Jan Mařík

La réductibilité du déterminant ayant des indéterminées pour éléments, si l'on le considere comme un polynôme sur an anneau commutatif

Acta Fac. Nat. Univ. Carol., Prague 1949, (1949). no. 191, 11 pp.

Persistent URL: `http://dml.cz/dmlcz/502085`

SPISY
VYDÁVANÉ
PŘÍRODOVĚDECKOU FAKULTOU
UNIVERSITY KARLOVY

ACTA
FACULTATIS
RERUM NATURALIUM
UNIVERSITATIS CAROLINAE

S. PRÁT
CURAVIT

1949. ČÍSLO 191.

Jan Mařík:

LA RÉDUCTIBILITÉ DU DÉTERMINANT AYANT DES INDÉTERMINÉES POUR ÉLÉMENTS, SI L'ON LE CONSIDÈRE COMME UN POLYNÔME SUR UN ANNEAU COMMUTATIF

PŘÍRODOVĚDECKÁ FAKULTA UNIVERSITY KARLOVY
FACULTAS RERUM NATURALIUM UNIVERSITATIS CAROLINAE,
VINIČNÁ 5, PRAHA II.
NA SKLADĚ MÁ
PŘÍKOPY 20, PRAHA II. F. ŘIVNÁČ PŘÍKOPY 20, PRAHA II.

Considérons d'abord le déterminant

$$D = \begin{vmatrix} x_{11}, & x_{12}, & \ldots, & x_{1n} \\ x_{21}, & x_{22}, & \ldots, & x_{2n} \\ x_{n1}, & x_{n2}, & \ldots, & x_{nn} \end{vmatrix},$$

dont les éléments x_{ik} sont algébriquement indépendents sur un champ d'integrité commutatif I. Dans la démonstration du fait que D est un polynôme irréductible sur I, on se sert du théorème que le degré du produit de deux polynômes est égal à la somme des degrés de ces deux facteurs. Ce théorème n'est pas vrai pour les anneaux qui contiennent des diviseurs de zéro; dans le seminaire de prof. Kořínek, on a posé cette question: Est-il possible que le déterminant D soit réductible, si l'on le considère comme un polynôme sur un anneau commutatif ayant l'élément un?

La réponse est contenue dans le

Théorème principal. *Soit O un anneau commutatif avec l'élément un. Pour que le déterminant D, considéré comme un polynôme dans les éléments x_{ik} algébriquement indépendents sur O, soit réductible, il faut et il suffit que O soit la somme directe de deux anneaux.*

Dans ce théorème on emploie la notion de la réductibilité d'un polynôme au sens de la divisibilité dans l'anneau $P = O[x_{11}, x_{12}, \ldots, x_{nn}]$. Un polynôme est dit réductible, s'il est le produit de deux facteurs dont aucun n'est unité dans l'anneau P. La définition ordinaire de la réductibilité est différente. Un polynôme est dit réductible au sens ordinaire, s'il est le produit de deux facteurs, dont chacun est un polynôme du degré au moins égal à un.

La démonstration du théorème principal est l'objet du présent travail. Il est clair, si O est la somme directe des anneaux O_1, O_2 et si l'on a $j_i \in O_i$ et f_i, $g_i \in O_i[x_{11}, x_{12}, \ldots, x_{nn}]$ tels que $j_1 + j_2 = 1$, $f_i \cdot g_i = j_i$ (par exemple $f_i = g_i = j_i$), où $i = 1, 2$, qu'on a aussi

$$D = (f_1 + f_2 D) \cdot (g_2 + g_1 D).$$

Dans la partie II de ce travail je montre qu'on obtient ainsi toutes les décompositions de D, ce qui entraîne facilement le théorème principal. Dans la partie I je détermine les unités, les idempotents et le radical de P, en supposant que l'anneau O soit connu.

Partie I.

Soit O un anneau commutatif avec l'élément un, désigné par 1. Si l'on désigne de plus par 0 l'élément zéro, on a $b + 0 = b$, $b \,.\, 1 = b$ pour tout $b \in O$. Un élément c est dit une unité, s'il existe un d tel que $cd = 1$.

