近世代数讲义

胡维

2026/07/04

WeMath **微信公众号**

目录

1 缘起：从方程到 Galois 理论

前言

时间过得真快，这个近世代数讲义上次是 2020 年秋完成的，其中不完善的地方长期没有得到修正和更新．最近发现很多同学在阅读 2020 年版的讲义，我想借本学期上《近世代数》的机会对讲义进行修订．

本讲义是 2020 年版在线讲义基础上的修订．我们将在微信公众号的合集中逐步替换原有内容．

顾名思义，近世代数讲的是发生在相对比较近代的代数故事．当然，由于咱们的教科书动不动就讲这个理论两千年以前就有人知道了，我们现在讲的近世代数的故事就相对来说比较近，其绚丽的开端大致在 200 年以前，并戏剧性的改变了代数以及数学的面貌．可以说，如果没有 200 年前那灿烂的绽放，就没有我们今天的电脑，手机，4G，5G，也就没有咱们的 WeMath 公众号．

缘起：解代数方程

请原谅我还是要将这个故事扯到两千年前．在人类的历史变迁中，可以说长期与方程斗智斗勇．对于线性方程组，中国人在《九章算术》里就给出了加减消元的解法，可以说是被人类轻松“碾压”．

但还有一类方程，人类到目前为止都不能说是完整的战胜，它就是“代数方程”，即为

$$f(x)=0$$

形式的方程，其中 $f(x)$ 是一个关于 x 的多项式．不服气的话，大家可以试试

$$x^5-x+1=0,$$

看看能不能在“有生之年”找到它在复数 $\mathbb{C}$ 内的精确解 (游戏规则：不能用级数或者极限来表示!)．

为了简便起见，本节的多项式都是有理数作为系数的多项式．

当然有人会说，我们有代数学基本定理，$f(x)$ 在 $\mathbb{C}[x]$ 可以分成一次因式的乘积，就像这样

$$f(x)=a(x-c_1)^{n_1}\cdots(x-c_r)^{n_r}$$

其中 $c_1,\cdots,c_r$ 都是复数，它们恰为 $f(x)=0$ 在 $\mathbb{C}$ 中的根．但如果要让你告诉我这些 c_1 到 c_r 都等于多少呀？是不是就傻眼了!

对于二次的代数方程 $x^2+bx+c=0$，如果不考虑负数开平方根的问题的话，这个方程也早已被人类征服，它的根是

$$x=\frac{-b\pm\sqrt{b^2-4c}}{2}$$

而三次和四次代数方程却直到 16 世纪才被人类搞定，其大体的传说如下：

> 1515 del Ferro 首先发现了一类三次方程的解法，但没有公开，只是临死前告诉了他的学生 Antonio Fior
>
> 1535 Fontana(江湖人称 Tartaglia) 重新发现了三次方程的解法，并赢得了 Fior 的挑战．Cardano 向 Tartaglia 求解法，在 Cardano 发誓保守这个秘密后获得了三次方程解法．
>
> 1545 后来 Cardano 发现了 del Ferro 原来已经知道三次方程的解法了，觉得这个不再是秘密，公开也不算违背誓言，于是在他的书《Ars Magna》中公开了这个解法
>
> Cardano 的学生 Ferrari 更是在这个基础上找到了 4 次方程的解法
>
> 据说 Tartaglia 非常生气，向 Cardano 发起挑战，但 Cardano 拒绝了他．Ferrari 迎接了 Tartaglia 挑战，并且战胜了他!

三次方程

$$x^3+ax^2+bx+c=0$$

总可以通过用 $x-a/3$ 替换 x 将方程化为

$$x^3+px+q=0$$

的形式．如果

$$4p^3+27q^2\geqslant 0,$$

此时方程的一个根是

$$\sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}$$

这里大家发现，它们的根都是方程的系数经过加、减、乘、除以及开若干次方得到，我们把这些运算统一称为代数运算，于是大家都“脑 (zi) 洞 (ran) 大 (er) 开 (ran)”的问：

问题 1. 对于有理系数多项式 $f(x)$, 其在 $\mathbb{C}$ 中的根是否都可以通过它的系数, 经过有限次的代数运算得到?

或者更大胆的问

问题 2. 对一般的 n 次有理系数多项式 $f(x)$, $f(x)=0$ 的根是否有统一的求根公式, 而这个公式的表达式中只有其系数的有限次代数运算?

在 Ferrari 找到 4 次代数方程的解法以后, 很多数学家都致力于寻找 5 次以上代数方程的求根公式. 出于信仰, 大家都相信

这个公式一定是存在的!

其中, 我们亲爱的 Lagrange(拉格朗日) 同学做了特别辛苦的努力.

拉格朗日的努力

拉格朗日先生 (1736-1813) 发现了一件很酷的事情. 对于 3 次代数方程

$$x^3+px+q=0$$

来说, 假设它的三个根为 x_1,x_2,x_3.

如果我们不着急直接求出这三个根, 而是 "曲线救国": 令

$$\omega=\frac{-1+\sqrt{3}\,\mathrm{i}}{2}$$

$$y_1=(x_1+\omega x_2+\omega^2x_3)^3$$
$$y_2=(x_1+\omega^2x_2+\omega x_3)^3$$

这里从 y_1 出发置换 x_1,x_2,x_3 的位置可能得到的多项式只有 y_1,y_2. 因此 y_1+y_2 和 y_1y_2 都在 x_1,x_2,x_3 的置换下不动, 是关于 x_1,x_2,x_3 的对称多项式. 利用根与系数关系, 如果你足够耐心的话, 你会发现

$$y_1+y_2=-27q$$
$$y_1y_2=-27p^3$$

因此, y_1,y_2 就是关于 y 的方程

$$y^2+27qy-27p^3=0$$

的两个根, 也就是说你可以先通过求一个 2 次方程求出 y_1 和 y_2, 然后用

$$\frac{\sqrt[3]{y_1}+\sqrt[3]{y_2}}{3}$$

求原方程的根, 这里 $\sqrt[3]{y_1}$ 和 $\sqrt[3]{y_2}$ 的取值满足:

$$\sqrt[3]{y_1}\cdot\sqrt[3]{y_2}=-3p$$

更酷的是, 他发现 4 次方程居然也可以这么干! 具体来说, 对于 4 次方程

$$x^4+ax^3+bx^2+cx+d=0$$

来说, 首先, 我们也可以将 x 替换成 $x-a/4$ 的话, 就可以消掉 x^3 项, 让方程变为

$$x^4+qx^2+rx+s=0$$

的形式.

假设它在 $\mathbb{C}$ 中的四个根为 x_1,x_2,x_3,x_4. 拉格朗日同学发现下面的 y_1,y_2,y_3

$$y_1=(x_1+x_2)(x_3+x_4)$$
$$y_2=(x_1+x_3)(x_2+x_4)$$
$$y_3=(x_1+x_4)(x_2+x_3)$$

是关于 y 的三次方程

$$y^3-2qy^2+(q^2-4s)y+r^2=0$$

的根 (跟上面一样, y_1,y_2,y_3 是从 y_1 出发置换 x_i 的位置能产生的所有不同的多项式). 先解这个三次方程, 求出 y_1,y_2,y_3, 然后再利用上面的三个等式去求出 x_1,x_2,x_3,x_4. 由

$$x_1+x_2+x_3+x_4=0$$
$$(x_1+x_2)(x_3+x_4)=y_1$$

可知

$$x_1+x_2 \text{ 和 } x_3+x_4$$

是关于 t 的二次方程

$$t^2+y_1=0$$

的根. 因此, 可假设

$$x_1+x_2=\sqrt{-y_1} \text{ 和 } x_3+x_4=-\sqrt{-y_1}$$

类似的有

$$x_1+x_3=\sqrt{-y_2} \text{ 和 } x_2+x_4=-\sqrt{-y_2}$$
$$x_1+x_4=\sqrt{-y_3} \text{ 和 } x_2+x_3=-\sqrt{-y_3}$$

这里需要注意的是, 通过计算可以发现, 由根与系数关系, 这里平方根的取值需要满足

$$\sqrt{-y_1}\cdot\sqrt{-y_2}\cdot\sqrt{-y_3}=-r.$$

根据这些平方根的取值可得原方程的解

$$x_1=\frac{\sqrt{-y_1}+\sqrt{-y_2}+\sqrt{-y_3}}{2}$$

$$x_2=\frac{\sqrt{-y_1}-\sqrt{-y_2}-\sqrt{-y_3}}{2}$$

$$x_3=\frac{\sqrt{-y_2}-\sqrt{-y_1}-\sqrt{-y_3}}{2}$$

$$x_4=\frac{\sqrt{-y_3}-\sqrt{-y_1}-\sqrt{-y_2}}{2}.$$

所以拉格朗日的想法是:

> 对于一个 n 次代数方程,能不能通过先解一个 $n-1$ 次方程 (称为原方程的一个预解式),然后利用这个 $n-1$ 次方程的根去求原来那个 n 次方程的根?

令人无比可惜的是,对一般的 5 次方程,拉格朗日怎么也找不到 4 次的预解式. 因此,拉格朗日怀疑 5 次以上的代数方程可能没有根式解公式.

Abel-Ruffini 定理

Ruffini 就在 1799 年率先表示一般 5 次以上的代数方程不 (im) 可 (possi) 能 (ble)有根式解公式 (问题2所要求的)! 但很快大家发现他的证明有严重的漏洞!

Abel(1802-1829)

20 多年后,年轻的 Abel(1802-1829) 完整的证明了这个结论,也就是

定理 1.1 **Abel-Ruffini 定理.** 一般的 $n \geqslant 5$ 次代数方程没有问题2所要求的根式解公式.

实际上 Abel 对问题1也进行了更多的讨论,也是就是虽然没有求根公式,但某些具体的高次方程的根还是可以由有理数经过代数运算得到的,比如 $x^5 = 2$.

Abel 这些内容都公开的发表在最早的数学杂志 crelle 上,也正好是发表在 crelle 的第一期. 其中,证明五次以上代数方程没有统一的求根公式就是下面这篇

> Abel, N. H. , Beweis der Unmöglichkeit, algebraische Gleichungen von höheren Graden als dem vierten allgemein aufzulösen. Crelle 1 (**1826**), 65–84.

题目点对点翻译下:

- Beweis(证明)
- Unmöglichkeit(不可能性)
- algebraische Gleichungen(代数方程)
- höheren Graden als dem vierten(高于五次)
- allgemein aufzulösen (一般解法)

如果大家感兴趣,而你的大学又买了在线期刊,你还可以在网上查到这篇论文,它是由德语写的,虽然 Abel 是挪威人.

20 岁 Galois 的刹那芳华

也是在那个年月里,更年轻的Galois(中文名: 伽罗瓦) (1811-1832),受拉格朗日想法的启发,创造性地引入了改变数学历史进程的一个概念: 群. (见下期)

Galois(1811-1832)

比较简单的群的例子是 $\{1, 2, \cdots, n\}$ 这个集合到自身的一一映射的全体 S_n, 实际上就是 1 到 n 的所有排列的全体,有 $n!$ 个元素.

给定任意一个有理系数多项式 $f(x)$, Galois 的办法是:

他能够从$f(x)$出发找到一个有限群,这个群现在称为 $f(x)$ 的 Galois 群,记作Gal(f). Galois 证明了:

定理 1.2. $f(x)=0$ 可以根式解当且仅当Gal(f) 是可解群. (见下期)

可解群这个性质我们到下一期再说,但有一点可以告诉大家,前面说的多项式 x^5-x+1 的 Galois 群是 S_5, 而 S_5 不具有上面所说的特殊性质!

也就是说 $x^5-x+1=0$ 不能根式解! 这里比较有意思的是,如果你直接思考 $x^5-x+1=0$ 是否可以根式解可能十年、二十年也找不到可行的思路,但如果要验证一个 120 个元素的群是不是可解群至少可能通过穷举来实现.

Galois 的创造在过去的近两百年中最重要的应用包括物理、化学分子结构、信息编码、信息加密等重要的领域. 令人无比扼腕叹息的是:

我们年轻的 Abel 因为穷 + 病在 26 岁就告别了他热爱的数学和亲爱的女朋友.

Galois 更是在不到 21 岁就卷入一场未知原因的决斗而丧命!

他们的刹那芳华在数学和科技的发展史上留下了光辉的一笔,天知道他们如果活久一点,今天的数学会是什么样子!

下期我们来仔细说道说道 Galois 到底说了个啥!

2 Galois 群

本期前言

上期我们听 Galois 说:

定理 2.1. 代数方程 $f(x)=0$ 可以根式解,当且仅当,其对应的 Galois 群Gal(f)是可解群.

我们将分两期说明什么是 “Galois 群” ,什么是 “可解群”.

这一期,我们就来说说有理系数多项式 $f(x)$ 的Galois 群到底是什么.

万物之对称性

或许我们或多或少都听起别人说过,Galois 是考虑了代数方程根的对称性.

当我第一次听说这句话的时候,我非常的疑惑:

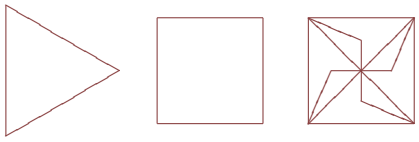
这些根有什么对称性可言呢?

实际上在 19 世纪,在数学、物理等多个领域不约而同的出现了同样一种想法:

利用事物的对称性来解决问题

这个想法在物理和化学中起到了很大的作用,比如化学中很多晶体的内部结构在能够精确测定前很久就已经利用其对称性预测出来了.

我们从最简单的图形开始. 大家来感受一下这些图形: 正三角形、正方形、正方形中带个图案,看看它们的对称性有什么不同?



根据我们的直观感觉,正三角形的对称性可以这样描述:

- 可以绕其中心旋转 $0, 2\pi/3, 4\pi/3$ 都能保证与原来的图形重合
- 可沿着其三条对称轴翻折,同样能保证与原来图形重合

也就是说, 正三角形有六种我们 “认可” 的变化方式, 使得变化后的图形与原图形重合.

同样的, 正方形有四种旋转变化, 和四种翻折变化, 共 8 种变化, 使得变化后图形与原图形重合.

如果你仔细看最后一种图形的话, 你会发现它沿原来正方形的四个对称轴翻折不会与原来的图形重合, 只有绕中心旋转 $0, \pi/2, \pi, 3\pi/2$ 四种变化能使得变化后图形与原图形重合.

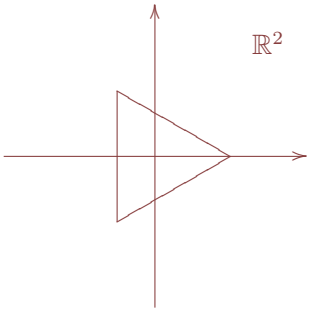
那我们怎样描述这些图形的对称性呢？ 最简单的当然是把所有我们 “认可” 的变化记录下来.

如何优雅的描述对称性

上面记录图形的对称性的做法虽然不错, 但不够酷, 不够优雅. 数学上描述一件事情很多时候都追求 “帅、酷、美” 且逻辑严格.

那怎样优雅的、数学的描述对称性呢？

实际上, 在我们说旋转, 翻折的时候, 已经不自觉的把图形先放到了一个我们非常熟悉的空间中. 就是这样



而旋转、翻折恰为 $\mathbb{R}^2$ 中的正交变换. 我们记 $\mathbb{R}^2$ 上所有正交变换的集合为 $\mathrm{O}(\mathbb{R}^2)$.

记正三角形为 Δ, 我们先将其中心放置于 $\mathbb{R}^2$ 的原点, 一个顶点放置于 x 轴上.

这样你会发现, 我们上面描述的正三角形的 6 种变化恰为所有 $\mathbb{R}^2$ 上的使得变化前后正三角形区域重合的正交变换的全体.

因此, 我们可以这样 “优雅” 的表示正三角形的对称性:

$$S(\Delta) := \{\sigma \in \mathrm{O}(\mathbb{R}^2) \mid \sigma(\Delta) = \Delta\}$$

当然根据实际情况的不同, 其对称性可能会打折扣, 比如我们把这个正三角形的中心钉在一个平板上, 这样翻折将没有办法实施.

这种情况下, 我们就需要缩小允许的变换范围, 制定新的游戏规则: 只允许旋转变换.

记所有 $\mathbb{R}^2$ 上的旋转变换为 $\mathrm{SO}(\mathbb{R}^2)$, 则在这个新的游戏规则下正三角形的对称性应记为

$$S(\Delta) := \{\sigma \in \mathrm{SO}(\mathbb{R}^2) | \sigma(\Delta) = \Delta\}$$

总结一下, 怎样描述事物的对称性:

- 记事物为 Δ
- 将 Δ 放入一个 “空间” V 中
- 根据需求考虑 V 上的某些变换 (比如上面的正交变换), 记这些变换全体为 $T(V)$
- 那么 Δ 在这种情况下的对称性可记为

$$S(\Delta) := \{\sigma \in T(V) \mid \sigma(\Delta) = \Delta\}$$

根的对称性与 Galois 群

这期的最后, 我们来看一下,

Galois 群到底是个什么东西？

给定一个有理系数多项式 $f(x)$, 根据代数学基本定理, 它在 $\mathbb{C}$ 中可以分解成一次因式的乘积. 假设它在 $\mathbb{C}$ 中的所有互不相同的根为

$$\Delta = \{\xi_1, \xi_2, \cdots, \xi_r\}$$

现在我们要考虑它的对称性, 根据经验, 我们需要看 Δ 到底在怎样的一个 “空间” 里, 这里 Galois 给我找了个不大不小的空间E是

$\mathbb{C}$ 中将 $\mathbb{Q} \cup \Delta$ 中的元素经过有限步加、减、乘、除得到的元素的全体.

这个 E 后面被称为是 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域.

那 Galois 需要的 E 上的变换是什么呢？

需要那些双射 $\sigma : E \longrightarrow E$, 满足

- σ 保持加法和乘法, 即 $\forall a, b \in E$,

$$\sigma(a + b) = \sigma(a) + \sigma(b)$$
$$\sigma(ab) = \sigma(a)\sigma(b)$$

- $\sigma(a) = a, \forall a \in \mathbb{Q}$ (实际上, 这一条可由上一条推出)

满足上面条件的 σ 称为 E 的 $\mathbb{Q}$ 自同构, 所有这些 σ 构成的集合记为 $\mathrm{Aut}_{\mathbb{Q}}(E)$, 称为 E 的 $\mathbb{Q}$-自同构群.

有意思是的, 满足上面的条件的 σ 就已经满足 $\sigma(\Delta) = \Delta$ 了, 证明如下:

证明. 假设

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

其中 $a_0, a_1, \cdots, a_n \in \mathbb{Q}$.

如果 $\xi \in \Delta$, 即 ξ 是 $f(x)$ 的根, 即

$$a_n\xi^n + \cdots + a_1\xi + a_0 = 0$$

两边用 σ 作用

$$\sigma(a_n\xi^n + \cdots + a_1\xi + a_0) = \sigma(0) = 0.$$

由于 σ 保持加法和乘法, 又固定有理数, 特别的,

$$\sigma(a_i) = a_i, i = 0, \cdots, n$$

因此, 上面的式子就变成

$$a_n\sigma(\xi)^n + \cdots + a_1\sigma(\xi) + a_0 = \sigma(0) = 0.$$

所以 $\sigma(\xi)$ 依然是 $f(x)$ 的根.

所以 $\sigma(\Delta) \subseteq \Delta$, 但 σ 是双射, 特别的是单射, 而 Δ 是个有限集合, 因此 $\sigma(\Delta)$ 必然跟 Δ 有同样多的元素, 又是 Δ 的子集, 因此 $\sigma(\Delta) = \Delta$.

Galois 眼中 $f(x)$ 的所有根的对称性可以描述为

$$\begin{aligned}\mathrm{Gal}(f) :&= \{\sigma \in \mathrm{Aut}_{\mathbb{Q}}(E) \mid \sigma(\Delta) = \Delta\} \\ &= \mathrm{Aut}_{\mathbb{Q}}(E)\end{aligned}$$

称为 $f(x)$ 的Galois 群. 给两个例子感受一下.

例 1.

$$f(x) = (x-1)(x-2)(x-3)(x-4)(x-5)$$
$$g(x) = x^2 + 1$$

对于 $f(x)$ 来说, 其根的集合

$$\Delta = \{1, 2, 3, 4, 5\}$$

由于 $\Delta \subseteq \mathbb{Q}$, 因此上面取的空间 $E = \mathbb{Q}$.

从 Galois 群的定义, 可以得知 $\mathrm{Gal}(f)$ 中的元素只有 $\mathbb{Q}$ 到自身的恒等映射, 即

$$\mathrm{Gal}(f) = \{\mathrm{id}\}$$

对于 $g(x) = x^2 + 1$ 来说, 其根的集合为

$$\Delta = \{\pm \mathrm{i}\}$$

通过简单研究可以发现, 分裂域 E 为

$$E = \{a + b\mathrm{i} | a, b \in \mathbb{Q}\}$$

由于 $\mathrm{Gal}(g)$ 中的 σ 必须把 $g(x)$ 的根映为 $g(x)$ 的根, 因此 i 在 σ 下的像只能是 $\pm$i.

这样, 根据 Galois 群的定义, 很容易发现

$$\mathrm{Gal}(g) = \{\mathrm{id}, \sigma\}$$

有两个映射, 一个是 E 到自身的恒等映射 id, 另一个是 E 到 E 的映射 σ, 它将 $a+b$i 映为 $a-b$i.

因此, 给人的感觉是 $f(x)$ 的根越复杂, 其 Galois 群就越复杂; 多项式的次数高不一定意味着 Galois 群更复杂.

那到底 $\mathrm{Gal}(f)$ 满足什么性质, $f(x) = 0$ 才可以根式解呢? 且看下回.

注 1. 假设有理系数多项式 $f(x)$ 在 $\mathbb{C}$ 中有 r 个互不相同的根

$$\xi_1, \xi_2, \cdots, \xi_r$$

令 S_r 为 $1, 2, \cdots, r$ 这 r 个数的置换, 即 $\{1, 2, \cdots, r\}$ 到自身的所有双射组成的集合. $f(x)$ 的 Galois 群也可以直观的理解为保持这 r 个根之间的代数关系的置换组成的集合, 即 $\mathrm{Gal}(f)$ 由所有满足下面条件的置换 σ 组成:

对任意 r 元多项式 g,

$$g(\xi_1, \xi_2, \cdots, \xi_r) = 0$$

当且仅当

$$g(\xi_{\sigma(1)}, \xi_{\sigma(2)}, \cdots, \xi_{\sigma(r)}) = 0$$

也就是说在应用 σ 置换这些根的位置, 不改变它们之间的代数关系 (用多元多项式来体现的关系).

3 群的定义

本期前言

上一期,我们描述了一个集合 (物体? 图形? Whatever) 的对称性. 一个多项式 $f(x)$ 的 Galois 群 $\mathrm{Gal}(f)$ 也是通过其根集的对称性给出.

本期我们说说到底 $\mathrm{Gal}(f)$ 具有什么样的性质才能使得 $f(x)=0$ 可以根式解.

群的定义

写到第三期了,还没有介绍群的定义! 真是令人发指!

先回顾下具体的 “群”,一个正三角形 Δ,将其中心放在平面 $\mathbb{R}^2$ 坐标原点,那么 Δ 的对称性由下面这个 “群” 来描述.

$$S(\Delta):=\{\sigma\in O(\mathbb{R}^2)\mid \sigma(\Delta)=\Delta)\}$$

这里 $O(\mathbb{R}^2)$ 是 $\mathbb{R}^2$ 上所正交变换的全体.

稍加观察,可以发现这个集合有以下特点:

- $\mathbb{R}^2$ 恒等映射属于 $S(\Delta)$
- $S(\Delta)$ 中两个映射的复合依然属于 $S(\Delta)$
- 映射的复合满足结合律, 即
$$\sigma(\tau\theta)=(\sigma\tau)\theta$$
对所有的 $\sigma,\tau,\theta\in S(\Delta)$ 成立
- $S(\Delta)$ 中映射的逆映射还在 $S(\Delta)$ 中.

群的定义正是由上面这些特点抽象而来.

定义 3.1. 假设非空集合 G 上有二元运算 “$\cdot$”
$$G\times G\longrightarrow G$$
$(x,y)\mapsto x\cdot y$ 我们称 $(G,\cdot)$ 是一个群(group),如果下面几条性质成立:

1. 结合律:
$$x\cdot(y\cdot z)=(x\cdot y)\cdot z,\ \forall x,y,z\in G$$
2. 有单位元: 存在 $e\in G$ 使得
$$e\cdot x=x\cdot e=x,\ \forall x\in G$$
3. 有逆元: $\forall x\in G$, 存在 $y\in G$ 使得
$$x\cdot y=e=y\cdot x$$

请大家各自找找这几条性质与上方的 $S(\Delta)$ 的几个特点的对应关系.

从 $S(\Delta)$ 抽象出后面这个群的定义并不是一件容易的事情,经过了很多数学家的努力才得到今天这个版本.

很多时候,为了记号简便,我们会省略运算 $\cdot$,将群 $(G,\cdot)$ 记为群 G, $a\cdot b$ 也经常被记为 ab.

单位元、逆元唯一性

在定义3.1中, e 称为群 G 的单位元. 但这里有个问题,会不会有多个单位元呢?

实际上,如果 e,e' 都是 G 中的单位元,根据单位元的性质,很容易发现:

$$e=ee'=e'$$

因此群 G 中的单位元是唯一的! 定义3.1中群 G 的两个元素 x,y 满足

$$xy=e=yx$$

称 y 是 x 的逆元,记为 x^{-1}. (与矩阵的逆对比一下)

每个元素的逆元也是唯一的! 实际上,如果 x 有两个逆元 y 和 z,那么

$$y=ye=y(xz)=(yx)z=ez=z$$

按照这个定义,上期考虑的 $S(\Delta)$, $\mathrm{Gal}(f)$ 在映射复合这个运算下构成群,其单位元都是恒等映射,而每个双射的逆元为其逆映射.

不仅如此,这个抽象的定义把很多我们平时所熟知的集合变成了群,验证下面这些是群.

集合	运算
$\mathbb{Z}$	整数加法
$\mathbb{R}^*$ 非零实数	实数乘法
$\mathrm{GL}_n(\mathbb{R})$ 所有 n 阶可逆矩阵	矩阵乘法
$\mathrm{SL}_n(\mathbb{R})$ 所有行列式为 1 的 n 阶方阵	矩阵乘法
S_n : $\{1,\cdots,n\}$ 到自身的所有双射	映射复合

上面这些例子中

$(\mathbb{Z},+)$ 的单位元是 0, 整数 i 的逆元是 $-i$

$\mathrm{GL}_n(\mathbb{R})$ 中的单位元是单位矩阵 I,矩阵 A 的逆元是其逆矩阵 A^{-1}

群中消去律

在群 $(G,\cdot)$ 中,如果有

$$ax=ay$$

两边左乘 a^{-1}, 则有

$$a^{-1}(ax)=a^{-1}(ay)$$

根据运算的结合性,我们得到

$$(a^{-1}a)x=(a^{-1}a)y,$$

由于 $a^{-1}a=e$, 所以

$$x = ex = ey = y.$$

也就是说, 在群中左边的消去律成立. 类似的, 右边的消去律也是成立的.

引理 3.2. 假设 G 是一个群, $a, x, y \in G$. 那么

$$ax = ay \Rightarrow x = y$$

$$xa = ya \Rightarrow x = y$$

子群及其判定

G 的某些子集 H 在 G 的运算下依然是群. 比如: $\mathrm{GL}_n(\mathbb{R})$ 是所有 n 阶可逆实矩阵构成的集合, 它在矩阵的乘法下构成群, $\mathrm{SL}_n(\mathbb{R})$ 是行列式为 1 的 n 阶实矩阵构成的全体, 它是 $\mathrm{GL}_n(\mathbb{R})$ 的子集, 它关于矩阵的乘法依然是群.

定义 3.3. 假设 $(G, \cdot)$ 是一个群, $H \subseteq G$ 是 G 的非空子集. 如果 $(H, \cdot)$ 也是一个群, 我们称 H 为 G 的一个子群(subgroup), 记作: $H \leqslant G$.

例如:

- $\mathrm{SL}_n(\mathbb{R}) \leqslant \mathrm{GL}_n(\mathbb{R})$
- $m\mathbb{Z} \leqslant \mathbb{Z}$, 这里 m 为正整数, $m\mathbb{Z} := \{mi | i \in \mathbb{Z}\}$
- 对任意群 G, $G \leqslant G$, $\{e\} \leqslant G$

群 VS 子群

假设 H 是群 G 的一个子群.

由于 $(H, \cdot)$ 也构成群, 至少 H 中两个元素做 "$\cdot$" 后还在 H 中, 即

$$h_1 \cdot h_2 \in H, \forall h_1, h_2 \in H$$

H 中有自己的单位元 e_H. 问题是:

$$e_H \text{ 跟 } G \text{ 的单位元 } e_G \text{ 有何区别?}$$

事实上

$$e_G \cdot e_H = e_H = e_H \cdot e_H$$

左边的等号是因为 e_G 中 G 中单位元, 右边的等号是因为 e_H 为 H 中单位元.

由上面的引理3.2, 两边消去 e_H 得 $e_G = e_H$. 所以

$$H \text{ 中的单位元与 } G \text{ 中单位元一致!}$$

最后, 比较下 H 中的元素在 H 中的逆元与它在 G 中的逆元有何不同.

设 $h \in H$ 在 G 中的逆元是 a, 在 H 中的逆元是 b, 则

$$b \cdot h = e_H = e_G = a \cdot h$$

根据引理3.2, 两边消去 h 得 $b = a$. 因此

$$h \text{ 在 } H \text{ 中的逆和在 } G \text{ 中的逆相同!}$$

子群的判定

怎样判断 G 的一个非空子集 H 是否为子群呢? 根据上面这些讨论, 可以总结如下.

命题 3.4. 假设 $(G, \cdot)$ 是一个群, 单位元为 e, 而 $H \subseteq G$ 是 G 的非空子集. 则 $H \leqslant G$ 当且仅当下面几条成立:

1. H 关于 "$\cdot$" 封闭, 即
$$h_1 \cdot h_2 \in H, \forall h_1, h_2 \in H$$
2. $e \in H$
3. 对任意 $h \in H$, 其在 G 中的逆元 $h^{-1} \in H$.

证明. 如果 $H \leqslant G$, 根据上面讨论, 结论 1, 2, 3 成立. 反过来, 如果 1, 2, 3 成立, 很容易根据群的定义验证 $(H, \cdot)$ 是一个群, 从而是 G 的子群. 这里需要注意的是, 由于 H 与 G 是相同的运算 "$\cdot$" , 因此 H 中运算 "$\cdot$" 是结合的.

注: 上面命题中的第 2 条可由其他两条推出. 我们还可以把这几条 "浓缩" 为一条

定理 3.5. 假设 $(G, \cdot)$ 是一个群, 而 $H \subseteq G$ 是 G 的非空子集. 则 $H \leqslant G$ 当且仅当, 对于任意 $a, b \in H$, 有

$$a \cdot b^{-1} \in H.$$

证明. 如果 $H \leqslant G$, 显然

$$a \cdot b^{-1} \in H, \forall a, b \in H.$$

反过来, 假设

$$a \cdot b^{-1} \in H, \forall a, b \in H.$$

我们将证明上面命题中的 1, 2, 3 都成立.

首先证明 G 的单位元 e 属于 H. 这个比较简单, 令 $a = b$, 根据假设

$$e = a \cdot b^{-1} \in H$$

其次, 对于任意 $h \in H$, 其在 G 中的逆

$$h^{-1} = e \cdot h^{-1}$$

由于 $e, h \in H$, 因此, 根据假设

$$e \cdot h^{-1} \in H, \text{从而 } h^{-1} \in H.$$

最后, 对于任意 $x, y \in H$, 前面已经证明了

$$y^{-1} \in H,$$

因此

$$x \cdot y = x \cdot (y^{-1})^{-1} \in H$$

这样上面命题中的 $1, 2, 3$ 均已证明, 因此 H 是 G 的子群.

3 可解群

最后来看下多项式 $f(x)$ 的 Galois 群要满足什么特殊性质方程 $f(x) = 0$ 才能根式解.

第一类满足这个性质的群是交换群, 也就是说

命题 3.6. 假设 $f(x)$ 为一个有理系数多项式, 如果 $\mathrm{Gal}(f)$ 是交换群, 即

$$\sigma\tau = \tau\sigma, \forall \sigma, \tau \in \mathrm{Gal}(f)$$

那么 $f(x) = 0$ 可以根式解.

这个命题本质上是由 Abel 先证明的, 只不过不是用群的语言, 由于这个原因, 交换群也称为 Abel 群.

$\mathrm{Gal}(f)$ 不交换, 是不是 $f(x) = 0$ 就不能根式解呢?

不是的, 所有 3 次方程都可以根式解, 但有些三次方程 (比如: $x^3 - 2$) 的 Galois 群并不是交换群.

定义 3.7. G 的子群 H 称为 G 的正规子群, 如果

$$aHa^{-1} \subseteq H, \forall a \in G$$

此时, 记 $H \lhd G$.

放大招了!

定理 3.8 Galois. 假设 $f(x)$ 是一个有理系数多项式, $\mathrm{Gal}(f)$ 为其 Galois 群. 那么 $f(x) = 0$ 可以根式解, 当且仅当, 存在子群序列

$$\{e\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = \mathrm{Gal}(f)$$

满足

$$abG_{i+1} = baG_{i+1}, \forall a, b \in G_i, 0 \leqslant i < n$$

G_i "相对于" G_{i+1} 是交换的. 这里

$$abG_{i+1} = \{abx \mid x \in G_{i+1}\}$$

满足定理条件的群称为可解群. 要证明上面这个定理, 需要差不多一个学期的时间!

这个定理把代数方程根式解的问题转化成了一个关于群的问题. 我们用例子来感受下两边的不同感觉. 比如第一期提到的

$$f(x) = x^5 - x + 1$$

通过一定的技巧, 可以证明 $\mathrm{Gal}(f) \simeq S_5$, 也就是 $\{1, 2, 3, 4, 5\}$ 到自身所有双射的全体.

如果让单纯去想 $f(x) = 0$ 能否根式解, 估计磨破脑壳十年内也未必能想清楚.

但如果让我们去想 S_5 是不是可解群, 估计十天内还是有希望的.

这就是这个定理神奇的地方!

最后我们简要介绍一些可解群的例子.

显然 Abel 群是可解群, 除此之外

两类可解群

群	贡献者
$\lvert G\rvert = p^a q^b$, p, q 为素数	W, Burnside[1]
$\lvert G\rvert$ 为奇数	W. Feit, J. G. Thompson[2]

不可解群也有很多, 特别的, S_n 在 $n \geqslant 5$ 时都不可解. 下期我们就来特别的介绍下群 S_n, 它将是我们这门课程里面最重要的例子之一.

参考文献

[1] W. Burnside, On Groups of Order palphaqbeta. *Proc. London Math. Soc.* (2) (1904), 388–392.

[2] W. Feit, J. G. Thompson, Solvability of groups of odd order. *Pacific J. Math.* 13 (1963), 775–1029.

4 思考题

练习 1. 假设非空集合 G 上满足结合律的二元运算 "$\cdot$" 还满足下面两个条件.

1. 存在右单位元 e, 即 $x \cdot e = x$ 对所有 $x \in G$ 成立;
2. 每个元素都有右逆, 即对任意 $x \in G$,

存在 $y \in G$ 使得 $x \cdot y = e$

证明: $(G, \cdot)$ 是一个群.

练习 2. 假设有限非空集合 G 上满足结合律的二元运算 "$\cdot$" 还满足消去律. 证明: $(G, \cdot)$ 是群.

练习 3. 证明: 有限群 G 的一个非空子集 H 是 G 的子群, 当且仅当 H 关于 G 的运算封闭.

4 对称群

本期导言

上一期, 我们介绍了群和子群的概念, 这一期我们来说说一类非常重要的群:

$S_n := \{\{1, \cdots, n\} \text{ 到自身双射 }\}$

S_n 在映射的复合这个运算下构成一个群, 称为n 阶对称群.

S_n 中的元素

为了简便, 我们把 $\{1, 2, \cdots, n\}$ 记为 $[1, n]$.

n 阶对称群 S_n 中的元素为 $[1, n]$ 到自身的一一映射, 比如:

$$\begin{array}{ccc} \sigma : [1,5] & \longrightarrow & [1,5] \\ 1 & \mapsto & 2 \\ 2 & \mapsto & 4 \\ 3 & \mapsto & 5 \\ 4 & \mapsto & 1 \\ 5 & \mapsto & 3 \end{array}$$

实际上就是把 1 到 5 这几个数字重新排个顺序. 因此我们把 S_n 元素称为 $1, \cdots, n$ 的置换.

S_n 有多少个元素?

很显然, S_n 中的元素个数与 $1, \cdots, n$ 的排列数一样多, 有 $n!$ 个元素.

S_n 中元素描述方式

要描述 S_n 的元素, 最先想到的就是上面例子给的方式, 以映射的形式写出. 但是这样做有一个缺点

实在是太占地儿了!

一个办法是将映射转 90 度写, 像这样

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$$

第二排的数字是第一排对应的数字在 σ 下的像. σ 的逆映射也一下就写出来了.

$$\sigma^{-1}=\begin{pmatrix}1&2&3&4&5\\4&1&5&2&3\end{pmatrix}$$

两个映射复合, 也挺容易

$$\sigma=\begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix}$$

$$\tau=\begin{pmatrix}1&2&3&4&5\\1&2&5&4&3\end{pmatrix}$$

$$\tau\sigma=\begin{pmatrix}1&2&3&4&5\\2&4&3&1&5\end{pmatrix}$$

这里 $\tau\sigma(1)=\tau(2)=2$, 其他计算也类似.

τ 保持 $1,2,4$ 不动, 只是把 3 和 5 换了个顺序, 而 $\tau\sigma$ 也是保持 3 和 5 不动, 再这样表示 τ 和 $\tau\sigma$ 就有点不划算了.

想想如果 $n=100$, 一个置换只是把 1 和 2 互换, 按照现在这种描述方式, 我们还需要傻乎乎的再写 98 对一样的数字!

k 循环

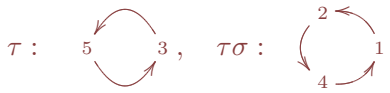
因此, 像上面 τ 这样的置换, 只是 3 和 5 对换, 我们就将它记为

$$\tau=(35)$$

上面的 $\tau\sigma$ 将 1 变为 2, 2 变为 4, 4 变为 1, 其他数字保持不动, 我们记为

$$\tau\sigma=(124)$$

如果我们用图形来表达的话就是这样



一般的, 如果 $i_1,\cdots,i_k$, $k\geqslant 1$ 是 $[1,n]$ 中互不相同的 k 个数字, 如果 $\sigma\in S_n$ 满足

$$\sigma(i_r)=i_{r+1},\forall 1\leqslant r\leqslant k-1$$

$$\sigma(i_k)=i_1$$

$$\sigma(j)=j,\forall j\notin\{i_1,\cdots,i_k\}$$

则称 σ 是一个k 循环, 记为

$$(i_1i_2\cdots i_k)$$

例如: (1345) 将 1 映为 3, 3 映为 4, 4 映为 5, 5 映为 1, 其他数字保持不变.

下面的小黑板描述了 k 循环的基本性质:

$(1345)=(3451)=(4513)=(5134)$

$(1345)^{-1}=(5431)=(1543)$

1 循环是恒等映射 e

σ 为 k 循环, 那么 $\sigma^k=e$

不相交循环

我们称两个循环

$$\sigma=(i_1\cdots i_k)$$

$$\tau=(j_1\cdots j_r)$$

不相交如果

$$\{i_1,\cdots,i_k\}\cap\{j_1,\cdots,j_r\}=\emptyset$$

引理 4.1. 假设 σ,τ 为 S_n 中两个不相交的循环. 则

$$\sigma\tau=\tau\sigma.$$

证明. 假设

$$\sigma=(i_1\cdots i_k)$$

$$\tau=(j_1\cdots j_r)$$

对于任意 $i\in\{i_1,\cdots,i_k\}$, $\sigma(i)$ 依然还在

$$\{i_1,\cdots,i_k\}$$

中. 由于

$$\{i_1,\cdots,i_k\}\cap\{j_1,\cdots,j_r\}=\emptyset$$

我们有

$$i,\sigma(i)\notin\{j_1,\cdots,j_r\}$$

因此

$$\tau(i)=i,\tau(\sigma(i))=\sigma(i)$$

从而

$$\sigma\tau(i)=\sigma(i)=\tau\sigma(i)$$

类似的, 对任意 $j\in\{j_1,\cdots,j_r\}$, 同样有

$$\sigma\tau(j)=\tau(j)=\tau\sigma(j)$$

对于既不在 $\{i_1,\cdots,i_k\}$ 中, 也不在 $\{j_1,\cdots,j_r\}$ 中的数 t, 有

$$\tau(t)=t=\sigma(t)$$

因此

$$\sigma\tau(t)=\sigma(t)=t$$

$$\tau\sigma(t)=\tau(t)=t$$

总结起来, 我们证明了对于所有 $[1,n]$ 中的整数 i, 都有 $\sigma\tau(i)=\tau\sigma(i)$, 因此 $\sigma\tau=\tau\sigma$.

表达为不相交循环乘积

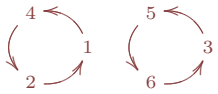
定理 4.2. 任意 S_n 中元素都可以表达成互不相交循环的乘积, 且这种表达在不计顺序的意义下是唯一的.

鉴于公众号文章的长度不宜过长, 我们不给这个定理的严格证明, 只做一个简单的解释, 小伙伴们可以随便找一本近世代数的书自行查阅.

举个例子.

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

看下 σ 作用在各个数字上的效果, 可以用图来表示



即将 1 映为 4, 4 映为 2, 2 映为 1; 3 映为 5, 5 映为 6, 6 映为 3; 保持 7 不动. 这时, 如果你考虑

$$(142)(356) \text{ 或者 } (356)(142)$$

你会发现它们都与 σ 是同样的效果, 也就是说

$$\sigma = (124)(356) = (356)(124)$$

大家可以看到, 这两个循环实际上是由 σ 作用的效果所决定的.

比较下 σ 的前后两种表达方式, 我们发现把 σ 写成 (142)(356) 形式有下面两个优点:

- 更简洁, 占地面积小
- σ 的作用效果更直观

表达成对换乘积

在进一步讨论之前, 我们看看相交的循环的乘积是个什么效果. 先看最简单的

$$(12)(13)$$

看下它的作用效果

$$\begin{aligned} 1 &\overset{(13)}{\mapsto} 3 \overset{(12)}{\mapsto} 3 \\ 3 &\overset{(13)}{\mapsto} 1 \overset{(12)}{\mapsto} 2 \\ 2 &\overset{(13)}{\mapsto} 2 \overset{(12)}{\mapsto} 1 \end{aligned}$$

因此, 其作用效果是将 1 映为 3, 3 映为 2, 2 映为 1, 组成一个循环 (132). 也就是说

$$(12)(13) = (132)$$

然而 “众生平等”, 数字 1, 2, 3 不过是 “芸芸众生” 中的平凡代表罢了, 因此对于任意 3 个不同的整数 $a, b, c \in [1, n]$, 都有

$$(ab)(ac) = (acb)$$

反过来, 也可以说任意一个三循环都可以写成两个 2 循环的乘积.

这个 “公式” 可以有变种:

$$(ab)(bc) = (ba)(bc) = (bca) = (abc)$$
$$(ac)(bc) = (ac)(cb) = (acb)$$

那么 4 循环, k 循环呢? 这个就不要怪我 “山寨” 了, 考虑 k 循环 $(12\cdots k)$, 可以验证

$$(23\cdots k)(1k) = (12\cdots k)$$

当然, 你愿意把它拆成 2 循环的乘积也是没有问题的 (只要根据这个规律继续就行)

$$(12\cdots k) = (k-1, k)\cdots(2k)(1k)$$

今后, 我们称一个 2 循环为对换.

结合定理4.2, 我们就有

推论 4.3. 每个 S_n 中的元素都对表达成为对换的乘积.

很显然, 这种表达方式并不是唯一的, 比如

$$(123) = (12)(23) = (13)(12)$$

3 S_n 中元素的奇偶性

S_n 中元素 σ 表达成对换的乘积并不是唯一, 那我们有什么可期待的呢?

我们可以期待 σ 表达成对换乘积的时候, 对换的个数的奇偶性是确定的.

比如 (123) 可以写成 2 个对换的乘积, 我们希望它永远不能写成 3 个或者其他奇数个对换的乘积.

要怎样证明这件事情呢? 实际上, 这个问题在我们学线性代数的行列式的定义那里已经解答过了, 只不过当时可能没有用对称群的语言, 而是讲排列的奇偶性. 这里, 我们介绍一个比较传统的方法, 主要是利用 S_n 中元素的运算规则.

证明. 假设 S_n 中某一元素有两种方式写成对换乘积

$$\tau_1\tau_2\cdots\tau_r = \theta_1\theta_2\cdots\theta_s$$

则有

$$\tau_1\tau_2\cdots\tau_r\theta_s^{-1}\theta_{s-1}^{-1}\cdots\theta_1^{-1} = e$$

由于对换的逆映射仍然是对换, 因此

$$\tau_1\tau_2\cdots\tau_r\theta_s\theta_{s-1}\cdots\theta_1 = e$$

我们需要证明 $r+s$ 为偶数. 对 $r+s$ 用数学归纳法. 当 $r+s=1$ 时, e 无法写成一个对换, 矛盾. 如果 $r+s=2$ 时, $r+s$ 已经是偶数, 结论成立. 现假设 $r+s>2$. 假设 a 出现在这些对换中, 即某个对换为 (ab) 形式, 如果它不是上面表达式中最左边的对换, 我们对其左边相邻的对换进行分类

$$(ab)(ab) = e$$
$$(ac)(ab) = (abc) = (ab)(bc)$$
$$(bc)(ab) = (cb)(ba) = (cba) = (ca)(cb)$$
$$(cd)(ab) = (ab)(cd)$$

对于第一种情况, $(ab)(ab)$ 可以约掉, 从而 e 可以写成 $r+s-2$ 个对换的乘积, 由归纳假设可知 $r+s-2$ 为偶数, 因此 $r+s$ 为偶数. 对于其他情形, a 向左移动一个位置, 反复利用上面表格中的等式, 要么我们可以将 e 写成 $r+s-2$ 个对换的乘积, 要么将 a 移动到最左边, 且后面的对换中不再出现 a. 假设此时表达式中最左边的对换为 (ab), 由于后面的对换不含 a, 作用在 a 上不变, 因此

$$e(a) = (ab)(a) = b$$

这与 e 为恒等映射矛盾. 因此 $r+s$ 为偶数.

如果 σ 可以写成奇数个对换的乘积, 我们称 σ 为奇置换, 否则, 称 σ 为偶置换. 由于 e 是偶置换, 且偶置换关于乘积和取逆封闭, 因此所有偶置换构成 S_n 的一个子群, 即

命题 4.4. 对 $n \geqslant 2$, S_n 中所有偶置换构成 S_n 的一个子群, 记为 A_n, 称为 n 阶交错群(alternating group).

对于 $n \geqslant 2$,

$$S_n \longrightarrow S_n, \sigma \mapsto (12)\sigma$$

诱导 S_n 中奇置换与偶置换之间的双射, 因此, 此时奇置换与偶置换的个数相等. 结合 $|S_n| = n!$, 我们有

$$|A_n| = \frac{n!}{2}.$$

4

元素的共轭

本期的最后, 告诉大家一个好玩的现象. 上面定理4.4的证明中, 我们用到了类似

$$(13)(12)(13)^{-1} = (32)$$

的事实. 我们再来举一个例子:

$$(125)(123)(125)^{-1} = (253)$$

实际上, 我们有下面这个统一的结论

定理 4.5. $(i_1 \cdots i_k)$ 为 S_n 中 k 循环, $\sigma \in S_n$. 则

$$\sigma(i_1 \cdots i_k)\sigma^{-1} = (\sigma(i_1), \cdots, \sigma(i_k))$$

也是一个 k 循环.

证明留作练习, 小伙伴们, 你能证明吗?

5 二面体群

本期前言

在抽象的理论学习之前,我想还应该再多了解一点具体的群的例子.

本期我们讨论另一类群的例子: 正 n 边形在 $\mathbb{R}^2$ 中的对称群 D_n,称为二面体群

1 二面体群简介

曾记否? 我们在讲对称的时候说到过正三角形和正方形的对称. 今天讲讲正 n 边形的对称. 回顾一下我们说的对称是啥意思. 给定一个正 n 边形 Δ_n, 我们把 Δ_n 的中心放置于 $\mathbb{R}^2$ 的原点, 其中一个顶点放在 x 轴上, 也就是说 Δ_n 的 n 个顶点的坐标是

$$A_k(\cos\frac{2k\pi}{n}, \sin\frac{2k\pi}{n}), k = 0, \cdots, n-1$$

Δ_n 的对称性描述为

$$S(\Delta_n) := \{\mathbb{R}^2 \text{ 上正交变换 } \sigma \mid \sigma(\Delta_n) = \Delta_n\}$$

在第 3 期中, 我们已经知道 $S(\Delta_n)$ 在映射的复合下是一个群, 这个群称为二面体群 (dihedral group), 记作 D_n.

这期就来看下 D_n 中有哪些元素? 它们之间的乘法有什么特点?

2 二面体群中的元素

由于 $\mathbb{R}^2$ 的正交变换只有两类

- 行列式为 1, 旋转变换
- 行列式为 -1, 翻折变换

旋转变换

其中满足 $\sigma(\Delta_n) = \Delta_n$ 的旋转变换比较清楚, 它们恰为那些旋转角度为 $2\pi/n$ 的整数倍的旋转变换. 记 ρ 为逆时针旋转 $2\pi/n$ 的旋转变换. 则 $S(\Delta_n)$ 中的所有的旋转变换为

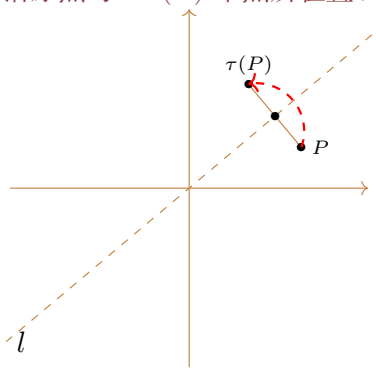
$$e, \rho, \cdots, \rho^{n-1}$$

其中 e 为恒等变换.

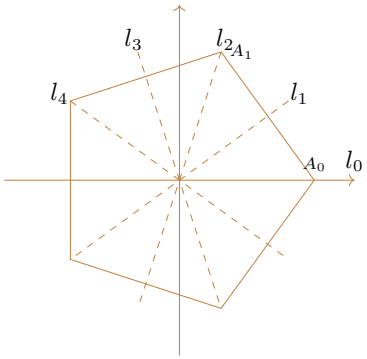
翻折变换

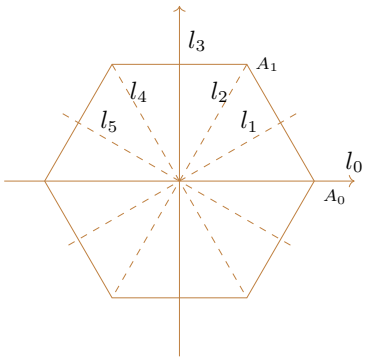
$\mathbb{R}^2$ 上的翻折变换 τ 由一个非原点 P 和它在 τ 下的像 $\tau(P)$ 确定:

τ 为沿原点与 $P\tau(P)$ 中点所在直线翻折



看两个例子: 正五边形和正六边形





可以发现, 它们的翻折对称轴恰为 A_0A_k 的中点与原点所在的直线 l_k, $k = 0, \cdots, n-1$.

将沿 l_k, $k = 0, 1, \cdots, n-1$ 的翻折变换记为 τ_k. $S(\Delta_n)$ 中的所有翻折变换为

$$\tau_0, \tau_1, \cdots, \tau_{n-1}$$

小结

二面体群 D_n 中的元素共有 $2n$ 个:

旋转: $e, \rho, \rho^2, \cdots, \rho^{n-1}$

翻折: $\tau_0, \tau_1, \cdots, \tau_{n-1}$

二面体群中元素乘积

旋转变换之间的乘积是很清楚的:

$$\rho^n = e$$
$$\rho^i \rho^j = \rho^{[i+j]}$$

其中 $[i+j]$ 是 $i+j$ 模 n 的余数. 比如, 当 $n=6$ 时

$$\rho^4 \rho^5 = \rho^{6+3} = \rho^3$$

本期从现在开始, 用 $[m]$ 表示整数 m 模 n 的余数.

