A NICE CONSTRUCTION OF THE QUADRATIC CLOSURE OF $F(2)$

CHRISTOPHE RAFFALLI

GAATI, University of French Polynesia

Abstract. We give an explicit representation of the quadratic closure of $F(2)$, the field with 2 elements. This representation enjoys nice recursive definitions for all operations, which we hope have a practical interest. We also establish nice algebraic properties of the construction.

1. Introduction

We give a construction of the quadratic closure of $F(2)$ by a sequence of splitting field of degree 2. The point is that we can choose a simple sequence of polynomials that are always irreducible (see definition 2).

We proceed by defining two sequences of elements $(\rho_k)_{k\in\mathbb{N}^*}$ and $(\mu_k)_{k\in\mathbb{N}}$ with $\rho_k, \mu_k \in F(2^{2^k})$, ρ_k being one of the root of $x^2+x+\mu_k$. We have some precise information about these elements and their construction which can be summarised in figure 1.

We obtain nice recursive definitions of all operations including square root and solutions of $x^2+x+a=0$. However, this operation are efficient asymptotically, but not as efficient as the best available implementations. We think the main reason is because we did not find a way to use the instruction for multiplication without carry available on modern processors that allow very fast polynomial and matrix multiplication in characteristic 2.

Nevertheless we think we gain some geometrical knowledge of the quadratic closure of $F(2)$ that may have some applications...

2. Construction

Notation 1. *For $k\in\mathbb{N}$, we denote by $\mathbb{K}_k$ the field $F(2^{2^k})$ and $\mathbb{K}=\bigcup_{k\in\mathbb{N}}\mathbb{K}_k$ the quadratic closure*[1] *of $\mathbb{K}_0=F(2)$.*

Definition 2. *We define by induction $\mu_k\in\mathbb{K}_k$ for $k\geq 0$, $T_k\in\mathbb{K}_k[X]$ for $k\geq 0$ and $\rho_k,\overline{\rho}_k\in\mathbb{K}_k$ for $k\geq 1$.*

- *$\mu_0=1\in\mathbb{K}_0$ and*
- *for $k\geq 0$: $T_k=X^2+X+\mu_k\in\mathbb{K}_k[X]$.*

E-mail address: christophe@raffalli.eu, christophe.raffalli@upf.pf.

[1] In general, quadraticaly closed means that all elements have square roots. In characteristic 2, quadraticaly closed means that all polynomials of degree 2 have roots. Indeed, the existence of square roots is always true and therefore not sufficient.

FIGURE 1. Diagram for the quadratic closure of $F(2)$

- *For $k > 0$, $\rho_k \in \mathbb{K}_k$ is one of the root of the polynomial T_{k-1},*
- *$\overline{\rho}_k = 1 + \rho_k$ the other root of T_{k-1} and*
- *$\mu_k = \rho_k^{-1} + 1 \in \mathbb{K}_k$.*

We first prove the following facts for $k > 0$:

Fact 3.

(1) $\rho_k \overline{\rho}_k = \mu_{k-1}$
(2) $\rho_k \mu_k = \overline{\rho}_k$ *which is equivalent to* $\rho_k \overline{\rho}_k^{-1} = \mu_k^{-1}$.
(3) $\rho_k^2 = \mu_k^{-1}\mu_{k-1}$ *and* $\overline{\rho}_k^2 = \mu_k \mu_{k-1}$
(4) $\mu_k^{-1} = \rho_k^2 \mu_{k-1}^{-1} = \mu_{k-1}^{-1}\rho_k + 1$ *and* $\mu_k = \overline{\rho}_k^2 \mu_{k-1}^{-1} = \mu_{k-1}^{-1}\overline{\rho}_k + 1$
(5) The polynomial T_k is irreducible in $\mathbb{K}_k$.
(6) $\rho_k, \overline{\rho}_k, \mu_k \in \mathbb{K}_k \setminus \mathbb{K}_{k-1}$.

Proof.

