Linear Algebra

枫聆

2021 年 2 月 20 日

目录

Vector Space

Definition of Vector Space

Definition 1.1. vector spaces 是一个具有加法 (addition) 和数量乘法 (salar multiplication) 的集合 V

- 加法是指对任意的元素 $u, v \in V$, 有 $u + v \in V$
- 数量乘法是指对任意的元素 $\lambda \in F$ 和 $v \in V$，有 $\lambda v \in V$

  同时它们存在下面的属性:

- 加法交换律 $\forall u, v \in V, u + v = v + u$
- 加法结合律 $\forall u, v, w \in V, (u + v) + w = u + (v + w)$ 和 $\forall a, b \in F, (ab)v = a(bv)$
- 加法单位元 $\forall v \in V, v + 0 = v$
- 加法逆元 $\forall v \in V, \exists v^{-1}, v + v^{-1} = 0$
- 数量乘法的单位元 $\forall v \in V, 1v = v$
- 分配律 $\forall v, w \in V, \forall a, b \in F, a(u + v) = au + av, (a + b)v = av + bv$

vector spaces 背后的直觉是什么？《linear algebra done right》上说来自于 F^n 上的 addition 和 scalar multiplication. 很明显 addition 包含了 abelian group 的所有性质，vector space 是 R-module 的特殊化，R-module 从结构上来说，要比 Ring(带单位元) 的性质要弱一些，主要体现在乘法上，弱化为数量乘法，表示把一个环作用在一个 abelian group 上，而不是环上的乘法. 这样做的好处是可以让可以把环上一些看起来不那么好性质都变得好一点，例如 ideal 在一般情况下并不一定还是一个环. 不那么好是相对于群的一些性质来说的，例如正规子群. 在定义了 module 之后，你会发现 ideal 就是一个 module，我们的操作终于都在一个东西下面了，不会轻易的跑出去.

我想这里多记录一些 R-module 的东西，如何把一个环弱化成一个模结构呢？首先我们需要一个 abelian group M，定义 "the left-action of a ring R on M" 为

$$\sigma\colon R \to \mathsf{End}_{Ab}(M)$$

是一个环同态. 可能这里有一个小疑问为什么 $\mathsf{End}_{Ab}(M)$ 是一个环结构？首先这个环里面的元素都是关于 M 的 endomorphisms, 乘法定义为 endomorphisms 之间的复合，加法定义为 $(f + g)(a) = f(a) + g(a)$，其中 $f, g \in \mathsf{End}_{Ab}(M)$. 我们说 σ 把 M 变成了一个 left-R-module，σ 这个映射可以理解为 left-R-module structure(算子)，

$$\sigma(r)(m) \in_R M$$

间接的定义了数量乘法，并且有一些有趣的性质:

- 分配律 $\sigma(r)(m_1+m_2)=\sigma(r)(m_1)+\sigma(r)(m_2)$
- 分配律 $\sigma(r_1+r_2)(m)=\sigma(r_1)(m)+\sigma(r_2)(m)$ (环同态下可以保证)
- 结合性 $\sigma(r_1r_2)(m)=\sigma(r_1)(\sigma(r_2)(m))$ (环同态下可以保证)
- 单位元 $\sigma(1)(m)=m$

如果要定义更清楚一点，可以这样

$$\rho\colon R\times M\to M$$

,ρ 和 σ 的关系为

$$\rho(r,m)=\sigma(r)(m)$$

, 但是这里不是环同态无法保证上面的一些性质，所以需要额外规定一些东西

- $\rho(r_1+r_2,m)=\rho(r_1,m)+\rho(r_2,m)$（分配律）
- $\rho(r,m_1+m_2)=\rho(r,m_1)+\rho(r,m_2)$（分配律）
- $\rho(r_1r_2,m)=\rho(r_1,\rho(r_2,m))$（结合率）
- $\rho(1,m)=m$ （单位元）

把 vector space 一般化的感觉是不是很爽？其实 R-module 在一定程度要比 vector space 更复杂，当用更抽象方式去理解 vector space，我们定义了一个 σ 环同态，这个环同态很精妙的把环作用在 abelian group 的 action 表示出来，所以我们用理解 R-module 的方式去理解 vector space，就是首先我们要有一个 abelian group 定义了加法，然后把一个 field 作用在了它之上，定义为数量乘法，最后我们就得到了这样的一个结构。

这篇 note 既然是在《linear algebra done right》的基础上记录的，我会尽可能的记录一些抽象的延伸的东西，让自己对 linear algebra 有一个不同于大学的颠覆性的认知。

Subspace

Definition 1.2. *如果 V 中的子集 U 是一个子空间，当且仅当满足以下条件:*

1. $0 \in U$
2. $u, w \in U$ 蕴含 $u + w \in U$
3. $a \in F$,$u \in U$ 蕴含 $au \in U$

也就是说，V 下子空间一定是子集，包含加法单位元，且在加法和数量乘法下封闭。

Definition 1.3. *定义 $U_1, \cdots, U_m$ 是 V 的子集. 这些子集的和表示为*

$$U_1 + \cdots + U_m = \{ u_1 + \cdots + u_m \mid u_1 \in U_1, \cdots, u_m \in U_m \}$$

