Math. J. Okayama Univ. 34 (1992), 13—20

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 (σ) 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;
$G_Z(\mathfrak{a}) = \{g \in G \mid g(\mathfrak{a}) \subset \mathfrak{a}\}$ the decomposition subgroup of an ideal $\mathfrak{a} \subset R$;
$G_T(\mathfrak{a}) = \{g \in G \mid \forall x \in R: g(x) - x \in \mathfrak{a}\}$ the inertia subgroup of $\mathfrak{a}$;
$\mathrm{Max}(R) = \{M \mid M$ is a maximal ideal of $R\}$;
$R^\times$ = the group of units of R;
F_q = the field with q elements.

In what follows, we fix a cyclic p^n-extension B/A with Galois group (σ) and we set:
$B_i = B^{(\sigma^{p^i})}$ for $0 \le i \le n$ (Clearly $B_0 = A$ and $B_n = B$);
$\mathrm{Max}_0(A) = \{M \in \mathrm{Max}(A) \mid MB_1 \in \mathrm{Max}(B_1)\}$, and abbreviate as follows:
$\mathrm{Max}_0 = \mathrm{Max}_0(A)$ 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 $\mathrm{Max}(A)$.

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

Partially supported by MES Grant No. 29/91.

$n \geq 2$. *Assume that*

(i) *the set* $\mathrm{Max}(A) \backslash \mathrm{Max}_0$ *is finite*;

(ii) *for every* $M \in \mathrm{Max}(A) \backslash \mathrm{Max}_0$ *the field* A/M *contains at least* p^n *elements.*

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

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 $\sigma^{p^{i-1}}(x) = x+1$. Set $b_k = \sigma^k(x) - x$ for $0 \leq k < p^i$. Then:

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

(b) $b_{k+1} = \sum_{j=0}^{k} \sigma^j(b_1)$ for $k < p^i - 1$. Indeed, assume that this is true for $k < p^i - 2$, then $b_{k+2} = \sigma(\sigma^{k+1}(x)) - x = \sigma(b_{k+1} + x) - x = \sum_{j=0}^{k} \sigma^{j+1}(b_1) + b_1$, 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, $\sigma^k(x) = \sigma^r \sigma^{p^{i-1}q}(x) = \sigma^r(x+q) = \sigma^r(x) + q$. Moreover, one has:

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

Lemma 3. *Let* C/A *be a cyclic* p^n*-extension with Galois group* (ρ). *If* $x \in C$ *is such that* $t_{(\rho)}(x) = 1$, *then* $\rho^i(x) \neq x$ *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* $\sigma^{p^{n-1}}(z) = z+1$. *Set* $b_k = \sigma^k(z) - z$ *for* $0 \leq k < p^n$. *Then for every* $M \in \mathrm{Max}_0$ *the following hold*:

(a) b_r *mod* $MB_{n-1} \notin A/M$ *for* $1 \leq r < p^{n-1}$;

(b) z *mod* MB *is primitive for* B/MB *over* A/M.

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

Proof. Let $M \in \mathrm{Max}_0$ and $\bar{B} = B/MB$. Then $\bar{B}$ is a cyclic p^n-extension of $\bar{A}$ with the induced action of σ. 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

$$\sigma^r(\bar{b}_1) - \bar{b}_1 = \sigma^r(\sigma(\bar{z}) - \bar{z}) - (\sigma(\bar{z}) - \bar{z})$$
$$= \sigma(\bar{b}_r) - \bar{b}_r = 0.$$

On the other hand, by Ramarks 2(b) $t_{(\sigma|B_{p^{n-1}})}(b_1) = b_{p^{n-1}} = 1$. According to Lemma 3 $\sigma^i(\bar{b}_1) \neq \bar{b}_1$ for every i, $1 \leq i < p^{n-1}$. This contradiction proves (a).