(1) Because ρ_k and $\overline{\rho}_k$ are the two roots of T_{k-1}.
(2) By definition of μ_k, $\rho_k \mu_k = 1 + \rho_k = \overline{\rho}_k$.
(3) Multiplying the equation $\rho_k \overline{\rho}_k = \mu_{k-1}$ and $\rho_k \overline{\rho}_k^{-1} = \mu_k^{-1}$ gives $\rho_k^2 = \mu_k^{-1}\mu_{k-1}$ and multiplying the first by the inverse of the second yields $\overline{\rho}_k^2 = \mu_k \mu_{k-1}$.
(4) Immediate from the previous item and the fact that ρ_k and $\overline{\rho}_k$ are the roots of T_{k-1} and therefore satisfies $\rho_k^2 = \rho_k + \mu_{k-1}$ and $\overline{\rho}_k^2 = \overline{\rho}_k + \mu_{k-1}$.
(5) We have

$$\begin{aligned}(a_1 + a_2\rho_k)\mu_k &= (a_1 + a_2\rho_k)(\mu_{k-1}^{-1}\overline{\rho}_k + 1)\\ &= a_1\mu_{k-1}^{-1}\overline{\rho}_k + a_1 + a_2\mu_{k-1}^{-1}\rho_k\overline{\rho}_k + a_2\rho_k\\ &= a_1\mu_{k-1}^{-1}\rho_k + a_1\mu_{k-1}^{-1} + a_1 + a_2 + a_2\rho_k\\ &= (\mu_{k-1}^{-1} + 1)a_1 + a_2 + (\mu_{k-1}^{-1}a_1 + a_2)\rho_k\end{aligned}$$

Therefore, the matrix of the multiplication by μ_k seen as an element of the $\mathbb{K}_{k-1}$ vector space and written in the basis $(1, \rho_k)$ is:

$$\begin{pmatrix}\mu_{k-1}^{-1} + 1 & 1\\ \mu_{k-1}^{-1} & 1\end{pmatrix}$$

This allows to relate the trace of μ_k and μ_{k-1}^{-1}:

$$Tr(\mu_k) = Tr(\mu_{k-1}^{-1})$$

Similarly,

$$\begin{aligned}(a_1 + a_2\rho_k)\mu_k^{-1} &= (a_1 + a_2\rho_k)(\mu_{k-1}^{-1}\rho_k + 1)\\ &= a_1 + a_1\rho_k\mu_{k-1}^{-1} + a_2\rho_k + a_2\rho_k^2\mu_{k-1}^{-1}\\ &= a_1 + a_1\rho_k\mu_{k-1}^{-1} + a_2\rho_k + a_2\rho_k\mu_{k-1}^{-1} + a_2\\ &= a_1 + a_2 + (\mu_{k-1}^{-1}a_1 + (\mu_{k-1}^{-1} + 1)a_2)\rho_k\end{aligned}$$

Therefore, the multiplication by μ_k^{-1} in the basis $(1, \rho_k)$ is:

$$\begin{pmatrix} 1 & 1 \\ \mu_{k-1}^{-1} & \mu_{k-1}^{-1} + 1 \end{pmatrix}$$

This gives:

$$Tr(\mu_k^{-1}) = Tr(\mu_{k-1}^{-1})$$

As we have $\mu_0 = 1$, This establishes that $Tr(\mu_k) = Tr(\mu_k^{-1}) = 1$ and therefore that T_k is irreducible.

(6) Immediate from the fact that T_k is irreducible. □

3. Complexity of the base algorithms

Notation 4. *For the implementation, we represent an element $a \in \mathbb{K}$ by a pair $(k, s(a))$ such that $a \in \mathbb{K}_k$ and $s(a)$ is a bit sequence of length 2^k, with the following rules*

- *If $k = 0$, then $s(a) = a \in \mathbb{K}_0 = \{0, 1\}$*
- *If $k > 0$, we can write $a = a_1 + a_2\rho_k$ and we impose $s(a) = s(a_1) \parallel s(a_2)$ where the symbol $\parallel$ represents the concatenation of bit sequences.*

We say that the representation is normal *if k is minimal.*

This representation allows to decompose an element a of $\mathbb{K}_{n+1}$ as $a_1 + a_2\rho_k$ in time $O(1)$ if we return a pointer within the bit sequence $s(a)$.

