Automorphic loops arising from module endomorphisms

By ALEXANDER GRISHKOV (São Paulo), MARINA RASSKAZOVA (Omsk)
and PETR VOJTĚCHOVSKÝ (Denver)

Abstract. A loop is automorphic if all its inner mappings are automorphisms. We construct a large family of automorphic loops as follows. Let $R$ be a commutative ring, $V$ an $R$-module, $E = \text{End}_R(V)$ the ring of $R$-endomorphisms of $V$, and $W$ a subgroup of $(E, +)$ such that $ab = ba$ for every $a, b \in W$ and $1 + a$ is invertible for every $a \in W$. Then $Q_{R,V}(W)$ defined on $W \times V$ by

$$(a, u)(b, v) = (a + b, u(1 + b) + v(1 - a))$$

is an automorphic loop.

A special case occurs when $R = k < K = V$ is a field extension and $W$ is a $k$-subspace of $K$ such that $k1 \cap W = 0$, naturally embedded into $\text{End}_K(K)$ by $a \mapsto M_a$, $bM_a = ba$. In this case we denote the automorphic loop $Q_{R,V}(W)$ by $Q_{k<K}(W)$.

We call the parameters tame if $k$ is a prime field, $W$ generates $K$ as a field over $k$, and $K$ is perfect when $\text{char}(k) = 2$. We describe the automorphism groups of tame automorphic loops $Q_{k<K}(W)$, and we solve the isomorphism problem for tame automorphic loops $Q_{k<K}(W)$. A special case solves a problem about automorphic loops of order $p^3$ posed by Jedlička, Kinyon and Vojtěchovský.

We conclude the paper with a construction of an infinite 2-generated abelian-by-cyclic automorphic loop of prime exponent.

\textbf{Mathematics Subject Classification:} Primary: 20N05; Secondary: 11R11, 12F99.
\textbf{Key words and phrases:} automorphic loop, automorphic loop of order $p^3$, automorphism group, semidirect product, field extension, quadratic extension, module, module endomorphism.

Research partially supported by the Simons Foundation Collaboration Grant 210176 to Petr Vojtěchovský.
1. Introduction

A groupoid $Q$ is a quasigroup if for all $x \in Q$ the translations $L_x : Q \to Q$, $R_x : Q \to Q$ defined by $yL_x = xy$, $yR_x = yx$ are bijections of $Q$. A quasigroup $Q$ is a loop if there is $1 \in Q$ such that $1x = x1 = x$ for every $x \in Q$.

Let $Q$ be a loop. The multiplication group of $Q$ is the permutation group $\text{Mlt}(Q) = \langle L_x, R_x : x \in Q \rangle$, and the inner mapping group of $Q$ is the subgroup $\text{Inn}(Q) = \{ \varphi \in \text{Mlt}(Q) : 1\varphi = 1 \}$.

A loop $Q$ is said to be automorphic if $\text{Inn}(Q) \leq \text{Aut}(Q)$, that is, if every inner mapping of $Q$ is an automorphism of $Q$. Since, by a result of Bruck [1], $\text{Inn}(Q)$ is generated by the bijections $T_x = R_x L_x^{-1}$, $L_{x,y} = L_x L_y L_{yx}^{-1}$, $R_{x,y} = R_x R_y R_{xy}^{-1}$, a loop $Q$ is automorphic if and only if $T_x$, $L_{x,y}$, $R_{x,y}$ are homomorphisms of $Q$ for every $x$, $y \in Q$. In fact, by [7, Theorem 7.1], a loop $Q$ is automorphic if and only if every $T_x$ and $R_{x,y}$ are automorphisms of $Q$. The variety of automorphic loops properly contains the variety of groups.

See [1] or [12] for an introduction to loop theory. The first paper on automorphic loops is [2]. It was shown in [2] that automorphic loops are power-associative, that is, every element of an automorphic loop generates an associative subloop. Many structural results on automorphic loops were obtained in [9], where an extensive list of references can be found.

1.1. The general construction. In this paper we study the following construction.

Construction 1.1. Let $R$ be a commutative ring, $V$ an $R$-module and $E = \text{End}_R(V)$ the ring of $R$-endomorphisms of $V$. Let $W$ be a subgroup of $(E, +)$ such that

(A1) $ab = ba$ for every $a, b \in W$, and

(A2) $1 + a$ is invertible for every $a \in W$,

where $1 \in E$ is the identity endomorphism on $V$.

Define $Q_{R,V}(W)$ on $W \times V$ by

$$(a, u)(b, v) = (a + b, u(1 + b) + v(1 - a)).$$

(1.1)

We show in Theorem 2.2 that $Q_{R,V}(W)$ is always an automorphic loop.

Two special cases of this construction appeared in the literature. First, in [6], the authors proved that commutative automorphic loops of odd prime power order
are centrally nilpotent, and constructed a family of (noncommutative) automorphic loops of order $p^3$ with trivial center by using the following construction.

**Construction 1.2.** Let $k$ be a field and $M_2(k)$ the vector space of $2 \times 2$ matrices over $k$ equipped with the determinant norm. Let $I$ be the identity matrix, and let $A \in M_2(k)$ be such that $kI \oplus kA$ is an anisotropic plane in $M_2(k)$, that is, $\det(aI + bA) \neq 0$ for every $(a, b) \neq (0, 0)$. Define $Q_k(A)$ on $k \times (k \times k)$ by $(a, u)(b, v) = (a + b, u(I + bA) + v(I - aA))$.

We will show in Section 4 that the loops $Q_k(A)$ are a special case of the construction $Q_{R,V}(W)$ and hence automorphic. If $k = \mathbb{F}_p$ then $Q_k(A)$ has order $p^3$, exponent $p$ and trivial center, by [6, Proposition 5.6].

Second, in [10], Nagy used a construction of automorphic loops based on Lie rings (cf. [8] and [9]) and arrived at the following.

**Construction 1.3.** Let $V, W$ be vector spaces over $\mathbb{F}_2$, and let $\beta : W \to \text{End}(V)$ be a linear map such that $a\beta b\beta = b\beta a\beta$ for every $a, b \in W$, and $1 + a\beta$ is invertible for every $a \in W$. Define a loop $(W \times V, \ast)$ by $(a, u) \ast (b, v) = (a + b, u(1 + b\beta) + v(1 + a\beta))$.

When $\beta$ is injective, Construction 1.3 is a special case of our Construction 1.1, and when $\beta$ is not injective, it is a slight variation. By [10, Proposition 3.2], $(W \times V, \ast)$ is an automorphic loop of exponent 2 and, moreover, if $\beta$ is injective and at least one $a\beta$ is invertible then $(W \times V, \ast)$ has trivial center.

### 1.2. The field extension construction.

Most of this paper is devoted to the following special case of Construction 1.1.

