HIROSHIMA MATH. J.
19 (1989), 309–318

Cyclic Galois extensions of regular local rings

Shiroh ITOH

(Received July 14, 1988)

§1. Introduction

Let R be a formal power series ring in d indeterminates over an algebraically closed field, and let L be a finite, abelian Galois extension of the field K of fractions of R such that the order of the Galois group is prime to the characteristic of K. Let S be the integral closure of R in L. As proved in [2], S is a free R-module of rank $n = |G|$, and hence it is a Cohen-Macaulay local ring of dimension d.

The R-algebra structure of a free R-module S defines structural constants $g(\chi, \chi') \in R$, where χ and χ' run through all characters of G(see §2); our main theorem in this note, Theorem 7 in §4, gives a condition which characterizes the invertibility of $g(\chi, \chi')$'s, and consequently, it gives a method to calculate the embedding dimension and the Cohen-Macaulay type of S. In the case that L is a cyclic Galois extension, we shall make a detailed discussion in §5; more precisely, we can compute these two numerical invariants whenever a defining equation $z^n = f$, $f \in R$, of the extension L over K is given.

Notation and terminology.

For a commutative ring A, A^* will denote the group of invertible elements in A.

Throughout this paper, R will be a noetherian domain containing an algebraically closed field K, L will be a finite Galois extension of the field K of fractions of R. We denote by G the Galois group of L over K. S will be the integral closure of R in L; we say that S is a Galois extension of R. We assume that R is a unique factorization domain (UFD), *G is abelian* and *$n = |G|$ is invertible in k.*

A character of an abelian group means a group homomorphism from it to k^*. Since the Galois group G is abelian, the set $\mathrm{Hom}(G, k^*)$ of all characters of G forms a group which is isomorphic to G; we denote by $\chi_1, \cdots, \chi_n$ the characters of the Galois group G. If H is a finite abelian group such that $(|H|, \text{char } k) = 1$, for a character χ of H, we put $e(\chi) = n^{-1}\sum_{\sigma \in H}\chi(\sigma^{-1})\sigma$; $e(\chi)$ is an element in the group ring $k[H]$.

§2. Abelian Galois extensions

In this section we shall summarize some facts on abelian Galois extensions of a UFD in order to define structural constants of S over R.

The following lemma is well known.

LEMMA 1. (1) $e(\chi_i)^2 = e(\chi_i)$ *for every* i; (2) $e(\chi_i)e(\chi_j) = 0$ *if* $i \neq j$; (3) $\sum_i e(\chi_i) = 1$.

Since L is naturally a left $K[G]$-module and S is a left $R[G]$-module, we have the following lemma.

LEMMA 2. (1) $L = e(\chi_1)L \oplus \cdots \oplus e(\chi_n)L$, *and therefore* $\dim_K e(\chi_i)L = 1$.
(2) $e(\chi_i)L = \{x \in L \mid \sigma x = \chi_i(\sigma)x$ *for all* $\sigma \in G\}$.
(3) $e(\chi_i)Le(\chi_j)L = e(\chi_i\chi_j)L$.
(4) $e(1)L = K$.

PROOF. The assertion (1) follows from Lemma 1, and the assertion (2) follows from the fact that, for every $\sigma \in G$ and $\chi \in \mathrm{Hom}(G, k^*)$, $\sigma e(\chi)x = (1/n)\sum_\tau \chi(\tau^{-1})\sigma\tau x = (1/n)\sum_\rho \chi(\rho^{-1}\sigma)\rho x = \chi(\sigma)e(\chi)x$. The assertions (3) and (4) follow from the assertion (2).

COROLLARY 3. (1) $S = e(\chi_1)S \oplus \cdots \oplus e(\chi_n)S$, *and* $e(\chi_i)S$ *is a free* R*-module of rank one for every* i.
(2) $e(\chi_i)Se(\chi_j)S$ *is contained in* $e(\chi_i\chi_j)S$.
(3) $e(1)S = R$.

PROOF. (1): The first assertion follows from Lemma 2; therefore, for every i, $e(\chi_i)S$ is a reflexive R-module of rank one, and hence it is a free R-module because R is a UFD. (3): Since $e(1)L = K$, we have $e(1)S \subseteq S \cap K = R$. On the other hand, we have $1 \in e(1)S$, because $e(1)1 = (1/n)\sum \sigma 1 = 1$. Therefore $e(1)S = R$.

