1 线性空间, 向量组和秩, 基和维数, 子空间的交, 并, 和, 直和, 线性同构, 商空间

定义 1. 一个非空集合 V, 具有加法运算, 且其元素和数域 K 的元素之间有数量乘法运算, 并且满足下述性质:

1. V 是 Abel 群
2. 数量乘法具有两种分配律
3. $1 \in K$, $1\alpha = \alpha$
4. $k, l \in K$, $(kl)\alpha = k(l\alpha)$

那么称 V 是数域 K 上的线性空间.

推论 1. 1. 成立加法消去律

2. $0\alpha = 0$
3. $k\mathbf{0} = \mathbf{0}$
4. 若 $k\alpha = 0$, 则 $k = 0$ 或 $\alpha = \mathbf{0}$
5. $(-1)\alpha = -\alpha$

通常我们验证某个 V 的子集合是不是线性空间时, 只需要注意加法和数量乘法的封闭性即可, 注意数量乘法的封闭性可以得到存在零元和负元. 也就是说子空间一定过" 原点". 子空间的定义就是字面意思.

我们称 V 中的元素为向量, 关于线性相关等一系列性质可以推广. 这里做以整理.

定义 2. **线性组合**, **向量组**, **线性表出**如前.

设 V 是数域 K 上的线性空间, 称其子集 S 线性无关, 如果

1. S 是空集
2. 若 S 是有限集, 则给这个集合的元素一种编号所得的向量组线性无关
3. 若 S 是无限集, 则 S 的任意子集都线性无关

定义 3. 设 V 是数域 K 上的线性空间, 称其子集 S 如果:

1. 线性无关
2. 任意 V 中的元素可以由 S 中的元素线性表出

则称 S 是线性空间 V 的一个**基**, 只含零向量的线性空间的基是空集.

引理 2 (Zorn)**.** 若一个偏序集的每一条链都有上界, 那么这个集合至少有一个极大元.

注. *记偏序集 R,*

1. *上界: A 是一个链, $\forall \alpha \in A, \alpha \leq \beta$, 称 β 是 A 的一个上界.*
2. *极大元: 称 β 是极大元, 如果不存在 $\alpha \in A$, $\alpha \geq \beta$ 且 $\alpha \neq \beta$, 换言之, 如果 $\alpha \geq \beta$, 则它们相等 (当然它们可能无法比较).*

定理 3. 任意线性空间都有一个基.

证明. V 中所有线性无关的子集组成的集合是一个偏序集, 且任取一个链 $\mathcal{A}$, 定义集合 $S=\bigcup_{A\in\mathcal{A}}A$, 则 S 线性无关 (任取其中的向量组, 从 $\mathcal{A}$ 是链得到存在 $A_i\in S$ 且 S 包含这个向量组, 故它们线性无关), 故 $S\in V$, 这说明 V 中任意的链都有上界, 根据 Zorn 引理, V 中存在极大元 $\mathcal{S}$, 其满足 V 中所有线性无关的子集要么是它的子集, 要么无法比较, 于是它不能被扩充, 任意向量 β, 有 $\{\beta\}\cup\mathcal{S}$ 线性相关, 于是 $\mathcal{S}$ 是 V 的一个基. □

定义 4. 如果一个数域 K 上的线性空间 V 的基是有限集, 称基中元素的个数为线性空间 V 的**维数**, 记作 $\dim V$, 如果 S 是无限基, 称 V 是无限维的.

基作为向量组是等价的, 所以它们的个数相等, 所以线性空间的维数是一定的. 故以上定义是良好的. 接下来按顺序得到一系列命题.

命题 4. 1. n 维线性空间中任意 $n+1$ 个向量一定线性相关

2. 设 V 是数域 K 上的一个线性空间, 设 $\alpha_1,\alpha_2,\cdots,\alpha_n\in V$, 以下叙述等价:
   - $\alpha_1,\alpha_2,\cdots,\alpha_n$ 线性无关
   - $\mathrm{span}(\alpha_1,\alpha_2,\cdots,\alpha_n)=V$
   - $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 V 的一个基.
3. **(基扩张定理)** 设 V 是一个 n 维线性空间, 向量组 $\beta_1,\beta_2,\cdots,\beta_m$ 是 V 中线性无关的 m 个向量, $m<n$, 则 V 的任意一个基 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 中存在 $n-m$ 个向量, 和 $\beta_1,\beta_2,\cdots,\beta_m$ 一起构成 V 的一个基.