**Construction 1.4.** Let $R = k < K = V$ be a field extension, and let $W$ be a $k$-subspace of $V$ such that $k1 \cap W = 0$. Embed $W$ into $\text{End}_k(K)$ via $a \mapsto M_a$, $bM_a = ba$. Denote by $Q_{k<K}(W)$ the loop $Q_{R,V}(W)$ of Construction 1.1.

Assuming the situation of Construction 1.4, the condition (A1) of Construction 1.1 is obviously satisfied because the multiplication in $K$ is commutative and associative. Moreover, $k1 \cap W = 0$ is equivalent to $1 + a \neq 0$ for all $a \in W$, which is equivalent to (A2). Construction 1.1 therefore applies and $Q_{k<K}(W)$ is an automorphic loop.

For the purposes of this paper, we call the parameters $k, K, W$ of Construction 1.4 *tame* if $k$ is a prime field, $W$ generates $K$ as a field over $k$, and $K$ is perfect when $\text{char}(k) = 2$.

In Corollary 3.3 we solve the isomorphism problem for tame automorphic loops $Q_{k<K}(W)$, given a fixed extension $k < K$, and in Theorem 3.5 we describe
the automorphism groups of tame automorphic loops $Q_{k<K}(W)$.

In particular, we solve the isomorphism problem when $k$ is a finite prime field and $K$ is a quadratic extension of $k$. This answers a problem about automorphic loops of order $p^3$ posed in [6], and it disproves [6, Conjecture 6.5].

Finally, in Section 5 we use the construction $Q_{k<K}(W)$ to obtain an infinite 2-generated abelian-by-cyclic automorphic loop of prime exponent.

2. Automorphic loops from module endomorphisms

Throughout this section, assume that $R$ is a commutative ring, $V$ an $R$-module, $W$ a subgroup of $E = (\text{End}_R(V), +)$ satisfying (A1) and (A2), and $Q_{R,V}(W)$ is defined on $W \times V$ by (1.1) as in Construction 1.1.

It is easy to see that $(0, 0) = (0_E, 0_V)$ is the identity element of $Q_{R,V}(W)$, and that $(a, u) \in Q_{R,V}(W)$ has the two-sided inverse $(-a, -u)$.

Using the notation $I_a = 1 + a$ and $J_a = 1 - a$, we can rewrite the multiplication formula (1.1) as

$$(a, u)(b, v) = (a + b, uI_b + vJ_a).$$

A straightforward calculation then shows that the left and right translations $L_{(a, u)}, R_{(a, u)}$ in $Q_{R,V}(W)$ are invertible, with their inverses given by

$$(a, u) \setminus (b, v) = (b, v)L_{(a, u)}^{-1} = (b - a, (v - uI_b - a)J_a^{-1}),$$

and

$$(b, v)/(a, u) = (b, v)R_{(a, u)}^{-1} = (b - a, (v - uJ_b - a)I_a^{-1}),$$

respectively. Hence $Q_{R,V}(W)$ is a loop.

The multiplication formula (1.1) yields $(a, 0)(b, 0) = (a + b, 0)$ and $(0, u)(0, v) = (0, u + v)$, so $W \times 0$ is a subloop of $Q_{R,V}(W)$ isomorphic to the abelian group $(W, +)$ and $0 \times V$ is a subloop of $Q_{R,V}(W)$ isomorphic to the abelian group $(V, +)$. Moreover, the mapping $Q_{R,V}(W) = W \times V \to W$ defined by $(a, u) \mapsto a$ is a homomorphism with kernel $0 \times V$. Thus $0 \times V$ is a normal subloop of $Q_{R,V}(W)$.

We proceed to show that $Q_{R,V}(W)$ is an automorphic loop.

Let $C_E(W) = \{ a \in E : ab = ba \text{ for every } b \in W \}$.

**Lemma 2.1.** For $d \in C_E(W)^*$ and $x \in V$ define $f_{(d,x)} : Q_{R,V}(W) \to Q_{R,V}(W)$ by

$$(a, u)f_{(d,x)} = (a, xa + ud).$$

Then $f_{(d,x)} \in \text{Aut}(Q_{R,V}(W))$. 
By Lemma 2.1, Thus
\[ L(xb + ud + vbd + xd - xa + vd) = (a, b) \]
The other hand, \((a, u)f(xb, ud + vbd + edx - xa + vd) = (a, b)(xb + vd) = (a, b, (xa + ud)I_d + (xb + vd)J_a)\], where the second coordinate is equal to \(x + xa + ud + vbd + xb - xda + vd - vda\). Note that \(ab = ba\) because \(a, b \in W\), and \(ad = da, bd = db\) because \(d \in C_E(W)\). The mapping \(f(xb, ud)\) is therefore an endomorphism of \(Q_{R, V}(W)\).

Suppose that \((a, u)f(xb, ud) = (b, v)f(xb, ud)\). Then \((a, xa + ud) = (b, xb + vd)\) implies \(a = b = d\) is invertible, we have \(u = v\), proving that \(f(xb, ud)\) is one-to-one.

Given \((b, v) \in Q_{R, V}(W)\), we have \((a, u)f(xb, ud) = (b, v)f(xb, ud)\) if and only if \((a, xa + ud) = (b, v). We can therefore take \(a = b\) and \(u = (v - xa)d^{-1}\) to see that \(f(xb, ud)\) is onto.

**Theorem 2.2.** The loops \(Q_{R, V}(W)\) obtained by Construction 1.1 are automorphic.

**Proof.** We have already shown that \(Q = Q_{R, V}(W)\) is a loop. In view of [7, Theorem 7.1], it suffices to show that for every \((a, u), (b, v) \in Q\) the inner mappings \(T(a, u), L(a, u, (b, v))\) are automorphisms of \(Q\). Using (2.1), we have
\[
(b, v)T(a, u) = (b, v)R(a, u)L_{(a, u)}^{-1} = (b + a, vI_a + uJ_b)L_{(a, u)}^{-1}
\]
\[= (b, (vI_a + uJ_b - uI_b)J_a^{-1}) = (b, u(J_0 - I_b)J_a^{-1} + vI_aJ_a^{-1})
\]
\[= (b, -2ubJ_a^{-1} + vI_aJ_a^{-1}) = (b, (-2ubJ_a^{-1})b + v(J_a^{-1}))\],
where we have also used \(bJ_a^{-1} = J_a^{-1}b\). Thus \(T(a, u) = f(xb, ud)\) with \(d = I_aJ_a^{-1}\) and \(x = -2ubJ_a^{-1} \in V\). Note that \(d \in C_E(W)^+\) by (A1), (A2). By Lemma 2.1, \(T(a, u) \in \text{Aut}(Q)\).

