Commutative centerless loops with metacyclic inner mapping groups

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

Loops '11, Třešť
25 July 2011

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Denis Simon

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 a unique $x \in R$ 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 faithful module over a commutative ring R. Let $s \in R$ and $t \in R^*$ be such that

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

is a 0-bijection of 0-order k. We define an operation $*$ on the set $Q = M \times \mathbb{Z}_k$ 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 loop with $\mathrm{Inn}(Q)$ metacyclic.
$N_\lambda = N_\rho = 0$, $N_\mu = M \times \{0\}$.
Q is automorphic if and only if $s = 1$.

Examples of 0-bijection

Example

$k = 2$ if and only if $s = -1$ and $t + 1 \in R^*$.

Example

Putting $s = 1$ and $t = -3$ we obtain $k = 3$ for any R where 2 is invertible.

Simplification

For the sake of simplicity, we shall assume the following:

- $s = 1$;
- $\mathrm{char}(R) \neq 2$;
- R is a field.

Examples of 0-bijection

Example

$k = 2$ if and only if $s = -1$ and $t + 1 \in R^*$.

Example

Putting $s = 1$ and $t = -3$ we obtain $k = 3$ for any R where 2 is invertible.

Simplification

For the sake of simplicity, we shall assume the following:

- $s = 1$;
- $\mathrm{char}(R) \neq 2$;
- R is a field.

Examples of 0-bijection

Example

$k = 2$ if and only if $s = -1$ and $t + 1 \in R^*$.

Example

Putting $s = 1$ and $t = -3$ we obtain $k = 3$ for any R where 2 is invertible.

Simplification

For the sake of simplicity, we shall assume the following:

- $s = 1$;
- $\mathrm{char}(R) \neq 2$;
- R is a field.

Examples of 0-bijection

Example

$k = 2$ if and only if $s = -1$ and $t + 1 \in R^*$.

Example

Putting $s = 1$ and $t = -3$ we obtain $k = 3$ for any R where 2 is invertible.

Simplification

For the sake of simplicity, we shall assume the following:

- $s = 1$;
- $\mathrm{char}(R) \neq 2$;
- R is a field.

Examples of 0-bijection

Example

$k = 2$ if and only if $s = -1$ and $t + 1 \in R^*$.

Example

Putting $s = 1$ and $t = -3$ we obtain $k = 3$ for any R where 2 is invertible.

Simplification

For the sake of simplicity, we shall assume the following:

- $s = 1$;
- $\mathrm{char}(R) \neq 2$;
- R is a field.

Examples of 0-bijection

Example

$k = 2$ if and only if $s = -1$ and $t + 1 \in R^*$.

Example

Putting $s = 1$ and $t = -3$ we obtain $k = 3$ for any R where 2 is invertible.

Simplification

For the sake of simplicity, we shall assume the following:

- $s = 1$;
- $\mathrm{char}(R) \neq 2$;
- R is a field.

Translating fractional mappings

Fact

A mapping

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

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

- *the number k is the minimal one satisfying* $\begin{pmatrix} 1 & 1 \\ t & 1 \end{pmatrix}^k \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ a \end{pmatrix}$, *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* $\ell \in \mathbb{N}$.

Translating fractional mappings

Fact

A mapping

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

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

- *the number k is the minimal one satisfying* $\begin{pmatrix} 1 & 1 \\ t & 1 \end{pmatrix}^k \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ a \end{pmatrix}$, *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* $\ell \in \mathbb{N}$.

Translating fractional mappings

Fact

A mapping

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

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

- *the number k is the minimal one satisfying*
  $$\begin{pmatrix} 1 & 1 \\ t & 1 \end{pmatrix}^k \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ a \end{pmatrix},$$ *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

- *The eigenvalues are non-zero;*
- $\mathrm{disc}(P) = 4t$ *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

- *The eigenvalues are non-zero;*
- $\mathrm{disc}(P) = 4t$ *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

- *The eigenvalues are non-zero;*
- $\operatorname{disc}(P) = 4t$ *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

- *The eigenvalues are non-zero;*
- $\mathrm{disc}(P) = 4t$ *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 element $\xi = \dfrac{\lambda}{\mu}$ has to be a primitive k-th root of unity and

- *if λ, μ lie in the basic field R then ξ lies in R too;*
- *if λ, μ do not lie in the basic field R then ξ lies in the quadratic extension $R[\lambda]$ and $N(\xi) = 1$.*

Definition

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

The element $\bar{\nu}$ is called the *conjugate* of ν. The elements ν 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 element $\xi = \dfrac{\lambda}{\mu}$ has to be a primitive k-th root of unity and