证明.

1. 否则维数大于 n
2. 若 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 线性无关, 取 $\beta\in V$, 根据 1, 则向量组 $\beta,\alpha_1,\alpha_2,\cdots,\alpha_n$ 线性相关, 即 β 可以由 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 线性表出. 若任意 β 可以由 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 线性表出, 则 V 的一个基也可以被 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 线性表出, 由基的定义知它们相互线性表出, $\alpha_1,\alpha_2,\cdots,\alpha_n$ 和这个基等价, 故 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 线性无关.
3. 假设任意的 α_i, $\beta_1,\beta_2,\cdots,\beta_m,\alpha_i$ 线性相关, 则基可被 $\beta_1,\beta_2,\cdots,\beta_m$ 线性表出, 则它们等价, 又 $m<n$, 矛盾, 故一定存在 α_i 使得 α_i, $\beta_1,\beta_2,\cdots,\beta_m,\alpha_i$ 线性无关, 归纳地取 α_i 直到取满.

□

由前面的命题, 线性空间 V 中的任意向量由某一基 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 线性表出的表法唯一:

$$\beta=c_1\alpha_1+c_2\alpha_2+\cdots+c_n\alpha_n$$

称这组数为 β 在基 α_i, $\beta_1,\beta_2,\cdots,\beta_m,\alpha_i$ 下的坐标, 称列向量 $(c_1,c_2,\cdots,c_n)^T\in K^n$ 是坐标向量.

基变换和坐标变换

设数域 K 上的线性空间 V, 给出向量的线性表示的方便记法:

$$(\beta_1,\beta_2,\cdots,\beta_m)=(\alpha_1,\alpha_2,\cdots,\alpha_n)A$$

其中 $A\in M_{n\times m}(K)$. 类似的, 我们可以向量组的加法和数乘运算, 进而把向量组看成 $n\times 1$ 的矩阵

命题 5. V 的一个基 $\alpha_1, \alpha_2, \cdots, \alpha_n$, 如果有线性无关的向量组 $\beta_1, \beta_2, \cdots, \beta_n$, 满足

$$(\beta_1, \beta_2, \cdots, \beta_n) = (\alpha_1, \alpha_2, \cdots, \alpha_n)A$$

则 $\beta_1, \beta_2, \cdots, \beta_n$ 也是基当且仅当 A 可逆.

证明. 以下推断均是'$\Longleftrightarrow$': 只需证 $(\beta_1, \beta_2, \cdots, \beta_n)$ 线性无关, 即 $(\beta_1, \beta_2, \cdots, \beta_n)\mathbf{k} = \mathbf{0}$ 只有零解, 即 $(\alpha_1, \alpha_2, \cdots, \alpha_n)A\mathbf{k} = \mathbf{0}$ 只有零解, 由 $(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 线性无关知 $A\mathbf{k} = \mathbf{0}$ 只有零解, 即 A 可逆. □

推论 6. 如果 V 的两个基 $(\beta_1, \beta_2, \cdots, \beta_n), (\alpha_1, \alpha_2, \cdots, \alpha_n)$ 满足 $(\beta_1, \beta_2, \cdots, \beta_n) = (\alpha_1, \alpha_2, \cdots, \alpha_n)A$, 那么向量 α 分别在两个基下的坐标 $\mathbf{X}, \mathbf{Y}$ 满足

$$\mathbf{Y} = A^{-1}\mathbf{X}$$

例 1. 见 *Lecture17 5.(3)*

子空间的运算

我们重点讨论不那么显然的直和与商空间, 对于子空间的交并和只需要记住以下结论, 并且会证明就行 (这里就不证了, 顺便**未来细说以下子空间的并**)

定理 7. 设 V 是数域 K 上的线性空间, $V_i, i \in I$ 是 V 的子空间, 则

1. $\bigcap\limits_{i\in I} V_i$ 是 V 的子空间
2. $\bigcup\limits_{i\in I} V_i$ 不是 V 的子空间, 若 K 中有无限多的元素.
3. $V_1 + V_2$ 是包含 V_1 和 V_2 的最小的子空间.

