Primitive Elements for Cyclic $p^n$-extensions of Commutative Rings

Annetta G. Aramova*
PRIMITIVE ELEMENTS FOR CYCLIC $p^n$-EXTENSIONS OF COMMUTATIVE RINGS

ANNETTA G. ARAMOVA

In this note we study the existence and the construction of a primitive element for a cyclic Galois $p^n$-extension, where $p$ is a prime natural number.

Let $A$ be a commutative unitary ring which is an algebra over the prime field $F_p$. Let $B$ be a Galois extension of $A$ (cf. [1, Theorem 1.3]) with cyclic Galois group $(\sigma)$ of order $p^n$. Such a $B$ will be called a cyclic $p^n$-extension of $A$. If $B$ is generated by a single element $z$ over $A$, i.e. $B = A[z]$, we say that $z$ is a primitive element for the extension $B/A$.

It is well known that a field Galois extension has a primitive element. But there are examples of Galois extensions of rings which have no primitive elements: cf. [4], [2, Remarks 3 and 4], [3, §2]. In [2, Theorem 5] Kikumasa and Nagahara found conditions for a cyclic $2^2$-extension to have a primitive element. The theorem below generalizes this result to an arbitrary cyclic $p^n$-extension.

Notation. For a group $G$ acting on a ring $R$, we set:

$R^G = \{ x \in R \mid g(x) = x \ \forall g \in G \}$;

$t_H(x) = \sum_{h \in H} h(x)$ for a subgroup $H$ of $G$;

$G_2(a) = \{ g \in G \mid g(a) \subset a \}$ the decomposition subgroup of an ideal $a \subset R$;

$G_T(a) = \{ g \in G \mid \forall x \in R : g(x) - x \in a \}$ the inertia subgroup of $a$;

$\text{Max}(R) = \{ M \mid M \text{ is a maximal ideal of } R \}$;

$R^* = \text{the group of units of } R$;

$F_q = \text{the field with } q \text{ elements}$.

In what follows, we fix a cyclic $p^n$-extension $B/A$ with Galois group $(\sigma)$ and we set:

$B_i = B^{\sigma^i}$ for $0 \leq i \leq n$ (Clearly $B_0 = A$ and $B_n = B$);

$\text{Max}_0(A) = \{ M \in \text{Max}(A) \mid MB_i \subset \text{Max}(B_i) \}$, and abbreviate as follows:

$\text{Max}_0 = \text{Max}_0(A)$ unless there are confusions.

Finally, for a ring $S \supset A$ we denote by $\bar{s}$ the image of $s \in S$ in $\bar{S} = S/MS$ when $M$ is fixed in $\text{Max}(A)$.

Theorem. Let $B/A$ be a cyclic $p^n$-extension with Galois group $(\sigma)$ and let

---

Partially supported by MES Grant No. 29/91.
$n \geq 2$. Assume that

(i) the set $\text{Max}(A) \setminus \text{Max}_0$ is finite;
(ii) for every $M \in \text{Max}(A) \setminus \text{Max}_0$ the field $A/M$ contains at least $p^n$ elements.

Then $B/A$ has a primitive element $z$ which is of the form $z = y_0 + \sum_{i=1}^{n-1} a_i y_i$, where $a_i \in A$ for $1 \leq i \leq n-1$, and $\sigma^{p-1}(y_i) = y_i + 1$ for $1 \leq i \leq n$.

**Lemma 1** (cf. e.g. [8, Corollary 2.2]). The element $z$ is primitive for $B/A$ if and only if $\sigma^k(z) - z \in B^*$ for $1 \leq k < p^n$.

**Remarks 2.** Note that for $0 \leq j < i \leq n$, $B_i$ is a cyclic $p^{i-j}$-extension of $B_j$ with Galois group $(\sigma^p|_{B_i})$.

