

## 巡回符号

$\mathcal{C}$  : 巡回符号

$$\iff \sigma = (1\ 2\ \cdots\ n) \in \text{Aut}(\mathcal{C})$$

$$\iff$$

$$((c_0, c_1, \dots, c_{n-1}) \in \mathcal{C} \Rightarrow (c_{n-1}, c_0, \dots, c_{n-2}) \in \mathcal{C})$$

$$\sigma = (1 \ 2 \ \cdots \ n) \in \mathfrak{S}_n, \sigma^n = 1$$

$$\mathbf{F}_q[\langle \sigma \rangle] \simeq \mathbf{F}_q[X]/(X^n - 1) =: R \curvearrowright V = \mathbf{F}_q^n$$

により、 $V$  : 階数  $1$  の自由  $R$ -加群

$$V = \mathbf{F}_q^n \simeq R$$

$$(1, 0, \dots, 0) \rightsquigarrow 1$$

$$(c_0, c_1, \dots, c_{n-1}) \rightsquigarrow c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}$$

$\mathcal{C}$  : 巡回符号  $\iff \mathcal{C}$  : 部分  $R$ -加群

$V \simeq R$  と同一視するとき

$\iff \mathcal{C} : R$  の **ideal**

---

$R$  : 可換環 に対し、

$\mathfrak{a} : R$  の **ideal**  $\iff$

- $\forall a, b \in \mathfrak{a} : a + b \in \mathfrak{a}$
- $\forall a \in \mathfrak{a}, \forall r \in R : ra \in \mathfrak{a}$

$C$  : 巡回符号

$\longleftrightarrow R = \mathbf{F}_q[X]/(X^n - 1)$  の **ideal**  $\mathfrak{a}$

$\longleftrightarrow \mathfrak{a} \supset (X^n - 1)$  なる  $\mathbf{F}_q[X]$  の **ideal**  $\mathfrak{a}$

**( $\mathbf{F}_q[X]$  : PID なので  $\exists f \in R : \mathfrak{a} = (f)$ )**

$\longleftrightarrow f | X^n - 1$  なる  $f \in \mathbf{F}_q[X]$

$X^n - 1 \in \mathbf{F}_q[X]$  の分解が判れば、  
巡回符号が分類・構成できる !!

$X^n - 1 = g(X)h(X) \in \mathbf{F}_q[X]$  のとき、

$$\begin{aligned} C &:= gR : \text{巡回符号} \simeq \mathbf{F}_q[X]/(h) \\ &= \{c(X) \in R \mid h(X)c(X) = 0 \text{ in } R\} \end{aligned}$$

$g$  : 生成元多項式 (generator polynomial)

$h$  : 検査多項式 (check polynomial)

$X^n - 1 \in \mathbf{F}_q[X]$  の分解はどうなるのか？

→ 有限体の拡大・Galois 理論

# 代数学からの準備

## 中国式剰余定理 (孫氏の定理)

$m, n$  : 互いに素のとき

$$\mathbf{Z}/mn\mathbf{Z} \simeq \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$$

$$x \bmod mn \iff (x \bmod m, x \bmod n)$$

$$bn \bmod mn \iff (1 \bmod m, 0 \bmod n)$$

$$am \bmod mn \iff (0 \bmod m, 1 \bmod n)$$

ここに、 $a, b$  は  $am + bn = 1$  を満たす整数  
(Euclid の互除法)



## 有限体

$\mathbf{Z}/m\mathbf{Z}$  : 体 (0 以外の元が全て可逆)

$\iff m = p$  : 素数

$\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$  :  $p$  元体

$F(X) \in \mathbf{F}_p[X]$  : 既約  $\implies \mathbf{F}_p[X]/(F)$  : 体

$\deg F = f$  のとき、 $\#(\mathbf{F}_p[X]/(F)) = p^f =: q$

$\mathbf{F}_q^\times = \langle g \rangle$  ( $\exists g \in \mathbf{F}_q^\times$ ) : 位数  $q - 1$  の巡回群

