SMALL LOOPS OF NILPOTENCY CLASS THREE WITH COMMUTATIVE INNER MAPPING GROUPS

ALEŠ DRÁPAL AND PETR VOJTĚCHOVSKÝ

Abstract. Groups with commuting inner mappings are of nilpotency class at most two, but there exist loops with commuting inner mappings and of nilpotency class higher than two, called *loops of Csörgő type*. In order to obtain small loops of Csörgő type, we expand our programme from *Explicit constructions of loops with commuting inner mappings*, European J. Combin. **29** (2008), 1662–1681, and analyze the following setup in groups:

Let G be a group, $Z \le Z(G)$, and suppose that $\delta : G/Z \times G/Z \to Z$ satisfies $\delta(x,x) = 1$, $\delta(x,y) = \delta(y,x)^{-1}$, $z^{yx}\delta([z,y],x) = z^{xy}\delta([z,x],y)$ for every x, y, $z \in G$, and $\delta(xy,z) = \delta(x,z)\delta(y,z)$ whenever $\{x,y,z\} \cap G'$ is not empty.

Then there is $\mu : G/Z \times G/Z \to Z$ with $\delta(x,y) = \mu(x,y)\mu(y,x)^{-1}$ such that the multiplication $x * y = xy\mu(x,y)$ defines a loop with commuting inner mappings, and this loop is of Csörgő type (of nilpotency class three) if and only if $g(x,y,z) = \delta([x,y],z)\delta([y,z],x)\delta([z,x],y)$ is nontrivial.

Moreover, G has nilpotency class at most three, and if g is nontrivial then $|G| \ge 128$, $|G|$ is even, and g induces a trilinear alternating form. We describe all nontrivial setups (G,Z,δ) with $|G| = 128$. This allows us to construct for the first time a loop of Csörgő type with an inner mapping group that is not elementary abelian.

1. Introduction

Let Q be a loop with neutral element 1. For $x \in Q$, let $L_x : Q \to Q$, $y \mapsto xy$ be the *left translation* by x, and $R_x : Q \to Q$, $y \mapsto yx$ the *right translation* by x in Q. Then

$$\operatorname{Mlt} Q = \langle L_x,\ R_x;\ x \in Q\rangle$$

is the *multiplication group* of Q,

$$\operatorname{Inn} Q = \{\varphi \in \operatorname{Mlt} Q;\ \varphi(1) = 1\}$$

is the *inner mapping group* of Q, and

$$Z(Q) = \{x \in Q;\ \varphi(x) = x \text{ for all } \varphi \in \operatorname{Inn} Q\}$$

is the *center* of Q.

Set $Z_1(Q) = Z(Q)$ and define $Z_{i+1}(Q)$ by $Z(Q/Z_i(Q)) = Q/Z_{i+1}(Q)$. Then Q is *(centrally) nilpotent* if $Z_m(Q) = 1$ for some m, and the *nilpotency class* $\mathrm{cl}(Q)$ of Q is the least integer m for which $Z_m(Q) = 1$ occurs.

The *associator subloop* $A(Q)$ of Q is the smallest normal subloop of Q such that $Q/A(Q)$ is a group. The *derived subloop* Q' is the smallest normal subloop of Q such that Q/Q' is a commutative group. Set $Q^{(1)} = Q'$ and $Q^{(i+1)} = (Q^{(i)})'$. Then Q is *solvable* if $Q^{(m)} = 1$ for some m.

2000 *Mathematics Subject Classification.* 20N05.

Key words and phrases. Loop, central nilpotency, nilpotent class three, commutative inner mapping group, symmetric trilinear form, loop of Csörgő type.

A. Drápal supported by the Institutional Grant MSM 0021620839 and by the Grant Agency of the Czech Republic 201/09/0296. P. Vojtěchovský supported by the Enhanced Sabbatical grant of the University of Denver.

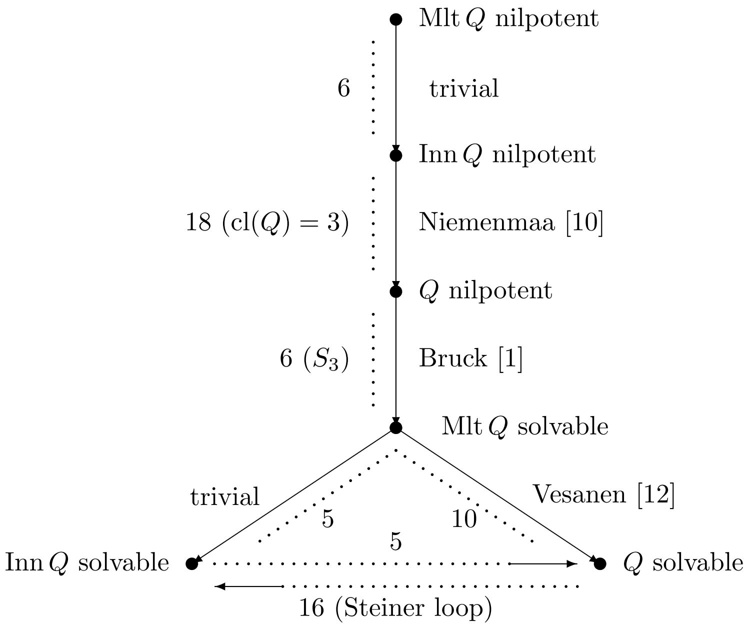

FIGURE 1. Implications among nilpotency and solvability of a finite loop Q, its inner mapping group $\mathrm{Inn}\,Q$, and its multiplication group $\mathrm{Mlt}\,Q$.

Questions concerning relations between nilpotency and solvability of Q, $\mathrm{Inn}\,Q$ and $\mathrm{Mlt}\,Q$ go back at least to 1940s and the foundational paper of Bruck, cf. [1, p. 278]. Figure 1 summarizes what is currently known about this problem for *finite* loops. In more detail and in chronological order:

- if Q is nilpotent then $\mathrm{Mlt}\,Q$ is solvable, by [1, Corollary II, p. 281],
- if $\mathrm{Mlt}\,Q$ is nilpotent then Q is nilpotent, by [1, Corollary III, p. 282],
- if $\mathrm{Mlt}\,Q$ is solvable then Q is solvable, by [12],
- if $\mathrm{Inn}\,Q$ is nilpotent then $\mathrm{Mlt}\,Q$ is solvable, by [7],
- if $\mathrm{Inn}\,Q$ is nilpotent then Q is nilpotent, by [10].

This accounts for all nontrivial implications in Figure 1. Moreover, no implications in the figure are missing, as is indicated by the dotted lines that represent counterexamples and give some information about their nature. For instance, there exists a Steiner loop Q of order 16 which is solvable but $\mathrm{Inn}\,Q$ is not solvable.

Our understanding of the situation is very incomplete, however. If $\mathrm{cl}(Q) = 2$ then $\mathrm{Inn}\,Q$ is abelian by a result of Bruck [1] but, conversely, if $\mathrm{Inn}\,Q$ is abelian we are still at a loss regarding the structure of the loop Q. For instance, we do not know if there exists a loop Q with $\mathrm{Inn}\,Q$ abelian and $\mathrm{cl}(Q) > 3$. We also do not know if there exists an odd order loop Q with $\mathrm{Inn}\,Q$ abelian and $\mathrm{cl}(Q) = 3$.

We call loops with $\mathrm{Inn}\,Q$ abelian and $\mathrm{cl}(Q) \geq 3$ of *Csörgő type* since Piroska Csörgő gave the first example of such a loop [2]. Her example is of order 128 and no known loop of Csörgő type has smaller order. In [5] we have reconstructed Csörgő's example by a method that defines a loop by modifying a group operation. We have shown that a vast number of such examples can be obtained by this method, even for the order 128.

All known examples of loops of Csörgő type of order 128 are very close to groups in the sense that their associator subloop consists of only two elements

In this paper we explore the power of the construction invented in [5]. We show that it cannot be used for odd order loops and that it yields no loop of order less than 128. We also describe all 125 groups of order 128 that can be used in the construction as the starting point. In all cases we obtain a loop Q such that $K = Q/A(Q)$ has $K' = Z(K)$ of order 8. There are 10 such groups K and all of them can occur in our construction. However, we do not know if all loops of Csörgő type can be obtained by our construction.

The original setup of [5] with its complicated subgroup structure (see (A_0)) is recalled in §2. In the same section we introduce the much simpler new setup that is based only on the group G, a central subgroup Z, and a mapping $\delta : G/Z \times G/Z \to Z$. We show that every original setup gives rise to a new setup, cf. Proposition 2.3.

After defining the radical $\operatorname{Rad}\varphi$ and the multiplicative part $\operatorname{Mul}\varphi$ for general mappings φ in §3, we investigate the radical and the multiplicative part of δ and of the three multiplicative mappings $f(x,y,z) = \delta([x,y],z)$, $g(x,y,z) = f(x,y,z)f(y,z,x)f(z,x,y)$ and $h(x,y,z) = [x,[y,z]]$.

In §5 we show how to obtain an original setup from a new setup. As far as the subgroup structure is concerned, it suffices to take $R = \operatorname{Rad}\delta$ and $N = G'R$, cf. Proposition 5.1. There is then an obvious choice for the mapping μ that will turn the new setup into an original setup. With any valid choice of μ we have $\mathrm{cl}(G) \le 3$, $\mathrm{cl}(G[\mu]) \le 3$. Moreover, $\mathrm{cl}(G[\mu]) = 3$ if and only if the mapping g is nontrivial.

§6 is concerned with minimal setups, that is, with nontrivial new setups with G as small as possible. We know from [5] that $|G| \le 128$ in a minimal setup. As a consequence of the Hall-Witt identity, we show that $|G|$ must be even in a nontrivial setup, and that $\operatorname{Im} f$ is a cyclic group of even order in a minimal setup. A more detailed analysis implies that $|G| \ge 128$, and that the equality $|G| = 128$ holds if and only if we find ourselves in one of the three scenarios of Theorem 7.3. Consequently, $\operatorname{Mul}\delta = N = G' \operatorname{Rad}\delta$ in all minimal setups, once again showing the relevance of $\operatorname{Mul}\delta$ and $\operatorname{Rad}\delta$ to the problem at hand.

In §7 we also show that the three scenarios of Theorem 7.3 do occur, and we describe how to construct all minimal setups. Proposition 7.4 characterizes the groups G/Z that occur in minimal setups. The groups G that occur in minimal setups can be found in Subsection 7.2. For each such group G we show how to construct all minimal setups based on it, starting with the determinant g that uniquely specifies the mapping f, which gives rise to δ via some free parameters.

There are many examples of loops of Csörgő type of order 128 due to the free parameters in the transition from f to δ, and also due to the numerous choices of μ for a given δ. Some explicit examples can be found in §8.

As a byproduct, we construct for the first time a loop Q of Csörgő type for which $\operatorname{Inn} Q$ is not elementary abelian. Recall that the structure of abelian $\operatorname{Inn} Q$ is a frequently studied but nor very well understood problem, consisting mostly of nonexistence results. It can be deduced from [3, Remarks 5.3 and 5.5] that if Q is a p-loop (that is, $|Q|$ is a power of p, p a prime) and $\operatorname{Inn} Q$ is abelian then $\operatorname{Inn} Q$ is a p-group. By [11], $\operatorname{Inn} Q$ is cyclic if and only if Q is an abelian group. If Q is a p-loop with $\mathrm{cl}(Q) > 2$ then $\operatorname{Inn} Q$ is isomorphic neither to $\mathbb{Z}_p \times \mathbb{Z}_p$, by [4, Theorem 4.2], nor to $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$, by [2]. If Q is finite, $k \ge 2$, p is an odd prime [9] or an even prime [4, Theorem 4.1], then $\operatorname{Inn} Q$ is not isomorphic to $\mathbb{Z}_{p^k} \times \mathbb{Z}_p$. On the positive side, taking the examples of [5] and of this paper into account, we now know that $\operatorname{Inn} Q$ can be isomorphic to $(\mathbb{Z}_2)^6$ or to $(\mathbb{Z}_4)^2 \times (\mathbb{Z}_2)^2$ when Q is a 2-loop with $\mathrm{cl}(Q) > 2$.

