THE REDUCTION THEOREM OF THE RELATIVE COHOMOLOGY GROUP IN ALGEBRAS, AND ITS APPLICATION[1]

HISASI OGAWA[2]

(Received November 28, 1959)

Introduction. G. Hochshild defined in [4] the relative cohomology group of algebras as follows: let k be a commutative ring with unit element 1. We consider an algebra A over k and its subalgebra B, which has the unit element 1 and is unitary. For a bi-A-module M, a k-n-linear function f of A to M is called to be *a cochain relative to* B with coefficient M if f satisfies the conditions

$$(1)\qquad bf(a_1,\ldots\ldots, a_n)=f(ba_1,\ldots\ldots, a_n)$$

$$(2)\qquad f(a_1,\ldots\ldots,a_ib, a_{i+1},\ldots\ldots, a_n)=f(a_1,\ldots\ldots, a_i, ba_{i+1},\ldots\ldots, a_n)$$

$$(3)\qquad f(a_1,\ldots\ldots, a_nb)=f(a_1,\ldots\ldots, a_n)b, \qquad b\in B,\ a_i\in A.$$

For $n = 0$, we set

$$C^0(A, B, M) = \{m \in M|(b \in B), \quad bm = mb\}.$$

We define the *coboundary operator* $D: C^n(A, B, M) \to C^{n+1}(A, B, M)$, such that

$$(4)\qquad (Df)(a_1,\ldots\ldots, a_{n+1}) = a_1f(a_2,\ldots\ldots, a_{n+1}) + \sum_{i=1}^{n}(-1)^i f(a_1,\ldots\ldots, a_ia_{i+1}, \ldots\ldots, a_{n+1}) + (-1)^{n+1}f(a_1,\ldots\ldots, a_n)a_{n+1}.$$

Thus we obtain the relative cohomology group $H^n(A, B; M)$.

In this paper, we shall show in § 1 that the reduction theorem of cup-products holds just in the same way as in the case of finite groups which R. Lyndon gave in [7]. (c f. [3]. Systematic descriptions for the reduction theorem of cap- and cup-products were given in [8]). Next, using this we shall decide the relative cohomology groups of some modules considered in p-adic number fields in connection with differents in § 2. (c f. [5]) In §3 we shall decide the same groups as § 2 considered now in p-adic division algebras. Recently I have seen that H. Kuniyoshi has also decided the (co-)homology groups of the same modules, more generally considered in p-adic normal simple algebras (see his forthcoming paper).

1) This discussion was published in Japanese in Annual Report of the Gakugei Faculty of the IWATE UNIV., 14(1953), 1–13.
2) Formerly HISASI YAMASAKI.

1. A cochain f is called *normal with respect to B* or simply *normal* if $f(a_1,\dots\dots, a_n) = 0$ whenever any one of a_i belongs to B. All cochains considered may be assumed to be normal almost in the same way as seen in p.p. 61-63 of [3].

Let J be a free ring over B, and F be a residue class ring modulo the ideal R, which is generated by $a\alpha - \alpha a$, $a \in k$, $\alpha \in F$, therefore an element of F commutes with an element of k. We shall call F a free ring over B commutative with k. Moreover we assume that $(F/R) \approx A$ with $P: F \to A$.

A cochain f over F is called to be *right-invariant* if $f(a_1, a_2, a_3,\dots\dots) = f(a'_1, a'_2, a'_3,\dots\dots)$, whenever $a_2 \equiv a'_2$, $a_3 \equiv a'_3,\dots\dots$ mod. R, and is called to be *fully invariant* if $f(a_1, a_2,\dots\dots) = f(a'_1, a'_2,\dots\dots)$, whenever $a_1 \equiv a'_1$, $a_2 \equiv a'_2,\dots\dots$, mod. R.

LEMMA 1. *If f is an n-cocycle over F, $n > 1$, then $f = Du_f$, with $(n-1)$-cochain u_f. Accordingly $H^n(F, B) = 0$ for any bi-F-module. Moreover, if f is right-invariant, then we see that u_f is also right-invariant.*

PROOF. We shall show, at first, that the $(n-1)$-cochain u_f for f can be obtained by the conditions (5), (6):

$$u(b, a_2,\dots\dots, a_{n+1}) = 0,\ b \in B,\ a_i \in F. \tag{5}$$

By x we denote a free generator of F or an element of B, then it holds that

$$u(xa_1, a_2,\dots\dots) = xu(a_1, a_2,\dots\dots) - f(x, a_1, a_2,\dots\dots). \tag{6}$$

In fact, by the induction on the length of the first variable together with (5), (6) and the normality of f, we see easily that (1), (2), (3) and the normality hold for u. It follows from this that $u(x, a_2,\dots\dots) = 0$, if we set $a_1 = 1$ in (6). We have, therefore, that

$$\begin{aligned} Du(x, a_2,\dots\dots) &= xu(a_2,\dots\dots) - u(xa_2,\dots\dots) \\ &= f(x, a_2,\dots\dots). \end{aligned}$$

Consequently, also the induction on the length of the first variable yields that $f = Du$. Indeed if we assume inductively that

$$Du(a_1, a_2,\dots\dots) = f(a_1, a_2,\dots\dots)$$

then, since f is a cocycle we have that

$$D(Du - f)(x, a_1, a_2,\dots\dots) = 0.$$

By the inductive assumption the left hand side reduces to

$$x(Du - f)(a_1, a_2,\dots\dots) - (Du - f)(xa_1, a_2,\dots\dots) + (Du - f)(x,\dots\dots)$$

$$= -(Du - f)(xa_1, a_2, \ldots\ldots).$$

Thus, we obtain

$$Du(xa_1, a_2, \ldots\ldots) = f(xa_1, a_2, \ldots\ldots),$$

i. e. $Du = f$.

If f is right-invariant, we see easily by induction that u is also right-invariant. From these facts, in view of the linearity of u, our assertion follows immediately. q. e. d.