定义子集和，是为了引入下面这个性质

Proposition 1.4. *定义 $U_1, \cdots, U_m$ 都是 V 中的子空间，则 $U_1 + \cdots + U_m$ 是包含 $U_1, \cdots, U_m$ 的最小子空间.*

证明. 最小的就是指 V 里面任意包含 $U_1, \cdots, U_m$ 的子空间都包含 $U_1 + \cdots + U_m$, 首先得证明一下 $U_1 + \cdots + U_m$ 是一个子空间，按照子空间的定义，加法单位元和封闭性都很显然，满足上述条件的子空间很也显然需要包含所有子空间对应的子集和。 □

Definition 1.5. *定义 $U_1, \cdots, U_m$ 都是 V 中的子空间，如果 $U_1 + \cdots + U_m$ 中的每个元素都有唯一分解形式即 $u_1, \cdots, u_m$，则 $U_1 + \cdots + U_m$ 是直和 (direct sum)，用 $U_1 \oplus \cdots \oplus U_m$ 表示。*

那怎么判定一个子集合是不是直和呢?

Proposition 1.6. *定义 $U_1, \cdots, U_m$ 都是 V 中的子空间, 如果 $U_1 + \cdots + U_m$ 是直和当且仅当 $u_1 + \cdots + u_m = 0$ 时，$u_1 = ... = u_m = 0$。*

即只需要 0 有唯一的表示形式就够了，来证明一下

证明. 假设

$$u_1 + \cdots + u_m = u_1' + \cdots + u_m'$$

, 整理一下

$$(u_1 - u_1') + \cdots + (u_m - u_m') = 0$$

,0 有唯一的表示方式，则 $u_1 = u_1', \ldots, u_m = u_m'(u_1 - u_1' \in U_1, \ldots, u_m - u_m' \in U_m)$ □

下面再来个特殊情况, 只有两个子空间，怎么判定它们的子集和是不是直和?

Proposition 1.7. 定义 U 和 W 是 V 中的两个子空间，如果 $U+W$ 是直和当且仅当 $U \cap W = 0$.

证明. 如果 $U+W$ 是直和，任取 $v \in U \cap W$, 则 $-v \in U \cap W$, 而 $0 = v + (-v)$, 所以 v 只能是 0.

如果 $U \cap W = \{0\}$, 我们假设还有 $0 = v + w$，其中 v, w 不为 0，则 $w = (-v)$, 则 $v \in U \cap W$，与前提矛盾. 所以 0 有唯一表示。 □

Finite-Dimensional Vector Space

Linear Combinations and Span

Definition 2.1. 给定 V 里面一系列向量 $v_1, v_2, \cdots, v_m$(vector list)，它们的线性组合表示为

$$a_1v_1 + a_2v_2 + \cdots + a_mv_m,$$

其中 $a_1, a_2, \cdots, a_m \in F$.

Definition 2.2. 给定 V 里面一系列向量 $v_1, v_2, \cdots, v_m$，所有的它们的线性组合构成的集合叫一个 **span**(linear span).

$$\text{span}(v_1, v_2, \cdots, v_m) = \{\, a_1v_1 + a_2v_2 + \cdots + a_mv_m \mid a_1, a_2, \cdots, a_m \in F \,\}.$$

空的 vector list 的 span 表示为 $\{0\}$.

下面是关于 span 一些有趣的性质.

Proposition 2.3. span 是包含当前 vector list 里面所有 vectors 的 smallest subspace.

证明. 首先你得证明 span 确实是一个 subspace，然后所有其他的 subspace 都包含它. span 是一个 subspace 是 clearly 的. 假设 U 这样一个 subspace，包含 $v_1, v_2, \cdots, v_m$. 则 $a_1v_1, a_2v_2, \cdots, a_mv_m$ 也是属于 U 的. 那么它们的和也应该是属于 U 的. 这就证明了 span 是含于 U 的. □

上面 span 是一个名词，那么下面 span 就是一个动词.

Definition 2.4. 如果 $\text{span}(v_1, v_2, \cdots, v_m)$ 等于 V，则称 $v_1, v_2, \cdots, v_m$ **spans** V

finite-dimensional vector space 的严格定义.

Definition 2.5. 如果一个 vector space 可以被一些 vector list spans, 则称这个 vector sapce 是 finite-dimensional.

这里没有用到 basis 的概念...

Definition 2.6. $\mathcal{P}(F)$ 用来表示 polynomials over F(所有系数属于 F 的多项式集合).

Linear Independence

Definition 2.7. 给定 V 上一个 vector list $v_1, v_2, \cdots, v_m$. 若要使得 $a_1v_1 + a_2v_2 + \cdots + a_mv_m = 0$，只能唯一取 $a_1 = a_2 = \cdots = a_m$. 则称 $v_1, v_2, \cdots, v_m$ **linearly independent**. 从另一方面说就是在 $\text{span}(v_1, v_2, \cdots, v_m)$ 里面的所有 vector 都有唯一表示形式.

empty vector list 同样被定义为 linearly independent.

下面是关于 linearly dependent 的一个小性质.

Lemma 2.8. 给定 V 上一组 linearly dependent 的 vector list $v_1, v_2, \cdots, v_m$. 则存在一个 $j \in \{1, 2, \cdots, m\}$ 使得下面两个命题成立.