2. The original setup and the new setup

As in [5], let G be a group and

$$(A_0) \qquad Z \leq R \leq N \trianglelefteq G,\ Z \leq Z(G),\ R \trianglelefteq G,\ G' \leq N,\ N/R \leq Z(G/R).$$

Let $\mu : G/R \times G/R \to Z$ be a mapping satisfying $\mu(1,x) = \mu(x,1) = 1$ for every $x \in G$, where we write $\mu(x,y)$ instead of the formally correct $\mu(xR, yR)$. Define $\delta : G/R \times G/R \to Z$ by

$$(A_1) \qquad \delta(x,y) = \mu(x,y)\mu(y,x)^{-1}.$$

Furthermore, consider the conditions

$$(A_2) \qquad \mu(xy,z) = \mu(x,z)\mu(y,z) \text{ whenever } \{x,y,z\} \cap N \neq \emptyset,$$

$$(A_3) \qquad \mu(x,yz) = \mu(x,y)\mu(x,z) \text{ whenever } \{x,y,z\} \cap N \neq \emptyset,$$

$$(A_4) \qquad z^{yx}\delta([z,y],x) = z^{xy}\delta([z,x],y) \text{ for every } x,\ y,\ z \in G.$$

The *original setup* consists of G, Z, R, N, μ and δ as above, satisfying (A_0)–(A_4).

Remark 2.1. *Note that we have also assumed $N' = 1$ as part of (A_0) in* [5]. *This is because we reconstructed the first example of Csörgő by means of nuclear extensions, cf.* [5, Section 2], *which we understood only with the added assumption that the normal nuclear subgroup is abelian. But the assumption $N' = 1$ is never used in §§4–7 of* [5]. *In particular, it is not used in any of the results of* [5] *that we need here.*

From the original setup we can define a loop $G[\mu]$ on G by

$$x * y = xy\mu(x,y),$$

and we obtain:

Proposition 2.2 ([5])**.** *Let $Q = G[\mu]$ be the loop obtained from an original setup. Then* $\mathrm{cl}(G) \leq 3$, $\mathrm{cl}(Q) \leq 3$ *and* $\mathrm{Inn}\, Q$ *is an abelian group. Moreover,* $\mathrm{cl}(Q) = 3$ *if and only if*

$$(2.1) \qquad \delta([x,y],z)\delta([y,z],x)\delta([z,x],y) \neq 1 \text{ for some } x,\ y,\ z \in G.$$

The condition (2.1) can be satisfied even if $\mathrm{cl}(G) = 2$, and we managed to obtain in [5] many examples of loops Q of order 128 with $\mathrm{cl}(Q) = 3$ and $\mathrm{cl}(\mathrm{Inn}\, Q) = 1$ from groups of nilpotency class two.

Unlike the original setup, the new setup will be based only on the groups G, $Z \leq Z(G)$, and the mapping δ.

Let G be a group and

$$(B_0) \qquad Z \leq Z(G).$$

Assume that $\delta : G/Z \times G/Z \to Z$ satisfies

$$(B_1) \qquad \delta(x,x) = 1 \text{ for every } x \in G,$$

$$(B_2) \qquad \delta(x,y) = \delta(y,x)^{-1} \text{ for every } x,\ y \in G,$$

$$(B_3) \qquad \delta(xy,z) = \delta(x,z)\delta(y,z) \text{ whenever } \{x,\ y,\ z\} \cap G' \neq \emptyset,$$

$$(B_4) \qquad z^{yx}\delta([z,y],x) = z^{xy}\delta([z,x],y) \text{ for every } x,\ y,\ z \in G.$$

The *new setup* consists of G, Z and δ as above, satisfying the conditions (B_0)–(B_4).

Proposition 2.3. *Every original setup gives rise to a new setup.*

Proof. Let G, Z, R, N, μ and δ be as in the original setup. We certainly have (B_0). The mapping δ is defined modulo R and hence modulo $Z \le R$. Conditions (B_1) and (B_2) follow from (A_1). If $\{x, y, z\} \cap G' \neq \emptyset$, we have $\{x, y, z\} \cap N \neq \emptyset$, and so $\delta(xy, z) = \mu(xy, z)\mu(z, xy)^{-1} = \mu(x, z)\mu(y, z)\mu(z, x)^{-1}\mu(z, y)^{-1} = \delta(x, z)\delta(y, z)$, by (A_2) and (A_3). Finally, the conditions (A_4) and (B_4) are identical. □

To show that every new setup gives rise to an original setup, we must find suitable subgroups R and N and a suitable mapping μ. This is accomplished in the next three sections, culminating in Proposition 5.5.

3. The radical and the multiplicative part

3.1. **The radical.** Let $(G, \cdot, 1)$ be a group and $(H, \cdot, 1)$ an abelian group. Let us define the radical $\operatorname{Rad}\varphi$ for a general mapping $\varphi : G^2 \to H$ satisfying

$$\varphi(1, x) = \varphi(x, 1) = 1 \text{ for every } x \in G. \tag{3.1}$$

Let

$$\operatorname{Rad}_2 \varphi = \{t \in G;\ \varphi(t, x) = \varphi(x, t) = 1 \text{ for all } x \in G\},$$
$$\operatorname{Rad}_1 \varphi = \{t \in G;\ \varphi(tx, y) = \varphi(xt, y) = \varphi(x, ty) = \varphi(x, yt) = \varphi(x, y) \text{ for all } x,\ y \in G\}.$$

It turns out (cf. Lemma 3.1(ii)) that $\operatorname{Rad}_1 \varphi$ is a subgroup of G. We can therefore define

$$\operatorname{Rad}\varphi = \operatorname{core}_G(\operatorname{Rad}_1 \varphi),$$

where $\operatorname{core}_G A$ is the largest normal subgroup of G contained in A, that is,

$$\operatorname{core}_G A = \bigcap_{g \in G} A^g = \{t \in G;\ t^g \in A \text{ for every } g \in G\}.$$

Call a mapping $\varphi : G^m \to H$ *multiplicative* if for every $1 \le i \le m$ and for every $x_1, \ldots, x_m \in G$ the induced mapping $\varphi(x_1, \ldots, x_{i-1}, -, x_{i+1}, \ldots, x_m) : G \to H$ is a homomorphism. A mapping $\varphi : G^m \to H$ is *symmetric* if

$$\varphi(x_1, \ldots, x_m) = \varphi(x_{\sigma(1)}, \ldots, x_{\sigma(m)}),$$

and *alternating* if

$$\varphi(x_1, \ldots, x_m) = \varphi(x_{\sigma(1)}, \ldots, x_{\sigma(m)})^{\operatorname{sgn}(\sigma)},$$

for every $x_1, \ldots, x_m \in G$ and every permutation σ of $\{1, \ldots, m\}$.

Lemma 3.1. *Let G be a group, H an abelian group, and $\varphi : G^2 \to H$ a mapping satisfying* (3.1)*. Then*

(i) $\operatorname{Rad}_1 \varphi \subseteq \operatorname{Rad}_2 \varphi$,
(ii) $\operatorname{Rad}_1 \varphi \le G$, $\operatorname{Rad}\varphi = \{t \in G;\ t^z \in \operatorname{Rad}_1 \varphi$ *for every* $z \in G\} \trianglelefteq G$,
(iii) *if φ is multiplicative then* $G' \le \operatorname{Rad}\varphi = \operatorname{Rad}_1 \varphi = \operatorname{Rad}_2 \varphi$.

Proof. Assume that $t \in \operatorname{Rad}_1 \varphi$. Then $\varphi(t, x) = \varphi(t \cdot 1, x) = \varphi(1, x) = 1$ for every $x \in G$, and, similarly, $\varphi(x, t) = 1$. Hence $t \in \operatorname{Rad}_2 \varphi$.

To establish (ii), assume that t, $s \in \operatorname{Rad}_1 \varphi$. Then $\varphi(tsx, y) = \varphi(sx, y) = \varphi(x, y)$, and similarly for all other defining conditions of $\operatorname{Rad}_1 \varphi$, so $ts \in \operatorname{Rad}_1 \varphi$. We have $\varphi(t^{-1}x, y) = \varphi(tt^{-1}x, y) = \varphi(x, y)$, where the first equality follows from $t \in \operatorname{Rad}_1 \varphi$. Hence $t^{-1} \in \operatorname{Rad}_1 \varphi$. The rest of (ii) is clear.

Assume that φ is multiplicative and let $t \in \operatorname{Rad}_2 \varphi$. Then $\varphi(tx, y) = \varphi(t, y)\varphi(x, y) = \varphi(x, y)$, and similarly for the other defining conditions of $\operatorname{Rad}_1 \varphi$, so $\operatorname{Rad}_1 \varphi = \operatorname{Rad}_2 \varphi$.

To show that $\operatorname{Rad}\varphi = \operatorname{Rad}_1\varphi$, it therefore suffices to prove that $\operatorname{Rad}_2\varphi \trianglelefteq G$. But for $t \in \operatorname{Rad}_2\varphi$ and x, $z \in G$, we have

$$\begin{aligned}\varphi(t^z, x) = \varphi(z^{-1}, x)\varphi(t, x)\varphi(z, x) &= \varphi(z^{-1}, x)\varphi(z, x)\varphi(t, x)\\ &= \varphi(z^{-1}z, x)\varphi(t, x) = \varphi(1, x)\varphi(t, x) = \varphi(t, x) = 1.\end{aligned}$$

A similar argument shows $\varphi(x, t^z) = 1$, hence $\operatorname{Rad}\varphi = \operatorname{Rad}_1\varphi = \operatorname{Rad}_2\varphi$. Now, $\varphi([x, y], z) = \varphi(x^{-1}, z)\varphi(y^{-1}, z)\varphi(x, z)\varphi(y, z) = 1$, so $G' \le \operatorname{Rad}\varphi$. □

We remark that it is not difficult to construct $\varphi : G^2 \to H$ such that $\operatorname{Rad}_2\varphi$ is not a subgroup of G, or such that $\operatorname{Rad}_1\varphi$ is not a normal subgroup of G. It is therefore necessary to transition from $\operatorname{Rad}_1\varphi$ to its core $\operatorname{Rad}\varphi$ if we wish to consider the mapping φ modulo its radical.

More precisely, $\varphi : G^2 \to H$ satisfying (3.1) induces a mapping $\varphi : (G/\operatorname{Rad}\varphi)^2 \to H$ with trivial radical, and we will often identity this induced mapping with φ.

Since we will also need the radical for multiplicative mappings $\varphi : G^3 \to H$, we set

$$\operatorname{Rad}\varphi = \{t \in G;\ \varphi(t, x, y) = \varphi(x, t, y) = \varphi(x, y, t) = 1 \text{ for every } x,\ y \in G\} \tag{3.2}$$

in such a case. It is then easy to see that $G' \le \operatorname{Rad}\varphi \trianglelefteq G$ and that φ is well-defined modulo $\operatorname{Rad}\varphi$ once again.

3.2. **The multiplicative part.** For a group G, an abelian group H and a mapping $\varphi : G^2 \to H$ satisfying (3.1) define the *multiplicative part* $\operatorname{Mul}\varphi$ of φ by

$$\begin{aligned}\operatorname{Mul}\varphi = \{t \in G;\ &\varphi(tx, y) = \varphi(t, y)\varphi(x, y) = \varphi(xt, y),\\ &\varphi(x, ty) = \varphi(x, t)\varphi(x, y) = \varphi(x, yt),\\ &\varphi(xy, t) = \varphi(x, t)\varphi(y, t),\\ &\varphi(t, xy) = \varphi(t, x)\varphi(t, y) \text{ for every } x,\ y \in G\}.\end{aligned}$$

Lemma 3.2. *Let G be a group, H an abelian group, and $\varphi : G^2 \to H$ a mapping satisfying* (3.1). *Then*

(i) $\operatorname{Mul}\varphi \le G$,
(ii) $\operatorname{Rad}\varphi \le \operatorname{Rad}_1\varphi \le \operatorname{Mul}\varphi$,
(iii) *if φ is multiplicative then* $\operatorname{Mul}\varphi = G$.

