BUCHSTEINER LOOPS AND CONJUGACY CLOSEDNESS

PIROSKA CSÖRGŐ AND ALEŠ DRÁPAL

Abstract. After exhibiting basic properties of Buchsteiner loops we introduce a construction based on rings that produces a Buchsteiner loop of order 128 that is not conjugacy closed (CC). We also show that all Buchsteiner loops of nilpotency class two are CC and discuss the squaring mapping of those CC and Buchsteiner loops Q in which both Q/N and $A \leq Z(Q)$ are boolean groups (N is the nucleus and A is the associator subloop). We prove that this mapping determines Q up to isomorphism when Q/A, N and the action of Q/A upon N are known.

If Q is a loop, then we set, as usual, $L(x,y) = L_{xy}^{-1}L_xL_y$ and $R(x,y) = R_{yx}^{-1}R_xR_y$. The *left multiplication group* of a loop Q is the permutation group generated by all $L_x : a \mapsto xa$, and we denote it by $\mathcal{L} = \mathcal{L}(Q)$. Similarly one defines the *right multiplication group* $\mathcal{R} = \mathcal{R}(Q)$. It is well known that $\mathcal{L}_1 = \{\varphi \in \mathcal{L};\ \varphi(1) = 1\}$ contains all mappings $L(x,y)$ and is generated by them. Similarly $\mathcal{R}_1 = \langle R(x,y);\ x,y \in Q\rangle$. We set $\operatorname{Mlt} Q = \langle \mathcal{L}, \mathcal{R}\rangle$, and call $\operatorname{Mlt} Q$ the *multiplication group* of Q. The *inner mapping group* $\operatorname{Inn} Q = (\operatorname{Mlt} Q)_1$ contains both $\mathcal{L}_1$ and $\mathcal{R}_1$, and is generated by $\mathcal{L}_1$, $\mathcal{R}_1$ and by all mappings $T_x = R_x^{-1}L_x$, $x \in Q$.

We shall be using the notational convention $L_{(X)} = \{L_x;\ x \in X\}$, for every $X \subseteq Q$. Similarly, $R_{(X)}$ denotes the set of all R_x, $x \in X$.

The introductory material of the first two sections partially overlaps with that of [6] and [8]. Section 3 starts with the fundamental result of [6] which states that if Q is a Buchsteiner loop with nucleus N, then Q/N is an abelian group of exponent four. The rest of Section 3 is mainly concerned with basic properties of Buchsteiner loops in which Q/N is of exponent two. The section finishes by outlining the content of Sections 4–7 (see also the Abstract).

The standard reference books for loop theory are [3] and [2].

1. Basic facts

By a *Buchsteiner loop* we shall understand a loop that fulfils the following law introduced by Hans Hoenig Buchsteiner [4]:

$$z\backslash(zx \cdot y) = (x \cdot yz)/z.$$

2000 *Mathematics Subject Classification.* Primary 20N05; Secondary 08A05.

Key words and phrases. Buchsteiner loop, nucleus.

The first author (P. Csörgő) was supported by Hungarian National Foundation for Scientific Research, grants T049841 and T038059. The second author (A. Drápal) was supported by institutional grant MSM 0021620839 and by Grant Agency of Charles University, Grant 444/2004. This paper was written while the second author was a Fulbright Research Scholar at University of Wisconsin-Madison.

Proposition 1.1. *A loop Q is a Buchsteiner loop if and only if any of the following identities holds for all $x, y, z \in Q$:*

$$R_y^{-1}L_xR_y = L_y^{-1}L_{yx}, \qquad R_z^{-1}L_x^{-1}L_yR_z = L_{zx}^{-1}L_{zy}, \qquad [R_x, L_y] = L(x,y),$$
$$L_y^{-1}R_xL_y = R_y^{-1}R_{xy}, \qquad L_z^{-1}R_x^{-1}R_yL_z = R_{xz}^{-1}R_{yz}, \qquad [L_x, R_y] = R(x,y).$$

Proof. The equality $R_y^{-1}L_xR_y = L_y^{-1}L_{yx}$ expresses the Buchsteiner identity $(x \cdot zy)/y = y\backslash(yx \cdot z)$. By inverting this equality and by multiplying it on the right by L_x one obtains $[R_y, L_x] = L(y, x)$. From the first equality we also get $R_z^{-1}L_x^{-1}L_yR_z = R_z^{-1}L_x^{-1}R_zR_z^{-1}L_yR_z = L_{zx}^{-1}L_zL_z^{-1}L_{zy} = L_{zx}^{-1}L_{zy}$. Setting $x = 1$ gives the first equality again. The rest is clear since the Buchsteiner identity is left-right symmetric. □

Corollary 1.2. *Let Q be a Buchsteiner loop. Then $(L(x,y))^{-1} = R(y,x)$ for all $x, y \in Q$. Furthermore, $\mathcal{R}_1 = \mathcal{L}_1 = \langle [L_x, R_y];\ x, y \in Q\rangle$.*

Corollary 1.3. *A loop Q is a Buchsteiner loop if and only if any of the following identities holds for all $x, y, z \in Q$:*

$$R_y^{-1}L_x^{-1}R_y = L_{yx}^{-1}L_y, \qquad R_zL_x^{-1}L_yR_z^{-1} = L_{z\backslash x}^{-1}L_{z\backslash y}, \qquad R_xL_yR_x^{-1} = L_{x\backslash 1}^{-1}L_{x\backslash y},$$
$$L_y^{-1}R_x^{-1}L_y = R_{xy}^{-1}R_y, \qquad L_zR_x^{-1}R_yL_z^{-1} = R_{x/z}^{-1}R_{y/z}, \qquad L_xR_yL_x^{-1} = R_{1/x}^{-1}R_{y/x}.$$

Proof. The equalities in the first two columns are connected to the equalities of Proposition 1.1 in a clear way, and the equalities of the third column are their obvious consequences. If $L_xR_yL_x^{-1} = R_{1/x}^{-1}R_{y/x}$ for all $x, y \in Q$, then $L_zR_x^{-1}R_yL_z^{-1} = R_{x/z}^{-1}R_{1/z}R_{1/z}^{-1}R_{y/z} = R_{x/z}^{-1}R_{y/z}$. □

The middle columns of Proposition 1.1 and Corollary 1.3 show that $L_x^{\varepsilon}R_y^{-1}R_zL_x^{-\varepsilon}$ is equal to $R^{-1}_{R_x^{-\varepsilon}(y)}R_{R_x^{-\varepsilon}(z)}$, for all $x, y, z \in Q$ and $\varepsilon \in \{-1, 1\}$. Proceeding by induction we can hence state:

Lemma 1.4. *Let Q be a Buchsteiner loop with elements $x_1, \dots, x_n$. For $\varepsilon_1, \dots, \varepsilon_n$ from $\{-1, 1\}$ set $\gamma = L_{x_1}^{\varepsilon_1} \dots L_{x_n}^{\varepsilon_n}$ and $\widehat{\gamma} = R_{x_n}^{-\varepsilon_n} \dots R_{x_1}^{-\varepsilon_1}$. Then*

$$\gamma R_y^{-1}R_z\gamma^{-1} = R^{-1}_{\widehat{\gamma}(y)}R_{\widehat{\gamma}(z)} \quad \text{for all} \quad y, z \in Q.$$

The next lemma gives another identity that characterizes Buchsteiner loops. Note that by inverting it we obtain the mirror version.

Lemma 1.5. *A loop Q is a Buchsteiner loop if and only if*

$$L_{xy}R_x^{-1}L_y^{-1} = R_zL_xR_{zx}^{-1} \quad \text{for all} \quad x, y, z \in Q.$$

Proof. When the equality is written as $L_y^{-1}R_{zx} = R_xL_{xy}^{-1}R_zL_x$, then it means $y\backslash(u \cdot zx) = ((xy)\backslash(xu \cdot z))x$, which can be expressed as $L_y^{-1}L_uR_x = R_xL_{xy}^{-1}L_{xu}$. □

Recall that the *associator subloop* $A(Q)$ is the least normal subloop A such that Q/A is a group.

