On extraspecial left conjugacy closed loops

Aleš Drápal

Charles University, Faculty of Mathematics and Physics, Sokolovská 83, 186 75 Praha 8, Czech Republic

Received 30 October 2004
Available online 5 June 2006
Communicated by Jan Saxl

Abstract

A loop \( Q \) is said to be left conjugacy closed (LCC) if \( L_x L_y L_x^{-1} \) is a left translation for all \( x, y \in Q \). We describe all LCC loops \( Q \) such that \( Q/Z \) is an elementary abelian \( p \)-group, where \( Z \triangleleft Q \) is a central subloop of order \( p \). We single out those that are right conjugacy closed as well, and show their connection to trilinear mappings and quadratic forms. Isomorphism classes are determined for the case \( Z = Z(Q) \), i.e. for the extraspecial loops.

© 2006 Elsevier Inc. All rights reserved.

Keywords: Left conjugacy closed loop; Multiplication group; Nucleus

0. Introduction

A loop \( Q \) is said to be extraspecial if \( Q/Z(Q) \) is an elementary abelian \( p \)-group and \( |Z(Q)| = p \). Extraspecial loops thus are defined as a direct generalization of extraspecial groups.

A loop \( Q \) is said to be left conjugacy closed (LCC) if for all \( x, y \in Q \) there exists \( a \in Q \) such that \( L_x L_y L_x^{-1} = L_a \). Here \( L_x \) stands for the left translation \( u \mapsto xu \). Right translations are denoted by \( R_x \), and we set \( T_x = R_x^{-1} L_x \) (in this paper mappings are composed starting from the right). If \( L_x L_y L_x^{-1} = L_a \), then \( a \) has to equal \( T_x(y) \), and

\[
L_x L_y L_x^{-1} = L T_x(y)
\]
can be regarded as an equational description of LCC loops. For other equivalent equations see [19, Theorem 1.1.1] and [8], where one can find further basic information on LCC loops. One of the results of the latter paper is extended in [5].

These loops were introduced by Soikis [22], and have been studied mainly in connection with CC loops (the loops that are both LCC and RCC) and with (left) Bol loops (loops that fulfill $L_x L_y L_z = L_x (L_y L_z)$). By P. Nagy and K. Strambach [19], a Bol loop is an LCC loop if and only if $x^2 \in N_\lambda$ for all $x \in Q$. Here $N_\lambda = N_\lambda(Q)$ means the left nucleus ($a \in Q; \ a(xy) = (ax)y$ for all $x, y \in Q$). The right nucleus is denoted by $N_\rho$.

The main purpose of this paper is to describe all extraspecial LCC loops. In fact, like when one describes all extraspecial groups, we shall be concerned with all finite LCC loop $Q$ such that $Q/Z$ is an abelian $p$-group and $Z$ a central subloop of order $p$. (A subloop is central if it is contained in the center $Z(Q)$. The center $Z(Q)$ consists of all elements $a$ that associate and commute with all elements of $Q$. One can characterize these elements as those that belong to $N_\lambda \cap N_\rho$ and satisfy $ax = xa$ for all $x \in Q$. It is easy to show that all central subloops are normal.)

This paper can be regarded as a continuation of [6], where there was started a systematic investigation of LCC loops of nilpotency class two. Theorem 2.1 reproduces a general construction of [6] that derives a loop $Q = G[b]$ from an abelian group $G$ by setting $x \cdot y = x + y + b(x, y)$, when there exists a subgroup $R \leq G$ such that $b(x + u, y + v) = b(x, y) \in R$ for all $x, y \in G$ and $u, v \in R$. The loop $Q$ is LCC if $b$ is zero preserving and additive on the right (i.e., additive in the second argument). To get extraspecial LCC loops we choose a $p$-element subgroup $Z = R \leq G$ such that $G/Z$ is elementary abelian. That gives only two classes for the choice of $G$, like in the case of extraspecial groups. In case of odd $p$ the group $G$ is thus equal either to an elementary abelian group, or to the product of the latter with a cyclic group of order $p^2$. The main result of the paper states that every extraspecial LCC loop $Q$ is isomorphic to some $G[b]$, and that $G[b_1] \cong G[b_2]$ when $b_1$ and $b_2$ are equivalent under (roughly speaking) scaling, the action of $\text{Aut}(G)$, and the addition of a symmetric biadditive form (cf. Theorem 6.6).

In Proposition 2.4 we show that extraspecial CC loops are in the case of an odd prime $p$ closely connected to trilinear forms. If $V = G/Z$ and $Q = G[b]$ is conjugacy closed, then $b(x, y) = f(x, y) + g(x, y)$, where $f : V \times V \times V \rightarrow Z$ is trilinear and $g : V \times V \rightarrow Z$ bilinear. The obtained general results are transferred to this more specialized setting in Section 7. The case of trivial $g$ corresponds to odd code loops defined by Richardson [21] for the purpose of describing some $p$-local subgroups of the Monster. This connection deserves much more detailed study. The first steps in this direction are done in [10].

If $p = 2$, then extraspecial LCC loops are Bol loops. Such loops were described by G. Nagy [18], and so one could regard this paper as a generalization of Nagy’s paper. However, the methods here are different, since we start from the LCC identity, and not the Bol identity. In Section 8 we show that our results can be applied to classify Bol loops of order eight in a way that seems to be more efficient than the original approach of Burn [3].

Some other papers dealing with LCC Bol loops are [17] and [14]. LCC loops $Q$ which satisfy $|Q : N_\lambda| = 2$ or $|Q : N_\rho| = 2$ are considered in [9]. There are several recent papers on CC loops that are more or less relevant to this research, let us name [7, 15, 16].

The multiplication group $(L_x, R_x; \ x \in Q)$ is denoted by $\text{Mlt} Q$. Left translations generate the left multiplication group $L = L(Q)$. For all $x, y \in Q$ set $L(x, y) = L_x^{-1} L_x L_y$ and put $L_1 = \{ \varphi \in L; \ \varphi(1) = 1 \}$. It is well known that $L_1$ is generated by mappings $L(x, y), x, y \in Q$. Note that elements $N_\rho$ are fixed pointwise by these mappings. We see that $N_\rho$ coincides with the set of points that are fixed by $L_1$. Loops with the property that each $\varphi \in L_1$ is an automorphism of $Q$
are called $A_L$-loops. It is not difficult to show (cf. [8,19]) that every LCC loop is an $A_L$-loop, and this fact will be used several times in the paper.

For a subloop $S$ of a loop $Q$ one defines the relative multiplication group $\mathcal{M}(S)$ as $\langle L_s, R_s; s \in Q \rangle$. If $S$ is central, then $L_s = R_s$ for all $s \in S$ and $\mathcal{M}(S) = \{L_s; s \in S\} \cong S$.

The paper is nearly self-contained. It relies on a number of statements coming from [6], but all of them have an easy proof. This is also true for the general statements from loop theory that we shall use.

Section 1 contains several statements about LCC loops which are stated in a level of generality that should allow further applications in future. In Proposition 1.2 we show that each LCC loop of nilpotency class two can be naturally associated with a 2-cocycle (in the sense of group extensions). In Theorem 1.9 we then show that this 2-cocycle is a 2-coboundary in a large class of $p$-loops which encompasses the loops of the main interest in this paper, i.e. the extraspecial LCC loops.

In Section 2 we describe, as already mentioned above, a construction of LCC loops, and state some of its properties. In Section 3 we recall several well-known facts about groups and bilinear forms. Section 4 contains the crucial calculation of Theorem 4.6 that shows how mappings $b$ arise from the loop structure. In Section 5 there appear several conditions under which $G[b_1] \cong G[b_2]$, and then we come to the synthesis of Section 6.

1. LCC loops abelian over a central subloop

We start by restating several propositions from [6]. Some of them come with proof, since here they appear in a slightly more general form, when a central subloop $Z$ is considered in place of the center $Z(Q)$. Note that if $Q/Z$ is an abelian group, then $Q$ is of nilpotency class at most two. Recall also that the center of $\text{Mlt } Q$ equals $\mathcal{M}(Z(Q))$ [1].

**Proposition 1.1.** Let $Q$ be a loop of nilpotency class two. Then $Q$ is left conjugacy closed if and only if $L / Z(\text{Mlt } Q)$ is abelian. This is true if and only if $L(x,y) = L(y,x)$ for all $x, y \in Q$.

**Proof.** See [6, Corollaries 3.2 and 3.4]. □

**Proposition 1.2.** Let $Q$ be an LCC loop and let $Z$ be a central subloop of $Q$ such that $Q/Z$ is an abelian group. Then the operation on $Q/Z \times L_1$ defined by

$$(xZ, \varphi) \cdot (yZ, \psi) = (xyZ, L(x, y)\varphi\psi)$$

is a well-defined group operation. This group is a homomorphic image of $\mathcal{L}$ under $L_x \varphi \mapsto (xZ, \varphi)$. It is abelian and the kernel of the homomorphism is equal to $\mathcal{M}(Z)$. Furthermore, when $L(-,-)$ is regarded as a mapping $Q/Z \times Q/Z \rightarrow L_1$, then it yields a 2-cocycle (i.e., a factor system).

**Proof.** Proceed as in the beginning of [6, Section 3]. Since $L_x \varphi \mapsto (x, \varphi)$ is an isomorphism of $\mathcal{L}$ onto a group defined on $Q \times L_1$ by

$$(x, \varphi) \cdot (y, \psi) = (xy, L(x, \varphi(y))\varphi\psi),$$
we can get the group of the proposition by factorization, provided \( L(x, \varphi(y)) = L(x', y') \) whenever \( x \equiv x' \) and \( y \equiv y' \mod Z \), for all \( x, x', y, y' \in Q \) and \( \varphi \in \mathcal{L}_1 \). Now, \( L(x, y) = L(x', y') \) follows from the centrality of \( Z \) immediately, and \( \varphi(y) \equiv y \mod Z \) since \( Q/Z \) is a group.

Since we assume that \( Q/Z \) is abelian and that \( Q \) is an LCC loop, the group obtained by factorization has to be abelian as well, by Proposition 1.1. Nothing else needs to be proved. \( \Box \)

The next proposition reiterates, amongst others, the standard definition of the \textit{commutator} of loop elements.

**Proposition 1.3.** Let \( Q \) be an LCC loop with a central subloop \( Z \) such that \( Q/Z \) is an abelian group. Then

\[
[x, y] = (yx)(xy) \in Z \quad \text{and} \quad [L_x, L_y] = L_{[x,y]} \in \mathcal{M}(Z)
\]

for all \( x, y \in Q \).

**Proof.** Use [6, Lemmas 4.1 and 4.2]. \( \Box \)

**Proposition 1.4.** Let \( Q \) be an LCC loop with a central subloop \( Z \) such that \( Q/Z \) is abelian. Associate with each \( \varphi \in \mathcal{L}_1 \) a mapping \( \xi_\varphi : Q/Z \to Z \) by \( \xi_\varphi(xZ) \cdot x = \varphi(x) \). Then \( \xi_\varphi \) is defined correctly and \( \xi_\varphi \in \text{Hom}(Q/Z, Z) \). The mapping \( \varphi \mapsto \xi_\varphi \) is a homomorphic embedding \( \mathcal{L}_1 \to \text{Hom}(Q/Z, Z) \).