3.1. Addition ($O(2^k)$).

Addition is straightforward using xor as we have $a_1 + a_2\rho_k + b_1 + b_2\rho_k = (a_1 + a_2) + (b_1 + b_2)\rho_k$.

3.2. Multiplication by μ_k and μ_k^{-1}.

Corollary 5. *(of the proof of facts 3) From the matrices of μ_k and μ_k^{-1} above we derive the following formula to multiply by μ_k and μ_k^{-1} an element of $\mathbb{K}_k$ written in the basis $(1, \rho_k)$:*

$$\begin{aligned} (a_1 + a_2\rho_k)\mu_k^{-1} &= (a_1 + a_2) + ((a_1 + a_2)\mu_k^{-1} + a_2)\rho_k \\ (a_1 + a_2\rho_k)\mu_k &= a_1\mu_k^{-1} + a_1 + a_2 + (a_1\mu_k^{-1} + a_2)\rho_k \end{aligned}$$

This gives the following recursive algorithm for the multiplication by μ_k^{-1}:

Input: $l, k \in \mathbb{N}$, $a \in \mathbb{K}_l$
Output: $a\mu_k^{-1} \in \mathbb{K}_{\max(k,l)}$

- If $l < k$, return $(a + a\mu_{k-1}^{-1}) + a\mu_{k-1}^{-1}\rho_k$
- If $l > k$ and $a = a_1 + a_2\rho_l$, return $a_1\mu_k^{-1} + a_2\mu_k^{-1}\rho_l$
- If $l = k$ and $a = a_1 + a_2\rho_l$, return $(a_1 + a_2) + ((a_1 + a_2)\mu_{k-1}^{-1} + a_2)\rho_k$

Figure 2. Multiplication by μ_k^{-1}

This algorithm is correct from $\mu_k^{-1} = \overline{\rho}_k\mu_{k-1}^{-1} + 1$ in fact 3 and the equation for $(a_1 + a_2\rho_k)\mu_k^{-1}$ within the proof of the same fact.

For the multiplication by μ_k we get the following similar algorithm, using the previous one:

Input: $l, k \in \mathbb{N}$, $a \in \mathbb{K}_l$
Output: $a\mu_k \in \mathbb{K}_{\max(k,l)}$

- If $l < k$, return $(a + a\mu_{k-1}) + a\mu_{k-1}\rho_k$
- If $l > k$ and $a = a_1 + a_2\rho_l$, return $a\mu_k = a_1\mu_k + a_2\mu_k\rho_l$
- If $l = k$ and $a = a_1 + a_2\rho_l$, return $(a_1\mu_{k-1}^{-1} + a_1 + a_2) + (a_1\mu_{k-1}^{-1} + a_2)\rho_k$

FIGURE 3. Multiplication by μ_k

Fact 6. *The recursive algorithm for multiplication of $a \in \mathbb{K}_l$ by μ_k and μ_k^{-1} have a complexity $O(2^{\max(k,l)})$, which is linear in the size 2^l of the representation of a when $l > k$, which is the commonly used case for this algorithm.*

Proof. Indeed, if $l \leq k$, there is only one recursive call on a data which is half smaller, and this is linear in the size of the data. If $l > k$ we have two recursive calls, but we see that we only have to do 2^{l-k} multiplication of elements of $\mathbb{K}_k$ by μ_k^{-1}, giving a complexity of $O(2^{l-k}2^k) = O(2^l)$. □

3.3. **Multiplication.** We have

$$\begin{aligned}(a_1 + a_2\rho_k)(b_1 + b_2\rho_k) &= a_1b_1 + (a_1b_2 + a_2b_1)\rho_k + a_2b_2\rho_k^2 \\ &= a_1b_1 + a_2b_2\mu_{k-1} + (a_1b_2 + a_2b_1 + a_2b_2)\rho_k \\ &= a_1b_1 + a_2b_2\mu_{k-1} + ((a_1 + a_2)(b_1 + b_2) + a_1b_1)\rho_k\end{aligned}$$

