GENERALIZED ARTIN-SCHREIER POLYNOMIALS

N. H. GUERSENZVAIG AND FERNANDO SZECHTMAN

Abstract. Let $F$ be a field of prime characteristic $p$ containing $F_{p^n}$ as a subfield. We refer to $q(X) = X^p - X - a \in F[X]$ as a generalized Artin-Schreier polynomial. Suppose that $q(X)$ is irreducible and let $C_q(X)$ be the companion matrix of $q(X)$. Then $ad C_q(X)$ has such highly unusual properties that any $A \in \text{gl}(m)$ such that $ad A$ has like properties is shown to be similar to the companion matrix of an irreducible generalized Artin-Schreier polynomial.

We discuss close connections with the decomposition problem of the tensor product of indecomposable modules for a 1-dimensional Lie algebra over a field of characteristic $p$, the problem of finding an explicit primitive element for every intermediate field of the Galois extension associated to an irreducible generalized Artin-Schreier polynomial, and the problem of finding necessary and sufficient conditions for the irreducibility of a family of polynomials.

1. Introduction

Let $F$ be an arbitrary field and let $M_m(F)$ the associative algebra of all $m \times m$ matrices over $F$. This becomes a Lie algebra, denoted by $\text{gl}(m, F)$ or simply $\text{gl}(m)$, under the usual bracket $[A, B] = AB - BA$. Each $A \in \text{gl}(m)$ gives rise to the linear map $ad A : \text{gl}(m) \to \text{gl}(m)$, given by $B \mapsto [A, B]$.

If $F$ has prime characteristic $p$ and $q(X) = X^p - X - a \in F[X]$ is an irreducible Artin-Schreier polynomial with companion matrix $C_q \in \text{gl}(p)$, it is not difficult to verify that:

- All eigenvalues of $ad C_q$ are in $F$;
- The eigenvalues of $ad C_q$ form a subfield of $F$;
- The centralizer of $C_q$ is a subfield of $M_p(F)$;
- All eigenvectors of $ad C_q$ are invertible in $M_p(F)$;
- All eigenspaces of $ad C_q$ have the same dimension;
- $ad C_q$ is diagonalizable with minimal polynomial $X^p - X$.

We wish to find all matrices $A \in \text{gl}(m)$ such that $ad A : \text{gl}(m) \to \text{gl}(m)$ has like properties.

Theorem 1.1. Let $F$ be a field and let $A \in \text{gl}(m, F)$. Then

(C1) All eigenvalues of $ad A$ are in $F$;
(C2) The eigenvalues of $ad A$ form a subfield of $F$;
(C3) The centralizer of $A$ is a subfield of $M_m(F)$,
if and only if
(C4) $F$ has prime characteristic $p$.

2000 Mathematics Subject Classification. Primary 12F10; Secondary 12F20, 17B50, 15A21.
Key words and phrases. Artin-Schreier polynomial; Lie algebra; Clebsch-Gordan formula; primitive element; Galois group; Dickson invariants.

The second author was supported in part by an NSERC discovery grant.
(C5) $A$ is similar to the companion matrix of a monic irreducible polynomial $h \in F[X]$ of degree $m$.

(C6) If $q \in F[X]$ is the separable part of $h$, i.e., $h(X) = q(X^p)$, $e \geq 0$, and $q$ is separable, then $q = X^{p^e} - X - a$, where $a \in F$, $n \geq 1$, and $F_{p^e}$ is a subfield of $F$.

Moreover, if (C4)-(C6) hold then: $q$ is irreducible; the subfield of $F$ formed by the eigenvalues of $ad A$ is precisely $F_{p^e}$; all eigenvectors of $ad A$ are invertible in $M_n(F)$; all eigenspaces of $ad A$ have dimension $p^{n+e}$; $ad A$ is diagonalizable if and only if $h$ itself is separable; the invariant factors of $ad A$ are

$$X^{p^{n+e}} - X^{p^e}, \ldots, X^{p^{n+e}} - X^{p^e},$$

so, in particular, the minimal polynomial of $ad A$ is $X^{p^{n+e}} - X^{p^e}$.

The most challenging part of the proof of Theorem 1.1 is to find the invariant factors of $ad A$, as this is depends on the solution to the following problem.

Let $L = \langle x \rangle$ be a 1-dimensional Lie algebra over a field $F$ and let $V$ and $W$ be indecomposable $L$-modules of respective dimensions $n$ and $m$ upon which $x$ acts with at least one eigenvalue from $F$.

**Question.** How does the $L$-module $V \otimes W$ decompose as the direct sum of indecomposable $L$-modules?

When $F$ has characteristic 0 we may derive an answer from the Clebsch-Gordan formula by imbedding $L$ into $\mathfrak{sl}(2)$. A direct computation in the complex case already appeared in [Ro] in 1934. The results in characteristic 0 fail, in general, in prime characteristic $p$, which is the case we require. The analogue problem for a cyclic $p$-group when $F$ has prime characteristic $p$ was solved by B. Srinivasan [S].

Her solution is of an algorithmic nature. Since then several algorithms have appeared. We mention [Ra], [Re] and, most recently, [I], although the literature is quite vast on this subject. For information on the decomposition of the exterior and symmetric squares of an indecomposable module of a cyclic $p$-group in prime characteristic $p$ see [GL]. What we need to be able to compute the invariant factors of $ad A$ in Theorem 1.1 is a closed formula for the decomposition of the $L$-module $V \otimes W$ when $n \leq m = p^e$, $e \geq 0$. This is achieved in [G].

In [G] we give an application to Galois theory of the polynomials appearing in Theorem 1.1. Let $F$ be a field of prime characteristic $p$ containing $F_{p^e}$ as a subfield and suppose that $q(X) = X^{p^e} - X - a \in F[X]$ is irreducible. Let $K/F$ be the corresponding Galois extension. Here $K = F[\alpha]$, where $\alpha \in K$ is a root of $q(X)$. Given an arbitrary intermediate field $E$ of $K/F$ we find a primitive element $\alpha_E$ such that $E = F[\alpha_E]$. We actually give a recursive formula to write $\alpha_E$ as a polynomial in $\alpha$ with coefficients in $F_{p^e}$. This is achieved by means of the so-called Dickson invariants, discovered by L. E. Dickson [D] in 1911.

