

歸去來兮辭

歸去來兮田園將蕪胡不歸既自以心為形役
奚惆悵而獨悲悟已往之不諫知來者之可追實
迷途其未遠覺今是而昨非舟搖以輕颺風飄
而吹衣問征夫以前路恨晨光之熹微乃瞻衡宇載
欣載奔僮僕歡迎稚子候門三迳就荒松菊猶存攜
劣入室有酒盈樽引壺觴以自酌眄庭柯以怡顏倚南
窓以寄傲審容膝之易安園日涉以成趣門雖設而長
關策扶老以流憩時矯首而遐觀雲無心而出岫鳥倦
飛而知還景翳翳以將入俯孤松而盤桓歸去來兮且
息交以請絕遊世與我而相違復駕言兮焉求悅親戚
之情話樂琴書以消憂農人告余以春及將有事於
西疇或命中車或棹孤舟既窈窕以尋壑二嶠嶮而
經丘木欣欣以向榮泉涓涓而始流善萬物之得時
感吾生之行休已矣乎寓形寓內復幾時曷不委心任去
留胡為乎遑兮欲何之富貴非吾願帝鄉不可期懷
良辰以孤往或植杖而耘矧登東皋以舒嘯臨清流而
賦詩聊乘化以歸盡樂夫天命復奚疑

辛亥九月十一日橫塘舟中書 徵明 昔年八十二

群与 Galois 理论 于品

2023 年秋季学期清华大学数学系课程讲义

Faire de l'Algèbre, c'est essentiellement calculer. — Algèbre, N. Bourbaki

目录

第 1 章	域扩张与经典几何问题	2
1.1	不超过四次的代数方程的解	2
1.2	域与域的扩张	4
1.3	三等分已知角	7
第 2 章	群和环的定义	11
2.1	群的定义	11
2.2	正规子群与商群	15
2.3	环的定义	18
2.4	对称群 S_n	20
第 3 章	群与群作用	27
3.1	群的作用	27
3.2	群作用的应用举例	30
3.2.1	Burnside 引理	30
3.2.2	S_6 非共轭的自同构	31
3.2.3	Sylow 定理	33
3.2.4	S_6 非共轭自同构另一个构造	36
第 4 章	群的结构与构造	38
4.1	半直积	38
4.2	有限生成交换群的分类	43
4.3	滤链	47
4.4	可解群	49
第 5 章	环与模	55
5.1	与环相关的基本概念	55
5.2	与整除性相关的几类特殊的环	60
5.3	主理想整环上的有限生成模	68
第 6 章	关于多项式的补充	77
6.1	多项式的导数	77
6.2	解式与判别式	77
6.3	对称多项式	80
第 7 章	域的扩张	83

7.1	代数扩张	83
7.2	代数闭包	86
7.2.1	代数闭包的存在性	86
7.2.2	关于域同态扩张的技术性引理	87
7.3	分裂域与正规扩张	90
7.4	可分扩张	95
7.4.1	单扩张与可分扩张	101
7.4.2	迹与范数映射	102
7.5	Galois 理论	103
7.5.1	Galois 对应	103
7.5.2	Galois 群在根上的作用	107
7.5.3	有限域	110
7.5.4	分圆扩张	111
7.5.5	循环扩张	113
7.5.6	尺规作图	116
7.5.7	多项式的根式解	119
7.6	$\text{mod } p$ 的理论	122
7.6.1	环的整扩张	123
7.6.2	数域中的整元素	125
7.6.3	素理想与 Galois 群	129
附录 A	作业题合集	136
A.1	第一次作业	136
A.2	第二次作业	141
A.3	第三次作业	144
A.4	第四次作业	147
A.5	第五次作业	150
A.6	第六次作业	154
A.7	第七次作业	159
A.8	第八次作业	163
附录 B	有关集合的回顾	168
B.1	商集	168
B.2	偏序关系与 Zorn 引理	169

序言

每一门合格的数学课程，总要交代课题背后的动机与核心的概念，并通过讲解真正重要的例子使得参加学习者掌握基本的思考方式和计算技术。在此之上，最重要的一点应该是展现该课程与其他学科的关联，特别是与当下研究前沿的内在逻辑。

2023 年秋，由于教学任务的特殊情况，我第一次教代数的课程。我的研究方向与前沿的代数几何、数论或者表示论少有交集，甚至极少用到很代数的工具，限于学识，在教学中难以展现这门古老又生气勃勃的课程在最新研究中的影踪，这是最大的遗憾与无奈。所以，我只能以学习者的视角而不是研究者的高度进入课程，期待能和同学分享自己的理解，也想传达那种非凡体验。每次备课或者准备习题，好似再次感受了大学第一次读 Galois 理论的时光，真实时空之外的各种代数结构搭起了新天地，这里晶莹剔透不染尘埃，提笔缓书便可驱使万物，真可挟飞仙以遨游，抱明月而长终。

这门课的主要任务是理解群的作用与 Galois 理论。群的作用更是贯穿始终，所以讲义也用了最多的笔墨。大体来说，通过十五周的课程与八次作业，我们基本上完成了任务，也有很多的疏漏。关于群作用方面很多具体计算似乎应挪到作业里，详细的讲解剥夺了同学们发现的乐趣。一些承诺要证明的命题，比如利用 Galois 理论研究 Cardano 或 Ferrari 的求根公式、主理想整环上有限生成模分类定理的唯一性部分等，最终由于遗忘没有出现。为了能严格证明 Galois 理论中的诸多经典例子，我们通过引入环、模以及多项式的理论作为辅助但没有把它们作为课程的重点。关于环的理论方面，更合理地处理可能是再用几次课程讲解 Dedekind 整环上分式理想的唯一分解，一方面可以清楚地展现理想这个概念的来龙去脉，另一方面可以对最后关于 Galois 群 $\bmod p$ 理论做自然的铺垫。当然，讲义中还密密麻麻的摆着打印错误。因为是都是去年的事了，我们就暂且这样吧，待下一次开课的时候再做改进。

2024 年元旦

第 1 章 域扩张与经典几何问题

L'Algèbre est généreuse, elle donne souvent plus qu'on ne lui demande.

—Jean le Rond D'Alembert

1.1 不超过四次的代数方程的解

给定二次方程

$$X^2 + aX + b = 0,$$

通过做代换 $X = Y - \frac{a}{2}$ (配方), 我们总可以消去 1 次项, 从而方程变成

$$X^2 + b = 0.$$

此时, 我们可以直接开方来构造方程的解。最终, 我们有求根公式

$$X = \frac{-a \pm \sqrt{a^2 - 4b}}{2}.$$

对于三次方程

$$X^3 + aX^2 + bX + c = 0,$$

通过做代换 $X = Y - \frac{a}{3}$, 我们总可以消去 2 次项, 从而方程变成

$$X^3 + aX + b = 0.$$

这个方程的三个解可以用如下的 Cardano 或者¹Tartaglia 的公式写出:

$$x_k = \omega^k \sqrt[3]{-\frac{b}{2} + \sqrt{\left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2}} + \omega^{2k} \sqrt[3]{-\frac{b}{2} - \sqrt{\left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2}},$$

其中, $k = 0, 1, 2$, $\omega = e^{\frac{2\pi}{3}i}$ 。

注 考虑方程 $X^3 - X - 6 = 0$, 2 是它的根。根据 Cardano 公式, 这个根可以表示为

$$\sqrt[3]{3 + \frac{11}{9}\sqrt{6}} + \sqrt[3]{3 - \frac{11}{9}\sqrt{6}}.$$

由此可见, 求根公式在实际操作时未必好用。

在理解 Galois 理论之前, 对该问题的任何评价都会流于肤浅。然而, 这里有一个便于记忆的方法, 使得我们可以独立推导以上公式: 我们假设 $X = u + v$ 是方程的解, 即用两个变量之和来表示 X 。此时, 方程 $X^3 + aX + b = 0$ 变成

$$u^3 + v^3 + b + (3uv + a)(u + v) = 0.$$

¹ $k = 0$ 的公式应该是 del Ferro 最早发现的。关于三次求根公式的故事曲折精彩, 所以不是我们课程关心的内容。

一个必要条件是

$$\begin{cases} u^3 + v^3 + b = 0, \\ 3uv + a = 0. \end{cases} \quad (1.1)$$

然而，方程(1.2)可以（通过 Vieta 公式）被视作是二次方程

$$\begin{cases} u^3 + v^3 = -b, \\ u^3 \cdot v^3 = -\frac{a^3}{27}. \end{cases} \quad (1.2)$$

的解。据此，我们可以求出解。

四次方程

$$X^4 + aX^3 + bX^2 + cX + d = 0,$$

的求根公式是 Cardan 的学生 Ferrari 发现的，他的想法是凑平方差公式，最后方程可以化为三次方程的求根问题。我们固定一个参数 ξ ，我们要将 $X^4 + aX^3$ 项写成 $X^2 + \frac{a}{2}X + \xi$ 的二次多项式，即

$$X^4 + aX^3 = \left(X^2 + \frac{a}{2}X + \xi\right)^2 - \left(2\xi + \frac{a^2}{4}\right)X^2 - a\xi X - \xi^2.$$

从而，

$$X^4 + aX^3 + bX^2 + cX + d = \left(X^2 + \frac{a}{2}X + \xi\right)^2 - \left[\left(2\xi + \frac{a^2}{4} - b\right)X^2 + (a\xi - c)X + (\xi^2 - d)\right].$$

我们寄希望于中括号一项是完全平方式，即

$$\left(2\xi + \frac{a^2}{4} - b\right)X^2 + (a\xi - c)X + (\xi^2 - d) = (\alpha X + \beta)^2.$$

如果上式成立，通过因式分解，我们就可以解四次方程。上式成立的条件自然是该二次多项式的判别式为 0，即

$$(a\xi - c)^2 - 4\left(2\xi + \frac{a^2}{4} - b\right)(\xi^2 - d) = 0.$$

这是关于 ξ 的三次方程，只要解出这样的 ξ 即可。

对于五次方程，Abel 在 1824 年证明了我们无法用系数通过加减乘除和开 n 次方的运算来表示方程的解，即五次方程没有求根公式。1830 年，Galois 将这项工作推广到了五次以及五次以上的方程并给出了具有求根公式的确切判断方式。我们课程的主旨之一就是理解 Galois 的工作。

1.2 域与域的扩张

定义 1.1

给定非空集合 K 。如果 K 上定义了乘法 \cdot 和加法 $+$ ，即有映射

$$K \times K \rightarrow K, (a, b) \mapsto a + b,$$

和

$$K \times K \rightarrow K, (a, b) \mapsto a \cdot b,$$

并且存在元素 $0_K, 1_K \in A$, $0_K \neq 1_K$, 使得

- 1)
 - 加法具有结合律, 即对任意的 $a_1, a_2, a_3 \in K$, 有 $(a_1 + a_2) + a_3 = a_1 + (a_2 + a_3)$;
 - 加法具有交换律, 即对任意的 $a, b \in K$, 有 $a + b = b + a$;
 - 0_K 是加法单位元, 即对任意的 $a \in K$, 有 $0_K + a = a + 0_K = a$;
 - 加法具有逆元, 即对任意的 $a \in K$, 存在 $-a \in K$, 使得 $a + (-a) = 0_K$ 。
- 2)
 - 乘法具有结合律, 即对任意的 $a_1, a_2, a_3 \in A$, 有 $(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3)$;
 - 乘法具有交换律, 即对任意的 $a, b \in K$, 有 $a \cdot b = b \cdot a$;
 - 1_K 是乘法单位元, 即对任意的 $a \in K$, 有 $1_K \cdot a = a \cdot 1_K$;
 - 乘法具有逆元, 即对任意的 $a \in K - \{0\}$, 存在 $a^{-1} \in K$, 使得 $a \cdot a^{-1} = 1_K$ 。
- 3) 乘法分配律成立: 对任意的 $a_1, a_2, a_3 \in A$, 有

$$(a_1 + a_2) \cdot a_3 = a_1 \cdot a_2 + a_1 \cdot a_3, \quad a_3 \cdot (a_1 + a_2) = a_3 \cdot a_1 + a_3 \cdot a_2.$$

我们就称 $(K, \cdot, +)$ 或 K 是一个域。



注 我们并不要求域 K 中的乘法是交换的。但是在本课程几乎所有的场合, K 都是交换的。

注 有以下几个简单的事实: 对任意的 $a \in K$, 加法逆元 $-a$ 是唯一的; 对任意的 $b \in K - \{0\}$, 乘法逆元 b^{-1} 也是唯一的。

对任意的 $a \in A$, $0 \cdot a = a \cdot 0 = 0$ 。

我们还用 $a - b$ 表示 $a + (-b)$ 。根据结合律, 容易看出 $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$, 我们把它简写成 $-a \cdot b$ 或者 $-ab$, 这里, 我们常用 ab 表示 $a \cdot b$ 。

例题 1.1 对于 $K = \mathbb{Q}, \mathbb{R}$ 或 \mathbb{C} , 使用通常的乘法和加法运算, 它们均为域。

定义 1.2

给定域 K , 给定集合 V 。如果 V 上定义了加法 $+$ 以及 K 对 V 的乘法, 即有映射

$$V \times V \rightarrow V, (v_1, v_2) \mapsto v_1 + v_2,$$

和

$$K \times V \rightarrow V, k \mapsto k \cdot v,$$

并且存在元素 $0_V \in V$, 使得

- 1)
 - 加法具有结合律, 即对任意的 $v_1, v_2, v_3 \in V$, 有 $(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$;

- 加法具有交换律, 即对任意的 $v_1, v_2 \in V$, 有 $v_1 + v_2 = v_2 + v_1$;
 - 0_V 是加法单位元, 即对任意的 $v \in V$, 有 $0_V + v = v$;
 - 加法具有逆元, 即对任意的 $v \in V$, 存在 $-v \in K$, 使得 $v + (-v) = 0_V$ 。
- 2) • 乘法具有结合律, 即对任意的 $a_1, a_2 \in K$ 和 $v \in V$, 有 $(a_1 \cdot a_2) \cdot v = a_1 \cdot (a_2 \cdot v)$;
- 1_K 是乘法单位元, 即对任意的 $v \in V$, 有 $1_K \cdot v = v$;
 - 乘法有分配律: 对任意的 $a_1, a_2, a \in K$ 和 $v_1, v_2, v \in V$, 有

$$(a_1 + a_2) \cdot v = a_1 \cdot v + a_2 \cdot v, \quad a \cdot (v_1 + v_2) = a \cdot v_1 + a \cdot v_2.$$

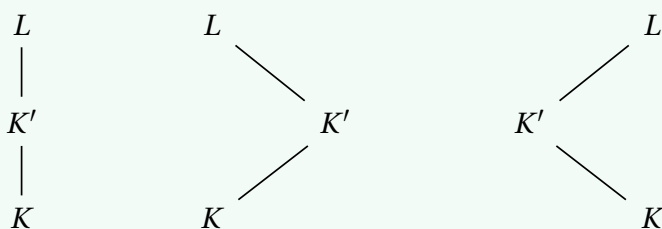
我们就称 V 是 K 上的线性空间或是 K -线性空间。



注 在线性代数的课程中, 定义线性无关性和维数的概念仅仅依赖于能在域 $K = \mathbb{Q}, \mathbb{R}$ 或者 \mathbb{C} 上做四则运算, 所以, 这些概念可以平行地移动到 K -线性空间上。

定义 1.3

L 是域, $K \subset L$ 。如果 K 在 L 的加法和乘法下封闭 (即对任意的 $a, b \in K$, 我们有 $a+b \in K$, $a \cdot b \in K$) 并且 K 在此加法和乘法下取逆也封闭 (即对任意的 $a, b \in K$ 和 $b \neq 0$, 我们有 $-a \in K$, $b^{-1} \in K$) 为域, 我们就称 K 为 L 的子域。我们还称 L 是 K 的扩张并记作 L/K 。如果 $K \subset K' \subset L$ 均为 L 的子域, 我们称 K' 为扩张 L/K 的中间域。我们通常用如下几种交换图表示这些关系:



练习 1.1 验证在 L 的加法和乘法下, K 是域。

练习 1.2 给定域扩张 L/K , $\{K'_i\}_{i \in I}$ 是一族中间域, 那么, $\bigcap_{i \in I} K'_i$ 也是 L 的子域。

注 给定域扩张 L/K , 根据 L 自身所带有的加法和乘法, L 成为 K -线性空间: 实际上, 对任意的 $a, b, c \in K$ 和 $x, y, z \in L$, 我们有 $a \cdot (x+y) = a \cdot x + a \cdot y$, $a \cdot (b \cdot x) = (ab) \cdot x$, $(a+b) \cdot x = a \cdot x + b \cdot x$, 这就验证了 L 作为 K 上线性空间所需要的公理。

如果 $\dim_K L < \infty$, 我们就称 L 是 K 的有限维扩张并记 $[L:K] = \dim_K L$ 。

例题 1.2 我们有如下的域扩张 $K = \mathbb{Q}, \mathbb{R}$ 或 \mathbb{C} , 使用通常的乘法和加法运算, 它们均为域。

我们知道 \mathbb{C}/\mathbb{R} 是有限维扩张并且 $[\mathbb{C}:\mathbb{R}] = 2$, 其中, $\{1, \sqrt{-1}\}$ 是一组基。

练习 1.3 试证明 \mathbb{R}/\mathbb{Q} 是无限维扩张。

例题 1.3 选定正整数 D , D 不是完全平方数。我们考虑所有的形如 $x + y\sqrt{D}$:

$$\mathbb{Q}(\sqrt{D}) = \{x + y\sqrt{D} \mid x, y \in \mathbb{Q}\}.$$

由于 \sqrt{D} 不是有理数, 所以, $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{D}) \subset \mathbb{R}$ (考虑 $x + 0\sqrt{D}$ 形式的数)。

练习 1.4 对于 $x + y\sqrt{D}, a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$, 证明, $x + y\sqrt{D} = a + b\sqrt{D}$ 等价于 $x = a, y = b$ 。

与有理数的情况类似, 我们研究 $\mathbb{Q}(\sqrt{D})$ 在四则运算下的性质:

- $\mathbb{Q}(\sqrt{D})$ 对加减法封闭。

对 $x + y\sqrt{D}, a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$, 我们有

$$(x + y\sqrt{D}) \pm (a + b\sqrt{D}) = (x \pm a) + (y \pm b)\sqrt{D} \in \mathbb{Q}(\sqrt{D}).$$

- $\mathbb{Q}(\sqrt{D})$ 对乘法封闭。

对 $x + y\sqrt{D}, a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$, 我们有

$$\begin{aligned} (x + y\sqrt{D}) \cdot (a + b\sqrt{D}) &= xa + yb(\sqrt{D})^2 + (xb + ya)\sqrt{D} \\ &= xa + ybD + (xb + ya)\sqrt{D} \in \mathbb{Q}(\sqrt{D}). \end{aligned}$$

- $\mathbb{Q}(\sqrt{D})$ 对除法封闭。

根据乘法封闭性, 只要说明如果 $a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$, 那么 $\frac{1}{a + b\sqrt{D}} \in \mathbb{Q}(\sqrt{D})$ 即可:

$$\begin{aligned} \frac{1}{a + b\sqrt{D}} &= \frac{a - b\sqrt{D}}{(a + b\sqrt{D})(a - b\sqrt{D})} = \frac{a - b\sqrt{D}}{a^2 - b^2D} \\ &= \frac{a}{a^2 - b^2D} + \frac{-b}{a^2 - b^2D}\sqrt{D} \end{aligned}$$

注意到 $\frac{a}{a^2 - b^2D}$ 和 $-\frac{b}{a^2 - b^2D}$ 是有理数, 从而 $\frac{1}{a + b\sqrt{D}} \in \mathbb{Q}(\sqrt{D})$ 。

综上所述, $\mathbb{Q}(\sqrt{D})$ 是 \mathbb{R} 的子域。进一步, 如果 \sqrt{D} 不是有理数, 那么, $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ 的次数为 2, 其中, $\{1, \sqrt{D}\}$ 是一组基。

命题 1.1

给定域扩张 L/K 和 E/L , 那么 E/K 是有限维的当且仅当 E/L 和 L/K 均为有限维的。此时, 我们还有 $[E:K] = [E:L][L:K]$ 。

证明 假设 E/K 是有限维的, 由于 L 是 E 的 K -线性子空间, 所以 L/K 是有限维的; 而对于 E 的一组基 $\{v_i\}_{1 \leq i \leq m}$, 那么, 它们的 L -线性组合显然张成 E , 所以, E/L 是有限维的。

假设 E/L 和 L/K 是有限维的。我们选取 $\{v_i\}_{1 \leq i \leq m}$ 是 E/L 的基, $\{w_j\}_{1 \leq j \leq n}$ 是 L/K 的基, 那么 $\{v_i \cdot w_j\}_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ 是 E/K 的基:

- $\{v_i \cdot w_j\}_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ 是 K -线性无关的: 假设 $\{\lambda_{i,j}\}_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \subset K$, 使得 $\sum_{i,j} \lambda_{i,j} v_i \cdot w_j = 0$ 。那么, 我们有

$$\sum_i \left(\sum_j \lambda_{i,j} w_j \right) v_i = 0 \Rightarrow \sum_j \lambda_{i,j} w_j = 0.$$

以上因为 $\sum_j \lambda_{i,j} w_j \in L$ 并且 $\{v_i\}_{1 \leq i \leq m}$ 是 E/L 的基。再利用 $\{w_j\}_{1 \leq j \leq n}$ 是 L/K 的基, 对任意的 i, j , 我们都有 $\lambda_{i,j} = 0$ 。这就证明了线性无关性。

- $\{v_i \cdot w_j\}_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ 是张成 E : 实际上, 对任意的 $x \in E$, 存在 $\{x_i\}_{1 \leq i \leq m} \subset L$, 使得 $\sum_i x_i v_i = x$ 。对每个 i , 存在 $\{\lambda_{i,j}\}_{1 \leq j \leq n} \in K$, 使得 $\sum_j \lambda_{i,j} w_j = x_i$, 从而,

$$x = \sum_i \left(\sum_j \lambda_{i,j} w_j \right) v_i = \sum_{i,j} \lambda_{i,j} v_i \cdot w_j.$$

从而, $\{v_i \cdot w_j\}_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ 可以张成 E 。

以上推导自然给出了 $[E:K] = [E:L][L:K]$ 。

定义 1.4

给定域扩张 L/K 和 L 的子集 M ，我们用 $K(M)$ 表示所有包含 M 的中间域的交。这是包含 M 的最小的子域，我们把它称作是由 M 所生成的子域。如果 M 是有限集 $\{m_1, \dots, m_n\}$ ，我们把 $K(M)$ 写成 $K(m_1, \dots, m_n)$ 。如果 $L = K(M)$ 并且 M 是有限集，我们称域扩张 L/K 是有限型的。



引理 1.1

给定域扩张 L/K 和 L 的子集 M 和 N ，那么，

- 1) $K(M)$ 恰为 L 中形如 $\frac{P(x_1, \dots, x_n)}{Q(x_1, \dots, x_n)}$ 的元素，其中， $n \geq 0$ ， $P, Q \in K[X_1, \dots, X_n]$ 是 K -系数的 n 元多项式， $x_1, \dots, x_n \in M$ 并且 $Q(x_1, \dots, x_n) \neq 0$ 。
- 2) $K(M \cup N) = K(M)(N) = K(N)(M)$ 。
- 3) $K(M) = \bigcup_{\substack{F \subset M \\ F \text{ 是有限集}}} K(F)$ 。



证明 显然。

1.3 三等分已知角

给定 \mathbb{R}^2 中的集合 \mathcal{S} 。过 \mathcal{S} 中任意的两点 $A, B \in \mathcal{S}$ 所给的直线被称作是 \mathcal{S} -直线；以 \mathcal{S} 中某点 $O \in \mathcal{S}$ 为圆心以 $|OA|$ 为半径（要求 $A \in \mathcal{S}$ ）所作的圆被称作是 \mathcal{S} -圆。

定义 1.5

给定 \mathbb{R}^2 中的集合 \mathcal{S} ，如果点 P 满足如下三个条件之一：

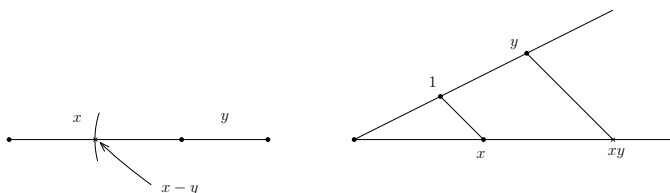
- P 是两条 \mathcal{S} -直线的交点；
- P 是一条 \mathcal{S} -直线和一个 \mathcal{S} -圆的交点（之一）；
- P 是两个 \mathcal{S} -圆的交点（之一）。

我们就称 P 是 \mathcal{S} -直接可作的。假设存在有限个点 P_1, \dots, P_m ，使得 P_i 是 $\mathcal{S} \cup \{P_0, \dots, P_{i-1}\}$ -直接可作的并且 $P = P_m$ ，我们就称 P 是 \mathcal{S} -可作的。



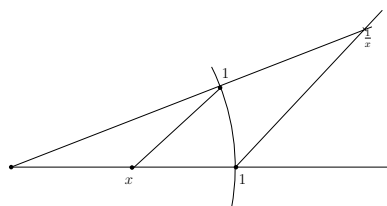
令 $\mathcal{S} = \{(0,0), (0,1)\} \subset \mathbb{R}$ ，对于 $x \in \mathbb{R}$ ，如果 x 是某个 \mathcal{S} -可作点的横坐标或者纵坐标，我们就称 x 是尺规可作的或者可作的。这些尺规可作的数满足如下性质：

- 1) 如果 x, y 是可作的，那么， $x \pm y$ 和 $x \cdot y$ 也是。以下的图示通过以下图示可以看出：



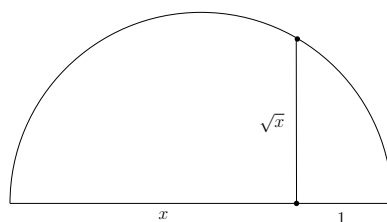
其中，我们做了过 y 点的平行线。

2) 如果 x, y 是可作的并且 $y \neq 0$ ，那么， $\frac{x}{y}$ 也是。



根据 1)，我们只需要按照上面的方式做出 $\frac{1}{x}$ 即可。

3) 如果 x 是可作的，那么， \sqrt{x} 也是。



注 以上前两条表明尺规可作的数构成一个域。

定理 1.1 (Wantzel, 1937)

$x \in \mathbb{R}$ 是尺规可作的当且仅当存在有限个域扩张

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_m \subset \mathbb{R}$$

使得 $[K_i : K_{i-1}] = 2$ ($i = 1, \dots, m$) 并且 $x \in K_m$ 。

特别地，如果 x 是尺规可作的，必存在 $\mathbb{Q} \subset K \subset \mathbb{R}$ ，使得 $x \in K$ 并且 $[K : \mathbb{Q}]$ 是 2 的幂。



引理 1.2

给定域扩张 $K \subset L \subset \mathbb{R}$ 并且 $[L : K] = 2$ 。那么，存在 $x \in L$ ， $x \notin K$ 并且 $x^2 \in K$ ， L 中每个元素都可以表示称为形如 $a + bx$ 的形式，其中， $a, b \in K$ 。



证明 任选 $y \in L - K$ ，那么， $\{1, y\}$ 是 L/K 的一组基础。从而，存在 $a, b \in K$ ，使得

$$y^2 = ay + b.$$

通过对以上二次方程配方， $x = y - \frac{a}{2}$ 满足要求。

证明 给定 $\mathcal{S} \subset \mathbb{R}^2$ ，假设 \mathcal{S} 的点的横纵坐标都落在域 $K \subset \mathbb{R}$ 中。假设 $P = (x, y)$ 是一个 \mathcal{S} -直接可作的，记 $L = K(x, y)$ ，那么， $[L : K] = 1$ 或 2。实际上，每一个 \mathcal{S} -直线和 \mathcal{S} -圆的都可以写成以 K 中数为系数的方程。

- 如果 P 是两条 \mathcal{S} -直线的交点，通过解两个 K -系数的线性方程， x 和 y 仍然是 K 中的数，所以， $K = L$ 。
- 如果 P 是一条 \mathcal{S} -直线和一个 \mathcal{S} -圆的交点。此时，我们解一个 K -系数的线性方程和一个 K -系数的二次方程的联立，通过先用线性方程代换掉一个变量，我们可以解一个一元二次方程来求得 x 或者 y 。利用二次方程的求根公式， L 可以通过 K 添加这个二次方程的判别式的根式得到， $L = K[\sqrt{\Delta}]$ ，这是一个二次扩张，其中， $1, \sqrt{\Delta}$ 张成了 L 。

- 如果 P 是两个 S -圆的交点, 定义它们的方程的二次项必然形如 $x^2 + y^2$, 通过相减, 我们就可以得到一个一次方程, 这就变成了前一个情形。

我们从 $\mathbb{Q} = K_0$ 出发, 通过有限步得到 (x, y) , 每一步使用上面的讨论, 我们就得到了

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_m \subset \mathbb{R}.$$

反之, 我们对 m 进行归纳。对于 $x \in K_m$, 存在 $a \in K_{m-1}$, 使得 $(x-a) \in K_{m-1}$ 。根据归纳, $(x-a)^2$ 是尺规可作的。根据之前的讨论, $\pm\sqrt{(x-a)^2}$ 是尺规可作的, 所以, x 也是可作的。

推论 1.1 (倍立方问题²)

$\sqrt[3]{2}$ 不是尺规可作的。



证明 如果 $\sqrt[3]{2}$ 是尺规可作的, 那么存在 $K \subset \mathbb{R}$, 使得 $\sqrt[3]{3} \in K$ 并且 $[K:\mathbb{Q}] = 2^m$ 。此时, 我们注意到

$$L = \mathbb{Q}[\sqrt[3]{3}, (\sqrt[3]{3})^2]$$

是 K 的子域。为此, 只要验证 $a + b\alpha + c\alpha^2$ 的倒数在 L 中即可。³。实际上, 利用公式

$$(x+y+z)(x^2+y^2+z^2-xy-yz-zx) = x^3+y^3+z^3-3xyz,$$

并代入 $x = a, y = b\alpha, z = c\alpha^2$, 据此, 上式右边所取值 d 落在 \mathbb{Q} 中, 从而, $a + b\alpha + c\alpha^2$ 的倒数为 $d^{-1}(x^2+y^2+z^2-xy-yz-zx) \in L$ 。据此, $[L:\mathbb{Q}] = 3$ 。然而, $[L:\mathbb{Q}]$ 整除 $[K:\mathbb{Q}] = 2^m$, 矛盾。

推论 1.2 (三等分已知角⁴)

$\cos(\frac{\pi}{9})$ 不是尺规可作的, 从而, 不能通过尺规作图三等分 60° 的角。



证明 给定一个角度为 θ 的角, 这等价于给出了 $\cos(\theta)$ 。据此, 我们要做出 $\cos(\frac{\theta}{3})$ 即可。根据三角函数的基本公式, 我们有

$$4\cos(\frac{\theta}{3})^3 - 3\cos(\frac{\theta}{3}) = \cos(\theta).$$

令 $x = \cos(\frac{\theta}{3})$ 并选取 $\theta = \frac{1}{3}\pi$, 所以,

$$4x^3 - 3x - \frac{1}{2} = 0.$$

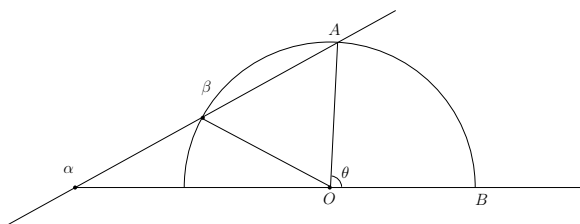
假设我们可以做出 $\frac{\pi}{9}$ 的角, 所以, 我们能做出上面方程的一个根 (这个方程有三个实数根)。通过考虑 $X = 2x$, 我们能做出

$$X^3 - 3X - 1 = 0$$

的根。我们将会证明, 这是一个在 $\mathbb{Q}[X]$ 中不可约的多项式并且 $[\mathbb{Q}(\xi):\mathbb{Q}] = 3$, 其中, ξ 是一个根。这不是 2^m 的因子。矛盾。

注 通过升级直尺和圆规, 我们可以三等分已知角。最著名的例子是 Archimedes 的“二刻度尺”。所谓的二刻度尺就是在一个直尺上标记了两个点 α 和 β 。

³在课堂上我给的证明有错误。为了找到 $a + b\alpha + c\alpha^2$ 的倒数, 最直接的方式就是利用 $X^3 - 2$ 是不可约多项式的性质说明 $X^3 - 2$ 与 $a + bX + cX^2$ 互素, 然后利用多项式的 Bézout 定理来构造 $a + b\alpha + c\alpha^2$ 的逆。然而, 我们在课程之后会用环商掉极大理想的语言更清楚的说明这一点, 所以, 这里我们就不追求证明的完备性了



给定角度 $\theta = \angle AOB$ ，我们做以 O 为圆心的圆并且选取半径 $|OA| = |OB|$ 恰好为 α 与 β 之间的距离。移动二刻度尺使得它过 A 点并且 α 落在 BO 的延长线上并且 β 落在圆上。此时，直尺与 BO 的延长线的夹角就三等分了已知角度。

注 著名的 Mohr-Mascheroni 定理说可以只用圆规完成尺规作图（做出相应的点而不是直线）。

推论 1.3 (化圆为方⁵)

π 不是尺规可作的。



证明 根据 Lindemann 的著名定理， π 是超越数，即 π 不满足任何一个有理系数的代数方程。如果 π 是尺规可作的，那么， $\pi \in K$ ，其中， K 是 \mathbb{Q} 的有限扩张（次数为 2^m ）。那么， $\{1, \pi, \pi^2, \dots, \pi^{2^m}\}$ 是 \mathbb{Q} -线性相关的，这就给出了关于 π 的一个有理系数的代数方程，矛盾。

第2章 群和环的定义

2.1 群的定义

定义 2.1

给定非空集合 G 。如果 G 上定义了乘法，即有映射

$$G \times G \rightarrow G, (g_1, g_2) \mapsto g_1 \cdot g_2,$$

并且存在元素 $e \in G$ ，使得

- 1) 对任意的 $g_1, g_2, g_3 \in G$ ，有结合律 $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$ ；
- 2) e 是乘法单位元，即对任意的 $g \in G$ ，有 $e \cdot g = g \cdot e$ ；
- 3) 每个 $g \in G$ 的逆元存在，即对任意的 g ，存在 $g^{-1} \in G$ ，使得 $g \cdot g^{-1} = g^{-1} \cdot g = e$ 。

我们就称 (G, \cdot) 或者 G 是一个群。我们也把 e 记作是 1_G 或 1 。



注 对任意的 $g \in G$ ， g 的逆元存在唯一：假设 g' 也是逆元，那么， $g \cdot g^{-1} = g \cdot g' = e$ 。对第一个等号左右两边同时乘以 g^{-1} ，根据结合律：

$$(g^{-1} \cdot g) \cdot g^{-1} = (g^{-1} \cdot g) \cdot g' \Rightarrow e \cdot g^{-1} = e \cdot g' \Rightarrow g^{-1} = g'.$$

注 如果对任意的 $g_1, g_2 \in G$ ，都有 $g_1 \cdot g_2 = g_2 \cdot g_1$ ，我们就称 (G, \cdot) 是交换群或 **Abel 群**。如果 $|G|$ 有限，我们就称 G 是有限群并把 $|G|$ 称作是群的阶；否则称之为无限群。

注 只有一个元素的群被称作是平凡群，这个元素恰好也是单位元。简单起见，我们通常把平凡群直接写成 1 。

例题 2.1 对于 $G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ 或 \mathbb{C} ，对任意的 $g_1, g_2 \in G$ ，我们定义 $g_1 \cdot g_2 = g_1 + g_2$ ，其中 $+$ 是 G 自然的加法运算。那么， G 是交换群，其中， 0 是单位元。一般而言，当 G 是交换群时，我们把乘法符号 \cdot 写成 $+$ ，把 g 的逆写成 $-g$ ，把单位元记作 0 。

例题 2.2 $G = \mathbf{GL}(n; K)$ 是 K 上 $n \times n$ 的可逆矩阵的集合，其中 $K = \mathbb{Q}, \mathbb{R}$ 或 \mathbb{C} 。我们选取 \cdot 为矩阵的乘法， e 为单位矩阵， $\mathbf{GL}(n; K)$ 显然是一个群。我们把它称作是 K 上的一般线性群。如果 $n \geq 2$ ， G 不是交换群。

例题 2.3 对称群 给定集合 X ，令 \mathfrak{S}_X 为 X 到自身双射的全体。对任意的 $g_1, g_2 \in \mathfrak{S}_X$ ，定义 $g_1 \cdot g_2$ 为 g_1 与 g_2 的复合，即

$$\begin{array}{ccc} X & \xrightarrow{g_2} & X \\ & \searrow g_1 \cdot g_2 & \downarrow g_1 \\ & & X \end{array}$$

那么， \mathfrak{S}_X 是群，其中，单位映射是群的单位元，元素在群中的逆恰为其对应的映射的逆。

例题 2.4 我们用 $\mathbb{Z}/n\mathbb{Z}$ 表示所有整数集除 n 的同余类，即

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\},$$

其中, $\bar{k} = \{m \in \mathbb{Z} \mid m \equiv k \pmod{n}\}$, $k = 0, \dots, n-1$. 对于任意的 $l \in \mathbb{Z}$, 我们也用 \bar{l} 表示其所对应的同余类, 那么, $\bar{k} + \bar{l} = \overline{k+l}$ 是良好定义加法并且 $\bar{0}$ 是单位元, 此时, $(\mathbb{Z}/n\mathbb{Z}, +)$ 是交换群。

对任意的 $g \in G$ 和 $n \geq 1$, 我们用 g^n 表示 $\underbrace{g \cdot g \cdots g}_n$, 用 g^{-n} 表示 $\underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_n$. 习惯上, 我们说 $g^0 = 1$. 假设存在 $g \in G$, 对任意的 $g' \in G$, 存在 $n \in \mathbb{Z}$, 使得 $g^n = g'$, 我们就称 G 是循环群并称 g 为其生成元。

那么, $(\mathbb{Z}/n\mathbb{Z}, +)$ 是循环群, 其中, $\bar{1}$ 是生成元. 证明, \bar{k} 是生成元当且仅当 $(k, n) = 1$.

例题 2.5 二面体群 \mathfrak{D}_n

考虑正 n 边形 $\text{Reg}_n \subset \mathbb{R}^2$, 其中心在原点 O 处. 对于平面 $\mathbb{R}^2 = \mathbb{C}$ 而言, 以 O 为圆心、旋转 $\frac{2k\pi}{n}$ 的变换 (其中 $k = 0, 1, \dots, n-1$) 可写成:

$$\rho_k: \mathbb{R}^2 \rightarrow \mathbb{R}^2, \begin{pmatrix} x \\ y \end{pmatrix} \rightarrow \begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) & -\sin\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) & \cos\left(\frac{2k\pi}{n}\right) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

令 $r = \rho_1$, 那么, $\rho_k = r^k$.

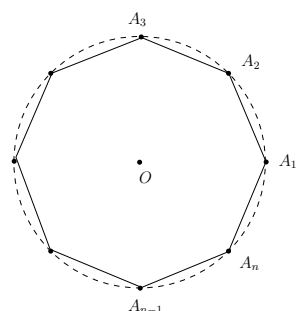
考虑 \mathbb{R}^2 到自身的反射. 当 n 是奇数时, R_k 是以过 A_k 与其对边中心的直线为反射轴的反射, 其中, $k = 1, 2, \dots, n$; 当 n 是偶数时, R'_k 是以过 A_k 与 A_{n+k} 的直线为反射轴的反射 (而 R''_k 是以过 $A_k A_{k+1}$ 的中点与 $A_{\frac{n}{2}+k} A_{\frac{n}{2}+k+1}$ 的中点的直线为反射轴的反射, 其中, $k = 1, 2, \dots, \frac{n}{2}$). 这些反射保持该正多边形, 比如说 n 为奇数时:

$$R_k: \text{Reg}_n \rightarrow \text{Reg}_n.$$

当然, 每个这样的映射都是双射并且其逆为其本身. 我们记以通过 A_1 的线为对称轴的反射为 s , 即 $s(x, y) = (x, -y)$.

以上我们构造了关于正多边形的 $2n$ 个对称 (即变换):

$$\mathfrak{D}_n = \{\rho_k, R_k\} \text{ 或者 } \{\rho_k, R'_k, R''_k\}.$$



实际上, $\{s, sr, sr^2, \dots, sr^{n-1}\}$ 恰好给出了 \mathfrak{D}_n : 因为 sr^k 为以过原点 O 和 $e^{-\frac{k}{n}\pi}$ 的直线为对称轴的反射. 所以,

$$\mathfrak{D}_n = \{1, r, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}.$$

我们有如下复合关系:

$$sr s = r^{-1}.$$

据此, 我们容易验证 \mathfrak{D}_n 是群。实际上, 对于 $x = r^k s$, $y = r^l s^b$, 其中, $b = 0$ 或 1 (如果 $x = r^k$, 很明显有 $xy \in \mathfrak{D}$)。根据 $sr s = r^{-1}$, 我们有

$$x \cdot y = r^k s \cdot r^l s^b = r^k \cdot r^{-l} \cdot s \cdot s^b = r^{k-l} s^{1+b}.$$

另外, $x^{-1} = x$, 因为 x 是反射对称。

容易看出, \mathfrak{D}_n 不是交换群。

定义 2.2

给定群 G , $H \subset G$ 为非空子集, 如果

- 1) (乘法封闭) 对任意的 $h_1, h_2 \in H$, $h_1 \cdot h_2 \in H$;
- 2) (取逆封闭) 对任意的 $h \in H$, $h^{-1} \in H$

我们就称 H 是 G 的子群, 并记作 $H < G$ 。



注 给定群 G , 如果 $H < G$, 那么 $1 \in H$ 。进一步, 使用 G 上的乘法, H 具有自然的群结构。

例题 2.6 令 \mathbb{C}^\times 为全体非零复数, 定义群乘法为通常的复数乘法, 这是一个群。尽管 $\mathbb{C}^\times \subset \mathbb{C}$, 但 $(\mathbb{C}^\times, \cdot)$ 不是 $(\mathbb{C}, +)$ 的子群。

令 $\mu^n(\mathbb{C})$ 为 \mathbb{C} 中所有 n 次单位根 (其中, $n \geq 1$), 即 $X^n - 1 = 0$ 的所有解, 这是 $\mathbb{C}^\times \subset \mathbb{C}$ 的子群。

令 \mathbb{R}^+ 为全体非零正数, 它在实数乘法下构成群。这是 \mathbb{R}^\times 或 \mathbb{C}^\times 的子群, 但不是 $(\mathbb{R}, +)$ 的子群。

例题 2.7 \mathbb{N} 为全体自然数 (包括 0), 它不是 (\mathbb{Z}, \cdot) 的子群, 因为并不满足取逆封闭。

例题 2.8 可逆的 n 阶上三角矩阵的全体 \mathcal{T} 是 $G = \mathbf{GL}(n; K)$ 的子群。

例题 2.9 生成一个子群 G 是群。

- 1) 假设 $\{G_i\}_{i \in I}$ 是 G 的一族子群, 那么, $\bigcap_{i \in I} G_i$ 是子群。
- 2) $S \subset G$ 并且 $S \neq \emptyset$, 则存在唯一的包含 S 的最小的 (在包含关系下) 子群。我们把它称作是由 S 所生成的子群并记作 $\langle S \rangle$ 。实际上, $\langle S \rangle$ 是包含 S 的所有子群之交。
- 3) $S \subset G$, 那么, $\langle S \rangle$ 具有如下描述:

$$\langle S \rangle = \{s_1^{n_1} \cdot s_2^{n_2} \cdots s_k^{n_k} \mid k \in \mathbb{N}, s_i \in S, n_i \in \mathbb{Z}, s_i \neq s_{i+1}\}.$$

实际上, 如果 $s_i = s_{i+1}$, 我们可以合并同类项。对于 $s_1^{n_1} \cdots s_k^{n_k}$ 和 $s_1^{n'_1} \cdots s_{k'}^{n'_{k'}}$, 它们相乘得

$$s_1^{n_1} \cdots s_k^{n_k} \cdot s_1^{n'_1} \cdots s_{k'}^{n'_{k'}}.$$

如果 $s_k = s'_1$, 我们可以将它们合并, 然后再看是否有相邻两项相同, 如此重复一直到得到上述对于 $\langle S \rangle$ 中元素所描述的形式。另外, 我们还有

$$(s_1^{n_1} \cdot s_2^{n_2} \cdots s_k^{n_k})^{-1} = s_k^{-n_k} \cdots s_2^{-n_2} \cdot s_1^{-n_1}.$$

- 4) 当 $S = \{g\}$ 时, 其中, $g \in G$ 。我们把它所生成的子群简记为 $\langle g \rangle$ 。此时,

$$\langle g \rangle = \{\cdots g^{-2}, g^{-1}, 1, g, g^2, \cdots\}.$$

如果存在正整数 n , 使得 $g^n = 1$, 那么, 我们用 $\text{ord}(g)$ 来记最小的那个这样的整数并称

它为 g 的阶。此时，我们说 g 是有限阶的元（否则称它是无限阶的元）。很明显， $\langle g \rangle$ 是有限群并且 $|\langle g \rangle| = n$ 。

5) 在二面体群中， $\langle r \rangle$ 所生成的子群恰好是所有的旋转所构成的子群。这个子群是 n 阶的。

练习 2.1 G 是群。

- 1) g 是有限阶的元， k 和 l 是整数。那么， $g^k = g^l$ 当且仅当 $\text{ord}(g) | k - l$ 。
- 2) G 是有限群，那么每个 $g \in G$ 都是有限阶的。如果 G 中每个元素都是有限阶的，它是否是有限群？

例题 2.10 G 是群。对任意的 $g \in G$ ，我们定义 g 的中心化子：

$$C_g(G) = \{h \in G | gh = hg\}.$$

这是 G 中与 g 交换的那些元素，它们构成一个子群。

令 $Z(G) = \bigcap_{g \in G} C_g(G)$ ，这是与 G 中一切元素均交换的元素构成的子群，我们把它称作是 G 的中心。

定义 2.3 (群同态)

(G_1, \cdot_1) 和 (G_2, \cdot_2) 是群， $\varphi: G_1 \rightarrow G_2$ 是映射。如果该映射保持乘法，即对任意的 $g, h \in G_1$ ，有

$$\varphi(g \cdot_1 h) = \varphi(g) \cdot_2 \varphi(h),$$

我们就称 φ 是 (G_1, \cdot_1) 和 (G_2, \cdot_2) 之间的群同态。我们用 $\text{Hom}(G_1, G_2)$ 表示它们之间所有的群同态。如果 φ 还是双射，我们称 φ 是 G_1 与 G_2 之间的一个群同构。如果 G_1 与 G_2 之间存在群同构，我们就称这两个群是同构的并记作是 $G_1 \simeq G_2$ 。



两个同构的群首先是两个同构的（有一对一的映射）集合，其次还具有同样的乘法结构。

注 对于群同态 $\varphi: G_1 \rightarrow G_2$ ，通过考虑 $\varphi(1_{G_1} \cdot 1_{G_1}) = \varphi(1_{G_1})$ ，我们有 $\varphi(1_{G_1}) = 1_{G_2}$ 。对任意的 $g \in G_1$ ，我们还有 $\varphi(g^{-1}) = \varphi(g)^{-1}$ 。

注 假设 $\varphi \in \text{Hom}(G_1, G_2)$ 是双射（群同构），那么（按照定义验证即可）， $\varphi^{-1} \in \text{Hom}(G_2, G_1)$ 。

注 两个群 G_1 和 G_2 同构，但是可以给出它们之间的同构映射 φ 可能不唯一。比如，我们取 G_1 和 G_2 均为 \mathbb{C}^\times ，那么，对任意的 $\lambda \in \mathbb{C}^\times$ ，映射 $z \mapsto \lambda z$ 都给出它们之间的同构。

注 群同态的复合还是群同态，即有映射

$$\text{Hom}(G, G') \times \text{Hom}(G', G'') \longrightarrow \text{Hom}(G, G''), (\varphi, \psi) \mapsto \psi \circ \varphi.$$

换言之， $\varphi \in \text{Hom}(G, G')$ ， $\psi \in \text{Hom}(G', G'')$ ，那么， $\psi \circ \varphi \in \text{Hom}(G, G'')$ 也是群同态。

注 我们把 G 到自身的群同构的全体记作是 $\text{Aut}(G)$ 。我们注意到利用映射的复合作为乘法， $\text{Aut}(G)$ 也是群。我们考虑对称群的例子，其中 $X = G$ 。据此，我们知道 $\text{Aut}(G) < \mathfrak{S}_G$ 是子群。

注 给定 $\varphi \in \text{Hom}(G_1, G_2)$ ，我们定义该映射的像为：

$$\text{Im}(\varphi) = \{\varphi(g) | g \in G_1\}.$$

我们有 $\text{Im}(\varphi) < G_2$ ，即群同态的像是 G_2 的子群。

我们定义该映射的核为：

$$\text{Ker}(\varphi) = \{g \in G_1 \mid \varphi(g) = 1_{G_2}\}.$$

我们有 $\text{Ker}(\varphi) < G_1$ ，即群同态的核是子群。

例题 2.11 行列式映射 $\det: \text{GL}(n; K) \rightarrow K^\times$ 是群同态，其中， K^\times 是 K 中非零元在标准乘法下所构成的群。指数映射 $\exp: \mathbb{C} \rightarrow \mathbb{C}^\times$ 是群同态。对数映射 $\log: \mathbb{R}^\times \rightarrow \mathbb{R}$ 也是群同态。

例题 2.12 G 是群， $g \in G$ 。那么，映射

$$\varphi_g: \mathbb{Z} \rightarrow G, \quad n \mapsto g^n$$

是群同态，其像 $\text{Im}(\varphi_g)$ 恰为 $\langle g \rangle$ 。我们注意到 φ 是单射当且仅当 $\text{Im}(\varphi_g) = \{e_1\} = 1$ 。所以，要验证群同态是否是单射只要看 e_2 的原像是否唯一即可。

例题 2.13 我们用 $\text{SL}(n; K)$ 表示 $\det: \text{GL}(n; K) \rightarrow K^\times$ 的核，这是行列式为 1 的矩阵构成的群，我们把它称作是 K 上的特殊线性群。

例题 2.14 通过考虑除以 n 的余数（即考虑一个整数所在的模 n 的同余类），我们有自然的群同态

$$\mathbb{Z} \xrightarrow{\text{mod } n} \mathbb{Z}/n\mathbb{Z}, \quad k \mapsto \bar{k}.$$

那么， $\text{Ker}(\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}) = n\mathbb{Z}$ 。这是能被 n 整除的整数所构成的子群。

例题 2.15 给定群 G ，对任意的 $g \in G$ ，我们定义共轭映射 $\text{Int}(g)$ ：

$$\text{Int}(g): G \rightarrow G, \quad h \mapsto \text{Int}(g)(h) = ghg^{-1}.$$

由于对任意的 $h_1, h_2 \in G$ ，我们有 $gh_1h_2g^{-1} = gh_1g^{-1} \cdot gh_2g^{-1}$ ，所以， $\text{Int}(g) \in \text{Hom}(G, G)$ 。另外， $\text{Int}(g)$ 是可逆映射，其逆为 $\text{Int}(g^{-1})$ ，从而， $\text{Int}(g) \in \text{Aut}(G)$ 。据此，我们可以考虑映射：

$$G \rightarrow \text{Aut}(G), \quad g \mapsto \text{Int}(g).$$

对任意的 $h \in G$ ，对任意的 $g_1, g_2 \in G$ ，我们有

$$\text{Int}(g_1g_2)(h) = g_1(g_2hg_2^{-1})g_1^{-1} = \text{Int}(g_1)(g_2hg_2^{-1}) = \text{Int}(g_1) \circ \text{Int}(g_2)(h).$$

这表明 $\text{Int}: G \rightarrow \text{Aut}(G)$ 是群同态。很明显， $\text{Ker}(\text{Int}) = Z(G)$ 。

2.2 正规子群与商群

定义 2.4

给定群 G 及其子群 H 。对任意的 $g \in H$ ，我们称如下集合为一个左陪集：

$$gH = \{gh \mid h \in H\}.$$



首先注意到，由于 H 是子群，所以对任意的 $h \in H$ ， $hH = 1 \cdot H = H$ 。假设 $g_1H \cap g_2H \neq \emptyset$ ，从而， $g_1h_1 = g_2h_2$ ，其中， $h_1 = h_2$ ，所以， $g_2 = g_1h_1h^{-1}$ 。从而， $g_2H = g_1h_1h^{-1}H = g_1(h_1h^{-1}H) = g_1H$ 。这表明 $\{gH\}_{g \in G}$ 给出了 G 的一个划分。这自然就定义了一个等价关系 \sim 。实际上， $g_1 \sim g_2$ 等

价于 $g_1^{-1}g_2^\epsilon H$ 。我们定义

$$G/H = \{gH \mid g \in G\}.$$

我们令 $[G:H] = |G/H|$ 并称之为 H 在 G 中的**指标**。类似地，我们可以定义**右陪集**：

$$Hg = \{gh \mid h \in H\}.$$

我们同样可以证明 $\{Hg\}_{g \in G}$ 给出了 G 的一个划分。这自然就定义了一个等价关系 \sim_r 。实际上， $g_1 \sim_r g_2$ 等价于 $g_1g_2^{-1} \in H$ 。我们用以下符号代表右陪集的集合：

$$H \backslash G = \{Hg \mid g \in G\}.$$

从此往后，我们基本上只处理左陪集的情形。我们注意到，对任意的 gH 和 $g'H$ ，有自然的双射：

$$gH \rightarrow g'H, x \mapsto g'g^{-1}x.$$

所以，如果 H 是有限子群，那么，其所有左陪集的元素个数均为 $|H|$ 。此时，如果 G 是有限集合，那么，

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

命题 2.1 (Lagrange)

G 是有限群，那么，其子群的元素个数整除 $|G|$ 。特别的，对任意的 $g \in G$ ， $\text{ord}(g) \mid |G|$ （从而， $g^{|G|} = 1$ ）。

证明 为了证明 $\text{ord}(g) \mid |G|$ ，只需要选取 $H = \{1, g, \dots, g^{\text{ord}(g)-1}\}$ 。

定义 2.5

H 是群 G 的子群。如果对任意的 $g \in G$ ， $gHg^{-1} = H$ ，其中， $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ ，我们就称 H 是**正规子群**并且记作是 $H \triangleleft G$ 。

注 为了验证 H 是正规子群，只需要验证对任意的 $h \in H$ ，对任意的 $g \in G$ ，有 $ghg^{-1} \in H$ 。这是因为，只要选取 $g = 1$ ，就给出了 $\bigcup_{g \in G} gHg^{-1} \supset H$ 。

例题 2.16 G 是交换群，那么每个子群都是正规子群。

例题 2.17 $n \geq 3$ ， $G = \mathfrak{S}_n$ 。那么， $H = \langle (12) \rangle$ 不是正规子群。

例题 2.18 $\varphi: G \rightarrow G'$ 是群同态，那么， $\text{Ker}(\varphi) \triangleleft G$ 。

这因为对任意的 $g \in G$ ，对任意的 $h \in \text{Ker}(\varphi)$ ，我们有

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g) \cdot 1_{G'} \cdot \varphi(g)^{-1} = 1.$$

所以， $ghg^{-1} \in \text{Ker}(\varphi)$ 。

例题 2.19 H 是群 G 的子群，我们定义 H 在 G 中的**正规化子**为：

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

容易验证，这是 G 的子群。按照定义，我们有

$$H \triangleleft N_G(H) < G.$$

这是 G 中使得 H 在其中为正规子群的最大子群。

假设 H 为 G 的子群，我们想要在 G/H 上面定义乘法。对于左陪集 g_1H 和 g_2H ，一个自然的定义可能是 $g_1H \cdot g_2H = g_1g_2H$ 。然而，由于 g_1H 还可以表述称 g'_1H ，其中， $g'_1 = g_1h$ ，所以，这个定义还给出了 $g'_1H \cdot g_2H = g_1hg_2H$ 。为了保证 g_1g_2H 与 g_1hg_2H 给出同样的左陪集，我们需要 $(g_1g_2)^{-1}g_1hg_2 = g_2^{-1}hg_2 \in H$ 才行！

定理 2.1

$H \triangleleft G$ 是正规子群。那么，在 G/H 存在唯一的群结构，使得自然的商映射

$$\pi: G \rightarrow G/H$$

是群同态。另外， $\text{Ker}(\pi) = H$ 。

实际上，左陪集的乘法如下定义： $g_1H \cdot g_2H = g_1g_2H$ 。



证明 我们定义 G/H 的乘法为 $g_1H \cdot g_2H = g_1g_2H$ 。假设 $g'_1H = g_1H$, $g'_2H = g_2H$ ，那么，存在 h_1 和 h_2 ，使得 $g'_1 = g_1h_1$, $g'_2 = g_2h_2$ 。我们现在验证如上乘法是良好定义的，即验证 $g_1g_2H = g'_1g'_2H$ 。实际上，我们有

$$g'_1g'_2H = g_1h_1g_2h_2H = g_1g_2 \cdot \underbrace{g_2^{-1}h_1g_2}_{\in H} \cdot h_2H = g_1g_2H.$$

根据定义， π 是群同态。唯一性也是明显的：为了保证 π 是群同态，我们必然有 $\pi(1_G) = 1_{G/H}$ ，所以， H 是 G/H 中的单位元。另外，

$$\pi(g_1 \cdot g_2) = \pi(g_1) \cdot \pi(g_2) \Leftrightarrow g_1H \cdot g_2H = g_1g_2H.$$

这说明群的结构也由同态决定。

注 假设 $K < H < G$ 是子群，那么， $[G:K] = [G:H][H:K]$ 。

命题 2.2

$H \triangleleft G$ 是正规子群， $\varphi: G \rightarrow G'$ 是群同态。如果 $H < \text{Ker}(\varphi)$ ，那么存在唯一的群同态 $\bar{\varphi}: G/H \rightarrow G'$ ，使得 $\bar{\varphi} \circ \pi = \varphi$ ，其中， $\pi: G \rightarrow G/H$ 是自然的同态。

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \downarrow \pi & \nearrow \bar{\varphi} & \\ G/H & & \end{array}$$

进一步，我们还有群同构 $\bar{\varphi}: G/\text{Ker}(\varphi) \xrightarrow{\cong} \text{Im}(\varphi)$ 。



证明 我们定义 $\bar{\varphi}(gH) = \varphi(g)$ 。由于 $H < \text{Ker}(\varphi)$ ，所以，对于 $g'H = gH$ ，利用 $g^{-1}g' \in H \subset \text{Ker}(\varphi)$ ，我们有 $\varphi(g^{-1}g') = 1$ ，从而， $\varphi(g) = \varphi(g')$ ，这说明 $\bar{\varphi}$ 是良好定义的。这是群同态以及 $\bar{\varphi} \circ \pi = \varphi$ 是平凡的。

选取 $H = \text{Ker}(\varphi)$ ，我们显然有满射

$$\bar{\varphi}: G/\text{Ker}(\varphi) \twoheadrightarrow \text{Im}(\varphi).$$

根据定义， $\varphi(g) = 1$ 当且仅当 $g \in \text{Ker}(\varphi)$ ，所以该同态也是单射，从而为同构。

注[术语: 短正合列] 给定群同态 $\varphi: H \rightarrow G$ 和 $\psi: G \rightarrow G'$ 。如果 φ 为单射, 我们把它记作是

$$1 \rightarrow H \xrightarrow{\varphi} G;$$

如果 ψ 为满射, 我们把它记作是

$$G \xrightarrow{\psi} G' \rightarrow 1;$$

如果 $\text{Im}(\varphi) = \text{Ker}(\psi)$, 我们把它记作是

$$H \xrightarrow{\varphi} G \xrightarrow{\psi} G'.$$

我们之后经常用到如下的短正合列:

$$1 \rightarrow H \xrightarrow{\varphi} G \xrightarrow{\psi} G' \rightarrow 1.$$

2.3 环的定义

定义 2.6

^a给定非空集合 A 。如果 A 上定义了乘法 \cdot 和加法 $+$, 即有映射

$$A \times A \rightarrow A, (a_1, a_2) \mapsto a_1 + a_2,$$

和

$$A \times A \rightarrow A, (a_1, a_2) \mapsto a_1 \cdot a_2,$$

并且存在元素 $0_A, 1_A \in A$, $0_A \neq 1_A$, 使得

- 1) $(A, +)$ 是交换群, 其中, 0_A 是加法单位元;
- 2) \bullet 乘法具有结合律, 即对任意的 $a_1, a_2, a_3 \in A$, 有 $(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3)$;
 \bullet 1_A 是乘法单位元, 即对任意的 $a \in A$, 有 $1_A \cdot a = a \cdot 1_A$;
- 3) 乘法分配律成立: 对任意的 $a_1, a_2, a_3 \in A$, 有

$$(a_1 + a_2) \cdot a_3 = a_1 \cdot a_3 + a_2 \cdot a_3, \quad a_3 \cdot (a_1 + a_2) = a_3 \cdot a_1 + a_3 \cdot a_2.$$

我们就称 $(A, \cdot, +)$ 或 A 是一个环。

^a更一般的环的定义不要求有乘法单位元, 这里的定义在一些文献中被称作是么环。



注 对任意的 $a \in A$, $0 \cdot a = a \cdot 0 = 0$ 。

注 A 是环。对任意的 $a \in A$, 我们用 $-a$ 表示其加法的逆元, 即 $a + (-a) = (-a) + a = 0$ 。我们还用 $a - b$ 表示 $a + (-b)$ 。根据结合律, 容易看出 $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$, 我们把它简写成 $-a \cdot b$ 或者 $-ab$, 这里, 我们常用 ab 表示 $a \cdot b$ 。

注 如果对任意的 $a, b \in A$, 都有 $a \cdot b = b \cdot a$, 我们就称 A 是交换环。

注 A 是环, 对任意的 $a \in G$, 如果存在 $a' \in A$, 使得 $a \cdot a' = 1$, 我们就称 a' 是 a 的一个右逆; 如果存在 $a'' \in A$, 使得 $a'' \cdot a = 1$, 我们就称 a'' 是 a 的一个左逆。假设 a 既有左逆又有右逆, 那么, 它们必然相同 (都等于 $a''aa'$) 并且唯一, 我们把它称作是 a 的逆。

注 K 是环。如果每个非零的 $\lambda \in K$ 均有逆, 那么 K 是域。

简而言之，域中可以做加减乘除（通过乘以逆）的四则运算，而环中可以做除了除法之外的运算。**注** 我们并不要求域 K 中的乘法是交换的。但是在本课程几乎所有的场合， K 都是交换的。

练习 2.2 我们用 A^\times 表示环 A 中的具有逆的元素（即有左逆又有右逆）的全体。证明， (A^\times, \cdot) 是群。

例题 2.20 对于 $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ 或 \mathbb{C} ，使用通常的乘法和加法运算，它们都是交换环。实际上，除了 \mathbb{Z} 之外，其余的环均为域。

例题 2.21 $M_n(A)$ 是环 A 上 $n \times n$ 的矩阵的集合，其中 A 是环。那么，在矩阵的加法和乘法下¹， $M_n(A)$ 是环，其中，单位矩阵和零矩阵对应着 $1_{M_n(A)}$ 和 $0_{M_n(A)}$ 。一般而言， $n \geq 2$ ， $M_n(A)$ 不是交换环。

对于域 K ，按定义，我们有 $M_n(A)^\times = \text{GL}(n, K)$ 。

例题 2.22 除了加法结构，我们在 $\mathbb{Z}/n\mathbb{Z}$ 上定义乘法 $\bar{k} \cdot \bar{l} = \overline{k \cdot l}$ 。不难验证，这是良好定义的。 $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ 是交换环。

如果 n 是合数，不妨假设 $n = n_1 \cdot n_2$ ，其中， $n_1, n_2 \geq 2$ 。那么， $\bar{n}_1 \cdot \bar{n}_2 = \bar{n} = 0$ 。很明显， \bar{n}_1 和 \bar{n}_2 均非零，所以，此时 $\mathbb{Z}/n\mathbb{Z}$ 不是域。

如果 p 是素数，那么，对任意的非零的 $\bar{k} \in \mathbb{Z}/p\mathbb{Z}$ ， k 是某个与 p 互素的整数。特别的， $(k, p) = 1$ 。那么，存在 $a, b \in \mathbb{Z}$ ，使得 $ak + bp = 1$ ，即 $\overline{ak} = 1$ ，从而 $\overline{ak} = 1$ 。这表明 k 有逆，从而 $\mathbb{Z}/p\mathbb{Z}$ 是域。

从此往后，对素数 p ，我们用 \mathbb{F}_p 表示域 $\mathbb{Z}/p\mathbb{Z}$ 。

例题 2.23 A 是环 A ，我们用 $A[X]$ 表示 A 上以 X 为不定元的多项式²的全体。每个非零的 $P \in A[X]$ ，均形如 $P(X) = \sum_{k=0}^n a_k X^k$ ，其中， $a_k \in A$ ， $a_n \neq 0$ 。我们把 n 称作是 P 的次数，并记作 $\deg P$ 。多项式之间的乘法和加法形式上与传统的做法一致，这给出了多项式环 $A[X]$ 。

- 如果 A 是交换环，那么， $A[X]$ 也是交换环。
- 如果 K 是域，那么，对任意的非零的 $P, Q \in K[X]$ ， $\deg(P \cdot Q) = \deg(P) + \deg(Q)$ 。
- 试举出例子， $P, Q \in A[X]$ 是非零多项式，但是 $P \cdot Q = 0$ 。

例题 2.24 给定拓扑空间 X ，那么，其（复值）连续函数空间 $C(X)$ 是环。某空间上函数所构成的环在数学中是环的重要例子。

定义 2.7

A 是环， $B \subset A$ 为其加法群的子群。如果 $1_A \in B$ 并且对任意的 $a, b \in B$ ， $a \cdot b \in B$ ，我们就称 B 是 A 的子环。



注 使用环 A 上的乘法和加法， A 的子环 B 具有自然的环结构。

例题 2.25 \mathbb{Z} 是 \mathbb{Q} 的子环但是不是子域，而 \mathbb{Q} 和 \mathbb{R} 都是 \mathbb{C} 的子域。

¹为了定义两个矩阵的乘法和加法，我们只用到了分量上的乘法和加法并且不需要使用乘法的逆或者交换律。

²注意，多项式不是函数。

定义 2.8 (环同态)

$(A_1, +_1, \cdot_1)$ 和 $(A_2, +_2, \cdot_2)$ 是环, $\varphi: A_1 \rightarrow A_2$ 是映射。如果该映射保持加法和乘法, 即对任意的 $a, b \in A_1$, 有

$$\varphi(a +_1 b) = \varphi(a) +_2 \varphi(b), \quad \varphi(a \cdot_1 b) = \varphi(a) \cdot_2 \varphi(b),$$

并且 $\varphi(1_{A_1}) = 1_{A_2}$ 。我们就称 φ 是以上两个环之间的环同态。我们用 $\text{Hom}(A_1, A_2)$ 表示它们之间所有的环同态。如果 φ 还是双射, 我们称 φ 是它们之间的一个环同构。如果 A_1 与 A_2 之间存在环同构, 我们就称这两个环是同构的并记作是 $A_1 \simeq A_2$ 。



注 假设 $\varphi \in \text{Hom}(A_1, A_2)$ 是环同态并且是双射, 那么 (按照定义验证即可), $\varphi^{-1} \in \text{Hom}(A_2, A_1)$ 。

注 对任意的 $\varphi \in \text{Hom}(A_1, A_2)$, 我们定义该映射的核为:

$$\text{Ker}(\varphi) = \{a \in A_1 \mid \varphi(a) = 0_{A_2}\}.$$

这是 A_1 的加法群的子群, 但是 $\text{Ker}(\varphi)$ 并非子环 ($1_{A_1} \notin \text{Ker}(\varphi)$)。

很明显, φ 为单射当且仅当 $\text{Ker}(\varphi) = \{0\}$ 。

例题 2.26 我们有自然的环同态

$$\mathbb{Z} \xrightarrow{\text{mod } n} \mathbb{Z}/n\mathbb{Z}, \quad k \mapsto \bar{k}.$$

其中, $\text{Ker}(\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}) = n\mathbb{Z}$ 。

引理 2.1 (常用)

K 是域, A 是环, $\varphi: K \rightarrow A$ 是环同态, 那么, φ 是单射。



证明 实际上, 对任意的 $k \in K^\times$, 我们有

$$\varphi(k) \cdot \varphi(k^{-1}) = \varphi(k \cdot k^{-1}) = \varphi(1) = 1.$$

所以, $k \notin \text{Ker}(\varphi)$ 。

2.4 对称群 \mathfrak{S}_n

我们现在研究 \mathfrak{S}_X , 其中 X 是有限集时。不妨假设 $X = \{1, 2, \dots, n\}$, 此时, 我们把 \mathfrak{S}_X 记作是 \mathfrak{S}_n 。按照定义, $g \in \mathfrak{S}$ 是一个 $\{1, 2, \dots, n\}$ 到自身的双射, 从而,

$$g: 1 \mapsto i_1, 2 \mapsto i_2, \dots, n \mapsto i_n,$$

其中, $\{1, 2, \dots, n\} = \{i_1, i_2, \dots, i_n\}$ 。这里, (i_1, i_2, \dots, i_n) 是 $\{1, 2, \dots, n\}$ 的一个排列组合。据此, 我们可以把 g 写成

$$g = \begin{bmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{bmatrix}$$

很明显, $|\mathfrak{S}_n| = n!$ 。

当 $n=2$ 和 3 时, 我们可以直接搞清楚群的结构。

\mathfrak{S}_2 只有两个元素 $\{1, g = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}\}$, 其中, $g^2 = 1$ 。所以, $\mathfrak{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ 。

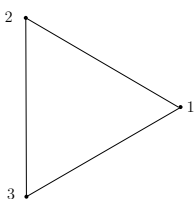
\mathfrak{S}_3 有 6 个元素

$$\left\{ 1, r = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}, s = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \right\}$$

我们可以直接验证:

$$r^2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}, sr = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, sr^2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$

另外, $r^3 = 1 = s^2$ 并且 $srs = r^{-1}$ 。根据我们对 \mathfrak{D}_3 的计算, 以上关系决定了群中元素的乘法。所以, \mathfrak{S}_3 与 \mathfrak{D}_3 是同构的。实际上, 我们考虑如下标号的正三角形:



对于 $g \in \mathfrak{D}_3$, 它把顶点 1 映射成顶点 i_1 , 2 映射成顶点 i_2 , 3 映射成顶点 i_3 , 从而, g 可以被看作是 \mathfrak{S}_3 中的元素 $\varphi(g)$ 。这就定义了

$$\varphi: \mathfrak{D}_3 \rightarrow \mathfrak{S}_3.$$

可以说明, 这是群同态。这实际上是我们之后要引入的群作用的想法。另外, 以上 i_1, i_2, i_3 恰好决定了 g , 从而以上映射是单射。另外, 以上两个群都是 6 阶群, 所以, φ 是同构。另外, 我们看到 \mathfrak{D}_3 的 r 和 s (这是以过点 1 和原点为轴的对称) 的作用恰好对应着 \mathfrak{S}_3 中的 r 和 s 。

我们现在把 \mathfrak{S}_n 中的元素分解成所谓的循环的乘积, 其中, $n \geq 1$ 。我们定义 $\{1, \dots, n\}$ 到自身的双射 σ 。给定 $k \leq n$ 和 k 元子集 $\{x_1, \dots, x_k\} \subset \{1, \dots, n\}$, 我们要求

$$\sigma(x) = \begin{cases} x, & x \notin \{x_1, \dots, x_k\}; \\ x_{i+1}, & x \in \{x_1, \dots, x_{k-1}\}; \\ x_1, & x = x_k. \end{cases}$$

这个映射可以如下形象地表示为 $\{x_1, \dots, x_k\}$ 的“轮换”(其他元素不变):

$$x_1 \mapsto x_2 \mapsto \dots \mapsto x_k \mapsto x_1.$$

我们把这样的 σ 称作是一个 k -循环并记作是 (x_1, x_2, \dots, x_k) 。对于 2-循环 (x, y) , 我们还称它是对换, 这个对换把 x 和 y 对换而其余的数不变。另外, 对于 k -循环 (x_1, x_2, \dots, x_k) 和 l -循环 (y_1, y_2, \dots, y_l) , 如果 $\{x_1, \dots, x_k\} \cap \{y_1, \dots, y_l\} = \emptyset$, 我们就说它们是不交的。很明显, 不交的循环在 \mathfrak{S}_n 中是交换的。

给定 $\sigma = \begin{bmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{bmatrix} \in \mathfrak{S}_n$, 这里 σ 把 k 映射到 $\sigma(k)$ 。

首先, 从某个 x_1 出发, x_1 被映射到 x_2 , x_2 被映射到 x_3 , 如此往复, 必然³有某个 k (第

³根据 σ 是双射

一次出现此情形), 使得 x_k 又被映射到 x_1 。

其次, 在除掉以上 $\{1, 2, \dots, n\} - \{x_1, \dots, x_k\}$ 上重复以上过程。那么, 存在某个 x_{k+1} , x_{k+1} 被映射到 x_{k+2} , x_{k+2} 被映射到 x_{k+3} , 如此往复, 必然有某个 l (第一次出现此情形), 使得 x_{l+l} 被映射回到 x_{k+1} 。按照要求, 我们显然有 $\{x_1, x_2, \dots, x_k\} \cap \{x_{k+1}, x_{k+2}, \dots, x_{k+l}\} = \emptyset$ 。

继续下去, 我们就可以把 g 写成两两不相交的循环之积:

$$g = (x_1, x_2, \dots, x_k)(x_{k+1}, x_{k+2}, \dots, x_{k+l}) \cdots (x_s, \dots, x_n).$$

定理 2.2

每个 $g \in \mathfrak{S}_n$ 都可写成两两不交的循环之积并且这些循环是唯一的。特别地, 由循环构成的子集可以生成 \mathfrak{S}_n 。



我们把以上分解写成 $g = \sigma_1 \cdot \sigma_2 \cdots \sigma_m$ 的形式, 其中, 我们把 $\sigma_1, \dots, \sigma_m$ 是长度分别为 k_1, k_2, \dots, k_m 的循环并且 $k_1 \geq k_2 \geq \dots \geq k_m$, 我们还要求不动的元素对应着 1-循环。此时, 我们称 g 是一个 (k_1, \dots, k_m) -型的元素, 这里 $k_1 + \dots + k_m = n$ 。

我们考虑如下 \mathfrak{S}_8 中的元素作为例子:

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 5 & 1 & 3 & 7 & 8 \end{bmatrix},$$

那么, 以上定理给出的分解为 $\sigma = (1, 2, 4, 5)(3, 6)$ 。这是一个 $(4, 2, 1, 1)$ -型的元素。

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 7 & 8 & 1 & 6 & 4 & 5 \end{bmatrix},$$

那么, 以上定理给出的分解为 $\beta = (1, 2, 3, 7, 4, 8, 5)$ 。然而, 这是一个 $(7, 1)$ -型的元素。我们还有

$$\beta = (1, 2, 3, 5) \cdot (3, 7) \cdot (7, 4, 8).$$

注意到, 这些循环之间是相交的而定理中的分解要求循环是两两不交的。

给定 $g \in \mathfrak{S}_n$, 我们研究其共轭作用:

$$\text{Int}(g): \mathfrak{S}_n \rightarrow \mathfrak{S}_n, \sigma \mapsto g\sigma g^{-1}.$$

先考虑 $\sigma = (x_1, \dots, x_k)$ 是 k -循环的情形。此时, 我们有

$$(g \cdot \sigma \cdot g^{-1})(g(x_j)) = g(x_{j+1}), \quad x_{k+1} = x_1.$$

而对于 $x \notin \{x_1, \dots, x_k\}$, 我们有

$$(g \cdot \sigma \cdot g^{-1})(g(x)) = g(x).$$

据此,

$$g \cdot (x_1, \dots, x_k) \cdot g^{-1} = (g(x_1), \dots, g(x_k)).$$

特别地, 对于 (k_1, \dots, k_m) -型的元素 $\sigma \in \mathfrak{S}_n$, 其共轭 $\text{Int}(g)(\sigma)$ 具有相同的类型。另外, 给定两个 (k_1, \dots, k_m) -型的元:

$$\alpha = (x_1, \dots, x_{k_1})(x_{k_1+1}, \dots, x_{k_1+k_2}) \cdots (x_{k_1+\dots+k_{m-1}}, \dots, x_n)$$

和

$$\beta = (y_1, \dots, y_{k_1})(y_{k_1+1}, \dots, y_{k_1+k_2}) \cdots (y_{k_1+\dots+k_{m-1}}, \dots, y_n),$$

定义 g 为 $x_i \mapsto y_i$, 其中, $i = 1, \dots, n$. 那么, $g\alpha g^{-1} = \beta$. 从而,

命题 2.3

\mathfrak{S}_n 中的两个元素 α 和 β 共轭^a当且仅当它们具有相同的型。

^a即存在 $g \in \mathfrak{S}_n$, 使得 $g\alpha g^{-1} = \beta$.