1. $v_j \in \text{span}(v_1, v_2, \cdots, v_{j-1})$;
2. 如果 j^{th} vector 从 $v_1, v_2, \cdots, v_m$ 中被去掉，则剩下的 vectors 构成的 span 依然等于 $\text{span}(v_1, v_2, \cdots, v_m)$.

这个 lemma 本质就是在 linearly dependent vector list 里面可以挑一个 vector 出来，它可以被其他的 vectors 表示.

证明. 因为 $v_1, v_2, \cdots, v_m$ linear independent，所以存在某个 $a_k, k \in \{1, \cdots, m\}$ 不等于 0，使得

$$a_1v_1 + a_2v_2 + \cdot + a_mv_m = 0.$$

让 j 表示最大值形如 $a_j \neq 0$. 则我们有

$$v_j = -\frac{a_1}{a_j}v_1 - \frac{a_2}{a_j}v_2 - \cdots - -\frac{a_{j-1}}{a_j}v_{j-1}.$$

□

还有一个比较直观的判定给定 vector list 是不是 linearly independent 的方法.

Proposition 2.9. linearly independent vector list 长度是小于等于 spanning vector list(vector list spans V) 的长度.

证明. 给定 $v_1, v_2, \cdots, v_m$ linearly independent 和 $u_1, u_2, \cdots, u_n$ spans V. 我们的目标是证明 $m \leq n$. 整个证明过程非常的有趣，会用 $v_1, v_2, \cdots, v_m$ 替换部分 $u_1, u_2, \cdots, u_n$.

首先我们考虑 $v_1, u_1, u_2, \cdots u_m$，现在这个 vector list 变成了 linearly dependent，因为 v_1 现在至少可以有两种表示方法了. 使用前面关于 linearly dependent 的 lemma 我们可以去掉某个 u_k，使得剩下的 vector list 还是 spans V. 我们称这个新的 vector list 为 B.

然后 by induction，我们可以把剩下的 $v_2, \cdots, v_m$ 也都加到 B 里面，同时每次 remove 一个 u_k. 我们必须考虑一下有没有足够多的 u_k 够我们 remove? 也就是说我们还剩下一些 v_i 放不进去 B. 假设存在这种情况，也就

是说现在 B 里面全是 v，所以 B 里面的 vectors 都是 linearly independent，并且 spans V，现在还剩下 v_i 还没放进去. 矛盾就来了，v_i 加上 B 里面的 vectors 就变成 linearly dependent 了. 所以是不存在这种情况的. 也就是说 $v_1, v_2, \cdots, v_m$ 是完全可以一一替换部分 $u_1, u_2, \cdots, u_n$ 的. 最后结论就是 $m \leq n$. □

Proposition 2.10. finite-dimensional vector space 的 subspace 还是 finite-dimensional.

证明. 这里还是一个构造证明，用 U 表示 V 上的 subspace. 如果 $U = \{0\}$，clearly. 如果 $U \neq \{0\}$，则我们从里面挑一个非零 vector v_1 出来. 如果 $U = \operatorname{span}(v_1)$，we are done. 反之我们接着取非零 $v_2 \in U$，这里还有有一个条件就是 $v_2 \notin \operatorname{span}(v_1)$.

一般地，如果 $U = \operatorname{span}(v_1, v_2, \cdots, v_{j-1})$，we are done. 反之我们接着取 $v_j \in U$，且 $v_j \notin \operatorname{span}(v_1, v_2, \cdots, v_{j-1})$. 你可以观察到这样取出来的 vector list 都是 linearly independent. 根据前面的 lemma 我们知道它的长度应该是小于任何的 spanning list，V 现在是 finite-dimensional，根据定义它可以被一些 vector list span. 所以最终我们这样的取法是会停下来的，因为长度被限制了，即 U 最终也会被一个 vector lists span，U 也是 finite-dimensional. 其实感觉有点找 basis 的感觉了. □

Bases

Definition 2.11. 若 V 上的一组 list of vectors 是 linearly independent 且 spans V，则称它是 V 上的一个 basis(基).

basis 更常见的另一种描述方式如下

Proposition 2.12. 若 V 上的一组 list $v_1, v_2, \cdots, v_m$ of vectors 是一个 basis 当且仅当任意的 $v \in V$ 都有唯一的表示 (linear combination)

$$v = a_1v_1 + a_2v2 + \cdots + a_mv_m.$$

其中 $a_1, a_2, \cdots, a_m \in F$.

还有一个比较显然的性质，就是任何一个 spanning list 都可以被 reduced 成一个 basis(同样一个 linearly independent vector list 也可以被 extended 成一个 basis). 继而 finite-dimensional vector space 中一定会有一个 basis.

Dimension

Definition 2.13. finite-dimensional vector space V 的 dimension 为 V 上的一个 basis 的长度，用 $\dim V$ 表示.

这个定义从侧面说明 basis 的长度取决于 V，而不取决于它本身.

Proposition 2.14. 给定 finite-dimensional V 上 subspace U. 则 $\dim U \leq \dim V$.

证明. 把 U 上的 basis 看做 V 中一个 linearly independent list. 而 V 上的 basis 看做 V 中一个 spanning list. 前面有 lemma 说明 linearly independent list 长度是小于 spanning list. □

快速根据长度来判断一个 list 是不是 basis 的方法

Proposition 2.15. 给定 finite-dimensional V.

1. linearly independent list with right length.
2. spanning list with right length.