DEFINITION. A G-base of S(over R) is a subset $\{\zeta(\chi) \mid \chi \in \mathrm{Hom}(G, k^*)\}$ of S such that $\zeta(1) = 1$ and, for every character χ of G, $\zeta(\chi)$ is an R-base of $e(\chi)S$. Let $\{\zeta(\chi)\}_\chi$ be a G-base of S. For any characters χ and χ' of G, we define $g(\chi, \chi')$ to be the element in R satisfying

$$\zeta(\chi)\zeta(\chi') = g(\chi, \chi')\zeta(\chi\chi').$$

For a character χ, we define $O(\chi)$ to be the ideal of R generated by

$$\{g(\chi', \chi'') \mid \chi'\chi'' = \chi,\ \chi' \neq 1 \text{ and } \chi'' \neq 1\}.$$

Although $g(\chi, \chi')$ depends on a choice of G-bases of S, it is uniquely determined up to units of R; therefore the ideal $O(\chi)$ does not depend on a choice of G-bases of S. By definition, $g(\chi, 1) = g(1, \chi) = 1$.

Assume that R and S are local rings with the maximal ideals M and N respectively such that $R/M = S/N$. Since N is also G-invariant, we have $N = e(\chi_1)N \oplus \cdots \oplus e(\chi_n)N$. By our assumption, $S/N(= e(\chi_1)S/e(\chi_1)N \oplus \cdots \oplus e(\chi_n)S/e(\chi_n)N) = R/M$; hence $N = M + \sum_{\chi \neq 1} e(\chi)S$. Consequently,

$$\dim_k N/N^2 = \dim_k M/(M^2 + O(1)) + \#\{\chi \neq 1 \mid O(\chi) \neq R\}$$

and, if R is regular,

$$\text{type } S = \#\{\chi(\neq 1) \mid g(\chi, \chi') \in M \text{ for all } \chi' \neq 1\},$$

where type S denotes the Cohen-Macaulay type of S, i.e. type S = the dimension of the socle of S/MS over $k(= \dim_k(MS :_S N)/MS)$. We shall use these equalities in later sections.

§3. $g(\chi, \chi') \cdots$ Part one

As we have discussed in the last part of the above section, it is very important to find good conditions which characterize the invertibility of $g(\chi, \chi')$'s. Throughout this section, we fix a G-base $\{\zeta(\chi)\}_\chi$ of S over R. The first fact to be remarked in this section is the following

LEMMA 4. *The discriminant ideal of S over R is generated by $\pm \prod_i ng(\chi_i, \chi_i^{-1})$, and therefore S is unramified over R if and only if $g(\chi, \chi^{-1})$ is invertible for every character χ of G. Moreover S is unramified over R if and only if $g(\chi, \chi')$ is invertible for any characters χ and χ' of G.*

PROOF. Since $\zeta(\chi_i)\zeta(\chi_j)\zeta(\chi_l) = g(\chi_i, \chi_j)g(\chi_i\chi_j, \chi_l)\zeta(\chi_i\chi_j\chi_l)$, we have $\mathrm{Tr}(\zeta(\chi_i)\zeta(\chi_j)) = 0$ if $\chi_i\chi_j \neq 1$ and $\mathrm{Tr}(\zeta(\chi_i)\zeta(\chi_j)) = ng(\chi_i, \chi_i^{-1})$ if $\chi_i\chi_j = 1$. Therefore det $\mathrm{Tr}(\zeta(\chi_i)\zeta(\chi_j)) = \pm \prod_i ng(\chi_i, \chi_i^{-1})$; thus the first assertion follows. Since $g(\chi, \chi^{-1})\zeta(\chi') = \zeta(\chi^{-1})\zeta(\chi)\zeta(\chi') = g(\chi, \chi')g(\chi^{-1}, \chi\chi')\zeta(\chi')$, we have $g(\chi, \chi^{-1}) = g(\chi, \chi')$ $g(\chi^{-1}, \chi\chi')$; thus the second asserton follows.

We first consider the case that R is a DVR *with the maximal ideal M and G is the inertia group of a maximal ideal of S.* In this case S is, in fact, a DVR; since $(n, \text{char } k) = 1$, the residue field of S is canonically isomorphic to the residue field of R and the ramification index of the maximal ideal of R is n(cf. [3, Chap. V, §10]). Let N be the maximal ideal of S. We have $\mathrm{H}^1(G, 1 + N) = 1$: Let $(u_\sigma)_\sigma$ be a 1-cocycle in $1 + N$, and put $v = n^{-1}\sum_\sigma u_\sigma^{-1}$; since $\tau v = n^{-1}\sum_\sigma \tau(u_\sigma^{-1}) = (n^{-1}\sum_\sigma u_{\tau\sigma}^{-1})u_\tau = vu_\tau$, we have $u_\tau = \tau v/v$; this shows that $\mathrm{H}^1(G, 1 + N) = 1$. It then follows from the exact sequence $1 \to 1 + N \to S^* \to (S/N)^* \to 1$ that the natural homomorphism $\mathrm{H}^1(G, S^*) \to \mathrm{H}^1(G, (S/N)^*)$ is injective; since G acts on S/N trivially, we have $H^1(G, (S/N)^*) \cong \mathrm{Hom}(G, (S/N)^*)$. Moreover the natural homomorphism $\mathrm{Hom}(G, S^*) \to \mathrm{Hom}(G, (S/N)^*)$ is an isomorphism, because *both groups are naturally isomorphic to* $\mathrm{Hom}(G, k^*)$. Therefore $\mathrm{Z}^1(G,$