作为应用, 由于 $4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1$, 所以, \mathfrak{S}_4 有 5 个共轭类。

定理 2.3

\mathfrak{S}_n 可以由所有的对换 $\{(x, y) | 1 \leq x < y \leq n\}$ 生成。进一步, 对于 $\sigma \in \mathfrak{S}_n$, 假设

$$\sigma = \sigma'_1 \cdot \sigma'_2 \cdots \sigma'_k = \sigma''_1 \cdot \sigma''_2 \cdots \sigma''_l,$$

是把 σ 写成对换乘积的两种方式, 那么, $k - l$ 是偶数。



证明 只要证明每个轮换 (x_1, x_2, \dots, x_k) 可以写成对换的乘积即可。实际上, 我们容易验证

$$(x_1, x_2, \dots, x_k) = (x_1, x_k) \cdots (x_1, x_3) \cdot (x_1, x_2).$$

或者, 我们有

$$(x_1, x_2, \dots, x_k) = (x_1, x_2) \cdot (x_2, x_3) \cdots (x_{k-1}, x_k).$$

根据 $\sigma'_1 \cdot \sigma'_2 \cdots \sigma'_k = \sigma''_1 \cdot \sigma''_2 \cdots \sigma''_l$, 我们得到

$$1 = \sigma''_1 \cdot \sigma''_2 \cdots \sigma''_l \cdot \sigma'_k \cdot \sigma'_2 \cdots \sigma'_1.$$

所以, 只需要证明如下结论: 如果 1 可以写成对换的乘积

$$1 = \sigma_1 \cdot \sigma_2 \cdots \sigma_m,$$

那么, m 是偶数。我们对 n (以及整个命题) 进行归纳: $n = 1$ 或者 2 是显然的。对于 $n \geq 3$, 我们先验证如下事实: 假设 $i, j, k < n$ 并且两两不同, 那么:

$$(a). (i, n)(j, k) = (j, k)(i, n), (b). (i, n)(i, j) = (i, j)(j, n), (c). (i, n)(j, n) = (i, j)(i, n).$$

如果在 $\{\sigma_1, \sigma_2, \dots, \sigma_m\}$ 中没有形如 (k, n) 的对换, 那么, σ 可以被看作是 \mathfrak{S}_{n-1} 中的元素。根据归纳假设, m 是偶数。否则, 我们可以利用 (a) 和 (b) 将 (i, n) 型的对换向右边替换。在调换过程中, 如果有 (i, n) 与 (j, n) 型的两个对换相邻, 我们可以用 (c) 消去其中的一个或者用 $(i, n)(i, n) = 1$ 消去这两个带 n 的对换。这种操作保证了 $\{\sigma_1, \sigma_2, \dots, \sigma_m\}$ 中至多有一个形如 (k, n) 的对换并且它 (如果存在) 只能是 σ_m 。我们现在证明这样的对换是不存在的。否则, 我们有

$$\sigma_m = \sigma_1 \cdot \sigma_2 \cdots \sigma_{m-1}.$$

左边 n 会被对换到其他的位置, 而右边所有对换都保持了 n , 矛盾。此时, 我们可以再次利用归纳假设完成证明。

定义 2.9

我们定义 \mathfrak{S}_n 中元素的指标为:

$$\varepsilon: \mathfrak{S}_n \rightarrow \{\pm 1\}, \sigma \mapsto \begin{cases} 1, & \text{可写成偶数个对换的乘积 (称为偶置换);} \\ -1, & \text{可写成奇数个对换的乘积 (称为奇数置换).} \end{cases}$$

这是一个群同态并且当 $n \geq 2$ 时是满射。我们定义

$$\mathfrak{A}_n = \text{Ker}(\varepsilon: \mathfrak{S}_n \rightarrow \{\pm 1\}),$$

即 \mathfrak{A}_n 为偶置换的全体。换而言之, 我们有如下正合列

$$1 \rightarrow \mathfrak{A}_n \xrightarrow{\subset} \mathfrak{S}_n \xrightarrow{\varepsilon} \mathbb{Z}/2\mathbb{Z} \rightarrow 1.$$



练习 2.3 证明, $\{\pm 1\}$ 在乘法下是群并且以上指标映射 ε 是群同态。

练习 2.4 $\sigma = (x_1, \dots, x_k)$ 是 k -循环, 计算 $\varepsilon(\sigma)$ 。

练习 2.5 证明, $|\mathfrak{A}_n| = \frac{1}{2}n!$, 其中, $n \geq 2$ 。

命题 2.4

假设 $n \geq 3$, 考虑 \mathfrak{A}_n 的两个子集:

$$A = \{(i, j)(k, l) \mid 1 \leq i, j, k, l \leq n, i \neq j, k \neq l\}, \quad B = \{(i, j, k) \mid 1 \leq i, j, k \leq n, i \neq j, i \neq k, k \neq j\}.$$

那么, $\langle A \rangle = \mathfrak{A}_n$, $\langle B \rangle = \mathfrak{A}_n$ 。



证明 $\langle A \rangle = \mathfrak{A}_n$ 由 \mathfrak{A}_n 的定义可得。现在证明 3-循环可以生成 \mathfrak{A}_n , 为此, 只要说明对任意的 $1 \leq i, j, k, l \leq n$, 其中, $i \neq j, k \neq l$, $(i, j)(k, l)$ 可以写成 3-循环的乘积。我们分情形讨论:

- $|\{i, j\} \cap \{k, l\}| = 2$, 显然。
- $|\{i, j\} \cap \{k, l\}| = 1$, 不妨假设 $j = l$ 。此时, $(i, j)(l, j) = (i, j, l)$ 。
- $|\{i, j\} \cap \{k, l\}| = \emptyset$, 我们有

$$(i, j)(k, l) = (i, j)(j, k)(j, k)(k, l) = (i, j)(j, k) \cdot (j, k)(k, l) = (i, j, k)(j, k, l).$$

综上所述, 命题得证。

例题 2.27 $(1, 2, 3)$ 这一个 3-循环即可生成 \mathfrak{A}_3 。

命题 2.5

假设 $n \geq 2$, 那么, 以下子集均生成 \mathfrak{S}_n :

- $S_1 = \{(1, k) \mid k = 2, \dots, n\}$;
- $S_2 = \{(k, k+1) \mid k = 1, \dots, n-1\}$;
- $S_3 = \{(1, 2), (1, 2, \dots, n)\}$ 。
- $S_4 = \{(i_0, j_0), (1, 2, \dots, n) \mid |i_0 - j_0| \text{ 与 } n \text{ 互素}\}$ 。



证明 对于 S_1 , 我们注意到 $(i, j) = (1, i)(1, j)(1, i)$, 从而所有对换在 $\langle S_1 \rangle$ 中。

对于 S_2 , 我们归纳地证明 $\langle S_2 \rangle \supset \mathfrak{S}_k$, 其中, $k \geq 2$ 。 $k=2$ 是显然的。假设 $\langle S_2 \rangle \supset \mathfrak{S}_k$, 那么, 对任意的 $i < k$, $(k, k+1)(i, k)(k, k+1) = (i, k+1)$, 这表明 $\langle S_2 \rangle$ 包含了 \mathfrak{S}_k 和所有的对换 $(i, k+1)$,

从而包含了 \mathfrak{S}_{k+1} , 这就完成了归纳证明。

对于 S_3 , 令 $g = (1, 2, \dots, n)$, 那么, $g^k(1) = k+1$, $g^k(2) = k+2$, 其中, $k \leq n-2$ 。据此, 我们知道

$$\text{Int}(g^k)((1, 2)) = (k, k+1), k = 0, 1, \dots, n-2.$$

所以, $\langle S_3 \rangle \supset S_2$, 命题得证。

对于 S_4 , 令 $l = |i_0 - j_0|$, 仿照 S_3 的情形, 利用内自同构 $\text{Int}(g^{\pm k})$, 我们只要 $|i - j| = l$, 那么, $(i, j) \in \langle S_4 \rangle$ 。我们观察到

$$\text{Int}(a + (k-2)l, a + (k-1)l)((a + (k-1), a + kl) = ((a + (k-2), a + kl).$$

我们还有

$$\text{Int}(a + (k-3)l, a + (k-2)l)((a + (k-2), a + kl) = ((a + (k-3), a + kl).$$

如此重复下去, 我们得到

$$\prod_{i=0}^{k-2} \text{Int}(a + il, a + (i+1)l)((a + (k-1), a + kl) = ((a, a + kl).$$

由于 l 与 n 互素, 我们选取 k , 使得 $kl \equiv 1 \pmod{n}$ 。此时, 我们回到了 S_3 的情形。实际上, S_2 也可以直接用这个方法证明。

对任意的群 G , 我们构造了群同态

$$\text{Int}: G \rightarrow \text{Aut}(G), g \mapsto \text{Int}(g).$$

其中, $\text{Ker}(\text{Int}) = Z(G)$ 。我们把 $\text{Aut}(G)$ 中形如 $\text{Int}(g)$ 形式的同构称作是 G 的**内自同构**。容易证明⁴, $\text{Im}(\text{Int}) \triangleleft \text{Aut}(G)$ 是正规子群, 我们定义群 G 的**外自同构群**为:

$$\text{Out}(G) = \text{Aut}(G) / \text{Im}(\text{Int}).$$

容易看出⁵, $Z(\mathfrak{S}_n) = 1$, 所以, \mathfrak{S}_n 的内自同构群与自身 \mathfrak{S}_n 同构。我们现在来刻画 \mathfrak{S}_n 的外自同构。

固定 \mathfrak{S}_n 到自身的同构 $\varphi \in \text{Aut}(\mathfrak{S}_n)$, 那么, 它把共轭的元素映射成共轭的元素, 所以, 把 \mathfrak{S}_n 的共轭类映射到 \mathfrak{S}_n 的共轭类 (可能是不同的共轭类)。我们考虑如下的共轭类:

$$T_k = \{g \in \mathfrak{S}_n \mid g \sim (1, 2)(3, 4) \cdots (2k-1, 2k)\},$$

其中, $2k \leq n$ 并且 \sim 表示共轭关系。对任意的对换 $\sigma \in T_1$, 由于 $\sigma^2 = 1$, 所以, $\varphi(\sigma)^2 = 1$ 。考虑 $\varphi(\sigma)$ 在轮换下的分解:

$$\varphi(\sigma) = (x_1, x_2, \dots, x_k)(x_{k+1}, x_{k+2}, \dots, x_{k+l}) \cdots (x_s, \dots, x_n),$$

容易看出, 只有每个循环的长度至多是 2 的时候, $\varphi(\sigma)^2 = 1$, 从而, $\varphi(\sigma)$ 落在某个 T_k 中。据此, 我们有双射 $\varphi: T_1 \rightarrow T_k$ 。现在来计算 T_k 中的元素个数:

$$|T_k| = \frac{1}{k!} \binom{n}{2} \binom{n-2}{2} \cdots \binom{n-2k+2}{2} = \frac{n(n-1) \cdots (n-2k+1)}{2^k k!}.$$

⁴参见第一次作业练习题 10

⁵参见第二次作业练习题 1

我们现在考虑方程 $|T_1| = |T_k|$:

$$\frac{n(n-1)}{2} = \frac{n(n-1) \cdots (n-2k+1)}{2^k k!} \Leftrightarrow 2^{k-1} = (n-2)(n-3) \cdots (n-k+1) \binom{n-k}{k}.$$

除 1, 2 之外, 任何两个连续的整数之积都要有奇素数的因子, 所以, 以上要求 $n-2 = n-k+1$, 即 $k=3$, 此时,

$$2^2 = (n-2) \binom{n-3}{3} \Rightarrow n=6.$$

容易验证, 除了以上情形之外⁶, $|T_1| = |T_k|$ 无解, 从而, $\varphi(T_1) = T_1$, 即 φ 将对换映射为对换。

现在假设 $n \neq 6$, 此时, φ 将对换映射为对换。我们考虑 \mathfrak{S}_n 的生成元的集合

$$\{\sigma_1 = (1, 2), \sigma_2 = (2, 3), \dots, \sigma_{n-1} = (n-1, n)\}.$$

我们称 σ_{k-1} 和 σ_k 是相邻的。如果以上两个元素不相邻, 那么, 它们是交换的。假设

$$\varphi((1, 2)) = (x_1, x_2), \varphi((2, 3)) = (y_1, y_2).$$

由于 (1, 2) 和 (2, 3) 不交换, 所以, (x_1, x_2) 和 (y_1, y_2) 不交换, 那么, $\{x_1, x_2\} \cap \{y_1, y_2\} \neq \emptyset$ 。通过重新标记, 我们可以假设

$$\varphi((1, 2)) = (x_1, x_2), \varphi((2, 3)) = (x_2, x_3).$$

再考虑 $\varphi((3, 4)) = (z_1, z_2)$ 。类似地推理给出 $\{x_2, x_3\} \cap \{z_1, z_2\} \neq \emptyset$, 然而, (1, 2) 和 (3, 4) 交换, 所以, (x_1, x_2) 和 (z_1, z_2) 不交换。据此, $\{x_2, x_3\} \cap \{z_1, z_2\} = \{x_3\}$ 。通过重新标号, 我们有 $\varphi((3, 4)) = (x_3, x_4)$ 。如此往复, 我们最终得到

$$\varphi((1, 2)) = (x_1, x_2), \varphi((2, 3)) = (x_2, x_3), \dots, \varphi((n-1, n)) = (x_{n-1}, x_n).$$

这表明我们可以选取

$$\sigma = \begin{bmatrix} 1 & 2 & \cdots & n \\ x_1 & x_2 & \cdots & x_n \end{bmatrix} \in \mathfrak{S}_n,$$

使得, $\varphi((k-1, k)) = \text{Int}(\sigma)((k-1, k))$ 。这些关系在 \mathfrak{S}_n 的生成元的集合上成立, 从而, $\varphi = \text{Int}(\sigma)$ 。综上所述, 我们证明了

定理 2.4

对 $n \neq 6$, 我们有 $\text{Out}(\mathfrak{S}_n) = 1$, 即 \mathfrak{S}_n 的每个自同构都是内自同构。



注 当 $n=6$ 时, 以上推理表明可能存在 φ , 使得 $\varphi: T_1 \rightarrow T_3$ 。此时, 我们必然有 $\varphi: T_3 \rightarrow T_1$ 。从而, $\varphi: T_1 \rightarrow T_1$ 。以上定理的证明对于 T^2 仍然适用, 从而, φ^2 是内自同构。实际上, 任意的两个自同构 $\varphi: T_1 \rightarrow T_3$ 和 $\varphi': T_1 \rightarrow T_3$, 我们都有 $\varphi \cdot \varphi': T_1 \rightarrow T_1$, 从而, $\varphi \cdot \varphi'$ 是内自同构。这说明, $\text{Aut}(\mathfrak{S}_6)/\text{Im}(\text{Int})$ 中至多有两个元素。从而, $\text{Out}(\mathfrak{S}_6) = 1$ 或者 $\mathbb{Z}/2\mathbb{Z}$ 。我们之后会证明 $\text{Out}(\mathfrak{S}_6) \neq 1$, 即 \mathfrak{S}_6 拥有非共轭作用的自同构。

⁶当 $n=6$ 时, 可能有 $\varphi(T_1) = T_3$, 我们之后会对 \mathfrak{S}_6 构造这种同构。

第3章 群与群作用

3.1 群的作用

定义 3.1

群 G 在集合 X 上的一个 (左) 作用指的是映射:

$$G \times X \longrightarrow X, (g, x) \mapsto g \cdot x,$$

它满足:

- 1) 对任意的 $x \in X$, 对任意的 $(g, g') \in G \times G$, 有 $g \cdot (g' \cdot x) = (gg') \cdot x$ 。
- 2) 对任意的 $x \in X$, $1_G \cdot x = x$ 。

我们通常用如下符号来记 $G \curvearrowright X$ 。



注 类似地, 我们还可定义群的右作用: 通过要求

$$X \times G \longrightarrow X, (x, g) \mapsto x \cdot g,$$

其中, 我们需要将上述定义中的第一条修正为: 对任意的 $(g, g') \in G \times G$, 有 $(x \cdot g) \cdot g' = x \cdot (gg')$ 。

我们通常用如下符号来记右作用 $X \curvearrowright G$ 。

注 给定 G 在 X 上的作用等价于给定从 G 到 X 的对称群 \mathfrak{S}_X 的群同态 τ 。实际上, 对所有的 $x \in X$ 和 $g \in G$, 有 $\tau(g)(x) = g \cdot x$, 所以, $\tau(g)$ 是 X 到自身的双射 (其逆为 $\tau(g^{-1})$)。根据定义中的 1),

$$\tau: G \rightarrow \mathfrak{S}_X, g \mapsto \tau(g)$$

是群同态。反之, 给定这样的 τ , 直接验证即知 $g \cdot x = \tau(g)(x)$ 是群 G 在 X 上的作用。

注 [轨道分解]

对于 X 中元素 x 和 y , 如果存在 $g \in G$, 使得 $x = g \cdot y$, 我们就说它们属于同一个轨道: $x \in X$ 的轨道定义

$$\text{orb}(x) = G \cdot x = \{g \cdot x \mid g \in G\}.$$

群 G 的作用将 X 分解为不同轨道的并。

实际上, 对于 $x, y \in G$ 的轨道 $\text{orb}(x)$ 和 $\text{orb}(y)$, 如果 $\text{orb}(x) \cap \text{orb}(y) \neq \emptyset$, 那么, $\text{orb}(x) = \text{orb}(y)$ 。因为我们可以选取 $g_1, g_2 \in G$, 使得 $g_1 \cdot x = g_2 \cdot y$ 。根据群作用的定义, $g_2^{-1} g_1 x = y$, 所以,

$$\text{orb}(y) = G \cdot y = (G \cdot g_2^{-1} g_1) x = G \cdot x = \text{orb}(x).$$

所以, X 的轨道分解给出了 X 上的等价关系。我们将 G 在 X 上 (左) 作用的轨道集合记为 $G \backslash X$ (右作用的情形记为 X / G)。

作为总结, $X = \coprod_{g \in G} \text{orb}(x) = \coprod_{G \backslash X} \text{orb}(x)$ 。

练习 3.1 对任意的 $\text{orb}(x) \in G \backslash X$, G 在该轨道上有自然的作用。

注 如果所有 X 中的点均落在同一个轨道中, 即 $|G \backslash X| = 1$, 我们就说 G 在 X 上的作用是传递的。特别地, G 在每个轨道上的作用是传递的。

由于 $X = \coprod_{G \backslash X} \text{orb}(x)$, 我们可以通过了解传递的群作用来理解 G 的作用。从这一点上我们可以想象轨道分解这个观点的重要性。

注 对任意的 $g \in G$, 如果 $g \cdot x = x$, 我们就称 x 是 g 的一个不动点。对任意的 $x \in X$, G 中使 x 不动的元素 g 所构成的子群, 被称作是 x 的稳定化子, 我们把它记作是

$$\text{Stab}_G(x) = \{g \in G \mid g \cdot x = x\}.$$

如果对任意的 $x \in X$, 有 $\text{Stab}(x) = 1$, 我们就称 G 的作用是自由的, 即除了单位元外, 任何的群元素都没有不动点。

另外, 如果除了 1_G 之外, 对任意的 g , 总有 $x \in X$, 使得 $g \cdot x = x$, 我们就称 G 的作用是忠实的。作用 $G \curvearrowright X$ 是忠实的当且仅当它所定义的群同态 $G \rightarrow \mathfrak{S}_X$ 是单射。

例题 3.11 维空间上的仿射变换 K 是域, 我们定义如下 K 到自身的映射的集合:

$$G = \{x \mapsto ax + b \mid a \in K^\times, b \in K\}.$$

以上集合在映射的复合下显然构成群, 我们把它称作是 1 维的仿射变换群。 G 显然在 K 上作用并且这个作用是传递的。对于 $x_0 \in K$, 我们有

$$\text{Stab}(x_0) = \{x \mapsto a(x - x_0) + x_0 \mid a \in K^\times\}.$$

所以, $\text{Stab}(x_0) \simeq K^\times$ 。

注 假设 G 在 X 上的作用是传递的, 那么, 对任意的 $x \in X$, 我们有双射

$$G/\text{Stab}(x) \rightarrow X, \quad g \cdot \text{Stab}(x) \mapsto g \cdot x,$$

其中, $G/\text{Stab}(x)$ 是左陪集的集合。(以上映射显然是满射。为了证明这是单射, 假设 $g \cdot \text{Stab}(x)$ 和 $g' \cdot \text{Stab}(x)$ 有同样的像, 那么, $g \cdot x = g' \cdot x$, 这表明 $g^{-1}g' \in \text{Stab}(x)$, 从而, $g \cdot \text{Stab}(x) = g' \cdot \text{Stab}(x)$ 。)

我们现在将 x 改为另外一个 $x' \in X$, 根据传递性, 存在 $g \in G$ 使得 $x' = g \cdot x$ 。此时,

$$\text{Stab}(x') = \text{Stab}(gx) = g \cdot \text{Stab}(x) \cdot g^{-1}.$$

(实际上, 我们有

$$hgx = gx \Leftrightarrow g^{-1}hgx = x.$$

从而 $g^{-1}\text{Stab}(x')g \subset \text{Stab}(x)$ 。) 所以, 基准点 x 的改变对应于其稳定化子的共轭变换。

反之, 给定 G 的子群 H , G 在 $X = G/H$ 可以通过左乘法进行作用 (对任意的 $g \in G$, 对任意的左陪集 $g'H \in G/H$, 我们定义 $g \cdot g'H = gg'H$)。这显然是传递的群作用并且 $H = \text{Stab}(H)$ 。

作为总结, 我们有: 给定一个 G 能传递地作用于其上的集合 X 等价于在模掉共轭的关系下给定 G 的一个子群。

注 G 是有限群, G 在集合 X 上的作用是传递的, 那么, X 是有限集并且 $|X| = |G|$ 。

例题 3.2 以上已经给出了如下典型的一个群的作用 (作用在由自身所定义的几何对象上): $H < G$ 是子群, $X = G/H$, G 可以通过左乘法作用在 X 上: 即对任意的 $g \in G$ 和左陪集 $g'H \in G/H$,

我们有 $g \cdot g'H = gg'H$ 。

假设 $H' < G$ 是另一个子群，那么，通过限制，我们仍然有 $H' \curvearrowright (G/H)$ 。此时， H' 的作用未必是传递的。对任意的 $g \in G$ ， $gH \in G/H$ 的稳定化子为

$$\text{Stab}(gH) = H' \cap gHg^{-1}.$$

这个计算表明，作用 $H' \curvearrowright (G/H)$ 的稳定化子与子群 H 的共轭相关联。

例题 3.3 假设 G 在 X 上作用，那么，对任意的 x ，以下自然的映射为双射：

$$G/\text{Stab}(x) \xrightarrow{\cong} \text{orb}(x), \quad g\text{Stab}(x) \mapsto g \cdot x.$$

根据上面的讨论，我们有

$$|G/\text{Stab}(x)| = |\text{orb}(x)|.$$

这就给出了如下公式：

定理 3.1 (轨道计数公式)

G 是有限群， G 在集合 X 上作用，我们假设 X 可以 G 的轨道分解为：

$$X = \coprod_{k=1}^m \text{orb}(x_k).$$

那么，

$$\frac{|X|}{|G|} = \sum_{k=1}^m \frac{1}{|\text{Stab}(x_k)|}.$$



例题 3.4 我们考虑 G 通过共轭作用于 G 本身，即

$$G \rightarrow \mathfrak{S}_G, \quad g \mapsto \text{Int}(g),$$

其中，对任意的 $x \in G$ ， $\text{Int}(g)(x) = gxg^{-1}$ 。我们称这个作用的轨道为 G 的共轭类，即对任意的 $x, y \in G$ ，它们落在同一个轨道中当且仅当存在 $g \in G$ ，使得 $gxg^{-1} = y$ 。给定 $x \in G$ ，它的稳定化子由是 G 中与 x 交换的元素所构成，即其中心化子 $C_x(G)$ 。根据以上轨道计数公式，我们有

$$1 = \sum_k \frac{1}{|C_{x_i}(G)|},$$

其中， x_i 为相应共轭类的代表元。

例题 3.5 p 是素数。如果一个群 G 的阶是 p 的幂，我们就称 G 群为 p -群。我们现在说明 $Z(G) \neq 1$ ，即 p -群有非平凡的中心。为此，我们考虑 G 通过共轭在 G 上的作用。此时，根据轨道公式，

$$p^f = |G| = \sum_{k=1}^m |\mathbf{O}_i| = 1 + \sum_{k=2}^m |\mathbf{O}_i|.$$

由于在共轭作用下， $\{1_G\}$ 是一个单独的轨道，所以，以上公式右边的第一个 1 代表着这个轨道的元素个数。然而，左边是 p 的倍数而右边每个轨道的元素个数是 p^f 的因子，所以，至少还有一个轨道，其元素个数也是 1。这个元素就在 $Z(G)$ 里面。

3.2 群作用的应用举例

3.2.1 Burnside 引理

我们证明如下关于轨道个数的计算公式：

命题 3.1 (Burnside)

假设有限群 G 作用在有限集 X 上，那么该作用的轨道个数是不动点个数的平均值，即

$$|G \backslash X| = \frac{1}{|G|} \sum_{g \in G} |X^g|. \quad (3.1)$$

其中，对任意的 $g \in G$ ， $X^g = \{x \in X | g \cdot x = x\}$ 。



证明 我们考虑集合 $G \times X$ 的子集：

$$S = \{(g, x) \in G \times X | g \cdot x = x\}.$$

我们有两种方式数 S 的元素个数。首先，根据 $S = \coprod_{g \in G} X^g$ ，我们有

$$|S| = \sum_{g \in G} |X^g|.$$

其次，根据 $S = \coprod_{x \in X} \text{Stab}(x)$ ，我们有

$$|S| = \sum_{x \in X} |\text{Stab}(x)| = \sum_{x \in X} \frac{|G|}{|\text{orb}(x)|}.$$

所以，

$$\sum_{x \in X} \frac{1}{|\text{orb}(x)|} = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

另外，我们有

$$\sum_{x \in X} \frac{1}{|\text{orb}(x)|} = \sum_{\text{orb}(x_i) \in G \backslash X} \left(\sum_{x \in \text{orb}(x_i)} \frac{1}{|\text{orb}(x)|} \right) = \sum_{\text{orb}(x_i) \in G \backslash X} 1 = |G \backslash X|.$$

这就给出了证明。

例题 3.6 有多少个 4 个顶点的简单图（顶点之间至多连一条边）？

固定 4 个点，在它们之间连或者不连边，这样构成的可能的图有 $2^{\binom{4}{2}} = 64$ 种，这是我们的构形空间 X 。对于 $G = \mathfrak{S}_4$ ，通过对 4 个顶点的置换（从而置换相应的边）， \mathfrak{S}_4 作用在 X 上，我们要计算 $\mathfrak{S}_4 \backslash X$ 。

\mathfrak{S}_4 中的 24 个元素可以分成如下几类

- 1；共 1 个。此时，所有 X 种元素在此元素作用下不变，从而， $|X^g| = 64$ 。
- 对换 (ab) ；共 6 个。根据对称性，考虑 $g = (12)$ ，此时，从 1 出发到 2，3 或者 4 的边就确定了从 2 出发到 1，3 或者 4 的边，从而，我们有 $2^3 \times 2 = 16$ 个不动点，即 $|X^g| = 16$ ，这里后面的 $\times 2$ 是考虑 3 和 4 之间是否连接一条边。
- 双对换 $(ab)(cd)$ ；共 3 个。与上面类似，对于这样的 g ，我们有 $|X^g| = 16$ 。
- 3-轮换 (abc) ；共 8 个。不妨考虑 $g = (123)$ ，对于 1 而言，它和 2 以及 4 的连线情况决定了所有的可能，从而， $|X^g| = 4$ 。

- 4-轮换 $(abcd)$; 共 6 个。不妨考虑 $g = (1234)$, 对于 1 而言, 它和 2 以及 3 的连线情况决定了所有的可能, 从而, $|X^g| = 4$ 。

根据 Burnside 引理, 我们就有

$$|\mathfrak{S}_4 \backslash X| = \frac{1}{24} (64 + 6 \times 16 + 3 \times 16 + 8 \times 4 + 6 \times 4) = 11.$$

所以, 一共有 11 个四顶点的简单图。

例题 3.7 单位圆上平均分布着 n 个点, 每个点可以染 m 种颜色。如果通过旋转, 两个图像是一样的, 我们就认为这两个染色方式是一样的。试问一共有多少种不同的染色?

对这 n 个点任意进行 m -染色, 共有 m^n 种方式, 这是构形空间 X 。对于这 n 个点的旋转对称群 $G = \mathbb{Z}/n\mathbb{Z}$, 通过对顶点的置换, G 作用在 X 上, 我们要计算 $G \backslash X$ 。

对于 $\mathbb{Z}/n\mathbb{Z}$ 中的元素 $g = \bar{k}$, 其中, $k \in \{0, 1, \dots, n-1\}$, 在 g 作用下不变的染色一共有 $m^{(n,k)}$, 其中, (n, k) 为这两个数的最大公约数。根据 Burnside 引理, 我们就有

$$|G \backslash X| = \frac{1}{n} \sum_{k=0}^{n-1} m^{(n,k)}.$$

特别地, 如果 $n = 4$, $m = 3$, 那么,

$$|G \backslash X| = \frac{1}{4} (3^4 + 3^1 + 3^2 + 3^1) = 24.$$

3.2.2 \mathfrak{S}_6 非共轭的自同构

首先, 我们有自然的作用 $\mathfrak{S}_6 \curvearrowright \{1, 2, 3, 4, 5, 6\}$ 。其次, 我们可以把 \mathfrak{S}_5 视作是某个 i 的稳定化子 $\text{Stab}(i)$, 其中, $i = 1, \dots, 6$ 。这就自然地 (有 6 种方式) 将 \mathfrak{S}_5 实现为 \mathfrak{S}_6 的子群。

现在作如下假设:

(•) $H < \mathfrak{S}_6$ 是具有 120 个元素的子群并且 $H \curvearrowright \{1, 2, 3, 4, 5, 6\}$ 是传递的。

很明显, 以上 6 种 \mathfrak{S}_5 到 \mathfrak{S}_6 嵌入所给出的子群并不满足上述假设。

定义 $X = \mathfrak{S}_6/H$ 是左陪集的集合, 那么, \mathfrak{S}_6 通过左乘法自然地作用在 X 上, 即对任意的 $g \in \mathfrak{S}_6$, 我们定义

$$g \cdot g_i H = (gg_i)H,$$

其中, $i = 0, 1, 2, 3, 4, 5$ 而 g_i 是左陪集中的代表元并且 $g_0 \in H$ 。所以, 我们构造了群同态

$$f: \mathfrak{S}_6 \longrightarrow \mathfrak{S}_X.$$

现在考虑这个作用在 H 上的限制 $H \curvearrowright X$, 由于 $H < \text{Stab}(g_0 H)$, 所以, 以上作用实际上给出了 $H \curvearrowright Y = \{g_1 H, g_2 H, g_3 H, g_4 H, g_5 H\}$ 。特别地, 我们有群同态

$$\varphi: H \longrightarrow \mathfrak{S}_Y \simeq \mathfrak{S}_5, \quad h \mapsto (g_i H \mapsto hg_i H).$$

我们证明, $\text{Ker}(\varphi) = N = 1$ 。实际上, 假设 $h \in N < H$, 那么, 对任意的 g_i , 我们都有 $g_i^{-1} h g_i \in H$, 从而, 对任意的 $g \in \mathfrak{S}_6$, $g^{-1} h g \in H$, 这表明 \mathfrak{S}_6 正规子群 $N' = \langle g N g^{-1} | g \in \mathfrak{S}_6 \rangle < H$ 。然而, \mathfrak{S}_6 的唯一非平凡的正规子群¹为 \mathfrak{A}_5 , 其指标为 2。由于 H 的指标为 6, 所以, N' 的指标至少是 6,

¹参见第二次作业的 B5)

从而, $N' = 1$, 这表明 $N = 1$ 。所以, φ 是单射。而 $|H| = |\mathfrak{S}_Y|$, 所以, φ 是群同构。

以上的讨论可以用如下的交换图表示:

$$\begin{array}{ccc} \mathfrak{S}_6 & \xrightarrow{f} & \mathfrak{S}_X \\ \uparrow & & \uparrow \\ H & \xrightarrow[\sim]{\varphi} & \mathfrak{S}_Y \end{array}$$

以上 f 必然为同构: 否则, $\text{Ker}(f) \simeq \mathfrak{A}_6$, 从而, $\text{Im}(f)$ 只有两个元素, 然而, H 的像就有至少 120 个元, 矛盾。

将 \mathfrak{S}_X 等同为 \mathfrak{S}_6 , 以上 f 就定义出 $\text{Aut}(\mathfrak{S}_6)$ 中的元素, 我们现在说明, f 不是内自同构。实际上, $f^{-1}(\mathfrak{S}_Y) = H$, 其中, \mathfrak{S}_Y 恰好是以上提到的 \mathfrak{S}_5 到 \mathfrak{S}_6 的 6 种标准的嵌入之一 (因为 $\mathfrak{S}_Y = \text{Stab}(g_0 H)$)。如果 f 是内自同构, 那么, f^{-1} 也是, 从而, $f^{-1}(\mathfrak{S}_Y) = H$ 也是固定某个元素所给出的 $\mathfrak{S}_5 \hookrightarrow \mathfrak{S}_6$, 然而, H 的作用是传递的, 矛盾。

我们转而构造 \mathfrak{S}_6 的满足以上 (\bullet) 的子群 H 。

考虑有限域 $\mathbb{F}_5 = (\mathbb{Z}/5\mathbb{Z}, +, \cdot)$ 上的标准 2 维线性空间 $V = \mathbb{F}_5 \oplus \mathbb{F}_5$ 。令 $\mathbf{P}^1(\mathbb{F}_5)$ 为 V 中的 1 维线性子空间的集合 (\mathbb{F}_5 上的 1 维射影空间), 它具有 6 个元素, 我们将它们标记为

$$\mathbf{P}^1(\mathbb{F}_5) = \{\ell_1, \ell_2, \ell_3, \ell_4, \ell_5, \ell_\infty\},$$

其中, ℓ_k 为 $(1, k)$ 所决定的 1 维线性子空间, 其中, $k = 1, \dots, 5$ 而 ℓ_∞ 为 $(0, 1)$ 所决定的 1 维线性子空间。

首先, 通过矩阵对向量的乘法, 群 $\mathbf{GL}(2; \mathbb{F}_5)$ 在 V 上有自然的作用。由于以上作用把 V 的 1 维线性子空间映射为 1 维线性子空间, 所以, 我们有 $\mathbf{GL}(2; \mathbb{F}_5) \curvearrowright \mathbf{P}^1(\mathbb{F}_5)$, 即有群同态

$$\mathbf{GL}(2; \mathbb{F}_5) \longrightarrow \mathfrak{S}_{\mathbf{P}^1(\mathbb{F}_5)}.$$

另外, $\mathbf{GL}(2; \mathbb{F}_5)$ 中的对角矩阵所构成的子群 D^\times 在 $\mathbf{P}^1(\mathbb{F}_5)$ 上的作用是平凡的。实际上, 通过简单计算, 我们知道

$$D^\times = \text{Ker}(\mathbf{GL}(2; \mathbb{F}_5) \rightarrow \mathfrak{S}_{\mathbf{P}^1(\mathbb{F}_5)}).$$

根据命题 2.2, 我们有单同态

$$\mathbf{GL}(2; \mathbb{F}_5) / D^\times \longrightarrow \mathfrak{S}_{\mathbf{P}^1(\mathbb{F}_5)} \simeq \mathfrak{S}_6.$$

令 $\mathbf{PGL}(2; \mathbb{F}_5) := \mathbf{GL}(2; \mathbb{F}_5) / D^\times$ 并且把, 我们就有单的群同态

$$\varphi: \mathbf{PGL}(2; \mathbb{F}_5) \longrightarrow \mathfrak{S}_6.$$

另外, $|\mathbf{GL}(2; \mathbb{F}_5)| = (5^2 - 1)(5^2 - 5)$ (第一列有 $5^2 - 1$ 个不同的向量, 第二列要与第一列线性无关, 所以只有 $5^2 - 5$ 个向量), 从而,

$$|\mathbf{PGL}(2; \mathbb{F}_5)| = \frac{1}{4} |\mathbf{GL}(2; \mathbb{F}_5)| = 120.$$

据此, $H = \text{Im}(\varphi) < \mathfrak{S}_6$ 是 120 阶的子群。另外, $\mathbf{GL}(2; \mathbb{F}_5)$ 在 $\mathbf{P}^1(\mathbb{F}_5)$ 上的作用是传递的, 所以, H 的作用也是传递的。

3.2.3 Sylow 定理

定义 3.2

G 是有限群, p 是素数, $|G| = n = p^k m$, 其中, $k \geq 1$, $(p, m) = 1$ 。如果 $S < G$ 是子群并且 $|H| = p^k$, 我们就称 S 是 G 的 Sylow p -子群或是 p -Sylow 子群。



注 Sylow p -子群 S 的共轭, 即形如 gSg^{-1} 的群, 仍然是 Sylow p -子群。特别地, G 可以 (通过共轭) 作用在所有 Sylow p -子群的集合上。我们将证明, 这个作用是传递的。从而, G 的 Sylow p -子群的个数整除 G 。

注 给定群 G 的子群 S , S 为 Sylow p -子群当且仅当 S 为 p -群且 $[G:S]$ 与 p 互素。

我们给出了两个具体的 Sylow p -子群的例子:

例题 3.8 令 $G = \mathbb{Z}/n\mathbb{Z}$, 其中 $n = p^k m$, $p \nmid m$ 。我们有自然同构²

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p^k\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

上式中右边第一个因子 (在乘积中形如 $(*, 1)$ 的元素) $\mathbb{Z}/p^k\mathbb{Z}$ 是唯一的 Sylow p -子群。

如果从上式子左边来看, 这个 Sylow p -子群中的元素恰好是 $\mathbb{Z}/n\mathbb{Z}$ 中 $\text{mod } m$ 得 1 的元素的全体, 这是因为上述同构由

$$\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/p^k\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, \quad \bar{a} \mapsto (a \pmod{p^k}, a \pmod{m}),$$

给出。

例题 3.9

K 是特征为 p 的有限域, 其元素个数为 $q = p^f$ 。我们将在后面的课程中构造这样的域。以下不妨假设 $K = \mathbb{Z}/p\mathbb{Z}$, 此时, $f = 1$, $q = p$ 。令 $G = \mathbf{GL}(n; K)$, 即 K 上 $n \times n$ 的可逆矩阵群。通过考虑 G 中元素每一列上的向量可能的选择, 利用乘法原理, 我们可以计算 G 的阶:

$$|G| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}) = p^{f \frac{n(n-1)}{2}} m, \quad m = \prod_{i=1}^n (q^i - 1).$$

我们注意到 $(p, m) = 1$ 。

令 S 为对角线上全为 1 的上三角矩阵所构成的子群, 它阶为明显是 $q^{\frac{n(n-1)}{2}} = p^{f \frac{n(n-1)}{2}}$ 。从而, S 是 G 的 Sylow p -子群。

例题 3.10 p 是素数, $|\mathfrak{S}_p| = p!$ 。那么, 由 p -循环 (x_1, x_2, \dots, x_p) 所生成的循环群给出了 \mathfrak{S}_p 中所有的 Sylow p -子群, 一共有 $\frac{1}{p}(p!) \div (p-1) = (p-2)!$ 个这样的 Sylow p -子群。根据 Wilson 定理, $(p-2)! \equiv 1 \pmod{p}$, 这是 Sylow 定理的一部分。

注 根据 Cayley 定理³, 每个有限群可以视作是某个对称群 \mathfrak{S}_n 的子群。实际上, 我们可以把有限群实现为一般线性群 $\mathbf{GL}(n; K)$ 的子群。

假设群 G 的阶为 n , 根据 Cayley 定理的证明, 通过左乘法 G 可以在自身上作用, 从而嵌入对称群 $\mathfrak{S}_G \simeq \mathfrak{S}_n$ 。我们再把 \mathfrak{S}_n 嵌入 $\mathbf{GL}(n; K)$ 中: 给定 $(e_i)_{1 \leq i \leq n}$ 为 K^n 的标准的基, 对任意

²参考第一次作业 A4)

³第一次作业练习题 14

的 $\sigma \in \mathfrak{S}_n$, 我们把 σ 映射成到线性变换 $e_i \mapsto e_{\sigma(i)}$, 其中, $i = 1, \dots, n$. 容易验证, 这个对应方式给出了 (单的) 群同态 $\mathfrak{S}_n \hookrightarrow \mathbf{GL}(n; K)$. 综上所述, 我们把 G 实现为 $\mathbf{GL}(n; K)$ 的子群. 在应用时, 我们通常选取 $K = \mathbb{F}_p$.

命题 3.2

G 是有限群, $|G| = n = p^k m$, 其中, p 是素数. S 是 G 的 Sylow p -子群, $H < G$ 为子群. 那么, 存在 $g \in G$, 使得 $H \cap gSg^{-1}$ 是 H 的 Sylow p -子群. 换言之, 通过对大群的 Sylow p -子群共轭可得到子群的 Sylow p -子群.

证明 我们考虑 H 通过左乘法在 $X = G/S$ 上的作用. 由于 S 是 Sylow p -子群, 所以 $|X|$ 的元素个数与 p 互素. 另外, 我们知道 $H \curvearrowright X$ 的稳定化子都形如 $H \cap gSg^{-1}$, 其中 $g \in G$.

由于 X 是轨道的并, 所以, 存在某个轨道 $\mathbf{O} = Hx = HgS$, 其元素个数不是 p 的倍数. 另外, $x = gS$ 的稳定化子为 $H \cap gSg^{-1}$, 由于 S 是 Sylow p -子群, 所以, $H \cap gSg^{-1}$ 是 p -群. 另外, 根据 $|\mathbf{O}| |H \cap gSg^{-1}| = |H|$, 我们知道 $[H : H \cap gSg^{-1}] = |\mathbf{O}|$ 与 p 互素. 这表明 $H \cap gSg^{-1}$ 恰好是 H 的一个 Sylow p -子群.

作为应用, 我们有

定理 3.2 (Sylow 第一定理)

有限群有 Sylow p -子群.

证明 给定有限群 G , 根据上述讨论, G 可以被看作是 $\mathbf{GL}(n; \mathbb{F}_p)$ 的子群, 而我们已经构造了 $\mathbf{GL}(n; \mathbb{F}_p)$ 的 Sylow p -子群, 所以, G 也有 Sylow p -子群.

我们还可以通过构造其它的群作用给出新的证明,

Sylow 第一定理的另一证明 (Miller-Wielandt): 假设 $|G| = qm = p^k m$, 其中, q 是 p 的幂, $p \nmid m$. 我们用 X 表示 q 元子集所构成的集合:

$$X = \{A \subset G \mid |A| = q\}.$$

那么, $|X| = \binom{qm}{q}$. 我们接受如下的同余关系:⁴

$$\binom{qm}{q} \equiv m \pmod{p},$$

其中, q 是 p 的幂, $p \nmid m$.

⁴实际上, 我们在多项式环 $\mathbb{F}_p[T]$ 中工作: 由于当 $k \neq 0, p$ 时, $p \mid \binom{p}{k}$, 所以, 对任意的多项式 $f(T)$ 和 $g(T)$, 根据二项式公式, 我们都有

$$(f + g)^p = f^p + g^p.$$

据此, 我们还得到

$$\left(\sum_{i=1}^l f_i(T)\right)^p = \sum_{i=1}^l f_i(T)^p.$$

我们现在计算 $(1 + T)^{qm}$:

$$(1 + T)^{qm} = (1 + T^q)^m = 1 + mT^q + \dots.$$

另外, 直接对 $(1 + T)^{qm}$ 进行二项式展开, T^q 的系数是 $\binom{qm}{q}$, 所以在 \mathbb{F}_p 中, $\binom{qm}{q} = m$.

群 G 可以通过左乘法作用于 X :

$$G \times X \rightarrow X, (g, A) \mapsto gA = \{ga | a \in A\}.$$

由于 $|X|$ 与 p 互素, 我们可以找到 $G \curvearrowright X$ 的轨道 \mathbf{O} , 其元素数目与 p 互素。任意选定 $A \in \mathbf{O}$, 令 $S = \text{Stab}(A)$ 为 A 的稳定化子。根据 $|\mathbf{O}| = [G:S]$, 这表明 $p \nmid [G:S]$, 从而, $|S|$ 已包含了 $|G|$ 的所有的 p 的幂, 即 $q \parallel |S|$ 。另外, 任选 $a \in A$, 由于 S 是 A 的中心化子, 所以可以定义映射

$$S \rightarrow A, g \mapsto ga.$$

这显然是单射, 从而, $|S| \leq |A| = q$ 。再根据 $q \parallel |S|$, $q = |s|$, 所以, H 为 Sylow p -子群。

推论 3.1 (Cauchy)

如果 p 整除 $|G|$, 那么, G 有阶为 p 的元素。



证明 S 是 G 的 Sylow p -子群, 这里, $S \neq 1$ 。任意选取非单位元 $x \in S$, 它的阶整除 $|S|$, 从而, 为 p 的幂 p^m , 其中 $m \geq 1$ 。那么, $x^{p^{m-1}}$ 的阶为 p 。

注 进一步分析 Miller-Wielandt 证明中轨道的性质, 可以给出关于 Sylow p -子群的更多性质。考虑 $G \curvearrowright X$ 的轨道分解 $X = \coprod_i \mathbf{O}_i$ 并对每个 i , 选取 $A_i \in X_i$, 从而, $\mathbf{O}_i = GA_i$ 。令 $S_i = \text{Stab}(A_i)$ 为 A_i 的稳定化子, 我们还有 $|\mathbf{O}_i||S_i| = |G|$ 。在上述证明中, 我们已经说明了 $|S_i| \leq p^n$ 。现在考虑以下两种可能:

- 1) $|S_i| < p^n$, 那么, $p \parallel |\mathbf{O}_i|$;
- 2) $|S_i| = p^n$, 那么该稳定化子群 S_i 是 Sylow p -子群。反之亦然: 假设 S 是 Sylow p -子群, 那么, 对任意的 $g \in G$, 我们有 $Sg \in X$, 并且这个元素稳定化子恰好是 S 。实际上, 如果 Sylow p -子群 S 保持某个 $A \in X$ 不变, 即 $SA \subset A$, 那么, $A = Sa$, 其中, $a \in A$ (因为 $Sa \subset A$ 并且两个集合同阶)。这表明 S 恰为 X 中形如 Sa 的元素的稳定化子。这些元素恰好是 S 的所有右陪集, 所以共有 $|G/S| = m$ 个。

以上给出了所有 Sylow p -子群的刻画。我们现在利用轨道来计算 X 的元素个数: 综上所述, 有

$$\begin{aligned} |X| &= \sum_{|S_i| < p^n} |\mathbf{O}_i| + \sum_{|S_i| = p^n} |\mathbf{O}_i| \\ &\equiv 0 + sm \pmod{p}. \end{aligned}$$

其中, 对于后一个情况, 每个轨道恰好有 m 个元素。这样的轨道个数是 s , 也恰好有 s 个 Sylow p -子群。由于 $|X| \equiv m \pmod{p}$, 所以, $s \equiv 1 \pmod{p}$ 。命题得证。

以上的证明还表明 s 模 p 只依赖于 $|G|$ (这里不需要 $\binom{q^m}{q} \equiv m \pmod{p}$)。特别地, 我们已经知道群 $\mathbb{Z}/|G|\mathbb{Z}$ 只有一个 Sylow p -子群, 所以, $s \equiv 1 \pmod{p}$ 。我们之后将给出有限群的 Sylow p -子群的个数除 p 余 1 这个结论的另一个证明。

定理 3.3 (Sylow 第二定理)

G 是有限群, 那么, G 的每个 p -子群都包含在某个 Sylow p -子群中。另外, G 的 Sylow p -子群两两共轭并且其个数模 p 余 1。



引理 3.1

P 是 p -群并且作用在有限集 X 上, $X^P = \{x \in X | gx = x, \forall g \in G\}$ 。那么, $|X| \equiv |X^P| \pmod{p}$ 。♡

证明 X^P 中的每个元素恰对应着只有一个元素的轨道, 而集合 $X - X^P$ 是那些元素个数大于 1 的轨道的并。由于 P 是 p -群, 后一种轨道的元素个数是 p 的倍数。命题得证。

我们现在证明 Sylow 第二定理的第一个结论。假设 P 是 G 的一个 p -子群, 任意选定 Sylow p -子群 S , 令 $X = G/S$ 。考虑 P 通过左乘法在 X 上的作用。根据上述引理,

$$|X^P| \equiv |X| \not\equiv 0 \pmod{p}.$$

这表明有 $gS \in X$, 使得, 对任意的 $h \in P$, $hgS = gS$, 即 $g^{-1}Pg \subset S$ 。从而, $H < gSg^{-1}$, 这就完成了第一个结论的证明。如果 P 是 Sylow p -子群, 通过比较元素个数, 我们还有 $P = gSg^{-1}$, 这就说明了所有的 Sylow p -子群都共轭。

我们现在给出定理中关于 Sylow p -子群个数的第二个证明。这个证明依赖于下述引理:

引理 3.2

如果 S 和 S' 是 G 的 Sylow p -子群并且 S' 正规化 S , 即对任意 $s' \in S$, 我们有 $s'Ss'^{-1} \subset S$, 那么, $S = S'$ 。♡

证明 由于 S' 正规化 S , 所以 S' 是 S 的正规化子⁵ $N_G(S)$ 的 Sylow p -子群, 而 S 也是 $N_G(S)$ 的 Sylow p -子群。由于 $N_G(S)$ 在 S 上共轭作用是平凡的, 根据定理中的第二个结论, S 是 $N_G(S)$ 中唯一的 Sylow p -子群。所以, $S = S'$ 。

我们令 X 为 G 的全体 Sylow p -子群的集合, 那么, S 可以通过共轭作用于 X , 即

$$S \times X \rightarrow X, (g, S') \mapsto gS'g^{-1}.$$

上述引理表明 $S \in X$ 是唯一一个被 S 固定的元素。应用引理 3.1, 我们得到 $|X| \equiv 1 \pmod{p}$ 。

注 令 X 为 G 的全体 Sylow p -子群的集合, G 可以通过共轭作用于 X 。根据以上定理, G 的作用是传递的, 所以, Sylow p -子群的个数必能整除 $|G|$ 。

3.2.4 \mathfrak{S}_6 非共轭自同构另一个构造

我们注意到 $|\mathfrak{S}_5| = 120$, 假设它有 s 个 Sylow 5-子群, 那么, s 除 5 余 1, 所以,

$$s = 1, 6, 11, 16, 21, 26, 31, 36, 41, 46, 51, 56, 61, \dots$$

另外, $s | 120$, 据此, $s = 1$ 或者 6。另外, 5-循环 $(1, 2, 3, 4, 5)$ 和 $(2, 1, 3, 4, 5)$ 生成了两个不同的 Sylow 5-子群, 所以, $s \geq 2$, 从而, $s = 6$ 。我们还可以如下推理: 如果 $s = 1$, 我们知道这个 Sylow 5-子群是正规子群, 这不可能。⁶

令 $X = \{S_1, \dots, S_6\}$ 是这 6 个 Sylow 5-子群的集合。通过 \mathfrak{S}_5 在 X 上共轭作用, 我们有传递

⁵我们回忆 H 是群 G 的子群, H 在 G 中的正规化子为 $N_G(H) = \{g \in G | gHg^{-1} = H\}$ 。

⁶参考第二次作业的 B4)

的群作用：

$$\varphi: \mathfrak{S}_5 \rightarrow \mathfrak{S}_X \simeq \mathfrak{S}_6.$$

根据作用的传递性，我们知道 $|\text{Ker}(\varphi)| \leq 120 \div 6 = 20$ ，从而⁷， $\text{Ker}(\varphi) = 1$ ，即 φ 是单射。令 $H = \text{Im}(\varphi)$ ，那么， $H < \mathfrak{S}_X \simeq \mathfrak{S}_6$ 是具有 120 个元素的子群并且 ${}^H X$ 是传递的，请参考 3.2.2 节的条件 (•)。

⁷参考第二次作业的 B4)

第4章 群的结构与构造

4.1 半直积

G 是群, $N \triangleleft G$ 是正规子群, $K < G$ 是子群。我们注意到 $N \cdot K$ 是子群, 实际上, 对任意的 $n, n' \in N$ 和 $k, k' \in K$, 我们有

$$(nk) \cdot (n'k') = (n \cdot kn'k^{-1}) \cdot (kk'), \quad (nk)^{-1} = (k^{-1}n^{-1}k) \cdot k.$$

由于 N 是正规子群, 以上计算表明 $N \cdot K < G$ 。我们注意到, 通过共轭, K 可以自然地作用在 N 上:

$$\text{Int}: K \rightarrow \mathfrak{S}_N, \quad k \mapsto \text{Int}(k): n \mapsto gng^{-1}.$$

我们进一步假设 $N \cdot K = G$ 并且 $N \cap K = 1$ 。如果 $nk = n'k'$, 那么, $n^{-1}n' = kk'^{-1} \in N \cap K = 1$, 所以, $n = n'$ 并且 $k = k'$ 。据此, 我们知道

$$N \times K \rightarrow G, \quad (g, k) \mapsto gk$$

是 $N \times K$ 与 G 之间的双射。然而, 作为群 $N \times K$ 与 G 未必同构: 因为在 $N \times K$ 中, 对任意的 $n \in N$ 和 $k \in K$, $(n, 1)$ 与 $(1, k)$ 交换; 然而其像在 G 中

$$nk = kn \Leftrightarrow \text{Int}(k)(n) = n.$$

所以, G 未必与 $N \times K$ 同构, 这是因为 G 中的乘法实际上应该写成

$$(nk) \cdot (n'k') = (n \cdot kn'k^{-1}) \cdot (kk') = (n \cdot \text{Int}(k)(n')) \cdot (k \cdot k').$$

仿照以上的讨论, 我们首先给出如下的**基本数据**: 群 N , 群 K 和 K 在 N 上的作用¹ $\varphi: K \rightarrow \text{Aut}(N)$ 。作为集合, 我们定义

$$N \rtimes_{\varphi} K \stackrel{\text{set}}{:=} N \times K.$$

按定义, $N \rtimes_{\varphi} K$ 中的元素均形如 (唯一的表示) (n, k) , 其中, $n \in N, k \in K$ 。为了给出 $N \rtimes_{\varphi} K$ 的群结构, 我们定义如下的乘法: 对任意的 $(n, k), (n', k') \in N \rtimes_{\varphi} K$, 令

$$(n, k) \cdot (n', k') = (n \cdot_N \varphi(k)(n'), k \cdot_K k'),$$

并令 $1 = (1_N, 1_K)$ 为单位元。首先, 对任意的 $(n, k) \in N \rtimes_{\varphi} K$, 我们有

$$(n, k) \cdot (1_N, 1_K) = (n \cdot_N \varphi(k)(1_N), k \cdot_K 1_K) = (n \cdot_N 1_N, k) = (n, k),$$

和

$$(1_N, 1_K) \cdot (n, k) = (1_N \cdot_N \varphi(1_K)(n), 1_K \cdot_K k) = (1_N \cdot_N \text{id}(n), 1_K \cdot_K k) = (n, k).$$

其次, 我们验证结合律: 对任意的 $(n, k), (n', k'), (n'', k'') \in N \rtimes_{\varphi} K$, 我们有

$$((n, k) \cdot (n', k')) \cdot (n'', k'') = (n\varphi(k)(n'), kk')(n'', k'') = (n\varphi(k)(n') \cdot \varphi(kk')(n''), kk'k''),$$

¹由于 $\varphi: K \rightarrow \text{Aut}(N) \subset \mathfrak{S}_N$, 所以, 对任意的 k , k 不仅作为 N 上的双射, 它还是群同态。

以及

$$\begin{aligned}(n, k) \cdot ((n', k') \cdot (n'', k'')) &= (n, k) \cdot (n' \varphi(k')(n''), k' k'') = (n \varphi(k)(n' \varphi(k')(n'')), k k' k'') \\ &= (n \varphi(k)(n') \cdot \varphi(k)(\varphi(k')(n'')), k k' k'') = (n \varphi(k)(n') \cdot \varphi(k k')(n''), k k' k'').\end{aligned}$$

最终, 对任意的 $(n, k) \in N \rtimes_{\varphi} K$, 我们有

$$(n, k)^{-1} = (\varphi(k^{-1})(n^{-1}), k^{-1}).$$

以上构造给出了半直积的构造。特别地, 如果 K 在 N 上的作用是平凡的, 那么, $N \rtimes_{\varphi} K \simeq N \times K$ 。

练习 4.1 证明, 集合之间的双射

$$N \times K \rightarrow N \rtimes_{\varphi} K, \quad (n, k) \mapsto (n, k)$$

是群同构当且仅当 K 在 N 上的作用是平凡的。

注 假设 G 是群, $K < G$ 是子群, 如果存在子群 $H < G$, 使得 $H \cap K = 1$ 并且 $N \cdot K = G$, 我们就说 H 是 K 在 G 中的一个补子群。

假设 $N \triangleleft G$ 是正规子群并且是 K 在 G 中的补子群。在此情形下, K 在 N 上的作用由共轭给出, 上述的构造给出了 $G \simeq N \rtimes_{\varphi} K$ 。为了简单期间, 我们经常把 G 写成 $G = N \rtimes K$ 。然而, 这个写法很很容易让人迷惑, 我们将避而不用。

注 我们有自然的群同态 $\pi_2: N \rtimes_{\varphi} K \rightarrow K$, 其中, $\pi_2(n, k) = k$ 。这是个满同态。另外, $\text{Ker}(\pi_2) = (N, 1) \subset N \rtimes_{\varphi} K$ 。容易看出, $\text{Ker}(\pi_2)$ 与 N 同构。所以, 我们有群同态的正合列:

$$1 \rightarrow N \rightarrow N \rtimes_{\varphi} K \xrightarrow{\pi_2} K \rightarrow 1.$$

另外, 我们还有群同态

$$\phi: K \rightarrow N \rtimes_{\varphi} K, \quad k \mapsto (1, k).$$

并且 $\pi_2 \circ \phi = \text{id}$ 。在这个情形下, 我们称 ϕ 是 π_2 的提升。如果一个正合列有这种提升, 我们就称以上正合列是分裂的。

直观上, 知道了 G 的正规子群 N 和商群 G/N , 还需要知道 G/N 在 N 上的共轭作用, 就可以确定 G 的结构。

注[唯一性] 给定一组基本数据: 群 N , 群 K 和 K 在 N 上的作用 $\varphi: K \rightarrow \text{Aut}(N)$ 。假设存在群 N' 和群 K' 以及群同构

$$\alpha: N' \xrightarrow{\simeq} N, \quad \beta: K \xrightarrow{\simeq} K',$$

我们可以构造 K' 在 N' 上的自然作用

$$\varphi': K' \rightarrow \text{Aut}(N'), \quad k' \mapsto \alpha^{-1} \circ \varphi(\beta(k')) \circ \alpha.$$

这由如下交换图给出:

$$\begin{array}{ccc} N & \xrightarrow{\varphi(\beta(k'))} & N \\ \alpha \uparrow & & \alpha \uparrow \\ N' & \xrightarrow{\alpha^{-1} \circ \varphi(\beta(k')) \circ \alpha} & N' \end{array}$$

那么, 映射

$$\Psi: N' \rtimes_{\varphi'} K' \longrightarrow N \rtimes_{\varphi} K, \quad (n', k') \mapsto (\alpha(n'), \beta(k')),$$

是群同构。

很明显, 上述映射是双射。我们只要验证这是群同态:

$$\begin{aligned} \Psi((n'_1, k'_1) \cdot (n'_2, k'_2)) &= \Psi\left((n'_1 \varphi'(k'_1)(n'_2), k'_1 k'_2)\right) = \Psi\left((n'_1 (\alpha^{-1} \circ \varphi(\beta(k'_1)) \circ \alpha)(n'_2), k'_1 k'_2)\right) \\ &= \left(\alpha[(n'_1 (\alpha^{-1} \circ \varphi(\beta(k'_1)) \circ \alpha)(n'_2)], \beta(k'_1 k'_2)\right) \\ &= \left(\alpha(n'_1)(\varphi(\beta(k'_1))(\alpha(n'_2))), \beta(k'_1)\beta(k'_2)\right). \end{aligned}$$

另外,

$$\Psi(n'_1, k'_1) \cdot \Psi(n'_2, k'_2) = (\alpha(n'_1), \beta(k'_1)) \cdot (\alpha(n'_2), \beta(k'_2)) = \left(\alpha(n'_1)(\varphi(\beta(k'_1))(\alpha(n'_2))), \beta(k'_1)\beta(k'_2)\right).$$

比较以上两个式子, 这就完成了证明。

例题 4.1 我们考虑二面体群 \mathfrak{D}_n 。所有旋转给出的子群 $N = \{1, r, \dots, r^{n-1}\} \simeq \mathbb{Z}/n\mathbb{Z}$ 是正规子群, $K = \{1, s\} \simeq$ 是由某一个反射给出的子群。根据 $srs = srs^{-1} = r^{-1}$, 我们知道共轭作用由如下的映射给出

$$\varphi: \mathbb{Z}/2\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/n\mathbb{Z}), \quad 0 \mapsto \text{id}, \quad 1 \mapsto (k \mapsto -k).$$

所以, $\mathfrak{D}_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/2\mathbb{Z}$ 。根据上面的练习, $\mathfrak{D}_n \not\simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 。

例题 4.2 K 是域, 我们考虑线性空间 K^n 上的 n 维仿射变换群。

$$\text{Aff}(n; K) := \{x \mapsto Ax + b \mid a \in \mathbf{GL}(n; K), b \in K\}.$$

平移变换和线性变换

$$\text{Trans}(n; K) = \{x \mapsto x + b \mid b \in K^n\}, \quad \mathbf{GL}(n; K) := \{x \mapsto Ax \mid A \in \mathbf{GL}(n; K)\},$$

均为 $\text{Aff}(n; K)$ 的子群, 其中, $\text{Trans}(n; K)$ 和 K^n 同构。另外, $\text{Trans}(n; K) \triangleleft \text{Aff}(n; K)$ 。我们现在计算 $\mathbf{GL}(n; K)$ 在 $\text{Trans}(n; K)$ 上的共轭作用。对任意的 $g(x) = Ax$ 和 $T_b(x) = x + b$, 我们有

$$g \cdot T_b \cdot g^{-1}(x) = x + Ab \Rightarrow \text{Int}(A)(b) = Ab.$$

所以,

$$\text{Aff}(n; K) \simeq K^n \rtimes_{\varphi} \mathbf{GL}(n; K),$$

其中,

$$\varphi: \mathbf{GL}(n; K) \rightarrow \text{Aut}(K^n), \quad A \mapsto (x \mapsto A \cdot x).$$

例题 4.3 阶较小群的几何实现: 例子 我们考虑 $G = \text{Aff}(2; \mathbb{F}_2)$, 它自然地作用在 $X = \mathbb{F}_2^2$ 上: 对每个 $(b, A) \in \mathbb{F}_2^2 \rtimes_{\varphi} \mathbf{GL}(2; \mathbb{F}_2)$, 我们都有

$$(b, A) \cdot x = x \mapsto Ax + b, \quad \forall x \in X = \mathbb{F}_2^2.$$

作为群作用, 我们自然有群同态

$$\text{Aff}(2; \mathbb{F}_2) \rightarrow \mathfrak{S}_{\mathbb{F}_2^2}.$$

这个映射是单射, 而 $|\mathfrak{S}_{\mathbb{F}_2^2}| = 4!$ 并且 $|\mathbb{F}_2^n \rtimes_{\varphi} \mathbf{GL}(2; \mathbb{F}_2)| = 4 \cdot 6 = 24$, 所以, 以上是群同构, 即

$$\text{Aff}(2; \mathbb{F}_2) \simeq \mathfrak{S}_4.$$

另外, $\mathbf{GL}(n; \mathbb{F}_2)$ 自然地作用在 \mathbb{F}_2^2 的 1 维线性子空间的集合 $\mathbf{P}^2(\mathbb{F}_2)$ 上 (此时即为非零向量的集合), 从而给出了群同态

$$\mathbf{GL}(n; \mathbb{F}_2) \rightarrow \mathfrak{S}_{\mathbf{P}^2(\mathbb{F}_2)}.$$

同样通过计算元素个数的方法, 我们知道

$$\mathbf{GL}(n; \mathbb{F}_2) \simeq \mathfrak{S}_3.$$

根据以上讨论, 我们得到了

$$\mathfrak{S}_4 \simeq \left(\mathbb{Z}/2\mathbb{Z}\right)^2 \rtimes_{\varphi} \mathfrak{S}_3.$$

在 \mathfrak{S}_4 , 我们考虑如下的子群

$$K_4 = \{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}.$$

很明显, 我们有 $K_4 \triangleleft \mathfrak{S}_4$. 这就是在同构

$$\left(\mathbb{Z}/2\mathbb{Z}\right)^2 \rtimes_{\varphi} \mathfrak{S}_3 \longrightarrow \mathfrak{S}_4$$

下 $\left(\mathbb{Z}/2\mathbb{Z}\right)^2$ 的像。而 \mathfrak{S}_3 的像是固定 1 的那些置换 (这里, 我们必须把 \mathbb{F}_2^2 上的元素如下标号: $1 = (0, 0), 2 = (1, 0), 3 = (0, 1), 4 = (1, 1)$)。

例题 4.4 pq 阶的群 G 是有限群, $|G| = pq$, 其中, $q < p$ 均为素数。我们要确定 G 的结构。

首先, 因为 Sylow p -子群的个数整除 q , 从而只能是 1 或者 q ; 进一步, Sylow p -子群的个数除以 p 的余数是 1。所以, 只能有一个 Sylow p -子群 N ; 类似地, Sylow q -子群的数目只能是 1 和 p 。

- 假设 $q \nmid p-1$, 此时, Sylow q -子群的数目除以 q 余 1, 从而, 恰好只有一个 Sylow q 子群 K 。此时, N 和 K 都是正规子群, 所以, 对任意的 $k \in K$ 和 $n \in N$, 我们有

$$nkn^{-1}k^{-1} = (nkn^{-1})k^{-1} = n(kn^{-1}k^{-1}) \in N \cap K.$$

由于 N 和 K 的元素个数是互素的, 所以, $N \cap K = 1$ 。据此, N 与 K 中的元素是交换的, 从而, $G = N \cdot K \simeq N \times K$ 。

作为总结, 如果 $q \nmid p-1$, $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ 。

- 假设 $q \mid p-1$, 我们选定一个 Sylow p -子群 K 。此时 K 未必是正规子群。我们考虑 K 在 N 上的共轭作用:

$$\varphi: K \rightarrow \text{Aut}(N), \quad k \mapsto (n \mapsto knk^{-1}).$$

由于 $N \simeq \mathbb{Z}/p\mathbb{Z}$, $K \simeq \mathbb{Z}/q\mathbb{Z}$, 所以, 我们认为以上的 φ 为

$$\varphi: \mathbb{Z}/q\mathbb{Z} \rightarrow \text{Aut}\left(\mathbb{Z}/p\mathbb{Z}\right) = \left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}.$$

以上, 因为 $\mathbb{Z}/q\mathbb{Z}$ 是循环群, 所以, 给出群同态 φ 等价于指定 $\text{Aut}\left(\mathbb{Z}/p\mathbb{Z}\right)$ 中的一个元素 w 并且要求该元素满足 $w^q = 1$ 。以上, $\text{Aut}\left(\mathbb{Z}/p\mathbb{Z}\right) = \left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}$ 是因为指定 $\text{Aut}\left(\mathbb{Z}/p\mathbb{Z}\right)$ 中的一个元素 σ 等价于指定 $\sigma(1) \in \mathbb{Z}/p\mathbb{Z}$ 的像。

综上所述, 由于 $(\mathbb{Z}/p\mathbb{Z})^\times$ 为 $p-1$ 阶的循环群 C_{p-1} , 所以,

$$\varphi: \mathbb{Z}/q\mathbb{Z} \rightarrow ((\mathbb{Z}/p\mathbb{Z})^\times, \cdot), \quad 1 \mapsto w,$$

其中, $w^q = 1$ 。在循环群 C_{p-1} 中, 满足 $w^q = 1$ 的元素有 q 个并且构成循环群。该群除了 1 之外任何一个元素都是生成元。另外, 如果 $w \neq 1$, 通过 $\mathbb{Z}/q\mathbb{Z}$ 到自身的复合, 我们可以保证 $\varphi(1)$ 取该循环群中的任意一个生成元。这样, 我们有如下两种情形:

- $\varphi(1) = 1$, 此时, $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$;
- $\varphi(1) = w \neq 1$, 此时, $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/q\mathbb{Z}$ 并且这个群并不交换 (半直积的唯一性)。

实际上, 这个半直积不依赖于 φ 的选取:

令 $A = \mathbb{Z}/p\mathbb{Z}$, $B = \mathbb{Z}/q\mathbb{Z}$, $\Sigma = \text{Aut}(B)$, 这三个群都是循环群², 我们指定它们的生成元 $a = 1 \in A$, $b \in B$ 和 $\sigma \in \Sigma$ 。这样, 这三个群的元素可以写成

$$A = \{1, a, a^2, \dots, a^{q-1}\}, \quad B = \{1, b, b^2, \dots, b^{p-1}\}, \quad \Sigma = \{1, \sigma, \sigma^2, \dots, \sigma^{q-2}\}.$$

我们指定群同态:

$$\varphi_0: B \longrightarrow \Sigma, \quad b \mapsto \sigma_0 = \sigma^{\frac{p-1}{q}}.$$

(注意到由于 B 是阶为 q 的循环群, 所以, b 在以上同态下的像 σ_0 一定要满足 $\sigma_0^q = 1$) 此时, 我们就有半直积 $\mathbb{Z}/p\mathbb{Z} \rtimes_{\varphi_0} \mathbb{Z}/q\mathbb{Z}$ 。

现在考虑另一个非平凡的群同态:

$$\varphi_1: B \longrightarrow \Sigma, \quad b \mapsto \sigma_1.$$

由于 σ_1 一定要满足 $\sigma_1^q = 1$, 所以, 存在 $k \in \{1, 2, \dots, q-1\}$, 使得 $\sigma_1 = \sigma^{k \frac{p-1}{q}}$ 。由于 k 与 q 互素, 存在 $m \in \{1, 2, \dots, q-1\}$, 使得 $k \cdot m \equiv 1 \pmod{p}$ 。从而,

$$\varphi_1(b^m) = \left(\sigma^{k \frac{p-1}{q}} \right)^m = \sigma^{km \frac{p-1}{q}} = \sigma^{\frac{p-1}{q}} = \sigma_0.$$

如果令 $b^m = b'$, 我们可以把 B 重新写成

$$B = \{1, b', b'^2, \dots, b'^{p-1}\}.$$

$$\varphi_1: B \longrightarrow \Sigma, \quad b' \mapsto \sigma_0.$$

它的形式与 φ_0 的一致。由此可见半直积 $\mathbb{Z}/p\mathbb{Z} \rtimes_{\varphi_1} \mathbb{Z}/q\mathbb{Z}$ 与 $\mathbb{Z}/p\mathbb{Z} \rtimes_{\varphi_0} \mathbb{Z}/q\mathbb{Z}$ 同构。我们考虑 1 维仿射变换群 $\text{Aff}(1; \mathbb{F}_p)$ 的子群

$$C'_{p,q} = \{x \mapsto ax + b \mid a \in \mathbb{F}_p^\times, a^q = 1; b \in \mathbb{F}_p\}.$$

容易看出, $C'_{p,q}$ 是非交换的并且恰好有 pq 个元素, 这就从几何上实现了以上 pq 阶的群 (并同时给出了这个群在 1 维仿射直线 \mathbb{F}_p 的作用)。

综上所述, 对阶为 pq 阶的群 G , 我们有

$$G \simeq \begin{cases} C_{pq}, & q \nmid p-1; \\ C_{pq} \text{ 或者 } C'_{p,q}, & q \mid p-1. \end{cases}$$

²参考第一次作业

4.2 有限生成交换群的分类

对于交换群 A ，我们用 $+$ 代表其乘法。如果存在有限个 x_1, \dots, x_n ，使得 $A = \langle x_1, \dots, x_n \rangle$ ，我们就称 $(A, +)$ 是有限生成的交换群。

例题 4.5 \mathbb{Z} 和 $\mathbb{Z}/n\mathbb{Z}$ 是（所有可能的）循环群，可以由一个元素生成，从而是有限生成的交换群，

例题 4.6 有限的交换群是有限生成的交换群。

例题 4.7 有限个有限生成的交换群的乘积仍然是有限生成的交换群。特别地， $\mathbb{Z}^r = \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{r \text{ 个}}$

也是有限生成的交换群。

练习 4.2 假设 $\mathbb{Z}^m \simeq \mathbb{Z}^n$ ，证明， $m = n$ 。

我们将证明利用 \mathbb{Z} ， $\mathbb{Z}/n\mathbb{Z}$ 和乘积，可以构造出所有的有限生成的交换群。

命题 4.1

A 是交换群。那么， A 是有限生成的交换群当且仅当存在整数 n 以及满的群同态 $\mathbb{Z}^n \rightarrow A$ 。

证明 我们把证明留作作业。

例题 4.8 格点子群 $n \geq 1$ ， V 是 \mathbb{R} -线性空间， $\dim_{\mathbb{R}} V = n$ 。假设 $G < V$ 是一个离散子群（作为 V 的加法子群），即对任意的 $g \in G$ ，存在开集 $O \subset \mathbb{R}^n$ ，使得 $G \cap O = \{g\}$ 。

练习 4.3 证明， $G < V$ 是离散子群当且仅当对任意的紧集 $K \subset V$ ， $G \cap K$ 是有限的。

对任意的基 $\mathbf{e} = (e_1, \dots, e_n) \in G$ 作为 \mathbb{R}^n ，我们定义其相应的格点集

$$\Gamma_{\mathbf{e}} = \bigoplus_{i=1}^n \mathbb{Z} e_i = \left\{ \sum_{i=1}^n k_i z_i \mid k_i \in \mathbb{Z} \right\}.$$

容易看出， $\Gamma_{\mathbf{e}}$ 是 V 的离散子群。另外，如果我们只考虑这个基中的部分元所生成的格点，比如对 $m < n$ ，

$$\bigoplus_{i=1}^m \mathbb{Z} e_i = \left\{ \sum_{i=1}^m k_i z_i \mid k_i \in \mathbb{Z} \right\}$$

也是 V 的离散子群。

我们现在说明，本质上格点集给出了 V 的所有的离散子群。我们不妨假设 G 张成的 \mathbb{R} -线性子空间 V' 恰好是 V （否则用 V' 代替 V ）。

命题 4.2

V 是 \mathbb{R} -线性空间， $\dim_{\mathbb{R}} V = n$ ， $G < V$ 是离散子群并且 $\text{span}_{\mathbb{R}}(G) = V$ 。那么，存在 V 基的 $\mathbf{e}' = (e'_1, \dots, e'_n)$ ，使得 $G = \Gamma_{\mathbf{e}'}$ 。

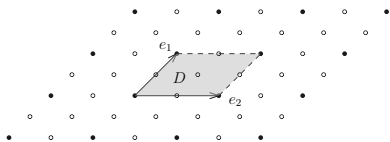
证明 我们对维数 n 归纳。

考虑 $n = 1$ 的情形。假设 $e_1 \in G$ 并且 $e_1 > 0$ 。由于 G 是离散的，所以， $G \cap [0, e_1]$ 是有限集合。特别地， $G \cap (0, e_1]$ 非空并且有限。令 $e'_1 = \min G \cap (0, e_1]$ ，那么，用 e_1 对 e'_1 进行带余除法，即存在正整数 l 和 $r \in [0, e'_1)$ ，使得 $e_1 = l \cdot e'_1 + r$ 。由于 G 是群，所以， $r \in G$ ；从而， $r \in G \cap (0, e_1]$ 。根据 e'_1 的最小性，只能有 $r = 0$ ，从而， $e_1 = l \cdot e'_1 \in \mathbb{Z} \cdot e'_1$ 。类似地，每个 $g \in G$ 都

是 e'_1 的倍数, 从而 $G = \mathbb{Z}e'_1$.

