ENUMERATION OF NILPOTENT LOOPS VIA COHOMOLOGY

DANIEL DALY AND PETR VOJTĚCHOVSKÝ

Abstract. The isomorphism problem for centrally nilpotent loops can be tackled by methods of cohomology. We develop tools based on cohomology and linear algebra that either lend themselves to direct count of the isomorphism classes (notably in the case of nilpotent loops of order $2q$, q a prime), or lead to efficient classification computer programs. This allows us to enumerate all nilpotent loops of order less than 24.

1. Introduction

A nonempty set Q equipped with a binary operation $\cdot$ is a *loop* if it possesses a neutral element 1 satisfying $1\cdot x = x\cdot 1 = x$ for every $x\in Q$, and if for every $x\in Q$ the mappings $Q\to Q$, $y\mapsto x\cdot y$ and $Q\to Q$, $y\mapsto y\cdot x$ are bijections of Q. From now on we will abbreviate $x\cdot y$ as xy.

Note that multiplication tables of finite loops are precisely normalized latin squares, and that groups are precisely associative loops.

The *center* $Z(Q)$ of a loop Q consists of all elements $x\in Q$ such that

$$xy = yx,\quad (xy)z = x(yz),\quad (yx)z = y(xz),\quad (yz)x = y(zx)$$

for every y, $z\in Q$. *Normal* subloops are kernels of loop homomorphisms. The center $Z(Q)$ is a normal subloop of Q. The *upper central series* $Z_0(Q)\le Z_1(Q)\le\cdots$ is defined by

$$Z_0(Q) = 1,\quad Q/Z_{i+1}(Q) = Z(Q/Z_i(Q)).$$

If there is $n\ge 0$ such that $Z_{n-1}(Q) < Z_n(Q) = Q$, we say that Q is *(centrally) nilpotent of class n*.

The goal of this paper is to initiate the classification of small nilpotent loops up to isomorphism, where by small we mean either that the order $|Q|$ of Q is a small integer, or that the prime factorization of $|Q|$ involves few primes.

Here is a summary of the paper, with $A = (A,+)$ a finite abelian group and $F = (F,\cdot)$ a finite loop throughout.

§2. Central extensions of A by F are in one-to-one correspondence with (normalized) cocycles $\theta : F\times F\to A$. Let $\mathcal{Q}(F,A,\theta)$ be the central extension of A by F via θ. If $\theta-\mu$ is a coboundary then $\mathcal{Q}(F,A,\theta)\cong\mathcal{Q}(F,A,\mu)$, that is, the two loops are isomorphic.

§3. The group $\mathrm{Aut}(F,A) = \mathrm{Aut}(F)\times\mathrm{Aut}(A)$ acts on the cocycles by

$$(\alpha,\beta):\theta\mapsto {}^{(\alpha,\beta)}\theta,\quad {}^{(\alpha,\beta)}\theta : (x,y)\mapsto \beta\theta(\alpha^{-1}x,\alpha^{-1}y).$$

For every $(\alpha,\beta)\in\mathrm{Aut}(F,A)$ we have $\mathcal{Q}(F,A,\theta)\cong\mathcal{Q}(F,A,{}^{(\alpha,\beta)}\theta)$.

Fix a cocycle θ, and let us write $\theta\sim\mu$ if there is $(\alpha,\beta)\in\mathrm{Aut}(F,A)$ such that ${}^{(\alpha,\beta)}\theta-\mu$ is a coboundary. If $\theta\sim\mu$, we have $\mathcal{Q}(F,A,\theta)\cong\mathcal{Q}(F,A,\mu)$. If the converse is true for

---

2000 *Mathematics Subject Classification.* Primary: 20N05. Secondary: 20J05, 05B15.

Key words and phrases. Nilpotent loop, classification of nilpotent loops, loop cohomology, group cohomology, central extension, latin square.

every μ, we say that θ is *admissible*. We describe several situations in which all cocycles are admissible.

§4. If all cocycles are admissible, the isomorphism problem for central extensions reduces to the study of the equivalence classes of $\sim$.

For $(\alpha,\beta)\in\mathrm{Aut}(F,A)$, let

$$\mathrm{Inv}(\alpha,\beta)=\{\theta;\theta-{}^{(\alpha,\beta)}\theta \text{ is a coboundary}\},$$

and for $H\subseteq\mathrm{Aut}(F,A)$, let

$$\mathrm{Inv}(H)=\bigcap_{(\alpha,\beta)\in H}\mathrm{Inv}(\alpha,\beta).$$

Then $\mathrm{Inv}(H)$ is a subgroup of cocycles, and $\mathrm{Inv}(H)=\mathrm{Inv}(\langle H\rangle)$, where $\langle H\rangle$ is the subgroup of $\mathrm{Aut}(F,A)$ generated by H.

For $H\le\mathrm{Aut}(F,A)$, let

$$\mathrm{Inv}^*(H)=\mathrm{Inv}(H)\setminus\bigcup_{H<K\le\mathrm{Aut}(F,A)}\mathrm{Inv}(K).$$

When $\theta\in\mathrm{Inv}^*(H)$, the $\sim$-equivalence class $[\theta]_\sim$ of θ is a union of precisely $[\mathrm{Aut}(F,A):H]$ cosets of coboundaries. It is not necessarily true that $[\theta]_\sim$ is contained in $\mathrm{Inv}^*(H)$, however, it is contained in

$$\mathrm{Inv}^*_c(H)=\bigcup_K\mathrm{Inv}^*(K),$$

where the union is taken over all subgroups K of $\mathrm{Aut}(F,A)$ conjugate to H. Moreover, $|\mathrm{Inv}^*_c(H)|=|\mathrm{Inv}^*(H)|\cdot[\mathrm{Aut}(F,A):N_{\mathrm{Aut}(F,A)}(H)]$, where $N_G(H)$ is the normalizer of H in G.

Hence, if every cocycle is admissible, we can enumerate all central extensions of A by F up to isomorphism as soon as we know $|\mathrm{Inv}^*(H)|$ for every $H\le\mathrm{Aut}(F,A)$, cf. Theorem 4.5.

§5. For $H,K\le\mathrm{Aut}(F,A)$, we have $\mathrm{Inv}(H)\cap\mathrm{Inv}(K)=\mathrm{Inv}(\langle H\cup K\rangle)$. Hence $|\mathrm{Inv}^*(K)|$ can be deduced from the cardinalities of the subgroups $\mathrm{Inv}(H)$ via the principle of inclusion and exclusion based on the subgroup lattice of $\mathrm{Aut}(F,A)$.

In turn, to find $|\mathrm{Inv}(H)|$, it suffices to determine the cardinalities of $\mathrm{Inv}(\alpha,\beta)$ for every $(\alpha,\beta)\in H$, and the way these subgroups intersect. When A is a prime field, the action $\theta\mapsto{}^{(\alpha,\beta)}\theta$ can be seen as a matrix operator on the vector space of cocycles, and its preimage of coboundaries is $\mathrm{Inv}(\alpha,\beta)$. It is therefore not difficult to find $\mathrm{Inv}(\alpha,\beta)$ by means of (computer) linear algebra even for rather large prime fields A and loops F.

§6. When $A=\mathbb{Z}_p$, $F=\mathbb{Z}_q$ and $p\ne q$ are primes, the dimension of $\mathrm{Inv}(\alpha,\beta)$ can be found without the assistance of a computer, cf. Theorem 6.5.

§7. Since every cocycle is admissible when $p=2$ and q is odd, Theorems 4.5 and 6.5 give a formula for the number of nilpotent loops of order $2q$, up to isomorphism, cf. Theorem 7.1. The asymptotic growth of the number of nilpotent loops of order $2q$ is determined in Theorem 7.3.

§8. Every central subloop contains $A=\mathbb{Z}_p$ for some prime p. Not every choice of A and F results in admissible cocycles, but we can work around this problem when A and F are small by excluding the subset $W(F,A)=\{\theta;\ Z(\mathcal{Q}(F,A,\theta))>A\}$, because all remaining cocycles will be admissible. When $W(F,A)$ is small, the isomorphism problem for $\{\mathcal{Q}(F,A,\theta);\theta\in W(F,A)\}$ can be tackled by a direct isomorphism check, using the GAP package LOOPS.

§9. This allows us to enumerate all nilpotent loops of order n less than 24 up to isomorphism, cf. Table 2. The computational difficulties are nontrivial, notably for $n = 16$ and $n = 20$. We accompany Table 2 by a short narrative describing the difficulties and how they were overcome.

There are $2,623,755$ nilpotent loops F of order 12, which is why the case $n = 24$ is out of reach of the methods developed here.

§10. In order not to distract from the exposition, we have collected references to related work and ideas at the end of the paper.

2. Central extensions, cocycles and coboundaries

We say that a loop Q is a *central extension of* A *by* F if $A \leq Z(Q)$ and $Q/A \cong F$.

A mapping $\theta : F \times F \to A$ is a *normalized cocycle* (or *cocycle*) if it satisfies

$$\theta(1, x) = \theta(x, 1) = 0 \text{ for every } x \in F. \tag{2.1}$$

For a cocycle $\theta : F \times F \to A$, define $\mathcal{Q}(F, A, \theta)$ on $F \times A$ by

$$(x, a)(y, b) = (xy, a + b + \theta(x, y)). \tag{2.2}$$

The following characterization of central loop extensions is well known, and is in complete analogy with the associative case:

Theorem 2.1. *The loop Q is a central extension of A by F if and only if there is a cocycle $\theta : F \times F \to A$ such that $Q \cong \mathcal{Q}(F, A, \theta)$.*

The cocycles $F \times F \to A$ form an abelian group $\mathrm{C}(F, A)$ with respect to addition

$$(\theta + \mu)(x, y) = \theta(x, y) + \mu(x, y).$$

When A is a field, $\mathrm{C}(F, A)$ is a vector space over A with scalar multiplication

$$(c\theta)(x, y) = c \cdot \theta(x, y).$$

Let

$$\mathrm{Map}_0(F, A) = \{\tau : F \to A;\ \tau(1) = 0\},$$
$$\mathrm{Hom}(F, A) = \{\tau : F \to A;\ \tau \text{ is a homomorphism of loops}\},$$

and observe:

Lemma 2.2. *The mapping* $\widehat{\ } : \mathrm{Map}_0(F, A) \to \mathrm{C}(F, A)$, $\tau \mapsto \widehat{\tau}$ *defined by*

$$\widehat{\tau}(x, y) = \tau(xy) - \tau(x) - \tau(y)$$

is a homomorphism of groups with kernel $\mathrm{Hom}(F, A)$.