其中 right length 表示 $\dim V$.

Proposition 2.16. 给定 finite-dimensional V 上的 subspace U_1 和 U_2.

$$\dim(U_1 + U_2) = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2).$$

证明. 首先给定 $U_1 \cap U_2$ 的 basis 为 $u_1, u_2, \cdots, u_m$，即 $\dim(U_1 \cap U_2) = m$. 在它的基础上分别 extend 到 U_1 和 U_2 的 basis 上. U_1 的 basis 为 $u_1, u_2, \cdots, u_m, v_1, v_2, \cdots, v_j$，$U_2$ 的 basis 为 $u_1, u_2, \cdots, u_m, w_1, w_2, \cdots, w_k$. 很自然我们希望有下面等式

$$\begin{aligned}\dim(U_1 \cap U_2) &= m + j + k \\ &= (m + j) + (m + k) - m \\ &= \dim U_1 + \dim U_2 + \dim(U_1 \cap U_2).\end{aligned}$$

这个等式成立的关键是要证明 $u_1, u_2, \cdots, u_m, v_1, v_2, \cdots, v_j, w_1, w_2, \cdots, w_k$ 是 $U_1 + U_2$ 的一个 basis. 即 proof

$$a_1 u_1 + a_2 u_2 + \cdots + a_m u_m + b_1 v_1 + b_2 v_2 + \cdots + b_j v_j + c_1 w_1 + c_2 w_2 + \cdots + c_k w_k = 0.$$

接下来就是把 w 移到一边，证明 $c_1 = c_2 = \cdots = c_m = 0$(remove v)，接着证明 a 和 c 都等于 0(linearly independent). □

Linear Maps

Definition 3.1. 给定两个 vector space V 和 W，若存在一个映射 $T\colon V\to W$ 使得

1. additivity(可加性): $\forall u,v\in V, T(u+v)=Tu+Tv$.
2. homogeneity(齐次性): $\forall v\in V, T(\lambda v)=\lambda(Tv)$.

则称这个映射是一个 linear maps(linear transformation)(线性映射). 也就说这个映射保留了加法运算和数量乘法.

Definition 3.2. V 和 W 之间所有 linear map 构成的集合记为 $\mathcal{L}(V,W)$.

Example 3.3. 有几种特殊的 linear map.

1. zero map: $0\in\mathcal{L}(V,W)$ 定义
$$0v=0$$
(0 在这里表示特殊 T 下同).
2. identity map: $I\in\mathcal{L}(V,W)$ 定义为
$$Iv=v.$$
3. differentiation map: $D\in\mathcal{L}(\mathcal{P}(R),\mathcal{P}(\mathbb{R}))$ 定义为
$$Dp=p'.$$
这里可以想一下导数的运算法则.
4. integration map: $T\in\mathcal{L}(\mathcal{P}(R),\mathbb{R})$ 定义为
$$Tp=\int_0^1 p(x)dx.$$
5. from F^n to F^m(m,n 都是正整数): 定义 $A_{j,k}\in F, j=1,\cdots,m, k=1,\cdots,n$，然后使得 $T\in\mathcal{L}(F^n,F^m)$
$$T(x_1,\cdots,x_n)=(A_{1,1}x_1+\cdots+A_{1,n}x_n, A_{m,1}x_1+\cdots+A_{m,n}x_n).$$

basis 在经过 linear map 的作用会变得如何呢?

Proposition 3.4. 给定 V 上一个 basis $v_1,v_2,\cdots,v_n$ 和 W 上一个 basis $w_1,w_2,\cdots,w_n$. 则存在一个唯一的 linear map $T\colon V\to W$ 使得
$$Tv_j=w_j, j=1,\cdots,n.$$

证明. 现在给定这样的 linear map T，我们要证明要它是唯一的，就是要说它对任意 $v \in V$ 都有一一对应的 $w \in W$. 让 $v = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n$，那么

$$\begin{aligned} T(a_1 v_1 + a_2 v_2 + \cdots + a_n v_n) &= T(a_1 v_1) + T(a_2 v_2) + \cdots + T(a_n v_n) \\ &= a_1 T(v_1) + a_2 T(v_2) + \cdots + a_n T(v_n) \\ &= a_1 w_1 + a_2 w_2 + \cdots + a_n w_n. \end{aligned}$$

Q.E.D. □

Algebraic Operations On $\mathcal{L}(V, W)$

Definition 3.5. 给定两个 linear map $S, T \in \mathcal{L}(V, W)$ 和 $\lambda \in F$. 其加法和数量乘法定义如下.

1. sum $S+T$: $(S+T)(v) = Sv + Tv$.
2. scalar product λT: $\lambda T(v) = \lambda(Tv)$.

其中 $v \in V$.

整个 $\mathcal{L}(V, W)$ 代数结构是一个 vector space, 这是一个比较重要的结论. 当然了你可能还需要验证一下其他的 axioms，例如乘法结合性，乘法单位元，分配律等等.

Definition 3.6. $\mathcal{L}(V, W)$ is a vector space

再引入一个 vector space U，讨论两个 linear maps 的 product 变得有意义了.

Definition 3.7. 给定 $T \in \mathcal{L}(U, V)$ 和 $S \in \mathcal{L}(V, W)$，则存在 product $ST \in \mathcal{L}(U, W)$ 使得

$$(ST)(u) = S(T(u)).$$

其中 $u \in U$.