我们假设 $\leq n-1$ 的时候命题成立. 现在选取 $e_1, \dots, e_n \in G$ 作为 V 的一组基. 我们考虑如下的区域

$$D = \{\lambda_1 e_1 + \dots + \lambda_n e_n \mid \lambda_1, \dots, \lambda_n \in [0, 1]\}.$$



对任意的 $v \in V$, 我们可以把它唯一地写成 Γ_e 与 D 的元素之和:

$$\begin{aligned} v &= v_1 e_1 + \dots + v_n e_n \\ &= \underbrace{(\lfloor v_1 \rfloor e_1 + \dots + \lfloor v_n \rfloor e_n)}_{v_\Gamma} + \underbrace{(\{v_1\} e_1 + \dots + \{v_n\} e_n)}_{v_D}. \end{aligned}$$

我们考虑 $G \cap D \subset G \cap \overline{D}$, 这是有限集. 定义线性映射

$$\pi_1: V \longrightarrow \mathbb{R}, \quad v_1 e_1 + \dots + v_n e_n \mapsto v_1.$$

这是满射, 其核为 $V' = \text{span}(e_2, \dots, e_n)$. 此时, $\pi_1(G) < \mathbb{R}$ 是子群. 我们来说明 $\pi_1(G)$ 是 \mathbb{R} 的离散子群. 按以上分解, $G = \Gamma_e + G \cap D$, 所以,

$$\pi_1(G) = \pi(\Gamma_e) + \pi_1(G \cap D) = \langle \pi_1(e_1) \rangle + \pi_1(G \cap D).$$

由于 $\pi_1(G \cap D)$ 是有限集, 所以, $\pi_1(G)$ 在 \mathbb{R} 中和任何紧集之交是有限的. 特别地, $\pi_1(G)$ 由某个 $\pi_1(e'_1)$ 生成, 其中, $e'_1 \in G$. 至此, 我们有 G 的子群 $\langle e'_1 \rangle$ 和 $G \cap V'$. 很显然, $\langle e'_1 \rangle \cap (G \cap V') = 0$ 并且 $\langle e'_1 \rangle + (G \cap V') = G$. 这表明 (根据半直积的理论), $G \simeq (G \cap V') \times \mathbb{Z}e'_1$. 对 $(G \cap V')$ 用归纳假设即可.

引理 4.1

A 是有限生成的交换群, $\{x_1, \dots, x_n\}$ 是 A 的一组生成元. 假设 $k_1, \dots, k_n \in \mathbb{Z}$ 并且其最大公约数为 1, 那么, 存在 $y_2, \dots, y_n \in A$, 使得 $\{k_1 x_1 + \dots + k_n x_n, y_2, \dots, y_n\}$ 也是 A 的一组生成元.



证明 对 $k = \sum_{i=1}^n |k_i|$ 进行归纳, 不妨假设 $|k_1| = \max\{|k_1|, \dots, |k_n|\}$. 如果 $k = 1$, 那么, $k_1 x_1 + \dots + k_n x_n = \pm x_1$, 此时, 我们选 $y_2 = x_2, \dots, y_n = x_n$ 即可.

我们现在做如下的归纳假设: 对任意的生成元 $\{x'_1, \dots, x'_n\}$, 对任意 $k'_1, \dots, k'_n \in \mathbb{Z}$, 只要它们的最大公约数为 1 并且 $\sum_{i=1}^n |k'_i| < k$, 我们就可以把 $k'_1 x'_1 + \dots + k'_n x'_n$ 扩充为 A 的总数不超过 n 个的一组生成元. 现在证明命题.

通过调整正负号, 我们不妨假设 $k_1 > 0$. 此时, $k_1 \geq |k_2|$, 根据 k_2 的符号 ε , 我们可以做如下的调整:

$$k_1 x_1 + \dots + k_n x_n = (k_1 - \varepsilon \cdot k_2) x_1 + k_2 (x_2 + \varepsilon x_1) + k_3 x_3 + \dots + k_n x_n.$$

此时, $x_1, x_2 + \varepsilon x_1, x_3, \dots, x_n$ 仍然是 A 的总数不超过 n 个的一组生成元, 并且

$$|k_1 - \varepsilon \cdot k_2| + |k_2| + \dots + |k_n| < k.$$

根据归纳假设，命题得证。

引理 4.2

A 是有限生成的交换群，那么， A 具有一组仿基，即存在生成元集 $\{x_1, \dots, x_n\}$ ，使得

$$\sum_{i=1}^n k_i x_i = 0 \Leftrightarrow k_i x_i = 0, i = 1, \dots, n.$$



证明 我们选取 A 生成元集 $\{x_1, \dots, x_n\}$ 使得 n 是最小的并进一步要求 $\text{ord}(x_1)$ 是可能最小的（可以是 ∞ ）。我们考虑 A 的子群 $A_0 = \langle x_1 \rangle$ 和 $A_1 = \langle x_2, \dots, x_n \rangle$ 。我们考虑群同态：

$$\varphi: A_0 \times A_1 \rightarrow A, (x_1, 1) \mapsto x_1, (1, x_i) \mapsto x_i, i \geq 2.$$

这显然是满射。现在说明 φ 是单射：假设 $\varphi((m_1 x_1, m_2 x_2 + \dots + m_n x_n)) = 0$ ，这里，我们总可以假设 $0 \leq m_1 < \text{ord}(x_1)$ ，目标是证明 $m_1 x_1 = 0$ ，所以不妨假设 $m_1 \geq 1$ 。设 $d = (m_1, \dots, m_n)$ 是它们的最大公约数，那么，

$$d(k_1 x_1 + k_2 x_2 + \dots + k_n x_n) = 0, k_i = \frac{m_i}{d}, (k_1, \dots, k_n) = 0.$$

根据上一个引理，我们可以找到 $y_1 = k_1 x_1 + k_2 x_2 + \dots + k_n x_n$ 和 y_2, \dots, y_n 作为生成元的集合，此时， $\text{ord}(y_1) \leq d \leq m_1 < \text{ord}(x_1)$ ，这与 $\text{ord}(x_1)$ 的最小性矛盾。

此时我们得到同构 $\langle x_1 \rangle \times A_1 \xrightarrow{\sim} A$ 并且 A_1 的生成元的数目不超过 $n-1$ （严格小于 A 的最少生成元的数目）。我们将这过程继续下去就得到了一组拟基。

定理 4.1 (有限生成交换群的结构)

A 是有限生成的交换群。那么，存在唯一一组 $r \in \mathbb{Z}_{\geq 0}, d_1, \dots, d_s \in \mathbb{Z}_{\geq 2}$ ，使得 $d_s \mid d_{s-1} \mid \dots \mid d_2 \mid d_1$ 并且

$$A \simeq \mathbb{Z}^r \times \prod_{i=1}^s \mathbb{Z}/d_i \mathbb{Z}.$$

我们把 r 称作是 A 的秩，把 d_1, \dots, d_s 称作是 A 的不变因子。



证明 根据前面关于仿基的引理，我们已经可以把 A 写成 $\mathbb{Z}^r \times \prod_{i=r+1}^n \mathbb{Z}/m_i \mathbb{Z}$ 的形式。此时，我们需要对 $\mathbb{Z}/m_i \mathbb{Z}$ 这些因子进行分解和重排。实际上，根据 m_i 的素因子分解，我们有³

$$m_i = \prod_p p^{\alpha_i(p)} \Rightarrow \mathbb{Z}/m_i \mathbb{Z} = \prod_p \mathbb{Z}/p^{\alpha_i(p)} \mathbb{Z}.$$

从而，

$$A \simeq \mathbb{Z}^r \times \prod_p \prod_{i=1}^s \mathbb{Z}/p^{\alpha_i(p)} \mathbb{Z}.$$

我们现在需要将上面的乘积重新组合。首先定义 d_1 。对每个 p ，假设 $\beta(p) = \max\{\alpha_i(p)\}_i$ ，那么，令 $d_1 = \prod_p \beta(p)$ 并将这一个 $\beta(p)$ 从 $\{\alpha_i(p)\}_i$ 中删除；然后定义 $\gamma(p) = \max\{\alpha_i(p)\}_i$ ， $d_2 = \prod_p \gamma(p)$ 并将这一个 $\gamma(p)$ 从 $\{\alpha_i(p)\}_i$ 中删除。以此类推。很明显， $d_2 \mid d_1, d_3 \mid d_2, \dots$ 。从而，

$$A \simeq \mathbb{Z}^r \left(\prod_p \mathbb{Z}/p^{\beta(p)} \mathbb{Z} \right) \times \left(\prod_p \mathbb{Z}/p^{\gamma(p)} \mathbb{Z} \right) \times \dots = \mathbb{Z}^r \times \prod_{i=1}^s \mathbb{Z}/d_i \mathbb{Z}.$$

³参考第一次作业 A4)

这就给出了存在性部分的证明。

为了证明定理中唯一性的部分，我们要说明 r, d_1, \dots, d_s 可以完全由 A 本身算出即可。为此，我们先给出一个关于循环群的引理：

引理 4.3

A 是循环群， p 是素数，那么，

$$p^{k-1}A/p^kA = \begin{cases} 0, & |A| < \infty, p^k \nmid |A|; \\ \mathbb{Z}/p\mathbb{Z}, & \text{其余情况。} \end{cases}$$



证明 令 x 为 A 的生成元，那么， $p^{k-1}x$ 也是 $p^{k-1}A$ 的生成元并且 $p \cdot p^{k-1}x \in p^kA$ ，这说明 $p^{k-1}A/p^kA$ 要么是 $\mathbb{Z}/p\mathbb{Z}$ 要么是 0。如果 $A \simeq \mathbb{Z}$ ，命题是显然的。我们以下假设 $A \simeq \mathbb{Z}/n\mathbb{Z}$ 是有限循环群。不妨设 $n = p^d \cdot m$ ，其中， $(m, p) = 1$ 。那么， $A \simeq \underbrace{\mathbb{Z}/p^d\mathbb{Z}}_{A'} \times \mathbb{Z}/m\mathbb{Z}$ 。由于

$$\mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}, \bar{a} \mapsto p^k \bar{a},$$

是同构，所以， $p^{k-1}\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/m\mathbb{Z} = p^k\mathbb{Z}/m\mathbb{Z}$ ，从而，

$$p^{k-1}A/p^kA \simeq p^{k-1}A'/p^kA'.$$

此时，如果 $d < k$ ，即 $p^k \nmid |A|$ ，那么， $p^{k-1}A' = p^{k-1}\mathbb{Z}/p^d\mathbb{Z} = 0$ ，从而， $p^{k-1}A'/p^kA' \simeq 0$ ；如果 $d \geq k$ ，那么， $p^{k-1}x' \neq 0$ （在 A' 在中），其中， x' 为 A' 的生成元。很明显， $p^{k-1}x' \notin p^kA'$ ，所以， $p^{k-1}A'/p^kA' \simeq \mathbb{Z}/p\mathbb{Z}$ 。

我们现在用 A 来计算 r, d_1, \dots, d_s ，其中， A 是有限生成的交换群。利用已知的（某一个）分解，我们有

$$p^{k-1}A/p^kA \simeq (\mathbb{Z}/p\mathbb{Z})^r \times \prod_{i=1}^s p^{k-1}(\mathbb{Z}/d_i\mathbb{Z})/p^k(\mathbb{Z}/d_i\mathbb{Z}).$$

此时，上述群的阶为 $p^{r+s(k)}$ ，其中， k 为 d_1, \dots, d_s 中是 p^k 的倍数的数的个数（恰好是前 k 个）。这样，当 k 从 1 开始递增时，我们就可以决定 d_1, \dots, d_s 中所含的 p 的因子的次幂，从而，决定了 d_1, \dots, d_s 。最终，我们可以选 p 使得它与所有 d_1, \dots, d_s 互素，此时， $A/pA \simeq (\mathbb{Z}/p\mathbb{Z})^r$ 决定了 r 。

例题 4.9 我们考虑 $A = \mathbb{Z}4\mathbb{Z} \times \mathbb{Z}6\mathbb{Z}$ 。根据分类定理，我们应该把它写成：

$$\begin{aligned} A &= \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \\ &= \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}. \end{aligned}$$

4.3 滤链

定义 4.1

G 是群。假设 G 的子群序列 $(G_i)_{0 \leq i \leq n}$ 满足

$$1 = G_n \triangleleft G_{n-1} \triangleleft G_{n-2} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G, \quad (4.1)$$

我们就称该子群序列为 G 的一个滤链。给定滤链，我们将商群序列 $(\text{gr}_i(G) = G_i/G_{i+1})_{i \leq n-1}$ 称作是该滤链的分次化并记作 $\text{gr}(G)$ ，其中，每个 $\text{gr}_i(G)$ 都被称作是该滤链的一个因子群。

我们将整数 n 称作是该滤链的长度。



注 我们强调，以上定义中仅要求 $G_i \triangleleft G_{i-1}$ 而 G_i 可能在 G_{i-2} 中不再是正规子群，其中， $i = 1, \dots, n-1$ 。

注 给定子群 $H < G$ ，我们定义

$$H_i = G_i \cap H.$$

由于 $G_i \triangleleft G_{i-1}$ ，所以， $G_i \cap H \triangleleft G_{i-1} \cap H$ 。这表明，滤链 (G_i) 诱导出子群上 H 的滤链 (H_i) 。

注 给定正规子群 $N \triangleleft G$ ，那么， $G_i \cap N \triangleleft G_i$ 。令

$$\left(\frac{G}{N}\right)_i := G_i/G_i \cap N.$$

由于 $G_i \triangleleft G_{i-1}$ ，所以⁴， $\left(\frac{G}{N}\right)_i \triangleleft \left(\frac{G}{N}\right)_{i-1}$ 。这表明，滤链 (G_i) 诱导出商群 G/N 上的滤链 $\left(\frac{G}{N}\right)_i$ 。

注 给定群同态的正合列

$$1 \rightarrow N \rightarrow G \rightarrow G/N \rightarrow 1.$$

根据以上两个注记，我们有⁵

$$1 \rightarrow N_i/N_{i+1} \rightarrow G_i/G_{i+1} \rightarrow \left(\frac{G}{N}\right)_i/\left(\frac{G}{N}\right)_{i+1} \rightarrow 1,$$

也就是说

$$1 \rightarrow \text{gr}_i(N) \rightarrow \text{gr}_i(G) \rightarrow \text{gr}_i\left(\frac{G}{N}\right) \rightarrow 1. \quad (4.2)$$

定义 4.2

给定群 G 的滤链 $(G_i)_{0 \leq i \leq n}$ ，如果每个 $\text{gr}_i(G)$ 都是单群，其中， $0 \leq i \leq n-1$ ，我们就称这个滤链为 **Jordan-Hölder 滤链**。



命题 4.3

有限群 G 必有 Jordan-Hölder 滤链。



证明 如果 $G = 1$ ，我们在(4.1)中取 $n = 0$ ；如果 G 为单群，则可取 $n = 1$ 。其他情形，我们对 G 的阶进行归纳：取 G 的阶最大的正规子群 N ，其中， $N \neq G$ 。由于 G 不是单群， $N \neq 1$ 。所以，

⁴参考第二次作业练习题 9

⁵参考第二次作业练习题 7,8

G/N 为单群⁶。由于 $|N| < |G|$ ，归纳假设给出了 N 的 Jordan-Hölder 滤链 (N_i) 。所以，我们可以选取 (G, N_0, N_1, \dots) 作为 G 的 Jordan-Hölder 滤链。证毕。

注 无限群未必有 Jordan-Hölder 滤链。

练习 4.4 证明，无限循环群 \mathbb{Z} 没有 Jordan-Hölder 滤链。

定理 4.2 (Jordan-Hölder)

任意给定群 G 的 Jordan-Hölder 滤链 $(G_i)_{0 \leq i \leq n}$ ，其因子群的集合 $\{\text{gr}_i(G)\}$ （可以有重复）在不计顺序的意义下与滤链的选取无关。

特别地，Jordan-Hölder 滤链（如果存在）的长度 n 与滤链的选取无关，我们将 n 称作是群 G 的长度并记作 $\ell(G)$ 。如果一个群没有 Jordan-Hölder 滤链，我们约定其长度为 ∞ 。

证明 根据 Jordan-Hölder 滤链的定义，因子群的集合 $\{\text{gr}_i(G)\}$ （可重复）中都是单群。对每个单群 S ，我们用 $n(G, (G_i), S)$ 表示 S 在 $(\text{gr}_i(G))$ 中出现的次数（在同构意义下）。我们的目标是证明 $n(G, (G_i), S)$ 与滤链 (G_i) 的选取无关。

我们对滤链的长度 n 进行归纳。当 $n \leq 1$ 时， G 要么是平凡群，要么是单群，结论不证自明。现在假定 $n \geq 2$ 并且假设 G 不是单群，所以可以选取正规子群 $N \triangleleft G$ ，使得 $N \neq 1, N \neq G$ 。我们考虑群的正合列

$$1 \rightarrow N \rightarrow G \rightarrow G/N \rightarrow 1,$$

以及滤链对此整合列所诱导的滤链的整合列(4.2)。由于 (G_i) 为 Jordan-Hölder 滤链，所以 $\text{gr}_i(G)$ 均为单群，其正规子群 $\text{gr}_i(N)$ 只能是 1 或 $\text{gr}_i(G)$ 。据此，我们可以把集合 $I = \{0, \dots, n-1\}$ 分划为两部分

$$I_1 = \{i \mid \text{gr}_i(N) = \text{gr}_i(G)\}, I_2 = \{i \mid \text{gr}_i(N) = 1\}.$$

我们自然有 $|I_1| + |I_2| = n$ 。利用 I_1 和 I_2 作为指标，我们得到 N 和 G/N 上 Jordan-Hölder 滤链。

另外，显然有 $|I_1| < n, |I_2| < n$ ，所以，我们可以对 N 和 G/N 用归纳假设：这表明 $n(N, (N_i)_{i \in I_1}, S)$ 和 $n(G/N, (G/N)_i)_{i \in I_2}, S)$ 与滤链的选取无关。又因为

$$\begin{aligned} n(G, (G_i), S) &= n(N, (N_i)_{i \in I_1}, S) + n(G/N, (G/N)_i)_{i \in I_2}, S) \\ &= n(N, S) + n(G/N, S). \end{aligned}$$

所以， $n(G, (G_i), S)$ 也与滤链的选取无关。

推论 4.1

对任意的正规子群 $N \triangleleft G$ ，我们有

$$\ell(G) = \ell(N) + \ell(G/N).$$

证明 上述证明已经给出了 $\ell(G) < \infty$ 的情形。当 $\ell(G) = \infty$ 时，那么， N 和 G/N 中至少有一个长度是无穷大，所以 $\ell(G) = \ell(N) + \ell(G/N)$ 仍然成立。

例题 4.10 Jordan-Hölder 定理的唯一性部分可以给出算术基本定理的唯一性部分的证明。

⁶参考第二次作业练习题 9

利用整数 n 的素因子分解 $n = p_1^{h_1} \cdots p_k^{h_k}$, 我们可以构造群 $G = \mathbb{Z}/n\mathbb{Z}$ 的 Jordan-Hölder 滤链:

$$\mathbb{Z}/n\mathbb{Z} \triangleright p_1\mathbb{Z}/n\mathbb{Z} \triangleright p_1^2\mathbb{Z}/n\mathbb{Z} \triangleright \cdots \triangleright p_1^{h_1}\mathbb{Z}/n\mathbb{Z} \triangleright p_1^{h_1}p_2\mathbb{Z}/n\mathbb{Z} \triangleright p_1^{h_1}p_2^2\mathbb{Z}/n\mathbb{Z} \triangleright \cdots$$

作为因子群, $\mathbb{Z}/n\mathbb{Z}$ 在 $\text{gr}G$ 中出现的次数恰好是 h_i , 这就给出了素因子分解的唯一性。

调整素因子的标号, 以上构造说明 Jordan-Hölder 滤链本身可能不是唯一的。

例题 4.11 (\mathfrak{S}_3 的滤链) $\mathfrak{A}_3 \triangleleft \mathfrak{S}_3$ 且指标为 2, 而 \mathfrak{S}_3 的 2 阶子群都不是正规子群。所以, \mathfrak{S}_3 有且只有一个 Jordan-Hölder 滤链:

$$1 \triangleleft \mathfrak{A}_3 \triangleleft \mathfrak{S}_3.$$

这个滤链的长度为 2, 其因子群为 2 阶和 3 阶的循环群。

例题 4.12 (\mathfrak{S}_4 的滤链) $\mathfrak{A}_4 \triangleleft \mathfrak{S}_4$ 且指标为 2。令 $D = \{1, \sigma_1, \sigma_2, \sigma_3\}$, 其中

$$\sigma_1 = (1, 2)(3, 4), \quad \sigma_2 = (1, 3)(2, 4), \quad \sigma_3 = (1, 4)(2, 3).$$

容易验证, D 是子群并且 $D \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 。进一步, $D \triangleleft \mathfrak{A}_4$ 是正规子群。对每个 i , 我们都有如下的 Jordan-Hölder 滤链:

$$1 \triangleleft \{1, \sigma_i\} \triangleleft D \triangleleft \mathfrak{A}_4 \triangleleft \mathfrak{S}_4.$$

通过计算群元素的个数, 我们知道其因子群有 3 个 2 阶循环群和 1 个 3 阶循环群。通过改变上式中的 i , 我们知道 \mathfrak{S}_4 的滤链选取并不唯一。

例题 4.13 (\mathfrak{S}_n 的滤链, $n \geq 5$) 由于此时 \mathfrak{A}_n 是单群并且是 \mathfrak{S}_n 中唯一非平凡的正规子群⁷, 所以 \mathfrak{S}_n 只有有唯一一个 Jordan-Hölder 滤链:

$$1 \triangleleft \mathfrak{A}_n \triangleleft \mathfrak{S}_n.$$

该滤链的因子群分别为 \mathfrak{A}_n 和 2 阶循环群。

4.4 可解群

G 是群。对于 $x, y \in G$, 我们定义它们的交换子或者换位子为⁸

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

$H < G$ 和 $K < G$ 是子群, 我们用 (H, K) 表示由所有 (x, y) 所生成的子群, 其中, $x \in H, y \in K$ 。我们把子群 (G, G) 称为 G 的换位子群或导出子群, 记作 $\mathbf{D}(G)$ 。**注** $\mathbf{D}(G) \triangleleft G$ 是正规子群。实际上, $\mathbf{D}(G)$ 是 G 的所谓的特征子群, 即对任意的自同构 (不仅仅是内自同构) $\varphi \in \text{Aut}(G)$, $\varphi(\mathbf{D}(G)) = \mathbf{D}(G)$ 。

⁷参考第二次作业的 B2) 和 B4)

⁸我们采取 Bourbaki 的约定, 更多文献中将换位子定义为 $xyx^{-1}y^{-1}$ 。这些差异对于整个理论没有影响。

命题 4.4

$H < G$ 是子群。那么, 如下两个命题等价:

- (1) $H \supset \mathbf{D}(G)$ 。
- (2) H 是正规子群并且 G/H 是交换群。



证明 假设 (1) 成立。那么, 对任意的 $h \in H$ 和 $g \in G$, 我们有

$$ghg^{-1} = ghg^{-1}h^{-1} \cdot h \in \mathbf{D}(G) \cdot H \subset H.$$

所以, $H \triangleleft G$ 。另外, 对任意的 $g_1, g_2 \in G$, 由于 $(g_1, g_2) \in \mathbf{D}(G) \subset H$, 所以, g_1H, g_2H 在 G/H 中交换。至此, 我们证明了 (2)。

假设 (2) 成立。考虑 $\mathbf{D}(G)$ 的任意一个生成元 (x, y) 。由于 G/H 是交换群, 所以, $(x, y) \in H$, 这表明 $\mathbf{D}(G) < H$, 即 (1) 成立。

注 要得到 G 的一个交换的商群, 以上命题表明我们至少要商掉 $\mathbf{D}(G)$ 。所以, $G/\mathbf{D}(G)$ 是 G 的极大的交换商群。我们称 $G/\mathbf{D}(G)$ 是群 G 的交换化并记为 G^{ab} 。

群的交换化就有如下的泛性质: 每个从 G 到某个交换群的群同态必然可以下降到 $G \rightarrow G^{\text{ab}}$ 上去, 这可以用如下的交换图来表示:

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & A \\ \downarrow & \nearrow \bar{\varphi} & \\ G^{\text{ab}} & & \end{array}$$

其中, A 是交换群, $\varphi: G \rightarrow A$ 是群同态, 上图表明必然存在群同态 $\bar{\varphi}: G^{\text{ab}} \rightarrow A$, 使得上图交换。

例题 4.14 假设 $n \geq 2$, 那么, $\mathfrak{S}_n^{\text{ab}} \simeq \mathbb{Z}/2\mathbb{Z}$ 。

$n = 2$ 的情形是明显的。

考虑 $n \neq 2$ 的情形, 此时 $\mathbf{D}(\mathfrak{S}_n) \neq 1$ 。由于 $\mathbf{D}(\mathfrak{S}_n)$ 中的元素必然都是偶置换给出的, $\mathbf{D}(\mathfrak{S}_n) < \mathfrak{A}_n$ 。实际上, 我们必然有 $\mathbf{D}(\mathfrak{S}_n) = \mathfrak{A}_n$, 这可以通过对如下换位子的计算得到: 对于 $i, j, k \leq n$, 我们有

$$((i, j), (j, k)) = (k, i, j).$$

所以, 这样可以给出所有的 3-循环。由于 \mathfrak{A}_n 由 3-循环生成, 所以, $\mathbf{D}(\mathfrak{S}_n) = \mathfrak{A}_n$ 。从而,

$$\mathfrak{S}_n^{\text{ab}} \simeq \mathfrak{S}_n / \mathfrak{A}_n \simeq \mathbb{Z}/2\mathbb{Z}.$$

例题 4.15 $n \geq 2$, K 是域, $G = \mathbf{GL}(n; K)$, 那么, $\mathbf{D}(G) = \mathbf{SL}(n; K)$ 。很明显, 很显然, $\mathbf{D}(\mathbf{GL}(n; K)) < \mathbf{SL}(n; K)$ 。我们证明反过来的包含关系: 这是线性代数中的一个经典结论。令 e_{ij} 为仅在 (i, j) 处为 1 而其余地方均为 0 的 $n \times n$ 的矩阵, 我们有如下的经典公式:

$$e_{ij} \cdot e_{kl} = \delta_{jk} e_{il}, \quad (4.3)$$

其中, δ_{jk} 是 Kronecker 符号。

首先考虑初等矩阵 $E_{ij}(\lambda)$, 其中 $\lambda \in K$, $i \neq j$ 。这个矩阵在对角线上都是 1, 在 (i, j) 处为

λ , 即 $E_{ij}(\lambda) = \mathbf{I} + \lambda e_{ij}$, 这里 \mathbf{I} 是单位矩阵。那么, $E_{ij}(\lambda)^{-1} = E_{ij}(-\lambda)$ 。利用(4.3), 我们有

$$(E_{ik}(\alpha), E_{kj}(\beta)) = E_{ik}(-\alpha)E_{kj}(-\beta)E_{ik}(\alpha)E_{kj}(\beta) = E_{ij}(\alpha\beta).$$

其中, 我们要求 $i \neq j$ 。选取 $\alpha = 1, \beta = \gamma$, 那么, 对任意的 $i \neq j$ 和 $\lambda \in K$, $E_{ij}(\lambda) \in \mathbf{D}(\mathbf{GL}(n; K))$ (实际上, 我们证明了 $E_{ij}(\lambda) \in \mathbf{D}(\mathbf{SL}(n; K))$)。

其次考虑 $D \in \mathbf{SL}(n; K)$ 中的对角矩阵。为此, 对于 $i \neq j$, 我们计算

$$\begin{aligned} & E_{ij}(\alpha)E_{ji}(\beta)E_{ij}(\mu)E_{ji}(\nu) \\ &= 1 + (\alpha + \mu + \alpha\beta\mu)e_{ij} + (\beta + \nu + \beta\mu\nu)e_{ji} + [(\alpha + \mu + \alpha\beta\mu)\nu + \alpha\beta]e_{ii} + \beta\mu e_{jj} \\ &= 1 + (\alpha + \mu + \alpha\beta\mu)e_{ij} + (\beta + \nu + \beta\mu\nu)e_{ji} + [\mu\nu + \alpha(\beta + \nu + \beta\mu\nu)]e_{ii} + \beta\mu e_{jj} \end{aligned}$$

然后计算下面乘积的非对角线项:

$$\begin{aligned} & E_{ij}(\alpha)E_{ji}(\beta)E_{ij}(\mu)E_{ji}(\nu) \cdot E_{ij}(\lambda) \\ &= \left(\alpha + \mu + \alpha\beta\mu + \lambda + [(\alpha + \mu + \alpha\beta\mu)\nu + \alpha\beta] \right) e_{ij} + (\beta + \nu + \beta\mu\nu)e_{ji} + \cdots \end{aligned}$$

我们令以上两个系数为 0, 这就给出了如下待定的方程:

$$\begin{cases} \beta + \nu + \beta\mu\nu = 0, \\ \alpha + \mu + \alpha\beta\mu + \lambda + [(\alpha + \mu + \alpha\beta\mu)\nu + \alpha\beta] \lambda = 0 \end{cases}$$

这等价于

$$\begin{cases} \beta + \nu + \beta\mu\nu = 0, \\ \alpha + \mu + \alpha\beta\mu + \lambda + \mu\nu\lambda = 0. \end{cases} \quad (4.4)$$

在此假设下, 我们有

$$E_{ij}(\alpha)E_{ji}(\beta)E_{ij}(\mu)E_{ji}(\nu) = 1 + (\alpha + \mu + \alpha\beta\mu)e_{ij} + \mu\nu e_{ii} + \beta\mu e_{jj}$$

所以,

$$E_{ij}(\alpha)E_{ji}(\beta)E_{ij}(\mu)E_{ji}(\nu) \cdot E_{ij}(\lambda) = (1 + \mu\nu)e_{ii} + \cdots$$

以下令 $\mu = 1$ 并且把 ν 视作是变量, 那么, (4.4) 的第一个方程给出 $\beta + 1 = (1 + \nu)^{-1}$, 这里, 我们要求 $\nu \neq -1$ (注意到, 在 \mathbb{F}_2 中, 这只能要求 $\nu = 0$)。代入第二个方程, 我们得到

$$\alpha = -(1 + \nu) - \lambda(1 + \nu)^2, \quad \beta = (1 + \nu)^{-1}, \quad \mu = 1.$$

这里, 可以取 $\lambda = 0$, 从而,

$$E_{ij}(-(1 + \nu))E_{ji}((1 + \nu)^{-1})E_{ij}(1)E_{ji}(\nu) = (1 + \nu)e_{ii} + (1 + \nu)^{-1}e_{jj}.$$

这样, 对于 $D \in \mathbf{SL}(n; K)$, 我们可以用以上 (最多 $4(n-1)$ 个形如 $E_{ij}(\lambda)$) 矩阵逐一地把对角线上都乘得到 1, 当然, 这里假设了 $1 + \nu \neq 0$ (对角线上已经是 1 的时候不需要做以上操作)。从而, 结合之间的结论, $D \in \mathbf{D}(\mathbf{SL}(n; K))$ 。

最终, 对任意的 $A \in \mathbf{SL}(n; K)$, 我们可以通过初等变换即左右乘以形如 $E_{ij}(\lambda)$ 的矩阵的方式使得 A 变成对角阵, 其行列式为 1, 从而, 结合上面结论, 我们就有 $A \in \mathbf{D}(\mathbf{SL}(n; K))$ 。

以上证明实际上给出了 $\mathbf{D}(\mathbf{SL}(n; K)) = \mathbf{SL}(n; K)$ 。

由于 $\det: \mathbf{GL}(n; K) \rightarrow K^\times$ 是满射而 $\text{Ker}(\det) = \mathbf{SL}(n; K)$, 所以, $\mathbf{GL}(n; K)^{\text{ab}} \simeq K^\times$ 。

通过对导出子群函子 $G \mapsto \mathbf{D}G$ 进行迭代迭代, 我们可以定义滤链 (子群序列) $\{\mathbf{D}^n G\}$:

$$\mathbf{D}^0 G = G, \mathbf{D}^1 G = \mathbf{D}G, \mathbf{D}^n G = \mathbf{D}(\mathbf{D}^{n-1} G) = (\mathbf{D}^{n-1} G, \mathbf{D}^{n-1} G), n \geq 1.$$

我们显然有

$$G \triangleright \mathbf{D}^1 G \triangleright \mathbf{D}^2 G \triangleright \cdots.$$

这个序列未必在有限步停止, 即使停止最后的群也未必是 1。但是我们总是可以定义

$$\mathbf{D}^\infty G = \bigcap_{n \geq 1} \mathbf{D}^n G.$$

定义 4.3

如果存在正整数 n , 使得 $\mathbf{D}^n G = 1$, 我们就称 G 为可解群^a。以下, 我们用 $d\ell(G)$ 表示使得 $\mathbf{D}^n G = 1$ 的最小正整数 n , 它被称作是 G 的可解类数或者导出长度。

^a代数方程可用根式求解当且仅当其 Galois 群可解, 这是术语“可解”的来源。



注 可解群的子群和商群都是可解的。

假设 G 可解并且 $d\ell(G) = n$ 。对于子群 H 而言, $\mathbf{D}^n H < \mathbf{D}^n G = 1$, 所以可解并且 $d\ell(H) \leq d\ell(G)$; 对于商群 G/N 而言, 我们有满射 $G \rightarrow G/N$, 那么, $\mathbf{D}G \rightarrow \mathbf{D}(G/N)$ 也是满射, 从而, $1 = \mathbf{D}^n G \rightarrow \mathbf{D}^n(G/N)$ 是满射, 所以, G/N 可解。

这里的推理表明导出长度不超过 n 的可解群的子群和商群的导出长度不超过 n 。

注 $d\ell(G) = 0$ 等价于 G 是平凡群; $d\ell(G) \leq 1$ 等价于 G 是交换群。特别地, 交换群是可解群。

注 有两个关于可解群的大定理。第一个是 Burnside 定理: $p^a q^b$ 阶的群可解, 其中, p 和 q 是素数。第二个是 Feit-Thompson 定理: 奇数阶的群可解。

命题 4.5

给定群 G 和正整数 n , 如下命题等价

- (1) G 是可解群并且 $d\ell(G) \leq n$ 。
- (2) G 有特征子群列 $G = G_0 > G_1 > \cdots > G_n = 1$, 使得 G_i/G_{i+1} 交换, 其中 $0 \leq i \leq n-1$ 。
- (2') G 有滤链 $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = 1$, 使得 G_{i+1} 是 G_i 的正规子群并且 G_i/G_{i+1} 交换, 其中 $0 \leq i \leq n-1$ 。
- (3) G 有交换的特征子群 A , 使得 G/A 可解并且 $d\ell(G/A) \leq n-1$ 。



证明 (1) \Rightarrow (2): 取 $G_i = \mathbf{D}^i G$; (2) \Rightarrow (2'): 显然; (2') \Rightarrow (1): 根据命题 4.4 对 k 归纳可得 $\mathbf{D}^k G < G_k$, 从而 $\mathbf{D}^n G = 1$ 。至此, (1), (2) 和 (2') 等价。

(1) \Rightarrow (3): 取 $A = \mathbf{D}^{n-1} G$, 由于 $\mathbf{D}A = 1$, 所以, A 是交换群。另外, $\mathbf{D}^{n-1}(G/A) \subset \mathbf{D}^{n-1}G/A = 1$ 。

(3) \Rightarrow (2): 根据 $d\ell(G/A) \leq n-1$, 存在 G 的正规子群序列 $G = A_0 \triangleright A_1 \triangleright \cdots \triangleright A_{n-1} = A$, 使得

$$G/A \triangleright A_1/A \triangleright \cdots \triangleright A_{n-1}/A = 1.$$

从而, $G \triangleright A_1 \triangleright \cdots \triangleright A_{n-1} \triangleright 1$ 满足 (2) 的要求。

推论 4.2 (有限可解群的等价定义)

G 是有限群, 则如下定义等价

- (1) G 可解。
- (2) G 有滤链 $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = 1$, 使得 G_{i+1} 是 G_i 的正规子群并且 G_i/G_{i+1} 交换, 其中 $0 \leq i \leq n-1$ 。
- (3) G 有滤链 $G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_m = 1$, 使得 H_{i+1} 是 H_i 的正规子群并且 H_i/H_{i+1} 是循环群, 其中 $0 \leq i \leq m-1$ 。



证明 只要证明 (2) \Rightarrow (3) 即可, 其余都是平凡的。实际上, 由于 G_i/G_{i+1} 是有限交换群, 根据交换群的结构定理, 存在子群序列 $G_i \triangleright G_i^1 \triangleright G_i^2 \triangleright \cdots \triangleright G_i^l \triangleright G_{i+1}$, 使得

$$G_i/G_{i+1} \triangleright G_i^1/G_{i+1} \triangleright \cdots \triangleright G_i^l/G_{i+1} \triangleright 1,$$

并且

$$G_i^j/G_i^{j+1} \simeq G_i^j/G_{i+1}/G_i^{j+1}/G_{i+1}$$

是交换群。我们将这些 G_i^j 添加到 G_i 中就可以得到所求的滤链。

命题 4.6

G 是群, $N \triangleleft G$ 是正规子群。如果 N 和 G/N 可解, 那么 G 也可解。进一步, 我们有

$$dl(G) \leq dl(N) + dl(G/N).$$



证明 令 $i = dl(N)$, $j = dl(G/N)$ 。那么, $\mathbf{D}^j G \subset N$, $\mathbf{D}^i N = 1$ 。所以, $\mathbf{D}^{i+j} G = \mathbf{D}^i (\mathbf{D}^j G) = 1$ 。

命题 4.7 (有限可解群的另一个等价定义)

G 是有限群, $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = 1$ 为其 Jordan-Hölder 序列。那么, G 可解当且仅当 G_i/G_{i+1} 为素数阶循环群, 其中 $0 \leq i \leq n-1$ 。



证明 如果 G_i/G_{i+1} 为素数阶循环群, 根据已经证明的等价命题中的 (3), G 可解; 反之, 如果 G 可解, 根据上一命题, G_i/G_{i+1} 可解。然而 G_i/G_{i+1} 同时也是单群, 其导出子群必然平凡。据此, G_i/G_{i+1} 只能是素数阶循环群。

例题 4.16

- 1) G 是非交换单群。那么, $\mathbf{D}(G) = G$, 从而, G 不可解决。据此, \mathfrak{S}_n 不可解, 因为它包含了 \mathfrak{A}_n 这个不可解的子群。
- 2) 当 $n \leq 4$ 时, \mathfrak{S}_n 可解。

只要对 $n = 4$ 证明即可 (其余均为其子群)。我们已经构造过 \mathfrak{S}_4 的 Jordan-Hölder 滤链:

$$1 \triangleleft \{1, \sigma_i\} \triangleleft D \triangleleft \mathfrak{A}_4 \triangleleft \mathfrak{S}_4.$$

其因子群均为素数阶循环群。

- 3) K 是域, V 是 n 维 K -线性空间, $V = V_0 \supset V_1 \supset \cdots \supset V_n = 0$ 是一列下降的线性子空间并

且 $\dim_K(V_i) = n - i$, $i = 0, \dots, n$ 。定义⁹

$$G = \{s \in \mathbf{GL}(V) \mid s: V_i \rightarrow V_i, 0 \leq i \leq n\}.$$

以及其子群序列 $(B_i)_{0 \leq i \leq n}$:

$$B_i = \{s \in G \mid (s-1)V_j \subset V_{i+j}, 0 \leq j \leq n-i\}.$$

特别地, $B_0 = G$ 而 $B_n = 1$ 。很明显, $B_0/B_1 = G/B_1$ 同构于对角矩阵构成的子群。我们证明, 对 $j+k \leq n$, 我们有 $(B_j, B_k) \subset B_{j+k}$:

任取 $s \in B_j$, $t \in B_k$ 和 $x \in V_i$, 根据定义, 存在 $v \in V_{i+j}$, $w \in V_{i+j}$, 使得 $tx = x + v$, $sx = x + w$ 。从而

$$stx = s(x + v) = x + w + v + t',$$

$$tsx = t(x + w) = x + v + w + t'',$$

其中, $t', t'' \in V_{i+j+k}$ 。从而, 在模 V_{i+j+k} 的意义下, $stx \equiv tsx$, 亦即 $s^{-1}t^{-1}stx \equiv x$, 所以 $(B_j, B_k) \subset B_{j+k}$ 。特别地, 我们得到

- 对 $0 \leq i \leq n$, $(B_0, B_i) \subset B_i$, 所以 B_i 是 $G = B_0$ 的正规子群。
- 对 $1 \leq i \leq n$, $(B_i, B_i) \subset B_{2i} \subset B_{i+1}$, 所以 B_i/B_{i+1} 是交换群 ($i \leq n-1$)。

据此, 滤链 $(B_i)_{0 \leq i \leq n}$ 满足命题4.5的 (2), 所以 G 是可解群。

⁹如果选一组基 (e_i) , 使得 $e_i \in V_i$, 那么, G 就是可逆上三角矩阵所构成的群。

第5章 环与模

5.1 与环相关的基本概念

我们回忆环 $(A, \cdot, +)$ 的定义: $(A, +, 0)$ 是交换群; $(A, \cdot, 1)$ 的乘法有结合律, 1 是乘法单位元; 乘法与加法通过分配律相容: 对任意的 $a_1, a_2, a_3 \in A$, 有

$$(a_1 + a_2) \cdot a_3 = a_1 \cdot a_3 + a_2 \cdot a_3, \quad a_3 \cdot (a_1 + a_2) = a_3 \cdot a_1 + a_3 \cdot a_2.$$

另外, 我们不假设乘法是交换的 (如果交换, A 是交换环) $a \cdot b = b \cdot a$, 我们就称 A 是交换环。

环 A 的子环指的是某个加法子群 B , $1 \in B$ 并且 B 对乘法封闭。

对 $a \in A$, 如果它有乘法下的逆元 (即存在 $b \in A$, 使得 $a \cdot b = b \cdot a = 1$), 我们就称 a 是可逆的。如果 A 中的所有非零元都是可逆的, 我们就称 A 是可除环。交换的可除环被称作域。

对环 A_1 和 A_2 之间的映射 $\varphi: A_1 \rightarrow A_2$, 如果它保持加法和乘法并且 $\varphi(1) = 1$, 我们就说 φ 是环同态。

对任意的 $\varphi \in \text{Hom}(A_1, A_2)$, 其核为 $\text{Ker}(\varphi) = \{a \in A_1 \mid \varphi(a) = 0\}$ 。由于 $1 \notin \text{Ker}(\varphi)$, 所以, $\text{Ker}(\varphi)$ 不是子环。它是所谓的理想:

定义 5.1

A 是环, $I \subset A$ 是子集。如果 I 是 A 的加法子群并且对任意的 $a \in A$ 和 $x \in I$, 我们都有 $a \cdot x \in I$, 我们就称 I 是 A 的一个左理想; 如果 I 是 A 的加法子群并且对任意的 $a \in A$ 和 $x \in I$, 我们都有 $x \cdot a \in I$, 我们就称 I 是 A 的一个右理想。如果 I 既是左理想又是右理想, 我们就说 I 是双边理想 (简称为理想)。



注 当我们谈理想 I 的时候, 我们约定 $1 \notin I$, 即 $I \neq A$ 。

注 A 是交换环, 那么其左理想或者右理想均为双边理想。

注 对环同态 $\varphi \in \text{Hom}(A_1, A_2)$, $\text{Ker}(\varphi)$ 是 (双边) 理想。

练习 5.1 A 是交换环。证明, A 是域当且仅当 A 只有 0 和 A 两个理想。

给定环 A 的 (双边) 理想 I , 我们可以构造其商环 A/I 。实际上, A/I 是加法群的商群, 它可以用如下的左陪集表示:

$$A/I = \{a + I \mid a \in A\}.$$

此时, $a + I = a' + I$ 当且仅当 $a - a' \in I$ 。我们现在定义 A/I 上的乘法:

$$(a + I) \cdot (b + I) := ab + I.$$

对于 $a + I = a' + I$, 我们知道 $ab - a'b = (a - a')b \in I$, 从而, $ab + I = a'b + I$ 。这表明以上乘法的定义不依赖于 $a + I$ 中代表元的选取。另外, 根据商群的定义, 我们还有

$$(a + I) + (b + I) := (a + b) + I.$$

容易验证, 在 A/I 中, $I = 0 + I$ 是加法零元 (因为 $I + I = I$), $1 + I$ 是乘法单位元。

练习 5.2 试验证以上定义的加法和乘法给出了 A/I 上的环结构。

注 商映射

$$\pi: A \rightarrow A/I, a \mapsto a + I,$$

是满的环同态。实际上, 对任意的 $a, b \in A$, 我们有

$$\pi(a+b) = a+b+I = (a+I) + (b+I) = \pi(a) + \pi(b), \quad \pi(ab) = ab+I = (a+I)(b+I) = \pi(a)\pi(b).$$

命题 5.1

A 和 B 是环, $I \subset A$ 是理想, $\varphi: A \rightarrow B$ 是环同态。如果 $I \subset \text{Ker}(\varphi)$, 那么存在唯一的环同态 $\bar{\varphi}: A/I \rightarrow B$, 使得 $\bar{\varphi} \circ \pi = \varphi$, 其中, $\pi: A \rightarrow A/I$ 是自然的同态。

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \downarrow \pi & \nearrow \bar{\varphi} & \\ A/I & & \end{array}$$

进一步, 我们还有环同构 $\bar{\varphi}: A/\text{Ker}(\varphi) \xrightarrow{\cong} \text{Im}(\varphi)$ 。



证明 对任意的 $a+I \in A/I$, 定义 $\bar{\varphi}(a+I) = \varphi(a)$ 。我们已经对加法群证明了以上定理的叙述, 为了完成证明, 只要验证 $\bar{\varphi}$ 是环同态即可而这是显然的。

例题 5.1 A 和 B 是环, $A \times B$ 也是¹那么, $I = A \times 0 = \{(a, 0) | a \in A\}$ 是 $A \times B$ 的理想。此时, $A \times B/I \simeq B$ 。

自此往后, 我们总是假设 A 是交换的。

例题 5.2 素理想与整环

A 是环, 对 $a \in A$, 如果存在 $b \in A$, 使得 $a \cdot b = 0$ 或者 $b \cdot a = 0$, 我们就称 a 是一个零因子。如果环 A 是交换的并且除了 0 之外没有其它的零因子, 我们就称 A 是整环。²换言之, 在整环 A 中, $a \cdot b = 0$ 意味着 $a = 0$ 或者 $b = 0$ 至少之一成立。

A 是环, $\mathfrak{p} \subset A$ 是理想, $\mathfrak{p} \neq A$ 。如果 $a \notin \mathfrak{p}$, $b \notin \mathfrak{p}$, 那么 $a \cdot b \notin \mathfrak{p}$, 我们就称 \mathfrak{p} 是素理想。

考虑整数环 \mathbb{Z} 。 p 是素数, 令 $(p) = \{kp | k \in \mathbb{Z}\}$ 。很明显, (p) 是理想。假设 $a, b \notin (p)$, 即 $p \nmid a, p \nmid b$, 所以, $p \nmid ab$, 即 $ab \notin (p)$ 。这表明 (p) 是素理想。另外, 如果 $n = n_1 \cdot n_2$ 是合数, 其中, $n_1, n_2 \geq 2$ 。令 $(n) = \{kn_1 n_2 | k \in \mathbb{Z}\}$, $n_1 \notin (n), n_2 \notin (n)$, 但是 $n_1 \cdot n_2 \in (n)$, 这表明 (n) 不是素理想。

练习 5.3 A 是交换环。证明, A 是整环等价于 (0) 是素理想。

根据定义, 如果 \mathfrak{p} 是素理想, 那么, $a \cdot b \in \mathfrak{p}$ 意味着 $a \in \mathfrak{p}$ 或者 $b \in \mathfrak{p}$ 至少之一成立。

我们可以用商环的性质来刻画素理想: 假设 A 是交换环, 理想 \mathfrak{p} 是素理想当且仅当 A/\mathfrak{p} 是整环。

证明是显然的: 如果 \mathfrak{p} 是素理想, 对任意的 $a+\mathfrak{p}, b+\mathfrak{p} \in A/\mathfrak{p}$, 如果 $(a+\mathfrak{p})(b+\mathfrak{p}) = \mathfrak{p}$, 那么, $ab \in \mathfrak{p}$, 从而不妨假设 $a \in \mathfrak{p}$, 所以, 在 A/\mathfrak{p} 中 $a+\mathfrak{p} = 0$; 反之, $a \cdot b \in \mathfrak{p}$, 从而, 在 A/\mathfrak{p}

¹参考第一次作业 A6)。

²我们强调整环 A 根据其定义是交换的。

中 $(a+p)(b+p)=0$, 不妨设 $a+p=0$, 从而, $a \in p$.

特别地, 我们知道 $\mathbb{Z}/p\mathbb{Z}$ 是整环. 当然, 我们知道 $\mathbb{Z}/p\mathbb{Z}$ 实际上是域. 我们有如下经典的习题:

练习 5.4 A 是整环并且 $|A| < \infty$, 那么, A 是域.

(提示: A 是整环, 所以, 对任意的 $a \neq 0$, 映射 $A \rightarrow A, x \mapsto a \cdot x$ 是单射)

例题 5.3 整环的分式域 A 是整环. 我们在 $A \times (A - \{0\})$ 上定义等价关系:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

练习 5.5 证明, 以上 \sim 是等价关系.

我们用 $\frac{a}{b}$ 表示 (a, b) 在 $\text{Frac}(A) = A \times (A - \{0\}) / \sim$ 中对应的等价类. 如果 $\lambda \in A - \{0\}$, 我们自然有 $\frac{\lambda a}{\lambda b} = \frac{a}{b}$.

我们定义

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

容易验证, 以上定义不依赖于代表元 a, b 的选取. 那么, 在以上运算下 $\text{Frac}(A)$ 是域 (其中, $\frac{1}{1}$ 是乘法单位元, $\frac{0}{1}$ 是加法单位元, $\frac{a}{b} \cdot \frac{b}{a} = \frac{1}{1} = 1$), 我们把它称作是 A 的分式域.

A 是环, $\{I_i\}_i$ 是理想的集合, 那么, 如下定义的 A 的子集均为理想:

$$\bigcap_i I_i, \quad I_1 + \cdots + I_n = \{x_1 + x_2 + \cdots + x_n \mid x_1 \in I_1, \dots, x_n \in I_n\},$$

$$I_1 \cdot I_2 \cdots I_n = \{\text{有限个形如 } x_1 x_2 \cdots x_n \text{ 的元素之和, 其中, } x_1 \in I_1, \dots, x_n \in I_n\}.$$

练习 5.6 证明如上集合均为理想.

根据定义, $I_1 + I_2$ 中的元素形如 $x_1 + x_2$, 其中, $x_1 \in I_1, x_2 \in I_2$; $I_1 \cdot I_2$ 中的元素形如 $\sum_{i=1}^k x_i y_i$, 其中, $x_i \in I_1, y_i \in I_2$. 给定 A 的非空子集 $S \subset I$, 根据以上关于理想交的性质, 则存在唯一的包含 S 的最理想 (在包含关系下) (S) . 这是包含 S 的所有理想的交集, 被称作是由 S 所生成的理想. 很明显,

$$(S) = \{S \text{ 中有限个元素之积的有限和}\}.$$

如果理想 I 由有限个元素的集合 $\{a_1, \dots, a_k\}$ 生成, 我们就称 I 是有限生成的并把它记作是 $I = (a_1, \dots, a_k)$. **注** 假设 $I_1 = (a_1, \dots, a_n), I_2 = (b_1, \dots, b_m)$, 那么,

$$I_1 + I_2 = (a_1, \dots, a_n, b_1, \dots, b_m), \quad I_1 \cdot I_2 = (a_i b_j, 1 \leq i \leq n, 1 \leq j \leq m).$$

如果 I 可以由一个元素 a 生成, 我们就称 I 是主理想并把它记作是 $I = (a)$.

定义 5.2

A (交换) 整环, 如果 A 的每个理想都是主理想, 我们就称 A 是主理想整环.



例题 5.4 \mathbb{Z} 是主理想整环. 假设 $I \subset \mathbb{Z}$ 是理想并且 $I \neq (0)$. 令 $d = \min I \cap \mathbb{Z}_{>0}$. 那么, 对任意的 $a \in I$, 根据带余除法, 存在唯一的 $b \in \mathbb{Z}$ 和 $r \in [0, d)$, 使得 $a = bd + r$. 然而, $r = a - bd \in I$

并且 $d = \min I \cap \mathbb{Z}_{\geq 0}$, 从而, $r = 0$, 即 $a = bd$, 所以, $I = (d)$ 。

定义 5.3

A 是环, $\mathfrak{m} \subset A$ 是理想并且 $\mathfrak{m} \neq A$ 。如果 \mathfrak{m} 是在包含关系下最大的这样的理想, 即对任意的理想 $\mathfrak{m} \subset I \subset A$, $I = \mathfrak{m}$ 或者 $I = A$ 二者必居其一, 我们就称 \mathfrak{m} 是一个极大理想。

注 极大理想是素理想。

实际上, 对任意的 $x \notin \mathfrak{m}$, 根据极大性, $(\mathfrak{m}, x) = A$ 。 (\mathfrak{m}, x) 中的元素形如 $ax + n$, 其中, $m \in \mathfrak{m}, a \in A$ 。所以, 存在 $m \in \mathfrak{m}, a \in A$, 使得 $ax + m = 1$ 。类似地, 对 $y \notin \mathfrak{m}$, 存在 $m' \in \mathfrak{m}, a' \in A$, 使得 $a'y + m' = 1$ 。据此, 我们有

$$aa'xy = (1 - m)(1 - m') = 1 \pmod{\mathfrak{m}}.$$

所以, $xy \notin \mathfrak{m}$ (否则 $1 \in \mathfrak{m}$), 即 \mathfrak{m} 是素理想。

命题 5.2

A 是环, I 是理想, 那么, 存在极大理想 \mathfrak{m} , 使得 $\mathfrak{m} \supset I$ 。

证明 考虑偏序集 $\mathcal{J} = \{J \supset I, J \text{ 是理想 } J \neq A\}$, 其中, 偏序由包含关系 $J_1 \leq J_2$ 指的是 $J_1 \subset J_2$ 。此时, 对任意的全序子集 $S \subset \mathcal{J}$, 我们令

$$J_* = \bigcup_{J \in S} J.$$

我们说明 J_* 是理想: 对任意的 $x, y \in J_*$, 存在 $J_1 \in S, J_2 \in S$, 使得 $x \in J_1, y \in J_2$ 。由于 S 是全序子集, 不妨假设 $x, y \in J_1 \supset J_2$, 此时, $x \pm y \in J_1 \subset J_*$ 。这表明 J_* 是 A 的加法子群。另外, 对任意的 $a \in A, ax \in J_1 \subset J_*$, 所以, J_* 是理想。

由于对任意的 $J \in S, 1 \notin J$, 所以, $1 \notin J_*$, 从而, $J_* \neq A$ 。以上表明, $J_* \in \mathcal{J}$ 。根据定义, J_* 是 S 的上界。根据 Zorn 引理, S 有极大元 \mathfrak{m} , 这就是所求的极大理想。

注 [极大理想与域] 假设 A 是交换环, 理想 \mathfrak{m} 是极大理想当且仅当 A/\mathfrak{m} 是域。(这将是我们将用来构造域的最重要的手段!)

如果 \mathfrak{m} 是极大理想, 对任意的非零的 $x + \mathfrak{m} \in A/\mathfrak{m}$, 按照定义, $x \notin \mathfrak{m}$ 。根据极大性, $(\mathfrak{m}, x) = A$, 所以, 存在 $m \in \mathfrak{m}, y \in A$, 使得 $xy + m = 1$ 。这表明 $y + \mathfrak{m} \in A/\mathfrak{m}$ 是 $x + \mathfrak{m} \in A/\mathfrak{m}$ 的乘法逆。

反之, 假设 $\mathfrak{m} \subset I \subset A$, 那么³, $I/\mathfrak{m} \subset A/\mathfrak{m}$ 是理想。如果 A/\mathfrak{m} 是域, 那么, $I/\mathfrak{m} =$ 或者 A/\mathfrak{m} , 从而, $I = \mathfrak{m}$ 或者 A 。

假设 p 是素数。对于 $(p) \subset \mathbb{Z}$, 由于 $\mathbb{Z}/p\mathbb{Z}$ 是域, 所以, (p) 是极大理想 (我们当然可以直接证明这一点)。然而, $(0) \subset \mathbb{Z}$ 不是极大理想。

A 是交换环, $I_1, \dots, I_n \subset A$ 是理想, 我们有自然的环同态:

$$\pi: A \rightarrow A/I_1 \times A/I_2 \times \cdots \times A/I_n, \quad x \mapsto (\pi_1(x), \pi_2(x), \dots, \pi_n(x)).$$

其中, $\pi_i: A \rightarrow A/I_i$ 是商映射。显而易见, $\text{Ker}(\pi) = \bigcap_{i=1}^n I_i$ 。

给定理想 $I, J \subset A$, 如果 $I + J = A$, 我们就称 I 与 J 互素。换言之, I 与 J 互素当且仅当

³参考第五次作业练习题 1

$1 \in I + J$ 。比如 $m, n \in \mathbb{Z}$ 是两个互素的整数, 根据 Bézout 定理, 存在 $a, b \in \mathbb{Z}$, 使得 $am + bn = 1$, 从而, 理想 (m) 与 (n) 互素。

引理 5.1 (中国剩余定理)

A 是交换环, $I_1, \dots, I_n \subset A$ 是两两互素的一组理想, $n \geq 2$ 。那么, $\bigcap_{i=1}^n I_i = \prod_{i=1}^n I_i$ 。进一步, $\pi: A \rightarrow A/I_1 \times \dots \times A/I_n$ 是满射。从而, 我们有环同构

$$A/I_1 \cdot I_2 \cdots I_n \xrightarrow{\cong} A/I_1 \cap I_2 \cap \dots \cap I_n \xrightarrow{\cong} A/I_1 \times A/I_2 \times \dots \times A/I_n.$$



证明 我们对 n 进行归纳。按照理想的定义, $I_1 \cdot I_2 \subset I_1 \cap I_2$, 现在证明反过来的包含关系: 假设 $x \in I_1 \cap I_2$ 。由于 $I_1 + I_2 = A$, 所以, 存在 $a_1 \in I_1, a_2 \in I_2$, 使得 $a_1 + a_2 = 1$ 。据此,

$$x = 1 \cdot x = \underbrace{a_1}_{\in I_1} \cdot \underbrace{x}_{\in I_1 \cap I_2 \subset I_2} + a_2 \cdot x \in I_1 \cdot I_2.$$

为了说明 π 是满射, 现在考虑任意的 $x_1 + I_1 \in A/I_1$ 和 $x_2 + I_2 \in A/I_2$, 我们构造 $x \in A$, 使得 $x - x_1 \in I_1, x - x_2 \in I_2$ 。实际上, 以上构造的 $a_1 + a_2 = 1$, 使得

$$\pi(a_1) = (1, 0), \quad \pi(a_2) = (0, 1).$$

从而, $x = a_1 x_1 + a_2 x_2$ 即为所求。

假设对任意 $< n$ 的整数命题成立, 其中, $n \geq 3$ 。我们首先证明 I_1 与 $I_2 \cdot I_3 \cdots I_n$ 互素, 换言之, $I_1 + I_2 \cdot I_3 \cdots I_n = A$ 。根据 $I_1 + I_k = A$, 存在 $a_k \in I_1, b_k \in I_k$, 使得, $a_k + b_k = 1$, 其中, $k \geq 2$ 。所以,

$$1 = (a_2 + b_2) \cdots (a_k + b_k) = a + \underbrace{b_2 \cdots b_n}_{\in I_2 \cdot I_3 \cdots I_n},$$

其中, a 是含有 a_k 的某些单项式之和, 从而, $a \in I_1$ 。据此, $1 \in I_1 + I_2 \cdot I_3 \cdots I_n$ 。根据 $n = 2$ 的情形以及归纳假设, 我们就有

$$I_1 \cdot (I_2 \cdot I_3 \cdots I_n) = I_1 \cap \left(\bigcap_{i=2}^n I_i \right) = \bigcap_{i=1}^n I_i.$$

另外, 根据 $n = 2$ 的情形以及归纳假设, 我们有满射

$$A/I_1 \cdot (I_2 \cdots I_n) \xrightarrow{\cong} A/I_1 \times A/I_2 \cdots I_n \xrightarrow{\cong} A/I_1 \times (A/I_2 \times \cdots \times A/I_n).$$

命题得证。

推论 5.1 (中国剩余定理)

给定 n_1, \dots, n_k 为两两互素的正整数, $n = n_1 \cdots n_k$ 。那么, 我们有环同构

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}, \quad x \bmod n \mapsto (x \bmod n_1, \dots, x \bmod n_k).$$



5.2 与整除性相关的几类特殊的环

定义 5.4 (在元素层次上的整除概念)

A 是整环。对于 $a, b \in A$, 如果存在 $q \in A$, 使得 $a = qb$, 我们就说 b 整除 a 并记作 $b \mid a$ 。
 对 $x \in A$, 如果对任意的 $a, b \in A$, 如果 $x \mid a \cdot b$ 就意味着 $x \mid a$ 或 $x \mid b$ 至少之一成立, 我们就说 x 是素元。
 对 $y \in A$, 假设 y 不是乘法可逆元 (即 $y \notin A^\times$), 如果 $x = a \cdot b$ 就意味着 $a \in A^\times$ 或 $b \in A^\times$ 至少之一成立, 我们就称 y 是不可约元素。
 对于 $a, b \in A$, 如果存在 $u \in A^\times$, 使得 $a = u \cdot b$, 我们就称 a 和 b 是相互伴随的。



注 我们可以在理想的层次上谈论以上概念:

- $b \mid a \Leftrightarrow a \in (b) \Leftrightarrow (a) \subset (b)$;
- x 是素元等价于 (x) 是素理想;

注 素元是不可约的。如果 x 是素元, $x = ab$, 不妨假设 $a = a'x$, 从而, $x = a'bx$ 。由于 A 是整环, 所以, $a'b = 1$, 据此, $b \in A^\times$ 。

然而, 不可约元未必是素元。我们之后会给出例子。

注

如果 A 是主理想整环, 一个元素是素元等价于该元素是不可约的。

假设 x 不可约, 考虑 (x) 以及极大理想 $\mathfrak{m} \supset (x)$, 此时, $\mathfrak{m} = (a)$, 所以, $x = ab$, 从而, $b \in A^\times$ 。这样, $\mathfrak{m} = (a) = (b^{-1}x) = (x)$, 从而, (x) 是极大理想也是主理想。

注 主理想整环的每个非零的素理想都是极大理想。

据此, 对于域 K 上的多项式环 $K[X]$, 如果 $P(X)$ 是不可约多项式, 那么 $K[X]/(P)$ 是域。

定义 5.5 (Euclid 整环)

A 是整环。如果存在映射

$$N: A \longrightarrow \mathbb{Z}_{\geq 0},$$

其中 $N(0) = 0$, 并对任意的 $a, b \in A$, 存在 (不要求唯一) $q, r \in A$ 使得 $a = qb + r$ 而且要么 $r = 0$ 要么 $N(r) < N(b)$, 我们就称 N 是 A 上的范数并称 A 是 **Euclid 整环**。



注 仿造算术的称呼, 我们把 q 叫做 a 除以 b 的商, r 则称作是余数。很明显, 对 Euclid 整环, 我们可以对 a 和 b 使用辗转相除法, 即存在 r_0, r_1, \dots, r_k , 使得

$$r_0 = a, r_1 = b, r_0 = q_1 r_1 + r_2, r_1 = q_2 r_2 + r_3, \dots, r_{k-1} = q_{k-1} r_k + r_{k+1},$$

其中, 对 $i = 1, \dots, k$, $0 < N(r_i) < N(r_{i-1})$ 并且 $r_{k+1} = 0$ 。

命题 5.3

Euclid 整环是主理想整环。



证明 A 是 Euclid 整环, 对任意的理想 $I \subset A$, 选取 $b \in I$, 使得 $N(b) = \min_{a \in I} N(a)$ 。那么, 对任

意的 $a \in I$, 存在 $q, r \in A$ 使得 $a = qb + r$. 如果 $r \neq 0$, 我们就有 $N(r) < N(b)$, 然而 $r = a - qb \in I$, 这和 $N(b)$ 的选择矛盾. 从而, $r = 0$, 即 $a = qb \in (b)$, 从而, $I = (b)$.

例题 5.5 \mathbb{Z} 是 Euclid 整环. 对 $n \in \mathbb{Z}$, 我们取 $N(n) = |n|$.

例题 5.6 K 是域, $K[X]$ 是多项式环⁴, 这是 Euclid 整环.

对 $P(X) \in K[X]$, 令 $N(P) = \deg(P)$. 由于对多项式 $F, G \in K[X]$, 我们可以做带余除法, 使得存在唯一的 $Q, R \in K[X]$, 满足 $G(X) = Q(X)F(X) + R(X)$ 并且 $\deg(R) < \deg(F)$, 这就给出了 $K[X]$ 上的范数.

利用之前的概念, 我们可以谈论所谓的不可约多项式. 假设 $P(X) \neq 0$ 是不可约多项式, $\deg P \geq 1$, 那么, (P) 是素理想也是极大理想 (参考之前关于主理想整环中不可约元也是素元的证明过程). 特别地, 给定次数至少是 1 的不可约多项式, $K[X]/_P$ 是域. 另外, 令 $d = \deg(P)$, 那么, $1, X, \dots, X^{d-1}$ 在 $K[X]/_P$ 中是 K -线性无关的,

例题 5.7 Gauss 整数环 $\mathbb{Z}[\sqrt{-1}]$ 是 Euclid 整环.

作为集合, $\mathbb{Z}[\sqrt{-1}] = \{x + y\sqrt{-1} | a, b \in \mathbb{Z}\}$. 容易看出, 在复数的加法和乘法下, $\mathbb{Z}[\sqrt{-1}]$ 是整环 (它在 \mathbb{C} 中对应着整系数的格点集). 我们定义

$$N: \mathbb{Z}[\sqrt{-1}] \longrightarrow \mathbb{Z}_{\geq 0}, \quad N(x + y\sqrt{-1}) = x^2 + y^2.$$

很明显, 我们有 $N(a \cdot b) = N(a)N(b)$. 对任意的 $a = x + y\sqrt{-1}$ 和 $b = z + w\sqrt{-1}$, 我们首先在 \mathbb{C} 中计算它们的商:

$$\frac{a}{b} = \frac{(xz + yw) + (yz - xw)\sqrt{-1}}{N(b)}.$$

对于整数环中的带余除法稍作修改, 我们可以找到 $q_1, q_2 \in \mathbb{Z}$, $r_1, r_2 \in [-\frac{1}{2}N(b), \frac{1}{2}N(b)]$, 使得

$$xz + yw = q_1 \cdot N(b) + r_1, \quad yz - xw = q_2 \cdot N(b) + r_2.$$

此时,

$$\frac{a}{b} = \frac{(xz + yw) + (yz - xw)\sqrt{-1}}{N(b)} = q_1 + q_2\sqrt{-1} + \frac{r_1 + r_2\sqrt{-1}}{N(b)}.$$

从而,

$$a = \underbrace{(q_1 + q_2\sqrt{-1})b}_q + \underbrace{\frac{r_1 + r_2\sqrt{-1}}{N(b)}b}_r = qb + r.$$

由于 $q \in \mathbb{Z}[\sqrt{-1}]$, 所以, $r \in \mathbb{Z}[\sqrt{-1}]$. 以下计算 $N(r)$:

$$N(r) = N\left(\frac{r_1 + r_2\sqrt{-1}}{N(b)}b\right) = \frac{N(r_1 + r_2\sqrt{-1})N(b)}{N(b)^2} = \frac{r_1^2 + r_2^2}{N(b)} < \frac{\frac{1}{4}N(b)^2 + \frac{1}{4}N(b)^2}{N(b)} < N(b).$$

这就证明了 $\mathbb{Z}[\sqrt{-1}]$ 是 Euclid 整环.

