et son diviseur premier $\Pi$.

*Dans le* $2^0$ *cas*: Soit $P(x) \epsilon \mathfrak{P}_j = \mathfrak{P}$.

Opérons d'abord dans $k[x]$. Il existe un entier $m$ tel que

$$\overline{P}^m . \, \overline{L}_0 \equiv 0(\overline{\mathfrak{J}}), \ \overline{L}_0 \not\equiv 0(\overline{\mathfrak{P}})$$

d'après la propriété 1 valable dans $k[x]$ (exemple 1). On en déduit dans $A[x]$:

$$wL_0 P^m = F(x) + \Pi(x)$$
$$wL_0 \not\equiv 0(\mathfrak{P}), \quad F(x) \epsilon \mathfrak{J}, \quad \Pi(x) \epsilon \Pi.$$

On a vu dans le $1°$ cas qu'il existe un entier $\sigma$ et un élément $l$ tels que

$$\Pi(x)^\sigma . \, l \equiv 0 \ (\mathfrak{J}), \ \ l \not\equiv 0(\mathfrak{p}).$$

On en tire, en multipliant par $l$ l'expression $w.L_0 P^m$ élevée à la puissance $\sigma$,

$$P^{m\sigma} . \, L \equiv 0(\mathfrak{J}), \ L \not\equiv 0(\mathfrak{P}),$$

soit

$$P^\rho \, L \equiv 0(\mathfrak{J}), \ L \not\equiv 0 \ (\mathfrak{P}).$$

Ainsi se trouve démontré le théorème de transfert pour la propriété 1:

THÉORÈME 1. *Quand la propriété* 1 *est valable pour l'anneau* $A$, *elle s'étend à l'anneau* $A[x_1, x_2, \ldots, x_n]$ *des polynomes à* $n$ *variables.*

En particulier, d'après l'exemple 1,

THÉORÈME 2. *Tout idéal* $\mathfrak{J}$ *dans l'anneau* $K[x_1, \ldots, x_n]$ *des polynomes à* $n$ *variables à coefficients dans un corps* $K$ *admet au moins un diviseur premier*

https://doi.org/10.4153/CJM-1950-006-9 Published online by Cambridge University Press

$\mathfrak{P}$, *différent de l'idéal unité, et tel que pour tout polynome $P$ de $\mathfrak{P}$, on puisse trouver un entier $\rho$ et un polynome $L$ vérifiant*

$$P^\rho . L \equiv 0(\mathfrak{J}), \; L \not\equiv 0(\mathfrak{P}).$$

**3. Le théorème des zéros de Hilbert.** $K$ étant un corps quelconque, le théorème des zéros de Hilbert s'énonce ainsi:

THÉORÈME 3. *Quand un polynome $f \epsilon K[x_1, \ldots, x_n]$ s'annule pour tous les zéros algébriques d'un idéal $\mathfrak{J}$, il existe un entier $\rho$ tel que $f^\rho \epsilon \mathfrak{J}$.*

La méthode de A. Rabinowitsch [6] exposée par B. L. van der Waerden ([7], §75, p. 11) ramène la démonstration de ce théorème au suivant:

THÉORÈME 4. *Dans l'anneau des polynomes $K[x_1, \ldots, x_n]$, un idéal qui n'a aucun zéro algébrique sur $K$ est nécessairement l'idéal unité.*

Ou encore, un idéal $\mathfrak{J} \neq \mathfrak{R}$ possède toujours au moins un zéro algébrique sur $K$.