其他情况呢: 旋转与翻折, 翻折与翻折, 翻折与旋转的乘积分别是什么样子呢?

τ_k 的另类实现

我们知道 τ_k 是一个翻折变换, 它将 A_0 变为 A_k, 也知道一个翻折变换由 A_0 在它下的像唯一确定. 也就是说如果一个翻折变换 τ 满足 $\tau(A_0) = A_k$, 则 $\tau = \tau_k$.

下面我们就找一个特殊的翻折变换

$$\rho^k \tau_0$$

它的行列式为 -1, 因此确实是翻折变换. A_0 在它下的像是谁呢?

$$\rho^k \tau_0(A_0) = \rho^k(A_0) = A_k$$

因此对于任意 $k = 0, \cdots, n-1$ 有

$$\rho^k \tau_0 = \tau_k$$

遵循这个思路, 我们还可以考虑

$$\tau_0 \rho^{n-k}$$

它也是一个翻折变换, 且

$$\tau_0 \rho^{n-k}(A_0) = \tau_0(A_{n-k}) = A_k$$

因此对于任意 $k = 0, \cdots, n-1$ 有

$$\tau_0 \rho_{n-k} = \tau_k$$

所以对于任意 $k = 0, \cdots, n-1$ 有

$$\rho^k \tau_0 = \tau_0 \rho^{n-k} = \tau_k$$

旋转与翻折的乘积

一个旋转 ρ^i 与一个翻折 τ_j 的乘积为

$$\rho^i \tau_j = \rho^i(\rho^j \tau_0) = \rho^{[i+j]} \tau_0 = \tau_{[i+j]}$$

翻折与旋转的乘积

一个翻折 τ_i 与一个旋转 ρ^j 的乘积为

$$\begin{aligned} \tau_i \rho^j &= \tau_0 \rho^{n-i} \rho^j \\ &= \tau_0 \rho^{[j-i]} \\ &= \tau_{[n-[j-i]]} = \tau_{[i-j]} \end{aligned}$$

翻折与翻折的乘积

$$\begin{aligned} \tau_i \tau_j &= \rho^i \tau_0 \tau_0 \rho^{n-j} \\ &= \rho^{[i+n-j]} = \rho^{[i-j]} \end{aligned}$$

二面体群的子群

二面体群 D_n 有几个很有意思的子群

$$\{e, \rho, \rho^2, \cdots, \rho^{n-1}\} \leqslant D_n$$
$$\{e, \tau_k\} \leqslant D_n$$

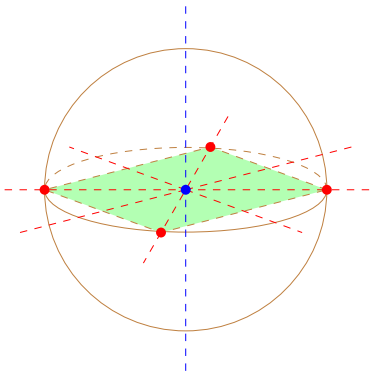
其中 $k = 0, \cdots, n-1$.

小伙伴们, 验证下这些确实是 D_n 的子群.

为什么叫二面体群?

那为什么 D_n 叫二面体群呢? 二面体是什么?

实际上, 如果你把正 n 边形 Δ_n 放到 $\mathbb{R}^3$ 中. 在三维空间中, 它就可以叫做“二面体”了: 只有上下两个面.



此时考虑 $\mathbb{R}^3$ 的旋转变换 (绕着一个轴旋转), 即 $\mathrm{SO}(\mathbb{R}^3)$, 仔细琢磨下, 你就会发现

$$\{\sigma \in \mathrm{SO}(\mathbb{R}^3) \mid \sigma(\Delta_n) = \Delta_n\}$$

恰为绕 z 轴旋转 $2k\pi/n$ 或者绕着 Δ_n 的几个对称轴旋转 180 度.

也就是说 D_n 的确是将正 n 边形在 $\mathbb{R}^3$ 中 (可称“二面体”) 只允许旋转变换下的对称群, 因此被称为二面体群.

6 循环子群

本期前言

回顾下 Galois 的定理:

假设 $f(x)$ 为有理系数多项式. $f(x)=0$ 可以根式解当且仅当 $f(x)$ 的 Galois 群是可解群.

这告诉我们, 要判断 $f(x)$ 是否可以根式是否可以根式解总共分两步:

- 求出 $f(x)$ 的 Galois 群 $\mathrm{Gal}(f)$
- 判断 $\mathrm{Gal}(f)$ 是否是可解

比把大象装进冰箱少一步!

如果跟另外一个人来分摊这两个工作的话, 像我这么懒的人, 肯定最先举手: 我做第二步!

实际上第一步真的很难, 要确定一个有理多项式的 Galois 群通常情况下是比较困难的.

我们知道一个群可解是意思是存在一个条件比较苛刻的子群序列, 也就是说如果你知道一个群的所有子群和它们之间的关系, 就应该能判断一个群是否可解.

既然我们挑了一个自认为比较简单的, 我们就立个 flag:

抽象的研究群的子群及子群之间的关系!

搜寻子群

现在开始, 我们就抽象的来讨论群的子群.

假设 $(G,\cdot)$ 是一个群, 我们省略其中的运算 "$\cdot$", 将 $a\cdot b$ 记为 ab.

现在我们就开始满世界找 G 的子群! 在头脑里努力的回忆子群的样子:

假设 H 是 G 的一个非空子集. 那么H 是 G 的子群当且仅当下面的条件成立

- H 对运算封闭
  $$\forall a,b\in H,\ ab\in H$$
- H 对取逆封闭
  $$\forall a\in H,\ a \text{ 在 } G \text{ 中的逆 } a^{-1}\in H$$

有了这把 "尚方宝剑", 我们就可以开始 "搜查" 所有 G 的子集, 一个个 "审问" 看它们是不是 G 的子群! 但当 G 的元素个数 (称为 G 的阶数) 稍微有点大时 (比如 16), 这样的子集就多得不得了 (2^{16} 个), 要把它们一个个 "审完", 咱们这辈子也不用做啥别的事了.

所以这样蛮干是不行的! 必须要先查一些 "可疑" 的子集! 哪些是可疑的子集呢?

以前考虑一个域 F 上向量空间 V 的子空间的时候, 对于任意 V 中的子集 X, 我们都能找出一个子空间:

$$\langle X\rangle := \{X \text{ 中向量的线性组合 }\}$$

我们是否可以利用这个经验?

生成子群

对群 G 的一个子集 X 来说, 我们也可以由 X 生成 G 的一个子群, 抽象的定义:

$$\langle X\rangle = \cap_{H\leqslant G, X\subseteq H} H$$

即包含 X 的 G 的子群的交集, 这里需要注意子群的交集依然是子群. 根据这个定义, $\langle X\rangle$ 为 G 的包含 X 的最小子群.

跟向量空间中子集生成的子空间相比, 这个定义比较抽象, 我们不清楚 X 生成的子群中到底包含哪些元素. 为此, 我们给出一个构造性的方法. 可以考虑关于 X 中元素 x 或者其逆 x^{-1} 的 "子符串", 比如

$$x_1x_2x_3^{-1}x_3x_2x_2^{-1}$$

其中 $x_1,x_2,x_3\in X$. 当然也可以是空字符串, 对每个这样的字符串 w, 我们可以计算其在 G 中的运算结果 $\phi(w)$ (将空字符串计算为单位元 e). 当然, 这里我们需要利用运算的结合律说明不管以什么顺序进行运算, 得到的结果是一致的, 比如上面的字符串运算后的结果为 x_1x_2. 把所有这样的运算结果收集起来

$$M := \{\phi(w)\mid w \text{ 是关于 } X, X^{-1} \text{ 的字符串 }\}$$

很容易发现, 这个集合是 G 的子群. 对每个字符串 w, 将其中的每个符号都取逆符号, 再前后颠倒顺序, 得到的字符串记为 w^{-1}, 比如, 记上面例子中字符串为 w, 则

$$w^{-1} = x_2x_2^{-1}x_3^{-1}x_3x_2^{-1}x_1^{-1}$$

容易检验

$$\phi(w_1)\phi(w_2)=\phi(w_1w_2)$$

其中 w_1w_2 为字符串 w_1,w_2 连接而成的新

字符串.

$$\phi(w)^{-1}=\phi(w^{-1})$$

这说明 M 是关于 G 中运算和取逆封闭的, 构成 G 的子群. 显然 M 包含 X, 且对任意 G 的包含 X 的子群 H 都有 $M\subseteq H$. 也就是说, M 是包含 X 的最小子群, 即

$$M=\langle X\rangle$$

称为由 X生成的子群 (subgroup generated by X).

循环子群

在研究向量空间的线性变换时, 一个向量生成的不变子空间称为循环子空间. 类似地, G 的一个元素 a 生成的子群 $\langle a\rangle$ 称为 G 的循环子群(cyclic subgroup).

显然我们有下面的性质.

- $e\in\langle a\rangle$
- $aa\in\langle a\rangle$
- $aaa\in\langle a\rangle$
- $aaaa\in\langle a\rangle$
- $\cdots\cdots$
- $a^{-1}\in\langle a\rangle$
- $a^{-1}a^{-1}\in\langle a\rangle$
- $a^{-1}a^{-1}a^{-1}\in\langle a\rangle$
- $\cdots\cdots$

这好家伙, 把 a 的一堆 “好哥们” 全部都扯进来了. 我们把这些好哥们用下面的记号来记

- m 个 a 的乘积 $(m>0)$
$$a^m:=aa\cdots a$$
- m 个 a^{-1} 的乘积 $(m>0)$
$$a^{-m}:=a^{-1}a^{-1}\cdots a^{-1}$$
- 单位元
$$a^0:=e$$

按照这种记号

$$\{a^i\mid i\in\mathbb{Z}\}\subseteq\langle a\rangle$$

再仔细看下左边这个集合元素的乘积有什么特点.

$$\begin{aligned}&a^ma^{-m}\\=&\underbrace{a\cdots a}_{m}\underbrace{a^{-1}\cdots a^{-1}}_{m}\\=&\underbrace{a\cdots a}_{m-1}e\underbrace{a^{-1}\cdots a^{-1}}_{m-1}\\=&\cdots\cdots\\=&aa^{-1}=e\end{aligned}$$

所以 a^m 与 a^{-m} 互为逆元. 这实际上说明了 a^i 的逆元是 a^{-i}, $\forall i\in\mathbb{Z}$.

a^i 与 a^j 的乘积呢? 大家可以分 i,j 同号和异号的不同情形验证下

$$a^ia^j=a^{i+j}$$
$$(a^i)^j=a^{ij}$$

这么看来这个集合 $\{a^i\mid i\in\mathbb{Z}\}$ 含单位元 e, 对运算封闭, 每个元素的 a^i 的逆元 a^{-i} 还在这个集合中.

因此 $\{a^i\mid i\in\mathbb{Z}\}$ 已经是 G 的一个子群. 总结一下

命题 6.1. 假设 G 是一个群, $a\in G$. 则
$$\{a^i\mid i\in\mathbb{Z}\}$$
是 G 的子群.

由于 $\langle a\rangle$ 是包含 a 的最小子群, 所以最终我们得到

$$\langle a\rangle\subseteq\{a^i\mid i\in\mathbb{Z}\}\subseteq\langle a\rangle$$

从而有

$$\langle a\rangle=\{a^i\mid i\in\mathbb{Z}\}$$

如果很碰巧 G 中存在一个元素 a 使得 $G=\langle a\rangle$, 则称 G 是一个循环群.

很显然循环群中元素乘法交换, 是 Abel 群

例 2. 假设 $G=(\mathbb{Z},+)$, 则
$$\langle 3\rangle=\{3i\mid i\in\mathbb{Z}\}$$
注意, 这里 G 中的运算是 “+” , 因此命题6.1中的 a^m 在这里体现为
$$a+a+\cdots+a=ma$$
取 $a=1$, 我们有
$$\langle 1\rangle=\{i\mid i\in\mathbb{Z}\}=\mathbb{Z}$$
因此 $(\mathbb{Z},+)$ 是循环群.

我们再来看一个例子

例 3. 考虑二面体群 $D_n, n \geqslant 3$. 回忆下

$$D_n = \{e, \rho, \rho^2, \cdots, \rho^{n-1}, \tau_0, \cdots, \tau_{n-1}\}$$

其中 ρ 是绕原点逆时针旋转 $2\pi/n$.

这样一来, 对任意 $i \in \mathbb{Z}$, 令 r 为 i 模 n 的余数, 也就是说 $r \in [0, n-1]$ 且存在整数 q 使得 $i = qn + r$. 从而

$$\begin{aligned}\rho^i &= \rho^{qn}\rho^r \\ &= (\rho^n)^q\rho^r \\ &= e^q\rho^r = \rho^r\end{aligned}$$

也就是说

$$\langle\rho\rangle = \{e, \rho, \cdots, \rho^{n-1}\}$$

只有 n 个元素.

D_n 不可能是循环群, 因为它不是 Abel 群.

4 循环子群的阶数

上面我们看到循环子群的阶数 (元素个数) 既可以是无穷, 也可以有限, 那什么时候无穷, 什么时候有限呢? 有限的时候, 有多少个元素呢?

现在我们假设 G 是一个群, a 是 G 中元素. 那么只能出现下面两种情形:

情形 1: $a^i \neq a^j, \forall i \neq j$. 显然此时 $\langle a\rangle$ 有无穷多个元素.

情形 2: 存在 $i < j$ 使得 $a^i = a^j$. 两边同右乘以 a^{-i} 有

$$e = a^j a^{-i} = a^{j-i}$$

也就是说存在一个正整数 $j - i$ 使得

$$a^{j-i} = e$$

引理 6.2. *a 是群 G 中的一个元素, 如果存在 $m > 0$ 使得 $a^m = e$, 则*

$$\langle a\rangle = \{a^i \mid 0 \leqslant i \leqslant m-1\}$$

如果 m 是最小的正整数使得 $a^m = e$, 则

$$e, a, \cdots, a^{m-1}$$

互不相同.

证明. 只需要证明 $a^i \in \{e, a, \cdots, a^{m-1}\}$ 对所有的整数 $i \in \mathbb{Z}$ 成立. 由带余除法, 存在 $q \in \mathbb{Z}, 0 \leqslant r \leqslant m-1$ 使得

$$i = qm + r$$

从而

$$\begin{aligned}a^i &= a^{qm}a^r \\ &= (a^m)^q a^r \\ &= e^q a^r = a^r\end{aligned}$$

因此 $a^i \in \{e, a, \cdots, a^{m-1}\}$.

假设 m 是最小的满足 $a^m = e$ 的正整数. 如果 $\{e, a, \cdots, a^{m-1}\}$ 中有两个元素相同, 即存在 $0 \leqslant k < l \leqslant m-1$ 但 $a^k = a^l$. 这样一来 $a^{l-k} = e$, 与 m 的最小性矛盾.

5 元素的阶

由上面的讨论, 我们发现, 循环子群 $\langle a\rangle$ 的阶分为两种情况: **无穷和有限**.

推论 6.3. *$\langle a\rangle$ 有限当且仅当存在正整数 m 使得 $a^m = e$. 此时*

$$|\langle a\rangle| = \text{最小的正整数 } m \text{ 使得 } a^m = e$$

证明. 由上面的讨论, 一共分为两种情形. $\langle a\rangle$ 有限当且仅当情形 2 出现, 此时存在 $m > 0$ 使得 $a^m = e$.

反过来, 如果存在 $m > 0$ 使得 $a^m = e$, 引理6.2保证了 $\langle a\rangle$ 有限.

由引理6.2, 此时

$$|\langle a\rangle| = \text{最小的正整数 } m \text{ 使得 } a^m = e$$

定义 6.4. *为了叙述方便, 我们定义*

$$\mathrm{o}(a) := |\langle a\rangle|$$

称为元素 a 的阶(order).

显然当 $\mathrm{o}(a)$ 有限时, 它正好是使得 $a^m = e$ 的最小的正整数 m.

由于 $\langle a\rangle = \langle a^{-1}\rangle$, 因此 $\mathrm{o}(a) = \mathrm{o}(a^{-1})$.

引理 6.5. *(1) 一个循环群的子群还是循环群*

(2) 如果 $\mathrm{o}(a) = m$, 则 $a^i = e$ 当且仅当 $m \mid i$.

证明. (1) 假设 $\langle a\rangle$ 是一个循环群, 而 H 是 $\langle a\rangle$ 的非平凡子群. 从而存在 $k \neq 0$ 使得 $a^k \in H$, 此时 $a^{-k} \in H$. 因此, 总存在 $k > 0$ 使得 $a^k \in H$.

令 m 为正整数集合

$$S := \{k > 0 \mid a^k \in H\}$$

中的最小数. 那么对于任意 $a^i \in H$, 利用带余除法

$$i = qm + r, 0 \leqslant r < m$$

此时

$$a^r = a^{i-mq} = a^i (a^m)^{-q} \in H$$

由 m 的最小性得 $r = 0$. 因此

$$m \mid i,\ a^i = (a^m)^q \in \langle a^m \rangle$$

即 $H \subseteq \langle a^m \rangle$. 另一个方面, $a^m \in H$, 从而 $\langle a^m \rangle \subseteq H$. 所以 $H = \langle a^m \rangle$ 是循环群.

(2). 由于 m 是最小的使得 $a^m = e$ 的正整数, 如果 $a^i = e$, 利用与 (1) 类似的带余除法可证明 $m \mid i$. 反过来, 如果 $m \mid i$, 即 $i = mq$, 这时

$$a^i = (a^m)^q = e$$

方幂的阶

如果 $\mathrm{o}(a) = \infty$, 显然 $\mathrm{o}(a^r) = \infty$ 对所有的正整数 r 成立.

如果 $\mathrm{o}(a) = m$, n 是一个正整数, 那 $\mathrm{o}(a^n)$ 等于多少呢? 实际上

命题 6.6. *假设 $\mathrm{o}(a) = m$, n 是一个正整数, $d = (m, n)$ 为 m 与 n 的最大公因数. 则*

(1) $\langle a^n \rangle = \langle a^d \rangle$

(2) $\mathrm{o}(a^n) = m/d$

证明. 由于 n 是 d 的倍数 ($n = dq$), 所以

$$a^n = (a^d)^q \in \langle a^d \rangle$$

因此 $\langle a^n \rangle \subseteq \langle a^d \rangle$.

另一方面, 由于 d 是 m, n 的最大公因数, 因此存在整数 u, v 使得

$$mu + nv = d$$

因此

$$a^d = a^{mu} (a^n)^v = e (a^n)^v \in \langle a^n \rangle$$

从而 $\langle a^d \rangle \subseteq \langle a^n \rangle$.

(2) $\langle a^d \rangle$ 中元素恰为那些

$$a^i,\ 0 \leqslant i < m \text{ 且 } d \mid i$$

一共有 m/d 个. 因此

$$\mathrm{o}(a^n) = |\langle a^n \rangle| = |\langle a^d \rangle| = m/d$$

考虑 n 阶循环群 $\langle a \rangle$ 中元素的阶, 我们发现对于每个 $d \mid n$, a^i 的阶为 d, 当且仅当

$$(i, n) = \frac{n}{d}$$

当且仅当

$$i = k \cdot \frac{n}{d}$$

其中 k 与 d 互素, 这样的 a^i 取决于 k, 共有 $\varphi(d)$ 个, 这里 $\varphi(d)$ 为欧拉函数, 表示 $1, 2, \cdots, d$ 中与 d 互素的数的个数, 比如 $\varphi(1) = 1$, $\varphi(4) = 2$ 等. 因此 d 阶元的个数恰为 $\varphi(d)$, 由此可以得到

$$n = \sum_{d>0, d \mid n} \varphi(d)$$

利用命题6.6和引理6.5, 我们很容易给出循环群的所有子群. 比如, 如果 $\langle a \rangle$ 是一个 6 阶循环群, 则它的所有子群为

$$\{e\}, \langle a^2 \rangle, \langle a^3 \rangle, \langle a \rangle$$

分别有 1, 3, 2, 6 个元素.

乘积的阶

本期最后, 我们来看下如果群 G 中有两个元素 a, b. 它们的阶为

$$\mathrm{o}(a) = m, \mathrm{o}(b) = n$$

那么它们的乘积 ab 的阶是多少呢?

这个一般情况下是不太好确定的. 但是

命题 6.7. *若 $ab = ba$ 且 m, n 互素, 那么*

$$\mathrm{o}(ab) = mn$$

证明. 由于 $ab = ba$, 所以

$$(ab)^{mn} = a^{mn} b^{mn} = e$$

因此 $\mathrm{o}(ab)$ 有限. 由引理6.5(2), 我们有

$$\mathrm{o}(ab) \mid mn$$

现假设 $\mathrm{o}(ab) = k$, 则

$$(ab)^k = e$$

由于 $ab = ba$, 因此

$$a^k b^k = (ab)^k = e$$

从而 $a^k = b^{-k}$, 所以

$$\mathrm{o}(a^k) = \mathrm{o}(b^{-k}) = \mathrm{o}(b^k)$$

从而

$$\frac{m}{(k,m)} = \frac{n}{(k,n)}$$

因此

$$m(k,n) = n(k,m)$$

由于 $(m,n) = 1$, 因此

$$m \mid (k,m), n \mid (k,n)$$

从而

$$m \mid k, n \mid k$$

再次利用 $(m,n) = 1$ 得到 $mn \mid k$.

所以 mn 与 $\mathrm{o}(ab)$ 相互整除, 都是正整数, 两者相等.

注: 如果 m,n 不互素, 大家可能觉得 ab 的阶数应该是 m,n 的最小公倍数. 实际上这个一般情况下不对. 比如: 在一个 12 阶的循环群 $\langle x\rangle$ 中, 即 $\mathrm{o}(x) = 12$, 令

$$a = x^4, b = x^2$$

我们有

$$ab = ba, \mathrm{o}(a) = 3, \mathrm{o}(b) = 6$$

但是

$$\mathrm{o}(ab) = \mathrm{o}(x^6) = 2$$

7 Lagrange 定理

本期前言

从现在开始, 我们要牢记我们吹过的牛:

研究群的子群以及子群之间的关系

对于一个给定的有限群 G, 理论上我们可以把它的每一个子集拿来“审问”, 最终能在“有限”的时间内找出其所有的子群.

但问题在于一个集合的子集的个数经常是“浩瀚如烟”, 这样一个个的测试通常是不可行的. 更重要的是, 这样做对于数学家来说是种“侮辱”!

因此问题的关键在于如何“有效率”的找出子群. 本期我们就来讲讲这么一个简单而神奇的定理, 它的一个比较简单的形式是

定理 7.1 拉格朗日定理. 假设 G 是一个有限群, $H \leqslant G$. 则 H 的元素个数一定整除 G 的元素个数.

Motivating examples

假设 G 为循环群, 即存在 $a \in G$ 使得

$$G = \langle a\rangle$$

假设 $|G| = m$, 从上一期我们知道

- G 中的元素为
$$e, a, a^2, \cdots, a^{m-1}$$
- G 的子群还是循环群, 即形如
$$\langle a^k\rangle, 0 \leqslant k \leqslant m-1$$
- 对 $0 \leqslant k \leqslant m-1$, $d = (k,m)$. 则
$$\langle a^k\rangle = \langle a^d\rangle$$
共有 m/d 个元素.

由此, 我们发现:

循环 G 的子群的阶数都整除 G 的阶数!

另外一个例子还是我们“可爱”的二面体群 D_n 它不是循环群, 有 $2n$ 个元素

$$e, \rho, \cdots, \rho^{n-1}$$

$$\tau_0, \cdots, \tau_{n-1}$$

其中所有的旋转变换放在一起

$$\{e, \rho, \cdots, \rho^{n-1}\} = \langle \rho \rangle$$

是 D_n 的一个循环子群, 有 n 个元素, 当然整除 D_n 的阶数 $2n$.

现在如果考虑 D_n 的循环子群 $\langle a \rangle$, 其中 a 是 D_n 中的一个元素. 分两种情形:

情形 1: a 是一个旋转变换, 那么 $\langle a \rangle$ 中全部都是旋转变换, 即

$$\langle a \rangle \leqslant \langle \rho \rangle$$

因此 $|\langle a \rangle|$ 整除 $|\langle \rho \rangle| = n$, 从而整除 $|D_n| = 2n$.

情形 2:a 是一个翻折, 那么 $a^2 = e$, 从而

$$\langle a \rangle = \{e, a\}$$

只有 2 个元素, 显然 2 整除 $|D_n| = 2n$.

有了这些例子, 我们就可以大胆的问:

问题 3. 对于有限群 G, 是否其子群的阶数都整除 G 的阶数?

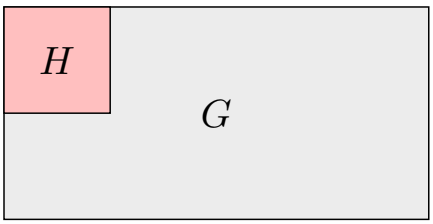
铺地砖

这一小节, 假设 G 是一个群 (不要求有限), 而 H 是 G 的一个子群.

针对上面这个问题, 我们采取铺地砖的策略:

试图用大小与 H 相同的 "地砖" 去铺满整个 G

第一块地砖非常好找, 就用 H



下一个 "地砖" 呢?

这是本期最关键的一个想法:

取任意元素 $a \in G$. 考虑

$$aH := \{ah \mid h \in H\}$$

它与 H 是否一样大呢?

实际上, 利用 a 是可逆的, 很容易证明

$$f_a : H \longrightarrow aH$$
$$h \mapsto ah$$

是双射.

H 本身也是这种形式: $H = eH$.

那么是不是可以用这些 aH 铺满整个 G 呢?

对于任意 $a \in G$, 我们都有

$$a = ae \in aH$$

因此这样的 "地砖" 确实可以铺满 G:

$$G = \bigcup_{a \in G} aH$$

现在 "地砖" 实在太多了, 每个 G 中的元素都会对应到一个 aH. 它们的并集又确实是整个 G, 只有一个可能

这些 "地砖" 之间可能有重叠的地方!

也就是说, 我们应该问

$$aH \cap bH = ?,\ a, b \in G$$

我们还是拿一个例子来找找感觉. 令 G 是一个 12 阶循环群, 由其一个元素 x 生成, 即

$$G = \{e, x, x^2, \cdots, x^{11}\}$$

记住 $x^{12} = e$. 假设

$$H = \langle x^3 \rangle = \{e, x^3, x^6, x^9\}$$

我们来看下这些 "地砖" 都什么样子.

$$eH = \{e, x^3, x^6, x^9\}$$
$$xH = \{x, x^4, x^7, x^{10}\}$$
$$x^2H = \{x^2, x^5, x^8, x^{11}\}$$
$$x^3H = \{x^3, x^6, x^9, x^{12} = e\}$$

我们发现 $x^3H = H$. 从上面的列表, 容易看出, 当 a 从 x^3 到 x^{11} 过程中, 上面这些 "地砖" 还是会重复出现.

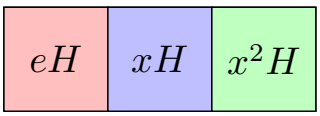
$$eH = x^3H = x^6H = x^9H$$
$$xH = x^4H = x^7H = x^{10}H$$
$$x^2H = x^5H = x^8H = x^{11}H$$

大家发现了什么? 大家有没有发现

- 两块 "地砖" 要么相等, 要么不相交
- 跟 "地砖" aH 相同的那些 "地砖" 恰为

$$bH, b \in aH$$

- 所有互不相同的 "地砖" 拼起来正好是 G



这会不会是一般的规律呢?

3 地砖（陪集）之间的关系

现在感觉不太好意思再说“地砖”了

定义 7.2. 假设 G 是一个群，H 是 G 的子群，那么“地砖”（最后一次）

$$aH, a \in G$$

称为 H 在 G 中的一个左陪集(left coset).

H 在 G 中的两个左陪集有啥关系呢?

命题 7.3. 假设 $H \leqslant G, a, b \in G$. 下面四条等价

1. $aH = bH$
2. $b \in aH$
3. $a^{-1}b \in H$
4. $aH \cap bH \neq \emptyset$

证明. $1 \Rightarrow 2$. $b = be \in bH = aH$

$2 \Rightarrow 3$. 由 2, 存在 $h \in H$ 使得

$$b = ah$$

两边左乘以 a^{-1} 得

$$a^{-1}b = a^{-1}ah = h \in H$$

$3 \Rightarrow 4$. 由 3, 存在 $h \in H$ 使得

$$a^{-1}b = h$$

所以

$$be = b = ah$$

等式左边属于 bH, 右边属于 aH. 因此

$$aH \cap bH \neq \emptyset$$

$4 \Rightarrow 1$. 假设

$$ah_1 = bh_2$$

属于 $aH \cap bH$, 其中 $h_1, h_2 \in H$. 那么对任意 $h \in H$, 我们有

$$ah = ah_1h_1^{-1}h = b(h_2h_1^{-1}h) \in bH$$

因此 $aH \subseteq bH$. 由于 a 与 b 对位对等, 同理可得 $bH \subseteq aH$.

仔细琢磨下这个命题中 1 和 4, 意思就是 H 在 G 中的**两个左陪集相等当且仅当它们交集非空!**

这说明

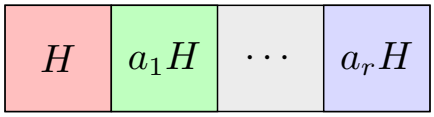
H 的两个陪集要么相等, 要么交集为空集!

由于 G 中每个元素 a 都必须在其中一个左陪集中(至少在 aH 中), 因此, 所有这些左陪集放在一起确实可以铺满整个 G.

$$G = \cup_{a \in G} aH$$

总结一下, 我们得到了一些大小跟 H 一致的左陪集, 不同的左陪集之间交集为空, 它们全部并起来还等于 G.

整体印象



G

4 拉格朗日定理

我们记

$$G/H := \{aH \mid a \in G\}$$

为 H 在 G 中的左陪集的全体. 左陪集的个数

$$[G : H] := |G/H|$$

称为子群 H 在 G 中的指数(index).

由前面的讨论我们可以得到

定理 7.4 拉格朗日定理. 假设 G 是一个有限群, $H \leqslant G$, 那么

$$|G| = [G : H] \cdot |H|$$

特别的

$$|H| \text{ 和 } [G : H] \text{ 都整除 } |G|.$$

5 元素的阶数

如果考虑群 G 循环子群 $\langle a \rangle$, 由拉格朗日定理, 它的阶数

$$|\langle a \rangle| = \mathrm{o}(a)$$

也必须整除 G 的阶数. 即

推论 7.5. 假设 G 是一个有限群, 那么 G 中元素的阶数都整除 G 的阶数 $|G|$.

也就是说, 如果 G 有 6 个元素, 那么 G 中元素的阶数只可能是 $1, 2, 3, 6$.

Warning: 这里并没有说 G 中 $2,3,6$ 阶元素都存在. 比如:

$$S_3=\{e,(12),(13),(23),(123),(132)\}$$

阶数是 6, 但其中只有 $1,2,3$ 阶元, 没有 6 阶元.

6 素数阶的群

还有一个比较特殊的情况是

$$|G|=p \text{ 是个素数}$$

令 $a\in G$ 不是单位元.

由推论7.5, $\mathrm{o}(a)$ 只能是 p 的因数: 1 或者 p.

但是 $a\neq e$, 因此 $\mathrm{o}(a)\neq 1$.

所以, $\mathrm{o}(a)$ 只能是 p, 从而 $\langle a\rangle\subseteq G$ 有 p 个元素.

但 G 总共也只有 p 个元素, 所以 $G=\langle a\rangle$, 是一个循环群, 也就是下面这个推论

推论 7.6. *素数阶群都是循环群.*

大家可以想像下, 如果没有拉格朗日定理, 是不是很难想像素数阶的群都是循环群?

7 右陪集

其实我们也可以考虑右陪集

$$Ha, a\in G$$

它们同样跟 H 有同样的大小:

$$\begin{aligned} g_a: H &\longrightarrow Ha\\ h &\mapsto ha \end{aligned}$$

是双射. 所有右陪集的全体记为

$$H\backslash G:=\{Ha\mid a\in G\}$$

作为练习, 大家可以证明

$$\begin{aligned} Ha=Hb&\Leftrightarrow ab^{-1}\in H\\ &\Leftrightarrow Ha\cap Hb\neq\emptyset \end{aligned}$$

大家注意到这里跟左陪集有点不一样

$$aH=bH\Leftrightarrow b^{-1}a\in H$$

$$Ha=Hb\Leftrightarrow ab^{-1}\in H$$

由于 H 对取逆封闭, 因此

$$\begin{aligned} ab^{-1}\in H&\Leftrightarrow (ab^{-1})^{-1}\in H\\ &\Leftrightarrow (b^{-1})^{-1}a^{-1}\in H\\ &\Leftrightarrow b^{-1}H=a^{-1}H. \end{aligned}$$

因此

$$Ha=Hb\Leftrightarrow a^{-1}H=b^{-1}H$$

利用这点, 可以证明

$$\begin{aligned} \theta: H\backslash G &\longrightarrow G/H\\ Ha &\mapsto a^{-1}H \end{aligned}$$

是一个双射, 也就是说 H 的左陪集的个数与右陪集的个数相同!

8 从等价关系方向看

如果在 G 上定义关系

$$a\sim b\Leftrightarrow a^{-1}b\in H$$

可以证明 "$\sim$" 是 G 上的一个等价关系, 而左陪集 aH 恰为 a 在关系 "$\sim$" 下的等价类, 即

$$\begin{aligned} aH&=\{x\in G\mid a\sim x\in H\}\\ &=\{x\in G\mid a^{-1}x\in H\} \end{aligned}$$

由等价关系的知识, 我们知道等价 "$\sim$" 给出 G 的一个划分, 即:

G 可以写成这些等价类的并, 且不同的等价类交集为空集.

从这里也能得到拉格朗日定理.

9 是拉格朗日证明的吗?

实际上拉格朗日并没有证明这个最一般的版本, 他在 1771 年证明了一件很有趣的事情.

给定一个 n 元多项式 $f(x_1,\cdots,x_n)$, 用 S_n 里面元素去置换 x_i 的位置, 即

$$\sigma f(x):=f(x_{\sigma(i)},\cdots,x_{\sigma(n)})$$

你会得到很多不同的多项式, 比如 $x_1+x_2-x_3$, 用 (13) 来置换就得到

$$x_3+x_2-x_1$$

当然, 有时候你也会得到跟原来同样的式项式, 比如用 (12) 来置换上面的多项式就得到

$$x_2 + x_1 - x_3$$

与原多项式相等.

拉格朗日证明了: 对于任意 n 元多项式 f, 通过置换得到的所有不同的多项式的个数总是整除 $n!$. 换成现在的语言是:

$$令\ H := \{\sigma \in S_n \mid \sigma f = f\}, 则$$
$$[S_n : H] \mid |S_n|$$

这在后面讲群作用的时候会讲到. 实际上, 在映射

$$S_n \longrightarrow \{\sigma f \mid \sigma \in S_n\}$$

中, 两个 $\sigma, \tau \in S_n$ 对应的多项式相等 ($\sigma f = \tau f$) 当且仅当

$$\sigma^{-1}\tau \in H$$

当且仅当 σ, τ 在同一个左陪集中 ($\sigma H = \tau H$). 这样 $\{\sigma f \mid \sigma \in S_n\}$ 中不同多项式的个数就等于 H 在 S_n 中的左陪集的个数, 即指数 $[S_n : H]$. 由拉格朗日定理, 指数整除对称群的阶数 $n!$.

比如上面的 $x_1 + x_2 - x_3$ 通过置换总共可以得到 3 个不同的多项式

$$x_1 + x_2 - x_3$$
$$x_2 + x_3 - x_1$$
$$x_1 + x_3 - x_2$$

后来柯西 (Cauchy) 证明了对称群的情形 (1844), 最终 1861 年, Jordan 证明了所有的情形.

下期继续我们的寻找子群之旅.

8 正规子群

本期前言

让我们牢记曾经发过的那个该死的誓言

研究群的子群和子群之间的关系

并继续我们的寻找子群之旅!

共轭子群

当你费劲全身力气找到一个子群的时候, 一定要尽量顺藤摸瓜的把它的兄弟姐妹都找出来.

给定一个有限群 G, 假设我们已经找到它的一个子群 H. 问之:

"你的兄弟姐妹子群呢? 有没有?"

H 很气愤的说: "上期你们把我的那些陪集都抓去了, 还不满足吗?"

对哈, 上次我们找到那么多陪集, 里面会不会有些也是子群呀? 回顾一下, H 在 G 中的左陪集:

$$aH = \{ah \mid h \in H\}, a \in G$$

上期我们知道

- 两个左陪集要么相等, 要么不相交
- $aH = bH$ 相等当且仅当 $b \in aH$
- $H = eH$ 也是左陪集

看到这几条, 会不会觉得很生气? 这些左陪集里面除了 H 以外, 根本就没有子群!

啊? 为啥呢?

你看嘛, 如果 $aH \neq H$, 也就是说 $aH \neq eH$, 由上面中间那一条, $e \notin aH$. 单位元都没有, 怎么会是子群呢?

再把 H 抓来揍一顿, H 实在受不了, 有气无力的说: "你们不会动动脑筋呀? aH 没有单位元, 你在右边再乘以 a^{-1} 不就有单位元了?"

对哈, 我怎么没想到, 看看

$$aHa^{-1} := \{aha^{-1} \mid h \in H\}$$

任取 aHa^{-1} 中两个元素

$$x = ah_1a^{-1}, y = ah_2a^{-1}$$

看下 xy^{-1} 是不是还在 aHa^{-1} 中.

$$\begin{aligned} xy^{-1} &= ah_1a^{-1}(ah_2a^{-1})^{-1} \\ &= ah_1a^{-1}(ah_2^{-1}a^{-1}) \\ &= a(h_1h_2^{-1})a^{-1} \end{aligned}$$

由于 $h_1, h_2 \in H$, 而 H 是 G 的子群, 因此

$$h_1h_2^{-1} \in H$$

从而

$$a(h_1h_2^{-1})a^{-1} \in aHa^{-1}$$

也就是说 aHa^{-1} 中任意两个元素 x, y, 都有

$$xy^{-1} \in aHa^{-1}$$

因此, 由我们在第 3 期的定理 5, 可得 aHa^{-1} 是 G 的子群.

哇! 终于钩到一个大鱼, 原来 H 后面藏着这么多其他子群呢

定义 8.1. 假设 H 是群 G 的一个子群, $a \in G$. 那么

$$aHa^{-1} \text{ 也是 } G \text{ 的子群,}$$

称为 H 在 G 中的共轭子群.

两瓢凉水

正在沾沾自喜的时候, 一个 Abel 群走过来:

"听说你们找到了一个子群的很多共轭子群, 我也有一个子群 H, 你们能不能帮我找找它的共轭子群呀？"

"放心吧, 这就开工!"

就是说 G 是 Abel 群, 而 $H \leqslant G$. 取 $a \in G$

$$\begin{aligned} aHa^{-1} &= \{aha^{-1} \mid h \in H\} \\ &= \{haa^{-1} \mid h \in H\} \ (G \text{ 是 Abel 群}) \\ &= \{h \mid h \in H\} = H \end{aligned}$$

呃？ 怎么还是 H?

S_3 也走了过来: "我那个由 (123) 生成的子群有没有共轭子群呀?"

啊？ 我看看先

$$H := \langle (123) \rangle = \{e, (123), (132)\}$$

一共三个元素, 一个单位元, 两个 3 循环.

我们知道 S_3 一共 6 个元素, 其他 3 个元素

$$(12), (13), (23)$$

都是 2 循环.

取 $\sigma \in S_3$

$$\sigma H\sigma^{-1} = \{\sigma e\sigma^{-1}, \sigma(123)\sigma^{-1}, \sigma(132)\sigma^{-1}\}$$

还记得吗？ 第 4 期定理 7 说的

$$\sigma(i_1 \cdots i_k)\sigma^{-1} = (\sigma(i_1), \cdots, \sigma(i_k))$$

就是说一个 k 循环被 σ 共轭以后还是 k 循环. 如果这样的话, $\sigma H\sigma^{-1}$ 还是一个单位元和两个 3 循环.

但 S_3 的这样的子集只有 $\langle (123) \rangle$. 也就是说

$$\sigma H\sigma^{-1} = H$$

呃？ 上面两种情形下 H 都没有与之共轭的其他子群!

定义 8.2. 假设 G 是一个群, H 是 G 的子群. 如果 G 中与 H 共轭的子群只有 H, 即

$$aHa^{-1} = H, \forall a \in G$$

则称 H 为 G 的一个正规子群 (normal subgroup), 记作:

$$H \lhd G$$

从上面的讨论可以看出:

任何 Abel 群的子群都是正规子群

爱恨交加

当我们发现一个子群是正规子群的时候, 是喜欢还是讨厌呢？

有人肯定会说, 当然是讨厌啦! 本来想通过共轭找到别的子群的, 这个群无论怎么共轭都是它自己, 你说气不气人？

但是我要说, 我们应该喜欢正规子群. 大家还记得我们第 3 期定理 6 中多项式 $f(x)$ 的 Galois 群 $\mathrm{Gal}(f)$ 满足什么条件方程 $f(x) = 0$ 才可以根式解吗？

回顾一下, 要满足的条件是:

G 是可解群, 即存在子群序列

$$\{e\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

满足: 对于任意 $i = 0, \cdots, n-1$

$$abG_{i+1} = baG_{i+1}, \forall a, b \in G_i$$

这里恰恰要求 G_{i+1} 是 G_i 的正规子群呀.

Warning:G_{i+1} 不一定是 G 的正规子群

4 正规子群的判定

对于群 G 的任意非空子集 X,Y, 我们定义

$$XY=\{xy\mid x\in X,y\in Y\}$$

比如, 向量空间 V 的两个子空间 U,W, 它们的和空间 $U+W$ 就是这种形式. 对于 G 的非空子集 X, 以及子群 $H\leqslant G$, 由于 $e\in H$, 因此

$$X\subseteq XH, X\subseteq HX$$

正规子群的几个等价条件如下:

定理 8.3. 假设 H 是群 G 的子群, 则下面几条等价

1. $aHa^{-1}=H,\forall a\in G$ (即 $H\lhd G$)
2. $aHa^{-1}\subseteq H,\forall a\in G$
3. $aH=Ha,\forall a\in G$
4. 对任意 $a,b\in G$, $(aH)(bH)=abH$

证明. $1\Rightarrow 2.$ 显然

$2\Rightarrow 3.$ 对任意 $h\in H$, $a\in G$, 由 2 得

$$aha^{-1}\in H$$

因此

$$ah=(aha^{-1})a\in Ha$$

所以 $aH\subseteq Ha$. 反过来由 2 得

$$a^{-1}ha=a^{-1}h(a^{-1})^{-1}\in H$$

从而

$$ha=a(a^{-1}ha)\in aH$$

所以 $Ha\subseteq aH$. 最终我们得到 $aH=Ha$.

$3\Rightarrow 4.$ 对任意 $h\in H$, 有

$$abh=(ae)(bh)\in(aH)(bH)$$

所以 $abH\subseteq(aH)(bH)$. 反过来, 对任意 $h_1,h_2\in H$, 由 3, 存在 $h_3\in H$, 使得 $h_1b=bh_3$, 从而

$$(ah_1)(bh_2)=a(h_1b)h_2=abh_3h_2\in abH$$

所以 $(aH)(bH)\subseteq abH$.

$4\Rightarrow 1.$ 对任意 $a\in G$, 根据 4 有

$$aHa^{-1}\subseteq aHa^{-1}H=(aa^{-1})H=H$$

$$a^{-1}Ha\subseteq a^{-1}HaH=(a^{-1}a)H=H$$

由第二个式子可得

$$H\subseteq aHa^{-1}$$

从而有 $aHa^{-1}=H$.

定理8.3的第 3 条有一个很有意思的推论

推论 8.4. 假设 H 是群 G 的一个子群.
如果 $[G:H]=2$, 则 $H\lhd G$.

证明. 我们证明

$$aH=Ha,\forall a\in G$$

如果 $a\in H$, 那么 $aH=H=Ha$.

如果 $a\notin H$, 则

$$aH\neq H, Ha\neq H$$

由上一期的内容, 两个左陪集不相同则交集为空, 对右陪集也正确. $H=eH=He$ 既是左陪集也是右陪集. 因此

$$aH\cap H=\emptyset=H\cap Ha$$

但是 $[G:H]=2$, 意味着

$$H, aH \text{ 是仅有的两个 } H \text{ 的左陪集}$$

$$H, Ha \text{ 是仅有的两个 } H \text{ 的右陪集}$$

所以

$$H\cup aH=G=H\cup Ha$$

因此 aH 和 Ha 都是 H 在 G 中的补集, 所以

$$aH=Ha.$$

由定理8.3第 3 条知 H 是 G 的正规子群.

由这个推论我们知道 S_n 中由所有偶置换组成的子群 A_n 是 S_n 的正规子群 (因为 $[S_n:A_n]=2$)

5 正规子群的几个基本事实

关于正规子群, 我们有下面一些基本的事实.

命题 8.5. 假设 G 是一个群.

1. $\{e\}$ 和 G 都是 G 的正规子群
2. G 的中心(center)
   $C(G):=\{x\in G\mid ax=xa,\forall a\in G\}$
   是 G 的正规子群.
3. 若 $N\leqslant H\leqslant G$ 且 $N\lhd G$, 那么 $N\lhd H$

证明留作练习. 这里我们对第 3 条稍微解释下, 第 3 条中 N 是 G 的正规子群, 说明 G 中的元素共轭在 N 上还是 N, 即

$$aNa^{-1}=N,\forall a\in G$$

由于 $H\leqslant G$ 是 G 的一部份, 因此 H 中的元素共轭在 N 上还是 N.

6 展望下期

正规子群还有哪些好处呢？下期将详细讨论这个话题.

最后做点小练习

练习 4. 1. 证明: $K_4 := \{e, (12)(34), (13)(24), (14)(23)\}$ 是 S_4 的正规子群.

2. 证明: 在 D_n 中, 所有的旋转变换组成的子群是 D_n 的正规子群.

3. 证明: $\mathrm{SL}_n(\mathbb{R})$ 是 $\mathrm{GL}_n(\mathbb{R})$ 的正规子群.

9 商群

本期前言

一开始, 我们看正规子群特别不顺眼 (它没有其他与之共轭的子群), 但后来我们发现要说明一个群的可解群恰恰需要正规子群.

本期我们继续讨论正规子群的可爱之处.

1 子群的乘积

在我们学习向量空间的时候, 给定一个向量空间 V 的两个子空间 U 和 W, 可以将它们两个 “加” 起来

$$U + W := \{u + w \mid u \in U, w \in W\}$$

它也是 V 的子空间.

对比一下, 我们看下群的情况

假设 G 是一个群, H, K 是 G 的两个子群, 那么能不能把它们 “加” 起来得到 G 的子群呢？

向量空间上的运算是加法, 所以可以 “加” 起来, 而群 G 的运算如果是 “$\cdot$” , 我们只能把 H 和 K “$\cdot$” 起来.

$$H \cdot K = \{h \cdot k \mid h \in H, k \in K\}$$

那它是不是还是 G 的子群呢？

来看个例子.

$$G = S_3$$
$$H = \langle (12) \rangle = \{e, (12)\}$$
$$K = \langle (13) \rangle = \{e, (13)\}$$

那 HK 是啥呢？

$$HK = \{e, (12), (13), (132)\}$$

一共 4 个元素, 不可能是 S_3 (6 个元素) 的子群. (为啥?)

这说明将群 G 两个子群 “乘” 起来一般情况下得不到 G 的子群. 但是

命题 9.1. 假设 G 是一个群, H 是 G 的子群, N 是 G 的正规子群, 那么

$$HN \text{ 和 } NH$$

都是 G 的子群.

证明. 现在 N 是 G 的正规子群, 也就是说

$$ana^{-1} \in N, \forall n \in H, a \in G$$

如果我们任取 HN 中两个元素

$$h_1n_1 \text{ 和 } h_2n_2$$

其中 $h_1, h_2 \in H$, $n_1, n_2 \in N$, 则有

$$\begin{aligned} &h_1n_1(h_2n_2)^{-1} \\ =&h_1n_1(n_2^{-1}h_2^{-1}) \\ =&h_1(h_2^{-1}h_2)n_1(n_2^{-1}h_2^{-1}) \\ =&h_1h_2^{-1}(h_2n_1n_2^{-1}h_2^{-1}) \end{aligned}$$

这里 $n_1n_2^{-1} \in N$, 被 h_2 共轭后还属于 N, 即

$$h_2n_1n_2^{-1}h_2^{-1} \in N$$

另外由于 H 是 G 的子群, 因此

$$h_1h_2^{-1} \in H$$

从而

$$h_1h_2^{-1}(h_2n_1n_2^{-1}h_2^{-1}) \in HN$$

即

$$h_1n_1(h_2n_2)^{-1} \in HN$$

总结起来, 我们任取 HN 中两个元素

$$h_1n_1 \text{ 和 } h_2n_2$$

证明了

$$h_1n_1(h_2n_2)^{-1} \in HN$$

由第 3 期定理 5 得 HN 是 G 的子群.

类似的可以证明 NH 也是 G 的子群.

通过证明大家可能发现, 对于 G 的两个子群 H 和 N, 实际上只要 H 中的元素共轭在 N 上还在 N 里面, 即

$$hNh^{-1} \subseteq N, \forall h \in H$$

就有 HN 和 NH 是 G 的子群.

如果它们都是正规子群呢?

命题 9.2. 如果 H, N 都是 G 的正规子群, 则 $HN \lhd G$.

证明. 如果 H, N 都是 G 的正规子群, 由上面的证明已经知道 HN 和 NH 都是 G 的子群. 只需要证明其为正规子群.

对于任意 $hn \in HN$, 其中 $h \in H, n \in N$, $a \in G$, 则

$$\begin{aligned} ahna^{-1} =&ah(a^{-1}a)na^{-1} \\ =&(aha^{-1})(ana^{-1}) \end{aligned}$$

由于 H 和 N 都是正规子群, 因此

$$aha^{-1} \in H, ana^{-1} \in N$$

所以

$$ahna^{-1} = (aha^{-1})(ana^{-1}) \in HN$$

即 HN 中元素在 G 中任意元素 a 的共轭下依然还在 HN 中, 所以 $HN \lhd G$.

2 群的直积

由上面的讨论, 如果把向量空间跟群做一个对比的话, 子空间应该对应到正规子群.

向量空间 V 的两个子空间 U 和 W, 如果

$$U \cap W = \{0\}, \text{我们有}$$

$$U + W = U \oplus W$$

是 U 和 W 的直和, 即 $U + W$ 中的元素可唯一分解为

$$u + w,\ u \in U, w \in W$$

形式. 群这里有没有这样性质呢? 实际上

命题 9.3. 假设 H 和 N 都是群 G 的正规子群且

$$H \cap N = \{e\}, \text{则}$$

(1) 对任意 $h \in H, n \in N$ 有 $hn = nh$.

(2) HN 中的元素可唯一分解为

$$hn, h \in H, n \in N$$

形式.

证明. (1). 考虑

$$hnh^{-1}n^{-1}$$

如果你把前三个元素组合在一起

$$(hnh^{-1})n^{-1}$$

发现前面括号里的元素是 h 共轭在一个 N 中的元素上, 由于 N 是正规子群, 因此

$$hnh^{-1} \in N$$

从而

$$(hnh^{-1})n^{-1} \in N$$

如果你把后三个元素组合在一起

$$h(nh^{-1}n^{-1})$$

你会发现后面括号里的元素还在 H 中, 从而

$$h(nh^{-1}n^{-1}) \in H$$

因此

$$hnh^{-1}n^{-1} \in H \cap N$$

但 $H \cap N = \{e\}$, 因此

$$hnh^{-1}n^{-1}=e$$

即 $hn=nh$.

(2). 假设某个元素有两种分解

$$hn=h_1n_1$$

两边左乘 h^{-1}, 右乘以 n_1^{-1}, 则有

$$nn_1^{-1}=h^{-1}h_1$$

左边属于 N, 右边属于 H, 但 $H\cap N=\{e\}$, 所以

$$nn_1^{-1}=e=h^{-1}h_1$$

从而有

$$n=n_1, h=h_1$$

因此 HN 中人元素都能唯一分解成

$$hn, h\in H, n\in N$$

的形式.