S^*) is generated by $B^1(G, S^*)$ and $\mathrm{Hom}(G, S^*) \cong \mathrm{Hom}(G, k^*)$. Choose now an element u in S so that $N = Su$. For every σ in G, $\sigma(u) = a(\sigma)^{-1}u$ for some $a(\sigma) \in S^*$. It is easy to see that $\{a(\sigma)^{-1}\}_\sigma$ is a 1-cocycle, and hence there exist an element φ in Hom $(G, S^*)(\cong \mathrm{Hom}(G, k^*))$ and an element b in S^* such that $a(\sigma)^{-1} = \varphi(\sigma)\sigma b/b$ for every σ. Then $\sigma(b^{-1}u) = \sigma(b)^{-1}a(\sigma)^{-1}u = \varphi(\sigma)b^{-1}u$(cf. [1]). *We may thus assume that there exists a character φ of G such that $\sigma(u) = \varphi(\sigma)u$ for all σ in G.* Such a character φ is unique (and is called the *basic character* of the inertia group G at the maximal ideal of S): Assume that there exist a character φ' of G and a generator v of N such that $\sigma(v) = \varphi'(\sigma)v$ for all σ in G, and write $v = au$ with $a \in S^*$; it is then easy to see that $\sigma(a) = \varphi(\sigma)^{-1}\varphi'(\sigma)a$ for all σ; since G acts on S/N trivially and $\varphi(\sigma)^{-1}\varphi'(\sigma)$ is an element in k for every σ, we must have $\varphi(\sigma)^{-1}\varphi'(\sigma) = 1$ for every σ; hence $\varphi = \varphi'$, and, in particular, a is an element in R.

Summarizing the above argument, we have

LEMMA 5. *With the same notation and assumption as above, we have the following assertions.*

(1) *There exists a unique character φ of G such that, for some generator u of N, $\sigma u = \varphi(\sigma)u$ for all σ in G.*

(2) *G is cyclic and* $\mathrm{Hom}(G, k^*)$ *is generated by φ.*

(3) *$S = e(\varphi^0)S \oplus e(\varphi)S \oplus \cdots \oplus e(\varphi^{n-1})S$, and $e(\varphi^i)S = Ru^i$ for every i with $0 \leq i \leq n$. In particular,*

(4) *for integers i and j with $0 \leq i, j < n$, $g(\varphi^i, \varphi^j)$ is invertible if and only if $i + j < n$.*

(5) *$g(\varphi^i, \varphi^{-i})$ generates the maximal ideal M of R for every $i = 1, \cdots, n-1$.*

PROOF. The assertion (1) has been proved already. (2): If σ is an element in ker φ, then $\sigma u = u$, and hence σ induces the identity mapping of the completion of S, because σ induces the identity mapping of S/N; therefore $\sigma = \mathrm{id}$. This shows that φ is an injective homomorphism. Thus G is isomorphic to a finite subgroup of k^*; therefore G is cyclic, and hence so is the character group of G. Let χ be any character of G. For a moment we denote by σ a generator of G. Since $\varphi(\sigma)$ is a primitive n-th root of 1, $\chi(\sigma) = \varphi(\sigma)^l$ for some integer l; and therefore $\chi = \varphi^l$. (3): The first assertion follows from Lemma 2. It is clear that u^i is an element in $e(\varphi^i)S$, and this implies that $e(\varphi^i)S = Ru^i$ because $S = \sum_i Ru^i$. (4) follows from (3). (5): We have $MS = N^n = u^nS$ because the ramification index of M is n. Since $u^n \in R$ and S is a free R-module, u^n generates M, and this proves the assertion.

Consider now the case that R is not necessarily a DVR. Let P be a height one prime ideal of S at which S is ramified over R, and let H be the inertia group of P; H is not trivial. Put $S' = S^H$ and $Q = P \cap S'$. Appying Lemma 5 to S'_Q, S_Q and H, we have a character φ of H satisfying the condition (1) of Lemma 5.

DEFINITION. With the same notation as above, we say that φ is the *basic character* at P, and we define, for every character χ of G, the order of χ at P, denoted by $\mathrm{ord}_p(\chi)$, to be a unique non-negative integer r satisfying $\chi|_H = \varphi^r$, $0 \leq r < |H|$.

