DEMONSTRATIO MATHEMATICA
Vol. XXXV No 3 2002

Magdi H. Armanious

COMMUTATIVE LOOPS OF EXPONENT 3 WITH $x \cdot (x \cdot y)^2 = y^2$

Abstract. It is well known that the class of Hall triple systems [5], Steiner triple systems in which each triangle generates an affine plane over GF(3), corresponds to the class of commutative Moufang loops of exponent 3 [6]. In this paper, we extend the class of algebras to the class of all commutative loops of exponent 3 satisfying the identity $x \cdot (x \cdot y)^2 = y^2$, corresponding to the class of all Steiner triple systems. Such a commutative loop of exponent 3 with $x \cdot (x \cdot y)^2 = y^2$ is polynomially equivalent to a squag.

1. Introduction

A Steiner triple system is a pair of two non-empty sets $(P; B)$ in which the set B is a class of all 3-element subsets of P such that for any two distinct elements $x, y \in P$ there is only one block $b \in B$ containing $\{x, y\}$ ([2], [7]).

A loop is a quasigroup with a neutral element, and a commutative loop is called a commutative Moufang loop of exponent 3 if it satisfies the Moufang identity $x \cdot (x \cdot (y \cdot z)) = (x \cdot y) \cdot (x \cdot z)$ and $x^3 = 1$ [1]. We can easily see that any commutative Moufang loop of exponent 3 satisfies the identity $x \cdot (x \cdot y)^2 = y^2$ by taking $y = z$ in the Moufang identity. A commutative loop of exponent 3 satisfying $x \cdot (x \cdot y)^2 = y^2$ will here be called a commutative quasi-Moufang loop of exponent 3 and more briefly a CQM-loop of exponent 3.

Bruck [1] has given a method for turning Steiner triple systems into the algebras of squags and sloops. Quackenbush [7] proved the 1-1-correspondence between Steiner triple systems and both squags and sloops. Klossek [6] has shown that the class of Steiner triple systems in which each triangle generates an affine plane over GF(3) corresponds to the class of all commutative Moufang loops of exponent 3. In section 2, we will prove the 1-1-correspondence between the class of all CQM-loops of exponent 3 and the class of all Steiner triple systems.

Klossek [6] has also proved that the commutative Moufang loops of exponent 3 are functionally equivalent to the distributive squags. To extend this relation, we have shown in section 3 that a CQM-loop of exponent 3 is functionally equivalent to a squag. And in section 4, we show that the CQM-loops of exponent 3 have the algebraic properties of congruence permutability, congruence uniformity, and that any congruence is uniquely determined by its congruence class containing the neutral element, which are the same as those of the commutative Moufang loops of exponent 3.

2. CQM-loops with $x^3 = 1$ and Steiner triple systems

In this section we will prove that there is a 1-1-correspondence between CQM-loops of exponent 3 and Steiner triple systems.

At first, we turn a Steiner triple system $(P; B)$ into an CQM-loop $(P; \cdot, e)$ of exponent 3. By choosing a fixed element $e \in P$, consider the operation "$\cdot$" defined on P as follows for all $x, y \in P$:

$$\text{(L)} \qquad x \cdot y := \begin{cases} e \Leftrightarrow \exists b = \{e, x, y\} \in B \\ x \Leftrightarrow y = e \\ z \Leftrightarrow x = y \neq e \& \{e, x, z\} \in B, \\ w \Leftrightarrow \exists b_1 = \{x, y, z\} \& b_2 = \{e, z, w\} \in B. \end{cases}$$

It is clear that the operation "$\cdot$" is a binary operation on the set P having e as a neutral element. And from the definition of the operation "$\cdot$", we have directly $x \cdot e = x$ and $x \cdot y = y \cdot x$ for all $x, y \in P$. Moreover, one can also see:

$$x^2 = z \Leftrightarrow \{e, x, z\} \in B \Leftrightarrow x \cdot x^2 = x \cdot z = e.$$

This means that $x^3 = e$ for all $x \in P$.