Pour établir le théorème 4, il suffit de le démontrer pour le diviseur premier $\mathfrak{P} \neq \mathfrak{R}$ dont l'existence est assurée par le théorème 2. Nous allons démontrer le théorème suivant, plus précis:

THÉORÈME 5. *Un idéal premier $\mathfrak{P}$ dans $K[x_1, \ldots, x_n]$ qui n'a aucun zéro algébrique sur $K$, est nécessairement l'idéal unité. De plus, un polynome $f$ qui s'annule pour tout zéro algébrique d'un idéal premier $\mathfrak{P}$ appartient nécessairement à $\mathfrak{P}$.*

Autrement dit, il existe toujours un zéro algébrique sur $K$ d'un idéal premier $\mathfrak{P}$ différent de $\mathfrak{R}$. De plus, si

$$f(x_1, x_2, \ldots, x_n) \not\equiv 0(\mathfrak{P})$$

on peut choisir ce zéro $(x'_1, x'_2, \ldots, x'_n)$ de façon que

$$f(x'_1, x'_2, \ldots, x'_n) \neq 0.$$

C'est sous cette forme que nous allons établir le théorème, par induction sur le nombre des variables. Nous n'aurons besoin pour cela que des remarques préliminaires du paragraphe 1.

Le cas $n = 1$ est bien connu. Supposons le théorème établi dans l'anneau $A = K[x_1, \ldots, x_{n-1}]$ et démontrons le dans l'anneau $A[x_n] = A[x] = K[x_1, \ldots, x_n]$. Soit

$$\mathfrak{p} = \mathfrak{P} \cap A \neq A,$$

la projection de $\mathfrak{P}$ dans $A$. D'après le lemme 1, l'idéal $\mathfrak{P}$ est complètement déterminé par $\mathfrak{p}$ et par

$$\bar{\mathfrak{P}} = \bar{\lambda}(\mathfrak{P}).$$

1°) $\bar{\mathfrak{P}} = 0$. L'idéal $\mathfrak{P}$ coincide avec l'idéal $\Pi$ des polynomes

$$F = a_n x^n + \ldots + a_0$$

à coefficients $a_n, \ldots, a_0$ dans $\mathfrak{p}$. Tout zéro algébrique de $\mathfrak{p}$ est alors zéro de $\mathfrak{P}$, quel que soit $x$. De plus, si

$$f = a_m x^m + \ldots + a_d x^d + \ldots + a_0 \not\equiv 0(\mathfrak{P})$$

https://doi.org/10.4153/CJM-1950-006-9 Published online by Cambridge University Press

l'un de ses coefficients n'est pas dans $\mathfrak{p}$; soit $a_d$ le premier coefficient non dans $\mathfrak{p}$. Quand $d = 0$, on a $a_0 \not\equiv 0(\mathfrak{p}),\ a_j \equiv 0(\mathfrak{p}).$ $(j > 0)$
On peut alors trouver un zéro algébrique de $\mathfrak{p}$, soit $(x'_1, x'_2, \ldots, x'_{n-1})$, tel que

$$a_0(x'_1, \ldots, x'_{n-1}) \neq 0.$$

Alors $(x'_1, x'_2, \ldots, x'_{n-1}, x'_n)$ est un zéro algébrique de $\mathfrak{P}$ dès que $x'_n$ est algébrique sur $K$, et on a pour ce zéro:

$$f(x'_1, \ldots, x'_n) \neq 0.$$

Quand $d > 0$, on choisit un zéro algébrique $(x'_1, \ldots, x'_{n-1})$ de $\mathfrak{p}$ tel que

$$a'_d = a_d(x'_1, \ldots, x_{n-1}) \neq 0,$$

puis pour $x_n$ un nombre algébrique sur $K$, distinct des racines de l'équation

$$a'_d x^d + \ldots + a'_0 = 0.$$

Cela est toujours possible car il y a toujours une infinité de nombres algébriques sur $K$. On obtient un zéro $(x'_1, \ldots, x'_{n-1}, x'_n)$ de $\mathfrak{P}$, algébrique sur $K$, tel que

$$f(x'_1, \ldots, x'_n) \neq 0.$$

2°) $\mathfrak{P} \neq 0$. On peut prendre la base de $\overline{\mathfrak{P}}$ sous la forme $\lambda\Psi(x) \neq 0$ avec