**Proof.** If \( z \in Z \), then \( \varphi(xz) = \varphi(x)z \) for all \( \varphi \in \mathcal{L}_1 \) and \( x \in Q \). Hence \( \xi_\varphi \) is well defined. If \( \varphi(x) = xa \) and \( \varphi(y) = yb \), then \( \varphi(xy) = (xa)(yb) \), since each \( \varphi \in \mathcal{L}_1 \) is an automorphism of \( Q \). Thus \( \xi_\varphi(xyZ) = ab = \xi_\varphi(xZ)\xi_\varphi(yZ) \), and \( \xi_\varphi \in \text{Hom}(Q/Z, Z) \). If \( \varphi, \psi \in \mathcal{L}_1, x \in Q, \varphi(x) = xa \) and \( \psi(x) = xb \), then \( \varphi\psi(x) = \varphi(xb) = \varphi(x)\varphi(b) \) equals \( xab \), as \( \varphi \in \mathcal{L}_1 \) fixes all elements of \( Z \leq N_\rho \). Hence \( \xi_{\varphi\psi} = \xi_\varphi\xi_\psi \), and the mapping \( \varphi \mapsto \xi_\varphi \) is an embedding of \( \mathcal{L}_1 \), indeed. \( \Box \)

If \( A \) and \( Z \) are abelian groups, and \( Z \) is of exponent \( m \), then \( \text{Hom}(A, Z) \) is of exponent \( m \) as well. Hence Proposition 1.4 yields

**Corollary 1.5.** Let \( Q \) be an LCC loop, with a central subloop \( Z \) such that \( Q/Z \) is abelian. If \( Z \) is of exponent \( m \), then \( \mathcal{L}_1 \) is of exponent \( m \) as well.

We shall now need another basic fact concerning LCC loops. Put \( M_\rho = \{a \in Q; \; R_a \in Z(\mathcal{L})\} \). Then

\[
Z(\mathcal{L}) = \{R_a; \; a \in Q\} \cap \mathcal{L} = \{R_a; \; a \in M_\rho\} \quad \text{and} \quad M_\rho \leq Z(N_\rho),
\]

in every LCC loop \( Q \), by [8, Theorem 2.8] and [7, Proposition 1.6].

Note that the subloop \( M_\rho \) does not need to be normal in general. However, if \( Q \) is nilpotent of class two, then the normality of \( M_\rho \) follows from \( Z(Q) \leq M_\rho \).

**Proposition 1.6.** Let \( Q \) be an LCC loop with a central subloop \( Z \) such that \( Q/Z \) is an abelian group. If \( Z \) is of exponent \( m \), then \( \mathcal{L}/Z(\mathcal{L}) \) is of exponent \( m \) as well.
Proof. Consider \( \psi \in \mathcal{L} \) and \( y \in Q \). Then \([\psi , L_y] \) belongs to \( \mathcal{M}(Z) \cong Z \), by Proposition 1.3. From that \([\psi^m , L_y] = [\psi , L_y]^m = \text{id}_Q \), which means \( \psi^m \in Z(\mathcal{L}) \). □

Corollary 1.7. Let \( Q \) be an LCC loop with a central subloop \( Z \) such that \( Q/Z \) is an abelian group. If \( Z \) is of exponent \( m \), then \( Q/M_\rho \) is of exponent \( m \) as well.

Proof. The action of \( \mathcal{L} \) on \( Q/M_\rho \) yields a group isomorphic to \( Q/M_\rho \). This group is a homomorphic image of \( \mathcal{L}/Z(\mathcal{L}) \) as all elements of \( Z(\mathcal{L}) \) act within the cosets of the normal subloop \( M_\rho \). □

Proposition 1.8. Let \( Q \) be an LCC loop with a central subloop \( Z \) such that \( Q/Z \) is of exponent \( m \). Suppose that both \( Z \) and \( Q/Z \) are of exponent \( m \). Then \( L/M_\rho \) is of exponent \( m \) as well, and \( L^m_x = L_{L_x^{-1}}(x) \in \mathcal{M}(Z) \) for all \( x \in Q \).

Proof. We have \( L^m_x = R_a \) for some \( a \in M_\rho \), by Proposition 1.6. Now, \( a = L_x^{-1}(x) = L_x^m(1) \in Z \), as \( Q/Z \) is of exponent \( m \). Therefore \( R_a = L_a \in \mathcal{M}(Z) \).

Now, \( \mathcal{L}/\mathcal{M}(Z) \) is abelian, by Proposition 1.2. The elements \( L_x \mathcal{M}(Z) \), \( x \in Q \), generate the group and are of exponent \( m \). The generated group is thus of exponent \( m \) as well. □

Theorem 1.9. Let \( Q \) be an LCC loop with a central subloop \( Z \) such that \( Q/Z \) is an abelian group. Suppose that both \( Z \) and \( Q/Z \) are of exponent \( p \), \( p \) a prime. Assume \( |Z| = p^h \) and \( |Q/Z| = p^k \), for some positive integers \( h \) and \( k \). Then

(i) \( \mathcal{L}_1 \) is an elementary abelian \( p \)-group, \( |\mathcal{L}_1| \leq p^{hk} \);
(ii) \( \mathcal{L}/\mathcal{M}(Z) \) is an elementary abelian \( p \)-group of order \( |Q/Z||\mathcal{L}_1| \leq p^{(h+1)k} \);
(iii) there exists \( \gamma : Q/Z \rightarrow \mathcal{L}_1 \) such that \( \gamma(Z) = \text{id}_Q \) and for all \( x, y \in Q \)

\[ L(x, y) = \gamma(xyZ)\gamma(xZ)^{-1}\gamma(yZ)^{-1}. \]

Proof. Point (i) follows from Proposition 1.4 and point (ii) from Propositions 1.2 and 1.8. The mapping \( L(\cdot, \cdot) \) is a 2-cocycle that yields an abelian extension of \( \mathcal{L}_1 \) by \( Q/Z \), by Proposition 1.2. This extension is split, by point (ii), and hence the 2-cocycle is a 2-coboundary. This implies the existence of \( \gamma \). □

We shall observe in Lemma 4.4 that the above theorem gives the possibility to reduce computations in \( Q \) to computations in \( \mathcal{L} \). We shall not need Theorem 1.9 in its full generality in this paper. Instead we shall work with the following immediate consequence.

Corollary 1.10. Let \( Q \) be an LCC loops with a \( p \)-element central subloop \( Z \) such that \( Q/Z \) is an elementary abelian \( p \)-group, \( p \) a prime. Then \( \mathcal{L}_1 \) and \( \mathcal{L}/\mathcal{M}(Z) \) are elementary abelian \( p \)-groups, and \( \mathcal{M}(Z) = \{ L_z : z \in Z \} \) is a \( p \)-element subgroup of \( \mathcal{L} \).

2. General construction

Let \( G \) and \( R \) be abelian groups, and let \( b : G \times G \rightarrow R \) be a mapping. Put

\[ \text{Rad}(b) = \{ u \in G : b(x + u, y) = b(x, y) = b(x, u + y) \text{ for all } x, y \in G \}. \]
It is clear that \( \text{Rad}(b) \) is a subgroup of \( G \).

Call \( b \) zero preserving if \( b(x, 0) = b(0, x) = 0 \) for all \( x \in G \). Call \( b : G \times G \to R \) additive on the right if \( b(x, y + z) = b(x, y) + b(x, z) \) for all \( x, y, z \in G \). Similarly define mappings that are additive on the left. Call \( b : G \times G \to R \) biadditive if it is additive both on the left and on the right. Triadditive mappings will be used as well.

**Theorem 2.1.** Let \( G \) be an abelian group with a subgroup \( R \). Let \( b : G \times G \to R \) be a zero preserving mapping with \( \text{Rad}(b) \supseteq R \) that is additive on the right. Then 

\[
x \cdot y = x + y + b(x, y)
\]

defines on \( G \) a left conjugacy closed loop. This loop is a group if and only if \( b \) is biadditive, and it is a CC loop if and only if 

\[
b(x + y, z) - b(x, z) - b(y, z) = b(x + z, y) - b(x, y) - b(z, y)
\]

for all \( x, y, z \in Q \).

**Proof.** This is a reproduction of [6, Theorem 3.5 and Lemma 5.4] (however, the CC identity is presented here in a different way). The claims are easy to verify, anyhow.

**Corollary 2.2.** Put \( f(x, y, z) = b(x + y, z) - b(x, z) - b(y, z) \), for all \( x, y, z \in G \). Then \( G(\cdot) \) is a CC-loop if and only if \( f : G \times G \times G \to R \) is a triadditive symmetric mapping.

**Proof.** By the definition of \( f \), \( f(x, y, z) = f(y, x, z) \) for all \( x, y, z \in G \). The CC condition of Theorem 2.1 yields \( f(x, y, z) = f(x, z, y) \), and \( f(x, y, z_1 + z_2) = f(x, y, z_1) + f(x, y, z_2) \) is a consequence of the fact that \( b \) is additive on the right. The rest is clear.

**Lemma 2.3.** Let \( F \) be a field of order \( p \), \( p \) an odd prime, and let \( V \) be a vector space over \( F \). Suppose that \( q : V \to F \) has the property that \( q(x + y) = q(x) - q(y) \) is a bilinear form. Then there exist a quadratic form \( q_0 : V \to F \) and a linear form \( q_1 : V \to F \) such that \( q = q_0 + q_1 \), and one can set \( q_0(x) = q(2x)/2 - q(x) \).

**Proof.** Define \( f(x, y) \) as \( \frac{1}{2}(q(x + y) - q(x) - q(y)) \). It suffices to show that \( q(x) - f(x, x) \) is a linear form, i.e. that

\[
q(x + y) - f(x + y, x + y) = q(x) - f(x, x) + q(y) - f(y, y)
\]

for all \( x, y \in Q \). However, this follows from \( 2f(x, y) = q(x + y) - q(x) - q(y) \).

**Proposition 2.4.** Let \( G \) be an abelian group with a \( p \)-element subgroup \( F \), \( p \) an odd prime, such that \( V = G/F \) is an elementary abelian \( p \)-group. Let \( b : V \to F \) be a zero preserving mapping that is additive on the right, and suppose that the loop operation \( x \cdot y = x + y + b(xF, yF) \) yields a CC loop. Then there exist a symmetric trilinear mapping \( f : V \times V \times V \to F \) and bilinear mapping \( g : V \times V \to F \) such that

\[
b(u, v) = f(u, u, v) + g(u, v)
\]

for all \( u, v \in V \).
On the other hand, if \( f : V \times V \times V \to F \) is symmetric trilinear, and \( g : V \times V \to F \) is bilinear, then
\[
x \cdot y = x + y + f(xF,xF,yF) + g(xF,yF)
\]
defines a CC loop on \( G \).

**Proof.** Put \( f(u,v,w) = \frac{1}{2}(b(u+v,w) - b(u,w) - b(v,w)) \). By Corollary 2.2, \( f : V^3 \to F \) is trilinear and symmetric. Set \( g(u,w) = b(u,w) - f(u,u,w) \), for all \( u, w \in V \). The mapping \( g \) is additive on the left by Lemma 2.3, and it is additive on the right because \( b \) has the same property. Hence \( g \) is bilinear. The converse statement can be easily verified by means of Theorem 2.1.

