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 2025/3/10
最后编译时间 March 10, 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 2　绪论：抽象代数思想

2.1　多项式方程：Galois 理论

我们先前已经跟着历史的脚步, 解决了三次方程和四次方程的求根公式. 这些求根公式有什么特征? 其中虽然有些成分比较复杂, 但是也只涉及了加减乘除以及乘幂和开根的算符, 这也就意味着, 只要有了求根公式, 我们哪怕让一个初中生来计算他也能够完全计算出来, 无论我们给定的是什么方程, 他都只需要把系数带进去而已. 我们称这样的多项式是**有根式解的**.

同时, 我们也很容易得知, 部分五次多项式是有根式解的. 非常平凡的例子

$$(x-1)^5 = 2$$

必然有根式解 $x_{1,2,3,4,5} = \sqrt[5]{2} + 1$. 而我们所进一步需要知道的是, 是否有五次乃至更高次数的多项式, 对于这么一个任意系数的多项式, 都有一个通用的求根公式. 也就是说, 任意一个五次及更高次的多项式, 是否是有根式解的?

这个问题困扰了数学家们很多年的时间.

公元 16 世纪, Cardano (虽然不是本人的成果) 和 Ferrari 分别解决了三次方程和四次方程的求根公式. 此后两百年, 再无人能够给出五次方程的求根公式. 我们先前分析 Cardano 公式的一切手段, 似乎看起来非常容易推广, 但全部在五次的情形失效.

更关键的是, 给出的公式虽然易于计算, 却又遗留了诸多麻烦. 我们看一个例子.

$$f(x) = (x-1)(x-2)(x-3) = x^3 - 7x + 6$$

我们一眼就能从因式分解中看出它的三个根来, 可如若我们代入 Cardano 公式, 就会计算出其中一个根为

$$u = g + h = \sqrt[3]{\frac{1}{2}(-6 + \sqrt{-400/27})} + \sqrt[3]{\frac{1}{2}(-6 - \sqrt{-400/27})}$$

显然, 大部分人都无法看出这是一个整数.

这带来一定的困扰. 比如说, 如果我们求解一个方程, 并且已知这个方程的解是一个整数. 但是我们只能用 Cardano 公式去计算, 那么繁杂的公式在开根号的步骤中就很有可能会导致误差进而让数值解离我们真正的解产生偏离, 对于一个整数的结果, 这样的偏离很有可能是致命的. 而基础数学, 正是这种不能接受计算误差的数学.

或许, 是我们的方向错了? 我们要解决的不是一个计算的问题, 而应该是一个数学结构上的证明, 怎样能让多项式根这么简单的问题变得清晰明了?

Lagrange 面对此问题的时候已经预见了五次方程无根式解的结果, 他也可以说是第一位将目光转向解直接关系的人. 他给出了置换的定义, 考虑了根的某种 "几何" 性质. 但他也无法在这个问题给出严格证明, 继而发展了他一部分理论的 Cauchy 也无法做到. 这一划时代的问题的真正突破要来到 19 世纪, 先是 Abel 和 Ruffini, 再是 Galois 的神奇理论, 真正终结了这一问题.

我们先来叙述一下 Galois 得到的结果.

Theorem 2.1.1. Galois 大定理 一个多项式方程是有根式解的当且仅当这个方程的 Galois 群是可解群. 进一步, 因为 n 次一般非常的 Galois 群是对称群 S_n, 而当 $n \geq 5$ 时, S_n 不是可解群; 当 $n \leq 4$ 时, S_n 是可解群, 因此, 五次及以上次数的方程没有根式解.

为了让我们简单地了解一下这个定理, 我们先来看看域.

域是通过交换环构造出来的.