§4. $g(\chi, \chi') \cdots$ Part two

Throughout this section we fix a G-base $\{\zeta(\chi)\}_\chi$ of S over R.

We first make some remarks: Let H be a subgroup of G, and put $S' = S^H$. Then S has two representations:

$$S = \sum_{\psi:\text{char.of}H} e(\psi)S$$
$$= \sum_{\chi:\text{char.of}G} e(\chi)S.$$

For a character ψ of H, it is easy to see that

$$e(\psi)S = \sum_{\chi:\text{char. of } G \text{ such that } \chi|H=\psi} e(\chi)S.$$

It is clear that

$$S' = \sum_{\chi:\text{char. of G such that } \chi|H=1} e(\chi)S$$

and, for a character χ of G with $\chi|_H = 1$, if we denote by χ^* the induced character of G/H, then

$$e(\chi)S = e(\chi^*)S'$$

Moreover $B' = \{\zeta(\chi) | \chi \in \mathrm{Hom}(G, k^*) \text{ such that } \chi|_H = 1\}$ is a G/H-base of S' over R; therefore, for characters χ and χ' of G such that $\chi|_H = \chi'|_H = 1$, we have $g(\chi, \chi') = g(\chi^*, \chi'^*)$(with respect to B').

LEMMA 6. *Let H be a subgroup of G such that H contains every inertia groups of the maximal ideals of S. Let χ_1 and χ_2 be characters of G, and assume that $g(\chi_1, \chi_2)$ is invertible. Then for any character χ of G such that $\chi|_H = 1$, $g(\chi_1\chi, \chi^{-1}\chi_2)$ is also invertible.*

PROOF. Note first that $g(\chi_1, \chi_2)g(\chi, \chi^{-1})\zeta(\chi_1\chi_2) = \zeta(\chi_1)\zeta(\chi_2)\zeta(\chi)\zeta(\chi^{-1})$ $= g(\chi_1, \chi)g(\chi_2, \chi^{-1})\zeta(\chi_1\chi)\zeta(\chi_2\chi^{-1}) = g(\chi_1, \chi)g(\chi_2, \chi^{-1})g(\chi_1\chi, \chi^{-1}\chi_2)\zeta(\chi_1\chi_2)$. Therefore it is sufficient to show that $g(\chi, \chi^{-1})$ is invertible if $\chi|_H = 1$. Note next that $S^H = \sum_{\chi|H=1} e(\chi)S = \sum_{\chi|H=1} e(\chi^*)S^H$, where χ^* is the character of G/H induced from χ. Since S^H is unramified over R, it follows from Lemma 4 that $g(\chi, \chi^{-1})(= g(\chi^*, \chi^{*-1}))$ is invertible

For a height one prime ideal P of S at which S is *ramified* over R, we denote by $H(P)$ the inertia group of P.

THEOREM 7. *$g(\chi_1, \chi_2)$ is invertible if and only if* $\mathrm{ord}_P(\chi_1) + \mathrm{ord}_P(\chi_2)$

$< |H(P)|$ *for every height one prime ideal P of S at which S is ramified over R.*

PROOF. To prove the assertion we may assume that R is a DVR and S is ramified over R by Lemma 4; let M be the maximal ideal of R. Let H be the inertia group of the maximal ideals of S; $H \neq (1)$ by our assumption. We put $S' = S^H$. For simplicity, we put $r = |H|$. By Lemma 5 (4), $\mathrm{ord}_P(\chi_1) + \mathrm{ord}_P(\chi_2) < r$ for every maximal ideal P of S if and only if $e(\chi_1|_H)Se(\chi_2|_H)S = e(\chi_1\chi_2|_H)S$.

Assume first that $\mathrm{ord}_P(\chi_1) + \mathrm{ord}_P(\chi_2) < r$ for every maximal ideal P of S, that is, $e(\chi_1|_H)Se(\chi_1\chi_2|_H)S$. Since $e(\chi_1\chi_2)S$ is isomorphic to R, and is a direct summand of $e(\chi_1\chi_2|_H)S$, there exist characters χ' and χ'' of G such that $\chi'|_H = \chi_1|_H$, $\chi''|_H = \chi_2|_H$, $\chi'\chi'' = \chi_1\chi_2$ and $g(\chi', \chi'')$ is invertible; since $\chi' = \chi\chi_1$ and $\chi'' = \chi^{-1}\chi_2$ for some χ with $\chi|_H = 1$, it follows from Lemma 6 that $g(\chi_1, \chi_2)$ is invertible.