In Section 4 we shall see that all extraspecial LCC loops are of the kind described in Theorem 2.1. Corollary 2.2 and Proposition 2.4 will then help us to characterize isomorphism classes of extraspecial CC loops for the case when the prime \( p \) is odd.

The case \( p = 2 \) clearly does not allow a description of CC loops similar to that of Proposition 2.4. The mapping \( f, f(x, y, z) = b(x + y, z) + b(y, z) + b(x, z) \), is symmetric and trilinear by Corollary 2.2. If \( p = 2 \), then we see that \( f \) has to be an alternating trilinear form. Mapping \( b : V \times V \to F \) that is additive on the right and yields \( f \) trilinear might be called a quadrilinear form. Aschbacher considers in [2, Section 11] triples \((T, b, f)\), where \( T : V \to F, F = \{0, 1\} \), satisfies \( T(x + y) = T(x) + T(y) + b(x, y) + b(y, x) \). Such triples are called in [2] a 3-form. They appear in the context of code loops, i.e. Moufang loops \( Q \) such that \( Q/Z \) is an elementary abelian 2-group, and \( Z \) is a 2-element normal subloop (a 2-element normal subloop is necessarily central). Since a CC loop \( Q \) is Moufang if and only if \( Q/N_\lambda \) is an elementary abelian 2-group, by [11], we see that extraspecial CC 2-loops are code loops. Code loops are studied in [2] as a tool to develop the Monster group (the Parker loop is a special case of a code loop). In [4] they are studied from the point of view of Moufang loops. The structure of a code loop \( Q \) is determined by the squaring mapping \( x \to x^2 \) and the commutator and the associator (which happens to be equal to the mapping \( f \)) can be obtained from the squaring mapping by the process of polarization [23]. We shall not repeat here these results and our treatment of code loops will be thus restricted.

### 3. Vector spaces and groups

This section contains several auxiliary statements and recalls some well-known facts.

**Lemma 3.1.** Let \( V \) be a vector space with a hyperplane \( \Omega \). Suppose that \( \Omega \) contains a subspace \( U \), and let \( B \) be a basis of \( U \). Furthermore, let \( T \subseteq V \) be a transversal to \( U \) (i.e., \( T + U = V \) and \( T \cap U = 0 \)). Finally, let \( W \subseteq V \) be a subspace such that \( U \subseteq W \) and \( W \setminus \Omega \neq \emptyset \). Then there exists \( S \subseteq T \) such that

1. \( S \cup B \) is a basis of \( V \), and
2. there exists exactly one \( w \in S \) with \( w \notin \Omega \), and this \( w \) belongs to \( W \).

**Proof.** Start from some \( w_0 \in W \setminus \Omega \). Then \( w_0 = w + u \) for \( u \in U \) and \( w \in T \), and \( U \subseteq \Omega \cap W \) yields \( w \in W \setminus \Omega \). Choose \( S_0 \subseteq \Omega \) so that \( B \cup S_0 \) is a basis of \( \Omega \). Then each \( s_0 \in S_0 \) can be
(uniquely) expressed as \( s + u \), where \( u \in U \) and \( s \in T \). Denote by \( S_1 \) the set of all \( s \) we have obtained in this way. \( S_1 \cup B \) is a basis of \( \Omega \) since \( U \subseteq \Omega \). We can hence set \( S = S_1 \cup \{ w \} \). \( \square \)

Let \( g \) be an alternating form on a finite-dimensional vector space \( V \). Then \( \text{Rad}(g) \) is a subspace of \( V \) and \( g \) induces a nondegenerate alternating form on \( V/\text{Rad}(g) \). (This form is equivalent to the restriction of \( g \) to \( W \times W \) if \( W \subseteq V \) is a complement to \( \text{Rad}(g) \).)

A subspace \( U \subseteq W \) is called (totally) isotropic if \( g(u_1, u_2) = 0 \) for all \( u_1, u_2 \in U \). The following fact is well known (one can prove it directly or as a consequence of Witt’s lemma):

**Lemma 3.2.** Let \( U \) be a maximal isotropic subspace of \((V, g)\), where \( g \) is an alternating form. Then

\[
2(\dim U) = \dim V + \dim \text{Rad}(g).
\]

For every subspace \( W \subseteq V \) one defines \( W^\bot \) as \( \{ x \in V; \ g(x, u) = 0 \text{ for all } u \in V \} \). Clearly \((W + \text{Rad}(g))^\bot = W^\bot \supseteq \text{Rad}(g)\). If \( W \supseteq \text{Rad}(g) \), then \( \dim W + \dim W^\bot = \dim V + \dim \text{Rad}(g) \). Hence from \( \text{Rad}(g) \subseteq W_1 \subseteq W_2 \) one gets \( \text{Rad}(g) \subseteq W_2^\bot \subseteq W_1^\bot \). As a consequence we obtain

**Lemma 3.3.** Let \( W \subseteq U \subseteq V \) be vector spaces, and let \( g \) be an alternating form on \( V \). If there exists \( u \in U \setminus W \), \( u \notin \text{Rad}(g) + W \), then there exists \( v \in V \) such that \( g(u, v) \neq 0 \) and \( g(w, v) = 0 \) for all \( w \in W \).

Let us recall how extraspecial groups are connected to alternating forms:

**Proposition 3.4.** Let \( G \) be a finite \( p \)-group with a central \( p \)-element subgroup \( C \) such that \( G/C \) is elementary abelian. Then

\[
g : G/C \times G/C \to C, \quad g(xC, yC) = [x, y]
\]

is an alternating bilinear form. The radical of \( g \) is equal to \( Z(G)/C \). A subgroup \( A \leq G \) is a maximal abelian subgroup if and only if \( C \leq A \) and \( A/C \) is a maximal isotropic subspace of \((G/C, g)\).

The mapping \( \sigma : G/C \to C, \sigma(xC) = xp \) is a linear form when \( p \) is odd and a quadratic form associated with \( g \) when \( p = 2 \).

The proof is direct and well known (cf. Section 8 of [2]).

**Lemma 3.5.** Let \( G \) be a finite \( p \)-group with a central \( p \)-element subgroup \( C \) such that \( G/C \) is elementary abelian. Let \( x_1, \ldots, x_k \in G \) be such that \( x_1C, \ldots, x_kC \) is a basis of \( G/C \). Then every element of \( G \) can be expressed in a unique way as \( x_1^{a_1} \cdots x_k^{a_k} c \), where \( c \in C \) and \( a_i \in \{0, 1, \ldots, p - 1\}, 1 \leq i \leq k \). Furthermore, if \( x_1^{a_1} \cdots x_k^{a_k} c \) and \( x_1^{b_1} \cdots x_k^{b_k} d \) are two such expressions, then

\[
x_1^{a_1} \cdots x_k^{a_k} c \cdot x_1^{b_1} \cdots x_k^{b_k} d = x_1^{a_1 + b_1} \cdots x_k^{a_k + b_k} c d \prod_{i > j} [x_i, x_j]^{a_i b_j}.
\]
Proof. For $x$, $y \in G$ one has $x^a y^b = y^b x^a[x^a, y^b] = y^b x^a[x, y]^{ab}$ for all integers $a$ and $b$, since $[x, y]$ centralizes both $x$ and $y$. The formula of the lemma is obtained by a repeated application of the latter identity. \qed

We conclude this section by a trivial observation that has important consequences.

Lemma 3.6. Let $G$ be a cyclic group of order 4. Let $x$ be its generator, and let $z = x^2$. Denote by $\oplus$ the addition modulo 2. If $a, b \in \{0, 1\}$, then $x^{a+b} = x^{a \oplus b} z^{ab}$.

4. Right nucleus and the additivity on the right

We shall first start by an easy general lemma:

Lemma 4.1. Let $Q$ be an LCC loop with an element $a$. Then

$$a \in M_\rho \iff L_a \in Z(\mathcal{L}) \mathcal{L}_1.$$ 

Proof. We have $Z(\mathcal{L}) = \{R_x; x \in M_\rho\}$, as mentioned in the paragraph ensuing Corollary 1.1. If $a \in M_\rho$, then $R_a \in \mathcal{L}$, $R_a^{-1} L_a = T_a \in \mathcal{L}_1$, and $L_a = R_a T_a \in Z(\mathcal{L}) \mathcal{L}_1$. If $L_a \in Z(\mathcal{L}) \mathcal{L}_1$, then there exist $b \in M_\rho$ and $\phi \in \mathcal{L}_1$ such that $L_a = R_b \phi$. That means $a = b$, and so $a \in M_\rho$. \qed

Let $Q$ be a finite LCC loop $Q$ that possesses a $p$-element central subloop $Z$ such that $Q/Z$ is an elementary abelian $p$-group, $p$ a prime. Then $\mathcal{L}_1$ and $\mathcal{L}/\mathcal{M}(Z)$ are elementary abelian $p$-groups, and $\mathcal{M}(Z) = \{L_z; z \in Z\}$ is a $p$-element central subgroup of $\mathcal{L}$, by Corollary 1.10.

We shall first describe how the right nucleus $N_\rho$ influences the structure of the left multiplication group $\mathcal{L}$. This is a step beyond the main line of the paper, and one can omit both following statements and proceed directly to Lemma 4.4. Right nuclei are of special interest in LCC loops (e.g. no finite LCC loop $Q$ with $N_\rho = 1$ seems to be known), and this is one of reasons why Proposition 4.3 is included.

Lemma 4.2. Let $A$ be a maximal abelian subgroup of $N_\rho$, $|A| = p^{t+1}$. Then $A \supseteq Z$. Choose $a_1, \ldots, a_t \in A$ such that $a_i, 1 \leq i \leq t$, generate, together with $Z$, the subgroup $A$. Denote by $\mathcal{A}$ the subgroup of $\mathcal{L}$ generated by all $L_{a_i}, 1 \leq i \leq t$, and by all $L_z, z \in Z$. Then $\mathcal{A}$ is an abelian group of order $p^{t+1}$, and $\mathcal{A} \mathcal{L}_1 \cong \mathcal{A} \times \mathcal{L}_1$ is an abelian group that contains all $L_a, a \in A$. Furthermore, $\mathcal{A} \mathcal{L}_1$ is a maximal abelian subgroup of $\mathcal{L}$.

Proof. From $Z(\mathcal{Q}) \leq N_\rho$, one gets $Z \leq Z(N_\rho)$, and hence $A$ has to contain $Z$. By Proposition 1.3, $[L_{a_i}, L_{a_j}] = L_{[a_i, a_j]} = \text{id}_\mathcal{Q}$, whenever $1 \leq i \leq j \leq t$. Thus, $A$ is abelian and $A \supseteq \mathcal{M}(Z)$. Since $\mathcal{M}(Z)$ is of order $p$ and $A/\mathcal{M}(Z)$ is elementary abelian with $t$ generators, there must be $|A| \leq p^{t+1}$. To get the equality, consider the action of $A$ on $N_\rho$. It is generated by the restriction of $L_{a_i}, 1 \leq i \leq t$, and of $L_z, z \in Z$, to $N_\rho$. The action of $A$ on $N_\rho$ hence coincides with the action of $A$ on $N_\rho$, by left translations. Thus $p^{t+1} = |A| \leq |A|$, and we see that $A$ acts on $N_\rho$, faithfully.

