ON THE DISTRIBUTIVE LAW

WU-YI HSIEANG

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

$$(x_1 + \cdots + x_m)(y_1 + \cdots + y_n) = x_1y_1 + \cdots + x_1y_n$$

$$+ x_2y_1 + \cdots + x_2y_n$$

$$+ \cdots$$

$$+ x_my_1 + \cdots + x_my_n \quad (m, n \text{ fixed}),$$

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 $(R, +, \cdot)$, $m, n = 2$, there exists a ring $(R, +, \ast)$ with the same domain and addition, and

$$a \ast b = a \cdot b - a \cdot 0 - 0 \cdot b + 0 \cdot 0 \quad \text{for all } a, b \in R.$$ 

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) \quad $\lambda(a + b) = \lambda(a) + \lambda(b),$ 

$\rho(a + b) = \rho(a) + \rho(b).$

Conversely, if $(R, +, \ast)$ is a ring with an element $e$ and two maps...
\( \lambda, \rho \) of \( R \) into \( R \) which satisfy the above two equations, then there exists an \((m, n)\)-distributive ring with the same addition, such that,
\[ a \cdot b = a \ast b + \rho(a) + \lambda(b) + e \]
and
\[ e = 0 \cdot 0, \quad \rho(a) = a \cdot 0 = 0 \cdot 0, \quad \lambda(a) = 0 \cdot a = 0 \cdot 0. \]

**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 \( a \ast b = a \cdot b - a \cdot 0 - 0 \cdot b + 0 \cdot 0 \) for all \( a, b \) in \( R \), then

3. \((a + b) \ast c = (a + b) \cdot c - (a + b) \cdot 0 - 0 \cdot c + 0 \cdot 0\)
\[= (a \cdot c + b \cdot c - 0 \cdot c) - (a \cdot 0 + b \cdot 0 - 0 \cdot 0) - 0 \cdot c + 0 \cdot 0\]
\[= (a \cdot c - a \cdot 0 - 0 \cdot c + 0 \cdot 0) + (b \cdot c - b \cdot 0 - 0 \cdot c + 0 \cdot 0)\]
\[= a \ast c + b \ast c,\]

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

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

For the converse, if \((R, +, \ast)\) is a ring with an element \( e \) and two maps \( \lambda, \rho \) of \( R \) into \( R \), which satisfy the conditions (i), (ii), we can easily define another triple \((R, +, \cdot)\) by
\[ a \cdot b = a \ast b + \lambda(b) + \rho(a) + e. \]

Then,

(a) \( \lambda(0) = \rho(0) = 0 \) (by (ii)) and \( 0 \cdot 0 = e. \)
(b) \( a \cdot 0 = a \ast 0 + \rho(a) + \lambda(0) + e \) or \( \rho(a) = a \cdot 0 = 0 \cdot 0. \)
(c) \( 0 \cdot b = 0 \ast b + \rho(0) + \lambda(b) + e \) or \( \lambda(b) = 0 \cdot b = 0 \cdot 0. \)
(d) \( (a_1 + \cdots + a_m) \cdot (b_1 + \cdots + b_n)\)
\[= \sum (a_i \ast b_j + \lambda(b_j) + \lambda(a_i) + e)\]
\[= \sum (a_i \ast b_j + \lambda(b_j) + \rho(a_i) + e)
- (m - 1)\lambda(b_1) - \cdots - (m - 1)\lambda(b_n)
- (n - 1)\rho(a_1) - \cdots - (n - 1)\rho(a_m)
- (mn - 1)e \]
\[= \sum a \cdot b_j \quad (i = 1, \cdots, m; j = 1, \cdots, n).\]
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 \((R, +, \ast)\) is associative and the additional condition

\[
[p(a) \ast c + \lambda(b) \ast c + e \ast c + \rho(a \ast b) + \rho^2(a) + \rho(\lambda(b) + \rho(e) + \lambda(c)]
\]

(iii) \(- [a \ast \rho(b) + a \ast \lambda(c) + a \ast e + \rho(a) + \lambda(b \ast c) + \lambda(\rho(b) + \lambda^2(c) + \lambda(e))] = 0\)

is satisfied.

