

# EXTENSIONS OF SPECIAL 3-FIELDS

STEVEN DUPLIJ AND WEND WERNER

ABSTRACT. We investigate finite field extensions of the unital 3-field, consisting of the unit element alone, and find considerable differences to classical field theory. Furthermore, the structure of their automorphism groups is clarified and the respective subfields are determined. In an attempt to better understand the structure of 3-fields that show up here we look at ways in which new unital 3-fields can be obtained from known ones in terms of product structures, one of them the Cartesian product which has no analogue for binary fields.

## 1. INTRODUCTION

Algebraic structure which is based on composing more than two elements can be traced back to early work of Dörnte [8] and Post [18] and has later shown an increase in interest, see for instance [3, 4, 5, 6, 9, 11, 12, 15, 16], and especially in physical model building [1, 2, 7, 17, 13, 14]. On many occasions, such a theory substantially profit from embedding objects into a larger structure in which such seemingly unconventional algebraic structure can be reduced to more conventional concepts. For a typical example see the brief discussion of ternary commutative groups in [10].

In cases where multiple algebraic operations of this kind are present (for example, the 3-fields investigated here) such an approach, however, is less successful, and the theory requires rather novel techniques. Our principal definition in the following is

**Definition 1.1.** A set  $R$  equipped with two operations  $R^3 \rightarrow R$ , called *ternary addition* and *ternary multiplication*, is called a *3-ring*, iff for each  $r, r_{1,2,3}, s_{1,2} \in R$

- (1) there are additive and, respectively, multiplicative *querelements*  $\bar{r} \in R$  and  $\hat{r}$  so that  $r \hat{+} \bar{r} \hat{+} r_1 = r_1$  as well as  $r \hat{r} r_1 = r_1$ ,
- (2)  $s_1 s_2 (r_1 \hat{+} r_2 \hat{+} r_3) = s_1 s_2 r_1 \hat{+} s_1 s_2 r_2 \hat{+} s_1 s_2 r_3$ , and
- (3) both operations are associative (i.e. no brackets are needed for multiple applications of these operations)

$R$  is called *commutative*, if the order of factors and summands can be permuted in any possible way, and *unital* iff there is an element  $1 \in R$  with  $1r = r$  for all  $r \in R$ .

A (unital) *3-field*  $K$  is a (unital) 3-ring iff for each  $k \in K$  there is  $\hat{k} \in K$  so that  $k \hat{k} k_1 = k_1$  for all  $k_1 \in K$ .

In a 3-ring (or, more generally, in a commutative 3-group), the presence of a multiplicative unit alone allows to introduce a binary product of commutative groups

$$x \cdot y = x1y, \tag{1.1}$$

which has the property that applying it twice on three factors results in the original ternary product. Similarly, for a 3-ring  $R$ , a zero element  $0$  is defined by requiring that

$$0xy = x0y = xy0 = 0 \quad \text{for all } x, y \in R. \tag{1.2}$$

Such an element is uniquely determined and as in the case of a 1-element for the multiplication, it allows for reducing ternary addition of  $R$  to a binary one.

The fields we will investigate in the following will come equipped with a ternary addition (and no zero element), and a multiplication that possesses a unit so that, right from the outset, we will assume multiplication to be binary. We then have

**Theorem 1.2** ([10] Theorems 3.4, 6.1). *A unital 3-field  $F$  embeds into a binary field  $K$  (with its inherited ternary addition and binary multiplication) if for each  $y \in F \setminus \{1\}$  the equation*

$$x + y - xy = 1 \tag{1.3}$$

*has the only solution  $x = 1$ . Whenever  $F$  is finite this happens if and only iff  $F = \{1\}$ .*

Let us explain some of the basic features of the theory that will be used in the following (details are in [10]).

To each unital 3-field  $F$  belongs a uniquely determined (binary) local ring  $\mathcal{U}(F)$  into which it embeds as the subset  $\mathcal{U}(F)^*$  of units in such a way that the ternary sum of  $F$  coincides with the binary sum of  $\mathcal{U}(F)$  applied twice. (And, conversely, the units of any local ring  $\mathcal{U}$  with residual field  $\mathbb{F}_2$  form a unital 3-field, with its inherited structure.) We have  $\mathcal{U}(F) = \mathcal{Q}(F) \cup F$ , where the binary non-unital ring  $\mathcal{Q}(F)$  consists of all mappings (pairs)  $q_{a,b} : f \mapsto f \hat{+} a \hat{+} b$ ,  $a, b \in F$ , with addition and multiplication coming from pointwise operations on the set of mappings  $F \rightarrow F$ . We will frequently make use of the fact that each  $q \in \mathcal{Q}(F)$  has a unique representation in the form  $q = q_{1,f}$ ,  $f \in F$ . As we will consider every unital 3-field  $F$  to be naturally embedded into the binary ring  $\mathcal{U}(F)$  so that the querelement  $\bar{f}$  from  $F$  becomes  $-f$ .

*Remark 1.3.* It is for this reason that we no longer will formally distinguish between the binary and ternary sums and write  $+$  throughout.

Any ternary morphism  $\phi : F_1 \rightarrow F_2$  canonically extends to a binary morphism  $\mathcal{Q}(\phi) : \mathcal{Q}(F_1) \rightarrow \mathcal{Q}(F_2)$  (and hence to a binary morphism  $\mathcal{U}(\phi) : \mathcal{U}(F_1) \rightarrow \mathcal{U}(F_2)$ ) via  $\phi(q_{a,b}) = q_{\phi(a),\phi(b)}$ . The kernel of  $\mathcal{Q}(\phi)$  is a binary ideal in  $\mathcal{U}(F_1)$ , and we will address these binary ideals of  $\mathcal{U}(F_1)$  as *the (ternary) ideals of  $F_1$* . We also will formally write a short exact sequence of unital 3-fields as

$$0 \longrightarrow J \longrightarrow F \longrightarrow F_0 \longrightarrow 0, \tag{1.4}$$

with the understanding that we actually are dealing with unital 3-fields  $F_1, F$  and  $F_0$ , a short exact sequence of binary rings,

$$0 \longrightarrow \mathcal{U}(F_1) \longrightarrow \mathcal{U}(F) \longrightarrow \mathcal{U}(F_0) \longrightarrow 0, \tag{1.5}$$

and the ideal  $J \subseteq \mathcal{Q}(F_1)$  arising as the kernel of the second arrow.

Using analogous definitions for unital 3-rings, the quotient of a unital 3-ring by an ideal  $J$  of  $\mathcal{U}(R)$  is a unital 3-field iff for any proper ideal  $J_0$  of  $\mathcal{U}(R)$  for which  $J \subseteq J_0$  it follows that  $J_0 \cap R = \emptyset$ . Note that this condition is automatically satisfied when  $R$  already is a 3-field.

The basic examples are the prime fields  $\text{TF}(n) = \{2k - 1 \mid k = 1, \dots, 2^{n-1}\} \subseteq \mathbb{Z}/2^n$  and  $\text{TF}(\infty)$ , the ternary field of quotients of the unital 3-ring  $2\mathbb{Z} + 1$ . As unital 3-fields, they are generated by the element 1. Since the unit of each unital 3-field  $F$  generates a uniquely determined prime field  $P_n$  inside  $F$ , the number of elements in this subfield, the characteristic  $\chi(F) = 2^{n-1}$  of  $F$ , is well-defined.

Extensions of 3-fields are a much more complicated subject than its binary counterpart. The present investigation is a first attempt at a deeper understanding. The next section

deals with products which exist thanks to the absence of a zero element. In some cases, they provide 3-field extensions. The final section is devoted to 3-field extensions of  $\{1\}$ , which are numerous and follow only in some cases the paths of Galois theory.

## 2. PRODUCTS OF 3-FIELDS

**2.1. Cartesian Products.** Since unital 3-fields are supposed to be proper, for each pair of unital 3-fields  $F_{1,2}$ , all elements of the Cartesian product  $F_1 \times F_2$  possess a multiplicative inverse so that  $F_1 \times F_2$  is itself a unital 3-field, under pointwise operations. For the same reason, however, there is no canonical embedding of one of these fields into  $F_1 \times F_2$ . (There is an exception in characteristic 1, though: In this case

$$\iota_1 : F_1 \rightarrow F_1 \times F_2, \quad \iota_1(f) = (f, 1_2) \quad (2.1)$$

is an embedding with  $\pi_1 \iota_1 = \text{Id}_{F_1}$ .)

**Theorem 2.1.** *Let  $F$  be a unital 3-field. Then the following are equivalent:*

- (1)  $F$  is the Cartesian product of two 3-fields  $F_{1,2}$ .
- (2) There are  $Q_{1,2} \subseteq Q(F)$  so that as a binary ring,  $Q(F) = Q_1 \oplus Q_2$ .

*Proof.* If  $F = F_1 \times F_2$  then  $q_{(a_1, a_2), (b_1, b_2)} \in Q(F_1 \times F_2)$  acts by  $q_{(a_1, a_2), (b_1, b_2)}(f_1, f_2) = (a_1 + b_1 + f_1, a_2 + b_2 + f_2)$  establishing the binary ring isomorphism

$$Z : Q(F_1 \times F_2) \rightarrow Q(F_1) \oplus Q(F_2), \quad q_{(a_1, a_2), (b_1, b_2)} \mapsto (q_{a_1, b_1}, q_{a_2, b_2}). \quad (2.2)$$

Assuming  $Q(F) = Q_1 \oplus Q_2$  as rings, both  $Q_i$  are ideals of  $Q(F)$  and hence yield 3-fields  $F_i = F/Q_i$  with corresponding quotient maps  $\pi_i$ . Then  $\pi(f) = (\pi_1(f), \pi_2(f))$  defines an injective morphism  $F \rightarrow F_1 \times F_2$  of 3-fields. Because  $\pi_1^{-1}(f_1) = f_1^0 + Q_1$  for some  $f_1^0 \in F$  and  $\pi_2(f_1^0 + Q_1) = F_2$ ,  $\pi$  is surjective.  $\square$

The above result and its proof can easily be extended to infinite products  $\prod_{i \in I} F_i$  of 3-fields, and this is the product in the categorical sense: Whenever, for a 3-field  $G$ , there are morphisms  $\psi_i : G \rightarrow F_i$  there is a unique mapping  $\psi : G \rightarrow \prod_{i \in I} F_i$  which can be shown to be a 3-field morphism.

