

Def. Given F -vector spaces U and V , let $\mathcal{L}(U, V)$ denote the set of all linear maps from U to V .

Prop. $\mathcal{L}(U, V)$ is an F -vector space. More precisely:

(a) given $I, \sigma \in \mathcal{L}(U, V)$, the sum

$$\begin{aligned} I + \sigma : U &\longrightarrow V \\ x &\longmapsto I(x) + \sigma(x) \end{aligned}$$

is in $\mathcal{L}(U, V)$.

(b) given $I \in \mathcal{L}(U, V)$ and $\lambda \in F$, the product

$$\begin{aligned} \lambda I : U &\longrightarrow V \\ x &\longmapsto \lambda \cdot I(x) \end{aligned}$$

is in $\mathcal{L}(U, V)$.

(c) $\mathcal{L}(U, V)$ is an F -vector space w.r.t. these operations.

Proof. Let $x, y \in U$ and let $\alpha, \beta \in F$. Then we have:

$$\begin{aligned} (\text{(a)}) \quad (I + \sigma)(\alpha x + \beta y) &= I(\alpha x + \beta y) + \sigma(\alpha x + \beta y) \\ &= \alpha I(x) + \beta I(y) + \alpha \sigma(x) + \beta \sigma(y) \\ &= \alpha(I(x) + \sigma(x)) + \beta(I(y) + \sigma(y)) \\ &= \alpha((I + \sigma)(x)) + \beta((I + \sigma)(y)). \end{aligned}$$

Hence $I + \sigma$ is a linear map.

$$\begin{aligned}
 (\text{b}) \quad (\lambda I)(\alpha x + \beta y) &= \lambda (I(\alpha x + \beta y)) \\
 &= \lambda (\alpha I(x) + \beta I(y)) \\
 &= \alpha \cdot \lambda \cdot I(x) + \beta \cdot \lambda \cdot I(y) \\
 &= \alpha \cdot (\lambda I)(x) + \beta \cdot (\lambda I)(y)
 \end{aligned}$$

Hence λI is a linear map.

(c) Addition in $L(U, V)$ is clearly commutative and the zero map $0: U \rightarrow V$, $u \mapsto 0_V$ clearly satisfies $0 + I = I = I + 0$ $\forall I \in L(U, V)$.

Let $I, \sigma, \rho \in L(U, V)$ and $x \in U$. Then

$$\begin{aligned}
 [(I + \sigma) + \rho](x) &= (I + \sigma)(x) + \rho(x) \\
 &= (I(x) + \sigma(x)) + \rho(x) \\
 &= I(x) + (\sigma(x) + \rho(x)) \\
 &= I(x) + (\sigma + \rho)(x) \\
 &= [I + (\sigma + \rho)](x)
 \end{aligned}$$

Since this equality holds for all $x \in U$, it shows that

$$(I + \sigma) + \rho = I + (\sigma + \rho).$$

Since this is true for all $I, \sigma, \rho \in L(U, V)$, this establishes the associativity of "+" in $L(U, V)$.

$$\begin{aligned}
 \text{Now } [\mathcal{I} + (-1)\mathcal{I}] (x) &= \mathcal{I}(x) + [(-1)\mathcal{I}](x) \\
 &= \mathcal{I}(x) + (-1)\mathcal{I}(x) \\
 &= 0 \\
 &= \dots = [(-1)\mathcal{I} + \mathcal{I}] (x)
 \end{aligned}$$

Hence $\mathcal{I} + (-1)\mathcal{I} = 0 = (-1)\mathcal{I} + \mathcal{I}$, so inverses exist in $\mathcal{L}(U, V)$.

Thus, $\mathcal{L}(U, V)$ is an abelian group under $+$.

Let $\mathcal{I}, \sigma \in \mathcal{L}(U, V)$ and let $\lambda \in F$. Then, for all $x \in U$,

$$\begin{aligned}
 [\lambda(\mathcal{I} + \sigma)](x) &= \lambda[(\mathcal{I} + \sigma)(x)] \\
 &= \lambda[\mathcal{I}(x) + \sigma(x)] \\
 &= \lambda \cdot \mathcal{I}(x) + \lambda \cdot \sigma(x) \\
 &= (\lambda\mathcal{I})(x) + (\lambda\sigma)(x) \\
 &= [\lambda\mathcal{I} + \lambda\sigma](x),
 \end{aligned}$$

$$\text{so } \lambda(\mathcal{I} + \sigma) = \lambda\mathcal{I} + \lambda\sigma.$$

Similarly, one can check (exercise)

