

行列環上の巡回符号について

大阪樟蔭女子大学・児童学部 松岡 学

Manabu Matsuoka

Faculty of Child Sciences,

Osaka Shoin Women's University

1 はじめに

有限体 $\mathbf{F}$ 上のベクトル空間 $\mathbf{F}^n = \{(a_0, \dots, a_{n-1}) \mid a_i \in \mathbf{F}\}$ の部分空間 C のことを長さ n の線形符号という。線形符号 $C \subseteq \mathbf{F}^n$ が条件

$$(a_0, a_1, \dots, a_{n-1}) \in C \text{ ならば } (a_{n-1}, a_0, a_1, \dots, a_{n-2}) \in C$$

を満たすとき、巡回符号であるという。

J. A. Wood は有限フロベニウス環上の符号理論を [8] において確立した。また、M. Greferath と M. E. O'Sullivan は有限フロベニウス環上のブロック符号を [2]. において調べた。

本稿においては、有限 QF 環上の符号理論を構築することを考察する。

以後特に断らない限り、 R は（必ずしも可換ではない）環、 n は 2 以上の自然数、 (g) は $g \in R[X]$ によって生成される両側イデアルを表すものとする。

2 QF 環

R を環とする。左 R -加群 P が射影加群であるとは、任意の全射 R -準同型写像 $g : M \rightarrow N$ と任意の R -準同型写像 $f : P \rightarrow N$ に対して、適当な R -準同型写像 $h : P \rightarrow M$ が存在して、 $f = g \circ h$ が成り立つことをいう。任意の射影加群が自由加群に埋め込まれることはよく知られている。

左 R -加群 Q が入射加群であるとは、任意の単射 R -準同型写像 $g : N \rightarrow M$ と任意の R -準同型写像 $f : N \rightarrow Q$ に対して、適当な R -準同型写像 $h : M \rightarrow Q$ が存在して、 $f = h \circ g$ が成り立つことをいう。任意の加群が入射加群に埋め込まれることはよく知られている。

環 R は R 自身が左（右）加群として入射的であるとき、左（右）自己入射環であるという。 R が左自己入射であり、右自己入射でもあるとき、単に自己入射環であるという。

左 R -加群 M がアルチン加群 とは M が部分加群に関して降鎖条件を満たすことであるという。

環 R は R 自身が左 (右) 加群としてアルチン加群であるとき、左 (右) アルチン環であるという。 R が左アルチンであり、右アルチンでもあるとき、単にアルチン環であるという。

降鎖条件の代わりに昇鎖条件にすることで、ネーター加群やネーター環を定義することができる。

有限環は明らかにアルチン環である。

M を左 R -加群とする。部分集合 $X \subseteq M$ に対して、 X の annihilator を

$$\text{ann}_l(X) = \{r \in R \mid \text{任意の } x \in X \text{ に対して } rx = 0\},$$

と定める。これは R の左イデアルとなる。右 R -加群の部分集合 X の annihilator $\text{ann}_r(X)$ も同様に定義される。これは R の右イデアルとなる。

定理 1. 任意の環 R に対して、次の条件は同値である。

- (1) R は右アルチンかつ右自己入射環である。
- (2) R は左アルチンかつ左自己入射環である。
- (3) R は右ネーター環であり、次の条件を満たす。
 - (3a) 任意の右イデアル $A \subseteq R$ に対して $\text{ann}_r(\text{ann}_l A) = A$ が成り立つ。
 - (3b) 任意の左イデアル $I \subseteq R$ に対して $\text{ann}_l(\text{ann}_r I) = I$ が成り立つ。

定義 2. 定理 1 の条件を満たす環を QF (quasi-Frobenius) 環と呼ぶ。

QF (quasi-Frobenius) 環の定義は左右対称であることが分かる。

任意の左 R -加群 ${}_R M$ に対して、 $M^* = \text{Hom}_R({}_R M, {}_R R)$ は、右 R -加群になる。 R の右からの作用は次のように定義される。

$$(f \cdot r)(m) = f(m) \cdot r$$

ここで、 $r \in R, m \in M, f \in M^*$ である。

自然な準同型写像 $\xi: M \rightarrow M^{**}$ を次のように定義する。

$$\xi(m)(f) = f(m)$$

ここで、 $m \in M, f \in M^*$ である。

自然な準同型写像 $\xi: M \rightarrow M^{**}$ が単射であるとき、加群 M は torsionless と呼ばれる。自然な準同型写像 $\xi: M \rightarrow M^{**}$ が全単射であるとき、加群 M は reflexive と呼ばれる。

定理 3. R を QF 環とする。任意の有限生成 R -加群 M は reflexive である。

M の任意の部分加群 A に対して、 $A^\circ = \{f \in M^* \mid f(A) = 0\}$ と定める。これは M^* の部分加群になる。

定理 4. R を QF 環、 ${}_R M$ を有限生成左 R -加群とする。 M の任意の部分加群 A に対して、左 R -加群の同型 $A^{\circ\circ} \cong A$ が成り立つ。

