Nuclear semidirect product of commutative automorphic loops

Jan Hora, Přemysl Jedlička

Department of Mathematics
Faculty of Engineering (former Technical Faculty)
Czech University of Life Sciences (former Czech University of Agriculture), Prague

3rd Milehigh
August 13, 2013
Denver, CO

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Semidirect product of groups

Fact (Semidirect product as a configuration)

Let G be a group and let $H < G$ and $K \lhd G$ such that $KH = G$ and $K \cap H = 1$. Then G is a semidirect product of K and H, denoted by $G = K \rtimes H$.

Fact (Semidirect product as a construction)

Let K, H be two groups and $\varphi : H \to \mathrm{Aut}(K)$ a homomorphism. Then the set $K \times H$ equipped with the binary operation

$$(a, i) * (b, j) = (a \cdot \varphi_i(b), i \cdot j)$$

is a group, denoted by $K \rtimes_\varphi H$.

Fact (The correspondence)

$K \times 1$ is a normal subgroup and $1 \times H$ is a subgroup of $K \rtimes_\varphi H$. On the other hand, starting with G, we can define φ_i as $k \mapsto k^i$.

Semidirect product of groups

Fact (Semidirect product as a configuration)

Let G be a group and let $H < G$ and $K \lhd G$ such that $KH = G$ and $K \cap H = 1$. Then G is a semidirect product of K and H, denoted by $G = K \rtimes H$.

Fact (Semidirect product as a construction)

Let K, H be two groups and $\varphi : H \to \mathrm{Aut}(K)$ a homomorphism. Then the set $K \times H$ equipped with the binary operation

$$(a, i) * (b, j) = (a \cdot \varphi_i(b), i \cdot j)$$

is a group, denoted by $K \rtimes_\varphi H$.

Fact (The correspondence)

$K \times 1$ is a normal subgroup and $1 \times H$ is a subgroup of $K \rtimes_\varphi H$. On the other hand, starting with G, we can define φ_i as $k \mapsto k^i$.

Semidirect product of groups

Fact (Semidirect product as a configuration)

Let G be a group and let $H < G$ and $K \triangleleft G$ such that $KH = G$ and $K \cap H = 1$. Then G is a semidirect product of K and H, denoted by $G = K \rtimes H$.

Fact (Semidirect product as a construction)

Let K, H be two groups and $\varphi : H \to \mathrm{Aut}(K)$ a homomorphism. Then the set $K \times H$ equipped with the binary operation

$$(a, i) * (b, j) = (a \cdot \varphi_i(b), i \cdot j)$$

is a group, denoted by $K \rtimes_\varphi H$.

Fact (The correspondence)

$K \times 1$ is a normal subgroup and $1 \times H$ is a subgroup of $K \rtimes_\varphi H$. On the other hand, starting with G, we can define φ_i as $k \mapsto k^i$.

Commutative automorphic loops

Definition

A loop Q is called *automorphic* if $\mathrm{Inn}(Q) \subseteq \mathrm{Aut}(Q)$.

Fact

Let Q be a commutative loop. Then $\mathrm{Inn}(Q) = \langle L_{x,y};\ x,y \in Q\rangle$, where $L_{x,y} = L_{xy}^{-1}L_xL_y$.

Corollary

A commutative loop Q is automorphic if and only if, for all $x,y,u,v \in Q$,

$$((uv \cdot x) \cdot y)/(xy) = ((ux \cdot y)/(xy)) \cdot ((vx \cdot y)/(xy)).$$

Commutative automorphic loops

Definition

A loop Q is called *automorphic* if $\mathrm{Inn}(Q) \subseteq \mathrm{Aut}(Q)$.

Fact

Let Q be a commutative loop. Then $\mathrm{Inn}(Q) = \langle L_{x,y};\ x, y \in Q\rangle$, *where* $L_{x,y} = L_{xy}^{-1} L_x L_y$.