Conversely assume that $g(\chi_1, \chi_2)$ is invertible, and suppose, on the contrary, that $e(\chi_1|_H)Se(\chi_2|_H)S$ is properly contained in $e(\chi_1\chi_2|_H)S$; since S' is a PID, there exists a non-invertible element a in S' such that $e(\chi_1|_H)Se(\chi_2|_H)S = ae(\chi_1\chi_2|_H)S$. Write $a = \sum a_\chi \zeta(\chi)$ with $a_\chi \in R$, where χ runs through all characters of G with $\chi|_H = 1$. It then follows from our assumption that the ideal generated by $\{a_\chi g(\chi, \chi^{-1}\chi_1\chi_2) | \chi \text{ such that } \chi|_H = 1\}$ is R, and hence there exists a character χ of G such that $a_\chi g(\chi, \chi^{-1}\chi_1\chi_2)$ is invertible. Let now Q be a maximal ideal of S' such that $a \in Q$. Since every maximal ideal of S' is of the form σQ with σ in G, and since $e(\chi_1|_H)S$, $e(\chi_2|_H)S$ and $e(\chi_1\chi_2|_H)S$ are all G-stable, we see that $e(\chi_1|_H)Se(\chi_2|_H)S$ is contained in $J(S')e(\chi_1\chi_2|_H)S$, where J(S') is the Jacobson radical of S'. (Note here that $e(\chi_1\chi_2|_H)S$ is a free S'-module of rank one.)Since S' is unramified over R, $J(S') = MS'$. where M is the maximal ideal of R, and hence a is an element in $MS = \sum M\zeta(\chi)$, where χ runs through all characters of G wih $\chi|_H = 1$. Therefore a_χ is not invertible; this is a contradiction.

COROLLARY 8. *$g(\chi, \chi^{-1})$ is invertible if and only if $\chi|_H = 1$ for every inertia group H of height one prime ideal of S at which S is ramified over R. Therefore if G is the inertia group of some height one prime ideal of S at which S is ramified over R, then $g(\chi, \chi^{-1})$ is not invertible for all non-trivial character χ of G.*

COROLLARY 9. *Assume that R and S are local rings with the maximal ideals M and N respectively such that $R/M = S/N$, and let χ be a character of G. Then the image of $\zeta(\chi)$ belongs to the socle of S/MS if and only if, for every character $\chi'(\neq 1)$ of G, there exists a height one prime ideal P of S at which S is ramified over R such that* $\mathrm{ord}_P(\chi) + \mathrm{ord}_P(\chi') \geq |H(P)|$.

PROPOSITION 10. *Let P be a height one prime ideal of S at which S is ramified over R, and let χ be a non-trivial character of G. Assume that*

$$g(\chi, \chi^{-1}) \in \mathfrak{p} = P \cap R (\text{i.e., } \chi|_{H(P)} \neq 1). \quad \textit{Then } g(\chi, \chi^{-1})R_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}.$$

PROOF. To prove the assertion we may assume that R is a DVR and $\mathfrak{p}$ is the maximal ideal of R. We put $H = H(P)$. Since S^H is unramified over R, $\mathfrak{p}S^H$ is the Jacobson radical of S^H. Hence, by Lemma 5(5), $e(\chi|_H)Se(\chi^{-1}|_H)S = \mathfrak{p}S^H$, multiplying this with $e(1)$, we see that $\mathfrak{p}$ is generated by $\{g\{\chi_1, \chi_1^{-1})|\chi_1$ such that $\chi_1|_H = \chi|_H\}$. On the other hand it follows from the proof of Lemma 6 that $g(\chi_1, \chi_1^{-1})g(\chi_1^{-1}\chi, \chi^{-1}\chi_1) = g(\chi_1, \chi_1^{-1}\chi)g(\chi_1^{-1}, \chi^{-1}\chi_1)g(\chi, \chi^{-1})$; hence if $\chi_1|_H = \chi|_H$, then $\chi^{-1}\chi_1|_H = 1$, and hence, by Corollary 8, $g(\chi_1, \chi_1{}^{-1}) \in g(\chi, \chi^{-1})R$. Thus the assertion follows.

§5. Cyclic Galois extensions

In this section we assume that G is a cyclic group (of order n). Let h be a positive integer with $h \geq 2$. We consider the case $R = k[[x_1, x_2, \cdots, x_h]]$, and therefore S is also a local ring. Let M and N be the maximal ideals of R and S respectively. For every $f \in R$, we put $o(f) = \min\{l | f \in M^l\}$.

