COMMUTATIVE AUTOMORPHIC LOOPS OF ORDER p^3

DYLENE AGDA SOUZA DE BARROS, ALEXANDER GRISHKOV,
AND PETR VOJTĚCHOVSKÝ

Abstract. A loop is said to be automorphic if its inner mappings are automorphisms. For a prime p, denote by $\mathcal{A}_p$ the class of all 2-generated commutative automorphic loops Q possessing a central subloop $Z \cong \mathbb{Z}_p$ such that $Q/Z \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Upon describing the free 2-generated nilpotent class two commutative automorphic loop and the free 2-generated nilpotent class two commutative automorphic p-loop F_p in the variety of loops whose elements have order dividing p^2 and whose associators have order dividing p, we show that every loop of $\mathcal{A}_p$ is a quotient of F_p by a central subloop of order p^3. The automorphism group of F_p induces an action of $\mathrm{GL}_2(p)$ on the three-dimensional subspaces of $Z(F_p) \cong (\mathbb{Z}_p)^4$. The orbits of this action are in one-to-one correspondence with the isomorphism classes of loops from $\mathcal{A}_p$. We describe the orbits, and hence we classify the loops of $\mathcal{A}_p$ up to isomorphism.

It is known that every commutative automorphic p-loop is nilpotent when p is odd, and that there is a unique commutative automorphic loop of order 8 with trivial center. Knowing $\mathcal{A}_p$ up to isomorphism, we easily obtain a classification of commutative automorphic loops of order p^3. There are precisely 7 commutative automorphic loops of order p^3 for every prime p, including the 3 abelian groups of order p^3.

1. Introduction

A *loop* is a set Q with a binary operation $\cdot$ and a neutral element $1 \in Q$ such that for every a, $b \in Q$ the equations $ax = b$ and $ya = b$ have unique solutions x, $y \in Q$, respectively. The element x satisfying $ax = b$ will be denoted by $a\backslash b$. See [1] for an introduction to the theory of loops.

Let Q be a loop. For $x \in Q$, the *left translation* $L_x : Q \to Q$ is defined by $L_x(y) = xy$, and the *right translation* $R_x : Q \to Q$ by $R_x(y) = yx$. The *inner mapping group* $\operatorname{Inn} Q$ of Q is the permutation group $\langle L_{x,y},\ R_{x,y},\ T_x;\ x,\ y \in Q\rangle$, where $L_{x,y} = L_{yx}^{-1} L_y L_x$, $R_{x,y} = R_{xy}^{-1} R_y R_x$, and $T_x = L_x^{-1} R_x$. Let $\operatorname{Aut} Q$ be the *automorphism group* of Q.

Denote by $Z(Q)$, $N(Q)$, $N_\lambda(Q)$ and $N_\mu(Q)$ the *center*, *nucleus*, *left nucleus* and *middle nucleus* of Q, respectively. For x, y, $z \in Q$, define the *associator* (x, y, z) of x, y, z by $(xy)z = (x(yz))(x, y, z)$. The *associator subloop* $A(Q)$ of Q is the smallest normal subloop H of Q such that Q/H is a group. Thus $A(Q)$ is the smallest normal subloop of Q containing all associators (x, y, z).

A loop Q is *nilpotent* if the series Q, $Q/Z(Q)$, $(Q/Z(Q))/Z(Q/Z(Q))$, ... terminates in 1 in finitely many steps. In particular, Q is of *nilpotency class two* if $Q/Z(Q) \neq 1$ is an abelian group.

2010 *Mathematics Subject Classification.* Primary: 20N05. Secondary: 20G40.

Key words and phrases. commutative automorphic loop, loops of order p^3, free commutative automorphic loop.

D. Barros's and A. Grishkov's stay at the University of Denver was partially supported by a grant from the Simons Foundation (grant 210176 to P. Vojtěchovský). P. Vojtěchovský thanks the Institute of Mathematics and Statistics at the University of São Paulo for hospitality and financial support.

A loop Q is said to be an *automorphic loop* (or *A-loop*) if $\operatorname{Inn} Q \leq \operatorname{Aut} Q$. Note that a commutative loop is automorphic if and only if $L_{x,y} \in \operatorname{Aut} Q$ for every $x, y \in Q$. This latter condition can be rewritten as

$$(yx)\backslash(y(x(ab))) = [(yx)\backslash(y(xa))][(yx)\backslash(y(xb))], \tag{A}$$

so a commutative loop is automorphic if and only if it satisfies the identity (A). Groups are certainly automorphic loops, but there are many other examples.

The study of automorphic loops began with the paper [2] of Bruck and Paige. Among other results and constructions, they showed that automorphic loops are power-associative (that is, every element generates a group) and satisfy the antiautomorphic inverse property $(xy)^{-1} = y^{-1}x^{-1}$. The implicit goal of [2] was to show that diassociative (that is, every two elements generate a group) automorphic loops are Moufang. This was eventually proved by Osborn [8] in the commutative case, and by Kinyon, Kunen and Phillips [7] in general.

Foundational results in the theory of commutative automorphic loops were obtained by Jedlička, Kinyon and Vojtěchovský in [4], for instance the Odd Order Theorem, the Cauchy Theorem, and the Lagrange Theorem. In the companion paper [5], the same authors noted that commutative automorphic loops of order p, $2p$, $4p$, p^2, $2p^2$ and $4p^2$ are abelian groups for every odd prime p, and they also constructed examples of nonassociative commutative automorphic loops of order p^3.

For a prime p, denote by $\mathcal{A}_p$ the class of all 2-generated commutative automorphic loops Q possessing a central subloop $Z \cong \mathbb{Z}_p$ such that $Q/Z \cong \mathbb{Z}_p \times \mathbb{Z}_p$. In this paper we classify the loops of $\mathcal{A}_p$ (cf. Theorem 6.1), and also commutative automorphic loops of order p^3 (cf. Theorem 6.3) up to isomorphism. It turns out that all loops of Theorem 6.3 were constructed already in [5], but the authors of [5] did not know whether their list was complete, and whether the constructed loops were pairwise nonisomorphic.

The classification of commutative automorphic loops of order p^3 is made possible by the fact that, when p is odd, commutative automorphic p-loops are nilpotent, cf. [6]. There is a unique commutative automorphic loop of order 8 that is not nilpotent, as can be seen quickly with a finite model builder (see [5, Section 3] for details and for a near-complete human classification of commutative automorphic loops of order 8).

In Section 2 we construct the free nilpotent class two commutative automorphic loop F on two generators. In Section 2 we find a normal subloop K_p of F so that $F_p = F/K_p$ is the free nilpotent class two commutative automorphic p-loop on two generators in the variety of loops whose elements have order dividing p^2 and whose associators have order dividing p.

In Section 4 we show that every loop of $\mathcal{A}_p$ is a quotient of F_p by a central subloop of order p^3, and we show that $\operatorname{Aut} F_p$ induces an action of $\mathrm{GL}_2(p)$ on $Z(F_p) \cong (\mathbb{Z}_p)^4$. Moreover, by Theorem 4.2, the orbits of this action on the Grassmanian of the three-dimensional subspaces of $Z(F_p)$ correspond to the isomorphism classes of loops from $\mathcal{A}_p$. The orbits are described in detail in Section 5 (cf. Propositions 5.3 and 5.4), yielding the main results in Section 6.

2. The free 2-generated commutative automorphic loop of nilpotency class two

Let Z be an abelian group and L a loop. Then a loop Q is a *central extension* of Z by L if $Z \leq Z(Q)$ and Q/Z is isomorphic to L. It is well known that Q is a central

extension of Z by L if and only if Q is isomorphic to a loop $\mathcal{Q}(Z, L, \theta)$ defined on $L \times Z$ with multiplication

$$(x_1, z_1)(x_2, z_2) = (x_1x_2, z_1z_2\theta(x_1, x_2)), \tag{2.1}$$

where $\theta : L\times L \to Z$ is a *(loop) cocycle*, that is, a mapping satisfying $\theta(x, 1) = \theta(1, x) = 1$ for every $x \in L$.