Proposition 1.6. *Let Q be a Buchsteiner loop. Then $\mathcal{L} \trianglelefteq \operatorname{Mlt} Q$, $\mathcal{R} \trianglelefteq \operatorname{Mlt} Q$, $\mathcal{L}_u = \mathcal{R}_u$ for every $u \in Q$, and*

$$[\mathcal{L}, \mathcal{R}] = \langle \mathcal{L}_u;\ u \in Q\rangle \trianglelefteq \operatorname{Mlt} Q = \mathcal{L}\mathcal{R}$$

has orbits that coincide with the cosets modulo the associator subloop $A(Q)$.

Proof. The normality of $\mathcal{L}$ and $\mathcal{R}$ is clear from Proposition 1.1. We have $\mathcal{L}_1 = \mathcal{R}_1 \le [\mathcal{L}, \mathcal{R}] \trianglelefteq \operatorname{Mlt} Q$, by Corollary 1.2. Thus $\langle \mathcal{L}_u;\ u \in Q \rangle \le [\mathcal{L}, \mathcal{R}]$. To get the converse inclusion note that $[\mathcal{L}, \mathcal{R}]$ is generated by all permutations of the form $[L_x, R_y]^\gamma$, where $x, y \in Q$ and $\gamma \in \operatorname{Mlt} Q$. The equality $\mathcal{L}_u = \mathcal{R}_u$ follows from the normality of $\mathcal{L}$ and $\mathcal{R}$. Orbits of $\langle \mathcal{L}_u;\ u \in Q \rangle$ yield cosets modulo $A(Q)$ in every loop Q. □

Lemma 1.7. *If Q is a Buchsteiner loop, then the right, left and middle nucleus coincide.*

Proof. We have $a \in N_\rho$ if and only if $R_a = L_x^{-1} R_a L_x$ for all $x \in Q$, and $a \in N_\mu$ if and only if $R_{ax} = R_x R_a$ for all $x \in Q$. From $L_x^{-1} R_a L_x = R_x^{-1} R_{ax}$ we see that both conditions are the same. Hence $N_\rho = N_\mu$, and a mirror argument yields $N_\lambda = N_\mu$. □

The centralizer of $\mathcal{R}$ in $\operatorname{Mlt} Q$ is equal to $L_{(N_\lambda)}$, in every loop Q. The centralizer of a normal subgroup is a normal subgroup, and orbits of a normal subgroup of $\operatorname{Mlt} Q$ yield cosets of a normal subloop. From Lemma 1.7 we hence obtain

Proposition 1.8. *If Q is a Buchsteiner loop, then $N = N_\lambda = N_\rho = N_\mu \trianglelefteq Q$. Furthermore, $L_{(N)} \trianglelefteq \operatorname{Mlt} Q$ and $R_{(N)} \trianglelefteq \operatorname{Mlt} Q$.*

Proposition 1.9. *Let Q be a Buchsteiner loop. Then there exists an isomorphism $\mathcal{L}/L_{(N)} \cong \mathcal{R}/R_{(N)}$ that sends $L_x L_{(N)}$ to $R_x^{-1} R_{(N)}$, for every $x \in Q$.*

Proof. Denote by F the group freely generated by all L_x, $x \in Q$, and consider the surjective homorphism $F \to \mathcal{R}/R_{(N)}$ that sends each L_x to $R_x^{-1} R_{(N)}$. We wish to show that the kernel of this homomorphism contains each $L_{x_1}^{\varepsilon_1} \dots L_{x_n}^{\varepsilon_n}$ such that it is in $\mathcal{L}$ equal to some L_a, $a \in N$, where $x_1, \dots, x_n \in Q$ and $\varepsilon_1, \dots, \varepsilon_n \in \{-1, 1\}$. This will suffice, since then we have a homomorphism $\mathcal{L}/L_{(N)} \to \mathcal{R}/R_{(N)}$, and a mirror argument yields the inverse homomorphism.

Consider $\gamma = L_{x_1}^{\varepsilon_1} \dots L_{x_n}^{\varepsilon_n}$ and put $\rho = \widehat{\gamma} = R_{x_1}^{-\varepsilon_1} \dots R_{x_n}^{-\varepsilon_n}$. From Lemma 1.4 one gets $\gamma R_x \gamma^{-1} = R_{\rho(1)}^{-1} R_{\rho(x)}$, for every $x \in Q$. Assume $\gamma \in L_{(N)}$. Then γ centralizes each R_x, and so $R_{\rho(1)} R_x = R_{\rho(x)}$, for each $x \in Q$. That means $\rho(1) = a \in N$, and $\rho = R_a \in R_{(N)}$, as required. □

2. Autotopisms and extra elements

If Q is a loop and α, β and γ are permutations of Q, then (α, β, γ) is said to be an *autotopism* of Q if and only if $\alpha(x)\beta(y) = \gamma(xy)$ for all $x, y \in Q$.

Proposition 2.1. *A loop Q is a Buchsteiner loop if and only if*

$$(L_x, R_x^{-1}, L_x R_x^{-1}) \text{ is an autotopism for all } x \in Q.$$

Proof. Note that the Buchsteiner identity can be expressed as $zx \cdot (y/z) = z((xy)/z)$. □

Corollary 2.2. *A Buchsteiner loop is commutative if and only if it is an abelian group.*

Proof. Commutativity of a loop Q means that $R_x = L_x$ for all $x \in Q$. The defining autotopisms of the Buchsteiner identity then get expressed as $(R_x, L_x^{-1}, \mathrm{id}_Q)$. However, such an autotopism exists if and only if x belongs to the middle nucleus. □

Let us recall one of the most standard results of loop theory:

Lemma 2.3. *Let Q be a loop, and let (α, β, γ) be an autotopism of Q such that $\alpha(1) = 1$. Then $\beta = \gamma$ and $\beta(x) = \alpha(x)\beta(1)$ for all $x \in Q$. The mapping α is an automorphism of Q if and only if $c = \beta(1)$ belongs to N_ρ.*

A loop Q is said to satisfy the *weak inverse property* (WIP) if $(xy)\backslash 1 = y\backslash(x\backslash 1)$ for all $x, y \in Q$. In other words, Q is a WIP loop if and only if $L_x L_y L_{xy}^{-1} \in \mathcal{L}_1$ for all $x, y \in Q$. The WIP loops have been introduced by Osborn [14] who also proved that the property is left-right symmetric. Thus Q is WIP if and only if $R_y R_x R_{xy}^{-1} \in \mathcal{R}_1$ (or $1/(xy) = (1/y)/x$) for all $x, y \in Q$.

Let Q be a Buchsteiner loop. By composing the autotopisms starting with L_x, L_y and L_{yx}^{-1} we get an autotopism

$$(L(y,x),\ R_{yx}R_y^{-1}R_x^{-1},\ R_{yx}L_{yx}^{-1}L_yR_y^{-1}L_xR_x^{-1}).$$

The second and the third components are equal, as $L_{yx} = L_y R_y^{-1} L_x R_y$, by Proposition 1.1. Of course, this equality follows from Lemma 2.3 as well. Consider also the mirror version of the above autotopism. From Lemma 2.3 (and from its mirror version) one immediately gets:

Lemma 2.4. *Let Q be a Buchsteiner group with elements x and y. Then $L(y,x) \in \operatorname{Aut} Q$ if and only if $a = ((1/x)/y)(yx) \in N$, and $R(x,y) \in \operatorname{Aut} Q$ if and only if $b = (yx)(x\backslash(y\backslash 1)) \in N$. In any case,*

$$R_{yx}R_y^{-1}R_x^{-1}L(y,x)^{-1} = R_a \text{ and } L_{yx}L_x^{-1}L_y^{-1}R(x,y)^{-1} = L_b.$$

We see that in every Buchsteiner loop Q the mappings $R_{yx}R_y^{-1}R_x^{-1}L(y,x)^{-1}$ and $L_{yx}L_x^{-1}L_y^{-1}R(x,y)^{-1}$ can be regarded as a measure how far Q is from WIP.

