

АССОЦИАТИВНАЯ СИСТЕМА КВАДРАТНЫХ МАТРИЦ

(Представлено академиком А. Н. Колмогоровым 23 IV 1954)

Множество G_n всех квадратных матриц n -го порядка над произвольным полем P образует ассоциативную систему относительно умножения матриц. Гомоморфизмы этой системы рассмотрены И. Мальцевым ⁽¹⁾ и Н. Сиверцевой ⁽²⁾.

В настоящей заметке дана внутренняя характеристика системы G_n . Результатом является следующая теорема:

Теорема. Пусть 0 — нуль, а $e_1, e_2, \dots, e_n$ — попарно переместимые примитивные* идемпотенты системы G . Система G тогда и только тогда изоморфна системе G_n всех квадратных матриц порядка n над некоторым полем P с заданной мультипликативной группой**, когда:

I. Подсистема $e_1 G e_1 \subset G$ изоморфна мультипликативной системе поля P . Для каждого e_k существует пара элементов $x_k \in G e_k$, $x_k \in G$ такая, что $x_k x_k = e_1$.

II. Для каждого примитивного идемпотента e системы G существует такой элемент $z \in G$ ($z \neq 0$), что $ze = 0$.

III. Каковы бы ни были n^2 элементов $x_{ik} \in e_i G e_k$ ($i, k = 1, 2, \dots, n$), существует (и только один) элемент $x \in G$ такой, что $e_i x e_k = x_{ik}$.

Необходимость условий I—III очевидна: в качестве e_i ($i = 1, 2, \dots, n$) можно взять матрицы, у которых i -й элемент главной диагонали равен 1, а все остальные элементы равны нулю.

Доказательство достаточности следует из приведенных ниже лемм 1—6, где G — произвольная система, удовлетворяющая условиям теоремы.

Пусть 1 — единица, а 0 — нуль поля P . Вследствие I каждый элемент подсистемы $e_1 G e_1$ можно обозначить через αe_1 , где $\alpha \in P$ ($1e_1 = e_1$, $0e_1 = 0$), причем $\alpha e_1 \cdot \beta e_1 = (\alpha \beta) e_1$. Кроме того, введем обозначения: $e_1 x_k e_k = e_{1k}$, $e_k x_k e_1 = e_{k1}$ (см. ⁽¹⁾) и

$$e_{i1} \cdot \alpha e_1 \cdot e_{1k} = \alpha e_{ik} \quad (1)$$

(вместо $1e_{ik}$ будем писать просто e_{ik}).

Лемма 1. При обозначениях (1) подсистема $e_i G e_k$ системы G ($i, k = 1, 2, \dots, n$) совпадает с множеством $\bigcup \alpha e_{ik}$ ($\alpha \in P$), причем $e_{ii} = e_i$, $0e_{ik} = 0$ и

$$\alpha e_{ij} \cdot \beta e_{jm} = (\alpha \beta) e_{im}, \quad \alpha e_{ij} \cdot \beta e_{km} = 0, \quad (j \neq k). \quad (2)$$

* Идемпотент $e \neq 0$ системы G называется примитивным, если в G не существует идемпотента e' ($e' \neq e$, $e' \neq 0$) такого, что $ee'e = e'$.

** Существуют неизоморфные поля с одной и той же мультипликативной группой, т. е. поля, изоморфные только относительно умножения ⁽³⁾.

Доказательство. По определению

$$e_{1k}e_{k1} = e_1, \quad e_{1k}e_k = e_{1k}, \quad e_k e_{k1} = e_{k1}. \quad (3)$$

Вследствие $\theta e_1 = 0$ и (1) получим $\theta e_{ik} = 0$. Обратно, если $\alpha e_{ik} = 0$, то из (3) следует, что $e_{1i} \cdot \alpha e_{ik} \cdot e_{k1} = \alpha e_1 = 0$, т. е. $\alpha = 0$.

Так как $e_i e_k = e_k e_i$ и e_i, e_k примитивны, то $e_i e_k = 0$ при $i \neq k$. Отсюда и из (1), (3) имеем (2). Из (1)–(3) и примитивности e_i получим, что $e_{ii} = e_i$.