On dit que b est un nilpotent, s'il existe un nombre naturel m tel que $b^m = 0$. Les relations $b^m = 0$, $c^n = 0$, $b^k \,.\, c^l \neq 0$ entraînent celles-ci: $k \leqq m - 1$, $l \leqq n - 1$, $k + l \leqq m + n - 2$; on a alors

$$(b + c)^{m+n-1} = \sum_{k+l=m+n-1} \binom{m+n-1}{k} b^k \,.\, c^l = 0,$$

car tous les termes de la somme sont zéro. On a aussi $(bd)^m = b^m \,.\, d^m = 0$ pour tout d. Donc l'ensemble de tous les nilpotents est un idéal, qui est dit le radical; nous le désignons par $\mathfrak{r}$. On dit que O est un anneau sans radical ou que O n'a pas de radical, si $\mathfrak{r}$ ne contient aucun élément différent de zéro. Si l'on a $b^m \equiv 0 \bmod \mathfrak{r}$, il existe un $c \in \mathfrak{r}$ tel que $b^m = c$ et on peut déterminer un nombre naturel n tel que $0 = c^n = b^{mn}$, d'où $b \equiv 0 \bmod \mathfrak{r}$. Donc l'anneau $O/\mathfrak{r}$ n'a pas de radical.

Un élément j est dit un idempotent, si l'on a $j^2 = j$ (et par suite, $j^n = j$ pour tout nombre naturel n). Soit $k = 1 - j$. On a $jk = j - j^2 = 0$, $k^2 = k - kj = k$; k est alors en même temps un idempotent. Soient (j), (k) les ideaux engendrés par j, k dans O. Si l'on a $bj = ck$, on a aussi $0 = bjk = ck^2 = ck = bj$, donc zéro est le seul élément contenu à la fois dans (j) et (k). Soit $j \neq 0 \neq k$; on a $O = (j) \dotplus (k)$. j (resp. k) est évidemment l'élément un de l'anneau (j) (resp. (k)). Soit inversement $O = O_1 \dotplus O_2$; on a $j \in O_1$, $k \in O_2$ tels que $1 = j + k$, $0 = jk$, d'où $j^2 = j$, $k^2 = k$, et $j \neq 0 \neq k$. Ayant trouvé tous les idempotents, on a trouvé aussi toutes les décompositions de O en somme directe, et réciproquement.

Soient $x_1, x_2, \ldots, x_N$ algébriquement indépendents sur O. Soit $P_N = O[x_1, x_2, \ldots, x_N]$; désignons par $\mathfrak{R}_N$ le radical de P_N. Cette partie contient la démonstration des théorèmes suivants:

Théorème 1. *Chaque classe idempotente de $O/\mathfrak{r}$ contient un et seulement un élément idempotent de O.*

Théorème 2. $\mathfrak{R}_N = \mathfrak{r}[x_1, x_2, \ldots, x_N]$.

Théorème 3. *Pour qu'un polynôme $f \in P_N$ soit une unité de P_N, il faut et il suffit que le terme absolu de f (le terme du degré zéro) soit une unité de O et que tous les autres coefficients appartiennent à $\mathfrak{r}$.*

Théorème 4. *Tous les idempotents de P_N appartiennent à O.*

Nous démontrons ces théorèmes à l'aide de quelques lemmes.

Lemme 1. *Si b est une unité de O et si $r \in \mathfrak{r}$, $b + r$ est aussi une unité de O.*

Démonstration: Il existe un $c \in O$ et un nombre naturel n tels que $bc = 1$, $r^n = 0$. Posons $s = -r$. On a $1 = b^n \,.\, c^n = (b^n - s^n) \,.\, c^n = (b - s) \,.\, (b^{n-1} + \ldots + s^{n-1}) \,.\, c^n$; $b - s = b + r$ est donc une unité.

Lemme 2. *Si b est une unité de $O/\mathfrak{r}$, b est aussi une unité de O.*

Démonstration: Il existe un c tel que $bc \equiv 1 \mod \mathfrak{r}$, par suite, $bc = 1 + r$, où $r \in \mathfrak{r}$. D'après le lemme 1, $1 + r$ est une unité de O, il existe alors un d tel que $1 = d(1 + r) = b(cd)$. Donc b est une unité de O.

