Finite dimensional factor algebras of $\mathbb{F}_2[X_1, \ldots, X_n]$ and their fixed point subalgebras

Miroslav Kureš
Institute of Mathematics
Brno University of Technology
Brno, Czech Republic
kures@fme.vutbr.cz

Abstract—Fixed point subalgebras of finite dimensional factor algebras of polynomials in $n$ indeterminates over the finite field $\mathbb{F}_2$ (with respect to all $\mathbb{F}_2$-algebra automorphisms) are fully described.

Keywords—polynomial; finite field; group of automorphisms; fixed point

I. INTRODUCTION

In [6], we consider local commutative $\mathbb{R}$-algebra $A$ with identity, the nilpotent ideal $n$, of which has a finite dimension as a vector space and $A/n = \mathbb{R}$ and study its subalgebra $SA$ of fixed elements, $SA = \{a \in A; \phi(a) = a \text{ for all } \phi \in \text{Aut}_{\mathbb{R}}A\}$, where $\text{Aut}_{\mathbb{R}}A$ is the group of $\mathbb{R}$-automorphisms of the algebra $A$. This research is motivated by differential geometry, where algebras in question are usually called Weil algebras and, in particular, the bijection between all natural operators lifting vector fields from $m$-dimensional manifolds to bundles of Weil contact elements and the subalgebra of fixed points $SA$ of a Weil algebra $A$ was determined (in [4]). Although in the known geometrically motivated examples is usually $SA = \mathbb{R}$ (such $SA$ is called trivial), there are some algebras for which $SA$ is a proper superset of $\mathbb{R}$ and they call attention to the geometry of corresponding bundles. Thus, the fundamental problem is a classification of algebras having $SA$ nontrivial. See [4], [5] for related geometric questions and the survey paper [8] for known results up to now, especially for a number of claims concerning the form of subalgebras of fixed points of various Weil algebras.

In this paper, we simply replace $\mathbb{R}$ by $\mathbb{F}_2$ and study quite analogous questions. We come to a different situation by this: mainly, factor rings are finite rings (see [1]) and there is the whole theory about this topic. It is known the ring automorphism problem lying in a decision if a finite ring has a non-identical automorphism or not. Results about fixed point subalgebras are also qualitatively totally different from the real case and they can have interesting applications in the coding theory and cryptography.

II. POLYNOMIALS OVER $\mathbb{F}_2$

Polynomials in $n$ indeterminates over $\mathbb{F}_2$ are the maps of the type

$$a: \mathbb{N}_0^n \to \mathbb{F}_2,$$

i.e. a multiindex maps onto an element of $\mathbb{F}_2$; the support of the map must be by definition finite. We define the addition of polynomials and the multiplication of polynomials by the usual way and use also the standard denotation for them. However, we consider only polynomials in this paper and not their evaluations (polynomial maps); the fatal inaccuracy of such a confusion is explained e.g. in [7]. With the mentioned operations, polynomials over $\mathbb{F}_2$ form the ring denoted by $\mathbb{F}_2[X_1, \ldots, X_n]$ or shortly by $\mathbb{F}_2[X]$.

II.1. Ideals in $\mathbb{F}_2[X]$ 

The (unique) maximal ideal of $\mathbb{F}_2[X]$ is

$$m = (X_1, \ldots, X_n).$$

Powers of $m$ represent notable class of ideals.

We mention another important ideal. For finite fields $\mathbb{F}_q$, the field ideal in $\mathbb{F}_q[X_1, \ldots, X_n]$ is defined as

$$f = (X_1^q - X_1, \ldots, X_n^q - X_n).$$

Thus, we have

$$f = (X_1^2 + X_1, \ldots, X_n^2 + X_n).$$

for $q = 2$.

III. ALGEBRAS $(D_2)_r$

In this section, we will study factor rings

$$(D_2)_r = \mathbb{F}_2[X_1, \ldots, X_n] / \mathfrak{m}^r,$$

where $r \in \mathbb{N}$.

III.1. Dual numbers over $\mathbb{F}_2$

As $D = \mathbb{R}[X] / (X^2)$ is usually called the algebra of dual numbers (which is definable promptly by $D = \{a_0 + a_1X; a_0, a_1 \in \mathbb{R}, X^2 = 0\}$), we obtain for $r = n = 1$

$$D_2 = (D_2)_1 = \mathbb{F}_2[X] / (X^2)$$

the algebra of dual numbers over $\mathbb{F}_2$. Elements of $D_2$ are expressible in the form

$$a_0 + a_1X; a_0, a_1 \in \mathbb{F}_2, X^2 = 0.$$
We observe that $D_2$ has the following additive and multiplicative tables:

| +  | 0  | 1  | X  | 1+X |
|----|----|----|----|-----|
| 0  | 0  | 1  | X  | 1+X |
| 1  | 1  | 0  | 1+X| X   |
| X  | X  | 1+X| 0  | 1   |
| 1+X| 1+X| X  | 1  | 0   |

As to classification of B. Fine, [2], this finite ring can be expressed as

$$(a, b; 2a = 2b = 0, a^2 = 0, b^2 = h, ab = a, ba = a).$$

(the case denoted by 'G' in [2]).

