PROCEEDINGS OF THE
10TH SYMPOSIUM ON RING THEORY

HELD AT SHINSHU UNIVERSITY, MATSUMOTO

AUGUST 18-20, 1977

EDITED BY

SHIZUO ENDO
Tokyo Metropolitan University

MANABU HARADA
Osaka City University

HIROYUKI TACHIKAWA
The University of Tsukuba

HISAO TOMINAGA
Okayama University

1978

OKAYAMA, JAPAN

PROCEEDINGS OF THE 10TH SYMPOSIUM ON RING THEORY

HELD AT SHINSHU UNIVERSITY, MATSUMOTO

AUGUST 18-20, 1977

EDITED BY

SHIZUO ENDO
Tokyo Metropolitan University

MANABU HARADA
Osaka City University

HIROYUKI TACHIKAWA
The University of Tsukuba

HISAO TOMINAGA
Okayama University

1 9 7 8

OKAYAMA, JAPAN

CONTENTS

LIST OF CONTRIBUTORS

Y. Kawada, Kyoto Technical University, Kyoto

T. Kanzaki, Osaka Women's University, Sakai

K. Kishimoto, Shinshu University, Matsumoto

K. Kitamura, Osaka University of Education, Osaka

S. Koshitani, The University of Tsukuba, Ibaraki

K. Masaike, Tokyo University of Art and Science, Koganei

T. Nagahara, Okayama University, Okayama

M. Sato, The University of Tsukuba, Ibaraki

T. Sumioka, Osaka City University, Osaka

M. Takeuchi, The University of Tsukuba, Ibaraki

Y. Tsushima, Osaka City University, Osaka

K. Yokogawa, Nara Women's University, Nara

LIST OF PARTICIPANTS

Akiba, Tomoharu	Kyoto University
Aoyama, Kanroku	Kumamoto University
Asano, Shigemoto	Tokyo Institute of Technology
Asano, Yoshihiro	Chiba University
Endo, Shizuo	Tokyo Metropolitan University
Fujita, Hisamasa	The University of Tsukuba
Fukawa, Masami	Tokai University
Harada, Manabu	Osaka City University
Harui, Hideki	Fukuoka University of Education
Hattori, Akira	The University of Tokyo
Hikari, Michitaka	Keio University
Hirano, Shinichi	The University of Tsukuba
Hirano, Yasuyuki	Okayama University
Hirao, Kimihiro	Okayama University
Hirata, Kazuhiko	Chiba University
Hongan, Motoshi	Tsuyama College of Technology
Ikehata, Shûichi	Okayama University
Imai, Masataka	Tokai University
Inatomi, Akira	Meiji University
Ishibashi, Hiroyuki	Josai University
Ishii, Tadamasa	Kinki University
Ishikawa, Takeshi	Tokyo Metropolitan University
Iwai, Akira	Kyoto University

Iwanaga, Yasuo	The University of Tsukuba
Izawa, Tatsuo	Shizuoka University
Kado, Jirô	Osaka City University
Kakiichi, Yoshiaki	Toyo University
Kanbara, Hikoji	Osaka City University
Kanzaki, Teruo	Osaka Women's University
Katayama, Hisao	Yamaguchi University
Kato, Toyonori	The University of Tsukuba
Kawada, Yutaka	Kyoto Technical University
Kawamoto, Naoki	Hiroshima University
Kikuchi, Teppei	Nara University of Education
Kishimoto, Kazuo	Shinshu University
Kitamura, Kazuo	Osaka University of Education
Kitamura, Yoshimi	Tokyo University of Art and Science
Koshitani, Shigeo	The University of Tsukuba
Kubo, Fujio	Hiroshima University
Kurata, Yoshiki	Yamaguchi University
Kutami, Mamoru	Yamaguchi University
Makino Ryôhei	Fukushima University
Marubayashi, Hidetoshi	Osaka University
Masaike, Kanzo	Tokyo University of Art and Science
Miyaji, Ikuo	Okayama University
Miyashita, Yôichi	The University of Tsukuba
Miyata, Takehiko	Osaka City University
Mogami, Isao	Tsuyama College of Technology
Morimoto, Shoji	Hagi Koen High School
Motose, Kaoru	Shinshu University

Murase, Ichiro	Tokyo Women's University
Nagahara, Takasi	Okayama University
Nakajima, Atsushi	Okayama University
Nakamoto, Taichi	Science University of Okayama
Nakane, Ken	Ibaraki University
Nemoto, Seiji	Tokai University
Ninomiya, Yasushi	Shinshu University
Nishida, Kenji	Hokkaido University
Nishikawa, Akira	Shinshu University
Nobusato, Yoshiyasu	Osaka City University
Ôbayashi, Tadao	Osaka City University
Ôhori, Masayuki	Shinshu University
Onodera, Takeshi	Hokkaido University
Osada, Naoki	Nagasaki University of Shipbuilding
Ōshiro, Kiyoichi	Yamaguchi University
Ôtake, Kôichirô	The University of Tsukuba
Otsuka, Kayo	Kyoto University
Sakane, Chikao	Tokyo University of Art and Science
Sato, Hideo	Wakayama University
Sato, Masahisa	The University of Tsukuba
Shigenaga, Kazuo	Ube College of Technology
Shirai, Kumie	Yamaguchi University
Sumioka, Takeshi	Osaka City University
Sumiyama, Takao	Aichi Technical University
Suzuki, Yasutaka	Niigata University
Tachikawa, Hiroyuki	The University of Tsukuba
Tahara, Ken-ichi	Aichi University of Education

Takeuchi, Mitsuhiro	The University of Tsukuba
Takeuchi, Tsutomu	Hirosaki University
Takeuchu, Yasuji	Kobe University
Tôgô, Shigeaki	Hiroshima University
Tominaga, Hisao	Okayama University
Tsushima, Yukio	Osaka City University
Ukegawa, Takasaburo	Kobe University
Wakamatsu, Takayoshi	The University of Tsukuba
Yamada, Toshihiko	Tokyo Metropolitan University
Yamagata, Kunio	The University of Tsukuba
Yamaguchi, Ken-ichi	Chiba University
Yasuda, Jun	Shizuoka University
Yokogawa, Kenji	Nara Women's University

PREFACE

This volume contains the articles presented at the 10th Symposium on Ring Theory held at Shinshu University, August 18-20, 1977.

The annual Symposium on Ring Theory was founded in 1968. The main aims of the Symposium are to provide a means for the dissemination of recent theories on rings and modules which are not yet widely known and to give algebraists an opportunity to report on recent progress in the ring theory.

The 10th Symposium itself was supported by the Scientific Research Grant of the Educational Ministry of Japan (Subject No. 230601).

The existence of the proceedings is due to the assistance and cooperation of the authors; the final typescript the efforts of the staff of the Department of Mathematics, Okayama University.

Finally we would like to thank Prof. K. Kishimoto for his unending patient and kind hospitality to the participants of the Symposium.

S. Endo

M. Harada

H. Tachikawa

H. Tominaga

ON FREE CYCLIC EXTENSIONS OF RINGS

Takasi NAGAHARA
Okayama University
and
Kazuo KISHIMOTO
Shinshu University

Throughout this paper, B will mean a (non-commutative) ring with identity element which has an automorphism ρ. As is [2], [3], [5] and [6], by $B[X;\rho]$, we denote the ring of all polynomials $\sum_i X^i b_i$ ($b_i \in B$) with an indeterminate X whose multiplication is defined by $bX = X\rho(b)$ for each $b \in B$. Moreover, by $B[X;\rho]_{(2)}$ (resp. $B[X;\rho]_{(n*)}$), we denote the subset of $B[X;\rho]$ of all polynomials $f = X^2 - Xa - b$ with $fB[X;\rho] = B[X;\rho]f$ and $Xa = aX$ (resp. $f = X^n - b$ with $fB[X;\rho] = B[X;\rho]f$). A polynomial $f \in B[X;\rho]_{(2)} \cup B[X;\rho]_{(n*)}$ is called to be separable (resp. Galois) if the factor ring $B[X;\rho]/fB[X;\rho]$ is a separable (resp. Galois) extension of B in the sense of [4]. The purpose of this note is to study (separable) polynomials f in $B[X;\rho]_{(2)} \cup B[X;\rho]_{(n*)}$ and the factor rings $B[X;\rho]/fB[X;\rho]$. Our results are all contained in [2], [3], [5] and [6]. However, the proofs contain some simplifications which are somewhat interest in alternative verifications.

In what follows, we shall summarize the notations which will be used very often in the subsequent study, and we shall use the following conventions:

Z = the center of B.

$B_1 = \{b \in B \mid \rho(b) = b\}$, $Z_1 = Z \cap B_1$.

$B(\rho^n) = \{b \in B \mid cb = b\rho^n(c)$ for all $c \in B\}$, where n is any integer, and $B_1(\rho^n) = B_1 \cap B(\rho^n)$.

$U(B)$ = the set of all inversible elements in B.

$U(B_1) = U(B) \cap B_1$, $U(Z_1) = U(B) \cap Z_1$.

b_l (resp. b_r) = the left (resp. right) multiplication effected by $b \in B$, and $\tilde{b} = b_l^{-1}b_r$ for any $b \in U(B)$.

Moreover, for a ring extension A/B and a set G of automorphisms in A, $J(G,A)$ denotes the subring $\{a \in A \mid \sigma(a) = a$ for all $\sigma \in G\}$, and A/B is called G-Galois if G is a group, $J(G,A) = B$, and there are elements $a_1, \ldots, a_n$, $a_1^*, \ldots, a_n^*$ such that $\sum_i a_i\sigma(a_i^*) = \delta_{1,\sigma}$ (Kronecker's delta) for all σ in G (cf. [4]).

1. On $B[X;\rho]_{(2)}$. First, we shall prove the following

Lemma 1.1. Let A be a ring extension of B with $A = xB + B$, and assume that there is a B-ring automorphism σ in A such that $x - \sigma(x)$ is inversible in A. Then $\{x, 1\}$ is a right free B-basis of A, and $J(\sigma,A) = B$.

Proof. Let $0 = xb_1 + b_o$ where $b_1, b_o \in J(\sigma,A)$. Then $0 = (xb_1 + b_o) - \sigma(xb_1 + b_o) = (x - \sigma(x))b_1$. Since $x - \sigma(x)$ is inversible, we have $b_1 = 0$, and so, $b_o = 0$. Thus $\{x, 1\}$ is right $J(\sigma,A)$-free. Since $B \subset J(\sigma,A)$ and $A = xB + B$, it follows that $\{x, 1\}$ is a right free $J(\sigma,A)$-basis of A, and $B = J(\sigma, A)$.

Lemma 1.2. Let A be a G-Galois extension of B such that $A = xB + B = Bx + B \neq B$. Then G is of order 2, and for $\sigma \neq 1$ in G, $x - \sigma(x)$ is inversible in A. Moreover, $\{x, 1\}$ is a right free B-basis of A and is also a left free B-basis of A.

Proof. Since A is G-Galois over B, there exist elements $u_1, \ldots, u_n, v_1, \ldots, v_n$ in A such that

$$\sum_i u_i\tau(v_i) = \delta_{1,\tau} \quad \text{for all} \quad \tau \in G.$$

Hence $\sum_i \tau^{-1}(u_i)v_i = \delta_{1,\tau}$ for all $\tau \in G$, that is,

$$\sum_i \tau(u_i)v_i = \delta_{\tau,1} \quad \text{for all} \quad \tau \in G.$$

Now, we set $v_i = b_ix + c_i$ ($b_i, c_i \in B$, $i = 1, \ldots, n$), $y = \sum_i u_ib_i$, and $z = \sum_i u_ic_i$. Then, for $\tau \in G$, we have $\sum_i u_i\tau(v_i) = y\tau(x) + z$. Let $\tau \neq 1$ be an arbitrary element of G. Then $1 = yx + z - (y\tau(x) + z) = y(x - \tau(x))$. This implies that $x - \tau(x)$ has a left inverse. By a similar method, we see that $x - \tau(x)$ has a right inverse. Hence $x - \tau(x)$ is inversible in A, and $x - \tau(x) = y^{-1}$. Thus, for any τ_1 in G with $\tau_1 \neq 1$, we have $x - \tau(x) = y^{-1} = x - \tau_1(x)$, and so, $\tau(x) = \tau_1(x)$. Since $A = xB + B$, it follows that $\tau = \tau_1$, and whence G is of order 2. The other assertions are direct consequences of Lemma 1.1.

Lemma 1.3. Let A be a ring extension of B such that $A = xB + B = Bx + B$, $\{x, 1\}$ is right B-free, and $x^2 = xa + b$ ($a, b \in B$). Assume that $xB = Bx$, and $ax = xa$. If $a^2 + 4b$

is inversible in B then A is Galois over B.

Proof. Let β be an arbitrary element of B. Since $xB = Bx$, we may write $\beta x = x\beta^*$ for some $\beta^* \in B$. Then $\beta(xa + b) = (x\beta^*)a + \beta b = x(\beta^* a) + \beta b$, $\beta x^2 = (x\beta^*)x = x^2\beta^{**} = (xa + b)\beta^{**} = x(a\beta^{**}) + b\beta^{**}$. This implies $\beta^* a = a\beta^{**}$. Since $\{\beta^* \mid \beta \in B\} = B$, it follows that $\beta a = a\beta^*$ for all $\beta \in B$. Hence we obtain that for any $\beta \in B$, $\beta(a - x) = (a - x)\beta^*$, and $a(a - x) = (x - a)a$. Moreover, we have $(a - x)^2 = a^2 - 2xa + x^2 = a^2 - 2xa + xa + b = (a - x)a + b$. Hence the mapping

$$\sigma : xb_1 + b_o \to (a - x)b_1 + b_o \quad (b_1, b_o \in B)$$

is a B-ring automorphism of A. Now, we assume that $a^2 + 4b$ is inversible in B. Then, since $(\sigma(x) - x)^2 = (a - 2x)^2 = a^2 - 4xa + 4x^2 = a^2 + 4b$, the difference $\sigma(x) - x$ is inversible in A. Hence $\sigma \neq 1$, $\sigma^2 = 1$, and $J(\sigma, A) = B$ by Lemma 1.2. Now, we set $u_1 = (a - 2x)^{-1}(a - x)$, $u_2 = (a - 2x)^{-1}$, $v_1 = 1$, and $v_2 = -x$. Then $\sum_i u_i\tau(v_i) = \delta_{1,\tau}$ for all $\tau \in \{1, \sigma\}$. Hence, it follows that A is a Galois extension of B with Galois group $\{1, \sigma\}$.

Now, as in [5, p.69], one will easily see the following

(i) $B[X;\rho]_{(2)} = \{X^2 - Xa - b \mid a \in B_1(\rho) \text{ and } b \in B_1(\rho^2)\}$.

For any $f = X^2 - Xa - b \in B[X;\rho]_{(2)}$, we denote the factor ring $B[X;\rho]/fB[X;\rho]$ by $B[x;\rho, a, b]$ where $x = X + fB[X;\rho]$, and we denote $a^2 + 4b$ by $\delta(f)$.

Next, we shall prove the following

Lemma 1.4. Let $f = X^2 - Xa - b \in B[X;\rho]_{(2)}$. Then f is separable over B if and only if there exist elements b_1, b_2, b_3 and b_4 in B such that

(ii) $1 = bb_1 + b_4$ (iii) $ab_1 + b_2 + b_3 = 0$

(iv) $bb_1 = ab_2 + \rho(b_4)$ (v) $b_1 \in B(\rho^{-2})$

(vi) $b_2 \in B(\rho^{-1})$ (vii) $\rho(b_2) = b_3$

(viii) $b_4 \in Z$.

Moreover, in this case, the subring $Z[a, b, b_1, \rho(b_1), b_2, b_3, b_4, \rho(b_4)]$ of B is a commutative ring, and in which there exist elements b_5 abd b_6 in B such that

(*) $4 = \delta(f)b_5 = b_5\delta(f)$, and $a = \delta(f)b_6 = b_6\delta(f)$.

Proof. We set $A = B[x; \rho, a, b]$ and assume f is separable over B. Then, the (left)A-(right)A-homomorphism

$$\phi : A \otimes_B A \to A \quad (\textstyle\sum_i a_i \otimes b_i \to \sum_i a_i b_i)$$

splits. Hence there exists an element e in $A \otimes_B A$ such that $\phi(e) = 1$ and $(c \otimes 1)e = e(1 \otimes c)$ for all $c \in A$. Since $A \otimes_B A = (x \otimes x)B + (x \otimes 1)B + (1 \otimes x)B + (1 \otimes 1)B$, we may write

$$e = (x \otimes x)b_1 + (x \otimes 1)b_2 + (1 \otimes x)b_3 + (1 \otimes 1)b_4$$

where $b_i \in B$, $i = 1, .. ,4$. Then, we have that $x^2b_1 + xb_2 + xb_3 + b_4 = 1$, $(x \otimes 1)e = e(1 \otimes x)$, and $(\alpha \otimes 1)e = e(1 \otimes \alpha)$ for each $\alpha \in B$. Since $\{x \otimes x, x \otimes 1, 1 \otimes x, 1 \otimes 1\}$ is a right free B-basis of $A \otimes_B A$, one will easily see that

(a) $1 = bb_1 + b_4$ (b) $ab_1 + b_2 + b_3 = 0$

(c) $ab_1 + b_3 = a\rho(b_1) + \rho(b_2)$ (d) $ab_2 + b_4 = b\rho(b_1)$

(e) $bb_1 = a\rho(b_3) + \rho(b_4)$ (f) $bb_2 = b\rho(b_3)$

(g) $\rho^2(\alpha)b_1 = b_1\alpha$ (h) $\rho(\alpha)b_2 = b_2\alpha$

(i) $\rho(\alpha)b_3 = b_3\alpha$ (j) $\alpha b_4 = b_4\alpha$

where α runs over all the elements of B. Conversely, if there exist elements b_1, b_2, b_3 and b_4 in B which satisfy the conditions (a - j) then the map ϕ (stated earlier) splits, that is, A is separable over B. Hence it suffices to prove that the system of conditions (ii - viii) is equivalent to that of conditions (a - j). Assume (ii - viii). Then, (vi, vii) imply that for each α in B, $\rho(\alpha)b_3 = \rho(\alpha)\rho(b_2) = \rho(\alpha b_2) = \rho(b_2\rho^{-1}(\alpha)) = \rho(b_2)\alpha = b_3\alpha$. Hence we have (i), that is,

(ix) $$b_2,\ b_3 \in B(\rho^{-1}).$$

Moreover, (v - ix, i - iii) imply (g - j, a, b) and that for each $i = 1, \ldots, 4$,

(x) $$ab_i = b_ia = a\rho(b_i) = \rho(ab_i) = \rho(b_ia) = \rho(b_i)a$$

(xi) $$bb_i = b_ib = b\rho^2(b_i) = \rho^2(bb_i) = \rho^2(b_ib) = \rho^2(b_i)b$$

$$bb_1 = 1 - b_4 = 1 - \rho^2(b_4).$$

As is easily seen, (iii, vii, x) imply $ab_1 + \rho(b_2) + \rho(b_3) = 0$ and

(xii) $\rho(b_2) = b_3$, $\rho(b_3) = b_2$, $ab_2 = a\rho(b_2) = ab_3 = a\rho(b_3)$.

Further, (x - xii, iv) imply (c - f). Thus, (a - j) are contained in (ii - viii). Conversely, assume (a - j). Then (g - j) imply (v, vi, viii - x). As is easily seen, (x) and (b, c) imply (xii) which contains (vii). Clearly, (xii) and (e) imply (iv). Hence (ii - viii) are contained in (a - j). Thus we obtain the first assertion. Now, by (ix, xii) and (xi), we have

(xiii) $$b_2^2 = b_2b_3 = b_3^2 = b_3b_2$$

(xiv) $$\rho^2(b_4) = b_4.$$

This and (v, xii) imply

(xv) $\quad b_1b_i = \rho^2(b_i)b_1 = b_ib_1 \quad (i = 1, .., 4).$

Moreover, by (ii, viii, xi), we have $1 = b\rho(b_1) + \rho(b_4)$, $\rho(b_4) \in Z$, and $bb_1 = b_1b$. Hence $0 = b_1(b\rho(b_1) + \rho(b_4)) - (b\rho(b_1) + \rho(b_4))b_1 = bb_1\rho(b_1) - b\rho(b_1)b_1$, that is, $bb_1\rho(b_1) = b\rho(b_1)b_1$. This and (v, x) imply that $\rho(bb_1\rho(b_1)) = \rho(b\rho(b_1)b_1) = \rho(bb_1\rho^{-1}(b_1)) = b\rho(b_1)b_1 = bb_1\rho(b_1)$, $\rho^2(b_1^2) = \rho^2(b_1\rho^{-2}(b_1)) = \rho^2(b_1)b_1 = b_1b_1 = b_1^2$, and $\rho(ab_2b_1) = ab_2b_1$. By (ii, xiv, iv, xii), $1 \cdot b_1$ is written as

$$b_1 = (bb_1 + b_4)b_1 = (bb_1 + \rho^2(b_4))b_1$$
$$= (bb_1 + b\rho(b_1) - a\rho(b_2))b_1 = bb_1^2 + b\rho(b_1)b_1 - ab_2b_1.$$

Hence, it follows that

(xvi) $\quad \rho^2(b_1) = b_1$, and $\rho(b_1)b_1 = b_1\rho^{-1}(b_1) = b\rho(b_1)$.

We set here $S = \{a, b, b_1, \rho(b_1), b_2, b_3, b_4, \rho(b_4)\}$. Then, by (viii, x - xvi), we have

(xvii) $uv = vu$ for each pair $u, v \in S$, and $\rho(S) = S$.

Hence the subring $Z[S]$ of B is a commutative ring. Moreover, from (iii, xii), we see the following

(xviii) $\quad a^2b_1 = a(-b_2 - b_3) = -ab_2 = -2ab_3.$

Now, we set $b_5 = b_1 + \rho(b_1)$. Then

(xix) $\quad \delta(f)b_5 = (a^2 + 4b)(b_1 + \rho(b_1))$

$= a(ab_1 + a\rho(b_1)) + 4(bb_1 + b\rho(b_1))$

$= 2a^2b_1 + 4(bb_1 + 1 - \rho(b_4))$ (by (x, ii))

$= 2(-2ab_2) + 4(ab_2 + 1) = 4$ (by (xviii, iv))

(xx) $\quad a = a(bb_1 + b_4) = a(bb_1 + \rho^2(b_4))$ (by (ii, xiv))

$= a(bb_1 + b\rho(b_1) - a\rho(b_2))$ (by (iv))

$= 2abb_1 - a^2b_2$ (by (x))

$$= 2(2abb_1 - a^2b_2)bb_1 - a^2b_2$$
$$= 4ab^2b_1^2 - a^2(2bb_1b_2 + b_2) \qquad \text{(by (xvii))}$$
$$= 4ab^2b_1^2 - (\delta(f) - 4b))(2bb_1b_2 + b_2)$$
$$= \delta(f)(b_5ab^2b_1^2 - (1 - b_5b)(2bb_1b_2 + b_2)) \qquad \text{(by (xix))}.$$

This completes the proof.

Now, we shall prove the following theorem which is one of the main results of this note.

<u>Theorem 1.5</u>. For $f \in B[X;\rho]_{(2)}$, f is Galois over B if and only if $\delta(f)$ is inversible in B.

<u>Proof</u>. Let $f = X^2 - Xa - b \in B[X;\rho]_{(2)}$, and set $A = B[x;\ \rho,\ a,\ b]$. If $\delta(f)$ is inversible in B then, by Lemma 1.3, A is Galois over B, and hence, f is Galois over B. To see the converse, we assume that f is Galois over B. Then, by Lemma 1.2, A is a Galois extension of B with Galois group of order 2, whose group will be written as $\{\sigma, 1\}$. Now, we set $c = x + \sigma(x)$. Then $\sigma(c) = c$, and so, $c \in B$. Since $x^2 - xa - b = 0$, we have $0 = (\sigma(x))^2 - \sigma(x)a - b = (c - x)^2 - (c - x)a - b = x(2a - c - \rho(c)) + c^2 - ca$, which shows

$$c + \rho(c) = 2a, \quad \text{and} \quad c^2 = ca.$$

By Lemma 1.2, $x - \sigma(x)$ is inversible in B, and

$$(x - \sigma(x))^2 = (2x - c)^2 = 4x^2 - 2x(c + \rho(c)) + c^2$$
$$= 4x^2 - 4xa + ca = b4 + ca = 4b + a\rho(c).$$

By [4, Th.1.5], A is separable over B, and so is f. Hence, by Lemma 1.4, $\delta(f)$ is a left and right divisor of 4 and a, and so is of $(x - \sigma(x))^2$. Thus, $\delta(f)$ is inversible in A.

Since A has a (left and right) free B-basis $\{x, 1\}$, it follows that $\delta(f)$ is inversible in B.

Next, we consider the following conditions.

(C_1) 2 is inversible in B.

(C_2) $\rho|Z$ (the restriction ρ to Z) = 1

(C_3) $B[X;\rho]_{(2)}$ contains a Galois polynomial.

Now, we shall prove the following

Theorem 1.6. Assume one of the conditions (C_1) - (C_3). Then, for an element $f \in B[X;\rho]_{(2)}$, the following conditions are equivalent.

(a) f is Galois over B.

(b) $\delta(f)$ is inversible in B.

(c) f is separable over B.

Proof. In virtue of Th.1.5 and [4, Th.1.5], it suffices to prove that (c) implies (b). Let $f = X^2 - Xa - b$ be a separable polynomial in $B[X;\rho]_{(2)}$, and set $A = B[x;\rho, a, b]$.

Case (C_1). Set $y = x - (1/2)a$, and $b' = (a^2 + 4b)/4$ Then $y^2 = b'$ and $A = yB + B$. Clearly $Y^2 - b' \in B[Y;\rho]_{(2)}$, and this is separable over B. Hence by Lemma 1.4, there exist elements b_1, b_2 and b_4 such that $1 = b'b_1 + b_4$, $b'b_1 = b_1b'$, $b'b_1 = \rho(b_4)$, and $b'\rho(b_1) = \rho^2(b_4) = b_4$ (by (ii, iv, xi)); hence $1 = b'b_1 + b'\rho(b_1) = b'(b_1 + \rho(b_1)) = (b_1 + \rho(b_1))b'$. Thus b' is inversible in B, and so is $a^2 + 4b = \delta(f)$.

Case (C_2). Let $\{b_1, b_2, b_3, b_4\}$ be a system of elements of B which satisfies the conditions (ii - viii). Then, by (ii, iv), we have that $1 = bb_1 + b_4 = bb_1 + bb_1 - ab_2 = (2bb_1 - ab_2)^2 = 4b^2b_1^2 - 4abb_1b_2 + a^2b_2^2$. Hence, it follows from Lemma 1.4(*) that $\delta(f)$ is inversible in B.

Case (C_3). In virtue of the case (C_1), we assume that 4 is not inversible in B, that is, $B \neq 4B$. By our assumption, there is a Galois polynomial $g = X^2 - Xu - v$ in $B[X;\rho]_{(2)}$. Then, by Th.1.5, $\delta(g) = u^2 + 4v$ is inversible in B, and hence $1 = ru^2 + 4rv$ for some $r \in B$. Now, since $f = X^2 - Xa - b$ is separable over B, by Lemma 1.4 there exists a system $\{b_1, b_2, b_3, b_4\}$ of elements in B which satisfies the conditions (ii - viii). In the rest of the proof, $h \equiv k$ denotes the congruence $h \equiv k$ modulo $4B$ in B. Then, noting $b_4 \in Z$, we have $\rho(b_4) \equiv ru^2\rho(b_4) \equiv rub_4u \equiv ru^2b_4 \equiv b_4$. Since $1 = bb_1 + b_4$ and $bb_1 = ab_2 + \rho(b_4)$, we obtain

$$1 \equiv bb_1 + b_4 \equiv bb_1 + \rho(b_4) \equiv bb_1 + bb_1 - ab_2 \equiv 2bb_1 - ab_2$$
$$\equiv (2bb_1 - ab_2)^2 \equiv a^2b_2^2.$$

Hence, it follows from Lemma 1.4(*) that

$$1 \in aB + 4B \in \delta(f)B = B\delta(f).$$

This shows that $\delta(f)$ is inversible in B.

<u>Remark</u>. Let $f = X^2 - Xa - b$ be a polynomial of $B[X;\rho]$ such that $fB[X;\rho] = B[X;\rho]f$. Then, as is easily seen, we have

(1) $\quad a \in B(\rho)$, $b \in B_1(\rho^2)$, and $ba = b\rho(a)$.

This implies the following

(2) $\quad ba = ab = b\rho(a) = \rho(a)b$

(3) $\quad a^2 = a\rho(a) = \rho(a)\rho(a) = \rho(a^2) \in B_1$.

We shall here assume that f is separable over B, that is, the factor ring $B[X;\rho]/fB[X;\rho]$ is separable over B. Then, by making use of the same methods as in the proof of Lemma 1.4, we see that there exist elements b_1, b_2 and b_4 in B which satisfies the following

(4) $1 = bb_1 + b_4$ (5) $ab_2 + b_4 = b\rho(b_1)$ (6) $b_4 \in Z$.

Then, it follows that

$$\begin{aligned}
\rho(a) &= \rho(a(bb_1 + b_4)) = \rho(abb_1) + \rho(ab_4) && \text{(by (4))}\\
&= \rho(a)b\rho(b_1) + \rho(a)\rho(b_4) && \text{(by (1))}\\
&= ab\rho(b_1) + \rho(a)\rho(b\rho(b_1) - ab_2) && \text{(by (2) and (5))}\\
&= ba\rho(b_1) + \rho(a)\rho^2(b_1) - \rho(a)\rho(a)\rho(b_2) && \text{(by (1) and (2))}\\
&= bb_1a + ab\rho^2(b_1) - aa\rho(b_2) && \text{(by (1) and (2))}\\
&= (1 - b_4)a + ba\rho^2(b_1) - ab_2a && \text{(by (4), (2) and (1))}\\
&= a(1 - b_4) + b\rho(b_1)a - (b\rho(b_1) - b_4)a && \text{(by (6), (1) and (5))}\\
&= abb_1 + b_4a = abb_1 + ab_4 && \text{(by (4) and (6))}\\
&= a(bb_1 + b_4) = a. && \text{(by (4))}
\end{aligned}$$

Hence, it follows that $f \in B[X;\rho]_{(2)}$. Therefore, by Th.1.5, we see that for $f = X^2 - Xa - b \in B[X;\rho]$ with $fB[X;\rho] = B[X;\rho]f$, f is Galois over B if and only if $f \in B[X;\rho]_{(2)}$ and $\delta(f)$ is inversible in B.

