Logarithmetics of Finite Quasigroups (II)

By HELEN POPOVA

(*Received* 25*th July*, 1951. *Revised* 9*th February*, 1955.)

1. *Introduction.*

In the first paper of this series (L.Q.I)[1] we have shown that the logarithmetic L_Q of a finite quasigroup Q is a quasigroup with respect to addition and that it is a subdirect union of the logarithmetics of the elements of Q.

In this second part we shall discuss further the structure of L_Q in its additive aspect, and obtain results concerning the order N of L_Q. For plain quasigroups (§3) the structure of $L_Q(+)$ is studied in more detail and it is shown that N is a power of n, the order of Q.

2. *The structure of* $L_Q(+)$.

Let $Q=(1, 2, \dots, n)$ be a quasigroup of order n. As in L.Q.I an element of L_Q is called a quasi-integer.

If r is the index of a power x^r, the corresponding quasi-integer is represented as the column vector $\{1^r, 2^r, \dots, n^r\}$. Such columns form the additive quasigroup $L_Q(+)$ in which vectors are added by forming products in Q of their corresponding elements:

$$\{i, \dots\}+\{j, \dots\}=\{ij, \dots\}. \tag{1}$$

Let the element 1 of Q generate a subquasigroup $Q_1=(a_1, a_2, \dots, a_{n_1})$ of order n_1, where $a_i a_j=a_{ij}$ $(i, j=1, \dots, n_1)$. Since 1^r generates Q_1 as r varies, L_Q must possess quasi-integers with $a_1, a_2, \dots, a_{n_1}$ in the first row. Let the quasi-integers be collected into classes, $A_{a_1}, A_{a_2}, \dots, A_{a_{n_1}}$ where A_{a_i} is the class of integers with a_i in the first row; and let $A_{a_i}+A_{a_j}$ denote the class of sums $\{a_i, \dots\}+\{a_j, \dots\}$. Let the orders of A_{a_i}, A_{a_j}, $A_{a_i}+A_a$ be p, q, t respectively.

---

[1] H. Popova, "Logarithmetics of finite quasigroups (I)", *Proc. Edinburgh Math. Soc.* (2), 9 (1954), 74–81.

It follows from (1) that $A_{a_i}+A_{a_j}\subset A_{a_{ij}}$; and also, by keeping $\{a_i, \ldots\}$ fixed, and letting $\{a_j, \ldots\}$ run through A_{a_j}, that $q\leqslant t$.

But since $L_Q(+)$ is a quasigroup

$$\{a_i, \ldots\}+\{x, \ldots\}=\{a_{ij}, \ldots\}$$

has a unique solution of the form $\{x, \ldots\}=\{a_j, \ldots\}$, and hence

$$A_{a_{ij}}\subset A_{a_i}+A_{a_j}, \quad q\geqslant t.$$

Consequently, the addition table (1) of L_Q can be partitioned into

$$A_{a_{ij}}=A_{a_i}+A_{a_j}; \tag{2}$$

and (by similar reasoning comparing p and t)

$$p=q=t.$$

The same argument can be applied to any row, and the result may be formulated as follows:

THEOREM 1. *Let Q be a quasigroup* $(1, \ldots, n)$ *and let the element m of Q generate a subquasigroup $Q_m=(a_1, a_2, \ldots, a_{n_m})$, of order n_m. Then if A_{a_i} denotes the set of all quasi-integers having a_i in their m-th row*

(i) *L_Q is homomorphic to Q_m by the correspondence*

$$(\textit{all quasi-integers of } A_{a_i})\rightarrow a_i;$$

(ii) *all A_{a_i} are of the same order, say P_m;*

(iii) *the order of L_Q is $N=n_mP_m$.*

It follows that

(iv) *N is a multiple of the least common multiple of all the n_m:*

$$[n_1, n_2, \ldots, n_m]\,|\,N.$$

As before, let 1 generate $Q_1=(a_1, a_2, \ldots, a_{n_1})$, and let A_{a_i} denote the class of quasi-integers represented by vectors whose first element is a_i, say $\{a_i, b_{is}, \ldots\}$. Keeping a_i fixed suppose that the element b_{is} takes k_i distinct values, and let B^{a_i} denote the corresponding class of k_i subvectors $\{a_i, b_{is}\}$. We may define

$$\{a_i, b_{is}\}+\{a_j, b_{js}\}=\{a_ia\ ,\ b_{\ s}b_{js}\}$$

https://doi.org/10.1017/S0013091500024883 Published online by Cambridge University Press

and define $B^{a_i}+B^{a_j}$ as the class of such sums. Then a repetition of an argument which led to Theorem 1 shows that

$$B^{a_i}+B^{a_j}=B^{a_{ij}}, \quad k_i=k_j=\ldots=k. \tag{3}$$

We have seen that all A_{a_i} are of the same order (Theorem 1) and that their quasi-integers have the same number, say k, of distinct elements in their second rows. We shall next show that the order of each A_{a_i} is a multiple of k. In order words, if $A_{a_i b_{is}}$ denotes the class of all quasi-integers with $\{a_i, b_{is}, \ldots\}$ in their first two rows, then all $A_{a_i b_{is}}$ are of the same order, and have the same number of distinct elements in their third rows.