定理 8 (维数公式)**.**

$$\dim(V_1 + V_2) = \dim V_1 + \dim V_2 - \dim(V_1 \cap V_2)$$

以上讨论都是有限维的.

证明. 留给未来的你做以复习, 提示, 从小的基开始选起. **明天起连看三天, 第十周周一写证明, 看你还能忘不** □

定义 5. 设 V 是数域 K 上的线性空间, V_1, V_2 是 V 的子空间, 如果 $V_1 + V_2$ 中的每一个向量 α 能够唯一地表示为

$$\alpha = \alpha_1 + \alpha_2, \quad \alpha_1 \in V_1,\ \alpha_2 \in V_2$$

称 $V_1 + V_2$ 是直和, 记作 $V_1 \oplus V_2$.

定理 9. 以下叙述等价

1. $V_1 + V_2 + \cdots + V_n$ 是直和;
2. $\sum\limits_{i=1}^{n} V_i$ 中零向量的表法唯一;
3. $V_i \cap (\sum\limits_{j=0, j\neq i}^{n} V_j) = 0$;
4. $\dim(V_1 + V_2 + \cdots + V_n) = \dim V_1 + \dim V_2 + \cdots + \dim V_n$;
5. 对于每个 i, V_i 取一个基, 合起来是 $\sum\limits_{i=1}^{n} V_i$ 的一个基.

证明.

(1)⟺(2) 充分性显然, 若 (2) 成立, 则假设 $\beta \in V$, 满足

$$\beta = \sum_{i=1}^{n} \alpha_i,\ \beta = \sum_{i=1}^{n} \gamma_i$$

做差得

$$0 = \sum_{i=1}^{n} (\alpha_i - \gamma_i)$$

由零向量表法唯一, 知 $(\alpha_i - \gamma_i) = 0$, 即 β 表法唯一.

(2)⟹(3) 任取 $\alpha \in V_i \cap (\sum\limits_{j=0, j\neq i}^{n} V_j) = 0$, 有 $-\alpha \in V_i, \alpha \in \sum\limits_{j=0, j\neq i}^{n} V_j$, 于是找到了一个在 $\sum\limits_{i=1}^{n} V_i$ 中的零的表法

$$0 = -\alpha + \alpha = -\alpha + \sum_{j=1, j\neq i}^{n} \alpha_j$$

得到 $\alpha = 0$

(3)⟺(4)

$$\dim(V_1 + V_2 + \cdots + V_n) = \dim(V_1 + V_2 + \cdots + V_{n-1}) + \dim V_1$$

归纳地, 得到

$$\dim(V_1 + V_2 + \cdots + V_n) = \dim V_1 + \dim V_2 + \cdots + \dim V_n$$

反之同理 (试着补充一下过程, 从维数公式出发)

(4)⟹(5) 取每个 V_i 里的一个基 $(\alpha_{i1}, \alpha_{i2}, \cdots, \alpha_{im_i})$ 构成一个向量组 S, 可知这个 S 可以表示 $V_1 + V_2 + \cdots + V_n$ 中的任意向量, 又由 (4), $V_1 + V_2 + \cdots + V_n$ 的维数为 $m_1 + m_2 + \cdots m_n$, 等于 S 中向量的个数. 由前面的命题知 S 是一个基.

(5)⟹(1) 假设有分解

$$0 = \alpha_1 + \alpha_2 + \cdots + \alpha_n$$

对任意的 $\alpha_i \in V_i$, 有 $\alpha_i = a_{i1}\alpha_{i1} + a_{i2}\alpha_{i2} + \cdot * + a_{in_i}\alpha_{in_i}$, 带入上式, 由 S 线性无关的所有系数 $a_{ij} = 0$, 故 $\alpha_i = 0$, 对所有的 i, 这说明 0 的表法唯一.

