Nilpotency in automorphic *p*-loops

Přemysl Jedlička[1], Michael K. Kinyon[2], Petr Vojtěchovský[2]

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

[2]Department of Mathematics
University of Denver

AAA 82, Potsdam
2?th June 2011

Quasigroups

Definition

Let $(G, \cdot)$ be a groupoid. The mapping $L_x : a \mapsto xa$ is called the *left translation* and the mapping $R_x : a \mapsto ax$ the right translation.

Definition (Combinatorial)

A groupoid $(Q, \cdot)$ is called a *quasigroup* if the mappings L_x and R_x are bijections, for each $x \in Q$.

Definition (Universal algebraic)

The algebra $(Q, \cdot, /, \backslash)$ is called a *quasigroup* if it satisfies the following identities:

$$x\backslash(x \cdot y) = y \qquad (x \cdot y)/y = x$$
$$x \cdot (x\backslash y) = y \qquad (x/y) \cdot y = x$$

Quasigroups

Definition

Let $(G, \cdot)$ be a groupoid. The mapping $L_x : a \mapsto xa$ is called the *left translation* and the mapping $R_x : a \mapsto ax$ the right translation.

Definition (Combinatorial)

A groupoid $(Q, \cdot)$ is called a *quasigroup* if the mappings L_x and R_x are bijections, for each $x \in Q$.

Definition (Universal algebraic)

The algebra $(Q, \cdot, /, \backslash)$ is called a *quasigroup* if it satisfies the following identities:

$$x\backslash(x \cdot y) = y \qquad (x \cdot y)/y = x$$
$$x \cdot (x\backslash y) = y \qquad (x/y) \cdot y = x$$

Loops

Definition

A quasigroup Q is called a *loop* if it contains the identity element.

Example (A minimal nonassociative loop)

	1	2	3	4	5
1	1	2	3	4	5
2	2	1	5	3	4
3	3	4	1	5	2
4	4	5	2	1	3
5	5	3	4	2	1

Multiplication Groups

Definitions

Let Q be a loop.

- The group generated by L_x and R_x, for all $x \in Q$, is called *the multiplication group* of Q and it is denoted by $\mathrm{Mlt}(Q)$.
- The subgroup of $\mathrm{Mlt}(Q)$ stabilizing the neutral element of Q is called *the inner mapping group* of Q and it is denoted by $\mathrm{Inn}(Q)$.

Fact

An inner mapping of a loop needs not to be an automorphism.

Definition

A loop Q is called an *automorphic loop* (or an *A-loop*) if $\mathrm{Inn}(Q) \leqslant \mathrm{Aut}(Q)$.

Multiplication Groups

Definitions

Let Q be a loop.

- The group generated by L_x and R_x, for all $x \in Q$, is called *the multiplication group* of Q and it is denoted by $\mathrm{Mlt}(Q)$.
- The subgroup of $\mathrm{Mlt}(Q)$ stabilizing the neutral element of Q is called *the inner mapping group* of Q and it is denoted by $\mathrm{Inn}(Q)$.

Fact

An inner mapping of a loop needs not to be an automorphism.

Definition

A loop Q is called an *automorphic loop* (or an *A-loop*) if $\mathrm{Inn}(Q) \leqslant \mathrm{Aut}(Q)$.

Multiplication Groups

Definitions

Let Q be a loop.

- The group generated by L_x and R_x, for all $x \in Q$, is called *the multiplication group* of Q and it is denoted by $\mathrm{Mlt}(Q)$.
- The subgroup of $\mathrm{Mlt}(Q)$ stabilizing the neutral element of Q is called *the inner mapping group* of Q and it is denoted by $\mathrm{Inn}(Q)$.

Fact

An inner mapping of a loop needs not to be an automorphism.

Definition

A loop Q is called an *automorphic loop* (or an *A-loop*) if $\mathrm{Inn}(Q) \leqslant \mathrm{Aut}(Q)$.

Multiplication Groups

Definitions

Let Q be a loop.

- The group generated by L_x and R_x, for all $x \in Q$, is called *the multiplication group* of Q and it is denoted by $\mathrm{Mlt}(Q)$.
- The subgroup of $\mathrm{Mlt}(Q)$ stabilizing the neutral element of Q is called *the inner mapping group* of Q and it is denoted by $\mathrm{Inn}(Q)$.

Fact

An inner mapping of a loop needs not to be an automorphism.

Definition

A loop Q is called an *automorphic loop* (or an *A-loop*) if $\mathrm{Inn}(Q) \leqslant \mathrm{Aut}(Q)$.

Multiplication Groups

Definitions

Let Q be a loop.

- The group generated by L_x and R_x, for all $x \in Q$, is called *the multiplication group* of Q and it is denoted by $\mathrm{Mlt}(Q)$.
- The subgroup of $\mathrm{Mlt}(Q)$ stabilizing the neutral element of Q is called *the inner mapping group* of Q and it is denoted by $\mathrm{Inn}(Q)$.