在命题9.2的情形下, 由唯一性, HN 的元素

$$hn, h\in H, n\in N$$

在 h 或者 n 的取法不同时, 结果 hn 也不同. 因此, 当 H, N 都是有限子群时, HN 的阶数 (元素个数) 为

$$|HN|=|H|\cdot|N|$$

恰好与 H 与 N 的笛卡尔乘积

$$H\times N:=\{(h,n)\mid h\in H, n\in N\}$$

元素个数相同.

命题9.3中的情形下, HN 称为 H 与 N 的直积.

在学习向量空间的时候, 任意两个向量空间 V 和 W, 它们的笛卡尔乘积 $V\times W$ 构成一个向量空间.

那上面的 H 与 N 的笛卡尔乘积是否也可以构成一个群呢?

命题 9.4. *H 和 G 为群, 则它们的笛卡尔乘积*

$$H\times G:=\{(h,g)\mid h\in H, g\in G\}$$

在运算

$$(h_1,g_1)(h_1,g_2):=(h_1h_2,\ g_1g_2)$$

下构成群. 称为 H 和 G 的外直积.

这个命题只需要简单验证下即可证明, 我们留作练习. 其单位元是 (e_H,e_G), 其中 e_H 和 e_G 分别是 H 和 G 的单位元.

思考下命题9.3中的 HN 和 $H\times N$ 有什么关系?

陪集成群—商群

上一期, 群 G 的子群 N 是 G 的正规子群有一个等价条件是:

> 对任意 $a,b\in G$, 两个陪集 aN, bN 作为 G 的子集, 它们的乘积满足
>
> $$aN\cdot bN=abN$$

这个对于非正规子群是不成立的. 比如

$$H=\{e,(12)\}\leqslant S_3$$

我们取它的两个左陪集

$$(13)H=\{(13),(13)(12)=(123)\}$$
$$(23)H=\{(23),(23)(12)=(132)\}$$

通过计算可以发现

$$(13)H(23)H=\{(132),(13),e\}$$

共有 3 个元素, 但是

$$(13)(23)H$$

只有两个元素. 所以

$$(13)H(23)H\neq(13)(23)H$$

因此, 正规子群 N 的所有左陪集放在一起

$$G/N=\{aN\mid a\in G\}$$

它上面有个乘法

$$aN\cdot bN=abN$$

有没有单位元呢?

$$N\cdot aN=eaN=aeN=aN\cdot N$$

因此这个乘法的单位元就是 N.

每个元素都有逆元?

$$aN\cdot a^{-1}N=aa^{-1}N=eN=N$$
$$a^{-1}N\cdot aN=a^{-1}aN=eN=N$$

因此 aN 在此乘法下的逆元就是 $a^{-1}N$.

这个乘法还是结合的 这个不用验证了吧.

因此 G/N 在这个乘法下真的构成群! 它的单位元就是 N 这个左陪集. G/N 称为 G 关于 N 的商群(quotient group).

例 4. $G=\mathbb{Z}$, $N=n\mathbb{Z}, n>0$. 由于 $\mathbb{Z}$ 是 Abel 群, 因此 $n\mathbb{Z}$ 是 $\mathbb{Z}$ 的正规子群. N 在 G 中的左陪集都形如

$$i+n\mathbb{Z}\ (\text{注意 }\mathbb{Z}\text{ 中运算为加法})$$

恰为与 i 模 n 同余的所有整数组成的集合. 为简便, 我们记

$$[i] := i + n\mathbb{Z}$$

并且

$$[i] + [j] = [i + j]$$

我们把 $\mathbb{Z}/n\mathbb{Z}$ 记为 $\mathbb{Z}_n$, 它有 n 个元素

$$[0], [1], \cdots, [n-1]$$

单位元是 $[0]$. 它还是一个循环群 (由 $[1]$ 生成).

可解群的正式定义

我们再来回顾可解群的描述.

定义 9.5. 有限群 G 是可解群, 如果存在子群序列

$$\{e\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

使得对于所有 $i = 0, \cdots, n-1$ 有

$$abG_{i+1} = baG_{i+1}, \forall a, b \in G_i$$

现在 G_{i+1} 是 G_i 的正规子群, 因此

$$abG_{i+1} = baG_{i+1}, \forall a, b \in G_i$$

等于说

$$G_i/G_{i+1} \text{ 是 Abel 群!}$$

因此, 可解群的正式定义就出炉了

定义 9.6. 有限群 G 是可解群, 如果存在子群序列

$$\{e\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

使得对于所有 $i = 0, \cdots, n-1$

$$G_i/G_{i+1} \text{ 是 Abel 群.}$$

10 第一同构定理

本期前言

这一期讲述群论中简单又极为重要的定理

群同态基本定理

群的同构

不知道大家注意到没有, 前面我们讲到的一些群的例子是很 “相似” 的, 比如

$$\langle \rho \rangle \leqslant D_3$$

$$\mathbb{Z}_3 = \mathbb{Z}/3\mathbb{Z}$$

它们都是 3 阶循环群. 元素分别是

$$\langle \rho \rangle = \{e, \rho, \rho^2\}$$

$$\mathbb{Z}_3 = \{[0], [1], [2]\}$$

考虑对应

$$\phi : \mathbb{Z}_3 \longrightarrow \langle \rho \rangle$$

$$[0] \mapsto e$$

$$[1] \mapsto \rho$$

$$[2] \mapsto \rho^2$$

我们很容易发现, 这个对应是与两边群的运算是协调的. 比如: 左边

$$[1] + [2] = [0]$$

右边

$$\rho\rho^2 = \rho^3 = e$$

即

$$\phi([1] + [2]) = \phi([1])\phi([2])$$

一般的, 假设

$$(G, \cdot) \text{ 和 } (H, *)$$

是两个群, 如果有一个双射

$$\phi : G \longrightarrow H$$

与 G 和 H 中的运算协调一致, 即

$$\phi(a \cdot b) = \phi(a) * \phi(b)$$

对所有 $a, b \in G$ 成立, 这时感觉 G 和 H 本质上是差不多的, 称 ϕ 为群 G 到 H 的一个同构(isomorphism). 此时称 G 与 H 同构, 记作

$$G \simeq H$$

这种情况下 G 和 H 的结构是一致的，它们的子群也是一一对应的，G 有某种性质 (比如可解) 当且仅当 H 具有同样的性质.

需要指出的是，并不是所有同构的群都这么容易看出来，有时候会隐藏得比较深，不容易看出来. 比如

$$\mathrm{SL}_n(\mathbb{R}) \text{ (行列式为 1 的 } n \text{ 阶实方阵)}$$

是

$$\mathrm{GL}_n(\mathbb{R}) \text{ (n 阶可逆实矩阵)}$$

的正规子群，对应的商群

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \text{ 与 } (\mathbb{R}^*, \cdot)$$

是同构的，但好像一下子看不出来.

又比如

$$K_4 = \{e, (12)(34), (13)(24), (14)(23)\}$$

是 S_4 的正规子群，你看得出来对应的商群

$$S_4/K_4 \text{ 与 } S_3$$

是同构的吗？下面要讲的方法将会让你很快看出来上面两组群确实是同构的.

2 群的同态

在学习向量空间的时候，我们除了考虑向量空间的同构，很多时候我们还需要考虑向量空间之间的线性映射.

回顾下，假设 V, W 是 $\mathbb{R}$ 上向量空间，映射

$$\sigma : V \longrightarrow W$$

称为一个线性映射，如果

$$\sigma(v_1 + v_2) = \sigma(v_1) + \sigma(v_2)$$
$$\sigma(kv) = k\sigma(v)$$

对所有 $v, v_1, v_2 \in V$, $k \in \mathbb{R}$ 成立. 也就是说 σ 保持向量的加法和数乘.

定义 10.1. 对于群 $(G, \cdot)$ 和 $(H, *)$ 而言，如果一个映射

$$\phi : G \longrightarrow H$$

满足

$$\phi(a \cdot b) = \phi(a) * \phi(b)$$

对所有的 $a, b \in G$ 成立，则称 ϕ 为一个群同态(group homomorphism)

与群同构相比，这里我们不再要求 ϕ 是双射.

可谓“退一步海阔天空”，没有了“双射”这个包袱，就很容易建立两个群之间的群同态. 比如:

$$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$i \mapsto [i]$$
$$\det : \mathrm{GL}_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$$
$$A \mapsto \det(A)$$

肯定很多人心里在打鼓，这又有什么用呢？

我们不妨看看一个群同态到底有什么特点.

现在开始，为记号方便，我们假设群 G 和 H 中的运算都是乘法，并略去不写.

假设

$$\phi : G \longrightarrow H$$

是群同态. 下面开一个简短的发布会.

群同态简短发布会实录

问 1: ϕ 你把单位元 e_G 映到哪里去了?

$$\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G)$$

因此

$$\phi(e_G)e_H = \phi(e_G)\phi(e_G)$$

两边左乘以 $\phi(e_G)^{-1}$, 得

$$e_H = \phi(e_G)$$

所以 ϕ 将 e_G 映为 e_H.

问 2: ϕ 把 G 中元素 a 的逆元映到哪里去了?

$$\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e_G) = e_H$$

因此

$$\phi(a^{-1}) = \phi(a)^{-1}$$

由问 1 和问 2, 其实就可以发现

命题 10.2. 假设

$$\phi : G \longrightarrow H$$

是一个群同态, K 是 G 的子群, 则 $\phi(K)$ 是 H 的子群. 特别的, ϕ 的像集 $\mathrm{Im}\,\phi$ 是 H 的子群.

证明. 任取

$$\phi(a), \phi(b) \in \phi(K)$$

其中 $a, b \in K$, 有

$$\phi(a)\phi(b)^{-1} = \phi(a)\phi(b^{-1}) \text{ (由问 2)}$$
$$= \phi(ab^{-1}) \text{ (ϕ 保运算)}$$

由于 $K \leqslant G$, 因此

$$ab^{-1} \in K$$

从而

$$\phi(a)\phi(b)^{-1} = \phi(ab^{-1}) \in \phi(K)$$

所以 $\phi(K) \leqslant H$.

还有一个问题.

问 3: 什么时候 ϕ 是单射?

大家肯定问,这还有啥好说的,ϕ 是单射的时候自然就是单射.

回想线性映射的时候,一个线性映射 σ 是单射只要看零向量的原像是不是只有零向量就行了. 群同态是否有类似的事情呢?

命题 10.3. 一个群同态

$$\phi : G \longrightarrow H$$

是单射当且仅当

$$\operatorname{Ker}\phi := \{a \in G \mid \phi(a) = e_H\}$$

只包含 e_G 一个元素.

这里 $\operatorname{Ker}\phi$ 称为 ϕ 的Kernel.

证明. 如果 ϕ 是单射,e_H 当然只能有一个原像 (由问 1,我们知道它有个原像是 e_G),即

$$\operatorname{Ker}\phi = \{e_G\}$$

反过来,如果 $\operatorname{Ker}\phi = \{e_G\}$, 即 e_G 是 e_H 在 ϕ 下唯一的原像.

现假设 $a, b \in G$ 满足

$$\phi(a) = \phi(b)$$

则

$$\begin{aligned}\phi(ab^{-1}) &= \phi(a)\phi(b^{-1}) \text{ (因为 } \phi \text{ 是群同态)}\\ &= \phi(a)\phi(b)^{-1} \text{ (由问 2)}\\ &= e_H\end{aligned}$$

所以

$$ab^{-1} \in \operatorname{Ker}\phi$$

由于 $\operatorname{Ker}\phi = \{e_G\}$, 所以

$$ab^{-1} = e_G$$

$$a = b$$

所以 ϕ 是单射.

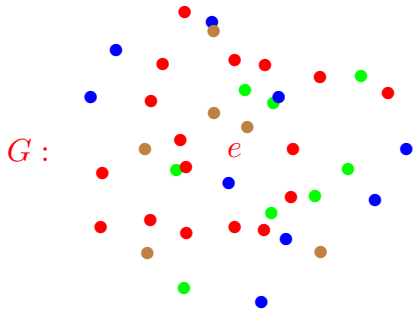
3 第一同构定理

假设

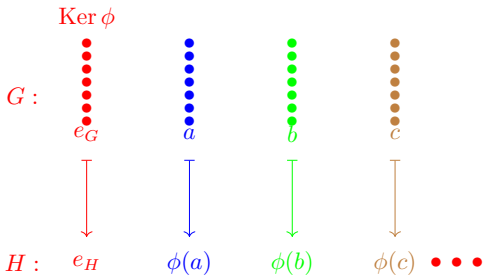
$$\phi : G \longrightarrow H$$

是一个群同态.

我们可以把 G 的元素杂乱无章的散落一地



有群同态 ϕ 后,根据像的不同,把它们重新排队



由定义,我们知道

$$\phi^{-1}(e_H) = \operatorname{Ker}\phi$$

也就是上面图中第一列为 $\operatorname{Ker}\phi$, 其他列呢?

第二列是 $\phi(a)$ 的所有原像,就是 G 中被 ϕ 映为 $\phi(a)$ 的那些元素,即

$$\{x \in G \mid \phi(x) = \phi(a)\}$$

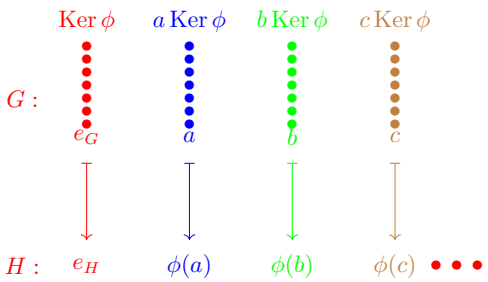
但是

$$\begin{aligned}&\phi(x) = \phi(a)\\ \Leftrightarrow &\phi(a)^{-1}\phi(x) = e_H\\ \Leftrightarrow &\phi(a^{-1})\phi(x) = e_H\\ \Leftrightarrow &\phi(a^{-1}x) = e_H\\ \Leftrightarrow &a^{-1}x \in \operatorname{Ker}\phi\\ \Leftrightarrow &x \in a\ \operatorname{Ker}\phi\end{aligned}$$

也就是说第二列恰为

$$a\ \operatorname{Ker}\phi$$

这样,上面的图就变成了这样



这个看上去怎么那么像左陪集呀?

慢着! 如果我没有记错的话,咱们还没有说明Ker ϕ 是 G 的子群吧?

引理 10.4. 假设 $\phi : G \longrightarrow H$ 是一个群同态, 那么 $\operatorname{Ker}\phi$ 是 G 的正规子群.

证明. 假设 $x, y \in \operatorname{Ker}\phi$. 则

$$\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} = e_H e_H^{-1} = e_H$$

因此

$$xy^{-1} \in \operatorname{Ker}\phi$$

所以 $\operatorname{Ker}\phi$ 是 G 的子群

另外任取 $g \in G$, $x \in \operatorname{Ker}\phi$, 我们有

$$\phi(gxg^{-1}) = \phi(g)e_H\phi(g)^{-1} = e_H$$

因此

$$gxg^{-1} \in \operatorname{Ker}\phi$$

所以 $\operatorname{Ker}\phi$ 是 G 的正规子群.

综合一下我们前面的讨论, 我们发现

命题 10.5. 假设 $\phi : G \longrightarrow H$ 为群同态, 那么存在一一对应

$$\overline{\phi} : G/\operatorname{Ker}\phi \longrightarrow \operatorname{Im}\phi$$
$$a\operatorname{Ker}\phi \mapsto \phi(a)$$

下面就是我们最重要的

第一同构定理

定理 10.6 第一同构定理. 假设 $\phi : G \longrightarrow H$ 是一个群同态, 那么

$$\overline{\phi} : G/\operatorname{Ker}\phi \longrightarrow \operatorname{Im}\phi$$
$$a\operatorname{Ker}\phi \mapsto \phi(a)$$ 是群同构.

证明. 前面我们已经知道 $\overline{\phi}$ 是一一映射, 只需要说明其保运算即可. 为了记号方便, 我们记

$$K := \operatorname{Ker}\phi$$

则有

$$\begin{aligned}\overline{\phi}((aK)(bK)) &= \overline{\phi}(abK)\\ &= \phi(ab)\\ &= \phi(a)\phi(b)\\ &= \overline{\phi}(aK)\overline{\phi}(bK)\end{aligned}$$

因此 $\overline{\phi}$ 保运算, 从而是群同构.

有了第一同构定理, 我们很容易得到一些群之间的同构. 例如: 假设 $\langle a\rangle$ 是一个 n 阶循环群, 容易验证

$$\pi : \mathbb{Z} \longrightarrow \langle a\rangle$$
$$i \mapsto a^i$$

是一个群同态. 它的 Kernel 是什么呢?

$$i \in \operatorname{Ker}\pi \Leftrightarrow a^i = e \Leftrightarrow n|i$$

因此

$$\operatorname{Ker}\pi = n\mathbb{Z}$$

另一方面, 显然 π 是满射, 即

$$\operatorname{Im}\pi = \langle a\rangle$$

由第一同构定理得

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \simeq \langle a\rangle$$

也就是说

所有 n 阶循环群都同构于 $\mathbb{Z}_n$.

例 5. 考虑取行列式

$$\det : \mathrm{GL}_n(\mathbb{R}) \longrightarrow R^*$$

我们已经知道它是一个群同态, 很显然它也是满射. 那它的 Kernel 是什么呢?

$$\begin{aligned}\operatorname{Ker}(\det) &= \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det(A) = 1\}\\ &= \mathrm{SL}_n(\mathbb{R})\end{aligned}$$

因此, 由第一同构定理

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \simeq \mathbb{R}^*$$

11 第二、第三同构定理

本期前言

上一期我们讲了

群同态基本定理

的第一同构定理

定理 11.1 **第一同构定理.** 假设 ϕ : $G \longrightarrow H$ 是一个群同态, 那么

$$\overline{\phi} : G/\operatorname{Ker}\phi \longrightarrow \operatorname{Im}\phi$$

$a \operatorname{Ker}\phi \mapsto \phi(a)$ 是群同构.

但我还是看不出来为啥

$$S_4/K_4 \simeq S_3$$

这一期我们就聊聊第一同构定理的两个应用

第二同构定理

第三同构定理 其实它们的本质都是第一同构定理, 但有时候直接用另外两个同构定理会更方便.

第二同构定理

第二同构定理就是针对 S_4/K_4 这种情况.

如果用第一同构定理, 要证明

$$S_4/K_4 \simeq S_3$$

最自然的想法是找一个从 S_4 到 S_3 的群的满同态 ϕ 使得 $\operatorname{Ker}\phi = K_4$, 但想来想去, 好像不太好找这么一个群同态.

倒过来 S_3 反而可以看成 S_4 的子群.

等等! 你说什么? S_3 是 S_4 的子群?

是呀, 怎么了?

我这里 K_4 可是 S_4 的正规子群!

是呀, 又能咋地?

子群和正规子群, 子群和正规子群...

它们乘起来还是 S_4 的子群呀.

对哈, 它们乘起来是哪个子群呢?

$$S_3 = \{e, (12), (13), (23), (123), (132)\}$$

$$K_4 = \{e, (12)(34), (13)(24), (14)(23)\}$$

它们的乘积 S_3K_4 同时包含 S_3 和 K_4. 取

$$(12) \in S_3, (12)(34) \in K_4$$

这两个元素都在 S_3K_4 中因此它们的乘积也应该在 S_3K_4 中, 所以

$$(34) = (12)(12)(34) \in S_3K_4$$

同样的道理

$$(13) \in S_3, (13)(24) \in K_4$$

$$(23) \in S_3, (14)(23) \in K_4$$

从而

$$(24) = (13)(13)(24) \in S_3K_4$$

$$(14) = (14)(23)(23) \in S_3K_4$$

请注意看上面这些蓝色元素

- 它们为 S_4 中所有的对换
- 它们都在 S_3K_4 中

由于 S_4 中元素都可以写成对换的乘积, 因此这些乘积还在 S_3K_4 中 (谁叫咱是子群呢). 所以

$$S_3K_4 = S_4$$

这样有个好处

K_4 的左陪集代表元可以全取 S_3 中元素

即

$$S_4/K_4 = \{\sigma K_4 \mid \sigma \in S_3\}$$

这样我们可以建立一个

从 S_3 到 S_4/K_4 的群的满同态呀!

$$\phi : S_3 \longrightarrow S_4/K_4$$

$$\sigma \mapsto \sigma K_4$$

(验证 ϕ 确实是群同态). 其 Kernel 是什么呢?

$$\begin{aligned}\operatorname{Ker}\phi &= \{\sigma \in S_3 \mid \sigma K_4 = K_4\} \\ &= \{\sigma \in S_3 \mid \sigma \in K_4\} \\ &= S_3 \cap K_4\end{aligned}$$

由第一同构定理

$$S_3/(S_3 \cap K_4) \simeq S_4/K_4$$

但是

$$S_3 \cap K_4 = \{e\}$$

因此

$$S_3 \simeq S_3/(S_3 \cap K_4)$$

从而

$$S_3 \simeq S_4/K_4$$

Oh Yeah! 终于证明成功! 总结下我们遇到了什么情况.

群 G 有两个子群

H 和 N

其中 N 是 G 的正规子群.

HN 还是 G 的子群并且

$$N \lhd HN$$

HN 关于 N 的商群就会是这样

$$HN/N = \{hN \mid h \in H\}$$

于是我们就愉快的构造了一个群同态

$$\phi : H \longrightarrow HN/N$$

$h \mapsto hN$ 这是一个满同态, 且

$$\begin{aligned}\operatorname{Ker}\phi &= \{h \in H \mid hN = N\} \\ &= \{h \in H \mid h \in N\} = H \cap N\end{aligned}$$

由第一同构定理

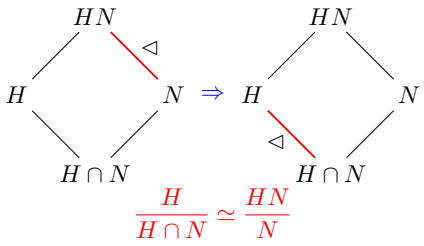
$$H/(H \cap N) \simeq HN/N$$

这就是我们的

定理 11.2 第二同构定理. 假设 H 是群 G 的子群, 而 N 是 G 的正规子群, 那么

$$H/(H \cap N) \simeq HN/N$$

这个定理可以用一个图来描述



例 6. $G = \mathrm{GL}_2(\mathbb{C}), H = \mathrm{SL}_2(\mathbb{C}), N = \{\mathbb{C}^* I_2\}$ 容易发现

$$HN = G,\ H \cap N = \{\pm I_2\}$$

由第二同构定理

$$HN/N \simeq H/(H \cap N)$$

即

$$\mathrm{GL}_2(\mathbb{C})/\mathbb{C}^* I_2 \simeq \mathrm{SL}_2(\mathbb{C})/\{\pm I_2\}$$

左边这个商群是射影一般线性群 (projective general linear group), 右边这个商群是射影特殊线性群 (projective special linear group). 分别记为

$$\mathrm{PGL}_2(\mathbb{C}), \mathrm{PSL}_2(\mathbb{C})$$

在 2 阶的时候, 虽然 $\mathrm{SL}_2(\mathbb{C})$ 比 $\mathrm{GL}_2(\mathbb{C})$ 小很多, 但当对它们取 “射影” 版本时, 它们就同构了.

2 第三同构定理

第三同构定理考虑的是这样一种情形

$$K \lhd G, N \lhd G$$

$$K \subseteq N \subseteq G$$

例如 $24\mathbb{Z} \subseteq 6\mathbb{Z} \subseteq \mathbb{Z}$. 这时有两个商群

$$G/K, G/N$$

对于 K 的每一个左陪集 gK, 显然

$$gK \subseteq gN$$

我们断言

gN 是唯一包含 gK 的 N 的左陪集

实际上, 若 aN 是另一个包含 gK 的左陪集, 特别地

$$g \in aN$$

但这样一来, 由命题7.3

$$gN = aN$$

这样我们可以建立一个简单的满同态

$$\pi : G/K \longrightarrow G/N$$

$$gK \mapsto gN$$

其 Kernel 是

$$\begin{aligned}&\{gK \in G/K \mid gN = N\} \\ =&\{gK \in G/K \mid g \in N\} \\ =&N/K\end{aligned}$$

由第一同构定理, 我们得到

$$(G/K)/(N/K) \simeq G/N$$

这就是

定理 11.3 第三同构定理. 假设 N 和 K 是 G 的正规子群且

$$K \subseteq N \subseteq G$$

则

$$(G/K)/(N/K) \simeq G/N$$

例 7. 假设 $d|n$ 是两个正整数, 那么

$$n\mathbb{Z} \subseteq d\mathbb{Z} \subseteq \mathbb{Z}$$

它们显然都是 $\mathbb{Z}$ 的正规子群. 由第三同构定理

$$(\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/d\mathbb{Z}$$

即 $\mathbb{Z}_n/d\mathbb{Z}_n \simeq \mathbb{Z}_d$.

12 满同态

本期前言

这一期讨论一个特殊的情况

本期总是假定

$$\phi : G \longrightarrow H$$

是一个群的满同态

然后讨论

G 的子群与 H 的子群之间的关系

一一对应

实际上这是一个比较简单的问题. 假设

$$H_1 \leqslant H$$

是 H 的一个子群, 取

$$\phi^{-1}(H_1) := \{a \in G \mid \phi(a) \in H_1\}$$

很容易证明

引理 12.1. $\phi^{-1}(H_1)$ 是 G 的子群且 $\operatorname{Ker}\phi \subseteq \phi^{-1}(H_1)$.

证明. 取任意 $a, b \in \phi^{-1}(H_1)$, 则

$$\begin{aligned}\phi(ab^{-1}) &= \phi(a)\phi(b^{-1}) \\ &= \phi(a)\phi(b)^{-1}\end{aligned}$$

由于

$$\phi(a), \phi(b) \in H_1$$

而 $H_1 \leqslant H$, 所以

$$\phi(a)\phi(b)^{-1} \in H_1$$

从而有

$$\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} \in H_1$$

所以 $ab^{-1} \in \phi^{-1}(H_1)$, 故而 $\phi^{-1}(H_1) \leqslant G$.

另外, 对任意 $a \in \operatorname{Ker}\phi$ 有

$$\phi(a) = e_H \in H_1$$

从而 $a \in \phi^{-1}(H_1)$. 所以 $\operatorname{Ker}\phi \subseteq \phi^{-1}(H_1)$.

这个引理告诉我们, 给一个 H 的子群 H_1, 取其在 ϕ 下的原像构成的集合

$$\phi^{-1}(H_1)$$

就是 G 中介于 $\operatorname{Ker}\phi$ 和 G 之间的子群.

也就是说我们有一个映射

$$\begin{aligned}\{H \text{ 的子群}\} &\to \{G \text{ 的包含 } \operatorname{Ker}\phi \text{ 的子群}\} \\ H_1 &\mapsto \phi^{-1}(H_1)\end{aligned}$$

实际上这是一个非常好的对应.

定理 12.2. 1. 上面的映射 ϕ^{-1} 是一一对应

2. $\phi^{-1}(\{e_H\}) = \operatorname{Ker}\phi$, $\phi^{-1}(H) = G$

3. 若 $H_1 \leqslant H_2 \leqslant H$, 则

$$\phi^{-1}(H_1) \leqslant \phi^{-1}(H_2)$$

如果 $H_1 \lhd H_2$, 则

$$\phi^{-1}(H_1) \lhd \phi^{-1}(H_2)$$

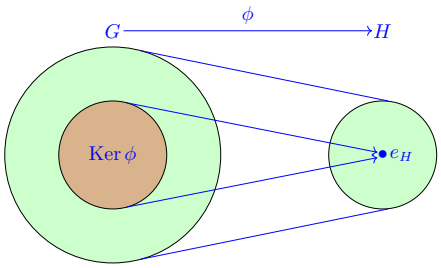
且对应的商群同构

$$H_2/H_1 \simeq \phi^{-1}(H_2)/\phi^{-1}(H_1)$$

4. 若 $H_1 \lhd H$, 则 $\phi^{-1}(H_1) \lhd G$ 且

$$G/\phi^{-1}(H_1) \simeq H/H_1$$

用一个图来感受下这个定理



证明. 1. 为证明 ϕ^{-1} 是双射, 我们为 ϕ^{-1} 找一个逆映射.

任给 G 的包含 $\operatorname{Ker}\phi$ 的子群 G_1, 由第 10 期的命题 2, G_1 在 ϕ 下的像集 $\phi(G_1)$ 是 H 的一个子群.

因此, 我们得到映射

$$\begin{aligned}\phi\colon \{G \text{ 的包含 } \operatorname{Ker}\phi \text{ 的子群}\} &\longrightarrow \{H \text{ 的子群}\} \\ G_1 &\mapsto \phi(G_1)\end{aligned}$$

要证明 ϕ^{-1} 是双射, 只需要证明

$$\phi(\phi^{-1}(H_1)) = H_1, \forall H_1 \leqslant H$$

$$\phi^{-1}(\phi(G_1)) = G_1, \forall \operatorname{Ker}\phi \leqslant G_1 \leqslant G$$

先来证明第一个. 对任意 $H_1 \leqslant H$, 由定义

$$\phi(\phi^{-1}(H_1)) \subseteq H_1$$

反过来, 对任意 $h \in H_1$, 由于

$$\phi : G \longrightarrow H$$

是满射, 因此存在 $a \in G$ 使得 $\phi(a) = h$. 所以

$$\begin{aligned}a &\in \phi^{-1}(H_1) \\ h = \phi(a) &\in \phi(\phi^{-1}(H_1))\end{aligned}$$

即 $H_1 \subseteq \phi(\phi^{-1}(H_1))$. 从而

$$\phi(\phi^{-1}(H_1)) = H_1$$

再证明第二个等式. 对任意

$$\operatorname{Ker}\phi \leqslant G_1 \leqslant G$$

由定义可知

$$G_1 \subseteq \phi^{-1}(\phi(G_1))$$

反过来, 对任意 $a \in \phi^{-1}(\phi(G_1))$ 有

$$\phi(a) \in \phi(G_1)$$

即存在 $b \in G_1$ 使得

$$\phi(a) = \phi(b)$$

从而

$$\phi(b^{-1}a) = \phi(b)^{-1}\phi(a) = e_H$$

所以 $b^{-1}a \in \operatorname{Ker}\phi$, 从而

$$a \in b\operatorname{Ker}\phi$$

但 $b \in G_1, \operatorname{Ker}\phi \subseteq G_1$, 所以

$$b\operatorname{Ker}\phi \subseteq G_1$$

故而 $a \in G_1$. 由此我们证明了

$$\phi^{-1}(\phi(G_1)) \subseteq G_1$$

所以

$$\phi^{-1}(\phi(G_1)) = G_1$$

2. 由定义可得

3. 显然 $H_1 \leqslant H_2$ 可以推出

$$\phi^{-1}(H_1) \leqslant \phi^{-1}(H_2)$$

假设 H_1 是 H_2 的正规子群. 我们可以建立群同态

$$f : \phi^{-1}(H_2) \longrightarrow H_2/H_1$$
$$a \mapsto \phi(a)H_1$$

Check 下 f 确为满同态, 因为

$$\phi : \phi^{-1}(H_2) \longrightarrow H_2$$

为满射. 计算下 $\operatorname{Ker} f$

$$\begin{aligned}\operatorname{Ker} f &= \{a \in \phi^{-1}(H_2) \mid \phi(a)H_1 = H_1\} \\ &= \{a \in \phi^{-1}(H_2) \mid \phi(a) \in H_1\} \\ &= \phi^{-1}(H_2) \cap \phi^{-1}(H_1) \\ &= \phi^{-1}(H_1)\end{aligned}$$

因此

$$\phi^{-1}(H_1) = \operatorname{Ker} f \lhd \phi^{-1}(H_2)$$

并且由群的第一同构定理

$$\phi^{-1}(H_2)/\phi^{-1}(H_1) \simeq H_2/H_1$$

4. 由 3 取 $H_2 = H$ 即得.

自然满同态

特别的, 假设 G 是一个群, 而 N 是 G 的正规子群, 那么

$$\pi : G \longrightarrow G/N$$
$$a \mapsto aN$$

是一个群的满同态且 $\operatorname{Ker}\pi = N$. 由上面的定理, 商群 G/N 的子群和 G 的包含 N 的子群一一对应. 上面这种满同态称为自然满同态

这种情况下, 一个比较大的群 G 被拆分成了一个小一点正规子群 N 和一个商群 G/N, 这个商群同样看起来比 G 要 “小” 一点.

一个比较有意思的想法是:

> 当 N 和 G/N 同时具有某种性质的时候, G有可能也具有这种性质

比如: 如果 N 和 G/N 的阶数都是一个素数 p 的方幂, 那么 G 的阶数也是 p 的方幂.

这个性质可能太无聊了, 来个有意思点的

定理 12.3. 假设 N 是有限群 G 的正规子群, 如果 N 和 G/N 都是可解群, 那么 G 也是可解群.

证明. N 可解是什么意思? (第 9 期)

就是存在子群序列

$$\{e\} = N_m \lhd N_{m-1} \lhd \cdots \lhd N_0 = N \ (*)$$

使得这些商群

$$N_i/N_{i+1}, i = 0, \cdots, m-1$$

都是 Abel 群.

G/N 可解呢, 就是存在

$$\{N\} = H_r \lhd H_{r-1} \lhd \cdots \lhd H_0 = G/N$$

使得对应的商群

$$H_i/H_{i+1}, i = 0, \cdots, r-1$$

都是 Abel 群. 由定理12.2, 我们有序列

$$N = \pi^{-1}(H_r) \lhd \pi^{-1}(H_{r-1}) \lhd \cdots \lhd \pi^{-1}(H_0) = G$$
$$(**)$$

且有商群同构

$$\pi^{-1}(H_i)/\pi^{-1}(H_{i+1}) \simeq H_i/H_{i+1}, i = 0, \cdots, r-1$$

因此

$$\pi^{-1}(H_i)/\pi^{-1}(H_{i+1}), i = 0, \cdots, r-1$$

也是 Abel 群. 我们把 (∗) 和 (∗∗) 拼起来就得到

$$\{e\} = N_m \lhd N_{m-1} \lhd \cdots \lhd N = \pi^{-1}(H_r)$$
$$\lhd \pi^{-1}(H_{r-1}) \lhd \cdots \lhd \pi^{-1}(H_0) = G$$

中这个序列中每个相应的商群都是 Abel 群, 因此 G 是可解群.

例 8. 比如 K_4 是 S_4 的正规子群, 且对应商群

$$S_4/K_4 \simeq S_3$$

K_4 为 Abel 群, 因此可解, 而

$$\{e\} \lhd A_3 \lhd S_3$$

为 S_3 的一个子群序列满足

$$A_3,\ S_3/A_3$$

分别是 3 阶和 2 阶群, 必是循环群, 从而是 Abel 群. 因此 S_3 可解.

利用定理12.3可得 S_4 可解.

例 9. 考虑 $\mathbb{Z}$ 的子群 $n\mathbb{Z}$, 对应是商群是 $\mathbb{Z}_n$.

$\mathbb{Z}$ 中包含 $n\mathbb{Z}$ 的子群是

$$\{d\mathbb{Z} \mid d \text{ 整除 } n\}$$

$\mathbb{Z}_n$ 的子群是

$$\{d\mathbb{Z}_n \mid d \text{ 整除 } n\}$$

自然满同态

$$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$$

给出它们的一一对应

$$\pi(d\mathbb{Z}) = d\mathbb{Z}_n$$

13 群作用

本期导言

写这一期, 真的感觉压力山大, 因为这是一个

想像力决定生产力

的超级项目

群在集合上的作用 (action)

它最“入门级”的应用:

每个有限群都同构于某个对称群的子群

看上去也不是显然的.

群怎么能作用在一个集合上呢? 且看分解.

集合的变换群

大多数“空间”都有其变换群, 就是

其到自身的保持其“结构”的双射的全体

其运算是映射的复合, 这个在第 2 期讲对称的时候就出现过了, 只不过没有给它一个“名份”.

n 维 F-向量空间 F^n 的变换群为

$$\mathrm{GL}(F^n) := \{F^n \text{ 到自身的线性自同构}\}$$

也就是 $M_n(F)$ 中的所有可逆矩阵的全体.

欧氏空间 $\mathbb{R}^n$ 的变换群是

$$\{\mathbb{R}^n \text{ 上的正交变换}\}$$

即所有的 n 阶正交矩阵.

那给定一个集合

$$X$$

呢? 其变换群是什么呢? 由于单纯的集合上没有运算, 没有长度, 没有任何“结构”可言, 因此, 其变换群就应该是

$$S(X) := \{X \text{ 到自身的双射}\}$$

例 10. 当 $X = \{1, 2, \cdots, n\}$ 时, $S(X)$ 就是 S_n.

当然, 今后还会学到很多“空间”, 都可以按照这个思想考虑其变换群.

这次我们只考虑集合的变换群.

2 集合的变换群的作用 (action)

现在假设 X 是一个集合, 其变换群

$$S(X)\ (X \text{ 到 } X \text{ 双射的全体})$$

中的每个元素 f(实际上就是一个 X 到 X 的双射)都可以“作用”在 X 上:

$$f : x \mapsto f(x)$$

例 11. $X = \{1,2,3\}$, $S(X) = S_3$ S_3 中元素都可以作用在 X 上, 比如:

$$\sigma = (123)$$

作用在 1 上得到 2, 作用在 2 上得到 3, 作用在 3 上得到 1.

3 其他群作用在 X 上

给定一个集合 X, 除了 $S(X)$ 可以作用在 X 上, 另外一个群 G 也想“作用”在 X 怎么办呢?

只有一个办法, 让 G 中的元素

$$\text{“化身”为 } S(X) \text{ 中元素 (双射)}$$

也就是让每个 G 中的元素都“扮演” $S(X)$ 中的一个角色. 换成数学语言, 给一个从 G 到 $S(X)$ 的映射

$$\phi : G \longrightarrow S(X)$$

这样 G 中的元素 g 就可以“作用”在 X 上了

$$g : X \longrightarrow X$$
$$x \mapsto \phi(g)(x)$$

g 就像 $\phi(g)$ 一样作用在 X 上.

例 12. 假设 Δ 为正 n 边形, 其顶点的集合记为

$$\Delta_0$$

此时 D_n 中的元素是 $\mathbb{R}^2$ 上的一些旋转或者翻折, 按理说这不是 $S(\Delta_0)$ 中的元素, 但由于 D_n 中的每个变换 σ 都将正 n 边形的顶点变为其顶点, 因此 σ 可以限制到 Δ_0 上“化身”为 Δ_0 的一个双射, 从而可以“作用”在 Δ_0 上.

Warning: 前方深坑!

问题 4. 是不是 G 中元素“随意”化身为 $S(X)$ 中的元素都是我们喜欢的呢?

例 13. Bad Example 比如: 我们将 3 阶循环群

$$\{e, a, a^2\}$$

的元素按下面的方式化身为 S_3 中元素

$$e \mapsto (12)$$
$$a \mapsto (23)$$
$$a^2 \mapsto (13)$$

看看它们“作用”在 $\{1,2,3\}$ 上有什么效果.

$$1 \xrightarrow{a} 1 \xrightarrow{a} 1$$
$$1 \xrightarrow{a^2} 3$$

这? 用 a 作用两次和用 a^2 作用效果不一样? 这叫什么作用呀? 真讨厌!

因此我们喜欢的作用应该是这样的

定义 13.1. 假设 X 是一个集合, G 是一个群, G 在 X 上的一个群作用是一个映射

$$\phi : G \longrightarrow S(X)$$

满足

$$\phi(a)\phi(b) = \phi(ab), \forall a, b \in G$$

即: ϕ 是一个群! 同! 态!

例 14. Good example 1

$G = \mathrm{SO}(\mathbb{R}^3)$ 是 $\mathbb{R}^3$ 上的所有旋转变换构成的群.

集合

$$X := S^2$$

是 $\mathbb{R}^3$ 中的单位球面. 我们知道单位球面上的点在旋转变换下的像还在单位球面上, 因此每个 $\mathbb{R}^3$ 上的旋转变换都可以化身为 $X = S^2$ 到自身的双射 (通过限制). 对应的群同态为

$$\mathrm{SO}(\mathbb{R}^3) \longrightarrow S(X)$$
$$\sigma \mapsto \sigma|_X$$

Good example 2

假设 Δ 是一个正 n 边形.

$$X := \Delta_0$$

是 Δ 的所有顶点组成的集合. Δ 的对称群 D_n 中每个元素将 Δ 的顶点映为顶点, 因此 D_n 通

过群同态

$$\begin{array}{ccc} D_n & \longrightarrow & S(\Delta_0) = S_n \\ \sigma & \mapsto & \sigma|_{\Delta_0} \end{array}$$

作用在 Δ_0 上.

4 换个说法

需要说明的是,考虑群在集合上的作用是一个非常考验脑洞的游戏,有些脑洞大开的人会找到一些让人意想不到的群作用.

我们整理下思路,要确定群 G 在集合 X 上的一个群作用需要做哪些事情?

- 给 G 中每个元素 a 找一个“扮演对象” $\phi(a)$: X 到自身的**双射** (需要证明是单,满)
- 证明
$$\phi(a)\phi(b) = \phi(ab), \forall a, b \in G$$

如果不是前面说的那些很自然的群作用,而是自己开的脑洞想出来的,要验证是不是群作用看上去工作量还不少.

其实有一个工作量相对比较少的办法.

对每个 $a \in G$, $x \in X$, 给定一个 X 中元素与之对应,记为 $a \cdot x$, 即给出一个映射

$$\phi : G \times X \longrightarrow X$$

$(a, x) \mapsto a \cdot x$ 这其实相当于将每个 $a \in G$ 化身为 X 到自身的映射

$$\phi_a : X \longrightarrow X$$

$x \mapsto a \cdot x$ 但不承诺这个映射是双射.

那要怎样才能保证上面这个 ϕ_a 是双射,且

$$G \longrightarrow S(X)$$
$$a \mapsto \phi_a$$

是群同态呢? 实际上只要保证下面两点就够了.

- $e \cdot x = x, \forall x \in X$
- $a \cdot (b \cdot x) = (ab) \cdot x, \forall a, b \in G, x \in X$

这里看上去没有要求 ϕ_a 是双射,但实际上把这两条翻译成映射的语言就是

- $\phi_e = \mathrm{id}_X$ (X 上恒等映射)
- $\phi_a \phi_b = \phi_{ab}$, $\forall a, b \in G$

这样就能保证

$$\phi_a \phi_{a^{-1}} = \phi_e = \mathrm{id}_X = \phi_{a^{-1}} \phi_a$$

对所有 $a \in G$ 成立,因此所有的 ϕ_a 都是双射. 由上面条件的第 2 个条件就知道

$$G \longrightarrow S(X)$$
$$a \mapsto \phi_a$$

是一个群同态.

这实际上说明只要为每个 $a \in G, x \in X$ 都给定一个 X 中元素

$$a \cdot x$$

满足

$$e \cdot x = x, \forall x \in X$$
$$(ab) \cdot x = a \cdot (b \cdot x), \forall a, b \in G, x \in X$$

这样就能给出一个 G 在 X 上的作用.

反过来,给 G 在 X 上的一个群作用

$$\phi : G \longrightarrow S(X)$$

只要我们记

$$a \cdot x := \phi(a)(x)$$

就会有

$$\begin{aligned} e \cdot x &= \phi(e)(x) \\ &= \mathrm{id}_X(x) = x \end{aligned}$$

对所有 $x \in X$ 成立.

$$\begin{aligned} (ab) \cdot x &= \phi(ab)(x) \\ &= \phi(a)\phi(b)(x) \\ &= \phi(a)(b \cdot x) \\ &= a \cdot (b \cdot x) \end{aligned}$$

对所有的 $a, b \in G, x \in X$ 成立.

由此可见群作用的定义13.1与下面这个定义是等价的,只是说法不一样而已.

定义 13.2. 群 G 在一个集合 X 上的一个群作用就是对每个 $a \in G$, $x \in X$ 给定一个

$$a \cdot x \in X$$

满足

- $e \cdot x = x$, $\forall x \in X$
- $(ab) \cdot x = a \cdot (b \cdot x)$, $\forall a, b \in G, x \in X$

5

群作用的例子

例 15. G 是一个群, $X = G$, 对每个 $a \in G$, $x \in G$, 我们给定

$$a \cdot x := ax$$

可以发现

- $e \cdot x = ex = x, \forall x \in X$
- $(ab) \cdot x = abx = a(bx) = a \cdot (b \cdot x)$
  $\forall a, b \in G, x \in X$

这个群作用称为 G 在自身上的左乘作用.

如果我们换一种方式, 指定

$$a \cdot x := axa^{-1}$$

的话, 可以发现

$$e \cdot x = exe^{-1} = x, \forall x \in X$$

对任意 $a, b \in G, x \in X$

$$\begin{aligned}(ab) \cdot x &= abx(ab)^{-1} \\ &= abxb^{-1}a^{-1} \\ &= a(bxb^{-1})a^{-1} \\ &= a \cdot (b \cdot x)\end{aligned}$$

这也是 G 在自身上的一个群作用, 我们通常称这个群作用为共轭作用.

上面这个左乘作用实际上会告诉我们一个意想不到的结论.

假设 G 是一个 n 阶群, 考虑 G 在自身上的左乘作用

$$a \cdot x := ax, \forall a, x \in G$$

换成群同态的语言

$$\begin{aligned}\phi : G &\longrightarrow S(G) \\ a &\mapsto (\phi(a) : x \mapsto ax)\end{aligned}$$

是个群同态. 那这个群同态的 Kernel 是什么呢?

$$\begin{aligned}\operatorname{Ker}\phi &= \{a \in G \mid \phi(a) = \mathrm{id}_G\} \\ &= \{a \in G \mid ax = x, \ \forall x \in G\} \\ &= \{e\}\end{aligned}$$

因此 ϕ 是单射. 这样我们得到一个很 “酷” 的结论:

$$G \text{ 同构于 } S(G) \text{ 的子群 } \operatorname{Im}\phi$$

而 G 有 n 个元素, 这意味着 $S(G) \simeq S_n$. 这样我们就得到下面这个群作用的 “入门级” 应用

定理 13.3 Cayley 定理. 对任意有限群 G, 都存在正整数 n 使得 G 同构于 S_n 的一个子群.

本期最后再列举几个群作用的例子.

例 16. 假设 G 是一个群, 而 H 是 G 的子群. 考虑

$$X := \{xH \mid x \in G\}$$

为 H 的左陪集的全体. 对任意 $a \in G$, $xH \in X$, 定义

$$a \cdot xH := axH$$

可以验证, 这是一个群作用.

跟前一个例子类似, 如果考虑

$$X = \{xHx^{-1} \mid x \in G\}$$

即同 H 的共轭子群组成的集合, 并定义

$$a \cdot xHx^{-1} := axHx^{-1}a^{-1}$$

$$\forall a \in G, xHx^{-1} \in X$$

这也是一个群作用.

这两个群作用将在我们后面讲 Sylow 定理时发挥巨大的作用!

例 17. $G = \mathrm{GL}_n(\mathbb{R})$, $X = M_n(\mathbb{R})$ 对于 $T \in G$, $A \in X$, 定义

$$T \cdot A := TAT^{-1}$$

例 18. $G = \mathrm{GL}_n(\mathbb{R}), X = \mathbb{R}^n$ 对于 $T \in G$, $v \in X$, 定义

$$T \cdot v := Tv$$

后面几期, 我们将看到群作用的神奇作用.

14 轨道的大小

本期导言

这一期我们来看下这个想像力决定生产力的群作用项目到底有什么稀奇的. 我只想说, 它轻轻的拂动一下曼妙的身姿, 就会有意料之外的金光出现, 请看本期讲述.

1 群作用的轨道

先来个简单的例子

$$G = \mathrm{SO}(\mathbb{R}^2)\text{: 平面上绕原点的旋转变换}$$

$$X = \mathbb{R}^2$$

$\mathrm{SO}(\mathbb{R}^2)$ 自然的作用在 $\mathbb{R}^2$ 上:

$$\mathrm{SO}(\mathbb{R}^2) \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

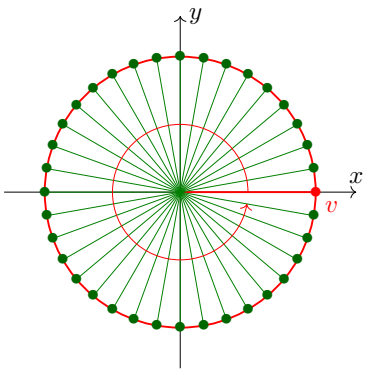
$$(A, v) \mapsto Av$$

这里我们将 $\mathbb{R}^2$ 中的点 v 写成列向量的形式. 当我们固定一个 $\mathbb{R}^2$ 中的点, 例如:

$$v := [1, 0]^T \in \mathbb{R}^2$$

在 $\mathrm{SO}(\mathbb{R}^2)$ 的作用下, 这个点会被变成哪些点呢?

$\mathrm{SO}(\mathbb{R}^2)$ 为所有绕原点的旋转变换, 因此 $v = [1, 0]^T$ 在这些旋转变换下可以得到的点恰为单位圆上所有的点.



它们恰好组成整个单位圆. 我们称之为 v 在 $\mathrm{SO}(\mathbb{R}^2)$ 的作用下的轨道(orbit).

定义 14.1. 一般的, 如果群 G 作用在一个集合 X 上

$$G \times X \longrightarrow X$$

$(a, x) \mapsto a \cdot x$ 对于 $x \in X$, 其在 G 的作用下得到的所有 X 中的元素组成的集合

$$O_x := \{a \cdot x \mid a \in G\}$$

称为 x 在 G 的作用下的轨道(orbit).

例 19. S_n 自然的作用在集合

$$\{1, \cdots, n\}$$

上. 1 在 S_n 下的轨道 O_1 是什么样子? 很显然 1 自己在 O_1 中, 因为

$$1 = e(1)$$

对于 $2 \leqslant i \leqslant n$, 我们有

$$(1i)(1) = i$$

因此整个 X 都包含在 O_1 中, 所以

$$O_1 = X$$

例 20. $\sigma = (124)(35) \in S_5$, 而

$$G = \langle \sigma \rangle$$

为 σ 在 S_5 中生成的循环子群. G 也可以自然的作用在

$$X = \{1, 2, 3, 4, 5\}$$

上. 那这几个元素在 G 作用下的轨道都是什么样子呢? 简单计算就会发现

$$O_1 = O_2 = O_4 = \{1, 2, 4\}$$

$$O_3 = O_5 = \{3, 5\}$$

2 不同轨道的关系

从例20我们看到, 有些元素在 G 作用下的轨道是一样的, 其实如果大家稍微仔细一点, 就会发现, 恰好是

同一轨道中的元素在 G 作用下的轨道一样

这个是不是一般的规律呢? 也许我们应该问一个更一般的问题.

问题 5. 假设群 G 作用在集合 X 上. 对于 X 中两个元素 x, y, 它们在 G 的作用下形成的轨道

$$O_x \text{ 和 } O_y$$

到底有什么关系?

先来看一个特殊的情况, 假设

$$y \in O_x$$

会不会像例20那样 $O_y = O_x$ 呢?

引理 14.2. 假设群 G 作用在集合 X 上, $x, y \in X$ 为 X 中两个元素. 那么

$$y \in O_x \Leftrightarrow O_x = O_y$$

证明. 如果 $O_x = O_y$, 特别的

$$y \in O_y = O_x$$

反过来, 假设 $y \in O_x$, 即存在 $a \in G$ 使得

$$y = a \cdot x$$

因此

$$\begin{aligned} O_y &= \{b \cdot y \mid b \in G\} \\ &= \{b \cdot (a \cdot x) \mid b \in G\} \\ &= \{(ba) \cdot x \mid b \in G\} \\ &\subseteq O_x \end{aligned}$$

由于

$$\begin{aligned} x &= e \cdot x \\ &= (a^{-1}a) \cdot x \\ &= a^{-1} \cdot (a \cdot x) \\ &= a^{-1} \cdot y \end{aligned}$$

因此, 同理可得 $O_x \subseteq O_y$. 所以 $O_x = O_y$.

推论 14.3. 假设群 G 作用在集合 X 上, $x, y \in X$ 为 X 中两个元素. 那么下面几条等价

1. $O_x = O_y$
2. $y \in O_x$
3. $O_x \cap O_y \neq \emptyset$

证明. 上的面引理已经证明了1 $\Leftrightarrow$ 2

2 $\Rightarrow$ 3. 由条件 2, 显然 $y \in O_x \cap O_y$, 因此

$$O_x \cap O_y \neq \emptyset.$$

3 $\Rightarrow$ 1. 假设

$$z \in O_x \cap O_y$$

由引理14.2

$$O_x = O_z, O_z = O_y$$

所以 $O_x = O_y$.