If $\phi \in \mathcal{L}_1$, then $\phi L_x \phi^{-1} = L_{\phi(x)}$, for every $x \in \mathcal{Q}$, since $\phi \in \text{Aut} \mathcal{Q}$. Each $\phi \in \mathcal{L}_1$ fixes all $x \in N_\rho$. Hence $\phi$ commutes with every $L_{a_i}, 1 \leq i \leq t$, and since $\mathcal{L}_1$ is abelian, by Corollary 1.10, we see that $\mathcal{A} \mathcal{L}_1$ is abelian as well.

$A$ acts faithfully on $N_\rho$, but $\mathcal{L}_1$ fixes each element of $N_\rho$. This gives $\mathcal{A} \mathcal{L}_1 \cong A \times \mathcal{L}_1$. 

\[
779\]
For every $a \in A$ one can find $\alpha \in A$ that coincides with $L_a$ on $N_\rho$. Then $\alpha^{-1}L_a \in \mathcal{L}_1$, and so $L_a \in A\mathcal{L}_1$ for each $a \in A$.

It remains to prove that $A\mathcal{L}_1$ is a maximal abelian subgroup of $\mathcal{L}$. Suppose that some $L_x \varphi, \varphi \in \mathcal{L}_1$, centralizes $A\mathcal{L}_1$. Since $\psi L_x \varphi \psi^{-1} = L_{\psi(x)} \varphi$ for every $\psi \in \mathcal{L}_1$, we see that there must be $\psi(x) = x$ for every $\psi \in \mathcal{L}_1$. That means $x \in N_\rho$. We have $L_a \in A\mathcal{L}_1$ for each $a \in A$, by the preceding part of the proof. Because $L_a L_x \varphi L_a^{-1} = L_a L_x L_a^{-1} \varphi = L_{axa^{-1}} \varphi$ is assumed to equal $L_x \varphi$, we see that $x \in N_\rho$ centralizes each $a \in A$. However, $A$ was chosen as a maximal subgroup of $N_\rho$. Thus $x \in A$. □

**Proposition 4.3.** Let $Q$ be a finite LCC loop with a central subloop $Z$. Suppose that $|Z| = p$ and that $Q/Z$ is an elementary abelian $p$-group, $p$ a prime. Then $\mathcal{L}/\mathcal{M}(Z)$ is an elementary abelian $p$-group, $|\mathcal{L}| = |Q|^2/|N_\rho|$, $Z(\mathcal{L}) = \langle R_a; a \in Z(N_\rho) \rangle$ and $|Q| = |N_\rho||\mathcal{L}_1|$.

**Proof.** Since $|\mathcal{L}| = |Q||\mathcal{L}_1|$ in every loop it suffices to prove $|Q| = |N_\rho||\mathcal{L}_1|$ and $Z(\mathcal{L}) = \langle R_a; a \in Z(N_\rho) \rangle$, by Corollary 1.10. Since $Z(\mathcal{L}) = \langle R_a; a \in M_\rho \rangle$, we have to show $M_\rho = Z(N_\rho)$. Since $M_\rho \leq Z(N_\rho)$ is always true, we need to prove $a \in Z(N_\rho) \Rightarrow a \in M_\rho$. The latter is equivalent to $L_a \in Z(\mathcal{L})\mathcal{L}_1$, by Lemma 4.1.

Assume $L_a \notin Z(\mathcal{L})\mathcal{L}_1$. Our goal is to show $a \notin Z(N_\rho)$. The commutator induces on $\mathcal{L}/\mathcal{M}(Z)$ an alternating form, by Corollary 1.10 and Proposition 3.4. The radical of this form is equal to $Z(\mathcal{L})/\mathcal{M}(Z)$. Let us use Lemma 3.3 in such a way that $W$ corresponds to $\mathcal{L}_1$ (more exactly to $\mathcal{L}_1\mathcal{M}(Z)/\mathcal{M}(Z)$) and $U$ corresponds to $(L_a)\mathcal{L}_1$. By the lemma there exists $L_b \psi, b \in Q$ and $\psi \in \mathcal{L}_1$, such that $[L_b \psi, \varphi] = \text{id}_Q$ for all $\varphi \in \mathcal{L}_1$, and $[L_b \psi, L_a] \neq \text{id}_Q$. The former condition gives $b \in N_\rho$. If $a \notin N_\rho$, then $a \notin Z(N_\rho)$. If $a \in N_\rho$, then $[L_b \psi, L_a] = [L_b, L_a] = [b, a] \neq \text{id}_Q$, by Proposition 1.3. This means $[b, a] \neq 1$, and so $a \notin Z(N_\rho)$ as well. We have proved $a \notin M_\rho \Rightarrow a \notin Z(N_\rho)$, which is what we needed.

The right nucleus $N_\rho$ is a group, and the order of a maximal abelian subgroup $A \leq N_\rho$ is determined by the formula $|A|^2 = |N_\rho||Z(N_\rho)|$. (This follows from Lemma 3.2 and Proposition 3.4.)

By Lemma 4.2, the order of a maximal abelian subgroup of $\mathcal{L}$ is equal to $|A||\mathcal{L}_1|$. From Corollary 1.10 and Proposition 3.4 we see that another application of Lemma 3.2 yields

$$|A|^2|\mathcal{L}_1|^2 = |\mathcal{L}|Z(\mathcal{L}) = |\mathcal{L}|Z(N_\rho) = |\mathcal{L}||A|^2/|N_\rho|,$$

where the last two equalities are based upon the previous parts of the proof. We have shown $|Q||\mathcal{L}_1| = |\mathcal{L}| = |N_\rho||\mathcal{L}_1|^2$, and $|Q| = |N_\rho||\mathcal{L}_1|$ follows. □

It seems natural to continue by defining $A$ as in Lemma 4.2 and by finding a symplectic basis that would contain a basis for $A$ and a basis for $\mathcal{L}_1$. One can then express elements of $\mathcal{L}$ by means of such a basis and use it to calculate the products of the loop multiplication. However, such an approach gives long formulas which do not seem to reveal much beyond their complexity. Hence we shall take another route. First we shall prove that the binary operation of $Q$ can be expressed by the general formula of Theorem 2.1, and then we shall be deriving consequences of that fact. Lemma 4.2 and Proposition 4.3 will not be referred to in the subsequent text.

The next lemma is auxiliary. It can be useful in other contexts as well since it is concerned with a certain general property of loops.
Lemma 4.4. Let $Q$ be a loop with a mapping $\gamma : Q \to \mathcal{L}_1$ such that
\[ L(x, y) = \gamma(xy)\gamma(x)^{-1}\gamma(y)^{-1} \]
for all $x, y \in Q$ and $\gamma(z) = 1$ for each $z \in Z \leq Z(Q)$. If $z \in Z \leq Z(Q)$ and $x_1, \ldots, x_k \in Q$, then
\[ L_{x_1}(x_2 \ldots (x_k z)) = L_{x_1}L_{x_2} \ldots L_{x_k}L_z\gamma(x_k) \ldots \gamma(x_1)(\gamma(x_1(x_2 \ldots x_k)))^{-1}. \]

Proof. We have $L(x, z) = \gamma(xz)\gamma(x)^{-1} = \text{id}_Q$ for each $x \in Q$, and so we see that $\gamma$ depends only on the coset modulo $Z$. For $k = 1$ the lemma clearly holds. Assume $k \geq 2$ and put $y = x_2 \ldots (x_k z)$. Then
\[ L_{x_1,y} = L_{x_1}L_yL_{x_1,y}^{-1} = L_{x_1}L_{x_2} \ldots L_{x_k}L_z\gamma(x_k) \ldots \gamma(x_2)\gamma(y)^{-1}\gamma(y)\gamma(x_1)y, \]
which is equal to the required $L_{x_1}L_{x_2} \ldots L_{x_k}L_z\gamma(x_k) \ldots \gamma(x_1)(\gamma(x_1(x_2 \ldots x_k)))^{-1}$. \Box

Lemma 4.5. Let $Q$ be a finite LCC loop with a $p$-element central subloop $Z$ such that $Q/Z$ is an elementary abelian $p$-group, $p$ a prime. Then there exist $e_1, \ldots, e_k \in Q$ such that $|Q/Z| = p^k$, and each $x \in Q$ can be expressed in a unique way as
\[ L_{e_1}^{a_1} \ldots L_{e_k}^{a_k}(z), \quad \text{where } z \in Z \text{ and } a_1, \ldots, a_k \in \{0, 1, \ldots, p - 1\}. \]

If $p$ is odd, then the elements $e_1, \ldots, e_k$ can be chosen in such a way that translations $L_{e_1^2}, \ldots, L_{e_k}$ are of order $p$, and the order of $L_{e_1}$ is either $p$ or $p^2$. In the former case every $L_x$, $x \in Q$, is of order $p$. In the latter case one can choose $e_1 \in Z(Q)$ when $Z(Q)$ is not of exponent $p$, and $e_1 \in N_p$ when $N_p$ is not of exponent $p$.

Proof. If $e_1, \ldots, e_k \in Q$ are such that $e_1Z, \ldots, e_kZ$ is a basis of $Q/Z$, then every coset modulo $Z$ has exactly one representative of the form $L_{e_1}^{a_1} \ldots L_{e_k}^{a_k}(1)$, where $a_1, \ldots, a_k \in \{0, 1, \ldots, p - 1\}$. The reason is that the coset of such an element is equal to $(e_1Z)^{a_1} \ldots (e_kZ)^{a_k}$. This makes the uniqueness clear. Note also that any $L_e^p$ is equal to some $L_z$, $z \in Z$, for every $e \in Q$, by Corollary 1.10.

Let $p$ be odd. We know that $L/\mathcal{M}(Z)$ is elementary abelian. The mapping $\psi \mapsto \psi^P$ is a homomorphism $\mathcal{L} \to \mathcal{M}(Z)$, by Proposition 3.4. Denote by $\Omega$ its kernel and assume $\Omega \neq \mathcal{L}$. Then $\Omega/\mathcal{M}(Z)$ is a hyperplane of $\mathcal{L}/\mathcal{M}(Z)$ and the cosets $L_x\mathcal{M}(Z), x \in Q$, form a transversal to $L_1\mathcal{M}(Z)/\mathcal{M}(Z)$. Note that $\Omega$ contains $L_1$, by Corollary 1.10. To choose $e_1, \ldots, e_k$ in a way that is required by the lemma, use Lemma 3.1 so that $W$ is induced by $L_1$ and by an additional left translation $L_a$, where $a \in Z(Q)$ or $a \in N_p \setminus Z(Q)$ or $a \in Q \setminus N_p$. \Box

Computations done in the proof of the following theorem form the decisive step on our way towards the proof of Theorem 6.6.

