ON COMMUTATIVE A-LOOPS OF ORDER *PQ*

PŘEMYSL JEDLIČKA AND DENIS SIMON

Abstract. We study a construction introduced by Aleš Drápal, giving raise to commutative A-loops of order kn where k and n are odd numbers. We show which combinations of k and n are possible if the construction is based on a field or on a cyclic group. We conclude that if p and q are odd primes, there exists a non-associative commutative A-loop of order pq if and only if p divides q^2-1 and such a loop is most probably unique.

1. Introduction

A *loop* is a quasigroup with a neutral element 1. An *inner mapping* of a loop is any composition of left and right translations (i.e. mappings $x \mapsto ax$ and $x \mapsto xa$) that fixes 1. If all inner mappings of a loop are automorphisms then the loop is called an *A-loop*. In spite of the fact that there are some results about A-loops in the 50's [2], a more thorough investigation started only in the recent years, see e.g. [8], [6], [7].

There are still not many examples of proper A-loops, for instance the only known commutative A-loops that are neither p-loops nor direct products were introduced by Aleš Drápal in [5]. Unfortunately, the article did not specify what orders can and what orders cannot be achieved via this construction.

We partially fill the gap. Whereas Drápal's construction is based upon an arbitrary commutative ring, we focus our attention to the rings $\mathbb{Z}/n\mathbb{Z}$ only. This is done in two steps, first we consider the p-element fields; it turns out that all the construction works exactly the same way for any fields and hence the proofs are pronounced in a general setting. In the second step we study general rings $\mathbb{Z}/n\mathbb{Z}$. In fact, we always consider n to be odd due to the following result: Kinyon, Vojtěchovský and the first author proved in [6] that every finite commutative A-loop is the direct product of its 2-component and of the rest (which is an odd order loop). Commutative A-loops which are 2-loops were intensively studied in [7]. Hence in this paper, we do not care of any ring where 2 is not invertible.

The main result, that we show here, is the description of all non-associative A-loop orders that can be obtained if Drápal's construction is based upon a field or upon $\mathbb{Z}/n\mathbb{Z}$. For instance, a non-associative loop based upon a field of size q can only have $k \cdot q$ elements, where k is an odd divisor either of $q-1$ or of $q+1$. Moreover, such a loop is unique (based on this construction). As a corollary we conclude that there exists a non-associative commutative A-loop of order pq, $p<q$ odd primes, if and only if p divides q^2-1 and we give an argument why we think that such a loop is the only commutative A-loop of order pq, up to isomorphism.

Date: May 31, 2009, *Version*: 0.8 β.

2000 *Mathematics Subject Classification.* Primary: 20N05 Quasigroups and loops; Secondary: 15A33 Matrices over special rings.

Key words and phrases. commutative A-loops, constructions of loops, matrices over finite fields, eigenvalues, quadratic extensions.

The first author is grateful for the hospitality provided by the Department of Mathematics of the University of Caen where he was a visitor while this work was completed. His research was supported by the Grant Agency of the Czech Republic, grant no. 201/07/P015.

An interesting feature of the paper is that although it establishes some facts in the loop theory, except of the last section we do not consider loops *en soi*, we work (nearly) entirely within the scope of fields or number rings. Hence the paper could well be read by someone not affected by loop theory.

The paper is organised as follows: in Section 2 we introduce the construction, especially so called 0-bijective fractional linear mappings which are the ground stone of the construction. In Section 3 we study these mappings in the context of projective spaces over fields which gives us necessary and sufficient conditions for the mappings to exist. In Section 4 we do the same work not upon fields but upon rings $\mathbb{Z}/n\mathbb{Z}$ which, of course, heavily depends on the results of Section 3. In Section 5 we prove that, in fields, A-loops of the same order obtained via different invertible coefficients have to be isomorphic and hence there exists a unique loop for each order. Finally, in Section 6 we deal with the case of commutative A-loops of order pq and their associated Bruck loops.

2. Drápal's construction

In this section we present a construction of loops introduced by Aleš Drápal in [5]. These loops were constructed so that their inner mapping groups are metacyclic. We give some of its properties here and we clarify the aims of this paper. As the majority of the paper does not need any loop theoretical arguments, we do not even define properly what a loop is. If the reader wants a detailed description anyway, we refer to [1]. Nevertheless, it should suffice to know that loops are "groups without associativity". We start with the definition of a mapping which is bijective on the orbit containing 0.

Definition. Let R be a commutative ring and let f be a partial mapping $R \to R$. We shall say that f is 0-*bijective* if

(1) $f^i(0)$ is defined for each $i \geq 1$;
(2) for each $i \geq 1$ there exists a unique $y \in R$ such that $f^i(y)$ is defined and equal to 0—we denote this element $f^{-i}(0)$; and
(3) $f(0) \in R^*$.

We say that a 0-bijective partial mapping f is of 0-*order* k, if k is the smallest positive integer such that $f^k(0) = 0$. We say that it is of 0-order ∞ if $f^k(0) \neq 0$ for all k.

In fact these 0-bijections are the structure we study through the entire article, but only those which can be given by a formula $f(x) = (sx+1)/(tx+1)$, for some elements s and t in R, with $s - t$ invertible. We shall denote these mappings $f_{s,t}$. They serve for the following construction:

Proposition 1 (Drápal [5])**.** *Let M be a module over a commutative ring R and let $f_{s,t} : R \to R$, for some $s, t \in R$ with $s - t \in R^*$, be a 0-bijective mapping of 0-order k. Then we can define a commutative loop Q on the set $M \times \mathbb{Z}/k\mathbb{Z}$ as follows:*

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

The loop is denoted $M[s, t]$. Its inner mapping group is the semidirect product $tM \rtimes G$, where $G = \langle 1 + tf^i(0)f^j(0) \rangle \leq R^*$.

Example. Let M be a module over a commutative ring R where 2 is invertible. Let $s = 1$ and $t = -3$. Then it is easy to see that $f^3_{1,-3}(0) = 0$ and hence $M[1, -3]$ is a loop defined on the set $M \times \mathbb{Z}/3\mathbb{Z}$.

We have not said yet that the construction gives something non-trivial, i.e. that we obtain non-associative loops. It is almost always the case:

Proposition 2 (Drápal [5]). *Let $Q = M[s,t]$ where M is a faithful module over a commutative ring R. If $t \neq 0$ then Q is not associative, otherwise Q is a group.*

As we already said in the introduction, our main aim is to describe A-loops that can be obtained via this construction. From this point of view, the most interesting is the case $s = 1$.

Theorem 3 (Drápal [5]). *Let $Q = M[s,t]$ where M is faithful module over a commutative ring R. If $s = 1$ then Q is an A-loop. On the other hand, if $t \in R^*$ and Q is an A-loop then $s = 1$.*

Hence we have many possible A-loops theoretically, the only problem is to know

- **Question 1**: Given a commutative ring R, which number k can appear as a 0-order of a 0-bijective mapping $f_{1,t}$?
- **Question 2**: Given a commutative ring R and a number k, how to find a t such that $f_{1,t}$ a 0-bijective mapping of the prescribed 0-order k?

Without answers to these questions we are confined just to try luck with random values of t and be surprised what loops do pop out from the construction.

Drápal's paper does not give an answer to any of both questions. It gives a hint how to construct some loops if we are not fixed neither on a specific k nor on a specific ring, but it is far from being sufficient. Therefore it is our task to do, to answer the questions above.

3. Orders of the mappings in fields

This section is the core of the paper. We are interested in describing the 0-orders of mappings $f_{s,t}$ when the base ring is $\mathbb{Z}/n\mathbb{Z}$. Naturally, the first case to consider is when $n = p$ is a prime number, that is $\mathbb{Z}/p\mathbb{Z}$ is the p-element field $\mathbb{F}_p$. It turns out though that there is not much difference between the behaviour of $f_{s,t}$ on p-element fields and general fields. Hence we can consider K to be any field and we can even present infinite examples. The only difference for infinite fields is the possibility to have infinite 0-orders. Such orders will be usually ignored since they cannot appear in finite fields.

We investigate here the questions stated in the previous section giving an answer for both of them, in the case of fields only, of course. We start the section in a more general setting considering s to be arbitrary because the proofs given do not depend on s much. However, at the end of the section, there is a result that we cannot prove but for $s = 1$.