We shall consider an A-module M as an F-module induced by $P:(F/R) \approx A$. For a right-invariant $(n-1)$-cochain u, r in R, it follows, from the facts that $ra_2 \in R$ and the right-invariantness of u, that

(7) $$Du(a_1, r, a_2, \ldots\ldots) = a_1 u(r, a_2, \ldots\ldots) - u(a_1 r, a_2, \ldots\ldots) + u(a_1, r a_2, \ldots\ldots)$$
$$= a_1 u(r, a_2, \ldots\ldots) - u(a_1 r, a_2, \ldots\ldots).$$

If Du is also right-invariant, we have

(8) $$a_1 u(r, a_2, \ldots\ldots) = u(a_1 r, a_2, \ldots\ldots).$$

The function u' with $(n-2)$ variables on F given by

(9) $$[u'(a_2, \ldots\ldots)]\,(r) = u(r, a_2, \ldots\ldots)$$

takes, therefore, its values in Hom(R, M), which is the group of all F-left-homomorphisms of R into M.

Hom(R, M) is a right-A-module with A-operators such that

(10) $$[h \circ a]\,(r) = h(r)a \qquad h \in \mathrm{Hom}(R, M),\ \alpha \in F,\ a \in A,\ r, r' \in R.$$

Whenever $P(\alpha) = a$, we put

(11) $$[\alpha \circ h]\,(r) = h(r\alpha),$$

then it holds that $[r' \circ h](r) = h(rr') = r\,h(r')$, because h is an F-left-homomorphism. Thus Hom(R, M) is a left-A-module with A-operators (11), because $r\,h(r') = P(r)h(r') = 0 \cdot h(r') = 0$.

Now if b in B, it holds that

$$[u'(b\,a_2, \ldots\ldots)](r) = u(r, b\,a_2, \ldots\ldots) = u(r\,b, a_2, \ldots\ldots) = [u'(a_2, \ldots\ldots)](rb)$$
$$= [b \circ u'(a_2, \ldots\ldots)]\,(r),$$

and this yields (1) of u'. (2) and the normality of u' follows from those of u.

(3) is derived from the fact that

$$[u'(\cdots, a_n b)](r) = u(r, \ldots\ldots, a_n b) = u(r, \ldots\ldots, a_n)\ b = [u'(\ldots\ldots, a_n) \circ b]\,(r).$$

And then since u is right-invariant, u' is also fully invariant, therefore, we may regard u' as a cochain over A, that is,

$$u' \in C^{n-2}(A, B; \mathrm{Hom}(R, M)).$$

Now that Du is right-invariant and $DDu = 0$, we may apply this for $Du = f$. Thus we conclude that $f' \in C^{n-1}(A, B, \mathrm{Hom}(R, M))$.

We have then, since $ra_2 \in R$,

$$[f'(a_2, \ldots\ldots, a_n)](r) = f(r, a_2, \ldots\ldots, a_n) = Du(r, a_2, \ldots\ldots, a_n)$$

$$= r\,u(a_2, \ldots\ldots) - u(r\,a_2, \ldots\ldots) + \sum_{t=2}^{n-1} (-1)^t u(r, \ldots\ldots) + (-1)^n u(r, \ldots\ldots, a_{n-1})a_n$$

$$= P(r)u(a_2, \ldots\ldots) - [u'(a_3, \ldots\ldots)](r\,a_2) + \sum_{i=2}^{n-1} (-1)^t [u'(a_2, \ldots\ldots)](r)$$

$$+ (-1)^n [u'(a_2, \ldots\ldots)](r)a_n = 0 - [a_2 \circ u'(a_3, \ldots\ldots)](r) + \sum_{i=2}^{n-1} (-1)^t [u'(a_2, \ldots\ldots)](r)$$

$$+ (-1)^n [u'(a_2, \ldots\ldots) \circ a_n](r) = -[Du'(a_2, \ldots\ldots, a_n)](r).$$

Consequently, we have

LEMMA 2. *If u is a right-invariant $(n-1)$-cochain over F, and if $f = Du$ is also right-invariant, then*

$$f' = -Du'. \tag{12}$$

If u is a right-invariant and f is fully invariant, then $Du' = f' = 0$, whence u' in $Z^{n-2}(A, B, \mathrm{Hom}(R, M))$.

PROOF. We may show only the latter, but it is clear from

$$[f'(a_2, \ldots\ldots)](r) = f(r, a_2, \ldots\ldots).$$

COROLLARY 2. 1. *If f is a righ-invariant n-cocycle over F, where $n > 1$, then*

$f' = -Du'_f$, a coboundary; if f is fully invariant, then $Du' = -f' = 0$, and u' is in $Z^{n-2}(A, B, \mathrm{Hom}(R, M))$.

PROOF. From LEMMA 1, a right-invariant f is Du_f with a right-invariant u_f, and then, we can apply LEMMA 2. q. e. d.

For a cochain f over A, we shall now define a fully invariant cochain f_P such that

$$f_P(a_1, a_2, \ldots\ldots) = f(Pa_1, Pa_2, \ldots\ldots),$$

where P is the homomorphism $F \to A \approx (F/R)$. The correspondence

$f \to f_P$ is univalent, and that, preserves (1)$\sim$(4), therefore, henceforth we shall not distinguish f and f_P.

Thus every $(n+2)$-cocycle f over A may be regarded as a fully invariant cocycle over F, and as such determines, in accordance with corollary 2.1, a cocycle u_f' in $Z^n[A, B, \mathrm{Hom}(R, M)]$, therefore the map $Wf = u'_f$, for all f in $Z^{n+2}(A, B; M)$ establishes an A-homomorphism

$$W: Z^{n+2}(\mathrm{A}, B, M) \to Z^n[A, B, \mathrm{Hom}(R, M)]. \tag{13}$$

LEMMA 3. *We assume that A has a linearly independent basis over B containing* 1. *For every cochain w in $C^n[A, B, \mathrm{Hom}(R, M)]$ there exists an $(n+1)$-cochain u over F such that u and $f = Du$ are right-invariant, and that $u' = w$.*

PROOF. We shall take b in B as a representative of the class modulo R containing b, then 0 represents 0-class. Further we shall assume that the representative of the class containing $P(a')$ is also a', then it holds that

$$P(ba') = P(b)\,P(a') = bP(a')$$
$$P(a'b) = P(a')P(b) = P(a')b.$$

Thus A has a linearly independent basis over B containing 1, and we may therefore preassign ba', $a'b$ as the representative of the class containing $bP(a')$, $P(a')b$ respectively.

