ON THE RING OF COMPLEX-VALUED FUNCTIONS ON A FINITE RING

YASUYUKI HIRANO

Abstract. Greferath, Fadden and Zumbrägel [3] consider rings of complex-valued functions on some finite rings R. In this paper we consider the structure of such rings. First we consider the case when R is a finite local ring. Next we consider the case when R is a finite semisimple ring. Finally we consider rings of complex-valued invariant functions on some finite rings.

1. Rings of functions from a finite ring to the field of complex numbers

Greferath, Fadden and Zumbrägel [3] consider rings of complex-valued functions on some finite rings. First we give some definitions.

Definition 1. Let R be a ring and let $\mathbf{C}$ denote the field of complex numbers. A function $f : R \to \mathbf{C}$ is said to be *finite* if $\{r \in R \mid f(r) \neq 0\}$ is a finite set.

Consider the set $\mathbf{C}^R = \{f \mid f : R \to \mathbf{C} \text{ is finite}\}$ of all finite functions from R to $\mathbf{C}$.

Definition 2. For $f,\ g \in \mathbf{C}^R$ and for $\lambda \in \mathbf{C}$ we define addition and scalar multiplication by

$$(f + g)(x) = f(x) + g(x)$$

$$(\lambda f)(x) = \lambda f(x).$$

Then $\mathbf{C}^R$ is a $\mathbf{C}$-vector space. We define multiplication by

$$(f * g)(x) = \sum_{\substack{a, b \in R \\ ab = x}} f(a)g(b).$$

Then $\mathbf{C}^R$ is a $\mathbf{C}$-algebra.

For any element $r \in R$, we define the function δ_r by

$$\delta_r(x) = \begin{cases} 1 & \text{if } x = r \\ 0 & \text{otherwise.} \end{cases}$$

Then δ_1 is is the identity of the $\mathbf{C}$-algebra $\mathbf{C}^R$. We can easily see that $\delta_r * \delta_s = \delta_{rs}$ for each $r,\ s \in R$. Also we can see that the set $\{\delta_r \mid r \in R\}$ forms a $\mathbf{C}$-basis of vector space.

The detailed version of this paper will be submitted for publication elsewhere.

Definition 3. Let R be a ring with addition $+$ and multiplication $\cdot$. We denote the semigroup algebra of the semigroup $(R, \ \cdot)$ over $\mathbf{C}$ by $\mathbf{C}[R]$. Any element of $\mathbf{C}[R]$ can be written as a finite sum of the form $\sum_{r\in R} a_r\hat{r}$. For the definition of semigroup algebras, see [4, Page 33].

Other definitions and some basic results in this paper can be found in [2]. We start with the following fundamental proposition.

Proposition 4. *Let R be a finite ring. Then the $\mathbf{C}$-algebra $\mathbf{C}^R$ is isomorphic to the semigroup algebra $\mathbf{C}[R]$ of multiplicative semigroup $(R, \ \cdot \ )$ of the ring R.*

Proof. Recall that the semigroup algebra $\mathbf{C}[R]$ is a $\mathbf{C}$-vector space with the $\mathbf{C}$-basis $\{\hat{r} \mid r \in R\}$ and multiplication defined by

$$\hat{r}\hat{s} = \widehat{rs}$$

for each $r, \ s \in R$. We define a mapping $\phi : \mathbf{C}^R \to \mathbf{C}[R]$ by $\phi(\delta_r) = \hat{r}$ for each $r \in R$. Then ϕ is an isomorphism of $\mathbf{C}$-algebras. $\square$

2. Semigroup rings

First we give some basic results on semigroup rings of the semigroups of some rings.

Proposition 5. *Let R be a ring, let I be an ideal of R and let $\mathbf{Z}$ denote the ring of rational integers.*

(1) *Let A denote the ideal of $\mathbf{Z}[R]$ generated by $\{\widehat{r+s} - \hat{r} - \hat{s} \mid r, s \in R\}$. Then $\mathbf{Z}[R]/A \cong R$.*

(2) *Let B denote the ideal of $\mathbf{C}[R]$ generated by $\{\hat{r} - \hat{s} \mid r - s \in I\}$. Then $\mathbf{C}[R]/B \cong \mathbf{C}[R/I]$.*

Proposition 6. *Let R be a finite ring, let R^* denote the group of units in R and let C denote the ideal of $\mathbf{C}[R]$ generated by $\{\hat{r} \mid r \in R - R^*\}$. Then $\mathbf{C}[R]/C \cong \mathbf{C}[R^*]$.*

For a ring R, $J(R)$ denotes the Jacobson radical of R.

