ON THE DISTRIBUTIVE LAW[1]

WU-YI HSIANG

1. **Introduction.** In the theory of rings, the two distributive laws give the only relations between addition and multiplication, and play an important role in the whole theory. The purpose of this paper is to give a full discussion of distributive law in its generalized form.

If the following equation

$$\begin{aligned}(x_1 + \cdots + x_m)(y_1 + \cdots + y_n) = {} & x_1y_1 + \cdots + x_1y_n \\ & + x_2y_1 + \cdots + x_2y_n \\ & + \cdots \\ & + x_my_1 + \cdots + x_my_n \quad (m, n \text{ fixed}),\end{aligned}$$

holds for all members x_i, y_j of an algebraic system $(R, +, \cdot)$ with two binary operations, we say that the (m, n)-distributive law holds in $(R, +, \cdot)$, and this identity will be denoted by $D_{m,n}$ hereafter.

DEFINITION. An abelian group R, closed with respect to multiplication, is called an (m, n)-distributive ring if the (m, n)-distributive law holds in $(R, +, \cdot)$ for fixed m and n. Here, we follow the definition given by Professor R. A. Beaumont in his paper, *Generalized rings* [1], but we do not require m, n to be greater than or equal to 2.

By a ring, we mean a not necessarily associative ring. Thus a ring is an (m, n)-distributive ring for every (m, n); an (m, n)-distributive ring, however, is not necessarily a ring.

2. FIRST FUNDAMENTAL THEOREM. *Corresponding to an (m, n)-ring $(R, +, \cdot)$, $m, n \geqq 2$, there exists a ring $(R, +, *)$ with the same domain and addition, and*

$$a * b = a\cdot b - a\cdot 0 - 0\cdot b + 0\cdot 0 \qquad \textit{for all } a, b \textit{ in } R.$$

Moreover, if we take $e = 0\cdot 0$, and $\lambda(a) = 0\cdot a - 0\cdot 0$, $\rho(a) = a\cdot 0 - 0\cdot 0$ for all a in R, then

(i) $\quad (mn - 1)e = 0, \quad (m - 1)\lambda(a) = 0, \quad (n - 1)\rho(a) = 0.$

(ii)
$$\begin{aligned}\lambda(a + b) &= \lambda(a) + \lambda(b), \\ \rho(a + b) &= \rho(a) + \rho(b).\end{aligned}$$

Conversely, if $(R, +, *)$ is a ring with an element e and two maps

Received by the editors January 28, 1959 and, in revised form, August 1, 1959.

[1] Some of the results of this paper have been obtained independently by T. Saitô of Tokyo, Japan.

λ, ρ of R into R which satisfy the above two equations, then there exists an (m, n)-distributive ring with the same addition, such that,

$$a\cdot b = a * b + \rho(a) + \lambda(b) + e$$

and

$$e = 0\cdot 0, \qquad \rho(a) = a\cdot 0 - 0\cdot 0, \qquad \lambda(a) = 0\cdot a - 0\cdot 0.$$

PROOF. We can easily check the following identities by direct computation:

1. $(mn-1)e=0$, $(m-1)\lambda(a)=0$, $(n-1)\rho(a)=0$.
2. $a\cdot(b+c)=a\cdot b+a\cdot c-a\cdot 0$, $(b+c)\cdot a=b\cdot a+c\cdot a-0\cdot a$.

Let $a * b=a\cdot b-a\cdot 0-0\cdot b+0\cdot 0$ for all a, b in R, then

3. $$\begin{aligned}(a+b) * c &= (a+b)\cdot c-(a+b)\cdot 0-0\cdot c+0\cdot 0\\ &= (a\cdot c+b\cdot c-0\cdot c)-(a\cdot 0+b\cdot 0-0\cdot 0)-0\cdot c+0\cdot 0\\ &= (a\cdot c-a\cdot 0-0\cdot c+0\cdot 0)+(b\cdot c-b\cdot 0-0\cdot c+0\cdot 0)\\ &= a * c+b * c,\end{aligned}$$

and similarly, $a * (b+c)=a * b+a * c$. Hence, $(R, +, *)$ is a ring with the same addition and multiplication defined as stated.