The image $\mathrm{B}(F, A) = \widehat{\mathrm{C}(F, A)} \cong \mathrm{Map}_0(F, A)/\mathrm{Hom}(F, A)$ is a subgroup (subspace) of $\mathrm{C}(F, A)$, and its elements are referred to as *coboundaries*.

When A is a field, the vector space $\mathrm{Map}_0(F, A)$ has basis $\{\tau_c;\ c \in F \setminus \{1\}\}$, where

$$\tau_c : F \to A, \quad \tau_c(x) = \begin{cases} 1, & \text{if } x = c, \\ 0, & \text{otherwise.} \end{cases} \tag{2.3}$$

Hence the vector space $\mathrm{B}(F, A)$ is generated by $\{\widehat{\tau_c};\ c \in F \setminus \{1\}\}$. Observe that for x, $y \in F \setminus \{1\}$ we have

$$\widehat{\tau_c}(x, y) = \begin{cases} 1, & \text{if } xy = c, \\ -1, & \text{if } x = c \text{ or } y = c \text{ but not } x = y, \\ -2, & \text{if } x = y = c, \\ 0, & \text{otherwise.} \end{cases} \tag{2.4}$$

Coboundaries play a prominent role in classifications due to this simple observation:

Lemma 2.3. *Let* $\widehat{\tau} \in \mathrm{B}(F, A)$*. Then* $f : \mathcal{Q}(F, A, \theta) \to \mathcal{Q}(F, A, \theta + \widehat{\tau})$ *defined by*

$$f(x, a) = (x, a + \tau(x))$$

is an isomorphism of loops.

The converse of Lemma 2.3 does not hold, making the classification of loops up to isomorphism nontrivial even in highly structured subvarieties, such as groups. Nevertheless it is clear that it suffices to consider cocycles modulo coboundaries, and we therefore define the *(second) cohomology* $\mathrm{H}(F, A) = \mathrm{C}(F, A)/\mathrm{B}(F, A)$.

3. The action of the automorphism groups and admissibility

Let $\mathrm{Aut}(F, A) = \mathrm{Aut}(F) \times \mathrm{Aut}(A)$. The group $\mathrm{Aut}(F, A)$ acts on $\mathrm{C}(F, A)$ via

$$\theta \mapsto {}^{(\alpha,\beta)}\theta, \quad {}^{(\alpha,\beta)}\theta : (x, y) \mapsto \beta\theta(\alpha^{-1}x, \alpha^{-1}y).$$

Indeed, we have ${}^{(\alpha\gamma,\beta\delta)}\theta = {}^{(\alpha,\beta)}({}^{(\gamma,\delta)}\theta)$, and ${}^{(\alpha,\beta)}(\theta + \mu) = {}^{(\alpha,\beta)}\theta + {}^{(\alpha,\beta)}\mu$. Since

$${}^{(\alpha,\beta)}\widehat{\tau} = \widehat{\beta\tau\alpha^{-1}},$$

the action of $\mathrm{Aut}(F, A)$ on $\mathrm{C}(F, A)$ induces an action on $\mathrm{B}(F, A)$ and on $\mathrm{H}(F, A)$. Moreover:

Lemma 3.1. *Let* $(\alpha, \beta) \in \mathrm{Aut}(F, A)$*. Then* $f : F \times A \to F \times A$ *defined by* $f(x, a) = (\alpha x, \beta a)$ *is an isomorphism* $\mathcal{Q}(F, A, \theta) \to \mathcal{Q}(F, A, {}^{(\alpha,\beta)}\theta)$*.*

Proof. Let $\cdot$ be the multiplication in $\mathcal{Q}(F, A, \theta)$ and $*$ the multiplication in $\mathcal{Q}(F, A, {}^{(\alpha,\beta)}\theta)$. Then

$$\begin{aligned} f((x, a) \cdot (y, b)) &= f(xy, a + b + \theta(x, y)) = (\alpha(xy), \beta(a + b + \theta(x, y))) \\ &= (\alpha(x)\alpha(y), \beta(a) + \beta(b) + \beta\theta(\alpha^{-1}\alpha x, \alpha^{-1}\alpha y)) \\ &= (\alpha(x)\alpha(y), \beta(a) + \beta(b) + {}^{(\alpha,\beta)}\theta(\alpha x, \alpha y)) \\ &= (\alpha x, \beta a) * (\alpha y, \beta b) = f(x, a) * f(y, b). \end{aligned}$$

□

As in §1, write $\theta \sim \mu$ if there is $(\alpha, \beta) \in \mathrm{Aut}(F, A)$ such that ${}^{(\alpha,\beta)}\theta - \mu \in \mathrm{B}(F, A)$. Then $\sim$ is an equivalence relation on $\mathrm{C}(F, A)$, and the equivalence class of θ is

$$[\theta]_\sim = \bigcup_{(\alpha,\beta)\in\mathrm{Aut}(F,A)} ({}^{(\alpha,\beta)}\theta + \mathrm{B}(F, A)).$$

By Lemmas 2.3 and 3.1, if $\theta \sim \mu$ then $\mathcal{Q}(F, A, \theta) \cong \mathcal{Q}(F, A, \mu)$. We say that θ is *admissible* if the converse is also true, that is, if $\mathcal{Q}(F, A, \theta) \cong \mathcal{Q}(F, A, \mu)$ if and only if $\theta \sim \mu$.

We remark that there exists an inadmissible cocycle $\theta \in \mathrm{C}(\mathbb{Z}_6, \mathbb{Z}_2)$. In the rest of this section we describe situations that guarantee admissibility.

Proposition 3.2. *Let* $Q = \mathcal{Q}(F, A, \theta)$*. If* $\mathrm{Aut}(Q)$ *acts transitively on* $\{K \le Z(Q);\ K \cong A,\ Q/K \cong F\}$ *then* θ *is admissible.*

Proof. Let $Q = \mathcal{Q}(F, A, \theta)$, and let $f : Q \to \mathcal{Q}(F, A, \mu)$ be an isomorphism. Let $K = f^{-1}(1 \times A)$. By our assumption, there is $g \in \mathrm{Aut}(Q)$ such that $g(1 \times A) = K$. Then $fg : Q \to \mathcal{Q}(F, A, \mu)$ is an isomorphism mapping $1 \times A$ onto itself. We can therefore assume without loss of generality that already f has this property.

Denote by $\cdot$ the multiplication in Q and by $*$ the multiplication in $\mathcal{Q}(F,A,\mu)$. Define $\beta : A \to A$ by $(1,\beta(a)) = f(1,a)$. Then

$$(1,\beta(a+b))=f(1,a+b)=f((1,a)\cdot(1,b))=f(1,a)*f(1,b)=(1,\beta a)*(1,\beta b)=(1,\beta a+\beta b),$$

which means that $\beta \in \mathrm{Aut}(A)$.

Define $\tau : F \to A$ and $\alpha : F \to F$ by $f(x,0) = (\alpha x, \tau x)$. Since $f(1,0) = (1,0)$, we have $\tau \in \mathrm{Map}_0(F,A)$. Moreover, calculating modulo A in both loops, we have

$$(\alpha(xy),0) \equiv f(xy,0)\equiv f((x,0)\cdot(y,0))\equiv f(x,0)*f(y,0)\equiv(\alpha x,0)*(\alpha y,0)\equiv(\alpha(x)\alpha(y),0),$$

and $\alpha \in \mathrm{Aut}(F)$ follows.

The isomorphism f satisfies

$$f(x,a) = f((1,a)\cdot(x,0)) = f(1,a)*f(x,0) = (1,\beta a)*(\alpha x,\tau x) = (\alpha x, \beta a+\tau x).$$

If is therefore the composition of the isomorphism $(x,a) \mapsto (x, a+\beta^{-1}\tau x)$ of Lemma 2.3 (with $\beta^{-1}\tau$ in place of τ) and of the isomorphism $(x,a)\mapsto(\alpha x,\beta a)$ of Lemma 3.1. This means that $\mu = {}^{(\alpha,\beta)}(\theta + \widehat{\beta^{-1}\tau})$, so $\mu \in {}^{(\alpha,\beta)}\theta + \mathrm{B}(F,A)$, $\theta \sim \mu$. □

We now investigate admissibility in abelian groups. The next two results can be proved in many ways from the Fundamental Theorem of Abelian Groups, which we use without warning.

Lemma 3.3. *Let p be a prime, and let*

$$A = \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_n}} \tag{3.1}$$

be an abelian p-group, where $e_1 \le \cdots \le e_n$. Let $x \in A$ be an element of order p. Then there exists a unique integer e_j such that: there is a complemented cyclic subgroup $B \le A$ satisfying $x \in B$ and $|B| = p^{e_j}$. Moreover,

$$A/\langle x\rangle \cong \mathbb{Z}_{p^{f_1}} \times \cdots \times \mathbb{Z}_{p^{f_n}},$$

where $f_i = e_i$ for every $i \ne j$, and $f_j = e_j - 1$.