Proof. To show (i), assume that t, $s \in \operatorname{Mul}\varphi$. Then $\varphi(tsx, y) = \varphi(t, y)\varphi(sx, y) = \varphi(t, y)\varphi(s, y)\varphi(x, y) = \varphi(ts, y)\varphi(x, y)$, and the conditions $\varphi(ts, y)\varphi(x, y) = \varphi(xts, y)$, $\varphi(x, tsy) = \varphi(x, ts)\varphi(x, y)\varphi(x, yts)$ are established similarly. We also have $\varphi(xy, ts) = \varphi(xy, t)\varphi(xy, s) = \varphi(x, t)\varphi(y, t)\varphi(x, s)\varphi(y, s) = \varphi(x, ts)\varphi(y, ts)$, hence $ts \in \operatorname{Mul}\varphi$. Now, $\varphi(t^{-1}, y)\varphi(tx, y) = \varphi(t^{-1}, y)\varphi(t, y)\varphi(x, y) = \varphi(t^{-1}t, y)\varphi(x, y) = \varphi(1, y)\varphi(x, y) = \varphi(x, y) = \varphi(t^{-1}tx, y)$ for every x, $y \in G$, and hence $\varphi(t^{-1}x, y) = \varphi(t^{-1}, y)\varphi(x, y)$ for every x, $y \in G$. The rest of (i) is similar.

To prove (ii), let $t \in \operatorname{Rad}_1\varphi$. Then $t \in \operatorname{Rad}_2\varphi$ by Lemma 3.1, and so $\varphi(tx, y) = \varphi(x, y) = \varphi(t, y)\varphi(x, y)$ for every x, $y \in G$. The conditions $\varphi(xt, y) = \varphi(t, y)\varphi(x, y)$ and $\varphi(x, ty) = \varphi(x, t)\varphi(x, y) = \varphi(x, yt)$ follow by a similar argument. The final two conditions $\varphi(xy, t) = \varphi(x, t)\varphi(y, t)$, $\varphi(t, xy) = \varphi(t, x)\varphi(t, y)$ hold trivially, as $t \in \operatorname{Rad}_2\varphi$.

Part (iii) is obvious. □

Lemma 3.3. *Let G be a group, H an abelian group, and $\varphi : G^2 \to H$ a mapping satisfying* (3.1). *Assume that $G' \le \operatorname{Mul}\varphi$. Then*

(i) $\operatorname{Mul}\varphi \trianglelefteq G$,
(ii) $\operatorname{Mul}\varphi/\operatorname{Rad}\varphi \le Z(G/\operatorname{Rad}\varphi)$.

Proof. Let $t \in \operatorname{Mul}\varphi$, $z \in G$. For (i), we want to show that $t^z \in \operatorname{Mul}\varphi$. We have, $\varphi(t^z x, y) = \varphi([z,t^{-1}]tx, y) = \varphi([z,t^{-1}], y)\varphi(t,y)\varphi(x,y) = \varphi([z,t^{-1}]t, y)\varphi(x,y) = \varphi(t^z, y)\varphi(x,y)$. The remaining defining conditions of $\operatorname{Mul}\varphi$ are verified analogously.

To prove (ii) it suffices to show that $[m,u] \in \operatorname{Rad}\varphi$ for every $m \in \operatorname{Mul}\varphi$, $u \in G$. By Lemma 3.1, it suffices to show that $[m,u]^z \in \operatorname{Rad}_1\varphi$. We prove $\varphi([m,u]^z x, y) = \varphi(x,y)$, and leave the rest to the reader. First, $\varphi([m,u]^z x, y) = \varphi([m^z, u^z]x, y) = \varphi([m^z,u^z], y)\varphi(x,y)$. Second, for every $t \in \operatorname{Mul}\varphi$ we have $\varphi(t,y)\varphi(x,y) = \varphi(tx,y) = \varphi(xt^x, y) = \varphi(x,y)\varphi(t^x,y)$ by (i), and so $\varphi(t^x,y) = \varphi(t,y)$, $\varphi([t,x],y) = \varphi(t^{-1}t^x, y) = \varphi(t^{-1},y)\varphi(t^x,y) = \varphi(t^{-1},y)\varphi(t,y) = \varphi(t^{-1}t,y) = 1$. Finally, as $m^z = t \in \operatorname{Mul}\varphi$, we get $\varphi([m^z,u^z],y) = 1$. □

4. Three multiplicative mappings

Suppose that G, Z and δ form a new setup. Since δ is defined modulo $Z \trianglelefteq G$, we see that $Z \le \operatorname{Rad}\delta$ when δ is considered as a mapping $G \times G \to Z$. The conditions (B_2), (B_3) imply that $G' \le \operatorname{Mul}\delta$. We will use these properties of $\operatorname{Rad}\delta$ and $\operatorname{Mul}\delta$ throughout.

Define f, g, $h : G^3 \to Z$ by

$$\begin{aligned} f(x,y,z) &= \delta([x,y],z), \\ g(x,y,z) &= f(x,y,z)f(y,z,x)f(z,x,y), \\ h(x,y,z) &= [x,[y,z]], \end{aligned} \tag{4.1}$$

where x, y, $z \in G$. (See Lemma 4.1(iv) for $\operatorname{Im} h \le Z$.) These three mappings and their radicals play a crucial role in the analysis of the new setup. Note that all three mappings are well-defined modulo $\operatorname{Rad}\delta$.

Lemma 4.1. *In the new setup G, Z, δ the following conditions are satisfied:*

(i) $z^{-xy}z^{yx} = [z,[y^{-1},x^{-1}]]$, $[G,G'] \le Z$, $\operatorname{cl}(G/Z) \le 2$, $\operatorname{cl}(G) \le 3$, *and* $f(z,x,y) = h(z,y,x)f(z,y,x)$,

(ii) f *is multiplicative,* $\operatorname{Mul}\delta \le \operatorname{Rad} f$, *and* $f(x,y,z) = f(y,x,z)^{-1}$,

(iii) g *is multiplicative,* $\operatorname{Rad} f \le \operatorname{Rad} g$, *and* $g(x,y,z) = g(y,z,x) = g(y,x,z)^{-1}$,

(iv) h *is multiplicative,* $\operatorname{Im} h \le Z$, $\operatorname{Rad} f \le \operatorname{Rad} h$, *and* $h(x,y,z) = h(x,z,y)^{-1}$,

(v) $G/\operatorname{Rad} g$ *is an elementary abelian* 2*-group, and the mapping* $g : G^3 \to Z$ *induces a trilinear alternating mapping* $(G/\operatorname{Rad} g)^3 \to \{a \in Z;\ a^2 = 1\}$.

Proof. (i) By (B_4), $z^{-xy}z^{yx} = f(z,x,y)f(z,y,x)^{-1} \in Z \le Z(G)$. Since $z^{-xy}z^{yx} = [z,[y^{-1},x^{-1}]]^{xy}$ holds in any group, we have $[z,[y^{-1},x^{-1}]] = f(z,x,y)f(z,y,x)^{-1} \in Z \le Z(G)$. Thus $[G,G'] \le Z$, $\operatorname{cl}(G/Z) \le 2$, and $\operatorname{cl}(G) \le 3$. In any group of nilpotency class three we have $[z,[y^{-1},x^{-1}]] = [z,[y,x]]$, so $h(z,y,x) = [z,[y,x]] = [z,[y^{-1},x^{-1}]] = f(z,x,y)f(z,y,x)^{-1}$.

(ii) f is well-defined modulo $\operatorname{Rad}\delta$ and $\operatorname{cl}(G/\operatorname{Rad}\delta) \le 2$ by (i). Since $[xy,z] = [x,z][y,z]$ in any group of nilpotency class 2, we have $f(xy,z,w) = \delta([xy,z],w) = \delta([x,z][y,z],w) = \delta([x,z],w)\delta([y,z],w) = f(x,z,w)f(y,z,w)$. Note that $f(x,yz,w) = f(x,y,w)f(x,z,w)$ follows similarly. Finally, using $G' \le \operatorname{Mul}\delta$, we have $f(x,y,zw) = \delta([x,y],zw) = \delta([x,y],z)\delta([x,y],w) = f(x,y,z)f(x,y,w)$.

We have shown that f is multiplicative, so $\operatorname{Rad} f$ is defined by (3.2). Let $t \in \operatorname{Mul}\delta$. Then

$$f(x,y,t) = \delta([x,y],t) = \delta(x^{-1},t)\delta(y^{-1},t)\delta(x,t)\delta(y,t) = \delta(x^{-1},t)\delta(x,t)\delta(y^{-1},t)\delta(y,t) = \delta(x^{-1}x,t)\delta(y^{-1}y,t) = 1.$$

Moreover, by Lemma 3.3(ii), $[t,x]\in\operatorname{Rad}\delta$, and we have $f(t,x,y)=\delta([t,x],y)=1$. The equality $f(x,t,y)=1$ follows similarly. Thus $\operatorname{Mul}\delta\le\operatorname{Rad}f$.

Finally, by multiplicativity of f and by $\delta([x,x],y)=1$, we have $1=f(xy,xy,z)=f(x,y,z)f(y,x,z)$.

(iii) The mapping g is multiplicative since f is, and it is clearly invariant under a cyclic shift of its arguments. If $t\in\operatorname{Rad}f$, we have $g(t,x,y)=f(t,x,y)f(x,y,t)f(y,t,x)=1$ for every x, $y\in G$, so $t\in\operatorname{Rad}g$. By (ii), $g(x,y,z)=f(x,y,z)f(y,z,x)f(z,x,y)=f(y,x,z)^{-1}f(z,y,x)^{-1}f(x,z,y)^{-1}=(f(y,x,z)f(x,z,y)f(z,y,x))^{-1}=g(y,x,z)^{-1}$.

(iv) By (i) and (ii), h is multiplicative and $\operatorname{Im}h\le Z$. Assume that $t\in\operatorname{Rad}f$. Then $h(t,x,y)=f(t,y,x)f(t,x,y)^{-1}=1$ and, similarly, $h(x,t,y)=h(x,y,t)=1$, so $t\in\operatorname{Rad}h$. Since $1=[y,[x,x]]=h(y,x,x)$, we have $h(x,y,z)=h(x,z,y)^{-1}$ by multiplicativity.

(v) Let us first show that $g(x,y,z)^2=1$ for every x, y, $z\in G$. In view of (iii), this is equivalent to $g(x,y,z)=g(y,x,z)$. Now,

$$\begin{aligned}g(y,x,z)&=f(y,x,z)f(x,z,y)f(z,y,x)\\&=f(y,z,x)[y,[z,x]]f(x,y,z)[x,[y,z]]f(z,x,y)[z,[x,y]]\\&=g(x,y,z)[x,[y,z]][y,[z,x]][z,[x,y]],\end{aligned}$$

by (iv). The Hall-Witt identity

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

valid in all groups yields $[x,[y,z]][y,[z,x]][z,[x,y]]=1$ in groups of nilpotency class 3, so we are done by (i).

The established identity $g(x,y,z)^2=1$ shows not only that the image of g is contained in the vector space $U=\{a\in Z;\ a^2=1\}$, but also that $G/\operatorname{Rad}g$ is of exponent two, since for every $x\in G$ we have $g(x^2,y,z)=g(x,y,z)^2=1$, by multiplicativity of g. □

5. Constructing loops of Csörgő type from the new setup

Proposition 5.1. *Suppose that G, Z, δ is a new setup. Set $R=\operatorname{Rad}\delta$ and $N=G'R$. Then δ is well-defined as a mapping $\delta: G/R\times G/R\to Z$, and (A_0) holds.*

Proof. By Lemma 3.1, $Z\le R\trianglelefteq G$ and δ is well defined modulo R. Obviously, $R\le N$, $G'\le N$, and $N\trianglelefteq G$. Since $[G,G']\le Z\le R$ by Lemma 4.1(i), we have $N/R=G'R/R\le Z(G/R)$. □

Suppose that G, Z, δ is a new setup, and let $R=\operatorname{Rad}\delta$, $N=G'R$, $\overline{G}=G/R$, $\overline{N}=N/R$. In view of Proposition 5.1, to obtain an original setup from G we only need to construct $\mu:\overline{G}\times\overline{G}\to Z$ so that (A_1)–(A_3) hold. We show how to construct all such mappings μ in principle (by rephrasing the problem in terms of compatible parameter sets below), and we construct one μ explicitly (see Lemma 5.2).