Finally, in [G] we discuss the actual existence of irreducible polynomials $q(X) = X^{p^e} - X - a \in F[X]$, with $F$ as in the previous paragraph. As explained in [G] if $n > 1$ and $q(X)$ is irreducible then $\alpha$ must be transcendental over $F$. This fact, together with the more general polynomials $q(X^p)$ considered in Theorem 1.1, lead us to study the irreducibility of polynomials of the form

$$h(X) = X^{p^{n+e}} - X^{p^e} - g(Z^r) \in F[X],$$

where $X$ and $Z$ are algebraically independent elements over an arbitrary field $K$ of prime characteristic $p$, $n > 0$, $r > 0$, $e \geq 0$, $F = K(Z)$, and $g(Z) \in K[Z]$ is a non-zero polynomial of degree relatively prime to $p$. Using results from [MS] and [G],
we obtain in [8] necessary and sufficient conditions for the irreducibility of \( h(X) \). In particular, \( X^{p^n} - X - g(Z^r) \in F[X] \) is irreducible for any \( n > 0, r > 0 \) and non-zero \( g \in K[Z] \) whose degree relatively prime to \( p \). This limitation on \( \deg(g) \) is needed, as the example \( X^{p^n} - X - Z^{p^n} - Z \) shows.

2. Eigenvalues

Let \( F \) be a field. For \( A \in M_m(F) \) let \( \chi_A \) and \( \mu_A \) denote the characteristic and minimal polynomials of \( A \). If \( b \in F \) is an eigenvalue of \( A \) we write \( E_b(A) \) for the corresponding eigenspace. If \( B \in M_m(F) \) we write \( A \sim B \) whenever \( A \) and \( B \) are similar. The companion matrix to a monic polynomial \( g \in F[X] \) of degree \( m \) will be denoted by \( C_g \).

**Lemma 2.1.** Let \( A \in M_m(F) \) and let \( C \) be the centralizer of \( A \) in \( M_m(F) \). Then \( C \) is a subfield of \( M_m(F) \) if and only if \( A \) is similar to the companion matrix of a monic irreducible polynomial in \( F[X] \) of degree \( m \).

**Proof.** If \( A \) is similar to the companion matrix of a monic polynomial of degree \( m \) - necessarily \( \mu_A \) - it is well-known \([8]\), §3.11, that \( C = F[A] \). If, in addition, \( \mu_A \) is irreducible, then \( C = F[A] \cong F[X]/(\mu_A) \) is a field.

Assume that \( C \) is a field. Then \( K = F[A] \) is a field, so \( \mu_A \) is irreducible and \( V \) is a vector space over \( K \). As such, \( C = \text{End}_K(V) \). If \( \dim_K(V) > 1 \) then \( \text{End}_K(V) \) is not a field. Thus \( \dim_K(V) = 1 \), so \( \dim_F(V) = [K : F] = \deg(\mu_A) \), whence \( A \) is similar to the companion matrix of \( \mu_A \).

**Lemma 2.2.** Let \( A \in \mathfrak{gl}(m) \) and let \( K \) be a splitting field of \( \mu_A \) over \( F \). Then \( \mu_{ad A} \) splits over \( K \). Moreover, if \( S_A \) and \( S_{ad A} \) denote the sets of eigenvalues of \( A \) and \( ad A \) in \( K \), respectively, then \( S_{ad A} = \{ \alpha - \beta : \alpha, \beta \in S_A \} \).

**Proof.** According to \([8]\), §4.2, we have \( A = D + N \), where \( D, N \in \mathfrak{gl}(m, K) \), \( D \) is diagonalizable, \( N \) is nilpotent, and \( [D, N] = 0 \). In particular, \( \chi_D = \chi_A \).

Moreover, \( ad A = ad D + ad N \), where \( ad D \) is diagonalizable, \( ad N \) is nilpotent, \( [ad D, ad N] = 0 \). As above, \( \chi_{ad D} = \chi_{ad A} \). It thus suffices to prove the statement for \( D \) instead \( A \), a well-known result also found in \([8]\), §4.2.

**Lemma 2.3.** Let \( A \in \mathfrak{gl}(m) \) and suppose that the centralizer \( C \) of \( A \) is a subfield of \( M_m(F) \). Suppose further that \( ad A \) has at least one non-zero eigenvalue \( b \) in \( F \). Then \( F \) has prime characteristic \( p \), every \( b \)-eigenvector of \( ad A \) is invertible in \( M_m(F) \), and \( E_b(ad A) \) has the same dimension as \( C = E_0(ad A) \).

**Proof.** Let \( K \) be a splitting field for \( \mu_A \) over \( F \). By Lemma 2.2 and assumption, there are eigenvalues \( \alpha, \beta \in K \) of \( A \) such that \( \alpha = \beta + b \) for some \( b \in F \). By Lemma 2.1 \( \mu_A \) is irreducible. By \([8]\), Theorem 4.4, there is an automorphism of \( K/F \) such that \( \beta \mapsto \beta + b \), where \( |\text{Aut}(K/F)| \leq [K : F] \) is finite. Since \( b \neq 0 \), \( F \) must have prime characteristic \( p \). Alternatively, \( \mu_A(X) \) and \( \mu_A(X + b) \) have a common root \( \beta \). Since they are irreducible in \( F[X] \), they must be equal. It follows that \( \mu_A(X) = \mu_A(X + ib) \), and hence \( \alpha + ib \) is a root of \( \mu_A(X) \), for every \( i \) in the prime field of \( F \). This forces the prime field of \( F \) to be finite.

Now \( X \in E_b(ad A) \) if and only if

\[
AX - XA = bX,
\]
i.e.

\[
(2.1) \quad AX = X(A + bI).
\]
By Lemma 2.3, \( A \sim C_{\mu_A(X)} \). But \( \mu_A(X) = \mu_A(X + b) \), so \( A + bI \sim C_{\mu_A(X + b)} + bI \). On the other hand, \( C_{\mu_A(X + b)} \) and \( C_{\mu_A(X + b)} + bi \) generate the same subalgebra, so their minimal polynomials have the same degree. Since, clearly, \( \mu_A(X) \) annihilates \( C_{\mu_A(X + b)} + bI \), it follows that \( \mu_A(X) \) is the minimal polynomial of \( C_{\mu_A(X + b)} + bI \). But \( \mu_A(X) \) has degree \( m \), so \( C_{\mu_A(X)} \sim C_{\mu_A(X + b)} + bI \). All in all, we deduce that \( A \sim A + bI \). Thus, there is \( S \in \text{GL}_m(F) \) such that \( A + bI = SAS^{-1} \). Replacing this in (2.1), yields

\[
AX = XSAS^{-1},
\]

i.e.

\[
AXS = XSA.
\]

Since \( A \) is cyclic, this equivalent, by [1], §3.11, to \( XS \in F[A] \), or \( X = f(A)S^{-1} \), for some \( f \in F[X] \). But \( F[A] \) is a field, so the result follows. □

We digress here to take another look at the fact, used above, that

\[
(2.2) \quad C_f(X) \sim C_{f(X + b)} + bI.
\]

This holds for any \( f \in F[X] \) and \( b \in F \). The interesting point here is that we can choose a similarity transformation realizing (2.2) that is completely independent of \( f \), i.e., the same transformation works for all \( f \).