Proof. Every element $x \in A$ of order p is of the form

$$x = (x_1 p^{e_1-1}, \dots, x_n p^{e_n-1}),$$

where $x_i \in \{0,\dots,p-1\}$ for every $1 \le i \le n$, and where $x_i \ne 0$ for some $1 \le i \le n$. Let j be the least integer such that $x_j \ne 0$. Consider the element

$$y = \frac{x}{p^{e_j-1}} = (0,\dots,0,x_j,x_{j+1}p^{e_{j+1}-e_j},\dots,x_n p^{e_n-e_j}).$$

Then $B = \langle y\rangle$ contains x, $|B| = p^{e_j}$, and

$$C = \mathbb{Z}_{p^{e_1}} \times \cdots \times Z_{p^{e_{j-1}}} \times 0 \times Z_{p^{e_{j+1}}} \times \cdots \times Z_{p^{e_n}}$$

is a complement of B in A (that is, $B\cap C = 0$ and $\langle B \cup C\rangle = A$). □

Proposition 3.4. *Let A be a finite abelian group. For a prime p dividing $|A|$ and for a finite abelian group F of order $|A|/p$, let*

$$X(p,F) = \{x \in A;\ |x| = p \text{ and } A/\langle x\rangle \cong F\}.$$

Then the sets $X(p,F)$ that are nonempty are precisely the orbits of the action of $\mathrm{Aut}(A)$ *on A.*

Proof. For a prime p, let A_p be the p-primary component of A. Then $A = A_{p_1}\times\cdots\times A_{p_m}$, for some distinct primes $p_1, \dots, p_m$, and $\mathrm{Aut}(A) = \mathrm{Aut}(A_{p_1})\times\cdots\times\mathrm{Aut}(A_{p_n})$. (For a detailed proof, see [8, Lemma 2.1].) We can therefore assume that $A = A_p$ is a p-group.

It is obvious that every orbit of $\mathrm{Aut}(A)$ is contained in one of the sets $X(p, F)$. It therefore suffices to prove that if x, $y \in X(p, F)$ then there is $\varphi \in \mathrm{Aut}(A)$ such that $\varphi(x) = y$.

Let A be as in (3.1). If A is cyclic of order p^{e_1} then $A/\langle x\rangle \cong \mathbb{Z}_{p^{e_1-1}}$, and we can assume that $x = ap^{e_1-1}$, $y = bp^{e_1-1}$, where $1 \le a$, $b \le p-1$. The automorphism of A determined by $1 \mapsto b/a$ (modulo p) then maps a to b and hence x to y.

Assume that $n > 1$. Let B_x, B_y be the complemented cyclic subgroups B obtained by Lemma 3.3 for x, y, respectively. Then $|B_x| = |B_y|$ since $A/\langle x\rangle \cong A/\langle y\rangle$, and hence the integer e_j determined by Lemma 3.3 is the same for x and y. We can in fact assume that already j is the same. Furthermore, we can assume that the isomorphism from

$$A/\langle x\rangle \cong \mathbb{Z}_{p^{e_1}}\times\cdots\times\mathbb{Z}_{p^{e_{j-1}}}\times B_x/\langle x\rangle\times\mathbb{Z}_{p^{e_{j+1}}}\times\cdots\times\mathbb{Z}_{p^{e_n}}$$

to

$$A/\langle y\rangle \cong \mathbb{Z}_{p^{e_1}}\times\cdots\times\mathbb{Z}_{p^{e_{j-1}}}\times B_y/\langle y\rangle\times\mathbb{Z}_{p^{e_{j+1}}}\times\cdots\times\mathbb{Z}_{p^{e_n}}$$

is componentwise, and maps $B_x/\langle x\rangle$ to $B_y/\langle y\rangle$. We can then extend $B_x/\langle x\rangle \to B_y/\langle y\rangle$ to an isomorphism $B_x \to B_y$ while sending x to y by the case $n = 1$, and hence obtain the desired automorphism of A. □

Corollary 3.5. *Let $Q = \mathcal{Q}(F, A, \theta)$ be an abelian group, $A = \mathbb{Z}_p$, p a prime. Then θ is admissible.*

Proof. Combine Propositions 3.2 and 3.4. □

Finally, we show that all cocycles are admissible in "small" situations.

Lemma 3.6. *There is no loop Q with $[Q : Z(Q)] = 2$.*

Proof. Assume, for a contradiction, that $|Q/Z(Q)| = 2$, and let $a \in Q \setminus Z(Q)$. Then every element of Q can be written as $a^i z$, where $i \in \{0, 1\}$ and $z \in Z(Q)$. For every i, j, $k \in \{0, 1\}$ and z_1, z_2, $z_3 \in Z(Q)$ we have $a^i z_1 \cdot (a^j z_2 \cdot a^k z_3) = a^i(a^j a^k)\cdot z_1 z_2 z_3$, and similarly, $(a^i z_1 \cdot a^j z_2)\cdot a^k z_3 = (a^i a^j)a^k \cdot z_1 z_2 z_3$. The two expressions are equal if any of i, j, k vanishes. So it remains to discuss the case $i = j = k = 1$. But then $a(aa) = (aa)a$, because $a^2 \in Z(Q)$. Hence Q is a group. It is well known that if Q is a group and $Q/Z(Q)$ is cyclic then $Q = Z(Q)$, a contradiction. □

Lemma 3.6 cannot be improved: for every odd prime p there is a nonassociative loop Q such that $|Q/Z(Q)| = p$, cf. Theorem 7.1.

Lemma 3.7. *Let $Q = \mathcal{Q}(F, A, \theta)$, $A = \mathbb{Z}_p$, p a prime. Assume further that one of the following conditions is satisfied:*

(i) $|Q| = p$,
(ii) $|Q| = pq$, *where q is a prime,*
(iii) $[Q : Z(Q)] \le 2$,
(iv) $|Q| < 12$.

Then θ is admissible.

Proof. When (i) or (iii) hold then Q is an abelian group by Lemma 3.6, and so θ is admissible by Corollary 3.5.

Assume that (ii) holds. If $Z(Q) > A$ then $Z(Q) = Q$ and we are done by Corollary 3.5. Else $Z(Q) = A$ and θ is admissible by Proposition 3.2, for trivial reasons.

To finish (iv), it remains to discuss the case $|Q| = 8$. If $Z(Q) = A$, θ is admissible by Proposition 3.2. If $Z(Q) > A$ then $Z(Q) = Q$ by Lemma 3.6, and we are done by Corollary 3.5. □

4. The invariant subspaces

For $(\alpha, \beta) \in \mathrm{Aut}(F, A)$, let

$$\mathrm{Inv}(\alpha, \beta) = \{\theta \in \mathrm{C}(F, A);\ \theta - {}^{(\alpha,\beta)}\theta \in \mathrm{B}(F, A)\}. \tag{4.1}$$

For $\emptyset \neq H \subseteq \mathrm{Aut}(F, A)$, let

$$\mathrm{Inv}(H) = \bigcap_{(\alpha,\beta)\in H} \mathrm{Inv}(\alpha, \beta). \tag{4.2}$$

Lemma 4.1. *Let $\emptyset \neq H \subseteq \mathrm{Aut}(F, A)$. Then $\mathrm{Inv}(H) = \mathrm{Inv}(\langle H\rangle)$.*

Proof. Assume that $\theta \in \mathrm{Inv}(\alpha, \beta) \cap \mathrm{Inv}(\gamma, \delta)$. Then $\theta - {}^{(\alpha,\beta)}\theta \in \mathrm{B}(F, A)$ and $\theta - {}^{(\gamma,\delta)}\theta \in \mathrm{B}(F, A)$. The second equation is equivalent to ${}^{(\alpha,\beta)}\theta - {}^{(\alpha,\beta)}({}^{(\gamma,\delta)}\theta) \in \mathrm{B}(F, A)$. Adding this to the first equation yields $\theta - {}^{(\alpha,\beta)}({}^{(\gamma,\delta)}\theta) = \theta - {}^{(\alpha\gamma,\beta\delta)}\theta \in \mathrm{B}(F, A)$. □

Corollary 4.2. *Let H, $K \leq \mathrm{Aut}(F, A)$. Then $\mathrm{Inv}(H) \cap \mathrm{Inv}(K) = \mathrm{Inv}(\langle H \cup K\rangle)$.*

For α, $\gamma \in \mathrm{Aut}(F)$ and β, $\delta \in \mathrm{Aut}(A)$, let ${}^{\gamma}\alpha = \gamma\alpha\gamma^{-1}$, ${}^{\delta}\beta = \delta\beta\delta^{-1}$.

Lemma 4.3. *Let (α, β), $(\gamma, \delta) \in \mathrm{Aut}(F, A)$. Then $\theta \in \mathrm{Inv}(\alpha, \beta)$ if and only if ${}^{(\gamma,\delta)}\theta \in \mathrm{Inv}({}^{\gamma}\alpha, {}^{\delta}\beta)$.*

Proof. The following conditions are equivalent:

$$\begin{aligned}
{}^{(\gamma,\delta)}\theta &\in \mathrm{Inv}({}^{\gamma}\alpha, {}^{\delta}\beta),\\
{}^{(\gamma,\delta)}\theta - {}^{({}^{\gamma}\alpha,{}^{\delta}\beta)}({}^{(\gamma,\delta)}\theta) &\in \mathrm{B}(F, A),\\
{}^{(\gamma,\delta)}\theta - {}^{(\gamma\alpha,\delta\beta)}\theta &\in \mathrm{B}(F, A),\\
{}^{(\gamma,\delta)}(\theta - {}^{(\alpha,\beta)}\theta) &\in \mathrm{B}(F, A),\\
\theta - {}^{(\alpha,\beta)}\theta &\in \mathrm{B}(F, A),\\
\theta &\in \mathrm{Inv}(\alpha, \beta).
\end{aligned}$$

□

For $\emptyset \neq H \leq \mathrm{Aut}(F, A)$, let

$$\mathrm{Inv}^*(H) = \{\theta \in \mathrm{C}(F, A);\ \theta \in \mathrm{Inv}(\alpha, \beta) \text{ if and only if } (\alpha, \beta) \in H\},$$
$$\mathrm{Inv}^*_c(H) = \bigcup_{(\alpha,\beta)\in\mathrm{Aut}(F,A)} \mathrm{Inv}^*({}^{(\alpha,\beta)}H).$$

As we are going to see, the cardinality of the equivalence class $[\theta]_\sim$ can be easily calculated for $\theta \in \mathrm{Inv}^*(H)$, provided θ is admissible.

