CMI ALGEBRA 1 (2021) ASSIGNMENT 1
- T. R. Ramadas

Soham Chatterjee

Roll: BMC202175

1. Let $P : V \to V$ be a map such that

$$P = \frac{1}{2}(I_V - i\mathcal{J})$$

Now if $v_1, v_2 \in V$ then

$$P(v_1 + v_2) = \frac{1}{2}((v_1 + v + 2) - i\mathcal{J}(v_1 + v_2)) = \frac{1}{2}(v_1 - i\mathcal{J}(v_1)) + \frac{1}{2}(v_2 - i\mathcal{J}(v_2)) = P(v_1) + P(v_2)$$

and

$$P(\lambda \cdot v_1) = \frac{1}{2}(\lambda \cdot v_1 - i\mathcal{J}(\lambda \cdot v_1)) = \frac{1}{2}(\lambda \cdot v_1 - i\lambda \cdot \mathcal{J}(v_1)) = \lambda \cdot \frac{1}{2}(v_1 - i\mathcal{J}(v_1)) = \lambda \cdot P(v_1)$$

Hence P is a linear map. Now

$$\begin{aligned}
P(P(v)) &= P\left(\frac{1}{2}(v - i\mathcal{J}(v))\right) \\
&= \frac{1}{2}\left(\frac{1}{2}(v - i\mathcal{J}(v)) - iJ\left(\frac{1}{2}(v - i\mathcal{J}(v))\right)\right) \\
&= \frac{1}{2}\left(\frac{1}{2}(v - i\mathcal{J}(v)) - \left(\frac{1}{2}(i\mathcal{J}(v) + \mathcal{J}(\mathcal{J}(v)))\right)\right) \\
&= \frac{1}{2}\left(\frac{1}{2}(v - i\mathcal{J}(v)) - \left(\frac{1}{2}(i\mathcal{J}(v) - v)\right)\right) \\
&= \frac{1}{2}(v - i\mathcal{J}(v)) \\
&= P(v)
\end{aligned}$$

Hence for a vector $v \in image(P)$, $P(v) = v$

Now, if $v \in V_{-i}$ then

$$\begin{aligned}
&\mathcal{J}(v) = -iv \\
\implies &i\mathcal{J}(v) = v \\
\implies &v - i\mathcal{J}(v) = 0_V \\
\implies &\frac{1}{2}(v - i\mathcal{J}(v)) = 0_V \\
\implies &P(v) = 0_V
\end{aligned}$$

Hence if $v \in V_{-i}$ then $v \in ker(P)$ therefore

$$V_{-i} \subseteq ker(P)$$

Now let $v \in ker(P)$ then

$$\begin{aligned}
&P(v) = 0_V \\
\implies &\frac{1}{2}(v - i\mathcal{J}(v)) = 0_V \\
\implies &v - i\mathcal{J}(v) = 0_V \\
\implies &v = i\mathcal{J}(v) \\
\implies &iv = -\mathcal{J}(v) \\
\implies &\mathcal{J}(v) = -iv
\end{aligned}$$

Hence if $v \in ker(P)$ then $v \in V_{-i}$ therefore

$$ker(P) \subseteq V_{-i}$$

Hence

$$V_{-i} = ker(P)$$

Now if $v \in V_i$ then

$$\mathcal{J}(v) = iv$$

$$\begin{aligned} P(v) &= \frac{1}{2}(v - i\mathcal{J}(v)) \\ &= \frac{1}{2}(v - i(iv)) \\ &= \frac{1}{2}(v + v) \\ &= v \end{aligned}$$

Hence if $v \in V_i$ then $v \in image(P)$ therefore

$$V_i \subseteq image(P)$$

Now let $v \in image(P)$ then $\exists\ u \in V$ such that $P(u) = v = \frac{1}{2}(u - i\mathcal{J}(u))$. Therefore

$$\begin{aligned} \mathcal{J}(v) &= \mathcal{J}(P(u)) \\ &= \mathcal{J}\left(\frac{1}{2}(u - i\mathcal{J}(u))\right) \\ &= \frac{1}{2}(\mathcal{J}(u) - \mathcal{J}(i\mathcal{J}(u))) \\ &= \frac{1}{2}(\mathcal{J}(u)) - i\mathcal{J}(\mathcal{J}(u)) \\ &= \frac{1}{2}(\mathcal{J}(u)) + iu) \\ &= i\frac{1}{2}(-i\mathcal{J}(u) + u) \\ &= iP(u) = iv \end{aligned}$$

Hence if $v \in image(P)$ then $v \in V_i$ therefore

$$image(P) \subseteq V_i$$

Hence

$$V_i = image(P)$$

Hence we need to prove that

$$V = ker(P) \oplus image(P)$$

Let $v \in V$. we can write $v = v - P(v) + P(v)$. Then

$$P(v) = P(v - P(v) + p(v)) = P(vP(v)) + P(P(v))$$

Here

$$\begin{aligned} P(v - P(v)) &= P(v) - P(P(v)) \\ &= P(v) - P(v) \\ &= 0_V \end{aligned}$$

Hence $v - P(v) \in ker(P)$ and $P(v) \in image(P)$. Hence any vector $v \in V$ it can be written as a sum of a vector from $ker(P)$ and a vector from $image(P)$. Hence

$$V \subseteq ker(P) \oplus image(P)$$

Now let $v \in ker(P) \oplus image(P)$. Then $\exists v_1 \in ker(P)$ and $v_2 \in image(P)$ such that

$$v = v_1 + v_2$$

As $v_1 \in ker(P)$, $v_1 \in V$. As the linear map P is $V \to V$, $image(P) \subseteq V$. Hence $v_2 \in V$ also. Therefore $v_1 + v_2 \in V$. Therefore

$$ker(P) \oplus image(P) \subseteq V$$

. Hence $V = ker(P) \oplus image(P) = V_i \oplus V_{-i}$ [Proved]

2. (a) The sets that span (=generate) $\mathbb{R}^3$ are $\underline{\mathcal{S}_2}, \underline{\mathcal{S}_3}, \underline{\mathcal{S}_4}$.
   (b) The linearly independent sets are $\underline{\mathcal{S}_1}, \underline{\mathcal{S}_2}$.
   (c) The bases are $\underline{\mathcal{S}_2}$.
3. The set $\{(1,0,0),(x,y,0),(x',y',z')\}$ is a basis of $\mathbb{R}^3$ iff $\underline{y \neq 0, z' \neq 0}$
4. V is a one dimensional vector space. Therefor any non zero vector of V is a basis of V.

- We are considering the characteristic 0 fields.

Let $f \in \mathbb{F}[x_1, x_2, \ldots, x_{n-1}, y]$ be an n-variate degree d polynomial which can be computed by an arithmetic circuit of size at most s. If g and h are polynomials of degree at least 1 such that $f = gh$ and $gcd(g,h) = 1$, then g and h have a circuit of size at most $poly(s,n,d)$. Let $f \in \mathbb{F}[x_1, x_2, \ldots, x_{n-1}, y]$ be an n-variate degree d polynomial which can be computed by an arithmetic circuit of size at most s. If there is a polynomial g and an integer e such that $f = g^e$, then g has a circuit of size at most $poly(s,n,d)$.