

# Mathematical Toolkit Assignment

Yota Toyama

October 19, 2016

1. (a)

$$\dim(A) = \text{rank}(A) + \text{null}(A) \quad (1)$$

$$n = m + \text{null}(A) \quad (2)$$

$$\text{null}(A) = n - m \quad (3)$$

(b)

$$\text{null}(A) = \dim(\ker(A)) \quad (4)$$

Then,  $\ker(A)$  can have a basis  $B$  s.t.  $\text{Span}(B) = \ker(A)$ . i.e.

$$\forall \mathbf{v} \in \ker(A), \exists a_1, \dots, a_{n-m} \in \mathbb{F}_2, \quad (5)$$

$$\mathbf{v} = a_1 \mathbf{b}_1 + \dots + a_{n-m} \mathbf{b}_{n-m} (b_i \in B) \quad (6)$$

$\therefore$  The answer is  $2^{n-m}$ .

(c)

$$\forall \mathbf{x} \text{ s.t. } \begin{cases} A\mathbf{x} = \mathbf{b} \\ A\mathbf{x}_0 = \mathbf{b} \end{cases} \quad (7)$$

$$\therefore A(\mathbf{x} - \mathbf{x}_0) = 0 \quad (8)$$

$$\mathbf{x} - \mathbf{x}_0 \in \ker(A) \quad (9)$$

Then, choosing each element of  $\mathbf{x}$  carefully (1 or 0),  $\mathbf{x} - \mathbf{x}_0$  can be any element of  $\mathbb{F}_2^n$ .

$$\therefore \{\mathbf{x} - \mathbf{x}_0 | A\mathbf{x} = \mathbf{b}\} = \ker(A) \quad (10)$$

$\therefore \mathbf{x} - \mathbf{x}_0$  has  $2^{n-m}$  solutions.

$\therefore \mathbf{x}$  has  $2^{n-m}$  solutions.

2. (a)

$$f(c\mathbf{v} + (-c)\mathbf{v}) \geq \min\{f(\mathbf{v}), f(\mathbf{v})\} \quad (11)$$

$$\therefore f(\mathbf{0}_V) \geq f(\mathbf{v}) \quad (12)$$

(b) Because every element  $\mathbf{v}_t \in V_t$  is in  $V$  by definition.

$$V_t \subseteq V \quad (13)$$

3.

$$p(x) = x^2 + bx + c \quad (14)$$

$$= (x - r_1)(x - r_2) \quad (15)$$

$$= x^2 - (r_1 + r_2)x + r_1r_2 \quad (16)$$

$$(17)$$

$$\therefore b = -r_1 - r_2, c = r_1r_2 \quad (18)$$

$$(19)$$

4.

$$\mu(P, Q) = \text{degree}(PQ) \quad (20)$$

$$= \text{degree}(QP) \quad (21)$$

$$= \mu(Q, P) \quad (22)$$

$$\mu(0, 0) = \text{degree}(0) \quad (23)$$

$$= 0 \quad (24)$$

$$\forall P \neq 0, \quad (25)$$

$$\mu(P, P) = \text{degree}(P^2) \quad (26)$$

$$= 2\text{degree}(P) \quad (27)$$

$$> 0 \quad (28)$$

$$\mu(P + Q, R) = \text{degree}((P + Q)R) \quad (29)$$

$$= \max\{\text{degree}(P), \text{degree}(Q)\} + \text{degree}(R) \quad (30)$$

$$\mu(P, R) + \mu(Q, R) = \max\{\text{degree}(P) + \text{degree}(R), \text{degree}(Q) + \text{degree}(R)\} \quad (31)$$

$$= \max\{\text{degree}(P), \text{degree}(Q)\} + \text{degree}(R) \quad (32)$$

$$\therefore \mu(P + Q, R) = \mu(P, R) + \mu(Q, R) \quad (33)$$

$$c \in \mathbb{R}, \quad (34)$$

$$\mu(cP, R) = \text{degree}(cPR) \quad (35)$$

$$= \text{degree}(PR) \quad (36)$$

$$\neq c\text{degree}(P, R) \quad (37)$$

$\therefore \mu(\cdot, R)$  is not a LT.

$\therefore \mu$  is not a IP.

5.

$$\alpha\beta\mathbf{x} = \lambda\mathbf{x} \quad (38)$$

$$\beta\alpha\beta\mathbf{x} = \beta(\lambda\mathbf{x}) \quad (39)$$

$$\beta\alpha(\beta\mathbf{x}) = \lambda(\beta\mathbf{x}) \quad (40)$$

$$(41)$$

$\therefore \lambda$  is an eigenvalue of  $\beta\alpha$ .

6. (a)

$$\varphi(\mathbf{v}) = \lambda\mathbf{v} \quad (42)$$

$$\varphi(\mathbf{v}) = \lambda\varphi(\mathbf{v}) \quad (43)$$

$$(\lambda - 1)\varphi(\mathbf{v}) = 0 \quad (44)$$

$$\lambda = 1_{\mathbb{F}} \vee \varphi(\mathbf{v}) = 0 \quad (45)$$

$$\lambda = 1_{\mathbb{F}} \vee \varphi(\mathbf{v}) = 0_{\mathbb{F}}\mathbf{v} \quad (46)$$

$$\therefore \lambda \in \{0_{\mathbb{F}}, 1_{\mathbb{F}}\} \quad (47)$$

(b) Let  $\forall \mathbf{v}, \varphi(\mathbf{v}) = \mathbf{v}_0$ . ( $\mathbf{v}_0$  is fixed.)

Then assume  $\varphi = \varphi^*$ .

If  $\mathbf{v} \neq \mathbf{w} \in V$ ,

$$\langle \mathbf{v}_0, \mathbf{w} \rangle = \langle \mathbf{v}, \varphi^*(\mathbf{w}) \rangle \quad (48)$$

$$\langle \mathbf{v}_0, \mathbf{w} \rangle = \langle \mathbf{v}, \mathbf{v}_0 \rangle \quad (49)$$

$$\langle \mathbf{w}, \mathbf{v}_0 \rangle = \langle \mathbf{v}, \mathbf{v}_0 \rangle \quad (50)$$

$$\mathbf{v} = \mathbf{w} \quad (51)$$

This is contradiction.

$\therefore$  not always  $\varphi = \varphi^*$ .

7. (a)

$$\langle \varphi(\mathbf{v}), \mathbf{w} \rangle = \langle \mathbf{v}, \varphi^*(\mathbf{w}) \rangle \quad (52)$$

$$\langle \varphi^*(\mathbf{w}), \mathbf{v} \rangle = \langle \mathbf{w}, \varphi(\mathbf{v}) \rangle \quad (53)$$

$$\therefore (\varphi^*)^* = \varphi \quad (54)$$