Consider the classes A_{a_1}, $A_{a_{11}}$. Let their quasi-integers be classified according to their second element b_{1s}, b_{11t} into classes

$$C^s, \ F^t$$

respectively. By the same method it can be shown that

$$C^i+C^j=F^{ij}$$

and that these classes are all of the same order, say p_1. Thus,

LEMMA 1. *The order of A_1 is*

$$p_1=kq_1 \tag{4}$$

where k is the number of distinct elements of Q in the second row of all vectors representing the quasi-integers of A_1, and q_1 is the number of quasi-integers having $\{1, 2, \ldots\}$ in their first two rows.

The last lemma may be generalised as follows:

LEMMA 2. *Let there be just p quasi-integers of L_Q for which the first m rows are the same row by row; then for any other quasi-integer there are p (including itself) whose first m rows are identical with it row by row.*

The lemma is true if any m rows are chosen.

We denote by B_i the set $a_{i1}, a_{i2}, \ldots, a_{ik}$ of all distinct elements in the second rows of the vectors representing the quasi-integers of A_{a_i}. If the element 2 generates Q_2 of order n_2 then

$$(B_1, B_2, \ldots, B_{n_2})=(b_1, b_2, \ldots, b_{n_2})$$

where ( ) denotes union. If $k=1$, B_i have no elements in common; but if $k>1$, there must exist B_i with common elements, for otherwise $(B_1, \ldots, B_{n_2})$ would have kn_2 distinct elements, which is impossible, the

https://doi.org/10.1017/S0013091500024883 Published online by Cambridge University Press

order of Q_2 being n_2. The product of B_i and B_j may be defined as the set of distinct products of their elements. Then by (3)

$$B_i B_j = B_{ij}, \tag{5}$$

a multiplication table which is isomorphic to Q.

THEOREM 2. *If B_r and B_s have an element in common, they have all elements in common.*

Let $B_r = B_{1m} = B_1 B_m$, $B_s = B_{1l} = B_1 B_l$ (which is always possible by quasigroup properties), and let $a_{1\alpha} a_{m\beta} = d_{\alpha\beta}$, $a_{1\alpha} a_{l\beta} = c_{\alpha\beta}$ ($\alpha, \beta = 1, \ldots, k$).

There being only k distinct elements d_{ij}, forming the set B_r, these by quasigroup properties must appear in each row and column of the $k \times k$ matrix $[d_{\alpha\beta}]$, which is thus a latin square. Similarly, $[c_{\alpha\beta}]$ is a $k \times k$ latin square formed from the k elements of B_s.

Now, if B_r, B_s have one common element, say $d_{1i} = c_{1j}$, then we must have $a_{mi} = a_{lj}$, and consequently

$$d_{1i} = c_{1j}, \ d_{2i} = c_{2j}, \ \ldots, \ d_{ki} = d_{kj},$$

that is, $B_r = B_s$.

THEOREM 3. *If amongst $B_1, B_2, \ldots, B_{n_2}$ there are r and only r which are the same as B_1, then for every B_i ($i = 1, 2, \ldots, n_2$), there exist r and only r B_j's which are the same as B_i.*

This follows from the multiplication table (5). For if (say) $B_1, \ldots, B_r$ are the same, then so are $B_i B_1, \ldots, B_i B_r$, that is $B_{i1}, \ldots, B_{ir}$ ($i = 1, 2, \ldots, n_2$). Thus there exist at least r B_{ij}'s which are the same as B_{i1}. Suppose there are $r+1$ such, say $B_{i1}, \ldots, B_{i,r+1}$; then

$$B_s B_{i1} = B_s B_{i2} = \ldots = B_s B_{i,r+1} \quad (i = 1, 2, \ldots, n_2)$$

and consequently

$$B_x B_{i1} = B_x B_{i2} = \ldots = B_x B_{i,r+1} \text{ where } B_x B_{i1} = B_1.$$

Thus, there are $r+1$ B_i's which are the same as B_1 — a contradiction. Therefore each B_{i1} ($i = 1, 2, \ldots, n_2$) has r and only r B_{ij}'s which consist of the same elements; and since $B_{i1}, \ldots, B_{in}$ is a permutation of $B_1, \ldots, B_n$, the theorem is proved.

3. *Plain quasigroups.*

According to Bruck[1], a quasigroup $Q = (1, 2, \ldots, n)$ is *simple* if it has

[1] R. H. Bruck, "Simple quasigroups", *Bull. American Math. Soc.*, 50 (1944), 769–781.

https://doi.org/10.1017/S0013091500024883 Published online by Cambridge University Press

no proper homomorph. A simple quasigroup which has no subquasigroups except itself will be called *plain*. If Q is plain, every element is a generator of Q, for otherwise it would generate a subquasigroup.

