ЗА РЕЛАЦИЈАТА ДИСТРИБУТИВНОСТ МЕЃУ АЛГЕБАРСКИТЕ ОПЕРАЦИИ

Год. збор. Филоз. фак., Прир.-мат. оддел, Скопје, 9 (1956), 23–29

1.

Во овој труд ќе разгледаме некои системи алгебарски операции во кои е дефинирана релацијата дистрибутивност, која не мора да биде универзална[1]). Случајот кога е последното исполнето, т. е. кога дистрибутивноста е универзална релација во даденият систем операции, е прилично исцрпно обработен во еден труд на В. Д. Белоусов ([1]).

Прво ќе се задржиме на некои познати работи од теоријата на алгебарските операции.

Дефиниција 1, 1. Бинарна алгебарска операција во множеството M е секое еднозначно пресликување $(x, y) \to z$ каде x, y и z се елементи од M, т. е. $x, y, z \in M$.

За пресликувањата од тој вид натаму ќе го употребуваме само зборот операција. Елементите од множеството во кое се дефинирани операциите ќе ги означуваме со мали латински слова, а операциите со големи, или пак со вообичаените симболи како „+“, „•“, „∘“. Со $A(x, y)$ $(x \circ y)$ ќе го обележуваме елементот од множеството M во кој се пресликува парот (x, y) со операцијата A („∘“).

Дефиниција 1, 2. Елементот α е лева (десна) нула за операцијата A ако $A(\alpha, x) = \alpha$ $(A(x, \alpha) = \alpha)$ за секое $x \in M$.

Дефиниција 1, 3. Елементот β е идентичен за операцијата B ако $B(x, \beta) = B(\beta, x) = x$ за секое $x \in M$.

Дефиниција 1, 4. Операцијата A е скратива со елементот a од лево (десно) ако од $A(a, x) = A(a, b)$ $(A(x, a) = A(c, a))$ — следува $x = b$ $(x = c)$ за секое $b \in M$ $(c \in M)$.

Од дадените дефиниции непосредно следува следната

Теорема 1, 1. Еден елемент не може да биде, во однос на иста операција, и идентичен и нулти. Ниедна операција не е скратива од лево (десно) со елемент што е за неа лева (десна) нула.

Во изнесената теорема, а и во текот на целата работа, претпоставуваме дека множеството во кое е дефиниран некој систем операции има барем 2 елементи.

Дефиниција 1,5. Операцијата A е лево (десно) дистрибутивна спрема операцијата B, ако $A[x, B(y, z)] = B[A(x, y), A(x, z)]$ $(A[B(x, y), z] = B[A(x, z), A(y, z)])$ за секоја тројка $x, y, z \in M$.

Во натамошната работа ние ќе претпоставуваме лева дистрибутивност, а при тоа ако е A дистрибутивна спрема B ќе пишуваме $A\, d\, B$. Добиените резултати можат лесно да се пренесат и на случајот кога дистрибутивноста е десна.

Примери:

1, 1. Сите операции од облик $A_q(x, y) = y\, x^{-1}\, q\, x$ дефинирани во некоја група G, каде секое $q \in G$ одредува една операција A_q, се меѓусебно, а и сами на себе дистрибутивни ([1], стр. 481).

1, 2. Операцијата множење од некое поле е дистрибутивна спрема собирањето, но кога полето има повеќе од 2 елементи, собирањето не е дистрибутивно спрема множењето и ни една од нив не е дистрибутивна спрема себе.

---

[1]) ρ е универзална релација во множеството F ако $x \rho y$ за секој пар $x, y \in M$ ([2], стр. 11).

Дефиниција 2, 1. Множеството операции Π е полудистрибутивен систем (ПДС), ако релациите $X\,d\,A; A\,d\,Y$ се решливи по X и Y во Π за секоја дадена операција $A\in\Pi$.

Примерот 1, 1 е очигледно ПДС, но 1, 2 не е, бидејќи не постои операција дистрибутивна спрема множењето нити операција спрема која е собирањето дистрибутивна.

Ќе дадеме уште два примера за ПДС-и.

Пример 2, 1. Множеството операции од облик $A_{\alpha,\beta,\gamma}(x,y)=\alpha x+\beta y+\gamma$ дефинирани во некое поле K, при што секоја тројка $\alpha,\beta,\gamma,\in K$ одредува една операција $A_{\alpha,\beta,\gamma}$, е ПДС.

