Math. J. Okayama Univ. 31 (1989), 57–71

ON PRIMITIVE ELEMENTS OF GALOIS EXTENSIONS OF COMMUTATIVE SEMI-LOCAL RINGS II

Dedicated to Professor Takasi Nagahara on his 60th birthday

ISAO KIKUMASA

Throughout this paper, all rings will be assumed to be commutative and to have identities, and a subring of a ring will mean one containing the same identity. Moreover, all Galois extensions will mean ones in the sense of [1]. A ring extension R/S will be called to be simple if R is generated by a single element over S, that is, R/S has a primitive element. Further, a Galois extension R/S will be called to be trivial if R is S-algebra isomorphic to the direct sum $S \oplus S \oplus \cdots \oplus S$ of S. For a G-Galois extension R/S, if G is a cyclic group then R/S will be called to be a cyclic extension.

In § 1, we present some preliminary results for our study in the subsequent sections. In § 2, we first consider the simplicity of Galois extensions which are the tensor products of Galois extensions over a field. We later study the simplicity of Galois extensions of a semi-local ring by using the results in the preceding part of this section. In § 3, we treat Galois extensions with no primitive elements. We give a condition that a Galois extension of a finite field is generated by m elements in this section. Furthermore, we also give a condition in case of a Galois extension of a semi-local ring.

In what follows, q will mean a power of a prime number and GF(q) will denote the finite field consisting of q elements. Moreover, "given a set S, a field K, a K-module M, a ring R, a group G of automorphisms of R, a subset H of G, and positive integers $m_1, \dots, m_n$", we will use the following conventions :

$|S|$ = the cardinal number of S.

$[M : K]$ = the dimension of ${}_K M$.

$\langle \sigma \rangle$ = the group generated by σ.

$R(H) = \{a \in R ;\ \sigma(a) = a$ for all $\sigma \in H\}$.

$\ell(R)$ = the length of the composition series of ${}_R R$.

(m_1, m_2) = the greatest common divisor of m_1 and m_2.

$\mathrm{Max}_i(m_i)$ = the maximum of $m_1, \dots, m_n$.

As to other notations and terminologies used in this paper we follow [4].

1. Preliminary Lemmas. In this section, we prepare some lemmas for our study in the subsequent sections.

We first recall the following lemma which is basic but important to study Galois extensions over fields.

Lemma 1.1 ([4, Lemma 1.1 and Lemma 1.2]). *Let K be a field and R/K a G-Galois extension. Then, there exists an H-Galois extension R_1/K such that*

(i) *R_1 is a field,*

(ii) *$|G| = |H|\ell(R)$, and*

(iii) *R is K-algebra isomorphic to $R_0 = R_1 \oplus \cdots \oplus R_r$ where $r = \ell(R)$, $R_i = R_1$ $(1 \leqq i \leqq r)$, and R_0 is a K-algebra with $K = \{(a, \dots, a)\ ;\ a \in K\}$.*

When this is the case, R_1 is isomorphic to any maximal subfield of R.

Remark 1.1. Let K be a finite field. If R/K is a Galois extension then, as in [4, Remark 1.1(3)], we can choose a cyclic group as a Galois group of R/K. Moreover, for any field extension L/K with $[L : K] < \infty$, L^r is a cyclic extension of $K = \{(a, \dots, a)\ ;\ a \in K\}$ where r is an arbitrary natural number and L^r is the direct sum of r copies of L (cf. [10, Lemma 1.1]). Hence, we may always regard a Galois extension over a finite field as a cyclic extension when we concern with the study of simplicity. Throughout, by $\mathrm{CG}(R/K)$, we denote a cyclic Galois group of R/K.

Now we set

$$\mathrm{N}_q(n) = (1/n) \textstyle\sum_{d|n} \mu(d) q^{n/d}$$

where μ is the Moebius function. If $K = \mathrm{GF}(q)$ then $\mathrm{N}_q(n)$ denotes the number of the monic irreducible polynomials in $K[X]$ of degree n (cf. [6, p. 93]). We shall present a lemma about some properties of this $\mathrm{N}_q(n)$.

Lemma 1.2. *Let d, m, n and t be positive integers.*

(1) *There holds the inequality*

$$q^{t-1}/t \leqq \mathrm{N}_q(t) \leqq q^t/t \leqq \mathrm{N}_{q^t}(1).$$

(2) *If $m \geqq 3$ and $n \geqq 2$ then*

$$\mathrm{N}_q(md)\mathrm{N}_q(nd)d \leqq \mathrm{N}_q(mnd).$$

(3) *In case* $m \geqq 2$ *and* $n \geqq 2$,

$$N_q(m)N_q(n) \leqq N_q(mn).$$

Proof. (1) It is obvious that the last inequality of (1) holds. Hence we shall show the first and second inequalities to hold.

