〈査読付論文〉

愛知工業大学研究報告
第４５号　平成２２年

On Wedderburn's Theorem

ウェダーバーンの定理について

Takao Sumiyama

隅山孝夫

Abstract. The fact that a finite division ring is commutative is well-known as Wedderburn's theorem. The purpose of this paper is to show a theorem which is a generalization of Wedderburn's theorem.

§0. Introduction

In what follows, a ring is an associative ring with 1. When R is a ring, $J(R)$ denotes the Jacobson radical of R. A ring R is called completely primary if $R/J(R)$ is a division ring.

A finite ring is a ring consisting of only finitely many elements. When R is a finite ring, the number of elements of R is called the order of R. It is easy to see that a finite ring is a direct sum of finite rings of prime-power order. So, if R is a finite, completely primary ring, the order of R is a prime-power.

Note that, though a finite division ring is commutative, a finite, completely primary ring is not necessarily commutative.

Let R be a commutative ring, and A be an algebra over R which is finitely generated as R-module. Let A^o be the opposite algebra of A. The algebra $A^e = A \otimes_R A^o$ over R is called the enveloping algebra of A. By the operation

$$(a \otimes b)x = axb,$$

A is a left A^e-module. The algebra A is called separable over R if A is projective as left A^e-module.

Let $\phi : A^e \longrightarrow A$ be the natural surjection given by $\phi(a \otimes b) = ab$. It is well-known that the following (i)-(iii) are equivalent (see, for instance, [2, §68, §69]).

(i) A is separable over R.

(ii) The exact sequence

$$0 \longrightarrow Ker(\phi) \longrightarrow A^e \xrightarrow{\phi} A \longrightarrow 0$$

splits, that is, there exists a left A^e-homomorphism $\alpha : A \longrightarrow A^e$ such that $\phi \circ \alpha = id_A$.

(iii) There exists an idempotent $e = \sum_i a_i \otimes b_i$ in A^e such that $(Ker\ \phi)e = 0$ and $\phi(e) = 1$.

If this is the case, the element e of A^e satisfying (iii) is called a separability idempotent for A.

愛知工業大学研究報告, 第45号, 平成22年, Vol. 45, Mar., 2010

§1.

Let R be a ring. When we say that S is a subring of R, S must contain 1 of R. The prime ring of R is the subring of R generated by 1. By what is stated above, if R is a finite, completely primary ring, the prime ring of R must be $\mathbf{Z}_{p^k} = \mathbf{Z}/(p^k)$, where p is a prime.

Proposition. *Let R be a finite, completely primary ring whose prime ring is $\mathbf{Z}_p$. If R is separable over $\mathbf{Z}_p$, then $J(R) = 0$, that is, R is a finite field.*

Proof. We shall show that $J(R)$ is projective as left R-module. Let

$$(\mathrm{E}) \qquad P \xrightarrow{\ \eta\ } J(R) \longrightarrow 0$$

be an exact sequence of left R-modules. As $J(R)$ is free over $\mathbf{Z}_p$, as $\mathbf{Z}_p$-modules, the sequence (E) splits. That is, there exists a left $\mathbf{Z}_p$-homomorphism $\alpha : J(R) \longrightarrow P$ such that $\eta \circ \alpha = id_{J(R)}$.

Let $e = \sum_i a_i \otimes b_i$ be a separability idempotent for R. Let us define $\alpha^* : J(R) \longrightarrow P$ by

$$\alpha^*(x) = \sum_i a_i \alpha(b_i x) \quad (x \in J(R)).$$

We shall show that α^* is a left R-homomorphism satisfying $\eta \circ \alpha^* = id_{J(R)}$.

For $x \in J(R)$,

$$\begin{aligned} \eta \circ \alpha^*(x) &= \eta(\sum_i a_i \alpha(b_i x)) \\ &= \sum_i a_i \eta(\alpha(b_i x)) \\ &= \sum_i a_i b_i x. \end{aligned}$$

As $\sum_i a_i b_i = 1$, we see $\eta \circ \alpha^*(x) = x$.

