Bull. Korean Math. Soc.
Vol. 20, No. 1, 1983

DERIVATION MODULES OF GROUP RINGS AND INTEGERS OF CYCLOTOMIC FIELDS

In Memory of Professor Dock Sang Rim

I. Y. CHUNG

1. Preliminaries

Let R be a commutative ring with 1, and A a unitary commutative R-algebra. By a *derivation module* of A, we mean a pair (M, d), where M is an A-module and $d : A \to M$ an R-derivation, i.e., d is an R-linear mapping such that $d(ab) = a(db) + b(da)$. A *derivation module homomorphism* $f : (M, d) \to (N, \delta)$ is an A-homomorphism $f : M \to N$ such that $f \circ d = \delta$. A derivation module of A, (U, d), is called a universal derivation module of A if for any derivation module of A, (M, δ), there exists a unique derivation module homomorphism $f : (U, d) \to (M, \delta)$. In fact, a universal derivation module of A exists in the category of derivation modules of A, and is unique up to unique derivation module isomorphisms [2, p. 101]. When (U, d) is a universal derivation module of R-algebra A, the A-module U is denoted by $U(A/R)$. For our convenience, $U(A/R)$ will also be called a universal derivation module of A, and d the R-derivation corresponding to $U(A/R)$. A list of basic properties are:

PROPOSITION 1. *Let $R[X]$ be a polynomial ring over R with X as a set of indeterminates. If U is a free $R[X]$-module with a set $\{u_x : x \in X\}$, where $u_x = u_y$ if and only if $x = y$ for $x, y \in X$, as basis and $d : R[X] \to U$ be an R-derivation defined by $df = \Sigma_x (\partial f / \partial x) u_x$, $f \in R[X]$, then (U, d) is a universal derivation module of $R[X]$.* (*see* [1, p. 8, Satz 2])

PROPOSITION 2. *Let A and B be commutative R-algebras, and $\mathfrak{f} : A \to B$ an onto algebra homomorphism. If (U, d) and (V, δ) are universal derivation modules of A and B respectively,*

$$(V, \delta) \cong (U/((\ker \mathfrak{f})U + A\, d(\ker \mathfrak{f})),\ \partial),$$

where the R-derivation $\partial : B \to U/((\ker \mathfrak{f})U + A\, d(\ker \mathfrak{f}))$ is defined by $\partial(b) = \nu(d(a))$ for some $a \in \mathfrak{f}^{-1}(b)$. Here,

$\nu : U \to U/((\ker \mathfrak{f})U + A\, d(\ker \mathfrak{f}))$ is the natural homomorphism.

Proof. V can be made into an A-module by defining $av = \mathfrak{f}(a)v$, for $a \in A$, $v \in V$. Then, $(V, \delta \circ \mathfrak{f})$ is a derivation module of A. Since (U, d) is a universal derivation module of A, there is a unique derivation module homomorphism $f : (U, d) \to (V, \delta \circ \mathfrak{f})$. It is easy to see that $\ker f = (\ker \mathfrak{f})U + Ad(\ker \mathfrak{f})$. Let $g : \nu(U) \to V$ be the isomorphism such that $g \circ \nu = f$. However, $\nu(U)$ can be made into a B-module by defining $b\nu(u) = \nu(au)$ for some $a \in \mathfrak{f}^{-1}(b)$, and g is also a B-isomorphism. This proves the Proposition.

COROLLARY 1. *Let $R[x]$ be a polynomial ring in one indeterminate x, J an ideal of $R[x]$ generated by $\{f_\alpha\}_{\alpha\in I}$, $f_\alpha\in R[x]$. Then the universal derivation module of $R[x]/J$ is $(R[x]/(J+J'), \partial)$, where J' is the ideal of $R[x]$ generated by the derivatives $\{f_\alpha'\}_{\alpha\in I}$, and $\partial : R[x]/J\to R[x]/(J+J')$ is the R-linear mapping such that $\partial(x^m+J)=mx^{m-1}+(J+J')$,*