If G is a group and $H \leq G$, let $N_G(H) = \{a \in G;\ {}^{a}H = H\}$ be the normalizer of H in G.

Lemma 4.4. *Let $H \leq G = \mathrm{Aut}(F, A)$. Then $|\mathrm{Inv}^*_c(H)| = |\mathrm{Inv}^*(H)| \cdot [G : N_G(H)]$.*

Proof. Since ${}^{a}H = {}^{b}H$ if and only if $a^{-1}b \in N_G(H)$, there are precisely $[G : N_G(H)]$ subgroups K of G conjugate to H.

Assume that $K \neq H$ are conjugate, $K = {}^{(\alpha,\beta)}H$. The mapping $f : \mathrm{C}(F, A) \to \mathrm{C}(F, A)$, $\theta \mapsto {}^{(\alpha,\beta)}\theta$ is a bijection. By Lemma 4.3, $f(\mathrm{Inv}(H)) = \mathrm{Inv}(K)$, and $f(\mathrm{Inv}^*(H)) =$

$\mathrm{Inv}^*(K)$, proving $|\mathrm{Inv}^*(H)| = |\mathrm{Inv}^*(K)|$. Since $K \neq H$, we have $\mathrm{Inv}^*(H) \cap \mathrm{Inv}^*(K) = \emptyset$ by definition. □

For a group G, denote by $\mathrm{Sub}_c(G)$ a set of subgroups of G such that for every $H \leq G$ there is precisely one $K \in \mathrm{Sub}_c(G)$ such that K is conjugate to H.

Theorem 4.5. *Let F be a loop and A an abelian group. Assume that θ is admissible for every $\theta \in \mathrm{C}(F,A)$. Let $G = \mathrm{Aut}(F,A)$. Then there are*

$$\sum_{H \in \mathrm{Sub}_c(G)} \frac{|\mathrm{Inv}^*_c(H)|}{|\mathrm{B}(F,A)| \cdot [G:H]} = \sum_{H \in \mathrm{Sub}_c(G)} \frac{|\mathrm{Inv}^*(H)|}{|\mathrm{B}(F,A)| \cdot [N_G(H):H]} \tag{4.3}$$

central extensions of A by F, up to isomorphism.

Proof. By Lemma 4.1,

$$\mathrm{C}(F,A) = \bigcup_{H \leq G} \mathrm{Inv}^*(H) = \bigcup_{H \in \mathrm{Sub}_c(G)} \mathrm{Inv}^*_c(H),$$

where the unions are disjoint. Let $\theta \in \mathrm{Inv}^*_c(H)$, for some $H \leq G$. Since θ is admissible, we have

$$[\theta]_\sim = \bigcup_{(\alpha,\beta) \in G} ({}^{(\alpha,\beta)}\theta + \mathrm{B}(F,A)) \subseteq \mathrm{Inv}^*_c(H),$$

where the equality follows by admissibility of θ, and the inclusion from Lemma 4.3.

Let K be the unique conjugate of H such that $\theta \in \mathrm{Inv}^*(K)$. We have ${}^{(\alpha,\beta)}\theta - {}^{(\gamma,\delta)}\theta \in \mathrm{B}(F,A)$ if and only if $\theta - {}^{(\alpha^{-1}\gamma,\beta^{-1}\delta)}\theta \in \mathrm{B}(F,A)$, which holds if and only if $\theta \in \mathrm{Inv}(\alpha^{-1}\gamma, \beta^{-1}\delta)$. Since $\theta \in \mathrm{Inv}^*(K)$, we see that ${}^{(\alpha,\beta)}\theta - {}^{(\gamma,\delta)}\theta \in \mathrm{B}(F,A)$ holds if and only if $(\alpha^{-1}\gamma, \beta^{-1}\delta) \in K$, or $(\alpha,\beta)K = (\gamma,\delta)K$. Hence $[\theta]_\sim$ is a union of $[G:K] = [G:H]$ cosets of $\mathrm{B}(F,A)$. We have established the first sum of (4.3). The second sum then follows from Lemma 4.4. □

5. Calculating the subspaces $\mathrm{Inv}(\alpha,\beta)$ by computer

Assume throughout this subsection that $A = \mathbb{Z}_p$, where p is a prime. Then $\mathrm{C}(F,A)$, $\mathrm{B}(F,A)$ and $\mathrm{H}(F,A)$ are vector spaces over $\mathrm{GF}(p)$.

For $(\alpha,\beta) \in \mathrm{Aut}(F,A)$ let $R = R(\alpha,\beta)$, $S = S(\alpha,\beta)$ be the linear operators $\mathrm{C}(F,A) \to \mathrm{C}(F,A)$ defined by

$$R(\alpha,\beta)\theta = {}^{(\alpha,\beta)}\theta,$$
$$S(\alpha,\beta)\theta = \theta - {}^{(\alpha,\beta)}\theta.$$

Hence $R(\alpha,\beta)$ is invertible, and $S(\alpha,\beta) = I - R(\alpha,\beta)$, where $I : \mathrm{C}(F,A) \to \mathrm{C}(F,A)$ is the identity operator.

As $\beta \in \mathrm{Aut}(\mathbb{Z}_p)$ is a scalar multiplication by $\beta(1)$, let us identify β with $\beta(1)$. Then $R(\alpha,\beta)$ is a matrix operator with rows and columns labeled by pairs of non-identity elements of F, where the only nonzero coefficient in row (x,y) is $-\beta$ in column $(\alpha^{-1}x, \alpha^{-1}y)$.

By definition of $\mathrm{Inv}(\alpha,\beta)$ and $S(\alpha,\beta)$, we have

$$\mathrm{Inv}(\alpha,\beta) = \{\theta \in \mathrm{C}(F,A);\ S(\alpha,\beta)\theta \in \mathrm{B}(F,A)\} = S(\alpha,\beta)^{-1}\mathrm{B}(F,A).$$

In order to calculate $\mathrm{Inv}(\alpha,\beta)$, we can proceed as follows:

- calculate the subspace $\mathrm{B}(F,A)$ as the span of $\{\widehat{\tau_c};\ 1 \neq c \in F\}$,
- calculate the kernel $\mathrm{Ker}\, S(\alpha,\beta)$ and image $\mathrm{Im}\, S(\alpha,\beta)$ as usual,
- find a basis $\mathcal{B}$ of the subspace $\mathrm{B}(F,A) \cap \mathrm{Im}\, S(\alpha,\beta)$,

- for $b \in \mathcal{B}$, find a particular solution θ_b to the system $S(\alpha,\beta)\theta_b = b$,
- then $\mathrm{Inv}(\alpha,\beta) = \mathrm{Ker}\, S(\alpha,\beta) \oplus \langle \theta_b;\ b \in \mathcal{B}\rangle$.

In particular, with $S = S(\alpha,\beta)$, we have

$$\begin{aligned}\dim \mathrm{Inv}(\alpha,\beta) &= \dim \mathrm{Ker}\, S + \dim(\mathrm{Im}\, S \cap \mathrm{B}(F,A))\\ &= \dim \mathrm{Ker}\, S + \dim \mathrm{Im}\, S + \dim \mathrm{B}(F,A) - \dim(\mathrm{Im}\, S + \mathrm{B}(F,A))\\ &= (|F|-1)^2 + \dim \mathrm{B}(F,A) - \dim(\mathrm{Im}\, S + \mathrm{B}(F,A)).\end{aligned}$$

Using a computer, it is therefore not difficult to find $\mathrm{Inv}(\alpha,\beta)$ and its dimension even for rather large loops $A = \mathbb{Z}_p$ and F. See §9 for more details.

Remark 5.1. *If it is preferable to operate modulo coboundaries, note that* $S(\alpha,\beta)(\theta + \widehat{\tau}) = S(\alpha,\beta)\theta + \tau - \widehat{\beta\tau\alpha^{-1}}$, *and view* $S(\alpha,\beta)$ *as a linear operator* $S(\alpha,\beta) : \mathrm{H}(F,A) \to \mathrm{H}(F,A)$ *defined by*

$$S(\alpha,\beta)(\theta + \mathrm{B}(F,A)) = (\theta - {}^{(\alpha,\beta)}\theta) + \mathrm{B}(F,A).$$

Then $\mathrm{Inv}(\alpha,\beta)/\mathrm{B}(F,A) = \mathrm{Ker}\, S(\alpha,\beta)$.

6. The subspaces $\mathrm{Inv}(\alpha,\beta)$ for $A = \mathbb{Z}_p$, $F = \mathbb{Z}_q$

If $H \le K \le \mathrm{Aut}(F,A)$, we have $\mathrm{Inv}(K) \le \mathrm{Inv}(H)$. Hence the subgroups $\mathrm{Inv}(H)$ will be incident in accordance with the upside down subgroup lattice of $\mathrm{Aut}(F,A)$, except that some edges in the lattice can collapse, i.e., it can happen that $\mathrm{Inv}(H) = \mathrm{Inv}(K)$ although $H < K$:

Example 6.1. *Let* $A = \mathbb{Z}_2$, $F = \mathbb{Z}_2 \times \mathbb{Z}_2$. *Then* $\mathrm{Aut}(F) \cong S_3$. *Let* H *be the subgroup of* $\mathrm{Aut}(F)$ *generated by a* 3*-cycle. Then it turns out that* $\mathrm{Inv}(H) = \mathrm{Inv}(\mathrm{Aut}(F))$.