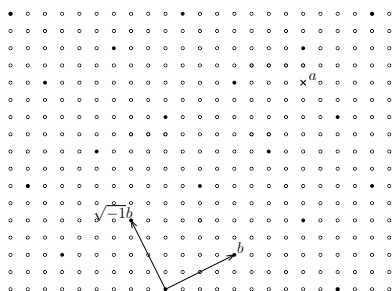
实际上, 对于 $a, b \in \mathbb{Z}[\sqrt{-1}]$, 考虑复数 $\frac{a}{b}$ 在格点集 $\mathbb{Z}[\sqrt{-1}]$ 中的位置, 那么, 存在 $q \in \mathbb{Z}[\sqrt{-1}]$, 使得

$$|\operatorname{Re}(q) - \operatorname{Re}(\frac{a}{b})| < \frac{1}{2}, \quad |\operatorname{Im}(q) - \operatorname{Im}(\frac{a}{b})| < \frac{1}{2}.$$

⁴参考 §2.3 的例子

特别地, $N(\frac{a}{b} - q) < \frac{1}{2}$ 。那么, 令 $r = a - qb$ 。我们就有

$$N(r) = N(b)N(\frac{a}{b} - q) < \frac{1}{2}N(b) = N(b).$$



另外, 我们还可以几何地考虑这个问题: 给定 b , 我们可以考虑 \mathbb{C} 上的格点集

$$\Gamma_{(b, \sqrt{-1}b)} = \{n \cdot b + m \cdot \sqrt{-1}b = (n + m\sqrt{-1})b | n, m \in \mathbb{Z}\}.$$

此时, 我们在 $\Gamma_{(b, \sqrt{-1}b)}$ 中找一个离 a 最近的格点即可 (每个格子都是正方形)。

练习 5.7 在 Gauss 整数环 $\mathbb{Z}[\sqrt{-1}]$ 中, 以上分解 $a = qb + r$ 是否唯一?

例题 5.8 我们会仔细研究形如 $\mathbb{Z}[\sqrt{D}]$ 的环, 其中, $D \in \mathbb{Z}$, 它们未必都是 Euclid 整环。

定义 5.6 (唯一分解整环 (UFD))

A 是整环。假设对任意的 $a \in A - (\{0\} \cup A^\times)$, 我们有如下的性质:

- 1) 存在 $n \geq 1$ 和 A 中的不可约元 p_1, \dots, p_n (可以重复), 使得 $a = p_1 \cdots p_n$;
- 2) 以上分解在相互伴随的意义下是唯一的: 如果 $a = q_1 \cdots q_m$ 是另一个分解, 其中, $m \geq 1$ 并且 q_1, \dots, q_m 是不可约元, 那么, $m = n$ 并且通过调整 q_1, \dots, q_m 的指标, 我们有 q_i 与 p_i 相伴随, $i = 1, \dots, n$ 。



注 \mathbb{Z} 显然是唯一分解整环, 然而, 必须要考虑相伴的问题, 因为我们总是有 $p \cdot q = (-p) \cdot (-q)$ 。

注 K 是域, 那么多项式环 $K[X]$ 是唯一分解整环。

注 在唯一分解整环中, 整除性可以从分解中不可约元素的次方直接读出: 假设

$$a = up_1^{d_1} p_2^{d_2} \cdots p_n^{d_n}, \quad b = vp_1^{e_1} p_2^{e_2} \cdots p_n^{e_n},$$

其中, $u, v \in A^\times$, p_i 和 q_j 都是不可约元素并且 d_i 和 e_j 都是非负整数。那么, $a | b$ 等价于 $d_i \leq e_i$, 其中, $i = 1, \dots, n$ 。

练习 5.8 证明如上命题。

注 在唯一分解整环中, 一个元素是素元等价于该元素是不可约的。

我们知道素元是不可约的, 现在证明不可约元 x 是素元, 即证明 (x) 是素理想。假设 $a, b \in A, ab \in (x)$, 所以, $ab = cx$, 其中, $c \in A$ 。不妨假设 $a, b \notin A^\times$, 从而, 有分解 $a = p_1 \cdots p_n, b = q_1 \cdots q_m$ 。对 c 进行分解, 根据唯一分解整环的定义, x 必然与某个 p_i 或者 p_j 相伴随, 不妨假设 $p_1 = ux$, 其中, $u \in A^\times$ 。据此, $a \in (x)$ 。

定理 5.1

主理想整环是唯一分解整环。



证明 A 是主理想整环, $a \in A - (\{0\} \cup A^\times)$ 。我们来构造 a 的分解: 如果 a 是不可约的, 那么, 分解自然存在; 否则, 我们可以把 a 写成 $a = a_1 \cdot b_1$, 其中, $a_1, b_1 \notin A^\times$; 如果 a_1, b_1 都是不可约的, 那么, 我们就找到了分解, 否则对 a_1 或者 b_1 进行分解, 通过重新标记, 我们得到 $a = a_1 \cdot a_2 \cdot b_2$; 然后对 a_1, a_2, b_2 进行同样的讨论, 据此, 如果在有限步没有停止, 那么, 我们就得到了无限的主理想的序列:

$$(a) \subset (a_1) \subset (a_2) \subset \cdots \subset A,$$

并且 $(a_i) \neq (a_{i+1})$ 。令 $I = \bigcup_{i \geq 1} (a_i)$, 这显然是理想。由于 $1 \notin A$, 所以, $I \neq A$ 。由于 A 是主理想整环, 所以, $I = (b)$ 。根据定义, 存在 $k, b \in (a_k)$, 那么, $I = (a_k)$, 从而, 以上序列实际上有限的, 矛盾。

下面证明分解的唯一性。假设 $a = p_1 \cdots p_n = q_1 \cdots q_m$ 是两个分解, 其中, p_i 和 q_j 都是不可约元。那么, $q_1 \cdots q_m \in (p_1)$ 。由于在主理想整环中, 不可约元是素元, 所以, (p_1) 是素理想, 从而, 存在某个 $q_j \in (p_1)$, 不妨假设是 $q_1 \in (p_1)$ 。从而, $q_1 = up_1$ 。由于 q_1 是不可约的, 那么, $u \in A^\times$ 。继续下去, 我们就给出了唯一性的证明。

注 我们有如下包含关系:

$$\{\text{Euclid 整环}\} \subset \{\text{主理想整环}\} \subset \{\text{唯一分解整环}\}.$$

在以上的环中, 一个元素是素元当且仅当它是不可约的。

例题 5.9 $A = \mathbb{Z}[\sqrt{-5}]$ 不是唯一分解整环, 其中, $\mathbb{Z}[\sqrt{-5}] = \{x + y\sqrt{-5} | a, b \in \mathbb{Z}\}$, 其元素的乘法和加法就是复数的乘法和加法。

我们考虑如下的分解:

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

我们需要说明以上分解的每个元素都是不可约的。我们借助于如下的映射:

$$N: \mathbb{Z}[\sqrt{-5}] \rightarrow \mathbb{Z}, \quad x + y\sqrt{-5} \mapsto x^2 + 5y^2.$$

注意到, $N(a \cdot b) = N(a)N(b)$ 。据此以及 $N(1) = 1$, 我们有 $A^\times = \{\pm 1\}$ ($y = 0$)。另外, 我们观察到

$$N(a) = 1 \Leftrightarrow a \in A^\times, \quad N(2) = 4, \quad N(3) = 9, \quad N(1 \pm \sqrt{-5}) = 6$$

并且 $2, 3 \notin N(\mathbb{Z}[\sqrt{-5}])$, 所以, $2, 3, 1 \pm \sqrt{-5}$ 是不可约的。所以, $\mathbb{Z}[\sqrt{-5}]$ 不是唯一分解整环。

例题 5.10 Gauss 整数环与 Fermat 的定理 $\mathbb{Z}[\sqrt{-1}]$ 是 Euclid 整环, 其中范数如下定义

$$N: \mathbb{Z}[\sqrt{-1}] \longrightarrow \mathbb{Z}_{\geq 0}, \quad N(x + y\sqrt{-1}) = x^2 + y^2.$$

另外, 对任意的 $a, b \in \mathbb{Z}[\sqrt{-1}]$, $N(a \cdot b) = N(a)N(b)$, 从而, $a \in \mathbb{Z}[\sqrt{-1}]^\times$ 等价于 $N(a) = 1$ 。据此, 我们有

$$\mathbb{Z}[\sqrt{-1}]^\times = \{\pm 1, \pm \sqrt{-1}\}.$$

利用 $N(a \cdot b) = N(a)N(b)$ 以及以上对 $\mathbb{Z}[\sqrt{-1}]^\times$ 的刻画, 如果对 $a \in \mathbb{Z}[\sqrt{-1}]$, $N(a) = p$, 其中, p 是 (\mathbb{Z} 中) 的素数, 那么, a 是 $\mathbb{Z}[\sqrt{-1}]$ 中的不可约元 (此时等价于素元)。

我们的目标是找到 $\mathbb{Z}[\sqrt{-1}]$ 的所有不可约元 (即素元)。由于 $\mathbb{Z}[\sqrt{-1}]$ 是主理想整环, 这

等价于去刻画 $\mathbb{Z}[\sqrt{-1}]$ 中所有的素理想。

假设 $\mathfrak{p} \subset \mathbb{Z}[\sqrt{-1}]$ 是 (非零) 素理想, 由于 $\mathbb{Z} \subset \mathbb{Z}[\sqrt{-1}]$ 是子环, 所以, $\mathfrak{p} \cap \mathbb{Z}$ 是 \mathbb{Z} 中的 (非零⁵) 素理想。由于 \mathbb{Z} 是主理想整环, 从而, $\mathfrak{p} \cap \mathbb{Z} = (p)$, 其中, p 是素数。⁶我们用如下的图标表示以上的分析:

$$\begin{array}{ccc} \mathfrak{p} & \xrightarrow{\subset} & \mathbb{Z}[\sqrt{-1}] \\ \uparrow & & \uparrow \\ \mathfrak{p} \cap \mathbb{Z}[\sqrt{-1}] = (p) & \xrightarrow{\subset} & \mathbb{Z} \end{array}$$

据此, 我们可以把每个 $\mathbb{Z}[\sqrt{-1}]$ 的素理想与 \mathbb{Z} 的一个特定的素数相关联。

假设 $p \in \mathbb{Z}$ 是素数, 由于 $N(p) = p^2$ 并且 p^2 的分解方式只有 $p^2 = 1 \cdot p^2 = p \cdot p$ 两种方式, 根据 $N(ab) = N(a)N(b)$, 作为 $\mathbb{Z}[\sqrt{-1}]$ 中的元素, 我们只有两种可能: 第一, p 在 $\mathbb{Z}[\sqrt{-1}]$ 中仍然不可约; 第二, p 在 $\mathbb{Z}[\sqrt{-1}]$ 中恰好可以写成两个不可约元之积。

为了判断 $(p) \subset \mathbb{Z}[\sqrt{-1}]$ 是否是素理想, 我们只要判断 $\mathbb{Z}[\sqrt{-1}]/p\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[\sqrt{-1}]/(p)$ 是否是整环。根据自然的复合映射

$$\mathbb{Z} \rightarrow \mathbb{Z}[\sqrt{-1}] \rightarrow \mathbb{Z}[\sqrt{-1}]/p\mathbb{Z}[\sqrt{-1}]$$

以及环同态的定理, 我们有环同态

$$\mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}[\sqrt{-1}]/p\mathbb{Z}[\sqrt{-1}].$$

通过定义 $X \mapsto \sqrt{-1}$, 我们得到环同态

$$\varphi: \mathbb{Z}/p\mathbb{Z}[X] \rightarrow \mathbb{Z}[\sqrt{-1}]/p\mathbb{Z}[\sqrt{-1}], \quad P(X) \mapsto P(\sqrt{-1}).$$

很明显, $\varphi(X^2 + 1) = 0$, 再次利用环同态的定理, 我们得到以下环同态:

$$\psi: \mathbb{Z}/p\mathbb{Z}[X]/(X^2 + 1) \xrightarrow{\simeq} \mathbb{Z}[\sqrt{-1}]/p\mathbb{Z}[\sqrt{-1}].$$

很明显, 这是满射。另外, 左右两边都恰好有 p^2 个元素, 所以以上是环同构。

综合以上讨论, 为了判断 $(p) \subset \mathbb{Z}[\sqrt{-1}]$ 是否是素理想, 我们只要判断 $\mathbb{Z}/p\mathbb{Z}[X]/(X^2 + 1)$ 是否是整环。我们有两种可能性:

- $X^2 + 1$ 是 $\mathbb{Z}/p\mathbb{Z}[X]$ 中的不可约多项式 (从而, $(X^2 + 1) \subset \mathbb{Z}/p\mathbb{Z}[X]$ 是素理想), 那么, $\mathbb{Z}/p\mathbb{Z}[X]/(X^2 + 1)$ 是整环。此时, p 是 $\mathbb{Z}[\sqrt{-1}]$ 中的素元。
- $X^2 + 1$ 是 $\mathbb{Z}/p\mathbb{Z}[X]$ 中可约, 那么, 我们必然有 $X^2 + 1 = (X + a)(X - a)$, 其中, $a^2 = -1$ 并且 $a \in \mathbb{Z}/p\mathbb{Z}$ 。这等价于说 $-1 \in \mathbb{Z}/p\mathbb{Z}$ 是完全平方 (如果 -1 不是完全平方, 该多项式不可约)。此时, $(X - a) + (X + a) = \mathbb{Z}/p\mathbb{Z}[X]$ (即这两个理想互素), 根据中国剩余定理,

$$\mathbb{Z}/p\mathbb{Z}[X]/(X^2 + 1) \simeq \mathbb{Z}/p\mathbb{Z}[X]/(X + a) \times \mathbb{Z}/p\mathbb{Z}[X]/(X - a).$$

⁵如果 $x + y\sqrt{-1} \in \mathfrak{p} - \{0\}$, 那么, $x^2 + y^2 \in \mathfrak{p} \cap \mathbb{Z}$ 。

⁶我们用到了如下重要的性质: $\varphi: A \rightarrow B$ 是环同态, $J \subset B$ 是理想, 那么, $\varphi^{-1}(J) \subset A$ 是理想。进一步, 如果 J 是素理想, 那么, $\varphi^{-1}(J)$ 也是素理想。

在文中所讨论例子的背景下, 我们有环同态 $\mathbb{Z} \hookrightarrow \mathbb{Z}[\sqrt{-1}]$ 。

这显然不是整环（因为 $(1,0) \cdot (0,1) = (0,0)$ ），从而， p 不是 $\mathbb{Z}[\sqrt{-1}]$ 中的素元。

以上分类讨论表明：

素数 p 在 $\mathbb{Z}[\sqrt{-1}]$ 中不可约当且仅当 -1 不是 $\mathbb{Z}/p\mathbb{Z}$ 中的完全平方。

这是初等数论中标准的二次剩余问题。假设 $\xi \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ 是该循环群的生成元，我们有 $-1 = \xi^d$ ，这里， $0 \leq d < p-1$ 。由于 $(-1)^2 = 1$ ，所以， $\xi^{2d} = 1$ ，从而， $p-1 \mid 2d$ 。根据要求， $2d < 2(p-1)$ ，从而， $2d = p-1$ 。我们分情况讨论：

- $p=2$ 。此时， $-1=1 \in \mathbb{Z}/2\mathbb{Z}$ 是完全平方。
- $p \equiv 1 \pmod{4}$ ，即 $p=4k+1$ 。此时， $-1 = \xi^{\frac{p-1}{2}} = \xi^{2k}$ 是完全平方。
- $p \equiv 3 \pmod{4}$ ，即 $p=4k+3$ 。此时， $-1 = \xi^{\frac{p-1}{2}} = \xi^{2k+1}$ 。如果 $-1 = b^2 = \xi^{2l}$ 是完全平方，那么， $\xi^{2k+1} = \xi^{2l}$ ，即 $\xi^{2k+1-2l} = 1$ 。这说明， $p-1 \mid 2k+1-2l$ 。然而， $p-1$ 是偶数，这是不可能的。从而， -1 不是完全平方。

综上所述，只有满足 $p \equiv 3 \pmod{4}$ 的素数 p 在 $\mathbb{Z}[\sqrt{-1}]$ 中仍然是不可约的。

当 $p \equiv 1 \pmod{4}$ 时，根据以上讨论，我们有

$$p = (x + y\sqrt{-1})(z + w\sqrt{-1}), \quad x, y, z, w \in \mathbb{Z}.$$

其中， $x + y\sqrt{-1}z + w\sqrt{-1}$ 是 $\mathbb{Z}[\sqrt{-1}]$ 中的不可约元素。另外，我们必然有

$$N(x + y\sqrt{-1}) = p \Rightarrow x^2 + y^2 = p \Rightarrow p = (x + y\sqrt{-1})(x - y\sqrt{-1}).$$

根据 $\mathbb{Z}[\sqrt{-1}]$ 的唯一分解性质， $z + w\sqrt{-1} \in \{\pm 1, \pm \pi\sqrt{-1}\} \cdot x - y\sqrt{-1}$ 。这就给出了 Fermat 的著名定理：素数 p 可以写成两个完全平方数之和当且仅当 $p \equiv 1 \pmod{4}$ ，进一步， $p = x^2 + y^2$ 的写法是唯一的。

另外，利用图表

$$\begin{array}{ccc} p & \xrightarrow{\subset} & \mathbb{Z}[\sqrt{-1}] \\ \uparrow & & \uparrow \\ p \cap \mathbb{Z}[\sqrt{-1}] = (p) & \xrightarrow{\subset} & \mathbb{Z} \end{array}$$

我们还找到了 $\mathbb{Z}[\sqrt{-1}]$ 中的所有不可约元（在相伴意义下的代表）

$$\{1 + \sqrt{-1}, x \pm y\sqrt{-1}, q \mid p, q \text{ 是素数}, x^2 + y^2 = 1, x > 0, y > 0, p \equiv 1 \pmod{4}; q \equiv 3 \pmod{4}\}$$

我们首先回忆，在唯一分解整环 A 中，对于 $a = up_1^{d_1}p_2^{d_2}\cdots p_n^{d_n}$ 和 $b = vp_1^{e_1}p_2^{e_2}\cdots p_n^{e_n}$ ，其中， $u, v \in A^\times$ ， p_i 和 q_j 都是不可约元素并且 d_i 和 e_j 都是非负整数。 $a \mid b$ 等价于 $d_i \leq e_i$ ，其中， $i = 1, \dots, n$ 。所以，我们可以定义 a 和 b 的最大公约数和最小公倍数。

给定 $P(X) \in A[X]$ ， $P(X) = a_nX^n + \cdots + a_1X + a_0$ ，令 $c(P)$ 为 a_0, a_1, \dots, a_n 的最大公约数（之一）， $c(P)$ 在伴随的意义下是唯一的。我们把这个量称作是 P 的容量（content）。

注 给定环同态 $A \rightarrow B$ ，我们有自然的同态 $A[X] \rightarrow B[X]$ 。

引理 5.2

A 是唯一分解整环， $P, Q \in A[X]$ ，那么， $c(P)c(Q)$ 与 $c(PQ)$ 相伴。



证明 先证明特殊情形: $c(P), c(Q) \in A^\times$ 。此时, $c(P)c(Q) \in A^\times$ 。假设 $P(X) = a_n X^n + \cdots + a_1 X + a_0$, $Q(X) = b_m X^m + \cdots + b_1 X + b_0$, 我们证明对任意的不可约元 p , $p \nmid c(PQ)$ 。由于 $c(P) \in A^\times$, 所以存在 $0 \leq k_0 \leq n$, 使得 $p \mid a_0, p \mid a_1, \dots, p \mid a_{k_0-1}$ 但是 $p \nmid a_{k_0}$ (否则 $p \mid c(P)$); 类似地, 存在 $0 \leq l_0 \leq m$, 使得 $p \mid b_0, p \mid b_1, \dots, p \mid b_{l_0-1}$ 但是 $p \nmid b_{l_0}$ 。那么, $(PQ)(X)$ 的 $X^{k_0+l_0}$ 的系数为恰为

$$a_{k_0} b_{l_0} + \sum_{k+l=k_0+l_0, (k,l) \neq (k_0, l_0)} a_k b_l = a_{k_0} b_{l_0} \pmod{p}.$$

由于 (p) 是素理想, $a_{k_0} b_{l_0} \notin (p)$, 所以, p 不整除这个系数。特别的, $p \nmid c(PQ)$ 。从而, $c(PQ) \in A^\times$ 。一般的情形, 我们可以先提取 P 和 Q 的系数的最大公约数。

引理 5.3 (Gauss 引理)

A 是唯一分解整环, $K = \text{Frac}(A)$ 为其分式域, $P(X) \in A[X]$ 。那么, $P(X)$ 在 $A[X]$ 中不可约当且仅当 $P(X)$ 在 $K[X]$ 中不可约。^a进一步, 如果在 $K[X]$ 中有 $P(X) = P_1(X)P_2(X)$, 其中, $\deg(P_i) \geq 1$, 那么存在 $k \in K^\times$, 使得 $kP_1(X), k^{-1}P_2(X) \in A[X]$ 。

^a我们约定 $P(X)$ 在 $A[X]$ 中不可约指的是它不能分解成两个次数更低的多项式之积。当然, 如果它的系数有公因数, 我们可以进一步提取, 所以, 我们通常不考虑这种情形。



证明 选取 $P(X) \in A[X]$ 并要求 $c(P) = 1$ 。假设 P 在 $K[X]$ 中可约, 即 $P(X) = P_1(X)P_2(X)$, 其中, $P_i(X) \in K[X]$ 的系数形如 $\frac{a'_i}{a''_i}$, $a'_i, a''_i \in A$ 。通过先通分再提取系数分子的最大公约数, 我们可以把 $P_i(X)$ 写成

$$P_1(X) = \frac{a'}{b'} Q_1(X), \quad P_2(X) = \frac{a''}{b''} Q_2(X),$$

其中, $Q_i(X) \in A[X]$ 并且 $c(Q_1), c(Q_2) \in A^\times$ 。从而,

$$P(X) = \frac{a' a''}{b' b''} Q_1(X) Q_2(X) = \frac{a'''}{b'''} Q_1(X) Q_2(X),$$

其中, 通过约分, 我们有 $a''' \in A$ 与 $b''' \in A$ 没有公共不可约因子。所以,

$$b''' P = a''' Q_1(X) Q_2(X).$$

从而,

$$b''' = c(b''' P) = c(a''' Q_1(X) Q_2(X)) = a'''.$$

这表明, $a''', b''' \in A^\times$, 所以, $P(X) = u Q_1(X) Q_2(X)$ 可约。这就完成了证明。

定理 5.2 (Gauss)

A 是唯一分解整环, 那么, $A[X]$ 也是。



证明 首先证明分解的存在性。对任意的 $P(X) \in A[X]$, 通过提取系数的最大公约数, 不妨假设 $c(P) = 1$ 。将 $P(X)$ 视作是 $K[X]$ 中的多项式, 其中, $K = \text{Frac}(A)$, 我们显然有 $P(X) = f_1(X) \cdots f_m(X)$ 。根据 Gauss 引理, 我们可以假设 $f_1(X), \dots, f_m(X)$ 都是 $A[X]$ 中的多项式 (可以要求其容量均为 1), 这就给出了存在性。

现在证明唯一性, 如果 $P(X) = f_1(X) \cdots f_m(X) = g_1(X) \cdots g_n(X)$, 那么, 通过将这些多项式视作是 $K[X]$ 中的多项式, 我们有 $m = n$ 并且 $f_k(x) = \lambda_k g_k(X)$, 其中, $\lambda_k \in K^\times$ 。对固定的 k , 我

们就有

$$a_k f_k(X) = b_k g_k(X),$$

其中, f_k, g_k 的容量为 1 并且 a_k 和 b_k 没有公因子。此时, 通过取容量, 我们知道 $a_k = b_k \bmod A^\times$, 从而, a_k, b_k 都是 A^\times 中元素, 这就完成了证明。

例题 5.11 如何判断不可约性 假设 $P(X) \in A[X]$ 并且 $\deg P \leq 3$, 那么, $P(X)$ 可约当且仅当 P 在 $K[X]$ 有根。假设 $x = \frac{b}{b'} \in K$ 是 P 的根, 其中, b 与 b' 没有公因子, 那么, b 整除 P 的常数项系数, b' 整除 P 的首项系数。

作为例子, 我们考虑 $\mathbb{Z}[X]$ 中的多项式 $X^3 + X - p$, 其中, p 是素数。那么, 如果它可约, 那么, 这个根只能是 ± 1 或者 $\pm p$ 。据此, 唯一的可能是 $p = 2$, $X - 1 \mid X^3 + X - 2$ 。其余情形该多项式不可约。

K 是域, $f(X) \in K[X]$ 并且 $f(X)$ 不是某个多项式的平凡, 那么, $Y^2 - f(X)$ 在 $K[X, Y]$ 中不可约。

令 $A = K[X]$, 注意到 $K[X, Y] = K[X][Y]$ 是唯一分解整环, 我们把 $Y^2 - f(X)$ 视作是 $A[Y]$ 中的元素。如果 $Y^2 - f(X)$ 可约, 那么, 在 $A[Y]$ 中就有

$$Y^2 - f(X) = (h_1(X)Y - g_1(X))(h_2(X)Y - g_2(X)), \quad h_i, g_i \in K[X].$$

待定系数表明 $h_1(X), h_2(X) \in A^\times = K$, 从而, 我们可以假设 $h_1(X) = h_2(X) = 1$, 此时, $g_1(X) + g_2(X) = 0$, 从而, $f(X) = g_1(X)^2$ 。

例题 5.12 不可约性的 Eisenstein 判别法 A 是唯一分解整环, $P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in A[X]$, $\mathfrak{p} \subset A$ 是素理想。假设

$$a_n \notin \mathfrak{p}, a_{n-1}, \dots, a_1, a_0 \in \mathfrak{p}, a_0 \notin \mathfrak{p}^2,$$

那么, $P(X)$ 在 $A[X]$ (和 $K[X]$) 中不可约。

我们用反证法, 如果 $P(X) = P_1(X)P_2(X)$, 那么, 在 $A/\mathfrak{p}[X]$ 中来看, 我们有

$$X^n = \overline{P_1}(X) \cdot \overline{P_2}(X) \Rightarrow \overline{P_1}(X) = X^k, \overline{P_2}(X) = X^l, k + l = n.$$

由于 $a_n \notin \mathfrak{p}$, 所以, $k \neq 0, l \neq 0$ 。从而, $P_1(X)$ 和 $P_2(X)$ 的常数项系数在 \mathfrak{p} 中 (因为在 A/\mathfrak{p} 中为 0), 从而, $a_0 \in \mathfrak{p}^2$ 。矛盾。

我们有两个经典应用:

1) p 是素数, 那么, $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$ 在 $\mathbb{Z}[X]$ 中不可约。

实际上, $\Phi_p(X)$ 不可约等价于 $\Phi_p(X+1)$ 不可约。然而,

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = p + \sum_{k=2}^p \binom{p}{k} X^{k-1}.$$

此时, 最高项系数为 1, 其余系数都被 p 整除但是 p^2 不整除常数项系数, 这就可以应用 Eisenstein 判别法。

5.3 主理想整环上的有限生成模

定义 5.7

A 是环, $(M, +)$ 是交换群。如果存在映射

$$A \times M \rightarrow M, (a, m) \mapsto a \cdot m,$$

使得对任意的 $a, a' \in A$ 和 m, m' , 我们有

$$1 \cdot m = m, a \cdot (a' \cdot m) = (a \cdot a') \cdot m,$$

$$a \cdot (m + m') = a \cdot m + a \cdot m', (a + a') \cdot m = a \cdot m + a' \cdot m,$$

我们就称 $(M, +)$ 或 M 是一个 (左) A -模。

如果 $N \leq M$ 是 M 的加法子群并且对任意的 $a \in A$ 和 $n \in N$, 都有 $a \cdot n \in N$, 我们就称 $(N, +)$ 是 M 的一个子 A -模或子模。



例题 5.13 A 是环, 那么, A 是 A -模。此时, $I \subset A$ 是子模当且仅当 I 是 A 的 (左) 理想。

例题 5.14 A 和 B 是环, $\varphi: A \rightarrow B$ 是环同态, 那么, B 具有自然的 A -模结构:

$$A \times B \rightarrow B, (a, b) \mapsto ba \cdot b := \varphi(a) \cdot_B b.$$

例题 5.15 如果 $A = K$ 是域, 那么, K -模是 K -线性空间。

如果 $A = \mathbb{Z}$, 那么, \mathbb{Z} -模是交换群。

例题 5.16 K 是域, $A = K[X]$ 是 K 上的多项式环, V 是 K -线性空间。给定线性映射 $T \in \text{End}_K(V)$, 我们可以给出 V 上的一个 $K[X]$ -模的结构:

$$K[X] \times V \rightarrow V, (P(X), v) \mapsto P(T)v.$$

也就是说, 对任意的 $P(X) = a_n X^n + \cdots + a_1 X + a_0$, 其中, $a_i \in K$, 我们令

$$P(X) \cdot v = a_n T^n(v) + \cdots + a_1 T(v) + a_0 v.$$

很显然, 我们有

$$(P + Q)(T) = P(T) + Q(T), (P \cdot Q)(T) = P(T) \circ Q(T).$$

所以, M 是 $K[X]$ -模 (由 T 决定)。

定义 5.8 (A -模同态)

$(M_1, +_1)$ 和 $(M_2, +_2)$ 是 A -模, $\varphi: M_1 \rightarrow M_2$ 是映射。如果该映射保持加法和乘法, 即对任意的 $a \in A$ 和 $m, m' \in M_1$, 有

$$\varphi(m +_1 m') = \varphi(m) +_2 \varphi(m'), \varphi(a \cdot_1 m) = a \cdot_2 \varphi(m),$$

我们就称 φ 是以上两个 A -模之间的 A -模同态 (也被称作是 A -线性映射)。我们用 $\text{Hom}_A(M_1, M_2)$ 表示它们之间所有的模同态。如果 φ 是双射, 我们称 φ 是它们之间的一个 A -模同构。如果 M_1 与 M_2 之间存在环同构, 我们称这两个 A -模是同构的并记作是 $M_1 \simeq M_2$ 。



注 假设 A 是交换环, $\text{Hom}_A(M_1, M_2)$ 具有自然的 A -模结构:

$$A \times \text{Hom}_A(M_1, M_2) \rightarrow \text{Hom}_A(M_1, M_2), (a, \varphi) \mapsto (a \cdot \varphi: m_1 \mapsto a \cdot \varphi(m_1)).$$

例题 5.17 给定 $\varphi \in \text{Hom}_A(M_1, M_2)$, $\text{Ker}(\varphi) := \{m \in M_1 \mid \varphi(m) = 0\}$. 这是 M_1 的子模. 另外, φ 是单射当且仅当 $\text{Ker}(\varphi) = \{0\}$.

给 A -模 M 及其子模 N , 我们可以构造其商模 M/N . 按定义, 这是加法群的商群:

$$M/N = \{m + N \mid m \in M\}.$$

它的 A -模结构由如下公式给出:

$$A \times M/N \rightarrow M/N, (a, m + N) \mapsto a(m + N) := am + N.$$

容易验证, 以上乘法的定义不依赖于 $m + N$ 中代表元的选取. 这就给出了商模 M/N 的定义. 另外, 商映射给出了自然的 A -模同态:

$$\pi: M \rightarrow M/N, m \mapsto m + N.$$

这是满的 A -模同态。

命题 5.4

M 和 M' 是 A -模, $N \subset M$ 是子模, $\varphi: M \rightarrow M'$ 是 A -模同态. 如果 $N \subset \text{Ker}(\varphi)$, 那么存在唯一的 A -模同态 $\bar{\varphi}: M/N \rightarrow M'$, 使得 $\bar{\varphi} \circ \pi = \varphi$, 其中, $\pi: M \rightarrow M/N$ 是自然的同态.

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & M' \\ \downarrow \pi & \nearrow \bar{\varphi} & \\ M/N & & \end{array}$$

进一步, 我们还有 A -模同构 $\bar{\varphi}: M/\text{Ker}(\varphi) \xrightarrow{\simeq} \text{Im}(\varphi)$.

证明 这个证明之前已经出现过两次, 这一次留给同学们验证。

$\{M_i\}_i$ 是一族 A -模. 我们在 $\prod_i M_i$ 上定义 A -模结构:

$$A \times \prod_i M_i \rightarrow \prod_i M_i, (a, (m_i \in M_i)_i) \mapsto (a \cdot m_i)_i.$$

容易验证, 这是 A -模. 我们把它称作是 $\{M_i\}_i$ 的乘积. 对每个 i_0 , 我们有投影映射 (A -模同态)

$$\pi_{i_0}: \prod_i M_i \rightarrow M_{i_0}, (m_i)_i \mapsto m_{i_0}.$$

我们还可以构造 $\{M_i\}_i$ 的直和 $\bigoplus_i M_i$. 作为集合, 我们有

$$\bigoplus_i M_i = \{(m_i)_i \in \prod_i M_i \mid \text{除去有限个 } i \text{ 之外, 其余 } m_i \text{ 均为 } 0\}.$$

其 A -模结构定义为

$$A \times \bigoplus_i M_i \rightarrow \bigoplus_i M_i, (a, (m_i \in M_i)_i) \mapsto (a \cdot m_i)_i.$$

对每个 i_0 , 我们有嵌入映射 (A -模同态)

$$\iota_{i_0}: M_{i_0} \rightarrow \bigoplus_i M_i \quad m_{i_0} \mapsto (0, \dots, 0, m_{i_0}, 0, \dots).$$

注 M 是 A -模, N_1, N_2 是子模。假设 $N_1 \cap N_2 = 0$ 并且 $N_1 + N_2 = M$, 其中,

$$N_1 + N_2 := \{n_1 + n_2 \mid n_1 \in N_1, n_2 \in N_2\}.$$

那么, $N \simeq N_1 \oplus N_2$ 。

例题 5.18 我们可以自然地定义 A -模 $A^n = \underbrace{A \oplus A \oplus \dots \oplus A}_n$ 。

实际上, 对任意的 $n \in N$, 根据 $N_1 \cap N_2 = 0$, 存在唯一的 $n_1 \in N_1, n_2 \in N_2$, 使得 $n = n_1 + n_2$ 。从而, 映射

$$N_1 \oplus N_2 \rightarrow N, (n_1, n_2) \mapsto n_1 + n_2$$

是双射。不难验证, 这是 A -模同态。

M 是 A -模, $\{M_i\}_i$ 是子模的集合, 那么, 如下 M 的子集均为子模:

$$\bigcap_i M_i, \quad M_1 + \dots + M_n = \{x_1 + x_2 + \dots + x_n \mid x_1 \in M_1, \dots, x_n \in M_n\}.$$

给定 M 的非空子集 $S \subset M$, 包含 S 的所有子模的交集是包含 S 的最小子模 (在包含关系下), 我们把它称作是由 S 所生成的子模, 并记作是 (S) 。如果 N 可以由一个元素 x 生成, 我们就称 N 是循环模。

与交换群的情形类似, 如果 M 可以由有限子集 S 生成, 我们就说 M 是有限生成的。 M 是有限生成的 A -模当且仅当存在整数 n 以及满的 A -模同态 $A^n \rightarrow M$ 。

如果 N 是循环模, 那么, 我们有满同态:

$$A \rightarrow M, \quad a \mapsto a \cdot x.$$

从而, $M \simeq A / (\text{Ker}(\varphi))$ 。所以, 循环 A -模都形如 A/I , 其中, I 是 A 的理想。这里, A/I 的 A -模结构由自然的投影映射 $A \rightarrow A/I$ 给出。

定义 5.9 (Noether 环)

如果 A 的每个理想都是有限生成的, 我们就称 A 是 Noether 环。



例题 5.19 主理想整环是 Noether 环。

注 Noether 环还有另外一个等价的定义: 环 A 满足所谓的上升理想链的稳定条件, 即对任意 A 中的理想链

$$I_1 \subset I_2 \subset \dots \subset I_n \subset \dots$$

存在 $n_0 \geq 1$, 使得当 $n \geq n_0$ 时, $I_n = I_{n_0}$ 。

假设 A 是 Noether 环, 我们证明以上的稳定条件: 令 $I = \cup_{k \geq 1} I_k$, 这显然是理想。如果 $1 \in I$, 那么, 存在 n_0 , 使得 $1 \in I_{n_0}$, 所以, 当 $n \geq n_0$ 时, 我们有 $A = I_n$; 如果 $1 \notin I$, 我们假设 $I = (x_1, \dots, x_l)$, 此时, 存在 n_0 , 使得 $x_1, \dots, x_l \in I_{n_0}$, 从而, 当 $n \geq n_0$ 时, 我们有 $I = I_n$ 。

反之, 任意选定理想 $I \subset A$, 任选 $x_1 \in I$, 考虑 $(x_1) \subset I$, 如果 I 不是有限生成, 那么有

$x_2 \in I - (x_1)$; 考虑 $(x_1, x_2) \subset I$, 如果 I 不是有限生成, 那么有 $x_3 \in I - (x_1, x_2)$ 。如此往复, 我们得到理想的升链:

$$(x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, x_2, \cdots, x_n) \subset \cdots$$

这个链是严格上升的, 矛盾。

根据定义, 如果 A 是 Noether 环, A 作为 A -模, 它的每个子模都是有限生成的。

命题 5.5

Noether 环上的有限生成模的子模也是有限生成的。

证明 假设 M 是 Noether 环 A 上的有限生成模, 它可以被 n 个元素生成。我们对 n 进行归纳。

当 $n=1$ 时, $M \simeq A/I$ ⁷, 其中, I 是理想。假设 $J \subset A/I$ 是子模, 这也是 A 中包含 I 的理想, 根据 A 是 Noether 环, J 是有限生成的。

假设问题对于具有不超过 $n-1$ 个生成元的 M 成立, 其中, $n \geq 2$ 。此时, 我们有

$$M = (x_1, x_2, \cdots, x_n) = Ax_1 + Ax_2 + \cdots + Ax_n.$$

$N \subset M$ 是子模。令 $M' = (x_1, x_2, \cdots, x_{n-1})$, 此时, M/M' 由 $x_n + M'$ 生成。在商映射 $\pi: M \rightarrow M/M'$ 下, $\pi(N) \subset M/M'$ 是子模, 所以, 它可以由有限个 $y_1 + M', \cdots, y_m + M'$ 生成。我们现在证明

$$N = N \cap M' + Ay_1 + Ay_2 + \cdots + Ay_m.$$

实际上, 对任意的 $x \in N$, 根据 y_i 的定义, 存在 a_1, \cdots, a_m , 使得 $\pi(x) = a_1\pi(y_1) + \cdots + a_m\pi(y_m)$ 。这表明 $x - (a_1y_1 + \cdots + a_my_m) \in \text{Ker}(\pi)$, 即 $x - (a_1y_1 + \cdots + a_my_m) \in N \cap M'$ 。根据归纳假设, $N \cap M'$ 是有限生成的, 从而, N 是有限生成。

练习 5.9 重要 A 是主理想整环, M 是由 n 个元素生成的模。重复上述证明并做相应的修改, 证明, 如果 $N \subset M$ 是子模, 那么, N 可以由不超过 n 个元素生成。

命题 5.6

A 是交换环, $\varphi: A^n \rightarrow A^m$ 是满的模同态。那么, $n \geq m$ 。特别地, $A^m \simeq A^n$ 当且仅当 $m = n$ 。

证明 任选极大理想 $\mathfrak{m} \subset A$, 令 $\mathfrak{m}^n = (x_1, \cdots, x_n)$, 其中, $x_1, \cdots, x_n \in \mathfrak{m}$ 。这是 A^n 的子模, 从而, 有自然的商映射:

$$A^n \longrightarrow A^n/\mathfrak{m}^n \simeq A/\mathfrak{m} \oplus \cdots \oplus A/\mathfrak{m}.$$

这是 n -维 A/\mathfrak{m} -线性空间。从而, 我们有如下的交换图

$$\begin{array}{ccc} A^n & \xrightarrow{\varphi} & A^m \\ \downarrow \pi & & \downarrow \pi \\ (A/\mathfrak{m})^n & \dashrightarrow & (A/\mathfrak{m})^m \end{array}$$

对任意的 $x \in \mathfrak{m}^n$, 它可以被写成 $x = (m_1, \cdots, m_n)$ 。此时, $\varphi(m_1, 0, \cdots, 0) = m_1 \cdot \varphi(1, 0, \cdots, 0) \in \mathfrak{m}^m$ 。这表明 $\mathfrak{m}^n \subset \text{Ker}(\pi \circ \varphi)$, 从而, 存在映射 $\psi: (A/\mathfrak{m})^n \rightarrow (A/\mathfrak{m})^m$, 使得以上图表是交换的。这

⁷ 因为我们有模的满射 $A \twoheadrightarrow M$, 从而, $M \simeq A/\text{Ker}(\varphi)$ 。

个映射还是满射，从而， $m \geq n$ （因为这是线性空间之间的满射）。

A 是交换环， p, q 是正整数， $\mathbf{M}_{p,q}(A)$ 是 A 系数的 $p \times q$ 的矩阵全体。我们还记 $\mathbf{M}_n(A) = \mathbf{M}_{n,n}(A)$ ，它在矩阵乘法下是环。我们定义

$$\mathbf{GL}(n; A) = \mathbf{M}_n(A)^\times.$$

这是 $n \times n$ 的可逆矩阵。另外，给定 $M \in \mathbf{M}_n(A)$ ，我们用 M^{ad} 表示其伴随矩阵（由余子式构成的矩阵）。我们仍然有

$$\det(M \cdot M') = \det(M)\det(M'), \quad M \cdot {}^t M^{\text{ad}} = {}^t M^{\text{ad}} \cdot M = \det(M) \cdot I.$$

注 利用以上关于伴随矩阵的公式，我们有 $\mathbf{GL}(n; A) = \{M \in \mathbf{M}_n(A) \mid \det(M) \in A^\times\}$ 。

现在考虑 $\mathbf{GL}(p; A) \times \mathbf{GL}(q; A)$ 在 $\mathbf{M}_{p,q}(A)$ 上的作用，其中，

$$(\mathbf{GL}(p; A) \times \mathbf{GL}(q; A)) \times \mathbf{M}_{p,q}(A) \rightarrow \mathbf{M}_{p,q}(A), \quad ((P, Q), M) \mapsto P \cdot M \cdot Q^{-1}.$$

我们的目标是在每个轨道中选取一个形式尽可能简单的代表元。

定理 5.3 (Smith 正规型)

A 是主理想整环， $M \in \mathbf{M}_{p,q}(A)$ 。那么，在 M 的轨道中存在如下形式的矩阵：

$$P \cdot M \cdot Q^{-1} = \left(\begin{array}{ccc|c} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_r \\ & & & \mathbf{0} \end{array} \right)$$

（不妨 $p \leq q$ ，以上 $r = \min(p, q) = q$ ）其中， a_1, \dots, a_r 是仅有的可能不为 0 的元素， $(a_1) \supset (a_2) \supset \dots \supset (a_r)$ 并且的 a_i 在相伴随的意义下是唯一的。



推论 5.2 (线性映射版本)

A 是主理想整环， $M \simeq A^q$ 和 $N \simeq A^p$ 是自由的 A -模。对任意的 A -模同态 $\varphi: M \rightarrow N$ ，存在 M 的基 u_1, \dots, u_q 和 N 的基 v_1, \dots, v_p 以及 $a_1, \dots, a_r \in A$ ，其中， $r \leq \min(p, q)$ ，使得

$$(a_1) \supset (a_2) \supset \dots \supset (a_r), \quad \varphi(u_i) = \begin{cases} a_i v_i, & i \leq r; \\ 0, & i > r. \end{cases}$$



命题 5.7 (主理想整环上自由模的子模结构)

A 是主理想整环， $M \simeq A^n$ 自由的 A -模， $N \subset M$ 是子模。那么， N 是自由的 A -模。进一步，存在 M 的基 e_1, \dots, e_n 以及 $r \leq n$ 和 $a_1, \dots, a_r \in A$ ，使得 $(a_1) \supset (a_2) \supset \dots \supset (a_r)$ 并且 $a_1 e_1, \dots, a_r e_r$ 是 N 的基。



证明 根据命题 5.5（以及之后的练习），存在 $r \leq n$ 以及 A -模同态 $\varphi: A^r \rightarrow N \subset M$ ，对此映射使用上一推论即可。

证明 [定理的证明] 我们对 $p+q$ 进行归纳。当 $p+q=2$ 时，命题明显成立。现在假设对 $k \geq 3$ ，对任意的 $p+q < k$ ，命题成立。我们现在对 $p+q=k$ 来证明该命题。

对 $a \in A$, 假设 $a = up_1^{e_1} \cdots p_k^{e_k}$ 是 a 用不可约元的唯一分解, 我们令 $F(a) = e_1 + \cdots + e_k$ 。对于 $M = (m_{i,j})_{i \leq p, j \leq q}$, 通过对 M 的左右乘以初等矩阵⁸ (调换两行或者两列), 我们可以假设对每个 $F(m_{1,1}) = \min_{i,j} F(m_{i,j})$ 。我们还令 $F(M) = \min_{i,j} F(m_{i,j})$ 。

我们现在考虑 M 的第一行和第一列的元素 $m_{1,j}$ 和 $m_{i,1}$, 其中, $i, j \geq 2$ 。分两种情况讨论:

(1) 存在某个 $m_{1,j}$ 或者 $m_{i,1}$ 不被 $m_{1,1}$ 整除。

通过对 M 的左右乘以初等矩阵, 不妨假设 $m_{1,2} \notin (m_{1,1})$ 。由于 A 是主理想整环, 所以存在 $d \in A$, 使得 $(d) = (m_{1,1}, m_{1,2})$ 。特别地, 由于 $(m_{1,1}) \neq (d)$ (否则 $m_{1,2} \in (m_{1,1})$), 我们有 $F(d) < F(m_{1,1})$ 。所以, 存在 $a, b \in A$, 使得

$$am_{1,1} + bm_{1,2} = d \Rightarrow ax + by = 1.$$

其中, $x = \frac{m_{1,1}}{d}$, $y = \frac{m_{1,2}}{d}$ 。我们构造分块对角的 $q \times q$ 矩阵⁹:

$$Q' = \begin{pmatrix} a & -y & & \\ b & x & & \\ & & 1 & \\ & & & \ddots \\ & & & & 1 \end{pmatrix}$$

根据 $ax + by = 1$, $Q' \in \mathbf{GL}(n; A)$ 。所以, $M \cdot Q'$ 的 $(1,1)$ 位置为 $am_{1,1} + bm_{1,2} = d$ 。此时, $F(d) < F(m_{1,1})$, 从而, 新得到的 M' 满足 $F(M') < F(M)$ 。

现在再通过调整行和列的位置, 我们可以假设 $F(m'_{1,1}) = F(M)$, 重复以上过程, 一直到 $m'_{1,j}$ 或者 $m'_{i,1}$ 均被 $m'_{1,1}$ 整除为止。

(2) 所有的 $m_{1,j}$ 或者 $m_{i,1}$ 都是 $m_{1,1}$ 的倍数。

此时, 我们可以通过对 M 左右乘以初等矩阵消去这些第一行和第一列这些位置的数, 使得 M 形如:

$$M = \begin{pmatrix} a_1 & 0 & 0 & 0 \\ 0 & * & * & * \\ \cdots & \cdots & \cdots & \cdots \\ 0 & * & * & * \end{pmatrix}$$

如果以上某个 $*$ 不是 a_1 的倍数, 我们可以将这一行加到第一行去, 此时, 我们回到了情形 (1)。如此往复, 我们可以假设所有的 $*$ 都是 a_1 的倍数。对 $*$ 所构成的矩阵可以提出这个因子, 然后利用归纳假设即可。

以上的推理还给出了具体的算法。

为了证明唯一性, 我们回忆所谓的 **Cauchy-Binet** 公式: 给定 A -系数的 $m \times n$ 矩阵 M 和 $n \times m$ 的矩阵 N , 其中, $m \leq n$ 。对任意的 $1 \leq j_1 < j_2 < \cdots < j_m \leq n$, 我们定义 $M_{\underline{j}}$ 为 M 的第 j_1, j_2, \dots, j_m 列 (按照既定的顺序) 给出的 $m \times m$ 的矩阵, $N_{\underline{j}}$ 为 N 的第 j_1, j_2, \dots, j_m 行 (按照

⁸这些初等矩阵是 $\mathbf{GL}(p; A)$ 或者 $\mathbf{GL}(q; A)$ 中的元素

⁹我们用到了 $q \geq 2$, 实际上, 如果 $q = 1$, 命题是显然的

既定的顺序) 给出的 $m \times m$ 的矩阵, 其中, $\underline{j} = (j_1, \dots, j_m)$ 。

对于 $m \times m$ 的矩阵 M , 它的行列式被定义为:

$$\det(M) = \sum_{\sigma \in \mathfrak{S}_m} \varepsilon(\sigma) M_{1\sigma(1)} M_{2\sigma(2)} \cdots M_{m\sigma(m)}.$$

我们有如下的 **Cauchy-Binet** 公式:

$$\det(M \cdot N) = \sum_{\underline{j}} \det(M_{\underline{j}}) \det(N_{\underline{j}}). \quad (5.1)$$

我们可以直接计算:

$$\begin{aligned} \det(M \cdot N) &= \sum_{\sigma \in \mathfrak{S}_m} \varepsilon(\sigma) (M \cdot N)_{1\sigma(1)} (M \cdot N)_{2\sigma(2)} \cdots (M \cdot N)_{m\sigma(m)} \\ &= \sum_{\sigma \in \mathfrak{S}_m} \sum_{k_1=1}^n \sum_{k_2=1}^n \cdots \sum_{k_m=1}^n \varepsilon(\sigma) M_{1k_1} N_{k_1\sigma(1)} M_{2k_2} N_{k_2\sigma(2)} \cdots M_{mk_m} N_{k_m\sigma(m)} \\ &= \sum_{k_1, \dots, k_m=1}^n M_{1k_1} M_{2k_2} \cdots M_{mk_m} \sum_{\sigma \in \mathfrak{S}_m} \varepsilon(\sigma) N_{k_1\sigma(1)} N_{k_2\sigma(2)} \cdots N_{k_m\sigma(m)}. \end{aligned}$$

令 $N_{\underline{k}}$ 为 $N_{\underline{j}}$ 为 N 的第 k_1, k_2, \dots, k_m 行给出的 $m \times m$ 的矩阵, 其中, k_1, k_2, \dots, k_m 可以有相同的数并且我们不要求大小的顺序。此时, 根据定义

$$\varepsilon(\sigma) N_{k_1\sigma(1)} N_{k_2\sigma(2)} \cdots N_{k_m\sigma(m)} = \det(N_{\underline{k}}).$$

特别地, 我们可以要求以上 $\det(M \cdot N)$ 的求和中 k_1, k_2, \dots, k_m 两两不同 (否则, 这样的项给出了有行一样的矩阵的行列式, 从而贡献是 0)。所以, \underline{k} 可以被视作是 \mathfrak{S}_m 中的元素。据此,

$$\det(M \cdot N) = \sum_{\underline{k} \in \mathfrak{S}_m} M_{1k_1} M_{2k_2} \cdots M_{mk_m} \det(M_{\underline{k}}).$$

另外, $\det(M_{\underline{k}}) = \varepsilon(\underline{k}) \det(M_{\underline{j}})$, 其中, $1 \leq j_1 < j_2 < \cdots < j_m \leq n$ 是对 k_1, \dots, k_m 的重新排序。所以,

$$\begin{aligned} \det(M \cdot N) &= \sum_{\underline{k} \in \mathfrak{S}_m} \varepsilon(\underline{k}) M_{1k_1} M_{2k_2} \cdots M_{mk_m} \det(M_{\underline{j}}) \\ &= \det(N_{\underline{j}}) \det(M_{\underline{j}}). \end{aligned}$$

特别地, 根据 Cauchy-Binet 公式, 对于 $n \times n$ 的矩阵, 我们有

$$\det(M \cdot N) = \det(M) \det(N).$$

定义 5.10

$M \in M_{p,q}(A)$, 对于 $1 \leq k \leq \min(p, q)$, 我们令 $c_k(M) \subset A$ 为 M 的所有 k 阶子式所生成的理想。当 $k \leq 0$ 时, 我们令 $c_k(M) = A$; 当 $k > \min(p, q)$ 时, 我们令 $c_k(M) = 0$ 。



引理 5.4

对任意的 $k \in \mathbb{Z}$, $P \in \mathbf{GL}(p; A)$, $Q \in \mathbf{GL}(q; A)$ 和 $M \in \mathbf{M}_{p,q}(A)$, 我们有 $c_k(M) = c_k(P \cdot M \cdot Q)$ 。



证明 首先利用 Cauchy-Binet 公式说明 $c_k(M \cdot Q) \subset c_k(M)$ 。我们考察 $M \cdot Q$ 中由前 k 行和前 k 列所给的余子式。令 $M(k)$ 为 M 的前 k 行所构成的 $k \times q$ 的矩阵, $Q(k)_k$ 为 Q 的前 k 列所构成的

$q \times k$ 的矩阵, 那么以上余子式即为

$$\det(M(k) \cdot Q(k)) = \sum_{\underline{j}} \det(M(k)_{\underline{j}}) \det(Q(k)_{\underline{j}}) \subset c_k(M).$$

对于其它的余子式可以同样讨论, 所以, $c_k(M \cdot Q) \subset c_k(M)$ 。利用 Q 可逆的, 我们还有 $c_k(M) = c_k(M \cdot Q \cdot Q^{-1}) \subset c_k(M \cdot Q)$ 。所以, $c_k(M) = c_k(M \cdot Q)$ 。对于 P 可以同样地讨论。

证明 [唯一性部分的证明] 对于

$$P \cdot M \cdot Q^{-1} = \left(\begin{array}{ccc|c} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_r \end{array} \middle| \begin{array}{c} \\ \\ \\ \mathbf{0} \end{array} \right)$$

容易看出, $c_k(P \cdot M \cdot Q^{-1}) = (a_1 \cdots a_k) = c_k(M)$ 。由于每个主理想的生成元在差一个 A^\times 中的元素意义下是唯一的, 所以, a_1, \dots, a_k 被唯一决定。

定理 5.4 (主理想整环上有限生成模的结构)

A 是主理想整环, M 有限生成的 A -模, $N \subset M$ 是子模。那么, 存在 $r, s \in \mathbb{Z}_{\geq 0}$ 和 $a_1, \dots, a_s \in A$, 使得 $(a_1) \supset (a_2) \supset \cdots \supset (a_s)$ 并且

$$M \simeq A^r \oplus A/(a_1) \oplus A/(a_2) \oplus \cdots \oplus A/(a_s).$$

进一步, 以上的 a_1, \dots, a_s 在相伴的意义下是唯一的。



证明 由于 M 是有限生成的, 所以, 存在满的 A -模同态 $\varphi: A^n \rightarrow M$, 从而, $M \simeq A^n / \text{Ker}(\varphi)$ 。我们对 A^n 及其子模 $\text{Ker}(\varphi)$ 用子模结构理论就给出了定理的存在性部分。唯一性部分请参考习题???

由于每个交换群都可以被看作是 \mathbb{Z} -模, 以上定理又重新给出了有限生成交换群的结构定理

定理 5.5

A 是有限生成的交换群。那么, 存在唯一一组 $r \in \mathbb{Z}_{\geq 0}, d_1, \dots, d_s \in \mathbb{Z}_{\geq 2}$, 使得 $d_s \mid d_1, d_{s-1} \mid d_{s-2}, \dots, d_2 \mid d_1$ 并且

$$A \simeq \mathbb{Z}^r \times \prod_{i=1}^s \mathbb{Z}/d_i \mathbb{Z}.$$



例题 5.20 Jordan 标准型 V 是有限维 \mathbb{C} -线性空间, $T \in \text{End}_{\mathbb{C}}(V)$ 是 \mathbb{C} -线性映射, 那么, V 可以被看作是 $\mathbb{C}[X]$ 上的有限生成模:

$$\mathbb{C}[X] \times V \rightarrow V, (P(X), v) \mapsto P(T)v.$$

即对复系数多项式 $P(X) = a_n X^n + \cdots + a_1 X + a_0$, 我们有

$$P(X) \cdot v = a_n T^n(v) + \cdots + a_1 T(v) + a_0 v.$$

根据分类定理, 存在首一多项式 $P_1, \dots, P_s \in A$, 使得 $(P_1) \supset (P_2) \supset \cdots \supset (P_s)$ 并且

$$V \simeq \mathbb{C}[X]/(P_1(X)) \oplus \mathbb{C}[X]/(P_2(X)) \oplus \cdots \oplus \mathbb{C}[X]/(P_s(X)).$$

我们要指出, 上面的分解是 $\mathbb{C}[X]$ -模的直和, 所以, 也是 \mathbb{C} -线性空间的直和。

在以上分解中, 我们没有自由的部分, 即 $r = 0$, 这是因为根据 Hamilton-Cayley 定理, $P_T(T) = 0$, 其中, $P_T(X) \in \mathbb{C}[X]$ 是 T 的特征多项式, 这表明 $P_T(T) = 0$ 。另外一个看法是, 如果 $r \geq 1$, 那么, $\dim_{\mathbb{C}} \mathbb{C}[X] = \infty$, 与 $\dim_{\mathbb{C}} V < \infty$ 相矛盾。

对于每个 $P_i(X)$, 我们把它分解为不可约首一的多项式之积 $P_i(X) = p_1(X)^{d_1} \cdots p_n(X)^{d_n}$, 根据中国剩余定理 (作为环)

$$\mathbb{C}[X]/(P_1(X)) \simeq \mathbb{C}[X]/(p_1(X)^{d_1}) \times \cdots \times \mathbb{C}[X]/(p_n(X)^{d_n}).$$

我们把每个部分都看作是 $\mathbb{C}[X]$ -模, 就有

$$\mathbb{C}[X]/(P_1(X)) \simeq \mathbb{C}[X]/(p_1(X)^{d_1}) \oplus \cdots \oplus \mathbb{C}[X]/(p_n(X)^{d_n}).$$

根据代数基本定理, $\mathbb{C}[X]$ 中每个不可约多项式都形如 $X - \lambda$, 其中, $\lambda \in \mathbb{C}$ 。从而, 作为 $\mathbb{C}[X]$ -模, 我们有分解

$$V \simeq \prod \mathbb{C}[X]/((X - \lambda)^d).$$

将以上视作是 \mathbb{C} -线性空间的分解, 我们只要搞清楚 X 在 $\mathbb{C}[X]/((X - \lambda)^d)$ 上的作用即可。作为 \mathbb{C} -线性空间, $1, X - \lambda, \dots, (X - \lambda)^{d-1}$ 这 d 个向量生成了 $\mathbb{C}[X]/((X - \lambda)^d)$ 。它们显然是线性无关的, 否则, 存在 a_0, \dots, a_{d-1} 使得

$$a_0 + a_1(X - \lambda) + \cdots + a_{d-1}(X - \lambda)^{d-1} = 0 \Rightarrow a_0 + a_1(X - \lambda) + \cdots + a_{d-1}(X - \lambda)^{d-1} \in ((X - \lambda)^d).$$

通过观察它们的系数, 我们只有 $a_0 = \cdots = a_{d-1} = 0$ 。这样, 我们在 $\mathbb{C}[X]/((X - \lambda)^d)$ 给出了一组基:

$$e_1 = 1, e_2 = X - \lambda, \dots, e_d = (X - \lambda)^{d-1}.$$

此时, X 的 (也是 T 的) 作用为

$$X \cdot e_1 = e_2 + \lambda e_1, \quad X \cdots e_2 = e_3 + \lambda e_2, \dots, X \cdot e_d = \lambda e_d.$$

这表明 X 或者说 T 在这个子空间上对应的矩阵是

$$\begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix}$$

第6章 关于多项式的补充

6.1 多项式的导数

K 是域, 对任意的 $P(X) \in K[X]$, 假设 $P(X) = a_n X^n + \cdots + a_1 X + a_0$, 我们定义

$$P'(X) = n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \cdots + 2 a_2 X + a_1.$$

很显然, 求导映射 $P \mapsto P'$ 是 K -线性的。我们仍然有 Leibniz 法则, 即对任意的 $P(X), Q(X) \in K[X]$, 我们有公式

$$(P \cdot Q)' = P' \cdot Q + P \cdot Q'.$$

我们观察到以上等式的左右两边对于 P 和 Q 都是 K -双线性的。从而, 只要对 $P(X) = X^m$ 和 $Q(X) = X^n$ 验证即可, 这是显然的。

6.2 解式与判别式

K 是域。给定多项式 $P(X), Q(X) \in K[X]$, $\deg(P) = n, \deg(Q) = m$ 。令 $K[X]_{\leq d}$ 是次数不超过 d 的多项式, 我们定义映射

$$\Phi: K[X]_{\leq m-1} \oplus K[X]_{\leq n-1} \longrightarrow K[X]_{\leq m+n-1}, \quad (A(X), B(X)) \mapsto A(X)P(X) + B(X)Q(X).$$

这是 K -线性映射并且定义域和值域的维数均为 $n+m$ 。我们分别指定 $K[X]_{\leq m-1} \oplus K[X]_{\leq n-1}$ 和 $K[X]_{\leq m+n-1}$ 的基:

$$\{e_1 = (1, 0), e_2 = (X, 0), \cdots, e_m = (X^{m-1}, 0), e_{m+1} = (0, 1), e_{m+2} = (0, X), \cdots, e_{m+n} = (0, X^{n-1})\}$$

和

$$\{E_1 = (1, 0), E_2 = (X, 0), \cdots, E_{m+n} = (0, X^{m+n-1})\}.$$

如果

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0, \quad Q(X) = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0.$$

那么,

$$\Phi(e_i) = a_0 E_i + a_1 E_{i+1} + \cdots + a_n E_{i+n}, \quad 1 \leq i \leq m;$$

$$\Phi(e_{m+j}) = b_0 E_j + b_1 E_{j+1} + \cdots + a_n E_{j+m}, \quad 1 \leq j \leq n.$$

用矩阵的语言, 我们有 $(n+m) \times (n+m)$ 的矩阵 (Sylvester 矩阵):

$$\Phi = \begin{pmatrix} a_0 & 0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & 0 & \cdots & 0 & b_1 & b_0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & 0 & \cdots & \cdots & \ddots & 0 \\ \cdots & \cdots & \cdots & \cdots & a_0 & b_{m-1} & b_{m-2} & \cdots & b_0 \\ \cdots & \cdots & \cdots & \cdots & a_1 & b_m & b_{m-1} & \cdots & b_1 \\ a_{n-1} & a_{n-2} & 0 & \cdots & \cdots & 0 & b_m & \cdots & b_2 \\ a_n & a_{n-1} & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & a_n & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \ddots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & a_n & a_{n-1} & 0 & \cdots & b_m & b_{m-1} \\ 0 & 0 & \cdots & 0 & a_n & 0 & \cdots & 0 & b_m \end{pmatrix}$$

我们令 $\text{Res}(P, Q)$ 为以上矩阵的行列式并称之为 P 与 Q 的解式。按定义, $\text{Res}(P, Q)$ 是两个多项式系数 $a_0, \dots, a_n, b_0, \dots, b_m$ 的多项式。

很显然, Φ 是线性空间的同构当且仅当 $\text{disc}(P, Q) \neq 0$ 。另外, 如果 Φ 是同构, 那么, 存在 $A, B \in K[X]$, 使得 $A(X)P(X) + B(X)Q(X) = 1$, 从而, P 与 Q 是互素的; 反之, P 与 Q 互素, 我们来说明 Φ 是同构, 如果不然, 存在 $A \in K[X]_{\leq m-1}, B \in K[X]_{\leq n-1}$ 使得 $(A, B) \in \text{Ker}(\Phi)$, 即

$$A(X)P(X) + B(X)Q(X) = 0 \Rightarrow A(X)P(X) = -B(X)Q(X).$$

由于 P 与 Q 互素, 所以, $A(X) \mid Q(X)$ 。然而, $\deg(A) < \deg(Q)$, 这说明, $A = 0$, 从而, $B = 0$ 。

综上所述, 我们证明

命题 6.1

给定多项式 $P, Q \in K[X]$, $(P, Q) = 1$ 当且仅当 $\text{Res}(P, Q) \neq 0$ 。

如果知道 P 和 Q 的根, 我们可以利用下面的公式计算 $\text{Res}(P, Q)$:

命题 6.2

假设 $P(X) = a_n \prod_{i=1}^n (X - x_i), Q(Y) = b_m \prod_{j=1}^m (Y - y_j)$, 那么,

$$\text{Res}(P, Q) = (-1)^{nm} a_n^m b_m^n \cdot \prod_{i=1}^n \prod_{j=1}^m (x_i - y_j).$$

证明 我们不妨假设 $a_n = b_m = 1$ (通过提取公因式以及提取行列式每一列中的 a_n 和 b_m)。此时, 根据 Vieta 定理, 每个 a_i 和 b_j 都是 x_i 与 y_j 的多项式, 从而, $\text{Res}(P, Q)$ 也是。我们现在说明 $\text{Res}(P, Q)$ 作为 x_i 与 y_j 的多项式 (\mathbb{Z} -系数) 是齐次多项式并且其次数为 $m+n$ 。根据 $\text{Res}(P, Q)$ 的定义, 作为行列式的展开, 其中的一项形如

$$M_{\sigma(1),1} M_{\sigma(2),2} \cdots M_{\sigma(m+n),n}.$$

根据矩阵 M 的形式, 当 $k \leq m$ 时, $M_{\sigma(k),k}$ 的次数是 $n - (\sigma(k) - k)$; 当 $k \geq m+1$ 时, $M_{\sigma(k),k}$ 的

次数是 $m - (\sigma(k) - (k - m))$ 。从而，总次数为

$$\sum_{k=1}^m \left[n - (\sigma(k) - k) \right] + \sum_{k=m+1}^{m+n} \left[m - (\sigma(k) - (k - m)) \right] = mn.$$

如果 $x_i = y_j$ ，根据 Φ 的定义，构造 $A = \frac{Q}{X-y_j}$ 和 $B = -\frac{P}{X-x_j}$ 使得 $AP + BQ = 0$ 。从而， $x_i - y_j \mid \text{Res}$ 。从而， $\text{Res} = \lambda \prod_{i=1}^n \prod_{j=1}^m (x_i - y_j)$ ，其中， $\lambda \in \mathbb{Z}$ 。Res 中由对角线一项所贡献的是 $a_0^m = (-1)^{nm} x_1^m \cdots x_n^m$ ；而乘积给的这一项是 $x_1^m \cdots x_n^m$ ，所以， $\lambda = (-1)^{nm}$ 。

推论 6.1

我们有

$$\text{Res}(P, Q) = (-1)^{\deg(P) \cdot \deg(Q)} \text{Res}(Q, P).$$



推论 6.2

假设 $P(X) = a_n \prod_{i=1}^n (X - x_i)$, $Q(Y) = b_m \prod_{j=1}^m (Y - y_j)$ ，那么，

$$\text{Res}(P, Q) = (-1)^{nm} a_n^m \prod_{i=1}^n Q(x_i) = b_m^n \prod_{j=1}^m P(y_j).$$



推论 6.3

假设多项式 P 和 Q 的根都落在 K 中。那么， P 和 Q 有公共根当且仅当 $\text{Res}(P, Q) = 0$ 。



推论 6.4

给定多项式 $P, Q \in K[X]$ ，假设 $P = BQ + R$ 是带余除法，其中， $\deg(R) < \deg(Q)$ 。那么，

$$\text{Res}(P, Q) = b_m^{n-\deg(R)} \text{Res}(Q, R).$$



证明 根据上面的推论，我们有

$$\begin{aligned} \text{Res}(P, Q) &= b_m^n \prod_{j=1}^m P(y_j) = b_m^n \prod_{j=1}^m [(BQ)(y_j) + R(y_j)] \\ &= b_m^n \prod_{j=1}^m R(y_j) = b_m^{n-\deg(R)} \text{Res}(Q, R). \end{aligned}$$

这就给出了要证明的公式。

定义 6.1 (判别式)

给定 $P \in K[X]$ ，其判别式定义为

$$\text{Disc}(P) := \text{Res}(P, P').$$



注 判别式用来判别 $P(X) = 0$ 是否有重根。假设 $P(X)$ 是首一多项式并且在 $K[X]$ 中， $P(X)$ 分裂，即 $P(X) = (X - \alpha_1) \cdots (X - \alpha_n)$ ，其中， α_i 为其根。此时， $\deg P' = n - 1$ 。根据 Leibniz 法则，我们有

$$P'(X) = \sum_{k=1}^n (X - \alpha_1) \cdots \overbrace{(X - \alpha_k)}^{\text{缺失}} \cdots (X - \alpha_n).$$

从而, $P'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j)$ 。所以,

$$\text{Disc}(P) = \text{Res}(P, P') = (-1)^{n(n-1)} \prod_{i=1}^n P'(\alpha_i) = \prod_{i=1}^n \prod_{j \neq i} (\alpha_i - \alpha_j) = \prod_{i \neq j} (\alpha_i - \alpha_j).$$

这说明 $\text{Disc}(P) = 0$ 等价于 P 有重根。

例题 6.1 二次多项式 $P(X) = aX^2 + bX + c$, 那么, $P'(X) = 2aX + b$ 。根据解式和判别式的定义, 我们有

$$\text{Disc}(P) = \det \begin{pmatrix} c & b & 0 \\ b & 2a & b \\ a & 0 & 2a \end{pmatrix} = a(4ac - b^2).$$

例题 6.2 三次多项式 $P(X) = X^3 + pX + q$, 那么, $P'(X) = 3X^2 + p$ 。根据解式和判别式的定义, 我们有

$$\text{Disc}(P) = \det \begin{pmatrix} q & 0 & p & 0 & 0 \\ p & q & 0 & p & 0 \\ 0 & p & 3 & 0 & p \\ 1 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 \end{pmatrix} = -(4p^3 + 27p^2).$$

例题 6.3 n 次多项式 $P(X) = X^n + aX + b$, 那么, $P'(X) = nX^{n-1} + a$ 。此时, 利用行列式的计算不再有优势。我们利用之前的推论中所得到的公式可以进行计算。首先,

$$\text{Disc}(P) = n^n \text{Res}(P, X^{n-1} + \frac{a}{n}).$$

假设 $\alpha_1, \dots, \alpha_{n-1}$ 是 $X^{n-1} + \frac{a}{n}$ 的 $n-1$ 个根, 那么,

$$\begin{aligned} \text{Disc}(P) &= n^n \prod_{j=1}^{n-1} P(\alpha_j) = n^n \prod_{j=1}^{n-1} (\alpha_j^n + a\alpha_j + b) \\ &= n^n \prod_{j=1}^{n-1} \left(-\frac{a}{n}\alpha_j + a\alpha_j + b \right) = n^n \left(\frac{n-1}{n}a \right)^{n-1} \prod_{j=1}^{n-1} \left(\alpha_j + \frac{n}{n-1}\frac{a}{b} \right) \\ &= n^n \left(-\frac{n-1}{n}a \right)^{n-1} \prod_{j=1}^{n-1} \left(-\frac{n}{n-1}\frac{b}{a} - \alpha_j \right) = n^n \left(-\frac{n-1}{n}a \right)^{n-1} P'(-\frac{n}{n-1}\frac{b}{a}) \\ &= n^n \left(-\frac{n-1}{n}a \right)^{n-1} \left(n \left(-\frac{n}{n-1}\frac{b}{a} \right)^{n-1} + a \right) \\ &\stackrel{?}{=} (-1)^{\frac{n(n-1)}{2}} (n^n b^{n-1} + (-1)^{n-1} (n-1)^{n-1} a^n). \end{aligned}$$

6.3 对称多项式

给定环 A , 我们考虑多元的多项式环 $A[X_1, \dots, X_n]$ 。对称群 \mathfrak{S}_n 可以在 $A[X_1, \dots, X_n]$ 上作用:

$$\mathfrak{S}_n \times A[X_1, \dots, X_n] \rightarrow A[X_1, \dots, X_n], \quad (\sigma, P) \mapsto (\sigma \cdot P)(X_1, \dots, X_n) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)}).$$

给定 $P \in A[X_1, \dots, X_n]$, 对任意的 $\sigma \in \mathfrak{S}_n, \sigma \cdot P = P$, 我们就称 P 是对称多项式。我们用 $A[X_1, \dots, X_n]^{\mathfrak{S}_n}$ 表示全体 A -系数的对称多项式。注 $A[X_1, \dots, X_n]^{\mathfrak{S}_n}$ 是 $A[X_1, \dots, X_n]$ 的子环。

例题 6.4 我们有 n 个基本的（整系数）对称多项式：

$$\sigma_1 = \sum_i X_i, \sigma_2 = \sum_{i < j} X_i X_j, \dots, \sigma_k = \sum_{i_1 < i_2 < \dots < i_k} X_{i_1} X_{i_2} \dots X_{i_k}, \dots, \sigma_n = X_1 \dots X_n.$$

给定一组整数指标 $I = (i_1, \dots, i_n)$, 其中, $i_1 \geq i_2 \geq \dots \geq i_n \geq 0$, 令 $\text{Stab}(I) = \{\sigma \in \mathfrak{S}_n \mid \sigma(i_1, \dots, i_n) = (i_1, \dots, i_n)\}$ 。我们定义

$$S_I = \sum_{\sigma \in \mathfrak{S}_n / \text{Stab}(I)} \sigma \cdot (X_1^{i_1} X_2^{i_2} \dots X_n^{i_n})$$

此时, $S_{(1,0,\dots,0)} = \sigma_1$, $S_{(1,1,\dots,1)} = \sigma_n$ 。以上定义中, 之所以要商掉 I 的稳定化子群是因为我们要避免重复的系数。

练习 6.1 $n=4$, $I = (2, 1, 1)$, 那么, $S_I = X_1^2 X_2 X_3 + X_2^2 X_1 X_3 + X_3^2 X_1 X_2$ 。然而, 我们有

$$\sum_{\sigma \in \mathfrak{S}_n} \sigma \cdot (X_1^{i_1} X_2^{i_2} X_3^{i_3}) = 2(X_1^2 X_2 X_3 + X_2^2 X_1 X_3 + X_3^2 X_1 X_2).$$