Since L is a cyclic Galois extension of K, there exists an elenent z in L such that $L = K(z)$ and $z^n \in K$. Put $z^n = f$. Let ζ be a primitive n-th root of 1, and let σ be an element in G such that $\sigma z = \zeta z$. Then σ is a generator of G. Without loss of generality we may assume that f is an element in R and has no multiple factors of order n. Let

$$f = af_1^{e(1)}f_2^{e(2)}\cdots f_r^{e(r)},\ a \in R^*,$$

be an irredundant prime decomposition of f. It is easy to see that if $\mathfrak{p}$ is a height one prime ideal of R such that $\mathfrak{p} \neq f_iR$ for all i, then S is unramified over R at $\mathfrak{p}$ and $S_\mathfrak{p} = R_\mathfrak{p}[z]$. *Throughout this section, we maintain these notations.*

We first show the following

LEMMA 11. *Let V be a noetherian local domain of dimesion one whose maximal ideal M' is generated by two elements x_0 and x_1 such that $x_1^{n(0)} = ax_0^{n(1)}$ for some invertible elemnt a. Put $d = \mathrm{GCD}(n(0), n(1))$. Assume that d is inverrible in V, $n(0) > n(1)$ and there exists an automorphism σ of V such that $\sigma a = a$, $\sigma x_0 = x_0$ and $\sigma x_1 = \zeta x_1$, where ζ is a primitive $n(0)$-th root of 1. Let W be the integral closure of V. Then the Jacobson radical of W is generared by an element t in W such that $\sigma t = \zeta^v t$, where v is an integer satisfying $vn(1) \equiv d (\mathrm{mod}\ n(0))$. Moreover the order of x_0 at the maximal ideals of W is $n(0)/d$.*

PROOF. We take the continued fraction expansion

$$n(0)/n(1) = r_0 + 1/(r_1 + 1/(r_2 + \cdots + 1/r_s))$$

with $r_s > 1$, and we define $n(2), \cdots, n(s+1)$ inductively as follows:

$$n(i)/n(i+1) = r_i + 1/(r_{i+1} + 1/(r_{i+2} + \cdots + 1/r_s))$$

for $i = 0, \cdots, s$. By definition $n(i) = r_i n(i+1) + n(i+2)$ for $i = 0, \cdots, s-2$, and moreover $n(s) = n(s+1)r_s = dr_s$ because $d = \mathrm{GCD}(n(0), n(1)) = \mathrm{GCD}(n(s), n(s+1)) = n(s+1)$. We then put $x_{i+1} = x_{i-1}/x_i^{r_i} - 1$ for $i = 1, \cdots, s+1$; inductively, we can see that $x_i^{n(i-1)} = c_i x_{i-1}^{n(i)}$, where $c_i = a$ or a^{-1}, for every $i = 1, \cdots, s+1$; thus each x_i is integral over V; moreover $W = V[x_2, \cdots, x_{s+1}]$ is a local ring whose maximal ideal is generated by x_s and x_{s+1}, and $W'[x_{s+2}]$ is a homomorphic image of $W'' = W'[T]/(c_{s+1}T^d - 1)$. Since W'' is unramified over W'', so is $W'[x_{s+2}]$ over W'. Therefore $x_{s+1}W'[x_{s+2}]$ is the Jacobson radical of $W'[x_{s+2}]$, and hence $W = W'[x_{s+2}] = V[x_2, \cdots, x_{s+2}]$. We put $v(0) = 0$, $v(1) = 1$ and $v(i+1) = v(i-1) + r_{i-1}v(i)$ for $i = 1, \cdots, s+1$. Moreover we put $v'(i) = (-1)^{i+1}v(i)$ for $i = 0, \cdots, s+1$. Since $x_{i+1} = x_{i-1}/x_i^{r_i} - 1$, we easily see that $\sigma x_i = \zeta^{v'(i)}x_i$ and $x_0 = x_i^{v(i+1)}x_{i+1}^{v(i)}$ for every i by the induction on i. Therfore $\sigma x_{s+1} = \zeta^{v'(s+1)}x_{s+1}$ and $x_0 = x_{s+1}^{v(s+2)}x_{s+2}^{v(s+1)}$. It follows from [4, Theorem 2.2 and Theorem 2.3], that $n(0) = v(s+2)n(s+1)$ and $(-1)^{s+1}n(s+1) \equiv -v(s+1)n(1) \pmod{n(0)}$. Since $n(s+1) = d$, the lemma follows.

We now put $d(i) = \mathrm{GCD}(n, e(i))$ and choose a positive integer $v(i)$ so that $v(i)e(i) \equiv d(i) \pmod{n}$ for $i = 1, \cdots, r$. Let ψ be the character of G satisfying $\psi(\sigma) = \zeta$. Let $H(i)$ be the inertia group of the prime ideals of S lying over f_iR, and let V_i be the localization of $R[z]$ with respect to $R\text{-}f_iR$. V_i is a local ring, and whose maximal ideal is generated by z and f_i satisfying the following conditions: $z^{n(0)} = \alpha f_i^{e(i)}$, $\alpha \in V_i^*$, $\sigma\alpha = \alpha$. Thus by Lemma 11 and [3, Chap. V, Theorem 24], we see that $H(i)$ is generated by $\sigma^{d(i)}$ and the basic character at the prime ideals is $\psi^{v(i)}|_{H(i)}$.