Let d be a fixed element of $J(R)$. Then $\tau : R \times R \longrightarrow P$ given by $\tau(x, y) = x\alpha(yd)$ is a $\mathbf{Z}_p$-bilinear mapping from $R \times R$ to P. By the property of tensor product, there exists a $\mathbf{Z}_p$-bilinear mapping $\sigma : R \otimes_{\mathbf{Z}_p} R \longrightarrow R$ such that $\sigma(x \otimes y) = \tau(x, y)$ $(x, y \in R)$.

From $(Ker\phi)e = 0$, for $r \in R$, it holds that

$$\sum_i (ra_i) \otimes b_i = \sum_i a_i \otimes (b_i r).$$

Hence,

$$\begin{aligned} r\alpha^*(d) &= r \sum_i a_i \alpha(b_i d) \\ &= \sum_i r a_i \alpha(b_i d) \\ &= \sigma(\sum_i (r a_i) \otimes b_i) \\ &= \sigma(\sum_i a_i \otimes (b_i r)) \\ &= \sum_i a_i \alpha(b_i r d) \\ &= \alpha^*(rd). \end{aligned}$$

So we see that α^* is an R-homomorphism, and $J(R)$ is projective as left R-module.

As every projective module over a completely primary ring is free ([1, p. 300, Corollary 26.7]), $J(R)$ is free as R-module. As $J(R)$ is a proper subset of R, we see $J(R)=0$.

§2.

The fact that a finite division ring is commutative is well-known as Wedderburn's theorem ([2, p. 458, Theorem 68.9]). The following is a generalization of this theorem.

Theorem. *Let R be a finite, completely primary ring whose prime ring is $\mathbf{Z}_{p^k}$. If R is separable over $\mathbf{Z}_{p^k}$, then R is commutative.*

Proof. Let $\mathbf{Z}_{p^k}[X]$ denote the ring of all polynomials of variable X with coefficients in $\mathbf{Z}_{p^k}$.

In what follows, when S is a finite set, $|S|$ denotes the number of elements of S. Since $K = R/J(R)$ is a finite field, there exists $\bar{a} \in K$ such that $K = \mathbf{Z}_p[\bar{a}]$ ($\mathbf{Z}_p[\bar{a}]$ denotes the subfield of K generated by $\bar{a}$). Let $|K| = p^r$, and $f(X) \in \mathbf{Z}_p[X]$ be the monic, minimal polynomial of $\bar{a}$. Let $a \in R$ be a pre-image of $\bar{a}$. Then the subring R_0 of R generated by a is a finite, commutative completely primary ring (since R_0 has no nontrivial idempotents) such that $R_0/J(R_0) = K$. By making use of Hensel's lemma, we can see that R_0 contains a subring S such that $|S| = p^{kr}$ and $S/J(S) = K$ (see [3, Theorem 8 (i)]).

Next, we shall show that R/pR is separable over $\mathbf{Z}_p$. To do this, we see that $\mathrm{Hom}_{(R/pR)^e}(R/pR,\ )$ is cokernel preserving.

Let T be a left $(R/pR)^e$-module. By the operation

$$(a \otimes b)x = (a+pR) \otimes (b+pR)x \quad (a, b \in R,\ x \in T),$$

T is a left R^e-module. We shall show that, as additive groups, $\mathrm{Hom}_{(R/pR)^e}(R/pR, T)$ is naturally isomorphic to $\mathrm{Hom}_{R^e}(R, T)$.

Let $f : R \longrightarrow T$ be an R^e-homomorphism. As $f(1)$ is in T, we can define

$$\varphi : \mathrm{Hom}_{R^e}(R, T) \longrightarrow \mathrm{Hom}_{(R/pR)^e}(R/pR, T)$$

by

$$\varphi(f)(a+pR) = (a+pR) \otimes (1+pR)f(1) \quad (a+pR \in R/pR).$$

It is easy to see that $\varphi(f)$ is in $\mathrm{Hom}_{(R/pR)^e}(R/pR, T)$.

