高等代数选讲

作者: ZZH

本讲义使用于 HEO 高等代数II 课程中,
内容由 LaTeX编译, 图片使用 GeoGebra 绘制.
参考多部书目, 仅用作学习讨论和笔记需求. 如有错误, 欢迎指正.
使用时间 2025/3/17
最后编译时间 April 1, 2025

每逢拾笔, 愿母亲安康.
本笔记摘选自巴猪数学讲义: 第二卷高等代数.
谨以彼书赠与女友与巴猪的陪伴.
祝诸位在数学上逢见挚爱.

摘自 Grassmann 扩张论. 您的理论如今已是大学入学必学的课程.

我始终坚信我在此科学上所付出的劳动不会白费, 它耗尽了我生命中最重要的阶段, 让我付出了超常的努力. 我当然知道我给出的这门科学的形式还不完善, 它一定是不完善的. 但是, 我知道而且有义务在此声明 (可能有人会认为我很狂妄), 即使这一成果再过十七年或更长时间还不被使用, 也没有真正融入到科学的发展之中, 它冲出遗忘的尘埃现身的时候也一定会到来, 现在沉睡着的思想结出硕果的那一天一定会到来. 我知道, 如果我今天还不能 (如我至今徒劳地期望那样) 把学者们吸引到我的周围, 用这些思想帮助他们成果累累, 促使其进步, 丰富其学识, 那么这种思想在将来一定会重生, 或许以另一种新形式, 与时代发展水乳交融. 因为真理是永恒不灭的.

摘自 Grothendieck 丰收与播种. 愿数学的远端没有硝烟.

我可以用同样的坚果意象来说明第二种方法:

第一种类比: 我首先想到的是将坚果浸泡在某种软化液体中——为何不直接用水呢? 你偶尔摩擦坚果以促进液体渗透,其余时间则静待其变. 经过数周甚至数月, 外壳逐渐变得柔软——当时机成熟, 仅需用手轻轻一压, 它便会如完美成熟的牛油果般自然裂开!

几周前, 我的脑海中闪现了另一幅图像.

那片等待被理解的未知, 仿佛一片坚硬的土地或泥灰岩, 抗拒着侵入...而海水无声无息地悄然上涨, 看似毫无动静, 潮水遥远得几乎听不见声响...但它终将温柔包裹住那顽固的物体.

代数就是这片 Rising Sea.

Lecture 5　线性空间的构建

5.1　域的构建与动机

对代数的第一次接触, 或许是在小学解方程的时候, 但正如我们在绪论内的代数发展中所谈论的, 解代数方程至少是距今两百年前的主流. 两百年内的代数, 则是针对着代数结构展开的, 而正式与这个范畴的第一次接触, 实际就是在线性空间之中.

既然是两百年前的事, 我们就让目光穿越回两百年前, 带着自下而上的视角看向今日之代数. 所谓自下而上, 就是从那些具体的例子出发, 来看看代数是如何被抽象出来的.

首先是域.

描述域的最简语言, 就是配备了四则运算的代数. 回忆一下我们从小是如何认识数的, 我们学习加法, 进而学习加法的逆运算减法; 学习乘法, 乘法的本意是加法的累积, 进而学习要难得多的除法, 难点在于除法对最自然的整数环是不封闭的. 我们每学习一个运算, 我们都要研究它的运算规则, 无外乎是结合律, 交换律, 分配律.

所谓代数结构是指这般的内容.

Definition 5.1.1 (**代数运算**)**.** 设一个非空集合 S, 在其上定义的映射

$$S \times S \to S$$
$$(a, b) \mapsto a \cdot b$$

称为 S 上的一个 (二元) **代数运算** "$\cdot$". 称配备了一个代数运算的二元组 $(S, \cdot)$ 为一个**代数结构**

运算往往具备着某些性质, 这些性质作为公理记录在二元组的 "$\cdot$" 之中. 其中最重要的四条为:

- **[C]** 交换律 commutativity : $a \cdot b = b \cdot a,\ \forall a, b \in S$
- **[A]** 结合律 associativity : $(a \cdot b) \cdot c = a \cdot (b \cdot c)\ \forall a, b, c \in S$
- **[Id]** 单位元 (存在性) identity : $\exists id \in S$ s.t. $id \cdot a = a \cdot id = a$.
- **[Iv]** 可逆性 invertiblity: $\forall\, a \in S,\ \exists b \in S$ s.t. $a \cdot b = b \cdot a = id$

这些性质的组合构造出截然不同的代数结构.