Definition 2.1.1. 交换环 commutative ring R 指的是一个配备了两种二元代数运算的集合, 分别称其为加法 $+$ 和乘法 $\cdot$. 满足如下的运算法则:

(i) R 关于加法 $+$ 构成一个 **Abel 群**R^+, 即:

  (a) **结合律 associativity:** 任意 $a, b, c \in R$ 有 $a + (b + c) = (a + b) + c$

  (b) **0 元 element 0:** 存在 $0 \in R$ 使得对任意 $a \in R$ 有 $0 + a = a$

  (c) **负元:** 对任意 $a \in R$, 存在 $a' \in R$ 使得 $a' + a = 0$, 记 a' 为 $-a$

  (d) **交换律 commutativity:** $a + b = b + a$

(ii) R 除了 0 关于乘法 $\cdot$ 构成一个交换的**幺半群 monoid** $R^\times = R - \{0\}$, 即:

  (a) **结合律 associativity:** 任意 $a, b, c \in R$ 有 $a(bc) = (ab)c$

  (b) **单位元 identity:** 存在 $1 \in R$ 使得对任意非 0 元 $a \in R$ 有 $1a = a$

  (c) **逆元 unit:** 对任意非 0 元 $a \in R$, 存在 $a' \in R$ 使得 $a'a = 1$, 记 a' 为 a^{-1}

  (d) **交换律 commutativity:** $ab = ba$

(iii) **分配律 distributivity:** 任意 $a, b, c \in R$ 有 $a(b + c) = ab + ac$, $(b + c)a = ba + ca$

我们如此略微繁琐地定义, 是为了后面阐述不交换的环. 这里需要补充的是, 如果循之根本, 环的定义不仅可以刨除乘法的交换性, 甚至可以刨除掉单位元的存在性. 只是如若刨除得过多, 则代数结构会变得模糊不清, 当谈论到环的时候, 我们一般讨论的还是性质比较好的环.

Definition 2.1.2. 域 field F 指的是一个配备了两种二元代数运算的集合, 分别称其为加法 $+$ 和乘法 $\cdot$. 满足如下的运算法则:

(i) F 关于加法 $+$ 构成一个 **Abel 群**F^+, 即:

(a) **结合律 associativity:** 任意 $a,b,c\in F$ 有 $a+(b+c)=(a+b)+c$

(b) **0 元 element 0:** 存在 $0\in F$ 使得对任意 $a\in F$ 有 $0+a=a$

(c) **负元:** 对任意 $a\in F$, 存在 $a'\in F$ 使得 $a'+a=0$, 记 a' 为 $-a$

(d) **交换律 commutativity:** $a+b=b+a$

(ii) F 除了 0 关于乘法 $\cdot$ 亦构成一个 Abel 群 $F^\times=F-\{0\}$, 即:

(a) **结合律 associativity:** 任意 $a,b,c\in F$ 有 $a(bc)=(ab)c$

(b) **单位元 identity:** 存在 $1\in F$ 使得对任意非 0 元 $a\in F$ 有 $1a=a$

(c) **逆元 unit:** 对任意非 0 元 $a\in F$, 存在 $a'\in R$ 使得 $a'a=1$, 记 a' 为 a^{-1}

(d) **交换律 commutativity:** $ab=ba$

(iii) **分配律 distributivity:** 任意 $a,b,c\in F$ 有 $a(b+c)=ab+ac$, $(b+c)a=ba+ca$

实际上域就是每个非 0 元皆可逆的交换环.

我们在定义矩阵之前曾简略地谈过域的概念, 彼时我们主要谈的是数域. 因此我们所能够面对的基本上无外乎 $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, 即复数域的子域. 但, 对于代数所要面临的问题而言, 数域显得有些贫瘠了. 分析学将目光集中在实数域上研究数学分析, (因为实数域是能够保持完备性的最小的数域, 而一旦没有完备性, 极限都无法被谈论; 与之相对的, 实变函数实际内容远远超出了对其名字的想象, 实变函数则是谈论更广的积分理论, 对 L^p 空间的研究比对实线性空间的研究要意义得多), 将目光集中在复数域上研究复变函数.

代数则不应该用数域来限制住自己, 就像我们如果要谈论一元多项式是否可约的问题, 对于有理数域只有一个必要条件的 **Eisenstein** 判别法; 对于实数域则只有判别式小于 0 的部分二次多项式和所有线性多项式; 对于复数域则由**代数学基本定理**可知, 当且仅当其为线性多项式. 如果我们把目标放得小一些, 我们仅仅需要一部分多项式可分解为线性多项式的乘积时, 是否还一定需要 $\mathbb{C}$ 这么大的数域?

我们接下来通过一个简单的例子来了解这一 "扩域" 的思想, 这一思想直接引导 Abel 对五次方程求根公式不存在性的证明, 更是直接让 Galois 将这一现象的代数结构剖析得 "明明白白". 在此之前我们先回忆一下多项式的两个定理.