Conversely, let $g : R/pR \longrightarrow T$ be an $(R/pR)^e$-homomorphism. We can define

$$\psi : \mathrm{Hom}_{(R/pR)^e}(R/pR, T) \longrightarrow \mathrm{Hom}_{R^e}(R, T)$$

by

$$\psi(g)(r) = g(r+pR) \quad (r \in R).$$

It is easy to see that $\psi(g)$ is in $\mathrm{Hom}_{R^e}(R,T)$, $\psi(\varphi(f)) = f$, and $\varphi(\phi(g)) = g$.

So we see that R/pR is separable over $\mathbf{Z}_{p^k}$.

As $(R/pR)\otimes_{\mathbf{Z}_{p^k}} = (R/pR)\otimes_{\mathbf{Z}_p}$, R/pR is separable over $\mathbf{Z}_p$. By Proposition, $J(R/pR) = 0$, which implies $J(R) = pR$.

Now, there exists the following natural sequence of surjective ring homomorphisms σ_i :

$$R = R/p^kR \xrightarrow{\sigma_k} R/p^{k-1}R \xrightarrow{\sigma_{k-1}} \cdots \xrightarrow{\sigma_2} R/pR = K ,$$

where $Ker(\sigma_i) = p^{i-1}R/p^iR$.

We see

$$\begin{aligned} |R| &= |K| \cdot \prod_{i=2}^{k} |Ker(\sigma_i)| \\ &= |K| \cdot \prod_{i=2}^{k} |p^{i-1}R/p^iR|. \end{aligned}$$

As $pR \otimes_{\mathbf{Z}_{p^k}} (p^i\mathbf{Z}_{p^k})$ is embedded in $R \otimes_{\mathbf{Z}_{p^k}} (p^i\mathbf{Z}_{p^k})$,

$$\begin{aligned} p^{i-1}R/p^iR &\cong (R \otimes_{\mathbf{Z}_{p^k}} (p^{i-1}\mathbf{Z}_{p^k}))/(R \otimes_{\mathbf{Z}_{p^k}} (p^i\mathbf{Z}_{p^k})) \\ &\cong (R \otimes_{\mathbf{Z}_{p^k}} (p^{i-1}\mathbf{Z}_{p^k}))/(pR \otimes_{\mathbf{Z}_{p^k}} (p^i\mathbf{Z}_{p^k}) + R \otimes_{\mathbf{Z}_{p^k}} (p^i\mathbf{Z}_{p^k})) \\ &\cong (R/pR) \otimes_{\mathbf{Z}_{p^k}} (p^{i-1}\mathbf{Z}_{p^k}/p^i\mathbf{Z}_{p^k}) \\ &\cong K \otimes_{\mathbf{Z}_{p^k}} (p^{i-1}\mathbf{Z}_{p^k}/p^i\mathbf{Z}_{p^k}). \end{aligned}$$

So,

$$|p^{i-1}R/p^iR| = |p^{i-1}\mathbf{Z}_{p^k}/p^i\mathbf{Z}_{p^k}|^r = p^r,$$

and

$$\begin{aligned} |R| &= |K| \cdot \prod_{i=2}^{k} |p^{i-1}R/p^iR| \\ &= p^r \cdot (p^r)^{k-1} \\ &= p^{kr}. \end{aligned}$$

As S is a subring of R and $|S| = |R|$, we see $S = R$. So R is commutative.

References

[1] F. W. Anderson and K. R. Fuller, Rings and Categories of Modules, Springer-Verlag, New York-Heidelberg-Berlin (1974).

[2] C. W. Curtis and I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Interscience, John Wiley, New York-London-Sydney (1962).

[3] R. Raghavendran, Finite associative rings, Compositio Math. 21 (1969), 195-229.