Fix an integer $i$, $1 \leq i \leq n$. According to [7, Theorem 1.2], applied to the extension $B_i/B_{i-1}$, there exists an element $x$ in $B_i$ such that $\sigma^{p-1}(x) = x + 1$. Set $b_k = \sigma^k(x) - x$ for $0 \leq k < p^i$. Then:

(a) $b_k \in B_{i-1}$. Indeed, $\sigma^{p-1}(b_k) = \sigma^k(x) - \sigma^{p-1}(x) = \sigma^k(x + 1) - (x + 1) = b_k$.

(b) $b_{k+1} = \sum_{j=0}^{k} \sigma^j(b_i)$ for $k < p^i - 1$. Indeed, assume that this is true for $k < p^i - 2$, then $b_{k+2} = \sigma^{p-1}(b_k) - x = \sigma(b_{k+1} + x) - x = \sum_{j=0}^{k} \sigma^{j+1}(b_i) + b_i$, hence (b) holds.

(c) $b_k = b_r + q$ for $k < p^{i-1} q + r$ with $0 \leq q < p$ and $0 \leq r < p^{i-1}$. Indeed, $\sigma^k(x) = \sigma^{p^{i-1} q + r} = \sigma^r(x + q) = \sigma^r(x + q)$. Moreover, one has:

(d) Except for $i = 1$ and $p = 2$ one has $t_{\sigma^1(b_i)}(x) = 0$. Indeed, by (c), $t_{\sigma^1(b_i)}(x) = \sum_{k=0}^{p^{i-1}-1} \sigma^k(x) = \sum_{k=0}^{p^{i-1}-1} \sum_{q=0}^{p^{i-1}-1} \sigma^r(x + q) = p \sum_{r=0}^{p^{i-1}-1} \sigma^r(x) + p^{i-1} \sum_{q=0}^{p^{i-1}-1} q$ which imples (d).

**Lemma 3.** Let $C/A$ be a cyclic $p^n$-extension with Galois group $(\rho)$. If $x \in C$ is such that $t_{\rho^i}(x) = 1$, then $\rho^i(x) = x$ for every $i$, $1 \leq i < p^n$.

**Proof.** This is easily shown: see e.g. the proof of Theorem 11 in [2].

**Lemma 4.** Let $z$ be such that $z \in B$, and $\sigma^{p^n}(z) = z + 1$. Set $b_k = \sigma^k(z) - z$ for $0 \leq k < p^n$. Then for every $M \in \text{Max}_0$ the following hold:

(a) $b_r \mod MB_{n-1} \not\equiv A/M$ for $1 \leq r < p^{n-1}$;
(b) $z \mod MB$ is primitive for $B/MB$ over $A/M$.

In particular, if $\text{Max}(A) = \text{Max}_0$, then $z$ is primitive for $B/A$.

**Proof.** Let $M \in \text{Max}_0$ and $\bar{B} = B/MB$. Then $\bar{B}$ is a cyclic $p^n$-extension of $\bar{A}$ with the induced action of $\sigma$. As $\bar{B}^{(\sigma^p)} = B_1/MB_1$ is a field, $\bar{B}$ is also a field by [7, Theorem 1.8]. By Remarks 2(a) one has $b_k \in B_{n-1}$.
Suppose that \( \bar{b}_r \in \bar{A} \) for some \( r, 1 \leq r < p^{n-1} \). Then
\[
\sigma^r(\bar{b}_i) - \bar{b}_i = \sigma^r(\sigma(\bar{z}) - \bar{z}) - (\sigma(\bar{z}) - \bar{z}) = \sigma(\bar{b}_r) - \bar{b}_r = 0.
\]
On the other hand, by Remarks 2(b) \( t_{(\sigma^{p_n-1})}(b_i) = b_{p^m-1} = 1 \). According to Lemma 3 \( \sigma^i(\bar{b}_i) \neq \bar{b}_i \) for every \( i, 1 \leq i < p^{n-1} \). This contradiction proves (a).

