# An application of the number theory in the non-associative algebra

Přemysl Jedlička[1], Denis Simon[2]

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

[2]Laboratoire de Mathématiques Nicolas Oresme
Université de Caen

SSAOS 2009

# 0-bijections

## Definition

Let $R$ be a ring. A partial mapping $f : R \to R$ is called a $0$-*bijection* if twe following conditions hold;

- $f^i(0)$ is defined for every $i \in \mathbb{N}$;
- for each $i \in \mathbb{N}$ there exists some $x \in R$ such that $f^i(x) = 0$: such an element is denoted by $f^{-i}(0)$;
- $f(0) \in R^*$.

If there exists $k \in \mathbb{N}$ such that $f^k(0) = 0$ then such $k$ is called the $0$-*order* of $f$.

# Drápal's Construction

## Theorem (Aleš Drápal)

*Let $M$ be a module over a commutative ring $R$. Suppose that there exists $t \in R$ such that*

$$f(x) = \frac{x+1}{tx+1}$$

*is a $0$-bijection of $0$-order $k$. We define an operation $*$ on the set $Q = M \times \mathbb{N}_k$ as follows:*

$$(a,i) * (b,j) = \left( \frac{a+b}{1 + tf^i(0)f^j(0)}, \, i+j \right).$$

*Then $(Q, *)$ is a commutative automorphic loop.*

## Example

Putting $t = -3$ we obtain $k = 3$ for any $R$ where $2$ is invertible.

# Drápal's Construction

**Theorem (Aleš Drápal)**

*Let $M$ be a module over a commutative ring $R$. Suppose that there exists t $\in R$ such that*

$$f(x) = \frac{x+1}{tx+1}$$

*is a $0$-bijection of $0$-order $k$. We define an operation $*$ on the set $Q = M \times \mathbb{N}_k$ as follows:*

$$(a,i) * (b,j) = \left( \frac{a+b}{1+tf^i(0)f^j(0)}\ ,\ i+j \right).$$

*Then $(Q,*)$ is a commutative automorphic loop.*

**Example**

Putting $t = -3$ we obtain $k = 3$ for any $R$ where $2$ is invertible.

# Translating fractional mappings

**Fact**

*A mapping*

$$f(x) = \frac{x+1}{tx+1}$$

*is a* $0$*-bijection of order* $k$ *if and only if*

- $\begin{pmatrix} 1 & 1 \\ t & 1 \end{pmatrix}^k \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ a \end{pmatrix}$, *for some* $a \in R$,
- $\begin{pmatrix} 1 & 1 \\ t & 1 \end{pmatrix}^\ell \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} b \\ 0 \end{pmatrix}$, *for no* $\ell \in \mathbb{N}$.

# Eigenvalues of the automorphism

## Definition

Denote

$$F = \begin{pmatrix} 1 & 1 \\ t & 1 \end{pmatrix},$$

Its characteristic polynomial is

$$P(x) = x^2 + 2x + 1 - t = (x - \lambda)(x - \mu)$$

## Fact

$\mathrm{disc}(P) = -t$ *hence* $\lambda = \mu$ *if and only if* $t = 0$.

# Eigenvalues of the automorphism

## Definition

Denote

$$F = \begin{pmatrix} 1 & 1 \\ t & 1 \end{pmatrix},$$

Its characteristic polynomial is

$$P(x) = x^2 + 2x + 1 - t = (x - \lambda)(x - \mu)$$

## Fact

$\mathrm{disc}(P) = -t$ *hence* $\lambda = \mu$ *if and only if* $t = 0$.

# Necessary condition for 0-order

## Lemma

- $\begin{pmatrix} 1 & 1 \\ t & 1 \end{pmatrix}^k \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ a \end{pmatrix}$ *if and only if* $\left(\frac{\lambda}{\mu}\right)^k = 1,$
- $\begin{pmatrix} 1 & 1 \\ t & 1 \end{pmatrix}^\ell \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} b \\ 0 \end{pmatrix}$ *if and only if* $\left(\frac{\lambda}{\mu}\right)^\ell = -1,$

## Corollary

*The order $k$ must be odd or infinite.*

# Necessary condition for 0-order

## Lemma

- $\begin{pmatrix} 1 & 1 \\ t & 1 \end{pmatrix}^k \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ a \end{pmatrix}$ *if and only if* $\left(\frac{\lambda}{\mu}\right)^k = 1$,
- $\begin{pmatrix} 1 & 1 \\ t & 1 \end{pmatrix}^\ell \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} b \\ 0 \end{pmatrix}$ *if and only if* $\left(\frac{\lambda}{\mu}\right)^\ell = -1$,

## Corollary

*The order $k$ must be odd or infinite.*

# Necessary and sufficient condition

**Proposition**

*The number $\xi = \frac{\lambda}{\mu}$ has to be a primitive $k$-th root of unity.*

- *if $\lambda, \mu$ lie in the basic field $\mathbb{F}_q$ then $k$ divides $q - 1$;*
- *if $\lambda, \mu$ do not lie in the basic field $\mathbb{F}_q$ then $N(\xi) = 1$ and therefore $k$ divides $q + 1$.*

**Definition**

Let $\nu$ lie in a quadratic extension of a field $K$. Then the *norm* of $\nu$ is computed as $N(\nu) = \nu \cdot \bar{\nu}$.

The element $\bar{\nu}$ is called the *conjugate* of $\nu$. The elements $\nu$ and $\bar{\nu}$ share the same minimal quadratic polynomial with coefficients in $K$, i.e. the polynomial $x^2 - (\nu + \bar{\nu})x + \nu\bar{\nu}$.

