Mathematical Toolkit Assignment 1

Yota Toyama

October 19, 2016

1. (a)

$$\begin{aligned} \dim(A) &= \mathrm{rank}(A) + \mathrm{null}(A) \\ n &= m + \mathrm{null}(A) \\ \mathrm{null}(A) &= n - m \end{aligned}$$

(b)

$$\mathrm{null}(A) = \dim(\ker(A))$$

Then, $\ker(A)$ can have a basis B.

i.e. $\forall \mathbf{v} \in \ker(A), \exists a_1, ..., a_{n-m} \in \mathbb{F}_2, \mathbf{v} = a_1\mathbf{b}_1 + \cdots + a_{n-m}\mathbf{b}_{n-m}$ ($\mathbf{b}_i \in B$)

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

(c)

$$\begin{aligned} \forall \mathbf{x} \text{ s.t. } A\mathbf{x} = \mathbf{b}, A(\mathbf{x} - \mathbf{x}_0) = 0 \because A\mathbf{x}_0 = \mathbf{b} \\ \therefore \ \mathbf{x} - \mathbf{x}_0 \in \ker(A) \end{aligned}$$

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

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

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

2. (a)

$$\begin{aligned} \forall \mathbf{v}, f(c\mathbf{v} + (-c)\mathbf{v}) &\geq \min\{f(\mathbf{v}), f(\mathbf{v})\} \\ f(\mathbf{0}_V) &\geq f(\mathbf{v}) \end{aligned}$$

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

$$V_t \subseteq V$$

3.

$$\begin{aligned}
p(x) &= x^2 + bx + c \\
&= (x - r_1)(x - r_2) \\
&= x^2 - (r_1 + r_2)x + r_1 r_2 \\
\therefore\ b &= -r_1 - r_2, c = r_1 r_2
\end{aligned}$$

I'm lost.

4.

$$\begin{aligned}
\mu(P, Q) &= \text{degree}(PQ) \\
&= \text{degree}(QP) \\
&= \mu(Q, P) \\
\mu(0, 0) &= \text{degree}(0) \\
&= 0 \\
\forall P \neq 0, \mu(P, P) &= \text{degree}(P^2) \\
&= 2\text{degree}(P) \\
&> 0 \\
\mu(P + Q, R) &= \text{degree}((P + Q)R) \\
&= \max\{\text{degree}(P), \text{degree}(Q)\} + \text{degree}(R) \\
\mu(P, R) + \mu(Q, R) &= \max\{\text{degree}(P) + \text{degree}(R), \text{degree}(Q) + \text{degree}(R)\} \\
&= \max\{\text{degree}(P), \text{degree}(Q)\} + \text{degree}(R) \\
\therefore\ \mu(P + Q, R) &= \mu(P, R) + \mu(P, Q) \\
c \in \mathbb{R}, \mu(cP, R) &= \text{degree}(cPR) \\
&= \text{degree}(PR) \\
&\neq c \cdot \text{degree}(P, R)
\end{aligned}$$

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

5.

$$\begin{aligned}
\alpha\beta\mathbf{x} &= \lambda\mathbf{x} \\
\beta\alpha\beta\mathbf{x} &= \beta(\lambda\mathbf{x}) \\
\beta\alpha(\beta\mathbf{x}) &= \lambda(\beta\mathbf{x})
\end{aligned}$$

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

6. (a)

$$\begin{gathered}
\varphi(\mathbf{v}) = \lambda\mathbf{v} \\
\varphi(\mathbf{v}) = \lambda\varphi(\mathbf{v}) \\
(\lambda - 1)\varphi(\mathbf{v}) = 0 \\
\lambda = 1_{\mathbb{F}} \vee \varphi(\mathbf{v}) = 0 \\
\lambda = 1_{\mathbb{F}} \vee \varphi(\mathbf{v}) = 0_{\mathbb{F}}\mathbf{v} \\
\therefore\ \lambda \in \{0_{\mathbb{F}}, 1_{\mathbb{F}}\}
\end{gathered}$$