Theorem 2.1.2. Eisenstein 判别法设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in\mathbb{Z}[x]$, 其中 $a_n\neq0$ 且 $n\geq1$. 若存在素数 p 使得:

1. $p\mid a_i$, 对于 $i=0,1,\cdots,n-1$;
2. $p\nmid a_n$;
3. $p^2\nmid a_0$.

则 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约.

Theorem 2.1.3. 代数学基本定理 每个次数 $n \geq 1$ 的复系数多项式 $P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$, 其中 $a_n \neq 0$,在复数域 $\mathbb{C}$ 中至少有一个根.

因此通过归纳, 每个 n 次复系数多项式在复数域 $\mathbb{C}$ 上可以分解为 n 个一次因式的乘积, 即

$$P(z) = a_n(z - r_1)(z - r_2)\cdots(z - r_n)$$

其中 $r_1, r_2, \cdots, r_n \in \mathbb{C}$ 是 $P(z)$ 的根 (可能有重复).

Example 2.1.1. 考虑 $f(x) = x^2 - 2$. 我们接下来来分析它的根的存在性, 等价地, 分析它是否能够被分解成线性函数的乘积.

1. 在 $\mathbb{Q}$ 上. 由 Eisenstein 判别法, 我们取 $p = 2$, 则满足三个条件, 因此 $f(x)$ 在 $\mathbb{Q}$ 上不可约. 又因为 $deg(f) = 2$, 可知 f 在 $\mathbb{Q}$ 中无根.
2. 在 $\mathbb{R}$ 上. $f(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.
3. 在 $\mathbb{C}$ 上. 由代数基本定理, 任意多项式的所有根都落在其中, 多项式亦可写成 $deg(f)$ 个线性多项式的乘积.

可是 $\mathbb{R}$ 比起 $\mathbb{Q}$ 显得太大了. 如果一个集合可以与自然数集 $\mathbb{N}$ 之间建立一个 1-1 映射, 则我们称它是**可数的**, 反之则称为不可数. 因为有理数从某个角度来看不过是整数对, $\mathbb{Q}$ 是可数的; 而通过构造 Cantor 对角线, 我们可以让无理数等价的无穷小数永远都无法排序, $\mathbb{R}$ 是不可数的.

于是乎, 新的问题就这么诞生了. 如何去寻找介于 $\mathbb{Q}$ 和 $\mathbb{R}$ 之间的一个域 k, 使得 $f(x)$ 的所有根 $Kerf^\flat := \{a \in \mathbb{R} : f(a) = 0\}$ 都被置于此域中呢? 换言之, 我们要寻找一个域 k 使得 $\mathbb{Q} \subset Kerf^\flat \subset k \subset \mathbb{R}$.

我们的方法如下.

首先我们知道, 由代数基本定理, 任意多项式的所有根都落在其中. 不计重数的话, 根的个数与多项式的次数相等. 因此, 凡是复数域上的多项式, 无论是有理系数多项式, 实系数多项式, 皆可在 $\mathbb{C}$ 中找到它的根. 对应 $f(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ 在 $\mathbb{C}$ 中的根为 $x_{1,2} = \pm\sqrt{2}$.

接下来, 我们尝试将 $\pm\sqrt{2}$ 添加进 $\mathbb{Q}$ 中. 记 $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. 读者可自行验证 $\mathbb{Q}(\sqrt{2})$ 是一个域.

于是 $\mathbb{Q}(\sqrt{2})$ 囊括了 $f(x)$ 的所有根, 已经达到了我们的要求. 我们还能证明它一定是包含 $Kerf^\flat$ 和有理数域的最小域. 即, 任取域 $K \supset Kerf^\flat \cup \mathbb{Q}$, 我们证明 $K \supset \mathbb{Q}(\sqrt{2})$. 由 $\mathbb{Q}(\sqrt{2})$ 的定义, 这是显然的.

我们继续观察 $\mathbb{Q}(\sqrt{2})$ 的结构, 它似乎与 $\mathbb{C}$ 的结构有些相似, 而复数域从某种意义上正是在实数轴外增加了一条虚数轴得到的, 那么是否 $\mathbb{Q}(\sqrt{2})$ 也具备着这种结构, 我们在有理数轴之外, 增添了一条 $\sqrt{2}$ 的轴?

