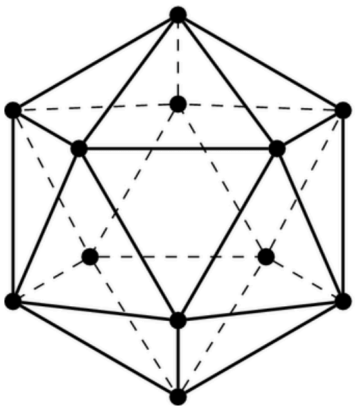
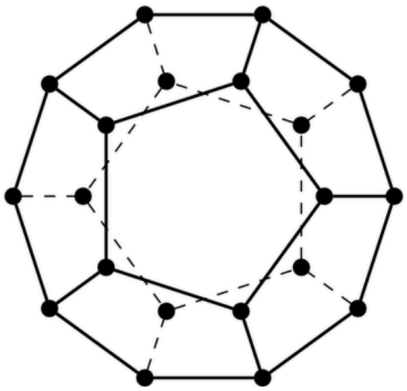
群与 Galois 理论

清华大学数学科学系与致理书院 2024 年秋季学期《抽象代数》讲义





于 品

2024 年 12 月 31 日

目录

前言

这份讲义按实际授课顺序与课堂板书，复述了 2024 年清华大学数学系与致理书院的必修课《抽象代数》秋季学期的全部内容。在前一年讲义的基础上，这次增加了更多例子、习题和打印错误，授课顺序也有调整，但其主旨还可沿用去年的说辞：每门合格的数学课程，都需要交代课题背后的动机与核心概念，并通过讲解真正重要的例子使学习者掌握基本的思考方式和计算技术。在此之上，最重要的一点是展现该课程与其他学科的关联，尤其是与当下研究前沿的内在逻辑。由于我的科研与代数前沿几乎垂直，我平时极少用到更为现代的代数工具，课堂上无法对与代数相关的最新科研成果做出引导性的评注，所能做的仅是在一些经典例子和计算上花心思，确实不能尽如人意。即使如此，过去两年备课过程中，我也积累了一些新的思考，尤其是如何取舍相关的素材。对一份讲义而言，前言部分似乎是记录这些思考的合适位置：一方面，可以展示课程内容的选择标准；另一方面，也不耽误具有不同数学标准和学术品味的同学的时间，他们可以选择其它风格的讲义。

围绕群、环、域的概念展开的《(抽象) 代数》是目前国内外数学系中非常成熟的课程，所涉及的概念和定理相对固定。考虑到一学期共 64 课时（清华的授课安排）以及同学们课后被各种通识课消耗的精力，课程内容难以有太多延展的空间。一种可能的尝试是在同样的内容下采取尽量现代的框架，特别是范畴论的语言。这种做法与当下数学系的学习风气相契合，相当数量的同学致力于“卷”所谓更抽象的理论。他们似乎过于认同工具的重要性，迷信更高级的数学概念可以轻松地解决相对初等和繁琐的问题。这也是我与同学们接触过程中感受到的一个重要印象。因此，在课堂上我们做了一些反向尝试，目的是鼓励同学们进行深度思考，并最终享受思考的过程，而知识的积累和数学语言的更新则水到渠成。具体来说，我们增加了大量例子，力图在多个场合将新概念与线性代数、射影几何、初等数论等已经熟知的领域相结合，通过在传统内容中运用新工具，帮助同学们更好地理解和掌握这些新概念。例如证明正二十面体的对称群是 5 个元素的偶置换群 $\mathfrak{A}_5$，例如展示 Galois 如何通过正二十面体将 $\mathfrak{A}_5$ 实现为有限域 $\mathbb{F}_{11}$ 上的射影变换群 $\mathbf{PSL}(2;\mathbb{F}_{11})$ 的子群，再例如利用 Fano 平面实现 $\mathbf{GL}(3;\mathbb{F}_2)$ 与 $\mathbf{PSL}(2;\mathbb{F}_7)$ 之间的例外同构。我的经验是，数学学习往往容易偏执于知识的积累，在一味的阅读中养成被动的学习习惯，忘记了子曰的“学而不思则殆”。没有前期深入思考的支撑，随着学问深度和难度的提升，疲惫感会慢慢积累，越来越力不从心，这样就慢慢消耗掉对数学的热爱。因此，在作业设计上我们尽量选择既重要又富有审美价值、且充满趣味的问题，目的是希望同学们能够通过思考踏实地掌握基础内容，体验到这些问题的美妙，从而在内心深处积蓄对数学的情感。

在组织讲义材料时，我倾向于选择那些在数学史上有故事的例子，认为这些有渊源的思想能让抽象的理论生气勃勃。中学时曾和父亲闲聊起那首“敕勒川，阴山下，天似穹庐，笼盖四野”的著名北朝民歌，当时我认为这首诗只写了水草丰美与山河壮丽，并未理解它为何如此出色。类似的情境，我后来在数学学习中也常遇到，即便搞懂了某些定理的每个细节，由于不了解它在体系中的位置，总觉得难以把握其背后的图像。记得父亲当时抿一下嘴说“我们讲讲敕勒歌的故事吧”，于是时空转到北朝时东魏大枭雄高欢暮年的最后一次远征，被西魏的韦孝宽挡在玉壁城外，苦苦围攻五十多天，无计可施，粮草殆尽，人马困乏，士卒死伤七万人。高欢由此大病，恰有流星坠入营地，流言四起，士气低落，军心动荡。高欢于是强忍病痛勉强正坐，大会将士以安军心。大将斛律金作敕勒歌，高欢也跟着唱起来，三军哀感流涕。有了这段历史，再读敕勒歌，敕勒川的蓝天、白云、无边的草原和成群的牛羊之间又鼓荡了英雄气概。这也是在课堂和讲义中提到历史背景的原因，希望同学们能从中感受到数学历史中的“天苍苍，野茫茫”。当然，我还记得父亲说：“高欢和斛律金是鲜卑人，在北边长大的，唱敕勒歌流泪的时候应该是想到了小时候的草原吧”。

2024 年 12 月 31 日。

引子

考虑二次方程

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

其中，系数 $a, b \in \mathbb{Q}$。通过代换 $X = Y - \frac{a}{2}$（配方），可以消去一次项从而将方程转变为

$$X^2 + b' = 0. \tag{0.1}$$

这里，b' 由 a 和 b 通过确定的代数运算所给出。对于方程(0.1)，可以使用开方运算来给出它的解。综合这一系列操作，我们可以给出二次方程的求根公式

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

对于三次方程

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

其中，系数 $a, b, c \in \mathbb{Q}$，我们仍可以通过代换 $X = Y - \frac{a}{3}$ 消去二次项。据此，不妨假设方程形如

$$X^3 + aX + b = 0. \tag{0.2}$$

方程(0.2)的三个根可以用如下的 Cardano[1]求根公式表达：

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

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

例子 0.1. 考虑方程

$$X^3 - X - 6 = 0.$$

容易看出，2 是这个方程的根。直接套用 Cardano 公式，这个根的表达如下：

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

然而，除非做一些详细的计算，要想看出以上表达式实际恰为 2 并不容易。由此可见，直接应用求根公式可能是效率不太高的代数操作。

注记 0.1 (三次方程求根公式的推导：一种想法)**.** 我们通过增加一个自由度的方式来解方程：令 $X = u + v$，即用两个变量 u 和 v 来表示一个变量 X。此时，方程(0.2)可以写成：

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

这个方程有解的一个充分条件是

$$\begin{cases} u^3 + v^3 + b = 0, \\ 3uv + a = 0. \end{cases} \tag{0.3}$$

[1] $k = 0$ 所对应的求根公式最早由 del Ferro 发现。

它自然等价于

$$\begin{cases} u^3 + v^3 = -b, \\ u^3 \cdot v^3 = -\frac{a^3}{27}. \end{cases} \tag{0.4}$$

根据 Vieta 公式，u^3 与 v^3 可被视作是二次方程

$$Y^2 + bY - \frac{a^3}{27} = 0$$

的解，根据二次方程的求根公式，我们可以解出 u^3 与 v^3 并进一步给出 u, v 以及 $X = u + v$。

我们还可以进一步研究四次方程

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

其中，系数 $a, b, c, d \in \mathbb{Q}$。四次方程仍然有求根公式，这是 Cardano 的学生 Ferrari 的工作，其关键想法是**凑平方差**，从而把问题约化为三次方程的求根。

首先，待定一个参数 ξ，利用 $X^2 + \frac{a}{2}X + \xi$ 的平方来代换掉 X^4 与 aX^3 这两个高次项，即

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

从而，

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

我们**希望**上式右边中括号一项是完全平方式，即

$$(2\xi + \frac{a^2}{4} - b)X^2 + (a\xi - c)X + (\xi^2 - d) = (\alpha X + \beta)^2. \tag{0.5}$$

在这个假设下，通过因式分解，原来的四次方程等价于

$$\left(X^2 + \frac{a}{2}X + \xi + (\alpha X + \beta)\right)\left(X^2 + \frac{a}{2}X + \xi - (\alpha X + \beta)\right) = 0.$$

此时，我们只要求解两个二次方程就可以给出原四次方程的解。最终，我们写下(0.5)为完全平方的条件，即这个二次多项式的判别式为 0：

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

这是关于 ξ 的三次方程，所以，我们还需要使用 Cardano 公式来求解 ξ。

以上的讨论给出了不超过四次的代数方程的根式解。然而，Abel 在 1824 年证明了不能通过对方程系数加、减、乘、除和开若干次方的运算来表示五次方程的根，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 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 域与线性空间

定义 1.1 (域的定义)**.** K 是集合并且至少有 2 个元素。如果 K 上定义了**乘法** $\cdot$ 和**加法** $+$，即映射

$$K \times K \to K, \quad (a,b) \mapsto a+b,$$

和

$$K \times K \to K, \quad (a,b) \mapsto a \cdot b,$$

并且存在元素 $0_K, 1_K \in K$，$0_K \neq 1_K$，使得如下公理成立：

1) – 0_K 是加法单位元，即对任意的 $a \in K$，有

$$0_K + a = a + 0_K = a;$$

– 加法满足结合律，即对任意的 $a_1, a_2, a_3 \in K$，有

$$(a_1 + a_2) + a_3 = a_1 + (a_2 + a_3);$$

– 加法满足交换律，即对任意的 $a, b \in K$，有

$$a + b = b + a;$$

– 加法有逆元，即对任意的 $a \in K$，存在 $-a \in K$，使得

$$a + (-a) = 0_K.$$

2) – 1_K 是乘法单位元，即对任意的 $a \in K$，有

$$1_K \cdot a = a \cdot 1_K;$$

– 乘法满足结合律，即对任意的 $a_1, a_2, a_3 \in K$，有

$$(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3);$$

– 乘法满足交换律，即对任意的 $a, b \in K$，有

$$a \cdot b = b \cdot a;$$

– 乘法具有逆元，即对任意的 $a \in K^\times := K - \{0\}$，存在 $a^{-1} \in K$，使得

$$a \cdot a^{-1} = 1_K.$$

3) 乘法和加法满足乘法分配律：对任意的 $a_1, a_2, a_3 \in K$，有

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

就称 $(K, \cdot, +)$ 或 K 是一个**域**。

注记 1.1. 在法语数学文献中，域的定义并不要求乘法交换。然而，绝大多数的数学情景下我们遇到的域都是交换的。另外，我们将在作业中证明著名的 Wedderburn 定理：K 是有限域[2]（不假设乘法交换性），那么 K 的乘法是交换的。

注记 1.2 (记号的澄清)**.** 有以下几个简单的事实：

- 通常用 ab 表示 $a \cdot b$。
- 通常把 $0_K, 1_K$ 简写成 $0, 1$。我们还用 -1 表示 -1_K。
- 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，我们还把它写成 $\frac{1}{b}$。
- 对任意的 $a \in K$，$0 \cdot a = a \cdot 0 = 0$。
- 对任意的 $a \in K$，$(-1) \cdot a = -a$。
- 用 $a - b$ 表示 $a + (-b)$。利用结合律容易证明 $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$，我们把它简写为 $-a \cdot b$ 或者 $-ab$。
- 用 $\frac{a}{b}$ 表示 $a \cdot b^{-1} = a \cdot \frac{1}{b}$。

例子 1.1. $\mathbb{Q}, \mathbb{R}$ 和 $\mathbb{C}$ 配备上通常的乘法和加法运算均为域。

例子 1.2. p 是素数。我们用 $\mathbb{Z}/p\mathbb{Z}$ 表示整数集除 n 的同余类，即

$$\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{p-1}\},$$

其中，$\overline{k} = \{m \in \mathbb{Z} | m \equiv k \pmod{p}\}$，$k = 0, \cdots, p-1$。换而言之，我们在 $\mathbb{Z}$ 上定义等价关系 $\sim$，其中，$m \sim n$ 当且仅当 $m \equiv n \pmod{p}$，那么，$\mathbb{Z}/p\mathbb{Z} := Z/\sim$。对于任意的 $l \in \mathbb{Z}$，用 $\overline{l}$ 表示它在 $\mathbb{Z}/p\mathbb{Z}$ 所对应的同余类。

在 $\mathbb{Z}/p\mathbb{Z}$ 上定义加法：对任意的 $k, l \in \mathbb{Z}$，规定 $\overline{k} + \overline{l} = \overline{k+l}$。容易验证，这是良好定义的，即这个定义不依赖于等价类中代表元的选择：如果 $\overline{k} = \overline{k'}, \overline{l} = \overline{l'}$，那么，$\overline{k+l} = \overline{k'+l'}$。这样定义的加法显然是交换的并且 $\overline{0}$ 是加法单位元。

在 $\mathbb{Z}/p\mathbb{Z}$ 上定义乘法：对任意的 $k, l \in \mathbb{Z}$，规定 $\overline{k} \cdot \overline{l} = \overline{k \cdot l}$。这是也良好定义的并且这个乘法是交换的，$\overline{1}$ 是乘法单位元。为了说明乘法有逆元，考虑任意的非零元 $\overline{k} \in \mathbb{Z}/p\mathbb{Z}$。由于 p 是素数，所以，$k\ p) = 1$（互素）。根据 Bézout 定理，存在 $a, b \in \mathbb{Z}$，使得 $ak + bp = 1$。那么，在 $\mathbb{Z}/p\mathbb{Z}$ 中，就有 $\overline{ak} = 1$，即 $\overline{a}\overline{k} = 1$。这表明 k 有逆元 a。

综上所述，$\mathbb{Z}/p\mathbb{Z}$ 配有以上定义的加法和乘法是域。

对素数 p，约定 $\mathbb{F}_p$ 表示域 $\mathbb{Z}/p\mathbb{Z}$。这是有限域，因为 $|\mathbb{F}_p| = p$。

[2]如果域 K 的元素个数是有限的，就称 K 是有限域。

定义 1.2 (域上的线性空间)**.** K 是域，V 是非空集合。如果 V 上配备了加法 $+$ 以及 K 对 V 的乘法，即映射

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

和

$$K \times V \to V, \ \ (k, v) \mapsto k \cdot v,$$

以及元素 $0_V \in V$，使得

1) – 加法满足结合律，即对任意的 $v_1, v_2, v_3 \in V$，有

$$(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3).$$

– 加法满足交换律，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) – 乘法满足结合律，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

$$1_K \cdot v = v.$$

– 乘法满足分配律：对任意的 $a_1, a_2, a \in K$ 和 $v_1, v_2, v \in V$，有

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

就称 V 是K **上的线性空间**或K**-线性空间**。

注记 1.3. 线性代数课程中我们讨论的线性空间通常定义在 $\mathbb{Q}, \mathbb{R}$ 或者 $\mathbb{C}$ 上。由于课程中基本概念与定理，譬如矩阵、行列式、线性映射、线性子空间、线性无关性、维数、基的存在性定理等只用到了以上域上的四则运算（加减乘除），所以，这些概念可以平行地搬到 K-线性空间上。

例子 1.3 (射影空间 $\mathbf{P}(V)$)**.** 给定 K-线性空间 V，$\dim_K V \geqslant 1$，令

$$\mathbf{P}(V) := \big\{ L \subset V \big| L \text{ 是 } 1 \text{ 维线性子空间} \big\}.$$

这是 V 中过原点的直线的集合。对于 $V^\times = V - \{0_V\}$，我们定义等价关系 $\sim$，其中，$v_1 \sim v_2$ 当且仅当存在 $k \in K^\times$，使得 $v_1 = k \cdot v_2$，那么，

$$\mathbf{P}(V) \simeq {}^{V^\times}\!/_{\sim}.$$

对于 K-线性子空间 $W \subset V$，${}^{W^\times}\!/_{\sim} \subset \mathbf{P}(V)$ 被称作是 $\mathbf{P}(V)$ 的一个**线性子空间**，其**维数**被定义为 $\dim_K W - 1$。当 $\dim_K W = 2$ 或 3 时，${}^{W^\times}\!/_{\sim}$ 分别被称作是 V 中的**直线**或**平面**。

假设 V 是 $n+1$ 维 K-线性空间，$(e_0,\cdots,e_n)$ 为 V 的一组基，那么，对任意的 $v=k_0e_0+k_1e_1+\cdots+k_ne_n\in V^\times$，其中，$k_0,k_1,\cdots,k_n$ 不全为 0，我们用 $[k_0:k_1:\cdots:k_n]$ 表示 v 的等价类，即过 v 的线性子空间。我们称 $[k_0:k_1:\cdots:k_n]$ 为 $\mathbf{P}(V)$ 上的**齐次坐标**。对任意的 $k\in K^\times$，显然有

$$[k_0:k_1:\cdots:k_n]=[k\cdot k_0:k\cdot k_1:\cdots:k\cdot k_n].$$

如果 K 是有限域，V 是有限维 K-线性空间，那么，$\mathbf{P}(V)$ 是有限集。我们将看到，这个集合将会提供很多有趣的群的例子。

练习 1.1. 给定射影空间 $\mathbf{P}(V)$，其中，V 是 K-线性空间。证明如下的性质：

1) 对任意两个不同的点 $x,x'\in\mathbf{P}(V)$，存在唯一的直线 $\ell\subset\mathbf{P}(V)$，使得 $x,x'\in\ell$。

2) 对任意两条不同的直线 $\ell,\ell'\subset\mathbf{P}(V)$，它们恰有一个交点。

3) 对任意两条不同的直线 $\ell,\ell'\subset\mathbf{P}(V)$，存在唯一的平面 $P\subset\mathbf{P}(V)$，使得 $\ell,\ell'\subset P$。

例子 1.4. 当 $K=\mathbb{F}_p$，$V=(\mathbb{F}_p)^2$ 时，$\mathbf{P}^1(\mathbb{F}_p):=\mathbf{P}(V)$，这个集合有 $p+1$ 个元素。

当 $K=\mathbb{F}_p$，$V=(\mathbb{F}_p)^{n+1}$ 时，$\mathbf{P}^n(\mathbb{F}_p):=\mathbf{P}(V)$，那么，

$$|\mathbf{P}^n(\mathbb{F}_p)|=\frac{p^{n+1}-1}{p-1}.$$

练习 1.2. 假设 $|K|=q$，$\mathbf{P}^{n-1}(K):=\mathbf{P}(K^n)$。

1) 证明，$\mathbf{P}^{n-1}(K)$ 的 $m-1$ 维线性子空间的个数为：

$$\begin{bmatrix}n\\m\end{bmatrix}_q:=\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})}{(q^m-1)(q^m-q)\cdots(q^m-q^{m-1})}.$$

2) 给定 $\mathbf{P}^{n-1}(K)$ 的 $l-1$ 维线性子空间 $\mathbf{P}(W)$，证明，$\mathbf{P}^{n-1}(K)$ 中包含 $\mathbf{P}(W)$ 的 $m-1$ 维线性子空间的个数为 $\begin{bmatrix}n-l\\m-l\end{bmatrix}_q$。

3) 证明，对 $k\leqslant n$，有如下恒等式

$$\begin{bmatrix}n\\k\end{bmatrix}_q+q^{n-k+1}\begin{bmatrix}n\\k-1\end{bmatrix}_q=\begin{bmatrix}n+1\\k\end{bmatrix}_q.$$

4) 证明，对 $n\geqslant 1$，有如下的多项式恒等式

$$\prod_{k=0}^{n-1}(1+q^kX)=\sum_{k=0}^{n}q^{\frac{k(k-1)}{2}}\begin{bmatrix}n\\k\end{bmatrix}_q X^k.$$

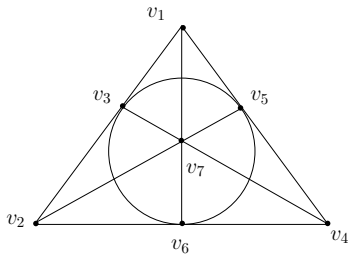
（这个等式被称作是 q-二项式展开，将 q 看作是变量，试考虑 $q\to 0$ 的极限。）

例子 1.5 (Fano 平面)**.** 给定三个不同的点 $l,l',l''\in\mathbf{P}(V)$，如果它们对应的 V 的 3 个 1 维线性子空间张成的空间维数为 2，我们就称 l,l',l'' **共线**。

用 0 和 1 表示 $\mathbb{F}_2$ 中元素，此时，$\mathbf{P}^2(\mathbb{F}_2):=\mathbf{P}(V)$ 有 7 个元素，每个元素都对应 $(\mathbb{F}_2)^3$ 中的一个非零向量，它们可以用坐标列举如下：

$$v_1=(0,0,1),\quad v_2=(0,1,0),\quad v_3=(0,1,1),$$
$$v_4=(1,0,0),\quad v_5=(1,0,1),\quad v_6=(1,1,0),\quad v_7=(1,1,1).$$

我们用如下的图表示 $\mathbf{P}^2(\mathbb{F}_2)$：

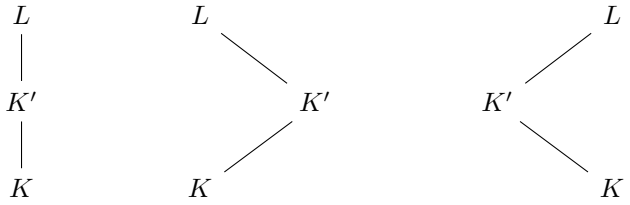


以上图中有 6 条直线段，每条这样的线段上的三个点都是共线的；图中圆形所经过的三个点也是共线的。

1.2 域扩张

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 $a,b \in K$，有 $a+b \in K$ 和 $a \cdot b \in K$）并且 K 对加法逆和乘法逆也封闭（即对任意的 $a,b \in K$ 和 $b \neq 0$，有 $-a \in K$ 和 $b^{-1} \in K$），就称 K 为 L 的**子域**。此时，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（此时 K 显然为 K' 的子域），称 K' 为扩张 L/K 的**中间域**。我们通常用如下类型的交换图表示：



练习 1.3. 证明，在 L 的加法和乘法下，K 是域。如果不加说明，我们总默认在 K 上的乘法与加法均为 L 中的乘法与加法。

注记 1.4 (由子集生成的域)**.** 给定域扩张 L/K，$\{K'_i\}_{i\in I}$ 是一族中间域，那么 $\bigcap\limits_{i\in I} K'_i$ 也是 L 的中间域。

根据这个性质，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[3]子域，我们把它称作是**由 M 所生成的子域**。如果 M 是有限集 $\{m_1,\cdots,m_k\}$，我们也把 $K(M)$ 记成 $K(m_1,\cdots,m_k)$。如果 $L=K(M)$ 并且 M 是有限集，那么域扩张 L/K 被称作是**有限型的**或**有限生成的**。

给定域 K,我们用 $K[X_1,X_2,\cdots,X_n]$ 表示 K 上的所有 n-元(n-个变量的多项式)。对于 $P \in K[X_1,\cdots,X_n]$，它形如

$$P(X_1,\cdots,X_n)=\sum_{\text{有限个 }\alpha} a_\alpha \cdot X_1^{\alpha_1}X_2^{\alpha_2}\cdots X_n^{\alpha_n}=\sum_{\text{有限个 }\alpha} a_\alpha \cdot X^\alpha,$$

其中，$a_\alpha \in K$，$\alpha=(\alpha_1,\cdots,\alpha_n)$ 是一个多重指标，$\alpha_i \in \mathbb{Z}_{\geqslant 0}$ 并且 $X^\alpha = X_1^{\alpha_1}X_2^{\alpha_2}\cdots X_n^{\alpha_n}$。

我们强调多项式与多项式函数是不同的代数对象，尽管多项式可以被视作是函数（映射）：给定域扩张 L/K 和 $P \in K[X_1,\cdots,X_n]$，定义

$$P: L^n \to L,\ \ (x_1,\cdots,x_n) \mapsto P(x_1,\cdots,x_n) := \sum_{\text{有限个 }\alpha} a_\alpha \cdot x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}.$$

[3]在包含关系下

命题 1. 给定域扩张 L/K, $M \subset L$ 是子集。那么, $K(M)$ 恰为 L 中形如 $\dfrac{P(x_1,\cdots,x_n)}{Q(x_1,\cdots,x_n)}$ 的元素, 其中, $n \geqslant 0$, $P,Q \in K[X_1,\cdots,X_n]$ 是 K-系数的 n 元多项式, $x_1,\cdots,x_n \in M$ 并且 $Q(x_1,\cdots,x_n) \neq 0$。

证明: 定义 L 的子集

$$K' = \left\{ \frac{P(x_1,\cdots,x_n)}{Q(x_1,\cdots,x_n)} \middle| P,Q \in K[X_1,\cdots,X_n], x_1,\cdots,x_n \in M \text{ 并且} Q(x_1,\cdots,x_n) \neq 0 \right\}.$$

首先证明 $K' \subset K(M)$。由于 $x_1,\cdots,x_n \in M \subset K(M)$ 并且在加减和乘法下 $K(M)$ 是封闭的, 所以, 对任意的 $P,Q \in K[X_1,\cdots,X_n]$, $P(x_1,\cdots,x_n), Q(x_1,\cdots,x_n) \in K(M)$。$K(M)$ 在除法下封闭表明 $\dfrac{P(x_1,\cdots,x_n)}{Q(x_1,\cdots,x_n)} \in K(M)$。从而, $K' \subset K(M)$。

由于 $K(M)$ 是包含 M 的最小的中间域, 只要证明 K' 是域即可。这是显然的, 因为形如 $\dfrac{P(x_1,\cdots,x_n)}{Q(x_1,\cdots,x_n)}$ 的元素在四则运算下仍然可以表达成这种形式。 □

注记 1.5 (有限性)**.** 对任意的 $M \subset L$, 我们有

$$K(M) = \bigcup_{\substack{F \subset M \\ F \text{ 是有限集}}} K(F).$$

实际上, $K(M)$ 中的每个元素都形如 $\dfrac{P(x_1,\cdots,x_n)}{Q(x_1,\cdots,x_n)}$, 它被包含由 M 中的一个有限集 $F = \{x_1,\cdots,x_n\}$ 所生成的子域中。

类似的, 对任意 L 中的子集 M 和 N, 我们有

$$K(M \cup N) = K(M)(N) = K(N)(M).$$

注记 1.6 (线性空间结构)**.** 给定域扩张 L/K, L 上的加法和以及 K 中元素与 L 种元素的乘法, 给出了 L 的 K-线性空间结构。

实际上, 对任意的 $a,b,c \in K$ 和 $x,y,z \in L$, 有

$$a \cdot (x+y) = a \cdot x + a \cdot y,\ a \cdot (b \cdot x) = (ab) \cdot x,\ (a+b) \cdot x = a \cdot x + b \cdot y.$$

这验证了 L 作为 K-线性空间的基本公理。

如果 $\dim_K L < \infty$, 就称 L 是 K 的**有限扩张**。我们称 $\dim_K L$ 为扩张 L/K 的**次数**并记作 $[L:K]$。

作为 K-线性空间的一组基 $\{e_i\}_{i \in I} \subset L$ 被称作是 L/K 的一组基。

例子 1.6. $\mathbb{C}/\mathbb{Q}$ 是域扩张, $\mathbb{R}$ 是一个中间域。

$\mathbb{C}/\mathbb{R}$ 是有限扩张并且 $[\mathbb{C}:\mathbb{R}] = 2$。实际上, 我们可以选取 $\{1, \sqrt{-1}\}$ 作为该扩张的基。

$\mathbb{R}/\mathbb{Q}$ 是不是有限扩张, 最简单的证明是观察到 $\mathbb{R}$ 是不可数集即可。

例子 1.7. 选定整数 D, D 不是完全平方数, 此时 $\sqrt{D}$ 不是有理数。考虑所有的形如 $x + y\sqrt{D}$ 的数:

$$\mathbb{Q}(\sqrt{D}) = \left\{ x + y\sqrt{D} \middle| x,y \in \mathbb{Q} \right\}.$$

由于 $\sqrt{D} \notin \mathbb{Q}$, 所以, $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{D}) \subset \mathbb{R}$。

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 $x = a, y = b$。

我们验证 $\mathbb{Q}(\sqrt{D})$ 在 ($\mathbb{C}$ 的) 四则运算下封闭:

- $\mathbb{Q}(\sqrt{D})$ 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。

  利用乘法封闭性，只要说明若 $a+b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$，则 $\frac{1}{a+b\sqrt{D}} \in \mathbb{Q}(\sqrt{D})$ 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 $\frac{1}{a+b\sqrt{D}} \in \mathbb{Q}(\sqrt{D})$。

以上证明了 $\mathbb{Q}(\sqrt{D})$ 是 $\mathbb{C}$ 的子域。实际上，$\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ 的次数为 2，其中，$\{1, \sqrt{D}\}$ 是一组基。

命题 2. 给定域扩张 L/K 和 E/L，E/K 是有限扩张当且仅当 E/L 和 L/K 均为有限扩张。

$$\begin{array}{c} E \\ | \\ L \\ | \\ K \end{array}$$

在此前提下，我们还有公式

$$[E:K] = [E:L][L:K].$$

证明：如果 E/K 是有限扩张，由于 L 是 E 的 K-线性子空间，所以 L/K 是有限扩张；而对于 E（作为 K-线性空间）的一组基 $\{v_i\}_{1\leqslant i\leqslant m}$，由于 $K \subset L$，它们的 L-线性组合显然张成 E，从而，E 也是有限维的 L-线性空间。

现在假设 E/L 和 L/K 是有限维的，选取 $\{v_i\}_{1\leqslant i\leqslant m}$ 是 E/L 的基，$\{w_i\}_{1\leqslant j\leqslant n}$ 是 L/K 的基。我们只要证明 $\{v_i \cdot w_j\}_{\substack{1\leqslant i\leqslant m \\ 1\leqslant j\leqslant n}}$ 是 E/K 的基即可，其中，$v_i \cdot w_j$ 是在 E 中相乘：

- $\{v_i \cdot w_j\}_{\substack{1\leqslant i\leqslant m \\ 1\leqslant j\leqslant n}}$ 是 K-线性无关的：如果 $\{\lambda_{i,j}\}_{\substack{1\leqslant i\leqslant m \\ 1\leqslant j\leqslant n}} \subset K$，使得 $\sum\limits_{i,j} \lambda_{i,j} v_i \cdot w_j = 0$，通过调整求和顺序，我们有

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

  以上括号中的系数 $\sum_j \lambda_{i,j} w_j \in L$，根据 $\{v_i\}_{1\leqslant i\leqslant m}$ 是 E/L 的基，对任意的 i，我们都有

  $$\sum_j \lambda_{i,j} w_j = 0.$$

  再利用 $\{w_i\}_{1\leqslant j\leqslant n}$ 是 L/K 的基，从而对任意的 i, j，都有 $\lambda_{i,j} = 0$。这证明了线性无关性。

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

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

  这表明 $\{v_i \cdot w_j\}_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}}$ 张成了 E。

另外，以上推导自然给出了 $[E:K] = [E:L][L:K]$。证毕。 □

1.3 应用：三等分已知角

给定 $\mathbb{R}^2$ 的子集 $\mathscr{S}$，由 $\mathscr{S}$ 中两点 $A, B \in \mathscr{S}$ 所决定的直线被称为$\mathscr{S}$**-直线**；以 $\mathscr{S}$ 中某点 $O \in \mathscr{S}$ 为圆心、以 $|OA|$ 为半径所作的圆，其中 $A \in \mathscr{S}$，被称为$\mathscr{S}$**-圆**。

定义 1.4 (尺规可作性)**.** 给定 $\mathscr{S} \subset \mathbb{R}^2$，如果点 P 满足如下三个条件之一：

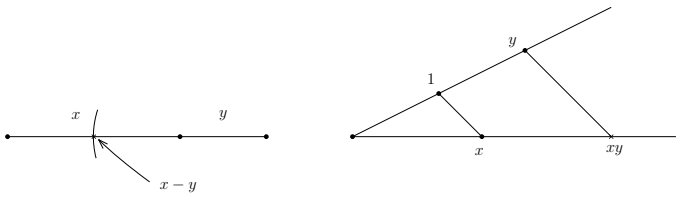
- P 是两条 $\mathscr{S}$-直线的唯一交点；
- P 是一条 $\mathscr{S}$-直线和一个 $\mathscr{S}$-圆的交点；
- P 是两个 $\mathscr{S}$-圆的交点；

就称 P 是$\mathscr{S}$**-直接可作的**。假设存在有限个点 $P_1, \cdots, P_m$，使得对任意的 $i \leqslant m$，P_i 是 $\mathscr{S} \cup \{P_1, \cdots, P_{i-1}\}$-直接可作的并且 $P_m = P$，就称 P 是$\mathscr{S}$**-可作的**。

令 $\mathscr{S}_0 = \{(0,0), (0,1)\} \subset \mathbb{R}$。如果 $x \in \mathbb{R}$ 是某个 $\mathscr{S}_0$-可作点的横坐标或者纵坐标，我们就称实数 x 是**尺规可作的**或者**可作的**。

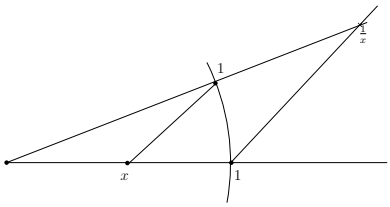
$\mathbb{R}$ 中尺规可作的数满足如下三条性质：

1) 若 x, y 是可作的，则 $x \pm y$ 和 $x \cdot y$ 可作。通过以下图示可以看出：



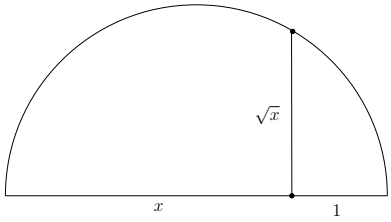
  其中，右图中需要做过 y 点的平行线。

2) 若 x, y 是可作的并且 $y \neq 0$，则 $\frac{x}{y}$ 可作。



根据 1)，只要按照上图的方式做出 $\frac{1}{x}$ 即可。

3) 若 x 是可作的，则 $\sqrt{x}$ 也可作。



注记 1.7. 从 $0,1$ 出发，根据前两条，$\mathbb{Q}$ 中的数是尺规可作的。

注记 1.8. 前两条表明尺规可作的数构成一个域。这是 $\mathbb{R}/\mathbb{Q}$ 的一个中间域。

定理 3 (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 $[K_i : K_{i-1}] = 2$ $(i = 1, \cdots, m)$ 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 4. *给定域扩张 L/K，$[L : K] = 2$。那么，存在 $x \in L$，$x^2 \in K$ 但是 $x \notin K$，使得 $\{1, x\}$ 是 L/K 的基。*

证明: 任选 $y \in L - K$，由于 $[L : K] = 2$，$\{1, y\}$ 是 L/K 的基。所以有 $a, b \in K$，使得

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

通过配方，$x = y - \frac{a}{2}$ 满足要求。 □

证明: 给定 $\mathscr{S} \subset \mathbb{R}^2$，假设 $\mathscr{S}$ 中所有点的横纵坐标都落在域 $K \subset \mathbb{R}$ 中。我们首先证明，如果 $P = (x, y)$ 是 $\mathscr{S}$-直接可作的，令 $L = K(x, y)$，那么 $[L : K] \leqslant 2$。注意到，我们可以把 $\mathcal{S}$-直线和 $\mathcal{S}$-圆写成以 K 的数为系数的方程的零点。

1) 若 P 是两条 $\mathcal{S}$-直线的交点，通过解两个 K-系数的线性方程联立所得到的方程组，其横纵坐标 x 和 y 仍是 K 中的数，从而 $K = L$，即 $[L : K] \leqslant 1$。

2) 如果 P 是 $\mathcal{S}$-直线和 $\mathcal{S}$-圆的交点。此时，需要解一个 K-系数的线性方程和一个 K-系数的二次方程的联立，可以通过先用线性方程代换掉一个变量，从而解一个一元二次方程来求得 x 或者 y。根据二次方程的求根公式，L 可以通过 K 添加该一元二次方程的判别式的平方根得到，即 $L = K[\sqrt{\Delta}]$，从而，$1, \sqrt{\Delta}$ 张成了 L。特别地，$[L : K] \leqslant 2$。

3) 如果 P 是两个 $\mathcal{S}$-圆的交点，它们对应的圆方程的二次项形如 $x^2 + y^2$。通过相减，就可以得到一个一次方程，这就化为前一情形。

从 $\mathbb{Q} = K_0$ 出发，通过有限步得到 (x, y)，上面的讨论表明每次添加新得到的数得到的域，如果与之前不同的话，扩张的次数必为 2。据此，我们得到

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

其中，$[K_i : K_{i-1}] = 2$，$i = 1, \cdots, m$。

反之，我们对 m 进行归纳。$m=0$ 时，命题自然成立。假设命题对小于 m 时均成立，对任意的 $x\in K_m$，存在 $a\in K_{m-1}$，使得 $(x-a)^2\in K_{m-1}$。根据归纳假设，$(x-a)^2$ 是尺规可作的。根据之前的讨论，$\pm\sqrt{(x-a)^2}$ 是尺规可作的，从而通过加减 a，x 也是可作的。 □

所谓的倍立方问题问是否可用尺规作出这样的长度，使得以该长度为棱长的立方体的体积恰为给定立方体的两倍？[4]

推论 5 (倍立方问题)**.** $\sqrt[3]{2}$ 不是尺规可作的。

证明: 我们使用反证法。若 $\sqrt[3]{2}$ 是尺规可作的，根据 Wantzel 的定理，存在子域 $K\subset\mathbb{R}$，使得 $\sqrt[3]{3}\in K$ 并且 $[K:\mathbb{Q}]=2^m$，$m\in\mathbb{Z}$。我们首先证明：

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

是 K 的子域，其中，如果令 $\alpha=\sqrt[3]{3}$，L 中的数均形如 $a+b\alpha+c\alpha^2$，这里，$a,b,c\in\mathbb{Q}$。根据 $\alpha^3=2$，L 中的数显然在加减和乘法下封闭，只要证明 $a+b\alpha+c\alpha^2$ 的倒数也在 L 中即可。实际上，我们 $x=a,y=b\alpha,z=c\alpha^2$ 代入下面的恒等式

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

容易看到，上式右边

$$d=a^3+b^3\alpha^3+c^3\alpha^6-3abc\alpha^3=a^3+2b^3+4c^3-6abc\in\mathbb{Q}.$$

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。 □

另一个著名的古典几何问题是研究是否可用尺规作出大小为给定角的三分之一的角？

推论 6 (三等分已知角)**.** $\cos(\frac{\pi}{9})$ 不是尺规可作的。特别地，不能通过尺规作图三等分 60° 的角。

证明: 由于 1 是尺规可作的，给定角度为 θ 的角等价于给出 $\cos(\theta)$。所以，三等分角度 θ 等价于研究 $\cos(\frac{\theta}{3})$ 是否尺规可作。根据三倍角公式，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，

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

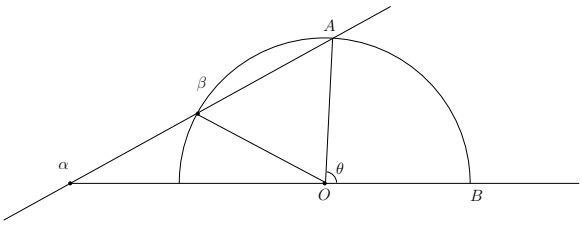
如果可以作 $\frac{\pi}{9}$ 的角，那么，就可以尺规作出以上方程的一个根（它有三个实数根）。通过考虑代换 $X=2x$，我们能做出

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

的根 ξ。我们在之后的课程中将证明，X^3-3X-1 是 $\mathbb{Q}[X]$ 中的不可约多项式，从而，$[\mathbb{Q}(\xi):\mathbb{Q}]=3$。然而，$[\mathbb{Q}(\xi):\mathbb{Q}]$ 不是 2^m 的因子，矛盾。 □

注记 1.9. 通过升级的直尺和圆规，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。

[4]公元前 429 年，为了遏制 Delos 岛的瘟疫，古希腊人根据神谕需要将阿波罗神殿中正立方体的祭坛（的体积）加大一倍。



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。

注记 1.10. 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）。

古典几何作图的另一著名问题是所谓的化圆为方，即是否可用尺规作出面积为恰好等于给定圆面积的正方形？[5]

推论 7 (化圆为方)**.** *π 不是尺规可作的。*

证明: 根据 Lindemann 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，$\{1, \pi, \pi^2, \cdots, \pi^{2^m}\}$ 这 $2^m + 1$ 个数是 $\mathbb{Q}$-线性相关的，即存在非零的 $a_0, a_1, \cdots, a_{2^m} \in \mathbb{Q}$，使得

$$a_0 + a_1 q + \cdots + a_{2^m} q^{2^m} = 0.$$

即 π 满足一个有理系数的代数方程，矛盾。 □

[5]传说古希腊的 Anaxagoras 是第一个研究这个问题的人，似乎与他监狱中观察圆形的太阳和方形的牢窗有关。

2 群、环和模的定义

2.1 群的定义和例子

定义 2.1. G 是非空集合，$e \in G$ 并且 G 上配有乘法：

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

满足如下性质

1) 对任意 $g_1, g_2, g_3 \in G$，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 $g \in G$，有 $e \cdot g = g \cdot e$;

3) 每个 $g \in G$ 有逆元存在，即对任意 g，存在 $g^{-1} \in G$，使得 $g \cdot g^{-1} = g^{-1} \cdot g = e$。

就称 $(G, \cdot)$ 或者 G 是**群**。我们通常把 e 记为 1_G 或 1。

注记 2.1. 对任意 $g \in G$，g 的逆元存在唯一：假设 g' 也是逆元，则 $g \cdot g^{-1} = g \cdot g' = e$。对第一个等号左右两边同乘 g^{-1}，利用结合律，我们有

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

对任意 $g \in G$ 和 $n \geqslant 1$，我们将使用如下记号：

$$g^n = \underbrace{g \cdot g \cdot \cdots \cdot g}_{n} \quad g^{-n} = \underbrace{g^{-1} \cdot g^{-1} \cdot \cdots \cdot g^{-1}}_{n}, \ \ g^0 = 1.$$

注记 2.2 (几种群)**.** 若对任意 $g_1, g_2 \in G$，$g_1 \cdot g_2 = g_2 \cdot g_1$，就称 $(G, \cdot)$ 是**交换群**或 **Abel 群**。若 $|G|$ 有限，就称 G 是**有限群**并把 $|G|$ 称作是群的**阶**；否则称 G 为**无限群**。

若存在 $g_0 \in G$，使得对任意 $g \in G$，存在 $n \in \mathbb{Z}$，$g_0^n = g$，就称 G 是**循环群**而 g_0 为其（一个）**生成元**。

只有一个元素的群（即 $G = \{e\}$）被称为**平凡群**。简单起见，我们把平凡群直接写成 1。

例子 2.1. 令 $G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ 或 $\mathbb{C}$，对任意 $g_1, g_2 \in G$，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，0 是单位元。

当 G 是交换群时，我们习惯上把乘法符号 $\cdot$ 写成 $+$，把 g 的逆写成 $-g$，把单位元记作 0。

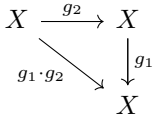
例子 2.2. 整数集除 n 的同余类 $\mathbb{Z}/n\mathbb{Z}$，即 $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$ 在加法 $\overline{k} + \overline{l} = \overline{k+l}$ 下是交换群。

实际上，$(\mathbb{Z}/n\mathbb{Z}, +)$ 是循环群，并且 $\overline{k}$ 是生成元当且仅当 $(k, n) = 1$。

例子 2.3 (域上的一般线性群)**.** K 是域，$G = \mathbf{GL}(n; K)$ 是 K 上 $n \times n$ 可逆矩阵的集合，令 $\cdot$ 为矩阵的乘法，e 为单位矩阵，$\mathbf{GL}(n; K)$ 是群（被称为**一般线性群**）。如果 $n \geqslant 2$，$\mathbf{GL}(n; K)$ 不是交换群。

练习 2.1. K 是有限域，$|K| = q$，试计算 $\left|\mathbf{GL}(2; K)\right|$。

例子 2.4 (集合的对称群)**.** X 是集合，$X \neq \emptyset$，$\mathfrak{S}_X$ 为 X 到自身的双射的集合。对任意 $g_1, g_2 \in \mathfrak{S}_X$，令 $g_1 \cdot g_2$ 为 g_1 与 g_2 的复合，即



那么，$(\mathfrak{S}_X, \cdot)$ 是群：单位映射是群的单位元而元素在群中的逆恰为其对应的映射的逆映射。

例子 2.5 (二面体群 $\mathfrak{D}_n$, $n \geqslant 3$)**.** $\Omega_n \subset \mathbb{R}^2$ 是正 n 边形，其中心是原点 O，顶点 $A_1 = (1, 0)$。我们考虑如下 $\mathbb{R}^2$ 到自身的双射：

- 以 O 为圆心、旋转 $\frac{2k\pi}{n}$ 的变换（其中 $k = 0, 1, \cdots, n-1$）可写成：

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

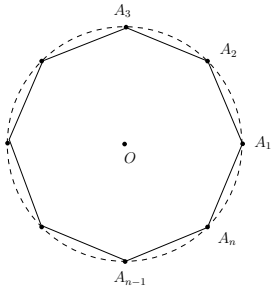
  令 $r = \rho_1$，那么，$\rho_k = r^k$。

- 若 n 是奇数，R_k 是以过 A_k 与其对边中心的直线为反射轴的反射（$k = 1, 2, \cdots, n$）；若 n 是偶数，R'_k 是以过 A_k 与 A_{n+k} 的直线为反射轴的反射，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（$k = 1, 2, \cdots, \frac{n}{2}$）。

  我们记以通过 A_1 的线为对称轴的反射为 s，即 $s(x, y) = (x, -y)$。

上述映射保持该正多边形，比如 n 为奇数时 $R_k : \Omega_n \to \Omega_n$ 是双射。另外，每个对称的逆为其本身。至此，我们构造了正多边形 Ω_n 的 $2n$ 个对称（即变换）：

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



由于 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，

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

另外，容易验证如下的复合关系：

$$srs = r^{-1}.$$

从而，$\mathfrak{D}_n$ 在映射的复合下称为群。实际上，对于 $x = r^k s$，$y = r^l s^b$，其中，$b = 0$ 或 1（若 $x = r^k$，显然 $xy \in \mathfrak{D}$）。根据 $srs = r^{-1}$，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）。

另外，当 $n \geqslant 3$ 时，$\mathfrak{D}_n$ 不是交换群。

定义 2.2. 给定群 G，$H \subset G$ 为非空子集，如果 H 对乘法和取逆封闭，即对任意 $h_1, h_2 \in H$，$h_1 \cdot h_2 \in H$ 以及对任意 $h \in H$，$h^{-1} \in H$，就称 H 是 G 的**子群**并记作 $H < G$。

注记 2.3. 给定群 G，$H < G$ 是子群，则 $1 = g \cdot g^{-1} \in H$。我们在 H 上使用 G 的乘法，从而子群 H 是群。

例子 2.6. G 是群，则 $\{1\}$ 和 G 都是子群。我们称这两个子群是**平凡的子群**。

例子 2.7. 自然数 $\mathbb{N}$（包括 0）不是 $(\mathbb{Z},+)$ 的子群，因为取逆不封闭。

例子 2.8. $\mathbb{C}^\times$ 为全体非零复数，其群乘法为复数的乘法，这是群。尽管 $\mathbb{C}^\times\subset\mathbb{C}$，但 $(\mathbb{C}^\times,\cdot)$ 不是 $(\mathbb{C},+)$ 的子群。

$n\geqslant 1$，令 $\mu^n(\mathbb{C})$ 为 $\mathbb{C}$ 中 n 次单位根的集合（$X^n-1=0$ 的所有根），这是 $\mathbb{C}^\times$ 的子群。

$\mathbb{R}^+$ 为全体正实数，它在实数乘法下构成群。$\mathbb{R}^+$ 是 $\mathbb{R}^\times$ 或 $\mathbb{C}^\times$ 的子群，但不是 $(\mathbb{R},+)$ 的子群。

例子 2.9. 可逆的 n 阶上三角矩阵的集合 $\mathcal{T}$ 是 $G=\mathbf{GL}(n;K)$ 的子群；对角线上均为 1 的 n 阶上三角矩阵的集合 $\mathcal{T}_1$ 也是 $G=\mathbf{GL}(n;K)$ 的子群

假设 $|K|=q$，其中 $q=p^m$，p 是素数。此时，

$$|\mathbf{GL}(n;K)|=\prod_{k=0}^{n-1}(q^n-q^k)=q^{\frac{n(n-1)}{2}}l,\quad |\mathcal{T}_1|=q^{\frac{n(n-1)}{2}},$$

其中，$(p,l)=1$。我们将看到，$\mathcal{T}_1$ 是 G 的 Sylow p-子群。

例子 2.10 (由子集生成的子群)**.** G 是群。

1) 假设 $\{G_i\}_{i\in I}$ 是 G 的一族子群，那么，$\bigcap\limits_{i\in I}G_i$ 是子群。

2) 子集 $S\subset G$ 并且 $S\neq\emptyset$，根据上述，存在唯一的、包含 S 的、最小的（在包含关系下）子群，它被称作是**由 S 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：

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

如果 G 的某个子群包含 S，它必然包含上述集合。所以，只要证明 $\langle S\rangle$ 是子群即可。

我们讨论 S 中元素的相乘。注意到如果 $s_i=s_{i+1}$，我们可以把 $s_i^{n_i}s_{i+1}^{n_{i+1}}$ 换成 $s_i^{n_i+n_{i+1}}$。对于 $s_1^{n_1}\cdots s_k^{n_k}$ 和 $s'^{n'_1}_1\cdots s'^{n'_{k'}}_{k'}$，它们相乘得

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

如果 $s_k=s'_1$，我们可以将采取上述替换，然后再看是否还有相邻两项相同，如此往复一直到得到上述对于 $\langle S\rangle$ 中元素的形式，这表明 $\langle S\rangle$ 对乘法封闭。

我们还有

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

这表明 $\langle S\rangle$ 对取逆封闭。

4) 当 $S=\{g\}$ 只由一个元素时，记它生成的子群为 $\langle g\rangle$。很明显，$\langle g\rangle$ 是循环群并且

$$\langle g\rangle=\{\cdots g^{-2},g^{-1},0,g,g^2,\cdots\}.$$

若有正整数 n，使得 $g^n=1$，就称 g 是**有限阶的元**（否则称之为**无限阶的元**）并用 $\mathrm{ord}(g)$ 来记最小的这种整数且称之为g **的阶**。此时，$\langle g\rangle$ 是有限循环群并且 $|\langle g\rangle|=n$。

我们注意到

- 若 g 是有限阶的元，$k,l\in\mathbb{Z}$，则 $g^k=g^l$ 当且仅当 $\mathrm{ord}(g)|k-l$。

– G 是有限群，则所有 $g \in G$ 均为有限阶的。

在二面体群 $\mathfrak{D}_n$ 中，$\langle r \rangle$ 生成的子群是 n 阶循环群，由所有旋转构成。

练习 2.2. G 是群且每个元素均为有限阶的，G 是否必为有限群?