Such a collapse has no impact on the formula (4.3) of Theorem 4.5, since only subgroups H with $\mathrm{Inv}^*(H) \ne \emptyset$ contribute to it.

We proceed to determine $\dim \mathrm{Inv}(\alpha,\beta)$.

In addition to the operators $R(\alpha,\beta)$ and $S(\alpha,\beta)$ on $\mathrm{C}(F,A)$, define $T(\alpha,\beta)$ by

$$T(\alpha,\beta)\theta = \theta + R(\alpha,\beta)\theta + \cdots + R(\alpha,\beta)^{k-1}\theta,$$

where $k = |\alpha|$.

Lemma 6.2. *Let* R, S, T *be operators on a finite-dimensional vector space* V *such that* $R^k = I$, $S = I - R$, $T = I + R + \cdots + R^{k-1}$. *Then* $\mathrm{Im}\, T \le \mathrm{Ker}\, S$ *and* $\mathrm{Im}\, S \le \mathrm{Ker}\, T$. *If* $\mathrm{Im}\, T = \mathrm{Ker}\, S$ *then* $\mathrm{Ker}\, T = \mathrm{Im}\, S$.

Proof. We have $TS = (I + R + \cdots + R^{k-1})(I - R) = (I + R + \cdots + R^{k-1}) - (R + R^2 + \cdots + R^k) = I - R^k = 0$ and $ST = (I - R)(I + R + \cdots + R^{k-1}) = TS$, which shows $\mathrm{Im}\, T \le \mathrm{Ker}\, S$, $\mathrm{Im}\, S \le \mathrm{Ker}\, T$.

Assume that $\mathrm{Im}\, T = \mathrm{Ker}\, S$. By the Fundamental Homomorphism Theorem,

$$\dim \mathrm{Im}\, T + \dim \mathrm{Ker}\, T = \dim V = \dim \mathrm{Im}\, S + \dim \mathrm{Ker}\, S = \dim \mathrm{Im}\, S + \dim \mathrm{Im}\, T,$$

so $\dim \mathrm{Ker}\, T = \dim \mathrm{Im}\, S$. Since $\mathrm{Im}\, S \le \mathrm{Ker}\, T$, we conclude that $\mathrm{Im}\, S = \mathrm{Ker}\, T$. □

Lemma 6.3. *Let* p, q *be primes,* $A = \mathbb{Z}_p$, $F = \mathbb{Z}_q$, $\alpha \in \mathrm{Aut}(F)$, $\beta \in \mathrm{Aut}(A)$.

(i) *If* $|\beta|$ *does not divide* $|\alpha|$ *then* $S(\alpha,\beta)$ *is invertible.*
(ii) *If* $|\beta|$ *divides* $|\alpha|$ *then* $\mathrm{Ker}\, S(\alpha,\beta) = \mathrm{Im}\, T(\alpha,\beta)$ *and* $\dim \mathrm{Ker}\, S(\alpha,\beta) = (q-1)^2/|\alpha|$.

Proof. Let $F^* = F \setminus \{0\}$, $k = |\alpha|$. The automorphism α acts on $F^* \times F^*$ via $(x,y)^\alpha = (\alpha^{-1}x, \alpha^{-1}y)$. Every α-orbit has size k. Let $t = (q-1)^2/k$, and let $\mathcal{O}_1, \dots, \mathcal{O}_t$ be all the distinct α-orbits on $F^* \times F^*$.

Let $R = R(\alpha,\beta)$, $S = S(\alpha,\beta)$, $T = T(\alpha,\beta)$. Throughout the proof, let $\theta \in \operatorname{Ker} S$, i.e.,

$$\theta(x,y) = \beta\theta(\alpha^{-1}x, \alpha^{-1}y) \tag{6.1}$$

for every x, $y \in F^*$. For every $1 \le i \le t$, let $(x_i, y_i) \in \mathcal{O}_i$. Define $\theta_i \in \mathrm{C}(F,A)$ by

$$\theta_i(x,y) = \begin{cases} \theta(x_i,y_i), & \text{if } (x,y) = (x_i,y_i), \\ 0, & \text{otherwise.} \end{cases}$$

Then

$$\theta = \sum_{i=1}^t T\theta_i = T(\sum_{i=1}^t \theta_i),$$

thus $\operatorname{Ker} S \le \operatorname{Im} T$.

The condition (6.1) implies $\theta(x,y) = \beta^k\theta(x,y)$ for every x, $y \in F^*$. If $|\beta|$ does not divide $|\alpha|$, we have $\beta^k \ne 1$, and therefore $\theta = 0$, proving $\operatorname{Ker} S = 0$.

Assume that $|\beta|$ divides $|\alpha|$. Then $R^k = I$, and $\operatorname{Im} T \le \operatorname{Ker} S$ by Lemma 6.2. Thus $\operatorname{Im} T = \operatorname{Ker} S$ and $\operatorname{Ker} T = \operatorname{Im} S$. Since θ is determined by the values $\theta(x_i, y_i)$, for $1 \le i \le t$, and since these values can be arbitrary, we see that $\dim \operatorname{Ker} S = t$. □

Lemma 6.4. *Let p, q be distinct primes, $A = \mathbb{Z}_p$, $F = \mathbb{Z}_q$, $\alpha \in \operatorname{Aut}(F)$, $\beta \in \operatorname{Aut}(A)$, and assume that $|\beta|$ divides $|\alpha|$. Then*

$$\dim\left(\operatorname{Ker} T(\alpha,\beta) \cap \mathrm{B}(F,A)\right) = (q-1)\left(1 - \frac{1}{|\alpha|}\right).$$

Proof. The set $\{\widehat{\tau_c};\ c \in F^*\}$ is linearly independent thanks to $p \ne q$. Let

$$\widehat{\tau} = \sum_{c\in F^*} \lambda_c \widehat{\tau_c},$$

for some $\lambda_c \in A$. An inspection of (2.4) reveals that

$$R(\alpha,\beta)\widehat{\tau_c} = \beta\widehat{\tau_{\alpha c}}. \tag{6.2}$$

Thus $\widehat{\tau}$ belongs to $\operatorname{Ker} T(\alpha,\beta) \cap \mathrm{B}(F,A)$ if and only if

$$\sum_c \lambda_c\widehat{\tau_c} + \beta\sum_c \lambda_c\widehat{\tau_{\alpha c}} + \cdots + \beta^{k-1}\sum_c \lambda_c\widehat{\tau_{\alpha^{(k-1)}c}} = 0. \tag{6.3}$$

The coefficient of $\widehat{\tau_c}$ in (6.3) is $\lambda_c + \beta\lambda_{\alpha^{-1}c} + \cdots + \beta^{k-1}\lambda_{\alpha^{-(k-1)}c}$, so the system (6.3) can be rewritten in terms of the coefficients λ_c as

$$\lambda_c + \beta\lambda_{\alpha^{-1}c} + \cdots + \beta^{k-1}\lambda_{\alpha^{-(k-1)}c} = 0, \text{ for } c \in F^*. \tag{6.4}$$

For any $1 \le i \le k$, the equation for c is a scalar multiple of the equation for $\alpha^i c$. On the other hand, each equation involves scalars c from only one orbit of α. Hence (6.4) reduces to a system of $(q-1)/|\alpha|$ linearly independent equations in variables λ_c, $c \in F^*$. It follows that the subspace of homogeneous solutions has dimension $(q-1)(1-1/|\alpha|)$. □

Theorem 6.5. *Let $p \ne q$ be primes, $A = \mathbb{Z}_p$, $F = \mathbb{Z}_q$, $\alpha \in \operatorname{Aut}(F)$, $\beta \in \operatorname{Aut}(A)$. Then*

$$\operatorname{Inv}(\alpha,\beta) = \operatorname{Ker} S(\alpha,\beta) + \mathrm{B}(F,A).$$

Moreover,

$$\dim(\operatorname{Inv}(\alpha,\beta)) = \begin{cases} q-1, & \text{if } |\beta| \text{ does not divide } |\alpha|, \\ (q-1) + (q-1)(q-2)/|\alpha|, & \text{otherwise.} \end{cases}$$

Thus

$$\dim(\mathrm{Inv}(\alpha,\beta)/\mathrm{B}(F,A)) = \begin{cases} 0, & \text{if } |\beta| \text{ does not divide } |\alpha|, \\ (q-1)(q-2)/|\alpha|, & \text{otherwise.} \end{cases}$$

Proof. Let $R = R(\alpha,\beta)$, $S = S(\alpha,\beta)$, $T = T(\alpha,\beta)$ and $B = \mathrm{B}(F,A)$. Assume that $|\beta|$ does not divide $|\alpha|$. Then S is invertible by Lemma 6.3, so $\mathrm{Inv}(\alpha,\beta) = S^{-1}B = B = \operatorname{Ker} S + B$, and we have $\dim \mathrm{Inv}(\alpha,\beta) = \dim B = q-1$ thanks to $p \neq q$.

Now assume that $|\beta|$ divides $|\alpha|$. By Lemmas 6.2, 6.3 and 6.4, we have $\operatorname{Im} T = \operatorname{Ker} S$, $\dim(\operatorname{Im} S \cap B) = (q-1)(1-1/|\alpha|)$, and $\dim \operatorname{Ker} S = (q-1)^2/|\alpha|$, so

$$\begin{aligned} \dim \mathrm{Inv}(\alpha,\beta) &= \dim \operatorname{Ker} S + \dim(\operatorname{Im} S \cap B) \\ &= (q-1)^2/|\alpha| + (q-1)(1-1/|\alpha|) \\ &= (q-1) + (q-1)(q-2)/|\alpha|. \end{aligned}$$

It remains to show that $\mathrm{Inv}(\alpha,\beta) = \operatorname{Ker} S + B$.