事实上, $\mathbb{Q}(\sqrt{2})$ 具备一定的线性结构, 它是一个 $\mathbb{Q}$ 上的 2 维线性空间, 它的一组基为 $1, \sqrt{2}$.

Exercise 2.1. 设 k 为域, $f(x) \in k[x]$ 且 $deg(f) = 2$ 或 3, 证明 f 不可约当且仅当 f 在 k 中无根.

Exercise 2.2. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ 是一个域.

Exercise 2.3. $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} : a, b \in \mathbb{Q}\}$ 是一个域吗? 尝试改进条件让它成为一个域, 并尝试让它变成一个域.

Definition 2.1.3. 设 K, k 为域, 如果 $k \subset K$ 并且 K 中的单位元 $1 \in k$, 则此时 k 是 K 的一个子域, 我们称 K 为 k 的一个**扩张域 extension field**, 并记为

$$K/k$$

.

在扩张域 K/k 中, 如果对一个元素 $\alpha \in K$ 存在一个非零多项式 $f(x) \in k[x]$ 使得 $f(\alpha) = 0$, 则我们称 α 在域 k 上是**代数的 algebraic**; 反之, 我们称 α 在域 k 上是**超越的 transcendental**.

如果 K 中的每一个元素 α 都是代数的, 则我们称扩张域 K/k 是**代数的 algebraic**.

如果对于一个域 k, 其上的多项式环 $k[x]$ 中的每一个非常数多项式 $f(x) \in k[x]$, $f(x)$ 都至少在 k 中有一个根, 则我们称 k 是一个**代数闭域 algebraic closed field**.

如果一个域已经是一个代数闭域, 例如 $\mathbb{C}$, 我们就无需去寻找它的扩张.

在分析学中, 我们要求实数系具有完备性, 这样我们能够保证其上每一个 "具有收敛倾向" 的序列 (即 Cauchy 列) 都收敛于其中某一个点上. 这个性质几乎成了分析中必备的基础, 因此我们转而去寻找实数系的子集中, 是否有一类具备此种性质的集合, 于是我们找到了闭集. 这也是为什么我们几乎所有有关实数完备性的定理都是落在闭域 (闭区间) 上的. 假如这种性质没办法得到保证, 则我们就要去寻求一个空间的完备化. 正是出于这种需要, 我们从有理数构造出了具有完备性的实数系.

在后续, 我们会用一种非常代数的方式构造出实数系. 公理化的构造几乎都是比较代数的, 甚至是比较集合论的, 因为没有公理化的定义, 就没有分析和计算的空间, 代数结构本身就是为了提供运算规律的. 在此层意义下, 基础的集合论, 代数, 拓扑学以及数学分析甚至不过是一种语言罢了.

如果一个数在 $\mathbb{Q}$ 上是代数的, 我们称其为**代数数**; 反之, 称其为**超越数**. Galois 理论甚至能够证明 π 和 e 是超越数.

Galois 正是用这种语言, 将理论的基础直接扎根于域论之中, 如你所见, 根式解就这么悄无声息地嵌入了域的扩张之中.

Galois 更为惊人的是, 构建了 Galois 群的概念, 他想让一个扩张域中原先的域在某种变换中保持不变, 而让扩张出来的那些空间, 那些多项式不可分解的空间进行变换. 而求根公式的对称性就蕴藏在这些变换之中, Galois 证明了域扩张和 Galois 群之间的

对应关系, 最后证明了一般求根公式对应的域扩张所对应的 Galois 群为 S_n, 这个群在 $n \geq 5$ 时是不可解群, 正是这种不可解性导致了它无法生成根式解.

其中诸多理论不是 Galois 那个时代的产物, 他也并非像如今教学般的一个定义一个定义地推进构建出理论来, 要知道, 他那个年代可没有后来代数学家注意到的 $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$ 这样的结构. 可以说, 如今学习的 Galois 理论已经几乎不算是 Galois 的理论, 他的前辈们只有些许的尝试, 而他甚至还没有来得及接受前辈们的指导: 考试落榜, 不得已考入一所师范院校 (后来巴黎高等师范学院); 撰写论文投稿, 因为内容太抽象被拒绝, 这样的事发生了三次; 参与政治活动被捕, 事业失业时情感破裂, 在失魂落魄的时候去与军人决斗; 决斗的前一晚写尽了自己一生的研究, 字里行间还塞着 "我没有时间了", 就这样倒在了自己的 21 岁上.