Furthermore,
\[(c, w)L_{(a, u), (b, v)} = ((b, v) \cdot (a, u)(c, w)L_{(a, u)}^{-1}
\]
\[= ((b, v)(a + c, uI_c + wJ_a))L_{(b + a, vI_c + uJ_a)}^{-1}
\]
\[= (b + a + c, vI_a + uI_c + wJ_aJ_b + wJ_aJ_b)L_{(b + a, vI_a + uJ_a)}^{-1}
\]
\[= (c, vI_a + c + uI_c + wJ_aJ_b - vI_aI_c - uJ_bI_c)J_a^{-1}
\]
\[= (c, vI_a + c - I_J_aI_c)J_a^{-1} + wJ_aJ_bJ_a^{-1}
\]
\[= (c, -vaJ_a^{-1} + wJ_aJ_bJ_a^{-1}) = (c, (-vaJ_a^{-1})c + w(J_aJ_bJ_a^{-1})).
\]
Thus \(L_{(a, u), (b, v)} = f(xb, ud)\) with \(d = J_aJ_bJ_a^{-1} \in C_E(W)^+\) and \(x = -vaJ_a^{-1} \in V\).

By Lemma 2.1, \(L_{(a, u), (b, v)} \in \text{Aut}(Q)\).\qed
For a loop $Q$, the *associator subloop* $\text{Asc}(Q)$ is the smallest normal subloop of $Q$ such that $Q/\text{Asc}(Q)$ is a group. Given $x, y, z \in Q$, the *associator* $[x, y, z]$ is the unique element of $Q$ such that $(xy)z = [x, y, z](x(yz))$, so

$$[x, y, z] = ((xy)z)/(x(yz)) = ((xy)z)R_{x(yz)}^{-1}.$$ 

It is easy to see that $\text{Asc}(Q)$ is the smallest normal subloop of $Q$ containing all associators.

**Lemma 2.3.** Let $Q = Q_{R,V}(W)$. Then

$$[(a,u),(b,v),(c,w)] = (0,(ubc - wab)I_{a+b+c})$$

for every $(a,u), (b,v), (c,w) \in Q$. In particular, $\text{Asc}(Q) \leq 0 \times V$.

**Proof.** The associator $[[a,u),(b,v),(c,w)]$ is equal to

$$((a,u)(b,v) \cdot (c,w))R_{(a,u),(b,v),(c,w)}^{-1}$$

$$= (a + b + c, (uI_b + vJ_a)I_{c} + wJ_{a+b})R_{(a+b+c,uI_{a+b+c}+(vI_{c}+wJ_{b})I_{c})}^{-1}$$

$$= (0,(uJ_bI_{c} + vJ_aI_{c} + wJ_{a+b} - uJ_{b+c} - vJ_{c}J_a - wJ_{b}J_a)I_{a+b+c})^{-1}$$

$$= (0,(ubc - wab)I_{a+b+c})^{-1}.$$ 

Since $0 \times V$ is a normal subloop of $Q$, we are done.

**Corollary 2.4.** Let $Q = Q_{R,V}(W)$.

(i) $Q$ is a group if and only if $W^2 = \{ab : a, b \in W\} = 0$.

(ii) If $VW^2 = V$ then $\text{Asc}(Q) = 0 \times V$.

**Proof.** (i) It is clear that $Q$ is a group if and only if $\text{Asc}(Q) = 0$. Suppose that $Q$ is a group. Taking $w = 0$ and $a = -(b + c)$ in Lemma 2.3, we get $[(a,u),(b,v),(c,w)] = (0,ubc)$, so $W^2 = 0$. Conversely, if $W^2 = 0$ then the formula of Lemma 2.3 shows that every associator vanishes.

(ii) As above, with $w = 0$ and $a = -(b + c)$ we get $[(a,u),(b,v),(c,w)] = (0,ubc)$. Since $VW^2 = V$, we conclude that $0 \times V \leq \text{Asc}(Q)$. The other inclusion follows from Lemma 2.3.

### 3. Automorphic loops from field extensions

Throughout this section we will assume that $R = k < K = V$ is a field extension, $k$ embeds into $K$ via $\lambda \mapsto \lambda 1$, and $W$ is a $k$-subspace of $K$ such that
k1 \cap W = 0$, where we identify $a \in W$ with $M_a : K \to K$, $b \mapsto ba$. We write $M_W = \{M_a : a \in W\}$.

We have already pointed out in the introduction that (A1), (A2) are then satisfied, giving rise to the automorphic loop $Q_{k<K}(W)$ of Construction 1.4. Note that the multiplication formula (1.1) on $W \times K$ makes sense as written even with addition and multiplication from $K$.

**Corollary 3.1.** Let $Q = Q_{k<K}(W)$ with $W \neq 0$. Then $\text{Asc}(Q) = 0 \times K$.

**Proof.** Let $0 \neq a \in W$ and note that $M_a$ is a bijection of $V$. Thus $VW^2 \supseteq VM_a\cdot M_a = V$, and we are done by Corollary 2.4.

### 3.1. Isomorphisms

We proceed to investigate isomorphisms between loops $Q_{k<K}(W)$ for a fixed field extension $k < K$.

Let $W_0, W_1$ be two $k$-subspaces of $K$ satisfying $k1 \cap W_0 = 0 = k1 \cap W_1$. Let 

$$S(W_0, W_1) = \{A : A \text{ is an additive bijection } K \to K \text{ and } A^{-1}M_{W_0}A = M_{W_1}\}.$$ 

Any $A \in S(W_0, W_1)$ induces the map $\bar{A} : W_0 \to W_1$ defined by 

$$A^{-1}M_aA = M_{aA}, \quad a \in W_0,$$

in fact an additive bijection $W_0 \to W_1$. Indeed: $\bar{A}$ is onto $W_1$ by definition; if $a, b \in W_0$ are such that $A^{-1}M_aA = A^{-1}M_bA$ then $M_a = M_b$ and $a = 1M_a = 1M_b = b$, so $\bar{A}$ is one-to-one; and $M_{(a+b)\cdot A} = A^{-1}M_{a+b}A = A^{-1}(M_a + M_b)A = A^{-1}M_aA + A^{-1}M_bA = M_{a\cdot \bar{A}} + M_{b\cdot \bar{A}}$, so $(a + b)\cdot \bar{A} = a\cdot \bar{A} + b\cdot \bar{A}$.

