Logarithmetics of Finite Quasigroups (I)

By HELEN POPOVA

(*Received* 25*th July*, 1951. *Read* 2*nd November*, 1951.)

1. *Introduction.*

The study of non-associative algebras led to the investigation of identities connecting powers of elements of such algebras. Thus Etherington[1] (1941, 1949, 1951) introduced the concept of the *logarithmetic* of an algebra, defining it roughly as " the arithmetic of the indices of the general element ".

Apart from a trivial observation on groups in §2, the only known result concerning logarithmetics of quasigroups seems to be the result due to Murdoch[2] (1939, Corollary to Theorem 10). In Etherington's terminology this result is expressed by saying that an abelian quasigroup is palintropic, which means that multiplication is commutative in its logarithmetic ($x^{rs} = x^{sr}$).

We introduce a new term *quasi-integer*; otherwise we follow Etherington in the definitions of §2.

I am grateful to Dr. I. M. H. Etherington for advice and criticisms.

2. *Definitions.*

A *groupoid* is a set closed with respect to a binary operation. A multiplicative groupoid with or without other operations such as + may be called an *algebra*. A (multiplicative) *quasigroup*[3] means a multiplicative groupoid within which the equations $ax = b$, $ya = b$ determine x and y uniquely, whenever a and b are given; it is *abelian* (Murdoch, 1939) or *entropic* (Etherington, 1949) if identically $ab \, . \, cd = ac \, . \, bd$.

---

[1] I. M. H. Etherington, " Some non-associative algebras in which the multiplication of indices is commutative ", *Journal London Math. Soc.*, 16 (1941), 48–55; " Non-associative arithmetics ", *Proc. Roy. Soc. Edinburgh* (A), 62 (1949), 442–453; " Non-commutative train algebras of rank 2 and 3 ", *Proc. London Math. Soc.* (2), 52 (1951), 241–252.

[2] D. C. Murdoch, " Quasigroups which satisfy certain generalised associative laws " *American J. of Math.*, 61 (1939), 509–522.

[3] B. A. Hausmann and O. Ore, " Theory of quasigroups ", *American J. of Math.*, 59 (1937), 983–1004.

https://doi.org/10.1017/S0013091500021325 Published online by Cambridge University Press

A *power* x^r of an element x of an algebra A is a continued product in which all factors are equal to x. The symbol r used to denote the power is the *index* of the power. The product of two powers x^r, x^s is denoted by x^{r+s}; a power of a power is indicated as a product in the index: $(x^r)^s = x^{rs}$; an iterated power is indicated by a power in the index: $(x^r)^r = x^{r^2}$, $\left((x^r)^r\right)^r = x^{r^3}$, etc. For example

$$x^{2.2+1} = (x^2)^2 x; \quad x^{(1+2.2)2} = \left(x.(x^2)^2\right)\left(x.(x^2)^2\right).$$

The *degree* of a power of x is the number of its factors x. Powers in which factors are absorbed one at a time on the right are called *principal*. The principal power of degree δ will be denoted x^δ. All other powers can be expressed in terms of principal powers by suitably partitioning the index and using brackets when necessary. Thus $x^4 = x^{(2+1)+1}$ is distinguished from $x^{1+3} = x^{1+(2+1)}$ and from $x^{1+(1+2)}$ and $x^{(1+2)+1}$.

A *quasi-integer* of an algebra A will be defined as the class of indices $r, s, \ldots$ such that $x^r = x^s = \ldots$ for all x of A.

It is easily seen that the quasi-integers can be added and multiplied like indices without inconsistency, and like indices they obey the rules[1]:

$$(rs)t = r(st), \quad r(s+t) = rs+rt,$$

but in general

$$r+(s+t) \neq (r+s)+t, \quad r+s \neq s+r, \quad rs \neq sr, \quad (s+t)r \neq sr+tr.$$

The algebra consisting of all quasi-integers of A together with operations $(+)$, $(.)$ is defined to be the *logarithmetic of* A and denoted by L_A. Thus for example the logarithmetic of a commutative or associative algebra is commutative or associative with respect to addition; in particular the logarithmetic of a group with finite period p is isomorphic with the ring of integers modulo p.