We have seen above that the element e and the maps λ and ρ satisfy (i), and it is routine to check that (ii) is satisfied.

For the converse, if $(R, +, *)$ is a ring with an element e and two maps λ, ρ of R into R, which satisfy the conditions (i), (ii), we can easily define another triple $(R, +, \cdot)$ by

$$a\cdot b = a * b + \lambda(b) + \rho(a) + e.$$

Then,

(a) $\lambda(0) = \rho(0) = 0$ (by (ii)) and $0\cdot 0 = e$.

(b) $a\cdot 0 = a * 0 + \rho(a) + \lambda(0) + e$ or $\rho(a) = a\cdot 0 - 0\cdot 0$.

(c) $0\cdot b = 0 * b + \rho(0) + \lambda(b) + e$ or $\lambda(b) = 0\cdot b - 0\cdot 0$.

(d) $$\begin{aligned}&(a_1 + \cdots + a_m)\cdot(b_1 + \cdots + b_n)\\ &\quad = (a_1 + \cdots + a_m) * (b_1 + \cdots + b_n) + \lambda(b_1 + \cdots + b_n)\\ &\qquad + \rho(a_1 + \cdots + a_m) + e\\ &\quad = \sum a_i * b_j + \lambda(b_1) + \cdots + \lambda(b_n) + \rho(a_1) + \cdots + \rho(a_m)\\ &\qquad + e\\ &\quad = \sum (a_i * b_j + \lambda(b_j) + \rho(a_i) + e)\\ &\qquad - (m-1)\lambda(b_1) - \cdots - (m-1)\lambda(b_n)\\ &\qquad - (n-1)\rho(a_1) - \cdots - (n-1)\rho(a_m) - (mn-1)e\\ &\quad = \sum a\cdot b_j \qquad\qquad (i = 1, \cdots, m; j = 1, \cdots, n).\end{aligned}$$

i.e. $(R, +, \cdot)$ thus defined is a (m, n)-ring with the desired properties. q.e.d.

COROLLARY 1. *$(R, +, \cdot)$ is associative if and only if $(R, +, *)$ is associative and the additional condition*

$$\text{(iii)}\quad \begin{aligned}&[\rho(a)*c+\lambda(b)*c+e*c+\rho(a*b)+\rho^2(a)+\rho\lambda(b)+\rho(e)+\lambda(c)]\\ &-[a*\rho(b)+a*\lambda(c)+a*e+\rho(a)+\lambda(b*c)\\ &\qquad+\lambda\rho(b)+\lambda^2(c)+\lambda(e)]=0\end{aligned}$$

is satisfied.

PROOF. 1.

$$\begin{aligned}(a*b)*c &= (a\cdot b-a\cdot 0-0\cdot b+0\cdot 0)*c\\ &= (a\cdot b)*c-(a\cdot 0)*c-(0\cdot b)*c+(0\cdot 0)*c\\ &= [(a\cdot b)\cdot c-(a\cdot b)\cdot 0-0\cdot c+0\cdot 0]\\ &\quad-[(a\cdot 0)\cdot c-(a\cdot 0)\cdot 0-0\cdot c+0\cdot 0]\\ &\quad-[(0\cdot b)\cdot c-(0\cdot b)\cdot 0-0\cdot c+0\cdot 0]\\ &\quad+[(0\cdot 0)\cdot c-(0\cdot 0)\cdot 0-0\cdot c+0\cdot 0]\\ &= (a\cdot b)\cdot c-(a\cdot b)\cdot 0-(a\cdot 0)\cdot c-(0\cdot b)\cdot c\\ &\quad+(a\cdot 0)\cdot 0+(0\cdot b)\cdot 0+(0\cdot 0)\cdot c-(0\cdot 0)\cdot 0,\\ a*(b*c) &= a*(b\cdot c-b\cdot 0-0\cdot c+0\cdot 0)\\ &= a*(b\cdot c)-a*(b\cdot 0)-a*(0\cdot c)+a*(0\cdot 0)\\ &= a\cdot(b\cdot c)-a\cdot(b\cdot 0)-a\cdot(0\cdot c)-0\cdot(b\cdot c)\\ &\quad+a\cdot(0\cdot 0)+0\cdot(b\cdot 0)+0\cdot(0\cdot c)-0\cdot(0\cdot 0).\end{aligned}$$

