BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(77), 2015, Pages 3–12
ISSN 1024–7696

On fixed point subalgebras of some local algebras over a field

Miroslav Kureš

Abstract. Fixed point subalgebras of some local algebras obtained as quotients of polynomial algebras over an arbitrary field F with respect to all F-algebra automorphisms are described.

Mathematics subject classification: 13H99, 16W20. Secondary 58A20, 58A32.
Keywords and phrases: Local algebra over a field, fixed point subalgebra.

Introduction

The notion of infinitely near points was initially part of the intuitive foundations of differential calculus. In the simplest terms, two points which lie at an infinitesimal distance apart are considered infinitely near [17]. Charles Ehresmann influenced by language of Taylor polynomials (which precised the infinite nearness in calculus) introduced the concept of r-jet in his paper [2] (1951). According to this, jets of smooth mappings are defined as equivalence classes of mappings. Presumably it was Ehresmann's initiative which stimulated the paper of André Weil [16] in which Weil, being experienced from his previous algebraic geometry research in the use of methods of commutative algebra, introduced the concept of infinitely near points on a smooth manifold as algebra homomorphisms from the algebra of smooth real functions on the manifold into a local $\mathbb{R}$-algebra (which is now called the Weil algebra).

The *Weil algebra* is defined as local commutative (and associative) $\mathbb{R}$-algebra A with identity, the nilpotent ideal $\mathfrak{n}_A$ of which has a finite dimension as a vector space and $A/\mathfrak{n}_A = \mathbb{R}$. André Weil in [15] commented on non-semisimple finite dimensional algebras that "*. . . on sait qu'on ne sait rien sur cette sorte d'algèbre*"; and Shafarevich in [13] noted that Weil's observation retains its validity up to this days. We remark also that the ideas about Weil algebras enter into models for synthetic differential geometry. Disentangling structures from geometric phenomena to their categorical formulation was a long process and it is described in [11].

It is well known that the *differential invariant* is defined as a G^r_n-equivariant mapping $f\colon Y \to Z$ from a G^r_n-manifold Y into a G^r_n-manifold Z (see [4]), where $G^r_n = \operatorname{inv} J^r_0(\mathbb{R}^n, \mathbb{R}^n)_0$ (invertible r-th order jets from $\mathbb{R}^n$ into $\mathbb{R}^n$ with source and target in $0 = (0, \dots, 0)$); G^r_n is a Lie group (called usually the *jet group* or the *differential group*), Y and Z are manifolds endowed with the left action of G^r_n and

$f(gy) = gf(y)$. However, G_n^r is (isomorphic to) the group of $\mathbb{R}$-algebra automorphisms of the Weil algebra $\mathbb{D}_n^r = \mathbb{R}[X_1, \dots, X_n]/\mathfrak{m}^{r+1}$, where $\mathfrak{m}$ is the maximal ideal in the algebra of real polynomials in n indeterminates. The group G_n^r can be generalized to $\mathrm{Aut}_{\mathbb{R}} A$ for an arbitrary Weil algebra A and $\mathrm{Aut}_{\mathbb{R}} A$ is, of course, a Lie group, too. The study of differential invariants has many applications: differential invariants completely characterize invariants systems of differential equations as well as invariant variational principles, see the monograph [12] of Peter J. Olver.

The study of the subalgebra $SA = \{a \in A; \phi(a) = a \text{ for all } \phi \in \mathrm{Aut}_{\mathbb{R}} A\}$ of a Weil algebra A, is motivated by some classifications problems in differential geometry, in particular, in the classification of all natural operators lifting vector fields from m-dimensional manifolds to bundles of Weil contact elements which was solved in [5]. Although in the known geometrically motivated examples is usually $SA = \mathbb{R}$ (such SA is called *trivial*), there are some algebras for which $SA \supsetneqq \mathbb{R}$ and they call attention to the geometry of corresponding bundles. Thus, the fundamental problem is a classification of algebras having SA nontrivial. In this paper, we study only the group of automorphisms of $\mathbb{D}_n^r$; nevertheless we replace $\mathbb{R}$ by an arbitrary field F and obtain new results — we come to a different situation in particular cases: for finite fields the considered algebras are *finite rings* and there is the whole theory about this topic. It is known the *ring automorphism problem* liying 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, for the finite fields, they can have interesting applications in the coding theory and cryptography.

