Bulletin of the Iranian Mathematical Society Vol. 39 *No. 4* (*2013*), *pp 725-742.*

ON p-SEMILINEAR TRANSFORMATIONS

Y. MA AND L. CHEN*

Communicated by Abbas Salemi Parizi

ABSTRACT. In this paper, we introduce p-semilinear transformations for linear algebras over a field $\mathbf{F}$ of positive characteristic p, discuss initially the elementary properties of p-semilinear transformations, make use of it to give some characterizations of linear algebras over a field $\mathbf{F}$ of positive characteristic p. Moreover, we find a one-to-one correspondence between p-semilinear transformations and matrices, and we prove a result which is closely related to the well-known Jordan-Chevalley decomposition of an element.

1. **Introduction**

People have got a detailed and comprehensive presentation of linear mappings[4]. As a natural generalization of linear mappings, the theory of semilinear mappings has important applications particularly in Mathieu group[2] and projective geometry [5, 3], and the matrix representation of a semilinear mapping on $\mathbf{C}^n$ was studied in [1]. There are much fewer results in linear algebras over a field of positive characteristic p than that of characteristic 0, and some basic properties on p-semilinear mappings for restricted Lie algebras were given by Strade

MSC(2010): Primary: 22A15, 54H10; Secondary 54D55, 20M15, 20M18.
Keywords: p-semilinear transformation, the matrix; Rank-nullity theorem, Jordan-Chevalley decomposition.
Received: 15 December 2011, Accepted: 12 April 2012.
∗Corresponding author

and Farnsteiner[7]. In this paper, we introduce p-semilinear transformations for linear algebras over a field $\mathbf{F}$ of positive characteristic p, discuss initially the elementary properties of p-semilinear transformations, make use of it to give some characterizations of linear algebras over a field $\mathbf{F}$ of positive characteristic p. Moreover, we find a one-to-one correspondence between all p-semilinear transformations and matrices, and a result closely related to the Jordan-Chevalley decomposition.

We proceed as follows. In Section 2, we recall some basic definitions, examples and propositions which will be used in what follows. In Section 3, we introduce the definition of the matrix of a p-semilinear transformation and discuss the relation between it and its matrix. Then we get the Rank-nullity theorem under p-semilinear transformations and a result closely related to the Jordan-Chevalley decomposition. In the end, we show that if $\mathbf{F}$ is an algebraically closed field and f is an injective p-semilinear transformation, then there is a basis such that the matrix of f respect to it is a unit matrix.

We let V be a finite-dimensional vector space over $\mathbf{F}$, where $\mathbf{F}$ is a field of characteristic p. Our notation and terminology are standard as may be found in[4, 5, 2].

2. **Preliminaries**

Definition 2.1. *Let V and W be vector spaces over $\mathbf{F}$, and let $f : V \to W$ be a mapping. f is called a p-semilinear mapping if $f(k\alpha + \beta) = k^p f(\alpha) + f(\beta),\ \forall\ \alpha, \beta \in V,\ \forall k \in \mathbf{F}$. A p-semilinear mapping $f : V \to V$ is called a p-semilinear transformation.*

Example 2.2. *Let $\mathbf{F}$ be a field of characteristic p. Clearly, $\mathbf{F}$ is a 1-dimensional vector space over $\mathbf{F}$. Consider the mapping $f : \mathbf{F} \to \mathbf{F}$ defined by $f(x) = x^p$. Then f is a p-semilinear transformation.*

For any $x, y, a \in \mathbf{F}$, we have

$$f(ax + y) = (ax + y)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} x^{p-i} y^i.$$

Since $i\binom{p}{i} = p\binom{p}{i}$, we have $p|\binom{p}{i},\ i = 1, \cdots, p-1$. Note that char$\mathbf{F}$=$p$, then

$$\binom{p}{i} = 0,\ i = 1, \cdots, p-1.$$

So $f(ax + y) = a^p x^p + y^p = a^p f(x) + f(y)$, i.e., f is a p-semilinear transformation.

Example 2.3. *Let $M_n(\mathbf{F})$ be the set of all $n \times n$-matrices and $\mathscr{P} : M_n(\mathbf{F}) \to M_n(\mathbf{F})$ be the mapping given by*

$$\mathscr{P}(A) = A^{(p)} := (a_{ij}^p)_{n\times n}, \forall A = (a_{ij})_{n\times n} \in M_n(\mathbf{F}).$$

Then $\mathscr{P}$ is a p-semilinear transformation.

We have $\mathscr{P}(A+B) = (A+B)^{(p)} = ((a_{ij}+b_{ij})^p)_{n\times n} = (a_{ij}^p+b_{ij}^p)_{n\times n} = A^{(p)}+B^{(p)} = \mathscr{P}(A)+\mathscr{P}(B)$ and $\mathscr{P}(kA) = (kA)^{(p)} = k^p A^{(p)} = k^p \mathscr{P}(A)$. So $\mathscr{P}$ is a p-semilinear transformation.

Remark 2.4. *The p-semilinear transformation $\mathscr{P}$ in Example 2.3 has the following properties:*

(1) $\mathscr{P}(AB) = \mathscr{P}(A)\mathscr{P}(B)$;

(2) $\mathscr{P}(A^{-1}) = \mathscr{P}(A)^{-1}$, where $A \in M_n(\mathbf{F})$ is a regular matrix.

(1) Since char($\mathbf{F}$)=p and $p|\binom{p}{i}$, $i = 1, \cdots, p-1$, it follows that $k_1^p + k_2^p = (k_1+k_2)^p, \forall k_1, k_2 \in \mathbf{F}$. Then we obtain

$$\begin{aligned}
\mathscr{P}(AB) &= (AB)^{(p)} \\
&= \left(\sum_{k=1}^n a_{ik}b_{kj}\right)^{(p)}_{n\times n} \\
&= \left(\left(\sum_{k=1}^n a_{ik}b_{kj}\right)^p\right)_{n\times n} \\
&= \left(\sum_{k=1}^n a_{ik}^p b_{kj}^p\right)_{n\times n} \\
&= A^{(p)}B^{(p)} \\
&= \mathscr{P}(A)\mathscr{P}(B).
\end{aligned}$$

(2) If A is regular, then A^{-1} exists and $(A^{-1})^{(p)}A^{(p)} = (A^{-1}A)^{(p)} = E^{(p)} = E$ by (1), where E is a unit matrix. Similarly, $A^{(p)}(A^{-1})^{(p)} = E$. Hence $(A^{-1})^{(p)} = (A^{(p)})^{-1}$, i.e., $\mathscr{P}(A^{-1}) = \mathscr{P}(A)^{-1}$.