注 在 S_I 中每个单项式恰好出现一次（数个数）。

注 对任意的 $P \in A[X_1, \dots, X_n]^{\mathfrak{S}_n}$, 存在有限个指标 I 以及 $a_I \in A$, 使得

$$P = \sum_{\text{有限}} a_I \cdot S_I.$$

注 对于指标 $I = (i_1, \dots, i_n)$ 和 $J = (j_1, \dots, j_n)$, 我们用字典序比较它们的大小, 即

$$I < J \Leftrightarrow \text{存在 } k \leq n, \text{ 使得 } i_1 = j_1, \dots, i_{k-1} = j_{k-1} \text{ 而 } i_k < j_k.$$

那么, 我们有

$$S_I \cdot S_J = S_{I+J} + \sum_{K < I+J} a_K \cdot S_K,$$

其中, $I+J = (i_1 + j_1, \dots, i_n + j_n)$ 。实际上, 只要观察到 $X_1^{i_1} \dots X_n^{i_n}$ 是 S_I 中所出现的最大指标即可。

定理 6.1

每个对称多项式都可以唯一的写成 $\sigma_1, \dots, \sigma_n$ 的多项式, 即

$$A[X_1, \dots, X_n]^{\mathfrak{S}_n} = A[\sigma_1, \dots, \sigma_n].$$



证明 首先证明存在性。只需要对 I 进行归纳, 证明每个 S_I 都可以写成 $\sigma_1, \dots, \sigma_n$ 的多项式。最小的 I 是 $I = (1, 0, \dots, 0)$, 此时, $S_I = \sigma_1$, 命题是显然的。假设对任意的 $I < K$ 命题都成立, 那么, 我们总可以 K 写成

$$K = I + (1, \dots, 1, 0, \dots, 0) = I + J, \quad I < K.$$

那么,

$$S_K = S_{I+J} = S_I \cdot S_J + \sum_{K' < I+J} a_{K'} \cdot S_{K'}.$$

右边每一项都是 $\sigma_1, \dots, \sigma_n$ 的多项式, 这就完成了归纳假设。

在证明唯一性。我们观察到对于任意的指标 $\alpha = (\alpha_1, \dots, \alpha_n)$, 我们有

$$\sigma_1^{\alpha_1} \sigma_2^{\alpha_2} \cdots \sigma_n^{\alpha_n} = S_{I(\alpha)} + \sum_{I < I(\alpha)} a_I \cdot S_I,$$

其中, $I(\alpha) = (\alpha_1 + \alpha_2 + \cdots + \alpha_n, \alpha_1 + \alpha_2 + \cdots + \alpha_{n-1}, \dots, \alpha_1)$ 。我们只要说明对任意的 $G \in A[Y_1, \dots, Y_n] - \{0\}$, $G(\sigma_1, \dots, \sigma_n)$ 在 $A[X_1, \dots, X_n]$ 中非零即可。实际上, 假设 $G(Y_1, \dots, Y_n) = \sum_{\alpha} a_{\alpha} \cdot Y^{\alpha}$, 其中, $a_{\alpha} \neq 0$ 。我们可以唯一的选出这样的 α , 使得 $I(\alpha)$ 是最大的, 那么, 此时在 $G(\sigma_1, \dots, \sigma_n)$ 用 S_I 的表达中, $S_{I(\alpha)}$ 的系数不是 0, 从而, $G(\sigma_1, \dots, \sigma_n) \neq 0$ 。

例题 6.5 判别式 令 $\Delta = \prod_{i < j} (X_i - X_j)$, 那么, $\sigma \Delta = \varepsilon(\sigma) \Delta$ 。从而, $\Delta \in A[X_1, \dots, X_n]^{\mathfrak{A}_n}$ 。此时, 我们有 $\Delta^2 \in A[X_1, \dots, X_n]^{\mathfrak{S}_n}$ 。根据定理, 我们就有 $\text{disc} \in A[Y_1, \dots, Y_n]$, 使得

$$\Delta^2 = \text{disc}(-1\sigma_1, \dots, (-1)^k \sigma_k, \dots, (-1)^n \sigma_n).$$

判别式多项式用来判断一个 n -次方程是否有重根。考虑

$$P(X) = (X - x_1)(X - x_2) \cdots (X - x_n) = X^n + a_1 X^{n-1} + \cdots + a_n.$$

根据 Vieta 定理, $a_k = (-1)^k \sigma_k$ 。所以,

$$\Delta^2(a_1, \dots, a_n) = \text{disc}(a_1, \dots, a_n) = \prod_{i \neq j} (x_i - x_j)^2.$$

我们注意到, 之前定义的判别式

$$\text{Disc}(P) = \prod_{i \neq j} (\alpha_i - \alpha_j).$$

所以, $\text{disc}(a_1, \dots, a_n) = (-1)^{\frac{n(n-1)}{2}} \text{Disc}(P)$ 。

练习 6.2 K 是域, $K(X_1, \dots, X_n) = \text{Frac}(K[X_1, \dots, X_n])$ 。证明,

$$K(X_1, \dots, X_n)^{\mathfrak{S}_n} = K(\sigma_1, \dots, \sigma_n).$$

练习 6.3 K 是域。证明,

$$K(X_1, \dots, X_n)^{\mathfrak{A}_n} = \{f + g\Delta \mid f, g \in K(\sigma_1, \dots, \sigma_n)\}.$$

注[Newton 公式] 令 $S_k = X_1^k + \cdots + X_n^k$ 。那么, 我们有

$$S_k - \sigma_1 S_{k-1} + \sigma_2 S_{k-2} - \cdots + (-1)^{k-1} \sigma_{k-1} S_1 + (-1)^k \sigma_k = 0.$$

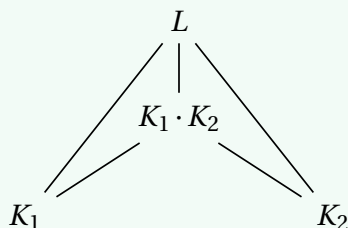
其中, 当 $k > n$ 时, 我们令 $\sigma_k = 0$ 。

以上公式形式上将一元多项式的系数用 Vieta 定理表述然后将变量 X 取作根 X_k 再对 k 求和。根据这个公式, 我们可以递归地计算所有的 $S_k \in A[\sigma_1, \dots, \sigma_n]$ 。

第7章 域的扩张

定义 7.1

给定域 L 与其子域 K_1, K_2 , 我们称 $K_1 \cdot K_2 := K_1(K_2) = K_2(K_1)$ 为 K_1 和 K_2 的复合域。



给定域 K , 我们有自然的环同态 $\varphi: \mathbb{Z} \rightarrow K$, 其中, $\varphi(n) = n \cdot 1_K$. 以上, 1_K 为 K 中单位元。如果 φ 为单射, 我们就称 K 的**特征为零**, 并记作 $\text{char}(K) = 0$; 否则, 存在唯一的素数, 使得 $\text{Ker}(\varphi) = p\mathbb{Z}$, 即 $p \cdot 1_K = 0$, 我们称 K 的**特征为 p** , 并记作 $\text{char}(K) = p$. 很明显, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 是特征为零的域而 $\mathbb{Z}/p\mathbb{Z}$ 是特征为 p 的域。

假设 $\text{Char}(K) = 0$, 那么, 环同态 $\varphi: \mathbb{Z} \rightarrow K$ 可以延拓到 \mathbb{Q} 上, 即 $\varphi(\frac{m}{n}) = \frac{\varphi(m)}{\varphi(n)}$, 其中, $m, n \in \mathbb{Z}$, 此时 K 总包含 (以唯一的方式) \mathbb{Q} 作为其子域; 假设 $\text{Char}(K) = p$, 那么, 环同态 $\varphi: \mathbb{Z} \rightarrow K$ 给出了域同态 $\bar{\varphi}: \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \rightarrow K$, 此时 K 总包含 (以唯一的方式) \mathbb{F}_p 作为其子域。我们称 \mathbb{Q} 和 \mathbb{F}_p 分别为以上两种情形下 K 的**本原域**。

引理 7.1

给定域扩张 L/K , 那么, $\text{Char}(K) = \text{Char}(L)$ 。



证明 考虑如下环同态的交换图表:

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & L \\ & \searrow \varphi' & \uparrow \\ & & K \end{array}$$

由于 $K \rightarrow L$ 是单射, 所以, $\text{Ker}(\varphi) = \text{Ker}(\varphi')$, 命题得证。

7.1 代数扩张

定义 7.2

给定域扩张 L/K 和 L'/K , $\varphi: L \rightarrow L'$ 是域同态。如果 $\varphi|_K = \text{id}_K$, 就称 φ 为 K -同态。

$$\begin{array}{ccc} L & \xrightarrow{\varphi} & L' \\ | & & | \\ K & \xrightarrow{\text{id}_K} & K \end{array}$$

我们用 $\text{Hom}_K(L, L')$ 表示所有的 K -同态, 用 $\text{End}_K(L)$ 表示所有的 L/K 到自身的 K -同态, 用 $\text{Aut}_K(L)$ 表示所有的 L/K 到自身的 K -同构。



练习 7.1 证明, $\text{Aut}_K(L)$ 具有自然的群结构。

定义 7.3

给定域扩张 L/K 和 $x \in L$, 如果存在非零多项式 $P(X) \in K[X]$, 使得 $P(x) = 0$, 我们就称 x 在 K 上是代数的; 否则, 就称 x 在 K 上是超越的。如果每个 $x \in L$ 都在 K 上是代数的, 我们就称域扩张 L/K 是代数扩张。此时, 存在唯一^a的次数最低的首一多项式 $P(X) \in K[X]$, 使得 $P(x) = 0$, 我们将 $P(X)$ 称作是 x 在 K 上的极小多项式。

^a利用 $K[X]$ 是主理想整环或者辗转相除法



注 根据极小多项式次数的最低性质, $P(X)$ 是 $K[X]$ 上的不可约多项式。

给定域扩张 L/K , $x \in L$ 在 K 上是代数的。考虑如下自然的环同态:

$$\text{ev}_x: K[X] \longrightarrow K[x], \quad Q(X) \longmapsto Q(x).$$

这是将多项式 $Q(X)$ 在 x 处取值。很明显, 这是满射。如果 $P(X)$ 是 x 在 K 上的极小多项式, 那么, $P \in \text{Ker}(\psi)$; 另外, 对于 $Q(X) \in \text{Ker}(\psi)$, 那么, 存在 $A, R \in K[X]$, $\deg(R) < \deg(P)$, 使得 $Q = AP + R$, 其中, P 是 x 的极小多项式。通过在 x 处取值, 我们得到 $R(x) = 0$, 根据 P 的次数的最小性, 我们知道 $R = 0$, 从而, $Q = AP$ 。这表明 $\text{Ker}(\psi) = (P(X))$ 。根据环同态第一定理, 我们得到环同构

$$K[X]/(P(X)) \xrightarrow{\cong} K[x] \subset L,$$

另外, $(P(X))$ 是极大理想¹, 所以, $K[x]$ 是域。

根据定义, 我们自然有 $K[x] \subset K(x)$ 。每个 $K(x)$ 中的元素都形如 $\frac{P(x)}{Q(x)}$, 其中, $P, Q \in K[X]$ 并且 $Q(x) \neq 0$ 。由于 $K[x]$ 是域, 所以, $\frac{P(x)}{Q(x)} \in K[x]$, 从而, $K[x] = K(x)$ 。我们还可以通过 $K(x)$ 的定义来说明这一点: $K(x)$ 是包含 x 的最小的域, 而由于 $K[x]$ 是域并且包含 x , 所以, $K[x] = K(x)$ 。

命题 7.1

给定域扩张 L/K 和 $x \in L$, 那么, x 在 K 上是代数的当且仅当 $K(x)/K$ 是有限扩张。此时, 我们有 $[K(x):K] = \deg P(X)$, 其中, $P(X)$ 为 x 的极小多项式并且有如下同构

$$K[X]/(P(X)) \xrightarrow{\cong} K[x] \xrightarrow{\cong} K(x).$$

进一步, $1, x, \dots, x^{\deg(P)-1}$ 是 $K(x)/K$ 的一组基。



证明 假设 $K(x)/K$ 是有限扩张, 那么, $1, x, \dots, x^n, \dots$ 在 K 上线性相关, 所以, 存在 $a_0, \dots, a_n \in K$,

¹主理想整环的非零素理想都是极大理想。我们还可以直接证明: 假设 $I \subset (P(X))$ 是非平凡理想, 那么, $I = (P_1(X))$, 这表明存在 $Q(X) \in K[X]$, 使得 $P(X) = P_1(X) \cdot Q(X)$, 然而, $P(X)$ 不可约, 所以只能有 $I = (P(X))$ 。

$a_n \neq 0$, 使得

$$a_0 + a_1x + \cdots + a_nx^n = 0 \Leftrightarrow P(x) = 0, P(X) = \sum_{k=0}^n a_k X^k.$$

所以, x 在 K 上是代数的。

反之, 假设 x 在 K 上是代数的并且 $P(X) = X^n + \sum_{k=0}^{n-1} a_k X^k$ 是 x 的极小多项式。另外, 根据 P 的最小性, $1, x, \dots, x^n$ 在 K 上线性相关但是 $1, x, \dots, x^{n-1}$ 线性无关。所以, $1, x, \dots, x^{n-1}$ 是 $K(x)/K$ 的基。至此, 命题中结论均已证明。

推论 7.1

有限扩张是代数扩张。



证明 这是以上证明过程的直接推论。

我们也可以直接证明: 考虑有限扩张 L/K 。对任意的 $x \in L$, $K(x)$ 是中间域, 从而, $K(x)/K$ 是有限扩张。根据以上命题, x 是代数的, 从而, L/K 是代数扩张。

推论 7.2

给定域扩张 L/K 。那么, 如下命题成立:

- 1) $M \subset L$ 是由在 K 上代数的元素组成的子集, 那么, $K(M)/K$ 是代数扩张。如果 M 还是有限的, 那么, $K(M)/K$ 是有限扩张。
- 2) 令 $K^{\text{alg}} = \{x \in L | x \text{ 在 } K \text{ 上代数的}\}$, 那么, $K \subset L$ 是子域。特别的, K^{alg}/K 是 L/K 中最大的、代数的中间域。



证明

假设 $M = \{m_1, \dots, m_k\} \subset L$ 是由在 K 上代数的元素组成的有限子集, 根据上述命题, $K(m_1)/K$ 是有限扩张。另外, m_2 在 $K(m_1)$ 上是代数的, 所以, $K(m_1, m_2)/K(m_1)$ 是有限扩张。从而, $K(m_1, m_2)/K$ 是有限扩张。以此类推, 我们得到 $K(m_1, \dots, m_k)/K$ 是有限扩张。

现在仅假设 $M = \{m_1, \dots, m_k\} \subset L$ 是由在 K 上代数的元素组成的子集, 对任意的 $x \in K(M)$, 按定义, 存在 $m_1, \dots, m_k \in M$, 使得 $x \in K(m_1, \dots, m_k)$ 。我们已经证明了 $K(m_1, \dots, m_k)/K$ 是有限扩张, 所以, x 在 K 上是代数的。这就证明了 $K(M)/K$ 是代数扩张。

为了说明 K 是子域, 可以对 $M = K$ 运用上一个结论, 从而 $K(K^{\text{alg}})$ 中元素均为代数的, 所以, $K(K^{\text{alg}}) \subset K$ 。这表明, $K(K^{\text{alg}}) = K$ 。

推论 7.3

给定 L/K 的中间域 E/K , 那么, L/K 是代数扩张当且仅当 L/E 和 E/K 均为代数扩张。



证明 推论的一个方向是平凡的。现在假设 L/E 和 E/K 均为代数扩张。对任意的 $x \in L$, 根据定义, 存在正整数 n 和 $e_0, \dots, e_{n-1} \in E$, 使得

$$x^n + e_{n-1}x^{n-1} + \cdots + e_1x + e_0 = 0.$$

这表明 x 在 $K(e_{n-1}, \dots, e_0)$ 上是代数的, $K(e_{n-1}, \dots, e_0, x)/K(e_{n-1}, \dots, e_0)$ 是有限扩张。另外, 由于

e_0, \dots, e_{n-1} 在 K 上是代数的, 所以, $K(e_{n-1}, \dots, e_0)/K$ 是有限扩张。综上所述, $K(e_{n-1}, \dots, e_0, x)/K$, 所以, x 在 K 上是代数的。

7.2 代数闭包

命题 7.2

K 是域, $P \in K[X]$, 那么, 存在有限域扩张 K_P/K , 使得 P 在 K_P 中有一个根。

证明 不妨假设 $P(X)$ 是不可约多项式, 考虑以下环同态的复合

$$K \hookrightarrow K[X] \longrightarrow K[X]/(P) = K_P.$$

这是 K 的有限扩张。对于 $X \in K[X]$, 我们记它在 K_P 中的像为 x_P , 那么, $P(x_P) = 0$ 。

命题 7.3

K 是域, 以下四个描述等价 (当它们之一成立时, K 被称作是代数封闭域):

- 1) 每个次数至少是 1 的多项式 $P \in K[X]$ 在 K 中有根;
- 2) $K[X]$ 中的不可约多项式 (默认次数至少是 1) 的次数均为 1;
- 3) 如果 L/K 是代数扩张, 那么 $L = K$ 。

证明 我们利用以上命题来证明 $3) \Rightarrow 1)$ 。其余步骤都是显然的。

定义 7.4

K 是域。如果 Ω/K 为代数扩张并且 Ω 是代数封闭的, 我们就称 Ω 为 K 的一个代数闭包。

7.2.1 代数闭包的存在性

引理 7.2

K 是域, $P(X) \in K[X]$ 。那么, 存在域扩张 L/K , 使得 P 在 L 中分裂, 即在 $L[X]$ 中, 我们有

$$P(X) = a(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n), \quad a \in K, \alpha_i \in K.$$

证明 我们对 P 的次数进行归纳。当 $\deg(P) = 0$ 或 1 时, 命题是平凡的。当 $\deg(P) \geq 2$ 时, 选取不可约多项式 $p(X) | P(X)$, 根据命题 7.2, $P(X)$ 在 K_P/K 中有一个根 α , 进一步考虑 $P(X) = Q(X)(X - \alpha) \in K_P[X]$, 利用归纳假设, 存在 L/K_P , 使得 $Q(X)$ 在 L 中分裂, 从而, P 也在 L 中分裂。

引理 7.3 (E.Artin)

K 是域, 存在域扩张 L/K , 使得对任意的 $P(X) \in K[X] - K$, P 在 L 中有根。

证明 我们定义多项式环

$$A := K[X_P | P \in K[X] - K] := \bigcup_{\substack{F \subset K[X] - K, \\ |F| < \infty}} K[X_P | P \in F].$$

令 $\mathfrak{J} = (P(X_P) | P \in K[X] - K)$, 这是 A 中由所有形如 $P(X_P)$ 的元素所生成的理想。我们证明 $\mathfrak{J} \neq A$: 若不然, 存在 $P_1, \dots, P_n \in K[X]$ 以及 $Q_1, \dots, Q_n \in A$, 使得

$$\sum_{k=1}^n Q_k \cdot P_k(X_{P_k}) = 1.$$

其中, 我们不妨假设 $Q_k = Q_k(X_{P_1}, \dots, X_{P_n})$ 。我们用变元 T_k 表示 X_{P_k} , 以上表明

$$\sum_{k=1}^n Q_k(T_1, \dots, T_n) \cdot P_k(T_k) = 1.$$

根据上一个引理, 存在域扩张 K' , 使得 P_k 在 K' 中有根 α_k , 其中, $k = 1, \dots, n$ 。据此, 我们可以构造环同态

$$K[T_1, \dots, T_k] \rightarrow K, \quad T_k \mapsto \alpha_k, \quad k = 1, \dots, n.$$

此时, 上式左端的像为 0 而右端的像为 1, 矛盾。

根据以上讨论, 存在极大理想 $\mathfrak{m} \supset \mathfrak{J}$, 令 $L = A/\mathfrak{m}$ 。根据 \mathfrak{J} 的定义, $X_P + \mathfrak{m}$ 是 $P(X)$ 的根。

给定域 K , 记以上操作得到的 $L = A/\mathfrak{m}$ 为 $E(K)$ 。对 $k \geq 1$, 我们定义 $E^{k+1}(K) = E(E^k(K))$ 。据此, 我们得到扩张的塔:

$$K \longrightarrow E(K) \longrightarrow E^2(K) \longrightarrow \dots \longrightarrow E^k(K) \longrightarrow \dots.$$

我们定义 $E^\infty(K) = \bigcup_{k \geq 1} E^k(K)$ 。我们来证明 $E^\infty(K)$ 是代数封闭域 (它显然是域)。实际上, 对任意的 $P(X) \in E^\infty(K)[X]$, 存在 $k \geq 1$, 使得 $P(X) \in E^k(K)[X]$ 。根据以上构造, $P(X)$ 的所有根都落在 $E^{k+1}(K) \subset E^\infty(K)$ 中, 所以, $E^\infty(K)$ 是代数封闭的。

最终, 我们定义 $\Omega = \{x \in E^\infty(K) | x \text{ 在 } K \text{ 上是代数封闭的}\}$, 这就是 K 的一个代数闭包, 具体参见引理 7.6。

7.2.2 关于域同态扩张的技术性引理

给定域扩张 L/K , $x \in L$ 并且 $P(X) \in K[X]$ 是 x 的极小多项式, 那么, 我们有域同构

$$\text{ev}_x: K[X]/(P(X)) \longrightarrow K(x) = K[x], \quad Q(X) \mapsto Q(x).$$

特别地, 由于 $K(x) \subset L$, 我们得到了 K -同态:

$$\text{ev}_x: K[X]/(P(X)) \longrightarrow L, \quad Q(X) \mapsto Q(x).$$

引理 7.4

给定域扩张 L/K 以及不可约多项式 $P(X) \in K[X] - K$ 。我们有如下的一一对应:

$$Z_P(L) := \{P(\alpha) = 0 | \alpha \in L\} \xrightarrow{1:1} \text{Hom}_K(K[X]/(P(X)), L), \quad \alpha \mapsto \text{ev}_\alpha.$$

特别地, $|\text{Hom}_K(K[X]/(P(X)), L)| \leq \deg(P)$ 。



注 简而言之, 多项式 $P(X)$ 在 L 中不同的根的个数恰好等于把 $K(x) \simeq K[X]/(P(X))$ 通过 K -同态

嵌入到 L 中的方式的个数。直观上，重根的出现会使得 $K(x)$ 到 L 的嵌入方式减少。

证明 给定 P 在 L 中的根 α ，那么，环同态

$$\text{ev}_\alpha: K[X] \rightarrow L, Q(X) \mapsto Q(\alpha),$$

的核是 $(P(X))$ ，从而给出了 K -同态：

$$\text{ev}_\alpha: K[X]/(P(X)) \rightarrow L, Q(X) \mapsto Q(\alpha).$$

反之，对任意的 K 同态：

$$\varphi: K[X]/(P(X)) \rightarrow L,$$

令 $\alpha = \varphi(X + (P(X)))$ ，由于 $P(X)$ 的像为 0 ，所以， $P(\alpha) = 0$ 。

容易看出，以上两个映射互为逆，从而给出了引理中的一一映射。

注 我们有

$$|\text{Aut}_K(K[X]/(P(X)))| = Z_P(K[X]/(P(X))) \leq \deg(P) = [K[X]/(P(X)) : K].$$

注 我们还有另外一种版本的表述。给定域 K 和不可约多项式 $P(X) \in K[X] - K$ ，给定域同态 $\sigma: K \rightarrow L$ 。我们定义 $P^\sigma(X) \in L[X]$ 为

$$P^\sigma(X) = \sum_{k=0}^n \sigma(a_k) X^k, \text{ 其中, } P(X) = \sum_{k=0}^n a_k X^k.$$

我们注意到

$$K[X] \rightarrow L[X], P \mapsto P^\sigma$$

是环同态。我们有如下的一一对应：

$$Z_{P^\sigma} \xrightarrow{1:1} \text{Hom}_\sigma(K[X]/(P(X)), L).$$

其中，域同态 $\varphi: \text{Hom}_\sigma(K[X]/(P(X)), L)$ 指的是对任意的 $k \in K$ 和 $y \in K[X]/(P(X))$ ，我们有

$$\varphi(k \cdot y) = \sigma(k) \varphi(y).$$

在应用的时候，我们总是愿意把 K 看作是 L 的子域。

命题 7.4 (域同态延拓 (对代数扩张) 的技术性命题)

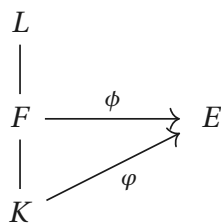
给定代数扩张 L/K ， E 是代数封闭域， $\varphi: K \rightarrow E$ 是域同态，那么，存在唯一的域同态 $\bar{\varphi}: L \rightarrow E$ 使得 $\bar{\varphi}|_K = \varphi$ 。

$$\begin{array}{ccc} L & \xrightarrow{\bar{\varphi}} & E = \bar{E} \\ \text{代数} \downarrow & \nearrow \varphi & \\ K & & \end{array}$$

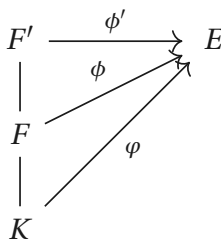
注 以上可以被视作是代数封闭域的泛性质。

注 以上，我们并不需要假设 L/K 是有限扩张。

证明 考虑如下集合 $\mathcal{X} = \{(F, \phi)\}$, 其中, F 是 L/K 的中间域, $\phi: F \rightarrow E$ 是域同态并且 $\phi|_K = \varphi$ 。



我们在 \mathcal{X} 上定义如下的偏序: $(F, \phi) \leq (F', \phi')$, 指的是 $F \subset F'$ 并且 $\phi'|_F = \phi$, 即



由于 $(K, \varphi) \in \mathcal{X}$, 所以, $\mathcal{X} \neq \emptyset$. 对 \mathcal{X} 的全序子集 $\{(F_i, \phi_i)\}_{i \in I} \subset \mathcal{X}$, 我们定义 $F_\infty := \bigcup_{i \in I} F_i$ 并且 $\phi_\infty|_{F_i} = \phi_i$, 这就给出了 $\{(F_i, \phi_i)\}_{i \in I}$ 的一个上界 (F_∞, ϕ_∞) . 根据 Zorn 引理, \mathcal{X} 中有极大元 (F, ϕ) . 我们只要证明 $F = L$ 即可。

如若不然, 那么有 $x \in L - F$, 考虑 x 在 F 上 (x 在 F 上仍然是代数的因为 L/F 自然是代数扩张) 的极小多项式 $P(X)$, 我们有域同构

$$\text{ev}_x: F[X]/(P(X)) \xrightarrow{\cong} F(x) \subset L.$$

通过 $\phi: F \rightarrow E$, 我们知道 P^ϕ 在 E 中有根 (因为 E 是代数封闭的), 根据前面的引理, 我们就有域同态

$$\bar{\phi}: F[X]/(P(X)) \rightarrow E.$$

从而, 我们有域同态

$$\bar{\phi} \circ (\text{ev}_x)^{-1}: F(x) \rightarrow E.$$

容易验证, $\bar{\phi}|_F = \phi$ 而 $F(x)$ 是严格比 F 的中间域, 这与 F 的极大性矛盾。证明完毕。

例题 7.1 代数闭包的唯一性 K 是域, Ω_i 是 K 的代数闭包, 即 Ω_i/K 是代数扩张并且 Ω_i 是代数封闭域, 其中, $i = 1, 2$. 根据以上命题, 我们有 $\varphi \in \text{Hom}_K(\Omega_1, \Omega_2)$ 以及 $\psi \in \text{Hom}_K(\Omega_2, \Omega_1)$, 通过复合, 我们就有 $\psi \circ \varphi \in \text{End}_K(\Omega_1)$. 由于域 K 的代数扩张的 K -自同态必然是自同构, 所以, $\psi \circ \varphi$ 是可逆的。类似地, $\varphi \circ \psi$ 也是, 从而, φ 和 ψ 均为同构。

对任意的域, 在 K -同构的意义下, 我们用 \bar{K} 表示它的代数闭包。如果 K 是代数封闭域, 我们显然有 $\bar{K} = K$ 。

引理 7.5

L/K 是代数扩张, 那么, $\text{End}_K(L) = \text{Aut}_K(L)$ 。



例题 7.2 $\bar{\mathbb{Q}}$ 的构造

²需要利用良序性验证 F_∞ 是域并且 ϕ_∞ 的定义不依赖于 i 的选取。

引理 7.6

给定域扩张 L/K , 假设 L 是代数封闭域。那么, $\Omega = \{x \in L \mid x \text{ 在 } K \text{ 上是代数的}\}$ 是 K 的代数闭包。



我们知道 $\Omega = K(\Omega)$ 是 K 的代数扩张, 现在证明 Ω 是代数封闭的。对任意的

$$P(X) = \omega_n X^n + \cdots + \omega_1 X + \omega_0 \in \Omega[X],$$

假设 $x \in L$ 是 P 的根 (因为 L 是代数封闭的), 我们来说明 $x \in \Omega$ 。为此, 只要证明 x 在 K 上是代数的。实际上, 由于 ω_i 在 K 上代数而 x 在 $K(\omega_1, \dots, \omega_n)$ 上的代数, 所以, 域扩张

$$K \longrightarrow K(\omega_1, \dots, \omega_n) \longrightarrow K(\omega_1, \dots, \omega_n, x)$$

是有限扩张, 从而, x 在 K 上是代数的。

特别地, 对 \mathbb{C}/\mathbb{Q} 使用这个构造, $\overline{\mathbb{Q}}$ 就是 \mathbb{C} 中有理系数多项式方程的解所给出的集合。

7.3 分裂域与正规扩张

定义 7.5

K 是域, $\{P_i(X)\}_{i \in I}$ 是 $K[X]$ 中一族多项式, L/K 是域扩张。如果

- 1) 所有多项式 $\{P_i(X)\}_{i \in I}$ 在 L 中分裂, 即对每个 $i \in I$, 存在 $\alpha_{i,j} \in L$ 以及 $a_i \in K$, 使得

$$P_i(X) = a_i(X - \alpha_{i,1})(X - \alpha_{i,2}) \cdots (X - \alpha_{i,n_i}).$$

- 2) $L = K(\{\alpha_{i,j}\}_{i \in I, j \leq n_i})$ 。

我们就称 L 是 K 的由 $\{P_i(X)\}_{i \in I}$ 给出的一个分裂域。

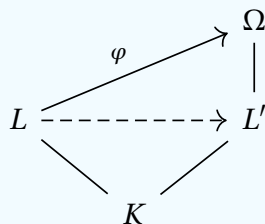


注 分裂域 L 是 K 的代数扩张, 因为它是 K 添加上代数元生成的。

注 在 \overline{K} 中考虑, 我们只要 (只能) 把 $\{P_i(X)\}_{i \in I}$ 的根都添加到 K 中就得到了上述所求的分裂域 $K(\{\alpha_{i,j}\}_{i \in I, j \leq n_i})$ 。换言之, (一个) 分裂域就是把一些多项式的 (所有) 根添加到 K 中所得到的域。

命题 7.5

K 是域, $\{P_i(X)\}_{i \in I}$ 是 $K[X]$ 中一族多项式, L 和 L' 都是 K 的由 $\{P_i(X)\}_{i \in I}$ 定义的分裂域并且 L' 落在代数封闭域 Ω 中。那么, 对任意的 $\varphi \in \text{Hom}_K(L, \Omega)$, 我们都有 $\varphi(L) \subset L'$, 即 $\varphi \in \text{Hom}_K(L, L')$ 。



特别地, 分裂域在 K -同构的意义下唯一。



证明 由于 $P_i(X)$ 是 K -系数的多项式, 所以, $P_i^\varphi = P$ 。从而, 在 Ω 中, 我们有

$$P(X) = P_i^\varphi(X) = a_i(X - \varphi(\alpha_{i,1}))(X - \varphi(\alpha_{i,2})) \cdots (X - \varphi(\alpha_{i,n_i})).$$

根据前一个注记, $L' = K(\{\varphi(\alpha_{i,j})\}_{i \in I, j \leq n_i})$ 。然而,

$$\varphi(L) = \varphi(K(\{\alpha_{i,j}\}_{i \in I, j \leq n_i})) = K(\{\varphi(\alpha_{i,j})\}_{i \in I, j \leq n_i}),$$

这就给出了证明。

假设 L 和 L' 是两个分裂域, 我们先把 L' 放到代数封闭域 Ω (比如选取 $\Omega = \overline{L'}$) 中去, 然后根据命题 7.4, 我们既有 $\varphi \in \text{Hom}_K(L, \Omega)$, 应用以上结论即可。

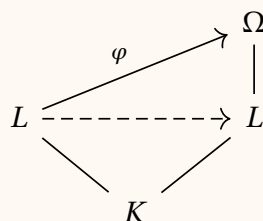
注 如果 $\{P_i(X)\}_{i \in I}$ 只有有限个多项式, 我们可以考虑 $P(X) = \prod_{i \in I} P_i(X)$, 那么, P 的分裂域与 $\{P_i(X)\}_{i \in I}$ 的分裂域相同。特别地, 此时的分裂域是 K 的有限扩张。

请注意, 我们在定义中不需要这个有限性 (没有有限性的假设会使得后面的推理略烦), 比如下面的定理中, 我们只假设 L/K 是代数扩张。

定理 7.1 (正规性的定义)

给定代数扩张 L/K , 如下四个叙述是等价的:

- 1) L 是 $K[X]$ 中某一族多项式 $\{P_i(X)\}_{i \in I}$ 的分裂域;
- 2) 对任意的域扩张 Ω/L , 其中, Ω 是代数封闭域, 对任意的 $\varphi \in \text{Hom}_K(L, \Omega)$, 都有 $\varphi(L) \subset L$;



- 3) 存在域扩张 Ω/L , 其中, Ω 是代数封闭域, 使得对任意的 $\varphi \in \text{Hom}_K(L, \Omega)$, 都有 $\varphi(L) \subset L$;
- 4) 对任意的不可约多项式 $P(X) \in K[X]$, 如果 $P(X)$ 在 L 中有根, 那么, $P(X)$ 在 $L[X]$ 中分裂 (为一次多项式的乘积)。

满足以上任何一条的代数扩张 L/K 被称作是正规扩张。^a

^a我们总是默认正规扩张是代数的。



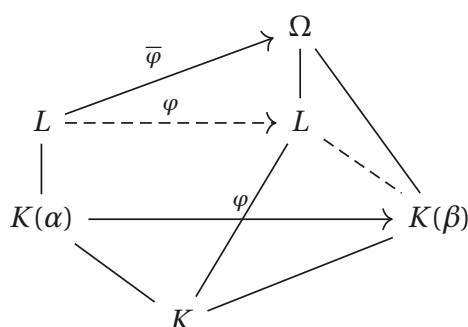
证明 根据命题 7.5, 我们有 1) \Rightarrow 2); 2) \Rightarrow 3) 是显然的。

证明 2) \Rightarrow 4)。给定 $\alpha \in L$ 为 P 的根, 考虑 P 的另外一个根 $\beta \in \Omega = \overline{K} \supset L$, 只要证明 $\beta \in L$ 即可。由于 (在 \overline{K} 中)

$$K(\alpha) \simeq K[X]/(P(X)) \simeq K(\beta),$$

我们可以选取 $\varphi: K(\alpha) \rightarrow K(\beta)$ 。由于 L 是 K 的代数扩张, 利用命题 7.4, 我们可以把 φ 延拓成

$\bar{\varphi}: L \rightarrow \Omega$, 即



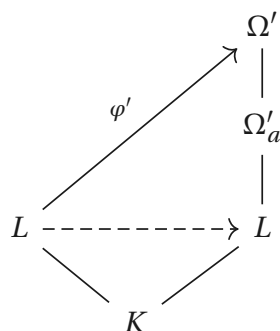
根据 2), $\bar{\varphi}(L) \subset L$, 从而, $\beta = \varphi(\alpha) \in L$ 。

证明 4) \Rightarrow 1)。我们定义如下一族多项式:

$$\{P_i\}_{i \in I} = \{P_x(X) = x \text{ 的极小多项式} \mid x \in L\}.$$

根据 4), 每个 P_i 在 L 中均为一次多项式的乘积; 很明显, L 由 K 添加了所有 P_i 的所有根 (都落在 L 中) 所生成, 所以, L 是 K 的一个分裂域。

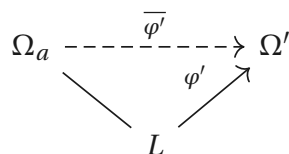
最后证明 3) \Rightarrow 2), 这是相对困难的一步。 Ω 已经由 3) 给定。我们考虑另外一个代数封闭的 Ω' 以及 $\varphi' \in \text{Hom}_K(L, \Omega')$, 即下图



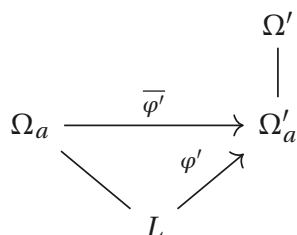
其中, 我们选取 Ω'_a 为 Ω' 中在 K 上的代数元所构成的子域。根据引理 7.6, Ω'_a 同构于 K 的代数闭包 \bar{K} , 它也是 L 的代数闭包 (因为 L 在 K 上是代数的)。类似地, 我们构造 Ω_a 为 Ω 中在 K 上的代数元所构成的子域, 它也同构于 K 的代数闭包 \bar{K} 。

$$K \text{ — } L \text{ — } \Omega_a \text{ — } \Omega.$$

根据命题 7.4, 我们可以对 $\varphi': L \rightarrow \Omega'$ 进行延拓:



我们强调, 以上的 $\bar{\varphi}'$ 是 L -同态。根据代数闭包的唯一性, 我们实际上有



以上, $\overline{\varphi'}$ 是代数封闭域之间的 L -同构。从而, $\overline{\varphi'}^{-1} \circ \varphi': L \rightarrow \Omega$ 。根据 3), $\overline{\varphi'}^{-1} \circ \varphi': L \rightarrow L$, 所以, $\varphi': L \rightarrow L$ 。

注 根据以上最后一个交换图, $\varphi(L) \subset \Omega'_a$, 从而, 我们可以一开始就假设 Ω 和 Ω' 均为 \overline{K} 即可 (差一个同构的意义下), 从而, 命题明显成立。

注 传统上, 我们通常采取 4) 作为正规扩张的定义并证明 1) 也是正规扩张的等价形式。

命题 7.6

给定正规扩张 L/K , 那么, 对任意的中间域 M , L/M 也是正规扩张。

注 M/K 未必是正规扩张: 我们可以考虑

$$\mathbb{Q} \longrightarrow \mathbb{Q}(\sqrt[4]{2}) \longrightarrow \mathbb{Q}(\sqrt[4]{2}, i),$$

其中, $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ 是正规的而 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ 不是正规的。

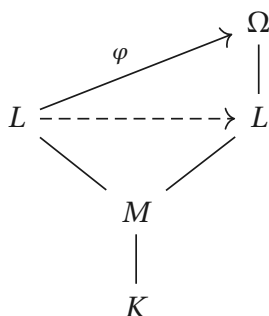
另外, 如果 L/M 和 M/K 是正规的, L/K 未必是正规扩张。我们可以考虑

$$\mathbb{Q} \longrightarrow \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt[4]{2}).$$

证明 利用定义中的 1), L 是一族 K 系数多项式 $\{P_i(X)\}_{i \in I}$ 的分裂域, 自然也是一族 M 系数多项式 $\{P_i(X)\}_{i \in I}$ 的分裂域。

也可以利用 4), 假设 $P(X)$ 是 $M[X]$ 中的不可约多项式, $P(\alpha) = 0$, 其中, $\alpha \in L$ 。考虑 α 在 K 上的极小多项式 $Q(X)$, 那么, 在 $M[X]$ 中, $P|Q$ 。由于 L/K 是正规扩张, $Q(\alpha) = 0$, 所以, Q 在 L 中分裂, 从而, P 在 L 中分裂。

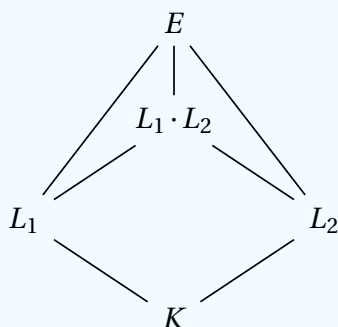
我们还可以利用 2) 来证明。对任意域扩张 Ω/L , 其中, Ω 是代数封闭的, 对任意的 $\varphi \in \text{Hom}_M(L, \Omega)$,



我们要说明 $\varphi(L) \subset L$ 。这是显然的, 因为我们 φ 自然可以看作是 $\text{Hom}_K(L, \Omega)$ 中的映射。

命题 7.7

给定域扩张 E/K , L_1 和 L_2 是中间域并且 L_1/K 和 L_2/K 是正规扩张。



那么, $L_1 \cdot L_2/K$ 也是正规扩张。



证明 L_1 是 K 添加了所有 $\{P_i\}_{i \in I}$ 的根所得到的分裂域, L_2 是 K 添加了所有 $\{Q_j\}_{j \in J}$ 的根所得到的分裂域。那么, $L_1 \cdot L_2$ 是 K 添加了所有 $\{P_i, Q_j\}_{i \in I, j \in J}$ 的根所得到的分裂域。

练习 7.2 试用 2) 或者 4) 来证明以上命题。

根据正规扩张中的等价定义 4), 如果 $\{M_i\}_{i \in I}$ 是扩张 L/K 的中间域并且对每个 i , M_i/K 是正规扩张, 那么, $\bigcap_{i \in I} M_i$ 是 K 的正规扩张。据此, 我们可以定义正规闭包的概念:

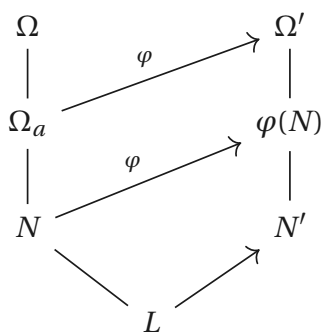
定理 7.2

L/K 是代数扩张, Ω 是代数封闭域并且 $\Omega \supset L$ 。那么, 在 Ω 中存在最小的^a、包含 L 的、 K 的正规扩张 N 。另外, 如果 Ω' 是另一个代数封闭域并且 $\Omega' \supset L$, N' 类似构造, 我们有 K -同构 $N \simeq N'$ 。我们称这个域为 L/K 的正规闭包。

^a在包含关系下



证明 我们选取 N 为 Ω 中包含 L 的所有 K 的 (代数的) 正规扩张之交即可。以下只证明唯一性:



令 Ω_a 为 L (或 K) 在 Ω 中的代数闭包。通过 $L \subset \Omega'$ 以及代数扩张同态延拓的技术性命题 7.4, 我们固定一个 $\varphi: \Omega_a \rightarrow \Omega'$, 使得上图交换。我们显然有 $\varphi(N)/K$ 是正规扩张, 所以, $\varphi(N) \supset N'$ (根据 N' 的最小性)。考虑 $\varphi^{-1}(N')$, 如果 $P(X) \in K[X]$ 在 $\varphi^{-1}(N')$ 中有根 α , 那么, $\varphi(\alpha) \in N'$ 是 P 的根, 从而, 所有的根都在 N' 中。据此, $\varphi^{-1}(N')$ 也包含了 P 的所有根, 从而, $\varphi^{-1}(N')/K$ 是正规扩张, 所以, $\varphi^{-1}(N') \supset N$ 。以上表明 $N \simeq_K N'$

注 由于 L/K 是代数的, 所以, L 是 K 添加 K 系数多项式 $\{P_i\}_{i \in I}$ 的某些根生成的, 为了得到 N , 我们把 $\{P_i\}_{i \in I}$ 的所有根都添加到 Ω 中即可。比如说, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ 不是正规的, 它的正规闭包是

$$N = \mathbb{Q}(\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i).$$

7.4 可分扩张

定义 7.6

K 是域, L/K 是代数扩张。如果多项式 $P \in K[X]$ 在 \bar{K} 中没有重根, 我们就称 P 是可分的; 否则称之为不可分的。对于 $x \in L$, 如果它的极小多项式是可分的, 我们就称 x 是可分的; 否则称之为不可分的。如果每个 $x \in L$ 都是可分的, 我们就称 L/K 是可分的; 否则称之为不可分的。



注 多项式 P 可分等价于 $(P, P') = 1$, 也等价于 $\text{Disc}(P) \neq 0$ 。

$P \in K[X]$ 是不可约多项式。那么, P 可分等价于 $P' \neq 0$ 。

实际上, 如果 P 可分, 那么, $(P, P') = 1$ 意味着 $P' \neq 0$; 反之, $P' \neq 0$ 并且 $\deg(P') < \deg(P)$, 由于 P 不可约, 只能有 $(P, P') = 1$ 。

注 假设 $P \in K[X]$ 是不可约多项式, 记 $P(X) = a_n X^n + \cdots + a_1 X + a_0$, 其中, $a_n \neq 0$ 。如果 P 是不可分的, 那么,

$$P'(X) = \sum_{k=1}^n k a_k X^{k-1} = n a_n X^{n-1} + \cdots.$$

我们必须有 $n \cdot a_n = 0$, 从而, 在 K 中我们有 $n = 0$ 。这表明 $\text{Char}(K) = p$, 其中, p 是素数。从而,

$$P'(X) = \sum_{p \nmid k} k a_k X^{k-1} = 0.$$

这表明

$$P(X) = \sum_{p \mid k} a_k X^k = Q(X^p).$$

由于 P 是不可约的, $Q(X)$ 也是。特别地, 如果 P 不可约并且不可分, 那么, $\deg(P) \geq p$ 。

很明显, 形如 $Q(X^p)$ 的多项式的导数为 0。

例题 7.3 令 $K = \mathbb{F}_p(T) = \text{Frac}(\mathbb{F}_p[T])$ 。根据 Eisenstein 判别, $P(X) = X^{p^2} + TX^p + T$ 在 $\mathbb{F}_p[T][X]$ 中不可约, 从而, 在 $K[X]$ 中也不可约。此时, $P(X) = Q(X^p)$, 其中, $Q(X) = X^p + TX + T$ 并且 $Q'(X) \neq 0$ 。特别地, Q 是可分的。


注 在特征零的情形下, 不可约多项式都是可分多项式。

注 假设 $\text{Char}(K) = p$, 我们有如下的 Frobenius 同态:

$$\text{Frob}: K \rightarrow K, x \mapsto x^p.$$

由于 $\text{Char}(K) = p$, 我们显然有 $(x + y)^p = x^p + y^p$ 。

引理 7.7

假设 $\text{Char}(K) = p$ 。那么，对任意的 $a \in K - K^p$ ， $X^p - a$ 是不可约多项式并且是不可分的。

证明 只需要证明 $X^p - a$ 是不可约。我们在 \bar{K} 中考虑，此时，存在唯一的 $b \in \bar{K}$ ，使得 $b^p = a$ 。³根据假设， $b \notin K$ 。从而， $X^p - a$ 只有一个根（重根）：

$$X^p - a = (X - b)^p.$$

如果该多项式可约，那么，

$$X^p - a = (X - b)^k \cdot (X - b)^l.$$

其中， $k, l \geq 2$ （因为 $b \notin K$ ）。它们都是有重根的多项式，从而是不可分的多项式，次数至少是 p ，那么， $X^p - a$ 的次数至少是 $2p$ ，矛盾。

引理 7.8

假设 K 的特征为 p ，不可约多项式 $P \in K[X]$ 的次数至少是 2 并且 P 只有一个根。那么，

$$P(X) = X^{p^n} - a, \quad a \notin \text{Im}(\text{Frob}).$$



证明 在 \bar{K} 中，我们有


$$P(X) = (X - b)^m = (X - b)^{p^n l} = (X^{p^n} - b^{p^n})^l, \quad m \geq 2, m = p^n l, (l, p) = 1.$$

从而， $P(X) = Q(X^{p^n})$ ，其中， $Q(X) = (X - b^{p^n})^l$ 。关键的观察是 $Q \in K[X]$ 并且是不可约的。此时，如果 $l \neq 1$ ，那么， Q 仍然只有一个根，从而，是不可分的，据此， $\deg(Q) = l$ 为 p 的倍数，矛盾。所以， $l = 1$ 。从而，

$$P(X) = X^{p^n} - b^{p^n} = X^{p^n} - a.$$

很明显， $a \notin \text{Im}(\text{Frob})$ ，否则， P 可约。


定义 7.7

K 是域，如果任意的不可约多项式 $P(X) \in K[X]$ 都是可分的，我们就称 K 是完美的 (perfect)。

练习 7.3 特征为零的域是完美域。

注 K 是完美的， L/K 是代数扩张，那么， L/K 是可分的。特别地，在特征零的范畴内，所有的代数扩张都是可分的。

命题 7.8

K 是特征为 p 的域。那么， K 是完美的当且仅当 Frob 是满射。

证明 如果 Frob 不是满射，那么，选取 $a \in K - \text{Frob}(K)$ ， $X^p - a$ 是不可约也不可分的多项式，从而， K 不完美。如果 Frob 是满射，假设 $P(X)$ 不可约，如果 $P(X)$ 还是不可分的，那么， $P'(X) = 0$ ，

³如果 $b'^p = a$ ，那么， $(b - b')^p = b^p - b'^p = 0$ ，从而， $b = b'$ 。

从而,

$$P(X) = \sum_{p|m} a_m X^m = \sum a_{kp} X^{kp}.$$

令 $\text{Frob}(b_k) = a_{kp}$, 那么,

$$P(X) = \left(\sum b_k X^k \right)^p.$$

这说明, $P(X)$ 可约。

例题 7.4 令 $K = \mathbb{F}_p(T) = \text{Frac}(\mathbb{F}_p[T])$ 。根据 Eisenstein 判别, $X^p - T \in K[X]$ 是不可约多项式。所以, $\mathbb{F}_p(T)$ 不是完美的。

一个代数扩张是否是可分的可以用所谓的可分次数来刻画。

给定代数扩张 L/K , 任选域同态 $\varphi: K \rightarrow E$, 其中, E 是代数封闭域。令

$$\text{Ext}_{L/K}(E, \varphi) = \{\psi \in \text{Hom}(L, E) \mid \psi|_K = \varphi\}.$$

这是 φ 到 L 上所有可能的扩张所构成的集合。对另一个可能的域同态 $\varphi': K \rightarrow E'$, 其中, E' 是代数封闭域。我们有集合之间的双射:

$$\text{Ext}_{L/K}(E, \varphi) \xrightarrow{1:1} \text{Ext}_{L/K}(E', \varphi').$$

实际上, 通过选取 $\varphi(K)$ 在 E 中的代数闭包, 我们可以假设 $E = \overline{\varphi(K)}$; 类似地, $E' = \overline{\varphi'(K)}$ 。根据代数闭包的唯一性, 我们有选取域同态 $\sigma: E \rightarrow E'$, 是的 $\psi' = \psi \circ \sigma$:

$$\begin{array}{ccc} E & \xrightarrow{\sigma} & E' \\ \swarrow \varphi & & \nearrow \varphi' \\ & K & \end{array}$$

那么, 我们可以构造双射

$$\text{Ext}_{L/K}(E, \varphi) \longrightarrow \text{Ext}_{L/K}(E', \varphi'), \quad \bar{\varphi} \mapsto \sigma \circ \bar{\varphi}.$$

其逆为 $\bar{\varphi}' \mapsto \sigma^{-1} \circ \bar{\varphi}$ 。

定义 7.8

对任意的代数扩张 L/K , 任任选域同态 $\varphi: K \rightarrow E$, 其中, E 是代数封闭的, 我们定义 L/K 的可分次数为

$$[L:K]_s := |\text{Ext}(E, \varphi)|.$$



注 如果 L/K 是有限扩张, 我们将证明 $[L:K]_s \leq [L:K]$ 并且 L/K 可分当且仅当 $[L:K]_s = [L:K]$ 。

例题 7.5 $[\mathbb{C}:\mathbb{R}]_s = 2$ 。

例题 7.6 令 $K = \mathbb{Q}$, $L = \mathbb{Q}[X]/X^3 - 2$ 。此时, $[L:K]_s = 3$, 因为 L 到 $\bar{\mathbb{Q}}$ 的像被 $X^3 - 2$ 的不同的根的个数决定。

例题 7.7 令 $L = \mathbb{F}_p(T) = \text{Frac}(\mathbb{F}_p[T])$, $K = \mathbb{F}_p(T^p) = L^p = \text{Frob}(L)$ 。此时, $[L:K] = p$, 因为 $T \in L$ 的极小多项式是 $X^p - T^p \in K[X]$, 即 $L = K[X]/X^p - T^p$ 。此时, $X^p - T^p$ 在 $\Omega = \bar{K}$ 中只有一个根, 从而, $[L:K]_s = 1$ 。这是一个纯不可分的扩张。

给定代数扩张 L/K 和中间域 $K \subset M \subset L$, 把某个 $\varphi: K \rightarrow E$ 延拓到 L 上等价于可以先延拓

到 M 上然后再延拓到 L 上, 即

$$\text{Ext}_{L/K}(E, \varphi) = \coprod_{\psi \in \text{Ext}_{M/K}(E, \varphi)} \text{Ext}_{L/M}(E, \psi).$$

根据以上集合的分解, 我们就得到了

命题 7.9

给定代数扩张 L/K 和中间域 $K \subset M \subset L$, $[L:K]_s$ 有限当且仅当 $[L:M]_s$ 和 $[M:K]_s$ 均有限。进一步, 我们还有

$$[L:K]_s = [L:M]_s [M:K]_s.$$

推论 7.4 (纯不可分扩张的刻画)

L/K 是代数扩张, 给定 $x \in L$, 如果 $[K(x):K]_s = 1$, 即 $K(x)/K$ 到 \bar{K} 的扩张只有一种方式, 我们就称 x 是纯不可分的。如果每个 $x \in L$ 都是纯不可分的, 我们就称 L/K 是纯不可分的。

那么, L/K 是纯不可分的等价于 $[L:K]_s = 1$ 。

证明 如果 $[L:K]_s = 1$, 那么, 对任意的 $x \in L$, 考虑中间域 $K(x) \subset L$, 我们有 $[K(x):K]_s \leq [L:K]_s = 1$, 所以, x 是纯不可分的。

反之, 给定 $\varphi: K \rightarrow \Omega$, 其中, Ω 是代数封闭域。由于对任意的 $x \in L$, $[K(x):K]_s = 1$, 所以 $K(x)/K$ 到 \bar{K} 的扩张是唯一的, 从而 x 的像是唯一决定的。据此, $|\text{Ext}_{L/K}(E, \varphi)| = 1$, 即 $[L:K]_s = 1$ 。

推论 7.5

给定代数扩张 L/K 和中间域 $K \subset M \subset L$ 。那么, L/K 是纯不可分的当且仅当 L/M 和 M/K 是纯不可分的。

命题 7.10

L/K 是代数扩张, $M \subset L$ 是子集并且 M 中的元素均为纯不可分的, 那么, $K(M)/K$ 是纯不可分的。

证明 由于对每个 $x \in M$, $[K(x):K]_s = 1$, 所以, $|\text{Ext}_{K(M)/K}(E, \varphi)| = 1$ 。

为了进一步刻画 $[L:K]$ 和 $[L:K]_s$ 之间的关联, 我们先研究单代数扩张的情形, 即 $L = K(x)$, 其中, $x \in L$ 并且是 K 上的代数元。此时, 回忆如下的双射:

$$Z_P(\Omega) \xrightarrow{1:1} \text{Hom}_K(K[X]/(P(X)), \Omega).$$

由于 Ω 是代数封闭的, 我们就得到如下重要结论: **注** $[K(x):K]_s$ 恰好是 x 极小多项式的不同根的个数。

- $\text{Char}(K) = 0$ 。此时, $[K(x):K]_s = [K(x):K] = \deg(P)$, 其中, P 是 x 的极小多项式。

- $\text{Char}(K) = p$ 。此时, 存在 $Q(X) \in K[X]$, 使得 $P(X) = Q(X^{p^n})$, 其中, n 是最大的。那么,

$$[K(x):K] = p^n [K(x):K]_s.$$

实际上, 由于 n 是最大的, 所以, $Q' \neq 0$ (Q 也是不可约的)。此时, Q 有 d 个不同的根而且没有重根。那么, P 也有 d 个不同的根 (从而 $[K(x):K]_s = d$) 但是每个的重数都是 p^n 。此时, $\deg(P) = p^n d$, 所以, $[K(x):K] = p^n d$ 。

我们有时也称 n 为 x 在 K 上不可分次数。

注 以上证明还表明 $x \in K(x) \subset L$ 是可分的 (当且仅当 $n=0$) 当且仅当 $[K(x):K] = [K(x):K]_s$ 。

定理 7.3

K 的特征为 p , L/K 是有限扩张。那么, 存在非负整数 $n \geq 0$ (被称作是 L/K 的不可分次数), 使得

$$[L:K] = p^n [L:K]_s.$$

进一步, $[L:K] = [L:K]_s$ 当且仅当 L/K 是可分扩张。



证明 我们可以把 L 写成 $K(x_1, \dots, x_k)$ 并令 $K_0 = K$, $K_i = K(x_1, \dots, x_i)$, 其中, $i = 1, \dots, k$ 。根据单代数扩张的情形, 我们有

$$[K_i:K_{i-1}] = p^{n_i} [K_i:K_{i-1}]_s.$$

取乘积并令 $n = \sum n_i$ 即可。

如果 L/K 是可分扩张, 那么, x_i 在 K_{i-1} 上也可分, 从而, $n_i = 0$, 所以, 以上 $n = 0$ 。

反之, 如果 L/K 不是可分扩张, 我们可以选取 x_1 是不可分元, 从而, $n_1 > 0$, 所以 $n > 0$ 。

推论 7.6

L/K 是有限的纯不可分扩张, 那么, $[L:K]$ 是 p 的幂, 其中, $p = \text{Char}(K)$ 。



推论 7.7

L/K 是域扩张, $M \subset L$ 是由某些代数的元组成的子集并且 M 中的元素均为可分的。那么, $K(M)/K$ 是可分的。



证明 实际上, 对任意的 $x \in K(M)$, 存在 x_1, \dots, x_k , 使得 $x \in K(x_1, \dots, x_k)$ 。定理的证明过程表明 $K(x_1, \dots, x_k)/K$ 是可分的, 从而, x 可分。

推论 7.8

给定代数扩张 L/K 和中间域 $K \subset M \subset L$ 。那么, L/K 是可分的当且仅当 L/M 和 M/K 是可分的。



证明 如果 L/K 是可分, 那么, M/K 显然是可分的。另外, 对任意的 $x \in L$, 由于 x 在 K 上的极小多项式是在 M 上的极小多项式的倍数 (作为 $M[X]$ 中的元素), 所以, x 在 M 上的极小多项式是没有重根的, 即 L/M 是可分的。

反之, 假设 L/M 和 M/K 是可分的, 对任意的 $x \in L$, 令

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0, \quad a_i \in M,$$

为 x 在 M 上的最小多项式。此时, $x \in K(a_0, \dots, a_{n-1}, x)$ 。此时, 令 $K_i = K(a_0, \dots, a_i)$, $K_n = K(a_0, \dots, a_{n-1}, x)$, 那么, 以上定理的证明过程表明 $K(a_0, \dots, a_{n-1}, x)/K$ 是可分的, 从而, x 可分。

推论 7.9

给定代数扩张 L/K , 那么, 存在唯一的最大的中间域 \bar{L}^s (被称作是 K 在 L 中的可分闭包), 使得 \bar{L}^s/K 可分。此时, L/\bar{L}^s 是纯不可分的, 即 $[L:\bar{L}^s]_s = 1$ 。

$$\begin{array}{c} L \\ \text{纯不可分} \Big| \\ \bar{L}^s \\ \text{(极大) 可分} \Big| \\ K \end{array}$$

进一步, 如果 $[L:K]_s < \infty$, 那么,

$$[L:K]_s = [\bar{L}^s:K]_s = [\bar{L}^s:K].$$



证明 由于在 K 上添加可分元得到的扩张还是可分的, 我们把 L 中所有可分元素加到 K 中就构造出了 \bar{L}^s 。现在证明 $[L:\bar{L}^s]_s = 1$ 。实际上, 只要说明对任意的 $x \in L$, $[\bar{L}^s(x):\bar{L}^s]_s = 1$ 即可, 这等价于证明了 x 在 $\bar{L}^s[X]$ 上的极小多项式 $P(X)$ 只有一个根。此时, 存在 $n \geq 1$, 使得 $P(X) = Q(X^{p^n})$ 并且 $Q' \neq 0$ 。那么, x^{p^n} 是 Q 的根, 从而, x^{p^n} 是可分的, 从而, $x^{p^n} \in \bar{L}^s$ 。这表明, $P(X) | X^{p^n} - x^{p^n} \in \bar{L}^s[X]$ 。而 $X^{p^n} - x^{p^n}$ 只有一个根, 从而, $P(X)$ 只有一个根 (从而到代数封闭域 Ω 的延拓是唯一的)。

如果 $[L:K]_s < \infty$, 公式 $[L:K]_s = [\bar{L}^s:K]_s = [\bar{L}^s:K]$ 是显然的。

例题 7.8 考虑单代数扩张 $K(x)/K$ 。假设 $P(X)$ 为 x 的极小多项式, $P(X) = Q(X^{p^n})$, 其中, n 是 x 的不可分次数, $Q \in K[X]$ 并且 Q 是可分的。那么, K 的可分闭包为 $K(x^{p^n})$, 即

$$\begin{array}{c} K(x) \\ \text{纯不可分} \Big| \\ K(x^{p^n}) \\ \text{可分} \Big| \\ K \end{array}$$

此时, x 在 $K(x^{p^n})$ 上的极小多项式为 $X^{p^n} - x^{p^n}$, 它只有一个根, 从而, $[K(x):K(x^{p^n})]_s = 1$ 。据此, $\overline{K(x)}^s = K(x^{p^n})$ 。

例题 7.9 根据上一例子, 如果 L/K 是代数扩张, 对任意的 $x \in L$, 令 n_x 为其不可分次数, 那么,

$$\bar{L}^s = K(\{x^{p^{n_x}} | x \in L\}).$$

7.4.1 单扩张与可分扩张

给定域扩张 L/K , 如果存在 $x \in L$, 使得 $L = K(x)$, 我们就说 L/K 是单扩张并称 x 是一个本原元素。

命题 7.11

L/K 是有限扩张。那么, L/K 是单扩张当且仅当它只有有限个中间域。

证明 如果 K 是有限域, 那么, L 也是, 由于 L^\times 是循环群, 所以, 选这个循环的生成元就可以生成 L 。以下总假设 K 是无限域。

假设 L/K 只有有限个中间域。不妨设 $L = K(x_1, \dots, x_d)$, 只要对 $d=2$ 证明该扩张为单扩张即可, 即假设 $L = K(x_1, x_2)$ 。由于 K 是无限域, 存在 $a, b \in K$, 使得

$$K(x_1 + ax_2) = K(x_1 + bx_2) = M, \quad a \neq b.$$

此时, $x_1 + ax_2, x_1 + bx_2 \in M$, 那么,

$$(a-b)x_2 = (x_1 + ax_2) - (x_1 + bx_2) \in M \Rightarrow x_2 \in M.$$

从而, $x_1 \in M$, 这说明 $L = M = K(x_1 + ax_2)$ 。

假设 $L = K(x)$, 令 $P(X) \in K[X]$ 为 x 在 K 上的极小多项式。任选 $M \subset K(x)$ 是中间域, 令 $P_M(X)$ 为 x 在 M 上的极小多项式, 那么, 在 $M[X]$ 上, 我们有 $P_M | P$ 。令

$$P_M(x) = X^m + a_{m-1}X^{m-1} + \dots + a_1X + a_0, \quad a_i \in M.$$

很显然, $K(a_0, \dots, a_m) \in M$ 。另外, $[K(x) : K(a_0, \dots, a_m)] \leq \deg(P_M) = [L : M]$, 从而, $M = K(a_0, \dots, a_m)$ 。所以, 中间域完全由 P_M 的系数决定。但是 P 的首一的因子 P_M 只有有限个, 从而只有有限个中间域。

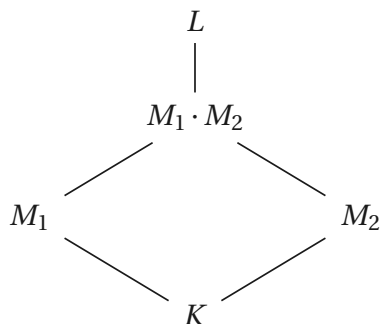
推论 7.10 (本原元素定理)

L/K 是有限可分扩张, 那么, 这是单扩张。

证明 给定 $\Omega = \overline{K}$, 令 \mathcal{P} 为 $\text{Hom}_K(L, \Omega)$ 的子集所组成的集合, 这是有限集。令 \mathcal{M} 为中间域组成的集合。我们证明如下映射为单射:

$$\Psi : \mathcal{M} \rightarrow \mathcal{P}, M \mapsto \text{Hom}_M(L, \Omega).$$

假设 $\text{Hom}_{M_1}(L, \Omega) = \text{Hom}_{M_2}(L, \Omega)$, 那么, 考虑如下图表:



容易看到, $\text{Hom}_{M_1}(L, \Omega) \subset \text{Hom}_{M_1 \cdot M_2}(L, \Omega)$, 所以,

$$|\text{Hom}_{M_1 \cdot M_2}(L, \Omega)| \geq |\text{Hom}_{M_1}(L, \Omega)|.$$

由于 L/K 可分, 所以, $L/M_1 \cdot M_2$ 和 L/M_1 都可分, 从而,

$$|\text{Hom}_{M_1 \cdot M_2}(L, \Omega)| = [L : M_1 \cdot M_2] \leq [L : M_1] = |\text{Hom}_{M_1}(L, \Omega)|.$$

结合以上两个不等式, 我们有 $[L : M_1 \cdot M_2] = [L : M_1]$, 从而, $M_1 \cdot M_2 = M_1 = M_2$ 。既然 Φ 为单射, 那么, L 由有限个中间域, 从而, L/K 是单扩张。

7.4.2 迹与范数映射

考虑有限扩张 L/K , 对任意的 $x \in L$, 我们考虑乘法映射:

$$m_x : L \rightarrow L, y \mapsto x \cdot y.$$

这是线性空间 L 上的 K -线性映射, 我们定义它的迹、行列式和特征多项式为:

$$\text{Tr}_{L/K}(x) = \text{Tr}(m_x), N_{L/K}(x) = \det(m_x), P_{L/K, x}(X) = \det(X \cdot I - m_x).$$

很明显, x 为 m_x 在域 L 上的特征值, 从而, $P_{L/K, x}(x) = 0$ 。注对于 $x \in L$, 令 $P(X)$ 为 x 在 K 上的极小多项式, 它和 $P_{L/K, x}(X)$ 之间的关系如下:

$$P_{L/K, x}(X) = P(X)^{[L:K(x)]}.$$

选取 e_1, \dots, e_m 为 $K(x)/K$ 的基, f_1, \dots, f_n 为 $L/K(x)$ 的基。那么, $\{e_i f_j\}_{i \leq m, j \leq n}$ 为 L/K 的基。考虑 $m_x : K(x) \rightarrow K(x)$ 的矩阵表示 M , 我们有 $\det(X \cdot I - M) = P(x)$ (实际上, 我们可以选取 e_1, \dots, e_n 为 $1, x, \dots, x^{m-1}$, 其中, $m = \deg(P)$)。我们知道在 L 上, m_x 的矩阵表示现在可以写成

$$\det \begin{pmatrix} M & 0 & \cdots & 0 \\ 0 & M & \cdots & 0 \\ & & \ddots & 0 \\ 0 & 0 & \cdots & M \end{pmatrix}.$$

这就给出了以上公式。

命题 7.12

以下映射为群同态:

$$\text{Tr}_{L/K} : (L, +) \rightarrow (K, +), N_{L/K} : (L^\times, \cdot) \rightarrow (K^\times, \cdot).$$

如果 $M \subset L$ 是中间域, 那么,

$$\text{Tr}_{L/M} \circ \text{Tr}_{M/K} = \text{Tr}_{L/K}, N_{L/M} \circ N_{M/K} = N_{L/K}.$$

证明 群同态的性质根据定义立得。以下研究迹 Tr 以及范数 N 映射的复合性质。

定理 7.4

L/K 为有限可分扩张, E/K 为域扩张并且 $|\text{Hom}_K(L, E)| = [L:K]$ 。那么, 对任意的 $x \in L$,

$$\text{Tr}_{L/K}(x) = \sum_{\sigma \in \text{Hom}_K(L, E)} \sigma(x), \quad N_{L/K}(x) = \prod_{\sigma \in \text{Hom}_K(L, E)} \sigma(x),$$

以及

$$P_{L/K, x}(X) = \prod_{\sigma \in \text{Hom}_K(L, E)} (X - \sigma(x)).$$



证明

7.5 Galois 理论

7.5.1 Galois 对应

给定正规 (代数) 扩张 L/K , 我们记 $\text{Gal}(L/K) = \text{Aut}_K(L)$ 并称之为 L/K 的 **Galois 群**。如果域扩张 L/K 是正规的也是可分的, 我们就称 L/K 为 **Galois 扩张**。对任意的子群 $H < \text{Gal}(L/K)$, 我们定义

$$L^H := \{x \in L \mid g(x) = x, \forall g \in H\}.$$

引理 7.9

L/K 是有限正规扩张, 我们有

$$[L:K]_s = |\text{Gal}(L/K)|.$$

特别地, 如果 L/K 是 Galois 扩张, 我们有

$$[L:K] = |\text{Gal}(L/K)|.$$



证明 我们选定域扩张 Ω/L , 其中, Ω 是代数封闭的。那么,

$$[L:K]_s = |\text{Ext}_{L/K}(\Omega, \text{id})| \stackrel{\text{正规}}{=} |\text{Ext}_{L/K}(L, \text{id})| = |\text{Gal}(L/K)|.$$

如果 L/K 是 Galois 扩张, 那么, $[L:K]_s = [L:K]$ 。

命题 7.13

L/K 是正规扩张, $G = \text{Gal}(L/K)$ 。那么, L^G/K 是纯不可分的, L/L^G 是 Galois 扩张并且

$$\text{Gal}(L/L^G) = G.$$

进一步, 我们有 $\bar{L}^s \cdot L^G = L$, $\bar{L}^s \cap L^G = K$ 。



证明 根据正规性的定义,

$$\text{Ext}_{L^G/K}(\Omega, \text{id}) = \text{Ext}_{L^G/K}(L, \text{id}).$$

根据定义, 对于每个 $\varphi \in \text{Ext}_{L^G/K}(L, \text{id})$, 它延拓到成 L 上的自同构之后在 L^G 上是单位元, 所

以, 以上集合只有一个元素, 从而, $[L^G:K]_s = 1$, 即 L^G/K 纯不可分。

现在证明 L/L^G 是可分的: 对任意的 $x_1 \in L$, 令 $P(X) \in L^G[X]$ 为 x_1 在 L^G 上的极小多项式, 它的所有根都落在 L 中 (因为 L/L^G 是正规的), 令 x_1, \dots, x_m 为 P 的所有不同的根。对任意的 $\sigma \in G$, 我们知道 $P^\sigma = P$ (因为 P 是 L^G 系数的)。从而, 对任意的根 x_i ,

$$0 = P(x_i) = P^\sigma(x_i) = \left(\prod_{\text{所有根}} (X - \alpha) \right)^\sigma = \prod_{\text{所有根}} (X - \sigma(\alpha)).$$

这表明 x_i 形如 $\sigma(\alpha)$, 记 $\sigma^{-1}(x_i)$ 仍然是根。从而, 我们得到了群作用:

$$\text{Gal}(L/K) \times \{x_1, \dots, x_m\} \rightarrow \{x_1, \dots, x_m\}.$$

令 $Q(X) = (X - x_1) \cdots (X - x_m)$, 那么, 对任意的 $g \in G$, $Q^g = Q$, 这说明 Q 的系数均落在 L^G 中。特别地, $P|Q$ 而 Q 无重根, 从而, P 是可分的。

最后来说明 $\text{Gal}(L/L^G) = G$ 。根据定义, $\text{Gal}(L/L^G) < \text{Gal}(L/K)$ 。另外, 对任意的 $g \in \text{Gal}(L/K)$, 按定义, g 在 L^G 上的作用是平凡的, 从而, $g \in \text{Gal}(L/L^G)$ 。

我们注意到 $\bar{L}^s \cap L^G/K$ 是 L^G 的中间域, 所以是纯不可分的, 它也是 \bar{L}^s 的中间域, 所以是可分的, 从而, $\bar{L}^s \cap L^G = K$; $L/\bar{L}^s \cdot L^G$ 是 L/\bar{L}^s 的中间域, 所以是纯不可分的, 也是 L/L^G 的中间域 (这是一个 Galois 扩张), 所以是可分的, 从而, $\bar{L}^s \cdot L^G = L$ 。

注 如果 L/K 是有限正规扩张, 我们还有

$$[L:L^G] = [L:K]_s = \text{Gal}(L/K), [L^G:K] = \frac{[L:K]}{[L:K]_s} = L/K \text{ 的不可分次数}.$$

定理 7.5 (Galois 对应定理)

L/K 是有限 Galois 扩张, 定义中间域的集合和子群的集合:

$$\mathcal{M} = \{K \subset M \subset L \mid M \text{ 是中间域}\}, \mathcal{S} = \{H < \text{Gal}(L/K) \text{ 是子群}\},$$

并用包含关系作为 \mathcal{M} 和 \mathcal{S} 上的偏序。那么, 我们有如下的反转偏序关系的 **Galois 对应** (以下映射互为逆):

$$\mathcal{M} \xrightarrow{1:1} \mathcal{S}, M \mapsto \text{Gal}(L/M), L^H \mapsto H.$$

$$\begin{array}{ccc} L & \text{-----} & 1 \\ \updownarrow & & \updownarrow \\ M_1 & \text{-----} & \text{Gal}(L/M_1) \\ \updownarrow & & \updownarrow \\ M_2 & \text{-----} & \text{Gal}(L/M_2) \\ \updownarrow & & \updownarrow \\ K & \text{-----} & \text{Gal}(L/K) \end{array}$$

$$\begin{array}{ccc} L & \text{-----} & 1 \\ \updownarrow & & \updownarrow \\ L^{H_1} & \text{-----} & H_1 \\ \updownarrow & & \updownarrow \\ L^{H_2} & \text{-----} & H_2 \\ \updownarrow & & \updownarrow \\ K & \text{-----} & \text{Gal}(L/K) \end{array}$$