**Lemma 2.4.** Let \( b \in F \). Then there exists \( S \in \text{GL}_m(F) \) such that for any monic polynomial \( f \in F[X] \) of degree \( m \), we have

\[
(2.3) \quad S^{-1}(C_{f(X)} + bI_m)S = C_{f(X)}.
\]

**Proof.** Let \( S \in \text{GL}_m(F) \) have diagonal entries 1, first superdiagonal entries \( b \), second superdiagonal entries \( b^2 \), and so on. For instance, if \( m = 4 \) then

\[
\begin{pmatrix}
1 & b & b^2 & b^3 \\
0 & 1 & b & b^2 \\
0 & 0 & 1 & b \\
0 & 0 & 0 & 1
\end{pmatrix}.
\]

We claim that (2.3) holds. Why is this true? It is a simple matrix calculation, but there is no need to calculate anything. Indeed, it is obvious that \( e_1 \), the first canonical vector of the column space \( F^m \), is a cyclic vector for \( B = C_{f(X + b)} + bI \). As seen the proof of Lemma 2.3, the minimal polynomial of \( B \) must be \( f(X) \). Therefore, relative to the basis \( e_1, Be_1, \ldots, B^{m-1}e_1 \) the matrix of the linear transformation that \( B \) represents in the canonical basis will be exactly \( C_{f(X)} \). If the columns of \( T \in \text{GL}_m(F) \) are formed by \( e_1, Be_1, \ldots, B^{m-1}e_1 \), this says that

\[
T^{-1}(C_{f(X)} + bI)T = C_{f(X)}.
\]

But \( e_1, Be_1, \ldots, B^{m-1}e_1 \) are exactly the columns \( S \), so \( S = T \). □

A more general result than (2.2) is [CS], Proposition 2.4:

**Proposition 2.5.** Let \( f, g \in F[X] \), where \( f \) is monic of degree \( m \geq 1 \), and \( g \) has degree \( d \geq 1 \) and leading coefficient \( a \). Then

\[
(2.4) \quad g(C_{a - m}f(g(X))) \sim C_f \oplus \cdots \oplus C_f, \quad d \text{ times}.
\]

We leave it to the reader to determine if, in analogy with Lemma 2.3, it is possible to choose a similarity transformation that depends on only \( g \) and not on \( f \).
3. Decomposition numbers

Let $F$ be a field and let $L = \langle x \rangle$ be a 1-dimensional Lie algebra over $F$. Let $V$ be an $L$-module of dimension $n$ and let $x_V$ be the linear operator that $x$ induces on $V$. Suppose that $x_V$ has at least one eigenvalue in $F$ and that $V$ is an indecomposable $L$-module. This means that there is a basis $B$ of $V$ relative to which the matrix $M_B(x_V)$ of $x_V$ is the upper triangular Jordan block $J_n(\alpha)$, where $\alpha \in F$ is the only eigenvalue of $x_V$.

Suppose next that $W$ is an indecomposable $L$-module of dimension $m$ and that $x_W$ has eigenvalue $\beta \in F$. As above, there is a basis $C$ of $W$ relative to which $M_C(x_V) = J_m(\beta)$.

As usual, we may view $V \otimes W$ as an $L$-module via

$$x(v \otimes w) = xv \otimes w + v \otimes xw, \quad v, w \in V.$$ 

Let $x_{V \otimes W}$ be the linear operator that $x$ induces on $V \otimes W$. It is easy to see that the minimal polynomial of $x_{V \otimes W}$ splits in $F$ and a single eigenvalue, namely $\alpha + \beta$. This follows from the well-known formula:

$$(3.1) \quad (x - (\alpha + \beta) \cdot 1)^{k}(v \otimes w) = \sum_{0 \leq i \leq k} \binom{k}{i} (x - \alpha \cdot 1)^{k-i}(v) \otimes (x - \beta \cdot 1)^{i}(w).$$

**Question 3.1.** How does $V \otimes W$ decompose as a direct sum of indecomposable $L$-modules?

That is, what is the length $\ell$ of $V \otimes W$ and what are the decomposition numbers $d_1 \geq \cdots \geq d_\ell$ such that

$$x_{V \otimes W} \sim J_{d_1}(\alpha + \beta) \oplus \cdots \oplus J_{d_\ell}(\alpha + \beta)?$$

Replacing $x_V$ by $x_V - \alpha \cdot 1$, $x_W$ by $x_W - \beta \cdot 1$, and $x_{V \otimes W}$ by $x_{V \otimes W} - (\alpha + \beta) \cdot 1$, we see that $\ell$ and the decomposition numbers $d_1 \geq \cdots \geq d_\ell$ are independent of $\alpha$ and $\beta$, and can be computed when $\alpha = 0 = \beta$.

When $F$ has characteristic 0 and $n \leq m$ then $\ell = n$, with decomposition numbers

$$m + n - 1, m + n - 3, \ldots, m - n + 3, m - n + 1.$$ 

This can obtained by imbedding $L$ into $\mathfrak{sl}(2)$ and using the Clebsch-Gordan formula [H], §22.5. These decomposition numbers are used in [CS] to classify all uniserial modules for a class of solvable Lie algebras.

The analogue of Question 3.1 for a cyclic $p$-group and $F$ of prime characteristic $p$ was solved by B. Srinivasan [S]. The answer is given recursively, rather than as a closed formula. Alternative algorithms can be found in [Ra] and [Re]. Presumably, Srinivasan’s results translate to our present set-up mutatis mutandis.

This section furnishes a closed formula in answer to Question 3.1 albeit only in the special case $m = p^e$, where $F$ has prime characteristic $p$ and $e \geq 0$, as required in the proof of Theorem 1.1.

**Lemma 3.2.** Let $p$ be a prime and let $e \geq 0$. Then $p|\binom{p^e}{i}$ for any $0 < i < p^e$.

*Proof.* Suppose $i, j, N \geq 0$ satisfy $i + j = N$. Let $v_p(a)$ denote the number of times that $p$ divides a given integer $a \neq 0$. Then

$$(3.2) \quad v_p(i! \times j!) \leq v_p(N!).$$

Indeed, according to the well-know formula [V], chapter 2:

$$v_p(N!) = \lfloor N/p \rfloor + \lfloor N/p^2 \rfloor + \lfloor N/p^3 \rfloor + \cdots.$$
Therefore,
\[ v_p(i! \times j!) = v_p(i!) + v_p(j!) = (i/j) + ([i/p] + [j/p]) + ([i/p^2] + [j/p^2]) + ([i/p^3] + [j/p^3]) + \cdots. \]

On the other hand, if \( a, b \) are real numbers then
\[ \{a\} + \{b\} \leq [a + b], \]
with equality if and only if
\[ \{a\} + \{b\} < 1, \]
where \( \{a\} = x - [x] \). This proves (3.2).