***(3)⟹(1)** 假设向量 α 有两种表示方式

$$\alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_n$$

$$\alpha = \beta_1 + \beta_2 + \cdots + \beta_n$$

其中 $\alpha_i, \beta_i \in V_i$, 那么有

$$V_i \ni \alpha_i - \beta_i = (\alpha_1 - \beta_1) + (\alpha_2 - \beta_2) + \cdots + (\alpha_n - \beta_n) \in (\sum_{j=0, j\neq i}^{n} V_j)$$

由于交集是空集, 故 $\alpha_i = \beta_i$, 这说明任意向量表示方法唯一, 即 $V_1 + V_2 + \cdots + V_n$ 是直和.

□

线性同构

定义 6. 设 V_1, V_2 是数域 K 上的线性空间, 设 $\sigma : V_1 \longrightarrow V_2$ 是一个双射, 且保持加法和数量乘法, 即

$$\sigma(\alpha+\beta) = \sigma(\alpha) + \sigma(\beta), \quad \sigma(k\alpha) = k\sigma(\alpha)$$

称 σ 是一个线性同构, 若 V_1, V_2 之间存在一个线性同构 σ, 称 V_1, V_2 是同构的, 记为 $V_1 \cong V_2$

注. 可以验证同构是一个等价关系.

同构可以从定义平凡地 (也许不那么平凡? 哪天你试试看 (P202)) 推得各种看上去显然的性质 (比如 $\sigma(0) = 0'$), 还有比较重要的性质: **域 F 上的两个有限维线性空间同构的充分必要条件是它们维数相等**, 证明只需要选取 V 的一个基 $(\alpha_1, \alpha_2, \cdots, \alpha_n)$, V' 的一个基 $(\gamma_1, \gamma_2, \cdots, \gamma_n)$, 定义映射

$$\sigma : V \longrightarrow V'$$
$$\alpha = \sum a_i\alpha_i \longmapsto \sum a_i\gamma_i$$

由基表示向量的唯一性得到 σ 是双射, 且容易验证是一个同构映射. 特别的, 我们得到坐标映射也是同构映射, 这样就可以通过研究 F^n 来研究线性空间.

定理 10 (同构定理)**.** 设 V 是域 F 上的 n 维线性空间, 则 V 同于列向量空间 F^n

定义 7. 设域 F 上的线性空间 V 中两个向量 $\mathbf{v}_1, \mathbf{v}_2$ 如果满足 $\mathbf{v}_1 - \mathbf{v}_2 \in U$, 则称 $\mathbf{v}_1, \mathbf{v}_2$ 等价 (是良好定义的! 请验证这个关系确实是一个等价关系.), 其中 U 是一个子空间. 记向量 $\mathbf{v}$ 的等价类为 $\mathbf{v}+U$, 称为 $\mathbf{v}$ 的 U-陪集, 由等价类的性质 (可以验证以下定义不依赖代表元的选取), 合理定义集合 V/U(V 对于子空间 U 的商集) 和其中的加法和数乘运算:

$$V/U := \{\mathbf{v}+U | \mathbf{v} \in V\}$$
$$(\mathbf{v_1}+U) + (\mathbf{v_2}+U) = (\mathbf{v_1}+\mathbf{v_2}) + U$$
$$k(\mathbf{v}+U) = (k\mathbf{v}) + U$$

可以验证 V/U 是一个线性空间! 我们称之为 V 关于子空间 U 商空间.

定理 11. 设 V 是域 F 上的一个有限维线性空间, U 是 V 的一个子空间, 则

$$\dim(V/U) = \dim V - \dim U$$

证明. 选取 U 的一个基 $(\alpha_1, \alpha_2, \cdots, \alpha_r)$, 可以扩充成 V 的一个基 $(\alpha_1, \alpha_2, \cdots, \alpha_r, \alpha_{r+1}, \cdots, \alpha_n)$, 下证 $S = (\alpha_{r+1}+U, ..., \alpha_n+U)$ 是 V/U 的一个基, 设

$$c_1(\alpha_{r+1}+U) + c_2(\alpha_{r+2}+U) + \cdots + c_{n-r}(\alpha_n+U) = 0+U$$