Вследствие (1), (3) $\alpha e_{ik} \in e_i G e_k$ при любом $\alpha \in P$. Обратно, пусть $x \in e_i G e_k$. Тогда $e_{1i} x e_{k1} \in e_1 G e_1$, $e_{1i} x e_{k1} = \alpha e_1$, $x = e_i x e_k = e_{1i} (e_{1i} x e_{k1}) e_{1k} = e_{1i} \cdot \alpha e_1 \cdot e_{1k} = \alpha e_{ik}$. Если при этом $x' \in e_i G e_k$, $e_{1i} x e_{k1} = e_{1i} x' e_{k1}$, то $x' = x$. Лемма доказана.

Лемма 2. Пусть $a, b \in G$, $e_i a e_j = 0$ при $j \neq j(i)$, $e_j b e_k = 0$ при $j \neq j(k)$, где $j(i)$ ($j(k)$) — один из индексов $1, 2, \dots, n$. Тогда для любого элемента $x \in G$

$$e_i (ax) e_k = e_i a e_{j(i)} \cdot e_{j(i)} x e_k, \quad e_i (xb) e_k = e_i x e_{j(k)} \cdot e_{j(k)} b e_k.$$

Из $e_i^2 = e_i$ и $e_i e_k = 0$ при $i \neq k$ получим, что $e_k (e_i a) e_m = e_k (e_i a e_{j(i)}) e_m$ при $k, m = 1, 2, \dots, n$. Вследствие III $e_i a = e_i a e_{j(i)}$ и, аналогично, $b e_k = e_{j(k)} b e_k$. Отсюда непосредственно следуют оба равенства леммы.

Лемма 3. Если a, b — любые элементы из G , $e_i a e_k = \alpha_{ik} e_{ik}$, $e_i b e_k = \beta_{ik} e_{ik}$ ($i, k = 1, 2, \dots, n$), то

$$e_i (ab) e_k = f(\alpha_{i1} \beta_{1k}, \alpha_{i2} \beta_{2k}, \dots, \alpha_{in} \beta_{nk}), \quad (4)$$

где $f(\alpha_1, \alpha_2, \dots, \alpha_n)$ однозначна, определена всюду в P и не зависит от индексов i, k .

Доказательство. Пусть $\gamma_j, \delta_j, \lambda_j$ ($j = 1, 2, \dots, n$) — любые элементы из P , $\lambda_j \neq 0$. Из III и леммы 2 следует, что в G существуют такие элементы c, d, s, t , для которых: $e_i c e_j = \gamma_j e_{ij}$, $e_j d e_1 = \delta_j e_{j1}$, $e_j t e_j = \lambda_j e_{jj}$, $e_j s e_j = \lambda_j^{-1} e_{jj}$ и $e_k c e_j = e_j d e_k = 0$ при $k \neq 1$; $e_j t e_k = e_j s e_k = 0$ при $k \neq j$ ($j = 1, 2, \dots, n$). Тогда $cd \in e_1 G e_1$, т. е. $cd = \varphi(\gamma_1, \gamma_2, \dots, \gamma_n; \delta_1, \delta_2, \dots, \delta_n) e_{11}$. Однозначность функции φ следует из III и однозначности действия в G .

Из лемм 2 и 1 получим, что $e_1 (ct) e_j = \gamma_j \lambda_j e_{1j}$, $e_j (sd) e_1 = \lambda_j^{-1} \delta_j e_{j1}$, $e_i (cts) e_k = e_i c e_k$. Вследствие III $cts = c$ и

$$\varphi(\gamma_j; \delta_j) e_{11} = cd = ct \cdot sd = \varphi(\lambda_j \gamma_j; \lambda_j^{-1} \delta_j) e_{11}.$$

Таким образом,

$$\varphi(\gamma_1, \gamma_2, \dots, \gamma_n; \delta_1, \delta_2, \dots, \delta_n) = f(\gamma_1 \delta_1, \gamma_2 \delta_2, \dots, \gamma_n \delta_n).$$

Пусть i, k — любые из индексов $1, 2, \dots, n$. Взяв $\gamma_j = \alpha_{ij}$, $\delta_j = \beta_{jk}$, получим из III и леммы 2: $e_i a = e_{i1} c$, $b e_k = d e_{1k}$ и $e_i (ab) e_k = e_{i1} (cd) e_{1k}$, откуда и следует (4).