In the special case \( N = p^e \) and \( 0 < i, j < p^e \), where \( i + j = p^e \), we have
\[ \{i/p^e\} + \{j/p^e\} = i/p^e + j/p^e = 1, \]
so the result follows. \( \square \)

**Proposition 3.3.** Let \( F \) be a field of prime characteristic \( p \) and let \( e \geq 0 \). Let \( L = \langle x \rangle \) be a 1-dimensional Lie algebra over \( F \). Let \( V \) and \( W \) be indecomposable \( L \)-modules of dimensions \( n \) and \( p^e \), respectively, where \( n \leq p^e \). Suppose that \( x \) has eigenvalues \( \alpha, \beta \in F \) when acting on \( V \) and \( W \), respectively. Then the \( L \)-module \( V \otimes W \) decomposes as the direct sum of \( n \) isomorphic indecomposable \( L \)-modules, each of which has dimension \( p^e \) and is acted upon by \( x \) with a single eigenvalue \( \alpha + \beta \). In symbols,
\[ \ell = n \text{ and } d_1 = \cdots = d_{p^e} = p^e. \]

**Proof.** As mentioned above, we may assume without loss of generality that \( \alpha = 0 \) and \( \beta = 0 \), and we will do so, mainly for simplicity of notation. For the same reason, we let \( m = p^e \).

Let \( B = \{v_1, \ldots, v_m\} \) and \( C = \{w_1, \ldots, w_m\} \) be bases of \( V \) and \( W \) relative to which \( M_B(x_V) = J_m(0) \) and \( M_C(x_W) = J_m(0) \).

Since \( n \leq m \), we have
\[ x_V^m = 0 \quad \text{and} \quad x_W^m = 0. \]

Therefore, Lemma 3.2 and 3.1 imply
\[ x_V^m \otimes W = 0. \]

We next view \( M = V \otimes W \) as a module for the polynomial algebra \( F[X] \) via \( x_V \otimes W \). We wish to show that \( M \) has elementary divisors \( X^m, \ldots, X^m \), with multiplicity \( n \).

It follows from (3.1) that
\[ x^{m-1}(v_1 \otimes w_m) = v_1 \otimes w_1 \neq 0. \]

Let \( N_1 \) be the \( F[X] \)-submodule of \( M \) generated by \( v_1 \otimes w_m \). Then \( N_1 \) has a single elementary divisor, namely \( X^m \).

Suppose that \( 1 \leq i < n \) and the \( F[X] \)-submodule of \( M \), say \( N_i \), generated by \( v_1 \otimes w_m, \ldots, v_i \otimes w_m \) has elementary divisors \( X^m, \ldots, X_m \), with multiplicity \( i \). Using (3.1) we see that \( v_{i+1} \otimes w_1 \) appears in \( x^{m-1}(v_{i+1} \otimes w_m) \) with coefficient 1. Since \( v_{i+1} \otimes w_1 \notin N_i \), the minimal polynomial of the vector \( v_{i+1} \otimes w_m + N_i \in M/N_i \) is \( X^m \).

The theory of finitely generated modules over a principal ideal domain implies that the \( F[X] \)-submodule of \( M \) generated by \( v_1 \otimes w_m, \ldots, v_i \otimes w_m, v_{i+1} \otimes x_m \) has elementary divisors \( X^m, \ldots, X_m \), with multiplicity \( i+1 \). The result now follows. \( \square \)
Note 3.4. Unlike what happens in characteristic 0, the decomposition of $V \otimes W$ for $L$ is not, in general, the same as for $\mathfrak{sl}(2)$. Indeed, suppose $F$ has characteristic 2 and let $V = W$ be the natural module for $\mathfrak{sl}(2)$. Then $V \otimes W$ is an indecomposable $\mathfrak{sl}(2)$-module, but decomposes as the direct sum of two indecomposable $L$-modules for $L = \langle x \rangle$, where $x, h, y$ is the standard basis of $\mathfrak{sl}(2)$.

Resuming our prior discussion, let $F$ be a field and let $L = \langle x \rangle$ be a 1-dimensional Lie algebra over $F$. Let $V_1, \ldots, V_s$ be $L$-modules with bases $B_1, \ldots, B_s$ relative to which $M_{B_i}(x_V) = J_{m_i}(\alpha_i)$, where $1 \leq i \leq s$ and $\alpha_i \in F$. Consider the $L$-module $V = V_1 \oplus \cdots \oplus V_s$. We may view $\mathfrak{gl}(V)$ as an $L$-module via:

$$x \cdot f = x V f - f x V .$$

Thus $x$ acts on $\mathfrak{gl}(V)$ via $ad x_V$. By Lemma 2.2, the eigenvalues of $ad x_V$ are $\alpha_i - \alpha_j$, where $1 \leq i, j \leq s$. We can view $\mathfrak{gl}(V)$ as the direct sum of the $L$-submodules

$$\text{Hom}(V_j, V_i) \cong V_j^* \otimes V_i, \quad 1 \leq i, j \leq s .$$

Here $V_j^*$ is an indecomposable $L$-module upon which $x$ acts with eigenvalue $-\alpha_j$. It is then clear that the generalized eigenspace of $ad x_V$ for a given eigenvalue $\gamma$ is the sum of all $\text{Hom}(V_j, V_i)$ such that $\alpha_i - \alpha_j = \gamma$.

Corollary 3.5. Keep the above notation and suppose, further, that $F$ has prime characteristic $p$ and all $L$-modules $V_i$ have the same dimension $p^e$, for some $e \geq 0$. Let $S = \{ \alpha_i - \alpha_j \mid 1 \leq i, j \leq s \}$, the set of distinct eigenvalues of $ad x_V$. Then the minimal polynomial of $ad x_V$ is $\prod (X - \gamma)^{p^e}$. Moreover, the elementary divisors of $ad x_V$ are $(X - \gamma)^{p^e}, \gamma \in S$, with multiplicity $p^e m(\gamma)$, where

$$m(\gamma) = \left| \{(i, j) \mid 1 \leq i, j \leq s, \alpha_i - \alpha_j = \gamma \} \right| .$$

4. Proof of Theorem

Suppose conditions (C4)-(C6) hold. Then $q$ is irreducible, since so is $h$. Let $K$ be a splitting field for $h$ over $F$. Since $q$ is separable, the number of distinct roots of $h$ in $K$ is exactly $p^n$.