赋予单代数运算的代数结构主要有如下的四种:

- 具备 [A] 的代数结构称为**半群 semi-group**,
- 具备 [A+Id] 的代数结构称为**幺半群 monoid**,
- 具备 [A+Id+Iv] 的代数结构称为**群 group**,
- 具备 [A+C+Id+Iv] 的代数结构称为 **Abel 群 (交换群) abelian group**.

Remark 5.1.1. 1) "$\cdot$" 不过是一个符号, 实际上它可以替换成任何的符号, 我们通常喜欢用 "+" 来表示具备交换律的运算; $\cdot$ 通常表示不交换的运算; "$\circ$" 表示函数的复合运算; 我们不去关注 "$-$" 和 "$\div$", 因为它们的出现无非就是 "+" 和 "$\cdot$" 可逆的场合以表示其逆运算, 特别地, $\cdot$ 的逆运算记作 $\square^{-1}$, 并且因为乘法往往不具备交换律要注意其位置.

2) 事实上, 代数就是满足运算封闭性的一个集合. 乍看之下似乎不能够再显然, 但是映射和同构的加入, 让这一切都丰富了起来.

3) 交换性往往是更强的要素, 事实上大多数数学对象并不具备交换性, 如映射 (函数) 的复合与矩阵的乘法. 但是结合律基本上是所有运算都应当具备的性质, 一旦结合律不成立, 则甚至连 $a\cdot b\cdot c$ 这样的写法都是违法的.

4) 配备的运算可以是多个, 但是要注意它们之间的联系. 孤立的两种运算对结构没有起到固定的作用.

Exercise 5.1. 验证幺半群 M 满足如下性质:

(1) 任意元素的逆元 (如果存在的话) 唯一.

(2) 单位元唯一.

在后续我们会发现对于线性映射也有类似的性质, 因为线性映射的全体与矩阵全体线性同构, 而矩阵全体是一个幺半群. 从下至上的代数构建的意义就在于此, 将一个性质放缩到最简单的条件上, 一层一层地把一个特别的代数结构的性质垒上去. 这也是为什么说线性代数是抽象代数的第一课, 不仅仅在于线性空间和矩阵是特殊的一类代数结构, 更在于其中具备的一些推理能够诱导出对抽象代数的讨论.

在小学时我们会反复强调减法和除法不可交换, 因此括号很重要, 所谓括号就是结合律, 显然的是减法和除法是不满足于结合律的. 这是因为减法和除法压根就不是群上的运算, 作为群的逆运算它们满足:

Proposition 5.1.1. 设群 $(G,\cdot)$, $\forall a,b,c\in G$ 满足:

(1) $(a^{-1})^{-1}=a$ 即逆的逆为原元素;

(2) $(ab)^{-1}=b^{-1}a^{-1}$;

(3) 若运算为 $+$, 则有 $(a-b)-c=a-(b+c)$;

(4) 若运算为 $+$, 则有 $a-b=-(b-a)$;

Example 5.1.1.

- $(\mathbb{N},\gcd())$ 是一个半群 (gcd() 表示最大公因数 greatest common divisor) . 只需验证结合律, 任取 $a,b,c\in\mathbb{N}$, 设 $d_1=\gcd(a,b),d_2=\gcd(b,c)$, 则 $\gcd(d_1,c)=\gcd(a,d_2)$, 因为一方面显然 $\gcd(d_1,c)\,|\,a,b,c$, 从而 $\gcd(a,d_2)\,|\,d_2\,|\,\gcd(d_1,c)\,|\,b,c$, 另一方面我们可以同理得到 $\gcd(d_1,c)\,|\,d_1\,|\,\gcd(a,d_2)\,|\,a,b$, 从而得到二者相互整除的伴随关系, 在 $\mathbb{N}$ 上, 两者直接相等 (在 $\mathbb{Z}$ 上则是相差 ±1) . 事实上,