In the rest of this section, we shall deal with the set of B-ring isomorphism classes of the factor rings $B[X;\rho]/fB[X;\rho]$ ($f \in B[X;\rho]_{(2)}$). For elements g and $g_1 \in B[X;\rho]_{(2)}$, if the factor rings $B[X;\rho]/gB[X;\rho]$ and $B[X;\rho]/g_1B[X;\rho]$ are B-ring isomorphic then we write $g \sim g_1$. Clearly, the relation $\sim$ is an equivalence relation in $B[X;\rho]_{(2)}$. By $B[X;\rho]_{(2)}^{\sim}$, we denote the set of equivalence classes in $B[X;\rho]_{(2)}$ with respect to the relation $\sim$, and we write $C = \langle g \rangle$ if $C \in B[X;\rho]_{(2)}$ and $g \in C$.

First, as a preliminary lemma, we shall prove the following

Lemma 1.7. Let β be an arbitrary element of $B(\rho)$. Then, the subalgebra of B generated by $Z \cup B_1(\rho) \cup B_1(\rho^2) \cup \{\beta\}$ is a commutative ring. Moreover,

(i) for any $\alpha \in Z$, $\alpha\beta = \rho(\alpha)\beta$, and for any $u_1 \in B_1(\rho)$, $u_1\beta = \beta u_1 = u_1\rho(\beta) = \rho(\beta)u_1 = \rho(\beta u_1)$.

(ii) If $\rho(\beta)\beta = \beta\rho(\beta)$ then $\beta\rho(\beta) = \beta^2 = \rho(\beta)\rho(\beta)$.

Proof. If $b \in B_1$ and $\beta_m \in B(\rho^m)$ $(m = 1, 2)$ then $b\beta_m = \beta_m\rho^m(b) = \beta_m b$. From this, we obtain the first assertion. To see (i), let $\alpha \in Z$ and $u_1 \in B_1(\rho)$. Then $\alpha\beta = \beta\rho(\alpha) = \rho(\alpha)\beta$, and $u_1\beta = \beta\rho(u_1) = \beta u_1 = u_1\rho(\beta) = \rho(\beta)\rho(u_1) = \rho(\beta)u_1 = \rho(\beta u_1)$. Moreover, if $\rho(\beta)\beta = \beta\rho(\beta)$ then $\beta^2 = \beta\rho(\beta) = \rho(\beta)\rho(\beta)$. This completes the proof.

Lemma 1.8. Let $g = X^2 - Xu - v$, $g_1 = X^2 - Xu_1 - v_1 \in B[X;\rho]_{(2)}$. Then, $g \sim g_1$ if and only if there exist elements α, β in B such that $\alpha \in U(Z)$, $\beta \in B(\rho)$, $u = \alpha u_1 + \beta + \rho(\beta)$, and $v = \alpha\rho(\alpha)v_1 - \alpha\beta u_1 - \beta^2$. In this case, there holds that $\rho(\beta)\beta = \beta\rho(\beta) = \beta^2 = \rho(\beta)\rho(\beta)$.

Proof. We consider $B[X;\rho]/gB[X;\rho] = xB + B$ and $B[X;\rho]/g_1B[X;\rho] = yB + B$, where $x = X + gB[X;\rho]$ and $y = X + g_1B[X;\rho]$. First, we assume that there are elements α, $\beta \in B$

such that $\alpha \in U(Z)$, $\beta \in B(\rho)$, $u = \alpha u_1 + \beta + \rho(\beta)$, and $v = \alpha\rho(\alpha)v_1 - \alpha\beta u_1 - \beta^2$. Then, for any $c \in B$,

$$c(y\alpha + \beta) = y\rho(c)\alpha + c\beta = y\alpha\rho(c) + \beta\rho(c) = (y\alpha + \beta)\rho(c),$$

$$\begin{aligned}(y\alpha + \beta)^2 &= y^2\rho(\alpha)\alpha + y(\rho(\beta)\alpha + \alpha\beta) + \beta^2 \\ &= y(u_1\rho(\alpha)\alpha + \rho(\beta)\alpha + \alpha\beta) + v_1\rho(\alpha)\alpha + \beta^2 \\ &= y(\alpha u_1 + \rho(\beta) + \beta)\alpha + (v + \alpha\beta u_1 + \beta^2) + \beta^2 \\ &= yu\alpha + v + \beta(\alpha u_1 + \beta + \rho(\beta)) \\ &= yu\alpha + v + \beta u = (y\alpha + \beta)u + v.\end{aligned}$$

Hence, noting $\alpha \in U(Z)$, the mapping $xc_1 + c_2 \to (y\alpha + \beta)c_1 + c_2$ $(c_1, c_2 \in B)$ is a B-ring isomorphism of $xB + B$ to $yB + B$. Thus we obtain $g \sim g_1$. Conversely, we assume that there is a B-ring isomorphism $\phi : xB + B \to yB + B$. Then $\phi(x) = y\alpha + \beta$ for some $\alpha, \beta \in B$. Since $y = (y\alpha + \beta)c_1 + c_2$ for some c_1 and $c_2 \in B$, the element α is inversible in B. Now, for any $c \in B$, $\phi(cx) = \phi(x\rho(c)) = (y\alpha + \beta)\rho(c) = y\alpha\rho(c) + \beta\rho(c)$, and $\phi(cx) = c\phi(x) = c(y\alpha + \beta) = y\rho(c)\alpha + c\beta$. Hence $\alpha\rho(c) = \rho(c)\alpha$ and $\beta\rho(c) = c\beta$ $(c \in B)$. This implies $\alpha \in U(Z)$ and $\beta \in B(\rho)$. Next, we note

$$\phi(x^2) = \phi(xu + v) = (y\alpha + \beta)u + v = y\alpha u + \beta u + v, \text{ and}$$

$$\begin{aligned}\phi(x^2) = \phi(x)^2 = (y\alpha + \beta)^2 &= y^2\rho(\alpha)\alpha + y(\rho(\beta)\alpha + \alpha\beta) + \beta^2 \\ &= y(u_1\rho(\alpha)\alpha + \rho(\beta)\alpha + \alpha\beta) + v_1\rho(\alpha)\alpha + \beta^2 \\ &= y(u_1\rho(\alpha) + \rho(\beta) + \beta)\alpha + v_1\alpha\rho(\alpha) + \beta^2.\end{aligned}$$

Then $\alpha u = (u_1\rho(\alpha) + \rho(\beta) + \beta)\alpha$, and $\beta u + v = v_1\alpha\rho(\alpha) + \beta^2$. Since $\alpha \in U(Z)$ and $u_1, \beta \in B(\rho)$, it follows

$$u = \alpha u_1 + \rho(\beta) + \beta, \text{ and}$$

$$\begin{aligned}v = v_1\alpha\rho(\alpha) + \beta^2 - \beta u &= \alpha\rho(\alpha)v_1 + \beta^2 - \beta(\alpha u_1 + \rho(\beta) + \beta) \\ &= \alpha\rho(\alpha)v_1 - \alpha\beta u_1 - \beta^2.\end{aligned}$$

Moreover, by Lemma 1.7, we have

$$\begin{aligned}\beta\rho(\beta) &= \beta(u - \alpha u_1 - \beta) = \beta u - \beta\alpha u_1 - \beta^2 \\ &= u\beta - \alpha u_1\beta - \beta^2 = (u - \alpha u_1 - \beta)\beta \\ &= \rho(\beta)\beta = \beta^2 = \rho(\beta)\rho(\beta).\end{aligned}$$

This completes the proof.

Now, for $f_i = X^2 - Xu_i - v_i$ with $u_i, v_i \in B$ $(i = 1, 2)$ and for $s \in B$, we write

$$f_1 \times f_2 = X^2 - Xu_1u_2 - (u_1^2v_2 + v_1u_2^2 + 4v_1v_2)$$

$$f_1 \times s = X^2 - Xu_1s - v_1s^2, \quad \text{and} \quad s \times f_1 = X^2 - Xsu_1 - s^2v_1.$$

Next, let R be the subring of B generated by $Z \cup B_1(\rho) \cup B_1(\rho^2)$. Then, by Lemma 1.7, R is a commutative ring. From this, one will easily see that for $f_i = X^2 - Xu_i - v_i$ with $u_i, v_i \in R$ $(i = 1, 2, 3)$ and for $s_1, s_2 \in R$,

$$f_1 \times f_2 = f_2 \times f_1, \quad (f_1 \times f_2) \times f_3 = f_1 \times (f_2 \times f_3),$$

$$f_1 \times s_1 = s_1 \times f_1, \quad (f_1 \times s_1) \times s_2 = f_1 \times (s_1s_2),$$

$$(f_1 \times f_2) \times s_1 = f_1 \times (f_2 \times s_1) = (f_1 \times s_1) \times f_2.$$

$$\delta(f_1 \times f_2) = \delta(f_1)\delta(f_2), \quad \delta(f_1 \times s_1) = \delta(f_1)s_1^2.$$

where $\delta(f_i) = u_i^2 + 4v_i$ $(i = 1, 2)$.

Moreover, throughout the rest of this section, $\bar{\rho}$ will mean the restriction of ρ to Z. Then, one will easily see that for $p \in Z$, $p \in Z(\bar{\rho}^n)$ if and only if $zp = \rho^n(z)p$ for all $z \in Z$, where n is any integer.

<u>Lemma 1.9</u>. Let $g \in B[X;\rho]_{(2)}$, $\xi \in U(Z_1)$, and $h \sim h_1 \in Z[X;\bar{\rho}]_{(2)}$. Then $g \times \xi$, $g \times h \in B[X;\rho]_{(2)}$, $g \sim g \times \xi$, and $g \times h \sim g \times h_1$.

Proof. Let $g = X^2 - Xu - v$, $h = X^2 - Xr - s$, and $h_1 = X^2 - Xr_1 - s_1$. Then

$$g \times \xi = X^2 - Xu\xi - v\xi^2$$

$$g \times h = X^2 + Xur - (u^2s + vr^2 + 4vs)$$

$$g \times h_1 = X^2 + Xur_1 - (u^2s_1 + vr_1^2 + 4vs_1).$$

Clearly $u\xi$, $ur \in B_1(\rho)$, $v\xi^2$ and $u^2s + r^2v + 4vs \in B_1(\rho^2)$. Hence $g \times \xi$, $g \times h \in B[X;\rho]_{(2)}$. If we set $\alpha = \xi$ and $\beta = 0$ then $u\xi = \alpha u + \beta + \rho(\beta)$ and $v\xi^2 = \alpha\rho(\alpha)v - \alpha\beta u - \beta^2$. Hence by Lemma 1.8, we obtain $g \times \xi \sim g$. Now, since $h \sim h_1$, by Lemma 1.8, there exist elements α, β in B such that

$$\alpha \in U(Z), \quad \beta \in B(\rho),$$

$$r = \alpha r_1 + \beta + \rho(\beta), \quad \text{and} \quad s = \alpha\rho(\alpha)s_1 - \alpha\beta r_1 - \beta^2$$

$$ur = u\alpha r_1 + u\beta + u\rho(\beta) = \alpha ur_1 + u\beta + \rho(u\beta), \quad u\beta \in B(\rho)$$

$$u^2s + vr^2 + 4vs = u^2(\alpha\rho(\alpha)s_1 - \alpha\beta r_1 - \beta^2) +$$

$$v(\alpha r_1 + \beta + \rho(\beta))^2 + 4v(\alpha\rho(\alpha)s_1 - \alpha\beta r_1 - \beta^2)$$

$$= \alpha\rho(\alpha)(u^2s_1 + vr_1^2 + 4vs_1) - \alpha(u\beta)ur_1 - (u\beta)^2.$$

This implies that $g \times h \sim g \times h_1$.

Lemma 1.10. Assume $\rho^2 = \theta_l^{-1}\theta_r$ for some $\theta \in U(B_1)$. Let g, g_1 and g_2 be elements of $B[X;\rho]_{(2)}$, and $g_1 \sim g_2$. Then

(i) $B(\rho^{2n}) = \theta^n Z$ for any integer n.

(ii) $g \times g_i \times \theta^{-1} \in Z[X;\bar{\rho}]_{(2)}$ $(i = 1, 2)$, $\bar{\rho}^2 = 1$, and $g \times g_1 \times \theta^{-1} \sim g \times g_2 \times \theta^{-1}$.

Proof. (i). If $u \in B(\rho^{2n})$ then, for any $c \in B$, $c(u\theta^{-n}) = u\theta^{2n}(c)\theta^{-n} = u\theta^{-n}c\theta^n\theta^{-n} = u\theta^{-n}c$, and hence $u\theta^{-n} \in Z$, that is, $u \in \theta^n Z$. Conversely, if $u \in \theta^n Z$ then $u = \theta^n z$ for some $u = \theta^n z$ for some $z \in Z$, and for any $c \in B$, $cu = c\theta^n z =$

$\theta^n\rho^{2n}(c)z = \theta^n z\rho^{2n}(c) = u\rho^{2n}(c)$, and whence $u \in B(\rho^{2n})$. This implies (i). (ii). Clearly $\rho^2|Z = 1$, and so, $\bar{\rho}^2 = 1$. Now, let $g = X^2 - Xu - v$ and $g_i = X^2 - Xu_i - v_i$ $(i = 1, 2)$. Then $g \times g_1 \times \theta^{-1} = X^2 - Xuu_1\theta^{-1} - (u^2v_1 + vu_1^2 + 4vv_1)\theta^{-2}$. Since $uu_1 \in B_1(\rho^2)$, we have $uu_1\theta^{-1} \in (\theta Z_1)\theta^{-1} = Z_1$ by (i). For any $\alpha \in Z$, $\alpha uu_1\theta^{-1} = u\rho(\alpha)u_1\theta^{-1} = uu_1\theta^{-1}\rho(\alpha)$. Hence we obtain $uu_1\theta^{-1} \in Z_1(\bar{\rho})$. Moreover, one will easily see that $(u^2v_1 + vu_1^2 + 4vv_1)\theta^{-2} \in B_1(\rho^4)\theta^{-2} = Z_1$. Therefore, it follows that $g \times g_1 \times \theta^{-1} \in Z[X;\bar{\rho}]_{(2)}$. Since $g_1 \sim g_2$, by Lemmas 1.8 and 1.7, there exist elements $\alpha, \beta \in B$ such that

$$\alpha \in U(Z),\ \beta \in B(\rho),$$

$$u_1 = \alpha u_2 + \beta + \rho(\beta),\ \text{and}\ v_1 = \alpha\rho(\alpha)v_2 - \alpha\beta u_2 - \beta^2,$$
$$uu_1\theta^{-1} = u(\alpha u_2 + \beta + \rho(\beta)\theta^{-1} = \alpha uu_2\theta^{-1} + 2\beta u\theta^{-1},\ \text{and}$$
$$\beta u\theta^{-1} \in Z_1(\bar{\rho}).$$

Next, we note

$$u^2v_1 + u_1^2v + 4vv_1 = u^2(\alpha\rho(\alpha)v_2 - \alpha\beta u_2 - \beta^2) + v(\alpha u_2 + \beta + \rho(\beta))^2 + 4v(\alpha\rho(\alpha)v_2 - \alpha\beta u_2 - \beta^2) = u^2\alpha\rho(\alpha)v_2 - u^2\alpha\beta u_2 - u^2\beta^2 + v(\alpha u_2\alpha u_2 + \beta\alpha u_2 + \rho(\beta)\alpha u_2 + \alpha u_2\beta + \beta^2 + \rho(\beta)\beta + \alpha u_2\rho(\beta) + \beta\rho(\beta) + \rho(\beta)\rho(\beta)) + v(4\alpha\rho(\alpha)v_2 - 4\alpha\beta u_2 - 4\beta^2).$$

Then, by Lemmas 1.7 and 1.8, we obtain

$$(u^2v_1 + vu_1^2 + 4vv_1)\theta^{-2} = \alpha\rho(\alpha)(u^2v_2 + vu_2^2 + 4vv_2)\theta^{-2} - \alpha(\beta u\theta^{-1})(uu_2\theta^{-1}) - (\beta u\theta^{-1})^2.$$

This implies that $g \times g_1 \times \theta^{-1} \sim g \times g_2 \times \theta^{-1}$, completing the proof.

<u>Lemma 1.11</u>. Assume that there is a Galois polynomial f in $B[X;\rho]_{(2)}$. Then $\rho^2 = \delta(f)_l^{-1}\delta(f)_r$, and $\delta(f) \in U(B_1)$.

Moreover, if $\rho^2 = \theta_l^{-1}\theta_r$ for some $\theta \in U(B_1)$ then, for any $g \in B[X;\rho]_{(2)}$,

$$g \times f \times f \times \theta^{-1} \sim g.$$

Proof. Let $f = X^2 - Xa - b$. Then, by Th.1.5, $\delta(f)$ is inversible in B, and $\delta(f) \in B_1(\rho^2)$. From this, one will easily see that $\rho^2 = \delta(f)_l^{-1}\delta(f)_r$. Now, let $\rho^2 = \theta_l^{-1}\theta_r$ for some $\theta \in U(B_1)$, and let $g = X^2 - xu - v$ be an arbitrary element of $B[X;\rho]_{(2)}$. Then, by Lemma 1.10(i), we have $\delta(f) = \theta z$ for some $z \in U(Z_1)$. Hence, by Lemma 1.9, we obtain $g \times f \times f \times \theta^{-1} \sim g \times f \times f \times \theta^{-1} \times z^{-1} = g \times f \times f \times \delta(f)^{-1}$. Hence it suffices to prove that

$$g \sim f \times f \times g \times \delta(g)^{-1}.$$

Now, we set $\delta = \delta(f)$ ($= a^2 + 4b$). Then,

$((f \times f) \times g) \times \delta^{-1} = X^2 - Xa^2u\delta^{-1} - (a^4b + (2a^2b + 4b^2)u^2 + 4(2a^2b + 4b^2)v)\delta^{-2} = X^2 - Xa^2u\delta^{-1} - ((a^2 + 4b)^2 + 2(a^2 + 4b)bu^2 - 4b^2u^2)\delta^{-2} = X^2 - Xa^2\delta^{-1} - (v - (-2bu\delta^{-1})u - (-2bu\delta^{-1})^2)$.

Moreover, since $a^2\delta^{-1} + 4b\delta^{-1} = 1$, we have

$$a^2u\delta^{-1} = u + 2(-2bu\delta^{-1}), \text{ and } -2bu\delta^{-1} \in B_1(\rho).$$

This implies $f \times f \times g \times \delta^{-1} \sim g$.

Corollary 1.12. The set $Z[X;\bar{\rho}]^{\sim}_{(2)}$ forms an abelian semigroup under the composition $\langle h\rangle\langle k\rangle = \langle h \times k\rangle$. If there is a Galois polynomial e in $Z[X;\bar{\rho}]_{(2)}$ then $\bar{\rho}^2 = 1$ and $Z[X;\bar{\rho}]^{\sim}_{(2)}$ has the identity element $\langle e \times e\rangle$.

Proof. If $h \sim h'$ and $k \sim k'$ in $Z[X;\bar{\rho}]_{(2)}$ then, by Lemma 1.9, $h \times k \sim h' \times k \sim h' \times k'$. Hence the composition

$\langle h\rangle\langle k\rangle$ is well defined. Moreover, this composition is associative and commutative. Hence this makes $Z[X;\bar{\rho}]^{\sim}_{(2)}$ into an abelian semigroup. Now, let e be a Galois polynomial in $Z[X;\bar{\rho}]_{(2)}$. Then, by virtue of Lemma 1.11, we have that $\bar{\rho}^2 = \delta(e)_l^{-1}\delta(e)_r = 1$, and for any $h \in Z[X;\bar{\rho}]_{(2)}$,

$$\langle h\rangle\langle e \times e\rangle = \langle h \times e \times e\rangle = \langle h \times e \times e \times 1^{-1}\rangle = \langle h\rangle.$$

Hence $\langle e \times e\rangle$ is the identity element of $B[X;\bar{\rho}]^{\sim}_{(2)}$.

Corollary 1.13. Assume $\rho^2 = \theta_l^{-1}\theta_r$ for some $\theta \in U(B_1)$, and let g be an element of $B[X;\rho]_{(2)}$. Then, the set $B[X;\rho]^{\sim}_{(2)}$ forms an abelian semigroup under the composition $\langle g_1\rangle\langle g_2\rangle = \langle g_1 \times g_2 \times g \times \theta^{-1}\rangle$.

Proof. Let $g_1 \sim g_1'$ and $g_2 \sim g_2'$ in $B[X;\rho]_{(2)}$. Then, by Lemma 1.10, we have $g_i \times g \times \theta^{-1}$, $g_i' \times g \times \theta^{-1} \in Z[X;\bar{\rho}]_{(2)}$, and $g_i \times g \times \theta^{-1} \sim g_i' \times g \times \theta^{-1}$ $(i = 1, 2)$. Hence by Lemma 1.9, we obtain

$$g_1 \times g_2 \times g \times \theta^{-1} = g_1 \times (g_2 \times g \times \theta^{-1}) \sim g_1 \times (g_2' \times g \times \theta^{-1}) =$$
$$g_2' \times (g_1 \times g \times \theta^{-1}) \sim g_2' \times (g_1' \times g \times \theta^{-1}) = g_1' \times g_2' \times g \times \theta^{-1}.$$

Hence the composition $\langle g_1\rangle\langle g_2\rangle$ is well defined. Moreover, this composition is associative and commutative. This completes the proof.

Now, we shall conclude this section with the following theorem which is one of our main results.

Theorem 1.14. Assume that there is a Galois polynomial f in $B[X;\rho]_{(2)}$. Then the set $B[X;\rho]^{\sim}_{(2)}$ forms an abelian semigroup under the composition $<g_1><g_2> = <g_1 \times g_2 \times f \times \delta(f)^{-1}>$ with the identity element $<f>$, and the subset $\{<g> \in B[X;\rho]^{\sim}_{(2)} \mid g$ is separable over $B\}$ coincides with the set of all inversible elements in the semigroup $B[X;\rho]^{\sim}_{(2)}$ which is a group of exponent 2. Moreover, the polynomial $f \times f \times \delta(f)^{-1}$ in $Z[X;\bar{\rho}]_{(2)}$ is Galois, and the semigroups $B[X;\rho]^{\sim}_{(2)}$ and $Z[X;\bar{\rho}]^{\sim}_{(2)}$ are isomorphic under the mapping $<g> \to <g \times f \times \delta(f)^{-1}>$.

Proof. By Lemma 1.11 and Cor.1.13, $B[X;\rho]^{\sim}_{(2)}$ forms an abelian semigroup under the composition

$$<g_1><g_2> = <g_1 \times g_2 \times f \times \delta(f)^{-1}>.$$

Now, let g be a separable polynomial in $B[X;\rho]_{(2)}$. Then, by Th.1.6, g is Galois over B. Hence, by Lemma 1.11, we have

$$g_1 \times g \times g \times \delta(f)^{-1} \sim g_1$$

for any $g_1 \in B[X;\rho]_{(2)}$, and in particular

$$g_1 \times f \times f \times \delta(f)^{-1} \sim g_1$$

$$g \times g \times f \times \delta(f)^{-1} = f \times g \times g \times \delta(f)^{-1} \sim f.$$

Thus, we obtain $<g_1><f> = <g_1>$, and $<g><g> = <f>$. Therefore, it follows that $<f>$ is the identity element of $B[X;\rho]^{\sim}_{(2)}$ and $<g>$ is an inversible element of $B[X;\rho]^{\sim}_{(2)}$ which is of order 2. Conversely, let $<g>$ be an inversible element of $B[X;\rho]^{\sim}_{(2)}$. Then $<g><h> = <f>$ for some $h \in B[X;\rho]_{(2)}$ and

$$g \times h \times f \times \delta(f)^{-1} \sim f$$

which are Galois over B. This shows that

$$\delta(g \times h \times f \times \delta(f)^{-1}) = \delta(g)\delta(h)\delta(f)\delta(f)^{-2}$$

is inversible in B by Lemma 1.5, and so is $\delta(g)$. Hence g is Galois over B. Thus, g is separable over B. Next, by Lemmas 1.9, 1.10 and 1.11, we have the mappings

$$\phi_f : B[X;\rho]_{(2)} \to Z[X;\bar\rho]_{(2)};\quad \phi_f(<g>) = <g \times f \times \delta(f)^{-1}>$$

$$\psi_f ; Z[X;\bar\rho]_{(2)} \to B[X;\rho]_{(2)};\quad \psi_f(<h>) = <h \times f>.$$

Then, by Lemma 1.11, we see

$$\psi_f\phi_f(<g>) = <g \times f \times \delta(f)^{-1} \times f> = <g>.$$

Since $\delta(f \times f \times \delta(f)^{-1}) = \delta(f)\delta(f)\delta(f)^{-2} = 1$, by Th.1.5, $f \times f \times \delta(f)^{-1}$ is a Galois polynomial in $Z[X;\bar\rho]_{(2)}$. Hence by Lemma 1.11 and Cor.1.12, we have

$$\begin{aligned}\phi_f\psi_f(<h>) &= <(h \times f) \times f \times \delta(f)^{-1}>\\ &= <(h \times f) \times (f \times f \times f \times \delta(f)^{-1}) \times \delta(f)^{-1}>\\ &= <h \times (f \times f \times \delta(f)^{-1}) \times (f \times f \times \delta(f)^{-1})> = <h>.\end{aligned}$$

Thus, ϕ_f is bijective. Moreover, we have

$$\begin{aligned}\phi_f(<g_1><g_2>) &= <g_1 \times g_2 \times f \times \delta(f)^{-1} \times f \times \delta(f)^{-1}>\\ &= <(g_1 \times f \times \delta(f)^{-1}) \times (g_2 \times f \times \delta(f)^{-1})>\\ &= \phi_f(<g_1>)\phi_f(<g_2>).\end{aligned}$$

Therefore, it follows that ϕ_f is an isomorphism of the semigroup $B[X;\rho]^{\sim}_{(2)}$ onto the semigroup $Z[X;\bar\rho]^{\sim}_{(2)}$, completing the proof.

2. <u>On</u> $B[X;\rho]_{(n*)}$. In this section, we assume that $\rho^n = u_l^{-1}u_r$ for some $u \in U(B_1)$, $n \in U(Z_1)$, and $U(Z_1)$ contains an element ζ so that $\zeta^n = 1$ and $1 - \zeta^i \in U(Z_1)$ $(i = 1, \ldots, n - 1)$. Moreover, G will mean a cyclic group of order n with a generator σ. As to notations, we use the following conventions: $LN_\rho(b;\, n) = \rho^{n-1}(b)\rho^{n-2}(b) \ldots \rho(b)b$ $(b \in B)$, and $LN_\rho(B;\, n) = \{LN_\rho(b;\, n) \mid b \in B\}$.

As is easily seen, if $X^n - b \in B[X;\rho]_{(n*)}$ then $b \in B_1(\rho^n)$, and conversely. Hence $B[X;\rho]_{(n*)} = \{X^n - b \mid b \in B_1(\rho^n)\}$.

For future reference, we put

$$\Omega_\rho(B) = \{B[X;\rho]/(X^n - b)B[X;\rho] \mid b \in B_1(\rho^n)\},$$

$$A = A_b \quad \text{and} \quad X + (X^n - b)B[X;\rho] = x_b$$

for each $A = B[X;\rho]/(X^n - b)B[X;\rho] \in \Omega_\rho(B)$.

Noting that $x_b^n = b \in B$. A_b can be regarded as a BG-module via $\sigma(\sum_{i=o}^{n-1} x_b^i b_i) = \sum_{i=o}^{n-1} (x_b\zeta)^i b_i$. In all that follows, we understand each $A_b \in \Omega_\rho(B)$ as a BG-module in the sense above. Given $A \in \Omega_\rho(B)$, the BG-ring isomorphism classes of A in $\Omega_\rho(B)$ will be denoted by $\langle A\rangle$, and we set $P_\rho(B) = \{\langle A\rangle \mid A \in \Omega_\rho(B)\}$.

Now, we shall begin our study with the following

Lemma 2.1. If A_b, $A_c \in \Omega_\rho(B)$, then the following are equivalent:

(1) $\langle A_b\rangle = \langle A_c\rangle$.

(2) There exists a B-ring isomorphism ϕ of A_b into A_c such that $\phi(x_b) = X_c\alpha$ for some $\alpha \in U(Z)$.

(3) $b = cLN_\rho(\beta;\ n)$ for some $\beta \in U(Z)$.

Proof. (1) $\rightarrow$ (2). Let ϕ be a BG-ring isomorphism of A_b into A_c, and $\phi(x_b) = \sum_{i=o}^{n-1} x_c^i b_i$ $(b_i \in B)$. Then $\sum_{i=o}^{n-1} x_c^i \zeta b_i = \phi\sigma(x_b) = \alpha\phi(x_b) = \sum_{i=o}^{n-1} (x_c^i\zeta)^i b_i$ implies $\phi(x_b) = x_c b_1$. Noting that $x_c\rho(d)b_1 = d(x_c b_1) = d\phi(x_b) = \phi(dx_b) = \phi(x_b\rho(d)) = x_c b_1\rho(d)$ and $\phi^{-1}(x_c) = x_b b_1'$ with some $b_1' \in B$, we can easily see $b_1 \in U(Z)$.

(2) $\rightarrow$ (3). This is obvious by $b = (x_b)^n = \phi(x_b^n) = (x_c\alpha)^n = x_c^n LN_\rho(\alpha;\ n) = cLN_\rho(\alpha;\ n)$.

(3) $\rightarrow$ (1). Let ϕ be the mapping of A_b into A_c defined

by $\sum_{i=o}^{n-1} x_b^i b_i \to \sum_{i=o}^{n-1} (x_c\beta)^i b_i$. Then $\phi(b) = \phi(x_b^n) = (x_c\beta)^n = cLN_\rho(\beta; n) = b$ and ϕ is a B-ring isomorphism. Moreover, $\sigma\phi(x_b) = \sigma(x_c\beta) = x_c\zeta\alpha = \phi\sigma(x_b)$ shows that ϕ is a BG-ring isomorphism.