Input: $k, l \in \mathbb{N}$, $a \in \mathbb{K}_k$ and $b \in \mathbb{K}_l$
Output: $ab \in \mathbb{K}_{\max k,l}$
If needed, we decompose $a = a_1 + a_2\rho_k$ and $b = b_1 + b_2\rho_l$

- If $l < k$, we return $ab_1 + ab_2\rho_k$
- If $l > k$, we return $a_1b + a_1b\rho_l$
- If $l = k$, we return $a_1b_1 + a_2b_2\mu_{k-1} + ((a_1 + a_2)(b_1 + b_2) + a_1b_1)\rho_k$

FIGURE 4. Multiplication algorithm

Fact 7. *The complexity our recursive algorithm for multiplication of $a \in \mathbb{K}_l$ by $b \in \mathbb{K}_k$ is $O(2^{\ln_2(3)\min(l,k)}2^{\max(l,k)-\min(l,k)})$.*

Proof. When $l = k$ there are 3 recursive calls on data that are half smaller and (recall that multiplication by μ_k and addition are linear). This leads to a Karatsuba like complexity.

When $l > k$ (resp. $k > l$), we have to do 2^{l-k} (resp. 2^{k-l}) multiplications in $\mathbb{K}_l$ (resp. $\mathbb{K}_k$). □

3.4. **Inverse.** For the inverse of $a_1 + a_2\rho_k$, we inverse the multiplication matrix

$$\begin{pmatrix} a_1 & a_2\mu_k \\ a_2 & a_1 + a_2 \end{pmatrix}^{-1} = (a_1(a_1 + a_2) + a_2^2\mu_k)^{-1} \begin{pmatrix} a_1 + a_2 & a_2\mu_k \\ a_2 & a_1 \end{pmatrix}$$

The first column of the inverse gives the inverse of $a_1 + a_2\rho_k$ and leads to the following algorithm:

Input: $k \in \mathbb{N}$, and $a \in \mathbb{K}_k$
Output: $a^{-1} \in \mathbb{K}_k$

- If $k = 0$, we return 1 if $a = 1$ otherwise produce an error.
- If $k > 0$, we decompose $a = a_1 + a_2\rho_k$, compute $\Delta = a_1(a_1 + a_2) + a_2^2\mu_k$ the determinant of the multiplication matrix (the norm of a) and return $\Delta^{-1}(a_1 + a_2 + a_2\rho_k)$

FIGURE 5. Algorithm for the inverse

As there is only one recursive call, the complexity is dominated by the 3 multiplications: $a_1(a_1 + a_2)$, $\Delta^{-1}(a_1 + a_2)$ and $\Delta^{-1}a_2$.

3.5. **Square and square root.** To compute the square and square root, we use

$$\begin{array}{rcl} (a_1 + a_2\rho_k)^2 & = & a_1^2 + a_2^2\rho_k^2 \\ & = & a_1^2 + a_2^2\mu_{k-1} + a_2^2\rho_k \\ \sqrt{a_1 + a_2\rho_k} & = & \sqrt{a_1 + a_2\mu_{k-1}} + \sqrt{a_2}\rho_k \text{by inverting the above} \end{array}$$

It is immediate to get recursive algorithm of complexity $O(k2^k)$ from these equations. We could hope for a linear $O(2^k)$ algorithm, which we could not obtain.

3.6. **Trace.** From the computation of subsection 3.3, we have that the multiplication by $a_1 + a_2\rho_k$ has the following matrix in the basis $(1, \rho_k)$:

$$\begin{pmatrix} a_1 & a_2\mu_k \\ a_2 & a_1 + a_2 \end{pmatrix}$$

Therefore, because traces are composable, we have $Tr(a_1 + a_2\rho_k) = Tr(a_1 + a_1 + a_2) = Tr(a_2)$. This ensures that the trace of $a \in \mathbb{K}_k$ (over F(2)) is the last (right most) bit of the representation of a. This is clearly $O(1)$.