Theorem 4.6. Let $Q$ be a finite LCC loop with a $p$-element central subloop $Z$ such that $Q/Z$ is an elementary abelian $p$-group, $p$ a prime. Then there exists a finite abelian $p$-group $G(+)$, $|G| = |Q|$, with a $p$-element subgroup $R$ such that $G/R$ is elementary abelian and $Q \cong G(-)$, where $x \cdot y = x + y + b(x, y)$ for some $b : G \times G \to R$, $\text{Rad}(b) \supseteq R$, $b$ zero preserving and additive on the right. If $|p| = 2$, then $G$ can be chosen to be elementary abelian.
Proof. Fix \( e_1, \ldots, e_k \in Q \) that fulfill conditions of Lemma 4.5. Let us have \( x = L_{e_1}^{a_1} \cdots L_{e_k}^{a_k}(c) \) and \( y = L_{e_1}^{b_1} \cdots L_{e_k}^{b_k}(d) \), where \( c, d \in Z(Q) \) and \( a_i, b_i \in \{0, 1, \ldots, p - 1\} \).

Choose a minimal set of generators \( \varphi_1, \ldots, \varphi_h \) of \( L_1 \). From Lemma 4.4 we see that there exists \( \varphi \in L_1 \) such that \( L_{x} = L_{e_1}^{a_1} \cdots L_{e_k}^{a_k} L_c \varphi \). Since \( \varphi \) depends only on \( a_1, \ldots, a_k \), we have

\[
L_{e_1}^{a_1} \cdots L_{e_k}^{a_k}(c) \quad \text{and} \quad L_{e_1}^{b_1} \cdots L_{e_k}^{b_k}(d)
\]

for some mappings \( \delta_s : \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p \to \mathbb{Z}_p \), \( 1 \leq s \leq h \). From Lemma 3.5 one obtains

\[
\varphi_1^{\delta_1(a_1, \ldots, a_k)} \cdots \varphi_h^{\delta_h(a_1, \ldots, a_k)} L_{e_1}^{b_1} \cdots L_{e_k}^{b_k}(d) = L_{e_1}^{b_1} \cdots L_{e_k}^{b_k} \prod_{s, j} [\varphi_{s, L_{e_j}}^{\delta_s(a_1, \ldots, a_k)} b_j] \quad \text{and}
\]

\[
L_{e_1}^{a_1} \cdots L_{e_k}^{a_k} L_{e_1}^{b_1} \cdots L_{e_k}^{b_k} = L_{e_1}^{a_1+b_1} \cdots L_{e_k}^{a_k+b_k} \prod_{i > j} [L_{e_i}, L_{e_j}]^{a_i b_j}.
\]

Fix now some \( z \in Z, z \neq 1 \). Let \( u_{s j} \) and \( v_{i j} \) be defined so that

\[
[\varphi_{s, L_{e_j}}] = L^{u_{s j}} z \quad \text{and} \quad [L_{e_i}, L_{e_j}] = L^{v_{i j}} z.
\]

Then

\[
x \cdot y = L_{e_1}^{a_1+b_1} \cdots L_{e_k}^{a_k+b_k} L_z^{\tau(x, y)}(cd),
\]

where

\[
\tau(x, y) = \sum u_{s j} \delta_s(a_1, \ldots, a_k) b_j + \sum v_{i j} a_i b_j.
\]

Set \( \eta_j(a_1, \ldots, a_k) = \sum_u u_{s j} \delta_s(a_1, \ldots, a_k) \). Under this notation

\[
\tau(x, y) = \sum \eta_j(a_1, \ldots, a_k) b_j.
\]

Identify \( L_{e_1}^{a_1} \cdots L_{e_k}^{a_k}(c^c) \) with \( (a_1, \ldots, a_k, c) \). We have obtained a general formula

\[
(a_1, \ldots, a_k, c)(b_1, \ldots, b_k, d) = \left( a_1 + b_1, \ldots, a_k + b_k, c + d + \sum_j \eta_j(a_1, \ldots, a_k) b_j \right).
\]

The addition in each coordinate runs according to the order of \( L_{e_i} \), i.e. modulo \( p \) or \( p^2 \).

Suppose first that \( p \) is odd. Then only \( L_{e_1} \) can be of order \( p^2 \) (see Lemma 4.5). If \( L_{e_1} \) is of order \( p \), then our formula corresponds to the requirements of the proposition. Indeed, set \( G = (\mathbb{Z}_p)^{k+1}, R = 0 \times \cdots \times 0 \times \mathbb{Z}_p \) and denote by \( b : G \times G \to R \) the mapping that sends each pair \( (a_1, \ldots, a_k, c, (b_1, \ldots, b_k, d)) \) to \( (0, \ldots, 0, \sum_j \eta_j(a_1, \ldots, a_k) b_j) \). It is clear immediately that \( b \) is zero preserving and right additive.

Assume now that \( L_{e_1} \) is of order \( p^2 \). Choose \( z \in Z \) so that \( L_{e_1}^p = L_z \). Then

\[
L_{e_1}^{a_1} \cdots L_{e_k}^{a_k} L_z^{c}(1) = L_{e_1}^{a_1+p c} L_{e_2}^{a_2} \cdots L_{e_k}^{a_k}(1),
\]

and hence we can write our general formula as

\[
(a_1 + p c, a_2, \ldots, a_k) \cdot (b_1 + p d, b_2, \ldots, b_k)
\]

\[
= \left( a_1 + b_1 + p(c + d) + p \sum_j \eta_j(a_1, \ldots, a_k) b_j, a_2 + b_2, \ldots, a_k + b_k \right).
\]
If one admits $0 \leq a_1 < p^2$ and $0 \leq b_1 < p^2$, then this can be simplified to

$$(a_1, \ldots, a_k) \cdot (b_1, \ldots, b_k) = \left( a_1 + b_1 + p \sum_j \eta_j(a_1, \ldots, a_k) b_j, a_2 + b_2, \ldots, a_k + b_k \right),$$

under the provision that $\eta_j(a_1, a_2, \ldots, a_k) = \eta_j(a'_1, a_2, \ldots, a_k)$ if $a_1 \equiv a'_1 \mod p$. We can now set $G = \mathbb{Z}_p^2 \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, $R = p \mathbb{Z}_p^2 \times 0 \times \cdots \times 0$, and the definition of $b$ is clear.

Suppose finally $p = 2$, and denote by $\oplus$ the addition modulo 2. Let $U \subseteq \{1, \ldots, k\}$ be the set of indices where $L_{e_i}$ is of order 4. By Lemma 3.6 the general formula can be written as

$$(a_1, \ldots, a_k) \cdot (b_1, \ldots, b_k) = \left( a_1 \oplus b_1, \ldots, a_k \oplus b_k, \sum_j \eta_j(a_1, \ldots, a_k) b_j + \sum_{j \in U} a_j b_j \right),$$

and the rest is clear. □

For $p$ odd we hence have either $G = V \times F$, or $G = W \times C$, where $V$ and $W$ are finite vector spaces over $F \cong \mathbb{Z}_p$, and $C$ is the cyclic group of order $p^2$. Furthermore, $R = 0 \times F$ or $R = 0 \times pC$.

5. Isomorphisms and power mappings

In this section we collect several statements that are useful for solving the isomorphism problem for extraspecial LCC loops and are of general character.

Throughout the section we shall assume that $G$ is an additive abelian group with a subgroup $R$ and that $b: G \times G \to R$ is a zero preserving mapping with $\text{Rad}(b) \supseteq R$ that is additive on the right. The loop with operation

$$x \cdot y = x + y + b(x, y)$$

will be denoted from here on by $G[b] = G[b(x, y)]$.

**Proposition 5.1.** Let $\varphi: G \to R$ be a group homomorphism with $R \subseteq \text{Ker} \varphi$, and let $q: G \to R$ be a mapping with $q(x + r) = q(x)$ for all $x \in G$ and $r \in R$ such that $f(x, y) = q(x + y) - q(x) - q(y)$ is a biadditive mapping $G \times G \to R$. Then

(i) $x \mapsto x + \varphi(x)$ is an automorphism of $G[b]$, and
(ii) $x \mapsto x + q(x)$ is an isomorphism $G[b] \cong G[b + f]$.

**Proof.** We have $b(x + \varphi(x), y + \varphi(y)) = b(x, y)$ and $\varphi(x) + \varphi(y) = \varphi(x + y) = \varphi(x + y + b(x, y))$. Hence $(x + \varphi(x)) \cdot (y + \varphi(y)) = x + y + b(x, y) + \varphi(x + y)$ is the image of $x \cdot y = x + y + b(x, y)$ under the mapping of point (i).

To verify (ii) note that the product of $x + q(x)$ and $y + q(y)$ in $G[b + f]$ is equal to $x + y + q(x) + q(y) + b(x, y) + f(x, y) = x + y + b(x, y) + q(x + y)$, which is the image of $x \cdot y = x + y + b(x, y)$ under the mapping $u \mapsto u + q(u)$. □
Lemma 5.2. Suppose that \( G/R = \langle e_1 R \rangle \oplus \cdots \oplus \langle e_k R \rangle \) for some \( e_1, \ldots, e_k \in G \) such that \( b(e_i, e_j) = 0 \) whenever \( 1 \leq i \leq j \leq k \). Then \( a_1 e_1 + \cdots + a_k e_k = L_{e_1}^{a_1} \cdots L_{e_k}^{a_k}(0) \), for all non-negative integers \( a_1, \ldots, a_k \).

Proof. Proceed by induction on \( s = a_1 + \cdots + a_k \). The cases \( s = 0 \) and \( s = 1 \) are clear. Assume \( s > 1 \) and choose the least index \( i \) with \( a_i \geq 1 \). Put \( x = (a_i - 1)e_i + a_{i+1}e_{i+1} + \cdots + a_k e_k \). Then \( x = L_{e_i}^{a_i-1} L_{e_{i+1}}^{a_{i+1}} \cdots L_{e_k}^{a_k}(0) \), by the induction assumption, and so \( L_{e_i}^{a_i} \cdots L_{e_k}^{a_k}(0) = e_i \cdot x = a_i e_i + \cdots + a_k e_k \cdot b(e_i, x) \). It remains to show \( b(e_i, x) = 0 \). However, that is immediate since \( b(e_i, x) = (a_i - 1)b(e_i, e_i) + a_{i+1}b(e_i, e_{i+1}) + \cdots + a_k b(e_i, e_k) \), and \( b(e_i, e_j) = 0 \) when \( k > j \geq i \). \( \square \)

Lemma 5.3. Suppose that \( G/R \) is of exponent 2, and let \( G/R = \langle e_1 R \rangle \oplus \cdots \oplus \langle e_k R \rangle \) for some \( e_1, \ldots, e_k \in G \) such that \( b(e_i, e_j) = 0 \) whenever \( 1 \leq i < j \leq k \). Then \( a_1 e_1 + \cdots + a_k e_k = L_{e_1}^{a_1} \cdots L_{e_k}^{a_k}(0) \) for all \( a_1, \ldots, a_k \in \{0, 1\} \).

