# PRIMITIVE ELEMENTS OF GALOIS EXTENSIONS OF FINITE FIELDS 

ISAO KIKUMASA AND TAKASI NAGAHARA<br>(Communicated by Louis J. Ratliff, Jr.)<br>Dedicated to Professor Nobuo Nobusawa on his sixtieth birthday


#### Abstract

As is well known, $\mathrm{N}_{q}(n)=(1 / n) \sum_{d \mid n} \mu(d) q^{n / d}$ coincides with the number of monic irreducible polynomials of $\operatorname{GF}(q)[X]$ of degree $n$. In this note we discuss the curve $n \mathrm{~N}_{X}(n)$ and the solutions of equations $n \mathrm{~N}_{X}(n)=b$ ( $b \geq n$ ). As a corollary of these results, we present a necessary and sufficient arithmetical condition for $R / K$ to have a primitive element.


## 0. Introduction

Throughout this paper, $K$ means a finite field, and all ring extensions of $K$ are assumed to be commutative and have an identity that is contained in $K$. Moreover, all Galois extensions mean that in the sense of [1]. A Galois extension $R / K$ is called simple if $R$ is $K$-algebra isomorphic to a factor ring $K[X] /(h)$ for some polynomial $h$ in $K[X]$, that is, $R / K$ has a primitive element.

In $[4,6,7]$ and etc., the authors made some studies on primitive elements of Galois extensions from several angles. On the other hand, the simplicity of separable extensions was recently discussed by J. -D. Thérond [14] in some directions. But, conditions studied in [14] are necessary and sufficient conditions so that "all" separable extensions of a semilocal ring have primitive elements. Hence, these conditions are not always applicable to discuss whether a given Galois extension is simple or not.

The purpose of this note is to study the solutions of a certain equation, which is concerned with finite fields and, using these results, to present arithmetical conditions for the simplicity of Galois extensions over $K$.

In §1 we consider a polynomial of degree $m$ :

$$
\mathrm{N}_{X}(m)=(1 / m) \sum_{d \mid m} \mu(d) X^{m / d}
$$

where $\mu$ is the Moebius function on the set of natural numbers. As in [9], for a finite field $\mathrm{GF}(q)$ with $q$ a power of a prime number, $\mathrm{N}_{q}(m)$ is the number of monic irreducible polynomials of $\operatorname{GF}(q)[X]$ of degree $m$. The aim

[^0]of this section is to pursue the curve of $m \cdot \mathrm{~N}_{X}(m)$ and to study the solutions of equations $m \cdot \mathrm{~N}_{X}(m)=b \quad(b \geq m)$ on the interval $[1, \infty)$.

In $\S 2$ we present a necessary and sufficient condition for the simplicity of Galois extensions of $K$. In this discussion, the solutions of the equations in the above play an important role.

In what follows, given a $K$-algebra $R$ and a set $S$, we use the following conventions: [ $R: K$ ] denotes the rank of $K$-module $R, l(R)$ the length of composition series of $R$-module $R$, and $|S|$ the cardinal number of $S$. Further, by $\mathbf{N}$ and $\mathbf{R}$, we denote the set of positive integers and the set of real numbers respectively.

## 1. An algebraic equation concerned with $\mathrm{N}_{q}(a)$

Let

$$
a=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \cdots p_{n}^{\alpha_{n}}
$$

where $n_{1}, \alpha_{1}, \alpha_{2}, \ldots, \alpha_{n} \in \mathbf{N}$ and $p_{1}, p_{2}, \ldots, p_{n}$ are distinct prime numbers. Then, we set

$$
\begin{align*}
& f(X)=\sum_{1 \leq e_{1}<e_{2}<\cdots<e_{i} \leq n, 0 \leq i \leq n}(-1)^{n-i} X^{p_{e_{1}} p_{e_{2}} \cdots p_{e_{i}}}  \tag{*}\\
& g(X)=X^{p_{1} p_{2} \cdots p_{n}}-f(X),
\end{align*}
$$

where $p_{e_{1}} p_{e_{2}} \cdots p_{e_{i}}=1$ if $i=0$. One will easily see that the number of terms in $f(X)$ is $\sum_{i=0}^{n}\binom{n}{i}=2^{n}$.