Note also that  $Q(F) = Q(F_1) \oplus Q(F_2)$  is not related to a similar decomposition of  $\mathcal{U}(F)$ , since

$$[Q(F_1) \oplus Q(F_2)] \cup [F_1 \times F_2] \neq [Q(F_1) \cup F_1] \oplus [Q(F_2) \cup F_2] \quad (2.3)$$

Observe that modifying a construction from [10] in order to create direct sums is futile: Letting, for an odd number of finite 3 fields  $F_1, \dots, F_n$  (odd, in order to have a unit and, possibly, invertibility),

$$\bigoplus_{i=1}^n F_i = \left\{ (f_i) \in \bigoplus_{i=1}^n \mathcal{U}(F_i) \mid \sum_{i=1}^n \partial(f_i) = 1 \right\} \quad (2.4)$$

where  $\partial : \mathcal{U}(F) \rightarrow \mathbb{F}_2$  denotes the natural grading for the unital 3-field  $F$ , it turns out that  $(f_i)$  possesses an inverse iff  $(f_i)^N = (1, \dots, 1)$  and it follows that the set of invertible elements within  $\bigoplus_{i=1}^n F_i$  equals  $\times_{i=1}^n F_i$ .

**2.2. Semi-direct Products and Unitization of Algebras.** We will base the notion of a semi-direct products of 3-fields on the concept of a split short exact sequence of unital 3-fields  $0 \rightarrow J \rightarrow F \rightarrow G \rightarrow 0$ .

**Definition 2.2.** The unital 3-field  $F$  is the (*internal*) *semi-direct* product of the ideal  $J \subseteq \mathcal{Q}(F)$  and the subfield  $G$  iff  $G$  is the image of an epimorphism  $\pi : F \rightarrow G$  with  $\text{Ker } \pi = J$  and right inverse  $\iota : G \rightarrow F$ .

More abstractly, semi-direct products are connected to algebras over 3-fields. Recall [10]

**Definition 2.3.** Let  $A$  be a binary ring and  $F$  a unital 3-field. We call  $A$  a binary algebra over  $F$ , iff  $F$  acts on  $A$  in such a way that, for all  $f, f_{1,2,3} \in F$  and  $a, a_{1,2} \in A$ ,

- (1)  $f(a_1 + a_2) = fa_1 + fa_2$
- (2)  $(f_1 + f_2 + f_3)a = f_1a + f_2a + f_3a$
- (3)  $(f_1f_2)a = f_1(f_2a)$
- (4)  $1_F a = a$

Similarly, we will call  $A$  a 3-algebra over  $F$  iff  $A$  is a 3-ring (with addition coming from an underlying commutative 3-group) equipped with a binary product so that, for all  $f, f_{1,2,3} \in F$  and  $a, a_{1,2} \in A$ ,

$$f(a_1 + a_2 + a_3) = fa_1 + fa_2 + fa_3 \quad (2.5)$$

while axioms (2)-(4) for a binary algebra are left untouched.

Note that we do not assume  $A$  to be unital.

*Example 2.4.*  $\mathcal{Q}(F)$  is an  $F$ -algebra where the action of  $F$  is given by  $f_1q_{1,f} = q_{f_1,f_1f}$ , whenever  $q_{1,f} \in \mathcal{Q}(F)$  and  $f_1 \in F$ .

*Example 2.5.* More generally, if the morphism of unital 3-fields  $\pi : F \rightarrow G$  possesses the right inverse  $\sigma : G \rightarrow F$ , the ideal  $J = \text{Ker } \mathcal{Q}(\pi)$  is a  $G$ -algebra with  $G$ -action  $g.j = \sigma(g)j$ .

We will also need the fact that a binary  $F$ -algebra  $A$  becomes a binary module over the local ring  $\mathcal{U}(F)$  by letting

$$q_{1,f}a = a + fa, \quad f \in F, \quad a \in A. \quad (2.6)$$

In case  $A$  is a 3-algebra,  $\mathcal{Q}(F)$  can only act on  $\mathcal{Q}(A)$  via

$$q_{1,f}q_{a,b} = q_{a,b+fa+fb}. \quad (2.7)$$

Semi-direct products for unital 3-fields will be related to the unitization of an algebra over a unital 3-field. There are two variants, one with purely binary operations, and another one for which addition becomes ternary.

**Definition 2.6.** Let  $A$  be an algebra over the unital 3-field  $F$ . Then the *binary unitization* of  $A$  is defined on the additive direct sum

$$A_F^{++} = \mathcal{U}(F) \oplus A \quad (2.8)$$

with multiplication

$$(u_1, a_1)(u_2, a_2) = (u_1u_2, u_1a_2 + u_2a_1 + a_1a_2). \quad (2.9)$$

*Ternary unitization* is based on the additively written commutative 3-group  $A_F^+ = F \oplus A$  and a binary product which is equal to the one in the binary case.

It is straightforward to check that  $A_F^{++}$  is a binary unital ring, and  $A_F^+$  is a unital 3-ring.

**Theorem 2.7.** *The unitization  $A^+$  of a nilpotent algebra  $A$  over the unital 3-field  $F$  is a unital 3-field, and it follows that  $A^+$  is a semi-direct product with canonical quotient map  $A^+ \rightarrow F$  and natural split  $F \rightarrow F \oplus 0$ .*

*Proof.* Since  $A^+$  always is a unital 3-ring we still have to show that each element  $(f, a)$  has an inverse. But, due to nilpotency of  $A$ ,

$$(1, a)^{-1} = \left( 1, \sum_{\nu=1}^N (-1)^\nu a^\nu \right) \quad (2.10)$$

for  $N$  large enough, and hence  $(f, a)^{-1} = f^{-1}(1, f^{-1}a)^{-1}$ .  $\square$

**Corollary 2.8.** *For a finite unital 3-field  $F_0$  a subfield  $F$  of  $F_0$ , and an ideal  $J \subseteq \mathcal{Q}(F_0)$  equipped with the natural action of  $F$ ,  $A_F^+$  is a unital 3-field.*

There are infinite unital 3-fields  $F$  for which  $\mathcal{Q}(F)$  is not nilpotent so in order to find 3-fields among unitizations we need to define invertibility before unitization.

**Definition 2.9.** An algebra  $A$  over a unital 3-field  $F$  is called a  $\mathcal{Q}$ -algebra iff for each  $a \in A$  there is  $a^\# \in A$  such that  $aa^\# = a + a^\#$ .

*Example 2.10.* The simplest example is an algebra  $A$  over the 3-field  $\text{TF}(0) = \{1\}$ . Equivalently,  $A$  is a binary ring such that  $a + a = 0$  for all  $a \in A$  and, at the same time, a (binary) algebra over  $\text{GF}(2)$ . If also  $a^2 = 0$  for all  $a \in A$ ,  $A_{\text{TF}(0)}^+$  is a unital 3-field in which  $(1, a)^{-1} = (1, a)$  for all  $a \in A$ . If the product of  $A$  vanishes identically and if we select a basis  $B$  for the vector space  $A$ , we find

$$A_{\text{TF}(0)}^+ \cong \text{TF}(1)^{|B|} \quad (2.11)$$

This example also covers the case in which  $F$  acts trivially on  $A$ , i.e.  $fa = a$ , for all  $f \in F$ ,  $a \in A$ .

*Example 2.11.* Each nilpotent algebra  $A$  over the unital 3-field  $F$  is a  $\mathcal{Q}$ -algebra with

$$a^\# = - \sum_{\nu=1}^N a^\nu, \quad (2.12)$$

where  $a^{N+1} = 0$ .

**Lemma 2.12.** *An algebra  $A$  over a unital 3-field  $F$  is a  $\mathcal{Q}$ -algebra if and only if  $A_F^+$  is a unital 3-field.*

*Proof.* Suppose  $A$  is a  $\mathcal{Q}$ -algebra. We must prove that each element is invertible, and, as in the proof of Theorem 2.7, it suffices to show  $(1, q)^{-1}$  exists. But it follows from the definition of  $q^\#$  that  $(1, q)(1, q^\#) = (1, 0)$ .

Conversely, if  $(1, q)$  has inverse  $(f, \bar{q})$  it follows that  $f = 1$  and  $q + \bar{q} + q\bar{q} = 0$  so that  $\bar{q}$  provides the  $\#$ -element, providing  $A$  with the structure of a  $\mathcal{Q}$ -algebra.  $\square$

**Theorem 2.13.** *Let  $F$  be a unital 3-field. There exists a bijective correspondence between the unitization of  $\mathcal{Q}$ -algebras  $A$  over  $F$  and semi-direct products of 3-fields  $J \rtimes F$ :*

- (1) *For each  $\mathcal{Q}$ -algebra  $A$  over  $F$ , the mapping  $\pi_{A,F} : A_F^+ \rightarrow F$ ,  $(f, a) \mapsto f$  establishes the short exact sequence of unital 3-fields*

$$0 \longrightarrow A \longrightarrow A_F^+ \longrightarrow F \longrightarrow 0 \quad (2.13)$$

*which is split by  $\sigma_{A,F} : f \mapsto (f, 0)$  and so,  $A_F^+ = A \rtimes F$ .*

(2) Conversely, each split exact sequence  $0 \rightarrow J \rightarrow F_0 \rightarrow F \rightarrow 0$  naturally defines the structure of a  $\mathcal{Q}$ -algebra over  $F$  on  $J$  and it follows that  $F_0 = J \rtimes F$  is isomorphic to  $J_F^+$ .

*Proof.* By the definition of  $A_F^+$  and Lemma 2.12,  $\pi_{A,F}$  and  $\sigma_{A,F}$  are morphisms of unital 3-fields giving rise to the split exact sequence  $0 \rightarrow A \rightarrow A_F^+ \rightarrow F \rightarrow 0$ .

In order to prove the second statement, denote by  $\sigma : F \rightarrow F_0$  the right inverse to the quotient morphism  $\pi : F_0 \rightarrow F$ . Example 2.5 shows  $J$  is a  $\mathcal{Q}$ -algebra over  $F$ , and the mapping

$$J_F^+ \longrightarrow F_0, \quad (f, q) \longmapsto \sigma(f) + q \quad (2.14)$$

is an isomorphism of unital 3-fields.  $\square$

*Example 2.14.* Let  $F$  be a subfield of  $F_0$  and  $J$  an ideal of  $\mathcal{U}(F_0)$ . For each  $q = q_{1,f} \in J$ ,  $q^\# = q_{1,f^{-1}}$  is in  $J$  since  $q^\# = -qq^\# - q$ . It follows that  $J$  is a  $\mathcal{Q}$ -algebra over  $F$  and so  $F \rtimes J$  is a unital 3-field.