Let $k = |\alpha|$. The coboundaries $\{\widehat{\tau_c};\ c \in F^*\}$ are linearly independent thanks to $p \neq q$. For $1 \le i \le m = (q-1)/k$, let c_i be a representative of the coset $c_i\langle\alpha\rangle$ in F^*, and assume that $\bigcup_{i=1}^m c_i\langle\alpha\rangle = F^*$. By (6.2), the set $\{R^\ell\widehat{\tau_{c_i}};\ 0 \le \ell \le k-2,$ $1 \le i \le m\}$ is linearly independent, and so is its S-image $\{R^\ell\widehat{\tau_{c_i}} - R^{\ell+1}\widehat{\tau_{c_i}};\ 0 \le \ell \le k-2,$ $1 \le i \le m\} \subseteq B$. This shows that $\dim(S(B) \cap B) \ge (q-1)(1-1/k)$. On the other hand, $\dim(\operatorname{Im} S \cap B) = (q-1)(1-1/k)$ by Lemma 6.4. Thus $\operatorname{Im} S \cap B = S(B) \cap B = S(B)$. But this means that $\mathrm{Inv}(\alpha,\beta) = S^{-1}B$ is equal to $\operatorname{Ker} S + B$. □

7. Nilpotent loops of order $2q$, q a prime

For $n \ge 1$, let $\mathcal{N}(n)$ be the number of nilpotent loops of order n up to isomorphism. In this section we find a formula for $\mathcal{N}(2q)$, where q is a prime, and describe the asymptotic behavior of $N(2q)$ as $q \to \infty$.

Loops of order 4 are associative, and, up to isomorphism, there are 2 nilpotent groups of order 4, namely $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Theorem 7.1. *Let q be an odd prime. For a positive integer d, let*

$$\mathrm{Pred}(d) = \{d';\ 1 \le d' < d,\ d/d' \text{ is a prime}\}$$

be the set of all maximal proper divisors of d. Then the number of nilpotent loops of order $2q$ up to isomorphism is

$$\mathcal{N}(2q) = \sum_{d \text{ divides } q-1} \frac{1}{d}\left(2^{(q-2)d} + \sum_{\emptyset \neq D \subseteq \mathrm{Pred}(d)} (-1)^{|D|} \cdot 2^{(q-2)\gcd D}\right). \tag{7.1}$$

Proof. By Lemma 3.6, the only central extension of $\mathbb{Z}_q$ by $\mathbb{Z}_2$ is the cyclic group $\mathbb{Z}_{2q}$. Since this group can also be obtained as a central extension of $\mathbb{Z}_2$ by $\mathbb{Z}_q$, we can set $A = \mathbb{Z}_2$, $F = \mathbb{Z}_q$. Then by Lemma 3.7, every $\theta \in \mathrm{C}(F,A)$ is admissible, so Theorem 4.5 applies.

We have $\mathrm{Aut}(F,A) = \mathrm{Aut}(F) = \langle\alpha\rangle \cong \mathbb{Z}_{q-1}$. The subgroup structure of $\mathrm{Aut}(F)$ is therefore transparent: for every divisor d of $q-1$ there is a unique subgroup $H_d = \langle\alpha^d\rangle$ of order $(q-1)/d$, and if d, d' are two divisors of $q-1$ then $\langle H_d \cup H_{d'}\rangle = H_{\gcd(d,d')}$.

By Theorem 6.5,

$$\dim \mathrm{Inv}(H_d) = \dim \mathrm{Inv}(\alpha^d) = (q-1) + (q-1)(q-2)/((q-1)/d) = (q-1) + (q-2)d,$$

so $\dim(\mathrm{Inv}(H_d)/\mathrm{B}(F,A)) = (q-2)d$.

TABLE 1. The number $\mathcal{N}(2q)$ of nilpotent loops of order $2q$, q a prime, up to isomorphism.

$2q$	$\mathcal{N}(2q)$
4	2
6	3
10	1,044
14	178,962,784
22	123,794,003,928,541,545,927,226,368
26	453,709,822,561,251,284,623,981,727,533,724,162,048
34	110,427,941,548,649,020,598,956,093,796,432,407,322,294,493,291,283,427,083,203,517,192,617,984

Note that H_d is a maximal subgroup of $H_{d'}$ if and only if $d' \in \mathrm{Pred}(d)$. For $\emptyset \neq D \subseteq \mathrm{Pred}(d)$, we have $\langle H_{d'};\ d' \in D\rangle = H_{\gcd D}$, and so

$$\bigcap_{d' \in D} \mathrm{Inv}(H_{d'}) = \mathrm{Inv}(H_{\gcd D})$$

by Corollary 4.2. Then

$$|\mathrm{Inv}^*(H_d)| = |\mathrm{Inv}(H_d)| + \sum_{\emptyset \neq D \subseteq \mathrm{Pred}(d)} (-1)^{|D|} \cdot |\mathrm{Inv}(H_{\gcd D})|$$

by the principle of inclusion and exclusion.

As $\mathrm{Aut}(F)$ is abelian, $[N_{\mathrm{Aut}(F)}(H_d) : H_d] = [\mathrm{Aut}(F) : H_d] = d$. The formula (7.1) then follows by Theorem 4.5. □

Example 7.2. *To illustrate* (7.1)*, let us determine* $\mathcal{N}(14) = \mathcal{N}(2 \cdot 7)$*. The divisors of* $q - 1 = 6$ *are* 6*,* 3*,* 2*,* 1*. Hence*

(7.2)

$$\mathcal{N}(14) = (2^{5\cdot 6} - 2^{5\cdot 3} - 2^{5\cdot 2} + 2^{5\cdot 1})/6 + (2^{5\cdot 3} - 2^{5\cdot 1})/3 + (2^{5\cdot 2} - 2^{5\cdot 1})/2 + 2^{5\cdot 1}/1 = 178,962,784.$$

Table 1 lists the number of nilpotent loops of order $2q$ up to isomorphism for small primes q. (It is by no means difficult to evaluate (7.1) for larger primes, say up to $q \leq 100$, but the decimal expansion of $\mathcal{N}(2q)$ becomes too long to display neatly in a table.)

Here is the asymptotic growth of $\mathcal{N}(2q)$:

Theorem 7.3. *Let* q *be an odd prime. Then the number of nilpotent loops of order* $2q$ *up to isomorphism is approximately* $2^{(q-2)(q-1)}/(q-1)$*. More precisely,*

$$\lim_{q \text{ prime},\ q \to \infty} \mathcal{N}(2q) \cdot \frac{q-1}{2^{(q-2)(q-1)}} = 1.$$

Proof. We prove the assertion by a simple estimate. To illustrate the main idea, note that (7.2) can be rewritten as

$$2^{30}/6 + 2^{15}(1/3 - 1/6) + 2^{10}(1/2 - 1/6) + 2^{5}(1 - 1/2 - 1/3 + 1/6).$$

Thus, upon rewriting (7.1) in a similar fashion, there will be no more than $q - 1$ summands, each of the form

$$2^{(q-2)d'}(1/d_1 \pm 1/d_2 \pm \cdots \pm 1/d_m). \tag{7.3}$$

A reciprocal $1/d$ appears in (7.3) if and only if there is a divisor d of $q-1$ and $D \subseteq \mathrm{Pred}(d)$ such that $\gcd D = d'$. Now, for every divisor d of $q - 1$ there is at most one subset $D \subseteq \mathrm{Pred}(d)$ such that $\gcd D = d'$ (because if $D = \{e_1, \ldots, e_n\}$, $d/e_i = p_i$ is a prime, then $\gcd D = d/(p_1 \cdots p_n)$ uniquely determines D). Hence the number of reciprocals in (7.3) cannot exceed $q-1$. Finally, the largest proper divisor of $q-1$ is $(q-1)/2$. Altogether,

$$\frac{2^{(q-2)(q-1)}}{q-1} - (q-1)2^{(q-2)(q-1)/2}(q-1) \leq N(2q) \leq \frac{2^{(q-2)(q-1)}}{q-1} + (q-1)2^{(q-2)(q-1)/2}(q-1),$$

thus

$$1 - \frac{(q-1)^3}{2^{(q-2)(q-1)/2}} \leq N(2q) \cdot \frac{(q-1)}{2^{(q-2)(q-1)}} \leq 1 + \frac{(q-1)^3}{2^{(q-2)(q-1)/2}},$$

and the result follows by the Squeeze Theorem. □

8. Inadmissible cocycles

Let $A = \mathbb{Z}_p$, F be as usual. The easiest (but slow) way to deal with inadmissible cocycles $\theta \in \mathrm{C}(F, A)$ is to treat separately the subset

$$W(F, A) = \{\theta \in \mathrm{C}(F, A);\ Z(\mathcal{Q}(F, A, \theta)) > A\} \subseteq \mathrm{C}(F, A).$$

We will refer to elements of $W(F, A)$ informally as *large center cocycles*. Note that the adjective "large" is relative to A. The subset $W(F, A)$ can be determined computationally as follows:

Let $Q = \mathcal{Q}(F, A, \theta)$. The element (x, a) belongs to $Z(Q)$ if and only if $\{(x, b);\ b \in A\} \subseteq Z(Q)$, which happens if and only if $x \in Z(F)$ and θ satisfies

$$\begin{aligned}
\theta(x, y) &= \theta(y, x),\\
\theta(x, y) + \theta(xy, z) &= \theta(y, z) + \theta(x, yz),\\
\theta(y, x) + \theta(yx, z) &= \theta(x, z) + \theta(y, xz),\\
\theta(y, z) + \theta(yz, x) &= \theta(z, x) + \theta(y, zx)
\end{aligned}$$

for all y, $z \in F$. The first condition ensures that (x, a) commutes with all elements of Q, and the last three conditions ensure that (x, a) associates with all elements of Q, no matter in which position (x, a) happens to be in the associative law. (Note that the last condition is a consequence of the first three.)