In the first section, we recall the real case and all definitions. The second section is devoted to local algebras of the first order: so called dual numbers and their generalizations plural numbers. Groups in question are general linear groups. The higher order case is studied in the third section. Corresponding groups of automorphisms are called (in the real case) jet groups. Possible applications are mentioned in the last section.

1 The real field: Weil algebras and jet groups

We recall that the *Weil algebra* is a local commutative $\mathbb{R}$-algebra A with identity, the nilradical (nilpotent ideal) $\mathfrak{n}_A$ of which has a finite dimension as a vector space and $A/\mathfrak{n}_A = \mathbb{R}$. Then we call the *order* of A the minimum $\mathrm{ord}(A)$ of the integers r satisfying $\mathfrak{n}_A^{r+1} = 0$ and the *width* $\mathrm{w}(A)$ of A the dimension $\dim_{\mathbb{R}}(\mathfrak{n}_A/\mathfrak{n}_A^2)$.

One can assume A is expressed as a finite dimensional quotient of the algebra $\mathbb{R}[X_1, \dots, X_n]$ of real polynomials in several indeterminates. Thus, the main example is

$$\mathbb{D}_n^r = \mathbb{R}[X_1, \dots, X_n]/\mathfrak{m}^{r+1},$$

$\mathfrak{m} = (X_1, \dots, X_n)$ being the maximal ideal of $\mathbb{R}[X_1, \dots, X_n]$ and we observe that $\mathrm{ord}(\mathbb{D}_n^r) = r$ and $\mathrm{w}(\mathbb{D}_n^r) = n$. Every other such algebra A of order r can be expressed in a form

$$A = \mathbb{R}[X_1, \dots, X_n]/\mathfrak{j} = \mathbb{R}[X_1, \dots, X_n]/\mathfrak{i} + \mathfrak{m}^{r+1},$$

where the ideal $\mathfrak{i}$ satisfies $\mathfrak{m}^{r+1} \subsetneqq \mathfrak{i} \subseteq \mathfrak{m}^2$ and is generated by a finite number of polynomials. The fact $\mathfrak{i} \subseteq \mathfrak{m}^2$ implies that the width of A is n as well. Clearly, A can be expressed also as

$$A = \mathbb{D}^r_n/\mathfrak{i},$$

where $\mathfrak{i}$ is an ideal in $\mathbb{D}^r_n$.

As to the group of automorphisms $\mathrm{Aut}_{\mathbb{R}} A$ of the algebra A, which is studied in this paper, we recall the well known fact (see [3]) that

$$\mathrm{Aut}_{\mathbb{R}} \mathbb{D}^r_n = G^r_n,$$

the *n-dimensional jet (differential) group of the order r*.

By a *fixed point* of A we mean every $a \in A$ satisfying $\phi(a) = a$ for all $\phi \in \mathrm{Aut}_{\mathbb{R}} A$. Let

$$SA = \{a \in A; \phi(a) = a \text{ for all } \phi \in \mathrm{Aut}_{\mathbb{R}} A\}$$

be the set of all fixed points of A. It is clear, that SA is a subalgebra of A containing constants (of couse, every automorphism sends 1 into 1), i.e. $SA \supseteq \mathbb{R}$. If $SA = \mathbb{R}$, we say that SA is *trivial*. For some classification results, see [8] and [9].

We will use the same terminology below although we will not focus only on the real field [1].