*Example 2.15.* Let  $F_0$  be a unital 3-field with unital subfield  $F_1$  and let  $F = F_0 \times F_1$ . Then  $\mathcal{Q}(F) = \mathcal{Q}(F_0) \oplus \mathcal{Q}(F_1)$  and  $\pi_2(f_0, f_1) \rightarrow f_1$  is a surjective morphism with kernel

$$J = \{q = q_{(1,1),(g_0,g_1)} \in \mathcal{Q}(F) \mid 0 = \mathcal{Q}(\pi_2)(q) = q_{1,f_1}\} = \mathcal{Q}(F_0) \oplus \{0\} \quad (2.15)$$

$\pi_2$  has the left inverse  $\sigma : F_1 \rightarrow F$ ,  $\sigma(f_1) = (f_1, f_1)$  which produces an action of  $\text{diag } F_1 \times F_1 \cong F_1$  on  $J$  given by

$$(f_1, f_1)q_{1,f_0} = f_1q_{1,f_0} = q_{1,f_1+f_1f_0^{-1}} \quad (2.16)$$

$J$  is a  $\mathcal{Q}$ -algebra over  $F_1$  with  $q_{1,f_0}^\# = q_{1,f_0^{-1}}$ , and the morphism  $\Phi : J_{F_1}^+ \rightarrow F_0 \times F_1$ ,

$$\Phi(f_1 \oplus q_{1,f_0}) = (f_1, f_1 + q_{1,f_0}) = (f_1, 1 + f_0 + f_1) \quad (2.17)$$

is an isomorphism.

**2.3. Creating a 3-field action.** We complement the above with an intrinsic characterization of the binary rings  $\mathcal{Q}(F)$ , this time without using the action of a unital 3-field. First an observation: The ring structure of  $\mathcal{Q}(F)$  uniquely determines the underlying unital 3-field.

**Proposition 2.16.** *Fix a unital 3-field  $F_{1,2}$  are unital 3-fields and suppose  $\Psi : \mathcal{Q}(F_1) \rightarrow \mathcal{Q}(F_2)$  is a binary ring morphism. Define  $\Phi : F_1 \rightarrow F_2$  through  $\Psi(q_{1,f}) = q_{1,\Phi(f)}$ . Then  $\Phi$  is a unital 3-field morphism which is an automorphism whenever  $\Psi$  is.*

*Proof.* Using the involved definitions, one checks that  $\Phi$  respects addition and multiplication of  $F$ . Furthermore,  $0 = \Psi(q_{1,\bar{1}}) = q_{1,\overline{\Phi(1)}}$ , and so  $\Phi$  is unital. If  $\Psi$  is an automorphism and  $\Psi^{-1}(q_{1,a}) = q(1, \widehat{\Phi}(a))$  then, necessarily  $\widehat{\Phi} = \Phi^{-1}$ .  $\square$

**Definition 2.17.** A commutative (binary) ring  $Q$  is called a  $\mathcal{Q}$ -ring iff

- (1) There exists a 2-unit  $\tau \in Q$  so that  $\tau q = q + q$  for all  $q \in Q$ .
- (2) For each  $q \in Q$  exists a unique  $\#$ -element  $q^\# \in Q$  with  $q^\#q = q + q^\#$ .

The morphisms between  $\mathcal{Q}$ -rings are those ring morphisms that map the respective  $\tau$ -elements onto each other and respect the  $\#$ -involution.

We note some consequences of these axioms:

- (1) A  $\mathcal{Q}$ -ring is never unital, since we would have  $1^\# = 1 + 1^\#$  and so  $1 = 0$ .
- (2)  $\tau^\# = \tau$  and  $\tau^n = 2^{n-1}\tau$

- (3) There might be more than one 2-element: two such elements  $\tau_{1,2}$  have to satisfy  $(\tau_1 - \tau_2)x = 0$  for all  $x \in Q$ .
- (4) Similarly,  $q_{1,2}^\# \in Q$  are  $\#$ -elements for  $q \in Q$  iff  $(q_1^\# - q_2^\#)(q - 1) = 0$ , within the unitization of  $Q$ . As we will see below, this determines the element  $q^\#$  uniquely.

**Theorem 2.18.**  *$Q$  is a  $\mathcal{Q}$ -ring, iff there is a unital 3-field  $F$  such that  $Q = \mathcal{Q}(F)$ .*

*Proof.* Suppose  $Q = \mathcal{Q}(F)$ . Then, letting  $\tau = q_{1,1}$  and  $q_{1,f}^\# = q_{1,f^{-1}}$ , we have turned  $\mathcal{Q}(F)$  into a  $\mathcal{Q}$ -ring. Conversely, whenever  $F$  is a  $\mathcal{Q}$ -ring, define ternary addition  $\hat{+}$  as well as binary multiplication  $\hat{\times}$  by

$$f_1 \hat{+} f_2 \hat{+} f_3 = f_1 + f_2 + f_3 - \tau, \quad f \hat{\times} g = \tau - f - g + fg \quad (2.18)$$

Then the querelement of  $f \in F$  for  $\hat{+}$  is  $\bar{f} = \tau - f$ , the distributive law holds since

$$f \hat{\times} (f_1 \hat{+} f_2 \hat{+} f_3) = 2\tau - 3f - f_1 - f_2 - f_3 + ff_1 + ff_2 + ff_3 = f \hat{\times} f_1 \hat{+} f \hat{\times} f_2 \hat{+} f \hat{\times} f_3, \quad (2.19)$$

also  $\tau \hat{\times} f = \overline{\tau + f - \tau f} = \bar{\bar{f}} = f$ , and  $f^\# \hat{\times} f = \overline{f + f^\# - ff^\#} = \bar{0} = \tau$ .  $\square$

**Corollary 2.19.** *For a nilpotent ring  $Q$  there exists a unital 3-field  $F$  with  $Q = \mathcal{Q}(F)$  iff  $Q$  contains a 2-unit  $\tau$ .*

*Example 2.20.* In the simplest case, when the product on a binary ring  $R$  of characteristic 2 vanishes, each element  $\tau \in R$  can serve as a 2-element, while  $r^\# = -r$ . For the resulting unital 3-field  $F(R)_\tau$  we have

$$r \hat{+} s \hat{+} t = r + s + t + \tau \quad r \hat{\times} s = r + s + \tau, \quad (2.20)$$

and whatever the choice of  $\tau \in R$ , the mapping  $\Phi_\tau : r \mapsto r + \tau$  provides an isomorphism between  $F(R)_0$  and  $F(R)_\tau$ .

*Example 2.21.* The rings of pairs  $Q(n) = \{2k \in \mathbb{Z}/2^n \mid k = 0, \dots, 2^{n-1} - 1\}$  for the 3-fields  $TF(n) = \{2k - 1 \in \mathbb{Z}/2^n \mid k = 1, \dots, 2^{n-1}\}$  are  $\mathcal{Q}$ -rings, with  $\tau = 2$  and, taking the inverse inside  $\mathbb{Z}/2^n$ ,

$$q^\# = \frac{q}{q-1}. \quad (2.21)$$

Similarly,  $Q(\infty) = \{p/q \mid p = 2r, q = 2s + 1, r, s \in \mathbb{Z}\}$  is a  $\mathcal{Q}$ -ring with  $\tau = 2$  and

$$(p/q)^\# = \frac{p}{p-q}. \quad (2.22)$$

Note that in these examples,  $\tau$  is unique.

*Example 2.22.* If  $A$  is a  $\mathcal{Q}$ -algebra over the unital 3-field  $F$ , the ideal  $\mathcal{Q}(F) \oplus A$  of the binary unitization  $A_F^{++}$  is (still a  $\mathcal{Q}$ -algebra over  $F$  but also) a  $\mathcal{Q}$ -ring, with  $\tau = (q_{1,1}, 0)$ . The map

$$\Psi : \mathcal{Q}(A_F^+) \longrightarrow \mathcal{Q}(F) \oplus A, \quad q_{(1,0),(f,a)} \longmapsto (q_{1,f}, a), \quad (2.23)$$

establishes an isomorphism.

### 3. 3-FIELD EXTENSIONS OF $\{1\}$

It could be argued that an extension of a 3-field  $F_0$  should be any unital 3-field  $F$  arising in a short exact sequence

$$0 \longrightarrow J \longrightarrow F \longrightarrow F_0 \longrightarrow 0, \quad (3.1)$$

where  $J$  is (identified with) an ideal of  $\mathcal{U}(F)$ . In this case,  $F = F_0 \times F_1$  would qualify as an extension of  $F_0$ , and the projection onto  $F_0$  leads to the short exact sequence

$$0 \longrightarrow \mathcal{Q}(F_1) \times 0 \longrightarrow F_0 \times F_1 \longrightarrow F_0 \longrightarrow 0. \quad (3.2)$$

We will nonetheless follow the established notion and call the unital 3-field  $F$  an extension of the unital 3-field  $F_0$  in case  $F_0$  embeds into  $F$ .

In the present situation the structure of all subfields is more complex: Since  $\{1\}$  being a subfield of a unital 3-field  $F$  is equivalent to  $\chi(F) = 1$ , these extensions coincide with all unital 3-fields of characteristic 1. The extensions we will consider here belong to the following class.

**Definition 3.1.** Fix a unital 3-field  $F$  as well as natural numbers  $n_1, \dots, n_k \in \mathbb{N}$  and put

$$F(n_1, \dots, n_k) = \left\{ 1 + \sum_{0 \neq \alpha} \varepsilon_\alpha (x-1)^\alpha \mid \varepsilon_\alpha \in \mathbb{F}_2, (x-1)^{n_\kappa} = 0, \kappa = 1, \dots, k \right\}. \quad (3.3)$$

Note that by using semi-direct sums we may reduce the number of variables in this example: Consider the map  $x_i \mapsto 1$  and extend it to an epimorphism  $\pi_i$  on  $F(n_1, \dots, n_k)$ ,

$$1 + \sum_{0 \neq \alpha} \varepsilon_\alpha (x-1)^\alpha \mapsto 1 + \sum_{0 \neq \alpha, \alpha_i=0} \varepsilon_\alpha (x-1)^\alpha \quad (3.4)$$

with image  $F(n_1, \dots, n_{i-1}, n_{i+1}, \dots, n_k)$  and kernel consisting of the ideal

$$\mathfrak{J}_i = (x_i - 1) \sum_{\alpha} \varepsilon_\alpha (x-1)^\alpha. \quad (3.5)$$

The elements of  $F(n_1, \dots, n_{i-1}, n_{i+1}, \dots, n_k)$  embed naturally into  $F(n_1, \dots, n_k)$  and act on  $\mathfrak{J}_i$  by multiplication so that

$$F(n_1, \dots, n_k) = F(n_1, \dots, n_{i-1}, n_{i+1}, \dots, n_k) \ltimes \mathfrak{J}_i \quad (3.6)$$

A slightly more sophisticated way of writing down these 3-field extensions is obtained in the following way.

**Definition 3.2.** Fix a finite Abelian binary group  $G$  as well as a local (binary) ring  $R$  with residual field  $\mathbb{F}_2 = \{0, 1\}$ . Consider the group algebra  $RG$  over  $R$ . Then

$$F_G = \{ f \in RG \mid f(0) \in R^* \} \quad (3.7)$$

is called the *ternary group algebra of  $G$  over the 3-field  $R^*$* .