Null Spaces and Ranges

Definition 3.8. 给定 linear map $T \in \mathcal{L}(V, W)$. 集合 $\{ v \in V \mid Tv = 0 \}$ 表示 **null space** of T，记为 null T.

null space 就是 0 的 preimage 收集起来.

Proposition 3.9. The null space is subspace.

证明. 我们要证明它在加法和数量乘法下封闭，并且 0 在里面. 对任意的 $u, v \in \text{null } T$，有

$$T(u+v) = T(u) + T(v) = 0,$$

所以 $u + v \in \text{null } T$. 同理 $T(\lambda u) = \lambda T(u), T(0) = T(0) + T(0) = 0$. □

现在我们可以用 null space 来说明 linear map 一些性质.

Proposition 3.10. 给定 linear map $T \in \mathcal{L}(V, W)$. T 是 injective 当且仅当 null $T = \{0\}$.

证明. 如果 T 是 injective，clearly null $T = \{0\}$. 如果 null $T = \{0\}$，假设 T 不是 injective，则存在 $a \neq b \in F$，使得 $T(a) = T(b)$. 我们可以稍微变换一下 $T(a-b) = T(a) - T(b)$，矛盾就来了，$(a-b) \in \text{null } T$，这是和前提矛盾的. □

Definition 3.11. 给定映射 $T\colon V \to W$. 集合 $\{ Tv \mid v \in V \}$ 表示 **range** of T，记为 range T.

Proposition 3.12. 若 $T \in \mathcal{L}(V, W)$，则 range T 是一个 subspace.

Foudamental Theorem of Linear Maps

Theorem 3.13. 给定 finite-dimensional V 和 linear map $T \in \mathcal{L}(V, W)$. 则 range T 也是 finite-dimensional 且有下面等式成立.

$$\dim V = \dim \operatorname{null} T + \dim \operatorname{range} T.$$

证明. 在前面我们知道 null T 是一个 subspace，假设它的 basis 为 $u_1, u_2, \cdots, u_m$. 我们可以把这个 basis extend 到 V 的 basis，即 $u_1, u_2, \cdots, u_m, v_1, v_2, \cdots, v_n$. 很显然我们想要证明 $\dim \operatorname{range} T = n$. 给定任意的 $v \in V$，那么

$$\begin{aligned} T(a_1u_1 + a_2u_2 + \cdots + a_mu_m + b_1v_1 + b_2v_2 + \cdots + b_nv_n) &= T(a_1u_1 + a_2u_2 + \cdots + a_mu_m) + T(b_1v_1 + b_2v_2 + \cdots + b_nv_n) \\ &= 0 + T(b_1v_1 + b_2v_2 + \cdots + b_nv_n) \\ &= b_1Tv_1 + b_2Tv_2 + \cdots + b_nTv_n. \end{aligned}$$

我们可以知道 $Tv_1, Tv_2, \cdots, Tv_n$ spans range T，所以 range T 是 finite-dimensional 的. 但是我们还要证明它们是 range T 的一个 basis，即它们还要 linearly independent. 要证明 $c_1Tv_1 + c_2Tv_2 + \cdots + c_nTv_n = 0$，那么

$$T(c_1v_1 + c_2v_2 + \cdots + c_nv_n) = 0.$$

由于 $v_1, v_2, \cdots, v_n$ 是 linearly independent , 且 $c_1Tv_1 + c_2Tv_2 + \cdots + c_nTv_n \notin \operatorname{null} T$. 所以 $c_1 = c_2 = \cdots = c_n = 0$. $\square$

这个 theorem 说明了一个重要的性质就是不存在一个 injective linear map 使得一个 finite-dimensional vector space 到一个更低维的 vector space. 反之 map to 一个更高维的 vector space 不会是一个满射.

Homogeneous system of linear equations

Proposition 3.14. 齐次线性方程组未知数的个数大于等式的个数，则有非零解.

证明. 首先得知道什么齐次线性方程组.

$$\sum_{k=1}^{n} A_{1,k}x_k = 0$$

$$\vdots$$

$$\sum_{k=1}^{n} A_{m,k}x_k = 0.$$

显然 $x_1 = x_2 = \cdots = x_n = 0$ 是这组方程组的解. 这是 trivial 的，我们要考虑的是有没有非零解的情况. 之前我们定义过一个 linear map $T: F^n \to F^m$.

$$T(x_1, \cdots, x_n) = (\sum_{k=1}^{n} A_{1,k}x_k, \cdots, \sum_{k=1}^{n} A_{m,k}x_k).$$

上面方程组可以用 $T(x_1, \cdots, x_n) = 0$ 来简洁的表示，注意这里的 0 是 F^m 中的加法单位元. 我们想要非零解，在这里只要保证 T 不是单射就行，即只要 null T 不是 $\{0\}$. 由 linear map 基本定理推出性质，injective 的一个充分条件是只要 $n > m$ 就行. 这就是当前命题的最本质的刻画. □

对于非齐次方程组也有类似的结论，但是有一些不一样.

Proposition 3.15. 对于非齐次方程组

$$\sum_{k=1}^{n} A_{1,k}x_k = c_1$$

$$\vdots$$

$$\sum_{k=1}^{n} A_{m,k}x_k = c_m.$$

当方程组的个数大于未知数的个数时，可以找到一些 $c_1, \cdots, c_m$ 使得方程误解.