Démonstration du théorème 1. Soit $b^2 \equiv b \mod \mathfrak{r}$. Soit $c = 1 - b$. On a

$$b + c \equiv 1, \; c^2 \equiv c, \; bc \equiv 0 \mod \mathfrak{r}.$$

Il existe un n tel que

$$b^n \,.\, c^n = 0 \tag{α}$$

et, comme $b^n \equiv b$, $c^n \equiv c$,

$$b^n + c^n \equiv 1. \tag{β}$$

D'après le lemme 2, $b^n + c^n$ est une unité de O, donc on a un d tel que

$$1 = db^n + dc^n. \tag{γ}$$

D'après (β), on a $1 \equiv d(b^n + c^n) \equiv d$, alors $b^n \equiv b^n \,.\, d \equiv b$. Multiplions ($\gamma$) par db^n; d'après (α), nous obtenons $db^n = (db^n)^2 + d^2 \,.\, b^n \,.\, c^n = (db^n)^2$; la classe de b contient l'élément idempotent $b^n \,.\, d$.

Soit maintenant

$$c_1{}^2 = c_1, \; c_2{}^2 = c_2, \; c_1 \equiv c_2 \mod \mathfrak{r}.$$

On a des éléments idempotents d_1, d_2 tels que

$$c_1 + d_1 = 1 = c_2 + d_2.$$

Il est $c_1 = c_2 + r$, par conséquent $d_1 = d_2 - r$, où $r \in \mathfrak{r}$. Parce que $0 = c_1 d_1 = c_2 d_2 = (c_2 + r) \,.\, (d_2 - r) = c_2 d_2 + r(d_2 - c_2) - r^2$, on a $r^2 = r(d_2 - c_2)$. Soit $r \neq 0$; dans ce cas, il existe un nombre naturel n tel que $r^n \neq 0$, $r^{n+1} = 0 = r^{n-1} \,.\, r \,.\, (d_2 - c_2)$, alors

$$0 = r^n \,.\, (d_2 - c_2).$$

Si nous multiplions cette relation par d_2, nous avons $0 = r^n \, . \, d_2{}^2 - r^n \, .$ $. \, d_2 c_2 = r^n \, . \, d_2$ et d'une manière analogue $0 = r^n c_2$, d'où $0 = r^n d_2 + r^n c_2 =$ $= r^n$ contrairement à l'hypothèse. Par conséquent $r = 0$, $c_1 = c_2$, d'où la proposition.

Lemme 3. *Pour que P_N n'ait pas de radical, il faut et il suffit que O n'ait pas de radical.*

Démonstration: Soit d'abord $N = 1$. La relation évidente $\mathfrak{r} \subset \mathfrak{R}_1$ montre que O n'a pas de radical, si P_1 n'a pas de radical. Soit inversement O sans radical, $f = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$; on a pour chaque m $f^m = \sum_{i=0}^{mn} c_i x^i$, $c_{mn} = a_n^m \neq 0$. Donc $f \neq 0 \Rightarrow f^m \neq 0$, c'est-à-dire que P_1 est sans radical. Pour le reste nous procédons par l'induction.

Démonstration du théorème 2. Si l'on a un $f \in \mathfrak{r}[x_1, x_2, \ldots, x_N]$, on a aussi $f \in \mathfrak{R}_N$, parce que chaque terme de f appartient à $\mathfrak{R}_N$. Soit maintenant $f^n = 0$. Considérons f comme un polynôme sur l'anneau $O/\mathfrak{r}$ qui est sans radical. D'après le lemme 3, tous les coefficients de f sont zéro dans $O/\mathfrak{r}$, par suite, $f \in \mathfrak{r}[x_1, x_2, \ldots, x_N]$.

Lemme 4. *Si $y_1, y_2, \ldots, y_N$ sont algébriquement indépendants sur $O/\mathfrak{r}$, les anneaux $P_N/\mathfrak{R}_N$ et $O/\mathfrak{r}[y_1, y_2, \ldots, y_N]$ sont isomorphes.*

Démonstration: On peut exprimer les éléments de tous les deux anneaux par les mêmes symboles avec les mêmes operations et, d'après le théorème 2, avec la même égalité.

Lemme 5. *Soit O sans radical; soit*

$$\left(\sum_{i=0}^{m} a_i x^i\right) . \left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{m+n} c_i x^i,$$

soit $c_K = c_{K+1} = \ldots = c_{m+n} = 0$. Si nous posons $a_{m+1} = a_{m+2} = \ldots =$ $= b_{n+1} = b_{n+2} = \ldots = 0$, la relation $j + l \geqq K$ entraîne $a_j b_l = 0$.