Thus, by means of the associativity of the operation "$\cdot$", we get $(a*b)*c=a*(b*c)$, the associativity of "$*$". And it is routine to check that (iii) holds when "$\cdot$" is associative.

2. If "$*$" is associative and if e, λ, ρ satisfy the additional condition (iii) besides (i), (ii), then it is obvious that $(R, +, \cdot)$ is an associative (m, n)-distributive ring.

3. SECOND FUNDAMENTAL THEOREM. *Let*

$$[(m_1, n_1), \cdots, (m_i, n_i), \cdots]$$

and $[(h_1, k_1), \cdots, (h_j, k_j), \cdots]$ be collections of ordered pairs of positive integers. For all algebraic systems $(R, +, \cdot)$ which are abelian groups under addition,

$(R, +, \cdot)$ *satisfies* $\{D_{m_1, n_1}, \cdots, D_{m_i, n_i}, \cdots\}$ *implies* $(R, +, \cdot)$

satisfies $\{D_{h_1,k_1}, \cdots, D_{h_j,k_j}, \cdots\}$ *if and only if*

$$(m_1 - 1, \cdots, m_i - 1, \cdots) \supseteq (h_1 - 1, \cdots, h_j - 1, \cdots),$$
$$(n_1 - 1, \cdots, n_i - 1, \cdots) \supseteq (k_1 - 1, \cdots, k_j - 1, \cdots),$$
$$(m_1n_1 - 1, \cdots m_in_i - 1, \cdots) \supseteq (h_1k_1 - 1, \cdots, h_jk_j - 1, \cdots).$$

By $(a, b, \cdots)$ we mean the ideal generated by $a, b, \cdots$ or the greatest common divisor of $a, b, \cdots$.

PROOF. We first prove the sufficiency. Let $(R, +, \cdot)$ be any abelian group, closed with respect to multiplication, and moreover, $D_{m_1, n_1}, \cdots, D_{m_i, n_i}, \cdots$ also hold.

There are only four possibilities, namely,

(i) $(m_1-1, m_2-1, \cdots)=(0)$ and $(n_1-1, n_2-1, \cdots)=(0)$,

(ii) $(m_1-1, m_2-1, \cdots)\neq(0)$ and $(n_1-1, n_2-1, \cdots)\neq(0)$,

(iii) $(m_1-1, m_2-1, \cdots)=(0)$ but $(n_1-1, n_2-1, \cdots)\neq(0)$,

(iv) $(m_1-1, m_2-1, \cdots)\neq(0)$ but $(n_1-1, n_2-1, \cdots)=(0)$.

In first case, $(m_1-1, m_2-1, \cdots)=(0)=(n_1-1, n_2-1, \cdots)$, we have $h_j=k_j=1$, for all j, so that $(R, +, \cdot)$ satisfies $\{D_{h_1,k_1}, D_{h_2,k_2}, \cdots\}$, trivially.