Furthermore, in [3] is presented that dual numbers over $F_2$, complex numbers over $F_2$ and paracomplex numbers over $F_2$ are isomorphic rings. We find easily the following result. (Analogously to the real case, by the subalgebra of fixed elements $SA$ of an $F_2$-algebra $A$ we mean the subalgebra of all elements $a$ such that $\phi(a) = a$ for all $F_2$-automorphisms $\phi$ of $A$ and if $S = F_2$, we call $A$ trivial.)

**PROPOSITION 1.** The group of all $F_2$-automorphisms of $D_2$ is trivial. It follows that for $A = D_2$ is $SA$ nontrivial as $SA = A$.

**PROOF.** Let $\phi$ be an $F_2$-automorphism of $D_2$. As $\phi(1) = 1$, $\phi$ is fully determined by a specification of $\phi(X)$. In general,

$$\phi(X) = b_0 + b_1X, b_0, b_1 \in F_2.$$

However, we have

$$0 = \phi(0) = \phi(X^2) = \phi(X) \phi(X) = b_0^2 + b_1^2X^2 = b_2^2,$$

thus, $b_0 = 0$, then, necessarily, $b_1 = 1$ for $\phi$ be a bijection. So, the group of all $F_2$-automorphisms of $D_2$ contains only one element: the identical automorphism. Then the rest of the claim becomes evident.

**III.2. The case $r > 1$, $n = 1$**

Elements of the algebra $(D_2)^r = (D_2)^r_1 = F_2[X_1, ..., X_n] / m^{r+1} = F_2[X] / (X^{r+1})$ have a form

$$a_0 + a_1X + a_2X^2 + ... + a_rX^r; a_0, a_1, a_2, ..., a_r \in F_2, X^{r+1} = 0.$$

We start with the following lemma.

**LEMMA 1.** Every endomorphism $\varphi$ of $(D_2)^r \rightarrow (D_2)^r$ determined by

$$\varphi(1) = 1$$
$$\varphi(X) = X + b_2X^2 + ... + b_rX^r; b_2, ..., b_r \in F_2$$

belongs to the group of all $F_2$-automorphisms of $(D_2)^r$.

**PROOF.** It suffices to describe $\varphi^{-1}$: we have

$$Y = \varphi(X) = X + b_2X^2 + ... + b_rX^r$$

$$Y^r = X^{r+1} + \text{terms of degree } > r-1$$

The last equation provides $X$ by $Y$'s, the last but one provides (after the substitution) $X^{-1}$ and so on.

We recall that $n$ denotes the ideal of nilpotent elements of $A$ (niradical of $A$). If an element $a \in A$ has the property $a^n = 0$ for all $a \in n$, we call $a$ the socle element of $A$. It is easy to find that all socle elements constitute an ideal; this ideal is called the socle of $A$ and denoted by $soc(A)$. Now, we can formulate the main result about automorphisms of $(D_2)^r$ including also the case $r = 1$.

**PROPOSITION 2.** For $r \in N$, let $A = (D_2)^r$. Every automorphism $\varphi: A \rightarrow A$ has a form

$$\varphi(1) = 1$$
$$\varphi(X) = X + b_2X^2 + ... + b_rX^r; b_2, ..., b_r \in F_2$$

It follows $SA$ is always nontrivial, in particular $soc(A) \subseteq SA$.

**PROOF.** It is evident that the endomorphism

$$\varphi(1) = 1$$
$$\varphi(X) = X + b_2X^2 + ... + b_rX^r; b_2, ..., b_r \in F_2$$

does not represent an automorphism. Further, $soc((D_2)^r) = \{aX^r; a \in F_2\}$ and $\varphi(X^r) = X^r$ was demonstrated already in the previous lemma.

**III.3. The case $r = 1$, $n > 1$**

Elements of the algebra $(D_2)_n = (D_2)_n^1 = F_2[X_1, ..., X_n] / m^2 = F_2[X_1, ..., X_n] / (X_1, ..., X_n)^2$ have a form

$$a_0 + a_1X_1 + a_2X_2 + ... + a_nX_n; a_0, a_1, a_2, ..., a_n \in F_2, X_iX_j = 0 \text{ for all } i, j \in \{1, ..., n\}.$$

**PROPOSITION 3.** The group of all $F_2$-automorphisms of $(D_2)_n$ is isomorphic to the general linear group $GL(n, F_2)$ of the order $n$ over $F_2$.