Lemma 2.5. *Let Q be a Buchsteiner loop. Then every element of $\mathcal{R}$ can be expressed as $R_x\gamma$, where $\gamma \in \langle R_{xy}R_x^{-1}R_y^{-1};\, x, y \in Q\rangle$.*

Proof. Every element of $\mathcal{L}$ can be expressed as $L_x^{-1}\varphi$, where $x \in Q$ and $\varphi \in \mathcal{L}_1$. From Proposition 1.9 we thus see that every element of $\mathcal{R}$ can be, modulo $R_{(N)}$, expressed as $R_x\widehat{\varphi}$. The permutation $\widehat{\varphi}$ clearly belongs to the subgroup of the lemma, and $R_aR_x = R_{xa}$ for every $a \in N$. □

Proposition 2.6. *Let Q be a Buchsteiner loop. The normalizer of $L_{(Q)}$ in $\mathcal{R}$ is equal to the product of subgroups $R_{(N)}$ and $\langle R_{xy}R_x^{-1}R_y^{-1};\, x, y \in Q\rangle$.*

Proof. A right translation R_x clearly normalizes $L_{(Q)}$ if and only if it centralizes $L_{(Q)}$, and that happens if and only if it centralizes $\mathcal{L}$. Thus R_x normalizes $L_{(Q)}$ if and only if $x \in N$. From Lemma 2.5 we hence see that it suffices to prove that each $R_{xy}R_x^{-1}R_y^{-1}$ normalizes $L_{(Q)}$. Now,

$$R_{xy}R_x^{-1}R_y^{-1}L_zR_yR_xR_{xy}^{-1} = L_{L(x,y)(1)}^{-1}L_{L(x,y)(z)} = L_{L(x,y)(z)} \text{ for every } z \in Q.$$

□

Proposition 2.6 indicates that a lot can be proved about Buchsteiner loops would it be true that the group $\langle R_{xy}R_x^{-1}R_y^{-1};\ x,y \in Q\rangle$ does not deviate too much from $\mathcal{R}_1$. In [6] one can find a long and complicated argument that this is indeed true, and that is how the fundamental result on Buchsteiner loops was obtained (c. f. Section 3).

Lemma 2.7. *Let x be an element of a Buchsteiner loop Q. Then*

$$R_xR_{1/x} = (L_{1/x}L_x)^{-1}, \quad R_{1/x} = L_xR_x^{-1}L_x^{-1}, \quad R_{x\backslash 1} = R_xL_xR_x^{-1}L_x^{-1}R_x^{-1}, \text{ and}$$
$$L_xL_{x\backslash 1} = (R_{x\backslash 1}R_x)^{-1}, \quad L_{x\backslash 1} = R_xL_x^{-1}R_x^{-1}, \quad L_{1/x} = L_xR_xL_x^{-1}R_x^{-1}L_x^{-1}.$$

Proof. The middle column follows from the third column of Corollary 1.3. The first column means $R(x,1/x) = L((1/x,x))^{-1}$ and $L(x,x\backslash 1) = (R(x\backslash 1,x))^{-1}$, which are special cases of Corollary 1.2. The third column can be easily obtained from the first two. □

The following proposition uses various standard properties of loop elements. For the sake of brevity, their definitions are reiterated within the statement.

Proposition 2.8. *Let x be an element of a Buchsteiner loop Q. The following is equivalent:*

(i) *x is an LIP element, i. e. $L_x^{-1} \in L_{(Q)}$,*
(ii) *x is an RIP element, i. e. $R_x^{-1} \in R_{(Q)}$,*
(iii) *x is an IP element, i. e. it has both LIP and RIP,*
(iv) *x is an LAP element, i. e. $L_x^2 \in L_{(Q)}$,*
(v) *x is an RAP element, i. e. $R_x^2 \in R_{(Q)}$,*
(vi) *x is a flexible element, i. e. $L_xR_x = R_xL_x$,*
(vii) *x is an extra element, i. e. $(xy \cdot z)x = x(y \cdot zx)$ for all $y,z \in Q$.*

Proof. The element x is an LIP element if and only if $L_{x\backslash 1} = L_x^{-1}$. By Lemma 2.7, the latter equality is equivalent to $L_x^{-1} = R_xL_x^{-1}R_x^{-1}$, which is the same as $R_xL_x = L_xR_x$. We get $R_xL_x = L_xR_x$ in a mirror way from RIP as well. We have proved the equivalence of (i), (ii), (iii) and (vi). From

$$xx \cdot y = x \cdot xy \Leftrightarrow xy = (x \cdot yx)/x \Leftrightarrow xy \cdot x = x \cdot yx$$

we get (vi) $\Leftrightarrow$ (iv), and the equivalence with RAP follows by a mirror argument. All extra elements are flexible, and hence it remains to prove the converse.

Assume $L_xR_x = R_xL_x$. Then $(L_x, R_x^{-1}, R_x^{-1}L_x)$ is an autotopism, by Proposition 2.1, and hence $(xy)(z/x) = (x\cdot yz)/x$ for all $y,z \in Q$. We get $(xy\cdot z)x = x(y\cdot zx)$ by replacing z with zx. □

3. The fundamentals and the outline

Let us start with the main result of [6]:

Theorem 3.1. *Let Q be a Buchsteiner loop. Then $N \trianglelefteq Q$ and Q/N is an abelian group of exponent four.*

In [6] one can also find a construction of a Buchsteiner loop Q such that Q/N really contains an element of order four. The least possible order of such a loop is 64, by [9].

A loop Q is said to be an *A_ℓ-loop* if $\mathcal{L}_1 \le \operatorname{Aut} Q$, and one speaks about an A_r-loop when the mirror phenomenon takes place. By coupling Theorem 3.1 with Lemma 2.4 we obtain:

Corollary 3.2. *Every Buchsteiner loop is both an A_ℓ-loop and an A_r-loop.*

The main purpose of this paper is to study some common features of Buchsteiner loops and conjugacy closed (CC) loops. A loop Q is said to be *left conjugacy closed* (LCC) if $L_x L_y L_x^{-1} \in L_{(Q)}$ for all $x, y \in Q$. A loop is *conjugacy closed* if it is both LCC and RCC. To prove that CC loops are also both A_ℓ-loops and A_r-loops is easy [10], and it is also true that $N \trianglelefteq Q$ in every CC loop Q, with Q/N being an abelian group. The proof of the latter fact is much shorter than that of Theorem 3.1. Despite that, the fact was regarded as an open problem for many years before it was proved by Basarab [1].

Let Q be a loop with elements x, y and z. The *associator* $[x, y, z]$ is defined as $(x \cdot yz)\backslash(xy \cdot z)$. If $N \trianglelefteq Q$ and $A = A(Q) \le N = N(Q)$, then Q/A acts on N by $x^{yA} = x^y = y\backslash(xy) = T_y^{-1}(x)$, and $A \le Z(N)$. That has been observed many times, let us cite, e.g., [13] and [11]. Under the mentioned conditions clearly $L(x, y)(z) = z[x, y, z]^{-1}$, and if Q is an A_ℓ-loop, then from $L(x, y)(uv) = L(x, y)(u)L(x, y)(v)$ one obtains

$$[x, y, uv] = [x, y, u]^v [x, y, v] \text{ for all } x, y, u, v \in Q.$$

If $A(Q) \le N \trianglelefteq Q$, then $L(x, y) = L(x', y')$ if $x \equiv x' \bmod N$ and $y \equiv y' \bmod N$ (this is easy, see, e. g., [7] for a detailed proof), and therefore the associator $[-, -, -]$ can be regarded as a mapping $(Q/N)^3 \to A(Q)$. The facts of this paragraph are considered as evident further on.

Kinyon and Kunen came [12] with the following useful characterization of CC loops:

Proposition 3.3. *A loop Q is a CC loop if and only if $A(Q) \le N(Q) \trianglelefteq Q$, $Q/N(Q)$ is an abelian group and $[x_1, x_2, x_3] = [x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}]$ for all $x_1, x_2, x_3 \in Q$ and all permutations $\sigma \in S_3$.*

A counterpart to Proposition 3.3 is the following characterization of Buchsteiner loops.

Proposition 3.4. *Let Q be a loop with $A(Q) \le N(Q) \trianglelefteq Q$. Then Q is a Buchsteiner loop if and only if $[x, y, z]^x = [y, z, x]^{-1}$ for all $x, y, z \in Q$.*

Proof. The equality of the proposition corresponds to the Buchsteiner identity since $x\backslash(xy \cdot z) = x\backslash(x \cdot yz)[x, y, z] = yz[x, y, z]$ and $(y \cdot zx)/x = (yz \cdot x[y, z, x]^{-1})/x = (yz([y, z, x]^{-1})^{x^{-1}} \cdot x)/x = yz([y, z, x]^{-1})^{x^{-1}}$. □

Call a group G *boolean* if $x^2 = 1$ for all $x \in G$.