$$\Psi(x) = a_d x^d + \ldots + a_0 \in \mathfrak{P} \quad .$$

et

$$a_d \not\equiv 0(\mathfrak{p}),\ d > 0.$$

Tout polynome $F(x) \epsilon A[x]$ peut être divisé par $\Psi(x)$ pour donner dans $A[x]$:

$$a_d^{\rho} F = Q \,.\, \Psi + R, \qquad d^0 R < d.$$

Si $F(x)$ est pris dans $\mathfrak{P}$, $\lambda R \epsilon \overline{\mathfrak{P}}$ car $\lambda\Psi\epsilon\overline{\mathfrak{P}}$.
On obtient alors

$$\lambda R = 0 \quad \text{ou} \quad R \epsilon \Pi$$

sans quoi le degré de $\lambda R$ serait inférieur au degré $d$ de la base $\lambda\Psi$ de $\overline{\mathfrak{P}}$. Donc, pour tout polynome $P \epsilon \mathfrak{P}$ il existe $a_d$ et $\Psi(x)$, fixes, et $\rho$, $Q(x)$, $\Pi(x)$ variables avec $P$, tels que

(1) $$a_d^{\rho} P(x) = Q(x) \,.\, \Psi(x) + \Pi(x), \quad a_d \not\equiv 0(\mathfrak{p}).$$

Soit

$$f(x_1, x_2, \ldots, x_n) \not\equiv 0(\mathfrak{P}).$$

Donc, dans $k[x]$, le polynome $\bar{f} = \lambda f$ est non multiple de $\overline{\Psi} = \lambda\Psi$, par suite premier avec lui. On peut alors écrire dans $k[x]$

$$1 = k_1(x) \,.\, \bar{f} + k_2(x) \,.\, \overline{\Psi},$$

ce qui donne dans $A[x] = K[x_1, \ldots, x_n]$

(2) $$w = U \,.\, f + V \,.\, \Psi + \Pi(x)$$

où $w$ est dans $A$ mais non dans $\mathfrak{p}$, tandis que $\Pi(x)$ est à coefficients dans $\mathfrak{p}$.

On peut trouver un zéro de $\mathfrak{p}$, algébrique sur $K$, soit $x'_1, \ldots, x'_{n-1}$, qui n'annule pas $w \,.\, a_d \not\equiv 0(\mathfrak{p})$. Il est donc tel que

$$w' \neq 0 \quad \text{et} \quad a'_d \neq 0.$$

Prenons pour $x_n = x$ une racine de

$$a'_d x^d + \ldots + a'_0 = 0.$$

On obtient, d'après (1), un zéro $(x'_1, \ldots, x'_n)$ de $\mathfrak{P}$, algébrique sur $K$, et ce zéro, d'après (2), ne peut annuler $f$:

$$f(x'_1, \ldots, x'_n) \neq 0.$$

Le théorème 5 est démontré, ainsi que le théorème des zéros de Hilbert.

Des démonstrations du théorème des zéros de Hilbert se trouvent aussi dans O. Zariski [9], qui suppose connue l'existence d'un idéal maximal, diviseur d'un idéal donné; cette affirmation nécessite l'axiome du choix; (cf. N. Bourbaki, traité de Mathématiques, *Algèbre*, chap. 1, §8, n°. 7). La démonstration exposée dans le traité de van der Waerden ([7], p. 10), utilise la théorie de l'élimination. Il existe aussi une démonstration élémentaire de R. Brauer [1].