Now, we consider the equation

$$
f(x)=a \mathrm{~N}_{q}(a)
$$

Then, as is shown in $\S 2, \xi:=q^{a /\left(p_{1} p_{2} \cdots p_{n}\right)}$ is a solution of this equation, that is, $f(\xi)=a \mathrm{~N}_{q}(a)$. Moreover, for $K=\mathrm{GF}(q)$, a $G$-Galois extension $R / K$ with $a=|G| / l(R)$ is simple if and only if $|G| \leq a \mathrm{~N}_{q}(a)=f(\xi)$.

In this section, we study the solutions of the algebraic equation

$$
f(x)=b \quad(a \leq b \in \mathbf{N})
$$

First we prove the following theorem, which plays an important role in our study.

Theorem 1.1. Let $f(X)$ and $g(X)$ be as in (*). Then
(1) $f(1)=0$ and $g(1)=1$.
(2) $f(x)$ and $g(x)$ are strictly increasing on the interval $[1, \infty)$.

Proof. It is obvious that

$$
f(1)=\sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}=(1-1)^{n}=0
$$

and so $g(1)=1-f(1)=1$. Hence we prove (2).

For the base $e$ of the natural logarithm, we set

$$
\begin{aligned}
& h_{0}(t)=e^{t} \quad(t>0) \\
& h_{1}(t)=h_{0}\left(p_{1} t\right)-h_{0}(t)
\end{aligned}
$$

(a)

$$
\begin{aligned}
& h_{i+1}(t)=h_{i}\left(p_{i+1} t\right)-h_{i}(t) \\
& \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \\
& h_{n}(t)=h_{n-1}\left(p_{n} t\right)-h_{n-1}(t) .
\end{aligned}
$$

Then, it is easily seen that

$$
\begin{equation*}
h_{n}(t)=h_{0}\left(p_{1} \cdots p_{n} t\right)-\sum_{i=0}^{n-2} h_{i}\left(p_{i+2} \cdots p_{n} t\right)-h_{n-1}(t), \tag{b}
\end{equation*}
$$

$$
\begin{equation*}
h_{n}(t)=\sum_{1 \leq e_{1}<e_{2}<\cdots<e_{i} \leq n, 0 \leq i \leq n}(-1)^{n-i}\left(e^{t}\right)^{p_{e_{1}} \cdots p_{e_{i}}}, \tag{c}
\end{equation*}
$$

where $p_{e_{1}} \cdots p_{e_{i}}=1$ when $i=0$.
Let $\Omega_{0}$ be the set of all strictly increasing functions $h(z)$ with $h(z)>0$ on the interval $] 0, \infty$ ) and, similarly, $\Omega_{1}$ on the interval ]1, $\infty$ ). Clearly, $h_{0}^{(m)}(t)=e^{t} \in \Omega_{0}$ for $m=0,1,2, \ldots$. Assume that $0 \leq i \leq n-1$ and $h_{i}^{(m)}(t) \in \Omega_{0}$ for $m=0,1,2, \ldots$. Then for any $t>0$ and each $m \geq 0$, we have $h_{i}^{(m)}\left(p_{i+1} t\right)>h_{i}^{(m)}(t)$ and so

$$
h_{i+1}^{(m)}(t)=p_{i+1}^{m} h_{i}^{(m)}\left(p_{i+1} t\right)-h_{i}^{(m)}(t)>0
$$

This means that $h_{i+1}^{(m)}(t) \in \Omega_{0}$ for $m=0,1,2, \ldots$. Hence, we get

$$
\begin{equation*}
h_{i}^{(m)}(t) \in \Omega_{0} \quad \text { for } 0 \leq i \leq n \text { and } m \geq 0 \tag{d}
\end{equation*}
$$

In particular, $h_{n}(t) \in \Omega_{0}$. We note here that the function $t=\log _{e} x$ belongs to $\Omega_{1}$. Since $f(X)=h_{n}\left(\log _{e} X\right)$ by (c), we obtain $f(x) \in \Omega_{1}$. Moreover, by (d),

$$
\sum_{i=0}^{n-2} h_{i}\left(p_{i+2} \cdots p_{n} t\right)+h_{n-1}(t) \in \Omega_{0}
$$