实际上 G 在 X 上的群作用在 X 上正好定义了一个等价关系

$$x \sim y: \exists a \in G \text{ 使得 } y = a \cdot x$$

而 O_x 正好是这个等价关系下 x 所在的等价类.

两个轨道之间要么相等, 要么交集为空.

因此, X 是所有互不相同的轨道的并 (不同的轨道之间交集为空).

轨道的大小

这一节我们总是假设群 G 作用在集合 X 上, 这一小节的问题是

问题 6. 轨道 O_x 中有多少个元素?

我们知道

$$O_x = \{a \cdot x \mid a \in G\}$$

理论上这个轨道的元素最多跟 G 的元素个数一样, 但不排除有些情况下不同的 G 中元素 a, b 作用在 x 上的结果一致, 即:

$$a \cdot x = b \cdot x$$

这样 O_x 中的元素就没有 G 的元素多了.

由此可见, 搞清楚啥时候 G 中的元素作用在 x 上的效果一样, 就能搞清楚轨道 O_x 有多少个元素. 那啥时候 $a, b \in G$ 满足

$$a \cdot x = b \cdot x$$

呢? 实际上, 这当且仅当

$$a^{-1} \cdot (a \cdot x) = a^{-1} \cdot (b \cdot x)$$

当且仅当

$$(a^{-1}b) \cdot x = x$$

也就是说, 当且仅当 $a^{-1}b$ 作用在 x 上保持 x 不动. 令

$$G_x := \{g \in G \mid g \cdot x = x\}$$

很容易发现 G_x 是 G 的子群 (包含 e, 对取逆和乘法封闭). 称为 x 的稳定化子(stablizer).

经过上面的讨论, 我们已经知道

$$a \cdot x = b \cdot x$$

当且仅当

$$a^{-1}b \in G_x$$

换成左陪集的语言就是

$$aG_x = bG_x$$

也可以说当且仅当 a, b 在同一个 G_x 的左陪集中 (如果不记得, 请看第 7 期第 3 小节)

这样

$$O_x = \{a \cdot x \mid a \in G\}$$

中有多少个元素就清楚了:

G_x 有多少个左陪集, O_x 就有多少元素

定理 14.4. 群 G 作用在集合 X 上,那么 O_x 与 G/G_x 之间有一个一一对映

$$G/G_x \longrightarrow O_x$$

$aG_x \mapsto a\cdot x$ 特别的 O_x 的元素个数与 G_x 在 G 中的指数 (左陪集个数) 相同,即

$$|O_x| = [G : G_x]$$

这个定理有一个很有意思的推论

推论 14.5. 在定理14.4中,如果 G 是有限群,则轨道 O_x 的元素个数整除 G 的阶数.

如果 O_x 中只有 x 这一个元素,就意味着 G 中的元素作用在 x 上都等于 x 自己,即

$$a\cdot x = x, \forall a \in G$$

这时,我们称 x 为这个群作用的不动点 (fixed point).

如果 $O_x = X$,也就是说 X 中全部元素组成一个轨道,我们就称这个群作用是可迁的(transitive).

例 21. S_n 自然的作用在 $\{1,\cdots,n\}$ 上. 考虑 n 所在的轨道 O_n. 我们来看下 n 的稳定化子

$$\{\sigma \in S_n \mid \sigma(n) = n\}$$

也就是保持 n 不动的所有置换,实际上就是 S_{n-1}. 由定理14.4得

$$|O_n| = [S_n : S_{n-1}] = n$$

也就是说 O_n 有 n 个元素,从而

$$O_n = \{1, 2, \cdots, n\}$$

因此这个群作用是可迁的.

共轭作用

有一个特别的群作用值得提出来单独说下,就是一个群 G 共轭的作用在自身上

$$a\cdot x := axa^{-1}, \forall a, x \in G$$

此时 x 所在的轨道记为

$$C_x := \{axa^{-1} \mid a \in G\}$$

称为 x 在 G 中的共轭类(conjugacy class). x 在这个共轭作用下的稳定化子记为

$$\begin{aligned} C_G(x) :&= \{a \in G \mid axa^{-1} = x\} \\ &= \{a \in G \mid ax = xa\} \end{aligned}$$

称为 x 的中心化子(centralizer). 由定理14.4

$$|C_x| = [G : C_G(x)]$$

x 是这个共轭作用的不动点当且仅当

$$C_G(x) = G$$

当且仅当 x 与 G 中所有元素都交换,即

$$x \in C(G) = \{b \in G \mid ba = ab, \forall a \in G\}$$

这里 $C(G)$ 是 G 的中心(center).

例 22. $G = S_3$, $x = (12)$, 则

$$C_G(x) = \{e, (12)\}$$

因此

$$|C_x| = [S_3 : C_G(x)] = 3$$

实际上

$$C_x = \{(12), (13), (23)\}$$

确实有 3 个元素.

一般的,一个有限群 G 共轭的作用在自身上,轨道恰为 G 中的那些共轭类,从而

$$G = \cup_{x\in G} C_x$$

当 $x \in C(G)$ 时,$C_x = \{x\}$ 只有一个元素,假设

$$C_{x_1}, \cdots, C_{x_m}$$

为所有 G 中元素个数大于 1 的互不相同的共轭类,则

$$|G| = |C(G)| + \sum_{i=1}^{m} |C_{x_i}|$$

这个等式称为 G 的类方程(class equation)

例 23. 如果 H 是群 G 的一个子群

$$X := \{xHx^{-1} \mid x \in G\}$$

G 共轭的作用在 X 上

$$a\cdot xHx^{-1} := axH(ax)^{-1}$$

则 $H \in X$ 在这个群作用下的稳定化子记为

$$N_G(H) := \{a \in G | aHa^{-1} = H\}$$

称为 H 的正规化子(normalizer)

由于此时 H 所在的轨道

$$O_H = \{aHa^{-1} \mid a \in G\} = X$$

根据定理14.4

$$|X| = [G : N_G(H)]$$

素数方幂阶群的作用

现在假设 p 是一个素数,而 G 是 p 的方幂阶群. 如果 G 作用在一个有限集合 X 上,则每个轨道 O_x 元素个数都整数 $|G|$(推论14.5), 因此要么

$$|O_x| = 1 \ (x \text{ 为不动点})$$

要么

$$|O_x| > 1, \text{此时必有 } p \text{ 整除 } |O_x|$$

假设 X_0 是所有不动点的集合, 而

$$O_{x_1}, \cdots, O_{x_m}$$

是所有元素个数大于 1 的轨道, 这样

$$O_x, x \in X_0, O_{x_1}, \cdots, O_{x_m}$$

为所有互不相同的轨道. 所以

$$\begin{aligned} |X| &= \sum_{x \in X_0} |O_x| + \sum_{i=1}^{m} |O_{x_i}| \\ &= |X_0| + \sum_{i=1}^{m} |O_{x_i}| \end{aligned}$$

由于这些 $|O_{x_i}|$ 都被 p 整除, 由此我们得到下面这个非常有用的引理.

引理 14.6. 假设 G 是一个 p 的方幂阶群, 作用在一个有限集合 X 上. 假设 X_0 是所有不动点的集合, 则

$$|X| \equiv |X_0| \pmod{p}$$

我们把这个引理应用到上面的共轭作用上, 就会得到下面这个推论

推论 14.7. 假设 p 是素数, G 是 $p^m > 1$ 阶群. 则

$$|C(G)| \equiv 0 \pmod{p}$$

特别的, 此时 $C(G)$ 不是平凡群.

证明. 当 G 共轭作用在自身上时, 不动点恰为其中心的元素, 由引理14.6, 我们有

$$|G| \equiv |C(G)| \pmod{p}$$

由于 $p^m > 1$, 因此 $m > 0$, 从而

$$|G| \equiv 0 \pmod{p}$$

因此

$$|C(G)| \equiv 0 \pmod{p}$$

由于 $e \in C(G), C(G)$ 显然不是空集, 因此

$$p \text{ 整除 } |C(G)|$$

故 $C(G)$ 不是平凡群.

推论 14.8. 假设 p 为一个素数. 则 p 的方幂阶群都是可解群.

证明. 我们对 $|G|$ 的阶数进行归纳, 若 $|G|$ 的阶数为 1 或者 p, 那么 G 为 Abel 群, 从而是可解群.

现假设 $|G| > p$. 由于

$$C(G) \lhd G$$

由拉格朗日定理

$$|C(G)| \text{ 和 } |G/C(G)|$$

都整除 $|G|$, 从而都是 p 的方幂. 由推论14.7, $C(G)$ 非平凡.

若 $C(G) = G$, 则 G 是 Abel 群, 从而是可解群.

若 $C(G) \neq G$, 由于 $C(G)$ 不是平凡群, 因此

$$C(G) \text{ 和 } G/C(G)$$

都是阶小于 $|G|$ 的 p 的方幂阶群. 由归纳假设

$$C(G) \text{ 和 } G/C(G)$$

都是可解群. 根据第 12 期第 2 小节定理 3, G 是可解群.

从这个推论大家可以看出, 群作用不经意的挥一挥衣袖, 就给我们带来了意想不到的效果, 如果它龙飞凤舞起来, 会是怎样一番景象!

15 轨道个数

本期导言

上期我们讨论了群作用下轨道的大小，另一个非常自然的问题是:

群作用在集合上有多少个轨道？

本期设定

在这一期中，我们总是假定

有限群 G 作用在有限集合 X 上

1 轨道个数的计算

上期知道 X 被划分成若干个轨道的无交并，即

$$X = O_1 \cup \cdots \cup O_m$$

每个轨道的大小，例如 $x \in O_1$，可由

$$|O_1| = [G : G_x]$$

来计算，其中

$$G_x = \{a \in G \mid a \cdot x = x\}$$

为 x 的稳定化子. 现在我们的问题是

一共有多少个轨道?

2 (NOT) Burnside's Lemma

针对这个问题，我们看下上面求轨道大小时候的一个现象.

假设 O 是其中一个轨道，$x \in O$，我们知道

$$G_x := \{a \in G \mid a \cdot x = x\}$$

的元素个数为

$$|G_x| = |G|/|O|$$

与 x 取 O 中哪个元素没有关系，也就是说每个 O 中的元素 z 都恰好有 $|G|/|O|$ 个 G 中的元素 a 使得

$$a \cdot z = z$$

如果我们把 G 和 O 的元素“配对”，考虑

$$\{(a, z) \in G \times O \mid a \cdot z = z\}$$

对每个 z 来说，恰好能找到 $|G|/|O|$ 个配对的 a，因此“配对”成功的总对数是

$$(|G|/|O|) \times |O| = |G|$$

即

$$|\{(a, z) \in G \times O \mid a \cdot z = z\}| = |G|$$

这下更是跟取哪个轨道都没有关系了!

现在假设我们一共有 m 个轨道

$$O_1, \cdots, O_m$$

那么每个 O_i 与 G “配对”的结果

$$|\{(a, z) \in G \times O_i \mid a \cdot z = z\}| = |G|$$

那么总的“配对”结果

$$\begin{aligned} &|\{(a, z) \in G \times X \mid a \cdot z = z\}| \\ =&\sum_{i=1}^{m} |\{(a, z) \in G \times O_i \mid a \cdot z = z\}| \\ =&m|G| \end{aligned}$$

而轨道的个数就很清楚了

轨道个数

$$m = |\{(a, z) \in G \times X \mid a \cdot z = z\}|/|G|$$

引理 15.1 (NOT) Burnside's Lemma. 假设有限群 G 作用在有限集合 X，记

$$X^g := \{x \in X \mid g \cdot x = x\}, \forall g \in G$$

则这个群作用下的轨道个数为

$$\frac{1}{|G|} \sum_{g \in G} |X^g|$$

证明. 由上面的讨论，只需要计算

$$\begin{aligned} &\frac{1}{|G|} |\{(g, x) \in G \times X \mid g \cdot x = x\}| \\ =&\frac{1}{|G|} \sum_{g \in G} |\{(g, x) \mid x \in X, g \cdot x = x\}| \\ =&\frac{1}{|G|} \sum_{g \in G} |\{x \in X \mid g \cdot x = x\}| \\ =&\frac{1}{|G|} \sum_{g \in G} |X^g| \end{aligned}$$

注

大多数参考书都称这个引理为 Burnside 引理，但实际上这个引理并不是 Burnside 证明的. 最初是由 Frobenius 在 1887 年证明 [3]，甚至据说 Cauchy 在 1845 年就知道. 它在 Burnside

在 1897 年出版的书 [1] 中出现, 并注明归功于 Frobenius, 但在 1911 年的第二版 [2] 中, 这个注记又被神秘的去掉了, 而这很有可能是造成现在误解的原因.

多彩的手链

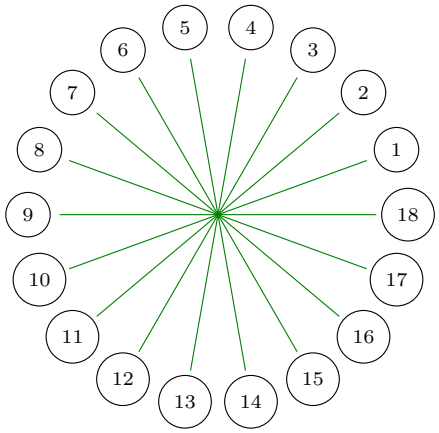
上面的NOT Burnside 引理可以被应用到一个经典的组合问题上.

我们来穿一个 n 个珠子的手链, 每个珠子可以有 k 种颜色选择, 最终我们能做出多少种不同的手链?

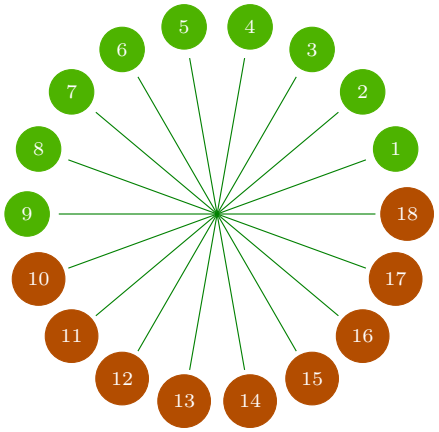
我特地查了下, 很多手链是 18 颗珠子.

如果一个朋友想送恋人每天一个不同的手链 (都是 18 颗珠子的), 连续送一年, 至少需要几种颜色的珠子?

我们可以把这些珠子的位置编个序号, 比如放在圆上.



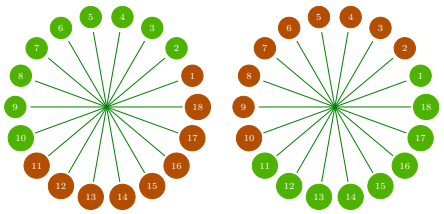
假设我们有 k 种颜色的珠子, 那么每个位置都可以选择其中一种颜色, 比如下面这个最差方案:



这样下来整个配珠方案的集合记为 X, 那么 X 的元素个数为 k^n.

对于 X 中的任何一种元素 (方案), 我们可以将其旋转或者翻折, 依然可以得到 X 中的其他方案, 因此二面体群 D_n 可以很舒服的作用在 X 上.

如果两种方案可以通过旋转或者翻折得到, 那这两种方案得到的手链是一样的. 比如下面这两种方案得到的手链就跟上面的手链是 “同款”!



那总共有多少种不同的呢? 稍微思考下不难发现:

两款方案得到相同的手链当且仅当它们可以通过旋转和翻折得到对方.

这样的话, 有多少种不同款就看 D_n 作用在 X 上有多少个不同的轨道了!

由 (NOT)Burnside 引理, 我们需要对 D_n 中每个元素, 计算其固定的 X 中元素的个数. 这个其实比较好做, 将 D_n 中的元素看作 S_n 中的转换, 这样 D_n 中的旋转 $2\pi/n$ 的变换就对应到

$$\rho = (12\cdots n)$$

其中一个翻折变换对应到

$$\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \cdots & 1 \end{pmatrix}$$

而 D_n 里面的所有元素正好对应到

$$\rho^i, \tau\rho^i, i = 0, \cdots, n-1$$

取一个 $\sigma \in D_n$, 我们将 σ 写成不相交循环的乘积

$$\sigma = c_1 \cdots c_r$$

WARNING: 这里不相交循环包括 1-循环

一个方案被 σ 固定, 当且仅当, 对于所有的 $i = 1, \cdots, n$, 第 i 个位置的珠子和第 $\sigma(i)$ 个位置的珠子是一样的, 根据我们把转换写成不相交循环的写法, 你会发现, 恰好是出现在同一个循环中那些位置的珠子必须一样. 每个循环可以选择 k 种颜色中的一种, 这样的方案共有

$$k^r \text{ 种}$$

通过这个方式, 我们可以看下 18 个珠子的手链, k 种颜色选择, 可以做出多少个不同的款式来.

元素 σ	循环个数	$\lvert X^\sigma \rvert$
e	18	k^{18}
ρ	1	k
ρ^2	2	k^2
ρ^3	3	k^3
ρ^4	2	k^2
ρ^5	1	k
ρ^6	6	k^6
可以总结了 (证明留种练习)		
$\rho^i, i = 0, \cdots, 17$	$(i, 18)$	$k^{(i,18)}$
想想为什么?		
无固定顶点翻折 (9 种)	9	k^9
有固定顶点翻折 (9 种)	10	k^{10}

由 (NOT)Burnside 引理, 轨道个数为

$$\frac{1}{36}\left(\sum_{i=0}^{17} k^{(i,18)} + 9(k^9 + k^{10})\right)$$

如果 $k = 2$, 结果就是

$$7685$$

也就是说每天送一个款, 可以送 20 年!!!

只有两种颜色为免太难看了吧, 要不 5 颜色? 会有多少款呢? 算下:

$$105966797755 \text{ 种}$$

如果每秒钟送一款不重样的话, 可以送

$$3360 \text{ 年!}$$

一般情形 对于 n 个珠子的手链, k 种颜色选择.

款式总数为

$n = 2l$ 为偶数

$$\frac{1}{2n}\left(l(k^l + k^{l+1}) + \sum_{i=1}^{n} k^{(i,n)}\right)$$

$n = 2l + 1$ 为奇数

$$\frac{1}{2n}\left(nk^{l+1} + \sum_{i=1}^{n} k^{(i,n)}\right)$$

证明留给读者.

参考文献

[1] W. Burnside, Theory of groups of finite order, Cambridge Univ. Press 1897.ta

[2] W. Burnside, Theory of groups of finite order, Cambridge Univ. Press 1911.

[3] G. Frobenius, Über die Congruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul, *J. Reine Angew. Math.* 101(1887), 273-299.

16 二平方定理的一句话证明

本期导言

这一期我们讲一个小学生都懂的定理

定理 16.1 **费马二平方定理.** 奇素数 p 可以写成两个整数的平方和当且仅当

$$p \equiv 1 \pmod 4$$

有人称之为史上最美的十个数学定理之一 (列第十位, 见 [1]).

更过分的是有个证明居然只有一句话!

1 二平方定理简介

很容易发现一个奇素数如果能写成两个整数的平方和, 必然一奇一偶, 从而必然模 4 余 1, 反过来呢? 模 4 余 1 的奇素数是不是都是两个整数的平方和呢?

实际上 Girard 在 1625 年就描述了什么样的整数可以分解为两个整数的平方和; Fermat 在 1640 年给 Marin Mersenne 的信 (1640 年 12 月 25 日) 中描述了素数或者其素数的方幂什么时候能写成两个整数的平方和, 正因为如此, 这个定理有时候也被称为

Fermat's Christmas theorem.

但很显然, 他们都没有公开给出证明.

2 一句话证明

这个定理最早出现的证明是 Euler 给出的 (使用无穷阶递降法), Lagrange 基于二次型的方法也给出了证明 (1775), 后来 Gauss 等其他数学家也给出过很多新的证明.

这里要说的是 1990 年发表在 American Mathematical Monthly 上的一句话证明[2].

A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ Is a Sum of Two Squares

D. Zagier

The involution on the finite set

$$S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$$

defined by

$$(x,y,z) \mapsto \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & x > 2y \end{cases}$$

has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x, y, z) \mapsto (x, z, y)$ also has a fixed point.

如果不懂群作用, 直接看上图的证明也是可以理解的. 这里从群作用的角度解释下, 没有学过群作用的读者请直接看下一小节.

证明. 考虑 2 阶循环群 $\{e, \rho\}$ 在集合

$$S := \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$$

上的作用, 定义 $\rho \cdot (x, y, z)$ 为

$$\begin{cases} (x + 2z, z, y - x - z), & \text{if } x < y - z; \\ (2y - x, y, x - y + z), & \text{if } y - z < x < 2y; \\ x - 2y, x - y + z, y), & \text{if } x > 2y. \end{cases}$$

(可验证这是一个群作用)

由于 $p = 4k + 1$, 很容易发现这个群作用有唯一的不动点 $(1, 1, k)$, 由于 S 的元素个数与不动点元素个数模 2 同余 (第 14 期引理 6), 因此 S 有奇数个元素, 考虑二阶循环群在 S 上的另一个作用:

$$\rho \cdot (x, y, z) := (x, z, y)$$

这个群作用也必然有不动点, 形如

$$(x, y, y) \text{ 形式, 即 } x^2 + (2y)^2 = p.$$

证毕.

其实上面的群作用中, 第一种情况与第三种情况相互转换, 只有第二种情况的 (x, y, z) 可能是不动点, 因此不动点 (x, y, z) 必须满足

$$x = 2y - x,\ z = x - y + z$$

即 $x = y$, 形如 (x, x, z), 但如此

$$p = x^2 + 4xz = x(x + 4z)$$

由于 p 为素数, $x = 1$. 因此不动点是 $(1, 1, k)$.

图形解释

我想大家看到这个证明的时候跟我原来一样, 很好奇别人是怎样想到这么神奇的证明的, 最近正好看到了一个巧妙的图形解释, 分享给大家.

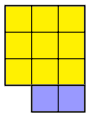
给定模 4 余 1 的素数 p, 对于集合

$$S := \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$$

中的元素 (x, y, z),

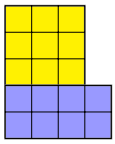
- 先画一个黄色的边长为 x 的正方形;

- 如果 $y < x < 2y$, 从这个正方形的右下顶点向左下方画一个宽为 y, 高为 z 的长方形



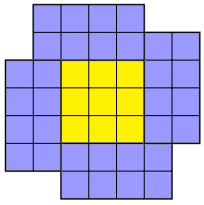
(3,2,1)

否则, 从这个正方形的左下顶点向右下方画一个宽为 y, 高为 z 的长方形;

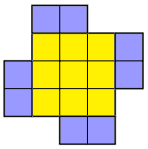


(3,4,2)

- 最后把这个长方形绕正方形的中心旋转 90 度, 180 度和 270 度.



(3,4,2)



(3,2,1)

对每个 $(x, y, z) \in S$, 对应图形的面积为

$$x^2 + 4xy = p$$

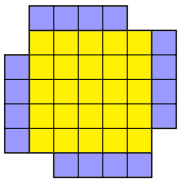
例如: $(3, 4, 2)$, 其图形面积为

$$3^2 + 4 \cdot 4 \cdot 2 = 41$$

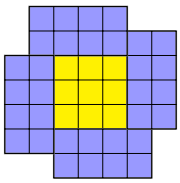
由于 $4 - 2 < 3 < 2 \cdot 4$, 因此 $(3, 4, 2)$ 在 ρ 的作用下的结果为

$$(2 \cdot 4 - 3, 4, 3 - 4 + 2) = (5, 4, 1)$$

对应的图形为



与原来 $(3, 4, 2)$ 的图形对比下



很神奇吧? 恰为之前的图形区域进行了简单的重新划分. 这里有趣之处在于, 上面 ρ 的作用正是对所有的图形进行这种重新划分区域的游戏.

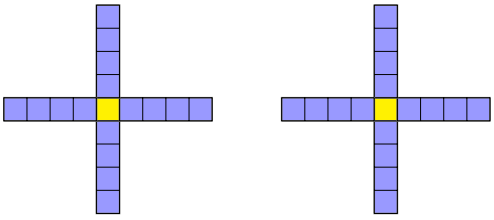
如果不信, 以 $p = 17$ 为例, 根据

$$17 = x^2 + 4yz$$

集合 S 中元素为

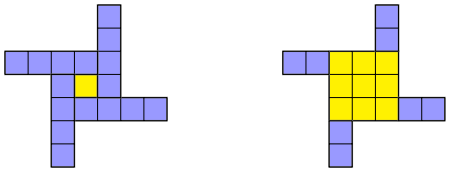
$$(1, 1, 4), (1, 4, 1), (1, 2, 2)$$
$$(3, 1, 2), (3, 2, 1)$$

它们在 ρ 的作用下对应关系如下:



(1,1,4) ↔ (1,1,4)

(1,2,2) ↔ (3,2,1)



(1,4,1) ↔ (3,1,2)

可以看到唯一的前后一致是 $(1,1,4)$.

因此 S 中有奇数个元素, 从而

$$S \longrightarrow S,\ (x,y,z) \mapsto (x,z,y)$$

必然有不动点, 即存在

$$(x,\ y,\ y) \in S$$

$$p = x^2 + 4yy = x^2 + (2y)^2.$$

啥时候整数是平方和

不过说真的, 啥时候一个整数是两个整数的平方和呢? 结论是这样的:

定理 16.2. 一个正整数是两个整数的平方和当且仅当其形如 $4k+3$ 的素因子的重数是偶数.

小结

本期这个群作用的想像力虽然稍微浮夸了一点, 但至少在一定程度上说明了当想像力足够的时候, 群作用的威力还是很大的!

参考文献

[1] D. Wells, The Penguin Book of Curious and Interesting Mathematics. London: Penguin Books (1997), 126 - 127.

[2] D. Zagier, D. (1990), A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares, American Mathematical Monthly, 97(1990) (2): 144, doi:10.2307/2323918, MR 1041893.

17 Sylow 第一定理

本期导言

如果现在还没有说服你群作用 "想像力决定生产力" 的话, 这期开始, 我们将介绍群作用的又一次精彩演出:

Sylow 定理

拉格朗日定理和 Sylow 定理也许可以并称为群论中最重要的两个定理.

Sylow 定理只需要用群 G 的阶这个最简单的信息就能推断出 G 的某些子群的是否存在以及可能有多少个!

Sylow 定理分为 3 个定理, 是 Sylow 在 1872 年证明的 [2], 这里的证明与原始证明并不完全一致, 特此说明.

关于 Sylow 其人

全名 Peter Ludwig Mejdell Sylow (1832-1918), 是挪威数学家, 他被广为人知的除了 Sylow 定理之外, 还有对 Abel 工作的整理. 他的数学生涯中, 大部分时间 (1856-1898) 的正式工作是中学教师, 但他的主要热情还是数学的研究, 由于这个原因, 他并不是一个成功的中学老师, 这也在很大程度上浪费了他的天赋和能力: 大学没有 Sylow 这样好的教授, 而中学又有 Sylow 这样差的老师.

Sylow 是家里 10 个兄弟姐妹之首, 一生未婚, 但充满热心和幽默感, 热爱户外活动. 如果大家对 Sylow 的生平感兴趣, 可以访问这个网页: https://mathshistory.st-andrews.ac.uk/Biographies/Sylow/

素数阶子群的存在性

关于有限群的子群有一个非常朴素的问题. 根据拉格朗日定理, 有限群 G 的子群的阶一定整除 $|G|$.

反过来如果 m 是 $|G|$ 的因子,G 是否一定存在 m 阶子群呢？特别的,如果 m 是 $|G|$ 的素因子呢？

问题 7. 假设 p 是群 G 的阶数 $|G|$ 的一个素因子,G 是否有 p 阶子群？

比如只知道群 G 的阶数为 60,G 是否存在 2 阶子群？是否存在 3 阶子群？是否存在 5 阶子群？

这个答案是肯定的、

引理 17.1 Cauchy 定理. 假设 p 是群 G 的阶数的素因子,那么 G 存在 p 阶子群.

证明. 我们把舞台留给群作用.

下面的证明来自 [1].

由于 p 阶群都是循环群,因此 G 有 p 阶子群当且仅当 G 存在 p 阶元.

考虑 p 个 G 的笛卡尔乘积

$$G \times \cdots \times G$$

的子集

$$X := \{(a_1, \cdots, a_p) \mid a_1 a_2 \cdots a_p = e\}.$$

X 中元素

$$(a_1, \cdots, a_p)$$

的前 $p-1$ 个位置都可以任意放 G 中的元素,只要最后一个位置放

$$a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$$

就行. 通过这个观察,可以得到以下两个结论：第一个结论是

$$|X| = |G|^{p-1}$$

第二个结论是

$$a_p(a_1 a_2 \cdots a_{p-1}) \text{ 也等于 } e.$$

因此

$$(a_p, a_1, a_2, \cdots, a_{p-1}) \text{ 也属于 } X$$

重复这个过程,就有

$$(a_{p-1}, a_p, a_1, \cdots, a_{p-2})$$
$$(a_{p-2}, a_{p-1}, a_p, a_1, \cdots, a_{p-3})$$
$$\cdots\cdots$$

都属于 X,因此 p 阶循环群

$$\langle (12\cdots p) \rangle$$

可以通过旋转元素的位置自然的作用在 X 上,从而

$$|X| \equiv |X_0| \pmod{p}$$

其中 X_0 是这个群作用的不动点集合,很显然 X_0 中的元素有如下形式

$$X_0 = \{(a, a, \cdots, a) \mid a^p = e\}$$

由于

$$|X| = |G|^{p-1},\ p \mid |G|$$

因此

$$|X| \equiv 0 \pmod{p}$$

从而

$$|X_0| \equiv 0 \pmod{p}$$

由于 X 中有个显然的不动点

$$(e, e, \cdots, e)$$

所以 $X_0 \neq \emptyset$, 但其元素个数模 p 余 0,从而至少有 p 个元素.

如此至少存在 $a \neq e$ 使得

$$(a, a, \cdots, a) \in X_0$$

即 $a^p = e$,从而 G 中有 p 阶元 a, 其生成的循环子群 $\langle a \rangle$ 为 G 的 p 阶子群.

这个引理有个有趣的推论.

推论 17.2. 一个有限群阶数为素数 p 的方幂当且仅当其中任意元素的阶都是 p 的方幂.

证明. 如果群 G 的阶数为 p 的方幂,由拉格朗日定理的推论,其中任意元素的阶都整除 G 的阶,从而也是 p 的方幂.

反过来,假设 G 中所有元素的阶都是 p 的方幂. 如果 G 的阶不是 p 的方幂,必有其他素因子 q,由引理17.1, G 有 q 阶元,与假设矛盾.

Sylow 第一定理

现在假设群 G 的阶数为

$$|G| = p^n m$$

其中 $n > 0$ 且 $(p, m) = 1$.

刚才已经知道 G 有 p 阶子群了,那 G 是否有 p^2 阶,p^3 阶, $\cdots$, p^n 阶子群呢？Sylow 在 1872 年证明了它们的确是存在的.

定理 17.3 Sylow 第一定理. 假设群 G 的阶为 $p^n m$,其中 p 为素数,$n > 0, (p, m) = 1$. 下面两条成立.

1. 对 G 的任意 p^k $(k < n)$ 阶子群 P,存在 G 的 p^{k+1} 阶子群 H 使得 $P \lhd H$.
2. 对任意 $1 \leqslant k \leqslant n$,$G$ 有 p^k 阶子群.

证明. 结合引理17.1, 只需要证明第 1 条.

现在让 P 作用在 P 的所有左陪集组成的集合 $X := G/P$ 上

$$P \times X \longrightarrow X$$
$$(a, xP) \mapsto axP$$

不动点的集合为

$$\begin{aligned} X_0 &= \{xP \mid axP = xP,\ \forall a \in P\} \\ &= \{xP \mid x^{-1}ax \in P,\ \forall a \in P\} \\ &= \{xP \mid x \in N_G(P)\} \\ &= N_G(P)/P \end{aligned}$$

这里

$$N_G(P) := \{x \in G \mid x^{-1}Px \subseteq P\}$$

为 P 的正规化子 (normalizer), 显然 $P \leqslant N_G(P)$ 且为 $N_G(P)$ 的正规子群.

由于 $|P| = p^k$, 由第 14 期引理 6

$$|X| \equiv |X_0| \pmod{p}$$

即

$$[G : P] \equiv [N_G(P) : P] \pmod{p}$$

由于 $k < n$, 因此

$$[G : P] = p^{n-k}m \text{ 被 } p \text{ 整除}$$

从而

$$p \text{ 也整除 } [N_G(P) : P]$$

由引理17.1, $N_G(P)/P$ 有一个 p 阶子群 $\overline{H}$, 令 H 为其在自然满同态

$$\pi : N_G(P) \longrightarrow N_G(P)/P$$

下的原像集, 则 H 为 $N_G(P)$ 的 p^{k+1} 阶子群 (从而也是 G 的子群), 且 P 是 H 的正规子群 (由 P 为 $N_G(P)$ 的正规子群可得).

p 群都可解

Sylow 第一定理的一个直接推论是

推论 17.4. *素数的方幂阶群都是可解群.*

证明. 假设 G 是 p^n 阶群, p 为素数. 利用定理17.3中第一条, 可得序列

$$\{e\} = P_0 \lhd P_1 \lhd P_2 \lhd \cdots \lhd P_n = G$$

使得

$$|P_k| = p^k, i = 0, \cdots, n$$

这样对任意 $k = 0, 1, \cdots, n-1$

$$P_{k+1}/P_k \text{ 是 } p \text{ 阶群}$$

必为循环群, 特别的是 Abel 群. 因此 G 可解.

12 阶群 A_4 没有 6 阶子群

需要指出的是并不是每个 $|G|$ 的因子 m, G 都有 m 阶子群的, 比如 A_4 有 12 个元素, 但 A_4 没有 6 阶子群.

实际上, 如果 A_4 有 6 阶子群 N. 由于 A_4 中有 8 个 3 循环, 因此存在 3 循环 $\sigma \notin N$. 考虑

$$N,\ \sigma N,\ \sigma^2 N$$

由于 $[A_4 : N] = 2$, 上面这 3 个陪集必然有两个是一样的.

显然 $N \neq \sigma N$.

如果 $N = \sigma^2 N$, 则

$$\sigma^{-1} = \sigma^2 \in N,$$

从而 $\sigma \in N$, 矛盾.

如果 $\sigma N = \sigma^2 N$, 则

$$\sigma = \sigma^{-1}\sigma^2 \in N$$

与假设矛盾.

参考文献

[1] J. H. McKay, Another proof of Cauchy's group theorem. Amer. Math. Monthly 66 (1959), 119.

[2] L. Sylow, Théorèmes sur les groupes de substitutions. Math. Ann. 5 (1872), 584–594

18 Sylow 第二、第三定理

本期导言

上期说到如果有限群 G 的阶数

$$|G| = p^n m$$

其中 p 是素数且与 m 互素, Sylow 居然能“无中生有”的证明 G 一定存在

$$p^k \text{ 阶群}, k = 0, \cdots, n$$

现在开始, 我们将其中阶最大的

$$p^n \text{ 阶子群}$$

称为 G 的Sylow p 子群.

问题 8. 这些 p 子群 (元素的阶都是 p 的方幂的子群, 或者说阶为 p 的方幂的子群) 之间是什么关系? 能不能确定这些 p 子群或者 Sylow p 子群的个数?

有没有可能再次无中生有的给个答案?

本期设定

这一期, 我们总是假定 G 是

$$p^n m \text{ 阶群}$$

其中 p 是素数且与 m 互素.

1 p 子群与 Sylow p 子群

由上期的 Sylow 第一定理可知, 任意 G 的 p 子群 Q 都可以“逐渐变大”包含在一个 Sylow p 子群之中. Sylow 第二定理将告诉我们一个更有意思的事实

定理 18.1 Sylow 第二定理. 假设 Q 是 G 的一个 p 子群, 而 P 是 G 的 Sylow p 子群. 那么存在 $x \in G$ 使得

$$x^{-1}Qx \subseteq P.$$

特别的, 任意两个 Sylow p 子群彼此共轭.

证明. 想想好像完全没有思路.

群作用有话要说

“到头来还得靠我!”

“是呀, 谁叫你厉害呢?”

那咋作用呢? 看上去最后也是要找个不动点的样子

$$x^{-1}Qx \subseteq P$$

等价于

$$x^{-1}ax \in P, \forall a \in Q, \text{即}$$

$$aP = axP, \forall a \in Q$$

很显然, 我们应该用 Q 作用在 P 的所有左陪集构成的集合 $X := G/P$ 上

$$Q \times X \longrightarrow X$$

$$(a, xP) \mapsto axP,\ a \in Q,\ x \in G$$

由于 Q 是 p 群, 因此

$$|X| \equiv |X_0| \pmod{p}$$

其中 X_0 是这个群作用下的不动点, 由于

$$|X| = |G/P| = [G : P] = m$$

不被 p 整除, 因此 $|X_0|$ 也不被 p 整除, 这样一来, 至少

$$X_0 \neq \emptyset$$

即存在 $xP \in X$ 满足

$$axP = xP, \forall a \in Q$$

由上面的讨论

$$x^{-1}Qx \subseteq P$$

如果 Q 也是 Sylow p 子群, 上面这个包含关系两边有相同的元素个数, 从而

$$x^{-1}Qx = P.$$

这就证完了? 是呀, 证完了, 再见!

2 Sylow 第二定理的后果

如果 P 是 G 的 Sylow p 子群, 那么

$$a^{-1}Pa,\ a \in G$$

也是 G 的子群, 且与 P 有相同的元素个数, 因此也是 G 的 Sylow p 子群. Sylow 第二定理告诉我们

$$\text{Sylow } p \text{ 子群都形如 } x^{-1}Px$$

如果换成群作用的语言, 令 X 为

$$G \text{ 所有 Sylow } p \text{ 子群构成集合}$$

考虑群作用

$$G \times, X \longrightarrow X$$

$$(a, Q) \mapsto a^{-1}Qa$$

P 在这个群作用下的轨道就是整个 X.

推论 18.2. 假设 P 为 G 的一个 Sylow p 子群. 令 X 为

$$G \text{ 所有 Sylow } p \text{ 子群构成集合}$$

则群作用

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (a, Q) & \longmapsto & a^{-1}Qa \end{array}$$

是可迁的, 且 Sylow p 子群的个数

$$n_p = |X| = [G : N_G(P)]$$

特别的 n_p 整除 m.

证明. 上在已经说明这个作用是可迁的, 现在 P 在这个作用下的稳定子群恰为其正规化子 $N_G(P)$, 由轨道大小公式

$$|X| = |O_P| = [G : N_G(P)]$$

因为 $P \leqslant N_G(P)$, 所以

$$m = [G : P] = [G : N_G(P)] \cdot [N_G(P) : P]$$

所以 $|X| = [G : N_G(P)]$ 整除 m.

推论 18.3. G 只有一个 Sylow p 子群 P 当且仅当 P 是 G 的正规子群.

证明. 由上面的证明, G 只有一个 Sylow p 子群当且仅当

$$[G : N_G(p)] = 1, \text{即}$$
$$G = N_G(P)$$

也就是说 P 是 G 的正规子群.

Sylow 第三定理

最后再来看看 Sylow 的另一个神奇的发现

命题 18.4. G 的 Sylow p 子群的个数模 p 余 1.

证明. 说实话, 即使知道结论, 只需要证明, 我也想不出什么办法来. 还是交给群作用吧.

前面已经知道 Sylow p 子群的个数为

$$[G : N_G(P)]$$

其中 P 为一个 Sylow P 子群, 也就是说个数与

$$N := N_G(P)$$

的左陪集的个数相同. 现在我们就要最后一次流氓, 让 P 作用在 N 的所有左陪集构成的集合上

$$\begin{array}{c} P \times G/N \longrightarrow G/N \\ (a, xN) \mapsto axN \end{array}$$

有没有不动点呢?

xN 是不动点当且仅当

$$axN = xN, \forall a \in P, \text{即}$$
$$x^{-1}ax \in N \, \forall a \in P, \text{再即}$$
$$x^{-1}Px \subseteq N$$

由于 P 是 N 的正规子群, 同时也是 N 的 Sylow p 子群 (想想为什么?)

由推论18.3, 它是 N 唯一的 Sylow p 子群, 因此

$$x^{-1}Px \subseteq N$$

($x^{-1}Px$ 也是 N 的 Sylow p 子群) 等价于

$$x^{-1}Px = P, \text{即}$$
$$x \in N_G(P) = N, \text{再即}$$
$$xN = N$$

所以上面的群作用只有唯一不动点 N, 由于 P 是 p 群, 因此

$$|G/N| \equiv 1 \pmod{p}$$

从而 G 的 Sylow p 子群的个数模 p 余 1.

总结起来

定理 18.5 Sylow 第三定理. 假设 n_p 为 G 的 Sylow p 子群个数, 则

$$n_p \mid m \text{ 且 } n_p \equiv 1 \pmod{p}$$

Sylow 定理的应用

Sylow 定理是有限群最重要的基础理论之一, 在单群分类等方面中起到了非常重要的作用.

这里列举几个比较容易理解的应用.

例 24. 15 阶群都是循环群.

实际上由 Sylow 定理, 15 阶群 G 的 Sylow 3 子群的个数整除 5, 又模 3 余 1, 因此只能是 1 个, 设为 P_3.

同样可以说明 15 阶群只有一个 Sylow 5 子群, 设为 P_5.

这样 P_3 和 P_5 都是 G 的正规子群, 由拉格朗日定理

$$P_3 \cap P_5$$

的阶数既整除 3 又整除 5, 只能是 1, 因此

$$P_3 \cap P_5 = \{e\}$$

这样一来

$$P_3P_5$$

是 P_3 和 P_5 的内直积.

取 P_3 生成元 a, P_5 生成元 b, 那么则有 $ab = ba$, 因此

$$\mathrm{o}(ab) = 3 \times 5 = 15$$

所以 $G = \langle ab \rangle$ 是循环群.

也可以换一个思路, 由于只有一个 Sylow 5 子群, 也只有一个 Sylow 3 子群, 因此只有 4 个 5 阶元, 2 个 3 阶元, 1 个 1 阶元, 其他 8 个元素都只能是 15 阶元, 因此 G 是循环群.

按照这个思路, 你可以证明很多阶的群都只能是循环群, 比如 35 阶, 65 阶群等等, 实际上有一个更一般的结论.

定理 18.6. *n 是一个正整数, 所有 n 阶群都是循环群当且仅当 n 没有平方因子且任意两个素因子 p, q 满足*

$$q \not\equiv 1 \pmod{p}$$

也等价于

$$(n, \varphi(n)) = 1$$

其中 φ 为欧拉函数.

对证明感兴趣的可以参考 [1, 2].

最后再看一个 Sylow 定理的应用.

定理 18.7 Wilson's Theorem. *$(p-1)! \equiv -1 \pmod{p}$ 成立当且仅当 p 为素数.*

证明. 这里只证明充分性, 必要性的证明很简单, 大家自己琢磨下.

现在假设 p 是素数, 考虑对称群 S_p, 它的 Sylow p 子群是 p 阶循环群.

而 S_p 中有 $(p-1)!$ 个 p 循环 (p 阶元), 由于不同的 p 阶循环群之间的交集只能是 e, 每个 p 阶循环群中有 $p-1$ 个 p 阶元, 因此 S_p 共有

$$\frac{(p-1)!}{p-1} = (p-2)!$$

个 Sylow p 子群.

由 Sylow 第三定理

$$(p-2)! \equiv 1 \pmod{p}$$

两边同乘以 $p-1$

$$(p-1)! \equiv -1 \pmod{p}$$

参考文献

[1] L. E. Dickson, Definitions of a group and a field by independent postulates, Trans. Amer. Math. Soc. 6 (1905), 198–204. http://www.ams.org/journals/tran/1905-006-02/S0002-9947-1905-1500706-2/S0002-9947-1905-1500706-2.pdf.

[2] T. Szele, Ueber die endlichen Ordnungszahlen, zu denen nur eine Gruppe gehoert, Comm. Math. Helv. 20 (1947), 265–267. https://eudml.org/doc/138922.

19 SO(3) 的有限子群

本期前言

本期我们将展现群作用的强大力量: 分类 $\mathrm{SO}(3,\mathbb{R})$ 的有限子群!

1 正多面体的对称群

$\mathrm{SO}(3,\mathbb{R})$ 为所有 3 阶行列式为 1 的正交矩阵的全体, 或者看作 $\mathbb{R}^3$ 上所有行列式为 1 的正交变换的全体. 我们先来看下 $\mathrm{SO}(3,\mathbb{R})$ 中的元素. 假设 $\sigma \in \mathrm{SO}(3,\mathbb{R})$ 但不是单位矩阵, 由于 σ 的特征多项多为 3 次实多项式, 根的模长均为 1, 且三根乘积为 1, 因此必有一根为 1, 也就是说 σ 一定有 1 这个特征值. 假设特征值 1 对应的特征子空间为 V_1. 我们断言 $\dim V_1 = 1$(练习!). 假设 $\mathfrak{n}_\sigma$ 为 V_1 中的一个单位向量, 从几何上看, σ 实际上是绕 $\mathfrak{n}_\sigma$ 这个轴的一个旋转变换.

如果我们有一个正多面体 Δ(凸多面体, 每个面都是正多边形, 每个顶点所在的面个数相同), 我们可以假设其中心到各顶点的距离都是 1, 那么我们可以把 Δ 的中心放在 $\mathbb{R}^3$ 中的原点, 则其各顶点都在单位球面 S^2 上, 设 Δ 的顶点集合为 Δ_0, 定义:

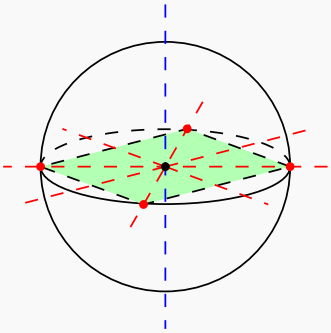
$$S(\Delta) := \{\sigma \in \mathrm{SO}(3,\mathbb{R}) | \sigma(\Delta_0) = \Delta_0\}$$

我们断言 $S(\Delta)$ 一定是一个有限群. 实际上, 令 $S(\Delta_0)$ 为集合 Δ_0 上的所有置换构成的群, 则 $S(\Delta_0) \cong S_{|\Delta_0|}$ 为有限群. 我们有一个自然的群同态

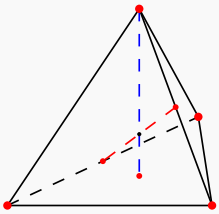
$$\begin{array}{ccc} \phi : S(\Delta) & \longrightarrow & S(\Delta_0) \\ \sigma & \mapsto & \sigma|_{\Delta_0} \end{array}$$

当 Δ 不是正 "2" 面体时, 由于 Δ_0 中点对应的向量能线性生成 $\mathbb{R}^3$, 如果 $\sigma|_{\Delta_0}$ 是恒等映射, 那么 σ 必为恒等变换. 因此, $\mathrm{Ker}\phi = \{I\}$, 从而 ϕ 是单射. 所以 $S(\Delta) \cong \mathrm{Im}\,\phi$ 是 $S(\Delta_0)$ 的子群, 为有限群.

例 25. 下面这个 "2" 面体 Δ, 其实就是个正方形, 它有 5 个对称轴, 除去恒等变换, 绕着蓝色对称轴旋转可以分别旋转 $\pi/2, \pi, 3\pi/2$, 绕着每条红色的对称轴则只能旋转 π. 因此 $S(\Delta)$ 共有 $3+4+1=8$ 个元素. 我们知道, 这就是我们通常的二面体群 D_4.



例 26. 又比如正四面体 Δ,



它有个 7 对称轴, 过每个顶点有一个对称轴, 过三组对边中点分别有一个对称轴, 除去恒等变换, 绕过顶点对称轴可以旋转 $2\pi/3, 4\pi/3$, 绕过对边中点的对称轴可旋转 π, 因此 $S(\Delta)$ 共有

$$4 \times 2 + 3 \times 1 + 1 = 12$$

个元素. 实际上, 将正四面体的四个顶点等同于 $1,2,3,4$, 我们有群同态

$$\begin{array}{ccc} \phi : S(\Delta) & \longrightarrow & S_4 \\ \sigma & \mapsto & \sigma|_{\Delta_0} \end{array}$$

此群态是单射 ($\mathrm{Ker}\phi = \{I\}$), 且其像集包含了所有的 3 循环, 因此 $\mathrm{Img}\ \phi$ 包含 A_4, 比较元素个数得 $S(\Delta) \cong \mathrm{Im}\,\phi = A_4$.

练习 5. 求出正六面体 (立方体) 的对称群.

2 $\mathrm{SO}(3,\mathbb{R})$ 的有限子群与群作用

对于 $\sigma \in \mathrm{SO}(3,\mathbb{R})$ 但非单位元, 从几何上看, σ 实际上是绕 $\mathfrak{n}_\sigma$ 这个轴的一个旋转变换. 设 $\mathfrak{n}_\sigma$ 所在

直线与单位球面的两个交点为 P_σ 和 $-P_\sigma$. 则 $\pm P_\sigma$ 为单位球面 S^2 上 σ 仅有的两个不动点.

若 G 是 $\mathrm{SO}(3,\mathbb{R})$ 的一个有限子群. 令

$$X := \{\pm P_\sigma | e \neq \sigma \in G\}$$

对于任意 $x \in X, \tau \in G$, 不妨设 $x = P_\sigma$ 或 $-P_\sigma$, 有

$$\begin{aligned}(\tau\sigma\tau^{-1}) \cdot \tau(x) &= \tau\sigma(x) \\ &= \tau(x)\end{aligned}$$

此时 $\tau\sigma\tau^{-1} \neq e$, 但 $\tau(x)$ 被 $\tau\sigma\tau^{-1}$ 固定, 也就是说

$$\tau(x) \in \{\pm P_{\tau\sigma\tau^{-1}}\} \subseteq X.$$

因此 G 可以自然的作用在 X 上: $\tau \cdot x = \tau(x)$.

作用的轨道个数

假设上面群作用的轨道个数为 N, 分别为

$$\mathcal{O}_1, \mathcal{O}_2, \cdots, \mathcal{O}_N$$

由 [NOT]Burnside 引理, 有

$$N = \frac{1}{|G|} \sum_{\sigma \in G} |\operatorname{Fix}(\sigma)|$$

其中

$$\operatorname{Fix}(\sigma) = \{x \in X \mid \sigma(x) = x\}$$

由于 G 中, 单位元 e 固定 $|X|$ 个元素, 而每个 $\sigma \neq e$ 固定 2 个元素, 因此

$$\sum_{\sigma \in G} |\operatorname{Fix}(\sigma)| = |X| + 2(|G| - 1)$$

因此

$$N = \frac{|X|}{|G|} + 2(1 - \frac{1}{|G|}) \qquad (*)$$

对每个轨道 $\mathcal{O}_i$, 设其中的代表元 x_i 对应的稳定子群为 G_i, 则有

$$|\mathcal{O}_i| = \frac{|G|}{|G_i|}$$

所以

$$\frac{|X|}{|G|} = \sum_{i=1}^{N} \frac{|\mathcal{O}_i|}{|G|} = \sum_{i=1}^{N} \frac{1}{|G_i|}$$

从而有

$$N = \sum_{i=1}^{N} \frac{1}{|G_i|} + 2(1 - \frac{1}{|G|}) \qquad (**)$$

将求和部分移到左边, 得

$$\sum_{i=1}^{N}(1 - \frac{1}{|G_i|}) = 2(1 - \frac{1}{|G|})$$

由于 $|G| \geqslant 2$, 所以

$$1 \leqslant 2\left(1 - \frac{1}{|G|}\right) < 2.$$

对于每个轨道 $\mathcal{O}_i$ 来说, 其由 G 中某些非单位元 σ 的一些固定点构成, 因此至少存在一个非单位元 $\sigma \in G_i$, 因此 $|G_i| \geqslant 2$. 所以上式左边的范围是

$$\frac{N}{2} \leqslant \sum_{i=1}^{N}\left(1 - \frac{1}{|G_i|}\right) < N$$

由此

$$1 < N, \quad \frac{N}{2} < 2$$

即 $1 < N < 4$, N 只可能是 2 或 3.

轨道个数 $N = 2$

由上面等式 $(*)$ 可得此时 $|X| = 2$, 两个点正好为 G 中所有非单位元素的共同的旋转轴与单位球面的两个交点, 由于此时 G 有限, 可知 G 是由其中旋转角度最小的旋转变换生成的循环群.