To prove that the equation $a \cdot x = b$ has a unique solution in P; we should consider the following four cases:

1. $e \cdot x = b \Rightarrow$ there is the unique solution $x = b$,

2. $a \cdot x = a \Rightarrow$ there is the unique solution $x = e$,

3. $a \cdot x = e \Leftrightarrow$ there is only one element x with $\{e, x, a\} \in B \Rightarrow$ there is the unique solution $x = a^2$,

4. $a \cdot x = b$ with $e \neq a \neq b \neq e \Rightarrow$ there are only two blocks b_1 & $b_2 \in B$ in the form $b_1 = \{e, b, d\} \& b_2 = \{a, d, c\} \Rightarrow$ there is a unique solution, that is $x = c$.

To complete the proof, we have to verify the identity $x \cdot (x \cdot y)^2 = y^2$. For all $x \& y \in P$;

$$\{x, y, z\} \in B \Leftrightarrow z = (x \cdot y)^2.$$

Then $x \cdot z = w \Leftrightarrow \exists_1 b_1 = \{x, z, y\} \& b_2 = \{e, y, w\} \in B$. Hence $w = y^2$ implies $x \cdot z = y^2$. Therefore, $x \cdot (x \cdot y)^2 = y^2$. This proves the first part.

Secondly, we consider a commutative loop $(L;\cdot,1)$ of exponent 3 and satisfying $x\cdot(x\cdot y)^2 = y^2$, and we turn it into a Steiner triple system $(L;B)$ by taking the set of triples B as the following:

$$B = \{\{x, y, (x\cdot y)^2\} : \text{for all } \{x,y\} \subseteq L\}.$$

To prove that $|\{x,y,(x\cdot y)^2\}| = 3$, suppose $(x\cdot y)^2 = x \Rightarrow x\cdot(x\cdot y)^2 = x^2 \Rightarrow x^2 = y^2 \Rightarrow 1 = y\cdot x^2 \Rightarrow y = x$, contradicting the fact that $y \neq x$. Also, if we suppose $(x\cdot y)^2 = y \Rightarrow x\cdot(x\cdot y)^2 = x\cdot y \Rightarrow y^2 = x\cdot y \Rightarrow y = x$, contradicting the assumption that $x \neq y$.

To show the triple $\{x, y, (x\cdot y)^2\}$ is the unique triple in B containing $\{x, y\}$; for all $\{x,y\} \subseteq P$, we consider the triple $\{x, (x\cdot y)^2, (x\cdot(x\cdot y)^2)^2\}$. From $x\cdot(x\cdot y)^2 = y^2$, we have $(x\cdot(x\cdot y)^2)^2 = y^4 = y$. Therefore, the triples $\{x, y, (x\cdot y)^2\}$ and $\{x, (x\cdot y)^2, (x\cdot(x\cdot y)^2)^2\}$ are equal. Similarly, the triples $\{x, y, (x\cdot y)^2\}$ and $\{y, (x\cdot y)^2, (y\cdot(x\cdot y)^2)^2\}$ are equal.

Hence the system $(L;B)$ is a Steiner triple system, and then the proof of the second direction of the correspondence is complete.

It will be convenient to note at this point that this correspondence is one to one. If we denote the CQM-loop with $x^3 = 1$ extracted from the Steiner triple system $(P;B)$ by $(P;\cdot_B,e)$ and the Steiner triple system extracted from the CQM-loop $(P;\cdot,e)$ with $x^3 = 1$ by $(P;B)$, then one can prove that $B_{.\mathbf{B}} = B$ as follows:

For any $\{x, y, (x._{\mathbf{B}}y)^2\} \in B$, if $e \in \{x,y\}$, then $(x._{\mathbf{B}}e)^2 = x._{\mathbf{B}}x = z \Leftrightarrow \{e, x, z\} \in B$. And if $e \notin \{x,y\}$, then $x._{\mathbf{B}}y = w \Leftrightarrow w = e$ or $\exists z$ such that $\{x,y,z\}\&\{e,w,z\} \in B \Leftrightarrow w._{\mathbf{B}}w = e$ or $w._{\mathbf{B}}w = z \Rightarrow \{x,y,e\} \in B$ or $\{x,y,z\} \in B \Rightarrow \{x,y,(x\cdot y)^2\} \in B$.