Démonstration: Si l'on a j, l tels que $j + l \geqq K$, $a_j b_l \neq 0$, il existe sûrement un $p \geqq K$ tel qu'il y a j_0, l_0 avec $j_0 + l_0 = p$, $a_{j_0} \, . \, b_{l_0} \neq 0$, mais que la relation $j + l > p$ entraîne $a_j b_l = 0$. (Évidemment $p \leqq m + n$.) On a $c_p = 0$, alors

$$0 = \ldots a_{j_0 - i} \, . \, b_{l_0 + i} + \ldots + a_{j_0} b_{l_0} + \ldots + a_{j_0 + i} \, . \, b_{l_0 - i} + \ldots \qquad (\delta)$$

Multiplions (δ) par $a_{j_0} b_{l_0}$; nous obtenons $(a_{j_0} b_{l_0})^2 = 0$, ce qui n'est pas possible, parce que O n'a pas de radical.

Lemme 6. *Soit O sans radical, c un nondiviseur de zéro; soient f, $g \in P_N$ tels que $fg = c$. Dans ce cas, f, $g \in O$. En particulier, chaque unité de P_N est aussi une unité de O.*

Démonstration: Soit d'abord $N = 1$, $(\sum_{i=0}^{m} a_i x^i) \cdot (\sum_{i=0}^{n} b_i x^i) = c$. La relation $a_0 b_0 = c$ entraîne que a_0, b_0 sont aussi des nondiviseurs de zéro. D'après le lemme 5, on a $0 = a_0 b_1 = a_0 b_2 = \ldots = a_1 b_0 = a_2 b_0 = \ldots \Rightarrow b_1 = b_2 = \ldots = a_1 = a_2 = \ldots = 0$. Pour le reste nous procédons par l'induction.

Démonstration du théorème 3. Soit b une unité de O, $r \in \mathfrak{R}_N$; d'après le lemme 1, $b + r$ est une unité de P_N. Soit réciproquement f une unité de P_N. Il existe un g tel que $fg = 1$. Le terme absolu de f est évidemment une unité de O. Si l'on considère la dernière relation comme une égalité de deux polynômes sur $O/\mathfrak{r}$, on voit d'après le lemme 6, que tous les coefficients de f, excepté le terme absolu, sont zéro mod $\mathfrak{r}$; d'où la proposition.

Lemme 7. *Soit O sans radical, b un nondiviseur de zéro de O, $f \in O[x]$, $f^2 = bf$. Dans ce cas, $f \in O$.*

Démonstration: On a évidemment $0^2 = b \cdot 0$; soit maintenant $f \neq 0$, $f = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$. Si nous comparons les degrés des polynômes f^2 et bf, nous obtenons la relation $2n = n$, par suite, $n = 0$.

Lemme 8. *Si O n'a a pas de radical, les idempotents de P_N appartiennent à O.*

Démonstration: Soit $N = 1$; d'après le lemme 7, $f^2 = 1 \cdot f$ entraîne $f \in O$. Pour le reste nous procédons par l'induction.

Démonstration du théorème 4. Soit $f \in P_N$, $f^2 = f$. Soit c le terme absolu de f, soit $g = f - c$. On a aussi $f^2 \equiv f \bmod \mathfrak{R}_N$; d'après le lemme 4, nous pouvons considérer cette relation comme une égalité de deux polynômes sur $O/\mathfrak{r}$. D'après le lemme 8, tous les coefficients de f, sauf le terme absolu, alors tous les coefficients de g, sont zéro mod $\mathfrak{r}$, par conséquent $f \equiv c \bmod \mathfrak{R}_N$. On a $f = c + g$, $f^2 = f$, $c^2 + 2gc + g^2 = c + g$. En comparant les termes absolus de ces polynômes, on a $c^2 = c$. Parce que $f^2 = f$, $f \equiv c \bmod \mathfrak{R}_N$, on a d'après le théorème 1 $f = c \in O$.

Partie II.

J'appelle un élément b *libre* (dans O), s'il possède les deux propriétés suivantes:

1. b est un nondiviseur de zéro (dans O).
2. Si l'on a $c \in O$, $c^2 = bc$, il existe un $d \in O$ tel que $c = db$.

Dans ce cas, on a $c^2 = d^2 b^2 = b \cdot db \Rightarrow d^2 = d$, donc d est un idempotent. Chaque unité est évidemment libre; mais il y a des anneaux qui contiennent les nondiviseurs de zéro, qui ne sont pas libres.