2 Dual and plural numbers

2.1 Dual numbers

Let F be an arbitrary field and $F[X]$ the ring of polynomials over F. Then $F[X]$ is an F-algebra thanks to the ring homomorphism mapping elements of F to constant polynomials in $F[X]$. The indeterminate X generates the maximal ideal (X) in $F[X]$. The quotient

$$\mathbb{D}_F = F[X]/(X)^2$$

is also an F-algebra and it is usually called the *algebra of dual numbers over F*. Then $\mathbb{D}_F$ has the unique maximal ideal generated by X (and so $\mathbb{D}_F$ is local). We can express $\mathbb{D}_F$ by

$$\mathbb{D}_F = \{a_0 + a_1X;\ a_0, a_1 \in F,\ X^2 = 0\}.$$

We will describe automorphisms of $\mathbb{D}_F$. For every such an automorphism ϕ

$$\phi(1_F) = 1_F$$

[1] In algebraic literature, there exists also the denotation $A^{\mathrm{Aut}_F A}$ for our SA assuming A is an F-algebra over a field F. Following [14], we can say that A is a *Galois extension* of F with *Galois group* $\mathrm{Aut}_F A$ if $F = A^{\mathrm{Aut}_F A}$. (This does not quite correspond with the definition in [14] where the Galois group is considered finite.) Then the problem of a triviality of SA identifies with the problem whether A is a Galois extension of F (with Galois group $\mathrm{Aut}_F A$) or not.

is satisfied and thus

$$\phi(a_0) = a_0 \text{ for every } a_0 \in F.$$

Further, in general,

$$\phi(X) = b_0 + b_1 X;\ b_0, b_1 \in F.$$

We compute

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

thus, by a comparing of coefficients standing at 1 at X, $b_0 = 0$, then, necessarily, b_1 must be invertible and thus non-zero for ϕ be a bijection.

Proposition 1. *Let $A = \mathbb{D}_F$. Then SA is nontrivial if and only if $F = \mathbb{F}_2$.*

Proof. We have derived that every automorphism ϕ acts by

$$\phi(a_0 + a_1 X) = a_0 + b_1 a_1 X;\ b_1 \in F - \{0_F\}.$$

Hence elements $a_1 X$ are fixed if and only if $b_1 = 1_F$: so we must have a field with only two elements 0_F and 1_F for it. □

2.2 Plural numbers

It is easy to generalize the concept of dual numbers to the quotient of the polynomial F-algebra in n indeterminates. We take the F-algebra

$$(\mathbb{D}_F)_n = F[X_1, \dots, X_n]/(X_1, \dots, X_n)^2$$

and call this F-algebra the *algebra of plural numbers over F*.

A general form of endomorphisms of $(\mathbb{D}_F)_n$ is

$$\begin{aligned} \phi(1) &= 1 \\ \phi(X_1) &= b_{10} + b_{11}X_1 + b_{12}X_2 + \cdots + b_{1n}X_n \\ \phi(X_2) &= b_{20} + b_{21}X_1 + b_{22}X_2 + \cdots + b_{2n}X_n \\ &\dots \\ \phi(X_n) &= b_{n0} + b_{n1}X_1 + b_{n2}X_2 + \cdots + b_{nn}X_n. \end{aligned}$$

However, we have

$$\begin{aligned} 0_F = {} & \phi(0_F) = \phi(X_1^2) = b_{10}^2 + b_{11}^2 X_1^2 + \cdots + b_{1n}^2 X_n^2 + 2b_{10}b_{11}X_1 + \cdots + 2b_{10}b_{1n}X_n = \\ & b_{10}(b_{10} + 2b_{11}X_1 + \cdots + 2b_{1n}X_n), \end{aligned}$$

thus, $b_{10} = 0$, and analogously $b_{20} = \cdots = b_{n0} = 0$. Now, the matrix $\begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{pmatrix}$ must be invertible for ϕ be a bijection. So, automorphisms of $(\mathbb{D}_F)_n$ form exactly the group $\mathrm{GL}(n, F)$.