Next, we shall show that \( \bar{b}_k \in \bar{B}_{p^{n-1}} \) for \( 1 \leq k < p^n \) and then (b) will follow from Lemma 1. Suppose that \( \bar{b}_k = 0 \) for some \( k, 1 \leq k < p^n \). Writing \( k = p^{n-1}q + r \) with \( 0 \leq q < p \) and \( 0 \leq r < p^{n-1} \), by Remarks 2(c) one has \( \bar{b}_r = -q \in \bar{A} \). Now (a) implies that \( r = 0 \), so \( k = p^{n-1}q \) and \( b_k = q \). But as \( k \geq 1, q > 0 \) and \( \bar{b}_k = q \neq 0 \) which is a contradiction.

**Lemma 5.** Let \( M \in \text{Max}(A) \) and \( t = |\text{Max}(B \upharpoonright MB)| \). Then \( t = p^m \) for some \( m, 0 \leq m \leq n \), and \( |\text{Max}(B_m \upharpoonright MB_m)| = t \). If \( M \in \text{Max}(A) \setminus \text{Max}_0 \) then \( t > 1 \) and \( N \cap B_m \in \text{Max}_0(B_m) \) for each \( N \in \text{Max}(B) \) with \( N \supset M \). Moreover, \( |\text{Max}(B_i \upharpoonright MB_i)| = p^i \) for \( 0 \leq i \leq m \).

**Proof.** For \( N, N' \in \text{Max}(B) \) with \( N \cap N' \supset MB \), there is an element \( r \) in \( (\sigma) \) such that \( \tau(N) = N' \). Hence \( ((\sigma)(\sigma)(N)) = t \) and \( (\sigma)(\sigma)(N) = (\sigma') \). Clearly \( t = p^m \) for some \( m, 0 \leq m \leq n \). Moreover, if \( N \cap B_m = N' \cap B_m \supset M \) then, there is an element \( \rho \in (\sigma^{p^m}) \) such that \( \rho(N) = N' \) which coincides with \( N \). Hence \( N \) is the unique maximal over \( N \cap B_m \), therefore \( (N \cap B_m)B = N \). Thus \( |\text{Max}(B_m \upharpoonright MB_m)| = p^m \) (cf. [9, (20.4)]) and [7, Lemma 1.4]). The other assertions will be easily seen.

**Lemma 6.** Assume that \( |\text{Max}(A) \setminus \text{Max}_0| < \infty \) and fix an integer \( i, 1 \leq i \leq n \). Then there exists an element \( y \in B_i \) with \( \sigma^{p^i-1}(y) = y + 1 \) and such that for every \( N \in \text{Max}(B_i \setminus B_i) \) with \( M = N \cap A \notin \text{Max}_0 \), there holds for \( \bar{b}_k = (\sigma^k(y) - y) \mod N \) (\( 0 \leq k < p^{i-1} \)) one of the following conditions:

(i) \( \bar{b}_k \in \{0, 1\} \);
(ii) \( \bar{b}_k \notin A/M \).

where for \( p^m = |\text{Max}(B_i \setminus MB_i)| \),

(α) if \( p^m < p^{i-1} \) and \( 1 \leq h < p^{i-1} \) then \( \bar{b}_{p^m} \notin A/M \),
(β) if \( p^m = p^{i-1} \) then \( \bar{b}_k \in \{0, 1\} \).

**Proof.** Let \( \text{Max}(A) \setminus \text{Max}_0 = \{M_v | 1 \leq v \leq w\} \). Then \( M_v B_{i-1} = \bigcap_{u=1}^v N_{uv} \) where \( N_{uv} \in \text{Max}(B_{i-1}) \) (e.g. [7, Lemma 1.4]), so that \( \text{Max}(B_{i-1} / M_v B_{i-1}) = \{N_{uv}/M_v B_{i-1} | 1 \leq j \leq t_v\} \). By Lemma 5, we have \( t_v \leq p^{i-1} \) for \( 1 \leq v \leq w \).