Навистина, лесно се покажува дека $A_{\alpha,\beta,\gamma}\,d\,A_{\alpha',1-\alpha',0}$ и $A_{0,\beta'',\frac{\gamma(\beta''-1)}{\alpha+\beta-1}}\,d\,A_{\alpha,\beta,\gamma}$ за $\alpha+\beta-1\neq 0$, а $A_{\alpha'',1,\gamma''}\,d\,A_{\alpha,\beta,\gamma}$ за $\alpha+\beta-1=0$.

Пример 2, 2. Множеството операции од облик $A_a^{i,j}(x,y)=a\,x^i\,y^j$ дефинирани во некоја комутативна група G, каде секоја тројка a, i, j одредува една операција $A_a^{i,j}$, при што $a\in G$, а i и j се цели броеви е исто така ПДС.

Навистина, од

$$A_a^{i,j}\left[x, A_b^{r,s}(y,z)\right]=a\,b^j.\,x^i\,y^{rj}\,z^{sj},$$

$$A_b^{r,s}\left[A_a^{i,j}(x,y), A_a^{i,j}(x,z)\right]=b\,a^{r+s}\,x^{i(r+s)}\,y^{rj}\,z^{sj}$$

после изедначување на десните страни се добиваат релациите

$$(1)\qquad a^{r+s-1}=b^{j-1},\quad x^{i(r+s-1)}=e,$$

(e е идентичниот елемент на групата). Ако ставиме $r+s-1=0$, $b=e$ релациите (1) ќе бидат, очигледно, исполнети, т. е. $A_a^{i,j}\,d\,A_e^{r,1-r}$. На ист начин се покажува дека $A_a^{0,i+j}\,d\,A_a^{i,j}$.

Обично при дадена тројка a, i, j постојат повеќе тројки b, r, s што ги задоволуваат релациите (1). Така например, ако G е периодична група и ако постои заеднички содржател n од редовите на сите елементи од G, втората од релациите (1) може да се замени со

$$(1')\qquad i(r+s-1)\equiv 0\pmod{n}.$$

Секое множество операции Π може да се смета за ПДС, оти ако тоа не е исполнето, проширувајќи го Π со операцијата E дефинирана со $E(x,y)=y$ добиваме ПДС, бидејќи $E\,d\,A$ и $A\,d\,E$, за секоја операција A. Спрема тоа не е од интерес проучувањето на најопштите ПДС-и.

Ќе се задржиме сега на случајот кога во множеството M се дефинирани три операции A, B и C.

Теорема 2, 1. Од: 1° $A\,d\,B$, $B\,d\,C$; 2° M има идентичен елемент f во однос на B, а e во однос на C; 3° B е скратива од десно со секој елемент $\neq e$, а C од лево со секој елемент од M – следува 4° $A(a,e)=e$, или 5° $A(a,x)=f$, за секое $x\in M$ при дадено $a\in M$.

Доказ. Прво ќе покажеме дека $B(x,e)=e$ (*). Навистина, од 1° и 2° следува $C[B(x,e),e]=B(x,e)=B[x,C(e,e)]=C[B(x,e)\,B(x,e)]$ од каде, спрема 3° се добива (*). На ист начин добиваме $B[f,A(a,e)]=A(a,e)=A[a,B(x,e)]=B[A(a,x),A(a,e)]$ т. е. $B[f,A(a,e)]=B[A(a,x),A(a,e)]$ (**). Ако $A(a,e)=e$, спрема (*) е исполнето и (**), но ако $A(a,e)\neq e$ може во (**) да се скрати со $A(a,e)$ и се добива $A(a,x)=f$.

Пример 2, 3. Ако во дадено поле K, покрај операциите собирање ($+$) и множење ($\bullet$), дефинираме нова операција „$\square$“ со релациите $a\square b=1$ за $b\neq 0$, $a\square 0=0$, добиваме систем операции „$\square$“, „$\bullet$“, „$+$“, што ги задоволуваат условите 1°, 2°, 3° и 4°, а и 5° за $x\neq 0$.

Пример 2, 4. Операциите „□“, „•“, „+“, ќе ги задоволуваат условите 1°, 2°, 3° и 5°, но не и 4°, ако операцијата „□“ ја дефинираме со $a \square b = 1$.

Со проширување на условите од последната теорема може да се уреди една од операциите да биде наполно одредена.