If $t=1$ then clearly $N_q(t)=q=q^t/t>q^{t-1}/t$. Moreover, in case t is a prime number,

$$\begin{aligned} q^{t-1}/t &\leqq (q-1)q^{t-1}/t=(q^t-q^{t-1})/t \\ &\leqq (q^t-q)/t=N_q(t)<q^t/t. \end{aligned}$$

Hence we may assume that $t=ps$ for some integer $s \geqq 2$ where p is the least prime divisor of t. We note here that, for any integer $k \geqq 1$,

$$\begin{aligned} N_q(t) &\geqq (q^t-(q^s+q^{s-1}+\cdots+q))/t>(q^t-q^{s+1})/t \\ &\geqq (q^{t-1}+q^{t-1}-q^{s+1})/t \geqq q^{t-1}/t \end{aligned}$$

since $t-1-(s+1)=s(p-1)-2 \geqq 0$, and further,

$$\begin{aligned} N_q(t) &\leqq (q^t-q^s+q^{s-1}+\cdots+q)/t \\ &\leqq (q^t-q^s+q^s)/t=q^t/t. \end{aligned}$$

Thus we have (1).

(2) By (1), $q^{mnd-1}/(mnd) \leqq N_q(mnd)$. On the other hand, also by (1), $N_q(md) \leqq q^{md}/(md)$ and $N_q(nd) \leqq q^{nd}/(nd)$, and so we see that

$$N_q(md)N_q(nd)d \leqq q^{md+nd}/(mnd).$$

Since $mnd-1-(md+nd) \geqq 0$, we have the inequality of (2).

(3) If $m \geqq 3$ and $n \geqq 2$ then, putting $d=1$ in (2), we have immediately the inequality of (3). Moreover, if $m \geqq 2$ and $n \geqq 3$ then it suffices to exchange m for n. In case $m=n=2$, by a direct computation, we obtain

$$N_q(mn)=(q^4-q^2)/4>(q^2-q)^2/4=N_q(m)N_q(n).$$

Hence we get (3).

Lemma 1.3. *Let* $K=\mathrm{GF}(q)$ *and* R/K *a Galois extension of rank* n. *Moreover, let* $t=n/\ell(R)$ *and*

$$f=\Pi_{d|t}(X^{q^d}-X)^{\mu(t/d)}=\Pi_{d|t}(X^{q^{t/d}}-X)^{\mu(d)}.$$

Then the following conditions are equivalent.

(i) *R/K is simple.*

(ii) $\ell(R) \leqq N_q(t)$.

(iii) *$R \cong K[X]/(g)$ for a factor g of degree n of f.*

In particular, R/K is simple and $\ell(R) = N_q(t)$ if and only if $R \cong K[X]/(f)$.

Proof. The equivalence (i) $\Leftrightarrow$ (ii) is shown in [4, Theorem 1.6].

(i) $\Leftrightarrow$ (iii) : As in [4, Theorem 1.4] and its proof, R/K is simple if and only if $R \cong K[X]/(g)$ for the product g of $\ell(R)$ distinct monic irreducible polynomials in $K[X]$ of degree t. On the other hand, by [6, Theorem 3.29], the polynomial f in the lemma is the product of all the monic irreducible polynomials in $K[X]$ of degree t. Hence our assertion is obtained.

Example 1.1. Let $K = GF(3)$ and R_i/K $(i = 1, 2, 3)$ Galois extensions such that $\ell(R_i) = i+1$ and $[R_i : K] = 2(i+1)$ for $i = 1, 2, 3$. Note that such Galois extensions surely exist (Remark 1.1). Now, we set

$$f = \prod_{d|2} (X^{3^{2/d}} - X)^{\mu(d)}.$$

Then,

$$\begin{aligned} f &= (X^{3^2} - X)^1 \cdot (X^3 - X)^{-1} = (X^9 - X)/(X^3 - X) \\ &= (X^2+1)(X^4+1) = X^6 + X^4 + X^2 + 1. \end{aligned}$$

By Lemma 1.3, we see that R_1/K and R_2/K are simple, and moreover,

$$R_1 \cong K[X]/(X^4+1) \text{ and } R_2 \cong K[X]/(X^6+X^4+X^2+1).$$

However, since f cannot be divided by any polynomial of degree 8, R_3/K is not simple.

2. Simplicity of Galois extensions of semi-local rings. A tensor product of two (and more than two) Galois extensions over a field is also a Galois extension. In this section, we first discuss whether a Galois extension maked by such a way is simple or not, and then, we study the simplicity of Galois extensions of a semi-local ring.

We begin our study in this section with the following lemma which is fundamental on simplicity of Galois extensions obtained as tensor products of Galois extensions over a field.

Lemma 2.1. *Let K be a finite field, and R/K and S/K Galois* *extensions. Moreover, let* R_1 *and* S_1 *be maximal subfields of* R *and* S *containing* K, *respectively.*

(1) *Assume that* $[R_1 : K] \nmid [S_1 : K]$ *and* $[S_1 : K] \nmid [R_1 : K]$. *If* R/K *and* S/K *are simple then* $(R \otimes_K S)/K$ *is so and non-trivial.*

(2) *In case that* $[R_1 : K] \mid [S_1 : K]$ *or* $[S_1 : K] \mid [R_1 : K]$, *if neither* R/K *nor* S/K *is simple then* $(R \otimes_K S)/K$ *is not simple.*