## Necessary and sufficient condition

### Proposition

*The number $\xi = \frac{\lambda}{\mu}$ has to be a primitive $k$-th root of unity.*

- *if $\lambda, \mu$ lie in the basic field $\mathbb{F}_q$ then $k$ divides $q - 1$;*
- *if $\lambda, \mu$ do not lie in the basic field $\mathbb{F}_q$ then $N(\xi) = 1$ and therefore $k$ divides $q + 1$.*

### Definition

Let $\nu$ lie in a quadratic extension of a field $K$. Then the *norm* of $\nu$ is computed as $N(\nu) = \nu \cdot \bar{\nu}$.

The element $\bar{\nu}$ is called the *conjugate* of $\nu$. The elements $\nu$ and $\bar{\nu}$ share the same minimal quadratic polynomial with coefficients in $K$, i.e. the polynomial $x^2 - (\nu + \bar{\nu})x + \nu\bar{\nu}$.

# Necessary and sufficient condition

## Proposition

*The number $\xi = \frac{\lambda}{\mu}$ has to be a primitive $k$-th root of unity.*

- *if $\lambda, \mu$ lie in the basic field $\mathbb{F}_q$ then $k$ divides $q - 1$;*
- *if $\lambda, \mu$ do not lie in the basic field $\mathbb{F}_q$ then $N(\xi) = 1$ and therefore $k$ divides $q + 1$.*

## Definition

Let $\nu$ lie in a quadratic extension of a field $K$. Then the *norm* of $\nu$ is computed as $N(\nu) = \nu \cdot \bar{\nu}$.

The element $\bar{\nu}$ is called the *conjugate* of $\nu$. The elements $\nu$ and $\bar{\nu}$ share the same minimal quadratic polynomial with coefficients in $K$, i.e. the polynomial $x^2 - (\nu + \bar{\nu})x + \nu\bar{\nu}$.

# Necessary and sufficient condition

## Proposition

*The number $\xi = \frac{\lambda}{\mu}$ has to be a primitive $k$-th root of unity.*

- *if $\lambda, \mu$ lie in the basic field $\mathbb{F}_q$ then $k$ divides $q - 1$;*
- *if $\lambda, \mu$ do not lie in the basic field $\mathbb{F}_q$ then $N(\xi) = 1$ and therefore $k$ divides $q + 1$.*

## Definition

Let $\nu$ lie in a quadratic extension of a field $K$. Then the *norm* of $\nu$ is computed as $N(\nu) = \nu \cdot \bar{\nu}$.

The element $\bar{\nu}$ is called the *conjugate* of $\nu$. The elements $\nu$ and $\bar{\nu}$ share the same minimal quadratic polynomial with coefficients in $K$, i.e. the polynomial $x^2 - (\nu + \bar{\nu})x + \nu\bar{\nu}$.

# Necessary and sufficient condition

## Proposition

*The number $\xi = \frac{\lambda}{\mu}$ has to be a primitive $k$-th root of unity.*

- *if $\lambda, \mu$ lie in the basic field $\mathbb{F}_q$ then $k$ divides $q - 1$;*
- *if $\lambda, \mu$ do not lie in the basic field $\mathbb{F}_q$ then $N(\xi) = 1$ and therefore $k$ divides $q + 1$.*

## Definition

Let $\nu$ lie in a quadratic extension of a field $K$. Then the *norm* of $\nu$ is computed as $N(\nu) = \nu \cdot \bar{\nu}$.

The element $\bar{\nu}$ is called the *conjugate* of $\nu$. The elements $\nu$ and $\bar{\nu}$ share the same minimal quadratic polynomial with coefficients in $K$, i.e. the polynomial $x^2 - (\nu + \bar{\nu})x + \nu\bar{\nu}$.

# Necessary and sufficient condition

## Proposition

*The number $\xi = \frac{\lambda}{\mu}$ has to be a primitive $k$-th root of unity.*

- *if $\lambda, \mu$ lie in the basic field $\mathbb{F}_q$ then $k$ divides $q - 1$;*
- *if $\lambda, \mu$ do not lie in the basic field $\mathbb{F}_q$ then $N(\xi) = 1$ and therefore $k$ divides $q + 1$.*

## Definition

Let $\nu$ lie in a quadratic extension of a field $K$. Then the *norm* of $\nu$ is computed as $N(\nu) = \nu \cdot \bar{\nu}$.
The element $\bar{\nu}$ is called the *conjugate* of $\nu$. The elements $\nu$ and $\bar{\nu}$ share the same minimal quadratic polynomial with coefficients in $K$, i.e. the polynomial $x^2 - (\nu + \bar{\nu})x + \nu\bar{\nu}$.

# Drápal's Construction, New Point of View

## Theorem

*Let $K$ be the $q$-element finite field, $\mathrm{char}(K) \neq 2$. Let $k$ be an odd divisor either of $q-1$ or of $q+1$. Take $\xi$, 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.*

## Conjecture

If $k$ and $q$ are primes then the construction gives the only (up to isomorphism) non-associative commutative automorphic loop of order $kq$.

# Drápal's Construction, New Point of View

**Theorem**

*Let $K$ be the $q$-element finite field, $\mathrm{char}(K) \neq 2$. Let $k$ be an odd divisor either of $q-1$ or of $q+1$. Take $\xi$, 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.*

**Conjecture**

If $k$ and $q$ are primes then the construction gives the only (up to isomorphism) non-associative commutative automorphic loop of order $kq$.

# Bibliography

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 commutative 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
to appear in Comm. in Alg.

P. Jedlička, M. K. Kinyon, P. Vojtěchovský:
Structure of commutative automorphic loops
to appear in Trans. of AMS

P. Jedlička, D. Simon:
Commutative automorphic loops of order $pq$ (preprint)