Straightforward calculation with (2.1) shows that the associator in $\mathcal{Q}(Z, L, \theta)$ is obtained by the formula

$$(x_1z_1, x_2z_2, x_3z_3) = \theta(x_1, x_2)\theta(x_1x_2, x_3)\theta(x_2, x_3)^{-1}\theta(x_1, x_2x_3)^{-1}. \tag{2.2}$$

Lemma 2.1. *Let Q be a commutative loop of nilpotency class two. Then:*

(i) $A(Q) \leq Z(Q)$.
(ii) $(a, b, a) = 1$, $(a, b, c) = (c, b, a)^{-1}$, *and* $(a, b, c)(b, c, a)(c, a, b) = 1$ *for every* a, b, $c \in Q$.
(iii) Q *is an automorphic loop if and only if* $(ab, c, d) = (a, c, d)(b, c, d)$ *for every* a, b, c, $d \in Q$.

Proof. (i) The inclusion $A(Q) \leq Z(Q)$ holds since $Q/Z(Q)$ is a group.

(ii) The identity $(a, b, a) = 1$ is equivalent to $(ab)a = a(ba)$, which obviously holds in any commutative loop. Using the fact that all associators are central, we can write $(cb)a(c, b, a)^{-1} = c(ba) = (ab)c = a(bc)(a, b, c) = (cb)a(a, b, c)$, and $(a, b, c) = (c, b, a)^{-1}$ follows. Finally, $(ab)c = a(bc)(a, b, c) = (bc)a(a, b, c) = b(ca)(a, b, c)(b, c, a) = (ca)b(a, b, c)(b, c, a) = c(ab)(a, b, c)(b, c, a)(c, a, b) = (ab)c(a, b, c)(b, c, a)(c, a, b)$, hence $(a, b, c)(b, c, a)(c, a, b) = 1$.

(iii) Note that $(ab)\backslash(a(bc)) = c(a, b, c)^{-1}$. The identity (A) is therefore equivalent to $ab(d, c, ab)^{-1} = a(d, c, a)^{-1}b(d, c, b)^{-1}$, which is equivalent to $(ab, c, d) = (a, c, d)(b, c, d)$, by (ii). □

Lemma 2.2. *Let Q be a commutative automorphic loop of nilpotency class two. Then:*

(i) *For every a, b, c, $d \in Q$,*

$$\begin{aligned}(ab, c, d) &= (a, c, d)(b, c, d),\\ (a, b, cd) &= (a, b, c)(a, b, d),\\ (a, bc, d) &= (a, d, b)(a, d, c)(b, a, d)(c, a, d).\end{aligned}$$

(ii) *For every a, b, c, $d \in Q$,*

$$(ab)(cd) = (ac)(bd)(ac, b, d)(b, a, c)(d, c, ab).$$

(iii) *For every a, $b \in Q$ and i, j, $k \in \mathbb{Z}$,*

$$(a^i, b^j, b^k) = (a, b, b)^{ijk}, \quad (b^i, a^j, b^k) = 1, \quad (b^i, b^j, a^k) = (b, b, a)^{ijk}.$$

(iv) *For every a, $b \in Q$ and i_1, i_2, j_1, j_2, k_1, $k_2 \in \mathbb{Z}$,*

$$(a^{i_1}b^{i_2}, a^{j_1}b^{j_2}, a^{k_1}b^{k_2}) = (a, a, b)^{j_1(i_1k_2-i_2k_1)}(a, b, b)^{j_2(i_1k_2-i_2k_1)}.$$

Proof. (i) The first equality is from Lemma 2.1(iii). Then $(a, b, cd) = (a, b, c)(a, b, d)$ follows by $(a, b, c) = (c, b, a)^{-1}$ of Lemma 2.1(ii). Finally, by Lemma 2.1(ii), we have $(a, bc, d) = (bc, d, a)^{-1}(d, a, bc)^{-1} = (a, d, b)(a, d, c)(b, a, d)(c, a, d)$.

(ii) We have

$$\begin{aligned}(ab)(cd) &= ((ab)c)d(ab,c,d)^{-1} = ((ab)c)d(d,c,ab) = (c(ab))d(d,c,ab)\\ &= ((ca)b)d(d,c,ab)(c,a,b)^{-1} = ((ca)b)d(d,c,ab)(b,a,c)\\ &= ((ac)b)d(d,c,ab)(b,a,c) = (ac)(bd)(d,c,ab)(b,a,c)(ac,b,d).\end{aligned}$$

(iii) We have $(b^i,a^j,b^k) = (b,a^j,b)^{ik} = 1$ by (i) and Lemma 2.1(ii). Using this fact and Lemma 2.1(ii) again, we get $(a^i,b^j,b^k) = (a,b^j,b)^{ik} = (b^j,b,a)^{-ik}(b,a,b^j)^{-ik} = (b^j,b,a)^{-ik} = (b,b,a)^{-ijk} = (a,b,b)^{ijk}$ and $(b^i,b^j,a^k) = (a^k,b^j,b^i)^{-1} = (a,b,b)^{-ijk} = (b,b,a)^{ijk}$.

(iv) Using parts (i), (ii) and (iii), we have

$$\begin{aligned}(a^{i_1}b^{i_2},a^{j_1}b^{j_2},a^{k_1}b^{k_2}) &= (a^{i_1},a^{j_1}b^{j_2},a^{k_1})(a^{i_1},a^{j_1}b^{j_2},b^{k_2})(b^{i_2},a^{j_1}b^{j_2},a^{k_1})(b^{i_2},a^{j_1}b^{j_2},b^{k_2})\\ &= (a^{i_1},a^{j_1}b^{j_2},b^{k_2})(b^{i_2},a^{j_1}b^{j_2},a^{k_1})\\ &= (a^{i_1},b^{k_2},a^{j_1})(a^{i_1},b^{k_2},b^{j_2})(a^{j_1},a^{i_1},b^{k_2})(b^{j_2},a^{i_1},b^{k_2})\\ &\quad\cdot(b^{i_2},a^{k_1},a^{j_1})(b^{i_2},a^{k_1},b^{j_2})(a^{j_1},b^{i_2},a^{k_1})(b^{j_2},b^{i_2},a^{k_1})\\ &= (a^{i_1},b^{k_2},b^{j_2})(a^{j_1},a^{i_1},b^{k_2})(b^{i_2},a^{k_1},a^{j_1})(b^{j_2},b^{i_2},a^{k_1})\\ &= (a,b,b)^{i_1j_2k_2}(a,a,b)^{i_1j_1k_2}(b,a,a)^{i_2j_1k_1}(b,b,a)^{i_2j_2k_1}\\ &= (a,a,b)^{j_1(i_1k_2-i_2k_1)}(a,b,b)^{j_2(i_1k_2-i_2k_1)}.\end{aligned}$$

□

Theorem 2.3. *Let F be the free commutative automorphic loop of nilpotency class two with free generators x_1, x_2, and let $z_1 = (x_1,x_1,x_2)$, $z_2 = (x_1,x_2,x_2)$. Then every element of F can be written uniquely as $x_1^{a_1}x_2^{a_2}z_1^{a_3}z_2^{a_4}$ for some a_1, a_2, a_3, $a_4 \in \mathbb{Z}$, and the multiplication in F is given by*

$$(x_1^{a_1}x_2^{a_2}z_1^{a_3}z_2^{a_4})(x_1^{b_1}x_2^{b_2}z_1^{b_3}z_2^{b_4}) = x_1^{a_1+b_1}x_2^{a_2+b_2}z_1^{a_3+b_3-a_1b_1(a_2+b_2)}z_2^{a_4+b_4+a_2b_2(a_1+b_1)}. \tag{2.3}$$