Remark. If $n = 2$, then $<A_b> = <A_c>$ if and only if A_b and A_c are B-ring isomorphic. For if ϕ is a B-ring isomorphism of A_b into A_c and $\phi(x_b) = x_c\alpha + \beta$ for some $\alpha, \beta \in B$, then $x_c\rho(\gamma)\alpha + \gamma\beta = \gamma(x_c\alpha + \beta) = \gamma\phi(x_b) = \phi(\gamma x_b) = \phi(x_b\rho(\gamma)) = x_c\alpha\rho(\gamma) + \beta\rho(\gamma)$ for each $\gamma \in B$ show that $\alpha \in U(Z)$ and $\gamma\beta = \beta\rho(\gamma)$. Hence $\beta^2 = \beta\rho(\beta)$. On the other hand, $b = \phi(x_b^2) = \phi(x_c\alpha + \beta)^2 = x_c^2 LN_\rho(\alpha; 2) + x_c(\alpha(\beta + \rho(\beta)) + \beta^2$ yields that $\beta + \rho(\beta) = 0$, and hence, $0 = \beta^2 + \beta\rho(\beta) = 2\beta^2$. Consequently, we have $\beta^2 = 0$. Therefore, the map ϕ' of A_b into A_c defined by $\phi'(x_b) = x_c\alpha$ is a B-ring isomorphism.

Let b be an element of $B_1(\rho^n)$. Then $cb = b\rho^n(c) = bu^{-1}cu$ for all $c \in B$ show that $bu^{-1} \in Z \cap B_1 = Z_1$. Since $uZ_1 \subset B_1(\rho^n)$ is obvious, we have the following

Lemma 2.2. $B_1(\rho^n)$ coincides with uZ_1.

Now, we are ready to prove the following

Theorem 2.3. (1) $P_\rho(B)$ is an abelian semigroup with the identity element $<A_u>$ under the composition $*$ defined by $<A_b>*<A_c> = <A_{bcu^{-1}}>$. Moreover, $<A_b>$ is an element of

$U(P_\rho(B))$ is and only if $b \in U(B)$.

(2) $P_\rho(B)$ is isomorphic to the factor semigroup $Z_1/LN_\rho(U(Z);\ n)$. In particular, $U(P_\rho(B))$ is isomorphic to $U(Z_1)/LN_\rho(U(Z);\ n)$.

Proof. (1) Since $\langle A_b\rangle = \langle A_c\rangle$ if and only if $b = cLN_\rho(\alpha;\ n)$ with some $\alpha \in U(Z)$ (Lemma 2.1), the assertion is evident by Lemma 2.2.

(2) By Lemma 2.2, the mapping $F\colon z \to \langle A_{uz}\rangle$ $(z \in Z_1)$ is a semigroup epimorphism of Z_1 onto $P_\rho(B)$. Then $Z_1/LN_\rho(U(Z);\ n)$ is isomorphic to $P_\rho(B)$ by Lemma 2.1, and the rest is obvious.

Proposition 2.4. If $A_b \in \Omega_\rho(B)$ then the following are equivalent:

(1) A_b is a separable extension.

(2) A_b/B is a strongly G-cyclic extension.

(3) b is inversible in B.

Proof. Since (2) → (1) is known and (3) → (2) is evident by $\sigma(x_b) = x_b\zeta$ (see [1]), it remains only to prove (1) → (3). Now, we assume (1). Write here $A = A_b$ and $x = x_b$. Then, the (left)A-(right)A-homomorphism $\phi : A \otimes_B A \to A$ $(a \otimes b \to ab)$ splits. Hence there exists an element e in $A \otimes_B A$ such that $\phi(e) = 1$ and $(c \otimes 1)e = e(1 \otimes c)$ for every $c \in A$. We may write

$$e = \sum_{i,j=o}^{n-1}(x^i \otimes x^j)(1 \otimes b_{ij}).$$

Then, we have

(1) $1 = \sum_{i,j=o}^{n-1} x^{i+j}b_{ij} = b_{oo} + \sum_{i+j=n} x^{i+j}b_{ij} + \sum_{i+j\neq o,n} x^{i+j}b_{ij}$

$$= b_{oo} + b\sum_{i+j=n} b_{ij}, \text{ and}$$

(2) $\sum_{i,j=o}^{n-1}(x^{i+j}\otimes x^j)(1\otimes b_{ij}) = (x\otimes 1)(\sum_{i,j=o}^{n-1}(x^i\otimes x^j)(1\otimes b_{ij}))$
$= (\sum_{i,j=o}^{n-1}(x^i\otimes x^j)(1\otimes b_{ij}))(1\otimes x) = \sum_{i,j=o}^{n-1}(x^i\otimes x^{j+1})(1\otimes\rho(b_{ij}))$.

Comparing the coefficients of $x\otimes 1$ in (2), we obtain $b_{oo} = b\rho(b_{1,n-1})$. Hence, it follows from (1) that $1 = bc = \rho^{-n}(c)b$, where $c = \sum_{i+j=n} b_{ij} + \rho(b_{1,n-1})$. Thus b is inversible in B. This completes the proof.

Now, let A/B be a strongly G-cyclic extension with $A_B \oplus\!> B_B$. Then, A is BG-ring isomorphic to $A_b \in \Omega_{\rho'}(B)$ for some automorphism ρ' and $b \in U(B)$ ([1]). Thus, if A/B is a strongly G-cyclic extension of ρ-automorphism type and $A_B \oplus\!> B_B$, then A is BG-ring isomorphic to some A_b with $\langle A_b\rangle \in U(P_\rho(B))$. Conversely, if $\langle A_b\rangle$ is in $U(P_\rho(B))$, then Th.2.3 and Prop.2.4 show that C/B is a strongly G-cyclic extension of ρ-automorphism type for any $C \in \langle A_b\rangle$. Summarizing those above, we obtain the following

<u>Corollary 2.5</u>. $U(P_\rho(B)) = \{\langle A\rangle \in P_\rho(B) \mid A/B \text{ is separable}\}$ represents the set of all BG-ring isomorphism classes of strongly G-cyclic extensions A of ρ-automorphism type with $A_B \oplus\!> B_B$.

The next is also an easy consequence of Th.2.3.

<u>Corollary 2.6</u>. If the restriction $\rho|Z$ of ρ to Z coincides with the identity then $P_\rho(B) \cong Z/U(Z)^n \cong P_1(B) \cong P_1(Z)$. In particular, (1) if ρ is inner then $P_\rho(B) \cong P_1(B)$, and (2) if B is commutative then $P_1(B) \cong B/U(B)^n$ (see [7]).

Remark. Let D be a derivation of B so that D(a + b) = D(a) + D(b) and D(ab) = D(a)b + aD(b) (a, b ∈ B). Then, we have a skew polynomial ring B[X;D] whose multiplication is defined by bX = Xb + D(b) for each b ∈ B. As to the polynomials in B[X;D], we have some studies [2, §3], [3, §2] and [5, §3] whose results are similar to that of this paper. However, this is somewhat complicated. Hence, the present paper was devoted only to study the polynomials in B[X;ρ].

References

[1] K. Kishimoto: On abelian extensions of rings II, Math. J. Okayama Univ., 15 (1971), 57-70.

[2] K. Kishimoto: A classification of free quadratic extensions of rings, Math. J. Okayama Univ. 18 (1976), 139-148.

[3] K. Kishimoto: A classification of free extensions of rings of automorphism type and derivation type, Math. J. Okayama Univ. 19 (1977), 163-169.

[4] Y. Miyashita: Finite outer Galois theory of non-commutative rings, Jour. Fac. Sci. Hokkaido Univ., Ser. I, 19 (1966), 114-134.

[5] T. Nagahara: On separable polynomials of degree 2 in skew polynomial rings, Math. J. Okayama Univ. 19 (1976), 65-95.

[6] T. Nagahara: Supplements to the previous paper "On separable polynomials of degree 2 in skew polynomial rings", Math. J. Okayama Univ. 19 (1977), 159-161.

[7] A. Nakajima: On a group of cyclic extensions over commutative rings, Math. J. Okayama Univ. 15 (1972), 163-172.

NOTE ON HERMITIAN FORMS OVER A NON COMMUTATIVE RING

Teruo KANZAKI
Osaka Women's University
and
Kazuo KITAMURA
Osaka University of Education

An aim of these notes is to give a characterization of a hermitian form over a non commutative ring by a matrix which is a generalization of a well known and basic fact over a field. We suppose that A is a non commutative ring with identity, and has an involution $A \to A$; $a \rightsquigarrow \bar{a}$ which satisfies $\overline{a+b} = \bar{a}+\bar{b}$, $\overline{ab} = \bar{b}\bar{a}$ and $\bar{\bar{a}} = a$ for all $a, b \in A$.

1. Hermitian left A-module (M,h,U). Let U be an A-bimodule. If U has an involution $U \to U$; $x \rightsquigarrow \bar{x}$ which is an additive homomorphism satisfying $\bar{\bar{x}} = x$ and $\overline{axb} = \bar{b}\bar{x}\bar{a}$ for every $x \in U$ and $a, b \in A$, then U is called an A-bimodule with involution. For an A-bimodule U with involution and a left A-module M, a map $h : M \times M \to U$ is called a hermitian form of M to U, if h satisfies $h(m+m',n) = h(m,n) + h(m',n)$, $h(am,bn) = ah(m,n)\bar{b}$ and $h(m,n) = \overline{h(n,m)}$ for all m, m' and n in M, and $a, b \in A$. We call (M,h,U) a hermitian left A-module. If $U = A$, we denote (M,h,A) by (M,h). If a map $\theta : M \to \mathrm{Hom}_A(M,U)$; $m \rightsquigarrow h(-,m)$ is bijective, then (M,h,U) is called non-degenerate. Suppose that I is

a finite or infinite set of indices. By U^I (resp. $U^{(I)}$), we denote the set of I-row vectors $(x_i)_{i\in I}$ with i-th component x_i in U for $i \in I$ (resp. the set of I-row vectors $(x_i)_{i\in I}$ with i-th component $x_i \in U$ and $x_i = 0$ for almost all $i \in I$). As usual, U^I and $U^{(I)}$ are a left A-module and its A-submodule. By ${}^tU^I$ (resp. ${}^tU^{(I)}$), we denote the set of I-column vectors ${}^t(x_i)_{i\in I}$ which are transposes of $(x_i)_{i\in I}$ in U^I (resp. in $U^{(I)}$). Then we regard ${}^tU^I$ and ${}^tU^{(I)}$ as a right A-module and its A-submodule. Especially, $A^{(I)}$ is a free left A-module and ${}^tA^{(I)}$ a free right A-module. By $H = (h_{ij})_{(i,j)\in I\times I}$ we denote an $I\times I$-matrix with (i,j)-component h_{ij} in U, and by $H^* = {}^t(\bar{h}_{ij})_{(i,j)\in I\times I}$ an $I\times I$-matrix with (i,j)-component $\bar{h}_{ji}$. If an $I\times I$-matrix H satisfies $H = H^*$, H is called a <u>hermitian matrix</u>. For a given hermitian $I\times I$-matrix H, we put $A^{(I)}H = \{(a_i)_{i\in I}H = (\sum_{i\in I} a_ih_{ij})_{j\in I} \in U^I;\ (a_i)_{i\in I} \in A^{(I)}\}$, and $h_H : A^{(I)}H \times A^{(I)}H \to U;\ ((a_i)_{i\in I}H, (b_i)_{i\in I}H) \rightsquigarrow \sum_{i,j\in I} a_ih_{ij}\bar{b}_j$. Then $A^{(I)}H$ is a left A-submodule of U^I, and h_H defines a hermitian form of $A^{(I)}H$ to U, since $\sum_{i,j\in I} a_ih_{ij}\bar{b}_j = ((a_i)_{i\in I}H)((b_i)_{i\in I})^* = (a_i)_{i\in I}((b_i)_{i\in I}H)^*$. By <H>, we denote the hermitian left A-module $(A^{(I)}H, h_H, U)$. If (M,h,U) is any hermitian left A-module and M has a generator $\{m_i\}_{i\in I}$, i.e. $M = \sum_{i\in I} Am_i$, then $H = (h(m_i,m_j))_{(i,j)\in I\times I}$ is a hermitian $I\times I$-matrix. We consider a map $\xi_M : M = \sum_{i\in I} Am_i \to A^{(I)}H;\ x = \sum_{i\in I} a_im_i \rightsquigarrow (h(x,m_i))_{i\in I} = (a_i)_{i\in I}H$. The map ξ_M is an epimorphism and defines a homomorphism of hermitian left A-modules (M,h,U) to <H>, i.e. the following diagram is made to commute;

$$\begin{array}{ccc} M \times M & \xrightarrow{\xi_M \times \xi_M} & A^{(I)}H \times A^{(I)}H \\ & {}_{h}\searrow \quad \swarrow_{h_H} & \\ & U & \end{array}$$

We denote such a homomorphism ξ_M by $\xi_M : (M,h,U) \to \langle H\rangle$. For a left A-module $M = \sum_{i\in I} Am_i$, we put $\mathrm{Ann}(A^{(I)};\{m_i\}_{i\in I}) = \{(a_i)_{i\in I} \in A^{(I)};\ \sum_{i\in I} a_i m_i = 0\}$ and $\mathrm{Ann}({}^tU^I;\ \mathrm{Ann}(A^{(I)};\{m_i\}_{i\in I})) = \{{}^t(x_i)_{i\in I} \in {}^tU^I;\ \sum_{i\in I} a_i x_i = 0$ for all $(a_i)_{i\in I} \in \mathrm{Ann}(A^{(I)};\{m_i\}_{i\in I})\}$. Then we have an A-isomorphism ϕ: $\mathrm{Hom}_A(M,U) \to \mathrm{Ann}({}^tU^I;\mathrm{Ann}(A^{(I)};\{m_i\}_{i\in I}))$; $f \mapsto (f(m_i))_{i\in I}$. For an $I\times I$-matrix H with components in U, we put $\mathrm{Ann}(A^{(I)};H) = \{(a_i)_{i\in I} \in A^{(I)};\ (a_i)_{i\in I}H = 0\}$.

The following lemma is easy.

<u>Lemma 1</u>. Let (M,h,U) be a hermitian left A-module, $M = \sum_{i\in I} Am_i$ and $H = (h(m_i,m_j))_{(i,j)\in I\times I}$. The following conditions are equivalent:

1) $\theta : M \to \mathrm{Hom}_A(M,U)$; $m \mapsto h(-,m)$ is injective.

2) $\mathrm{Ann}(A^{(I)};\{m_i\}_{i\in I}) = \mathrm{Ann}(A^{(I)};H)$.

3) $\xi_M : (M,h,U) \to \langle H\rangle$ is an isomorphism.

<u>Theorem 1</u>. Let (M,h,U) be a hermitian left A-module, $M = \sum_{i\in I} Am_i$ and $H = (h(m_i,m_j))_{(i,j)\in I\times I}$. Then (M,h,U) is non-degenerate if and only if $\xi_M : (M,h,U) \to \langle H\rangle$ is an isomorphism and $\mathrm{Ann}({}^tU^I;\ \mathrm{Ann}(A^{(I)};H)) = H\,{}^tA^{(I)}$.

<u>Proof</u>. Using the isomorphism $\phi : \mathrm{Hom}_A(M,U) \to \mathrm{Ann}({}^tU^I;\mathrm{Ann}(A^{(I)};\{m_i\}_{i\in I}))$, we get that $\theta : M \to \mathrm{Hom}_A(M,U)$; $m \mapsto h(-,m)$

is surjective if and only if $\mathrm{Ann}({}^{t}U^{I};\ \mathrm{Ann}(A^{(I)};\{m_i\}_{i\in I}) \subset H\,{}^{t}A^{(I)}$. By Lemma 1, θ is an isomorphism if and only if ξ_M is an isomorphism and $\mathrm{Ann}({}^{t}U^{I};\ \mathrm{Ann}(A^{(I)};H)) \subset H\,{}^{t}A^{(I)}$.

2. <u>The case $U = A$.</u>

<u>Theorem 2</u>. Assume that (M,h) is a non-degenerate hermitian left A-module, $M = \sum_{i\in I} Am_i$ and $H = (h(m_i,m_j))_{(i,j)\in I\times I}$. Then M is A-projective if and only if there is a column finite $I\times I$-matrix K (i.e. all the columns of K are contained in ${}^{t}A^{(I)}$) such that HK is a row finite matrix (i.e. all the rows of HK are contained in $A^{(I)}$) and $(HK)H = H$.

<u>Proof</u>. Under the assumption of (M,h), we suppose that M is A-projective. By the isomorphism ξ_M, $A^{(I)}H$ is A-projective, and an A-epimorphism $\mu_H : A^{(I)} \to A^{(I)}H;\ (a_i)_{i\in I} \mapsto (a_i)_{i\in I}H$ is split. Hence there is an A-homomorphism $\nu : A^{(I)}H \to A^{(I)}$ such that $\xi_H \circ \nu = I$. Taking a j-projection $p_j : A^{(I)} \to A;\ (a_i)_{i\in I} \mapsto a_j;\ (j \in I)$, we consider a composition $p_j\circ\nu\circ\xi_M$ which is contained in $\mathrm{Hom}_A(M,A)$. By the isomorphism $\phi : \mathrm{Hom}_A(M,A) \to \mathrm{Ann}({}^{t}A^{I}:\ \mathrm{Ann}(A^{(I)};\{m_i\}_{i\in I})) = \mathrm{Ann}({}^{t}A^{I};\ \mathrm{Ann}(A^{(I)};H)) = H\,{}^{t}A^{(I)}$, we get $\phi(p_j\circ\nu\circ\xi_M) = {}^{t}(p_j\circ\nu\circ\xi_M(m_i))_{i\in I}\ H\,{}^{t}(a_{ij})_{i\in I}$ for some ${}^{t}(a_{ij})_{i\in I} \in {}^{t}A^{(I)}$. If we put $K = (a_{ij})_{(i,j)\in I\times I}$, then K is a column finite $I\times I$-matrix. Since the i-th row of HK is $(p_j\circ\nu\circ\xi_M(m_i))_{j\in I} = \nu(\xi_M(m_i))$ and is contained in $A^{(I)}$ for each $i \in I$, the matrix $HK = (p_j\circ\nu\circ\xi_M(m_i))_{(i,j)\in I\times I}$ is row finite. Since $\mu_H\circ\nu = I$ and

the i-th row of H is $(h(m_i,m_j))_{j\in I} = \xi_M(m_i) = \mu_H(\nu\circ\xi_M(m_i)) = (p_j\circ\nu\circ\ {}_M(m_i))_{j\in I}H$, we get $H = (HK)H$. The converse is easy from the fact that an A-homomorphism $\nu : A^{(I)}H \to A^{(I)}$; $(a_i)_{i\in I}H \mapsto (a_i)_{i\in I}(HK) = ((a_i)_{i\in I}H)K$ satisfies $\mu_H\circ\nu = I$, i.e. $\mu_H : A^{(I)} \to A^{(I)}H$ is split.

<u>Theorem 3</u>. Assume that (M,h) is a hermitian left A-module such that M is finitely generated over A, and put $M = \sum_{i=1}^{n} Am_i$ and $H = (h(m_i m_j))_{(i,j)\in I\times I}$, where $I = \{1, 2, \ldots, n\}$. Then (M,h) is both non-degenerate and A-projective if and only if $\xi_M : (M,h) \to \langle H\rangle$ is an isomorphism and H is a von Neumann regular element in the matrix ring A_n of degree n, i.e. there is K in A_n such that $HKH = H$.

<u>Proof</u>. If (M,h) is both non-degenerate and A-projective, then by Theorems 1 and 2, ξ_M is an isomorphism and there is K in A_n such that $HKH = H$. Conversely, suppose that there is $K \in A_n$ such that $HKH = H$. We denote the unit matrix in A_n by E. Then we have $(HK - E)H = 0$, and so all the rows of $(HK - E)$ are contained in $\mathrm{Ann}(A^n;H)$. Hence every element x in $\mathrm{Ann}({}^tA^n;\ \mathrm{Ann}(A^n;H))$ satisfies $(HK - E)x = 0$, and so $x = H(Kx)$ is contained in $H\,{}^tA^n$. Therefore, we get $\mathrm{Ann}({}^tA^n;\ \mathrm{Ann}(A^n;H)) = H\,{}^tA^n$. Since ξ_M is an isomorphism, it follows that (M,h) is non-degenerate from Theorem 1 and is A-projective from Theorem 2.

<u>Corollary 1</u>. Let H be a hermitian matrix in A_n. Then $\langle H\rangle$ is both non-degenerate and A-projective if and only if

H is a von Neumann regular element in A_n.

3. A-submodule of (M,h).

Theorem 4. Let (M,h) be a hermitian left A-module. Suppose that $X = \sum_{i=1}^{n} Ax_i$ is an A-submodule of M such that the $n\times n$-matrix $H = (h(x_i,x_j))$ is a von Neumann regular element in A_n. Then there is an A-submodule X' of X which satisfies the following conditions;

1) (X',h) is both non-degenerate and A-projective,

2) $X' = \sum_{i=1}^{n} Ax_i'$ and $H = (h(x_i,x_j)) = (h(x_i',x_j'))$,

3) $X = X' \oplus X''$, where (X'',h) is totally isotropic and $X'' = X^{\perp} \cap X$.

Proof. Since H is a von Neumann regular element in A_n, $\langle H\rangle$ is both non-degenerate and A-projective, and so an A-epimorphism $\xi_X : X \to A^nH;\ x = \sum_{i=1}^{n} a_ix_i \rightsquigarrow (a_1,\dots,a_n)H = (h(x,x_1),\dots,h(x,x_n))$ is split. Namely, there are A-submodules X' and X'' of X such that $X = X' \oplus X''$ and $X'' = \operatorname{Ker}\xi_X$. Put $x_i = x_i' + x_i''$ for $x_i' \in X'$ and $x_i'' \in X''$, $i = 1, 2, \dots, n$. Then it follows that $X' = \sum_{i=1}^{n} Ax_i'$, $X'' = \sum_{i=1}^{n} Ax_i'' = X^{\perp} \cap X$ and $h(x_i,x_j) = h(x_i',x_j')$ for $i, j = 1, 2, \dots, n$. Furthermore, $\xi_X|_{X'} = \xi_{X'} : X' \to A^nH$ is an isomorphism, and so (X',h) ($\cong \langle H\rangle$) is both non-degenerate and A-projective.

Theorem 5. Let (M,h) be a hermitian left A-module. Suppose that $X = \sum_{i=1}^{n} Ax_i$ is a totally isotropic A-submodule of M and there is an A-submodule $Y = \sum_{i=1}^{n} Ay_i$ of M such that an $n \times n$-matrix $L = (h(x_i, y_j))$ with the (i,j)-component $h(x_i, y_j)$ is a von Neumann regular element in A_n. Then there are A-submodules $X' = \sum_{i=1}^{n} Ax_i' \subset X$ and $Y' = \sum_{i=1}^{n} Ay_i' \subset Y$ such that $L = (h(x_i', y_j'))$ and $X = X' \oplus (X + Y)^{\perp} \cap X$, and $(X' + Y', h)$ becomes a metabolic left A-module which is both non-degenerate and A-projective.

<u>Proof.</u> If L is a von Neumann regular element in A_n, i.e. there is $K \in A_n$ satisfying $HKH = H$, then A^nL is A-projective. Because, a map $\mu_L : A^n \to A^nL$; $(a_1, \ldots, a_n) \rightsquigarrow (a_1, \ldots, a_n)L$ is split by a map $\mu_K : A^nL \to A^n$; $(a_1, \ldots, a_n)L \rightsquigarrow (a_1, \ldots, a_n)LK$. The map $\xi_X : X \to A^nL$; $x = \sum_{i=1}^{n} a_i x_i \rightsquigarrow (a_1, \ldots, a_n)L = (h(x, y_1), \ldots, h(x, y_n))$ is also split. Hence, it follows that there is an A-submodule X' such that $X = X' + \operatorname{Ker} \xi_X$, $\operatorname{Ker} \xi_X \subset X \cap (X + Y)^{\perp}$ and $\xi_X|_{X'} : X' \to A^nL$ is an A-isomorphism. Put $x_i = x_i' + x_i''$ for $x_i' \in X'$ and $x_i'' \in \operatorname{Ker} \xi_X$. Then we have $L = (h(x_i, y_j)) = (h(x_i', y_j))$. Since $L^* = (h(y_i, x_j'))$ is also regular, i.e. $L^*K^*L^* = L^*$ is satisfied, an A-epimorphism $\xi_Y : Y \to A^nL^*$; $y = \sum_{i=1}^{n} a_i y_i \rightsquigarrow (a_1, \ldots, a_n)L^* = (h(y, x_1'), \ldots, h(y, x_n'))$ is also split, in fact A-homomorphisms $\mu_{K^*}: A^nL^* \to A^n$; $(a_1, \ldots, a_n)L^* \rightsquigarrow (a_1, \ldots, a_n)L^*K^*$ and $\eta_Y : A^n \to Y$; $(a_1, \ldots, a_n) \rightsquigarrow \sum_{i=1}^{n} a_i y_i$ satisfy $\xi_Y \circ \eta_Y \circ \mu_{K^*} = I$ on A^nL^*. Then we have $Y = Y' \oplus \operatorname{Ker} \xi_Y$, where $Y' = \eta_Y \circ \mu_{K^*}(A^nL^*)$, and $\xi_Y|_{Y'} : Y' \to A^nL^*$ is an A-isomorphism whose inverse is $\eta_Y \circ \mu_{K^*}$. Put $y_i = y_i' + y_i''$ for $y_i' \in Y'$ and $y_i'' \in \operatorname{Ker} \xi_Y$. Then it follows that $L^* = (h(y_i, x_j')) =$

$(h(y_i', x_j'))$, $Y' = \sum_{i=1}^{n} Ay_i'$ and $y_i' = \eta_Y \circ \mu_{K*} \xi_Y(y_i') = \eta_Y((h(y_i', x_1'), \ldots, h(y_i', x_n')))$ for $i = 1, 2, \ldots, n$. Put $B = (h(y_i', y_j'))$ an $n \times n$-matrix with (i,j)-component $h(y_i', y_j')$. Then we have $B = L^*K^*B$. Now, we consider an A-submodule $X' + Y' = \sum_{i=1}^{n} Ax_i' + \sum_{i=1}^{n} Ay_i'$ of (M,h). Then a $2n \times 2n$-matrix $F = \begin{pmatrix} 0 & L \\ L^* & B \end{pmatrix}$ is the matrix of $(X' + Y', h)$ with respect to the generator $x_1', \ldots, x_n', y_1', \ldots, y_n'$. We show that $\xi_{X'+Y'} : (X' + Y', h) \to \langle F \rangle; \sum_{i=1}^{n} a_i x_i' + \sum_{i=1}^{n} b_i y_i' \longmapsto (a_1, \ldots, a_n, b_1, \ldots, b_n)F$ is an isomorphism. If $\sum_{i=1}^{n} a_i x_i' + \sum_{i=1}^{n} b_i y_i'$ is in $\operatorname{Ker} \xi_{X'+Y'}$, then we have $\xi_Y(\sum_{i=1}^{n} b_i y_i') = (b_1, \ldots, b_n)L^* = 0$ and $\xi_X(\sum_{i=1}^{n} a_i x_i') + (h(\sum_{i=1}^{n} b_i y_i', y_1'), \ldots, h(\sum_{i=1}^{n} b_i y_i', y_n')) = (a_1, \ldots, a_n)L + (b_1, \ldots, b_n)B = 0$. Since $\xi_Y|_{Y'}$ and $\xi_X|_{X'}$ are isomorphisms, we get $\sum_{i=1}^{n} b_i y_i' = 0$ and $\xi_X(\sum_{i=1}^{n} a_i x_i') = -(h(\sum_{i=1}^{n} b_i y_i', y_1), \ldots, h(\sum_{i=1}^{n} b_i y_i', y_n')) = 0$, and so $\sum_{i=1}^{n} a_i x_i' = 0$. Hence $\operatorname{Ker} \xi_{X'+Y'} = 0$, that is, $\xi_{X'+Y'}$ is an isomorphism. Using $L^*K^*B = B$, we get $\begin{pmatrix} 0 & L \\ L^* & B \end{pmatrix} \begin{pmatrix} -K^*BK & K^* \\ K & B \end{pmatrix} \begin{pmatrix} 0 & L \\ L^* & B \end{pmatrix} = \begin{pmatrix} 0 & L \\ L^* & B \end{pmatrix}$. Hence, F is a von Neumann regular element in A_{2n}, and $(X' + Y', h)$ is both non-degenerate and A-projective. Since $\xi_Y|_{Y'}$ is an isomorphism, we have $X'^{\perp} \cap Y' = 0$. From the fact $X' \cap Y' \subset X'^{\perp} \cap Y' = 0$, it follows that $X' + Y' = X' \oplus Y'$ and $X'^{\perp} \cap (X' + Y') = X' + (X'^{\perp} \cap Y') = X'$. Therefore, $(X' + Y', h)$ is metabolic. Since $X = X' \oplus \operatorname{Ker} \xi_X$, $\operatorname{Ker} \xi_X \subset (X + Y)^{\perp} \cap X \subset (X' + Y')^{\perp} \cap X$ and $X' \cap (X' + Y')^{\perp} = 0$, $X = X' \oplus (X + Y)^{\perp} \cap X$ is concluded.

Corollary 2. If A is a von Neumann regular ring, then a non-degenerate hermitian left A-module (M,h) with maximum (or minimum) condition for non-degenerate A-submodules has the following split:

$$(M,h) \cong \langle a_1\rangle \perp \cdots \perp \langle a_r\rangle \perp \left\langle\begin{pmatrix} 0 & b_1 \\ \bar{b}_1 & 0\end{pmatrix}\right\rangle \perp \cdots \perp \left\langle\begin{pmatrix} 0 & b_s \\ \bar{b}_s & 0\end{pmatrix}\right\rangle ,$$

where a_i and b_i are some elements in A with $\bar{a}_i = a_i$. If A is a semi-simple Artinian ring, then every non-degenerate hermitian left A-module has the above split.

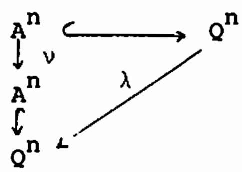
Proof. See [1].

4. A-submodule of a hermitian module over the maximal quotient ring of A. In this section, we consider a maximal left quotient ring Q of A, and suppose that Q has an involution which is an extension of the involution of A. If Q is a classical quotient ring, the involution of A can be extended to an involution of Q.