**Proof.** 1.

\[
(a \ast b) \ast c = (a \ast b + a \ast 0 + 0 \ast b + 0 \ast 0) \ast c
\]

\[
= [(a \ast b) \ast c - (a \ast b) \ast 0 - 0 \ast c + 0 \ast 0]
- [(a \ast 0) \ast c - (a \ast 0) \ast 0 - 0 \ast c + 0 \ast 0]
+ [(0 \ast b) \ast c - (0 \ast b) \ast 0 - 0 \ast c + 0 \ast 0]
= (a \ast b) \ast c - (a \ast b) \ast 0 - (a \ast 0) \ast c - (0 \ast b) \ast c
+ (a \ast 0) \ast 0 + (0 \ast b) \ast 0 + (0 \ast 0) \ast c - (0 \ast 0) \ast 0,
\]

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

2. If \(" \ast\)\) is associative and if \(e, \lambda, \rho\) 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

\[
[(m_1, n_1), \ldots, (m_i, n_i), \ldots]
\]

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

\((R, +, \cdot)\) satisfies \(\{D_{m_1, n_1}, \ldots, D_{m_i, n_i}, \ldots\}\) implies \((R, +, \cdot)\)
satisfies \( \{ D_{h_1,k_1}, \ldots, D_{h_j,k_j}, \ldots \} \) if and only if

\[
(m_1 - 1, \ldots, m_i - 1, \ldots) \supseteq (h_1 - 1, \ldots, h_j - 1, \ldots),
\]
\[
(n_1 - 1, \ldots, n_i - 1, \ldots) \supseteq (k_1 - 1, \ldots, k_j - 1, \ldots),
\]
\[
(m_1n_1 - 1, \ldots, m_in_i - 1, \ldots) \supseteq (hk_1 - 1, \ldots, hjk_j - 1, \ldots).
\]

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

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

There are only four possibilities, namely,

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

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

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

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

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

If \((m_1 - 1, m_2 - 1, \ldots) \neq (0)\) and \((n_1 - 1, n_2 - 1, \ldots) \neq (0)\), in this case, there exists at least one \(m_1\), say \(m_1\), greater than one, if \(m_1 > 1\), then \((R, +, \cdot)\) is an \((m_1, n_1)\)-distributive ring. If \(n_1 = 1\), then there must exist another \(n_2\), 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 \((R, +, \cdot)\) with \(a \ast b = a \cdot b - a \cdot 0 - 0 \cdot b + 0 \cdot 0\) as we have proved in First Fundamental Theorem.

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

\[
(m_i - 1, m_2 - 1, \ldots) = (d_1),
\]
\[
(n_i - 1, n_2 - 1, \ldots) = (d_2),
\]
\[
(m_in_i - 1, m_2n_2 - 1, \ldots) = (d_3),
\]

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
we can easily see that 

\[(h_j - 1)X(a) = 0, \quad (k_j - 1)p(a) = 0,\]

and

\[(h_jk_j - 1)e = 0.\]

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

\[a \cdot (b + c) = a \cdot b + a \cdot c + (n_i - 2)(a \cdot 0)\]

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

Put \((n_1 - 1, \ldots, n_i - 1, \ldots) = (d_i)\). Then,

\[(m_1n_1 - 1, \ldots, m_in_i - 1, \ldots) = (d_i),\]

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

\[a \cdot (b_1 + \cdots + b_{kj}) = a \cdot (b_1 + \cdots + b_{kj}) + a \cdot 0\]

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
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 $(m_i-1)$, $(n_i-1)$, $(m_i n_i-1)$, respectively, and let $\Pi$ be the ring of integers, $\Pi_d = \Pi/(d)$.