Galois 的法语论文最近几年被发布了出来, 也有英语的版本, 只有寥寥 9 页 (也不能怪法国科学院的).

无独有偶的是, 同样的年少天才, 同样的论文做出绝世成果却不受重视, Abel 也倒在了 27 岁的寒夜中, 穷困潦倒.

值此时机, 有一言赠与读者.

不要让直觉被域框住, 我的意思是, 不要让理想被置于平凡.

你会明白这句话的意思的.

2.2 近世代数: 对数学本原结构的同构

时间终于离我们稍近了一点, 大约在两百年以内了. 我们先前说到 Galois 在研究五次方程的求根公式的过程中构造了群这一结构, 并且通过研究域的结构完完整整地破解了五次乃至更高次方程的求根公式. 因此, 我们可以认为从 Galois 开始, 抽象代数真正地得以建立起来.

当然, 这是一个漫长的过程, 经历了无数代数学家的工作, 让 Galois 理论的书籍从原先的 9 页逐步增厚成如今的教科书.

数学家们研究具体的问题, 从中发现或者建造了一些结构, 以帮助他们攀登摘取顶上的甜美果实. 但时间有限, 生命有限, 攀登的依仗往往是脆弱甚至一次性的, 但足够指明可行之路. 后面的数学家为了让楼房建造起来, 让高楼变成地基, 寻着先人的道路建造起完美而又健壮的代数结构来. 他们环绕四周, 因为地基平稳, 可以尽情地眺望而不用担心危险, 他们能够发现比那颗果实更广袤的世界, 有人继续铤而走险, 也有人潜心构建, 这才成就了我们手中的书籍, 一座巴别塔.

Galois 理论是条漫长的道路, 代数更是旅行半生都不一定能看到什么美妙画面的地方. 因此, 在跟着数学家们上楼梯记忆路线之前, 不妨让我们来一趟旅游路线的大巴, 不同于先前的热气球, 我们是顺着路线走的.

2.2.1 等价关系和集合的划分

下面给出的等价关系可以建立代数中重要的等价类与商集概念.

Definition 2.2.1. 如果集合 S是它的一些非空子集的并集, 其中每两个不相等的子集不相交, 那么把这些子集组成的集合称为S的一个**划分**.

Example 2.2.1. 日历与同模关系

想象以下我们的日历表, 如果今天是星期一, 那么每过7天都将是星期一. 用数学的语言来说, 就是假设我们日历中的每一天对应着一个正整数, 且0对应星期日, 则每个除以7余1的日子就是星期一.

用数学的符号来说,说 a 对 7 同模余于 b, 记作

$$a \mod 7 = b \mod 7 \Leftrightarrow a \equiv b \pmod 7 \Leftrightarrow a - b \equiv 0 \pmod 7$$

$$a \equiv b \pmod 7 \Leftrightarrow (a,b) \in \bigcup_{i=0}^{6} (H_i \times H_i)$$

这一例子由星期 (同模) 这一关系诱导出了日历的划分 (同余类), 这暗示我们应当去寻找这一关系的特殊性.

Definition 2.2.2. 设 S 是一个非空集合,我们把$S \times S$的一个非空子集W 叫做S 上的一个 **二元关系**; 如果$(a,b) \in W$, 那么称 a 与b 有 W 关系,记作 $aWb\,(a \sim b)$.

集合 S 上的一个二元关系被称作**等价关系**, 如果它具有下列性质:

i. **反射性:** $a \backsim a, \forall a \in S$.

ii. **对称性:** 若 $a \backsim b$, 则$b \backsim a$.

iii. **传递性:** 若 $a \backsim b$, 且$b \backsim c$, 则$a \backsim c$.

那么称它是一个等价关系.

可以很自然地验证同余关系是一个等价关系.