In the entire section we shall work in a field K, with characteristic different from 2. As usual, things behave differently in characteristic 2 and as we have already explained in the introduction, this case is not very interesting.

It was observed already in [5] that a mapping $f_{s,t} = \frac{sx+1}{tx+1}$, with

$$s \neq t$$

can be viewed as an automorphism of the projective line $\mathbb{P}^1(K)$ over K given by the matrix

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

(we keep dropping the indices when they are evident from the context). Hence we can translate the notion of 0-order to automorphisms of projective lines. But we shall be a bit more careful since an automorphism is always a 0-bijection.

Definition. Let F be an automorphism of the projective line $\mathbb{P}^1(K)$. We say that F is of *projective* 0*-order* k if k is the smallest positive integer such that $F^k\binom{0}{1} = \binom{0}{x}$, for some $x \in K^*$.
We say that F *meets infinity* at ℓ, if $F^\ell\binom{0}{1} = \binom{x}{0}$, for some $x \in K^*$. We say simply

that F meets infinity if there is some ℓ at which it happens.
We say that F is of 0-*order* k if F is of projective 0-order k and never meets infinity.

It is immediate from the definition that a mapping $f_{s,t}$ is of 0-order k if and only if the corresponding automorphism $F_{s,t}$ is of 0-order k. First of all, we shall get rid of trivial cases:

Lemma 4. *The projective* 0*-order of* $F_{s,t}$ *can never be equal to* 1*.*

Proof. This is because $F\binom{0}{1} = \binom{1}{1}$. □

Lemma 5. *Let* s *and* t *be distinct elements of* K*. The projective* 0*-order of* $F_{s,t}$ *is* $k = 2$ *if and only if* $s = -1$*. If* $s = -1$*, then* $F_{-1,t}$ *does not meet infinity.*

Proof. From the relation $F^2 = \begin{pmatrix} s^2+t & s+1 \\ st+t & t+1 \end{pmatrix}$ it is clear that the projective 0-order of F is 2 if and only if $s = -1$. Since $F\binom{0}{1} = \binom{1}{1}$, we see that F does not meet infinity at 1, hence, by periodicity, $F_{-1,t}$ never meets infinity. □

From now on, we will assume that $s \neq -1$, and hence that the projective 0–order of $F_{s,t}$ is $k > 2$.

Let $\lambda = \lambda_{s,t}$ and $\mu = \mu_{s,t}$ be the eigenvalues of the matrix $F_{s,t}$ These are the roots of the characteristic polynomial $P_{s,t} = x^2 - (s+1)x + s - t$ and belong to the algebraic closure of K (in fact they belong at most to a quadratic extension of K). They satisfy $\lambda + \mu = s + 1$ and $\lambda\mu = s - t$. Since $s \neq t$, none of the eigenvalues can be 0. The discriminant of P is

$$D_{s,t} = (s-1)^2 + 4t \, .$$

This value is $D_{s,t} = 0$ if and only if $t = -\left(\frac{s-1}{2}\right)^2$. This is the case we investigate first.

Proposition 6. *Assume that* $t = -\left(\frac{s-1}{2}\right)^2$ *and* $s \neq -1$*.*

The projective 0*-order of* $F_{s,t}$ *depends on the characteristic of the field* K *and is equal to*

$$k = \begin{cases} p & \text{if } \operatorname{char}(K) = p, (p \neq 2) \\ \infty & \text{if } \operatorname{char}(K) = 0 \end{cases}$$

If $s = 1$*, then* $F_{1,0}$ *does not meet infinity.*

If $s \neq 1$*, then* $F_{s,t}$ *meets infinity at* ℓ *if and only if* $\ell = 1 + \frac{2}{s-1}$*. In particular, in odd characteristic* p *it meets infinity if and only if* s *belongs to the prime field* $\mathbb{F}_p$*.*

Proof. We first remark that the assumption $s \neq -1$ implies that $t \neq s$. We have $F = \frac{s+1}{2} \cdot I + N$, where $N = \begin{pmatrix} (s-1)/2 & 1 \\ -(s-1)^2/4 & -(s-1)/2 \end{pmatrix}$ and I is the identity matrix. Note that $N^2 = 0$ and that $\frac{s+1}{2}$ is invertible in K. Hence, using binomial expansion, we get $F^i = \left(\frac{s+1}{2}\right)^i \cdot I + i \cdot \left(\frac{s+1}{2}\right)^{i-1} \cdot N$. The first coordinate of the vector $F^i\binom{0}{1}$ is then $i \cdot \left(\frac{s+1}{2}\right)^{i-1}$ which is zero if and only if i is zero, whence the value of the projective 0-order.

The second coordinate of $F^i\binom{0}{1}$ is $\left(\frac{s+1}{2}\right)^i + i \cdot \left(\frac{s+1}{2}\right)^{i-1} \cdot \left(-\frac{s-1}{2}\right)$ which is equal to zero if and only if $i = 1 + \frac{2}{s-1}$ (if $s = 1$, this is never equal to zero).

In odd characteristic p, the conclusion is clear from the relation $i = 1 + \frac{2}{s-1}$. □

The previous proposition is in fact interesting in the case $s \neq 1$ only. Indeed, if $s = 1$ and $t = -(\frac{s-1}{2})^2$ then $t = 0$. But the choice $t = 0$ gives raise to a group, according to Proposition 2.

We are now finished with the case $D_{s,t} = 0$ and we can proceed with the generic case $D_{s,t} \neq 0$, i.e. $\lambda \neq \mu$. We recall that from the relation $\lambda\mu = s - t$, we have seen that λ and μ cannot be equal to 0.

Proposition 7. *Assume that $D_{s,t} \neq 0$. For $i \geq 0$ we have*

$$F_{s,t}^i \binom{0}{1} = \begin{pmatrix} \frac{\lambda^i - \mu^i}{\lambda - \mu} \\ \frac{\lambda^i(1-\mu) - \mu^i(1-\lambda)}{\lambda - \mu} \end{pmatrix}.$$

The projective 0-order of $F_{s,t}$ is equal to the order of $\frac{\lambda}{\mu}$ in the multiplicative group $\overline{K}^*$, that is the smallest positive integer such that $\left(\frac{\lambda}{\mu}\right)^k = 1$.

If $t = 0$, then $F_{s,0}$ does not meet infinity. If $t \neq 0$, then $\lambda - 1$ and $\mu - 1$ are both nonzero, and the mapping $F_{s,t}$ meets infinity at ℓ if $\left(\frac{\lambda}{\mu}\right)^\ell = \frac{\lambda - 1}{\mu - 1}$.

Proof. Since F has two distinct eigenvalues, there exists a regular matrix S, with coefficients in $\overline{K}$, such that $F = S \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right) S^{-1}$. Hence $F^i \binom{0}{1} = S \left(\begin{smallmatrix} \lambda^i & 0 \\ 0 & \mu^i \end{smallmatrix}\right) S^{-1} \binom{0}{1} = \lambda^i A + \mu^i B$ for some vectors A and B. From the independent linear relations $F^0 \binom{0}{1} = A + B = \binom{0}{1}$ and $F^1 \binom{0}{1} = \lambda A + \mu B = \binom{1}{1}$, we find the solution

$$A = \begin{pmatrix} \frac{1}{\lambda - \mu} \\ \frac{1 - \mu}{\lambda - \mu} \end{pmatrix}, \qquad B = \begin{pmatrix} \frac{-1}{\lambda - \mu} \\ -\frac{1 - \lambda}{\lambda - \mu} \end{pmatrix},$$

giving the first part of the proposition.

The projective 0-order of F is the smallest positive integer k such that $F^k \binom{0}{1} = \binom{0}{x}$. From the previous relation, this is the smallest positive integer such that $\frac{\lambda^k - \mu^k}{\lambda - \mu} = 0$ and hence $\lambda^k = \mu^k$.