Proof. Let $K = \mathrm{GF}(q)$. By Lemma 1.1, we have

$$R \cong R_1 \oplus \cdots \oplus R_r \text{ and } S \cong S_1 \oplus \cdots \oplus S_s$$

where $r = \ell(R)$, $s = \ell(S)$, $R_i = R_1$ $(1 \leqq i \leqq r)$, $S_j = S_1$ $(1 \leqq j \leqq s)$, and R_1 and S_1 are fields. Then, we have

$$R \otimes_K S \cong \textstyle\sum_{i,j} \oplus (R_i \otimes_K S_j).$$

Now we put $d = ([R_1 : K], [S_1 : K])$. Then, $[R_1 : K] = md$ and $[S_1 : K] = nd$ for some integers m and n with $m \geqq 1$, $n \geqq 1$ and $(m, n) = 1$. Further, there exist subfields E_1 and F_1 of R_1 and S_1, respectively, such that $E_1 \cong F_1$ and $[E_1 : K] = [F_1 : K] = d$. We may assume that $E := E_1 = F_1$. Since E/K is a Galois extension of rank d, $E \otimes_K S_1$ is K-algebra isomorphic to the direct sum of d copies of S_1. Hence,

$$\begin{aligned} R_1 \otimes_K S_1 &\cong R_1 \otimes_E E \otimes_K S_1 \cong R_1 \otimes_E (S_1 \oplus \cdots \oplus S_1) \\ &\cong (R_1 \otimes_E S_1) \oplus \cdots \oplus (R_1 \otimes_E S_1) \quad (d \text{ times}) \end{aligned}$$

and so,

$$R \otimes_K S \cong (R_1 \otimes_E S_1) \oplus \cdots \oplus (R_1 \otimes_E S_1) \quad (rsd \text{ times}).$$

Since $[R_1 : E] = m$ and $[S_1 : E] = n$ are relatively prime, $R_1 \otimes_E S_1$ is a field with $[(R_1 \otimes_E S_1) : K] = mnd$.

(1) Let R/K and S/K be simple. Then, using Lemma 1.3, we get $r \leqq \mathrm{N}_q(md)$ and $s \leqq \mathrm{N}_q(nd)$. Moreover, let $[R_1 : K] \nmid [S_1 : K]$ and $[S_1 : K] \nmid [R_1 : K]$. Then we may assume, without loss of generality, that $m \geqq 3$ and $n \geqq 2$. Hence, by Lemma 1.2(2),

$$\ell(R \otimes_K S) = rsd \leqq \mathrm{N}_q(md)\mathrm{N}_q(nd)d \leqq \mathrm{N}_q(mnd).$$

This implies that $(R \otimes_K S)/K$ is simple. Further, it is obvious that $(R \otimes_K S)/K$ is non-trivial.

(2) Assume that $[R_1 : K] \mid [S_1 : K]$ or $[S_1 : K] \mid [R_1 : K]$. Then $m = 1$ or $n = 1$. Hence it suffices to prove the assertion in case $m = 1$. If

R/K and S/K are not simple then $r > \mathrm{N}_q(d)$ and $s > \mathrm{N}_q(nd)$. Hence we obtain

$$\ell(R \otimes_K S) = rsd > \mathrm{N}_q(d)\mathrm{N}_q(nd)d \geqq \mathrm{N}_q(nd).$$

Combining this with Lemma 1.3, we have the assertion (2).

Proposition 2.2. *Let $K = \mathrm{GF}(q)$ and S_i/K a Galois extension such that $[S_i : K] = p^{\alpha_i}$ where p is a prime number and $\alpha_i \geqq 1$ for each i $(1 \leqq i \leqq n)$. Let $t := \mathrm{Max}_i([S_i : K]/\ell(S_i)) = [S_1 : K]/\ell(S_1)$. Then $(S_1 \otimes_K S_2 \otimes_K \cdots \otimes_K S_n)/K$ is simple if and only if $\ell(S_1)\prod_{i=2}^{n}[S_i : K] \leqq \mathrm{N}_q(t)$. When this is the case, S_1/K is simple.*

Proof. Let L_i be a maximal subfield of S_i containing K for every i $(1 \leqq i \leqq n)$. Then, we have $L_1 \otimes_K L_i = L_1 \oplus \cdots \oplus L_1$ ($[L_i : K]$ times). From this, one will easily see that L_1 is a maximal subfield of $R := S_1 \otimes_K S_2 \otimes_K \cdots \otimes_K S_n$ and $\ell(R) = \ell(S_1)\prod_{i=2}^{n}[S_i : K]$. Hence, it follows from Lemma 1.3 that R/K is simple if and only if

$$\ell(S_1)\prod_{i=2}^{n}[S_i : K] \leqq \mathrm{N}_q(t).$$

When this is the case, we have $\ell(S_1) \leqq \mathrm{N}_q(t)$, and whence S_1/K is simple.

Lemma 2.3. *Let K be a field and S_i/K $(i = 1,\dots, n)$ Galois extensions such that $[S_i : K]$ and $[S_j : K]$ are relatively prime for each $i \neq j$. If all the S_i/K are simple and non-trivial then so is $(S_1 \otimes_K S_2 \otimes_K \cdots \otimes_K S_n)/K$.*

Proof. It is enough to verify our assertion in case $n = 2$. For we have the lemma by induction if $n \geqq 3$.