This implies that $g(x) \in \Omega_{1}$ by (b). Combining these with the fact that $f(x)$ and $g(x)$ are continuous on $(-\infty,+\infty)$, we have assertion (2).
Corollary 1.2. Let $g(X)$ be as in (*). Then

$$
x \leq g(x) \leq \sum_{i=1}^{n} x^{\left(p_{1} p_{2} \cdots p_{n}\right) / p_{i}} \quad \text { for } x \geq 1
$$

In particular, if $n=1$ then $x=g(x)$.
Proof. Let $n=1$. Then obviously $x=g(x)$ and so we assume that $n \geq 2$.
Let $h_{i}(0 \leq i \leq n)$ be as in the proof of Theorem 1.1. Then, as is easily seen, we have

$$
0 \leq h_{i}(t) \leq h_{0}\left(p_{1} p_{2} \cdots p_{i} t\right) \quad \text { for } t \geq 0
$$

Hence, it follows that

$$
\begin{aligned}
0 \leq h_{i}\left(p_{i+2} \cdots p_{n} t\right) & \leq h_{0}\left(p_{1} \cdots p_{i} p_{i+2} \cdots p_{n} t\right) \\
& =\left(e^{t}\right)^{\left(p_{1} p_{2} \cdots p_{n}\right) / p_{i+1}} \quad(0 \leq i \leq n-2),
\end{aligned}
$$

and

$$
0 \leq h_{n-1}(t) \leq\left(e^{t}\right)^{\left(p_{1} p_{2} \cdots p_{n}\right) / p_{n}}
$$

Thus, by (b), we obtain that

$$
\begin{aligned}
g\left(e^{t}\right) & =\sum_{i=0}^{n-2} h_{i}\left(p_{i+2} \cdots p_{n} t\right)+h_{n-1}(t) \\
& \leq \sum_{i=0}^{n-2}\left(e^{t}\right)^{\left(p_{1} \cdots p_{n}\right) / p_{i+1}}+\left(e^{t}\right)^{\left(p_{1} \cdots p_{n}\right) / p_{n}}=\sum_{i=1}^{n}\left(e^{t}\right)^{\left(p_{1} \cdots p_{n}\right) / p_{i}} .
\end{aligned}
$$

Next, by (b) again, we have

$$
\begin{aligned}
g\left(e^{t}\right) & =h_{0}\left(p_{2} \cdots p_{n} t\right)+\left(\sum_{i=0}^{n-2} h_{i}\left(p_{i+2} \cdots p_{n} t\right)+h_{n-1}(t)\right) \\
& =h_{0}\left(p_{2} \cdots p_{n} t\right)+C=\left(e^{t}\right)^{p_{2} \cdots p_{n}}+C,
\end{aligned}
$$

where $C \geq 0$. Then $g\left(e^{t}\right)-e^{t}=\left(\left(e^{t}\right)^{p_{2} \cdots p_{n}}-e^{t}\right)+C \geq 0$ for $t \geq 0$. Setting $x=e^{t} \quad(x \geq 1)$, we obtain our assertion.
Corollary 1.3. Let $f(X)$ and $g(X)$ be given as (*).
(1) If $x \geq 2$ then $f(x) \geq g(x)$.
(2) If $0 \leq x \leq 1$ then $|f(x)|<2^{n}$.
(3) For $b \in \mathbf{R}$ with $b \geq 2^{n}$, the equation $f(x)=b$ has a solution in $] 1, \infty)$, which is unique in $] 0, \infty$ ).

