Jan Mařík

Приводимость определителя с неизвестными в качестве элементов, если его принять за полином над коммутативным кольцом

Czechoslovak Mathematical Journal, Vol. 2 (1952), No. 3, 279–293

Persistent URL: http://dml.cz/dmlcz/100052

ПРИВОДИМОСТЬ ОПРЕДЕЛИТЕЛЯ С НЕИЗВЕСТНЫМИ В КАЧЕСТВЕ ЭЛЕМЕНТОВ, ЕСЛИ ЕГО ПРИНЯТЬ ЗА ПОЛИНОМ НАД КОММУТАТИВНЫМ КОЛЬЦОМ

ЯН МАРЖИК (Jan Mařík), Прага.

(Поступило в редакцию 8/III 1952 г.)

В 1. части автор находит делители единицы, идемпотенты, делители нуля и радикал кольца полиномов над коммутативным кольцом.

Во 2. части доказано необходимое и достаточное условие для того, чтобы определитель, рассматриваемый как полином, был приводимым.

Рассмотрим прежде всего определитель

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

с элементами x_{ik} алгебраически независимыми над коммутативным кольцом I без делительей нуля. При доказательстве того факта, что D является неприводимым полиномом над I, мы воспользуемся теоремой, что степень произведения двух полиномов равна сумме степеней этих двух сомножителей. Эта теорема не имеет места для колец, содержащих делители нуля; в семинаре проф. Коржинка был поднят следующий вопрос: может ли определитель D быть приводимым, если его рассматривать как полином над коммутативным кольцом, имеющим единицу?

Ответ содержится в

Главной теореме. *Пусть O — коммутативное кольцо с единицей. Для того, чтобы определитель D, рассматриваемый как полином относительно элементов x_{ik} алгебраически независимых над O, был приводимым, необходимо и достаточно, чтобы O было прямой суммой двух колец.*

В этой теореме мы пользуемся понятием приводимости полинома в смысле делимости в кольце $P = O[x_{11}, x_{12}, \ldots, x_{nn}]$. Полином называется приводимым, если он равен произведению двух сомножителей, ни один из которых не является делителем единицы кольца P. Обычное определение приводимости не совпадает с этим. В обычном смысле полином называется приводимым, если он представляет произведение двух сомножителей, каждый из которых является полиномом степени по крайней мере первой.

Доказательство главной теоремы составляет предмет настоящей работы. Ясно, что если O — прямая сумма колец O_1, O_2 и если $j_i \in O_i$ и $f_i, g_i \in O_i[x_{11}, x_{12}, \ldots, x_{nn}]$ такие, что $j_1 + j_2 = 1$, $f_i \cdot g_i = j_i$ (например $f_i = g_i = j_i$), где $i = 1, 2$, то будет также иметь место

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

Во II части этой работы я покажу, что таким обра:ом мы получим все разложения D, откуда легко следует справедливость главной теоремы. В I части я нахожу делители единицы, идемпотенты, делители нуля и радикал кольца P.

Часть первая.

Пусть O — коммутативное кольцо с единицей, которую мы обозначим через 1. Если, кроме того, обозначить через 0 нулевой элемент, то мы получим $b + 0 = b$, $b \cdot 1 = b$ для всех $b \in O$. Элемент c называется делителем единицы, если существует d такое, что $cd = 1$.

Мы называем b нильпотентом, если существует натуральное число m такое, что $b^m = 0$. Соотношения $b^m = 0$, $c^n = 0$, $b^k \cdot c^l \neq 0$ влекут за собой следующие: $k \leqq m - 1$, $l \leqq n - 1$, $k + l \leqq m + n - 2$; тогда мы имеем

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

так как все члены суммы равны нулю. Кроме того имеет место $(bd)^m = b^m \cdot d^m = 0$ для всех d. Следовательно, множество всех нильпотентов будет идеалом, который называется радикалом; мы его обозначим через $\mathfrak{r}$. Мы говорим, что O — кольцо без радикала или что O не содержит радикала, если в $\mathfrak{r}$ не имеется ни одного элемента, отличного от нуля. Если имеет место $b^m \equiv 0 \bmod \mathfrak{r}$, то существует некоторое $c \in \mathfrak{r}$ такое, что $b^m = c$ и можно найти натуральное число n такое, что $0 = c^n = b^{mn}$, откуда $b \equiv 0 \bmod \mathfrak{r}$. Итак, кольцо $O/\mathfrak{r}$ не имеет радикала.