Remark 1. General linear groups are widely studied. Especially, for the finite case, the order of $GL(n, \mathbb{F}_{p^k})$ (p a prime number, $k \in \mathbb{N}$) is

$$\prod_{i=0}^{n-1} \left(p^{nk} - p^{ik} \right).$$

Proposition 2. *Let $n \in \mathbb{N}$, $n > 2$, $A = (\mathbb{D}_F)_n$. Then SA is always trivial.*

Proof. We show that the element $a = a_1 X_1 + \cdots + a_n X_n$ cannot be fixed. Of course, we can assume that one of a_i, say a_1, is non-zero. Let us consider the (diagonal) automorphism ϕ

$$\begin{array}{rcl} \phi(1_F) & = & 1_F \\ \phi(X_1) & = & bX_1 \\ \phi(X_2) & = & X_2 \\ & \cdots & \\ \phi(X_n) & = & X_n, \qquad \text{where } b \neq 0_F. \end{array}$$

Let us first suppose that $b \neq 1_F$. Then evidently $\phi(a) \neq a$. However, we have not always a possibility to take $b \neq 1_F$. It occurs in the case $F = \mathbb{F}_2$.

So, in the rest of this proof, let $F = \mathbb{F}_2$. Let $i, j \in \{1, \ldots, n\}$, $i \neq j$. Then $\phi_{(i,j)} \colon (\mathbb{D}_2)_n \to (\mathbb{D}_2)_n$ given by

$$\begin{array}{rcl} \phi_{(i,j)}(1) & = & 1 \\ \phi_{(i,j)}(X_i) & = & X_i + X_j \\ \phi_{(i,j)}(X_k) & = & X_k \text{ for all } k \in \{1, \ldots, n\}, k \neq i \end{array}$$

belongs to $\mathrm{Aut}_{\mathbb{F}_2} (\mathbb{D}_{\mathbb{F}_2})_n$ becasue it is clear that $\phi_{(i,j)}$ meets the general form above. First, let us suppose that $a_1 = \cdots = a_n = 1$ and prove that the element

$$X_1 + X_2 + \cdots + X_n$$

is not fixed. For this, it suffices to take some automorphism $\phi_{(i,j)}$, e.g. $\phi_{(1,2)}$ sends $X_1 + X_2 + \cdots + X_n$ onto $X_1 + X_2 + X_2 + X_3 + \cdots + X_n = X_1 + X_3 + \cdots + X_n$. 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

$$X_{k_1} + X_{k_2} \cdots + X_{k_h}$$

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 $\phi_{(i,j)}$: it sends $X_{k_1} + X_{k_2} \cdots + X_{k_h}$ onto $X_{k_1} + X_{k_2} \cdots + X_{k_h} + X_j$.

So, $SA = F$ is always trivial. □

3 Higher order case

3.1 One indeterminate

Of course, the powers of the maximal ideal (X) represent notable class of ideals in $\mathbb{D}_F$. For $r \in \mathbb{N}$, $r > 1$, we will study the algebra

$$(\mathbb{D}_F)^r = F[X]/(X)^{r+1}.$$

Elements of $(\mathbb{D}_F)^r$ have a form

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

We start with the following lemma.

Lemma 1. *Automorphisms* $\phi\colon (\mathbb{D}_F)^r \to (\mathbb{D}_F)^r$ *have a form*

$$\begin{array}{rcl} \phi(1) & = & 1 \\ \phi(X) & = & b_1X + b_2X^2 + \cdots + b_rX^r;\ b_1 \in F - \{0_F\},\ b_2, \ldots, b_r \in F. \end{array}$$

Proof. It suffices to describe ϕ^{-1}. We have

$$\begin{array}{rcl} Y & = & \phi(X) = b_1X + b_2X^2 + \cdots + b_rX^r \\ Y^2 & = & b_1^2X^2 + \text{terms of degree} > 2 \\ & & \ldots \\ Y^{r-1} & = & b_1^{r-1}X^{r-1} + \text{a term of degree } r \\ Y^r & = & b_1^rX^r \end{array}$$

The last equation provides X^r as $b_1^{-r}Y^r$, the last but one provides (after the substitution) X^{r-1} and so on.