Let $T=\{t_1=1,\dots,t_n\}$ be a transversal to $\overline{N}$ in $\overline{G}$. We say that

$$\mathcal{P}=\{\psi_k;\ k\in\overline{N}\}\cup\{\varphi_i;\ 1\le i\le n\}\cup\{\tau_{ij};\ 1\le i\le j\le n\}\tag{5.1}$$

is a *compatible parameter set* if

- $\psi_k:\overline{G}\to Z$ is a homomorphism for every $k\in\overline{N}$,
- $\psi_{k'}(k)=\delta(k',k)\psi_k(k')$ for every k, $k'\in\overline{N}$,
- $\varphi_i:\overline{N}\to Z$ is a homomorphism for every $1\le i\le n$,
- $\psi_k(t_i)=\varphi_i(k)$ for every $k\in\overline{N}$ and $1\le i\le n$,
- $\tau_{ij}\in G$ for every $1\le i\le j\le n$, and $\tau_{1i}=1$ for every $1\le i\le n$.

Note that $\psi_k(1) = 1$, $\psi_1(k) = \delta(1,k)\psi_k(1) = 1$ and $\varphi_1(k) = \psi_k(1) = 1$ holds for every $k \in \overline{N}$ in a compatible parameter set.

Lemma 5.2. *In a new setup G, Z, δ, let $R = \operatorname{Rad}\delta$, $N = G'R$, $\overline{G} = G/R$, $\overline{N} = N/R$, and let $T = \{t_1 = 1, \dots, t_n\}$ be a transversal to $\overline{N}$ in $\overline{G}$. For every $k \in \overline{N}$, let $\psi_k = \delta(k,-)$. For every $1 \le i \le n$, let $\varphi_i = \delta(-,t_i)$. For every $1 \le i \le j \le n$, let $\tau_{ij} = \delta(t_i,t_j)$. Then $\mathcal{P}$ of (5.1) is a compatible parameter set.*

Proof. We have $G' \le \operatorname{Mul}\delta$, $R \le \operatorname{Mul}\delta$ by Lemma 3.2, and so $N \le \operatorname{Mul}\delta$. Then ψ_k and φ_i are homomorphisms. For k, $k' \in N$, the equality $\psi_{k'}(k) = \delta(k',k)\psi_k(k')$ is equivalent to $\delta(k,k') = 1$. Now, $\delta(N,N) = \delta(G'R,G'R) = \delta(G',G')$ and $\delta([x,y],G') = f(x,y,G') = 1$ by Lemma 4.1(ii). Finally, the equality $\psi_k(t_i) = \varphi_i(k)$ holds trivially. □

Given a compatible parameter set $\mathcal{P}$, define $\mu_{\mathcal{P}} = \mu : \overline{G} \times \overline{G} \to Z$ as follows:

$\mu(k,k') = \psi_k(k')$ for every k, $k' \in \overline{N}$,

$\mu(k,t_i) = \varphi_i(k)$ for every $k \in \overline{N}$, $1 \le i \le n$,

$\mu(t_i,k) = \delta(t_i,k)\mu(k,t_i)$ for every $k \in \overline{N}$, $1 \le i \le n$,

$\mu(t_i,t_j) = \tau_{ij}$ for every $1 \le i \le j \le n$,

$\mu(t_j,t_i) = \delta(t_j,t_i)\mu(t_i,t_j)$ for every $1 \le i \le j \le n$,

$\mu(kt,k't') = \mu(k,k')\mu(k,t')\mu(t,k')\mu(t,t')$ for every k, $k' \in \overline{N}$, t, $t' \in T$.

Observe that $\mu_{\mathcal{P}}$ is well-defined. (The first five lines do not lead to a contradiction: $\mu(k,1) = \psi_k(1) = 1$ according to the first line and $\mu(k,1) = \varphi_1(k) = 1$ according to the second line, $\mu(1,k) = \psi_1(k) = 1$ according to the first line and $\mu(1,k) = \delta(1,k)\mu(k,1) = 1$ according to the third line. We also have $\mu(1,t_i) = \varphi_i(1) = 1$ by the second line and $\mu(1,t_i) = \tau_{1i} = 1$ by the fourth line, $\mu(t_i,1) = \delta(t_i,1)\mu(1,t_i) = 1$ by the third line and $\mu(t_i,1) = \delta(t_i,1)\mu(1,t_i) = 1$ by the fifth line. Finally, $\mu(t_i,t_i) = \delta(t_i,t_i)\mu(t_i,t_i)$ in the fifth line is sound thanks to (B_1). Adding the sixth line also does not lead to a contradiction: $\mu(k1,k'1) = \mu(k,k')\mu(k,1)\mu(1,k')\mu(1,1) = \mu(k,k')$, $\mu(k1,1t_i) = \mu(k,1)\mu(k,t_i)\mu(1,1)\mu(1,t_i) = \mu(k,t_i)$, similarly for $\mu(t_i,k)$, and we have $\mu(1t_i,1t_j) = \mu(1,1)\mu(1,t_j)\mu(t_i,1)\mu(t_i,t_j) = \mu(t_i,t_j)$.)

Lemma 5.3. *Let G, Z, δ be a new setup, $R = \operatorname{Rad}\delta$, $N = G'R$, $\overline{G} = G/R$, $\overline{N} = N/R$, and let $\mathcal{P}$ be a compatible parameter set. Then $\mu = \mu_{\mathcal{P}}$ satisfies (A_1)–(A_3).*

Proof. It suffices to show (A_1) and (A_2), as (A_3) is a consequence: if $\{x,y,z\} \cap \overline{N} \ne \emptyset$, we have

$$\begin{aligned}\mu(x,yz) &= \delta(x,yz)\mu(yz,x) = \delta(yz,x)^{-1}\mu(yz,x)\\ &= \delta(y,x)^{-1}\delta(z,x)^{-1}\mu(y,x)\mu(z,x) = \delta(x,y)\mu(y,x)\delta(x,z)\mu(z,x) = \mu(x,y)\mu(x,z).\end{aligned}$$

Let us prove (A_1). We have $\mu(k,k') = \psi_k(k') = \delta(k,k')\psi_{k'}(k) = \delta(k,k')\mu(k',k)$. Since $\mu(t_i,k) = \delta(t_i,k)\mu(k,t_i)$ for every $k \in \overline{N}$ and $1 \le i \le n$, we have $\mu(k,t_i) = \delta(t_i,k)^{-1}\mu(t_i,k) = \delta(k,t_i)\mu(t_i,k)$, too. Also, $\mu(t_j,t_i) = \delta(t_j,t_i)\mu(t_i,t_j)$ for every $1 \le i \le j \le n$, which yields $\mu(t_i,t_j) = \delta(t_j,t_i)^{-1}\mu(t_j,t_i) = \delta(t_i,t_j)\mu(t_i,t_j)$, too. Using the already established equalities, we have $\mu(kt,k't') = \mu(k,k')\mu(k,t')\mu(t,k')\mu(t,t') = \delta(k,k')\mu(k',k)\delta(k,t')\mu(t',k)\delta(t,k')\mu(k',t)\delta(t,t')\mu(t',t) = \delta(kt,k't')\mu(k't',kt)$ for every k, $k' \in \overline{N}$, t, $t' \in T$, which is (A_1).

We split the proof of (A_2) into three cases, depending on which of the arguments x, y, z in (A_2) belongs to $\overline{N}$. In all situations, we will assume that k, k', $k'' \in \overline{N}$ and t, t', $t'' \in T$.

Case $x \in \overline{N}$. We have $\mu(kk't', k''t'') = \mu(kk', k'')\mu(kk', t'')\mu(t', k'')\mu(t', t'')$ and also $\mu(k, k''t'')\mu(k't', k''t'') = \mu(k, k'')\mu(k, t')\mu(k', k'')\mu(k', t'')\mu(t', k'')\mu(t', t'')$, so we need to check that $\mu(kk', t'') = \mu(k, t'')\mu(k', t'')$, or, with $t'' = t_i$, $\varphi_i(kk') = \varphi_i(k)\varphi_i(k')$, which is true.

Case $y \in \overline{N}$. Recall that $\overline{N} \le Z(\overline{G})$. Thus $\mu(ktk', k''t'') = \mu(kk't, k''t'')$, while $\mu(kt, k''t'')\mu(k', k''t'') = \mu(k', k''t'')\mu(kt, k''t'') = \mu(k'kt, k''t'') = \mu(kk't, k''t'')$ by the case $x \in \overline{N}$.

Case $z \in \overline{N}$. Using $\overline{N} \le Z(\overline{G})$ and the case $x \in \overline{G}$ once again, we have $\mu(ktk't', k'') = \mu(kk'tt', k'') = \mu(kk', k'')\mu(tt', k'') = \mu(k, k'')\mu(k', k'')\mu(tt', k'')$, $\mu(kt, k'')\mu(k't', k'') = \mu(k, k'')\mu(t, k'')\mu(k', k'')\mu(t', k'')$, so we need to check that $\mu(tt', k'') = \mu(t, k'')\mu(t', k'')$. By (A_1) this is equivalent to $\delta(tt', k'')\mu(k'', tt') = \delta(t, k'')\mu(k'', t)\delta(t', k'')\mu(k'', t')$, or $\mu(k'', tt') = \mu(k'', t)\mu(k'', t')$, or $\psi_{k''}(tt') = \psi_{k''}(t)\psi_{k''}(t')$, which is true. □

The converse of Lemma 5.3 is also true:

Lemma 5.4. *Let G, Z, δ be a new setup, $R = \operatorname{Rad}\delta$, $N = G'R$, $\overline{G} = G/R$, $\overline{N} = N/R$. Suppose that $\mu : \overline{G} \times \overline{G} \to Z$ satisfies (A_1)–(A_3). Then there exists a compatible parameter set $\mathcal{P}$ such that $\mu = \mu_{\mathcal{P}}$.*

Proof. For every $k \in \overline{N}$, let $\psi_k = \mu(k, -) : \overline{G} \to Z$. By (A_3), ψ_k is a homomorphism. Moreover, $\psi_{k'}(k) = \mu(k', k) = \delta(k', k)\mu(k, k') = \delta(k', k)\psi_k(k')$ by (A_1). For every $1 \le i \le n$, let φ_i be the restriction of $\mu(-, t_i)$ to $\overline{N}$. By (A_2), φ_i is a homomorphism. Moreover, $\psi_k(t_i) = \mu(k, t_i) = \varphi_i(k)$ for every $k \in \overline{N}$, $1 \le i \le n$. Finally, for $1 \le i \le j \le n$, let $\tau_{ij} = \mu(t_i, t_j)$. Then $\mathcal{P} = \{\psi_k;\ k \in \overline{N}\} \cup \{\varphi_i;\ 1 \le i \le n\} \cup \{t_{ij};\ 1 \le i \le j \le n\}$ is a compatible parameter set, and we can use it to obtain $\nu = \mu_{\mathcal{P}} : \overline{G} \times \overline{G} \to Z$. It remains to show that $\nu = \mu$.

We have $\nu(k, k') = \psi_k(k') = \mu(k, k')$ for every k, $k' \in \overline{N}$; $\nu(k, t_i) = \varphi_i(k) = \mu(k, t_i)$ for every $k \in \overline{N}$, $1 \le i \le n$; $\nu(t_i, k) = \delta(t_i, k)\nu(k, t_i) = \delta(t_i, k)\mu(k, t_i) = \mu(t_i, k)$ for every $k \in \overline{N}$, $1 \le i \le n$, by (A_1); $\nu(t_i, t_j) = \tau_{ij} = \mu(t_i, t_j)$ for every $1 \le i \le j \le n$; $\nu(t_j, t_i) = \delta(t_j, t_i)\nu(t_i, t_j) = \delta(t_j, t_i)\mu(t_i, t_j) = \mu(t_j, t_i)$ for every $1 \le i \le j \le n$, by (A_1); and, finally, $\nu(kt, k't') = \nu(k, k')\nu(k, t')\nu(t, k')\nu(t, t') = \mu(k, k')\mu(k, t')\mu(t, k')\mu(t, t') = \mu(kt, k't')$, by (A_2) and (A_3). □

Summarizing:

Proposition 5.5. *Assume that G, Z, δ form a new setup, and let $R = \operatorname{Rad}\delta$, $N = G'R$. Let $\mu : G/R \times G/R \to Z$ be a mapping satisfying (A_1)–(A_3), which is guaranteed to exist. Then G, Z, R, N, μ, δ form an original setup.*

In particular, with $Q = G[\mu]$, we have $\operatorname{cl}(G) \le 3$, $\operatorname{cl}(Q) \le 3$, and $\operatorname{cl}(\operatorname{Inn} Q) = 1$. Moreover, $\operatorname{cl}(Q) = 3$ if and only if (2.1) is satisfied.