- *if λ, μ lie in the basic field R then ξ lies in R too;*
- *if λ, μ do not lie in the basic field R then ξ lies in the quadratic extension $R[\lambda]$ and $N(\xi) = 1$.*

Definition

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

The element $\bar{\nu}$ is called the *conjugate* of ν. The elements ν 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 element $\xi = \dfrac{\lambda}{\mu}$ has to be a primitive k-th root of unity and

- *if λ, μ lie in the basic field R then ξ lies in R too;*
- *if λ, μ do not lie in the basic field R then ξ lies in the quadratic extension $R[\lambda]$ and $N(\xi) = 1$.*

Definition

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

The element $\bar{\nu}$ is called the *conjugate* of ν. The elements ν 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 element $\xi = \dfrac{\lambda}{\mu}$ *has to be a primitive k-th root of unity and*

- *if* λ, μ *lie in the basic field* R *then* ξ *lies in* R *too;*
- *if* λ, μ *do not lie in the basic field* R *then* ξ *lies in the quadratic extension* $R[\lambda]$ *and* $N(\xi) = 1$.

Definition

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

The element $\bar{\nu}$ is called the *conjugate* of ν. The elements ν 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 element $\xi = \dfrac{\lambda}{\mu}$ *has to be a primitive k-th root of unity and*

- *if* λ, μ *lie in the basic field* R *then* ξ *lies in* R *too;*
- *if* λ, μ *do not lie in the basic field* R *then* ξ *lies in the quadratic extension* $R[\lambda]$ *and* $N(\xi) = 1$.

Definition

Let ν lie in a quadratic extension of a field K. Then the *norm* of ν is computed as $N(\nu) = \nu \cdot \bar{\nu}$.
The element $\bar{\nu}$ is called the *conjugate* of ν. The elements ν 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 element $\xi = \dfrac{\lambda}{\mu}$ *has to be a primitive k-th root of unity and*

- *if* λ, μ *lie in the basic field* R *then* ξ *lies in* R *too;*
- *if* λ, μ *do not lie in the basic field* R *then* ξ *lies in the quadratic extension* $R[\lambda]$ *and* $N(\xi) = 1$.

Definition

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

Examples of suitable primitive roots

Examples

- Let $R = \mathbb{F}_q$. Then
  1. $\sqrt[k]{1}$ lies in R iff k divides $q-1$;
  2. $\sqrt[k]{1}$ is quadratic and of norm 1 iff k divides $q+1$.
- Let $R = \mathbb{Q}$. Then only $\sqrt[3]{1}$ is quadratic.
- Let $R = \mathbb{R}$. Then all roots of 1 lie in $\mathbb{C}$ and are of norm 1.

Examples of suitable primitive roots

Examples

- Let $R = \mathbb{F}_q$. Then
  1. $\sqrt[k]{1}$ lies in R iff k divides $q-1$;
  2. $\sqrt[k]{1}$ is quadratic and of norm 1 iff k divides $q+1$.
- Let $R = \mathbb{Q}$. Then only $\sqrt[3]{1}$ is quadratic.
- Let $R = \mathbb{R}$. Then all roots of 1 lie in $\mathbb{C}$ and are of norm 1.

Examples of suitable primitive roots

Examples

- Let $R = \mathbb{F}_q$. Then
  1. $\sqrt[k]{1}$ lies in R iff k divides $q-1$;
  2. $\sqrt[k]{1}$ is quadratic and of norm 1 iff k divides $q+1$.
- Let $R = \mathbb{Q}$. Then only $\sqrt[3]{1}$ is quadratic.
- Let $R = \mathbb{R}$. Then all roots of 1 lie in $\mathbb{C}$ and are of norm 1.

Examples of suitable primitive roots

Examples

- Let $R = \mathbb{F}_q$. Then
  1. $\sqrt[k]{1}$ lies in R iff k divides $q-1$;
  2. $\sqrt[k]{1}$ is quadratic and of norm 1 iff k divides $q+1$.
- Let $R = \mathbb{Q}$. Then only $\sqrt[3]{1}$ is quadratic.
- Let $R = \mathbb{R}$. Then all roots of 1 lie in $\mathbb{C}$ and are of norm 1.

Examples of suitable primitive roots

Examples

- Let $R = \mathbb{F}_q$. Then
  1. $\sqrt[k]{1}$ lies in R iff k divides $q - 1$;
  2. $\sqrt[k]{1}$ is quadratic and of norm 1 iff k divides $q + 1$.
- Let $R = \mathbb{Q}$. Then only $\sqrt[3]{1}$ is quadratic.
- Let $R = \mathbb{R}$. Then all roots of 1 lie in $\mathbb{C}$ and are of norm 1.