Proposition 3.5. *Let Q be an A_ℓ-loop with $N \trianglelefteq Q$ such that Q/N is a boolean group. Then Q is a Buchsteiner loop if and only if $[x, y, z] = [y, z, x]$ for all $x, y, z \in Q$.*

Proof. Consider elements x, y and z. We assume $1 = [x^2, y, z] = [x, y, z]^x [x, y, z]$, and that means that the identity of Proposition 3.4 is really equivalent to $[x, y, z] = [y, z, x]$. □

Corollary 3.6. *Let Q be an A_ℓ-loop with $N \trianglelefteq Q$ such that Q/N is a boolean group and $A(Q) \le Z(Q)$. Then $A(Q)$ is a boolean group too. Furthermore, Q is a Buchsteiner loop if and only if $[x,y,z] = [y,z,x]$ for all $x,y,z \in Q$, and Q is a conjugacy closed loop if and only if $[x,y,z] = [y,x,z] = [x,z,y]$ for all $x,y,z \in Q$.*

Proof. Consider elements x, y and z. Then $1 = [x^2,y,z] = [x,y,z]^x[x,y,z] = [x,y,z]^2$, and the rest follows from Propositions 3.4 and 3.5. □

If we assume that Q is a Buchsteiner loop, then the assumptions of Corollary 3.6 can be reduced to $A(Q) \le Z(Q)$:

Proposition 3.7. *Let Q be a Buchsteiner loop with $A(Q) \le Z(Q)$. Then both $A(Q)$ and Q/N are boolean groups, and $[x,y,z] = [y,z,x]$ for all $x,y,z \in Q$.*

Proof. We assume $[x,y,z] = [x,y,z]^x = [y,z,x]^{-1}$ for all $x,y,z \in Q$, by Proposition 3.4. Thus $[x,y,z] = [y,z,x]^{-1} = [z,x,y] = [x,y,z]^{-1}$, and $[x^2,y,z] = [x,y,z]^2 = 1$. □

By [7], if Q is a Buchsteiner loop, then $Q/Z(Q)$ has to be a CC loop. We shall call a Buchsteiner loop *proper* if it is not conjugacy closed. The proper Buchsteiner loops thus have to have a nontrivial centre. In Section 4 we shall show that a Buchsteiner loop of nilpotency class two has to be conjugacy closed. A proper conjugacy closed loop thus cannot be obtained from abelian groups too easily. In Section 5 we shall describe a general construction which derives Buchsteiner loops from (non-unitary) rings. An example based on this construction is worked out in Section 6. The construction yields loops that fulfil the conditions of Lemma 3.6. In Section 7 we consider such loops from a general point of view, and show that their structure is determined by the squaring mapping.

It is not difficult to show (c. f. [8]) that a CC loop is a Buchsteiner loop if and only if Q/N is a boolean group. However, as we shall observe, not every Buchsteiner loop such that Q is boolean modulo the nucleus has to be conjugacy closed.

4. Nilpotency class two

In loops one often works not only with the associator $[x,y,z] = (x \cdot yz)\backslash(xy \cdot z)$, but also with the commutator $[x,y] = (yx)\backslash(xy)$. In some cases the associators and commutators are bound together:

Lemma 4.1. *Let Q be a loop with $A(Q) \le N$ such that Q/N is an abelian group, and let x, y and z be elements of Q. Then*

$$[xy,z] = [x,z]^y[y,z][x,z,y]^{-1}[x,y,z][z,x,y].$$

Proof. Let us start from the identity $xy \cdot z = (x \cdot yz)[x,y,z]$ that defines the associator. We get $xy \cdot z = (x \cdot zy)[y,z][x,y,z]$ since all commutators belong to the nucleus. Working further on we obtain $xy \cdot z = (xz \cdot y)[x,z,y]^{-1}[y,z][x,y,z]$, and $xz \cdot y = zx[x,z] \cdot y = zx \cdot y[x,z]^y = (z \cdot xy)[z,x,y][x,z]^y$. We have $A(Q) \le Z(N)$ (c. f. Section 3), and so by substituting the latter equality to the former one we get

$$xy \cdot z = (z \cdot xy)[x,z]^y[y,z][x,z,y]^{-1}[x,y,z][z,x,y].$$

The statement follows from this equality immediately since $xy \cdot z$ can be also expressed as $(z \cdot xy)[xy,z]$. □

Theorem 4.2. *Let Q be Buchsteiner loop of nilpotency class two. Then Q is conjugacy closed.*

Proof. We assume that all associators and commutators are central. In particular, both Q/N and $A(Q)$ are boolean groups, by Proposition 3.7. Choose $x, y, z \in Q$, and compute $[yx, z] = [xy[y,x], z]$ by means of Lemma 4.1, with $[y, x]$ in place of y. We get $[yx, z] = [xy, z]$. Express now both $[xy, z]$ and $[yx, z]$ by means of Lemma 4.1 and compare the results. We obtain

$$[x, z, y] = [x, z, y][x, y, z][z, x, y] = [y, z, x][y, x, z][z, y, x] = [y, z, x],$$

since the associators are invariant to cyclic shifts, by Proposition 3.7. The equality we have obtained means that the associators are in fact invariant to every permutation of variables, and the conjugacy closedness thus follows from Proposition 3.3. □

Proposition 4.3. *Let Q be a Buchsteiner loop such that Q/N is a boolean group of order ≤ 4. Then Q is conjugacy closed.*

Proof. The associators are invariant to cyclic shifts, by Proposition 3.5. That implies $[x, y, y] = [y, x, y] = [y, y, x]$ for all $x, y \in Q$. Using Proposition 3.4 we get $[xy, x, y] = [x, x, y]^y[y, x, y] = [x, y, x]^{-1}[y, x, y]$. The associators depend only upon classes modulo N, and hence $[xy, x, y] = [yx, x, y] = [y, x, y]^x[x, x, y] = [y, x, y]^{-1}[x, y, x]$. Thus $[xy, x, y]$ is of exponent two, and invariant to the exchange of x and y. Therefore $[xy, x, y] = [xy, y, x]$. We see that each of $[x, y, x]$ and $[xy, x, y]$ is invariant under every permutation of arguments. Choose $u, v \in Q$ such that uN and vN generate Q/N. Each nontrivial associator of Q can be clearly obtained by permuting the arguments of some $[x, y, x]$ or $[xy, x, y]$, where $x, y \in \{u, v\}$. □

5. The ring construction

We shall work with associative rings $R(+, -, 0)$ that do not have to possess a unit. Examples of such rings are *semigroup rings* $F[S]$ over a field F and a semigroup S with multiplicative operation $\sum a_s s \cdot \sum b_t t = \sum (a_s b_t)(st)$. If S possesses an absorbing element (a zero) $z = 0$, then the zero of the ring and the zero of the semigroup can be identified. This leads to a ring defined on formal sums $\sum a_s s$, where $s \in S^{\#} = S \setminus \{0\}$, with multiplicative operation

$$\sum\nolimits_{s \in S^{\#}} a_s s \cdot \sum\nolimits_{t \in S^{\#}} b_t t = \sum\nolimits_{u \in S^{\#}} \Big(\sum\nolimits_{\substack{(s,t) \in (S^{\#})^2 \\ st=u}} a_s b_t\Big) u.$$

Such a ring will be denoted by $F[S]_0$.