Proof. By Proposition 2.3, (A_0) holds. With the compatible parameter set $\mathcal{P}$ of Lemma 5.2, the mapping $\mu = \mu_{\mathcal{P}}$ satisfies (A_1)–(A_3), by Lemma 5.3. Hence G, Z, R, N, μ, δ form an original setup. Then $\operatorname{cl}(G)$, $\operatorname{cl}(Q)$ and $\operatorname{cl}(\operatorname{Inn} Q)$ depend only on δ, and are as in Proposition 2.2. □

6. Structural properties of minimal setups

A new setup G, Z, δ with g as in (4.1) is said to be *nontrivial* if $g \ne 1$. By Proposition 5.5, the associated loop $Q = G[\mu]$ satisfies $\operatorname{cl}(Q) = 3$ if and only if the setup is nontrivial. A nontrivial setup is said to be *minimal* if $|G|$ is as small as possible.

In [5], the original setup yielded many loops Q of order 128 with $\operatorname{Inn} Q$ abelian and $\operatorname{cl}(Q) = 3$. Hence we can assume $|G| \le 128$ in a minimal setup.

In this section we show that $|G|$ is even in any nontrivial setup, that $|G| = 128$ in a minimal setup, and obtain many structural results that allow us to describe all minimal setups in the next section.

The investigation will be guided by the already established inclusions

$$G \geq \operatorname{Rad} g \geq \operatorname{Rad} f \geq \operatorname{Mul} \delta \geq \operatorname{Rad} \delta \geq Z \tag{6.1}$$

valid in any new setup, cf. Lemmas 3.2, 4.1. It is natural to work with $\operatorname{Mul}\delta$ rather than $N = G' \operatorname{Rad}\delta \leq \operatorname{Mul}\delta$ here.

Lemma 6.1. *In a minimal setup G, Z, δ the group Z is cyclic of even order, and $g : (G/\operatorname{Rad} g)^3 \to \{a \in Z;\ a^2 = 1\}$ is a nontrivial trilinear alternating form.*

Proof. Assume that G, Z, δ is a minimal setup and Z is not cyclic. Then $Z = Z_1 \times \cdots \times Z_k$ for some cyclic groups Z_i and $k \geq 2$. Let $\pi_i : Z \to Z_i$ be the canonical projections. Since $g : G^3 \to Z$ satisfies $g \neq 1$, there is j such that $\pi_j g : G^3 \to Z_j$ satisfies $\pi_j g \neq 1$.

Let $Y = \prod_{i \neq j} Z_i$, $\overline{G} = G/Y$, $\overline{Z} = Z/Y \cong Z_j$, and define $\overline{\delta} : \overline{G}^2 \to \overline{Z}$ by $\overline{\delta}(xY, yY) = \pi_j \delta(x, y)$. Then $\overline{G}$, $\overline{Z}$, $\overline{\delta}$ is a new setup. Let $\overline{g}$ be associated with $\overline{\delta}$ in a way analogous to (4.1). Then $\overline{g} = \pi_j g \neq 1$, a contradiction with the minimality of $|G|$.

Thus Z is cyclic. Assume that it is of odd order. Then $U = \{a \in Z;\ a^2 = 1\} = 1$ and the setup is trivial by Lemma 4.1(v), a contradiction.

Since $U = \{a \in Z;\ a^2 = 1\} \cong \mathbb{Z}_2$, we can view $G/\operatorname{Rad} g$ as a vector space over the two-element field and identify g with a nontrivial trilinear alternating form, by Lemma 4.1(v). □

Lemma 6.2. *In a minimal setup, if x, y, $z \in G$ are such that $g(x, y, z) \neq 1$ then $G = \langle x, y, z \rangle Z$.*

Proof. Let $L = \langle x, y, z \rangle Z$. Since $Z \leq Z(G)$, $Z \leq L$ and $L \cap Z(G) \leq Z(L)$, we have $Z \leq Z(L)$. Restrict δ to $L \times L$. Then L, Z, δ is a new setup (i.e., the conditions (B_1)–(B_4) hold with L in place of G) and since x, y, $z \in L$, this setup is nontrivial. □

Lemma 6.3. *In a minimal setup, let L be a subgroup satisfying $Z \leq L \trianglelefteq G$. Then G/L is generated by at most 3 elements. In particular, $G/\operatorname{Rad} g$ is an elementary abelian group of order 8.*

Proof. We know that $G/\operatorname{Rad} g$ is an elementary abelian 2-group by Lemma 4.1(v) and we must have $\dim(G/\operatorname{Rad} g) \geq 3$ to ensure $g \neq 1$. The rest follows from Lemma 6.2. □

Lemma 6.4. *In a nontrivial setup, $|\operatorname{Mul}\delta/\operatorname{Rad}\delta|$ is even and $|G|$ is even. Moreover, if $\operatorname{Mul}\delta/\operatorname{Rad}\delta$ is an elementary abelian 2-group then $G/\operatorname{Rad} f$ is an elementary abelian 2-group, too.*

Proof. Suppose first that $\operatorname{Mul}\delta/\operatorname{Rad}\delta$ is of odd order k and choose x, y, $z \in G$ with $g(x, y, z) \neq 1$. Then $g(x, y, z) = g(x^k, y^k, z^k)$ by Lemma 4.1(iii), (v). On the other hand, $[x^k, y^k](\operatorname{Rad}\delta) = ([x, y]^{k^2})\operatorname{Rad}\delta = \operatorname{Rad}\delta$, since $G' \leq \operatorname{Mul}\delta$ and $\operatorname{cl}(G/\operatorname{Rad}\delta) \leq 2$. Then $f(x^k, y^k, z^k) = \delta([x^k, y^k], z^k) = 1$, thus $g(x^k, y^k, z^k) = 1$, a contradiction.

Now suppose that $\operatorname{Mul}\delta/\operatorname{Rad}\delta$ is an elementary abelian 2-group. Then for every x, y, $z \in G$ we have $f(x^2, y, z) = \delta([x^2, y], z) = \delta([x, y]^2, z) = 1$, and similarly $f(x, y^2, z) = 1$. This implies $f(x, y, z^2) = g(x, y, z^2) = 1$ by Lemma 4.1(v). □

Lemma 6.5. *In a minimal setup, $\operatorname{Rad} f = \operatorname{Rad} g$ and $\operatorname{Im} f \setminus \{1\}$ consists of the unique involution of Z.*

Proof. Suppose first that $G/\operatorname{Rad} f$ is not an elementary abelian 2-group. If $|Z| = 2$ then $f(x^2, y, z) = f(x, y, z)^2 = 1$ by Lemma 4.1, a contradiction. Thus $|Z| \geq 4$ by Lemma 6.1. By Lemma 6.4 we have $|\operatorname{Mul}\delta/\operatorname{Rad}\delta| \geq 4$. By Lemma 4.1(v), $G/\operatorname{Rad} g$ is elementary abelian, and thus $|\operatorname{Rad} g/\operatorname{Rad} f| \geq 2$. Since $|G/\operatorname{Rad} g| = 8$ by Lemma 6.3, we have $|G| > 128$, and so the setup is not minimal.

Now suppose that $G/\operatorname{Rad} f$ is elementary abelian. Then $\dim(G/\operatorname{Rad} f) \leq 3$ by Lemma 6.3 and $\operatorname{Rad} g = \operatorname{Rad} f$ follows. Also, $1 = f(x^2, y, z) = f(x, y, z)^2$, so every nontrivial value of f is an involution in Z, and this involution is unique by Lemma 6.1. □

We have shown that in a minimal setup we must have $|G/\operatorname{Rad} g| = 8$, $|\operatorname{Mul}\delta/\operatorname{Rad}\delta| \geq 2$ even, and $|Z| \geq 2$ even. We proceed in two directions, depending on whether $Z(G/\operatorname{Rad}\delta)$ is a subgroup of $\operatorname{Rad} f/\operatorname{Rad}\delta$ or not.

6.1. $Z(G/\operatorname{Rad}\delta)$ is a subgroup of $\operatorname{Rad} f/\operatorname{Rad}\delta$.

Lemma 6.6. *Let H be a 2-group of order ≥ 16, and $H/Z(H)$ an elementary abelian 2-group of order 8. Then H' is an elementary abelian subgroup of $Z(H)$ and is of order ≥ 4. If $|H'| = 4$, then there exist u, v, $w \in H$ that generate H modulo $Z(H)$ and satisfy $ab = c$, $1 \notin \{a, b, c\}$, where $a = [u, v]$, $b = [v, w]$ and $c = [w, u]$.*

Proof. The mapping $[-,-]$ induces a nondegenerate alternating bilinear mapping of $H/Z(H)$ into $H' \leq Z(H)$. From $[x^2, y] = [x, y]^2 = 1$ we see that H' has to be elementary abelian. If $|H'| \leq 2$ then $[-,-] : (H/Z(H))^2 \to H'$ is an alternating bilinear form with trivial radical and $\dim(H/Z(H)) = 3$, which is impossible. Therefore $|H'| \geq 4$.

Assume that H' is the Klein group, and let $H/Z(H)$ be generated by x, y, z. Then H' is generated by $[x, y]$, $[y, z]$ and $[z, x]$. Note that at most one of $[x, y]$, $[y, z]$, $[z, x]$ is trivial, else the three elements do not generate H'. The three elements cannot all be the same for the same reason.

If all $[x, y]$, $[y, z]$, $[z, x]$ are nontrivial and distinct, we automatically have $[x, y][y, z] = [z, x]$ and are done. If all three are nontrivial and precisely two coincide, say $[x, y] = [y, z]$, then $[xz, y] = [x, y][z, y] = 1$ and $[y, z]$, $[z, xz] = [z, x]$ are two distinct nontrivial elements of H'. We can therefore assume that $[x, y] = 1$ and $[y, z]$, $[z, x]$ are two distinct nontrivial elements of H'. Then $u = zx$, $v = zy$, $w = z$ do the job, as $[u, v] = [zx, zy] = [z, y][x, z][x, y] = [z, y][x, z] = [zy, z][z, zx] = [v, w][w, u]$ is not equal to 1. □

Lemma 6.7 (Baer). *Let H be a group and $H/Z(H)$ an abelian group. For a prime p let $e(p)$ be the exponent of the p-primary component of $H/Z(H)$. Then $\mathbb{Z}_{e(p)} \times \mathbb{Z}_{e(p)} \leq H/Z(H)$.*

Proposition 6.8. *In a minimal setup, let $\overline{G} = G/\operatorname{Rad}\delta$ and assume that $Z(\overline{G}) \leq \operatorname{Rad} f/\operatorname{Rad}\delta$. Then $Z(\overline{G}) = \operatorname{Rad} f/\operatorname{Rad}\delta = \overline{G}'$ is elementary abelian of order 8 and $\operatorname{Rad} f = \operatorname{Mul}\delta$.*

Proof. Let $\overline{\operatorname{Rad} f} = \operatorname{Rad} f/\operatorname{Rad}\delta$ and $\overline{\operatorname{Mul}\delta} = \operatorname{Mul}\delta/\operatorname{Rad}\delta$. From $Z(\overline{G}) \leq \overline{\operatorname{Rad} f} < \overline{G}$ we see that $\overline{G}$ is not abelian. Hence $\operatorname{cl}(\overline{G}) = 2$ by Lemma 4.1(i), and we have $1 < \overline{G}' \leq Z(\overline{G}) < \overline{G}$.