Let $R = S_1$ and $S = S_2$. Then, by Lemma 1.1, we may write

$$R = E_1 \oplus \cdots \oplus E_r \text{ and } S = F_1 \oplus \cdots \oplus F_s,$$

$E_i = E_1$, $F_j = F_1$ $(1 \leqq i \leqq r,\ 1 \leqq j \leqq s)$, and E_1 and F_1 are fields. Since $([R : K], [S : K]) = 1$, $([E_1 : K], [F_1 : K]) = 1$. Moreover, since R/K and S/K are non-trivial, we have $[E_1 : K] \nmid [F_1 : K]$ and $[F_1 : K] \nmid [E_1 : K]$. Therefore it follows from Lemma 2.1 that $(R \otimes_K S)/K$ is simple and non-trivial if K is a finite field. Assume that $|K| = \infty$. Then, it suffices to show that $(R \otimes_K S)/K$ is non-trivial. However, it is clear by the argument in the above.

We have already noted that, for a G-Galois extension R over a finite field K, we may replace G with a cyclic group $CG(R/K)$. Using this fact we obtain the following corollary.

Corollary 2.4. *Let $K = GF(q)$ and R/K a Galois extension with $[R : K] = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ where the p_i are distinct prime numbers and each $\alpha_i \geqq 1$. Moreover, put $\langle \sigma \rangle = CG(R/K)$ and $S_i = R(\langle \sigma^{p_i^{\alpha_i}} \rangle)$ $(1 \leqq i \leqq n)$.*

(1) *If S_i/K is simple and non-trivial for each i $(1 \leqq i \leqq n)$ then so is R/K.*

(2) *Let $t_i = p_i^{\alpha_i}/\ell(S_i)$ $(i = 1, \dots, n)$. If $t_i \neq 1$ and $p_i^{\alpha_i} \leqq q^{t_i} - q^{t_i/p_i}$ for all i $(1 \leqq i \leqq n)$ then R/K is simple and non-trivial.*

Proof. Since each S_i/K is a cyclic extension of rank $p_i^{\alpha_i}$ and $R = S_1 \otimes_K S_2 \otimes_K \cdots \otimes_K S_n$, we have (1) immediately from Lemma 2.3. Moreover, (2) is obtained as a direct consequence of (1) and Lemma 1.3.

Remark 2.1. Let K be a field and R/K a G-Galois extension. If G is a nilpotent group then we can write $G = P_1 \times \cdots \times P_n$ where the P_i are the Sylow subgroups of G. Hence, though K is infinite, if G is nilpotent then the above corollary (1) holds by using the given G and the fixring $R(P_1 \cdots P_{i-1} P_{i+1} \cdots P_n)$ in R instead of $CG(R/K)$ and S_i, respectively.

We here present some examples.

Example 2.1. (1) Let $K = GF(4)$. We consider $R = K \oplus K$ and $S = K \oplus K \oplus K$. Then R/K and S/K are Galois extensions whose ranks are relatively prime. Moreover, they are trivial and simple by Lemma 1.3. However, since $\ell(R \otimes_K S) = 6 > 4 = N_4(1)$, $(R \otimes_K S)/K$ is not simple by the lemma.

(2) Let $K = GF(2)$, $R = GF(4) \oplus GF(4)$ and $S = GF(8)$. Then R/K and S/K are Galois extensions such that $[R : K]$ and $[S : K]$ are relatively prime. We here consider

$$R \otimes_K S \cong (GF(4) \otimes_K GF(8)) \oplus (GF(4) \otimes_K GF(8)).$$

Since $GF(4) \otimes_K GF(8)$ is a field, we have $\ell(R \otimes_K S) = 2 < 9 = N_2(6)$ (cf. [6, p. 553]). Hence $(R \otimes_K S)/K$ is simple because of Lemma 1.3. Further, this is non-trivial. However, R/K is not simple since $\ell(R) = 2 > 1 = N_2(2)$.

(3) Let $K = GF(2)$, $R = GF(4) \oplus GF(4)$ and $S = GF(8) \oplus GF(8) \oplus GF(8)$. Then, R/K and S/K are not simple, and their ranks are

relatively prime. In this case, $(R \otimes_K S)/K$ is simple. Indeed, $\ell(R \otimes_K S) = 6 < 9 = \mathrm{N}_2(6)$.

Lemma 2.5. *Let $K = \mathrm{GF}(q)$ and R/K a $\langle\sigma\rangle$-Galois extension with $[R:K] = p^\alpha u$ where p is a prime number, $\alpha \geqq 1$ and $(p, u) = 1$. Assume that there is a subfield M of R properly containing K such that, for $t := [M:K]$, t is a power of p and*

$$p^\alpha \leqq q^t - q^{t/p}.$$

Then, $R(\langle\sigma^{p^\alpha}\rangle)$ is simple and non-trivial over K.

Proof. Let L be a maximal subfield of R containing M. Moreover, set $S_1 = R(\langle\sigma^{p^\alpha}\rangle)$ and $S_2 = R(\langle\sigma^u\rangle)$. Then, $R = S_1 \otimes_K S_2$. Let L_i be a maximal subfield of S_i containing K $(i = 1, 2)$. Then, by [4, Lemma 1.1 and Lemma 1.2], we see that $S_i \cong L_i \oplus \cdots \oplus L_i$ ($\ell(S_i)$ times) for $i = 1, 2$, and $R \cong L' \oplus \cdots \oplus L'$ ($\ell(S_1)\ell(S_2)$ times) for $L' := L_1 \otimes_K L_2$. Since L' is a field, it follows that $L \cong L'$. Hence, since $t \mid [L:K]$ and $(p, [L_2 : K]) = 1$, we have $t \mid [L_1 : K]$. This implies that S_1/K is non-trivial. Noting $[S_1 : K] = p^\alpha$, we obtain from our assumption and Lemma 1.2(3) that, for $k := [L_1 : K]$,

$$\ell(S_1) = p^\alpha/k \leqq p^\alpha/t \leqq (1/t)(q^t - q^{t/p}) = \mathrm{N}_q(t) \leqq \mathrm{N}_q(k).$$

Thus S_1/K is simple by Lemma 1.3.