Proposition 2.5. *Suppose that V is a vector space. If $f : V \to V$ is linear and $\mathscr{A} : V \to V$ is p-semilinear, then $f\mathscr{A}$ and $\mathscr{A}f$ are p-semilinear.*

Proof. It is easy to obtain that

$$f\mathscr{A}(k\alpha+\beta) = f(k^p\mathscr{A}(\alpha)+\mathscr{A}(\beta)) = k^p f\mathscr{A}(\alpha) + f\mathscr{A}(\beta),$$

so $f\mathscr{A}$ is p-semilinear. Similarly, $\mathscr{A}f$ is p-semilinear. □

Proposition 2.6. *Let V be a vector space and the set $\mathrm{End}^p_{\mathbf{F}}(V)$ be all p-semilinear transformations. Define $(f+g)(\alpha) := f(\alpha)+g(\alpha)$ and $(k\cdot f)(\alpha) := k(f(\alpha))$, for any $f,g \in \mathrm{End}^p_{\mathbf{F}}(V)$ and $\alpha \in V$. Then $\mathrm{End}^p_{\mathbf{F}}(V)$ is a vector space.*

Proof. Since

$$\begin{aligned}(f+g)(k\alpha+\beta) &= f(k\alpha+\beta)+g(k\alpha+\beta)\\ &= k^p f(\alpha)+f(\beta)+k^p g(\alpha)+g(\beta)\\ &= k^p(f(\alpha)+g(\alpha))+(f(\alpha)+g(\alpha))\\ &= k^p(f+g)(\alpha)+(f+g)(\alpha),\end{aligned}$$

$f+g \in \mathrm{End}^p_{\mathbf{F}}(V)$.

Since

$$\begin{aligned}(k\cdot f)(l\alpha+\beta) &= k(f(l\alpha+\beta))\\ &= k(l^p f(\alpha)+f(\beta))\\ &= l^p(k\cdot f)(\alpha)+(k\cdot f)(\beta),\end{aligned}$$

$k\cdot f \in \mathrm{End}^p_{\mathbf{F}}(V)$.

Hence $\mathrm{End}^p_{\mathbf{F}}(V)$ is a vector space. □

Remark 2.7. *In general, if $f,g \in \mathrm{End}^p_{\mathbf{F}}(V)$, then $fg \notin \mathrm{End}^p_{\mathbf{F}}(V)$. Because $(fg)(k\alpha+\beta) = f(g(k\alpha+\beta)) = f(k^p g(\alpha)+g(\beta)) = k^{p^2}(fg)(\alpha) + (fg)(\beta) \neq k^p(fg)(\alpha)+(fg)(\beta)$.*

Let $\mathbf{F}^p := \{\alpha^p | \alpha \in \mathbf{F}\}$. $\mathbf{F}$ is perfect if $\mathbf{F} = \mathbf{F}^p$.

3. The matrix of p-semilinear transformations

In the sequel V is assumed to be a vector space over $\mathbf{F}$ and $\dim V = n$. Define $f^0(x) = x, \forall\, x \in V$.

Proposition 3.1. *Let $\alpha_1, \cdots, \alpha_n$ be a basis of V. Then for arbitrary n vectors $\beta_1, \cdots, \beta_n \in V$, there exists a unique p-semilinear transformation $\mathscr{A}$ such that $\mathscr{A}(\alpha_i) = \beta_i, 1 \leqslant i \leqslant n$.*

Proof. Define $\mathscr{A}: V \to V$ by

$$\mathscr{A}\left(\sum_{i=1}^n k_i\alpha_i\right) = \sum_{i=1}^n k_i^p \beta_i.$$

Then $\mathscr{A}$ satisfies

$$\mathscr{A}(\alpha_i) = \beta_i, 1 \leqslant i \leqslant n.$$

One can write any elements α, β of V as

$$\alpha = \sum_{i=1}^{n} k_i\alpha_i, \beta = \sum_{i=1}^{n} l_i\alpha_i \in V,\ k_i, l_i \in \mathbf{F},$$

then the equality

$$\begin{aligned} \mathscr{A}(k\alpha+\beta) &= \mathscr{A}\left(\sum_{i=1}^{n}(kk_i+l_i)\alpha_i\right) = \sum_{i=1}^{n}(kk_i+l_i)^p\beta_i \\ &= k^p\sum_{i=1}^{n}k_i^p\beta_i + \sum_{i=1}^{n}l_i^p\beta_i = k^p\mathscr{A}(\alpha)+\mathscr{A}(\beta) \end{aligned}$$

yields that $\mathscr{A}$ is p-semilinear.

Suppose that $\mathscr{B}: V \to V$ is p-semilinear satisfying $\mathscr{B}(\alpha_i) = \beta_i, 1 \leqslant i \leqslant n$. Then

$$\mathscr{B}\left(\sum_{i=1}^{n}k_i\alpha_i\right) = \sum_{i=1}^{n}k_i^p\beta_i = \mathscr{A}\left(\sum_{i=1}^{n}k_i\alpha_i\right)$$

implies $\mathscr{A} = \mathscr{B}$, hence $\mathscr{A}$ is uniquely determined by the conditions. □

It follows immediately from Proposition 3.1 that a p-semilinear transformation is uniquely determined by its action on a given basis.

Definition 3.2. *Let $\{\alpha_1, \cdots, \alpha_n\}$ be a basis of V and $\mathscr{A}: V \to V$ a p-semilinear transformation. Then every vector $\mathscr{A}(\alpha_i)$ can be written as a linear combination of the vectors $\{\alpha_1, \cdots, \alpha_n\}$,*

$$\mathscr{A}(\alpha_i) = \sum_{k=1}^{n} a_{ki}\alpha_k,\ 1 \leqslant i \leqslant n.$$

So $\mathscr{A}$ determines an $n\times n$-matrix $\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$, which is denoted by A. A is called the matrix of $\mathscr{A}$ respect to the basis $\alpha_1, \cdots, \alpha_n$.

