BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 2(45), 2004, Pages 49–54
ISSN 1024–7696

On orders of elements in quasigroups

Victor Shcherbacov

Abstract. We study the connection between the existence in a quasigroup of (m, n)-elements for some natural numbers m, n and properties of this quasigroup. The special attention is given for case of (m, n)-linear quasigroups and (m, n)-T-quasigroups.

Mathematics subject classification: 20N05.
Keywords and phrases: Quasigroup, medial quasigroup, T-quasigroup, order of an element of a quasigroup.

1 Introduction

We shall use basic terms and concepts from books [1, 2, 11]. We recall that a binary groupoid (Q, A) with n-ary operation A such that in the equality $A(x_1, x_2) = x_3$ knowledge of any two elements of x_1, x_2, x_3 the uniquely specifies the remaining one is called a *binary quasigroup* [3]. It is possible to define a binary quasigroup also as follows.

Definition 1. *A binary groupoid $(Q, \circ)$ is called a quasigroup if for any element (a, b) of the set Q^2 there exist unique solutions $x, y \in Q$ to the equations $x \circ a = b$ and $a \circ y = b$ [1].*

An element $f(b)$ of a quasigroup $(Q, \cdot)$ is called a *left local identity element* of an element $b \in Q$, if $f(b) \cdot b = b$.

An element $e(b)$ of a quasigroup $(Q, \cdot)$ is called a *right local identity element* of an element $b \in Q$, if $b \cdot e(b) = b$.

The fact that an element e is a *left (right) identity element* of a quasigroup $(Q, \cdot)$ means that $e = f(x)$ for all $x \in Q$ (respectively, $e = e(x)$ for all $x \in Q$).

The fact that an element e is an *identity element* of a quasigroup $(Q, \cdot)$ means that $e(x) = f(x) = e$ for all $x \in Q$, i.e. all left and right local identity elements in the quasigroup $(Q, \cdot)$ coincide [1].

A quasigroup $(Q, \cdot)$ with an identity element is called a *loop.* In a loop $(Q, \cdot)$ there exists a unique identity element. Indeed, if we suppose, that 1 and e are identity elements of a loop $(Q, \cdot)$, then we have $1 \cdot e = 1 = e$.

Quasigroups are non-associative algebraic objects that, in general, do not have an identity element. Therefore there exist many ways to define the order of an element in a quasigroup.

In works [5, 6] the definition of an (n, m)-identity element of a quasigroup $(Q, \cdot)$ and some results on topological medial quasigroups with an (n, m)-identity element were given. These articles were our starting-point by the study of (m,n)-order of elements in quasigroups.

As usual $L_a : L_a x = a \cdot x$ is the left translation of quasigroup $(Q,\cdot)$, $R_a : R_a x = x \cdot a$ is the right translation of quasigroup $(Q,\cdot)$, $Mlt(Q,\cdot)$ denotes the group generated by the set of translations $\{L_x, R_y \,|\, \text{for all } x, y \in Q\}$.

An element d of a quasigroup $(Q,\cdot)$ with the property $d \cdot d = d$ is called an *idempotent element*. By ε we mean the *identity permutation*.

Definition 2. *A quasigroup $(Q,\cdot)$ defined over an abelian group $(Q,+)$ by $x \cdot y = \varphi x + \psi y + c$, where c is a fixed element of Q, φ and ψ are both automorphisms of the group $(Q,+)$, is called a T-quasigroup [9, 10].*

A quasigroup $(Q,\cdot)$ satisfying the identity $xy \cdot uv = xu \cdot yv$ is called a *medial quasigroup*. By Toyoda theorem (T-theorem) every medial quasigroup $(Q,\cdot)$ is a T-quasigroup with additional condition $\varphi\psi = \psi\varphi$ [1,2].

A loop $(Q,\cdot)$ with the identity $x(y \cdot xz) = (xy \cdot x)z$ is called a *Moufang loop*; a loop with the identity $x(y \cdot xz) = (x \cdot yx)z$ is called a *left Bol loop*.

A Moufang loop is *diassociative*, i.e. every pair of its elements generates a subgroup; a left Bol loop is a *power-associative loop*, i.e. every its element generates a subgroup [1, 4, 11].

A left Bol loop $(Q,\cdot)$ with the identity $(xy)^2 = x \cdot (y^2 \cdot x)$ is called a *Bruck loop*. Any Bruck loop has the property $I(x \cdot y) = Ix \cdot Iy$, where $x \cdot Ix = 1$ for all $x \in Q$ [11].

Definition of the order of an element of a power-associative loop $(Q,\cdot)$ can be given as definition of the order of an element in case of groups [7].