证明. 这里就变成了 $T(x_1, \cdots, x_n) = (c_1, \cdots, c_m)$. 要使得它没有解，我们可以让 range T 只是 F^m 一个 subspace，即 T 不是一个 surjective. 所以 $n < m$ 就可以有一个充分条件来满足这一点. □

Matrices

Definition 3.16. 一个经典的 $m \times n$ matrix.

$$\begin{pmatrix} A_{1,1} & \cdots & A_{1,n} \\ \vdots & & \vdots \\ A_{m,1} & \cdots & A_{m,n} \end{pmatrix}$$

Definition 3.17. 给定一个 linear map $T \in \mathcal{L}(V,W)$，V 上的一个 basis $v_1,\cdots,v_n$ 和 W 上的一个 basis $w_1,\cdots,w_m$. 用 $\mathcal{M}(T)$ 表示 $m \times n$ matrix of T. 其中 $A_{j,k}$ 定义为

$$Tv_k = A_{1,k}w_1 + \cdots + A_{m,k}w_m.$$

这个定义的直觉是什么呢? 当给定一个 linear map $T\colon V \to W$ 和 V 上一个 basis $v_1,\cdots,v_n$. 那么 $Tv_1,\cdots,Tv_n$ 是 range T 的一个 basis，所以它们 spans range T. 这里的想法就是把 $Tv_1,\cdots,Tv_n$ 和 W 上的 basis 联系起来了.

matrix 的加法和数量乘法定义. 直觉来源于下面两个命题.

Proposition 3.18. 给定两个 linear map $S,T \in \mathcal{L}(V,W)$，$\lambda \in F$.

1. $\mathcal{M}(S+T) = \mathcal{M}(S) + \mathcal{M}(T)$.

2. $\mathcal{M}(\lambda T) = \lambda \mathcal{M}(T)$.

在思考上面的命题时候，我们脑子里面必须有了一些 fixed base，例如 V 上一个 basis $v_1,\cdots,v_n$，和 W 上一个 basis $w_1,\cdots,w_m$. $S+T$ 还是一个 $\mathcal{L}(V,W)$ 中的 linear map，所以 $w_1,\cdots,w_m$ 也是它的一个 basis. 例如

$$\begin{aligned}(S+T)v_k &= Sv_k + Tv_k \\ &= \sum_{r=1}^{m} A_{r,k}w_r + \sum_{r=1}^{m} C_{r,k}w_r \\ &= \sum_{r=1}^{m}(A_{r,k}+C_{r,k})w_r.\end{aligned}$$

矩阵的乘法需要单独拿出来讲一下，在这里我们需要再额外定义 U 和它的一个 basis $u_1,\cdots,u_p$. 给定两个 linear maps $T\colon U \to V$ 和 $S\colon V \to W$，它们的复合 ST 也是一个 linear map. 那么现在有一个问题是 $\mathcal{M}(ST)$ 是否等于 $\mathcal{M}(S)\mathcal{M}(S)$?

但是在此之前，我们并没有定义矩阵乘法. 如果我们希望上面的问题有一个 positive answer，定义 $\mathcal{M}(S) = A$

和 $\mathcal{M}(T) = C$，取 $1 \le k \le p$，那么

$$
\begin{aligned}
(ST)u_k &= S(\sum_{r=1}^{n} C_{r,k} v_r) \\
&= \sum_{r=1}^{n} C_{r,k} \sum_{j=1}^{m} A_{j,r} w_j \\
&= \sum_{j=1}^{m} (\sum_{r=1}^{n} A_{j,r} C_{r,k}) w_j.
\end{aligned}
$$

所以 ST 也是一个 $m \times p$ matrix，这个结果是非常自然的，描述 basis 在 linear map 之间传递. 所以我们由此给出一个正式的矩阵乘法的定义.

Definition 3.19. 给定 $m \times n$ matrix A 和 $n \times p$ matrix C. 则 $m \times p$ product matrix AC 的第 j 行和第 k 列定义为

$$
(AC)_{j,k} = \sum_{r=1}^{n} A_{j,r} C_{r,k}.
$$

可以形象的记忆就是 A 的第 j 行的元素分别乘上 C 的第 k 列的元素.

$$
(AC)_{j,k} = A_{j,\cdot} C_{\cdot,k}
$$

其中 $A_{j,\cdot}$ 表示第 j 行 $1 \times n$ 矩阵，$C_{\cdot,k}$ 表示第 k 列 $n \times 1$ 矩阵. 还是刻画成了两个矩阵的乘法.

Proposition 3.20. 特别地,

$$
(AC)_{\cdot,k} = AC_{\cdot,k}
$$

表示 AC 的第 k 的列等于 A 乘上 C 的第 k 的列 (fixed k).

Proposition 3.21. 给定一个 $m \times n$ matrix A 和 $n \times 1$ matrix $c = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$. 那么

$$
Ac = c_1 A_{\cdot,1} + \cdots + c_n A_{\cdot,n}.
$$

换句话说就是在刻画一个 linear combination.