Proposition 7. *Let R be a finite local ring and let R^* denote the group of units in R. Then $J(\mathbf{C}[R]) = \sum_{r\in J(R)} \mathbf{C}(\hat{r} - \hat{0})$ and $\mathbf{C}[R]/J(\mathbf{C}[R]) \cong \mathbf{C}\hat{0} \oplus \mathbf{C}[R^*]$.*

Example 8. Consider the ring $R = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{pmatrix} \ \middle| \ a, \ b, \ c \in GF(2) \right\}$. Then $|R| = 2^4 = 16$. Then $R^* = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{pmatrix} \ \middle| \ a \neq 0, \ b, \ c \in GF(2) \right\}$. We can easily see that R^* is the dihedral group D_8 of order 8 and so $\mathbf{C}[R^*] \cong \mathbf{C}^4 \oplus M_2(\mathbf{C})$. Therefore $\mathbf{C}[R]/J(\mathbf{C}[R]) \cong \mathbf{C}^5 \oplus M_2(\mathbf{C})$.

By Proposition 7 we have the following corollaries.

Corollary 9. *Let R be a finite commutative local ring and let n denote the number of elements of R^*. Then $\mathbf{C}[R]$ is the direct sum of $n+1$ finite commutative local rings.*

Corollary 10. *Let R be a finite commutative ring and suppose that $R = R_1 \oplus \cdots \oplus R_d$, where $R_1, \cdots R_d$ are finite commutative local rings. Then $\mathbf{C}^R$ is the direct sum of $(|R_1^*| + 1) \times \cdots \times (|R_d^*| + 1)$ finite commutative local rings.*

Corollary 11. *Consider the Galois field $G(n,p)$. Then the $\mathbf{C}$-algebra $\mathbf{C}^{G(n,p)}$ is isomorphic to $\mathbf{C}^{p^n}$.*

Let V be a vector space over $\mathbf{C}$. We define a multiplication on the $\mathbf{C}$-linear space $\mathbf{C} \oplus V$ by the formula $(a, v) \cdot (b, w) = (ab, aw + bv)$ for any $a,\ b \in \mathbf{C},\ v,\ w \in V$. Then $\mathbf{C} \oplus V$ becomes an $\mathbf{C}$-algebra. We denote this algebra by $\mathbf{C} \ltimes V$.

Example 12. Consider the ring $\mathbf{C}[\mathbf{Z}/8\mathbf{Z}]$ and let $g_i = \hat{i} - \hat{0}$ for $i = 1, 2, \cdots, 7$. Then $\mathbf{C}[\mathbf{Z}/8\mathbf{Z}]$ is the direct sum of two sided ideals $\mathbf{C}\hat{0}$ and $S = \mathbf{C}g_1 + \mathbf{C}g_2 + \cdots + \mathbf{C}g_7$. The identity of the ring S is g_1. Let us set $e_1 = (1/4)(g_1 - g_3 - g_5 + g_7)$, $e_2 = (1/4)(g_1 + g_3 - g_5 - g_7)$, $e_3 = (1/4)(g_1 - g_3 + g_5 - g_7)$ and $e_4 = (1/4)(g_1 + g_3 + g_5 + g_7)$. Then $e_1,\ e_2,\ e_3,\ e_4$ are orthogonal central primitive idempotents of S and $g_1 = e_1 + e_2 + e_3 + e_4$. We can easily see $e_1 S \cong \mathbf{C}$, $e_2 S \cong \mathbf{C}$, $e_3 S \cong \mathbf{C} \ltimes \mathbf{C}$ and $e_4 S \cong \mathbf{C} \ltimes (\mathbf{C} \oplus \mathbf{C})$. Therefore $\mathbf{C}[\mathbf{Z}/8\mathbf{Z}] \cong \mathbf{C}^3 \oplus \{\mathbf{C} \ltimes \mathbf{C}\} \oplus \{\mathbf{C} \ltimes (\mathbf{C} \oplus \mathbf{C})\}$.

3. Rings of functions from a finite semisimple ring to the field of complex numbers

In this section we consider the case when the ring R is a finite simple ring.