Dans les lemmes 9—11, O est toujours sans radical.

Lemme 9. *Si b est libre dans O, b est libre aussi dans P_N.*

Démonstration: C'est une conséquence immédiate du lemme 7, parce que b est évidemment un nondiviseur de zéro dans P_N.

Lemme 10. *Si a_1 est libre dans O, $a_0 + a_1x$ est libre dans $O[x]$.*

Démonstration: $a_0 + a_1x$ est certainement un nondiviseur de zéro. Soit $f = \sum_{i=0}^{n} d_i x^i$, $d_n \neq 0$, $f^2 = (a_0 + a_1x)\, f$. En comparant les degrés, on a $2n = n + 1$, par conséquent $n = 1$. On a alors

$$d_1^{\,2} = a_1 \,.\, d_1, \tag{ε}$$

$$2d_0 \,.\, d_1 = a_0 \,.\, d_1 + a_1 \,.\, d_0. \tag{ζ}$$

D'après (ε), il existe un j tel que $j^2 = j$, $d_1 = j \,.\, a_1$. (ζ) entraîne $2d_0 j a_1 = a_0 j a_1 + a_1 d_0 \Rightarrow d_0 = j(2d_0 - a_0) = j^2(2d_0 - a_0) = j(j(2d_0 - a_0)) = jd_0$. Posons dans ($\zeta$) $d_0 = jd_0$, $d_1 = ja_1$. Nous avons $2d_0 j a_1 = a_0 j a_1 + a_1 j d_0 \Rightarrow d_0 j a_1 = a_0 j a_1 \Rightarrow d_0 j = a_0 j$; mais $d_0 = d_0 j$, d'où $f = j(a_0 + a_1x)$.

Lemme 11. *Le déterminant*

$$D = \begin{vmatrix} x_{11}, & x_{12}, & \ldots, & x_{1n} \\ x_{21}, & x_{22}, & \ldots, & x_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ x_{n1}, & x_{n2}, & \ldots, & x_{nn} \end{vmatrix}$$

est libre dans $O[x_{11}, x_{12}, \ldots, x_{nn}]$.

Démonstration: Si $n = 1$, le lemme 10 entraîne le lemme 11. Supposons que le lemme 11 est vrai pour $n - 1 \geqq 1$. On a $D = B + D_{11}x_{11}$, où $B, D_{11} \in O[x_{12}, x_{13}, \ldots, x_{nn}]$. D_{11} est libre dans $O[x_{22}, x_{23}, \ldots, x_{nn}]$; d'après le lemme 9, D_{11} est libre aussi dans $O[x_{12}, x_{13}, \ldots, x_{nn}]$, d'après le lemme 10, $B + D_{11}x_{11} = D$ est libre dans $O[x_{11}, x_{12}, \ldots, x_{nn}]$.

Théorème 5. *Soit $P = O[x_{11}, x_{12}, \ldots, x_{nn}]$,*

$$D = \begin{vmatrix} x_{11}, & x_{12}, & \ldots, & x_{1n} \\ x_{21}, & x_{22}, & \ldots, & x_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ x_{n1}, & x_{n2}, & \ldots, & x_{nn} \end{vmatrix}.$$

Soit $D = F \,.\, G$, $F \in P$, $G \in P$.

Dans ce cas, on a $(i = 1, 2)$ $f_i \in P$, $g \in P$, $j_i \in O$ tels que

$$f_i = f_i \cdot j_i, \; g_i = g_i \,.\, j_i, \; f_i \,.\, g_i = j_i,$$

$$j_1 + j_2 = 1,\ j_1 j_2 = 0,$$
$$F = f_1 + f_2 D,\ G = g_2 + g_1 D.$$

Démonstration: Supposons d'abord O sans radical. Désignons x_{11} par x. On a des polynômes F_i, G_i, B, D_1 indépendents de x (D_1 étant le complément de x dans D) tels que