**Theorem 3.3.**  $F_G$  is a 3-field, extending  $R^*$ , and, in case  $R = \{0, \dots, 2^n - 1\} = \mathcal{U}(1, 3, \dots, 2^n - 1)$ , each finite unital field extensions of the unital 3-field  $\{1, 3, \dots, 2^n - 1\}$  which is contained in an extension generated by a single elements is isomorphic to one of these fields.



**3.1. Extensions of characteristic 0, generated by a single element.** We are going to consider extensions of  $F_0 = \text{TF}(0) = \{1\}$ , with prime field identical to  $\text{TF}(0)$ , and generated by a single element.

**Theorem 3.4.** *Any finite unital 3-field  $F$  of characteristic 1 which is generated by a single element  $x$  is isomorphic to  $F_0(n_P)$  where  $n_P$  is the smallest natural number with  $(1-x)^n = 0$ . If  $j(P) = \min\{i \mid \eta_i \neq 0\}$  then  $n_P = \lceil n/k \rceil$ .*

*Proof.* Consider the polynomial 3-ring  $F_0[x] = \{1 + \sum_{\nu=1}^n \varepsilon_\nu (x-1)^\nu \mid \varepsilon_\nu \in \mathbb{F}_2\}$  for which  $\mathcal{U}F_0[x]$  is the principal domain  $\mathbb{F}_2[x]$ . Consequently, whenever  $F$  is generated by a single element, there is a polynomial  $P \in \mathcal{Q}F_0[x] = \{\sum_{\nu=0}^n \varepsilon_\nu (x-1)^\nu \mid \varepsilon_\nu \in \mathbb{F}_2\}$  such that  $F = F_0[x]/\langle P \rangle$ . The polynomial  $P$  cannot be of the form

$$P = (x-1)^n \left( 1 + (x-1)^k + \sum_{\nu=k+1}^N \pi_\nu (x-1)^\nu \right), \quad \pi_\nu \in \mathbb{F}_2, \quad (3.8)$$

because then  $\langle 1 + (x-1)^k + \sum_{\nu=k+1}^N \pi_\nu (x-1)^\nu \rangle$  would be strictly larger than  $\langle P \rangle$ , intersect  $F_0[x]$  and thus contradict [10][Theorem 1]. So,  $P = (x-1)^n$  for the smallest  $n$  with  $(x-1)^n = 0$  within the 3-field  $F$ .  $\square$

Any attempt at creating a theory related to classical Galois theory has to deal with a number of obstacles, one of them, for example, the less useful factorization of polynomials: In  $F_0(4)$ , for example, the polynomial  $1 + (x-1) + (x-1)^3 = [1 + (x-1)][1 + (x-1)^3]$  vanishes at 1 when using the right hand representation, while it takes the value 1 when 1 is plugged into  $1 + (x-1) + (x-1)^3$ .

**Proposition 3.5.** *The ideals of  $F_0(n)$  are*

$$\mathfrak{I}_k = \left\{ \sum_{\nu \geq k} \varepsilon_\nu (x-1)^\nu \mid \varepsilon_\nu \in \mathbb{F}_2 \right\}, \quad k = 1, \dots, n-1 \quad (3.9)$$

Consequently,  $F_0(n)$  never is a Cartesian product of 3-fields.

*Proof.* Since the ring  $\mathcal{U}F_0(n) = \{\sum_{\nu=0}^{n-1} \varepsilon_\nu (x-1)^\nu \mid \varepsilon_i \in \mathbb{F}_2\}$  is principal, for each proper ideal  $\mathfrak{I}$  in  $\mathcal{Q}F_0(n)$  the ideal

$$\langle \mathfrak{I}, F_0(n) \rangle = \left\{ \sum q_i (1+r_i) \mid q_i \in \mathfrak{I}, r_i \in \mathcal{Q}F_0(n) \right\} \subseteq \mathfrak{I} + \mathfrak{I} \quad (3.10)$$

is the same as  $\mathfrak{I}$  and so  $\mathfrak{I} = \langle P_0 \rangle$ , with  $P_0 \in \mathcal{Q}F_0(n)$ . Since each  $P \in \mathcal{Q}F_0(n)$  can be written  $P = (x-1)^s(1+R)$ ,  $(1+R)$  invertible,  $1 \leq s \leq n-1$ , it follows that the ideals of  $\mathcal{Q}F_0(n)$  are precisely those of the form  $\mathfrak{I}_k = \langle (x-1)^k \rangle$ . But  $\mathfrak{I}_s \cap \mathfrak{I}_t = \mathfrak{I}_{\max\{s,t\}}$ ,  $\mathfrak{I}_s + \mathfrak{I}_t = \mathfrak{I}_{\min\{s,t\}}$  and, by applying Theorem 2.1, we conclude that  $F_0(n)$  never is a proper Cartesian product of 3-fields.  $\square$

Whether or not  $F_0(n)$  can be written as a semi-direct product is a slightly more delicate question, and we will return to it elsewhere.

**Lemma 3.6.** *Denote by  $\varphi_n : F_0(n) \rightarrow F_0(n)$  the Frobenius morphism  $P \mapsto P^2$ , by  $F_0(n)^2$  its image, and, for  $k \geq 2$  let  $\mu_{n,k} : F_0(n) \rightarrow F_0(k)$  be defined by*

$$\mu_{n,k} \left( 1 + \sum_{i=1}^{n-1} \varepsilon_i (x-1)^i \right) = 1 + \sum_{i=1}^{k-1} \varepsilon_i (x-1)^i. \quad (3.11)$$

(1)  $\varphi_n$  and  $\mu_{n,k}$  are morphisms,

$$\text{Ker } \varphi_n = \mathfrak{J}_{\lfloor n/2 \rfloor}, \quad \text{and} \quad \text{Ker } \mu_{n,k} = \mathfrak{J}_k \quad (3.12)$$

(2) The product on  $\text{Ker } \varphi_n$  vanishes identically so that  $(1 + P_1)(1 + P_2) = 1 + P_1 + P_2$ .

*Proof.* (1) Both maps are well-known (and easily seen to be) morphisms. Furthermore, the image of  $\varrho_n$  can naturally be embedded into  $F_0(n)$ .  $\square$

The additive structure of  $F_0(n)$  is most transparent on  $\mathcal{U}F_0(n)$ , which is a (binary) vector space with basis  $\{(x-1)^k \mid k = 0, \dots, n-1\}$ . The multiplicative structure of these fields is the following.

**Theorem 3.7.** *Each element  $f \in F_0(n)$  has a uniquely defined factorization  $f = \gamma_0^{\alpha_0} \dots \gamma_K^{\alpha_K}$  where*

$$\gamma_k = 1 + (x-1)^{2^{k+1}} \quad 0 \leq 2k+1 \leq n-1, \quad (3.13)$$

and it follows that the multiplicative group underlying  $F_0(n)$  is isomorphic to the direct product  $C_{n,0} \times \dots \times C_{n,K_n}$  of the cycles  $C_{n,k}$  of the  $\gamma_k$ , with  $K_n = \max\{k \mid 2k+1 \leq n-1\}$ , and  $C_{n,k} \cong \mathbb{Z}/2^{s(n,k)}$ ,  $s(n,k) = \min\{2^t \mid 2^t k \geq n\}$ . Consequently, with respect to its multiplicative structure,

$$F_0(n) \cong \prod_{0 \leq 2k+1 \leq n} (\mathbb{Z}/2^{s(n,k)})^{r(n,k)}, \quad (3.14)$$

*Proof.* The cases  $n = 2$  is trivial, and the elements of  $F_0(3)$  are  $\gamma_0^k$ ,  $k = 0, \dots, 3$ . If the statement is true for  $F_0(n)$ ,  $f \in F_0(n+1)$  has a uniquely defined factorization  $f = g\gamma_0^{\alpha_0} \dots \gamma_K^{\alpha_K}$  where  $g \in \{1 + \varepsilon(x-1)^n \mid \varepsilon = 0, 1\}$ , the multiplicative kernel of the canonical morphism  $\pi : F_0(n+1) \rightarrow F_0(n)$ . If  $n$  is odd, this already proves the claim; in case  $n$  is even and  $g \neq 1$  we must have  $g = (1 + (x-1)^\ell)^{2^m}$ ,  $\ell$  odd, and the statement of the result follows for  $n+1$ .  $\square$

**3.2. Intermediate Fields.** We start with slightly generalizing Corollary 2.19.

**Theorem 3.8.** *Suppose  $Q$  is a nilpotent ring with 2-unit  $\tau$  and let  $F$  be the unital 3-field with  $\mathcal{Q}(F) = Q$ .*

- (1)  $Q' \rightsquigarrow 1 + Q' \subseteq F$  establishes a one-to-one correspondence between the subrings  $Q'$  of  $Q$  with  $\tau \in Q'$  and the unital 3-subfields  $F'$  of  $F$ .
- (2) The unital 3-subfield  $F_0$  is generated by elements  $1 + q_1, \dots, 1 + q_n$  iff  $\mathcal{Q}(F_0)$  is generated by  $\tau = q_{1,1}$  and  $q_1, \dots, q_n$ .
- (3) The automorphisms  $\Phi$  of  $F$  leaving the subfield  $F'$  pointwise fixed correspond to the automorphisms  $\mathcal{Q}\Phi$ , leaving  $Q' = \mathcal{Q}(F')$  pointwise fixed.

*Proof.* (1) If  $F_0$  is a unital 3-subfield of  $F$ , the unit of  $F_0$  must equal the one in  $F$ , and  $\mathcal{Q}(F_0)$  is a subring containing  $\zeta = q_{1,1}$  which has the property that  $\zeta q = q + q$  for all  $q \in \mathcal{Q}(F_0)$ . Note that  $1 + \mathcal{Q}(F_0) = F_0$ .

Conversely, assume that  $Q \subseteq \mathcal{Q}(F)$  with  $\tau \in Q$  and define  $F_1 = \{f \in F \mid q_{1,f} \in Q\}$ . We have  $1 \in F_1$  since  $\tau \in Q$  and  $-1 \in F_1$  because  $0 \in Q$ . It follows similarly that for all  $f, g \in F_1$ ,

$$1 + f + g \in F_1, \quad f + g + gf \in F_1, \quad (3.15)$$

and that there is  $\check{f}$  with  $1 + f + \check{f} = -1$ . From this, and the nilpotency of  $Q$  it follows that  $F_1$  is unital 3-field such that  $F_1 = 1 + Q$ .