Элемент j называется идемпотентом, если имеет место $j^2 = j$ (а значит и $j^n = j$ для всякого натурального числа n). Пусть $k = 1 - j$. Тогда будет $jk = j - j^2 = 0$, $k^2 = k - kj = k$; отсюда и k будет одновременно идемпотентом. Пусть (j), (k) — идеалы, порожденные соответственно j, k в O. Если $bj = ck$, будет также $0 = bjk = ck^2 = ck = bj$, следовательно, нуль будет единственным элементом, содержащимся одновременно как в (j), так и в (k). Пусть $j \neq 0 \neq k$; имеем $O = (j) \dotplus (k)$. j (соотв. k) является, очевидно, единицей кольца (j) [соотв. (k)]. Пусть наоборот $O = O_1 \dotplus O_2$; имеем $j \in O_1$, $k \in O_2$ такие, что $1 = j + k$, $0 = jk$, откуда $j^2 = j$, $k^2 = k$ и $j \neq 0 \neq k$. Найдя все идемпотенты, мы этим самым отыскали все разложения кольца O на прямую сумму и наоборот.

Пусть $x_1, x_2, \ldots, x_N$ — алгебраически независимые элементы над O. Пусть $P_N = O[x_1, x_2, \ldots, x_N]$; обозначим через $\mathfrak{R}_N$ радикал из P_N. В этой части мы докажем следующие теоремы:

Теорема 1. *Каждый идемпотентный класс кольца $O/\mathfrak{r}$ содержит один и только один идемпотентный элемент кольца O.*

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

Теорема 3. *Для того, чтобы полином $f \in P_N$ был делителем единицы в P_N, необходимо и достаточно, чтобы свободный член f (член нулевой степени) был делителем единицы в O и чтобы все остальные коэффициенты принадлежали к $\mathfrak{r}$.*

Теорема 4. *Все идемпотенты из P_N принадлежат колцу O.*

Теорема 5.*) *Полином $f \in P_N$ является делителем нуля в P_N тогда и только тогда, когда существует $c \in O$, $c \neq 0$ такое, что $cf = 0$.*

Мы докажем эти теоремы с помощью нескольких лемм.

Лемма 1. *Если b — делитель единицы из O и если $r \in \mathfrak{r}$, то $b + r$ будет также делителем единицы кольца O.*

Доказательство: Существует $c \in O$ и натуральное число n такие, что $bc = 1$, $r^n = 0$. Положим $s = -r$. Имеем $1 = b^n \,.\, c^n = (b^n - s^n) \,.\, c^n = (b - s) \,.\, (b^{n-1} + \ldots + s^{n-1}) \,.\, c^n$; следовательно, $b - s = b + r$ будет делителем единицы.

Лемма 2. *Если b — делитель единицы кольца $O/\mathfrak{r}$, то b будет также делителем единицы кольца O.*

---

*) Когда рукопись работы была уже закончена, проф. *Коржинек* обратил внимание автора на то, что теорема 5 при $N = 1$ содержится в работе *Mc Coy*, *The American Mathematical Monthly*, Vol. **49** (1942), 286—295. Доказательство приводит *A. Forsythe* (*The American Mathematical Monthly*, Vol. **50** (1943), 7—8).

Доказательство: Существует c такое, что $bc \equiv 1 \bmod \mathfrak{r}$, следовательно, $bc = 1 + r$, где $r \in \mathfrak{r}$. Согласно лемме 1, $1 + r$ будет делителем единицы кольца O, и тогда существует d такое, что $1 = d(1 + r) = b(cd)$. Следовательно, b является делителем единицы кольца O.

Доказательство теоремы 1. Пусть $b^2 \equiv b \bmod \mathfrak{r}$. Пусть $c = 1 - b$. Имеем

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

Существует n такое, что

$$b^n \,.\, c^n = 0 \tag{1}$$

и, так как $b^n \equiv b$, $c^n \equiv c$,

$$b^n + c^n \equiv 1. \tag{2}$$

Согласно лемме 2, $b^n + c^n$ является делителем единицы в O, следовательно, имеется d такое, что

$$1 = db^n + dc^n. \tag{3}$$

Согласно (2) имеем $1 \equiv d(b^n + c^n) \equiv d$, откуда $b^n \equiv b^n \,.\, d \equiv b$. Помножим (3) на db^n; в силу (1) мы получим $db^n = (db^n)^2 + d^2 \,.\, b^n \,.\, c^n = (db^n)^2$; класс элемента b содержит идемпотентный элемент $b^n \,.\, d$. Пусть теперь

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

Мы имеем идемпотентные элементы d_1, d_2 такие, что

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

Имеет место $c_1 = c_2 + r$, следовательно $d_1 = d_2 - r$, где $r \in \mathfrak{r}$.