Suppose (M,h) is a hermitian left Q-module. For an A-submodule X of M, the submodule $S(X)$ generated by $\{h(x,y);\ x,\ y \in X\}$ will be called the scale of X. The scale $S(X)$ becomes an A-sub-bimodule of Q, and is stable by the involution of Q, i.e. $\overline{S(X)} = S(X)$. Then $(X,h,S(X))$ is regarded as a hermitian left A-module in the sense of § 1.

Theorem 6. Suppose that A is a left non-singular ring (cf. [2], p. 76), Q is a left maximal quotient ring of A, and that (M,h) is a hermitian left Q-module. If $X = \sum_{i=1}^{n} Ax_i$ is an A-submodule of M such that, for the $n\times n$-matrix $H = (h(x_i,x_j))$, $\xi_X : X \to A^nH;\ x = \sum_{i=1}^{n} a_ix_i \rightsquigarrow (a_1, \ldots, a_n)H = (h(x,x_1),\ldots,h(x,x_n))$ is an isomorphism, then it follows that X is A-projective if and only if there is a matrix K in Q_n such that $HK \in A_n$ and $HKH = H$.

Proof. If X is A-projective, then so is A^nH. Then an A-epimorphism $\mu_H : A^n \to A^nH;\ (a_1,\ldots,a_n) \rightsquigarrow (a_1,\ldots,a_n)H$ is split, hence there is an A-homomorphism $\nu : A^nH \to A^n$ such that $\mu_H \circ \nu = I$. Since Q^n is A-injective, there is an A-homomorphism $\lambda : Q^n \to Q^n$ making the following diagram commute;



Since W is a rational extension of A (cf. [2], p. 81), so is Q^n also of A^n, because, for any $x = (x_1,\ldots,x_n)$ and $y = (y_1,\ldots,y_n) \neq 0$ in Q^n, there is $a \in A$ such that $ax = (ax_1,\ldots,ax_n) \in A^n$ and $ay = (ay_1,\ldots,ay_n) \neq 0$ (cf. [2], p. 79). Put $\lambda((\underbrace{0,\ldots,0}_{(i-1)\text{-times}},1,0,\ldots,0)) = (q_{i1},\ldots,q_{in})$ for $q_{ij} \in Q$, and $K = (q_{ij})$ an $n\times n$-matrix with (i,j)-component q_{ij}. Then $\lambda((a_1,\ldots,a_n)) = (a_1,\ldots,a_n)K$ is satisfied for all $(a_1,\ldots,a_n) \in A^n$. We consider an A-homomorphism $f : Q^n \to Q^n;\ (x_1,\ldots,x_n) \rightsquigarrow \lambda((x_1,\ldots,x_n)) - (x_1,\ldots,x_n)K$ which carries all the elements of A^n to 0. By the rationality of Q^n over A^n, we get $f = 0$, i.e. $\lambda((x_1,\ldots,x_n)) = (x_1,\ldots,x_n)K$

for every $(x_1,\ldots,x_n) \in Q^n$. Therefore, we have $A^nHK = \lambda(A^nH) = \nu(A^nH) \subset A^n$, i.e. $HK \in A^n$, and $HKH = H$ from the fact $\mu_H \circ \nu = I$. The converse is obvious.

Theorem 7. Under the same assumption on A, Q and (M,h) as in Theorem 6, let $X = \sum_{i=1}^{n} Ax_i$ be an A-submodule of M, and $H = (h(x_i,x_j))$ the $n{\times}n$-matrix with (i,j)-component $h(x_i,x_j)$. Then $(X,h,S(X))$ is both non-degenerate and A-projective if and only if $\xi_X : (X,h,S(X)) \to \langle H\rangle$ is an isomorphism and there is an $n{\times}n$-matrix K in Q_n such that $S(X)^n.K \subset A^n$ and $HKH = H$.

Proof. Suppose that $(X,h,S(X))$ is both non-degerated and A-projective. By Theorem 6, there is $K \in Q_n$ such that $HK \in A_n$ and $HKH = H$. Since HK is an idempotent in Q_n, we have $\mathrm{Ann}(A^n;H) = A^n(E - HK)$ and $\mathrm{Ann}({}^tS(X)^n;\ \mathrm{Ann}(A^n;H)) = HK.{}^tS(X)^n$. Furthermore, by Theorem 1 we have $HK.{}^tS(X)^n = H.{}^tA^n$. $K' = K^*HK$ satisfies identities $HK'H = H$ and $K'^* = K'$, and so $K'^*.{}^tS(X)^n = K^*HK.{}^tS(X)^n = K^*H.{}^tA^n$ and $S(X)^nK' = A^nHK \subset A^n$. Namely, K' is a required matrix in Q_n. Conversely, suppose that K is a matrix in Q_n such that $S(X)^nK \subset A^n$ and $HKH = H$. Then every row of HK is contained in $S(X)^nK$, and so $HK \in A_n$. Put $K' = K^*HK$. Then $S(X)^nK' = S(X)^nK^*HK = S(X)^n(HK)^*K \subset S(X)^nK \subset A^n$ and $\mathrm{Ann}(A^n;H) = A^n(E - EK')$. Hence, we get $\mathrm{Ann}({}^tS(X)^n;\ \mathrm{Ann}(A^n;H)) = HK'.{}^tS(X)^n = H(S(X)^nK')^* \subset H.{}^tA^n$. By Theorems 1 and 2, $(X,h,S(X))$ is both non-degenerate and A-projective.

References

[1] T. Kanzaki: Notes on hermitian forms over a ring, to appear.

[2] C. Faith: Algebra II: Ring Theory, Grund. Math. Wiss. 191, Springer, 1976.

S-S-BIMODULE STRUCTURE OF S/R-AZUMAYA ALGEBRA AND 7-TERMS EXACT SEQUENCE

Kenji YOKOGAWA
Nara Women's University

Introduction. Let R be a commutative ring, and S a commutative R-algebra which is a finitely generated faithful projective R-module. An R-Azumaya algebra A is called an S/R-Azumaya algebra if A contains S as a maximal commutative subalgebra and is left S-projective. A(S/R) denotes the isomorphism (compatible with the maximal commutative embeddings of S) classes of S/R-Azumaya algebras. Then we have the following exact sequences [3]:

$$0 \to H^1(S/R,U) \to \mathrm{Pic}(R) \to H^0(S/R,\mathrm{Pic}) \to H^2(S/R,U) \to$$
$$\to \mathrm{Br}(S/R) \to H^1(S/R,\mathrm{Pic}) \to H^3(S/R,U),$$
$$\mathrm{Pic}(S) \xrightarrow{\mathrm{End}} A(S/R) \to \mathrm{Br}(S/R) \to 0$$

where $H^i(S/R,U)$ and $H^i(S/R,\mathrm{Pic})$ denote the i-th Amitsur's cohomology groups of the extension S/R with respect to the units functor U and Picard group functor Pic respectively, and Br(S/R) denotes the Brauer group of R-Azumaya algebras split by S.

The first exact sequence is obtained concretely in [5] when S/R is a separable Galois extension and in [8] when S/R is a Hopf Galois extension. From the exact sequences, we know that an S/R-Azumaya algebra is related to the 1-cocycle (with respect to the functor Pic), especially to the rank one

$S\otimes_R S$-projective module. But we remark that S/R-Azumaya algebras are not necessarily $S\otimes_R S$-projective (viewed as S-S-bimodule) [8].

We shall investigate the $S\otimes_R S$-module structure of S/R-Azumaya algebras and construct the 7-terms exact sequence concretely. The details will be omitted and will be found in [9].

Throughout each $\otimes$, End, etc. are taken over R unless otherwise stated, and repeated tensor products of S are denoted by exponents; $S^q = S\otimes\ldots\otimes S$ with q-factors. We shall consider S^q as an S-algebra on the first term. In order to indicate the module structure, we write if necessary, $S_1\otimes S_2$ instead of $S^2 = S\otimes S$, ${}_{S_1}M_{S_2}$ instead of $S^2 = S_1\otimes S_2$-module M etc.

1. S^2-module structure of S/R-Azumaya algebras

Lemma 1.1. Let M be a projective S-module of rank one, then

$$\mathrm{End}(M) \simeq (M\otimes S)\otimes_{S^2}(S\otimes M^*)\otimes_{S^2}\mathrm{End}(S)$$

as S^2-modules, where $M^* = \mathrm{Hom}_S(M,S)$.

Proof. $\psi : (M\otimes S)\otimes_{S^2}(S\otimes M^*)\otimes_{S^2}\mathrm{End}(S) \to \mathrm{End}(M)$ defined by $\psi(m(m\otimes s)\otimes(t\otimes f)\otimes g)(n) = tg(f(sn))m$ gives a desired S^2-isomorphism.

Now, let A be an S/R-Azumaya algebra then A is split by S. Hence there exists a projective S^2-module M of rank one such that $S \otimes A \cong \mathrm{End}_S(M)$ as S-algebras. From Lemma 1.1 $\mathrm{End}_S(M) \cong (M \otimes_S S^2) \otimes_{S^3} (S^2 \otimes_S M^*) \otimes_{S^3} \mathrm{End}_S(S^2) = ({}_{S_1}M_{S_2} \otimes S_3) \otimes_{S^3} ({}_{S_1}M^*{}_{S_3} \otimes S_2) \otimes_{S^3} \mathrm{End}_S(S^2)$. Let $P = (({}_{S_1}M_{S_2} \otimes S_3) \otimes_{S^3} ({}_{S_1}M^*{}_{S_3} \otimes S_2)) \otimes_{S^3} S^2 = ((M \otimes_{S^2} S_1) \otimes S_2) \otimes_{S^2} {}_{S_1}M^*{}_{S_2}$, where S^2 is regarded as S^3-module by $\mu \otimes 1 : S^3 \to S^2$, μ is the multiplication of S. Then we have an S^2-isomorphism $A \cong P \otimes_{S^2} \mathrm{End}(S)$, P is a projective S^2-module of rank one.

Let Φ be the composite of S^2-isomorphisms $\mathrm{End}_{S_1 \otimes S_2}({}_{S_1}M_{S_3} \otimes S_2) \cong S_1 \otimes A \otimes S_2 \cong S_1 \otimes S_2 \otimes A \cong \mathrm{End}_{S_1 \otimes S_2}(S_1 \otimes {}_{S_2}M_{S_3})$, where the middle isomorphism is the one induced by the twisting homomorphism $A \otimes S_2 \cong S_2 \otimes A$. Then there exists a projective S^2-module Q of rank one such that $({}_{S_1}M_{S_3} \otimes S_2) \otimes_{S_1 \otimes S_2} {}_{S_1}Q_{S_2} \cong S_1 \otimes {}_{S_2}M_{S_3}$ as $\mathrm{End}_{S_1 \otimes S_2}(S_1 \otimes {}_{S_2}M_{S_3})$-modules, hence as S^3-modules. Tensoring with S^2 over S^3 (regarding S^2 as an S^3-module by $1 \otimes \mu : S^3 \to S^2$), we get an S^3-isomorphism $M \otimes_{S^2} Q \cong S \otimes (M \otimes_{S^2} S)$. Using these isomorphisms, we can easily prove that P is a 1-cocycle of the extension S/R with respect to the functor Pic (we call simply 1-cocycle).

Let $S \otimes A \cong \mathrm{End}_S(N)$ for another projective S^2-module N of rank one. Then we can easily prove that the 1-cocycles obtained from M and N are S^2-isomorphic.

In order to prove the uniqueness of 1-cocycle P, we prepare the following

Lemma 1.2 (cf. [6] I.4.2). Let T be a commutative R-algebra which is a finitely generated faithful projective R-module, and let P, Q be finitely generated projective T-modules of rank one. Then

$$\mathrm{Hom}_{T\otimes T}(P\otimes Q, Q\otimes P) \simeq \mathrm{Hom}_{T\otimes T}(\mathrm{End}(P), \mathrm{End}(Q)) .$$

Especially, $\mathrm{Iso}_{T\otimes T}(P\otimes Q, Q\otimes P)$ corresponds to $\mathrm{Iso}_{T\otimes T}(\mathrm{End}(P),$ $\mathrm{End}(Q))$.

Let P, P' be 1-cocycles such that $A \simeq P\otimes_{S^2}\mathrm{End}(S) \simeq P'\otimes_{S^2}\mathrm{End}(S)$ as S^2-modules. Then $\mathrm{End}_S(P^*) \simeq \mathrm{End}_S(P'^*)$ as S^3-modules by Lemma 1.1 and cocycle conditions of P, P'. From Lemma 1.2, we get an S^3-isomorphism

$$P^*\otimes_S P'^* = ({}_{S_1}P^*{}_{S_2}\otimes S_3)\otimes_{S^3}({}_{S_1}P'^*{}_{S_3}\otimes S_2) \simeq P'^*\otimes_S P^*$$

$$= ({}_{S_1}P'^*{}_{S_2}\otimes S_3)\otimes_{S^3}({}_{S_1}P^*{}_{S_3}\otimes S_2).$$

Thus $({}_{S_1}P^*{}_{S_2}\otimes S_3)\otimes_{S^3}({}_{S_1}P_{S_3}\otimes S_2) \simeq ({}_{S_1}P'{}_{S_2}\otimes S_3)\otimes_{S^3}({}_{S_1}P'{}_{S_3}\otimes S_2)$, the left side is isomorphic to $S\otimes P$ and the right side is isomorphic to $S\otimes P'$. Hence $P \simeq P'$ as S^2-modules.

Summing up, we get

<u>Theorem 1.3.</u> Let A be an S/R-Azumaya algebra, then there exists a unique 1-cocycle P such that A is isomorphic to $P\otimes_{S^2}\mathrm{End}(S)$ as S^2-modules and $S\otimes A$ is isomorphic to $\mathrm{End}_S(P^*)$ as S-algebras, where $P^* = \mathrm{Hom}_{S^2}(P, S^2)$.

Next we shall start from a 1-cocycle P and an S^3-isomorphism $\phi : S^2\otimes_S P^* = {}_{S_1}P^*{}_{S_3}\otimes S_2 \simeq (S_1\otimes_{S_2}P^*{}_{S_3})\otimes_{S^3}({}_{S_1}P^*{}_{S_2}\otimes S_3)$. Define the S^4-isomorphism ϕ_1 as follows; $\phi_1 = 1\otimes\phi$: $S_1\otimes_{S_2}P^*{}_{S_4}\otimes S_3 \simeq (S_1\otimes S_2\otimes_{S_3}P^*{}_{S_4})\otimes_{S^4}(S_1\otimes_{S_2}P^*{}_{S_3}\otimes S_4)$, identity on S_1, and similarly we define ϕ_2, ϕ_3. Let $u(\phi) \in \mathrm{End}_{S^4}$

$({}_{S_1}P^*{}_{S_4}\otimes S_2 \otimes S_3)$ be the composite $\phi_3^{-1}\cdot\phi_1^{-1}\otimes_{S^4}1\cdot 1\otimes_{S^4}(\phi\otimes 1)\cdot\phi_2$ and consider $u(\phi)$ as a unit of S^4 by homothety. As is easily checked, $u(\phi)$ is a 3-cocycle (w.r.t. functor U) and $u(\alpha\phi)$ is cohomologous to $u(\phi)$ for any unit $\alpha \in S^3$.

Theorem 1.4. Let P be a 1-cocycle with an S^3-isomorphism $\phi : {}_{S_1}P^*{}_{S_3}\otimes S_2 \cong (S_1\otimes {}_{S_2}P^*{}_{S_3})\otimes_{S^3}({}_{S_1}P^*{}_{S_2}\otimes S_3)$. Then $A = P\otimes_{S^2}\mathrm{End}(S)$ has an S/R-Azumaya algebra structure, if and only if $u(\phi)$ is a coboundary.

Proof. First we assume $A = P\otimes_{S^2}\mathrm{End}(S)$ is an S/R-Azumaya algebra. Then $S\otimes A \cong \mathrm{End}_S(P^*)$ as S-algebras. Define the S^2-algebra isomorphism

$$\Phi : \mathrm{End}_{S_1\otimes S_2}({}_{S_1}P^*{}_{S_3}\otimes S_2) = S_1\otimes A\otimes S_2$$
$$\cong S_1\otimes S_2\otimes A = \mathrm{End}_{S_1\otimes S_2}(S_1\otimes_{S_2}P^*{}_{S_3})$$

by the twisting homomorphism $A\otimes S_2 \to S_2\otimes A$. Then Φ is a descent homomorphism, that is, if we define $\Phi_1 = 1\otimes\Phi$: $S_1\otimes \mathrm{End}_S(P^*)\otimes S \cong S_1\otimes S\otimes \mathrm{End}_S(P^*)$, identity on S_1, and Φ_2, Φ_3 similarly, then $\Phi_2 = \Phi_1\cdot\Phi_3$. Since Φ is an S^2-algebra isomorphism, there exists a projective S^2-module Q of rank one such that ${}_{S_1}P^*{}_{S_3}\otimes S_2 \overset{\phi'}{\cong} (S_1\otimes_{S_2}P^*{}_{S_3})\otimes_{S_1\otimes S_2}{}_{S_1}Q_{S_2} = (S_1\otimes_{S_2}P^*{}_{S_3})\otimes_{S^3}({}_{S_1}Q_{S_2}\otimes S_3)$ as S^3-modules and Φ is induced by this isomorphism ϕ'. From the cocycle condition of P, $Q \cong P^*$. Then $\Phi_2 = \Phi_1\cdot\Phi_3$ claims that 3-cocycle $u(\phi')$ is a coboundary. Hence $u(\phi)$ is a coboundary. Conversely, let $u(\phi)$ be a coboundary then we may assume $u(\phi) = 1\otimes 1\otimes 1\otimes 1$.

Let ϕ^* be the isomorphism $S\otimes P \cong (P^*\otimes S)\otimes_{S^3}({}_{S^1}P_{S^3}\otimes S_2)$ induced from ϕ by duality pairing. We consider $S\otimes A = (S\otimes P)\otimes_{S^3}End_S(S^2)$ equals $End_S(P^*) = (P^*\otimes S)\otimes_{S^3}({}_{S^1}P_{S^3}\otimes S_2)$ $\otimes_{S^3}End_S(S^2)$ by $\phi^*\otimes_{S^3}1$. Then $S\otimes A$ has an S-algebra structure. Define $\Phi : S\otimes A\otimes S \cong S\otimes S\otimes A$ by the twisting homomorphism, then $\Phi_2 = \Phi_1\cdot\Phi_3$. From the theory of faithfully flat descent, if Φ is an S^2-algebra isomorphism (this can be proved by localization) then the descent module A has an R-algebra (necessarily an S/R-Azumaya algebra) structure.

2. 7-terms exact sequence

In this section we make homomorphisms $\theta_1, \dots, \theta_6$ of the exact sequence

$$(2.1)\qquad \begin{aligned} 0 \to H^1(S/R,U) &\xrightarrow{\theta_1} Pic(R) \xrightarrow{\theta_2} H^0(S/R,Pic) \xrightarrow{\theta_3} H^2(S/R,U) \xrightarrow{\theta_4} \\ &\to Br(S/R) \xrightarrow{\theta_5} H^1(S/R,Pic) \xrightarrow{\theta_6} H^3(S/R,U) \end{aligned}$$

The verifications of the well-defineness, exactness, etc. are all omitted.

Let $\rho = \sum_i x_i\otimes y_i \in S^2$ be a 1-cocycle (w.r.t. functor U). We make a new End(S)-module ${}_\rho S$ as follows;

${}_\rho S = S$ as S-module, $f\cdot s = \sum_i x_i f(y_i s)$, $f\in End(S)$, $s\in S$. In reality, ${}_\rho S$ is an End(S)-module. Define θ_1 as the homomorphism induced by the one which carries ρ to $Hom_{End(S)}(S, S)$. Define θ_2 as the homomorphism induced by tensoring with S over R.

Let P be a 0-cocycle (w.r.t. functor Pic) with S^2-isomorphism $\zeta : S\otimes P \cong P\otimes S$. Define ζ_1 as follows; $\zeta_1 =$

$1 \otimes \zeta : S_1 \otimes S \otimes P \simeq S_1 \otimes P \otimes S$, identity on S_1, and similarly define ζ_2, ζ_3. Put $v(\zeta) = \zeta_2^{-1} \cdot \zeta_3 \cdot \zeta_1 \in \mathrm{End}_{S^3}(S \otimes S \otimes P)$ and consider $v(\zeta)$ as in S^3. Then $v(\zeta)$ is a 2-cocycle. We define θ_3 as the homomorphism induced from the one which carries 0-cocycle P, $\zeta : S \otimes P \simeq P \otimes S$ to $v(\zeta)$.

Let $\sigma = \sum_i x_i \otimes y_i \otimes z_i$ be a normal 2-cocycle (w.r.t. functor U), and define a new multiplication "$*$" on End(S) by setting

$$(f*g)(s) = \sum_i x_i f(y_i g(z_i s)), \quad s \in S,\ f,\ g \in \mathrm{End}(S).$$

This algebra $A(\sigma)$ is an S/R-Azumaya algebra. We define θ_4 as the homomorphism induced from the one which carries σ to $A(\sigma)$. We define θ_5 and θ_6 as the homomorphisms induced from Theorem 1.3 and Theorem 1.4 respectively.

<u>Theorem 2.2.</u> The homomorphisms $\theta_1, \ldots, \theta_6$ defined above make the sequence (2.1) exact.

References

[1] M. Auslander and O. Goldman: The Brauer group of a commutative ring, Trans. Amer. Math. Soc. 97 (1960), 367-409.

[2] H. Bass: The Morita Theorems, Lecture Notes at University of Oregon, 1962.

[3] S. U. Chase and A. Rosenberg: Amitsur cohomology and the Brauer group, Mem. Amer. Math. Soc. 52 (1965), 34-79.

[4] F. DeMeyer and E. Ingraham: Separable Algebras over Commutative Rings, Lecture Notes in Math. 181, Springer,

1971.

[5] T. Kanzaki: On generalized crossed product and Brauer group, Osaka J. Math. 5 (1968), 175-188.

[6] M.-A. Knus and M. Ojanguren: Théorie de la Descente et Algèbres d'Azumaya, Lecture Notes in Math. 389, Springer, 1974.

[7] M. E. Sweedler: Multiplication alternation by two-cocycles, Illinois J. Math. 15 (1971), 302-323.

[8] K. Yokogawa: On $S \otimes_R S$-module structure of S/R-Azumaya algebras, Osaka J. Math. 12 (1975), 673-690.

[9] K. Yokogawa: An application of the theory of descent to the $S \otimes_R S$-module structure of S/R-Azumaya algebras, to appear.

ON LONG'S H-AZUMAYA ALGEBRA*)

Mitsuhiro TAKEUCHI

The University of Tsukuba

Introduction. Let k be a field. Let H be a commutative and cocommutative Hopf algebra over k, and $\eta: H\otimes H \to k$ be a Hopf pairing. Let A and B be H-comodule algebras. Then, $A\otimes B$ is a k-algebra with multiplication defined by

$$(a\otimes b)(x\otimes y) = \sum_{(b)(x)} \eta(x_{(H)}\otimes b_{(H)})ax_{(A)}\otimes b_{(B)}y$$

and is denoted by $A\#_\eta B$. An H-comodule algebra A is called η-Azumaya, if it is non-zero finite dimensional over k and there are an H-comodule algebra B and H-comodules V and W which are non-zero finite dimensional over k such that

$$A\#_\eta B \simeq \mathrm{End}\ V, \qquad B\#_\eta A \simeq \mathrm{End}\ W$$

as H-comodule algebras. The set of equivalence classes of η-Azumaya algebras form a group $B_\eta(k,H)$ with multiplication induced by $\#_\eta$.

Let F be a commutative and cocommutative Hopf algebra over k, and $\omega: F\otimes H \to k$ a Hopf pairing. Define a Hopf pairing

$$\Omega: (F\otimes H)\otimes(F\otimes H) \to k$$

by $\Omega((p\otimes q)\otimes(u\otimes v)) = \omega(p\otimes v)\varepsilon(q)\varepsilon(u)$. If A and B are $F\otimes H$-comodule algebras, then $A\#_\Omega B = A\#_\omega B$ as algebras. An Ω-Azumaya algebra is called an F-H-Azumaya algebra (with respect to ω),

---

*) This is derived from the author's article [9] which includes all the proofs omitted here.

and we write

$$B_{\Omega}(k,F\otimes H) = B_{\omega}(k,F,H).$$

Let H° be the dual Hopf algebra of H, and consider the canonical Hopf pairing $\gamma: H^{\circ}\otimes H \to k$ given by $\gamma(X\otimes x) = X(x)$. Then finite dimensional H-dimodule algebras in the sense of Long [4] are identified with finite dimensional $H^{\circ}\otimes H$-comodule algebras. Long's smash product # coincides with $\#_{\gamma}$, and H-Azumaya algebras are the same as our H°-H-Azumaya algebras. Hence we have a group isomorphism $BD(k,H) \simeq B_{\gamma}(k,H^{\circ},H)$.

Let $Sp\, H$ be the commutative affine k-group scheme represented by H. An H-comodule algebra is identified with a pair (A,ρ) where $\rho: Sp\ H \to \mathcal{A}ut(A)$ is a homomorphism of group sheaves. If A is Azumaya, we obtain the following central exact sequence of affine k-group schemes

$$\pi(A): 1 \to \mu \to X \to Sp\ H \to 1.$$

Let $\mathrm{Ext}_{\mathrm{cent}}(Sp\ H,\mu)$ denote the abelian group of isomorphism classes of central extensions of $Sp\ H$ by μ. The map $A \mapsto \pi(A)$ induces the following split exact sequence of abelian groups:

$$1 \to B(k) \to BC(k,H) \overset{\pi}{\to} \mathrm{Ext}_{\mathrm{cent}}(Sp\ H,\mu) \to 1$$

where $B(k)$ denotes the usual Brauer group of k. Beattie [1] constructs a similar exact sequence in a different manner.

Suppose the following condision:

(*) If A is an Azumaya F-comodule algebra and B an Azumaya H-comodule algebra, then $A\#_{\omega}B$ is Azumaya.

Then the set of equivalence classes of Azumaya $F\otimes H$-comodule algebras $BC(k,F\otimes H)$ is a monoid with multiplication induced by $\#_\omega$ and we have

$$1 \to B(k) \to BC(k, F\otimes H) \overset{\psi}{\to} \mathrm{Ext}_{\mathrm{cent}}(Sp\ F \times Sp\ H, \mu) \to 1.$$

Hence $\mathrm{Ext}_{\mathrm{cent}}(Sp\ F \times Sp\ H, \mu)$ has a quotient monoid structure. The purpose of this paper is to describe the monoid structure.

1. Notation and Definition. Let k be a commutative ring with unit. We write $\otimes$ and End instead of $\otimes_k$ and End_k. If V is a k-module, V^* denotes $\mathrm{Hom}_k(V,k)$. The group of units of a ring R is denoted by U(R). If a and b are objects of a category $\underline{\underline{A}}$, we denote by $\underline{\underline{A}}(a,b)$ the set of $\underline{\underline{A}}$-morphisms of a to b. We refer the reader to [5] for the theory of coalgebras and Hopf algebras. The structure maps of a k-coalgebra C are denoted by $\Delta: C \to C\otimes C$ and $\varepsilon: C \to k$. We use the sigma notation $\Delta(c) = \sum_{(c)} c_{(1)} \otimes c_{(2)}$, $c \in C$. The set of group-like elements in C is denoted by $\mathrm{gr}_k(C)$ or $\mathrm{gr}(C)$. If V is a right C-comodule with structure $\chi: V \to V\otimes C$, we use the notation:

$$\chi(v) = \sum_{(v)} v_{(V)} \otimes v_{(C)}, \quad (1\otimes\Delta)\chi(v) = \sum_{(v)} v_{(V)} \otimes v_{(C,1)} \otimes v_{(C,1)}$$

$v \in V$. The antipode of a Hopf algebra is denoted by S. A right H-comodule algebra, where H is a Hopf algebra, is a k-algebra and a right H-comodule A whose structure map $\chi: A \to A\otimes H$ is an algebra map.

To denote the multiplication of an abelian group, we use the additive notation most of the paper. But the multiplicative notation is also used here and there. Let G_j and H_i be abelian groups. A homomorphism $f: G_1 \times \dots \times G_n \to H_1 \times \dots \times H_m$ is identified with an $m \times n$ matrix $A = (a_{ij})$ with $a_{ij}: G_j \to H_i$

by the rule:

$$f(x_1,\ldots,x_n) = (y_1,\ldots,y_m)$$

if and only if

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = A\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum_j a_{1j}(x_j) \\ \vdots \\ \sum_j a_{mj}(x_j) \end{pmatrix} .$$

Let $\underline{\underline{M}}_k$ be the category of commutative k-algebras. A k-functor (resp. a k-group functor) is a functor from $\underline{\underline{M}}_k$ into the category of sets $\underline{\underline{E}}$ (resp. of groups). They form a category $\underline{\underline{M}}_k\underline{\underline{E}}$ (resp. $\underline{\underline{Gr}}_k$). The affine k-functor of $R \in \underline{\underline{M}}_k$ is denoted $Sp\ R$. A map $\sigma\colon A \to B$ of $\underline{\underline{M}}_k$ is an fppf-covering if B is a faithfully flat A-algebra of finite presentation. It determines an equalizer diagram in $\underline{\underline{M}}_k$: $A \overset{\sigma}{\to} B \underset{j}{\overset{i}{\rightrightarrows}} B \otimes_A B$ where $i(b) = b \otimes 1$, $j(b) = 1 \otimes b$. A k-functor is called a k-sheaf if it preserves all finite products and all such equalizer diagrams as above. A k-group sheaf means a k-group functor which is a k-sheaf as a k-functor.

Let V be a k-module and A a k-algebra. The following k-group functors are k-group sheaves:

$GL(V)\colon T \to GL_T(T\otimes V)$, $\mu^A\colon T \to U(T\otimes A)$, $Aut(A)\colon T \to Aut_{T\text{-}alg}(T\otimes A)$.

If V and A are k-finite projective, they are affine algebraic [3, II, §1, 2.4 and 2.6]. We write $\mu^k = \mu$.

Let G be a commutative k-group functor. We denote by $\hat{G}$ the Cartier dual [3, II, §1, 2.10] of G. It is the k-group functor: $T \to \underline{\underline{Gr}}_T(G_T,\mu_T)$. It is a k-group sheaf, since μ is [3, III, §5, 1.6]. There is a canonical homomorphism: $G \to \hat{\hat{G}}$ Each homomorphism of commutative k-group functors $f\colon G \to E$

induces a homomorphism $\hat{f}: \hat{E} \to \hat{G}$.