Теорема 2, 2. Од: 1° $A\,d\,B$, $A\,d\,C$, $B\,d\,C$, при што последната дистрибутивност е и лева и десна, 2° M е поле во однос на операциите A и C со карактеристика $p \neq 2$ — следува 3° $B(x, y) = 0$.

Доказ. Ги внесуваме ознаките $A \equiv$ „•“, $B \equiv$ „□“, $C \equiv$ „+“. Нека $a \square b = \alpha$. Спрема 1° и 2° добиваме $2 \bullet \alpha = a \square b + a \square b = a \square (2 \bullet b)$ и $4 \bullet \alpha = a \square (2 \bullet b) + a \square (2 \bullet b) = (2 \bullet a) \square (2 \bullet b) = 2 \bullet (a \square b) = 2 \bullet \alpha$, од каде следува $\alpha = 0$.

На конкретен пример ќе покажиме дека, кога полето има карактеристика $p = 2$, може да биде и $a \square b \neq 0$.

Пример 2, 5. Нека $M = \{0, 1, \alpha, \alpha^2\}$ е полето $GF(4)$ каде операциите собирање и множење се дефинирани со таблиците

•	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

+	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

и нека во M дефинираме уште две операции, „□“ и „Δ“, со таблиците

□	0	1	α	α^2
0	0	0	0	0
1	0	1	α^2	α
α	0	α^2	α	1
α^2	0	α	1	α^2

Δ	0	1	α	α^2
0	0	0	0	0
1	0	α	1	α^2
α	0	1	α^2	α
α^2	0	α^2	α	1

Лесно се покажува дека „•“ d „□“, „•“ d „Δ“, „•“ d „+“, „□“ d „+“, „Δ“ d „+“, од коешто следува дека тројката операции „•“, „□“, „+“ („•“, „Δ“, „+“) ги задоволува условите од последната теорема и покрај тоа што не е $x \square y = 0$ ($x \Delta y = 0$).

Сличен пример за полињата со 2, 8, 16 и 32 елементи не може да се даде, а веројатно тоа не може да се направи со било кое поле што е различно од полето $GF(4)$.

При извесни услови, една од операциите може да биде наполно одредена и кога се земени во обзир само две операции, што се гледа например од следната

Теорема 2, 3. Од: 1° „□“ d „∘“, „∘“ d „□“; 2° M е група во однос на операцијата „∘“ со идентичен елемент e – следува 3° $x \square y = y$.

Доказ. Од 1° и 2° очигледно следува $x \square e = e$, од каде добиваме $x \square y = (e \circ x) \square (y \circ e) = [(y \circ y^{-1}) \circ x] \square (y \circ e) = [y \circ (y^{-1} \circ x)] \square (y \circ e) = y \circ [(y^{-1} \circ x) \square e] = y \circ e = y$.

Сега ќе разгледаме еден вид ПДС-и во кои релацијата дистрибутивност дефинира обратно еднозначно пресликување.

Дефиниција 2, 2. ПДС Π е еднозначно дистрибутивен (ЕДС), ако релациите $X\,d\,A$, $A\,d\,Y$ имаат еднозначно одредени решенија $X, Y \in \Pi$ кога $A \in \Pi$ е дадена операција.

Дефиниција 2, 3. Подсистем од ЕДС Π е секое подмножество $\Pi' \subseteq \Pi$ што е и самото ЕДС.

Дефиниција 2, 4. ЕДС Π е прост (ПЕДС) ако не содржи прави подсистеми.

Како што е познато, при секое обратно еднозначно пресликување φ на некое множество F во себе, тоа се разложува на дисјунктни класи од облик $\{a_1, a_2, a_3 \ldots a_{n-1}, a_n\}$ каде $\varphi(a_i) = a_{i+1}$ за $i < n$, а $\varphi(a_n) = a_1$ и $\{\ldots a_{-n}, \ldots a_{-1}, a_0, a_1, \ldots a_n \ldots\}$ каде $\varphi(a_i) = a_{i+1}$. Од тоа, бидејќе дистрибутивноста кај ЕДС-и е пресликување од тој вид, следува точноста на следната.

Теорема 2, 4. Секој ЕДС, што не е прост, може да се разложи на дисјунктни прости подсистеми. Секој бесконечен (конечен) ПЕДС може да се подреди слично на целите броеви (циклично), а при тоа секоја операција да биде дистрибутивна на наредната.

Оваа теорема ни укажува на тоа дека изучувањето на ЕДС-и може да се спроведи, во главно со разгледувањето на нивните прости подсистеми.