В леммах 4–6 a, b — такие элементы из G , что

$$e_i a e_j = \alpha_j e_{ij}, \quad e_j b e_i = e_{ji}, \quad e_k a e_j = e_j b e_k = 0 \text{ при } k \neq 1. \quad (5)$$

Лемма 4. Определенная в лемме 3 $f(\alpha_1, \alpha_2, \dots, \alpha_n)$ симметрическая функция своих аргументов.

Доказательство. Пусть $u \in G$, i — любой из индексов $2, 3, \dots, n$, $e_{1i} u e_i = e_{1i}$, $e_{ii} u e_i = e_{ii}$, $e_j u e_j = e_{jj}$ ($j \neq 1, i$); во всех остальных случаях $e_k u e_m = 0$.

Из леммы 2 следует, что

$$e_1 (ui) e_1 = \alpha_i e_{11}, \quad e_1 (ui) e_i = \alpha_i e_{1i}, \quad e_1 (ui) e_j = \alpha_j e_{1j} \quad (j \neq 1, i),$$

$$e_1 (ui^2) e_k = \alpha_k e_{1k}, \quad e_k (ub) e_1 = e_{k1} \quad (k = 1, 2, \dots, n).$$

Из III и из леммы 2 заключаем, что $au^2 = a$, поэтому $f(\alpha_1, \alpha_2, \dots, \alpha_n) e_{11} = ab = au \cdot ub = f(\alpha_1, \alpha_2, \dots, \alpha_{i-1}, \alpha_1, \alpha_{i+1}, \dots, \alpha_n) e_{11}$.
 Лемма 5. Пусть $\alpha, \beta, \lambda, \alpha_j$ — любые элементы из P . Тогда

$$f(\alpha, \theta, \theta, \dots, \theta) = \alpha, \quad (6)$$

$$f(\lambda\alpha_1, \lambda\alpha_2, \dots, \lambda\alpha_n) = \lambda f(\alpha_1, \alpha_2, \dots, \alpha_n), \quad (7)$$

$$f(\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n) = f(\alpha_1, \dots, f(\alpha_2, \alpha_3, \dots, \alpha_n, \theta), \theta, \dots, \theta), \quad (8)$$

$$f(f(\alpha, \beta, \theta, \dots, \theta), \gamma, \theta, \dots, \theta) = f(\alpha, f(\beta, \gamma, \theta, \dots, \theta), \theta, \dots, \theta). \quad (9)$$

Доказательство. Из леммы 2 получим, что

$$f(\alpha, \theta, \dots, \theta) e_{11} = \alpha e_{11} \cdot b = \alpha e_{11} \cdot e_1 b e_1 = \alpha e_{11};$$

$$(\lambda e_{11} \cdot a) e_j = \lambda e_{11} \cdot e_1 a e_j = \lambda \alpha_j e_{1j},$$

$$f(\lambda\alpha_1, \lambda\alpha_2, \dots, \lambda\alpha_n) e_{11} = (\lambda e_{11} \cdot a) b = \lambda e_{11} (ab) = \lambda e_{11} \cdot f(\alpha_1, \alpha_2, \dots, \alpha_n) e_{11}.$$

Таким образом, (6) и (7) доказаны. Пусть теперь $c, d \in G$, $e_1 c e_1 = e_{11}$, $e_j c e_2 = e_{j2}$ ($j \neq 1$), $e_j d e_1 = e_{j1}$ ($j = 1, 2$); во всех остальных случаях $e_j c e_k = 0$; $e_j d e_k = 0$. Применяя III и лемму 2, получим, что $cd = b$. Но из лемм 2 и 3 следует $e_1(ac) e_1 = \alpha_1 e_{11}$, $e_1(ac) e_2 = f(\theta, \alpha_2, \alpha_3, \dots, \alpha_n) e_{12}$, $e_1(ac) e_j = 0$ при $j \neq 1, 2$. Поэтому

$$f(\alpha_1, \alpha_2, \dots, \alpha_n) e_{11} = ab = ac \cdot d = f(\alpha_1, f(\theta, \alpha_2, \dots, \alpha_n), \theta, \dots, \theta) e_{11}.$$

Чтобы доказать (8), остается лишь применить лемму 4.