**Proposition 3.2.** For $i \in \{0, 1\}$, let $Q_i = Q_{k<K}(W_i)$ with $W_i \neq 0$. Suppose that $K$ is perfect if $\text{char}(k) = 2$. Then there is a one-to-one correspondence between the set $\text{Iso}(Q_0, Q_1)$ of all isomorphisms $Q_0 \to Q_1$ and the set $S(W_0, W_1) \times K$. The correspondence is given by 

$$\Phi : \text{Iso}(Q_0, Q_1) \to S(W_0, W_1) \times K, \quad f\Phi = (A, c),$$

where $(A, c)$ are defined by 

$$(0, u)f = (0, uA) \quad \text{and} \quad (a, 0)f = (aA, c \cdot a\bar{A}),$$

and by the converse map

$$\Psi : S(W_0, W_1) \times K \to \text{Iso}(Q_0, Q_1), \quad (A, c)\Psi = f,$$

where $f$ is defined by

$$(a, u)f = (a\bar{A}, c \cdot a\bar{A} + uA). \quad (3.1)$$
PROOF. Given \( A \in S(W_0, W_1) \) and \( c \in K \), let \( f : Q_0 \to Q_1 \) be defined by (3.1). It is not difficult to see that \( f \) is a bijection. We claim that \( f \) is a homomorphism. Indeed, \( A \) is additive, we have

\[
(a, u)f \cdot (b, v)f = (aA, c \cdot aA + uA)(bA, c \cdot bA + vA) = (aA + bA, (c \cdot aA + uA)I_{bA} + (c \cdot bA + vA)J_{aA})
\]

and

\[
((a, u)(b, v))f = (a + b, uI_b + vJ_a)f = ((a + b)A, c \cdot (a + b)A + (uI_b + vJ_a)A),
\]

so it remains to show \( AI_{bA} = I_bA \) and \( AJ_{aA} = J_aA \) for every \( a, b \in W_0 \). This follows from \( A^{-1}M_aA = M_aA \), and we conclude that \( \Psi \) is well-defined.

Conversely, let \( f : Q_0 \to Q_1 \) be an isomorphism. Corollary 3.1 gives \( \text{Asc}(Q_0) = 0 \times K = \text{Asc}(Q_1) \), and so \( (0 \times K)f = 0 \times K \). Hence there is a bijection \( A : K \to K \) such that \( (0, u)f = (0, uA) \) for every \( u \in K \). Then \( (0, uA + vA) = (0, uA)(0, vA) = (0, u)f(0, v)f = ((0, u)(0, v))f = (0, u + v)f = (0, (u + v)A) \) shows that \( A \) is additive.

Let \( B : W_0 \to W_1, C : W_0 \to K \) be such that \( (a, 0)f = (aB, aC) \) for every \( a \in W_0 \). Note that \( (0, 0)f = (0, 0) \) implies \( 0B = 0 = 0C \). Because \( (a, u) = (a, 0)(0, uJ_a^{-1}) \), we must have

\[
(a, u)f = (a, 0)f \cdot (0, uJ_a^{-1})f = (aB, aC)(0, uJ_a^{-1}A) = (aB, aC + uJ_a^{-1}A)J_{aB}). \tag{3.2}
\]

This proves that \( B \) is onto \( W_1 \). Since

\[
((a + b)B, (a + b)C) = (a + b, 0)f = ((a, 0)(b, 0))f = (a, 0)f \cdot (b, 0)f = (aB, aC)(bB, bC) = (aB + bB, aCI_{bB} + bCJ_{aB}),
\]

\( B \) is additive. To show that \( B \) is one-to-one, suppose that \( aB = bB \). Then \( (a - b)B = 0 \) by additivity, and \( a = b \) follows from the fact that \( (0, K)f = (0, K) \).

We also deduce from the above equality that

\[
(a + b)C = aC + aC \cdot bB + bC - bC \cdot aB. \tag{3.3}
\]

Using (3.3) and \( (a + b)C = (b + a)C \), we obtain \( 2(aC \cdot bB) = 2(bC \cdot aB) \). If \( \text{char}(k) \neq 2 \), we deduce

\[
aC \cdot bB = bC \cdot aB. \tag{3.4}
\]
If $\text{char}(k) = 2$, we can use (3.3) repeatedly to get
\[
bC = ((a + b) + a)C = (a + b)C + aC + (a + b)C \cdot aB + aC \cdot (a + b)B
\]
\[
= (aC + bC + aC \cdot bB + bC \cdot aB) + aC
\]
\[
+ (aC + bC + aC \cdot bB + bC \cdot aB) \cdot aB + aC \cdot aB + aC \cdot bB
\]
\[
= bC + aC \cdot bB + bC \cdot aB \cdot aB.
\]
Hence $aC \cdot bB \cdot aB = bC \cdot aB \cdot aB$. When $a \neq 0$, we can cancel $aB \neq 0$ and deduce (3.4). When $a = 0$, (3.4) holds thanks to $0B = 0 = 0C$.

Therefore, in either characteristic, we can fix an arbitrary $0 \neq b \in W_0$ and obtain from (3.4) the equality $aC = ((bB)^{-1} \cdot bC) \cdot aB$ for every $a \in W_0$. Hence $aC = c \cdot aB$ for some (unique) $c \in K$.

We proceed to show that
\[
A^{-1}M_aA = M_{aB}
\]
for every $a \in W_0$. By (3.2),
\[
(a, u)f \cdot (b, v) = (aB, aC + uJ_a^{-1}A_{aB})(bB, bC + vJ_b^{-1}A_{bB})
\]
\[
= (aB + bB, (aC + uJ_a^{-1}A_{aB})I_{bB} + (bC + vJ_b^{-1}A_{bB})J_{aB})
\]
is equal to
\[
((a, u)(b, v))f = (a+b, uI_b+vJ_a)f = ((a+b)B, (a+b)C + (uI_b+vJ_a)J_{a+b} A_{(a+b)B}).
\]
Thus
\[
(a+b)C + (uI_b+vJ_a)J_{a+b}^{-1}A_{(a+b)B} = (aC + uJ_a^{-1}A_{aB})I_{bB} + (bC + vJ_b^{-1}A_{bB})J_{aB}.
\]
Since $(a+b)C = aC I_{bB} + bC J_{aB}$ by (3.3), the last equality simplifies to
\[
(uI_b + vJ_a)J_{a+b}^{-1}A_{(a+b)B} = uJ_a^{-1}A_{aB}I_{bB} + vJ_b^{-1}A_{bB}J_{aB}.
\]
With $v = 0$ we obtain the equality of maps $K \to K$
\[
I_bJ_{a+b}^{-1}A_{(a+b)B} = J_a^{-1}A_{aB} I_{bB}.
\]
Similarly, with $u = 0$ we deduce another equality of maps $K \to K$, namely
\[
J_aJ_{a+b}^{-1}A_{(a+b)B} = J_b^{-1}A_{bB}J_{aB}.
\]
Using both (3.6) and (3.7), we see that
\[
I_b^{-1}J_a^{-1}A_{aB}I_{bB} = J_{a+b}^{-1}A_{(a+b)B} = J_a^{-1}J_b^{-1}A_{bB}J_{aB},
\]
and upon commuting certain maps and canceling we get $I_b^{-1}A_{bB} = J_b^{-1}A_{bB}$, and therefore also $J_aA_{bB} = I_aA_{bB}$. Upon expanding and canceling like terms,
we get $2M_b = 2AM_b$. If char($k$) ≠ 2, we deduce $M_bA = AM_b$ and (3.5).