Let u be a function with $(n+1)$-variables on F such that for r in R

$$u(a' + r, a_2, \dots\dots) = [w(P(a_2), \dots\dots)](r), \tag{14}$$

then u is right-invariant, for w is fully invariant. Set $a' = 0$ in (14), then

$$u(r, a_2, \dots\dots) = [u'(a_2, \dots\dots)]\ (r) = [w(P(a_2), \dots\dots)](r),$$

and this means that $u' = w$.

This u is an element of $C^{n+1}(F, B; M)$. Indeed, since $u(b, a_2, \dots\dots) = [w(\dots\dots)](0) = 0$, u is normal with respect to the first variable, and the normalities relative to the remaining variables follow from those of w. Next we shall show (1), (2), (3) for u. Since ba' is the preassigned representative and br is in R, it holds that

$$\begin{aligned} u[b(a' + r), \dots\dots] &= u(ba' + br, \dots\dots) = [w(\dots\dots)]\,(br) \\ &= b[w(\dots\dots)](r) \text{ (because } w \text{ is an } F\text{-left-homomorphism.)} \\ &= bu(a' + r, \dots\dots), \end{aligned}$$

thus (1) holds for u. (3) follows from

$$\begin{aligned} u(\dots\dots, a_nb) &= w[\dots\dots, P(a_nb)]\,(r) = w[\dots\dots, P(a_n)b]\,(r) \\ &= [w[\dots\dots, P(a_n)]\circ b]\,(r) = w[\dots\dots, P(a_n)]\,(r)b = u(\dots\dots, a_n)b. \end{aligned}$$

It holds further that

$$u[a' + r, ba_2, \ldots\ldots] = w[P(ba_2), \ldots\ldots]\ (r) = w[bP(a_2), \ldots\ldots](r)$$
$$= [b \circ w[P(a_2), \ldots\ldots]]\ (r) = w[P(a_2), \ldots\ldots](rb) = u(rb, a_2 \ldots\ldots)$$
$$= u(a'b + rb, a_2, \ldots\ldots) = u[(a' + r)b, a_2, \ldots\ldots)],$$

because $a'b$ is the preassigned representative, this is (2) for the first variable. Finally the fact that

$$u[a' + r, a_2, \ldots\ldots, a_i b, a_{i+1}, \cdots] = u[a' + r,\ a_2, \ldots\ldots, a_i, ba_{i+1}, \ldots\ldots]$$

is the direct consequence of (2). Thus u is really in $C^{n+1}(F, B, M)$.

As was seen above, u is right-invariant and $u' = w$. Then it holds that

$$au(r, a_2, \ldots\ldots) = aw[P(a_2), \ldots\ldots]\ (r) = w[P(a_2), \ldots\ldots](ar)$$
$$= u(ar, a_2, \ldots\ldots) \quad \text{(because } ar \text{ is in } R\text{)},$$

therefore, we obtain that for $f = Du$,

$$f(a_1, r, a_2, \ldots\ldots) = 0. \tag{15}$$

Thus f is invariant with respect to the second variable, and the invariantness for $a_2, \ldots\ldots$ follows from those of u, therefore, we see that f is right-invariant by means of its linearity. q. e. d.

Now the proof of the reduction theorem will be carried out just in the same way as in [8]. That is,

LEMMA 4. *Every cocycle* w *in* $Z^n(A, B, \mathrm{Hom}(R, M))$ *for* $n > 0$ *is cohomologous to* Wf *for some cocycle* f *in* $Z^{n+2}(A, B; M)$, *that is,* W *induces an epimorphism* W *of* $H^{n+2}(A, B; M)$ *onto* $H^n(A, B; \mathrm{Hom}(R, M))$.

LEMMA 5. *If* f *is an* $(n+2)$*-coboundary in* $B^{n+2}(A, B, M)$, *and* $n > 0$, *then* Wf *is a coboundary in* $B^n(A, B, \mathrm{Hom}(R, M))$.

LEMMA 6. *If* f *is in* $Z^{n+2}(A, B, M)$, *and* Wf *is in* $B^n(A, B, \mathrm{Hom}(R, M))$, *then* f *is in* $B^{n+2}(A, B, M)$, *thus,* W *is an isomorphism.*

(For the proofs of these lemmas, see [8].)

This completes the proof of the CUP PRODUCT REDUCTION THEOREM.[3)]

Let k *be a commutative ring containing the unit element* 1, B *be a* k*-algebra containing* 1, *and* A *be a* k*-algebra containing* B *and having a linearly independent basis over* B. *Suppose that* F *be a free ring over* B *commutative with* k*-element, and* P *be the canonical homomorphism* F *onto*

3) A generalisation and the dual for cap product have been obtained in [8].

(F/R), *which is isomorphic onto* A. *Then the map* W *in* (13) *induces an isomorphism*

$$H^{n+2}(A, B, M) \approx H^{n}(A, B, \mathrm{Hom}(R, M)), \qquad \textit{for } n>0,$$

where a bi-A*-module* M *is considered as an* F*-module induced by* P, $\mathrm{Hom}(R, M)$ *is the group of all* F*-left-homomorphisms, and* A *operates on* $\mathrm{Hom}(R, M)$ *as follows: for* $h \in \mathrm{Hom}(R, M)$, $r \in R$, $a \in A$, $P(\alpha) = a$ *we define* $[h \circ a](r) = h(r)a$ *and* $[a \circ h](r) = h(r\alpha)$.

2. Let k be a p-adic number field, K be its extension of a finite degree, L be the maximal unramified field between k and K, and D be the different of (K/k); B, A, B_L be the principal order of k, K, L respectively, P be the prime ideal of A, and M be the group (A/P^r), $r = 1, 2, \ldots\ldots$ Then Y.Kawada showed the following theorem and characterized the different.