By definition, F meets infinity at ℓ if $F^\ell \binom{0}{1} = \binom{x}{0}$. From the previous relation, this is equivalent to $\frac{\lambda^\ell(1-\mu) - \mu^\ell(1-\lambda)}{\lambda - \mu} = 0$. We have $(1 - \lambda)(1 - \mu) = P(1) = -t$. If $t = 0$ then $P(1) = 0$ hence either $\lambda = 1$ or $\mu = 1$ (but not both). By symmetry, we may assume that $\mu = 1$ and $\lambda \neq 1$. In this case, the condition that F meets infinity at ℓ simplifies to $1 = 0$, which is clearly impossible. When $t \neq 0$, we have $P(1) \neq 0$, hence λ and μ are different from 1. In this case, the condition that F meets infinity at ℓ simplifies to $\left(\frac{\lambda}{\mu}\right)^\ell = \frac{1 - \lambda}{1 - \mu}$.

□

This proposition gives us a first answer to our question 1 stated in section 2 when the base ring is a field.

Corollary 8. *Let $F_{s,t}$ be a mapping defined over a field K (of odd characteristic), such that $D_{s,t} \neq 0$. Assume that $F_{s,t}$ has projective 0-order $k > 2$.*

- *If $D_{s,t}$ is a square in K, then K contains a primitive k-th root of unity.*
- *If $D_{s,t}$ is not a square in K, then the quadratic extension $K(\sqrt{D_{s,t}})$ contains a primitive k-th root of unity of norm 1.*

Proof. From Proposition 7, it is immediate that $\frac{\lambda}{\mu}$ is a primitive k-th root of unity in $K(\sqrt{D})$. If D is not a square in K, then the eigenvalues λ and μ are conjugate in the quadratic extension $K(\sqrt{D})$, hence $\frac{\lambda}{\mu}$ has norm 1. □

In order to apply this corollary to a finite field, it is useful to have the following description of the roots of unity in finite fields:

Proposition 9. *Let $K = \mathbb{F}_q$ with $q = p^n$ ($p \neq 2$). For an integer $k > 0$, we have*

- $\mathbb{F}_q$ *contains a primitive* k*-th root of unity if and only if* k *is a divisor of* $q-1$.
- $\mathbb{F}_{q^2}$ *contains a primitive* k*-th root of unity of norm* 1 *in the extension* $\mathbb{F}_{q^2}/\mathbb{F}_q$ *if and only if* k *is a divisor of* $q+1$.

Proof. The first assertion is an immediate consequence of the fact that the multiplicative group $\mathbb{F}_q^*$ is cyclic of order $q-1$. Consider now the second assertion. The norm map is a surjective homomorphism $\mathbb{F}_{q^2}^* \twoheadrightarrow \mathbb{F}_q^*$, hence its kernel is a subgroup of $\mathbb{F}_{q^2}^*$, of order $(q^2-1)/(q-1) = q+1$. This kernel is therefore the cyclic subgroup of order $q+1$, whence the conclusion. □

By Corollary 8, we have given a partial answer to our question 1. In order to prove that this in fact a complete answer, we need to study the converse property, and in fact to answer our question 2.

Proposition 10. *Assume that the field* K *contains a primitive* k*–th root of unity for* $k > 2$*. Then, for each* $s \in K$, $s \neq -1$, *there exist exactly* $\varphi(k)/2$ *choices of* $t \in K$ *such that* $F_{s,t}$ *is of projective* 0*-order* k, *namely* $t = \frac{(\zeta-s)(s\zeta-1)}{(\zeta+1)^2}$, *where* ζ *is any primitive* k*-th root of unity.*

Remark. In this proposition, $\varphi(k)$ denotes Euler's function.

Proof. Assume that $F_{s,t}$ is of projective 0-order $k > 2$. Then by Proposition 7, the quotient of the eigenvalues $\zeta = \frac{\lambda}{\mu}$ is a primitive k–th root of unity. We have the relations $\lambda = \zeta\mu$ and $\lambda + \mu = s + 1$, hence $\mu = \frac{s+1}{\zeta+1}$ and $\lambda = \frac{\zeta(s+1)}{\zeta+1}$. From this we get $s - t = \lambda\mu = \zeta\frac{(s+1)^2}{(\zeta+1)^2}$, whence $t = \frac{(\zeta-s)(s\zeta-1)}{(\zeta+1)^2}$.

Conversely, assume that $t = \frac{(\zeta-s)(s\zeta-1)}{(\zeta+1)^2}$, where ζ is a primitive k-th root of unity in K. With this choice, we have $(x - \frac{s+1}{\zeta+1})(x - \frac{\zeta(s+1)}{\zeta+1}) = x^2 - (s+1)x + s - \frac{(\zeta-s)(s\zeta-1)}{(\zeta+1)^2} = P_{s,t}$. According to Proposition 7, the projective 0-order of $F_{s,t}$ is the smallest k' such that $\left(\frac{s+1}{\zeta+1}\right)^{k'} = \left(\frac{\zeta(s+1)}{\zeta+1}\right)^{k'}$ or equivalently such that $1 = \zeta^{k'}$. By definition of ζ, the projective 0–order of $F_{s,t}$ is exactly k.

In order to finish the proof of the proposition, it only remains to prove that the map $\zeta \mapsto t$ is 2-to-1, since there are exactly $\varphi(k)$ primitive k-th roots of unity in K.

We have $t = \frac{(\zeta-s)(s\zeta-1)}{(\zeta+1)^2} = \left(\frac{(s+1)(\zeta-1)}{2(\zeta+1)}\right)^2 - \left(\frac{s-1}{2}\right)^2$. We look at the equality the other way round saying

$$\frac{\zeta-1}{\zeta+1} = \pm\frac{2}{s+1}\cdot\sqrt{t + \left(\frac{s-1}{2}\right)^2} = \pm\frac{2}{\lambda+\mu}\cdot\sqrt{\frac{D}{4}} = \pm\frac{2}{\lambda+\mu}\cdot\frac{\lambda-\mu}{2} = \pm\frac{\lambda-\mu}{\lambda+\mu}$$

which leads to $\zeta = \lambda/\mu$ or $\zeta = \mu/\lambda$. This proves that two different values of ζ give rise to the same value of t if and only if they are inverse to one other, and that the map $\zeta \mapsto t$ is 2-to-1 when $k > 2$. □

Example. Let $K = \mathbb{C}$. Then, for any s and k, there exists $F_{s,t}$ of projective 0-order k since all k-th roots of 1 lie in $\mathbb{C}$. Furthermore, if we consider $s = 1$ and $t = 4$, the corresponding eigenvalues are $\lambda = -1$ and $\mu = 3$, hence $\frac{\lambda}{\mu}$ is not a root of unity in $\mathbb{C}$ and $F_{1,4}$ has projective 0-order $k = \infty$. A counting argument would prove that almost all choice of s and t gives an $F_{s,t}$ with infinite projective 0-order.

Proposition 11. *Assume that a quadratic extension* L *of* K *contains a primitive* k*–th root of unity for* $k > 2$*, of norm* 1*. Then, for each* $s \in K$, $s \neq -1$, *there exist*

exactly $\varphi(k)/2$ choices of $t \in K$ such that $F_{s,t}$ is of projective 0-order k, namely $t = \frac{(\zeta-s)(s\zeta-1)}{(\zeta+1)^2}$, where ζ is any primitive k-th root of unity in L.

Proof. Everything in this proposition is already contained in Proposition 10 (applied to the field L), except that the given formula for t indeed gives an element of K when $s \in K$ and ζ has norm 1. Let $\overline{\zeta}$ and $\overline{t}$ be the conjugates of ζ and t in the extension L/K. We have $\zeta\overline{\zeta} = 1$. Starting from the definition of $\overline{t}$ and multiplying the numerator and the denominator by ζ^2, we obtain

$$\overline{t} = \frac{(\overline{\zeta} - s)(s\overline{\zeta} - 1)}{(\overline{\zeta} + 1)^2} = \frac{(1 - s\zeta)(s - \zeta)}{(1 + \zeta)^2} = t \ .$$

□

Remark. This result suggests a more symmetrical expression for t:

$$t = -\frac{(\zeta - s)(\zeta^{-1} - s)}{(\zeta + 1)(\zeta^{-1} + 1)} \ .$$

Putting things together, we have now a complete answer to our questions 1 and 2 in the case of fields. In fact, this result is only concerned with the projective 0-order and not the general 0-order, that is it does not say anything about the question of meeting infinity. We shall answer this question later but only when $s = 1$.