Proposition 5.1. *Let R be a ring. Define multiplication on R^3 by*

$$(x, y, z) \cdot (u, v, w) = (x + u + zv, y + v + zw, z + w).$$

Then $R^3(\cdot)$ is a loop, and $(0, 0, 0)$ is the neutral element. The set $\{(x, 0, 0);\ x \in R\}$ forms a central subloop. If $\alpha_i = (x_i, y_i, z_i) \in R^3$, $1 \leq i \leq 3$, then

$$[\alpha_1, \alpha_2, \alpha_3] = (-z_1 z_2 z_3, 0, 0).$$

Proof. Only routine calculations are needed. To verify the part about the associator note that

$$\alpha_1 \cdot \alpha_2\alpha_3 = (z_1z_2z_3 + \sum_{i<j} z_iy_j + \sum_k x_k, \sum_{i<j} z_iz_j + \sum_k y_k, \sum_k z_k), \text{ and}$$

$$\alpha_1\alpha_2 \cdot \alpha_3 = (\sum_{i<j} z_iy_j + \sum_k x_k, \sum_{i<j} z_iz_j + \sum_k y_k, \sum_k z_k).$$

□

The loops of the proposition have central associators. Since we are interested in Buchsteiner loops, we have to assume that $xyz + xyz = 0$ for all $x, y, z \in R$, by Proposition 3.7. For simplicity we shall assume that $x + x = 0$ for all $x \in R$, i. e. that R is of characteristic two. In view of Propositions 3.3 and 3.7 the following two consequences do not require a proof.

Corollary 5.2. *Let R be a ring of characteristic two. Then the loop of Proposition 5.1 satisfies the Buchsteiner law if and only if $xyz = yzx$ for all $x, y, z \in R$. If this holds, then the loop is not conjugacy closed if and only if there exists $(x, y, z) \in R^3$ such that $xyz \neq xzy$.*

Corollary 5.3. *The loop of Proposition 5.1 is conjugacy closed whenever R is a commutative ring.*

Let R be a ring in which $xyz = yzx$ holds for all $x, y, z \in R$. If R possesses a unit, say 1, then $xz = x1z = 1zx = zx$, and the loop is CC, by Corollary 5.3. Hence we cannot use unitary rings to produce Buchsteiner loops by means of Proposition 5.1. If $R = F[S]$ is a semigroup ring, then the necessary condition for the equality $xyz = yzx$ is the satisfaction of the same equality in the semigroup S. We shall now observe that the converse holds as well. Note that we assume that F is a field just for simplicity—one can consider any commutative unitary ring in place of F.

Lemma 5.4. *Let F be a field and S a semigroup. If $stu = tus$ for all $s, t, u \in S$, then $abc = bca$ for all $a, b, c \in F[S]$. That holds also for all $a, b, c \in F[S]_0$ if S possesses an absorbing element.*

Proof. Indeed, if $a = \sum a_s s$, $b = \sum b_t t$ and $c = \sum c_u u$, then

$$abc = \sum a_sb_tc_u stu = \sum b_tc_ua_s tus = bca.$$

□

We thus need to construct a semigroup S such that $stu = tus$ for all $s, t, u \in S$, and such that $stu \neq sut$ for some $s, t, u \in S$. One cannot obtain S as a multiplication in a group ring since S would contain a unit. However, one can start from a graded group ring, say just with three components, so that $(\alpha_1, \alpha_2, \alpha_3)(\beta_1, \beta_2, \beta_3) = (0, \alpha_1\beta_1, \alpha_1\beta_2 + \alpha_2\beta_1)$. The product $\alpha\beta\gamma$ then equals $(0, 0, \alpha_1\beta_1\gamma_1)$, which does not really seem to solve our problem since groups with $xyz = yzx$ are necesarilly commutative. However, if one starts with a non-commutative group G that contains elements x, y and z such that $xyz = yzx$ and $yz \neq zy$, then it may be possible to modify the definition of the graded group ring in such a way that some products $(\alpha_1, 0, 0)(\beta_1, 0, 0)$ yield $(0, 0, 0)$ instead of $(0, \alpha_1\beta_1, 0)$ with the effect that the situation of $xyz \neq xzy$ is retained and the situations with $\alpha_1\beta_1\gamma_1 \neq \beta_1\gamma_1\alpha_1$ are excised.

We shall now present a class of semigroups S that fulfil our needs. The simplest example of the class can be obtained by the process described in the preceding paragraph, by applying it to $G = Q_8$, the group of quaternions, and to $(x, y, z) = (i, j, k)$.

Proposition 5.5. *Let $S = A \cup B \cup \{0, c\}$, where $A = \bigcup A_i$ and $B = \bigcup B_i$, $1 \le i \le 3$, with all unions being disjoint and all sets nonempty, $c \ne 0$. Let $\cdot$ be a binary operation on S such that*

(1) *$xy \in B_{i+2}$ if $(x, y) \in A_i \times A_{i+1}$;*
(2) *$xy = c$ if $(x, y) \in (A_i \times B_i) \cup (B_i \times A_i)$; and*
(3) *$xy = 0$ in all other cases.*

Then $S(\cdot)$ is a semigroup, $xyz \in \{0, c\}$ for all $x, y, z \in S$, and $xyz = c$ if and only if $(x, y, z) \in A_i \times A_{i+1} \times A_{i+2}$, for some $i \in \{1, 2, 3\}$. (The indices are computed modulo 3.)

Proof. If any of $x, y, z \in S$ belongs to B_i, $1 \le i \le 3$, or to $\{0, c\}$, then both $x \cdot yz$ and $xy \cdot z$ have to vanish. Assume $x \in A_i$, $y \in A_j$ and $z \in A_k$, where $i, j, k \in \{1, 2, 3\}$. Note that neither xy nor yz can be an element of B_j. Thus $x \cdot yz = xy \cdot z = 0$ if $i = j$ or $j = k$. Similarly, $xy \notin B_i$ and $yz \notin B_k$, and so we get zeros again if $i = k$. If $j \equiv i + 1$ and $k \equiv i + 2 \bmod 3$, then $xy \in B_k$ and $yz \in B_i$, and thus $x \cdot yz = xy \cdot z = c$. If $j \equiv k + 1$ and $i \equiv k + 2 \bmod 3$, then $xy = 0 = yz$. □

Proposition 5.6. *Let S be a semigroup constructed in Proposition 5.5. Put $R = F[S]_0$, where $F = \{0, 1\}$ is the two-element field, and consider the loop on R^3 described in Proposition 5.1. This loop fulfils the Buchsteiner law and is not conjugacy closed.*

Proof. From Proposition 5.5 and from Lemma 5.4 we see that R fulfils the conditions of Corollary 5.2. □

Corollary 5.7. *There exists a proper Buchsteiner loop Q such that $A(Q) \le Z(Q)$.*

6. Small order

Put $F = \{0, 1\}$ and let S be a semigroup on $\{a_1, a_2, a_3, b_1, b_2, b_3, c, 0\}$ such that

$$a_i a_{i+1} = b_{i+2},\ a_i b_i = b_i a_i = c, \text{ and } xy = 0$$

in all other cases, $1 \le i \le 3$. Put $R = F[S]_0$ and denote by R_3 the loop on R^3 defined by the formula of Proposition 5.1. From Proposition 5.6 we know that R_3 is a proper Buchsteiner loop.

Lemma 6.1. *The set of all $(\lambda c, \sum_{i \in I} b_i, \sum_{j \in J} a_j)$, where $\lambda \in \{0, 1\}$, $I \subseteq \{1, 2, 3\}$ and $J \subseteq \{1, 2, 3\}$, forms a subloop of R_3.*

Proof. The loop R_3 is finite, and hence it suffices to show that the set is closed under multiplication. We have

$$(\lambda c, \sum_{i \in I} b_i, \sum_{j \in J} a_j) \cdot (\lambda' c, \sum_{i' \in I'} b_{i'}, \sum_{j' \in J'} a_{j'}) =$$
$$((\lambda + \lambda')c + \sum a_j b_{i'}, \sum b_i + \sum b_{i'} + \sum a_j a_{j'}, \sum a_j + \sum a_{j'}).$$

Each of products $a_j b_{i'}$ is equal to c or to 0, and each product $a_j a_{j'}$ is equal to 0 or to b_{j+2}. □

Let the subloop described in Lemma 6.1 be denoted by Q_3.