Fact

An inner mapping of a loop needs not to be an automorphism.

Definition

A loop Q is called an *automorphic loop* (or an *A-loop*) if $\mathrm{Inn}(Q) \leqslant \mathrm{Aut}(Q)$.

Basic properties of A-loops

Fact

Any characteristic subloop of an A-loop is normal.

Theorem (R. H. Bruck, J. L. Paige)

Every monogenerated subloop of an A-loop is a group.

Notation

We write x^3 instead of $x \cdot (x \cdot x)$ or $(x \cdot x) \cdot x$.
We write x^{-1} instead of $1/x$ or $x\backslash 1$.

Basic properties of A-loops

Fact

Any characteristic subloop of an A-loop is normal.

Theorem (R. H. Bruck, J. L. Paige)

Every monogenerated subloop of an A-loop is a group.

Notation

We write x^3 instead of $x \cdot (x \cdot x)$ or $(x \cdot x) \cdot x$.
We write x^{-1} instead of $1/x$ or $x\backslash 1$.

Basic properties of A-loops

Fact

Any characteristic subloop of an A-loop is normal.

Theorem (R. H. Bruck, J. L. Paige)

Every monogenerated subloop of an A-loop is a group.

Notation

We write x^3 instead of $x \cdot (x \cdot x)$ or $(x \cdot x) \cdot x$.
We write x^{-1} instead of $1/x$ or $x\backslash 1$.

p-loops

Definition

Let Q be a loop where each element generates a cyclic subgroup and let p be a prime. The loop is called a *p-loop* if, for each $x \in Q$, there exists k, such that $x^{p^k} = 1$.

Theorem (P. J., M. K., P. V.)

Let Q be a finite commutative automorphic loop and let p be a prime. Then Q is a p-loop if and only if $|Q| = p^k$ for some k.

p-loops

Definition

Let Q be a loop where each element generates a cyclic subgroup and let p be a prime. The loop is called a *p-loop* if, for each $x \in Q$, there exists k, such that $x^{p^k} = 1$.

Theorem (P. J., M. K., P. V.)

Let Q be a finite commutative automorphic loop and let p be a prime. Then Q is a p-loop if and only if $|Q| = p^k$ for some k.

Commutatives A-loops of odd orders

Proposition (P. J., M. K., P. V.)

Let $(Q, \cdot)$ be a commutative A-loop of an odd order. We associate to Q an operation $\circ$ defined as:

$$x \circ y = \sqrt{(x \cdot y^2)/x^{-1}}$$

Then Q is a Bruck loop. Moreover, the powers in $(Q, \cdot)$ coincide with the powers in $(Q, \circ)$

Corollary

- *Lagrange theorem,*
- *If $p \mid |Q|$, for p prime, then there exists $x \in Q$ of order p,*
- *Existence of Sylow p-subloops,*
- *Solvability.*

Commutatives A-loops of odd orders

Proposition (P. J., M. K., P. V.)

Let $(Q, \cdot)$ be a commutative A-loop of an odd order. We associate to Q an operation $\circ$ defined as:

$$x \circ y = \sqrt{(x \cdot y^2)/x^{-1}}$$

Then Q is a Bruck loop. Moreover, the powers in $(Q, \cdot)$ coincide with the powers in $(Q, \circ)$

Corollary

- *Lagrange theorem,*
- *If $p \mid |Q|$, for p prime, then there exists $x \in Q$ of order p,*
- *Existence of Sylow p-subloops,*
- *Solvability.*

Commutatives A-loops of odd orders

Proposition (P. J., M. K., P. V.)

Let $(Q, \cdot)$ be a commutative A-loop of an odd order. We associate to Q an operation $\circ$ defined as:

$$x \circ y = \sqrt{(x \cdot y^2)/x^{-1}}$$

Then Q is a Bruck loop. Moreover, the powers in $(Q, \cdot)$ coincide with the powers in $(Q, \circ)$

Corollary

- *Lagrange theorem,*
- *If $p \mid |Q|$, for p prime, then there exists $x \in Q$ of order p,*
- *Existence of Sylow p-subloops,*
- *Solvability.*

Commutatives A-loops of odd orders

Proposition (P. J., M. K., P. V.)

Let $(Q, \cdot)$ be a commutative A-loop of an odd order. We associate to Q an operation $\circ$ defined as:

$$x \circ y = \sqrt{(x \cdot y^2)/x^{-1}}$$

Then Q is a Bruck loop. Moreover, the powers in $(Q, \cdot)$ coincide with the powers in $(Q, \circ)$

Corollary

- *Lagrange theorem,*
- *If $p \mid |Q|$, for p prime, then there exists $x \in Q$ of order p,*
- *Existence of Sylow p-subloops,*
- *Solvability.*

Commutatives A-loops of odd orders

Proposition (P. J., M. K., P. V.)