If we want the trace of $a \in \mathbb{K}_k$ over $\mathbb{K}_l$, we only have to retain the 2^l rightmost bits of the representation of a over 2^k bits.

3.7. **Solving $X^2+X+a = 0$.** We know that in characteristic 2, any degree 2 equation can be reduced either to the computation of a square root or the resolution of $X^2+X+b_2 = 0$.

From the computation of the square, we know that

$$(a_1 + a_2\rho_k)^2 + a_1 + a_2\rho_k = a_1^2 + a_2^2\mu_{k-1} + a_1 + (a_2^2 + a_2)\rho_k$$

Input: $k \in \mathbb{N}$, and $a \in \mathbb{K}_k$
Output: $b \in \mathbb{K}_{k+1}$ such that $b^2 + b + a = 0$ (the other solution is $b + 1$).

- If $k = 0$, we return ρ_1 if $a = 1$ otherwise we return 0.
- If $k > 0$, we decompose $a = a_1 + a_2\rho_k$.
  - If $Tr(a_2) = 0$, we solve recursively $b_2^2 + b_2 + a_2 = 0$ and get two solutions b_2 and $b_2' = b_2 + 1$. We define $c = \mu_k(a_2 + b_2) + a_1$ and $c' = \mu_k(a_2 + b_2') + a_1 = c + \mu_k$. if $Tr(c) = 0$, we solve $b_1^2 + b_1 + c = 0$ and return $b_1 + b_2\rho_k$ otherwise, we solve $b_1^2 + b_1 + c' = 0$ and return $b_1 + b_2'\rho_k$.
  - If $Tr(a_2) = 1$, we solve $b_1^2 + b_2 + a + \mu_k = 0$ and return $b_1 + \rho_k$.

FIGURE 6. Algorithm solving $x^2 + x + a$

Hence, solving $X^2 + X + (b_1 + b_2\rho_k) = 0$ is equivalent to the system

$$\begin{cases} a_1^2 + a_2^2\mu_{k-1} + a_1 &= b_1 \\ a_2^2 + a_2 &= b_2 \end{cases}$$

Let us assume that $b_1, b_2 \in \mathbb{K}_{k-1}$ hence $b_1 + b_2\rho_k \in \mathbb{K}_k$.

If $Tr(b_2) = 0$, we search $a_1, a_2 \in \mathbb{K}_{k-1}$ and we find a_2 by a recursive call solving $a_2^2 + a_2 = b_2$. This leads to the equation $a_1^2 + a_1 = a_2^2\mu_{k-1} + b_1$ or $a_1^2 + a_1 = (a_2+1)^2\mu_{k-1} + b_1$. We can chose to solve the equation such that the trace of the second member is 0. We need to use $Tr(\mu_{k-1}) = 1$ to ensure that one of the two traces is 0.

If $Tr(b_2) = 1$, we take $a_2 = 1$ (which gives $a_2^2 + a_2 = 0$) and $a_1 \in \mathbb{K}_k$ and we solve $a_1^2 + a_1 = b_1 + b_2\rho_k + \mu_{k-1}$. We do have $Tr(b_1 + b_2\rho_k + \mu_{k-1}) = Tr(b_2) + Tr(\mu_{k-1}) = 0$ ensuring the existence of two solutions. This gives the algorithm of figure 6.

4. Other properties

Definition 8. *For $k > 0$, we define $\phi_k : \mathbb{K}_k \to \mathbb{K}_{k-1}$ as the square root of the norm (the determinant of the multiplication matrix, as seen in subsection 3.4):*

$$\phi_k(a + b\rho_k) = \sqrt{a(a + b) + b^2\mu_{k-1}}$$

Fact 9. *ϕ_k is a group morphism from $(\mathbb{K}_k^*, \times)$ to $(\mathbb{K}_{k-1}^\star, \times)$ which is the identity when restricted on $\mathbb{K}_{k-1}$.*