If $(m_1-1, m_2-1, \cdots)\neq 0$ and $(n_1-1, n_2-1, \cdots)\neq 0$, in this case, there exists at least one m, say m_1, greater than one, if $n_1>1$, then $(R, +, \cdot)$ is an (m_1, n_1)-distributive ring. If $n_1=1$, then there must exist another n, say n_2, greater than one, if $m_2>1$, then $(R, +, \cdot)$ is an (m_2, n_2)-distributive ring; if $m_2=1$, then $D_{m_1,1}$ and D_{1,n_2} hold, and hence D_{m_1,n_2} also holds, and $(R, +, \cdot)$ is an (m_1, n_2)-distributive ring.

After all, there exists a corresponding ring $(R, +, *)$ with $a * b = a\cdot b - a\cdot 0 - 0\cdot b + 0\cdot 0$ as we have proved in First Fundamental Theorem.

It follows from D_{m_i,n_i} for fixed i, that

$$(m_in_i - 1)e = 0,$$
$$(m_i - 1)\lambda(a) = 0,$$
$$(n_i - 1)\rho(a) = 0.$$

We have, therefore, if

$$(m_1 - 1, m_2 - 1, \cdots) = (d_1),$$
$$(n_1 - 1, n_2 - 1, \cdots) = (d_2),$$
$$(m_1n_1 - 1, m_2n_2 - 1, \cdots) = (d_3),$$

then $d_3e=0$, $d_2\rho(a)=0$, $d_1\lambda(a)=0$.

Now, we can show that D_{h_j,k_j} also holds in $(R, +, \cdot)$. Since

$$(h_j - 1) \in (d_1),$$
$$(k_j - 1) \in (d_2),$$
$$(h_j k_j - 1) \in (d_3),$$

we can easily see that

$$(h_j - 1)\lambda(a) = 0, \qquad (k_j - 1)\rho(a) = 0,$$

and

$$(h_j k_j - 1)e = 0.$$

But, by definition of $(R, +, *)$, $a \cdot b = a * b + \rho(a) + \lambda(b) + e$ for all a, b in R, so that

$$(a_1 + \cdots + a_{h_j}) \cdot (b_1 + \cdots + b_{k_j}) = \sum a_s \cdot b_t$$

as in (d) of the First Fundamental Theorem.

If $$(m_1 - 1, \cdots, m_i - 1, \cdots) = (0)$$

and

$$(n_1 - 1, \cdots, n_i - 1, \cdots) \neq (0),$$

then $m_i = 1$ for all i and $n_i \geqq 2$ for some i.

Let $(R, +, \cdot)$ be an algebraic system such that $(R, +)$ is an abelian group and $D_{1,n_1}, \cdots, D_{1,n_i}, \cdots$ hold.

Then, $a \cdot 0 = a \cdot (n_i 0) = n_i(a \cdot 0)$, or $(n_i - 1)(a \cdot 0) = 0$.

$$\begin{aligned} a \cdot (b + c) &= a \cdot (b + c + (n_i - 2)0) \\ &= a \cdot b + a \cdot c + (n_i - 2)(a \cdot 0) \qquad (1) \\ &= a \cdot b + a \cdot c - a \cdot 0. \end{aligned}$$

Define $a * b = a \cdot b - a \cdot 0$, and, we have, by (1), $a * (b + c) = a * b + a * c$.

Put $(n_1 - 1, \cdots, n_i - 1, \cdots) = (d_1)$. Then,

$$\begin{aligned} &(m_1 n_1 - 1, \cdots, m_i n_i - 1, \cdots) \\ &\qquad = (1 \cdot n_1 - 1, \cdots, 1 \cdot n_i - 1, \cdots) = (d_1), \end{aligned}$$

and $d_1(a \cdot 0) = 0$, for all a in R. Since $(h_1 - 1, \cdots, h_j - 1, \cdots) \subseteq (m_1 - 1, \cdots, m_i - 1, \cdots) = (0)$, and $(k_1 - 1, \cdots, k_j - 1, \cdots) \subseteq (d_1)$, we have $h_j = 1$ and $(k_j - 1) \in (d_1)$. But,