Definition 3. *The order of an element b of the power-associative loop $(Q,\cdot)$ is the order of the cyclic group $< b >$ which it generates.*

2 $(\mathbf{m},\mathbf{n})$-orders of elements

Definition 4. *An element a of a quasigroup $(Q,\cdot)$ has the order (m,n) (or element a is an (m,n)-element) if there exist natural numbers m, n such that $L_a^m = R_a^n = \varepsilon$ and the element a is not the (m_1,n_1)-element for any integers m_1, n_1 such that $1 \le m_1 < m$, $1 \le n_1 < n$.*

Remark 1. It is obvious that m is the order of the element L_a in the group $Mlt(Q,\cdot)$, n is the order of the element R_a in this group. Therefore it is possible to name the (m,n)-order of an element a as well as the (L,R)-order or the left-right-order of an element a.

Remark 2. In the theory of non-associative rings ([8]) often one uses so-called left and right order of brackets by multiplying of elements of a ring $(R,+,\cdot)$, namely $(\dots(((a_1 \cdot a_2) \cdot a_3) \cdot a_4)\dots)$ is called the left order of brackets and $(\dots(a_4 \cdot (a_3 \cdot (a_2 \cdot a_1)))\dots)$ is called the right order of brackets.

So the (m,n)-order of an element a of a quasigroup $(Q,\cdot)$ is similar to the order of an element a of a non-associative ring $(R,+,\cdot)$ with the right and the left orders of brackets respectively.

Proposition 1. *In a diassociative loop $(Q, \cdot)$ there exist only (n, n)-elements.*

Proof. If we suppose that there exists an element $a \in Q$ of diassociative loop of order (m, n), then in this case we have $L_a^m x = a \cdot (a \cdot \ldots (a \cdot x) \ldots) = a^m x = L_{a^m} x$.

Therefore $L_a^m = \varepsilon$ if and only if $a^m = 1$, where 1 is the identity element of the loop $(Q, \cdot)$. Similarly $R_a^n = \varepsilon$ if and only if $a^n = 1$.

From the last two equivalences and Definitions 3, 4 (from the minimality of numbers m, n) it follows that in a diassociative loop $m = n$, i.e. in diassociative loop there exist only (n, n)-elements. □

Remark 3. It is clear that Proposition 1 is true for Moufang loops and groups since these algebraic objects are diassociative.

From Definition 4 it follows that $(1, 1)$-element is the identity element of a quasigroup $(Q, \cdot)$, i.e. in this case the quasigroup $(Q, \cdot)$ is a loop.

Proposition 2. *Any $(1, n)$-element is a left identity element of a quasigroup $(Q, \cdot)$. In any quasigroup such element is unique and in this case the quasigroup $(Q, \cdot)$ is so-called a left loop i.e. $(Q, \cdot)$ is a quasigroup with a left identity element.*

Any $(m, 1)$-element is a right identity element of a quasigroup $(Q, \cdot)$, the quasigroup $(Q, \cdot)$ is a right loop.

Proof. If in a quasigroup $(Q, \cdot)$ an element a has the order $(1, n)$, then $a \cdot x = L_a^{\cdot} x = x$ for all $x \in Q$. If we suppose that in a quasigroup $(Q, \cdot)$ there exist left identity elements e and f, then we obtain that equality $x \cdot a = a$, where a is some fixed element of the set Q, will have two solutions, namely, e and f are such solutions. We obtain a contradiction. Therefore in a quasigroup there exists a unique left identity element. □

Using the language of quasigroup translations it is possible to re-write the definition of an (n, m)-identity element from [5, 6] in the form:

Definition 5. *An idempotent element e of a quasigroup $(Q, \cdot)$ is called an (m, n)-identity element if and only if there exist natural numbers m, n such that $(L_e^{\cdot})^m = (R_e^{\cdot})^n = \varepsilon$.*

Hence any (m, n)-identity element of a quasigroup $(Q, \cdot)$ can be called as well as *idempotent element of order* (m, n) or an *idempotent (m, n)-element*.

Theorem 1. *A quasigroup $(Q, \cdot)$ has an (m, n)-identity element 0 if and only if there exist a loop $(Q, +)$ with the identity element 0 and permutations φ, ψ of the set Q such that $\varphi 0 = \psi 0 = 0$, $\varphi^n = \psi^m = \varepsilon$, $x \cdot y = \varphi x + \psi y$ for all $x, y \in Q$.*

Proof. Let a quasigroup $(Q, \cdot)$ have an idempotent element 0 of order (m, n). Then the isotope $(R_0^{-1}, L_0^{-1}, \varepsilon)$ of the quasigroup $(Q, \cdot)$ is a loop $(Q, +)$ with the identity element 0, i.e. $x + y = R_0^{-1} x \cdot L_0^{-1} y$ for all $x, y \in Q$ ([1]). From the last equality we have $x \cdot y = R_0 x + L_0 y$, $R_0 0 = L_0 0 = 0$. Then $\varphi = R_0$, $\psi = L_0$, $L_0^m = \psi^m = R_0^n = \varphi^n = \varepsilon$.