Од теоремата 2, 3 непосредно следува дека, ако во множеството M две операции чинат ПЕДС, M не може да биде група во однос на една од нив.

На крајот, на еден пример, ќе покажеме дека може да се реализира ПЕДС со произволен број операции.

Пример 2, 6. Нека G е комутативна група со ред $n = p_1 \cdot p_2 \cdots p_{k-1} \cdot p_k$ каде p_i се различни прости броеви. Множеството операции $\Pi = \{A_1, A_2, \cdots, A_{k-1}, A_k\}$ дефинирани со $A_\nu(x, y) = a_\nu\, x^{p_\nu}\, y^{\frac{n}{p_{\nu-1}} - p_\nu + 1}$, при што a_ν е елемент од G со ред $p_{\nu-1}$ $(p_0 = p_k)$, е ПЕДС.

Ќе покажеме дека $A_\nu\, d\, A_{\nu+1}$ и дека релацијата $A_\nu\, d\, A_\mu$ не е задоволена во ниеден друг случај. Навистина, ако ставиме $a_\nu = a$, $p_\nu = i$, $\frac{n}{p_{\nu-1}} - p_\nu + 1 = j$, $a_{\nu+1} = b$, $p_{\nu+1} = r$, $\frac{n}{p_\nu} - p_{\nu+1} + 1 = s$, добиваме $r + s - 1 = \frac{n}{p_\nu}$, т. е. $i(r+s-1) \equiv 0 \pmod n$, а исто и $b^{i(j-1)} = a^{r+s-1} = e$, од коешто следува дека $A_\nu\, d\, A_{\nu+1}$, оти се задоволени релациите (1) од примерот 2, 2. При истото значение на a, i, j, ако означиме $r = p_\mu$, $s = \frac{n}{p_{\mu-1}} - p_\mu + 1$, добиваме $r + s - 1 = \frac{n}{p_{\mu-1}}$ т. е. $i(r+s-1) = \frac{p_\nu \cdot n}{p_{\mu-1}} \not\equiv 0 \pmod n$ за $\mu \neq \nu - 1$, а од тоа следува дека не е $A_\nu\, d\, A_\mu$. Значи Π е ПЕДС со k операции.

ЛИТЕРАТУРА

[1] В. Д. Белоусов: О дистрибутывных системах операций, Матем. сб. т. 36 (1955), № 3, 479—500, Москва.

[2] P. Dubreil: ALGEBRE tome I, Paris, 1954.

ON THE RELATION DISTRIBUTIVITY BETWEEN BINARY OPERATIONS
(Summary)

1. We shall consider here some sets of binary operations in which the relation distributivity is defined.

M denotes the set in which certain operations are defined, while its elements are denoted with $a, b, c, \cdots, \alpha, \beta, \gamma, \cdots, x, y, z \cdots$; Π is a set of operations: $A, B, C, \cdots, X, Y, Z, \cdots$ „$\bullet$“, „$+$“, „$\circ$“; $(M; \Pi)$ is the system of the set M and of the set Π of the operations which are defined in M.

Definitions 1, 1.

a) α *is a left identity element (zero) for* A *if* $A(\alpha, x) = x$ $(A(\alpha, x) = \alpha)$ *for every* x; *a right identity element (zero) can be defined similarly.*

b) B *is left (right) cancelable with* b, *if from* $B(b, x) = B(b, y)$ $(B(z, b) = B(u, b))$ — *it follows* $x = y$ $(z = u)$.

Definition 1, 2. A *is left (right) distributive according to* B, *if* $A[x, B(y, z)] = B[A(x, y), A(x, z)]$ $(A[B(x, y), z] = B[A(x, z), A(y, z)])$ *for every triple* x, y, z.

AdB denotes that A is left distributive according to B.

It is easy to see that this is correct:

Theorem 1, 1. *From the propositions:* 1° AdB; 2° β *is a left (right) identity element for* B; 3° B *is right (left) cancelable with every element of* M — *it follows:* 4° β *is a right zero for* A.

2. Here we consider some systems of the form $(M; A, B)$ and $(M; A, B, C)$.

Theorem 2, 1. *From the propositions:* 1° AdB, BdA; 2° $(M; A)$ *is a group* — *it follows:* 3° *every* $y \in M$ *is a right zero for* B.