$$\begin{aligned} a \cdot (b_1 + \cdots + b_{k_j}) &= a * (b_1 + \cdots + b_{k_j}) + a \cdot 0 \\ &= a * b_1 + \cdots + a * b_{k_j} + a \cdot 0 \\ &= a \cdot b_1 + \cdots + a \cdot b_{k_j} - (k_j - 1)a \cdot 0 \\ &= a \cdot b_1 + \cdots + a \cdot b_{k_j}, \end{aligned}$$

i.e., $D_{h_j,k_j} \equiv D_{1,k_j}$ holds in $(R, +, \cdot)$ for all j.

Now it is obvious that the fourth part can be proved in just the same way.

For the proof of necessity, we construct the following example.

Let d_1, d_2, d_3 be the greatest common divisors of (m_i-1), (n_i-1), (m_in_i-1), respectively, and let Π be the ring of integers, $\Pi_d = \Pi/(d)$.

Let $G = \{(n, i, j, k) \mid n \in \Pi,\ i \in \Pi_{d_1},\ j \in \Pi_{d_2},\ k \in \Pi_{d_3}\}$, and define $(n_1, i_1, j_1, k_1) + (n_2, i_2, j_2, k_2) = (n_1+n_2, i_1+i_2, j_1+j_2, k_1+k_2)$,

$$\rho(n, i, j, k) = (0, 0, n+j, 0),$$
$$\lambda(n, i, j, k) = (0, n+i, 0, 0).$$

We have

$$\begin{aligned}
\rho(g_1+g_2) &= \rho(g_1) + \rho(g_2),\\
\lambda(g_1+g_2) &= \lambda(g_1) + \lambda(g_2),\\
\rho^2(g_1) &= \rho(g_1), \qquad \lambda^2(g) = \lambda(g),\\
\rho\lambda(g_1) &= \lambda\rho(g_1) = (0, 0, 0, 0),\\
\rho(e) &= \lambda(e) = 0 \quad \text{where} \quad e = (0, 0, 0, 1),\\
d_1\lambda(g_1) &= 0, \qquad d_2\rho(g_1) = 0,
\end{aligned} \tag{2}$$

and $d_3e = d_3(0, 0, 0, 1) = (0, 0, 0, 0)$, for all g_1, g_2 in G.

Define $(G, +, \cdot)$ by taking $g_1 \cdot g_2 = \lambda(g_2) + \rho(g_1) + e$. Then,

$$\begin{aligned}
(g_1 \cdot g_2) \cdot g_3 &= \lambda(g_3) + \rho(\lambda(g_2) + \rho(g_1) + e) + e\\
&= \lambda(g_3) + \rho\lambda(g_2) + \rho^2(g) + \rho(e) + e\\
&= \lambda(g_3) + \rho(g_1) + e,\\
g_1 \cdot (g_2 \cdot g_3) &= \lambda(\lambda(g_3) + \rho(g_2) + e) + \rho(g_1) + e\\
&= \lambda^2(g_3) + \lambda\rho(g_2) + \lambda(e) + \rho(g_1) + e\\
&= \lambda(g_3) + \rho(g_1) + e,
\end{aligned}$$

i.e., $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$.

$$\begin{aligned}
&(g_1 + \cdots + g_{m_i})(l_1 + \cdots + l_{n_i})\\
&\quad = \lambda(l_1 + \cdots + l_{n_i}) + \rho(g_1 + \cdots + g_{m_i}) + e\\
&\quad = \lambda(l_1) + \cdots + \lambda(l_{n_i}) + \rho(g_1) + \cdots + \rho(g_{m_i}) + e.
\end{aligned}$$

$$\begin{aligned}
\sum g_il_j &= \sum (\lambda(l_j) + \rho(g_i) + e)\\
&= m_i\lambda(l_1) + \cdots + m_i\lambda(l_{n_i})\\
&\quad + n_i\rho(g_1) + \cdots + n_i\rho(g_{m_i}) + m_in_ie\\
&= \lambda(l_1) + \cdots + \lambda(l_{n_i}) + \rho(g_1) + \cdots + \rho(g_{m_i}) + e,
\end{aligned}$$

since $d_1 | (m_i - 1)$, $d_2 | (n_i - 1)$, $d_3 | (m_i n_i - 1)$. Thus, D_{m_i, n_i} holds in $(G, +, \cdot)$ for all i.