Proof. Proceed again by induction on \( s = a_1 + \cdots + a_k \). Assume \( s > 1 \) and let \( i \) be the least with \( a_i = 1 \). Put \( x = a_{i+1}e_{i+1} + \cdots + a_k e_k \). The induction assumption gives \( L_{e_i}^{a_i} \cdots L_{e_k}^{a_k}(0) = e_i \cdot x = a_i e_i + \cdots + a_k e_k \cdot b(e_i, x) \), and \( b(e_i, x) = a_{i+1}b(e_i, e_{i+1}) + \cdots + a_k b(e_i, e_k) = 0 \). \( \square \)

Lemma 5.4. Consider \( x, y \in G \) and \( j \geq 0 \). In \( Q = G[b] \) 
\[
L_b^j(y) = jx + y + jb(x, y) + \binom{j}{2}b(x, x) 
\]

Proof. Proceed by induction on \( j \). One has \( x \cdot (jx + y) = (j+1)x + y + jb(x, x) + b(x, y) \), and \( j + \binom{j}{2} = \binom{j+1}{2} \). \( \square \)

Proposition 5.5. Let both \( R \) and \( G/R \) be of exponent \( p \), \( p \) an odd prime. Put \( Q = G[b] \) and consider \( x \in Q \). Then \( L_b^p(y) = y + px \) for all \( y \in Q \). Furthermore, \( x \mapsto px \) is an endomorphism of \( Q \), and its kernel consists of all \( x \in Q \) with \( L_b^x \) of exponent \( p \).

Proof. We have \( L_b^p(y) = y + px + pb(x, y) + \binom{p}{2}b(x, x) \), by Lemma 5.4. However, \( p \) divides \( \binom{p}{2} \), and \( R \) is of exponent \( p \). Thus \( L_b^p(y) = y + px \). Clearly, \( p(x + y + b(x, y)) = px + py \), and \( px \cdot py = px + py \) follows from \( px, py \in R \). \( \square \)

The following proposition is worth stating, despite the fact that its proof is easy enough to be omitted.

Proposition 5.6. Let \( Q = G[b] \). Then \( x \in N_2 \) if and only if \( b(y_1 + y_2, x) = b(y_1, x) + b(y_2, x) \) for all \( y_1, y_2 \in Q \), and \( x \in N_p \) if and only if \( b(x + y_1, y_2) = b(x, y_2) + b(y_1, y_2) \) for all \( y_1, y_2 \in Q \). Furthermore, \( Z(Q) = \{ x \in N_2 ; b(x, y) = b(y, x) \ \text{for all} \ y \in Q \} \).

Corollary 5.7. Let \( Q = G[b] \). Then \( Z(Q) = R \) if and only if for each \( x \in G \setminus R \) there exist \( y_1, y_2 \in G \) with \( b(x, y_1) \neq b(y_1, x) \) or \( b(x + y_1, y_2) \neq b(x, y_2) + b(y_1, y_2) \).

6. Isomorphisms of extraspecial LCC loops

By Theorem 4.6 every extraspecial LCC loop is of the form \( G[b] \), where either \( G = V \times F \), \( V \) a finite vector space over \( F \cong \mathbb{Z}_p \), \( p \) a prime, or \( G = W \times C \), where \( C \) is a cyclic group of
order $p^2$, and $W$ is a finite vector space over $F = pC \cong \mathbb{Z}$. In the former case $R = 0 \times F$, and in the latter case $R = 0 \times pC$ (which can also be expressed as $0 \times F$).

If $G = W \times C$, then define $V$ as $W \times C / pC = G / (0 \times pC)$. The mapping $b : G \times G \to R$ can be regarded as a mapping $V \times V \to F$. On the other hand, any $b : V \times V \to F$ that is zero preserving and right additive can be identified with its lift to $G \times G \to R$. In such a case we shall denote the corresponding loop by $G[b]$ as well.

**Lemma 6.1.** Assume $G = V \times F$, and consider $\lambda \in F^*$ and $\tau \in GL(V)$. Then

(i) $G[b(x, y)] \cong G[b(\tau(x), \tau(y))]$, $(x, i) \mapsto (\tau^{-1}(x), i)$, and

(ii) $G[b(x, y)] \cong G[\lambda b(x, y)]$, $(x, i) \mapsto (\lambda x, \lambda i)$.

**Proof.** The product of $(\tau^{-1}(x), i)$ and $(\tau^{-1}(y), j)$ in $G[b(\tau(x), \tau(y))]$ is equal to $(\tau^{-1}(x + y), i + j + b(x, y))$, which is the image of $(x, i) \cdot (y, j) = (x + y, i + j + b(x, y))$.

The product of $(x, \lambda i)$ and $(y, \lambda j)$ in $G[\lambda b(x, y)]$ is equal to $(x + y, \lambda i + \lambda j + \lambda b(x, y))$, which is the image of $(x, i) \cdot (y, j)$ again. □

In the next lemma (and similarly elsewhere) we denote by $\lambda^{-1}$ the multiplicative inverse modulo $p^2$.

**Lemma 6.2.** Assume $G = W \times C$, and consider $\lambda \in \mathbb{Z}_{p^2} \setminus p\mathbb{Z}_{p^2}$ and $\alpha \in Aut G$. Suppose that $\alpha(x) = x$ for all $x \in 0 \times pC$:

(i) $G[b(x, y)] \cong G[b(\alpha(x), \alpha(y))]$, $x \mapsto \alpha^{-1}(x)$, and

(ii) $G[b(x, y)] \cong G[b(\lambda x, y)]$, $x \mapsto \lambda^{-1} x$.

**Proof.** The product of $\alpha^{-1}(x)$ and $\alpha^{-1}(y)$ in $G[b(\alpha(x), \alpha(y))]$ is equal to $\alpha^{-1}(x + \alpha^{-1}(y) + b(x, y)) = \alpha^{-1}(x + y + b(x, y))$, as $b(x, y) \in 0 \times pC$.

The product of $\lambda^{-1} x$ and $\lambda^{-1} y$ in $G[b(\lambda x, y)]$ gives $\lambda^{-1} x + \lambda^{-1} y + b(x, \lambda^{-1} y) = \lambda^{-1} (x + y + b(x, y))$, as $b$ is additive on the right. □

It is natural to expect that the case $W \times C$ will offer fewer isomorphisms than the $V \times C$. Point (ii) of Lemma 6.2 seems to suggest that for $W \times C$ there exist isomorphisms that do not have a parallel in the case $V \times F$. But that is not true, as the mapping $(x, i) \mapsto (\lambda^{-1} x, \lambda^{-1} i)$, $\lambda \in \mathbb{Z}_{p^2}^*$, can be composed from the mappings $(x, i) \mapsto (\lambda^{-1} x, \lambda^{-1} i)$ and $(x, i) \mapsto (\lambda^{-1} x, i)$, which gives an isomorphism $G[b] \cong G[\lambda^{-1} b(\lambda x, \lambda y)] = G[b(\lambda x, y)]$.

To exploit Lemma 6.2 fully we need to know what the automorphisms of $W \times C$ look like.

**Lemma 6.3.** The automorphisms of $W \times C$ are of the form $(u, i) \mapsto (\tau(u) + i w, \lambda i + \mu(u))$, where $\tau \in GL(W)$, $w \in W$, $\lambda, \mu \in \mathbb{Z}_{p^2}^*$ and $\mu : W \to pC$ is a group homomorphism (a linear form, in fact). Every such automorphism can be expressed as $\alpha \beta$, where $\alpha$ fixes each $(0, pi)$, $i \in C$, and $\beta(u, i) = (\lambda u, \lambda i)$ for some $\lambda \in \mathbb{Z}_{p^2}^*$. Each automorphism of $W \times C$ induces an automorphism of $V = W \times C / pC$, and $\tau \in GL(V)$ can be obtained in this way if and only if $W \times 0$ is its proper subspace.

**Proof.** Elements of exponent $p$ form the subgroup $W \times pC$, and $(0, g)$, $g$ a generator of $C$, is mapped by each automorphism to an element of order $p^2$. The rest is easy. □
**Proposition 6.4.** Let $V$ be a finite vector field over a prime field $F$. Suppose that $b_t$, $t \in \{1, 2\}$, are zero preserving mappings $V \times V \to F$ that are additive on the right. Let $Q_t$ be the loop on $V \times F$ with $(x, i) \cdot (y, j) = (x + y, i + j + b_t(x, y))$ for all $x, y \in V$ and $i, j \in F$. An isomorphism $\psi : Q_1 \cong Q_2$ that maps $0 \times F$ onto $0 \times F$ exists if and only if

$$b_2(x, y) = \lambda b_1(\tau(x), \tau(y)) + f(x, y)$$

for some $\lambda \in F^*$, $\tau \in GL(V)$ and a bilinear symmetric form $f : V \times V \to F$. If $|F| = 2$, then $f$ has to be an alternating bilinear form.

**Proof.** If $b_2$ and $b_1$ are related by $\lambda$, $\tau$ and $f$, then the isomorphism $Q_1 \cong Q_2$ follows from Lemma 6.1 and Proposition 5.1.

Assume the existence of $\psi : Q_1 \cong Q_2$. Since $0 \times F$ is mapped onto $0 \times F$ by $\psi$, one gets an isomorphism of $Q_1/(0 \times F)$ and $Q_2/(0 \times F)$ which yields an automorphism of $V$. Denote it by $\tau$. Since $(x, i) \mapsto (\tau^{-1}(x), i)$ is an isomorphism of $Q_2 = G[b_2]$ and of $G[2,\tau(x), \tau(y)]$, $G = V \times F$, by Lemma 6.1, we can assume $\tau = \text{id}_V$.

Thus $\psi$ maps every $(x, i) \in V \times F$ to some $(x, j)$.

Fix now a basis $e_1, \ldots, e_k$ of the vector space $V$. If $|F| \geq 3$, then there exists a symmetric bilinear form $f_t$ such that $f_t(e_i, e_j) = -b_t(e_i, e_j)$ whenever $k \geq j \geq i \geq 1$. If $|F| = 2$, find alternating form $f_t$ with $f_t(e_i, e_j) = b_t(e_i, e_j)$, $k \geq j > i \geq 1$.

From Proposition 5.1 we see that one can assume $f_t(e_i, e_j) = 0$ when $k \geq j > i \geq 1$. In addition, $f_t(e_i, e_i) = 0$ can be assumed when $k \geq i \geq 1$ and $|F| \geq 3$.

For each $e_j$, $1 \leq j \leq k$, now consider $i_j \in F$ with $\psi(e_j, 0) = (e_j, i_j)$. Denote by $\varphi$ the linear form $\varphi : V \to F$ which is determined by $\varphi(e_j) = -i_j$. Then $\alpha : (x, i) \mapsto (i, i + \varphi(x))$ is an automorphism of $Q_2$, by Proposition 5.1, and $\alpha \psi$ fixes each $(e_j, 0)$. We can replace $\psi$ by $\alpha \psi$, and then Lemmas 5.2 and 5.3 yield $\psi(x, 0) = (x, 0)$ for every $x \in V$. It is clear that $\psi$ must be one of the isomorphisms described in point (i) of Lemma 6.1. \qed

**Proposition 6.5.** Let $p$ be an odd prime and let $G$ be an abelian additive $p$-group with subgroups $W$ and $C$ such that $G = W \times C$, $W$ is elementary abelian and $C$ is cyclic of order $p^2$. Suppose that $b_t$, $t \in \{1, 2\}$, are zero preserving mappings $G \times G \to pC$ that are additive on the right and satisfy $\text{Rad}(b) \geq pC$. Let $Q_t$ be the loop on $G$ with $x \cdot y = x + y + b_t(x, y)$ for all $x, y \in G$. Then $Q_1 \cong Q_2$ if and only if there exist $\alpha \in \text{Aut} G$, $\lambda \in F^*$ and a biadditive symmetric mapping $f : G \times G \to pC$ such that $\alpha(p i) = pi$ for all $i \in C$, $\text{Rad}(f) \geq pC$, and

$$b_2(x, y) = b_1(\lambda \alpha(x), \alpha(y)) + f(x, y)$$

for all $x, y \in G$.