Proposition 12. *Assume that $d(i) = 1$ for all i (e.g., n is a prime number), and that, if $r = 1$, f_1 is contained in M^2. Then the following conditions are equivalent:*

(1) *S is a Gorenstein ring;*

(2) *S is a hypersurface;*

(3) $e(1) = \cdots = e(r)$.

Proof. Note first that, for every height one prime ideal P of S at which S is ramified over R, G is the inertia group of P, and hence $\mathrm{ord}_P(\chi) \neq 0$ for all non-trivial characters χ of G; thus by Corollary 9, the image of $\zeta((\psi^{v(i)})^{n-1})$ in S/MS is an element in the socle of S/MS. Therefore if S is a Gorenstein ring, then $v(1)(n-1) \equiv \cdots \equiv v(r)(n-1) \pmod{n}$, i.e. $v(1) = \cdots = v(r)$; since $v(i)e(i) \equiv 1 \pmod{n}$ for $i = 1, \cdots, r$, we have $e(1) = \cdots = e(r)$. Hence (1) implies (3). Assume now (3). Then, by definition, $v(1) = \ldots = v(r)$. We put $v = v(1)$. By Corollary 8, $O(1)$ is contained in every f_iR, and therefore $O(1)$ is contained in M^2. By Lemma 11 above, ψ^v is the basic character at the prime ideal of S lying over f_iR for every i. It then follows from Theorem 7 that $O(\chi) = R$ if $\chi \neq 1, \psi^v$. Therefore S is a hypersurface.

We now consider the case that $d(i) > 1$ for some i.

For integers i and l such that $1 \leq i \leq r$ and $0 < l < n$, we denote by $w(i, l)$ the integer satisfying the conditions $0 < w(i, l) < n/d(i)$ and $le(i)/d(i) \equiv w(i, l)(\text{mod } n/d(i))$; in other words, $w(i, l)$ is the order of ψ^l at the prime ideals of S lying over $f_i R$. We also denote by $\zeta^{\sim}(\psi^l)$ the image of $\zeta(\psi^l)$ in S/MS.

The next proposition then follows from Theorem 7 and Proposition 10.

PROPOSITION 13. (1) *The following two conditions are equivalent*:

(E1) $O(\psi^l) = R$.

(E2) *There exist integers* l_1 and l_2 such that

(a) $0 < l_j < n$ *for* $j = 1, 2$,

(b) $l_1 + l_2 \equiv l \ (\text{mod } n)$, *and*

(c) $w(i, l_1) + w(i, l_2) < n/d(i)$ *for every* i.

(2) *Moreover the following two conditions are equivalent*:

(S1) $\zeta^{\sim}(\psi^l)$ *is an element in the socle of* S/MS.

(S2) *For any integer* l' *with* $0 < l' < n$, *there exists an integer* i *such that* $1 \leq i \leq r$ *and* $w(i, l) + w(i, l') \geq n/d(i)$.

(3) $g(\psi^l, \psi^{-l}) = a\prod_{w(i,l)\neq 0} f_i$ *for some* $a \in R^*$.

By using the above proposition, we can compute the embedding dimension and the Cohen-Macaulay type of S. In the rest of this section, we shall give some examples.

EXAMPLE. $z^5 = f_1^2 f_2^3$.

Since $d(1) = d(2) = 1$, $e(1)/d(1) = 2$, $e(2)/d(2) = 3$, and $n/d(1) = n/d(2) = 5$, we easily have the table of $w(i, l)$'s:

i \ l	0	1	2	3	4	$n/d(i)$
1 (f_1R)	0	2	4	1	3	5
2 (f_2R)	0	3	1	4	2	5

It then follows from Proposition 13 that $O(\psi^l) \neq R$ for all l with $0 < l < 5$, $\zeta^{\sim}(\psi^l)$ is an element in the socle of S/MS and $0(1) \subseteq M^2$. Therefore type $S = 4$ and emb. dim $S = h + 4$.

EXAMPLE. $z^{e(1)e(2)} = f_1^{e(1)} f_2^{e(2)}$ *with* $(e(1)), e(2)) = 1$.