Theorem 12. *Let K be a field and $s \neq -1$ be any element of K. Let $k > 2$ be an integer and assume that $\mathrm{char}(K) \nmid 2k$. There exists $t \in K$ such that $F_{s,t}$ is of projective 0-order k if and only if a primitive k-th root of unity*

- *either lies in K*
- *or lies in a quadratic extension of K and is of norm 1 with respect to K.*

If one of these conditions is fulfilled then there exist exactly $\varphi(k)/2$ choices of t, namely $t = \frac{(\zeta-s)(s\zeta-1)}{(\zeta+1)^2}$, where ζ is a primitive k-th root of unity.

Example. Let us take $K = \mathbb{R}$. For every $k > 2$, the k-th roots of unity are complex numbers of norm 1 and hence, for every $s \neq -1$, there exists a $t \in \mathbb{R}$ such that $F_{s,t}$ is of projective 0-order k. This value of k is obtained for example for $s = 1$ and $t = -\frac{1-\cos(2\pi/k)}{1+\cos(2\pi/k)} = -\tan^2(\pi/k)$.

Example. Let us take $K = \mathbb{Q}$. A primitive k-th root of unity lies in a quadratic extension of $\mathbb{Q}$ if and only if $k = 3$, 4, or 6. Hence the only possible finite projective 0-orders are respectively 3, 4, and 6. These values are made possible for example by the values $s = 1$ and respectively $t = -3$, $t = -1$, and $t = -1/3$.

Now we are done with examining the projective 0-order and it is time to study when $F_{s,t}$ meets infinity. However it does not seem to be easy to solve, except in the case $s = 1$. The mapping $F_{1,0}$ was studied in Proposition 6.

Lemma 13. *Let $t \neq 0$ be an element of K. Assume that $F_{1,t}$ is of projective 0-order k. Then $F_{1,t}$ meets infinity at ℓ if and only if k is a finite even integer and ℓ is an odd multiple of $k/2$.*

Proof. According to Proposition 7, $F_{1,t}$ meets infinity at ℓ if $(\lambda/\mu)^\ell = (\lambda-1)/(\mu-1)$. Under the condition $s = 1$, λ and μ are roots of the polynomial $P_{1,t}$ that can be rewritten as $P_{1,t} = (x-1)^2 - t$, which implies that $\lambda - 1$ and $\mu - 1$ are equal to $\pm\sqrt{t}$. In particular, the quotient $(\lambda - 1)/(\mu - 1)$ is equal to -1. We deduce from the relation $(\lambda/\mu)^\ell = -1$ that $(\lambda/\mu)^{2\ell} = 1$, hence k is a finite even integer, and ℓ is an odd multiple of $k/2$.

□

We are now ready to write down the conclusion for the case $s = 1$.

Theorem 14. *Let K be a field of characteristic different from 2, and $k > 1$ be an integer. There exists a 0-bijection $f(x) = (x+1)/(tx+1)$ of finite 0-order k, for some $t \in K$ if and only if k is odd and one of the following three conditions is satisfied:*

- *k is equal to the characteristic of K;*
- *a primitive k-th root of unity lies in K;*
- *a primitive k-th root of unity is an element of norm 1 in a quadratic extension of K.*

In particular, if K is the finite field $\mathbb{F}_q$, for $q = p^n$, then such a 0-bijection exists if and only if k is odd and

- *$k = p$*
- *or $k \mid (q-1)$,*
- *or $k \mid (q+1)$.*

Proof. The fact that k has to be odd was proved in Lemma 13. The case $t = 0$ was studied in Proposition 6 and corresponds to the case $k = \mathrm{char}(K)$ (if not 0). The other cases, including the explicit construction of t, were established in Theorem 12. The reformulation for the finite field case results from Proposition 9. □

4. Orders of mappings in $\mathbb{Z}/n\mathbb{Z}$

Our main task is to describe the behaviour of the mappings $f_{s,t}$ on rings $\mathbb{Z}/n\mathbb{Z}$. Again, we shall consider n to be odd.

As in the field case, we study first the projective version of the mapping $f_{s,t} = \frac{sx+1}{tx+1}$ and compute its projective 0-order. Secondly, we determine whether this projective mapping meets infinity or not. Before we can proceed, we need to adapt the definitions.

Let R be a commutative ring. We denote by R^* the multiplicative group of invertible elements of R. This group acts componentwise on R^2. If $(a, b) \in R^2$ is such that the ideal $aR + bR$ is equal to R, then the same is true for the ideal $uaR + ubR$ when $u \in R^*$. This allows the definition of the projective line :

$$\mathbb{P}^1(R) = \{(a, b) \in R^2, aR + bR = R\}/R^* .$$

The group $G_2(R)$ of 2×2 matrices $F = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with invertible determinant $(ad-bc) \in R^*$ acts on $\mathbb{P}^1(R)$ by the classical formulae. Its elements define automorphisms of $\mathbb{P}^1(R)$. This is in particular the case for $F_{s,t} = \left(\begin{smallmatrix} s & 1 \\ t & 1 \end{smallmatrix}\right)$ when

$$(s - t) \in R^* .$$

We also define its characteristic polynomial $P_{s,t} = x^2 - (s+1)x + s - t$ with discriminant $D_{s,t} = (s-1)^2 + 4t$, exactly as in section 3.

Definition. Let F be an automorphism of the projective line $\mathbb{P}^1(R)$. We say that F is of *projective 0-order* k if k is the smallest positive integer such that $F^k\binom{0}{1} = \binom{0}{x}$, for some $x \in R^*$.
We say that F *meets infinity* at ℓ, if $F^\ell\binom{0}{1} = \binom{x}{y}$, for some $(x, y) \in R^2$, $y \notin R^*$. We say simply that F meets infinity if there is some ℓ at which it happens.
We say that F is of *0-order* k if F is of projective 0-order k and never meets infinity.

When R is a field, all these definitions coincide with those defined in section 3.

As in the field case, it is immediate from the definition that a mapping $f_{s,t}$ is of 0-order k if and only if the corresponding automorphism $F_{s,t}$ is of 0-order k.

The work is already done in the case $\mathbb{Z}/p\mathbb{Z}$, for p prime, at least when $s = 1$. This knowledge, of course, is useful when studying $\mathbb{Z}/n\mathbb{Z}$ in general. There are two cases to be considered, one of which is very easy.

Proposition 15. *Let $R = \mathbb{Z}/mn\mathbb{Z}$, where m and n are coprime, and let $s \in R$. Then there exists some $t \in R$ with $s - t \in R^*$ such that $f_{s,t}$ is of 0-order k if and only if the reduction modulo m of $f_{s,t}$ is of 0-order k_1 in $\mathbb{Z}/m\mathbb{Z}$, the reduction modulo n of $f_{s,t}$ is of 0-order k_2 in $\mathbb{Z}/n\mathbb{Z}$, and k is the least common multiple of k_1 and k_2.*

Proof. Use the Chinese remainder theorem. □

The other case leaves much more work and concerns the ring $R = \mathbb{Z}/p^r\mathbb{Z}$, for p prime. In this context, the condition $s - t \in R^*$ is equivalent to $s \not\equiv t \pmod p$.

We consider first the situation when $D_{s,t} \equiv 0 \pmod p$, and generalize Proposition 6 in Proposition 17. Before this, we need a lemma.

Lemma 16. *Let A and B be 2×2 matrices, with coefficients in $\mathbb{Z}$. Let p be a prime number and $\alpha \geq 1$ be an integer. If $A \equiv B \pmod{p^\alpha}$ and $B \equiv \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right) \pmod p$, then $A^p \equiv B^p \pmod{p^{\alpha+1}}$.*

Proof. Let C be the matrix with integer coefficients such that $A = B + p^\alpha C$. Expanding the product, we find $A^p \equiv B^p + p^\alpha(B^{p-1}C + B^{p-2}CB + \cdots + CB^{p-1}) \pmod{p^{\alpha+1}}$. The condition $B \equiv \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right) \pmod p$ implies that the sum in brackets is $B^{p-1}C + B^{p-2}CB + \cdots + CB^{p-1} \equiv pC \equiv 0 \pmod p$, and we get $A^p \equiv B^p \pmod{p^{\alpha+1}}$. □

Proposition 17. *Let s and t be elements of the ring $R = \mathbb{Z}/p^r\mathbb{Z}$, such that $s \not\equiv t \pmod p$. If $D_{s,t} \equiv 0 \pmod p$, then the projective 0-order of $F_{s,t}$ is equal to*

$$k = \begin{cases} p^r & \text{if } p \geq 5 \\ p^{r-q+1} & \text{if } p = 3 \text{ and } q = v_3(D_{s,t} + 3(s-t)) \end{cases}$$

If furthermore $s \equiv 1 \pmod p$ (in which case the condition $D_{s,t} \equiv 0 \pmod p$ simplifies to $t \equiv 0 \pmod p$), then $F_{s,t}$ does not meet infinity.