THEOREM 1. (Y.Kawada)[4] *For* $i = 1, 2$,

$$H^i(A, B, M) \approx H^i(A, B_L, M) \tag{16}$$

and

$$H^i(A, B, M) \begin{cases} \approx (A/P^r) & \textit{if } P^r \supset D, \\ \approx (A/D) & \textit{if } P^r \subset D. \end{cases} \tag{17}$$

We shall show further

COROLLARY. (16) *and* (17) *remain valid for every positive integer* $i = 1, 2, 3, \ldots\ldots$

PROOF. In the application of the reduction theorem, we may take the polynomial ring $B[x]$ of one variable x over B as a free ring F over B (the basic ring k there is now the rational integer ring $\mathbf{Z}$.), since all rings considered are commutative. Then A has a minimal basis over B consisting of one element θ, because the residue class ring (A/P) is a separable extension of that of B(Theorem 11 of IV, 6 in [1]). Then the ideal R in the reduction theorem is the principal ideal generated by the monic irreducible polynomial $f(x)$ over B, of which root is θ. Since $A, (A/P^r)$ is commutative, it holds that for α, β in F, g in $\mathrm{Hom}(R, (A/P^r))$,

$$g(\alpha f(x)\beta) \equiv \alpha\beta g(f(x)) \qquad (\mathrm{mod.}\ P^r),$$

therefore, g is decided uniquely if $g(f(x))\,(\mathrm{mod.}\ P^r)$ is given. From this we

4) In [5], this was proved for the commutative cohomology groups, i.e., $f(a, b) = f(b, a)$ ……But even if we except this commutativity and so take our relative group, this theorem remains valid with the proof slightly modified. Therefore we shall omit the proof.

see that

$$\mathrm{Hom}(R, (A/P^r)) \approx (A/P^r).$$

Therefore our reduction theorem reduces to

$$H^{n+2}(A, B, M) \approx H^n(A, B, M), \ n>0.$$

Together with (17) in THEOREM 1, we obtain (17) in our corollary.

Similarly we obtain (17) in the case of (A/B_L). Now that L is the maximal unramified extension between k and K, the relative different of (K/L) is nothing but that of (K/k).

Combining both (17), we have (16) in our corollary. q. e. d.

3. Let k be also a p-adic number field, $\mathfrak{o}$ be its principal order, $\mathfrak{S}$ be a central division algebra over k, $\mathfrak{A}$ be its principal order, $\mathfrak{P}$ be the extension in $\mathfrak{A}$ of the prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, π be a prime elment of $\mathfrak{P}$. If $[\mathfrak{S}:k] = n^2$, there exists an unramified extension of k such that $\mathfrak{S} \supset L \supset k$, $[L:k] = n$. And if $\mathfrak{o}/\mathfrak{p} \approx GF(q)$,

$$L = k(\omega), \qquad \omega^{q^n-1} = 1.$$

Let B be the principal order of L, and $\mathfrak{P}_L$ be the extension in B of $\mathfrak{p}$. As a generator of the Galois group of (L/k), which is the cyclic group of the order n, we may take σ with $\omega^\sigma = \omega^q$. Then $\mathfrak{S}$ is represented as a cyclic crossed product such that

$$\mathfrak{S} = L + L\pi + \dots\dots + L\pi^{n-1},$$

$\pi\alpha = \alpha^T\pi$, α in L, where T is σ^i with $(i, n) = 1$, and π^n is a prime element of $\mathfrak{p}$, which we shall again denote by p, and may be considered as in $\mathfrak{o}$.

Regarding $\mathfrak{o}$, $\mathfrak{A}$, B as algebras over $\mathbf{z}$; Y.Kawada showed in [6]

THEOREM 2. (Kawada) *For $r \geqq 1$, we have*

$$H^1(\mathfrak{A}, \mathfrak{o}, (\mathfrak{A}/\mathfrak{P}^r)) \approx H^1(\mathfrak{A}, B, (\mathfrak{A}/\mathfrak{P}^r)).$$

$$H^1(\mathfrak{A}, B, (\mathfrak{A}/\mathfrak{P}^r)) \begin{cases} \approx 0, & \textit{if } r \equiv 1 \pmod{n}, \\ \approx \textit{the additive group of } GF(q) & \textit{if } r \not\equiv 1 \pmod{n}. \end{cases}$$

For the 2-dimensional case we shall show

THEOREM 3. *If $r \geqq 1$, then*

(18) $$H^2(\mathfrak{A}, \mathfrak{o}, (\mathfrak{A}/\mathfrak{P}^r)) \approx H^2(\mathfrak{A}, B, (\mathfrak{A}/\mathfrak{P}^r)).$$

$$H^2(\mathfrak{A}, B, \mathfrak{A}/\mathfrak{P}^r) \begin{cases} \approx \textit{the additive group of } GF(q^n), & \textit{if } r \equiv 1 \pmod{n} \\ \approx \textit{the additive group of } GF(q), & \textit{if } r \not\equiv 1 \pmod{n}. \end{cases}$$

PROOF. For $f \in Z^2(\mathfrak{A}, \mathfrak{o}, (\mathfrak{A}/\mathfrak{P}^r))$, $\alpha \in \mathfrak{A}$, it holds that

$$\omega^j f(\omega^i, \alpha) - f(\omega^{j+i}, \alpha) + f(\omega^j, \omega^i\alpha) - f(\omega^j, \omega^i)\,\alpha \equiv 0 \pmod{\mathfrak{P}^r},$$

we have therefore

$$f(\omega^i, \alpha) \equiv \omega^{R-j} f(\omega^{j+i}, \alpha) - \omega^{R-j} f(\omega^j, \omega^i\alpha) + \omega^{R-j} f(\omega^j, \omega^i)\alpha, \tag{19}$$

where $q^n - 1 = R$. By adding up (19) from $j = 0$ to $j = R - 1$, we have

$$Rf(\omega^i, \alpha) \equiv \sum_{j=0}^{R-1} \omega^{R-j} f(\omega^{j+i}, \alpha) - Rg(\omega^i\alpha) + Rg(\omega^i)\alpha,$$

where

$$\sum_{j=0}^{R-1} \omega^{R-j} f(\omega^j, \alpha) = Rg(\alpha).$$

The first term on the right reduces to $R\omega^i g(\alpha)$ by taking the sum with respect to $j + i = k$. On account of $R \not\equiv 0 \pmod{\mathfrak{P}^r}$, we obtain that $f(\omega^j, \alpha) \equiv Dg(\omega^j, \alpha)$, therefore, we may consider from the beginning that $f(\omega^j, \alpha) \equiv 0$. Consequently (1) for f follows from the D-relation

$$\omega^i f(\alpha, \beta) - f(\omega^i\alpha, \beta) + f(\omega^i, \alpha\beta) - f(\omega^i, \alpha)\,\beta \equiv 0.$$

Similarly by setting $\left(\sum_{j=0}^{R-1} f(\alpha, \omega^j)\omega^{R-j}\right)/R = g(\alpha)$, we may consider that $f(\alpha, \omega^j) \equiv 0$, and (3) follows also from the D-relation.