Take an \( x \in B_i \) such that \( \sigma^{p^i}(x) = x + 1 \) (cf. Remarks 2). Then \( \sigma^k(x) - x \)
$\in B_{i-1}$ for $0 \leq k < p^{i-1}$. By the Chinese remainder theorem, we can choose an element $b \in B_{i-1}$ such that $b = \sigma^{i-1}(x) - x \pmod{N_{i}}$ for every $v$, $1 \leq v \leq \omega$, and for every $j$, $1 \leq j \leq t_{v}$. Now, we set $y = x + b$. Then $\sigma^{p^{i-1}}(y) = \sigma^{\omega}(x) + b = x + 1 + b = y + 1$ and $y = \sigma^{i-1}(x) \pmod{N_{i}B_{i}}$ for $1 \leq v \leq \omega$, $1 \leq j \leq t_{v}$. Moreover $b = 0 \pmod{N_{i}}$ and $\sigma^{\omega}(y) = \sigma^{\omega}(x) + \sigma^{\omega}(b) = \sigma^{\omega}(x) \pmod{N_{i}}$ for $1 \leq v \leq \omega$ by Lemma 5.

Fix $v$, $1 \leq v \leq \omega$, and set $M = M_{v}$, $t = t_{v}$, $N = N_{v}$, $N_{j} = N_{j,v}$. Then for $G = (\sigma|_{N_{i}})$, $t = [G : G_{2}(N)]$, so that $t = p^{m}$ for some $m$, $0 \leq m \leq i-1$, $G_{2}(N) = (\sigma^{p^{m}}|_{N_{i}})$, $N_{j} = \sigma^{j-1}(N)$ for $1 \leq j \leq t$, and $B_{i}^{\infty}(N) = B_{m}$. Moreover, $N_{j}$ is the unique prime over $m_{j} = N_{j} \cap B_{m}$, therefore $m_{j}B_{i-1} = N_{j}$. Thus $|\text{Max}(B_{m})| = t$, where $B_{m} = B_{m}/MB_{m}$, (cf. Lemma 5).

Now we shall show that for $k = tq + s$ with $0 \leq s < t$ and $0 \leq q < p^{i-m-1}$ one has:

(a) $\sigma^{q}(y) = \begin{cases} \sigma^{(q+1)}(y) \pmod{N_{i}B_{i}} & \text{for } 1 \leq j \leq s; \\ \sigma^{q}(y) \pmod{N_{i}B_{i}} & \text{for } s+1 \leq j \leq t. \end{cases}$

From $y - \sigma^{i-1}(x) \in N_{i}B_{i}$, it follows that $\sigma(y) - \sigma^{i}(x) \in \sigma(N_{i}B_{i})$ and since $\sigma(N_{j}) = N_{j+1}$, one obtains:

$\sigma(y) = \begin{cases} \sigma^{i}(y) \pmod{N_{i}B_{i}} & \text{for } 2 \leq j+1 \leq t. \end{cases}$

Assume that:

(b) $\sigma^{q}(y) = \begin{cases} \sigma^{q}(y) \pmod{N_{i}B_{i}} & \text{for } 1 \leq j \leq s; \\ y \pmod{N_{i}B_{i}} & \text{for } s+1 \leq j \leq t. \end{cases}$

Clearly $\sigma^{i}$ acts on $B_{i}/N_{i}B_{i}$ ($1 \leq j \leq t$). In case $1 \leq j \leq s$, we have $\sigma^{q+i}(y) \pmod{N_{j+1}B_{i}} = \sigma^{i}(\sigma(y)) \pmod{N_{j+1}B_{i}} = \sigma^{i}(y) \pmod{N_{j+1}B_{i}}$ ($2 \leq j+1 \leq s+1$). In case $s+1 \leq j \leq t-1$, we have $\sigma^{q+1}(y) \equiv \sigma(y) \equiv y \pmod{N_{j+1}B_{i}}$. Moreover in case $j = t$, we have $\sigma^{q+i}(y) \equiv \sigma(y) \pmod{N_{i}B_{i}} \equiv \sigma^{i}(y) \pmod{N_{i}B_{i}}$. Hence (b) holds for $\sigma^{*+1}$. Then $\sigma^{q}(y) \pmod{N_{j}B_{i}} = \sigma^{q}(\sigma^{i}(y) \pmod{N_{j}B_{i}}) = \sigma^{q}(y) \pmod{N_{j}B_{i}}$, therefore using (b), we obtain (a).