注记 2.4. 假设 $x, y \in G$ 的阶分别为 k, l，其中，$(k, l) = 1$ 并且 $x \cdot y = y \cdot x$。那么，$x \cdot y$ 的阶为 kl。令 $d = \mathrm{ord}(x \cdot y)$，根据

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

我们有 $l \mid d$。同理，$k \mid d$，所以，$kl \mid d$。据此，$\mathrm{ord}(x \cdot y) = kl$。

如果不加 x 和 y 可交换的假设，则 $\mathrm{ord}(x \cdot y)$ 没有规律可言。实际上，我们考虑 $\mathbf{SL}(2; \mathbb{C})$，即行列式为 1 的 2×2 复矩阵构成的群。令

$$A = \begin{pmatrix} \xi_a & 0 \\ 0 & \xi_a^{-1} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & -1 \\ 1 & \xi_b + \xi_b^{-1} \end{pmatrix}, \quad U_t = \begin{pmatrix} 1 & t \\ 0 & 1, \end{pmatrix},$$

其中，$t \in \mathbb{C}$ 待定，$\xi_a = e^{\frac{2\pi i}{a}}, \xi_b = e^{\frac{2\pi i}{b}}$。

很明显，$\mathrm{ord}(A) = a$；由于 B 的两个特征值为 ξ_b 和 ξ_b^{-1}，从而，$\mathrm{ord}(B) = b$；特别地，$B_t = U_t \cdot B \cdot U_t^{-1}$ 的阶为 b。

对于 B 的计算表明，如果一个矩阵 $C \in \mathbf{SL}(2; \mathbb{C})$（行列式为 1）满足 $\mathrm{tr}(C) = \xi_c + \xi_c^{-1}$ 并且 $\xi_c^c = 1$，其中，c 是使得 $\xi_c^c = 1$ 成立的最小整数，那么，$\mathrm{ord}(C) = c$。

现在考虑 $A \cdot B_t$ 的阶。根据上面的讨论，我们计算

$$\mathrm{tr}(A \cdot B_t) = (\xi_a - \xi_a^{-1})t + \xi_a^{-1}(\xi_b + \xi_b^{-1}).$$

只要令选择 t 满足方程

$$(\xi_a - \xi_a^{-1})t + \xi_a^{-1}(\xi_b + \xi_b^{-1}) = \xi + \xi^{-1},$$

我们就有 $\mathrm{ord}(A \cdot B_t) = c$，其中，$c$ 可以任意指定而 $\mathrm{ord}(A) = a, \mathrm{ord}(B_t) = b$。

我们还可以进一步找到有限群 G，存在 $A, B_t \in G$，使得 $\mathrm{ord}(A) = a, \mathrm{ord}(B_t) = b$ 而 $\mathrm{ord}(A \cdot B_t) = c$，其中 c 是任意的。根据 Dirichlet 定理，选取素数 p，使得 $p \equiv 1 \mod abc$。根据初等数论中原根的存在性，${\mathbb{F}_p}^{\times}$ 是 $p-1$ 阶循环群，从而，存在 ξ_a, ξ_b 和 ξ_c，使得 $\xi_a^a = \xi_b^b = \xi_c^c = 1$，其中，类似于前述，我们要求 a, b, c 这三个指标都是最小的。此时，我们定义 $\mathbf{SL}(2; \mathbb{F}_p)$ 中的元素：

$$A = \begin{pmatrix} \xi_a & 0 \\ 0 & \xi_a^{-1} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & -1 \\ 1 & \xi_b + \xi_b^{-1} \end{pmatrix}, \quad U_t = \begin{pmatrix} 1 & t \\ 0 & 1, \end{pmatrix},$$

其中，$t \in \mathbb{F}_p$。容易看出，以上对于 $\mathbf{SL}(2; \mathbb{C})$ 的计算仍然成立。

例子 2.11 (中心化子、群的中心)**.** G 是群，$g \in G$，定义 g 的**中心化子**：

$$\mathrm{C}_g(G) = \{h \in G | gh = hg\}.$$

这是子群，由群中与 g 交换的元素构成。

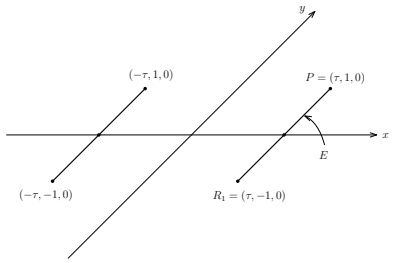
G 的**中心**Z(G) 是群中与所有元素均交换的元素组成的子群，按定义，我们有

$$\mathrm{Z(G)} = \bigcap_{g \in G} \mathrm{C}_g(G).$$

2.1.1 补充：正二十面体的对称

Euclid 在原本的第十三卷讨论正二十面体。在一条注解中，他说 Theaetetus 可能是第一个发现正二十面的数学家。

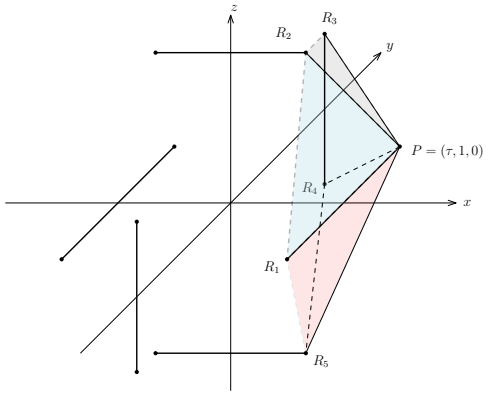
考虑三维空间 $\mathbb{R}^3$。在 $z=0$ 定义的平面上放置两条线段：线段 E 与 y-轴平行，端点为 $P=(\tau,1,0)$ 和 $R_1=(\tau,-1,0)$，其中点落在 x 轴上；第二条线段与 E 关于 y 轴对称，其端点为 $(-\tau,1,0)$ 和 $(-\tau,-1,0)$。



对以上四个端点 $(\pm\tau,\pm1,0)$ 的 x,y,z 坐标进行轮换可以得到 12 个点：

$$\{(\pm\tau,\pm1,0),\ (\pm1,0,\pm\tau\},\ (0,\pm\tau,\pm1)\}$$

考虑这 12 个点的凸包 $\mathbf{I}$（$\mathbf{I}$ 是 icosahedron 的缩写）给出的多面体。利用关于凸多面体的 Euler 定理（即 $v-e+f=2$，其中，v 是顶点个数，e 是边数，f 是面数），它有 12 个顶点，30 条边和 20 个面。请参考 3 维示意图：



图中与 P 相邻的五个点 $R_1,\cdots,R_5$ 分别为

$$R_1=(\tau,-1,0),\ R_2=(1,0,\tau),\ R_3=(0,\tau,1),\ R_4=(0,\tau,-1),\ R_5=(1,0,-\tau).$$

注意到 $|PR_1|=2$。为了保证 $|PR_i|=2$，其中，$i=2,\cdots,5$，通过计算可知：

$$\tau=\frac{\sqrt{5}+1}{2}\quad\Rightarrow\quad\tau^2-\tau-1=0.$$

一个重要的观察是 $R_1,R_2,\cdots,R_5$ 五点共面：实际上，它们的坐标均满足方程

$$\tau x+y=\tau.$$

上述方程定义出 $\mathbb{R}^3$ 中的一个平面，直线 OP 与这个平面垂直，其中，O 是原点。

a) $\triangle PR_1R_2,\triangle PR_2R_3,\triangle PR_3R_4,\triangle PR_4R_5,\triangle PR_5R_1$ 是 5 个全等的正三角形（边长为 2）。$\mathbb{R}^3$ 的以 OP 为旋转轴，旋转 $\frac{2}{5}\pi,\frac{4}{5}\pi,\frac{6}{5}\pi,\frac{2}{5}\pi$ 以及 $0\cdot\pi$ 保持该二十面体不变。共有 12 个顶点决定了 6 个旋转轴，从而共有 $4\times6=24$ 个这样的旋转。

b) 变换 $(x,y,z)\mapsto(y,z,x)$ 及它与自己复合 $(x,y,z)\mapsto(z,x,y)$ 也可以被实现为旋转变换：第一个变换的旋转轴是过 O 以及 $(1,1,1)$ 点的直线而旋转的角度为 $\frac{2}{3}\pi$；第二个变换有同样的旋转轴而旋转的角度是 $\frac{4}{3}\pi$。注意到旋转轴是过 O 与面 PR_2R_3 中心的直线。正二十面体的 20 个面决定了 10 个旋转轴，从而共有 $2\times 10=20$ 个这样的旋转。

c) 变换 $(x,y,z)\mapsto(-x,-y,z)$ 也是旋转变换，其轴为 z 轴而旋转的角度是 π。注意到旋转轴是 R_2 与 $(-1,0,\tau)$ 所决定的边的中点与 O 的连线。正二十面体的 30 条边决定了 15 个旋转轴，从而有 $1\times 15=15$ 个这样的旋转。

以上共有 $24+20+15=59$ 个旋转，加上单位映射（旋转的角度为 0），给出了有 60 个元素的集合 $G_{\mathbf{I}}$。

注记 2.5. 我们将证明 $G_{\mathbf{I}}$ 在映射复合下构成群并且这个群是阶最小的非交换单群。

对于以上 c) 中的变换，还可以考虑如下变体

c') 我们有 8 个变换 $(x,y,z)\mapsto(\pm x,\pm y,\pm z)$。它们由反射映射 $(x,y,z)\mapsto(-x,y,z)$，$(x,y,z)\mapsto(x,-y,z)$ 和 $(x,y,z)\mapsto(x,y,-z)$ 复合得到，其中有 4 个不是旋转。

注记 2.6 (正二十面体的定义)**.** 在平面几何中，正多边形可以用如下直观来描述：我们可以通过旋转和对称把任何的边和顶点互换。按照这种逻辑，我们现在解释 $\mathbf{I}$ 是正二十面体。

令 (F,E,V) 为 $\mathbf{I}$ 的一个（面边点）三元组，即 F 为面，E 为边，V 为顶点并且 $V\subset E\subset F$。那么，对任意的三元组 (F',E',V')，那么可以通过上述 $a),b)$ 和 $c')$ 中的变换以及它们的复合，使得

$$F\mapsto F',\ E\mapsto E',\ V\mapsto V'.$$

令 $V_0=P$，$E_0=PR_1$，$F_0=PR_1R_2$，请参考上图中的淡蓝色三角形。我们只要说明对任意的三元组 (F,E,V)，可以通过 $a),b)$ 和 $c')$ 映射的复合实现

$$F\mapsto F_0,\ E\mapsto E_0,\ V\mapsto V_0.$$

1) 通过 $c')$ 中的 $(x,y,z)\mapsto(-x,-y,-z)$，不妨假设 $V\in\{P,R_1,R_2,R_3,R_4,R_5\}$。

2) 再通过 $a)$ 中的 5 个旋转（包括单位映射），不妨假设 $V\in\{P,R_1\}$。

3) 再通过 $c')$ 中的 $(x,y,z)\mapsto(x,-y,z)$，不妨假设 $V=P$。

4) 再通过 $a)$ 中的 5 个旋转（包括单位映射），不妨假设 $E=E_0=PR_1$，$V=P$（P 在旋转下不动）。

5) 经过以上四个步骤，$F=F_0$ 或者 PR_1R_5（请参考上图中的淡红色三角形）。此时，我们可以通过 $c')$ 中的 $(x,y,z)\mapsto(x,y,-z)$ 把 PR_1R_5 映射成 F_0。

练习 2.3. 证明，对任意三元组 (F,E,V) 和 (F',E',V')，可以通过 $a),b)$ 和 $c')$ 映射的复合给出的映射 φ，使得

$$\varphi: F\mapsto F',\ E\mapsto E',\ V\mapsto V'.$$

（以上只证明了 $(F',E',V')=(F_0,E_0,V_0)$ 的情形）

2.2 群同态

定义 2.3 (群同态)**.** $(G_1,\cdot_1)$ 和 $(G_2,\cdot_2)$ 是群，$\varphi: G_1\to G_2$ 是映射。如果 φ 保持乘法，即对任意 $g,h\in G_1$，有

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

就称 φ 是 $(G_1,\cdot_1)$ 到 $(G_2,\cdot_2)$ 的**群同态**。我们用 $\mathrm{Hom}(G_1,G_2)$ 表示群同态组成的集合。

如果群同态 φ 是双射，就称 φ 是 G_1 到 G_2 的**群同构**。

注记 2.7. 同构的群首先作为集合是同构的（之间存在双射），进一步它们具有同样的乘法结构。

注记 2.8. 对于群同态 $\varphi: G_1\to G_2$，通过考虑 $\varphi(1_{G_1}\cdot 1_{G_1})=\varphi(1_{G_1})$ 即知 $\varphi(1_{G_1})=1_{G_2}$。另外，对任意 $g\in G_1$，$\varphi(g^{-1})=\varphi(g)^{-1}$。

注记 2.9. 假设 $\varphi\in\mathrm{Hom}(G_1,G_2)$ 是群同构，那么 $\varphi^{-1}\in\mathrm{Hom}(G_2,G_1)$ 也是群同构。

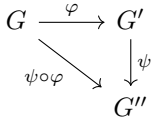
注记 2.10. 若有 G_1 到 G_2 的群同构，就称它们是**同构的**并记作是 $G_1\simeq G_2$。注意到这个符号并不精确，因为没说明 φ 是如何定义的。实际上，群 G_1 和 G_2 同构而它们之间的同构映射 φ 可能不唯一。

假设 G_1 和 G_2 均为 $\mathbb{C}^\times$，对任意的 $\lambda\in\mathbb{C}^\times$，映射 $z\mapsto\lambda\cdot z$ 均为 G_1 到 G_2 的同构。

注记 2.11 (同态的复合)**.** 群同态的复合仍为群同态，即有映射

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

其中，G,G',G'' 是群。换而言之，若 $\varphi\in\mathrm{Hom}(G,G')$，$\psi\in\mathrm{Hom}(G',G'')$，则 $\psi\circ\varphi$ 也是群同态。



用 $\mathbf{Aut}(G)$ 表示 G 到自身的群同构的集合，配有映射的复合作为 $\mathbf{Aut}(G)$ 上的乘法，那么 $\mathbf{Aut}(G)$ 是群。我们称 $\mathbf{Aut}(G)$ 是 G 的**自同构群**。

考虑集合 G（忘掉其群结构）的对称群 $\mathfrak{S}_G$，它由所有 G 到自身的双射构成。$\mathrm{Aut}(G)$ 中的元素还要尊重 G 的群结构，从而 $\mathrm{Aut}(G)<\mathfrak{S}_G$ 是子群。

注记 2.12 (群同态的像与核)**.** 给定群同态 $\varphi\in\mathrm{Hom}(G_1,G_2)$，定义 φ 的**像**$\mathrm{Im}(\varphi)$ 和**核**$\mathrm{Ker}(\varphi)$ 分别为

$$\mathrm{Im}(\varphi)=\big\{\varphi(g)\big|g\in G_1\big\},\quad\mathrm{Ker}(\varphi)=\big\{g\in G_1\big|\varphi(g)=1_{G_2}\big\}.$$

那么，$\mathrm{Ker}(\varphi)<G_1$ 是子群，$\mathrm{Im}(\varphi)<G_2$ 也是子群。

注意到 φ 是单射当且仅当 $\mathrm{Ker}(\varphi)=\{1\}$；$\varphi$ 是满射当且仅当 $\mathrm{Im}(\varphi)=\{1\}$。在群论中常用一个结论是为说明 φ 是单射只要验证 $1\in G_2$ 的原像唯一。

实际上，如果 $\mathrm{Ker}(\varphi)=\{1\}$，假设 $g,h\in G$ 使得 $\varphi(g)=\varphi(h)$，那么，$\varphi(gh^{-1})=\varphi(g)\varphi(h)^{-1}=1$，即 $gh^{-1}\in\mathrm{Ker}(\varphi)$。这表明 $gh^{-1}=1$，即 $g=h$。所以，φ 是单射。

例子 2.12. 我们有几个经典的群同态：

- K 是域，$n\geqslant 1$ 行列式映射

  $$\det:\mathbf{GL}(n;K)\to K^\times$$

  是群同态。令 $\mathbf{SL}(n;K)=\mathrm{Ker}\,(\det)$，这是行列式为 1 的 $n\times n$ 的矩阵构成的群，被称为K **上的特殊线性群**。

- 指数映射 $\exp : \mathbb{C} \to \mathbb{C}^\times$ 是群同态，$\mathrm{Ker}(\exp) = 2\pi i\mathbb{Z}$。
- 对数映射 $\log : \mathbb{R}^\times \to \mathbb{R}$ 是群同态，$\mathrm{Ker}(\log) = \{1\}$。
- $\bmod n$ 映射。考虑除 n 的余数给出自然的群同态

$$\mathbb{Z} \xrightarrow{\bmod n} \mathbb{Z}/n\mathbb{Z}, \qquad k \mapsto \overline{k}.$$

它的核是能被 n 整除的整数，即 $\mathrm{Ker}\big(\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}\big) = n\mathbb{Z}$。

例子 2.13. G 是群，$g \in G$，则映射

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

是群同态，其像 $\mathrm{Im}(\varphi_g)$ 为 $\langle g \rangle$。

例子 2.14. G 是群，对任意 $g \in G$，定义共轭映射 $\mathrm{Int}(g)$：

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

对任意 $h_1, h_2 \in G$，有 $gh_1h_2g^{-1} = gh_1g^{-1} \cdot gh_2g^{-1}$，从而 $\mathrm{Int}(g) \in \mathrm{Hom}(G, G)$；由于 $\mathrm{Int}(g)$ 可逆，其逆为 $\mathrm{Int}(g^{-1})$，从而 $\mathrm{Int}(g) \in \mathrm{Aut}(G)$。所以，我们定义了映射：

$$\mathrm{Int} : G \to \mathrm{Aut}(G), \quad g \mapsto \mathrm{Int}(g).$$

对任意 $h, g_1, g_2 \in G$，我们有

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

所以，$\mathrm{Int} : G \to \mathrm{Aut}(G)$ 是群同态。我们显然有 $\mathrm{Ker}(\mathrm{Int}) = \mathrm{Z}(G)$。我们称像 $\mathrm{Int}(G) < \mathrm{Aut}(G)$ 是 G 的**内自同构群**。

2.3 正规子群与商群

定义 2.4. G 是群 G，$H < G$ 是子群。对任意 $g \in G$，称如下集合为一个**左陪集**：

$$gH = \big\{gh \big| h \in H\big\}.$$

由于 H 是子群，所以对任意 $h \in H$，$hH = 1 \cdot H = H$。我们说明 $g_1H \cap g_2H \neq \emptyset$ 当且仅当 $g_1H = g_2H$。实际上，如果 $g_1H \cap g_2H \neq \emptyset$，那么存在 $h_1, h_2 \in H$，使得 $g_1h_1 = g_2h_2$。所以，$g_2 = g_1h_1h_2^{-1}$。此时，

$$g_2H = g_1h_1h_2^{-1}H = g_1\big(h_1h_2^{-1}H\big) = g_1H.$$

这表明 $\{gH\}_{g \in G}$ 是 G 的一个划分，从而定义出等价关系 $\sim$。实际上，$g_1 \sim g_2$ 等价于 $g_1^{-1}g_2 \in H$。

我们定义左陪集的集合

$$G/H = \big\{gH \big| g \in G\big\},$$

并称 $[G : H] = \big|G/H\big|$ 为 H 在 G 中的**指标**。

类似地，定义**右陪集**为：

$$Hg = \big\{gh \big| h \in H\big\}.$$

同样可以证明 $\{Hg\}_{g\in G}$ 是 G 的一个划分并定义了等价关系 $\sim_r$。实际上，$g_1 \sim_r g_2$ 等价于 $g_1 g_2^{-1} \in H$。为了区别于左陪集的空间，右陪集的集合记作：

$$_H\backslash^G = \{Hg | g \in G\}.$$

我们今后基本上只处理左陪集的情形。

注记 2.13 (左陪集的元素个数)**.** 对任意的 gH 和 $g'H$，如下映射为双射：

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

特别地，若 H 是有限子群，则其每个左陪集的元素个数均为 $|H|$。如果进一步 G 是有限群，我们就有

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

命题 8 (Lagrange)**.** *若 G 是有限群，则其子群的元素个数整除 $|G|$。特别的，对任意 $g \in G$，$\mathrm{ord}(g) \mid |G|$。*

证明: 以上注记已经给出了第一部分的证明。为了证明 $\mathrm{ord}(g)||G|$，只要考虑子群 $H = \{1, g, \cdots, g^{\mathrm{ord}(g)-1}\}$ 即可。 □

注记 2.14. 如果 G 是有限群，则对任意的 $g \in G$，$g^{|G|} = 1$。

特别的，考虑乘法群 $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$，其中，$\overline{k}\cdot\overline{l} = \overline{kl}$。那么，对任意的 $k \in \mathbb{Z}((k,p) = 1)$，由于 $\left|\left(\mathbb{Z}/p\mathbb{Z}\right)^\times\right| = p-1$，在 $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ 中我们有 $\overline{k}^{p-1} = \overline{1}$，即对任意的与 p 互素的整数 k，有 $k^{p-1} \equiv 1 \mod p$。这是初等数论中的 Fermat 小定理。

定义 2.5. H 是群 G 的子群。如果对任意 $g \in H$，$gHg^{-1} = H$，其中，$gHg^{-1} = \{ghg^{-1} | h \in H\}$，就称 H 是**正规子群**并记作 $H \lhd G$。

注记 2.15. 为了验证 H 是正规子群，只要对任意 $h \in H, g \in G$，验证 $ghg^{-1} \in H$：因为我们显然有 $\bigcup_{g\in G} gHg^{-1} \supset H$。

例子 2.15. G 是交换群，其所有子群都是正规子群。

例子 2.16. $n \geqslant 3$，$G = \mathfrak{D}_n$。那么，$\langle r\rangle$ 是正规子群而 $\langle s\rangle$ 不是正规子群。

例子 2.17. 群同态的核是正规子群，即若 $\varphi : G \to G'$ 是群同态，则 $\mathrm{Ker}(\varphi) \lhd G$。

对任意 $g \in G$ 和 $h \in \mathrm{Ker}(\varphi)$，我们验证

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

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

例子 2.18. H 是群 G 的子群，定义 H 在 G 中的**正规化子**为：

$$\mathrm{N}_G(H) = \{g \in G | gHg^{-1} = H\}.$$

容证 $\mathrm{N}_G(H)$ 是 G 的子群。按定义，我们有

$$H \lhd \mathrm{N}_G(H) < G.$$

这是 G 的使得 H 在其中为正规子群的最大子群。

注记 2.16. G 是群，$K < H$ 是 G 的子群，我们有

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

以上公式的证明是简单的集合计数。

G 是群，H 为子群，我们希望在 G/H 上面定义乘法。对左陪集 g_1H 和 g_2H，自然的尝试是要求

$$g_1H \cdot g_2H := g_1g_2H.$$

我们必须验证以上是良好定义的。假设 $g_1' = g_1h$，其中，$h \in H$，那么，$g_1H = g_1'H$。所以，上述直观的定义还应该给出

$$g_1H \cdot g_2H = g_1'H \cdot g_2H := g_1'g_2H = g_1hg_2H.$$

为了保证两个公式给出了同样的陪集，我们要保证 $(g_1g_2)^{-1}g_1hg_2 = g_2^{-1}hg_2 \in H$。根据以上元素选择的任意性，这等价于 H 是正规子群。

定理 9. *$H \lhd G$ 是正规子群。在 G/H 存在唯一的群结构，使得自然的商映射*

$$\pi : G \longrightarrow G/H$$

是群同态。另外，$\mathrm{Ker}(\pi) = H$。

实际上，左陪集的乘法定义为 $g_1H \cdot g_2H = g_1g_2H$。

证明： 定义 G/H 上乘法为 $g_1H \cdot g_2H = g_1g_2H$，这是良好定义的：假设 $g_1'H = g_1H$，$g_2'H = g_2H$，则存在 $h_1, h_2 \in H$，使得 $g_1' = g_1h_1, g_2' = g_2h_2$，从而

$$g_1'g_2'H = g_1h_1g_2h_2H = g_1g_2 \cdot \underbrace{g_2^{-1}h_1g_2}_{\in H} \cdot h_2H = g_1g_2H.$$

此时，

$$\pi(g_1 \cdot g_2) = (g_1 \cdot g_2)H = g_1H \cdot g_2H = \pi(g_1)\pi(g_2)$$

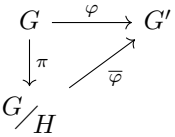
所以，π 是群同态。

唯一性是明显的：为了保证 π 是群同态，必须有 $\pi(1_G) = 1_{G/H}$，即 H 是 G/H 中的单位元。另外，

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

这表明群的乘法结构由同态决定。 □

定理 10. *G 是群，$H \lhd G$ 是正规子群，$\varphi : G \to G'$ 是群同态。若 $H < \mathrm{Ker}(\varphi)$，则存在唯一的群同态 $\overline{\varphi} : G/H \to G'$，使得 $\overline{\varphi} \circ \pi = \varphi$，其中，$\pi : G \to G/H$ 是自然的同态。*



进一步，我们还有群同构 $\overline{\varphi} : G/\mathrm{Ker}(\varphi) \xrightarrow{\simeq} \mathrm{Im}(\varphi)$。

证明： 对任意的左陪集 gH，定义

$$\overline{\varphi}(gH) = \varphi(g).$$

对于 $g'H = gH$，由于 $g^{-1}g' \in H \subset \mathrm{Ker}(\varphi)$ 以及 $H < \mathrm{Ker}(\varphi)$，有 $\varphi(g^{-1}g') = 1$，即 $\varphi(g) = \varphi(g')$，这表明 $\overline{\varphi}$ 是良好定义的。映射 $\overline{\varphi}$ 是群同态。另外，我们显然有 $\overline{\varphi} \circ \pi = \varphi$。

选取 $H = \mathrm{Ker}(\varphi)$，我们显然有满射

$$\overline{\varphi} : {}^{G}\!\diagup_{\mathrm{Ker}(\varphi)} \twoheadrightarrow \mathrm{Im}(\varphi).$$

根据定义，$\varphi(g) = 1$ 当切仅当 $g \in \mathrm{Ker}(\varphi)$，所以该同态是单射，从而为同构。 □

注记 2.17. 这是本课程中最基本和最经常用到的定理。作为一个典型的应用，我们证明

推论 11. *G 是群，$g \in G$，那么 $\langle g \rangle$ 要么与 $\mathbb{Z}$ 同构，要么与 ${}^{\mathbb{Z}}\!\diagup_{n\mathbb{Z}}$ 同构，其中，$n = \mathrm{ord}(g)$。*

证明： 考虑群同态 $\varphi : \mathbb{Z} \to G$，其中，$\varphi(m) = g^m$，$m \in \mathbb{Z}$。那么，$\varphi(\mathbb{Z}) = \langle g \rangle$。如果 $\mathrm{Ker}(\varphi) = \{0\}$，根据以上定理，$\mathbb{Z} \simeq \langle g \rangle$；否则，$\mathrm{Ker}(\varphi) = n\mathbb{Z}$，其中，$n$ 是 $\mathrm{Ker}(\varphi)$ 最小的正整数，从而，${}^{\mathbb{Z}}\!\diagup_{n\mathbb{Z}} \simeq \langle g \rangle$。 □

我们把与 ${}^{\mathbb{Z}}\!\diagup_{n\mathbb{Z}}$ 同构的群称为**n-阶循环群**，把与 $\mathbb{Z}$ 同构的群称为**无限循环群**。上面的证明表明循环群（即由一个元素生成的群）只有这两种。

注记 2.18 (短正合列的记号)**.** 给定群同态 $\varphi : H \to G$ 和 $\psi : G \to G'$。如果 φ 为单射，把它记作是

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

如果 ψ 为满射，把它记作是

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

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

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

我们将经常用如下群同态的短正合列：

$$1 \to H \xrightarrow{\varphi} G \xrightarrow{\psi} G' \to 1,$$

它表明 φ 是单射，ψ 是满射并且 $\mathrm{Im}(\varphi) = \mathrm{Ker}(\psi)$。比如说，给定群同态 $\varphi : G \to G'$，我们有

$$1 \to \mathrm{Ker}(\varphi) \to G \xrightarrow{\varphi} \mathrm{Im}(\varphi) \to 1.$$

例子 2.19. *G 是群，考虑内自同构映射 $\mathrm{Int} : G \to \mathbf{Aut}(G)$。$\mathbf{Aut}(G)$ 中形如 $\mathrm{Int}(g)$ 形式的同构称作是 G 的**内自同构**，它们组成的集合为 $\mathrm{Int}(G) := \mathrm{Im}(\mathrm{Int}) \lhd \mathbf{Aut}(G)$ 是正规子群。实际上，对任意的 $g, h \in G, \varphi \in \mathbf{Aut}(G)$，我们有*

$$\big(\varphi \circ \mathrm{Int}_g \circ \varphi^{-1}\big)(h) = \varphi(g\varphi^{-1}(h)g^{-1}) = \varphi(g)h\varphi(g)^{-1} = \mathrm{Int}_{\varphi(g)}(h)$$

*我们定义群 G 的**外自同构群**为：*

$$\mathrm{Out}(G) = {}^{\mathrm{Aut}(G)}\!\diagup_{\mathrm{Im}(\mathrm{Int})}.$$

从而，我们得到下述正合列

$$1 \to \mathrm{Z}(G) \longrightarrow G \xrightarrow{\mathrm{Int}} \mathrm{Int}(G) \to 1, \tag{2.1}$$

以及

$$1 \to G \xrightarrow{\mathrm{Int}} \mathbf{Aut}(G) \to \mathrm{Out}(G) \to 1. \tag{2.2}$$

2.4 环的定义

定义 2.6. [6]集合 A 非空并且 $|A|\geqslant 2$。如果 A 上定义了乘法 $\cdot$ 和加法 $+$，即有映射

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

和

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

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) – 乘法具有结合律，即对任意 $a_1,a_2,a_3\in A$，有 $(a_1\cdot a_2)\cdot a_3=a_1\cdot(a_2\cdot a_3)$；
   – 1_A 是乘法单位元，即对任意 $a\in A$，有 $1_A\cdot g=g\cdot 1_A$；

3) 乘法分配律成立：对任意的 $a_1,a_2,a_3\in A$，有

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

就称 $(A,\cdot,+)$ 或 A 是一个**环**。

注记 2.19 (记号的澄清)**.** 有以下几个简单的事实：

- 对任意的 $a\in A$，$0\cdot a=a\cdot 0=0$。
- 对任意 $a\in A$，用 $-a$ 表示其加法的逆元，即 $a+(-a)=(-a)+a=0$；用 $a-b$ 表示 $a+(-b)$；根据结合律，$-(a\cdot b)=(-a)\cdot b=a\cdot(-b)$，我们把这个结果简写成 $-a\cdot b$ 或者 $-ab$；用 ab 表示 $a\cdot b$。

注记 2.20. 如果对任意 $a,b\in A$，$a\cdot b=b\cdot a$，就称 A 是**交换环**。

注记 2.21. 给定 $a\in G$，如果存在 $a'\in A$，使得 $a\cdot a'=1$，就称 a' 是 a 的一个**右逆**；类似地，如果存在 $a''\in A$，使得 $a''\cdot a=1$，就称 a'' 是 a 的一个**左逆**。

注意到，如果 a 即有左逆又有右逆，它们必然相同（都等于 $a''aa'$）并且唯一。此时，它被称为 a 的**逆**。

用 $A^\times$ 表示环 A 中有逆的元素（即有左逆又有右逆）的元素的集合。很明显，$(A^\times,\cdot)$ 是群。

根据定义，如果每个非零的 $a\in A$ 均有逆，那么 A 是**域**（我们并不要求域的乘法是交换的）。简而言之，域可以做加减乘除（乘逆）的四则运算而环只能做加减乘这三种运算。

例子 2.20. $\mathbb{Z},\mathbb{Q},\mathbb{R}$ 或 $\mathbb{C}$ 配有通常的乘法和加法运算构成交换环。实际上，除 $\mathbb{Z}$ 之外，其余的环均为域。

例子 2.21. A 是环，$\mathbf{M}_n(A)$ 是环 A 上 $n\times n$ 的矩阵的集合。注意到，矩阵的乘法和加法只用到了分量上的乘法和加法并且不使用乘法的逆或者交换律，所以，在矩阵的加法和乘法下，$\mathbf{M}_n(A)$ 是环，其单位矩阵和零矩阵对应着 $1_{\mathbf{M}_n(A)}$ 和 $0_{\mathbf{M}_n(A)}$。

一般而言，$n\geqslant 2$，$\mathbf{M}_n(A)$ 不是交换环。

对于域 K，有 $M_n(K)^\times=\mathbf{GL}(n,K)$。

对于交换环 A，我们仍然可以定义行列式：

$$\det:\mathbf{M}_n(A)\to A,\ \ M\mapsto\sum_{(k_1,\cdots,k_n)\text{为 }(1,\cdots,n)\text{ 的排列}}(-1)^{\sigma(k_1,\cdots,k_n)}M_{1,k_1}M_{2,k_2}\cdots M_{n,k_n},$$

[6]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幺环。

其中，$M_{i,j} \in A$ 为 M 在第 i 行第 j 列处的数而 $\sigma(k_1, \cdots, k_n)$ 为排列 $(k_1, \cdots, k_n)$ 的奇偶性。此时，我们仍然有

$$M \cdot M^* = \det(M) \cdot \mathbf{I}_n,$$

其中，M^* 为 M 的伴随矩阵，$\mathbf{I}_n$ 为单位矩阵。从而，$M \in \mathbf{M}_n(A)^\times$ 当且仅当 $\det(M) \in A^\times$。

例子 2.22. $n \geqslant 2$。在 $\mathbb{Z}/n\mathbb{Z}$ 上定义乘法，对任意的 $\overline{k}, \overline{l} \in \mathbb{Z}/n\mathbb{Z}$，定义

$$\overline{k} \cdot \overline{l} = \overline{k \cdot l}.$$

容易看出这是良好定义的。这样，我们就得到了交换环 $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$。

如果 n 是合数，即 $n = n_1 \cdot n_2$，$n_1, n_2 \geqslant 2$。那么，$\overline{n_1} \cdot \overline{n_2} = \overline{n} = 0$。由于 $\overline{n_1}$ 和 $\overline{n_2}$ 均非零，所以 $\mathbb{Z}/n\mathbb{Z}$ 不是域，因为 $\overline{n_1}$ 没有逆。

另外，如果 $n = p$ 是素数，我们已经构造了域 $\mathbb{Z}/p\mathbb{Z}$。

例子 2.23 (多项式环)**.** A 是环，$A[X]$ 是 A 上以 X 为不定元的多项式的集合，即每个 $P \in A[X]$ 均形如

$$P(X) = \sum_{k=0}^{n} a_k X^n.$$

其中，$a_k \in A$，$a_n \neq 0$。这里，n 被称为P **的次数**并记作 $\deg P$。另外多项式之间的乘法和加法形式上与传统一致，这就是多项式环 $A[X]$ 的定义。

另外，我们强调多项式不是多项式函数。

我们有如下简单的性质：

a) 若 A 是交换环，则 $A[X]$ 也是交换环。

b) 若 K 是域，则对任意非零的 $P, Q \in K[X]$，$\deg(P \cdot Q) = \deg(P)\deg(Q)$。

作为练习，试举例使得 $P, Q \in A[X]$ 是非零多项式而 $P \cdot Q = 0$。

例子 2.24. 拓扑空间 X 上的（复值）连续函数空间 $C(X)$ 是环，其中，乘法和加法按照通常的方式定义。

例子 2.25 (K-代数)**.** K 是域，A 是环并且是 K-线性空间，如果对任意的 $x, y \in A$ 和 $k \in K$，我们有

$$k \cdot (x \cdot_A y) = (kx) \cdot_A y = x \cdot_A (ky),$$

就称 A 是K**-代数**。

我们有如下三类重要的例子：

- K 是域，多项式环 $K[X]$ 是 K-代数。
- K 是域，$n \times n$ 的矩阵环 $\mathbf{M}_n(K)$ 是 K-代数。
- K 是域，G 是群，所谓的**群代数** $K[G]$ 定义如下：$K[G]$ 是 K-线性空间并且 $\{e_g \big| g \in G\} \subset K[G]$ 是一组基；对任意的 $x = \sum_{g \in G} x_g e_g, y = \sum_{h \in G} y_h e_h \in K[G]$（以上均为有限和），其中，$x_g, y_h \in K$，其乘法由下面公式给出：

  $$x \cdot y = \sum_{g \in G} \sum_{h \in G} x_g y_h e_{gh}.$$

  这是一个 K-代数，它的乘法记录了群 G 的乘法。

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 B 对乘法封闭, 即对任意 $a, b \in B$, $a \cdot b \in B$, 就称 B 是 A 的**子环**。

使用环 A 的加法和乘法，子环 B 具有自然的环结构。

例子 2.26. $\mathbb{Z}$ 是 $\mathbb{C}$ 的子环（不是子域）而 $\mathbb{Q}$ 和 $\mathbb{R}$ 是 $\mathbb{C}$ 的子域。

定义 2.8 (环同态)**.** $(A_1, +_1, \cdot_1)$ 和 $(A_2, +_2, \cdot_2)$ 是环，$\varphi : A_1 \to A_2$ 是映射。如果 φ 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 $\varphi(1_{A_1}) = 1_{A_2}$，就称 φ 是从 A_1 到 A_2 的**环同态**。我们用 $\mathrm{Hom}(A_1, A_2)$ 表示从 A_1 到 A_2 的环同态的集合。如果环同态 φ 是双射，就称 φ 是从 A_1 到 A_2 的一个**环同构**；如果 A_1 与 A_2 之间存在环同构，就称这两个环是**同构的**并记作是 $A_1 \simeq A_2$。

注记 2.22. 给定从 A_1 到 A_2 的环同构 φ，它的逆

$$\varphi^{-1} : A_2 \longrightarrow A_1$$

是环同态（也是双射），即 $\varphi^{-1} \in \mathrm{Hom}(A_2, A_1)$。

注记 2.23. 对任意的 $\varphi \in \mathrm{Hom}(A_1, A_2)$，它**核**定义为

$$\mathrm{Ker}(\varphi) = \left\{ a \in A_1 \middle| \varphi(a) = 0_{A_2} \right\}.$$

这是 A_1 的加法子群，但是 $\mathrm{Ker}(\varphi)$ 并非子环，因为 $1_A \notin \mathrm{Ker}(\varphi)$。

另外，φ 为单射当且仅当 $\mathrm{Ker}(\varphi) = \{0\}$。

例子 2.27. $\mod n$ 映射是环同态

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

其中，$\mathrm{Ker}\left(\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}\right) = n\mathbb{Z}$。

引理 12 (常用)**.** *K 是域，A 是环，$\varphi : K \to A$ 是环同态，则 φ 是单射。*

证明: 实际上，对任意 $k \in K^\times$，有

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

所以，$k \notin \mathrm{Ker}(\varphi)$。从而，$\mathrm{Ker}(\varphi) = \{0\}$。 □

2.5 模的定义

模可以被视作是环上的线性空间:

定义 2.9. A 是环，$(M, +)$ 是交换群。如果存在映射

$$A \times M \to M, \quad (a, m) \mapsto a \cdot m,$$

使得对任意 $a, a' \in A, m, m' \in M$，有

$$\begin{cases} 1 \cdot m = m, \\ a \cdot (a' \cdot m) = (a \cdot a') \cdot m, \\ a \cdot (m + m') = a \cdot m + a \cdot m', \\ (a + a') \cdot m = a \cdot m + a' \cdot m, \end{cases}$$

就称 $(M,+)$ 或 M 是 **(左)A-模**。

如果 $N<M$ 是 M 的加法子群并且对上述乘法封闭，即对任意 $a\in A$ 和 $n\in N$，有 $a\cdot n\in N$，就称 $(N,+)$ 是 M 的一个**子 A-模**或**子模**。在 A 对 M 的乘法下，N 是 A-模。

例子 2.28. K 是域，则 K-模是 K-线性空间。

例子 2.29. 对于整数环 $\mathbb{Z}$，$\mathbb{Z}$-模 M 是交换群，其中，对于 $a\in\mathbb{Z},m\in M$，

$$a\cdot m=\underbrace{m+m+\cdots+m}_{a\text{ 次}}.$$

例子 2.30. A 和 B 是环，$\varphi:A\to B$ 是环同态，则 B 具有自然的 A-模结构：

$$A\times B\to B,\ \ (a,b)\mapsto a\cdot b:=\varphi(a)\cdot_B b.$$

例子 2.31. K 是域，$A=K[X]$ 为 K 上的多项式环，V 是 K-线性空间。给定线性映射 $T\in\mathbf{End}_K(V)$，这定义出 V 上的 $K[X]$-模的结构：

$$K[X]\times V\to V,\ \ (P(X),v)\mapsto P(X)\cdot v=P(T)\cdot v.$$

即对任意 $P(X)=a_nX^n+\cdots+a_1X+a_0\in K[X]$，其中，$a_i\in K$，要求

$$P(T)\cdot v=a_n\cdot T^n(v)+\cdots+a_1\cdot T(v)+a_0\cdot v.$$

很显然，我们有

$$(P+Q)(T)\cdot v=P(T)\cdot v+Q(T)\cdot v,\ \ (P\cdot Q)(T)\cdot v=P(T)\cdot\big(Q(T)\cdot v\big).$$

这是最重要的一类 $K[X]$-模（由线性映射 T 决定）。

定义 2.10 (A-模同态)**.** $(M_1,+_1)$ 和 $(M_2,+_2)$ 是 A-模，$\varphi:M_1\to M_2$ 是加法群同态并且保持乘法，即对任意的 $a\in A$ 和 $m,m'\in M_1$，有

$$\varphi(m+_1m')=\varphi(m)+_2\varphi(m'),\ \ \varphi(a\cdot_1m)=a\cdot_2\varphi(m),$$

就称 φ 是从 M_1 到 M_2 的**A-模同态**或**A-线性映射**。我们用 $\mathrm{Hom}_A(M_1,M_2)$ 表示从 M_1 到 M_2 的模同态的集合。如果 φ 是双射，称 φ 是它们之间的**A-模同构**。如果 M_1 与 M_2 之间存在 A-模同构，就称 M_1 和 M_2 是**同构的**并记为 $M_1\simeq M_2$。

注记 2.24. A 是交换环，则 $\mathrm{Hom}_A(M_1,M_2)$ 具有自然的 A-模结构：

$$A\times\mathrm{Hom}_A(M_1,M_2)\to\mathrm{Hom}_A(M_1,M_2),\ (a,\varphi)\mapsto\Big(a\cdot\varphi:m_1\mapsto a\cdot_2\varphi(m_1)\Big).$$

例子 2.32. 给定 A-模之间的同态 $\varphi\in\mathrm{Hom}_A(M_1,M_2)$，它的**核**定义为：

$$\mathrm{Ker}(\varphi):=\big\{m\in M_1\big|\varphi(m)=0\big\}.$$

这是 M_1 的子模。

另外，φ 是单射当且仅当 $\mathrm{Ker}(\varphi)=\{0\}$。

例子 2.33. 给定 A-模 M 及其子模 M，我们可以构造其**商模** M/N。

首先将 M 视为交换群，其所有子群均为正规子群，从而，我们可以定义商群：

$$M/N = \{m+N | m \in M\}.$$

这自然也是交换群，其 A-模结构由如下公式给出：

$$A \times M/N \to M/N, \quad (a, m+N) \mapsto a(m+N) := am+N.$$

这个乘法的定义不依赖于 $m+N$ 中代表元的选取，即若 $m+N = m'+N$，则 $am+N = am'+N$，这是因为 $m-m' \in N$，从而，$am-am' \in N$。至此，我们定义了商模 M/N。另外，自然的投影映射是 A-模同态：

$$\pi : M \to M/N, \quad m \mapsto m+N.$$

这个同态是满射。

命题 13. *M 和 M' 是 A-模，$N \subset M$ 是子模，$\varphi : M \to M$ 是 A-模同态。如果 $N \subset \mathrm{Ker}(\varphi)$，那么存在唯一的 A-模同态 $\overline{\varphi} : M/N \to M'$，使得 $\overline{\varphi} \circ \pi = \varphi$，其中，$\pi : M \to M/N$ 是自然的同态。*

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & M' \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \overline{\varphi}} & \\ M/N & & \end{array}$$

进一步，我们还有 A-模同构 $\overline{\varphi} : M/\mathrm{Ker}(\varphi) \xrightarrow{\simeq} \mathrm{Im}(\varphi)$。

证明： 对任意 $m+N$，定义

$$\overline{\varphi}(m+N) = \varphi(m).$$

现在验证这是良好定义的：对 $m+N = m'+N$，$m-m' \in N \subset \mathrm{Ker}(\varphi)$，从而，$\varphi(m) = \varphi(m')$。容易看出，映射 $\overline{\varphi}$ 是 A-模同态并且 $\overline{\varphi} \circ \pi = \varphi$。

选取 $N = \mathrm{Ker}(\varphi)$，我们显然有满射

$$\overline{\varphi} : M/\mathrm{Ker}(\varphi) \twoheadrightarrow \mathrm{Im}(\varphi).$$

根据定义，$\varphi(m+N) = 1$ 当切仅当 $m \in \mathrm{Ker}(\varphi)$，所以该同态是单射，从而为同构。 □

2.6 对称群 $\mathfrak{S}_n$

这一节研究有限集 X 的对称群 $\mathfrak{S}_X$。不妨设 $X = \{1, 2, \cdots, n\}$ 并 $\mathfrak{S}_X$ 记为 $\mathfrak{S}_n$。按照定义，每个 $g \in \mathfrak{S}$ 都是 $\{1, 2, \cdots, n\}$ 到自身的双射，即

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

其中，$\{i_1, i_2, \cdots, i_n\} = \{1, 2, \cdots, n\}$，也就是说 $(i_1, i_2, \cdots, i_n)$ 是 $\{1, 2, \cdots, n\}$ 的一个排列。从而，$|\mathfrak{S}_n| = n!$。我们用下面的记号来表示 g：

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

例子 2.34. $\mathfrak{S}_2$ 有 2 个元素，即 1 和 $g=\begin{pmatrix}1&2\\2&1\end{pmatrix}$。此时，$g^2=1$。从而，$\mathfrak{S}_2\simeq\mathbb{Z}/2\mathbb{Z}$。从 $\mathfrak{S}_2$ 到 $\mathbb{Z}/2\mathbb{Z}$ 的同构映射为 $\varphi:1\mapsto\overline{0},\ g\mapsto\overline{1}$。

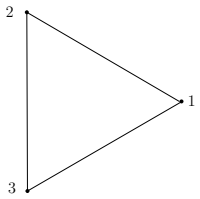
例子 2.35. $\mathfrak{S}_3$ 有 6 个元素，罗列如下：

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

我们可以直接验证如下的乘积关系：

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

并且 $r^3=1=s^2$ 并且 $srs=r^{-1}$。这与 $\mathfrak{D}_3$ 群中元素乘法满足的关系一致。我们据此断言 $\mathfrak{S}_3$ 与 $\mathfrak{D}_3$ 是同构的。实际上，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_2，2 映射成顶点 i_3，从而，g 可以被看作是 $\mathfrak{S}_3$ 中的元素 $\varphi(g)=\begin{pmatrix}1&2&3\\i_1&i_2&i_3\end{pmatrix}$。这就定义了

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

这是群同态（这恰好是下一章群作用的观点）。由于三角形的顶点的移动决定了三角形，以上 i_1,i_2,i_3 就决定了 g。从而，φ 是单射。考虑到 $|\mathfrak{S}_3|=|\mathfrak{D}_3|=6$，$\varphi$ 是群同构。另外，$\mathfrak{D}_3$ 的 r（旋转 $\frac{2\pi}{3}$）和 s（以过点 1 和对边中点的线为轴的对称）的作用恰好对应 $\mathfrak{S}_3$ 中的 r 和 s。

我们考虑 $\mathfrak{S}_n$ 中一种特殊的映射：**循环**。给定 $k\leqslant n$ 和 k 元子集 $\{x_1,\cdots,x_k\}\subset\{1,\cdots,n\}$，按如下方式定义 $\{1,\cdots,n\}$ 到自身的双射 σ：

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

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

$$x_1\mapsto x_2\mapsto\cdots x_k\mapsto x_1.$$

这样的 σ 被称作是一个k-**循环**并简记为 $(x_1,x_2,\cdots,x_k)$，k 也被称作是 σ 的长度。2-**循环** (x,y)（总假设 $x\neq y$）被称作是**对换**：它把 x 和 y 交换位置而保持其余位置不变。我们规定2-**循环**就是恒等映射。

给定 k-循环 $\sigma=(x_1,x_2,\cdots,x_k)$ 和 l-循环 $\tau=(y_1,y_2,\cdots,y_l)$，如果 $\{x_1,\cdots,x_k\}\cap\{y_1,\cdots,y_l\}=\emptyset$，就称它们是**不交的**。如果循环 σ 和 τ 不交，那么它们交换，即 $\sigma\cdot\tau=\tau\cdot\sigma$。

对任意 $\sigma=\begin{pmatrix}1 & \cdots & n\\ \sigma(1) & \cdots & \sigma(n)\end{pmatrix}\in\mathfrak{S}_n$（这个记号即说明 $\sigma: k\mapsto\sigma(k)$。

从某个 x_1 出发，x_1 被 σ 映射到 x_2，x_2 被 σ 映射到 x_3，如此往复，存在这样的 k，使得 x_k 又被 σ 映射到 x_1。我们还要求 k 是最小的。

我们再在集合 $\{1,2,\cdots,n\}-\{x_1,\cdots,x_k\}$ 上重复以上过程，即从某个 x_{k+1} 出发，x_{k+1} 被 σ 映射到 x_{k+2}，x_{k+2} 被 σ 映射到 x_{k+3}，如此往复，使得第一次出现 l，x_{l+l} 被 σ 映射回 x_{k+1}。根据构造，我们显然有 $\{x_1,x_2,\cdots,x_k\}\cap\{x_{k+1},x_{k+2},\cdots,x_{k+l}\}=\emptyset$。

继续以上过程，g 的作用就于如下两两不相交的循环之积相同：

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

根据构造，这些循环是由 g 唯一决定的。

命题 14. *$\mathfrak{S}_n$ 中每个元素均可唯一地（不计顺序）表示成两两不交的循环之积。特别地，由循环构成的子集可生成 $\mathfrak{S}_n$。*

注记 2.25. 对于 $g\in\mathfrak{S}_n$，把它分解为 $g=\sigma_1\cdot\sigma_2\cdots\sigma_m$，其中，$\sigma_1,\cdots,\sigma_m$ 分别是长度为 $k_1,k_2,\cdots,k_m$ 的循环并且 $k_1\geqslant k_2\geqslant\cdots\geqslant k_m$ 并且 $k_1+\cdots+k_m=n$（要求在 g 作用下不动的数对应着 1-循环）。按照以上规则，我们就称 g 是$(k_1,\cdots,k_m)$**-型**的。

例子 2.36. 考虑 $\mathfrak{S}_8$ 中的元素：

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

根据上面命题的推理过程，容易得到 $\alpha=(1,2,4,5)(3,6)$，它这是 $(4,2,1,1)$-型的。

我们还可以考虑

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

容易看出 $\beta=(1,2,3,7,4,8,5)$，从而是 $(7,1)$-型的。另外，我们还可以把 β 写成下面循环的乘积：

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

后两个循环是相交的，这和上述命题唯一性的部分不矛盾。

注记 2.26 (共轭的计算)**.** 对 $g\in\mathfrak{S}_n$，其共轭

$$\mathrm{Int}(g):\mathfrak{S}_n\to\mathfrak{S}_n,\quad \sigma\mapsto g\sigma g^{-1},$$

的计算是关于 $\mathfrak{S}_n$ 研究中最基本的技术手段。

先研究 g 对 k-循环 $\sigma=(x_1,\cdots,x_k)$ 的共轭。分情况计算 $\big(g\cdot\sigma\cdot g^{-1}\big)(g(x))$：

- $x=x_j$。此时，
$$\big(g\cdot\sigma\cdot g^{-1}\big)(g(x_j))=g(x_{j+1}),\quad x_{k+1}=x_1.$$
- $x\notin\{x_1,\cdots,x_k\}$。此时，
$$\big(g\cdot\sigma\cdot g^{-1}\big)(g(x))=g(x).$$

综上所述，我们得到共轭公式：

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

练习 2.4. 证明，若 $n \geqslant 3$，则 $\mathfrak{S}_n$ 的中心是平凡的，即 $\mathrm{Z}(\mathfrak{S}_n) = 1$。

命题 15. *$\mathfrak{S}_n$ 中的元素 α 和 β 共轭（即有 $g \in \mathfrak{S}_n$，使得 $g\alpha g^{-1} = \beta$）当且仅当它们具有相同的型。*

证明: 对于 $(k_1, \cdots, k_m)$-型的 $\sigma \in \mathfrak{S}_n$，有 $\sigma = \sigma_1 \cdot \sigma_2 \cdots \sigma_m$，其中，$\sigma_i$ 为 k_i-循环。我们计算其共轭：

$$\mathrm{Int}(g)(\sigma) = g\sigma_1 g^{-1} \cdot g\sigma_2 g^{-1} \cdots g\sigma_m g^{-1}.$$

上述公式表明 $g\sigma_i g^{-1}$ 仍为 k_i-循环，从而，$\mathrm{Int}(g)(\sigma)$ 与 g 具有相同的型。反之，任给两个 $(k_1, \cdots, k_m)$-型的元素：

$$\begin{cases} \alpha = (x_1, \cdots, x_{k_1})(x_{k_1+1}, \cdots, x_{k_1+k_2}) \cdots (x_{k_1+\cdots+k_{m-1}+1}, \cdots, x_n), \\ \beta = (y_1, \cdots, y_{k_1})(y_{k_1+1}, \cdots, y_{k_1+k_2}) \cdots (y_{k_1+\cdots+k_{m-1}+1}, \cdots, y_n), \end{cases}$$

我们定义 $g \in \mathfrak{S}_n$ 使得对 $i = 1, \cdots, n$，$g(x_i) = y_i$。根据上述公式，$g\alpha g^{-1} = \beta$。从而， □

注记 2.27. 对于群 G 以及 $x, y \in G$，如果存在 $g \in G$，使得 $gxg^{-1} = y$，就称x **与** y **共轭**并记作 $x \sim y$。这显然是 G 上的一个等价关系。给定 $g \in G$，用 $\mathrm{Conj}(g)$ 表示与 g 共轭的元素的集合。据此，我们可以把 G 分划称如下的共轭类的无交并：

$$G = \coprod_{[g] \in G/\sim} \mathrm{Conj}(g).$$

根据上述命题，$\mathfrak{S}_n$ 的共轭类由其型决定，从而，其共轭类的个数是将 n 分拆成若然个不同的正整数之和的方式的个数。

当 $n = 4$ 时，由于 $4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$，从而 $\mathfrak{S}_4$ 有 5 个共轭类。

本节之末我们会用 $\mathfrak{S}_n$ 的共轭类来研究其自同构群 $\mathbf{Aut}(\mathfrak{S}_n)$。

注记 2.28 (对称群的共轭映射的意义)**.** 给定 n 元集合 X 和 Y 并考虑相应的对称群 $\mathfrak{S}_X$ 和 $\mathfrak{S}_Y$，它们分别是 X 和 Y 到自身的双射在映射复合作为乘法下所构成的群。

现在任意指定双射 $f : X \to Y$，据此可以构造 $\mathfrak{S}_X$ 与 $\mathfrak{S}_Y$ 之间的群同构，由如下交换图定义：

$$\begin{array}{ccc} X & \xrightarrow{\sigma} & X \\ {\scriptstyle f}\downarrow & \overset{f^{-1}}{\nwarrow} & \downarrow{\scriptstyle f} \\ Y & \xrightarrow{f\circ\sigma\circ f^{-1}} & Y \end{array}$$

即定义映射

$$F_f : \mathfrak{S}_X \to \mathfrak{S}_Y, \quad \sigma \mapsto F_f(\sigma) = f \circ \sigma \circ f^{-1}.$$

容易证明 F_f 是群同构。

作为例子，选取 $X = Y = \{1, 2, \cdots, n\}$，$f = g \in \mathfrak{S}_n$，则 g 可被视为 $\mathfrak{S}_n$ 中的元素并具有明显的意义：将 $1, 2, \cdots, n$ 重新标号。此时，上述 F_f 就是共轭 $\mathrm{Int}(g)$，它的含义是将 $\{1, 2, \cdots, n\}$ 重新标注顺序后对 $\mathfrak{S}_n$ 的影响。

定理 16. *对换 $\{(x, y) | 1 \leqslant x < y \leqslant n\}$ 的集合生成 $\mathfrak{S}_n$，即每个 $\mathfrak{S}_n$ 可以写成对换之积。进一步，对于 $\sigma \in \mathfrak{S}_n$，若*