Furthermore, $Z(F) = N_\lambda(F) = N_\mu(F) = N(F) = A(F) = \langle z_1,z_2\rangle \cong \mathbb{Z}^2$. The loop F is the central extension of the free abelian group $\langle z_1,z_2\rangle$ by the free abelian group with free generators x_1, x_2 via the cocycle

$$\theta(x_1^{a_1}x_2^{a_2},x_1^{b_1}x_2^{b_2}) = z_1^{-a_1b_1(a_2+b_2)}z_2^{a_2b_2(a_1+b_1)}. \tag{2.4}$$

Finally, the associator in F is given by

$$(x_1^{a_1}x_2^{a_2}z_1^{a_3}z_2^{a_4},x_1^{b_1}x_2^{b_2}z_1^{b_3}z_2^{b_4},x_1^{c_1}x_2^{c_2}z_1^{c_3}z_2^{c_4}) = z_1^{b_1(a_1c_2-a_2c_1)}z_2^{b_2(a_1c_2-a_2c_1)}. \tag{2.5}$$

Proof. Consider the mapping $\widehat{\theta}:\mathbb{Z}^2\times\mathbb{Z}^2\to\mathbb{Z}^2$ defined by

$$\widehat{\theta}((a_1,a_2),(b_1,b_2)) = (-a_1b_1(a_2+b_2),a_2b_2(a_1+b_1)),$$

and let $\widehat{F} = \mathcal{Q}(\mathbb{Z}^2,\mathbb{Z}^2,\widehat{\theta})$. By (2.1), $\widehat{F}$ is defined on $\mathbb{Z}^4$ by

$$(a_1,a_2,a_3,a_4)(b_1,b_2,b_3,b_4) = (a_1+b_1,a_2+b_2,a_3+b_3-a_1b_1(a_2+b_2),a_4+b_4+a_2b_2(a_1+b_1)).$$

It follows that $Z(\widehat{F}) \geq \{(0,0,a_3,a_4);\ a_i\in\mathbb{Z}\}$ and $\widehat{F}$ is a commutative loop of nilpotency class at most two.

With $a=(a_1,a_2,a_3,a_4)$, $b=(b_1,b_2,b_3,b_4)$, $c=(c_1,c_2,c_3,c_4)\in\widehat{F}$, a straightforward evaluation of (2.2) yields

$$(a,b,c) = (0,0,b_1(a_1c_2-a_2c_1),b_2(a_1c_2-a_2c_1)).$$

Hence $Z(\widehat{F}) = \{(0,0,a_3,a_4);\ a_i \in \mathbb{Z}\}$. Another routine calculation gives the identity $(ab,c,d) = (a,c,d)(b,c,d)$ in $\widehat{F}$, so, by Lemma 2.1(iii), $\widehat{F}$ is an automorphic loop. With $e_1 = (1,0,0,0)$, $e_2 = (0,1,0,0)$, $e_3 = (0,0,1,0)$, $e_4 = (0,0,0,1)$, note that $(e_1,e_1,e_2) = e_3$, $(e_1,e_2,e_2) = e_4$, and $e_1^{a_1}e_2^{a_2}e_3^{a_3}e_4^{a_4} = (a_1,a_2,a_3,a_4)$.

Let now F be as in the statement of the theorem. By Lemmas 2.1 and 2.2, any word in x_1, x_2 can be written as $x_1^{a_1}x_2^{a_2}z_1^{a_3}z_2^{a_4}$, for some $a_i \in \mathbb{Z}$. Consider the homomorphism $\widehat{\ } : F \to \widehat{F}$ determined by $\widehat{x_1} = e_1$, $\widehat{x_2} = e_2$. Since $\widehat{z_1} = e_3$ and $\widehat{z_2} = e_4$, we see that $\widehat{\ }$ maps $x_1^{a_1}x_2^{a_2}z_1^{a_3}z_2^{a_4}$ onto $e_1^{a_1}e_2^{a_2}e_3^{a_3}e_4^{a_4} = (a_1,a_2,a_3,a_4)$. This means that $\widehat{\ } : F \to \widehat{F}$ is in fact an isomorphism, and that every element of F can be written uniquely as $x_1^{a_1}x_2^{a_2}z_1^{a_3}z_2^{a_4}$.

We have now established all claims of the theorem except for $Z(F) = N_\lambda(F) = N_\mu(F) = N(F)$. By Lemma 2.2, $(x_1, x_1^{a_1}x_2^{a_2}, x_2) = z_1^{a_1}z_2^{a_2}$, so $N_\mu(F) \le Z(F)$. Since $Z(Q) \le N(Q) = N_\lambda(Q) \cap N_\rho(Q) \le N_\mu(Q)$ holds in any automorphic loop Q by [2, Corollary to Lemma 2.8], we are done. □

3. The loops K_p and $F_p = F/K_p$

Let K_p be the smallest normal subloop of F containing $\{a^{p^2};\ a \in F\} \cup \{a^p;\ a \in A(F)\}$.

Lemma 3.1. $K_p = \{(p^2c_1, p^2c_2, pc_3, pc_4);\ c_i \in \mathbb{Z}\}$.

Proof. Let $c \in F$ and $z \in Z(F)$. Since $(cz)^k = c^kz^k$, K_p is generated by elements of the form $(c_1,c_2,0,0)^{p^2}$ and $(0,0,c_3,c_4)^p$. By (2.3), $(0,0,c_3,c_4)^p = (0,0,pc_3,pc_4)$. An easy induction on $k \ge 1$ shows that

$$(c_1,c_2,0,0)^k = (kc_1, kc_2, -c_1^2c_2\sum_{i=1}^{k-1}(i+i^2), c_2^2c_1\sum_{i=1}^{k-1}(i+i^2)).$$

Since

$$\sum_{i=1}^{p^2-1}(i+i^2) = (p^2-1)p^2/2 + (p^2-1)p^2(2p^2-1)/6$$

is divisible by p, it follows that K_p is the smallest normal subloop containing $S = \{(p^2c_1, p^2c_2, pc_3, pc_4);\ c_i \in \mathbb{Z}\}$.

We claim that $S = K_p$. A short calculation with (2.3) shows that S is closed under multiplication and division. Recall that $(ab)\backslash(a(bc)) = c(a,b,c)^{-1}$. Hence to prove that S is a normal subloop it suffices to show that $(a,b,c) \in S$ for every a, $b \in F$ and $c \in S$. By (2.5), the associator $((a_1,a_2,a_3,a_4),(b_1,b_2,b_3,b_4),(p^2c_1,p^2c_2,pc_3,pc_4))$ is equal to $(0,0,b_1(p^2a_1c_2 - p^2a_2c_1), b_2(p^2a_1c_2 - p^2a_2c_1))$, which is an element of S. □

As in [5], for integers $0 \le a$, $b < p$, define the modular overflow indicator by

$$(a,b)_p = \begin{cases} 0, \text{ if } a+b < p, \\ 1, \text{ otherwise.} \end{cases}$$

Let $F_p = F/K_p$.