Theorem 3.3. *Let $\{\alpha_1, \cdots, \alpha_n\}$ be a basis of V and $\mathscr{A}: V \to V$ a p-semilinear transformation and A the matrix of $\mathscr{A}$ with respect to the basis $\alpha_1, \cdots, \alpha_n$. Define $\varphi: End_{\mathbf{F}}^p(V) \to M_n(\mathbf{F})$ by $\varphi(\mathscr{A}) = A$, then φ is an isomorphism.*

Proof. Suppose that $\mathscr{A}, \mathscr{B} \in \mathrm{End}_{\mathbf{F}}^p(V)$ and A, B are the ... corresponding matrices respectively, then

$\varphi(\mathscr{A}) = \varphi(\mathscr{B}) \Rightarrow A = B \Rightarrow (\mathscr{A}(\alpha_1), \cdots, \mathscr{A}(\alpha_n)) = (\mathscr{B}(\alpha_1), \cdots, \mathscr{B}(\alpha_n)) \Rightarrow \mathscr{A}(\alpha_i) = \mathscr{B}(\alpha_i) \Rightarrow \mathscr{A} = \mathscr{B}$. Hence φ is injective.

For every $A \in M_n(\mathbf{F})$, it is clear that there exist $\beta_1, \cdots, \beta_n \in V$ such that $(\beta_1, \cdots, \beta_n) = (\alpha_1, \cdots, \alpha_n)A$. By the use Proposition 3.1, then there is a p-semilinear transformation $\mathscr{A}$ satisfying $\mathscr{A}(\alpha_i) = \beta_i, i = 1, \cdots, n$, hence $\varphi(\mathscr{A}) = A$, which implies that φ is surjective.

The equality

$$\begin{aligned}(k\mathscr{A} + l\mathscr{B})(\alpha_i) &= k(\mathscr{A}(\alpha_i)) + l(\mathscr{B}(\alpha_i)) \\ &= k(a_{1i}, \cdots, a_{ni}) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} + l(b_{1i}, \cdots, b_{ni}) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \\ &= (ka_{1i} + lb_{1i}, \cdots, ka_{ni} + lb_{ni}) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}\end{aligned}$$

implies that $\varphi(k\mathscr{A} + l\mathscr{B}) = kA + lB = k\varphi(\mathscr{A}) + l\varphi(\mathscr{B})$.

Therefore, φ is an isomorphism as desired. □

We now prove the following theorem that will show how the matrix of a p-semilinear transformation $\mathscr{A} : V \to V$ is changed under a basis-transformation in V. We will need

Lemma 3.4. *Let $\alpha_1, \cdots, \alpha_n$ be a basis of V and $\mathscr{A} : V \to V$ be a p-semilinear transformation and A its matrix with respect to the basis $\alpha_1, \cdots, \alpha_n$. If $\alpha = k_1\alpha_1 + \cdots + k_n\alpha_n$ and $\mathscr{A}(\alpha) = \tilde{k}_1\alpha_1 + \cdots + \tilde{k}_n\alpha_n$, where $k_i, \tilde{k}_i \in \mathbf{F}, 1 \le i \le n$, then we have*

$$(\tilde{k}_1, \cdots, \tilde{k}_n)^T = A(k_1^p, \cdots, k_n^p)^T.$$

Proof. It is easy to show that

$$\begin{aligned}\mathscr{A}(\alpha) &= \mathscr{A}(k_1\alpha_1 + \cdots + k_n\alpha_n) \\ &= k_1^p\mathscr{A}(\alpha_1) + \cdots + k_n^p\mathscr{A}(\alpha_n) \\ &= (\mathscr{A}(\alpha_1), \cdots, \mathscr{A}(\alpha_n))(k_1^p, \cdots, k_n^p)^T \\ &= (\alpha_1, \cdots, \alpha_n)A(k_1^p, \cdots, k_n^p)^T\end{aligned}$$

and $\mathscr{A}(\alpha) = \tilde{k}_1\alpha_1 + \cdots + \tilde{k}_n\alpha_n = (\alpha_1, \cdots, \alpha_n)(\tilde{k}_1, \cdots, \tilde{k}_n)^T$. So the result follows. □

Theorem 3.5. *Let $\eta_1, \cdots, \eta_n$ and $\tilde{\eta}_1, \cdots, \tilde{\eta}_n$ be two bases of V satisfying $(\tilde{\eta}_1, \cdots, \tilde{\eta}_n) = (\eta_1, \cdots, \eta_n)T$, where $T \in M_n(\mathbf{F})$ is nonsingular. Suppose* *that the matrices of a p-semilinear transformation $\mathscr{A}$ with respect to the above bases are A and $\tilde{A}$ respectively, then*

$$\tilde{A} = T^{-1}AT^{(p)}.$$

Proof. Since $(\tilde{\eta}_1, \cdots, \tilde{\eta}_n) = (\eta_1, \cdots, \eta_n)T$, it follows from Lemma 3.4 that

$$(\mathscr{A}(\tilde{\eta}_1), \cdots, \mathscr{A}(\tilde{\eta}_n)) = (\eta_1, \cdots, \eta_n)AT^{(p)}.$$

Note that

$$(\mathscr{A}(\tilde{\eta}_1), \cdots, \mathscr{A}(\tilde{\eta}_n)) = (\tilde{\eta}_1, \cdots, \tilde{\eta}_n)\tilde{A},$$

and

$$\begin{aligned}(\mathscr{A}(\tilde{\eta}_1), \cdots, \mathscr{A}(\tilde{\eta}_n)) &= (\eta_1, \cdots, \eta_n)AT^{(p)} \\ &= (\tilde{\eta}_1, \cdots, \tilde{\eta}_n)T^{-1}AT^{(p)}.\end{aligned}$$

Thus $\tilde{A} = T^{-1}AT^{(p)}$. □

Theorem 3.6. *Let $\alpha_1, \cdots, \alpha_n$ be a basis of V and $\mathscr{A} : V \to V$ a p-semilinear transformation and $A = (a_{ij})_{n\times n}$ the matrix of $\mathscr{A}$ with respect to the basis $\alpha_1, \cdots, \alpha_n$. If there is another basis $\beta_1, \cdots, \beta_n$ such that*

$$(\beta_1, \cdots, \beta_n) = (\alpha_1, \cdots, \alpha_n)A,$$

then the following statements hold:

(1) $\beta_i = \mathscr{A}(\alpha_i), i = 1, \cdots, n$.