Definition 2.2.3. 设"$\sim$"是集合S上的一个等价关系. 任取 $a \in S$, 令$[a] := \{x \in S : x \sim a\}$ 称所定义的 $[a]$ 为S对于关系 "$\sim$" 关于 a 的一个等价类. 即 $x \in [a] \Leftrightarrow x \sim a$.

如果$a \in [a]$, 称 a 为等价类 $[a]$ 的一个代表 (不唯一).

有了这些定义之后我们可以更加 "数学地" 考虑星期问题, 也就是模算数中的同余问题. 在初步的代数学学习中, 我们所接触到的群环域都可以由此展开, 因此是需要注意的重点课题.

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z} : x \equiv 0 \pmod 7\},\\
[1] &= \{x \in \mathbb{Z} : x \equiv 1 \pmod 7\},\\
&\cdots\\
[6] &= \{x \in \mathbb{Z} : x \equiv 6 \pmod 7\}.
\end{aligned}$$

他们都叫做模7剩余类, 而 $\{[0],[1],\cdots,[6]\}$ 是 $\mathbb{Z}$ 的一个划分.

Proposition 2.2.1. 设$\sim$是集合 S 上的一个等价关系, 则 $[a]=[b]\Leftrightarrow a\sim b$.

Proof. $\Rightarrow$: 由定义, $a\in[a]=[b]\Rightarrow a\sim b$.

$\Leftarrow$: $\forall x\in[a], x\sim a$ 由等价关系的传递性结合条件, 可得 $x\backsim b$ 即证明了$[a]\subset[b]$. 另一个方向同理. □

Proposition 2.2.2. 设 $\sim$ 是集合 S 上的一个等价关系, 若 $[a]\neq[b]$, 则 $[a]\cap[b]=\varnothing$.

Proof. 采用反证法,假设$\exists x\in[a]\cap[b]$, 则$x\sim a, x\sim b$ 再由等价关系的传递性, 得到矛盾. □

上述的两个似乎显然的命题仅仅是一个集合论关系的练手, 更重要的是, 他们可以很简单地得到下述定理的证明.

Theorem 2.2.1. 若集合S上有一个等价关系 $\sim$, 则所有等价类组成的集合是 S 的一个划分.

Exercise 2.4. 证明上述定理.

这理清了我们对于集合划分的一个惯性思路: 找到一个合适的等价关系, 通过等价关系构造等价类, 进而形成集合的一个划分.

下面的命题告诉我们, 反过来也是正确的.

Proposition 2.2.3. 设 $\Gamma=\{\omega_1,\cdots,\omega_n\}$ 为集合S的一个划分, 则存在一个等价关系 $\sim$, 使得 Γ 由它的所有等价类组成.

Proof. 我们很自然地可以给出这一关系的形式:

$$a\sim b\Leftrightarrow a,b\in\omega_i,\forall i\in\{1,\cdots,n\}$$

容易验证这是一个等价关系, 并且划分与等价类是一样的. □

Exercise 2.5. 补全上述定理的证明.

给出了集合的划分, 我们就很容易定义商集, 商集就是等价类的集族.

Definition 2.2.4. 商集

设 $\sim$ 是集合 S 上的一个等价关系, 则所有等价类组成的集合成为 S 对于 $\sim$ 的商集, 记作 $S/\sim$.

当然,它是集合S的一个划分.

下面我们介绍等价类的一大作用, 我们将用有理数列的 Cauchy 列构造等价类, 进而构建实数系.

读者是否还记得我们先前曾写下 $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$ 的构造? 事实上, 用代数的方法公理化地构造数集, 对于建造一套合理的数学系统具备着重要的意义. 在数学分析课本上, 大部分书籍是通过定义实数为无穷小数来进行的, 为了规避后续的麻烦, 仅仅是用无穷小数的方法来证明确界原理, 进而实数的完备性都是等价的. 但是这种处理方式有一个最大的问题, 无穷小数的运算并不像看起来那么显然, 很多书本也几乎是搪塞着过去的, 这也是为什么后续从未再提过这回事的一大原因. 除此之外很多书籍或许会在附录里放着实数的 Dedkind分割构造法, 这个方法又过于冗长, 涉及太多集合论和公理化的手段. 而在定义了极限和 Cauchy 列之后, 用 Cantor 基本列 (Cauchy 列) 来构造实数, 不失为一种有趣的好方法.