Conversely, let $x \cdot y = \varphi x + \psi y$, where $(Q, +)$ is a loop with the identity element 0, $\varphi 0 = \psi 0 = 0$, $\varphi^m = \psi^n = \varepsilon$. Then the element 0 is an idempotent element of quasigroup $(Q, \cdot)$ of order (m, n) since $L_0^{\cdot} y = \psi y$, $R_0^{\cdot} x = \varphi x$ and $(L_0^{\cdot})^m = \psi^m = \varepsilon$, $(R_0^{\cdot})^n = \varphi^n = \varepsilon$. $\square$

3 $(\mathbf{m}, \mathbf{n})$-linear quasigroups

Definition 6. *A quasigroup $(Q, \cdot)$ of the form $x \cdot y = \varphi x + \psi y$, where φ, ψ are automorphisms of a loop $(Q, +)$ such that $\varphi^n = \psi^m = \varepsilon$, will be called an (m, n)-linear quasigroup.*

Taking into consideration Theorem 1 we see that any (m, n)-linear quasigroup $(Q, \cdot)$ is a linear quasigroup over a loop $(Q, +)$ with at least one (m, n)-idempotent element.

Lemma 1. *In an (m, n)-linear quasigroup $(Q, \cdot)$ of the form $x \cdot y = \varphi x + \psi y$, where $(Q, +)$ is a group, we have*
$L_a^{\cdot} = L_{\varphi a}^{+} \psi$, $(L_a^{\cdot})^k = L_c^{+} \psi^k$, $c = \varphi a + \psi \varphi a + \dots + \psi^{k-1} \varphi a$,
$R_a^{\cdot} = R_{\psi a}^{+} \varphi$, $(R_a^{\cdot})^r = R_d^{+} \varphi^r$, $d = \psi a + \varphi \psi a + \dots + \varphi^{r-1} \psi a$.

Proof. It is well known that if $\varphi \in Aut(Q, \cdot)$, i.e. if $\varphi(x \cdot y) = \varphi x \cdot \varphi y$ for all $x, y \in Q$, then $\varphi L_x y = L_{\varphi x} \varphi y$, $\varphi R_y x = R_{\varphi y} \varphi x$. Indeed, we have $\varphi L_a x = \varphi(a \cdot x) = \varphi a \cdot \varphi x = L_{\varphi a} \varphi x$, $\varphi R_b x = \varphi(x \cdot b) = \varphi x \cdot \varphi b = R_{\varphi b} \varphi x$.

Using these last equalities we have

$$(L_x^{\cdot})^2 = L_{\varphi x}^{+} \psi L_{\varphi x}^{+} \psi = L_{\varphi x + \psi \varphi x}^{+} \psi^2, \quad (L_x^{\cdot})^3 = L_{(\varphi x + \psi \varphi x) + \psi^2 \varphi x}^{+} \psi^3,$$

and so on. $\square$

Proposition 3. *An element a of an (m, n)-linear quasigroup $(Q, \cdot)$ over a group $(Q, +)$ has the order (k, r), where $k, r \in N$, if and only if $\varphi a + \psi \varphi a + \dots + \psi^{k-1} \varphi a = 0$, $\psi a + \varphi \psi a + \dots + \varphi^{r-1} \psi a = 0$, $k = m \cdot i$, $r = n \cdot j$, where i, j are some natural numbers.*

Proof. It is possible to use Lemma 1. If an element $a \in Q$ has an order $(k, \_)$, then the permutation $L_a^k = L_c^{+} \psi^k$, where $c = \varphi a + \psi \varphi a + \dots + \psi^{k-1} \varphi a$ is the identity permutation. This is possible only in two cases: (i) $L_c^{+} = \psi^{-k} \neq \varepsilon$; (ii) $L_c^{+} = \varepsilon$ and $\psi^k = \varepsilon$.

