

**Lemma**

Let  $R$  be a ring. Let  $V$  be a free  $R$ -module with a basis  $v_1, \dots, v_d$ . If  $M$  is an  $R$ -module and  $x_1, \dots, x_d \in M$  (just random elements, not necessarily distinct or basis), then there exists a unique  $R$ -module homomorphism  $T : V \rightarrow M$  with  $T(v_i) = x_i$ .

*Proof.* We first show existence. Define

$$T\left(\sum_{i=1}^d r_i v_i\right) := \sum_{i=1}^d r_i x_i.$$

Since the  $v_i$ 's form a basis, this representation is well-defined for arbitrary inputs. It is immediate that this transformation is linear and satisfies  $T(v_i) = x_i$ .

Now for uniqueness, suppose  $T_1, T_2$  both satisfy the requirements. It follows that  $(T_2 - T_1)(v_i) = 0$  for all  $i$  (note  $T_2 - T_1$  is an  $R$ -module homomorphism). By linearity  $T_2 - T_1 \equiv 0$ , completing the proof of uniqueness.  $\square$

Let  $R$  be a commutative ring and  $S, T$  be linear transformations from  $M$  to  $N$ . Then it follows that  $S + T$  and  $rT$  for  $r \in R$  are also well-defined linear transformations. That is,  $\text{Hom}_R(M, N) := \{T : M \rightarrow N : T \text{ is a } R\text{-module homomorphism}\}$  is another module / vector space.

In particular, if  $\dim(M) = m$  and  $\dim(N) = n$ , then  $\dim \text{Hom}_R(M, N) = mn$ . (Think matrices!)



Let  $F$  be a field and  $V_1, V_2$  vector spaces over  $F$ . Let  $T_i : V_i \rightarrow W_i$  be linear transformations. Then  $T \equiv T_1 \otimes T_2 : V_1 \otimes V_2 \rightarrow W_1 \otimes W_2$  defined by

$$(T_1 \otimes T_2)(v_1 \otimes v_2) := T_1 v_1 \otimes T_2 v_2$$

is a well-defined linear transformation.

**Lemma**

Let  $F$  be a field and  $V, W$  finite-dimensional vector fields over  $F$ . Let  $T : V \rightarrow W$  be a linear transformation. Then there exists a basis  $v_1, \dots, v_d$  of  $V$  and a basis  $w_1, \dots, w_e$  of  $W$  such that  $T(v_i) = w_i$  for  $i \leq m$  and  $T(v_i) = 0$  for  $i > m$  for some  $m$ . We say  $m$  is the **rank** of  $T$ , or equivalently  $\dim T(V)$ .

*Proof.* We first choose a basis  $v_{m+1}, \dots, v_d$  for  $\ker(T)$ . We extend it to a basis for  $V$  by adding  $v_1, \dots, v_m$ . Let  $w_i = T(v_i)$  for  $i \leq m$ . We claim  $w_1, \dots, w_m$  are linearly independent. Suppose  $\sum_{i=1}^m a_i w_i = 0$ . That is,  $\sum_{i=1}^m a_i T(v_i) = T\left(\sum_{i=1}^m a_i v_i\right) = 0$ . That is, the linear combination  $\sum_{i=1}^m a_i v_i \in \ker(T)$  but  $v_1, \dots, v_m \notin \ker(T)$ . That means it must be 0, and consequently  $a_i = 0$ , and we are done.  $\square$

**Corollary**

Suppose  $S, T : V \rightarrow W$  are linear transformations. Then there exist isomorphisms  $\varphi : V \rightarrow V$  and  $\gamma : W \rightarrow W$  with  $T = \gamma S \varphi$  if and only if  $\text{rank}(T) = \text{rank}(S)$ .

The collection of all linear transformations from  $V \rightarrow V$  where  $V$  is a vector space over field  $F$  will be denoted as either  $\mathcal{L}(V)$ ,  $\mathcal{L}(V, V)$ ,  $\text{Hom}_F(V, V)$ , or  $\text{End}_F(V)$  (**endomorphisms**). We have  $\dim \text{End}_F(V) = \dim(V)^2$ .

Finally, we define the set of all invertible endomorphisms on  $V$  to be the **general linear group** (it is a group)

$$\text{GL}(V) := \{T \in \text{End}_F(V) : T \text{ invertible}\} = \{T \in \text{End}_F(V) : T \text{ bijective}\}$$

with  $\text{id} : V \rightarrow V$  being the identity.

### Lemma

If  $\dim V = n < \infty$  and  $T \in \text{End}_F(V)$  (or if  $T : V \rightarrow W$  with  $\dim W = \dim V$ ), then TFAE:

- (1)  $T$  is invertible,
- (2)  $T$  is injective,
- (3)  $T$  is onto, and
- (4)  $\text{rank}(T) = n$ .

Note that the claim fails if  $\dim V = \infty$ . Consider  $V = \mathbb{R}[x]$ . Let  $T : V \rightarrow V$  be defined by  $Tf(x) := f'(x)$ . Every polynomial has a polynomial antiderivative so  $T$  is onto, but clearly it is not injective.

## 0.1 Matrices

Let  $R$  be a ring and  $M_{m \times n}(R)$  denote the set of  $m \times n$  matrices over  $R$ . Addition and scalar multiplication as defined normally and they form an Abelian group and an  $R$ -module. Matrix multiplication is also defined the standard way. As usual, matrix multiplication is distributive, associative, but not commutative. That is,  $M_{n \times n}(R) = M_n(R)$  is a ring. The set of invertible matrices form a group, namely  $\text{GL}_n(R)$ .