## Frobenius 自己同型・有限体の Galois 群

$q = p^f$ ,  $a, b \in \mathbf{F}_q$  のとき、

$$(a + b)^p = a^p + b^p$$

$$(ab)^p = a^p b^p$$

$\varphi : \mathbf{F}_q \longrightarrow \mathbf{F}_q$  : 体自己同型

$$x \longmapsto x^p$$

$$\varphi(x) = x \iff x \in \mathbf{F}_p$$

$$\text{Gal}(\mathbf{F}_q/\mathbf{F}_p) = \langle \varphi \rangle, \quad \varphi^f = 1$$

$q = 2, n = l$  : 奇素数のとき、

$$X^3 - 1 = (X + 1)(X^2 + X + 1)$$

$$X^5 - 1 = (X + 1)(X^4 + X^3 + X^2 + X + 1)$$

$$X^7 - 1 = (X + 1)(X^3 + X + 1)(X^3 + X^2 + 1)$$

$$X^{11} - 1 = (X + 1)(X^{10} + X^9 + \cdots + X + 1)$$

$$X^{13} - 1 = (X + 1)(X^{12} + X^{11} + \cdots + X + 1)$$

$$X^{17} - 1 = (X + 1)(X^8 + X^5 + X^4 + X^3 + 1) \\ (X^8 + X^7 + X^6 + X^4 + X^2 + X + 1)$$

$$X^{19} - 1 = (X + 1)(X^{18} + X^{17} + \cdots + X + 1)$$

$$\begin{aligned}
 X^{23} - 1 &= (X + 1) \\
 &\quad (X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1) \\
 &\quad (X^{11} + X^{10} + X^6 + X^5 + X^4 + X^2 + 1)
 \end{aligned}$$

$$X^{29} - 1 = (X + 1)(X^{28} + X^{27} + \cdots + X + 1)$$

$$\begin{aligned}
 X^{31} - 1 &= (X + 1)(X^5 + X^2 + 1)(X^5 + X^3 + 1) \\
 &\quad (X^5 + X^3 + X^2 + X + 1) \\
 &\quad (X^5 + X^4 + X^2 + X + 1) \\
 &\quad (X^5 + X^4 + X^3 + X + 1) \\
 &\quad (X^5 + X^4 + X^3 + X^2 + 1)
 \end{aligned}$$

$$X^{37} - 1 = (X + 1)(X^{36} + X^{35} + \cdots + X + 1)$$

$q = 2, n = l$  : 奇素数のとき、

$2 : \text{mod } l$  で平方剰余  $\iff l \equiv \pm 1 \pmod{8}$   
(平方剰余の第 2 補充法則)

この時は、 $\langle 2 \text{ mod } l \rangle \subset F_l^{\times 2}$

$Q := F_l^{\times 2}$  : 平方剰余全体

$N := F_l^{\times} \setminus F_l^{\times 2} = uF_l^{\times 2}$  : 平方非剰余全体  
( $u$  : 平方非剰余の 1 つ)

$Q, N$ : 共に **Galois** 不変

$$f_Q(X) := \prod_{a \in Q} (X - \zeta_l^a)$$

$$f_N(X) := \prod_{a \in N} (X - \zeta_l^a)$$

とすると、

$$f_Q(X), f_N(X) \in \mathbf{F}_2[X]$$

で、

$$X^l - 1 = (X - 1)f_Q(X)f_N(X)$$

と分解する

$$X^l - 1 = (X - 1)f_Q(X)f_N(X)$$

これから構成される符号  $\longrightarrow$  **平方剰余符号**  
(quadratic residue code, QR code)

実際にはこの因数分解を求めるのが面倒  
 $\longrightarrow$  冪等生成元 (idempotent generator)  
を用いると便利

$$X^l - 1 = (X - 1)f_Q(X)f_N(X)$$

これから構成される符号  $\longrightarrow$  平方剰余符号  
(quadratic residue code, QR code)

実際にはこの因数分解を求めるのが面倒  
 $\longrightarrow$  冪等生成元 (idempotent generator)  
を用いると便利