# リードソロモン符号

## 1　基礎知識

### 1.1　多項式環

$R$ を可換環とするとき、$R$ 上の元を係数とする多項式全体の集合

$$R[T] := \left\{ a_0 + a_1 T^1 + \cdots + a_n T^n \;\middle|\; n \in \mathbb{Z}, 0 \leq n, a_0, \ldots a_n \in R \right\}$$

は可換環を成す。これを多項式環という。

**証明 1**　hoge

また、$R[T]$ 上のある元 $f(T)$ が

$$f(T) = a_0 + a_1 T^1 + \cdots + a_n T^n$$

と書かれて $a_n \neq 0$ であるとき、$n$ を $f(T)$ の次数といい deg(f(T)) と書く。

### 1.2　多項式環上での除法

ある体 $K$ による多項式環 $K[T]$ に除法が定義される。

**定理 1（除法）**　ある $f(T), g(T) \in K[T], g(T) \neq 0$ に対して

$$f(T) = q(T)g(T) + r(T) \quad (\deg(\mathrm{r(T)}) < \deg(\mathrm{g(T)}))$$

を満たす $q(T), r(T) \in K[T]$ の組が唯一つ存在し $q(T)$ を商、$r(T)$ を剰余という。また $r(T)$ が $r(T) = 0$ であるとき、$g(T)$ は $f(T)$ を割り切るといい $g(T) \mid f(T)$ と書く。そして 2 つの多項式 $f(T), g(T) \in K[T]$ を割り切るモニックな多項式を最大公約多項式という。ここでモニックな多項式とは最高次数の係数が 1 であるような多項式のことである。

### 1.2.1　イデアル

**定理 2（イデアル）**　ある可換環 $R$ に対して、$R$ の部分集合 $I$ が以下の 2 つを満たすとき、$I$ を $R$ のイデアルという。

1. $a, b \in I \Rightarrow a + b \in I$
2. $a \in I, r \in R \Rightarrow ar \in I$

ある $a \in R$ によって

$$(a) = \{ax \mid x \in R\}$$

と書かれる $(a)$ はイデアルであり、$a$ によって生成される単項イデアルという。また、$a, b \in R$ によって

$$(a, b) = \{ax + by \mid x, y \in R\}$$

と書かれる [tex: (a, b) ] もイデアルである。

体 $K$ 上の多項式環 $K[T]$ も可換環であるため $K[T]$ にもイデアルが存在する。このとき、$K[T]$ のイデアルは単項イデアルしか存在しない。

**証明 2**　$I \neq \{0\}$ を $K[T]$ のイデアルとする。$I$ の元のうち最も次元が小さい元を $f(T)$ とする。

ここで、任意に $g(T)$ をとる。そして $g(T)$ を $f(T)$ で割ると

$$g(T) = q(T)f(T) + r(T) \quad (\deg(\mathrm{r(T)}) < \deg(\mathrm{f(T)}))$$

を満たす $q(T), r(T) \in K[T]$ が存在する。また式を変形すると

$$\begin{aligned} & g(T) = q(T)f(T) + r(T) \\ \rightleftharpoons\ & r(T) = g - q(T)f(T) \\ \rightleftharpoons\ & r(T) = g + q(T)(-f(T)) \end{aligned}$$

となる。$f(T), g(T) \in I$ であったこととイデアルの定義から $r(T) \in I$ が得られる。ここで、$r(T) \neq 0$ とすると $\deg(\mathrm{r(T)}) < \deg(\mathrm{f(T)})$ であることから $f(T)$ の最小性に矛盾する。したがって $r(T) = 0$ である。よって $g(T) = q(T)f(T)$ となり $g(T) \in (f(T))$ となる。したがって $I \subset (f(T))$ である。

逆に $f(T) \in I$ であるため $(f(T)) \subset I$ でもある。

以上より $I = (f(T))$ が示された。

また、$f(T), g(T) \in K[T]$ によって生成されるイデアル $(f(T), g(T))$ は $f(T)$ と $g(T)$ の最大公約多項式を $h(T)$ とすると

$$(f(T), g(T)) = (h(T))$$

が成立する。

**証明 3**　上述の定理により、ある $n(T) \in K[T]$ が存在し

$$(f(T), g(T)) = (n(T))$$

である。ここで、$f(T), g(T) \in (f(T), g(T))$ なので $f(T), g(T) \in (n(T))$ である。よって $n(T) \mid f(T)$ かつ $n(T) \mid g(T)$ であり、$n(T)$ は $f(T), g(T)$ の公約多項式となる。したがって $n(T) \mid h(T)$ である。

次に、$n(T) \in (f(T), g(T))$ であるため、$n(T) = f(T)x_0(T) + g(T)y_0(T)$ となる $x_0(T), y_0(T) \in K[T]$ が存在する。したがって $h(T) \mid n(T)$ である。

以上より $n(T) \mid h(T)$ かつ $h(T) \mid n(T)$ であるから、ある $q(T), p(T) \in K[T]$ によって

$$h(T) = p(T)n(T)\ n(T) = q(T)h(T)$$

と表される。この式から $n(T)$ を消去すると $h(T) = p(T)q(T)h(T)$ となり、$h(T) \neq 0$ であるため

$$p(T)q(T) = 1$$

となる。したがって $p(T) = q(T) = \pm 1$ となり、$n(T) = h(T), n(T) = -h(T)$ となる。また、$(h(T)) = (-h(T))$ であるため $(f(T), g(T)) = (h(T))$ が示された。

### 1.2.2　不定方程式

さて $(f(T), g(T)) = (h(T))$ であるため、多項式環 $K[T]$ 上の $x(T), y(T) \in K[T]$ を不定元とする不定方程式

$$x(T)f(T) + y(T)g(T) = z(T)$$

は $z(T)$ を $f(T)$ と $g(T)$ の最大公約多項式によって割り切ることできるときに解が存在する。また $x(T) = x\_0(T), y(T) = y\_0(T)$ を一つの解とすると

$$(x_0(T) + m(T)g(T))f(T) + (y_0(T) - m(T)f(T))g(T) = z(T)$$

は任意の $m(T) \in K[T]$ に対して成立する。

したがって、ある不定方程式

$$x(T)f(T) + y(T)g(T) = z(T)$$

の解を一つ得ることができれば他の解も得ることができる。