Let G and $\mathcal{D}$ be commutative k-group functors, and $\mathrm{Bim}_k(G \times \mathcal{D}, \mu)$ the group of <u>bimultiplicative</u> morphisms: $G \times \mathcal{D} \to \mu$. It is naturally identified with $\underline{\underline{\mathrm{Gr}}}_k(G,\mathcal{D})$ or $\underline{\underline{\mathrm{Gr}}}_k(\mathcal{D},G)$. Thus

$$\mathrm{Bim}_k(G \times \mathcal{D}, \mu) \simeq \underline{\underline{\mathrm{Gr}}}_k(G,\hat{\mathcal{D}}) \simeq \underline{\underline{\mathrm{Gr}}}_k(\mathcal{D},\hat{G}).$$

If $\phi: G \times \mathcal{D} \to \mu$ is bimultiplicative, we denote by $\phi': \mathcal{D} \to \hat{G}$ and $\phi'': G \to \hat{\mathcal{D}}$ the corresponding homomorphisms. Hence

$$\phi'(y)(x) = \phi''(x)(y) = \phi(x,y), \quad x \in G(T),\ y \in \mathcal{D}(T),\ T \in \underline{\underline{M}}_k.$$

If $G \to \hat{G}$, then $\hat{\phi}' = \phi''$. If $\mathcal{D} \simeq \hat{\mathcal{D}}$, then $\hat{\phi}'' = \phi'$.

For the theory of k-sheaves and k-group sheaves, we refer to [3, III] and [6, §1].

Let $\mathcal{D}$ be a commutative k-group sheaf and S a k-sheaf. A <u>$\mathcal{D}$-torsor over S</u> [3, III, §4] is an epimorphism of k-sheaves $X \to S$, where $\mathcal{D}$ acts on X so that $\mathcal{D} \times X \simeq X \times_S X$. The isomorphism classes of $\mathcal{D}$-torsors over S form an abelian group $\tilde{H}^1(S,\mathcal{D})$ [3, III, §4, 4.1] with addition given as follows: If X and Y are $\mathcal{D}$-torsors over S, then $X \vee^{\mathcal{D}} Y$ is a $\mathcal{D}$-torsor over $S \times S$, where $X \vee^{\mathcal{D}} Y$ is the cokernel k-sheaf of

$$X \times \mathcal{D} \times Y \underset{I\times\psi}{\overset{\phi\times I}{\rightrightarrows}} X \times Y$$

with the actions $\phi: \mathcal{D} \times X \to X$ and $\psi: \mathcal{D} \times Y \to Y$. Let $X \vee_S^{\mathcal{D}} Y$ be the pullback of $X \vee^{\mathcal{D}} Y$ along the diagonal map $\Delta: S \to S \times S$. Then $\mathrm{cl}(X \vee_S^{\mathcal{D}} Y) = \mathrm{cl}(X) + \mathrm{cl}(Y)$ in $\tilde{H}^1(S,\mathcal{D})$.

Let $\mathcal{D}$ be a commutative k-group sheaf and G a k-group sheaf. An exact sequence of k-group sheaves

$$\alpha: 1 \to \mathcal{D} \to X \to G \to 1$$

is a <u>central extension of G by $\mathcal{D}$</u> if the subgroup $\mathcal{D}(T)$ is central in $X(T)$ for each $T \in \underline{\underline{M}}_k$. (The sequence is exact if $X/\tilde{D} \simeq G$ with the notation of [3, p.324]). The isomorphism classes of central extensions of G by D form an abelian group, which we denote by $\mathrm{Ext}_{\mathrm{cent}}(G,D)$ [3, III, §6, 1.5]. If $f\colon G' \to G$ is a homomorphism of k-group sheaves, we denote by

$$\alpha f\colon 1 \to D \to X \times_{G'} G \to G' \to 1$$

the central extension of G' by D obtained by pullback along f. The map

$$\mathrm{Ext}_{\mathrm{cent}}(G,D) \to \mathrm{Ext}_{\mathrm{cent}}(G',D), \quad \mathrm{cl}(\alpha) \mapsto \mathrm{cl}(\alpha f)$$

is a homomorphism of abelian groups. Let

$$\beta\colon 1 \to D \to Y \to G \to 1$$

be another central extension. Then

$$\alpha \vee \beta\colon 1 \to D \to X \vee^{D} Y \to G \times G \to 1$$

is a central extension, where $X \vee^{D} Y$ is a quotient group sheaf of $X \times Y$. If $\Delta\colon G \to G \times G$ denotes the diagonal map, then

$$\mathrm{cl}((\alpha \vee \beta)\Delta) = \mathrm{cl}(\alpha) + \mathrm{cl}(\beta)$$

in the group $\mathrm{Ext}_{\mathrm{cent}}(G,D)$.

With α and X as above, consider the commutator map

$$[\ ,\ ]\colon X \times X \to X, \quad (x,y) \mapsto xyx^{-1}y^{-1}.$$

Since $[xa,yb] = [x,y]$ for each $a,b \in D(T)$, this induces a morphism

$$\partial(\alpha)\colon G \times G \to X, \quad (\bar{x},\bar{y}) \mapsto [x,y].$$

Assume G is commutative. Then $[X,X] \subset D$ and $\partial(\alpha)$ induces a bimultiplicative morphism $\partial(\alpha)\colon G \times G \to D$. It is alternating in the sense of $\partial(\alpha)(\bar{x},\bar{x}) = 0$, hence

$$\partial(\alpha)'' = -\partial(\alpha)'\colon G \to \hat{G}.$$

Let $\underline{\underline{W}}_k$ be the category of cocommutative k-coalgebras, and

$\underline{\underline{W}}'_k$ the full subcategory of those coalgebras which are colimits of k-finite projective cocommutative k-coalgebras. If $C, D \in \underline{\underline{W}}'_k$ then $C \otimes D \in \underline{\underline{W}}'_k$. If k is a field, $\underline{\underline{W}}'_k = \underline{\underline{W}}_k$. For each $C \in \underline{\underline{W}}'_k$, we define a k-functor

$$Sp^*C\colon \underline{\underline{M}}_k \to \underline{\underline{E}}, \qquad T \mapsto gr_T(T \otimes C)$$

where $gr_T(T \otimes C)$ denotes the set of group-like elements of the T-coalgebra $T \otimes C$. Such a k-functor is called a formal k-scheme. They are k-sheaves.

Group objects in $\underline{\underline{W}}_k$ are the same as cocommutative k-Hopf algebras. Hence, if H is a cocommutative k-Hopf algebra, then Sp^*H is a k-group sheaf. Such k-group sheaves are called formal k-groups.

For the theory of formal schemes and groups, the reader can refer to [7, (1.1)] and [8].

2. The #-product of group sheaf extensions. Let G and $\mathcal{D}$ be commutative k-group sheaves where $G \simeq \hat{\hat{G}}$ and $\mathcal{D} \simeq \hat{\hat{\mathcal{D}}}$ under the canonical homomorphisms. Let

$$\omega\colon \hat{G} \times \hat{\mathcal{D}} \to \mu$$

be a bimultiplicative morphism and

$$\omega\colon \hat{G} \to \mathcal{D}, \qquad \omega'\colon \hat{\mathcal{D}} \to G$$

the corresponding homomorphisms. Let

$$\alpha\colon 1 \to \mu \to X \to G \to 1,$$

$$\beta\colon 1 \to \mu \to Y \to \mathcal{D} \to 1$$

be central extensions. We define a central extension

$$\alpha \square \beta\colon 1 \to \mu \to X\#Y \to G \times \mathcal{D} \to 1$$

where $X\#Y = X \vee^{\mu} Y$ as a μ-torsor over $G \times \mathcal{D}$. We write $x\#y =$

$x \vee y$, $x \in X(T)$, $y \in Y(T)$, $T \in \underline{\underline{M}}_k$. The product of $X \# Y$ is defined by

$$(x\#y)(u\#v) = \omega(\partial(\alpha)'(\bar{u}),\partial(\beta)'(\bar{y}))xu\#yv$$

$x,u \in X(T)$, $y,v \in Y(T)$, $T \in \underline{\underline{M}}_k$. Then $X\#Y$ is a k-group sheaf with this product and with unit $1\#1$, and that $\alpha \square \beta$ is a central extension. We define

$$\kappa = \kappa(\alpha,\beta) = \begin{pmatrix} 1 & \omega'\partial(\beta)' \\ -\omega''\partial(\alpha)' & 1 \end{pmatrix} : G \times \mathcal{D} \to G \times \mathcal{D}$$

If $\kappa(\alpha,\beta)$ is an isomorphism, we put

$$\alpha\#\beta = (\alpha \square \beta)\kappa(\alpha,\beta)^{-1}.$$

Under the above notations we can prove the following

<u>Theorem 2.1</u>. Let $\omega_0 : \hat{G} \times \hat{G} \to \mu$ be a bimultiplicative morphism. Assume that $\kappa(\alpha,\beta)$ (with respect to ω_0) is an isomorphism for each $\alpha,\beta \in \mathrm{Ext}_{\mathrm{cent}}(G,\mu)$. Then the product

$$\alpha.\beta = (\alpha\#\beta)\Delta$$

where $\Delta = \binom{1}{1} : G \to G \times G$, is associative with unit 0.

<u>Theorem 2.2</u>. Let k be a field and $G,\mathcal{D}$ be commutative affine k-group schemes. Then the following are equivalent:

i) $\kappa(\alpha,\beta)$ is an isomorphism for each $\alpha \in \mathrm{Ext}_{\mathrm{cent}}(G,\mu)$, and $\beta \in \mathrm{Ext}_{\mathrm{cent}}(\mathcal{D},\mu)$.

ii) $\omega'\partial(\beta)'\,\omega''\partial(\alpha)' : G \to G$ is nilpotent, for each $\alpha \in \mathrm{Ext}_{\mathrm{cent}}(G,\mu)$, and $\beta \in \mathrm{Ext}_{\mathrm{cent}}(\mathcal{D},\mu)$.

iii) Such data as follow do not exist: $G = G_1 \times K$, $\mathcal{D} = \mathcal{D}_1 \times L$ in $\underline{\underline{Gr}}_k$, G_1 and $\mathcal{D}_1$ are finite affine $\neq 0$, $\sigma \in \mathrm{Ext}_{\mathrm{cent}}(G_1,\mu)$, $\zeta''\partial(\sigma)' : G_1 \simeq \mathcal{D}_1$, where $\zeta = \omega\,|(\hat{G}_1 \times \hat{\mathcal{D}}_1)$.

3. Azumaya algebras. The following theorem is a sheaf theoretical version of the well-known Noether-Skolem theorem [2, p.110, Th.1].

Theorem 3.1. Let A be an Azumaya k-algebra. Then μ^A and $\mathcal{Aut}(A)$ are smooth affine algebraic k-group schemes, and the following is a central extension of k-group sheaves:

$$e(A):\ 1 \to \mu \to \mu^A \xrightarrow{inn} \mathcal{Aut}(A) \to 1$$

where $inn(a)(x) = axa^{-1}$, $a \in \mu^A(T)$, $x \in T \otimes A$, $T \in \underline{\underline{M}}_k$.

Let G be a (non-commutative) k-group sheaf. A G-module algebra means a couple (A,ρ) where A is a k-algebra and ρ: $G \to \mathcal{Aut}(A)$ a homomorphism of k-group sheaves. A G-module means a couple (M,σ) where M is a k-module and σ: $G \to GL(M)$ a homomorphism of k-group sheaves. When $G = Sp\ R$ is an affine k-group with a commutative Hopf algebra R, G-module algebras are identified with R-comodule algebras, and conversely. When $G = Sp^*H$ be a formal k-group with a cocommutative Hopf algebra H, H-module algebras are identified with Sp^*H-module algebras, and conversely.

Long's Brauer groups BM(k,H)[4, p.564] and BC(k,R)[4, p. 574] are generalized as follow:

Let M be a k-finite projective G-module. Then the map

$$\rho:\ G \to \mathcal{Aut}(\mathrm{End}(M))$$

given by $\rho(g)(f) = \sigma(g)f\sigma(g)^{-1}$, $g \in G(T)$, $f \in T$ End(M), where σ is the structure map of M and $T \in \underline{\underline{M}}_k$, is well defined. With the structure, End(M) is a G-module algebra. If N is another G-module which is k-finite projective, then we have

$$\mathrm{End}(M)\otimes \mathrm{End}(N) \cong \mathrm{End}(M\otimes N)$$

as G-module algebras. Let A be a G-module algebra which is k-finite projective. If the canonical homomorphism $A\otimes A^{op} \to \mathrm{End}(A)$ of G-module algebras is an isomorphism and A is k-faithful, then A is called an Azumaya G-module algebra. In the category of Azumaya G-module algebras, we define $A \sim B$ if there exist G-modules M and N which are finite projective and faithful as k-modules such that

$$A \otimes \mathrm{End}(M) \cong B\otimes \mathrm{End}(N)$$

as G-module algebras. This is an equivalence relation and the quotient set is a commutative group with multiplication induced by $\otimes$. The group is denoted by $B(k,G)$. If $H \in \underline{\underline{W}}'_k$, then we have

$$B(k,Sp\ R) = BC(k,R) \quad \text{and} \quad B(k,Sp^*H) = BM(k,H).$$

If A is an Azumaya G-module algebra with structure ρ, we have a central extension

$$\pi(A) = e(A)\rho \in \mathrm{Ext}_{cent}(G,\mu),$$

and hence we have a homomorphism of abelian groups

$$\pi\colon B(k,G) \to \mathrm{Ext}_{cent}(G,\mu)$$

which is induecd by $A \mapsto e(A)\rho$.

Theorem 3.2. Let $G = Sp\ R$ be an affine k-group scheme. If k is a field or if R is finite projective as a k-module, then π is surjective. Hence we have a split exact sequence of abelian groups

$$1 \to B(k) \xrightarrow{i} BC(k,R) \xrightarrow{\pi} \mathrm{Ext}_{cent}(Sp\ R,\mu) \to 1,$$

where $B(k)$ is the usual Brauer group of k and i is the canonical inclusion.

Let F and H be commutative and cocommutative k-Hopf algebras. A k-linear map $\omega: F\otimes H \to k$ is called a Hopf pairing if it measures F to k and H to k [5, §7.0].

Let A be an F-comodule algebra and B an H-comodule algebra with structure maps $\chi_F: A \to A\otimes F$ and $\chi_H: B \to B\otimes H$. The smash product algebra $A\#B$ of A and B is defined as follows: $A\#B = A\otimes B$ as a k-module. We write $a\#b = a\otimes b$. The multiplication is defined by

$$(a\#b)(x\#y) = \sum_{(x)(b)} \omega(x_{(F)}\otimes b_{(H)})ax_{(A)}\#b_{(B)}y$$

$a,x \in A$, $b,y \in B$, where the comodule structures of A and B are denoted by $\chi_F(a) = \sum_{(x)} x_{(A)}\otimes x_{(F)}$ and $\chi_H(b) = \sum_{(b)} b_{(B)}\otimes b_{(H)}$. This is an associative k-algebra with unit $1\#1$.

The F-comodule algebra A is an H-module algebra with structure

$$h(a) = \sum_{(a)} \omega(a_{(F)}\otimes h)a_{(A)}$$

$h \in H$, $a \in A$. Our smash product $A\#B$ coincides with the smash product of the H-module algebra A and the H-comodule algebra B define by Long [4, (3.2)]. Long's theory of H-comodule algebras [4] can be generalized.

If A is an H-comodule algebra which is finite projective as a k-module, there are two homomorphisms of H-comodule algebras [4, (4.1)]

$$\Gamma: A\#\bar{A} \to \mathrm{End}(A), \qquad \Lambda: \bar{A}\#A \to \mathrm{End}(A)^{op}$$

where

$$\Gamma(a\#\bar{b})(c) = \sum_{(b)(c)} \omega_0(c_{(H)}\otimes b_{(H)})ac_{(A)}b_{(A)},$$

$$\Lambda(\bar{a}\#b)(c) = \sum_{(a)(c)} \omega_0(a_{(H)} \otimes c_{(H)}) a_{(A)} c_{(A)} b,$$

and ω_0: $H \otimes H \to k$ is a Hopf pairing. An $\underline{\omega_0}$-Azumaya algebra is an H-comodule algebra which is finite projective and faithful as a k-module and for which Γ, Λ are isomorphisms [4, (4.2)]. End(M) is ω_0-Azumaya, if M is an H-comodule which is finite projective and faithful as a k-module. If A and B are ω_0-Azumaya algebras, then so are A#B and $\bar{A}$ [4, (4.3)]. In the category of ω_0-Azumaya algebras, we define $A \sim B$ if there exist k-finite projective and faithful H-comodules M, N such that

$$A\#End(M) \simeq B\#End(N)$$

as H-comodule algebras. The equivalence classes of ω_0-Azumaya algebras form a group $B_{\omega_0}(k,H)$ with multiplication induced by $\#_{\omega_0}$ and inverse induced by $A \mapsto \bar{A}$ [4, (4.4), (4.5)].

Consider the Hopf pairing

$$\Omega: (F \otimes H) \otimes (F \otimes H) \to k$$

given by $\Omega(a \otimes x \otimes b \otimes y) = \omega(a \otimes y)\varepsilon(x)\varepsilon(b)$. An Ω-Azumaya algebra is called an <u>F-H-ω-Azumaya algebra</u>, or simply an <u>F-H-Azumaya algebra</u>. We denote $B_\Omega(k, F \otimes H) = B_\omega(k,F,H)$.

If A and B are $F \otimes H$-comodule algebras, then $A\#_\Omega B = A\#_\omega B$ with respect to the underlying F-comodule and H-comodule structures. Each F-comodule algebra is an $F \otimes H$-comodule algebra with the trivial H-coaction, and this construction transforms into #, and Azumaya F-comodule algebras into F-H-Azumaya algebras, hence induces a homomorphism of groupoid $BC(k,F) \to B_\omega(k,F,H)$ which is injective [4, p.589]. A similar injective homomorphism $BC(k,H) \to B_\omega(k,F,H)$ also exists, and we have

$B(k) \subset BC(k,F) \cap BC(k,H)$.

If k is a field, finite dimensional <u>H-dimodule algebras</u> are identified with finite dimensional $H^\circ \otimes H$-comodule algebras. Thus H-Azumaya H-dimodule algebras are the same as our H°-H-Azumaya algebras, and we have the isomorphism

$$BD(k,H) \cong B_\gamma(k,H^\circ,H)$$

where $\gamma: H^\circ \otimes H \to k$ is the canonical Hopf pairing.

Let k be a field. Then $\omega: F \otimes H \to k$ induces two Hopf algebra maps $\omega': H \to F^\circ$ and $\omega'': F \to H^\circ$. The Hopf algebra map $\omega'' \otimes 1: F \otimes H \to H^\circ \otimes H$ makes each $F \otimes H$-comodule algebra an $H^\circ \otimes H$-comodule algebra. This construction transforms the smash product $\#_\omega$ into $\#_\gamma$, and preserves the Γ- and Λ-homomorphisms. Hence F-H-Azumaya algebras are H°-H-Azumaya algebras, and a homomorphism of groups

$$B_\omega(k,F,H) \to B_\gamma(k,H^\circ,H) = BD(k,H)$$

is induced.

The structure of F-H-Azumaya algebras are as follows.

<u>Theorem 3.3</u>. Let k be a field, and let one of $Sp\,F$ and $Sp\,H$ be prosmooth. Then F-H-Azumaya algebras are semisimple.

<u>Theorem 3.4</u>. Let k be a field. Suppose that one of the affine groups $Sp\,F$ and $Sp\,H$ is prosmooth and the one or the other is connected. Then all F-H-Azumaya algebras are central simple.

Since F-H-Azumaya algebras are H°-H-Azumaya and F-F°-Azumaya, we have the following:

<u>Corollary 3.5</u>. Let k be a field. Suppose that a prosmooth group and a connected group appear in the four affine groups *Sp* F, *Sp* F°, *Sp* H, *Sp* H°. (We include the case when one group is prosmooth and connected.) Then all F-H-Azumaya algebras are Azumaya algebras.

Assume that all F-H-Azumaya algebras are Azumaya k-algebras. If A is an Azumaya F-comodule algebra, and B an Azumaya H-comodule algebra, then A#B is an Azumaya algebra, since $BC(k,F) \cup BC(k,H) \subset B_\omega(k,F,H)$. Hence the class of Azumaya $F \otimes H$-comodule algebra are closed under the product #. Since the product is compatible with the Brauer equivalence, a monoid structure is induced on $BC(k,F \otimes H)$. Similarly, if all ω_0-Azumaya algebras are Azumaya, the class of Azumaya H-comodule algebras are closed under $\#_{\omega_0}$, hence $BC(k,H)$ is a monoid with multiplication induced by $\#_{\omega_0}$.

<u>Proposition 3.6</u>. With the above hypothesis, the group $B_\omega(k,F,H)$ is the group of units of the monoid $BC(k,F \otimes H)$. The group $B(k)$ is contained in the center of it. Similarly, the group $B_{\omega_0}(k,H)$ is the group of units of the monoid $BC(k,H)$.

<u>Theorem 3.7</u>. Suppose that the class of Azumaya H-comodule algebras are closed under $\#_{\omega_0}$, and that $\kappa(\alpha,\beta)$ (with respect to ω_0) is an isomorphism for each $\alpha,\beta \in \mathrm{Ext}_{\mathrm{cent}}(Sp\ H,\mu)$. Then the map $\pi\colon BC(k,H) \to \mathrm{Ext}_{\mathrm{cent}}(Sp\ H,\mu)$ is a homomorphism of monoid, with kernel $B(k)$.

Applying the above to $\Omega: (F\otimes H)\otimes(F\otimes H) \to k$, we have the following

Theorem 3.8. Assume the following two conditions are satisfied:

i) If A is an Azumaya F-comodule algebra and B an Azumaya H-comodule algebra, then $A\#_\omega B$ is an Azumaya algebra.

ii) $\kappa(\alpha,\beta)$ (with respect to ω) is isomorphic, for each $\alpha \in \mathrm{Ext}_{\mathrm{cent}}(Sp\ F,\mu)$ and $\beta \in \mathrm{Ext}_{\mathrm{cent}}(Sp\ H,\mu)$.

Then, we have an exact sequence of monoids

$$1 \to B(k) \xrightarrow{i} BC(k,F\otimes H) \xrightarrow{\pi} \mathrm{Ext}_{\mathrm{cent}}(Sp\ F \times Sp\ H,\mu).$$

If all F-H-Azumaya algebras are Azumaya, then i) follows and the above induces an exact sequence of groups

$$1 \to B(k) \xrightarrow{i} B_\omega(k,F,H) \xrightarrow{\pi} U(\mathrm{Ext}_{\mathrm{cent}}(Sp\ F \times Sp\ H,\mu))$$

where $U(M)$ denotes the group of units of the monoid M.

If k is a field, then the condition i) implies ii) there.

In [1] Beattie constructs a split exact sequence

$$1 \to B(k) \to BM(k,H) \to \mathrm{Gal}(k,H) \to 1$$

where H is a k-finite projective, commutative and cocommutative Hopf k-algebra, $\mathrm{Gal}(k,H)$ the group of Galois H-objects. Since $\mathrm{Gal}(k,H) \approx \mathrm{Ext}_{\mathrm{cent}}(Sp^*H,\mu)$ and $BM(k,H) = BC(k,H^*)$, the above gives an exact sequence

$$1 \to B(k) \to BC(k,H^*) \xrightarrow{\pi} \mathrm{Ext}_{\mathrm{cent}}(Sp\ H^*,\mu) \to 1.$$

Then we can show that $\pi' = -\pi$ with the notation of Th.3.2.

References

[1] M. Beattie: A direct sum decomposition for the Brauer group of H-module algebras, J. Algebra 43 (1976), 686-693.

[2] N. Bourbaki: Algèbre, Chap. 8, Hermann, Paris, 1958.

[3] M. Demazure and P. Gabriel: Groupes algébriques (Tome I), North Holland Publishing Co. Amsterdam, 1970.

[4] F. W. Long: The Brauer group of dimodule algebras, J. Algebra 31 (1974), 559-601.

[5] M. Sweedler: Hopf algebras, W. A. Benjamin, Inc. New York, 1969.

[6] M. Takeuchi: On extensions of affine groups by μ^A, Com. Algebra, to appear.

[7] M. Takeuchi: On extensions of formal groups by μ^A, Com. Algebra, to appear.

[8] M. Takeuchi: Formal schemes and groups over fields, Com. Algebra 15, to appear.

[9] M. Takeuchi: The #-product of group sheaf extensions applied to Long's theory of dimodule algebras, Algebra-Berichte, to appear.

ON DOMINANT MODULES AND DOMINANT RINGS

Yutaka KAWADA
Kyoto Technical University

In [11] Kato introduced a notion of dominant modules: Let A be a ring, W_A a faithful, finitely generated projective module, and $B = \mathrm{End}(W_A)$ the endomorphism ring of W_A. Then he called W_A dominant if ${}_BW$ is lower distinguished, i.e. contains a copy of each simple right B-module, and further obtained a categorical characterization of a dominant module [11] and a structure theorem for a ring having a dominant module [12]. Rutter [26] also obtained another characterization on a dominant module.

In this paper we shall cast its finite generation out of the definition of dominant modules; that is, a faithful projective module W_A with $B = \mathrm{End}(W_A)$ is called a dominant module provided every simple factor module of ${}_BW$ is embedded into $S({}_BW)$, the socle of ${}_BW$ (and at the same time, in fact, each simple component of $S({}_BW)$ is isomorphic to a simple factor module of ${}_BW$). Our definition coincides with the original for the case where W_A is finitely generated, because then ${}_BW$ is a generator and so is upper distinguished, i.e. every simple right B-module is isomorphic to a simple factor module of ${}_BW$. A ring A will be called right(resp. left) dominant if there exists a dominant right (resp. left) A-module. In particular, in case A has a finitely generated, dominant module, A will be called a right (resp. left) dominant ring of finite type.[1)]

The requirement to extend the definition of dominant modules has been motivated by the next:

<u>Theorem 5.7.</u> Let A be a ring. Then A is an endomorphism ring of a generator-cogenerator, say ${}_BW$, if and only if A satisfies the next three conditions:

(i) $A = Q_\ell$, the maximal left quotient ring of A itself.

(ii) A is a right dominant ring of finite type.

(iii) A is a left $\aleph$-QF 3 ring. (Its definition will be stated later and of course A is a left dominant ring.)

Moreover, B has only finitely many isomorphism classes of simple left B-modules if and only if A becomes a left QF 3 ring in (iii) above mentioned.

This theorem is a generalization of a result of Ringel and Tachikawa [24] concerning the endomorphism ring of a linearly compact generator-cogenerator.

The purpose of this paper is to investigate not only dominant modules but also dominant rings in our sense. To do so, as a preliminary § 1 is devoted to establish Theorem 1.1 concerning locally projective modules, which will play an important rôle on characterizing dominant modules, and which will be interesting by itself.

---

1) A right (resp. left) dominant ring differs from a dominant ring defined in [28, p. 226].

In § 2, main results obtained by Kato [11, 12] and Rutter [26] will be extended to our case. In particular we shall establish two criteria on dominant modules: The first (Theorem 2.1) contains an extension of the characterization due to Rutter, which asserts that a projective module W_A is dominant if and only if $Tr(W_A)$, the trace ideal of W_A, is the smallest dense left ideal of A. The second (Theorem 2.2) contains an extension of the categorical characterization due to Kato, which asserts that a projective module W_A with $B = End(W_A)$ is dominant if and only if the functor $Hom_B({}_BW_A, -)$ and ${}_BW_A \otimes -$ induce an equivalence $\mathcal{G}({}_BW) \sim \mathcal{D}(E({}_AA))$, where $E({}_AA)$ denotes the injective hull of ${}_AA$ and $\mathcal{G}({}_BW)$ (resp. $\mathcal{D}(E({}_AA))$) denotes the full subcategory consisting of all left B-modules generated by ${}_BW$ (resp. of all left A-modules with $E({}_AA)$-dominant dimension ≥ 2).

In § 3, we shall state an intrinsic characterization of right dominant rings (Theorem 3.1) and show that the property of rings to be right dominant is Morita-invariant (Proposition 3.3).

In § 4, we shall treat a special but a useful right (resp. left) dominant ring: A ring A will be called right pseudo-perfect provided there are pairwise non-isomorphic, local idempotents $\{e_\lambda \mid \lambda \in \Lambda\}$ of A such that $[\sum_\lambda \oplus e_\lambda A]_A$ is dominant. Then it is remarkable that, in the above, $\sum_\lambda \oplus e_\lambda A$ is dominant if and only if $\sum_\lambda \oplus e_\lambda A$ is faithful and the distinct simple components of $S({}_AA)$ coincide with $\{Ae_\lambda/Je_\lambda \mid \lambda \in \Lambda\}$ up to multiplicity where $J = J(A)$, the

Jacobson radical of A (Theorem 4.1), and that $\sum_\lambda \oplus e_\lambda A$ is minimal dominant, i.e. is isomorphic to a direct summand of any dominant module and so is uniquely determined up to isomorphism (Proposition 4.3). A property of rings to be right pseudo-perfect is Morita-invariant (Proposition 4.5).

The class of right pseudo-perfect rings contains semi-perfect rings with essential left socle (and so right perfect rings) as well as right QF 3 rings, and another example will be given by the endomorphism rings of upper distinguished cogenerators (Theorem 4.7).

In §5, we shall treat a more special right(resp. left) pseudo-perfect ring: A ring A will be called right $\aleph$-QF 3 if there exist pairwise orthogonal and pairwise non-isomorphic, local idempotents $\{e_\lambda \mid \lambda \in \Lambda\}$ of A such that each $e_\lambda A$ $(\lambda \in \Lambda)$ is an injective module with a simple socle, and that $[\sum_\lambda e_\lambda A]_A$ is faithful. Similarly left $\aleph$-QF 3 rings are defined. In case the cardinal of Λ is finite, this is nothing else a right (resp. left) QF 3 ring.