Proof. Immediate from the property of the determinant and square root. □

Fact 10. *We have $\phi_k(\mu_k) = \phi_k(\mu_k^{-1}) = 1$*

Proof. From 3 we have $\mu_k^{-1} = 1 + \mu_{k-1}^{-1}\rho_k$. Hence $\phi_k(\mu_k^{-1}) = 1 + \mu_{k-1}^{-1} + \mu_{k-1}^{-2}\mu_{k-1} = 1$. From this we get $\phi_k(\mu_k) = 1$ because ϕ_k is a group morphism. □

Lemma 11. *Let $k \in \mathbb{N}$, $\alpha \in \mathbb{K}_k$ with $Tr(\alpha) = 1$ and define $f_\alpha(x) = \alpha(1 + x)^{-1}$ and $g_\alpha : \{0, 1, 2, 3, ..., 2^{2^k} - 1\} \to \mathbb{K}_k$ by $g_\alpha(m) = f_\alpha^m(0)$. We show that g_α is a well defined bijection and $g_\alpha(2^{2^k} - 1) = 1$.*

We also have the extra property that $g_\alpha(2^{2^k}-1-m) = 1+g_\alpha(m)$ *for* $m \in \{0,1,2,3,...,2^{2^k}-1\}$.

Proof. Clearly, $f_\alpha(x)$ is defined for $x \neq 1$. For $x \neq 0$, $f_\alpha^{-1}(x) = 1+\alpha x^{-1}$. This means that the orbits of f_α are a sequence starting at 0 and ending at 1 plus some closed cycles. We just need to show that there are no cycle.

We define the sequence $a_{(n\in\mathbb{N})}$ by $a_0 = 1$, $a_1 = 0$ and for $n > 1$, $a_n = a_{n-1} + \alpha a_{n-2}$ and we show by induction that for $n \geq 0$,

$$f_\alpha^n(x) = \alpha\frac{a_n x + a_{n+1}}{a_{n+1}x + a_{n+2}}$$

- For $n = 0$, we have

$$f_\alpha^0(x) = x = \alpha\frac{x+0}{0x+\alpha} = \alpha\frac{a_0x+a_1}{a_1x+a_2}$$

- For $n > 0$, we have

$$\begin{aligned} f_\alpha^{n+1}(x) &= f_\alpha^n(f_\alpha(x)) \\ &= \alpha\frac{a_n\alpha(1+x)^{-1}+a_{n+1}}{a_{n+1}\alpha(1+x)^{-1}+a_{n+2}} \text{ by induction hyp.} \\ &= \alpha\frac{a_n\alpha+a_{n+1}(1+x)}{a_{n+1}\alpha+a_{n+2}(1+x)} \\ &= \alpha\frac{a_{n+1}x+a_{n+1}+a_n\alpha}{a_{n+2}x+a_{n+2}+a_{n+1}\alpha} \\ &= \alpha\frac{a_{n+1}x+a_{n+2}}{a_{n+2}x+a_{n+3}} \end{aligned}$$

Thus, for $n > 0$, we have

$$\begin{aligned} & f_\alpha^n(x) = x \\ \Leftrightarrow\ & \alpha\frac{a_nx+a_{n+1}}{a_{n+1}x+a_{n+2}} = x \\ \Leftrightarrow\ & \alpha a_nx+\alpha a_{n+1} = a_{n+1}x^2+a_{n+2}x \\ \Leftrightarrow\ & a_{n+1}x^2+(a_{n+2}+\alpha a_n)x+\alpha a_{n+1} = 0 \\ \Leftrightarrow\ & a_{n+1}x^2+a_{n+1}x+\alpha a_{n+1} = 0 \\ \Leftrightarrow\ & x^2+x+\alpha = 0 \text{ because } a_{n+1} \neq 0 \text{ if } n > 0 \end{aligned}$$

This equation does not have any solution in $\mathbb{K}_k$ as we assumed $Tr(\alpha) = 1$. This proves that there are no cycle.