PROPOSITION 3. *Let $A_1, \ldots, A_n$ be unitary commutative R-algebras, and (U_i, d_i) a universal derivation module of A_i for each $i=1, \ldots, n$. Let $A=A_1\otimes_R\ldots\otimes_R A_n$, $U=\oplus_{i=1}^n (A\otimes_{A_i} U_i)$, and $d : A\to U$ is an R-derivation defined by*

$$d(\Sigma_\alpha a_{\alpha_1}\ldots a_{\alpha_n}) = \sum_\alpha(\sum_{j=1}^n a_{\alpha_1}\ldots\hat{a}_{\alpha_j}\ldots a_{\alpha_n}\otimes d_j a_{\alpha_j}),$$

where $a_{\alpha_i}\in A_i$, and $\hat{a}_{\alpha_j}$ denotes the omission of a_{α_j}.
Then, (U, d) is a universal derivation module of A.
(see [3, p. 52, Theorem 2]).

2. Derivation module of group rings

In this section, the structure of universal derivation module $U(RG/R)$ of group ring RG (as R-algebra) is explained. Every group G is multiplicative even if it is abelian.

THEOREM 1. *Let $G=\langle g\rangle$ be a cyclic group of order m, generated by g. Suppose that $V=(R/(m))G$, the group ring of G over $R/(m)$, where (m) is the ideal of R generated by $m\in R$. Let $\delta : RG\to V$ be the R-linear mapping such that $\delta(g^r)=\bar{r}g^{r-1}$, for all integer r, where $\bar{r}=r+(m)\in R/(m)$. Then (V, δ) is a universal R-derivation module of RG.*

Proof. Let $R[x]$ be a polynomial ring in one indeterminate x, and J the ideal of $R[x]$ generated by $1-x^m$. Then, $R[x]/J\to RG$ by $x+J\mapsto g$ is an isomorphism. By Proposition 1, $(R[x], d)$ is a universal derivation module of $R[x]$, where $d : R[x]\to R[x]$ is an R-linear mapping such that $d(f)=f'$, the derivative of f in $R[x]$. By Corollary 1, $U(RG/R)\cong R[x]/(J+J')$, where J' is the ideal of $R[x]$ generated by mx^{m-1}. It is not hard to see that $R[x]/(J+J')\cong(R/(m))G$, by $x+J+J'\mapsto g$. By Corollary 1 again, the corresponding derivation $\partial : R[x]/J\to R[x]/(J+J')$ is the R-linear mapping such that $\partial(x^r+J)=rx^{r-1}+J+J'$. Hence,

$$(R[x]/(J+J'), \partial)\cong(V, \delta),$$

and (V, δ) is a universal derivation module of RG.

THEOREM 2. *Let $G=\langle g\rangle$ be an infinite cyclic group generated by g, and let $U=RG$, and $d : RG\to U$ be the R-linear mapping such that $d(g^r)=rg^{r-1}$ for all integer r. Then (U, d) is a universal derivation module of RG.*

Proof. d is obviously an R-derivation, For an arbitrary derivation module (M, δ) of RG, let $\lambda : RG\to M$ be the RG-homomorphism such that $\lambda(1)=\delta(g)$. It is obvious that λ is the unique homomorphism such that $\lambda\circ d=\delta$.

THEOREM 3. *Let G be a finitely generated abelian group, and be decomposed into a direct product of cyclic groups, i.e.,*

$$G=G_1\times\cdots\times G_k\times G_{k+1}\times\cdots\times G_{k+p},$$

where each G_i, $i=1,\ldots,k$, *is a finite froup of order* m_i, *and for each* $i=k+1,\ldots,k+p$, G_i *is an infinite cyclic group. Let*

$$U=(\oplus_{i=1}^{k}((R/(m_i))G)u_i)\oplus(\oplus_{i=k+1}^{k+p}(RG)u_i)$$

where each $((R/(m_i))G)u_i$ *is an one dimensional free* $(R/(m_i))G$*-module with* $\{u_i\}$ *as basis, for* $i=1,\ldots,k$, *and* $(RG)u_i$ *is a free* RG*-module with* $\{u_i\}$ *as basis for* $i=k+1,\ldots,k+p$. *Suppose that each* G_i *is generated by* g_i, *then any element* $x\in RG$ *can be expressed as*

$$x=\sum_{(\nu)}r_{(\nu)}g_1^{\nu_1}\cdots g_{k+p}^{\nu_{k+p}}.$$

Let $d: RG\to U$ *be the* R*-linear mapping such that*

$$d(x)=\sum_{i=1}^{k+p}(\partial x/\partial g_i)u_i,$$

where $\partial x/\partial g_i$ *is the partial derivative of* x *with respect to* g_i. *Then* (U,d) *is a universal derivation module of* RG. *(To avoid any confusion later, we remark that in this theorem* $U=U(RG/R)$, *not* $U(RG/Z)$.*)*