轨道个数 $N = 3$

现在开始, 我们假设有 3 个轨道, 轨道的代表元记为

$$x, y, z$$

相应的稳定子群和三个轨道分别为

$$G_x, G_y, G_z$$
$$\mathcal{O}_x, \mathcal{O}_y, \mathcal{O}_z$$

由上面式 $(**)$, 可得

$$\frac{1}{|G_x|} + \frac{1}{|G_y|} + \frac{1}{|G_z|} = 1 + \frac{2}{|G|} \qquad (***)$$

由于 $|G_x|, |G_y|, |G_z|$ 都是大于等于 2 的整数, 满足

$$\frac{1}{|G_x|} + \frac{1}{|G_y|} + \frac{1}{|G_z|} > 1$$

由于 x, y, z 地位对等, 可假设

$$|G_x| \leqslant |G_y| \leqslant |G_z|$$

$(|G_x|, |G_y|, |G_z|)$ 所有可能的情况是:

$$(2,2,n), n \geqslant 2$$
$$(2,3,m), m = 3,4,5$$

6

二面体群

先来考虑

$$(|G_x|, |G_y|, |G_z|) = (2,2,n), n \geqslant 2$$

的情况, 根据式 $(***)$, 有

$$1 + \frac{2}{|G|} = \frac{1}{2} + \frac{1}{2} + \frac{1}{n}$$

所以 $|G| = 2n$.

情形 1: $n = 2$. 此时

$$|G_x| = |G_y| = |G_z| = 2$$
$$|\mathcal{O}_x| = |\mathcal{O}_y| = |\mathcal{O}_z| = \frac{|G|}{2} = 2$$

令 x', y', z' 为三个轨道中与 x, y, z 不同的另一个元素, g_x, g_y, g_z 为 G_x, G_y, G_z 中的非单位元. 若 $x' \neq -x$, 则 x' 与 x 不在同一直线上, 而 g_x 是绕 x 的旋转, 只固定 $\pm x$, 所以 $g_x(x') \neq x'$, 但 $\{x, x'\}$ 这个轨道只有两个元素, 这使得 $g_x(x') = x$, 从而

$$\begin{aligned} x' &= g_x^2(x') \\ &= g_x(g_x(x')) \\ &= g_x(x) = x \end{aligned}$$

产生矛盾. 因此 $x' = -x$. 同样有 $y' = -y$, $z' = -z$. 这样一来, 我们看到 x, y, z 分别在三个不同的方向上, 下面我们说明他们彼此垂直. 由于 $y \neq \pm x$, 因此 $g_x(y) \neq y$, 这使得 $g_x(y) = -y$. 变换 g_x 是绕轴 x 的旋转, 阶为 2, 因此是旋转 π, 旋转的结果是把 y 变成了 $-y$, 由此可见 x 与 y 垂直. 同理可得 x, z, y, z 相互垂直, 所以 x, y, z 组成两两垂直的三个向量, 而 G 中包含 g_x, g_y, g_z, 都是 2 阶元, 可验证 $g_x g_y = g_z$. 由于 $|G| = 4$, 因此 $G = \{g_x, g_y, g_z, e\}$, 同构于 D_2.

情形 2: $n > 2$. 此时

$$|G_x| = |G_y| = 2, |G_z| = n$$
$$|\mathcal{O}_x| = |\mathcal{O}_y| = n, |\mathcal{O}_z| = 2$$

由于 G_z 是绕 z 旋转构成的有限群, 必为循环群, 生成元设为 g, 即:

$$G_z = \{e, g, \cdots, g^{n-1}\}$$

可以看出 $x \neq \pm z$(因为 $|G_x| = 2$, $G_z = G_{-z}$ 阶数为 $n > 2$), 可以证明

$$x, g(x), \cdots, g^{n-1}(x)$$

两两不同, 否则

$$g^{i-j}(x) = x \text{ 而 } g^{i-j} \neq e,$$

由于 g 的方幂都是绕 z 的旋转, 如果不是恒等变换, 只能固定 $\pm z$, 这使得 $x = \pm z$, 矛盾. 因此

$$\mathcal{O}_x = \{x, g(x), \cdots, g^{n-1}(x)\}$$

由于 g 保距离, 而 $g(z) = z$, 因此这 n 个点到 z 都距离都相同, 而它们自己又形成一个正 n 边形.

$$g(x) - x = g^2(x) - g(x) = \cdots$$

由于 $\mathcal{O}_{-z}$ 与 $\mathcal{O}_z$ 有相同的元素个数, 由情形 1 中讨论知

$$\mathcal{O}_z = \{\pm z\}.$$

假设 $G_x = \{e, g_x\}$, 则有 $g_x(z) \neq z$ (x, z 不同方向), 所以 $g_x(z) = -z$, 从而有 x 与 z 彼此垂直. 由此可见由

$$x, g(x), \cdots, g^{n-1}(x)$$

组成的正 n 边形 Δ 在与 z 垂直且过原点的平面上. 由于 $\Delta_0 = \mathcal{O}_x$, 我们有

$$G \leqslant S(\Delta)$$

即 G 中所有元素 σ 都满足 $\sigma(\Delta_0) = \Delta_0$. 我们前面的例子已经计算过 $S(\Delta) \cong D_n$ 正好也有 $2n$ 个元素, 所以 $G = S(\Delta) \cong D_n$.

7

正多面体的对称群

现在假设

$$(|G_x|, |G_y|, |G_z|) = (2,3,m)$$

其中 $m = 3,4,5$. 根据式 $(***)$, 有

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{m} = 1 + \frac{2}{|G|}$$

所以

$$|G| = \frac{12m}{6-m}$$
$$|\mathcal{O}_x| = \frac{6m}{6-m}, |\mathcal{O}_y| = \frac{4m}{6-m}, |\mathcal{O}_z| = \frac{12}{6-m}$$

$m = 3$ 的情形

此时, $|G| = 12$,

$$|\mathcal{O}_x| = 6, |\mathcal{O}_y| = |\mathcal{O}_z| = 4$$

令 Δ 为 $\mathcal{O}_z$ 中的四个点做为顶点的多面体, 与上面的情况类似有, $G \leqslant S(\Delta)$. 我们将证明 $\mathcal{O}_z$ 中的四个点做为顶点的多面体是正四面体. 由之前的

计算已知 $S(\Delta) \cong A_4$ 正好也有 12 个元素, 从而 $G = S(\Delta) \cong A_4$.

任取 $\mathcal{O}_z$ 中一点 u, 由于 $\mathcal{O}_z$ 有 4 个点, 其中至少还有一点 $v \neq \pm u$. 由于

$$|G_u| = |G_z| = 3,$$

所以 G_u 为 3 阶循环群, 假设生成元为 g, 则

$$v, g(v), g^2(v)$$

两两不同构成正三角形, 且与 u 等距. 由于它们都在 $\mathcal{O}_z$ 中, 因此

$$\mathcal{O}_z = \{u, v, g(v), g^2(v)\}.$$

这告诉我们 $\mathcal{O}_z$ 中的任意三个点都组成正三角形, 且与第四个点等距, 因此它们的确构成正四面体的个 4 个顶点.

$m = 4$ 的情形

此时

$$|G_x| = 2, |G_y| = 3, |G_z| = 4$$
$$|G| = \frac{12 \times 4}{6 - 4} = 24$$
$$|\mathcal{O}_x| = 12, |\mathcal{O}_y| = 8, |\mathcal{O}_z| = 6$$

令 Δ 为 $\mathcal{O}_z$ 中的六个点做为顶点的多面体, 与上面的情况类似有, $G \leqslant S(\Delta)$. 我们将证明 $\mathcal{O}_z$ 中的六个点做为顶点的多面体是正八面体. 其对称轴: 4 组对面中心连线 (可转 $2\pi/3$ 整数倍), 6 组对边中点连线 (可转 π 整数倍), 3 组对点连线 (可转 $\pi/2$ 整数倍), 其对称群共有

$$4 \times 2 + 6 \times 1 + 3 \times 3 + 1 = 24$$

个元素. (练习: 这个对称群同构于 S_4, 提示: 将 $S(\Delta)$ 作用在连接 4 组对面中心点的线段上, 或者考虑正八面体的对偶几何体, 即立方体, 八面体可以立方体 6 个面的中心连接而成, 立方体的对称群与正八面体的对称群相同, 然后将立方体的对称群作用在立方体的 4 组最长对角线上)

同样取 $\mathcal{O}_z$ 中任意一点 u, 其稳定子群 G_u 为 4 阶循环群, 生成元为 g(绕 u 旋转 $\pi/2$), 令 v 为这个轨道中不同于 $\pm u$ 的点, 则

$$v, g(v), g^2(v), g^3(v)$$

两两不同, 组成正方形, 且与 u 等距. 它们也都不可能等于 $-u$ (因为它们都不被 g 固定). 另外

$$|\mathcal{O}_{-u}| = |\mathcal{O}_u| = 6$$

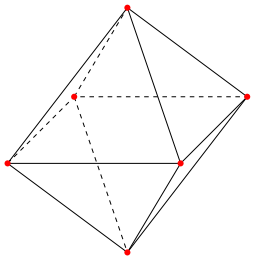
因此 $-u$ 也只能在这个轨道中, 所以这个轨道中的元素是

$$u, v, g(v), g^2(v), g^3(v), -u$$

同样的道理 $-v$ 也在这个轨道中, 因此只能是 $g(v), g^2(v), g^3(v)$ 中的一个 (实际上只能是 $g^2(v)$). 因此

$$v, g(v), g^2(v), g^3(v)$$

形成的正方形在过原点的平面内 (含 v 和 $-v$). 所以 u 与 $g^i(v)$ 垂直, 且均为单位向量, 所以 $v, g(v), g^2(v), g^3(v)$ 到 u 和 $-u$ 的距离都是 $\sqrt{2}$, 而它们组成的正方形的边长亦为 $\sqrt{2}$, 因此它们构成正八面体的 6 个顶点.



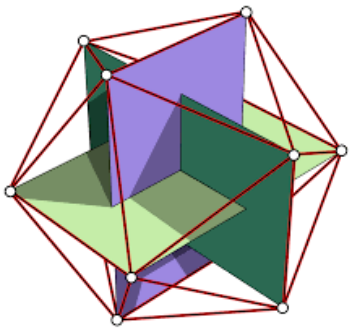
$m = 5$ 的情形

此时

$$|G_x| = 2, |G_y| = 3, |G_z| = 5$$
$$|G| = \frac{12 \times 5}{6 - 5} = 60$$
$$|\mathcal{O}_x| = 30, |\mathcal{O}_y| = 20, |\mathcal{O}_z| = 12$$

令 Δ 为 $\mathcal{O}_z$ 中的 12 个点做为顶点的多面体, 与上面的情况类似有, $G \leqslant S(\Delta)$. 我们将证明 $\mathcal{O}_z$ 中的 12 个点做为顶点的多面体是正二十面体. 同样的思路, 说明正二十面体的对称群是 A_5 恰有 60 个元素, 从而 $G = S(\Delta) \cong A_5$.

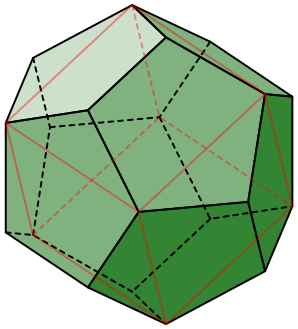
先看下正二十面体长什么样子, 它的顶点为三个彼此垂直的长方形 (长宽比为 $1 + \sqrt{5} : 2$)



对称轴: 6 组对顶点 (可转 $2\pi/5$ 整数倍), 10 组对面中心连线 (可转 $2\pi/3$ 整数倍, 15 组对棱中点连线 (可转 π 整数倍)), 其对称群共有

$$6 \times 4 + 10 \times 2 + 15 \times 1 + 1 = 60$$

个元素, 这个群同构于 A_5? 要说明这个群同构于 A_5, 可以考虑正二十面体的对偶几何体——正十二面体.



正十二面体中有 5 个像红色线条描述的立方体 (每个立方体由三组对边确定, 正十二面体有 30 条边), 而旋转对称变换会置换这个五个立方体 (需要亿点点想像力), 这样可以说明正十二面体的旋转对称群是 A_5, 从而正二十面体的旋转对称群也是 A_5.

这里取出 $\mathcal{O}_z$ 中一点 u, G_u 是 5 阶循环群, 生成元为 g(绕 u 旋转 $2\pi/5$), v 为该轨道中不同于 $\pm u$, 且与 z 距离最小的一点, 则

$$v, g(v), g^2(v), g^3(v), g^4(v)$$

构成正五边形, 且与 u 等距. 值得注意的是 $-v$ 不在此五点 (如果在, 那么 v 和 $-v$ 中点, 也就是原点在这个正五边形内,u 与这个五边形所在面垂直, 从而 O 是这个五边形的中心, 但正五边形中从中心到各顶点的向量没有在一条直线上的, 而向量 v 和 $-v$ 在一点直线上, 矛盾). 显然 $-v$ 与不是 $-u$. 从而

$$-v, -g(v), -g^2(v), -g^3(v), -g^4(v)$$

形成正五边形, 且与 $-u$ 等距. 另外, 由于 $G_{-u} = G_u$ 与 G_z 同构, 因此 $-u$ 所在的轨道也是 12 个元素, 从而 $-u \in \mathcal{O}_z$. 因此这个轨道的中的点分别是

$$\pm u, \pm g^i(v), 0 \leqslant i \leqslant 4$$

从上面的分析我们看到, 选择这个轨道的任意点 u, 其它点到 u 的距离有三种:

u 到 v 的距离

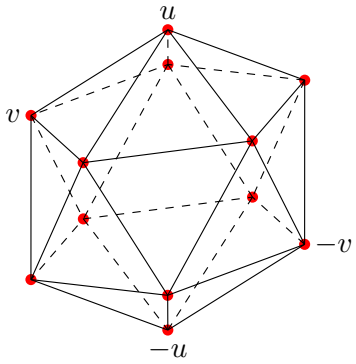
$$0 < d < \sqrt{2}$$

u 到 $-v$ 的距离

$$\sqrt{2} < \sqrt{4 - d^2} < 2$$

u 到 $-u$ 的距离 2.

如下图



由于 u 是选择是该轨道中任意一点, 比如选 v, 则发现轨道中与其它点与 v 的距离同样是 $d\sqrt{4 - d^2}$ 和 2 (因为 d 是 u 与 v 的距离, 小于$\sqrt{2}$, 根据前面的分析 d 是由选定的点唯一确定的). 这样下去, 我们发现图中每个棱长都相等, 每个面都是正三角形, 每个点对应的向量的负向量对应的点也在这个正多面体上, 为正二十面体.

由此我们就在同构意义下全部确定了 $SO(3, \mathbb{R})$ 的有限子群, 它们分别是

$$C_n,\ D_n,\ A_4,\ S_4 \text{ 和 } A_5$$

其中 A_4 对应的是正四面体的旋转对称群, S_4 是立方体和正八面体的旋转对称群, A_5 是正十二面体和正二十面体的旋转对称群.

20 可解群

本期导言

学了这么多群的知识, 是该下山去

"闯荡江湖" 了.

记得我们 "上山" 的目的之一就是想了解

怎样判断一个群是否可解.

这一期我们就来聊聊这个话题.

1 Abel 商群与换位子群

回忆下可解群的定义, 如果存在子群序列

$$\{e\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_0 = G$$

使得相应的每个商群

$$G_i/G_{i+1}$$

都是 Abel 群, 则称 G 可解.

给定群 G, 怎么知道这样的子群序列是否存在呢? 如果存在, 怎么去寻找呢?

把任务分解下, 先实现一个小目标:

怎么判断一个商群是不是 Abel 群?

假设 $N \lhd G$ 是 G 的正规子群, 商群 G/N 是 Abel 的是啥意思呢? 就是

$$abN = baN,\ \forall a, b \in G$$

而这等价于

$$Nab = Nba$$

进一步等价于

$$ab(ba)^{-1} \in N,\ \forall a, b \in G$$

为了记号方便, 现在记

$$[a, b] := (ab)(ba)^{-1} = aba^{-1}b^{-1}$$

称为 a, b 的换位子(commutator).

引理 20.1. 换位子有下面几个重要性质

$$[a, b]^{-1} = [b, a]$$

$$x[a, b]x^{-1} = [xax^{-1}, xbx^{-1}]$$

$$[a, b] = e \quad \text{当且仅当} \quad ab = ba$$

对所有的 $a, b, x \in G$ 成立.

只需要简单检验就能证明.

这个引理也说明了一件很有趣的事情, 如果你取 G 中所有

可以写成若干个换位子的乘积

的元素构成的子集, 记为 G', 你会发现

G' 对乘法和取逆封闭

$$gG'g^{-1} \subseteq G',\ \forall g \in G$$

对乘法封闭很显然, 因为若干个换位子的乘积乘以另外若干个换位子的乘积, 得到更多的 (但还是若干个) 换位子的乘积.

由于换位子的逆还是换位子, 因此 G' 对取逆也是封闭的.

最后, 给定 G' 中一个元素

$$h_1 \cdots h_m$$

其中 h_i 都是换位子, $\forall g \in G$, 我们有

$$g(h_1 \cdots h_m)g^{-1}$$
$$= (gh_1g^{-1})(gh_2g^{-1}) \cdots (gh_mg^{-1})$$

由于换位子被共轭后还是换位子, 由上式, 它们的乘积被共轭后依然是换位子的乘积. 这样可以得到下面这个结论.

引理 20.2. 1. G' 是 G 的正规子群.

2. 如果 N 是 G 的正规子群, 那么 G/N 是 Abel 群当且仅当 $G' \subseteq N$.

证明. 由上面的小黑板可得

G' 是 G 的正规子群

本节一开始就讨论了 $N \lhd G$ 满足

G/N 是 Abel 子群

当且仅当

$$(ab)(ba)^{-1} \in N,\ \forall a, b \in G$$

即

$$[a, b] \in N,\ \forall a, b \in G$$

而这恰好等价于 $G' \subseteq N$.

G' 称为 G 的换位子群或者导群.

2 判断群是否可解的方法

我们看到, 对一个群来说, 其换位子群 G' 不仅是 G 的正规子群, 而且是

使得商群为 Abel 群的最小的正规子群

现在假设 G 可解, 即存在

$$\{e\} = G_m \lhd G_{m-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

使得

$$\text{所有 } G_i/G_{i+1} \text{ 是 Abel 群.}$$

换成上面换位子群的语言就是

$$G_i' \subseteq G_{i+1}, \forall i$$

我们来捋一捋啊.

$$G' = (G_0)' \subseteq G_1$$
$$(G_1)' \subseteq G_2$$
$$\cdots\cdots$$

由换位子群的定义,一个群的子群的换位子群一定包含在大群的换位子群中(因为子群的换位子都是大群的换位子). 由于

$$G' \subseteq G_1$$

因此

$$(G')' \subseteq (G_1)'$$

由此我们得到

$$(G')' \subseteq (G_1)' \subseteq G_2$$

这个游戏可以一直玩下去

$$((G')')' \subseteq ((G_1)')' \subseteq (G_2)' \subseteq G_3$$

如果递归定义

$$G^{(0)} = G$$
$$G^{(i+1)} = (G^i)', \forall i \geqslant 0$$

上面的游戏玩下去就得到

$$G^{(i)} \subseteq G_i, \forall i \geqslant 0$$

特别的

$$G^{(m)} \subseteq G_m = \{e\}$$

从而

$$G^{(m)} = \{e\}.$$

因此,如果 G 可解,那么

$$\text{存在 } m > 0 \text{ 使得 } G^{(m)} = \{e\}$$

反过来,如果

$$G^{(m)} = \{e\} \text{ 对某个 } m > 0 \text{ 成立}$$

我们可以轻松得到如下序列

$$\{e\} = G^{(m)} \lhd G^{(m-1)} \lhd \cdots \lhd G^{(1)} \lhd G^{(0)} = G$$

使得每个商群

$$G^{(i)}/G^{(i+1)} \text{ 是 Abel 群}$$

这是因为 $G^{(i+1)}$ 恰为 $G^{(i)}$ 的换位子群.

因此 G 是可解群. 总结起来

定理 20.3. 有限群 G 是可解群当且仅当

$$\text{存在 } m > 0 \text{ 使得 } G^{(m)} = \{e\}.$$

这个定理给了我们判断一个群是否可解的一个可行方案: 就是不停的计算换位子群,先算 G 的换位子群,再算其换位子群的换位子群,一直算下去,如果最终能“萎缩”到 $\{e\}$,G 就是可解群,否则就是不可解的.

可解群的子群可解

上面的定理还告诉我们

推论 20.4. 可解群的子群是可解群.

证明. 对于 $H \leqslant G$,按定义有

$$H^{(i)} \subseteq G^{(i)}, \forall i \geqslant 0$$

再利用定理20.3可得.

其实,大家设身处地的想想,如果没有上面的判定定理,要说明可解群的子群也是可解群感觉还没有那么容易.

这个推论同时也说明,如果一个群有个子群是不可解的,那么这个群也不可解.

本期最后将证明 A_5 不可解,这将造成

$$S_n, n \geqslant 5 \text{ 不可解}$$

可解群的商群可解

当然也可以问

$$\text{可解群的商群是否可解?}$$

下面这个引理会让答案变得很明显.

引理 20.5. 假设 $N \lhd G, H \leqslant G$,那么

$$(HN/N)' = H'N/N$$

证明. 对于 $h_1, h_2 \in H$

$$\begin{aligned}[h_1N, h_2N] &= (h_1N)(h_2N)(h_1N)^{-1}(h_2N)^{-1} \\ &= h_1N \cdot h_2N \cdot h_1^{-1}N \cdot h_2^{-1}N \\ &= h_1h_2h_1^{-1}h_2^{-1}N \\ &= [h_1, h_2]N\end{aligned}$$

引理中左边 $(HN/N)'$ 中的元素为若干个上式左边形式元素的乘积,而引理中右边 $H'N/N$ 中元素为若干个上式中右边形式元素的乘积,引理得证.

利用这个引理,我们就很容易得到

推论 20.6. 可解群的商群是可解群.

证明. 假设 $N \lhd G$ 而 G 可解.

由引理20.5

$$(G/N)' = (GN/N)' = G'N/N$$

接着玩

$$(G/N)^{(2)} = (G'N/N)' = G^{(2)}N/N$$

这样一直下去 (请用数学归纳法书写)

$$(G/N)^{(i)} = G^{(i)}N/N, \forall i \geqslant 0$$

由于 G 可解, 存在正整数 m 使得

$$G^{(m)} = \{e\}$$

对应的

$$(G/N)^{(m)} = \{e\}N/N = \{N\}$$

为商群 G/N 的单位元群.

由定理20.3, 商群 G/N 可解.

第一个不可解群 A_5

本期最后来认识最小的不可解群 A_5, 即由 S_5 所有偶置换构成的群.

命题 20.7. A_5 的正规子群只有

$$\{e\} \text{ 和 } A_5$$

特别的, A_5 不可解.

证明. 这里采用一个无赖的证明方法.

正规子群都是共轭类的并, 我们先把 A_5 的共轭类全部找出来.

A_5 为 S_5 的 4 个共轭类的并

$$\text{单位元 } e$$

$$5 \text{ 循环 } 24 \text{ 个}$$

$$3 \text{ 循环 } 20 \text{ 个}$$

$$\text{两个不相交 } 2 \text{ 循环乘积}, 15 \text{ 个}$$

这几个共轭类在 A_5 中变成了 5 个共轭类: 上面的第二类分成了两个大小都是 12 的共轭类.

要算这些共轭的大小其实很容易, 对每个元素 σ, 计算它在 A_5 中的共轭类大小, 只需要计算其在 A_5 中的中心化子

$$C_{A_5}(\sigma) = \{\tau \in A_5 \mid \tau\sigma\tau^{-1} = \sigma\}$$

利用群作用的轨道公式有共轭类大小

$$|C_\sigma| = [A_5 : C_{A_5}(\sigma)]$$

如此一来, A_5 的共轭类大小分别是

$$1,\ 15,\ 20,\ 12,\ 12$$

由于 A_5 的正规子群都是若干个共轭类的并, 且必须包含单位元 e 组成的共轭类, 由上面这些共轭大小, 共轭类的并要成为 A_5 的子群, 其元素个数又必须整除 $|A_5|$, 唯二的可能性是

$$1 \text{ 和 } 1 + 15 + 20 + 12 + 12 = 60$$

也就是下面两个子群

$$\{e\},\ A_5$$

由于 A_5 不交换, 因此不可能找到可解群定义中所需要的子群序列, 因此 A_5 不可解.

A_5 是 $S_n,\ n \geqslant 5$ 的子群, A_5 不可解, 那么

推论 20.8. $S_n,\ n \geqslant 5$ 不可解.

记得这门课一开始的时候, 我们说过

$$f(x) = x^5 - x + 1$$

的 Galois 群 $\mathrm{Gal}(f)$ 同构于 S_5, 现在我们已经知道 S_5 不是可解群了, 由 Galois 的定理, 代数方程 $f(x) = 0$ 就不能根式解.

至于为什么 $\mathrm{Gal}(f) \simeq S_5$ 这个问题需要留到 Galois 理论中才能说得明白.

像 A_5 这样没有“真正”(非单位元群, 非自身) 的正规子群的群称为单群 (simple group), 而不交换的单群没有可能找到可解群需要的子群序列, 是不可解群.

下期我们将用“优雅”的方式证明

$$A_n,\ n \geqslant 5 \text{ 是单群}$$

21 单群

本期导言

上期我们看到了 A_5 是单群 (即除单位元群和自身外没有其他正规子群). 本期我们证明

$$A_n,\ n\geqslant 5$$

都是单群, 并简要介绍下史上最浩大的数学工程 (也许没有之一)

有限单群分类定理

以及一般的群如何由单群 “组装” 而成.

$A_n, n\geqslant 5$ 是单群

这里提供比较经典的证明方法.

本小节总假设 $n\geqslant 5$

分为下面几个步骤 1

证明 A_n 的元素都可以写成 3 循环的乘积 2

证明 A_n 中所有 3 循环组成一个共轭类 3

证明 A_n 的正规子群 $N\neq\{e\}$ 必然包含一个 3 循环, 从而只能是 A_n

引理 21.1 **第一步.** A_n 中元素都可以写成 3 循环的乘积.

证明. 我们证明任意两个对换的乘积可以写成 3 循环的乘积, 从而 A_n 中的元素都能写成 3 循环的乘积.

两个对换的乘积有如下三种形式

$$(ab)(ab),\ (ab)(ac),\ (ab)(cd)$$

前两种形式

$$\begin{aligned}(ab)(ab)&=e=(abc)(acb)\\(ab)(ac)&=(acb)\end{aligned}$$

最后一种情形

$$\begin{aligned}(ab)(cd)&=(ab)(bc)(bc)(cd)\\&=(abc)(bcd)\end{aligned}$$

由于 $A_n(n\geqslant 3)$ 中元素都是上述三种元素的乘积, 因此 $A_n(n\geqslant 3)$ 中所有元素都是三循环的乘积.

引理 21.2 **第二步.** A_n 中所有 3 循环组成一个共轭类.

证明. 只需要证明 A_n 中的任意 3 循环 τ 都与 (123) 共轭. 我们已经知道它们在 S_n 中是共轭的, 即存在 $\sigma\in S_n$ 使得

$$\sigma\tau\sigma=(123)$$

如果 σ 是偶置换, 就正合我意, 否则

$$(45)\sigma \text{ 就是偶置换, 且}$$

$$(45)\sigma\tau\sigma^{-1}(45)^{-1}=(45)(123)(45)=(123)$$

因此 3 循环 τ 总与 (123) 在 A_n 中共轭.

第三步有很多种证明.

这里采用 GTM73[2, 第 50 页] 的证明

引理 21.3 **第三步.** 假设

$$\{e\}\neq N\lhd A_n$$

那么 N 至少包含一个 3 循环.

证明. 任取 N 中的非单位元 $\sigma\neq e$, 分解成互不相交循环的乘积

$$\sigma=\pi_1\pi_2\cdots\pi_k$$

其中 π_i 是不相交的循环.

情形 1: 分解中有长度大于 3 的循环

不妨设

$$\pi_1=(123\cdots r),\ r>3$$

取 $\phi=(123)$, 则 ϕ 与 $\pi_i,\ i>1$ 交换, 因此

$$\begin{aligned}\phi\sigma\phi^{-1}&=\phi\pi_1\phi^{-1}\pi_2\cdots\pi_r\\&=\phi\pi_1\phi^{-1}\pi_1^{-1}\sigma\\&=(124)\sigma\end{aligned}$$

由于 N 是正规子群, 因此

$$(\phi\sigma\phi^{-1})\sigma^{-1}=(124)\in N$$

这种情形下 N 包含循环 (124).

情形 2: 分解中循环长度都不超过 3, 有至少两个 3 循环 (此时 $n\geqslant 6$)

不妨设

$$\pi_1=(123),\ \pi_2=(456)$$

令 $\phi=(124)$, 则 ϕ 与 $\pi_i, i>2$ 交换, 从而

$$\begin{aligned}\phi\sigma\phi^{-1}&=\phi\pi_1\pi_2\phi^{-1}\pi_3\cdots\pi_k\\&=\phi\pi_1\pi_2\phi^{-1}\pi_2^{-1}\pi_1^{-1}\sigma\\&=(12534)\sigma\in N\end{aligned}$$

因此

$$\phi\sigma\phi^{-1}\sigma^{-1}=(12534)\in N$$

转化为第一种情形.

情形 3: 分解中循环长度都不超过 3, 恰有一个 3 循环

不妨设 $\pi_1 = (123)$ 是 3 循环, 此时 $\pi_i, i > 1$ 都是对换, 从而 N 包含元素

$$\sigma^2 = \pi_1^2\pi_2^2\cdots\pi_k^2 = (132)$$

情形 4: 分解中全部都是对换

不妨设

$$\pi_1 = (12),\ \pi_2 = (34)$$

令 $\phi = (123)$, 跟前面一样, ϕ 与 $\pi_i, i > 2$ 交换, 通过计算可以发现

$$\begin{aligned}\phi\sigma\phi^{-1} &= \phi\pi_1\pi_2\phi^{-1}\pi_2^{-1}\pi_1^{-1}\sigma\\ &= (13)(24)\sigma\end{aligned}$$

因此

$$(13)(24) = \phi\sigma\phi^{-1}\sigma^{-1} \in N$$

记 $\tau = (13)(24)$, 令 $\eta = (125)$, 则有

$$\tau(\eta\tau\eta^{-1}) = (135) \in N$$

综合起来, N 总包含一个 3 循环.

上面三步做完就可以下结论

定理 21.4. 对任意

$$\{e\} \neq N \lhd A_n,\ n \geqslant 5$$

有 $N = A_n$, 即 $n \geqslant 5$ 时, A_n 是单群.

有限单群分类定理

如果 G 是个 Abel 群, 根据 Cauchy 定理, G 存在 $|G|$ 的任意素因子阶的子群, 同时也是正规子群. 此时 G 是单群当且仅当 G 是素数阶循环群, 即

Abel 单群恰为所有素数阶循环群

非 Abel 的呢, 除了上面的 $A_n, n \geqslant 5$, 还有没有其他的单群呢?

有的, 而且还有很多, 19 世纪 E. Mathieu (1861, 1873) 在寻找多重传递置换群的时候就发现了一类群, 它们中有 5 个是单群, 现在记为

$$M_{11},\ M_{12},\ M_{22},\ M_{23},\ M_{24}$$

是 26 个 (基于不同分类标准, 也有人说 27 个) 零散单群中的 5 个, 它们分别是

$$S_{11},\ S_{12},\ S_{22},\ S_{23},\ S_{24}$$

的子群.

Hölder 在 1892 年就 “意想天开” 的问:

有没有可能分类所有的有限单群?

1911 年 Burnside 就猜测

所有非 Abel 单群都是偶数阶的

这个猜想在 1963 年得到了证实, 即

Feit-Thompson 定理 [1]

这一定理无疑给了数学家们极大的信心, 1972 年 Gorenstein 提出了 “16 步走” 的单群分类计划, 大体上在这个方案的指引下, 往后的 10 年, 一场轰轰烈烈的单群分类运动在群论界展开.

1983 年, Gorenstein 宣称有限单群分类定理已经完成 (事后证明, 当时还不太成熟), 每个有限单群都是下列单群之一

- 素数阶循环群
- $A_n,\ n \geqslant 5$
- Lie 型单群
- 26 个零散单群

这些单群虽然很多, 但它们大多数都是一些特定对象的对称群.

零散单群中最大的 Monster 群, 阶数为

$$2^{46}3^{20}5^9 7^6 11^2 13^3 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71$$

大约为 8×10^{53}, 它实际上真正被构造出来 (Griess, 1982) 的样子是一个

196884 维交换非结合代数

的自同构群.

单群分类定理的证明 (大部分集中在 1955-2004 年) 分散在超过一百个作者, 几百篇上万页的学术论文中, 有些证明还是借助计算机证明的. 因此这个定理直到现在还有很多数学家不愿意相信.

也有一些数学家将自己的晚年都投入到整理这些证明中, 因为他们害怕

这些证明, 如果在它们被遗忘之前不能整理成更可读的版本的话, 将慢慢在数学的现实世界里消失, 埋藏在那些被人们遗忘的废纸堆里.

在 Gorenstein 宣称有限单群分类定理后不久, Gorenstein, Lyons 和 Solomon 等人就开始着手整理这个定理的简化版证明, 原始证明中的一些小漏洞大部分都很快被消灭, 其中一个比较大的漏洞, Smith 和 Aschbacher 花了 7 年时间才修补完成 (2004 年完成).

到目前为止, 这个简化版的完整证明还没有全部完成, 据说会在 2023 年完成, 一共分为 12 本书, 每本 400 页左右, 让我们拭目以待.

单群是“原子”

为什么要分类有限单群呢？其实这个想法非常朴素，就像整数分解素数一样，我们总是希望比较大的群可以由一些比较小的群组成，就像分子由原子组成一样.

给定一个有限群 G，我们可以先找 G 的一个极大正规子群，即

$$G_1 \neq G$$
$$\text{不存在 } H \lhd G \text{ 满足 } G_1 \subset H \subset G$$

由于 G/G_1 的正规子群与 G 中包含 G_1 的正规子群一一对应，因此这实际上等价于说

$$G/G_1 \text{ 是单群}$$

继续找 G_1 的极大正规子群 G_2，G_2 的极大正规子群 G_3，长此以往，由于群的阶数越来越小，最终我们将得到

$$\{e\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

使得所有的

$$G_i/G_{i+1} \text{ 都是单群}$$

这样的序列称为 G 的一个合成序列 (composition series).

但这里有个 Bug 是，上面的合成序列并不是唯一的，这连带着就很让人怀疑这些商群会不会也不是唯一的？

然而，事实并非如此.

定理 21.5 Jordan-Hölder 定理. *假设 G 是有限群，而*

$$\{e\} = G_{n+1} \lhd G_n \lhd \cdots \lhd G_2 \lhd G_1 = G$$
$$\{e\} = H_{m+1} \lhd H_m \lhd \cdots \lhd H_2 \lhd H_1 = G$$

为 G 的两个合成序列，则

$$m = n$$

存在置换 $\sigma \in S_n$，使得

$$G_i/G_{i+1} \simeq H_{\sigma(i)}/H_{\sigma(i)+1},\ \forall i$$

上面这个定理说明，给定一个群，其合成序列中的这些商群是由 G 唯一确定的一些单群，称之为 G 的合成因子 (composition factors). 它们就是构成 G 的那些“原子”.

可解群的“原子”就相当简单.

推论 21.6. *有限 G 是可解群当且仅当其所有的合成因子都是素数阶循环群.*

证明. 如果 G 可解，利用可解群的子群和商群都可解这两点可以说明 G 的合成因子都是可解群. 作为单群，这些合成因子可解唯一的可能性就是它们是交换的单群，即素数阶循环群.

反过来，如果 G 的每个合成因子都是素数阶循环群，那么其合成序列的每个商群都是 Abel 群，因此 G 可解.

如果真的是单群分类“定理”的话，很多原来的群论问题都能够得到解决，从 1980 年到现在，有很多群论和群表示论的工作是基于单群分类定理来做的.

参考文献

[1] W. Feit, J. G. Thompson, Solvability of groups of odd order. *Pacific J. Math.* 13 (1963), 775–1029.

[2] T. Hungerford, Algebra. Springer-Verlag, New York, 1980.

22 环论初步

本期导言

让我们暂时告别“烧脑”的群论, 进入相对轻松的

环论 (ring theory) 世界

这个在数论上成长起来的理论.

环论简史

任何一本抽象代数的书都会告诉你, 环就是一个集合上有两种满足一定公理的运算: 加法和乘法, 就像整数全体 $\mathbb{Z}$, 有理数 $\mathbb{Q}$, 或者 n 阶实矩阵的全体 $M_n(\mathbb{R})$ 一样.

但是什么样的故事激发了人们来定义和研究环的呢? 这些运算满足的公理又是怎样来的呢?

实际上环论早期还是由 (扩展) 整数的分解开始的, 比如 Gauss 证明 Fermat 的素数二平方定理的过程中需要将奇素数 p 在

$$\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$$

中进行分解, 这里的 $\mathbb{Z}[i]$ 就具有加法和乘法两种运算, 最后成为我们今天研究的“环”的一份子.

但环论产生的最大动力还是来自于对 Fermat's Last Theorem(费马大定理) 的研究, 即

> 对于 $n\geqslant 3$, 不存在正整数 x,y,z 使得
> $$x^n+y^n=z^n$$

这个定理最后在 1995 年由 Wiles 证明. 先来看下这个定理早期的一些进展.

年份	情形	数学家
1640 左右	$n=4$	Fermat(费马)
1753	$n=3$	Euler(欧拉)
1825	$n=5$	Legendre 和 Dirichlet
1832	$n=14$	Dirichlet
1839	$n=7$	Lamé

1847 年 Lamé 宣称他证明了费马大定理, 但 Liouville 指出他的证明依赖于某些“环”中的元素的唯一分解性质, 而这个性质多半不一定成立, 用今天的话说, 就好像在 $\mathbb{Z}[\sqrt{-3}]$ 中, 4 可以有两种分解

$$4=2\times 2$$
$$4=(1+\sqrt{-3})(1-\sqrt{-3})$$

而 2 和 $1\pm\sqrt{-3}$ 都不能再继续分解了.

但 $\mathbb{Z}[i]$ 中却呈现出另一番景象, 在 $\mathbb{Z}[i]$ 中, 每个元素都能像整数唯一分解成素数的乘积一样唯一分解.

实际上, 如果取

$$\omega=\frac{-1+\sqrt{3}i}{2}$$

为三次单位根, 那么

$$\mathbb{Z}[\omega]=\{a+b\omega+c\omega^2 \mid a,b,c\in\mathbb{Z}\}$$

中依然存在像整数中那样的唯一分解性质, 而这个性质可以用来证明费马大定理 $n=3$ 的情形.

紧接着, 在 1847 年, Kummer 用他发明的 “ideal complex numbers” 证明了费马大定理的 $n<100$ 除 $n=37,59,67,74$ 的所有情形.

天才的 Dedekind 把根据 “ideal complex numbers” 的性质定义了 ideal(我们称之为 “理想”), 从此环开始有了它的抽象的雏形, Dedekind 还将素数的概念推广到了素理想, 后来 Dedekind, Weber, Hilbert 等还研究了多项式 “环” 的问题.

环的公理化定义还是要归功于史上最伟大的女数学家之一的 Emmy Noether, 她将多项式 “环” 和前面这些数 “环” 的研究统一成 “交换环” (指其中的乘法是交换的).

而非交换的环则走了另外一条路与交换环相遇. 非交换的环也许应该起步于 Hamilton 的四元数环, 加上后面的矩阵方阵的性质. 这些集合也有加法和乘法, 与之前的多项式和数的区别在于, 这里的乘法并不是交换的.

交换和非交换的 “环” 在 1930 年代终于合为一体, 成为今天环的定义

定义 22.1. 假设 R 是一个非空集合且 R 上有两种二元运算, 记为 $+$ 和 $\cdot$, 满足下列性质

1. $(R,+)$ 是 Abel 群
2. $(R,\cdot)$ 满足结合律

3. 对任意 $a,b,c\in R$, 两个分配律成立

$$a\cdot(b+c)=a\cdot b+a\cdot c$$
$$(b+c)\cdot a=b\cdot a+c\cdot a$$

环的例子

很显然, 前面说过的

$$\mathbb{Z},\mathbb{Z}[i],\mathbb{Z}[\sqrt{-3}],M_n(\mathbb{R})$$

等都有加法和乘法两种运算, 在加法下是 Abel 群, 乘法满足结合律, 而乘法对加法满足分配律, 因此他们全部都是环 (ring).

这里需要指出的是, 由于这里并没有要求乘法有单位元, 因此像 $2\mathbb{Z}$(全体偶数) 这样的集合在加法和乘法下也构成环.

另外, 在群论中见到的

$$\mathbb{Z}_n\text{: 模 } n \text{ 的剩余类}$$

上面已经有个加法

$$(i+n\mathbb{Z})+(j+n\mathbb{Z})=i+j+\mathbb{Z}$$

并且在这个加法下确为 Abel 群. 如果你大胆一点, 在上面定义乘法

$$(i+n\mathbb{Z})(j+n\mathbb{Z})=ij+n\mathbb{Z}$$

可以很容易验证这个乘法是良好定义的, 且满足结合律以及对于之前的加法的分配律, 因此

$$(\mathbb{Z}_n,+,\cdot)$$

下也构成环, 这个环在后面我们讲中国剩余定理以及其应用 (RSA 加密方法) 的时候将起到非常重要的作用.

环中运算的基本性质

环上有两个运算: 加法和乘法.

其加法的单位元记为 0, 称为零元

一个元素 a 在加法下的逆元记为 $-a$.

为了简便, $a+(-b)$ 将记为 $a-b$.

乘法如果有单位元则记为 1.

它们满足几个比较简单的基本性质

引理 22.2.

$$0\cdot a=a\cdot 0=0$$
$$-(a\cdot b)=(-a)\cdot b=a\cdot(-b)$$

证明. $a\cdot 0=a\cdot(0+0)=a\cdot 0+a\cdot 0$

两边同时加上 $-(a\cdot 0)$, 可得

$$0=a\cdot 0$$

类似可得 $0\cdot a=0$.

$$a\cdot b+(-a)\cdot b=(a+(-a))\cdot b=0\cdot b=0$$

因此

$$-(a\cdot b)=(-a)\cdot b$$

同样的道理可得

$$-(a\cdot b)=a\cdot(-b)$$

让人操碎心的乘法

一个环在加法下是 Abel 群, 已经好得不能再好了, 因此, 当我们对环进行区分时, 都是以其乘法的性质来区别的, 如:

$$\text{有 1 环: 乘法有单位元的环}$$
$$\text{交换环: 乘法满足交换律的环}$$

零因子

在我们比较

$$\mathbb{Z}_6 \text{ 与 } \mathbb{Z}$$

的区别的时候, 我们会发现, 在 Z_6 中会出现

$$(2+6\mathbb{Z})(3+6\mathbb{Z})=0+6\mathbb{Z}$$

也就是说 $\mathbb{Z}_6$ 中的两个非零元

$$2+6\mathbb{Z} \text{ 和 } 3+6\mathbb{Z}$$

的乘积为零元, 而 $\mathbb{Z}$ 中则不会发生这样的现象.

如果环 R 中两个非零元 a,b 的乘积 $ab=0$, 则称 a 为 R 的左零因子, b 称为 R 的右零因子, 此时, 我们称环 R 有零因子.

$\mathbb{Z}$ 上不会发生这样的现象 (两个非零元的乘积为零), 我们称 $\mathbb{Z}$ 无零因子.

如果元素 a 不是零因子, 有个很大的好处

引理 22.3. 假设 a 为环 R 中非零元.

1. 如果 a 不是左零因子, 那么

$$a\cdot b=a\cdot c\Rightarrow b=c$$

2. 如果 a 不是右零因子, 那么

$$b\cdot a=c\cdot a\Rightarrow b=c$$

证明. 由

$$a\cdot b=a\cdot c$$

可得

$$a\cdot(b-c)=0$$

由于 a 不是左零因子, 因此

$$b-c=0$$

即 $b=c$. 另一种情形类似.

元素的逆元

由于环在加法下是 Abel 群, 每个元素在加法下都有逆元, 因此我们这里说逆元还是针对乘法.

如果 R 是有 1 环, 即乘法有单位元. 此时会发生这样的现象: 有些元素在乘法下有逆元, 即

$$a\cdot b=1=b\cdot a$$

称 b 与 a 为可逆元, 记 $a^{-1}=b$.

$R=M_n(\mathbb{R})$ 中, 乘法下有逆元的恰为那些可逆矩阵.

稍微反直觉的是 $\mathbb{Z}$, 整数中可逆的元素跟我们想的可能不太一样. 按定义需要满足

$$mn=nm=1$$

的整数 m,n 互逆, 但这样的话 m 和 n 只能是 ±1, 因此 $\mathbb{Z}$ 中的可逆元是 ±1, 而不是所有非零元.

$\mathbb{Z}_n$ 中的可逆元呢? 这个环一共 n 个元素

$$i+n\mathbb{Z},\ i=0,\cdots,n-1$$

如果其中两个元素

$$i+n\mathbb{Z}\text{ 和 }j+n\mathbb{Z}\text{ 互逆}$$

则有

$$ij+n\mathbb{Z}=1+n\mathbb{Z}$$

即存在整数 s, 使得

$$ij-1=sn$$

从而

$$ij+sn=1$$

所以 i 与 n 都互素.

反过来, 如果 i 与 n 互素, 则存在整数 j,s, 使得

$$ij+sn=1$$

从而

$$(i+n\mathbb{Z})(j+n\mathbb{Z})=1+\mathbb{Z}$$

即 $i+n\mathbb{Z}$ 在 $\mathbb{Z}_n$ 中可逆.

总结起来, $\mathbb{Z}_n$ 中可逆的元素恰为

$$\{i+n\mathbb{Z}\mid i\text{ 与 }n\text{ 互素 }\}$$

环的单位元群

一个有 1 环 R 中的可逆元称为 R 的单位(unit), R 中所有单位的全体记为 $U(R)$, 它在 R 的乘法下显然构成一个群, 称为 R 的单位元群(The unit group).

由上面的讨论, 我们有

环 R	$U(R)$
$\mathbb{Z}$	$\{\pm1\}$
$\mathbb{Z}_n$	$\{i+n\mathbb{Z}\mid(i,n)=1\}$
$M_n(\mathbb{R})$	$\mathrm{GL}_n(\mathbb{R})$
$\mathbb{R}$	$\mathbb{R}^*=\mathbb{R}\backslash\{0\}$

当 p 为素数时, $1,2,\cdots,p-1$ 都与 p 互素, 因此

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

共有 $p-1$ 个元素, 跟拉格朗日定理结合起来有个很神奇的应用.

定理 22.4 Fermat 小定理. 假设 p 为素数, 则对任意整数 a, 有

$$a^p\equiv a\pmod p$$

证明. 如果考虑 $\mathbb{Z}_p$ 中元素

$$a+p\mathbb{Z}$$

如果 $p\mid a$, 则 $p\mid a^p$, 因此

$$a^p\equiv0\equiv a\pmod p$$

如果 $p\nmid a$, 则

$$a+p\mathbb{Z}\in U(\mathbb{Z}_p)$$

由拉格朗日定理, 其阶数必然整除 $U(\mathbb{Z}_p)$ 的阶数 $p-1$, 从而

$$(a+p\mathbb{Z})^{p-1}=1+p\mathbb{Z}$$

从而

$$(a+p\mathbb{Z})^p=a+p\mathbb{Z},\text{即}$$

$$a^p+p\mathbb{Z}=a+p\mathbb{Z}$$

所以

$$a^p-a\in p\mathbb{Z}$$

$$a^p\equiv a\pmod p$$

6 整环、除环、域

最后来看我们比较关心的环的种类.

整环

整环指的是满足下面条件的环

有 1、交换、无零因子

比如: $\mathbb{Z}$, $\mathbb{Q}[x], \mathbb{Z}[x], \mathbb{Z}[i]$ 等.

域

一个域(field) 指得是满足

有 1, 交换, 每个非零元都可逆

的环, 也就是所有非零元都可逆的整环. 例如:

$$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p (p \text{ 为素数})$$

除环

一个除环是指满足

有 1, 每个非零元都可逆

的环, 跟域的区别是除环不一定交换.

7 Hamilton 四元数环

显然所有的域都是除环, 问题是有没有不是域的除环呢?

有的! 这里举一个经典的例子:

Hamilton 四元数环

Hamilton 四元数环 $\mathbb{H}$ 是一个 4 维的实向量空间, 它的一组基记为

$$1,\ i,\ j,\ k$$

并规定它们之间的乘积为

$$i^2 = j^2 = k^2 = ijk = -1$$

可以验证 $\mathbb{H}$ 满足结合率, 是一个环, 但它不是交换的.

这个环的乘积有非常有趣的性质, i, j, k 之间的乘法规律与在维空间中的外积乘法规律相同.

$$ij = k,\ jk = i,\ ki = j$$

有点像 “时间加空间” 形成的向量空间, 放在物理中是描述时空的很好的模型, 比如洛伦兹变换和狭义相对论就可以用 $\mathbb{H}$ 中的乘法简洁的描述 (由于我有限的物理知识已经忘得差不多了, 等我学会了再跟大家聊).

如果把 i, j, k 生成的三维空间看做现实中的三维空间的话, 取

$$v = x_1 i + y_1 j + z_1 k$$

$$w = x_2 i + y_2 j + z_2 k$$

那么它们在 $\mathbb{H}$ 中的乘积

$$vw = v \times w - v \cdot w$$

恰为对两个向量外积与内积的差.

下面我们来证明 $\mathbb{H}$ 是一个除环, 对任意 $\mathbb{H}$ 中的非零元

$$a + xi + yj + zk$$

记 $v = xi + yj + zk$, 我们有

$$\begin{aligned}(a + xi + yj + zk)(a - xi - yj - zk) &= (a + v)(a - v) \\ &= a^2 + av - av - v \times v + v \cdot v \\ &= a^2 + x^2 + y^2 + z^2\end{aligned}$$

由此可见, $\mathbb{H}$ 中的任意非零元

$$a + xi + yj + zk$$

的逆元是

$$\frac{a - xi - yj - zk}{a^2 + x^2 + y^2 + z^2}$$

网络上有很多关于 Hamilton 怎么发现四元数环的传说, 以及四元数环的应用, 大家可以通过搜索

Hamilton Quaternion

阅读更多关于四元数环的内容.

23 环同态与理想

本期导言

环也许是最励志的代数对象, 因为它有

理想 (ideal)

且看分解!

环的同态, 第一同构定理

回想群论里, 我们利用群同态来比较两个群之间的差异和联系. 线性代数里, 我们用线性映射来比较两个向量空间.

这个思想可以说讨论各种代数结构的信仰.

如果考虑两个环之间的联系应该考虑什么样的映射呢? 很显然这个映射应该像群同态和线性映射一样保持两边的运算.

再回想下咱们环是什么? 一个环 $(R,+,\cdot)$ 是一个 Abel 群 $(R,+)$ 的基础上有一个满足结合律乘法 "$\cdot$" , 并且乘法相对于加法满足分配律.

由此看来, 联系两个环的映射应该如下

定义 23.1. 假设 R 和 S 是两个环, 它们之间的一个环同态 (ring homomorphism) 是一个映射

$$\phi : R \longrightarrow S$$

满足对任意 $a,b \in R$

$$\phi(a+b) = \phi(a) + \phi(b)$$
$$\phi(a\cdot b) = \phi(a)\cdot\phi(b)$$

有了两个环之间的环同态

$$\phi : R \longrightarrow S$$

我们怎么比较这两个环呢?

如果我们突然失忆, 忘记两个环的乘法, 此时 ϕ 依然不失为 R 到 S 的加法群同态, 有

$$\operatorname{Ker}\phi = \{a \in R \mid \phi(a) = 0\}$$

根据群同态基本定理的第一同构定理, 有群群同构

$$R/\operatorname{Ker}\phi \simeq \operatorname{Im}\phi$$
$$a + \operatorname{Ker}\phi \mapsto \phi(a)$$

这时我们恢复记忆, 很容易发现右边

$$\operatorname{Im}\phi$$

上依然有乘法

$$\phi(a)\cdot\phi(b) = \phi(a\cdot b)$$

这样 $\operatorname{Im}\phi$ 既是 S 的 Abel 子群又对乘法封闭, 这样的子集称为 S 的子环(subring).