**PROOF.** A general form of endomorphisms of $(D_2)_n$ is

$$\varphi(1) = 1$$
$$\varphi(X_1) = b_{10} + b_{11}X_1 + b_{12}X_2 + ... + b_{1n}X_n$$
$$\varphi(X_2) = b_{20} + b_{21}X_1 + b_{22}X_2 + ... + b_{2n}X_n$$

$$\varphi(X_n) = b_{n0} + b_{n1}X_1 + b_{n2}X_2 + ... + b_{nn}X_n.$$

However, we have

$$0 = \varphi(0) = \varphi(X_i^2) = \varphi(X_i \varphi(X_i)) = b_{i0}^2 + b_{i1}^2X_i^2 + ... + b_{in}^2X_n^2 = b_{i0}^2,$$

thus, $b_{i0} = 0$, and analogously, $b_{i2} = ... = b_{i(n-1)} = 0$. Now, the matrix $(b_{ij})$ must be invertible for $\varphi$ be a bijection. So, automorphisms of $(D_2)_n$ corresponds exactly with the group $GL(n, F_2)$. \(\square\)
III.4. The case $r > 1$, let $\text{SA}$ of fixed points of $A$ is always trivial.

PROOF. It is clear that $\phi_{\langle i, j \rangle}$ meets the form from the proof of the previous proposition.

REMARK 1. We remark that the order of $\text{GL}(n, 2)$ is $\Pi_{i=0}^{n-1}(2^n-2)$.

PROPOSITION 4. For $n \in \mathbb{N}$, $n > 1$, let $A = (\mathbb{D}_2)_n$. Then the subalgebra $\text{SA}$ of fixed points of $A$ is always trivial.

PROOF. First, we prove that the element $X_1 + X_2 + \ldots + X_n$

is not fixed. For this, it suffices to take some automorphism $\phi_{\langle i, j \rangle}$, e.g. $\phi_{\langle i, j \rangle}$ sends $X_1 + X_2 + \ldots + X_n$ onto $X_1 + X_2 + \ldots + X_n$. Second, let $\{k_1, \ldots, k_h\}$ be a (non-empty) proper subset of $\{1, \ldots, n\}$, i.e. $h < n$. We prove that the element

$X_1 + X_2 + \ldots + X_{k_1} + X_{k_2} + \ldots + X_{k_h}$

is not fixed, too. We take $i \in \{k_1, \ldots, k_h\}$ and $j \in \{1, \ldots, n\}$ = $\{k_1, \ldots, k_h\}$ and apply $\phi_{\langle i, j \rangle}$: it sends $X_{k_1} + X_{k_2} + \ldots + X_{k_h}$ onto $X_{k_1} + X_{k_2} + \ldots + X_{k_h} + X_1$. So, $\text{SA} = \mathbb{F}_2$.

III.5. Summary

The previous assertions provide the following summary theorem ($r, n \in \mathbb{N}$).

THEOREM. The subalgebra $\text{SA}$ of fixed points of $A = (\mathbb{D}_2)_n$ is nontrivial if and only if $n = 1$.

REFERENCES

[1] G. Bini and F. Flamini, Finite Commutative Rings and Their Applications, Kluwer Academic Publishers 2002.
[2] B. Fine, “Classification of finite rings of order $p^2$,” Mathematics Magazine 66, No. 4, 1993, pp. 248–252.
[3] J. Hrdina, M. Kureš and P. Vašik, “A note on tame polynomial automorphisms and the security of TTM cryptosystem,” Applied and Computational Mathematics 9, No. 2, 2010, pp. 226–233.
[4] M. Kureš and W. M. Mikulski, “Natural operators lifting vector fields to bundles of Weil contact elements,” Czechoslovak Mathematical Journal 54 (129), 2004, pp. 855–867.
[5] M. Kureš and W. M. Mikulski, “Natural operators lifting 1-forms to bundles of Weil contact elements,” Bulletin of the Irish Mathematical Society 49, 2002, pp. 23–41.
[6] M. Kureš and D. Sehnal, “The order of algebras with nontrivial fixed point subalgebras,” Lobachevskii Journal of Mathematics 25, 2007, pp. 187–198.
[7] M. Kureš, “The composition of polynomials by the substitution principle,” Journal of Discrete Mathematical Sciences & Cryptography 13, No. 6, 2010, pp. 543–552.
[8] M. Kureš, “Fixed point subalgebras of Weil algebras: from geometric to algebraic questions,” in Complex and Differential Geometry, Springer Proceedings of Mathematics 2011, pp. 183–192.