The set of all quasi-integers of A together with the operation of addition or multiplication only will be denoted by $L_A(+)$, $L_A(.)$ respectively.

Every subset of a finite quasigroup Q which is closed with respect to multiplication satisfies the quotient axiom and is therefore a subquasigroup. In particular all powers of an element a of Q form a quasigroup Q_a. We

---

[1] I. M. H. Etherington, " On non-associative combinations ", *Proc. Roy. Soc. Edinburgh*, 59 (1939), 153–162.

shall say that Q_a is *generated* by a; its logarithmetic will be called the *logarithmetic of* a and denoted by L_a.

3. *Quasi-integers of a finite algebra.*

A quasi-integer of an algebra A consisting of a finite number of elements can be represented by the vector

$$r = \begin{bmatrix} a_1^r \\ \vdots \\ a_n^r \end{bmatrix}, \tag{1}$$

which sometimes will be written as:

$$r = \{a_p^r\}_{p=1,\dots,n} \quad \text{or} \quad r = \{a_1^r, \dots, a_n^r\}$$

where $a_1, \dots, a_n$ are all elements (or, if preferred, all non-idempotent elements) of A. Two indices r, s are equal in L_A (*i.e.* belong to the same quasi-integer) if and only if $a_i^r = a_i^s$ for $i = 1, 2, \dots, n$, that is if and only if they are represented by the same vectors. If corresponding elements of two vectors $r = \{a_p^r\}$ and $s = \{a_p^s\}$ $(p = 1, 2, \dots, n)$ are multiplied, we obtain $\{a_p^{r+s}\}$ which is the vector denoting $r+s$. The s-th powers of the elements of $r = \{a_p^r\}_{p=1,\dots,n}$ form the vector $\{a_p^{rs}\}_{p=1,\dots,n}$ which is rs. Consequently, if quasi-integers r, s are given as $r = \{\lambda_p\}$, $s = \{\mu_p\}$ where $p = 1, 2, \dots, n$, then

$$r+s = \{\lambda_p \mu_p\}, \quad rs = \{\lambda_p^s\}, \quad sr = \{\mu_p^r\} \qquad (p = 1, 2, \dots, n).$$

Multiplication in L_A has an obvious matrix representation. If in the k-th row of the vector r stands the element a_i of A, then the element in the k-th row of the vector rs is a_i^s which we find in the i-th row of the vector s. If we denote a_i by a row vector with 1 in the i-th column and other elements zero:

$$a_i = (0 \dots 010 \dots 0) \tag{2}$$

and write vectors r, s as matrices formed by substituting the vectors (2) in the expressions (1) of r, s, then rs is the matrix product.

Example 1. Investigating the logarithmetic of the quasigroup Q consisting of elements 1, 2, 3, 4, given by the multiplication table

	1	2	3	4
1	3	1	4	2
2	4	2	1	3
3	1	3	2	4
4	2	4	3	1

we observe that any quasi-integer of L_Q can, since 2 is idempotent, be completely determined by the set of elements $(1^r, 3^r, 4^r) = (m, n, s)$, where m, n, s can take any values amongst 1, 2, 3, 4. Thus:

Quasi-integers:	1	2	3	1+2	4	1+3	2.2	(1+2)+1	1+(1+2)	5	...
Elements of Q:											
1	1	3	1	4	3	3	2	2	2	1	
3	3	2	1	3	4	1	2	2	2	3	
4	4	1	2	2	3	4	3	3	4	4	

and we may denote quasi-integers of L_Q by vectors such as

$$1 = \begin{bmatrix}1\\3\\4\end{bmatrix} = (1+3)+3; \quad (1+2) = \begin{bmatrix}4\\3\\2\end{bmatrix}; \quad 2.2 = \begin{bmatrix}2\\2\\3\end{bmatrix}; \quad 2 = \begin{bmatrix}3\\2\\1\end{bmatrix};$$

$$1+(1+2) = \begin{bmatrix}2\\2\\4\end{bmatrix}; \quad \ldots .$$

It may be verified that the 64 such vectors all occur in L_Q.