进一步, 扩张 M/K 是正规扩张^a当且仅当 $\text{Gal}(L/M) \triangleleft \text{Gal}(L/K)$ 是正规子群并且在此情形下, 我们有

$$\text{Gal}(M/K) = \text{Gal}(L/K) / \text{Gal}(L/M).$$

^a从而是 Galois 扩张

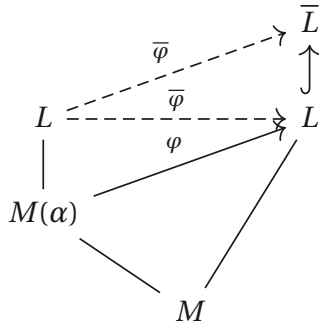


证明 我们用 $\Phi: \mathcal{M} \rightarrow \mathcal{S}$ 和 $\Psi: \mathcal{S} \rightarrow \mathcal{M}$ 表示上述对应映射。我们证明 $\Psi \circ \Phi = \text{id}_{\mathcal{M}}$, 即对给定的 $M \in \mathcal{M}$, 证明 $L^{\text{Gal}(L/M)} = M$:

令 $M' = L^{\text{Gal}(L/M)}$, 按定义, $M \subset M'$, 只要证明 $M' \subset M$ 即可。如若不然, 选取 $\alpha \in M' - M$ 并用 $P(X)$ 表示 α 在 M 上的极小多项式。此时, $\deg(P) \geq 2$ 。

$$\begin{array}{ccc} M(\beta) & \hookrightarrow & L \\ \uparrow \varphi & & \downarrow \\ M(\alpha) & \hookrightarrow & M' \\ & & \downarrow \\ & & M \end{array}$$

由于 L/M 是正规扩张, 所以, P 的所有根都在 L 中。另外, L/M 是可分扩张, 我们可以选取 $\beta \in L$, 使得 $P(\beta) = 0$ 并且 $\beta \neq \alpha$ 。由于 $M(\beta)$ 与 $M(\alpha)$ 同构, 我们选取 $\varphi \in \text{Hom}_M(M(\alpha), M(\beta))$, 从而, $\varphi \in \text{Hom}_M(M(\alpha), L)$ 。



此时, φ 可以被扩张成 $\bar{\varphi}: L \rightarrow \bar{L}$ 。由于 L/M 是正规扩张, 所以, $\bar{\varphi}: L \rightarrow L$, 即 $\bar{\varphi} \in \text{Gal}(L/M)$ 。然而, 对于 $\alpha \in M'$, $\bar{\varphi}(\alpha) = \beta \neq \alpha$, 矛盾。**注** 在以上证明 $\Psi \circ \Phi = \text{id}_{\mathcal{M}}$ 的过程中, 我们并不需要假设 L/K 是有限扩张。作为应用, 我们考虑 $\bar{\mathbb{Q}}/\mathbb{Q}$, 这是 Galois 扩张。对任意的 $\alpha \in \bar{\mathbb{Q}}$, $\alpha \in \mathbb{Q}$ 当且仅当对任意的 $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, $\sigma(\alpha) = \alpha$ 。

我们现在证明 $\Psi \circ \Phi = \text{id}_{\mathcal{S}}$, 即对给定的 $H \in \mathcal{S}$, 证明 $\text{Gal}(L/L^H) = H$ 。根据定义 $H < \text{Gal}(L/L^H)$, 特别地, 我们有

$$|H| \leq |\text{Gal}(L/L^H)| = [L : L^H].$$

由于 L/L^H 是有限可分扩张, 根据本原元素定理, 存在 $\alpha \in L$, 使得 $L = L^H(\alpha)$ 。考虑如下 L -系数的多项式

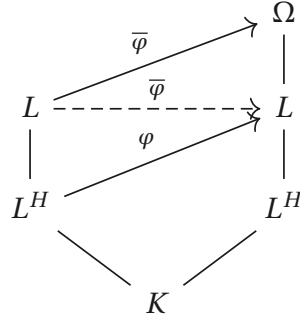
$$Q(X) = \prod_{h \in H} (X - h(\alpha)).$$

很明显, Q 的系数是 $\{h(\alpha) | h \in H\}$ 的对称多项式, 从而, 它们均在 H 的作用下不变。根据 L^H 的定义, 我们有 $Q(X) \in L^H[X]$ 。令 $P(X) \in L^H[X]$ 是 α 的极小多项式, 由于 $Q(\alpha) = 0$, 所以, 在 $L^H[X]$ 中, 我们有 $Q | P$ 。特别地,

$$|H| = \deg(Q) \geq \deg(P) = [L^H(\alpha) : L^H] = [L : L^H].$$

综合以上不等式, 我们就证明了 $H = \text{Gal}(L/L^H)$ 。

假设 $H \triangleleft \text{Gal}(L/K)$, 为了说明 L^H/K 是正规扩张, 任意选取 $\varphi \in \text{Hom}_K(L^H, \Omega)$, 其中, $\Omega = \bar{L} \supset L$, 我们证明 $\varphi(L^H) = L^H$:

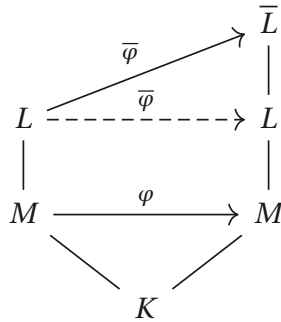


首先把 φ 延拓成 $\bar{\varphi} \in \text{Hom}_K(L, \Omega)$, 由于 L/L^H 是正规扩张, 所以, $\bar{\varphi} \in \text{Hom}_K(L, L)$, 从而, $\bar{\varphi} \in \text{Gal}(L/K)$ 。为了证明 $\varphi(L^H) \subset L^H$, 我们任选 $x \in L^H$, 只要证明对任意的 $h \in H$, $h(\bar{\varphi}(x)) = \bar{\varphi}(x)$ 即可。这等价于 $(\bar{\varphi}^{-1} \cdot h \cdot \bar{\varphi})(x) = x$ 。由于 $H \triangleleft \text{Gal}(L/K)$, $\bar{\varphi}^{-1} \cdot h \cdot \bar{\varphi} \in H$ 而 $x \in L^H$, 以上等式是显然的。

假设 M/K 是正规扩张, 那么, 对任意的 $\varphi \in \text{Gal}(L/K)$, 我们有 $\varphi(M) \subset M$ 。通过 φ 在 M 上的限制, 我们有群同态:

$$\text{Res} : \text{Gal}(L/K) \rightarrow \text{Gal}(M/K).$$

另外, 对每个 $\varphi \in \text{Gal}(M/K)$, 我们总能将它延拓成 $\text{Gal}(L/K)$ 中的元素 $\bar{\varphi}$:



所以, 以上的限制映射是满射:

$$\text{Res} : \text{Gal}(L/K) = \text{Hom}_K(L, \bar{L}) \twoheadrightarrow \text{Hom}_K(M, \bar{L}) = \text{Gal}(M/K).$$

按照定义, $\text{Ker}(\text{Res}) = \text{Gal}(L/M)$, 即

$$1 \longrightarrow \text{Gal}(L/M) \xrightarrow{\subset} \text{Gal}(L/K) \xrightarrow{\text{Res}} \text{Gal}(M/K) \longrightarrow 1.$$

这就完成了整个证明。

7.5.2 Galois 群在根上的作用

L/K 是有限 Galois 扩张, 那么, L 是某个多项式 $P(X) \in K[X]$ 的分裂域。由于 L/K 是可分的, 我们可以假设 $P(X)$ 是可分的多项式, 从而其根是两两不同的。令 $Z_P(L) = \{\alpha_1, \dots, \alpha_d\}$ 为 P 在 L 中根的集合, 其中, $d = \deg(P)$ 。根据分裂域的定义, 我们还有 $L = K(\alpha_1, \dots, \alpha_d)$ 。

由于 P 是 K -系数多项式, 所以, $P^\sigma = P$ 。对任意的 $\alpha \in Z_P(L)$, $P(\alpha) = 0$, 从而,

$$0 = P(\alpha) = P^\sigma(\alpha) = P(\sigma(\alpha)).$$

所以, $\sigma(\alpha) \in Z_P(L)$ 也是根。据此, 我们构造了映射

$$\text{Gal}(L/K) \times Z_P(L) \longrightarrow Z_P(L), (\sigma, \alpha) \mapsto \sigma(\alpha).$$

由于对任意的 $\sigma_1, \sigma_2 \in \text{Gal}(L/K)$, 我们显然有 $\sigma(\sigma_2(\alpha)) = (\sigma_1 \cdot \sigma_2)(\alpha)$, 以上映射给出了 Galois 群 $\text{Gal}(L/K)$ 在根的集合 $Z_P(L)$ 上的作用 $\text{Gal}(L/K) \curvearrowright Z_P(L)$ 。根据群作用的定义, 我们有群同态

$$\text{Gal}(L/K) \longrightarrow \mathfrak{S}_{Z_P(L)}.$$

由于 $L = K(\alpha_1, \dots, \alpha_d) = K(Z_P(L))$, 所以, 如果 $\sigma \in \text{Ker}(\text{Gal}(L/K) \rightarrow \mathfrak{S}_{Z_P(L)})$, 那么, σ 固定每个 $\alpha \in Z_P(L)$, 从而, σ 固定 L , 即 $\sigma = 1$ 。这表明以上作用为忠实的, 即

$$\text{Gal}(L/K) \longrightarrow \mathfrak{S}_{Z_P(L)}$$

是单同态。

定理 7.6

K 是域, $P \in K[X]$ 为可分的多项式, L 是 P 的分裂域。那么, $\text{Gal}(L/K)$ 在根的集合上的作用 $Z_P(L)$ 是忠实的:

$$1 \rightarrow \text{Gal}(L/K) \longrightarrow \mathfrak{S}_{Z_P(L)}.$$

这个作用是传递的当且仅当 P 是不可约多项式。



证明 只要研究传递性与可约性之间的关系。

如果 P 是可约的, 那么, $P(X) = P_1(X)P_2(X)$, 其中, $P_1, P_2 \in K[X]$ 。从而, $Z_P(L) = Z_{P_1}(L) \sqcup Z_{P_2}(L)$ 。我们注意到 $Z_{P_1}(L)$ 和 $Z_{P_2}(L)$ 都不是空集。对任意的 $\alpha \in Z_{P_1}(L)$, 很明显, $P_1(\sigma(\alpha)) = P_1^\sigma(\alpha) = P_1(\alpha) = 0$ 。这表明,

$$\text{Gal}(L/K) \times Z_{P_1}(L) \longrightarrow Z_{P_1}(L).$$

对 $Z_{P_2}(L)$, 以上仍然成立。所以, $\text{Gal}(L/K) \curvearrowright Z_P(L)$ 至少有 2 个轨道从而不是传递的。

如果 P 是不可约的, 我们用反证法证明 $\text{Gal}(L/K) \curvearrowright Z_P(L)$ 是传递的: 假设 $\{\alpha_1, \dots, \alpha_{d'}\}$ 是一个轨道并且 $d' < d = \deg(P)$ 。考虑多项式

$$Q(X) = (X - \alpha_1) \cdots (X - \alpha_{d'}).$$

那么, 对任意的 $\sigma \in \text{Gal}(L/K)$, 我们有

$$Q^\sigma(X) = (X - \sigma(\alpha_1)) \cdots (X - \sigma(\alpha_{d'})) = Q(X).$$

由于 Q^σ 是 σ 在 Q 的系数上的作用, 根据 $K = L^{\text{Gal}(L/K)}$, $Q(X) \in K[X]$ 。另外, 由于 $P(\alpha_1) = 0$,

所以, P 是 α_1 的极小多项式, 而 $Q(\alpha_1) = 0$, 从而, $P \mid Q$, 但是 $\deg(P) > \deg(Q) = d'$, 矛盾。

根据以上证明, 我们还有如下的性质: **注** 假设 L 是可分多项式 $P(X) \in K[X]$ 的分裂域并且 P 是 m 个不可约多项式的乘积, 即 $P(X) = P_1(X) \cdot P_m(X)$, 那么, $\text{Gal}(L/K) \curvearrowright Z_P(L)$ 具有 m 个轨道并且每个轨道都对应着某个 $P_i(X)$ 的根。

例题 7.10 考虑域扩张 $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, 我们来计算其 Galois 群 $G = \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ 。

利用中间域

$$\mathbb{Q} \longrightarrow \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3}),$$

我们知道该扩张次数为 4, 从而, $|G| = 4$ 。据此, $G \simeq \mathbb{Z}/4\mathbb{Z}$ 或者 $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 。

我们注意到 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 是 $(X^2 - 2)(X^2 - 3)$ 在 \mathbb{Q} 上的分裂域, 根据以上对于 Galois 群在根上作用的讨论, 我们有单射

$$G \hookrightarrow \mathfrak{S}_{\{\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}\}} \simeq \mathfrak{S}_4$$

并且该作用有 2 个轨道。从而, $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (如果 $G \simeq \mathbb{Z}/4\mathbb{Z}$, 那么它的作用只能有 1 个轨道)。在以上 $\mathfrak{S}_{\{\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}\}} \simeq \mathfrak{S}_4$ 的等同中, 我们要求 $1 \mapsto \sqrt{2}, 2 \mapsto -\sqrt{2}, 3 \mapsto \sqrt{3}, 4 \mapsto -\sqrt{3}$ 。根据乘积 $(X^2 - 2)(X^2 - 3)$, 1, 2 和 3, 4 分别为 G 作用的轨道。所以, 作为 \mathfrak{S}_4 的子群, 我们有

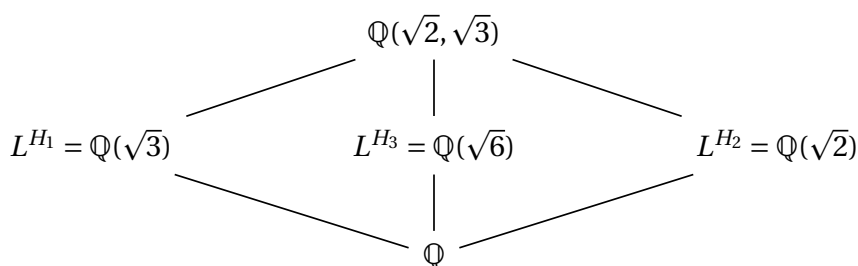
$$G = \langle (1, 2), (3, 4) \rangle.$$

特别地, $G = \{1, \sigma, \tau, \sigma \cdot \tau\}$, 其中,

$$\begin{cases} \sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}, \\ \tau(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}, \\ (\sigma \cdot \tau)(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}, \end{cases}$$

其中, $a, b, c, d \in \mathbb{Q}$ 。

G 共有 3 个非平凡的⁴子群, $H_1 = \langle \sigma \rangle$, $H_2 = \langle \tau \rangle$ 和 $H_3 = \langle \sigma \cdot \tau \rangle$ 。根据 Galois 对应定理, 它们给出了如下的中间域:



例题 7.11 令 $j = e^{\frac{2}{3}\pi i}$, 我们考虑 \mathbb{Q} 上不可约多项式 $X^3 - 2$ 的分裂域 $\mathbb{Q}(\sqrt[3]{2}, j)$ 。由于 $X^3 - 2$ 不可约, 所以,

$$G \hookrightarrow \mathfrak{S}_3,$$

其中, $G = \text{Gal}(\mathbb{Q}(\sqrt[3]{2}, j))$ 。根据中间域

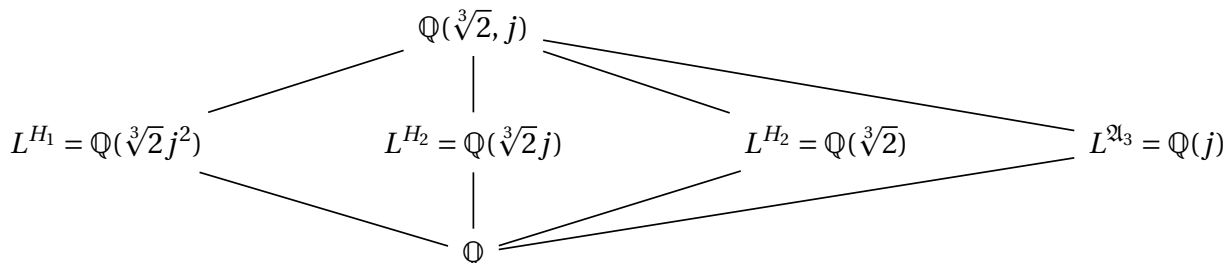
$$\mathbb{Q} \longrightarrow \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{Q}(\sqrt[3]{2}, j),$$

⁴我们只要考虑 $H < G$ 使得 $H \neq G$, $H \neq 1$ 。

这是 6 次扩张, 所以, $G \simeq \mathfrak{S}_3$. 令 1 对应着根 $\sqrt[3]{2}$, 2 和 3 对应着 $\sqrt[3]{2}j$ 和 $\sqrt[3]{2}j^2$. 我们注意到取复共轭 $z \mapsto \bar{z}$ 是 G 中的元, 它对应着对换 (2,3). 我们还知道 \mathfrak{S}_3 有 4 个非平凡子群:

$$H_1 = \langle (1,2) \rangle, H_2 = \langle (1,3) \rangle, H_3 = \langle (2,3) \rangle, \mathfrak{A}_3 = \langle (1,2,3) \rangle.$$

它们所对应的中间域为



以上, $\mathfrak{A}_3 \triangleleft \mathfrak{S}_3$ 是正规子群, 从而, $\mathbb{Q}(j)/\mathbb{Q}$ 是正规扩张 (显然) 而其余中间域对于 \mathbb{Q} 都不是正规扩张。

例题 7.12 令 L 为多项式 $P(X) = X^5 - 6X + 3$ 在 \mathbb{Q} 上的分裂域。根据 Eisenstein 判别法 (mod 3), $P(X)$ 是不可约多项式。此时, 我们没办法很快地计算 $[L:\mathbb{Q}]$ 的具体值。

先具体分析 $P(X)$ 根的分布。首先, $P'(X) = 5(X^4 - \frac{6}{5})$ 在 \mathbb{R} 上恰好有两个根 $\pm\sqrt[4]{\frac{6}{5}}$ 。我们注意到

$$P(\sqrt[4]{\frac{6}{5}}) = -\frac{24}{5}\sqrt[4]{\frac{6}{5}} + 3 < 0, \quad P(-\sqrt[4]{\frac{6}{5}}) = \frac{24}{5}\sqrt[4]{\frac{6}{5}} + 3 > 0.$$

从而, $P(X)$ 在 \mathbb{R} 上共有 3 个根 $x_1 < x_2 < x_3$, 其余 2 个根是复根 (非实数), 它们是 x_4 和 $x_5 = \bar{x}_4$ 。特别地, 我们知道复共轭映射 $z \mapsto \bar{z}$ 是 $G = \text{Gal}(L/\mathbb{Q})$ 中的一个 2-阶元, 它对应着 $G \hookrightarrow \mathfrak{S}_5$ 中的对换 (4,5)。另外, 由于 $P(X)$ 不可约, 所以, $\mathbb{Q}(x_1)$ 是中间域并且其次数为 5, 所以, $5 \mid |G| = [L:\mathbb{Q}]$ 。这表明, G 中有 5 阶元, 从而, G 中有一个 5-循环 (a, b, c, d, e) 。根据第二次作业 A5), 一个对换和 5-循环可以生成 \mathfrak{S}_5 , 从而, $\text{Gal}(L/\mathbb{Q}) \simeq \mathfrak{S}_5$ 。特别地, $[L:\mathbb{Q}] = 120$ 。

另外, 我们回忆一下首一多项式的判别式的定义:

$$\Delta := \prod_{i < j} (x_i - x_j).$$

我们知道

$$\text{Disc}(P) := \Delta^2 = \prod_{i < j} (x_i - x_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (x_i - x_j)$$

在 $\text{Gal}(L/\mathbb{Q})$ 的作用下不变, 从而, $\Delta^2 \in \mathbb{Q}$ 。对于多项式

$$P(X) = X^n + aX + b,$$

我们有

$$\text{Disc}(P) := \Delta^2 = (-1)^{\frac{n(n-1)}{2}} (n^n b^{n-1} + (-1)^{n-1} (n-1)^{n-1} a^n).$$

对于 $P(X) = X^5 - 6X + 3$, 我们有

$$\Delta^2 = 5^5 \times 3^4 - 4^4 \times 6^5 = 3^4 \times (-21451).$$

根据定义, $\Delta := \prod_{i < j} (x_i - x_j)$ 在 \mathfrak{A}_5 作用下不变而 $L^{\mathfrak{A}_5}$ 对应着 \mathbb{Q} 的一个二次扩张 E , 其中,

$\Delta \in E$ 。特别地, $E = \mathbb{Q}(\sqrt{-21351})$ 。这是唯一一个在 \mathbb{Q} 上是 2 次的中间域。

7.5.3 有限域

K 是有限域, $\text{char}(K) = p$, 我们有自然地域同态:

$$\mathbb{F}_p \longrightarrow K.$$

据此, 我们知道 $|K| = p^n$, 其中, $n = [K : \mathbb{F}_p]$ 。

定理 7.7

p 是素数。对任意的 $n \geq 1$, 存在有 p^n 元素的有限域 K 。进一步, 具有 p^n 元素的有限域在同构意义下是唯一的, 它们都同构于 $X^{p^n} - X$ 的分裂域。



注 假设 q 为素数的幂, 我们用 \mathbb{F}_q 表示具有 q 个元素的有限域。

证明 K 显然是 \mathbb{F}_p 的代数扩张, 我们不妨假设 $K \subset \overline{\mathbb{F}_p}$ 。如果这样的 K 存在, 由于 K^\times 是循环群, 从而, 对任意的 $x \in K^\times$, $x^{p^n-1} = 1$ 。所以, 对任意的 $x \in K$, 我们有

$$x^{p^n} - x = 0.$$

所以, K 是 $X^{p^n} - X$ 的分裂域 (因为 $X^{p^n} - X$ 在 $\overline{\mathbb{F}_p}$ 中恰好有 $p^n = |K|$ 个根, 它们都在 K 中), 从而唯一性部分是显然的。

为了证明存在性, 根据上面的讨论, 我们定义

$$K := \{x \in \overline{\mathbb{F}_p} \mid x^{p^n} - x = 0\}.$$

因为 $|K| = p^n$, 只要证明 K 是域即可。实际上, 对任意的 $x, y \in K$, 我们有

$$(x + y)^{p^n} = x^{p^n} + y^{p^n} = x + y, (x \cdot y)^{p^n} = x \cdot y, (x^{-1})^{p^n} = x^{-1}.$$

命题得证。

假设 $q = p^n$, 考虑域扩张 $\mathbb{F}_q/\mathbb{F}_p$ 。由于 \mathbb{F}_p 是完美域, 这是可分扩张; 由于 \mathbb{F}_q 是 $X^{p^n} - X$ 在 \mathbb{F}_p 上的分裂域, 这是正规扩张。所以, $\mathbb{F}_q/\mathbb{F}_p$ 是 Galois 扩张。

定理 7.8

对于 $q = p^n$, $\text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ 是 n 阶循环群并且其生成元为

$$\text{Frob} : \mathbb{F}_q \rightarrow \mathbb{F}_q, x \mapsto x^p.$$

对任意的 $m \mid n$, $\mathbb{F}_q/\mathbb{F}_p$ 具有唯一的中间域 \mathbb{F}_{p^m} (它是 $X^{p^m} - X$ 的分裂域) 并且它们给出了所有的中间域。进一步, $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m})$ 是 $\frac{n}{m}$ 阶的循环群, 它由 Frob^m 生成。



证明 由于 $[\mathbb{F}_q : \mathbb{F}_p] = n$, 所以, $\text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ 有 n 个元素。我们自然有 $\text{Frob} \in \text{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ 。另外, $\text{Frob}^n = x^{p^n} = x$, 对于循环群的生成元 $\xi \in \mathbb{F}_q^\times$, $\text{Frob}^k(\xi) = \xi$ 当且仅当 $n-1 \mid k-1$, 从而, $\text{Frob}^k \neq 1$, 其中, $1 \leq k \leq n-1$ 。据此, $\text{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \{\text{Frob}^k \mid 0 \leq k \leq n-1\}$, 所以,

$$\text{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle \text{Frob} \rangle.$$

对任意的 $m \mid n$, $X^{p^m} - X$ 的分裂域给出了定理中所要求的中间域。由于 n 阶循环群的子群是 m 阶循环群, 其中, $m \mid n$, 根据 Galois 对应定理, 我们就给出了所有的中间域。根据 Galois 对应定理, 我们还有

$$\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) \simeq \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) / \text{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) \simeq \langle \text{Frob}^m \rangle.$$

这就完成了证明。

注 对任意的 p 的幂 q , $\text{Gal}(\mathbb{F}_{q^l}/\mathbb{F}_q)$ 是 l 阶循环群。

7.5.4 分圆扩张

对任意的域 K 和正整数 $n \geq 1$, 我们定义 K 中 n -次单位根的集合:

$$\mu_n(K) = \{x \in K \mid x^n - 1 = 0\}.$$

很明显, $|\mu_n(K)| \leq n$ 。另外, $\mu_n(K)$ 是 K^\times 的子群, 从而是循环群。我们称 $\mu_n(K)$ 的生成元为 K 中的 n -次本原单位根。

注 如果 $n_1 \mid n_2$, 那么, $\mu_{n_1}(K) < \mu_{n_2}(K)$ 是子群。

注 我们有 $|\mu_n(K)| \mid n$, 这是因为对任意的 $x \in \mu_n(K)$, 总有 $x^n = 1$ 。

注 当 $\text{char}(K) = p$ 时, 令 $m = mp^k$, 其中, $p \nmid m$ 。此时, $x^n - 1 = 0$ 等价于 $(x^m - 1)^{p^k} = 0$, 从而, $\mu_n(K) = \mu_m(K)$ 。

我们回忆分圆多项式的定义 (参考第六次作业问题 B):

$$\Phi_n(X) := \prod_{\substack{\xi \in \mu_n(\overline{\mathbb{Q}}), \\ \xi \text{ 本原}}} (X - \xi).$$

考虑 $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 对 Φ_n 的作用。由于它把 n -次本原根映射成 n -次本原根, 从而对任意的 $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, 我们有 $\Phi_n^\sigma = \Phi_n$ 。据此, $\Phi_n(X) \in \mathbb{Q}[X]$ 。另外, 根据如下公式

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X)$$

以及 Gauss 引理⁵, 我们知道 $\Phi_n(X) \in \mathbb{Z}[X]$ 。我们将通过研究所谓的分圆域来证明 $\Phi_n(X)$ 是不可约多项式。

定义 7.9 (分圆域)

K 是域, $n \geq 1$, ξ 是 \overline{K} 中的一个 n -次本原单位根。当 $\text{char}(K) = p$ 时, 还要求 $(p, n) = 1$ 。我们称 $K(\xi) \subset \overline{K}$ 是 K 的 n -次分圆域或者 n -次分圆扩张。



注 $K(\xi)$ 不依赖于 n -次本原单位根的选取, 因为 $K(\xi) = K(\mu_n(\overline{K}))$ 。

由于我们有唯一的映射 $\iota: \mathbb{Z} \rightarrow K$, 通过对系数作用, 我们就得到 $\Phi_n^K(X) \in K[X]$ 。

⁵ A 是唯一分解整环, $K = \text{Frac}(A)$ 为其分式域。如果在 $K[X]$ 中有 $P(X) = P_1(X)P_2(X)$, 其中, $\deg(P_i) \geq 1$, 那么, 存在 $k \in K^\times$, 使得 $kP_1(X), k^{-1}P_2(X) \in A[X]$ 。在以上应用时, 我们注意到 $X^n - 1$ 以及那些分圆多项式 Φ_d 都是首一的。

定理 7.9

$K(\xi)/K$ 是 K 的 n -次分圆扩张^a, $P(X)$ 是 ξ 在 K 上的极小多项式。那么, $K(\xi)/K$ 是 Galois 扩张, $P(X) \mid \Phi_n^K(X)$ 并且我们有如下的群的群同态:

$$\text{Gal}(K(\xi)/K) \longrightarrow \left(\mathbb{Z}/n\mathbb{Z}\right)^\times, \sigma \mapsto k_\sigma,$$

其中, $\sigma(\xi) = \xi^{k_\sigma}$ 。

^a当 $\text{char}(K) = p$ 时, 我们总是假设 $(p, n) = 1$ 。



证明 $K(\xi)$ 是 $X^n - 1$ 的分裂域, 所以 $K(\xi)/K$ 是正规扩张; $(X^n - 1)' = nX^{n-1} \neq 0$ (因为当 $\text{char}(K) = p$ 时, $(p, n) = 1$), 所以, $X^n - 1$ 是可分的多项式, 所以 $K(\xi)/K$ 是可分扩张。从而, $K(\xi)/K$ 是 Galois 扩张。为了证明 $P(X) \mid \Phi_n^K(X)$, 只要说明 $\Phi_n^K(\xi) = 0$ 即可。实际上, 我们在 $K[X]$ 中考虑分解:

$$X^n - 1 = \prod_{d \mid n} \Phi_d^K(X).$$

令 $X = \xi$, 从而, 存在 $d \mid n$, 使得 $\Phi_d^K(\xi) = 0$ 。我们现在说明 $d = n$: 否则 $\Phi_d^K(\xi) = 0$, 其中, $d < n$, 那么, $\xi^d = 1$ (因为 $X^d - 1 = \prod_{d' \mid d} \Phi_{d'}^K(X)$), 这与 ξ 是本原的矛盾 (在 \bar{K} 中, 由于 $(p, n) = 1$, 我们恰有 n 个根)。

由于 $\sigma \in \text{Gal}(K(\xi)/K)$ 作用在 $\Phi_n(X)$ 根的集合上, 所以存在 k_σ , 使得 $\sigma(\xi) = \xi^{k_\sigma}$, 其中, $(k_\sigma, n) = 1$, 这就定义出定理中的群同态 (以上映射是群同态是显然的)。由于 $K(\xi)$ 是单扩张, 所以该同态为单射。

注 $|\text{Gal}(K(\xi)/K)| = [K(\xi):K]$ 整除 $\varphi(n)$ 。

例题 7.13 我们证明 n -次分圆扩张 $\mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q}$ 的次数恰好是 $\varphi(n)$, 从而 $\Phi_n(X)$ 是不可约的。

实际上, 只要证明 $\text{Gal}(K(\xi)/K) \rightarrow \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ 是满射即可, 因为每个本原根 ξ' 恰好等于某个 $\sigma(\xi)$, 从而 $\mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q}$ 在 $\Phi_n(X)$ 的根上的作用是传递的, 所以, $\Phi_n(X)$ 不可约。

为了说明 $\text{Gal}(K(\xi)/K) \rightarrow \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ 是满射, 这要证明对任意的 $l \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$, 存在 $\sigma \in \text{Gal}(K(\xi)/K)$, 使得 $\sigma(\xi) = \xi^l$ 。我们只要对 l 是素数证明即可 ($(l, n) = 1$)。令 $P(X)$ 为 ξ 在 \mathbb{Q} 上的极小多项式, $Q(X)$ 为 ξ^l 在 \mathbb{Q} 上的极小多项式, 只要证明 $Q(X) = P(X)$ 即可, 因为此时 $P \mid \Phi_n$, $\text{Gal}(K(\xi)/K)$ 在这个不可约因子的根的作用上是传递的, 从而有 σ , 使得 $\sigma(\xi) = \xi^l$ 。我们用反证法, 假设 $P \neq Q$

首先, $Q(\xi^l) = 0$, 从而, $P(X) \mid Q(X^l)$, 所以, 存在 $A(X) \in \mathbb{Z}[X]$ (Gauss 引理), 使得

$$Q(X^l) = P(X)A(X).$$

其次, ξ^l 是 $X^n - 1$ 的根, 所以, $Q(X) \mid X^n - 1$ 。由于 P 和 Q 均为不可约的并且 $P \neq Q$, 所以, P 和 Q 互素。根据 Gauss 引理, 我们有如下在 $\mathbb{Z}[X]$ 中的等式:

$$X^n - 1 = P(X)Q(X)B(X).$$

在 $\mathbb{F}_l[X]$ 中考虑第一个等式, 我们有

$$Q(X)^l = P(X)A(X) \cdots \cdots \pmod{l}.$$

令 $R(X)$ 为 $P(X)$ 在 $\mathbb{F}_l[X]$ 中的一个不可约因子, 那么, $R \mid Q^l$, 从而, $R \mid Q$. 另外, 在第二个等式中, R^2 整除 $P \cdot Q$, 从而, $R^2 \mid X^n - 1$, 这与 $X^n - 1$ 在 $\mathbb{F}_l[X]$ 中是可分的矛盾。

例题 7.14 我们考虑有限域 \mathbb{F}_q , 其中, $q = p^l$. 现在来计算 \mathbb{F}_q 上的 n -次分圆域 $\mathbb{F}_q(\xi)$ 的次数 $[\mathbb{F}_q(\xi) : \mathbb{F}_q]$. 根据有限域的理论, $\text{Gal}(\mathbb{F}_q(\xi)/\mathbb{F}_q)$ 是循环群并且

$$\text{Gal}(\mathbb{F}_q(\xi)/\mathbb{F}_q) = \langle \sigma : x \mapsto x^q \rangle.$$

从而, $\text{Im}(\text{Gal}(\mathbb{F}_q(\xi)/\mathbb{F}_q) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times)$ 由 σ 的像生成, 它把 ξ 映射成 ξ^q . 从而, σ 在 $(\mathbb{Z}/n\mathbb{Z})^\times$ 中恰好是 $q \pmod{n}$. 特别地, $[\mathbb{F}_q(\xi) : \mathbb{F}_q]$ 恰好是 q 在 $(\mathbb{Z}/n\mathbb{Z})^\times$ 的阶。

例题 7.15 Galois 反问题 对任意的有限交换群 A , 存在数域 ${}^6K/\mathbb{Q}$, 使得 $\text{Gal}(K/\mathbb{Q}) \simeq A$. 特别地, 任意的有限交换群 A 都可以实现为 $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ 的商群。

根据有限生成交换群的分类定理, 存在 $d_1, \dots, d_s \in \mathbb{Z}_{\geq 2}$, 使得

$$A \simeq \prod_{i=1}^s \mathbb{Z}/d_i\mathbb{Z}$$

并且 $d_1 \mid d_2, d_2 \mid d_3, \dots, d_{s-1} \mid d_s$. 根据 Dirichlet 定理⁷, 对每个 $i = 1, \dots, s$, 我们选取素数 p_i , 使得 $p_i \equiv 1 \pmod{d_i}$. 令 $n = p_1 p_2 \cdots p_s$, 我们考虑 \mathbb{Q} 上的 n -次分圆域 $\mathbb{Q}(\xi)/\mathbb{Q}$, 其中 ξ 为 n -次本原单位根, 那么,

$$\text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^s (\mathbb{Z}/p_i\mathbb{Z})^\times \simeq \prod_{i=1}^s \mathbb{Z}/(p_i - 1)\mathbb{Z}.$$

根据 $d_i \mid p_i - 1$, $\mathbb{Z}/d_i\mathbb{Z}$ 是 $\mathbb{Z}/(p_i - 1)\mathbb{Z}$ 的商群:

$$1 \rightarrow d_i\mathbb{Z}/(p_i - 1)\mathbb{Z} \rightarrow \mathbb{Z}/(p_i - 1)\mathbb{Z} \rightarrow \mathbb{Z}/d_i\mathbb{Z} \rightarrow 1.$$

从而, A 是 $\text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ 的商群, 即有 $H \simeq \prod_{i=1}^s d_i\mathbb{Z}/(p_i - 1)\mathbb{Z}$, 使得 $\text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})/H \simeq A$. 此时, 根据 Galois 对应, $K = \mathbb{Q}(\xi)^H$ 的 Galois 群为 A .

7.5.5 循环扩张

给定 Galois 扩张 L/K . 如果 $\text{Gal}(L/K)$ 是循环群, 我们就称 L/K 是循环扩张; 如果 $\text{Gal}(L/K)$ 是交换群, 我们就称 L/K 是 **Abel 扩张**

引理 7.10 (特征的线性不相关性, E. Artin)

G 是群, K 是域, $\text{Funt}(G, K)$ 是 G 上 K -值函数的 K -线性空间, $\chi_1, \dots, \chi_k \in \text{Hom}(G, K^\times)$ 是群同态 (被称作是特征). 那么, χ_1, \dots, χ_k 在 $\text{Funt}(G, K)$ 中线性无关。



证明 对 k 进行归纳, 其中 $k = 1$ 是显然的. 假设命题对不超过 k 个特征成立, 现在考虑如下

⁶按定义, 数域就是 \mathbb{Q} 的有限扩张

⁷参见第八次作业问题 D

的线性关系：

$$a_1\chi_1(g) + \cdots + a_k\chi_k(g) + a_{k+1}\chi_{k+1}(g) = 0, \quad \forall g \in G,$$

其中, $a_1, \dots, a_{k+1} \in K$ 。由于 $\chi_k \neq \chi_{k+1}$, 我们选取 $h \in G$, 使得 $\chi_k(h) \neq \chi_{k+1}(h)$ 。在上述线性关系中把 g 替换成 gh , 利用 χ_i 均为群同态, 我们得到

$$a_1\chi_1(h)\chi_1(g) + \cdots + a_k\chi_k(h)\chi_k(g) + a_{k+1}\chi_{k+1}(h)\chi_{k+1}(g) = 0, \quad \forall g \in G.$$

对前一个线性关系乘以 $\chi_k(h)$ 并与上面这个等式相减, 我们得到

$$a_1(\chi_1(h) - \chi_k(h))\chi_1(g) + \cdots + a_{k-1}(\chi_{k-1}(h) - \chi_k(h))\chi_{k-1}(g) + a_{k+1}(\chi_{k+1}(h) - \chi_k(h))\chi_{k+1}(g) = 0, \quad \forall g \in G.$$

利用归纳假设, 这说明 $a_{k+1}(\chi_{k+1}(h) - \chi_k(h)) = 0$, 从而, $a_{k+1} = 0$ 。此时, 我们又回到了 k 个特征的情形, 利用归纳假设就可以完成证明。

引理 7.11 (Hilbert 90)

L/K 是次数为 n 的循环扩张, $\sigma \in \text{Gal}(L/K)$ 是生成元, $x \in L$ 。那么,

$$\begin{cases} N_{L/K}(x) = 1 & \Leftrightarrow \text{存在 } y \in L, \text{ 使得 } x = \frac{y}{\sigma(y)}; \\ \text{Tr}_{L/K}(x) = 0 & \Leftrightarrow \text{存在 } y \in L, \text{ 使得 } x = y - \sigma(y). \end{cases}$$



证明 假设 $\text{Gal}(L/K) = \langle \sigma \rangle = \{1, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$ 。

如果 $x = \frac{y}{\sigma(y)}$, 那么,

$$N_{L/K}(x) = \prod_{k=0}^{n-1} (\sigma^k(x)) = \frac{\prod_{k=0}^{n-1} (\sigma^k(y))}{\prod_{k=0}^{n-1} (\sigma^{k+1}(y))} = 1.$$

反之 (E. Artin), $N_{L/K}(x) = 1$, 即 $x\sigma(x)\cdots\sigma^{n-1}(x) = 1$ 。我们考虑 L 到自身的 K -线性映射:

$$\psi = \text{id} + x\sigma + (x\sigma(x))\sigma^2 + \cdots + (x\sigma(x)\cdots\sigma^{n-2}(x))\sigma^{n-1}.$$

这是 n 个特征的线性组合, 根据 Artin 引理, 存在 $y \in L$, 使得 $\psi(y) \neq 0$ 。我们计算 $\sigma(\psi(y))$:

$$\begin{aligned} \sigma(\psi(y)) &= \sigma(y) + \sigma(x)\sigma^2(y) + \sigma(x)\sigma^2(x)\sigma^3(y) \\ &\quad + \cdots + \sigma(x)\sigma^2(x)\cdots\sigma^{n-2}(x)\sigma^{n-1}(y) + \underbrace{\sigma(x)\sigma^2(x)\cdots\sigma^{n-1}(x)}_{=x^{-1}}y \\ &= x^{-1} [x\sigma(y) + x\sigma(x)\sigma^2(y) + x\sigma(x)\sigma^2(x)\sigma^3(y) + \cdots + x\sigma(x)\sigma^2(x)\cdots\sigma^{n-2}(x)\sigma^{n-1}(y) + y] \\ &= x^{-1}\psi(y). \end{aligned}$$

所以, $x = \frac{\psi(y)}{\sigma(\psi(y))}$ 。

如果 $x = y - \sigma(y)$, 那么,

$$\text{Tr}_{L/K}(x) = \sum_{k=0}^{n-1} (\sigma^k(x)) = \sum_{k=0}^{n-1} \sigma^k(y) - \sum_{k=0}^{n-1} \sigma^{k+1}(y) = 0.$$

反之, $\text{Tr}_{L/K}(x) = 0$, 即 $x + \sigma(x) + \cdots + \sigma^{n-1}(x) = 0$ 。由于 L/K 是可分的, 所以⁸,

$$\text{Tr}_{L/K} : L \times L \rightarrow K, (x_1, x_2) \mapsto \text{Tr}_{L/K}(x_1x_2),$$

⁸参考第七次作业的题目 A

是非退化的。特别地, 存在 $z \in L$, 使得 $\text{Tr}_{L/K}(z) \neq 0$ 。令

$$y = x\sigma(z) + (x + \sigma(x))\sigma^2(z) + \cdots + (x + \sigma(x) \cdots + \sigma^{n-2}x)\sigma^{n-1}(z).$$

那么,

$$\begin{aligned}\sigma(y) &= \sigma(x)\sigma^2(z) + (\sigma(x) + \sigma^2(x))\sigma^2(z) + \cdots + \underbrace{(\sigma(x) + \sigma^2(x) \cdots + \sigma^{n-1}x)}_{=-x} z \\ &= -xz + (x + \sigma(x))\sigma^2(z) + (x + \sigma(x) + \sigma^2(x))\sigma^2(z) + \cdots \\ &\quad - x(\sigma^2(z) + \sigma^2(z) + \cdots + \sigma^{n-1}(z)) \\ &= y - x(z + \sigma(z) + \sigma^2(z) + \cdots + \sigma^{n-1}(z)) = y - x\text{Tr}_{L/K}(z).\end{aligned}$$

从而, $x = \frac{1}{\text{Tr}_{L/K}(z)}(y - \sigma(y))$ 。

定理 7.10 (Kummer)

K 是域并且 $|\mu_n(K)| = n$ (即 $X^n - 1$ 可分并且 K 包含所有 n -次单位根), L/K 是有限扩张。那么, 以下两个叙述等价:

- 1) L/K 是 n 次循环扩张;^a
- 2) 存在 $a \in K$, 对任意的 $d > 1, d | n$, $a \notin K^d$, 使得 L 是 $X^n - a$ 在 K 上的分裂域。此时, $X^n - a$ 是 $K[X]$ 上的不可约多项式并且 $L = K(\alpha)$, 其中, α 是该多项式的某个 (任意) 根。

^a按定义, 循环扩张是 Galois 扩张。



证明 首先证明 1) \Rightarrow 2)。假设 σ 是 $\text{Gal}(L/K)$ 的生成元, ξ 是 K 中的一个 n -次本原单位根。由于 $\text{Tr}_{L/K}(\xi^{-1}) = 1$, 根据 Hilbert 90, 存在 $\alpha \in L$, 使得 $\xi^{-1} = \frac{\alpha}{\sigma(\alpha)}$, 从而,

$$\sigma(\alpha) = \xi \cdot \alpha \quad \sigma^k(\alpha) = \xi^k \cdot \alpha, \quad k = 0, 1, \dots, n-1.$$

特别地, 由于 ξ 是本原的, 所以, 以上 $\sigma^k(\alpha)$ 两两不同。以上等式应该被视作是 $\text{Gal}(L/K)$ 在根上的作用。此时,

$$P(X) = \prod_{k=0}^{n-1} (X - \sigma^k(\alpha)) \in K[X]$$

是 α 的不可约多项式, 我们还有

$$P(X) = \prod_{k=0}^{n-1} (X - \xi^k \alpha) = X^n - \alpha^n = X^n - a.$$

最终, 我们说明 $a \notin K^d$, 其中, $1 < d | n$ 。否则, $b^d = a$, 其中 $b \in K$ 。从而,

$$P(X) = (X^{\frac{n}{d}})^d - b^d = (X^{\frac{n}{d}} - b)Q(X)$$

是可约的, 矛盾。

其次证明 2) \Rightarrow 1)。我们现在假设存在 $a \in K$, 对任意的 $d > 1, d | n$, $a \notin K^d$, 使得 L 是 $X^n - a$ 在 K 上的分裂域。(将证明 $X^n - a$ 不可约)

首先, L/K 是正规扩张; 其次, 令 α 为 $X^n - a$ 在 L 中的一个根, 那么, 它的所有根恰好是 $\{\alpha, \xi\alpha, \dots, \xi^{n-1}\alpha\}$, 其中, ξ 是 K 中的一个 n -次本原单位根。 $|\mu_n(K)| = n$, 它们是一个可分多

项式的根, 从而, L/K 是可分扩张。所以, L/K 是 Galois 扩张。另外, 考虑 $\text{Gal}(L/K)$ 在以上多项式的根上的作用, 我们得到单的群同态:

$$\text{Gal}(L/K) \longrightarrow \mu_n(K), g \mapsto \zeta_g, \text{ 其中 } g(\alpha) = \zeta_g \alpha.$$

特别地, 这表明 $\text{Gal}(L/K)$ 是循环群。以下, 我们证明

$$X^n - a = \prod_{k=0}^{n-1} (X - \xi^k \alpha)$$

是不可约的。据此, 因为 $\text{Gal}(L/K)$ 在根上的作用是传递的, 我们就有 $\text{Gal}(L/K) \simeq \mu_n(K)$ 是 n 阶循环群。假设 $Q|P$ 是 P 的一个首一的因子, 那么, $Q(X) = (X - \xi^{i_1} \alpha) \cdots (X - \xi^{i_m} \alpha)$, 其中, $1 \leq m < n$ 。从而, (因为 $\xi \in K$)

$$\xi^{i_1} \alpha \cdot \xi^{i_2} \alpha \cdots \xi^{i_m} \alpha \in K \Rightarrow \alpha^m \in K.$$

由于 $\alpha^n \in K$, 所以, 对于 $d = (n, m) < n$, 我们有 $\alpha^d \in K$ 。此时, $d | n$ 。所以, $a = \alpha^n = (\alpha^d)^{\frac{n}{d}} \in K^{\frac{n}{d}}$, 矛盾。

7.5.6 尺规作图

根据 Wantzel 定理, $x \in \mathbb{R}$ 是尺规可作的当且仅当存在有限个域扩张

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_m \subset \mathbb{R}$$

使得 $[K_i : K_{i-1}] = 2$ ($i = 1, \dots, m$) 并且 $x \in K_m$ 。通过添加 i 以及考虑 z 的实部和虚部, 我们知道 $z \in \mathbb{C}$ 是尺规可作的当且仅当存在有限个域扩张

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_m \subset \mathbb{C}$$

使得 $[K_i : K_{i-1}] = 2$ ($i = 1, \dots, m$) 并且 $z \in K_m$ 。通过考虑 z 在 \mathbb{Q} 上的最小多项式 $P(X)$ 以及域同构 $\mathbb{Q}[X]/(P) \simeq \mathbb{Q}(z) \subset K_m$, 我们知道 $\deg(P)$ 是 2 的幂。

定理 7.11

$z \in \mathbb{C}$ 是代数数 (即 z 在 \mathbb{Q} 上是代数的), $P(X) \in \mathbb{Q}[X]$ 为其极小多项式。那么, z 是尺规可作的当且仅当 $P(X)$ 在 \mathbb{Q} 上的分裂域的次数为 2 的幂。



证明 令 L 为 z 的分裂域, z_1, \dots, z_n 为 P 在 L 中所有的根。

假设 z 是尺规可作的, 那么存在域扩张的序列

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_m \subset \mathbb{C},$$

使得 $[K_i : K_{i-1}] = 2$ ($i = 1, \dots, m$) 并且 $z \in K_m$ 。选取 Galois 扩张 M/\mathbb{Q} , 使得 $M \supset K_m \cup L$ 。对每个根 z_j , 存在 $g \in \text{Gal} M/\mathbb{Q}$, 使得 $g(z) = z_i$, 那么, 我们有域扩张的序列

$$\mathbb{Q} = g(K_0) \subset g(K_1) \subset \cdots \subset g(K_m) \subset \mathbb{C},$$

使得 $[g(K_i) : g(K_{i-1})] = 2$ ($i = 1, \dots, m$) 并且 $g(z) = z_j \in K_m$ 。所以, P 的每个根都是尺规可作的。此时, 由于尺规可作的复数是 \mathbb{C} 的子域而 $L = \mathbb{Q}(z_1, \dots, z_n)$, 所以, 每个 L 中的元素都是尺规可作的。特别地, 由于 L/\mathbb{Q} 是有限可分扩张, 所以存在 $\xi \in L$, 使得 $L = \mathbb{Q}(\xi)$ 。由于 ξ 是尺规

可作的, 所以, $[L:\mathbb{Q}]$ 为 ξ 的极小多项式的次数, 从而是 2 的幂。

反之, $[L:\mathbb{Q}] = 2^m$, 从而, $\text{Gal}(L/\mathbb{Q})$ 是 2-群。根据以下引理, 存在滤链 $\text{Gal}(L/\mathbb{Q}) = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = 1$, 使得

$$G_{i-1}/G_i \simeq \mathbb{Z}/p\mathbb{Z}, \quad i = 1, \dots, n.$$

根据 Galois 对应定理, 存在中间域 $\mathbb{Q} = M_0 \subset M_1 \subset \cdots \subset L$, 使得 $[M_i:M_{i-1}] = 2$, 其中, $i = 1, \dots, n$ 。根据 Wantzel 的定理, 每个 M_i 中的元素都是尺规可作的。

引理 7.12

G 是 p -群, 其中 $|G| = p^n$ 。那么, 存在滤链 $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = 1$, 使得

$$G_{i-1}/G_i \simeq \mathbb{Z}/p\mathbb{Z}, \quad i = 1, \dots, n.$$



证明 我们对 n 进行归纳。 $n=1$ 时, 命题是平凡的。假设命题对 $< n$ 的整数都成立, 当 $|G| = p^n$ 时, 由于 p -群的中心非平凡, 我们取 $G_{n-1} < Z(G)$, 使得 $G_{n-1} \simeq \mathbb{Z}/p\mathbb{Z}$ 。我们还有 $G_{n-1} \triangleleft G$ 。那么, G/G_{n-1} 是阶为 p^{n-1} 群。根据归纳假设, 我们有 G 的子群 G_i , 其中, $i = 1, \dots, n-2$, 使得

$$G/G_{n-1} \triangleright G_1/G_{n-1} \triangleright \cdots \triangleright G_{n-2}/G_{n-1} \triangleright 1,$$

并且

$$G_i/G_{n-1}/G_{i+1}/G_{n-1} \simeq \mathbb{Z}/p\mathbb{Z}.$$

所以, $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = 1$ 为所求的滤链。

令 $F_m = 2^{2^m} + 1$, 其中, $m = 1, 2, \dots$ 。如果 m 使得 F_m 是素数, 我们就称 F_m 为 **Fermat 素数**。我们可以计算

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537.$$

它们都是素数而 $641 \mid F_5$ 。

定理 7.12

正 n 边形是尺规可作的当且仅当 n 形如 $2^m F_{l_1} \cdots F_{l_k}$, 其中, $l_1 < \cdots < l_k$ 。



证明 如果正 n 边形可作, 由于我们可以二等分已知角, 从而正 $2n$ 边形也可作; 如果我们可以做正 n 边形和正 m 边形, 其中, n 和 m 互素, 那么, 我们可以做正 nm 边形: 根据 Bézout 定理, 存在 $a, b \in \mathbb{Z}$, 使得 $an + bm = 1$, 从而, $\frac{a}{m} + \frac{b}{n} = \frac{1}{nm}$ 。据此,

$$e^{\frac{1}{mn}2\pi} = e^{\frac{a}{m}2\pi} \cdot e^{\frac{b}{n}2\pi}$$

也是尺规可作的。

根据上面的讨论, 我们只要对奇素数 p 证明:

1) 正 p 边形尺规可作当且仅当 p 是 Fermat 素数。

2) p 是 Fermat 素数, 正 p^2 -边形不是尺规可作的。

正 p 边形尺规可作当且仅当 $e^{\frac{2\pi i}{p}}$ 是尺规可作, 它的分裂域的次数为 $p-1$ 。从而, 只能是 p 为 Fermat 素数时, 正 p 边形尺规可作。

另外, 正 p^2 边形尺规可作当且仅当 $e^{\frac{2\pi i}{p^2}}$ 是尺规可作, 它的分裂域的次数为 $\varphi(p^2) = p(p-1)$, 这显然不是 2 的幂, 从而, 正 p^2 -边形不是尺规可作的。

例题 7.16 我们考虑 $P(X) = X^4 + X^3 - X^2 - X + 1$ 在 \mathbb{Q} 上的分裂域 L/\mathbb{Q} 。

首先说明 $P(X)$ 是 $\mathbb{Q}[X]$ 上的不可约多项式。我们利用 $\text{mod } 2$ 的方法。在 $\mathbb{F}_2[X]$ 中, $P(X)$ 对应着多项式 $\bar{P}(X) = X^4 + X^3 + X^2 + X + 1$ 。首先, \bar{P} 在 \mathbb{F}_2 中没有根, 如果 $P(X)$ 可约, 那么, 它的根必然在 \mathbb{F}_4 中。令 $\mathbb{F}_4 = \mathbb{F}_2(a)$, 那么, a 的极小多项式为 $X^2 + X + 1$, 从而, $\mathbb{F}_4 = \{0, 1, a, a+1\}$ 。通过直接计算, 我们知道 $\bar{P}(a) = a+1, \bar{P}(a+1) = a$, 从而, P 是不可约的。

由于 $P(X)$ 是实系数多项式, 所以, 在 $\mathbb{C}[X]$ 中, 它可以被写成

$$P(X) = (X^2 + aX + b)(X^2 + \bar{a}X + \bar{b}).$$

据此,

$$\begin{cases} a + \bar{a} = 1, \\ a\bar{a} + b + \bar{b} = -1, \\ a\bar{b} + b\bar{a} = -1, \\ b\bar{b} = 1. \end{cases}$$

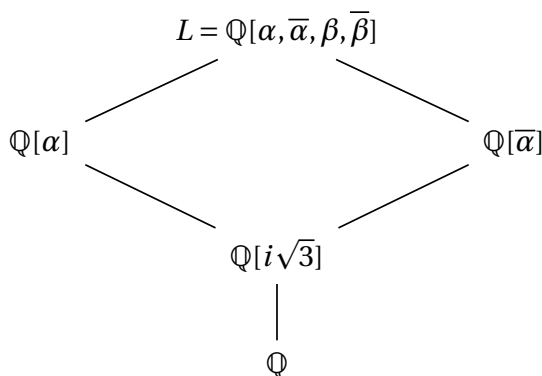
当 $b = \bar{b} = -1$ 是, 第一个与第三个方程一样, 此时, 我们可以解出来 a , 从而,

$$P(X) = (X^2 + \frac{1+i\sqrt{3}}{2}X - 1)(X^2 + \frac{1-i\sqrt{3}}{2}X - 1).$$

任意选取 α 为 $P(X)$ 的根。根据以上因式分解, $\frac{1+i\sqrt{3}}{2} \in \mathbb{Q}(\alpha)$, 即 $i\sqrt{3} \in \mathbb{Q}(\alpha)$, 从而, 我们有域扩张

$$\mathbb{Q} \longrightarrow \mathbb{Q}(i\sqrt{3}) \longrightarrow \mathbb{Q}(\alpha)$$

不妨假设 α 是 $X^2 + \frac{1+i\sqrt{3}}{2}X - 1$ 的根而另一个根是 β , 那么, $X^2 + \frac{1+i\sqrt{3}}{2}X - 1$ 的根是 $\bar{\alpha}$ 和 $\bar{\beta}$ 。此时, 我们有域扩张的图表:



这表明 $[L:\mathbb{Q}] = 8$, 从而, $P(X)$ 的所有根都是尺规可作的。

以下我们计算 $\text{Gal}(L/\mathbb{Q})$ 。注 将 \mathfrak{S}_4 视作是在 $\{1, 2, 3, 4\}$ 上作用的变换群, $H < \mathfrak{S}_4$ 并且 H 在 $\{1, 2, 3, 4\}$ 上的作用是传递的, 我们要找出所有可能的 H 。很显然, $4 \mid |H|$ 并且 $|H| \mid 24$, 所以, $|H| = 4, 8, 12$ 或者 24 。

- $|H| = 24$, 从而, $H = \mathfrak{S}_4$ 。

- $|H| = 12$, 我们知道 $H = \mathfrak{A}_4$ 。

实际上, 该群的指标为 2, 从而 $H \triangleleft \mathfrak{S}_4$ 。特别地, H 中不能包含任何的对换, 否则通过共轭它包含所有对换, 从而 $H = \mathfrak{S}_4$ 。所以, H 中包含所有的 $(a, b)(c, d)$ 型置换, 从而包含 \mathfrak{A}_4 。

- $|H| = 12$, 我们知道 $H = \mathfrak{A}_4$ 。

实际上, 该群的指标为 2, 从而 $H \triangleleft \mathfrak{S}_4$ 。特别地, H 中不能包含任何的对换, 否则通过共轭它包含所有对换, 从而 $H = \mathfrak{S}_4$ 。所以, H 中包含所有的 $(a, b)(c, d)$ 型置换, 从而包含 \mathfrak{A}_4 。

- $|H| = 8$, 那么, $H = \mathfrak{D}_4$ 。

此时, H 为某个 \mathfrak{S}_4 的 Sylow 2-子群。由于所有的 Sylow 2-子群同构, 所以, 我们只要给出一个 \mathfrak{S}_4 的 Sylow 2-子群的结构即可。考虑正 4 边形的对称群 \mathfrak{D}_4 作用在 4 个顶点集上, 我们得到 $\mathfrak{D}_4 \hookrightarrow \mathfrak{S}_4$ 。

- $|H| = 4$, 那么, $H = \mathbb{Z}/4\mathbb{Z}$ 或者 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 。

根据上述讨论, 同构共轭, H 落在 Sylow 2-子群 \mathfrak{D}_4 中。它的传递的 4 阶子群为 $\mathbb{Z}/p\mathbb{Z}$ (由旋转 $\frac{\pi}{2}$ 来实现) 或者 $\langle (1, 2)(3, 4), (1, 4)(2, 3) \rangle$ 。

根据以上注记, $P(X) = X^4 + X^3 - X^2 - X + 1$ 在 \mathbb{Q} 上分裂域的 Galois 群为 \mathfrak{D}_4 。

7.5.7 多项式的根式解

在这一节中, 我们只讨论特征为 0 的域 (为了让叙述变得简单并且这已经是大家最关心的情形了)。假设 K 是这样的一个域, $P \in K[X]$, 如果 P 在 \bar{K} 的每个根都有有限步得到并且每一步都是对前面步骤已经得到数 (包括 K) 进行一次加减乘除或者开某个 n 次方的操作, 我们就说 P 是**根式可解的**。类似于尺规作图问题, 我们可以用域的语言来叙述:

定义 7.10

假设 K 的特征为零, L/K 是域扩张。如果存在中间域的序列:

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = L$$

使得对任意的 $i = 1, \dots, m$, 存在 $x_i \in K_i$ 以及正整数 d_i , 使得 $K_i = K_{i-1}(x_i)$ 并且 $x_i^{d_i} \in K_{i-1}$, 我们就称 L/K 是**根式扩张**。换言之, L 是通过对 K 添加有限个 d_i 次方根而得到的。

对于多项式 $P(X) \in K[X]$, 如果存在根式扩张 L/K , 使得 P 在 L 中分裂 (成 1 次多项式之积), 我们就称 $P(X)$ 在 K 上有**根式解**。



注 给定域扩张 L/K 以及中间域 $K \subset M \subset L$, 如果 L/M 和 M/K 是根式扩张, 那么, L/K 也是。

引理 7.13 (技术性引理: 过渡到 Galois 扩张)

域 K 的特征为零, L/K 是根式扩张, 那么, L 在 \bar{K} 中的正规闭包 N 也是 K 的根式扩张。

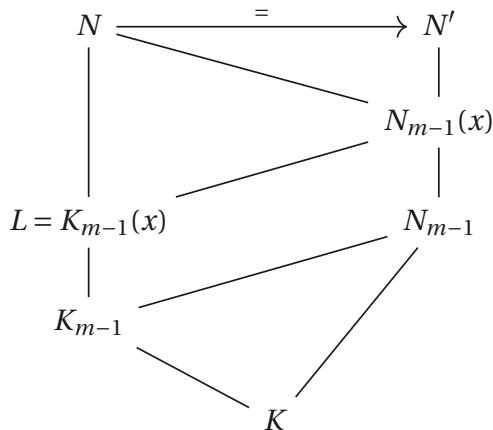


注 L 由 K 添加上 $P(X) \in K[X]$ 的某些根生成。我们把 $P(X)$ 的所有根都添加到 K 中就得到了 L 在 \bar{K} 中的正规闭包 N 。

证明 L/K 是根式扩张, 所以存在如果存在中间域的序列:

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = L$$

使得对任意的 $i = 1, \dots, m$, 存在 $x_i \in K_i$ 以及正整数 d_i , 使得 $K_i = K_{i-1}(x_i)$ 并且 $x_i^{d_i} \in K_{i-1}$ 。我们对 m 进行归纳。当 $m = 0$ 时, 命题是显然的。假设命题对 $m-1$ 成立。



我们选取 $x \in L$, 使得 $L = K_{m-1}(x)$ 并且 $x^d \in K_{m-1}$; 令 N_{m-1} 为 K_{m-1} 在 \bar{K} 中的正规闭包; 令 N 为 $K_m = L$ 在 \bar{K} 中的正规闭包。由于 $x \in L \subset N$, $K_{m-1} \subset L \subset N$, 从而, $N_{m-1}(x) \subset N$ 。令 N' 为 $N_{m-1}(x)$ 的正规闭包, 从而, $N = N'$ 。根据归纳假设, N_{m-1}/K 是根式扩张, 只要证明 N'/N_{m-1} 是根式扩张即可。由于 $N_{m-1}(x)/N_{m-1}$ 是根式扩张 (因为 $x^d \in N_{m-1}$), 只要说明 $N'/N_{m-1}(x)$ 是根式扩张: 根据正规扩张的构造, N' 可以看作是从 $N_{m-1}(x)$ 出发, 逐次加入 x 的极小多项式的根 x_1, \dots, x_l 。由于 $x^d \in N_{m-1}$, 从而, 每次加入的 $x_i^d \in N_{m-1}$, 这当然是根式扩张。

定理 7.13 (Galois)

域 K 的特征为零, L/K 是有限的 Galois 扩张。那么, 如下两个命题等价:

- 1) 存在 K 的根式扩张 M , 使得 $K \subset L \subset M$;
- 2) $\text{Gal}(L/K)$ 是可解群。



我们首先做一些准备工作: 仿照 Kummer 理论, K 是域并且 $|\mu_n(K)| = n$, L 是 $X^n - a$ 在 K 上的分裂域。那么, $\text{Gal}(L/K)$ 是 $\mu_n(K)$ 的子群, 它通过

$$\text{Gal}(L/K) \longrightarrow \mu_n(K), g \mapsto \zeta_g, \text{ 其中 } g(\alpha) = \zeta_g \alpha.$$

来实现。

注 可解群的子群和商群都是可解的。

对于群 G 以及其正规子群 $N \triangleleft G$, 如果 N 和 G/N 可解, 那么 G 也可解。

有限可解群 G 有如下两个等价定义:

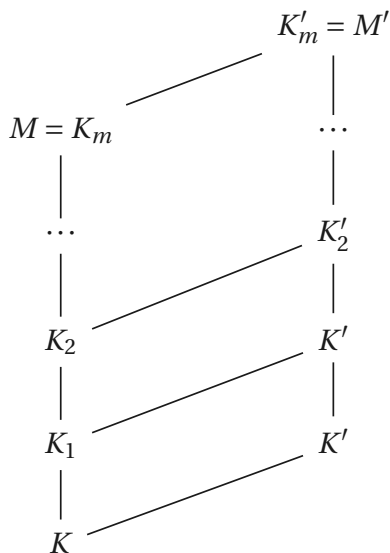
- G 有滤链 $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = 1$, 使得 G_{i+1} 是 G_i 的正规子群并且 G_i/G_{i+1} 交换, 其中 $0 \leq i \leq n-1$ 。
- G 有滤链 $G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_m = 1$, 使得 H_{i+1} 是 H_i 的正规子群并且 H_i/H_{i+1} 是循环群, 其中 $0 \leq i \leq m-1$ 。

证明 1) \Rightarrow 2)。我们选取 $L \subset M$, 使得 M 为 L 的正规闭包, 此时, M/K 也是根式扩张。只要证

明 $\text{Gal}(M/K)$ 是可解群即可, 因为 $\text{Gal}(L/K)$ 为其商群。我们选取

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = M,$$

其中, $K_i = K_{i-1}(x_i)$ 并且 $x_i^{d_i} \in K_{i-1}$, $1 \leq i \leq m$ 。为了使用 Kummer 理论的想法, 令 K'_i 为 K_i 上添加上 (在代数封闭域 \bar{K} 中) $X^{d_1 d_2 \cdots d_m} - 1$ 的所有根, 我们就得到如下扩张的示意图。



很明显, 我们仍然有 $K'_i = K'_{i-1}(x_i)$ 并且 $x_i^{d_i} \in K'_{i-1}$, 所以, $M' = K'_m$ 仍然是 K' 上的根式扩张。另外, K'_m/K 是 Galois 扩张: K_m/K 是 Galois 扩张, 所以, K_m 是 K 上某个多项式 $P(X)$ 的分裂域, 从而, K'_m 是 K 上多项式 $P(X)$ 和 $X^{d_1 d_2 \cdots d_m} - 1$ 的分裂域, 从而是 Galois 扩张。考虑如下的正合序列:

$$1 \rightarrow \text{Gal}(M'/K') \rightarrow \text{Gal}(M'/K) \rightarrow \text{Gal}(K'/K) \rightarrow 1.$$

根据分圆域的理论, $\text{Gal}(K'/K)$ 是交换群。所以, 只要证明 $\text{Gal}(M'/K')$ 是可解群即可。

以上的讨论使得我们可以假设 K 中含有所有的 $d_1 d_2 \cdots d_m$ 次单位根, 从而可以使用 Kummer 理论 (以上注记)。此时, 每个 K_i/K_{i-1} 都是循环扩张 (K_i 现在是添加了 $X^{d_i} - x_i^{d_i}$ 的所有根), 通过考虑 $K_{i-1} \subset K_i \subset M$, 我们知道 $\text{Gal}(M/K_i)$ 是 $\text{Gal}(M/K_{i-1})$ 的正规子群。如果令 $G_i = \text{Gal}(M/K_i)$, 我们就得到滤链:

$$G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset 1,$$

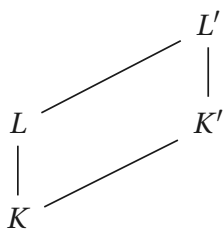
并且

$$G_{i-1}/G_i = \text{Gal}(M/K_{i-1})/\text{Gal}(M/K_i) \simeq \text{Gal}(K_i/K_{i-1})$$

是循环群。从而, $G_0 = \text{Gal}(M/K)$ 是可解群。

2) \Rightarrow 1)。此时, $\text{Gal}(L/K)$ 是可解群, 我们要构造根式扩张 M/K , 使得 $L \subset M$ 。为了使用 Kummer 理论的想法, 令 K' 和 L' 分别为 K 和 L 添加上 (在代数封闭域 \bar{K} 中) $[L:K]!$ 次的所有

单位根所得到的域，即



与之前的讨论类似，我们知道 L'/K 是 Galois 扩张。另外， L/K 是 Galois 扩张，从而， $\text{Gal}(L'/L) \triangleleft \text{Gal}(L'/K)$ 。另外，分圆扩张 L'/L 是 Abel 扩张而 $\text{Gal}(L'/K)$ 是可解群，从而， $\text{Gal}(L'/K)$ 是可解群，从而，其子群 $\text{Gal}(L'/K')$ 也是可解群。另外， $[L':K'] \leq [L:K]$ ：假设 $L = K(\alpha)$ ， $P(X)$ 为 α 在 K 上的极小多项式，那么， $L' = K'(\alpha)$ 而 α 在 K' 上的极小多项式的次数不超过 $\deg(P)$ 。从而， K' 包含了所有 $[L':K']!$ 次单位根。由于 K' 为 K 添加了一个本原单位根，所以，只要对 L'/K' 证明命题就可以了。

综上所述，我们可以假设 K 包含了所有的 $[L:K]!$ 次单位根。由于 $\text{Gal}(L/K)$ 可解，所以存在滤链

$$\text{Gal}(L/K) = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{m-1} \triangleright G_m = 1,$$

使得 G_{i-1}/G_i 是循环群，其中， $i = 1, 2, \dots, m$ 。令 $K_i = L^{G_i}$ ，那么，我们有域扩张的序列：

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = L,$$

由于 $G_1 \triangleleft G_0$ ，所以， K_1/K_0 是 Galois 扩张；由于 $G_2 \triangleleft G_1$ ，所以， K_2/K_1 是 Galois 扩张；以此类推， K_i/K_{i-1} 为 Galois 扩张，它们的 Galois 群为 $[K_i:K_{i-1}]$ 次的，其中根， $[K_i:K_{i-1}] \mid [L:K]$ ，从而， K_{i-1} 中包含所有的 $[K_i:K_{i-1}]$ 次单位根。根据 Kummer 理论，存在 $x_i \in K_i$ ，使得 $K_i = K_{i-1}(x_i)$ 并且 $x_i^{[K_i:K_{i-1}]} \in K_{i-1}$ 。这表明， L/K 是根式扩张。

至此，我们完整地证明了 Galois 的定理。

例题 7.17 对于 $X^5 - 6X + 3 \in \mathbb{Q}[X]$ ，其分裂域的 Galois 群为 \mathfrak{S}_5 ，这是不可解群。从而，方程 $X^5 - 6X + 3 = 0$ 在 \mathbb{Q} 上没有根式解。

7.6 mod p 的理论

我们首先回忆 Noether 环的定义：这是每个理想都是有限生成的环。与之等价的定义方式是它满足上升理想链的稳定条件，即对环 A 中任意的理想链

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$$

存在 $n_0 \geq 1$ ，使得当 $n \geq n_0$ 时， $I_n = I_{n_0}$ 。

我们还证明了 Noether 环上有限生成模的子模是有限生成的。

定义 7.11

A 是环, M 是 A -模。如果下述两个等价条件之一成立:

- 1) M 的每个子模都是有限生成;
- 2) M 满足上升子模的稳定条件, 即对 M 中任意的子模链

$$M_1 \subset M_2 \subset \cdots \subset M_n \subset \cdots$$

存在 $n_0 \geq 1$, 使得当 $n \geq n_0$ 时, $M_n = M_{n_0}$ 。

我们就称 M 是 **Noether 模**。



注 以上等价性的证明和 Noether 环情形的证明一致, 这里不再赘述。

引理 7.14

给定 A -模的正合列

$$0 \rightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \rightarrow 0,$$

那么, M 是 Noether 模等价于 M' 和 M'' 均为 Noether 模。



证明 假设 M 是 Noether 模。每个 M' 的子模都是 M 的子模, 从而是有限生成的; 作为 M 的商模, 每个 M'' 中的上升子模序列都可以提升为 M 中的上升子模序列, 从而, 在 M 中稳定, 进而在 M'' 中稳定。

假设 M' 和 M'' 为 Noether 模。 N 为 M 的子模, 那么, 在 $M'' = M/M'$ 中, N 对应着 $N/N \cap M'$ 。根据 M'' 的 Noether 性, 存在 $x_1, \dots, x_k \in N$, 使得 $\{x_i + M'\}_{i \leq k}$ 生成了 $N/N \cap M'$; 根据 M' 的 Noether 性, 存在 $y_1, \dots, y_l \in N \cap M'$, 使得 $\{y_j\}_{j \leq l}$ 生成了 $N \cap M'$ 。从而, 对任意的 $z \in N$, 利用 $\{x_i + M'\}_{i \leq k}$, 存在 $a_i \in A$, 使得 $z - \sum_{i \leq k} a_i x_i \in M'$, 从而, $z - \sum_{i \leq k} a_i x_i \in M' \cap N$; 再利用 $\{y_j + M'\}_{j \leq l}$, 我们就有 $b_j \in A$, 使得

$$z - \sum_{i \leq k} a_i x_i = \sum_{j \leq l} b_j y_j.$$

这表明 $\{x_i\}_{i \leq k} \cup \{y_j\}_{j \leq l}$ 生成了 N , 所以, M 是 Noether 模。

推论 7.11

Noether 环上的有限生成模是 Noether 模。



证明 A 是 Noether 环。按定义, 将 A 视作是 A -模, 那么, A 是 Noether 模。考虑自然的正合列

$$0 \rightarrow A \rightarrow A \oplus A^n \rightarrow A^n \rightarrow 0,$$

利用上述引理对 n 进行归纳就说明了 A^n 是 Noether 模。每个有限生成的 A -模都是某个 A^n 的商模, 根据上述引理, 这是 Noether 模。