Lemma 3.2. *F_p is isomorphic to the loop defined on $(\mathbb{Z}_p)^6$ with multiplication*

$$\begin{aligned}(a_1,a_2,a_3,a_4,a_5,a_6)&(b_1,b_2,b_3,b_4,b_5,b_6)\\ &= (a_1+b_1, a_2+b_2,\\ &\quad a_3+b_3+(a_1,b_1)_p, a_4+b_4+(a_2,b_2)_p,\\ &\quad a_5+b_5-a_1b_1(a_2+b_2), a_6+b_6+a_2b_2(a_1+b_1)).\end{aligned}$$

Moreover, $Z(F_p) = N(F_p) = N_\lambda(F_p) = N_\mu(F_p) = 0\times 0\times(\mathbb{Z}_p)^4$.

Proof. Note that $(a_1,a_2,a_3,a_4)K_p = (b_1,b_2,b_3,b_4)K_p$ if and only if $a_1\equiv b_1 \pmod{p^2}$, $a_2\equiv b_2\pmod{p^2}$, $a_3\equiv b_3\pmod p$ and $a_4\equiv b_4\pmod p$. Thus F_p is isomorphic to $\mathbb{Z}_{p^2}\times\mathbb{Z}_{p^2}\times\mathbb{Z}_p\times\mathbb{Z}_p$ with multiplication

$$(a_1,a_2,a_3,a_4)(b_1,b_2,b_3,b_4) = (a_1+b_1, a_2+b_2, a_3+b_3-a_1b_1(a_2+b_2), a_4+b_4+a_2b_2(a_1+b_1)).$$

For $n\in\mathbb{Z}_{p^2}$, write $n = n'+pn''$, where $0\le n', n'' < p$. Then the addition in $\mathbb{Z}_{p^2}$ can be expressed on $\mathbb{Z}_p\times\mathbb{Z}_p$ by $n+m = (n',n'')+(m',m'') = (n'+m', n''+m''+(n',m')_p)$.

If we split a_1, a_2, b_1, b_2 in this way in the above multiplication formula, we obtain the multiplication formula

$$\begin{aligned}(a_1',a_2',a_1'',a_2'',a_3,a_4)&(b_1',b_2',b_1'',b_2'',b_3,b_4)\\ &= (a_1'+b_1', a_2'+b_2',\\ &\quad a_1''+b_1''+(a_1',b_1')_p, a_2''+b_2''+(a_2',b_2')_p,\\ &\quad a_3+b_3-a_1'b_1'(a_2'+b_2'), a_4+b_4+a_2'b_2'(a_1'+b_1'))\end{aligned}$$

on $(\mathbb{Z}_p)^6$, since we can calculate modulo p in the last two coordinates.

We clearly have $0\times 0\times(\mathbb{Z}_p)^4\le Z(F_p)$. Consider $(a_1,a_2,0,0,0,0)\ne 1$. Then

$$\begin{aligned}((1,0,0,0,0,0)&(a_1,a_2,0,0,0,0))(0,1,0,0,0,0)\\ &= (1+a_1, 1+a_2, (a_1,1)_p, (a_2,1)_p, -a_1a_2, a_2(1+a_1)),\end{aligned}$$

while

$$\begin{aligned}(1,0,0,0,0,0)&((a_1,a_2,0,0,0,0)(0,1,0,0,0,0))\\ &= (1+a_1, 1+a_2, (a_1,1)_p, (a_2,1)_p, -a_1(a_2+1), a_2a_1).\end{aligned}$$

Hence $(a_1,a_2,0,0,0,0)\notin N_\mu(F_p)$, and $Z(F_p) = N_\lambda(F_p) = N_\mu(F_p) = N(F_p) = 0\times 0\times(\mathbb{Z}_p)^4$ follows. □

Arguing similarly to the proof of Theorem 2.3, we see that F_p is the free nilpotent class two p-loop on two generators

$$x = (1,0,0,0,0,0),\quad y = (0,1,0,0,0,0) \tag{3.1}$$

in the variety of commutative automorphic loops satisfying the identities $a^{p^2} = 1$ and $(a,b,c)^p = 1$.

The following symbols will be useful in expressing powers of elements in F_p. For $0\le a < p$ and $k\ge 1$ let

$$[k,a]_p = (a,a)_p + (a,(2a) \bmod p)_p + \cdots + (a,((k-1)a) \bmod p)_p.$$

In particular, $[1,a]_p = 0$.

We now show why the case $p = 3$ must be treated separately.

Lemma 3.3. *For $(a_1,a_2,a_3,a_4,a_5,a_6) \in F_p$ and $k \geq 1$, $(a_1,a_2,a_3,a_4,a_5,a_6)^k$ is equal to*

$$(ka_1, ka_2, ka_3 + [k,a_1]_p, ka_4 + [k,a_2]_p, ka_5 - a_1^2 a_2 \sum_{i=1}^{k-1}(i+i^2), ka_6 + a_1 a_2^2 \sum_{i=1}^{k-1}(i+i^2)).$$

In particular,

$$(a_1,a_2,a_3,a_4,a_5,a_6)^p = \begin{cases} (0,0,a_1,a_2,0,0), & \text{if } p \neq 3, \\ (0,0,a_1,a_2,a_1^2a_2,-a_1a_2^2), & \text{if } p = 3. \end{cases}$$

Proof. The general formula follows by a simple induction on k, using the multiplication of Lemma 3.2. Suppose that $k = p$. For $0 \leq a < p$ we have

$$[p,a]_p = (a,a)_p + (a,(2a) \bmod p)_p + \cdots + (a,((p-1)a) \bmod p)_p = \sum_{i=1}^{p-1}(a,i)_p.$$

Since $(a,i)_p = 1$ if and only if $a + i \geq p$, we conclude that $[p,a]_p = a$. Finally, let

$$t_p = \sum_{i=1}^{p-1}(i+i^2) = (p-1)p/2 + (p-1)p(2p-1)/6.$$

If $p > 3$, we obviously have $t_p \equiv 0 \pmod p$. Also, $t_2 = 1 + 1^2 = 2 \equiv 0 \pmod 2$ and $t_3 = 1 + 1^2 + 2 + 2^2 \equiv -1 \pmod 3$. □

Lemma 3.4. *Let x, $y \in F_p$ be the free generators of F_p from* (3.1)*. Then $x^p = (0,0,1,0,0,0)$, $y^p = (0,0,0,1,0,0)$, $(x,x,y) = (0,0,0,0,1,0)$, $(x,y,y) = (0,0,0,0,0,1)$. Moreover, $Z(F_p) = 0\times0\times\langle x^p\rangle\times\langle y^p\rangle\times\langle(x,x,y)\rangle\times\langle(x,y,y)\rangle$, $A(F_p) = 0\times0\times0\times0\times(\mathbb{Z}_p)^2$, and*

$$(a_1,a_2,a_3,a_4,a_5,a_6) = x^{a_1}y^{a_2}(x^p)^{a_3}(y^p)^{a_4}(x,x,y)^{a_5}(x,y,y)^{a_6} \tag{3.2}$$

for every $(a_1,a_2,a_3,a_4,a_5,a_6) \in F_p$.

Proof. We have $x^p = (0,0,1,0,0,0)$, $y^p = (0,0,0,1,0,0)$ by Lemma 3.3. A quick calculation yields $(xx)y = (2,1,(1,1)_p,0,0,0)$, $x(xy) = (2,1,(1,1)_p,0,-1,0)$, so $(x,x,y) = (0,0,0,0,1,0)$. The equality $(x,y,y) = (0,0,0,0,0,1)$ follows by a similar argument. The structure of $Z(F_p)$ and $A(F_p)$ is now clear.