Theorem 2.6. *Let $K = \mathrm{GF}(q)$ and R/K a Galois extension with $[R:K] = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ where $p_1, \ldots, p_n$ are distinct primes and each $\alpha_i \geqq 1$. Assume that, for every i $(1 \leqq i \leqq n)$, there is a subfield M_i of R properly containing K such that $t_i := [M_i : K]$ is a power of p_i and*

$$p_i^{\alpha_i} \leqq q^{t_i} - q^{t_i/p_i}.$$

Then R/K is simple and non-trivial.

Proof. Let S_i be as in Corollary 2.4. Then $R = S_1 \otimes_K \cdots \otimes_K S_n$ and, by Lemma 2.5, each S_i is simple and non-trivial over K. Therefore R/K is simple by Lemma 2.3.

Corollary 2.7. *Let $K = \mathrm{GF}(q)$ and R/K a Galois extension with $[R:K] = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ where $p_1, \ldots, p_n$ are distinct primes and $\alpha_i \geqq 1$ for $i = 1, \ldots, n$. Let L be a maximal subfield of R and $[L:K] = p_1^{\beta_1} \cdots p_n^{\beta_n}$. Then*

R/K is simple and non-trivial if one of the following conditions is satisfied :

(a) $\beta_i \geqq 1$ *and* $p_i^{\alpha_i} \leqq q^{t_i} - q^{t_i/p_i}$ *with* $t_i = p_i^{\beta_i}$ *for all* i $(1 \leqq i \leqq n)$.

(b) $\beta_i \geqq 1$ *and* $(p_i - 1)/\log_2 p_i \geqq \alpha_i$ *for all* i $(1 \leqq i \leqq n)$.

When this is the case, the condition of $\beta_i \geqq 1$ $(1 \leqq i \leqq n)$ *is equivalent to that* $p_i | ([R : K]/\ell(R))$ $(1 \leqq i \leqq n)$.

Proof. Case (a) : Since L is a finite field, L contains subfields M_i with $[M_i : K] = p_i^{\beta_i}$ $(i = 1, \ldots, n)$. Hence the assertion is immediate from Theorem 2.6.

Case (b) : From the condition of (b), it follows that

$$p_i^{\alpha_i} \leqq 2^{p_i - 1} \leqq q^{p_i - 1} \leqq q^{p_i - 1}(q^{t_i - p_i + 1} - q^{(t_i/p_i) - p_i + 1}) \leqq q^{t_i} - q^{t_i/p_i}$$

where $i = 1, \ldots, $ n. Hence R/K is simple and non-trivial by (a).

The other assertion follows immediately from that $[R : K] = [L : K] \cdot \ell(R)$ (Lemma 1.1).

Remark 2.2. (1) In the statement of Theorem 2.6, the condition "properly" is necessary. For example, consider the case that $K = GF(5)$ and $R = GF(5^2) \oplus \cdots \oplus GF(5^2)$ the direct sum of 12 copies of $GF(5^2)$. Then R/K is a Galois extension of rank $2^3 \cdot 3$. Choose $GF(5^2) = \{(a, \ldots, a) ; a \in GF(5^2)\} (\subset R)$ and K as M_1 and M_2 respectively. Then, the condition $p_i^{\alpha_i} \leqq q^{t_i} - q^{t_i/p_i}$ is fulfilled for each i. But, since $\ell(R) = 12 > 10 = N_q([R : K]/\ell(R))$, R/K is not simple because of Lemma 1.3.

(2) Let $K = GF(2)$ and $R = GF(2^6) \oplus GF(2^6)$. Then, R/K is a simple Galois extension of rank $2^2 \cdot 3$. Moreover, by [4, Lemma 1.2], every maximal subfield of R containing K is isomorphic to $GF(2^6)$. Hence, if M_1 is a subfield of R properly containing K such that $t_1 = [M_1 : K]$ is a power of $p_1 = 2$ then $M_1 \cong GF(2^2)$. In this case,

$$p_1^{\alpha_1} = 2^2 > 2^2 - 2 = q^{t_1} - q^{t_1/p_1}.$$

This shows that the converse of Theorem 2.6 does not hold.

(3) In Corollary 2.7, the condition $(p_i - 1)/\log_2 p_i \geqq \alpha_i$ is independent of $|K|$ and $\ell(S_i)$. Moreover, since the function $y = (x-1)/\log_2 x$ is monotone increasing on the interval $x \geqq 2$, this inequality holds if p_i is large enough. For example, for a G-Galois extension R over a finite field K, if $|G| = 7^2 \cdot 13^3$ then

$$(7-1)/\log_2 7 > 6/3 = 2 \text{ and } (13-1)/\log_2 13 > 12/4 = 3.$$

Hence if $\ell(R) \leqq 7 \cdot 13^2$ then the Galois extension R/K is simple.