Theorem 13. *Let R be a finite ring. Then the following are equivalent:*
(i) *R is a finite semisimple ring.*
(ii) *$\mathbf{C}^R$ is a semisimple Artinian ring.*

A von Neumann regular ring is a ring R such that for every a in R there exists an x in R such that $a = axa$. Since a semisimple Artinian ring is von Neumann regular, we have the following corollary.

Corollary 14. *Let R be a finite semisimple ring. Then, for any function $f \in \mathbf{C}^R$, there exists a function $g \in \mathbf{C}^R$ such that $a = a * x * a$.*

Example 15. Let $M_2(GF(2))$ denote the ring of 2×2 matrices over the field $GF(2)$. Then we can prove that $\mathbf{C}[M_2(GF(2))]$ is a semiprime ring. Let us set $H = M_2(GF(2)) - GL_2(GF(2))$. Then we can see that $\mathbf{C}[H] \cong \mathbf{C} \oplus M_3(\mathbf{C})$. In fact, let
$O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $e_3 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $e_4 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, $e_5 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$, $e_6 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$, $e_7 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$, $e_8 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ and $e_9 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. Then $E = \hat{O}, F_1 = \hat{e_1} - \hat{O}, F_2 = \hat{e_2} - \hat{O}, F_3 = (\hat{e_1} - \hat{O}) + (\hat{e_2} - \hat{O}) + (\hat{e_3} - \hat{O}) + (\hat{e_4} - \hat{O}) - (\hat{e_5} - \hat{O}) - (\hat{e_6} - \hat{O}) - (\hat{e_7} - \hat{O}) - (\hat{e_8} - \hat{O}) + (\hat{e_9} - \hat{O})$ are primitive orthogaonal idempotents, and $\mathbf{C}[H] = \mathbf{C}E \oplus \mathbf{C}[H](F_1 + F_2 + F_3) \cong \mathbf{C} \oplus M_3\mathbf{C})$. Since $GL_2(GF(2)) \cong S_3$, we have $\mathbf{C}[M_2(GF(2))]/\mathbf{C}[H] \cong \mathbf{C}[S_3]$. It is easily see that $\mathbf{C}[S_3] \cong \mathbf{C} \oplus \mathbf{C} \oplus M_2(\mathbf{C})$. Hence $\mathbf{C}[M_2(GF(2))]$ is isomorphic to the semisimple Artinian ring $\mathbf{C} \oplus \mathbf{C} \oplus \mathbf{C} \oplus M_2(\mathbf{C}) \oplus M_3(\mathbf{C})$.

Question 16. Let R be a (not necessarily finite) semiprime ring. Is $\mathbf{C}[R]$ semiprime?

Question 17. Let R be a finite semisimple ring and let C be a commutative ring. What conditions on C imply that $C[R]$ is a separable algebra over C? The definition of separability can be found in [1, Page 40].

4. Invariant functions

Let R ba a finite ring. A function $f : R \to \mathbf{C}$ is said to be *right invariant* if $f(ax) = f(a)$ for all $a \in R$ and all $x \in R^*$. Similarly we define a *left invariant function*. A right and left invariant function is called an *invariant function*.

Theorem 18. *Let R ba a finite ring.*

(1) *If we set $e = (1/|R^*|)\sum_{x \in R^*} \hat{x} \in \mathbf{C}[R]$, then e is an idempotent.*
(2) *The set of right invariant functions becomes the right ideal $\mathbf{C}[R]e$.*
(3) *The set of invariant functions becomes the ring $e\mathbf{C}[R]e$.*

Corollary 19. *Let R be a finite semisimple ring. The ring of invariant functions from R to $\mathbf{C}$ is a semisimple Artinian ring.*

References

[1] F. DeMeyer and E. Ingraham, Separable Algebras Over Commutative Rings, Lecture Notes **181**, 1971(Springer-Verlag).

[2] Y.A. Drozd and V.V. Kirichenko, Finite-dimensional algebras, Springer-Verlag, Berlin, 1994.

[3] M. Greferath, C.M. Fadden and J. Zumbrägel,*Characteristics of invariant weights related to code equivalence over rings*, Des. Codes Cryptography **66**(1-3) (2013), 145–156.

[4] J. Okniński, Semigroup Algebras, CH/CRC Pure & Applie Vol.**138**, Dekker, 1991.

Department of Mathematics Education
Graduate School of Education
Naruto University of Education
Naruto 772-8502, Japan

E-mail address: yahirano @ naruto-u.ac.jp