For every $1 \leq k < p$, $[k,1]_p = (1,1)_p + \cdots + (1,k-1)_p = 0$. Therefore for every $0 \leq k$, $\ell < p$ we have $x^k = (k,0,0,0,0,0)$, $y^\ell = (0,\ell,0,0,0,0)$, and $x^k y^\ell = (k,\ell,0,0,0,0)$. Equation (3.2) follows. □

Lemma 3.5. *If $H \leq F_p$ contains xz, yz' for some z, $z' \in Z(F_p)$ then $H = F_p$.*

Proof. Since $(xz)^p = x^p z^p = x^p$, $(yz')^p = y^p$, $(xz,xz,yz') = (x,x,y)$ and $(xz,yz',yz') = (x,y,y)$, Lemma 3.4 implies $Z(F_p) \leq H$. But then also x, $y \in H$ and $H = F_p$. □

4. The induced action

Lemma 4.1. *Let $\rho = \left(\begin{smallmatrix}\alpha_1 & \alpha_2 \\ \beta_1 & \beta_2\end{smallmatrix}\right) \in \mathrm{GL}_2(p)$. Then ρ induces an automorphism $\widehat{\rho}$ of F_p by*

$$\widehat{\rho}(x) = (\alpha_1,\alpha_2,0,0,0,0) = x^{\alpha_1}y^{\alpha_2}, \quad \widehat{\rho}(y) = (\beta_1,\beta_2,0,0,0,0) = x^{\beta_1}y^{\beta_2}, \tag{4.1}$$

where x, y are the free generators (3.1) *of F_p. Moreover, if $\lambda \in \operatorname{Aut} F_p$ then there are $\rho \in \mathrm{GL}_2(p)$ and $\sigma \in \operatorname{Aut} F_p$ such that $\lambda = \widehat{\rho}\sigma$ and $\sigma(z) = z$ for every $z \in Z(F_p)$.*

Proof. Let $\rho \in \mathrm{GL}_2(p)$. Since x, y are free generators of F_p, the formula (4.1) correctly defines $\widehat{\rho}$ as an endomorphism of F_p. We claim that $\widehat{\rho}$ is an automorphism of F_p. Indeed, by Lemma 3.3 we have

$$\widehat{\rho}(x)^{\beta_2}\widehat{\rho}(y)^{-\alpha_2}Z(F_p) = (x^{\alpha_1\beta_2}y^{\alpha_2\beta_2})(x^{-\beta_1\alpha_2}y^{-\beta_2\alpha_2})Z(F_p) = x^{\det\rho}Z(F_p),$$
$$\widehat{\rho}(x)^{-\beta_1}\widehat{\rho}(y)^{\alpha_1}Z(F_p) = (x^{-\alpha_1\beta_1}y^{-\alpha_2\beta_1})(x^{\beta_1\alpha_1}y^{\beta_2\alpha_1})Z(F_p) = y^{\det\rho}Z(F_p).$$

Thus xz, $yz' \in \langle\widehat{\rho}(x), \widehat{\rho}(y)\rangle$ for some z, $z' \in Z(F_p)$, and $\widehat{\rho}$ is onto F_p by Lemma 3.5.

Now let $\lambda \in \mathrm{Aut}\, F_p$, where $\lambda(x) = x^{\alpha_1}y^{\alpha_2}z_x$, $\lambda(y) = x^{\beta_1}y^{\beta_2}z_y$ for some $0 \leq \alpha_1$, α_2, β_1, $\beta_2 < p$ and z_x, $z_y \in Z(F_p)$. Then λ induces an automorphism of $F_p/Z(F_p) \cong \mathbb{Z}_p \times \mathbb{Z}_p$ by $xZ(F_p) \mapsto (\alpha_1, \alpha_2)$ and $yZ(F_p) \mapsto (\beta_1, \beta_2)$, which means that $\rho = \left(\begin{smallmatrix}\alpha_1 & \alpha_2\\ \beta_1 & \beta_2\end{smallmatrix}\right)$ belongs to $\mathrm{GL}_2(p)$, and we can consider the induced automorphism $\widehat{\rho} \in \mathrm{Aut}\, F_p$.

Let $\tau = \lambda^{-1}\widehat{\rho} \in \mathrm{Aut}\, F_p$. Then $\tau(x) = \lambda^{-1}\widehat{\rho}(x) = \lambda^{-1}(\widehat{\rho}(x)z_x z_x^{-1}) = \lambda^{-1}(\lambda(x)z_x^{-1}) = xz$, where $z = \lambda^{-1}(z_x^{-1}) \in Z(F_p)$. Similarly, $\tau(y) = yz'$ for some $z' \in Z(F_p)$. Then $\tau(x^p) = \tau(x)^p = (xz)^p = x^p$, $\tau(y^p) = y^p$, and $\tau((x,x,y)) = (\tau(x), \tau(x), \tau(y)) = (xz, xz, yz') = (x,x,y)$, $\tau((x,y,y)) = (x,y,y)$. By Lemma 3.4, τ is identical on $Z(F_p)$. □

Recall that $\mathcal{A}_p$ is the class of all 2-generated commutative automorphic loops Q possessing a central subloop $Z \cong \mathbb{Z}_p$ such that $Q/Z \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Note that among the three abelian groups $(\mathbb{Z}_p)^3$, $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ and $\mathbb{Z}_{p^3}$ of order p^3 only $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ belongs to $\mathcal{A}_p$.

Theorem 4.2. *Let p be a prime.*

(i) *Let $Q \in \mathcal{A}_p$. Then there is an epimorphism $\varphi : F_p \to Q$ with $\ker\varphi \leq Z(F_p)$.*

(ii) *Let Q_1, $Q_2 \in \mathcal{A}_p$, and let $\varphi_i : F_p \to Q_i$ be the induced epimorphisms with $\ker(\varphi_i) \leq Z(F_p)$. Then $Q_1 \cong Q_2$ if and only if there is $\rho \in \mathrm{GL}_2(p)$ such that $\ker\varphi_2 = \widehat{\rho}(\ker\varphi_1)$.*

Proof. (i) Let a, $b \in Q$ be such that $\langle a, b\rangle = Q$. Since Q is 2-generated and of nilpotency class at most two, there is an epimorphism $\psi : F \to Q$ such that $\psi(x_1) = a$, $\psi(x_2) = b$, using the notation of Theorem 2.3.

We have $c^{p^2} = 1$ for every $c \in Q$ (else Q is cyclic), and $c^p = 1$ for every $c \in A(Q)$ (because Q/Z is a group and so $A(Q) \leq Z \cong \mathbb{Z}_p$). We have just shown that $\psi(c) = 1$ for every generator c of K_p, and thus $K_p \leq \ker(\psi)$. Let $\varphi : F_p \to Q$ be the epimorphism induced by ψ, that is, $\varphi(cK_p) = \psi(c)$.

Suppose, for a contradiction, that $\ker\varphi$ is not contained in $Z(F_p)$. Then there is $x^iy^jz \in \ker\varphi \setminus Z(F_p)$ for some $0 \leq i$, $j < p$ and $z \in Z(F_p)$, where we can assume without loss of generality that $i > 0$. Let $H = \langle x^iy^jz, y\rangle$. Then $x^iz' \in H$ for some $z' \in Z(F_p)$, and so $xz'' \in H$ for some $z'' \in Z(F_p)$. By Lemma 3.5, $H = F_p$. But then $Q = \varphi(F_p) = \varphi(\langle x^iy^jz, y\rangle) = \varphi(\langle y\rangle)$ is cyclic, a contradiction.