**4. Décomposition d'un idéal dans $K[x_1, \ldots, x_n]$ en idéaux primaires.** L'hypothèse de la base finie dans un anneau $A$ entraine comme on le sait la propriété des "chaines de diviseurs, "([2] p. 134, ou [7] p. 26), qui exprime qu'une suite non décroissante d'idéaux

$$\mathfrak{J}_1 \subseteq \mathfrak{J}_2 \subseteq \ldots \subseteq \mathfrak{J}_k \subseteq \mathfrak{J}_{k+1} \subseteq \ldots$$

est stationnaire à partir d'un certain rang $k$.

$$\mathfrak{J}_k = \mathfrak{J}_{k+j} \quad \text{pour tout } j > 0.$$

La propriété I, au §2, a pour conséquence (conséquence I): les éléments $Q$ tels qu'il existe un élément $L$ vérifiant

$$Q \,.\, L \equiv 0(\mathfrak{J}), \quad L \not\equiv 0(\mathfrak{P})$$

forment un idéal primaire $\mathfrak{Q}$ admettant $\mathfrak{P}$ pour idéal premier associé.

On a évidemment

$$\mathfrak{J} \subseteq \mathfrak{Q} \subseteq \mathfrak{P}.$$

Il est possible de préciser dans *l'hypothèse de la base finie.*

LEMME 2. *L'idéal $\mathfrak{J}$ est alors l'intersection de l'idéal primaire $\mathfrak{Q}$ et d'un idéal,*

$$\mathfrak{J} + (M)$$

*qui n'admet plus $\mathfrak{P}$ comme diviseur premier.*

$(M)$ désigne l'idéal principal de base $M$, et $\mathfrak{J}+(M)$ l'idéal ayant pour base l'ensemble constitué par la base de $\mathfrak{J}$ et par $M$.

Soit

$$\mathfrak{Q} = (Q_1, \ldots, Q_s).$$

Il existe pour chaque $Q_j (j = 1, 2, \ldots, s)$, un élément $L_j \not\equiv (\mathfrak{P})$ tel que

$$Q_j L_j \equiv 0(\mathfrak{J}).$$

https://doi.org/10.4153/CJM-1950-006-9 Published online by Cambridge University Press

On a donc, en posant $L = \prod_j L_j$,

$$\mathfrak{Q} \,.\, L \equiv 0(\mathfrak{J}) \quad \text{avec} \quad L \not\equiv 0(\mathfrak{P}).$$

D'autre part, d'après un raisonnement connu ([7] §82, p. 36) la propriété des chaines de diviseurs entraine l'existence d'un entier $K$ tel que[3]

$$\mathfrak{J} : L^k = \mathfrak{J} : L^{k+1}.$$

Posons $L^k = M \not\equiv 0(\mathfrak{P})$; nous allons montrer que

$$\mathfrak{J} = \mathfrak{Q} \cap (\mathfrak{J} + (M)).$$

$\mathfrak{J}$ est évidemment inclus dans l'intersection de $\mathfrak{Q}$ et de $\mathfrak{J} + (M)$. Réciproquement, soit $c$ un élément de cette intersection:

$$c = a + bL^k \quad \text{avec } a \epsilon \mathfrak{J}.$$

$c$ appartenant à $\mathfrak{Q}$, on a

$$cL \epsilon \mathfrak{J} \quad \text{d'où} \quad bL^{k+1} \epsilon \mathfrak{J}.$$

Par suite

$$b \epsilon \mathfrak{J} : L^{k+1} = \mathfrak{J} : L^k.$$

Donc

$$bL^k \epsilon \mathfrak{J}$$

et

$$c \epsilon \mathfrak{J}.$$

Le lemme 2 s'applique naturellement à l'anneau $K[x_1, \ldots, x_n]$, d'après le théorème de la base finie de Hilbert, et d'après le théorème 2.

Il suffit pour établir la décomposition en idéaux primaires de tout idéal dans $K[x_1, \ldots, x_n]$. En effet, si l'idéal

$$\mathfrak{J}_1 = \mathfrak{J} + (M) \supset \mathfrak{J}$$

n'est pas l'idéal unité, il admet d'après le théorème 2 un diviseur premier $\mathfrak{P}_1 \neq \mathfrak{R}$ auquel le lemme 2 s'applique. On forme

$$\mathfrak{J}_2 = \mathfrak{J}_1 + (M_1) \supset \mathfrak{J}_1.$$

L'opération prend fin après un nombre fini $k$ d'opérations; car en la poursuivant indéfiniment on formerait une chaine infinie d'idéaux

$$\mathfrak{J} \subset \mathfrak{J}_1 \subset \mathfrak{J}_2 \subset \ldots \subset \mathfrak{J}_k \subset \ldots$$

ce qui est contraire à la propriété des chaines de diviseurs. L'idéal $\mathfrak{J}_{k+1}$ est donc l'idéal unité, et on a

$$\mathfrak{J} = \mathfrak{Q} \cap \mathfrak{Q}_1 \cap \ldots \cap \mathfrak{Q}_k.$$