Proof. (1) If $n=1$ then $f(x)-g(x)=x^{p_{1}}-2 x=x\left(x^{p_{1}-1}-2\right) \geq 0$ for $x \geq 2$.
Let $n \geq 2$ and $\alpha=p_{1} p_{2} \cdots p_{n}$. Without loss of generality, we can assume that $p_{1}<p_{2}<\cdots<p_{n}$. Then $\alpha \geq 2 p_{2} p_{3} \cdots p_{n} \geq p_{2} p_{3} \cdots p_{n}+2$. Hence the degree of the leading term of $g(x)$ is not greater than $\alpha-2$. Since all the terms in $g(x)$ have distinct degrees, we have

$$
g(x) \leq x^{\alpha-2}+x^{\alpha-3}+\cdots+x+1
$$

and so,

$$
\begin{aligned}
f(x)-g(x) & =x^{\alpha}-2 g(x) \\
& \geq x^{\alpha}-2\left(x^{\alpha-2}+x^{\alpha-3}+\cdots+x+1\right) \\
& \geq x^{\alpha}-x\left(x^{\alpha-2}+x^{\alpha-3}+\cdots+x+1\right) \\
& >x^{\alpha}-\left(x^{\alpha}-1\right) /(x-1) \\
& =\left(x^{\alpha}(x-2)+1\right) /(x-1)>0 \quad(x \geq 2) .
\end{aligned}
$$

Thus we obtain $f(x) \geq g(x)$ for $x \geq 2$.
(2) Obviously $f(0)=0$ and, by Theorem 1.1(1), $f(1)=0$. Hence we can assume that $0<x<1$. Then the absolute value of each term in $f(x)$ is less than 1 and the number of terms in $f(x)$ is $2^{n}$. Thus we have $|f(x)|<2^{n}$.
(3) This is a direct consequence of (2), Theorem 1.1(2) and $\lim _{x \rightarrow \infty} f(x)=$ $\infty$.

The following theorem is one of our main results in this note.

Theorem 1.4. Let $f(X)$ and $g(X)$ be defined by (*), and let $b \in \mathbf{N}$ with $b \geq p_{1} p_{2} \cdots p_{n}$. Then, the equation
$(* *) \quad f(x)=b \quad(x>0)$
has a unique solution. Furthermore, for the solution $x_{0}$ of the equation (**), the following inequality holds:

$$
1<x_{0} \leq g\left(x_{0}\right) \leq b
$$

Proof. Since $b \geq p_{1} p_{2} \cdots p_{n} \geq 2^{n}$, the equation $f(x)=b \quad(x>0)$ has a unique solution $x_{0}$ with $x_{0}>1$ by Corollary 1.3. Further, it follows immediately from Corollary 1.2 that $x_{0} \leq g\left(x_{0}\right)$. Let $\alpha$ be a real number with $1 / b<$ $\alpha \leq 1$. Then, since the equation $g(x)=\alpha b \quad(x>1)$ has a unique solution by Theorem 1.1, we write this by $x_{1}$. Moreover, let $x_{2}$ be the root of the equation $x^{p_{1} p_{2} \cdots p_{n}}=(\alpha+1) b=g\left(x_{1}\right)+b$. Suppose that $g\left(x_{2}\right) \leq \alpha b$. Then, by Theorem 1.1(2), we have $x_{2} \leq x_{1}$ and so

$$
f\left(x_{0}\right)=b=x_{2}^{p_{1} p_{2} \cdots p_{n}}-g\left(x_{1}\right) \leq x_{1}^{p_{1} p_{2} \cdots p_{n}}-g\left(x_{1}\right)=f\left(x_{1}\right) .
$$

In virtue of Theorem 1.1 again, we get $x_{0} \leq x_{1}$ and whence $g\left(x_{0}\right) \leq g\left(x_{1}\right)=$ $\alpha b \leq b$. Hence, to prove the theorem, all we must do is to show that the inequality $g\left(x_{2}\right) \leq \alpha b$ holds for some $\alpha$ in $\left.] 1 / b, 1\right]$. In case $b \geq 2 n^{2}$, take 1 as $\alpha$. Then it follows from Corollary 1.2 that

$$
\begin{aligned}
g\left(x_{2}\right) & \leq \sum_{i=1}^{n} x_{2}^{\left(p_{1} p_{2} \cdots p_{n}\right) / p_{i}}=\sum_{i=1}^{n}((\alpha+1) b)^{1 / p_{i}} \\
& \leq n((\alpha+1) b)^{1 / 2}=\sqrt{2 n^{2} b} \leq \sqrt{b \cdot b}=b=\alpha b, \quad \text { for } \alpha=1
\end{aligned}
$$