Hence for every $1 \neq x \in Z(F)$ we can solve the above linear equations and obtain the subspace $W_x(F, A) \leq \mathrm{C}(F, A)$ such that $\theta \in W_x(F, A)$ if and only if $(x, A) \subseteq Z(\mathcal{Q}(F, A, \theta))$. Then

$$W(F, A) = \bigcup_{1 \neq x \in Z(F)} W_x(F, A),$$

and this subset can be determined by the principle of inclusion and exclusions on the subspaces $W_x(F, A)$, $1 \neq x \in Z(F)$.

Importantly, every cocycle $\theta \in \mathrm{C}(F, A) \setminus W(F, A)$ is admissible, since then $\mathcal{Q}(F, A, \theta)$ possesses a unique central subloop of the cardinality $|A|$, namely A.

When A, F are small, we can complete the isomorphism problem by first constructing the loops $\mathcal{Q}(F, A, \theta)$ for all $\theta \in W(F, A)/\mathrm{B}(F, A)$ and then sorting them up to isomorphism by standard algorithms of loop theory. Since these algorithms are slow, dealing with large center cocycles is the main obstacle in pushing the enumeration of nilpotent loops past order $n = 23$.

Table 2. The number of nilpotent loops up to isomorphism.

n	A	F	$\#Q$, $Z(Q) > A$	$\#Q$
4	$\mathbb{Z}_2$	$\mathbb{Z}_2$	2	2
6	$\mathbb{Z}_2$	$\mathbb{Z}_3$	1	3
8	$\mathbb{Z}_2$	$\mathbb{Z}_4$	2	80
8	$\mathbb{Z}_2$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	2	60
8	$\mathbb{Z}_2$	4	3	139
9	$\mathbb{Z}_3$	$\mathbb{Z}_3$	2	10
10	$\mathbb{Z}_2$	$\mathbb{Z}_5$	1	$1,044$
12	$\mathbb{Z}_2$	$\mathbb{Z}_6$	6	$1,049,560$
12	$\mathbb{Z}_2$	$L_{6,2}$	4	$1,048,576$
12	$\mathbb{Z}_2$	$L_{6,3}$	4	$525,312$
12	$\mathbb{Z}_2$	6	11	$2,623,485$
12	$\mathbb{Z}_3$	$\mathbb{Z}_4$	1	196
12	$\mathbb{Z}_3$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	1	76
12	$\mathbb{Z}_3$	4	2	272
12				$2,623,755$
14	$\mathbb{Z}_2$	$\mathbb{Z}_7$	1	$178,962,784$
15	$\mathbb{Z}_3$	$\mathbb{Z}_5$	1	$66,626$
15	$\mathbb{Z}_5$	$\mathbb{Z}_3$	1	5
15				$66,630$
16	$\mathbb{Z}_2$	8	$9,284$	$466,409,543,467,341$
18	$\mathbb{Z}_2$	9	34	$157,625,987,549,892,128$
18	$\mathbb{Z}_3$	$\mathbb{Z}_6$	10	$2,615,147,350$
18	$\mathbb{Z}_3$	$L_{6,2}$	14	$5,230,176,602$
18	$\mathbb{Z}_3$	L_{6_3}	10	$2,615,147,350$
18	$\mathbb{Z}_3$	6	34	$10,460,471,302$
18				$157,625,998,010,363,396$
20	$\mathbb{Z}_2$	10	$2,798,987$	$4,836,883,870,081,433,134,082,379$
20	$\mathbb{Z}_5$	$\mathbb{Z}_4$	1	$1,985$
20	$\mathbb{Z}_5$	$\mathbb{Z}_2 \times \mathbb{Z}_2$	1	685
20	$\mathbb{Z}_5$	4	2	$2,670$
20				$4,836,883,870,081,433,134,085,047$
21	$\mathbb{Z}_3$	$\mathbb{Z}_7$	1	$17,157,596,742,628$
21	$\mathbb{Z}_7$	$\mathbb{Z}_3$	1	6
21				$17,157,596,742,633$
22	$\mathbb{Z}_2$	$\mathbb{Z}_{11}$	1	$123,794,003,928,541,545,927,226,368$

9. Enumeration of nilpotent loops of order less than 24

The results are summarized in Table 2. A typical line of the table can be read as follows: "$\#Q$" is the number of nilpotent loops (up to isomorphism) of order n that are central extensions of the cyclic group $A = \mathbb{Z}_p$ by the nilpotent loop F of order n/p. If only the order of F is given, F is any of the nilpotent loops of order n/p. If no information about A and F is given, any pair (A, F) with $A = \mathbb{Z}_p$, F nilpotent of order n/p can be used. Finally, "$\#Q$, $Z(Q) > A$" is the number of nilpotent loops with center larger than A. Since this makes sense only when A is specified, we omit "$\#Q$, $Z(Q) > A$" in the other cases.

By Lemma 3.7, we can apply the formula (4.3) safely until we reach order $n = 12$.

For every prime p there is a unique nilpotent loop of order p up to isomorphism, namely the cyclic group $\mathbb{Z}_p$.

The number of nilpotent loops of order $2q$, q a prime, is determined by Theorem 7.1. Note, however, that the theorem does not produce the loops. Since we need all nilpotent loops of order 6 and 10 explicitly in order to compute the number of nilpotent loops of order 12, 18 and 20, we must obtain the nilpotent loops of order 6, 10 by other means (a direct isomorphism check on $\mathrm{H}(F, A)$ will do).

In accordance with Theorem 7.1, there are 3 nilpotent loops of order 6. Beside the cyclic group of order 6, the other two loops are

$L_{6,2}$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	3	6	5
3	3	4	5	6	1	2
4	4	3	6	5	2	1
5	5	6	2	1	3	4
6	6	5	1	2	4	3.

,

$L_{6,3}$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	3	6	5
3	3	4	5	6	1	2
4	4	3	6	5	2	1
5	5	6	1	2	4	3
6	6	5	2	1	3	4

.

9.1. **n=8.** Case $A = \mathbb{Z}_2$, $F = \mathbb{Z}_4$. We have $\mathrm{Aut}(A) = 1$, $\mathrm{Aut}(F) = \langle\alpha\rangle \cong \mathbb{Z}_2$, and $\dim \mathrm{Hom}(F, A) = 1$, $\dim \mathrm{B}(F, A) = 2$, $\dim \mathrm{C}(F, A) = 9$. Computer yields $\dim \mathrm{Inv}(\alpha) = 7$. Hence (4.3) shows that there are

$$\frac{2^7}{2^2} + \frac{2^9 - 2^7}{2^2 \cdot 2} = 80$$

central extensions of $\mathbb{Z}_2$ by $\mathbb{Z}_4$, up to isomorphism.

Case $A = \mathbb{Z}_2$, $F = \mathbb{Z}_2 \times \mathbb{Z}_2$. We have $\mathrm{Aut}(A) = 1$, $\mathrm{Aut}(F) = \langle\sigma, \rho\rangle \cong S_3$, where $|\sigma| = 2$, $|\rho| = 3$. Furthermore, $\dim \mathrm{Hom}(F, A) = 2$, $\dim \mathrm{B}(F, A) = 1$ and $\dim \mathrm{C}(F, A) = 9$. The three subspaces $\mathrm{Inv}(\sigma)$, $\mathrm{Inv}(\sigma\rho)$, $\mathrm{Inv}(\sigma\rho^2)$ have dimension 6, and any two of them intersect precisely in $\mathrm{Inv}(\rho)$ (see Example 6.1), which has dimension 3. By (4.3), there are

$$\frac{2^3}{2} + 3 \cdot \frac{2^6 - 2^3}{2 \cdot 3} + \frac{2^9 - 3 \cdot 2^6 + 2 \cdot 2^3}{2 \cdot 6} = 60$$

central extensions of $\mathbb{Z}_2$ by $\mathbb{Z}_2 \times \mathbb{Z}_2$.

In order to pinpoint the number of nilpotent loops of order 8, we must determine which loops are obtained both as central extensions of $\mathbb{Z}_2$ by $\mathbb{Z}_4$ and of $\mathbb{Z}_2$ by $\mathbb{Z}_2 \times \mathbb{Z}_2$. First of all, $\mathbb{Z}_2 \times \mathbb{Z}_4$ is such a loop. Assume that Q is another such loop. Then $|Z(Q)| > 2$ and hence Q is an abelian group by Lemma 3.6. Now, $Q \neq \mathbb{Z}_8$ since every factor $Z_8/\langle x\rangle$ by an involution is isomorphic to $\mathbb{Z}_4$. Finally, $Q \neq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ since every factor by an involution is of exponent 2. We conclude that there are $80 + 60 - 1 = 139$ nilpotent loops of order 8.

9.2. **n=9.** We have $A = \mathbb{Z}_3$, $F = \mathbb{Z}_3$, $\dim \mathrm{Hom}(F, A) = 1$, $\dim \mathrm{B}(F, A) = 1$ and $\dim \mathrm{C}(F, A) = 4$. Also, $\mathrm{Aut}(A) = \langle\beta\rangle \cong \mathbb{Z}_2$, $\mathrm{Aut}(F) = \langle\alpha\rangle \cong \mathbb{Z}_2$.

By computer, $\mathrm{Inv}(\beta) = \mathrm{B}(F, A)$ has dimension 1, $\dim \mathrm{Inv}(\alpha) = 2$, $\dim \mathrm{Inv}(\alpha\beta) = 4$, and $\mathrm{Inv}(\alpha\beta) \cap \mathrm{Inv}(\alpha) = \mathrm{Inv}(\beta)$. Then (4.3) gives

$$\frac{3}{3} + \frac{3^3 - 3}{3 \cdot 2} + \frac{3^2 - 3}{3 \cdot 2} + \frac{3^4 - 3^3 - 3^2 + 3}{3 \cdot 4} = 10$$

nilpotent loops of order 9.

9.3. **n=12.** For the first time we have to worry about admissibility, and hence we have to calculate the subsets $W(F,A)$.