Corollary

A commutative loop Q is automorphic if and only if, for all $x, y, u, v \in Q$,

$$((uv \cdot x) \cdot y)/(xy) = ((ux \cdot y)/(xy)) \cdot ((vx \cdot y)/(xy)).$$

Commutative automorphic loops

Definition

A loop Q is called *automorphic* if $\mathrm{Inn}(Q) \subseteq \mathrm{Aut}(Q)$.

Fact

Let Q be a commutative loop. Then $\mathrm{Inn}(Q) = \langle L_{x,y};\ x, y \in Q \rangle$, *where* $L_{x,y} = L_{xy}^{-1} L_x L_y$.

Corollary

A commutative loop Q is automorphic if and only if, for all $x, y, u, v \in Q$,

$$((uv \cdot x) \cdot y)/(xy) = ((ux \cdot y)/(xy)) \cdot ((vx \cdot y)/(xy)).$$

Nuclear semidirect product

Let $(Q, +)$ be a commutative automorphic loop. We consider subloops H and K of Q such that

- $K + H = Q$ and $K \cap H = \{0\}$;
- $K \lhd H$;
- K and H are abelian groups;
- $K \leqslant N_\mu(Q)$.

Example

Let Q be the non-associative commutative Moufang loop with 81 elements. Q is of exponent 3 and there exists a normal subgroup of order 27 and hence $Q \cong \mathbb{Z}_3^3 \rtimes \mathbb{Z}_3$. However $N(Q) \cong \mathbb{Z}_3$.

Lemma

If $a, b \in K$ and $i, j \in H$ as above then

$$(a+i)+(b+j) = L_{i,j}(a+b)+(i+j).$$

Nuclear semidirect product

Let $(Q,+)$ be a commutative automorphic loop. We consider subloops H and K of Q such that

- $K+H=Q$ and $K \cap H = \{0\}$;
- $K \lhd H$;
- K and H are abelian groups;
- $K \leqslant N_\mu(Q)$.

Example

Let Q be the non-associative commutative Moufang loop with 81 elements. Q is of exponent 3 and there exists a normal subgroup of order 27 and hence $Q \cong \mathbb{Z}_3^3 \rtimes \mathbb{Z}_3$. However $N(Q) \cong \mathbb{Z}_3$.

Lemma

If $a,b \in K$ and $i,j \in H$ as above then

$$(a+i)+(b+j) = L_{i,j}(a+b)+(i+j).$$

Nuclear semidirect product

Let $(Q, +)$ be a commutative automorphic loop. We consider subloops H and K of Q such that

- $K + H = Q$ and $K \cap H = \{0\}$;
- $K \lhd H$;
- K and H are abelian groups;
- $K \leqslant N_\mu(Q)$.

Example

Let Q be the non-associative commutative Moufang loop with 81 elements. Q is of exponent 3 and there exists a normal subgroup of order 27 and hence $Q \cong \mathbb{Z}_3^3 \rtimes \mathbb{Z}_3$. However $N(Q) \cong \mathbb{Z}_3$.

Lemma

If $a, b \in K$ and $i, j \in H$ as above then

$$(a + i) + (b + j) = L_{i,j}(a + b) + (i + j).$$

Nuclear semidirect product

Let $(Q,+)$ be a commutative automorphic loop. We consider subloops H and K of Q such that

- $K+H=Q$ and $K\cap H=\{0\}$;
- $K \lhd H$;
- K and H are abelian groups;
- $K \leqslant N_{\mu}(Q)$.

Example

Let Q be the non-associative commutative Moufang loop with 81 elements. Q is of exponent 3 and there exists a normal subgroup of order 27 and hence $Q \cong \mathbb{Z}_3^3 \rtimes \mathbb{Z}_3$. However $N(Q) \cong \mathbb{Z}_3$.