From Lemma 4(a) and Lemma 5, applied to the extension $B_{i}/B_{m}$, it follows that $b_{h} \pmod{N_{j}} \notin B_{m}/m_{j}$ for $1 \leq j \leq t$, $1 \leq h < p^{i-m-1}$. Hence by (a) one has:

(c) $b_{h} \pmod{N_{j}} = \begin{cases} 0 & \text{for } q = 0, s+1 \leq j \leq t; \\ 1 & \text{for } q = p^{i-m} - 1, 1 \leq j \leq s; \\ \notin B_{m}/m_{j} & \text{otherwise}. \end{cases}$

If $t = p^{i-1}$ then $q = 0$ and so, by (a), $b_{h} \pmod{N_{j}} \in \{0, 1\}$ for $1 \leq j \leq t$. This
completes the proof of the lemma.

**Proof of the theorem.** For every $i$, $1 \leq i \leq n$, take the element $y_i \in B_i$ constructed in Lemma 6.

Let $M \in \text{Max}(A) \setminus \text{Max}_0$ and set $p^n = |\text{Max}(\overline{B}_{n-1})|$. Then $m \leq n - 1$. By condition (ii) one can choose elements $a_{iw} \in A$, $1 \leq i \leq n - 1$, such that 1, $\overline{a}_{i1}, \cdots, \overline{a}_{in}$ are linearly independent in $\overline{A}$ over $F_p$, and $\overline{a}_{iw} = 0$ for $m + 1 \leq i \leq n - 1$. According to (i), for every $1 \leq i \leq n - 1$, there is an $a_i \in A$ such that $a_i \equiv a_{iw} \pmod{M}$ for each $M \in \text{Max}(A) \setminus \text{Max}_0$.

We shall prove that $z = y_n + \sum_{i=1}^{n-1} a_i y_i$ is primitive for $B/A$, by showing that $b_k = \sigma^k(z) - z \in B_{n-1}$ for $1 \leq k < p^n$ (cf. Lemma 1 and Remarks 2(a)).

Let $N \in \text{Max}(B_{n-1})$ and set $M = N \cap A$.

If $M \in \text{Max}_0$, then as $\sigma^{p^{n-1}}(z) = z + 1$, by Lemma 4(b) and Lemma 1 one has $b_k \notin N$ for $1 \leq k < p^n$.

Let $M \notin \text{Max}_0$. Then $z = \tilde{y}_n + \sum_{i=1}^{n-1} \tilde{a}_i \tilde{y}_i$, where $1, \tilde{a}_1, \cdots, \tilde{a}_m$ are linearly independent over $F_p$.

Take a $k$, $0 \leq k < p^n$, and write it in the form $k = p^{n-1}q_{n-1} + \sum_{j=0}^{n-2} p^j q_j$ with $0 \leq q_j < p$ for $0 \leq j \leq n - 1$. Set:

\[ k_i = \sum_{j=0}^{i-2} p^j q_j \quad \text{for} \quad 2 \leq i \leq n, \quad r = k_n; \]

\[ b_{iw} = \sigma^i(y_i) - y_i, \quad \tilde{b}_{iw} = b_{iw} \pmod{N \cap B_{n-1}} \quad \text{for} \quad 0 \leq v < p^n, 1 \leq i \leq n. \]

As $\sigma^p(y_i) = y_i$, by Remark 2(c) one has $b_{ik} = q_0$ and $b_{ik} = b_{ik} + q_{i-1}$ for $2 \leq i \leq n$.