Case $A=\mathbb{Z}_2$, $F=\mathbb{Z}_6$. Let $\mathrm{Aut}(F)=\langle\alpha\rangle\cong\mathbb{Z}_2$. The subset $W(F,A)$ is in fact a subspace: Let $x\in F$ be the unique involution and $y\in F$ an element of order 3. If $\theta\in W_y(F,A)$ then $Z(\mathcal{Q}(F,A,\theta))=\mathcal{Q}(F,A,\theta)$ by Lemma 3.6. Thus $W_y(F,A)\subseteq W_x(F,A)=W(F,A)$.

Computer calculation yields $\dim W(F,A)=7$, $\dim \mathrm{B}(F,A)=4$, $\dim\mathrm{Inv}(\alpha)=15$, and $\dim(W(F,A)\cap\mathrm{Inv}(\alpha))=6$. Thus there are

$$\frac{2^{25}-2^7-(2^{15}-2^6)}{2^4\cdot 2}+\frac{2^{15}-2^6}{2^4}=1,049,594$$

loops Q with $|Q|=12$ and $Q/Z(Q)=\mathbb{Z}_6$. Among the $2^7/2^4=8$ loops constructed from the large center cocycles, 6 are nonisomorphic.

Case $A=\mathbb{Z}_2$, $F=L_{6,2}$. By computer, $\mathrm{Aut}(F)=1$, $\dim\mathrm{B}(F,A)=5$, $\dim W(F,A)=7$. Thus there are

$$\frac{2^{25}-2^7}{2^5}=1,048,572$$

loops Q with $|Q|=12$ and $Q/Z(Q)=F$. The $2^7/2^5=4$ loops corresponding to cocycles in $W(F,A)$ are pairwise nonisomorphic.

Case $A=\mathbb{Z}_2$, $F=L_{6,3}$. Then computer gives $\mathrm{Aut}(F)=\langle\alpha\rangle\cong\mathbb{Z}_2$, $\dim\mathrm{B}(F,A)=5$, $\dim W(F,A)=7$, $\dim\mathrm{Inv}(\alpha)=16$, and $W(F,A)\le\mathrm{Inv}(\alpha)$. Thus there are

$$\frac{2^{25}-2^{16}}{2^5\cdot 2}+\frac{2^{16}-2^7}{2^5}=525,308$$

nilpotent loops Q with $|Q|=12$ and $Q/Z(Q)=F$. The $2^7/2^5=4$ loops corresponding to large center cocycles are pairwise nonisomorphic.

Among the $6+4+4$ loops with $|Z(Q)|>2$ found so far, 11 are nonisomorphic.

Case $A=\mathbb{Z}_3$, $|F|=4$. If $Z(Q)>A$ then $[Q:Z(Q)]\le 2$, so all cocycles in $\mathrm{C}(F,A)$ are admissible by Lemma 3.7. The details are in Table 2.

If a nilpotent loop of order 12 is a central extension of both $\mathbb{Z}_2$ and of $\mathbb{Z}_3$, it is an abelian group by Lemma 3.6, and hence it is isomorphic to $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_3$ or to $\mathbb{Z}_4\times\mathbb{Z}_3$. We have counted these two loops twice and must take this into account.

9.4. **n=15.** Either $A=\mathbb{Z}_3$, $F=\mathbb{Z}_5$ or $A=\mathbb{Z}_5$, $F=\mathbb{Z}_3$. In both cases, all cocycles are admissible by Lemma 3.7. Most subspaces $\mathrm{Inv}(H)$ can be determined by Theorem 6.5. The two cases overlap only in $\mathbb{Z}_3\times\mathbb{Z}_5$.

9.5. **n=16.** This is a more difficult case due to the 139 nilpotent loops F_1, …, F_{139} of order 8.

Cases $A=\mathbb{Z}_2$, $F=F_i$. We calculate the subsets $W_i=W(F_i,A)$, and treat admissible cocycles outside W_i as usual. (In one of the cases, the automorphism group $\mathrm{Aut}(F,A)=\mathrm{Aut}(F)$ is the simple group of order 168, the largest automorphism group we had to deal with in the entire search.) We filter the large center loops up to isomorphism.

We now need to filter the union of the 139 sets of large center loops up to isomorphism. This can be done efficiently as follows: Let $Q=\mathcal{Q}(F,A,\theta)$ where $\theta\in W_i$. For every central involution x of Q, calculate $Q/\langle x\rangle$ and determine its isomorphism type. If $Q/\langle x\rangle$ is isomorphic to some F_j with $j<i$, we have already seen Q and can discard it.

9.6. **n=18.** See Table 2.

9.7. **n=20.** This is the computationally most difficult case, due to the $1,044$ nilpotent loops of order 10. See §10 for more. The efficient filtering of large center loops is crucial here. On the other hand, $1,008$ out of the $1,044$ nilpotent loops of order 10 have trivial automorphism groups.

9.8. **n=21.** This case is analogous to $n = 15$.

10. Related ideas and concluding remarks

For an introduction to loop theory see Bruck [1] or Pflugfelder [14].

The study of (central) extensions of groups by means of cocycles goes back to Schreier [16]. The abstract cohomology theory for groups was initiated by Eilenberg and MacLane in [2]–[4], and it has grown into a vast subject.

Eilenberg and MacLane were also the first to investigate cohomology of loops. In [5], they imposed conditions on loop cocycles that mimic those of group cocycles, and calculated some cohomology groups. A more natural theory (by many measures) of loop cohomology has been developed in [9] by Johnson and Leedham-Green. As in this paper, their third cohomology group vanishes, since they impose no conditions on the (normalized) loop 2-cocycles.

We are not aware of any work on the classification of nilpotent loops *per se*. In the recent paper [10], McKay, Mynert and Myrvold enumerated all loops of order $n \leq 10$ up to isomorphism. We believe that all results in §4–§9 are new.

This being said, the central notion of admissible cocycles must have surely been noticed before, but since it is of limited utility in group theory (where much stronger structural results are available to attack the isomorphism problem of central extensions), it has not been investigated in the more general setting of loops. The experienced reader will recognize the mappings S and T of §6 as the consecutive differentials in a free resolution of a cyclic group, cf. [6, Ch. 2].

The computational tools developed here are applicable to finitely based varieties of loops, and can therefore be used to classify nilpotent loops of small orders in such varieties. One merely has to start with the appropriate space of cocycles (determined by a system of linear equations, just as in the group case). The first author intends to undertake this classification for loops of Bol-Moufang type, cf. [15]. The classification of all Moufang loops of order $n \leq 64$ and $n = 81$ can be found in [12]. The classification of Bol loops has been started in [11]. The LOOPS [13] package contains libraries of small loops in certain varieties, including Bol and Moufang loops.

All calculations in this paper have been carried out in the GAP [7] package LOOPS. We wrote two mostly independent codes, and the calculations have been done twice (except for the loops of order 20), once with each code. The enumeration of nilpotent loops of order 20 took more than 90 percent of the total calculation time, about 2 days on a single-processor Unix machine. Both codes and the multiplication tables of all nilpotent loops of order $n \leq 10$ can be downloaded at the second author's web site `http://www.math.du.edu/~petr`.

References

[1] R. H. Bruck, A survey of binary systems, Third printing, corrected, *Ergebnisse der Mathematik und ihrer Grenzgebiete* **20**, Springer-Verlag, 1971.

[2] S. Eilenberg and S. MacLane, *Group extensions and homology*, Ann. of Math., Second Series, **43**, no. **4** (Oct. 1942), 757–831.

[3] S. Eilenberg and S. MacLane, *Cohomology Theory in Abstract Groups I*, Ann. of Math., Second Series, **48**, no. **1** (Jan. 1947), 51–78.

[4] S. Eilenberg and S. MacLane, *Cohomology Theory in Abstract Groups II*, Ann. of Math., Second Series, **48**, no. **1** (Apr. 1947), 326–341.
[5] S. Eilenberg and S. MacLane *Algebraic cohomology groups and loops*, Duke Math. J. **14** (1947), 435–463.
[6] L. Evens, The cohomology of groups, *Oxford Mathematical Monographs*, The Clarendon Press, 1991.
[7] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.4; Aachen, St Andrews (2006). (Visit http://www-gap.dcs.st-and.ac.uk/˜gap).
[8] C. J. Hillar and D. L. Rhea, *Automorphisms of finite abelian groups*, Amer. Math. Monthly **114** (2007), no. **10**, 917–923.
[9] K. W. Johnson and C. R. Leedham-Green, *Loop cohomology*, Czechoslovak Math. J. **40**(**115**) (1990), no. **2**, 182–194.
[10] B. McKay, A. Meynert, W. Myrvold, *Small Latin squares, quasigroups, and loops*, J. Combin. Des. **15** (2007), no. **2**, 98–119.
[11] G. E. Moorhouse, *Bol loops of small order*, technical report, http://www.uwyo.edu/moorhouse/pub/bol/.
[12] G. P. Nagy and P. Vojtěchovský, *The Moufang loops of order* 64 *and* 81, J. Symbolic Comput. **42** (2007), no. **9**, 871–883.
[13] G. P. Nagy and P. Vojtěchovský, LOOPS: *Computing with quasigroups and loops in* GAP, download at http://www.math.du.edu/loops.
[14] H. O. Pflugfelder, Quasigroups and Loops: Introduction, *Sigma series in pure mathematics* **7**, Heldermann Verlag Berlin, 1990.
[15] J. D. Phillips and P. Vojtěchovský, *The varieties of loops of Bol-Moufang type*, Algebra Universalis **54** (2005), no. **3**, 259–271.
[16] O. Schreier, *Über die Erweiterung von Gruppen I.*, Monatsh. Math. Phys. **34** (1926), no. **1**, 165–180.

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

Department of Mathematics, University of Denver, 2360 S Gaylord St, Denver, CO 80208, U.S.A.