La démonstration suivante, plus longue, il est vrai, révèle mieux, à ce qu'il me semble, la structure des idéaux de polynomes à coefficients dans un corps $K$. Elle parait plus adaptée à l'étude des variétés algébriques.

D'autre part elle dispense de l'axiome du choix, sous la forme restreinte utilisée dans la démonstration précédente comme dans la démonstration de E. Noether. ([7] §83.)

---

[3]On forme la chaine de diviseurs:

$$\mathfrak{Q} = \mathfrak{J} : L \subseteq \mathfrak{J} : L^2 \subseteq \ldots \subseteq \mathfrak{J} : L^k \subseteq \mathfrak{J} : L^{k+1} \subseteq \ldots$$

Une notion importante dans $K[x_1, \ldots, x_n]$, est celle de dimension d'un idéal premier $\mathfrak{P}$; soient $\xi_1, \ldots, \xi_n$ les classes de $x_1, \ldots, x_n$ modulo $\mathfrak{P}$.

L'anneau $K[x_2, \ldots, x_n]/\mathfrak{P}$ est un domaine d'intégrité dont le corps des quotients est

$$K(\xi_1 \ldots, \xi_n).$$

La dimension de $\mathfrak{P}$ est alors la dimension sur $K$ du corps $K$ $(\xi_1, \ldots, \xi_n)$. C'est le nombre maximum d'éléments algébriquement indépendants sur $K$ parmi les $\xi_j (j = 1, 2, \ldots, n)$. Rappelons la propriété suivante concernant les dimensions: ([7], §90, p. 63 ou [8] chap. II, th. 3, p. 28).

LEMME 3. *Soit $\mathfrak{P}$ un idéal premier dans $\mathfrak{R} = K[x_1, \ldots, x_n]$, différent de $\mathfrak{R}$, et de dimension $d$. Soit $\mathfrak{P}'$ un diviseur premier de $\mathfrak{P}$, différent de $\mathfrak{R}$, de dimension $d'$. On a*

$$d' \leqslant d$$

*et l'égalité n'a lieu que si $\mathfrak{P}' = \mathfrak{P}$.*

Maintenant, la préparation du théorème suivant est suffisante:

THÉORÈME 6. *Tout idéal $\mathfrak{J}$ dans l'anneau des polynomes $\mathfrak{R} = K[x_1, \ldots, x_n]$ est intersection d'un nombre fini d'idéaux primaires.*

Si $\mathfrak{J}$ remplit $\mathfrak{R}$, il est premier, donc primaire. Nous pouvons donc supposer $\mathfrak{J} \neq \mathfrak{R}$. Le raisonnement s'effectue par induction sur le nombre des variables.

Le cas $n = 1$ est bien connu. Supposons alors le théorème valable dans $K[x_1, \ldots, x_{n-1}] = A$ et considérons la projection de $\mathfrak{J}$ dans $A$:

$$\mathfrak{i} = \mathfrak{J} \cap A.$$

C'est une intersection d'idéaux primaires

$$\mathfrak{i} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_t$$

chaque $\mathfrak{q}_j$ ayant pour idéal premier associé $\mathfrak{p}_j$. Les $\mathfrak{p}_j$ de dimension maximum $d$ $(0 \leqslant d \leqslant n - 1)$ sont nécessairement minimaux pour $\mathfrak{i}$, car si $\mathfrak{p}$ est l'un de ces idéaux, un diviseur premier $\mathfrak{p}'$ tel que