If $b<2 n^{2}$ then $\left(n, p_{1} p_{2}, b\right)=(2,6,6)$ or $(2,6,7)$ because $b \geq p_{1} p_{2} \cdots p_{n} \geq$ $2 \cdot 3 \cdots n(n+1)$. Let $n=2$ and $p_{1} p_{2}=b=6$. Then, putting $\alpha=2 / 3, x_{2}^{6}=10$ and so

$$
\begin{aligned}
g\left(x_{2}\right) & =x_{2}^{3}+x_{2}^{2}-x_{2}=\sqrt{10}+\sqrt[3]{10}-\sqrt[6]{10} \\
& <3.2+2.2-1.4=4=\alpha b
\end{aligned}
$$

Similarly, in case that $n=2, p_{1} p_{2}=6$, and $b=7$, we put $\alpha=6 / 7$. Then

$$
g\left(x_{2}\right)=\sqrt{13}+\sqrt[3]{13}-\sqrt[6]{13}<4+3-1=\alpha b
$$

This completes the proof.
Remark 1.5. In the notation of Theorem 1.4, we denote the solution $x_{0}$ of the equation (**) by $x_{0}(a, b)$. Moreover, we set

$$
\varepsilon(a, b)=g\left(x_{0}(a, b)\right) / b
$$

Then
(1) $0<\varepsilon(a, b) \leq 1$.
(2) If $b=p_{1}^{\beta_{1}} p_{2}^{\beta_{2}} \cdots p_{n}^{\beta_{n}}$ where $\beta_{i} \in \mathbf{N} \quad(i=1,2, \ldots, n)$ then

$$
x_{0}(a, b)=x_{0}(b, b) \quad \text { and } \quad \varepsilon(a, b)=\varepsilon(b, b)
$$

In addition, we put $\varepsilon(1, b)=0$.

Example 1.6. Let $a=2 \cdot 3$ and $b=2^{3} \cdot 3^{2}$. Then the equation ( $* *$ ) in Theorem 1.4 is

$$
x^{6}-x^{3}-x^{2}+x-72=0 \quad(x>0)
$$

As is easily seen, the solution $x_{0}(6,72)$ of this equation satisfies

$$
2.0902<x_{0}(6,72)<2.0903
$$

Moreover, from this inequality, we obtain

$$
0.158<\varepsilon(6,72)<0.159
$$

## 2. Primitive elements of Galois extensions of finite fields

Throughout this section, let $q$ be a power of a prime number. We begin this section with the following lemma, which is fundamental.

Lemma 2.1 [7, Theorem 1.6]. Let $R$ be a Galois extension of rank $b$ of $\operatorname{GF}(q)$. Then the extension $R / \mathrm{GF}(q)$ is simple if and only if $l(R) \leq \mathrm{N}_{q}(b / l(R))$.

Combining this lemma with the results in $\S 1$, we have the following theorem, which is a generalization of [5, Proposition 1].

Theorem 2.2. Let $R$ be a G-Galois extension of $\operatorname{GF}\left(p^{s}\right), b=|G|$, and $a=$ $b / l(R)$. Then the extension $R / \mathrm{GF}\left(p^{s}\right)$ is simple if and only if

$$
l(R) \leq b s /\left(\log _{p} b+\log _{p}(1+\varepsilon(a, b))\right)
$$

where $\varepsilon(a, b)$ is the constant given in §1, which depends only on $b$ and the prime divisors of $a$. In particular, when any prime divisor of $b$ divides $a$, the extension $R / \operatorname{GF}\left(p^{s}\right)$ is simple if and only if