Thus (18) is proved.

Now we shall take a system of representatives λ_i in L of $(B/\mathfrak{P}_L)$, then every element of $\mathfrak{A}$ has the unique representation $\sum \lambda_i \pi^i$. For a cocycle f in $Z^2(\mathfrak{A}, B, (\mathfrak{P}/\mathfrak{A}^r))$, the B-linearity (1), (3) yields that

$$f\left(\sum \lambda_i \pi^i, \sum \lambda'_j \pi^j\right) \equiv \sum \lambda_i \lambda'^{T^i}_j f(\pi^i, \pi^j) \tag{20}$$

Accordingly, to decide f, we have only to assign

$$f(\pi^i, \pi^j) \qquad 0 \leqq i,\ j \leqq n - 1.$$

Now in the formula

$$\pi^i f(\pi^j, \pi^k) - f(\pi^{i+j}, \pi^k) + f(\pi^i, \pi^{j+k}) - f(\pi^i, \pi^j)\pi^k \equiv 0 \tag{21}$$

we have if $i \neq 0$, $k \neq 0$,

$$f(\pi^{i+j}, \pi^k) \equiv f(\pi^i, \pi^{j+k}) \pmod{\mathfrak{P}}.$$

We can therefore set

$$f(\pi^i, \pi^j) \equiv \mu_{i+j} \qquad \pmod{\mathfrak{P}} \tag{22}$$

independently of the division $i+j$ into the sum of i and j.

If we define a B-linear g such that, $g(\pi^i)=\mu_i$. $0\leqq i\leqq n-1$, then g is decided over $\mathfrak{A}$, because $\pi^n-p=0$. In the formula

$$(f-Dg)\,(\pi^i,\pi^j)\equiv f(\pi^i,\pi^j)-\pi^i g(\pi^j)+g(\pi^{i+j})-g(\pi^i)\pi^j \qquad (\text{mod. } \mathfrak{P}),$$

if $i\neq 0$, $j\neq 0$, then we have writing $(f-Dg)$ simply f

(23) $$f(\pi^i,\pi^j)\equiv\mu_{i+j}\equiv 0 \qquad (\text{mod. } \mathfrak{P}).$$

In the similar way as from (22) to (23), we have inductively that $\mu_{i+j}\equiv 0$ (mod. $\mathfrak{P}^r$), $(i\neq 0,\ j\neq 0)$. We have further that $f(1,\pi^i)\equiv f(\pi^i,1)\equiv 0$(mod. $\mathfrak{P}^r$), therefore, it holds that

(24) $$\mu_0\equiv\mu_1\equiv\ldots\ldots\equiv\mu_{n-1}\equiv 0 \quad (\text{mod. } \mathfrak{P}^r).$$

Let Z' be the group of all cocycles as (24), then we may consider that

$$H^2=(Z/B)\approx Z'/(Z'\cap B)$$

For Dg' in $(Z'\cap B)=B'$, $0\leqq i+j\leqq n-1$, it holds that, from (24),

$$Dg(\pi^i,\pi^j)\equiv\pi^i g(\pi^j)-g(\pi^{i+j})+g(\pi^i)\pi^j\equiv 0,$$

we see therefore that

(25) Dg in B' operates as a differentiation on π^i with $0\leqq i\leqq n-1$.

When $0\leqq i+j\leqq n-1$, $0\leqq j+k\leqq n-1$, since it follows from (21), (24) that $f(\pi^{i+j},\pi^k)\equiv f(\pi^i,\pi^{j+k})$, we may set independently of the division of i and j into the sum $i+j$

(26) $$f(\pi^i,\pi^j)\equiv\mu_{i+j},\ 0\leqq i,\ j\leqq n-1.$$

If we set $j=n-1-i$, $k=n-j$ in (21), then i,j,k are smaller than n, therefore it holds that

$$\pi^i\mu_n-\mu_{n+i}+f(\pi^i,\pi^n)+f(\pi^i,\pi^j)\pi^k\equiv 0.$$

The third term on the left vanishes, because $\pi^n=p$ and f is B-normal, and the fourth term also vanishes by (24). We have thus $\pi^i\mu_n\equiv\mu_{n+i}$, and similarly $\mu_{n+k}\equiv\mu_n\pi^k$ by setting $i=n-j$, $i=n-1-k$ in (21). Consequently we obtain

(27) $$\pi^i\mu_n\equiv\mu_{n+i}\equiv\mu_n\pi^i.$$

Conversely we shall show that whenever μ_n is given so as to satisfy (20), (24), (26), (27), then f becomes a cocycle relative to B, and that, its μ_n is nothing but the given μ_n.

(a) If $i+j<n$, $j+k<n$, the first and fourth terms on the left of (21) vanish from (24) and the second and third vanish from (26).

(b) If $i+j \geqq n$, $j+k<n$, or $i+j<n$, $j+k \geqq n$, we shall show only the former. The latter is proved similarly. Now we set $i+j=n+a$, then $a<n$. The first of (21) vanishes from (24). The second is

$$-f(\pi^{i+j}, \pi^{k}) \equiv -f(\pi^{n}\pi^{a}, \pi^{k}) \equiv -pf(\pi^{a}, \pi^{k}) \equiv -p\mu_{a+k},$$

then $a+k<n$ since $j+k<n$, therefore, this vanishes also from (24). Finally the third and the fourth cancels each other:

$$f(\pi^{i}, \pi^{j+k}) - f(\pi^{i}, \pi^{j})\pi^{k} \equiv \mu_{i+j+k} - \mu_{i+j}\pi^{k} \equiv \mu_{n}\pi^{a+k} - \mu_{n}\pi^{a}\pi^{k} \equiv 0.$$