$$\mathfrak{i} \subseteq \mathfrak{p}' \subseteq \mathfrak{p}$$

serait diviseur d'un $\mathfrak{p}_j$ (cf. exemple 2); sa dimension, d'après le lemme 3, serait supérieure ou égale à celle de $\mathfrak{p}$ et inférieure ou égale à celle de $\mathfrak{p}_j$; comme la dimension de $\mathfrak{p}_j$ ne peut dépasser celle de $\mathfrak{p}$, l'égalité est obligatoire, ce qui entraine d'après le lemme 3

$$\mathfrak{p}' = \mathfrak{p}.$$

$\mathfrak{p}$ étant minimal pour $\mathfrak{i}$, nous avons vu (exemple 2) que ces deux idéaux vérifient la propriété 1. Le problème d'extension concernant $\mathfrak{i}$, $\mathfrak{p}$ et $\mathfrak{J}$ se traite alors avec succès. Deux cas peuvent se présenter, d'après l'étude faite au paragraphe 2.

1°) *Il n'y a qu'un nombre fini de solutions $\mathfrak{P}_1, \ldots, \mathfrak{P}_j$ qui se projettent suivant $\mathfrak{p}$.*

(C'etait le deuxième cas envisagé au paragraphe 2.)

Prenons l'idéal $\mathfrak{P}_1$ et soit $\mathfrak{Q}_1$ l'idéal primaire correspondant. On a (lemme 2):

$$\mathfrak{J} = \mathfrak{Q}_1 \cap (\mathfrak{J} + (M_1);$$

aucun des $\mathfrak{P}_j$ $(j = 2, \ldots, r)$ n'est diviseur de $\mathfrak{Q}_1$, car ils sont tous minimaux pour $\mathfrak{J}$, donc pour $\mathfrak{Q}_1$ ou pour $\mathfrak{J} + (M_1) = \mathfrak{J}_1$ et le seul diviseur premier minimal de $\mathfrak{Q}_1$ est $\mathfrak{P}_1$. Chacun des $\mathfrak{P}_j (j \geqslant 2)$ doit donc être diviseur premier minimal pour l'idéal $\mathfrak{J}_1$. D'ailleurs, tout diviseur premier de $\mathfrak{J}_1$ qui se projette suivant $\mathfrak{p}$ est nécessairement diviseur premier de $\mathfrak{J}$ ayant $\mathfrak{p}$ pour projection dans $A$; il coïncide avec l'un des $\mathfrak{P}_j (j \geqslant 2)$. Posons

$$\mathfrak{i}_1 = \mathfrak{J}_1 \cap A.$$

Des relations

$$\mathfrak{J} \subseteq \mathfrak{J}_1 \subseteq \mathfrak{P}_2$$

on tire en projetant dans $A = K[x_1, \ldots, x_{n-1}]$:

$$\mathfrak{i} \subseteq \mathfrak{i}_1 \subseteq \mathfrak{p}.$$

$\mathfrak{p}$ est donc diviseur premier de $\mathfrak{i}_1$, minimal pour $\mathfrak{i}_1$ puisqu'il l'est pour $\mathfrak{i}$. Il vérifie pour $\mathfrak{i}_1$ la propriété 1 (exemple 2). Le problème d'extension traité pour $\mathfrak{i}_1$, $\mathfrak{p}$ et $\mathfrak{J}_1$ donne nécessairement pour solutions $\mathfrak{P}_2, \ldots, \mathfrak{P}_r$. Considérons $\mathfrak{P}_2$ et l'idéal primaire associé $\mathfrak{q}'_2$. Le lemme 2 donne

$$\mathfrak{J}_1 = \mathfrak{Q}'_2 \cap (\mathfrak{J}_1 + (M_2)), \qquad M_2 \not\equiv 0(\mathfrak{P}_2).$$