Suppose that $b_k \in N$. Then, from $\sigma^k(z) - z \equiv 0 \pmod{N}$, it follows that

\[ \tilde{b}_{nr} = -q_{n-1} - \sum_{i=2}^{n} \tilde{a}_i (\tilde{b}_{ik} + q_{i-1}) - \tilde{a}_1 q_0. \]

From Lemma 5, one obtains that $|\text{Max}(\overline{B}_{n-1})| = p^{r-1}$ for $2 \leq i \leq m$. Hence $\tilde{b}_{ik} \in \{0, 1\}$ for $2 \leq i \leq m$ by Lemma 6(b) (noting $k_i < p^{r-1}$). Therefore $\tilde{b}_{nr} \in \overline{A}$, which implies that Lemma 6(i) is fulfilled for $\tilde{b}_{nr}$, that is, $\tilde{b}_{nr} \in \{0, 1\}$. Now, from the linear independence of $1, \tilde{a}_1, \cdots, \tilde{a}_m$ over $F_p$, we conclude that $q_0 = 0$, $\tilde{b}_{ik} + q_{i-1} = 0$ for $2 \leq i \leq m$, and $\tilde{b}_{nr} = -q_{n-1}$. Assume that $q_j = 0$ for $0 \leq j \leq u < m - 1$. Then $k_{u+2} = 0$ and so $b_{u+2,k_{u+2}} = 0$. Therefore $q_{u+1} = 0$. Hence $q_j = 0$ for $1 \leq j \leq m - 1$. Hence, if $m = n - 1$ then $r = 0$, $b_{nr} = 0$ and so $q_{n-1} = 0$ which implies $k = 0$. In case $m < n - 1$, we have $r = \sum_{j=m}^{n-2} p^j q_j = p^m \sum_{j=m}^{n-2} p^{j-m} q_j < p^np^{m-1}$ and $\tilde{b}_{nr} = -q_{n-1} \in A/M$. According to Lemma 6(a) this is possible only if $\sum_{j=m}^{n-2} p^{j-m} q_j = 0$. But then $r = 0$, $b_{nr} = 0$ and so $q_{n-1} = 0$. Hence $k = 0$. Therefore, it follows that $b_k \notin N$ for $1 \leq k < p^n$. 

**Produced by The Berkeley Electronic Press, 1992**
Thus, $b_k \in B^{n}_{k-1}$ for every $k, 1 \leq k < p^n$, which completes the proof of the theorem.

Remarks 7. Now we shall comment on the assumptions of the theorem. It is known [7, Theorem 1.2] that a cyclic $p$-extension always has a primitive element, so we can assume $n \geq 2$. In [4, Lemma 2] (cf. also [2, Lemma 3]) it is shown that condition (ii) is necessary for a cyclic $2^2$-extension to have a primitive element. However, there are examples of a $3^2$-extension [2, Remark 2] and of a $2^3$-extension [2, Remark 3] which show that this condition is not necessary in general. But if condition (ii) does not hold, then there are extensions which have no primitive elements: cf. e.g. the example of a $2^2$-extension of $F_4$ in [2, Remark 4]. On the other hand, in [8, Theorem 2.4] it is proved that every separable extension of an $LG$ ring $R$ of degree $d$ has a primitive element if and only if for every $M \in \text{Max}(R)$, $R/M$ has at least $d$ elements. (A commutative ring $R$ with identity is called an $LG$ ring if whenever a polynomial $g$ in $R[X_1, \cdots, X_n]$ represents a unit over $R_M$, for each $M \in \text{Max}(R)$, then $g$ represents a unit over $R$.)

Example 9 below shows that when condition (i) is not fulfilled, then there are extensions which have no primitive elements. However, this condition is not necessary in general: cf. Example 10 below.

In [2, Theorem 11] it is shown that if $\text{Max}(A) = \text{Max}_a$, then $B/A$ has a primitive element with trace 1. Taking an idea from the proof of this theorem (cf. Lemma 3), we find a primitive element with trace 0 (cf. Lemma 4 and Lemma 2(c)), which is used in order to establish the main result.

Finally, note that using [5, Théorème 2.3] we may assume that $p$ is a prime natural number in the Jacobson radical of $A$.

Lemma 8. If $n \geq 2$ and $B^* \subset A$, then $B/A$ has no primitive element.

Proof. Assume that $B = A[z]$. Then by Lemma 1 one has $\sigma(z) - z = a \in B^*$, so that $a \in A$. Hence $\sigma^p(z) = z + p\sigma = z$ which contradicts Lemma 1.