In the other direction, if $\{x,y,z\} \in B$, then $e \in \{x,y,z\}$; say $z = e$ or $e \notin \{x,y,z\}$. For the first case, if $z = e$, then

$$x._{\mathbf{B}}y = e \Rightarrow (x._{\mathbf{B}}y)^2 = z \Rightarrow \{x,y,z\} \in B_{.\mathbf{B}}.$$

For the second case, if $e \notin \{x,y,z\}$, then

$$x._{\mathbf{B}}y = w \Leftrightarrow \{e,z,w\} \in B \Leftrightarrow w._{\mathbf{B}}w = z \Leftrightarrow (x._{\mathbf{B}}y)^2 = z \Leftrightarrow \{x,y,z\} \in B_{.\mathbf{B}}.$$

Clearly one can also prove that the binary operation "$._{\mathbf{B}}$" is the same as the binary operation "$\cdot$". This completes our discussion of the one to one correspondence.

The Steiner triple system $(P;B)$ exists iff $|p| \equiv 1 \text{ or } 3 \pmod 6$ ([6], [7]). Then a CQM-loop $(L;\cdot,1)$ of exponent 3 exists iff $|L| \equiv 1 \text{ or } 3 \pmod 6$.

In the general case, the correspondence between the CQM-loops $(L;\cdot,e)$ of exponent 3 and the Steiner triple systems depends on the choice of the element e. Then for two different elements $e_1 \neq e_2$, the class of subalgebras of each corresponding commutative quasi-Moufang loop of exponent 3 depends on the choice of the neutral element e. This means that the two commutative loops $(L; \cdot_1, e_1)$ and $(L; \cdot_2, e_2)$ corresponding to a Steiner triple system may not be isomorphic. On the other hand, the commutative loops $(L; ._1, e_1)$ and $(L; ._2, e_2)$ are isomorphic, if they satisfy the Moufang identity [6].

A subspace of a Steiner triple system $(P; B)$ is a set $S \subseteq P$ that is closed under forming blocks. Accordingly, there is a 1-1 correspondence between the class of subalgebras and the class of subspaces containing the neutral element.

3. Relation between squags and CQM-loops of exponent 3

Klossek [6] proved that a commutative Moufang loop of exponent 3 is polynomially equivalent to a distributive squag. By using the same relations between the fundamental operations used by Klossek [6], one can prove that a CQM-loop $(L; \cdot, e)$ of exponent 3 is polynomially equivalent to a squag $(L; \otimes)$, as in the following theorem.

THEOREM. (I) *If* $(L; \otimes)$ *is a squag, and* $x \cdot y := e \otimes (x \otimes y)$ *for* $e \in L$, *then* $(L; \cdot, e)$ *is a CQM-loop of exponent* 3.

(II) *If* $(L; \cdot, e)$ *is a CQM-loop of exponent* 3 *and* $x * y := x^2 \cdot y^2$, *then* $(L; *)$ *is a squag.*

Proof. It is clear in the first part (I) that the operation "$\cdot$" is a commutative binary operation having e as a neutral element and $x^3 = e \otimes (x \otimes (e \otimes x) = e$. Also, $x \cdot (x \cdot y)^2 = x \cdot ((x \cdot y) \cdot (x \cdot y)) = e \otimes (x \otimes (e \otimes ((e \otimes (x \otimes y)) \otimes (e \otimes (x \otimes y))))) = e \otimes y = e \otimes (y \otimes y) = y^2$.

In the second part (II) , the operation "$*$" is a commutative binary operation and $x * x = x^4 = x$. Also, $x * (x * y) = x^2 \cdot (x^2 \cdot y^2)^2$.