D'où en posant

$$\mathfrak{J}_2 = \mathfrak{J}_1 + (M_2)$$

il vient

$$\mathfrak{J} = \mathfrak{Q}_1 \cap \mathfrak{Q}'_2 \cap \mathfrak{J}_2,$$

et comme

$$\mathfrak{J} \subseteq \mathfrak{Q}_2 \subseteq \mathfrak{Q}'_2$$

on a aussi

$$\mathfrak{J} = \mathfrak{Q}_1 \cap \mathfrak{Q}_2 \cap \mathfrak{J}_2$$

avec

$$\mathfrak{J}_2 = \mathfrak{J} + (M_1) + (M_2).$$

On démontre, comme on l'a fait pour $\mathfrak{J}_1$, que l'idéal $\mathfrak{J}_2$ admet comme diviseurs premiers qui se projettent suivant $\mathfrak{p}$ dans $A$, les idéaux, $\mathfrak{P}_2, \ldots, \mathfrak{P}_r$, et qu'il n'admet que ceux là . On arrive ainsi de proche en proche à la décomposition

$$\mathfrak{J} = \mathfrak{Q}_1 \cap \mathfrak{Q}_2 \cap \ldots \cap \mathfrak{Q}_r \cap \mathfrak{A}$$

avec

$$\mathfrak{A} = \mathfrak{J} + (M_1) + \ldots + (M_r) \qquad\qquad M_j \not\equiv 0(\mathfrak{P}_j)$$

et

$$\mathfrak{a} = \mathfrak{A} \cap A \not\equiv 0(\mathfrak{p})$$

car si $\mathfrak{a} \subseteq \mathfrak{p}$, les solutions du problème d'extension pour $\mathfrak{a}$, $\mathfrak{p}$ et $\mathfrak{A}$ seraient à choisir parmi les $\mathfrak{P}_j$, dont aucun ne convient.

2°) *La solution minimale du problème d'extension est l'idéal* $\Pi$ *des polynomes* $F(x)$ *dont les coefficients dans* $A$ *appartiennent à* $\mathfrak{p}$.

https://doi.org/10.4153/CJM-1950-006-9 Published online by Cambridge University Press

Le lemme 2 donne

$$\mathfrak{J} = \mathfrak{Q} \cap \mathfrak{J}',$$

$\mathfrak{Q}$ étant l'idéal primaire correspondant à $\Pi$, avec

$$\mathfrak{J}' = \mathfrak{J} + (M), \qquad M \not\equiv 0(\Pi).$$

La projection

$$\mathfrak{i}' = \mathfrak{J}' \cap A$$

de $\mathfrak{J}'$ dans $A$ peut encore admettre $\mathfrak{p}$ comme diviseur premier, nécessairement minimal. Le problème d'extension traité pour $\mathfrak{i}'$, $\mathfrak{J}'$ et $\mathfrak{p}$ donne alors une ou plusieurs solutions minimales diviseurs premiers de $\Pi$, mais il ne peut rentrer dans le même type que le problème concernant $\mathfrak{i}$, $\mathfrak{J}$ et $\mathfrak{p}$ car sa solution minimale serait $\Pi$ ce qui est impossible puisque $M \not\equiv 0(\Pi)$, et par suite $\mathfrak{J}' \not\equiv 0(\Pi)$. Il rentre alors dans le type traité précédemment, ce qui permet d'écrire

$$\mathfrak{J} = \mathfrak{Q} \cap \mathfrak{Q}_1 \cap \ldots \cap \mathfrak{Q}_j \cap \mathfrak{A}.$$