For the extra property, it is true for $m = 0$. Assuming it hold for m, we have:

$$\begin{aligned} g_\alpha(m+1) &= f_\alpha(g_\alpha(m)) \\ &= \alpha(1+g_\alpha(m))^{-1} \\ &= \alpha g_\alpha(2^{2^k}-1-m)^{-1} \text{by induction hyp.} \\ &= 1+f_\alpha^{-1}(g_\alpha(2^{2^k}-1-m)) \end{aligned}$$

$$= \quad g_\alpha(2^{2^k} - 1 - m - 1) \tag{4.1}$$

□

Lemma 12. *We define* $\mathbb{O}_k = \{\beta \in \mathbb{K}_k, \phi_k(\beta) = 1\}$ *and define* $\sigma_k : \mathbb{K}_k \to \mathbb{K}_{k-1} \cup \{\infty\}$ *by* $\sigma_k(a_1 + a_2\rho_k) = a_1 a_2^{-1}$ *if* $a_2 \neq 0$ *and* $\sigma_k(a_1) = \infty$ *if* $a_1 \in \mathbb{K}_{k-1}$. *Remark that* $\mathbb{O}_k \cap \mathbb{K}_{k-1} = \{1\}$.

For $a, b \in \mathbb{K}_k \setminus \mathbb{K}_{k-1}$, *we have*

$$\sigma_k(ab) = \frac{\sigma_k(a)\sigma_k(b) + \mu_{k-1}}{1 + \sigma_k(a) + \sigma_k(b)}$$

We define a binary operation $\diamond$ *on* $\mathbb{K}_{k-1} \cup \{\infty\}$ *by:*

- ∞ *is neutral*
- $x \diamond y = \frac{xy + \mu_{k-1}}{x+y+1}$ *if* $x, y \in \mathbb{K}_{k-1}$ *and* $x + y + 1 \neq 0$
- $x \diamond y = \infty$ *if* $x + y + 1 = 0$

The above equation establishes that σ_k *is a abelian group morphism between* $(\mathbb{K}_k^*, \times)$ *and* $(\mathbb{K}_{k-1} \cup \{\infty\}, \diamond)$.

Moreover, σ_k *is an isomorphism when restricted to* $\mathbb{O}_k$.

Proof. Let $a = a_1 + a_2\rho_k \in \mathbb{K}_k \setminus \mathbb{K}_{k-1}$, $b = b_1 + b_2\rho_k \in \mathbb{K}_k \setminus \mathbb{K}_{k-1}$. First we assume that $ab \neq 1$ and compute:

$$\begin{aligned} ab &= a_1b_1 + a_2b_2\mu_{k-1} + (a_1b_2 + a_2b_1 + a_2b_2)\rho_k \\ \sigma_k(ab) &= \frac{a_1b_1 + a_2b_2\mu_{k-1}}{a_1b_2 + a_2b_1 + a_2b_2} \\ &= \frac{\sigma_k(a)\sigma_k(b) + \mu_{k-1}}{\sigma_k(a) + \sigma_k(b) + 1} \end{aligned}$$

If $ab = 1$, the we have $a_1b_2 + a_2b_1 + a_2b_2 = 0$ hence dividing by a_2b_2, we find $\sigma_k(a) + \sigma_k(b) + 1 = 0$ and we do have $\sigma_k(ab) = \infty = \sigma_k(a) \diamond \sigma_k(b)$.

This is enough to establish that σ_k is a abelian group morphism between $(\mathbb{K}_k^*, \times)$ and $(\mathbb{K}_{k-1} \cup \{\infty\}, \diamond)$.