Proposition 6.2. *Put $Q = Q_3$. Then Q is a Buchsteiner loop of order 128 that is not conjugacy closed, $A(Q) = Z(Q)$ is of order two, and $|N(Q)| = 16$.*

Proof. If $\alpha_k = (\lambda_k c, \sum_{i_k \in I_k} b_{i_k}, \sum_{j_k \in J_k} a_{j_k})$, $k \in \{1,2,3\}$, then $[\alpha_1, \alpha_2, \alpha_3] = (\sum a_{j_1} a_{j_2} a_{j_3}, 0, 0)$, where $(j_1, j_2, j_3) \in J_1 \times J_2 \times J_3$, by Lemma 5.1. A subloop of a Buchsteiner loop has to be a Buchsteiner loop, and the associator formula shows that Q_3 inherits fully the associator behaviour of R_3. We also see that $(u, v, w) \in N(Q)$ if and only if $w = 0$, and so it remains to prove that $(c, 0, 0)$ is the only nontrivial central element.

If $\alpha = (0, 0, \sum_{j \in J} a_j)$ and $\beta = (0, \sum_{i \in I} b_i, 0)$, then $[\beta, \alpha] = (\lambda c, 0, 0)$, where $\lambda \equiv |I \cap J| \bmod 2$. Hence $\beta \notin Z(Q)$. □

Lemma 6.3. *Every nontrivial normal subloop of Q_3 contains the centre.*

Proof. Let U be a normal subloop of S. If $\alpha_3 \in U \setminus N(Q)$, then the associator formula guarantees the existence of $\alpha_1, \alpha_2 \in Q$ such that $(c, 0, 0) = [\alpha_1, \alpha_2, \alpha_3]$. We have $L(\alpha_1, \alpha_2)(\alpha_3) = \alpha_3[\alpha_1, \alpha_2, \alpha_3]^{-1}$, and so $(c, 0, 0) \in U$.

Suppose that $U \leq N(Q)$ and consider $\beta \in U \setminus Z(Q)$. Then $T_\alpha^{-1}(\beta) \in U$, and $[\beta, \alpha]$ belongs to U too, since it equals $\beta \backslash T_\alpha^{-1}(\beta) \in U$, as $(\alpha\beta)(\beta\backslash(\alpha\backslash(\beta\alpha))) = \beta\alpha$. The formula at the end of the proof of Proposition 6.2 shows that we can always choose α in such a way that $[\beta, \alpha] = (c, 0, 0)$. □

It is worth noting that the defining relations for $Q/Z(Q)$ are easy to state. Identify a_i with $(0, 0, a_i)Z(Q)$. Then $Q/Z(Q)$ can be expressed by $\langle a_1, a_2, a_3;$ $[a_i, a_{i+1}]^2 = 1 = a_i^2, [a_i, a_{i+1}] = [a_i, a_{i+1}]^{a_j} \rangle$. Indeed, it is straightforward to verify that these relations really hold, and, on the other hand, that a group with such relations has at most 64 elements. The group $G = Q/Z(Q)$ is of nilpotency class two, with $Z(G) = N/Z(Q)$ being an elementary abelian group of order 8 with generators $(a_i a_{i+1})^2 = [a_i, a_{i+1}]$.

Note also that $N(Q)$ is an elementary abelian group of order 16.

Lemma 6.4. *Every proper subloop of Q_3 is conjugacy closed.*

Proof. Let P be a subloop of Q. If $PN \neq Q$, then $P/(P \cap N) \cong (PN)/N$ and $P \cap N \subseteq N(P)$ imply that $P/N(P)$ is a boolean group of order ≤ 4, and so one can use Proposition 4.3. Assume $PN = Q$ and put $G = Q/Z(Q)$. For each $i \in \{1,2,3\}$ there exists an $n_i \in N$ such that $n_i(0, 0, a_i) \in P$. Therefore $(c, 0, 0) \in P$. Put $U = S/Z(Q)$. We assume $UZ(G) = G$, and hence for all $i \in \{1,2,3\}$ there exists $a_i' \in U$ such that $a_i' = a_i z_i$ for some $z_i \in Z(G)$. Then $[a_i, a_{i+1}] = [a_i', a_{i+1}'] \in U$, and thus $U \geq Z(G)$, $U = G$ and $P = Q$. We see that no proper subloop P of Q satisfies $PN = Q$. □

Call a loop Q a *minimal proper Buchsteiner loop* if it is a proper Buchsteiner loop such that each proper subloop and each proper factor are conjugacy closed. From Lemmas 6.3 and 6.4 we directly obtain:

Corollary 6.5. *Loop Q_3 is a minimal proper Buchsteiner loop.*

Loops R_3 and Q_3 are historically the oldest proper Buchsteiner loops. Their discovery refuted the conjecture that all Buchsteiner loops are conjugacy closed. Later it was established that 32 is the least order for which proper Buchsteiner loops exist [9]. However, up to now none of the other proper Buchsteiner loops found was described in a way that allows easy computations, and so Q_3 seems to remain to be the most transparent proper Buchsteiner loop.

Lemma 6.6. *Let $\alpha = (\lambda c, \sum_{i\in I} b_i, \sum_{j\in J} a_j)$ be an element of Q_3. Then α is an extra element if and only if $|J| \le 1$, and $\alpha = \beta^2$ for some $\beta \in Q_3$ if and only if $J = \emptyset$ and $|I| \ne 2$.*

Proof. The element α is an extra element if and only if $[\alpha, \beta, \alpha] = (0,0,0)$, for all $\beta \in Q_3$, by point (vi) of Proposition 2.8. Put $a = \sum_{j\in J} a_j$. From the associator formula we see that α is an extra element if and only if $axa = a^2x = 0$ holds for all $x = \sum_{j'\in J'} a_{j'}$ (the multiplication being that of the ring $F[S]_0$). If $a^2 \ne \{0, c\}$, then clearly $a^2x \ne 0$ for some choice of x. The element α is hence an extra element if and only if $a^2 \in \{0, c\}$, and that is true exactly when $|J| \le 1$.

Note that $\alpha^2 = (\sum a_j b_i, \sum a_j a_{j'}, 0)$, where $i \in I$ and $j, j' \in J$. Now, $\sum a_j b_i = \nu c$, where $\nu \equiv |I \cap J| \bmod 2$. If $J \ne \emptyset$, then the size of $I \cap J$ can be both even and odd, and so the leftmost term of a square element can be both c and 0, independently of the middle term. If $|J| \le 1$, then the middle term vanishes. If $J = \{i, i+1\}$, then it equals b_{i+1}, and it is equal to $b_1 + b_2 + b_3$ when $J = \{1, 2, 3\}$. □

We see that neither squares nor extra elements of a Buchsteiner loop have to form a subloop. This contrasts with the situation of CC loops. By [12, Theorem 4.12] extra elements of a CC loop yield a normal subloop. The squares, of course, need not form a subgroup even in a group.

It is no coincidence that all squares of Q_3 are extra elements. Such an inclusion holds in all Buchsteiner loops since, by [6], all associators $[x^2, y, z^2]$ are trivial, and so each square is flexible, and hence extra.

7. Squares

The most famous CC loop is the Parker loop that can be used for a construction of the Monster group. It belongs to the wider class of *code loops* [5], i. e. conjugacy closed loops that are boolean modulo a two-element central subloop.

The structure of a code loop is determined by the squaring operation $x \mapsto x^2$, and we shall show that a similar result can be obtained for Buchsteiner loops with $A(Q) \le Z(Q)$.

From Proposition 3.7 and Lemma 4.1 we directly obtain:

Lemma 7.1. *Let Q be a Buchsteiner loop with $A(Q) \le Z(Q)$. Then $[xy, z] = [x, z]^y [y, z][z, y, x]$.*

Let Q be a Buchsteiner loop with central associators, i. e. with $A(Q) \le Z(Q)$. The associators depend only upon the classes modulo N, and so there exists a mapping $A : (Q/N)^3 \to A(Q)$, $A(xN, yN, zN) = [x, y, z]$. This mapping is invariant under cyclic shifts. A commutator $[x, y]$ does not change when x or y are replaced by an element equivalent modulo $Z(Q)$. Hence there exists a mapping $C : G^2 \to N$, $C(xA(Q), yA(Q)) = [x, y]$, where $G = Q/A(Q)$. We have $C(h, g) = C(g, h)^{-1}$ since $xy[y, x] = yx$ implies $yx[y, x]^{-1} = xy$. The group $A(Q)$ is boolean, and hence the squaring mapping $x \to x^2$ gives rise to a mapping $P : G \to A(Q)$ since $x^2 = (xa)^2$ whenever $x \in Q$ and $a \in A(Q)$.