**Proof.** From Proposition 5.5 we see that $pC$ is the set of elements in $Q_t$ that can be expressed as $L^p_i(0)$, $x \in G$. Hence an isomorphism $\psi : Q_1 \cong Q_2$ has to map $pC$ onto $pC$. If $b_2$ can be obtained from $b_1$ by means of $\alpha$, $\lambda$ and $f$, then $Q_1 \cong Q_2$ follows from Proposition 5.1 and Lemma 6.2.

Suppose that we have an isomorphism $\psi : Q_1 \cong Q_2$. From Proposition 5.5 we also get that $\psi$ must map $W \times pC$ onto $W \times pC$. Thus $\psi$ induces an automorphism of $V = W \oplus C/pC$ (which we identify with $G/pC$) that maps $W$ onto $W$. By Lemma 6.3 there exist $\alpha \in \text{Aut} G$ and $\lambda \in Z^*_{p^2}$ such that $x \mapsto \alpha(\lambda x)$ (which is an automorphism of $G$) induces the same automorphism.
of $V$. The mapping $x \mapsto \alpha^{-1}(\lambda^{-1}x)$ is the inverse automorphism of $G$, and by Lemma 6.2 it is also an isomorphism of $Q_2 = G[b_2]$ onto $G[b_2(\lambda x, \alpha(y))]$. The composition of $\psi$ with this isomorphism induces $\mathrm{id}_V$, and hence we can assume that $\psi(x)$ and $x$ differ by an element of $pC$, for all $x \in G$.

Choose now $e_2, \ldots, e_k$ a basis of $W$, and choose $e_1$ to be a generator of $C$. Then $e_1 + pC, \ldots, e_k + pC$ is a basis of $V$. Proceed now like in the proof of Proposition 6.4, using Proposition 5.1 and Lemma 5.2. Here we turn $\psi$ into the identity mapping since each element of $G$ can be expressed as $L_{e_2}^{a_1}L_{e_2}^{a_2}\cdots L_{e_k}^{a_k}(0)$, for some nonnegative $a_1, \ldots, a_k$. □

In Proposition 6.4 we did not describe all possible isomorphisms $Q_1 \cong Q_2$, but only those that map $0 \times F$ onto $0 \times F$. If both $Q_i$ are extraspecial, then $0 \times F$ is equal to their center, and hence each isomorphism must be of this kind. We can hence state

**Theorem 6.6.** Each extraspecial LCC $p$-loop, $p$ a prime, is isomorphic to some $G[b]$, where $G$ is either an elementary abelian $p$-group, or $G$ is a product of the latter with a cyclic group of order $p^2$, and $b : G \times G \to R$ is a zero preserving mapping that is additive on the right, $R = \text{Rad}(b) \leq G$, $|R| = p$ and $G/R$ elementary abelian. The loop operation of $G[b]$ is given by $x \cdot y = x + y + b(x, y)$, and a loop $G[b]$ is extraspecial if the additional conditions of Corollary 5.7 are satisfied. Propositions 6.4 and 6.5 give conditions under which $G[b_1]$ is isomorphic to $G[b_2]$.

7. Extraspecial CC loops

We have already mentioned in Section 2 that extraspecial CC 2-loops are Moufang. Enough information on this subject can be found in [2,4,12,13]. Here we shall consider extraspecial CC loops of odd order.

Let $G$ be an abelian $p$-group with a $p$-element central subloop $F$ such that $\bar{G} = G/F$ is elementary abelian. Write $\bar{x}$ in place of $xF$, for every $x \in G$. For a trilinear symmetric form $f: \bar{G} \times \bar{G} \times \bar{G} \to F$ and an alternating form $g: \bar{G} \times \bar{G} \to F$ denote by $G[f, g]$ the loop with

$$x \cdot y = x + y + f(\bar{x}, \bar{x}, \bar{y}) + g(\bar{x}, \bar{y}).$$

Loop $G[f, g]$ is conjugacy closed, by Theorem 2.1.

**Theorem 7.1.** Let $Q$ be a CC loop such that $Q/Z$ is an elementary abelian $p$-group, $p$ an odd prime, and $Z$ is a $p$-element central subloop. Then $Q$ is isomorphic to some $G[f, g]$. If $Q = G[f, g]$, then the associator $[x, y, z] = (x \cdot yz) \backslash (xy \cdot z)$ is equal to $2f(\bar{x}, \bar{y}, \bar{z})$, for all $x, y, z \in G$.

**Proof.** Each bilinear form $\bar{G} \times \bar{G} \to F$ can be (uniquely) represented as $g + h$, where $g$ is an alternating form and $h$ a symmetric form. The symmetric form can be removed when isomorphism classes are considered, by Proposition 5.1. Computation of the associator can be done easily, and the rest follows from Proposition 2.4 and Theorem 4.6. □

Let $V$ be a vector space over $F$, and for $i \in \{1, 2\}$ let $f_i$ and $g_i$ be a trilinear and bilinear form from $V$ to $F$, respectively. Say that pairs $(f_1, g_1)$ and $(f_2, g_2)$ are similar if and only if there exists $\tau \in GL(V)$ and $\lambda \in F^*$ such that $f_2(x, y, z) = \lambda f_1(\tau(x), \tau(y), \tau(z))$, and $g_2(x, y) = \lambda g_1(\tau(x), \tau(y))$, for all $x, y, z \in V$. 
Theorem 7.2. Let G = V × F be an elementary abelian p-group, p = |F| an odd prime. For r ∈ {1, 2} consider a trilinear form fr and a bilinear form gr, both on G/F ∼= V, with values in F. An isomorphism G[f1, g1] ∼= G[f2, g2] that maps 0 × F onto 0 × F exists if and only if the pairs (f1, g1) and (f2, g2) are similar.

Proof. It is simpler to consider fr and gr as forms on V. The operation can be then presented as (x, i) · (y, j) = (x + y, i + j + fr(x, x, y) + gr(x, y)). From Proposition 6.4 we see that the isomorphism takes place if and only if

\[ f_2(x, x, y) + g_2(x, y) = λ f_1(τ(x), τ(x), τ(y)) + λ g_1(τ(x), τ(y)) + h(x, y), \]

where λ ∈ F*, τ ∈ GL(V) and h : V × V → F a symmetric bilinear form. Computation of the associators yields f_2(x, x, y) = λ f_1(τ(x), τ(x), τ(y)), and so there must be g_2(x, y) = λ g_1(τ(x), τ(y)) + h(x, y). A sum of an alternating form with a symmetric form is alternating if an only if the symmetric part (i.e., h) is equal to zero. □

The case when G is not elementary abelian does not seem to offer such a similarly nice description of isomorphism classes. We shall give only the procedural description which follows from Proposition 6.5.

Let G = W × C, where W is elementary abelian and C is cyclic of order p^2. Put F = pC and identify V = W × C/F with G. The forms of G[f, g] will be regarded as defined on V.

Proposition 7.3. Denote by γ a generator of C/F, and for r ∈ {1, 2} let fr and gr be a symmetric trilinear form and alternating bilinear form on V, respectively. Then G[f1, g1] ∼= G[f2, g2] if and only if there exist τ ∈ GL(V) and λ ∈ F* such that τ(W × 0) = W × 0, τ(0, γ) = (w, λ γ) for some w ∈ W, and

\[ f_2(x, y, z) = λ^{-1} f_1(τ(x), τ(y), τ(z)) \quad \text{and} \quad g_2(x, y) = λ^{-1} g_1(τ(x), τ(y)) \]

for all x, y, z ∈ V.

Proof. By Proposition 6.5, the isomorphism takes place if and only the mapping f_2(x, y, z) + g_2(x, y) equals to some f_1(α(λ x), α(λ x), α(γ)) + g_1(α(λ x), α(γ)) + h(x, y), where h is a symmetric bilinear form, and α and λ are derived from Proposition 6.5. The meaning of α here is somewhat modified. In Proposition 6.5 it denotes an automorphism of W × C that fixes elements of 0 × F pointwise. Here we consider its factorization to an automorphism of V. It is easy to see that F is fixed pointwise if and only if the factorization fixes (0, γ). Furthermore, α maps W × 0 onto itself (see also Lemma 6.3). The linearity gives f_1(α(λ x), α(λ x), α(γ)) = λ^{-1} f_1(α(λ x), α(λ x), α(λ γ)) and, similarly, g_1(α(λ x), α(γ)) = λ^{-1} g_1(α(λ x), α(λ γ)). The symmetric form vanishes like in the proof of Theorem 7.2, and by setting τ(x) = α(λ x) we obtain all of the claimed properties. □

8. Bol loops of order 8

For a loop Q put L(Q) = {L_a; \ a ∈ Q}. LCC loops can be characterized by the property that L(Q) is closed under the operation x y x^{-1} (i.e., x, y ∈ L(Q) ⇒ x y x^{-1} ∈ L(Q)). Now, (left) Bol loops are those that have L(Q) closed under the operation x y x. It is easy to see that if x ∈ L(Q),
then \(x^k \in L(Q)\) for every integer \(k\) (cf. [20]). Hence Bol loops also are closed under the operation \(x^{-1}yx^{-1}\).

To see that a class of loops is isotopically invariant (universal), it suffices to show that it is closed under left principal isotopes \(x \circ y = x/e \cdot y\), and the right principal isotopes \(x \circ y = x \cdot f/y\). The left isotopes have the left translation of \(x\) equal to \(L_{x/e}\), and so the set \(L(Q)\) does not change. Hence the left isotopes of both Bol loops or LCC loops also are Bol or LCC, respectively. The right isotopes of LCC loops do not have to be LCC. The left translations of the right principal isotope are equal to \(L_xL_f^{-1}\). We claim that if a subset \(S\) of a group \(G\) is closed under operations \(aba\) and \(a^{-1}\), then the set \(Sa^{-1}\), \(a \in S\), is closed under the operation \(aba\) as well. Indeed, for all \(a, b \in S\) we are concerned with \(af^{-1}bf^{-1}af^{-1}\). However, \(bf^{-1}af^{-1} \in S\), \(a = ab\) \(a \in S\), and so \(af^{-1}bf^{-1}af^{-1} = a^{-1}f^{-1} \in Sf^{-1}\).

We have proved that Bol loops are isotopically invariant. This is a well-known fact. Our proof (which belongs to loop-theoretical folklore) is a bit shorter than the usual one, and was included to prepare ground for the application of isotopy below.

**Lemma 8.1.** Let \(Q\) be a loop:

(i) If \(Q\) is a Bol loop, then it is LCC if and only if \(Q/N_\lambda\) is of exponent two.

(ii) If \(Q\) is power associative, and \(Q/Z(Q)\) is a cyclic group, then \(Q = Z(Q)\).