Now, in the rest of this section, we study the simlicity of Galois extensions of a semi-local ring. For this purpose, let A denote a semi-local ring and $\{M_1,\dots, M_m\}$ the set of maximal ideals of A.

First we shall prove the following theorem.

Theorem 2.8. *Let $S_1,\dots, S_n$ be Galois extensions of A whose ranks are relatively prime. If the extensions $(S_i/MS_i)/(A/M)$ $(1 \leqq i \leqq n)$ are simple and non-trivial for each maximal ideal M of A then so is $(S_1 \otimes_A S_2 \otimes_A \cdots \otimes_A S_n)/A$.*

Proof. Let M be an arbitrary maximal ideal of A. Moreover, we set $R = S_1 \otimes_A \cdots \otimes_A S_n$. Then

$$R/MR = S_1/MS_1 \otimes_{A/M} \cdots \otimes_{A/M} S_n/MS_n.$$

It is well-known that $[S_i/MS_i : A/M] = \mathrm{rank}_A S_i$ for $i = 1,\dots, n$. Since the $\mathrm{rank}_A S_i$ are relatively prime, it follows from Lemma 2.3 that R/MR is simple over A/M. Therefore, in virtue of [4, Proposition 2.1], we obtain that R/A is simple.

Corollary 2.9. *Let $S_1,\dots, S_n$ be Galois extensions of A with $\mathrm{rank}_A S_i = n_i$ $(1 \leqq i \leqq n)$ such that the n_i are relatively prime. If all S_i/A are simple and $\ell(S_i) < n_i$ for $i = 1,\dots, n$ then $(S_1 \otimes_A S_2 \otimes_A \cdots \otimes_A S_n)/A$ is simple.*

Proof. Let M be an arbitrary maximal ideal of A. Since S_i/A is simple, so is $(S_i/MS_i)/(A/M)$ for each i. Moreover, the extensions $(S_i/MS_i)/(A/M)$ are non-trivial for all i $(1 \leqq i \leqq n)$. Otherwise, for some i,

$$\ell(S_i) \geqq \ell(S_i/MS_i) = [S_i/MS_i : A/M] = n_i > \ell(S_i)$$

which is a contradiction. It follows therefore from Theorem 2.8 that $(S_1 \otimes_A \cdots \otimes_A S_n)/A$ is simple.

Corollary 2.10. *Let R/A be a G-Galois extension such that G is nilpotent and $G = P_1 \times P_2 \times \cdots \times P_n$ where the P_i are Sylow subgroups of G. For each i $(1 \leqq i \leqq n)$, let S_i be the fixring of $P_1 \cdots P_{i-1} P_{i+1} \cdots P_n$ in R. If the $(S_i/MS_i)/(A/M)$ are simple and non-trivial for all maximal ideals M of A then so is R/A.*

Proof. We see that $R = S_1 \otimes_A \cdots \otimes_A S_n$ and the $\mathrm{rank}_A S_i$ are relatively prime. Hence the assertion is a direct consequence of Theorem 2.8.

Now, let T/K be a G-Galois extension. Let K be a field and L an arbitrary maximal subfield of T containing K. Then, by [4, Lemma 1.2], any maximal subfield of T containing K is K-isomorphic to L. Given a prime number p, $p(T/K)$ denotes a power p^{α} such that $\alpha \geqq 0$, $p^{\alpha} | [L:K]$ and $p^{\alpha+1} \nmid [L:K]$. Clearly, if $p(T/K) \neq 1$ then $p | [L:K]$ and p is a divisor of $[T:K]$. Next, let $K = \mathrm{GF}(q)$. $[T:K] = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ and $[L:K] = p_1^{\beta_1} \cdots p_n^{\beta_n}$. Then $p_i(T/K) = p_i^{\beta_i}$ $(i = 1, \ldots, n)$. Therefore, it follows from Corollary 2.7 that T/K is simple and non-trivial if one of the following conditions is satisfied:

(a) $p_i(T/K) \neq 1$ and $p_i^{\alpha_i} \leqq q^{p_i(T/K)} - q^{p_i(T/K)/p_i}$ for all i $(1 \leqq i \leqq n)$.

(b) $p_i(T/K) \neq 1$ and $(p_i - 1)/\log_2 p_i \geqq \alpha_i$ for all i $(1 \leqq i \leqq n)$.

Let A be a semi-local ring with the maximal ideals M_i $(1 \leqq i \leqq m)$, and R/A a G-Galois extension with $|G| = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ where the p_i are distinct primes. We set here

$$\Omega = \{ j ;\ |A/M_j| < \infty,\ 1 \leqq j \leqq m \}.$$

If Ω is empty then R/A is simple by [4, Corollary 1.5 and Proposition 2.1]. Combining this and the above facts with the result of [4, Proposition 2.1], we obtain the following theorem under the above situation.