Let $\beta \in K$ be a root of $h$. The $\beta + b$ is a root of $h$ for every $b \in F_p^n$. Indeed, since $b^n = b$, we have

$$h(\beta + b) = \beta^{p^n + n} + (b^n)^{p^e} - \beta^{p^e} - b^{p^e} - a = h(\beta) = 0 .$$

It follows that $\beta + b, b \in F_p^n$, are the distinct roots of $h$ in $K$, each repeated $p^e$ times. By Lemma 2.2, $\mu_{ad A}$ splits in $K$ and the set of eigenvalues of $ad A$ is precisely $F_p^n$. Moreover, by Lemma 2.4, the centralizer of $A$ is a subfield of $M_m(F)$. In particular, conditions (C1)-(C3) hold.

Furthermore, by Lemma 2.3, all eigenvectors of $ad A$ are invertible in $M_m(F)$ and all eigenspaces of $ad A$ have dimension $p^{n+c}$. Thus, the sum of the dimensions of all eigenspaces of $ad A$ is $p^{2n+c}$. This equals the dimension of $\mathfrak{gl}(m)$, namely $m^2 = p^{2(n+c)}$, if and only if $e = 0$. Therefore, $ad A$ is diagonalizable if and only if $h$ is separable.

Regardless of whether $e = 0$ or not, we claim that the invariant factors of $ad A$ are $X^{p^n+c} - X^{p^e}, \ldots, X^{p^n+c} - X^{p^e}$, with multiplicity $p^{n+c}$. For this purpose, we may assume without loss of generality that $F = K$. Hence $\mu_{ad A}$ splits in $F$, by Lemma 2.2. Thus $A$ is similar to the direct sum of the companion matrices to $X^{p^e} - \beta^{p^e} = (X - \beta)^{p^e}$, as $\beta$ runs through the $p^n$ distinct roots of $h$ in $F$. Hence,
Lemma 2.1 shows that (C5) holds.

It follows from Corollary 3.5 that the elementary divisors of \(ad A\) are \((X - b)^{p^n}\), \(b \in F_{p^n}\), each with multiplicity \(p^{n+e}\). Since \(\Pi \prod_{b \in F_{p^n}} (X - b) = X^{p^n} - X\), the claim follows.

Suppose conversely that (C1)-(C3) hold. Since the eigenvalues of \(ad A\) form a subfield of \(F\), we see that \(ad A\) has a non-zero eigenvalue in \(F\). It follows from Lemma 2.2 that (C4) holds. Since the centralizer of \(\alpha\) is a root of \(F\), we deduce that all irreducible factors of \(\alpha\) have the same degree. Let \(\sigma \in G\). Then \(\sigma \alpha \sigma^{-1}\) is also a root of \(q\). Indeed, \(b \mapsto b^{\sigma}\) is an automorphism of \(F_{p^n}\), so \(c = b^{\sigma}\) for some \(b \in F_{p^n}\). Therefore,

\[
q(\alpha + c) = \mu_A(\beta + b) = 0.
\]

Thus \(F[\alpha]\) is a splitting field for \(q\) over \(F\). Since \(q\) is separable, we deduce that \(F[\alpha]/F\) is a finite Galois extension, whose Galois group we denote by \(G\). We claim that \(\alpha^{p^n} - \alpha \in F\). To see this, it suffices to show that \(\alpha^{p^n} - \alpha \in F\) is fixed by every \(\sigma \in G\). Let \(\sigma \in G\). Then \(\sigma(\alpha)\) must be a root of \(q\), so \(\sigma(\alpha) = \alpha + b\) for some \(b \in F_{p^n}\). Therefore,

\[
\sigma(\alpha^{p^n} - \alpha) = (\alpha + b)^{p^n} - (\alpha + b) = \alpha^{p^n} - \alpha,
\]

as required. Thus \(\alpha^{p^n} - \alpha = a \in F\), so \(X^{p^n} - X - a \in F[X]\) has \(\alpha\) as root. Hence \(q(X^{p^n} - X - a)\). Since these polynomials have the same degree and are monic, they must be equal. This completes the proof of the theorem.

5. Primitive elements of intermediate fields in a Galois extension

Let \(F\) be a field of prime characteristic \(p\) having \(F_{p^n}\) as a subfield and consider the generalized Artin-Schreier polynomial \(q = X^{p^n} - X - a \in F[X]\). Let \(\alpha\) be a root of \(q\) in a field extension of \(F\). Then \(\alpha + b, b \in F_{p^n}\), are all roots of \(q\). Indeed,

\[
q(\alpha + b) = \alpha^{p^n} + b^{p^n} - \alpha - b - a = q(\alpha) = 0.
\]

Thus \(F[\alpha]\) is a splitting field for \(q\) over \(F\). Moreover, all roots of \(q\) have the same degree over \(F\), since \(F[\alpha] = F[\alpha + b]\) for any \(b \in F_{p^n}\). Thus, all irreducible factors of \(q\) in \(F[X]\) have the same degree. Let \(G\) be the Galois group of \(F[\alpha]/F\). We claim that \(G\) is elementary abelian \(p\)-group. Indeed, let \(\sigma, \tau \in G\). Then \(\sigma(\alpha) = \alpha + b\) and \(\tau(\alpha) = \alpha + c\) for some \(b, c \in F_{p^n}\). Therefore \(\sigma^p = 1\) and \(\sigma \tau = \tau \sigma\), as claimed. Since \(|G| = [F[\alpha] : F]\), which is the degree the minimal polynomial of \(\alpha\) over \(F\), we deduce that all irreducible factors of \(q\) in \(F[X]\) have degree \(p^m\) for a unique \(0 \leq m \leq n\).
If \( a = 0 \) it is obvious that \( m = 0 \). If \( a \neq 0 \) and \( F = F_p^m \) then \( m = 1 \). More generally, if \( F \) algebraic over \( F_p^a \) and there is no \( b \in F \) such that \( q(b) = 0 \) then \( m = 1 \). Indeed, let \( f \) be the minimal polynomial of \( a \) over \( F \) and let \( p^m \) be its degree. By assumption \( m > 0 \). Let \( E \) be the subfield of \( F \) obtained by adjoining \( a \) and the coefficients of \( f \) to \( F_p^a \). Then \( f \) is irreducible and a factor of \( q \) in \( E[X] \). By above, \( \text{Gal}(E[a]/E) \) is an elementary abelian group of order \( p^m \). Since \( E \) is a finite field, \( \text{Gal}(E[a]/E) \) is cyclic, so \( m = 1 \).

Assume henceforth that \( q \) is actually irreducible. Then \( K = F[a] \) is a splitting field for \( q \) over \( F \) and \( G = \text{Gal}(K/F) \) is an elementary abelian \( p \)-group of order \( p^m \). More explicitly, for \( b \in F_p^m \), let \( \sigma_b \in G \) be defined by \( \sigma_b(a) = a + b \). Then \( b \mapsto \sigma_b \) defines a group isomorphism \( F_p^m \to G \). In particular, \( G \) has normal subgroups of all possible orders.