Remark. We use here the notation $v_3(x)$ for the valuation at the prime 3. Since it is evaluated at elements of $\mathbb{Z}/3^r\mathbb{Z}$, this valuation is always bounded by r, including at 0.

Proof. We can assume that $r \geq 2$, since the case $r = 1$ is contained in Proposition 6. The condition $D \equiv 0 \pmod p$ implies that we can write $t = -\left(\frac{s-1}{2}\right)^2 + pa$ for some a defined modulo p^{r-1}. We have $s - t = s + \left(\frac{s-1}{2}\right)^2 - pa = \left(\frac{s+1}{2}\right)^2 - pa$, hence $u = \frac{s+1}{2}$ is invertible. With the notation $N = \begin{pmatrix} (s-1)/2 & 1 \\ -(s-1)^2/4 & -(s-1)/2 \end{pmatrix}$ and $A = \left(\begin{smallmatrix}0 & 0\\ 1 & 0\end{smallmatrix}\right)$, we have $F = uI + N + paA$, where $B = N + paA$ satisfies $B^2 = paI$.

For the next argument, we have to separate the cases $p \geq 5$ and $p = 3$.

Consider first the case $p \geq 5$. For $i \geq 4$, we have $B^i \equiv 0 \pmod{p^2}$, hence

$$\begin{aligned} F^p &\equiv u^pI + pu^{p-1}B + \tfrac{p(p-1)}{2}u^{p-2}B^2 + \tfrac{p(p-1)(p-2)}{6}u^{p-3}B^3 && \pmod{p^2} \\ &\equiv \left(u^p + \tfrac{ap^2(p-1)}{2}u^{p-2}\right)I + \left(pu^{p-1} + \tfrac{ap^2(p-1)(p-2)}{6}u^{p-3}\right)B && \pmod{p^2} \\ &\equiv u^pI + \left(pu^{p-1} + \tfrac{ap^2(p-1)(p-2)}{6}u^{p-3}\right)B && \pmod{p^2} \end{aligned}$$

Since $p \geq 5$, the coefficient $\frac{ap^2(p-1)(p-2)}{6}$ is divisible by p^2 and the expression simplifies to

$$\begin{aligned} F^p &\equiv u^pI + pu^{p-1}B && \pmod{p^2} \\ &\equiv u^pI + pu^{p-1}N && \pmod{p^2} \end{aligned}$$

This relation can be written as $F^p \equiv vI + p^q wN \pmod{p^{q+1}}$, where $v = u^p$ and $w = u^{p-1}$ are invertible, and $q = 1$.

If $p = 3$, we have $F^3 = u^3 I + 3u^2 B + 3uB^2 + B^3 = (u^3 + 9au)I + 3(u^2 + a)B$, where $u^3 + 9au$ is invertible since u is invertible. By definition, we have $q = v_3\left(D_{s,t} + 3(s-t)\right) = v_3\left(3(u^2+a)\right)$. If $q = r$, we have directly $F^3 = (u^3 + 9au)I$ and we get the conclusion that the projective 0-order of F is 3. If $q < r$, we can write

$$F^3 \equiv (u^3 + 9au)I + 3(u^2 + a)N \pmod{p^{q+1}}\,.$$

or $F^p \equiv vI + p^q wN \pmod{p^{q+1}}$, where v and w are invertible.

We have now exactly the same relations is both cases $p \geq 5$ and $p = 3$, and we can finish the proof with a common argument. The coefficient v is invertible, so that we can apply Lemma 16 to $v^{-1}F^p$ and get by induction

$$\begin{aligned} F^{p^\alpha} &\equiv (vI + p^v wN)^{p^{\alpha-1}} && \pmod{p^{q+\alpha}} \\ &\equiv v^{p^{\alpha-1}} I + p^{q+\alpha-1} wN && \pmod{p^{q+\alpha}} \end{aligned}$$

for all $1 \leq \alpha \leq r - q + 1$. For $\alpha = r - q$, this gives $F^{p^{r-q}}\binom{0}{1} = v^{p^{r-q-1}}\binom{0}{1} + p^{r-1}w\binom{1}{-(s-1)/2}$. Inspecting the first coefficient reveals that the projective 0-order of F is not a divisor of p^{r-q}. For $\alpha = r - q + 1$, this gives $F^{p^{r-q+1}}\binom{0}{1} = v^{p^{r-q}}\binom{0}{1}$, hence the projective 0-order of F is exactly p^{r-q+1}, as announced in the proposition.

So far we considered the projective 0-order and not the 0-order itself. It remains to determine whether $F_{s,t}$ meets infinity. By definition, $F_{s,t}$ meets infinity at ℓ if the reduction modulo p of $F_{s,t}$ meets infinity at ℓ. When $s \equiv 1 \pmod{p}$, Proposition 6 says that the reduction modulo p of $F_{s,t}$ does not meet infinity, hence $F_{s,t}$ does not meet infinity at all. □

Hence the case $D_{s,t} \equiv 0 \pmod{p}$ is finished and we can focus on the case when $D_{s,t} \not\equiv 0 \pmod{p}$.

We first suppose that $D_{s,t}$ is an invertible square in R, or equivalently that it is a nonzero square modulo p.

Proposition 18. *Let $R = \mathbb{Z}/p^r\mathbb{Z}$*

- *Let s, t be elements of R with $s \not\equiv t \pmod{p}$. If $D_{s,t}$ is a nonzero square modulo p, then the projective 0-order of $F_{s,t}$ is of the form $k = k'p^m$ where $m < r$ and k' is the projective 0-order of the reduction modulo p of $F_{s,t}$. In particular, k' satisfies $1 < k' \mid (p-1)$.*
  If furthermore $s \equiv 1 \pmod{p}$ (and t is a nonzero square modulo p) then $F_{s,t}$ meets infinity if and only if k is even.
- *Let s be an element of R with $s \not\equiv -1 \pmod{p}$, and $k = k'p^m$ be an integer with $m < r$ and $2 < k' \mid (p-1)$. There exist exactly $\varphi(k)/2$ choices of $t \in R$, $t \not\equiv s \pmod{p}$, such that $F_{s,t}$ is of projective 0-order k.*

Proof. Consider the first part of the proposition, and let s and t be as required. We can apply the results of the section 3 to the reduction of F modulo p. In particular, since $D \not\equiv 0 \pmod{p}$, there exist exactly two distinct roots λ_p and μ_p of the characteristic polynomial P modulo p. They satisfy $\lambda_p\mu_p \equiv s - t \pmod{p}$, hence λ_p and μ_p are invertible. Since p is odd, an application of Hensel Lemma implies that D is in fact a square in $\mathbb{Z}/p^r\mathbb{Z}$ and that there exist exactly two distinct elements λ and μ of $\mathbb{Z}/p^r\mathbb{Z}$ such that $P(\lambda) = P(\mu) = 0$. These elements satisfy furthermore $\lambda \equiv \lambda_p \pmod{p}$ and $\mu \equiv \mu_p \pmod{p}$, and also the relation $\lambda\mu = s - t$, hence are both invertible. Another useful relation is $(\lambda - \mu)^2 = D$, hence $\lambda - \mu$ is also invertible.

The expression of $F^i\binom{0}{1}$ in terms of λ, μ and i given in Proposition 7 still applies in our context. Inspecting its first coefficient implies that the projective 0-order of F is again the multiplicative order of the invertible element λ/μ, or equivalently the smallest positive integer k such that $(\lambda/\mu)^k = 1$.