Let Q be a plain quasigroup, and let N be the order of L_Q. We know that $N \leqslant n^n$ (a stronger result was proved in L.Q.I), and we shall prove that N is always some power of n. As examples, the plain quasigroups with multiplication tables

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

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

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

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

have logarithmetics of orders 4, 4^2, 4^3, 4^4. This was found by actually constructing the logarithmetics. On the other hand the simple (not plain) quasigroup given by

	1	2	3	4	5
1	2	1	4	5	3
2	1	2	5	3	4
3	4	5	3	1	2
4	5	3	2	4	1
5	3	4	1	2	5

has logarithmetic of order 2, all powers x^r being equal to either x or x^2 $(x = 1, 2, 3, 4, 5)$.

If Q is plain Theorem 1 becomes:

THEOREM 4. *If $Q = (1, 2, \ldots, n)$ is a plain quasigroup of order n, and A_i denotes the set of all quasi-integers having i in their m-th row, then*

(i) *$L_Q(+)$ is homomorphic to Q by*

$$(\textit{all quasi-integers of } A_i) \to i;$$

(ii) *all A_i are of the same order, say p;*

(iii) *the order of L_Q is $N = np$.*

THEOREM 5. *In a plain quasigroup the orders of B_i are either* 1 *or n.*

Since Q is plain, 2 is a generator of Q. Consequently, the elements of the classes $B_1, \ldots, B_n$ exhaust Q. It follows at once that if all B_i are mutually exclusive, then each B_i consists of one and only one element.

Suppose B_i are of order $k > 1$; then there exist at least two B_i's, say B_1 and B_2, with elements in common. By Theorem 2, B_1 and B_2 are the same. Let r be the number of B_i's which are the same as B_1 say

$$B_1 = B_2 = \ldots = B_r.$$

If $r = n$, all B_i are the same; consequently $Q = B_i$ and the order of B_i is n. So suppose $r < n$. Then there exists at least one B_j distinct from $B_1, \ldots, B_r$, and, by Theorem 3, r such: say

$$B_{r+1} = \ldots = B_{2r}, \quad B_{r+1} \neq B_1.$$

It follows from Theorem 3 that $B_i \cap B_j = 0$ for all $i = 1, \ldots, r$ and $j = r+1, \ldots, 2r$. Continuing this process we find that r divides n:

$$n = rs,$$

and that all B_i's fall into s mutually exclusive classes, each consisting of r identical B_i's:

$$D_1 = (B_1, \ldots, B_r), \quad D_2 = (B_{r+1}, \ldots, B_{2r}), \quad \ldots, \quad D_s = (B_{n-r+1}, \ldots, B_n).$$

The same classification divides the n elements of Q into s classes, so that r must be the same as k, the order of each B_i.

Hence the multiplication table (5) can be replaced by

$$D_\alpha D_\beta = D_{\alpha\beta} \quad (\alpha, \beta = 1, \ldots, s),$$

showing that the D_α's form a homomorph of Q. Since Q is simple, $s = n$ or $s = 1$, and $k = r = 1$ or n.

THEOREM 6. *Let $Q = (1, 2, \ldots, n)$ be a plain quasigroup of prime order n, such that 2 generates Q. If B_1 and B_2 are the same, then all B_i ($i = 1, \ldots, n$) are the same.*

If the order k of B_i is less than n, then by the proof of Theorem 5,

$$n = ks$$

and this, since n is prime, is only possible if $k = 1$ or $k = n$. Since 2 generates Q, the B_i's exhaust Q, and if two B_i's are the same, k cannot equal 1. Consequently $k = n$, and each of the B_i's consists of all the n elements of Q.

THEOREM 7. *The order of the logarithmetic of a plain quasigroup is a power of the order of the quasigroup.*

By combining $N = np$ (Theorem 4) and Lemma 1, the order of L_Q can be expressed as $N = nkq$ where N, n, k are the orders of L_Q, Q, B_i respectively and q is the order of the class of all the quasi-integers with $\{1, 2, \ldots\}$ in the first two rows. We denote by $B_{1,2,\ldots,k-1}$ the set of all distinct elements of Q in the k-th row of the quasi-integers $\{1, 2, \ldots, k-1, \ldots\}$ $(k = 2, \ldots, n)$. Then if the orders of $B_{1,\ldots,i}$ are m_i we have (Lemma 2)

$$N = n m_1 m_2 \ldots m_{n-1}$$

where, by Theorem 5, m_i are either 1 or n. The theorem follows.

DEPARTMENT OF MATHEMATICS,
UNIVERSITY OF ABERDEEN.

https://doi.org/10.1017/S0013091500024883 Published online by Cambridge University Press