Suppose that \( m \) satisfies \( 0 \leq m \leq n \). Let \( H \) be a subgroup of \( G \) of order \( p^m \). Then the fixed field \( E = K^H \) of \( H \) satisfies \( [K : E] = p^m \). Since \( F[a] = E[a] \), the minimal polynomial \( \mu_{a,E} \) of \( a \) over \( E \) must have degree \( p^m \). In fact,

\[
\mu_{a,E}(X) = \prod_{\sigma \in H} (X - \alpha^\sigma).
\]

Since \( \mu_{a,E}(X) \) divides \( q = X^{p^n} - X - a \in E[X] \), it follows that all irreducible factors of \( q \) in \( E[X] \) have degree \( q^m \). In fact,

\[
X^{p^n} - X - a = \prod_{\sigma \in \text{Gal}(E/F)} \mu_{a,E}(X)^\sigma.
\]

Let

\[
(5.1) \quad \alpha_H = \prod_{\sigma \in H} \alpha^\sigma.
\]

Since every \( \sigma \in G \) is of the form \( \sigma_b \) for \( b \in F_p^m \), it follows that \( \alpha_H \) is a monic polynomial in \( a \) of degree \( p^m \) with coefficients in \( F_p^m \). Since \( a \) has degree \( p^n \) over \( F \), the degree of \( \alpha_H \) over \( F \) is at least \( p^{n-m} \). But clearly \( \alpha_H \in E \), where \( [E : F] = p^{n-m} \). It follows that \( E = F[\alpha_H] \).

As just noted, \( \alpha_H \) as an \( F_p^m \)-linear combination of powers of \( a \). In fact, we may use the so-called Dickson invariants, found by L. E. Dickson [D] in 1911, to obtain a sharper result. These invariants have been revisited numerous times (see, for instance, [H2] and [SH]).

Consider the polynomial \( \Phi_m \) in the polynomial algebra \( F[a, B_1, \ldots, B_m] \), defined as follows:

\[
(5.2) \quad \Phi_m(A, B_1, \ldots, B_m) = \prod_{s_1, \ldots, s_m} (A + s_1 B_1 + \cdots + s_m B_m).
\]

Clearly \( \Phi_m \) is \( \text{GL}_m(F_p) \)-invariant. Dickson showed that

\[
\Phi_m = A^{p^m} + f_{m-1}(B_1, \ldots, B_m) A^{p^{m-1}} + \cdots + f_1(B_1, \ldots, B_m) A p + f_0(B_1, \ldots, B_m) A,
\]

where \( f_0, \ldots, f_{m-1} \in F_p[B_1, \ldots, B_m] \) are algebraically independent and generate \( F_p[B_1, \ldots, B_m] \) as an \( \text{GL}_m(F_p) \)-module. Moreover, \( \Phi_m \), and hence \( f_{m-1}, \ldots, f_0 \), can be recursively computed from

\[
(5.3) \quad \Phi_0 = A,
\]

\[
(5.4) \quad \Phi_i = \Phi_{i-1}(A, B_1, \ldots, B_{i-1})^p - \Phi_{i-1}(B_1, B_1, \ldots, B_{i-1}) p^i \Phi_{i-1}(A, B_1, \ldots, B_{i-1}).
\]
Let $\sigma_{b_1}, \ldots, \sigma_{b_m}$ be generators of $H$. This means that $\sigma_{b_1}, \ldots, \sigma_{b_m}$ are in $H$ and that $b_1, \ldots, b_m$ are linearly independent over $F_p$. It follows from (5.1) that

$$\alpha_H = \prod_{s_1, \ldots, s_m \in F_p} (\alpha + s_1 b_1 + \cdots + s_m b_m) = \Phi_m(\alpha, b_1, \ldots, b_m).$$

This, together with (5.3) and (5.4) allows us to recursively find $c_0, \ldots, c_{m-1} \in F_p^n$ such that

$$\alpha_H = \alpha^{p^m} + c_{m-1} \alpha^{p^{m-1}} + \cdots + c_1 \alpha^p + c_0 \alpha.$$

In certain special cases we actually have $c_0, \ldots, c_{m-1} \in F_p$, in which case we will say that $H$ has property $P$.

Let $R$ be the subgroup of $F_p^n$ that corresponds to $H$ under $F_p^n \to G$. Thus, $R$ is an $F_p$-subspace of $F_p^n$, namely the $F_p$-span of $b_1, \ldots, b_m$.

**Lemma 5.1.** $H$ has property $P$ if and only if $R$ is invariant under the Frobenius automorphism of $F_p^n$, in which case

$$\alpha_H = f_R(\alpha),$$

where

$$f_R(Y) = \prod_{b \in R} (Y + b).$$

**Proof.** We start by showing that $H$ has property $P$ if and only if $f_R \in F_p^n[Y]$ has coefficients in $F_p$.

Suppose first that there exist $c_{m-1}, \ldots, c_0 \in F_p$ such that

$$\alpha_H = \alpha^{p^m} + c_{m-1} \alpha^{p^{m-1}} + \cdots + c_1 \alpha^p + c_0 \alpha.$$

Set

$$f(Y) = Y^{p^m} + c_{m-1} Y^{p^{m-1}} + \cdots + c_1 Y^p + c_0 Y \in F_p[Y].$$

Let $b \in R$. Since $\alpha_H^\sigma_b = \alpha_H$, it follows that

$$f(b) = 0.$$

Therefore $f_R = f \in F_p[Y]$. Conversely, if $f_R \in F_p[Y]$ then

$$\alpha_H = \prod_{b \in R} (\alpha + b) = f_R(\alpha),$$

which is an $F_p$-linear combination of $\alpha^{p^m}, \ldots, \alpha^p, \alpha$ with first coefficient 1.

Let $\tau$ be the Frobenius automorphism of $F_p^n$. Then $f_R \in F_p^n[Y]$ if and only if

$$f_R(Y) = f_R(Y^\tau) = \prod_{b \in R} (Y^\tau + b^\tau) = \prod_{b \in R^\tau} (Y + b) = f_R^\tau(Y),$$

which is equivalent to $R = R^\tau$. □

Suppose that $R$ is actually a subfield of $F_p^n$. Then $R$ is certainly invariant under $b \mapsto b^\tau$. Moreover, $f_R(Y) = Y^{p^m} - Y$. Therefore, in this case,

$$\alpha_H = \alpha^{p^m} - \alpha.$$

In particular, $\alpha_H = a$.