Suppose that char($k$) = 2. Then (3.6) with $a = b$ yields $I_bA = I_b^{-1}AI_bB$, so $I_b^2A = AI_b^2$. Since $M_b^2 = M_{b^2}$ and $I_b^2 = I_{b^2}$, we get $I_{b^2}A = AI_{b^2}B$, $M_{b^2}A = AM(I_{b^2}B)^2$ and $A^{-1}M_{b^2}A = M_{(b^2)}^2$. Since $K$ is perfect (this is the only time we use this assumption), the last equality shows that every $A^{-1}M_bA$ is of the form $M_{e}$, so, in particular, $A^{-1}M_bA = M_e$ for some $e$. Then $M_b^2 = (A^{-1}M_bA)^2 = A^{-1}M_b^2A = M_{b^2}^2$, and evaluating this equality at 1 yields $e^2 = (bB)^2$ and $e = bB$.

We have again established (3.5).

Since $A : K \rightarrow K$ is an additive bijection, (3.5) holds and $\text{Im}(B) = W_1$, it follows that $A \in S(W_0, W_1)$ and $B = A : W_0 \rightarrow W_1$. We therefore have $(a, 0)f = (aA, c \cdot aA)$, and $\Phi$ is well-defined by $(A, c) = f\Phi$.

It remains to show that $\Psi$ and $\Phi$ are mutual inverses. If $f \in \text{Iso}(Q_0, Q_1)$ and $f\Phi = (A, c)$, then (3.5) yields $J^{-1}_aAJ_b = A$. This means that (3.2) can be rewritten as (3.1), and thus $f\Phi\Psi = f$. Conversely, suppose that $(A, c) \in S(W_0, W_1) \times K$ and let $f = (A, c)\Psi$ and $(D, d) = f\Phi = (A, c)\Psi\Phi$. Then $(0, u)f = (0, uA)$ by (3.1) and $(0, u)f = (0, uD)$ by definition of $\Phi$, so $a = D$. Finally, $(a, 0)f = (aA, c \cdot aA)$ by (3.1) and $(a, 0)f = (aA, d \cdot aD) = (aA, d \cdot aA)$ by definition of $\Psi$, so $c = d$. □

3.2. Isomorphisms and automorphisms in the tame case. For the rest of this section suppose that the triple $k$, $K$, $W_i$ is tame, that is, $k$ is a prime field, $(W_i)_k = K$, and $K$ is perfect if char($k$) = 2. In particular, $W_i \neq 0$. Let $\text{GL}_k(K)$ be the group of all $k$-linear transformations of $K$, and let Aut($K$) be the group of all field automorphisms of $K$.

Since $k$ is prime, any additive bijection $K \rightarrow K$ is $k$-linear, and so $S(W_0, W_1) = \{A \in \text{GL}_k(K) : A^{-1}M_{W_i}A = M_{W_i}\}$. We have shown that $A \in S(W_0, W_1)$ gives rise to an additive bijection $A : W_0 \rightarrow W_1$. This map extends uniquely into a field automorphism $A$ of $K$ such that $A^{-1}M_aA = M_a$ for every $a \in K$.

To see this, first note that $A \in \text{GL}_k(K)$ implies $A^{-1}M_{ab}A = A^{-1}M_bA = A^{-1}M_aAA^{-1}M_bA$, $A^{-1}M_{a+b}A = A^{-1}(M_a + M_b)A = A^{-1}M_aA + A^{-1}M_bA$ and $A^{-1}M_{\lambda}A = M_{\lambda}$ for every $a, b \in K$ and $\lambda \in k$. If $A$ is already defined on $a, b$, let $(a + b)\bar{A} = a\bar{A} + b\bar{A}$, $(ab)\bar{A} = a\bar{A} \cdot b\bar{A}$, and $(\lambda a)\bar{A} = \lambda \cdot a\bar{A}$, where $\lambda \in k$.

This procedure defines $A$ well. For instance, if $ab = c + d$, we have $a\bar{A} \cdot b\bar{A} = 1M_{a+b} = 1M_{a}M_{b} = 1A^{-1}M_{a}AA^{-1}M_{b}A = 1A^{-1}M_{ab}A = 1A^{-1}M_{c+d}A = 1(A^{-1}M_{c}A + A^{-1}M_{d}A) = 1(M_{c} + M_{d})A = c\bar{A} + d\bar{A}$, and so on.

Here is a solution to the isomorphism problem for a fixed extension $k < K$:

**Corollary 3.3.** For $i \in \{0, 1\}$, let $k$, $K$, $W_i$ be a tame triple and $Q_i = $
$Q_{k,K}(W)$. Then $Q_0$ is isomorphic to $Q_1$ if and only if there is $\varphi \in \text{Aut}(K)$ such that $W_0\varphi = W_1$.

**Proof.** Suppose that $f : Q_0 \to Q_1$ is an isomorphism. By Proposition 3.2, $f$ induces a map $\bar{A} \in S(W_0, W_1)$, which gives rise to $\bar{A} : W_0 \to W_1$, which extends into $\bar{A} \in \text{Aut}(K)$ such that $W_0\bar{A} = W_1$.

Conversely, suppose that $\varphi \in \text{Aut}(K)$ satisfies $W_0\varphi = W_1$. Then for every $a \in W_0$ and $b \in K$ we have $b\varphi^{-1} M_a \varphi = ((b\varphi^{-1}) \cdot a) \varphi = b\varphi^{-1} \varphi \cdot a \varphi = b \cdot a \varphi = b M_a \varphi$, so $\varphi \in S(W_0, W_1)$. The set $S(W_0, W_1) \times K$ is therefore nonempty, and we are done by Proposition 3.2.

We proceed to describe the automorphism groups of tame loops $Q_{k,K}(W)$. Let $S(W) = S(W, W) = \{A \in \text{GL}_k(K) : A^{-1} M_W A = M_W \}$.

**Lemma 3.4.** Suppose that $k$, $K$, $W$ is a tame triple. Then the mapping $S(W) \to \text{Aut}(K)$, $A \mapsto \bar{A}$ is a homomorphism with kernel $N(W) = M_K$ and image $I(W) = \{C \in \text{Aut}(K) : WC = W \}$. Moreover, $S(W) = I(W) N(W)$ is isomorphic to the semidirect product $I(W) \ltimes K^*$ with multiplication $(A, c)(B, d) = (A c B, d)$.