但左边

$$R/\operatorname{Ker}\phi$$

上有没有乘法呢? 如果有的话, 刚才的群同构

$$R/\operatorname{Ker}\phi \simeq \operatorname{Im}\phi$$

就有可能变成一个环同构 (环同态 + 双射), 从而成功 "致敬" 群同态基本定理的第一同构定理.

从现在开始, 我们省略乘法的 "$\cdot$"

实际上, 如果定义

$$(a+\operatorname{Ker}\phi)(b+\operatorname{Ker}\phi) = ab + \operatorname{Ker}\phi$$

的话, 我们肯定会问它是不是 well-defined? 也就是说如果

$$a + \operatorname{Ker}\phi = a' + \operatorname{Ker}\phi$$
$$b + \operatorname{Ker}\phi = b' + \operatorname{Ker}\phi$$

是否有

$$ab + \operatorname{Ker}\phi = a'b' + \operatorname{Ker}\phi?$$

翻译一下就是, 如果

$$a - a' \in \operatorname{Ker}\phi$$
$$b - b' \in \operatorname{Ker}\phi$$

是否有

$$ab - a'b' \in \operatorname{Ker}\phi?$$

实际上

$$\begin{aligned} ab - a'b' &= ab - ab' + ab' - a'b' \\ &= a(b-b') + (a-a')b' \end{aligned}$$

利用下面这个引理很容易证明

$$a(b-b') + (a-a')b'$$

的确是属于 $\operatorname{Ker}\phi$ 的.

引理 23.2. 对任意 $r \in R, u \in \operatorname{Ker}\phi$

$$ru \in \operatorname{Ker}\phi$$

$$ur \in \operatorname{Ker}\phi$$

利用这个引理, 上面的

$$a(b-b') \in \operatorname{Ker}\phi \text{ (因为 } b-b' \in \operatorname{Ker}\phi)$$
$$(a-a')b' \in \operatorname{Ker}\phi \text{ (因为 } a-a' \in \operatorname{Ker}\phi)$$

由于 $\operatorname{Ker}\phi$ 是 R 的加法子群, 对加法封闭, 因此

$$a(b-b') + (a-a')b' \in \operatorname{Ker}\phi$$

引理的证明. 这个证明很简单, 只需要用 ϕ 作用上去看看就可以了.

$$\phi(ru) = \phi(r)\phi(u) = \phi(r)\cdot 0 = 0$$
$$\phi(ur) = \phi(u)\phi(r) = 0\cdot\phi(r) = 0$$

因此 ru 和 ur 都属于 $\operatorname{Ker}\phi$.

所以 $R/\operatorname{Ker}\phi$ 上真的有个 well-defined 的乘法

$$(a+\operatorname{Ker}\phi)(b+\operatorname{Ker}\phi)=ab+\operatorname{Ker}\phi$$

和其上原有的加法

$$\begin{aligned}&(a+\operatorname{Ker}\phi)+(b+\operatorname{Ker}\phi)\\=&(a+b)+\operatorname{Ker}\phi\end{aligned}$$

合并一处, 很容易发现 $R/\operatorname{Ker}\phi$ 在加法和乘法下构成环, 并且原来的群同构

$$\begin{aligned}R/\operatorname{Ker}\phi&\longrightarrow\operatorname{Im}\phi\\a+\operatorname{Ker}\phi&\mapsto\phi(a)\end{aligned}$$

在保持加法的同时也保持乘法, 从而是

环同构!

这样我们就 “致 (shan) 敬 (zhai)” 了群同态基本定理的第一同构定理

定理 23.3 环同态基本定理-第一同构定理.
假设有环同态

$$\phi:R\longrightarrow S$$

那么我们有环同构

$$\begin{aligned}R/\operatorname{Ker}\phi&\simeq\operatorname{Im}\phi\\a+\operatorname{Ker}\phi&\mapsto\phi(a)\end{aligned}$$

环的理想

上面的 $\operatorname{Ker}\phi$ 是这样一种存在:

1. 它是 R 的加法子群
2. 对应的加法商群 $R/\operatorname{Ker}\phi$ 上有乘法

$$\begin{aligned}&(a+\operatorname{Ker}\phi)(b+\operatorname{Ker}\phi)\\=&ab+\operatorname{Ker}\phi\end{aligned}$$

这个商群上有乘法最关键的地方就在上面的引理23.2, 即对所有的 $r\in R, u\in\operatorname{Ker}\phi$

$$ru, ur \text{ 依然属于 } \operatorname{Ker}\phi$$

一般的, 如果

1. I 是 R 的加法子群
2. 对任意 $r\in R, u\in I$ 有

$$ru, ur\in I$$

也就是说 I 中元素与任意元素的乘积还在 I 中.

那么加法商群 R/I 上有 well-defined 乘法

$$(a+I)(b+I)=ab+I$$

(证明跟上面 $I=\operatorname{Ker}\phi$ 的情形一致), 从而使得这个商群 R/I 成为一个环. 此时

$$\begin{aligned}&I \text{ 为 } R \text{ 的一个理想(ideal), 记为 } I\lhd R\\&R/I \text{ 为 } R \text{ 关于 } I \text{ 的商环}\end{aligned}$$

很显然, 任意 R 到 S 的环同态的 Kernel 都是 R 的理想.

其实每个理想都确实也是某个环同态的 Kernel: 假设 I 是环 R 的一个理想, 只需要考虑自然满同态

$$\begin{aligned}\pi:R&\longrightarrow R/I\\a&\mapsto a+I\end{aligned}$$

以前我们已经知道 π 是加群同态且 $\operatorname{Ker}\pi=I$, 只需要验证 π 的确是环同态即可, 也就是验证 π 保持乘法, 而这个是显而易见的.

$$\begin{aligned}\pi(ab)&=ab+I\\&=(a+I)(b+I)\\&=\pi(a)\pi(b).\end{aligned}$$

另外, 每个环 R 都有一些比较无聊的理想, 比如:

$$\{0\} \text{ 和 } R$$

这些称为 R 的平凡理想 (trivial ideal).

理想的例子

现在我已经迫不及待的想看看一些环的理想到底是什么样子? 相应的商环到底是什么? 这个理想能给我们带来什么好处?

先看最简单的例子: 整数环 $\mathbb{Z}$.

假设 I 是 $\mathbb{Z}$ 的理想, 它首先得是 $\mathbb{Z}$ 的加法子群. 在加法下 $\mathbb{Z}$ 是循环群, 其子群也是循环群, 因此 I 只能是某个 $m\mathbb{Z}(m$ 为整数), 即所有 m 的倍数组成的集合.

这样的子群是不是真的都是理想呢? 只需要验证是否满足理想定义的第二条就行了: 对任意 $mx\in m\mathbb{Z}, r\in\mathbb{Z}$, 有

$$r(mx)=(mx)r=mrx\in m\mathbb{Z}$$

所以 $m\mathbb{Z}, m\in\mathbb{Z}$ 恰为 $\mathbb{Z}$ 的所有理想.

对每个 $m\mathbb{Z}$, 它对应的商环我们已经见过了, 就是

$$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$$

理想的交、和、乘积

给定环 R 的两个理想 I 和 J, 其实我们还可以得到相关的一些 R 的理想, 比较典型的是下面几个

$$I \cap J$$

$$I + J = \{x + y \mid x \in I, y \in J\}$$

$$IJ = \{\text{有限和} \sum x_k y_k \mid x_k \in I, y_k \in J\}$$

作为练习, 大家可以验证下它们确实依然是 R 的理想.

前面两个大家都比较容易理解, 最后 IJ 这个需要说两句, 如果将 IJ 定义为

$$\{xy \mid x \in I, y \in J\}$$

的话, IJ 将不一定对加法封闭, 可能都不是 R 的加法子群, 更别提理想了.

更多“致敬”同态基本定理

跟群同态基本定理一样, 除了第一同构定理以外, 也可以有第二同构定理和第三同构定理, 以及商环的理想与原来环的理想之间的对应关系.

定理 23.4 第二同构定理. 假设 R 是一个环, I 是 R 理想, 而 S 是 R 的子环, 则有环同构

$$S/(S \cap I) \simeq (S + I)/I$$

证明. 这个证明跟群同态基本定理的第二同构定理没有本质的区别.

首先大家验证下 $S + I$ 确实还是 R 的子环, 这样 I 也是 $S + I$ 的理想, 考虑环同态

$$\pi : S \longrightarrow (S + I)/I$$

$$s \mapsto s + I$$

它是满同态且 Kernel 正好是 $S \cap I$, 由第一同构定理就完成证明!

定理 23.5 第三同构定理. 假设 R 是一个环, 而 $I \subseteq J$ 是 R 的两个理想, 那么 J/I 是 R/I 的理想且有环同构

$$(R/I)/(J/I) \simeq R/J$$

证明. 这个证明也是个体力劳动, 考虑环同态

$$\phi : R/I \longrightarrow R/J$$

$$a + I \mapsto a + J$$

(well-defined?)

这是个环的满同态且 Kernel 正好是

$$J/I$$

由第一同构定理得证.

关于环的满同态同样有下面的定理

定理 23.6. 假设

$$\phi : R \longrightarrow S$$

是环的满同态, 则

$$\{R \text{ 的包含 } \operatorname{Ker}\phi \text{ 的理想 (或子环)}\}$$

与

$$\{S \text{ 的理想 (或子环)}\}$$

一一对应, 对应关系是

$$J \mapsto \phi(J), \forall I \subseteq J \lhd R$$

$$K \mapsto \phi^{-1}(K), \forall K \lhd S$$

证明. 实际上, 将 ϕ 看作加群的同态, 我们已经能够得到 R 的含 I 的加法子群与 S 的加法子群之间的一一对应, 大家只需要验证下, 这个对应下总是把理想 (子环) 变为理想 (子环) 就行了.

考虑自然满同态

$$\pi : R \longrightarrow R/I$$

我们可以得到下面的推论.

推论 23.7. 假设 I 是环 R 的一个理想, 那么商环 R/I 的理想 (子环) 与 R 中含 I 的理想 (子环) 一一对应

24 中国剩余定理

本期前言

上期说到理想的定义，环同态基本定理，还没有告诉我们理想有什么好处呢？本期来看看怎么用理想来解决数的问题

中国剩余定理

(Chinese Remainder Theorem) 这是近世代数中唯一以中国命名的定理.

你知道么？这个定理还与现在珠算口诀以及卷尺的发明有一面之缘，且看本期道来.

1 数的问题用理想描述

上期我们看到 $\mathbb{Z}$ 的理想恰为那些 $m\mathbb{Z}$，每个这样的理想都由一个整数 m 决定.

那整数的关系是否能用理想来描述呢？

比如 $m \mid n$？容易发现，这等价于

$$n\mathbb{Z} \subseteq m\mathbb{Z}$$

$(m,n)=d$? 很不容易发现，这等价于

$$m\mathbb{Z}+n\mathbb{Z}=d\mathbb{Z}$$

实际上，仔细思考下，这个也没有那么难以理解. 由于 m,n 都是 d 的倍数，因此左边集合中的元素都是 d 的倍数，因此

$$m\mathbb{Z}+n\mathbb{Z} \subseteq d\mathbb{Z}$$

另一方面，由于 d 是 m,n 的最大公因数，因此存在整数 s,t 使得

$$d=ms+nt$$

所以 $d \in m\mathbb{Z}+n\mathbb{Z}$，从而

$$d\mathbb{Z} \subseteq m\mathbb{Z}+n\mathbb{Z}$$

因此

$$m\mathbb{Z}+n\mathbb{Z}=d\mathbb{Z}$$

推论：m,n 互素当且仅当

$$m\mathbb{Z}+n\mathbb{Z}=\mathbb{Z}$$

假设 m,n 的最小公倍数是 $[m,n]$，则

$$[m,n]\mathbb{Z}=m\mathbb{Z}\cap n\mathbb{Z}$$

总结成一张小表

整数语言	理想语言
$m \mid n$	$n\mathbb{Z} \subseteq m\mathbb{Z}$
$(m,n)=d$	$m\mathbb{Z}+n\mathbb{Z}=d\mathbb{Z}$
$(m,n)=1$	$m\mathbb{Z}+n\mathbb{Z}=\mathbb{Z}$
$l=[m,n]$	$l\mathbb{Z}=m\mathbb{Z}\cap n\mathbb{Z}$
mn	$mn\mathbb{Z}=(m\mathbb{Z})(n\mathbb{Z})$

2 理想为数

现在我们可以把目光转向

有 1 环

这是广泛的环，整数环 $\mathbb{Z}$，多项式环，还有复数域的那些子环，全矩阵环都可以进入火力范围.

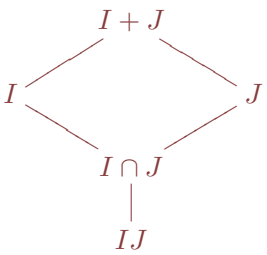
假设 R 是一个有 1 环，像 $\mathbb{Z}$ 中一样，我们可以把 R 中的理想当作数来对待，比如，我们可以定义

理想的关系	定义
理想 I 整除 J	$J \subseteq I$
理想 I 与 J 互素	$I+J=R$

解释这样做有什么好处之前，回顾上期两个理想 I 与 J 的几种运算

$$I+J,\ IJ,\ I\cap J$$

这些都是 R 的理想，它们之间的包含关系可用下面的图表示



由于理想的吸收性质得

$$IJ \subseteq I,\ IJ \subseteq J$$

所以

$$IJ \subseteq I\cap J$$

另外，由于 I 中元素 x 都可以写成

$x+0$ 的形式，属于 $I+J$

因此 $I \subseteq I+J$, 同理 $J \subseteq I+J$.

引理 24.1. 对任意环 R, 假设 I, J, K 为环 R 的三个理想, 则有

$$(I+J)K = IK + JK$$
$$K(I+J) = KI + KJ$$

证明. 由于 $I \subseteq I+J$, 所以

$$IK \subseteq (I+J)K$$

同理

$$JK \subseteq (I+J)K$$

作为理想 $(I+J)K$ 关于加法封闭, 因此

$$IK + JK \subseteq (I+J)K$$

反过来, $(I+J)K$ 中的元素为有限和

$$\sum (x_t + y_t)z_t$$

其中 $x_t \in I$, $y_t \in J$, $z_t \in K$. 这里每一项

$$(x_t + y_t)z_t = x_t z_t + y_t z_t \in IK + JK$$

$IK + JK$ 同样对加法封闭, 所以

$$\sum (x_t + y_t)z_t \in IK + JK$$

从而

$$(I+J)K \subseteq IK + JK$$

所以

$$(I+J)K = IK + JK$$

同理, 我们有

$$K(I+J) = KI + KJ$$

引理得证.

好了, 现在我们可以用两个例子来说明下把理想看成数有什么好处了.

比如整数中有这样的结论

$$m \mid rn,\ (m,n) = 1 \Rightarrow m \mid r$$

翻译成理想的语言

如果

$$(r\mathbb{Z})(n\mathbb{Z}) \subseteq m\mathbb{Z},\ n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$$

那么

$$r\mathbb{Z} \subseteq n\mathbb{Z}$$

放到一般有 1 环中:

命题 24.2. 假设 I, J, K 为有 1 环 R 的理想满足

$$IJ \subseteq K \ (K \text{ 整除 } IJ)$$

$$J + K = R \ (K \text{ 与 } J \text{ 互素}) \text{ 那么}$$
$$I \subseteq K \ (K \text{ 整除 } I)$$

证明. 由于 R 是有 1 环, 所以

$$IR = I$$

结合引理24.1

$$I = IR = I(J+K) = IJ + IK$$

由理想的收性质

$$IK \subseteq K$$

加上 $IJ \subseteq K$, 因此

$$IJ + IK \subseteq K$$

所以

$$I \subseteq K$$

这个证明是不是很神奇?

咱们可以再来一个.

$$(m, r) = 1,\ (n, r) = 1$$
$$\Rightarrow (mn, r) = 1$$

翻译成理想语言

如果

$$m\mathbb{Z} + r\mathbb{Z} = \mathbb{Z}$$
$$n\mathbb{Z} + r\mathbb{Z} = \mathbb{Z}$$

那么

$$(m\mathbb{Z})(n\mathbb{Z}) + r\mathbb{Z} = \mathbb{Z}$$

在有 1 环中:

命题 24.3. 假设 I, J, K 为有 1 环 R 的理想, 满足

$$I + K = R,\ J + K = R$$

那么

$$IJ + K = R$$

证明. 首先由于 R 是有 1 环, 所以

$$RR = R$$

且看操作

$$\begin{aligned} R &= RR \\ &= (I+K)(J+K) \\ &= IJ + IK + KJ + KK \\ &\subseteq IJ + K \end{aligned}$$

最后一步包含关系由 K 的吸收性质得到.

显然 $IJ + K \subseteq R$, 所以

$$R = IJ + K$$

大家可以自己看看还有哪些整数的结论在有 1 环或者有 1 交换环中依然正确.

中国剩余定理

现在来到本期的重头戏:

中国剩余定理

它最早出现在《孙子算经》

> 今有物不知其数, 三三数之剩二, 五五数之剩三, 七七数之剩二, 问物几何?

这是同余方程问题, 即求一个整数 x, 模 3 余 2, 模 5 余 3, 模 7 余 2, 写成方程组形式

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

它是否有解? 又怎么求解呢?

在秦九韶 (1208-1268) 的《数书九章》中有一般的解法, 针对上面这个特殊的例子, 程大位 (1533-1606) 更是在他的《新编直指算法统宗》中将解法编成了一首诗.

三人同行七十稀
五树梅花廿一枝
七子团圆正半月
除百零五便得知

这里解释下, 这首诗的意思是为 3, 5, 7 分别找一个特别的数

3	$b_3 = 70$
5	$b_5 = 21$
7	$b_7 = 15$

这三个数有个特点是

$b_3 = 70$ 模 3 余 1, 模 5、模 7 余 0
$b_5 = 21$ 模 5 余 1, 模 3、模 7 余 0
$b_7 = 15$ 模 7 余 1, 模 3、模 5 余 0

这样

$$2b_3 + 3b_5 + 2b_7$$

就会满足题目要求的条件:

模 3 余 2, 模 5 余 3, 模 7 余 2

同时, 与之相差 105 的数依然满足这个条件, 因为 105 模 3, 5, 7 都余 0, 相差 105 不影响模 3, 5, 7 后的结果. 用图表表示

三人同行七十稀	$b_3 = 70$	$\times 2 = 140$
五树梅花廿一枝	$b_5 = 21$	$\times 3 = 63$
七子团圆正半月	$b_7 = 15$	$\times 2 = 30$
	求和	233
	除百零五	-105×2
	便得知	23

这就是我们老祖先比较聪明的地方, 用一个例子告诉你一个普遍存在的道理. 我想到这里大家已经知道这里的一般结论是什么了, 就是下面这个定理.

定理 24.4 中国剩余定理整数版. 假设

$$n_1, \cdots, n_s$$

为两两互素的整数, 对任意整数

$$x_1, \cdots, x_s$$

同余方程组

$$x \equiv x_1 \pmod{n_1}$$
$$x \equiv x_2 \pmod{n_2}$$
$$\cdots\cdots$$
$$x \equiv x_s \pmod{n_s}$$

有解且两个解之间相差

$$n_1 \cdots n_s$$

的倍数.

能不能把这个定理翻译成环论的语言?

感觉有一定难度, 需要环的一个构造方法. 如果我们有 s 个环

$$R_1, \cdots, R_s$$

那么它们的笛卡尔乘积

$$R_1 \times \cdots \times R_s$$

依然构成环, 其加法为

$$(x_1, \cdots, x_s) + (y_1, \cdots, y_s)$$
$$= (x_1 + y_1, \cdots, x_s + y_s)$$

乘法是

$$(x_1, \cdots, x_s)(y_1, \cdots, y_s)$$
$$= (x_1 y_1, \cdots, x_s y_s)$$

说白了就是加法和乘法都是分别进行, 很容易验证这个笛卡尔乘积的确是环.

有了这个构造, 就可以把中国剩余定理翻译成环论语言了.

定理 24.5 中国剩余定理整数环版. 假设

$$n_1, \cdots, n_s$$

为两两互素的整数, 那么环同态

$$\begin{aligned}\pi : \mathbb{Z} &\longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z} \\ x &\mapsto (x + n_1\mathbb{Z}, \cdots, x + n_s\mathbb{Z})\end{aligned}$$

是满射, 且诱导环同构

$$\mathbb{Z}/(n_1 \cdots n_s\mathbb{Z}) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$$

这个满射说的正是上面的同余方程组有解, 也就是说, 对任意整数

$$x_1, \cdots, x_s$$

都存在整数 x 使得

$$\begin{aligned}&(x + n_1\mathbb{Z}, \cdots, x + n_s\mathbb{Z}) \\ =\ &(x_1 + n_1\mathbb{Z}, \cdots, x_s + n_s\mathbb{Z})\end{aligned}$$

即满足上面的同余方程组

$$x \equiv x_i \pmod{n_i}, 1 \leqslant i \leqslant s$$

根据环同态基本定理第一同构定理, 上面的环同构正好说的是

$$\operatorname{Ker}\pi = n_1 \cdots n_s\mathbb{Z}$$

即同余方程的任意两个解之间相差

$$n_1 \cdots n_s$$

的倍数.

中国剩余定理有 1 环版

我们有理想之间的互素关系, 可以把定理24.5升级为有 1 环中的命题.

定理 24.6 中国剩余定理有 1 环版. 假设

$$I_1, \cdots, I_s$$

是有 1 环 R 中两两互素的理想, 即

$$I_i + I_j = R, \forall i \neq j$$

则环同态

$$\begin{aligned}\pi : R &\longrightarrow R/I_1 \times \cdots \times R/I_s \\ x &\mapsto (x + I_1, \cdots, x + I_s)\end{aligned}$$

是满射, 且诱导环同构

$$R/(I_1 \cap \cdots \cap I_s) \simeq R/I_1 \times \cdots \times R/I_s$$

证明. 就像整数的情形一样, 这里的关键是要找到一组 R 中元素

$$b_1, \cdots, b_s$$

使得

$$b_i + I_i = 1 + I_i, 1 \leqslant i \leqslant s$$

$$b_i + I_j = 0 + I_j, \forall i \neq j$$

这样的元素是否真的存在呢?

还好我老谋深算, 在前面证明了命题24.3. 对于这 s 个理想中的任意一个 I_i, 其他理想都与它互素, 即

$$I_i + I_k = R, \forall k \neq i$$

由命题24.3

$$I_i + \prod_{k \neq i} I_k = R$$

这样 R 中的单位元 1 可以表达成

$$1 = u_i + b_i$$

的形式, 其中

$$u_i \in I_i, b_i \in \prod_{k \neq i} I_k$$

这样一来 b_i 与 1 相差 I_i 中元素 u_i, 从而有

$$b_i + I_i = 1 + I_i$$

b_i 又在除 I_i 之外的其他理想的乘积理想中, 由理想的吸收性质

$$\prod_{k \neq i} I_k \subseteq I_j, \forall j \neq i$$

所以对任意 $j \neq i$

$$b_i + I_j = 0 + I_j$$

满足上面的条件.

现在任取

$$R/I_1 \times \cdots \times R/I_s$$

中元素

$$(x_1 + I_1, \cdots, x_s + I_s)$$

令

$$x = x_1b_1 + \cdots + x_sb_s$$

对每个固定的 $1 \leqslant i \leqslant s$, 等式右边除了 x_ib_i 以外, 其他的

$$x_jb_j, j \neq i$$

都在 I_i 中 (因为 $b_j \in I_i$). 所以

$$\begin{aligned}x + I_i &= x_ib_i + I_i \\ &= (x_i + I_i)(b_i + I_i) \\ &= (x_i + I_i)(1 + I_i) \\ &= x_i + I_i\end{aligned}$$

因此

$$\pi(x) = (x_1 + I_1, \cdots, x_s + I_s)$$

这就证明了 π 是满同态.

$\operatorname{Ker}\pi$ 恰好是 R 中的元素 x 满足

$$x + I_i = 0 + I_i, \forall 1 \leqslant i \leqslant s$$

也就是说

$$x \in I_i, \forall 1 \leqslant i \leqslant s$$

所以

$$\operatorname{Ker}\pi = I_1 \cap \cdots \cap I_s$$

由第一同构定理得环同构

$$R/(I_1 \cap \cdots \cap I_s) \simeq R/I_1 \times \cdots \times R/I_s$$

需要注意的是,在 $\mathbb{Z}$ 中,当

$$n_1, \cdots, n_s$$

两两互素时,有

$$n_1 \cdots n_s \mathbb{Z} = n_1 \mathbb{Z} \cap \cdots \cap n_s \mathbb{Z}$$

那上面定理中,是否满足

$$I_1 \cap \cdots \cap I_s = I_1 \cdots I_s$$

呢? 答案是: 当 R 是有 1 交换环时满足!

命题 24.7. 在有 1 交换环 R 中,假设理想

$$I_1, \cdots, I_s$$

两两互素,那么

$$I_1 \cap \cdots \cap I_s = I_1 \cdots I_s$$

这个证明只要利用下面这个引理,结合引理24.1,以及对 s 用数学归纳法就行了.

引理 24.8. 假设 I, J 是有 1 交换环的两个理想且

$$I + J = R$$

那么

$$I \cap J = IJ$$

证明. 只要验证

$$I \cap J \subseteq IJ$$

即可,且看

$$\begin{aligned} I \cap J &= (I \cap J)R \quad (R \text{ 有 } 1) \\ &= (I \cap J)(I + J) \\ &= (I \cap J)I + (I \cap J)J \\ &= I(I \cap J) + (I \cap J)J \quad (R \text{ 交换}) \\ &\subseteq IJ + IJ \\ &= IJ \end{aligned}$$

所以在中国剩余定理的有 1 交换环版本中,如果愿意,可以把

$$I_1 \cap \cdots \cap I_s$$

换成

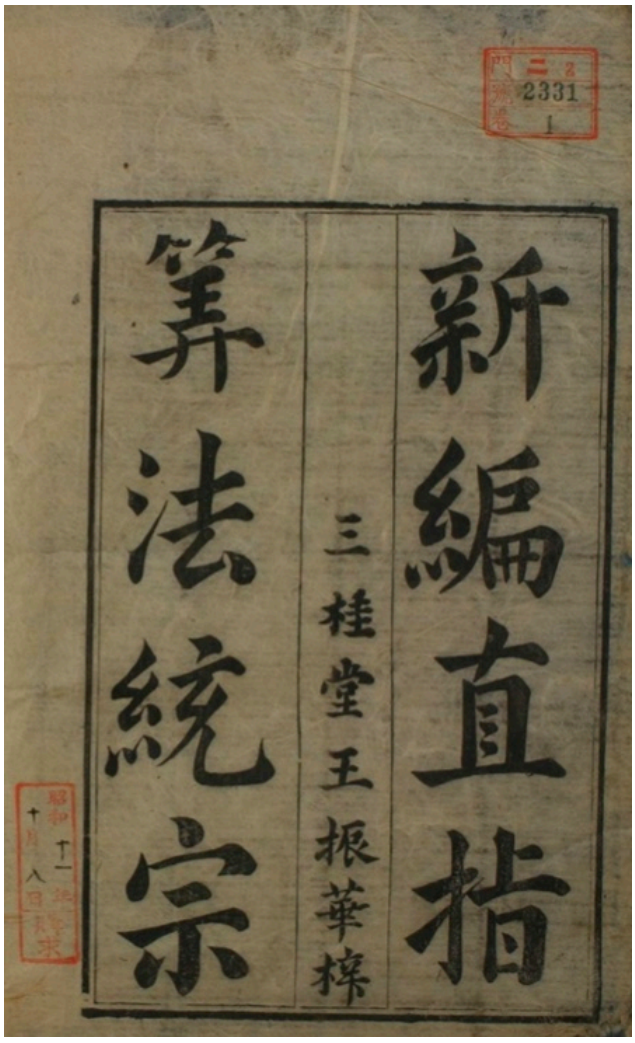
$$I_1 \cdots I_s$$

程大位的《算法统宗》

在找程大位口诀的过程中,顺便翻了他的

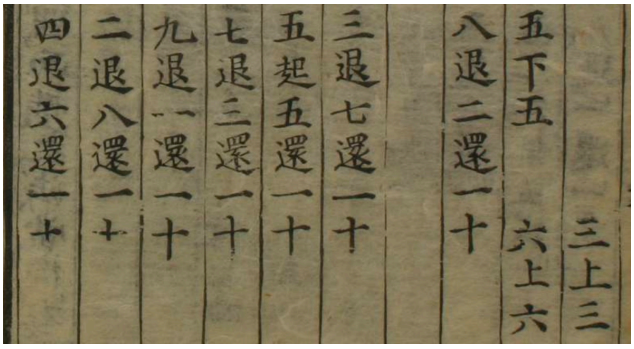
《新编直指算法统宗》

这也许是古代中国发行量最大的数学书了,我在网上找到日本某图书馆 1936 年的藏书



在程大位那个时代,人们还经常用筹算,很不方便,这本“算法统宗”是程大位毕生心血的结晶,他搜集了许多书籍,遍访名师,经过数十年的努力,公元 1592 年六十岁的他终于写成了《直指算法统宗》一书.

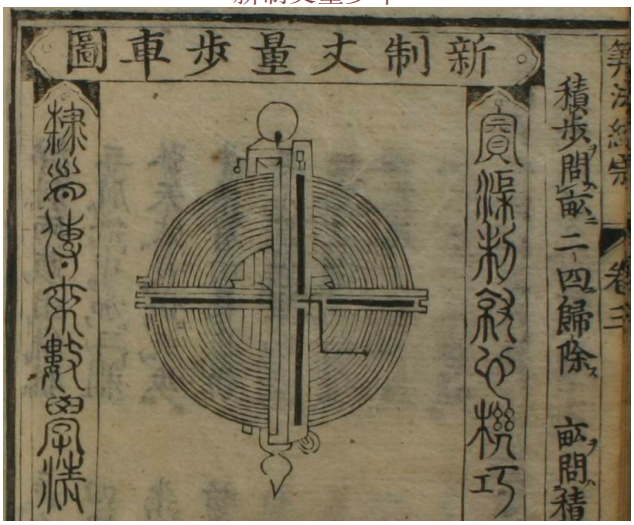
这本书的出现完成了由筹算到珠算的彻底转变,大家看看里面的珠算口诀



没错,这些产生无比强大生产力的珠算口诀正是出自这本书!

另外,这本书里还有一件有趣的发明

新制丈量步车



用现在的语言就是: 卷尺!

最后,虽然程大位先生有一个非常嚣张的名字,但他一辈子没有做过官!

25 RSA

本期导言

本期介绍中国剩余定理的经典应用:

RSA 加密方法

在影视剧中,我们看到过很多用密码本的方法. 本期要讲的 RSA 加密方法与密码本之类的方法完全不同,到现在依然是最安全的加密方法之一.

每次你打开电脑,输入 https 开头的网址,RSA 加密方法就已经开始在保护你的数据安全.

本期记号

对于正整数 m

$[0,m)$: 小于 m 的非负整数的集合

$[x]_m$: 整数 x 模 m 的余数

1 中国剩余定理

回顾上期中国剩余定理的整数环版.

定理 25.1 中国剩余定理整数环版. 假设

$$n_1,\cdots,n_s$$

是 s 个两两互素的正整数. 令

$$n=n_1n_2\cdots n_s$$

则有环同构

$$\begin{aligned}\mathbb{Z}_n &\to \mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_s}\\ [x]_n &\mapsto ([x]_{n_1},\cdots,[x]_{n_s})\end{aligned}$$

2 RSA 加密设定

说起加密,我们就不得不说起 Alice 和 Bob 这两个冤家,自从 1978 年他们被“发明”以来,就成为

密码届最著名的 CP, 任何一本密码学的书上好像都是这两个家伙在互相传递信息, 还生怕别人知道.

这不, 他们又有一些小秘密想告诉对方了, 但很遗憾, 物理上的距离, 让他们的消息传递必须经过一个不靠谱第三方 Eve.

这对 CP 感觉 Alice 比较主动, 她想给 Bob 发个消息, 于是 Bob 做了如下的操作:

1. 选两个不同的“非常大”的素数
$$p, q, \text{令 } n := pq$$
2. 计算
$$\varphi(n) = (p-1)(q-1)$$
并选定
$$1 < e < \varphi(n) \text{ 使得 } e \text{ 与 } \varphi(n) \text{ 互素}$$
3. 利用辗转相除法求出
$$1 < d < \varphi(n) \text{ 使得}$$
$$de + k\varphi(n) = 1$$
4. 为了安全, 销毁 p, q 以及 $\varphi(n)$.

这样剩下的信息只有三个数字
$$n, e, d$$
分为两对
$$(n, e) \text{ 和 } (n, d)$$
一般情况下选定的 e 比较简单, 而 d 则比较复杂. 现在让 Eve 把 n 和 e 传给 Alice, 带话:

这是我的“公钥”, 用它来加密你的消息吧.

由于 Eve 并不值得信任, 可以在这个“公钥”上签名, 免得 Eve 私自更改“公钥”. 至于 d(与 n 合起来称为私钥)

打死也不能告诉别人!

RSA 加密解密过程

现在 Alice 拿到公钥 n 和 e, 她就可以给 Bob 发消息了, 比如发一个

“啥时候出差回来呀?”

先想办法这句话转化成数字 x, 比如我们可以用 UTF8 对照表或者四角号码什么的.

由于 n 特别大, 我们可以假定 $x \in [0, n)$. 万一 x 比 n 大怎么办? 把这句话拆成多组进行传输.

怎么加密 x 呢?

用 n 和 e 定义函数
$$E : [0, n) \longrightarrow [0, n)$$
$$x \mapsto [x^e]_n$$
就是先取 x 的 e 次方, 再求它模 n 的余数.

这个就是我们的加密函数(encryption).

Alice 在 $E(x)$ 上签名, 让 Eve 传给 Bob.

Eve 拿着 $E(x)$ 一脸懵逼:

“这是个什么玩意?”

Bob 拿到 $E(x)$ 后找了个没人的地儿, 偷偷了拿出了自己的私钥 (n, d), 考虑函数
$$D : [0, n) \longrightarrow [0, n)$$
$$y \mapsto [y^d]_n$$
先将 y 做 d 次幂, 再求它模 n 的余数.

这就解密函数(decryption).

啥意思? 就是说, 如果用 D 作用在 $E(x)$ 上就可以得到 x. 即
$$D(E(x)) = x$$
这样就完成了加密和解密的过程!

那为什么 $DE(x) = x$ 呢? 实际上

定理 25.2. $DE = ED = \mathrm{id}$ 是 $[0, n)$ 上的恒等映射.

证明. 证明的关键是利用中国剩余定理.

对于任意 $[0, n)$ 中的整数 x
$$DE(x) = ED(x) = [x^{ed}]_n$$
所以定理等价于: 对任意 $u \in \mathbb{Z}_n$
$$u^{ed} = u$$
由于 $n = pq$ 且 p 与 q 互素, 由中国剩余定理, 存在环同构
$$\mathbb{Z}_n \longrightarrow \mathbb{Z}_p \times \mathbb{Z}_q$$
假设 u 在这个同构下的像为
$$(a, b), \quad \text{其中 } a \in \mathbb{Z}_p, b \in \mathbb{Z}_q$$
由于环同构保持乘法, 我们需要证明
$$(a, b)^{ed} = (a, b), \text{即:}$$
$$a^{ed} = a$$
$$b^{ed} = b$$
先来证明第一个, 如果
$$a = 0$$
则显然
$$a^{ed} = 0^{ed} = 0 = a$$
若 $a \neq 0$, 由于 $\mathbb{Z}_p$ 是域, 所以 $\mathbb{Z}_p$ 中的所有非零元(共 $p-1$ 个) 关于乘法是一个群. 现在
$$ed - 1 = -k\varphi(n) = -k(p-1)(q-1)$$
被 $p-1$ 整除, 由拉格朗日定理推论
$$a^{ed-1} = 1$$
这里 1 为 $\mathbb{Z}_p$ 中乘法单位元, 从而
$$a^{ed} = a$$

总结起来, 无论 a 是否为 $\mathbb{Z}_p$ 中零元, 都有

$$a^{ed} = a$$

同样的道理可得

$$b^{ed} = b$$

证明完毕!

现在我们知道, Bob 可以用解密函数 D 来解密 Alice 利用公钥加密后的信息 $E(x)$.

Bob 要回消息怎么办?

需要注意: 千万不能用函数 D 把回复的消息 y 加密成 $D(y)$, 然后傻乎乎的等着 Alice 用 E 去解密得到 $ED(y) = y$. 不要忘了, Eve 知道 n 和 e 的, 从而也知道函数 E.

正确的做法是, Alice 重新找两个素数, 建立新的公钥和私钥, 然后把公钥给 Bob. 他回消息的时候用 Alice 的公钥进行加密.

Eve 好像懂了

时间久了, Alice 跟 Bob 也没什么话说, 翻来复去都是那几句. 这样 Eve 就经常拿到同样的密文 $E(x)$, 结合两个人的各种表现, 就有机会猜出来 x 是什么.

有没有办法避免这个呢?

有没有可能做到:

传递同样信息, 但每次加密后又不同?

可以的, 只要给消息 x 加点干扰项"

随机的生成一个固定长度的数 r, 长度为 l, 跟 x 拼起来

$$X := r||x$$

这样虽然 x 是同一个, 但每次的 r 不一样, 因此 X 不同, 如果为了更安全, 还可以再找一个函数 Pre 和它的反函数 Post(这个自己找去), 使得

$$\mathrm{Post} \cdot \mathrm{Pre}(X) = X$$

这样我们传递的过程就变成这样

1. 随机生成 r, 长度为 l, 与 x 拼成
$$X = r||x$$
2. 用函数 Pre 作用
$$\mathrm{Pre}(X)$$
3. 用 E 加密
$$E \cdot \mathrm{Pre}(X)$$
4. 让 Eve 传递消息

(很懵圈, 怎么又不一样)

5. Bob 解密
$$D \cdot E \cdot \mathrm{Pre}(X) = \mathrm{Pre}(X)$$
6. 用 Post 函数作用
$$\begin{aligned}&\mathrm{Post} \cdot D \cdot E \cdot \mathrm{Pre}(X)\\ &= \mathrm{Post} \cdot \mathrm{Pre}(X) = X\end{aligned}$$
7. 由于 $X = r||x$, 去掉前 l 个数字得到 x

一本正经的说, 这种想法叫什么呢? 这种想法的名字就是 OAEP:

Optimal Asymmetric Encryption Padding

跟 RSA 联合就称为 RSA-OAEP. 如果感兴趣, 可以在网上搜索这个关键词查找.

RSA 的安全性来自哪里?

为什么叫做 RSA 呢?

这是因为这个算法是 1977 年 Ron Rivest, Adi Shamir 和 Leonard Adleman 一起提出的. 当时他们三人都在麻省理工学院工作. RSA 就是他们三人姓氏开头字母拼在一起组成的.

实际上 1973 年, 在英国政府通讯总部工作的数学家 Clifford Cocks 也给出了一个相同的算法, 但他的发现被列入机密, 一直到 1997 年才被解密.

RSA 的安全性主要来自于

对于非常大的整数 n, 如果不知道 p, q, 计算 $\varphi(n)$ 或者对 n 分解因式都是需要很长时间的.

练习 6. 你能利用多个 (大于 2) 素数构造跟 RSA 类似的加密解密函数吗?

RSA 的缺点

RSA 有个很大的缺点是

加密解密过程太累!

需要很大的计算量, 是一种比较 "昂贵" 的加密方法, 现在网络传输往往需要传输大量的数据, 如果完全用 RSA 来加密解密将是非常占用资源的, 因此现

在大量数据的传输一般都是 RSA 与另一种加密方法 AES 联合使用.

AES 的特点是加密解密速度快,但加密和解密是同一个密码,与 RSA 合用,RSA 负责对 AES 的密码进行加密 (这个活最轻松),而数据的加密这个重体力活就交给 AES 去做!

26 素理想与极大理想

本期导言

回到我们的

有 1 交换环

前面我们说了它的理想可以看成数,一些整数的结论也可以用理想来证明,而证明还很简单.

现在我有个问题:

什么样的理想能取代素数的位置?

素数

回顾下整数中的素数: $p \neq 0, \pm 1$ 满足

p 不能被 $\pm 1, \pm p$ 之外的整数整除

在 $\mathbb{Z}$ 中,素数还有个性质

$$p \mid ab \Rightarrow p \mid a \text{ 或者 } p \mid b$$

在整数中这两条实际是等价的.

还记得整除关系用理想是怎么描述的么?

整数语言	理想语言
$m \mid n$	$n\mathbb{Z} \subseteq m\mathbb{Z}$
mn	$mn\mathbb{Z} = (m\mathbb{Z})(n\mathbb{Z})$

把上面两个性质分别翻译成理想的语言.

如果

$$p\mathbb{Z} \subseteq m\mathbb{Z}$$

则

$$m\mathbb{Z} = p\mathbb{Z} \text{ 或者 } m\mathbb{Z} = \pm 1\mathbb{Z} = \mathbb{Z}$$

如果

$$(m\mathbb{Z})(n\mathbb{Z}) \subseteq p\mathbb{Z}$$

则

$$m\mathbb{Z} \subseteq p\mathbb{Z} \text{ 或者 } n\mathbb{Z} \subseteq p\mathbb{Z}$$

2 素理想, 极大理想

有 1 交换环中的素理想和极大理想正是从上面两种性质抽象出来

定义 26.1. 假设 R 是有 1 交换环, $\mathfrak{p} \neq R$ 是 R 的理想, 它称为 R 的

$$\text{素理想(prime ideal)},$$

如果对任意 R 的理想 I, J 有

$$IJ \subseteq \mathfrak{p} \Rightarrow I \subseteq \mathfrak{p} \text{ 或者 } J \subseteq \mathfrak{p}$$

R 的理想 $\mathfrak{m} \neq R$ 称为 R 的

$$\text{极大理想(maximal ideal)},$$

如果对于任意 R 的理想 I 有

$$\mathfrak{m} \subsetneq I \Rightarrow I = R$$

由于这里没有限制理想不是零理想, 这使得 $\mathbb{Z}$ 中的零理想是素理想:

$$(m\mathbb{Z})(n\mathbb{Z}) \subseteq \{0\} \Rightarrow m\mathbb{Z} = \{0\} \text{ 或 } n\mathbb{Z} = \{0\}$$

但不是极大理想:

$$\{0\} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$$

这里理想 $2\mathbb{Z}$ 真包含零理想, 但它不是 $\mathbb{Z}$, 所以零理想不是极大理想.

但对于 $\mathbb{Z}$ 中的非零理想来说, 素理想和极大理想是等价的, 这个由上面素数的两个等价性质可得到.

3 素理想的判定

要判定一个理想是不是素理想还是挺麻烦的, 比如在 $R = \mathbb{Z}[x]$ 中, 由 x 生成的理想

$$(x) = xR$$

是不是素理想?

在有 1 交换环 R 中, 任意一个元素 $a \in R$ 都可以生成一个 R 的理想

$$(a) := aR = \{ar \mid r \in R\}$$

这种由一个元素生成的理想称为

$$\text{主理想 (principal ideal)}$$

例如 $\mathbb{Z}$ 的理想全部都是主理想.

如果 a 是 R 中的可逆元, 则 $(a) = R$. 实际上, 对任意 $r \in R$ 有

$$r = ra^{-1}a \in (a)$$

当然由两个元素 $a, b \in R$ 也能生成一个理想

$$(a, b) := aR + bR = \{ar + bs \mid r, s \in R\}$$

这其实是包含 a, b 最小的理想.

实际上, 任何 R 的子集 X 都能生成一个理想

$$(X) = \{ \text{有限和 } \sum x_k r_k \mid x_k \in X, r_k \in R\}$$

不说远了, 怎么判定理想是否为素理想呢?

命题 26.2. 假设 $\mathfrak{p} \neq R$ 是有 1 交换环 R 的理想, 则下面几条等价

1. 对任意 R 的理想 I, J

$$IJ \subseteq \mathfrak{p} \Rightarrow I \subseteq \mathfrak{p} \text{ 或 } J \subseteq \mathfrak{p}$$

2. 对任意 $a, b \in R$

$$ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \text{ 或 } b \in \mathfrak{p}$$

3. 对任意 $a, b \in R$

$$a, b \notin \mathfrak{p} \Rightarrow ab \notin \mathfrak{p}$$

4. 商环 $R/\mathfrak{p}$ 是整环

证明. $1 \Rightarrow 2$. 由于 $ab \in \mathfrak{p}$, 所以

$$abR = (aR)(bR) \subseteq \mathfrak{p}$$

由 1 得

$$aR \subseteq \mathfrak{p} \text{ 或者 } bR \subseteq \mathfrak{p}$$

由于 R 是有 1 环, 所以

$$r = r1 \in rR, \forall r \in R$$

从而

$$a \in \mathfrak{p} \text{ 或者 } b \in \mathfrak{p}$$

$2 \Leftrightarrow 3$. 互为逆否命题.

$3 \Rightarrow 4$. 在商环 $R/\mathfrak{p}$ 中, 假设

$$a + \mathfrak{p} \text{ 和 } b + \mathfrak{p} \text{ 不是零元, 即}$$

$$a \notin \mathfrak{p},\ b \notin \mathfrak{p}$$

由 3 得 $ab \notin \mathfrak{p}$, 从而

$$(a + \mathfrak{p})(b + \mathfrak{p}) = (ab + \mathfrak{p})$$

在商环 $R/\mathfrak{p}$ 中不是零元. 因此 $R/\mathfrak{p}$ 中没有零因子. 由于它已经是有 1 的交换环, 现在又没有零因子, 所以 $R/\mathfrak{p}$ 是整环.

$4 \Rightarrow 1$. 现在假设 R 的理想 I, J 满足

$$IJ \subseteq \mathfrak{p}$$

如果

$$I \nsubseteq \mathfrak{p},\ J \nsubseteq \mathfrak{p}$$

则存在

$$a \in I \backslash \mathfrak{p}, b \in J \backslash \mathfrak{p}$$

从而

$$a + \mathfrak{p} \text{ 和 } b + \mathfrak{p} \text{ 都不是 } R/\mathfrak{p} \text{ 中零元}$$

由 4, $R/\mathfrak{p}$ 是整环, 所以

$$(a+\mathfrak{p})(b+\mathfrak{p})=(ab+\mathfrak{p})$$

也不是 $R/\mathfrak{p}$ 中零元, 即

$$ab\notin\mathfrak{p}$$

但是 $ab\in IJ\subseteq\mathfrak{p}$, 与假设矛盾!

有了这个命题后, 素理想的判定就简单多了, 比如上面 $R=\mathbb{Z}[x]$ 中由 x 生成的主理想, 只要考虑环同态

$$\phi:\mathbb{Z}[x]\longrightarrow\mathbb{Z}$$
$$f(x)\mapsto f(0)$$

可以发现这是个环的满同态, 同时

$$\begin{aligned}\operatorname{Ker}\phi&=\{f(x)\mid f(0)=0\}\\&=\{xg(x)\mid g(x)\in\mathbb{Z}[x]\}=(x)\end{aligned}$$

由环同态基本定理

$$\mathbb{Z}[x]/(x)\simeq\mathbb{Z}$$

是整环, 所以 (x) 是 $\mathbb{Z}[x]$ 的素理想.

推论 26.3. 有 1 交换环 R 是整环当且仅当其零理想是素理想.

证明. 由上面命题的 4 得到.

极大理想的判定

极大理想怎么判定呢? 跟素理想的判定相似的, 可以用相应的商环的判定.

命题 26.4. 假设 $\mathfrak{m}\neq R$ 是有 1 交换环 R 的理想. 那么 $\mathfrak{m}$ 是极大理想当且仅当 $R/\mathfrak{m}$ 是域.

证明. 由于 $R/\mathfrak{m}$ 的理想与 R 中包含 $\mathfrak{m}$ 的理想一一对应, $\mathfrak{m}$ 是极大理想说的是 R 中包含 $\mathfrak{m}$ 的理想只有 $\mathfrak{m}$ 和 R, 这等价于 $R/\mathfrak{m}$ 中的理想只有零理想和 $R/\mathfrak{m}$ 本身.

定理的证明就由下面的命题来完成.

命题 26.5. 一个有 1 交换环是域当且仅当它没有非平凡的理想.

证明. 假设 S 是有 1 交换环, 如果 S 是域, 则 S 的任意非零理想 I 都包含一个可逆元 a, 但可逆元生成的主理想是 S, 所以

$$S=(a)\subseteq I\subseteq S$$

所以 $I=S$. S 没有非平凡的理想.

反过来, 假设 S 没有非平凡理想.

对任意 S 中非零元 a, 由其生成的主理想 $(a)=aS$ 是 S 的非零理想, 由假设只能有

$$aS=S$$

从而存在 $s\in S$ 使得

$$as=1$$

因此 a 是 S 中的可逆元. 这样 S 中所有非零元都可逆, 但它本身是有 1 交换的, 所以 S 是域.

由此可见 $\mathbb{Z}$ 中, 素数 p 生成的主理想

$$p\mathbb{Z}$$

是极大理想, 因为对应的商环 $\mathbb{Z}/p\mathbb{Z}$ 是域.

极大理想 VS 素理想

由素理想和极大的判定, 很容易发现

推论 26.6. 一个有 1 交换环的极大理想也是素理想

证明. 极大理想对应的商环是域, 当然也是整环, 所以极大理想也是素理想.

素理想和极大理想的存在性

如果我们想得更多一点, 希望愉快的讨论任意有 1 交换环中的素理想的问题, 有个无法回避的问题是

素理想和极大理想在存在性?

由于极大理想也是素理想, 只需要说明极大理想的存在性就能说明素理想的存在性.

这方面很无奈, 我们必须要在 Zorn 引理下进行工作, Zorn 引理与选择公理等价.

简要的介绍下选择公理.

一个非空集合 X 上的二元关系 $\leqslant$ 称为偏序, 如果它满足

1. $x\leqslant x,\forall x\in X$

2. $x \leqslant y, y \leqslant x \Rightarrow x = y$
3. $x \leqslant y, y \leqslant z \Rightarrow x \leqslant z$

此时 $(X, \leqslant)$ 称为偏序集.

比如环 R 的所有理想组成的集合在集合的包含关系下组成偏序集.

偏序集中并不是所有的元素都能比较大小, 最简单的, 比如 $\{1,2\}$ 的所有子集组成的集合, 在包含关系下, $\{1\}$ 和 $\{2\}$ 就互相没有包含关系, 因此在包含关系下无法比较.

偏序集 $(X, \leqslant)$ 的非空子集 Y 称为全序子集, 如果任意 $y_1, y_2 \in Y$, 它们都能比较大小, 即

$$y_1 \leqslant y_2 \text{ 或者 } y_2 \leqslant y_1$$

引理 26.7 Zorn 引理. 假设 $(X, \leqslant)$ 是偏序集满足其任意全序子集 Y 都有上界, 即存在 $u \in X$ 使得

$$y \leqslant u, \forall y \in Y,$$

则 X 中存在极大元, 即存在 $m \in X$ 使得

$$m \leqslant x \Rightarrow m = x$$

定理 26.8. 有 1 交换环存在极大理想

证明. 假设 R 是有 1 交换环, 考虑集合

$$\mathfrak{X} := \{R \text{ 中不含 1 的理想}\}$$

显然 $\mathfrak{X}$ 非空, 因为零理想属于 $\mathfrak{X}$.

现假设 $\mathcal{Y}$ 为 $\mathfrak{X}$ 全序子集, 取 $\mathcal{Y}$ 中理想的并

$$J = \cup_{I \in \mathcal{Y}} I$$

我们断言 J 是 R 的理想且不含 1.

由于 $\mathcal{Y}$ 的所有 I 都不含 1, 因此它们的并集也不会含 1. 另外, 由于这些 I 都有吸收性质, 所以 J 也有这个性质. 实际上, 对任意 $a \in J, r \in R$, 存在 $I \in \mathcal{Y}$ 使得

$$a \in I, \text{从而 } ra \in I \subseteq J.$$

最后假设 $a, b \in J$, 而存在 $I, I' \in \mathcal{Y}$ 使得

$$a \in I, b \in I'$$

由于 $\mathcal{Y}$ 是全序子集, 因此

$$I \subseteq I' \text{ 或者 } I' \subseteq I$$

不妨设 $I \subseteq I'$, 因此

$$a, b \in I', \text{从而 } a - b \in I' \subseteq J$$

因此 J 在加法下是 R 的子群, 又满足吸收性质, 从而是 R 的理想.