(2) There exists a p-semilinear transformation $\mathscr{B} : V \to V$ such that $\mathscr{B}(\beta_i) = \alpha_i$ and the matrix of $\mathscr{B}$ respect to $\alpha_1, \cdots, \alpha_n$ is $(A^{-1})^{(p)}$.

Proof. (1) It is easy.

(2) Since $\alpha_1, \cdots, \alpha_n$ and $\beta_1, \cdots, \beta_n$ are bases of V, A is nonsingular and suppose that $A^{-1} = (\tilde{a}_{ij})_{n\times n}$. Define $\mathscr{B} : V \to V$ by

$$\mathscr{B}(\sum_{i=1}^{n} k_i\alpha_i) = \sum_{i=1}^{n} k_i^p \left(\sum_{j=1}^{n} \tilde{a}_{ji}^p \alpha_j\right).$$

Then we can obtain that

$$\begin{aligned}\mathscr{B}(\beta_i) &= \mathscr{B}\left(\sum_{k=1}^{n} a_{ki}\alpha_k\right)\\ &= \sum_{k=1}^{n} a_{ki}^p \left(\sum_{j=1}^{n} \tilde{a}_{jk}^p \alpha_j\right)\\ &= \sum_{j=1}^{n}\left(\sum_{k=1}^{n} \tilde{a}_{jk}^p a_{ki}^p\right)\alpha_j\\ &= \sum_{j=1}^{n}\left(\sum_{k=1}^{n} \tilde{a}_{jk} a_{ki}\right)^p \alpha_j.\end{aligned}$$

Since

$$\sum_{k=1}^{n} \tilde{a}_{jk} a_{ki} = \delta_{ij},$$

we have

$$\mathscr{B}(\beta_i) = \sum_{j=1}^{n}\left(\sum_{k=1}^{n} \tilde{a}_{jk} a_{ki}\right)^p \alpha_j = \alpha_i.$$

Suppose that $\alpha = \sum_{i=1}^{n} k_i\alpha_i, \beta = \sum_{i=1}^{n} l_i\alpha_i \in V,\ k \in \mathbf{F}$, then the equality

$$\begin{aligned}\mathscr{B}(k\alpha+\beta) &= \mathscr{B}\left(\sum_{i=1}^{n}(kk_i + l_i)\alpha_i\right)\\ &= \sum_{i=1}^{n}(kk_i+l_i)^p\left(\sum_{j=1}^{n}\tilde{a}_{ji}^p\alpha_j\right)\\ &= k^p\sum_{i=1}^{n}k_i^p\left(\sum_{j=1}^{n}\tilde{a}_{ji}^p\alpha_j\right) + \sum_{i=1}^{n} l_i^p\left(\sum_{j=1}^{n}\tilde{a}_{ji}^p\alpha_j\right)\\ &= k^p\mathscr{B}(\alpha) + \mathscr{B}(\beta)\end{aligned}$$

shows that $\mathscr{B}$ is a p-semilinear transformation. Since

$$\mathscr{B}(\alpha_i) = \sum_{j=1}^{n}\tilde{a}_{ji}^p\alpha_j = (\alpha_1, \cdots, \alpha_n)\begin{pmatrix}\tilde{a}_{1i}^p\\ \vdots\\ \tilde{a}_{ni}^p\end{pmatrix},$$

we complete the proof. □

Proposition 3.7. *Let $\mathscr{A} : V \to V$ be a p-semilinear transformation. If $\alpha_1, \cdots, \alpha_n \in V$ are linearly dependent, then $\mathscr{A}(\alpha_1), \cdots, \mathscr{A}(\alpha_n)$ are linearly dependent.*

Proof. Since $\alpha_1, \cdots, \alpha_n \in V$ are linearly dependent, there exists a system of scalars $k_i \in \mathbf{F}$ such that

$$k_1\alpha_1 + \cdots + k_n\alpha_n = 0$$

and at least one $k_i \neq 0$, without loss of generality, we may assume that $k_1 \neq 0$. By applying $\mathscr{A}$ on the left and right side of the above identity, we obtain

$$k_1^p\mathscr{A}(\alpha_1) + \cdots + k_n^p\mathscr{A}(\alpha_n) = 0.$$

$k_1 \neq 0$ yields $k_1^p \neq 0$, so $\mathscr{A}(\alpha_1), \cdots, \mathscr{A}(\alpha_n)$ are linearly dependent. □

Lemma 3.8. *Let $\mathscr{A} : V \to V$ be a p-semilinear transformation. If $\alpha_1, \cdots, \alpha_n \in V$ are linearly independent and $\mathscr{A}$ is bijective, then $\mathscr{A}(\alpha_1), \cdots, \mathscr{A}(\alpha_n)$ are linearly independent.*

Proof. Since $\alpha_1, \cdots, \alpha_n$ are linearly independent, $\alpha_i \neq 0, i = 1, \cdots, n$. Then $\mathscr{A}(\alpha_i) \neq 0, i = 1, \cdots, n$ since $\mathscr{A}$ is injective. Suppose that $\{\mathscr{A}(\alpha_1), \cdots, \mathscr{A}(\alpha_k)\}$ is a maximal independent system in $\{\mathscr{A}(\alpha_1), \cdots, \mathscr{A}(\alpha_n)\}$.

If $k = n$, then the lemma is proved.

If $k < n$, then extend $\{\mathscr{A}(\alpha_1), \cdots, \mathscr{A}(\alpha_k)\}$ to a basis of V: $\mathscr{A}(\alpha_1)$, $\cdots$, $\mathscr{A}(\alpha_k)$, β_{k+1}, $\cdots$, β_n. Since $\mathscr{A}$ is surjective, there exist $\{\gamma_1, \cdots, \gamma_n\}$ such that $\beta_i = \mathscr{A}(\gamma_i), i = 1, \cdots, n$, which implies that $\mathscr{A}(\alpha_1), \cdots, \mathscr{A}(\alpha_k), \mathscr{A}(\gamma_{k+1}), \cdots, \mathscr{A}(\gamma_n)$ form a basis of V and hence they are linearly independent.