Example 2. Suppose that $r = \{3, 2, 1, 4\}$ $s = \{3, 2, 4, 3\}$. (This could refer to the logarithmetic of Ex. 1, with $r = 1+3$, $s = 4$, since the element 2 is idempotent.) Then we have $1^s = 3$, $2^s = 2$, $3^s = 4$, $4^s = 3$, giving

$$rs = \{3^s, 2^s, 1^s, 4^s\} = \{4, 2, 3, 3\}.$$

As in the previous section, denoting the elements 1, 2, 3, 4 of Q by row vectors $(1\ldots)$, $(.1..)$, $(..1.)$, $(\ldots 1)$ respectively, we can write the column vectors r, s as matrices. In this notation

$$rs = \begin{bmatrix} . & . & 1 & . \\ . & 1 & . & . \\ 1 & . & . & . \\ . & . & . & 1 \end{bmatrix} \begin{bmatrix} . & . & 1 & . \\ . & 1 & . & . \\ . & . & . & 1 \\ . & . & 1 & . \end{bmatrix} = \begin{bmatrix} . & . & . & 1 \\ . & 1 & . & . \\ . & . & 1 & . \\ . & . & 1 & . \end{bmatrix}$$

4. *Properties of* $L_Q(+)$.

Let L_i $(i = 1, 2, \ldots)$ be any finite or infinite set of algebras, distinct or identical, with operations $(+)$, $(.)$ uniquely defined by

$$q_i + p_i = r_i, \quad q_i p_i = t_i, \quad q_i, p_i, r_i, t_i \in L_i \qquad (i = 1, 2, \ldots)$$

and consider the set $L^\times$ of all symbols

$$\{q_1, q_2, \ldots\}, \quad q_i \in L_i \qquad (i = 1, 2, \ldots),$$

https://doi.org/10.1017/S0013091500021325 Published online by Cambridge University Press

with operations (+), (.) defined as

$$\{q_1, \ldots\}+\{p_1, \ldots\}=\{r_1, \ldots\}, \quad \{q_1, \ldots\}\{p_1, \ldots\}=\{t_1, \ldots\};$$

then $L^\times$ is called the *direct union*[1] of $L_1, L_2, \ldots$.

LEMMA. *The direct union $L^\times$ of the logarithmetics L_i of all the elements 1, 2, …, n of a finite quasigroup is a finite quasigroup with respect to addition.*

For the elements of $L^\times$ are vectors such as

$$r=\{p^{r_p}\}, \quad s=\{p^{s_p}\} \qquad (p=1, 2, \ldots, n).$$

Obviously $r+s=\{p^{r_p+s_p}\}$ belongs to $L^\times$, and it remains to prove that the equations $r+x=s$, $y+r=s$ always have unique solutions x, y in $L^\times$.

Now $r+x=s$ is equivalent to the set of n equations

$$p^{r_p} x_p = p^{s_p}.$$

Since all powers of p form a quasigroup, each of these equations has a unique solution of the form $x_p=p^{X_p}$. Thus $r+x=s$ has the unique solution $x=\{p^{X_p}\}$, which is in $L^\times$. Similarly for $y+r=s$.

THEOREM 1. *The logarithmetic of a finite quasigroup is a quasigroup with respect to addition.*

For the vectors of L_Q, say $r=\{p^r\}$, $s=\{p^s\}$, $p=1, \ldots, n$, may also be regarded as vectors of $L^\times$. Thus the logarithmetic of Q is a subset of a finite additive quasigroup $L^\times$, closed with respect to addition, and therefore is a quasigroup with respect to addition.