(ii) Suppose that $\kappa : Q_1 \to Q_2$ is an isomorphism and consider the diagram (4.2), where $N_i = \ker\varphi_i$.

$$\begin{array}{ccccccccc} 1 & \to & N_2 & \to & F_p & \stackrel{\varphi_2}{\to} & Q_2 & \to & 1\\ & & \uparrow\mu & & \uparrow\lambda & & \uparrow\kappa & & \\ 1 & \to & N_1 & \to & F_p & \stackrel{\varphi_1}{\to} & Q_1 & \to & 1. \end{array} \tag{4.2}$$

Since φ_2 is onto Q_2, there are x', $y' \in F_p$ such that $\varphi_2(x') = \kappa\varphi_1(x)$ and $\varphi_2(y') = \kappa\varphi_1(y)$. As F_p has free generators x, y, an endomorphism $\lambda : F_p \to F_p$ is determined by the values $\lambda(x) = x'$, $\lambda(y) = y'$, and we have $\varphi_2\lambda = \kappa\varphi_1$. Moreover, $\langle x', y'\rangle$ intersects

every coset of N_2 in F_p, else $\varphi_2\lambda = \kappa\varphi_1$ is not onto Q_2. Then $\langle x', y'\rangle$ also intersects every coset of $Z(F_p) \geq N_2$ in F_p, in particular the cosets $xZ(F_p)$, $yZ(F_p)$. By Lemma 3.5, $\lambda \in \operatorname{Aut} F_p$.

Let μ be the restriction of λ to N_1. Then for $n \in N_1$ we have $\varphi_2\lambda(n) = \kappa\varphi_1(n) = \kappa(1) = 1$. Thus $\mu(n) = \lambda(n) \in \ker(\varphi_2) = N_2$, and μ is a monomorphism $N_1 \to N_2$. Since $|F_p/N_i| = |Q_i|$, $Q_1 \cong Q_2$, and F_p is finite, it follows that $|N_1| = |N_2|$ and $\mu : N_1 \to N_2$ is an isomorphism. By Lemma 4.1, we can write $\lambda = \widehat{\rho}\sigma$ for some $\rho \in \mathrm{GL}_2(p)$ and $\sigma \in \operatorname{Aut} F_p$ such that $\sigma(z) = z$ for every $z \in Z(F_p)$. Since $N_1 \leq Z(F_p)$ by (i), it follows that $N_2 = \mu(N_1) = \lambda(N_1) = \widehat{\rho}\sigma(N_1) = \widehat{\rho}(N_1)$.

Conversely, suppose there is $\rho \in \mathrm{GL}_2(p)$ such that $\widehat{\rho}(N_1) = N_2$. Define $\kappa : Q_1 \to Q_2$ by $\kappa(\varphi_1(u)) = \varphi_2\widehat{\rho}(u)$. This correctly defines κ because φ_1 is onto Q_1, and if $\varphi_1(u) = \varphi_1(v)$ then $uN_1 = vN_1$, $\widehat{\rho}(u)N_2 = \widehat{\rho}(v)N_2$, and $\varphi_2\widehat{\rho}(u) = \varphi_2\widehat{\rho}(v)$. Moreover, κ is a homomorphism (since φ_1, φ_2, $\widehat{\rho}$ are homomorphisms), it is onto Q_2 (since $\widehat{\rho}$, φ_2 are onto), and it is one-to-one (since $\kappa(\varphi_1(u)) = 1$ implies $\varphi_2\widehat{\rho}(u) = 1$, $\widehat{\rho}(u) \in N_2$, $u \in N_1$, $\varphi_1(u) = 1$). □

Note that $|\ker\varphi| = |F_p|/|Q| = p^6/p^3 = p^3$ in Theorem 4.2.

5. The orbits

By Theorem 4.2, in order to classify the loops of $\mathcal{A}_p$ up to isomorphism, it suffices to describe the orbits of the action of $\mathrm{GL}_2(p)$ from Lemma 4.1 on 3-dimensional subspaces of $Z(F_p) \cong (\mathbb{Z}_p)^4$.

From now on, we will write $Z(F_p) = \langle x^p\rangle \oplus \langle y^p\rangle \oplus \langle (x,x,y)\rangle \oplus \langle (x,y,y)\rangle$ additively, and we will not distinguish between $\rho \in \mathrm{GL}_2(p)$ and the induced automorphism $\widehat{\rho}$ of F_p. Moreover, we will write $\rho(x,x,y)$ instead of the formally correct $\rho((x,x,y))$.

For the rest of this section, let $G = \mathrm{GL}_2(p)$, $V = \langle x^p\rangle \oplus \langle y^p\rangle$, and $W = \langle (x,x,y)\rangle \oplus \langle (x,y,y)\rangle$.

Lemma 5.1. *The action of G on $Z(F_p)$ from Lemma 4.1 is given by*

$$\rho(x^p) = \begin{cases} \alpha_1 x^p + \alpha_2 y^p, & \text{if } p \neq 3, \\ \alpha_1 x^p + \alpha_2 y^p + \alpha_1^2\alpha_2(x,x,y) - \alpha_1\alpha_2^2(x,y,y), & \text{if } p = 3, \end{cases}$$

$$\rho(y^p) = \begin{cases} \beta_1 x^p + \beta_2 y^p, & \text{if } p \neq 3, \\ \beta_1 x^p + \beta_2 y^p + \beta_1^2\beta_2(x,x,y) - \beta_1\beta_2^2(x,y,y), & \text{if } p = 3, \end{cases}$$

$$\rho(x,x,y) = \alpha_1 \det\rho\,(x,x,y) + \alpha_2 \det\rho\,(x,y,y),$$

$$\rho(x,y,y) = \beta_1 \det\rho\,(x,x,y) + \beta_2 \det\rho\,(x,y,y),$$

where $\rho = \left(\begin{smallmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{smallmatrix}\right) \in \mathrm{GL}_2(p)$.

In particular, W is always an invariant subspace, and V is an invariant subspace if $p \neq 3$.

Proof. We have $\rho(x^p) = \rho(x)^p = (\alpha_1, \alpha_2, 0, 0, 0, 0)^p$ by definition. By Lemma 3.3, $(\alpha_1, \alpha_2, 0, 0, 0, 0)^p$ equals $(0, 0, \alpha_1, \alpha_2, 0, 0)$ when $p \neq 3$, and $(0, 0, \alpha_1, \alpha_2, \alpha_1^2\alpha_2, -\alpha_1\alpha_2^2)$ when $p = 3$. Similarly for $\rho(y^p)$. Calculating in F_p, we have

$$\begin{aligned} \rho(x,x,y) &= (\rho(x), \rho(x), \rho(y)) = (x^{\alpha_1}y^{\alpha_2}, x^{\alpha_1}y^{\alpha_2}, x^{\beta_1}y^{\beta_2}) \\ &= (x,x,y)^{\alpha_1(\alpha_1\beta_2 - \alpha_2\beta_1)}(x,x,y)^{\alpha_2(\alpha_1\beta_2 - \alpha_2\beta_1)} \end{aligned}$$

by Lemma 2.2(iv), and so $\rho(x,x,y) = \alpha_1 \det\rho\,(x,x,y) + \alpha_2 \det\rho\,(x,y,y)$ in the additive notation of $Z(F_p)$. Similarly for $\rho(x,y,y)$. □

Given a subspace N of $Z(F_p)$, denote by $G(N)$ the orbit of N under the action of G.