作为预备, 我们先保持有理数域 $\mathbb{Q}$ 上的四则运算, 序型 (即大小关系), 以及度量 (即距离定义).

目标: 实数系

我们需要构建出的实数系必须具备以下三个性质.

域公理: 实数系是一个域.

序公理: 实数系是一个全序集, 并循域的运算具备不等式的性质. 即

1. **三歧性**: 对于任意两个实数 a 和 b, 以下三种关系恰好有一种成立: $a < b$, $a = b$, $a > b$.
2. **传递性**: 如果 $a < b$, $b < c$ 则 $a < c$.
3. **加法保序性**: 如果 $a < b$ 则 $a + c < b + c$.
4. **乘法保序性**: 如果 $a < b$, $c > 0$ 则 $ac < bc$.

完备性公理: 确界原理.

Step 1: 构建 Cauchy 列

我们将极限的叙述由 "任取一个正实数 ε" 改为 "任取一个正整数 k, 记 $\varepsilon = 1/k$", 由有理数的稠密性, 这两者是等价的. 我们借此定义有理数域上的 Cauchy 列 $\{a_n\} \subset \mathbb{Q}$: 任取一个正整数 k, 记 $\varepsilon = 1/k$, 存在 $N \in \mathbb{N}^+$ 使得当 $n, m \geq N$ 时, $|a_n - a_m| < 1/k$. 这样我们就能够保证运算都还保持在有理数上.

记有理数系上的所有 Cauchy 列为

$$\mathcal{C} := \{a_n : \{a_n\}\text{为 Cauchy 列}\}$$

Step 2: 定义等价关系

我们于 Cauchy 列族 $\mathcal{C}$ 上定义等价关系 $\sim$ 如下:

$$\{a_n\} \sim \{b_n\} \Leftrightarrow \lim_{n\to\infty}(a_n - b_n) = 0$$

遵循我们先前对 Cauchy 列定义的修改, 这里的 $\lim_{n\to\infty}(a_n - b_n) = 0$ 指的是: 任取一个正整数 k, 记 $\varepsilon = 1/k$, 存在 $N \in \mathbb{N}^+$ 使得当 $n, m \geq N$ 时, $|a_n - b_n| < 1/k$.

我们可以验证这是一个等价关系. 反身性和对称性显然, 传递性由三角不等式即可得到.

Step 3: 构造商集

有了等价关系, 我们可以循此构造出商集

$$\mathbb{R} = \mathcal{C}/\sim = \{[a_n], [b_n], \cdots\}$$

这一步的想法是非常自然的. 我们先前已经了解, 有理数域的最大弊端就在于极限并不封闭, 而为了让极限封闭, 我们将其完备化. 原本的有理数域虽然看着非常稠密, 但是实际上每个有理数之间都满是空洞, 一个序列非常容易就会朝着空洞不断地前进, 因此我们就要填上这个空洞. 就像我们在构造扩张域时, 我们会将多项式的根拿到域里面构造出一个包含这些元素最小的域, 我们现在正是把这些极限都拿进有理数里, 构造出最小的完备域.

Step 4: 构造域结构

构造域结构, 无非就是构造运算. 令 $\alpha = [\{a_n\}] \in \mathbb{R}$, $\beta = [\{b_n\}] \in \mathbb{R}$, $\alpha' = [\{a'_n\}] \in \mathbb{R}$, $\beta' = [\{b'_n\}] \in \mathbb{R}$.

$+$:

$$\alpha + \beta := [\{a_n + b_n\}]$$

不难看出加法是封闭的.

首先验证运算 (映射) 是良定的, 即设 $\alpha = \alpha'$, $\beta = \beta'$, 验证 $\alpha + \beta = \alpha' + \beta'$.

由 $\alpha = \alpha'$, $\beta = \beta'$, 可知 $\lim_{n\to\infty}(a_n - a'_n) = \lim_{n\to\infty}(b_n - b'_n) = 0$ 因而 $\lim_{n\to\infty}(a_n + b_n - (a'_n + b'_n)) = 0$ 于是说明了 $\alpha + \beta = \alpha' + \beta'$.

其次我们验证域关于加法的其他运算法则. 0 元我们设为 $\theta := [\{0, 0, \cdots, 0, \cdots\}]$ 其他的皆可容易验证.