Lemma

If $a,b \in K$ and $i,j \in H$ as above then

$$(a+i)+(b+j)=L_{i,j}(a+b)+(i+j).$$

Nuclear semidirect product

Let $(Q,+)$ be a commutative automorphic loop. We consider subloops H and K of Q such that

- $K+H=Q$ and $K\cap H=\{0\}$;
- $K \lhd H$;
- K and H are abelian groups;
- $K \leqslant N_\mu(Q)$.

Example

Let Q be the non-associative commutative Moufang loop with 81 elements. Q is of exponent 3 and there exists a normal subgroup of order 27 and hence $Q \cong \mathbb{Z}_3^3 \rtimes \mathbb{Z}_3$. However $N(Q) \cong \mathbb{Z}_3$.

Lemma

If $a,b\in K$ and $i,j\in H$ as above then

$$(a+i)+(b+j)=L_{i,j}(a+b)+(i+j).$$

External semidirect product

Proposition

Let H and K be two abelian groups and let φ be a mapping $\varphi : H^2 \to \mathrm{Aut}(K)$. We define an operation $*$ on $Q = K \times H$ as follows:

$$(a, i) * (b, j) = (\varphi_{i,j}(a + b), i + j).$$

Then Q is a commutative automorphic loop if and only if

1. $\varphi_{i,j} = \varphi_{j,i}$;
2. $\varphi_{i,0} = \mathrm{id}_K$;
3. $\varphi_{i,j} \circ \varphi_{k,n} = \varphi_{k,n} \circ \varphi_{i,j}$;
4. $\varphi_{i,j,k} = \varphi_{j,k,i} = \varphi_{k,i,j}$;
5. $\varphi_{i,j+k} + \varphi_{j,i+k} + \varphi_{k,i+j} = \mathrm{id}_K + 2\varphi_{i,j,k}$;

for all $i, j, k, n \in H$, where $\varphi_{i,j,k} = \varphi_{i,j+k} \circ \varphi_{j,k}$.

$[Q : K] = 2$

Example

Let $H \cong \mathbb{Z}_2$. Then

$$\varphi_{0,0} = \varphi_{1,0} = \varphi_{0,1} = \mathrm{id}_K .$$

The only other non-trivial condition is

$$\begin{aligned} \varphi_{1,0} + \varphi_{1,0} + \varphi_{1,0} &= \mathrm{id}_K + 2\varphi_{1,1,1} \\ 3\,\mathrm{id}_K &= \mathrm{id}_K + 2\,\mathrm{id}_K \circ \varphi_{1,1} \\ 2\,\mathrm{id}_K &= 2\varphi_{1,1} \end{aligned}$$

In other words, $\varphi_{1,1}(2x) = 2x$.

$[Q : K] = 2$

Example

Let $H \cong \mathbb{Z}_2$. Then

$$\varphi_{0,0} = \varphi_{1,0} = \varphi_{0,1} = \mathrm{id}_K\,.$$

The only other non-trivial condition is

$$\begin{aligned} \varphi_{1,0} + \varphi_{1,0} + \varphi_{1,0} &= \mathrm{id}_K + 2\varphi_{1,1,1} \\ 3\,\mathrm{id}_K &= \mathrm{id}_K + 2\,\mathrm{id}_K \circ \varphi_{1,1} \\ 2\,\mathrm{id}_K &= 2\varphi_{1,1} \end{aligned}$$

In other words, $\varphi_{1,1}(2x) = 2x$.

Loops of odd order

Proposition

Let M be a faithful module over a ring R, $2 \in R^*$, and let $r \in R^*$ be of a multiplicative order $k \in \mathbb{N} \cup \{\infty\}$. Suppose that $(r^i + 1) \in R^*$, for each $i \in \mathbb{Z}$. Then the set $M \times \mathbb{Z}_k$, equipped with the operation

$$(a, i) * (b, j) = \left(\frac{(r^i + 1)(r^j + 1)}{2 \cdot (r^{i+j} + 1)} \cdot (a + b), i + j \right)$$

is a commutative automorphic loop.