$$\gcd(\gcd(a,b),c)=\gcd(a,b,c)=\gcd(a,\gcd(b,c))$$

- 同理, $(\mathbb{N},\mathrm{lcm}())$ 是一个半群 (lcm() 表示最小公倍数 least common multiple) .
- $(\mathbb{N},+)$ 是一个幺半群,单位元为 0; $(\mathbb{Z},+)$ 是一个 Abel 群; $(\mathbb{Z}^*,\times)$ 是一个幺半群, 单位元为1 ($\mathbb{Z}^*:=\mathbb{Z}-0$); n 阶矩阵关于矩阵的乘法构成一个幺半群, 单位元为 $\boldsymbol{I}_n$; n 阶矩阵关于矩阵的加法构成一个不交换的群.
- 令 $\mathbb{Z}_m:=\mathbb{Z}/(m)$ 表示模 m 同余关系下的商集, 称作模 m 同余环. 其中模 m 同余关系定义为 $a\sim b\Leftrightarrow m\,|\,(a-b)$ 是一个等价关系, 刻画的是 a 和 b 在除以 m 后有相同的余数. 于 $\mathbb{Z}_m$ 上构造加法为 $[a]+[b]=[a+b]$, 构造乘法为 $[a][b]=[ab]$, 则 $(\mathbb{Z}_m,+)$ 为 Abel 群, $(\mathbb{Z}_m,\cdot)$ (默认对乘法时都无 0 元) 为幺半群.
- 设 M 为一个幺半群, 其中的单位元为 e. 则 $U(M):=\{a\in M:\exists\,a^{-1}\in M\}$ 为群, 称作 M 的单位群.
- $U((\mathbb{N},+))=(0)$, $U((\mathbb{Z},\cdot))=(1)$,
- 因为 $\forall[a]\in(\mathbb{Z}_m,\cdot)$, a 可逆当且仅当 $\gcd(a,m)=1$, 从而

$$\mathbb{Z}_m^*:=U(\mathbb{Z}_m,\cdot)=\{[a]\in\mathbb{Z}_m:\gcd(a,m)=1\}$$

因此, 特别地,

$$\mathbb{Z}_p^*=U(\mathbb{Z}_p^*)$$

为一个 Abel 群, 其中 p 为素数.

考察例子中的 $\mathbb{Z}_p$, 它同时对 $+$ 和 $\cdot$ 构成 Abel 群, 对于配备了更多运算的代数结构, 我们可研究的内容就进一步扩大了.

有了前面的预备, 我们对域的定义可以更加简单. **域**是配备了两个运算的代数结构 $F:=(S,(+,\cdot))$, 它关于加法和乘法 (除去加法的单位元 0) 分别构成一个 Abel 群. 除此之外, 为了将两个运算联系在一起 (这样的想法来自于将乘法视为加法的累积), 我们还需要一则原则:

- **[D]** 分配律 distributivity : $a\cdot(b+c)=a\cdot b+a\cdot c$, $(b+c)\cdot a=b\cdot a+c\cdot$, $\forall a,b,c\in S$

具备这一切的域, 就具备了四则运算. 可以验证, $\mathbb{Z}_p$ 是一个域, 并且它的阶 (视作集合的基数) 为 $|\mathbb{Z}_p| = p$ 个, 和我们所学的数域不同, 这是一个**有限域**.

Exercise 5.2. 环 R 是一个赋有两个代数运算加法和乘法的代数结构, R 关于加法构成 Abel 群 R^+, 关于乘法构成一个半群 R^*, 两个运算之间配备了分配律 [D]. 证明: 加法的单位元 0 一定是乘法的不可逆元.

我们更常研究结构更好的一些代数结构, 比如说**含 1 的交换环**, 它是一个环, 且它关于乘法构成一个交换的幺半群 (即具备 [C],[A],[Id]) R^*. 更不用提域. 因此上述练习中提到的性质完全可以推广至交换环与域之中, 而域中想要让 F^* 成为一个 Abel 群, 势必是要去掉 0 的, 为了方便我们在讨论环上的乘法代数结构时, 都是去掉 0 的.

Remark 5.1.2. 因此, 如果有人问你 1/0 是多少, 从代数角度来回答, 0 不是可逆元, 仅此而已.

因为域关于两个运算都为 Abel 群, 为了区分开两者的单位元和逆元, 我们记 0 为加法的单位元, 记 1 为乘法的单位元; 记 $-\square$ 为加法的逆元 (称为负元), 记 $\square^{-1}$ 为乘法的逆元; 根据群的性质, 上述内容皆唯一.

Remark 5.1.3. 分配律是将域上的两个运算联接的纽带. 通过我们的论述可以看出, 如若没有分配律, 我们完全可以这么去定义一个域上的两个运算: 取 $S = \mathbb{Z}$, 取 $+$ 为整数的加法, 取 $\odot$ (为了将其与普通的乘法区分开, 这样记) 为 $a \odot b = a + b + 1$ 则有单位元 -1, 每个元素 a 都有逆元 $-a - 2$ 分配律显然. 两则运算彼此独立甚至平行, 但研究后者对整数环并无意义.