(c) If $i+j \geqq n$, $j+k \geqq n$, put $i+j=n+a$, $j+k=n+b$, then $a+k=i+b$ and

$$\begin{aligned}
&\pi^{i}f(\pi^{j}, \pi^{k}) - f(\pi^{i+j}, \pi^{k}) + f(\pi^{i}, \pi^{j+k}) - f(\pi^{i}, \pi^{j})\pi^{k} \\
&\equiv \pi^{i}\mu_{j+k} - f(p\pi^{a}, \pi^{k}) + f(\pi^{i}, \pi^{b}p) - \mu_{i+j}\pi^{k} \\
&\equiv \pi^{i}\pi^{b}\mu_{n} - pf(\pi^{a}, \pi^{k}) + f(\pi^{i}, \pi^{b})p - \mu_{n}\pi^{a}\pi^{k} \\
&\equiv (\pi^{i+b} - \pi^{a+k})\mu_{n} - p(\mu_{a+k} - \mu_{i+b}) \\
&\equiv 0 \qquad \text{(from (27))}.
\end{aligned}$$

Thus f is well determined whenever μ_n is given as (27). We shall examine this condition: $\pi\mu_n \equiv \mu_n\pi$ in detail. Suppose that

(28) $$\mu_n \equiv \lambda_0 + \lambda_1\pi + \dots\dots + \lambda_{r-1}\pi^{r-1} \pmod{\mathfrak{P}^r},$$

λ_i are representatives of $(B/\mathfrak{P}_L)$, then from the condition we have

$$\begin{aligned}
0 \equiv \pi\mu_n - \mu_n\pi \equiv (\lambda_0^{T} - \lambda_0) + (\lambda_1^{T} - \lambda_1)\pi + \dots\dots \\
+ (\lambda_{r-2}^{T} - \lambda_{r-2})\pi^{r-1} + (\lambda_{r-1}^{T} - \lambda_{r-1})\pi^{r} \pmod{\mathfrak{P}^r}.
\end{aligned}$$

Since an element of B $\lambda = \sum_{i=0}^{n-1} a_i\omega^i$, a_i in $\mathfrak{o}$, having the property $\lambda^T - \lambda \equiv \sum a_i((\omega^{iT} - (\omega^i)) \equiv 0 \pmod{\mathfrak{P}_L}$ is with $a_i \equiv 0 \pmod{\mathfrak{P}_L}$ $i=1,\dots\dots,(n-1)$ i. e., λ is an element of $\mathfrak{o}$. Therefore,

(29) *In* (28) λ_{r-1} *is a representative of* $B/\mathfrak{P}_L$, $\lambda_0, \lambda_1, \dots\dots, \lambda_{r-2}$ *are representatives of* $\mathfrak{o}/p$.

Since f is further normal relative to B, it holds that

$$\begin{aligned}
\mu_n\omega &\equiv f(\pi^{n-1}, \pi)\ \omega = f(\pi^{n-1}, \pi\omega) \equiv f(\pi^{n-1}, \omega^{T}\pi) \\
&\equiv f(\pi^{n-1}\omega^{T}, \pi) \equiv f(\omega^{Tn}\pi^{n-1}, \pi) \equiv f(\omega\pi^{n-1}, \pi) \\
&= \omega f(\pi^{n-1}, \pi) \equiv \omega\mu_n,
\end{aligned}$$

and

$$\begin{aligned}
\omega\mu_n - \mu_n\omega \equiv \lambda_0(\omega - \omega) + \lambda_1(\omega^{T} - \omega)\pi + \dots\dots \\
+ \lambda_{r-1}(\omega^{T(r-1)} - \omega)\pi^{r-1} \equiv 0 \pmod{\mathfrak{P}^r}.
\end{aligned}$$

Accordingly, let 0 be also the representative of the 0-class of $(B/\mathfrak{P}_L)$, then we see that

$$(30)\qquad \begin{cases} \text{if } i \equiv 0(\text{mod. } n), \text{ then every } \lambda_i \text{ is an arbitrary representative of } (B/\mathfrak{P}_L), \\ \text{if } i \not\equiv 0(\text{mod. } n), \text{ then } \lambda_i = 0. \end{cases}$$

From (29) and (30) we obtain the condition of f to be a cocycle by means of μ_n:

(31)

(a) *if* $r = 1$, *then we may take an arbitrary representative of* $(B/\mathfrak{P}_L)$ *as* λ_0 *in* $\mu_n \equiv \lambda_0$ (mod. $\mathfrak{P}$).

(b) *if* $r \equiv 1$ (mod. n) *say* $r = tn + 1$, *then*

$$\mu_n \equiv \underset{(\mathfrak{o}/\mathfrak{p})}{\lambda_0} + \underset{(\mathfrak{o}/\mathfrak{p})}{\lambda_n}\pi^n + \ldots\ldots + \underset{(\mathfrak{o}/\mathfrak{p})}{\lambda_{(t-1)n}}\pi^{(t-1)n} + \underset{(B/\mathfrak{P}_L)}{\lambda_{tn}}\pi^{tn} \quad (\text{mod. } \mathfrak{P}^{tn+1})$$

(c) *if* $r \not\equiv 1$ (mod. n), *say* $r = tn + s$, $s \neq 1$, $0 \leqq s < n$, *then*

$$\mu_n \equiv \underset{(\mathfrak{o}/\mathfrak{p})}{\lambda_0} + \underset{(\mathfrak{o}/\mathfrak{p})}{\lambda_n}\pi_n + \ldots\ldots + \underset{(\mathfrak{o}/\mathfrak{p})}{\lambda_{(t-1)n}}\pi^{(t-1)n} + \underset{(\mathfrak{o}/\mathfrak{p})}{\lambda_{tn}}\pi^{tn} \quad (\text{mod. } \mathfrak{P}^{tn+s}).$$

Next we shall consider the condition of μ_n to be a coboundary Dg. Since g is B-normal, we have

$$\omega^T g(\pi) \equiv g(\omega^T \pi) \equiv g(\pi\omega) \equiv g(\pi)\omega.$$

Thus, for

$$g(\pi) \equiv \lambda_0 + \lambda_1\pi + \ldots\ldots + \lambda_{r-1}\pi^{r-1} \ (\text{mod. } \mathfrak{P}^r),$$

it holds that

$$\omega^T g(\pi) - g(\pi)\omega$$
$$\equiv \lambda_0(\omega^T - \omega) + \lambda_1(\omega^T - \omega^T)\pi + \lambda_2(\omega^T - \omega^{T^2}) + \ldots\ldots + \lambda_{r-1}(\omega^T - \omega^{T^{(r-1)}})\pi^{r-1}$$
$$(\text{mod. } \mathfrak{P}^r).$$

From this we may take arbitrary λ_i if $i \equiv 1$ (mod. n), and $\lambda_i = 0$ if $i \not\equiv 1$(mod. n).