$\times$:

$$\alpha \cdot \beta := [\{a_n \cdot b_n\}]$$

不难看出乘法的封闭性, 只需要借助到 Cauchy 列的有界性即可.

良定性由 $\lim_{n\to\infty}(a_n b_n - a'_n b'_n) = 0$ 可知, 其不过是数学分析的简单语言罢了. 单位元我们自然设为 $\iota := [\{1, 1, \cdots, 1, \cdots\}]$.

逆元我们并不是那么容易设定, 需要借助到 Cauchy 列的基本性质: Cauchy 列是必定有界的, 因此序列中的数都是可以给定的, 并且如果 *Cauchy* 列趋向于 0 的话, 那么它就属于 θ, 一个非 0 的元素中的每个序列, 对于任意一个误差, 必能找到一个项, 使它之后的项都始终与 0 保持在这个误差之外. 因此, 一个非 0 项 $\alpha = [\{a_n\}]$, 它的逆元可以定义为 $\alpha^{-1} := [\{s_n\}]$ 其中当 $a_n \neq 0$ 时 $s_n = a_n^{-1}$, 当 $a_n = 0$ 时 $s_n = 0$.

除此之外的其他的皆可容易验证, 不过是极限的四则运算性罢了.

Step 5: 构造序结构

首先定义正性: $\alpha > 0$ 当且仅当: 存在一个正整数 k, 存在 $N \in \mathbb{N}^+$ 使得当 $n > N$ 时, $a_n > 1/k$.

定义序关系为

$$\alpha > \beta \Leftrightarrow \alpha - \beta > 0$$

容易验证其满足序公理.

Step 6: 实数完备性

此处我们证明确界原理, 即最小上界的存在性. 思路是通过阿基米德性, 构造出一个 "实数" 的最小上界. 此处过程比较麻烦, 略.

Step 7: 有理数域的嵌入

并且, 我们可以构建映射 $\mathbb{Q} \to \mathbb{R}$ 使得 $q \mapsto [\{q, q, \cdots, q, \cdots\}]$, 这是一个单射. 于是 $\mathbb{Q}$ 嵌入 $\mathbb{R}$ 中成为其子域.

不难证明这样的嵌入也是保持有理数域上的序结构和域性质.

于是证明完毕.

2.2.2 群环域

2.2.3 同态和同构

2.3 前沿代数学简介

2.3.1 代数几何简介

Vakil 有一本非常著名的 notes, 现在广泛地被很多数学生用来学习代数几何, 比起传统的类似于 GTM 52 (Hartshorn) 这样的书, 这本未出版的笔记更加易于上手. 它的名字叫做《The Rising Sea : Foudations of Algebraic Geometry》. 书的标题源自于现代代数几何的开创者 Gronthendick 在他的自传《Harvest and Planting》 (原文毫无疑问是法文) 中所提到的一个比喻.

> (翻译含义参考 deepseek R1)
>
> I can illustrate the second approach with the same image of a nut to be opened.
>
> 我可以用同样的坚果意象来说明第二种方法:
>
> The first analogy that came to my mind is of immersing the nut in some softening liquid, and why not simply water? From time to time you rub so the liquid penetrates better, and otherwise you let time pass. The shell becomes more flexible through weeks and months - when the time is ripe, hand pressure is enough, the shell opens like a perfectly ripened avocado!
>
> 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!
>
> A different image came to me a few weeks ago.
>
> 几周前, 我的脑海中闪现了另一幅图像.
>
> The unknown thing to be known appeared to me as some stretch of earth or hard marl, resisting penetration... the sea advances insensibly in silence, nothing seems to happen, nothing moves, the water is so far off you hardly hear it... yet it finally surrounds the resistant substance.
>
> 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.

Gronthendick 认为, 学习乃至研究的过程有两种. 一种是对着最艰难的部分握紧镐子拼了命地凿; 另一种就是干脆让自己的海平面不断地升高——海洋是自然存在的, 不

需要被发明, 我们只是发现了潮水自然在时间的推动中将岸边的礁石腐蚀得布满空洞这一对海洋而言再自然不过的现象罢了.....海洋当然不是为了腐蚀这礁石而存在的, 这浸入, 不过是顺便的罢了.