Example 9. Let $k$ be an algebraically closed field of characteristic 2 and let $B = k[x, y]$ be the polynomial ring in 2 indeterminates. Let $\sigma$ be the $k$-linear endomorphism of $B$ defined by $\sigma(x) = x + 1$, $\sigma(y) = x^2 + y + 1$. Then $\sigma$ is an automorphism of $B$ and $B$ is a cyclic $2^2$-extension of $A = B^{(\sigma)}$ which has no primitive element.

Indeed, as $y = \sigma(y) - (\sigma(x))^2$, we have $B = k[\sigma(x), \sigma(y)]$, therefore $\sigma$ is an...
automorphism. Since $\sigma^4(x) = x$, $\sigma^4(y) = y + 1$ and $\sigma^4(y) = y$, the order of $\sigma$ is 4.

Let $N \in \text{Max}(B)$. Then $N = (x - a, y - b)$ for some $a, b \in k$ and $B/N = k$. Hence, $\sigma$ being $k$-linear, $G_r(N) = G_r(N)$. Thus by [1, Theorem 1.3] $B$ is a Galois extension of $A$ if and only if $G_r(N) = 1$ for every $N \in \text{Max}(B)$. Suppose that $\sigma^i(N) \subset N$ for some $i, 1 \leq i < 4$. Then $\sigma^i(x - a) = x + i - a \in N$, therefore $i = 2$. But $\sigma^2(y - b) = y + 1 - b \notin N$. Hence $G_2(N) = 1$.

Note that $\text{Max}_0 = \phi$: if $M = N \cap A \in \text{Max}_0$, then $MB = N$ (cf. [7, Theorem 1.8]), but this is a contradiction to $G_2(N) = 1$. Thus condition (i) of the theorem does not hold.

By Lemma 7, $B/A$ has no primitive element.

**Example 10.** Let $B = F_\rho[x]$ be the polynomial ring with $q = \rho^k$. Let $\tau$ be an automorphism of $F_\bar{q}$ of order $\rho$ and let $a \in F_\bar{q}$ be such that $\tau(a) = a$. Define the automorphism $\sigma$ of $B$ by $\sigma|_{F_\bar{q}} = \tau$ and $\sigma(x) = x + a$. Then $B$ has a primitive element over $A = B^{\langle \sigma \rangle}$, although $|\text{Max}(A)/\text{Max}_0| = \infty$.

Indeed, since $\sigma^i(x) = x + 1$ and $\sigma^i(a) = a$, the order of $\sigma$ is $\rho^2$. As $\sigma^i(x) - x \in F_\bar{q}$ for $1 \leq i < \rho^2$, for every $N \in \text{Max}(B)$ one has $G_r(N) = 1$, therefore $B$ is a Galois extension of $A$ [1, Theorem 1.3], and by Lemma 1, $x$ is primitive for $B/A$.

If $f(x) = \sum_{i=0}^{\infty} a_i x^i \in A$ with $a_m \neq 0$, then $f(x) = \sigma^k(f(x)) = \sum_{i=0}^{\infty} a_i(x + 1)^i$. Equating the coefficients of $x^{m-1}$, one finds $a_{m-1} = a_{m-1} + ma_m$, so that $m = 0 \ (\rho)$.

Now let $N = (f(x)) \in \text{Max}(B)$ and $M = N \cap A$. Note that $M \in \text{Max}_0$ if and only if $G_2(N) = (\sigma)$. But if $G_2(N) = (\sigma)$, then $\sigma(f(x)) = f(x)g(x)$ with $g(x) \in B$, which is fulfilled if and only if $g(x) = 1$, i.e. $f(x) \in A$. Therefore, if $\deg f(x) \not\equiv 0 \ (\rho)$, then $f(x) \notin A$ and $G_2(N) \neq (\sigma)$. Thus $|\text{Max}(A)/\text{Max}_0| = \infty$.

**References**


A. G. ARAMOVA


INSTITUTE OF MATHEMATICS,
UL. "ACAD. G. BONCHEV" 8, 1113 SOFIA, BULGARIA

(Received May 11, 1990)