Example

— M a vector space over a field of characteristics different from 2,
— $R = \mathrm{End}(M)$; we see M as an R-module
— r an automorphism of M,
— k odd.

Loops of odd order

Proposition

Let M be a faithful module over a ring R, $2 \in R^*$, and let $r \in R^*$ be of a multiplicative order $k \in \mathbb{N} \cup \{\infty\}$. Suppose that $(r^i + 1) \in R^*$, for each $i \in \mathbb{Z}$. Then the set $M \times \mathbb{Z}_k$, equipped with the operation

$$(a, i) * (b, j) = \left(\frac{(r^i + 1)(r^j + 1)}{2 \cdot (r^{i+j} + 1)} \cdot (a + b), i + j \right)$$

is a commutative automorphic loop.

Example

— M a vector space over a field of characteristics different from 2,
— $R = \mathrm{End}(M)$; we see M as an R-module
— r an automorphism of M,
— k odd.

Small normal subgroup

Lemma

If $|K| \leqslant 3$ then $K \rtimes_\varphi H$ is a group.

Example

$K = \mathbb{Z}_4$, $H = \mathbb{Z}_2$, $\varphi_{1,1} = 3$

Lemma

Let $K \cong \mathbb{Z}_4$. Then $\varphi_{i+j,k} = \varphi_{i,k} \circ \varphi_{j,k}$.

Small normal subgroup

Lemma

If $|K| \leqslant 3$ then $K \rtimes_{\varphi} H$ is a group.

Example

$K = \mathbb{Z}_4$, $H = \mathbb{Z}_2$, $\varphi_{1,1} = 3$

Lemma

Let $K \cong \mathbb{Z}_4$. Then $\varphi_{i+j,k} = \varphi_{i,k} \circ \varphi_{j,k}$.

Small normal subgroup

Lemma

If $|K| \leqslant 3$ *then* $K \rtimes_{\varphi} H$ *is a group.*

Example

$K = \mathbb{Z}_4$, $H = \mathbb{Z}_2$, $\varphi_{1,1} = 3$

Lemma

Let $K \cong \mathbb{Z}_4$. *Then* $\varphi_{i+j,k} = \varphi_{i,k} \circ \varphi_{j,k}$.

Bilinear forms

Proposition

Let $K = \mathbb{Z}_{n^2}$, for some $n \in \mathbb{N}$. Let H be an abelian group and let $\alpha : H^2 \to \mathbb{Z}_n$ be a symmetric bilinear form. We define

$$\varphi_{i,j} : x \mapsto (\alpha(i,j) \cdot n + 1) \cdot x.$$

Then $K \rtimes_\varphi H$ is a commutative automorphic loop.

Proposition

Let $K = \mathbb{Z}_{p^2}$, for some prime p. Let H be an elementary abelian p-group. Let α_1, α_2 be two symmetric bilinear forms $H^2 \to \mathbb{Z}_p$. Let Q_1 and Q_2 be two loops obtained from α_1 and α_2. Then $Q_1 \cong Q_2$ if and only if α_1 and α_2 are equivalent.

Bilinear forms

Proposition

Let $K = \mathbb{Z}_{n^2}$, for some $n \in \mathbb{N}$. Let H be an abelian group and let $\alpha : H^2 \to \mathbb{Z}_n$ be a symmetric bilinear form. We define

$$\varphi_{i,j} : x \mapsto (\alpha(i,j) \cdot n + 1) \cdot x.$$

Then $K \rtimes_\varphi H$ is a commutative automorphic loop.

Proposition

Let $K = \mathbb{Z}_{p^2}$, for some prime p. Let H be an elementary abelian p-group. Let α_1, α_2 be two symmetric bilinear forms $H^2 \to \mathbb{Z}_p$. Let Q_1 and Q_2 be two loops obtained from α_1 and α_2. Then $Q_1 \cong Q_2$ if and only if α_1 and α_2 are equivalent.