Then, in the above, $\sum_\lambda e_\lambda A$ is minimal dominant and the simple components of $S({}_A A)$ as well as $S(A_A)$ are completely determined up to multiplicity (Theorem 5.1), and an analogue of Colby and Rutter [5] concerning right QF 3 rings holds good (Proposition 5.4). Of course a property of rings to be right $\aleph$-QF 3 is Morita-invariant. As an important example of right (resp. left) $\aleph$-QF 3 rings we have the endomorphism ring of a generator-cogenerator (Theorem 5.7) as was stated before.

Throughout this paper rings and modules will be assumed to be unitary, and for a right A-module M we shall denote by $E(M_A)$, $J(M_A)$, $S(M_A)$, $Tr(M_A)$, $End(M_A)$ and by $Biend(M_A)$ respectively the injective hull, the Jacobson radical, the socle, the trace ideal, the endomorphism ring and the bi-endomorphism ring (i.e. the double centralizer) of M_A. For subsets $X \subset A$ and $Y \subset M_A$ we shall denote by $r_X(Y)$ and $\ell_Y(X)$ respectively the right annihilator of Y in X and the left annihilator of X in Y, i.e.

$$r_X(Y) = \{x \in X \mid Yx = 0\} \quad \text{and} \quad \ell_Y(X) = \{y \in Y \mid yX = 0\} .$$

Similarly these notations will be used for a left A-module M. ${}_A\mathcal{M}$ (resp. $\mathcal{M}_A$) will always denote the category of all left (resp. right) A-modules.

1. Preliminary (locally projective modules). The present section is devoted to establish Theorem 1.1 concerning locally projective modules, which will play an important rôle on characterizing dominant modules, and which will be interesting by itself.

Theorem 1.1. Let W_A be a locally projective module with $B = End(W_A)$, and set $T = Tr(W_A)$, $R = Tr({}_BW)$ and $W^* = Hom_A(W_A, A_A)$. Denote by $\mathcal{S}({}_AA)$ and $\mathcal{S}({}_BB)$ respectively the family consisting of all isomorphism classes of simple left A-modules M with $TM = M$, and of simple left B-modules N with $RN = N$. Then there exists a bijection between $\mathcal{S}({}_AA)$ and $\mathcal{S}({}_BB)$, via

$${}_AM \longmapsto {}_BW \otimes_A M, \qquad M \in \mathcal{S}({}_AA)$$

$$ {}_AW^* \otimes_B N/J({}_AW^* \otimes_B N) \longleftarrow {}_BN, \qquad N \in S({}_BB) \ . $$

Moreover, $S({}_AA)$ and $S({}_BB)$ respectively coincide with the families consisting of all isomorphism classes of simple factor modules of ${}_ATW^*$, and of simple factor modules of ${}_BW$.

2. Dominant modules. As was stated in the introduction, we shall extend the definition of dominant modules as follows: A faithful projective module W_A with $B = \mathrm{End}(W_A)$ is said to be dominant provided every simple fator module of ${}_BW$ is embedded into $S({}_BW)$. In case W_A is finitely generated this coincides with the original. In this section we shall establish two characterizations of dominant modules (Theorems 2.1 and 2.2) and prove several properties of dominant modules, which contain the extensions of the results of Kato [11, 12, 13] and Rutter [26].

Theorem 2.1. Let W_A be a projective module with $B = \mathrm{End}(W_A)$ and set respectively $T = \mathrm{Tr}(W_A)$ and $R = \mathrm{Tr}({}_BW)$. Then the following statements are equivalent:

(a) W_A is dominant.

(b) W_A is faithful, and $RN = N \Rightarrow N \hookrightarrow S({}_BW)$ for simple left B-modules N.

(c) W_A is faithful, and $TM = M \Rightarrow M \hookrightarrow S({}_AA)$ for simple left A-modules M.

(d) W_A is faithful, and $r_A(X) = 0 \Rightarrow W = WX$ for maximal left ideals X of A.

(e) T is the smallest dense left ideal of A.

Moreover, in the above statements (b), (c) and (d), "$\Longrightarrow$" may be replaced by "$\Longleftrightarrow$".

Remark. In case W_A is finitely generated projective, Rutter obtained (a) $\Longleftrightarrow$ (e) [26, Theorem 1.4].

Following Kato [13], for a right ideal I of A, we shall call a left A-module M I-injective if the functor $\mathrm{Hom}_A(-, {}_AM)$ is exact on all short exact sequences (in ${}_A\mathcal{M}$) $0 \to X' \to X \to X'' \to 0$ with $IX'' = 0$. Evidently ${}_AM$ is I-injective if and only if $\mathrm{Ext}^1_A(X,M) = 0$ for every left A-module X with $IX = 0$.

Following Tachikawa [30], for an injective module ${}_AE$, a left A-module M is said to be E-dom.dim $M \geq n$ if there exists an exact sequence

$$0 \to M \to E_1 \to \dots \to E_n$$

where each E_i $(i = 1, \dots, n)$ is a direct product of copies of E.

Now, we can state the second criterion on dominant modules.

Theorem 2.2. Let W_A be a projective module with $B = \mathrm{End}(W_A)$, and set $T = \mathrm{Tr}(W_A)$ and $R = \mathrm{Tr}({}_BW)$ respectively. Then the following statements are equivalent:

(a) W_A is dominant.

(b) $\mathcal{D}(E({}_AA)) = {}_T\mathcal{L}$, where $\mathcal{D}(E({}_AA))$ and ${}_T\mathcal{L}$ denote respectively the full subcategory of ${}_A\mathcal{M}$ such as

$$\mathcal{D}(E({}_AA)) = \{{}_AM \mid E({}_AA)\text{-dom.dim } M \geq 2\}$$

and

$$_{T}\mathcal{L} = \{_A M \mid {}_A M \text{ is T-injective and } r_M(T) = 0\}.$$

(c) The functors $\mathrm{Hom}_B({}_B W_A, -): {}_B\mathcal{M} \to {}_A\mathcal{M}$ and ${}_B W_A \otimes - :$ ${}_A\mathcal{M} \to {}_B\mathcal{M}$ induce an equivalence

$$\mathcal{G}({}_B W) \sim \mathcal{D}(E({}_A A)),$$

where $\mathcal{G}({}_B W)$ denotes the full subcategory of ${}_B\mathcal{M}$ generated by ${}_B W$, i.e. $\mathcal{G}({}_B W) = \{{}_B N \mid RN = N\}$.

<u>Remark.</u> In case W_A is (faithful) finitely generated projective, $\mathcal{G}({}_B W) = {}_B\mathcal{M}$ and Kato obtained (a) $\Leftrightarrow$ (c) [11, Theorem 1] and observed (a) $\Leftrightarrow$ (b) (cf. [13, Corollary 7.3]).[2)]

From Theorem 2.1 several properties on dominant modules will be deduced. The next is an extension of Kato [10, Corollary 5].

<u>Corollary 2.3.</u> Let W_A be a dominant module with $Q =$ $\mathrm{Biend}(W_A)$. Then Q is the maximal left quotient ring of A.

For left (or right) A-modules L_1 and L_2, define $L_1 \overset{W}{\sim} L_2$ (resp. $L_1 \sim L_2$) if each of L_1 and L_2 is isomorphic to a direct summand of a direct sum (resp. a finite direct sum) of copies of the other. Then the next is an extension

---

2) Recently I have received a preprinit [22] from K. Nishida. He also has obtained (a') $\Rightarrow$ (c) independently. Here (a') implies the case where W_A is faithful, locally projective and where every simple factor module of ${}_B W$ is embedded into $S({}_B W)$. (However, replacing (a) by (a'), Theorem 2.1 is valid and so is Theorem 2.2 for a locally projective W_A.)

of Rutter [26, Corollary 1.6].

Corollary 2.4. Let W_A be a dominant module and V_A a given module. Then V_A is dominant if and only if $V_A \overset{w}{\sim} W_A$.

The following is also an extension of Kato [12, Remark 2].

Corollary 2.5. Let W_A be a dominant module. Then ${}_A[E(S({}_AA))]$ is faithful.

Finally, for a projective module W_A with a dual basis $\{u_\lambda, f_\lambda \mid \lambda \in \Lambda\}$, we shall call $\sum_{\lambda\in\Lambda} f_\lambda(W)$ the right pretrace ideal of W_A associated with $\{u_\lambda, f_\lambda \mid \lambda \in \Lambda\}$. This depends on the choice of its dual basis.

Proposition 2.6. Let W_A be a dominant module with a right pretrace ideal T_0 and Q the maximal left quotient ring of A, and set $A_0 = \mathbb{Z}1_A + T_0$ where $\mathbb{Z}$ denotes the ring of rational integers. Then, for any subring C of Q containing A_0, W_C is a dominant module with $CT_0 = \mathrm{Tr}(W_C)$ and with $Q = \mathrm{Biend}(W_C)$, and hence CT_0 is the smallest dense left ideal of C, Q is a maximal left quotient ring of C and Q_C is torsionless.

3. Dominant rings. As was stated in the introduction, a ring A is said to be right (resp. left) dominant if there exists a dominant right (resp. left) A-module. In particular A is called a right (resp. left) dominant ring of finite type

if there exists a finitely generated, dominant right (resp. left) A-module.

As for dominant rings it seems to the author until hitherto there is no intrinsic characterization (cf. [12, Theorem 1]). But using (e) in Theorem 2.1 it is readily obtained.

Theorem 3.1. A ring A is right dominant if and only if A has the smallest dense left ideal T and there exist elements $t_{\lambda\mu}$ in T, $(\lambda, \mu) \in \Lambda \times \Lambda$, with an index set Λ, satisfying the next three conditions:

(i) For each $\mu \in \Lambda$, $t_{\lambda\mu} = 0$ for almost all $\lambda \in \Lambda$.

(ii) $\sum_{\mu\in\Lambda} t_{\lambda\mu}t_{\mu\nu} = t_{\lambda\nu}$ for every $(\lambda, \nu) \in \Lambda \times \Lambda$.

(iii) $T = \sum_{\lambda,\mu\in\Lambda} At_{\lambda\mu}A$.

In particular, A is right dominant of finite type if and only if there exists a finite index set Λ in the above.

The next is a direct consequence of Proposition 2.6.

Corollary 3.2. Let A be a right dominant ring, T the smallest dense left ideal of A, and $t_{\lambda\mu}$, $(\lambda, \mu) \in \Lambda \times \Lambda$, the elements of T satisfying (i), (ii) and (iii) in Theorem 3.1. Further let Q be the maximal left quotient ring of A, and set respectively $T_0 = \sum_{\lambda,\mu} t_{\lambda\mu}A$ and $A_0 = \mathbb{Z}1_A + T_0$. Then any subring C of Q containing A_0 is a right dominant ring, and further CT_0 is the smallest dense left ideal of C, Q is the maximal left quotient ring of C and Q_C is torsionless.

Proposition 3.3. A property of a ring to be right (or left) dominant is Morita-invariant.

4. Pseudo-perfect rings. Recall that an idempotent e of a ring A is said to be local provided eAe is a local ring; that is, eAe/eJe is a division ring where $J = J(A)$, the Jacobson radical of A. As is well-known, e is local $\Leftrightarrow$ Ae/Je is simple $\Leftrightarrow$ eA/eJ is simple.

Two idempotents e and f in A are said to be isomorphic to each other provided $eA \cong fA$. As is well known, $eA \cong fA \Leftrightarrow Ae \cong Af \Leftrightarrow Ae/Je \cong Af/Jf \Leftrightarrow eA/eJ \cong fA/fJ$.

Now, in this section we shall treat a special but a useful right (or left) dominant ring: A ring A is defined to be right pseudo-perfect if there are pairwise non-isomorphic, local idemporents $\{e_\lambda \mid \lambda \in \Lambda\}$ of A such that $[\sum_{\lambda\in\Lambda}\oplus\, e_\lambda A]_A$ is dominant. Similarly left pseudo-perfect rings will be defined.

Such a dominant module is characterized by the next

Theorem 4.1. Let A be a ring and $\{e_\lambda \mid \lambda \in \Lambda\}$ pairwise non-isomorphic, local idempotents of A. Then the following statements are equivalent:

(a) $[\sum_\lambda \oplus\, e_\lambda A]_A$ is dominant.

(b) $[\sum_\lambda \oplus\, e_\lambda A]_A$ is faithful and $Ae_\lambda/Je_\lambda \lhd S({}_AA)$ for every $\lambda \in \Lambda$, i.e. $\sum_{\lambda\in\Lambda}\oplus\, Ae_\lambda/Je_\lambda \overset{W}{\sim} S({}_AA)$.

(c) ${}_A[E(S({}_AA))]$ is faithful, and $\sum_{\lambda\in\Lambda}\oplus\, Ae_\lambda/Je_\lambda \overset{W}{\sim} S({}_AA)$.

Remark. In case Λ is a finite set, the equivalence (a) $\Leftrightarrow$ (c) was essentially obtained by Kato [12, Corollary].

As the equivalence (a) $\Leftrightarrow$ (b) in the above is useful, we shall restate it as follows:

Corollary 4.2. A ring A is right pseudo-perfect if and only if there exist pairwise non-isomorphic, local idempotents $\{e_\lambda \mid \lambda \in \Lambda\}$ of A such that $S({}_A A) \overset{w}{\sim} \sum_{\lambda \in \Lambda} \oplus Ae_\lambda / Je_\lambda$ and $[\sum_{\lambda \in \Lambda} e_\lambda A]_A$ is faithful.

In view of Corollary 4.2, the implication below is valid: right perfect rings $\Rightarrow$ semiperfect rings with essential left socle $\Rightarrow$ right pseudo-perfect rings (of finite type), which will justify the denomination of "right pseudo-perfect".

In case A is a right (or left) dominant ring, a dominant module is called minimal dominant provided it is isomorphic to a direct summand of any dominant module.

Proposition 4.3. Let A be a right (or left) pseudo-perfect ring. Then A has a minimal dominant module. Moreover a minimal dominant module is uniquely determined within isomorphism.

As for the endomorphism ring of a minimal dominant module we have the next

Proposition 4.4. Let A be a right pseudo-perfect ring with the minimal dominant module $W_A = \sum_{\lambda \in \Lambda} \oplus e_\lambda A$ where

$\{e_\lambda \mid \lambda \in \Lambda\}$ are the same as in the definition, and assume $S({}_A A) \overset{w}{\sim} \sum_{\lambda \in \Lambda} \oplus S(Ae_\lambda)$. Let us set $B = \mathrm{End}(W_A)$. Then B is a right pseudo-perfect ring with a minimal dominant module $\sum_{\lambda \in \Lambda} \oplus E_\lambda B$ and with $S({}_B B) \overset{w}{\sim} \sum_{\lambda \in \Lambda} \oplus S(BE_\lambda)$, where $\{E_\lambda \mid \lambda \in \Lambda\}$ are pairwise non-isomorphic, local idempotents of B.

Apparently we may send away local idempotents out of the definition of right pseudo-perfect rings, which will be done by using the notion of a projective cover (cf. [3]).

Proposition 4.5. A ring A is right pseudo-perfect if and only if there are pairwise non-isomorphic, simple right A-modules M_λ $(\lambda \in \Lambda)$ such that each M_λ has a projective cover P_λ and $[\sum_{\lambda \in \Lambda} \oplus P_\lambda]_A$ is dominant. Accordingly, a property of a ring to be right pseudo-perfect is Morita-invariant.

Proposition 4.6. Let A be a right pseudo-perfect ring with the minimal dominant module $\sum_{\lambda \in \Lambda} \oplus e_\lambda A$ stated in the definition. Denote by A_0 and Q respectively the ring $\mathbb{Z}1_A + \sum_{\lambda \in \Lambda} e_\lambda A$ and the maximal left quotient ring of A. Then any subring C of Q containing A_0 is right pseudo-perfect.

Now following Azumaya [2], a left B-module N is called upper distinguished if every simple left B-module is isomorphic to a simple factor module of ${}_B N$. Then we have the next

Theorem 4.7. Let ${}_B W$ be an upper distinguished cogenerator with $A = \mathrm{End}({}_BW)$. Then A is a left pseudo-perfect ring.

5. ℵ-QF 3 rings. As was stated in the introduction, in order to establish an intrinsic characterization of the endomorphism ring of a generator-cogenerator we shall extend the notion of a right (resp. left) QF 3 ring: A ring A is defined to be right ℵ-QF 3 if there exist pairwise orthogonal and pairwise non-isomorphic, local idempotents $\{e_\lambda \mid \lambda \in \Lambda\}$ of A such that each $e_\lambda A$ $(\lambda \in \Lambda)$ is an injective module with a simple socle, and that $[\sum_{\lambda \in \Lambda} e_\lambda A]_A$ is faithful.[3] Similarly left ℵ-QF 3 rings will be defined.

As for the structure of a right ℵ-QF 3 ring we have the next

Theorem 5.1. Let A be a right ℵ-QF 3 ring. Then the following assertions are valid.

(i) A right ℵ-QF 3 ring is a right pseudo-perfect ring. More precisely, $[\sum_{\lambda \in \Lambda} e_\lambda A]_A$ stated in the definition is nothing else a minimal dominant module and is uniquely determined within isomorphism.

(ii) $S({}_AA) \overset{w}{\sim} \sum_{\lambda \in \Lambda} \oplus Ae_\lambda / Je_\lambda$, $S(A_A) \overset{w}{\sim} \sum_{\lambda \in \Lambda} \oplus S(e_\lambda A) \subset r_A(J)$ where $J = J(A)$, and $S(e_\lambda A) \not\cong S(e_\lambda A)$ if $\lambda \neq \mu$.

(iii) $E(S({}_AA))$ is faithful, $E(A_A)$ is torsionless, and $Q_r \subset Q_\ell$ where Q_r (resp. Q_ℓ) denotes the maximal right (resp. left) quotient ring of A.

---

3) ℵ represents the cardinal (finite or infinite) of Λ.

Remark. In case A is a right QF 3 ring, $Q_r \subset Q_\ell$ in (iii) was first obtained by Ringel and Tachikawa [24, Lemma 1.4].

Recall that a ring A is called right QF 3 if it has a minimal faithful right A-module; that is, a faithful module which is isomorphic to a direct summand of every faithful module. Obviously a right $\aleph$-QF 3 ring of finite type is nothing else a right QF 3 ring (cf. [5, Theorem 1]), and then a minimal dominant module coincides with a minimal faithful module (cf. [26, Corollary 1.2], [12, Example 1]).

The next means a "minimal faithfulness" of a minimal dominant module.

Corollary 5.2. Let A be a right $\aleph$-QF 3 ring and W_A a minimal dominant module. Then,

(i) $W_A \lessdot M_A$ for every faithful module M_A.

(ii) Any deletion of a non-zero direct summand out of W_A amounts to a loss of its faithfulness.

The former half of the following is well known for artinian QF 3 rings.

Corollary 5.3. Let A be both a right and a left $\aleph$-QF 3 ring (i.e. $\aleph$-QF 3 ring), and let $\sum_{\lambda\in\Lambda} e_\lambda A$ and $\sum_{\gamma\in\Gamma} Af_\gamma$ be respectively the minimal dominant module stated in the definition. Then there is a bijection π of Λ onto Γ such that

$S(e_\lambda A) \cong f_{\pi(\lambda)}A/f_{\pi(\lambda)}J$ and $S(Af_{\pi(\lambda)}) \cong Ae_\lambda/Je_\lambda$, and $Q_r = Q_\ell$ where Q_r (resp. Q_ℓ) denotes the maximal right (resp. left) quotient ring of A.

The following gives a criterion on a right $\aleph$-QF 3 ring, which is an analogue of Colby and Rutter [5, Theorem 1].

Proposition 5.4. Let A be a ring. Then A is a right $\aleph$-QF 3 ring if and only if there are pairwise non-isomorphic, simple right A-modules $\{M_\lambda \mid \lambda \in \Lambda\}$ such that $[\sum_{\lambda \in \Lambda}\oplus E(M_\lambda)]_A$ is faithful and projective. Furthermore, in this case $S(A_A) \overset{w}{\sim} \sum_{\lambda \in \Lambda}\oplus M_\lambda$ holds.

Corollary 5.5. The property of a ring to be right (resp. left) $\aleph$-QF 3 is Morita-invariant.

The next is a slight extension of a portion of Tachikawa [32, Proposition 4.3].

Proposition 5.6. Let A be a right $\aleph$-QF 3 ring and Q_r the maximal right quotient ring of A. Then any subring C of Q_r containing A is a right $\aleph$-QF 3 ring.

Remark. Compare this with Proposition 4.6. The distinction between them will imply a peculiarity of $\aleph$-QF 3 rings.

At last we shall establish a structure theorem on endomorphism rings of generator-cogenerators, which is a natural generalization of Ringen and Tachikawa [24, Theorem 2.1], and which will supply us many examples of left (or right) $\aleph$-QF 3 rings.

Theorem 5.7. Let A be a ring. Then A is an endomorphism ring of a generator-cogenerator, say ${}_BW$, if and only if A satisfies the following three conditions:

(i) $A = Q_\ell$, the maximal left quotient ring of A.

(ii) A is a right dominant ring of finite type.

(iii) A is a left $\aleph$-QF 3 ring.

Moreover, B has only finitely many isomorphism classes of simple left B-modules if and only if A becomes a left QF 3 ring in (iii) above mentioned.

Remark. Another characterization on endomorphism rings of generator-cogenerators was obtained by Tachikawa [30, Theorem 4], Kato [11, Example 3] and by Morita [21, Corollary 8.4] respectively. Their characterizations are rather categorical than ours.

In Theorem 5.7 ${}_BW$ is not uniquely determined in view of Corollary 2.6. However the next holds:

Corollary 5.8. Let ${}_{B'}W'$ as well as ${}_BW$ be a generator-cogenerator with $A = \mathrm{End}({}_BW) \cong \mathrm{End}({}_{B'}W')$. Then there is an equivalence $F: {}_B\mathcal{M} \sim {}_{B'}\mathcal{M}$ with $F(W) = W'$.

The following are direct consequences of Theorem 5.7, and Corollary 5.9 has been observed by Kato, too.

Corollary 5.9. Let B be a semiperfect ring and ${}_BW$ a generator-cogenerator. Then $A = \mathrm{End}({}_BW)$ is a left QF 3 ring.

Corollary 5.10 (cf. Sugano [29]). Let A be a ring. Then ${}_AA$ is a cogenerator if and only if A is a left $\aleph$-QF 3 ring with a lower distinguished, minimal dominant module. Moreover, in this case $A = Q_\ell$, the maximal left quotient ring of A itself.

This is an abstract of the paper "On dominant modules and dominant rings", which will be published elsewhere.

References

[0] F. W. Anderson and E. A. Rutter, Jr.: Rings and Categories of Modules, GMT 13, Springer, 1973.

[1] G. Azumaya: Corrections and supplementaries to my paper concerning Remak-Krull-Schmidt's theorem, Nagoya Math. J. 1 (1950), 117-124.

[2] G. Azumaya: Completely faithful modules and self-injective rings, Nagoya Math. J. 27 (1966), 697-708.

[3] H. Bass: Finitistic dimension and a homological generalization of semi-primary rings, Trans. Amer. Math. Soc. 95 (1960), 466-488.

[4] N. Bourbaki: Algèbre Commutative, Chap. 1 et 2, Hermann, 1961.

[5] R. R. Colby and E. A. Rutter, Jr.: QF-3 rings with zero singular ideal, Pacific J. Math. 28 (1969), 303-308.

[6] C. Faith: Lectures on Injective Modules and Quotient Rings, Lecture Notes in Math. 49, Springer, 1967.

[7] C. Faith: Algebra: Rings, Modules and Categories I, Grund. Math. Wiss. 190, Springer, 1973.

[8] P. Gabriel: Des catégories abeliennes, Bull. Soc. Math. France 90 (1962), 323-448.

[9] G. S. Garfinkel: Universally torsionless and trace module, Trans. Amer. Math. Soc. 215 (1976), 119-144.

[10] T. Kato: U-dominant dimension and U-localization (unpublished).

[11] T. Kato: Dominant modules, J. Algebra 14 (1970), 341-349.

[12] T. Kato: Structure of dominant modules, J. Algebra 39 (1976), 563-570.

[13] T. Kato: Duality between colocalization and localization (to appear).

[14] T. Kato: Morita contexts and equivalences (to appear).

[15] Y. Kawada: A note on cogenerators in the category of modules, Proc. Japan Acad. 48 (1972), 470-473.

[16] J. Lambek: On Utumi's ring of quotients, Canad. J. Math. 15 (1963), 363-370.

[17] J. Lambek: Torsion Theories, Additive Semantics and Rings of Quotients, Lecture Notes in Math. 177, Springer, 1971.

[18] K. Masaike: On quotient rings and torsionless modules, Sci. Rep. Tokyo Kyoiku Daigaku A 11 (1971), 26-30.

[19] K. Morita: Duality for modules and its applications to the theory of rings with minimum condition, Sci. Rep. Tokyo Kyoiku Daigaku A 6 (1958), 83-142.

[20] K. Morita: A theorem on Frobenius extensions, Sci. Rep. Tokyo Kyoiku Daigaku A 10 (1969), 79-87.

[21] K. Morita: Localizations in categories of modules I, Math. Z. 114 (1970), 121-144.

[22] K. Nishida: Category equivalences and locally projective modules (to appear).

[23] B. L. Osofsky: A generalization of quasi-Frobenius rings, J. Algebra 4 (1966), 373-387.

[24] C. M. Ringel and H. Tachikawa: QF-3 rings, J. Reine Angew. Math. 272 (1975), 49-72.

[25] E. A. Rutter, Jr.: PF-modules, Tôhoku Math. J. 23 (1971), 201-206.

[26] E. A. Rutter, Jr.: Dominant modules and finite localizations, Tôhoku Math. J. 27 (1975), 225-239.

[27] B. Stenström: Rings and Modules of Quotients, Lecture Notes in Math. 273, Springer, 1971.

[28] B. Stenström: Rings of Quotients, Grund. Math. Wiss. 217, Springer, 1975.

[29] K. Sugano: A note on Azumaya's theorem, Osaka J. Math. 4 (1967), 157-160.

[30] H. Tachikawa: On splitting of module categories, Math. Z. 111 (1969), 145-150.

[31] H. Tachikawa: On left QF-3 rings, Pacific J. Math. 32 (1970), 255-268.

[32] H. Tachikawa: Quasi-Frobenius Rings and Generalizations, Lecture Notes in Math. 351, Springer, 1973.

[33] Y. Utumi, On quotient rings, Osaka J. Math. 8 (1956), 1-18.

[34] R. B. Warfield, Jr.: A Krull-Schmidt theorem for infinite sums of modules, Proc. Amer. Math. Soc. 22 (1969), 460-465.

[35] B. Zimmermann-Huisgen: Pure submodules of direct products of free modules, Math. Ann. 224 (1976), 233-245.

ON EQUIVALENCES BETWEEN MODULE CATEGORIES

Masahisa SATO
The University of Tsukuba

Introduction. Let ${}_AU_B$ be an A-B bimodule, and $T = - \otimes_A U$: Mod-A $\to$ Mod-B, $H = \mathrm{Hom}_B(U_B,-)$: Mod-B $\to$ Mod-A additive functors with canonical natural transformations $\Phi : TH \to 1_{\text{Mod-B}}$ and $\Psi : 1_{\text{Mod-A}} \to HT$. In a previous paper [5], we have studied the conditions of U_B, under which T and H induce category equivalences Mod-A ~ Im(T) and Mod-A ~ Gen(U_B) respectively.

In the present paper, we shall study the equivalences between certain full subcategories of Mod-A and Mod-B respectively. G. Azumaya has given an important example of this kind of equivalence, which says that if ${}_AU$ is a projective A-module and $B = \mathrm{End}({}_AU)$, then $\mathrm{Im}(T) = \mathrm{Gen}(U_B) = \overline{\mathrm{Gen}}(U_B)$ and $\Phi_M : TH(M_B) \to M_B$ is an isomorphism for any $M_B \in \mathrm{Gen}(U_B)$ [Azumaya Symposium held at Tokyo University of Education, September 1-2, 1975].

In this paper, we shall study more in detail two kinds of equivalences Im(H) ~ Im(T) and Im(H) ~ $\overline{\mathrm{Gen}}(U_B)$ respectively which are induced by functors T and H. In §1, we shall study the equivalence Im(H) ~ Im(T) induced by functors T and H, that is, there exist natural isomorphisms $u : TH \to 1_{\mathrm{Im}(T)}$ and $v : 1_{\mathrm{Im}(H)} \to HT$. But we shall show the above equivalence Im(H) ~ Im(T) holds if and only if one of the following conditions is satisfied. (1) There exists a natural isomorphism $u : TH \to 1_{Im(T)}$. (2) There exists a natural isomorphism $v : 1_{Im(H)} \to HT$. (3) $\Phi : TH \to 1_{Im(T)}$ is an isomorphism. (4) $\Psi : 1_{Im(H)} \to HT$ is an isomorphism. These proofs are categorical and enable us to see that they holds only under the situation $T : \mathcal{C} \to \mathcal{D}$, $H : \mathcal{D} \to \mathcal{C}$ are functors between categories $\mathcal{C}$ and $\mathcal{D}$ provided T is a left adjoint of H. In many papers, even when there exists a natural isomorphism $u : TH \to 1_{Im(T)}$, it seems that $Im(H)$ and $H(Im(T))$ are distinguished. We remark they are equal and for the criterion of the equivalence $Im(H) \sim Im(T)$, it is required only to calculate Φ or Ψ. As the categorical characterization of $Im(H) \sim Im(T)$, we prove $Im(H)$ (resp. $Im(T)$) is a coreflective subcategory (resp. reflective subcategory) of Mod-A (resp. Mod-B) with coreflector $HT : \text{Mod-A} \to Im(H)$ (resp. reflector $TH : \text{Mod-B} \to Im(T)$).

In §2, we shall study the equivalence $Im(H) \sim \overline{Gen}(U_B)$. As the generalization of Morita's results [3, Theorem 1.1] that T and H induce a category equivalence $Im(H) \sim \text{Mod-B}$ if and only if ${}_AU$ is of type FP and $B = End({}_AU)$, we get the following result: Let $C = End(U_B)$. T and H induce a category equivalence $Im(T) \sim \overline{Gen}(U_B)$ if and only if ${}_CC \otimes_A U_B \cong {}_CU_B$ (canonically) and U_B generates any submodule of direct sums of U_B. Furthermore several equivalent conditions using the property $Im(H) \sim Im(T)$ will be given in the theorem.