Suppose that

$$(d_1) \supseteq (h_1 - 1, \cdots, h_j - 1, \cdots),$$
$$(d_2) \supseteq (k_1 - 1, \cdots, k_j - 1, \cdots),$$

and

$$(d_3) \supseteq (h_1 k_1 - 1, \cdots, h_j k_j - 1, \cdots)$$

is not true. Then there exists at least a pair, (h_1, k_1) say, such that one of the following relations holds.

(i) $(h_1 - 1) \notin (d_1)$,

(ii) $(k_1 - 1) \notin (d_2)$,

(iii) $(h_1 k_1 - 1) \notin (d_3)$.

Let $a = (1, 0, 0, 0)$. Then we have

$$(h_1 0) \cdot (a + (k_1 - 1)0) = 0 \cdot a = \lambda(a) + \rho(0) + e = (0, 1, 0, 1),$$

and

$$h_1(0 \cdot a) + h_1(k_1 - 1)(0 \cdot 0)$$
$$= (0, h_1, 0, h_1) + (0, 0, 0, h_1(k_1 - 1)) = (0, h_1, 0, h_1 k_1).$$

Now $(0, 1, 0, 1) = (0, h_1, 0, h_1 k_1)$ implies that $(h_1 - 1) \in (d_1)$, and $(h_1 k_1 - 1) \in (d_3)$ we can show, similarly, $(k_1 - 1) \in (d_2)$. Hence if D_{h_1, k_1} is satisfied, we are led to a contradiction. Thus D_{h_1, k_1} is not satisfied in $(G, +, \cdot)$ and this completes the proof. q.e.d.

REMARK 1. The above theorem is unchanged, if we assume that $(R, +, \cdot)$ is also associative.

COROLLARY 2. *For all systems* $(R, +, \cdot)$, $\{(R, +)$ *is an abelian group,* $D_{m_1, n_1}\}$ *is equivalent to* $\{(R, +)$ *is an abelian group,* $D_{m_2, n_2}\}$ *if and only if* $m_1 = m_2$, $n_1 = n_2$.

COROLLARY 3. *The two distributive laws of a ring,* $D_{1,2}$ *and* $D_{2,1}$ *can never be replaced by one of the form* $D_{m,n}$.

PROOF. For the case of $D_{1,2}$ and $D_{2,1}$, $d_1 = d_2 = d_3 = 1$.

If these two distributive laws can be replaced by one, say $D_{m,n}$ then, by second fundamental theorem, we have,

$$m - 1 = 1, \qquad n - 1 = 1, \qquad mn - 1 = 1$$

which is clearly a contradiction.

COROLLARY 4. *For any infinite set of distributive laws*

$$\{D_{m_1,n_1};\ D_{m_2,n_2};\ \cdots\},$$

there always exists a finite subset equivalent to it.

PROOF. This follows from the Second Fundamental Theorem and the fact that an infinite set of positive integers has a finite subset with the same greatest common divisor.

Acknowledgment. I am grateful to the referee for many valuable suggestions.

REFERENCES

1. R. A. Beaumont, *Generalized rings*, Proc. Amer. Math. Soc. vol. 9 (1958) pp. 876–881.

2. Toru Saito, *Note on the distributive laws*, Amer. Math. Monthly vol. 11 (1959) pp. 280–283.

NATIONAL TAIWAN UNIVERSITY,
TAIPEI, CHINA