

## 抽象代数学

$$\Lambda(A) = \left\{ 1 + a_1 T + a_2 T^2 + a_3 T^3 + \dots \right\} \\ a_1, a_2, a_3, \dots \in A$$

$$(f)_w + (g)_w = (fg)_w$$

$$(1 - aT)_w \cdot (g)_w = (g(aT))_w$$

$$\begin{aligned} ((1 - aT)(1 - bT))_w (g)_w &= ((1 - aT)_w + (1 - bT)_w) \cdot (g)_w \\ &= (1 - aT)_w (g)_w + (1 - bT)_w (g)_w \end{aligned}$$

$$= (g(aT))_w + (g(bT))_w$$

$$= (g(a \cdot b \cdot T))_w$$

$(f)_w (g)_w$  : 求めたい。  
因数分解

$$(a(T))_w (b(T))_w = \left( \prod_{j=1}^d b(1 - \alpha_j T) \right)_w$$

$$a(T) = (1 - \alpha_1 T) \cdots (1 - \alpha_d T)$$

$$= \left( b(1 - \alpha_1 T) \cdots b(1 - \alpha_d T) \right)_w = \left( 1 + w_1 T + w_2 T^2 + \cdots \right)$$

$$b(T) = 1 + b_1 T + b_2 T^2 + b_3 T^3 + \cdots$$

9:50 ~

$$\frac{1}{x} \text{ in } \mathbb{Z}/p^e\mathbb{Z} \quad \mathbb{Z}/p$$

$$[x] \text{ mod } p^e$$

$(x, p^e) = 1$  GCD. 互除法

$$ax + p^e b = 1$$

$$[x][ax] = 1$$

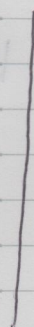
$x$  の逆元

$$xy \sim 1$$

$$xy = 1 + c \quad c \text{ is d.}$$

$$x^{-1} = y^{-1} (1+c)^{-1} = 1 - c + c^2 - c^3 + \dots$$

$$x_n \mapsto \frac{x_n + \frac{2}{x_n}}{2} \approx x_{n+1}$$



$$(1 - aT)_w$$

$$(1 + aT + bT^2)_w = (1 + aT)_w + (1 + bT^2)_w + (1 + Ta\zeta + T^2a^2\zeta^2)_w$$

$$\left( (1 + aT)(1 + bT^2) \right)_w$$

$$1 + aT + bT^2 + a\zeta T^3$$

$$(1 - \alpha)^d_w = d(-1)_w$$

$$(1 - aT^n)_w$$

$$= \left( \prod_{k=0}^{n-2} (1 - \alpha \zeta^k) \right)_w = \sum_k (1 - \alpha \zeta^k)_w$$

$\alpha$ :  $a$  の  $n$  重根.

$\zeta$ : 1 の原始  $n$  重根.