1. <u>The equivalence of $Im(H) \sim Im(T)$</u>. Throughout this paper, a ring means an associative ring with unit and Mod-R

denotes the category of unital right R-modules. For a bimodule ${}_AU_B$, we consider two additive functors, $T = - \otimes_A U : \text{Mod-}A \to \text{Mod-}B$ and $\text{Hom}_B(U_B,-) : \text{Mod-}B \to \text{Mod-}A$. We can consider their canonical natural transformations $\Phi : TH \to 1_{\text{Mod-}B}$ and $\Psi : 1_{\text{Mod-}A} \to HT$ defined by $\Phi_M(\sum f \otimes u) = \sum f(u)$ for any $f \in \text{Hom}_B(U_B,M_B)$ and $u \in U$, $(\Psi_N(n))(u) = n \otimes u$ for any $n \in N$ and $u \in U$. For functors T and H, we can also consider a natural isomorphism $\eta : \eta(N_A,M_B) : \text{Hom}_B(T(N_A),M_B) \to \text{Hom}_A(N_A,H(M_B))$ defined by $\{\eta(f)(n)\}(u) = f(n \otimes u)$ for any $f \in \text{Hom}_B(T(N_A),M_B)$, $n \in N_A$ and $u \in U_B$.

<u>Lemma 1.1</u>. The notations are as above. The following relations hold for any $N_A \in \text{Mod-}A$ and $M_B \in \text{Mod-}B$.

(1) $\eta(N_A,T(N_A))(1_{T(N_A)}) = \Psi_{N_A}$ and

$\eta^{-1}(H(M_B),M_B)(1_{H(M_B)}) = \Phi_{M_B}$.

(2) $\tilde{f} = H(\eta^{-1}(f))\cdot\Psi_{N_A}$ for any $f \in \text{Hom}_A(N_A,H(M_B))$, and

$g = \Phi_{M_B}\cdot T(\eta(g))$ for any $g \in \text{Hom}_B(T(N_A),M_B)$.

(3) $\Phi_{T(N_A)}\cdot T(\Psi_N) = 1_{T(N_A)}$ and $H(\Phi_{M_B})\cdot\Psi_{H(M_B)} = 1_{H(M_B)}$.

<u>Proof</u>. These can be proved by routine calculations.

A B-module M_B is called "U_B-codominant dimension $\geq n$" if there exists an exact sequence:

$$X_n \to X_{n-1} \to \cdots\cdots\cdots\cdots \to X_2 \to X_1 \to M_B \to 0$$

where X_i's are isomorphic to direct sums of U_B's; denoted by "U_B-codom. dim. $M_B \geq n$". Let $U^*_A = \text{Hom}_B({}_AU_B,Q_B)$ where Q_B is an injective cogenerator. An A-module N_A is called

"U^*_A-dominant dimension $\geq n$" if there exists an exact sequence:

$$0 \to N_A \to Y_1 \to Y_2 \to \cdots\cdots\cdots \to Y_{n-1} \to Y_n$$

where Y_i's are direct products of U^*_A; denoted by "U^*_A-dom. dim. $N_A \geq n$". So we put $\mathrm{Gen}(U_B) = \{M_B \mid U_B\text{-codom. dim. } M_B \geq 1\}$, $C(U_B) = \{M_B \mid U_B\text{-codom. dim. } M_B \geq 2\}$, $L(U^*_A) = \{N_A \mid U^*_A\text{-dom. dim. } N_A \geq 2\}$, $\mathrm{Im}(T) = \{M_B \mid M_B$ is isomorphic to $N \otimes_A U$ for some $N_A \in$ Mod-A$\}$, $\mathrm{Im}(H) = \{N_A \mid N_A$ is isomorphic to $\mathrm{Hom}_B(U_B, M_B)$ for some $M_B \in$ Mod-B$\}$, and $\overline{\mathrm{Gen}}(U_B)$ the smallest subclass of Mod-B which contains $\mathrm{Gen}(U_B)$ and closed under taking submodules, factors and direct sums. By the same notations as above, we will often mean the full subcategory of Mod-B or Mod-A whose objects are modules in each class if there is no confusion.

Although we are only concerned with the equivalences between module categories, the following fact will be described in general situation since it is very conspicuous in the theory of equivalences between any categories. The notations η, Φ, Ψ denote usual ones similarly defined as above.

Lemma 1.2. Let $\mathcal{C}$, $\mathcal{D}$ be any categories and $T : \mathcal{C} \to \mathcal{D}$, $H : \mathcal{D} \to \mathcal{C}$ functors where T is a left adjoint functor of H. If H considered as $H : \mathrm{Im}(T) \to \mathrm{Im}(H)$ is a full functor, then $\Phi_{T(N)} : THT(N) \to T(N)$ is an isomorphism for any object N in $\mathcal{C}$. Dually, if $T : \mathrm{Im}(H) \to \mathrm{Im}(T)$ is a full functor, then $\Psi_{H(M)}$ is an isomorphism for any object M in $\mathcal{D}$.

Proof. Since $\Psi_{HT(N)} \in \mathrm{Hom}_{\mathcal{C}}(HT(N), HTHT(N))$, there exists

$g \in Hom_{\mathcal{D}}(T(N), THT(N))$ such that $H(g) = \Psi_{HT(N)}$ for any $N \in \mathcal{C}$. By Lemma 1.1 (which is satisfied by replacing the modules N_A and M_B with the objects of $\mathcal{C}$ and $\mathcal{D}$ respectively), $\eta(g \cdot \Phi_{T(N)}) = H(g \cdot \Phi_{T(N)}) \cdot \Psi_{HT(N)} = H(g) \cdot H(\Phi_{T(N)}) \cdot \Psi_{HT(N)} = H(g) \cdot 1_{HT(N)} = H(g) = \Psi_{HT(N)} = \eta(1_{THT(N)})$. Hence $g \cdot \Phi_{T(N)} = 1_{THT(N)}$, so $\Phi_{T(N)}$ is a monomorphism, thus it is an isomorphism by Lemma 1.1. Dually we can prove the latter statement.

<u>Theorem 1.3</u>. Let ${}_AU_B$ be an A-B bimodule. Other notations are as above. The following assertions are equivalent:

(1) $T = - \otimes_A U : Im(H) \to Im(T)$ and $H = Hom_B(U_B, -) : Im(T) \to Im(H)$ are mutually inverse category equivalences.

(2) $T : L(U^*{}_A) \to C(U_B)$ and $H : C(U_B) \to L(U^*{}_A)$ are mutually inverse category equivalences.

(3) There are natural isomorphisms $u : THT \to T$ and $v : H \to HTH$.

(3)* $\Phi_T : THT \to T$ and $\Psi_H : H \to HTH$ are isomorphisms.

(4) There is a natural isomorphism $u : THT \to T$.

(4)* $\Phi_T : THT \to T$ is an isomorphism.

(5) There is a natural isomorphism $v : H \to HTH$.

(5)* $\Psi_H : H \to HTH$ is an isomorphism.

(6) $Cok(\Psi_N) \otimes_A U = 0$ for any $N_A \in$ Mod-A.

(7) $Hom_B(U_B, Ker(\Phi_M)) = 0$ for any $M_B \in$ Mod-B.

(8) The functor $HT :$ Mod-A $\to Im(H)$ is a left adjoint functor of the inclusion functor $I : Im(H) \to$ Mod-A.

(8)* The functor $TH :$ Mod-B $\to Im(T)$ is a right adjoint functor of the inclusion functor $J : Im(T) \to$ Mod-B.

Proof. We claim that in general $\mathrm{Im}(T) \subset C(U_B)$ and $\mathrm{Im}(H) \subset L(U^*{}_A)$.

(2) implies (1). Since $C(U_B) \subset \mathrm{Im}(T)$ and $L(U^*{}_A) \subset \mathrm{Im}(H)$, (1) holds.

(1) implies (2). We prove only $C(U_B) \subset \mathrm{Im}(T)$ and $L(U^*{}_A) \subset \mathrm{Im}(H)$. Let $M_B \in C(U_B)$, and $\sum_{\oplus} U_B \xrightarrow{f} \sum_{\oplus} U_B \to M_B \to 0$ an exact sequence. Since $\sum_{\oplus} U_B \in \mathrm{Im}(T)$, we have a commutative diagram:

$$\begin{array}{ccccccc} TH(\sum_{\oplus} U_B) & \xrightarrow{TH(f)} & TH(\sum_{\oplus} U_B) & \to & TH(\mathrm{Cok}(H(f))) & \to & 0 \\ \downarrow u_{\sum_{\oplus} U_B} & & \downarrow u_{\sum_{\oplus} U_B} & & & & \\ \sum_{\oplus} U_B & \xrightarrow{f} & \sum_{\oplus} U_B & \longrightarrow & M_B & \longrightarrow & 0 \end{array}$$

where $u : TH \to 1_{\mathrm{Im}(T)}$ is a natural isomorphism. Thus M_B is isomorphic to $T(\mathrm{Cok}(H(f)))$, and hence $M_B \in \mathrm{Im}(T)$. Similarly, we have $L(U^*{}_A) \subset \mathrm{Im}(H)$.

(3)* implies (3), (4*) implies (4) and (5)* implies (5) evidently, and the converses are particular cases of Lemma 1.2.

The equivalence of (1) and (3) is also clear by Lemma 1.2, and the equivalences of (4)* and (6), (5)* and (7) are clear by Lemma 1.1 (3). Evidently, (3)* implies (4)* and (5)*.

(5)* and (7) imply (3)*. We prove only that $\Phi_{T(N)}$ is a monomorphism for any $N \in$ Mod-A. Since $\mathrm{Im}(T) \subset C(U_B) \subset \mathrm{Gen}(U_B)$, $\mathrm{Ker}(\Phi_{T(N)}) = \mathrm{Cok}(\Psi_N) \otimes_A U$ is generated by U_B, but $\mathrm{Hom}_B(U_B, \mathrm{Ker}(\Phi_{T(N)})) = 0$, so $\mathrm{Ker}(\Phi_{T(N)}) = 0$ by Lemma 1.1 (3).

(4)* and (6) imply (3)*. For any $M_B \in$ Mod-B, $0 = \mathrm{Cok}(\Psi_{H(M)}) \otimes_A U = \mathrm{Hom}_B(U_B, \mathrm{Ker}(\Phi_M)) \otimes_A U$. Thus $\mathrm{Cok}(\Psi_{H(M)}) = \mathrm{Hom}_B(U_B, \mathrm{Ker}(\Phi_M)) = 0$, so $\Psi_{H(M)}$ is an epimorphism, and therefore an isomorphism by Lemma 1.1 (3).

(3)* implies (8)*. Since $T : Im(H) \to Im(T)$ is full and faithful, we have isomorphisms for any $K_B \in Im(T)$ and $M_B \in$ Mod-B:

$$Hom_B(K_B, TH(M_B)) \xrightarrow{Hom_B(\Phi_K, TH(M_B))} Hom_B(TH(K_B), TH(M_B)) \xrightarrow{T^{-1}}$$

$$\to Hom_A(H(K_B), H(M_B)) \xrightarrow{\eta^{-1}(H(K),M)} Hom_B(TH(K_B), M_B) \xrightarrow{Hom_B(\Phi_K^{-1}, N_B)}$$

$$\to Hom_B(J(K_B), M_B)$$

where $T^{-1}(f)$ is defined by $T(T^{-1}(f)) = f$ for any $f \in Hom_B(TH(K_B), TH(M_B))$. The composition map is $Hom_B(K_B, \Phi_{M_B})$ by routine calculations, and hence it satisfies the naturality. Thus TH is a right adjoint functor of J.

(3)* implies (8). Similar as above.

(8) implies (4). Im(H) is a coreflective subcategory of Mod-A with coreflector $HT : \text{Mod-A} \to Im(H)$, so that there exists a natural isomorphism $u : TH \cdot J \to 1_{Im(T)}$. Hence $u_{T(N)} : THT(N_A) \to T(N_A)$ is an isomorphism for any $N_A \in$ Mod-A.

(8)* implies (4)*. Similar as above.

This completes the proof of the theorem.

<u>Example</u>. If one of the following properties is assumed then there holds (6) or (7) in Theorem 1.3:

(1) $B = End({}_AU)$ and $I \cdot U = U$ where I is the trace ideal of ${}_AU$.

(2) $A = End(U_B)$ and $U \cdot J = U$ where J is the trace ideal of U_B.

Corollary 1.4. If U_B is a weakly self-generator and T and H induce an equivalence $\mathrm{Im}(H) \sim \mathrm{Im}(T)$, then $\mathrm{Im}(T) = \mathrm{Gen}(U_B)$. Here, U_B is called "a weakly self-generator" if $\mathrm{Hom}_B(U_B, M_B) = 0$ implies $M_B = 0$ for any $M_B \in \overline{\mathrm{Gen}}(U_B)$.

Proof. We consider an exact sequence:

$$0 \to \mathrm{Ker}(\Phi_M) \to \mathrm{Hom}_B(U_B, M_B) \xrightarrow{\Phi_M} M_B$$

Clearly, if $M_B \in \mathrm{Gen}(U_B)$ then Φ_M is an epimorphism. By Theorem 1.3, $\mathrm{Hom}_B(U_B, \mathrm{Ker}(\Phi_M)) = 0$ for any $M_B \in \mathrm{Gen}(U_B)$, but U_B is a weakly self-generator and $\mathrm{Ker}(\Phi_M) \in \overline{\mathrm{Gen}}(U_B)$. Hence $\mathrm{Ker}(\Phi_M) = 0$. This means Φ_M is an isomorphism for any $M_B \in \mathrm{Gen}(U_B)$.

2. The equivalence $\mathrm{Im}(H) \sim \mathrm{Gen}(U_B)$. The main theorem of this section is due to the next lemma, which has been shown in [6, Lemma 1.4].

Lemma 2.1. Let ${}_CU_B$ be a C-B bimodule, and $C = \mathrm{End}(U_B)$. The following statements are equivalent:

(1) $\mathrm{Hom}_B({}_CU_B, M_B) \otimes {}_CU_B \cong M_B$ canonically for any $M_B \in \mathrm{Gen}(U_B)$.

(2) $\mathrm{Gen}(U_B) = \overline{\mathrm{Gen}}(U_B)$.

(3) ${}_CU$ is a flat C-module and the functor $\mathrm{Hom}_B(U_B, -) : \mathrm{Gen}(U_B) \to \text{Mod-}C$ is full and faithful.

Theorem 2.2. Let ${}_AU_B$ be an A-B bimodule, and $C = \mathrm{End}(U_B)$. The following statements are equivalent:

(1) $T : Im(H) \to \overline{Gen}(U_B)$ and $H : \overline{Gen}(U_B) \to Im(H)$ are mutually inverse category equivalences.

(2) $T : L(U^*_A) \to \overline{Gen}(U_B)$ and $H : \overline{Gen}(U_B) \to L(U^*_A)$ are mutually inverse category equivalences.

(3) There exists a natural isomorphism $u : TH \to 1_{\overline{Gen}(U_B)}$.

(3)* $\Phi_M : TH(M_B) \to M_B$ is an isomorphism for any $M_B \in \overline{Gen}(U_B)$.

(4) $Gen(U_B) = \overline{Gen}(U_B)$ and ${}_CC \otimes_A U_B \cong {}_CU_B$.

(4)* $Gen(U_B) = \overline{Gen}(U_B)$ and ${}_CC \otimes_A U_B \cong {}_CU_B$ canonically.

(5) $Gen(U_B) = \overline{Gen}(U_B)$ and $\Phi_{T(N)} : THT(N_A) \to T(N_A)$ is an isomorphism for any $N \in$ Mod-A.

(6) ${}_CU$ is flat, U_B is a weakly self-generator and $\Phi_{T(N)} : THT(N_A) \to T(N_A)$ is an isomorphism for any $N_A \in$ Mod-A.

<u>Proof</u>. The equivalence of (1) —— (3)* is clear by Theorem 1.3, and (1) implies (4) evidently.

(4) implies (4)*. Let $h : {}_CC \otimes_A U_B \to {}_CU_B$ be a C-B homomorphism obtained by assumption, $s : {}_AU_B \to {}_AC \otimes_A U_B$ an A-B homomorphism, and $t : {}_CC \otimes_A U_B \to {}_CU_B$ a C-B homomorphism defined by $s(u) = 1_C \otimes u$ and $t(\sum c \otimes u) = \sum c \cdot u$ respectively, where $u \in U$ and $c \in C$. Clearly t is an A-B homomorphism and $t \cdot s = 1_{{}_AU_B}$, so ${}_AC \otimes_A U_B = Im(s) \oplus Ker(t)$ as A-B bimodule. Thus ${}_AU_B = h(Im(s)) \oplus h(Ker(t))$ as A-B bimodule. Put $e_1 : {}_AU_B \to h(Im(s))$ and $e_2 : {}_AU_B \to h(Ker(t))$ projections onto each component. Then they are elements of C. Now, $f = t \cdot h^{-1} : {}_CU_B \to {}_CU_B$ is a C-B epimorphism, so $fe_1 = e_1f$ and $fe_2 = e_2f$. But $fe_2(U_B) = th^{-1}(h(Ker(t)) = t(Ker(t)) = 0$, so that $0 = e_2f(U) = e_2(U) = h(Ker(t))$. Thus $Ker(t) = 0$, which means t

is an isomorphism.

(4)* implies (3)*. For any $M_B \in \overline{\mathrm{Gen}}(U_B)$, $\mathrm{Gen}(U_B) = \overline{\mathrm{Gen}}(U_B)$ induces a canonical isomorphism $\Phi^*_M : \mathrm{Hom}_B({}_CU_B, M_B) \otimes {}_CU_B \to M_B$ defined by $\Phi^*_M(f \otimes u) = f(u)$ for any $f \in \mathrm{Hom}_B({}_CU_B, M_B)$ and $u \in U$ (Lemma 2.1). Let $t : {}_CC \otimes_A U_B \to {}_CU_B$ be a canonical isomorphism. Then we have a commutative diagram:

$$\begin{array}{ccc}
\mathrm{Hom}_B({}_CU_B, M_B) \otimes {}_CC \otimes_A U_B & \xrightarrow{\mathrm{Hom}_B({}_CU_B, M_B) \otimes t} & \mathrm{Hom}_B({}_CU_B, M_B) \otimes {}_CU_B \\
\downarrow \text{nat.} & & \downarrow \Phi^*_M \\
\mathrm{Hom}_B({}_AU_B, M_B)\ \ {}_AU_B & \xrightarrow{\qquad\Phi_M\qquad} & M_B
\end{array}$$

where vertical maps are isomorphisms. Hence Φ_M is an isomorphism for any $M_B \in \overline{\mathrm{Gen}}(U_B)$.

(1) implies (5) and (5) implies (6). These are obvious by Theorem 1.3 and Lemma 2.1.

(6) implies (1). By Corollary 1.4, $H : \mathrm{Gen}(U_B) \to \text{Mod-}A$ is full and faithful. First, we show that the functor $\mathrm{Hom}_B({}_CU_B, -) : \mathrm{Gen}(U_B) \to \text{Mod-}C$ is full. Choose any $D \in \mathrm{Hom}_C(\mathrm{Hom}_B({}_CU_B, M_B), \mathrm{Hom}_B({}_CU_B, N_B))$, which can be regarded as an A-homomorphism. Thus there is a unique B-homomorphism $h : M_B \to N_B$ such that $D(g) = h \cdot g$ for any $g \in \mathrm{Hom}_B({}_AU_B, M_B)$. But $\mathrm{Hom}_B({}_AU_B, M_B) = \mathrm{Hom}_B({}_CU_B, M_B)$, and hence $D(g) = h \cdot g$ for any $g \in \mathrm{Hom}_B({}_CU_B, M_B)$. Similarly we can see that $\mathrm{Hom}_B({}_CU_B, -)$ is faithful. Now, recalling that ${}_CU$ is flat, $\mathrm{Gen}(U_B) = \overline{\mathrm{Gen}}(U_B) = \mathrm{Im}(T)$ by Lemma 2.1. This completes the proof of the theorem.

<u>Corollary 2.3</u> (K. Morita [3, Theorem 1.1]). Let ${}_AU_B$ be

an A-B bimodule, and $C = \mathrm{End}(U_B)$. Then the following statements are equivalent:

(1) $T = -\otimes_A U : \mathrm{Im}(H) \to \text{Mod-}B$ and $H = \mathrm{Hom}_B(U_B,-) : \text{Mod-}B \to \mathrm{Im}(H)$ are mutually inverse category equivalences.

(2) $T : L(U^*_A) \to \text{Mod-}B$ and $H : \text{Mod-}B \to L(U^*_A)$ are mutually inverse category equivalences.

(3) There is a natural equivalence $u : TH \to 1_{\text{Mod-}B}$.

(4) $\Phi : TH \to 1_{\text{Mod-}B}$ is an isomorphism.

(5) U_B is a generator and ${}_CC \otimes_A U_B \cong {}_CU_B$.

(6) U_B is a generator and ${}_CC \otimes_A U_B \cong {}_CU_B$ canonically.

(7) ${}_AU$ is of type FP and $B \cong \mathrm{End}({}_AU)$ canonically.

Here, ${}_AU$ is said to be of type FP if ${}_SU$ is finitely generated projective over the bicommutator S of ${}_AU$ and ${}_SS \otimes_A U_R \cong {}_SU_R$ canonically provided $R = \mathrm{End}({}_AU)$ (and $S = \mathrm{End}(U_R)$).

Proof. The equivalence of (1) — (6) is a direct consequence of Theorem 2.2.

(6) implies (7). Since U_B is a generator, ${}_CU$ is finitely generated projective and $B \cong \mathrm{End}({}_CU)$ canonically. Hence it remains to show $B \cong \mathrm{End}({}_AU)$ canonically. In fact the composition map of the following isomorphisms is canonical: $B \cong \mathrm{End}({}_CU) \cong \mathrm{Hom}_C({}_CC \otimes_A U, {}_CU) \cong \mathrm{Hom}_A({}_AU, \mathrm{Hom}_C({}_CC_A, {}_CU)) \cong \mathrm{Hom}_A({}_AU, {}_AU)$.

(7) implies (6). Since C is the bicommutator of ${}_AU$, $B \cong \mathrm{End}({}_CU)$ canonically. Thus U_B is a generator, since ${}_CU$ is finitely generated projective.

Corollary 2.4 (G. Azumaya). Let ${}_AU$ be a projective A-module, and $B = End({}_AU)$. Then T and H induce a category equivalence $Im(H) \sim \overline{Gen}(U_B)$.

Proof. Let I and J be the trace ideals of ${}_AU$ in A and of U_B in B, respectively. Since $I \cdot U = U$ and $(Cok(\Psi_N)) \cdot I = 0$ for any $N_A \in$ Mod-A, T and H induce an equivalence $Im(H) \sim Im(T)$ by Theorem 1.3 (6). Furthermore, for any $x \in U$, $x \in xJ$ by dual basis lemma. Hence $Gen(U_B) = \overline{Gen}(U_B)$, since $Gen(U_B) = \{M_B \in \text{Mod-B} \mid M_B \cdot J = M_B\}$.

References

[1] K. R. Fuller: Density and equivalences, J. Algebra 29 (1974), 528-550.

[2] Y. Kawada: Retracts and coretracts of categories of modules, unpublished.

[3] K. Morita: Localization in categories of modules I, Math. Z. 114 (1973), 121-144.

[4] T. Onodera: Codominant dimension and Morita equivalences, Hokkaido Math. J. 6 (1977), 169-182.

[5] M. Sato: Fuller's theorem on equivalences, to appear in J. Algebra.

[6] B. Zimmerman-Huisgen: Endomorphism rings of self-generators, Pacific J. Math. 61 (1975), 587-602.

ENDOMORPHISMS OF MODULES OVER MAXIMAL ORDERS

Kanzo MASAIKE

Tokyo University of Art and Science

Throughout this note R is a right order (cf. [4]) in a right Artinian ring Q. Let M be a right R-module, $T = \mathrm{End}(M_R)$ and $M^* = \mathrm{Hom}(M_R, R_R)$. Then, there exists a derived Morita context $(,) : M^* \otimes_T M \to R$ and $[,] : M \otimes_R M^* \to T$ such that $f[m, f'] = (f, m)f'$ and $m(f, m') = [m, f]m'$ for all $m, m' \in M$, $f, f' \in M^*$ ([1], [7]). In the following the images (M, M^*) and $[M, M^*]$ are denoted respectively by I and U. Let P_I and P_U be the smallest Gabriel filters (additive topology [9]) of R and T respectively which contain I and U. Then, B. Müller [7] showed that there exists an equivalence between quotient categories determined by P_I and P_U. One of the purposesof this paper is to apply the above result of Müller to endomorphism rings of modules over maximal orders in Artinian rings.

A right R-module M is said to be torsion free in the sense of Levy [5] if no non-zero element of M is annihilated by a regular element of R. Let $C_R = \{M_r \in \text{Mod-}R \mid M$ is (isomorphic to) a submodule of a right R-module W such that W is a direct product of copies of R_R and W/M is torsion free in the sense of Levy$\}$. We shall say that a right R-module M satisfies the condition (A), if M is isomorphic to a direct summand of a right R-module K such that $K \subset$

$\bigoplus_{i=1}^{n} R$ and $KQ = \bigoplus_{i=1}^{n} Q$. If Q is semi-simple, every finite dimensional torsionless right R-module satisfies (A). In [6], it is proved that if M satisfies (A) then $T = \mathrm{End}(M_R)$ is a right order in $S = \mathrm{End}(M \otimes_R Q_Q)$.

Lemma 1. If M_R satisfies (A), then

(i) $M^* \otimes_T S = (M \otimes_R Q_Q)^*$.

(ii) The trace ideal I contains a regular element, if and only if $M \otimes_R Q$ is a progenerator as a Q-module.

Let us denote by $L_I(\ )$ the quotient functor (localization functor) with respect to P_I.

Lemma 2. Assume R is a maximal right order, M_R is torsionless, I contains a regular element and T has a classical quotient ring $S = \mathrm{End}(M \otimes_R Q_Q)$. If $Y \in C_R$, then $L_I(Y) = Y$ and $\mathrm{Hom}(M_R, Y_R) \in C_T$.

Proposition 1. If Q and S are Morita equivalent right Artinian rings and R is a maximal right order in Q, there exists a maximal right order T in S such that the following statements hold:

(i) There exists a faithful right R-module $M \subset \bigoplus_{i=1}^{n} R$ and a faithful right T-module $N \subset \bigoplus_{i=1}^{m} T$ such that $T \cong \mathrm{End}(M_R)$ and $R \cong \mathrm{End}(N_T)$.

(ii) There exists a category equivalence between C_R and C_T.

Remark. Even if we replace the notion of maximal right order by maximal $\underset{\sim}{\ell}$ right order, Proposition 1 (i) remains true, generalizing and sharpening the results of C. Faith [3] and J. Robson [8].

Theorem 1. Let Q be a quasi-Frobenius ring. Then a ring T is a maximal right order whose classical right quotient ring is Morita equivalent to Q, if and only if T is isomorphic to an endomorphism ring of a right module M over a maximal right order R in Q, where M satisfies the following conditions:

(a) $M \in C_R$ and is finite dimensional.

(b) $M \otimes_R Q$ is Q-projective.

Proposition 2. Let R be a maximal two-sided order in a quasi-Frobenius ring Q, and M a finite dimensional faithful right R-module such that $M \otimes_R Q$ is Q-projective. Then, M is R-reflexive if and only if $M \in C_R$.

In [2] J. H. Cozzens has proved that if R is a maximal two-sided order in a semi-simple ring Q and M is a finite dimensional reflexive faithful right R-module then $\mathrm{End}(M_R)$ is a maximal order. In this case $M = L_I(M) \in C_R$ by Lemma 2 and Proposition 2. Now, by making use of a hereditary torsion theory induced by the trace ideal of M, we can prove the following

Theorem 2. Let R be a maximal right order in a quasi-Frobenius ring Q, and M a finite dimensional torsionless faithful right R-module such that $M \otimes_R Q$ is Q-projective. Then the following conditions are equivalent:

(i) $T = \mathrm{End}(M_R)$ is a maximal right order.

(ii) $L_I(M) \in C_R$, and every $f \in \mathrm{Hom}(J_R, M_R)$ is extended to an element of T, provided J is a submodule of M_R such that M/J is a P_I-torsion module.

References

[1] H. Bass: The Morita Theorems, University of Oregon, 1962.

[2] J. H. Cozzens: Maximal orders and reflexive modules, Trans. Amer. Math. Soc. 219 (1976), 323-336.

[3] C. Faith: Noetherian simple rings, Bull. Amer. Math. Soc. 70 (1964), 730-731.

[4] N. Jacobson: The Theory of Rings, Amer. Math. Soc. Math. Surveys 2, Providence, 1942.

[5] L. Levy: Torsion-free and divisible modules over non-integral domains, Canad. J. Math. 15 (1963), 132-157.

[6] K. Masaike: Endomorphism rings of modules over orders in Artinian rings, Proc. Japan Acad. 46 (1970), 89-93.

[7] B. J. Müller: The quotient category of Morita context, J. Algebra 28 (1974), 389-407.

[8] J. C. Robson: Artinian quotient rings, Proc. London Math. Soc. 17 (1967), 600-616.

[9] B. Stenström: Rings and Modules of Quotients, Lecture Notes in Math. 273, Springer, 1971.

ON FINITE DIMENSIONAL QF-3' RINGS

Takeshi SUMIOKA
Osaka City University

This note is a revised version of the part of finite dimensional QF-3' rings in [11]. Let R be a ring with unity. An R-module means a unital R-module and "torsion theory" means the Lambek torsion theory, whose torsion radical is denoted by t. Let M be a right R-module. Then a chain

$$\cdots \subset M_{i-1} \subset M_i \subset M_{i+1} \subset \cdots$$

of submodules of M is called a <u>t-chain</u> of M if M_{i+1}/M_i is not a torsion module for each i. M is called <u>finite dimensional</u> if both any ascending and any descending t-chains of M terminate. R is called <u>right finite dimensional</u> if R_R is finite dimensional (refer Goldman [3] for these definitions and properties). We say the dimension of M is equal to n and denote it by $\dim M = n$, if M has a t-chain of length n but no t-chains of length more than n. In particular $\dim M = 0$ if M is a torsion module. We define $\dim M = \infty$ if M has a t-chain of length n for any number n.