Next, we shall show that $\bar{b}_k \in \bar{B}_{n-1}^{\times}$ 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 in the form $k = p^{n-1}q + r$ 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 $M \in \mathrm{Max}(A)$ and $t = |\mathrm{Max}(B/MB)|$. Then $t = p^m$ for some m, $0 \leq m \leq n$, and $|\mathrm{Max}(B_m/MB_m)| = t$. If $M \in \mathrm{Max}(A)\backslash\mathrm{Max}_0$ then $t > 1$ and $N \cap B_m \in \mathrm{Max}_0(B_m)$ for each $N \in \mathrm{Max}(B)$ with $N \supset M$. Moreover, $|\mathrm{Max}(B_i/MB_i)| = p^i$ for $0 \leq i \leq m$.*

Proof. For $N, N' \in \mathrm{Max}(B)$ with $N \cap N' \supset MB$, there is an element τ in (σ) such that $\tau(N) = N'$. Hence $[(\sigma) : (\sigma)_Z(N)] = t$ and $(\sigma)_Z(N) = (\sigma^t)$. 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 ρ in (σ^{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 $|\mathrm{Max}(B_m/MB_m)| = p^m$ (cf. [9, (20.4)] and [7, Lemma 1.4]). The other assertions will be easily seen.

Lemma 6. *Assume that $|\mathrm{Max}(A)\backslash\mathrm{Max}_0| < \infty$ 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 $N \in \mathrm{Max}(B_{i-1})$ with $M = N \cap A \notin \mathrm{Max}_0$, there holds for $\tilde{b}_k = (\sigma^k(y) - y)$ mod N $(0 \leq k < p^{i-1})$ one of the following conditions:*

(i) $\tilde{b}_k \in \{0, 1\}$;

(ii) $\tilde{b}_k \notin A/M$,

where for $p^m = |\mathrm{Max}(B_{i-1}/MB_{i-1})|$,

(α) *if $p^m < p^{i-1}$ and $1 \leq h < p^{i-m-1}$ then $\tilde{b}_{p^m h} \notin A/M$,*

(β) *if $p^m = p^{i-1}$ then $\tilde{b}_k \in \{0, 1\}$.*

Proof. Let $\mathrm{Max}(A)\backslash\mathrm{Max}_0 = \{M_v \mid 1 \leq v \leq w\}$. Then $M_v B_{i-1} = \bigcap_{j=1}^{t_v} N_{vj}$ where $N_{vj} \in \mathrm{Max}(B_{i-1})$ (e.g. [7, Lemma 1.4]), so that $\mathrm{Max}(B_{i-1}/M_v B_{i-1}) = \{N_{vj}/M_v B_{i-1} \mid 1 \leq j \leq t_v\}$. 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 $\sigma^{p^{i-1}}(x) = x + 1$ (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 $b \equiv \sigma^{j-1}(x) - x \pmod{N_{vj}}$ for every v, $1 \leq v \leq w$, and for every j, $1 \leq j \leq t_v$. Now, we set $y = x + b$. Then $\sigma^{p^{i-1}}(y) = \sigma^{p^{i-1}}(x) + b = x + 1 + b = y + 1$ and $y \equiv \sigma^{j-1}(x) \pmod{N_{vj}B_i}$ for $1 \leq v \leq w$, $1 \leq j \leq t_v$. Moreover $b \equiv 0 \pmod{N_{v1}}$ and $\sigma^{t_v}(y) = \sigma^{t_v}(x) + \sigma^{t_v}(b) \equiv \sigma^{t_v}(x) \pmod{N_{v1}}$ for $1 \leq v \leq w$ by Lemma 5.

Fix v, $1 \leq v \leq w$, and set $M = M_v$, $t = t_v$, $N = N_{v1}$, $N_j = N_{vj}$. Then for $G = (\sigma|_{B_{i-1}})$, $t = [G : G_Z(N)]$, so that $t = p^m$ for some m, $0 \leq m \leq i-1$, $G_Z(N) = (\sigma^{p^m}|_{B_{i-1}})$, $N_j = \sigma^{j-1}(N)$ for $1 \leq j \leq t$, and $B_{i-1}^{G_Z(N)} = B_m$. Moreover, N_j is the unique prime over $\boldsymbol{m}_j = N_j \cap B_m$, therefore $\boldsymbol{m}_j B_{i-1} = N_j$. Thus $|\mathrm{Max}(\bar{B}_m)| = t$, where $\bar{B}_m = B_m/MB_m$, (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:

$$\text{(a)} \quad \sigma^k(y) \equiv \begin{cases} \sigma^{t(q+1)}(y) \pmod{N_jB_i} & \text{for } 1 \leq j \leq s; \\ \sigma^{tq}(y) \pmod{N_jB_i} & \text{for } s+1 \leq j \leq t. \end{cases}$$