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

$$\begin{gathered}
\forall \mathbf{v}, \mathbf{w} \in V \text{ s.t. } \mathbf{v} \neq \mathbf{w}, \\
\langle \varphi(\mathbf{v}), \mathbf{w} \rangle = \langle \mathbf{v}, \varphi^*(\mathbf{w}) \rangle \\
\langle \mathbf{v}_0, \mathbf{w} \rangle = \langle \mathbf{v}, \mathbf{v}_0 \rangle \\
\langle \mathbf{w}, \mathbf{v}_0 \rangle = \langle \mathbf{v}, \mathbf{v}_0 \rangle \\
\mathbf{v} = \mathbf{w} \ \lightning
\end{gathered}$$

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

7. (a)

$$\begin{gathered}
\langle \varphi(\mathbf{v}), \mathbf{w} \rangle = \langle \mathbf{v}, \varphi^*(\mathbf{w}) \rangle \\
\langle \varphi^*(\mathbf{w}), \mathbf{v} \rangle = \langle \mathbf{w}, \varphi(\mathbf{v}) \rangle \\
\therefore\ (\varphi^*)^* = \varphi
\end{gathered}$$

(b)

$$\begin{aligned}
\forall \mathbf{v} \in \ker(\varphi), \varphi(\mathbf{v}) &= 0 \\
\langle \varphi(\mathbf{v}), \mathbf{w} \rangle &= 0 \\
\langle \mathbf{v}, \varphi^*(\mathbf{w}) \rangle &= 0 \\
\mathbf{v} &\in (\operatorname{im}(\varphi^*))^{\perp} \\
\forall \mathbf{v} \in (\operatorname{im}(\varphi^*))^{\perp}, \forall \mathbf{w} \in W, \langle \mathbf{v}, \varphi^*(\mathbf{w}) \rangle &= 0 \\
\langle \varphi(\mathbf{v}), \mathbf{w} \rangle &= 0 \\
\varphi(\mathbf{v}) &= 0 \\
\mathbf{v} &\in \ker(\varphi) \\
\therefore\ \ker(\varphi) &= (\operatorname{im}(\varphi^*))^{\perp}
\end{aligned}$$

(c)

$$\begin{aligned}\forall \mathbf{w} \in \mathrm{im}(\varphi), \exists \mathbf{v} \in V \text{ s.t. } \mathbf{w} = \varphi(\mathbf{v}), \forall \mathbf{w'} \in \ker(\varphi^*), \langle \mathbf{w}, \mathbf{w'} \rangle &= \langle \varphi(\mathbf{v}), \mathbf{w'} \rangle \\ &= \langle \mathbf{v}, \varphi^*(\mathbf{w'}) \rangle \\ &= 0 \\ \mathbf{w} &\in (\ker(\varphi^*))^{\perp}\end{aligned}$$

$$\begin{aligned}\forall \mathbf{v} \in V, \forall \mathbf{w} \in \ker(\varphi^*), \varphi^*(\mathbf{w}) &= 0 \\ \langle \mathbf{v}, \varphi^*(\mathbf{w}) \rangle &= 0 \\ \therefore \ \mathrm{im}(\varphi) = (\ker(\varphi^*))^{\perp}\end{aligned}$$

(d)

$$\begin{aligned}\mathrm{rank}(\varphi) &= \dim(\mathrm{im}(\varphi)) \\ &= \dim((\ker(\varphi^*))^{\perp}) \\ &= \dim(W) - \dim(\ker(()\varphi^*)) \\ &= \dim(im(\varphi^*)) \\ &= \mathrm{rank}(\varphi^*)\end{aligned}$$

(e)

$$\begin{aligned}\text{Let } \ A = BC, B \in \mathbb{C}^{m \times r}, C \in \mathbb{C}^{r \times n} \\ \text{then } \ A_{i,:} = \sum_{j=1}^{r} B_{i,j} C_{i,:} \\ A_{:,i} = \sum_{j=1}^{r} C_{j,i} B_{:,i}\end{aligned}$$

$$\therefore \ \begin{cases} rank_{row}(A) \le rank_{row}(C) \le r \\ rank_{column}(A) \le rank_{column}(B) \le r \end{cases}$$

Choose a minimal r.
Then rows of C form a minimal spanning set of rows of A.
And, columns of C form a minimal spanning set of columns of A.
$\therefore r$ is the rank of both row and column spaces of A.

$$\therefore \ rank_{row}(A) = rank_{column}(A)$$