On the other hand, we cannot allow any more general form of automorphisms: it is evident if we consider an endomorphism

$$\begin{array}{rcl} \phi(1) & = & 1 \\ \phi(X) & = & b_1X + b_2X^2 + \cdots + b_rX^r \end{array}$$

with $b_1 = 0$ that its kernel is nontrivial and hence does not represent an automorphism. □

For an F-algebra A in question and its nilradical $\mathfrak{n}_A$, if an element $a \in A$ has the property $au = 0$ for all $u \in \mathfrak{n}_A$, 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 $\operatorname{soc} A$.

Lemma 2. *Let p be a prime number, $k \in \mathbb{N}$, $F = \mathbb{F}_{p^k}$ the finite field, $l \in \mathbb{N}$, $r = l(p^k - 1)$. Then for $A = (\mathbb{D}_F)^r$ all elements in* $\operatorname{soc} A$ *belong to SA.*

Proof. It is well known that for every $x \in F$, $x \neq 0$ the equality

$$x^{p^k-1} = 1$$

holds (the generalization of Little's Fermat Theorem for finite fields). As $X^r \in \operatorname{soc} A$ maps onto $b_1^r X^r$, for r which is the l-multiple of $p^k - 1$ is $b_1^r = 1$. □

Example 1. Let us consider $A = (\mathbb{D}_{\mathbb{F}_2})^3$. Then the element $a = X^2 + X^3$ belongs to SA. We compute

$$\phi(X^2 + X^3) = X^2 + b_2X^3 + b_2X^3 + X^3 = X^2 + X^3$$

and we see that a is fixed. Hence there exist elements of SA not belonging to $\operatorname{soc} A$, cf. [10], Proposition 2.

Proposition 3. *Let $A = (\mathbb{D}_F)^r$. For fields of characteristic 0, SA is trivial. For finite fields, SA is nontrivial and contains* $\operatorname{soc} A$.

Proof. The proof follows directly from the previous two lemmas and their proofs. □

3.2 More indeterminates

Let us consider the n-dimensional ($n > 1$) case now. Elements of the algebra

$$A = (\mathbb{D}_F)_n^r = F[X_1, \ldots, X_n]/(X_1, \ldots, X_n)^{r+1}$$

have a form

$$\begin{aligned}
&a_0 + \\
&a_1X_1 + a_2X_2 + \cdots + a_nX_n + \\
&a_{11}X_1^2 + a_{12}X_1X_2 + \cdots + a_{nn}X_n^2 + \\
&\cdots + \\
&a_{\underbrace{1\ldots1}_{r}}X_1^r + a_{\underbrace{1\ldots12}_{r}}X_1^{r-1}X_2 + \ldots a_{\underbrace{n\ldots n}_{r}}X_n^r; \\
&\quad a_0, a_1, \ldots, a_{\underbrace{n\ldots n}_{r}} \in F.
\end{aligned}$$

On basis of previous results we can find out nature of this general case now.

Proposition 4. *For $r \in \mathbb{N}$, $n \in \mathbb{N}$, $n > 1$, let $A = (\mathbb{D}_F)_n^r$. Then the subalgebra SA of fixed points of A is always trivial.*

Proof. Obviously, elements of $\mathrm{GL}(n, F)$ represent automorphisms also for $(\mathbb{D}_F)_n^r$. Of course, not *all* automorphisms, however, these (*linear*) automorphisms suffice for our following considerations. In the proof, we use formally partial derivations $\frac{\partial}{\partial X_j}$ for an expressing whether elements of A contain X_j in some non-zero power or not.

Let $u \in A$ and let exist $i, j \in \{1, \dots, n\}$ such that $\frac{\partial u}{\partial X_i} \neq 0$ and $\frac{\partial u}{\partial X_j} = 0$. Analogously with the case $r = 1$, $n > 1$, we apply $\phi_{(i,j)}$ for the demonstration that u can not be fixed.