则向量具有等价关系

$$(c_1\alpha_{r+1} + c_2\alpha_{r+2} + \cdots + c_{n-1}\alpha_n - 0) \in U$$

由 α 的选取方式, 它们线性无关, 故系数均为零, 故 S 线性无关. 又对任意的 $(\beta+U) \in V/U$, 设

$$\beta = d_1\alpha_1 + d_2\alpha_2 + \cdots + d_n\alpha_n = \gamma + d_{r+1}\alpha_{r+1} + \cdots + d_n\alpha_n$$

其中 $\gamma \in U$，故 β 和 $(d_{r+1}\alpha_{r+1} + \cdots + d_n\alpha_n)$ 等价，

$$\beta + U = d_{r+1}(\alpha_{r+1} + U) + c_2(\alpha_{r+2} + U) + \cdots + c_{n-r}(\alpha_n + U)$$

从而证明了任意 β 可由 S 线性表出，从而 S 是一个基. □

注. 熟悉一下商空间

如果 $\eta \in U$, 那么 $(\eta - 0) \in U$, 所以 $\eta + U = 0 + U = U$

U 是商空间的零元.

试着简化上述证明的写法.

反之, 如果得到了商空间 V/U 的一个基, 我们选取代表元张成的子空间, 能否从它得到全空间?

定理 12. 如果商空间 V/U 的一个基为 $(\beta_1 + U, \cdots, \beta_t + U)$, 令

$$W = \operatorname{span}(\beta_1, \cdots, \beta_t)$$

则 $V = U \oplus W$, 且 $(\beta_1, \cdots, \beta_t)$ 是 W 的一个基.

证明. (自己尝试) 由于 $(\beta_1 + U, \cdots, \beta_t + U)$ 是一个基, 所以

$$k_1(\beta_1 + U) + \cdots + k_t(\beta_t + U) = U$$

只有零解, 即 $k_1\beta_1 + k_2\beta_2 + \cdots + k_t\beta_t \in U$ 当且仅当系数全为零, 故 $k_1\beta_1 + k_2\beta_2 + \cdots + k_t\beta_t = 0$ 当且仅当系数全为零, 且

$$\operatorname{span}(\beta_1, \beta_2, \cdots, \beta_t) \cap U = 0$$

故 $W + U$ 是直和, 进而

$$\dim V = \dim(V/U) + \dim U = \dim W + \dim U = \dim(W + U)$$

最后一个等号用到直和, 故 $V = U + W$. □

证明. (丘) 先证 $V = U + W$, 任取 $\alpha \in V$, 由于 $(\beta_1 + U, \cdots, \beta_t + U)$ 是 V/U 的一个基, 因此

$$\begin{aligned} \alpha + U &= a_1(\beta_1 + U) + a_2(\beta_2 + U) + \cdots + a_t(\beta_t + U) \\ &= (a_1\beta_1 + a_2\beta_2 + \cdots + a_t\beta_t) + U \end{aligned}$$

从而 $\eta = \alpha - (a_1\beta_1 + a_2\beta_2 + \cdots + a_t\beta_t) \in U$, 注意到 $(a_1\beta_1 + a_2\beta_2 + \cdots + a_t\beta_t) \in W$, 故任意的 $\alpha \in V$ 可以写成 $\alpha = \eta + \beta \in U + W$. 故 $V = U + W$(另一个方向的包含关系显然)

再证 $V = U + W$ 是直和, 任取 $\gamma \in U \cap W$, 可以

□

2 一元多项式环的通用性质, 整除, 带余除法, 最大公因式, 互素, 不可约多项式

定义 8. 数域 K 上的一元多项式是指如下的表达式

$$f(x) = a_n x^n + ... + a_1 x + a_0$$

其中 a_i 称为系数, 如果 a_n 不等于零, 称 $a_n x^n$ 为 $f(x)$ 的**首项**, 称 n 是 $f(x)$ 的**次数**, 记作 $\deg f(x)$, 将数域 K 上的一元多项式的集合记为 $K[x]$, 定义其上的加法乘法如下:

$$f(x) + g(x) := \sum_{i=0}^{n} (a_i + b_i) x^i$$

$$f(x)g(x) := \sum_{s=0}^{n+m} \left(\sum_{i+j=s} a_i b_j \right) x^s$$

称 $f(x) = g(x)$ 当且仅当每一个系数不为零的项相同.