При $n > 2$ (9) непосредственно следует из (8) и леммы 4. При $n = 2$ (9) вытекает из равенства произведений $xu \cdot b$ и $x \cdot ub$, где $x, y, b \in G$; $e_1 x e_j = e_{1j}$, $e_j b e_1 = e_{j1}$ ($j = 1, 2$), $e_1 y e_1 = \alpha e_{11}$, $e_1 y e_2 = \beta e_{12}$, $e_2 y e_2 = \gamma e_{22}$, $e_2 x e_j = e_j b e_2 = e_2 y e_1 = 0$.

Лемма 6. Для всякого элемента $\alpha \in P$ существует такой элемент $\alpha' \in P$, что $f(\alpha, \alpha', \theta, \dots, \theta) = \theta$.

Доказательство. Используя III и леммы 1, 2, убедимся, что определенный в (5) элемент b является идемпотентом. Пусть $d^2 = d$, $bdb = d$. Тогда, вследствие $b e_k = 0$ при $k \neq 1$ и леммы 2,

$$e_i d e_k = e_i b d b e_k = 0 \text{ при } k \neq 1;$$

$$e_i d e_1 = e_i b d b e_1 = e_{i1} \cdot e_1 d e_1 \cdot e_{11} = e_{i1} \cdot \delta e_{11} = \delta e_{i1};$$

$$\delta e_{i1} = e_i \delta e_1 = e_i d^2 e_1 = e_i d e_1 \cdot e_1 d e_1 = \delta^2 e_{i1}.$$

$\delta^2 = \delta$. Если $\delta = \theta$, то $d = 0$; если $\delta = 1$, то $d = b$, т. е. b — примитивный идемпотент. Вследствие II в G существует такой элемент $z \neq 0$, что $zb = 0$. По крайней мере один из элементов $e_i z e_j = \alpha_{ij} e_{ij}$ отличен от нуля (иначе было бы $z = 0$). Если $\alpha_{km} \neq 0$, то из $e_k(zb) e_1 = f(\alpha_{k1}, \alpha_{k2}, \dots, \alpha_{km}, \dots, \alpha_{kn}) e_{k1} = 0$ и из лемм 5 и 4, обозначив $f(\alpha_{k1}, \alpha_{k2}, \dots, \alpha_{k, m-1}, \theta, \alpha_{k, m+1}, \dots, \alpha_{kn}) = \beta$, получим $f(\alpha_{km}, \beta, \theta, \dots, \theta) = \theta$.

Для любого элемента $\alpha \in P$ найдем γ из уравнения $\alpha_{km} \gamma = \alpha$. Вследствие (7) $f(\alpha, \beta \gamma, \theta, \dots, \theta) = \theta$. Лемма доказана.

Введем обозначение

$$f(\alpha, \beta, \theta, \dots, \theta) = \alpha + \beta \quad (\alpha, \beta \in P). \quad (10)$$

Из лемм 4—6 следует, что множество P относительно действия (10) и заданного в нем действия умножения является полем.

III и лемма 1 устанавливают взаимно-однозначное соответствие между элементами системы G и матрицами системы G_n над полем P : матрице $(\alpha_{ik}) \in G_n$ соответствует элемент $a \in G$, если $e_i a e_k = \alpha_{ik} e_{ik}$ ($i, k = 1, 2, \dots, n$).

Из (8) и леммы 3 следует изоморфизм систем G и G_n : если

$$e_i a e_k = \alpha_{ik} e_{ik}, \quad e_i b e_k = \beta_{ik} e_{ik} \quad (i, k = 1, 2, \dots, n),$$

то

$$e_i (ab) e_k = \left(\sum_{j=1}^n \alpha_{ij} \beta_{jk} \right) e_{ik}.$$

Харьковский государственный
педагогический институт
им. Г. С. Сковороды

Поступило
14 XII 1953

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

¹ А. И. Мальцев, ДАН, 90, № 3, 333 (1953). ² Н. Сиверцева, Матем. сборн., 24, № 1, 101 (1949). ³ А. К. Сушкевич, Зап. Харків. матем. т-ва, 4, 145 (1930).