Так как $0 = c_1d_1 = c_2d_2 = (c_2 + r) \,.\, (d_2 - r) = c_2d_2 + r(d_2 - c_2) - r^2$, мы получим $r^2 = r(d_2 - c_2)$. Пусть $r \neq 0$; в этом случае существует натуральное число n такое, что $r^n \neq 0$, $r^{n+1} = 0 = r^{n-1} \,.\, r \,.\, (d_2 - c_2)$, откуда

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

Если умножить это соотношение на d_2, мы получим $0 = r^n \,.\, d_2^2 - r^n \,.\, d_2c_2 = r^n \,.\, d_2$ и аналогично $0 = r^n \,.\, c_2$, откуда $0 = r^n \,.\, d_2 + r^n \,.\, c_2 = r^n$, в противоречии с предположением. Итак, $r = 0$, $c_1 = c_2$, откуда следует наше утверждение.

Лемма 3. *Для того, чтобы P_N не имело радикала, необходимо и достаточно, чтобы O не имело радикала.*

Доказательство: Пусть прежде всего $N = 1$. Очевидное соотношение $\mathfrak{r} \subset \mathfrak{R}_1$ показывает, что O не имеет радикала, если P_1 не имеет радикала. Наоборот, пусть O будет без радикала,

$f = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$; для всякого m будет $f^m = \sum_{i=0}^{mn} c_i x^i$, $c_{mn} = a_n^m \neq 0$. Следовательно, $f \neq 0 \Rightarrow f^m \neq 0$, другими словами P_1 не имеет радикала. Доказательство заканчивается по методу индукции.

Доказательство теоремы 2. Пусть $f \in \mathfrak{r}[x_1, x_2, \ldots, x_N]$, тогда будет также $f \in \mathfrak{R}_N$, так как каждый член f принадлежит к $\mathfrak{R}_N$. Пусть теперь $f^n = 0$. Примем f за полином над кольцом $O/\mathfrak{r}$, не имеющим радикала. По лемме 3 все коэффициенты f равны нулю в $O/\mathfrak{r}$, следовательно, $f \in \mathfrak{r}[x_1, x_2, \ldots, x_N]$.

Лемма 4. *Если $y_1, y_2, \ldots, y_N$ — алгебраически независимые элементы над $O/\mathfrak{r}$, то кольца $P_N/\mathfrak{R}_N$ и $O/\mathfrak{r}[y_1, y_2, \ldots, y_N]$ изоморфны.*

Доказательство: Элементы обоих колец можно выразить теми же самыми символами с теми же операциями и, вследствие теоремы 2, с тем же равенством.

Лемма 5. *Пусть O не имеет радикала; пусть*

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

Пусть $c_K = c_{K+1} = \ldots = c_{m+n} = 0$. Если положить $a_{m+1} = a_{m+2} = \ldots = b_{n+1} = b_{n+2} = \ldots 0$, то соотношение $j + l \geqq K$ влечет за собой $a_j b_l = 0$.

Доказательство: Если имеем j, l такие, что $j + l \geqq K$, $a_j b_l \neq 0$, то наверное существует $p \geqq K$ такое, что существуют j_0, l_0 со свойством $j_0 + l_0 = p$, $a_{j_0} b_{l_0} \neq 0$, причем, однако, соотношение $j + l > p$ влечет за собой $a_j b_l = 0$. (Очевидно $p \leqq m + n$.) Имеем $c_p = 0$, откуда

$$0 = \ldots a_{j_0 - i} . b_{l_0 + i} + \ldots + a_{j_0} . b_{l_0} + \ldots + a_{j_0 + i} . b_{l_0 - i} + \ldots \qquad (4)$$

Умножим (4) на $a_{j_0} . b_{l_0}$; мы получим $(a_{j_0} . b_{l_0})^2 = 0$, что невозможно, так как O не имеет радикала.

Лемма 6. *Пусть O не имеет радикала, c не является делителем нуля; пусть $f, g \in P_N$ таковы, что $fg = c$. В этом случае $f, g \in O$. В частности, каждый делитель единицы в P_N принадлежит кольцу O.*

Доказательство: Положим сначала $N = 1$, $(\sum_{i=0}^{m} a_i x^i) . (\sum_{i=0}^{n} b_i x^i) = c$. Соотношение $a_0 b_0 = c$ показывает, что и a_0, b_0 не являются делителями нуля. Согласно лемме 5 мы имеем $0 = a_0 b_1 = a_0 b_2 = \ldots = a_1 b_0 = a_2 b_0 = \ldots \Rightarrow b_1 = b_2 = \ldots =$

$= a_1 = a_2 = \ldots = 0$. Доказательство заканчиваем по методу индукции.

Доказательство теоремы 3. Пусть b — некоторый делитель единицы в O, $r \in \mathfrak{R}_N$; согласно лемме 1, $b + r$ является делителем единицы в P_N. Наоборот, пусть f — делитель единицы в P_N. Существует g такое, что $fg = 1$. Свободный член f будет, очевидно, делителем единицы в O. Если последнее соотношение рассматривать как равенство двух полиномов над $O/\mathfrak{r}$, то вследствие леммы 6 легко видеть, что все коэффициенты f, за исключением свободного члена, равны $0 \bmod \mathfrak{r}$; отсюда справедливость теоремы.