7.6.1 环的整扩张

给定环 B 及其子环 $A \subset B$, 我们也说 B 是 A 的**扩张**。对任意的 $x \in B$, 如果存在首一的多项式 $P(X) \in A[X]$, 使得 $P(x) = 0$, 我们就称 x 在 A 上是**整的**或者说它是 A 上的**整元素**。

命题 7.14

对 $x \in B$, $A[x] = \{P(x) \mid P(X) \in A[X]\} \subset B$ 显然是 A -模。那么, 如下三个叙述是等价的:

- 1) x 在 A 上是整的;
- 2) $A[x]$ 是有限生成模;
- 3) 存在有限生成的 A -子模 $M \subset B$, 使得 $1 \in M$ 并且 $x \cdot M \subset M$ 。



证明 $1) \Rightarrow 2)$: 假设 $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$, 其中, $a_i \in A$ 。那么, 对任意的 $y \in A[x]$, 凡是它含有 x 的比 $n-1$ 次更高的次幂, 我们就用 $x^n = -(a_{n-1}x^{n-1} + \cdots + a_1x + a_0)$ 进行替换, 从而, $1, x, \cdots, x^{n-1}$ 生成了 $A[x]$ 。

$2) \Rightarrow 3)$ 是显然的; 现在证明 $3) \Rightarrow 1)$ 。假设 $x_1, \cdots, x_n \in M$ 生成了 M , 那么, 对每个 $i \leq n$, $x \cdot x_i \in M$ 。从而, 存在 a_{ij} , 其中, $j \leq n$, 使得

$$x \cdot x_i = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n.$$

令 $A = (a_{ij}) \in \mathbf{M}_n(A)$ 为 $n \times n$ 的 A -系数矩阵, 那么,

$$(x \cdot \mathbf{I} - A) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0.$$

左右两边乘以 $(x \cdot \mathbf{I} - A)$ 的伴随矩阵 $(x \cdot \mathbf{I} - A)^*$, 我们得到

$$(x \cdot \mathbf{I} - A)^* (x \cdot \mathbf{I} - A) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \det(x \cdot \mathbf{I} - A) \cdot \mathbf{I} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0.$$

由于 $1 \in M$, 我们知道 $\det(x \cdot \mathbf{I} - A) = 0$ 这就给出了 x 所满足的代数方程 (首一)。

推论 7.12

给定环的扩张 $A \subset B$, 如果 $x, y \in B$ 在 A 上是整的, 那么, $A[x, y]$ 是有限生成 A -模。特别地, $x \pm y$ 和 $x \cdot y$ 在 A 上也是整的。



证明 $x, y \in B$ 在 A 上是整的, 从而, 存在 $m, n \geq 1$, 使得

$$x^n = a_{n-1}x^{n-1} + \cdots + a_1x + a_0, \quad y^m = b_{m-1}y^{m-1} + \cdots + b_1y + b_0,$$

其中, $a_i, b_j \in A$ 。通过以上关系, 我们总可以将 x^n 和 y^m 替换为较小的次数, 从而, $\{x^i y^j \mid 0 \leq i \leq n, 0 \leq j \leq m\}$ 生成了 $A[x, y]$ 。根据以上命题, $A[x, y]$ 中的每个元素 z 都满足 $z \cdot A[x, y] \subset A[x, y]$, 从而是整的。

注 利用同样的证明, 以上结论可以加强为: 如果 $x_1, \cdots, x_k \in B$ 在 A 上是整的, 那么, $A[x_1, \cdots, x_k]$ 是有限生成 A -模。

根据推论, 我们有如下定义

定义 7.12

给定环的扩张 $A \subset B$, 如下集合

$$\overline{A} := \{x \in B \mid x \text{ 在 } A \text{ 上是整的}\}$$

是 B 的子环并且 $A \subset \overline{A}$ 。我们称 \overline{A} 为 A 在 B 中的整闭包。如果 $\overline{A} = B$, 我们就称 B 在 A 上是整的。

如果 A 是整环, $K = \text{Frac}(A)$ 并且 A 在 K 中的整闭包是 A , 我们就称 A 是整闭的。

**引理 7.15**

给定环的扩张 $A \subset B \subset C$, 如果 B 在 A 上是整的, C 在 B 上是整的, 那么, C 在 A 上是整的。



证明 对任意的 $x \in C$, 存在 $b_1, \dots, b_{n-1} \in B$, 使得

$$x^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0 = 0.$$

根据以上引理, $A[b_0, \dots, b_{n-1}]$ 为有限生成的 A -模。利用上述关系, $A[b_0, \dots, b_{n-1}, x]$ 仍然为有限生成的 A -模, 从而, x 在 A 上是整的。

引理 7.16

A 是唯一分解整环, 那么, A 是整闭的。



证明 令 $x = \frac{b}{a} \in \text{Frac}(A)$, 其中, $(a, b) = 1$ 。假设存在 a_1, \dots, a_{n-1} , 使得

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0 \Rightarrow b^n = -(a_{n-1}ab^{n-1} + \dots + a_1a^{n-1}b + a_0a^n).$$

以上, 我们在第一个方程左右两边同时乘了 a^n 。令 p 为 a 的一个不可约因子 (如果存在的话), 那么, p 整除方程右边, 从而, p 整除 b^n 。这表明, $p \mid b$, 这和 $(a, b) = 1$ 矛盾。从而, $a \in A^\times$, 所以, $x \in A$ 。

7.6.2 数域中的整元素

从此往后, 我们几乎之下如下的场合下讨论整扩张:

$$\begin{array}{ccc} B & \text{----} & L \\ \vdots & & \vdots \\ A & \text{----} & K \end{array}$$

A 是整环, $K = \text{Frac}(A)$ 为其分式域, L/K 为代数扩张, B 为 A 在 L 中的整闭包。**注** 我们有 $(A^\times)^{-1}B = L$ 。

实际上, 对任意的 $x \in L$, 根据 L/K 的代数性, 存在 $a_i, b_i \in A$, 使得

$$x^n + \frac{a_{n-1}}{b_{n-1}}x^{n-1} + \dots + \frac{a_1}{b_1}x + \frac{a_0}{b_0} = 0.$$

令 $d = b_{n-1}b_{n-2} \cdots b_1b_0 \in A$, 两边同时乘以 d^n , 我们得到

$$(dx)^n + c_{n-1}(dx)^{n-1} + \cdots + c_1(dx) + c_0 = 0,$$

其中, $c_i \in A$ 。所以, $dx \in B$, 这表明, $x \in (A^\times)^{-1}B$ 。

命题 7.15

如果 A 是整闭的, $K = \text{Frak}(A)$, L/K 为代数扩张, B 为 A 在 L 中的整闭包。那么, 对任意的 $x \in B$, 其极小多项式 $P(X) \in A[X]$ 。特别地 (假设 L/K 为有限扩张), $\text{Tr}_{L/K}(x), N_{L/K}(x) \in A$ 。

证明 由于 $x \in B$, 存在 $P_0(X)$ 为 $A[X]$ 中首一的多项式, 使得 $P_0(x) = 0$, 从而, $P \mid P_0$ 。令 $\mathcal{R}(P_0)$ 为 $P_0(X)$ 在 $\bar{K} \supset L$ 中的所有根, 类似可定义 $\mathcal{R}(P)$ 。根据定义, 每个 $y \in \mathcal{R}(P_0)$ 在 A 上都是整的, 所以, 每个 $y \in \mathcal{R}(P)$ 在 A 上都是整的。由于 P 的系数都是 $\mathcal{R}(P)$ 中元素的整系数对称多项式, 所以, 它们都 A 上的整元素。另外, $P \in K[X]$, 根据 A 的整闭性, $P \in A[X]$ 。

根据第七次作业的问题 A, 当 L/K 是有限扩张时, 对任意的 $x \in L$, 对乘法映射:

$$m_x: L \longrightarrow L, y \mapsto x \cdot y.$$

它的迹、行列式和特征多项式给出了 $\text{Tr}_{L/K}$ 和 $N_{L/K}$:

$$\text{Tr}_{L/K}(x) = \text{Tr}(m_x), N_{L/K}(x) = \det(m_x), P_{L/K, x}(X) = \det(X \cdot I - m_x).$$

其中, A5) 表明

$$P_{L/K, x}(X) = P(X)^{[L:K(x)]}.$$

从而, $P_{L/K, x}(X) \in A[X]$ 。特别地, $\text{Tr}_{L/K}(x), N_{L/K}(x) \in A$ 。

命题 7.16 (有限性)

如果 A 是整闭的 Noether 环, $K = \text{Frak}(A)$, L/K 为有限可分扩张, B 为 A 在 L 中的整闭包。那么, B 是有限生成的 A -模。特别地, 如果 A 是主理想整环, 那么, B 是自由模并且其秩为 $[L:K]$

证明 根据 $(A^\times)^{-1}B = L$, 选取 L 作为 K -线性空间的一组基 $\{x_1, \dots, x_n\} \subset B$ 。

$$\begin{array}{ccc} B' = \bigoplus_{j=1}^n Ay_j & & \\ \vdots & \searrow \subset & \\ B & \text{-----} & L \\ \vdots & & \vdots \\ A & \text{-----} & K \end{array}$$

根据可分性, L/K 的可分性, 双线性型

$$L \times L \longrightarrow K, (x, y) \mapsto \text{Tr}_{L/K}(x \cdot y).$$

非退化, 从而, 我们有 K -线性空间的同构:

$$L \longrightarrow L^*, x \mapsto (y \mapsto \text{Tr}_{L/K}(x \cdot y)).$$

据此, 我们可以选取 $\{y_i\}_{1 \leq i \leq n} \subset L$ 为 $\{x_1, \dots, x_n\}$ 的对偶基, 即

$$\mathrm{Tr}_{L/K}(x_i \cdot y_j) = \delta_{ij}^j, \quad 1 \leq i, j \leq n.$$

令 $B' = \{x \in L \mid \mathrm{Tr}_{L/K}(x \cdot x_j) \in A, 1 \leq j \leq n\}$ 。这显然是 A -模并且 $B \subset B'$ 。另外, 对任意的 $x \in B'$, 我们有

$$x = \sum_{j=1}^n \mathrm{Tr}_{L/K}(x \cdot x_j) y_j.$$

这说明 B' 是有限生成的 A -模, 其中 $\{y_i\}_{1 \leq i \leq n}$ 是一组生成元。由于 A 是 Noether 环, 从而, B' 是 Noether 模, 进而其子模 B 是有限生成的。

如果 A 是主理想整环, 由于 $B \subset L$ 是无挠的, 根据主理想整环上有限生成模的分类定理, B 是自由的 A -模。另外, 令 $B'' := \bigoplus_{j=1}^n A x_j$, 那么, 我们有

$$B'' \subset B \subset B'.$$

由于 B'' 和 B' 都是秩为 $[L:K]$ 的自由模, 所以 B 也是。

例题 7.18 对数域的应用 令 $A = \mathbb{Z}$, $K = \mathbb{Q}$, L 为 \mathbb{Q} 的有限扩张, $B = \mathcal{O}_L$ 为 \mathbb{Z} 在 L 中的整闭包:

$$\begin{array}{ccc} \mathcal{O}_L & \text{-----} & L \\ \vdots & & \vdots \\ \mathbb{Z} & \text{-----} & \mathbb{Q} \end{array}$$

我们称 \mathcal{O}_L 为 L 所对应的**整数环**。根据以上命题, \mathcal{O}_L 是秩为 $[L:\mathbb{Q}]$ 的自由交换群。

注[函数域的情形] \mathbb{F}_q 是有限域, $A = \mathbb{F}_q[X]$, $K = \mathrm{Frak}(A) = \mathbb{F}_q(X)$, L/K 为有限扩张, B 为 A 在 L 中的整闭包。那么, B 是有限生成的 A -模。特别地, B 是自由模并且其秩为 $[L:K]$ 。

在这种特殊情形下, 我们不需要假设 L/K 是可分的。证明该结论需要先研究 L/K 是纯不可分的情形, 由于之后我们不会用到这个结论, 所以在此不给出细节。

注[数域与函数域的扩张] 考虑 \mathbb{Q} (或 $\mathbb{F}_q(X)$) 的有限扩张 K , 令 \mathcal{O}_K 为 K 的整数环; L 为 K 的有限扩张, $B = \mathcal{O}_L$ 为 $A = \mathcal{O}_K$ 在 L 中的整闭包。从而, $B = \mathcal{O}_L$ 也是 \mathbb{Z} (或 $\mathbb{F}_q[X]$) 在 L 中的整闭包。

$$\begin{array}{ccc} \mathcal{O}_L & \text{-----} & L \\ \vdots & & \vdots \\ \mathcal{O}_K & \text{-----} & K \\ \vdots & & \vdots \\ \mathbb{Z} & \text{-----} & \mathbb{Q} \end{array} \qquad \begin{array}{ccc} B & \text{-----} & L \\ \vdots & & \vdots \\ A & \text{-----} & K \\ \vdots & & \vdots \\ \mathbb{F}_q[X] & \text{-----} & \mathbb{F}_q(X) \end{array}$$

我们称 \mathcal{O}_L 为 L 所对应的**代数整数环**。根据以上命题, \mathcal{O}_L 是秩为 $[L:\mathbb{Q}]$ 的自由交换群。

例题 7.19 二次数域的整数环 d 是不包含任何平方因子的整数, $K = \mathbb{Q}(\sqrt{d})$, 我们来计算 \mathcal{O}_K 。

对于 $x = a + b\sqrt{d} \in K$, $a, b \in \mathbb{Q}$, 我们有

$$x^2 - 2ax + a^2 - b^2d = 0.$$

从而, $x \in \mathcal{O}_K$ 等价于 $2a \in \mathbb{Z}, a^2 - b^2d \in \mathbb{Z}$ 。特别地, 我们有

$$(2a)^2 - (2b)^2d \in \mathbb{Z} \Rightarrow (2b)^2d \in \mathbb{Z} \Rightarrow 2b \in \mathbb{Z}.$$

另外, 根据以上讨论, 我们显然有 $\mathbb{Z} + \mathbb{Z}\sqrt{d} \subset \mathcal{O}_K$ 。

假设 $a = \frac{1}{2}a'$, 其中, $a' \in \mathbb{Z}$ 为奇数。此时, 考虑关系 $a^2 - b^2d \in \mathbb{Z}$, 很明显, $b \notin \mathbb{Z}$, 从而, $b = \frac{1}{2}b'$, 其中, $a' \in \mathbb{Z}$ 为奇数。那么,

$$a^2 - b^2d \in \mathbb{Z} \Rightarrow \frac{1}{4}(a'^2 - b'^2d) \in \mathbb{Z}.$$

由于 $a'^2 \equiv b'^2 \equiv 1 \pmod{4}$, 以上等价于说 $d \equiv 1 \pmod{4}$ 。据此, 我们得到

$$\mathcal{O}_K = \begin{cases} a + b\sqrt{d}, & a, b \in \mathbb{Z} & d \equiv 2, 3 \pmod{4}; \\ \frac{1}{2}(a + b\sqrt{d}), & a, b \in \mathbb{Z}, a \equiv b \pmod{2}, & d \equiv 1 \pmod{4}. \end{cases}$$

练习 7.4 证明, $\mathbb{Z}[\sqrt{5}]$ 不是整闭的。

例题 7.20 $\mathbb{Q}(e^{\frac{2\pi i}{p}})$ 的整数环, p 是素数 令 $\xi = e^{\frac{2\pi i}{p}}$, $L = \mathbb{Q}(e^{\frac{2\pi i}{p}})$, 考虑 L/\mathbb{Q} 。我们知道 ξ 的极小多项式为

$$X^{p-1} + \cdots + X + 1.$$

特别地, $\xi \in \mathcal{O}_L$ 并且 $\bigoplus_{j=0}^{p-2} \mathbb{Z} \cdot \xi^j \subset \mathcal{O}_L$ 。

根据以上极小多项式, 我们有

$$\mathrm{Tr}_{L/\mathbb{Q}}(\xi^k) = \begin{cases} p, & k=0; \\ -1, & 1 \leq k \leq p-1. \end{cases}$$

我们现在计算

$$N_{L/\mathbb{Q}}(1 - \xi) = (-1)^{p-1}p.$$

一个直接的方法就是利用 $1, \xi, \dots, \xi^{p-2}$ 作为 L/\mathbb{Q} 的基, 从而对 m_ξ 所对应的矩阵直接计算行列式。另一个是利用

$$P(X) = X^{p-1} + \cdots + X + 1 = \frac{X^p - 1}{X - 1} \Rightarrow Q(X) = P(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \cdots + p.$$

那么, $\xi - 1$ 是 $Q(X)$ 的根, 从而,

$$N_{L/\mathbb{Q}}(\xi - 1) = \prod_{\sigma \in \mathrm{Gal}(L/\mathbb{Q})} \sigma(\xi - 1) = p.$$

特别地, 这就给出了上述结论。

另外, 我们还有

$$N_{L/\mathbb{Q}}(\xi - 1) = (-1)^{p-1} \prod_{k=1}^{p-1} (1 - \xi^k) = (-1)^{p-1}p.$$

从而,

$$p = \prod_{k=1}^{p-1} (1 - \xi^k).$$

特别地, $p \in \mathcal{O}_L \cdot (1 - \xi)$, 其中, $\mathcal{O}_L \cdot (1 - \xi)$ 是 \mathcal{O}_L 的主理想。由于 $1 - \xi \notin \mathcal{O}_L^\times$, 所以, $\mathcal{O}_L \cdot (1 - \xi) \cap \mathbb{Z} = p\mathbb{Z}$

(因为 $\mathcal{O}_L \cdot (1 - \xi)$ 要包含在某个素理想 \mathfrak{p} 中而 $\mathfrak{p} \cap \mathbb{Z}$ 是 \mathbb{Z} 中的素理想并且包含 p)。

令 $x \in \mathcal{O}_L$, 那么, 对任意的 $\sigma \in \text{Gal}(L/\mathbb{Q})$, $\sigma(x) \in \mathcal{O}_L$ (因为它们都满足同样的首一的整系数多项式)。从而,

$$\sigma(x \cdot (1 - \xi)) = \sigma(x) \cdot (1 - \xi^{k_\sigma}) = \sigma(x) \cdot (1 + \xi + \cdots + \xi^{k_\sigma - 1})(1 - \xi) \in \mathcal{O}_L \cdot (1 - \xi).$$

据此,

$$\text{Tr}_{L/\mathbb{Q}}(x \cdot (1 - \xi)) = \sum_{\sigma \in \text{Gal}(L/\mathbb{Q})} \sigma(x \cdot (1 - \xi)) \in \mathcal{O}_L \cdot (1 - \xi).$$

另一方面, $\text{Tr}_{L/\mathbb{Q}}(x \cdot (1 - \xi)) \in \mathbb{Z}$ 。从而,

$$\text{Tr}_{L/\mathbb{Q}}(x \cdot (1 - \xi)) \in p\mathbb{Z}, \quad \forall x \in \mathcal{O}_L.$$

假设 $x = a_0 + a_1\xi + \cdots + a_{p-2}\xi^{p-2} \in \mathcal{O}_L$, 其中, $a_0, \dots, a_{p-2} \in \mathbb{Q}$ 。那么,

$$\begin{aligned} \text{Tr}_{L/\mathbb{Q}}(x \cdot (1 - \xi)) &= \text{Tr}_{L/\mathbb{Q}}\left(a_0(1 - \xi) + \sum_{i=1}^{p-2} a_i \xi^i - \sum_{i=1}^{p-2} a_i \xi^{i+1}\right) \\ &= \text{Tr}_{L/\mathbb{Q}}(a_0(1 - \xi)) + \sum_{i=1}^{p-2} a_i \xi^i - \sum_{i=1}^{p-2} a_i \xi^{i+1} \\ &= pa_0. \end{aligned}$$

从而, $pa_0 \in p\mathbb{Z}$, 所以, $a_0 \in \mathbb{Z}$ 。另外, $\xi^{-1} = \xi^{p-1} \in \mathcal{O}_L$, 从而,

$$a_1 + a_2\xi + \cdots + a_{p-2}\xi^{p-2} = (x - a_0) \cdot \xi^{-1} \in \mathcal{O}_L.$$

从而, $a_1 \in \mathbb{Z}$ 。重复这个过程, 我们得到 $a_i \in \mathbb{Z}$, $i = 0, \dots, p-2$ 。最终, 我们证明

$$\mathcal{O}_{\mathbb{Q}(\xi)} = \mathbb{Z}[\xi], \quad \xi = e^{\frac{2\pi i}{p}}.$$

7.6.3 素理想与 Galois 群

以下我们研究 A 与 B 的素理想之间的关联。首先, 我们不加证明的引用如下定理:

定理 7.14 (Cohen-Seidenberg)

给定环的整扩张 $A \subset B$, $\mathfrak{p} \subset A$ 是素理想。

$$\begin{array}{ccc} \mathfrak{q} & \text{---} & B \\ \vdots & & \mid \text{整} \\ \mathfrak{p} & \text{---} & A \end{array}$$

那么, 存在素理想 $\mathfrak{q} \subset B$, 使得 \mathfrak{q} 在 \mathfrak{p} 之上, 即 $\mathfrak{q} \cap A = \mathfrak{p}$ 。



Cohen-Seidenberg 定理的证明并不困难, 自然的做法是利用对 \mathfrak{p} 的局部化 (参考第五次作业)。这个证明过程与我们的主旨关联不大, 所以略去。

注 \mathfrak{p} 是极大理想当且仅当 \mathfrak{q} 是极大理想。

实际上, 我们有环的扩张 $A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}$, 这是整扩张。

如果 \mathfrak{p} 是极大理想, 那么, A/\mathfrak{p} 是域, 从而, 对任意的 $x \in B/\mathfrak{q}$, 存在 $a_0, \dots, a_{n-1} \in A/\mathfrak{p}$, 其中, $a_0 \neq 0$, 使得

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0 \Rightarrow x \cdot a_0^{-1}(x^{n-1} + a_{n-1}x^{n-2} + \dots + a_1) = 1.$$

这说明 x 有逆, 从而, B/\mathfrak{q} 是域, 所以, \mathfrak{q} 是极大理想。

反之, \mathfrak{q} 是极大理想, 那么, B/\mathfrak{q} 是域。对任意的 $x \in A/\mathfrak{p}$, x^{-1} 在 A/\mathfrak{p} 上是整的, 从而, 存在 $a_0, \dots, a_{n-1} \in A/\mathfrak{p}$, 其中, $a_0 \neq 0$, 使得

$$x^{-n} + a_{n-1}x^{1-n} + \dots + a_1x^{-1} + a_0 = 0 \Rightarrow x^{-1} = -(a_{n-1} + \dots + a_1x^{n-2} + a_0x^{n-1}) \in A/\mathfrak{p}.$$

所以, A/\mathfrak{p} 是域, 即 \mathfrak{p} 是极大理想。

考虑 $K_0 = \mathbb{Q}$ (或 $K_0 = \mathbb{F}_q(X)$) 的有限扩张 K , 令 A 为 $A_0 = \mathbb{Z}$ (或 $A_0 = \mathbb{F}_q[X]$) 在 K 中的整闭包, L 为 K 的有限扩张, B 为 A 在 L 中的整闭包。

$$\begin{array}{ccccc} I_{\mathfrak{p}} & \text{---} & B & \text{---} & L \\ | & & | & & | \\ \mathfrak{p} & \text{---} & A & \text{---} & K \\ & & | & & | \\ & & A_0 & \text{---} & K_0 \end{array}$$

令 $I_{\mathfrak{p}} = \{\mathfrak{q} \subset B \mid \mathfrak{q} \text{ 是素理想并且在 } \mathfrak{p} \text{ 之上}\}$ 。根据 Cohen-Seidenberg 定理, $I_{\mathfrak{p}} \neq \emptyset$ 。

考虑 $\mathfrak{p} \cap A_0$, 这是 A_0 中的素理想, 从而是 A_0 中的极大理想 (因为 A_0 是主理想整环)。从而, \mathfrak{p} 是 A 中的极大理想。特别地, 每个 $\mathfrak{q} \in I_{\mathfrak{p}}$ 都是 B 中的极大理想。这表明

$$I_{\mathfrak{p}} = \{\mathfrak{q} \subset B \mid \mathfrak{q} \text{ 是素理想并且在 } \mathfrak{p} \text{ 之上}\} = \{\mathfrak{q} \supset \mathfrak{p} \cdot B \mid \mathfrak{q} \text{ 是素理想}\}.$$

注[有限性] 利用 A 和 B 是 Noether 环, 我们可以证明每个 $I_{\mathfrak{p}}$ 都是有限集。然而, 我们以下只对 L/K 是 Galois 扩张的情形证明这个结果 (据此应该也能推出一般的结论)。

定理 7.15

A, B, K, L 和 \mathfrak{p} 如上所述, 进一步假设 L/K 是 Galois 扩张。那么, $\text{Gal}(L/K)$ 可以传递的作用在 $I_{\mathfrak{p}}$ 上:

$$\text{Gal}(L/K) \times I_{\mathfrak{p}} \rightarrow I_{\mathfrak{p}}, (\sigma, \mathfrak{q}) \mapsto \sigma(\mathfrak{q}).$$

特别地, $|I_{\mathfrak{p}}| \leq |\text{Gal}(L/K)|$ 。



注 对于 $x \in B$, x 满足一个 A -系数的首一多项式所给的方程。很明显, $\sigma(x)$ 也满足同样的方程, 其中, $\sigma \in \text{Gal}(L/K)$ 。从而, $\sigma(x) \in B$ 。这就给出了环同构:

$$\begin{array}{ccc} B & \xrightarrow{\sigma} & B \\ | & & | \\ A & \xrightarrow{=} & A \end{array}$$

特别地, 对于 $\mathfrak{q} \in I_{\mathfrak{p}}$, $\sigma(\mathfrak{q})$ 仍然是 B 中的素理想; 由于 $\sigma|_A = \text{id}$, 所以, \mathfrak{q} 仍在 \mathfrak{p} 之上。这就给出了定理中的群作用。

证明 现在证明 $\text{Gal}(L/K)$ 在 $I_{\mathfrak{p}}$ 上的作用传递。如若不然, 选取 $\mathfrak{q}, \mathfrak{q}' \in I_{\mathfrak{p}}$, 使得 $\mathfrak{q} \notin \{\sigma(\mathfrak{q}') \mid \sigma \in \text{Gal}(L/K)\}$ 。

$\text{Gal}(L/K)$ 。由于它们都是极大理想，所以是两两互素的。根据中国剩余定理，

$$\pi: B \rightarrow B/\mathfrak{q} \times \prod_{\sigma \in \text{Gal}(L/K)} B/\sigma(\mathfrak{q}')$$

是满射，从而，存在 $x \in B$ ，使得

$$\begin{cases} x \equiv 0 \pmod{\mathfrak{q}}; \\ x \equiv 1 \pmod{\sigma(\mathfrak{q}'), \forall \sigma \in \text{Gal}(L/K)}. \end{cases}$$

根据范数映射的定义以及上面第一个同余式， $N_{L/K}(x) \in \mathfrak{q} \cap A = \mathfrak{p}$ ；根据第二个同余式，对任意的 $\sigma \in \text{Gal}(L/K)$ ， $\sigma(x) \equiv 1 \pmod{\mathfrak{q}'}$ ，从而， $N_{L/K}(x) = \prod_{\sigma \in \text{Gal}(L/K)} \sigma(x) \notin \mathfrak{q}'$ ，特别地， $N_{L/K}(x) \notin \mathfrak{q}' \cap A = \mathfrak{p}$ ，矛盾。

定义 7.13

任意给定 $\mathfrak{q} \in I_{\mathfrak{p}}$ ，我们定义 \mathfrak{q} 的分解群为以上作用在 \mathfrak{q} 出的稳定化子：

$$\mathfrak{D}_{\mathfrak{q}} := \{\sigma \in \text{Gal}(L/K) \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}.$$

注 注意到对于其他的 $g(\mathfrak{q}) \in I_{\mathfrak{p}}$ ，其中， $g \in \text{Gal}(L/K)$ ，我们有

$$G_{g(\mathfrak{q})} = g\mathfrak{D}_{\mathfrak{q}}g^{-1}.$$

从而，所有 $\mathfrak{q} \in I_{\mathfrak{p}}$ 定义的分解群均同构。

给定 $\sigma \in \mathfrak{D}_{\mathfrak{q}}$ ，根据 $\sigma: B \rightarrow B$ 和 $\sigma: \mathfrak{q} \rightarrow \mathfrak{q}$ ，我们有域同构 $\bar{\sigma}: B/\mathfrak{q} \rightarrow B/\mathfrak{q}$ 。

$$\begin{array}{ccc} B & \xrightarrow{\sigma} & B \\ \downarrow & & \downarrow \\ B/\mathfrak{q} & \xrightarrow{\bar{\sigma}} & B/\mathfrak{q} \end{array}$$

另外， $\bar{\sigma}: A/\mathfrak{p} \rightarrow A/\mathfrak{p}$ 是单位映射 id ，从而，我们得到

$$\begin{array}{ccc} B/\mathfrak{q} & \xrightarrow{\bar{\sigma}} & B/\mathfrak{q} \\ & \searrow \quad \swarrow & \\ & A/\mathfrak{p} & \end{array}$$

注 如果我们选取 $A = \mathbb{Z}$ ， $\mathfrak{p} = (p)$ 为素数 p 对应的素理想。由于 B 是有限生成的 \mathbb{Z} -模，所以，域扩张

$$\begin{array}{c} B/\mathfrak{q} \\ | \\ \mathbb{Z}/(p) = \mathbb{F}_p \end{array}$$

是有限扩张。这表明， B/\mathfrak{q} 是有限域。

特别地，我们得到群同态

$$\text{Res}_{\mathfrak{q}}: \mathfrak{D}_{\mathfrak{q}} \longrightarrow \text{Gal}(B/\mathfrak{q}/A/\mathfrak{p}).$$

特别地, $\text{Gal}(\overline{B}/\overline{q}/\overline{A}/\overline{p})$ 是循环群, 因为这是有限域的扩张。我们还称以上同态的核 \mathfrak{I}_q 为 q 的惯性群:

$$\mathfrak{I}_q := \text{Ker}(\text{Res}_q : \mathfrak{D}_q \longrightarrow \text{Gal}(\overline{B}/\overline{q}/\overline{A}/\overline{p})).$$

我们现在对 L/K 使用 Galois 理论。根据 Galois 对应, 令 L^q 为 G_q 的中间域, 即

$$\begin{array}{ccccc} q & \xrightarrow{\quad} & B & \xrightarrow{\quad} & L \\ | & & | & & | \\ \tau = q \cap B^q & \xrightarrow{\quad} & B^q = B \cap L^q & \xrightarrow{\quad} & L^q \\ | & & | & & | \\ p & \xrightarrow{\quad} & A & \xrightarrow{\quad} & K \end{array} \quad \begin{array}{c} 1 \\ | \\ G_q \\ | \\ \text{Gal}(L/K) \end{array}$$

令 $B^q = B \cap L^q$, 这是 A 在 L^q 中的整闭包; 令 $\tau = q \cap B^q$, 这是 B^q 中的素理想, 它在 p 之上。那么, q 是唯一一个在 τ 上的理想: 实际上, $\text{Gal}(L/L^q) = G_q$ 在 τ 上所有理想的集合上的作用是传递的, 根据 G_q 的定义, 只有一个这样的 q 。

我们现在证明域扩张

$$\overline{A}/\overline{p} \longrightarrow \overline{B^q}/\overline{\tau}$$

是平凡的域扩张, 即 $\overline{A}/\overline{p} = \overline{B^q}/\overline{\tau}$ 。

选取 $x \in B^q$, 我们构造 $z \in A$, 使得 $z \equiv x \pmod{\tau}$: 根据中国剩余定理, 存在 $y \in B^q$, 使得

$$\begin{cases} y \equiv x \pmod{\tau}; \\ y \equiv 1 \pmod{\sigma^{-1}(q) \cap B^q}, \forall \sigma \in \text{Gal}(L/K) - \mathfrak{D}_q. \end{cases}$$

以上, 我们用到了 q 为 τ 上唯一的素理想, 从而, $\sigma^{-1}(q) \cap B^q \neq \tau$ 。根据以上同余关系, 我们有

$$\begin{cases} y \equiv x \pmod{\tau}; \\ \sigma(y) \equiv 1 \pmod{\tau}, \forall \sigma \in \text{Gal}(L/K) - \mathfrak{D}_q. \end{cases}$$

从而, $z = N_{L^q/K}(y) \equiv x \pmod{\tau}$ 。

定理 7.16

Res_q 为满的群同态。



证明 根据上面的讨论, 我们可以假设 $L^q = K$ 。令 $K_p = \overline{A}/\overline{p}$, $L_q = \overline{B}/\overline{q}$, 那么, 存在 $x \in B$, 使得它在 L_q 中的像 \bar{x} 满足 $L_q = K_p(\bar{x})$ (这是有限域的扩张)。令 $P(X) \in A[X]$ 为 x 在 K 上的极小多项式, $Q(X)$ 为 \bar{x} 在 K_p 上的极小多项式。通过 $\text{mod } p$, 我们有 $\overline{P}(X) \in K_p[X]$ 并且 $Q(X) \mid \overline{P}(X)$, 这是因为 \bar{x} 是 $\overline{P}(X)$ 的根。

对任意的 $\overline{\sigma} \in \text{Gal}(L_q/K_p)$, $\overline{\sigma}$ 完全由 $\overline{\sigma}(\bar{x})$ 决定。另外, $\overline{\sigma}(\bar{x})$ 仍然是 Q 的根, 从而是 $\overline{P}(X)$ 的根, 所以, 存在 $P(X)$ 的根 $y \in L$, 使得 $y = \overline{\sigma}(\bar{x}) \pmod{q}$ 。先选定 $\sigma' \in \text{Hom}_K(K(x), L)$, 使得 $\sigma'(x) = y$, 再将 σ' 扩张成 $\sigma \in \text{Hom}_K(L, L)$ 。这个 σ 给出了 $\overline{\sigma}$ 。

以上的定理给出了以下正合列:

$$1 \rightarrow \mathfrak{I}_q \longrightarrow \mathfrak{D}_q \longrightarrow \text{Gal}(B/\mathfrak{q}/A/\mathfrak{p}) \rightarrow 1.$$

命题 7.17

假设 $L = K(x)$, $P(X)$ 为 x 在 K 上的极小多项式。如果 $\overline{P}(X) \in K_{\mathfrak{p}}[X] = A/\mathfrak{p}[X]$ 是可分的, 那么, 惯性群 \mathfrak{I}_q 是平凡的。特别地, 我们有群同构

$$\mathfrak{D}_q \xrightarrow{\simeq} \text{Gal}(B/\mathfrak{q}/A/\mathfrak{p}).$$



证明 $P(X)$ 在 L 中分裂, 即 $P(X) = (X - x_1) \cdots (X - x_n)$, 其中, $x_1 = x, x_2, \dots, x_n \in L$ 。通过 mod \mathfrak{q} , 在 L_q 中, 我们有

$$\overline{P}(X) = (X - \overline{x_1}) \cdots (X - \overline{x_n}), \quad \overline{x_i} \neq \overline{x_j}, 1 \leq i < j \leq n.$$

对任意的 $\sigma \in \mathfrak{I}_q$, 按定义, $\overline{\sigma(\overline{x_i})} = \overline{x_i}$ 。我们考虑 $\sigma(x) = x_j$ 并决定 x_j 。由于 $\overline{\sigma(x_1)} = \overline{x_1}$, 这说明 $j = 1$, 从而, $\sigma(x) = x$, 所以, $\sigma = 1$ 。

ā 我们可以用同样的想法研究不可约多项式的分裂域:

$$\begin{array}{ccccc} \mathfrak{q} & \text{---} & B & \text{---} & L \\ | & & | & & | \\ \mathfrak{p} & \text{---} & A & \text{---} & K \end{array}$$

定理 7.17

$P(X)$ 为 $A[X]$ 上的首一不可约多项式, L 为 P 的分裂域, $\mathfrak{p} \subset A$ 为素理想, $\mathfrak{q}, K_{\mathfrak{p}} = A/\mathfrak{p}, L_{\mathfrak{q}} = B/\mathfrak{q}$ 如前所述, $\overline{P}(X)$ 是 P 在 $K_{\mathfrak{p}}[X]$ 中的像。

假设 $\overline{P}(X)$ 是可分的, 那么, $L_{\mathfrak{q}}$ 是 \overline{P} 在 $K_{\mathfrak{p}}$ 上的分裂域并且 $\mathfrak{D}_q \simeq \text{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}})$ 。

进一步, 如果 $\overline{P}(X) = \overline{P_1}(X)\overline{P_2}(X)\cdots\overline{P_l}(X)$ 是 \overline{P} 在 $K_{\mathfrak{p}}[X]$ 中的不可约分解, 其中, $\overline{P_i}(X)$ 为不可约多项式。根据可分性, P 在 L 上根的集合 $Z_P(L)$ 可以写成:

$$Z_P(L) = Z_1 \cup Z_2 \cup \cdots \cup Z_l,$$

使得 mod \mathfrak{q} 之后 Z_i 恰好给出了 $Z_{\overline{P_i}}(L_{\mathfrak{q}})$ ($\overline{P_i}$ 在 $L_{\mathfrak{q}}$ 上根的集合)。那么, 对任意的 $\sigma \in \mathfrak{D}_q$ 和 $i \leq l$, $\sigma(Z_i) = Z_i$ 。



注 由于 \overline{P} 是可分的, 从而, 它没有重根。据此, P 在 L 上无重根, 这表明 L/K 是 Galois 扩张。

证明 在 L 中, 我们有 $P(X) = (X - x_1) \cdots (X - x_n)$, 其中, $x_1, x_2, \dots, x_n \in L$ 。通过 mod \mathfrak{q} , 在 $L_{\mathfrak{q}}$ 中, 我们有

$$\overline{P}(X) = (X - \overline{x_1}) \cdots (X - \overline{x_n}), \quad \overline{x_i} \neq \overline{x_j}, 1 \leq i < j \leq n.$$

其中, $x_i \equiv \overline{x_j} \pmod{q}$ 并且 $\overline{x_j} \in L_q$ 。我们考虑 L_q/K_p 的中间域:

$$\begin{array}{ccc} L_q & & 1 \\ | & & | \\ K_p(\overline{x_1}, \dots, \overline{x_n}) & & \text{Gal}(L_q/K_p(\overline{x_1}, \dots, \overline{x_n})) \\ | & & | \\ K_p & & \text{Gal}(L_q/K_p) \end{array}$$

对任意的 $\sigma \in \mathfrak{D}_q$, 由于 σ 把 P 的根映射成 P 的根, 所以, σ 把每个 $\overline{x_i}$ 映射成某个 $\overline{x_i}$, 据此, 我们有群同态

$$\mathfrak{D}_q \longrightarrow \text{Gal}(K_p(\overline{x_1}, \dots, \overline{x_n})/K_p), \sigma \mapsto \overline{\sigma}.$$

由于 $\{\overline{x_i}\}_{i \leq n}$ 两两不同, 所以, $\overline{\sigma}(\overline{x_i}) = \overline{x_j}$ 决定了 $\sigma(x_i) = x_j$, 从而, 上述群同态是单射。根据 Galois 对应定理以及 Res_q 映射的满射性质, 我们有如下交换图表:

$$\begin{array}{ccc} \mathfrak{D}_q & \xrightarrow{\text{Res}_q} & \text{Gal}(L_q/K_p) \\ & \searrow \text{单} & \downarrow \text{满} \\ & & \text{Gal}(K_p(\overline{x_1}, \dots, \overline{x_n})/K_p) \end{array}$$

所以, 所有的映射都是双射, 进而 $K_p(\overline{x_1}, \dots, \overline{x_n}) = L_q$ 并且 $\mathfrak{D}_q \simeq \text{Gal}(L_q/K_p)$ 。

以下, 假设 $\overline{P}(X) = \overline{P_1}(X)\overline{P_2}(X)\cdots\overline{P_l}(X)$ 是 \overline{P} 在 $K_p[X]$ 中的不可约分解, 我们证明对任意的 $\sigma \in \mathfrak{D}_q$ 和 $i \leq l$, $\sigma: Z_i \rightarrow Z_i$ 。实际上, 对 σ 在 $\text{Gal}(L_q/K_p)$ 中的像 $\overline{\sigma}$ 而言, 我们显然有 $\overline{\sigma}: \overline{Z_i} \rightarrow \overline{Z_i}$, 这里, $\overline{Z_i}$ 为 Z_i 中的元素 mod q 之后的像, 从而, 只能有 $\sigma: Z_i \rightarrow Z_i$ 。

作为推论, 我们就得到了如下的著名定理:

定理 7.18 (Dedekind)

$P(X)$ 为首一的、整系数 n 次不可约多项式, L 是 P 在 \mathbb{Q} 上的分裂域, 通过在 P 的根上的作用, 将 $\text{Gal}(L/\mathbb{Q})$ 视为 \mathfrak{S}_n 的子群。假设存在素数 p , 使得 $\overline{P}(X)$ 是可分的, 其中 \overline{P} 是 P 在 $\mathbb{F}_p[X]$ 中的像。

令 $\overline{P}(X) = \overline{P_1}(X)\cdots\overline{P_l}(X)$ 为 \overline{P} 在 $\mathbb{F}_p[X]$ 中的不可约分解, 其中, 对 $i = 1, \dots, l$, $\deg(\overline{P_i}) = n_i$ 。

那么, 存在 (n_1, \dots, n_l) -型的 $\sigma \in \text{Gal}(L/\mathbb{Q}) < \mathfrak{S}_n$ (把 σ 写成两两不交的循环之积)。



证明 这是上一个定理的直接推论: 我们取 $A = \mathbb{Z}, K = \mathbb{Q}, p = (p)$ 。此时, $\mathfrak{D}_q \simeq \text{Gal}(L_q/\mathbb{F}_p)$ 。由于 $\text{Gal}(L_q/\mathbb{F}_p)$ 是循环群, 我们选取 $\sigma \in \mathfrak{D}_q < \text{Gal}(L_q/\mathbb{F}_p) < \mathfrak{S}_n$, 使得 σ 给出该循环群的生成元。因为 $\overline{P_i}(X)$ 是不可约的, σ 在 Z_i 上的作用是传递的, 从而, σ 在 Z_i 这 d_i 个根上给出了一个 d_i -循环。命题得证。

例题 7.21 计算多项式 $P(X) = X^4 + 4X^3 + 2X^2 + 3X - 5$ 在 \mathbb{Q} 上的分裂域 L 的 Galois 群 $\text{Gal}(L/\mathbb{Q})$ 。

在 \mathbb{F}_2 中考虑, 我们有 $\overline{P}(X) = X^4 + X + 1$ 。容易看出, \overline{P} 在 \mathbb{F}_2 和 \mathbb{F}_4 中没有根, 从而, \overline{P} 是不可约的。据此, $\text{Gal}(L/\mathbb{Q})$ 中有 4-循环。

在 \mathbb{F}_3 中考虑, 我们有 $\bar{P}(X) = X^4 + X^3 + 2X^2 + 1$ 。容易看出, \bar{P} 在 \mathbb{F}_3 恰有一个根 -1 。从而,

$$\bar{P}(X) = (X+1)(X^3 - X + 1).$$

并且 $X^3 - X + 1$ 是不可约的。据此, $\text{Gal}(L/\mathbb{Q})$ 中有 3-循环。

以上表明 $|\text{Gal}(L/\mathbb{Q})| \geq 3 \times 4 = 12$, 所以, $\text{Gal}(L/\mathbb{Q})$ 为 \mathfrak{S}_4 或者 \mathfrak{A}_4 。

在 \mathbb{F}_5 中考虑, 我们有 $\bar{P}(X) = X^4 - X^3 + 2X^2 - 2X$, 从而,

$$\bar{P}(X) = X(X-1)(X^2+2).$$

此时, X^2+2 在 $\mathbb{F}_5[X]$ 上不可约。据此, $\text{Gal}(L/\mathbb{Q})$ 中有对换。从而, $\text{Gal}(L/\mathbb{Q}) \neq \mathfrak{A}_4$ 。

综上所述, $\text{Gal}(L/\mathbb{Q}) \simeq \mathfrak{S}_4$ 。

练习 7.5 证明, 多项式 $P(X) = X^6 + 22X^5 - 9X^4 + 12X^3 - 37X^2 - 29X - 15$ 在 \mathbb{Q} 上的分裂域 L 的 Galois 群同构于 \mathfrak{S}_6 。

附录 A 作业题合集

A.1 第一次作业

A. 乘积结构

A1) (G_1, \cdot_1) 和 (G_2, \cdot_2) 是群。我们在 $G_1 \times G_2$ 上如下定义乘法：

$$(g_1, g_2) \cdot (g'_1, g'_2) := (g_1 \cdot_1 g'_1, g_2 \cdot_2 g'_2).$$

证明，在以上乘法下， $G_1 \times G_2$ 是群并且其单位元为 $(1_1, 1_2)$ 。我们把这个群称作是 G_1 与 G_2 的乘积。

A2) 证明，投影映射

$$\pi_1 : G_1 \times G_2 \rightarrow G_1, (g_1, g_2) \mapsto g_1,$$

和

$$\pi_2 : G_1 \times G_2 \rightarrow G_2, (g_1, g_2) \mapsto g_2,$$

是群同态。它们的核是什么？

A3) (泛性质) 给定群 (G_1, \cdot_1) 和 (G_2, \cdot_2) 。证明，存在唯一的¹群 G 以及唯一的群同态 $p_i : G \rightarrow G_i$ ($i = 1, 2$) 使得对任意的群 H 和任意的群同态 $\varphi_i : H \rightarrow G_i$ ($i = 1, 2$)，存在唯一的 $\psi : H \rightarrow G$ ，使得 $p_i \circ \psi = \varphi_i$ ($i = 1, 2$)。

$$\begin{array}{ccc} H & \xrightarrow{\varphi_1} & G_1 \\ \varphi_2 \downarrow & \searrow \psi & \uparrow p_1 \\ G_2 & \xleftarrow{p_2} & G \end{array}$$

(提示：利用 A2) 给出 G 的存在性；利用 ψ 的唯一性证明 G 的唯一性)

A4) 给定互素的正整数 n_1 和 n_2 。利用 A3) 证明，

$$\mathbb{Z}/n_1 n_2 \mathbb{Z} \rightarrow \mathbb{Z}/n_i \mathbb{Z}, \bar{k} \mapsto k \pmod{n_i}, \quad i = 1, 2,$$

给出了群同构

$$\mathbb{Z}/n_1 n_2 \mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/n_1 \mathbb{Z} \times \mathbb{Z}/n_2 \mathbb{Z}.$$

以上， $\mathbb{Z}/n\mathbb{Z}$ 表示的是（加法）循环群。

A5) C_1 和 C_2 是两个有限阶的循环群，那么， $C_1 \times C_2$ 是否是循环群？

A6) $(A_1, +_1, \cdot_1)$ 和 $(A_2, +_2, \cdot_2)$ 是环。我们在 $A_1 \times A_2$ 上如下定义加法 $+$ 和乘法 \cdot ：

$$(a_1, a_2) + (a'_1, a'_2) := (a_1 +_1 a'_1, a_2 +_2 a'_2), \quad (a_1, a_2) \cdot (a'_1, a'_2) := (a_1 \cdot_1 a'_1, a_2 \cdot_2 a'_2).$$

证明，选取加法单位元 $(0_1, 0_2)$ 和乘法单位元 $(1_1, 1_2)$ ， $A_1 \times A_2$ 在以上运算下是环。我们把

¹在同构的意义下

这个环称作是 A_1 与 A_2 的乘积。进一步证明，投影映射

$$\pi_1: A_1 \times A_2 \rightarrow A_1, (a_1, a_2) \mapsto a_1,$$

和

$$\pi_2: A_1 \times A_2 \rightarrow A_2, (a_1, a_2) \mapsto a_2,$$

是环同态。

- A7) (泛性质) 给定环 A_1 和 A_2 。证明，存在唯一的²环 A 以及唯一的环同态 $p_i: A \rightarrow A_i$ ($i = 1, 2$) 使得对任意的环 B 和任意的环同态 $\varphi_i: B \rightarrow A_i$ ($i = 1, 2$)，存在唯一的 $\psi: B \rightarrow A$ ，使得 $p_i \circ \psi = \varphi_i$ ($i = 1, 2$)。

$$\begin{array}{ccc} B & \xrightarrow{\varphi_1} & A_1 \\ \varphi_2 \downarrow & \searrow \psi & \uparrow p_1 \\ A_2 & \xleftarrow{p_2} & A \end{array}$$

- A8) 给定互素的正整数 m 和 n 。证明，我们有环同构³

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

(提示：使用中国剩余定理)

- A9) A 和 B 是环， A^\times 和 B^\times 是它们的乘法可逆元所构成的（乘法）群。证明，我们有群同构

$$(A \times B)^\times \simeq A^\times \times B^\times,$$

其中，红色的 \times 代表着环的乘积，蓝色的 \times 代表着群的乘积。

B. 域的有限乘法子群是循环群

给定正整数 n ，Euler 的 ϕ -函数给出 $1, \dots, n$ 中与 n 互素的数的个数：

$$\phi(n) = |\{1 \leq k \leq n \mid (k, n) = 1\}|.$$

- B1) 证明， $|\left(\mathbb{Z}/n\mathbb{Z}\right)^\times| = \phi(n)$ ，其中， $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ 是环 $\mathbb{Z}/n\mathbb{Z}$ 的可逆元组成的（乘法）子群。
B2) 证明， ϕ 具有如下乘性：对任意互素的正整数 n 和 m ，有

$$\phi(nm) = \phi(n)\phi(m).$$

进一步，如果 $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ 是它的素因子分解，其中， p_i 为不同的素数而指标 α_i 均为正整数，证明：

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

- B3) 证明，对任意正整数 n ，对任意与 n 互素的整数 a ，有 $a^{\phi(n)} \equiv 1 \pmod{n}$ 。特别地，当 p 为素数时，这给出了 Fermat 小定理。
B4) (有限循环群子群的分类) 证明，作为加法群，对每个 n 的因子 d ， $\mathbb{Z}/n\mathbb{Z}$ 恰有一个阶为

²在同构的意义下

³请与 A4) 仔细对比

d 的循环子群 C_d 。进一步, $\mathbb{Z}/n\mathbb{Z}$ 的每个子群均形如 C_d , 其中, $d|n$ 。

B5) 证明, 对任意的正整数 n , 我们有公式

$$n = \sum_{d|n} \phi(d).$$

B6) K 是域, $G < K^\times$ 是有限群, $|G| = n$ 。对任意的 $d|n$, 令 G_d 为 G 中阶为 d 的元素组成的集合。证明,

$$n = \sum_{d|n, G_d \neq \emptyset} \phi(d).$$

B7) 证明, G 是循环群。

B8) 证明, $(\mathbb{Z}/p\mathbb{Z})^\times$ 是循环群, 其中, p 是素数。

Algebra is the metaphysics of arithmetic.

— John Ray

练习题 (不提交)

1. G 是群, $H \subset G$ 是有限子集并且对乘法封闭⁴. 证明, H 是子群.
2. 假设 $\{G_i\}_{i \in I}$ 是 G 的一族正规子群, 那么, $\bigcap_{i \in I} G_i$ 也是正规子群.
3. 有限集 G 上定义了满足结合律的乘法 $G \times G \rightarrow G, (g_1, g_2) \mapsto g_1 \cdot g_2$. 假设以下两点成立:
 - 对任意的 $g, x, y \in G$, 有 $g \cdot x = g \cdot y \Rightarrow x = y$;
 - 对任意的 $g, x, y \in G$, 有 $x \cdot g = y \cdot g \Rightarrow x = y$.
 证明, G 在此乘法下是群.
4. 试给出所有 (在同构意义下) 阶数不超过 5 的群.
5. G 是群, $H < G$ 是子群并且 $[G:H] = 2$. 证明, $H \triangleleft G$ 是正规子群. 如果 $[G:H] = n$, 其中, $n \geq 3$, 结论是否成立?
6. G 是群, $H < G$ 是子群并且 $[G:H] = n$. 证明, 如果 H 是唯一的指标为 n 的子群, 那么 $H \triangleleft G$ 是正规子群.
7. (循环群的分类) G 是循环群. 证明, 或 $G \simeq \mathbb{Z}$, 或有正整数 n 使得 $G \simeq \mathbb{Z}/n\mathbb{Z}$, 二者必居其一.
8. G 是 mn 阶的交换群, 其中, m, n 为互素. 如果存在 $g, h \in G$, 使得其阶分别为 m 和 n , 证明, G 为循环群.
9. G 是群并且它只有有限个子群. 证明, G 是有限群.
10. G 是群. 对任意的 $g \in G$, 共轭映射 $\text{Int}(g)$ 的定义如下:

$$\text{Int}(g): G \rightarrow G, h \mapsto \text{Int}(g)(h) = ghg^{-1}.$$

证明, 以上映射给出群同态:

$$G \rightarrow \text{Aut}(G), g \mapsto \text{Int}(g).$$

并且 $\text{Ker}(\text{Int}) = Z(G)$ 而 $\text{Im}(\text{Int}) \triangleleft \text{Aut}(G)$ 是正规子群.

11. 试在二面体群 \mathcal{D}_4 中找到两个子群 $K < H < G$, 使得 $K \triangleleft H$, $H \triangleleft \mathcal{D}_4$, 但是 K 不是 \mathcal{D}_4 的正规子群? 这表明正规子群的关系并不传递.
12. G 是群, K 和 H 为其子群并且 $K \triangleleft H$, $H \triangleleft G$. 证明, 如果 H 是循环群, 那么 $K \triangleleft G$.
13. (四元数群) 令 $\mathbf{Q}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, 一共有 8 个元素. 定义 1 为单位元; 对任意的 $\pm x \in \mathbf{Q}_8$, 令 $(-1) \cdot (\pm x) = (\pm x) \cdot (-1) = \mp x$; 定义乘法:

$$i \cdot j = -j \cdot i = k, j \cdot k = -k \cdot j = i, k \cdot i = -i \cdot k = j, i^2 = j^2 = k^2 = -1.$$

证明, 以上给出群结构. 试找出它所有的子群并证明这些子群都是正规子群. \mathbf{Q}_8 与二面体群 \mathcal{D}_4 是否同构?

14. (Cayley 定理: 每个 (有限) 群都同构于 (有限) 对称群的子群) G 是群. 令 $X = G$, 定义映射:

$$\varphi: G \rightarrow \mathfrak{S}_X, g \mapsto \varphi(g): x \mapsto g \cdot_G x, \forall x \in X.$$

⁴即对任意的 $h_1, h_2 \in H$, $h_1 \cdot h_2 \in H$.

证明, G 是单的群同态 (从而, $G \simeq \text{Im}(\varphi)$)。

15. 证明, \mathbb{Q}/\mathbb{Z} 是无限群但是每个元素的阶都是有限的。

16. G 是群, 定义映射

$$\text{Inv}: G \rightarrow G, g \mapsto g^{-1}.$$

证明, G 是交换群当且仅当 Inv 是群同态。

17. G 是群, 如果对任意的 $g \in G$, $g^2 = 1$, 证明, G 是交换群

18. $\mathbb{Z}/p\mathbb{Z}$ 是 p -阶加法循环群, 其中, p 是素数。证明, $\text{Aut}(\mathbb{Z}/p\mathbb{Z})$ 是循环群。如果把 p 替换成 6 或者 8, 结论是否成立?

19. G 是群, H, K 为其子群。我们定义 $H \cdot K = \{h \cdot k | h \in H, k \in K\}$ 。证明, $H \cdot K$ 为子群当且仅当 $H \cdot K = K \cdot H$ 。

20. G 是群, H, K 为其有限子群。证明,

$$|H \cdot K| = \frac{|H||K|}{|H \cap K|}.$$

21. G 是群, H, K 为其子群。证明, $H \cap K < H$ 并且

$$[H : H \cap K] \leq [G : K].$$

假设 $[G : K]$ 有限, 进一步证明以上等号成立当且仅当 $G = K \cdot H$ 。

22. G 是群, H, K 为其有限指标的子群。证明,

$$[G : H \cap K] \leq [G : H][G : K].$$

并且等号成立当且仅当 $G = K \cdot H$ 。

23. $\varphi: G \rightarrow A$ 是群同态, A 是交换群。证明, G 中任意的包含 $\text{Ker}(\varphi)$ 的子群都是正规子群。

A.2 第二次作业

A. 对称群 \mathfrak{S}_n 的生成子集

假设 $n \geq 2$, 那么, 以下子集均生成 \mathfrak{S}_n :

- A1) 证明, $S_1 = \{(1, k) | k = 2, \dots, n\}$ 生成 \mathfrak{S}_n 。
- A2) 证明, $S_2 = \{(k, k+1) | k = 1, \dots, n-1\}$ 生成 \mathfrak{S}_n 。
- A3) 假设 $S = \{(i, j)\}$ 是一些置换 (2-循环) 的集合并且 S 生成 \mathfrak{S}_n , 那么, $|S|$ 的最小值是多少?
- A4) 证明, $S_3 = \{(1, 2), (1, 2, \dots, n)\}$ 生成 \mathfrak{S}_n 。
- A5) 假设 $|i_0 - j_0|$ 与 n 互素。证明, $S_4 = \{(i_0, j_0), (1, 2, \dots, n)\}$ 生成 \mathfrak{S}_n 。

B. 交错群 \mathfrak{A}_n ($n \geq 5$) 是单群

如果群 G 除了 1 和本身之外没有其它的正规子群, 我们就称 G 是单群。很明显, 循环群只有在其阶为素数时为单群。

B0) 给出 \mathfrak{A}_3 和 \mathfrak{A}_4 的正规子群。

B1) 我们按照以下步骤证明 \mathfrak{A}_5 是单群:

- B1-1) 假设 $N \triangleleft \mathfrak{A}_5$ 是正规子群并且 $N \neq 1$ 。假设 N 包含一个双置换 (两个不交的置换之积), 不妨设为 $\sigma = (1, 2)(3, 4)$, 证明, $\tau = (1, 5)(3, 4)$ 在 \mathfrak{A}_5 中与 σ 共轭。特别地, 证明 $\sigma\tau$ 是 3-循环。
- B1-2) 假设 $N \triangleleft \mathfrak{A}_5$ 是正规子群并且 $N \neq 1$ 。假设 N 包含一个 5-循环, 不妨设为 $\sigma = (1, 2, 3, 4, 5)$, 证明, $\tau = (2, 3, 1, 4, 5)$ 在 \mathfrak{A}_5 中与 σ 共轭。特别地, 证明 $\tau\sigma^2$ 是 3-循环。
- B1-3) 假设 $N \triangleleft \mathfrak{A}_5$ 是正规子群并且 $N \neq 1$ 。证明, N 包含所有的 3-循环, 从而, \mathfrak{A}_5 是单群。

B2) 我们还可以按照以下步骤证明 \mathfrak{A}_5 是单群

- B2-1) 证明, \mathfrak{A}_5 有五个共轭类并且每个共轭类中的元素个数分别为 1, 12, 12, 15 和 20。
- B2-2) 子群 $N \subset \mathfrak{A}_5$ 在 \mathfrak{A}_5 的共轭下不变。证明, $|N|$ 只能等于 1, 13, 16, 21, 25, 28, 33, 36, 40, 45, 48 和 60。
- B2-3) 证明, \mathfrak{A}_5 是单群。

B3) 以下假设 $n \geq 6$ 并且 \mathfrak{A}_{n-1} 是单群。假设 $N \triangleleft \mathfrak{A}_n$ 是正规子群并且 $N \neq 1$, $N \neq \mathfrak{A}_n$ 。

- B3-1) 如果存在 $\sigma \in N - \{1\}$ 使得 $\sigma(n) = n$, 证明, $N = \mathfrak{A}_n$ 。
- B3-2) 证明, 对任意的 $\sigma \in N - \{1\}$, 只要 $\{i, j\} \cap \{\sigma(n), n\} = \emptyset$, 那么, $\tau\sigma\tau^{-1}\sigma = 1$, 其中, $\tau = (i, j)(n, \sigma(n))$ 。
- B3-3) 同上, 证明, $\sigma^2 = 1$ 并且 $\sigma: \{i, j\} \rightarrow \{i, j\}$ 。(提示: 考虑 $\sigma^{-1}\tau\sigma\tau^{-1}$)
- B3-4) 证明, $\sigma = (n, \sigma(n))$ 从而得到矛盾。据此, \mathfrak{A}_n 是单群。

B4) 假设 $n \geq 5$, $G \triangleleft \mathfrak{S}_n$ 为正规子群, 证明, 如果 $G \neq 1$, $G \neq \mathfrak{S}_n$, 那么, $G = \mathfrak{A}_n$ 。

- B5) 证明, $N = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ 是 \mathfrak{S}_4 的正规子群并且 $N \triangleleft \mathfrak{A}_4$ 。 \mathfrak{S}_4/N 是哪一个群?
- B6) 假设 $n \geq 5$, $H < \mathfrak{S}_n$ 为子群, $d = [\mathfrak{S}_n : H]$ 。证明, 存在群同态 $\varphi: \mathfrak{S}_n \rightarrow \mathfrak{S}_d$, 使得 $\text{Ker}(\varphi) < H$ 。据此证明, 如果 $H \neq \mathfrak{A}_n, \mathfrak{S}_n$, 那么, $d \geq n$ 。
- B7) 证明, 对于 $n \geq 2$, 存在单的群同态 $\mathfrak{S}_n \rightarrow \mathfrak{A}_{n+2}$ (从而 \mathfrak{S}_n 可被视作是 \mathfrak{A}_{n+2} 的子群) 但是不存在单的群同态 $\mathfrak{S}_n \rightarrow \mathfrak{A}_{n+1}$ 。

C'est que **la symétrie**, c'est l'ennui, et l'ennui est le fond même du deuil.

\mathfrak{S}_n 令人烦闷, 而烦闷是悲伤之源。

Les Misérables (悲惨世界) V. Hugo,

练习题（不提交）

1. 证明, $Z(\mathfrak{S}_n) = 1$, 其中, $n \neq 2$ 。
2. 试找出二面体群 \mathfrak{D}_n 的所有正规子群, 计算 $Z(\mathfrak{D}_n)$ 并找出 \mathfrak{D}_n 的所有共轭类。
3. 四元数群 \mathbb{Q}_8 有多少共轭类? (参考第一次作业练习题 13)
4. \mathfrak{S}_4 中有多少个子群同构于 \mathfrak{S}_3 , 有多少个子群同构于 \mathfrak{S}_2 ?
5. \mathfrak{A}_4 中是否有 6 阶子群?
6. G 是群, $H < G$ 是子群。证明, H 是正规子群当且仅当 H 的每个左陪集都是右陪集。
7. (第二同构定理) G 是群, $K < G$, $N \triangleleft G$ 。证明, $N \cap K \triangleleft K$ 并且有自然的群同构:

$$K/N \cap K \xrightarrow{\cong} NK/N.$$

8. (第三同构定理) G 是群, $K \triangleleft G$, $H \triangleleft G$ 并且 $K < H$ 。证明, $H/K \triangleleft G/K$ 并且有自然的群同构:

$$(G/K)/(H/K) \xrightarrow{\cong} G/H.$$

9. (子群对应定理) $\varphi: G \rightarrow G'$ 是满的群同态, 我们有如下双射:

$$\{H \mid H < G, H \supset \text{Ker}(\varphi)\} \xrightarrow{1:1} \{H' \mid H' < G'\}, H \mapsto \varphi(H).$$

进一步, 假设以上对应把 H 映射成 H' , 那么, H 是 G 的正规子群当且仅当 H' 是 G' 的正规子群。

假设 $N \triangleleft G$ 是正规子群, 对 $G \rightarrow G/N$ 使用子群对应定理, 你得到什么结论?

10. G_i 是群, $N_i \triangleleft G_i$ 是正规子群, 其中, $i = 1, 2$ 。证明, $N_1 \times N_2$ 是 $G_1 \times G_2$ 的正规子群并且有同构

$$G_1/N_1 \times G_2/N_2 \xrightarrow{\cong} G_1 \times G_2 / N_1 \times N_2.$$

11. (半直积: 初见) G 是群, $K \triangleleft G$, $H \triangleleft G$, $K \cap H = 1$ 并且 $\langle K \cup H \rangle = G$ 。证明, $G/K \cong H$ 。
12. 请给出 8 阶群 (在同构意义下) 的清单。

A.3 第三次作业

A. 60 阶的单群

G 是群，其阶为 60， s_p 为其 Sylow p -子群的个数，如果 $s_5 \neq 1$ ，那么 G 是单群。我们用反证法证明这个结论。假设 $H \triangleleft G$ 并且 $H \neq 1, H \neq G$ 。

- A1) 证明， $s_2 \in \{1, 3, 5, 15\}$ ， $s_3 \in \{1, 4, 10\}$ ， $s_5 = 6$ 。
- A2) 假设 $|H|$ 是 5 的倍数，证明， $|H| = 30$ ；进一步证明， H 只有一个 Sylow 5-子群。据此推出矛盾。
- A3) 假设 $|H| \leq 4$ 。证明， G/H 只有一个 Sylow 5-子群；进一步证明存在 $H' \triangleleft G$ ， $H' \neq G$ 并且 $|H'|$ 是 5 的倍数。据此推出矛盾。
- A4) 假设 $|H| = 6$ 或者 $|H| = 12$ 。证明， H 只有一个 Sylow 2-子群或只有一个 Sylow 3-子群。据此推出矛盾。

以下假设 G 是阶为 60 的单群， s_p 为其 Sylow p -子群的个数。

- A5) $H < G$ 是子群并且 $H \neq G$ 。证明， $[G:H] \geq 5$ 。进一步证明，如果 $[G:H] = 5$ ，那么， $G \simeq \mathfrak{A}_5$ 。
- A6) 证明， $s_2 \in \{5, 15\}$ ， $s_3 = 4$ ， $s_5 = 6$ 。
- A7) 假设 $s_2 = 5$ ，证明， $G \simeq \mathfrak{A}_5$ 。
- A8) 假设 $s_2 = 15$ ，证明，存在 Sylow 2-子群 P 和 Q ，使得 $|P \cap Q| = 2$ 。进一步证明 $P \cap Q$ 的正规化子的指标为 5，即 $[G:N_G(P \cap Q)] = 5$ 。
- A9) 证明，阶为 60 的单群在同构的意义下只能是 \mathfrak{A}_5 并计算 s_2 的值。

B. 不存在 180 阶的单群

G 是群，其阶为 180，那么， G 不是单群。我们用反证法证明这个结论。以下 s_p 为 G 的 Sylow p -子群的个数，

- B1) (常用结论) 证明， p^2 阶的群必然是交换群，其中， p 是素数。
- B2) 证明， $s_3 = 10$ 。
- B3) 证明， $s_5 = 36$ 。
- B4) P 和 Q 是不同的 Sylow 3-子群，证明， $P \cap Q = 1$ 。(提示：假设 $g \in P \cap Q - \{1\}$ ，考虑其中心化子 $C_g(G)$)
- B6) 据上述结论推出矛盾。

C. 与 Sylow p -子群相关的补充

- C1) G 是有限群， $S < G$ 是一个 Sylow p -子群。证明， $[G:N_G(S)] \equiv 1 \pmod{p}$ 。
- C2) G 是有限群， $S < G$ 是一个 Sylow p -子群， $H \triangleleft G$ 是正规子群。证明， $S \cap H$ 是 H 的 Sylow p -子群。

C3) G 是有限群, $H \triangleleft G$ 是正规子群, $\pi: G \rightarrow G/H$ 是自然投影。证明, 如果 $S < G$ 是 Sylow p -子群, 那么, $\pi(S)$ 是 G/H 的 Sylow p -子群; 反之, 如果 $S' < G/H$ 是 Sylow p -子群, 那么, 存在 G 的 Sylow p -子群 S , 使得 $\pi(S) = S'$ 。

C4) (Frattini 技巧)

- 群 G 作用在集合 X 上, $H < G$ 是子群, 那么, ${}^G H \curvearrowright X$ 诱导出 ${}^H H \curvearrowright X$ 。假设 ${}^H H \curvearrowright X$ 是传递的, 证明, 对任意的 $x \in X$, $G = H \cdot \text{Stab}_G(x)$ 。
- (Frattini) G 是群, $H \triangleleft G$ 是有限的正规子群, $S < H$ 是 H 的一个 Sylow p -子群。证明, $G = H \cdot N_G(S)$ 。

C5) G 是有限群, $S < G$ 是一个 Sylow p -子群, $H < G$ 是子群并且 $H \supset N_G(S)$ 。证明, $H = N_G(H)$ 。

C6) G 是有限群, $S < G$ 是一个 Sylow p -子群。证明, $N_G(S) = N_G(N_G(S))$ 。

The theory of groups is a branch of mathematics in which one does something to something and then compares the results with the result of doing the same thing to something else, or something else to the same thing.

———— James R. Newman

练习题（不提交）

1. 证明，除了阶为 1 和 2 的群外，每个群都有非平凡的自同构。
2. (交换性的一个有用判据) G 是群。证明， G 是交换群等价于 $G/Z(G)$ 是循环群。
3. (对称群指标的另一种定义) 定义映射

$$\varepsilon': \mathfrak{S}_n \rightarrow \{\pm 1\}, \sigma \mapsto \varepsilon'(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

证明， ε' 是群同态并且与之前定义的指标映射 ε 一致。

4. G 是有限群， h 为其共轭类的个数。令 $C = \{(x, y) \in G \times G | xy = yx\}$ ，证明， $|C| = h|G|$ 。
5. 有限群 G 作用在有限集 X 上。证明，如果 $G \curvearrowright X$ 是忠实的，那么， $|G|$ 整除 $|X|!$ ；如果 $G \curvearrowright X$ 是自由的，那么， $|G|$ 整除 $|X|$ 。
6. (C.Jordan 的定理) 有限群 G 作用在有限集 X 上。证明，如果 $G \curvearrowright X$ 是传递的，那么存在 $g \in G$ ，使得对任意的 $x \in X$ ， $g \cdot x \neq x$ 。
7. (Ore 的定理) G 是有限群， p 是 $|G|$ 的最小素因子， $H < G$ 是子群。如果其指标 $[G:H] = p$ ，证明， H 是正规子群。
8. 不用单群的概念来证明
 - 存在唯一非平凡的群同态 $\mathfrak{S}_n \rightarrow \mathbb{Z}/2\mathbb{Z}$ 。
 - 不存在非平凡的群同态 $\mathfrak{A}_n \rightarrow \mathbb{Z}/2\mathbb{Z}$ 。
 - \mathfrak{A}_n 是 \mathfrak{S}_n 中唯一的指标为 2 的子群。
 - \mathfrak{A}_4 没有 6 阶子群。
9. p 是素数， $H < \mathfrak{S}_p$ 是 p -阶子群。
 - 证明，恰有一个 $\sigma \in H$ ，使得 $\sigma(1) = 2$ 。
 - 证明， \mathfrak{S}_p 有 $(p-2)!$ 个 Sylow p -子群。
10. p 是奇素数， $p \leq n < p^2$ 。证明， \mathfrak{S}_n 的 Sylow p -子群是交换群。
11. p 是奇素数， $n = p^2$ 。证明， \mathfrak{S}_n 的 Sylow p -子群不交换。
12. $n \geq 2$ ，子群 $H < \mathfrak{S}_n$ 的指标为 n 。证明， $H \simeq \mathfrak{S}_{n-1}$ 。

A.4 第四次作业

A. 最少的生成元个数

G 是群, 如果存在有限个 x_1, \dots, x_n , 使得 $G = \langle x_1, \dots, x_n \rangle$, 我们就称 G 是有限生成的。以上最小可能的 n 被称作是 G 的最少的生成元个数, 记作 $\min_{\text{gen}}(G)$ 。我们规定 $\min_{\text{gen}}(\{1\}) = 0$ 。

A1) 证明, $\min_{\text{gen}}(G) = 1$ 等价于 G 是非平凡的循环群。

A2) 假设 $n \geq 3$ 。证明, $\min_{\text{gen}}(\mathfrak{S}_n) = 2$ 。

A3) p 是素数, r 是自然数, $G = \underbrace{\left(\mathbb{Z}/p\mathbb{Z}\right)^r}_{r \text{ 个}} = \mathbb{Z}/p\mathbb{Z} \times \dots \times \mathbb{Z}/p\mathbb{Z}$ 。证明, $\min_{\text{gen}}(G) = r$ 。

(提示: 将 G 视为 $\mathbb{Z}/p\mathbb{Z}$ -线性空间)

A4) G 是有限生成群, 假设有满的群同态 $\varphi: G \rightarrow G'$ 。证明, G' 是有限生成群并且

$$\min_{\text{gen}}(G') \leq \min_{\text{gen}}(G).$$

A5) G 是群, $H \triangleleft G$ 是正规子群。证明, 如果 H 和 G/H 是有限生成的, 那么, G 也是并且

$$\min_{\text{gen}}(G) \leq \min_{\text{gen}}(G/H) + \min_{\text{gen}}(H).$$

A6) 对于群 $A = \prod_{i=1}^s \mathbb{Z}/d_i\mathbb{Z}$, 其中, $s \in \mathbb{Z}_{\geq 1}, d_1, \dots, d_s \in \mathbb{Z}_{\geq 2}$, 使得 $d_s \mid d_1, d_{s-1} \mid d_{s-2}, \dots, d_2 \mid d_1$ 。证明, $\min_{\text{gen}}(A) = s$ 。

A7) 对于群 $A = \mathbb{Z}^r = \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_{r \text{ 个}}$ 。证明, $\min_{\text{gen}}(A) = r$ 。据此证明, 如果 $\mathbb{Z}^r \simeq \mathbb{Z}^{r'}$, 那么, $r = r'$ 。

A8) (子群生成元个数可以更多) 对任意的 $n \geq 3$, 给出如下的例子: G 是群, $H < G$ 是子群, $\min_{\text{gen}}(G) = 2$ 而 $\min_{\text{gen}}(H) = n$ 。

A9) (有限生成群的子群未必有限生成) 令 $G = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle < \mathbf{GL}(2; \mathbb{Q})$ 是由两个元素生成的群。证明, $H = \left\{ \begin{pmatrix} 1 & \frac{m}{2^k} \\ 0 & 1 \end{pmatrix} \mid k \in \mathbb{Z}_{\geq 0}, m \in \mathbb{Z} \right\}$ 是 G 的子群并且不是有限生成的。

A10) (有限生成交换群子群的生成元个数) G 是有限生成交换群, $H < G$ 是子群。证明,

$$\min_{\text{gen}}(H) \leq \min_{\text{gen}}(G).$$

(提示: 找一个 $g \in G$, 使得 $\min_{\text{gen}}(G/\langle g \rangle) < \min_{\text{gen}}(G)$)

A11) $r \geq 1$, A 是 \mathbb{Z}^r 的子群。证明, 存在 $r' \leq r$, 使得 $A \simeq \mathbb{Z}^{r'}$ 。

B. 阶为 p^3 的群有 5 个, $p \neq 2$

假设 p 是奇素数。用 \mathbb{F}_p 表示 p 个元素的有限域, 用 $\mathbb{Z}/p\mathbb{Z}$ 表示其加法群。

B1) 在同构意义下, 写下所有阶为 2^3 的群和阶为 p^2 的群。

- B2) 我们在课上用对角线均为 1 的上三角矩阵给出了 $\mathbf{GL}(2; \mathbb{F}_p)$ 一个 Sylow 子群。计算 $\mathbf{GL}(2; \mathbb{F}_p)$ 中 Sylow p -子群的个数。
- B3) 给定两个非平凡的群同态 $\varphi: \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbf{GL}(2; \mathbb{F}_p)$ 和 $\varphi': \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbf{GL}(2; \mathbb{F}_p)$ 。对任意的整数 k , 令 $\varphi_k(x) = \varphi(kx)$, 其中, $x \in \mathbb{Z}/p\mathbb{Z}$ 。证明, 存在 $A \in \mathbf{GL}(2; \mathbb{F}_p)$ 和 $k = 1, 2, \dots, p-1$, 使得对任意的 $x \in \mathbb{Z}/p\mathbb{Z}$, 有
- $$\varphi'(x) = A \cdot \varphi_k(x) \cdot A^{-1}.$$
- B4) 在同构的意义下, 可能的半直积 $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes_{\psi} \mathbb{Z}/p\mathbb{Z}$ 恰有两个。进一步证明, 其中恰有一个是非交换群并且其中心同构于 $\mathbb{Z}/p\mathbb{Z}$ 。
- B5) G 是群, $|G| = p^3$ 。假设 G 不是循环群并且存在 $g \in G$ 使得 $\text{ord}(g) = p^2$ 。证明, $\langle g \rangle \triangleleft G$ 。
- B6) 证明, 在同构的意义下, 上一个问题中的群恰好两个。
- B7) 在同构意义下, 写下所有阶为 p^3 的群。

I do not believe there is anything useful which men can know with exactitude that they cannot know by arithmetic and algebra.