In code loops the mappings P, C and A are interconnected by the polarization process [15], with C and A being the second and the third derived mapping of P, respectively.

For simplicity, let us regard A also as a mapping $G^3 \to A(Q)$. The associators are central and of exponent two, and so one can read the equality of Lemma 7.1 in the form

$$A(k, h, g) = C(g, k)^h C(h, k) C(gh, k)^{-1} \text{ for all } g, h, k \in G.$$

Other expressions can be obtained by applying a cyclic shift. The equation tells that C determines A if there are known G and N and the action of G upon N.

The mapping A is compatible with multiplication in each coordinate. This is also true for the mapping $D : (Q/N)^2 \to A(Q)$, $D(u, v) = A(u, v, u)A(v, u, v)$. This mapping fulfils $D(u, u) = 1$ and $D(u, v) = D(v, u)$. If $A(Q)$ consists of only two elements, then we can regard Q/N as a vector space over $A(Q)$. In such a case D becomes an alternating bilinear form.

Lemma 7.2. *Let Q be a Buchsteiner loop with $A(Q) \le Z(Q)$, and let x and y be elements of Q. Then*

$$(xy)^2 = x^2 y^2 [y, x]^y [y, x, y][x, y, x].$$

Proof. We have $(xy)^2 = xy \cdot xy = x(y \cdot xy)[x, y, xy] = x(yx \cdot y)[y, x, y]d$, where $d = [x, y, xy] = [x, y, x][x, y, y] = [y, x, y][x, y, x]$. By continuing we obtain $(xy)^2 = x(xy[y, x] \cdot y)[y, x, y]d = x(xy \cdot y)[y, x, y][y, x]^y d = x(x \cdot y^2)[y, x]^y d$, and this is equal to $x^2 y^2 [y, x]^y d$ since $y^2 \in N$. $\square$

Lemma 7.2 can be expressed by the equation

$$C(g, h) = (P(gh)^{-1} P(g) P(h))^{h^{-1}} D(g, h) \text{ for all } g, h \in G.$$

The question is whether we can express $D(g, h)$ only by means of P. The associator formula of Lemma 7.1 gives $A(h, g, h) = C(g, h)C(hg, h)^{-1}$ since $C(h, h) = 1$. Let us express $C(g, h)$ and $C(hg, h)^{-1}$ by the commutator formula of Lemma 7.2. The D-parts together contribute $D(g, h)D(hg, h) = D(g, h)D(h, h)D(g, h) = D(g, h)^2 = 1$. Hence

$$A(h, g, h) = (P(gh)^{-1} P(g) P(h) P(h)^{-1} P(hg)^{-1} P(hgh))^{h^{-1}} = \\ P(gh)^{-1} P(g) P(hg)^{-1} P(hgh) \text{ for all } g, h \in G.$$

Thus $A(g, h, g) = P(hg)^{-1} P(h) P(gh)^{-1} P(ghg) = P(gh)^{-1} P(ghg) P(hg)^{-1} P(h) = P(h)^{-1} P(hg) P(ghg)^{-1} P(gh)$ since all associators are central and of exponent two. Therefore

$$D(g, h) = A(g, h, g)A(h, g, h) = P(h)^{-1} P(hg) P(ghg)^{-1} P(g) P(hg)^{-1} P(hgh).$$

Let us record the preceding observations as a lemma.

Lemma 7.3. *Let Q be a Buchsteiner loop with $A(Q) \le Z(Q)$, and let x and y be elements of Q. Then $[x, y, x] = (xy)^{-2} x^2 (yx)^{-2} (xy \cdot x)^2$ and*

$$[x, y, x][y, x, y] = x^{-2} (xy)^2 (yx \cdot y)^{-2} y^2 (xy)^{-2} (xy \cdot x)^2.$$

We have already observed that in our situation the squares x^2, $x \in Q$, depend only upon the class x modulo $A(Q)$. Let $\alpha^{(2)}$ mean x^2 when $\alpha = xA(Q)$.

Proposition 7.4. *Let Q_1 and Q_2 be two Buchsteiner loops with $A(Q_i) \le Z(Q_i)$, $i \in \{1,2\}$, and let $g : Q_1/A(Q_1) \cong Q_2/A(Q_2)$ and $h : N(Q_1) \to N(Q_2)$ be isomorphisms such that $g(nA(Q_1)) = h(n)A(Q_2)$ and $h(n^\alpha) = h(n)^{g(\alpha)}$ for all $n \in N(Q_1)$ and $\alpha \in Q_1/A(Q_1)$. If $h(\alpha^{(2)}) = g(\alpha)^{(2)}$ for all $\alpha \in Q_1/A(Q_1)$, then there exists an isomorphism $f : Q_1 \cong Q_2$ that induces both g and h.*

Proof. Denote by Γ the class of all bijections $f : Q_1 \to Q_2$ that induce both g and h (that means that the restriction of f to $N(Q_1)$ yields h, and the factorization modulo $A(Q_i)$ yields g). The question is if f can be chosen in such a way that $f(xy) = f(x)f(y)$ for all $x, y \in Q$.

If $f \in \Gamma$ and $x \in Q_1$, then $f(x^2) = h(x^2) = h((xA(Q_1))^{(2)}) = g(xA(Q_1))^{(2)} = (f(x)A(Q_2))^{(2)} = f(x)^2$. Thus $f(x^2) = f(x)^2$ for all $f \in \Gamma$ and all $x \in Q_1$. From Lemmas 7.1, 7.2 and 7.3 we see that this implies $f([x, y]) = [f(x), f(y)]$ and $f([x, y, z]) = [f(x), f(y), f(z)]$, for all $x, y, z \in Q_1$ and all $f \in \Gamma$.

The group $Q_1/N(Q_1)$ is boolean, and hence can be considered as a vector space. Let $e_i \in Q_1$, $i \in I$, be such that the cosets $e_iN(Q_1)$ form a basis of $Q_1/N(Q_1)$. Choose an linear ordering $<$ of I. For a nonempty finite subset $J \subseteq I$ denote by $\omega(J)$ the maximum element of J, and set also $\omega(\emptyset) = \emptyset$ and $\alpha(J) = J \setminus \{\omega(J)\}$. Define recursively $e_\emptyset = 1$ and $e_J = e_{\alpha(J)}e_{\omega(J)}$. For example, if $J = \{i, j, k\}$ and $i < j < k$, then $e_J = (e_ie_j)e_k$.

For every $i \in I$ choose $f(e_i) \in g(e_iA(Q_1))$ and define recursively $f(e_J) = f(e_{\alpha(J)})f(e_{\omega(J)})$. Every $x \in Q_1$ possesses a unique expression in the form e_Jn, where J is a finite subset of I and $n \in N(Q_1)$. The definition of the mapping $f : Q_1 \to Q_2$ gets complete by setting $f(x) = f(e_J)h(n)$. By reviewing the definition we easily observe that f belongs to Γ.

Let J and K be two finite subsets of I, and suppose that $f(e_Je_K) = f(e_J)f(e_K)$. Then for all $n, m \in N(Q_1)$ we obtain $f(e_Jn \cdot e_Km) = f(e_Je_K \cdot n^{e_KA(Q_1)}m) = f(e_Je_K)h(n^{e_KA(Q_1)}m) = f(e_Je_K)h(n)^{g(e_KA(Q_1)}h(m)$, and that can be expressed as $f(e_J)f(e_K)h(n)^{f(e_K)A(Q_2)}h(m) = f(e_J)h(n)f(e_K)h(m) = f(e_Jn)f(e_Km)$.

To prove $f(e_Je_K) = f(e_J)f(e_K)$ we shall proceed by induction on $s = |J| + |K|$. The cases $J = \emptyset$ and $K = \emptyset$ are clear, and so we can assume that both J and K are nonempty. Thus $s \ge 2$. Put $o = \omega(J)$, $p = \omega(K)$, $J' = \alpha(J)$ and $K' = \alpha(K)$. If $p > o$ and $K' = \emptyset$, then the desired identity is a reiteration of the definition of f. Let us assume that this case does not take place. If $s = 2$, then either $o = p$ or $o > p$. In the former case $f(e_o^2) = f(e_o)^2$ because $f \in \Gamma$. In the latter case $f(e_oe_p) = f(e_pe_0 \cdot [e_0, e_p]) = f(e_pe_o)h([e_o, e_p]) = f(e_p)f(e_o)[f(e_o), f(e_p)] = f(e_0)f(e_p)$.