现在 J 是 R 的理想又不含 1, 因此

$$J \in \mathfrak{X}$$

显然 J 是 $\mathcal{Y}$ 的上界:

$$I \subseteq J, \forall I \in \mathcal{Y}$$

由 Zorn 引理, $\mathfrak{X}$ 存在极大元 $\mathfrak{m}$, 即

$$\mathfrak{m} \subseteq I, I \in \mathfrak{X} \Rightarrow \mathfrak{m} = I$$

这实际上说的就是 $\mathfrak{m}$ 是 R 的极大理想. 我们来翻译下, I 是 R 的理想

$$I \in \mathfrak{X} \Leftrightarrow 1 \notin I \Leftrightarrow I \neq R$$

如果 $1 \notin I$, 显然 $R \neq I$, 反过来如果 $R \neq I$, 那么 1 一定不属于 I, 否则

$$R = (1) \subseteq I, \text{造成 } I = R, \text{矛盾!}$$

这样上面的条件就变成: 假设 I 是 R 的理想

$$\mathfrak{m} \subseteq I, I \neq R \Rightarrow \mathfrak{m} = I$$

即 $\mathfrak{m}$ 是 R 的极大理想.

实际上, 我们也可以利用 Zorn 引理直接证明素理想的存在性, 只需要考虑这样的子集

$$S \subseteq R, 0 \notin S \text{ 且 } S \text{ 关于乘法封闭}$$

称为可乘子集, $\{1\}$ 是一个特殊的可乘子集. 将 Zorn 引理应用于

$$\mathfrak{X}_S = \{I \lhd R \mid I \cap S = \emptyset\}$$

其中的极大元将是 R 的素理想.

总结

对一个有 1 交换环来说, 素理想是它非常宝贵的资源, 所有素理想组成的集合蕴含了这个环丰富的信息, 它上面有一个拓扑空间的结构称为 Zariski 拓扑. 感兴趣的读者可以自行扩展学习.

27 唯一分解整环

本期导言

回想环论开始的地方，特别想知道像

$$\mathbb{Z}[\xi],\ \xi \text{ 是单位根}$$

这样的环是不是跟整数环和多项式环一样有唯一分解的性质，这个性质最初用来研究费马大定理等数论问题.

本期希望能搭一个理论的框架，讨论下唯一分解性质怎样准确的描述，从哪些方向去寻找这样的环.

整环中元素的分解

在 $\mathbb{Z}$ 中每一个非零非 ± 1 的整数都可以分解成不能再分解的整数 (素数) 的乘积，而且这种分解在不计顺序和正负号的意义下是唯一的.

在 $\mathbb{Q}[x]$ 中，每一个正次数多项式 (非零非常数多项式) 都可以分解成不可约多项式的乘积，并且这种分解在不计顺序和相差非零常数倍的意义下是唯一的.

现在给定一个整环 R(整环包含了我们感兴趣的 $\mathbb{C}$ 的那些子环，如 $\mathbb{Z}[i]$ 等)，我们期望的元素的分解是什么呢？

给定 R 中的元素 $a \in R$，如果 $b, c \in R$ 使得

$$a = bc$$

我们称 b 和 c 整除 a，记作

$$b \mid a, c \mid a$$

如果用理想的语言来描述就是

$$a \in bR = (b)$$

或者等价的

$$(a) = aR \subseteq bR = (b)$$

即 a 生成的主理想包含于 b 生成的主理想.

如果两个非零元 a 与 b 相互整除

$$a \mid b, b \mid a$$

则存在 $c, d \in R$ 使得

$$a = bc, b = ad$$

从而

$$a = adc$$

由于 R 是整环而 $a \neq 0$，可消去 a，得到

$$1 = dc$$

也就是说 c, d 是 R 中互逆的两个元素，因此 a 与 b 的差距就是差一个可逆元素倍

$$a = bc, b = ad.$$

这就好像 $\mathbb{Z}$ 中的

$$3 = (-3) \times (-1), -3 = 3 \times (-1)$$

或者 $\mathbb{Q}[x]$ 中的

$$2x - 2 = 2(x - 1), x - 1 = \tfrac{1}{2}(2x - 2)$$

一样，这种情况我们称 a 与 b相伴.

把 a 与 b 相互整除翻译成理想的语言就是

$$(a) \subseteq (b), (b) \subseteq (a)$$

即

$$(a) = (b)$$

上面这种

$$a = bc(\text{其中 } c \text{ 可逆})$$

的分解并不是“真的”把 a 分解了，此时

$$b = ac^{-1}$$

a 与 b 的地位的对等的.

那怎样的分解才算是真的分解呢？

对一个 R 中的非零元 a，如果分解

$$a = bc$$

中 b 和 c 都不是可逆元 (还记得吗？环中的可逆元称为单位)，那么 b 和 c 就称为 a 的真因子.

很显然可逆元没有真因子，但可逆元并不是我们分解中关心的元素.

定义 27.1. 整环 R 中，如果一个非零非单位的元素 p 没有真因子，则称 p 为 R 中的不可约元(irreducible element).

比如，$\mathbb{Z}$ 中的不可约元是素数，$\mathbb{Q}[x]$ 中的不可约元就是 $\mathbb{Q}[x]$ 中的不可约多项式.

如果用理想的语言来说呢?

引理 27.2. 假设 R 是整环，则有

1. $a, b \in R$ 非零，b 是 a 的真因子当且仅当
$$(a) \subsetneq (b) \subsetneq R.$$
2. $p \in R$ 非零非单位，p 不可约当且仅当
$$(p) \subsetneq (c) \Rightarrow (c) = R$$
此时称 (p) 为 R 的极大主理想.

证明. 1.$\Rightarrow$. 由假设存在分解

$$a = bc$$

其中 b, c 都不是单位，从而

$$(b) \subsetneq R$$

($(b) = R$ 当且仅当 b 是单位)

由 $b \mid a$ 得 $(a) \subseteq (b)$.

如果 $(a) = (b)$, 则 a 与 b 相伴, 存在分解

$$a = bd, \text{其中 } d \text{ 为单位}$$

从而 $bc = bd$, 由于 $a \neq 0$, 因此 $b \neq 0$, 两边消去 b 得 $c = d$ 为单位, 与假设矛盾. 因此

$$(a) \subsetneq (b) \subsetneq R$$

$\Leftarrow$. 反过来, 如果

$$(a) \subsetneq (b) \subsetneq R$$

可得 $a = bc$, 由于 $(b) \subsetneq R$, 所以 b 不是单位. 如果 c 是单位, 则 a 与 b 相伴, 从而 $(a) = (b)$, 与假设矛盾! 所以 c 也不是单位. 因此 b 是 a 的真因子.

2是1的直接推论.

注意, 上面引理结论 2 中说的极大主理想指的是 (p) 与所有不等于 R 的主理想相比, 它在包含关系下是极大的. 总结下

	理想语言
$b \mid a$	$(a) \subseteq (b)$
a 与 b 相伴	$(a) = (b)$
b 是 a 的真因子	$(a) \subsetneq (b) \subsetneq R$
非零非单位 p 不可约	(p) 为极大主理想

推论 27.3. 假设 p, q 为整环 R 中不可约元. 如果 $p \mid q$ 则 p 与 q 相伴.

证明. 由上表 $(q) \subseteq (p)$, 但 (q) 为极大主理想, 又 $(p) \neq R$, 所以 $(q) = (p)$, 即 p 与 q 相伴.

2 唯一分解整环

有了不可约元素后, 我们就知道想要的环是什么样子了, 它就是

定义 27.4. 一个整环 R 称为唯一分解环 (unique factorization domain, 简记: UFD), 如果下面两条成立

1. 对任意非零非单位 $a \in R$ 可以分解为不可约元的乘积:
$$a = p_1 \cdots p_m$$
2. 如果非零非单位的 $a \in R$ 有两种方式分解成不可约元的乘积:
$$a = p_1 \cdots p_m = q_1 \cdots q_n$$
则 $m = n$ 且适当调整顺序后有
$$p_i \text{ 与 } q_i \text{ 相伴}, i = 1, \cdots, n$$

按照这个定义, 对于 $\mathbb{Z}$ 和 $\mathbb{Q}[x]$, 我们在初等数论或者高等代数中证明过它们是唯一分解环.

证明的关键是第 2 条分解的唯一性, 大家还记得证明的关键点是哪里么? 回顾下, 比如 $\mathbb{Z}$ 中有两种素分解

$$p_1 \cdots p_m = q_1 \cdots q_n$$

则有

$$p_m \mid q_1 \cdots q_n$$

从而必然整除右边乘积中的某一项! 不妨设

$$p_m \mid q_n$$

这样 p_m 与 q_n 相伴 (由推论27.3), 上面的分解两边消去 p_m 可得

$$p_1 \cdots p_{m-1} = cq_1 \cdots q_{n-1}$$

其中 c 是 $\mathbb{Z}$ 中的可逆元, 现在两边的不可约元的个数都减少了一个, 剩下的就交给数学归纳法去解决了.

大家也许发现了, 素数有个性质

$$p \mid ab \Rightarrow p \mid a \text{ 或 } p \mid b$$

正是这个性质决定了上面分解的唯一性.

那不可约元是不是都有这个性质呢?

不一定, 比如在 $\mathbb{Z}[\sqrt{-3}]$ 中, 可以证明 2 是不可约元, 并且

$$4 = 2 \times 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

所以

$$2 \mid (1 + \sqrt{-3})(1 - \sqrt{-3})$$

但 $2 \nmid 1 \pm \sqrt{-3}$!

实际上, $1 \pm \sqrt{-3}$ 也是 $\mathbb{Z}[\sqrt{-3}]$ 中的不可约元.

而 $\mathbb{Z}[\sqrt{-3}]$ 中的单位只有

$$\pm 1$$

所以 2 与 $1 \pm \sqrt{-3}$ 并不相伴, 所以 4 在 $\mathbb{Z}[\sqrt{-3}]$ 中分解并不唯一, 因此 $\mathbb{Z}[\sqrt{-3}]$ 并不是唯一分解环, 咎其原因, 正是因为它的不可约元并不具有像上面素数那样的性质.

定义 27.5. 整环 R 中的非零非单位 p 称为一个素元(prime element), 如果

$$p \mid ab \Rightarrow p \mid a \text{ 或 } p \mid b$$

换成理想的语言则是

$$ab \in (p) \Rightarrow a \in (p) \text{ 或 } b \in (p)$$

即 (p) 是 R 的素理想.

素元 VS 不可约元

如果 p 是素元, 它显然不可能有真因子, 从而是不可约元. 否则假设

$$p = bc$$

其中 b, c 都不是单位, 则

$$p \mid b \text{ 或 } p \mid c$$

不妨设 $p \mid b$, 则 $b = pd$, 从而

$$p = pdc$$

两边消去 p 得 $1 = bc$, 所以 c 是单位, 与假设矛盾! 所以 p 是不可约元. 即

素元一定是不可约元!

唯一分解的关键: 不可约 = 素元

如果 R 中所有不可约元都是素元, 假设

$$p_1 \cdots p_m = q_1 \cdots q_n$$

是两种不可约元的乘积, 跟 $\mathbb{Z}$ 中的证明一样, 可以证明 $m = n$ 且调整顺序后有

$$p_i \text{ 与 } q_i \text{ 相伴}, i = 1, \cdots n$$

详细的证明大家可以作为练习.

另一方面, 唯一分解环中的不可约元也一定是素元.

引理 27.6. 假设 p 为唯一分解环 R 中的不可约元, 则 p 为素元.

证明. 假设 $p \mid ab$, 则 $ab = pc$.

将 a, b, c 分别分解成不可约元的乘积

$$a = p_1 \cdots p_s$$

$$b = q_1 \cdots q_r$$

$$c = v_1 \cdots v_t$$

则

$$p_1 \cdots p_s q_1 \cdots q_r = pv_1 \cdots v_t$$

由唯一分解性, p 必然和某个 p_i 或者 q_j 相伴, 从而有 $p \mid a$ 或 $p \mid b$.

总结起来

定理 27.7. 一个整环 R 是唯一分解整环当且仅当下面两条成立:

1. 对任意非零非单位 $a \in R$ 可以分解为不可约元的乘积:
$$a = p_1 \cdots p_m$$
2. R 中的不可约元都是素元.

这是我们寻找唯一分解环的方向:

努力找不可约元都是素元的整环

小结

最后把上面的表格补充下

	理想语言
$b \mid a$	$(a) \subseteq (b)$
a 与 b 相伴	$(a) = (b)$
b 是 a 的真因子	$(a) \subsetneq (b) \subsetneq R$
非零非单位 p 不可约	(p) 为极大主理想
非零非单位 p 为素元	(p) 为素理想

唯一分解环的第一个条件我们还没有转化成理想的语言, 这个留到下期来处理!

28 主理想整环与欧氏环

本期导言

上期建立了唯一分解环的理论框架

定理 28.1. 一个整环 R 是唯一分解环, 当且仅当下面两条成立

1. 任意非零非单位的元素都可以分解成有限个不可约元的乘积.
2. 所有的不可约元都是素元.

本期利用这个定理寻找唯一分解环.

发挥理想语言的威力

回顾下上期最后的表格, 在整环 R 中

	理想语言
$b \mid a$	$(a) \subseteq (b)$
a 与 b 相伴	$(a) = (b)$
b 是 a 的真因子	$(a) \subsetneq (b) \subsetneq R$
非零非单位 p 不可约	(p) 为极大主理想
非零非单位 p 为素元	(p) 为素理想

从这个表格中, 我们清楚的看到, 一个非零非单位的元素 a 是不可约元当且仅当其生成的主理想 (a) 是极大主理想, 为素元当且仅当 (a) 素理想.

这样定理28.1条件 2 用理想的语言就是

所有极大主理想都是素理想

那条件 1 能解释成理想的语言么?

想像下一个非零非单位的元素不能写成有限个不可约元素的乘积是个什么状况?

假设 a 是这样的元素, 首先 a 一定是可约的, 也就是存在真因子, 即存在分解

$$a = a_1 b_1$$

使得 a_1 和 b_1 都不是单位, 并且 a_1 和 b_1 中至少有一个不能分解成有限个不可约元素的乘积 (如果都可以的话, 那么 a 也可以), 不妨设 a_1 不能写成有限个不可约元的乘积.

由于 a_1 是 a 的真因子, 由上表得

$$(a) \subsetneq (a_1) \subsetneq R$$

现在 a_1 也不能写成有限个不可约元的乘积, 由上面的过程, a_1 存在真因子 a_2 也不能写成有限个不可约元的乘积, 从而

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq R$$

这个过程可以无限的做下去, 最后得到一个无限的升链

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq R$$

总结下

如果 R 中存在元素 a 不能分解为有限个不可约元素乘积, 那么存在无限上升的主理想链

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$$

把这个结论做下逆否命题, 就得到

命题 28.2. 假设整环 R 中不存在无限上升的主理想链

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$$

则 R 中的所有非零非单位都可以分解为有限个不可约元的乘积.

只看这个命题的话, 感觉很难想像主理想的升链能够元素的分解产生这么强的联系, 这就是用理想的语言产生的强大力量!

主理想整环

上一小节, 我们为定理28.1条件 2 找到了个充要条件

所有极大主理想都是素理想

找到了定理28.1条件 1 的充分条件

不存在无限上升的主理想链

现在我们就朝着这两个方向努力!

最简单的想法是:

如果 R 的理想都是主理想会怎样?

回顾: 极大主理想, 就是满足条件

$$(a) \subsetneq (b) \Rightarrow (b) = R$$

的理想 (a). 既然现在所有的理想都是主理想, 这个条件就变成了: 对任意理想 I

$$(a) \subsetneq I \Rightarrow I = R.$$

这分明说的是

(a) 是极大理想!

从而也必然是素理想!

也就是说如果 R 的所有理想都是主理想的话,那么所有的极大主理想都是极大理想,从而都是素理想!这样 R 的所有不可约元都是素元!

这样的环是很好的唯一分解环的候选对象,我们称之为

$$\text{主理想整环(principal ideal domain)}$$

简称: PID.

现在 PID 满足定理28.1条件 2 了,要成为唯一分解环,只需要再满足条件 1.

是否满足呢?

我们可以利用条件 1 的充分条件,看看 R 中是否存在无限上升的主理想链.

反证法!假设

$$(a_0) \subsetneq (a_1) \subsetneq \cdots$$

为 R 中无限上升的主理想链,取

$$I = \cup_{i\geqslant 0}(a_i)$$

由于这些 (a_i) 在包含关系下是全序,上次利用 Zorn 引理证明极大理想的存在性时,我们已经证明过,这些理想的并依然还是 R 的理想,即 I 依然是 R 的理想.

但 R 所有理想都是主理想,这意味着

$$\text{存在 } b \in R \text{ 使得 } I = (b)$$

这样就有

$$b \in I = \cup_{i\geqslant 0}(a_i)$$

所以存在 n 使得 $b \in (a_n)$,从而

$$I = (b) \subseteq (a_n) \subsetneq (a_{n+1}) \subseteq I$$

得到矛盾!

所以定理28.1的条件 1 也满足,这样就证明了下面这个定理.

定理 28.3. 主理想整环是唯一分解环.

跑到这里,我才想起来,有没有环的理想都是主理想呢?

别慌!前面我们已经看到过,$\mathbb{Z}$ 的所有理想都是主理想.

更多主理想整环

实际上,除了 $\mathbb{Z}$ 以外,任意域 K 上的一元多项式环 $K[x]$ 也是主理想整环.

假设 I 是 $K[x]$ 的非零理想,而 $f(x)$ 为 I 中次数最低的非零多项式,我们断言:

$$I = (f(x)) \text{ 是由 } f(x) \text{ 生成的主理想}$$

实际上,对任意 I 中的多项式 $g(x)$,根据带余除法,存在 $q(x), r(x) \in K[x]$ 使得

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

其中 $r(x) = 0$ 或者

$$r(x) \neq 0,\ \deg r(x) < \deg f(x).$$

由于

$$r(x) = g(x) - q(x)f(x) \in I$$

而 $f(x)$ 是 I 中次数最低非零多项式,因此

$$r(x) = 0, \text{否则 } r(x) \text{ 是 } I \text{ 中次数更低的}$$

$$\text{即: } g(x) = q(x)f(x) \in (f(x)).$$

所以

$$I \subseteq (f(x)) \subseteq I$$

从而 $I = (f(x))$ 是由 (x) 生成的主理想.

这样我们就证明了

定理 28.4. 域上的一元多项式环是主理想整环.

欧氏环

实际上,整数环 $\mathbb{Z}$ 和域上一元多项式环 $K[x]$ 上都有带余除法,只不过一个的余数是用绝对值来控制,一个是用多项式的次数来控制.

从上面的证明可以看出,带余除法就决定了这个环是主理想整环.

我们称整环 R 上有“带余除法”,如果存在

$$N : R\backslash\{0\} \longrightarrow \mathbb{N}_+$$

使得 $\forall a, b \in R, b \neq 0$,存在 $q, r \in R$ 使得

$$a = qb + r, \text{满足}$$

$$r = 0 \text{ 或者 } r \neq 0, N(r) < N(b).$$

有带余除法的环称为

$$\text{欧氏环(Euclidean Domain)}$$

在 $\mathbb{Z}$ 中,映射 $N = |\cdot|$ (取绝对值),而在域上的一元多项式环中 $N = \deg$.

与上面 $K[x]$ 的情况几乎一样,有下面定理

定理 28.5. 欧氏环都是主理想整环.

关于欧氏环的例子,由于大多数课本都举的是高斯整环 $\mathbb{Z}[i]$ 的例子,咱们这里举一个稍微不一样

的

$$\mathbb{Z}[\omega], \omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$$

ω 是三次单位根, 满足

$$1 + \omega + \omega^2 = 0, \text{ 即: } \omega^2 = -1 - \omega$$

因此 $\mathbb{Z}[\omega]$ 中元素都形如

$$a + b\omega, a, b \in \mathbb{Z}$$

现在定义

$$N : \mathbb{Q}[\omega] \longrightarrow \mathbb{Q}_{\geqslant 0}$$
$$x + y\omega \mapsto |x + y\omega|^2 = x^2 + xy + y^2$$

将 N 限制到 $\mathbb{Z}[\omega]$ 上得到

$$N : \mathbb{Z}[\omega] \backslash \{0\} \longrightarrow \mathbb{N}_+$$
$$a + b\omega \mapsto a^2 + ab + b^2$$

由于 N 是取模长的平方, 因此

$$N(\alpha\beta) = N(\alpha)N(\beta), \forall \alpha, \beta \in \mathbb{Z}[\omega]$$

如果 $\beta \neq 0$, 我们需要寻找 $q \in \mathbb{Z}[\omega]$ 使得

$$r = \alpha - q\beta$$

要么为零, 要么 $N(r) < N(\beta)$. 如果 $r \neq 0$, 这等价于证明

$$N(\alpha/\beta - q) = N(r/\beta) < 1$$

现在

$$\alpha/\beta = \alpha\bar{\beta}/|\beta|^2 \in \mathbb{Q}[\omega]$$

因此存在 $x, y \in \mathbb{Q}$ 使得

$$\alpha/\beta = x + y\omega$$

取 $a, b \in \mathbb{Z}$ 使得

$$|a - x| \leqslant \tfrac{1}{2}, |b - y| \leqslant \tfrac{1}{2}$$

令

$$q = a + b\omega$$

则有

$$\begin{aligned} N(\alpha/\beta - q) &= N((x - a) + (y - b)\omega) \\ &= (x - a)^2 + (x - a)(y - b) + (y - b)^2 \\ &\leqslant \frac{3}{2}(x - a)^2 + \frac{3}{2}(y - b)^2 \\ &\leqslant \frac{3}{4} < 1 \end{aligned}$$

这样我们就找到了满足条件的 q:

$$\alpha = q\beta + r$$

使得

$$N(r) < N(\beta)$$

所以 $\mathbb{Z}[\omega]$ 是欧氏环, 是主理想环, 进而是唯一分解环.

29 Gauss 引理

本期导言

我们已经知道

$$\{\text{欧氏环}\} \subseteq \{\text{主理想整环}\} \subseteq \{\text{唯一分解环}\}$$

但像 $\mathbb{Z}[x]$ 这样的环并不是主理想整环, 那它是不是唯一分解环呢?

答案是肯定的! 实际上

定理 29.1. 如果 R 是唯一分解环, 那么 $R[x]$ 也是.

$\mathbb{Z}[x]$ 的唯一分解性

$$\sqrt{2}$$

关于 $\mathbb{Z}[x]$ 的唯一分解性, 我们在高等代数里面已经见过了. 还记得么?

命题 29.2. 假设非零多项式 $f(x) \in \mathbb{Z}[x]$ 在 $\mathbb{Q}[x]$ 中存在分解

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

那么 $f(x)$ 在 $\mathbb{Z}[x]$ 中存在分解

$$f(x) = g_1(x)h_1(x), \text{且}$$
$$g(x) \text{ 与 } g_1(x) \text{ 在 } \mathbb{Q}[x] \text{ 中相伴}$$
$$h(x) \text{ 与 } h_1(x) \text{ 在 } \mathbb{Q}[x] \text{ 中相伴}$$

这个命题的一个推论是:

多项式 $f(x)$ 在 $\mathbb{Z}[x]$ 中不可约, 则其在 $\mathbb{Q}[x]$ 中也不可约!

现在将 $f(x)$ 在 $\mathbb{Z}[x]$ 中分解成不可约多项式的乘积, 如果有两种不同的分解

$$f(x) = ap_1(x) \cdots p_m(x)$$
$$f(x) = bq_1(x) \cdots q_n(x)$$

其中 a, b 是非零整数, 而

$$p_i(x), q_j(x), 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n$$

为 $\mathbb{Z}[x]$ 中不可约多项式, 这些多项式在 $\mathbb{Q}[x]$ 中依然是不可约的, 由于 $\mathbb{Q}[x]$ 是主理想整环, 从而是唯一分解环, 因此

$$m=n,\text{且适当调整顺序后有}$$
$$p_i(x)\text{ 与 }q_i(x)\text{ 在 }\mathbb{Q}[x]\text{ 中相伴},1\leqslant i\leqslant m$$
需要注意的是,这些不可约多项式必为本原多项式(所有系数的最大因子是 1),再次利用上面的命题,很容易发现
$$p_i(x)\text{ 与 }q_i(x)\text{ 在 }\mathbb{Z}[x]\text{ 中相伴},1\leqslant i\leqslant m$$
所以
$$p_i(x)=\pm q_i(x),1\leqslant i\leqslant m$$
从而 $a=\pm b$,这样,在不计正负号的情况下,a,b 在 $\mathbb{Z}$ 中有同样的素分解,从而 $f(x)$ 在 $\mathbb{Z}[x]$ 中是唯一分解的.

由于次数和首项系数绝对值的限制,显然 $\mathbb{Z}[x]$ 中任意元素都能分解成若干个不可约元的乘积.

结合上面说的唯一分解性质可得 $\mathbb{Z}[x]$ 是唯一分解环!

2 整环的商域

现在把 $\mathbb{Z}$ 换成任意唯一分解环,上面的证明是否依然成立?

在 $\mathbb{Z}[x]$ 的情形,至关重要的一点是,我们转化成了 $\mathbb{Q}[x]$ 中的问题,那对一般的唯一分解环 R,我不禁要问:
$$\mathbb{Q}\text{ 将安出?}$$
也就是说,是否可以找到一个域 K,使得其与 R 的关系就恰似 $\mathbb{Q}$ 与 $\mathbb{Z}$ 的关系,什么关系呢?
$$\mathbb{Q}\text{ 中的元素都是 }\frac{m}{n}\text{ 的形式}$$
其中 $m,n\in\mathbb{Z}$ 且 $n\neq 0$,也就是说
$$\mathbb{Q}=\{mn^{-1}\mid m,n\in\mathbb{Z},n\neq 0\}$$
我们需要寻找的域 K 就应该是这样的一个域:

> R 是 K 的子环,有相同的乘法单位元,且
> $$K=\{ab^{-1}\mid a,b\in R,b\neq 0\}$$

那这样的域是否存在呢?

幸运的是,我们可以通过暴力方法构造出这样一个域出来,方法如下:

考虑笛卡尔乘积
$$R\times R^*:=\{(a,b)\mid a,b\in R,b\neq 0\}$$
上的等价关系
$$(a,b)\sim(c,d)\Leftrightarrow ad=bc$$
并把所有对应的等价类记为
$$[\tfrac{a}{b}]$$
令 K 为所有这些等价类构成的集合
$$K:=\{[\tfrac{a}{b}]\mid(a,b)\in R\times R^*\}$$
在 K 上定义加法和乘法:
$$[\frac{a}{b}]+[\frac{c}{d}]:=[\frac{ad+bc}{bd}]$$
$$[\frac{a}{b}]\cdot[\frac{c}{d}]:=[\frac{ac}{bd}]$$
(需要验证定义的加法和乘法是良定义的!)

可以验证 K 在所定义的加法和乘法下构成环,且
$$\text{零元为 }[\tfrac{0}{1}],\text{乘法单位元为 }[\tfrac{1}{1}]$$
对每个非零元 $[\frac{a}{b}]$,即
$$[\tfrac{a}{b}]\neq[\tfrac{0}{1}]$$
也就是 $a\neq b\cdot 0=0$,其逆元为
$$[\tfrac{b}{a}]$$
所以 K 是一个域. 同时 R 可以通过映射
$$R\longrightarrow K$$
$$a\mapsto[\tfrac{a}{b}]$$
将 R 看作 K 的子环,如果您没有强迫症,可以认为 R 就是 K 的子环,这样满足条件的域 K 就找到了.(如果有强迫症,可以去看看那个恶心的挖补定理)

满足上面条件的域是唯一的么?

实际上,如果还有一个域 F 也满足
$$R\text{是}F\text{的子域}$$
$$F=\{ab^{-1}\mid a,b\in R\times R^*\}$$
很容易发现,我们可以定义
$$K\longrightarrow F$$
$$[\tfrac{a}{b}]\mapsto ab^{-1}$$
(验证这个映射是良定义的! 且保持加法和乘法.)

这样我们得到从 K 到 F 的环满同态,其 Kernel 是 K 的理想,只能是 $\{0\}$ 和 K 自己.

这个环同态显然不是零,因此其 Kernel 不是 K,只能是零,从而为单同态.

因此它实际上是 K 到 F 的同构.

所以满足上述条件的域 K 实际上在同构意义下是唯一的,我们称之为 R 的一个商域(quotient field).

显然 $\mathbb{Q}$ 是 $\mathbb{Z}$ 的一个商域.

> **注:** 定义商域的过程中,实际上只需要 R 是整环即可.

唯一分解环上的 Gauss 引理

有了商域, 我们就可以把 $\mathbb{Z}[x]$ 中的 Gauss 引理“山寨”到 $R[x]$ 上, 其中 R 是任意唯一分解环.

定义 29.3. 假设 R 是唯一分解环, 如果 $f(x)\in R[x]$ 的所有系数在 R 中互素 (最大公因子是单位), 则称 $f(x)$ 为 $R[x]$ 中的本原多项式(primitive polynomial).

引理 29.4 Gauss 引理. 假设 R 为唯一分解环, 那么 $R[x]$ 中两个本原多项式的乘积依然是本原多项式.

证明. 假设

$$f(x),g(x)\in R[x]$$

都是本原多项式.

如果 $f(x)g(x)$ 不是本原多项式, 那么存在 R 中的不可约元 p, 使得 p 整除 $f(x)g(x)$ 所有的系数.

记 $\overline{R}:=R/(p)$ 并考虑环同态

$$\pi:R\longrightarrow\overline{R}$$
$$r\mapsto r+(p)$$

它诱导环同态

$$R[x]\longrightarrow\overline{R}[x]$$
$$h(x)\mapsto\overline{h}(x)$$

其中 $\overline{h}(x)$ 的系数为 $h(x)$ 对应的系数在 π 下的像.

令 $h(x)=f(x)g(x)$, 由定义可得

$$\overline{h}(x)=0\text{ 是零多项式}$$

由于 $f(x)$ 和 $g(x)$ 都是本原多项式, 因此 p 不可能整除 $f(x)$ 或 $g(x)$ 的所有系数, 也就是说

$$\overline{f}(x)\neq 0,\overline{g}(x)\neq 0$$

由于 $R[x]\longrightarrow\overline{R}[x]$ 是环同态, 因此

$$\overline{f}(x)\overline{g}(x)=\overline{h}(x)$$

也就是说在 $\overline{R}[x]$ 中, 两个非零多项式的乘积居然可能是零多项式. 下面我们将用事实打脸!

由于 p 为 R 中不可约元, 而 R 是唯一分解环, 因此 p 是 R 中素元, 从而 (p) 为 R 的素理想, 进一步得到 $\overline{R}$ 是整环.

$\overline{R}$ 是整环可以推出 $\overline{R}[x]$ 也是整环, 因此

$$\overline{f}(x)\overline{g}(x)\neq 0$$

产生矛盾!

有了 Gauss 引理, 就可以着手“山寨”命题29.2

命题 29.5. 假设 R 是唯一分解环, 而 K 是 R 的一个商域. 如果非零多项式 $f(x)\in R[x]$ 在 $K[x]$ 中存在分解

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

那么 $f(x)$ 在 $R[x]$ 中存在分解

$$f(x)=g_1(x)h_1(x),\text{且}$$
$$g(x)\text{ 与 }g_1(x)\text{ 在 }K[x]\text{ 中相伴}$$
$$h(x)\text{ 与 }h_1(x)\text{ 在 }K[x]\text{ 中相伴}$$

证明. 这个证明跟高等代数里的证明差不多, 实际上是个体力劳动.

首先存在非零元 $r,s\in R$ 互素且

$$f(x)=rs^{-1}g_0(x)h_0(x)$$

其中 $g_0(x),h_0(x)$ 为 $R[x]$ 中的本原多项式. 实际上由于

$$K=\{ab^{-1}\mid a,b\in R,b\neq 0\}$$

因此存在 $0\neq b_1,b_2\in R$ 使得

$$b_1g(x)\text{ 和 }b_2h(x)\text{ 都属于 }R[x]$$

再把它们的系数的最大公因子提出来, 分别记为 a_1 和 a_2, 则

$$g_0(x):=a_1^{-1}b_1g(x)$$
$$h_0(x):=a_2^{-1}b_2h(x)$$

为 $R[x]$ 中本原多项式且

$$f(x)=(a_1a_2)(b_1b_2)^{-1}g_0(x)h_0(x)$$

最后消去 a_1a_2 与 b_1b_2 的最大公因子得

$$rs^{-1}=(a_1a_2)(b_1b_2)^{-1}\text{ 且 }r,s\text{ 互素}$$

现在

$$sf(x)=rg_0(x)h_0(x)$$

因此 s 整除右边多项式所有的系数, 由于 s 与 r 互素, 由唯一分解环的性质, s 整除 $g_0(x)h_0(x)$ 的所有系数.

由 Gauss 引理 $g_0(x)h_0(x)$ 依然是本原多项式, 所有系数的最大公因子是单位, 因此 s 只能是 R 中单位 (即可逆元). 所以, 实际上

$$rs^{-1}\in R,\text{令}$$
$$g_1(x)=rs^{-1}g_0(x),h_1(x)=h_0(x)$$

命题得证.

推论 29.6. 假设 R 是唯一分解环, 而 K 是它的商域. $f(x)\in R[x]$ 为正次数多项式, 那么

1. $f(x)$ 在 $R[x]$ 中不可约, 则其在 $K[x]$ 中亦不可约.

2. 如果 $R[x]$ 中两个不可约多项式 $p(x), q(x)$ 在 $K[x]$ 中相伴, 那么它们在 $R[x]$ 中亦相伴.

证明. 第一个结论可由上面的命题立即得到.

第二个结论中, 由于 $p(x), q(x)$ 不可约, 至少它们都是本原多项式 (不然可分解成一个 R 中的非单位与一个本原多项式的乘积).

现在 $p(x)$ 与 $q(x)$ 在 $K[x]$ 中相伴, 因此存在 R 中互素的两个元素 r, s 使得

$$p(x) = s^{-1}rq(x), \text{从而}$$
$$sp(x) = rq(x)$$

由命题29.5证明中同样的方法可证 r, s 都是 R 中单位, 因此

$$p(x) \text{ 与 } q(x) \text{ 在 } R[x] \text{ 中相伴}$$

跟本期第 1 小节的证明一样可得定理29.1:

定理 29.7 **定理29.1.** 如果 R 是唯一分解环, 那么 $R[x]$ 也是唯一分解环.

推论 29.8. 如果 R 是唯一分解环, 那么它上的多元多项式环

$$R[x_1, \cdots, x_n]$$

也是唯一分解环.

上面的定理和推论告诉我们一个事实:

有许多唯一分解环并不是主理想整环

30 唯一分解性的进一步例子

本期导言

我们前面学过 $\mathbb{Z}[\sqrt{-1}]$ 和 $\mathbb{Z}[\sqrt{-2}]$ 都是欧氏环. 本期我们来讨论下 $\mathbb{Z}[\sqrt{-D}]$ 的情况, 其中 D 为正整数. 这实际上跟一个经典的初等数论问题相关:

问题 9. 一个素数 p 何时能分解为 $x^2 + Dy^2$ 的形式? 其中 x, y 为整数.

$D = 1$ 的情形就是所谓的费马二平方定理.

唯一分解性和素数的分解

先来讨论上面那个数论问题, 假设 D 为正整数, 如果一个素数 p 可以分解为

$$p = x^2 + Dy^2$$

两边模 p 可以发现, x 和 y 都不能被 p 整除. 因此在有限域 $\mathbb{Z}_p$ 中, x 和 y 都非零, 从而可逆. 下面等式在 $\mathbb{Z}_p$ 中成立

$$(\frac{x}{y})^2 = -D$$

从而 $-D$ 在 $\mathbb{Z}_p$ 中存在平方根.

我们将证明下面这个有趣的定理.

定理 30.1. 假设 D 为正整数且 $\mathbb{Z}[\sqrt{-D}]$ 是唯一分解整环. 那么素数 p 存在分解

$$p = x^2 + Dy^2, x, y \in \mathbb{Z}$$

当且仅当 $-D$ 在 $\mathbb{Z}_p$ 中有平方根.

证明. 上面我们已经证明了必要性. 这里只需要再证明充分性. 假设 $-D$ 在 $\mathbb{Z}_p$ 中有平方根, 即存在整数 m 使得

$$m^2 + D \equiv 0 \pmod{p}$$

即存在整数 n, 使得

$$m^2 + D = pn$$

在 $\mathbb{Z}[\sqrt{-D}]$ 中有

$$(m + \sqrt{-D})(m + \sqrt{-D}) = pn$$

我们断言 p 在环 $\mathbb{Z}[\sqrt{-D}]$ 一定是可约的. 否则, 由于 $\mathbb{Z}[\sqrt{-D}]$ 是唯一分解环, 不可约元也是素元, 而 p 不可约将导致其为素元, 必整除

$$m \pm \sqrt{-D}$$

之一, 即存在整数 a, b, 使得

$$p(a + b\sqrt{-D}) = m \pm \sqrt{-D}$$

从而 $pb = \pm 1$, 产生矛盾.

因此 p 在 $\mathbb{Z}[\sqrt{-D}]$ 中可约, 存在真分解, 即

$$p = (a + b\sqrt{-D})(c + d\sqrt{-D})$$

且右边两个因子都不是 $\mathbb{Z}[\sqrt{-D}]$ 中的单位 (可逆元). 两边在 $\mathbb{C}$ 中取模长平方得

$$p^2 = (a^2 + Db^2)(c^2 + Dd^2)$$

等式右边为两个正整数的乘积. 要么它们都是 p, 要么一个为 p^2, 另一个为 1.

但在环 $\mathbb{Z}[\sqrt{-D}]$ 中, 如果一个元素 z 的模长平方为 1, 其共轭复数 $\bar{z}$ 也在 $\mathbb{Z}[\sqrt{-D}]$ 中, 且 $z\bar{z} = 1$, 从而 z 在环 $\mathbb{Z}[\sqrt{-D}]$ 中可逆, 为其中的单位.

因此在我们前面的假设下

$$(a^2 + Db^2) \text{ 和 } (c^2 + Dd^2)$$

都不等于 1(否则为 $\mathbb{Z}[\sqrt{-D}]$ 中单位, 与假设矛盾). 因此

$$a^2 + Db^2 = p$$

需要指出的是, 由上面的证明可得

$$p = (a + b\sqrt{-D})(a - b\sqrt{-D})$$

从而 $c = a, d = -b$. 另外, $a \pm b\sqrt{-D}$ 实际上还是 $\mathbb{Z}[\sqrt{-D}]$ 中的不可约元. 因此分解

$$p = (a + b\sqrt{-D})(a - b\sqrt{-D})$$

是由 p 唯一确定的.

那为什么 $a \pm b\sqrt{-D}$ 为 $\mathbb{Z}[\sqrt{-D}]$ 中的不可约元呢? 实际上 $\mathbb{Z}[\sqrt{-D}]$ 中任意模长平方为素数的元素 z 都是不可约的. 如果 z 有分解

$$z = z_1 z_2$$

那么

$$|z|^2 = |z_1|^2 |z_2|^2$$

由于 $|z_1|^2, |z_2|^2$ 都是整数, 而 $|z|^2$ 是素数, 因此

$$|z_1|^2 = 1 \text{ 或 } |z_2|^2 = 1$$

不妨设 $|z_1|^2 = 1$, 则

$$z_1 \bar{z}_1 = |z_1|^2 = 1$$

从而 z_1 在 $\mathbb{Z}[\sqrt{-D}]$ 中可逆, 为单位. 这说明 z 没有真分解, 从而不可约.

真的是唯一分解环么?

定理30.1成立的前提条件是

$$\mathbb{Z}[\sqrt{-D}]$$

是唯一分解整环, 但问题是它是么? 我们之前已经知道当 $D = 3$ 时, 它不是唯一分解整环呀. 对其他的整数呢? 会不会大多数情况下都不是唯一分解整环呢? 如果是这样的话, 大家可能会对定理30.1很失望. 但塞翁失马, 焉知非福, 利用定理30.1反而可以让我们轻松说明

推论 30.2. 对于 $D \geqslant 3$, $\mathbb{Z}[\sqrt{-D}]$ 不是唯一分解整环.

证明. 假设 $\mathbb{Z}[\sqrt{-D}]$ 是唯一分解整环. 由定理30.1, 任意素数 p 存在分解

$$p = x^2 + Dy^2, x, y \in \mathbb{Z}$$

当且仅当 $-D$ 在 $\mathbb{Z}_p$ 中有平方根. 我们取 $p = 2$, 由于 $\mathbb{Z}_2$ 中的两个元素 $0, 1$ 都有平方根, 由定理30.1, 存在分解

$$2 = x^2 + Dy^2, x, y \in \mathbb{Z}$$

当 $D \geqslant 3$ 时, 这显然是不可能的. 因此, 当 $D \geqslant 3$ 时, $\mathbb{Z}[\sqrt{-D}]$ 不是唯一分解整环.

费马二平方定理

当 $D = 1$ 时, 定理30.1说明一个素数 p 能写成两个整数的平方和当且仅当 -1 在 $\mathbb{Z}_p$ 中有平方根. 由于 $2 = 1^2 + 1^2$ 总是成立, 我们只考虑 p 为奇素数的情况, 此时 $\mathbb{Z}_p$ 中 $-1 \neq 1$, -1 有平方根等价于乘法群 $\mathbb{Z}_p^*$ 中存在 4 阶元. 由于 $\mathbb{Z}_p^*$ 是循环群, 这进一步等价于 $p - 1$ 被 4 整除, 即

$$p \equiv 1 \pmod 4$$

推论 30.3. 奇素数 p 可以分解为两个整数的平方和当且仅当

$$p \equiv 1 \pmod 4$$

不计符号和顺序, 分解是唯一的.

31 主理想整环的进一步例子

本期导言

今天在讲域的单扩张时,需要用到主理想整环的一个性质

所有的非零素理想都是极大理想

想起来主理想整环其实有两个很有意思的刻画方式:

定理 31.1. 一个整环 R 是主理想整环,当且仅当,R 的所有素理想都是主理想.

定理 31.2. 一个唯一分解整环 R 是主理想整环,当且仅当,R 的所有非零素理想都是极大理想.

这一期我们就来讲讲这两个定理.

代数单扩张与主理想整环

讲到代数元的单扩张时,有下面这个事情发生.假设 α 是域 K 上的代数元,那么

$$K[\alpha]=K(\alpha)\cong K[x]/(p(x))$$

其中 $p(x)$ 为 α 在 K 上的极小多项式. 原因是,考虑环同态

$$\pi: K[x]\longrightarrow K[\alpha], f(x)\mapsto f(\alpha)$$

因为 α 为 K 上代数元,此时 $\operatorname{Ker}\pi$ 非零. 由环同态基本定理

$$K[x]/\operatorname{Ker}\pi\cong K[\alpha]$$

由于 $K[\alpha]$ 是域 $K(\alpha)$ 的子环,没有零因子,所以 $\operatorname{Ker}\pi$ 是 $K[x]$ 的非零素理想. 但 $K[x]$ 是主理想整环,$\operatorname{Ker}\pi=(p(x))$ 为主理想. 此时 $p(x)$ 为 $K[x]$ 的素元,从而是 $K[x]$ 中不可约元. 根据不可约元的理想描述,$(p(x))$ 为 $K[x]$ 的极大主理想. 再次利用 $K[x]$ 为主理想整环,所有的极大主理想自动升级为极大理想,因此 $\operatorname{Ker}\pi$ 是 $K[x]$ 的极大理想.

由这个过程,大家很容易发现下面这个事实.

命题 31.3. 主理想整环的非零素理想都是极大理想.

定理31.1的证明

实际上,要想让一个整环变成主理想整环,只需要要求其所有的素理想都是主理想就够了 (放过其他理想),也就是我们开篇说的定理31.1.

下面我们给出证明.

定理*31.1*的证明. 只需要证明充分性,现在假设 R 的素理想都是主理想.

令 $\mathcal{X}$ 为 R 所有非主理想构成的集合. 我们断言 $\mathcal{X}$ 是空集. 否则,可在 $\mathcal{X}$ 中利用 Zorn 引理. 假设 $\mathcal{Y}$ 为 $\mathcal{X}$ 的全序子集,跟咱们讨论素理想的存在性时一样,$\mathcal{Y}$ 中所有理想的并集

$$I=\bigcup_{Y\in\mathcal{Y}}Y$$

也是 R 的理想. 如果 $I=(a)$ 为主理想,则存在 $Y\in\mathcal{Y}$ 使得 $a\in Y$, 从而 $I\subseteq Y\subseteq I$. 所以 $I=Y$ 不是主理想,与假设矛盾. 因此 I 并不是主理想,即 $I\in\mathcal{X}$. 显然 I 包含 $\mathcal{Y}$ 中的所有理想,为 $\mathcal{Y}$ 在 $\mathcal{X}$ 中的一个上界. 由 Zorn 引理,$\mathcal{X}$ 中存在极大元 $\mathfrak{a}$.

由于 R 的素理想都是主理想,而 $\mathfrak{a}$ 不是主理想,因此 $\mathfrak{a}$ 不是素理想,存在 $x,y\notin\mathfrak{a}$ 使得 $xy\in\mathfrak{a}$.

此时理想 $I:=(\mathfrak{a},x)$ 严格包含 $\mathfrak{a}$. 由 $\mathfrak{a}$ 的极大性,I 不属于 $\mathcal{X}$, 也就是说 I 是主理想,假设 $I=(\alpha)$.

现考虑理想

$$J=\{r\in R\mid rI\subseteq\mathfrak{a}\}$$

则有 $\mathfrak{a}\subseteq J, y\in J$, 从而 $(\mathfrak{a},y)\subseteq J$ 再次利用 $\mathfrak{a}$ 的极大性可知 J 为主理想,不妨设 $J=(\beta)$. 根据 J 的定义有

$$JI\subseteq\mathfrak{a}$$

另外,对任意 $u\in\mathfrak{a}$, 有 $u\in(\alpha)$, 所以存在 $v\in R$ 使得

$$u=v\alpha$$

这同时说明 $v\in J$, 所以 $u\in JI$. 这就证明了 $\mathfrak{a}=JI=(\alpha\beta)$, 与 $\mathfrak{a}$ 不是主理想矛盾.

因此 $\mathcal{X}$ 为空集,R 的所有理想均为主理想.

3

定理31.2的证明

同样的我们只需要证明充分性. 也就是说现在 R 是唯一分解整环, 且每个非零素理想都是极大理想, 我们需要证明 R 是主理想整环.

定理*31.2*充分性. 由定理31.1, 我们只需要证明所有的素理想都是主理想. 首先 0 理想当然是主理想, 现假设 $\mathfrak{p}$ 为非零素理想. 取 $\mathfrak{p}$ 中非零元 r, 显然 r 不可逆 (否则 $\mathfrak{p}=R$). 由于 R 是唯一分解整环, 因此 r 可以分解为不可约元素的乘积:

$$r = p_1 p_2 \cdots p_n$$

由于 $\mathfrak{p}$ 是素理想, 这导致存在某个 $p_i \in \mathfrak{p}$. 从而

$$(p_i) \subseteq \mathfrak{p}$$

现在 p_i 是不可约元, 由于 R 是唯一分解整环, 因此 p_i 也是 R 是素元, 也就是说主理想 (p_i) 是非零素理想, 根据假设, (p_i) 为极大理想, 从而

$$(p_i) = \mathfrak{p}$$

因此 $\mathfrak{p}$ 为主理想.

32 $\mathbb{Z}[\xi]$: 主理想整环但非欧氏环

本期前言

我们很多《近世代数》的教科书上说明主理想整环不一定是欧氏环都用的是下面这个例子: 令

$$\xi = \frac{1+\sqrt{-19}}{2}$$

然后说环 $\mathbb{Z}[\xi]$ 是主理想整环, 但不是欧氏环.

本期我们就来证明这个结论.

1

$\mathbb{Z}[\xi]$ 的基本性质

通过直接计算可得下列性质:

- $\xi \cdot \overline{\xi} = 5$
- $\xi^2 = \xi - 5$
- $\overline{\xi} = 1 - \xi$
- 对实数 a, b, $|a+b\xi|^2 = a^2 + 5b^2 + ab$

根据这几个特点, 可以发现

$\mathbb{Z}[\xi]$ 的单位 (可逆元) 只有 ± 1

实际上, 如果

$$a + b\xi, a, b \in \mathbb{Z}$$

是单位, 那么存在整数 c, d, 使得

$$1 = (a+b\xi)(c+d\xi)$$

两边取模长平方可得

$$1 = (a^2 + 5b^2 + ab)(c^2 + 5d^2 + cd)$$

这导致 $b = d = 0$, $a = c = \pm 1$.

另外, 类似的分析可得

$2, 3$ 在 $\mathbb{Z}[\xi]$ 中不可约

如若不然, 有整数 a, b, c, d, 使得

$$2 \text{ 或 } 3 = (a+b\xi)(c+d\xi)$$

且

$$a + b\xi \neq \pm 1$$
$$c + d\xi \neq \pm 1$$

同样两边取模长平方可得

$$(a^2 + 5b^2 + ab)(c^2 + 5d^2 + cd) = 4 \text{ 或 } 9$$

如果 b 或者 d 不为零, 左边的两个因数都大于 4, 不可能是 4 或者 9 的因数, 因此 $b = d = 0$, 从而 $2 = ac$, 其中 a 和 c 之一必为 ± 1, 从而 $a + b\xi = \pm 1$ 或者 $c + d\xi = \pm 1$, 产生矛盾!

2 $\mathbb{Z}[\xi]$ 不是欧氏环

定理 32.1. $\mathbb{Z}[\xi]$ 不是欧氏环

证明. 用反证法, 假设 $\mathbb{Z}[\xi]$ 是欧氏环, 而

$$d : \mathbb{Z}[\xi] \longrightarrow \mathbb{N}$$

是相应的映射使得, 对任意 $a, b \in \mathbb{Z}[\xi]$ 且 $b \neq 0$, 存在 $q \in \mathbb{Z}[\xi]$ 使得

$$a = qb + r$$

满足 $r = 0$ 或者 $r \neq 0$ 但 $d(r) < d(b)$.

取 m 为 $\mathbb{Z}[\xi]$ 中非零非单位, 使得 $d(m)$ 最小. 注意到 $\mathbb{Z}[\xi]$ 中的单位只有 ± 1, 因此 $d(m)$ 最小的含义是:

$$d(m) \leqslant d(a), \text{ 对任意 } 0, \pm 1 \neq a \in \mathbb{Z}[\xi]$$

考虑带余除法

$$2 = qm + r$$

由 $d(m)$ 的最小性可得 r 只能是 $0, \pm 1$.

如果 $r = 0$, 则 $m \mid 2$, 由于 m 不是单位, 2 不可约, 这导致 $2 = mu$, 其中 u 是 $\mathbb{Z}[\xi]$ 中的单位, 从而 $m = \pm 2$.

如果 $r = -1$, 可得 $m \mid 3$, 可得 $m = \pm 3$.

$r = 1$ 不可能发生, 因此这会导致 $m \mid 1$, 从而 m 是单位, 跟假设矛盾.

因此 $m = \pm 2, \pm 3$. 最后考虑带余除法

$$\xi = qm + r$$

其中 $r = 0$ 或者 $r \neq 0$ 但 $d(r) < d(m)$, 从而 r 也只能是 $0, \pm 1$. 逐个验证所有可能性可发现

$$q = \frac{\xi - r}{m}$$

都不属于 $\mathbb{Z}[\xi]$, 因此这个带余除法不成立, 产生矛盾!

3 $\mathbb{Z}[\xi]$ 是主理想整环

我们需要证明 $\mathbb{Z}[\xi]$ 的非零理想都是由一个元素生成的.

在这一小节, 为了记号方便, 我们记

$$R = \mathbb{Z}[\xi]$$

主要的想法是这样的:

> 对任意 R 的非零理想 I, 取 I 中模长 (平方) 最小的非零元b, 然后证明 $I = bR$ 是由 b 生成的主理想.
>
> 证明也是用反证法, 假设 $I \neq bR$. 我们努力寻找 $a \in I \backslash bR$ 和 $p, q \in R$, 使得
>
> $$0 \neq |ap - bq| < |b|$$
>
> 或者等价的
>
> $$0 \neq |\tfrac{a}{b} \cdot p - q| < 1$$
>
> $ap - bq \in I$ 非零, 但模长小于 $|b|$, 产生矛盾!

证明中需要用到一个基本的事实, 复数

$$z = x + yi, |y| < \tfrac{\sqrt{3}}{2}$$

则存在整数 m 使得

$$|z - m| < 1$$

实际上, 这是显而易见的, 选取整数 m 使得

$$|m - x| \leqslant \tfrac{1}{2}$$

则有

$$|z - m|^2 = (m - x)^2 + y^2 < \tfrac{1}{4} + \tfrac{3}{4} = 1$$

定理 32.2. $R = \mathbb{Z}[\xi]$ 是主理想整环.