**Proof.** With $A, B \in S(W)$ and $a \in K$ we have $M_a A B = (AB)^{-1} M_a (AB) = B^{-1} A^{-1} M_a AB = B^{-1} M_a AB = M_a AB$, so $AB = \bar{A} \bar{B}$. The kernel of this homomorphism is equal to $N(W) = \{A \in S(W) : M_a A = AM_a \text{ for every } a \in K \}$. If $A \in N(W)$, we can apply the defining equality to 1 and deduce $a A = (1A)a$, so $A = M_1 A \in M_K$. Conversely, if $M_b \in M_K$, then obviously $M_b \in N(W)$.

For the image, note that $\bar{A}$ satisfies $W \bar{A} = W$. We have seen above that $\bar{A} \in \text{Aut}(K)$. Conversely, if $C \in \text{Aut}(K)$ satisfies $WC = W$ then $C \in S(W)$, and $C^{-1} M_a C = M_a C$ for every $a \in K$ because $C$ is multiplicative. Thus $C = \bar{C} \in I(W)$.

Since $I(W)$, $N(W)$ are subsets of $S(W)$, we have $S(W) N(W) \subseteq S(W)$. To show that $S(W) \subseteq I(W) N(W)$, let $A \in S(W)$ and consider $D = (A \bar{A})^{-1} A \in S(W)$. Then $D^{-1} M_a A = \bar{A}^{-1} \bar{A} M_a A = A^{-1} M_a A = M_a \bar{A}$ shows that $D \in N(W)$. Then $A = \bar{A} D$ is the desired decomposition.

Let $A, B \in S(W) = I(W) N(W) = I(W) M_K$, where $A = \bar{A} M_c$, $B = \bar{B} M_d$ for some $c, d \in K^*$. Then $AB = \bar{A} \bar{B} M_{c+d} = \bar{A} \bar{B} M_{c} M_{d} = \bar{A} \bar{B} M_{c} M_{d}$. □

**Theorem 3.5.** Let $Q = Q_{k,K}(W)$, where $k$ is a prime field, $K$ is a field extension, $W$ is a $k$-subspace of $K$ such that $k1 \cap W = 0$, and $\langle W \rangle_k = K$. If $\text{char}(k) = 2$, suppose also that $K$ is a perfect field. Then the group $\text{Aut}(Q)$ is isomorphic to the semidirect product $S(W) \ltimes K$ with multiplication $(A, c)(B, d) = (AB, cB + d)$. 

Automorphic loops arising from module endomorphisms 297
PROOF. By Proposition 3.2, there is a one-to-one correspondence between the sets $\text{Aut}(Q)$ and $S(W) \times K$. Suppose that $f \Phi = (A, c)$, $g \Phi = (B, d)$, so that $(a, u)f = (a\bar{A}, c \cdot a\bar{A} + uA)$ and $(a, u)g = (a\bar{B}, d \cdot a\bar{B} + uB)$ for every $(a, u) \in W \times K$. Then

$$(a, u)fg = (a\bar{A}, c \cdot a\bar{A} + uA)(a\bar{B}, d \cdot a\bar{B} + (c \cdot a\bar{A} + uA)B).$$

We want to prove that $(fg)\Phi = (AB, cB + d)$, which is equivalent to proving

$$(a, u)fg = (a\bar{A}B, (cB + d) \cdot a\bar{A}B + uAB).$$

Keeping $\bar{A}\bar{B} = \bar{AB}$ of Lemma 3.4 in mind, it remains to show that $(c \cdot a\bar{A})B = cB \cdot a\bar{A}B$, but this follows from $B^{-1}M_{a\bar{A}}B = M_{a\bar{A}B}$. □

A finer structure of $\text{Aut}(Q_{k<K}(W))$ is obtained by combining Theorem 3.5 with Lemma 3.4.

4. Automorphic loops of order $p^3$

The following facts are known about automorphic loops of odd order and prime power order.

Automorphic loops of odd order are solvable [9, Theorem 6.6]. Every automorphic loop of prime order $p$ is a group [9, Corollary 4.12]. More generally, every automorphic loop of order $p^2$ is a group, by [3] or [9, Theorem 6.1]. For every prime $p$ there are examples of automorphic loops of order $p^3$ that are not centrally nilpotent [9], and hence certainly not groups.

There is a commutative automorphic loop of order $2^3$ that is not centrally nilpotent [5]. By [6, Theorem 1.1], every commutative automorphic loop of odd order $p^k$ is centrally nilpotent. For any prime $p$ there are precisely 7 commutative automorphic loops of order $p^3$ up to isomorphism [4, Theorem 6.4].

We will use a special case of Corollary 3.3 to construct a class of pairwise non-isomorphic automorphic loops of odd order $p^3$, for $p$ odd.

Suppose that $p$ is odd. The field $\mathbb{F}_{p^2}$ can be represented as $\{x + y\sqrt{d} : x, y \in \mathbb{F}_p\}$, where $d \in \mathbb{F}_p$ is not a square. Let $\mathbb{F}_p = k < K = \mathbb{F}_{p^2}$, and let

$$W_0 = k\sqrt{d} \text{ and } W_a = k(1 + a\sqrt{d}) \text{ for } 0 \neq a \in \mathbb{F}_p.$$  

We see that every $W_a$ is a 1-dimensional $k$-subspace of $K$ such that $k1 \cap W_a = 0$. Conversely, if $W$ is a 1-dimensional $k$-subspace of $K$ such that $k1 \cap W = 0$, there is $a + b\sqrt{d}$ in $W$ with $a, b \in k$, $b \neq 0$. If $a = 0$ then $W = W_0$. Otherwise
$a^{-1}(a + b \sqrt{d}) = 1 + a^{-1}b \sqrt{d} \in W,$ and $W = W_{a^{-1}}b$. Hence there is a one-to-one correspondence between the elements of $k$ and 1-dimensional $k$-subspaces $W$ of $K$ satisfying $k1 \cap W = 0$, given by $a \mapsto W_a$.

**Theorem 4.1.** Let $p$ be a prime and $\mathbb{F}_p = k < K = \mathbb{F}_{p^2}$.

(i) Suppose that $p$ is odd. If $a, b \in k$, then the automorphic loops $Q_{k<K}(W_a), Q_{k<K}(W_b)$ of order $p^3$ are isomorphic if and only if $a = \pm b$. In particular, there are $(p+1)/2$ pairwise non-isomorphic automorphic loops of order $p^3$ of the form $Q_{k<K}(W)$, where we can take $W \in \{W_a : 0 \leq a \leq (p-1)/2\}$.

(ii) Suppose that $p = 2$. Then there is a unique automorphic loop of order $p^3$ of the form $Q_{k<K}(W)$ up to isomorphism.