Classification of bilinear forms

Fact

Let V be a vector space over a finite field F of characteristics p. If $p > 2$ then there exist 2 non-degenerate symmetric bilinear forms, up to equivalence, namely

$$\begin{pmatrix} 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \quad \textit{and} \quad \begin{pmatrix} 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \\ 0 & \cdots & 0 & a \end{pmatrix}$$

where a is not a quadratic residue.

If $p = 2$ and $\dim V$ is odd then there exists only one non-degenerate symmetric bilinear form, up to equivalence.

If $p = 2$ and $\dim V$ is even then there exist two such forms, one of them alternating.

Classification of bilinear forms

Fact

Let V be a vector space over a finite field F of characteristics p. If $p > 2$ then there exist 2 non-degenerate symmetric bilinear forms, up to equivalence, namely

$$\begin{pmatrix} 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \\ 0 & \cdots & 0 & a \end{pmatrix}$$

where a is not a quadratic residue.
If $p = 2$ and $\dim V$ is odd then there exists only one non-degenerate symmetric bilinear form, up to equivalence.
If $p = 2$ and $\dim V$ is even then there exist two such forms, one of them alternating.

Bilinear mapping φ

Observation

Let $\varphi : H^2 \to \mathrm{Aut}(K)$ be bilinear. Then the φ satisfies the conditions of the semidirect product if and only if

1. *φ is symmetric,*
2. *granted,*
3. *$\mathrm{Im}\,\varphi$ is commutative,*
4. *granted,*
5. *???*

Lemma

Let R be a unitary ring and let $n \in \mathbb{N}_0$. Then the following properties are equivalent:

- *there exists G, a commutative subgroup of R^*, such that, for all $a, b, c \in G$, we have $na = n$ and $ab + ac + bc = 1 + 2abc$;*
- *there exist elements $x_1, x_2, \ldots$ in R such that $nx_i = 0$ and $x_i x_j = 0$, for all i, j.*

Bilinear mapping φ

Observation

Let $\varphi : H^2 \to \mathrm{Aut}(K)$ be bilinear. Then the φ satisfies the conditions of the semidirect product if and only if

1. *φ is symmetric,*
2. *granted,*
3. *$\mathrm{Im}\,\varphi$ is commutative,*
4. *granted,*
5. *???*

Lemma

Let R be a unitary ring and let $n \in \mathbb{N}_0$. Then the following properties are equivalent:

- *there exists G, a commutative subgroup of R^*, such that, for all $a, b, c \in G$, we have $na = n$ and $ab + ac + bc = 1 + 2abc$;*
- *there exist elements $x_1, x_2, \ldots$ in R such that $nx_i = 0$ and $x_i x_j = 0$, for all i, j.*

Bilinear mapping φ

Observation

Let $\varphi : H^2 \to \mathrm{Aut}(K)$ be bilinear. Then the φ satisfies the conditions of the semidirect product if and only if

1. *φ is symmetric,*
2. *granted,*
3. *$\mathrm{Im}\,\varphi$ is commutative,*
4. *granted,*
5. *???*

Lemma

Let R be a unitary ring and let $n \in \mathbb{N}_0$. Then the following properties are equivalent:

- *there exists G, a commutative subgroup of R^*, such that, for all $a, b, c \in G$, we have $na = n$ and $ab + ac + bc = 1 + 2abc$;*
- *there exist elements $x_1, x_2, \ldots$ in R such that $nx_i = 0$ and $x_i x_j = 0$, for all i, j.*

Construction with a bilinear mapping

Theorem

Let K be an abelian group and let $n \in \mathbb{N}_0$. Let X be a subset of $\mathrm{End}(K)$ satisfying $nX = X^2 = 0$. Denote $G = \langle X + \mathrm{id}_K \rangle_{\mathrm{Aut}(K)}$. Let φ be a symmetric bilinear $\mathbb{Z}_n$-module mapping $H^2 \to G$. Then $K \rtimes_\varphi H$ is a commutative automorphic loop.