**Corollary 5.2.** If $b_1, \ldots, b_m \in F_p^n$ are linearly independent over $F_p$, then

$$f_0(b_1, \ldots, b_m) = -1,$$

whereas $f_j(b_1, \ldots, b_m) = 0$, if $1 \leq j \leq m - 1$.

Corollary 5.2 is not true, in general, if $b_1, \ldots, b_m \in R$ are linearly dependent over $F_p$, as the case $m = 2$ will confirm by taking $b_1 = 1 = b_2$ for $j = 0, 1$. 

Example 5.3. Here we furnish examples of subspaces \( R \) of \( F_p^n \) that are invariant under \( b \mapsto b^p \) but are not subfields of \( F_p^n \), even when \( m | n \).

Suppose first \( m = 1 \), where \((p - 1) | n \) and \( p \) is odd. Take \( c \in F_p \), \( c \neq 0 \), and set

\[
 f(Y) = Y^p - cY \in F_p[Y].
\]

Since \( Y^{p^{n-1}} \equiv Y \mod f \), it follows that \( f \) splits in \( F_{p^{n-1}} \) and hence in \( F_{p^n} \). The roots of \( f \) in \( F_{p^n} \) form a 1-dimensional, Frobenius-invariant, subspace \( R \) of \( F_{p^n} \), which is not a field, since \( F_p \) is the only 1-dimensional subfield of \( F_{p^n} \) and 0 is the only element of \( F_p \) that is a root of \( f \).

Suppose next that \( m = 2 \), where \( 2p | n \) and \( p \) is odd. Let

\[
(5.6) \quad f(Y) = \prod_{j \in F_p} (Y^p - Y - j).
\]

Thus, \( f \) is the product of all Artin-Schrier polynomials in \( F_p[Y] \). This readily implies that the roots of \( f \) form a 2-dimensional, Frobenius-invariant, subspace \( R \) of \( F_{p^n} \) containing \( F_p \). In particular, \( f(cY) = f(Y) \) for all \( 0 \neq c \in F_p \). Since \( Y | f(Y) \) and \( f(Y) \) has degree \( p^2 \), it follows that

\[
 f(Y) = Y^{p^2} + aY^p + bY,
\]

where \( a, b \in F_p \). Using (5.6) and \( p > 1 \) to compute \( a, b \) reveals that

\[
 f(Y) = Y^{p^2} - Y^p - Y.
\]

However, the subfield of \( F_{p^n} \) obtained by adjoining \( R \) to \( F_p \) is \( F_{p^n} \). Since \( p > 2 \), it follows that \( R \) is not a subfield of \( F_{p^n} \).

6. Existence of irreducible generalized Artin-Schreier polynomials

We begin this section by giving an elementary example of an irreducible Artin-Schreier polynomial. We then furnish substantially more general examples, which require the use of preliminary results from \([G]\) and \([MS]\). In fact, we give necessary and sufficient conditions for a polynomial

\[
 g(X) = X^{p^{n+e}} - X^{p^e} - g(Z') \in F[X]
\]

to be irreducible, where \( X \) and \( Z \) are algebraically independent elements over an arbitrary field \( K \) of prime characteristic \( p \), \( n > 0 \), \( r > 0 \), \( e \geq 0 \), \( F = K(Z) \), and \( g(Z) \in K[Z] \) is non-zero of degree relatively prime to \( p \).

Recall that an element \( \pi \) of and an integral domain \( D \) is irreducible if \( d \) is neither 0 nor a unit and whenever \( \pi = ab \) with \( a, b \in D \) then \( a \) or \( b \) is a unit.

It is easy to see that \( X^{p^r} - X - Z \) is irreducible in \( K[X][Z] \), hence in \( K[X, Z] \) and therefore in \( K[Z][X] \). It follows from Gauss’ Lemma (see \([J]\), §2.16) that \( X^{p^r} - X - Z \) is irreducible in \( F[X] \).

Theorem 6.1. (see \([MS]\), Proposition 1.8.9). Let \( D \) be an integral domain. Let \( X, Z \) be algebraically independent elements over \( D \). Let \( f \in D[X] \) and \( g \in D[Z] \). If \( \gcd(\deg(f), \deg(g)) = 1 \), then \( h(X, Z) = f(X) - g(Z) \) is irreducible in \( D[X, Z] \).

Theorem 6.2. (see \([G]\), Theorem 1.1). Let \( D \) be a unique factorization domain. Let \( t \) be any positive integer and let \( f \) be an irreducible polynomial in \( D[Z] \) of positive degree \( m \), leading coefficient \( a \) and nonzero constant term \( b \). Suppose that for each prime \( p \) dividing \( t \) and any unit \( u \) of \( D \) at least one of the two following statements is true:

(A) \( ua \notin D^p \);
Theorem 6.4. Let $\langle B \rangle$ (i) $(−1)^m ub \notin D^p$ and (ii) $ub \notin D^2$, if $4|t$.

Then $f(Z^t)$ is irreducible in $D[Z]$.

Theorem 6.3. (see [G], Corollary 4.6 (b)). Let $D$ be a unique factorization domain of prime characteristic $p$. Let $f(Z) \in D[Z]$ be an arbitrary polynomial of positive degree that is irreducible in $D[Z]$, and let $s$ be any positive integer. Then $f(Z^s)$ is reducible in $D[Z] \iff$ there exists a unit $u$ of $D$ such that $uf(Z) \in D^p[Z]$.

We can now prove the following result.

Theorem 6.4. Let $K$ be a field of prime characteristic $p$. Let $X, Z$ be algebraically independent elements over $K$ and set $F = K(Z)$. Let $n, e, r$ be integers such that $n > 0, r > 0$ and $e \geq 0$.

Let $g(Z) = c_0 + c_1 Z + \cdots + c_n Z$ be any polynomial whose degree $d$ is coprime with $p$. Then $h(X, Z) = (Xp^n)^r - X^p - g(Z)$ is irreducible in $F[X]$ if and only if at least one of the following conditions is satisfied:

(i) $p \nmid r$, (ii) $e = 0$, (iii) $g(Z) \notin K^p[Z]$.

Proof. By unique factorization in $\mathbb{Z}$ there exist a positive integer $r_0$ coprime with $p$ and a non-negative integer $s$ such that $r = r_0 p^s$, so $p|s$ if and only if $s \geq 1$.

Suppose first none of the conditions (i)-(iii) is fulfilled. Thus $e \geq 1$, $s \geq 1$ and $g(Z) \in K^p[Z]$. The last two conditions imply $g(Z^r) = Q^p(Z)$ for some $Q(Z)$ in $K[Z]$, and now the first condition implies that $h(X, Z)$ is a $p$th power in $F[X]$.

Suppose next that at least one of the conditions (i)-(iii) holds. We wish to show that $h(X, Z)$ is irreducible in $F[X]$.