$$
l(R) \leq b s /\left(\log _{p} b+\log _{p}(1+\varepsilon(b, b))\right)
$$

Proof. Put $q=p^{s}$. In case $l(R)=b$, it follows from Lemma 2.1 and the fact $\mathrm{N}_{q}(1)=q$ that $R / K$ is simple if and only if $l(R) \leq q$, which is equivalent to that $l(R) \leq b s /\left(\log _{p} b+\log _{p}(1+\varepsilon(a, b))\right)$. Hence we assume that $l(R) \neq b$. Let $a=p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \cdots p_{n}^{\alpha_{n}}$ where $n, \alpha_{1}, \alpha_{2}, \ldots, \alpha_{n} \in \mathbf{N}$, and $p_{1}, p_{2}, \ldots, p_{n}$ are distinct prime numbers. Moreover, let $f(X)$ be given as $(*)$. Then,

$$
\begin{aligned}
a \mathrm{~N}_{q}(a)= & \sum_{d \mid a} \mu(d) q^{a / d} \\
= & q^{a}-q^{a / p_{1}}-q^{a / p_{2}}-\cdots+q^{a\left(p_{1} p_{2}\right)}+q^{a /\left(p_{1} p_{3}\right)}+\cdots \\
& +\cdots+(-1)^{i} q^{a\left(p_{e_{1}} p_{e_{2}} \cdots p_{e_{i}}\right)}+\cdots+(-1)^{n} q^{a /\left(p_{1} p_{2} \cdots p_{n}\right)} \\
= & f\left(q^{a /\left(p_{1} p_{2} \cdots p_{n}\right)}\right),
\end{aligned}
$$

where $1 \leq e_{1}<e_{2}<\cdots<e_{i} \leq n$. We have already noted that $f(x)$ is strictly increasing on $x>1$ by Theorem 1.1 and $x_{0}(a, b)>1$ by Theorem 1.4. Hence the inequality $f\left(x_{0}(a, b)\right) \leq f\left(q^{a /\left(p_{1} p_{2} \cdots p_{n}\right)}\right)$ is equivalent to $x_{0}(a, b) \leq$ $q^{a /\left(p_{1} p_{2} \cdots p_{n}\right)}$. Since $l(R) \leq \mathrm{N}_{q}(a)$ if and only if $b \leq a \mathrm{~N}_{q}(a)$, it follows from

Lemma 2.1 that

$$
\begin{aligned}
R / K \text { is simple } & \Longleftrightarrow b \leq f\left(q^{a /\left(p_{1} p_{2} \cdots p_{n}\right)}\right) \\
& \Longleftrightarrow f\left(x_{0}(a, b)\right) \leq f\left(q^{a /\left(p_{1} p_{2} \cdots p_{n}\right)}\right) \\
& \Longleftrightarrow x_{0}(a, b) \leq q^{a /\left(p_{1} p_{2} \cdots p_{n}\right)} \\
& \Longleftrightarrow \log _{q}\left(x_{0}(a, b)^{p_{1} p_{2} \cdots p_{n}}\right) \leq a \\
& \Longleftrightarrow \log _{q}\left(b+g\left(x_{0}(a, b)\right)\right) \leq a \\
& \Longleftrightarrow b / \log _{q}\left(b+g\left(x_{0}(a, b)\right)\right) \geq b / a=l(R)
\end{aligned}
$$

Since $q=p^{s}$, we have

$$
\begin{aligned}
b / \log _{q}\left(b+g\left(x_{0}(a, b)\right)\right) & =b /\left(\log _{p}\left(b+g\left(x_{0}(a, b)\right)\right) / \log _{p} q\right) \\
& =b s /\left(\log _{p} b+\log _{p}\left(1+g\left(x_{0}(a, b)\right) / b\right)\right) \\
& =b s /\left(\log _{p} b+\log _{p}(1+\varepsilon(a, b))\right)
\end{aligned}
$$

Combining this with the previous equivalence relation, we obtain the first part of our assertion. The second assertion follows from Remark 1.5(2).