So, let $v \in A$ be not of such a type and let σ be a permutation of n-tuple $(X_1, \dots, X_n)$ for which $\sigma(v) \neq v$. As permutations of $(X_1, \dots, X_n)$ are also elements of $\mathrm{GL}(n, F)$, we find again that v can not be fixed.

Therefore we take $w \in A$ such that $\frac{\partial w}{\partial X_i} \neq 0$ for all $i \in \{1, \dots, n\}$ and such that does not exist any permutation of $(X_1, \dots, X_n)$ yielding a transformation of w. Nevertheless, a "symmetry" of w will be again unbalanced by $\phi_{(i,j)}$, e. g. $\phi_{(1,2)}$. Hence we have an automorphism for which not even w is fixed.

Thus, only zero power elements of A remain fixed with respect to all automorphisms: SA is trivial. □

4 Comments to applications

We do not intend go into detail in this section and define at length every mentioned concept; just informative comments are here.

4.1 The real case: Weil contact elements

Now, let M be a smooth manifold and let the Weil algebra A have width $\mathrm{w}(A) = k < m = \dim M$ and order $\mathrm{ord}(A) = r$. Every A-velocity V (see [3]) determines an underlying $\mathbb{D}^1_k$-velocity $\underline{V}$. We say V is *regular* if $\underline{V}$ is regular, i.e. having maximal rank k (in its local coordinates). Let us denote $\mathrm{reg}\, T^A M$ the open subbbundle of $T^A M$ of regular velocities on M. The *contact element of type* A or briefly the *Weil contact element* on M determined by $X \in \mathrm{reg}\, T^A M$ is the equivalence class

$$\mathrm{Aut}_{\mathbb{R}}\, A_M(X) = \{\phi(X); \phi \in \mathrm{Aut}_{\mathbb{R}}\, A\}.$$

We denote by $K^A M$ the set of all contact elements of type A on M. Then

$$K^A M = \mathrm{reg}\, T^A M / \mathrm{Aut}_{\mathbb{R}}\, A$$

has a differentiable manifold structure and $\mathrm{reg}\, T^A M \to K^A M$ is a principal fiber bundle with the structure group $\mathrm{Aut}_{\mathbb{R}}\, A$. Moreover, $K^A M$ is a generalization of the bundle of higher order contact elements $K^r_k M = \mathrm{reg}\, T^r_k M / G^r_k$ introduced by Claude Ehresmann. We remark that the local description of regular velocities and contact elements is covered by the paper [6].

We have deduced in [5] and [7] the following results:

There is a one-to-one correspondence between all natural operators lifting vector fields from m-manifolds to the bundle functor K^A of Weil contact elements and the subalgebra of fixed elements SA of A.

There is a one-to-one correspondence between all natural affinors on K^A and the subalgebra of fixed elements SA of A.

All natural operators lifting 1-forms from m-dimensional manifolds to the bundle functor K^A of Weil contact elements are classified for the case of dwindlable Weil algebras: they represent constant multiples of the vertical lifting.

4.2 The finite case: Cryptography, coding theory

Finite structures are extensively applied in cryptography. The problem of developing new public key cryptosystem had occupied the cryptographic research fields for the last decades. So called multivariate cryptosystems use polynomial automorphisms, in particular, there are known tame transformation methods using for ciphering compositions of affine automorphisms and de Jonquières automorphisms. The security of such systems is based on the difficulties in decomposition of a composed polynomial automorphism.

So, the natural modification of these public key cryptosystems is a use of local (finite) algebras instead polynomial. The role of automorphisms remains unchanged. Surely, it is important to understand the subalgebra of fixed elements (which are not transformed under any automorphism).