证明.

$$
\begin{aligned}
Ac &= \begin{pmatrix} \left(\sum\limits_{r=1}^{n} A_{1,r}C_{r,1}\right) \\ \vdots \\ \left(\sum\limits_{r=1}^{n} A_{n,r}C_{r,1}\right) \end{pmatrix} \\
&= \begin{pmatrix} A_{1,1}C_{1,1} \\ \vdots \\ A_{n,1}C_{1,1} \end{pmatrix} + \cdots + \begin{pmatrix} A_{1,n}C_{n,1} \\ \vdots \\ A_{n,n}C_{n,1} \end{pmatrix} \\
&= C_{1,1} \begin{pmatrix} A_{1,1} \\ \vdots \\ A_{n,1} \end{pmatrix} + \cdots + C_{n,1} \begin{pmatrix} A_{1,n} \\ \vdots \\ A_{n,n} \end{pmatrix}
\end{aligned}
$$

□

以上都是从不同的方向去思考矩阵乘法.

Example 3.22. 先给出一个 classic 矩阵乘法.

$$
\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 6 & 5 & 4 & 3 \\ 2 & 1 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 10 & 7 & 4 & 1 \\ 26 & 19 & 12 & 5 \\ 42 & 31 & 20 & 9 \end{pmatrix}
$$

那么其中结果的第 2 列可以表示为

$$
\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 5 \\ 1 \end{pmatrix} = \begin{pmatrix} 7 \\ 19 \\ 31 \end{pmatrix}
$$

还可以用 linear combination 的眼观来看

$$
\begin{pmatrix} 7 \\ 19 \\ 31 \end{pmatrix} = 5 \begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix} + 1 \begin{pmatrix} 2 \\ 4 \\ 6 \end{pmatrix}
$$

Invertibility

Definition 3.23. 给定一个 linear map $T \in \mathcal{L}(V, W)$. 若存在另外一个 linear map $S \in \mathcal{L}(W, V)$，使得 ST 和 TS 都是 identity map. 则称 T 是可逆的 (invertible)，S 是 T 的逆元.

Proposition 3.24. 一个可逆的 linear map 有唯一的逆元.

证明. 给定可逆 linear map $T \in \mathcal{L}(V, W)$. 假设它有两个逆元 S_1 和 S_2，那么

$$S_1 = S_1 I = S_1 T S_2 = I S_2 = S_2.$$

□

自然地，我们需要思考一个 linear map 什么时候可逆?

Proposition 3.25. 一个 linear map 可逆当且仅当它是 injective 和 surjective.

证明. 给定 linear map $T \in \mathcal{L}(V, W)$.

($\Leftarrow$) 若 T 是 injective 和 surjective，则 $T(v) = w$ 一一对应的且能取到所有的 $w \in W$，那么 S 直接把对应的 $T(v)$ 送到 v 即可.

($\Rightarrow$) 若 T 可逆，那么存在 $S \in \mathcal{L}(W, V)$ 使得 $ST = I$ 和 $TS = I$. 从 $TS = I$ 可以知道 T 一个 surjective，注意这里的 I 是 $W \to W$，表示 $T(S(w))$ 可以取到任意的 $w \in W$. 若存在 v_1, v_2 使得 $T(v_1) = T(v_2)$，则 $S(T(v_1)) = S(T(v2))$，由于 $ST = I$，所以 $v_1 = v_2$，即 T 是一个 injective. □

Isomorphic Vector Spaces

Definition 3.26. 若两个 vector spaces 之间一个可逆的 linear map，则称这两个 vector space 是同构的 (isomorphic)，这个可逆的 linear map 称为 isomorphism.

The Greek word **isos** means equal; the Greek word **morph** means shape. Thus isomorphic literally means equal shape.

Proposition 3.27. 两个 finite-dimensional vector spaces over F 同构当且仅当它们有相同的维数 (dimension).

证明. 设两个 vector spaces 分别为 V 和 W.

($\Rightarrow$) 若 V 和 W 同构. 因此 V 和 W 之间有一个 isomorphism. 前面我们知道可逆的 linear map 是 injective 和 surjective 的. 根据 linear map 的基本定理

$$\dim V = \dim \operatorname{null} V + \dim \operatorname{range} V.$$

这里有 null $V = 0$，同时 range $V = W$. 所以 $\dim V = \dim W$.

($\Leftarrow$) 若 V 和 W 拥有相同的 dimension. 分别挑 V 上的 basis $v_1, \cdots, v_n$ 和 W 上的 basis $w_1, \cdots, w_n$. 我们定义一个 linear map T，使得

$$T(c_1 v_1 + \cdots + c_n v_n) = c_1 w_1 + \cdots + c_n v w_n.$$

我们需要说明 T 是 well-defined. $\forall v \in V$，都可以被 $v_1, \cdots, v_n$ 唯一表示，继而对应的 $w \in W$ 也是被 $w_1, \cdots, w_n$ 唯一表示的. 很显然这是一个 linear map. 同时 null $T = \{0\}$，所以 T 是一个 injective. 并且 T 的函数值可以 spans W，所以 T 是一个 surjective. 最后 T 是一个 isomorphism. □

我们来思考一个有趣的 isomophism.

Proposition 3.28. 给定 V 上 basis $v_1, \cdots, c_n$ 和 W 上的 basis $w_1, \cdots, w_m$. 任意一个 $T \in \mathcal{L}(V, W)$，都能确定一个 $\mathcal{M}(T) \in F^{m,n}$. 那么 $\mathcal{L}(V, W)$ 和 $F^{m,n}$ 同构，其中 $\mathcal{M}$ 是 isomorphism.