Лемма 7. *Пусть O — кольцо без радикала, b не является делителем нуля в O, $f \in O[x]$, $f^2 = bf$. В таком случае $f \in O$.*

Доказательство: Очевидно $0 \in O$; пусть теперь будет $f \neq 0$, $f = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$. Если сравнить степени полиномов f^2 и bf, то мы получим соотношение $2n = n$, а следовательно, $n = 0$.

Лемма 8. *Если O не имеет радикала, то идемпотенты из P_N принадлежат к O.*

Доказательство: Пусть $N = 1$; согласно лемме 7, из $f^2 = 1 \cdot f$ следует $f \in O$. Доказательство закончим по методу индукции.

Доказательство теоремы 4. Пусть $f \in P_N$, $f^2 = f$. Пусть c — свободный член f и пусть $g = f - c$. Мы можем рассматривать соотношение $f^2 = f$ как равенство двух полиномов над $O/\mathfrak{r}$. По лемме 8 все коэффициенты f кроме свободного члена, т. е. все коэффициенты g, равны $0 \bmod \mathfrak{r}$, следовательно $f \equiv c \bmod \mathfrak{R}_N$. Имеем $f = c + g$, $f^2 = f$, $c^2 + 2gc + g^2 = c + g$. Сравнивая свободные члены этих полиномов, мы получим $c^2 = c$. Так как $f^2 = f$, $f \equiv c \bmod \mathfrak{R}_N$, то согласно теореме 1 будет $f = c \in O$.

Замечание: Теорему 5 мы докажем сначала для $N = 1$; вместо x_1 будем писать x. Пусть тогда полином $f \in O[x]$ является делителем нуля. В таком случае существует $g \in O[x]$, $g \neq 0$ такой, что $fg = 0$. Полиномы f, g будем теперь считать фиксированными; напишем

$$f = \sum_{i=0}^{m} a_i x^i, \quad g = \sum_{i=0}^{n} b_i x^i,$$

где a_i, b_i — элементы кольца O. (Буквы a_i, b_i будут иметь в леммах 9 и 10 то же значение.) Мы хотим найти $c \in O$, $c \neq 0$ такое, чтобы имело место $cf = 0$. Так как $g \neq 0$, то для некоторого j должно быть $b_j \neq 0$; положим $b_j = c_0$. Если $c_0 f = 0$, выберем $c = c_0 = b_j$. Иначе существует a_{i_1} такое, что $c_0 a_{i_1} \neq 0$; тогда положим $c_0 a_{i_1} = c_1 \neq 0$. Если $c_1 f = 0$, выберем $c = c_1$; иначе существует a_{i_2} такое, что $c_1 a_{i_2} = b_j a_{i_1} a_{i_2} \neq 0$ и выберем $c_2 = c_1 a_{i_2}$. Таким же образом поступаем и далее. Нам нужно теперь доказать, что для некоторого p будет $c_p f = 0$ (согласно нашему построению будет $c_p \neq 0$). Для этого введем такое обозначение: Если k целое, $k \geqq 0$, то пусть S_k обозначает систему всех елементов из O, которые можно выразить в виде произведения k коэффициентов полинома f (одинаковых или различных); это значит, что имеет место $t \in S_k$ тогда и только тогда, когда существуют $i_1, i_2, \ldots, i_k$, $0 \leqq i_j \leqq m$ для $j = 1, 2, \ldots, k$, так что

$$t = a_{i_1} a_{i_2} \ldots a_{i_k}.$$

Система S_0 содержит только пустое произведение, т. е. элемент 1. Построенные нами элементы $c_0, c_1, c_2, \ldots$ примут теперь вид $b_j = b_j t_0, b_j t_1, b_j t_2, \ldots$, где $1 = t_0 \in S_0$, $t_1 = a_{i_1} \in S_1$, $t_2 = a_{i_1} a_{i_2} \in S_2$ и т. д. Итак, для доказательства теоремы 5 в случае одного переменного достаточно доказать, что для некоторого q будет $b_j t f = 0$ для $j = 0, 1, \ldots, n$ и для каждого $t \in S_q$ или, что то же самое, доказать, что $b_j t = 0$ для каждого j и каждого $t \in S_{q+1}$. Существование такого q будет доказано в Лемме 10; а именно, можно выбрать $q = n$ (= степени полинома g). Однако, перед этим нам нужно доказать еще одну лемму.

Лемма 9. *Пусть* $f = \sum_{i=0}^{m} a_i x^i$, $g = \sum_{j=0}^{n} b_j x^j$, $fg = 0$. *Пусть* k — *целое,* $0 \leqq k \leqq n$; *пусть* $d \in O$. *Допустим, что*

$$b_j t d = 0 \tag{5}$$

для $j = 0, 1, \ldots, n - k$ *и для любого* $t \in S_k$. *Тогда имеет место* (5) *для* $j = 0, 1, \ldots, n$ *и для любого* $t \in S_k$.