Now, the group $(\mathbb{Z}/p^r\mathbb{Z})^*$ is cyclic of order $(p-1)p^{r-1}$, hence the projective 0-order k of F is $k = k'p^m$ with $k' \mid (p-1)$ and $m < r$. More precisely, we have an isomorphism of groups:

$$\phi : (\mathbb{Z}/p^r\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{r-1}\mathbb{Z}$$

(the group on the left is multiplicative and the groups on the right are additive). The first coordinate of ϕ in $\mathbb{Z}/(p-1)\mathbb{Z}$ is given by the reduction modulo p followed by the isomorphism $(\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$. This isomorphism shows that k' is equal to multiplicative order of λ_p/μ_p in $(\mathbb{Z}/p\mathbb{Z})^*$, that is by the projective 0-order of the reduction of F modulo p according to Proposition 7.

When $s \equiv 1 \pmod p$, we can apply Lemma 13 and deduce that F meets infinity modulo p if and only if k' is even, hence also in R.

Consider now the second part of the proposition and let s and k be as required. Using the isomorphism ϕ, we see that there are exactly $\varphi(k)$ choices of $\zeta \in R^*$ that are of multiplicative order exactly k. Since $k' > 2$, we have $\zeta \not\equiv -1 \pmod p$, hence $\zeta + 1$ is invertible. The rest of the proof is analogous to the proof of Proposition 10. In particular, the value of t is given by the same formula $t = \frac{(\zeta - s)(s\zeta - 1)}{(\zeta+1)^2}$. □

The case when $D_{s,t}$ is an invertible nonsquare in R (or equivalently when it is not a square modulo p) is similar but technically less transparent. Exactly as in the case of fields where the eigenvalues were found in a quadratic extension, we need to build a quadratic extension of R containing the eigenvalues.

Proposition 19. *Let $R = \mathbb{Z}/p^r\mathbb{Z}$*

- *Let s, t be elements of R with $s \not\equiv t \pmod p$. If $D_{s,t}$ is not a square modulo p, then the projective 0-order of $F_{s,t}$ is of the form $k = k'p^m$ where $m < r$ and k' is the projective 0-order of the reduction modulo p of $F_{s,t}$. In particular, k' satisfies $1 < k' \mid (p+1)$.*
  If furthermore $s \equiv 1 \pmod p$ (and t is not a square modulo p) then $F_{s,t}$ meets infinity if and only if k is even.
- *Let s be an element of R with $s \not\equiv -1 \pmod p$, and $k = k'p^m$ be an integer with $m < r$ and $2 < k' \mid (p+1)$. There exist exactly $\varphi(k)/2$ choices of $t \in R$, $t \not\equiv s \pmod p$, such that $F_{s,t}$ is of projective 0-order k.*

Proof. Let $d \in \mathbb{Z}$ be an integer which is not a square modulo p. We consider the quadratic field $L = \mathbb{Q}(\sqrt{d})$ and $\mathcal{O}$ its ring of integers. By construction the polynomial $x^2 - d$ is irreducible modulo p, hence the ideal $p\mathcal{O}$ is a prime ideal of $\mathcal{O}$ (see [3, §4.8] for more justification). In particular, $\mathcal{O}/p\mathcal{O}$ is a finite field with p^2 elements and the ring $R' = \mathcal{O}/p^r\mathcal{O}$ contains a copy of R. There are group isomorphisms

$$(\mathcal{O}/p\mathcal{O})^* \;\cong\; \mathbb{Z}/(p^2-1)\mathbb{Z}$$

and

$$(\mathcal{O}/p^r\mathcal{O})^* \;\cong\; (\mathcal{O}/p\mathcal{O})^* \times \mathcal{O}/p^{r-1}\mathcal{O} \;\cong\; \mathbb{Z}/(p^2-1)\mathbb{Z} \times (\mathbb{Z}/p^{r-1}\mathbb{Z})^2 \,.$$

The first one is the well known fact that the multiplicative group of a finite field is cyclic and the second one is proved in [4, Prop 4.2.4 and 4.2.8].

Let us now come to the proof of the first part of the proposition, and let s and t be elements as required. We can use exactly the same argument as for the previous proposition: the reduction of the characteristic polynomial P has exactly two distinct roots λ_p and μ_p in $\mathcal{O}/p\mathcal{O}$, and by a Hensel lifting, P has exactly

two distinct roots λ and μ in R'. We can then use the formula of Proposition 7 and deduce that the projective 0-order of F is the multiplicative order of λ/μ in $(\mathcal{O}/p^r\mathcal{O})^*$. Using the isomorphism, we deduce that this order is of the form $k = k'p^m$ with $m < r$ and $k' \mid (p^2-1)$. But we also deduce that k' is the projective 0-order of the reduction modulo p of F, hence, according to the results of section 3, is a divisor of $p+1$.

When $s \equiv 1 \pmod{p}$, we can apply Lemma 13 and deduce that F meets infinity modulo p if and only if k' is even, hence also in R.

For the second part of the proposition, let s and k be as required. Following the same proof as for Proposition 18, we see that there are exactly $\varphi(k)$ choices of $\zeta \in R'^*$ that are of multiplicative order exactly k, and exactly $\varphi(k)/2$ choices of $t \in R'$, given by the formula $t = \frac{(\zeta-s)(s\zeta-1)}{(\zeta+1)^2}$, such that $F_{s,t}$ is of projective 0-order k. It remains to prove that t is indeed in R and not only in R'.

The norm map from $\mathcal{Q}(\sqrt{d})$ to $\mathcal{Q}$ sends $p^r\mathcal{O}$ to $p^r\mathbb{Z}$, and defines another norm map from R'^* to R^*, which is a group homomorphism. Its image contains trivially all the squares of R^* as the norm of elements of R^*, but also contains $d = \mathrm{norm}(\sqrt{d})$. Hence the norm is surjective and its kernel is a subgroup of R'^* of order $(p+1)p^{r-1}$. From this, we see that the elements of order $p+1$ in R'^* have norm 1. Now, the same proof as for Proposition 11 will again give the conclusion that $t \in R$. □

Hence we can conclude what happens for any $\mathbb{Z}/n\mathbb{Z}$ if $s = 1$.

Theorem 20. *Let $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_m^{r_m}$ be the prime factorization of a positive odd number and let $k > 1$ be an integer. Then there exists $t \in \mathbb{Z}/n\mathbb{Z}$ such that $f_{1,t}$ is a 0-bijection from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ of 0-order k if and only if k is odd and there exist $k_1, \ldots, k_m$ and $\varepsilon_1, \ldots, \varepsilon_m$ satisfying the three conditions:*

- *$\varepsilon_i \in \{-1, 0, 1\}$, $k_i = k_i' p^{e_i}$, where $2 < k_i' \mid (p_i + \varepsilon_i)$ and $e_i < r_i$, for all $1 \le i \le m$;*
- *if $\varepsilon_i = 0$ and $p_i > 3$, for some i, then $k_i = p_i^{r_i}$;*
- *the least common multiple of $k_1, \ldots, k_m$ is k.*

Proof. We make an induction on m. Suppose first that $m = 1$. We have seen in Lemma 13 that $F_{1,t}$, for $t \not\equiv 0 \pmod{p}$, meets infinity if and only if its projective order is even. But if $t \equiv 0 \pmod{p}$ then k_1 is a divisor of $p_1^{r_1}$, according to Proposition 17. Hence k has to be odd.

The previous three propositions ensure that the theorem holds in the case of $m = 1$. The induction step can be done using Proposition 15. □

5. The question of isomorphism

From now on, we shall consider the case $s = 1$ only. We know already when there exists an appropriate fractional mapping of 0-order k on R, in the case when R is a field or a quotient of $\mathbb{Z}$. Nevertheless, we do not know still if different choices of t, that lead to the same k, give raise to different A-loops or not. The answer depends on the ring. For fields and $\mathbb{Z}/p^r\mathbb{Z}$ there exist a unique loop for each admissible 0-order. In the other cases there can be more isomorphism classes. We shall ignore the case $t = 0$ since the associated loop is a group then, according to Proposition 2.

From now on, R is either a field or $\mathbb{Z}/n\mathbb{Z}$. We are in a special case, namely $s = 1$, hence some things, that we have already established, simplify substantially. It is useful to have a description what elements can be obtained as $f^i(0)$.