Let $G = \{(i, j, k) | n \in \Pi$, $i \in \Pi_{d_1}$, $j \in \Pi_{d_2}$, $k \in \Pi_{d_3}\}$, 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

$$\rho(g_1 + g_2) = \rho(g_1) + \rho(g_2),$$
$$\lambda(g_1 + g_2) = \lambda(g_1) + \lambda(g_2),$$
$$\rho^2(g_1) = \rho(g_1), \quad \lambda^2(g) = \lambda(g),$$

(2) $$\rho \lambda(g_1) = \lambda \rho(g_1) = (0, 0, 0, 0),$$
$$\rho(e) = \lambda(e) = 0 \quad \text{where} \quad e = (0, 0, 0, 1),$$
$$d_1 \lambda(g_1) = 0, \quad d_2 \rho(g_1) = 0,$$

and $d_3 e = d_3(0, 0, 0, 1) = (0, 0, 0, 0)$, 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,

$$(g_1 \cdot g_2) \cdot g_3 = \lambda(g_3) + \rho(\lambda(g_2) + \rho(g_1) + e) + e$$
$$= \lambda(g_3) + \rho \lambda(g_2) + \rho(g_1) + e$$
$$= \lambda(g_3) + \rho(g_1) + e,$$
$$g_1 \cdot (g_2 \cdot g_3) = \lambda(\lambda(g_3) + \rho(g_2) + e) + \rho(g_1) + e$$
$$= \lambda^2(g_3) + \rho(g_2) + \lambda(e) + \rho(g_1) + e$$
$$= \lambda(g_3) + \rho(g_1) + e,$$

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

$$(g_1 + \cdots + g_m) (l_1 + \cdots + l_n)$$
$$= \lambda(l_1 + \cdots + l_n) + \rho(g_1 + \cdots + g_m) + e$$
$$= \lambda(l_1) + \cdots + \lambda(l_n) + \rho(g_1) + \cdots + \rho(g_m) + e.$$

$$\sum g_j = \sum (\lambda(l_j) + \rho(g_j) + e)$$
$$= m \lambda(l_1) + \cdots + m \lambda(l_m)$$
$$+ n \rho(g_1) + \cdots + n \rho(g_m) + m n e$$
$$= \lambda(l_1) + \cdots + \lambda(l_n) + \rho(g_1) + \cdots + \rho(g_m) + e,$$
since \(d_1|\langle m_i-1\rangle\), \(d_2|\langle n_i-1\rangle\), \(d_3|\langle m,n_i-1\rangle\). Thus, \(D_{m_i,n_i}\) holds in \((G, +, \cdot)\) for all \(i\).

Suppose that
\[
\begin{align*}
(d_1) & \supseteq (h_1 - 1, \ldots, h_j - 1, \ldots)
\quad \\
(d_2) & \supseteq (k_1 - 1, \ldots, k_j - 1, \ldots)
\end{align*}
\]
and
\[
\begin{align*}
(d_3) & \supseteq (h_1k_1 - 1, \ldots, h_jk_j - 1, \ldots)
\end{align*}
\]
is not true. Then there exists at least a pair, \((h_1, k_1)\) say, such that one of the following relations holds.

(i) \((h_1 - 1) \not\in (d_1)\),

(ii) \((k_1 - 1) \not\in (d_2)\),

(iii) \((h_1k_1 - 1) \not\in (d_3)\).

Let \(a = (1, 0, 0, 0)\). Then we have
\[
\begin{align*}
(h_10) \cdot (a + (k_1 - 1)0) &= 0 \cdot a = \lambda(a) + \rho(0) + e = (0, 1, 0, 1),
\quad \\
h_1(0 \cdot a) + h_1(k_1 - 1)(0 \cdot 0)
&= (0, h_1, 0, h_1) + (0, 0, 0, h_1(k_1 - 1)) = (0, h_1, 0, h_1k_1).
\end{align*}
\]
Now \((0, 1, 0, 1) = (0, h_1, 0, h_1k_1)\) implies that \((h_1 - 1) \not\in (d_1)\), and \((h_1k_1 - 1) \not\in (d_3)\) we can show, similarly, \((k_1 - 1) \not\in (d_2)\). 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 \((R, +, \cdot)\), \(\{(R, +)\text{ is an abelian group, } D_{m_1,n_1}\}\) is equivalent to \(\{(R, +)\text{ is an abelian group, } D_{m_2,n_2}\}\) 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,
\[
m - 1 = 1, \quad n - 1 = 1, \quad mn - 1 = 1
\]
which is clearly a contradiction.

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


NATIONAL TAIWAN UNIVERSITY,
TAIPEI, CHINA