Доказательство: Для $k = 0$ наше утверждение тривиально. Предположим, что оно справедливо для $k - 1$, $0 \leqq k - 1 < n$. Для каждого $t \in S_k$ существуют $t' \in S_{k-1}$ и индекс i такие, что $t = a_i t'$. Пусть тогда имеет место

$$b_j a_i t' d = 0 \tag{6}$$

для $j = 0, 1, \ldots, n - k$, для всех i и для всех $t' \in S_{k-1}$ (что является как раз предположениями леммы 9); докажем, что (6) имеет место для всех i, всех j и всех $t' \in S_{k-1}$. Этим будет, очевидно, доказана и лемма 9.

Если положить $a_{-1} = 0$, то (6) справедливо всегда, когда имеет место $i = -1$. Перейдем тепер к доказатеству по методу индукции утверждения V_p: (6) имеет место для всех j и для всех $t' \in S_{k-1}$, если $-1 \leqq i \leqq p$.

Мы установили, что утверждение V_p справедливо для $p = -1$. Пусть оно справедливо для $p-1$, $-1 \leqq p-1 < m$; мы докажем, что оно справедливо и для p. В силу $fg = 0$ будет

$$\sum_{i+j=n+p-k+1} a_i b_j = \ldots a_{p-1} b_{n-k+2} + a_p b_{n-k+1} + a_{p+1} b_{n-k} + \ldots = 0 \tag{7}$$

(для $p = m$ ($k = 1$) положим $a_{p+1} = 0$ ($b_{n-k+2} = 0$)). Выберем произвольно $t' \in S_{k-1}$ и умножим (7) на элемент $t'd$. Члены вида $a_i b_j t'd$ для $i < p$ равны нулю в силу V_{p-1}; однако, для $i > p$ будет $j \leqq n-k$ и согласно предположению о справедливости (6) мы получим снова $a_i b_j t'd = 0$. Итак, остается

$$b_{n-k+1} a_p t'd = 0. \tag{8}$$

Положив $a_p d = d'$, мы видим, что имеет место

$$b_j t'd' = 0 \tag{9}$$

согласно (6) для $j = 0, 1, \ldots, n-k$, а согласно (8) и для $j = n-(k-1)$ (и для любого $t' \in S_{k-1}$). Мы предположили, что лемма 9 справедлива для $k-1$; если положить в ней d' вместо d, то ввиду (9) получим

$$b_j a_p t'd = b_j t'd' = 0$$

для любого j и любого $t' \in S_{k-1}$.

Этим доказано утверждение V_p, а следовательно и справедливость (6) для любых i, j и любых $t' \in S_{k-1}$. Этим доказана и лемма 9.

Лемма 10. *Теорема 5 справедлива для* $N = 1$.

Доказательство: Согласно предыдущему замечанию достаточно доказать, что имеет место

$$b_j a_i t = 0 \tag{10}$$

для любых i, j и для любых $t \in S_n$.

Если снова положить $a_{-1} = 0$, то (10) справедливо для $i = -1$. Выберем p, $-1 \leqq p-1 < n$, и предположим, что (10) имеет место для всех j и всех $t \in S_n$ в случае, если $-1 \leqq i \leqq p-1$. Выбрав произвольно $t \in S_n$, умножим на него соотношение

$$\sum_{i+j=p} a_i b_j = \ldots + a_{p-1} b_1 + a_p b_0 = 0.$$

Так как по предположению имеет место $a_i b_j t = 0$ для $i < p$, получаем

$$a_p b_0 t = 0.$$

Если теперь положить в лемме 9 $k = n$, $d = a_p$, то будут выполнены предположения, а следовательно и утверждение; итак, имеет место

$$a_p b_j t = 0$$

для $j = 0, 1, \ldots, n$.

Этим доказано соотношение (10) для $i = p$, а поэтому и для любого i; одновременно доказана и теорема 5 для $N = 1$.

Лемма 11. *Пусть* $f_1, f_2, \ldots, f_n$, $h \in O[x]$, $h \neq 0$, $f_i h = 0$ *для* $i = 1, 2, \ldots, n$. *Тогда существует* $c \in O$, $c \neq 0$ *такое, что имеет место*

$$f_i c = 0$$

для $i = 1, 2, \ldots, n$.

Доказательство: Положим

$$r_i = 1 + \text{степень } f_i,\ s_i = r_1 + r_2 + \ldots + r_i$$
$$(i = 1, 2, \ldots, n - 1).$$

Пусть далее

$$F = f_1 + x^{s_1} f_2 + \ldots + x^{s_{n-1}} f_n.$$

(Полином F составлен так, чтобы полиномы $f_1, x^{s_1} f_2, \ldots, x^{s_{n-1}} f_n$,,не перекрывали'' друг друга.)