Lemma 21. *Let $t \in R^*$ be such that $t-1 \in R^*$ and $f_{1,t}$ is of finite 0-order k. Then $k > 2$ and*

(i) $t = \left(\frac{\zeta-1}{\zeta+1}\right)^2$ *where* ζ *is an element of multiplicative order* k *(in an extension of* R*).*

(ii) The roots of the characteristic polynomial are $\lambda = \frac{2\zeta}{\zeta+1}$ *and* $\mu = \frac{2}{\zeta+1}$.

(iii) $F^i_{1,t}\binom{0}{1} = \begin{pmatrix} \frac{\lambda^i-\mu^i}{\lambda-\mu} \\ \frac{\lambda^i+\mu^i}{2} \end{pmatrix}$

(iv) $f^i_{1,t}(0) = \dfrac{\zeta+1}{\zeta-1} \cdot \dfrac{\zeta^i-1}{\zeta^i+1}$

Proof. (i) was stated in Proposition 12 for fields; for $R = \mathbb{Z}/p^r\mathbb{Z}$ it is the same according to the proofs of Proposition 18 or 19. In the case of $\mathbb{Z}/mn\mathbb{Z}$, for m and n coprime, we use the induction and the Chinese remainder theorem.

For proving (ii) just check that $\lambda + \mu = 2$ and $\lambda\mu = 1 - t$.

(iii) Something similar was written in Proposition 7 with the exception that the second coordinate was $\frac{\lambda^i(1-\mu)-\mu^i(1-\lambda)}{\lambda-\mu}$. But $\frac{1-\mu}{\lambda-\mu} = \frac{\zeta+1-2}{\zeta+1} \cdot \frac{\zeta+1}{2\zeta-2} = \frac{1}{2}$ and analogously $\frac{1-\lambda}{\lambda-\mu} = -\frac{1}{2}$. Hence the second coordinate simplifies to $(\lambda^i + \mu^i)/2$.

(iv) By (iii), we have $f^i_{1,t}(0) = \frac{\lambda^i-\mu^i}{\lambda-\mu} \cdot \frac{2}{\lambda^i+\mu^i}$. Replacing 2 by $\lambda+\mu$ and using the relation $\frac{\lambda}{\mu} = \zeta$, we get $f^i_{1,t}(0) = \frac{\zeta^i-1}{\zeta-1} \cdot \frac{\zeta+1}{\zeta^i+1}$. □

As a byproduct, we can rewrite Proposition 1 in a better looking way, at least for the case $t \in R^*$.

Proposition 22. *Let* M *be a module over a ring* R*, which is either a field or the ring* $\mathbb{Z}/n\mathbb{Z}$*. Suppose that there exists* ζ*, an element of an odd order* k*, lying either in* R^**, or in a quadratic extension of* R *and being of norm* 1*, with respect to* R*. Then we can define a commutative A-loop on the set* $M \times \mathbb{Z}/k\mathbb{Z}$ *as follows:*

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

This loop is equal to $M[1, t]$ *for* $t = \left(\frac{\zeta-1}{\zeta+1}\right)^2$.

Proof. It was described in Theorem 14 and Theorem 20 that for the specified choices of k there exists a t such that $f_{1,t}$ is of 0-order k. According to Lemma 21, we have $t = \left(\frac{\zeta-1}{\zeta+1}\right)^2$ and $f^i(0) = \frac{\zeta+1}{\zeta-1} \cdot \frac{\zeta^i-1}{\zeta^i+1}$. Hence $1 + tf^i(0)f^j(0) = \frac{2(\zeta^{i+j}+1)}{(\zeta^i+1)(\zeta^j+1)}$ and we insert this expression into Proposition 1. □

We are ready now to tackle the problem of isomorphism. We shall use the result Drápal found when studying his construction.

Proposition 23 (Drápal [5])**.** *Let* M *be a faithful module over a commutative ring* R*. Let* $t, t' \in R^*$ *be of the same finite* 0*-order* k*. Then an isomorphism* $M[1, t] \cong M[1, t']$ *which restricts to the identity upon* $M \times \{0\}$ *exists if and only if* $t' = td^2$ *for some* $d = f^r(0)$*, where* $1 \le r < k$*,* $r \in \mathbb{Z}^*_k$*. This condition is necessary and sufficient when* $M(+)$ *is a cyclic group.*

We already know what elements can be $f^r(0)$ and hence we can give an immediate answer: the construction is unique in the case of invertible elements in a field or in $\mathbb{Z}/p^r\mathbb{Z}$.

Proposition 24. *Let* M *be a faithful module over* R*, which is either a field or* $\mathbb{Z}/p^r\mathbb{Z}$*. Let* $t, t' \in R^*$ *be of the same finite* 0*-order* k*. Then the loops* $M[1, t]$ *and* $M[1, t']$ *are isomorphic.*

Proof. Write $t = \left(\frac{\zeta-1}{\zeta+1}\right)^2$ and $t' = \left(\frac{\zeta'-1}{\zeta'+1}\right)^2$. The element ζ is of multiplicative order k in R^* and so is the element ζ'. Since all k-th roots of 1 belong to the cyclic group generated by ζ, there exists some i such that $\zeta' = \zeta^i$.

According to Lemma 21 we have $f^i(0) = \frac{\zeta+1}{\zeta-1} \cdot \frac{\zeta^i-1}{\zeta^i+1}$ which is the d we are looking for. Indeed,

$$td^2 = \left(\frac{\zeta-1}{\zeta+1}\right)^2 \cdot \left(\frac{\zeta+1}{\zeta-1} \cdot \frac{\zeta^i-1}{\zeta^i+1}\right)^2 = \left(\frac{\zeta'-1}{\zeta'+1}\right)^2 = t'$$

Now the conditions of Proposition 23 are fulfilled. □

The unicity does not hold in the general case; the smallest examples, brought by the following proposition, are two non-isomorphic loops of order $5 \cdot 11 \cdot 19$.

Proposition 25. *Let $R = \mathbb{Z}/pq\mathbb{Z}$, where p and q are distinct primes. Let and odd $k > 2$ divide either $p-1$ or $p+1$ as well as either $q-1$ or $q+1$. Then there exist exactly $\varphi(k)/2$ non-isomorphic loops of order kpq, obtained as $R[1,t]$ for some $t \in R^*$.*

Proof. We have $R \cong \mathbb{F}_p \times \mathbb{F}_q$. A mapping F is of 0-order k on R if and only if both projections are of 0 order k on R. There exist exactly $\varphi(k)/2$ choices of such a t_p in $\mathbb{F}_p$ and there exist exactly $\varphi(k)/2$ choices of such a t_q in $\mathbb{F}_q$, thus giving $\varphi(k)^2/4$ choices of $t = (t_p, t_q)$.

We have $t_p = (\zeta_p - 1)/(\zeta_p + 1)$ where ζ_p is a primitive k-th root of 1 in $\mathbb{F}_p$. But $t_p = (\zeta_p^{-1} - 1)/(\zeta_p^{-1} + 1)$ too and these are both possibilities how to obtain t_p from a primitive k-th root of 1 in $\mathbb{F}_p$. The same holds for t_q and therefore there are four possibilities how to obtain t, namely from (ζ_p, ζ_q), (ζ_p, ζ_q^{-1}), (ζ_p^{-1}, ζ_q) and $(\zeta_p^{-1}, \zeta_q^{-1})$.

Now we follow the proof of Proposition 24. The cyclic group generated by (ζ_p, ζ_q) has $\varphi(k)$ elements; they give raise to $\varphi(k)/2$ different values of t' since (ζ_p^i, ζ_q^i) gives the same t' as $(\zeta_p^{-i}, \zeta_q^{-i})$. The elements from the cyclic subgroup generated by (ζ_p, ζ_q^{-1}) follow the structure of the subgroup generated by (ζ_p, ζ_q), meaning that the first coordinate is the same and the second is inverted, and therefore the same values of t' are obtained. Hence, according to Proposition 23, one loop with a given t is isomorphic to exactly $\varphi(k)/2$ loops $R[1,t']$ (including itself).