Examples of suitable primitive roots

Examples

- Let $R = \mathbb{F}_q$. Then
  1. $\sqrt[k]{1}$ lies in R iff k divides $q - 1$;
  2. $\sqrt[k]{1}$ is quadratic and of norm 1 iff k divides $q + 1$.
- Let $R = \mathbb{Q}$. Then only $\sqrt[3]{1}$ is quadratic.
- Let $R = \mathbb{R}$. Then all roots of 1 lie in $\mathbb{C}$ and are of norm 1.

Drápal's Construction, New Point of View

Theorem (A. Drápal; P. J. & D. Simon)

Let R be a field, $\mathrm{char}(R) \neq 2$. Take ξ, a k-th primitive root of unity, k odd, such that $\xi \in R$ or ξ lies in a quadratic extension of R and $N(\xi) = 1$. We define an operation $*$ on the set $Q = R \times \mathbb{Z}_k$ 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.

Corollary

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

Drápal's Construction, New Point of View

Theorem (A. Drápal; P. J. & D. Simon)

Let R be a field, $\operatorname{char}(R) \neq 2$. Take ξ, a k-th primitive root of unity, k odd, such that $\xi \in R$ or ξ lies in a quadratic extension of R and $N(\xi) = 1$. We define an operation $*$ on the set $Q = R \times \mathbb{Z}_k$ 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.

Corollary

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

Construction of Bruck loops of order pq

Theorem (P. J. & D. Simon)

Let R be a field, $\mathrm{char}(R) \neq 2$. Take ξ, a k-th primitive root of unity, k odd, such that $\xi \in R$ or ξ lies in a quadratic extension of R and $N(\xi) = 1$. We define an operation $\circ$ on the set $Q = R \times \mathbb{Z}_k$ as follows:

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

Then $(Q, \circ)$ is a Bruck loop with $Z(Q) = 0$.

Different cases

How the considerations differ in other cases:

- if R is not a field then we have to construct a projective line over R;
- if R is not a field then we have to understand the primitive roots of unity;
- if R is not a field then we have to compute in quadratic extensions of R;
- if s is general then $\left(\xi^i \cdot (\xi - s) + \xi s - 1\right) \in R^*$ for all $i \in \mathbb{Z}$;

Different cases

How the considerations differ in other cases:

- if R is not a field then we have to construct a projective line over R;
- if R is not a field then we have to understand the primitive roots of unity;
- if R is not a field then we have to compute in quadratic extensions of R;
- if s is general then $\left(\xi^i \cdot (\xi - s) + \xi s - 1\right) \in R^*$ for all $i \in \mathbb{Z}$;

Different cases

How the considerations differ in other cases:

- if R is not a field then we have to construct a projective line over R;
- if R is not a field then we have to understand the primitive roots of unity;
- if R is not a field then we have to compute in quadratic extensions of R;
- if s is general then $\left(\xi^i \cdot (\xi - s) + \xi s - 1\right) \in R^*$ for all $i \in \mathbb{Z}$;

Different cases

How the considerations differ in other cases:

- if R is not a field then we have to construct a projective line over R;
- if R is not a field then we have to understand the primitive roots of unity;
- if R is not a field then we have to compute in quadratic extensions of R;
- if s is general then $\left(\xi^i \cdot (\xi - s) + \xi s - 1\right) \in R^*$ for all $i \in \mathbb{Z}$;

Enumeration of loops of order $k \cdot q$

Theorem (P.J.)

Let q be an odd prime and let $k > 1$. The number of centerless loops of order $k \cdot p$, with the middle nucleus equal to $\mathbb{Z}_q$, that arise from the construction, is, up to isomorphism,

• $q - 2$	*if* $k = 2$	
• $\dfrac{q-k+2}{2}$	*if* k *is an odd divisor of* $q+1$	*(one of them automorphic)*
• $\dfrac{q-k+1}{2}$	*if* k *is an even divisor of* $q+1$	
• $\dfrac{q-k}{2}$	*if* k *is an odd divisor of* $q-1$	*(one of them automorphic)*
• $\dfrac{q-k-1}{2}$	*if* k *is an even divisor of* $q-1$	
• 0	*otherwise*	

Bibliography

A. Drápal:
A class of commutative loops with metacyclic inner mapping groups
Comment. Math. Univ. Carolin. **49**,3 (2008) 357–382.

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

P. Jedlička
On commutative loops of order pq with metacyclic inner mapping group and trivial center
Comment. Math. Univ. Carolin. **51** (2010), no. 2, 253–261