Так как $Fh = 0$, то существует $c \in O$, $c \neq 0$ такое, что $Fc = 0$. Из построения полинома F легко вытекает, что имеет место и $f_i c = 0$ для $i = 1, 2, \ldots, n$.

Доказательство теоремы 5. Мы уже знаем, что теорема 5 справедлива для $N = 1$; предположим, что она справедлива для $N - 1 \geq 1$. Пусть $f, g \in P_N = O[x_1, \ldots, x_N]$, $g \neq 0$, $fg = 0$. Полиномы f, g можно считать полиномами относительно $N - 1$ переменных $x_2, \ldots, x_N$ над кольцом $O[x_1]$; пусть например

$$f = \Sigma f_{i_2 i_3 \ldots i_N} x_2^{i_2} x_3^{i_3} \ldots x_N^{i_N},$$

где $f_{i_2 i_3 \ldots i_N} \in O[x_1]$. Согласно индукционному предположению существует $h \in O[x_1]$ такое, что имеет место $fh = 0$ или

$$f_{i_2 i_3 \ldots i_N} \cdot h = 0$$

для любого полинома $f_{i_2 i_3 \ldots i_N}$. Однако, имеется только конечное количество этих полиномов; поэтому, согласно лемме 11 существует $c \in O$, $c \neq 0$ такое, что имеет место

$$f_{i_2 i_3 \ldots i_N} \cdot c = 0$$

для любого из этих полиномов. Отсюда справедливо и $fc = 0$. Этим доказана теорема 5.

Я называю элемент b *свободным* (в O), если он обладает двумя следующими свойствами:

1. b не является делителем нуля (в O).

2. Если $c \in O$, $c^2 = bc$, то существует $d \in O$ такое, что $c = db$.

В этом случае имеет место $c^2 = d^2b^2 = b \cdot db \Rightarrow d^2 = d$, следовательно, d является идемпотентом. Каждый делитель единицы будет, очевидно, свободным; однако, имеются кольца, содержащие не-делители нуля, которые не свободны.

В леммах 12—14 O предполагается не имеющим радикала.

Лемма 12. *Если b свободно в O, то b свободно и в P_N.*

Доказательство: Лемма следует непосредственно из леммы 8, так как b, очевидно, не является делителем нуля в P_N.

Лемма 13. *Если a_1 свободно в O, то $a_0 + a_1x$ свободно в $O[x]$.*

Доказательство: $a_0 + a_1x$ наверное не является делителем нуля. Пусть $f = \sum_{i=0}^{n} d_i x^i$, $d_n \neq 0$, $f^2 = (a_0 + a_1x)\, f$. Сравнивая степени, мы получаем $2n = n + 1$, следовательно, $n = 1$. Отсюда

$$d_1^2 = a_1 d_1, \tag{11}$$

$$2d_0 d_1 = a_0 d_1 + a_1 d_0. \tag{12}$$

Согласно (11) существует j такое, что $j^2 = j$, $d_1 = ja_1$. (12) влечет за собой $2d_0ja_1 = a_0ja_1 + a_1d_0 \Rightarrow d_0 = j(2d_0 - a_0) = j^2(2d_0 - a_0) = j(j(2d_0 - a_0)) = jd_0$. Положим в (12) $d_0 = jd_0$, $d_1 = ja_1$. Имеем $2d_0ja_1 = a_0ja_1 + a_1jd_0 \Rightarrow d_0ja_1 = a_0ja_1 \Rightarrow d_0j = a_0j$; однако $d_0 = d_0j$, откуда $f = j(a_0 + a_1x)$.

Лемма 14. *Определитель*

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

являерся свободным в $O[x_{11}, x_{12}, \ldots, x_{nn}]$.

Доказательство: Если $n = 1$, лемма 13 влечет за собой лемму 14. Допустим, что лемма 14 справедлива для $n - 1 \geq 1$. Имеем $D = B + D_{11}x_{11}$, где B, $D_{11} \in O[x_{12}, x_{13}, \ldots, x_{nn}]$. D_{11} свободно в $O[x_{22}, x_{23}, \ldots, x_{nn}]$; согласно лемме 12 D_{11} свободно также в $O[x_{12}, x_{13}, \ldots, x_{nn}]$, согласно лемме 13 $B + D_{11}x_{11}$ свободно в $O[x_{11}, x_{12}, \ldots, x_{nn}]$.