Lemma 5.2. *Let N be a 3-dimensional subspace of $Z(F_p)$, and assume that $p \neq 3$.*

(i) *If $W \not\subseteq N$ then $N \in G(\langle v_1, v_2 + w_2, (x,x,y)\rangle)$ for some v_1, $v_2 \in V$ and $w_2 \in W$.*
(ii) *If $V \not\subseteq N$ then $N \in G(\langle x^p, v_2 + w_2, w_3\rangle)$ for some $v_2 \in V$ and w_2, $w_3 \in W$.*

Proof. (i) Since $\dim N = 3$ and $\dim W = 2$, there is $w \in W$ such that $N \cap W = \langle w\rangle$. The subspace W is invariant by Lemma 5.1, so there is $\rho \in G$ such that $\rho(w) = (x,x,y)$. Since $\dim(N \cap V) \geq 1$ and $G(V) = V$, there is $v_1 \in V \cap \rho(N)$. Any element of $Z(F_p)$ can be written as $v_2 + w_2$ for some $v_2 \in V$, $w_2 \in W$. Part (ii) is similar. □

Proposition 5.3. *Assume that $p \neq 3$. Let*

$$\begin{aligned}
O_1 &= G(\langle x^p\rangle \oplus W),\\
O_2 &= G(V \oplus \langle (x,x,y)\rangle),\\
O_3 &= G(\langle x^p, y^p + (x,y,y), (x,x,y)\rangle),\\
O_4 &= G(\langle y^p, x^p + (x,y,y), (x,x,y)\rangle),\\
O_5 &= G(\langle y^p, \lambda x^p + (x,y,y), (x,x,y)\rangle),
\end{aligned}$$

where λ is not a square in $\mathbb{Z}_p$. (When $p = 2$, every element of $\mathbb{Z}_p$ is a square, and we let $O_5 = \emptyset$.) Then $O_1 \cup O_2 \cup O_3 \cup O_4 \cup O_5$ is a disjoint union of all 3-dimensional subspaces of $Z(F_p)$.

Proof. Let N be a 3-dimensional subspace of $Z(F_p)$. Throughout the proof, assume that all elements v_i belong to V, and all elements w_i belong to W.

First suppose that $W \subseteq N$. Then $V \not\subseteq N$ (else $Z(F_p) = V \oplus W \subseteq N$, a contradiction), so Lemma 5.2 implies that $N \in G(\langle x^p, v_2 + w_2, w_3\rangle)$. Since $G(W) = W \subseteq N$, we have $W \subseteq \langle x^p, v_2 + w_2, w_3\rangle$, so $\langle x^p, v_2 + w_2, w_3\rangle = \langle x^p, v_2\rangle \oplus W$. Thus $v_2 \in \langle x^p\rangle$ and $N \in O_1$.

Now suppose that $V \subseteq N$. Then $W \not\subseteq N$ and Lemma 5.2 implies that $N \in G(\langle v_1, v_2 + w_2, (x,x,y)\rangle)$. Since $V \subseteq N$ and $G(V) = V$, we deduce $N \in G(V \oplus \langle (x,x,y)\rangle) = O_2$. Conversely, any element of O_2 contains V.

Finally suppose that $V \not\subseteq N$ and $W \not\subseteq N$. By Lemma 5.2, $N \in G(\langle v_1, v_2 + w_2, (x,x,y)\rangle)$. Note that $\langle v_1, v_2\rangle = V$, else $\langle v_1, v_2 + w_2, (x,x,y)\rangle = \langle v_1, w_2, (x,x,y)\rangle$, and either this subspace contains W (when $w_2 \notin \langle (x,x,y)\rangle$), a contradiction, or it has dimension 2 (when $w_2 \in \langle (x,x,y)\rangle$), a contradiction again. Also, $\langle w_2, (x,x,y)\rangle = W$, else $\langle v_1, v_2 + w_2, (x,x,y)\rangle = \langle v_1, v_2, (x,x,y)\rangle$, $V \subseteq N$, a contradiction. We can therefore assume that $N \in G(\langle v_1, v_2 + \gamma(x,y,y), (x,x,y)\rangle)$, where $\gamma \neq 0$, $\langle v_1, v_2\rangle = V$ and $v_1 = \tau_1 x^p + \tau_2 y^p$ for some τ_1, τ_2.

Suppose first that $\tau_2 = 0$. Then $N \in G(\langle x^p, y^p + \gamma(x,y,y), (x,x,y)\rangle)$ for some $\gamma \neq 0$. Consider $\rho = \left(\begin{smallmatrix} \alpha_1 & 0 \\ 0 & \beta_2 \end{smallmatrix}\right) \in G$, where $\beta_2 = (\alpha_1\gamma)^{-1}$. Then $\rho(x^p) = \alpha_1 x^p$, $\rho(y^p) = \beta_2 y^p$, $\rho(x,x,y) = \alpha_1^2\beta_2(x,x,y)$ and $\rho(y^p + \gamma(x,x,y)) = \beta_2 y^p + \gamma\alpha_1\beta_2^2(x,y,y) = \beta_2(y^p + (x,y,y))$. Hence $N \in O_3$.

Now suppose that $\tau_2 \neq 0$. Consider $\rho = \left(\begin{smallmatrix} \alpha_1 & 0 \\ \beta_1 & \beta_2 \end{smallmatrix}\right) \in G$, where $\beta_1 = -\tau_1\alpha_1/\tau_2$. Then $\rho(x,x,y) = \alpha_1^2\beta_2(x,x,y)$, $\rho(x,y,y) = \beta_1\alpha_1\beta_2(x,x,y) + \alpha_1\beta_2^2(x,x,y)$, and $\rho(v_1) = \tau_1\alpha_1 x^p + \tau_2(\beta_1 x^p + \beta_2 y^p) = \tau_2\beta_2 y^p$. Hence we have $N \in G(\langle y^p, x^p + \gamma(x,y,y), (x,x,y)\rangle)$ for some $\gamma \neq 0$. Consider again $\rho = \left(\begin{smallmatrix} \alpha_1 & 0 \\ 0 & \beta_2 \end{smallmatrix}\right) \in G$. Then $\rho(\langle y^p, x^p + \gamma(x,y,y), (x,x,y)\rangle) = \langle y^p, \alpha_1 x^p + \gamma\alpha_1\beta_2^2(x,y,y), (x,x,y)\rangle = \langle y^p, x^p + \gamma\beta_2^2(x,y,y), (x,x,y)\rangle$, and we conclude that either $N \in O_4$ or $N \in O_5$, depending on whether γ is a square in $\mathbb{Z}_p$.

It remains to show that $O_1, \dots, O_5$ are pairwise disjoint. If $N \in O_1$, we have $W \subseteq N$, and thus $O_1 \cap O_i = \emptyset$ for $i > 1$. If $N \in O_2$, we have $V \subseteq N$, and thus $O_2 \cap O_i = \emptyset$ for $i > 2$.

Suppose that $N \in O_3 \cap O_4$. Then there is $\rho = \left(\begin{smallmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{smallmatrix}\right) \in G$ such that, without loss of generality, $N = \langle y^p, x^p + (x,y,y), (x,x,y)\rangle = \rho(\langle x^p, y^p + (x,y,y), (x,x,y)\rangle) = \langle \alpha_1 x^p + \alpha_2 y^p, \beta_1 x^p + \beta_2 y^p + w_1, w_2\rangle$. Since $y^p \in N$, we conclude that $\alpha_1 x^p \in N$. Should $\alpha_1 \neq 0$, we would have $V \subseteq N$, a contradiction. Hence $\alpha_1 = 0$ and $\rho(x,x,y) = \alpha_2 \det\rho\ (x,y,y) \in N$. As $\alpha_2 \neq 0$, we see that $(x,y,y) \in N$, $x^p \in N$, $V \subseteq N$, a contradiction again. Therefore $O_3 \cap O_4 = \emptyset$. Similarly, $O_3 \cap O_5 = \emptyset$.