Example

$K = \mathbb{Z}_{n^2}, X = \{n\}, G = \{kn + 1; k \in \mathbb{Z}\}$.

Example

— K, H: vector spaces over a field F of characteristic n,
— $M_{i,j}$ is a square matrix with 1 on position i, j and 0 elsewhere,
— X is a set $\{M_{i,j}$; no index is repeated twice$\}$.

Construction with a bilinear mapping

Theorem

Let K be an abelian group and let $n \in \mathbb{N}_0$. Let X be a subset of $\mathrm{End}(K)$ satisfying $nX = X^2 = 0$. Denote $G = \langle X + \mathrm{id}_K \rangle_{\mathrm{Aut}(K)}$. Let φ be a symmetric bilinear $\mathbb{Z}_n$-module mapping $H^2 \to G$. Then $K \rtimes_\varphi H$ is a commutative automorphic loop.

Example

$K = \mathbb{Z}_{n^2}, X = \{n\}, G = \{kn + 1; k \in \mathbb{Z}\}$.

Example

— K, H: vector spaces over a field F of characteristic n,
— $M_{i,j}$ is a square matrix with 1 on position i, j and 0 elsewhere,
— X is a set $\{M_{i,j};$ no index is repeated twice$\}$.

Loops of order p^3

Proposition

There exist at least 6 non-isomorphic commutative automorphic loops of order p^3, for p prime, namely

- $\mathbb{Z}_p^3$, $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$,
- $K = \mathbb{Z}_{p^2}$, $H = \mathbb{Z}_p$, $X = \{p\}$, φ *equivalent to the scalar product,*
- $K = \mathbb{Z}_{p^2}$, $H = \mathbb{Z}_p$, $X = \{p\}$, φ *not equivalent to the scalar product (for p odd),*
- $K = \mathbb{Z}_p^2$, $H = \mathbb{Z}_p$, $X = \left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\}$, φ *non-degenerate,*
- $K = \mathbb{Z}_2^2$, $H = \mathbb{Z}_2$, $\varphi_{1,1}$ *of order 3.*

Theorem (de Barros, Grishkov, Vojtěchovský)

There exist exactly 7 non-isomorphic commutative automorphic loops of order p^3, for p prime.

Loops of order p^3

Proposition

There exist at least 6 non-isomorphic commutative automorphic loops of order p^3, for p prime, namely

- $\mathbb{Z}_p^3$, $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$,
- $K = \mathbb{Z}_{p^2}$, $H = \mathbb{Z}_p$, $X = \{p\}$, φ *equivalent to the scalar product,*
- $K = \mathbb{Z}_{p^2}$, $H = \mathbb{Z}_p$, $X = \{p\}$, φ *not equivalent to the scalar product (for p odd),*
- $K = \mathbb{Z}_p^2$, $H = \mathbb{Z}_p$, $X = \left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\}$, φ *non-degenerate,*
- $K = \mathbb{Z}_2^2$, $H = \mathbb{Z}_2$, $\varphi_{1,1}$ *of order 3.*

Theorem (de Barros, Grishkov, Vojtěchovský)

There exist exactly 7 non-isomorphic commutative automorphic loops of order p^3, for p prime.