Proof. Let α be the identity element of the group, and x^{-1} the inverse element for x. According to the above propositions we obtain:

$B(x, y) = B[A(\alpha, x), A(y, \alpha)] = B\{A[A(y, y^{-1}), x], A(y, \alpha)\} = B\{A[y, A(y^{-1}, x)], A(y, \alpha)\} = A\{y, B[A(y^{-1}, x), \alpha]\} =$ (according to the theorem 1, 1) $= A(y, \alpha) = y$.

Theorem 2, 2. *From the proposition:* 1° AdB, BdC; 2° $\beta(\gamma)$ *is a left (right) identity element for* $B(C)$; 3° $B(C)$ *is right (left) cancelable with every element* $b \neq \gamma$ (c) — *it follows:* 4° $A(a, \gamma) = \gamma$, *or* 5° $A(a, x) = \beta$ *for every* x, *if* a *is given.*

Proof. According to the propositions: 1° and 2° we obtain $B[\beta, A(a, \gamma)] = A(a, \gamma) =$ (according to the theorem 1, 1) $= A[a, B(x, \gamma)] = B[A(a, x), A(a, \gamma)]$ from which, if $A(a, \gamma) \neq \gamma$, according to the proposition 3°, it follows $A(a, x) = \beta$.

Theorem 2, 3. *From the propositions:* 1° AdB, AdC, BdC, *where the last distributivity is both left and right;* 2° $(M; A, C)$ *is a field with characteristic* $p \neq 2$ — *it follows:* 3° $B(x, y) = 0$, *where* 0 *is the zero of the field.*

Proof. Let $A \equiv$ „$\bullet$“, $B \equiv$ „$\circ$“, $C \equiv$ „$+$“, and $x \circ y = z$. According te the above propositions we obtain $2 \bullet z = x \circ y + x \circ y = x \circ (y + y) = x \circ (2 \bullet y)$, also $4 \bullet z = x \circ (2 \bullet y) + x \circ (2 \bullet y) = (x + x) \circ (2 \bullet y) = (2 \bullet x) \circ (2 \bullet y) = 2 \bullet (x \circ y) = 2 \bullet z$; hence it follows $z = 0$.

Example 2, 1. Let M be the field $GF(4) = \{0, 1, \alpha, \alpha^2\}$, in which, beside the addition $(+)$ and the multiplipllication $(\bullet)$, a new operation „$\circ$“ is being defined with: $x \circ 0 = 0 \circ x = 0$; $x \circ x = x$; $x \circ y = x + y$, if $x \bullet y \neq 0$ and $x \neq y$. Thus, we obtain a triple „$\bullet$“, „$\circ$“, „$+$“ which satisfies the proposition 1° and 2° also, except for characteristic, although it is not always $x \circ y = 0$.

3. **Definition 3, 1.** $(M; \Pi)$ *is a semidistiburive system* (SDS), *if the relations* XdA, AdY *are solvable in* Π *for given* $A \in \Pi$.

Example 3, 1. Let M be a commutative group, and Π the set of the operations which are defined with $A_a^{i,j}(x, y) = a x^i y^j$, where $a \in M$, and i, j are integers. The system $(M; \Pi)$ is a SDS; the relation $A_a^{i,j} d A_b^{r,s}$ is correct if $a^{r+s-1} = b^{j-1}$ and $i(r+s-1) \equiv 0 \pmod{n}$, where n is a common multiple of orders of all elements, and $n = 0$, if such common multiple does not exist.

In cases where M is a cyclic group with order $n = p_1 p_2 \cdots p_{k-1} p_k$, where p_i are different prims, we give the example 3,2 in which the distributivity is an ordered relation, and the example 3,3 where the distributivity defines a one-one mapping in Π.

Example 3,2 (3,3). Let $\Pi = \{A_1, A_2, A_3 \cdots A_{k-1}, A_k\}$, where

$$A_\nu(x, y) = a_\nu x^{\prod_\nu^k p_i} \cdot y^{n - \prod_\nu^k p_i + 1} \left(A_\nu(x, y) = a_\nu x^{p_\nu} y^{\frac{n}{p_{\nu-1}} - p_\nu + 1} \right)$$

and $a_\nu \in M$ is of the order $\prod_\nu^k p_i$ $(p_{\nu-1}, p_0 \equiv p_k)$. It can be easely seen that the relation $A_\nu \, d \, A_\mu$ is correct only if $\nu \leqslant \mu$ $(\nu = \mu - 1)$.

The considerations of general SDS is of no interest, because every system becomes SDS if the set Π is extended by the operation E defined with $E(x, y) = y$.