(iii) If \(Q\) is finite and \(S\) is its subloop of order \(|Q|/2\), then \(S\) is a normal subgroup.

(iv) If \(S\) is a normal subgroup of order 2, then \(S\) is a central normal subgroup.

**Proof.** Point (i) is proved in [19]. Point (ii) can be proved in the same way as the corresponding group-theoretical statement. Points (iii) and (iv) are easy and well known.

We have mentioned that \(L_x^k\) is a left translation for all integers \(k\) and all \(x \in Q\), for every Bol loop \(Q\). It follows that \(Q\) is power associative, and \(L_x^k = L_x^kQ\). In other words, Bol loops are left power alternative.

**Proposition 8.2.** Let \(Q\) be a Bol loop of order 8. Then \(Q\) is LCC, and it is either an abelian group, or \(Z(Q)\) has exactly two elements.

**Proof.** The points of Lemma 8.1 will be referred to in the proof directly as (i), (ii), (iii) and (iv). Let us assume that \(Q\) is a Bol loop on eight elements, and suppose that it is not an abelian group. It will suffice to show \(|Z(Q)| = 2\). Indeed, in such a case \(Q/Z(Q)\) has to be of exponent two, by (ii), and so (i) applies. Since \(Q\) cannot contain an element of order eight, there are only two possibilities: either every \(x \in Q\), \(x \neq 1\), is of order two, or \(Q\) contains an element of order four. We shall assume the latter case, and return to the former one at the end of the proof.

From (ii) and (iv) we also see that it suffices to find at least one 2-element normal subgroup. If \(Q\) contains two different subloops \(S_1\) and \(S_2\) of index two, then \(S_1 \cap S_2\) is a subloop, as \(Q/S_1 \cong S_1S_2/S_1 \cong S_2/S_1 \cap S_2\).

Let \(S = \{1, a, z, a^{-1}\}\) be the only 4-element subgroup of \(Q\). For every \(x \in Q \setminus S\) the translation \(L_xL_zL_x = L_x(xz)\) is of order 2, and the normality of \(S\) implies \(x \cdot zx = z\). Hence \(zx = xz\) for all \(x \in Q\). Choose \(x, y \in Q \setminus S\) such that \(xy = z\). To get a contradiction, we shall show that \(D = \{x, y, z, 1\}\) is a subloop of \(Q\). To prove it note first that \(xz = x \cdot xy = y = zx\), and so \(zy = z \cdot zx = x\). This verifies that \(D\) is closed under multiplication by \(x\) and \(z\) on the left. We also have \(yz = zy = x\), and \(yx = z\) follows from \(yz = x = y \cdot yx\).
Assume now that $L_x^2 = \text{id}_Q$ for every $x \in Q$. Let there exist $e, f \in Q$ such that $(L_eL_f)^2 \neq \text{id}_Q$, and consider the right principal isotope with operation $x \circ y = x \cdot f \setminus y$. Then $Q(\circ)$ is a Bol loop with a nontrivial center, by the preceding part of the proof, and so both $Q(\circ)$ and $Q(\cdot)$ have a nontrivial center which is of order two. If $(L_xL_y)^2 = \text{id}_Q$ for all $x, y \in Q$, then $L_xL_y = L_yL_x$ for all $x, y \in Q$, which means that $L$ is commutative. Hence it is regular and $Q$ is an abelian group. □

Bol loops of order 8 were classified by Burn [3]. His proof runs by a direct combinatorial argument during which the left translations are constructed for representatives of all isomorphism classes. The length of the proof exceeds three pages, and a lot of verifications is needed.

From Proposition 8.2 and from point (ii) of Lemma 8.1 we see that every nonassociative Bol loop of order 8 is an extraspecial LCC loop. To classify all of them, one can use Theorem 4.6 and Proposition 6.4. In this way we get a shorter proof of Burn’s theorem. The bulk of our proof is Proposition 8.2 and the following lemma.

**Lemma 8.3.** Define an equivalence $\sim$ on the set of $3 \times 3$ matrices over $F = \{0, 1\}$ in such a way that

1. $(m_{ij}) = M \sim N = (n_{ij})$ if there exists a permutation $\tau \in S_3$ with $n_{ij} = m_{\tau(i)\tau(j)}$ for all $i, j \in \{1, 2, 3\}$, and

2. every matrix $M$ is equivalent to $M + A$, where $A$ is the matrix with zeros on the diagonal, and ones out of the diagonal.

Consider only those matrices $M$, in which the sum of all columns is a zero vector, and the sum of all rows is a nonzero vector. The equivalence $\sim$ yields on these matrices six classes, and the following matrices are their representatives:

\[
\begin{pmatrix}
0 & 0 & 0 \\
0 & 0 & 0 \\
1 & 1 & 0
\end{pmatrix}
\quad
\begin{pmatrix}
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & 1
\end{pmatrix}
\quad
\begin{pmatrix}
0 & 0 & 0 \\
1 & 0 & 1 \\
0 & 1 & 1
\end{pmatrix}
\quad
\begin{pmatrix}
0 & 0 & 0 \\
0 & 1 & 1 \\
1 & 0 & 1
\end{pmatrix}
\quad
\begin{pmatrix}
1 & 0 & 1 \\
0 & 1 & 1 \\
0 & 1 & 1
\end{pmatrix}
\quad
\begin{pmatrix}
M_1 \\
M_2 \\
M_3
\end{pmatrix}
\quad
\begin{pmatrix}
M_4 \\
M_5 \\
M_6
\end{pmatrix}
\]

**Proof.** Let $M = (m_{ij})$ be a matrix with zero sum of columns and nonzero sum of rows. Denote the rows by $a_i$ and the columns by $b_i$, $i \in \{1, 2, 3\}$. Denote also the diagonal by $d$. Consider all of them as vectors in $F^3$. For each vector $u$ denote by $|u|$ the number of ones in the vector. By (2), only matrices with $|a_1| + |a_2| + |a_3| - |d| \leq 3$ need to be investigated. Furthermore, only matrices with $\sum a_i \neq 0$ and $\sum b_i = 0$ are considered.

If $|d| = 0$, then we can assume $|a_3| \neq 0$, which implies $|a_3| = 2$ and $|a_1| = 0 = |a_2|$. Clearly $M = M_1$.

If $|d| = 1$, then we can assume $a_3 = (0, 1, 1)$. The case $|a_1| = |a_2| = 0$ gives $M_2$. Let $a_1$ or $a_2$ be a nonzero vector. If $|a_1| = 2$ and $|a_2| = 0$, then $\sum a_i = 0$. The only possible completion with $|a_1| = 0$ and $|a_2| = 2$ is $M_3$.

If $|d| = 2$, then we assume $m_{2,2} = m_{3,3} = 1$. It follows $|a_2| + |a_3| - |d| = 2$, and hence there must be $|a_1| = 0$. If $a_2 = a_3 = (0, 1, 1)$, then we get again the zero sum of rows. Therefore $a_3 = (1, 0, 1)$ can be assumed. Matrices $M_4$ and $M_5$ give the two possible completions.

Finally, let us have $|d| = 3$. Then $|a_i| = 2$ for every $i \in \{1, 2, 3\}$, and so $\sum |a_i| = \sum |b_i| = 6$. If $|b_i| = 2$ for every $i$, then $\sum a_i = 0$. Thus we can assume $|b_3| = 3$. The symmetry between the
first and the second coordinate implies that we also can assume \(a_3 = (0, 1, 1)\). The rest of \(M_6\) is forced out by \(|a_1| = 2 = |a_2|\) and \(|d| = 3\). \(\Box\)

**Theorem 8.4.** Let \(V\) be a 4-element vector space over \(F = \{0, 1\}\), with nonzero elements \(\{e, f, g\}\). For \(b : V \times V \to F\) denote by \(V(b)\) the loop on \(V \times F\) with \((x, i) \cdot (y, j) = (x + y, i + j + b(x, y))\). Let \(b_t : V \times V \to F, 1 \leq t \leq 6\), be zero preserving mappings that are right linear, and satisfy

\[
\begin{align*}
    b_1(f, e) &= 1, \\
    b_2(f, f) &= 1, \\
    b_3(f, e) &= b_3(g, f) = 1, \\
    b_4(e, f) &= b_4(g, e) = 1, \\
    b_5(e, e) &= b_5(f, f) = 1, \\
    b_6(e, e) &= b_6(f, f) = b_6(g, f),
\end{align*}
\]

with \(b_t(x, y) = 0\) for all other \((x, y) \in \{e, f, g\} \times \{e, f\}\) (the values \(b_t(x, g)\) are determined by the right linearity). All loops \(V(b_t), 1 \leq t \leq 6\), are nonassociative left Bol loops, and every such loop of order 8 is isomorphic to exactly one of them.

**Proof.** By Proposition 8.2 every nonassociative Bol loop \(Q\) of order eight happens to be an LCC loop with \(|Z(Q)| = 2\). The loop \(Q\) is extraspecial, since \(Q/Z(Q)\) is of exponent 2, by point (i) of Lemma 8.1. Hence it is of the form \(V(b)\) for some zero preserving right additive mapping \(b : V \times V \to F\). We do not wish \(Q\) to be a group, and hence \(b\) is not left additive, by Theorem 2.1. Values \(b(x, y)\), where \(x, y \in \{e, f, g\}\), can be represented by a \(3 \times 3\) matrix, and the right (or left) additivity corresponds to the fact that the sum of columns (or rows) is zero, respectively. Since \(GL(V)\) acts on \(\{e, f, g\}\) as a symmetric group, we get isomorphic loops when the matrices have they rows and columns permuted by the same permutation, by Proposition 6.4. The matrix \(A\) from Lemma 8.3 is the matrix of the only nontrivial symmetric bilinear form on \(V\). Proposition 6.4 thus tells that two matrices represent an isomorphic loop if and only if they are equivalent in the sense of Lemma 8.3. To describe a matrix of \(b\) it suffices to give values for two columns. Each \(b_i, 1 \leq i \leq 6\), corresponds to the matrix \(M_i\), but the labeling of rows (and columns) is different. For \(M_1\) and \(M_2\) use \(e, g, f\), for \(M_3, M_4\) and \(M_6\) use \(e, f, g\), and \(M_5\) corresponds to \(g, e, f\). \(\Box\)

The proof of Lemma 8.3 gives, in fact, a classification for the case of zero row sum as well. Besides the zero matrix one obtains matrices

\[
\begin{pmatrix}
0 & 1 & 1 \\
0 & 0 & 0 \\
0 & 1 & 1
\end{pmatrix}
\quad \text{and} \quad
\begin{pmatrix}
1 & 0 & 1 \\
1 & 1 & 0 \\
0 & 1 & 1
\end{pmatrix}.
\]

The first matrix corresponds to the dihedral group \(D_8\), and the second one to the group of quaternions \(Q_8\).

Methods of this paper clearly offer themselves for further generalization. While LCC loops can be expected to show a large structural diversity, with CC loops one can hope for strong
classifying theorems. Nevertheless, it seems that to study LCC loops of certain specific properties might be the most efficient approach to CC loops.

Acknowledgment

The author thanks the referee for many suggestions how to improve the quality of presentation.

References

[10] A. Drápal, P. Vojtěchovský, Code loops of both parities, manuscript.