Let $s > 2$ and $K' = \emptyset$. Then $f(e_Je_K) = f(e_{J'}e_o \cdot e_p) = f(e_{J'} \cdot e_oe_p)h([e_{J'}, e_o, e_p])$. If $o = p$, then $f(e_Je_K) = f(e_{J'})(f(e_o))^2[f(e_{J'}), f(e_o), f(e_o)] = f(e_{J'})f(e_o) \cdot f(e_o) = f(e_J)f(e_K)$. If $o > p$, then $f(e_Je_K) = f(e_{J'} \cdot e_pe_o)[f(e_o), f(e_p)][f(e_{J'}), f(e_o), f(e_p)]$. Now, $f(e_{J'} \cdot e_pe_o) = f(e_{J'}e_p \cdot e_o)[f(e_{J'}), f(e_p), f(e_o)]$ and $e_{J'}e_p = e_{J''}n$ for some $n \in N(Q_1)$ and a finite set $J'' \subseteq I$ such that $|J''| \le |J|$ and $\omega(J'') < o$. We have $f(e_{J'}e_p \cdot e_o) = f(e_{J''}n \cdot e_o) = f(e_{J''}n)f(e_o) = f(e_{J'}e_p) \cdot f(e_o) = f(e_{J'})f(e_p) \cdot f(e_o)$, by the induction assumption and by $f(e_{J''}e_o) = f(e_{J''})f(e_o)$. Working back we get $f(e_{J'} \cdot e_pe_o) = f(e_{J'}) \cdot f(e_p)f(e_o)$ and $f(e_Je_K) = f(e_{J'}) \cdot f(e_o)f(e_p)[f(e_{J'}, f(e_o), f(e_p)] = f(e_{J'})f(e_o) \cdot f(e_p) = f(e_J)f(e_K)$.

If $s > 2$ and $K' \ne \emptyset$, then the induction assumption and the preceding part of the proof yield $f(e_J \cdot e_{K'}e_p) = f(e_Je_{K'} \cdot e_p)f([e_J, e_{K'}, e_p]) = f(e_J)f(e_{K'}) \cdot f(e_p)[f(e_J), f(e_{K'}), f(e_p)]$, and that gives $f(e_J) \cdot f(e_{K'}f(e_p) = f(e_J)f(e_K)$. $\square$

Proposition 7.5. *Let $\mathcal{Q}$ be a class of Buchsteiner loops such that all elements Q of $\mathcal{Q}$ share $A = A(Q)$, $N = N(Q)$, $G = Q/A$ and the action of $G = Q/A$ upon N. Assume that G centralizes A (in other words $A(Q) \le Z(Q)$ for all $Q \in \mathcal{Q}$.) Let $\bar{e}_i \in G$, $i \in I$ generate G modulo N/A. If $Q \in \mathcal{Q}$, and $e_i \in \bar{e}_i$, $h \in I$, then the quantities e_i^2, $[e_i, e_j]$ and $[e_i, e_j, e_k]$ depend only upon classes $\bar{e}_i$, $\bar{e}_j$ and $\bar{e}_k$, for all $i, j, k \in I$.*

For all $i \in I$, $(i, j) \in I^2$ and $(i, j, k) \in I^3$ consider $d_i \in N$, $c_{ij} \in N$ and $a_{ijk} \in A$, respectively. There exists, up to isomorphism, at most one loop $Q \in \mathcal{Q}$ such that $e_i^2 = d_i$, $[e_i, e_j] = c_{ij}$ and $[e_i, e_j, e_k] = a_{ijk}$.

Proof. We know that x^2, $[x, y]$ and $[x, y, z]$ depend only upon cosets modulo $A(Q)$, and this is also true, of course, for the special case of $(x, y, z) = (e_i, e_j, e_k)$.

We shall show that x^2 can be uniquely derived from d_i, c_{ij} and a_{ijk}. Associators are linear in each variable, so $[x, y, z]$ is known for all $x, y, z \in Q$. The commutators have to satisfy $[x, y]^{-1} = [y, x]$, and hence Lemma 7.1 can be used to derive them all. However, note that to be rigorous we have to use, in addition, the variants of the lemma that express $[x/y, z]$ and $[x\backslash y, z]$ since we are proving that $[x, y]$ is known for all x and y from the subloop generated by $\{e_i;\ i \in I\} \cup N$. Elements $n \in N$ may be included because $[n, x] = n^{-1}n^x$ for all $x \in Q$ and $n \in N$. Lemma 7.2 can be now used in a similar manner to prove that it is possible to uniquely derive all second powers.

The rest follows from Proposition 7.4 when used with $g = \mathrm{id}_G$ and $h = \mathrm{id}_N$. □

Let us consider again mappings P, C and A. Proposition 7.5 states that Q is determined, up to isomorphism, by all $P(\bar{e}_i) = d_i$, $C(\bar{e}_i, \bar{e}_j) = c_{ij}$ and $A(\bar{e}_i, \bar{e}_j, \bar{e}_k) = a_{ijk}$. There are some obvious necesary conditions for Q to exist, like $c_{ji} = c_{ij}^{-1}$ and $a_{ijk} = a_{jki}$. We defer the constructive counterpart of Proposition 7.5 to later studies.

Let us finally remark that if the mapping D vanishes, i. e. if $[x, y, x] = [y, x, y]$ for all $x, y \in Q$, then Q has to be a WIP loop. Indeed, an A_ℓ-loop Q is a WIP loop if and only if $y(x(yx)) = (yx)(yx)$ for all $x, y \in Q$, by [8]. In our situation this means $1 = [y, x, yx] = [y, x, y][y, x, x] = [y, x, y][x, y, x]$. So, in fact, Q is a WIP loop if and only if D vanishes. However, in such a case we get a CC loop since all WIP Buchsteiner loops are conjugacy closed [6, 8].

References

[1] A. S. Basarab: Klass LK-lup, *Mat. Issled.* **120** (1991), 3–7, 118.
[2] V. D. Belousov: *Osnovy teorii kvazigrupp i lup*, Nauka, Moskva, 1967.
[3] R. H. Bruck: *A survey of binary systems*, Springer Verlag, 1958.
[4] H. H. Buchsteiner: O nekotorom klasse binarnych lup, *Mat. Issled.* **39** (1976), 54–66.
[5] R. L. Griess: Code loops, *J. Algebra* **100** (1986), 224–234.
[6] P. Csörgő, A. Drápal and M. K. Kinyon: Buchsteiner loops (submitted).
[7] P. Csörgő and A. Drápal: Loops that are conjugacy closed modulo the center (submitted).
[8] A. Drápal and P. Jedlička: On loop identities that can be obtained by a nuclear identification (submitted).
[9] A. Drápal and M. K. Kinyon: Buchsteiner loops: constructions and associators (submitted).
[10] E. G. Goodaire and D. A. Robinson: A class of loops which are isomorphic to all loop isotopes, *Canad. J. Math.* **34** (1982), 662–672.
[11] M. K. Kinyon, K. Kunen and J. D. Phillips: Diassociativity in conjugacy closed loops, *Comm. Algebra* **32** (2004), 767–786.
[12] M. K. Kinyon and K. Kunen: Power-associative, conjugacy closed loops, *J. Algebra* **304** (2006), 679–711.

[13] K. Kunen: The structure of conjugacy closed loops, *Trans. Amer. Math. Soc.* **352** (2000), 2889–2911.
[14] J. M. Osborn: Loops with the weak inverse property, *Pacific J. Math.* **10** (1960), 295–304.
[15] H. N. Ward: Combinatorial polarization, *Discrete Math.* **26** (1979), 185–197.

Dept. of Mathematics, Eötvös University, Pázmány Péter sétány 1/C, H-1117 Budapest, Hungary
E-mail address: ska@cs.elte.hu

Dept. of Mathematics, Charles University, Sokolovská 83, 186 75 Praha 8, Czech Rep.
E-mail address: drapal@karlin.mff.cuni.cz