Proposition 3.7 shows that $\alpha_1, \cdots, \alpha_k, \gamma_{k+1}, \cdots, \gamma_n$ are linearly independent and so they form a basis of V, then we have $L(\alpha_{k+1}, \cdots, \alpha_n) = L(\gamma_{k+1}, \cdots, \gamma_n)$. Hence $\alpha_{k+1}, \cdots, \alpha_n$ can be written as

$$\alpha_i = \sum_{j=k+1}^{n} c_{ij}\gamma_j, i = k+1, \cdots, n.$$

Suppose that

$$q_1\mathscr{A}(\alpha_1) + \cdots + q_n\mathscr{A}(\alpha_n) = 0,$$

then we have

$$q_1\mathscr{A}(\alpha_1)+\cdots+q_k\mathscr{A}(\alpha_k)+q_{k+1}\mathscr{A}\left(\sum_{j=k+1}^{n}c_{k+1,j}\gamma_j\right)+\cdots+q_n\mathscr{A}\left(\sum_{j=k+1}^{n}c_{nj}\gamma_j\right)=0$$

which implies $q_1=\cdots=q_k=0$ and $q_{k+1}\mathscr{A}(\alpha_{k+1})+\cdots+q_n\mathscr{A}(\alpha_n)=0$. Now assume that $\{\mathscr{A}(\alpha_{k+1}),\cdots,\mathscr{A}(\alpha_m)\}$ is a maximal independent system in $\{\mathscr{A}(\alpha_{k+1}),\cdots,\mathscr{A}(\alpha_n)\}$.

If $m=n$, then the lemma is proved.

If $m<n$, proceed in the same way as above and we will obtain $q_{k+1}=\cdots=q_m=0$. Since n is finite, the procedure will stop in finite(at most n) steps.

Finally, we have $q_1=\cdots=q_n=0$, and so $\mathscr{A}(\alpha_1),\cdots,\mathscr{A}(\alpha_n)$ are linearly independent. □

Theorem 3.9. *Let $\alpha_1,\cdots,\alpha_n$ be a basis of V and $\mathscr{A}:V\to V$ be a p-semilinear transformation and A be its matrix with respect to the basis $\alpha_1,\cdots,\alpha_n$. If $\mathscr{A}$ is bijective, then A is nonsingular.*

Proof. It is easy to show that

$$\begin{aligned}
&k_1\mathscr{A}(\alpha_1)+\cdots+k_n\mathscr{A}(\alpha_n)=0\\
\Longleftrightarrow\quad&(\mathscr{A}(\alpha_1),\cdots,\mathscr{A}(\alpha_n))(k_1,\cdots,k_n)^T=0\\
\Longleftrightarrow\quad&(\alpha_1,\cdots,\alpha_n)A(k_1,\cdots,k_n)^T=0\\
\Longleftrightarrow\quad&A(k_1,\cdots,k_n)^T=0.
\end{aligned}$$

Since $\alpha_1,\cdots,\alpha_n$ are linearly independent and $\mathscr{A}$ is bijective, $\mathscr{A}(\alpha_1),\cdots,\mathscr{A}(\alpha_n)$ are linearly independent by Lemma 3.8. Then $k_i=0, i=1,\cdots,n$. Hence A is nonsingular. □

Theorem 3.10. *Assume that $\mathbf{F}$ is a perfect field, i.e., $\mathbf{F}=\mathbf{F}^p$. Let $\alpha_1,\cdots,\alpha_n$ be a basis of V and $\mathscr{A}:V\to V$ be a p-semilinear transformation and A be its matrix with respect to the basis $\alpha_1,\cdots,\alpha_n$. If A is nonsingular, then $\mathscr{A}$ is bijective.*

Proof. Assume that $\beta = b_1\alpha_1 + \cdots + b_n\alpha_n, \gamma = c_1\alpha_1 + \cdots + c_n\alpha_n \in V$, then

$$\begin{aligned}\mathscr{A}(\beta) &= \mathscr{A}(\gamma) \Rightarrow (\alpha_1, \cdots, \alpha_n)A\begin{pmatrix} b_1^p \\ \vdots \\ b_n^p \end{pmatrix} \\ &= (\alpha_1, \cdots, \alpha_n)A\begin{pmatrix} c_1^p \\ \vdots \\ c_n^p \end{pmatrix} \Rightarrow A\begin{pmatrix} b_1^p - c_1^p \\ \vdots \\ b_n^p - c_n^p \end{pmatrix} \\ &= 0.\end{aligned}$$

Since A is regular, $\begin{pmatrix} b_1^p - c_1^p \\ \vdots \\ b_n^p - c_n^p \end{pmatrix} = 0$. Then $b_i^p = c_i^p, i = 1, \cdots, n$, so this yields $b_i = c_i, i = 1, \cdots, n$, which implies $\beta = \gamma$. Thus, $\mathscr{A}$ is injective.

For every $\beta = b_1\alpha_1 + \cdots + b_n\alpha_n \in V$, we have

$$\begin{aligned} & \mathscr{A} \text{ is surjective} \\ \Longleftrightarrow\ & \exists\, \alpha = (\alpha_1, \cdots, \alpha_n)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in V \text{ such that } \mathscr{A}(\alpha) = \beta \\ \Longleftrightarrow\ & (\alpha_1, \cdots, \alpha_n)A\begin{pmatrix} x_1^p \\ \vdots \\ x_n^p \end{pmatrix} = (\alpha_1, \cdots, \alpha_n)\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \\ \Longleftrightarrow\ & A\begin{pmatrix} x_1^p \\ \vdots \\ x_n^p \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}.\end{aligned}$$

We have $\begin{pmatrix} x_1^p \\ \vdots \\ x_n^p \end{pmatrix} = A^{-1}\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ since A is nonsingular.

Note that $\mathbf{F} = \mathbf{F}^p$. The following statements hold:

(1) there exists $B = (b_{ij})_{n\times n}$ such that $A^{-1} = B^{(p)} = (b_{ij}^p)_{n\times n}$ and

(2) there exists c_i such that $b_i = c_i^p, i = 1, \cdots, n$.