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

是把 σ 写成对换之积的两种方式，则 $k - l$ 是偶数。

证明：只要证明轮换可被写成对换之积即可。实际上，我们容易验证

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

或者

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

现在证明 $k - l$ 是偶数。将等式 $\sigma_1' \cdot \sigma_2' \cdots \sigma_k' = \sigma_1'' \cdot \sigma_2'' \cdots \sigma_l''$ 左边的元素逐一取逆，我们得到

$$1 = \sigma_1'' \cdot \sigma_2'' \cdots \sigma_l'' \cdot \sigma_k' \cdot \sigma_2' \cdots \sigma_1'.$$

所以，该命题等价于证明若 1 可以写成对换之积 $1 = \sigma_1 \cdot \sigma_2 \cdots \sigma_m$，则 m 是偶数。

我们对 n 进行归纳。当 $n = 1$ 或 2 时，命题是明显的。当 $n \geqslant 3$，$1 \leqslant i, j, k \leqslant n - 1$ 并且 i, j, k 两两不同，我们有如下等式：

$$\begin{cases} (a). \quad (i, n)(j, k) = (j, k)(i, n), \\ (b). \quad (i, n)(i, j) = (i, j)(j, n), \\ (c). \quad (i, n)(j, n) = (i, j)(i, n). \end{cases}$$

1) 若 $\{\sigma_1, \sigma_2, \cdots, \sigma_m\}$ 中没有形如 (i, n) 的对换，其中，$i < n$，则 σ 可以被视为 $\mathfrak{S}_{n-1}$ 中的元素。根据归纳假设，m 是偶数。

2) 若 $\{\sigma_1, \sigma_2, \cdots, \sigma_m\}$ 中有形如 (i, n) 的对换（姑且称之为带 n 的对换），我们利用 (a) 和 (b) 将 (i, n) 型的对换挪向右边。在这个过程中，如果有 (i, n) 与 (j, n) 型的两个对换相邻，我们就用 (c) 消去其中的一个带 n 的对换或者用 $(i, n)(i, n) = 1$ 消去两个带 n 的对换。以上操作保证了 $\{\sigma_1, \sigma_2, \cdots, \sigma_m\}$ 中带 n 的对换的个数减少，直至最多有一个带 n 的对换并且（若存在）这个带 n 的对换只能是 σ_m（在最右边）。现在证明，将 1 分解为对换之积，只有 σ_m 为带 n 的对换是可能的。否则，考虑如下等式

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

左边 n 会被调到其它位置而右边所有对换都保持了 n，矛盾。

此时我们回到了 1) 的情况，可再次用归纳假设完成证明。

证毕。 □

定义 2.11. 若 $\sigma \in \mathfrak{S}_n$ 是偶数个对换之积，就称 σ 为**偶置换**；否则称为**奇置换**。据此，我们定义**指标映射**：

$$\varepsilon : \mathfrak{S}_n \to \{\pm 1\}, \quad \sigma \mapsto \begin{cases} 1, & \sigma \text{ 是偶置换}; \\ -1, & \sigma \text{ 是奇置换}. \end{cases}$$

将 $\{\pm 1\}$ 等同为 2 阶循环群，则 ε 群同态并且当 $n \geqslant 2$ 时是满射。另外，n 阶**交错群**$\mathfrak{A}_n$ 被定义为：

$$\mathfrak{A}_n = \mathrm{Ker}\big(\varepsilon : \mathfrak{S}_n \to \{\pm 1\}\big).$$

这是偶置换的集合。

注记 2.29. 我们有如下正合列

$$1 \to \mathfrak{A}_n \xrightarrow{\subset} \mathfrak{S}_n \xrightarrow{\varepsilon} \{\pm 1\} \to 1.$$

特别地，当 $n \geqslant 2$ 时，$|\mathfrak{A}_n| = \frac{1}{2} n!$。

例子 2.37. $\sigma=(x_1,\cdots,x_k)$ 是 k-循环，则 $\varepsilon(\sigma)=(-1)^{k+1}$。

命题 17. 令 $n\geqslant 3$，$\mathfrak{A}_n$ 可以被如下子集生成：

$$\begin{cases} A=\big\{(i,j)(k,l)\big|1\leqslant i,j,k,l\leqslant n, i\neq j, k\neq l\big\},\\ B=\big\{(i,j,k)\big|1\leqslant i,j,k\leqslant n, i\neq j, i\neq k, k\neq j\big\}. \end{cases}$$

证明：根据 $\mathfrak{A}_n$ 的定义，$\langle A\rangle=\mathfrak{A}_n$。为了证明 B 可以生成 $\mathfrak{A}_n$，只要证明每个形如 $(i,j)(k,l)$ 的元素可被写成 3-循环之积即可，其中，$1\leqslant i,j,k,l\leqslant n$ 并且 $i\neq j, k\neq l$。我们分情形讨论：

1) $\big|\{i,j\}\cap\{k,l\}\big|=2$。此时，$(i,j)(k,l)=1$，结论显然成立。

2) $\big|\{i,j\}\cap\{k,l\}\big|=1$，不妨设 $j=k$。此时，$(i,j)(k,l)=(i,j)(j,l)=(i,j,l)$ 是 3-循环。

3) $\big|\{i,j\}\cap\{k,l\}\big|=\emptyset$。此时，我们有

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

根据 2) 的结论，上式是两个 3-循环之积。

综上所述，命题得证。 □

例子 2.38. $(1,2,3)$ 生成了 $\mathfrak{A}_3$。特别地，$\mathfrak{A}_3\simeq{}^{\mathbb{Z}}\!/\!_{3\mathbb{Z}}$。

命题 18. 假设 $n\geqslant 2$，则 $\mathfrak{S}_n$ 可以被以下子集生成：

- $S_*=\big\{(k,k+1)\big|k=1,\cdots,n-1\big\}$，其中，$S_*$ 中的元素被称作是**基本对换**；
- $S_1=\big\{(1,k)\big|k=2,\cdots,n\big\}$；
- $S_2=\big\{(1,2),(1,2,\cdots,n)\big\}$。

证明：对于 S_1，根据共轭公式，对任意的 $i<j$，$(i,j)=(1,i)(1,j)(1,i)$，从而，$\langle S_1\rangle$ 包含了所有对换，所以，$\langle S_1\rangle=\mathfrak{S}_n$。

对于基本对换的集合 S_*，对 k 归纳来证明 $(1,k)\in\langle S_*\rangle$。首先，$k=1,2$ 时结论显然成立。假设 $(1,k)\in\langle S_*\rangle$，根据共轭公式，有 $(k,k+1)(1,k)(k,k+1)=(1,k+1)$，这就完成了归纳证明。所以，$S_1\subset\langle S_*\rangle$，根据上面的结论，$\langle S_*\rangle=\mathfrak{S}_n$

对于 S_2，令 $g=(1,2,\cdots,n)$。对任意则 $k\leqslant n-2$，我们有

$$g^k(1)=k+1,\ g^k(2)=k+2.$$

利用共轭公式，我们有

$$g^k\cdot(1,2)\cdot g^{-k}=(k,k+1), k=0,1,\cdots,n-2.$$

所以，$S_*\subset\langle S_2\rangle$，从而 $\langle S_2\rangle=\mathfrak{S}_n$

□

例子 2.39 (逆序对与最短的基本对换之积)**.** 假设 $n\geqslant 2$，对任意 $g=\begin{pmatrix}1&\cdots&n\\ g(1)&\cdots&g(n)\end{pmatrix}\in\mathfrak{S}_n$，定义

$$\ell(g)=\big|\{(i,j)\big|1\leqslant i<j\leqslant n, g(i)>g(j)\}\big|.$$

如果 $1 \leqslant i < j \leqslant n$ 而 $g(i) > g(j)$，我们就说 (i,j) 是 g 的一个逆序对。以上，$\ell(g)$ 为所有 g 的逆序对的个数。

任意 $g \in \mathfrak{S}_n$，我们将 $g = \sigma_1 \cdot \sigma_m$ 写成基本对换的积，即要求 $\sigma_i \in S_*$。那么，$m \geqslant \ell(g)$ 并且可以将 g 写成 $\ell(g)$ 个基本对换之积。

如果 $\ell(g) = 0$，只能有 $g = 1$，以上结论显然成立。如果 $\ell(g) > 0$，必然存在 k，使得 $g(k) > g(k+1)$，此时，$g \cdot (k, k+1)$ 与 g 相比，逆序对恰好减少 1。重复以上操作，就得到 $m \geqslant \ell(g)$ 并给出了将 g 写成 $\ell(g)$ 个基本对换之积的构造。

特别地，$g \in \mathfrak{A}_n$ 当且仅当 $\ell(g)$ 是偶数。

练习 2.5. 当 $n \geqslant 3$ 时，证明，$|i_0 - j_0|$ 与 n 互素，则 $\{(i_0, j_0), (1, 2, \cdots, n)\}$ 生成 $\mathfrak{S}_n$。

例子 2.40 ($n \neq 2, 6$，$\mathbf{Out}(\mathfrak{S}_n) = 1$)**.** 假设 $n \geqslant 3$。由于 $\mathrm{Z}(\mathfrak{S}_n) = 1$，根据正合列(2.1)，$\mathfrak{S}_n$ 的内自同构群与 $\mathfrak{S}_n$ 同构。我们现在研究 $\mathfrak{S}_n$ 的外自同构，请参考正合列(2.2)。

任意选定 $\varphi \in \mathbf{Aut}(\mathfrak{S}_n)$，$\varphi$ 将共轭的元映成共轭的元素，将 $\mathfrak{S}_n$ 的共轭类映成共轭类：对于共轭类 $\mathrm{Cong}(g)$，$\varphi(\mathrm{Cong}(g))$ 可能与 $\mathrm{Cong}(g)$ 不同；对不同的共轭类 $\mathrm{Cong}(g)$ 和 $\mathrm{Cong}(h)$，一定有 $\varphi(\mathrm{Cong}(g)) \neq \varphi(\mathrm{Cong}(h))$。

考虑如下特殊的共轭类：

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

其中，$2k \leqslant n$，$\sim$ 表示共轭关系。对任意 $\sigma \in T_1$，$\sigma^2 = 1$，从而 $\varphi(\sigma)^2 = 1$。通过考虑将 $\varphi(\sigma)$ 分解为轮换：

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

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

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

我们现在考虑方程 $|T_1| = |T_k|$：

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

除 $1, 2$ 之外，任何两个连续整数之积有奇素数因子，上式要求 $n - 2 = n - k + 1$，即 $k = 3$，此时，

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

所以，当 $n \neq 6$ 时，$|T_1| = |T_k|$ 等价于 $k = 1$，φ 将对换映射为对换。考虑 $\mathfrak{S}_n$ 的生成元的集合

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

并称 σ_{k-1} 和 σ_k 是相邻的。若以上两元素不相邻，则它们交换。假设

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

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，可以假设

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

再考虑 $\varphi\big((3,4)\big) = (z_1, z_2)$。类似地推理给出 $\{x_2, x_3\} \cap \{z_1, z_2\} \neq \emptyset$。另外，$(1,2)$ 和 $(3,4)$ 交换，所以 (x_1, x_2) 和 (z_1, z_2) 交换。据此，$\{x_2, x_3\} \cap \{z_1, z_2\} = \{x_3\}$。通过重新标号，我们有 $\varphi\big((3,4)\big) = (x_3, x_4)$，其中，$x_1, x_2, x_3, x_4$ 两两不同。如此往复，我们最终得到

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

所以可选取

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

使得，$\varphi\big((k-1,k)\big) = \mathrm{Int}(\sigma)\big((k-1,k)\big)$。这些关系在 $\mathfrak{S}_n$ 的生成元集合上成立，从而，$\varphi = \mathrm{Int}(\sigma)$。综上所述，若 $n \neq 6$，则 $\mathfrak{S}_n$ 的每个自同构都是内自同构，即 $\mathrm{Out}(\mathfrak{S}_n) = 1$。

注记 2.30. 当 $n = 6$ 时，公式

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

给出 $k = 3$。此时，可能存在 φ，使得 $\varphi(T_1) = T_3$。此时，必然有 $\varphi(T_3) = T_1$。通过复合，$\varphi^2(T_1) = T_1$。以上的推导对于 φ^2 仍成立，从而 φ^2 是内自同构。

进一步，任给 $\varphi, \varphi' \in \mathbf{Aut}(\mathfrak{S}_6)$，若 $\varphi(T_1) = T_3$ 和 $\varphi'(T_1) = T_3$，则 $(\varphi \cdot \varphi')(T_1) = T_1$，同样的理由表明 $\varphi \cdot \varphi'$ 是内自同构。这说明 $\mathbf{Aut}(\mathfrak{S}_6)/\mathrm{Im(Int)}$ 中至多有两个元素。从而，$\mathbf{Out}(\mathfrak{S}_6) = 1$ 或者 $\mathbb{Z}/2\mathbb{Z}$。

我们之后会构造 $\mathfrak{S}_6$ 的非共轭自同构，从而证明 $\mathfrak{S}_6 \simeq \mathbb{Z}/2\mathbb{Z}$。

2.7 习题

2.7.1 乘积结构

1. $(G_1, \cdot_1)$ 和 $(G_2, \cdot_2)$ 是群，在 $G_1 \times G_2$ 上如下定义乘法：

   $$(g_1, g_2) \cdot (g_1', g_2') := \big(g_1 \cdot_1 g_1', g_2 \cdot_2 g_2'\big).$$

   证明，在以上乘法下，$G_1 \times G_2$ 是群并且其单位元为 $(1_1, 1_2)$。这个群被称为 G_1 与 G_2 的**乘积**。

2. 证明，投影映射

   $$\pi_1 : G_1 \times G_2 \to G_1, \ \ (g_1, g_2) \mapsto g_1,$$

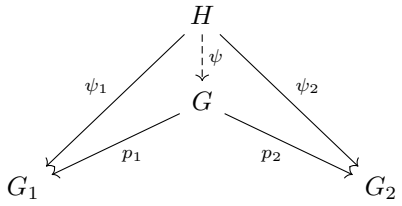
   和

   $$\pi_2 : G_1 \times G_2 \to G_2, \ \ (g_1, g_2) \mapsto g_2,$$

   是群同态。它们的核是什么?

3. (泛性质) 给定群 $(G_1, \cdot_1)$ 和 $(G_2, \cdot_2)$。证明，存在唯一的[7]群 G 以及唯一的群同态 $p_i : G \to G_i$ $(i = 1, 2)$ 使得对任意的群 H 和任意的群同态 $\varphi_i : H \to G_i$ $(i = 1, 2)$，存在唯一的 $\psi : H \to G$，使得 $p_i \circ \psi = \varphi_i$ $(i = 1, 2)$。

[7]在同构的意义下



特别地，我们有如下的集合之间的同构：

$$\mathrm{Hom}(H, G_1 \times G_2) \simeq \mathrm{Hom}(H, G_1) \times \mathrm{Hom}(H, G_2), \quad \psi \mapsto \big(p_1 \circ \psi, p_2 \circ \psi\big).$$

（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）

4. 给定互素的正整数 n_1 和 n_2。利用 A3) 证明，

$$\mathbb{Z}/_{n_1 n_2 \mathbb{Z}} \to \mathbb{Z}/_{n_i \mathbb{Z}}, \quad \overline{k} \mapsto k \pmod{n_i}, \quad i = 1, 2,$$

给出了群同构

$$\mathbb{Z}/_{n_1 n_2 \mathbb{Z}} \xrightarrow{\simeq} \mathbb{Z}/_{n_1 \mathbb{Z}} \times \mathbb{Z}/_{n_2 \mathbb{Z}}.$$

以上，$\mathbb{Z}/_{n\mathbb{Z}}$ 表示的是（加法）循环群。

5. 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？

6. $(A_1, +_1, \cdot_1)$ 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 $\cdot$：

$$(a_1, a_2) + (a_1', a_2') := \big(a_1 +_1 a_1', a_2 +_2 a_2'\big), \quad (a_1, a_2) \cdot (a_1', a_2') := \big(a_1 \cdot_1 a_1', a_2 \cdot_2 a_2'\big).$$

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

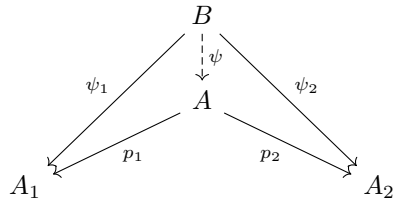
$$\pi_1 : A_1 \times A_2 \to A_1, \quad (a_1, a_2) \mapsto a_1,$$

和

$$\pi_2 : A_1 \times A_2 \to A_2, \quad (a_1, a_2) \mapsto a_2,$$

是环同态。

7. （泛性质）给定环 A_1 和 A_2。证明，存在唯一的[8]环 A 以及唯一的环同态 $p_i : A \to A_i$（$i = 1, 2$）使得对任意的环 B 和任意的环同态 $\varphi_i : B \to A_i$（$i = 1, 2$），存在唯一的 $\psi : B \to A$，使得 $p_i \circ \psi = \varphi_i$（$i = 1, 2$）。



[8]在同构的意义下

8. 给定互素的正整数 m 和 n。证明，我们有**环同构**[9]

$$\mathbb{Z}/_{mn\mathbb{Z}} \xrightarrow{\simeq} \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}}.$$

（提示：使用中国剩余定理）

9. 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

$$(A \times_{\text{ring}} B)^\times \simeq A^\times \times_{\text{group}} B^\times,$$

其中，$\times_{\text{ring}}$ 代表着环的乘积，$\times_{\text{group}}$ 代表着群的乘积。

2.7.2 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 $1, \cdots, n$ 中与 n 互素的数的个数：

$$\phi(n) = \left|\left\{1 \leqslant k \leqslant n \middle| (k,n) = 1\right\}\right|.$$

1. 证明，$\left|\left(\mathbb{Z}/_{n\mathbb{Z}}\right)^\times\right| = \phi(n)$，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。

2. 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：

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}).$$

3. 证明，对任意正整数 n，对任意与 n 互素的整数 a，有 $a^{\phi(n)} \equiv 1 \ (\text{mod} n)$。特别地，当 p 为素数时，这给出了 Fermat 小定理。

4. （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 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，$d|n$。

5. 证明，对任意的正整数 n，我们有公式

$$n = \sum_{d|n} \phi(d).$$

6. 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，

$$n = \sum_{d|n, G_d \neq \emptyset} \phi(d).$$

7. 证明，G 是循环群。

8. 证明，$\left(\mathbb{Z}/_{p\mathbb{Z}}\right)^\times$ 是循环群，其中，p 是素数。

9. 对于奇素数 p 和 $m \geqslant 2$，我们证明 $\left(\mathbb{Z}/_{p^m\mathbb{Z}}\right)^\times$ 是循环群：

[9] 请与第四问对比

- 证明，$(1+p)^{p^k} \equiv 1+p^{k+1} \mod p^{k+2}$，其中 $k \geqslant 0$。据此证明 $\overline{p+1} \in \left(\mathbb{Z}/p^m\mathbb{Z}\right)^\times$ 的阶为 p^{m-1}。
- 证明，存在 $\overline{k} \in \left(\mathbb{Z}/p^m\mathbb{Z}\right)^\times$，其阶为 $p-1$。
- 证明，存在 $\bar{l} \in \left(\mathbb{Z}/p^m\mathbb{Z}\right)^\times$，使得 $\langle \bar{l} \rangle = \left(\mathbb{Z}/p^m\mathbb{Z}\right)^\times$。

10. 对于 $m \geqslant 2$，我们给出 $\left(\mathbb{Z}/2^m\mathbb{Z}\right)^\times$ 的结构：

    - 证明，$(1+2^2)^{2^k} \equiv 1+2^{k+2} \mod 2^{k+3}$，其中 $k \geqslant 0$。据此证明，$\overline{5} \in \left(\mathbb{Z}/2^m\mathbb{Z}\right)^\times$ 的阶为 2^{m-2}。
    - 证明，映射（以下左边是加法群，右边是乘法群）

    $$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z} \longrightarrow \left(\mathbb{Z}/2^m\mathbb{Z}\right)^\times, \quad (a,b) \mapsto (-1)^a 5^b \mod 2^m.$$

    是群同构。

11. （Gauss）证明，对任意正整数 n，$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ 是循环群当且仅当 n 形如 $1, 2, 4, p^m$ 或 $2p^m$，其中，$m \geqslant 1$ 而 p 为奇素数。此时，$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ 的每个生成元 $\bar{l}$ 都被称为 n 的**原根**。

2.7.3 线性群中元素的阶的几个命题

1. 令 $\mathbf{M}_n(\mathbb{Z})$ 为整系数的 $n \times n$ 矩阵的集合，令

$$\mathbf{GL}(n;\mathbb{Z}) = \left\{A \in \mathbf{M}_n(\mathbb{Z}) \middle| \ A\text{可逆并且 } A^{-1} \in \mathbf{M}_n(\mathbb{Z})\right\}.$$

- 证明，$\mathbf{GL}(n;\mathbb{Z}) = \left\{A \in \mathbf{M}_n(\mathbb{Z}) \middle| \det(A) = \pm 1\right\}$。
- 如果 $A \in \mathbf{GL}(2;\mathbb{Z})$ 的阶有限，证明，$\mathrm{ord}(A) \in \{1,2,3,4,6\}$。
- 证明，存在只依赖于 n 的常数 C_n，若 $A \in \mathbf{GL}(n;\mathbb{Z})$ 的阶有限，则 $\left|\mathrm{ord}(A)\right| \leqslant C_n$。

2. p 是素数，q 是 p 的幂，域 $\mathbb{F}_q$ 有 q 个元素。我们已知 $\mathbf{GL}(n;\mathbb{F}_q)$ 共有 $\prod_{k=0}^{n-1}(q^n - q^k)$ 个元素。

- 对任意的 $A \in \mathbf{GL}(n;\mathbb{F}_q)$，证明，集合 $\left\{P(A) \middle| P \in \mathbb{F}_q[X]\right\}$ 至多有 q^n 个元素。以上，对于 $P(X) = \sum_{k=0}^{n} a_k X^k$，其中，$a_k \in \mathbb{F}_q$，我们定义 $P(A) = \sum_{k=0}^{n} a_k \cdot A^k$。
- 证明，对任意的 $A \in \mathbf{GL}(n;\mathbb{F}_q)$，$\mathrm{ord}(A) \leqslant q^n - 1$。
- 给定如下的结论：存在 $K = \mathbb{F}_q$ 的域扩张 $L = \mathbb{F}_{q^n}$，使得 $[L:K] = n$。证明，存在 $A \in \mathbf{GL}(n;\mathbb{F}_q)$，$\mathrm{ord}(A) = q^n - 1$。

所以，$\mathbf{GL}(n;\mathbb{F}_q)$ 中元素的阶的最大值恰好是 $q^n - 1$。

2.7.4 有限群乘积的消去定理

在练习题部分，我们将证明如下的**子群对应定理**：$\varphi : G \twoheadrightarrow G'$ 是满的群同态，我们有如下双射：

$$\left\{H \middle| H < G, H \supset \mathrm{Ker}(\varphi)\right\} \xrightarrow{1:1} \left\{H' \middle| H' < G'\right\}, \quad H \mapsto \varphi(H).$$

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。

这个定理可以用来研究有限群乘积的消去定理。

给定有限群 G, G'，以下两个数值是非负整数：

$$M\big(G,G'\big)=|\mathrm{Hom}(G,G')|,\quad I\big(G,G'\big)=\big|\{\varphi\in\mathrm{Hom}(G,G')\big|\varphi\text{ 为单射}\}\big|.$$

1. 证明如下等式，其中，以下是对所有 G 的正规子群 H 来求和：

$$M\big(G,G'\big)=\sum_{H\lhd G}I\left({}^{G}\!/_{H},G'\right)$$

2. 证明，对每个 G 的正规子群 H 存在整数 λ_H，使得

$$I\big(G,G'\big)=\sum_{H\lhd G}\lambda_H\cdot M\left({}^{G}\!/_{H},G'\right).$$

   特别地，以上等式中的系数 $\big\{\lambda_H\big|H\lhd g\big\}$ 不依赖于 G'。

3. 假设 G_1,G_2,G' 是有限群并且 $G_1\times G'\simeq G_2\times G'$。证明，$I\big(G_1,G'\big)=I\big(G_2,G'\big)$。

4. （消去定理）证明，若 G_1,G_2,G' 是有限群并且 $G_1\times G'\simeq G_2\times G'$，则 $G_1\simeq G_2$。

5. 令 G_1 和 G_2 为有限维 $\mathbb{F}_2$-线性空间，G' 为 $\mathbb{F}_2$-线性空间且其基有可数无限个元素。证明，$G_1\times G'\simeq G_2\times G'$。特别地，这一组 G_1,G_2,G' 不满足消去定理。

2.7.5 练习题

1. G 是群，$H\subset G$ 是有限子集并且对乘法封闭[10]。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 $G\times G\to G$，$(g_1,g_2)\mapsto g_1\cdot g_2$。假设以下两点成立：

   - 对任意的 $g,x,y\in G$，有 $g\cdot x=g\cdot y\quad\Rightarrow\quad x=y$；
   - 对任意的 $g,x,y\in G$，有 $x\cdot g=y\cdot g\quad\Rightarrow\quad x=y$。

   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，$H\lhd G$ 是正规子群。如果 $[G:H]=n$，其中，$n\geqslant 3$，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 $H\lhd G$ 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。

[10]即对任意的 $h_1,h_2\in H$，$h_1\cdot h_2\in H$。

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 $\mathrm{Int}(g)$ 的定义如下：

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

证明，以上映射给出群同态：

$$G \to \mathrm{Aut}(G), \quad g \mapsto \mathrm{Int}(g).$$

并且 $\mathrm{Ker}(\mathrm{Int}) = \mathrm{Z}(G)$ 而 $\mathrm{Im}(\mathrm{Int}) \lhd \mathrm{Aut}(G)$ 是正规子群。

11. 试在二面体群 $\mathfrak{D}_4$ 中找到两个子群 $K < H < G$，使得 $K \lhd H$，$H \lhd \mathfrak{D}_4$，但是 K 不是 $\mathfrak{D}_4$ 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 $K \lhd H$，$H \lhd G$。证明，如果 H 是循环群，那么 $K \lhd G$。

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 $\mathfrak{D}_4$ 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：

$$\varphi : G \to \mathfrak{S}_X, \quad g \mapsto \varphi(g) : x \mapsto g \cdot_G x, \quad \forall x \in X.$$

证明，G 是单的群同态（从而，$G \simeq \mathrm{Im}(\varphi)$）。

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

$$\mathrm{Inv} : G \to G,\ g \mapsto g^{-1}.$$

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，$\mathrm{Aut}\left(\mathbb{Z}/p\mathbb{Z}\right)$ 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

$$[H : H \cap K] \leqslant [G : K].$$

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，

$$[G : H \cap K] \leqslant [G : H][G : K].$$

并且等号成立当且仅当 $G = K \cdot H$。

23. $\varphi : G \to A$ 是群同态，A 是交换群。证明，G 中任意的包含 $\mathrm{Ker}(\varphi)$ 的子群都是正规子群。

24. 证明，$\mathrm{Z}(\mathfrak{S}_n) = 1$，其中，$n \neq 2$。

25. 试找出二面体群 $\mathfrak{D}_n$ 的所有正规子群，计算 $\mathrm{Z}(\mathfrak{D}_n)$ 并找出 $\mathfrak{D}_n$ 的所有共轭类。

26. 四元数群 $\mathbb{Q}_8$ 有多少共轭类?（参考第一次作业练习题 13）

27. $\mathfrak{S}_4$ 中有多少个子群同构于 $\mathfrak{S}_3$，有多少个子群同构于 $\mathfrak{S}_2$?

28. $\mathfrak{A}_4$ 中是否有 6 阶子群?

29. 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。

30.（第二同构定理）G 是群，$K < G$，$N \lhd G$。证明，$N \cap K \lhd K$ 并且有自然的群同构：

$$K\big/_{N \cap K} \xrightarrow{\simeq} NK\big/_{N}.$$

31.（第三同构定理）G 是群，$K \lhd G$，$H \lhd G$ 并且 $K < H$。证明，$H\big/_K \lhd G\big/_K$ 并且有自然的群同构：

$$\left(G\big/_K\right)\Big/\left(H\big/_K\right) \xrightarrow{\simeq} G\big/_H.$$

32.（子群对应定理）$\varphi : G \twoheadrightarrow G'$ 是满的群同态，我们有如下双射：

$$\left\{H \middle| H < G, H \supset \mathrm{Ker}(\varphi)\right\} \xrightarrow{1:1} \left\{H' \middle| H' < G'\right\}, \quad H \mapsto \varphi(H).$$

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 $N \lhd G$ 是正规子群，对 $G \to G\big/_N$ 使用子群对应定理，你得到什么结论?

33. G_i 是群，$N_i \lhd G_i$ 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

$$G_1\big/_{N_1} \times G_2\big/_{N_2} \xrightarrow{\simeq} G_1 \times G_2\big/_{N_1 \times N_2}.$$

34.（半直积：初见）G 是群，$K \lhd G$，$H \lhd G$，$K \cap H = 1$ 并且 $\langle K \cup H \rangle = G$。证明，$G\big/_K \simeq H$。

35. 请给出 8 阶群（在同构意义下）的清单。

3 群作用

3.1 基本定义

定义 3.1 (群作用)**.** 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 $x \in X$，对任意的 $(g, g') \in G \times G$，有 $g \cdot (g' \cdot x) = (g \cdot_G g') \cdot x$。

2) 对任意 $x \in X$，$1_G \cdot x = x$。

为了书写方便，通常用如下符号来记以上的群作用：${}^{G}\curvearrowright X$。

注记 3.1. 我们可以类似地定义群的**右作用**。要求存在映射

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

并满足

1) 对任意 $x \in X$ 和 $(g, g') \in G \times G$，有 $(x \cdot g) \cdot g' = x \cdot (g \cdot_G g')$。

2) 对任意 $x \in X$，$x \cdot 1_G = x$。

右作用可以被简记为 $X^{\curvearrowleft G}$。

例子 3.1. 给定群作用 ${}^{G}\curvearrowright X$ 和 $Y \subset X$，如果对任意 $g \in G, y \in Y$，$g \cdot y \in Y$，那么，

$$G \times Y \longrightarrow Y, \ \ (g, y) \mapsto g \cdot y,$$

是 G 在 Y 上的作用。

例子 3.2. 给定群作用 ${}^{G}\curvearrowright X$ 和子群 $H < G$，则

$$H \times X \longrightarrow X, \ \ (h, x) \mapsto h \cdot x,$$

是 H 在 Y 上的作用。

注记 3.2. 给定 G 在 X 上的作用等价于给定从 G 到 $\mathfrak{S}_X$ 的群同态 τ。

一方面，对任意 $x \in X$ 和 $g \in G$，定义 $\tau(g)(x) = g \cdot x$。这是 X 到自身的双射，其逆为 $\tau(g^{-1})$。根据群作用的定义，

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

是群同态。

另一方面，给定群同态 $\tau : G \to \mathfrak{S}_X$，定义映射

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

容易验证，这是 G 在 X 上的作用。

注记 3.3 (轨道分解)**.** 对于 $x, x' \in X$，若存在 $g \in G$，使得 $x = g \cdot x'$，则称 x, x' 属于同一**轨道**。这里，我们把 $x \in X$ 的轨道定义为

$$\mathrm{orb}(x) = G \cdot x = \big\{ g \cdot x \big| g \in G \big\}.$$

很明显，如果 x, x' 属于同一轨道，则 $\mathrm{orb}(x) = \mathrm{orb}(x')$（参考以下证明）。

群 G 对集合 X 的作用的一个重要性质就是它将 X 分解为不同轨道的无交并。

考虑 $x, y \in G$ 的轨道 $\mathrm{orb}(x)$ 和 $\mathrm{orb}(y)$，若 $\mathrm{orb}(x) \cap \mathrm{orb}(y) \neq \emptyset$，则 $\mathrm{orb}(x) = \mathrm{orb}(y)$。因为我们可以选 $g_1, g_2 \in G$，使得 $g_1 \cdot x = g_2 \cdot y$，从而，$g_2^{-1} g_1 x = y$。据此，

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

我们将 G 在 X 上（左）作用的轨道集合记为 ${}_{G}\backslash^{X}$（右作用情形记为 ${}^{X}/_{G}$）。

作为总结，我们有

$$X = \coprod_{g \in G} \mathrm{orb}(x) = \coprod_{{}_{G}\backslash^{X}} \mathrm{orb}(x),$$

并且当 X 是有限集时，有如下计数公式：

$$|X| = \sum_{{}_{G}\backslash^{X}} |\mathrm{orb}(x)|.$$

注记 3.4. 如果 X 中的点都在同一个轨道里，即 $\big|{}_{G}\backslash^{X}\big| = 1$，就称 G 在 X 上的作用是**传递**的。

考虑轨道 $\mathrm{orb}(x) \in {}_{G}\backslash^{X}$，由于 $G \cdot \mathrm{orb}(x) = \mathrm{orb}(x)$，$G$ 在该轨道上有自然的作用。这个作用明显是传递的。

根据轨道分解 $X = \coprod_{{}_{G}\backslash^{X}} \mathrm{orb}(x)$，通过研究传递的群作用可以理解 G 在 X 上的作用。

注记 3.5. 对任意 $g \in G$，如果 $g \cdot x = x$，就称 x 是 g 的一个**不动点**。对任意 $x \in X$，G 中使 x 不动的元构成子群，它被称作是 x 的**稳定化子**并记作 $\mathrm{Stab}_G(x)$ 或 $\mathrm{Stab}(x)$：

$$\mathrm{Stab}_G(x) = \big\{ g \in G \big| g \cdot x = x \big\}.$$

如果对任意 $x \in X$，$\mathrm{Stab}(x) = 1$，就称 G 的作用是**自由的**，也就是说除了单位元外，任何的 $g \in G$ 都没有不动点。

另外，若对任意 $g \in G - \{1\}$，存在 $x \in X$，使得 $g \cdot x \neq x$，就称 G 的作用是**忠实的**。${}^{G}\curvearrowright X$ 是忠实的等价于对应的群同态 $G \to \mathfrak{S}_X$ 是单射。

例子 3.3. 给定群作用 ${}^{G}\curvearrowright X$，即给定群同态 $\tau : G \to \mathfrak{S}_X$，我们自然有单的群同态

$${}^{G}/_{\mathrm{Ker}(\tau)} \longrightarrow \mathfrak{S}_X.$$

这给出忠实的群作用 ${}^{G}/_{\mathrm{Ker}(\tau)}\curvearrowright X$。

定义 3.2 (群作用之间的态射)**.** 群 G 在 X 上以及群 G' 在 X' 上的作用分别由如下映射给出：

$$\begin{cases} F : G \times X \longrightarrow X, \ \ (g, x) \mapsto g \cdot x, \\ F' : G' \times X' \longrightarrow X', \ \ (g', x') \mapsto g' \cdot x', \end{cases}$$

如果存在群同态 $\varphi : G \to G'$ 和映射 $\psi : X \to X'$，使得对任意 $g \in G$ 和 $x \in X$，有

$$\psi(g \cdot x) = \varphi(g) \cdot \psi(x),$$

就称 (φ, ψ) 是 ${}^{G}\!\curvearrowright\! X$ 到 ${}^{G'}\!\curvearrowright\! X'$ 的**态射**。

当 φ 为群同构并且 ψ 为双射是，就称 (φ, ψ) 是 ${}^{G}\!\curvearrowright\! X$ 到 ${}^{G'}\!\curvearrowright\! X'$ 的**同构**并说 ${}^{G}\!\curvearrowright\! X$ 和 ${}^{G'}\!\curvearrowright\! X'$ 是同构的。

以上定义中的态射可以用如下交换图来表示：

$$\begin{array}{ccc} G \times X & \xrightarrow{F} & X \\ {\scriptstyle \varphi\times\psi}\downarrow & & \downarrow{\scriptstyle \psi} \\ G' \times X' & \xrightarrow{F'} & X' \end{array}$$

3.2 群作用的基本例子

3.2.1 几何上的例子

例子 3.4. 给定集合 X 及其对称群 $\mathfrak{S}_X$，则

$$\mathfrak{S}_X \times X \longrightarrow X, \quad (g, x) \mapsto g(x),$$

是群作用。这个作用是传递的也是忠实的。对任意的 $x \in X$，$\mathrm{Stab}(x)$ 可以被看作是 $\mathfrak{S}_{X-\{x\}}$。

特别地，$\mathfrak{S}_n$ 自然地作用在 $\{1, 2, \cdots, n\}$ 上，即对任意的 k，$g \cdot k = g(k)$ 并且每个 $\mathrm{Stab}(k)$ 可以被看作是 $\mathfrak{S}_{n-1}$。

例子 3.5. K 是域，V 是有限维 K-线性空间，$\mathbf{GL}(V)$ 是 $\mathbf{End}_K(V)$ 中可逆 K-线性映射构成的群。那么，$\mathbf{GL}(V)$ 自然地作用在 V 上：

$$\mathbf{GL}(V) \times V \to V, \quad (g, v) \mapsto g \cdot v = g(v).$$

我们还考虑 $\mathbf{GL}(V)$ 的子群，它们也自然地作用在 V 上。

在应用时，通常考虑 $V = K^n$，此时 $\mathbf{GL}(V) = \mathbf{GL}(n; K)$。当 $K = \mathbb{F}_q$（q 个元素的有限域）时，$\mathbf{GL}(V) = \mathbf{GL}(n; \mathbb{F}_q)$ 是有限群。

例子 3.6 (群的表示)**.** K 是域，V 是 K-线性空间，G 在 V 上的一个**线性表示**或**表示**指的是群同态

$$\rho : G \to \mathbf{GL}(V).$$

其中，$\dim_K V$ 被称为该表示的**次数**。线性空间 V 也被称作是 G 的**表示空间**或者简称为 G 的**表示**。

表示 ρ 给出了 G 在 V 上的作用：

$$G \times V \to V, \quad (g, v) \mapsto g \cdot v = \rho(g)(v).$$

我们注意到对任意的 $g \in G$,

$$g : V \to V, \quad v \mapsto g(v),$$

是 K-线性同构。

简要回顾群代数 $K[G]$ 的概念，$K[G]$ 是 K 线性空间并有基 $\{e_g\}_{g\in G}$ 满足 $e_g \cdot e_{g'} = e_{gg'}$。用 g 代替 e_g，可以更简便地书写 $K[G]$ 的元素及其乘法：

$$x = \sum_{g\in G} x(g) \cdot g, \; y = \sum_{h\in G} y(h) \cdot h, \quad x \cdot y = \sum_{g\in G} \sum_{h\in G} x(g)y(h)g \cdot h.$$

其中,$x(g), h(g) \in K$。

如果 V 是 G 的表示，我们定义

$$K[G] \times V \to K[G], \quad (x, v) \mapsto x \cdot v = \sum_{g \in G} x(g) g \cdot v,$$

其中，$x = \sum_{g \in G} x(g) \cdot g$。从而，$V$ 成为 $K[G]$-模。

例子 3.7 (射影空间 $\mathbf{P}(V)$)**.** 给定 K-线性空间 V（这里我们假设其维数为 $n+1$），$\mathbf{P}(V)$ 是 V 中过原点的线的集合。当 $V = K^{n+1}$ 时，$\mathbf{P}(V)$ 被记作 $\mathbf{P}^n(K)$。对任意的齐次坐标 $[k_0 : k_1 : \cdots : k_n]$，它对应着 K^{n+1} 中过 $(k_0, k_1, \cdots, k_n)$ 的直线。

对任意 $g \in \mathbf{GL}(V)$，$g : V \to V$ 将过原点的线映射为过原点的线。据此，我们定义

$$\mathbf{GL}(V) \times \mathbf{P}(V) \longrightarrow \mathbf{P}(V), \quad (g, \ell) \mapsto g \cdot \ell = g(\ell).$$

这是 $\mathbf{GL}(V)$ 在 $\mathbf{P}(V)$ 上的作用。

根据例子3.3，我们考虑

$$\tau : \mathbf{GL}(V) \longrightarrow \mathfrak{S}_{\mathbf{P}(V)}.$$

此时，$\mathrm{Ker}(\tau) = \big\{ g \in \mathbf{GL}(V) \big| g(\ell) = \ell,\ \ell \in \mathbf{P}(V) \big\}$。对任意 V 的基 $\{e_i\}_{i=1,\cdots,n+1}$，$g \in \mathrm{Ker}(\tau)$ 意味着对每个 i，都有 $g(e_i) = \lambda_i \cdot e_i$，其中，$\lambda_i \in K^\times$。现在说明这些 λ_i 均相等：考虑 $e_1 + e_2$ 在 V 中对应的直线，根据 g 的定义，

$$g(e_1 + e_2) = \lambda_1 e_1 + \lambda_2 e_2 = \lambda_1 \left(e_1 + \frac{\lambda_2}{\lambda_1} e_2 \right)$$

与 $e_1 + e_2$ 是共线的，从而，$\lambda_1 = \lambda_2$。

通过以上讨论，我们得到 $\mathrm{Ker}(\tau) = K^\times \cdot \mathbf{I}$，其中，$\mathbf{I}$ 是单位映射。据此，我们有

$$1 \to K^\times \overset{k \mapsto k \cdot \mathbf{I}}{\longrightarrow} \mathbf{GL}(V) \xrightarrow{\tau} \mathfrak{S}_{\mathbf{P}(V)}.$$

于是，我们定义

$$\mathbf{PGL}(V) := {\mathbf{GL}(V)}\big/{K^\times \cdot \mathbf{I}} = {\mathbf{GL}(V)}\big/{K^\times}.$$

那么，$\mathbf{PGL}(V)$ 可以忠实地作用在 $\mathbf{P}(V)$ 上。当 $V = K^{n+1}$ 时，我们记

$$\mathbf{PGL}(n+1; K) := {\mathbf{GL}(n+1; K)}\big/{K^\times \cdot \mathbf{I}_{n+1}},$$

其中，$\mathbf{I}_{n+1}$ 是 $(n+1) \times (n+1)$ 的单位矩阵。

我们还考虑 $\mathbf{GL}(n+1; K)$ 的子群 $\mathbf{SL}(n+1; K)$，此时显然有 $\mathbf{SL}(n+1; K)$ 在 K^{n+1} 上的作用：

$$\mathbf{SL}(n+1; K) \times \mathbf{P}^n(K) \longrightarrow \mathbf{P}^n(K), \quad (g, \ell) \mapsto g \cdot \ell = g(\ell).$$

此时，我们有

$$\mathrm{Ker}\big(\mathbf{SL}(n+1; K) \longrightarrow \mathfrak{S}_{\mathbf{P}^n(K)}\big) = \mathbf{SL}(n+1; K) \cap K^\times \cdot \mathbf{I}_{n+1} = \mu_{n+1}(K),$$

其中，$\mu_{n+1}(K)$ 为 K 中的 n-次单位根的子群（因为要求 $\det(\xi \cdot \mathbf{I}_{n+1}) = 1$）。据此，我们定义

$$\mathbf{PSL}(n+1; K) := {\mathbf{SL}(n; K)}\big/{\mu_{n+1}(K) \cdot \mathbf{I}_{n+1}},$$

此时，$\mathbf{PSL}(n+1; K)$ 可以忠实地作用在 $\mathbf{P}^n(K)$ 上。

例子 3.8 (1 维仿射变换)**.** K 是域，定义如下 K 到自身的映射的集合：

$$\mathbf{Aff}_1(K) = \big\{ f_{a,b} : x \mapsto ax + b \big| a \in K^\times,\, b \in K \big\}.$$

集合 $\mathbf{Aff}_1(K)$ 配上映射的复合作为乘法构成群，它被称为是K **上的 1 维的仿射变换群**。$\mathbf{Aff}_1(K)$ 在 K 有自然的作用。这个作用显然是传递的。对于 $x_0 \in K$，我们有

$$\mathrm{Stab}(x_0) = \big\{ x \mapsto a(x - x_0) + x_0 \big| a \in K^\times \big\}.$$

从而，$\mathrm{Stab}(x_0) \simeq K^\times$。实际上，我们有

$$K^\times \xrightarrow{\simeq} \mathrm{Stab}(x_0) < \mathbf{Aff}_1(K), \quad a \mapsto f_{a,(1-a)x_0}.$$

例子 3.9 (一个具体的例子)**.** 考虑有限域 $\mathbb{F}_5 = (\mathbb{Z}/5\mathbb{Z}, +, \cdot)$，$\mathbf{P}^1(\mathbb{F}_5)$ 有 6 个元素：

$$\mathbf{P}^1(\mathbb{F}_5) = \{\ell_1, \ell_2, \ell_3, \ell_4, \ell_5, \ell_6\},$$

其中，对 $k = 1, \cdots, 5$，$\ell_k = [1 : k]$，$\ell_6 = [0 : 1]$。那么，$\mathbf{GL}(2; \mathbb{F}_5)$ 在 $\mathbf{P}^1(\mathbb{F}_5)$ 的作用给出：

$$\begin{array}{ccc} \mathbf{GL}(2;\mathbb{F}_5) & \xrightarrow{\tau} & \mathfrak{S}_{\mathbf{P}^1(\mathbb{F}_5)} \\ \big\downarrow{\scriptstyle \pi} & \nearrow_{\overline{\tau}} & \\ \mathbf{PGL}(2;\mathbb{F}_5) & & \end{array}$$

另外，对 $\mathbf{P}^1(\mathbb{F}_5)$ 中元素的标号将 $\mathfrak{S}_{\mathbf{P}^1(\mathbb{F}_5)}$ 等同于 $\mathfrak{S}_6$，上述构造给出一个单的同态：

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

根据

$$|\mathbf{PGL}(2;\mathbb{F}_5)| = \frac{1}{4}|\mathbf{GL}(2;\mathbb{F}_5)| = \frac{1}{4}(5^2 - 1)(5^2 - 5) = 120,$$

我们得到了 $\mathfrak{S}_6$ 的一个 120 阶的子群 $H = \mathrm{Im}(\varphi) < \mathfrak{S}_6$。

由于 $\mathbf{GL}(2;\mathbb{F}_5)$ 传递地作用在 $\mathbf{P}^1(\mathbb{F}_5)$ 上，作为 $\mathfrak{S}_6$ 的子群，H 在 6 个元素 $\{\ell_1, \ell_2, \ell_3, \ell_4, \ell_5, \ell_6\}$ 上的作用也是传递的。

作为总结，$\mathfrak{S}_6$ 有 120 阶的子群 H，它在 $\{\ell_1, \cdots, \ell_6\}$ 上的自然作用是传递的。另外，$\mathfrak{S}_6$ 的的子群 $\mathrm{Stab}(\ell_k)$（都与 $\mathfrak{S}_5$ 同构）在 $\{\ell_1, \cdots, \ell_6\}$ 上的自然作用不传递。

3.2.2 群作用在由自身所构造的对象上的例子

例子 3.10 (作用在左陪集空间上)**.** G 是群，$H < G$ 是子群，$X = G/H$，G 通过左乘法作用在 X 上：

$$G \times G/H \longrightarrow G/H, \quad (g, g'H) \mapsto (g \cdot g')H.$$

注意到，以上映射是良好定义的。因为 $((g_1 \cdot g_2) \cdot g')H = (g_1 \cdot (g_2 \cdot g'))H$，上述映射给出了群的作用。另外，这个作用显然是传递的。

给定子群 $H' < G$，我们自然有群作用 $H' \curvearrowright \left(G/H\right)$：

$$H' \times G/H \longrightarrow G/H, \quad (h', g'H) \mapsto (h' \cdot g')H.$$

我们注意到 H' 的作用**未必**传递的。

对任意 $g' \in G$，我们计算 $g'H \in {}^{G}\!/_{H}$ 的稳定化子：

$$g \cdot g'H = g'H \;\Rightarrow\; g'^{-1}gg'H = H \;\Rightarrow g \in g'Hg'^{-1}.$$

所以，对群作用 ${}^{H'}\!\curvearrowright \left({}^{G}\!/_{H}\right)$ 而言，

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

这个计算将 ${}^{H'}\!\curvearrowright \left({}^{G}\!/_{H}\right)$ 的稳定化子与子群 H 的共轭关联在一起。

注记 3.6. 若 G 传递地作用在 X 上，则对任意 $x \in X$，映射

$$\varphi_x : {}^{G}\!/_{\mathrm{Stab}(x)} \longrightarrow X, \quad g \cdot \mathrm{Stab}(x) \mapsto g \cdot x,$$

是双射，其中 ${}^{G}\!/_{\mathrm{Stab}(x)}$ 是左陪集的集合。

φ_x 显然是满射，现在证明单射性：若 $\varphi_x(g\cdot\mathrm{Stab}(x)) = \varphi_x(g'\cdot\mathrm{Stab}(x))$，则 $g\cdot x = g'\cdot x$，即 $g'^{-1}g \in \mathrm{Stab}(x)$，从而，$g \in g' \cdot \mathrm{Stab}(x)$，所以，$g \cdot \mathrm{Stab}(x) = g' \cdot \mathrm{Stab}(x))$。

现在研究另一点 $x' \in X$ 的稳定化子。根据传递性，存在 $g \in G$ 使得 $x' = g \cdot x$。此时，

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

从而，$g^{-1}\mathrm{Stab}(x')g \subset \mathrm{Stab}(x)$。据此，我们得到如下公式：

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

简而言之，基准点 x 的改变对应于其稳定化子的共轭。

上述计算表明，用 G 通过左乘法作用在 ${}^{G}\!/_{\mathrm{Stab}(x)}$ 与 ${}^{G}\!\curvearrowright X$ 是同构的，请参考定义。实际上，这两个群作用之间的同构由如下映射给出：

$$\begin{cases} \varphi : G \to G, \quad g \mapsto g, \\ \psi : {}^{G}\!/_{\mathrm{Stab}(x)} \to X, \quad g\mathrm{Stab}(x) \mapsto g \cdot x. \end{cases}$$

另外，用 G 通过左乘法作用在 ${}^{G}\!/_{\mathrm{Stab}(x)}$ 与 ${}^{G}\!/_{\mathrm{Stab}(x')}$ 是同构的，其中 $x' = gx$。实际上，这两个群作用之间的同构由如下映射给出：

$$\begin{cases} \varphi : G \to G, \quad g \mapsto g, \\ \psi : {}^{G}\!/_{\mathrm{Stab}(x)} \to {}^{G}\!/_{\mathrm{Stab}(x')}, \quad h\mathrm{Stab}(x) \mapsto g^{-1}h \cdot \mathrm{Stab}(x). \end{cases}$$

反之，给定 G 的子群 H，G 通过左乘法作用在 ${}^{G}\!/_{H}$ 上，这是传递的并且 $H = \mathrm{Stab}(H)$。

作为总结：**给定 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 的子群**。

练习 3.1. G 是有限群并且传递地作用在集合 X 上。证明，X 是有限集并且 $|X|$ 整除 $|G|$。

作为上述讨论的应用，我们证明所谓的轨道计数公式：

注记 3.7 (轨道计数公式)**.** 群 G 作用在集合 X 上，对任意 $x \in X$，以下映射为双射：

$$ {}^{G}\!/_{\mathrm{Stab}(x)} \xrightarrow{\simeq} \mathrm{orb}(x), \quad g\mathrm{Stab}(x) \mapsto g \cdot x.$$

从而，

$$\left|{}^{G}\!/_{\mathrm{Stab}(x)}\right| = \left|\mathrm{orb}(x)\right|.$$

假设 G 是有限群并且在有限集 X 上作用，根据作用的轨道分解：

$$X = \coprod_{k=1}^{m} \mathrm{orb}(x_k),$$

其中，m 为作用的轨道数目，就得到如下公式

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

例子 3.11. G 是群，$H \lhd G$ 是正规子群。G 通过共轭可以作用在 H 上：

$$G \times H \longrightarrow H, \quad g \mapsto (x \mapsto gxg^{-1})$$

即

$$G \to \mathfrak{S}_H, \quad g \mapsto \mathrm{Int}(g).$$

当 $H = G$ 时，以上共轭作用的轨道为恰为 G 的共轭类。给定 $x \in G$，其稳定化子由是与 x 交换的元素构成，即其中心化子 $\mathrm{C}_x(G)$)。根据轨道计数公式，我们得到共轭类的公式：

$$\boxed{\sum_i \frac{1}{|\mathrm{C}_{x_i}(G)|} = 1},$$

其中，以上对 G 的共轭类求和而 x_i 为相应共轭类的代表元。

p 是素数。若群 G 的阶是 p 的幂，就称 G 为**p-群**。作为以上共轭作用的应用，我们证明

命题 19. *p-群的中心非平凡。*

证明: G 为 p-群，为了证明 $\mathrm{Z}(G) \neq 1$，只要考虑 G 通过共轭在 G 上的作用并说明除了 $1 \in G$ 的轨道，还有轨道的恰好有一个元素即可（这个元素显然在 $\mathrm{Z}(G)$ 里）。根据共轭类公式：

$$p^f = |G| = \sum_{k=1}^{m} |\mathrm{Conj}(x_i)| = 1 + \sum_{k=2}^{m} |\mathrm{Conj}(x_i)|,$$

其中，m 为共轭类的个数。在共轭作用下，$\{1 \in G\}$ 是一个单独的轨道，上式右边的 1 代表该轨道的元素个数。然而，上式左边整除 p 但是右边每个 $|\mathrm{Conj}(x_i)|$ 都整除 p^f，从而右边其余轨道不可能均为 p 的倍数。据此，还有其它轨道其元素个数也是 1。 □

例子 3.12 ($\mathfrak{S}_6$ 的非平凡外自同构)**.** 请参考例3.9。令 $H < \mathfrak{S}_6$ 是有 120 个元素的子群并且 ${}^{H}\!\curvearrowright\{1,2,3,4,5,6\}$ 是传递的，$X = {}^{\mathfrak{S}_6}\!/_{H}$，则 $|X| = 6$。我们记

$$X = \{g_0H, g_1H, \cdots, g_5H\},\ Y = \{g_1H, g_2H, g_3H, g_4H, g_5H\},$$

其中 $g_0 \in H$。考虑 $\mathfrak{S}_6$ 通过左乘法在 X 上的作用，这定义了群同态

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

我们证明，通过 X 中的元素的标号将 $\mathfrak{S}_X$ 与 $\mathfrak{S}_6$ 等同，则上述 $f : \mathfrak{S}_6 \to \mathfrak{S}_6$ 是同构但不是内自同构。

以上群作用给出了 H 在 X 上的作用 ${}^{H}\!\curvearrowright X$。由于 $H < \mathrm{Stab}(g_0H)$，${}^{H}\!\curvearrowright X$ 给出了 H 在 Y 上的作用。特别地，我们有群同态