Case (i) is impossible. Indeed, if we suppose that $L_c^{+} = \psi^{-k}$, then we have $L_c^{+} 0 = \psi^{-k} 0$, where 0 is the identity element of the group $(Q, +)$. Further we have $\psi^{-k} 0 = 0$, $L_c^{+} 0 = 0$, $c = 0$, $L_c^{+} = \varepsilon$, $\psi^k = \varepsilon$. Therefore, if the element a has the order $(k, \_)$, then $L_c^{+} = \varepsilon$ and $\psi^k = \varepsilon$. Further, since $\psi^m = \varepsilon$, we have that $k = m \cdot i$ for some natural number $i \in N$.

Converse. If $\varphi a + \psi \varphi a + \dots + \psi^{k-1} \varphi a = 0$, $L_c^{+} = \varepsilon$ and $\psi^k = \varepsilon$ for some element a, then this element has the order $(k, \_)$.

Therefore an element a of an (m, n)-linear quasigroup $(Q, \cdot)$ over a group $(Q, +)$ will have the order $(k, \_)$ if and only if $L_c^{+} = \varepsilon$, i.e. $c = 0$, where $c = \varphi a + \psi \varphi a + \dots + \psi^{k-1} \varphi a$ and $\psi^k = \varepsilon$, i.e. $k = m \cdot i$ for some natural number $i \in N$.

Similarly any element a of an (m,n)-linear quasigroup $(Q,\cdot)$ over a group $(Q,+)$ will have the order $(\_,r)$ if and only if $R^+_d=\varepsilon$, i.e. $d=0$, where $d=\psi a+\varphi\psi a+\cdots+\varphi^{r-1}\psi a$ and $\varphi^r=\varepsilon$. Further, since $\varphi^r=\varepsilon$, we have that $r=n\cdot j$ for some natural number $j\in N$. $\square$

Proposition 4. *The number M of elements of order (mi,nj) in an (m,n)-linear quasigroup $(Q,\cdot)$ over a group $(Q,+)$ is equal to $|K(\varphi)\cap K(\psi)|$ where $K(\varphi)=\{x\in Q\,|\,\psi x+\varphi\psi x+\cdots+\varphi^{nj-1}\psi x=0\}$, $K(\psi)=\{x\in Q\,|\,\varphi x+\psi\varphi x+\cdots+\psi^{mi-1}\varphi x=0\}$.*

Proof. From Proposition 3 it follows that an element a of an (m,n)-linear quasigroup $(Q,\cdot)$ over a group $(Q,+)$ has the order (mi,nj) if and only if $\varphi a+\psi\varphi a+\cdots+\psi^{mi-1}\varphi a=0$ and $\psi a+\varphi\psi a+\cdots+\varphi^{nj-1}\psi a=0$.

In other words an element a of (m,n)-linear quasigroup $(Q,\cdot)$ over a group $(Q,+)$ has the order (mi,nj) if and only if $a\in K(\varphi)\cap K(\psi)$.

Therefore $M=|K(\varphi)\cap K(\psi)|$. $\square$

Theorem 2. *Any $(2,2)$-linear quasigroup $(Q,\cdot)$ over a loop $(Q,+)$ such that all elements of $(Q,\cdot)$ have the order $(2,2)$ can be represented in the form $x\cdot y=Ix+Iy$, where $x+Ix=0$ for all $x\in Q$.*

Proof. In this case we have $(L^{\cdot}_x)^2=L^+_{\varphi x}L^+_{\psi\varphi x}\psi^2=L^+_{\varphi x}L^+_{\psi\varphi x}=\varepsilon$ for any $x\in Q$. Then $\varphi x+(\psi\varphi x+0)=\varepsilon 0=0$ for all $x\in Q$. Therefore $x+\psi x=0$, $\psi x=-x=Ix$.

By analogy we have that $\varphi x=-x=Ix$ for all $x\in Q$. Indeed, $(R^{\cdot}_x)^2=R^+_{\psi x}R^+_{\varphi\psi x}\varphi^2=R^+_{\psi x}R^+_{\varphi\psi x}=\varepsilon$, $\psi x+\varphi\psi x=0$, $x+\varphi x=0$, $\varphi x=Ix$. $\square$

Remark 4. From Theorem 2 it follows that any $(2,2)$-linear quasigroup $(Q,\cdot)$ such that all elements of $(Q,\cdot)$ have the order $(2,2)$ exists only over a loop with the property $I(x+y)=Ix+Iy$ for all $x,y\in Q$, where $x+Ix=0$ for all $x\in Q$. A loop with this property is called an *automorphic-inverse property loop (AIP-loop).*

We notice, the Bruck loops, the commutative Moufang loops, the abelian groups are AIP-loops.