(2) The subring  $Q_0$  generated by  $\tau$  and  $q_1, \dots, q_n$  consists of the elements  $k\tau + \sum_{\alpha} \varepsilon_{\alpha} q^{\alpha}$ ,  $k \in \mathbb{N}_0$ . Note that due to nilpotency, this ring is of finite characteristic. Then  $1 + Q_0$  is a unital 3-field, consisting of elements  $k + \sum_{\alpha} \varepsilon_{\alpha} q^{\alpha}$ ,  $k$  odd, and resolving the brackets in  $k + \sum_{\alpha} \varepsilon_{\alpha} (1+q)^{\alpha}$  shows that  $1 + Q_0$  is the unital 3-field generated by 1 and  $1 + q_1, \dots, 1 + q_n$ . Conversely, if  $F_0$  is generated by  $1, 1 + q_1, \dots, 1 + q_n$ ,  $\mathcal{Q}(F_0)$  contains  $\tau, q_1, \dots, q_n$  and thus the binary ring  $Q_0$ , generated by these elements. By the first part of this proof,  $F_0 = 1 + Q_0$ , and so  $Q_0 = \mathcal{Q}(F_0)$ .

(3) This follows from the involved definitions.  $\square$

*Remark 3.9.* The last theorem can be easily generalized to  $\mathcal{Q}$ -rings and their  $\mathcal{Q}$ -subrings, where a  $\mathcal{Q}$ -subring  $Q_1$  of the  $\mathcal{Q}$ -ring  $Q$  is defined by the requirement that  $\tau \in Q_1$  and that  $Q_1$  is invariant under the  $\#$ -operation.

**Corollary 3.10.** *For each ideal  $J$  of the finite unital 3-field  $F$  the subalgebra  $1 + J$  a unital subfield.*

*Proof.* For  $\zeta = q_{1,1} \in \mathcal{Q}(F)$  we have  $\zeta = q(q-1)^{-1} \in J$ .  $\square$

**Corollary 3.11.** *For a unital 3-subfield  $F$  of  $F_0(n)$  which is generated by polynomials  $P_1, \dots, P_g$  there exist natural numbers  $n_1, \dots, n_g$  such that  $F \cong F_0(n_1, \dots, n_g)$ .*

*Example 3.12.* The smallest subfields, those of order 2, are generated by polynomials

$$1 + (x-1)^k(1 + P_1) = (1 + (x-1)^k)(1 + P_1) - P_1 \quad (3.16)$$

with  $2k \geq n$ . We call  $k$  the *lower degree* of the subfield. As we will see, the automorphisms which are constant on such a field are of the form  $\Psi_P$  with  $P_0 = (x-1) + (x-1)^{\ell}(1 + P_1)$  with  $\ell \geq n - k + 1$  so that  $\text{Aut } F_0(n)$  cannot distinguish between subfields of the same degree in terms of fixed point subgroups. On the other hand, all elements of  $\text{Aut } F_0(n)$  preserve  $k$ , and, since

$$\Psi(1 + P_1) = (\Psi(P) - 1) \Psi(x-1)^{-k} - 1 = (x-1)^k(1 + Q_1), \quad (3.17)$$

*Example 3.13.* The subfield of squares,  $F_0(n)^2 = \{f \in F_0(n) \mid f = 1 + \sum_{\nu \geq 1} \eta_{\nu} (x-1)^{2\nu}\}$  is isomorphic to all subfields generated by a polynomial of the form  $f_0 = 1 + (x-1)^2 f_1$ ,

We will need

**Lemma 3.14.** *Fix a natural number  $\alpha$ , write  $\alpha = \sum_{\nu=0}^{n_{\alpha}} \alpha_{\nu} 2^{\nu}$ ,  $\alpha_{\nu} = 0, 1$ , and let*

$$N_{\alpha} = \left\{ \sum_{\nu=0}^{n_{\alpha}} \varepsilon_{\nu} \alpha_{\nu} 2^{\nu} \mid \varepsilon_{\nu} = 0, 1 \right\}. \quad (3.18)$$

Then

$$[1 + (x-1)^k]^{\alpha} = 1 + \sum_{n \in N_{\alpha}} (x-1)^{kn}. \quad (3.19)$$

Conversely, given  $N \subseteq \{1, \dots, n-1\}$ , then  $P_N = 1 + \sum_{\nu \in N} (x-1)^{\nu} = (1 + (x-1)^k)^{\alpha}$  iff  $N \subseteq k\mathbb{N}$  and

$$N = \left\{ \sum_{\nu} \varepsilon_{\nu} 2^{\nu} \mid k2^{\nu} \in N, \varepsilon_{\nu} = 0, 1 \right\} \cap \{1, \dots, n-1\}. \quad (3.20)$$

*Proof.* We have

$$(1 + (x-1)^k)^{\alpha} = \prod_{\nu=0}^{n_{\alpha}} (1 + (x-1)^{k2^{\nu}})^{\alpha_{\nu}}, \quad (3.21)$$

and each subset  $N' \subseteq \{\nu \mid \alpha_\nu = 1\}$  corresponds to exactly one of the summands  $(x-1)^{kn}$  of  $1 + \sum_{n \in N_\alpha} (x-1)^{kn}$ , where  $n = \sum_{\nu \in N'} 2^\nu$  (and with  $n = 0$  for the empty set).  $\square$

We start with a ‘local’ version Theorem 3.4.

**Lemma 3.15.** *The unital 3-subfield generated by  $P = 1 + (x-1)^k(1 + P_k) \in F_0(n)$  is given by*

$$\langle P \rangle = \left\{ 1 + \sum_{0 < ki \leq n-1} \eta_i (x-1)^{ki} (1 + P_k)^i \mid \eta_i \in \mathbb{F}_2 \right\} =: F_1 \quad (3.22)$$

and is isomorphic to

$$\langle 1 + (x-1)^k \rangle = \left\{ 1 + \sum_{0 < i \leq (n-1)/k} \eta_i (x-1)^{ki} \mid \eta_i \in \mathbb{F}_2 \right\}. \quad (3.23)$$

*Proof.* By (a slight modification of) Lemma 3.14 the elements of  $\langle P \rangle$  belong to  $F_1$ , and since  $F_1$  is a unital 3-field,  $\langle P \rangle \subseteq F_1$ . By Theorem 3.4, the isomorphism class of  $\langle P \rangle$  is determined by the minimal number  $n_P$  with  $(P-1)^{n_P} = 0$ . This number is the same for  $P$  and  $1 + (x-1)^k$  hence  $\langle P \rangle \cong \langle 1 + (x-1)^k \rangle$  are both of cardinality  $2^{n_P-1}$ . Since also  $F_1$  is of this cardinality,  $F_1 = \langle P \rangle$ .  $\square$

**Theorem 3.16.**  *$F \subseteq F_0(n)$  is a subfield iff there are natural numbers  $g_1, \dots, g_k \leq n-1$ ,  $k \leq n-1$ , with*

$$\begin{aligned} F &\cong F_0(n; g_1, \dots, g_k) := \langle 1 + (x-1)^{g_1}, \dots, 1 + (x-1)^{g_k} \rangle = \\ &= \left\{ 1 + \sum_{1 \leq \nu_1 g_1 + \dots + \nu_k g_k \leq n-1} \varepsilon_{\nu_1 \nu_2 \dots \nu_k} (x-1)^{\nu_1 g_1 + \dots + \nu_k g_k} \mid \varepsilon_{\nu_1 \dots \nu_k} \in \mathbb{F}_2 \right\} =: G(n; g_1, \dots, g_k). \end{aligned} \quad (3.24)$$

*Proof.* In order to see that  $F_0(n; g_1, \dots, g_k)$  is unital 3-subfield it suffices to show that it is a unital 3-subring. But this is obvious, and it follows that  $F_0(n; g_1, \dots, g_k)$  is contained in  $G(n; g_1, \dots, g_k)$ . By Lemma 3.15,

$$\begin{aligned} 1 + (x-1)^{\mu g_i + \nu g_j} &= \\ &= (1 + (x-1)^{\mu g_i})(1 + (x-1)^{\nu g_j}) - (1 + (x-1)^{\mu g_i}) - (1 + (x-1)^{\nu g_j}) \end{aligned} \quad (3.25)$$

is contained in  $F_0(n; g_1, \dots, g_k)$ , and similarly,  $1 + (x-1)^{\nu_1 g_1 + \dots + \nu_k g_k} \in F_0(n; g_1, \dots, g_k)$ . Using induction over the number of elements in  $\{\varepsilon_{\nu_1, \dots, \nu_k} = 1\}$  with the induction step of adjoining  $1 + (x-1)^{\langle \mu, g \rangle}$  to  $1 + \sum_{1 \leq \langle g, \nu \rangle \leq n-1} \varepsilon_\nu (x-1)^{\langle \nu, g \rangle}$  being established by

$$\begin{aligned} 1 + (x-1)^{\langle \mu, g \rangle} + \sum_{1 \leq \langle g, \nu \rangle \leq n-1} \varepsilon_\nu (x-1)^{\langle \nu, g \rangle} &= \\ &= 1 + (1 + (x-1)^{\langle \mu, g \rangle}) + \left( 1 + \sum_{1 \leq \langle g, \nu \rangle \leq n-1} \varepsilon_\nu (x-1)^{\langle \nu, g \rangle} \right), \end{aligned} \quad (3.26)$$

one shows that, conversely,  $G(n; g_1, \dots, g_k) \subseteq F_0(n; g_1, \dots, g_k)$ .  $\square$

Let  $F \subseteq F_0(n)$  be a subfield. We call the semigroup

$$\text{Ex } F = \{\alpha \in \mathbb{Z}/n \mid 1 + (x - a)^\alpha \in F\} \quad (3.27)$$

the *exponents* of  $F$ . The proof of the following results rest on

**Lemma 3.17.** *Suppose  $S$  is a sub-semigroup of the additive semigroup  $\mathbb{Z}/n$  and  $N_0$  one of its subsets. Then*

(1) *there are uniquely determined elements  $s_1 < \dots < s_k \in S$  with*

$$s_{\varkappa+1} = \min S \setminus \{z_1 s_1 + \dots + z_\varkappa s_\varkappa \mid z_i \in \mathbb{Z}/n\} \quad (3.28)$$

$$S = \{z_1 s_1 + \dots + z_k s_k \mid z_i \in \mathbb{Z}/n\} \quad (3.29)$$

*Equivalently, none of the  $s_i$  divides  $s_j$ .*

(2) *The sub-semigroup  $S(N_0)$  generated by  $N_0$  can be constructed inductively by letting  $s_1 = \min N_0$  and  $s_{n+1} = \min N_0 \setminus \{z_1 s_1 + \dots + z_n s_n \mid z_1, \dots, z_n \in \mathbb{N}\}$  as long as the latter set is not empty. If  $M$  is the index before this happens,*

$$S(N_0) = \setminus \{z_1 s_1 + \dots + z_M s_M \mid z_1, \dots, z_M \in \mathbb{N}\} \quad (3.30)$$

**Corollary 3.18.** *The set of isomorphism classes of subfields of  $F_0(n)$  is order isomorphic to the set of sub-semigroups of the additive semigroup  $\mathbb{Z}/n$ . Furthermore, two subfields  $F_{1,2}$  of  $F_0(n)$  are isomorphic iff  $\text{Ex } F_1 = \text{Ex } F_2$ .*