注. *可以验证这是一个环, 如果一个带有加法和乘法结构的集合 R 满足*

1. $(R, +)$ 是交换群

2. 乘法满足结合律.

3. 乘法对加法具有 (左右) 分配律

则称 $(R, +, \cdot)$ 是一个环, 如果乘法还满足交换率则是交换环, 满足存在乘法单位元则是有单位元的环.

注. *称 x 是不定元 (x 不属于 K), 补充定义系数全为零的多项式称为零多项式, 记为 0, 定义 $\deg 0 = -\infty$, 其中*

1. $-\infty + -\infty = -\infty$

2. $n + -\infty = -\infty, \forall n \in \mathbb{N}$

3. $n > -\infty, \forall n \in \mathbb{N}$

命题 13. 设 $f(x), g(x) \in K[x]$, 则有

$$\deg(f \pm g) \leq \max\{\deg f, \deg g\}$$

$$\deg(fg) = \deg f + \deg g$$

证明. 交给你了 (从定义得到就好啦) □

一元多项式环立刻满足很多环的性质, 但是你对环不熟悉, 所以这里列举一些

1. 各种唯一
2. 可以定义减法
3.

一元多项式还有自己独特的性质, 比如

1. 乘法满足消去律 (因为 $f(x), g(x) \neq 0$ 能够推出 $f(x)g(x) \neq 0$ (不存在不平凡的零因子, 或者叫**无零因子环**))
2. 有单位元 ($f(x) = 1$)
3. 是交换环 (即使 $M_n(K)$ 不是交换环, 但是 $K[A]$ 是交换环)

满足上述三条的环称为**整环**

命题 14. 环 R 的一个子集 R_1 是一个子环的充分必要条件是 R_1 对 R 的减法和乘法都封闭

$$a, b \in R_1 \implies a - b \in R_1, ab \in R_1$$

减法保证了零元的存在性, 进而保证了负元的存在性, (又或者从减法的定义知, 这条保证了负元的存在, 进而保证了零元的存在, 这样之前的叙述只是证明的顺序) 并且本身保证了加法封闭, 我目前把它理解成一种处理上的技巧.

定理 15. R 是一个有单位元的交换环, 可以看成是一个数域 K 的扩环, 其中 K 道 R 的子环 R_1 保持加法和乘法的双射记作 τ. 任意给定 $t \in R$, 令

$$\begin{aligned} \sigma : K[x] \quad &\longrightarrow \quad R \\ f(x) = \sum_{i=0}^{n} a_i x^i \quad &\longmapsto \quad \sum_{i=0}^{n} \tau(a_i) t^i =: f(t) \end{aligned}$$

则 σ 是 $K[x]$ 到 R 的一个映射, 且保持加法和乘法运算.

证明. 根据定义, $\sum_{i=0}^{n} a_i x^i$ 的表法唯一 (这很重要!), 这保证了 σ 是一个映射, 而了 σ 保持乘法和加法是平凡的 (因为子环 R_1 和 K 是交换环 □

注. 目前还不太能理解, R 中除子环以外的元素为什么可以用多项式的形式表示? 这是一定的吗?

注. 好像又有点理解了, 这是在说如果 R 可以看成 K 的一个扩环, 则任意 R 中的元素, 都可以带入到 $K[x]$ 里面而保持原来的 $K[x]$ 的等式. 保证这样合法性的是我们证明了"带入"是一个映射.

于是我们只需要好好研究 $K[x]$ 的性质, 之后可以方便推广.