Example 2. As a toy exercise, we can consider $A = (\mathbb{D}_{\mathbb{F}_4})^2$ and take e.g. polynomials in two indeterminates Y_1, Y_2 over A, i.e. elements of $(\mathbb{D}_{\mathbb{F}_4})^2\,[Y_1, Y_2]$. In multivariate public key cryptosystems, the cipher procedure is based on composed polynomial automorphisms, which are used as the public key. Let us imagine a simple scheme based on the composition $\pi = \lambda_2 \circ \tau \circ \lambda_1$ of affine (λ_1 and λ_2) and de Jonquières (τ) $\mathbb{F}_4$-automorphisms which play a role of a private key. Without a decomposition of π, it is not easy to find π^{-1} which is necessary for decryption. Of course, a descryption of fixed elements is the substantial feature of such a system.

We only remark that local finite algebras are used also in the coding theory, for detail see [1].

Acknowledgment. The author was supported by the project NETME+ (LO1202) co-funded by the Ministry of Education of the Czech Republic under the National Sustainability Programme I.

References

[1] Bini G., Flamini F. *Finite Commutative Rings and Their Applications.* Kluwer Academic Publishers, 2002.

[2] Ehresmann C. *Les prolongements d'une variété différentiable, I.* CRAS Paris, 1951, **233**, 598–600.

[3] Kolář I., Michor P. W., Slovák J. *Natural Operations in Differential Geometry.* Springer Verlag, 1993.

[4] Krupka D., Janyška J. *Lectures on Differential Invariants.* Univerzita J. E. Purkyně, Brno, 1990.

[5] Kureš M., Mikulski W. M. *Natural operators lifting vector fields to bundles of Weil contact elements.* Czechoslovak Mathematical Journal, 2004, **54**, 855–867.

[6] Kureš M. *Local approach to higher order contact elements.* Reports on Mathematical Physics, 2006, **58**, No. 2, 393–409.

[7] Kureš M., Mikulski W. M. *Natural operators lifting 1-forms to bundles of Weil contact elements.* Bulletin of the Irish Mathematical Society, 2002, **49**, 23–41.

[8] Kureš M., Sehnal D. *The order of algebras with nontrivial fixed point subalgebras.* Lobachevskii Journal of Mathematics, 2007, **25**, 187–198.

[9] Kureš M. *Fixed point subalgebras of Weil algebras: from geometric to algebraic questions.* Complex and Differential Geometry, Springer Proceedings of Mathematics, 2011, 183–192.

[10] Kureš M. *Finite dimensional factor algebras of* $\mathbb{F}_2[X_1, \dots, X_n]$ *and their fixed point subalgebras.* Open Journal of Applied Sciences, **2**, Suppl. (2012) World Congress on Engineering and Technology (Beijing), 2012, 212–214.

[11] Mac Lane S. *The genesis of mathematical structures, as exemplified in the work of Charles Ehresmann.* Cahiers de Toplogie et Géométrie Différentielle Catégoriques, 1980, **21**, No. 4, 353–365.

[12] Olver P. J. *Applications of Lie Group to Differentianl Equations.* Springer, 1993.

[13] Shafarevich I. R. *Degeneration of semisimple algebras.* Communications in Algebra, 2001, **29**, No. 9, 3943–3960.

[14] Villamayor O. E. *Separable algebras and Galois extensions.* Osaka Journal of Mathematics, 1967, **4**, 161–171.

[15] Weil A. *Généralisation des fonctions abeliénnes.* Journal de Mathématiques Pures et Apliquées, 1938, **17**, 47–87.

[16] Weil A. *Théorie des points proches sur les variétés différentiables.* Géométrie différentielle, Colloques Internationaux du Centre National de la Recherche Scientifique, Strasbourg, 1953, 111–117.

[17] Wikipedia contributors. *Infintely near point.* Wikipedia, The Free Encyklopedia, September 9, 2012.

Miroslav Kureš
Institute of Mathematics
Brno University of Technology
Technická 2, 61669 Brno
Czech Republic
E-mail: *kures@fme.vutbr.cz*

Received September 16, 2014