- $(\lambda + \mu)\mathcal{I} = \lambda\mathcal{I} + \mu\mathcal{I} \quad \forall \lambda, \mu \in F, \forall \mathcal{I} \in \mathcal{L}(U, V)$
- $(\lambda\mu)\mathcal{I} = \lambda(\mu\mathcal{I}) \quad \forall \lambda, \mu \in F, \forall \mathcal{I} \in \mathcal{L}(U, V)$
- $1_F \mathcal{I} = \mathcal{I} \quad \forall \mathcal{I} \in \mathcal{L}(U, V).$

□

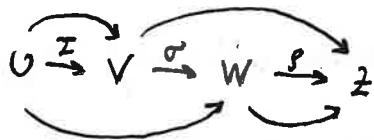
Prop. Let U, V, W, Z be \mathbb{F} -vector spaces.

(a) If $\tau \in \mathcal{L}(U, V)$ and $\sigma \in \mathcal{L}(V, W)$, then the composition
 $\sigma\tau = \sigma \circ \tau : U \rightarrow W$ (defined as $(\sigma\tau)(x) = \sigma(\tau(x)) \quad \forall x \in U$)
is in $\mathcal{L}(U, W)$.

(b) If $\tau_1, \tau_2 \in \mathcal{L}(U, V)$ and $\sigma \in \mathcal{L}(V, W)$, then
 $\sigma(\tau_1 + \tau_2) = \sigma\tau_1 + \sigma\tau_2$.

(c) If $\tau \in \mathcal{L}(U, V)$, and $\sigma_1, \sigma_2 \in \mathcal{L}(V, W)$, then
 $(\sigma_1 + \sigma_2)\tau = \sigma_1\tau + \sigma_2\tau$.

(d) If $\tau \in \mathcal{L}(U, V)$, $\sigma \in \mathcal{L}(V, W)$ and $\rho \in \mathcal{L}(W, Z)$, then
 $\rho(\sigma\tau) = (\rho\sigma)\tau$.



Proof:

(a) Let $x, y \in U$ and $\alpha, \beta \in \mathbb{F}$. Then

$$\begin{aligned} (\sigma\tau)(\alpha x + \beta y) &= \sigma(\tau(\alpha x + \beta y)) \\ &= \sigma(\alpha\tau(x) + \beta\tau(y)) \\ &= \alpha\sigma(\tau(x)) + \beta\sigma(\tau(y)) \\ &= \alpha(\sigma\tau)(x) + \beta(\sigma\tau)(y), \end{aligned}$$

so $\sigma\tau \in \mathcal{L}(U, W)$.

(b) Let $x \in U$. Then

$$\begin{aligned}
 [\sigma(\tau_1 + \tau_2)](x) &= \sigma((\tau_1 + \tau_2)(x)) \\
 &= \sigma(\tau_1(x) + \tau_2(x)) \\
 &= \sigma(\tau_1(x)) + \sigma(\tau_2(x)) \\
 &= (\sigma\tau_1)(x) + (\sigma\tau_2)(x) \\
 &= (\sigma\tau_1 + \sigma\tau_2)(x).
 \end{aligned}$$

Hence, $\sigma(\tau_1 + \tau_2) = \sigma\tau_1 + \sigma\tau_2$.

(c) Similar to (b).

(c) Follows by associativity of functions. □

Def. A ring is an abelian group R (written additively) together with a binary operation $\cdot : R \times R \rightarrow R$ satisfying the following:

$$(i) \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z \quad \forall x, y, z \in R$$

$$\begin{array}{l}
 (ii) \quad x \cdot (y + z) = x \cdot y + x \cdot z \\
 \quad \quad \quad (y + z) \cdot x = y \cdot x + z \cdot x
 \end{array} \quad \left. \right\} \quad \forall x, y, z \in R$$

(iii) there exists an element $1_R \in R$ such that

$$1_R \cdot x = x = x \cdot 1_R \quad \forall x \in R.$$

Examples

- 1) \mathbb{Z} is a ring under standard addition and multiplication.
- 2) For any positive integer n , $\mathbb{Z}/n\mathbb{Z}$ is a ring under addition and multiplication modulo n .
- 3) Any field is a ring.
- 4) The set of $n \times n$ matrices with coefficients in any ring is again a ring under matrix addition and multiplication.
- 5) By the previous proposition, if U is any F -vector space then $\mathcal{L}(U, U)$ is a ring under addition and composition of functions. Note that the multiplicative identity is the identity map $I_U \in \mathcal{L}(U, U)$.

We call $\mathcal{L}(U, U)$ the ring of endomorphisms of U , and we denote it by $\text{End}(U)$. An element $\mathcal{I} \in \mathcal{L}(U, U)$ is called an endomorphism of U .