推论 16. 很快啊! 得到以下简单推论

1. $f(x)g(x) \neq 0 \implies \deg f(x) \leq \deg f(x)g(x)$
2. $c = f(x)g(x) \implies \deg f(x) = \deg g(x) = 0$

整除和带余除

我们定义如果多项式 $f(x)$ 可以写成 $f(x)=g(x)h(x)$, 则称 $f(x)$ 可以被 $h(x)$ 或 $h(x)$ 整除, 记号是 $g(x)\mid f(x)$. 整除有些关于零次多项式, 零多项式, 本身整除的平凡的性质, 这些和你所想当然的没有什么差别, 此处略过, 它们的证明也很简单, 只需要按照定义写出来即可. 这里定义一个关系 $\sim$, 我们称 $f(x)\sim g(x)$ 如果它们能相互整除, 也叫相伴. 而

$$f(x)\sim g(x)\Longleftrightarrow f(x)=cg(x)$$

是显然的. 试着补充证明.

注. 整除关系具有传递性和反身性, 不具有对称性

命题 17. 如果 $g(x)\mid f_i(x), i=1,2,\cdots,s$ 那么对任意 $u_1(x),u_2(x),\cdots,u_s(x)\in K[x]$ 都有

$$g(x)\sim\sum_{i=1}^{s}u_i(x)f_i(x)$$

或者说如果 $g(x)$ 整除一系列 $f_i(x)$ 那么 $g(x)$ 也整除它们的倍式和.

定理 18. 设 $f(x),g(x)\in K[x]$, 则存在唯一的一对多项式 $h(x),r(x)$, 满足

$$f(x)=h(x)g(x)+r(x),\ \deg r(x)<\deg g(x)$$

称 $f(x)$ 为被除式，$g(x)$ 为除式, $h(x)$ 为商式, $r(x)$ 称为余式.

证明. 存在性: 设 $\deg g(x)=m$,

$m=0$, 此时

$$f(x)=\left(\frac{1}{g(x)}f(x)\right)g(x)+0$$

$m>0$**, 且** $\deg f(x)<m$

$$f(x)=0\ g(x)+f(x)$$

$m>0$**, 且** $\deg f(x)\geq m$ 设 $f(x),g(x)$ 的首项分别为 a_nx^n,b_mx^m, 对 n 做数学归纳法, 设 $n-1$ 次多项式可做带余除法, 则

$$f_1(x)=f(x)-a_nb_m^{-1}x^{n-m}g(x)$$

的首项次数小于 n, 故 $\deg f_1<n$,

$$f_1(x)=h_1(x)g(x)+r_1(x)$$

从而

唯一性: 设

$$f(x)=h(x)g(x)+r(x)$$

$$f(x)=h_1(x)g(x)+r_1(x)$$

相减得

$$(h_1(x)-h(x))g(x)=r(x)-r_1(x)$$

故 $\deg g(x)+\deg(h_1(x)-h(x))=\deg(r(x)-r_1(x))<\deg g(x)$, 从而 $h_1(x)-h(x)$ 只能是零多项式, 进而 $r(x)=r_1(x)$

□

这个大概还是很有用的, 嗯, **定理 6** 是很重要的! 由带余除法表示的唯一性立即得出整除性不随域的扩大而改变.

练习. *整数环 Z 上也有带余除法, 试着证明存在性和唯一性*

互素

如果 $K[x]$ 中 $c(x)\mid f(x)$, $c(x)\mid g(x)$, 称 $c(x)$ 是 $f(x)$ 和 $g(x)$ 的公因式.

定义 9. $K[x]$ 中, $d(x)$ 是 $f(x)$ 和 $g(x)$ 的最大公因式, 如果任意的公因式可以整除 $d(x)$.

注. *由定义得到*

1. *0 和 0 的最大公因式是 0*
2. *两个多项式的最大公因式相伴*
3. *$f(x)$ 是 $f(x)$ 和 0 的最大公因式*
4. *$f(x), g(x)$ 不全为零, 则它们的最大公因式不为零.*

我们用 $(f(x), g(x))$ 表示首项为一的最大公因式.

引理 19. 如果有 $f(x) = h(x)g(x) + r(x)$, 那么 $f(x), g(x)$ 的最大公因式也是 $g(x), r(x)$ 的最大公因式.