证明. 令 I 为 R 是非零理想, 而 $b \in I$ 是 I 中模长最小的非零元, 并假设 $I \neq bR$. 我们将证明存在

$$a \in I \backslash bR, p, q \in R$$

使得

$$0 \neq |\tfrac{a}{b} \cdot p - q| < 1$$

从而有

$$0 \neq |ap - bq| < |b|$$

但 $ap - bq \in I$, 这与 $|b|$ 的最小性矛盾.

先任取 $a \in I \backslash bR$, 则

$$a/b \in \mathbb{Q}[\xi]$$

由于 ξ 的虚部是 $\sqrt{19}/2$, 通过移动 ξ 的整数倍可使得

$$\tfrac{a}{b} + n\xi = x + yi$$

的虚部 y 在 $\pm\sqrt{19}/4$ 之间, 其中 $n \in \mathbb{Z}$. 这时, 我们可以取

$$a' = a + nb, \text{ 属于 } I, \text{ 但不属于 } bR$$

且有

$$a'/b = x + yi$$

因此, 我们可以不妨假设

$$a/b = x + yi$$

其中虚部 y 在 $\pm\sqrt{19}/4$ 之间.

如果 $|y| < \sqrt{3}/2$, 我们前面说过 $x + yi$ 与某个整数 $q \in R$ 的差的模长小于 1, 即

$$|\tfrac{a}{b} - q| < 1$$

取 $p = 1$, 得

$$|\tfrac{a}{b} \cdot p - q| < 1$$

如果 $|y| \geqslant \sqrt{3}/2$, 我们可以假设

$$\tfrac{\sqrt{3}}{2} \leqslant y \leqslant \tfrac{\sqrt{19}}{4}$$

(如果 $y < 0$, 我们可以用 $-a$ 替换 a). 此时

$$\tfrac{2a}{b} - \xi$$

的虚部为

$$2y - \tfrac{\sqrt{19}}{2}$$

在 $\sqrt{3} - \sqrt{19}/2$ 和 0 之间, 但

$$\sqrt{19} < \sqrt{27} = 3\sqrt{3}$$

因此

$$0 > \sqrt{3} - \tfrac{\sqrt{19}}{2} > -\tfrac{\sqrt{3}}{2}$$

从而存在整数数 q', 使得

$$|\tfrac{2a}{b} - \xi - q'| < 1$$

取 $q = \xi + q' \in R, p = 2$, 就得到

$$|\tfrac{a}{b} \cdot p - q| < 1 \quad (*)$$

当然, 这里我们没有说明

$$\tfrac{a}{b} \cdot p - q \neq 0$$

注意到上面两种情况中, p 只取 $1, 2$. 在 $p = 1$ 时

$$\tfrac{a}{b} - q = 0$$

不可能发生. 如若不然

$$a = bq \in bR$$

与假设矛盾. 当 $p = 2$ 时, 在上面式 $(*)$ 中, 如果

$$\tfrac{a}{b} \cdot 2 - q = 0$$

这里 $q = q' + \xi$, 其中 q' 是个整数.

如果 $q' = 2k - 1$ 是奇数, 我们有

$$\tfrac{2(a-kb)}{b} \cdot \xi = (-1 + \xi)\xi = -5$$

重新取 $a' = a - kb$, $p = \xi$, $q = -3$, 我们有

$$\tfrac{a'}{b} \cdot p - q = \tfrac{1}{2}$$

模长小于 1, 此时 $a' \notin bR, p, q \in R$ 满足要求.

如果 $q' = 2k$ 是奇数, 我们有

$$\tfrac{2(a-kb)}{b} \cdot \overline{\xi} = \xi \cdot \overline{\xi} = 5$$

重新取 $a' = a - kb \notin bR$, $p = \overline{\xi} \in R$, $q = 2$, 我们有

$$\tfrac{a'}{b} \cdot p - q = \tfrac{1}{2}$$

模长小于 1, 满足要求.

总结起来, 无论哪种情况, 我们都能找到 $a \in I \backslash bR$, $p, q \in R$, 使得

$$0 \neq |\tfrac{a}{b} \cdot p - q| < 1$$

定理得证.

参考文献

[1] Oscar A. Campoli, A principal ideal domain that is not a Euclidean domain, *Amer. Math. Monthly*, 95(1988), 868–871.

33 域

本期导言

由于期末考试已经很近了,春节也不远了,所以我们先写写域论的东西,更多唯一分解环的内容包括整环的商域都留到后面再写.

1 Why 域?

咱们课程一开始就是关心代数方程的求根问题. 对于一个有理系数多项式

$$f(x) \in \mathbb{Q}[x]$$

假设它在 $\mathbb{C}$ 中根为

$$\xi_1, \cdots, \xi_r$$

考虑 $\mathbb{C}$ 的包含

$$\mathbb{Q} \text{ 和 } \{\xi_1, \cdots, \xi_r\}$$

的最小子域 E.

实际上 E 是所有如下形式复数的集合

$$\frac{g(\xi_1, \cdots, \xi_r)}{h(\xi_1, \cdots, \xi_r)}$$

其中, $g(x_1, \cdots, x_r)$ 和 $h(x_1, \cdots, x_r)$ 都是 $\mathbb{Q}$ 上的 r 元多项式且满足

$$h(\xi_1, \cdots, \xi_r) \neq 0$$

这个域称为 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域.

Galois 告诉我们 $f(x) = 0$ 可以根式解, 当且仅当其 Galois 群

$$\mathrm{Gal}(f) := \mathrm{Aut}_{\mathbb{Q}} E \text{ 是可解群}$$

我们最关心的就是像 E 这些复数域的子域.

当然 $\mathbb{Q}$ 也是 E 的子域.

E 相对于 $\mathbb{Q}$ 的结构决定了 f 的 Galois 群, 因此讨论域 E 之于 $\mathbb{Q}$ 的结构是非常有意思的一件事情.

2 子域与扩域

给定一个域 E 和它的子域 K:

$$(K, +) \leqslant (E, +)$$
$$(K^*, \cdot) \leqslant (E^*, \cdot)$$

此时 E 称为 K 的一个扩域, 这个比较好理解, 借助 02 年韩阳老师给我们上课时说的一句话 “他是你兄弟, 你就是他哥”, 说得正是子域与扩域的关系.

怎样描述 E 与 K 之间的关系? 怎样求出它们之间的 Galois 群?

$$\mathrm{Aut}_K E := \{\sigma \in \mathrm{Aut}(E) \mid \sigma|_K = \mathrm{id}\}$$

这些都是我们关心的问题.

从哪里开始思考这些问题呢?

我们可以考虑夹在 K 与 E 之间的域, 即

$$L \text{ 是 } E \text{ 的子域, 同时又是 } K \text{ 的扩域}$$

称 L 为 K 和 E 的中间域. 通过讨论中间域的多少以及它们之间的关系来讨论 E 与 K 之间的相对关系.

K 与 E 之间有多少中间域呢?

实际上任取 E 中若干个元素

$$\alpha_1, \cdots, \alpha_r$$

都可以 “构造” 出一个 K 和 E 之间的中间域

$$K(\alpha_1, \cdots, \alpha_r)$$

它是 E 的含 K 和 $\alpha_1, \cdots, \alpha_r$ 的最小子域, 为所有如下形式元素的集合:

$$\frac{g(\alpha_1, \cdots, \alpha_r)}{h(\alpha_1, \cdots, \alpha_r)}$$

其中 g, h 都是 $K[x_1, \cdots, x_r]$ 中多项式满足

$$g(\alpha_1, \cdots, \alpha_r) \neq 0.$$

3 单扩张

最简单的中间域莫过于

$$K(\alpha)$$

其中 $\alpha \in E$, 称为

$$K \text{ 的单扩张(simple extension).}$$

例如: $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\pi)$ 等.

之所以说 $K(\alpha)$ 相对于 K 比较简单, 是因为有一个非常自然的环同态

$$\phi : K[x] \longrightarrow K(\alpha)$$
$$g(x) \mapsto g(\alpha)$$

可以用于比较 $K[x]$ 与 $K(\alpha)$ 的关系.

考虑 ϕ 的 Kernel 分为两种情况

$$\mathrm{Ker}\,\phi = \{0\} \text{ 和 } \mathrm{Ker}\,\phi \neq \{0\}$$

4 超越元

第一种情况

$$\operatorname{Ker}\phi=\{0\}$$

就是说没有非零的多项式 $g(x)$ 能够使得 $g(\alpha)=0$, 换个角度说, 就是

$$1,\alpha,\alpha^2,\cdots$$

是 K 线性无关的! 这种情况, 我们称 α 是 K 上的超越元.

此时 ϕ 是单射, $K[x]$ 与它在 ϕ 的像集

$$K[\alpha]=\{g(\alpha)\mid g\in K[x]\}$$

作为环是同构的, 而这个同构

$$\phi:K[x]\longrightarrow K[\alpha]$$
$$g(x)\mapsto g(\alpha)$$

可以扩展成一个域同构

$$K(x)\longrightarrow K(\alpha)$$
$$\frac{g(x)}{h(x)}\mapsto\frac{g(\alpha)}{h(\alpha)}$$

这里 $K(x)$ 是 K 上有理多项式的集合, 即

$$\{\frac{g(x)}{h(x)}\mid g(x),h(x)\in K[x],\text{其中 }h(x)\neq 0\}$$

5 代数元

第二种情况

$$\operatorname{Ker}\phi\neq\{0\}$$

就是说存在非零的多项式 $g(x)$ 使得

$$g(\alpha)=0$$

当然也可以说存在 $n>0$ 使得

$$1,\alpha,\alpha^2,\cdots,\alpha^n$$

是 K 线性相关的. 这种情况, 我们称 α 是 K 上的代数元.

这种情况就比较有趣了, $\operatorname{Ker}\phi$ 是所有满足

$$g(\alpha)=0$$

的多项式 $g(x)$ 组成的集合, 是 $K[x]$ 的理想, 而 $K[x]$ 是主理想整环, 因此

$$\operatorname{Ker}\phi=(m(x))$$

是由一个非零多项式 $m(x)$ 生成的理想.

此时 $m(x)$ 是 $\operatorname{Ker}\phi$ 中次数最低的非零多项式, 也就是满足 $m(\alpha)=0$ 的最低次数多项式, 称为 α 在 K 上的极小多项式.

看上去跟矩阵的极小多项式有点像, 但跟矩阵的极小多项式还有一个非常大的区别:

引理 33.1. *α 的极小多项式在 $K[x]$ 中不可约.*

证明. 由环同态基本定理第一同构定理

$$K[x]/\operatorname{Ker}\phi\simeq K[\alpha]$$

作为域 $K(\alpha)$ 的子环, $K[\alpha]$ 没有零因子, 是整环, 因此

$$\operatorname{Ker}\phi\text{ 是 }K[x]\text{ 的素理想}$$

由于 $\operatorname{Ker}\phi=(m(x))$, 这等于说

$$m(x)\text{ 是 }K[x]\text{ 中素元}$$

从而 $m(x)$ 是 $K[x]$ 中不可约元!

一般矩阵的极小多项式不一定不可约, 而这里 α 的极小多项式一定不可约.

故事还没有完, $m(x)$ 在 $K[x]$ 中不可约, 用理想的语言就是

$$(m(x))\text{ 是 }K[x]\text{ 的极大主理想}$$

由于 $K[x]$ 的理想都是主理想, 这等于说

$$(m(x))\text{ 是 }K[x]\text{ 的极大理想}$$

这句话又等价于说

$$K[x]/(m(x))\text{ 是域}$$

这告诉我们

$$K[\alpha]\simeq K[x]/(m(x))\text{ 也是域}$$

这个域既包含了 K, 也包含了 α, 而 $K(\alpha)$ 是最小的满足这个条件的域, 因此

$$K(\alpha)\subseteq K[\alpha],\text{但 }K[\alpha]\subseteq K(\alpha)$$

因此 $K(\alpha)=K[\alpha]$.

总结成下面的定理

定理 33.2. *所设 α 是 K 上的代数元, 则*

$$K(\alpha)=K[\alpha].$$

例如: $\alpha=\sqrt{2}$, 则

$$\mathbb{Q}(\sqrt{2})=\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$$

为什么这里只有两个系数 a,b 呢? 因为 $\sqrt{2}$ 的极小多项式为

$$x^2-2$$

对于任意 $g(x)\in\mathbb{Q}[x]$, 利用带余除法, 存在 $r(x)=a+bx$, 和 $q(x)\in\mathbb{Q}[x]$, 使得

$$g(x)=q(x)(x^2-2)+r(x)$$

从而

$$g(\sqrt{2})=q(\sqrt{2})(\sqrt{2}^2-2)+r(\sqrt{2})$$
$$=r(\sqrt{2})=a+b\sqrt{2}$$

一般的,对于域 K 上的代数元 α,假设其极小多项式 $m(x)$ 次数为 n.

对于任意 $g(x)\in K[x]$,存在 $q(x),r(x)\in K[x]$ 使得

$$g(x)=q(x)m(x)+r(x)$$

其中

$$r(x)=b_0+b_1x+\cdots+b_{n-1}x^{n-1}$$

从而

$$\begin{aligned}g(\alpha)&=q(\alpha)m(\alpha)+r(\alpha)=r(\alpha)\\&=b_0+b_1\alpha+\cdots+b_{n-1}\alpha^{n-1}\end{aligned}$$

是 $1,\alpha,\cdots,\alpha^{n-1}$ 的 K 线性组合.

另一方面,这些

$$1,\alpha,\cdots,\alpha^{n-1}$$

也是 K 线性无关的,否则,存在次数不超过 $n-1$ 的非零 K 系数非零多项式 $h(x)$,使得 $h(\alpha)=0$. 这样

$$h(x)\in\operatorname{Ker}\phi=(m(x)),\text{即 }m(x)\mid h(x)$$

产生矛盾!

总结下!

定理 33.3. 假设 α 是域 K 上代数元,极小多项式 $m(x)$ 的次数为 n,则

$$\dim_K K(\alpha)=\deg m(x)=n$$

作为 K 空间,$K(\alpha)$ 的一组基是

$$1,\alpha,\cdots,\alpha^{n-1}.$$

怎样寻找极小多项式

那怎样寻找一个代数元的极小多项式呢? 上面怎么一口咬定 x^2-2 是 $\sqrt{2}$ 在 $\mathbb{Q}$ 上的极小多项式呢?

实际上根据代数元的极小多项式一定是不可约多项式这个特点,寻找代数元的极小多项式比寻找矩阵的极小多项式要简单很多.

命题 33.4. 假设 α 是域 K 上代数元,而 $p(x)\in K[x]$ 满足 $p(\alpha)=0$ 和下面两个条件之一

1. $p(x)$ 不可约
2. $\dim_K K(\alpha)=\deg p(x)$

那么 $p(x)$ 是 α 的极小多项式.

证明. 实际上,由于 $p(x)=0$,所以

$$m(x)\mid p(x)$$

命题中两个条件都能导致

$$m(x)\text{ 与 }p(x)\text{ 相伴}$$

也就是说它们只是差一个非零常数倍,因此 $p(x)$ 也是 α 在 K 上的极小多项式.

比如上面的 $g(x)=x^2-2$ 是 $\mathbb{Q}[x]$ 中不可约多项式且 $g(\sqrt{2})=0$,因此它是 $\sqrt{2}$ 在 $\mathbb{Q}$ 是的极小多项式.

再来个复杂点的例子.

例 27. $\alpha=\sqrt{2}+\sqrt{3}$ 它在 $\mathbb{Q}$ 上的极小多项式 $m(x)$ 是?

通过平方可以发现

$$(\alpha^2-5)^2=24$$

因此多项式

$$g(x)=x^4-10x^2+1$$

满足 $g(\alpha)=0$,从而 $m(x)\mid g(x)$.

在下一期我们将能证明

$$\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}+\sqrt{3})=4$$

根据命题33.4,$g(x)$ 是 α 的极小多项式.

当然,我们也可以通过证明 $g(x)$ 在 $\mathbb{Q}[x]$ 中不可约来说明它是 α 的极小多项式.

这里我们讨个巧,既不用下一期的知识,又不用费力去证明 $g(x)$ 是不可约的. 由于

$$1/\alpha=\sqrt{3}-\sqrt{2}$$

因此

$$\sqrt{2}=\tfrac{1}{2}(\alpha-1/\alpha)\in\mathbb{Q}(\alpha)$$

因此

$$\mathbb{Q}(\sqrt{2})\subseteq\mathbb{Q}(\alpha)$$

但是

$$\alpha=\sqrt{2}+\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$$

因此 $\mathbb{Q}(\sqrt{2})\subsetneq\mathbb{Q}(\alpha)$,从而

$$\begin{aligned}\deg m(x)&=\dim_{\mathbb{Q}}\mathbb{Q}(\alpha)\\&>\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt{2})=2\end{aligned}$$

很容易发现 $g(x)$ 没有有理根,因此在 $\mathbb{Q}[x]$ 中并没有 1 次因式,从而也没有 3 次因式,而 $m(x)$ 又是 $g(x)$ 在 $\mathbb{Q}[x]$ 中的大于 2 次的因式,因此 $\deg m(x)=4$,迫使 $m(x)$ 与 $g(x)$ 相伴,所以 $g(x)$ 也是 α 在 $\mathbb{Q}$ 上的极小多项式.

34 有限扩张

本期导言

我们继续从不同的维度来讨论域扩张.

1 有限扩张

还是从多项式的分裂域说起, 假设 $f(x)$ 为有理系数多项式, 而

$$\xi_1, \cdots, \xi_r$$

为 $f(x)$ 在复数域中所有的根, 我们很想知道 $f(x)$ 的分裂域

$$E = \mathbb{Q}(\xi_1, \cdots, \xi_r)$$

相对于 $\mathbb{Q}$ 的性质, 比如

$$\dim_{\mathbb{Q}} E \text{ 是否有限?}$$

一般的, 假设 K 是 L 的子域, 扩域 L 可以看成 K 向量空间, 数乘就是 K 中元素与 L 中元素在 L 中相乘.

为了方便, 有时我们会用记号

$$L/K$$

表示 L 是 K 的扩域.

由于看着记号 $\dim_K L$ 不爽, 我们改用一个比较简单的记号

$$[L : K] := \dim_K L$$

称为 L/K 的扩张次数.

如果 $[L : K] < \infty$, 称 L 是 K 的有限扩张.

两个有限扩张拼起来是不是有限扩张呢?

就是说, 如果有域扩张

$$K \subseteq L \subseteq E$$

且 $[L : K]$ 和 $[E : L]$ 都有限, 那么

$$[E : K] \text{ 是否依然有限?}$$

如你所料, 答案是肯定的.

引理 34.1. 假设 $E/L, L/K$ 是有限扩张, 则 E/K 也是有限扩张, 并且

$$[E : K] = [E : L][L : K]$$

证明. 这个证明是个体力劳动.

假设 L 作为 K 向量空间有一组基

$$\alpha_1, \cdots, \alpha_n$$

而 E 作为 L 向量空间有一组基

$$\beta_1, \cdots, \beta_m$$

我们断言

$$\alpha_i\beta_j, 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m$$

是 K 向量空间 E 的一组基.

实际上, 假设 K 线性组合

$$\sum_{i,j} \lambda_{ij}\alpha_i\beta_j = 0$$

其中 $\lambda_{ij} \in K$. 可以写成

$$\beta_1, \cdots, \beta_m$$

的 L 线性组合

$$\sum_j (\sum_i \lambda_{ij}\alpha_i)\beta_j = 0$$

由于 $\beta_1, \cdots, \beta_m$ 是 L 线性无关, 因此对任意固定的 $1 \leqslant j \leqslant m$, 有

$$\sum_{i=1}^{n} \lambda_{ij}\alpha_i = 0$$

再由 $\alpha_1, \cdots, \alpha_n$ 的 K 线性无关性得

$$\lambda_{ij} = 0, \forall i, j.$$

这说明

$$\alpha_i\beta_j, 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m$$

是 K 线性无关的, 另一方面任意 E 中元素都能写成 $\beta_j, 1 \leqslant j \leqslant m$ 的 L 线性组合, 而这个线性组合的系数 (在 L 中) 又都能写成 $\alpha_1, \cdots, \alpha_n$ 的 K 线性组合, 因此, E 中所有元素都能写成

$$\alpha_i\beta_j, 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m$$

的 K 线性组合.

结合起来

$$\alpha_i\beta_j, 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m$$

是 K 向量空间 E 的一组基, 因此

$$[E : K] = mn = [E : L][L : K].$$

2 有限扩张与代数扩张

如果 L/K 为有限扩张, 设 $[L : K] = n$.

对任意 $\alpha \in L$, 有

$$1, \alpha, \cdots, \alpha^n$$

必然 K 线性相关, 从而是 K 上的代数元.

即 L 中所有元素都是 K 上的代数元.

域扩张 E/K 中,如果 E 中所有元素都是 K 上的代数元,我们称 E 为 K 的代数扩张. 如果 E/K 不是代数扩张,即 E 中存在 K 上的超越元,则称 E/K 为超越扩张.

我们已经看到

命题 34.2. 有限扩张是代数扩张.

但是,还是有个问题,前面多项式的分裂域

$$\mathbb{Q}(\xi_1,\cdots,\xi_r)$$

是不是 $\mathbb{Q}$ 上的有限扩张或者代数扩张?

这里每个 ξ_i 都是 $\mathbb{Q}$ 上的代数元,一下子扩张这么多代数元,还是代数扩张或者有限扩张么?

可以抽象成下面这个问题

问题 10. 假设 L 是 K 的扩域,而

$$\alpha_1,\cdots,\alpha_r\in L$$

是 K 上的代数元. 试问: $K(\alpha_1,\cdots,\alpha_r)$ 是否为 K 上的有限扩张? 代数扩张?

如果 $r=1$,这实际上就是代数元对应的单扩张,由上期,我们知道其扩张的次数就是对应的极小多项式的次数,必为有限扩张.

$r>1$ 时,看上去比较麻烦,如果你注意到

$$K(\alpha_1,\cdots,\alpha_r)=K(\alpha_1,\cdots,\alpha_{r-1})(\alpha_r)$$

问题就简单了. 实际上右边包含

$$K\text{ 和 }\alpha_1,\cdots,\alpha_r$$

因此

$$K(\alpha_1,\cdots,\alpha_r)\subseteq K(\alpha_1,\cdots,\alpha_{r-1})(\alpha_r)$$

反过来,左边也包含

$$K(\alpha_1,\cdots,\alpha_{r-1})\text{ 和 }\alpha_r$$

所以

$$K(\alpha_1,\cdots,\alpha_{r-1})(\alpha_r)\subseteq K(\alpha_1,\cdots,\alpha_r)$$

所以

$$K(\alpha_1,\cdots,\alpha_r)=K(\alpha_1,\cdots,\alpha_{r-1})(\alpha_r)$$

现在,α_r 是 K 上的代数元,它必然也是 $K(\alpha_1,\cdots,\alpha_{r-1})$ 上的代数元. 所以

$$[K(\alpha_1,\cdots,\alpha_r):K(\alpha_1,\cdots,\alpha_{r-1})]<\infty$$

利用数学归纳法,我们可以愉快的假设

$$[K(\alpha_1,\cdots,\alpha_{r-1}):K]<\infty$$

这样就得到下面的命题

命题 34.3. 假设 L 是 K 的扩域,而

$$\alpha_1,\cdots,\alpha_r\in L$$

是 K 上的代数元. 那么

$$K(\alpha_1,\cdots,\alpha_r)\text{ 是 }K\text{ 上的有限扩张.}$$

也是代数扩张. 特别的,K 上的代数元的和、差、积、取逆依然是 K 上的代数元.

实际上所有的有限扩张都是上面这种形式.

如果 L/K 是有限扩张,而

$$\alpha_1,\cdots,\alpha_r$$

为 L 作为 K 向量空间的一组基,显然

$$\alpha_1,\cdots,\alpha_r$$

都是 K 上的代数元且

$$L\subseteq K(\alpha_1,\cdots,\alpha_r)\subseteq L$$

所以

$$L=K(\alpha_1,\cdots,\alpha_r)$$

跟命题34.3合并得到下面定理

定理 34.4. 假设 L/K 是域扩张. 那么 L/K 是有限扩张当且仅当存在 K 上的代数元

$$\alpha_1,\cdots,\alpha_r\in L$$

使得

$$L=K(\alpha_1,\cdots,\alpha_r)$$

需要指出的是,并不是所有的代数扩张都是有限扩张,比如把 $\mathbb{C}$ 中在 $\mathbb{Q}$ 上的代数元都拿出来,构成集合 $\mathcal{A}$,由于代数元的和、差、积、取逆还是代数元,所以 $\mathcal{A}$ 是域且包含 $\mathbb{Q}$,它显然是 $\mathbb{Q}$ 上代数扩张,但不是 $\mathbb{Q}$ 上的有限扩张!

扩张次数的计算

上面的讨论非常有助于我们计算有限扩张的扩张次数,比如上期的问题

$$[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=?$$

令 $\alpha=\sqrt{2}+\sqrt{3}$, 上期已经知道

$$\sqrt{2}=\frac{1}{2}(\alpha-1/\alpha)\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$$
$$\sqrt{3}=\frac{1}{2}(\alpha+1/\alpha)\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$$

所以

$$\mathbb{Q}(\sqrt{2},\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2}+\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$$

从而

$$\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$$

这样可以转化为两个域扩张

$$\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{2})\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$$

现在

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]$$
$$=[\mathbb{Q}(\sqrt{2})(\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$$

这是因为 $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$, 所以

$$[\mathbb{Q}(\sqrt{2})(\sqrt{3}):\mathbb{Q}(\sqrt{2})]>1$$

但 $(\sqrt{3})^2\in\mathbb{Q}(\sqrt{2})$, 所以

$$[\mathbb{Q}(\sqrt{2})(\sqrt{3}):\mathbb{Q}(\sqrt{2})]\leqslant 2$$

这样就得到

$$\begin{aligned}&[\mathbb{Q}(\sqrt{2})(\sqrt{3}):\mathbb{Q}]\\=&[\mathbb{Q}(\sqrt{2})(\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]\\=&2\times 2=4\end{aligned}$$

所以

$$[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=4.$$

4

代数扩张链

假设有域的扩张链

$$K\subseteq L\subseteq E$$

当 $L/K, E/L$ 都是有限扩张的时候, 前面知道 E/K 也是有限扩张. 其实上反过来也对, 如果 E/K 是有限扩张, L/K 和 E/L 必然也是有限扩张.

代数扩张是否具有同样的性质?

答案再一次是: YES!

定理 34.5. 假设有域的扩张链

$$K\subseteq L\subseteq E$$

那么 E/K 是代数扩张当且仅当 E/L 和 L/K 都是代数扩张.

证明. 假设 E/K 是代数扩张.

对任意 $\alpha\in E$, 存在非零多项式 $f(x)\in K[x]$ 使得 $f(\alpha)=0$, 但 $f(x)$ 同时也是 $L[x]$ 中多项式, 所以 α 也是 L 上的代数元, 因此 E/L 是代数扩张.

另一方面 $L\subseteq E$, 此时 L 中元素也都是 K 上的代数元, 所以 L/K 也是代数扩张.

反过来, 假设 E/L 和 L/K 都是代数扩张. 我们需要证明 E 中的任意元素 α 都是 K 上的代数元.

由于 E/L 是代数扩张, 因此 α 是 L 上的代数元, 存在非零多项式

$$f(x)=a_0+a_1x+\cdots+a_nx^n\in L[x]$$

使得 $f(\alpha)=0$, 现在

$$a_0,a_1,\cdots,a_n\in L$$

这样一来 α 实际上是

$$K(a_0,a_1,\cdots,a_n)$$

上的代数元, 所以

$$[K(a_0,\cdots,a_n)(\alpha):K(a_0,\cdots,a_n)]<\infty$$

由于 L/K 也是代数扩张, 所以

$$a_0,\cdots,a_n$$

都是 K 上的代数元. 由命题34.3

$$K(a_0,\cdots,a_n)$$

是 K 上有限扩张, 合起来得到

$$K(a_0,\cdots,a_n)(\alpha)$$

是 K 上的有限扩张, 从而是代数扩张, 特别的 α 是 K 上的代数元.

所以 E/K 是代数扩张!

35 分裂域

本期导言

这一期, 咱们集中精力研究下分裂域.

1 多项式的分裂域

前面已经讨论过, 如果有理多项式 $f(x)$ 在复数域内所有根为

$$\xi_1, \cdots, \xi_r$$

那么域

$$\mathbb{Q}(\xi_1, \cdots, \xi_r)$$

称为 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域.

很多数学工作者比较作, 如果一件事情只能在有理数上做, 其他域上不能做, 总会让人如梗在喉!

也就是说, 现在给一个任意域 K 上的多项式 $f(x)$, 你给我找个分裂域看看?

这时候存在的第一个困难是: 没有了复数域, 怎么去找 K 的扩域, 使得 $f(x)$ 可以在这个扩域上分解成一次因式的乘积?

至少可以问: 是否存在一个 K 扩域, 使得 $f(x)$ 在这个扩域里至少有一个根?

好在这个问题简单一点.

引理 35.1. 假设 K 是域, 而 $f(x)$ 是 K 上的正次数多项式. 那么存在 K 的单扩张 $K(\alpha)$ 使得

1. α 是 $f(x)$ 的根, 即 $f(\alpha)=0$.
2. $[K(\alpha):K] \leqslant \deg f(x)$.

证明. 取 $f(x)$ 的不可约因式 $p(x)$, 考虑

$$L = K[x]/(p(x))$$

由于 $p(x)$ 不可约, 因此 $(p(x))$ 是 $K[x]$ 的极大主理想, 又因为 $K[x]$ 的理想都是主理想, 因此 $(p(x))$ 是 $K[x]$ 的极大理想. 所以

$$L = K[x]/(p(x)) \text{ 是域}$$

记

$$I = (p(x))$$

现在我们将 K 看作 L 的子域, 将

$$k \text{ 与 } k+I \text{ 等同看待}$$

令 $\alpha = x + I$

由于 $p(x) \mid f(x)$, 所以 $f(x) \in I$, 从而

$$f(\alpha) = f(x+I) = f(x) + I = I$$

为 L 中零元, 所以 α 是 $f(x)$ 在 L 中的根, 另外, L 中的元素都形如

$$g(x) + I = g(\alpha)$$

因此

$$L = K(\alpha)$$

最后

$$\begin{aligned}[K(\alpha):K] &= [K[x]/(p(x)):K] \\ &= \deg p(x) \leqslant \deg f(x)\end{aligned}$$

有这个引理, 就能给 $f(x)$ 造 "分裂域" 了.

定理 35.2. 假设 $f(x)$ 为域 K 上的 $n>0$ 次多项式. 那么, 存在 K 的扩域 E 满足

1. $f(x)$ 在 $E[x]$ 中分解成一次因式乘积
$$f(x) = a(x-\xi_1)\cdots(x-\xi_n)$$
其中 $a \in K$ 为 $f(x)$ 的首项系数.
2. $E = K(\xi_1, \cdots, \xi_n)$
3. $[E:K] \leqslant n!$

证明. 对 n 用数学归纳法.

$n=1$. 此时

$$f(x) = ax - b, \xi_1 = b/a \in K$$

取 $E = K$ 即可.

现假设 $n>1$. 由上面的引理, 存在 K 的单扩张

$$K(\alpha)$$

使得

$$f(\alpha) = 0, [K(\alpha):K] \leqslant \deg f(x) = n$$

令 $L = K(\alpha)$, 则 $f(x)$ 在 L 中可分解为

$$f(x) = (x-\alpha)g(x)$$

其中 $g(x) \in L[x]$ 且 $\deg g(x) = n-1$.

由归纳假设存在 L 的扩域 E 使得

1. $g(x)$ 在 $E[x]$ 中分解为
$$a(x-\xi_1)\cdots(x-\xi_{n-1})$$
2. $E = L(\xi_1, \cdots, \xi_{n-1})$
3. $[E:L] \leqslant (n-1)!$

合并在一起, 在 $E[x]$ 中

$$\begin{aligned}f(x) &= (x-\alpha)g(x) \\ &= a(x-\xi_1)\cdots(x-\xi_{n-1})(x-\alpha)\end{aligned}$$

可分解为一次因式乘积.

$$\begin{aligned} E &= L(\xi_1, \cdots, \xi_{n-1}) \\ &= K(\alpha)(\xi_1, \cdots, \xi_{n-1}) \\ &= K(\xi_1, \cdots, \xi_{n-1}, \alpha) \end{aligned}$$

另外

$$\begin{aligned} [E:K] &= [E:L][L:K] \\ &\leqslant (n-1)! \times n = n! \end{aligned}$$

令 $\xi_n = \alpha$ 即可完成证明.

满足定理35.2条件的 E 称为 $f(x)$ 在 K 上的一个分裂域.

值得注意的是,对于 K 和 E 的任何中间域 $L, f(x)$ 也是 $L[x]$ 中多项式,按照定义 E 也是 $f(x)$ 在 L 上的分裂域.

2 分裂域的唯一性

当我们放弃有理数的特殊情况来挑战一般域的情况时,我们不得不面临一个问题:

$$\text{分裂域 } E \text{ 的选择不是唯一的!}$$

随之而来的是,这时候 $f(x)$ 的 Galois 群如果定义成

$$\mathrm{Gal}(f) = \mathrm{Aut}_K E$$

还是不是良定义的,会不会随着 E 的选取的不同而使得 $\mathrm{Aut}_K E$ 变化很大? 会不会不同构?

这一小节,咱们就来了断这个后顾之忧.

这里我们需要一个技术性的引理.

引理 35.3. 假设

$$\sigma : K_1 \longrightarrow K_2$$

是域同构,对任意 $f(x) \in K_1[x]$,用

$$\sigma f(x) \in K_2(x)$$

表示将 $f(x)$ 的所有系数用 σ 作用后得到的多项式. 如果 $K_1(\alpha)$ 和 $K_2(\beta)$ 分别是 K_1 和 K_2 的单扩张,使得它们的极小多项式分别是 $p(x)$ 和 $\sigma p(x)$,那么存在域同构

$$\theta : K_1(\alpha) \longrightarrow K_2(\beta)$$

使得

$$\theta|_{K_1} = \sigma, \theta(\alpha) = \beta$$

证明. 令 θ 是下面几个域同构的复合.

$$K_1(\alpha) \longrightarrow K_1[x]/(p(x))$$

$$\sigma : K_1[x]/(p(x)) \longrightarrow K_2[x]/(\sigma p(x))$$

$$K_2[x]/(\sigma p(x)) \longrightarrow K_2(\beta)$$

下点苦力验证即可.

上面引理中 $\theta|_{K_1} = \sigma$ 也可以用下面的交换图来描述.

$$\begin{array}{ccc} K_1 & \hookrightarrow & K_1(\alpha) \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\theta} \\ K_2 & \hookrightarrow & K_2(\beta) \end{array}$$

其中水平方向是域之间的嵌入映射.

定理 35.4. 假设

$$\sigma : K_1 \longrightarrow K_2$$

是域同构,E_1 是 $K_1[x]$ 中多项式 $f(x)$ 在 K_1 上的一个分裂域,而 E_2 是 $\sigma f(x)$ 在 K_2 上的一个分裂域,那么存在域同构

$$\phi : E_1 \longrightarrow E_2$$

使得 $\phi|_{K_1} = \sigma$,用交换图表示

$$\begin{array}{ccc} K_1 & \hookrightarrow & E_1 \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\phi} \\ K_2 & \hookrightarrow & E_2 \end{array}$$

证明. 对 $[E_1 : K_1]$ 利用数学归纳法.

如果 $[E_1 : K_1] = 1$,即 $E_1 = K_1$,此时 $f(x)$ 在 $K_1[x]$ 中可以写成一次因式的乘积

$$f(x) = a(x - k_1) \cdots (x - k_n)$$

此时

$$\sigma f(x) = \sigma(a)(x - \sigma(k_1)) \cdots (x - \sigma(k_n))$$

在 $K_2[x]$ 上可以分解成一次因式的乘积,因此 $\sigma f(x)$ 在 K_2 上的分裂域只能是 K_2. 所以 $E_2 = K_2$. 这种情形下只需要取 $\phi = \sigma$ 即可.

现在假设 $[E_1 : K_1] > 1$.

此时 $f(x)$ 在 E_1 的根不可能全都在 K_1 中.

令 $\alpha \in E_1 \backslash K_1$ 是 $f(x)$ 的根.

假设 $p(x) \in K_1[x]$ 为 α 的极小多项式,则 $p(x) \mid f(x)$,从而 $\sigma p(x) \mid \sigma f(x)$.

作为 $\sigma f(x)$ 的因式,$\sigma p(x)$ 在 E_2 中也能分解成一次因式的乘积,特别的存在根 β.

由于 $\sigma p(x)$ 跟 $p(x)$ 一样不可约,因此它是 β 的极小多项式.

目前我们面临的情况: α 和 β 的极小多项式分别是 $p(x)$ 和 $\sigma p(x)$,由引理35.3,域同构

$$\theta : K_1(\alpha) \longrightarrow K_2(\beta)$$

和交换图

$$\begin{array}{ccc} K_1 & \hookrightarrow & K_1(\alpha) \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\theta} \\ K_2 & \hookrightarrow & K_2(\beta) \end{array}$$

现在我们拥有的情况

1. 域同构 $\theta : K_1(\alpha) \longrightarrow K_2(\beta)$
2. $\theta f(x) = \sigma f(x)$
3. E_1 是 $f(x)$ 在 $K_1(\alpha)$ 上分裂域.
4. E_2 是 $\theta f(x)$ 在 $K_2(\beta)$ 上分裂域.
5. $[E_1 : K_1(\alpha)] < [E_1 : K_1]$

由归纳假设, 存在域同构

$$\phi : E_1 \longrightarrow E_2$$

使得下图交换

$$\begin{array}{ccc} K_1(\alpha) & \hookrightarrow & E_1 \\ {\scriptstyle\theta}\downarrow & & \downarrow{\scriptstyle\phi} \\ K_2(\beta) & \hookrightarrow & E_2 \end{array}$$

把两个交换图合并一处

$$\begin{array}{ccccc} K_1 & \hookrightarrow & K_1(\alpha) & \hookrightarrow & E_1 \\ {\scriptstyle\sigma}\downarrow & & {\scriptstyle\theta}\downarrow & & \downarrow{\scriptstyle\phi} \\ K_2 & \hookrightarrow & K_2(\beta) & \hookrightarrow & E_2 \end{array}$$

定理得证.

在上面的定理中, 取 $K_1 = K_2$ 和 $\sigma = \mathrm{id}$, 可得分裂域的唯一性.

推论 35.5. *假设 E_1 和 E_2 是 $K[x]$ 中多项式 $f(x)$ 在 K 上的分裂域, 则存在域同构*

$$\phi : E_1 \longrightarrow E_2$$

使得 $\phi|_K = \mathrm{id}$, 此时

$$\mathrm{Aut}_K E_1 \longrightarrow \mathrm{Aut}_K E_2$$

$\rho \mapsto \phi\rho\phi^{-1}$ *为群同构.*

36 有限域

本期导言

咱们通常见到的域都是 $\mathbb{C}, \mathbb{Q}$ 等等, 很少见到有限个元素的域, 到目前为止, 我们见过的有限域好像只有

$$\mathbb{Z}_p \ (p \text{ 为素数}).$$

实际上还有很多有限域, 它们在编码和密码理论中发挥着非常重要的作用. 比如前面我们讲过一句的 AES 加密方法就是现在非常主流的数据加密方法, 它的原理是考虑有限域中的运算, 这个后面有空再详细聊.

这一期, 咱们讨论有限域的一般理论.

1 域的特征 (characteristic)

想想 $\mathbb{C}$, $\mathbb{Q}$ 等域, 它们与 $\mathbb{Z}_p$ (p 为素数) 有什么区别呢?

有一个重要的区别就是, 在 $\mathbb{C}$ 中, 一个非零的元素 a, 任意多个 a 加起来都不会是零, 而 $\mathbb{Z}_p$ 就比较坑, 任意一个非零元 a, p 个 a 加起来

$$a + \cdots + a = (1 + \cdots + 1)a = 0a = 0$$

一般的, 在域 K 中, 单位元为 1, 如果任意多个 1 的和都不为零, 则称 K 的特征为 0.

反之, 如果存在正整数 $n > 0$, 使得 n 个 1 的和为 0, 令

$$p = \min\{n \mid n \text{ 个 } 1 \text{ 的和为 } 0\}$$

称 K 的特征为 p.

此时 p 必为素数, 否则 $p = mn$ 且 $m, n < p$

$$\underbrace{1 + \cdots + 1}_{p} = \underbrace{(1 + \cdots + 1)}_{m}\underbrace{(1 + \cdots + 1)}_{n}$$

由 p 的最小性, 右边 m 个 1 的和, n 个 1 的和都不为零, 因此它们的乘积亦不为零, 与左边为零矛盾!

同时, 对任意 $a \in K$, 有

$$\underbrace{a + \cdots + a}_{p} = \underbrace{(1 + \cdots + 1)}_{p}a = 0a = 0$$

K 的特征记为 $\mathrm{char}\, K$.

例如: $\mathrm{char}\, \mathbb{Q} = 0, \mathrm{char}\, \mathbb{Z}_p = p$

由域的特征的定义可以看出,它只跟域中单位元 1 的性质有关,因此一个域和它的子域、扩域的特征相同!

2 最小子域:素域

对每个域 K 来说,它都有一个最小的子域,称为它的素域

考虑环同态

$$\eta : \mathbb{Z} \longrightarrow K$$

将 $\mathbb{Z}$ 中的 n 映为 K 中的 $n1$,即 $|n|$ 个 1 的和 $(n > 0)$ 或者和的负元 $(n \leqslant 0)$.

当 $\operatorname{char} K = 0$ 时,η 是单射,从而可以扩展成为 $\mathbb{Q}$ 到 K 的环的单同态,仍记为 η

$$\eta : \mathbb{Q} \longrightarrow K$$

它的像 $\eta(\mathbb{Q})$ 是与 $\mathbb{Q}$ 同构的域,它是 K 的最小子域 (很显然,K 的任意子域都包含 0 和 1,从而包含 $\eta(\mathbb{Z})$,从而包含 $\eta(\mathbb{Q})$).

因此 $\operatorname{char} K = 0$ 时,K 的素域与 $\mathbb{Q}$ 同构.

当 $\operatorname{char} K = p > 0$ 时呢? 此时

$$\eta : \mathbb{Z} \longrightarrow K$$

不是单射,其 Kernel 恰为

$$\operatorname{Ker} \eta = p\mathbb{Z}$$

由环同态基本定理第一同构定理,

$$\mathbb{Z}/p\mathbb{Z} \longrightarrow \operatorname{Im} \eta$$

为环同构,这里左边为 $\mathbb{Z}_p$ 是域,因此 $\operatorname{Im} \eta$ 也是域,从而是 K 的子域,但任何 K 的子域都含 0 和 1,从而含 $\eta(\mathbb{Z}) = \operatorname{Im} \eta$.

因此这种情况下 K 的素域与 $\mathbb{Z}_p$ 同构.

3 有限域的存在性

由域的特征的定义,特征为 0 的域的素域与 $\mathbb{Q}$ 同构,因此有无限多个元素.

所以有限域的特征必定不为 0.

现在假设 E 是有限域,特征 $\operatorname{char} E = p$,并假设其素域为 K.

上面已经知道 K 与 $\mathbb{Z}_p$ 同构,有 p 个元素.

由于 E 是有限域,作为 K 的扩域,其扩张次数必定有限,假设

$$[E : K] = n$$

那么 E 是 n 维 K 向量空间,作为向量空间与 K^n 同构,共有

$$|K|^n = p^n$$

个元素. 因此有限域的元素个数只能是素数的方幂,而这个素数正好就是这个域的特征. 那给定一个 $n > 0, p^n$ 个元素的域是不是真的存在呢?

定理 36.1. 假设 p 为素数,$n > 0$ 为正整数,那么

$$f(x) = x^{p^n} - x$$

在 $\mathbb{Z}_p$ 上的分裂域 E 为 p^n 个元素的域且每个 p^n 个元素的域都与 E 同构.

证明. 为记号简单,记 $q = p^n$. 由于

$$f'(x) = qx^{q-1} - 1 = -1$$

注意这里 $f(x)$ 是 $\mathbb{Z}_p[x]$ 中多项式,因此 x^{q-1} 的系数 $q = p^n$ 在 $\mathbb{Z}_p$ 中为 0.

由此

$$(f(x), f'(x)) = 1$$

所以 $f(x)$ 在 E 中没有重根,共有 q 个互不相同的根. 记

$$S := \{f(x) \text{ 在 } E \text{ 中的 } q \text{ 个根 }\}$$

由于 $\mathbb{Z}_p$ 中的元素 a 都满足

$$a^p = a$$

从而

$$a^q = ((a^p)^p)^{\cdots p} = a$$

所以 $\mathbb{Z}_p$ 中元素都是 $f(x)$ 在 E 中的根,因此

$$\mathbb{Z}_p \subseteq S.$$

现在任取 $\alpha, \beta \in S$,即

$$\alpha^q = \alpha, \beta^q = \beta$$

则

$$\begin{aligned}(\alpha - \beta)^q &= \alpha^q + (-\beta)^q \\ &= \alpha + (-1)^q \beta^q \\ &= \alpha - \beta\end{aligned}$$

这里二项式展开的中间项的系数都被 p 整除,在 $\mathbb{Z}_p$ 中为零. 因此

$$\alpha - \beta \in S$$

如果 $\beta \neq 0$,则

$$(\alpha/\beta)^q = \alpha^q/\beta^q = \alpha/\beta$$

所以 $\alpha/\beta \in S$.

由此 S 在加法下是 E 的子群,去掉零后在乘法下是 E^* 的子群,即 S 是 E 的子域.

记 $S=\{\alpha_1,\cdots,\alpha_q\}$

按照分裂域的定义

$$E=\mathbb{Z}_p(\alpha_1,\cdots,\alpha_q)$$

由于 S 本身也包含 $\mathbb{Z}_p$, 所以

$$\mathbb{Z}_p(\alpha_1,\cdots,\alpha_q)\subseteq S\subseteq E$$

可得 $E=S$. 因此 E 恰有 q 个元素.

现在假设 L 是另一个 q 个元素的域, 其素域 K 必与 $\mathbb{Z}_p$ 同构.

L^* 中共有 $q-1$ 个元素, 因此

$$\alpha^{q-1}=1,\forall\alpha\in L^*$$

加上零的特点, 合并起来

$$\alpha^q=\alpha,\forall\alpha\in L$$

所以 L 中的元素恰为 $f(x)$ 在 L 中的全部根, 这样一来

$$L=K(L)$$

为 $f(x)$ 在 K 上的分裂域.

值得注意的是, 这里域同构

$$\sigma:K\longrightarrow\mathbb{Z}_p$$

将 K 中的 ±1 映为 $\mathbb{Z}_p$ 中的 ±1, 因此这个同构将 $K[x]$ 中的

$$x^q-x$$

对应到 $\mathbb{Z}_p[x]$ 中的 x^q-x.

由上期分裂域的性质, 存在域同构

$$\phi:E\longrightarrow L$$

使得 $\phi|_K=\sigma$

用类似的办法, 可以证明下面这个定理

定理 36.2. *K 是一个 q 元域, $m>0$ 是整数, 那么存在 K 的扩域 L 使得 $[L:K]=m$. 此时*

$$|L|=|K|^m=q^m.$$

证明. 考虑

$$x^{q^m}-x$$

在 K 上的分裂域, 剩余的证明与定理 36.1的证明类似.

有限域的结构

给定一个 p^n 个元素的域, 它包含哪些子域? 比如一个 3^6 元域有没有 3^2 元子域? 如果有, 会有几个?

16 元域是否有 8 元子域?

定理 36.3. *假设 E 是一个 p^n 个元素的域, p 为素数. E 存在 p^m 个元素的子域当且仅当 $m\mid n$.*

当 $m\mid n$ 时, E 有唯一的 p^m 元子域.

证明. 假设 E 的素域为 K, K 与 $\mathbb{Z}_p$ 同构.

$\Rightarrow$ 若 L 是 E 的 p^m 个元素的子域, 那么

$$K\subseteq L\subseteq E$$

由于

$$|L|=p^m=|K|^m$$

所以 $[L:K]=m$. 假设 $[E:L]=r$, 则

$$n=[E:K]=[E:L][L:K]=mr$$

所以 $m\mid n$.

$\Leftarrow$ 现在假设 $m\mid n, n=mr$, 则

$$\begin{aligned}p^n-1&=(p^m)^r-1\\&=(p^m-1)((p^m)^{r-1}+\cdots+p^m+1)\end{aligned}$$

所以 $p^m-1\mid p^n-1$, 不妨设

$$p^n-1=(p^m-1)s$$

再次利用等式

$$t^s-1=(t-1)(t^{s-1}+t^{s-2}+\cdots+1)$$

得

$$x^{p^m}-x\text{ 整除 }x^{p^n}-x$$

现在 E 是

$$x^{p^n}-x$$

在 K 上的分裂域, 必然包含一个

$$x^{p^m}-x$$

在 K 上的分裂域 L, 这个 L 的元素个数恰为 p^m, 其元素恰为

$$x^{p^m}-x$$

在 E 中所有的根.

如果 M 是 E 的另一个 p^m 元素的子域, 那么 M 中的元素 α 都满足

$$\alpha^{p^m}=\alpha$$

为

$$x^{p^m}-x$$

在 E 中的根, 所以

$$M\subseteq L$$

由于两边元素个数相同, 所以 $M=L$, 也就是说 L 是 E 的唯一 p^m 元子域.

这个定理告诉我们一个 p^n 元域的子域情况完全由 n 的因子确定!

现在我们可以回答前面的问题了, 由于

$$2 \mid 6$$

因此 3^6 元域包含一个 3^2 元子域.

$$16 = 2^4, 8 = 2^3, 3 \nmid 4$$

因此 16 元域没有 8 元子域.

$32 = 2^5$, 由于 5 的因子只有 5 和 1, 因此 32 元域只有两个子域, 一个是它自身, 另一个是它的素域, 而 16 元域反而有 3 个子域, 分别有 $16 = 2^4, 4 = 2^2$, $2 = 2^1$ 个元素.

有限域的乘法群是循环群

最后来看有限域的一个重要特点.

定理 36.4. 假设 E 是有限域, 那么 E^* 在乘法下是循环群, 特别的有限域之间的域扩张都是单扩张.

在证明之前, 需要补一个交换群的性质.

引理 36.5. 假设 G 是有限交换群, m 是 G 中元素的最大阶数, 那么

$$o(a) \mid m, \forall a \in G$$

证明. 假设 $o(b) = m$.

如果存在 $a \in G$ 使得

$$o(a) = n \nmid m$$

那么必存在 n 的素因子 p 使得

$$n = p^i n_1, m = p^j m_1 \text{ 且 } j < i$$

$$p \nmid n_1, p \nmid m_1$$

如此一来

$$o(b^{p^i}) = \frac{m}{(m, p^i)} = m_1$$

$$o(a^{n_1}) = \frac{n}{(n, n_1)} = p^i$$

由于 G 是交换群, 因此上面这两个元素相互交换, 而它们的阶彼此互素, 因此

$$o(b^{p^i} a^{n_1}) = m_1 p^i > m_1 p^j = m$$

导致矛盾!

定理*36.4*的证明. 假设 E 是 q 元域, 我们知道

$$\alpha^{q-1} = 1, \forall \alpha \in E^*$$

令

$$m = \max\{o(\alpha) \mid \alpha \in E^*\}$$

因此 $m \leqslant q - 1$.

另一方面, 由于 E^* 是交换群, 由上面的引理, E^* 所有元素的阶都整除 m, 从而

$$\alpha^m = 1, \forall \alpha \in E^*$$

即所有 E^* 中元素都是多项式

$$x^m - 1$$

在 E 中的根, 但 $x^m - 1$ 在 E 中至多有 m 个根, 因此

$$q - 1 = |E^*| \leqslant m$$

所以 $m = q - 1$, 令 $\alpha \in E^*$ 中满足

$$o(\alpha) = m = q - 1$$

的元素, 则由 α 生成的循环群 $\langle \alpha \rangle$ 有 $q-1$ 个元素, 只能是整个 E^*. 所以 $E^* = \langle \alpha \rangle$ 是循环群.

如果 L 是 E 的子域, 显然

$$E \subseteq L(\alpha) \subseteq E$$

所以 E/L 是单扩张.