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

$$\sigma(y) \equiv \begin{cases} \sigma^t(y) \pmod{N_1B_i}; \\ y \pmod{N_{j+1}B_i} & \text{for } 2 \leq j+1 \leq t. \end{cases}$$

Assume that:

$$\text{(b)} \quad \sigma^s(y) \equiv \begin{cases} \sigma^t(y) \pmod{N_jB_i} & \text{for } 1 \leq j \leq s; \\ y \pmod{N_jB_i} & \text{for } s+1 \leq j \leq t. \end{cases}$$

Clearly σ^t acts on B_i/N_jB_i $(1 \leq j \leq t)$. In case $1 \leq j \leq s$, we have $\sigma^{s+1}(y)$ mod $N_{j+1}B_i = \sigma^t(\sigma(y) \bmod N_{j+1}B_i) = \sigma^t(y) \bmod N_{j+1}$ $(2 \leq j+1 \leq s+1)$. In case $s+1 \leq j \leq t-1$, we have $\sigma^{s+1}(y) \equiv \sigma(y) \equiv y \pmod{N_{j+1}B_i}$. Moreover in case $j = t$, we have $\sigma^{s+1}(y) \equiv \sigma(y) \pmod{\sigma(N_j)B_i} \equiv \sigma^t(y) \pmod{N_1B_i}$. Hence (b) holds for σ^{s+1}. Then $\sigma^k(y) \bmod N_jB_i = \sigma^{tq}\sigma^s(y) \bmod N_jB_i = \sigma^{tq}\,(\sigma^s(y) \bmod N_jB_i)$, therefore using (b), we obtain (a).

From Lemma 4(a) and Lemma 5, applied to the extension B_i/B_m, it follows that $b_{th} \bmod N_j \notin B_m/\boldsymbol{m}_j$ for $1 \leq j \leq t, 1 \leq h < p^{i-m-1}$. Hence by (a) one has:

$$\text{(c)} \quad b_k \bmod N_j \begin{cases} = 0 & \text{for } q = 0,\ s+1 \leq j \leq t; \\ = 1 & \text{for } q = p^{i-m-1}-1,\ 1 \leq j \leq s; \\ \notin B_m/\boldsymbol{m}_j & \text{otherwise.} \end{cases}$$

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

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

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

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

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

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

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

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

$$k_i = \sum_{j=0}^{i-2} p^j q_j \text{ for } 2 \le i \le n,\ r = k_n\,;$$

$$b_{iv} = \sigma^v(y_i) - y_i,\ \tilde{b}_{iv} = b_{iv} \bmod N \cap B_{i-1} \text{ for } 0 \le v < p^n,\ 1 \le i \le n.$$

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

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

$$\tilde{b}_{nr} = -q_{n-1} - \sum_{i=2}^{m} \bar{a}_i (\tilde{b}_{ik_i} + q_{i-1}) - \bar{a}_1 q_0.$$

From Lemma 5, one obtains that $|\mathrm{Max}(\bar{B}_{i-1})| = p^{i-1}$ for $2 \le i \le m$. Hence $\tilde{b}_{ik_i} \in \{0, 1\}$ for $2 \le i \le m$ by Lemma 6(β) (noting $k_i < p^{i-1}$). Therefore $\tilde{b}_{nr} \in \bar{A}$, 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, $\bar{a}_1, \cdots, \bar{a}_m$ over F_p, we conclude that $q_0 = 0$, $\tilde{b}_{ik_i} + q_{i-1} = 0$ for $2 \le i \le m$, and $\tilde{b}_{nr} = -q_{n-1}$. Assume that $q_j = 0$ for $0 \le j \le u < m-1$. Then $k_{u+2} = 0$ and so $b_{u+2, k_{u+2}} = 0$. Therefore $q_{u+1} = 0$. Hence $q_j = 0$ for $1 \le j \le m-1$. 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 $r = \sum_{j=m}^{n-2} p^j q_j = p^m \sum_{j=m}^{n-2} p^{j-m} q_j < p^m p^{n-m-1}$ and $\tilde{b}_{nr} = -q_{n-1} \in A/M$. According to Lemma 6($\alpha$) 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 $1 \le k < p^n$.