Proof. It is well known that

$$RG\cong RG_1\otimes_R RG_2\otimes_R\ldots\otimes_R RG_{k+p}.$$

Hence, by Proposition 3,

$$U\cong\sum_{i=1}^{k+p}(RG\otimes_{RG_i}U(RG_i/R)).$$

By Theorem 1 and Theorem 2,

$$U(RG_i/R)\cong\begin{cases}((R/(m_i))G_i)u_i, & \text{for } i=1,\ldots,k\\ (RG_i)u_i, & \text{for } i=k+1,\ldots,k+p.\end{cases}$$

Also, it is easy to see that

$$RG\otimes_{RG_i}U(RG_i/R)\cong\begin{cases}((R/(m_i))G)u_i, & \text{for } i=1,\ldots,k\\ (RG)u_i, & \text{for } i=k+1,\ldots,k+p.\end{cases}$$

By using Theorem 1, Theorem 2, and Proposition 3, it is not hard to check that d is the corresponding R-derivation.
It follows that (U,d) is a universal derivation module of RG.

3. Algebraic integers of cyclotomic fields

Let $Q(\sqrt[n]{1})$ be the cyclotomic field of order n over the field, Q, of rational numbers. In this section, R will always denote the ring of algebraic integers of $Q(\sqrt[n]{1})$, namely, $R=$alg. int. $\{Q(\sqrt[n]{1})\}$. In Section 2, we were interested in $U(RG/R)$, but in this section, we will study about the universal derivation modules $U(R/Z)$ and $U(RG/Z)$, where Z is the ring of integers. Hence, all derivations are Z-derivations, and R and RG are considered as Z-algebras.

Let $\pi_n(x)$ be the cyclotomic polynomial of order n, and θ a primitive nth root of 1. It is well known [4, p. 140] that $R=Z[\theta]$. Moreover, since $\pi_n(x)$ is a monic polynomial in $Z[x]$, $R\cong Z[x]/(\pi_n(x))$, where $(\pi_n(x))$ is the ideal of $Z[x]$ generated by $\pi_n(x)$. By Corollary 1,

$$U(R/Z)\cong Z[x]/(\pi_n(x))+(\pi_n'(x)),$$

where $\pi_n'(x)$ is the derivative of $\pi_n(x)$. It is obvious that

$$U(R/Z)\cong Z[\theta]/(\pi_n'(\theta))=R/(\pi_n'(\theta)),$$

where $(\pi_n'(\theta))$ is the ideal of R (or $Z[\theta]$)generated by $\pi_n'(\theta)$.

THEOREM 4. *Let* $R=$alg. int. $\{Q(\sqrt[n]{1})\}$, *where* $n=p_1^{\alpha_1}\dots p_k^{\alpha_k}$. *Then, there exist ideals* $I_1,\dots,I_k$ *of* R *such that* $(p_i^{\alpha_i})\subset I_i\subset(p_i^{\alpha_i-1})$, *where inclusions are proper, and*

$$U(R/Z)\cong R/I_1\oplus\dots\oplus R/I_k.$$

The proof of Theorem 4 is formulated as a consequence of the following Lemmas 1 and 2.

LEMMA 1. *Let* $n=p^\alpha t$, $t>1, p\backslash t$, *and let* θ *be a primitive nth root of* 1. *If* $\tau=\theta^{p^{\alpha-1}}$, τ *is a primitive* (pt)*th root of* 1, *and* $p=\pi_t(\tau)r$, *for some non-unit* $r\in R$.