The following is a corollary of the above theorem, and it is also a direct consequence of [14, Théorème de l'élément primitif].
Corollary 2.3. Let $R / K$ be a Galois extension. If $[R: K] \leq|K|$ then $R / K$ is simple.
Proof. Let $b=[R: K] \leq|K|=p^{s}$ and $a=b / l(R)$. Then $s \geq 1$. By Remark 1.5 , there holds either

$$
l(R)=b \leq b s / \log _{p} b=b s /\left(\log _{p} b+\log _{p}(1+\varepsilon(a, b))\right)
$$

or

$$
l(R) \leq b / 2 \leq b s /(s+1) \leq b s /\left(\log _{p} b+\log _{p}(1+\varepsilon(a, b))\right)
$$

Whence $R / K$ is simple in virtue of Theorem 2.2.
Example 2.4. By [4, 7], we see that there exists a $G$-Galois extension $R / \mathrm{GF}(q)$ satisfying $q=5,|G|=72$, and $l(R)=12$. Put $b=|G|$ and $a=b / l(R)$. Then the equation ( $* *$ ) in Theorem 1.4 coincides with that in Example 1.6. Using this fact, we know that the right-hand side in the inequality of Theorem 2.2 is more than 26.1 and less than 26.2. Hence $R / \operatorname{GF}(q)$ is simple by Theorem 2.2. On the other hand, there exists a $G$-Galois extension $R / \mathrm{GF}(q)$ such that $q=5,|G|=6^{6}$, and $l(R)=6^{5}$. Then, by a direct computation, we see that $l(R)>b s /\left(\log _{p} b+\log _{p}(1+\varepsilon(a, b))\right)$. Hence, in this case, $R / \operatorname{GF}(q)$ is not simple.

## Acknowledgment

The authors would like to express their gratitude to Professor K. Motose for his helpful suggestions.

## References

1. S. U. Chase, D. K. Harrison, and Alex Rosenberg, Galois theory and Galois cohomology of commutative rings, Mem. Amer. Math. Soc., no. 52, Amer. Math. Soc., Providence, RI, 1965, pp. 15-33.
2. F. Demeyer and E. Ingraham, Separable algebras over commutative rings, Lecture Notes in Math., vol. 181, Springer-Verlag, Berlin, Heidelberg, and New York, 1971.
3. G. J. Janusz, Separable algebras over commutative rings, Trans. Amer. Math. Soc. 122 (1966), 461-479.
4. I. Kikumasa, On primitive elements of Galois extensions of commutative semi-local rings. II, Math. J. Okayama Univ. 31 (1989), 57-71.
5. I. Kikumasa and T. Nagahara, On primitive elements of Galois extensions of finite commutative algebras, Math. J. Okayama Univ. 32 (1990), 13-24.
6. Primitive elements of cyclic extensions of commutative rings, Math. J. Okayama Univ. 29 (1987), 91-102.
7. I. Kikumasa, T. Nagahara, and K. Kishimoto, On primitive elements of Galois extensions of commutative semi-local rings, Math. J. Okayama Univ. 31 (1989), 31-55.
8. K. Kishimoto, Notes on biquadratic cyclic extensions of a commutative ring, Math. J. Okayama Univ. 28 (1986), 15-20.
9. R. Lidl and Niederreiter, Finite fields, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, Massachusetts, 1983.
10. T. Nagahara, On separable polynomials over a commutative ring. II, Math. J. Okayama Univ. 15 (1972), 189-197.
11. T. Nagahara and A. Nakajima, On cyclic extensions of commuative rings, Math. J. Okayama Univ. 15 (1971), 81-90.
12. ___, On separable polynomials over a commutative ring. IV, Math. J. Okayama Univ. 17 (1974), 49-58.
13. R. S. Pierce, Associative algebras, Graduate Texts in Math., vol. 88, Springer-Verlag, Berlin, Heidelberg, and New York, 1982.
14. J. -D. Thérond, Le théorème de l'élmént primitif pour un anneau semi-local, J. Algebra 105 (1987), 29-39.
15. O. Villamayor and D. Zelinsky, Galois theory for rings with finitely many idempotents, Nagoya Math. J. 27 (1966), 721-731.
16. P. Wolf, Algebraische theorie der Galoisschen algebren, VEB Deutscher Verlag der Wissenschaften, Berlin, 1956.

Department of Mathematics, Okayama University, Okayama 700, Japan


[^0]:    Received by the editors May 30, 1990 and, in revised form, December 12, 1990.
    1980 Mathematics Subject Classification (1985 Revision). Primary 13B05; Secondary 13B25, 12E12.