**3.3. The group of automorphisms and the global involution.** For the following it is important to observe that the elements of

$$\mathcal{Q}F_0(n) = \left\{ \sum_{i=1}^{n-1} \varepsilon_i (x-1)^i \mid \varepsilon_i \in \mathbb{F}_2 \right\} \quad (3.31)$$

are in 1-1 correspondence with unital endomorphisms  $\Phi$  of  $F_0(n)$ : Each such  $\Phi$  is uniquely determined by the polynomial  $P_\Phi = \mathcal{Q}\Phi(x-1) \in \mathcal{Q}F_0(n)$  and, conversely, any polynomial  $P = 1 + P_0 \in F_0(n) = 1 + \mathcal{Q}F_0(n)$  provides a unital endomorphisms  $\Phi_P$ , defined for  $Q = 1 + Q_0(x-1) \in F_0(n)$  by

$$\Phi_P(1 + Q_0(x-1)) = 1 + Q_0 \circ P_0 \pmod{(x-1)^n}. \quad (3.32)$$

This map is well-defined because the ideal generated by  $(x-1)^n$  for the ternary polynomial ring  $F_0[x]$  within

$$\mathcal{Q}F_0[x] = \left\{ \sum_{i=1}^N \varepsilon_i (x-1)^i \mid N \in \mathbb{N}, \varepsilon_i \in \mathbb{F}_2 \right\} \quad (3.33)$$

is invariant under composition with polynomials in  $(x-1)$  from the right. It is additive and respects multiplication because

$$\begin{aligned} \Phi_P((1 + Q_0(x-1))(1 + R_0(x-1))) &= \\ &= 1 + (Q_0(x-1) + R_0(x-1) + Q_0(x-1)R_0(x-1)) \circ P_0 = \\ &= \Phi_P(1 + Q_0(x-1)) \Phi_P(1 + R_0(x-1)) \end{aligned} \quad (3.34)$$

Since  $\Phi_Q \circ \Phi_P = \Phi_{Q \circ P}$  we have shown the first part of

**Theorem 3.19.** *The mapping  $\Phi \mapsto \mathcal{Q}\Phi(x-1)$  establishes an isomorphism between the ring of unital endomorphisms of  $F_0(n)$  with respect to composition of maps and  $\mathcal{Q}F_0(n)$ , equipped with composition of polynomials in the variable  $(x-1)$ .*

*Under this identification, a polynomial  $P$  corresponds to an automorphism of  $F_0(n)$  iff there is a polynomial  $Q \in F_0(n)$  such that  $P_0 \circ Q_0 = P_0 \circ Q_0 = (x-1)$  which is equivalent to*

$$\mathcal{Q}\Phi(x-1) = (x-1) + \sum_{i=2}^{n-1} \varepsilon_k(x-1)^k. \quad (3.35)$$

*Proof.* We still have to show the final statement. For arbitrary  $n = \alpha_0 + \alpha_1 2 + \dots + \alpha_N 2^N \in \mathbb{N}$ ,  $\alpha_\nu \in \mathbb{F}_2$  and any polynomial  $P_0 = \sum_{i=1}^{n-1} \varepsilon_k(x-1)^k$

$$P_0^n = \left( \sum_{i=1}^{n-1} \varepsilon_k(x-1)^k \right)^{\alpha_0} \left( \sum_{i=1}^{n-1} \varepsilon_k(x-1)^{2k} \right)^{\alpha_1} \dots \left( \sum_{i=1}^{n-1} \varepsilon_k(x-1)^{2^N k} \right)^{\alpha_N}, \quad (3.36)$$

with some of the factors of highest order potentially equal to zero. Accordingly, for no polynomial  $Q_0$ ,  $Q_0 \circ P_0$  has  $(x-1)$  as lowest term if  $P_0$  doesn't, and any polynomial  $P_0$  giving rise to an automorphism must have  $(x-1)$  as lowest term.<sup>1</sup> (This could also be shown by using the ideal structure of  $F_0(n)$ .)

For the converse, we represent  $\Phi_P$  with  $P_0 = (x-1)^k(1+P_1)$  as a matrix with respect to the basis  $(x-1)^\nu$ ,  $\nu = 1, \dots, n-1$ , of  $\mathcal{U}(F_0(n))$ . Writing

$$\Phi_P [(x-1)^\nu] = (x-1)^\nu(1+P_1)^\nu \quad (3.37)$$

as row vectors, it turns out that the resulting matrix is upper triangular with 1's on the main diagonal so that  $\Phi_P$  must be invertible.  $\square$

Using the multinomial identity

$$(a_1 + \dots + a_m)^n = \sum_{i_1 + \dots + i_m = n} \frac{n!}{i_1! \dots i_m!} a_1^{i_1} \dots a_m^{i_m} \quad (3.38)$$

we find for the polynomial  $P_0 = (x-1) + \sum_{\nu=2}^{n-1} \varepsilon_\nu(x-1)^\nu$

$$P_0^k = \sum_{i_1 + \dots + i_{n-1} = k} \frac{k!}{i_1! \dots i_{n-1}!} \varepsilon_2 \dots \varepsilon_{n-1} (x-1)^{i_1 + 2i_2 + \dots + (n-1)i_{n-1}} = \quad (3.39)$$

$$= \sum_{\ell=k}^{n-1} \left( \sum_{i_1 + 2i_2 + \dots + (n-1)i_{n-1} = \ell} \frac{k!}{i_1! \dots i_{n-1}!} \varepsilon_2 \dots \varepsilon_{n-1} \right) (x-1)^\ell \quad (3.40)$$

On the other hand, over  $\mathbb{F}_2$ , and with  $n = \sum_{\nu=0}^N n_\nu 2^\nu$ ,

$$(a_1 + \dots + a_m)^n = \prod_{\nu=0}^N (a_1^{2^\nu} + \dots + a_m^{2^\nu})^{n_\nu} \quad (3.41)$$

and

$$P_0^k = \prod_{\nu=0}^N \left( (x-1)^{2^\nu} + \dots + \varepsilon_\mu (x-1)^{2^\nu \mu} \dots + \varepsilon_m (x-1)^{2^\nu m} \right)^{n_\nu} \quad (3.42)$$

<sup>1</sup>Note that this is different for polynomials  $P$  of the form  $1 + \sum_{k \geq 1} \varepsilon_k x^k$ , since large powers of the polynomial  $x$  might contain a constant term. For example, in  $F_0(5)$ ,  $x^5 = x^4 + x - 1$ , and also  $(x + x^2 + x^4) \circ (1 + x + x^2) = x$ .

**Corollary 3.20.** *The coefficients of  $A_P = (\alpha_{k\ell}^P)$  are*

$$\alpha_{k\ell}^P = \sum_{i_1+2i_2+\dots+(n-1)i_{n-1}=\ell} \frac{k!}{i_1! \dots i_{n-1}!} \varepsilon_2 \dots \varepsilon_{n-1}, \quad (3.43)$$

for  $k = 1, \dots, n-1$ ,  $\ell = k, \dots, n-1$ .

If  $o(\Phi_P) = 2^{\ell(\Phi_P)}$  denotes the order of  $\Phi_P \in \text{Aut } F_0(n)$  then  $\Phi_P^{-1} = \Phi_P^{o(\Phi_P)-1}$ . An algorithm of lower complexity is obtained using matrix products

**Corollary 3.21.** *Let  $P = 1 + (x-1) + P_1 = \sum_{\nu=0}^n \varepsilon_\nu (x-1)^\nu$  be the polynomial that belongs to  $\Phi_P \in \text{Aut}(F)$ . Then the coefficients of the polynomial  $\hat{P} = \sum_{\nu=0}^n \hat{\varepsilon}_\nu (x-1)^\nu$  for which  $\Phi_P^{-1} = \Phi_{\hat{P}}$  can be recursively calculated using*

$$\hat{\varepsilon}_0 = \hat{\varepsilon}_1 = 1 \quad \hat{\varepsilon}_\ell = \hat{\varepsilon}_1 \varepsilon_\ell^{(1)} + \hat{\varepsilon}_2 \varepsilon_\ell^{(2)} + \dots + \hat{\varepsilon}_{\ell-1} \varepsilon_\ell^{(\ell-1)} \quad (3.44)$$

**Lemma 3.22.** *Let  $s_n = -\sum_{\nu=1}^{n-1} (x-1)^\nu \in \mathcal{Q}F_0(n)$ . Then  $R_n := \Phi_{s_n}$  has order 2 and*

$$R_n \left[ 1 + \sum_{i=1}^{n-1} \varepsilon_i (x-1)^i \right] = 1 + \sum_{i=1}^{n-1} \varepsilon_i ((x-1)^\#)^i. \quad (3.45)$$

*Proof.* Since, with respect to multiplication,

$$s_n = 1 + [(x-1) - 1]^{-1} \quad (3.46)$$

it follows that  $1 + (s_n - 1)^{-1} = (x-1)$  or,  $s_n \circ s_n = (x-1)$  (which is equivalent to observing that  $q \mapsto q^\#$  is an involution, Definition 2.9 and Example 2.11). The somewhat more explicit form for  $R_n$  is a consequence of the fact that  $s_n = (x-1)^\#$ .  $\square$

**Lemma 3.23.** *A group  $G$  of order  $2n$  has a representation  $\mathbb{Z}/2 \rtimes H$  iff  $G$  contains a normal subgroup  $H$  of order  $n$  as well as an involution  $r \in G \setminus H$ .*

*Proof.* The short exact sequence  $H \rightarrow G \rightarrow \mathbb{Z}/2$  can be split by mapping the non-unit of  $\mathbb{Z}/2$  to  $r$ .  $\square$

**Lemma 3.24.** *Define*

$$M_{n,k} : \text{Aut } F_0(n) \rightarrow \text{Aut } F_0(k), \quad M_{n,k} \Phi(x + \mathfrak{J}_k) = \Phi(x) + \mathfrak{J}_k, \quad (3.47)$$

where  $1 + \sum_{\nu=1}^{n-1} \varepsilon_\nu (x-1)^\nu + \mathfrak{J}_k \in F_0(n)/\mathfrak{J}_k$  is identified with  $1 + \sum_{\nu=1}^{k-1} \varepsilon_\nu (x-1)^\nu \in F_0(k)$ .