4 $(\mathbf{m},\mathbf{n})$-linear T-quasigroups

Theorem 3. *If in an (m,n)-linear T-quasigroup $(Q,\cdot)$ of the form $x\cdot y=\varphi x+\psi y$ over an abelian group $(Q,+)$ the maps $\varepsilon-\varphi,\varepsilon-\psi$ are permutations of the set Q, then all elements of the quasigroup $(Q,\cdot)$ have order (m,n).*

Proof. It is easy to see that if the maps $\varepsilon-\varphi,\varepsilon-\psi$ are permutations of the set Q, then $m>1,n>1$. From Proposition 4 it follows that the number M of elements of the order (m,n) is equal to the number $|K(\varphi)\cap K(\psi)|$, where

$$K(\varphi)=\{x\in Q|(\varepsilon+\varphi+\ \ldots\ +\varphi^{n-1})\psi x=0\},$$
$$K(\psi)=\{x\in Q|(\varepsilon+\psi+\ \ldots\ +\psi^{m-1})\varphi x=0\}.$$

Since the map $\varepsilon-\varphi$ is a permutation of the set Q, we have: $\varepsilon+\varphi+\ \ldots\ +\varphi^{n-1}=(\varepsilon+\varphi+\ \ldots\ +\varphi^{n-1})(\varepsilon-\varphi)(\varepsilon-\varphi)^{-1}=(\varepsilon-\varphi+\varphi-\varphi^2+\varphi^2-\ \ldots\ -\varphi^n)(\varepsilon-\varphi)^{-1}=(\varepsilon-\varphi^n)(\varepsilon-\varphi)^{-1}$. Since $\varphi^n=\varepsilon$ we obtain that $K(\varphi)=Q$.

By analogy it is proved that $K(\psi) = Q$. Therefore $K(\varphi) \cap K(\psi) = Q$. □

A quasigroup $(Q, \cdot)$ with the identities $x \cdot (y \cdot z) = (x \cdot y) \cdot (x \cdot z)$, $(x \cdot y) \cdot z = (x \cdot z) \cdot (y \cdot z)$ is called a *distributive quasigroup* [1].

Corollary 1. *In any medial distributive (m, n)-linear quasigroup all its elements have order (m, n).*

Proof. It is known that any medial distributive quasigroup $(Q, \cdot)$ can be presented in the form $x \cdot y = \varphi x + \psi y$, where $(Q, +)$ is an abelian group and $\varphi + \psi = \varepsilon$ [1, 12]. Therefore conditions of Theorem 3 are fulfilled in any medial distributive (m, n)-linear quasigroup. □

Acknowledgment. The author thanks G.B. Belyavskaya, E.A. Zamorzaeva and V.Yu. Kirillov for their helpful comments.

References

[1] Belousov V.D. *Foundations of the Theory of Quasigroups and Loops.* Moscow, Nauka, 1967 (in Russian).

[2] Belousov V.D. *Elements of the Quasigroup Theory, A special course.* Kishinev, Kishinev State University Press, 1981 (in Russian).

[3] Belousov V.D. *n-Ary Quasigroups*, Shtiinta, Kishinev, 1972 (in Russian).

[4] Chein O., Pflugfelder H.O., Smith J.D.H. *Quasigroups and Loops: Theory and Applications.* Heldermann Verlag, Berlin, 1990.

[5] Choban M.M., Kiriyak L.L. *The topological quasigroups with multiple identities.* Quasigroups and Related Systems, 2002, **v. 9**, p. 9–32.

[6] Choban M.M., Kiriyak L.L. *The medial topological quasigroups with multiple identities.* Applied and Industrial Mathematics. Oradea, Romania and Chishinau, Moldova. August 17-25. Kishinev, 1995, p. 11.

[7] Marshall Hall, Jr. *The Theory of Groups.* The Macmillan Company, New York, 1959.

[8] Jevlakov K.A., Slin'ko A.M., Shestakov I.P., Shirshov A.I. *Rings Close to Associative.* Moskov, Nauka, 1978 (in Russian).

[9] Kepka T., Nemec P. *T-quasigroups. Part II.* Acta Universitatis Carolinae, Math. et Physica, 1971, **12**, no. 2, p. 31–49.

[10] Nemec P., Kepka T. *T-quasigroups. Part I.* Acta Universitatis Carolinae, Math. et Physica, 1971, **12**, no. 1, p. 39–49.

[11] Pflugfelder H.O. *Quasigroups and Loops: Introduction.* Heldermann Verlag, Berlin, 1990.

[12] Shcherbacov V.A. *On linear quasigroups and their automorphism groups.* Mat. issled., vyp. 120, Kishinev, Ştiinţa, 1991, p. 104–113.

Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
5 Academiei str.
Chişinău, MD−2028
Moldova
E-mail: *scerb@math.md*

Received June 28, 2004