In fact, the two identities $x \cdot (x \cdot y)^2 = y^2$ and $x^2 \cdot (x^2 \cdot y^2)^2 = y$ are equivalent in the commutative loop of exponent 3. This completes the proof. ∎

According to this theorem, it will be convenient to note the following two remarks:

Let $(L; \otimes)$ be a squag. By the first part (I), we have that $(L; \cdot, e)$ is a commutative loop, and by the second part (II), we again get that $(L; *)$ is a squag. In fact, $(L; \otimes)$ may be different from $(L; *)$, because $x * y = x^2 \cdot y^2 = e \otimes ((e \otimes x) \otimes (e \otimes y))$ and the right-hand side of the equation is equal to $x \otimes y$ if and only if the squag $(L; \otimes)$ is distributive.

On the other hand, if we begin with a CQM-loop $(L; \cdot, e)$ of exponent 3, then from the second part (II), we obtain that $(L; *)$ is a squag, and from the first part (I), $(L; \bullet, e)$ becomes again a CQM-loop of exponent 3. Then we have the same result that $(L; \cdot, e)$ and $(L; \bullet, e)$ are equal if and only if the commutative loop $(L; \cdot, e)$ is Moufang.

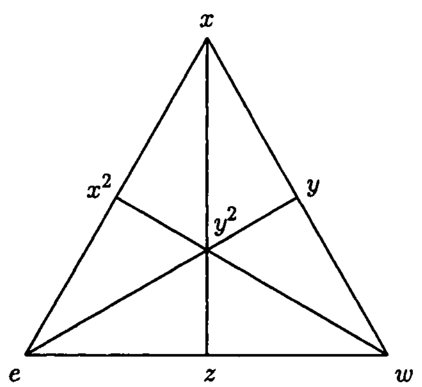
The second remark is that the Steiner identity $x \otimes (x \otimes y) = y$ in squags is translated, by using the above relation between the operations "$\cdot, e$" and

"$\otimes$" stated in the above theorem, into the identity $x^2 \cdot (x^2 \cdot y^2)^2 = y$. But if we use the identity $x^2 \cdot (x^2 \cdot y^2)^2 = y$ to define our main class of CQM-loops of exponent 3 instead of the identity $x \cdot (x \cdot y)^2 = y^2$, then the correspondence between this class of algebras and Steiner triple systems will not be one to one.

To show this difference, we consider the correspondence between the Steiner triple system $(P; B)$ and the commutative loop $(P; \cdot, e)$ of exponent 3 with $x^2 \cdot (x^2 \cdot y^2)^2 = y$.

Take the binary operation "$\cdot_{\mathbf{B}}$" defined by the same definition as given in (L). Accordingly, the definition of $B_{\cdot}$ will be equal to $\{\{x, y, x^2 \cdot y^2\} : x \& y \in P\}$ to guarantee the system $(P; B_{\cdot})$ becomes a Steiner triple system. Consequently, we can deduce that $B_{\cdot \mathbf{B}} \neq B$ and the binary operation "$\cdot_{\mathbf{B}}$." is not the same binary operation as "$\cdot$". This means that the correspondence will not be one to one.

To illustrate this observation, we take the Steiner triple system STS(7) $= (P; B)$, and by choosing the neutral element e as in the figure, then $x \cdot y = z$ and $x^2 \cdot y^2 = z$. This means that the block $\{x, y, w\} \in B$ and the block $\{x, y, z\} \in B_{\cdot \mathbf{B}}$, therefore, $B \neq B_{\cdot \mathbf{B}}$.



On the other hand, $(x \cdot y)^2 = x^2 \cdot y^2$ holds in the commutative Moufang loops of exponent 3. This means that $B = B_{\cdot \mathbf{B}}$ and $\{x, y, x^2 \cdot y^2\} = \{x, y, (x \cdot y)^2\}$ is valid only in the correspondence between the subvariety of commutative Moufang loops of exponent 3 and the subclass of the Hall triple systems [5].