(1) *Identifying  $F_0(k)$  with  $F_0(n)/\mathfrak{J}_k$ , if  $\Phi = \Phi_P$  with  $P = (x-1) + \sum_{\nu=2}^{n-1} \varepsilon_\nu (x-1)^\nu$  then*

$$M_{n,k} \Phi_P = (x-1) + \sum_{\nu=2}^{k-1} \varepsilon_\nu (x-1)^\nu, \quad (3.48)$$

and  $\text{Ker } M_{n,k}$  is equal to

$$\Gamma_{n,k} = \left\{ \Phi_P \in \text{Aut } F_0(n) \mid P_0 = (x-1) + \sum_{\nu=k}^{n-1} \varepsilon_\nu (x-1)^\nu, \varepsilon_\nu \in \mathbb{F}_2 \right\} \quad (3.49)$$

(2) *Restricting  $M_{n,k+1}$  to  $\Gamma_{n,k}$  yields an exact sequence*

$$0 \longrightarrow \Gamma_{n,k+1} \longrightarrow \Gamma_{n,k} \longrightarrow \Gamma_{k+1,k} \longrightarrow 0 \quad (3.50)$$

*This sequence splits whenever  $k > 2$  so that in this case,*

$$\Gamma_{n,k} \cong \Gamma_{n,k+1} \rtimes \mathbb{F}_2. \quad (3.51)$$

(3) Similarly,  $\varphi_n$  generates the group morphism

$$\varrho_n : \text{Aut } F_0(n) \rightarrow \text{Aut } (F_0(n)^2), \quad \varrho_n(\Phi) = \Phi|_{F_0(n)^2} \quad (3.52)$$

Identifying the subfield of squares in  $F_0(n)$  with  $F_0(\lfloor \frac{n}{2} \rfloor)$ , the effect of  $\varrho_n$  on the polynomial  $P$  representing  $\Phi = \Phi_P$  can be seen as

$$\varrho_n : \text{Aut } F_0(n) \rightarrow \text{Aut } F_0\left(\left\lfloor \frac{n}{2} \right\rfloor\right), \quad P \mapsto P|_{F_0(\lfloor \frac{n}{2} \rfloor)} \quad (3.53)$$

In this picture,  $\Phi_P \in \text{Ker } \varrho_n$  iff  $P = (x-1) + \sum_{\nu \geq \lfloor n/2 \rfloor} \varepsilon_\nu (x-1)^\nu$ .

(4) Accordingly, for each  $k$  with  $2^k \leq n$  there is a short exact sequence

$$G_{n,k} \longrightarrow \text{Aut } F_0(n) \longrightarrow \text{Aut } \left( (F_0(n)^{2^k}) \cong \text{Aut } F_0\left(\left\lfloor \frac{n}{2^k} \right\rfloor\right) \right) \quad (3.54)$$

where  $G_{n,k}$  is the normal subgroup of automorphisms for which  $1 + (x-1)^{2^k}$  is a fixed point. The polynomials  $P_0$ , representing  $\Phi \in G_{n,k}$  via  $\Phi(1 + (x-1)) = 1 + P_0(x-1)$ , are characterized by

$$P_0 = (x-1) + \sum_{i > (n-1)/2^k} \varepsilon_i (x-1)^i = (x-1) + (x-1)^{\lfloor (n-1)/2^k \rfloor} \sum_{i=1}^{n-1-\lfloor (n-1)/2^k \rfloor} \varepsilon_i (x-1)^i, \quad \varepsilon_i \in \mathbb{F}_2, \quad (3.55)$$

and it follows that  $G_{n,1}$  is commutative.

*Proof.* (1) Because  $\mathfrak{J}_k = \text{Ker } \mu_{n,k} = \left\{ \sum_{i=k+1}^{n-1} \varepsilon_i (x-1)^i \mid \varepsilon_i \in \mathbb{F}_2 \right\}$  is invariant under substitution by any polynomial  $Q_0 = (x-1) + \sum_{i=2}^n \eta_i (x-1)^i$  (which also follows from Lemma 3.5, each  $\Phi \in \text{Aut } F_0(n)$  acts on  $F_0(n)/\text{Ker } \mu_{n,k} = F_0(k)$  by substitution and an application of  $\mu_{n,k}$ ). The resulting element  $M_{n,k}(\Phi) \in \text{Aut } F_0(k)$  then maps  $x-1$  to  $\mu_{n,k} P_0$  for  $\Phi = \Phi_P \in \text{Aut } F_0(n)$ . Consequently,  $M_{n,k} : \text{Aut } F_0(n) \rightarrow \text{Aut } F_0(k)$  is a morphism with kernel consisting of automorphisms  $\Phi_P \in \text{Aut } F_0(n)$  such that for all  $Q = 1 + \sum_{i=1}^{k-1} q_i (x-1)^i$

$$\mu_{n,k} \Phi_P(Q) = \mu_{n,k} (1 + Q_0 \circ P_0) = Q. \quad (3.56)$$

which shows that  $P = 1 + (x-1) + \sum_{i=k}^n \eta_i (x-1)^i$ .

(2) The short exact sequence is established using (1). Polynomials for elements of  $\Gamma_{n,k} \setminus \Gamma_{n,k+1}$  are of the form  $P = (x-1) + (x-1)^k + \sum_{i=k+1}^{n-1} \varepsilon_i (x-1)^i$  so that  $R_n \notin \Gamma_{n,k} \setminus \Gamma_{n,k+1}$  if  $k > 2$ . The claim follows from Lemma 3.22 and Lemma 3.23.

(3)  $\varrho_n(\Phi)$  is a well-defined morphism. Identifying  $F_0(\lfloor n/2 \rfloor)$  with  $F_0(n)^2$  via  $\sigma_n(P) = P^2$ , one has for  $P = (x-1) + \sum_{\nu=2}^{n-1} \varepsilon_\nu (x-1)^\nu$

$$\sigma_n^{-1} \varrho_n(\Phi_P) \sigma_n(x-1) = \sigma_n^{-1} P^2 = (x-1) + \sum_{\nu=2}^{\lfloor n/2 \rfloor} \varepsilon_\nu (x-1)^\nu \quad (3.57)$$

The elements  $\Phi_P$  in the kernel  $G_{n,k}$  of  $\varrho_n^k$  restrict to all polynomials  $\sum_{i:2^k \leq n-1} \varepsilon_i (x-1)^{i2^k}$  as the identity or,  $\sum_{i:2^k \leq n-1} \varepsilon_i P_0(x-1)^{i2^k} = \sum_{i:2^k \leq n-1} \varepsilon_i (x-1)^{i2^k}$ . Equivalently,  $P_0^{2^k} = (x-1)^{2^k}$ , showing that  $P_0 = (x-1) + \sum_{n \leq i2^k} \varepsilon_i (x-1)^i$ . The commutativity of  $G_{n,1}$  is a consequence



of the fact that for  $P_0, Q_0 \in G_{n,1}$  we have

$$P_0 \circ Q_0(x-1) = Q_0(x-1) + \sum_{i=\lceil n/2 \rceil}^{n-1} \varepsilon_i Q_0^i(x-1) = Q_0(x-1) + P_0(x-1) \quad (3.58)$$

□

**Corollary 3.25.** *For each  $n \geq 3$ ,*

$$\text{Aut } F_0(n) \cong \mathbb{F}_2 \rtimes \mathbb{F}_2 \dots \rtimes \mathbb{F}_2, \quad (3.59)$$

*an  $(n-2)$ -fold semi-direct product of  $\mathbb{F}_2$ .*

*Proof.* By induction, this is a consequence of Lemma 3.6 (2). □

This last result by itself does not reveal much of the structure of  $\text{Aut } F_0(n)$ : Analogous results hold for each nilpotent Lie groups and, in all likelihood, it is possible to obtain the former by showing that  $\text{Aut } F_0(n)$  is a (nilpotent) Lie group in characteristic 2. More information can be gained by further investigating the involution that is underlying the proof of the above result.

**Definition 3.26.** Let  $f \in F_0(n)$  as well as  $\Phi \in \text{Aut } F_0(n)$ .

(1) Define conjugations  $f^*$  and  $\Phi^*$  by

$$f^* = R_n(f) \quad \Phi^*(f) = \Phi(f^*)^*, \quad (3.60)$$

(2) and we denote the 1-eigenspaces of these involutions by

$$F_0(n)_1 = \{f \in F_0(n) \mid f^* = f\}, \quad \text{Aut } F_0(n)_1 = \{\Phi \in \text{Aut } F_0(n) \mid \Phi^* = \Phi\} \quad (3.61)$$

*Example 3.27.* All elements of  $\mathfrak{J}_k$  with  $k \geq n/2$  are contained in  $F_0(n)_1$ , because if  $f = (x-1)^k$  then, for  $k = \sum_{n_0} \alpha_\nu 2^\nu$

$$f^* = s_n^k = \prod_{n_0} \left( \sum_{\mu=1}^{n-1} (x-1)^{\nu \alpha_\nu 2^\nu} \right) \quad (3.62)$$

## APPENDIX A. A REPRESENTATION OF THE TRUNCATED NOTTINGHAM GROUPS $\text{Aut } F_0(3) - \text{Aut } F_0(7)$

The case  $n = 2$  is trivial, for  $n = 3$  the polynomials  $1 + (x-1)$  and  $P(x) = 1 + (x-1) + (x-1)^2$  give rise to identity as well as to the automorphism with representing matrix

$$A_P = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad (A.1)$$

If  $n = 4$ , besides the identity,  $P_1 = 1 + (x-1) + (x-1)^2$ ,  $P_2 = 1 + (x-1) + (x-1)^3$  and  $P_3 = 1 + (x-1) + (x-1)^2 + (x-1)^3$  correspond to

$$A_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad A_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad A_3 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (A.2)$$

which is the cyclic group  $C_4$ . For  $n = 5$ ,  $P_\alpha = 1 + (x-1) + \sum_{i=2}^4 \alpha_{i-2}(x-1)^i$ , with  $(\alpha_0, \alpha_1, \alpha_2)$  representing the binary representation of  $\alpha$ , produces the matrices

$$A_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad A_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad A_2 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad A_3 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (\text{A.3})$$

$$A_4 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad A_5 = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad A_6 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad A_7 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \quad (\text{A.4})$$

As observed earlier, this group is isomorphic to the dihedral group of order 8, i.e.  $C_4 \times C_2$ . Similarly for  $n = 6$ ,  $P_\alpha = 1 + (x-1) + \sum_{i=2}^5 \alpha_{i-2}(x-1)^i$ , with  $(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$  again the binary representation of  $\alpha$  we have

$$A_0 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad A_1 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad A_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad A_3 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad (\text{A.5})$$

$$A_4 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad A_5 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad A_6 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad A_7 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad (\text{A.6})$$

$$A_8 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad A_9 = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad A_{10} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad A_{11} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad (\text{A.7})$$

$$A_{12} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad A_{13} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad A_{14} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad A_{15} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad (\text{A.8})$$

Calculating the cycle graph of this group, it turns out to be  $G_{16}^3 = K_4 \times C_4 = (C_4 \times C_2) \times C_2$ , where  $K_4$  denotes the Klein 4-group, (Wikipedia, List of small groups).