Loops of order p^3

Proposition

There exist at least 6 non-isomorphic commutative automorphic loops of order p^3, for p prime, namely

- $\mathbb{Z}_p^3$, $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$,
- $K = \mathbb{Z}_{p^2}$, $H = \mathbb{Z}_p$, $X = \{p\}$, φ *equivalent to the scalar product,*
- $K = \mathbb{Z}_{p^2}$, $H = \mathbb{Z}_p$, $X = \{p\}$, φ *not equivalent to the scalar product (for p odd),*
- $K = \mathbb{Z}_p^2$, $H = \mathbb{Z}_p$, $X = \left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\}$, φ *non-degenerate,*
- $K = \mathbb{Z}_2^2$, $H = \mathbb{Z}_2$, $\varphi_{1,1}$ *of order 3.*

Theorem (de Barros, Grishkov, Vojtěchovský)

There exist exactly 7 non-isomorphic commutative automorphic loops of order p^3, for p prime.

Loops of order p^3

Proposition

There exist at least 6 non-isomorphic commutative automorphic loops of order p^3, for p prime, namely

- $\mathbb{Z}_p^3$, $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$,
- $K = \mathbb{Z}_{p^2}$, $H = \mathbb{Z}_p$, $X = \{p\}$, φ *equivalent to the scalar product,*
- $K = \mathbb{Z}_{p^2}$, $H = \mathbb{Z}_p$, $X = \{p\}$, φ *not equivalent to the scalar product (for p odd),*
- $K = \mathbb{Z}_p^2$, $H = \mathbb{Z}_p$, $X = \left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\}$, φ *non-degenerate,*
- $K = \mathbb{Z}_2^2$, $H = \mathbb{Z}_2$, $\varphi_{1,1}$ of order 3.

Theorem (de Barros, Grishkov, Vojtěchovský)

There exist exactly 7 non-isomorphic commutative automorphic loops of order p^3, for p prime.

Loops of order p^3

Proposition

There exist at least 6 non-isomorphic commutative automorphic loops of order p^3, for p prime, namely

- $\mathbb{Z}_p^3$, $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$,
- $K = \mathbb{Z}_{p^2}$, $H = \mathbb{Z}_p$, $X = \{p\}$, φ *equivalent to the scalar product,*
- $K = \mathbb{Z}_{p^2}$, $H = \mathbb{Z}_p$, $X = \{p\}$, φ *not equivalent to the scalar product (for p odd),*
- $K = \mathbb{Z}_p^2$, $H = \mathbb{Z}_p$, $X = \left\{ \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \right\}$, φ *non-degenerate,*
- $K = \mathbb{Z}_2^2$, $H = \mathbb{Z}_2$, $\varphi_{1,1}$ *of order* 3.

Theorem (de Barros, Grishkov, Vojtěchovský)

There exist exactly 7 non-isomorphic commutative automorphic loops of order p^3, for p prime.

Loops of order p^3

Proposition

There exist at least 6 non-isomorphic commutative automorphic loops of order p^3, for p prime, namely

- $\mathbb{Z}_p^3$, $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$,
- $K = \mathbb{Z}_{p^2}$, $H = \mathbb{Z}_p$, $X = \{p\}$, φ *equivalent to the scalar product,*
- $K = \mathbb{Z}_{p^2}$, $H = \mathbb{Z}_p$, $X = \{p\}$, φ *not equivalent to the scalar product (for p odd),*
- $K = \mathbb{Z}_p^2$, $H = \mathbb{Z}_p$, $X = \left\{ \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \right\}$, φ *non-degenerate,*
- $K = \mathbb{Z}_2^2$, $H = \mathbb{Z}_2$, $\varphi_{1,1}$ *of order* 3.

Theorem (de Barros, Grishkov, Vojtěchovský)

There exist exactly 7 non-isomorphic commutative automorphic loops of order p^3, for p prime.

Bibliography

D. A. S. de Barros, A. Grishkov, P. Vojtěchovský:
Commutative automorphic loops of order p^3
to appear in Journal of Algebra and its Applications

J. Hora, P. Jedlička:
Nuclear semidirect product of commutative automorphic loops
to appear in Journal of Algebra and its Applications

P. Jedlička, M. K. Kinyon, P. Vojtěchovský:
Structure of commutative automorphic loops
Transactions of AMS 363,1 (2011), 365–384