$$F = \sum_{i=0}^{m} F_i x^i,\ G = \sum_{i=0}^{n} G_i x^i,\ D = B + D_1 x.$$

En vertu de la relation $D = F \cdot G$, on a

$$F_0 G_1 + F_1 G_0 = D_1.$$

D'après le lemme 5, on a

$$F_1 G_1 = 0$$

et, pour $l > 1$,

$$F_0 G_l = F_1 G_l = F_l G_0 = F_l G_1 = 0. \qquad (\eta)$$

Soit encore

$$\varphi = F_0 G_1,\ \psi = F_1 G_0.$$

Si $l > 1$, on a d'après (η) $F_l \cdot \varphi = F_l G_1 F_0 = 0$, $F_l \cdot \psi = F_l G_0 F_1 = 0$, par suite, $F_l(\varphi + \psi) = F_l D_1 = 0$. D'après le lemme 11, D_1 est un nondiviseur de zéro, alors $F_l = 0$ et d'une manière analogue $G_l = 0$. Donc on a

$$F = F_0 + F_1 x,\ G = G_0 + G_1 x.$$

Parce que $F_1 G_1 = 0$, on a $\varphi \cdot \psi = 0$; $\varphi + \psi = D_1$ entraîne alors $\varphi^2 = \varphi D_1$. D'après les lemmes 11 et 9, D_1 est libre, donc on a un j_1 tel que

$$\varphi = j_1 D_1,\ j_1^2 = j_1.$$

Dans ce cas, il existe un j_2 tel que

$$\psi = j_2 D_1,\ j_1 + j_2 = 1,\ j_1 j_2 = 0.$$

D'après le théorème 4, j_1, j_2 appartiennent à O. Soit O_i (resp. P_i) l'idéal, engendré par j_i dans O (resp. dans P); $i = 1, 2$. Soit par exemple $j_1 \neq 0$. Dans ce cas, O_1, P_1 sont les anneaux sans radical, dont l'élément un est j_1, et on a $P_1 = O_1[x_{11}, x_{12}, \ldots, x_{nn}]$. Parce que

$$j_1 F_0 \cdot j_1 G_1 = j_1 \varphi = j_1 D_1,$$

$j_1 G_1$ est un nondiviseur de zéro dans P_1; et en vertu de $j_1 F_1 \cdot j_1 G_1 = 0$, on a $j_1 F_1 = 0$, par suite

$$j_1 F = j_1 F_0.$$

Soit $R_1 = O_1[x_{22}, x_{23}, \ldots, x_{nn}]$. Puisqu'on a $j_1 D_1 \in R_1$ et $j_1 F_0 \cdot j_1 G_1 = j_1 D_1$, le polynôme $j_1 F_0 = j_1 F$ est — d'après le lemme 6 — un élément de R_1; $j_1 F$

est alors indépendent de x_{1k} (et x_{k1}) pour tout k. Choisissons un k quelconque et désignons x_{1k} par $\bar{x}$. On a maintenant

$$F = \overline{F}_0 + \overline{F}_1\bar{x},\ G = \overline{G}_0 + \overline{G}_1\bar{x},\ D = \overline{B} + D_k\bar{x}$$

et ensuite $j_1F = j_1\overline{F}_0 + j_1\overline{F}_1\bar{x}$; mais j_1F est indépendent de $\bar{x}$, or $j_1\overline{F}_1 = 0$, $j_1F = j_1\overline{F}_0$. Parce qu'on a $D_k = \overline{F}_1\overline{G}_0 + \overline{F}_0\overline{G}_1$, on a aussi $j_1D_k = j_1\overline{F}_0\overline{G}_1 = = j_1F\overline{G}_1$. j_1D_k est indépendent de x_{lk} pour tout l; d'après le lemme 6, j_1F est indépendent de x_{lk} pour tout l et tout k, alors

$$j_1F = c_1 \in O_1.$$

Parce que $c_1 \,.\, j_1G = j_1D$, chaque coefficient de j_1D est divisible par c_1; on a un $d_1 \in O_1$ tel que $c_1d_1 = j_1$ et $d_1c_1j_1G = j_1G = d_1j_1D = d_1D$, or,

$$j_1G = d_1D.$$

Si $j_2 = 0$, c'est-à-dire $j_1 = 1$, on a $j_1F = F = c_1 \in O_1$, $j_1G = G = d_1D$; si nous posons $f_1 = c_1$, $g_1 = d_1$, $f_2 = g_2 = 0$, nous voyons que le théorème 5 est vrai dans ce cas.

Si $j_2 \neq 0$, on a d'une manière analogue $c_2, d_2 \in O_2$, c_2, d_2 étant tels que $c_2d_2 = j_2$, $d_2 = j_2G$, $j_2F = c_2D$ et

$$F = j_1F + j_2F = c_1 + c_2D,\ G = d_2 + d_1D,$$

d'où la proposition.