Consequently, $g(\pi)$ reduces to the form:

$$(32)\qquad g(\pi) \equiv \lambda_1\pi + \lambda_2\pi^{n+1} + \ldots\ldots + \lambda_{(t-1)}\pi^{(t-1)n+1} + \lambda_{tn}\pi^{tn+1} \ (\text{mod. } \mathfrak{P}^r).$$

By means of (25), we shall compute μ_n of Dg in B', taking the fact $g(\pi^n) \equiv g(p) \equiv 0$ in account:

$$Dg(\pi, \pi^{n-1}) \equiv \pi g(\pi^{n-1}) - g(\pi^n) + g(\pi)\pi^{n-1}$$
$$\equiv \pi^{n-1} g(\pi) + \pi^{n-2} g(\pi)\pi + \pi^{n-3} g(\pi)\pi^2 + \ldots\ldots + g(\pi)\pi^{n-1}$$
$$\equiv \lambda_1^{T^{(n-1)}}\pi^n + \lambda_2^{T^{(n-1)}}\pi^{2n} + \ldots\ldots + \lambda_{(t-1)}^{T^{(n-1)}}\pi^{tn}$$

$$+ \lambda_1^{T^{(n-2)}} \pi^n + \lambda_2^{T^{(n-2)}} \pi^{2n} + \ldots\ldots + \lambda_{(t-1)}^{T^{(n-2)}} \pi^{tn}$$
$$+ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$+ \lambda_1 \pi^n + \lambda_2 \pi^{2n} + \ldots\ldots + \lambda_{(t-1)} \pi^{tn} \pmod{\mathfrak{P}^r}$$
$$\equiv (Sp_{(L/k)} \lambda_1) \pi^n + (Sp_{(L/k)} \lambda_2) \pi^{2n} + \ldots\ldots + (Sp_{(L/k)} \lambda_{(t-1)}) \pi^{tn} \pmod{\mathfrak{P}^r}.$$

Evidently,

$$\pi (Sp_{(L/k)} \lambda) \pi^{in} \equiv (Sp_{(L/k)} \lambda) \pi^{in} \pi,$$

and then (27) holds also for μ_n of Dg. (L/k) is unramified and $(B/\mathfrak{P}_L)$ is a finite field, therefore, $(\mathfrak{o}/\mathfrak{p})$ is filled up with $(Sp_{(L/k)} \lambda) \pmod{\mathfrak{P}_L}$, [2]. Consequently we see for Dg,

$$\mu_n \equiv 0 + \underset{(\mathfrak{o}/\mathfrak{p})}{\lambda_n} \pi^n + \underset{(\mathfrak{o}/\mathfrak{p})}{\lambda_{2n}} \pi^{2n} + \ldots\ldots + \underset{(\mathfrak{o}/\mathfrak{p})}{\lambda_{tn}} \pi^{tn} \pmod{\mathfrak{P}^r} \tag{33}$$

Whenever μ_n is given, f is uniquely decided by (20), (24), (26), (27) and its linearity. Therefore, in comparision with (31), (33), we have our assertion. That is, H^2 is isomorphic with $(B/\mathfrak{P}_L)$ as a module if $r = 1$, and if $r \not\equiv 1 \pmod{n}$ only the first $(\mathfrak{o}/\mathfrak{p})$ remains. At last, if $r \equiv 1 \pmod{n}$, the first term $(\mathfrak{o}/\mathfrak{p})$ and the last term $(B/\mathfrak{P}_L)/(\mathfrak{o}/\mathfrak{p})$ remain. Therefore, combining these, H^2 is isomorphic with $(B/\mathfrak{P}_L)$ as a module. q. e. d.

THEOREM 4. *If $n \geqq 1$, there exist the following isomorphisms:*

$$H^{2n-1}(\mathfrak{A}, B, (\mathfrak{A}/\mathfrak{P}^r)) \approx H^1$$
$$H^{2n}(\mathfrak{A}, B, (\mathfrak{A}/\mathfrak{P}^r)) \approx H^2.$$

PROOF. We shall give the proof by applying the reduction theorem. Now, $\mathfrak{A}$ is generated by the single element π over B and the basic ring is the ring of all rational integers, and then F is a usual free ring of one variable over B. The kernel R of the natural homomorphism from F onto $\mathfrak{A}$, which maps X to π, is an ideal generated by

$$A = X^n - p, \; A' = X\omega - \omega^{q^i} X,$$

where $(i, n) = 1$.

For the simplicity from now on we shall denote $f(a_1, a_2, a_3, \ldots\ldots, a_{n+2})$ of H^{n+2}, $u(\ ,a_3, \ldots\ldots, a_{n+2})$ constructed by f, in (5), (6), and the corresponding u' of H^n defined by (9); $u(r, a_3, \ldots\ldots, a_{n+2}) = [u'(a_3, \ldots\ldots, a_{n+2})]\,(r)$ $r \in R$, by $f(a_1, a_2)$, $u(r)$ and $u'(r)$ respectively.

Then, if b is in B, it holds, as will be seen below, that

$$u(AX) \equiv u(XA) \equiv Xu(A) \pmod{\mathfrak{P}^r} \tag{34}$$

$$(35) \qquad u(Ab) \equiv u(bA) \equiv bu(A) \qquad (\text{mod. } \mathfrak{P}^r)$$

$$(36) \qquad u(A'X) \equiv u(XA') \equiv 0 \qquad (\text{mod. } \mathfrak{P}^r)$$

$$(37) \qquad u(A'b) \equiv u(bA') \equiv 0 \qquad (\text{mod. } \mathfrak{P}^r)$$

Even if we put u' in place of u, the above four equalities remain valid. Thus for α, α', β, β' of F it follows from the linearity of u' that

$$u'(\alpha A\alpha' + \beta A'\beta') \equiv \alpha\alpha' u'(A) \qquad (\text{mod. } \mathfrak{P}^r),$$

which means that u' is decided if we assign $u'(A)\,(\text{mod. } \mathfrak{P}^r)$. Since $W: f \to u'$ is an epimorphism, therefore, we have an isomorphism

$$H^n[\mathfrak{A}, B, \text{Hom}(R, M)] \approx H^n(\mathfrak{A}, B, M),$$

which maps $[u'(a_3, \ldots\ldots, a_{n+2})](A)$ to $u'(a_3, \ldots\ldots, a_{n+2})$.