Let $(Q, \cdot)$ be a commutative A-loop of an odd order. We associate to Q an operation $\circ$ defined as:

$$x \circ y = \sqrt{(x \cdot y^2)/x^{-1}}$$

Then Q is a Bruck loop. Moreover, the powers in $(Q, \cdot)$ coincide with the powers in $(Q, \circ)$

Corollary

- *Lagrange theorem,*
- *If $p \mid |Q|$, for p prime, then there exists $x \in Q$ of order p,*
- *Existence of Sylow p-subloops,*
- *Solvability.*

Commutatives A-loops of odd orders

Proposition (P. J., M. K., P. V.)

Let $(Q, \cdot)$ be a commutative A-loop of an odd order. We associate to Q an operation $\circ$ defined as:

$$x \circ y = \sqrt{(x \cdot y^2)/x^{-1}}$$

Then Q is a Bruck loop. Moreover, the powers in $(Q, \cdot)$ coincide with the powers in $(Q, \circ)$

Corollary

- *Lagrange theorem,*
- *If $p \mid |Q|$, for p prime, then there exists $x \in Q$ of order p,*
- *Existence of Sylow p-subloops,*
- *Solvability.*

Nilpotency of loops

Fact

Every p-group is nilpotent.

Definition

Let Q be a loop. The *center* of Q is the set

$$Z(Q) = \{a \in Q;\ \varphi(a) = a\ \forall \varphi \in \mathrm{Inn}(Q)\}$$

Definition

Let Q be a loop. The *upper central series* of Q is

$$Z_0(Q) \leqslant Z_1(Q) \leqslant Z_2(Q) \leqslant \cdots \leqslant Z_n(Q) \leqslant \cdots \leqslant Q,$$

where $Z_0(Q) = \{1\}$ and $Z_i(Q)$ is the preimage of $Z\big(Q/Z_{i-1}(Q)\big)$. If there exists some n such that $Z_n(Q) = Q$ then Q is said to be *(centrally) nilpotent of class n.*

Nilpotency of loops

Fact

Every p-group is nilpotent.

Definition

Let Q be a loop. The *center* of Q is the set

$$Z(Q) = \{a \in Q;\ \varphi(a) = a\ \forall \varphi \in \mathrm{Inn}(Q)\}$$

Definition

Let Q be a loop. The *upper central series* of Q is

$$Z_0(Q) \leqslant Z_1(Q) \leqslant Z_2(Q) \leqslant \cdots \leqslant Z_n(Q) \leqslant \cdots \leqslant Q,$$

where $Z_0(Q) = \{1\}$ and $Z_i(Q)$ is the preimage of $Z\big(Q/Z_{i-1}(Q)\big)$. If there exists some n such that $Z_n(Q) = Q$ then Q is said to be *(centrally) nilpotent of class n.*

Nilpotency of loops

Fact

Every p-group is nilpotent.

Definition

Let Q be a loop. The *center* of Q is the set

$$Z(Q) = \{a \in Q;\ \varphi(a) = a\ \forall \varphi \in \mathrm{Inn}(Q)\}$$

Definition

Let Q be a loop. The *upper central series* of Q is

$$Z_0(Q) \leqslant Z_1(Q) \leqslant Z_2(Q) \leqslant \cdots \leqslant Z_n(Q) \leqslant \cdots \leqslant Q,$$

where $Z_0(Q) = \{1\}$ and $Z_i(Q)$ is the preimage of $Z\big(Q/Z_{i-1}(Q)\big)$.
If there exists some n such that $Z_n(Q) = Q$ then Q is said to be *(centrally) nilpotent of class n.*

Nilpotency of loops

Fact

Every p-group is nilpotent.

Definition

Let Q be a loop. The *center* of Q is the set

$$Z(Q) = \{a \in Q;\ \varphi(a) = a\ \forall\varphi \in \mathrm{Inn}(Q)\}$$

Definition

Let Q be a loop. The *upper central series* of Q is

$$Z_0(Q) \leqslant Z_1(Q) \leqslant Z_2(Q) \leqslant \cdots \leqslant Z_n(Q) \leqslant \cdots \leqslant Q,$$

where $Z_0(Q) = \{1\}$ and $Z_i(Q)$ is the preimage of $Z\big(Q/Z_{i-1}(Q)\big)$. If there exists some n such that $Z_n(Q) = Q$ then Q is said to be *(centrally) nilpotent of class n*.

Nilpotency of commutative automorphic p-loops

Theorem (P. J., M. K., P. V.)