Soit maintenant O un anneau quelconque; soit $D = F \,.\, G$. Considérons cette relation comme une égalité de deux polynômes sur $O/\mathfrak{r}$ et désignons par $\mathfrak{R}$ le radical de P. D'après ce que nous avons montré, le théorème 5 est vrai, si nous remplaçons l'égalité $=$ par la congruence $\equiv$ $\equiv \bmod \mathfrak{R}$. D'après le théorème 1, il existe j_1, j_2, qu'on a non seulement $j_1 + j_2 \equiv 1$, $j_1j_2 \equiv 0$, mais encore $j_1 + j_2 = 1$, $j_1j_2 = 0$.

Soit $j_1 \neq 0 \neq j_2$; désignons par a_i (resp. b_i) les éléments j_if_i (resp. j_ig_i), $i = 1, 2$. On a $a_i \,.\, b_i \equiv j_i$. D'après le lemme 1, $a_i \,.\, b_i$ est une unité de P_i; a_i, b_i sont alors unités de P_i.

Parce que $f_i \equiv a_i$, $g_i \equiv b_i$, on a

$$f_i = a_i + r_i,\ g_i = b_i + s_i,\ \text{où}\ r_i, s_i \in \mathfrak{R}.$$

En vertu de $F \equiv f_1 + f_2D$, $G \equiv g_2 + g_1D$, on a

$$F = a_1 + r_1 + a_2D + r_2D + r_3 = a_1 + a_2D + R,$$

$$G = b_2 + s_2 + b_1D + s_1D + s_3 = b_2 + b_1D + S,$$

où $r_3, s_3, R, S \in \mathfrak{R}$.

On a aussi

$$j_1D = j_1F \cdot j_1G = (a_1 + j_1R)(b_1D + j_1S).$$

Puisque a_1 est une unité de P_1 et j_1R appartient au radical de P_1, on voit que

$$c_1 = a_1 + j_1R$$

est une unité de P_1. Donc il existe un $d_1 \in P_1$ tel que $c_1d_1 = j_1$, par suite $d_1j_1D = d_1D = d_1c_1(b_1D + j_1S)$, c'est-à-dire que

$$d_1D = b_1D + j_1S.$$

Soit $d_2 = b_2 + j_2S$; d'une manière analogue, il existe un $c_2 \in P_2$ tel que $c_2d_2 = j_2$. Parce que $j_2D = j_2F \cdot j_2G = (a_2D + j_2R)(b_2 + j_2S)$, on a

$$c_2D = a_2D + j_2R.$$

Donc on a $F = a_1 + j_1R + a_2D + j_2R = c_1 + c_2D$, $G = b_2 + j_2S + b_1D + j_1S = d_2 + d_1D$. Si nous posons f_i, g_i, au lieu de c_i, d_i, nous voyons que le théorème 5 est vrai.

Soit par exemple $j_2 = 0$; nous pouvons appliquer la même démonstration, si nous remplaçons chaque élément de O_2 par zéro.

Démonstration du théorème principal. Soit O irréductible, c'est-à-dire qu'il n'y a pas des anneaux O_1, O_2 tels que $O = O_1 \dot{+} O_2$. Dans ce cas, un de deux élements j_1, j_2, par exemple j_2, du théorème 5 est zéro et on a $D = f_1g_1D$. Comme D est un nondiviseur de zéro, on a $1 = f_1g_1$; par suite, $F = f_1$ est une unité.

Soit maintenant O réductible, $O = (j_1) \dot{+} (j_2)$. Soient f_i, g_i tels que $f_i, g_i \in (j_i)$, $f_i \cdot g_i = j_i$, $i = 1, 2$. Soit b le terme absolu de f_1. Si $F = f_1 + f_2D$ était une unité, b serait une unité de O; ce n'est pas vrai, parce que $b \in (j_1)$, b est alors un diviseur de zéro. Donc on a une décomposition dans le sens de la théorie de divisibilité.

K tisku doporučil prof. dr Vl. Kořínek.

Za úpravu a jazykovou stránku odpovídá autor.

Autoribus ipsis rerum, formae, orationis ratio reddenda est.

Author alone is responsible for the form, style, and all opinions expressed in his communications.