Then we can obtain that

$$\begin{pmatrix} x_1^p \\ \vdots \\ x_n^p \end{pmatrix} = B^{(p)} \begin{pmatrix} c_1^p \\ \vdots \\ c_n^p \end{pmatrix} = \left(B \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \right)^{(p)}.$$

It follows that

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = B \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix},$$

i.e., there exists $\alpha \in V$ such that $\mathscr{A}(\alpha) = \beta$, which implies $\mathscr{A}$ is surjective. The result follows. □

Corollary 3.11. *Let* $\mathbf{F}$ *be a perfect field,* $\alpha_1, \cdots, \alpha_n$ *a basis of* V, $\mathscr{A}: V \to V$ *a* p*-semilinear transformation and* A *be its matrix of* $\mathscr{A}$ *with respect to the basis* $\alpha_1, \cdots, \alpha_n$*. Then* $\mathscr{A}$ *is bijective if and only if* A *is regular.*

Proof. It follows immediately from Theorems 3.9 and 3.10. □

Lemma 3.12. *If* $f : V \to V$ *is a* p*-semilinear transformation and* $\pi : V \to V/\mathrm{Ker} f$ *is the canonical projection, then* f *induces a* p*-semilinear bijective mapping* $\bar{f}$ *from* $V/\mathrm{Ker} f$ *onto* $\mathrm{Im} f$ *such that* $\bar{f}\pi = f$*.*

Proof. $V/\mathrm{Ker} f$ is well defined since $\mathrm{Ker} f$ is an $\mathbf{F}$-subspace of V. Consider the following mapping

$$\begin{aligned} \bar{f} : V/\mathrm{Ker} f &\longrightarrow \mathrm{Im} f \\ \bar{\alpha} &\longmapsto f(\alpha) \end{aligned}$$

then it's clear that $\bar{f}\pi = f$.

Since

$$f(\alpha) = f(\beta) \Rightarrow f(\alpha - \beta) = 0 \Rightarrow \alpha - \beta \in \mathrm{Ker} f \Rightarrow \bar{\alpha} = \bar{\beta},$$

$\bar{f}$ is injective.

$\forall \beta \in \mathrm{Im} f$, there exists $\alpha \in V$ such that $f(\alpha) = \beta$, then we have $\bar{f}(\bar{\alpha}) = f(\alpha) = \beta$, so $\bar{f}$ is surjective. Note that

$$\bar{f}(k\bar{\alpha} + \bar{\beta}) = \bar{f}(\overline{k\alpha + \beta}) = f(k\alpha + \beta) = k^p f(\alpha) + f(\beta) = k^p \bar{f}(\bar{\alpha}) + \bar{f}(\bar{\beta}).$$

Thus, $\bar{f}$ is a bijective p-semilinear mapping from $\mathbf{F}$-space $V/\mathrm{Ker} f$ onto $\mathbf{F}^p$-space $\mathrm{Im} f$ such that $\bar{f}\pi = f$ as desired. □

Theorem 3.13 (Rank-nullity theorem)**.** *If* $f : V \to V$ *is a* p*-semilinear transformation, then* $\dim_{\mathbf{F}} V = \dim_{\mathbf{F}} \mathrm{Ker} f + \dim_{\mathbf{F}^p} \mathrm{Im} f$.

Proof. It follows from Lemma 3.12 that

$$\dim_{\mathbf{F}^p}\mathrm{Im}f = \dim_{\mathbf{F}}V/\mathrm{Ker}f = \dim_{\mathbf{F}}V - \dim_{\mathbf{F}}\mathrm{Ker}f.$$

The result holds. □

Corollary 3.14. *Suppose that $f : V \to V$ is a p-semilinear transformation, then the following conditions are equivalent:*
(1) f is injective, $\mathbf{F}$ is perfect.
(2) f is surjective.

Proof. (1) ⇒(2) Since $\mathbf{F} = \mathbf{F}^p$, $\mathrm{Im}f$ is an $\mathbf{F}$-subspace of V and $\dim_{\mathbf{F}}\mathrm{Im}f = \dim_{\mathbf{F}^p}\mathrm{Im}f = \dim_{\mathbf{F}}V - \dim_{\mathbf{F}}\mathrm{Ker}f = \dim_{\mathbf{F}}V$, which implies $\mathrm{Im}f = V$.

(2) ⇒(1) Note that $\dim_{\mathbf{F}}V \geqslant \dim_{\mathbf{F}^p}\mathrm{Im}f = \dim_{\mathbf{F}^p}V$ and $\dim_{\mathbf{F}}V \leqslant \dim_{\mathbf{F}^p}V$, then $\dim_{\mathbf{F}}V = \dim_{\mathbf{F}^p}V$, which implies $\mathbf{F} = \mathbf{F}^p$ and $\dim_{\mathbf{F}}\mathrm{Ker}f = 0$. □

Here is the result closely related to the Jordan-Chevalley decomposition.

Theorem 3.15. *Suppose that $\mathbf{F}$ is a perfect field and $f : V \to V$ is a p-semilinear transformation. Consider the sets $V' = \{x \in V | f^k(x) = 0, \exists\, k \in \mathbb{N}\}$ and $V'' = \{x \in V | x = \sum\limits_{i=1}^{n} \alpha_i f^i(x), \exists\, n \in \mathbb{N}, \alpha_1, \cdots, \alpha_n \in \mathbf{F}\}$, then the following statements hold:*
(1) V', V'' are f-invariant subspaces of V.
(2) $V = V' \oplus V''$.

Proof. (1) It is easy to prove V' is an f-invariant subspace of V since f is p-semilinear. We will show that V'' is an f-invariant subspace of V.

Assume that $x, y \in V'', \alpha \neq 0 \in \mathbf{F}$. Then there exists $\alpha_1, \cdots, \alpha_n$, $\beta_1, \cdots, \beta_n \in \mathbf{F}$ such that $x = \sum\limits_{i=1}^{n} \alpha_i f^i(x), y = \sum\limits_{j=1}^{m} \beta_j f^j(y)$. Let $\gamma_i = \alpha_i(\alpha^{p^i-1})^{-1}$, then we have

$$\sum_{i=1}^{n} \gamma_i f^i(\alpha x) = \sum_{i=1}^{n} \alpha_i(\alpha^{p^i-1})^{-1}\alpha^{p^i-1}\alpha f^i(x) = \alpha \sum_{i=1}^{n} \alpha_i f^i(x) = \alpha x,$$

which implies $\alpha x \in V''$.