We know that there are $\varphi(k)^2/4$ choices of t which are split into isomorphism classes of $\varphi(k)/2$ elements. Hence there are $\varphi(k)/2$ isomorphism classes. □

We do not give any result for $t \notin R^*$ since the article of Drápal does not give us a tool for studying it. Nevertheless, it seems that something similar to Proposition 23 is true here: a computer computation using the GAP package Loops [9] gives $\mathbb{Z}/25\mathbb{Z}[1,5] \cong \mathbb{Z}/25\mathbb{Z}[1,20] \ncong \mathbb{Z}/25\mathbb{Z}[1,10] \cong \mathbb{Z}/25\mathbb{Z}[1,15]$. In other words, they are isomorphic if and only if t and t' differ by a square. Another example is $\mathbb{Z}/27\mathbb{Z}[1,6] \ncong \mathbb{Z}/27\mathbb{Z}[1,15]$ to see that it concerns 3-loops too.

A different question is whether, given a $t \in \mathbb{F}_p^*$, there is an isomorphism between $\mathbb{F}_{p^r}[1,t]$ and $\mathbb{Z}/p^r\mathbb{Z}[1,t]$. The answer is easy there: according to Proposition 1, we have $\mathrm{Inn}(\mathbb{F}_{p^r}[1,t]) \cong \mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/(p-1)\mathbb{Z}$ and $\mathrm{Inn}(\mathbb{Z}/p^r\mathbb{Z}[1,t]) \cong \mathbb{Z}/p^r\mathbb{Z} \rtimes \mathbb{Z}/p^{r-1}(p-1)\mathbb{Z}$. Hence the loops cannot be isomorphic.

6. Loops of a semiprime order

The first motivation when writing this article was to describe all commutative A-loops of order kp, for k and p primes (not necessarily distinct). First half of the section deals with this question; the work is nearly done up to one result which is expected to appear till the end of 2009.

Any construction of commutative A-loops of an odd order is helpful when studying Bruck loops too: Kinyon, Vojtěchovský and the first author proved in [6] that when $(Q,\cdot)$ is a non-associative commutative A-loop of an odd order then there exists an operation $\circ$ on Q defined as

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

such that $(Q,\circ)$ is a non-associative Bruck loop. In the second half of the section we give the explicit formula of the Bruck loop that arises this way from the commutative A-loops studied here.

But first look at commutative A-loops of order kp.

Theorem 26. *Let $k \leq p$ be two primes. Then there exists a non-associative commutative A-loop of order kp if and only if $k > 2$ and k divides $p^2 - 1$.*

Proof. "If": Let ζ be a primitive k-th root of 1 within $\mathbb{F}_{p^2}$ and put $t = \left(\frac{\zeta-1}{\zeta+1}\right)^2$. Then $\mathbb{Z}_p[1,t]$ is a commutative A-loop of order kp, according to Lemma 21 and Proposition 3. It is not associative according to Proposition 2.

"Only if": It was proved in [7] that commutative A-loops of orders $2p$ and p^2 are groups. Hence we can suppose $2 < k < p$. It was already said, in the beginning of the section, that once $(Q,\cdot)$ is an odd order commutative A-loop, there exists a non-associative Bruck loop of the same cardinality, namely $(Q,\circ)$. And according to Sharma [11], there exists a non-associative Bruck loop of order kp, for such k and p, if and only if k divides $p^2 - 1$. □

It is highly probable that such a loop is unique.

Conjecture 27. *Let k and p be two primes. Then there exists at most one non-associative commutative A-loop of order kp, up to isomorphism.*

Idea of a proof: Aleš Drápal decided once to characterise all loops with metacyclic inner mapping groups and trivial centers. It turned out that these loops fall into six types of constructions. The construction described in Proposition 1 is the only one of them bearing commutative A-loops.

It was proved in [7] that a commutative A-loop of order kp must have a trivial center and a normal subloop of order p. From this, it is easy to prove that such a loop must have a metacyclic inner mapping group. Hence it must fall into one of the categories described by Drápal and that means that it must be achievable by the construction of this paper. And, according to Proposition 24, all constructed loops of order kp are isomorphic.

The only reason why we call it a conjecture here rather than a theorem, is that the characterisation, we mentioned, has not been written yet and thus we cannot check its correctness. □

Now we shall concentrate on the Bruck loops associated to our commutative A-loops.

Theorem 28. *Let M be a module over a ring R, which is either a field or the ring $\mathbb{Z}/n\mathbb{Z}$. Suppose that there exists ζ, an element of an odd order k, lying either in R^*, or in a quadratic extension of R and being of norm 1, with respect to R. Then we can define a loop on the set $M \times \mathbb{Z}/k\mathbb{Z}$ as follows:*

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

This loop is a Bruck loop.

Proof. The proof is a straightforward calculation only. In the beginning of the section we explained how to associate a Bruck loop to an odd order commutative

A-loop. Here we compute the operation $\circ$ associated to the operation $\cdot$ given in Proposition 22. We see immediately that $(a,i)^{-1} = (-a,-i)$ and $(a,i)/(b,j) = \left(a \cdot \frac{2(\zeta^i+1)}{(\zeta^{i-j}+1)(\zeta^j+1)} - b, i-j\right)$. The element $(a,i)^{\frac{1}{2}}$ is the only element (b,j) such that $(b,j)^2 = (a,i)$. It is again easy to check $(a,i)^{\frac{1}{2}} = \left(a \cdot \frac{\zeta^i+1}{(\zeta^{\frac{i}{2}}+1)^2}, \frac{i}{2}\right)$. Hence we can compute $(a,i) \circ (b,j) = \big(((a,i)\cdot(b,j)^2)/(-a,-i)\big)^{\frac{1}{2}}$ which gives eventually the expression from the theorem. □

Some Bruck loops of order kp were presented in [10]. It is not difficult to show that the Bruck loops constructed there are the same as the loops given in Theorem 28 for $R = \mathbb{F}_p$. However, our construction is explicit while the construction in [10] needed some recursive sequences to be found first.

In fact, these Bruck loops are the only known Bruck loops of order kp. It is conjectured that there exist no more such Bruck loops than these. One possible way to prove it is using the correspondence between commutative A-loops and Bruck loops together with Conjecture 27. But we still do not know whether this correspondence is a bijection.

Open Question. *The mapping $(Q,\cdot) \mapsto (Q,\circ)$ is a mapping from the set of all commutative A-loops of odd order to the set of all Bruck loops of odd order. Is this mapping injective or surjective?*

References

[1] R. H. Bruck: *A survey of binary systems*, 3rd corrected printing, Ergebnisse der Mathematik und Ihrer Grenzgebiete, new series, volume **20**, Springer-Verlag (1971).

[2] R. H. Bruck, L. J. Paige: *Loops whose inner mappings are automorphisms*, Ann. of Math. (2) **63** (1956), 308–323.

[3] H. Cohen: *A Course in Computational Algebraic Number Theory*, 4th corrected printing, GTM **138**, Springer-Verlag (2000).

[4] H. Cohen: *Advanced Topics in Computational Algebraic Number Theory*, GTM **193**, Springer-Verlag (1999).

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

[6] P. Jedlička, M. Kinyon, P. Vojtěchovský: *Structure of commutative automorphic loops*, preprint (2009).

[7] P. Jedlička, M. Kinyon, P. Vojtěchovský: *Constructions of commutative automorphic loops*, preprint (2009).

[8] M. Kinyon, K. Kunen, J. D. Philips: *Every diassociative A-loop is Moufang*, Proc. Amer. Math. Soc **130** (2002) 619–624.

[9] G. Nagy, P. Vojtěchovský: *LOOPS: Computing with quasigroups and loops*, version 2.1.0, package for GAP, `http://www.math.du.edu/loops` .

[10] H. Niederreiter, K. H. Robinson: *Bol loops of order pq*, Math. Proc. Cambridge Philos. Soc., **89** (1981), 241–256.

[11] B. L. Sharma: *Bol loops of order pq with $q \mid (p^2-1)$*, Bolletino della Unione matematica italiana **1**,2 (1987), 163–169.

Department of Mathematics, Faculty of Engineering, Czech University of Life Sciences, Kamýcká 129, 165 21, Prague 6 – Suchdol, Czech Republic

E-mail address: `jedlickap@tf.czu.cz`

Université de Caen, LMNO - UMR 6139, Campus II - Boulevard Maréchal Juin, BP 5186, 14032 Caen Cedex, France

E-mail address: `denis.simon@math.unicaen.fr`