**Proof.** (i) By Theorem 2.2, the loops $Q_a = Q_{k<K}(W_a)$ and $Q_b = Q_{k<K}(W_b)$ are automorphic loops of order $p^3$. By Corollary 3.3, the loops $Q_a, Q_b$ are isomorphic if and only if there is an automorphism $\varphi$ of $K$ such that $W_a \varphi = W_b$. Let $\sigma$ be the unique nontrivial automorphism of $K$, given by $(a + b \sqrt{d})\sigma = a - b \sqrt{d}$. Then $W_a \sigma = W_{-a}$ for every $a \in k$. Therefore $Q_a$ is isomorphic to $Q_b$ if and only if $a = \pm b$. The rest follows.

Part (ii) is similar, and follows from Corollary 3.3 by a direct inspection of subspaces and automorphisms of $\mathbb{F}_4$. □

We will now show how to obtain the loops of Construction 1.2 as a special case of Construction 1.4.

**Lemma 4.2.** Let $k$ be a field and $A \in M_2(k) \setminus kI$. Then $kI + kA$ is an anisotropic plane if and only if $kI + kA$ is a field with respect to the operations induced from $M_2(k)$.

**Proof.** Certainly $kI + kA$ is an abelian group. It is well known and easy to verify directly that every $A \in M_2(k)$ satisfies the characteristic equation

$$A^2 = \text{tr}(A)A - \det(A)I.$$  

This implies that $kI + kA$ is closed under multiplication, and it is therefore a subring of $M_2(k)$.

If $kI + kA$ is a field then every nonzero element $B \in kI + kA$ has an inverse in $kI + kA$, so $B$ is an invertible matrix and $kI + kA$ is an anisotropic plane. Conversely, suppose that $kI + kA$ is an anisotropic plane, so that every nonzero element $B \in kI + kA$ is an invertible matrix. The characteristic equation for $B$ then implies that $B^{-1} = (\det(B)^{-1})(\text{tr}(B)I - B)$, certainly an element of $kI + kA$, so $kI + kA$ is a field. □
Proposition 4.3. Let $k$ be a field. Let

$$S = \{Q_{k<K}(W) : k < K \text{ is a quadratic field extension}, \quad \dim_k(W) = 1, \quad k1 \cap W = 0\},$$

$$T = \{Q_k(A) : A \in M_2(k), \quad kI + kA \text{ is an anisotropic plane}\}.$$ 

Then, up to isomorphism, the loops of $S$ are precisely the loops of $T$.

Proof. Let $Q_{k<K}(W) \in S$. Then there is $\theta \in K$ such that $W = k\theta$, $K = k(\theta)$, and $\theta^2 = e + f\theta$ for some $e, f \in k$. The multiplication in $K$ is determined by $(a + b\theta)(c + d\theta) = (ac + bd\theta^2) + (ad + bc)\theta$ and $\theta^2 = e + f\theta$. With respect to the basis $\{1, \theta\}$ of $K$ over $k$, the multiplication by $\theta$ is given by the matrix $A = M_\theta = \begin{pmatrix} 0 & 1 \\ e & f \end{pmatrix}$.

The multiplication on $kI + kA$ is then determined by $(aI + bA)(cI + dA) = (acI + bdA^2) + (ad + bc)A$ and $A^2 = -\det(A)I + \text{tr}(A)A = eI + fA$, so $kI + kA$ is a field isomorphic to $K$. By Lemma 4.2, $kI + kA$ is an anisotropic plane, and the loop $Q_k(A)$ is defined.

The multiplication in $Q_{k<K}(W)$ on $W \times V = k\theta \times (k1 + k\theta)$ is given by $(a\theta, u)(b\theta, v) = (a\theta + b\theta, u(1 + b\theta) + v(1 - a\theta))$, while the multiplication in $Q_k(A) = Q_k(M_\theta)$ on $k \times (k \times k)$ is given by $(a, u)(b, v) = (a + b, u(1 + b\theta) + v(1 - a\theta))$. This shows that $Q_{k,K}(W)$ is isomorphic to $Q_k(A)$, and $S \subseteq T$.

Conversely, if $Q_k(A) \in T$ then the anisotropic plane $K = kI + kA$ is a field by Lemma 4.2, clearly a quadratic extension of $k$. Moreover, $W = kA$ is a 1-dimensional $k$-subspace of $K$ such that $k1 \cap W = 0$, so $Q_{k<K}(W) \in S$. We can again show that $Q_{k<K}(W)$ is isomorphic to $Q_k(A)$.

The conjecture 6.5 of [6] stated that there is precisely one isomorphism type of loops $Q_{F_2}(A)$, two isomorphism types of loops $Q_{F_3}(A)$, and three isomorphism types of loops $Q_{F_p}(A)$ for $p \geq 5$. The conjecture was verified computationally in [6] for $p \leq 5$, using the GAP package LOOPS [11]. Since $F_p$ is the unique quadratic extension of $F_p$, Theorem 4.1 and Proposition 4.3 now imply that the conjecture is actually false for every $p > 5$. (But note that $(p + 1)/2$ gives the calculated answer for $p = 3$ and $p = 5$, and the case $p = 2$ is also in agreement.)

The full classification of automorphic loops of order $p^3$ remains open.

5. Infinite examples

We conclude the paper by constructing an infinite 2-generated abelian-by-cyclic automorphic loop of exponent $p$ for every prime $p$. 

Lemma 5.1. Let $p$ be an odd prime, $k = \mathbb{F}_p$, $K = \mathbb{F}_p((t))$ the field of formal Laurent series over $\mathbb{F}_p$, $W = \mathbb{F}_p[t]$, and $Q = Q_{k\prec K}(W)$ the automorphic loop from Construction 1.4 defined by $(1.1)$ on $W \times K = \mathbb{F}_p t \times \mathbb{F}_p((t))$. Let $L = \langle (t, 0), (0, 1) \rangle$ be the subloop of $Q$ generated by $(t, 0)$ and $(0, 1)$. Then $L = W \times U$, where $U$ is the localization of $\mathbb{F}_p[t]$ with respect to $\{1+a : a \in W\}$. Moreover, $L$ is an infinite nonassociative 2-generated abelian-by-cyclic automorphic loop of exponent $p$.

Proof. First we observe that $W \times U$ is a subloop of $Q$. Indeed, $W \times U$ is clearly closed under multiplication. Since $(1 \pm a)^{-1} \in U$ for every $a \in W$ by definition, the formulas $(2.1)$, $(2.2)$ show that $W \times U$ is closed under left and right divisions, respectively. To prove that $L = W \times U$, it therefore suffices to show that $W \times U \subseteq L$.

We claim that $0 \times \mathbb{F}_p[t] \subseteq L$, or, equivalently, that $(0, t^m) \in L$ for every $m \geq 0$.