4. Some properties of CQM-loops of exponent 3

The cyclic group C_3 of order 3 is a commutative Moufang loop of exponent 3, and the variety HSP(C_3) generated by C_3 is the smallest nontrivial subvariety of the class of all commutative quasi-Moufang loops of exponent

3, where H, S and P are the operators of the direct product, the subalgebra and the homomorphic image respectively [3]. The identity of the subvariety HSP (C_3) is $x \cdot (y \cdot (z \cdot w) = (x \cdot z) \cdot (y \cdot w)$. This latter identity is equivalent to the associative law. In fact, the finite algebras of the subvariety HSP(C_3) correspond to the groups $(\mathrm{GF}(3)^n; \oplus, e)$, where the operation $\oplus$ is defined by $x \oplus y = e + 2x + 2y$, for a fixed element $e \in \mathrm{GF}(3)$ and for any positive integer n ([4], [6]).

The concepts of a subloop and a normal subloop in CQM-loops of exponent 3 have the same meaning and relations as in commutative Moufang loops ([1], [6]).

$(S; \cdot, 1)$ is a subloop of a loop $(L; \cdot, 1)$ if $\emptyset \neq S \subseteq L$ and $(S; \cdot, 1)$ is a loop with the same operations "$\cdot$ and 1". A subloop $(S; \cdot, 1)$ is a normal subloop of $(L; \cdot, 1)$ if $S \cdot (x \cdot y) = (S \cdot x) \cdot y$ for all x, y in L. There is a one to one correspondence between the class of normal subloops and the class of all congruences on a CQM-loop of exponent 3.

In fact, if N is a normal subloop of $\mathbf{L} = (L; \cdot, e)$, then $\theta_N := \{(x, y) \in L^2 : x^2 \cdot y \in N\}$ is a congruence on $\mathbf{L}$ and $[e]\theta_N = N$. And if θ is a congruence on $\mathbf{L}$, then $[e]\theta = N_\theta$ is a normal subloop of $\mathbf{L}$ and $\theta_{N_\theta} = \theta$.

The congruences on a CQM-loop of exponent 3 have the same properties as in the commutative Moufang loop, as will be shown in the following theorem :

THEOREM. *The congruences of a CQM-loop* $\mathbf{L} = (L; \cdot, e)$ *of exponent* 3 *have the following properties*:

(i) $\theta \circ \phi = \phi \circ \theta$; *for any two congruences* θ *and* ϕ *of* $\mathbf{L}$.

(ii) *The congruence classes have the same cardinal number*; *for any congruence of any finite CQM-loop of exponent* 3.

Proof. It is well known that an equational class [3] has permutable congruences iff it has a Mal'cev term $p(x, y, z)$ satisfying $p(x, y, y) = x$ and $p(x, x, z) = z$. By taking $p(x, y, z) := (y \cdot (x.z)^2)^2$ one can directly prove (i).

(ii) By taking the map $f_{a,b} : [a]\theta \to [b]\theta$ defined by $f_{a,b}(x) = (x \cdot (a \cdot b)^2)^2$, one can proof that $f_{a,b}$ is a bijective mapping. This completes the proof of the theorem . ∎

References

[1] R. H. Bruck, *A Survey of Binary Systems*, Springer, Heidelberg 1971.

[2] B. Ganter, H. Werner, *Co-ordinatizing Steiner systems*, Ann. Discrete Math. 7 (1980), 3–24.

[3] G. Grätzer, *Universal Algebra*, D. van Nostrand Company, Inc. Princeton, New Jersey, Toronto, London, Melbourne 1968.

[4] A. J. Guelzow, *Representation of finite nilpotent squags*, Discrete Math. 154 (1996), 63–76.
[5] M. Hall, Jr, *Automorphisms of Steiner triple systems*, IBM J. 5 (1960), 460–472.
[6] S. Klossek, *Kommutative Spiegelungsraume*, Mitt. Math. Sem. Univ. Giessen 117 (1975).
[7] R. W. Quackenbush, *Varieties of Steiner loops and Steiner quasigroups*, Canadian. J. Math. 28 (1978), 1187–1198.

MATHEMATICS DEPARTMENT
FACULTY OF SCIENCE
MANSOURA UNIVERSITY
MANSOURA, EGYPT

Received May 4, 2001; revised version November 22, 2001.