Theorem 2.11. *Let R/A be a G-Galois extension.*

(1) *If Ω is empty then R/A is simple.*

(2) *Assume that Ω is non-empty. Set $q_j = |A/M_j|$ and $t_{ij} = p_i((R/M_jR)/(A/M_j))$ $(j \in \Omega,\ i = 1, \ldots, n)$. Then, R/A is simple and non-trivial if one of the following conditions is satisfied:*

(a) *$t_{ij} \neq 1$ and $p_i^{\alpha_i} \leqq q_j^{t_{ij}} - q_j^{t_{ij}/p_i}$ for all i $(1 \leqq i \leqq n)$ and all $j \in \Omega$.*

(b) *$t_{ij} \neq 1$ and $(p_i - 1)/\log_2 p_i \geqq \alpha_i$ for all i $(1 \leqq i \leqq n)$ and all $j \in \Omega$.*

3. Generating elements of Galois extensions of finite fields. The main objects of our study in this section are Galois extensions of finite fields with no primitive elements. We study conditions that a Galois extension of a finite field can be generated by m elements for a positive integer m.

We first give a lemma in case of a trivial Galois extension.

Lemma 3.1. *Let $K = \mathrm{GF}(q)$ and R/K a trivial Galois extension. Then, R is generated by m elements over K if and only if $\ell(R) \leqq q^m$.*

Proof. Let m be an integer such that $\ell(R) \leqq q^m$, and put $s = q^m$. Moreover, let $S = K_1 \oplus \cdots \oplus K_s$ where $K_i = K\ (1 \leqq i \leqq s)$. Since R is a direct summand of S, if S is generated by m elements over K then so does R. Hence, in order to show the "if" part of the lemma, it is enough to prove that for S/K. As is noted in Remark 1.1, S/K is a cyclic $\langle\sigma\rangle$-extension where $K = \{(a,\ldots, a)\ ;\ a \in K\}$. We set $T_i = S(\sigma^{q^i})$ for $i = 0, 1,\ldots, m$. Let $1 \leqq i \leqq m$ and M an arbitrary maximal ideal of T_{i-1}. Since S/T_{i-1} is Galois and S is semi-local, T_{i-1} is semi-local and there exists a maximal ideal M' of S with $M' \cap T_{i-1} = M$. Noting $S \equiv K \pmod{M'}$ and $T_{i-1} \supset K$, we obtain $T_{i-1} \equiv K \pmod{M}$. Hence $|T_{i-1}/M| = |K| = q$ for all maximal ideals M of T_{i-1}. Since T_i/T_{i-1} is a Galois extension of rank q, T_i/T_{i-1} is simple by [4, Corollary 2.2]. Noting $T_m = S$ and $T_0 = K$, we see that S/K has a generating system consisting of m elements.

To see the converse, we set $r = \ell(R)$ and $R = K^r := K \oplus \cdots \oplus K$ (r times). Let R be generated by m elements $z_1,\ldots, z_m$ over K. We first consider $K[z_k]\ (1 \leqq k \leqq m)$. Put $z_k = (c_1,\ldots, c_r)\ (c_i \in K)$ and let $\{c'_1,\ldots, c'_s\}$ be the maximal subset of $\{c_1,\ldots, c_r\}$ such that $c'_i \neq c'_j$ if $i \neq j$. It is obvious that $s_k := s \leqq q$. Then, $z'_k = (c'_1, \ldots, c'_s)$ is an element of K^s and $K[z_k] \cong K[z'_k] = K^s$ (cf. [4, Theorem 1.4]). From this, we obtain

$$\ell(R) \leqq [K[z_1,\ldots, z_m] : K] \leqq [(K[z_1] \otimes_K \cdots \otimes_K K[z_m]) : K] = s_1 s_2 \cdots s_m \leqq q^m.$$

This completes the proof.

Theorem 3.2. *Let $K = \mathrm{GF}(q)$ and R/K a Galois extension and $t = [R : K]/\ell(R)$.*

(1) *Let m be a positive integer satisfying the following inequality:*

$$\ell(R) \leqq \mathrm{N}_q(t) \cdot q^{t(m-1)}.$$

Then, R is generated by m elements over K.

(2) *Assume that R is generated by m elements over K. Then,*

$$\ell(R) \leqq q^{tm}.$$

Proof. Let $L = \mathrm{GF}(q^t)$ and L^n denote the direct sum of n copies of L for $n \geqq 1$. By Lemma 1.1, we may consider $R = L^{\ell(R)}$.

(1) Let m be a positive integer such that $\ell(R) \leqq \mathrm{N}_q(t)\cdot q^{t(m-1)}$. Further, put $u = \mathrm{N}_q(t)$ and $v = q^{t(m-1)}$. Then, by Lemma 1.3, L^u is generated by an element over K. Moreover, L^v is generated by $m-1$ elements

over L because of Lemma 3.1. Since R is a direct summand of $L^{uv} \cong L^u \otimes_L L^v$, R/K has a generating system consisting of m elements.

(2) Assume that R is generated by m elements over K, and so, over L. Then, since R/L is a trivial Galois extension, our assertion is obtained from Lemma 3.1.

We here study Galois extensions generated by 2 elements in particular.

Let p be a prime number, $K = \mathrm{GF}(q)$, R/K a Galois extension of rank p^m $(m \geqq 1)$ and $t = p^m/\ell(R)$. Moreover, let L be a maximal subfield of R containing K. Then, as a direct consequence of Lemma 1.3, we obtain the following (a)—(c).

(a) If $t \neq 1$ and $\ell(R) > (1/t)(q^t - q^{t/p})$ then R/K is not simple.

(b) Assume that $t = 1$ and $\ell(R) > q$. Then R/K is not simple.