Let $Q(\cdot)$ be a commutative automorphic loop of an odd order with associated Bruck loop $Q(\circ)$. Then, for each non-negative integer n,

$$Z_n(Q, \circ) = Z_n(Q, \cdot)$$

Corollary

Commutative automorphic p-loops are nilpotent, for each odd prime p.

Nilpotency of commutative automorphic p-loops

Theorem (P. J., M. K., P. V.)

Let $Q(\cdot)$ be a commutative automorphic loop of an odd order with associated Bruck loop $Q(\circ)$. Then, for each non-negative integer n,

$$Z_n(Q, \circ) = Z_n(Q, \cdot)$$

Corollary

Commutative automorphic p-loops are nilpotent, for each odd prime p.

Drápal's Construction

Theorem (A. Drápal, refined by P. Jedlička & D. Simon)

Let K be the q-element finite field, $\operatorname{char}(K) \neq 2$. Let k be an odd divisor either of $q-1$ or of $q+1$. Take ξ, a k-th primitive root of unity. We define an operation $*$ on the set $Q = K \times \mathbb{Z}_k$ as follows:

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

Then $(Q,*)$ is a commutative automorphic loop, $|Q|$ is odd and $Z(Q) = 1$.

Commutative automorphic 2-loops with trivial center

Proposition (P. J., M. K., P. V.)

Let G be a vector space over $\mathbb{F}_2$ and let f be an automorphism of V. We construct an operation $*$ on $Q = V \times \mathbb{F}_2$ as follows:

$$(\vec{v}, i) * (\vec{w}, j) = (f^{i \cdot j}(\vec{v} + \vec{w}), i + j).$$

Then Q is a commutative automorphic loop of exponent 2. If f is identical then Q is a group, otherwise $Z(Q) = \{\vec{u} \in V;\ f(\vec{u}) = \vec{u}\} \times 0$.

Corollary

There exist commutative automorphic 2-loops with trivial center.

Commutative automorphic 2-loops with trivial center

Proposition (P. J., M. K., P. V.)

Let G be a vector space over $\mathbb{F}_2$ and let f be an automorphism of V. We construct an operation $*$ on $Q = V \times \mathbb{F}_2$ as follows:

$$(\vec{v}, i) * (\vec{w}, j) = (f^{i \cdot j}(\vec{v} + \vec{w}), i + j).$$

Then Q is a commutative automorphic loop of exponent 2. If f is identical then Q is a group, otherwise $Z(Q) = \{\vec{u} \in V; f(\vec{u}) = \vec{u}\} \times 0$.

Corollary

There exist commutative automorphic 2-loops with trivial center.

Anisotropic planes

Definition

Let K be a field and let $M(2, K)$ be the vector space of 2×2 matrices over K. A subspace W of $M(2, K)$ is called *anisotropic*, if $\det A \neq 0$, for every $A \in W$.

Lemma

Let $A \in M(2, K)$. The subspace $\langle A, I \rangle$ is an anisotropic plane if and only if A has no eigenvalues in K.

Anisotropic planes

Definition

Let K be a field and let $M(2,K)$ be the vector space of 2×2 matrices over K. A subspace W of $M(2,K)$ is called *anisotropic*, if $\det A \neq 0$, for every $A \in W$.

Lemma

Let $A \in M(2,K)$. The subspace $\langle A, I \rangle$ is an anisotropic plane if and only if A has no eigenvalues in K.

Automorphic p-loops with trivial center

Theorem (P. J., M. K., P. V.)

Let $A \in GL(2,p)$ has no eigenvalue in $\mathbb{Z}_p$. We define a binary operation $*$ on $\mathbb{Z}_p \times \mathbb{Z}_p^2$ as follows:

$$(a,\vec{v}) * (b,\vec{w}) = (a+b,\ \vec{v}\cdot(I+bA) + \vec{w}\cdot(I-aA)).$$

The algebra $(\mathbb{Z}_p \times \mathbb{Z}_p^2, *)$ is an automorphic loop with trivial center.

References

- R. H. Bruck, J. L. Paige:
  Loops whose inner mappings are automorphisms,
  The Annals of Math., 2nd Series, **63**, no. 2, (1956), 308–323
- A. Drápal: A class of comm. loops with metacyclic inner mapping groups, Comment. Math. Univ. Carolin. **49**,3 (2008) 357–382.
- P. Jedlička, M. K. Kinyon, P. Vojtěchovský:
  Constructions of commutative automorphic loops
  Comm. in Alg., **38**,9 (2010), 3243–3267
- P. Jedlička, M. K. Kinyon, P. Vojtěchovský: Structure of commutative automorphic loops, Trans. of AMS, **363** (2011), no. 1, 365–384
- P. Jedlička, M. K. Kinyon, P. Vojtěchovský: Nilpotency in automorphic loops of odd prime power order submitted to J. of Algebra
- P. Jedlička, D. Simon: Commutative A-loops of order *pq* (preprint)