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

我们说明 $\mathrm{Ker}(\varphi) = N = 1$。实际上，若 $h \in N < H$，则对任意 g_i，$g_i^{-1}hg_i \in H$，从而对任意 $g \in \mathfrak{S}_6$，$g^{-1}hg \in H$，所以 $\mathfrak{S}_6$ 正规子群 $N' = \langle gNg^{-1} | g \in \mathfrak{S}_6 \rangle < H$。但是 $\mathfrak{S}_6$ 唯一非平凡的正规子群[11]为 $\mathfrak{A}_6$，其指标为 2，而 H 的指标为 6，从而 $[\mathfrak{S}_6 : N'] \geqslant 6$，所以，$N' = 1$。这表明 $N = 1$，即 φ 是单射。另外，$|H| = |\mathfrak{S}_Y|$，所以 φ 是群同构。

以上的讨论可交换图表示：

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

f 必为同构：否则，$\mathrm{Ker}(f) \simeq \mathfrak{A}_6$，从而，$\mathrm{Im}(f)$ 只有两个元素，然而仅 H 的像就至少 120 个元素，矛盾。

现在将 $\mathfrak{S}_X$ 等同为 $\mathfrak{S}_6$，则 $f \in \mathrm{Aut}(\mathfrak{S}_6)$。我们注意到 $f^{-1}(\mathfrak{S}_Y) = H$，并且 $\mathfrak{S}_Y$ 恰为 $\mathfrak{S}_5$ 到 $\mathfrak{S}_6$ 的标准嵌入之一（因为 $\mathfrak{S}_Y = \mathrm{Stab}(g_0 H)$）。如果 f 是内自同构，则 f^{-1} 也是，从而 $f^{-1}(\mathfrak{S}_Y) = H$ 是固定某元素所给的 $\mathfrak{S}_5 \hookrightarrow \mathfrak{S}_6$，这与 H 的作用是传递的相矛盾。

3.3 群作用的应用举例

3.3.1 双传递性与单群的 Iwasawa 判定

假设 G 是群，X 是集合，$|X| \geqslant 2$ 并且 G 作用在 X 上。那么，G 自然地作用在 $X \times X$ 上：

$$G \times (X \times X) \to X \times X, \quad \big(g, (x, y)\big) \mapsto (g \cdot x, g \cdot y).$$

令 Δ 为 $X \times X$ 的对角线，即由形如 $\Delta = \{(x, x) | x \in X\}$。若 G 在 $X \times X - \Delta$ 上的作用是传递的，则称 G 在 X 上的作用是**双传递的**。换而言之，双传递的群作用满足如下要求：对任意 $x_1, x_2 \in X, y_1, y_2 \in X$，$x_1 \neq y_1$，$x_2 \neq y_2$，存在 $g \in G$，使得 $gx_1 = x_2$，$gy_1 = y_2$。特别地，我们知道 $\overset{G}{\curvearrowright} X$ 是传递的。另外，双传递的定义等价于说 $\overset{G}{\curvearrowright} (X \times X)$ 恰好有两个轨道 Δ 和 $X \times X - \Delta$。

练习 3.2. 给定传递的群作用 $\overset{G}{\curvearrowright} X$，其中，$|X| \geqslant 2$。证明，该作用是双传递的等价于存在 $x \in X$，使得 $\mathrm{Stab}(x)$ 在 $X - \{x\}$ 上的作用是传递的。

定理 20 (Iwasawa 判据)**.** *群 G 作用在集合 X 上，$|X| \geqslant 2$ 并且该作用是双传递的。假设存在 $x \in G$ 以及 $A < \mathrm{Stab}(x)$ 使得*

1) A 是 $\mathrm{Stab}(x)$ 的交换的正规子群；

2) $\{gAg^{-1} | g \in G\}$ 生成 G。

那么，对任意正规子群 $N \lhd G$，$\mathbf{D}(G) < N$ 或 $N < \mathrm{Ker}(G \to \mathfrak{S}_X)$ 二者必居其一。

注记 3.8. 定理中的 $\mathbf{D}(G)$ 是 G 的**换位子群**或**导出子群**是群，它是由 G 中所有形如 $ghg^{-1}h^{-1}$ 的元素生成的子群。我们显然有 $\mathbf{D}(G) \lhd G$。

我们可以计算对称群 $\mathfrak{S}_n$ 和交错群 $\mathfrak{A}_n$ 的换位子群。以下，我们忽略 $n = 1, 2$ 这个两个平凡的情形。

例子 3.13 ($\mathbf{D}(\mathfrak{S}_n) = \mathfrak{A}_n, n \geqslant 3$)**.** 我们显然有 $\mathbf{D}(\mathfrak{S}_n) \lhd \mathfrak{A}_n$ ($\mathbf{D}(\mathfrak{S}_n)$ 中的元是偶置换)。现在证明 $\mathbf{D}(\mathfrak{S}_n) = \mathfrak{A}_n$。注意到，对于 $i, j, k \leqslant n$，有

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

从而，$\mathbf{D}(\mathfrak{S}_n)$ 包含所有的 3-循环。

[11] 参考作业3.6.2的 B4)

例子 3.14 ($\mathbf{D}(\mathfrak{A}_n) = \mathfrak{A}_n, n \geqslant 5$)**.** 当 $n \geqslant 5$ 时，$\mathbf{D}(\mathfrak{A}_n)$ 中的 3-循环是相互共轭的。（参见习题 XXX）特别地，$\sigma = (i,j,k)$ 与 $\sigma^2 = (i,k,j)$ 共轭（实际上，由于 $n \geqslant 5$，不妨假 $i,j,k \neq 1,2$，此时，用 $(1,2)(j,k)$ 对 σ 共轭即可），即有 $g \in \mathfrak{A}_n$，使得 $g\sigma g^{-1} = \sigma^2$。从而，

$$\sigma = g\sigma g^{-1}\sigma^{-1} \in \mathbf{D}(\mathfrak{A}_n).$$

从而，$\mathbf{D}(\mathfrak{A}_n)$ 包含所有的 3-循环。

Iwasawa 判据的证明. 假设 $N \not\subset \mathrm{Ker}(G \to \mathfrak{S}_X)$，其中，$N \lhd G$。我们的目标是说明 $N \supset \mathbf{D}(G)$。

- 第一步，证明 N 在 X 上作用是传递的。对任意 $x \in X$，它在 N 的作用下的轨道为 $Nx = \{nx | n \in N\}$。那么，
  - 选取 $x \in X$，使得 $N \cdot x \neq \{x\}$。
    由于 $N \not\subset \mathrm{Ker}(G \to \mathfrak{S}_X)$，所以有 $n \in N$ 以及 $x \in X$ 使得 $nx \neq x$。
  - $N \cdot x$ 在 $\mathrm{Stab}(x)$ 的作用下不变，即对任意的 $g \in \mathrm{Stab}(x)$，$gNx \subset Nx$。
    实际上，对任意的 $nx \in Nx$，其中，$n \in N$，我们有
    $$gnx = gng^{-1}gx = gng^{-1}x \in Nx,$$
    以上我们用到了 $N \lhd G$ 以及 $g \in \mathrm{Stab}(x)$。
  - $\mathrm{Stab}(x)N \cdot x \supset X - \{x\}$。
    由于 G 的左右是双传递的，所以，$\mathrm{Stab}(x)(Nx - \{x\}) \supset X - \{x\}$。

  综上所述，$N \cdot x \supset X - \{x\}$，所以，$N$ 在 X 上作用是传递的。
- 第二步，证明 $\{nAn^{-1} | n \in N\}$ 生成 G。
  - $G = N \cdot \mathrm{Stab}(x) = \mathrm{Stab}(x) \cdot N$（因为 N 是正规的）。
    对任意 $g \in G$，由于 N 的作用是传递的，存在 $n \in N$，使得 $nx = gx$，即 $g^{-1}nx = x$。所以，$g^{-1}n = h \in \mathrm{Stab}(x)$。从而，$g = nh^{-1} \in N\mathrm{Stab}(x)$。
  - $\{gAg^{-1} | g \in G\} = \{nAn^{-1} | n \in N\}$。
    实际上，我们把 g 写成 $g = nh$。由于 $A \lhd \mathrm{Stab}(x)$，从而，
    $$gAg^{-1} = n \cdot hAh^{-1} \cdot n^{-1} = nAn^{-1}.$$

综合以上讨论，我们有 $G = \langle \{nAn^{-1} | n \in N\} \rangle = AN$（因为 $nan^{-1} = a(a^{-1}na)n^{-1} \in AN$）。特别地，群同态

$$A \hookrightarrow G \longrightarrow {}^{G}\!/_{N}$$

是满射。由于 A 是交换群，所以，${}^{G}\!/_{N}$ 是交换群。特别地，任意 $ghg^{-1}h^{-1} \in G$ 都落在 $N = \mathrm{Ker}(G \to {}^{G}\!/_{N})$，即 $\mathbf{D}(G) \subset N$。 □

如果群 G 除了 1 和 G 外没有其它正规子群，就称 G 是**单群**。应用 Iwasawa 判据，我们可以证明：

例子 3.15 ($\mathfrak{A}_5$ 是单群)**.** 在上述定理中，我们选取 $G=\mathfrak{A}_5$，$X=\{1,2,3,4,5\}$，那么，$\mathrm{Ker}(G\to\mathfrak{S}_X)=1$ 并且 $^{G\curvearrowright}X$ 是双传递的。

选取 $x=5$，此时，$\mathrm{Stab}(x)=\mathfrak{A}_4$ 并选取

$$A=\{1,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}\simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}\times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}.$$

这是 $\mathfrak{A}_4$ 中的交换的正规子群。我们现在说明 $\{gAg^{-1}|g\in\mathfrak{A}_5\}$ 生成 $\mathfrak{A}_5$：通过考虑 $(1,2,5)(1,2)(3,4)(1,2,5)^{-1}=(2,5)(3,4)$，$\{gAg^{-1}\}$ 包含了所有的 $(i,j)(k,l)$ 型元素，其中，i,j,k,l 两两不同。另外，通过考虑 $(1,2)(3,4)\cdot(1,5)(3,4)=(1,5,2)$，我们知道所有的 3-循环都可以生成，从而可以生成 $\mathfrak{A}_5$。

假设 $N\lhd\mathfrak{A}_5$，Iwasawa 判据表明 $N\subset\mathrm{Ker}(G\to {}^{G}\!/_{N})=1$ 或者 $N\supset\mathbf{D}(\mathfrak{A}_5)=\mathfrak{A}_5$，从而，$\mathfrak{A}_5$ 为单群。

例子 3.16 (剪切映射与 $\mathbf{SL}(n;K)$ 的导出子群)**.** K 是域，V 是 n-维 K-线性空间，$t\in\mathbf{SL}(V)$，如果 $\dim\mathrm{Ker}(t-1)=n-1$，就称 t 是**剪切映射**。根据定义，$\mathrm{rank}(t-1)=1$

选取 V 的基 $\{e_1,\cdots,e_{n-1},e_n\}$，使得 $e_1,\cdots,e_n\in\mathrm{Ker}(g-1)$，由于 $\det(t)=1$，所以

$$t(e_n)=e_n+x_1e_1+\cdots+x_{n-1}e_{n-1}$$

据此，g 可以用如下矩阵表示

$$t=\begin{pmatrix}1&&&x_1\\&\ddots&&\\&&1&x_{n-1}\\&&&1\end{pmatrix}=\begin{pmatrix}\mathbf{I}_{n-1}&x\\0&1\end{pmatrix},$$

其中，$x=x_1e_1+\cdots+x_{n-1}e_{n-1}$。通过调换 $1,\cdots,n-1$，不妨假设 $x_{n-1}\neq0$。令 $e_i'=\begin{cases}e_i,\ i\neq n-1;\\ x,\ i=n-1.\end{cases}$。

在 $\{e_i'\}$ 下，t 的矩阵表示为

$$t_n:=\begin{pmatrix}1&&&0\\&\ddots&&0\\&&1&1\\&&&1\end{pmatrix}.$$

特别地，以上讨论表明在 $\mathbf{GL}(n;K)$ 中，所有剪切映射均与 t_n 共轭。

当 $n>2$ 时，为了在 $\mathbf{SL}(n;K)$ 中讨论剪切映射 t 的共轭，我们用 $g\in\mathbf{GL}(n;K)$ 进行共轭，从而，$gtg^{-1}=t_n$。由于 $n>2$，令

$$h=\begin{pmatrix}\det(g)^{-1}&&&\\&1&&\\&&\ddots&\\&&&1\end{pmatrix}.$$

那么，$(hg)t(hg)^{-1}=t_n$ 并且 $hg\in\mathbf{SL}(n;K)$。

在 $\mathbf{SL}(n;K)$ 中，我们有一大类剪切映射的例子：$t_{i,j}(\lambda)=1+\lambda E_{i,j}$ 是剪切映射，其中，$\lambda\in K^\times$，$E_{i,j}$ 是在第 i 行第 j 列为 1 而其余位置均为 0 的矩阵。另外，在 $\mathbf{SL}(2;K)$ 中，我们有

$$\begin{pmatrix}1&a\\0&1\end{pmatrix}\begin{pmatrix}1&0\\b&1\end{pmatrix}\begin{pmatrix}1&c\\0&1\end{pmatrix}=\begin{pmatrix}1+ab&abc+a+c\\b&1+cb\end{pmatrix}.$$

令 $a=c=-b^{-1}$，则 $\begin{pmatrix}1 & -b^{-1}\\ b & 1\end{pmatrix}$ 可以被剪切映射生成；进而 $\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}1 & -b^{-1}\\ b & 1\end{pmatrix}=\begin{pmatrix}b & 0\\ 0 & b^{-1}\end{pmatrix}$ 也可以被生成。据此，我们知道 $\mathbf{SL}(V)$ 可以被剪切映射的集合生成，这是因为以上 $\{t_{i,j}(\lambda)\}\subset\mathbf{SL}(n;K)$ 以及所构造出的矩阵都对应着初等变换而每个 $g\in\mathbf{SL}(n;K)$ 都可以通过初等变换变成单位矩阵。

作为总结以上讨论的总结，我们有如下结论：

- 对任意的 $n\geqslant 2$，$\mathbf{SL}(n;K)$ 可以被剪切映射生成；
- 对任意的 $n\geqslant 3$，$\mathbf{SL}(n;K)$ 中的剪切映射是相互共轭的。

引理 21. *当 $n\geqslant 3$ 或 $n=2,|K|\geqslant 4$ 时，有*

$$\mathbf{D}\big(\mathbf{GL}(n;K)\big)=\mathbf{SL}(n;K),\quad \mathbf{D}\big(\mathbf{SL}(n;K)\big)=\mathbf{SL}(n;K).$$

证明： 只要证明 $\mathbf{SL}(n;K)\subset\mathbf{D}\big(\mathbf{SL}(n;K)\big)$ 即可。我们证明一个充分条件：存在某个剪切 $t\in\mathbf{SL}(n;K)$，它形如 $t=xyx^{-1}y^{-1}$，其中，$x,y\in\mathbf{SL}(n;K)$。在此条件下，根据以上讨论，对任意的剪切 t'，存在 $g\in\mathbf{GL}(n;K)$，使得

$$t'=gtg^{-1}=gxg^{-1}\cdot gyg^{-1}\cdot\left(gxg^{-1}\right)^{-1}\cdot\left(gyg^{-1}\right)^{-1}.$$

其中，$gxg^{-1},gyg^{-1}\in\mathbf{SL}(n;K)$。这表明 $\mathbf{D}\big(\mathbf{SL}(n;K)\big)$ 包含所有剪切映射，从而，$\mathbf{SL}(n;K)\subset\mathbf{D}\big(\mathbf{SL}(n;K)\big)$。

当 $n=2$ 时，我们计算

$$\begin{pmatrix}a & 0\\ 0 & a^{-1}\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & 0\\ 0 & a^{-1}\end{pmatrix}^{-1}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^{-1}=\begin{pmatrix}1 & a^2-1\\ 0 & 1\end{pmatrix}.$$

当 $|K|\geqslant 4$ 时，存在 $a\in K^\times$，使得 $a^2-1\neq 0$，上式就给出一个剪切映射。

当 $n\geqslant 3$ 时，我们计算

$$\begin{pmatrix}g & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}\mathbf{I}_{n-1} & v\\ 0 & 1\end{pmatrix}\begin{pmatrix}g & 0\\ 0 & 1\end{pmatrix}^{-1}\begin{pmatrix}\mathbf{I}_{n-1} & v\\ 0 & 1\end{pmatrix}^{-1}=\begin{pmatrix}1 & g(v)-v\\ 0 & 1\end{pmatrix}.$$

其中，$g\in\mathbf{SL}(n-1;K),v\in K^{n-1}$。由于 $n-1\geqslant 2$，只要选取剪切映射 $g\in\mathbf{SL}(n-1;K)$ 以及 $g(v)-v\neq 0$ 即可。 □

命题 22. *当 $n\geqslant 3$ 或 $n=2,|K|\geqslant 4$ 时，$\mathbf{PSL}(n;K)$ 是单群。*

证明： 当 $n\geqslant 2$ 时，$G=\mathbf{SL}(n;K)$ 在 $X=\mathbb{P}^{n-1}(K)$ 上的作用是双传递的：对任意的 $v_1,w_1,v_2,w_2\in K^n$，其中，v_i 与 w_i 不共线，显然有矩阵 $g\in G$ 使得 $g(v_1)=v_2$，$g(w_1)=w_2$。

令 $x=[0:0:\cdots:1]\in\mathbb{P}^{n-1}(K)$，则 $\mathrm{Stab}(x)$ 中的矩阵形如

$$P_{g,v}=\begin{pmatrix}g & v\\ 0 & \det(g)^{-1}\end{pmatrix},\ g\in\mathbf{GL}(n;K),v\in K^{n-1}.$$

那么，

$$A=\left\{P_{1,v}=\begin{pmatrix}1 & v\\ 0 & 1\end{pmatrix},\ v\in K^{n-1}\right\}\simeq K^{n-1}$$

是 $\mathrm{Stab}(x)$ 的交换的正规子群。

当 $n\geqslant 3$ 时，我们已经证明了 $P_{1,v}=t_n$ 的共轭可以给出所有剪切映射，其中，$v=(0,\cdots,1)$。由于剪切映射生成了 $\mathbf{SL}(n;K)$，从而，$\{gAg^{-1}|g\in G\}$ 生成 G。

当 $n=2$ 时，利用 $\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\in A$，我们计算共轭

$$\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}^{-1}=\begin{pmatrix}1 & 0\\ -a & 1\end{pmatrix}.$$

我们已经证明了形如 $\begin{pmatrix}1 & *\\ 0 & 1\end{pmatrix}$ 和 $\begin{pmatrix}1 & 0\\ * & 1\end{pmatrix}$ 的矩阵生成 $\mathbf{SL}(2;K)$。

另外，我们有

$$\mathrm{Ker}\big(\mathbf{SL}(n;K)\to\mathfrak{S}_{\mathbb{P}^{n-1}(K)}\big)=\mu_n(K)$$

以及 $\mathbf{D}(\mathbf{SL}(n;K))=\mathbf{SL}(n;K)$。

根据 Iwasawa 判据，若 $N\lhd\mathbf{SL}(n;K)$ 并且 $N\neq\mathbf{SL}(n;K)$，那么，$\mathbf{SL}(n;K)\subset\mu_n(K)$。从而，根据

$$\mathbf{SL}(n;K)\big/\mu_n(K)\xrightarrow{\simeq}\mathbf{PSL}(n;K),$$

我们知道 $\mathbf{PSL}(n;K)$ 的正规子群必为 1 或 $\mathbf{PSL}(n;K)$。 □

3.3.2 Burnside 引理

我们证明如下关于轨道个数的计算公式：

命题 23 (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*

$$\big|G\backslash X\big|=\frac{1}{|G|}\sum_{g\in G}|X^g|. \tag{3.1}$$

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：

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

我们有两种方式来数 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 $S=\coprod_{x\in X}\mathrm{Stab}(x)$，我们有

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

所以，

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

另外，我们有

$$\sum_{x\in X}\frac{1}{|\mathrm{orb}(x)|}=\sum_{\mathrm{orb}(x_i)\in G\backslash X}\Big(\sum_{x\in\mathrm{orb}(x_i)}\frac{1}{|\mathrm{orb}(x)|}\Big)=\sum_{\mathrm{orb}(x_i)\in G\backslash X}1=\big|G\backslash X\big|.$$

这就给出了证明。 □

例子 3.17. 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

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

所以，一共有 11 个四顶点的简单图。

例子 3.18. 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 $g=\overline{k}$，其中，$k\in\{0,1,\cdots,n-1\}$，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

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

特别地，如果 $n=4$，$m=3$，那么，

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

3.3.3 Sylow 定理

定义 3.3. G 是有限群，p 是素数，$|G|=n=p^km$，其中，$k\geqslant 1$，$(p,m)=1$。如果 $S<G$ 是子群并且 $|S|=p^k$，就称 S 是 G 的 Sylow p-子群或是 **p-Sylow 子群**。

$S<G$ 是子群，则 S 为 Sylow p-子群当且仅当 S 为 p-群且 $[G:S]$ 与 p 互素。

注记 3.9 (群作用的一个例子)**.** Sylow p-子群 S 的共轭，即形如 gSg^{-1} 的群，仍是 Sylow p-子群。特别地，G 可以（通过共轭）作用在 Sylow p-子群的集合上。

我们给出了两个具体的 Sylow p-子群的例子:

例子 3.19. 令 $G=\mathbb{Z}/n\mathbb{Z}$，其中 $n=p^km$，$p\nmid m$。我们有自然同构[12]

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

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。

从上式左边来看，该 Sylow p-子群中的元素恰为 $\mathbb{Z}/n\mathbb{Z}$ 中 mod m 得 1 的元素，这因为上述同构由如下映射给出：

$$\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/p^k\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z},\ \ \overline{a}\mapsto\big(a\ (\mathrm{mod}\ p^k),a\ (\mathrm{mod}\ m)\big).$$

例子 3.20. 请参考例2.9。K 是域且 $|K|=q$，其中 $q=p^m$，p 是素数。此时，

$$|\mathbf{GL}(n;K)|=\prod_{k=0}^{n-1}(q^n-q^k)=q^{\frac{n(n-1)}{2}}l,\ \ |\mathfrak{T}_1|=q^{\frac{n(n-1)}{2}},$$

其中，$\mathfrak{T}_1$ 为对角线上全为 1 的上三角矩阵所构成的子群。由于 $l=\prod_{i=1}^{n}(q^i-1)$，从而，$(p,l)=1$。所以，$\mathfrak{T}_1$ 是 $\mathbf{GL}(n;K)$ 的 Sylow p-子群。

例子 3.21. p 是素数，考察 $\mathfrak{S}_p$ 的 Sylow p-子群。由于 $|\mathfrak{S}_p|=p(p-1)!$ 并且 $\big(p,(p-1)!\big)=1$，由 p-循环 $(x_1,x_2,\cdots,x_p)$ 生成的循环群给出了 $\mathfrak{S}_p$ 中所有的 Sylow p-子群。容易看出，一共有 $(p-1)!\div(p-1)=(p-2)!$ 个这样的 Sylow p-子群。

另外，根据下面即将证明的 Sylow 定理，Sylow p-子群的个数模 p 余 1，即 $(p-2)!\equiv1(\mathrm{mod}\ p)$，这是初等数论中的 Wilson 定理。

注记 3.10. 根据 Cayley 定理[13]，每个有限群均可视为某个对称群 $\mathfrak{S}_n$ 的子群。实际上，还可以把有限群实现为一般线性群 $\mathbf{GL}(n;K)$ 的子群，其中，K 为任意给定的域。

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 $(e_i)_{1\leqslant i\leqslant n}$ 为 K^n 的标准的基，对任意的 $\sigma\in\mathfrak{S}_n$，我们把 σ 映射成到线性变换 $e_i\mapsto e_{\sigma(i)}$，其中，$i=1,\cdots,n$。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。

以上构造可以用群代数的语言表达：群代数 $K[G]$ 是 K 线性空间，它具有基 $\{e_g\}_{g\in G}$ 并且满足乘法 $e_g\cdot e_{g'}=e_{gg'}$。我们定义

$$G\longrightarrow\mathbf{GL}(K[G]),\ \ g\mapsto(e_{g'}\mapsto e_{gg'}).$$

这是单的群同态，它将 G 实现为 $\mathbf{GL}(K[G])$ 的子群。

在应用时，我们通常选取 $K=\mathbb{F}_p$。

命题 24. *G 是有限群，$|G|=p^km$，其中，p 是素数并且 $(p,m)=1$。假设 S 是 G 的 Sylow p-子群，$H<G$ 为子群，则存在 $g\in G$，使得 $H\cap gSg^{-1}$ 是 H 的 Sylow p-子群。换而言之，通过对大群的 Sylow p-子群共轭可得到子群的 Sylow p-子群。*

证明： 证明的思想是考虑群作用在由自身所构造的对象上，请参考例3.10。

令 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。由于 X 是以上作用的轨道的并，必存在某个轨道 $\mathbf{O}=H\cdot x=H\cdot gS$，其元素个数不是 p 的倍数。

[12]参考2.7.1

[13]请参见练习题2.7.5一节

对群作用 $^{H}\curvearrowright X$，$x = gS$ 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。根据 $|\mathbf{O}||H \cap gSg^{-1}| = |H|$，则 $[H : H \cap gSg^{-1}] = |\mathbf{O}|$ 与 p 互素。这表明 $H \cap gSg^{-1}$ 是 H 的 Sylow p-子群。 □

作为应用，我们有

定理 25 (Sylow 第一定理)**.** *有限群有 Sylow p-子群。*

证明: 给定有限群 G，G 可视为 $\mathbf{GL}(n;\mathbb{F}_p)$ 的子群。根据例3.20，$\mathbf{GL}(n;\mathbb{F}_p)$ 有 Sylow p-子群，从而 G 有 Sylow p-子群。 □

利用群作用在由自身所构造的对象上的观点，我们还可以构造其它的群作用给出 Sylow 定理的证明：

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

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

那么，$|X| = \binom{qm}{q}$。我们有如下 $\bmod p$ 的同余关系：[14]

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

其中，q 是 p 的幂，$p \nmid m$。

群 G 通过左乘法作用于 X，即

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

由于 $|X|$ 与 p 互素，存在 $^{G}\curvearrowright X$ 的轨道 $\mathbf{O}$，其元素数目与 p 互素。任选 $A \in \mathbf{O}$，令 $S = \mathrm{Stab}(A)$ 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 $|G|$ 中所有 p 的幂，即 $q \mid |S|$。

另外，任选 $a \in A$，由于 S 是 A 的中心化子，所以以下映射是良好定义的：

$$S \longrightarrow A, \quad g \mapsto ga.$$

这显然是单射，从而，$|S| \leqslant |A| = q$。再根据 $q \mid |S|$，$q = |S|$，所以 S 为 Sylow p-子群。

推论 26 (Cauchy)**.** *若 p 整除 $|G|$，则 G 有阶为 p 的元素。*

证明: S 是 G 的 Sylow p-子群，任选非单位元 $x \in S$，它的阶整除 $|S|$，不妨假设这个阶为 p^m，其中 $m \geqslant 1$。那么，$x^{p^{m-1}}$ 的阶为 p。 □

[14]在多项式环 $\mathbb{F}_p[T]$ 中进行计算。由于当 $k \neq 0, p$ 时，$p \mid \binom{p}{k}$，对任意多项式 $f(T), g(T) \in \mathbb{F}_p[T]$，根据二项式公式，有

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

从而，对任意的 $f_1(T), \cdots, f_l(T) \in \mathbb{F}_p[T]$，有

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

我们利用上述公式计算 $(1+T)^{qm}$：

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

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

注记 3.11. 进一步分析以上证明中的轨道分解，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 $A_i\in\mathbf{O}_i$，从而，$\mathbf{O}_i=G\cdot A_i$。令 $S_i=\mathrm{Stab}(A_i)$ 为 A_i 的稳定化子，那么，$|\mathbf{O}_i||S_i|=|G|$。上述推理已经证明了 $|S_i|\leqslant p^k$。现在考虑以下两种可能：

1) $|S_i|<p^k$，那么，$p\mid|\mathbf{O}_i|$；

2) $|S_i|=p^k$，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，则对任意 $g\in G$，$S\cdot g\in X$ 并且其稳定化子恰为 S。实际上，如果 Sylow p-子群 S 保持某个 $A\in X$ 不变，即 $SA\subset A$，则 $A=Sa$，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

$$\begin{aligned}|X|&=\sum_{|S_i|<p^k}|\mathbf{O}_i|+\sum_{|S_i|=p^k}|\mathbf{O}_i|\\&\equiv 0+sm\ (\mathrm{mod}\ p).\end{aligned}$$

其中，s 是 Sylow p-子群的个数。对于 $|S_i|=p^k$ 的情形，每个轨道恰好有 m 个元素。由于 $|X|=m\ (\mathrm{mod}\ p)$，所以 $s=1\ (\mathrm{mod}\ p)$。这表明 Sylow p-子群的个数除 p 余 1。

注记 3.12. 上述等式

$$|X|\equiv 0+sm\ (\mathrm{mod}\ p).$$

的推导并未用到 G 的具体结构，所以 s 模 p 只依赖于 $|G|$（这里不需要使用 $\binom{qm}{q}\equiv m\bmod p$）。特别地，群 ${}^{\mathbb{Z}}\!/_{|G|\mathbb{Z}}$ 只有一个 Sylow p-子群，所以 $s\equiv 1\ (\mathrm{mod}\ p)$。

我们以下将给出有限群 Sylow p-子群的个数除 p 余 1 的另一个证明。

定理 27 (Sylow 第二定理)**.** *G 是有限群，则其每个 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 28. *G 是 p-群并且作用在有限集 X 上，令*

$$X^G=\big\{x\in X\big|gx=x,\forall g\in G\big\}.$$

那么，$|X|\equiv|X^G|\ (\mathrm{mod}\ p)$。

证明： X^G 中的元素恰对应只有一个元素的轨道，而集合 $X-X^G$ 是那些元素个数大于 1 的轨道的并。由于 G 是 p-群，后一种轨道的元素个数是 p 的倍数。所以，$|X|\equiv|X^G|\ (\mathrm{mod}\ p)$。 □

Sylow 第二定理的证明. 先证明第一个结论：假设 P 是 G 的 p-子群，任选 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，

$$|X^P|\equiv|X|\neq 0\ (\mathrm{mod}\ p).$$

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，$P<gSg^{-1}$ 而 gSg^{-1} 显然是 Sylow p-子群。

另外，若 P 是 Sylow p-子群，通过比较元素个数，$P<gSg^{-1}$ 意味着 $P=gSg^{-1}$，这证明了所有的 Sylow p-子群均共轭。 □

现在给出定理中关于 Sylow p-子群个数的新证明，它依赖于下述引理：

引理 29. *若 S 和 S' 是 G 的 Sylow p-子群并且 S' 正规化 S，即对任意 $s' \in S$，有 $s'Ss'^{-1} < S$，则 $S = S'$。*

证明： 由于 S' 正规化 S，所以 S' 是 S 的正规化子[15] $\mathrm{N}_G(S)$ 的 Sylow p-子群。另外，S 也是 $\mathrm{N}_G(S)$ 的 Sylow p-子群并且 $\mathrm{N}_G(S)$ 在 S 上共轭作用是平凡的，根据定理中的第二个结论，S 是 $\mathrm{N}_G(S)$ 中唯一的 Sylow p-子群。所以，$S = S'$。 □

现在令 X 为 G 的全体 Sylow p-子群的集合，S 可以通过共轭作用在 X 上，即

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

上述引理表明 $S \in X$ 是唯一一个被 S 固定的元素。根据引理 28，$|X| \equiv 1 \pmod{p}$。

注记 3.13. 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。Sylow 第二定理表明该作用是传递的，所以 Sylow p-子群的个数必能整除 $|G|$。

例子 3.22 ($\mathfrak{S}_6$ 非共轭自同构另一个构造)**.** 先考察 $\mathfrak{S}_5$ 的 Sylow 5-子群。根据例3.21，共有 $s = (5-2)! = 6$ 个这样的子群。我们也可以利用 Sylow 定理的结论来计算，由于 s 除 5 余 1，我们枚举以下可能性：

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

另外，根据 $|\mathfrak{S}_5| = 120$，$s \mid 120$，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 $s \geqslant 2$，从而 $s = 6$。

我们还可以利用 $\mathfrak{S}_5$ 的唯一非平凡正规子群为 $\mathfrak{A}_5$ 来排除 $s = 1$ 的情形：若不然，Sylow 第二定理表明这个 Sylow 5-子群是正规子群，矛盾。

令 $X = \{S_1, \cdots, S_6\}$ 是 Sylow 5-子群的集合。通过共轭，$\mathfrak{S}_5$ 在 X 上给出了传递的群作用：

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

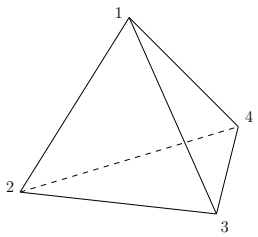
根据作传递性，$|\mathrm{Ker}(\varphi)| \leqslant 120 \div 6 = 20 < 60 = |\mathfrak{A}_5|$，根据 $\mathfrak{S}_5$ 的唯一非平凡正规子群为 $\mathfrak{A}_5$，我们可以断言 $\mathrm{Ker}(\varphi) = 1$，即 φ 是单射。令 $H = \mathrm{Im}(\varphi)$，那么，$H < \mathfrak{S}_X \simeq \mathfrak{S}_6$ 是有 120 个元素的子群并且 ${}^{H}\!\curvearrowright X$ 是传递的。

这里的构造满足例3.12中的条件。

3.3.4 正多面体的对称群

正四面体的对称群是 $\mathfrak{A}_4$ 用 $\mathbf{SO}(3)$ 表示 3×3 的行列式为 1 的正交矩阵的集合，这是 $\mathbb{R}^3$ 中旋转的所构成的群。对任意 $g \in \mathbf{SO}(3)$，若 $g \neq 1$，则 g 的不动点只有其旋转轴。

给定中心在原点的正四面体 $\mathbf{T}$ 并对其顶点如下标号：



[15] H 是群 G 的子群，H 在 G 中的**正规化子**被定义为 $\mathrm{N}_G(H) = \{g \in G | gHg^{-1} = H\}$。

现在考虑 $\mathbf{T}$ 的对称群：

$$\mathrm{Sym}^+(\mathbf{T}) := \big\{g \in \mathbf{SO}(3)\big|g\big(\mathbf{T}\big) = \mathbf{T}\big\}$$

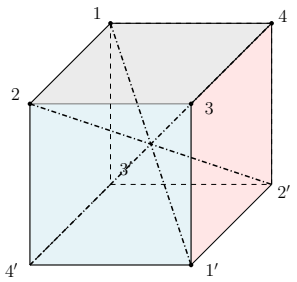
这是 $\mathbf{SO}(3)$ 的子群并自然地作用在 $\mathbf{T}$ 上。我们证明 $\mathrm{Sym}^+(\mathbf{T}) \simeq \mathfrak{A}_4$。

每个 $g \in \mathrm{Sym}^+(\mathbf{T})$ 把正四面体的顶点映到顶点，通过标号，我们认为 g 给出了 $\varphi(g) \in \mathfrak{S}_4$。例如，以过顶点 1 及其对面中心为轴的角度为 $\frac{2\pi}{2}$ 的旋转 g，把顶点 2 映成 3、3 映成 4、4 映成 2，所以，$\varphi(g) = (2,3,4) \in \mathfrak{S}_4$。据此 $\mathrm{Sym}^+(\mathbf{T})$ 作用在顶点集合 $\{1,2,3,4\}$ 上，从而有群同态：

$$\varphi : \mathrm{Sym}^+(\mathbf{T}) \longrightarrow \mathfrak{S}_4.$$

另外，若 g 固定了所有的顶点，则 $g = 1$，从而 φ 是单射。我们现在来决定 φ 的像 $\mathrm{Im}(\varphi) < \mathfrak{S}_4$。实际上，绕着过顶点以及其对面中心为轴的旋转给出了所有的 3-循环，它们生成了 $\mathfrak{A}_4$。所以，$\mathfrak{A}_4 < \mathrm{Im}(\varphi) < \mathfrak{S}_4$。若 $\mathrm{Im}(\varphi) \neq \mathfrak{A}_4$，则 $\mathrm{Im}(\varphi) = \mathfrak{S}_4$，从而存在 g，使得 $\varphi(g) = (3,4)$，从而，$g(1) = 1, g(2) = 2$，从而 g 在旋转轴外有不动点，这不可能。

正六面体的对称群是 $\mathfrak{S}_4$　考虑中心在原点的正六面体 $\mathbf{C}$：把一个面上的顶点标号为 $1,2,3,4$ 而与它们中心对称的顶点则标号为 $1',2',3',4'$。



它的对称群为

$$\mathrm{Sym}^+(\mathbf{C}) := \big\{g \in \mathbf{SO}(3)\big|g\big(\mathbf{C}\big) = \mathbf{C}\big\}$$

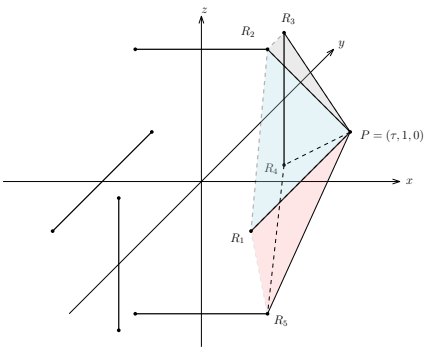
这是 $\mathbf{SO}(3)$ 的子群并自然地作用在 $\mathbf{T}$ 上。

对 $a = 1,2,3,4$，用 X 表示过 a 与 a' 的直线 ℓ_a 的集合，即 $X = \{\ell_1, \ell_2, \ell_3, \ell_4\}$。每个 $g \in \mathrm{Sym}^+(\mathbf{C})$ 把 $\ell \in X$ 映射成某个 $\ell' \in X$，从而有群作用

$$\varphi : \mathrm{Sym}^+(\mathbf{T}) \to \mathfrak{S}_X.$$

φ 显然是单射。它的像 $\mathrm{Im}(\varphi)$ 包含所有绕某个 ℓ_i 的角度为 $\frac{2\pi}{3}$ 和 $\frac{4\pi}{3}$ 的旋转，即所有 3-循环，从而 $\mathfrak{A}_4 < \mathrm{Im}(\varphi)$。另外，以对边中点为轴、以 π 为角度的旋转给出 $\mathfrak{S}_X$ 中的一个对换，从而，$\mathrm{Im}(\varphi)$ 包含 $\mathfrak{A}_4$ 之外的元素。根据 $[\mathfrak{S}_4 : \mathfrak{A}_4] = 2$，$\mathrm{Im}(\varphi) = \mathfrak{S}_4$。

正二十面体的对称群是 $\mathfrak{A}_5$　考虑正二十面体 $\mathbf{I}$：



其中，我们可以参考2.1.1一节中正二十面体的定义。它的对称群定义是 $\mathbf{SO}(3)$ 的子群：

$$\mathrm{Sym}^+(\mathbf{I}) := \big\{g \in \mathbf{SO}(3) \big| g\big(\mathbf{I}\big) = \mathbf{I}\big\}.$$

除单位元外，我们罗列出 $\mathrm{Sym}^+(\mathbf{I})$ 的**部分**（可能是所有）元素：

a) 绕以过对顶点的直线为轴、角度为 $\frac{k}{5}\pi$ 的旋转（$k = 1, 2, 3, 4$），共有 24 个。

b) 绕以过对面中心的直线为轴、角度为 $\frac{k}{3}\pi$ 的旋转（$k = 1, 2$），共有 20 个。

c) 绕以过对边中点的直线为轴、角度为 π 的旋转，共有 15 个。

连同单位映射，以上给出了 $\mathrm{Sym}^+(\mathbf{I})$ 中 60 个元素 $G_{\mathbf{I}}$。首先证明 $\langle G_{\mathbf{I}}\rangle = \mathrm{Sym}^+(\mathbf{I})$。给定 $g \in \mathrm{Sym}^+(\mathbf{I})$，令 $P' = g \cdot P$。

- 如果 $P' \notin \{P, R_1, R_2, R_3, R_4, R_5\}$，可选取 $\sigma \in G_{\mathbf{I}}$，使得 $\sigma P' \in \{P, R_1, R_2, R_3, R_4, R_5\}$：实际上，不妨设 $P' \in \{-P, -R_1\}$，选以 z 轴为对称轴、旋转角度为 π 的旋转 σ，则 $\sigma(P') \in \{R_1, P'\}$。所以，通过复合 $G_{\mathbf{I}}$ 中元素，我们可以假设 $gP' \in \{P, R_1, R_2, R_3, R_4, R_5\}$。
- 进一步复合以过面 PR_kR_{k+1} 及其对面的中心为轴的旋转，我们可以假设 $gP = P$。此时，g 的旋转轴为过 P 与 $-P$ 的直线，所以只能是某个绕以过 P 和 $-P$ 直线为轴、角度为 $\frac{k}{5}\pi$ 的旋转的旋转。

这就证明了 $\mathrm{Sym}^+(\mathbf{I}) = \langle G_{\mathbf{I}}\rangle$。

其次，我们证明 $\mathrm{Sym}^+(\mathbf{I}) = G_{\mathbf{I}}$。考虑 $\mathrm{Sym}^+(\mathbf{I})$ 作用在 $\mathbf{I}$ 的 12 个顶点集上，这个作用是传递的。顶点 P 的稳定化子 $\mathrm{Stab}(x)$ 恰有 5 个元素。从而，

$$|\mathrm{Sym}^+(\mathbf{I})| = |\mathrm{Stab}(x)| \times 12 = 60.$$

特别地，我们有 $\mathrm{Sym}^+(\mathbf{I}) = G_{\mathbf{I}}$。

最终，我们研究 $\mathrm{Sym}^+(\mathbf{I})$ 的群结构。一个三**线组**指的是过原点的三条相互垂直的直线并且每条直线都通过 $\mathbf{I}$ 的某对边的中点，比如 x, y, z 三个轴组成这样的一个三线组。令 X 是三线组的集合，则 $|X| = 5$（每个三线组对应 $\mathbf{I}$ 的 6 条边）。$\mathrm{Sym}^+(\mathbf{I})$ 中的元素保持 $\mathbb{R}^3$ 中间直线的正交性并且把 $\mathbf{I}$ 的边的中点映射为边的中点，所以，$\mathrm{Sym}^+(\mathbf{I})$ 自然地作用在 X 上：

$$\varphi : \mathrm{Sym}^+(\mathbf{I}) \longrightarrow \mathfrak{S}_X \simeq \mathfrak{S}_5.$$

以下证明 φ 是单射：

引理 30. *对 $g \in \mathrm{Sym}^+(\mathbf{I}) - \{1\}$（用 ℓ_g 表示其旋转轴），存在 $\mu(g) \in \mathrm{Sym}^+(\mathbf{I})$（未必唯一），使得 $\ell_{\nu(g)} \perp \ell_g$ 并且 $\mu(g)^2 = 1$（即 $\mu(g)$ 为绕过对边中点的直线为轴的旋转）。*

证明：对 $\mathrm{Sym}^+(\mathbf{I})$ 的元素进行枚举证明：

1) 绕以过对顶点的直线为轴的旋转：比如轴是过 P 的直线，选取 $\mu(g)$ 为以 z 轴为轴的旋转。

2) 绕以过对面中心的直线为的轴旋转，比如轴过 $(1,1,1)$（面 PR_1R_2 的中心），则选取 $\mu(g)$ 为以过 R_1R_5 的中点的轴垂直，这因为

$$R_1=(\tau,-1,0),R_5=(1,0,-\tau)\quad\Rightarrow\quad\frac{1}{2}\big(R_1+R_5\big)=\frac{1}{2}(1+\tau,-1,-\tau).$$

3) 绕以过对边中点的直线为轴的旋转，比如轴是 z 轴，则选 $\mu(g)$ 为以 y 或 x 轴为轴的旋转。

以上罗列所有的可能，命题得证。 □

如果 $g\in\mathrm{Ker}(\varphi)$ 并且 $g\neq 1$。那么，g 固定三线组 x,y,z。从而，g 给出了 $\{x,y,z\}$ 到自身的映射。特别地，$g^5\neq 1$（因为 $\langle g\rangle$ 作用在 3 个元素的集合上，若 g 的阶是 5，则 $g(x)=x,g(y)=y,g(z)=z$，这表明 g 为 1 或者 -1，矛盾），从而 g 不是 5 阶的旋转。

根据引理中的构造，$\mu(g)$ 所的轴 $\ell_{\mu(g)}$ 一定是某个三线组的元素，记此三线组为 $\{\ell_{\mu(g)},\ell_2,\ell_3\}$。根据 $g\in\mathrm{Ker}(\varphi)$，有

$$g:\{\ell_{\mu(g)},\ell_2,\ell_3\}\longrightarrow\{\ell_{\mu(g)},\ell_2,\ell_3\}$$

另外，因为 $\ell_g\perp\ell_{\mu(g)},\ell_{\mu(g)}$ 在 g 的作用下一定改变，从而 $g^2=1$：如若不然，$g^3=1$，则 $\ell_{\mu(g)},g\big(\ell_{\mu(g)}\big),g^2\big(\ell_{\mu(g)}\big)$ 是与 ℓ_g 垂直的平面上的三条不同的直线，但是 $\{\ell_{\mu(g)},g\big(\ell_{\mu(g)}\big),g^2\big(\ell_{\mu(g)}\big)\}=\{\ell_{\mu(g)},\ell_2,\ell_3\}$ 是两两垂直的，矛盾。

此时，唯一可能为 $g^2=1$，不妨设 g 为以 z 轴为轴的旋转，它把 R_1R_2 的中点 $\frac{1}{2}(\tau+1,-1,\tau)$ 映射成 $\frac{1}{2}(-\tau-1,+1,\tau)$，它们的内积为

$$\frac{1}{2}(\tau+1,-1,\tau)\cdot\frac{1}{2}(-\tau-1,+1,\tau)=-\frac{1}{2}\,(\tau+1)$$

这表明 g 把过 R_1R_2 的中点的线所在的三线组映射成另外的三线组，与 $g\in\mathrm{Ker}(\varphi)$ 矛盾。

综上所述，$\varphi:\mathrm{Sym}^+(\mathbf{I})\longrightarrow\mathfrak{S}_X$ 是单射，从而 $\varphi\big(\mathrm{Sym}^+(\mathbf{I})\big)$ 是 $\mathfrak{S}_5$ 的 60 阶的子群。我们已构造 20 个 3 阶元，它们的像必然是 $\mathfrak{S}_5$ 中的 3-循环并且 $\mathfrak{S}_5$ 中共有 20 个 3-循环。所以，$\varphi\big(\mathrm{Sym}^+(\mathbf{I})\big)$ 包含 3-循环生成的子群，从而 $\varphi:\mathrm{Sym}^+(\mathbf{I})=\mathfrak{A}_5$。

注记 3.14. 还可以利用习题3.6.2的想法先证明 $\mathrm{Sym}^+(\mathbf{I})$ 是单群来说明 φ 是单射。

注意到如果 $g\in\mathbf{SO}(3)$ 是以直线 ℓ 为旋转轴、角度为 θ 的旋转，那么，对任意 $h\in\mathbf{SO}(3)$，$h\cdot g\cdot h^{-1}$ 是以直线 $h(\ell)$ 为旋转轴、角度为 θ 的旋转。据此，对任意的 $g,g'\in\mathbf{SO}(3)$，g 与 g' 共轭当且仅当它们的旋转角度相同。

利用以上的观察不难说明，$\mathrm{Sym}^+(\mathbf{I})$ 一共有如下几个共轭类：

旋转角度	0	$\frac{2}{5}\pi$	$\frac{4}{5}\pi$	$\frac{2}{3}\pi$	π
元素个数	1	12	12	20	15

由于 $\mathrm{Sym}^+(\mathbf{I})$ 的非平凡正规子群一定是以上若干个共轭类的并，所以其元素个数只能是以下集合中的某个数：

$$\{13,16,21,25,28,33,36,40,45,48\},$$

但它们不是 60 的约数，从而，$\mathrm{Sym}^+(\mathbf{I})$ 是单群。

注记 3.15. 正二十面体的 3 组对边中点连线给出一个正八面体，一共有 5 个这样的正八面体。$\mathrm{Sym}^+(\mathbf{I})$ 在这些八面体构成的集合上的作用给出它到 $\mathfrak{A}_5$ 的同构。

3.3.5 PSL$(2;K)$ 与分式线性变换以及 Galois 的一个命题

K 是域，规定 $K\cup\{\infty\}$ 的运算法则：

$$a\pm\infty=\infty,\ \frac{b}{\infty}=0,\ c\cdot\infty=\infty,\ \frac{c}{\infty}=0,\ \frac{\infty}{\infty}=1,\ 0\cdot\infty=0,$$

其中，$a,b,c\in K$ 并且 $c\neq 0$。

固定如下双射

$$\Phi:K\cup\{\infty\}\longrightarrow\mathbf{P}^1(K),\qquad k\mapsto[k:1],\ k\in K;\quad \infty\mapsto[1:0].$$

我们定义 $\mathbf{GL}(2;K)$ 在 $K\cup\{\infty\}$ 上的作用（直接计算可以证明这是群作用），

$$\mathbf{GL}(2;K)\times K\cup\{\infty\}\longrightarrow K\cup\{\infty\},\ \left(\begin{pmatrix}a&b\\c&d\end{pmatrix},x\right)\mapsto\begin{pmatrix}a&b\\c&d\end{pmatrix}\cdot x=\frac{ax+b}{cx+d}.$$

由于 $k\cdot\begin{pmatrix}1&0\\0&1\end{pmatrix}$ 的作用是平凡的，其中，$k\in K^\times$，以上诱导出群作用

$$\mathbf{PGL}(2;K)\times K\cup\{\infty\}\longrightarrow K\cup\{\infty\}.$$

特别地，以上定义的 $\mathbf{PGL}(2;K)\longrightarrow\mathfrak{S}_{K\cup\{\infty\}}$ 是单射。

注记 3.16. 以上的群作用与 $\mathbf{GL}(2;K)$ 在 $\mathbf{P}^1(K)$ 的作用是同构的，请参考定义3.6。实际上，$\Phi^{-1}([x:y])=\frac{x}{y}$（如果 $y\neq 0$）。固定 $g=\begin{pmatrix}a&b\\c&d\end{pmatrix}$，我们有

$$g\cdot[x:y]=[ax+by:cx+dy].$$

所以，

$$\Phi^{-1}\left(g\cdot[x:y]\right)=\frac{ax+by}{cx+dy}=\frac{a\frac{x}{y}+b}{c\frac{x}{y}+d}=g\cdot\Phi^{-1}([x:y]).$$

例子 3.23 (∞ 的稳定化子)**.** 我们有

$$\mathrm{Stab}(\infty)=\left\{\begin{pmatrix}a&b\\0&1\end{pmatrix}\in\mathbf{PSL}(2;K)\right\}$$

它们对应的分式线性变换为 $x\mapsto ax+b$，这是例3.8中定义的 1 维的仿射变换群。总之，$\mathrm{Stab}(\infty)=\mathbf{Aff}_1(K)$。

例子 3.24. 我们有

$$\mathbf{Scal}:=\mathrm{Stab}(\infty)\cap\mathrm{Stab}(0)=\left\{x\mapsto kx\middle|k\in K^\times\right\},$$

这是以 0 为中心的伸缩变换。注意到 **Scal** 不是 $\mathrm{Stab}(\infty)$ 的正规子群。

平移变换子群为

$$\mathbf{Parellel}=\left\{\begin{pmatrix}1&b\\0&1\end{pmatrix}\middle|b\in K\right\}.$$

这是 $\mathrm{Stab}(\infty)$ 的子群并且是正规子群。另外，$\mathbf{Parellel}\cap\mathbf{Scal}=1$。

矩阵 $\begin{pmatrix}0&1\\1&0\end{pmatrix}$ 对应着反演映射 $\mathbf{Inv}:x\mapsto\frac{1}{x}$。

例子 3.25. 利用矩阵的行列变换可以看出子群 **Parellel** 与反演映射生成了所有分式线性变换，即 $\langle \mathbf{Parellel}, \mathbf{Inv}\rangle = \mathbf{PSL}(2;K)$。

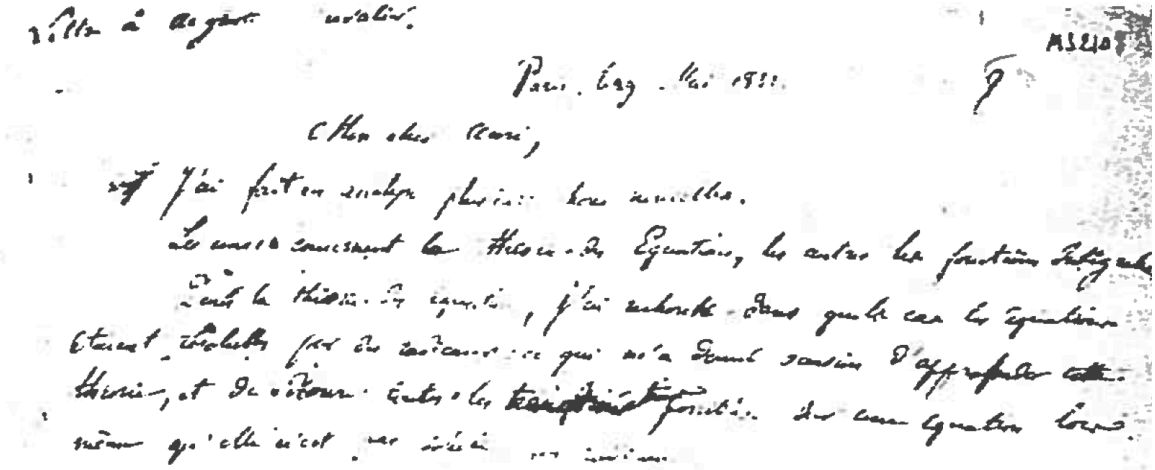
命题 31. $\mathbf{PGL}(2;K)$ 在 $K\cup\{\infty\}$ 上的作用是 3-传递的，即对任意的 (x,y,z) 和 (x',y',z')，其中，$\{x,y,z\}\subset K\cup\{\infty\}$ 两两不同，$\{x',y',z'\}\subset \cup\{\infty\}$ 两两不同，存在唯一的 $g\in\mathbf{PGL}(2;K)$，使得 $g(x)=x', g(y)=y', g(z)=z'$。