Теорема 6. *Пусть* $P = O[x_{11}, x_{12}, \ldots, x_{nn}]$,

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

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

В этом случае существуют $f_i \in P$, $g_i \in P$, $j_i \in O$ $(i = 1, 2)$, *так что*

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

$$j_1 + j_2 = 1,\ j_1 j_2 = 0,$$

$$F = f_1 + f_2 D,\ G = g_2 + g_1 D.$$

Доказательство: Предположим сначала, что O не имеет радикала. Обозначим x_{11} через x. Имеем полиномы F_i, G_i, B, D_1 независимые от x (причем D_1 является алгебраическим дополнением элемента x в D) такие что

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

В силу соотношения $D = F \,.\, G$ получаем

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

По лемме 5 будет

$$F_1 G_1 = 0$$

и для $l > 1$

$$F_0 G_l = F_1 G_l = F_l G_0 = F_l G_1 = 0. \tag{13}$$

Пусть далее

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

Если $l > 1$, в силу (13) получим $F_l \varphi = F_l G_1 F_0 = 0$, $F_l \psi = \psi F_l G_0 F_1 = 0$, следовательно, $F_l(\varphi + \psi) = F_l D_1 = 0$. По лемме 14 D_1 не будет делителем нуля, откуда $F_l = 0$ и аналогично $G_l = 0$. Итак

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

Так как $F_1 G_1 = 0$, имеет место $\varphi\psi = 0$; $\varphi + \psi = D_1$ влечет тогда за собой $\varphi^2 = \varphi D_1$. По леммам 14 и 12 D_1 свободно, следовательно имеется j_1 такое, что

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

В этом случае существует j_2 такое что

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

По теореме 4 j_1, j_2 принадлежат к O. Пусть O_i (соотв. P_i) будет идеалом, порожденным j_i в O (соотв. в P); $i = 1, 2$. Пусть например $j_1 \neq 0$. В этом случае O_1, P_1 являются кольцами без радикалов, единицей которых будет j_1, и мы получим $P_1 = O_1[x_{11}, x_{12}, \ldots, x_{nn}]$. Так как

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

то $j_1 G_1$ не будет делителем нуля в P_1; в силу соотношения $j_1 F_1 \cdot j_1 G_1 = 0$ получим $j_1 F_1 = 0$ и следовательно

$$j_1 F = j_1 F_0.$$

Пусть $R_1 = O_1[x_{22}, x_{23}, \ldots, x_{nn}]$. Так как $j_1 D_1 \in R_1$ и $j_1 F_0 \cdot j_1 G_1 = j_1 D_1$, полином $j_1 F_0 = j_1 F$ будет — согласно лемме 6 — элементом из R_1; $j_1 F$ будет тогда независимым от x_{1k} (и от x_{k1}) для всех k. Зададим произвольное k и обозначим x_{1k} через $\bar{x}$. Тогда мы получаем

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

и далее $j_1 F = j_1 \bar{F}_0 + j_1 \bar{F}_1 \bar{x}$; однако, $j_1 F$ не зависит от $\bar{x}$, следовательно, $j_1 \bar{F}_1 = 0$, $j_1 F = j_1 \bar{F}_0$. Так как $D_k = \bar{F}_1 \bar{G}_0 + \bar{F}_0 \bar{G}_1$, будет $j_1 D_k = j_1 \bar{F}_0 \bar{G}_1 = j_1 F \bar{G}_1$. $j_1 D_k$ не зависит от x_{lk} для всех l; согласно лемме 6 $j_1 F$ не зависит от x_{lk} для всех l и всех k, откуда

$$j_1 F = c_1 \in O_1.$$

Так как $c_1 \cdot j_1 G = j_1 D$, каждый коэффициент выражения $j_1 D$ делится на c_1; существует $d_1 \in O_1$ такое, что $c_1 d_1 = j_1$ и $d_1 c_1 j_1 G = j_1 G = d_1 j_1 D = d_1 D$, так что

$$j_1 G = d_1 D.$$

Если $j_2 = 0$, то есть $j_1 = 1$, то будет $j_1 F = F = c_1 \in O_1$, $j_1 G = G = d_1 D$; положив $f_1 = c_1$, $g_1 = d_1$, $f_2 = g_2 = 0$, мы видим, что теорема 6 в этом случае справедлива.

Если $j_2 \neq 0$, аналогично получаем c_2, $d_2 \in O_2$, где c_2, d_2 таковы, что $c_2 d_2 = j_2$, $d_2 = j_2 G$, $j_2 F = c_2 D$ и

$$F = j_1 F + j_2 F = c_1 + c_2 D,\ G = d_2 + d_1 D,$$

что нам и требовалось для доказательства.

Пусть теперь O будет произвольным кольцом; пусть $D = F \cdot G$. Рассматривая это соотношение как равенство двух полиномов над $O/\mathfrak{r}$, обозначим через $\mathfrak{R}$ радикал в P. В силу показанного выше теорема 6 сохраняет силу, если заменить равенство $=$ сравнением $\equiv \mod \mathfrak{R}$. По теореме 1 существуют такие j_1, j_2, что имеет место не только $j_1 + j_2 \equiv 1$, $j_1 j_2 \equiv 0$, но и $j_1 + j_2 = 1$, $j_1 j_2 = 0$; откуда (вследствие теоремы 4) $j_1, j_2 \in O$.