We now show that it is an isomorphism when restricted to $\mathbb{O}_k$. Let $x \in \mathbb{K}_{k-1} \cup \{\infty\}$, for $a = a_1 + a_2\rho_k \in \mathbb{K}_k$, if $x \neq \infty$, we have

$$\begin{aligned} a \in \mathbb{O}_k \wedge \sigma_k(a) = x \quad &\Leftrightarrow \quad a_1(a_1 + a_2) + a_2^2\mu_{k-1} = 1 \wedge a_1a_2^{-1} = x \\ &\Leftrightarrow \quad x(x+1) + \mu_{k-1} = a_2^{-2} \wedge a_1 = xa_2 \\ &\Leftrightarrow \quad a_2^{-1} = \sqrt{x(x+1) + \mu_{k-1}} \wedge a_1 = xa_2 \end{aligned}$$

If $x = \infty$, we have $a \in \mathbb{O}_k \wedge \sigma_k(a) = \infty$ implies $a_2 = 0$ and $a_1 = 1$. This establishes that σ_k is a bijection by showing how to compute the unique antecedent of $x \in \mathbb{O}_k$. □

Corollary 13. *We define* $\alpha_k = \sqrt{\mu_k^{-1}}$. *For* $x \in \mathbb{K}_{k-1} \setminus \{1\}$, *we have* $\sigma_k(\alpha_k) \diamond x = \mu_{k-1}(1+x)^{-1} = f_{\mu_{k-1}}(x)$, $\sigma_k(\alpha_k) \diamond 1 = \infty$ *and* $\sigma_k(\alpha_k) \diamond \infty = \sigma_k(\alpha_k) = 0$.

Proof. From lemma 3, if $k > 0$, we have $\rho_k^2 = \mu_k^{-1}\mu_{k-1}$ hence $\mu_k^{-1} = \rho_k^2\mu_{k-1}^{-1}$ and therefore $\alpha_k = \rho_k\alpha_{k-1}$. We also have $\alpha_0 = 1$ from $\mu_0 = 1$. Hence $\sigma_k(\alpha_k) = 0$ and from the definition of $\diamond$, we get $\sigma_k(\alpha_k) \diamond x = \mu_{k-1}(1+x)^{-1} = f_{\mu_{k-1}}(x)$ if $x \neq 1$ and $\sigma_k(\alpha_k) \diamond 1 = \infty$. □

Lemma 14. *μ_k is of order $2^{2^{k-1}} + 1$.*

Proof. Corollary 13 and lemma 11 establishes that the operation $x \mapsto \sigma_k(\alpha_k) \diamond x$ has a unique cyclic orbit of length $2^{2^{k-1}} + 1$ in $\mathbb{K}_{k-1} \cup \{\infty\}$. As σ_k is a group morphism (lemma 12), this establishes that α_k is of order $2^{2^{k-1}} + 1$. As we are in characteristic 2 and every element has a unique square root, this shows that $\mu_k = \alpha_k^{-1}$ is of the same order. □

Corollary 15. *From the previous lemmas, we deduce that*

$$\mathbb{K}_k^* \simeq \mathbb{K}_{k-1}^* \times (\mathbb{K}_{k-1} \cup \infty) \simeq \mathbb{K}_{k-1}^* \times \mathbb{Z}/(2^{2^{k-1}} + 1)\mathbb{Z}.$$

The first isomorphism is given by $x \mapsto (\phi_k(x), \sigma_k(x\phi_k^{-1}(x)))$ and the second by $x \mapsto (\phi_k(x), \log_{\mu_k}(x\phi_k^{-1}(x)))$.

Proof. The isomorphism $\mathbb{K}_k^* \simeq \mathbb{K}_{k-1}^* \times (\mathbb{K}_{k-1} \cup \infty)$ is given by $x \mapsto (\phi_k(x), \sigma_k(x\phi_k^{-1}(x)))$. Indeed, $x \mapsto (\phi_k(x), x\phi_k^{-1}(x))$ is an isomorphism $\mathbb{K}_k^* \simeq \mathbb{K}_{k-1}^* \times \mathbb{O}_k$ and we conclude use lemma 12.

For the second isomorphism $\mathbb{K}_k^* \simeq \mathbb{K}_{k-1}^* \times \mathbb{Z}/(2^{2^{k-1}} + 1)\mathbb{Z}$, we remark that $\mu_k^n \in \mathbb{O}_k$ by fact 10 and the order of μ_k being the cardinal of $\mathbb{O}_k$, we can conclude. The isomorphism is therefore $x \mapsto (\phi_k(x), \log_{\mu_k}(x\phi_k^{-1}(x)))$. □