(c) If $\ell(R) \leqq (1/t)(q^t - q^{t/p})$ then R/K is simple. In case $t = 1$, if $\ell(R) \leqq q$ then R/K is simple.

Even if R/K has no primitive elements as in (a) and (b), if $\ell(R) \leqq \mathrm{N}_q(t)q^t$ then R/K has a generating system consisting of 2 elements. In this case, more in detail the following proposition holds.

Proposition 3.3. *In the notation of the above, the following* (1) *and* (2) *hold.*

(1) *If E is an intermediate field of L/K with $E \subsetneqq L$ then, R/E is simple if and only if $\ell(R) \leqq (k/t)(q^t - q^{t/p})$ for $k = [E:K]$.*

(2) *R/L is simple if and only if $\ell(R) \leqq q^t$.*

Proof. Let E be an intermediate field of L/K and $k = [E:K]$. We first note that $L \cong \mathrm{GF}(q^t)$ by Lemma 1.1. Further, as is seen in Remark 1.1, a ring extension R/E is a Galois extension of rank $\ell(R)t/k$. Hence, R/E is simple if and only if $\ell(R) \leqq \mathrm{N}_{q^k}(t/k)$ because of Lemma 1.3. Noting that if $E = L$ then $t/k = 1$, we obtain the assertion from the definition of $\mathrm{N}_q(t/k)$.

Remark 3.1. Under the hypotheses of Proposition 3.3, we see that if $\ell(R) \leqq q^t$ then R/K has a generating system consisting of 2 elements in which one is in L. At the same time, the proposition shows that if $q^t < \ell(R) \leqq (1/t)(q^t - q^{t/p})q^t$ then both generating elements of R/K must be contained in $R \backslash L$.

Finally, we present a theorem concerned with generating elements of

Galois extensions of a semi-local ring. Let A be a semi-local ring and $\{M_1,\ldots, M_m\}$ the set of maximal ideals of A. Moreover, let R/A be a G-Galois extension and, as in § 2, set $\Omega = \{j;\ |A/M_j| < \infty,\ 1 \leqq j \leqq m\}$. Then, by Theorem 2.11, if Ω is empty then R/A is simple. Hence we assume that Ω is non-empty. Then we have the following theorem as a direct consequence of Theorem 3.2 and [4, Proposition 2.1].

Theorem 3.4. *Put* $q_j = |A/M_j|$ *and* $t_j = |G|/\ell(R/M_jR)$ $(j \in \Omega)$.

(1) *Let* m_j *be a positive integer such that*

$$\ell(R/M_jR) \leqq \mathrm{N}_{q_j}(t_j)\cdot q_j^{t_j(m_j-1)}$$

for each $j \in \Omega$. *Then,* R *is generated by* $\mathrm{Max}_{j\in\Omega}(m_j)$ *elements over* A.

(2) *If* R *is generated by* m *elements over* A *then, for any* $j \in \Omega$,

$$\ell(R/M_jR) \leqq q_j^{t_jm}.$$

Corollary 3.5. *Under the hypotheses of Theorem* 3.4, *assume that* $|G| = p^\alpha$ *with* p *a prime and* $\alpha \geqq 1$. *Let* m_j *be a positive integer such that*

$$p^\alpha \leqq q_j^{t_jm_j} - q_j^{t_j(m_j-1+1/p)}$$

for each $j \in \Omega$. *Then* R *is generated by* $\mathrm{Max}_{j\in\Omega}(m_j)$ *elements over* A.

References

[1] S. U. Chase, D. K. Harrison and Alex Rosenberg : Galois theory and Galois cohomology of commutative rings, Mem. Amer. Math. Soc. 52 (1965), 15−33.

[2] G. J. Janusz : Separable algebras over commutative rings, Trans. Amer. Math. Soc. 122 (1966), 461−479.

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

[4] 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.

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

[6] R. Lidl and Niederreiter : Finite fields, Encyclopedia of Mathematics and Its Applications 20, Addison-Wesley, 1983.

[7] T. Nagahara : On separable polynomials over a commutative ring II, Math. J. Okayama Univ. 15 (1972), 149−162.

[8] T. Nagahara : On splitting rings of separable skew polynomials, Math. J. Okayama Univ. 26 (1984), 71−85.

[9] T. Nagahara and A. Nakajima : On cyclic extensions of commutative rings, Math. J. Okayama Univ. 15 (1971), 81−90.

[10] T. NAGAHARA and A. NAKAJIMA : On separable polynomials over a commutative ring IV, Math. J. Okayama Univ. 17 (1974), 49−58.

[11] J.-D. THÉROND : Le théorème de l'élément primitif pour un anneau semi-local, J. Alg. 105 (1987), 29−39.

[12] O. VILLAMAYOR and D. ZELINSKY : Galois theory for rings with finitely many idempotents, Nagoya Math. J. 27 (1966), 721−731.

DEPARTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY
OKAYAMA 700, JAPAN

(*Received August 10, 1988*)

Added in Proof: The results of [4, Theorem 1.6] and Lemma 1.3 have been sharpened in "On primitive elements of Galois extensions of commutative rings," Proc. 21st Symp. Ring Theory (Hirosaki Univ., Hirosaki, 1988), 14−20 (with T. Nagahara). The details and other assertions will appear lately.