A submodule N of M is called <u>closed</u> if M/N is torsion-free. Let E be an injective hull of R_R. For a submodule X of M (resp. $\mathrm{Hom}_R(M,E)$), we denote its annihilator in $\mathrm{Hom}_R(M,E)$ (resp. M) by $\ell(X)$ (resp. $r(X)$). Then we note that N is a closed submodule of M if and only if $N = r(X)$ for some $X \subset \mathrm{Hom}_R(M,E)$ (see Shock [9, Theorem 3.2]), since for a submodule L of M such that $N \subset L$, L/N is a torsion module $\Leftrightarrow \mathrm{Hom}_R(L/N,E) = 0 \Leftrightarrow \ell(N)L = 0 \Leftrightarrow L \subset r\ell(N)$. We denote the set of closed submodules of M by $C(M)$.

See Faith [2, § 3 Proposition 1] for the equivalence of (2) and (4) in the next lemma and Shock [9, Corollary 3.3] for that of (1) and (2).

<u>Lemma 1</u>. The following properties for a right R-module M are equivalent:

(1) Every ascending t-chain of M terminates.

(2) $C(M)$ is noetherian.

(3) For every set of right R-modules L_α $(\alpha \in A)$ and every R-homomorphism $f : \bigoplus_{\alpha\in A} L_\alpha \to M$, there exists a finite subset B of A such that $\mathrm{Im}\, f/\mathrm{Im}\, fi$ is a torsion module, where i is a canonical injection $\bigoplus_{\beta\in B} L_\beta \to \bigoplus_{\alpha\in A} L_\alpha$.

(4) For every submodule N of M, there exists a finitely generated submodule L of N such that N/L is a torsion module.

<u>Proof</u>. (1) $\Rightarrow$ (3) $\Rightarrow$ (4). Those are clear.

(3) $\Rightarrow$ (2). Let $M_1 \subset M_2 \subset \ldots$ be a chain of closed submodules of M. Consider a natural map $f : \bigoplus_{i=1}^{\infty} M_i \to M$. Then there is an integer n such that $\bigcup_{i=1}^{\infty} M_i/M_n$ ($= f(\bigoplus_{i=1}^{\infty} M_i)/f(\bigoplus_{i=1}^{n} M_i)$) is a torsion module. Since M_n is closed, $M_i = M_{i+1}$ for each $i \geq n$.

(2) $\Rightarrow$ (1). Let $M_1 \subset M_2 \subset \ldots$ be a t-chain of M. If M_i'/M_i is the torsion submodule of M/M_i, M_i' is closed in M

and $M_i' \subsetneq M_{i+1}'$. Thus the above t-chain terminates.

(4) ⇒ (1). Let $M_1 \subset M_2 \subset \ldots$ be a t-chain of M. We put $N = \bigcup_{i=1}^{\infty} M_i$. Then there is a finitely generated submodule L of N such that N/L is a torsion module, and so L is contained in some M_i, which implies that the above t-chain terminates.

We can similarly show the following lemma.

<u>Lemma 1'</u>. For a right R-module M, the following properties are equivalent:

(1) Every descending t-chain of M terminates.

(2) $C(M)$ is artinian.

(3) For every set of torsion-free right R-modules L_α ($\alpha \in A$) and every R-homomorphism $f : M \to \prod_{\alpha \in A} L_\alpha$, there exists a finite subset B of A such that Ker f = Ker pf, where p is a canonical projection $\prod_{\alpha \in A} L_\alpha \to \prod_{\beta \in B} L_\beta$.

The following lemma is immediate from the fact that for an exact sequence $0 \to A \to B \to C \to 0$ of R-modules, B is a torsion module if and only if A and C are torsion modules.

<u>Lemma 2</u>. Let $0 \to L \to M \to N \to 0$ be an exact sequence of right R-modules. Then $C(M)$ is noetherian (resp. artinian) if and only if so are $C(L)$ and $C(N)$. Moreover we have $\dim M = \dim L + \dim N$.

By Lemma 2, we see easily that if M is finite dimensional, dim M = n for some n. A right R-module M is called FI if M is imbedded in some finitely generated right R-module. Let E be an injective hull of R_R. R is called <u>right QF-3'</u> if every finitely generated (or FI) submodule of E is torsionless. Such a ring is investigated by Masaike [5], and under some conditions by Sato [7, 8]. If M is a right R-module, we denote $\mathrm{Hom}_R(M,R)$ and $\mathrm{Ext}^1_R(M,R)$ by M^* and M_*, respectively. The next lemma will be clear.

<u>Lemma 3</u>. Let R be a right QF-3' ring.

(1) For an FI right R-module M, M is a torsion module if and only if $M^* = 0$.

(2) For a right ideal I of R, I is closed in R_R if and only if I is a right annihilator ideal.

See [11] for the following theorem and corollary.

<u>Theorem 4</u>. Let R be a right finite dimensional ring. Then the following conditions are equivalent:

(1) R is QF-3'.

(2) dim M = dim M* for every FI right and every FI left R-module M.

<u>Corollary 5</u>. Let R be a finite dimensional QF-3' ring.

(1) For a finite dimensional right R-module M, M* is reflexive.

(2) For a finitely generated right R-module M, M_* is

a torsion module.

(3) For a finite dimensional torsion-free right R-module M, M is torsionless if and only if dim M = dim M*.

Sato has shown that (1) implies (2) in the following proposition.

Proposition 6. Let Q be the maximal right quotient ring of R. Then the following conditions are equivalent:

(1) Q is a left quotient ring.

(2) For every finitely generated torsion right R-module M, M_* is a torsion module.

Proof. Let I be a dense right ideal of R and consider an exact sequence $0 \to R \to Q \to Q/R \to 0$. Then we have an isomorphism $\mathrm{Hom}_R(R/I, Q/R) \cong (R/I)_*$, since $\mathrm{Hom}_R(R/I, Q) = 0$ and $\mathrm{Ext}^1_R(R/I, Q) = 0$ (see Stenström [10]).

(1) $\Rightarrow$ (2). It suffices to show that M_* is a torsion module for every cyclic torsion right R-module $M = R/I$. We have a monomorphism $\mathrm{Hom}_R(R/I, Q/R) \to \mathrm{Hom}_R(R, Q/R) \cong Q/R$, which is derived from an exact sequence $0 \to I \to R \to R/I$. Thus $(R/I)_*$ is a torsion module, since Q/R is a torsion left R-module.

(2) $\Rightarrow$ (1). Let $\bar{q}$ be an element of Q/R. Then $R/I \cong \bar{q}R$ for some dense right ideal I of R and hence we can regard $\bar{q}$ as an element of $\mathrm{Hom}_R(R/I, Q/R)$. Since $\mathrm{Hom}_R(R/I, Q/R)$ ($\cong (R/I)_*$) is a torsion module. $R\bar{q}$ is also a torsion module. Thus Q/R is a torsion left R-module, which implies that Q

is a left quotient ring.

Lemma 7. Let R be a ring satisfying the descending chain condition on annihilator right ideals. If R is right QF-3' then E (= $E(R_R)$) is flat.

Proof. By Lemma 3, $C(R_R)$ is artinian. Let M be a finitely generated submodule of E. Then M is torsionless and by Lemma 1' M is imbedded in a free right R-module. Thus E is flat by Rutter [6, Lemma 2].

We call a ring R right QF-3 if R has a minimal faithful right R-module.

Theorem 8. Let R be a ring. Then the following statements are equivalent:

(1) R is a right QF-3' and right perfect ring satisfying the ascending chain condition on annihilator right ideals.

(2) R is semi-primary QF-3.

Proof. Assuming (1), by Faith [2, § 4 Proposition 1], R is semi-primary and hence $C(R_R)$ is artinian, since $C(R_R)$ is noetherian. Therefore by Lemma 7 E is projective and then by Jans [4, Theorem 3.2] R is right QF-3. Thus by Colby and Rutter [1, Theorem 1.3] and Faith [2, §3 Proposition 3], R is QF-3. The converse is followed by Colby and Rutter [1, Theorem 1.3], Faith [2, § 3 Proposition 3] and Tachikawa [12, p. 47].

References

[1] R. R. Colby and E. A. Rutter: Generalizations of QF-3 algebras, Trans. Amer. Math. Soc. 153 (1971), 371-386.

[2] C. Faith: Rings with ascending condition on annihilators, Nagoya Math. J. 27 (1966), 179-191.

[3] O. Goldman: Elements of non commutative arithmetic I, J. Algebra 35 (1975), 308-341.

[4] J. P. Jans: Projective injective modules, Pacific J. Math. 9 (1959), 1103-1108.

[5] K. Masaike: On quotient rings and torsionless modules, Sci. Rep. Tokyo Kyoiku Daigaku A 11 (1971), 26-30.

[6] E. A. Rutter: A characterization of QF-3 rings, Pacific J. Math. 51 (1974), 533-536.

[7] H. Sato: A duality of torsion modules over a QF-3 one-dimensional Gorenstein ring, Sci. Rep. Tokyo Kyoiku Daigaku A 13 (1975), 28-36.

[8] H. Sato: On localization of a 1-Gorenstein ring, Sci. Rep. Tokyo Kyoiku Daigaku A 13 (1977), 188-193.

[9] P. C. Shock: Injectivity, annihilators and orders, J. Algebra 19 (1971), 96-103.

[10] B. Stenström: Rings and Modules of Quotients, Lecture Notes in Math. 237, Springer, 1971.

[11] T. Sumioka: On non-singular QF-3' rings with injective dimension ≤ 1, Osaka J. Math. (to appear).

[12] H. Tachikawa: Qauasi-Frobenius Rings and Generalization, Lecture Notes in Math. 351, Springer, 1973.

NILPOTENCY INDICES OF THE RADICALS OF MODULAR GROUP RINGS

Shigeo KOSHITANI
The University of Tsukuba

Let K be a field, G a finite group, KG the group algebra of G over K, and $J(KG)$ the radical of KG. We are interested in relations between ring-theoretical properties of KG and the structure of G. Particularly, in the present note we shall study the nilpotency index $t(G)$ of $J(KG)$, which is the least positive integer such that $J(KG)^{t(G)} = 0$ (cf. Remarks of R. Brauer [19, p. 144, Problem 15]).

Since $KG/J(KG)$ is a separable K-algebra (cf. [12, Proposition 12.11]), we may assume that K is algebraically closed. To begin with we shall state the results concerning the nilpotency index of the radical of KG which are obtained until now.

(1) Maschke [2, (15.6)]: $t(G) = 1$ if and only if $\mathrm{char}(K) = 0$, or $\mathrm{char}(K) = p > 0$ and $p \nmid |G|$.

Hence assume that $\mathrm{char}(K) = p > 0$ and $p \mid |G|$ throughout this note.

(2) Jennings [8]: If P is a p-group of order p^r, then

(i) $t(P) = \sum_{i \geq 1} id_i(p-1)+1$, where $K_i = \{x \in P \mid x - 1 \in J(KP)^i\}$ and $|K_i/K_{i+1}| = p^{d_i}$.

(ii) $r(p-1)+1 \leq t(P) \leq p^r$ (cf. [25, Lemma 2.3]).

(3) Morita [13], Clarke [1]: If G is a p-solvable group of p-length 1 with a p-Sylow subgroup P, then $t(G) = t(P)$.

(4) Wallace [24]: $t(G) = 2$ if and only if $p = 2$ and G has a 2-Sylow subgroup of order 2.

(5) Dade [3] (cf. [15, Remark 1]):

(i) If B is a block of KG with a cyclic defect group D, then $t(B) \leq |D|$, where $t(B)$ is the nilpotency index of the radical $J(B)$ of B.

(ii) If G has a cyclic p-Sylow subgroup P, then $t(G) \leq |P|$.

(6) Wallace and Dade (cf. [15, Remark 2]): If $p = 3$ and G has a 3-sylow subgroup of order 3, then $t(G) = 3$.

(7) Tsushima [21], Passman [18]: If G is a p-solvable group with a p-Sylow subgroup P, then $t(G) \leq |P|$.

(8) Wallace [25]: If G is a p-solvable group with a p-Sylow subgroup of order p^r, then $t(G) \geq r(p-1)+1$.

(9) Kupisch [11], Janusz [7] (cf. [10, Theorem 3] and [17, Theorem 2]):

(i) When B is a block of KG with a cyclic defect group D, B is a serial (generalized uniserial) ring if and only if $t(B) = |D|$.

(ii) If KG is serial, then $t(G) = |P|$, where P is a p-Sylow subgroup of G. It is to be noted that when G is a p-solvable group with a cyclic p-Sylow subgroup, then KG is serial (cf. [13, Theorem 8], [20, Theorem 3] and [22, Theorem 3]).

(10) Holvoet [5]: Let P be a p-group of order p^r $(r \geq 2)$ of the following types;

(i) P is an abelian group of type (p^{r-1}, p),

(ii) $p = 2$, $r = 3$ and $P \cong D_3$ or Q_3,

(iii) $p = 2$, $r \geq 4$ and $P \cong D_r$, Q_r, S_r or $M_r(2)$,

(iv) $p \neq 2$, $r \geq 3$ and $P \cong M_r(p)$,

where D_r, Q_r and S_r are a dihedral group, a generalized quaternion group and a semi-dihedral group of order 2^r, respectively, and $M_r(p) = \langle a, b \mid a^p = b^{p^{r-1}} = 1, a^{-1}ba = b^{p^{r-2}+1} \rangle$ (cf. [4, Chap. 2 and Chap. 5]). Then $t(P) = p^{r-1} + p - 1$.

(11) Motose [14]: For two finite groups G_1 and G_2, $t(G_1 \times G_2) = t(G_1) + t(G_2) - 1$.

(12) Ninomiya [16]:

(i) Let G be a p-solvable group of p-length 1 with a p-Sylow subgroup P of order p^r. Then $t(G) = r(p-1)+1$ if and only if P is elementary abelian, and $t(G) = p^r$ if and only if P is cyclic.

(ii) When G is a p-solvable group with a p-Sylow subgroup P, then $t(G) = 3$ if and only if $p = 3$ and $|P| = 3$, or $p = 2$ and P is an elementary abelian group of order 4.

K. Motose [16] showed that for a p-solvable group G the first part of (12) (i) does not hold in general. On the other hand, the last part of (12) (i) holds for any p-solvable group G. That is to say,

(13) Tsushima [23], Koshitani [10]: Let G be a p-solvable group with a p-Sylow subgroup P. Then $t(G) = |P|$ if and only if P is cyclic.

(14) (Cf. [9, Remark 3]). If P is a semi-direct product of two cyclic p-groups P_1 and P_2, then $t(P) = t(P_1) + t(P_2) - 1$.

It is to be noted that for two p-groups P_1 and P_2, (14) does not hold in general.

Now, let P be a p-group of order p^r $(r \geq 2)$. All p-groups P such that t(P) are the lower bound $r(p-1)+1$ or the upper bound p^r are determined by (12). So in this note we shall consider p-groups P such that t(P) are not equal to $r(p-1)+1$ or p^r. The main result of this note can be stated as folloes:

<u>Theorem</u>. Let P be a p-group of order p^r $(r \geq 2)$. Then the following conditions are equivalent:

(i) $t(P) = p^{r-1}+p-1$.

(ii) $p^{r-1} < t(P) < p^r$.

(iii) P is not cyclic and has a cyclic subgroup of index p.

(iv) P is one of the following types (cf. (10));

(a) P is an abelian group of type (p^{r-1},p).

(b) $p = 2$, $r = 3$ and $P \cong D_3$ or Q_3,

(c) $p = 2$, $r \geq 4$ and $P \cong D_r$, Q_r, S_r or $M_r(2)$,

(d) $p \neq 2$, $r \geq 3$ and $P \cong M_r(p)$.

It follows from Theorem that $p^{r-1}+p-1$ is the secondarily highest nilpotency index of $J(KP)$.

Proof of Theorem. (i) $\Rightarrow$ (ii) is trivial. (iii) $\Leftrightarrow$ (iv) is obtained by [4, Chap. 5, Theorem 4.4]. (iv) $\Rightarrow$ (i) is proved by (10). Therefore it suffices to prove the next lemma by (12) (i).

Lemma. Let P be a p-group of order p^r $(r \geq 1)$. If $t(P) > p^{r-1}$, then P has an element of order p^{r-1}.

Proof. We use induction on r. It is clear for $r = 1$ or 2. Assume that $r = 3$. When P is abelian, it is trivial from (11). When P is nonabelian, by [6, I.14.10 Satz], P is one of the following types;

(i) $p = 2$ and $P \cong D_3$ or Q_3,

(ii) $p \neq 2$ and $P \cong M_3(p)$ or $M(p) = \langle a, b, c \mid a^p = b^p = c^p = 1, a^{-1}ba = bc, b^{-1}cb = c, a^{-1}ca = c\rangle$.

Suppose that $p \neq 2$ and $P = M(p)$. Put $x = a - 1$, $y = b - 1$ and $z = c - 1$ in KP. Since $yx = xyz + xz + yz + xy + z$, $zx = xz$ and $zy = yz$, we have

$$y^t x^s \in \sum_{\substack{i+j+2k \geq s+t \\ 0 \leq i \leq s}} Kx^i y^j z^k \qquad \text{for all } s \text{ and } t$$

by induction. Hence it follows that $G_i = \{x^s y^t z^u \mid 0 \leq s, t, u$

$\leq p-1$, $s+t+2u \geq i\}$ is a K-basis of $J(KP)^i$ by induction. This implies that $t(P) = (p-1)+(p-1)+2(p-1)+1 = 4p-3 \leq p^2$. This is a contradiction. So the assertion is proved for $r = 3$. Assume that $r \geq 4$ and it is proved for p-groups of orders $p, p^2, \ldots, p^{r-1}$. There is an element $c \in Z(P)$ of order p, where $Z(P)$ is the center of P. Put $C = \langle c \rangle$. Since $t(P) > p^{r-1}$, by [25, Theorem 2.4], it follows that $t(P/C) > p^{r-2}$. Hence P/C has an element bC $(b \in P)$ of order p^{r-2}. Now, suppose that P has no elements of order p^{r-1}. So $|b| = p^{r-2}$ and P/C is not cyclic. By [4, Chap. 5, Theorem 4.4], P/C is one of the following types;

Case 1. P/C is an abelian group of type (p^{r-2},p).

Case 2. $p = 2$ and $P/C \cong D_{r-1}$.

Case 3. $p = 2$ and $P/C \cong Q_{r-1}$.

Case 4. $p = 2$, $r \geq 5$ and $P/C \cong S_{r-1}$.

Case 5. $p = 2$ and $r \geq 5$, or $p \neq 2$ and $P/C \cong M_{r-1}(p)$.

Case 1. We can put $P/C = \langle aC, bC \mid (aC)^p = (bC)^{p^{r-2}} = C, abC = baC \rangle$. $|a| = p$ or p^2. If $|a| = p^2$, we may put $a^p = c$. Since P/C is abelian, P is a semi-direct product of $\langle a \rangle$ by $\langle b \rangle$. Hence, by (14), $t(P) = p^{r-2}+p^2-1 \leq p^{r-1}$, and this is a contradiction. Thus $|a| = p$. If $b^{-1}a^{-1}ba = 1$, P is an abelian group of type (p^{r-2},p,p). So $t(P) = p^{r-2}+2p-2 \leq p^{r-1}$ from (11). Hence we can put $b^{-1}a^{-1}ba = c$. Thus $P = \langle a, b, c \mid a^p = b^{p^{r-2}} = c^p = 1, a^{-1}ba = bc, a^{-1}ca = c, b^{-1}cb = c \rangle$. By the same method as calculating $t(M(p))$, we know $t(P) = (p-1)+(p^{r-2}-1)+2(p-1)+1 = p^{r-2}+3p-3 \leq p^{r-1}$. So we have a contradiction in Case 1.

The proofs in Cases 2, 3 and 4 are similar to that in Case 5. Henceforth we shall restrict our attention to Case 5.

Case 5. Put $P/C = \langle aC, bC \mid (aC)^p = (bC)^{p^{r-2}} = C, a^{-1}baC = b^{p^{r-3}+1}C\rangle$. $|a| = p$ or p^2. Put $f = p^{r+3}+1$. If $b^{-f}a^{-1}ba = 1$ and $|a| = p$, P is a direct product of $M_{r-1}(p)$ and a cyclic group of order p. It follows from (10) and (11) that $t(P) = p^{r-2}+2p-2 \le p^{r-1}$. If $b^{-f}a^{-1}ba = 1$ and $|a| = p^2$, we may put $a^p = c$, and so P is a semi-direct product of $\langle b\rangle$ by $\langle a\rangle$. Hence, by (14), $t(P) = p^{r-2}+p^2-1 \le p^{r-1}$. If $b^{-f}a^{-1}ba \ne 1$ and $|a| = p$, we can put $b^{-f}a^{-1}ba = c$. Thus $P = \langle a, b, c \mid a^p = b^{p^{r-2}} = c^p = 1, a^{-1}ba = b^fc, a^{-1}ca = c, b^{-1}cb = c\rangle$. Since $f \ge 4$ and $f \equiv 1 \pmod p$, as in the calculation of $t(M(p))$, $t(P) = p^{r-2}+3p-3 \le p^{r-1}$. If $b^{-f}a^{-1}ba \ne 1$ and $|a| = p^2$, we may set $a^p = c$ and $b^{-f}a^{-1}ba = c^h$ for some h $(1 \le h \le p-1)$. Hence $P = \langle a, b, c \mid a^p = c, b^{p^{r-2}} = c^p = 1, a^{-1}ba = b^fc^h, a^{-1}ca = c, b^{-1}cb = c\rangle$. Since $f \ge 4$, $f \equiv 1 \pmod p$ and $(a - 1)^p = c - 1$, as calculating $t(M(p))$, $t(P) = (p-1)+(p^{r-2}-1)+p(p-1)+1 = p^{r-2}+p^2-1 \le p^{r-1}$. Thus we obtain a contradiction in Case 5. We have therefore verified Lemma.

From (3) we have

<u>Corollary</u>. Let G be a p-solvable group of p-length 1 with a p-Sylow subgroup P and $|P| = p^r$ $(r \ge 2)$. Then the following conditions are equivalent:

(i) $t(G) = p^{r-1}+p-1$.

(ii) $p^{r-1} < t(G) < p^r$.

(iii) P is not cyclic and has a cyclic subgroup of index p.

(iv) P is one of the following types;

(a) P is an abelian group of type (p^{r-1}, p).

(b) $p = 2$, $r = 3$ and $P \cong D_3$ or Q_3.

(c) $p = 2$, $r \geq 4$ and $P \cong D_r$, Q_r, S_r or $M_r(2)$.

(d) $p \neq 2$, $r \geq 3$ and $P \cong M_r(p)$.

Remark. For a p-solvable group G of p-length ≥ 2, the same statement as Corollary does not hold in general. Assume that $p = 2$ and that G is the symmetric group of degree 4. G is a 2-solvable group of order 24 of 2-length 2. On the other hand, $t(G) = 4 \neq 2^2+2-1$ by [16, Proposition] and a 2-Sylow subgroup of G is a dihedral group of order 8.

References

[1] R. J. Clarke: On the radical of the group algebra of a p-nilpotent group, J. Austral. Math. Soc. 13 (1972), 119-123.

[2] C. W. Curtis and I. Reiner: Representation Theory of Finite Groups and Associative Algebras, Interscience, New York, 1962.

[3] E. C. Dade: Blocks with cyclic defect groups, Ann. Math. 84 (1966), 20-48.

[4] D. Gorenstein: Finite Groups, Harper and Row, New York, 1968.

[5] R. Holvoet: De groepalgebra van een eindige p-groep over een veld met karacteristiek p, Natuurkundig Tijdschrift 42e Jaargang IV (1969), 157-170.

[6] B. Huppert: Endliche Gruppen I, Springer, Berlin, 1967.

[7] G. J. Janusz: Indecomposable modules for finite groups, Ann. Math. 89 (1969), 209-241.

[8] S. A. Jennings: The structure of the group ring of a p-group over a modular field, Trans. Amer. Math. Soc. 50 (1941), 175-185.

[9] S. Koshitani: Group rings of metacyclic p-groups, Proc. Japan Acad. 52 (1976), 269-272.

[10] S. Koshitani: On the nilpotency indices of the radical of group algebras of p-solvable groups, Proc. Japan Acad. 53A (1977), 13-16.

[11] H. Kupisch: Projektive Moduln endlicher Gruppen mit zyklischer p-Sylow-Gruppe, J. Algebra 10 (1968), 1-7.

[12] G. O. Michler: Blocks and centers of group algebras, Lectures on Rings and Modules, Lecture Notes in Math. 246, Springer, Berlin, 1972, 429-563.

[13] K. Morita: On group rings over a modular field which possess radicals expressible as principal ideals, Sci. Rep. Tokyo Bunrika Daigaku A 4 (1951), 177-194.

[14] K. Motose: On C. Loncour's results, Proc. Japan Acad. 50 (1974), 570-571.

[15] K. Motose: On radicals of principal blocks, Hokkaido Math. J. 6(1977), 255-259.

[16] K. Motose and Y. Ninomiya: On the nilpotency index of the radical of a group algebra, Hokkaido Math. J. 4 (1975), 261-264.

[17] K. Motose and Y. Ninomiya: On generalized uniserial blocks, Math. J. Okayama Univ. 19 (1977), 141-145.

[18] D. S. Passman: Radicals of twisted group rings, Proc. London Math. Soc. 20 (1970), 409-437.

[19] T. L. Saaty (ed.): Lectures on Modern Mathematics I, Interscience, New York, 1963.

[20] B. Srinivasan: On the indecomposable representations of a certain class of groups, Proc. London Math. Soc. 10 (1960), 497-513.

[21] Y. Tsushima: Radicals of group algebras, Osaka J. Math. 4 (1967), 179-182.

[22] Y. Tsushima: A group algebra of a p-solvable group, Osaka J. Math. 5 (1968), 89-98.

[23] Y. Tsushima: Some notes on the radical of a finite group ring, to appear.

[24] D. A. R. Wallace: Group algebras with radicals of square zero, Proc. Glasgow Math. Assoc. 5 (1962), 158-159.

[25] D. A. R. Wallace: Lower bounds for the radical of the group algebra of a finite p-soluble group, Proc. Edinburgh Math. Soc. 16 (1968/69), 127-134.

PROBLEMS ON THE RADICAL OF A FINITE GROUP RING

Yukio TSUSHIMA

Osaka City University

Throughout we shall use the following notation: p is a fixed prime number, G a finite group with a Sylow p-subgroup of order p^a, and k is a field of characteristic p containing the $|G|$-th roots of unity. We denote by J the Jacobson radical of the group ring kG.

1. As was posed by Brauer [1], there has been the following problem.

<u>Problem 1</u>. How can we characterize by group-theoretical properties the following numbers?

(1) the dimension of J over k.

(2) the exponent of J, namely the smallest integer t such that $J^t = 0$.

The first question in the above will be connected with

<u>Problem 2</u>. Suppose we find some non-equivalent irreducible k-representations of G. Then how can we check whether or not they are all the non-equivalent ones?

Of course, one method is to find the number of the p-regular classes of G. On the other hand, if $\{\phi_1, \phi_2, \dots, \phi_r\}$

is the full set of distinct Brauer characters of G and if u_i is the degree of the principal indecomposable Brauer character corresponding to ϕ_i for each i $(1 \leq i \leq r)$, then we have $\sum_{i=1}^{r} f_i u_i$, where $f_i = \phi_i(1)$. Hence, it seems natural to ask

<u>Problem 3</u>. Can we find u_i if f_i were known?

For a p-solvable group, a complete answer to the above is given by Fong.

<u>Theorem 1</u> (Fong [3]). Suppose G is p-solvable. Then we have $u_i = p^a f_i'$, where f_i' is the p'-part of f_i.

2. Nextly, we are concerned with the second question of Problem 1. For an artinian ring R, we denote by t(R) the exponent of the radical of R. If R = kG, then we put t(G) = t(R).

If G is a p-group, then t(G) may be computed from a knowledge of certain normal series of G (Jennings [4]).

Another intersting result is the following, which was first noted by Clarke [2], but the proof is direct from a result of Morita [5].

<u>Theorem 2</u> (Clarke [2]). Suppose G is a p-solvable group of p-length one. Then there holds t(G) = t(P).

Here we dare to ask

Problem 3. Is it true $t(G) = t(G/H)$ for any normal p'-subgroup of G?

If G is p-solvable, this is equivalent to

Problem 4. Let B be a principal p-block (ideal) of kG. Then, is it true $t(B) = t(G)$?

Recall that if G^* is a representation group of G over k then kG^* is the direct sum of the non-isomorphic twisted group rings of G over k. Therefore, if H is restricted to be a central subgroup of G, Problem 3 is equivalent to

Problem 5. Is it true $t(G) \geq t(A)$ for any twisted group ring A of G over k?

Concerning with a bound for $t(G)$, we know that $t(G) \leq p^a$ if G is p-solvable (Tsushima [6]). In addition, we get

Theorem 3 (Tsushima [7]). Suppose G is p-solvable. If $t(G) = p^a$, then P is cyclic.

3. As far as the radical is concerned, the following problem seems most proper.

Problem 6. How can we characterize the elements of J?

For $\lambda \in kG$, we let $\sigma(\lambda)$ be the sum of the coefficients of G which appear in λ.

<u>Theorem 4</u> (Tsushima [7]). If $\lambda \in J$, then $\sigma(g\lambda) = 0$ for all $g \in G$. The converse is true, provided G is p-solvable.

Finally, we mention

<u>Theorem 5</u> (Tsushima [7]). The following statements are equivalent:

(1) J is generated over kG by central elements.

(2) JB is generated over kG by central elements, where B is the principal block (ideal) of kG.

(3) G is p-nilpotent and P is abelian.

References

[1] R. Brauer: Lectures on modern mathematics I (Ed. by T. L. Saaty), Wiley, New York, 1963.

[2] R. J. Clarke: On the radical of the group ring of a p-nilpotent group, J. Austral. Math. Soc. 13 (1972), 119-123.

[3] P. Fong: Solvable groups and modular representations, Trans. Amer. Math. Soc. 103 (1962), 484-494.

[4] S. A. Jennings: The structure of the group ring of a p-group over a modular field, Trans. Amer. Math. Soc. 50 (1941), 175-185.

[5] K. Morita: On group rings over a modular field which possess radicals expressible as principal ideals, Sci. Rep. T.B.D. 4 (1951), 177-194.

[6] Y. Tsushima: Radicals of group algebras, Osaka J. Math. 4 (1967), 179-182.

[7] Y. Tsushima: Some notes on the radical of a finite group ring, to appear.