Consequently, our reduction theorem means that $H^{n+2}[\mathfrak{A}, B, (\mathfrak{A}/\mathfrak{P}^r)] \approx H^n[\mathfrak{A}, B, (\mathfrak{A}/\mathfrak{P}^r)]$, from which, together with theorems 2, 3, our assertion follows immediately.

Now, we shall show (34),……, (37), (writing $=$ in stead of $\equiv$).

It holds that $u(b) = 0$, b in B, and that, if we put $a_1 = 1$ in (6),

$$(38) \qquad u(X) = 0.$$

From this, and (6) with $a_1 = X$, we see

$$(39) \qquad u(X^2) = -f(X, X).$$

Similarly it follows inductively from $f(\ , 1) = 0$ that

$$(40) \qquad u(X^i) = -\sum_{j=1}^{i} X^{i-j} f(X, X^{i-1}).$$

In the same way we have

$$(41) \qquad n(X^i b) = -\sum_{j=1}^{i} X^{i-j} f(X, X^{i-1}b).$$

Thus we obtain that

$$\begin{aligned} u(XA) &= Xu(A) && \text{(from (8))} \\ &= X[u(X^n) - u(p)] && \text{(by the linearity)} \\ &= X[u(X^n)] && \text{(from (5)).} \end{aligned}$$

Accordingly (40) yields that

$$(42) \qquad u(XA) = -\sum_{i=1}^{n} X^{n-i+1} f(X, X^{i-1}).$$

On the other hand

$$u(AX) = u(X^{n+1} - pX) = u(X^{n+1}) - u(pX)$$

$$= u(X^{n+1}) - pu(X) \qquad \text{(by the } B\text{-normality)}$$
$$= u(X^{n+1}) \qquad \text{(from (38))}$$
$$= u(X^{n+1}) - u(X)p = u(X^{n+1}) - u(Xp)$$
$$= u(X^{n+1} - Xp) = u(XA),$$

thus (34) is obtained. In the similar way as (42) we have

$$u(bA) = bu(A) = -b\sum_{i=1}^{n} X^{n-i} f(X, X^{i-1}). \tag{43}$$

Meanwhile it holds that

$$u(Ab) = u(X^n b - pb) = u(X^n b) - u(pb)$$
$$= u(X^n b) \qquad \text{(by the } B\text{-normality)}$$
$$= -\sum_{i=1}^{n} X^{n-i} f(X, X^{i-1}b),$$

where f is fully invariant, and then modulo R that

$$= -\sum_{i=1}^{n} X^{n-i} f(X, b^{\tau^{(i-1)}} X^{i-1})$$
$$= -\sum_{i=1}^{n} X^{n-i} f(Xb, {}^{\tau^{(i-1)}} X^{i-1}) \quad \text{(by the } B\text{-normality)}$$
$$= -\sum_{i=1}^{n} X^{n-i} f(b^{\tau^i} X, X^{i-1}) \quad \text{(since } f \text{ is fully invariant)}$$
$$= -\sum_{i=1}^{n} X^{n-i} b^{\tau^i} f(X, X^{i-1}) \quad \text{(by the } B\text{-normality)},$$

where $\omega^{q^i} = \omega^{\tau}$. Since M is an F-module induced by the natural homomorphism of F onto A, we see by computing modulo R that

$$= -\sum_{i=1}^{n} b^{\tau^n} X^{n-i} f(X, X^{i-1})$$
$$= -\sum_{i=1}^{n} b\, X^{n-i} f(X, X^{i-1}).$$

From this together with (43) follows (35).

As for (36),

$$u(XA') = Xu(A') \text{ (from (8))},$$

further from (6) and the B-normality of u,

$$= X(Xu(\omega) - f(X, \omega) - \omega^{\tau} u(X)),$$
$$= 0,$$

because of the B-normalities and the third by (38). Similarly we have

$$\begin{aligned} u(A'X) &= u(X\omega X - \omega^T X^2) \\ &= Xu(\omega X) - f(X, \omega X) - \omega^T u(X^2) \\ &= X\omega u(X) - f(X\omega, X) + \omega^T f(X, X) \\ &= \qquad - f(X\omega, X) + f(\omega^T X, X) \\ &= -f(A', X) \\ &= 0 \quad , \end{aligned}$$

since f is fully invariant.
Thus (36) is proved. Finally as for (37),

$$\begin{aligned} u(bA') &= bu(A') = bu(X\omega) - bu(\omega^T X) \\ &= bXu(\omega) - bf(X,\omega) - b\omega^T u(X) \\ &= 0, \end{aligned}$$

because u and f are B-normal. By the same reason we see that

$$\begin{aligned} u(A'b) &= u(X\omega b) - u(\omega^T X b) \\ &= Xu(\omega b) - f(X, \omega b) - \omega^T u(Xb) \\ &= -\omega^T X u(b) + \omega^T f(X, b) \\ &= 0, \end{aligned}$$

so that (37) is also shown and we have proved all our assertions.

q. e. d.

REFERRENCES

[1] ARTIN, E., Algebraic numbers and algebraic functions I, Princeton Univ. & New York Univ. (1950–1951) lecture note, pp. 83.
[2] DEURING, M., Algebren, Erg. d. Math., Leipzig (1935), Satz. 2. s. 109.
[3] EILENBERG, S. AND MACLANE, S., Cohomology theory in abstract groups I, Ann. of Math., 48(1947), 51–78.
[4] HOCHSCHILD, G., Relative homological algebra. A. M. S., 82(1956), 246–269.
[5] KAWADA, Y., On the derivations in number fields. Ann. of Math., 54(1951), 302–314.
[6] KAWADA, Y., On the derivations in algebra. Scientific Papers of college of General Education University of Tokyo, 2(1952), 1–13.
[7] LYNDON, R., New proof for a theorem of Eilenberg and MacLane. Ann. of Math., 50 (1949), 731–735.
[8] YAMASAKI, H., On products of Hochschild groups, Tohoku Math. J., 11(1959), 147–161.

IWATE UNIVERSITY.