Suppose that $N \in O_4 \cap O_5$. We can assume that $N = \langle y^p, \lambda x^p + (x,y,y), (x,x,y)\rangle = \rho(\langle y^p, x^p + (x,y,y), (x,x,y)\rangle) = \langle \beta_1 x^p + \beta_2 y^p, v_1 + w_1, w_2\rangle$, where λ is not a square. If $\beta_1 \neq 0$, we conclude that $x^p \in N$, $V \subseteq N$, a contradiction. Thus $\beta_1 = 0$, $\det\rho = \alpha_1\beta_2$, and $\alpha_1 x^p + \alpha_2 y^p + \alpha_1\beta_2^2(x,y,y) \in N$, $\alpha_1 x^p + \alpha_1\beta_2^2(x,y,y) \in N$, $\lambda x^p + \lambda\beta_2^2(x,y,y) \in N$, and since also $\lambda x^p + (x,y,y) \in N$, we have $(\lambda\beta_2^2 - 1)(x,y,y) \in N$. As λ is not a square, $\lambda\beta_2^2$ is not a square, but 1 is a square, thus $\lambda\beta_2^2 - 1 \neq 0$, $(x,y,y) \in N$, $W \subseteq N$, a contradiction. □

Proposition 5.4. *Suppose that $p = 3$, and let*

$$\begin{aligned} O_1 &= G(\langle x^p\rangle \oplus W),\\ O_2 &= G(V \oplus \langle (x,x,y)\rangle),\\ O_3 &= G(\langle x^p + (x,y,y), y^p, (x,x,y)\rangle),\\ O_4 &= G(\langle x^p - (x,y,y), y^p, (x,x,y)\rangle),\\ O_5 &= G(\langle x^p - (x,y,y), y^p + (x,y,y), (x,x,y)\rangle). \end{aligned}$$

Then $O_1 \cup O_2 \cup O_3 \cup O_4 \cup O_5$ is a disjoint union of all 3-dimensional subspaces of $Z(F_p)$.

Proof. We leave the proof to the reader, who will need Lemma 5.1 and an argument similar to the proof of Proposition 5.3. Alternatively, the proof can be accomplished by a direct computer calculation, for instance in `GAP`. (The calculation will in addition show that the cardinalities of $O_1, \dots, O_5$ are 12, 4, 12, 4 and 8, respectively, for the correct total of $40 = (3^4-1)(3^4-3)(3^4-3^2)/((3^3-1)(3^3-3)(3^3-3^2))$ subspaces.) □

6. Main result

Theorem 6.1. *Let p be a prime, and let $\mathcal{A}_p$ be the class of all 2-generated commutative automorphic loops Q possessing a central subloop $Z \cong \mathbb{Z}_p$ such that $Q/Z \cong \mathbb{Z}_p \times \mathbb{Z}_p$. If $p = 2$, let $O_1, \dots, O_4$ be as in Proposition 5.3. If $p = 3$, let $O_1, \dots, O_5$ be as in Proposition 5.4. If $p > 3$, let $O_1, \dots, O_5$ be as in Proposition 5.3. For every i, let $N_i \in O_i$ and $Q_i = F_p/N_i$. Then $Q \in \mathcal{A}_p$ is isomorphic to precisely one Q_i. Moreover, Q_i is a group if and only if $i = 1$.*

Proof. Combine Theorem 4.2 and Propositions 5.3, 5.4. It remains to show that Q_i is a group if and only if $i = 1$. Now, $Q_i = F_p/N_i$ is a group if and only if $A(F_p) \leq N_i$. By Lemma 3.4, $A(F_p) = W$. A quick inspection of the orbits shows that only N_1 contains W. □

We conclude the paper with a classification of commmutative automorphic loops of order p^3.

Lemma 6.2. *Let p be a prime and let Q be a nilpotent commutative automorphic loop of order p^3. If Q is not a group then $Q \in \mathcal{A}_p$.*

Proof. The center of Q is a nontrivial normal associative subloop of Q, hence of order dividing p^3. Let Z be a central subloop of Q of order p, so $Z \cong \mathbb{Z}_p$. Then Q/Z is a commutative automorphic loop of order p^2, necessarily a group by [5]. Since Q is power-associative, Q/Z cannot be cyclic, else Q is associative. Hence $Q/Z \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Assume for a while that Q is not 2-generated. Then any two elements of Q generate a proper subloop of Q, hence a group of order at most p^2. Thus Q is diassociative. By the already-mentioned result of Osborn [8], Q is a commutative Moufang loop. But commutative Moufang loops of order p^3 are associative by [1], a contradiction. Hence Q is 2-generated. □

The only commutative automorphic loop of order 8 with trivial center has been described in [5, Section 3]. Its multiplication table is

(6.1)

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	1	2	7	8	5	6
4	4	3	2	1	8	7	6	5
5	5	6	7	8	1	4	2	3
6	6	5	8	7	4	1	3	2
7	7	8	5	6	2	3	1	4
8	8	7	6	5	3	2	4	1

Theorem 6.3 (Commutative automorphic loops of order p^3)**.** *Let p be a prime. If $p = 2$, let $O_2, \ldots, O_4$ be as in Proposition 5.3. If $p = 3$, let $O_2, \ldots, O_5$ be as in Proposition 5.4. If $p > 3$, let $O_2, \ldots, O_5$ be as in Proposition 5.3. For every i, let $N_i \in O_i$ and $Q_i = F_p/N_i$.*

There are precisely 7 commutative automorphic loops of order p^3 up to isomorphism, including the three abelian groups $(\mathbb{Z}_p)^3$, $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$, $\mathbb{Z}_{p^3}$. If p is odd, the nonassociative commutative automorphic loops of order p^3 are precisely the loops $Q_2, \ldots, Q_5$. If $p = 2$, the nonassociative commutative automorphic loops of order p^3 are precisely the loops $Q_2, \ldots, Q_4$, and the loop with multiplication table (6.1).

Proof. The three abelian groups of order p^3 are certainly automorphic.

By a result of [6], every commutative automorphic loop of odd order p^k is nilpotent. Hence every nonassociative automorphic loop of odd order p^3 is in $\mathcal{A}_p$, by Lemma 6.2. The loops of $\mathcal{A}_p$ are classified up to isomorphism in Theorem 6.1, and they include the abelian group Q_1 ($\cong \mathbb{Z}_p \times \mathbb{Z}_{p^2}$).

When $p = 2$ we can proceed similarly, except that we have to account for the unique commutative automorphic loop (6.1) of order 8 with trivial center. □

Theorem 6.3 proves [5, Conjecture 5.12] and answers [5, Problem 5.13].

References

[1] R. H. Bruck, A Survey of Binary Systems, Springer-Verlag, 1971.

[2] R. H. Bruck and L. J. Paige, *Loops whose inner mappings are automorphisms*, Ann. of Math. (2) **63** (1956), 308–323.

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

[4] P. Jedlička, M. Kinyon and P. Vojtěchovský, *The structure of commutative automorphic loops*, Trans. Amer. Math. Soc. **363** (2011), 365–384.
[5] P. Jedlička, M. Kinyon and P. Vojtěchovský, *Constructions of commutative automorphic loops*, Comm. Algebra **38** (2010), no. **9**, 3243–3267.
[6] P. Jedlička, M. Kinyon and P. Vojtěchovský, *Nilpotency in automorphic loops of prime power order*, J. Algebra **350** (2012), no. **1**, 64–76.
[7] M. K. Kinyon, K. Kunen and J. D. Phillips, *Every diassociative A-loop is Moufang*, Proc. Amer. Math. Soc. **130** (2002), 619–624.
[8] J. M. Osborn, *A theorem on A-loops*, Proc. Amer. Math. Soc. **9** (1958), 347–349.

(Barros, Grishkov) Institute of Mathematics and Statistics, University of Sao Paulo, Rua do Matão, 1010, Cidade Universitária, São Paulo, SP, Brazil, CEP 05508-090
E-mail address, Barros: dylene@ime.usp.br

E-mail address, Grishkov: shuragri@gmail.com

(Vojtěchovský) Department of Mathematics, University of Denver, 2360 S Gaylord St, Denver, Colorado 80208, USA
E-mail address, Vojtěchovský: petr@math.du.edu