3 環上の巡回符号

R を有限環とする。 R^n の階数が k の左自由部分加群 $C \subseteq R^n$ を、 R 上の左線形 $[n, k]$ -符号とよぶ。 n を線形符号 C の長さという。

R 上に次のような標準的な内積を定義する。

$x = (x_0, x_1, \dots, x_{n-1}), y = (y_0, y_1, \dots, y_{n-1}) \in R^n$ に対して

$$\langle x, y \rangle = \sum_{i=0}^{n-1} x_i y_i$$

左線形符号 C の双対符号 $C^\perp$ を次のように定義する。

$$C^\perp = \{a \in R^n \mid \text{任意の } c \in C \text{ に対して } \langle c, a \rangle = 0\}.$$

明らかに $C^\perp$ は R 上の右線形符号になる。

命題 5. 有限環 R の左線形符号 C に対して、右加群としての同型 $C^\perp \cong C^\circ$ が成り立つ。

定理 4 と命題 5 より、次のことが成り立つ。

定理 6. R を有限 QF 環、 C を R^n の左線形符号とする。このとき、 $(C^\perp)^\perp = C$ が成り立つ。

双対符号 $C^\perp$ の階数に関しては、次が成り立つ。

定理 7. R を有限 QF 環、 $C \subseteq R^n$ を有限階数の左自由部分加群とする。このとき、 $C^\perp$ は有限階数の右自由加群であり、階数は、 $\text{rank} C^\perp = n - \text{rank} C$ となる。

定理 5 と定理 6 に関しては、環 R が有限であるという条件は必要ない。

次に、巡回符号を定義する。

定義 8. C を R 上の長さが n の左線形符号とする。 C が条件

$$(a_0, a_1, \dots, a_{n-1}) \in C \text{ ならば } (a_{n-1}, a_0, a_1, \dots, a_{n-2}) \in C$$

を満たすとき、巡回符号であるという。

巡回符号は多項式環の剰余環の左イデアルとみなすことができる。左 R -加群としての準同型写像 $\rho : R^n \rightarrow R[X]/(x^n - 1)$ を $a = (a_0, a_1, \dots, a_{n-1})$ に対して、同値類 $\overline{a_{n-1}X^{n-1} + \dots + a_1X + a_0}$ を対応させる写像と定義する。このとき、 R^n の巡回符号と $R[X]/(x^n - 1)$ の左イデアルを ρ を通して同一視することができる。

4 行列環の構成と巡回符号

歪多項式環を用いることで、行列環を構成する。

定義 9. R を環, θ をその自己準同型写像とする。 S を $1, x, x^2, \dots$ を基底とする左自由 R -加群とし、積を $x^i x^j = x^{i+j}$ と $xr = \theta(r)x$ により定める。ここで、 $r \in R$ とする。このように構成された環 S を歪多項式環と呼び、記号 $R[x; \theta]$ で表わす。

位数が p の有限体を成分とする行列環を、歪多項式環を用いて構成する。

定理 10. $\mathbf{F}_{p^r}$ を位数が p^r の有限体とし、 σ をそのフロベニウス写像とする。このとき、次の同型が成り立つ。

$$\mathbf{F}_{p^r}[x; \sigma] \cong M_r(\mathbf{F}_p).$$

行列環の巡回符号を具体的に求めるには、行列環を係数とする多項式環の剰余環の構造を決定する必要がある。

例 11. 行列環 $R = M_2(\mathbf{F}_2)$ に対して、中心は $Z = \mathbf{F}_2$ であり、次の同型が成り立つ。

$$R[x]/(x^3 - 1) \cong R \otimes_Z Z[x]/(x^3 - 1) \cong M_2(\mathbf{F}_2) \oplus M_2(\mathbf{F}_4).$$

今後は、行列環だけでなく、一般の QF 環の巡回符号を決定する方法を開発する必要がある。

参考文献

- [1] D. Boucher and P. Solé, *Skew constacyclic codes over Galois rings*, Advances in Mathematics of Communications, Volume **2**, No. **3** (2008), 273–292.
- [2] M. Greferath, M. E. O’Sullivan, *On bounds for codes over Frobenius rings under homogeneous weights*, Discrete Math, **289** (2004), 11–24.
- [3] Y. Hirano, *On admissible rings*, Indag. Math. **8** (1997), 55–59.
- [4] S. Ikehata, *On separable polynomials and Frobenius polynomials in skew polynomial rings*, Math. J. Okayama. Univ. **22** (1980), 115–129.
- [5] T. Y. Lam, *Lectures on Modules and Rings*, Graduate Texts in Mathematics, Vol. 189, Springer-Verlag, New York, 1999.
- [6] S. R. López-Permouth, B. R. Parra-Avila and S. Szabo, *Dual generalizations of the concept of cyclicity of codes*, Advances in Mathematics of Communications, Volume **3**, No. **3** (2009), 227–234.

- [7] B. R. McDonald, *Finite Rings With Identity, Pure and Applied Mathematics*, Vol. 28, Marcel Dekker, Inc., New York, 1974.
- [8] J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math, **121** (1999), 555–575.