Consider the set

$$W = \Big\{ \sum_{i=0}^{n} \lambda_i f^i(x) + \sum_{j=0}^{m} \mu_j f^j(y) | n \in \mathbb{N}, \lambda_i, \mu_j \in \mathbf{F} \Big\},$$

then W is an f-invariant subspace of V and $f(W)$ is an $\mathbf{F}$-subspace of W since $\mathbf{F}$ is perfect. Note that

$$x = \sum_{i=1}^{n} \alpha_i f^i(x) = f\left(\sum_{i=0}^{n-1} \alpha_{i+1}^{\frac{1}{p}} f^i(x)\right) \in f(W),$$

$$y = \sum_{j=1}^{m} \beta_j f^j(y) = f\left(\sum_{j=0}^{n-1} \beta_{j+1}^{\frac{1}{p}} f^j(x)\right) \in f(W),$$

then $f^i(x), f^j(y) \in f(W)$ and so $W \subseteq f(W)$. Then $W = f(W)$ and $\mathrm{Ker} f|_W = 0$ by Theorem 3.13.

Let $w \in W$ and consider $U = \{\sum\limits_{i=1}^{n} \gamma_i f^i(w) | n \in \mathbb{N}, \gamma_i \in \mathbf{F}\}$, then U is an f-invariant subspace of W and f induces a bijective p-semilinear mapping $\bar{f} : W/U \to W/U$, $x + U \mapsto f(x) + U$. Note that $\bar{f}(w + U) = f(w) + U = U$, then $w \in U$. Hence for $x + y \in W$, there exist $\alpha_1, \cdots, \alpha_n \in \mathbf{F}$ such that $x + y = \sum\limits_{i=1}^{n} \alpha_i f^i(x + y)$. This shows V'' is a subspace of V.

(2) Since $\dim V < \infty$, $\{f^k(x), 0 \leq k < \infty\}$ are linearly dependent. If $\forall\ k \geqslant 0, n \geqslant 1$, $f^k(x)$ cannot be written as a linear combination of $f^{k+1}(x)$, $\cdots$, $f^{k+n}(x)$. In particular, $x = f^0(x)$ cannot be written as a linear combination of $f(x), \cdots, f^n(x)$. Then if there are $\alpha_0, \cdots, \alpha_n$ such that $\alpha_0 x + \alpha_1 f(x) + \cdots + \alpha_n f^n(x) = 0$, we must have $\alpha_0 = 0$(otherwise x is a linear combination of $f(x), \cdots, f^n(x)$, which is a contradiction), and hence $\alpha_1 f(x) + \cdots + \alpha_n f^n(x) = 0$. At the same time, $f(x)$ cannot be written as a linear combination of $f^2(x), \cdots, f^n(x)$, which implies $\alpha_1 = 0$. Likewise, $\alpha_2 = \cdots = \alpha_n = 0$. Now we have shown that $x, f(x), \cdots, f^n(x)$ are linearly independent, $\forall\ n \in \mathbb{N}$, this is a contradiction. Therefore, we can find $k \geqslant 0, \alpha_1, \cdots, \alpha_n \in \mathbf{F}$ such that $f^k(x) = \sum\limits_{i=1}^{n} \alpha_i f^{k+i}(x)$, then $f^k(x) \in V''$.

Consider the set

$$W = \Big\{ \sum_{i=0}^{m} \beta_i f^{k+i}(x) | m \in \mathbb{N}, \beta_i \in \mathbf{F} \Big\}.$$

Use the same method in (1), we have $W = f(W)$. So $f^k(x) \in W$ implies there exists $x_1 \in W \subseteq V''$ such that $f(x_1) = f^k(x)$. Similarly, there exists $x_2 \in W \subseteq V''$ such that $f(x_2) = x_1$, by induction, we can find $x'' \in W \subseteq V''$ such that $f^k(x'') = f^k(x)$. Define $x' := x - x''$, then $f^k(x') = f^k(x) - f^k(x'') = 0$, which implies $x' \in V'$, and so $V = V' + V''$.

Suppose that $x \in V' \cap V''$, then there exists $k \in \mathbb{N}$ such that $f^k(x) = 0$. Consider the set

$$W = \Big\{ \sum_{i=0}^{n} \alpha_i f^i(x) | n \in \mathbb{N}, \alpha_i \in \mathbf{F} \Big\}.$$

In the same way it is shown that $f(W) = W$ and $\mathrm{Ker} f = 0$, then $f^{k-1}(x) = 0$ since $f^k(x) = 0$ and $f^{k-1}(x) \in W$. Similarly, $f^{k-2}(x) = \cdots = x = 0$. Therefore $V' \cap V'' = \{0\}$ and so $V = V' \oplus V''$ as desired. □

We will show that if $\mathbf{F}$ is an algebraically closed field and f is an injective p-semilinear transformation, then there is a basis such that the matrix of f respect to which is a unit matrix.

Theorem 3.16. *Suppose that $\mathbf{F}$ is an algebraically closed field and $f : V \to V$ is an injective p-semilinear transformation. Then there exists a basis $\{x_i, i = 1, \cdots, n\}$ of V such that*

$$f(x_i) = x_i,\ \ i = 1, 2, \cdots, n.$$

Proof. Consider

$$W := \Big\{ \sum_{i=0}^{n} \alpha_i f^i(x) | n \in \mathbb{N}, \alpha_i \in \mathbf{F} \Big\},$$

then W is finite-dimensional, so there is a minimal element $m \in \mathbb{N}$ such that $f^m(x) \in \langle x, \cdots, f^{m-1}(x) \rangle$. It's clear that $\{x, \cdots, f^{m-1}(x)\}$ are linearly independent and suppose $f^m(x) = \sum_{i=1}^{m} \alpha_i f^{i-1}(x)$.

If $\alpha_1 = 0$, then

$$f\Big(f^{m-1}(x) - \sum_{i=2}^{m} \alpha_i^{\frac{1}{p}} f^{i-2}(x) \Big) = 0$$

shows that $f^{m-1}(x) - \sum_{i=2}^{m} \alpha_i^{\frac{1}{p}} f^{i-2}(x)$ is a zero of f, so

$f^{m-1}(x) = \sum_{i=2}^{m} \alpha_i^{\frac{1}{p}} f^{i-2}(x)$ since f is injective.

Then $f^{m-1}(x) \in \langle x, \cdots, f^{m-2}(x) \rangle$. This contradicts the choice of m, so we must have $\alpha_1 \neq 0$.