证明: 实际上，对任意的 $\{x_1,y_1,z_1\}\subset K\cup\{\infty\}$，映射

$$x\mapsto \frac{y_1-z_1}{y_1-x_1}\frac{x-x_1}{x-z_1}$$

是唯一使得 $g(x_1)=0, g(y_1)=1, g(z_1)=\infty$ 的分式线性变换。 □

1832 年 5 月 29 日，也就是那场著名决斗的前夜，Galois 把构思已久的几个定理写在给挚友 Auguste Chevalier 的信里：



"··· 我的研究有了新的进展，部分关于方程的理论而另一部分涉及函数的积分。在方程方面，通过研究何种情形方程可通过根式解出，我可以真正深入理论来描述对一个方程所有可能的变换，即使该方程的解不能通过根式给出。

这些想法可以写成三篇文章。第一篇已完成，Possion 教授对此有不同见解，但我仍坚持它的重要性并进行了必要的修正。第二篇包含了一些相当有趣的应用。以下是最重要内容的总结：

·····

我一生中常常敢于提出一些自己不确定的命题，但在这里的内容在我却反复思考了一年有余 ···

恳求你公开邀请 Jacobi 或 Gauss 发表意见，不是对这些定理的正确性，而是对它们的重要性 ···"

注意到，$\mathbf{PGL}(2;\mathbb{F}_p)$ 可以自然得作用在具有 $p+1$ 个元素的集合 $\mathbf{P}^1(\mathbb{F}_p)$ 上。在绝笔信中，Galois 想理解 $\mathbf{PGL}(2;\mathbb{F}_p)$ 是否能作用在一个元素个数不超过 p 的集合上，他的思考可以给出如下有趣的性质：

命题 32. $\mathbf{PGL}(2;\mathbb{F}_{11})$ 有一个同构于 $\mathfrak{A}_5$ 的子群。

首先注意到 $\left|\mathbf{PGL}(2;\mathbb{F}_{11})\right| = 1320 = 2^3\times 3\times 5\times 11$。通过实现为分式线性变换，我们将 $\mathbf{PGL}(2;\mathbb{F}_{11})$ 视作是 $\mathfrak{S}_{\mathbb{F}_{11}\cup\infty}$ 的子群并尝试把 $\mathbf{PGL}(2;\mathbb{F}_{11})$ 中的元素写成 $\mathfrak{S}_{\{0,1,2,\cdots,10,\infty\}}$ 中循环的分解。

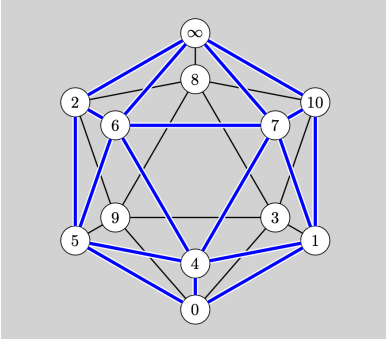
对于 $g_1=\begin{pmatrix}2 & 0\\ 0 & 2^{-1}\end{pmatrix}$，它对应着 $\mathbb{F}_{11}$ 中乘 4 的运算。从而，

$$g_1=(1,4,5,9,3)(10,7,6,2,8).$$

对于 $g_2 = \begin{pmatrix} 7 & 1 \\ 1 & 5 \end{pmatrix}$，我们可以计算

$$g_2 = (0,9,3)(1,5,8)(2,10,4)(7,6,\infty).$$

实际上，利用在 $\mathbb{F}_{11}$ 中 $2\times 6 = 3\times 4 = 5\times 9 = 7\times 8 = 10^2 = 1$，计算是简单的。现在考虑如下的正二十面体，其中，我们用 $\mathbb{F}_{11}\cup\{\infty\}$ 对其顶点进行标记：



此时，g_1 对应着绕过 0 和 ∞ 的轴而角度为 $\frac{2\pi}{5}$ 的旋转；g_1 对应着绕过面 $0,9,3$ 和面 $7,6,\infty$ 的中心为轴而角度为 $\frac{2\pi}{3}$ 的旋转。

将 $\mathrm{Sym}^+(\mathbf{I})$ 和 $\mathbf{PGL}(2;\mathbb{F}_{11})$ 视作是 $\mathfrak{S}_{\{0,\cdots,10,\infty\}}$ 的子群，那么，$g_1, g_2 \in \mathrm{Sym}^+(\mathbf{I})$。特别地，$S = \langle g_1, g_2\rangle \subset \mathrm{Sym}^+(\mathbf{I}) \simeq \mathfrak{A}_5$ 并且自然有 $S < \mathbf{PGL}(2;\mathbb{F}_{11})$。由于 g_1 和 g_2 的阶分别是 3 和 5，从而，$|S| \geqslant 15$。特别地，$[\mathrm{Sym}^+(\mathbf{I}) : S] \leqslant 4$。我们考虑 $\mathrm{Sym}^+(\mathbf{I})$ 通过左乘法作用在 $X = {}^{\mathrm{Sym}^+(\mathbf{I})}\!/_{S}$ 上，这给出了群同态

$$\varphi : \mathrm{Sym}^+(\mathbf{I}) \longrightarrow \mathfrak{S}_X.$$

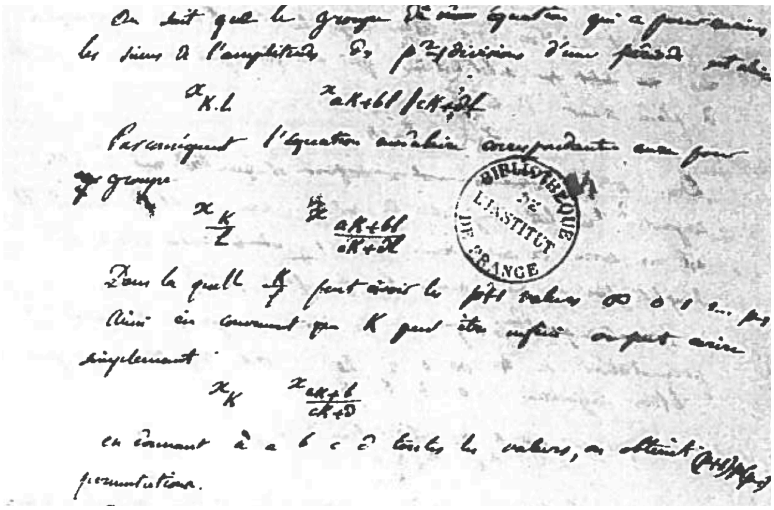
由于 $|X| \leqslant 4$，$|\mathrm{Sym}^+(\mathbf{I})| = 60 > 24 \geqslant \mathfrak{S}_X$。所以，$\mathrm{Ker}(\varphi) \neq 1$。又因为 $\mathrm{Sym}^+(\mathbf{I}) \simeq \mathfrak{A}_5$ 是单群，所以，φ 是平凡的，从而，$S = \mathrm{Sym}^+(\mathbf{I})$。这就证明了 $\mathrm{Sym}^+(\mathbf{I}) < \mathbf{PGL}(2;\mathbb{F}_{11})$。

另外，注意到 g_1 与 g_2 的行列式为 1，我们实际上找到了 $\mathbf{PSL}(2;\mathbb{F}_{11})$ 的同构于 $\mathfrak{A}_5$ 的子群。实际上，还可以考虑映射的复合：

$$\begin{array}{ccc} \mathfrak{A}_5 & \xrightarrow{\subset} & \mathbf{PGL}(2;\mathbb{F}_{11}) \\ & \searrow^{\varphi} & \downarrow{\scriptstyle \pi} \\ & & \mathbf{PSL}(2;\mathbb{F}_{11}) \end{array}$$

由于 $\mathfrak{A}_5$ 是单群，不难看出 $\mathrm{Ker}(\varphi) = 1$，从而，$\varphi$ 给出了 $\mathfrak{A}_5$ 到 $\mathbf{PSL}(2;\mathbb{F}_{11})$ 的嵌入。

注记 3.17. Galois 在信中利用分式线性变换来讨论群（每个群都应被视作是变换群！）：



他也明确写下了 $(1,4,5,9,3)$ 与 $(10,7,6,2,8)$ 这两个循环。请参考以下用 tex 重新录入的原文：

http://denise.vella.chemla.free.fr/transc-Galois-Lettre-a-Chevalier.pdf

3.4 群的半直积

3.4.1 基本定义

G 是群，$K < G$ 是子群，$N \lhd G$ 是正规子群。通过共轭，K 自然地作用在 N 上：

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

我们断言 $N \cdot K = \{n \cdot k | n \in N, k \in K\}$ 是子群：对任意 $n, n' \in N, k, k' \in K$，有

$$(nk) \cdot (n'k') = \left(n \cdot kn'k^{-1}\right) \cdot \left(kk'\right) \in N \cdot K$$

以及

$$(nk)^{-1} = \left(k^{-1}n^{-1}k\right) \cdot k \in N \cdot K.$$

以上计算的关键是利用 N 为正规子群。类似地，我们还得到 $N \cdot K = K \cdot N$。另外，注意到 $(nk) \cdot (n'k') = nn' \cdot kk'$ 未必成立并且 N 与 K 中的元素相乘未必交换。

进一步假设 $N \cdot K = G$ 并且 $N \cap K = 1$ 并定义映射

$$\phi : N \times K \to G, \quad (g, k) \mapsto gk.$$

我们证明，ϕ 是 $N \times K$（这是群的乘积）与 G 之间的双射（未必是群同态）：根据 $N \cdot K = G$，ϕ 是满射；若 $nk = n'k'$，则 $n^{-1}n' = kk'^{-1} \in N \cap K = 1$，从而，$n = n'$ $k = k'$，所以，ϕ 是单射。

我们注意到，作为群 $N \times K$ 与 G 未必同构：$N \times K$ 中，对任意 $n \in K$ 和 $k \in K$，$(n, 1)$ 与 $(1, k)$ 交换；它们在 G 中的像为 n, k，但是它们未必交换。实际上，对任意的 $x, x' \in G$，它们可以被唯一地表示成 $x = nk, x' = n'k'$ 并且在 G 中的乘法应写成

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

定义 3.4 (半直积)**.** 给定如下的基本数据：群 N，群 K 以及 K 在 N 上的作用 $\varphi : K \to \mathbf{Aut}(N)$（从而，对任意 $k \in K$，$\varphi(k)$ 是 N 到自身的同构）。作为集合，定义

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

那么，$N \rtimes_\varphi K$ 中的元素可唯一表示为 (n,k)，其中，$n \in n, k \in K$。$N \rtimes_\varphi K$ 上的乘法定义如下：对任意 $(n,k),(n',k') \in N \rtimes_\varphi K$，令

$$(n,k)\cdot(n',k') = \big(n \cdot_{_N} \varphi(k)(n'), k \cdot_{_K} k'\big),$$

并令 $1 = (1_{_N}, 1_{_K})$ 为单位元。以上下指标 K 和 N 强调使用 K 和 N 中的乘法。我们称如上构造的 $N \rtimes_\varphi K$ 为 N 和 K 在 φ 下的**半直积**。

注记 3.18 (验证群结构)**.** 首先验证 1 是单位元：对任意 $(n,k) \in N \rtimes_\varphi K$，有

$$(n,k)\cdot(1_{_N},1_{_K}) = \big(n \cdot_{_N} \varphi(k)(1_{_N}), k \cdot_{_K} 1_{_K}\big) = \big(n \cdot_{_N} 1_{_N}, k\big) = (n,k),$$

和

$$(1_{_N},1_{_K})\cdot(n,k) = \big(1_{_N} \cdot_{_N} \varphi(1_{_K})(n), 1_{_K} \cdot k\big) = \big(1_{_N} \cdot_{_N} \mathrm{id}(n), 1_{_K} \cdot k\big) = (n,k).$$

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

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

利用 φ 是群同态，我们就有

$$\varphi(k)\big(\varphi(k')(n'')\big) = \varphi(kk')(n'').$$

从而，结合律成立。

最终，验证逆元的存在性。对任意 $(n,k) \in N \rtimes_\varphi K$，有

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

以上构造给出了半直积的构造。

注记 3.19. 若 K 对 N 的作用平凡，则 $N \rtimes_\varphi K \simeq N \times K$。不难证明，双射

$$\phi : N \times K \to N \rtimes_\varphi K,\ \ (n,k) \mapsto (n,k)$$

是群同构当且仅当作用 φ 是平凡的。

例子 3.26. G 是群，$K < G$ 是子群，若存在子群 $H < G$，使得 $H \cap K = 1$ 且 $N \cdot K = G$，就称 H 是 K 在 G 中的**补子群**。

如果 $N \lhd G$ 是正规子群，K 在 G 中的补子群，那么，K 可以通过共轭在 N 上作用。此时，上面的讨论给出了群同构

$$G \simeq N \rtimes_{K \overset{\text{Int}}{\curvearrowright} N} K.$$

简单起见，人们常把上述同构写成 $G = N \rtimes K$。

注记 3.20. 考虑自然的投影同态

$$\pi_2 : N \rtimes_\varphi K \to K, \quad (n,k) \mapsto k.$$

这是满同态并且 $\mathrm{Ker}(\pi_2) = N \times 1 \subset N \rtimes_\varphi K$。很明显，$\mathrm{Ker}(\pi_2)$ 与 N 同构。我们得到群同态的正合列：

$$1 \to N \longrightarrow N \rtimes_\varphi K \xrightarrow{\pi_2} K \to 1,$$

其中，$N \longrightarrow N \rtimes_\varphi K$ 由 $n \mapsto (n,1)$ 给出。

另外，我们还有群同态

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

并且 $\pi_2 \circ \phi = \mathrm{id}$。我们称这样的 ϕ 是 π_2 的提升。如果正合列有提升，则称它是**分裂的**。如上提升的存在性可以用群的上同调理论来刻画，我们不再做深入的讨论。

关于上述正合列的讨论是提示如下的直观：给定 G 的正规子群 N 和商群 G/N，若清楚 G/N 在 N 上的共轭作用，就可确定 G 的结构。

注记 3.21 (半直积的唯一性)**.** 给定一组基本数据，即群 N，群 K 以及 K 对 N 的作用 $\varphi : K \to \mathbf{Aut}(N)$。若存在群 N' 和群 K' 以及群同构

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

则可以构造 K' 在 N' 上的自然作用

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

以上由交换图给出：

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

我们断言映射

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

是群同构。这个群同构给出了半直积唯一性的含义。

很明显 Φ 是双射，以下验证它是群同态：

$$\begin{aligned} \Psi\big((n_1',k_1')\cdot(n_2',k_2')\big) &= \Psi\Big(\big(n_1'\varphi'(k_1)(n_2'), k_1'k_2'\big)\Big) = \Psi\Big(\big(n_1'\big(\alpha^{-1}\circ\varphi\big(\beta(k_1')\big)\circ\alpha\big)(n_2'), k_1'k_2'\big)\Big) \\ &= \Big(\alpha\big[\big(n_1'\big(\alpha^{-1}\circ\varphi\big(\beta(k_1')\big)\circ\alpha\big)(n_2')\big], \beta(k_1'k_2')\big)\Big) \\ &= \Big(\alpha(n_1')\big(\varphi\big(\beta(k_1')\big)(\alpha(n_2')), \beta(k_1')\beta(k_2')\big)\Big). \end{aligned}$$

另外，

$$\Psi(n_1',k_1')\cdot\Psi(n_2',k_2') = (\alpha(n_1'),\beta(k_1'))\cdot(\alpha(n_2'),\beta(k_2')) = \Big(\alpha(n_1')\big(\varphi\big(\beta(k_1')\big)(\alpha(n_2')), \beta(k_1')\beta(k_2')\big)\Big).$$

从而，$\Psi\big((n_1',k_1')\cdot(n_2',k_2')\big) = \Psi(n_1',k_1')\cdot\Psi(n_2',k_2')$。

3.4.2 基本例子

例子 3.27. G 是群，$N \lhd G, K \lhd G$ 均为正规子群，$N \cdot K = G$ 并且 $N \cap K = 1$。那么，

$$G \simeq N \times K.$$

我们知道 $G \simeq N \rtimes_{K \overset{\text{Int}}{\curvearrowright} N} K$。对任意 $k \in K, n \in N$，有

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

所以，群作用 ${}^{K\overset{\text{Int}}{\curvearrowright}}N$ 是平凡的。从而，$G \simeq N \times K$。

例子 3.28. 二面体群 $\mathfrak{D}_n$ 中旋转构成的子群 $N = \{1, r, \cdots, r^{n-1}\} \simeq \mathbb{Z}\big/_{n\mathbb{Z}}$ 是正规的，$K = \{1, s\} \simeq \mathbb{Z}\big/_{2\mathbb{Z}}$ 是某反射生成的子群。根据 $srs = srs^{-1} = r^{-1}$，K 在 N 上的共轭由如下同态给出

$$\varphi : \mathbb{Z}\big/_{2\mathbb{Z}} \to \mathbf{Aut}\big(\mathbb{Z}\big/_{n\mathbb{Z}}\big), \quad 0 \mapsto \mathrm{id},\ 1 \mapsto (k \mapsto -k).$$

所以，

$$\boxed{\mathfrak{D}_n \simeq \mathbb{Z}\big/_{n\mathbb{Z}} \rtimes_{\varphi} \mathbb{Z}\big/_{2\mathbb{Z}}}.$$

由于 φ 非平凡，$\mathfrak{D}_n \not\simeq \mathbb{Z}\big/_{n\mathbb{Z}} \times \mathbb{Z}\big/_{2\mathbb{Z}}$。

例子 3.29. K 是域，线性空间 K^n 上的 n 维仿射变换群为

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

平移变换和线性变换

$$\mathrm{Trans}(n;K) := \big\{x \mapsto x + b \big| b \in K^n\big\},\ \mathbf{GL}(n;K) := \big\{x \mapsto Ax \big| A \in \mathbf{GL}(n;K)\big\},$$

均为 $\mathbf{Aff}_n(K)$ 的子群，其中，$\mathrm{Trans}(n;K) \simeq K^n$ 并且 $\mathrm{Trans}(n;K) \lhd \mathbf{Aff}_n(K)$。

我们计算 $\mathbf{GL}(n;K)$ 在 $\mathrm{Trans}(n;K)$ 上的共轭作用：对任意 $g(x) = Ax$ 和 $T_b(x) = x + b$，有

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

所以，

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

其中，

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

例子 3.30 (阶较小群几何实现的例子)**.** $G = \mathbf{Aff}_2(\mathbb{F}_2)$ 自然地作用在 $X = \mathbb{F}_2^2$ 上：

$$\mathbf{Aff}_2(\mathbb{F}_2) \times \mathbb{F}_2^2 \to \mathbb{F}_2^2, \quad \big((b, A), x\big) \mapsto (b, A) \cdot x = Ax + b.$$

这给出群同态

$$\varphi : \mathbf{Aff}_2(\mathbb{F}_2) \longrightarrow \mathfrak{S}_{\mathbb{F}_2^2}.$$

以上同态显然是单射。我们计算 $|\mathfrak{S}_{\mathbb{F}_2^2}| = 4!$ 以及 $|\mathbb{F}_2^2 \rtimes_{\varphi} \mathbf{GL}(2;\mathbb{F}_2)| = 4 \cdot 6 = 24$，所以 φ 群同构，即

$$\boxed{\mathbf{Aff}_2(\mathbb{F}_2) \simeq \mathfrak{S}_4}.$$

我们把 $\mathbb{F}_2^2$ 的元素按照如下方式标号：$1\to(0,0),2\to(1,0),3\to(0,1),4\to(1,1)$。

另外，$\mathbf{GL}(n;\mathbb{F}_2)$ 在 $\mathbf{P}^2(\mathbb{F}_2)$ 上的自然作用给出群同态

$$\mathbf{GL}(n;\mathbb{F}_2)\to\mathfrak{S}_{\mathbf{P}^2(\mathbb{F}_2)}\simeq\mathfrak{S}_3.$$

通过计算元素个数可知 $\mathbf{GL}(n;\mathbb{F}_2)\simeq\mathfrak{S}_3$。从而，

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

我们可以具体分析同构：

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

考虑 $\mathfrak{S}_4$ 的正规子群 $K_4\lhd\mathfrak{S}_4$：

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

我们有

$$K_4=\mathrm{Im}\left(\left(\mathbb{Z}\big/2\mathbb{Z}\right)^2\hookrightarrow\left(\mathbb{Z}\big/2\mathbb{Z}\right)^2\rtimes_\varphi\mathfrak{S}_3\xrightarrow{\psi}\mathfrak{S}_4\right).$$

此时，$\big\{(1,\sigma)\big|\sigma\in\mathfrak{S}_3\big\}$ 的像是 $\mathfrak{S}_4$ 中固定 1 的那些置换，请参考上述 $\mathbb{F}_2^2$ 中元素的标号方式并注意到 $\mathbf{P}^1(\mathbb{F}_2)$ 可以完全等同于 $\mathbb{F}_2^2$ 中的非零向量。

例子 3.31 (pq 阶群的分类与实现)**.** G 是有限群，$|G|=pq$，$q<p$ 均为素数，现在确定 G 的结构。

G 只有一个 Sylow p-子群N（从而 $N\lhd G$），这因为 Sylow p-子群的个数整除 q 并且除 p 余 1 而 $p>q$；类似地，Sylow q-子群的个数为 1 或 p。

我们分两种情形讨论：

1) $q\nmid p-1$，$G\simeq\mathbb{Z}\big/p\mathbb{Z}\times\mathbb{Z}\big/q\mathbb{Z}\simeq\mathbb{Z}\big/pq\mathbb{Z}$。

   由于 Slyow q-子群的个数除 q 余 1，所以恰有一个 Sylow q-子群 K。此时，N 和 K 均为正规子群并且 $N\cap K=1$（因为 $|N\cap K|$ 整除 $|N|$ 和 $|K|$ 的最大公约数）。根据例3.27，$G=N\cdot K\simeq N\times K$。

2) $q|p-1$，G 为 $\mathbb{Z}\big/p\mathbb{Z}$ 与 $\mathbb{Z}\big/q\mathbb{Z}$ 的半直积，其中，$\mathbb{Z}\big/q\mathbb{Z}$ 对 $\mathbb{Z}\big/p\mathbb{Z}$ 的作用参考如下证明。

   选定某个 Sylow q-子群 K（未必是正规子群），考虑 K 在 N 上的共轭作用：

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

   由于 $N\simeq\mathbb{Z}\big/p\mathbb{Z}$，$K\simeq\mathbb{Z}\big/q\mathbb{Z}$，同态 φ 可被视作

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

   我们对以上同态作如下的解释：

   - $\mathbf{Aut}\left(\mathbb{Z}\big/p\mathbb{Z}\right)=\left(\mathbb{Z}\big/p\mathbb{Z}\right)^\times$：因为指定 $\mathbf{Aut}\left(\mathbb{Z}\big/p\mathbb{Z}\right)$ 某元素 w 等价于指定 $w(1)\in\left(\mathbb{Z}\big/p\mathbb{Z}\right)^\times$。
   - 给出群同态 φ 等价于指定 $\mathbf{Aut}\left(\mathbb{Z}\big/p\mathbb{Z}\right)$ 中某元素 w 并且要求 $w^q=1$（因为 $\mathbb{Z}\big/q\mathbb{Z}$ 是循环群）。

我们把 φ 形象地表示为

$$\varphi : \mathbb{Z}/q\mathbb{Z} \to \left(\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}, \cdot \right), \quad 1 \mapsto w \text{ (要求 } w^q = 1).$$

由于 $\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}$ 为 $p-1$ 阶循环群，所以 $\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}$ 中满足 $w^q = 1$ 的 w 恰好有 q 个并且构成 q 阶循环子群。进一步，该子群除 1 外任一元素均为生成元。另外，如果 $w = \varphi(1) \neq 1$，通过选取 $\mathbb{Z}/q\mathbb{Z}$ 的生成元（即指定 $K \simeq \mathbb{Z}/q\mathbb{Z}$ 的同构方式），可以保证 $\varphi(1) = w$ 取该子群的任意生成元。

我们进而研究如下两种情形：

- $\varphi(1) = 1$。从而，K 在 N 上的共轭作用平凡，所以，

$$G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

- $\varphi(1) = w \neq 1$。此时，$G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/q\mathbb{Z}$ 并且 G 不是交换群。进一步，这个半直积在群同构的意义下不依赖于 $\varphi(1) = w$ 的选取：

  令 $A = \mathbb{Z}/p\mathbb{Z}$，$B = \mathbb{Z}/q\mathbb{Z}$，$\Sigma = \mathbf{Aut}(A)$，它们是循环群。我们用乘号标记 A, B 和 Σ 中的乘法并指定相应的生成元为 $a \in A$，$b \in B$ 和 $\sigma \in \Sigma$，那么，

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

  由于 B 的阶为 q，b 在任一从 B 到 Σ 的同态下的像要满足 $\sigma_0^q = 1$。我们**指定**群同态：

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

  这个同态给出了半直积 $\mathbb{Z}/p\mathbb{Z} \rtimes_{\varphi_0} \mathbb{Z}/q\mathbb{Z}$。

  现考虑另一非平凡的群同态：

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

  由于 $\sigma_1^q = 1$，存在 $1 \leqslant k \leqslant q-1$，使得 $\sigma_1 = \sigma^{k\frac{p-1}{q}}$；由于 $(k, q) = 1$ 互素，存在 $1 \leqslant m \leqslant q-1$，使得 $k \cdot m \equiv 1 \mod p$。从而，

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

  令 $b' = b^m$，B 和 φ_1 可被重新写成

$$B = \{1, b', b'^2, \cdots, b'^{p-1}\}, \quad \varphi_1 : B \longrightarrow \Sigma, \quad b' \mapsto \sigma_0.$$

  它的形式与 φ_0 的一致。据此可见，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。

注记 3.22. 当 $q|p-1$ 时，考虑 1 维仿射变换群 $\mathbf{Aff}_1(\mathbb{F}_p)$ 的子群

$$\mathbf{Aff}_1(\mathbb{F}_p; q) = \left\{ x \mapsto ax + b \middle| a \in \mathbb{F}_p^{\times}, a^q = 1; b \in \mathbb{F}_p \right\}.$$

那么，$\mathbf{Aff}_1(\mathbb{F}_p; q)$ 恰有 pq 个元素并且非交换。$\mathbf{Aff}_1(\mathbb{F}_p; q)$ 是上述唯一的 pq 阶非交换群在几何上的实现并给出该群在维仿射直线 $\mathbb{F}_p$ 的作用。

综上所述，我们可以分类 pq 阶的群 G：

$$G \simeq \begin{cases} \mathbb{Z}/pq\mathbb{Z}, & q \nmid p-1; \\ \mathbb{Z}/pq\mathbb{Z} \text{ 或 } \mathbf{Aff}_1(\mathbb{F}_p; q), & q \mid p-1. \end{cases}$$

3.5 有限生成交换群的分类

我们用 $+$ 表示交换群 A 中的乘法。若有有限个 $x_1,\cdots,x_n\in A$，使得 $A=\langle x_1,\cdots,x_n\rangle$，则称 $(A,+)$ 是**有限生成的交换群**。这些元素 $\{x_i\}_{i\leqslant n}$ 被称作是 A 的一组生成元。

例子 3.32. $\mathbb{Z}$ 和 $\mathbb{Z}/n\mathbb{Z}$ 是循环群，它们均由一个元素生成，从而是有限生成的交换群。我们将证明一些 $\mathbb{Z}$ 与 $\mathbb{Z}/n\mathbb{Z}$ 的乘积给出所有的有限生成交换群。

例子 3.33. 有限交换群是有限生成的交换群。

例子 3.34. 有限个有限生成交换群之积是有限生成的交换群。特别地，$\mathbb{Z}^r=\underbrace{\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}}_{r\text{ 个}}$ 是有限生成的交换群。

注记 3.23. 有限生成的交换群的商群是有限生成的。

实际上，令 $B<A$ 为子群，那么，陪集 $x_1B,\cdots,x_nB$ 生成了 A/B。

注记 3.24. A 是交换群，则 A 是有限生成的当且仅当存在非负整数 n 以及满同态 $\mathbb{Z}^n\to A$。

由于通过满同态 $\mathbb{Z}^n\to A$ 可以把 A 视作是 $\mathbb{Z}^n$ 的商群，所以，A 是有限生成的饭；反之，若 A 由 $x_1,\cdots,x_n$ 生成，则可定义满的群同态

$$\mathbb{Z}^n\longrightarrow A,\quad(\lambda_1,\cdots,\lambda_n)\mapsto\sum_{i=1}^n\lambda_ix_i.$$

注记 3.25. 给定交换群的正合列，

$$0\to B\xrightarrow{\iota}A\xrightarrow{\pi}C\to 0.$$

若 B 和 C 均为有限生成的交换群，A 亦然。特别地，对于交换群 A，如果其子群 B 与商群 A/B 均为有限生成的，则 A 也是有限生成的。

实际上，令 $\{b_1,\cdots,b_k\}$ 和 $\{c_1,\cdots,c_l\}$ 分别是 B 和 C 的生成元，对 $i\leqslant l$，任选 $a_i\in\pi^{-1}(c_i)\subset A$。那么，$a_1,\cdots,a_l,\iota(b_1),\cdots,\iota(b_k)$ 生成 A。实际上，对任意的 $a\in A$，存在 $\lambda_1,\cdots,\lambda_l\in\mathbb{Z}$，使得

$$\pi(x)=\sum_{i=1}^l\lambda_ic_i\quad\Leftrightarrow\quad\pi\left(x-\sum_{i=1}^l\lambda_ia_i\right)=0.$$

从而，$x-\sum_{i=1}^l\lambda_ia_i\in\mathrm{Ker}(\pi)=\mathrm{Im}(\iota)$。从而，存在 $\lambda_1',\cdots,\lambda_l'\in\mathbb{Z}$，使得

$$x-\sum_{i=1}^l\lambda_ia_i=\sum_{j=1}^k\lambda_j'\iota(b_j)\quad\Leftrightarrow\quad x=\sum_{i=1}^l\lambda_ia_i+\sum_{j=1}^k\lambda_j'\iota(b_j).$$

注记 3.26. 有限生成的交换群的子群是有限生成的。

直接用定义证明这个命题需要对 A 的生成元个数 n 进行归纳。若 $n=1$，则 A 为循环群，其子群均为循环群，命题显然成立。假设命题对 $n=k$ 成立。现在考虑 $A=\langle x_1,\cdots,x_k,x_{k+1}\rangle$ 以及子群 $A'=\langle x_1,\cdots,x_k,x_{k+1}\rangle$ 和任意一个子群 $B<A$。

由于 $B\cap A'\subset\mathrm{Ker}(B\hookrightarrow A\to A/A')$，所以，$B/B\cap A'$ 可以被视作是 A/A' 的子群。由于 A/A' 可以由一个元素生成，从而，$B/B\cap A'$ 可由一个元素生成。我们于是得到如下正合列的交换图：

$$\begin{array}{ccccccccc}
1 & \longrightarrow & A' & \xrightarrow{\subset} & A & \xrightarrow{\pi} & A/A' & \longrightarrow & 1\\
 & & \uparrow{\scriptstyle\subset} & & \uparrow{\scriptstyle\subset} & & \uparrow{\scriptstyle\subset} & & \\
1 & \longrightarrow & A'\cap B & \xrightarrow{\subset} & B & \xrightarrow{\pi} & B/B\cap A' & \longrightarrow & 1
\end{array}$$

归纳假设表明 $A' \cap B$ 是有限生成的。根据第二行的正合列，B 是有限生成的。

以上证明表明，B 的生成元个数不超过 A 的生成元个数。特别地，如果有单同态

$$\varphi : \mathbb{Z}^m \longrightarrow \mathbb{Z}^n,$$

则 $m = n$。

注记 3.27. 若有满的群同态 $\psi : \mathbb{Z}^m \twoheadrightarrow \mathbb{Z}^n$，则 $m \geqslant n$。

我们用所谓 mod p 的技巧来证明此命题。考虑自然的同态

$$\bmod p : \mathbb{Z}^n \longrightarrow \left(\mathbb{Z}/p\mathbb{Z}\right)^n, \quad (k_1, \cdots, k_n) \mapsto (k_1 \bmod p, \cdots, k_n \bmod p).$$

很明显，$p\mathbb{Z}^n = \mathrm{Ker}(\bmod p)$，所以，$\mathbb{Z}^n/p\mathbb{Z}^n \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^n$。现在考虑如下交换图：

$$\begin{array}{ccc} \mathbb{Z}^m & \xrightarrow{\quad\psi\quad} & \mathbb{Z}^n \\ \downarrow{\scriptstyle \bmod p} & & \downarrow{\scriptstyle \bmod p} \\ \left(\mathbb{Z}/p\mathbb{Z}\right)^m = \mathbb{Z}^m/p\mathbb{Z}^m & \xrightarrow{\overline{\psi}} & \left(\mathbb{Z}/p\mathbb{Z}\right)^n \end{array}$$

由于上图右边的 mod p 映射是满射，所以，$\overline{\psi} : \left(\mathbb{Z}/p\mathbb{Z}\right)^m \to \left(\mathbb{Z}/p\mathbb{Z}\right)^n$ 是满射。注意到，这是 $\mathbb{F}_p$-线性空间之间的线性映射，根据维数的关系，就有 $m \geqslant n$。

例子 3.35 (最重要的例子：格点子群)**.** V 是 n 维 $\mathbb{R}$-线性空间，其中 $n \geqslant 1$。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 $O \subset V$，使得 $G \cap O = \{g\}$。根据定义，$G < V$ 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。

任选 V 的基 $\mathfrak{e} = (e_1, \cdots, e_n)$，定义 $\mathfrak{e}$ 的格点集为

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

这是 V 的离散子群。

如果只考虑 $\mathfrak{e}$ 中的部分元所生成的格点，比如对 $m < n$，考虑 $\{e_1, \cdots, e_m\}$ 所生成的

$$\bigoplus_{i=1}^{m} \mathbb{Z}e_i = \{ \sum_{i=1}^{m} k_i z_i | k_i \in \mathbb{Z} \}.$$

这也是 V 的离散子群。

上述格点集给出了 V 的所有的离散子群：

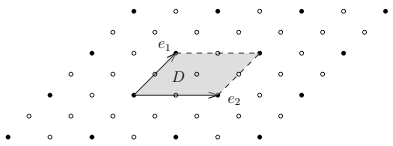
定理 33. *V 是 n 维 $\mathbb{R}$-线性空间，$G < V$ 是离散子群并且 $\mathrm{span}_{\mathbb{R}}(G) = V$。那么，存在 V 基的 $\mathfrak{e}' = (e'_1, \cdots, e'_n)$，使得 $G = \Gamma_{\mathfrak{e}'}$。*

证明： 对维数 n 归纳。

$n = 1$ 时，不妨设 $e_1 \in G$ 并且 $e_1 > 0$。由于 G 是离散子群，所以 $G \cap [0, e_1]$ 是有限集。特别地，$G \cap (0, e_1]$ 是非空的有限集。令 $e'_1 = \min G \cap (0, e_1]$。用 e_1 对 e'_1 进行带余除法，则存在正整数 l 和 $r \in [0, e'_1)$，使得 $e_1 = l \cdot e'_1 + r$。由于 G 是群，所以 $r \in G$。根据 e'_1 的最小性，$r = 0$，这表明 $e_1 = l \cdot e'_1 \in \mathbb{Z}$。类似地，每个 $g \in G$ 均为 e'_1 的倍数，从而 $G = \mathbb{Z} \cdot e'_1$。

假设对小于 n 的所有维数命题成立。选取 $e_1, \cdots, e_n \in G$ 作为 V 的一组基并考虑如下的基本区域

$$D = \{\lambda_1 e_1 + \cdots + \lambda_n e_n | \lambda_1, \cdots, \lambda_n \in [0, 1)\}.$$



对任意 $v \in V$，仿照以上的带余除法，它唯一地表达为 $\Gamma_{\mathfrak{e}}$ 与 D 的元素之和：

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

其中，$\lfloor x \rfloor$ 为不超过 x 的最大整数，$\{x\} = x - \lfloor x \rfloor$。所以，

$$G = \Gamma_{\mathfrak{e}} + G \cap D.$$

根据 G 为离散子群，$G \cap D \subset G \cap \overline{D}$ 是有限集。定义线性映射

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

那么，π_1 为满射并且 $\mathrm{Ker}(\pi_1) = V' = \mathrm{span}(e_2, \cdots, e_n)$。此时，$\pi_1(G) < \mathbb{R}$ 是子群。我们断言 $\pi_1(G)$ 是 $\mathbb{R}$ 的离散子群。根据 $G = \Gamma_{\mathfrak{e}} + G \cap D$，我们有

$$\pi_1(G) = \pi(\Gamma_{\mathfrak{e}}) + \pi_1(G \cap D) = \langle \pi_1(e_1) \rangle + \pi_1(G \cap D).$$

由于 $\pi_1(G \cap D)$ 是有限集，所以 $\pi_1(G)$ 在 $\mathbb{R}$ 中和任何紧集的交有限。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，$\langle e_1' \rangle \cap \big(G \cap V'\big) = 0$ 并且 $\langle e_1' \rangle + \big(G \cap V'\big) = G$。这表明，$G \simeq \big(G \cap V'\big) \times \mathbb{Z} e_1$。对 $\big(G \cap V'\big)$ 用归纳假设即可。 □

定理 34 (有限生成交换群的结构)**.** *对每个有限生成的交换群 A，存在唯一一组整数 $r \geqslant 0, d_1, \cdots, d_s \geqslant 2$，使得 $d_s \mid d_{s-1}, d_{s-1} \mid d_{s-2}, \cdots, d_2 \mid d_1$ 并且*

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

*我们称 r 为 A 的***秩***，称 $(d_1, \cdots, d_s)$ 为 A 的***不变因子***。*

引理 35. *$\{x_1, \cdots, x_n\}$ 是有限生成的交换群 A 的一组生成元，$k_1, \cdots, k_n \in \mathbb{Z}$ 且其最大公约数为 1。那么，存在 $y_2, \cdots, y_n \in A$，使得 $\{k_1 x_1 + \cdots + k_n x_n, y_2, \cdots, y_n\}$ 也是 A 的一组生成元。*

证明: 不妨假设 $|k_1| \geqslant |k_2| \geqslant \cdots \geqslant |k_n|\}$。通过调整正负号，还可以假设 $k_1 > 0$。

我们对 $k = \sum_{i=1}^{n} |k_i|$ 进行归纳，具体的归纳假设如下：对任意生成元 $\{x_1', \cdots, x_n'\}$ 和任意 $k_1', \cdots, k_n' \in \mathbb{Z}$，若 $k_1', \cdots, k_n'$ 的最大公约数为 1 且 $\sum_{i=1}^{n} |k_i'| < k$，就可以把 $k_1' x_1' + \cdots + k_n' x_n'$ 扩充为 A 的总数不超过 n 个的一组生成元。

若 $k = 1$，则 $k_1 x_1 + \cdots + k_n x_n = \pm x_1$，此时选取 $y_2 = x_2, \cdots, y_n = x_n$ 即可。

现在证明 k 的情形。此时，$k_1 \geqslant |k_2|$，根据 k_2 的符号 ε，我们可以做如下的调整：

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

此时，$x_1, x_2+\varepsilon x_1, x_3, \cdots, x_n$ 仍然是 A 的总数不超过 n 个的一组生成元。注意到 $k_2 \neq 0$（否则 $k_2 = \cdots = k_n = 0$，根据 $k_1, \cdots, k_n$ 的最大公约数为 1，就有 $k_1 = 1$，所以这是 $k = 1$ 的情况），从而

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

根据归纳假设，命题得证。 □

引理 36. 有限生成的交换群 A 具有**仿基**，即存在生成元集 $\{x_1, \cdots, x_n\} \subset A$，使得

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

证明：选取 A 生成元集 $\{x_1, \cdots, x_n\}$ 使得生成元个数 n 是最小的并在此前提下要求 $\mathrm{ord}(x_1)$ 是最小的（可以是 ∞）。考虑 A 的子群 $A_0 = \langle x_1 \rangle$ 和 $A_1 = \langle x_2, \cdots, x_n \rangle$ 以及群同态：

$$\varphi : A_0 \times A_1 \to A,\ \ (a_0, a_1) \mapsto a_0 \cdot a_1.$$

特别地，我们有 $\varphi\big((x_1, 1)\big) \mapsto x_1$，$\varphi\big((1, x_i)\big) = x_i$，其中，$i \geqslant 2$。从而，$\mathrm{Im}(\varphi)$ 包含 A 的生成元集，从而为满射。

现在证明 φ 是单射：假设 $\varphi\left((m_1 x_1, \sum_{i=2}^{s} m_i x_i\right) = 0$，其中，不妨假设 $0 \leqslant m_1 < \mathrm{ord}(x_1)$。我们的目标是证明 $m_1 x_1 = 0$（从而 $\sum_{i=2}^{s} m_i x_i = 0$），所以不妨设 $m_1 \geqslant 1$。考察这组数的最大公约数 $d = (m_1, \cdots, m_n)$，则

$$d\big(k_1 x_1 + k_2 x_2 + \cdots + k_n x_n\big) = 0,\ \ k_i = \frac{m_i}{d},\ (k_1, \cdots, k_n) = 1.$$

根据上一引理，可以选取 $y_1 = k_1 x_1 + \sum_{i=2}^{s} k_i x_i$ 和 $y_2, \cdots, y_n$ 作为生成元的集合，但是

$$\mathrm{ord}(y_1) \leqslant d \leqslant m_1 < \mathrm{ord}(x_1).$$

这与 $\mathrm{ord}(x_1)$ 的最小性矛盾。

以上推理证明了 $\langle x_1 \rangle \times A_1 \xrightarrow{\simeq} A$ 并且 A_1 的生成元数目不超过 $n-1$。特别地，A_1 的生成元数目严格小于 A_0 的最少生成元。我们再对 A_1 进行以上的分解并将此程继续下去就可以得到一组拟基。 □

注记 3.28. 以上证明表明，A 可以写成一些循环群 A_i 的乘积。特别地，A 与 $\mathbb{Z}^r \times \prod_{i=r+1}^{n} \mathbb{Z}/m_i\mathbb{Z}$ 形式的群同构。

注记 3.29 (有限生成交换群结构定理的存在性部分的证明)**.** 根据上述仿基的命题，可假设 $A \simeq \mathbb{Z}^r \times \prod_{i=r+1}^{n} \mathbb{Z}/m_i\mathbb{Z}$ 的。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[16]

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

从而，

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

[16]参考习题2.7.1

现在将上面的乘积重新组合。首先定义 d_1：对每个 p，令 $\beta(p)=\max\{\alpha_i(p)\}_i$，则令 $d_1=\prod_p \beta(p)$ 并将这一个 $\beta(p)$ 从 $\{\alpha_i(p)\}_i$ 中删除。其次定义 d_2，令 $\gamma(p)=\max\{\alpha_i(p)\}_i$ 以及 $d_2=\prod_p \gamma(p)$ 并将这一个 $\beta(p)$ 从 $\{\alpha_i(p)\}_i$ 中删除。以此类推，我们自然有 $d_2 \mid d_1, d_3 \mid d_2 \cdots$。从而，

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

这就完成了定理中存在性的证明。

为了证明唯一性，只要说明 $r, d_1, \cdots, d_s$ 可以完全由 A 本身计算即可。先证明关于循环群的一个性质：

引理 37. *A 是循环群，p 是素数，那么，*

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

证明： 设 x 为 A 的生成元，则 $p^{k-1}x$ 是 $p^{k-1}A$ 的生成元并且 $p \cdot p^{k-1}x \in p^kA$。从而，

$$p^{k-1}A/p^kA \simeq \mathbb{Z}/p\mathbb{Z} \text{ 或 } 0.$$

引理对 $A \simeq \mathbb{Z}$ 是显然的，以下假设 A 是有限循环群，即 $A \simeq \mathbb{Z}/n\mathbb{Z}$，并且 $n=p^d \cdot m$，其中，$(m,p)=1$。那么，$A \simeq \mathbb{Z}/p^d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} = A' \times \mathbb{Z}/m\mathbb{Z}$，其中，$A'=\mathbb{Z}/p^d\mathbb{Z}$。由于 $(m,p)=1$，所以对任意的 l，群同态

$$\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z},\ \ \overline{a} \mapsto p^l\overline{a},$$

是同构。取 $l=k-1, l$，我们有 $p^{k-1}\cdot \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/m\mathbb{Z}$，$p^k \cdot \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/m\mathbb{Z}$。从而，

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

此时，我们可以专注于 $p^{k-1}A'/p^kA'$，其中，$A'=\mathbb{Z}/p^d\mathbb{Z}$：

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

综合上述，我们就完成了引理的证明。 □

有限生成交换群结构定理的唯一性部分的证明. 任给存在性部分的一个分解 $A \simeq \mathbb{Z}^r \times \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$，我们有

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

上述群的阶为 $p^{r+s(k)}$，其中，$s(k)$ 为 $d_1, \cdots, d_s$ 中能被 p^k 整除的数的个数。根据 $d_1 \mid d_2 \mid \cdots \mid d_2$，这些数恰好是前面的 $d_1, \cdots, d_{s(k)}$。这样，当 k 取遍 $\{1,2,\cdots,\}$ 时，我们可以通过 $s(k)$ 的值决定 $d_1, \cdots, d_s$ 所含 p 因子的幂，从而决定 $d_1, \cdots, d_s$。通过选取 p 与所有 $d_1, \cdots, d_s$ 互素，我们知道 $A/pA \simeq \big(\mathbb{Z}/p\mathbb{Z}\big)^r$ 决定了 r。所以，秩 r 和不变因子 $d_1, \cdots, d_s$ 完全由群 A 本身决定。这就给出了唯一性。 □

例子 3.36. 我们研究 $A=\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ 的分解。根据分类定理，我们应该把它写成：

$$A \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

此时，根据上述构造过程，$d_1=2^2\times 3$，$d_2=2$。从而，

$$A \simeq \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

3.6 习题

3.6.1 对称群 $\mathfrak{S}_n$ 中的计算

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

1. 假设 $S = \big\{(i,j)\big\}$ 是一些对换（2-循环）的集合并且 S 生成 $\mathfrak{S}_n$，那么，$|S|$ 的最小值是多少?
2. 假设 $|i_0 - j_0|$ 与 n 互素。证明，$S_4 = \big\{(i_0, j_0), (1, 2, \cdots, n)\big\}$ 生成 $\mathfrak{S}_n$。
3. 假设 $n \geqslant 5$。证明，$\mathfrak{A}_n$ 中的所有 3-循环是（在 $\mathfrak{A}_n$ 中）相互共轭的。
4. 证明，$\mathfrak{A}_5$ 可以被双对换 $\{(i,j)(k,l) | 1 \leqslant i,j,k,l \leqslant 5$且两两不同$\}$ 生成。
5. （$\mathfrak{A}_5$ 的自同构群）令 $G = \mathfrak{A}_5$。
   a) 假设 $x = (12)(34) \in G$，$y \in G$ 的是一个 3 阶元。证明，xy 的阶为 5 当且仅当 y 的两个不动点一个在 $\{1,2\}$ 中并且另一个在 $\{3,4\}$ 中。
   b) 令 $X = \{(u,v) \in G \times G \big| u, v, uv$ 的阶分别为 $2,3,5\}$，证明，$|X| = 120$。
   c) $\mathbf{Aut}(G)$ 作用在 X 上，证明，这个作用是自由的。据此，$|\mathbf{Aut}(G)| \leqslant 120$。由于 $\mathbf{Aut}(G)$ 包含 $\mathfrak{S}_5$，从而 $\mathbf{Aut}(G) = \mathfrak{S}_5$。
6. （$\mathfrak{A}_4$ 的自同构群）用 $(2,3,3)$（元素的阶）替换 $(2,3,5)$，试用类似的方法证明 $\mathbf{Aut}(\mathfrak{A}_4) = \mathfrak{S}_4$。
7. （$\mathfrak{S}_4$ 的自同构群）用 $(2,3,4)$（元素的阶）替换 $(2,3,5)$，试用类似的方法证明 $\mathbf{Aut}(\mathfrak{S}_4) = \mathfrak{S}_4$。
8. 试用上面关于 $\mathfrak{A}_4$ 的自同构群的结论直接证明上一结果。

3.6.2 交错群 $\mathfrak{A}_n$（$n \geqslant 5$）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。

1. 给出 $\mathfrak{A}_3$ 和 $\mathfrak{A}_4$ 的正规子群。
2. 我们按照以下步骤证明 $\mathfrak{A}_5$ 是单群：
   - 假设 $N \lhd \mathfrak{A}_5$ 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。
   - 假设 $N \lhd \mathfrak{A}_5$ 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。
   - 假设 $N \lhd \mathfrak{A}_5$ 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。
3. 我们还可以按照以下步骤证明 $\mathfrak{A}_5$ 是单群
   - 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。
   - 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。
   - 证明，$\mathfrak{A}_5$ 是单群。
4. 以下假设 $n \geqslant 6$ 并且 $\mathfrak{A}_{n-1}$ 是单群。假设 $N \lhd \mathfrak{A}_n$ 是正规子群并且 $N \neq 1$，$N \neq \mathfrak{A}_n$。

- 如果存在 $\sigma \in N - \{1\}$ 使得 $\sigma(n) = n$，证明，$N = \mathfrak{A}_n$。
- 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，$\tau = (i, j)(n, \sigma(n))$。
- 同上，证明，$\sigma^2 = 1$ 并且 $\sigma : \{i, j\} \to \{i, j\}$。（提示：考虑 $\sigma^{-1}\tau\sigma\tau^{-1}$）
- 证明，$\sigma = \big(n, \sigma(n)\big)$ 从而得到矛盾。据此，$\mathfrak{A}_n$ 是单群。

5. 假设 $n \geqslant 5$，$G \lhd \mathfrak{S}_n$ 为正规子群，证明，如果 $G \neq 1$，$G \neq \mathfrak{S}_n$，那么，$G = \mathfrak{A}_n$。

6. 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 $N \lhd \mathfrak{A}_4$。$\mathfrak{S}_4 \big/ N$ 是哪一个群?