域是线性空间的根源, 我们最熟悉的代数结构矩阵就是定义在域之上的. 回忆矩阵的运算的全部定义, 几乎必须要基于域的四则运算展开, 其中除法或许可以尝试摘除 (因为除法并未参与到矩阵的运算定义甚至矩阵的逆中) 但是如下的例子就会发现环 (可以初步理解为不具备乘法交换律和乘法可逆性的域) 上的矩阵会变得格外复杂:

考虑

$$\boldsymbol{A} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

假若 a, b 均不为 0, 但是又均不可逆, 则矩阵 $\boldsymbol{A}$ 不可逆. 同样的想法驱动下, 会发现矩阵最根本的 Gauss 消元法都进行不下去, 从而矩阵的种种性质都将举步维艰.

当然, 对这种情况的研究虽然是将问题变困难了, 反而将视角变得更开阔, 能接触到更广的天空. 对这一理论的研究藏在了模论之中.

接下来我们看几个例子, 从这些例子中出发去寻觅线性空间的结构.

- **向量空间** F^n 向量空间上配备了两种运算, 两种都是按坐标的运算, 一种是加法, 一种是数乘. 向量空间循加法构成了一个 Abel 群, 但是对数乘并不构成一个代数

运算, 因为数乘本质是如下的运算:

$$\begin{aligned} F^n \times F &\to F^n \\ (\boldsymbol{\alpha}, k) &\mapsto k\boldsymbol{\alpha} = (ka_1, ka_2, \cdots, ka_n)^T \end{aligned}$$

其中 $\boldsymbol{\alpha} = (a_1, a_2, \cdots, a_n)^T$. 因此其数乘一定是伴随着一个域 F 的二元运算.

此外, 也许此刻会联想到在二次型中提到的双线性型 $\boldsymbol{\alpha}^T\boldsymbol{\beta}$ 并非 F^n 上的代数运算, 可以认为它是与其伴随的行向量空间 F_n 之间的二元运算 $F^n \times F_n \to F$, 它射入的也并非向量空间本身.

- $m \times n$ **阶矩阵** $\mathcal{M}_{m,n}(F)$ 我们可以将向量空间上的加法和数乘都自然地推广到矩阵上.
  - 在这里也可以注意到矩阵的乘法越来越反自觉, 因为矩阵的乘法的本质是将一个向量映射到另一个向量, 蕴含的几何思想是坐标变换. 事实上, n 阶方阵全体 $\mathcal{M}_n(F)$ 关于矩阵的加法和乘法构成一个有 1 的环, 其关于矩阵的乘法构成一个幺半群. 而所有可逆矩阵的全体记为 $GL_n(F)$ 它是一个环, 不具备交换性, 由于矩阵的加法没什么太多可研究的, 我们的目光往往集中在其乘法上, $GL_n(F)$ 于这层意义下称为**一般线性群**.
  - 所以我们身边就有这么一个例子, 它是我们即将要讨论的线性空间, 又是抽象代数中的环, 因此矩阵的一般理论或许在线性代数范畴下是说不完全的. 而到了高等线性代数中, 矩阵只是张量的一个例子.
  - 如果把域改成一般的含有 1 的交换环 R, $\mathcal{M}_n(R)$ 依旧能够定义加法乘法和数乘, 它关于加法和数乘依旧构成线性空间, 关于加法和乘法依旧构成一个含有 1 ($\boldsymbol{I}_n$) 的非交换环.

- **域** F **上的多项式全体** $F[x]$ 它与矩阵相仿, 分别有加法乘法和数乘三种运算. 更一般的, 我们依旧可以将 F 改为一个含有 1 的交换环 R, $R[x]$ 关于加法和数乘构成线性空间, 关于加法和乘法构成一个含有 1 (也就是 1) 的交换环.

  如若我们限制多项式的次数, 对于次数不超过 n 次的多项式全体 $F_n[x]$, 其对于乘法显然是不封闭的. 因此我们只考虑它的线性结构.

从例子中看我们其实可以把域的限制放松到环上, 这是我们在讨论完域上的线性空间之后所要做的必要推广, 虽然这会让空间的结构变得更加复杂 (矩阵的大部分性质都会作废) 但是也是研究更深层次数学的必由之路.