Case (i). Suppose $p \mid r$. Therefore $p \mid dr$. Since $g(Z^r)$ has degree $dr$, from the case $D = K$, $f(X) = Xp^{se} - X^{p^e}$ of Theorem 6.1 with $g(Z^r)$ instead of $g(Z)$, we see that $h(X, Z)$ is irreducible in $K[X, Z]$, hence in $K[Z][X]$ and therefore in $F[X]$ by Gauss’ Lemma.

Case (ii). Suppose $e = 0$. The previous case guarantees that $Xp^n - X - g(Z^{r_0})$ is irreducible in $F[X]$, so we can suppose $s \geq 1$. Let $D = K[X]$. Therefore $f(Z) = Xp^n - X - g(Z^{r_0})$ is an irreducible polynomial in $D[Z]$ of degree $m = dr_0$ and constant term $b = Xp^n - X - c_0$. Since $Xp^n - X - c_0$ has no repeated roots, for any $u \in K^*$ (i.e., for any unit $u$ of $D$) we have $(-1)^m ub \notin D^p$ as well as $ub \notin D^2$ if $4|p^s$ (i.e., if $p = 2$ and $s \geq 2$). Thus part (B) of Theorem 6.2 is satisfied with $D = K[X]$ and $t = p^s$. We conclude that $f(Z^p)$ is irreducible in $D[Z]$, and therefore in $K[Z][X]$. Hence $h(X, Z) = f(Z^{p^s})$ is irreducible in $F[X]$ by Gauss’ Lemma.

Case (iii). Assume $g(Z) \notin K^p[Z]$. From the cases (i) and (ii) we can assume $s \geq 1$ and $e \geq 1$. Suppose, if possible, that $h(X, Z)$ is reducible in $F[X]$. Letting $D = K[X]$ we get, via Gauss’ Lemma, that $h(X, Z)$ is irreducible in $K[Z][X]$, and therefore in $D[Z]$. Letting $f(Z) = Xp^n - X - g(Z^{r_0})$ we get that $f(Z^p) = h(X, Z)$ is reducible in $D[Z]$. But, as seen above, $f(Z) = Xp^n - X - g(Z^{r_0})$ is irreducible in $D[Z]$ of positive degree $m = dr_0$. Hence, by Theorem 6.3 there exists a unit $u$ of $D$ and $Q \in D^p[Z]$ such that $uf(Z) = Q(Z)$. In other words, there exist $u \in K^*$ and $Q_0, Q_1, \ldots, Q_m \in K[X]$ such that

$$u\left(X^{p^n+r} - X^p - \sum_{0 \leq k \leq d} c_k Z^{k r_0}\right) = \sum_{0 \leq k \leq m} Q_k Z^k.$$
Equating coefficients of like monomials we obtain
\[ u(X^{p^{n+e}} - X^{p^e} - c_0) = Q_0^p \] and \[ uc_k = Q_{kr_0}^p \in K^p \] for \( k = 1, \ldots, d \).

Since \( Q_0 \) has degree \( m_0 = p^{n+e-1} \), there must exist \( d_0, d_1, \ldots, d_{m_0} \) in \( K \) such that
\[
Q_0 = \sum_{0 \leq k \leq m_0} d_k X^k,
\]
whence
\[
(6.1) \quad u(X^{p^{n+e}} - X^{p^e}) - uc_0 = \sum_{0 \leq k \leq m_0} d_k^p X^{kp}.
\]
Equating leading coefficients yields
\[ u = d_{m_0}^p \in K^p, \]
so \( c_k \in K^p \) for \( k = 1, \ldots, d \).

But
\[ u(X^{p^{n+e}} - X^{p^e}) = \left( d_{m_0} X^{p^{e-1}} (X - 1)^{p^{n-1}} \right)^p, \]
so (6.1) gives
\[ uc_0 = u(X^{p^{n+e}} - X^{p^e}) - Q_0^p = \left( d_{m_0} X^{p^{e-1}} (X - 1)^{p^{n-1}} - Q_0 \right)^p \in K[X]^p \cap K = K^p, \]
and a fortiori \( c_0 \in K^p \). Hence all \( c_i \in K^p \), against the fact that \( g(Z) \notin K^p[Z] \). □

**Acknowledgments.** We are grateful to D. Stanley for fruitful conversations, and R. Guralnick and A. Zalesski for useful references.

**References**

[CS] L. Cagliero and F. Szechtman, *Uniserial modules of certain solvable Lie algebras*, in preparation.

[D] L. E. Dickson, *A Fundamental System of Invariants of the General Modular Linear Group with a Solution of the Form Problem*, Trans. A.M.S. 12 (1911) 75-98.

[G] N. H. Guersenzvaig, *Elementary criteria for irreducibility of \( f(X^r) \)*, Israel J. Math. 169 (2009) 109-123.

[I] K. Iima and R. Iwamatsu, *On the Jordan decomposition of tensored matrices of Jordan canonical forms*, Math. J. Okayama Univ. 51 (2009) 133-148.

[GL] R. Gow and T. J. Laffey, *J. Group Theory*, 9 (2006) 659-672.

[GS] N. Guerszenzvaig and F. Szechtman, *Is every matrix similar to a polynomial in a companion matrix?*, Linear Algebra Appl. 437 (2012) 1611-1627.

[J] N. Jacobson, *Basic Algebra I*, Freeman, New York, 1985.

[H] J. E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Springer-Verlag, New York, 1972.

[H2] J. E. Humphreys, *Another look at Dickson’s invariants for finite linear groups*, Comm. Algebra 22 (1994) 4773-4779.

[MS] M. Mignotte and D. Ţeţeşcu, *Polynomials, An Algorithmic Approach*, Springer-Verlag, Singapore, 1999.

[Ra] T. Ralley, *Decomposition of products of modular representations*, Bull. Amer. Math. Soc. 72 (1966) 1012–1013.

[Re] J.-C. Renaud, *The decomposition of products in the modular representation ring of a cyclic group of prime power order*, J. Algebra 58 (1979) 1–11.

[Ro] W. E. Roth, *On direct product matrices*, Bull. Amer. Math. Soc. 40 (1934) 461–468.

[S] B. Srinivasan, *The modular representation ring of a cyclic \( p \)-group*, Proc. London Math. Soc. (3) 14 (1964) 677-688.

[St] R. Steinberg, *On Dickson’s theorem on invariants*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 34 (1987) 699-707.

[V] I. M. Vinogradov, *An introduction to the theory of numbers*, Pergamon Press, London, 1955.
Av. Corrientes 3985 6A, (1194) Buenos Aires, Argentina
E-mail address: nguersenz@fibertel.com.ar

Department of Mathematics and Statistics, University of Regina, Canada
E-mail address: fernando.szechtman@gmail.com