7. 假设 $n \geqslant 5$，$H < \mathfrak{S}_n$ 为子群，$d = [\mathfrak{S}_n : H]$。证明，存在群同态 $\varphi : \mathfrak{S}_n \to \mathfrak{S}_d$，使得 $\mathrm{Ker}(\varphi) < H$。据此证明，如果 $H \neq \mathfrak{A}_n, \mathfrak{S}_n$，那么，$d \geqslant n$。

8. 证明，对于 $n \geqslant 2$，存在单的群同态 $\mathfrak{S}_n \to \mathfrak{A}_{n+2}$（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 $\mathfrak{S}_n \to \mathfrak{A}_{n+1}$。

3.6.3 $\mathbf{PSL}(2; \mathbb{F}_2) \simeq \mathfrak{S}_3, \mathbf{PSL}(2; \mathbb{F}_3) \simeq \mathfrak{A}_4$

循环群只有在其阶为素数时为单群。

1. 证明，$\mathbf{GL}(2; \mathbb{F}_2) \simeq \mathbf{PGL}(2; \mathbb{F}_2) \simeq \mathbf{SL}(2; \mathbb{F}_2) \simeq \mathbf{PSL}(2; \mathbb{F}_2)$。

2. $\mathbf{GL}(2; \mathbb{F}_2)$ 在 $\mathbb{P}^1(\mathbb{F}_2)$ 的自然的作用给出同态

$$\varphi : \mathbf{GL}(2; \mathbb{F}_2) \longrightarrow \mathfrak{S}_{\mathbb{P}^1(\mathbb{F}_2)} \simeq \mathfrak{S}_3,$$

其中，后一个同构由以下对应给出 $[1:0] \to 1, [1:1] \to 1, [0:1] \to 3$。证明，$\varphi$ 是群同构。

3. $\mathbf{GL}(2; \mathbb{F}_3)$ 在 $\mathbb{P}^1(\mathbb{F}_3)$ 上自然的作用给出同态

$$\varphi : \mathbf{GL}(2; \mathbb{F}_3) \longrightarrow \mathfrak{S}_{\mathbb{P}^1(\mathbb{F}_3)} \simeq \mathfrak{S}_4,$$

其中，后一个同构由以下对应给出 $[1:0] \to 1, [1:1] \to 2, [1:2] \to 3, [0:1] \to 4$。计算 $\mathrm{Ker}(\varphi)$ 并证明 φ 诱导出同构

$$\overline{\varphi} : \mathbf{PGL}(2; \mathbb{F}_3) \xrightarrow{\simeq} \mathfrak{S}_4.$$

4. 证明，对 $n \geqslant 2$，$\mathfrak{S}_n$ 的指标为 2 的子群必为 $\mathfrak{A}_n$。据此，利用 $\mathbf{PSL}(2; \mathbb{F}_3)$ 在 $\mathbb{P}^1(\mathbb{F}_3)$ 的上自然作用证明：

$$\mathbf{PSL}(2; \mathbb{F}_3) \simeq \mathfrak{A}_4.$$

5. 证明，

$$\mathbf{SL}(2; \mathbb{F}_4) \simeq \mathbf{PSL}(2; \mathbb{F}_4) \simeq \mathfrak{A}_5.$$

（提醒：对任意的 $x \in \mathbb{F}_4$，$2x = 0$。特别地，$1 = -1$。）

6. $n \geqslant 5$，$H < \mathfrak{S}_n$ 的是指标为 n 的子群。证明，$H \simeq \mathfrak{S}_{n-1}$。据此，利用 $\mathbf{PGL}(2; \mathbb{F}_5)$ 在 $\mathbb{P}^1(\mathbb{F}_5)$ 的上自然作用证明：

$$\mathbf{PGL}(2; \mathbb{F}_5) \simeq \mathfrak{S}_5.$$

7. 一个不同构的结论。

   - 证明，$\mathbf{SL}(3;\mathbb{F}_4)$ 中恰有一个共轭类使得其元素的阶为 2。进一步，这个共轭类中的元素均恰为剪切映射。
   - 证明，自然的映射 $\mathbf{SL}(3;\mathbb{F}_4) \to \mathbf{PSL}(3;\mathbb{F}_4)$ 给出了这两个群中阶为 2 的元素的一一对应。
   - 证明，$\mathfrak{A}_8$ 与 $\mathbf{PSL}(3;\mathbb{F}_4)$ 是具有 20160 个元素但是不同构的单群。

3.6.4 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 $H \lhd G$ 并且 $H \neq 1, H \neq G$。

1. 证明，$s_2 \in \{1,3,5,15\}$，$s_3 \in \{1,4,10\}$，$s_5 = 6$。
2. 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。
3. 假设 $|H| \leqslant 4$。证明，G/H 只有一个 Sylow 5-子群；进一步证明存在 $H' \lhd G$，$H' \neq G$ 并且 $|H'|$ 是 5 的倍数。据此推出矛盾。
4. 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。
5. $H < G$ 是子群并且 $H \neq G$。证明，$[G:H] \geqslant 5$。进一步证明，如果 $[G:H] = 5$，那么，$G \simeq \mathfrak{A}_5$。
6. 证明，$s_2 \in \{5,15\}$，$s_3 = 4$，$s_5 = 6$。
7. 假设 $s_2 = 5$，证明，$G \simeq \mathfrak{A}_5$。
8. 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 $[G : \mathrm{N}_G(P \cap Q)] = 5$。
9. 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。

3.6.5 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，

1. （常用结论）证明，p^2 阶的群必然是交换群，其中，p 是素数。
2. 证明，$s_3 = 10$。
3. 证明，$s_5 = 36$。
4. 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 $C_g(G)$）
5. 据上述结论推出矛盾。

3.6.6 与 Sylow p-子群相关的补充

1. G 是有限群，$S < G$ 是一个 Sylow p-子群。证明，$[G : \mathrm{N}_G(S)] \equiv 1 \pmod{p}$。
2. G 是有限群，$S < G$ 是一个 Sylow p-子群，$H \lhd G$ 是正规子群。证明，$S \cap H$ 是 H 的 Sylow p-子群。
3. G 是有限群，$H \lhd G$ 是正规子群，$\pi : G \to {}^{G}\!/_{H}$ 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 $\pi(S) = S'$。
4. （Frattini 技巧）
   - 群 G 作用在集合 X 上，$H < G$ 是子群，那么，${}^{G\curvearrowright}X$ 诱导出 ${}^{H\curvearrowright}X$。假设 ${}^{H\curvearrowright}X$ 是传递的，证明，对任意的 $x \in X$，$G = H \cdot \mathrm{Stab}_G(x)$。
   - （Frattini）G 是群，$H \lhd G$ 是有限的正规子群，$S < H$ 是 H 的一个 Sylow p-子群。证明，$G = H \cdot \mathrm{N}_G(S)$。
5. 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，$H = \mathrm{N}_G(H)$。
6. G 是有限群，$S < G$ 是一个 Sylow p-子群。证明，$\mathrm{N}_G(S) = \mathrm{N}_G(\mathrm{N}_G(S))$。

3.6.7 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，

1. （常用结论）证明，p^2 阶的群必然是交换群，其中，p 是素数。
2. 证明，$s_3 = 10$。
3. 证明，$s_5 = 36$。
4. 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 $C_g(G)$）
5. 据上述结论推出矛盾。

3.6.8 $\mathbf{PSL}(2;\mathbb{F}_7)$ 与 $\mathbf{GL}(3;\mathbb{F}_2)$ 同构

我们记 $\mathbf{P}^1(\mathbb{F}_p)$ 为 $\mathbb{F}_p \cup \{\infty\}$，对于 $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{GL}(2;\mathbb{F}_p)$，它通过分式线性变换在 $\mathbf{P}^1(\mathbb{F}_p)$ 上作用：

$$g \cdot x = \frac{ax+b}{cx+d}.$$

这给出了单的群同态

$$\mathbf{PGL}(2;\mathbb{F}_p) \longrightarrow \mathfrak{S}_{\mathbf{P}^1(\mathbb{F}_p)} \simeq \mathfrak{S}_{p+1}.$$

从而，我们可以把 $\mathbf{PGL}(2;\mathbb{F}_p)$ 视为 $\mathfrak{S}_{p+1}$（因为 $\left|\mathbf{P}^1(\mathbb{F}_p)\right| = p+1$）中阶为 $p^3 - p$ 并且在 $\{1, 2, \cdots, p+1\}$ 上传递作用的子群。考虑群 $\mathbf{PGL}(2;\mathbb{F}_p)$ 通过分式线性变换在 $\mathbf{P}^1(\mathbb{F}_p)$ 上的作用，令 $\mathbf{Aff}_1(\mathbb{F}_p) = \mathrm{Stab}(\infty)$。容易看出，$\mathbf{Aff}_1(\mathbb{F}_p)$ 在 $\mathbb{F}_p = \mathbf{P}^1(\mathbb{F}_p) - \{\infty\}$ 上的作用是双传递的并且 $\left\langle \mathbf{Aff}_1(\mathbb{F}_p), \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle = \mathbf{PGL}(2;\mathbb{F}_p)$。

Zassenhaus 有一个有意思的结果：令 $X=\mathbf{P}^1(\mathbb{F}_p)$，$G<\mathfrak{S}_X$ 的阶为 p^3-p 并且在 X 上传递作用，那么，存在 $\sigma\in\mathfrak{S}_X$，使得 $\sigma G\sigma^{-1}=\mathbf{PGL}(2;\mathbb{F}_p)$。我们对 $p=3 \mod 4$ 的情形证明该结论，证明的想法是逐步在 G 中构造出 $\mathbf{Aff}_1(\mathbb{F}_p)$ 以及 $\begin{pmatrix}0&1\\1&0\end{pmatrix}$ 所对应的对象。

我们使用如下的约定与假设：

$$G<\mathfrak{S}_X,\ |G|=p^3-p,\ \mathbf{PGL}(2;\mathbb{F}_p)<\mathfrak{S}_X,\ \alpha(x)=x+1\in\mathbf{Aff}_1(\mathbb{F}_p),$$

并且 G 在 X 上的作用是传递的。

1. 证明，G 包含 p-循环从而存在 $\sigma\in G$，使得 $\alpha\in\sigma G\sigma^{-1}$。

   自此，假设 $\alpha\in G$。

2. 令 $G_\infty=\big\{g\in G\big|g(\infty)=\infty\big\}$。证明，$|G_\infty|=p^2-p$，$P=\langle\alpha\rangle\lhd G_\infty$ 并且对任意 $g\in G_\infty$，存在 $a\in[1,p)$，使得 $g\cdot\alpha=\alpha^a\cdot g$（$a$ 当然依赖于 g）。

3. 证明，$G_\infty=\mathbf{Aff}_1(\mathbb{F}_p)$。

4. 证明，G 在 X 上的作用是 3-传递的并且若 $g\in G$ 固定任 3 个不同的点则 $g=1$。

   以下选取 $\gamma\in G$ 使得 $\gamma(0)=\infty,\gamma(\infty)=0,\gamma(1)=1$（我们希望它对应着 $\begin{pmatrix}0&1\\1&0\end{pmatrix}$）并令

   $$\begin{cases}C=\big\{g\in G\big|g(\infty)=\infty,g(0)=0\big\},\\ C'=\mathrm{C}_{\mathfrak{S}_X}(C)=\big\{g\in G\big|gc=cg,\forall c\in C\big\}.\end{cases}$$

5. 证明，C 是阶为 $p-1$ 的循环群并由某个（$\mathfrak{S}_X$ 中的）$p-1$ 循环生成；$C'=\langle C,(0,\infty)\rangle$，其中，$(0,\infty)$ 是 $\mathfrak{S}_X$ 中的对换。

6. 证明，若 G 中有对换，则 $G=\mathfrak{S}_X$，从而 $p=2$ 或 3。

   自此，假设 $p\geqslant 5$ 并且 $(0,\infty)\notin G$。

7. 证明，$C'\cap G=C$ 并且

   $$\mathrm{Int}(\gamma):G\to G,\ g\mapsto\gamma g\gamma^{-1}$$

   是阶为 2 的自同构。

8. 证明，存在 $n\in[2,p-2]$，使得 $n^2=1 \mod p-1$ 并且对任意的 $c\in C$，$\mathrm{Int}(\gamma)(c)=c^n$；对任意的 $x\in X-\{\infty\}$，$\gamma\cdot x=x^n$，其中，x^n 是在 $X-\{\infty\}=\mathbb{F}_p$ 中的运算。

9. 证明，$n\equiv -1 \mod \frac{p-1}{2}$。（提示：$\gamma$ 至多有两个不动点）

10. 证明，如果 $p=3 \mod 4$，那么，$n+1=0 \mod p-1$ 并且 $G=\mathbf{PGL}(2;\mathbb{F}_p)$。

    至此，我们在 $p=3 \mod 4$ 的假设下证明了 Zassenhaus 的结论。

11. （应用）G 是群，p 是素数，$|G| = p^3 - p$。我们做如下假设：如果 $H \lhd G$ 并且 $|H|$ 整除 $p^2 - p$，那么 $H = 1$。

    (a) 证明，G 有 $p+1$ 个 Sylow p-子群。

    (b) 证明，G 通过共轭在 Sylow p-子群的集合上的作用是忠实的。

    (c) 证明，若 $p = 3 \mod 4$，则 $G \simeq \mathbf{PGL}(2; \mathbb{F}_p)$。

12. （$\mathbf{GL}(3; \mathbb{F}_2) \simeq \mathbf{PSL}(2; \mathbb{F}_7)$）令 $N = \mathbf{GL}(3; \mathbb{F}_2)$，则 $A \in N$ 为 3×3 的矩阵。定义 $\mathbb{Z}/2\mathbb{Z}$ 在 N 上的作用为：

$$\psi : \mathbb{Z}/2\mathbb{Z} \to \mathbf{Aut}(N), \quad 1 \mapsto \left(A \mapsto {}^tA^{-1}\right).$$

    令 $G = N \rtimes_\psi \mathbb{Z}/2\mathbb{Z}$。

    (a) 证明，不存在 $M \in \mathbf{GL}(3; \mathbb{F}_2)$，使得对任意的 $A \in \mathbf{GL}(3; \mathbb{F}_2)$，${}^tAMA = M$ 并进一步证明 G 的正规子群的指标不等于 2。

    (b) 证明，G 只有一个非平凡正规子群 $N \times \{0\} = \left\{(A, 0) \in N \rtimes_\psi \mathbb{Z}/2\mathbb{Z} \middle| A \in N\right\} \simeq N$。

    (c) 证明，$G \simeq \mathbf{PGL}(2; \mathbb{F}_7), N \simeq \mathbf{PGL}(2; \mathbb{F}_7)$。这就证明了 $\mathbf{GL}(3; \mathbb{F}_2) \simeq \mathbf{PSL}(2; \mathbb{F}_7)$。

3.6.9 最少的生成元个数

G 是群，如果存在有限个 $x_1, \cdots, x_n$，使得 $G = \langle x_1, \cdots, x_n \rangle$，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 $\min_{\text{gen}}(\{1\}) = 0$。

1. 证明，$\min_{\text{gen}}(G) = 1$ 等价于 G 是非平凡的循环群。

2. 假设 $n \geqslant 3$。证明，$\min_{\text{gen}}(\mathfrak{S}_n) = 2$。

3. p 是素数，r 是自然数，$G = \left(\mathbb{Z}/p\mathbb{Z}\right)^r = \underbrace{\mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}}_{r \text{ 个}}$。证明，$\min_{\text{gen}}(G) = r$。

   （提示：将 G 视为 $\mathbb{Z}/p\mathbb{Z}$-线性空间）

4. G 是有限生成群，假设有**满的**群同态 $\varphi : G \longrightarrow G'$。证明，$G'$ 是有限生成群并且

$$\min_{\text{gen}}(G') \leqslant \min_{\text{gen}}(G).$$

5. G 是群，$H \lhd G$ 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

$$\min_{\text{gen}}(G) \leqslant \min_{\text{gen}}\left(G/H\right) + \min_{\text{gen}}(H).$$

6. 对于群 $A = \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$，其中，$s \in \mathbb{Z}_{\geqslant 1}, d_1, \cdots, d_s \in \mathbb{Z}_{\geqslant 2}$，使得 $d_s \mid d_1, d_{s-1} \mid d_{s-2}, \cdots, d_2 \mid d_1$。证明，$\min_{\text{gen}}(A) = s$。

7. 对于群 $A = \mathbb{Z}^r = \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ 个}}$。证明，$\min_{\text{gen}}(A) = r$。据此证明，如果 $\mathbb{Z}^r \simeq \mathbb{Z}^{r'}$，那么，$r = r'$。

8. （子群生成元个数可以更多）对任意的 $n \geqslant 3$，给出如下的例子：G 是群，$H < G$ 是子群，$\min_{\text{gen}}(G) = 2$ 而 $\min_{\text{gen}}(H) = n$。

9. （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，$H=\left\{\begin{pmatrix}1&\frac{m}{2^k}\\0&1\end{pmatrix}\middle| k\in\mathbb{Z}_{\geqslant 0}, m\in\mathbb{Z}\right\}$ 是 G 的子群并且不是有限生成的。

10. （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，

$$\min_{\text{gen}}(H)\leqslant \min_{\text{gen}}(G).$$

（提示：找一个 $g\in G$，使得 $\min_{\text{gen}}\left(G/\langle g\rangle\right)<\min_{\text{gen}}(G)$）

11. $r\geqslant 1$，A 是 $\mathbb{Z}^r$ 的子群。证明，存在 $r'\leqslant r$，使得 $A\simeq\mathbb{Z}^{r'}$。

3.6.10 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。

1. 在同构意义下，写下所有阶为 2^3 的群和阶为 p^2 的群。
2. 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。
3. 给定两个非平凡的群同态 $\varphi:\mathbb{Z}/p\mathbb{Z}\longrightarrow\mathbf{GL}(2;\mathbb{F}_p)$ 和 $\varphi':\mathbb{Z}/p\mathbb{Z}\longrightarrow\mathbf{GL}(2;\mathbb{F}_p)$。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 $k=1,2,\cdots,p-1$，使得对任意的 $x\in\mathbb{Z}/p\mathbb{Z}$，有
$$\varphi'(x)=A\cdot\varphi_k(x)\cdot A^{-1}.$$
4. 在同构的意义下，可能的半直积 $\left(\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}\right)\rtimes_\psi\mathbb{Z}/p\mathbb{Z}$ 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 $\mathbb{Z}/p\mathbb{Z}$。
5. G 是群，$|G|=p^3$。假设 G 不是循环群并且存在 $g\in G$ 使得 $\operatorname{ord}(g)=p^2$。证明，$\langle g\rangle\lhd G$。
6. 证明，在同构的意义下，上一个小问题中的群恰好两个。
7. 在同构意义下，写下所有阶为 p^3 的群。

3.6.11 射影几何、Fano 平面与 $\mathbf{GL}(3;\mathbb{F}2)$

给定非空集合 Π 和 Λ，我们把 Π 中的元素 p 称作**点**，Λ 中的元素 l 称作**线**。集合 Π 和 Λ 之间**重合关系**（incidence relation）指的是乘积集合的子集 $I\subset\Pi\times\Lambda$。对任意的 $(p,l)\in\Pi\times\Lambda$，若 $(p,l)\in I$，我们就说**点** p **在线** l **上**或**线** l **过点** p。进一步，如果以下三条公理成立：

公理 1 两点确定一条线，即对任两个不同的点 $p,p'\in\Pi$，存在唯一的线 $l\in\Lambda$，使得 l 过 p 且过 p'；

公理 2 两线交于一个点，即对任两条不同的线 $l,l'\in\Pi$，存在唯一的点 $p\in\Lambda$，使得 l 和 l' 均过 p；

公理 3 存在四个不同的点 $p_1,p_2,p_3,p_4\in\Pi$，任意的 $l\in\Lambda$ 不能同时过其中的三点。

我们就称 $\big(\Pi,\Lambda;I\big)$ 或 Π 为**射影平面**。在公理 2 的条件下，我们还称 p 是 l 与 l' 的**交点**。

$\big(\Pi,\Lambda;I\big)$ 和 $\big(\Pi',\Lambda';I'\big)$ 为射影平面，如果存在双射

$$\varphi:\Pi\to\Pi',\quad \psi:\Lambda\to\Lambda',$$

使得 $(p,l)\in I$ 当且仅当 $(\varphi(p),\psi(l))\in I'$，就称 (φ,ψ) 是 $\big(\Pi,\Lambda;I\big)$ 与 $\big(\Pi',\Lambda';I'\big)$ 之间的**同构**。令 $\mathbf{Aut}\big(\Pi,\Lambda;I\big)$ 为 $\big(\Pi,\Lambda;I\big)$ 到自身同构的集合，它在映射的复合下是群。

1. **第一部分，射影平面与 Fano 平面**

   K 是域，V 是 3 维 K-线性空间，V^* 为其对偶。令 $\Pi=\mathbf{P}(V),\Lambda=\mathbf{P}(V^*)$。我们要把 $\mathbf{P}(V)$ 中的线定义为 V 中的 2 维线性子空间：对任意的 $p\in\Pi$，不妨选取 $p\in V$ 作为其代表；对任意的 $l\in\Lambda$，不妨选取 $l\in V^*$ 作为其代表，我们定义

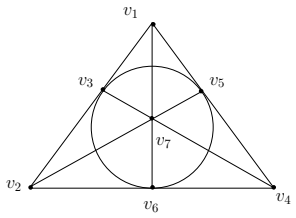
   $$I=\big\{(p,l)\big|l(p)=0\big\}.$$

   证明，以上是良好定义的并且 $\big(\Pi,\Lambda;I\big)$ 为射影平面。

2. $\big(\Pi,\Lambda;I\big)$ 为射影平面。证明，存在四条不同的线 $l_1,l_2,l_3,l_4\in\Lambda$，任意的 $p\in\Pi$ 不能同时在其中的三条线上。据此构造重合关系 $I^*\subset\Lambda\times\Pi$，使得 $\big(\Lambda,\Pi;I^*\big)$ 为射影平面。

3. （元素个数最小的射影平面的构造）令 $\Pi=\mathbf{P}^2(\mathbb{F}_2)$，则 $|\Pi|=7$ 每个点均对应 $(\mathbb{F}_2)^3$ 中非零向量

   $$v_1=(0,0,1),v_2=(0,1,0),v_3=(0,1,1),v_4=(1,0,0),v_5=(1,0,1),v_6=(1,1,0),v_7=(1,1,1).$$

   上图中有 6 条直线段和一个圆，每个这样的图形上有三个点，它们对应着 Λ。这个射影平面被称作是**Fano 平面**。

   (a) $\big(\Pi,\Lambda;I\big)$ 为射影平面，$p_1,p_2,p_3,p_4\in\Pi$ 满足公理 3。令 l_{ij} 为过 p_i 与 p_j 的直线，其中，$1\leqslant i,j\leqslant 4$；令 p_5,p_6,p_7 分别为 l_{12} 与 l_{34}、l_{13} 与 l_{24} 以及 l_{14} 与 l_{23} 的交点。证明，$\{p_1,\cdots,p_7\}$ 这 7 个点两两不同。

   (b) $\big(\Pi,\Lambda;I\big)$ 为射影平面并且 $|\Pi|=7$。假设 $p_1,p_2,p_3,p_4\in\Pi$ 满足公理 3，以上已经构造了 6 条线 l_{ij} 并且 $\{p_1,\cdots,p_7\}=\Lambda$。令 l_∞ 为过 p_5,p_6 的线，证明，l_∞ 过 p_7。进一步证明，$\Lambda=\{l_{ij},l_\infty,1\leqslant i,j\leqslant 4\}$ 恰有 7 条线并且每条线恰好过 3 个点。

   (c) 证明，以下映射

   $$\begin{cases} p_1\mapsto(1,1,1),\quad p_2\mapsto(1,0,1),\quad p_3\mapsto(1,1,0),\\ p_4\mapsto(1,0,0),\quad p_5\mapsto(0,1,0),\quad p_6\mapsto(0,0,1),\quad p_7\mapsto(0,0,1).\end{cases}$$

   可以给出 $\big(\Pi,\Lambda;I\big)$ 到 Fano 平面的同构。

   以上证明了 Fano 平面是元素个数最小的唯一的（在同构意义下）射影平面。

4. **第二部分，群 $\mathbf{GL}(3;\mathbb{F}_2)$ 中 Fano 平面的结构**

   $\mathbf{GL}(3;\mathbb{F}_2)$ 在 Fano 平面的点集 Π 上有自然作用；$\mathbf{GL}(3;\mathbb{F}_2)$ 在 Fano 平面的线集 Λ 上也有自然作用（把直线映射称直线）。所以，$\mathbf{GL}(3;\mathbb{F}_2)$ 可以自然地作用在 $\Pi\times\Lambda$ 上。这个作用有几个轨道?

5. 在 $\mathbf{GL}(3;\mathbb{F}_2)$ 中的**标准 Borel 子群**B 是对角线线上均为 1 的上三角矩阵的集合，包含 B 的子群被称作是**标准抛物子群**，比如下述的 $P,Q<\mathbf{GL}(3;\mathbb{F}_2)$：

$$B=\left\{\begin{pmatrix}1&*&*\\0&1&*\\0&0&1\end{pmatrix}\right\},\quad P=\left\{\begin{pmatrix}*&*&*\\*&*&*\\0&0&1\end{pmatrix}\right\},\quad Q=\left\{\begin{pmatrix}1&*&*\\0&*&*\\0&*&*\end{pmatrix}\right\}.$$

   我们注意到 $P\cap Q=B$，$Q=\mathrm{Stab}\big((1,0,0)\big)$，其中，$p=(1,0,0)\in\Pi$。试找出直线 $l\in\Lambda$，使得 $P=\mathrm{Stab}(l)$。证明，与 P 和 Q 共轭的矩阵恰好都是 7 个并且 P 与 Q 不共轭。

6. 假设 $P'<\mathbf{GL}(3;\mathbb{F}_2)$ 与 P 共轭，$Q'<\mathbf{GL}(3;\mathbb{F}_2)$ 与 Q 共轭。证明，存在 $(p',l')\in\Pi\times\Lambda$，使得 P' 和 Q' 分别为 l' 与 p' 的稳定化子并且

$$|P'\cap Q'|=\begin{cases}8,&\text{若 }p'\text{ 在 }l'\text{ 上;}\\6,&\text{若 }p'\text{ 不在 }l'\text{ 上.}\end{cases}$$

7. 按如下方式定义 P 和 Q 的子群：

$$M=\left\{\begin{pmatrix}*&*&0\\*&*&0\\0&0&1\end{pmatrix}\right\},\quad U=\left\{\begin{pmatrix}1&0&*\\0&1&*\\0&0&1\end{pmatrix}\right\},\quad N=\left\{\begin{pmatrix}1&0&0\\0&*&*\\0&*&*\end{pmatrix}\right\},\quad V=\left\{\begin{pmatrix}1&*&*\\0&1&0\\0&0&1\end{pmatrix}\right\}.$$

   证明，$U\lhd P$ 并且 $P=U\rtimes M$；$V\lhd Q$ 并且 $Q=V\rtimes N$。

8. 证明，U 和 V 在 $\mathbf{GL}(3;\mathbb{F}_2)$ 中不共轭；每个 $\mathbf{GL}(3;\mathbb{F}_2)$ 中同构于 $\mathbb{Z}\big/2\mathbb{Z}\times\mathbb{Z}\big/2\mathbb{Z}$ 的子群都共轭于 U 或者 V；U 和 V 在 $\mathbf{GL}(3;\mathbb{F}_2)$ 中各有 7 个与之共轭的子群，它们被记作

$$\Pi'=\{U_1,U_2,\cdots,U_7\},\quad \Lambda'=\{V_1,V_2,\cdots,V_7\}.$$

9. 证明，对任意 $U'\in\Pi',V'\in\Lambda'$，若 $U'\cap V'\neq\emptyset$，则 $U'\cap V'=\{1,z\}$，其中，$z\in\mathbf{GL}(3;\mathbb{F}_2)$ 是一个 2 阶元。进一步，z 的中心化子 $\mathrm{C}(z):=\mathrm{C}_{\mathbf{GL}(3;\mathbb{F}_2)}(z)$ 是 $\mathbf{GL}(3;\mathbb{F}_2)$ 的包含 U' 和 V' 的 Sylow 2-子群。

10. 证明，$\mathbf{GL}(3;\mathbb{F}_2)$ 中恰有 21 个 2 阶元并且它们两两共轭。进一步证明以下映射是双射：

$$\big\{\mathbf{GL}(3;\mathbb{F}_2)\text{ 中的 2 阶元}\big\}\longrightarrow\big\{\mathbf{GL}(3;\mathbb{F}_2)\text{ 的 Sylow 2-子群}\big\},\quad z\mapsto\mathrm{C}(z).$$

11. 定义 Π' 和 Λ' 上的重合关系：

$$I'=\big\{(U',V')\in\Pi'\times\Lambda'\big|U'\cap V'\neq\emptyset\big\}$$

    证明，(Π',Λ',I') 是 Fano 平面。

12. **第三部分，应用：$\mathbf{PSL}(2;\mathbb{F}_7)\simeq\mathbf{GL}(3;\mathbb{F}_2)$**

证明，$\mathbf{PSL}(2;\mathbb{F}_7)$ 中的 2 阶元有 21 个并且以下为其（矩阵表示的）清单：

$$z_1=\begin{pmatrix}4&3\\6&3\end{pmatrix},z_2=\begin{pmatrix}1&1\\5&6\end{pmatrix},z_3=\begin{pmatrix}1&6\\2&6\end{pmatrix},z_4=\begin{pmatrix}1&4\\3&6\end{pmatrix},z_5=\begin{pmatrix}1&5\\1&6\end{pmatrix},z_6=\begin{pmatrix}4&2\\2&3\end{pmatrix},$$
$$z_7=\begin{pmatrix}1&3\\4&6\end{pmatrix},z_8=\begin{pmatrix}0&2\\3&0\end{pmatrix},z_9=\begin{pmatrix}0&4\\5&0\end{pmatrix},z_{10}=\begin{pmatrix}2&1\\2&5\end{pmatrix},z_{11}=\begin{pmatrix}4&4\\1&3\end{pmatrix},z_{12}=\begin{pmatrix}4&5\\5&3\end{pmatrix},$$
$$z_{13}=\begin{pmatrix}2&2\\1&5\end{pmatrix},z_{14}=\begin{pmatrix}4&6\\3&3\end{pmatrix},z_{15}=\begin{pmatrix}2&4\\4&5\end{pmatrix},z_{16}=\begin{pmatrix}1&2\\6&6\end{pmatrix},z_{17}=\begin{pmatrix}2&5\\6&5\end{pmatrix},z_{18}=\begin{pmatrix}0&1\\6&0\end{pmatrix},$$
$$z_{19}=\begin{pmatrix}2&6\\5&5\end{pmatrix},z_{20}=\begin{pmatrix}4&1\\4&3\end{pmatrix},z_{21}=\begin{pmatrix}2&3\\3&5\end{pmatrix}.$$

13. 证明，$\mathbf{GL}(3;\mathbb{F}_2)$ 中同构于 $\mathbb{Z}\!\diagup\!2\mathbb{Z}\times\mathbb{Z}\!\diagup\!2\mathbb{Z}$ 的子群共有 14 个，每个群以及群中的元素由如下清单给出：

$$\Pi''=\left\{\begin{matrix}\{1,z_1,z_8,z_{10}\},\{1,z_2,z_7,z_{17}\}\\\{1,z_3,z_{16},z_{21}\},\{1,z_4,z_5,z_{19}\},\\\{1,z_6,z_{11},z_{20}\},\{1,z_9,z_{13},z_{14}\},\\\{1,z_{12},z_{15},z_{18}\}\end{matrix}\right\},\quad\Lambda''=\left\{\begin{matrix}\{1,z_1,z_{12},z_{14}\},\{1,z_2,z_5,z_{15}\}\\\{1,z_3,z_4,z_{13}\},\{1,z_6,z_8,z_{21}\},\\\{1,z_7,z_{10},z_{16}\},\{1,z_8,z_{11},z_{19}\},\\\{1,z_9,z_{17},z_{20}\}\end{matrix}\right\},$$

并且以上 Π'' 与 Λ'' 恰好是这些群的共轭类。

14. 定义 Π'' 和 Λ'' 上的重合关系：

$$I''=\big\{(p,l)\in\Pi''\times\Lambda''\big|p\cap l\neq\emptyset\big\}.$$

证明，(Π'',Λ'',I'') 是 Fano 平面。

15. 证明，$\mathbf{PSL}(2;\mathbb{F}_7)\simeq\mathbf{GL}(3;\mathbb{F}_2)$。

16. **第四部分，利用交比构造 Fano 平面来证明 $\mathbf{PSL}(2;\mathbb{F}_7)\simeq\mathbf{GL}(3;\mathbb{F}_2)$**

对任意四个不同的 $z_1,z_2,z_3,z_4\in\mathbf{P}^1(\mathbb{F}_p)=\mathbb{F}_p\cup\{\infty\}$，定义其交比为

$$[z_1,z_2;z_3,z_4]=\frac{\frac{z_1-z_3}{z_1-z_4}}{\frac{z_2-z_3}{z_2-z_4}}=\frac{z_1-z_3}{z_1-z_4}\cdot\frac{z_2-z_4}{z_2-z_3}.$$

证明，$[z_1,z_2;z_3,z_4]$ 在 $\mathbf{PGL}(2;\mathbb{F}_p)$ 的作用下不变，即对任意 $g\in\mathbf{PGL}(2;\mathbb{F}_p)$，

$$[g(z_1),g(z_2);g(z_3),g(z_4)]=[z_1,z_2;z_3,z_4].$$

（提示：先证明 $\mathbf{PGL}(2;\mathbb{F}_p)$ 可由形如 $\begin{pmatrix}1&*\\0&1\end{pmatrix},\begin{pmatrix}*&0\\0&*\end{pmatrix}$ 和 $\begin{pmatrix}0&1\\1&0\end{pmatrix}$ 的矩阵生成）

17. 给定四个不同的 $z_1,z_2,z_3,z_4\in\mathbb{F}_p\cup\{\infty\}$，令 $\lambda=[z_1,z_2;z_3,z_4]$。考虑对称群 $\mathfrak{S}_4$ 在集合 $\{z_1,z_2,z_3,z_4\}$ 上的作用：对任意 $\sigma\in\mathfrak{S}_4$，$\sigma(z_i)=z_{\sigma(i)}$，其中，$i=1,2,3,4$。证明，$\{\sigma(\lambda)=[z_{\sigma(1)},z_{\sigma(2)};z_{\sigma(3)},z_{\sigma(4)}]\big|\sigma\in\mathfrak{S}_4\}$ 所有可能的取值为 $\lambda,\frac{1}{\lambda},1-\lambda,\frac{1}{1-\lambda},\frac{\lambda}{1-\lambda},\frac{1-\lambda}{\lambda}$。令

$$H=\{1,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}<\mathfrak{S}_4,$$

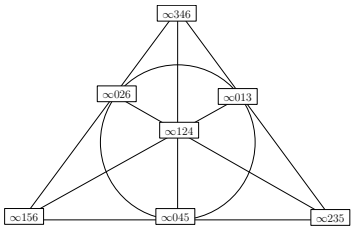
证明，对任意的 $\sigma\in H$，$\sigma(\lambda)=\lambda$。

18. 证明，恰好有 28 个四元子集 $\{z_1,z_2,z_3,z_4\}\subset\mathbb{F}_7\cup\{\infty\}$，使得 $[z_1:z_2:z_3:z_4]=3$。特别地，通过计算证明含有 ∞ 的子集有 14 个，它们由如下两个集合给出：

$$\Pi_*=\left\{\begin{matrix}\{\infty,0,1,3\},\{\infty,0,2,6\},\\ \{\infty,0,4,5\},\{\infty,1,2,4\}\\ \{\infty,1,5,6\},\{\infty,2,3,5\}\\ \{\infty,3,4,6\}\end{matrix}\right\},\quad \Lambda_*=\left\{\begin{matrix}\{\infty,0,2,3\},\{\infty,0,1,5\},\\ \{\infty,0,4,6\},\{\infty,1,3,4\}\\ \{\infty,1,2,6\},\{\infty,2,4,5\}\\ \{\infty,3,5,6\}\end{matrix}\right\}$$

19. 我们定义 Π_* 与 Λ_* 之间的重合关系为

$$I_*=\big\{(p,l)\in\Pi_*\times\Lambda_*\big||p\cap l|=3\big\}.$$



证明，(Π_*,Λ_*,I_*) 是 Fano 平面。

20. 证明，$\{p,\overline{p},l,\overline{l}\big|p\in\Pi_*,l\in\Lambda_*\}$，$\mathbf{PSL}(2;\mathbb{F}_7)\simeq\mathbf{GL}(3;\mathbb{F}_2)$ 恰好给出了所有交比为 3 的 28 个集合，其中，$\overline{p}$ 和 $\overline{l}$ 分别为 p 和 l 在 $\mathbf{P}^1(\mathbb{F}_7)$ 中的补集。从而，$\mathbf{PSL}(2;\mathbb{F}_7)$ 可以作用在 $\{\{p,\overline{p}\},\{l,\overline{l}\}\big|p\in\Pi_*,l\in\Lambda_*\}$ 上给出同构 $\mathbf{PSL}(2;\mathbb{F}_7)\simeq\mathbf{GL}(3;\mathbb{F}_2)$。

3.6.12 练习题

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 ${}^{G}\!/_{\mathrm{Z}(G)}$ 是循环群。
3. （对称群指标的另一种定义）定义映射

$$\varepsilon':\mathfrak{S}_n\to\{\pm\},\quad \sigma\mapsto\varepsilon'(\sigma)=\prod_{1\leqslant i<j\leqslant n}\frac{\sigma(i)-\sigma(j)}{i-j}.$$

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 $\mathfrak{S}_n \to \mathbb{Z}/2\mathbb{Z}$。
   - 不存在非平凡的群同态 $\mathfrak{A}_n \to \mathbb{Z}/2\mathbb{Z}$。
   - $\mathfrak{A}_n$ 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，$p \leqslant n < p^2$。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. $n \geqslant 2$，子群 $H < \mathfrak{S}_n$ 的指标为 n。证明，$H \simeq \mathfrak{S}_{n-1}$。

13. 证明，四元数群 $\mathbf{Q}_8$ 不能写成两个非平凡子群的半直积。

14. N 是群，K 是循环群，$\varphi : K \to \mathrm{Aut}(N))$ 和 $\psi : K \to \mathrm{Aut}(N))$ 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）

15. G 是 p-群，$|G| = p^k$。证明，对任意的 $l \leqslant k$，存在正规子群 $H \lhd G$，使得 $|H| = p^l$。（提示：利用 $\mathrm{Z}(G) \neq 1$ 以及 $G \to G/\mathrm{Z}(G)$ 进行归纳）

16. 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 $\mathbb{Z}^n \to A$。

17. A 是交换群。我们定义 A 中的**挠元素**为下面集合中的元：

$$A^{\mathrm{tor}} = \{x \in A | \text{存在} n \in \mathbb{Z}, \text{使得 } nx = 0\}.$$

    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 $A \simeq A^{\mathrm{tor}} \times \mathbb{Z}^r$，其中，$r$ 是 A 的秩。

18. A 和 B 是交换群。证明，$(A \times B)^{\mathrm{tor}} \simeq A^{\mathrm{tor}} \times B^{\mathrm{tor}}$。

19. 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 $H \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$。

20. 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 $G \simeq \prod_{n\text{ 个}} \mathbb{Z}/2\mathbb{Z}$。

21. 对任意的 $n \geqslant 1$。证明，存在 $\mathbb{R}$ 的子群 G，使得 $G \simeq \prod_{n\text{ 个}} \mathbb{Z}$。

22. A, B 和 C 是有限生成的交换群。证明如下两个结论：

$$1)\ A \times A \simeq B \times B \ \Rightarrow\ A \simeq B;\ 2)\ A \times C \simeq B \times C \ \Rightarrow A \simeq B.$$

4 环与模

4.1 环论的一些基本概念

回顾环 $(A,\cdot,+)$ 的定义，请参考2.4一节：$(A,+,0)$ 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

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

另外，环中的乘法可以不是交换的：如果对任意的 $a,b\in A$，$a\cdot b=b\cdot a$，A 被称作是交换环。

B 是 A 的子环，指的是 $B<A$ 为加法子群、$1\in B$ 并且 B 对乘法封闭。

具有逆元的 $a\in A$ 被称为可逆的，即存在 $b\in A$，使得 $a\cdot b=b\cdot a=1$。用 $A^\times$ 表示 A 中可逆元之集。很明显，$(A^\times,\cdot)$ 是群。另外，若 $A^\times=A-\{0\}$，即非零元均可逆，则称 A 是**可除环**。按定义，交换可除环被称为域。

如果环 A_1 和 A_2 间的映射 $\varphi:A_1\to A_2$ 保持加法和乘法并且 $\varphi(1)=1$，就称 φ 是环同态。我们用 $\mathbf{Hom}(A_1,A_2)$ 表示从 A_1 到 A_2 的换同态的集合。同态 $\varphi\in\mathrm{Hom}(A_1,A_2)$ 的核定义为：

$$\mathrm{Ker}(\varphi)=\big\{a\in A_1\big|\varphi(a)=0\big\}.$$

由于 $1\notin\mathrm{Ker}(\varphi)$，$\mathrm{Ker}(\varphi)$ 不是子环。

定义 4.1. A 是环，$I\subset A$ 是 A 的加法子群。若对任意 $a\in A$ 和 $x\in I$，均有 $a\cdot x\in I$，则称 I 是 A 的**左理想**；若对任意 $a\in A$ 和 $x\in I$，均有 $x\cdot a\in I$，则称 I 是 A 的**右理想**。若 I 即是左理想又是右理想，则称 I 是**双边理想**（简称为理想）。

注记 4.1. 特别地，$I\neq A$。另外，若 A 是交换环，则其左理想或者右理想均为双边理想，此时，我们不再区分左右。

例子 4.1. 对任意环同态 $\varphi:A_1\to A_2$，$\mathrm{Ker}(\varphi)$ 是 A_1 的（双边）理想。

实际上，对任意的 $a\in A_1$ 和 $x\in\mathrm{Ker}(\varphi)$，有

$$\varphi(a\cdot x)=\varphi(a)\varphi(x)=0,\quad \varphi(x\cdot a)=\varphi(x)\varphi(a)=0.$$

例子 4.2. 给定环 A 中的元素 a，令 $(a)=A\cdot a=\big\{a'\cdot a\big|a'\in A\big\}$，这是 A 的左理想。

例子 4.3. A 是交换环，则 A 是域等价于 A 只有 0 这一个理想。

事实上，如果 A 不是域，存在 $a\neq0$，使得 a 没有逆，从而，$(a)\subset A$ 是理想。这与 A 只有 0 这一个理想矛盾。

注记 4.2. 给定环 A 的 (双边) 理想 I，我们可构造**商环**$A\!\diagup\!_I$。

首先，取 $A\!\diagup\!_I$ 为 A 的加法群的商群，其中，理想 I 被视作是 A 的正规子群。按定义，这是如下左陪集的集合：

$$A\!\diagup\!_I=\big\{a+I\big|a\in A\big\}.$$

其中，$a+I=a'+I$ 当且仅当 $a-a'\in I$。根据商群的定义，$A\!\diagup\!_I$ 的加法定义为

$$(a+I)+(b+I):=(a+b)+I.$$

其中，$I=0+I$ 是加法零元。

我们再定义 A/I 上的乘法：

$$(a+I)\cdot(b+I) := ab+I.$$

对于 $a+I=a'+I$，由于 $ab-a'b=(a-a')b\in I$（利用 I 是左理想），从而 $ab+I=a'b+I$。这表明 A/I 上乘法的定义不依赖于 $a+I$ 中代表元的选取；类似的，利用 I 是右理想，上述乘法也不依赖于 $b+I$ 中代表元的选取。很明显，$1+I$ 是乘法单位元。

上述定义的加法和乘法也满足结合律，从而给出了 A/I 上的环结构。我们把 A/I 称作是 A 对 I 的**商环**。商映射

$$\pi : A \longrightarrow A/I,\quad a\mapsto a+I,$$

是满的环同态。实际上，对任意 $a,b\in A$，有

$$\pi(a+b)=a+b+I=(a+I)+(b+I)=\pi(a)+\pi(b),\quad \pi(ab)=ab+I=(a+I)(b+I)=\pi(a)\pi(b).$$

另外，上述等式表明，在集合 A/I 商存在唯一的环结构，使得 π 为环同态。

我们已熟知命题13是构造群之间同态的重要工具。类似的，我们有如下命题：

命题 38. *A 和 B 是环，$I\subset A$ 是理想，$\varphi : A\to B$ 是环同态。若 $I\subset \mathrm{Ker}(\varphi)$，则存在唯一的环同态 $\overline{\varphi}: A/I\to B$，使得 $\overline{\varphi}\circ\pi=\varphi$，其中，$\pi : A\to A/I$ 是自然的同态。*

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \overline{\varphi}} & \\ A/I & & \end{array}$$

进一步，映射 $\overline{\varphi}: A/\mathrm{Ker}(\varphi)\xrightarrow{\simeq}\mathrm{Im}(\varphi)$ 是环同构。

证明： 对 $a+I\in A/I$，我们定义 $\overline{\varphi}(a+I)=\varphi(a)$。根据命题13，只要证明 $\overline{\varphi}$ 是环同态，这只是例行公事般的验证。 □

例子 4.4. A 和 B 是环，$A\times B$ 也是[17]，则 $I=A\times 0=\{(a,0)|a\in A\}$ 是 $A\times B$ 的理想。此时，$A\times B/I\simeq B$。

约定. 自此，除部分习题，总假定 A 是交换环。

例子 4.5 (素理想与整环的定义)**.** A 是环，对 $a\in A$，若存在 $b\in A$，使得 $a\cdot b=0$ 或者 $b\cdot a=0$，则称 a 是一个**零因子**。如果环 A 是交换环并且除 0 外无其它零因子，则称 A 是**整环**。

注意，按定义整环 A 总是交换的。换而言之，A 是整环，则 $a\cdot b=0$ 意味着 $a=0$ 或 $b=0$（至少之一成立）。根据定义，域是整环。

A 是环，$\mathfrak{p}\subset A$ 是理想并且 $\mathfrak{p}\neq A$。若对任意的 $a,b\in A$，$a\cdot b\in\mathfrak{p}$ 意味着 $a\in\mathfrak{p}$ 或 $b\in\mathfrak{p}$，则称 $\mathfrak{p}$ 是**素理想**。

$\mathfrak{p}$ 是素理想的一个等价定义是 $a\notin\mathfrak{p}$，$b\notin\mathfrak{p}$，则 $a\cdot b\notin\mathfrak{p}$。

我们考虑整数环 $\mathbb{Z}$ 的素理想。假设 p 是素数，令 $(p)=\{pn|n\in\mathbb{Z}\}$，则 (p) 是理想。若 $a,b\notin(p)$，即 $p\nmid a, p\nmid b$，从而 $p\nmid ab$，即 $ab\notin(p)$。这表明 (p) 是素理想。另外，若 $n=n_1\cdot n_2$ 是合数，其中 $n_1,n_2\geqslant 2$，令 $(n)=\{kn|k\in\mathbb{Z}\}$，那么，$n_1\notin(n), n_2\notin(n)$，但是 $n_1\cdot n_2\notin(n)$，这表明 (n) 不是素理想。根据之后关于 $\mathbb{Z}$ 是主理想整环的性质，$\mathbb{Z}$ 中的素理想均形如 (p)，其中，p 是素数。

[17]参考2.7.1

注记 4.3. A 是交换环，$(0) := \{0\}$。那么，A 是整环等价于 (0) 是素理想。

我们可以用商环来刻画素理想：

引理 39. *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： 若 $\mathfrak{p}$ 是素理想，则对任意 $a+\mathfrak{p}, b+\mathfrak{p} \in A/\mathfrak{p}$ 并满足 $(a+\mathfrak{p})(b+\mathfrak{p}) = \mathfrak{p}$，要证明 $a+\mathfrak{p} = 0$ 或 $b+\mathfrak{p} = 0$，即 $a \in \mathfrak{p}$ 或 $b \in \mathfrak{p}$。按定义，$(a+\mathfrak{p})(b+\mathfrak{p}) = ab+\mathfrak{p} = \mathfrak{p}$，从而，$ab \in \mathfrak{p}$，根据 $\mathfrak{p}$ 是素理想，$a \in \mathfrak{p}$ 或 $b \in \mathfrak{p}$。

若 $A/\mathfrak{p}$ 是整环，那么 $a \cdot b \in \mathfrak{p}$ 等价于说 $A/\mathfrak{p}$ 中 $(a+\mathfrak{p})(b+\mathfrak{p}) = 0$，所以可不妨设 $a+\mathfrak{p} = 0$，即 $a \in \mathfrak{p}$。这表明 $\mathfrak{p}$ 是素理想。 □

例子 4.6. $\mathbb{Z}/p\mathbb{Z}$ 是整环，这是因为 $(p) = p\mathbb{Z}$ 是素理想。当然，我们知道 $\mathbb{Z}/p\mathbb{Z}$ 实际上是域。请参考如下注解：

注记 4.4. A 是只有有限个元素的整环，则 A 是域。

实际上，对任意的 $a \in A$，考虑映射

$$\varphi : A \to A,\ x \mapsto a \cdot x.$$

由于 A 是整环，所以 φ 是单射。又因为 A 的元素个数限，从而 φ 是满射。特别地，存在 $b \in A$，使得 $\varphi(b) = 1$，即 $a \cdot b = 1$。这表明 a^{-1} 是存在的。

例子 4.7 (分式域的构造)**.** A 是整环。我们在集合 $A \times (A - \{0\})$ 上定义等价关系：

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad ad = bc.$$

不难验证，以上 $\sim$ 的确是等价关系。用 $\frac{a}{b}$ 表示 (a, b) 在 $\mathrm{Frac}(A) = A \times (A - \{0\})/\sim$ 中对应的等价类。特别地，对任意的 $\lambda \in A - \{0\}$，自然有 $\frac{\lambda a}{\lambda b} = \frac{a}{b}$。

我们在 $\mathrm{Frac}(A)$ 定义加法和乘法：

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ad}{bd}.$$

不难验证，以上定义不依赖于代表元 a, b 的选取，即若 $(a, b) \sim (a', b'), (c, d) \sim (c', d,)$，我们有

$$\frac{a'd'+b'c'}{b'd'} = \frac{ad+bc}{bd}, \quad \frac{a'd'}{b'd'} = \frac{ad}{bd}.$$

我们规定 $\frac{1}{1}$ 是乘法单位元，$\frac{0}{1}$ 是加法单位元，那么，$\frac{a}{b} \cdot \frac{b}{a} = \frac{1}{1}$。特别地，在以上运算下 $\mathrm{Frac}(A)$ 是域。我们把 $\mathrm{Frac}(A)$ 称作 A 的**分式域**。

4.2 关于理想的一些操作

A 是环，$I_1, \cdots, I_n$ 是 A 的理想，定义

$$I_1 + \cdots + I_n = \{x_1 + x_2 + \cdots + x_n | x_1 \in I_1, \cdots, x_n \in I_n\},$$
$$I_1 \cdot I_2 \cdots \cdot I_n = \{\text{有限个形如 } x_1 x_2 \cdots x_n \text{ 的元素之和，其中} x_1 \in I_1, \cdots, x_n \in I_n\}.$$

很明显，这两个集合是 A 的理想并且 $I_1 \cdot I_2 \cdots \cdot I_n \subset I_1 + \cdots + I_n$。当 $n = 2$ 时，$I_1 + I_2$ 中的元素形如 $x + y$，其中 $x \in I_1, y \in I_2$；$I_1 \cdot I_2$ 中的元素形如 $\sum_{i=1}^{m} x_i y_i$，其中，$x_i \in I_1$，$y_i \in I_2$。

我们注意到如果 $\{I_i\}_{i\in\Lambda}$ 是理想的集合，那么，$\bigcap_{i\in\Lambda} I_i$ 也是理想。给定 A 的非空子集 $S\subset A$，包含 S 的所有理想之交是包含 S 的最小理想（在包含关系下），我们把它记作 (S) 并称之为**由 S 所生成的理想**。很明显，(S) 中的元素均形如

$$\sum_{\text{有限和}} a\cdot s,\ \text{其中 } s\in S, a\in A.$$

若理想 I 由有限集 $\{a_1,\cdots,a_k\}$ 生成，则称 I 是**有限生成的**并记作 $I=(a_1,\cdots,a_k)$。

若 I 由一个元素 a 生成，则称 I 是**主理想**并记作 $I=(a)$。

注记 4.5. 假设 $I_1=(a_1,\cdots,a_n), I_2=(b_1\cdots,b_m)$，那么，

$$I_1+I_2=(a_1,\cdots,a_n,b_1,\cdots,b_m),\ \ I_1\cdot I_2=(a_ib_j, 1\leqslant i\leqslant n, 1\leqslant j\leqslant m).$$

定义 4.2. A 是整环，若其理想均为主理想，则称 A 是**主理想整环**。

例子 4.8. $\mathbb{Z}$ 是主理想整环。

对任意的理想 $I\subset\mathbb{Z}$，不妨设 $I\neq(0)$。令 $d=\min I\cap\mathbb{Z}_{>0}$，则 $I=(d)$。实际上，对任意 $a\in I$，根据带余除法，存在唯一 $b\in\mathbb{Z}$ 和 $r\in[0,d)$，使得 $a=bd+r$。我们注意到 $r=a-bd\in I$ 而 $d=\min I\cap\mathbb{Z}_{\geqslant 0}$，从而 $r=0$，即 $a=bd$，所以，$a\in(d)$。根据 a 选取的任意性，$I\subset(a)$，所以 $I=(a)$。

例子 4.9. K 是域，则多项式环 $K[X]$ 是主理想整环。

对任意的非零理想 $I\subset K[X]$，令 $P(X)$ 为 I 中次数最小的多项式。我们证明 $I=\big(P(X)\big)$。实际上，对任意 $Q(X)\in I$，根据带余除法，存在唯一 $A(X),R(X)\in K[X]$，使得 $Q(X)=A(X)P(X)+R(X)$ 并且 $\deg(R)<\deg(P)$ 或 $R(X)=0$。根据 P 的次数最小性，从而 $R=0$，即 $Q(X)=A(X)P(X)$，所以 $Q(X)\in(P)$。根据 Q 选取的任意性，$I\subset\big(P(X)\big)$，所以 $I=\big(P(X)\big)$。

定义 4.3. A 是环，$\mathfrak{m}\subset A$ 是理想并且 $\mathfrak{m}\neq A$。若 $\mathfrak{m}$ 在包含关系下是最大的，即对任意理想 I，$\mathfrak{m}\subset I\subset A$ 意味着 $I=\mathfrak{m}$ 或 $I=A$ 成立，则称 $\mathfrak{m}$ 是**极大理想**。

注记 4.6. 极大理想是素理想。

实际上，对任意 $x\notin\mathfrak{m}$，根据极大性，$(\mathfrak{m},x)=A$。由于 $(\mathfrak{m},x)$ 中的元素均形如 $ax+m$，其中 $m\in\mathfrak{m}, a\in A$，从而存在 $m\in\mathfrak{m}, a\in A$，使得 $ax+m=1$。类似地，对任意 $y\notin\mathfrak{m}$，存在 $m'\in\mathfrak{m}, a'\in A$，使得 $a'y+m'=1$。据此，我们有

$$aa'xy=(1-m)(1-m')=1 \bmod \mathfrak{m}.$$

所以，$xy\notin\mathfrak{m}$（否则 $1\in\mathfrak{m}$）。这就证明了 $\mathfrak{m}$ 是素理想。

命题 40. *A 是环，I 是理想并且 $I\neq A$，则存在极大理想 $\mathfrak{m}$，使得 $\mathfrak{m}\neq A$ 并且 $\mathfrak{m}\supset I$。*

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 $J_1\preceq J_2$ 指的是 $J_1\subset J_2$。此时，对任意的全序子集 $S\subset\mathcal{J}$，令

$$J_*=\bigcup_{J\in S} J.$$

现在证明 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 $J_1\supset J_2$，从而 $x,y\in J_1$。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，$J_*\neq A$。所以，$J_*\in\mathcal{J}$。根据定义，J_* 是 S 的上界。根据 Zorn 引理，S 有极大元 $\mathfrak{m}$，这是极大理想。 □

注记 4.7 (利用极大理想构造域)**.** A 是交换环，那么理想 $\mathfrak{m}$ 是极大理想当且仅当 $A/\mathfrak{m}$ 是域。

若 $\mathfrak{m}$ 是极大理想，则对任意非零 $x+\mathfrak{m}\in A/\mathfrak{m}$，有 $x\notin\mathfrak{m}$。根据极大性，$(\mathfrak{m},x)=A$，从而存在 $m\in\mathfrak{m},y\in A$，使得 $xy+m=1$。这表明 $y+\mathfrak{m}$ 是 $x+\mathfrak{m}$ 在 $A/\mathfrak{m}$ 中的乘法逆。

反之，假设 $\mathfrak{m}\subset I\subset A$，不难看出 $I/\mathfrak{m}\subset A/\mathfrak{m}$ 是理想。由于 $A/\mathfrak{m}$ 是域，则 $I/\mathfrak{m}=$ 或者 $A/\mathfrak{m}$，从而，$I=\mathfrak{m}$ 或者 A。

例子 4.10. p 是素数，由于 $\mathbb{Z}/p\mathbb{Z}$ 是域，所以 $(p)=p\mathbb{Z}$ 是 $\mathbb{Z}$ 的极大理想（也可直接证明）。然而，$(0)\subset\mathbb{Z}$ 是素理想但不是极大理想。

我们以下来证明中国剩余定理。A 是交换环，$I_1,\cdots,I_n\subset A$ 是理想，我们有自然的环同态：

$$\pi:A\to A/I_1\times A/I_2\times\cdots\times A/I_n,\quad x\mapsto\big(\pi_1(x),\pi_2(x),\cdots,\pi_n(x)\big).$$

其中，$\pi_i:A\to A/I_i$ 是商映射。显而易见，$\mathrm{Ker}(\pi)=\bigcap_{i=1}^n I_i$。

给定理想 $I,J\subset A$，若 $I+J=A$，就称 I 与 J **互素**。换而言之，I 与 J 互素当且仅当 $1\in I+J$。这个概念是从整数环中类比而来的：$m,n\in\mathbb{Z}$ 是互素，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 41 (中国剩余定理)**.** *A 是交换环，$n\geqslant 2$，$I_1,\cdots,I_n\subset A$ 是理想并且两两互素。那么，$\bigcap_{i=1}^n I_i=\prod_{i=1}^n I_i$。进一步，$\pi:A\to A/I_1\times\cdots\times A/I_n$ 是满射，从而有环同构*

$$A/I_1\cdot I_2\cdots I_n\xrightarrow{\simeq}A/I_1\cap I_2\cap\cdots\cap I_n\xrightarrow{\simeq}A/I_1\times A/I_2\times\cdots\times A/I_n.$$