构建在含有 1 的环 R 上的线性空间, 我们称其为 **R-模 R-module**.

2025 年的 Abel 奖颁给了柏原正树 Masaki Kashiwara, 以表彰他对代数分析和表示论的重要贡献, 尤其是其在 D-Module 上做出的发展.

代数分析起源于 Hilbert 第 21 问题, 思考将一类特殊的常微分方程的解的存在性与几何的层 (sheaf) 论相结合, 用几何的方法去研究分析的问题. 而后二战结束之后, 在一众数学家的推动之下, 代数几何得到了空前的发展, 因此代数几何就成为了微分方程代数化转变成代数拓扑上的中间桥梁. D-Module 就是重要的中间桥梁, 它的本质是我们刚才所提到的 R-模, 不过根基是建立在层和簇 (variety) 上的. 因此想要学习相关理论, 就至少要将代数基础建立在更高层次的概型 (scheme) 与范畴 (category) 之上.

5.2 线性空间

伴随着线性空间定义的提出, 我们正式地迈进了代数的范畴.

Definition 5.2.1. [线性空间 Linear Space] 设 F 是一个域, 域 F 上的线性空间 V 是一个配备了两个运算的代数结构 $(V,+,(F,\cdot))$, V 关于加法 $+$ 构成一个 Abel 群 V^+, V 的数乘 $\cdot$ 则遵循:

$$V \times F \to V$$
$$(\boldsymbol{v}, k) \mapsto k\boldsymbol{v}$$

数乘运算满足:

(1) **结合律** $k(l\boldsymbol{v}) = (kl)\boldsymbol{v}$.

(2) **单位元** $1\boldsymbol{v} = v$.

(3) **数乘分配律** $(k+l)\boldsymbol{v} = k\boldsymbol{v} + l\boldsymbol{v}$

(4) **加法分配律** $k(\boldsymbol{v}+\boldsymbol{w}) = k\boldsymbol{v} + k\boldsymbol{w}$

其中 k, l 为域 F 中的任意元素, 称为标量 , $\boldsymbol{v}$ 和 $\boldsymbol{w}$ 为线性空间 V 中的任意元素, 称为向量.

Definition 5.2.2. [子空间] 设 V 为域 F 上的一个线性空间. 若 V 的一个子集 W 在域 F 上关于 V 定义的加法与数乘构成一个线性空间, 则称 W 是 V 的子空间.

Example 5.2.1.

- 最为平凡的, $V = (\mathbf{0})$ 是只有零向量的线性空间. $(\mathbf{0})$ 是所有线性空间的子空间.
- 显然域 F 为其自身上的一个线性空间, 加法和数乘循域 F 上的加法和乘法. 这个性质能够让我们去研究有限域的结构. 在这层意义之下, 域 F 的子域 k 为 F 的一个子空间.
- 域 F 上的向量空间 F^n 为一个线性空间, 加法和数乘循向量的加法和数乘. 选取其上的任一向量组 $(\boldsymbol{\alpha_1}, \boldsymbol{\alpha_2}, \cdots, \boldsymbol{\alpha_m})$ 其所有的线性组合

  $$span((\boldsymbol{\alpha_1}, \boldsymbol{\alpha_2}, \cdots, \boldsymbol{\alpha_m})) := \{k_1\boldsymbol{\alpha_1} + \cdots + k_m\boldsymbol{\alpha_m} : \forall k_1, \cdots, k_m \in F\}$$

  是一个 F^n 的一个子空间, 称其为由向量组 $(\boldsymbol{\alpha_1}, \boldsymbol{\alpha_2}, \cdots, \boldsymbol{\alpha_m})$ 张成的子空间.
- 域 F 上的一元多项式全体 $F[x]$ 为一个线性空间, 加法和数乘循多项式的加法和乘法 (与 0 次多项式的). 次数小于等于 n 的一元多项式全体 $F_n[x]$ 为它的一个子空间.

- 区间 $[0,1]$ 上的连续函数全体 $C[0,1]$ 为 $\mathbb{R}$ 上的一个线性空间, 加法和数乘循函数的加法和乘法 (与常值函数的). 则 $\mathbb{R}$ 上的全体多项式函数 $\mathbb{R}^\flat[x]$ 为它的一个子空间, 所有光滑函数 $C^\infty[0,1]$ 也为它的一个子空间.