Les idéaux $\mathfrak{Q}$, $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_r$ sont primaires et leurs idéaux premiers se projettent dans $A$ suivant $\mathfrak{p}$, l'idéal $\mathfrak{A}$ se projette dans $A$ suivant un idéal $\mathfrak{a}$ n'admettant plus $\mathfrak{p}$ pour diviseur premier.[4] Les diviseurs premiers de $\mathfrak{a}$ ayant la dimension $d$ sont nécessairement minimaux pour $\mathfrak{a}$ car se sont des diviseurs premiers minimaux de $\mathfrak{i}$. Ils sont en nombre fini; on les épuise par la méthode précédente en raisonnant sur $\mathfrak{A}$ au lieu de $\mathfrak{J}$. On met ainsi $\mathfrak{J}$ sous la forme:

$$\mathfrak{J} = \mathfrak{J}_d \cap \mathfrak{F}$$

où $\mathfrak{J}_d$ est l'intersection d'idéaux primaires dont les projections dans $A$ appartiennent à des idéaux premiers de dimension $d$, et $\mathfrak{F}$ un idéal dont la projection dans $A$ n'admet aucun diviseur premier de dimension supérieure ou égale à $d$.

Dans la deuxième étape, on se débarrasse en raisonnant sur $\mathfrak{F}$, des diviseurs premiers de sa projection dont la dimension est $d - 1$. Et ainsi de suite, après chaque étape la dimension des diviseurs premiers de la projection descend. On arrive, si l'idéal unité n'a pas été rencontré en chemin, à une projection dont les diviseurs premiers sont de dimension zéro, donc tous minimaux. On s'en débarrasse de la même façon; il reste un idéal sans diviseur premier minimal, c'est à dire l'idéal unité. Par suite

$$\mathfrak{J} = \mathfrak{J}_d \cap \mathfrak{J}_{d-1} \cap \ldots \cap \mathfrak{J}_0,$$

l'idéal $\mathfrak{J}_h$ rassemblant l'intersection des idéaux primaires en nombre fini, dont les projections dans $A$ ont des diviseurs premiers associés de dimension $h$.

Les théorèmes d'unicité sur la décomposition s'établissent ensuite par la méthode classique, sans utiliser l'axiome du choix (van der Waerden [7], §84, pp. 39-43).

[4]Les diviseurs premiers minimaux de $\mathfrak{a}$ comprennent en particulier les diviseurs premiers minimaux de $\mathfrak{i}$ distincts de $\mathfrak{p}$, car si $\mathfrak{p}'$ est l'un de ces diviseurs il donne naissance à des diviseurs premiers minimaux de $\mathfrak{J}$ qui sont diviseurs premiers minimaux de $\mathfrak{Q}$ ou $\mathfrak{Q}_j$ $(j = 1, 2, \ldots, r)$ ou $\mathfrak{A}$. Ils ne peuvent l'être pour $\mathfrak{Q}$ ou $\mathfrak{Q}_j$ car ils coïncideraient avec $\pi$ ou $\mathfrak{Q}_j$. Leur projection dans $A$ serait $\mathfrak{p}$ au lieu de $\mathfrak{p}'$.

## References

[1] R. Brauer, "A Note on Hilbert's Nullstellensatz," *Bull. Amer. Math. Soc.*, vol. 54 (1948), 894-896.

[2] P. Dubreil, Algèbre, tome I (Gauthier-Villars, 1946).

[3] D. Hilbert, "Über die Theorie der algebraischen Formen," *Math. Ann.*, vol. 36 (1890), 473.

[4] W. Krull, *Idealtheorie* (Ergebnisse der Math., IV, 3, 1935).

[5] E. Lasker, "Zur Theorie der Moduln und Ideale," *Math. Ann.*, vol. 60 (1905), 20, 116.

[6] A. Rabinowitsch, *Math. Ann.*, vol. 102 (1929), 518.

[7] B. L. van der Waerden, *Moderne Algebra*, tome II (Grundl. der Math. Wissensch., vol. 34. Berlin, 1931).

[8] A. Weil, *Foundations of Algebraic Geometry* (Amer. Math. Soc. Colloq. Publications, vol. 29, 1946).

[9] O. Zariski, "A New Proof of Hilbert's Nullstellensatz," *Bull. Amer. Math. Soc.*, vol. 53 (1947), 362-368.

*Tours, France*