证明. 前面我们在定义矩阵加法和数量乘法的时候，已经可以表明 $\mathcal{M}$ 是一个 linear map 了. 我们需要证明它是可逆的，即它是 injective 和 surjective.

若 $\mathcal{M}(T) = 0$，这里 matrix 等于 0 表示 $F^{m,n}$ 中的零矩阵. 那么 $Tv_k = 0, k = 1, \cdots, n$，则 T 是一个 zero linear map. 所以 $\mathcal{M}$ 是 injective 的. 对于 $\forall A \in F^{m,n}$

$$Tv_k = \sum_{r=1}^{m} A_{r,k} w_j.$$

显然 $\mathcal{M}(T) = A$. 所以 $\mathcal{M}$ 是 surjective. (这里可以意味着 $A_{j,k}$ 可以取遍所有 F) □

如果能从它们的 dimension 去证明上面的命题就好了，但是 $\mathcal{L}(V, W)$ 的 dimension 并没有那么显然.

Proposition 3.29. 给定 V 和 W 都是 finite-dimensional. 则 $\mathcal{L}(V, W)$ 也是 finite-dimensional，其中

$$\dim \mathcal{L}(V, W) = \dim V \dim W.$$

Linear Maps Thought of as Matrix Multiplication

之前我们定义了 matrix of a linear map，现在我们来定义 matrix of a vector.

Definition 3.30. 给定 V 上的 *basis* $v_1, \cdots, v_n$ 和 $v \in V$. 那么 *matrix of* v 表示为

$$\mathcal{M}(v) = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix},$$

其中 $c_1, \cdots, c_n$ 使得

$$v = c_1 v_1 + \cdots + c_2 v_n.$$

所以这里有一个很自然的式子把它们联系起来.

$$\mathcal{M}(T)_{\cdot,k} = \mathcal{M}(Tv_k).$$

Proposition 3.31. 给定 linear map $T \in \mathcal{L}(V, W)$ 和 $v \in V$. 给定 V 上的 basis $v_1, \cdots, v_,$ 和 W 上的 basis $w_1, \cdots, w_m$. 那么

$$\mathcal{M}(Tv) = \mathcal{M}(T)\mathcal{M}(v).$$

证明. 假定 $v = c_1 v_1 + \cdots + c_n v_n$，其中 $c_1, \cdots, c_n \in F$. 那么

$$Tv = c_1 T v_1 + \cdots c_n T v_n.$$

继而

$$\begin{aligned} \mathcal{M}(Tv) &= c_1 \mathcal{M}(Tv_1) + \cdots + c_n \mathcal{M}(Tv_n) \\ &= c_1 \mathcal{M}(T)_{\cdot,1} + \cdots + c_n \mathcal{M}(T)_{\cdot,n} \\ &= \mathcal{M}(T)\mathcal{M}(v). \end{aligned}$$

注意这里用了很多的变换，第一个变换是矩阵的 scalar multiplication，第二个是前面的式子，第三个矩阵乘法中的特殊的 linear combination. □

这个命题到底有什么用呢？每一个 $m \times n$ matrix 都蕴含了一个 $F^{n,1}$ 到 $F^{m,1}$ 的 linear map.

$$x \in F^{n,1}, Ax \in F^{m,1}.$$

其中 A 和 x 被换成了 $\mathcal{M}(T)$ 和 $\mathcal{M}(v)$，这个换法是个 isomorphism.

Operators

Definition 3.32. 一个 vector sapce V 到自身的 linear map $V \to V$ 被称为 operator，V 上所有的 operators 构成的集合记为 $\mathcal{L}(V)$，即 $\mathcal{L}(V) = \mathcal{L}(V, V)$.

Example 3.33. 两个 *operators* 的例子.

1. *multiplication by* x^2*:* $T \in \mathcal{L}(\mathcal{P}(\mathbb{R}), \mathcal{P}(\mathbb{R}))$

$$(Tp)(x) = x^2 p(x).$$

2. *backward shift:* $T \in \mathcal{L}(F^\infty, F^\infty)$

$$T(x_1, x_2, x_3, \cdots) = (x_2, x_3, \cdots).$$

operator 其实就是 endomorphism，可以把条件加强一点变成 automorphism(自同构). 也就是说需要把 operator 变成一个 isomorphism.

Proposition 3.34. 给定 finite-dimensional V 和 operator $T \in \mathcal{L}(V)$. 下面条件相互等价

1. T is invertible.
2. T is injective.
3. T is surjective.

注意这里必须是finitie-dimensional. 也就是说现在判定 invertible 不需要 injective 和 surjective 同时满足.

证明. 我们再写一遍 foundamental theorem

$$\dim V = \dim \operatorname{null} V + \dim \operatorname{range} V.$$

$(2 \Rightarrow 3)$ 若 T 是 injective，上面的式子就变成了 $dimV = dim\text{range } T$. range T 是 V 的一个 subspace. 若要上述式子成立，则 range $T = V$，所以 T 是一个 surjective.

$(3 \Rightarrow 2)$ 若 T 是 surjective，range $T = V$ 上面的式子就变成了 $0 = \dim \operatorname{null} T$. 所以 T 是一个 injective.

其他方向的推导都比较 clearly. □