Recall that we have $|G| \leq 128$, and thus $|\overline{G}| \leq 64$. By Lemma 6.4, $|\overline{\operatorname{Mul}\delta}| = 2k$ for some $k \geq 1$, so $|\overline{G}|$ is divisible by $16k$, which means that either $\overline{G}$ is a 2-group or $|\overline{G}| = 48 = 16 \cdot 3$. Since $\overline{G}$ is nilpotent, $\overline{G}'$ has to be a 2-group in any case.

We claim that if $\overline{G}'$ is elementary abelian then $\overline{G}/Z(\overline{G})$ is elementary abelian and $|\overline{G}'| \geq 4$. Indeed, we have $[x^2, y] = [x, y]^2 = 1$ so $\overline{G}/Z(\overline{G})$ is elementary abelian, its order cannot exceed 8 (by Lemma 6.3), hence it is equal to 8 (as $Z(\overline{G}) \le \overline{\operatorname{Rad} f}$), and so $|\overline{G}\,'| \ge 4$ follows by Lemma 6.6.

If $|\overline{G}\,'| = 2$, we have a contradiction with the claim. We can therefore assume that $|\overline{G}\,'| \ge 4$, and thus also $|Z(\overline{G})| \ge 4$.

Suppose for a while that $|Z(\overline{G})| = 4$ and $Z(\overline{G}) = \overline{\operatorname{Rad} f}$. Then $\overline{G}/Z(\overline{G}) \cong G/\operatorname{Rad} f$ is elementary abelian of order 8, and we are in the situation of Lemma 6.6 with $|\overline{G}\,'| = 4$. Let u, v, w be as in Lemma 6.6, so $[v,w] = [u,v][u,w]r$ for some $r \in \operatorname{Rad}\delta$. We have $g(u,v,w) \neq 1$, and we can assume, say, $f(v,w,u) \neq 1$. Now, $f(u,v,u) = h(u,v,u)$ and $f(u,w,u) = h(u,w,u)$. That means that $f(v,w,u) = \delta([v,w],u) = \delta([u,v][u,w]r,u) = \delta([u,v],u)\delta([u,w],u) = h(u,v,u)h(u,w,u) = [u,[v,u]][u,[w,u]] = [u,[v,w]] = h(u,v,w)$. However, that yields $g(u,v,w) = f(v,w,u)h(u,v,w) = 1$, a contradiction.

Now suppose that $|Z(\overline{G})| = 4$ and $Z(\overline{G}) < \overline{\operatorname{Rad} f}$. Then $|\overline{\operatorname{Rad} f}| = 8$ and $|\overline{G}/Z(\overline{G})| > 8$, so $\overline{G}/Z(\overline{G})$ cannot be elementary abelian by Lemma 6.3. But $\overline{G}/\overline{\operatorname{Rad} f}$ is elementary abelian, $|\overline{\operatorname{Rad} f}/Z(\overline{G})| = 2$, a contradiction with Lemma 6.7.

It remains to consider the situation $|\overline{G}\,'| \ge 4$, $|Z(\overline{G})| = 8$, $Z(\overline{G}) = \overline{\operatorname{Rad} f}$. Then $\overline{G}/Z(\overline{G}) \cong G/\operatorname{Rad} f$ is elementary abelian of order 8. If $|\overline{G}\,'| = 4$, we reach a contradiction by Lemma 6.6 as above. We therefore have $\overline{G}\,' = Z(\overline{G})$. Since $G' \le \operatorname{Mul}\delta$, we have $\overline{G}\,' \le \overline{\operatorname{Mul}\delta}$, and $\operatorname{Mul}\delta = \operatorname{Rad} f$ follows. As $\overline{G}/\overline{G}\,'$ is elementary abelian, we must have $1 = [x^2, y] = [x,y]^2$, which shows that $\overline{G}\,'$ itself is elementary abelian. □

6.2. $Z(G/\operatorname{Rad}\delta)$ is not a subgroup of $\operatorname{Rad} f/\operatorname{Rad}\delta$.

Proposition 6.9. *In a minimal setup, suppose that $Z(G/\operatorname{Rad}\delta)$ is not contained in $\operatorname{Rad} f/\operatorname{Rad}\delta$. Then $|\operatorname{Rad}\delta/Z| \ge 4$. Moreover, if $|\operatorname{Rad}\delta/Z| = 4$ then $\operatorname{Rad}\delta/Z$ is the Klein group.*

Proof. We will use Lemma 4.1 freely in this proof. Let $\overline{G} = G/\operatorname{Rad}\delta$ and let $a \in G \setminus \operatorname{Rad} f$ be such that $a\operatorname{Rad}\delta \in Z(\overline{G})$. Then $[a,r] \in \operatorname{Rad}\delta$ for every $r \in G$, and thus $f(r,a,s)^{-1} = f(a,r,s) = \delta([a,r],s) = 1$ for every r, $s \in G$. Fix x, $y \in G$ such that $f(x,y,a) \neq 1$, and note that $g(x,y,a) = f(x,y,a) \neq 1$. Also fix $b = [x,y]$.

Then $\delta(b,a) = f(x,y,a) \neq 1$. Moreover, $\delta(b,rs) = \delta(b,r)\delta(b,s)$ for every r, $s \in G$, since $G' \le \operatorname{Mul}\delta$. If $s \in \operatorname{Rad} f$, we get $\delta(b,rs) = \delta(b,r)\delta(b,s) = \delta(b,r)f(x,y,s) = \delta(b,r)$. We thus consider $\delta(b,-)$ as a homomorphism $G/\operatorname{Rad} f \to \operatorname{Im} f$. Since $|\operatorname{Im} f| = 2$ by Lemma 6.5 and $|G/\operatorname{Rad} f| = 8$, $\delta(b,-)$ has kernel of size 4.

Fix u, $v \in G$ such that $\langle u,v,a\rangle\operatorname{Rad} f = G$ and $\delta(b,u) = \delta(b,v) = 1$. We claim that $[u,v] \notin \operatorname{Rad}\delta$. Indeed, should $[u,v] \in \operatorname{Rad}\delta$, then $[r,s] \in \operatorname{Rad}\delta$ for every r, $s \in \{u,v,a\}$, and so $f(r,s,t) = \delta([r,s],t) = 1$ for every r, s, $t \in G$, a contradiction.

By Lemma 6.2, $G = \langle x,y,a\rangle Z$ and so $G = \langle x,y,a\rangle\operatorname{Rad}\delta$, too. The group $\overline{G}\,'$ is then generated by $\{[x,y]\operatorname{Rad}\delta,\ [a,x]\operatorname{Rad}\delta,\ [a,y]\operatorname{Rad}\delta\} = \{[x,y]\operatorname{Rad}\delta\}$ and is therefore cyclic. Since $[u,v] \notin \operatorname{Rad}\delta$, we have $[u,v]\operatorname{Rad}\delta = [x,y]^m\operatorname{Rad}\delta$ for some m. Then $f(u,v,u) = \delta([u,v],u) = \delta([x,y]^m,u) = \delta(b,u)^m = 1$ and, similarly, $f(u,v,v) = 1$. It follows that $f(r,s,t) = 1$ for all r, s, $t \in \{u,v,a\}$, except possibly for $f(u,v,a) = f(v,u,a)$. But then we must have $f(u,v,a) = f(v,u,a) \neq 1$, else f is trivial.

We claim that $[a,u^i] = [a,u]^i$ for every i. The claim is certainly true for $i = 1$. The group identity $[r,st] = [r,t][r,s][[r,s],t]$ yields $[a,u^iu] = [a,u][a,u^i][[a,u^i],u]$, so it suffices to show that $[[a,u^i],u] = 1$. Now, $[[a,u^i],u] = [u,[a,u^i]]^{-1} = h(u,a,u^i)^{-1} = h(u,a,u)^{-i}$, and $h(u,a,u) = h(u,a,u)f(u,a,u) = f(u,u,a) = 1$. Similarly, $[a,v^i] = [a,v]^i$ for every i.

We also claim that

$$[a,u]^iZ \neq [a,v]Z \text{ and } [a,v]^iZ \neq [a,u]Z \text{ for every } i. \tag{6.2}$$

Indeed, if $[a,u]^i = [a,v]z$ for some $z \in Z$, we have $1 = h(u,a,u) = h(u,a,u)^i = h(u,a,u^i) = [u,[a,u^i]] = [u,[a,v]z] = [u,[a,v]] = f(u,v,a)f(u,a,v) = f(u,v,a) \neq 1$, a contradiction. The other case is similar.

By (6.2), $[a,u] \notin Z$, $[a,v] \notin Z$, and $[a,v]Z \neq [a,u]Z$. If $[a,u]^2 \notin Z$, (6.2) yields $|\operatorname{Rad}\delta/Z| \geq 4$, as desired. If $[a,u]^2 \in Z$ then $|\operatorname{Rad}\delta/Z|$ is even, and hence also $|\operatorname{Rad}\delta/Z| \geq 4$.

Finally, let us assume that $\operatorname{Rad}\delta/Z$ is a cyclic group of order 4. Then one of $[a,u]Z$, $[a,v]Z$ generates $\operatorname{Rad}\delta/Z$, a contradiction with (6.2). □

Lemma 6.10. *In a minimal setup, suppose that $Z(G/\operatorname{Rad}\delta)$ is not a subgroup of $\operatorname{Rad} f/\operatorname{Rad}\delta$. Let $K = G/Z$. Then $|K'| \geq 8$. If $|\operatorname{Rad} f/Z| = 8$ then $K' = Z(K) = \operatorname{Rad} f/Z$.*

Proof. With the notation of the proof of Proposition 6.9, $\operatorname{Rad}\delta/Z$ is the Klein group generated by $[a,u]Z$, $[a,v]Z$, and the commutator $[u,v]Z$ does not belong to $\operatorname{Rad}\delta$, which implies $|K'| \geq 8$. For the rest of the proof assume that $|\operatorname{Rad} f/Z| = 8$.

As $G' \leq \operatorname{Mul}\delta \leq \operatorname{Rad} f$ and $|K'| \geq 8$, we must have $K' \geq \operatorname{Rad} f/Z$. On the other hand, $G/\operatorname{Rad} f \cong (G/Z)/(\operatorname{Rad} f/Z)$ is an abelian group by Lemmas 6.3 and 6.5, so $K' = \operatorname{Rad} f/Z$.

Since $\operatorname{cl}(K) = 2$ by Lemma 4.1, we have $K' \leq Z(K)$. For the other inclusion, let $r \in Z(K)$. Then $[r,s] \in Z$ for every $s \in G$, so $f(s,r,t) = f(r,s,t) = \delta([r,s],t) = 1$ and $f(s,t,r) = [s,[r,t]]f(s,r,t) = [s,[r,t]] = 1$ for every r, $t \in G$. Hence $r \in \operatorname{Rad} f/Z = K'$. □

7. The minimal setups

We will need the following two lemmas concerning small 2-groups:

Lemma 7.1. *Let K be a group such that*

$$|K| = 64,\ |K'| = 8,\ \text{and } K' = Z(K). \tag{7.1}$$

Then both K' and K/K' are elementary abelian of order 8. In addition, there are e_1, e_2, $e_3 \in K$ such that $\{e_1K', e_2K', e_3K'\}$ is a basis of K/K', and $\{[e_1,e_2], [e_1,e_3], [e_2,e_3]\}$ is a basis of K'.

Proof. The group $K/K' = K/Z(K)$ is elementary abelian, else $|K/Z(K)| > 8$ by Lemma 6.7, a contradiction. For all x, $y \in K$ we then get $[x,y]^2 = [x,y^2] = 1$, and so K' is elementary abelian too. The rest is clear. □

Lemma 7.2. *Let G be a group such that $|G| = 128$ and $\operatorname{cl}(G) = 2$. Then $|G'| \leq 8$. If also $|G'| = 8$ then $|Z(G)| \leq 16$.*

Proof. The commutator can be seen as a bilinear mapping $G/Z(G) \to G'$. The group $G/Z(G)$ cannot be cyclic. Suppose for a while that $|G'| > 8$. Then $|G/Z(G)| \leq 8$. Assume that $G/Z(G)$ is elementary abelian of order 8. Then there are e_1, e_2, $e_3 \in G$ such that every commutator is of the form $[e_1^{a_1}e_2^{a_2}e_3^{a_3}, e_1^{b_1}e_2^{b_2}e_3^{b_3}]$, which is a product of $[e_1,e_2]$, $[e_1,e_3]$ and $[e_2,e_3]$ thanks to $\operatorname{cl}(G) = 2$. Since $[e_i,e_j]^2 = [e_i,e_j^2] = 1$ by $e_j^2 \in Z(G)$, we see that $G' \leq Z(G)$ is an elementary abelian 2-group generated by three elements, so $|G'| \leq 8$, a contradiction. We can argue similarly when $G/Z(G) \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ or when $G/Z(G)$ is elementary abelian of order 4.