证明. 记 $c(x)$ 是 $f(x), g(x)$ 的公因式, 那么由 $r(x) = f(x) - h(x)g(x)$ 知 $c(x)$ 是 $r(x)$ 的因式, 进而是 $r(x), g(x)$ 的公因式, 反之同理, 所以它们具有完全相同的公因式. 进而具有相同的最大公因式. □

这保证了可以用辗转相除法求最大公因式. 并且由辗转相除的过程我们得到以下推论

推论 20 (*). 任意 $K[x]$ 中的两个多项式 $f(x), g(x)$, 存在它们的一个最大公因式 $d(x)$, 且存在 $u(x), v(x) \in K[x]$, 使得

$$d(x) = u(x)f(x) + v(x)g(x)$$

很重要!!!

定义 10. 称多项式 $f(x), g(x)$ 互素, 如果它们的首一最大公因式是 1

定理 21. $f(x), g(x)$ 互素的充分必要条件是存在 $u(x), v(x) \in K[x]$, 使得

$$u(x)f(x) + v(x)g(x) = 1$$

证明. 只证充分性, 如果该式成立, 则任意公因式 $c(x)$ 都能整除 1, 这说明 $\deg c(x) = 0$, 故它们的首一最大公因式是 1. □

这些结论基于辗转相除法, 进而基于带余除法, 所以我们知道域的扩大不影响上述结论. 互素满足以下性质

1. 如果 $f(x) \mid g(x)h(x)$, 且 $(f(x), g(x)) = 1$, 那么 $f(x) \mid h(x)$

   证明. 可知成立 $u(x)f(x) + v(x)g(x) = 1$, $f(x)p(x) = g(x)h(x)$, 于是

   $$u(x)f(x)h(x) + v(x)g(x)h(x) = u(x)f(x)h(x) + v(x)f(x)p(x) = h(x)$$

   故 $f(x) \mid h(x)$ □

3 线性映射及运算, 幂等变换和投影, 核与象, 核的商空间同构象, 线性映射的矩阵表示, 过渡矩阵, 相似矩阵

定义 11. 设 V 和 W 是域 F 上的线性空间, 映射 $\varphi\colon V \to W,\ \alpha \mapsto \beta$, 其保持加法和数量乘法运算

$$\varphi(\alpha+\beta)=\varphi(\alpha)+\varphi(\beta),\ \varphi(k\alpha)=k\varphi(\alpha)$$

称 φ 为 V 到 W 的一个线性映射.

注. *线性同构是满足以上条件的双射. 线性映射保持很好的性质 (比如一定把零向量映射为零向量), 注意可能会把线性无关的向量组映射为线性相关的向量组. (但是如果原向量组线性相关, 那么映射后一定线性相关)*

通过线性映射保持加法和数乘, 线性映射被一个基的映射完全刻画, 存在性和唯一性都由此入手.

定理 22. 如果一个线性映射把 V 的一个基 $(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 映射到 W 中的任意 n 个向量 $(\beta_1,\beta_2,\cdots,\beta_n)$, 则该映射唯一.

证明. 构造一个映射分别把 α_i 映射到 β_i, 可知这个映射是唯一的. □

记 V 到 W 线性映射的全体为 $\mathrm{Hom}(V,W)$, 平凡的定义其上的加法和数量乘法 (验证是良好定义的), 得到 $\mathrm{Hom}(V,W)$ 是域 F 上的一个线性空间. 定义映射的乘法为映射的复合, 该乘法满足结合律 (显然), 满足分配律 (容易验证), 所以特别的, 对于线性变换, $\mathrm{Hom}(V,V)$ 是一个有单位元的环.

定义 12. 一个非空集合 $\mathcal{A}$ 如果有加法, 乘法运算, 以及域 F 与 $\mathcal{A}$ 的纯量乘法运算, 并且 $\mathcal{A}$ 对于加法和纯量乘法运算是域 F 上的一个线性空间, $\mathcal{A}$ 对于加法和乘法是一个有单位元的环, $\mathcal{A}$ 的乘法和纯量乘法满足

$$k(\alpha\beta)=(k\alpha)\beta=\alpha(k\beta),\ \forall k\in F,\alpha,\beta\in\mathcal{A}$$

则称 $\mathcal{A}$ 是域 F 上的一个代数, 称线性空间 $\mathcal{A}$ 的维数为代数 $\mathcal{A}$ 的维数.

$\mathrm{Hom}(V,V)$ 是域 F 上的一个代数.