Proof. In case $n=p^\alpha q^\beta$, $t=q^\beta$ and $\theta^{p^{\alpha-1}q^\beta}$ is a primitive pth root of 1. It is well known [4, p. 139] that

$$p=(\theta^{p^{\alpha-1}q^\beta}-1)^{p-1}u, \text{ where } u \text{ is a unit in } R.$$

Since $t=q^\beta$, $\pi_t(x)=(x^{q^\beta}-1)/(x^{q^{\beta-1}}-1)$. Substituting $\theta^{p^{\alpha-1}}$ for x and clearing the denominator,

$$(\theta^{p^{\alpha-1}q^{\beta-1}}-1)\pi_t(\theta^{p^{\alpha-1}})=\theta^{p^{\alpha-1}q^\beta}-1.$$

Hence,

$$p=(\theta^{p^{\alpha-1}q^\beta}-1)^{p-2}(\theta^{p^{\alpha-1}q^{\beta-1}}-1)\pi_t(\theta^{p^{\alpha-1}})u.$$

Since $\theta^{p^{\alpha-1}q^{\beta-1}}-1$ is a non-unit in R,

$$p=\pi_t(\tau)r, \text{ for some non-unit } r \text{ in } R.$$

To prove the Lemma, we use the induction on the number of distinct prime factors of t. Let

$$t=q^\beta q_1^{\beta_1}\dots q_k^{\beta_k}, \text{ and } s=q_1^{\beta_1}\dots q_k^{\beta_k}.$$

Then $n=p^\alpha q^\beta q_1^{\beta_1}\dots q_k^{\beta_k}$. Since $\pi_t(x)=\prod_{d\mid t}(x^d-1)^{\mu(t/d)}$,

where μ is a Möbius μ-function [4, p. 136],

$$\pi_s(x^{q^{\beta-1}})\pi_t(x)=\pi_s(x^{q^\beta}).$$

Substituting $\theta^{p^{\alpha-1}}$ for x, and using the fact that $\theta^{p^{\alpha-1}q^\beta}$ is a primitive (ps)th root of 1, by the induction hypothesis,

$$p=\pi_s(\theta^{p^{\alpha-1}q^\beta})r_1, \text{ where } r_1 \text{ is a non-unit in } R.$$

Thus,

$$p=\pi_t(\theta^{p^{\alpha-1}})r=\pi_t(\tau)r,$$

for some non-unit r in R.

LEMMA 2. *If* $n=p_1^{\alpha_1}\dots p_k^{\alpha_k}$,

$$(p_1^{\alpha_1}\dots p_k^{\alpha_k})\subset(\pi_n'(\theta))\subset(p_1^{\alpha-1}\dots p_k^{\alpha_k-1}),$$

where π_n' *is the derivative of* π_n, *and the inclusions are proper.*

Proof. In case $n=p^\alpha$, $(x^{p^{\alpha-1}}-1)\pi_n(x)=x^{p^\alpha}-1$. By differentiating both sides of the equation and substituting θ for x,

$$(\theta^{p^{\alpha-1}}-1)\ \pi_n'(\theta)=p^{\alpha}\theta^{p^{\alpha-1}}.$$

Since $\theta^{p^{\alpha-1}}(=\theta^{-1})$ is a unit in R, $\pi_n'(\theta)\supset(p^{\alpha})$.
On the other hand, since $p=(\theta^{p^{\alpha-1}}-1)^{p-1}$ (unit in R),

$$\pi_n'(\theta)=p^{\alpha-1}(\theta^{p^{\alpha-1}}-1)^{p-2}(\text{unit in } R).$$

Hence,

$$(p^{\alpha})\subset\pi_n'(\theta)\subset(p^{\alpha-1}).$$

We use induction on the number of distinct prime factors of n.
Suppose that $n=p^{\alpha}p_1^{\alpha_1}\dots p_k^{\alpha_k}$, and $t=p_1^{\alpha_1}\dots p_k^{\alpha_k}$.
As in the proof of Lemma 1,

$$\pi_t(x^{p^{\alpha-1}})\pi_n(x)=\pi_t(x^{p^{\alpha}}).$$

Taking the derivatives of both sides of the equation, and substituting θ for x,

$$\pi_t(\theta^{p^{\alpha-1}})\pi_n'(\theta)=p\theta^{p^{\alpha}-1}\pi_t'(\theta^{p^{\alpha}}).$$