Example 3. The quasigroup Q of order four

	1	2	3	4
1	2	4	3	1
2	3	1	2	4
3	1	3	4	2
4	4	2	1	3

has logarithmetic consisting of only four quasi-integers

$$1=\begin{bmatrix}1\\2\\3\\4\end{bmatrix}, \quad 2=\begin{bmatrix}2\\1\\4\\3\end{bmatrix}, \quad 3=\begin{bmatrix}3\\4\\1\\2\end{bmatrix}, \quad 1+2=\begin{bmatrix}4\\3\\2\\1\end{bmatrix}.$$

In this case $L_Q(+)$ is isomorphic with Q.

[1] G. Birkhoff, "On the structure of abstract algebras", *Proc. Cambridge Phil. Soc.*, 31 (1935), 433–454.

5. L_Q *as a subdirect union.*

Let $L^{\times}$ be a direct union of an arbitrary set of additive quasigroups L_i, the elements of $L^{\times}$ being denoted by

$$l = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}, \quad \alpha_i \varepsilon L_i.$$

If L is a subquasigroup of $L^{\times}$, and

$$q = \{q_1, q_2, \ldots, q_n\} \varepsilon L,$$

the correspondence $q \to q_i$ defines a homomorphism of L into L_i and therefore on to a subquasigroup L_i' of L_i. If for every i $L_i' = L_i$, L is a *subdirect union* of the quasigroups L_i.

Let Q be a quasigroup $(1, 2, \ldots, n)$. We denote by L_i the logarithmetic of the element i of Q $(i = 1, 2, \ldots, n)$.

Let i^x take n_i distinct values $\beta_{i1}, \beta_{i2}, \ldots, \beta_{in_i}$ when x varies $(i = 1, 2, \ldots, n)$. The direct union

$$L^{\times} = L_1 + L_2 + \ldots + L_n$$

consists of all $n_1 n_2 \ldots n_n$ possible vectors

$$\{a_1, a_2, \ldots, a_n\} \quad \text{where} \quad a_i \varepsilon L_i.$$

The logarithmetic of Q does not necessarily contain all those vectors. However (Theorem 1), it forms a quasigroup with respect to addition, which is a subquasigroup of $L^{\times}$.

All the vectors representing the quasi-integers of L_Q may be written in a matrix

$$L = \begin{bmatrix} \alpha_{11} \cdots \alpha_{1N} \\ \cdots \cdots \cdots \\ \alpha_{n1} \cdots \alpha_{nN} \end{bmatrix}$$

where n is the order of Q, N that of L_Q, and $\alpha_{ij} \varepsilon L_i$.

From the fact that L_Q is the set of *all* distinct values of $\{1, \ldots, n\}^x$ when x is varied, it follows that in the i-th row of the matrix L there appear necessarily all distinct elements of L_i. Therefore, if we collect the quasi-integers with $\beta_{i1}, \beta_{i2}, \ldots, \beta_{in_i}$ in the i-th row into classes $A_{i1}, \ldots, A_{in_i}$ respectively, the homomorphisms $q \to q_i$ above are

$$A_{i1} \to \beta_{i1}, \; A_{i2} \to \beta_{i2}, \; \ldots, \; A_{in_i} \to \beta_{in_i} \quad (i = 1, 2, \ldots, n).$$

Each of them defines the homomorphism of L_Q on to L_i

$$L_Q \to L_i \quad (i = 1, 2, \ldots, n)$$

https://doi.org/10.1017/S0013091500021325 Published online by Cambridge University Press

and we have proved:

THEOREM 2. *The logarithmetic of a quasigroup is a subdirect union of the logarithmetics of its elements.*

By the order n_i of the element i of a quasigroup Q we understand the order of the quasigroup generated by it.

COROLLARY 1. *The order of L_Q cannot exceed the product of the orders of all elements of Q:*

$$N \leqslant n_1 n_2 \ldots n_n.$$

For $n_1 n_2 \ldots n_n$ is the order of the direct union.

COROLLARY 2. *If L_Q has order $N = n_1 n_2 \ldots n_n$, then it is the direct union of the logarithmetics of all elements of Q.*

(Compare Example 1.)

Example 4. The logarithmetic of the quasigroup.