Thus, $b_k \in B_{n-1}^{\times}$ 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 2^3-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 $M \in \mathrm{Max}(R)$, R/M has at least d elements. (A commutative ring R with identity is called an LG ring if whenever a polynomial g in $\mathrm{R}[X_1, \cdots, X_m]$ represents a unit over R_M, for each $M \in \mathrm{Max}(R)$, 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 $\mathrm{Max}(A) = \mathrm{Max}_0$, 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, Theorem 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* $B^{\times} \subset A$, *then* B/A *has no primitive element.*

Proof. Assume that $B = A[z]$. Then by Lemma 1 one has $\sigma(z) - z = a \in B^{\times}$, so that $a \in A$. Hence $\sigma^p(z) = z + pa = z$ 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 σ be the k-linear endomorphism of B defined by $\sigma(x) = x+1$, $\sigma(y) = x^2+y+1$. Then σ 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 σ is an automorphism. Since $\sigma^2(x) = x$, $\sigma^2(y) = y+1$ and $\sigma^4(y) = y$, the order of σ is 4.

Let $N \in \mathrm{Max}(B)$. Then $N = (x-a, y-b)$ for some $a, b \in k$ and $B/N = k$. Hence, σ being k-linear, $G_T(N) = G_Z(N)$. Thus by [1, Theorem 1.3] B is a Galois extension of A if and only if $G_Z(N) = 1$ for every $N \in \mathrm{Max}(B)$. 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 $G_Z(N) = 1$.

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

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

Example 10. Let $B = F_p[x]$ be the polynomial ring with $q = p^p$. Let τ be an automorphism of F_q of order p and let $\alpha \in F_q$ be such that $\mathrm{tr}_{(\tau)}(\alpha) = 1$. Define the automorphism σ of B by $\sigma|_{F_q} = \tau$ and $\sigma(x) = x+\alpha$. Then B has a primitive element over $A = B^{(\sigma)}$, although $|\mathrm{Max}(A)\backslash\mathrm{Max}_0| = \infty$.

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

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

Now let $N = (f(x)) \in \mathrm{Max}(B)$ and $M = N \cap A$. Note that $M \in \mathrm{Max}_0$ if and only if $G_Z(N) = (\sigma)$. But if $G_Z(N) = (\sigma)$, 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 $\deg f(x) \not\equiv 0$ (p), then $f(x) \notin A$ and $G_Z(N) \neq (\sigma)$. Thus $|\mathrm{Max}(A)\backslash\mathrm{Max}_0| = \infty$.

References

[1] S. Chase, D. Harrison and A. Rosenberg: Galois theory and Galois cohomology of commutative rings, Mem. Am. Math. Soc. **52** (1965), 15—33.

[2] I. Kikumasa and T. Nagahara: Primitive elements of cyclic extensions of commutative rings, Math. J. Okayama Univ. **29** (1987), 91—102.

[3] K. Kikumasa and T. Nagahara: On primitive elements of Galois extensions of finite commutative algebras, Math. J. Okayama Univ. **32** (1990), 13—24.

[4] K. Kishimoto: Notes on biquadratic cyclic extensions of a commutative ring, Math. J. Okayama Univ. **28** (1986), 15—20.

[5] A. Micali et A. Paques: Sur l'existence d'élément primitif et base normale, Bull. Soc. Math. Belg.

40 (1988), 289—295.
[6] T. Nagahara : On separable polynomials over a commutative ring II, Math. J. Okayama Univ. 15 (1972), 149—162.
[7] T. Nagahara and A. Nakajima : On cyclic extensions of commutative rings, Math. J. Okayama Univ. 15 (1971), 81—90.
[8] A. Paques : On the primitive element and normal basis theorems, Comm. in Algebra 16 (1988), 433—455.
[9] G. Scheja und U. Storch : Lokale Verzweigungstheorie, Schriftenreihe der Mathematischen Institutes der Universität Freiburg i. Ue. Nr. 5, WS 1973/74.

Institute of Mathematics,
ul. "Acad. G. Bonchev" 8, 1113 Sofia, Bulgaria

(Received May 11, 1990)