Consider the polynomial

$$H(x) = \alpha_1^{p^{m-1}} x^{p^m} + \alpha_2^{p^{m-2}} x^{p^{m-1}} + \cdots + \alpha_m x^p - x \in \mathbf{F}[x].$$

Then there exists a nonzero element β_m to be a zero of $H(x)$ since $\mathbf{F}$ is algebraically closed. Now define inductively

$$\beta_1 := \beta_m^p \alpha_1;\ \beta_i := \beta_m^p \alpha_i + \beta_{i-1}^p,\ 2 \leqslant i \leqslant m-1.$$

We will show that β_m satisfies the formula as well:

$$\begin{aligned}
\beta_m^p \alpha_m + \beta_{m-1}^p &= \beta_m^p \alpha_m + (\beta_m^p \alpha_{m-1} + \beta_{m-2}^p)^p \\
&= \beta_m^p \alpha_m + \beta_m^{p^2} \alpha_{m-1}^p + \beta_{m-2}^{p^2} \\
&= \cdots \\
&= \beta_m^p \alpha_m + \beta_m^{p^2} \alpha_{m-1}^p + \cdots + \beta_m^{p^m} \alpha_1^{p^{m-1}} \\
&= \beta_m,
\end{aligned}$$

then $y := \sum_{i=1}^{m} \beta_i f^{i-1}(x)$ is an element of W. Since $\{x, \cdots, f^{m-1}(x)\}$ are linearly independent and $\beta_m \neq 0$, we obtain that $y \neq 0$ and

$$\begin{aligned}
f(y) &= \sum_{i=1}^{m} \beta_i^p f^i(x) = \sum_{i=2}^{m} \beta_{i-1}^p f^{i-1}(x) + \beta_m^p f^m(x) \\
&= \sum_{i=2}^{m} \beta_{i-1}^p f^{i-1}(x) + \beta_m^p \sum_{i=1}^{m} \alpha_i f^{i-1}(x) \\
&= \sum_{i=2}^{m} (\beta_{i-1}^p + \beta_m^p \alpha_i) f^{i-1}(x) + \beta_m^p \alpha_1 x \\
&= \sum_{i=1}^{m} \beta_i f^{i-1}(x) = y.
\end{aligned}$$

Then we have found an element $y \in W \setminus \{0\}$ such that $f(y) = y$.

Suppose we have already constructed $x_1, \cdots, x_r$ linearly independent satisfying $f(x_i) = x_i$. Consider $V \setminus \langle x_1, \cdots, x_r \rangle$, then the restriction of f to $V \setminus \langle x_1, \cdots, x_r \rangle$(denoted by $\bar{f}$) is also injective. Likewise, we can find $\bar{y} \neq 0$ such that $\bar{f}(\bar{y}) = \bar{y}$, i.e., $y \notin \langle x_1, \cdots, x_r \rangle$ and $f(y) - y \in \langle x_1, \cdots, x_r \rangle$. Let $f(y) - y = \sum_{i=1}^{r} \alpha_i x_i$ and suppose that $\delta_i \in \mathbf{F}$ is a zero of the polynomial $x^p - x + \alpha_i$, then $x_{r+1} := \sum_{i=1}^{r} \delta_i x_i + y$ satisfies the relation

$$\begin{aligned} f(x_{r+1}) &= \sum_{i=1}^{r} \delta_i^p f(x_i) + f(y) \\ &= \sum_{i=1}^{r} (\delta_i - \alpha_i) f(x_i) + f(y) \\ &= \sum_{i=1}^{r} (\delta_i - \alpha_i) x_i + y + \sum_{i=1}^{r} \alpha_i x_i \\ &= \sum_{i=1}^{r} \delta_i x_i + y = x_{r+1}. \end{aligned}$$

If $x_{r+1} \in \langle x_1, \cdots, x_r \rangle$, then $y \in \langle x_1, \cdots, x_r \rangle$ since $\sum_{i=1}^{r} \delta_i x_i \in \langle x_1, \cdots, x_r \rangle$, which is a contradiction. Hence $x_{r+1} \notin \langle x_1, \cdots, x_r \rangle$, which implies $x_1, \cdots, x_{r+1}$ are linearly independent. Note that $\dim V = n$, then we can find n linearly independent elements $\{x_1, \cdots, x_n\}$ and they form a basis of V satisfying $f(x_i) = x_i,\ i = 1, \cdots, n$. □

Corollary 3.17. *Suppose that* $\mathbf{F}$ *is an algebraically closed field and* $f : V \to V$ *is an injective* p*-semilinear transformation. Then there exists a basis such that the matrix of* f *respect to which is a unit matrix.*

Proof. It follows from Theorem 3.16. □

Acknowledgments

The authors would like to thank the referee for carefully reading and checking the paper both for its English as well as its mathematics. The authors were partially Supported by NNSF of China (No. 11171055), NSF of Jilin province (No.201115006), Scientific Research Foundation for Returned Scholars Ministry of Education of China and the Fundamental Research Funds for the Central Universities(No. 11SSXT146).

References

[1] J. H. Bevis, Frank J. Hall and Robert E. Hartwig, The Drazin inverse of a semilinear transformation and its matrix representation, *Linear Algebra Appl.* **97** (1987) 229–242.

[2] J. N. Bray, D. F. Holt and C. M. Roney-Dougal, Certain classical groups are not well-defined, *J. Group Theory* **12** (2009), no. 2, 171–180.

[3] U. Dempwolff, J. Chris Fisher and A. Herman, Semilinear transformations over finite fields are Frobenius maps, *Glasgow Math. J.* **42** (2000) 289–295.
[4] W. H. Greub, Linear Algebra, 4th Ed, Springer-Verlag, New York-Berlin, 1981.
[5] K. W. Gruenberg and A. J. Weir, Linear Geometry, D. Van Nostrand Co., Inc., Princeton, N. J. Toronto, Ont.-London, 1967.
[6] N. Jacobson, Restricted Lie algebras of characteristic p, *Trans. Amer. Math. Soc.* **50** (1941) 15–25.
[7] H. Strade and R. Farnsteiner, Modular Lie Algebras and Their Representations, Marcel Dekker, Inc., New York, 1988.

Yao Ma
School of Mathematics and Statistics, Northeast Normal University, Changchun 130024, P. R. China
Email: may703@nenu.edu.cn.

Liangyun Chen
School of Mathematics and Statistics, Northeast Normal University, Changchun 130024, P. R. China
Email: chenly640@nenu.edu.cn