First note that for any integer $m$ we have
\[
(0, t^m)(0, t) \cdot (0, 0)^{-1}(0, t^m) = (t, t^m(1 + t))(-t, t^m(1 + t)) = (0, 2(t^m - t^{m+2})). \tag{5.1}
\]
We have $(0, t^0) = (0, 1) \in L$ by definition. The identity $(5.1)$ with $m = 0$ then yields $(0, 2(1 - t^2)) \in L$, so $(0, t^2) \in L$. Since also
\[
(-t, 0) \cdot (0, 1)(t, 0) = (-t, 0)(t, 1 + t) = (0, 1 + 2t + t^2)
\]
belongs to $L$, we conclude that $(0, t) \in L$. The identity $(5.1)$ can then be used inductively to show that $(0, t^m) \in L$ for every $m \geq 0$.

We now establish $0 \times U \subseteq L$ by proving that $(0, (1 + a)^n) \in L$ for every $n \in \mathbb{Z}$ and every $a \in W = \mathbb{F}_p$. We have already seen this for $n \geq 0$. The identity
\[
((a, 0) \backslash (0, (1 - a)^m))/(-a, 0) = (-a, (1 - a)^m)/(-a, 0) = (0, (1 - a)^m-2)
\]
then proves the claim by descending induction on $m$, starting with $m = 1$.

Given $(a, 0) \in W \times 0 \subseteq L$ and $(0, u) \in 0 \times U \subseteq L$, we note that $(0, u(a(1 - a)^{-1})) \in L$, and thus
\[
(a, 0)(0, u) \cdot (0, u(a(1 - a)^{-1})) = (a, u(1 - a))(0, u(a(1 - a)^{-1})) = (a, u)
\]
is also in $L$, concluding the proof that $W \times U \subseteq L$.

The loop $L$ is certainly infinite and 2-generated, and it is automorphic by Theorem 2.2. The homomorphism $W \times U \rightarrow \mathbb{F}_p$, $(it, u) \mapsto i$ has the abelian group $(U, +)$ as its kernel and the cyclic group $(\mathbb{F}_p, +)$ as its image, so $L$ is abelian-by-cyclic. An easy induction yields $(a, u)^m = (ma, mu)$ for every $(a, u) \in Q$ and $m \geq 0$, proving that $L$ has exponent $p$. Finally, $(t, 0)(0, t) \cdot (0, 1)^{-1} = (2t, 1 - 2t) \neq (2t, 1 - 2t + t^2) = (t, 0) \cdot (t, 0)(0, 1)$ shows that $L$ is nonassociative. \qed
Lemma 5.2. Let $k = \mathbb{F}_2$, $K = \mathbb{F}_2((t))$ the field of formal Laurent series over $\mathbb{F}_2$, $W = \mathbb{F}_2[t]$, and $Q = Q_{k<K}(W)$ the automorphic loop from Construction 1.4 defined by (1.1) on $W \times K = \mathbb{F}_2t \times \mathbb{F}_2((t))$. Let $L = \langle (t, 0), (0, 1) \rangle$ be the subloop of $Q$ generated by $(t, 0)$ and $(0, 1)$. Then $L = \{(it, f(1 + t)^i) : f \in U, i \in \{0, 1\}\}$, where $U$ is the localization of $\mathbb{F}_2[t^2]$ with respect to $\{1 + t^2\}$. Moreover, $L$ is an infinite nonassociative 2-generated abelian-by-cyclic commutative automorphic loop of exponent 2.

Proof. In our situation the multiplication formula (1.1) becomes

$$(a, u)(b, v) = (a + b, u(1 + b) + v(1 + a)),$$

so $Q$ is commutative and of exponent 2. Note that (2.1) becomes

$$(a, u) \setminus (b, v) = (a + b, (v + u(1 + a + b))(1 + a)^{-1}).$$

Let us first show that $S = \{(it, f(1 + t)^i) : f \in U, i \in \{0, 1\}\} = (0 \times U) \cup (t, 0)(0 \times U)$ is a subloop of $Q$. Indeed, $0 \times U \subseteq S$ is a subloop, and with $f, g \in U$, we have

$$(t, f(1 + t)) \setminus (t, g(1 + t)) = (0, f(1 + t)^2 + g(1 + t)^2) = (0, (f + g)(1 + t^2)),
\quad (0, f) \setminus (t, g(1 + t)) = (t, g(1 + t) + f(1 + t)) = (t, (g + f)(1 + t)),
\quad (t, f(1 + t)) \setminus (0, g) = (t, g + f(1 + t)^2)(1 + t)^{-1}
\quad = (t, (g(1 + t)^2)^{-1} + f)(1 + t),
\quad (t, f(1 + t)) \setminus (t, g(1 + t)) = (0, g(1 + t) + f(1 + t))(1 + t)^{-1} = (0, g + f),$$

always obtaining an element of $S$.

To prove that $S = L$, it suffices to show that $(0, t^{2m}), (0, t^{2m}(1 + t^2)^{-1}) \in L$ for every $m \geq 0$, since this implies $0 \times U \subseteq L$ and thus $S = (0 \times U) \cup (t, 0)(0 \times U) \subseteq L$. We have $(0, 1) \in L$ by definition, $(t, 1 + t) = (t, 0)(0, 1) \in L$, $(t, (1 + t)^{-1}(1 + t)) = (t, 0) \setminus (0, 1) \in L$, and $(0, 1 + (1 + t^2)^{-1}) = (t, 1 + t) \setminus (t, (1 + t^2)^{-1}(1 + t)) \in L$, so also $(0, (1 + t^2)^{-1}) \in L$. The inductive step follows upon observing the identity

$$(t, 0) \cdot (0, u)(t, 0) = (t, 0)(t, u(1 + t)) = (0, u(1 + t^2)).$$

The loop $L$ is certainly infinite, 2-generated, commutative, automorphic and of exponent 2. It is abelian-by-cyclic because the map $L \to \mathbb{F}_2$, $(it, f(1 + t)^i) \mapsto i$ is a homomorphism with the abelian group $(U, +)$ as its kernel and the cyclic group $(\mathbb{F}_2, +)$ as its image. Finally, $(t, 0)(t, 0) \cdot (0, 1) = (0, 1) \neq (0, 1 + t^2) = (t, 0) \cdot (t, 0)(0, 1)$ shows that $L$ is nonassociative.

Acknowledgments. We thank the three anonymous referees for useful comments, particularly for pointing out a counting mistake in an earlier version of Theorem 4.1(ii).
References


ALEXANDER GRISHKOV
INSTITUTE OF MATHEMATICS
AND STATISTICS
UNIVERSITY OF SÃO PAULO
05508-090 SÃO PAULO, SP
BRAZIL
E-mail: grishkov@ime.usp.br

PETR VOJTĚCHOVSKÝ
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF DENVER
2280 S VINE ST, DENVER
COLORADO 80208
USA
E-mail: petr@math.du.edu

MARINA RASSKAZOVA
OMSK SERVICE INSTITUTE
644099 OMSK
RUSSIA
E-mail: marinarasskazova1@gmail.com

(Received February 6, 2015; revised September 4, 2015)