Note first that $n/d(1) = e(2)$, $n/d(2) = e(1)$ and $e(i)/d(i) = 1$ for $i = 1, 2$. Hence $l \equiv w(1, l)(\text{mod } e(2))$ and $l \equiv w(2, l)(\text{mod } e(1))$ for every l. Choose now positive integers r and s so that $0 < r < e(2)$, $0 < s < e(1)$ and $re(1) + se(2) \equiv 1 \ (\text{mod } e(1)e(2))$. It is clear that, by definition, $w(1, re(1)) = w(2, se(2)) = 1$ and $w(2, re(1)) = w(1, se(2)) = 0$; and moreover $w(1, ire(1)) = i$ and $w(2, ire(1)) = 0$ for every integer i such that $0 < i < e(2)$; similarly, $w(2, ise(2)) = i$ and $w(1, ise(2)) = 0$ for every integer i such that $0 < i < e(1)$.

We shall show that, for an integer l *with* $0 < l < e(1)e(2)$, $O(\psi^l) = R$ *if and only if* $l \neq re(1)$, $se(2)$. Let l be an integer such that $0 < l < n$. Then there exist integers i and j such that $0 \leq i < e(2)$, $0 \leq j < e(1)$ and $ire(1) + jse(2) \equiv l \pmod{e(1)e(2)}$. If $ij \neq 0$, we can write $\psi^l = \psi^{ire(1)}\psi^{ise(2)}$; since $w(1, ire(1)) + w(1, jse(2)) = i < e(2)$ and $w(2, ire(1)) + w(2, jse(2)) = j < e(1)$, it follows from Theorem 7 that $g(\psi^{ire(1)}, \psi^{jse(2)})$ is invertible, and hence $O(\psi^l) = R$. If $i > 1$ and $j = 0$, we can write $\psi^l = \psi^{(i-1)re(1)}\psi^{re(1)}$; by using the same argument as above, we see that $g(\psi^{(i-1)re(1)}, \psi^{re(1)})$ is invertible, and hence $O(\psi^l) = R$. Similarly if $i = 0$ and $j > 0$, we have $O(\psi^l) = R$. Suppose that we can write $\psi^{re(1)} = \psi^a\psi^b$ so that $g(\psi^a, \psi^b)$ is invertible; by our assumption, $w(2, a) + w(2, b) < e(1)$. Since $w(2, re(1)) = 0$, we have $w(2, a) + w(2, b) \equiv w(2, re(1)) \equiv 0 \pmod{e(1)}$, and hence $w(2, a) = w(2, b) = 0$. Hence we can write $a \equiv a're(1) \pmod{n}$ and $b \equiv b're(1) \pmod{n}$ with $0 < a', b' < e(2)$; thus we have $1 \equiv a' + b' \pmod{e(2)}$ and, by our assumption, $a' + b' < e(2)$; this is a contradiction. Therefore $O(\psi^{re(1)}) \neq R$, and similarly $O(\psi^{jse(2)}) \neq R$. As for $O(1)$, it is easy to see that $O(1) = (f_1, f_2)R$.

We put $t = n - 1$; then $t \equiv (e(2) - 1)re(1) + (e(1) - 1)se(2) \pmod{n}$. Since $w(1, t) = e(2) - 1$ and $w(2, t) = e(1) - 1$, $\zeta^{\sim}(\psi^t)$ is an element in the socle of S/MS. Conversely assume that $\zeta^{\sim}(\psi^l)$, with $0 < l < n$, is an element in the socle of S/MS, and choose integers i and j so that $0 \leq i < e(2)$, $0 \leq i < e(1)$ and $ire(1) + jse(2) \equiv l \pmod{n}$. Since $w(1, l) = i$ and $w(2, l) = j$, our assumption on ψ^l implies that $w(1, l) + w(1, re(1)) \geq e(2)$ and $w(2, l) + w(2, se(2)) \geq e(1)$; hence $i = e(2) - 1$ and $j = e(1) - 1$. Therefore $l = t$.

Consequently, S is a Gorenstein local ring with $\text{emb.dim} S = h + \#\{i \mid o(f_i) \neq 1\}$.

References

[1] P. Griffith, Normal extensions of regular local rings, Journal of Algebra **105** (1987), 465–475.

[2] P. Roberts, Abelian extensions of regular local rings, Proc. Amer. Math. Soc. **78** (1980), 307–310.

[3] O. Zariski and P. Samuel, Commutative Algebra vol. 1, Graduate Texts in Math. No. **28**, Springer-Verlag, 1975.

[4] T. Takagi, Lectures on the Elementary Theory of Numbers (Japanese), Second edition, Kyoritu-sha Shoten, 1971.

Department of Mathematics,
Faculty of Science,
Hiroshima University *)

*) Present address: Department of Mathematics, Faculty of Integrated Arts and Sciences, Hiroshima University.