	1	2	3	4
1	2	3	4	1
2	4	1	2	3
3	3	2	1	4
4	1	4	3	2

consists of 16 quasi-integers which are the columns of the matrix

$$L = \begin{bmatrix} 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 4 & 4 & 4 & 4 \\ 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 4 & 4 & 4 & 4 & 3 & 3 & 3 & 3 \\ 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 & 2 & 1 & 4 & 3 & 2 & 1 & 4 & 3 & 2 & 1 & 4 & 3 \end{bmatrix}.$$

The logarithmetics of the elements 1, 2, 3, 4 are

$$L_1 = (1, 2, 3, 4), \quad L_2 = (1, 2, 3, 4), \quad L_3 = (1, 2, 3, 4), \quad L_4 = (1, 2, 3, 4).$$

So the direct union consists of 256 vectors. The logarithmetic, however, has order 16, and the homomorphisms $q \to q_i$ are:

(1) $q \to q_1$:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 \\ 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} \to 1, \quad \begin{bmatrix} 2 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} \to 2, \quad \begin{bmatrix} 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 4 \\ 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} \to 3, \quad \begin{bmatrix} 4 & 4 & 4 & 4 \\ 3 & 3 & 3 & 3 \\ 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} \to 4,$$

https://doi.org/10.1017/S0013091500021325 Published online by Cambridge University Press

which implies $L_Q \to L_1$. Similarly

(2) $q \to q_2$:

$$\begin{bmatrix} 2&2&2&2 \\ 1&1&1&1 \\ 1&2&3&4 \\ 2&1&4&3 \end{bmatrix} \to 1, \quad \begin{bmatrix} 1&1&1&1 \\ 2&2&2&2 \\ 1&2&3&4 \\ 2&1&4&3 \end{bmatrix} \to 2, \quad \begin{bmatrix} 4&4&4&4 \\ 3&3&3&3 \\ 1&2&3&4 \\ 2&1&4&3 \end{bmatrix} \to 3, \quad \begin{bmatrix} 3&3&3&3 \\ 4&4&4&4 \\ 1&2&3&4 \\ 2&1&4&3 \end{bmatrix} \to 4,$$

(3) $q \to q_3$:

$$\begin{bmatrix} 1&2&3&4 \\ 2&1&4&3 \\ 1&1&1&1 \\ 2&2&2&2 \end{bmatrix} \to 1, \quad \begin{bmatrix} 1&2&3&4 \\ 2&1&4&3 \\ 2&2&2&2 \\ 1&1&1&1 \end{bmatrix} \to 2, \quad \begin{bmatrix} 1&2&3&4 \\ 2&1&4&3 \\ 3&3&3&3 \\ 4&4&4&4 \end{bmatrix} \to 3, \quad \begin{bmatrix} 1&2&3&4 \\ 2&1&4&3 \\ 4&4&4&4 \\ 3&3&3&3 \end{bmatrix} \to 4,$$

(4) $q \to q_4$:

$$\begin{bmatrix} 1&2&3&4 \\ 2&1&4&3 \\ 2&2&2&2 \\ 1&1&1&1 \end{bmatrix} \to 1, \quad \begin{bmatrix} 1&2&3&4 \\ 2&1&4&3 \\ 1&1&1&1 \\ 2&2&2&2 \end{bmatrix} \to 2, \quad \begin{bmatrix} 1&2&3&4 \\ 2&1&4&3 \\ 4&4&4&4 \\ 3&3&3&3 \end{bmatrix} \to 3, \quad \begin{bmatrix} 1&2&3&4 \\ 2&1&4&3 \\ 3&3&3&3 \\ 4&4&4&4 \end{bmatrix} \to 4,$$

which shows that the homomorphisms $q \to q_2$, $q \to q_3$, $q \to q_4$ imply the homomorphisms

$$L_Q \to L_2, \quad L_Q \to L_3, \quad L_Q \to L_4$$

respectively. So that, for every i, $L_i' = L_i$, and L_Q is a subdirect union of L_1, L_2, L_3 and L_4.

DEPARTMENT OF MATHEMATICS,
UNIVERSITY OF ABERDEEN.