Hence $|G'| \le 8$. Suppose that $|G'| = 8$. To show that $|Z(G)| \le 16$, it suffices to prove that $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ is impossible. This is once again easy. □

We can now summarize our results on minimal setups:

Theorem 7.3. *Let G, Z, δ be a minimal setup. Then $|G|$ is even and $|G| \ge 128$. If $|G| = 128$ then $|Z| = 2$, $\operatorname{Rad} g = \operatorname{Rad} f = \operatorname{Mul}\delta = G'Z$, $\operatorname{Mul}\delta/\operatorname{Rad}\delta$ is an elementary abelian 2-group, $G/\operatorname{Rad} g$ is an elementary abelian group of order 8, $K = G/Z$ satisfies (7.1), and one of the following scenarios holds, with $\overline{G} = G/\operatorname{Rad}\delta$:*

- (i) *$\mathrm{cl}(G)$=2, $G' < \operatorname{Mul}\delta = Z(G)$, $Z(\overline{G}) = \operatorname{Rad} f/\operatorname{Rad}\delta = \overline{G}\,'$, $|\operatorname{Mul}\delta/\operatorname{Rad}\delta| = 8$, $\operatorname{Rad}\delta = Z$, $f = g$, or*
- (ii) *$\mathrm{cl}(G)$=3, $Z = [G, G']$, $G' = \operatorname{Mul}\delta$, $Z(\overline{G}) = \operatorname{Rad} f/\operatorname{Rad}\delta = \overline{G}\,'$, $|\operatorname{Mul}\delta/\operatorname{Rad}\delta| = 8$, $\operatorname{Rad}\delta = Z$, or*
- (iii) *$\mathrm{cl}(G)$=3, $Z = [G, G'] \le G' = \operatorname{Mul}\delta$, $Z(\overline{G})$ is not a subgroup of $\operatorname{Rad} f/\operatorname{Rad}\delta$, $|\operatorname{Mul}\delta/\operatorname{Rad}\delta| = 2$, $\operatorname{Rad}\delta/Z$ is the Klein group.*

Proof. We know that $|G| = 128$ can occur thanks to the examples constructed already in [5]. Assume that $|G| \le 128$. Then $G/\operatorname{Rad} g$ is an elementary abelian group of order 8 by Lemma 6.3, $|\operatorname{Mul}\delta/\operatorname{Rad}\delta| \ge 2$ by Lemma 6.4, and $\operatorname{Rad} g = \operatorname{Rad} f$ by Lemma 6.5. Let $K = G/Z$.

If $Z(\overline{G}) \le \operatorname{Rad} f/\operatorname{Rad}\delta$ then $Z(\overline{G}) = \operatorname{Rad} f/\operatorname{Rad}\delta = \overline{G}\,'$ is elementary abelian of order 8 and $\operatorname{Rad} f = \operatorname{Mul}\delta$ by Proposition 6.8. This implies $\operatorname{Rad}\delta = Z$, $|Z| = 2$, and $|G| = 128$. By Proposition 6.8 again, K satisfies (7.1).

If $Z(\overline{G})$ is not a subgroup of $\operatorname{Rad} f/\operatorname{Rad}\delta$ then $|\operatorname{Rad}\delta/Z| \ge 4$ by Proposition 6.9 and hence $\operatorname{Rad} f = \operatorname{Mul}\delta$, $|\operatorname{Mul}\delta/\operatorname{Rad}\delta| = 2$, $|\operatorname{Rad}\delta/Z| = 4$, $|Z| = 2$ and $|G| = 128$. By Proposition 6.9, $\operatorname{Rad}\delta/Z$ is then the Klein group. Since $|\operatorname{Rad} f/Z| = 8$, Lemma 6.10 yields (7.1).

In either case, let $M = \operatorname{Rad} g = \operatorname{Rad} f = \operatorname{Mul}\delta$. As (7.1) holds, there are e_1, e_2, $e_3 \in G$ such that $\{e_1M, e_2M, e_3M\}$ is a basis of G/M, and $\{[e_1, e_2]Z, [e_1, e_3]Z, [e_2, e_3]Z\}$ is a basis of M/Z. Using $|Z| = 2$ and Lemma 4.1, we have

$$f(e_2, e_3, e_1) = [e_2, [e_1, e_3]]f(e_2, e_1, e_3) = [e_2, [e_1, e_3]]f(e_1, e_2, e_3),$$
$$f(e_3, e_1, e_2) = f(e_1, e_3, e_2) = [e_1, [e_2, e_3]]f(e_1, e_2, e_3).$$

Thus

$$1 \ne g(e_1, e_2, e_3) = [e_2, [e_1, e_3]][e_1, [e_2, e_3]]f(e_1, e_2, e_3). \tag{7.2}$$

If $Z(\overline{G})$ is not a subgroup of $\operatorname{Rad} f/\operatorname{Rad}\delta$ then $|\operatorname{Rad}\delta/Z| = 4$ and we can assume without loss of generality that $[e_1, e_2]\operatorname{Rad}\delta = [e_1, e_3]\operatorname{Rad}\delta$. Then

$$\begin{aligned} f(e_1, e_2, e_3) &= \delta([e_1, e_2], e_3) = \delta([e_1, e_3], e_3) = f(e_1, e_3, e_3) \\ &= f(e_3, e_1, e_3) = [e_3, [e_3, e_1]]f(e_3, e_3, e_1) = [e_3, [e_3, e_1]]\delta([e_3, e_3], e_1) = [e_3, [e_3, e_1]] \end{aligned}$$

and therefore

$$1 \ne g(e_1, e_2, e_3) = [e_2, [e_1, e_3]][e_1, [e_2, e_3]][e_3, [e_3, e_1]]. \tag{7.3}$$

We have $G' \le \operatorname{Mul}\delta$, $Z \le \operatorname{Mul}\delta$, so $G'Z \le \operatorname{Mul}\delta$. Since $|Z| = 2$ and $[G, G'] \le Z$, the following three conditions are equivalent: $[G, G'] < Z$, $[G, G'] = 1$, $\mathrm{cl}(G) = 2$.

Suppose that $\mathrm{cl}(G) = 2$. Then $Z(\overline{G}) \le \operatorname{Rad} f/\operatorname{Rad}\delta$, since the other alternative implies (7.3), a contradiction with $[G, G'] = 1$. Furthermore, $|G'| \le 8$ by Lemma 7.2. Since $|K'| = |G'Z/Z| = 8$, we have $|G'Z| = 16$, and so $|G'| = 8$, $G' < \operatorname{Mul}\delta$, $Z(G) \ge G'Z = \operatorname{Mul}\delta$. By the second part of Lemma 7.2, $Z(G) = \operatorname{Mul}\delta$. Finally, $f(x, y, z) = f(y, z, x) = f(x, z, y)$ by Lemma 4.1 and $\mathrm{cl}(G) \le 2$, so $g(x, y, z) = f(x, y, z)^3 = f(x, y, z)$.

Now suppose that $\mathrm{cl}(G) = 3$. Then $Z = [G, G'] \le G'$, so $K' = (G/Z)' = G'Z/Z = G'/Z$, which implies $|G'| = 16$ and thus $G' = G'Z = \mathrm{Mul}\,\delta$. The rest of (ii), (iii) has already been established. □

It is now easy to characterize all groups G/Z from minimal setups. Note that these groups are of interest for the associated loops $Q = G[\mu]$, too, since $G/Z \cong Q/Z$.

Proposition 7.4. *A group K appears as G/Z in a minimal setup if and only if K satisfies* (7.1)*. All such groups appear already in scenario (i) of Theorem 7.3.*

Proof. By Theorem 7.3, $K = G/Z$ from a minimal setup satisfies (7.1). Conversely, assume that K satisfies (7.1). Then $K = G/Z$ for some G in scenario (i) by the results of [5, §5]. □

7.1. **Constructing minimal setups for scenarios (ii) and (iii).** We show how to construct all minimal setups. Note that all minimal setups of scenario (i) of Theorem 7.3 were constructed already in [5, §5], so it suffices to work with scenarios (ii) and (iii).

First we obtain a few auxiliary facts about minimal setups.

Lemma 7.5. *Let G, Z, δ be a minimal setup. Then for every basis $\{e_1, e_2, e_3\} \subseteq G$ of $G/\mathrm{Rad}\,g$ we have* (7.2)*. In particular, g and f are determined already by G and $\mathrm{Rad}\,g$.*

Proof. By Theorem 7.3, $G/\mathrm{Rad}\,g$ is an elementary abelian group of order 8. Let $\{e_1\,\mathrm{Rad}\,g,\ e_2\,\mathrm{Rad}\,g,\ e_3\,\mathrm{Rad}\,g\}$ be a basis of $G/\mathrm{Rad}\,g$. Since g is nontrivial, it is the determinant, so $g(e_i, e_j, e_k) \ne 1$ if and only if i, j, k are distinct. This determines g as a mapping $G\times G\times G \to Z$. We have derived (7.2) in the proof of Theorem 7.3. It remains to show that f is determined by g and G. Indeed, $1 = f(e_i, e_i, e_i)$, $1 = f(e_i, e_i, e_j)$ determines $f(e_i, e_j, e_i)$ and $f(e_j, e_i, e_i)$ by Lemma 4.1, $f(e_1, e_2, e_3)$ is determined by (7.2), and this value determines $f(e_i, e_j, e_k)$ whenever i, j, k are distinct. □

Let G, Z, δ be a minimal setup from scenario (ii) or (iii), and let $R = \mathrm{Rad}\,\delta$, $M = \mathrm{Mul}\,\delta = \mathrm{Rad}\,f = \mathrm{Rad}\,g$. Note that $M = N = G'R = G'$ here, by Theorem 7.3.

By Lemma 7.1, there are e_1, e_2, $e_3 \in G$ such that $\{e_1M,\ e_2M,\ e_3M\}$ is a basis for G/M, and $\{[e_1, e_2]Z,\ [e_1, e_3]Z,\ [e_2, e_3]Z\}$ is a basis for M/Z.

In scenario (ii), $Z = R$, so we have a basis for M/R. In scenario (iii), $|R/Z| = 4$, and we can therefore assume without loss of generality that $[e_1, e_2]R = [e_1, e_3]R$.

We finally turn to the construction of all minimal setups. Let us therefore forget about δ, f and g, but let us keep the groups G, M, R, Z and the elements e_1, e_2, e_3. Our goal is to construct a nontrivial setup G, Z, δ with $M = \mathrm{Mul}\,\delta$ and $R = \mathrm{Rad}\,\delta$. Let $Z = \{1, -1\}$.

First of all, the mapping $g : (G/M)^3 \to Z$ must be a trilinear alternating form, and hence we must and can set

$$g(e_i, e_j, e_k) = \begin{cases} -1, & \text{if } i,\ j,\ k \text{ are distinct,} \\ 1, & \text{else,} \end{cases}$$

and then extend g linearly.

Next we need a multiplicative mapping $f : (G/M)^3 \to Z$ such that $g(x, y, z) = f(x, y, z)f(y, z, x)f(z, x, y)$ and such that f behaves as in Lemma 4.1. Anticipating the equality $\delta([x, y], z) = f(x, y, z)$, we must set

$$f(e_i, e_i, e_j) = 1 \text{ for } 1 \le i,\ j \le 3.$$

Then Lemma 4.1 forces

$$f(e_i, e_j, e_i) = f(e_j, e_i, e_i) = [e_i, [e_i, e_j]] \text{ for } 1 \le i,\ j \le 3.$$

By Lemma 7.5, we must set

$$f(e_1, e_2, e_3) = f(e_2, e_1, e_3) = -[e_1, [e_2, e_3]][e_2, [e_1, e_3]],$$

and then Lemma 4.1 forces

$$f(e_1, e_3, e_2) = f(e_3, e_1, e_2) = -[e_2, [e_1, e_3]],$$
$$f(e_2, e_3, e_1) = f(e_3, e_2, e_1) = -[e_1, [e_2, e_3]].$$

A straightforward calculation yields $g(e_i, e_j, e_k) = f(e_i, e_j, e_k)f(e_j, e_k, e_i)f(e_k, e_i, e_i)$ for every $1 \le i,\ j,\ k \le 3$.