Пусть $j_1 \neq 0 \neq j_2$; обозначим через a_i (соотв. b_i) элементы $j_i f_i$ (соотв. $j_i g_i$), $i = 1, 2$. Имеем $a_i \,.\, b_i \equiv j_i$. По лемме 1 $a_i \,.\, b_i$ является делителем единицы в P_i; следовательно, a_i, b_i являются делителями единицы в P_i.

Так как $f_i \equiv a_i$, $g_i \equiv b_i$, получим

$$f_i = a_i + r_i, \; g_i = b_i + s_i,$$

где $r_i, s_i \in \mathfrak{R}$.

В силу $F \equiv f_1 + f_2 D$, $G \equiv g_2 + g_1 D$ имеет место

$$F = a_1 + r_1 + a_2 D + r_2 D + r_3 = a_1 + a_2 D + R,$$

$$G = b_2 + s_2 + b_1 D + s_1 D + s_3 = b_2 + b_1 D + S,$$

где $r_3, s_3, R, S \in \mathfrak{R}$.

Итак

$$j_1 D = j_1 F \cdot j_1 G = (a_1 + j_1 R)(b_1 D + j_1 S).$$

Так как a_1 — делитель единицы в P_1 и $j_1 R$ принадлежит радикалу из P_1, то легко видеть, что

$$c_1 = a_1 + j_1 R$$

является делителем единицы в P_1. Итак, существует $d_1 \in P_1$ такое, что $c_1 d_1 = j_1$, следовательно, $d_1 j_1 D = d_1 D = d_1 c_1 (b_1 D + j_1 S)$, иначе говоря

$$d_1 D = b_1 D + j_1 S.$$

Пусть $d_2 = b_2 + j_2 S$; аналогично существует $c_2 \in P_2$ такое, что $c_2 d_2 = j_2$. Так как $j_2 D = j_2 F \cdot j_2 G = (a_2 D + j_2 R)(b_2 + j_2 S)$, мы получим

$$c_2 D = a_2 D + j_2 R.$$

Итак, мы получаем $F = a_1 + j_1 R + a_2 D + j_2 R = c_1 + c_2 D$, $G = b_2 + j_2 S + b_1 D + j_1 S = d_2 + d_1 D$. Если подставить f_i, g_i вместо c_i, d_i, мы видим, что теорема 6 верна.

Пусть, например, $j_2 = 0$; мы можем применить тот же ход доказательства, если заменить все элементы из O_2 нулями.

Доказательство главной теоремы. Пусть O неприводимо, т. е. оно не содержит колец O_1, O_2 таких, что $O = O_1 \dotplus O_2$. В этом случае один из двух элементов j_1, j_2, например j_2, из теоремы 6 равен нулю и мы получаем $D = f_1 g_1 D$. Ввиду того, что D не является делителем нуля, мы имеем $1 = f_1 g_1$; следовательно, $F = f_1$ будет делителем единицы.

Пусть теперь O приводимо, $O = (j_1) \dot{+} (j_2)$. Пусть f_i, g_i таковы что $f_i, g_i \in (j_i)$, $f_i \cdot g_i = j_i$, $i = 1, 2$. Пусть b — свободный член полинома f_1. Если бы $F = f_1 + f_2 D$ было делителем единицы, то b было бы делителем единицы в O; это не верно, так как $b \in (j_1)$, поэтому b является делителем нуля. Итак, мы получаем разложение в смысле делимости.

Résumé.

La réductibilité du déterminant ayant des indéterminées pour élements, si l'on le considère comme un polynôme sur un anneau commutatif.

JAN MAŘÍK, Praha.

(Reçu le 8 Mars 1952.)

Considérons d'abord le déterminant D, dont les éléments x_{ik} sont algébriquement indépendents sur un champ d'intégrité 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 les 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 $P = O[x_{11}, x_{12}, \ldots, \ldots, x_{nn}]$. 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 est 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, les diviseurs de zéro et le radical de P, en supposant que l'anneau O soit connu; c'est-à-dire je démontre les théorèmes suivants ($\mathfrak{r}$, resp. $\mathfrak{R}$ désigne le radical de O, resp. P):

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

Théorème 2. $\mathfrak{R} = \mathfrak{r}[x_{11}, x_{12}, \ldots, x_{nn}]$.

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

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

Théorème 5. *Pour qu'un polynôme $f \in P$ soit un diviseur de zéro dans P, il faut et il suffit qu'il existe un $c \in O$, $c \neq 0$ tel que $cf = 0$.*