—— Nicolas Malebranche

练习题（不提交）

1. 证明，四元数群 \mathbf{Q}_8 不能写成两个非平凡子群的半直积。⁵
2. N 是群， K 是循环群， $\varphi: K \rightarrow \text{Aut}(N)$ 和 $\psi: K \rightarrow \text{Aut}(N)$ 是群同态。证明，如果 $\varphi(K) = \psi(K)$ ，那么， $N \rtimes_{\varphi} K \simeq N \rtimes_{\psi} K$ 。（提示：请参考第四周讲义关于 pq 阶群分类的讨论）
3. G 是 p -群， $|G| = p^k$ 。证明，对任意的 $l \leq k$ ，存在正规子群 $H \triangleleft G$ ，使得 $|H| = p^l$ 。（提示：利用 $Z(G) \neq 1$ 以及 $G \rightarrow G/Z(G)$ 进行归纳）
4. A 是交换群。证明， A 是有限生成的交换群当且仅当存在整数 n 以及满的群同态 $\mathbb{Z}^n \rightarrow A$ 。
5. A 是交换群。我们定义 A 中的**挠元素**为下面集合中的元：

$$A^{\text{tor}} = \{x \in A \mid \text{存在 } n \in \mathbb{Z}, \text{ 使得 } nx = 0\}.$$

证明， A^{tor} 是 A 的子群。进一步证明如果 A 是有限生成的，那么， A^{tor} 是有限群并且 $A \simeq A^{\text{tor}} \times \mathbb{Z}^r$ ，其中， r 是 A 的秩。

6. A 和 B 是交换群。证明， $(A \times B)^{\text{tor}} \simeq A^{\text{tor}} \times B^{\text{tor}}$ 。
7. A 是有限交换群。证明，如果 A 不是循环群，那么，存在素数 p 和 A 的子群 H ，使得 $H \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ 。
8. G 是有限群并且对任意的 $g \in G$ ，有 $g^2 = 1$ 。证明，存在非负整数 n ，使得 $G \simeq \prod_{n \uparrow} \mathbb{Z}/2\mathbb{Z}$ 。
9. 对任意的 $n \geq 1$ 。证明，存在 \mathbb{R} 的子群 G ，使得 $G \simeq \prod_{n \uparrow} \mathbb{Z}$ 。
10. A, B 和 C 是有限生成的交换群。证明如下两个结论：

$$1) A \times A \simeq B \times B \Rightarrow A \simeq B; \quad 2) A \times C \simeq B \times C \Rightarrow A \simeq B.$$

⁵四元数群的定义参考第一次作业的练习题 13

A.5 第五次作业

A. 分式域的推广：局部化

在此问题中，字母 A 表示是某个给定的交换环，

A1) 给定子集 $S \subset A$ ，如果

- $1 \in S$;
- 对任意的 $s_1, s_2 \in S$ ，有 $s_1 \cdot s_2 \in S$ 。

我们就称 S 是**乘性子集**。证明，以下两个集合是乘性子集： $\{1, f, f^2, \dots\}$ ，其中， $f \in A$ ； $A - \mathfrak{p}$ ，其中， \mathfrak{p} 是素理想（特别的，如果 A 是整环， $A - \{0\}$ 是乘性子集）。

A2) 我们在 $A \times S$ 上定义等价关系： $(a, s) \sim (a', s')$ 指的是存在 $t \in S$ ，使得 $as' \cdot t = a's \cdot t$ 。证明，以上给出了 $A \times S$ 上的一个等价关系。

令 $A_S = A \times S / \sim$ ，我们用 $\frac{a}{s}$ 表示 (a, s) 所在的等价类。证明，对任意的 $s' \in S$ ，我们有 $\frac{s'a}{s's} = \frac{a}{s}$ 。

A3) 我们在 A_S 上定义如下的加法和乘法：

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

通过验证以上是良定义的来证明， A_S 在以上运算下成为一个环并指出它的乘法和加法单位元。进一步，我们还有自然的环同态：

$$\iota: A \rightarrow A_S, a \mapsto \frac{a}{1}.$$

我们把 A_S 称作是 A 对乘性子集 S 的**局部化**。

A4) 令 $S_0 = \{a \in A \mid ab = 0 \Leftrightarrow b = 0\}$ 。证明， S_0 是乘性子集。我们称 A_{S_0} 为 A 的**全分式环**。进一步证明 $\iota: A \rightarrow A_{S_0}$ 是单射并且此时 $\frac{a}{s} = \frac{a'}{s'}$ 当且仅当 $as' = a's$ 。

A5) 给定乘性子集 $S \subset A$ 。证明， $\text{Ker}(\iota) = \{a \in A \mid \text{存在 } s \in S, \text{ 使得 } as = 0\}$ 。进一步证明， ι 为单射当且仅当 $S \subset S_0$ 。

A6) (局部化的泛性质) A, S, A_S 和 $\iota: A \rightarrow A_S$ 如上述。试验证， $\iota(S) \subset (A_S)^\times$ 。

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \downarrow \iota & \nearrow \psi & \\ A_S & & \end{array}$$

证明，对任意的环 B 和环同态 $\varphi: A \rightarrow B$ ，如果 $\varphi(S) \subset B^\times$ ，则存在唯一的环同态 $\psi: A_S \rightarrow B$ ，使得 $\psi \circ \iota = \varphi$ 。

A7) A, S, A_S 和 $\iota: A \rightarrow A_S$ 如上述， $\widehat{S} = \{a \in A \mid \text{存在 } b \in A, \text{ 使得 } ab \in S\}$ 。证明， $\widehat{S} = \iota^{-1}((A_S)^\times)$ 。进一步证明环同构 $A_S \xrightarrow{\cong} A_{\widehat{S}}$ ，其中， $\frac{a}{1}$ 的像是 $\frac{a}{1}$ 。

A8) A 和 B 是交换环， $\varphi: A \rightarrow B$ 是环同态， $S \subset A$ 和 $T \subset B$ 是乘性子集并且 $\varphi(S) \subset T$ 。证明，

存在唯一的环同态 $\psi: A_S \rightarrow B_T$, 使得如下图表交换⁶:

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \downarrow \iota & & \downarrow \iota \\ A_S & \xrightarrow{\psi} & B_T \end{array}$$

A9) (理想与局部化) $I \subset A$ 是理想, 令 I_S 为 $\iota(I)$ 在 A_S 中生成的理想。

• 证明, $I_S = \{\frac{a}{s} | a \in I, s \in S\}$ 。进一步证明, $I_S = A_S$ 当且仅当 $S \cap I \neq \emptyset$ 。

• $J \subset A_S$ 是理想, 证明, $(\iota^{-1}(J))_S = J$ 。

A10) (素理想与局部化) 我们证明 A_S 中的素理想与 A 中与 S 不交的素理想一一对应。

• $\mathfrak{p} \subset A$ 是素理想并且 $\mathfrak{p} \cap S = \emptyset$, 证明, \mathfrak{p}_S 为 A_S 中的素理想。

• $\mathfrak{q} \subset A_S$ 是素理想, 证明, $\iota^{-1}\mathfrak{q}$ 是 A 中唯一满足 $\mathfrak{p}_S = \mathfrak{q}$ 的素理想。

A11) $\mathfrak{p} \subset A$ 是素理想, $S = A - \mathfrak{p}$, 令 $A_{\mathfrak{p}} = A_S$ 。证明, $A_{\mathfrak{p}}$ 是局部环 (即只有一个极大理想的环) 并确定它的极大理想。

A12) (局部化与商可交换) $I \subset A$ 是理想, $S \subset A$ 是乘性子集, $\pi: A \rightarrow A/I$ 是商映射, $\pi(S) \subset A/I$ 也是乘性子集。证明, 存在自然的环同构

$$(A/I)_{\pi(S)} \xrightarrow{\cong} A_S/I_S.$$

A13) 给定 $f \in A$, $S = \{1, f, f^2, \dots\}$, 记 $A_f = A_S$ 。证明, 我们有环同构

$$A[X]/(1-fX) \xrightarrow{\cong} A_f, \quad X \mapsto \frac{1}{f}.$$

B. $\mathbb{Z}[\sqrt{d}]^{\times}$ 与 Pell 方程, $d \neq \square, d > 0$

假设 $d \in \mathbb{Z}$ 不是完全平方数。令

$$\mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} | x, y \in \mathbb{Z}\}, \quad \mathbb{Q}[\sqrt{d}] = \{x + y\sqrt{d} | x, y \in \mathbb{Q}\}.$$

B1) 证明, $\mathbb{Z}[\sqrt{d}]$ 是环而 $\mathbb{Q}[\sqrt{d}]$ 为其分式域。

B2) 证明, 如果 $d < 0$, $\mathbb{Z}[\sqrt{d}]$ 是 \mathbb{C} 中的格点 (从而是离散的); 如果 $d > 0$, $\mathbb{Z}[\sqrt{d}]$ 在 \mathbb{R} 中稠密。

B3) 对任意的 $z = x + y\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, 我们定义 $\bar{z} = x - y\sqrt{d}$ (请注意, 如果 $d > 0$, 这不是复共轭)。证明, 环 $\mathbb{Z}[\sqrt{d}]$ 的自同构群 $\text{Aut}(\mathbb{Z}[\sqrt{d}])$ 恰有 2 个元素。

B4) 对任意的 $z \in \mathbb{Q}[\sqrt{d}]$, 我们定义 $N(z) = z \cdot \bar{z}$ 。证明, 对任意的 $a, b \in \mathbb{Q}[\sqrt{d}]$, $N(a \cdot b) = N(a) \cdot N(b)$ 并且 $N(\mathbb{Z}[\sqrt{d}]) \subset \mathbb{Z}$ 。据此证明: $\mathbb{Z}[\sqrt{d}]^{\times} = \{z \in \mathbb{Z}[\sqrt{d}] | N(z) = \pm 1\}$ 。

B5) 对于 $d < 0$, 试计算 $\mathbb{Z}[\sqrt{d}]^{\times}$ 。

当 $d > 0$ 时, $\mathbb{Z}[\sqrt{d}]^{\times}$ 的结构要复杂的多。实际上,

$$N(z = x + y\sqrt{d}) = \pm 1 \Leftrightarrow x^2 - dy^2 = \pm 1.$$

上述方程通常被称作是 Pell 方程。研究 $\mathbb{Z}[\sqrt{d}]^{\times}$ 可以给出以上方程所有的整数解。

⁶请查阅图表交换的含义

- B6) 证明, $\mathbb{Z}[\sqrt{2}]^{\times} \cap (1, 3) = \{1 + \sqrt{2}\}$ 。
- B7) 证明, $\mathbb{Z}[\sqrt{2}]^{\times} = \{\pm(1 + \sqrt{2})^k \mid k \in \mathbb{Z}\}$ 并给出群同构 $\mathbb{Z}[\sqrt{2}]^{\times} \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 。
- B8) 如何刻画 Pell 方程 $x^2 - 2y^2 = 1$ 和 $x^2 - 2y^2 = -1$ 的所有整数解?
以下假设 $d > 0$ 。
- B9) 证明, 有序列 $\{z_n\}_{n \geq 1} \subset \mathbb{Z}[\sqrt{d}]^{\times}$, 使得 $\lim_{n \rightarrow \infty} z_n = 0$ 而 $\{N(z_n)\}_{n \geq 1}$ 是有界的。
(提示: 使用标准的 Dirichlet 引理: 对任意的 $\alpha \in \mathbb{R}$, 对任意的正整数 M , 存在整数 p 和正整数 $q \leq M$, 使得 $|p - q\alpha| < \frac{1}{M}$ 。这个引理可以用抽屉原理直接证明或者请从文献中查阅证明)
- B10) 证明, 存在上述序列的子序列 $\{w_n\}_{n \geq 1}$ 以及整数 k , 使得对任意的 $n, m \geq 1$, 我们有 $N(w_n) = k$ 并且 $w_n \bar{w}_m \in k\mathbb{Z}[\sqrt{d}]$ 。(提示: 考虑 w_n 在 $\mathbb{Z}[\sqrt{d}]/k\mathbb{Z}[\sqrt{d}]$ 中的像)
- B11) 证明, $\mathbb{Z}[\sqrt{d}]^{\times}$ 是无限集。
- B12) 证明, $\mathbb{Z}[\sqrt{d}]^{\times} \cap (0, \infty)$ 是乘法群 $(0, \infty)$ 的离散子群, 即对任意的 $0 < a < b < \infty$, $\mathbb{Z}[\sqrt{d}]^{\times} \cap (a, b)$ 是有限的。
- B13) 证明, 存在 $\eta_d \in (1, \infty)$ (被称作是基本单位), 使得 η_d 生成了 $\mathbb{Z}[\sqrt{d}]^{\times} \cap (0, \infty)$ 。特别地, $\mathbb{Z}[\sqrt{d}]^{\times} \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 。
(注意到: 对任意的 $u \in \mathbb{Z}[\sqrt{d}]^{\times} - \{\pm 1\}$, 四个点 $\pm u, \pm \bar{u}$ 在区间 $(-\infty, -1), (-1, 0), (0, 1), (1, \infty)$ 中各有一个)

If one proves the equality of two numbers a and b by showing first that a is less than or equal to b and then a is greater than or equal to b , it is unfair, one should instead show that they are really equal by disclosing the inner ground for their equality.

—— Emmy Noether

练习题（不提交）

1. A 是环（未必交换）。证明，如果 $a \in A$ 是幂零元⁷， $b \in A^\times$ 并且 $ab = ba$ ，那么 $a + b$ 可逆；如果 $a, b \in A$ 是幂零元并且 $ab = ba$ ，那么 $a + b$ 是幂零元；
2. 证明，如果 $ab \in A$ 是幂零元，那么， ba 也是幂零元。据此，给出 $(1 - ab)^{-1}$ 与 $(1 - ba)^{-1}$ 之间的联系。据此证明，如果 $1 - ab \in A^\times$ ，那么， $1 - ba \in A^\times$ 。
3. A 是交换环， $\mathfrak{Nil}(A) = \{a \in A \mid \text{存在 } n \geq 1, \text{ 使得 } a^n = 0\}$ ， $\text{Spec}(A)$ 是 A 的所有素理想的集合。证明， $\mathfrak{Nil}(A) = \bigcap_{\mathfrak{p} \in \text{Spec}(A)} \mathfrak{p}$ 。
4. A 是交换环， $\text{SpecMax}(A)$ 是其极大理想的集合，其 **Jacobson 根式理想** 被定义为 $J(A) = \bigcap_{\mathfrak{m} \in \text{SpecMax}(A)} \mathfrak{m}$ 。证明， $a \in J(A)$ 当且仅当对任意的 $b \in A$ ， $1 - ab \in A^\times$ 。
5. A 是环， I 是双边理想。那么，我们有如下的一一对应

$$\{A \text{ 的左理想 } J \supset I\} \xrightarrow{1:1} \{A/I \text{ 的左理想}\}, J \mapsto J/I.$$
6. A 和 B 是交换环， $\varphi: A \rightarrow B$ 是环同态。证明，对任意的理想 $J \subset B$ ， $\varphi^{-1}(J) \subset A$ 是理想。
7. A 和 B 是交换环， $\varphi: A \rightarrow B$ 是环同态。证明，如果 $\mathfrak{q} \subset B$ 是素理想， $\varphi^{-1}(\mathfrak{q}) \subset A$ 也是素理想。进一步利用 $\mathbb{Z} \rightarrow \mathbb{Q}$ 的自然映射说明极大理想的逆像未必是极大的。
8. A 是（交换）环， $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ 是素理想， I 是理想。如果 $I \subset \bigcup_{i=1}^n \mathfrak{p}_i$ ，证明，存在 i_0 ，使得 $I \subset \mathfrak{p}_{i_0}$ 。
9. A 是（交换）环， I_1, \dots, I_n 是素理想， \mathfrak{p} 是素理想。如果 $\bigcap_{i=1}^n I_i \subset \mathfrak{p}$ ，证明，存在 i_0 ，使得 $I_{i_0} \subset \mathfrak{p}$ 。特别地，如果 $\bigcap_{i=1}^n I_i = \mathfrak{p}$ ，那么，存在 i_0 ，使得 $I_{i_0} = \mathfrak{p}$ 。
10. A 是环， I 和 J 是理想并且 I 与 J 互素（即 $I + J = A$ ）。证明，对任意的 $n \geq 1$ ， I^n 与 J^n 互素。
11. A 是环（未必交换），子集 $S \subset A$ 的中心化子 $\mathbf{Z}_S(A)$ 是 A 中在乘法意义下与 S 中所有元素均交换的元素的集合。证明， $\mathbf{Z}_S(A)$ 是 A 子环。
12. K 是域， $A = K[X]$ 是 K 上的多项式环， V 是 K -线性空间。给定线性映射 $T \in \text{End}_K(V)$ 可以给出 V 上的一个 $K[X]$ -模的结构：

$$K[X] \times V \rightarrow V, (P(X), v) \mapsto P(T)v.$$

证明， V 上的每一个 $K[X]$ -模的结构都恰好有某个 $T \in \text{End}_K(V)$ 唯一决定。

⁷即存在 $n \geq 1$ ，使得 $a^n = 0$

A.6 第六次作业

A. 关于 $\mathbb{Z}[\sqrt{d}]$ 上的一些代数和算术性质

假设 d 是整数（目前不要求 d 不包含平方因子）。

A1) (最大公约数与最小公倍数的概念) A 是整环, $a_1, \dots, a_n \in A$. 假设存在 $d \in A$ 使得对任意的 i , $d \mid a_i$ 并且对任意的 $d' \in A$, 使得对任意的 i , $d' \mid a_i$, 就一定有 $d' \mid d$, 我们就称 d 是 a_1, \dots, a_n 的一个**最大公约数**; 假设存在 $m \in A$ 使得对任意的 i , $a_i \mid m$ 并且对任意的 $m' \in A$, 使得对任意的 i , $a_i \mid m'$, 就一定有 $m \mid m'$, 我们就称 d 是 a_1, \dots, a_n 的一个**最小公倍数**. 我们在课堂上证明了唯一分解整环中最大公约数和最小公倍数是存在的。

- A 是整环, $a, b, c \in A - \{0\}$. 证明, $(a) \cap (b) = (c)$ 等价于 c 是 a, b 的一个最小公倍数. 进一步证明, 如果 a 是素元并且 $a \nmid b$, 那么, ab 是 a, b 的一个最小公倍数.
- A 是整环, $a, b, c \in A - \{0\}$. 如果 $(a) + (b) = (c)$, 证明 c 是 a, b 的一个最大公约数. 然而, 如果 c 是 a, b 的一个最大公约数, 未必有 $(a) + (b) = (c)$, 请参考最后一小问.
- 证明, 在 $\mathbb{Z}[\sqrt{-5}]$ 中, 2 和 $1 + \sqrt{-5}$ 有最大公约数.
- 证明, 在 $\mathbb{Z}[\sqrt{-5}]$ 中, 2 和 $1 + \sqrt{-5}$ 没有最小公倍数. 这表明 $\mathbb{Z}[\sqrt{-5}]$ 不是唯一分解整环.
- 证明, 在 $\mathbb{Z}[\sqrt{-5}]$ 中, $(2, 1 + \sqrt{-5})$ 不是主理想.

A2) 我们按照以下步骤证明: 如果 $d < -2$, 那么, $\mathbb{Z}[\sqrt{d}]$ 不是主理想整环.

- 证明, $(1 + \sqrt{-3}, 1 - \sqrt{-3})$ 不是 $\mathbb{Z}[\sqrt{-3}]$ 中的主理想.⁸
- 证明, $(2, \sqrt{-4})$ 不是 $\mathbb{Z}[\sqrt{-4}]$ 中的主理想.⁹
- 令 $\xi = \begin{cases} \sqrt{d}, & 2 \mid d; \\ 1 + \sqrt{d}, & 2 \nmid d \end{cases}$. 证明, $(2, \xi) = 2\mathbb{Z} + \xi\mathbb{Z}$.
- 证明, 如果 $d < -4$, $(2, \xi)$ 不是主理想. (提示: 先证明 $\mathbb{Z}[\sqrt{d}]$ 中 $N(x) \leq 4$ 的元素只有 $\pm 1, \pm 2$, 其中, $d < -4$)

A3) 假设 d 不是完全平方数, 我们按照以下步骤证明 $\mathbb{Z}[\sqrt{d}]$ 是 Noether 环:

- 给定理想 $0 \neq I \subset \mathbb{Z}[\sqrt{d}]$, 证明, 存在正整数 n , 使得 $I \cap \mathbb{Z} = (n)$.
- 证明, 作为加法群, $\mathbb{Z}[\sqrt{d}]$ 每个非零理想的指标是有限的.
- 证明, 对任意的正整数 n , 只有有限个理想 $I \subset \mathbb{Z}[\sqrt{d}]$, 使得 $I \cap \mathbb{Z} = (n)$.
- 证明, $\mathbb{Z}[\sqrt{d}]$ 是 Noether 环.

A4) 当 $d = -1, -2, 2$ 时, $\mathbb{Z}[\sqrt{d}]$ 是 Euclid 整环, 其中, 我们取范数¹⁰为 $\|z\| = |N(z)| = |z \cdot \bar{z}|$.

(提示: 回忆课上关于 Gauss 整数环是 Euclid 整环: 对 $a, b \in \mathbb{Z}[\sqrt{-1}]$, 选取 $q \in \mathbb{Z}[\sqrt{-1}]$,

⁸实际上, 通过研究 $2 \cdot 2 = (1 + \sqrt{3})(1 - \sqrt{3})$, 我们知道 $\mathbb{Z}[\sqrt{-3}]$ 不是唯一分解整环.

⁹实际上, 通过研究 $-2 \cdot 2 = \sqrt{-4} \cdot \sqrt{-4}$, 我们知道 $\mathbb{Z}[\sqrt{-4}]$ 不是唯一分解整环.

¹⁰按定义, 对于 $z = x + y\sqrt{d}$, $\bar{z} = x - y\sqrt{d}$, 这未必是复共轭.

使得

$$|\operatorname{Re}(q) - \operatorname{Re}(\frac{a}{b})| < \frac{1}{2}, \quad |\operatorname{Im}(q) - \operatorname{Im}(\frac{a}{b})| < \frac{1}{2}.$$

此时, 如果令 $r = a - qb$, $N(r) < N(b)$.)

A5) (一个 Diophantine 方程: Fermat) 我们按照以下步骤证明 $y^2 = x^3 - 2$ 的整数解只有 $(x, y) = (3, \pm 5)$:

- 证明, $\mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$ 。
- 证明, 如果 y 是奇数, 那么, $y + \sqrt{-2}$ 与 $y - \sqrt{-2}$ 互素。
- 假设整数 (x, y) 满足 $y^2 = x^3 - 2$ 。证明, 存在 $a, b \in \mathbb{Z}$, 使得 $y + \sqrt{-2} = (a + b\sqrt{-2})^3$ 。
- 利用上述表达式证明 $(x, y) = (3, \pm 5)$ 。

A6) 试求 $y^2 = x^3 - 1$ 的所有整数解。

B. 分圆多项式

对于 $n \geq 1$, 令 $\xi_n = e^{\frac{1}{n}2\pi i}$, 那么, $\{\xi_n^k\}_{0 \leq k \leq n-1}$ 给出了 $X^n - 1$ 在 \mathbb{C} 上的所有根, 我们把它们称作是 (\mathbb{C} 上的) n -次单位根。如果 $(k, n) = 1$, 我们就称 ξ_n^k 是一个本原的 n -次单位根并定义如下的首一 (首项系数为 1) 的多项式

$$\Phi_n(X) = \prod_{(k, n)=1, 1 \leq k \leq n} (X - \xi_n^k).$$

这个 $\Phi_n(X) \in \mathbb{C}[X]$ 被称作是 n -次分圆多项式。

B1) 证明, $\prod_{d|n} \Phi_d(X) = X^n - 1$ 。(请参考第一次作业)

B2) 计算 $\Phi_1(X)$ 和 $\Phi_p(X)$, 其中, p 为素数。

B3) 通过对 n 归纳证明, $\Phi_n(X) \in \mathbb{Z}[X]$ 。

B4) 假设 $z_0 \in \mathbb{C}$ 。证明, $I_{z_0} = \{Q(X) \in \mathbb{Q}[X] \mid Q(z_0) = 0\}$ 是 $\mathbb{Q}[X]$ 中的主理想。进一步证明, 如果 $I_{z_0} \neq 0$, 存在唯一的首一多项式 $P(X) \in \mathbb{Q}[X]$, 使得 $I_{z_0} = (P)$ 并且 $P(X)$ 是 $\mathbb{Q}[X]$ 中的不可约多项式。我们把 P 称作是 z_0 的极小多项式。

B5) ζ 是一个本原的 n -次单位根, 证明, 其极小多项式 $P(X) \in \mathbb{Z}[X]$ 。

B6) p 是素数并且 $(p, n) = 1$, 我们按照如下方式证明 ζ^p 也是 $P(X)$ 的根:

- 证明, $\mathbb{Z}[\zeta] = \left\{ \sum_{\text{有限和}} a_k \zeta^k \mid a_k \in \mathbb{Z}, k = 1, 2, \dots \right\}$ 是整环。
- 证明, 在 $\mathbb{Z}[\zeta]$ 中, $p \mid P(\zeta^p)$ 。(提示: 考虑 $P(X^p) - P(X)^p$)
- 如果 $P(\zeta^p) \neq 0$, 证明, 存在 $Q \in \mathbb{Z}[X]$, 使得

$$X^n - 1 = P(X)Q(X).$$

- 对上式中 X 求导数, 证明, 在环 $\mathbb{Z}[\zeta]$ 中, $p \mid n$ 。继而推出矛盾。

B7) 证明, $\Phi_n(X)$ 在 $\mathbb{Q}[X]$ 不可约。(提示: 研究 P 与 Φ_n 的关系)

注 在他 1796 年 10 月 9 日的数学日记中, Gauss 记录了 $\Phi_p(X)$ 在 $\mathbb{Q}[X]$ 不可约的性质, 其中, p 是素数; 在 1808 年 6 月 12 日的数学日记中, Gauss 记录了 $\Phi_n(X)$ 在 $\mathbb{Q}[X]$ 不可约的性质。文献中可考的关于 $\Phi_n(X)$ 不可约的证明, 较早一例可能是 Kronecker 在 1854 年的论文。

The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic.

_____ Gauss

练习题 (不提交)

1. $\mathbb{Z}[X]$ 是否是唯一分解整环, 是否是主理想整环? 主理想整环的子环是否是主理想整环? 唯一分解整环的子环是否是唯一分解整环?
2. A 是环 (未必交换)。证明, $\mathbf{M}_n(A)$ 双边理想必然形如 $\mathbf{M}_n(I)$, 其中, $I \subset A$ 是双边理想。如果 K 是域, 试决定 $\mathbf{M}_n(K)$ 的所有双边理想。
3. K 是域, V 是有限维 K -线性空间, $\mathbf{End}_K(V)$ 是 V 上线性变换所定义的环。对任意的 V 的 K -线性子空间 $W \subset V$, 我们定义

$${}_W J = \{\varphi \in \mathbf{End}_K(V) \mid \text{Ker}(\varphi) \supset W\}, \quad J_W = \{\varphi \in \mathbf{End}_K(V) \mid \text{Im}(\varphi) \subset W\}.$$

证明, ${}_W J$ 和 J_W 分别是 $\mathbf{End}_K(V)$ 中的左理想和右理想并且都是主理想。进一步证明, 我们有如下的一一对应:

$$\{V \text{ 的线性子空间}\} \xrightarrow{1:1} \{\mathbf{End}_K(V) \text{ 中左理想}\}, \quad W \mapsto {}_W J,$$

$$\{V \text{ 的线性子空间}\} \xrightarrow{1:1} \{\mathbf{End}_K(V) \text{ 中右理想}\}, \quad W \mapsto J_W.$$

4. 环 $\mathbf{M}_n(\mathbb{Z}/p\mathbb{Z})$ 中一共有多少个极大的左理想? 当 $n=4$ 时, 环 $\mathbf{M}_4(\mathbb{Z}/p\mathbb{Z})$ 中一共有多少个左理想?
5. A 是交换环, $I \subset A$ 是理想, M 是 A -模。验证, $I \cdot M = \{ \sum_{\text{有限和}} a_i \cdot x_i \mid a_i \in I, x_i \in M \}$ 是 M 的子模。证明, $M/I \cdot M$ 具有 A/I -模的结构。特别地, $M/\mathfrak{m} \cdot M$ 是 A/\mathfrak{m} 线性空间, 其中, \mathfrak{m} 是极大理想。
6. A 是交换环, M 是 A -模, $N \subset M$ 是子模。证明, 我们有如下的一一对应

$$\{N' \text{ 是 } M \text{ 的子模且 } N' \supset N\} \xrightarrow{1:1} \{M/N \text{ 的子模}\}, \quad N' \mapsto N'/N.$$

7. A 是交换环, M', M 和 M'' 是 A -模, 假定我们有如下正合列¹¹:

$$0 \rightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \rightarrow 0.$$

证明, 如下三个叙述等价:

- 作为 A -模, $M \simeq M' \oplus M''$;
- 存在 A -模同态 $s: M'' \rightarrow M$, 使得 $\psi \circ s = \text{id}_{M''}$;
- 存在 A -模同态 $p: M \rightarrow M'$, 使得 $p \circ \varphi = \text{id}_{M'}$ 。

以上发生的话, 我们就称改正合列是分裂的。

¹¹这里指的是 $\varphi: M' \rightarrow M$ 是单的 A -模同态, $\psi: M \rightarrow M''$ 是满的 A -模同态并且 $\text{Ker}(\psi) = \text{Im}(\varphi)$ 。
更一般的, 所谓的 A -模的正合列

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_{n-2}} M_{n-1} \xrightarrow{\varphi_{n-1}} M_n$$

指的是 $\varphi_j: M_k \rightarrow M_{k+1}$ 是 A -模同态并且 $\text{Im}(\varphi_k) = \text{Ker}(\varphi_{k+1})$, 其中, $j=1, 2, \dots, n-1$ 而 $k=1, 2, \dots, n-2$ 。我们还经常省略掉映射而把正合列写成

$$M_1 \longrightarrow M_2 \longrightarrow \cdots \longrightarrow M_{n-1} \longrightarrow M_n.$$

8. (五引理) 给定 A -模同态的交换图表:

$$\begin{array}{ccccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & M_5 \\ \downarrow \psi_1 & & \downarrow \psi_2 & & \downarrow \psi_3 & & \downarrow \psi_4 & & \downarrow \psi_5 \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & N_5 \end{array}$$

假设上下两行都是正合列。

- ψ_1 是满射, ψ_2, ψ_4 是单射。证明, ψ_3 是单射。

- ψ_5 是单射, ψ_2, ψ_4 是满射。证明, ψ_3 是满射。

特别地, 如果 $\psi_1, \psi_2, \psi_4, \psi_5$ 是同构, 那么, ψ_3 也是同构。

9. A 是交换环, M, M' 和 N 是 A -模, 试描述 $\text{Hom}_A(M, N)$ 上自然的 A -模结构。给定 A -模同态 $\varphi: M' \rightarrow M$ 。证明, 如下映射

$$\hat{\varphi}: \text{Hom}_A(M, N) \rightarrow \text{Hom}_A(M', N), \quad f \mapsto \varphi g,$$

和

$$\hat{\varphi}: \text{Hom}_A(N, M') \rightarrow \text{Hom}_A(N, M), \quad g \mapsto \varphi \circ g,$$

是 A -模同态。进一步证明所谓的 $\text{Hom}_A(\cdot, \cdot)$ 的左正合性:

- 给定 A -模的正合列

$$0 \rightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'',$$

我们有如下 A -模的正合列

$$0 \rightarrow \text{Hom}_A(N, M') \xrightarrow{\hat{\varphi}} \text{Hom}_A(N, M) \xrightarrow{\hat{\psi}} \text{Hom}_A(N, M'').$$

- 给定 A -模的正合列

$$M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \rightarrow 0,$$

我们有如下 A -模的正合列

$$0 \rightarrow \text{Hom}_A(M'', N) \xrightarrow{\hat{\psi}} \text{Hom}_A(M, N) \xrightarrow{\hat{\varphi}} \text{Hom}_A(M', N).$$

10. A 是整环, M 是 A -模, 对于 $x \in M$, 如果存在 $a \in A - \{0\}$, 使得 $a \cdot x = 0$, 我们就称 x 是**挠元素**。证明, 挠元素的全体 $T(M)$ 是 M 的子模。给定 A -模同态 $\varphi: M \rightarrow N$, 证明, 有自然的 A -模同态 $T(\varphi): T(M) \rightarrow T(N)$ 。

- 给定 A -模的正合列

$$0 \rightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'',$$

证明, 我们有如下 A -模的正合列

$$0 \rightarrow T(M') \xrightarrow{T(\varphi)} T(M) \xrightarrow{T(\psi)} T(M'').$$

- 试构造 A -模的满同态 $M \xrightarrow{\psi} M''$, 使得 $T(\psi): T(M) \rightarrow T(M'')$ 不是满射。

A.7 第七次作业

A. 迹与范数

L/K 是域的有限扩张, 对任意的 $x \in L$, 考虑乘法映射:

$$m_x: L \longrightarrow L, y \mapsto x \cdot y.$$

这是 K -线性空间 L 上的 K -线性映射, 它的迹、行列式和特征多项式分别记作:

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}(m_x), N_{L/K}(x) = \det(m_x), P_{L/K, x}(X) = \det(X \cdot I - m_x).$$

- A1) 假设 $x \in K$, 试计算 $\mathrm{Tr}_{L/K}(x), N_{L/K}(x)$ 和 $P_{L/K, x}(X)$ 。对一般的 $x \in L$, 证明 $P_{L/K, x}(X) \in K[X]$ 并且 $P_{L/K, x}(X)$ 在 L 中有根。
- A2) 假设 $d \in K$ 但是 $d \notin K^2$, $L = K(\sqrt{d})$, $x = a + b\sqrt{d}$ 。证明, 存在唯一的域同构 $\sigma \in \mathrm{Aut}_K(L)$, 使得 $\sigma(\sqrt{d}) = -\sqrt{d}$ 并且

$$\mathrm{Tr}_{L/K}(x) = 2a = x + \sigma(x), N_{L/K}(x) = a^2 - db^2 = x \cdot \sigma(x), P_{L/K, x}(X) = (X - x)(X - \sigma(x)).$$

- A3) 证明, 以下映射为群同态:

$$\mathrm{Tr}_{L/K}: (L, +) \rightarrow (K, +), N_{L/K}: (L^\times, \cdot) \rightarrow (K^\times, \cdot).$$

- A4) (迹的传递性) 如果 $K \subset M \subset L$ 是中间域。证明,

$$\mathrm{Tr}_{M/K} \circ \mathrm{Tr}_{L/M} = \mathrm{Tr}_{L/K}.$$

(提示: 选取 $\{e_i\}_{i \leq m}$ 和 $\{f_j\}_{j \leq n}$ 分别为 M/K 和 L/M 的基, 此时 $\{e_i f_j\}_{i \leq m, j \leq n}$ 为 L/K 的基。那么,

$$x \cdot f_j = \sum_{j'=1}^n m_{jj'} f_{j'}, m_{jj'} \in M; m_{jj'} \cdot e_i = \sum_{i'=1}^m k_{jj', ii'} e_{i'}, k_{jj', ii'} \in K.$$

利用上述公式计算)

- A5) 对于 $x \in L$, 令 $P_{\min}(X)$ 为其在 K 上的极小多项式。证明,

$$P_{L/K, x}(X) = P_{\min}(X)^{[L:K(x)]}.$$

(提示: 选取 $\{e_i\}_{i \leq m}$ 和 $\{f_j\}_{j \leq n}$ 分别为 $K(x)/K$ 和 $L/K(x)$ 的基, 此时 $\{e_i f_j\}_{i \leq m, j \leq n}$ 为 L/K 的基)

- A6) 对于 $x \in L$, $P_{\min}(X)$ 为其在 K 上的极小多项式, x_1, x_2, \dots, x_d 为 $P_{\min}(X)$ 在 K 的某个分裂域中所有的根 (即 $P_{\min}(X) = \prod_{i=1}^d (X - x_i)$)。证明,

$$\mathrm{Tr}_{L/K}(x) = [L:K(x)] \left(\sum_{i=1}^d x_i \right), N_{L/K}(x) = \left(\prod_{i=1}^d x_i \right)^{[L:K(x)]}.$$

- A7) L/K 为有限可分扩张, Ω/K 为域扩张并且 Ω 是代数封闭的。那么, 对任意的 $x \in L$,

$$\mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in \mathrm{Hom}_K(L, \Omega)} \sigma(x), N_{L/K}(x) = \prod_{\sigma \in \mathrm{Hom}_K(L, \Omega)} \sigma(x),$$

以及

$$P_{L/K, x}(X) = \prod_{\sigma \in \text{Hom}_K(L, \Omega)} (X - \sigma(x)).$$

A8) L/K 为有限扩张, Ω/K 如上。那么, 对任意的 $x \in L$,

$$\text{Tr}_{L/K}(x) = p^n \sum_{\sigma \in \text{Hom}_K(L, \Omega)} \sigma(x), \quad N_{L/K}(x) = \left(\prod_{\sigma \in \text{Hom}_K(L, \Omega)} \sigma(x) \right)^{p^n},$$

其中, $p^n = \frac{[L, K]}{[L, K]_s}$ 为扩张的不可分次数。

A9) (迹和范数的传递性) 如果 $K \subset M \subset L$ 是中间域。证明,

$$\text{Tr}_{M/K} \circ \text{Tr}_{L/M} = \text{Tr}_{L/K}, \quad N_{M/K} \circ N_{L/M} = N_{L/K}.$$

(为简单起见, 你可以只对可分情形进行证明)

A10) K 是域, $P(X) \in K[X]$ 为首一的不可约多项式, $d = \deg(P)$, α 为 P 在 \bar{K} 中的一个根。证明,

$$\text{Disc}(P) = (-1)^{\frac{1}{2}d(d-1)} N_{K(\alpha)/K}(P'(\alpha)).$$

以上, $\text{Disc}(P) := \prod_{i < j} (\alpha_i - \alpha_j)^2$, 其中, $\{\alpha_i\}$ 为 P 在 \bar{K} 中的所有根 (包括重根)。

A11) L/K 为有限扩张, $x \in L$ 在 K 上不可分。证明, $\text{Tr}_{L/K}(x) = 0$ 。

A12) L/K 为有限扩张并且不是可分的。证明, $\text{Tr}_{L/K} \equiv 0$ 。

A13) 考虑对称 K -双线性的二次型

$$L \times L \longrightarrow K, (x, y) \mapsto \text{Tr}_{L/K}(x \cdot y).$$

对任意的 $x \in L$, 存在 $y \in L$, 使得 $\text{Tr}_{L/K}(x \cdot y) \neq 0$, 我们就称这个二次型是**非退化的**, 否则是**退化的**。证明, 如果 $\text{char}(K) = 0$, 以上二次型非退化; 如果 L/K 不是可分的, 以上二次型退化。

A14) 假设 L/K 是可分的, 从而, $L = K(x)$, $n = [L : K]$ 。证明, $\text{Tr}_{L/K}(x^k)$ 中至少有一个非零, 其中, $k = 0, 1, \dots, n-1$ 。

A15) 证明, L/K 是可分的等价于二次型

$$L \times L \longrightarrow K, (x, y) \mapsto \text{Tr}_{L/K}(x \cdot y).$$

非退化。

B. Wedderburn 定理

F 是可除环, 即对任意非零的 $a \in F$, 存在 $b \in F$, 使得 $ab = ba = 1$ 。我们证明有限可除环一定是交换环, 从而 F 是域。以下我们假设 $|F| < \infty$ 。

B1) 令 $Z = \{x \in F \mid \text{对任意的 } y \in F, \text{ 有 } xy = yx\}$ 为 F 的中心。证明, Z 是域。令 $q = |Z|$, 证明, 存在 $n \geq 0$, 使得 $|F| = q^n$ 。

B2) 对任意的 $x \in F$, 令 $C_x = \{y \in F \mid xy = yx\}$ 。证明, C_x 是 F 的子环并且存在整数 n_x 使得 $|C_x| = q^{n_x}$ 。

- B3) 对于 $x \in F^\times$, 令 $\text{Conj}(x) = \{yxy^{-1} | y \in F^\times\}$ 。证明, $|\text{Conj}(x)| = \frac{q^n - 1}{q^{n_x} - 1}$ 并证明 $n_x | n$ 。
- B4) 证明, 如果 $x \notin Z$, 那么, $\Phi_n(q)$ 整除 $|\text{Conj}(x)|$, 其中, $\Phi_n(X)$ 为第 n 个分圆多项式。¹²
- B5) 证明, $\Phi_n(q) | q - 1$ 从而 $n = 1$ 。
- (利用 F^\times 通过共轭作用在自身上的轨道分解)

Si maintenant vous me donnez une équation que vous aurez choisie à votre gré, et que vous désiriez connaître si elle est ou non résoluble par radicaux, je n'aurai rien à y faire que de vous indiquer le moyen de répondre à votre question, sans vouloir charger ni moi ni personne de la faire. En un mot les calculs sont impraticables.

——— Galois

¹²参见第六次作业题目 B

练习题 (不提交)

1. 给定域扩张 L/K , 其中, K 是有限域并且 $|K| = q$. 证明, 任意的映射 $f: K \rightarrow L$ 都是多项式, 即证明对任意的 $x \in K$,

$$f(x) = \sum_{a \in K} (f(a)(1 - (x - a)^{q-1})).$$

2. 试找出域扩张 $\mathbb{Q}(\sqrt[4]{7})/\mathbb{Q}$ 所有的中间域。
3. L/K 是代数扩张, $\alpha, \beta \in L$ 并且其在 K 上的极小多项式分别为 $P(X), Q(X) \in K[X]$. 证明, 如果 $\deg(P)$ 与 $\deg(Q)$ 互素, 那么, α 在 $K(\beta)$ 上的极小多项式也是 $P(X)$. 据此, 计算 $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})/\mathbb{Q}$ 的次数。
4. 证明, $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, 找出 $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ 所有的中间域并计算 $\sqrt{2} + \sqrt{3}$ 在 \mathbb{Q} 上的极小多项式。
5. 计算 $\sqrt{2} + \sqrt{3} + \sqrt{5}$ 在 \mathbb{Q} 上的极小多项式。
6. p 是奇素数, 试计算 $\mathbb{Q}(\cos(\frac{2\pi}{p}))/\mathbb{Q}$ 的扩张次数。
7. 给定单代数扩张 $K(x)/K$. 证明, 如果 $[K(x):K]$ 是奇数, 那么, $K(x) = K(x^2)$.
8. K 是有限域, 那么, K 必然不是代数封闭的。(提示: 参考 Euclid 关于有无穷多素数的证明)
9. L/K 是域扩张。
- M 是中间域, 即 $K \subset M \subset L$, $\alpha \in L$ 在 K 上是代数的。令 $P_{\alpha, K}(X)$ 为 α 在 K 上的极小多项式, $P_{\alpha, M}(X)$ 为 α 在 M 上的极小多项式。证明, 在 $M[X]$ 中, 我们有 $P_{\alpha, M}(X) \mid P_{\alpha, K}(X)$ 。
 - 假设 L/K 是代数的。如果每个 K -系数多项式均在 $L[X]$ 中分裂 (成 1 次多项式之积), 证明, L 是 K 的一个代数闭包。
10. K 是域并且是可数的。证明, $K[X]$ 也是可数的。我们记 $K[X] = \{P_1, P_2, \dots, P_n, \dots\}$ 并归纳地定义 $K_0 = K$, K_n 为 $P_n(X)$ 在 K_{n-1} 上的分裂域。证明, $L := \bigcup_{n \geq 1} K_n$ 是 K 的一个代数闭包。
11. 给定域 L 及其子域 K_1, K_2 , 假设 $L/K_1 \cap K_2$ 是代数扩张。证明, 如果 L/K_1 和 L/K_2 是正规扩张, 那么, $L/K_1 \cap K_2$ 也是正规扩张。
12. K 是域, $P(X) \in K[X] - K$, L 为 K 的分裂域。证明, $[L:K] \mid n!$, 其中, $d = \deg(P)$ 。
13. p 是素数, $P(X) = X^p - X + 1 \in \mathbb{F}_p[X]$, 证明, P 是不可约的。进一步计算 $P(X)$ 的分裂域的次数。
- (提示: 如果 $\alpha \in \bar{\mathbb{F}}$ 是 P 的根, 那么, 对任意的 $a \in \mathbb{F}_p$, $\alpha + a$ 也是根)
14. L/K 是正规扩张, $P(X) \in K[X]$ 是不可约, 假设 P_1 与 P_2 是 $P(X)$ 在 $L[X]$ 中的两个首一的、不可约的因子。证明, 存在 $\sigma \in \text{Aut}_K(L)$, 使得 $P_1^\sigma = P_2$ 。
15. L/K 是代数扩张。证明, L/K 是正规扩张当且仅当对任意的不可约多项式 $P(X) \in K[X]$, 它在 $L[X]$ 中的不可约的因子的次数都是相同的。

A.8 第八次作业

A. Artin-Schreier 理论

Artin-Schreier 理论是对循环扩张的 Kummer 理论的补充，它研究域特征为 p 且 Galois 群为 p -阶循环群的情况。

A') K 是特征为 p 的域， $a \in K$ ， $P(X) = X^p - X - a$ ， L 是 P 在 K 上的分裂域。

A'1) 证明，如果 $x \in L$ 是 P 的根，那么，

$$P(X) = (X - x)(X - (x + 1)) \cdots (X - (x + p - 1)).$$

A'2) 证明， P 在 $K[X]$ 中或者不可约或者可以写成一次因式的乘积。

A'3) 假设 P 在 $K[X]$ 中不可约， $x \in L$ 为 P 的一个根。证明，以下映射

$$\text{Gal}(L/K) \longrightarrow \mathbb{F}_p, \quad g \mapsto g(x) - x$$

是群同构。特别地， $\text{Gal}(L/K) \simeq \mathbb{Z}/p\mathbb{Z}$ 。

A'') K 是特征为 p 的域， L/K 是 Galois 扩张并且 $\text{Gal}(L/K) \simeq \mathbb{Z}/p\mathbb{Z}$ ， σ 是 $\text{Gal}(L/K)$ 的一个生成元。

A''1) 证明，存在 $y \in L$ ，使得 $\sum_{k=0}^{p-1} \sigma^k(y) = -1$ 。

A''2) 令 $x = \sum_{k=0}^{p-1} k \sigma^k(y)$ ，证明， $\sigma(x) = x + 1$ 。

A''3) 证明， $P(X) = \prod_{k=0}^{p-1} (X - \sigma^k(x))$ 是 x 的极小多项式并且 $a = x^p - x \in K$ 。

A''4) 证明， L 是 $X^p - X - a$ 在 K 上的分裂域。

利用以上的 Artin-Schreier 理论，即 A')+A'')，我们展示 p^{m-1} 阶的循环扩张与 p^m 阶的循环扩张之间的关系 ($m \geq 2$)。从而，我们可以递归地研究阶为 p 的幂的循环扩张 (总假设 K 的特征为 p)。

A''') K 是特征为 p 的域， L/K 是阶为 p^m 的循环扩张， σ 是 $\text{Gal}(L/K)$ 的一个生成元， $\tau = \sigma^{p^{m-1}}$ ， $M = L^{\langle \tau \rangle}$ 。

A'''1) 证明，存在 $\lambda \in M$ ， $P(X) = X^p - X - \lambda$ 在 L 中有根 θ 并且 $L = M(\theta)$ ， $\tau(\theta) = \theta + 1$ 。

A'''2) 证明，存在 $\beta \in M$ ，使得 $\sigma(\theta) = \theta + \beta$ 。

A'''3) 证明， $K(\theta) = L$ 。

A'''4) 证明， $\sigma(\lambda) - \lambda = \beta^p - \beta$ 并且 $\text{Tr}_{M/K}(\beta) = 1$ 。

A'''5) (与之后无关) 令 $Q(X) = X^p - X$ 。证明，存在 $a \in K$ ，使得 $\underbrace{Q(Q(\cdots(Q(X))\cdots))}_{\text{共 } m \text{ 个}} - a$ 是

θ 在 K 上的极小多项式。

A''''') K 是特征为 p 的域， M/K 是阶为 p^{m-1} 的循环扩张 ($m \geq 2$)， σ 是 $\text{Gal}(M/K)$ 的一个生成元。假设 $\beta \in M$ 并且 $\text{Tr}_{M/K}(\beta) = 1$ 。¹³

A''''1) 证明，存在 $\lambda \in M$ ，使得 $\sigma(\lambda) - \lambda = \beta^p - \beta$ 。(提示：使用 Hilbert 90)

A''''2) $P(X) = X^p - X - \lambda$ 是 $M[X]$ 中的不可约多项式。

¹³根据 M/K 是有限可分的以及 $\text{Tr}_{M/K} : M \times M \rightarrow K$ 是非退化的，这种 β 总是存在。

A''3) 令 L 为 $P(X)$ 对 M 的分裂域, θ 为 P 在 L 中的一个根。证明, L/K 是阶为 p^m 的循环扩张并且存在 σ 在 L 上的延拓 $\bar{\sigma} \in \text{Gal}(L/K)$ 使得 $\bar{\sigma}$ 生成了 $\text{Gal}(L/K)$ 并且 $\bar{\sigma}(\theta) = \theta + \beta$ 。

B. 正十七边形的具体构造

令 $\xi = e^{\frac{2\pi}{17}i}$, $K = \mathbb{Q}$, $L = \mathbb{Q}(\xi)$ 。我们要通过具体计算 $\cos(\frac{2\pi}{17})$ 来说明 $e^{\frac{2\pi}{17}i}$ 是尺规可作的。

B1) 证明, 通过对 $X^{17} - 1$ 的根的作用, 我们有群同构

$$\text{Gal}(L/K) \xrightarrow{\cong} \left(\mathbb{Z}/17\mathbb{Z}\right)^\times$$

并且 $\sigma: \xi \mapsto \xi^3$ 是 $\text{Gal}(L/K)$ 的一个生成元。

B2) 以下是 $H_0 = \text{Gal}(L/K)$ 的一个 Jordan-Hölder 滤链:

$$H_0 \triangleright H_1 \triangleright H_2 \triangleright H_3 \triangleright H_4 = 1,$$

其中, $H_j = \langle \sigma^{2^j} \rangle$, $j = 1, 2, 3, 4$ 。利用 Galois 对应证明, $e^{\frac{2\pi}{17}i}$ 是尺规可作的。

B3) 令 $a_0 = \sum_{k=0}^7 \sigma^{2k}(\xi)$, $a_1 = \sum_{k=0}^7 \sigma^{2k+1}(\xi)$, 计算 $a_0 + a_1$ 和 $a_0 \cdot a_1$ 并给出 a_0 与 a_1 的值。

B4) 令 $b_j = \sum_{k=0}^3 \sigma^{4k+j}(\xi)$, 其中, $j = 0, 1, 2, 3$ 。计算 $b_0 + b_2$ 和 $b_0 \cdot b_2$ 并给出 b_0, b_1, b_2, b_3 的值。

B5) 令 $c_j = \sum_{k=0}^1 \sigma^{8k+j}(\xi)$, 其中, $j = 0, 1, \dots, 7$ 。计算 $c_0 + c_4$ 和 $c_0 \cdot c_4$ 并证明

$$\cos\left(\frac{2\pi}{17}\right) = \frac{1}{16} \left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + \sqrt{68 + 12\sqrt{17} - 4\sqrt{34 - 2\sqrt{17}} - 8\sqrt{34 + 2\sqrt{17}}} \right).$$

C. 代数基本定理的证明

我们用 Galois 理论证明 $\mathbb{C} = \mathbb{R}(i)$ 是代数封闭域。

C1) 证明, 每个奇数次的实系数多项式在 \mathbb{R} 上总有根。

C2) 证明, 每个 $\mathbb{R}(i)$ 系数的二次多项式的根都在 $\mathbb{R}(i)$ 中。

C3) 假设 $P(X) \in \mathbb{C}[X]$, 证明, 存在有限 Galois 扩张 L/\mathbb{R} , 使得 L 包含 i 和 P 的所有根。

C4) 令 H 为 $\text{Gal}(L/\mathbb{R})$ 的 Sylow 2-子群, 证明, $L^H = \mathbb{R}$ 。据此证明 $\text{Gal}(L/\mathbb{R})$ 是 2-群, 即其元素个数是 2 的幂。

(提示: 将 L^H 写成单代数扩张)

C5) 证明, 存在子群 $H' < \text{Gal}(L/\mathbb{R})$, 其指标为 2 并进一步证明 $L^{H'} = \mathbb{R}(i)$ 。

C6) 证明代数基本定理。

D. Dirichlet 定理的特例 (不提交)

经典的 Dirichlet 定理 (1837) 表明, 对任意互素的正整数 a, b , 存在无限多个素数 p , 使得 $p \equiv b \pmod{a}$ 。Dirichlet 的证明用到了复解析函数。我们可以用分圆多项式给出 $b = 1$ 的情形。

D1) 给定非常数的多项式 $P(X) \in \mathbb{Z}[X]$, 证明, 以下集合是无限集合:

$$\{d \in \mathbb{Z} | d \geq 0, \text{ 存在非负整数 } n, \text{ 使得 } d | P(n)\}.$$

D2) 令 $P(X) = \frac{X^a - 1}{\Phi_a(X)}$. 证明, 存在素数 p 和整数 n , 使得 $p | \Phi_a(n)$ 但是 $p \nmid P(n)$.

(提示: 在 $\mathbb{Q}[X]$ 中, 存在 $U(X), V(X)$, 使得 $U(X)P(X) + V(X)\Phi_a(X) = 1$)

D3) 计算 n 在 $(\mathbb{Z}/p\mathbb{Z})^\times$ 中的阶。

D4) 证明, 存在素数 p , 使得 $p \equiv 1 \pmod{a}$.

D5) 证明, 存在无限个素数 p , 使得 $p \equiv 1 \pmod{a}$. (提示: 对合适的 a 使用 D4) 的结论)

E. 二次互反律

$p > 2$ 是素数, 对任意的 $x \in \mathbb{Z}$, 将它视作是 \mathbb{F}_p 中的元素。如果 $x \neq 0$, 其 Legendre 符号 $\left(\frac{x}{p}\right)$ 的定义如下:

$$\left(\frac{x}{p}\right) = \begin{cases} 1, & x \text{ 是 } \mathbb{F}_p \text{ 中的完全平方}^{14} \\ -1, & x \text{ 不是 } \mathbb{F}_p \text{ 中的完全平方。} \end{cases}$$

E1) 证明, 映射 $(\mathbb{F}_p)^\times \rightarrow \{\pm 1\}$, $x \mapsto \left(\frac{x}{p}\right)$ 是满的群同态并且 $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$ (在 \mathbb{F}_p 中计算)。特别地, 我们得到 $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ 。

E2) 利用 Galois 理论计算 $\left(\frac{2}{p}\right)$ 。令 ζ 为 $\overline{\mathbb{F}_p}$ 中 8 次本元单位根。

- 证明, $(\zeta + \zeta^{-1})^2 = 2$ 。
- 证明, $\left(\frac{2}{p}\right) = 1$ 当且仅当 $\text{Frob}(\zeta + \zeta^{-1}) = \zeta + \zeta^{-1}$ 。
- 证明, $\left(\frac{2}{p}\right) = (-1)^{\frac{(p-1)(p+1)}{8}}$ 。

E3) $\ell > 2$ 是素数并且 $p \neq \ell$, ξ 为 $\overline{\mathbb{F}_p}$ 中 ℓ 次本元单位根。由 ℓ 给出的 Gauss 和为

$$S = \sum_{x \in \mathbb{F}_\ell^\times} \left(\frac{x}{\ell}\right) \xi^x.$$

证明, $S^2 = (-1)^{\frac{\ell-1}{2}} \ell$. (提示: 计算 $S^2 = \sum_{x \in \mathbb{F}_\ell^\times} \sum_{y \in \mathbb{F}_\ell^\times} \left(\frac{xy}{\ell}\right) \xi^{x+y} = \sum_{x \in \mathbb{F}_\ell^\times} \sum_{z \in \mathbb{F}_\ell^\times} \left(\frac{x^2 z}{\ell}\right) \xi^{x+zx}$)

E4) 证明, $S \in \mathbb{F}_p$ 等价于 $\left(\frac{p}{\ell}\right) = 1$ 。

E5) 证明二次互反律:

$$\left(\frac{p}{\ell}\right) \left(\frac{\ell}{p}\right) = (-1)^{\frac{p-1}{2} \frac{\ell-1}{2}}.$$

This skipping is another important point. It should be done whenever a proof seems too hard or whenever a theorem or a whole paragraph does not appeal to the reader. In most cases he will

be able to go on and later he may return to the parts which he skipped.

—— Emil Artin

练习题 (不提交)

1. 证明, $\mathbb{Q}(\sqrt{1+\sqrt{2}})/\mathbb{Q}$ 不是 Galois 扩张而 $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ 是 Galois 扩张。
2. K 是有限域。证明, 对任意的 $n \geq 1$, 存在 n -次不可约多项式。
3. \mathbb{F}_q 是有 q 个元素的有限域, $I(d)$ 是 $\mathbb{F}_q[X]$ 中 d -次首一不可约多项式的个数。证明

$$q^n = \sum_{d|n} d \cdot I(d).$$

(提示: 考虑 $X^{q^n} - X$ 的因式分解)

4. K 是域, p 是素数, $P \in K[X]$ 是可分的、不可约多项式, $\deg(P) = p$ 。 L 是 K 的分式域, α 是 P 在 L 中的一个根。证明, 存在 $\text{Gal}(L/K)$ 中的一个 p 阶元 σ , 使得

$$P(X) = (X - \alpha)(X - \sigma(\alpha)) \cdots (X - \sigma^{p-1}(\alpha)).$$

进一步证明, 如果存在 P 的另一个根 $\beta \in K(\alpha)$, 那么, $L = K(\alpha)$ 。

5. L/\mathbb{Q} 是 (有限) 循环扩张并且包含 $\mathbb{Q}(\sqrt{-d})$ 作为中间域, 其中, d 为正整数。证明, $4 \nmid [L:\mathbb{Q}]$ 。
6. (重要结论) K 是域并且其特征不是 3, $P \in K[X]$ 是 3 次不可约多项式, L 为 P 在 K 上的分裂域。证明,

$$\text{Gal}(L/K) = \begin{cases} \mathfrak{A}_3, & \text{如果 } \text{Disc}(P) \text{ 是 } K \text{ 中的完全平方;} \\ \mathfrak{S}_3, & \text{如果 } \text{Disc}(P) \text{ 不是 } K \text{ 中的完全平方.} \end{cases}$$

7. L/K 是有限 Galois 扩张并且 $\text{Gal}(L/K) \simeq \mathfrak{S}_n$, 其中, $n \geq 5$ 。任意给定 $x \in L$, $P(X) \in K[X]$ 为其极小多项式。证明, 如果 $\deg(P) > 2$, 那么 $\deg(P) \geq n$ 。如果 $n = 4$, 是否有反例?
8. K 是域, $P(X) \in K[X]$ 为可分的不可约多项式, L 为 P 在 K 上的分裂域, 假设 $\text{Gal}(L/K)$ 为交换群, $x \in L$ 为 P 的一个根。证明, $L = K(x)$ 。
9. 试计算以下 \mathbb{Q} -系数多项式在 \mathbb{Q} 上分裂域 (作为 \mathbb{Q} 的扩张) 的 Galois 群:
 - 1) $X^3 - 3X + 1$;
 - 2) $X^4 + 4$;
 - 3) $X^8 + 1$;
 - 4) $3X^5 - 12X^3 + 12X - 1$;
10. p_1, p_2, \dots, p_d 是 d 个不同的素数, $L = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_d})$ 。证明, L/\mathbb{Q} 是 Galois 扩张并计算其 Galois 群。据此证明, $\sqrt{15} \notin \mathbb{Q}(\sqrt{10}, \sqrt{42})$ 。

附录 B 有关集合的回顾

B.1 商集

对于集合 A , A 上的一个等价关系指的是 $A \times A$ 的子集 \mathcal{E} , 对于 $(a, b) \in \mathcal{E}$, 我们把它写成 $a \sim b$ (称作 a 和 b 等价), 并且如下的性质成立:

- 1) (自反性) 对任意的 $a \in A$, $a \sim a$ (或者对任意的 $a \in A$, $(a, a) \in \mathcal{E}$);
- 2) (对称性) 如果 $a \sim b$, 那么, $b \sim a$ (或者如果 $(a, b) \in \mathcal{E}$, 那么, $(b, a) \in \mathcal{E}$);
- 3) (传递性) 如果 $a \sim b$, $b \sim c$, 那么, $a \sim c$ (或者如果 $(a, b), (b, c) \in \mathcal{E}$, 那么, $(a, c) \in \mathcal{E}$).

对任意群的 $a \in A$, 令 \bar{a} (或者 $[a]$) 表示

$$\bar{a} = [a] = \{b \in A \mid b \sim a\} \subset A.$$

我们将这样的集合称作是 \sim 的一个等价类, 因为它是将相互等价的那些元素放到了一起。那么, $a \in \bar{a}$; 如果 $a \sim b$, 则 $\bar{a} = \bar{b}$; 对任意的 $a, b \in A$, 要么 $[a] = [b]$ 要么 $[a] \cap [b] = \emptyset$ 。所以, \sim 的等价类构成了 A 的一个划分:

$$A = \coprod \bar{a}.$$

反之, 假设 $A = \coprod_{i \in I} A_i$ 是 A 的一个划分, 即 $\cup_i A_i = A$ 并且 $\{A_i\}_{i \in I}$ 是两两不交的, 那么, 对任意的 $a, b \in A$, 我们规定 $a \sim b$ 当且仅当存在某个 A_i , 使得 $a, b \in A_i$, 这显然给出了一个等价关系。作为总结, 我们有

引理 B.1

给定集合 A 上的一个等价关系等价于给出集合 A 的一个划分。



给定集合 A 上的等价关系, 我们定义其等价类的集合为商集, 即

$$A/\sim = \{\bar{a} \mid a \in A\}.$$

我们有自然商映射:

$$\pi: A \rightarrow A/\sim, \quad a \mapsto \pi(a) = \bar{a}.$$

这显然是满射。按照定义, 对于 $a, b \in A$, $\pi(a) = \pi(b)$ 当且仅当 $a \sim b$ 。

命题 B.1 (商集的泛性质)

给定集合 A 以及 A 上的等价关系。那么, 对任意的集合 B 以及映射 $f: A \rightarrow B$, 存在映射 $\tilde{f}: A/\sim \rightarrow B$ 使得如下图表交换 (即 $f = \tilde{f} \circ \pi$)

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow \pi & \nearrow \tilde{f} & \\ A/\sim & & \end{array}$$

当且仅当对任意的 $a \sim a'$, 我们有 $f(a) = f(a')$ 。



证明 假设 $f = \tilde{f} \circ \pi$ 。对于 $a \sim a'$ ，按定义， $\pi(a) = \pi(a')$ ，所以， $\tilde{f}(\pi(a)) = \tilde{f}(\pi(a'))$ ，从而， $f(a) = f(a')$ 。假设对任意的 $a \sim a'$ ，都有 $f(a) = f(a')$ ，那么，对任意的 $\bar{a} \in A/\sim$ ，我们令 $\tilde{f}(\bar{a}) = f(a)$ 。容易看出 \tilde{f} 是良好定义的并且满足要求。

注 满足命题要求的 \tilde{f} 是唯一的。这个命题会始终贯穿我们的课程（用来构造映射）。

B.2 偏序关系与 Zorn 引理

对于集合 A ， A 上的一个序关系指的是 $A \times A$ 的子集 \mathcal{O} ，对于 $(a, b) \in \mathcal{O}$ ，我们把它写成 $a \leq b$ ，并且如下的性质成立：

- 1) (自反性) 对任意的 $a \in A$ ， $a \leq a$ （或者对任意的 $a \in A$ ， $(a, a) \in \mathcal{O}$ ）；
- 2) (传递性) 如果 $a \leq b$ ， $b \leq c$ ，那么， $a \leq c$ （或者如果 $(a, b), (b, c) \in \mathcal{O}$ ，那么， $(a, c) \in \mathcal{O}$ ）。
- 3) 对任意的 $a, b \in A$ ，如果 $a \leq b$ ， $b \leq a$ ，那么， $a = b$ （或者如果 $(a, b), (b, a) \in \mathcal{O}$ ，那么， $a = b$ ）。

注 偏序的偏一字，指的对于 $a, b \in A$ ，我们未必可以比较它们的大小，即 $a \leq b$ 和 $b \leq a$ 可能都不成立。如果对任意的 $a, b \in A$ ， $a \leq b$ 和 $b \leq a$ 至少一者成立，我们称之为全序集。

给定偏序集 (A, \leq) 以及 A 的子集 $S \subset A$ 。如果 $a \in A$ ，使得对任意的 $s \in S$ ，均有 $s \leq a$ ，我们称 a 是 S 的一个上界；如果进一步 $a \in S$ ，我们就称 a 是 S 的最大元。很明显，最大元如果存在必然唯一。类似地，我们可以定义下界和最小元。

给定偏序集 (A, \leq) ，如果 A 的每个子集 S 都有最小元，我们就称之为良序集。很明显，良序集是全序集合（考虑具有两个元素的子集）。对于良序集，我们有超限归纳法：

定理 B.1 (超限归纳法)

(A, \leq) 是良序集， $S \subset A$ 为子集。做作如下假设：给定 $a \in A$ ，假设条件 $x < a$ 可以推出 $x \in S$ ，那么，这样的 $a \in S$ 。那么， $S = A$ 。



注 符号 $x < a$ 指的是 $x \leq a$ 但是 $x \neq a$ 。

证明 如若不然，令 a_0 为 $A - S$ 的最小元，特别的， $a_0 \in A - S$ 。那么，对任意的 $x \leq a_0$ ($x \neq a_0$)，由于 a_0 为最小元，所以 $x \notin A - S$ ，从而， $x \in S$ 。按照要求， $a_0 \in S$ ，矛盾。

给定偏序集 (A, \leq) ， $I \subset A$ 是子集，如果对任意 $x \in I$ ，对任意的 $y \leq x$ ，都有 $y \in I$ ，我们就称 I 是一个左半轴。如果 \leq 是全序，对任意的 $x \in A$ ， $A_x = \{y \in A | y < x\}$ 是一个左半轴。

我们还可以定义 S 的极大元。假设 $s \in S$ 并且在 S 中不能找出其它的 $s' \in S$ ，使得 $s \leq s'$ ，我们就称 s 是 S 的一个极大元。类似地，我们可以定义极小元。极大元和极小元即是存在也未必唯一。

定理 B.2 (Zorn 引理)

(A, \leq) 是偏序集，如果任意全序子集^a $S \subset X$ 都有上界，那么， A 有极大元。

^a即在 S 我们仍然使用 A 的偏序，此时对 S 而言它是全序集



证明 用反证法，假设 A 中无极大元。令 $\mathcal{S} = \{S \subset A | S \text{ 是全序子集}\}$ 。对每个 $S \in \mathcal{S}$ ，令 a 为 S 的一个上界，由于 A 没有最大元素，所以存在 $a < b$ ，那么， b 也是 S 的上界并且 $b \notin S$ 。我们定

义

$$\mathcal{T} = \{(S, b) \mid S \in \mathcal{S}, b \text{ 是 } S \text{ 的上界并且 } b \notin S\}.$$

我们考虑满射

$$\pi: \mathcal{T} \rightarrow \mathcal{S}, (S, b) \mapsto S.$$

根据选择公理¹，存在映射 $\ell: \mathcal{S} \rightarrow \mathcal{T}$ ，使得 $\ell \circ \pi = \text{id}_{\mathcal{S}}$ ，即对任意的全序子集 S ，我们指定其上界 $\ell(S)$ 并且 $\ell(S) \notin S$ 。

对于子集 $W \subset A$ ，如果 W 是良序集（从而落在 \mathcal{S} 中）并且对任意的 $x \in I$ ， $\ell(W_x) = x$ ，我们就称 I 满足性质 (ℓ) 。我们现在说明，如果 W 和 W' 为满足性质 (ℓ) 的子集，那么，如下两种情形必居其一：

- 1) $W \subset W'$ 并且 W 是 W' 中的一个左半轴；
- 2) $W' \subset W$ 并且 W' 是 W 中的一个左半轴。

- 证明这个叙述：令 $\mathcal{J} = \{I \subset W \cap W' \mid I \text{ 是 } W \text{ 中的左半轴也是 } W' \text{ 中的左半轴}\}$ ，很明显， $J = \bigcup_{I \in \mathcal{J}} I \in \mathcal{J}$ 而且是在包含关系下的最大元。若 $J = W$ ，那么 1) 成立；如果 $J = W'$ ，那么 2) 成立。否则，存在 $w \in W - J$ ，使得 w 是 $W - J$ 中的最小元素；存在 $w' \in W' - J$ ，使得 w' 是 $W' - J$ 中的最小元素。根据定义，我们就有 $J = W_w$ 和 $J = W'_{w'}$ 。由于 J 满足性质 (ℓ) ，所以， $w = \ell(W_w) = \ell(W'_{w'}) = w'$ 。此时， $J \cup \{w\} \in \mathcal{J}$ ，与 J 是最大元相矛盾。

以下令 W 为 A 中所有满足性质 (ℓ) 的集合的并集，我们来说明 W 也满足性质 (ℓ) 。

首先说明 W 是良序集：对任意的 $V \subset W$ ，假设 X 满足性质 (ℓ) 并且 $X \cap V \neq \emptyset$ ，那么， $V \cap X$ 有最小元 x ，我们现在说明 x 是 V 的最小元：对任意的 $v \in V$ ，存在满足性质 (ℓ) 的 Y ，使得 $v \in Y$ 。根据前面所证，要么 $X \subset Y$ 并且 X 是 Y 中的一个左半轴，要么 $Y \subset X$ 并且 Y 是 X 中的一个左半轴。无论哪种情况， x 既然是 $V \cap X$ 的最小元，也是 $V \cap Y$ 有最小元，从而， $x \leq v$ 。

其次，我们说明对任意的 $x \in W$ ，都有 $\ell(W_x) = x$ ：假设 X 满足性质 (ℓ) 并且 $x \in X$ ，所以， $X_x \subset W_x$ （因为 $X \subset W$ ）。对任意的 $y \in W$ ， $y < x$ ，存在满足性质 (ℓ) 的 Y ，使得 $y \in Y$ 。如果 $Y \subset X$ 并且 Y 是 X 中的一个左半轴，那么， $y \in X$ ，从而 $y \in X_x$ ； $X \subset Y$ 并且 X 是 Y 中的一个左半轴，那么， $X_x = Y_x$ ，然而 $y \in Y_x$ ，所以， $y \in X_x$ 。总之， $X_x = W_x$ ，所以， $\ell(W_x) = \ell(X_x) = x$ 。

现在考虑 $W \cup \{\ell(W)\}$ ，很明显它也满足性质 (ℓ) ，这与 W 是最大的这样的集合相矛盾。

¹ X 是集合，对任意的 $x \in X$ ， $F(x)$ 是非空集合。那么，对每个 x ，我们可以指定 $f(x) \in F(x)$ 。