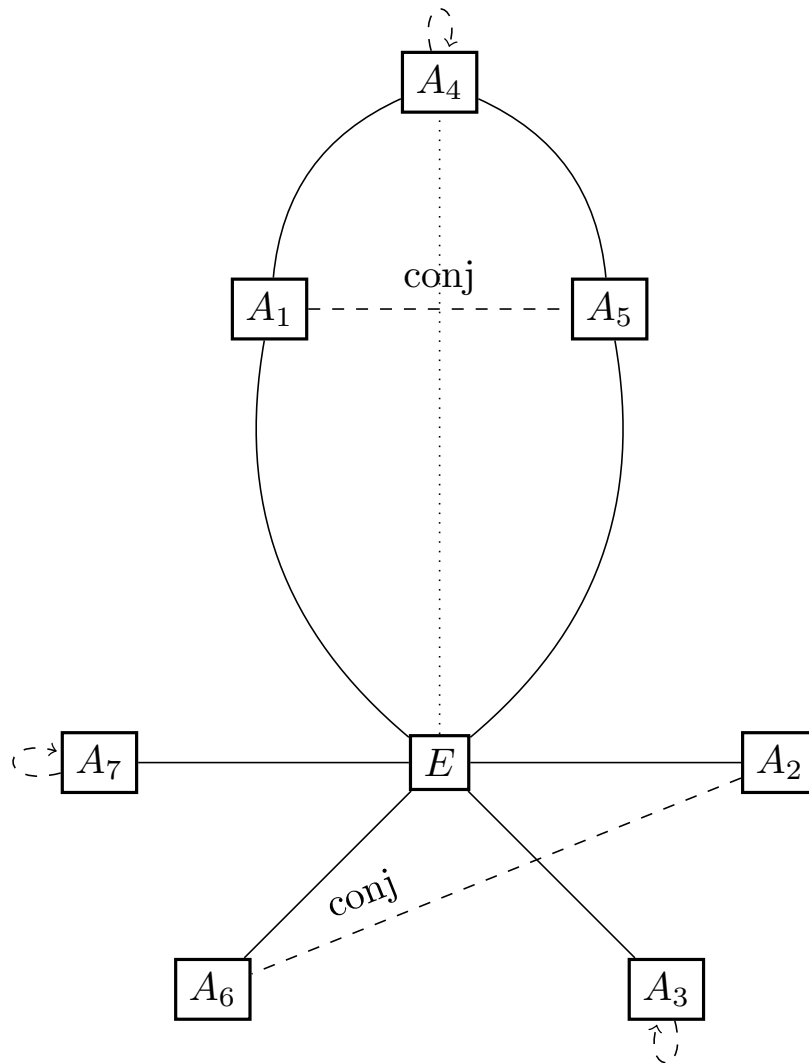


FIGURE 1. Cycle graph for  $\text{Aut } F_0(5) = C_4 \rtimes C_2 = D_4$ , the Dihedral Group of order 8, with  $C_2$  acting by inversion. The dotted lines indicate conjugation, as in Definition 3.26.

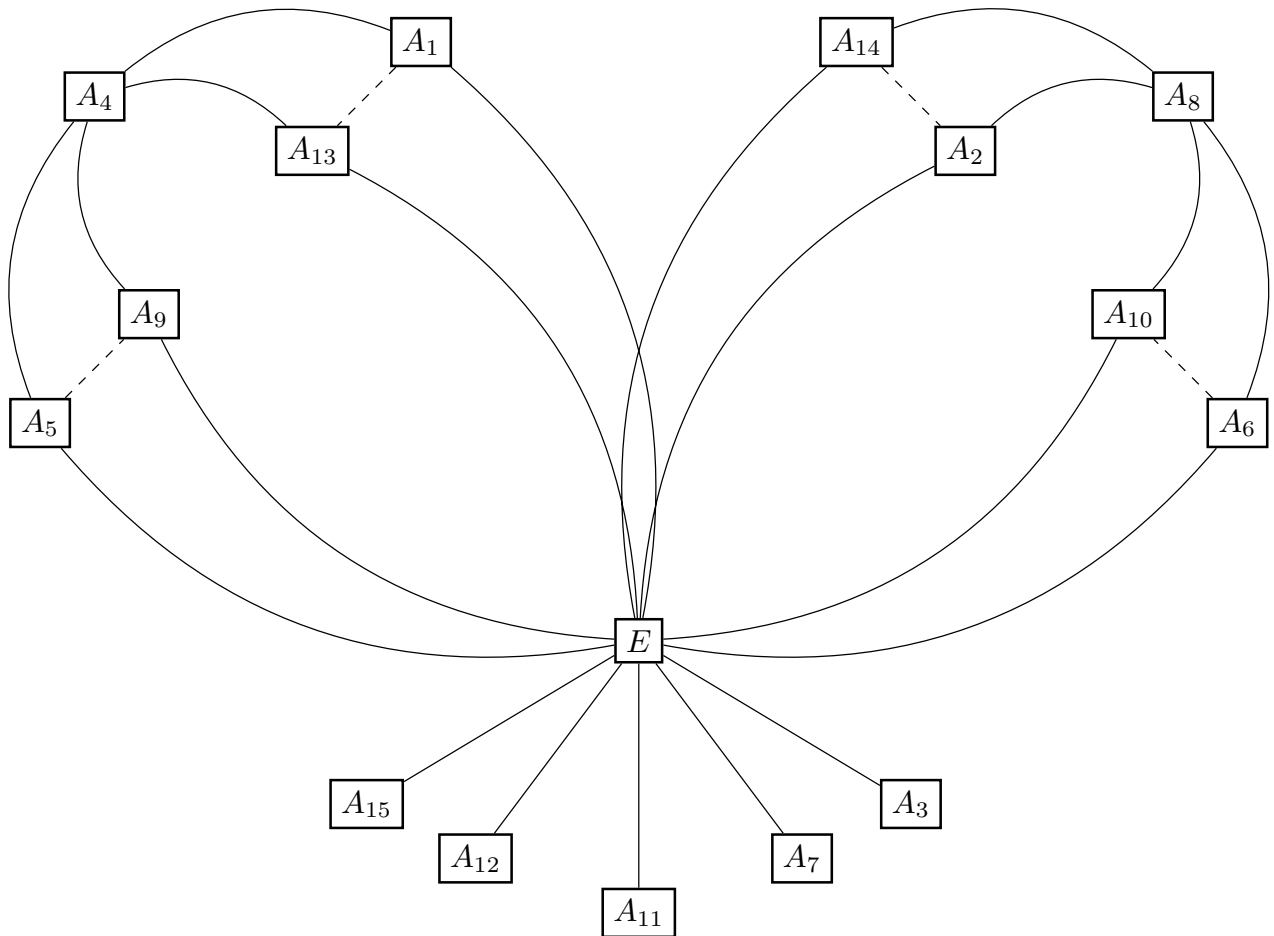


FIGURE 2. *Cycle graph for  $\text{Aut } F_0(6) = ((C_4 \times C_2) \times C_2)$ .*

## REFERENCES

- [1] R. Ablamowicz, *On the structure of ternary Clifford algebras and their irreducible representations*, Adv. Appl. Clifford Algebr. **32** (2022), 39.
- [2] J. Bagger and N. Lambert, *Gauge symmetry and supersymmetry of multiple M2-branes*, Phys. Rev. **D77** (2008), 065008.
- [3] D. Bohle and W. Werner, *A K-theoretic approach to the classification of symmetric spaces*, J. Pure and App. Algebra **219** (2015), 4295–4321.
- [4] N. Celakoski, *On  $(F, G)$ -rings*, God. Zb., Mat. Fak. Univ. Kiril Metodij Skopje **28** (1977), 5–15.
- [5] G. Crombez, *The Post coset theorem for  $(n, m)$ -rings*, Ist. Veneto Sci. Lett. Arti, Atti, Cl. Sci. Mat. Natur. **131** (1973), 1–7.
- [6] G. Crombez and J. Timm, *On  $(n, m)$ -quotient rings*, Abh. Math. Semin. Univ. Hamb. **37** (1972), 200–203.
- [7] J. de Azcarraga and J. M. Izquierdo,  *$n$ -Ary algebras: A review with applications*, J. Phys. **A43** (2010), 293001.
- [8] W. Dörnte, *Untersuchungen über einen verallgemeinerten Gruppenbegriff*, Math. Z. **29** (1929), 1–19.
- [9] S. Duplij, *Polyadic Algebraic Structures*, IOP Publishing, Bristol, 2022.
- [10] S. Duplij and W. Werner, *Structure of unital 3-fields*, Math. Semesterber. **68** (2021), 27–53.
- [11] H. A. Elgendy and M. R. Bremner, *Universal associative envelopes of  $(n+1)$ -dimensional  $n$ -Lie algebras*, Commun. Algebra **40** (2012), 1827–1842.
- [12] P. M. Higgins, *Completely semisimple semigroups and epimorphisms*, Proc. Amer. Math. Soc. **96** (1986), 387–390.
- [13] R. Kerner, *Ternary algebraic structures and their applications in physics*, in 23rd International Colloquium on Group Theoretical Methods in Physics, (V. Dobrev, A. Inomata, G. Pogosyan, L. Mardoyan, and A. Sisakyan, eds.), Joint Inst. Nucl. Res., JINR Publishing, Dubna, 2000 (arXiv preprint: math-ph/0011023).
- [14] R. Kerner, *A  $Z_3$  generalization of Pauli’s principle, quark algebra and the Lorentz invariance*, in The Sixth International School on Field Theory and Gravitation, (J. Alves Rodrigues, Waldyr, R. Kerner, G. O. Pires, and C. Pinheiro, eds.), Vol. 1483 of *AIP Conference Series*, 2012, pp. 144–168.
- [15] A. G. Kurosh, *Multioperator rings and algebras*, Russian Math. Surveys **24** (1969), 1–13.
- [16] J. J. Leeson and A. T. Butson, *On the general theory of  $(m, n)$  rings.*, Algebra Univers. **11** (1980), 42–76.
- [17] Y. Nambu, *Generalized Hamiltonian dynamics*, Phys. Rev. **7** (1973), 2405–2412.
- [18] E. L. Post, *Polyadic groups*, Trans. Amer. Math. Soc. **48** (1940), 208–350.

CENTER FOR INFORMATION TECHNOLOGY (WWU IT), WESTFÄLISCHE WILHELMS-UNIVERSITÄT MÜNSTER, RÖNTGENSTRASSE 7-13, D-48149 MÜNSTER, GERMANY

*Email address:* douplii@uni-muenster.de, sduplij@gmail.com

MATHEMATISCHES INSTITUT, WESTFÄLISCHE WILHELMS-UNIVERSITÄT MÜNSTER, EINSTEINSTRASSE 62, D-48149 MÜNSTER, GERMANY