We can now extend f linearly into a mapping $(G/M)^3 \to Z$, and force $\mathrm{Rad}\, f = M$.

Finally, we need to construct $\delta : (G/R)^3 \to Z$ so that $\delta([x, y], z) = f(x, y, z)$ and (B_1)–(B_4) hold. We will encounter a difficulty in scenario (iii), which is why we only managed to answer some questions concerning scenario (iii) using a computer.

Set

$$\delta([e_i, e_j], e_k) = f(e_i, e_j, e_k) \text{ for } 1 \le i,\ j,\ k \le 3.$$

Since $G' = M$, we can now attempt to extend δ into a mapping $M/R \times \{e_1, e_2, e_3\} \to Z$. This unique extension is well defined in scenario (ii), as the values $[e_1, e_2]$, $[e_1, e_3]$, $[e_2, e_3]$ are linearly independent modulo R. But in scenario (iii) the extension might not exist, and this can be verified with a computer in each particular case.

Assuming that $\delta : M/R \times \{e_1, e_2, e_3\} \to Z$ is well-defined, we extend it routinely into a mapping $M/R \times G/R \to Z$, using $M = \mathrm{Rad}\, f$.

The last step is to extend δ into a mapping $G/R \times G/R \to Z$, and this involves some free parameters. Namely, let $T = \{t_1 = 1,\ \ldots,\ t_n\}$ be a transversal to M/R in G/R, and for $1 \le i,\ j \le 3$ choose $\delta(t_i, t_j)$ as follows:

$$\begin{aligned} &\delta(t_1, t_j) = 1 \text{ for every } 1 \le j \le n,\\ &\delta(t_i, t_j) \text{ arbitrary when } 1 < i < j \le n,\\ &\delta(t_j, t_i) = \delta(t_i, t_j)^{-1} \text{ when } 1 < i < j \le n,\\ &\delta(t_i, t_i) = 1 \text{ for every } 1 \le i \le n. \end{aligned} \tag{7.4}$$

Every element $h \in G/R$ can be written uniquely as $h = mt$ for some $m \in M/R$, $t \in T$. We define $\delta : G/R \times G/R \to Z$ by

$$\delta(mt, m't') = \delta(m, t')\delta(m', t)^{-1}\delta(t, t'),$$

where $\delta(m, t')$, $\delta(m', t)$ have already been defined above. We leave it to the reader to check that this correctly defines $\delta : G \times G \to Z$ satisfying (B_1)–(B_4) and $\delta([x, y], z) = f(x, y, z)$.

We have arrived at a minimal setup G, Z, δ.

7.2. **The groups G in minimal setups.** For the sake of completeness, we now describe the groups G and G/Z that appear in individual scenarios of Theorem 7.3:

- The groups G/Z of scenario (i) (respective (ii)) are precisely the groups K satisfying (7.1). There are 10 such groups, identified as $(64, 73)$–$(64, 82)$ in GAP [6].
- The groups G/Z of scenario (iii) are precisely the groups $(64, 73)$–$(63, 76)$ and $(64, 80)$ of GAP, by computer search.
- The groups G of scenario (i) are precisely the groups G such that: $\mathrm{cl}(G) = 2$, there is $Z \le Z(G)$ such that $|Z| = 2$ and $K = G/Z$ satisfies (7.1). There are 19 such groups, identified in GAP as $(128, m)$ for $m \in$ {170–178, 1116–1119, 1121–1123, 1125, 1126, 1132}.

- The groups G of scenario (ii) are precisely the groups G such that: $\mathrm{cl}(G) = 3$, $Z = [G, G'] \le Z(G)$, $|Z| = 2$, and $K = G/Z$ satisfies (7.1). There are 106 such groups, identified as $(128, 731)$–$(128, 836)$ in GAP.
- The groups G of scenario (iii) are precisely the 10 groups $(128, m)$ for $m \in \{742$, 749, 753, 754, 761, 762, 776, 794, 823, $830\}$ of GAP, by computer search.

8. Examples of loops of Csörgő type

Very many examples of loops of Csörgő type can be constructed from Theorem 7.3 due to the free parameters (in (7.4) and (5.1)) used in the top to bottom construction of μ from g. All examples listed below were obtained with the LOOPS [8] package for GAP [6] by using trivial values for all free parameters.

To get a loop of Csörgő type as in scenario (ii) of Theorem 7.3, let G be the group of order 128 generated by $g_1, \dots, g_7$ with $Z(G) = \langle g_5, g_6, g_7\rangle$ subject to the relations $g_1^2 = 1$, $[g_2, g_1] = g_4$, $[g_3, g_1] = g_5$, $[g_4, g_1] = g_7$, $[g_3, g_2] = g_6$, $[g_4, g_2] = g_7$, $g_3^2 = 1$, $[g_4, g_3] = 1$, $g_4^2 = g_7$, $g_5^2 = 1$, $g_6^2 = 1$, $g_7^2 = 1$. (This is the group identified as $(128, 731)$ in GAP.)

Then $G' = \langle g_4, Z(G)\rangle$ and $\mathrm{cl}(G) = 3$. Set $Z = R = \langle g_7\rangle$, $M = G'$, $e_1 = g_1$, $e_2 = g_2$, $e_3 = g_3$. Then the resulting loop $Q = G[\mu]$ satisfies $|Q| = 128$, $\mathrm{cl}(Q) = 3$, $\mathrm{Inn}\, Q \cong \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $|\mathrm{Mlt}\, Q| = 8192$.

To get a loop of Csörgő type as in scenario (iii) of Theorem 7.3, let G be the group of order 128 generated by $g_1, \dots, g_7$ with $Z(G) = \langle g_4g_5g_6, g_7\rangle$ subject to relations $g_1^2 = 1$, $[g_2, g_1] = g_4$, $[g_3, g_1] = g_5$, $[g_4, g_1] = g_7$, $[g_5, g_1] = 1$, $[g_6, g_1] = g_7$, $g_2^2 = 1$, $[g_3, g_2] = g_6$, $[g_4, g_2] = g_7$, $[g_5, g_2] = g_7$, $[g_6, g_2] = 1$, $g_3^2 = 1$, $[g_4, g_3] = 1$, $[g_5, g_3] = 1$, $[g_6, g_3] = 1$, $g_4^2 = g_7$, $[g_5, g_4] = 1$, $[g_6, g_4] = 1$, $g_5^2 = 1$, $[g_6, g_5] = 1$, $g_7^2 = 1$. (This is the group identified as $(128, 742)$ in GAP.)

Then $G' = \langle g_4, g_5, g_6, g_7\rangle$ and $\mathrm{cl}(G) = 3$. Set $Z = \langle g_7\rangle$, $R = \langle g_5, g_6, g_7\rangle$, $M = G'$, and $e_1 = g_1$, $e_2 = g_2$, $e_3 = g_2g_3$. Then R/Z is the Klein group, and the resulting loop $Q = G[\mu]$ satisfies $|Q| = 128$, $\mathrm{cl}(Q) = 3$, $\mathrm{Inn}\, Q \cong \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $|\mathrm{Mlt}\, Q| = 8192$.

8.1. A class of examples with $\mathrm{Inn}\, Q$ not elementary abelian.

Lemma 8.1. *Let $Q = G[\mu]$ be constructed from a minimal setup. For $x \in Q$, let $T_x = R_x^{-1}L_x$ be the conjugation by x in Q. Then $(T_x)^2y = y^{x^2}f(y, x, x)$ for every x, $y \in Q$.*

Proof. By Theorem 7.3 we have $|Z| = 2$. By [5, Lemma 4.4],

$$T_x(y) = y^x\mu(y, x)\mu(x, y^x)^{-1} = y^x\mu(y, x)\mu(x, y^x).$$

Then

$$(T_x)^2y = T_x(y^x\mu(y, x)\mu(x, y^x)) = y^{x^2}\mu(y, x)\mu(x, y^x)\mu(y^x, x)\mu(x, y^{x^2}),$$

where we have used $\mathrm{Im}\, \mu \le Z \le Z(G)$ and $Z \le \mathrm{Rad}\, \mu$. Now, $\mu(x, y^x)\mu(y^x, x) = \delta(y^x, x) = \delta(y[y, x], x) = \delta(y, x)\delta([y, x], x) = \delta(y, x)f(y, x, x)$ by $G' \le \mathrm{Mul}\, \delta$, and thus $(T_x)^2y = y^{x^2}\mu(y, x)\delta(y, x)f(y, x, x)\mu(x, y^{x^2})$. Furthermore, $\mu(y, x)\delta(y, x)\mu(x, y^{x^2}) = \mu(x, y)\mu(x, y[y, x^2]) = \mu(x, y)\mu(x, y)\mu(x, [y, x^2]) = \mu(x, [y, x^2])$, and $[y, x^2] = [y, x]^2z$ for some $z \in Z$, so $\mu(x, [y, x^2]) = \mu(x, [y, x]^2) = \mu(x, [y, x])^2 = 1$. □

By Lemma 8.1, in order to obtain $Q = G[\mu]$ from a minimal setup so that $\mathrm{Inn}\, Q$ is not elementary abelian, it suffices to choose $K = G/Z$ as one of the groups satisfying (7.1), take G as a central extension of K by the cyclic group of order 2 so that $[y, x^2] \ne 1$

(hence $y^{x^2} \neq y$) and $[x,[x,y]] = 1$ (hence $f(y,x,x) = f(x,x,y)[x,[x,y]] = [x,[x,y]] = 1$) for some $x,\, y \in G$.

References

[1] R. H. Bruck, *Contributions to the theory of loops*, Trans. Amer. Math. Soc. **60** (1946), 245–354.

[2] P. Csörgő, *Abelian inner mappings and nilpotency class greater than two*, European J. Combin. **28** (2007), 858–868.

[3] P. Csörgő and T. Kepka, *On loops whose inner permutations commute*, Comment. Math. Univ. Carolin. **45** (2004), 213–221.

[4] P. Csörgő, A. Jančařík and T. Kepka, *Generalized capable abelian groups*, Non-associative algebra and its applications 129–136, Lect. Notes Pure Appl. Math. **246**, Chapman and Hall/CRC, Boca Raton, FL, 2006.

[5] A. Drápal and P. Vojtěchovský, *Explicit constructions of loops with commuting inner mappings*, European J. Combin. **29** (2008), 1662-1681.

[6] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.12; 2008. (http://www.gap-system.org)

[7] M. Mazur, *Connected transversals to nilpotent groups*, J. Group Theory **10** (2007), no. **2**, 195–203.

[8] G. P. Nagy and P. Vojtěchovský, *LOOPS: Computing with quasigroups and loops*, version 2.1.0, package for GAP. Distribution website: http://www.math.du.edu/loops

[9] M. Niemenmaa, *On finite loops whose inner mapping groups are abelian*, Bull. Austral. Math. Soc. **65** (2002), 477–484.

[10] M. Niemenmaa, *Finite loops with nilpotent inner mapping groups are centrally nilpotent*, Bull. Austral. Math. Soc. **79** (2009), 109–114.

[11] M. Niemenmaa and T. Kepka, *On multiplication group of loops*, J. Algebra **135** (1990), 112–122.

[12] A. Vesanen, *Solvable groups and loops*, J. Algebra **180** (1996), no. **3**, 862–876.

E-mail address, Drápal: `drapal@karlin.mff.cuni.cz`

(Drápal) Department of Algebra, Charles University, Sokolovská 83, 186 75 Prague, Czech Republic

E-mail address, Vojtěchovský: `petr@math.du.edu`

(Vojtěchovský) Department of Mathematics, University of Denver, 2360 S Gaylord St, Denver, Colorado 80208, USA