By the induction hypothesis,

$$(p_1^{\alpha_1}\dots p_k^{\alpha_k})\subset(\pi_t'(\theta^{p^{\alpha}})),$$

and hence,

$$(\pi_n'(\theta))\supset(p^{\alpha}p_1^{\alpha_1}\dots p_k^{\alpha_k}).$$

By Lemma 1, $p=\pi_t(\theta^{p^{\alpha}})r$, for some non-unit in R. Hence,

$$\pi_n'(\theta)=p^{\alpha-1}r\theta^{p^{\alpha}-1}\pi_t'(\theta^{p^{\alpha}}).$$

By the induction hypothesis again, $(\pi_t'(\theta^{p^{\alpha}}))\subset(p_1^{\alpha_1-1}\dots p_k^{\alpha_k-1})$.
Thus,

$$(\pi_n'(\theta))\subset(p^{\alpha-1}p_1^{\alpha_1-1}\dots p_k^{\alpha_k-1}).$$

This proves Lemma 2.

Proof of Theorem 4. It is explained in the beginning of this section that $U(R/Z)\cong R/(\pi_n'(\theta))$. By Lemma 2,

$$(p_1^{\alpha_1}\dots p_k^{\alpha_k})\subset(\pi_n'(\theta))\subset(p_1^{\alpha_1-1}\dots p_k^{\alpha_k-1}).$$

R is a Dedekind domain, and hence, let

$$(\pi_n'(\theta))=\prod_{\mathfrak{p}}\mathfrak{p}_{\nu}^{\nu_{\mathfrak{p}}},$$

be the factorization into prime ideals. Let

$$I_i=\prod_{\mathfrak{p}\supset(p_i)}\mathfrak{p}_{\nu}^{\nu_{\mathfrak{p}}},$$

then $(p_i^{\alpha_i})\subset I_i\subset(p_i^{\alpha_i-1})$, for $i=1,\dots,k$, and

$$(\pi_n'(\theta))=I_1\dots I_k.$$

$\{I_1,\dots,I_k\}$ is a set of pairwise relatively prime integral ideals of R, and hence by the Chinese Remainder Theorem

$$U(R/Z)\cong R/I_1\dots I_k\cong R/I_1\oplus\dots\oplus R/I_k.$$

THECREM 5. *If* $R=$alg. int. $\{Q(\sqrt[n]{1})\}$, $U(R/Z)$ *is a finite abelian (additive) group.*

Proof.: By Theorem 4, $U(R/Z) \cong R/I_1 \oplus \ldots \oplus R/I_k$.

R is known to be a free Z-module of dimension N, where $N=\varphi(n)$ which is the number of positive integers less than or equal to n that are relatively prime to n. Let $\{\lambda_1, \ldots, \lambda_N\}$ be a Z-basis of R. Then $R/(p_i^{\alpha_i})$ is isomorphic to a direct sum of N copies of $Z/Zp_i^{\alpha_i}$ (Notice that we have been using $(p_i^{\alpha_i})$ as the ideal of R generated by $p_i^{\alpha_i}$, hence the ideal of Z generated by $p_i^{\alpha_i}$ is denoted by $Zp_i^{\alpha_i}$.) $I_i \supset (p_i^{\alpha_i})$ implies that the order of the additive group R/I_i is less than or equal to that of $R/(p_i^{\alpha_i})$, which is finite. Hence, each R/I_i is a finite abelian group and $U(R/Z)$ is a finite abelian group.

References

1. R. Berger, *Über verschiedene Differentenbegriffe*, S.-B. Heidelberger Akad. Wiss. Math-nat. K1. 1960/61, 1-44. MR 24 #A1293.
2. I. Y. Chung, *On free joins of algebras and Kähler's differential forms*, Abh. Math Sem. Univ. Hamburg **35** (1970), 92-106. MR 43 #7426.
3. _____, *Derivation modules of free joins and $\mathfrak{M}$-adic completions of algebras*, Proc. Amer. Math. Soc. **34** (1972), 49-56. MR 45 #5122.
4. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure and Appl. Math., **XI**, Interscience, New York, 1962. MR 26 #2519.

Department of Mathematical Sciences,
University of Cincinnati,
Cincinnati, Ohio 45221
U. S. A