证明： 对 n 进行归纳。$n=1$ 是显然的。当 $n=2$ 时候，由于 $I_1\cdot I_2\subset I_1\cap I_2$，只要证明反向的包含关系：对任意 $x\in I_1\cap I_2$，证明 $x\in I_1\cap I_2$。根据 $I_1+I_2=A$，存在 $a_1\in I_1,a_2\in I_2$，使得 $a_1+a_2=1$。据此，

$$x=1\cdot x=\underbrace{a_1}_{\in I_1}\cdot\underbrace{x}_{\in I_2}+\underbrace{a_2}_{\in I_2}\cdot\underbrace{x}_{\in I_1}\in I_1\cdot I_2.$$

先证明 π 是满射：对任意的 $x_1+I_1\in A/I_1,x_2+2_1\in A/I_2$，构造 $x\in A$，使得 $x-x_1\in I_1,x-x_2\in I_2$。实际上，以上的 $a_1+a_2=1$ 给出了

$$\pi(a_1)=(0,1),\quad\pi(a_2)=(1,0).$$

从而，将 $a_1+a_2=1$ 视作是单位分解，我们有 $x=a_1x_1+a_2x_2$ 满足 $x-x_1\in I_1,x-x_2\in I_2$。

假设命题对 $n-1$ 成立，其中，$n\geqslant 3$。我们先证明 I_1 与 $I_2\cdot I_3\cdots I_n$ 互素，即 $I_1+I_2\cdot I_3\cdots I_n=A$。对每个 $k\geqslant 2$，根据 $I_1+I_k=A$，存在 $a_k\in I_1,b_k\in I_k$，$a_k+b_k=1$。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 是含有某个 a_i 的单项式之和，从而 $a\in I_1$。据此，$1\in I_1+I_2\cdot I_3\cdots I_n$。根据 $n=2$ 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

$$A/I_1\cdot(I_2\cdots I_n)\xrightarrow{\simeq}A/I_1\times A/I_2\cdots I_n\xrightarrow{\simeq}A/I_1\times\Big(A/I_2\times\cdots\times A/I_2\Big).$$

命题得证。 □

推论 42 (中国剩余定理)**.** *若 $n_1,\cdots,n_k$ 为两两互素的正整数，$n=n_1\cdots n_k$，则有环同构*

$$\mathbb{Z}/n\mathbb{Z}\xrightarrow{\simeq}\mathbb{Z}/n_1\mathbb{Z}\times\mathbb{Z}/n_2\mathbb{Z}\times\cdots\times\mathbb{Z}/n_k\mathbb{Z},\quad x\bmod n\mapsto\big(x\bmod n_1,\cdots,x\bmod n_k\big).$$

4.3 与整除相关的几类环

定义 4.4 (元素层次上的整除概念)**.** A 是整环。

给定 $a,b\in A$，若有 $q\in A$，使得 $a=qb$，则称b **整除** a 并记作 $b\mid a$。

给定 $x\in A$，若对任意 $a,b\in A$，$x\mid a\cdot b$ 意味着 $x\mid a$ 或 $x\mid b$，则称 x 是**素元**。

给定 $y\in A$ 并假设 $y\notin A^\times$（对乘法不可逆），假设对任意 $a,b\in A$，若 $x=a\cdot b$，则 $a\in A^\times$ 或 $b\in A^\times$，就称 y 是**不可约元**。

给定 $a,b\in A$，$a,b\in A$，若有 $u\in A^\times$，使得 $a=u\cdot b$，则称 a 和 b 是**伴随的**。

注记 4.8. 上述概念可在理想的层次上表述：

1) 整除性：$b\mid a\ \Leftrightarrow a\in(b)\ \Leftrightarrow(a)\subset(b)$；

2) 素元：x 是素元等价于 (x) 是素理想。

以上叙述的证明是平凡的。

注记 4.9. 素元是不可约的。

实际上，给定素元 x，若 $x=ab$，则 $x\mid ab$，从而可不妨设 $x\mid a$，即存在 a'，使得 $a=a'x$，从而，$x=a'bx$。由于 A 是整环，所以 $a'b=1$，即 $b\in A^\times$，从而 x 是不可约的。

我们之后会举例说明：不可约元未必是素元。

注记 4.10. A 是主理想整环，则素元等价于不可约元。

只要证明不可约元为素元即可。对任意的不可约元 $x\in A$，考虑 (x) 以及极大理想 $\mathfrak{m}\supset(x)$。由于 A 为主理想整环，存在 $a\in A$，使得 $(a)=\mathfrak{m}\supset(x)$。所以，存在 $b\in A$，使得 $x=ab$。由于 x 不可约，$b\in A^\times$。这样，$\mathfrak{m}=(a)=(b^{-1}x)=(x)$。特别地，由于极大理想是素理想，$(x)$ 是素理想，从而 x 是素元。

以上推理还给出了如下命题：

命题 43. 主理想整环的非零素理想是极大理想。

注记 4.11. 考虑域 K 上的多项式环 $K[X]$。由于 $K[X]^\times=K^\times$，$P(X)\in K[X]$ 是不可约元等价于传统意义上的不可约多项式。另外，$K[X]$ 是主理想整环，所以对任意的不可约多项式 P，(P) 是极大理想，从而 $K[X]\big/(P)$ 是域。

考虑映射的复合：

$$K\xrightarrow{\subset}K[X]\xrightarrow{\pi}K[X]\big/(P).$$

这是环同态，从而是域同态。由此可见，我们得到域扩张

$$\begin{array}{c}K[X]\big/(P)\\ \big|\\ K\end{array}$$

令 $d=\deg(P)$，不妨 $P=X^d+a_{d-1}X^{d-1}+\cdots+a_1X+a_0$，其中，$a_i\in K$。那么，$\pi(P)=0$ 意味着在 $K[X]\big/(P)$ 中，我们有

$$\overline{X}^d=-a_{d-1}\overline{X}^{d-1}-\cdots-a_1\overline{X}-a_0,$$

其中，$\overline{X}=\pi(X)$。据此，我们知道 $1,\overline{X},\cdots,\overline{X}^{d-1}$（的 K-线性组合）生成了 $K[X]/P$。另外，$1,\overline{X},\cdots,\overline{X}^{d-1}$ 是 K-线性无关的，因为若有 $b_0,\cdots,b_{d-1}\in K$，使得在 $K[X]/(P)$ 中，$\sum_{k=0}^{d-1}b_k\overline{X}^k$，则 $\sum_{k=0}^{d-1}b_kX^k\in\mathrm{Ker}(\pi)=(P)$，从而，$P$ 整除 $\sum_{k=0}^{d-1}b_kX^k$。由于 P 不可约且次数为 d，从而，$\sum_{k=0}^{d-1}b_kX^k=0$，这就证明了线性无关性。

所以，$1,\overline{X},\cdots,\overline{X}^{d-1}$ 是一组基础。特别地，$[K[X]/P:K]=\deg(P)$。

定义 4.5 (Euclid 整环)**.** A 是整环。若存在映射

$$N:A\longrightarrow\mathbb{Z}_{\geqslant 0},$$

使得 $N(0)=0$ 并对任意的 $a,b\in A$，存在（不要求唯一）$q,r\in A$ 使得 $a=qb+r$ 且要么 $r=0$ 要么 $N(r)<N(b)$，则称 N 是 A 上的**范数**。如果整环 A 具有范数，则称之为 **Euclid 整环**。

对于上述表达式 $a=qb+r$，我们称 q 为 a 除以 b 的**商**，称 r 为**余数**。

注记 4.12. 在 Euclid 整环 A 中有辗转相除法：对任意 $a,b\in A$，存在 $r_0,r_1,\cdots r_k$，使得

$$r_0=a,r_1=b,r_0=q_1r_1+r_2,r_1=q_2r_2+r_3,\cdots,r_{k-1}=q_{k-1}r_k+r_{k+1}.$$

其中，对 $i=1,\cdots,k$。由于 $N(r_i)<N(r_{i-1})$ 并且 N 在非负整数中取值，从而存在 k，使得 $r_{k+1}=0$。

例子 4.11. $\mathbb{Z}$ 是 Euclid 整环。对 $n\in\mathbb{Z}$，我们取 $N(n)=|n|$。

例子 4.12. K 是域，$K[X]$ 是多项式环，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。

命题 44. *Euclid 整环是主理想整环。*

证明: 对任意理想 $I\subset A$，选取 $b\in I$，使得 $N(b)=\min_{a\in I-\{0\}}N(a)$。根据 Eulcid 整环的定义，对任意 $a\in I$，存在 $q,r\in A$ 使得 $a=qb+r$。那么，$r=0$：否则 $N(r)<N(b)$，然而 $r=a-qb\in I$，这与 b 的范数最小矛盾。从而，$a=qb\in(b)$。这表明，$I=(b)$ 为主理想。 □

例子 4.13. Gauss 整数环 $\mathbb{Z}[\sqrt{-1}]$ 是 Euclid 整环。

作为集合，定义 $\mathbb{Z}[\sqrt{-1}]=\{a+b\sqrt{-1}|a,b\in\mathbb{Z}\}$，这是 $\mathbb{C}$ 中整系数的格点集。在复数的运算下，$\mathbb{Z}[\sqrt{-1}]$ 是 $\mathbb{C}$ 的子环，从而是整环。

定义 $\mathbb{Z}[\sqrt{-1}]$ 上的范数

$$N:\mathbb{Z}[\sqrt{-1}]\longrightarrow\mathbb{Z}_{\geqslant 0},\quad N(x+y\sqrt{-1})=x^2+y^2.$$

我们还有 $N(a\cdot b)=N(a)N(b)$。

对任意 $a=x+y\sqrt{-1},b=z+w\sqrt{-1}\in\mathbb{Z}[\sqrt{-1}]$，在 $\mathbb{C}$ 中计算其商：

$$\frac{a}{b}=\frac{(xz+yw)+(yz-xw)\sqrt{-1}}{N(b)}.$$

考虑略作修正的带余除法稍作修改：存在 $q_1,q_2\in\mathbb{Z}$，$r_1,r_2\in\big[-\frac{1}{2}N(b),\frac{1}{2}N(b)\big)$，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，

$$a=\underbrace{(q_1+q_2\sqrt{-1})}_{q}b+\underbrace{\frac{r_1+r_2\sqrt{-1}}{N(b)}b}_{r}=qb+r.$$

由于 $q\in\mathbb{Z}[\sqrt{-1}]$，从而 $r\in\mathbb{Z}[\sqrt{-1}]$。以下计算 $N(r)$：

$$\begin{aligned}N(r)=N\left(\frac{r_1+r_2\sqrt{-1}}{N(b)}b\right)&=\frac{N(r_1+r_2\sqrt{-1})N(b)}{N(b)^2}=\frac{r_1^2+r_2^2}{N(b)}\\&<\frac{\frac{1}{4}N(b)^2+\frac{1}{4}N(b)^2}{N(b)}<N(b).\end{aligned}$$

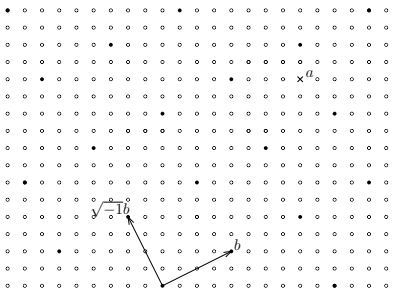
这就证明了 N 为范数，从而 $\mathbb{Z}[\sqrt{-1}]$ 是 Euclid 整环。

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

$$|\mathrm{Re}(q)-\mathrm{Re}(\frac{a}{b})|<\frac{1}{2},\ \ |\mathrm{Im}(q)-\mathrm{Im}(\frac{a}{b})|<\frac{1}{2}.$$

特别地，$N(\frac{a}{b}-q)<\frac{1}{2}$。那么，令 $r=a-qb$。我们就有

$$N(r)=N(b)N(\frac{a}{b}-q)<\frac{1}{2}N(b)=N(b).$$



还可以几何地考虑上述带余除法：给定 b，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）。

定义 4.6 (唯一分解整环)**.** A 是整环。对任意的 $a\in A-\left(\{0\}\cup A^\times\right)$，有

1) 存在 $n\geqslant 1$ 和 A 中不可约元 $p_1,\cdots,p_n$（可重复），使得 $a=p_1\cdots p_n$；

2) 以上分解在伴随意义下唯一：若 $a=q_1\cdots q_m$，$m\geqslant 1$ 且 $q_1,\cdots,q_m$ 是不可约元，则 $m=n$ 且通过调整脚标，对任意的 i，q_i 与 p_i 伴随。

注记 4.13. $\mathbb{Z}$ 是唯一分解整环并且素因数分解在伴随意义下唯一：比如对任意的素数 p,q，有 $p\cdot q=(-p)\cdot(-q)$，这里，$\mathbb{Z}^\times=\{1,-1\}$。

注记 4.14. K 是域，多项式环 $K[X]$ 也是唯一分解整环，这对应着多项式分解为不可约多项式的乘积。

注记 4.15. A 是唯一分解整环，那么，每个 $a \in A$ 可以写成：

$$a = up_1^{d_1} p_2^{d_2} \cdots p_n^{d_n},$$

其中，$p_1, \cdots, p_d$ 是不可约元，$u \in A^\times$。特别地，元素之间的整除性可从分解中不可约元素的幂读出：即对

$$a = up_1^{d_1} p_2^{d_2} \cdots p_n^{d_n}, \quad b = vp_1^{e_1} p_2^{e_2} \cdots p_n^{e_n},$$

其中，$u, v \in A^\times$，p_i 为不可约元且 d_i, e_i 为非负整数，$a \mid b$ 等价于 $d_i \leqslant e_i$，其中 $i = 1, \cdots, n$。

注记 4.16. 唯一分解整环中元素为素元等价于它是不可约的。

已知素元不可约，现在证明不可约元 $x \in A$ 是素元，即证 (x) 是素理想。对任意 $a, b \in A, ab \in (x)$，即有 $c \in A$，使得 $ab = cx$。不妨设 $a, b \notin A^\times$，考虑它们的分解 $a = up_1 \cdots p_n, b = vq_1 \cdots q_m$，其中，$p_i, q_j$ 为不可约元。对 c 和 x 也做类似分解，根据分解的唯一性以及 $ab = cx$，x（不可约元）与某个 p_i 或 p_j 伴随，不妨假设 $p_1 = wx$，其中，$w \in A^\times$，那么

$$a = u \cdot w \cdot x \cdot p_2 \cdots p_n \in (x).$$

这说明 (x) 是素理想。

定理 45. 主理想整环是唯一分解整环。

证明：任选 $a \in A$，其中，$a \notin \{0\} \cup A^\times$，我们来构造 a 的分解。

若 a 不可约，则 $a = a$ 为所要的分解。

否则，有 $a = a_1 \cdot b_1$，其中 $a_1, b_1 \notin A^\times$。特别地，$(a) \subset (a_1)$。若 a_1, b_1 都是不可约的，那么 $a = a_1 \cdot b_1$ 为所求。若不然，将 a_1 和 b_1 分解成为乘积 $a_2 \cdot a_2'$ 和 $b_2 \cdot b_2'$，则有 $a = a_2 \cdot a_2' \cdot b_2 \cdot b_2'$。特别地，我们有 $(a_1) \subset (a_2)$；然后对 a_2, a_2', b_2, b_2' 进行同样的讨论，以此类推。如果上述构造在有限步即停止，我们就得到了 a 的分解。否则，我们得到了无限长的主理想序列：

$$(a) \subset (a_1) \subset (a_2) \subset \cdots \subset A,$$

并且 $(a_i) \neq (a_{i+1})$。令 $I = \bigcup_{i \geqslant 1} (a_i)$，这是 A 的理想。由于对任意的 i，$1 \notin (a_i)$，所以 $I \neq A$。根据 A 是主理想整环，$I = (c)$。根据定义 I 的构造，存在 k，使得 $c \in (a_k)$，则 $I = (a_k)$。这说明该理想序列有限，矛盾。

最终证明分解的唯一性：$a = up_1 \cdots p_n = vq_1 \cdots q_m$ 是两个分解，其中，$u, v \in A^\times$ 而 p_i 和 q_j 都是不可约元。那么，$q_1 \cdots q_m \in (p_1)$。我们知道主理想整环中的不可约元是素元，所以，(p_1) 是素理想。从而，存在某个 $q_j \in (p_1)$，比如说 $q_1 \in (p_1)$，$q_1 = wp_1$。由于 q_1 不可约，则 $w \in A^\times$。从而，

$$up_2 \cdots p_n = vw \cdot q_2 \cdots q_m.$$

如此继续下去，唯一性是明显的。 □

注记 4.17. 我们已经证明了如下包含关系：

$$\{\text{Euclid 整环}\} \subset \{\text{主理想整环}\} \subset \{\text{唯一分解整环}\}.$$

并且在以上三种情形下某元素为素元等价于它是不可约的。

例子 4.14. $A=\mathbb{Z}[\sqrt{-5}]$ 不是唯一分解整环。

作为集合，$\mathbb{Z}[\sqrt{-5}]=\{x+y\sqrt{-5}|a,b\in\mathbb{Z}\}$，它上面的运算为复数的四则运算。特别地，这是 $\mathbb{C}$ 的子环。

在 $A=\mathbb{Z}[\sqrt{-5}]$ 上，我们有分解：

$$6=2\times 3=(1+\sqrt{-5})(1-\sqrt{-5}).$$

我们证明 $2,3,1\pm\sqrt{-5}$ 是不可约的且它们两两不伴随。我们考虑如下的范数映射：

$$N:\mathbb{Z}[\sqrt{-5}]\to\mathbb{Z},\quad x+y\sqrt{-5}\mapsto x^2+5y^2.$$

对任意的 $a,b\in A$，我们有 $N(a\cdot b)=N(a)N(b)$。特别地，如果 $a\in A$，令 $b=a^\times$，则

$$N(a)N(b)=N(1)=1.$$

由于 $N(a)$ 和 $N(b)$ 是非负整数，所以 $N(a)=1$，从而，$A^\times=\{\pm 1\}$。对以上计算稍加分析即可得出

$$N(a)=1\ \Leftrightarrow\ a\in A^\times.$$

另外，我们观察到

$$N(2)=4,\ N(3)=9,\ N(1\pm\sqrt{-5})=6$$

并且 $2,3\notin N(\mathbb{Z}[\sqrt{-5}])$，所以 $2,3,1\pm\sqrt{-5}$ 是不可约的。另外，不存在 $u\in A^\times$，使得 $u(1+\sqrt{-5})=1-\sqrt{-5}$。所以，以上元素两两不伴随。所以，$\mathbb{Z}[\sqrt{-5}]$ 不是唯一分解整环。

例子 4.15 (Gauss 整数环的应用：Fermat 的定理)**.** 我们已经证明了 $\mathbb{Z}[\sqrt{-1}]$ 是 Euclid 整环，其范数为

$$N:\mathbb{Z}[\sqrt{-1}]\longrightarrow\mathbb{Z}_{\geqslant 0},\quad N(x+y\sqrt{-1})=x^2+y^2.$$

另外，对任意 $a,b\in\mathbb{Z}[\sqrt{-1}]$，$N(a\cdot b)=N(a)N(b)$。从而，借助范数 N，我们可以计算 $\mathbb{Z}[\sqrt{-1}]^\times:a\in\mathbb{Z}[\sqrt{-1}]^\times$ 等价于 $N(a)=1$。所以，

$$\mathbb{Z}[\sqrt{-1}]^\times=\{\pm 1,\pm\sqrt{-1}\}.$$

根据 $N(a\cdot b)=N(a)N(b)$ 以及 $\mathbb{Z}[\sqrt{-1}]^\times=N^{-1}(1)$，若 $p\in\mathbb{Z}$ 是素数，$a\in\mathbb{Z}[\sqrt{-1}]$ 使得 $N(a)=p$，则 a 是 $\mathbb{Z}[\sqrt{-1}]$ 的不可约元（等价于素元）。

我们要刻画 $\mathbb{Z}[\sqrt{-1}]$ 的不可约元，这是主理想整环，只要刻画 $\mathbb{Z}[\sqrt{-1}]$ 中素理想即可。假设 $\mathfrak{p}\subset\mathbb{Z}[\sqrt{-1}]$ 是（非零）素理想，$\mathbb{Z}\subset\mathbb{Z}[\sqrt{-1}]$ 是子环，我们考虑 $\mathfrak{p}\cap\mathbb{Z}$ 是 $\mathbb{Z}$ 的非零素理想：

- 对任意的 $x+y\sqrt{-1}\in\mathfrak{p}-\{0\}$，我们有 $x^2+y^2=(x-y\sqrt{-1})(x+y\sqrt{-1})\in\mathfrak{p}\cap\mathbb{Z}$，从而，$\mathfrak{p}\cap\mathbb{Z}\neq 0$。
- $\mathfrak{p}\cap\mathbb{Z}$ 是素理想。

  我们对环同态环同态 $\mathbb{Z}\hookrightarrow\mathbb{Z}[\sqrt{-1}]$ 应用如下命题：[18]对任意环同态 $\varphi:A\to B$，$\mathfrak{p}\subset B$ 是理想，则 $\varphi^{-1}(\mathfrak{p})\subset A$ 也是理想并且若 $\mathfrak{p}$ 是素理想，则 $\varphi^{-1}(\mathfrak{p})$ 亦然。

由于 $\mathbb{Z}$ 是主理想整环，所以存在素数 p，使得 $\mathfrak{p}\cap\mathbb{Z}=(p)$。所以，每个 $\mathbb{Z}[\sqrt{-1}]$ 的素理想都与某个 $\mathbb{Z}$ 中的素数相关联。下面交换图概括了上述分析：

$$\begin{array}{ccc}\mathfrak{p} & \xrightarrow{\ \subset\ } & \mathbb{Z}[\sqrt{-1}]\\ \uparrow & & \uparrow\\ \mathfrak{p}\cap\mathbb{Z}=(p) & \xrightarrow{\ \subset\ } & \mathbb{Z}\end{array}$$

[18]证明请参考习题 XXX

由于 $N(p)=p^2$ 并且 p^2 在 $\mathbb{Z}$ 中分解方式只有 $p^2=1\cdot p^2=p\cdot p$ 两种，根据 $N(ab)=N(a)N(b)$，作为 $\mathbb{Z}[\sqrt{-1}]$ 中的元素，仅有两种可能：

- 第一，p 在 $\mathbb{Z}[\sqrt{-1}]$ 中仍不可约；
- 第二，p 在 $\mathbb{Z}[\sqrt{-1}]$ 中恰可写成两个不可约元之积。

我们现在判断 $(p)\subset\mathbb{Z}[\sqrt{-1}]$ 是否是素理想，这等价于研究 $\mathbb{Z}[\sqrt{-1}]\big/p\mathbb{Z}[\sqrt{-1}]=\mathbb{Z}[\sqrt{-1}]\big/(p)$ 是否是整环。通过复合映射

$$\mathbb{Z}\to\mathbb{Z}[\sqrt{-1}]\to\mathbb{Z}[\sqrt{-1}]\big/p\mathbb{Z}[\sqrt{-1}]$$

以及环同态的基本定理，我们得到环同态

$$\mathbb{F}_p=\mathbb{Z}\big/p\mathbb{Z}\longrightarrow\mathbb{Z}[\sqrt{-1}]\big/p\mathbb{Z}[\sqrt{-1}].$$

我们考虑环同态

$$\varphi:\mathbb{F}_p[X]\longrightarrow\mathbb{Z}[\sqrt{-1}]\big/p\mathbb{Z}[\sqrt{-1}],\quad P(X)\mapsto P(\sqrt{-1}).$$

由于 $\varphi(X^2+1)=0$，根据环同态的基本定理，我们得到

$$\psi:\mathbb{F}_p[X]\big/(X^2+1)\xrightarrow{\simeq}\mathbb{Z}[\sqrt{-1}]\big/p\mathbb{Z}[\sqrt{-1}].$$

这很明显是满射。另外，$\mathbb{F}_p[X]\big/(X^2+1)$ 有 p^2 个元素；通过研究 Gauss 整数对应的格点我们知道 $\mathbb{Z}[\sqrt{-1}]\big/p\mathbb{Z}[\sqrt{-1}]$ 也恰有 p^2 个元素，所以 φ 是环同构。

综合以上讨论，$(p)\subset\mathbb{Z}[\sqrt{-1}]$ 是素理想等价于 $\mathbb{F}_p[X]\big/(X^2+1)$ 是整环。我们有两种可能性：

- X^2+1 是 $\mathbb{F}_p[X]$ 中的不可约多项式。此时，$(X^2+1)\subset\mathbb{F}_p[X]$ 是素理想，所以 $\mathbb{F}_p[X]\big/(X^2+1)$ 是整环。此时，p 是 $\mathbb{Z}[\sqrt{-1}]$ 的素元。
- X^2+1 是 $\mathbb{F}_p[X]$ 中可约。此时必然有 $X^2+1=(X+a)(X-a)$，其中 $a^2=-1$ 且 $a\in\mathbb{F}_p$。这等价于 $-1\in\mathbb{F}_p$ 是完全平方（若 -1 不是完全平方，该 X^2+1 不可约）。另外，理想 $(X-a)$ 与 $(X+a)$ 互素（因为 $(X-a)+(X+a)=\mathbb{F}_p[X]$），根据中国剩余定理，

  $$\mathbb{F}_p[X]\big/(X^2+1)\simeq\mathbb{F}_p[X]\big/(X+a)\times\mathbb{F}_p[X]\big/(X-1).$$

  这不是整环（因为 $(1,0)\cdot(0,1)=(0,0)$），从而 p 不是 $\mathbb{Z}[\sqrt{-1}]$ 的素元。

总之，素数 p 在 $\mathbb{Z}[\sqrt{-1}]$ 中不可约当且仅当 -1 不是 $\mathbb{Z}\big/p\mathbb{Z}$ 中的完全平方。

这是初等数论中标准的二次剩余问题：假设 ξ 是循环群 ${\mathbb{F}_p}^\times$ 的生成元，则 $-1=\xi^d$，其中 $0\leqslant d<p-1$。特别地，$2d<2(p-1)$。由于 $\xi^{2d}=1$（因为 $(-1)^2=1$），所以 $p-1|2d$。根据 $2d<2(p-1)$，$2d=p-1$，即 $d=\frac{p-1}{2}$。我们分情况讨论：

- $p=2$。此时，$-1=1\in\mathbb{Z}\big/2\mathbb{Z}$ 是完全平方。
- $p\equiv1\mod4$，即 $p=4k+1$。此时，$-1=\xi^{\frac{p-1}{2}}=\xi^{2k}$ 是完全平方。
- $p\equiv3\mod4$，即 $p=4k+3$。此时，$-1=\xi^{\frac{p-2}{2}}=\xi^{2k+1}$。如果 $-1=b^2=\xi^{2l}$ 是完全平方，则 $\xi^{2k+1}=\xi^{2l}$，即 $\xi^{2k+1-2l}=1$，从而 $p-1\mid2k+1-2l$。然而 $p-1$ 是偶数，矛盾。所以，-1 不是完全平方。

综上所述，只有满足 $p \equiv 3 \mod 4$ 的素数 p 在 $\mathbb{Z}[\sqrt{-1}]$ 中仍为不可约的。

当 $p \equiv 1 \mod 4$ 时，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，$z + w\sqrt{-1} \in \{\pm, \pm\sqrt{-1}\} \cdot x - y\sqrt{-1}$。这就给出了 Fermat 的著名结果：素数 p 可写成两个完全平方数之和 $x^2 + y^2$ 当且仅当 $p \equiv 1 \mod 4$。进一步，$p = x^2 + y^2$ 的写法是唯一的。

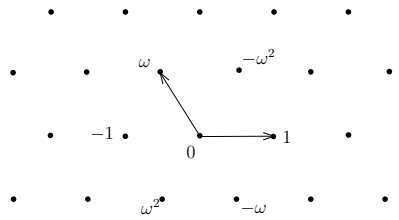
另外，交换图表

$$\begin{array}{ccc} \mathfrak{p} & \xrightarrow{\quad\subset\quad} & \mathbb{Z}[\sqrt{-1}] \\ \uparrow & & \uparrow \\ \mathfrak{p} \cap \mathbb{Z} = (p) & \xrightarrow{\quad\subset\quad} & \mathbb{Z} \end{array}$$

给出了 $\mathbb{Z}[\sqrt{-1}]$ 中所有不可约元（在伴随意义下）

$$\big\{1 + \sqrt{-1}, x \pm y\sqrt{-1}, q \big| q \equiv 3 \mod 4 \text{ 是素数}; q \equiv 3 \mod 4 \text{ 是素数且 } x^2 + y^2 = 1, x > 0, y > 0\big\}.$$

例子 4.16 (Eisenstein 整数环及其应用：$n = 3$ 时的 Fermat 大定理)**.** 令 $\omega = e^{\frac{2\pi}{3}i}$。作为集合，定义 Eisenstein 整数为 $\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\}$，这是 $\mathbb{C}$ 上的正三角形的格点集：



根据 $\omega^2 + \omega + 1 = 0$，在复数的运算下 $\mathbb{Z}[\omega]$ 是 $\mathbb{C}$ 的子环，从而是整环。

定义 $\mathbb{Z}[\omega]$ 上的范数

$$N : \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}_{\geqslant 0}, \quad N(a + b\omega) = |a + b\omega|^2.$$

实际上，我们有

$$N(a + b\omega) = a^2 - ab + b^2 = \frac{1}{4}\big((2a - b)^2 + 3b^2\big) \in \mathbb{Z}_{\geqslant 0}.$$

在 $\mathbb{Z}[\omega]$ 中，范数最小的非零元素为 $\{\pm 1, \pm\omega, \pm\omega^2\}$，其余非零元素的范数至少是 3。根据 $N(x \cdot y) = N(x)N(y)$，我们就可以断言

$$\mathbb{Z}[\omega]^\times = \{\pm 1, \pm\omega, \pm\omega^2\} \simeq \mathbb{Z}\big/6\mathbb{Z}.$$

我们现在证明 $\mathbb{Z}[\omega]$ 在范数 N 下是 Euclid 整环：注意到以每个格点为中心放置一个半径为 1 的开圆盘就可以覆盖整个复平面 $\mathbb{C}$，从而，对任意的 $z \in \mathbb{C}$，存在 $q \in \mathbb{Z}[\omega]$，使得 $|z - q| < 1$。对任意的 $a, b \in \mathbb{Z}[\omega]$，则存在 $q \in \mathbb{Z}[\omega]$，使得

$$|q - \frac{a}{b}| < 1 \quad \Leftrightarrow \quad |a - bq| < |b|.$$

令 $r = a - bq \in \mathbb{Z}[\omega]$，则 $a = q \cdot b + r$ 并且 $N(r) < N(b)$。这就证明了 $\mathbb{Z}[\omega]$ 是 Euclid 整环。[19]

[19] 同样的想法也可以用来证明 Gauss 整数环 $\mathbb{Z}[\sqrt{-1}]$ 是 Euclid 整环。

在 $\mathbb{Z}[\omega]$ 中，$1-\omega$ 是素元（因为其范数为 3）。另外，范数为 3 的元素共有 6 个，它们为 $\mathbb{Z}[\omega]^\times\cdot(1-\xi)$。尽管 3 在 $\mathbb{Z}$ 中是素数，但是它在 $\mathbb{Z}[\omega]$ 中可以分解：通过 $N(3)=9$，我们不难猜到

$$3=(1-\omega)(1-\overline{\omega})=(1-\omega)(1-\omega^2)=u(1-\omega)^2,\ \ u\in\mathbb{Z}[\omega]^\times.$$

利用 $\mathbb{Z}[\omega]$ 中的唯一分解定理，我们来证明方程 $x^3+y^3=z^3$ 的整数解必然满足 $xyz=0$。

用反证法，假设 x,y,z 均非零。不妨假设 x,y,z 两两互素（否则可以通过约掉公因子化为此情形）。注意到 x,y 在 $\mathbb{Z}$ 中互素，那么必然在 $\mathbb{Z}[\omega]$ 中互素，因为 $(x)+(y)$ 已经包含了元素 1。由于整数的三次方除 9 的余数必然是 0 或 ±1，所以，x,y,z 中必有某个数被 3 整除。通过将方程变形为 $x^3+(-z)^3=(-y)^3$，总可假设 $3\mid z$。特别地，$3\mid x+y$（因为 $3\mid x^3+y^3$ 意味着 x,y 除 3 一个余数为 1 而另一个余数为 -1）。所以，我们只要研究如下方程的非零整数解即可：

$$x^3+y^3=\left(3^kz\right)^3,\ \ k\geqslant1\text{ 且 }3\nmid z,\ \ \cdots\cdots\ (*)$$

我们可以将该方程分解为

$$(x+y)(x+\omega y)(x+\omega^2y)=\left(3^kz\right)^3.$$

由于 $3\mid x+y$，所以，$1-\omega\mid x+y$。由于 $x+\omega y-(x+y)=(1-\omega)y$，所以，$1-\omega\mid x+\omega y$；类似的，$1-\omega\mid x+\omega^2y$。所以，$1-\omega$ 是 $x+y,x+\omega y$ 和 $x+\omega^2y$ 的共约数。实际上，它还是最大公约数：对任意的公约数 w，有

$$w\mid(x+\omega y)-(x+y)=(1-\omega)y,\ \ w\mid(x+\omega y)-\omega(x+y)=(1-\omega)x.$$

由于 x 与 y 在 $\mathbb{Z}[\omega]$ 中互素，所以，$w\mid1-\omega$。实际上，这个证明表明 $x+y,x+\omega y$ 和 $x+\omega^2y$ 中任两个数的最大共约数均为 $1-\omega$。

利用 $3=(1-\omega)(1-\omega^2)$ 并且 $1-\omega$ 与 $1-\omega^2$ 伴随，我们将 $(*)$ 写成

$$(x+y)\cdot\frac{x+\omega y}{1-\omega}\cdot\frac{x+\omega^2y}{1-\omega^2}=3^{3k-1}z^3,$$

其中，以上每一个项都是 Eisenstein 整数并且左边三项两两互素（注意到 $(1-\omega)^2\mid x+y$，从而，$x+\omega y$ 与 $x+\omega^2y$ 中恰含一个 $1-\omega$ 的因子）。由于 $3\mid x+y$，根据唯一分解定理，所以

$$\begin{cases}x+y=3^{3k-1}w^3,\\ x+\omega y=(a+b\omega)^3,\end{cases}$$

其中，$a,b\in\mathbb{Z}$ 而 $w\in\mathbb{Z}[\omega]$。由于 $w^3\in\mathbb{Q}\subset\mathbb{R}$，通过考察 w 的幅角，w 落在过原点 0 和 $1,\omega$ 或 ω^2 的直线上。通过对 w 乘 ω 或 ω^2，不妨假设 $w\in\mathbb{R}$，从而，$w\in\mathbb{R}\cap\mathbb{Z}[\omega]=\mathbb{Z}$。所以，我们还可要求上面式子中的 $w\in\mathbb{Z}$。另外，我们注意到 $3\nmid w$。

利用 $\omega^2=-\omega-1$，我们计算

$$x+\omega y=(a+b\omega)^3=\left(a^3+3a^b-6ab^2+b^3\right)-(a^3+3ab^2-6a^2b+b^3).$$

所以，

$$\begin{cases}x=a^3+3a^2b-6ab^2+b^3,\\ y=-a^3-3ab^2+6a^2b-b^3.\end{cases}$$

从而，

$$3^{3k-1}w^3=x+y=9ab(a-b)\ \ \Leftrightarrow\ \ ab(a-b)=\left(3^{k-1}w\right)^3.$$

其中，上面式子左右两边每一项均为整数。由于 x, y 互素，所以，a, b 互素，从而 $a, b, a-b$ 两两互素（特别地，$a, b, a-b$ 均非零）。考虑 $(a, b, a-b, w) \to (a-b, -b, a, -w)$ 或者 $(a, b, a-b, w) \to (b-a, -a, b, w)$，根据整除与互素关系，我们不妨假设

$$a = \left(3^{k-1}z'\right)^3,\ b = (x')^3,\ a-b = (y')^3,$$

其中，$x', y', z' \in \mathbb{Z}$ 且非零。所以，

$$(x')^3 + (y')^3 = \left(3^{k-1}z'\right)^3,\ \text{且 } 3 \nmid z'.$$

以上，$3 \nmid z'$ 是因为 $3 \nmid w$。与 $(*)$ 做比较，我们总可以一直进行上述操作来降低 k，最终得到 $(*)$ 中 $k = 0$，这与先前讨论的 $3 \mid xyz$ 矛盾。

4.4 多项式环

4.4.1 可约与不可约

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 都是不可约元素且 d_i 和 e_j 是非负整数，$a \mid b$ 等价于 $d_i \leqslant e_i$，其中 $i = 1, \cdots, n$。所以，我们可定义 a 和 b 的最大公约数

$$\text{g.c.d.}(a, b) = p_1^{\min\{d_1, e_1\}}p_2^{\min\{d_2, e_2\}}\cdots p_n^{\min\{d_n, e_n\}}$$

和最小公倍数

$$\text{l.c.m.}(a, b) = p_1^{\max\{d_1, e_1\}}p_2^{\max\{d_2, e_2\}}\cdots p_n^{\max\{d_n, e_n\}}.$$

很明显，最大公约数和最小公倍数的定义在伴随的意义下唯一。对于多个元素的最大公约数和最小公倍数也可以类似的定义。

现在考虑 A-系数的多项式环。给定 $P(X) \in A[X]$，它可以被写成

$$P(X) = a_nX^n + \cdots + a_1X + a_0,$$

其中，$a_n \neq 0$。令 $c(P)$ 为 $a_0, a_1, \cdots, a_n$ 的最大公约数，那么，$c(P)$ 在伴随的意义下唯一。我们称 $c(P)$ 为多项式 P 的**容量**（content）。

引理 46. *A 是唯一分解整环，$P, Q \in A[X]$，则 $c(P)c(Q)$ 与 $c(PQ)$ 伴随。*

证明： 假设 $c(P), c(Q) \in A^\times$，先在这个特殊情形下证明引理。

我们要证明 $c(P \cdot Q) \in A^\times$，即对任意不可约元 $p \in A$，证明 $p \nmid c(P \cdot Q)$。令

$$P(X) = a_nX^n + \cdots + a_1X + a_0,\ \ Q(X) = b_mX^m + \cdots + b_1X + b_0,$$

其中，$a_n, b_m \neq 0$。由于 $c(P) \in A^\times$，则 $p \nmid c(P)$，从而存在 $0 \leqslant k_0 \leqslant n$，使得 $p \mid a_0, p \mid a_1, \cdots, p \mid a_{k_0-1}$ 但 $p \nmid a_{k_0}$；类似地，存在 $0 \leqslant l_0 \leqslant m$，使得 $p \mid b_0, p \mid b_1, \cdots, p \mid b_{l_0-1}$ 但 $p \nmid b_{l_0}$。那么，多项式 $P \cdot Q$ 中 $X^{k_0+l_0}$ 项的系数恰为

$$a_{k_0}b_{l_0} + \overbrace{\sum_{\substack{k+l=k_0+l_0,\\(k,l)\neq(k_0,l_0)}} a_kb_l}^{\text{在理想 } (p) \text{ 中}} = a_{k_0}b_{l_0} \mod (p).$$

由于 (p) 是素理想，$a_{k_0}b_{l_0} \notin (p)$，所以 p 不整除此系数。特别的，$p \nmid c(P \cdot Q)$。这就证明了 $c(P \cdot Q) \in A^\times$。

对于一般情形，我们先提取 P 和 Q 系数的最大公约数即可。 □

定理 47 (Gauss 引理)**.** *A 是唯一分解整环，$K = \mathrm{Frac}(A)$ 为其分式域。那么，$P(X) \in A[X]$ 在 $A[X]$ 中不可约[20]当且仅当 $P(X)$ 在 $K[X]$ 中不可约。*

进一步，若在 $K[X]$ 中有 $P(X) = P_1(X)P_2(X)$ 且 $\deg(P_i) \geqslant 1, i = 1, 2$，则有 $k \in K^\times$，使得 $kP_1(x), k^{-1}P_2(X) \in A[X]$。

证明: 我们选取 $P(X) \in A[X]$。由于 A 是唯一分解整环，通过提取系数的最大公约数，不妨假设 $c(P) = 1$。

如果 P 在 $K[X]$ 中可约，即 $P(X) = P_1(X)P_2(X)$，其中每个 $P_i(X) \in K[X]$ 的每个系数均形如 $\frac{a'}{a''}$，$a', a'' \in A$。先通分并提取公分母、再提取系数分子的最大公约数，$P_i(X)$ 可以被表示为如下形式：

$$P_1(X) = \frac{a'}{b'}Q_1(X), \quad P_2(X) = \frac{a''}{b''}Q_2(X),$$

其中，$Q_i(X) \in A[X]$ 并且 $c(Q_1), c(Q_2) \in A^\times$。从而，

$$P(X) = \frac{a'a''}{b'b''}Q_1(X)Q_2(X) = \frac{a'''}{b'''}Q_1(X)Q_2(X),$$

通过约分，我们可以假设 $a''' \in A$ 与 $b''' \in A$ 没有公共的不可约因子。所以，

$$b'''P = a'''Q_1(X)Q_2(X).$$

从而，

$$b''' = c(b'''P) = c\big(a'''Q_1(X)Q_2(X)\big) = a'''.$$

这表明，$a''', b''' \in A^\times$，所以，$P(X) = uQ_1(X)Q_2(X)$ 是可约。命题中的所有结论至此都得到了证明。 □

定理 48 (Gauss)**.** *若 A 是唯一分解整环，则 $A[X]$ 亦然。*

证明: 首先通过在 $K[X]$ 中工作来证明在 $A[X]$ 中分解的存在性，其中 $K = \mathrm{Frac}(A)$。

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，我们自然可以分解

$$P(X) = P_1(X) \cdots P_m(X).$$

根据 Gauss 引理，通过对以上每个多项式乘以某个 K 中的数，可假设 $P_1(X), \cdots, P_m(X)$ 是 $A[X]$ 中的多项式，这就给出了存在性。实际上，由于 $c(P) = 1$，所以，$c(P_1) \cdots c(P_m) = 1$，从而，对所有的 i，都有 $c(P_i) \in A^\times$。

再证明分解的唯一性。假设

$$P(X) = P_1(X) \cdots P_m(X) = Q_1(X) \cdots Q_n(X),$$

其中，P_i 和 Q_j 都是 $A[X]$ 中的不可约多项式并且容量为 1。通过将它们视为 $K[X]$ 中的多项式，根据 Gauss 引理，它们仍然是不可约的。从而，$m = n$ 并且通过调整脚标对任意 k，$P_k(x) = \lambda_k Q_k(X)$，其中 $\lambda_k \in K^\times$。对固定的 k，我们就有

$$a_k P_k(X) = b_k Q_k(X),$$

其中，$\lambda_k = \frac{b_k}{a_k}, a_k, b_k \in A$ 并且 a_k 和 b_k 没有公因子。通过取容量，由于 $c(P_k) = c(Q_k) = 1$，从而，$a_k = b_k \mathrm{mod} A^\times$，从而 $\lambda_k \in A^\times$。这表明 $P_k(x)$ 与 $Q_k(X)$ 伴随。至此，我们完成了证明。 □

[20] $P(X)$ 在 $A[X]$ 中不可约指的是 P 不能分解成两个次数更低的多项式之积，其中，我们要求每个多项式的次数至少是 1。

注记 4.18. 给定环同态 $\varphi : A \to B$，通过对系数作用，我们有自然的环同态

$$\Phi : A[X] \to B[X],\quad P(X) = \sum_{i=0}^{n} a_i X^i \mapsto \Phi\big(P(X)\big) = \sum_{i=0}^{n} \varphi(a_i) X^i.$$

以上将 $A[X]$ 中多项式视为 $K[X]$ 中多项式是根据同态：

$$A \to K,\ a \mapsto \frac{a}{1}.$$

例子 4.17 (判断不可约性)**.** 假设 A 是唯一分解整环，$P(X) \in A[X]$ 并且 $\deg P \leqslant 3$。若 P 可约，则必有一个 1 次的因子。从而，$P(X)$ 可约当且仅当 P 在 $K[X]$ 有根。我们可以把 P 写成 $P(X) = a_3X^3 + a_2X^2 + a_1X + a_0$，其中，$a_i \in A$。如果 $x = \frac{b}{b'} \in K$ 是 P 的根，其中，不妨假设 b 与 b' 无公因子，则

$$a_3 b^3 + a_2 b^2 b' + a_1 b b'^2 + a_0 b'^3 = 0.$$

从而，b 整除 P 的常数项系数 a_0，b' 整除 P 的首项系数 a_3。

- 考虑 $\mathbb{Z}[X]$ 中的多项式 $P(X) = X^3 + X - p$，其中 p 是素数。如果 P 可约，根据上面讨论，其根 $\frac{b}{b'}$ 只能是 ± 1 或者 $\pm p$。代入 P 计算可知，只能 $p = 2$ 并且此时 $X - 1 \mid X^3 + X - 2$；其余情形 P 不可约。
- K 是域，$f(X) \in K[X]$ 并且 $f(X)$ 不是某多项式的平方，则 $Y^2 - f(X)$ 在 $K[X, Y]$ 中不可约。

  令 $A = K[X]$，则 A 是唯一分解整环，从而，$A[Y] = K[X][Y] = K[X, Y]$ 是唯一分解整环。将 $Y^2 - f(X)$ 视为 $A[Y]$ 中的多项式，若 $Y^2 - f(X)$ 可约，则在 $A[Y]$ 中有

  $$Y^2 - f(X) = \big(h_1(X)Y - g_1(X)\big)\big(h_2(X)Y - g_2(X)\big),\quad h_i, g_i \in K[X].$$

  比较系数即有 $h_1(X), h_2(X) \in A^\times = K$，乘 K 中的数，不妨设 $h_1(X) = h_2(X) = 1$，此时，

  $$Y^2 - f(X) = \big(Y - g_1(X)\big)\big(Y - g_2(X)\big) = Y^2 - (g_1(X) + g_2(X))Y + g_1(X)g_2(X).$$

  比较系数即有 $g_1(X) + g_2(X) = 0$，从而 $f(X) = g_1(X)^2$，矛盾。

例子 4.18 (Eisenstein 判别法)**.** A 是唯一分解整环，$P(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in A[X]$，$\mathfrak{p} \subset A$ 是素理想。假设

$$a_n \notin \mathfrak{p},\ a_{n-1}, \cdots, a_1, a_0 \in \mathfrak{p},\ a_0 \notin \mathfrak{p}^2,$$

那么，$P(X)$ 在 $A[X]$（和 $K[X]$）中不可约。

用反证法。若 $P(X) = P_1(X)P_2(X)$，通过自然同态 $A[X] \to {}^{A}\!/_{\mathfrak{p}}[X]$，我们在 ${}^{A}\!/_{\mathfrak{p}}[X]$ 中工作：

$$a_nX^n = \overline{P_1}(X) \cdot \overline{P_2}(X) \quad \Rightarrow \quad \overline{P_1}(X) = bX^l,\ \overline{P_2}(X) = cX^k,\ k + l = n.$$

由于 $a_n \notin \mathfrak{p}$，$k \neq 0, l \neq 0$。上式表明 $P_1(X)$ 和 $P_2(X)$ 的常数项系数在 $\mathfrak{p}$ 中（在 ${}^{A}\!/_{\mathfrak{p}}$ 中为 0），所以 $a_0 \in \mathfrak{p}^2$。矛盾。

Eisenstein 判别法有如下经典应用：若 p 是素数，则 $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$ 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，

$$\Phi_p(X + 1) = \frac{(X + 1)^p - 1}{(X + 1) - 1} = p + \sum_{k=2}^{p} \binom{p}{k} X^{k-1}.$$

该多项式的最高项系数为 1，其余系数都被 p 整除但 p^2 不整除常数项系数。Eisenstein 判别法表明 $\Phi_p(X)$ 不可约。

4.4.2 多项式的导数

K 是域，对任意 $P(X)\in K[X]$，$P(X)=a_nX^n+\cdots+a_1X+a_0$，定义其导数为

$$P'(X)=na_nX^{n-1}+(n-1)a_{n-1}X^{n-2}+\cdots+2a_2X+a_1.$$

求导映射 $P\mapsto P'$ 显然是 K-线性的。

引理 49 (Leibniz 法则)**.** *对任意的* $P(X),Q(X)\in K[X]$，有

$$(P\cdot Q)'=P'\cdot Q+P\cdot Q'.$$

证明: 证明的关键是观察到上述等式两边分别对于 P 和 Q 均为 K-双线性的。所以，只要对 $P(X)=X^m$ 和 $Q(X)=X^n$ 验证即可：

$$(X^m\cdot X^n)'=(m+n)X^{m+n-1}=mX^{m-1}X^n+X^m\cdot nX^{n-1}.$$

这就证明了 Leibniz 法则。 □

例子 4.19. 给定域扩张 L/K，$P(X)\in K[X]$ 并且 P 在 L 中有重根，即存在 $m\geqslant 2$ 以及 $\xi\in L$，在 $L[X]$ 中，有

$$P(X)=(X-\xi)^mQ(X).$$

那么，

$$P'(X)=m(X-\xi)^{m-1}Q(X)+(X-\xi)^mQ'(X)=(X-\xi)^{m-1}\big(mQ(X)+(X-\xi)Q'(x)\big).$$

所以，P 与 P' 在 $L[X]$ 中有公因子 $X-\xi$。尽管 $X-\xi$ 可能不是 $K[X]$ 中的元素，但实际上 P 与 P' 在 $K[X]$ 中有公因子：若不然，P 与 P' 在 $K[X]$ 中互素，所以，存在 $A(X),B(X)\in K[X]$，使得

$$A(X)P(X)+B(X)P'(X)=1.$$

在 $L[X]$ 中令 $X=\xi$，上式左边为 0，矛盾。综上所述，$P(X)\in K[X]$ 若在 K 的某个 L 中有重根，则 P 与 P' 不互素。所以，如果 P 与 P' 互素，则 P 在 K 的任意扩张 L 中无重根。

4.4.3 解式与判别式

K 是域，$P(X),Q(X)\in K[X]$ 是多项式且 $\deg(P)=n,\deg(Q)=m$。令 $K[X]_{\leqslant d}$ 为次数不超过 d 的多项式所构成的线性空间，考虑 K-线性映射

$$\Phi:K[X]_{\leqslant m-1}\times K[X]_{\leqslant n-1}\longrightarrow K[X]_{\leqslant m+n-1},\quad \big(A(X),B(X)\big)\mapsto A(X)P(X)+B(X)Q(X).$$

很明显，K 的定义域和值域的维数均为 $n+m$。

我们指定 $K[X]_{\leqslant m-1}\times K[X]_{\leqslant n-1}$ 一组基：

$$\big\{e_1=(1,0),e_2=(X,0),\cdots,e_m=(X^{m-1},0),e_{m+1}=(0,1),e_{m+2}=(0,X),\cdots,e_{m+n}=(0,X^{n-1})\big\}$$

也指定 $K[X]_{\leqslant m+n-1}$ 的一组基：

$$\big\{E_1=1,E_2=X,\cdots,E_{m+n}=X^{m+n-1}\big\}.$$

对于

$$\begin{cases} P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0, \\ Q(X) = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0, \end{cases}$$

我们可以计算

$$\begin{aligned} \Phi(e_i) &= a_0 E_i + a_1 E_{i+1} + \cdots + a_n E_{i+n}, \quad 1 \leqslant i \leqslant m; \\ \Phi(e_{m+j}) &= b_0 E_j + b_1 E_{j+1} + \cdots + b_m E_{j+m}, \quad 1 \leqslant j \leqslant n. \end{aligned}$$

所以，Φ 可以表示为 $(n+m)\times(n+m)$ 的 Sylvester 矩阵：

$$M = \begin{pmatrix} a_0 & 0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & 0 & \cdots & 0 & b_1 & b_0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & 0 & \cdots & \cdots & \ddots & 0 \\ \cdots & \cdots & \cdots & \cdots & a_0 & b_{m-1} & b_{m-2} & \cdots & b_0 \\ \cdots & \cdots & \cdots & \cdots & a_1 & b_m & b_{m-1} & \cdots & b_1 \\ a_{n-1} & a_{n-2} & 0 & \cdots & \cdots & 0 & b_m & \cdots & b_2 \\ a_n & a_{n-1} & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & a_n & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \ddots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & a_n & a_{n-1} & 0 & \cdots & b_m & b_{m-1} \\ 0 & 0 & \cdots & 0 & a_n & 0 & \cdots & 0 & b_m \end{pmatrix} \tag{4.1}$$

我们定义 $\mathrm{Res}(P,Q) := \det(M)$ 并称之为 P 与 Q 的**解式**。

注记 4.19. $\mathrm{Res}(P,Q)$ 是两个多项式系数 $a_0,\cdots,a_n,b_0,\cdots,b_m$ 的整系数多项式。

可以利用结式来判断两个多项式是否互素：

命题 50. *给定多项式 $P,Q\in K[X]$，$(P,Q)=1$ 当且仅当 $\mathrm{Res}(P,Q)\neq 0$。*

证明： 注意到，Φ 是线性空间之间的同构当且仅当 $\mathrm{disc}(P,Q)\neq 0$。

如果 $\mathrm{Res}(P,Q)\neq 0$，那么 Φ 是同构。特别地，Φ 是满射，从而有 $A,B\in K[X]$，使得 $A(X)P(X)+B(X)Q(X)=1$。这表明 P 与 Q 是互素的。

如果 P 与 Q 互素，我们来说明 Φ 是同构：若不然，$\mathrm{Ker}(\Phi)\neq 0$，则存在 $A\in K[X]_{\leqslant m-1}, B\in K[X]_{\leqslant n-1}$ 使得

$$A(X)P(X)+B(X)Q(X)=0 \quad\Rightarrow\quad A(X)P(X)=-B(X)Q(X).$$

由于 P 与 Q 互素并且 Q 整除 $A\cdot P$，所以 $Q\mid A$。然而 $\deg(A)<\deg(Q)$，这表明 $A=0$，从而 $B=0$，矛盾。

综上所述，命题得证。 □

我们可用两个多项式的根计算其结式：

引理 51. *给定 $P(X)=a_n\prod_{i=1}^n(X-x_i), Q(Y)=b_m\prod_{j=1}^m(Y-y_j)$，则*

$$\mathrm{Res}(P,Q)=(-1)^{nm}a_n^m b_m^n\cdot\prod_{i=1}^n\prod_{j=1}^m(x_i-y_j). \tag{4.2}$$

证明: 根据行列式 M 的定义，不妨设 $a_n = b_m = 1$。

根据 Vieta 定理，每个 a_i 和 b_j 分别是 $\{x_1, \cdots, x_n\}$ 与 $\{y_1, \cdots, y_m\}$ 的整数系数多项式，所以 $\mathrm{Res}(P, Q)$ 是 $\{x_1, \cdots, x_n, y_1, \cdots, y_m\}$ 的整数系数多项式。现在证明 $\mathrm{Res}(P, Q)$ 是 $\{x_1, \cdots, x_n, y_1, \cdots, y_m\}$ 的齐次多项式且其次数为 $m + n$。作为行列式的，$\mathrm{Res}(P, Q)$ 的一项形如

$$M_{\sigma(1),1} M_{\sigma(2),2} \cdots M_{\sigma(m+n),m+n},$$

其中，$\sigma \in \mathfrak{S}_{n+m}$。

注意到系数 a_i 是 $n - i$ 次齐次多项式，b_j 是 $m - j$ 次齐次多项式。根据矩阵 M 的形式(4.1)，当 $k \leqslant m$ 时，$M_{\sigma(k),k}$ 的次数是 $n - \big(\sigma(k) - k\big)$；当 $k \geqslant m+1$ 时，$M_{\sigma(k),k}$ 的次数是 $m - \big(\sigma(k) - (k-m)\big)$。从而，总次数为

$$\sum_{k=1}^{m} \Big[n - \big(\sigma(k) - k\big)\Big] + \sum_{k=m+1}^{m+n} \Big[m - \big(\sigma(k) - (k-m)\big)\Big] = mn.$$

若 $x_i = y_j$，则 $A = \dfrac{Q}{X - y_j}$ 和 $B = -\dfrac{P}{X - x_j}$ 均为非零多项式并且 $A \cdot P + B \cdot Q = 0$。根据 Φ 的定义，$\mathrm{Ker}(\Phi) \neq 0$，从而 $\mathrm{Res}\big|_{x_i = y_j} = 0$。所以对所有的 i, j，均有 $x_i - y_j \mid \mathrm{Res}$，所以

$$\prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j) \mid \mathrm{Res}(x_1, \cdots, x_n, y_1, \cdots, y_m).$$

由于上面两个多项式的次数相同，所以存在 $\lambda \in K$，使得

$$\mathrm{Res}(x_1, \cdots, x_n, y_1, \cdots, y_m) = \lambda \prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j).$$

我们现在计算 λ。Res 中由对角线上的项给出的是 $a_0^m = (-1)^{nm} x_1^m \cdots x_n^m$；而乘积 $\displaystyle\prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j)$ 中这一项是 $x_1^m \cdots x_n^m$，所以 $\lambda = (-1)^{nm}$。命题得证。 □

注记 4.20. 我们将证明，对任意的 $P \in K[X]$，总有域扩张 L/K，使得若将 P 视作是 L-系数的多项式，则 P 在 L 中有 n 个根，即在 $L[X]$ 中，有 $P(X) = a_n \prod_{i=1}^{n} (X - x_i)$，其中，$x_i \in L$。

另外，对任意的 $P, Q \in K[X]$，将它们视作是 $L[X]$ 中的多项式，其结式 $\mathrm{Res}(P, Q)$ 在 L 中计算的结果与在 K 中计算的结果一致。

推论 52. 结式 $\mathrm{Res}(P, Q)$ 满足如下对称性

$$\mathrm{Res}(P, Q) = (-1)^{\deg(P) \cdot \deg(Q)} \mathrm{Res}(Q, P).$$

证明: 可以选取 K 的扩张 L/K，使得 P 和 Q 的根都落在 L 中。此时，以上公式显然成立。关于上述扩张的存在性以及选取域扩张进行证明的想法，在下一章就会变得自然且简单，这里暂且不表。

当然，直接运用矩阵 M 的表达，这个命题也是显然的。 □

推论 53. 假设在 $K[X]$ 中有 $P(X) = a_n \displaystyle\prod_{i=1}^{n} (X - x_i), Q(Y) = b_m \prod_{j=1}^{m} (Y - y_j)$，则

$$\mathrm{Res}(P, Q) = (-1)^{nm} a_n^m \prod_{i=1}^{n} Q(x_i) = b_m^n \prod_{j=1}^{m} P(y_j).$$

推论 54. *P 和 Q 在 K 的某个扩张 L/K 中有公共根当且仅当 $\mathrm{Res}(P,Q)=0$。*

证明: 如果多项式 P 和 Q 的根都落在 K 中，根据(4.2)，命题显然成立。对于一般的情形，我们只要注意到结式 $\mathrm{Res}(P,Q)$ 的计算结果不依赖于域扩张即可。 □

推论 55. *给定多项式 $P,Q,B,R\in K[X]$，其中，$P=BQ+R$ 并且 $\deg(R)<\deg(Q)$，则*

$$\mathrm{Res}(P,Q)=b_m^{n-\deg(R)}\mathrm{Res}(R,Q),$$

其中，$n=\deg(P)$ 而 b_m 为 Q 的最高次项系数。

证明: 假设 $Q(Y)=b_m\prod_{j=1}^m(Y-y_j)$，则

$$\begin{aligned}\mathrm{Res}(P,Q)&=b_m^n\prod_{j=1}^m P(y_j)=b_m^n\prod_{j=1}^m\left[(BQ)(y_j)+R(y_j)\right]\\&=b_m^n\prod_{j=1}^m R(y_j)=b_m^{n-\deg(R)}\mathrm{Res}(R,Q).\end{aligned}$$

命题得证。 □

定义 4.7 (判别式)**.** 给定 $P\in K[X]$，其**判别式**定义为

$$\mathrm{Disc}(P):=\mathrm{Res}(P,P').$$

注记 4.21. 可以判别式判别多项式 $P(X)$ 是否有重根，请参考例子4.19。

给定 n 次首一多项式 $P(X)\in K[X]$ 中，假设在 K 的扩张 L/K 中有 n 个根，即

$$P(X)=(X-\alpha_1)\cdots(X-\alpha_n),$$

其中 $\alpha_i\in L$。那么，P' 的次数为 $n-1$。根据 Leibniz 法则，我们计算

$$P'(X)=\sum_{k=1}^n(X-\alpha_1)\cdots(X-\alpha_{k-1})\overbrace{(X-\alpha_k)}^{\text{缺失}}(X-\alpha_{k+1})\cdots(X-\alpha_n).$$

从而，$P'(\alpha_i)=\prod_{j\neq i}(\alpha_i-\alpha_j)$。所以，

$$\begin{aligned}\mathrm{Disc}(P)=\mathrm{Res}(P,P')&=(-1)^{n(n-1)}\prod_{i=1}^n P'(\alpha_i)\\&=(-1)^{n(n-1)}\prod_{i\neq j}(\alpha_i-\alpha_j)=(-1)^{\frac12 n(n-1)}\prod_{i<j}(\alpha_i-\alpha_j)^2.\end{aligned}$$

所以，对首一多项式而言，

$$\boxed{\mathrm{Disc}(P)=(-1)^{\frac12 n(n-1)}\prod_{i<j}(\alpha_i-\alpha_j)^2.}\tag{4.3}$$

这说明 $\mathrm{Disc}(P)=0$ 等价于 P 有重根。

例子 4.20. $P(X)=aX^2+bX+c$ 是二次多项式，则 $P'(X)=2aX+b$。根据定义，有

$$\mathrm{Disc}(P)=\det\begin{pmatrix}c&b&0\\b&2a&b\\a&0&2a\end{pmatrix}=a(4ac-b^2).$$

例子 4.21. $P(X)=X^3+pX+q$ 是三次多项式，则 $P'(X)=3X^2+p$。根据定义，有

$$\mathrm{Disc}(P)=\det\begin{pmatrix} q & 0 & p & 0 & 0\\ p & q & 0 & p & 0\\ 0 & p & 3 & 0 & p\\ 1 & 0 & 0 & 3 & 0\\ 0 & 1 & 0 & 0 & 3\end{pmatrix}=4p^3+27p^2.$$

例子 4.22. $P(X)=X^n+aX+b$ 是 n 次多项式，则 $P'(X)=nX^{n-1}+a$。使用行列式进行计算的可行性很低，我们转而利用结式的性质进行化简。首先，

$$\mathrm{Disc}(P)=n^{n-1}\mathrm{Res}(P,X^{n-1}+\frac{a}{n}).$$

假设 $\alpha_1,\cdots,\alpha_{n-1}$ 是 $X^{n-1}+\frac{a}{n}$ 的 $n-1$ 个根，则

$$\begin{aligned}\mathrm{Disc}(P)&=n^{n-1}\prod_{j=1}^{n-1}P(\alpha_j)=n^n\prod_{j=1}^{n-1}(\alpha_j^n+a\alpha_j+b)\\&=n^{n-1}\prod_{j=1}^{n-1}\big(-\frac{a}{n}\alpha_j+a\alpha_j+b\big)=n^{n-1}\left(\frac{n-1}{n}a\right)^{n-1}\prod_{j=1}^{n-1}\big(\alpha_j+\frac{n}{n-1}\frac{b}{a}\big)\\&=n^{n-1}\left(-\frac{n-1}{n}a\right)^{n-1}\prod_{j=1}^{n-1}\big(-\frac{n}{n-1}\frac{b}{a}-\alpha_j\big)=n^{n-1}\left(-\frac{n-1}{n}a\right)^{n-1}P'(-\frac{n}{n-1}\frac{b}{a})\\&=n^{n-1}\left(-\frac{n-1}{n}a\right)^{n-1}\left(n\big(-\frac{n}{n-1}\frac{b}{a}\big)^{n-1}+a\right)\\&=n^nb^{n-1}+(-1)^{n-1}(n-1)^{n-1}a^n.\end{aligned}$$

4.4.4 对称多项式

考虑环 A 上的多项式环 $A[X_1,\cdots,X_n]$，对称群 $\mathfrak{S}_n$ 可以在 $A[X_1,\cdots,X_n]$ 上作用：

$$\mathfrak{S}_n\times A[X_1,\cdots,X_n]\to A[X_1,\cdots,X_n],\quad \big(g,P\big)\mapsto(g\cdot P)(X_1,\cdots,X_n)=P(X_{g(1)},\cdots,X_{g(n)}).$$

对多项式 $P\in A[X_1,\cdots,X_n]$，若对任意 $g\in\mathfrak{S}_n$，$g\cdot P=P$，则称 P 是**对称多项式**。我们用 $A[X_1,\cdots,X_n]^{\mathfrak{S}_n}$ 表示全体 A-系数的对称多项式，不难看出，$A[X_1,\cdots,X_n]^{\mathfrak{S}_n}$ 是 $A[X_1,\cdots,X_n]$ 的子环。我们的目标是确定 $K[X_1,\cdots,X_n]^{\mathfrak{S}_n}$ 的代数结构，其中，K 是域。

例子 4.23. 以下 n 个整系数多项式被称作是**基本对称多项式**：

$$\begin{cases}\sigma_1=\sum_i X_i,\\ \sigma_2=\sum_{i<j}X_iX_j,\\ \cdots\\ \sigma_k=\sum_{i_1<i_2<\cdots<i_k}X_{i_1}X_{i_2}\cdots X_{i_k},\\ \cdots\\ \sigma_n=X_1\cdots X_n.\end{cases}$$

给定 n 元整数指标 $I=(i_1,\cdots,i_n)$，其中，$i_1\geqslant i_2\geqslant\cdots\geqslant i_n\geqslant 0$，定义

$$\mathrm{Stab}(I)=\left\{g\in\mathfrak{S}_n\middle|g\cdot X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}=X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}\right\}$$

以及

$$S_I=\sum_{g\in\mathfrak{S}_n/\mathrm{Stab}(I)}g\cdot(X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}).$$

以上的求和中，$g\in\mathfrak{S}_n/\mathrm{Stab}(I)$ 可以被理解为每个陪集在 $\mathfrak{S}_n$ 中的代表元。

例子 4.24. 若 $I=(1,0,\cdots,0)$，则对换 $(1,2),\cdots,(1,n)$ 和 1 可以作为左陪集 $\mathfrak{S}_n/\mathrm{Stab}(I)$ 的代表元，从而，

$$S_{(1,0,\cdots,0)}=X_1+\sum_{k=2}^{n}(1,k)\cdot X_1=\sigma_1.$$

若 $I=(1,1,\cdots,1)$，则 $\mathrm{Stab}(I)=\mathfrak{S}_n$，从而，$\mathfrak{S}_n/\mathrm{Stab}(I)$ 只有一个代表元 1。那么，

$$S_{(1,1,\cdots,1)}=X_1X_2\cdots X_n=\sigma_n.$$

注记 4.22. 以上求和之所以要商掉 $\mathrm{Stab}(I)$ 是因为要避免重复的系数，比如说，对 $I=(1,1,\cdots,1)$，

$$\sum_{g\in\mathfrak{S}_n/\mathrm{Stab}(I)}g\cdot(X_1X_2\cdots X_n)=n!\cdot\sigma_n.$$

再例如当 $n=3$ 时候，考虑 $I=(2,1,1)$，则 $\mathrm{Stab}(I)=\{1,(2,3)\}$。从而，

$$S_I=X_1^2X_2X_3+X_2^2X_1X_3+X_3^2X_1X_2.$$

然而

$$\sum_{g\in\mathfrak{S}_3}g\cdot(X_1^{i_1}X_2^{i_2}X_3^{i_3})=2\big(X_1^2X_2X_3+X_2^2X_1X_3+X_3^2X_1X_2\big).$$

命题 56. *对任意的 n 元整数指标 $I=(i_1,\cdots,i_n)$，有 $S_I\in A[X_1,\cdots,X_n]^{\mathfrak{S}_n}$。进一步，每个 S_I 恰好包含 $\left|\mathfrak{S}_n/\mathrm{Stab}(I)\right|$ 个单项式，每个这样的单项式的系数恰为 1。*

证明: 对任意的 $g'\in\mathfrak{S}_n$，有

$$g'\cdot S_I=\sum_{g\in\mathfrak{S}_n/\mathrm{Stab}(I)}g'g\cdot(X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n})=\sum_{g'g\in\mathfrak{S}_n/\mathrm{Stab}(I)}g'g\cdot(X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}).$$

当 g 取遍 $\mathfrak{S}_n/\mathrm{Stab}(I)$ 的任一组代表元时，$g'g$ 也取遍 $\mathfrak{S}_n/\mathrm{Stab}(I)$ 的一组代表元。所以，$g'\cdot S_I=S_I$。 □

引理 57. *对任意的 $P\in A[X_1,\cdots,X_n]^{\mathfrak{S}_n}$，存在有限个指标 I 以及 $a_I\in A$，使得*

$$P=\sum_{\text{有限}}a_I\cdot S_I.$$

证明: 考虑 P 的一个单项式 $a_IX_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$，其中，$a_I\neq 0$。对任意 $g\in\mathfrak{S}_n$，$a_IX_{g(1)}^{i_1}X_{g(2)}^{i_2}\cdots X_{g(n)}^{i_n}$ 也是 P 中的一个单项式。据此，不妨假设 $i_1\geqslant i_2\geqslant\cdots\geqslant i_n$ 并且 I 为对应的 n 元整数指标。特别地，

$$a_IS_I=\sum_{g\in\mathfrak{S}_n/\mathrm{Stab}(I)}a_I\cdot(X_{g(1)}^{i_1}X_{g(2)}^{i_2}\cdots X_{g(n)}^{i_n})$$

中的每一项都作为 P 中的单项式出现，从而，$P-a_IS_I$ 是单项式个数较少的对称多项式。重复这个过程就可以将 P 写成 $\sum_{\text{有限}}a_I\cdot S_I$ 的形式。 □

注记 4.23. 对于 n 元整数指标 $I=(i_1,\cdots,i_n)$ 和 $J=(j_1,\cdots,j_n)$，用**字典序**可以比较它们的大小，即

$$I<J \quad\Leftrightarrow\quad \text{存在 } k\leqslant n,\ \text{使得 } i_1=j_1,\cdots,i_{k-1}=j_{k-1} \text{ 而 } i_k<j_k.$$

特别地，对任意的两个不同的 n 元整数指标 I 和 J，$I<J$ 或 $I>J$ 二者必居其一。

引理 58. *对任意的 n 元整数指标 I 和 J，我们有*

$$S_I\cdot S_J=S_{I+J}+\sum_{K<I+J}a_K\cdot S_K,$$

其中，$I+J=(i_1+j_1,\cdots,i_n+j_n)$，$K$ 为 n 元整数指标而 $a_K\in A$。

证明: 对于 $I=(i_1,\cdots,i_n)$ 和 $J=(j_1,\cdots,j_n)$，$X_1^{i_1}\cdots X_n^{i_n}$ 和 $X_1^{j_1}\cdots X_n^{j_n}$ 分别是 S_I 和 S_J 中出现的最大指标的单项式，从而，$X_1^{i_1+j_1}\cdots X_n^{i_n+j_n}$ 是 $S_I\cdot S_J$ 中出现的最大指标的单项式。根据引理57的证明，S_{I+J} 的每一项都恰在 $S_I\cdot S_J$ 中出现一次并且其余项对应的指标都严格小于 $I+J$，所以，$S_I\cdot S_J-S_{I+J}$ 形如 $\sum_{K<I+J}a_K\cdot S_K$。 □

定理 59. *每个对称多项式 $P\in A[X_1,\cdots,X_n]^{\mathfrak{S}_n}$ 可唯一地表示成 $\sigma_1,\cdots,\sigma_n$ 的多项式，即*

$$A[X_1,\cdots,X_n]^{\mathfrak{S}_n}=A[\sigma_1,\cdots,\sigma_n].$$

证明: 只要证明对每个 n 元整数指标 I，S_I 可写成 $\sigma_1,\cdots,\sigma_n$ 的 A-系数多项式，那么，每个对称多项式亦然。我们对 I 根据字典序进行归纳：最小的 I 是 $(1,0,\cdots,0)$，此时 $S_I=\sigma_1$，命题显然成立。给定 n 元整数指标 K，假设对任意 $I<K$，S_I 可表示成 $\sigma_1,\cdots,\sigma_n$ 的多项式。我们首先把 K 写成

$$K=I+(1,\cdots,1,0,\cdots,0)=I+J,\ \ I<K,\ J=(\underbrace{1,\cdots,1}_{\text{k}},0,\cdots,0).$$

注意到 $S_J=\sigma_k$。根据上一引理，我们有

$$S_K=S_{I+J}=S_I\cdot\sigma_k+\sum_{K'<I+J}a_{K'}\cdot S_{K'}.$$

右边每一项均为 $\sigma_1,\cdots,\sigma_n$ 的多项式，所以 S_K 也是。这就完成了归纳假设的证明。

现在证明对任意 $P\in A[X_1,\cdots,X_n]^{\mathfrak{S}_n}$，存在唯一的 $Q\in A[Y_1,\cdots,Y_n]$，使得

$$P(X_1,\cdots,X_n)=Q(\sigma_1,\cdots,\sigma_n).$$

对任意指标 $\alpha=(\alpha_1,\cdots,\alpha_n)$，其中，$\alpha_1,\cdots,\alpha_n\geqslant 0$，定义 n 元整数指标 $I(\alpha)$ 为

$$I(\alpha)=(\alpha_1+\alpha_2+\cdots+\alpha_n,\alpha_1+\alpha_2+\cdots+\alpha_{n-1},\cdots,\alpha_1).$$

那么，

$$\sigma_1^{\alpha_1}\sigma_2^{\alpha_2}\cdots\sigma_n^{\alpha_n}=S_{I(\alpha)}+\sum_{I<I(\alpha)}a_I\cdot S_I.$$

如果存在另一个 $Q'\in A[Y_1,\cdots,Y_n]$，使得 $P(X_1,\cdots,X_n)=Q'(\sigma_1,\cdots,\sigma_n)$。为了说明 $Q=Q'$，只要对任意 $G\in A[Y_1,\cdots,Y_n]-\{0\}$，证明 $G(\sigma_1,\cdots,\sigma_n)$ 在 $A[X_1,\cdots,X_n]$ 中非零即可（取 $G=Q-Q'$）。实际上，我们把 G 写成

$$G(Y_1,\cdots,Y_n)=\sum_{\alpha=(\alpha_1,\cdots,\alpha_n)}a_\alpha\cdot Y^\alpha$$

其中，$a_\alpha\neq 0$。选择这样的指标 α，使得 $I(\alpha)$ 在字典序下最大。那么，当我们把 $G(\sigma_1,\cdots,\sigma_N)$ 写成 $\sum_{\text{有限}}a_I\cdot S_I$ 的形式时，$S_{I(\alpha)}$ 的系数非零。从而，$G(\sigma_1,\cdots,\sigma_n)\neq 0$。 □

例子 4.25. K 是域，$K(X_1,\cdots,X_n)=\mathrm{Frac}(K[X_1,\cdots,X_n])$ 为多项式环 $K[X_1,\cdots,X_n]$ 的分式域。由于 $K[X_1,\cdots,X_n]$ 是唯一分解整环，通过约去公因子，每个 $K(X_1,\cdots,X_n)$ 中的元素 $f(X_1,\cdots,X_n)$ 都可唯一写成 $\frac{P(X_1,\cdots,X_n)}{Q(X_1,\cdots,X_n)}$ 的形式，其中，P 和 Q 在 $K[X_1,\cdots,X_n]$ 中互素并且 Q 是首一的。对称群 $\mathfrak{S}_n$ 可以在 $K(X_1,\cdots,X_n)$ 上作用：

$$\mathfrak{S}_n\times K(X_1,\cdots,X_n)\to K(X_1,\cdots,X_n),\quad \big(g,f\big)\mapsto (g\cdot f)(X_1,\cdots,X_n)=f(X_{g(1)},\cdots,X_{g(n)}).$$

很明显，$(g\cdot f)(X_1,\cdots,X_n)=\dfrac{g\cdot P}{g\cdot Q}$。很明显，$g\cdot P$ 和 $g\cdot Q$ 在 $K[X_1,\cdots,X_n]$ 中也互素并且 $g\cdot Q$ 也是首一的。所以，

$$g\cdot f=f\quad\Leftrightarrow\quad\frac{g\cdot P}{g\cdot Q}=\frac{P}{Q}\quad\Leftrightarrow\quad Q\cdot(g\cdot P)=P\cdot(g\cdot Q).$$

通过整除关系，我们必然有 $Q=g\cdot Q$，从而，$P=g\cdot P$。特别地，$P,Q\in K[X_1,\cdots,X_n]^{\mathfrak{S}_n}=K[\sigma_1,\cdots,\sigma_n]$。

令

$$K(X_1,\cdots,X_n)^{\mathfrak{S}_n}=\big\{f\in K(X_1,\cdots,X_n)\big|\text{对任意的 } g\in\mathfrak{S}_n,g\cdot f=f\big\},$$

那么，上面的推理表明

$$K(X_1,\cdots,X_n)^{\mathfrak{S}_n}=K(\sigma_1,\cdots,\sigma_n).$$

例子 4.26 (判别式)**.** 令 $\Delta=\prod\limits_{i<j}(X_i-X_j)$，则 $g\cdot\Delta=\varepsilon(g)\Delta$，其中，$\varepsilon:\mathfrak{S}_n\to\{\pm1\}$ 是指标映射。

考虑交错群 $\mathfrak{A}_n$ 在 $A[X_1,\cdots,X_n]$ 上作用：

$$\mathfrak{A}_n\times A[X_1,\cdots,X_n]\to A[X_1,\cdots,X_n],\quad \big(g,P\big)\mapsto (g\cdot P)(X_1,\cdots,X_n)=P(X_{g(1)},\cdots,X_{g(n)}).$$

令

$$A[X_1,\cdots,X_n]^{\mathfrak{A}_n}=\big\{P\in A[X_1,\cdots,X_n]\big|\text{对任意的 } g\in\mathfrak{A}_n,g\cdot P=P\big\},$$

这也是 $A[X_1,\cdots,X_n]$ 的子环。由于 $\varepsilon(\mathfrak{A}_n)=1$，所以，$\Delta\in A[X_1,\cdots,X_n]^{\mathfrak{A}_n}$。

另外，我们显然有 $\Delta^2\in A[X_1,\cdots,X_n]^{\mathfrak{S}_n}$ 是对称多项式，所以可以被表示为 $\sigma_1,\cdots,\sigma_n$ 的多项式。根据(4.3)，将 $X_1,\cdots,X_n$ 想象成

$$P(X)=(X-X_1)(X-X_2)\cdots(X-X_n)=X^n-\sigma_1X^{n-1}+\cdots+(-1)^{n-1}\sigma_{n-1}X+(-1)^n\sigma_{n-1}$$

的根，那么

$$\Delta^2=(-1)^{\frac{1}{2}n(n-1)}\mathrm{Disc}(P)\big(-\sigma_1,\sigma_2,\cdots,(-1)^k\sigma_k,\cdots,(-1)^n\sigma_n\big).$$

其中，对于首一多项式 $P=X^m+\sum_{i=0}^{n-1}a_iX^i$，$\mathrm{Disc}(a_{n-1},\cdots,a_0)$ 是 $\{a_0,\cdots,a_{n-1}\}$ 的整系数多项式。

作为结论，给定首一多项式：

$$P(X)=(X-x_1)(X-x_2)\cdots(X-x_n)=X^n+b_1X^{n-1}+\cdots+b_n.$$

其中，对 $1\leqslant k\leqslant n$，$b_k=(-1)^k\sigma_k$，令

$$\mathrm{disc}(P):=\Delta^2(b_1,\cdots,b_n)=\prod_{i\neq j}(x_i-x_j)^2.$$

之前定义的判别式为

$$\mathrm{Disc}(P)=\prod_{i\neq j}(x_i-x_j).$$

所以，

$$\mathrm{disc}=(-1)^{\frac{n(n-1)}{2}}\mathrm{Disc}(P).$$

判别式的意义在于利用它是否为零来断定 P 是否有重根。

例子 4.27. K 是域，我们计算 $K[X_1,\cdots,X_n]^{\mathfrak{A}_n}$。

由于 $\mathfrak{A}_n$ 是 $\mathfrak{S}_n$ 的子群，所以，$K[X_1,\cdots,X_n]^{\mathfrak{S}_n}\subset K[X_1,\cdots,X_n]^{\mathfrak{A}_n}$。对任意 $g\in\mathfrak{S}_n$ 和 $P\in K[X_1,\cdots,X_n]^{\mathfrak{A}_n}$，我们有 $g\cdot P\in K[X_1,\cdots,X_n]^{\mathfrak{A}_n}$：只要验证对任意 $h\in\mathfrak{A}_n$，$h\cdot(g\cdot P)=g\cdot P$ 即可，而这等价于 $\left(g^{-1}hg\right)\cdot P=P$。由于 $\mathfrak{A}_n\lhd\mathfrak{S}_n$，以上显然成立。据此，我们得到自然的群作用：

$$\mathfrak{S}_n\times K[X_1,\cdots,X_n]^{\mathfrak{A}_n}\longrightarrow K[X_1,\cdots,X_n]^{\mathfrak{A}_n}.$$

由于 $\mathfrak{A}_n$ 的作用是平凡的，我们自然有

$$\mathfrak{S}_n\diagup\mathfrak{A}_n\times K[X_1,\cdots,X_n]^{\mathfrak{A}_n}\longrightarrow K[X_1,\cdots,X_n]^{\mathfrak{A}_n},$$

其中，对任意的 $g\in\mathfrak{S}_n-\mathfrak{A}_n$，$g\cdot P$ 不依赖于 g 的选取（它们都对应着 $\mathfrak{S}_n\diagup\mathfrak{A}_n$ 中同一个左陪集）并且 $g^2\cdot P=P$。

对任意的 d，令 $K[X_1,\cdots,X_n]_d^{\mathfrak{A}_n}$ 为 $A[X_1,\cdots,X_n]^{\mathfrak{A}_n}$ 中 d 次齐次的多项式，由于以上作用保持次数，我们自然有

$$K[X_1,\cdots,X_n]^{\mathfrak{A}_n}=\bigoplus_{d\geqslant 0}K[X_1,\cdots,X_n]_d^{\mathfrak{A}_n}$$

每个 $K[X_1,\cdots,X_n]_d^{\mathfrak{A}_n}$ 均为有限维 K-线性空间，现在对 $g\in\mathfrak{S}_n-\mathfrak{A}_n$，考虑线性映射

$$g:K[X_1,\cdots,X_n]_d^{\mathfrak{A}_n}\longrightarrow K[X_1,\cdots,X_n]_d^{\mathfrak{A}_n},\quad P\mapsto g\cdot P.$$

由于 $g^2=1$，那么，

$$K[X_1,\cdots,X_n]_d^{\mathfrak{A}_n}=V_d^+\oplus V_d^-,$$

其中，V_d^+ 和 V_d^- 分别为特征值为 1 和 -1 的特征子空间。根据定义，

$$V_d^+=K[X_1,\cdots,X_n]_d^{\mathfrak{S}_n},$$

即 d 次齐次对称多项式。对任意的 $P\in V_d^-$，有 $g\cdot P=-P$，所以对换 $(i,j)\in\mathfrak{S}_n$ 的作用为

$$P(X_1,\cdots,X_i,\cdots,X_j,\cdots,X_n)=-P(X_1,\cdots,X_j,\cdots,X_i,\cdots,X_n).$$

特别地，令 $X_i=X_j$，则 $P(X_1,\cdots,X_j,\cdots,X_j,\cdots,X_n)$，即 X_i-X_j 整除 P。特别地，当我们取遍所有可能的 i,j 时，就证明了 $\Delta\mid P$。由于 $g\cdot\Delta=-\Delta$，所以，多项式 $Q=\dfrac{P}{\Delta}\in K[X_1,\cdots,X_n]^{\mathfrak{S}_n}$。据此，我们证明了

$$K[X_1,\cdots,X_n]^{\mathfrak{A}_n}=\left\{P+Q\cdot\Delta\middle|P,Q\in K[\sigma_1,\cdots,\sigma_n]\right\}.$$

例子 4.28 (Newton 公式)**.** 令 $S_k=X_1^k+\cdots+X_n^k$，这是对称对多项式，所以 S_k 是 $\sigma_1,\cdots,\sigma_n$ 的多项式。为了具体的计算出 S_k，我们可以利用著名的 Newton 公式：

$$S_k-\sigma_1S_{k-1}+\sigma_2S_{k-2}-\cdots+(-1)^{k-1}\sigma_{k-1}S_1+k(-1)^k\sigma_k=0,$$

其中，当 $k>n$ 时，规定 $\sigma_k=0$。由于 $S_1=\sigma_1$，我们可递归地计算所有的 $S_k\in A[\sigma_1,\cdots,\sigma_n]$。特别地，$S_k$ 为 $\sigma_1,\cdots,\sigma_n$ 的整系数多项式。

我们对 $k\geqslant n$ 的情形证明 Newton 公式。考虑 $K[X_1,\cdots,X_n][Y]$ 中的多项式

$$P(Y)=(Y-X_1)(Y-X_2)\cdots(Y-X_n)=Y^n-\sigma_1Y^{n-1}+\cdots+(-1)^{n-1}\sigma_{n-1}Y+(-1)^n\sigma_n.$$

从而，$P(X_j)=0$，即

$$X_j^n-\sigma_1X_j^{n-1}+\cdots+(-1)^{n-1}\sigma_{n-1}X_j+(-1)^n\sigma_n=0.$$

对 j 求和，我们就证明了

$$S_n-\sigma_1S_{n-1}+\sigma_2S_{n-2}-\cdots+(-1)^{n-1}\sigma_{n-1}S_1+n(-1)^n\sigma_n=0.$$

如果 $k>n$，对 $P(X_j)=0$ 乘以 X_j^{k-n} 就给出

$$X_j^k-\sigma_1X_j^{k-1}+\cdots+(-1)^{n-1}\sigma_{n-1}X_j^{k-n+1}+(-1)^n\sigma_nX_j^{k-n}=0.$$

对 j 求和也给出了 Newton 公式（其最后几项均为 0）。

现在假设 $k<n$。我们计算 σ_iS_{k-i}, 其中, $1\leqslant i\leqslant k-2$。考虑给定 n 元整数指标 $I_i=(\underbrace{1,\cdots,1}_{i\text{ 个}},0,\cdots,0)$ 和 $I'_{k-i}=(k-i,0,\cdots,0)$。那么，

$$\begin{aligned}\sigma_iS_{k-i}=S_{I_i}\cdot S_{I'_{k-i}}&=\Big(\sum X_1\cdots X_i+\cdots\Big)\Big(\sum X_1^{k-i}\Big)\\&=\sum X_1^{k-i+1}\cdots X_i+\sum X_1^{k-i}X_2\cdots X_iX_{i+1}=S_{J_i}+S_{J'_i},\end{aligned}$$

其中，$J_i=(k-(i-1),\underbrace{1,\cdots,1}_{i-1\text{ 个}},0,\cdots,0),J_i=(k-i,\underbrace{1,\cdots,1}_{i\text{ 个}},0,\cdots,0)$。

当 $i=k-1$ 时，以上计算要稍作修改：

$$\begin{aligned}&\sigma_{k-1}S_1\Big(\sum X_1\cdots X_{k-1}+\cdots\Big)\Big(\sum X_1\Big)\\&\quad=\sum X_1^2X_2\cdots X_{k-1}+k\sum X_1X_2\cdots X_iX_{i+1}=S_{J_{k-2}}+kS_{J_{k-1}},\end{aligned}$$

其中，$J_i=(k-(i-1),\underbrace{1,\cdots,1}_{i-1\text{ 个}},0,\cdots,0),J_i=(k-i,\underbrace{1,\cdots,1}_{i\text{ 个}},0,\cdots,0)$ 由于 $S_k=S_{J_0}$ 所以，

$$\begin{aligned}&S_k-\sigma_1S_{k-1}+\sigma_2S_{k-2}-\cdots+(-1)^{k-1}\sigma_{k-1}S_1+k(-1)^k\sigma_k\\=&S_{J_0}-\big(S_{J_0}+S_{J_1}\big)+\big(S_{J_1}+S_{J_2}\big)+(-1)^{k-1}\big(S_{J_{k-2}}+kS_{J_{k-1}}\big)+k(-1)^k\sigma_k\\=&(-1)^{k-1}k\left(S_{J_{k-1}}-\sigma_k\right)=0.\end{aligned}$$

这就完成了 Newton 公式的证明。

4.5 主理想整环上的有限生成模

先简要回忆模的定义，请参考2.5节。A 是环（未必交换），(左)A-模 M 指的是交换群 $(M,+)$ 以及乘法映射

$$A\times M\to M,\ \ (a,m)\mapsto a\cdot m,$$

使得对任意的 $a,a'\in A$ 和 m,m'，有

$$\begin{aligned}&1\cdot m=m,\ \ a\cdot(a'\cdot m)=(a\cdot a')\cdot m,\\&a\cdot(m+m')=a\cdot m+a\cdot m',\ \ (a+a')\cdot m=a\cdot m+a'\cdot m,\end{aligned}$$

M 的加法子群 N 如果对 A 的乘法封闭，则 N 为 M 的子模。

例子 4.29. A 是环，那么，A 对自身的乘法使得 A 成为 A-模。按定义，$I \subset A$ 是子模当且仅当 I 是 A 的（左）理想。

更多的例子请参考2.5节。

给定 A-模 M_1, M_2，它们之间的 A-模同态指的是加法群同态 $\varphi : M_1 \to M_2$ 并且对任意 $a \in A$ 和 $m \in M_1$，有

$$\varphi(a \cdot m) = a \cdot \varphi(m).$$

同态的核定义为 $\mathrm{Ker}(\varphi) := \big\{m \in M_1 \big| \varphi(m) = 0\big\}$。它是 M_1 的子模且 φ 是单射当且仅当 $\mathrm{Ker}(\varphi) = \{0\}$。

给 A-模 M 及其子模 N，我们还可以定义商模 $M/N = \big\{m + N \big| m \in M\big\}$，其中 $a(m+N) := am + N$。商映射

$$\pi : M \to M/N, \quad m \mapsto m + N.$$

是满的 A-模同态。特别地，我们有所谓的同态定理，请参考命题13：M 和 M' 是 A-模，$N \subset M$ 是子模，$\varphi : M \to M'$ 是 A-模同态。若 $N \subset \mathrm{Ker}(\varphi)$，则有唯一的 A-模同态 $\overline{\varphi} : M/N \to M'$，使得 $\overline{\varphi} \circ \pi = \varphi$，即

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & M' \\ \downarrow{\scriptstyle \pi} & \nearrow_{\overline{\varphi}} & \\ M/N & & \end{array}$$

进一步，我们还有 A-模同构 $\overline{\varphi} : M/\mathrm{Ker}(\varphi) \xrightarrow{\simeq} \mathrm{Im}(\varphi)$。

注记 4.24. 与商群的情形类似（证明完全一致），我们有如下的一一对应：

$$\big\{M \text{ 的子模 } N' \supset N\big\} \xrightarrow{1:1} \big\{M/N \text{ 的子模 } \overline{N'}\big\}, \quad N' \mapsto N'/N.$$

4.5.1 有限生成模与 Noether 性

以下总假设 A 是交换环。

给定一族 A-模 $\big\{M_i\big\}_{i \in I}$，那么 $\prod\limits_{i \in I} M_i$ 具有 A-模结构：

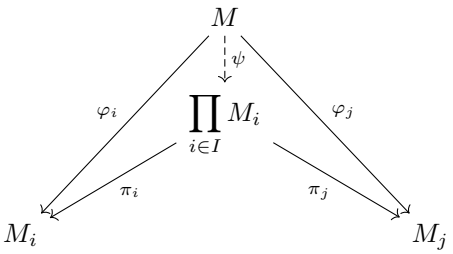
$$A \times \prod_{i \in I} M_i \to \prod_i M_i, \quad \big(a, (m_i \in M_i)_{i \in I}\big) \mapsto (a \cdot m_i)_{i \in I}.$$

它被称作是 $\big\{M_i\big\}_{i \in I}$ 的**乘积**。对每个指标 $i_0 \in I$，投影映射

$$\pi_{i_0} : \prod_i M_i \to M_{i_0}, \quad (m_i)_{i \in I} \mapsto m_{i_0}.$$

是 A-模同态。

$\prod\limits_{i \in I} M_i$ 具有以下的泛性质：



对任意 A-模 M 和任意一族 A-模同态 $\varphi_i : M \to M_i$，其中 $i \in I$，存在唯一的 A-模同态 $\psi : M \to \prod_{i\in I} M_i$，使得对任意的 $i \in I$，$\pi_i \circ \psi = \varphi_i$，即

$$\prod_{i\in I} \mathbf{Hom}_A(M, M_i) = \mathbf{Hom}_A\left(M, \prod_{i\in I} M_i\right).$$

证明请参考习题2.7.1。

我们还可构造 $\{M_i\}_{i\in I}$ 的**直和** $\bigoplus_{i\in I} M_i$。作为集合，令

$$\bigoplus_{i\in I} M_i = \{(m_i)_{i\in I} \in \prod_{i\in I} M_i | \text{除有限个 } i \text{ 外，其余 } m_i \text{ 均为 } 0\}.$$

那么，$\bigoplus_{i\in I} M_i$ 的 A-模结构定义为

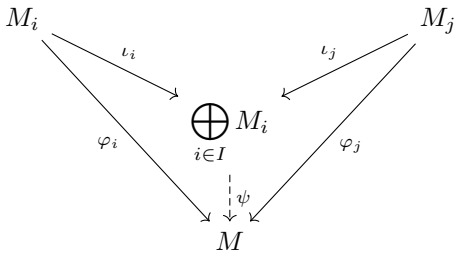
$$A \times \bigoplus_{i\in I} M_i \to \bigoplus_{i\in I} M_i, \quad \big(a, (m_i \in M_i)_{i\in I}\big) \mapsto (a \cdot m_i)_{i\in I}.$$

对每个指标 $i_0 \in I$，我们有嵌入映射

$$\iota_{i_0} : M_{i_0} \to \bigoplus_{i\in I} M_i \quad m_{i_0} \mapsto (, 0, \cdots, 0, m_{i_0}, 0 \cdots).$$

这是 A-模同态。

$\bigoplus_{i\in I} M_i$ 也具泛性质：



对任意 A-模 M 和任意一族 A-模同态 $\varphi_i : M_i \to M$，其中 $i \in I$，存在唯一的 A-模同态 $\psi : \bigoplus_{i\in I} M_i \to M$，使得对任意的 $i \in I$，$\psi \circ \iota_i = \varphi_i$，即

$$\prod_{i\in I} \mathbf{Hom}_A(M_i, M) = \mathbf{Hom}_A\left(\bigoplus_{i\in I} M_i, M\right).$$

注记 4.25. 再给定一族 A-模 $\{M_i'\}_{i\in I}$，它们和 $\{M_i\}_{i\in I}$ 用同样的指标 I。若对每个 $i \in I$，有 A-模同构 $f_i : M_i' \to M_i$，那么，$\bigoplus_{i\in I} M_i'$ 与 $\bigoplus_{i\in I} M_i$ 同构。

对任意的 $i \in I$，我们有 A-模同态：

$$M_i' \xrightarrow{f_i} M_i \xrightarrow{\iota_i} \bigoplus_{i\in I} M_i.$$

这就给出了 A-模同态：

$$\bigoplus_{i\in I} M_i' \longrightarrow \bigoplus_{i\in I} M_i.$$

利用 $f_i^{-1}: M_i \to M_i'$ 可以构造出上述映射的逆，这就给出了 $\bigoplus_{i\in I} M_i'$ 与 $\bigoplus_{i\in I} M_i$ 之间的同构。

特别地，如果 $\{M_i\}_{i\in I}$ 中每个 M_i 均与 A 同构，就用 A^I 记它们的直和（的同构等价类）并称之为**自由 A-模**。我们称 $|I|$ 为此自由模的**秩**。定义 A-模 $A^n = \underbrace{A\oplus A\oplus\cdots\oplus A}_{n\text{ 个}}$。如果 M 是自由 A-模，$\{x_i\}_{i\in I}\subset M$ 使得映射

$$A^I \longrightarrow M,\ \ (a_i)_{i\in I}\mapsto \sum_{i\in I} a_i x_i$$

是 A-模同构（根据定义 $(a_i)_{i\in I}\in A^I$ 中只有有限个 a_i 非零，从而上述求和为有限和），就称 $\{x_i\}_{i\in I}$ 是 M 的一组**基**。此时，对任意的 $x\in M$，存在唯一一组 $(a_i)_{i\in I}$，其中只有有限个 a_i 非零，使得 $x=\sum_{i\in I} a_i x_i$。

例子 4.30. M 是 A-模，N_1, N_2 是子模，若 $N_1\cap N_2 = 0$ 且 $N_1+N_2=M$，其中，

$$N_1+N_2 := \{n_1+n_2 | n_1\in N_1, n_2\in N_2\}.$$

那么，$M\simeq N_1\oplus N_2$。

实际上，根据自然的嵌入映射 $N_i\to M,\ \ n_i\mapsto n_i$，我们自然有映射

$$\psi: N_1\oplus N_2 \longrightarrow M,\ \ (n_1,n_2)\mapsto n_1+n_2.$$

由于 $N_1+N_2=M$，所以 ψ 是满射；对任意的 $(n_1,n_2)\in \mathrm{Ker}(\varphi)$，$n_1=-n_2\in N_1\cap N_2=0$，所以，$\mathrm{Ker}(\varphi)=0$，即 ψ 是单射。综上所述，ψ 是同构。

给定 A-模 M，$\{M_i\}_{i\in I}$ 是 A 的某些子模构成的集合，我们定义

$$\sum_{i\in I} M_i = \left\{ 有限和 \sum_{i\in I} x_i \middle| x_i\in M_i \right\}.$$

这显然是 M 的子模。另外，$\bigcap_{i\in I} M_i$ 也是子模，据此，考虑 M 的非空子集 $S\subset M$，包含 S 的所有子模之交是在包含关系下含 S 的最小子模，它被称为**由 S 生成的子模**并记作 (S)。

如果 M 由某个有限子集 S 生成，则称 M 是**有限生成的 A-模**。如果模 M 可由单个元素 x 生成，则称 M 是**循环模**、x 为 M 的**生成元**并记作 $N=A\cdot x$。

注记 4.26. 循环 A-模形如 A/I，其中 I 是理想。

实际上，I 是 A 的理想（从而是 A 的子模），那么，A/I 是循环模，因为 $1+I$ 是其生成元；反之，若 M 是循环模，则有满同态

$$\varphi: A\to M,\ \ a\mapsto a\cdot x.$$

从而，$M\simeq A/\mathrm{Ker}(\varphi)$。我们注意到 $\mathrm{Ker}(\varphi)$ 是 A 的理想。

注记 4.27. M 是有限生成的当且仅当有整数 n 及满同态 $A^n\to M$。

实际上，若有满同态 $\varphi: A^n\to M$，则 $(1,0,\cdots,0),\cdots,(0,0,\cdots,1)$ 的像生成了 M；反之，令 $s_1,\cdots,s_n$ 为 M 的生成元，可以构造满同态

$$\varphi: A^n\to M,\ \ (a_1,\cdots,a_n)\mapsto a_1s_1+\cdots+a_ns_n.$$

定义 4.8. 若环 A 的每个理想均为有限生成的，则称 A 为 **Noether 环**。

例子 4.31. 主理想整环是 Noether 环。

注记 4.28 (Noether 环的等价定义)**.** 给定环 A，所谓的**理想升链的稳定条件**指的是对任意 A 中的理想升链

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots,$$

存在 $n_0 \geqslant 1$，使得当 $n \geqslant n_0$ 时，$I_n = I_{n_0}$。

我们证明：A 是 Noether 环等价于 A 满足理想升链的稳定条件。

若 A 是 Noether 环，考虑任意上述的理想升链，令 $I = \cup_{k\geqslant 1} I_k$，这是 A 的理想。根据 Noether 性，存在 $x_1, \cdots, x_l \in A$，使得 $I = (x_1, \cdots, x_l)$。根据 I 的定义，存在 n_0，使得 $x_1, \cdots, x_l \in I_{n_0}$，所以当 $n \geqslant n_0$，我们有 $I \subset I_n$。从而，$I_n = I_{n_0}$。

若 A 满足理想升链的稳定条件，假设存在不是有限生成的理想 $I \subset A$。任选 $x_1 \in I$ 且 $x_1 \neq 0$，考虑 $(x_1) \subset I$，由于 I 不是有限生成，必有 $x_2 \in I - (x_1)$；再考虑 $(x_1, x_2) \subset I$，由于 I 不是有限生成，必有 $x_3 \in I - (x_1, x_2)$。如此反复就得到理想的升链：

$$(x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, x_2, \cdots, x_n) \subset \cdots$$

该链的相邻两理想之间是严格包含关系，这与理想升链的稳定条件矛盾。

若 A 是 Noether 环，按定义，A 作为 A-模，其子模均为有限生成的。更一般地，我们有如下命题

命题 60. *Noether 环上的有限生成模的子模也是有限生成的。*

证明: A 是 Noether 环，A-模 M 可被 n 个元素生成，我们对 n 进行归纳。

若 $n = 1$，我们已经证明了 $M \simeq {}^{A}\!/_{I}$。对于子模 $J \subset {}^{A}\!/_{I}$，这是 A 中包含 I 的理想，根据 Noether 性，J 是有限生成的。

现在假设对具有不超过 $n-1$ 个生成元的 A-模命题成立（$n \geqslant 2$），我们考虑

$$M = (x_1, x_2, \cdots, x_n) = Ax_1 + Ax_2 + \cdots + Ax_n,$$

及其子模 N。令 $M' = (x_1, x_2, \cdots, x_{n-1})$，则 ${}^{M}\!/_{M'}$ 由 $x_n + M'$ 生成。在商映射 $\pi : M \to {}^{M}\!/_{M'}$ 下，$\pi(N) \subset {}^{M}\!/_{M'}$ 是子模。根据 $n = 1$ 情形的归纳假设，$\pi(N)$ 可以由有限个 $y_1 + M', \cdots, y_m + M'$ 生成。我们注意到

$$N = N \cap M' + Ay_1 + Ay_2 + \cdots + Ay_m.$$

实际上，对任意 $x \in N$，根据 y_i 的定义，存在 $a_1, \cdots, a_m$，使得 $\pi(x) = a_1\pi(y_1) + \cdots + a_m\pi(y_m)$，所以 $x - (a_1y_1 + \cdots + a_my_m) \in \mathrm{Ker}(\pi)$，即 $x - (a_1y_1 + \cdots + a_my_m) \in N \cap M'$。这就给出了上述等式。

根据归纳假设，$N \cap M'$ 是有限生成的，从而 N 是有限生成。 □

注记 4.29. 注记3.26是该命题的特例，其证明的思想是一样的。实际上，当 A 是主理想整环时，上述证明表明：若 M 可由 n 个元素生成的模，那么每个子模 $N \subset M$ 也可由不超过 n 个元素生成。这与注记3.26一致，因为交换群是 $\mathbb{Z}$-模而 $\mathbb{Z}$ 是主理想整环。

类似于 mod p 的技巧（参考注记3.27），通过商掉极大理想，我们也可以利用域上的线性代数来研究模：

命题 61. *A 是交换环，$\varphi : A^n \to A^m$ 是满的模同态，则 $n \geqslant m$。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。考虑有自然的商映射：

$$A^n \to {}^{A}\!/_{\mathfrak{m}} \oplus \cdots \oplus {}^{A}\!/_{\mathfrak{m}}, \quad (x_1, \cdots, x_n) \mapsto (x_1 + \mathfrak{m}, \cdots, x_n + \mathfrak{m}).$$

这个映射的核是 $\mathfrak{m}^n$，所以

$$A^n\big/\mathfrak{m}^n \simeq A\big/\mathfrak{m} \oplus \cdots \oplus A\big/\mathfrak{m}.$$

这是 n-维 $A\big/\mathfrak{m}$-线性空间。再考虑映射的复合 $\psi = \pi \circ \varphi$

$$\begin{array}{ccc} A^n & \xrightarrow{\quad\varphi\quad} & A^m \\ & \searrow^{\psi} & \downarrow{\scriptstyle \pi} \\ & & \left(A\big/\mathfrak{m}\right)^m \end{array}.$$

很明显，$\mathfrak{m}^n \subset \mathrm{Ker}(\psi)$，所以，存在满射 $\overline{\psi}: \left(A\big/\mathfrak{m}\right)^n \to \left(A\big/\mathfrak{m}\right)^n$，请参考如下交换图

$$\begin{array}{ccc} A^n & \xrightarrow{\quad\varphi\quad} & A^m \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \left(A\big/\mathfrak{m}\right)^n & \xrightarrow{\quad\overline{\psi}\quad} & \left(A\big/\mathfrak{m}\right)^m \end{array}$$

这是线性空间之间的满射，所以 $m \geqslant n$。 □

引理 62. *A 是主理想整环，$M \simeq A^I$ 是自由模，$\{e_i\}_{i\in I}$ 为 M 的一组基，$N \subset M$ 为子模。$J \subset I$ 为子集并且 $J \neq I$，任选 $i_0 \neq I - J$，$J' = J \cup \{i_0\}$。令 M_J 和 $M_{J'}$ 为 $\{e_j\}_{j\in J}$ 和 $\{e_{j'}\}_{j'\in J'}$ 在 M 中生成的自由子模。*

若 $M_J \cap N$ 是自由模，则 $M_{J'} \cap N$ 是自由模。进一步，要么 $M_{J'} \cap N = M_J \cap N$，要么存在 $M_J \cap N$ 的基 $\{f_k\}_{k\in K(J)}$ 以及 $f_{i_0} \in M_{J'} \cap N$ 使得 $\{f_k\}_{k\in K(J)} \cup \{f_{i_0}\}$ 为 $M_{J'} \cap N$ 的基。

证明: 考虑交换图

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M_J & \xrightarrow{\subset} & M_{J'} & \xrightarrow{\pi} & A & \longrightarrow & 1 \\ & & \uparrow{\scriptstyle \subset} & & \uparrow{\scriptstyle \subset} & & \uparrow{\scriptstyle \subset} & & \\ 1 & \longrightarrow & M_J \cap N & \xrightarrow{\subset} & M_{J'} \cap N & \xrightarrow{\pi} & \pi(M_{J'} \cap N) = (a) & \longrightarrow & 1 \end{array}$$

其中，定义

$$\pi : M_{J'} \to A,\ \sum_{i\in J'} a_i e_i \mapsto a_{i_0}.$$

那么，$\mathrm{Ker}(\pi) = M_J$。这个映射给出了上述图中第一行的正合列。

不妨设 $\pi(M_{J'} \cap N) \simeq (a) \neq 0$，其中，$a \in A$：否则上述图的第二行给出 $M_{J'} \cap N \simeq M_J \cap N$，命题明显成立。任选 $f_{i_0} \in M_{J'} \cap N$，使得 $\pi(f_{i_0}) = a$。现在证明 $\{f_k\}_{k\in K(J)} \cup \{f_{i_0}\}$ 是 $M_{J'} \cap N$ 的一组基：对任意的 $x \in M_{J'} \cap N$，$\pi(x) \in (a)$，从而有 $b \in A$，使得 $\pi(x) = ba$，则 $\pi(x - b \cdot f_{i_0}) = 0$，所以 $x - b \cdot f_{i_0} \in M_J \cap N$，从而有 $a_k \in A$，使得

$$x - b \cdot f_{i_0} = \sum_{k\in K(J)} a_k \cdot f_k.$$

这说明 $\{f_k\}_{k\in K(J)} \cup \{f_{i_0}\}$ 生成了 $M_{J'} \cap N$。另外，若

$$b \cdot f_{i_0} + \sum_{k\in K(J)} a_k \cdot f_k = 0.$$

先作用 π，则 $b = 0$，从而 $\sum_{k\in K(J)} a_k \cdot f_k = 0$，那么，$a_k = 0$，所以 $\{f_k\}_{k\in K(J)} \cup \{f_{i_0}\}$ 是 $M_{J'} \cap N$ 的基。综上所述，命题成立。 □

定理 63. *A 为主理想整环，M 是自由 A-模，$N\subset M$ 为其子模，则 N 是也是自由 A-模。*

注记 4.30. 证明的困难之处在于并不需要假设 M 是有限生成。定理在很多场合有着重要的应用，比如说 X 是拓扑空间，为了定义 X 的奇异同调 $H_*(X;\mathbb{Z})$，对任意 k，我们研究它的 k-次奇异链复形 $S_k(X)$，这是由所有 k-单形生成的自由交换群（即自由的 $\mathbb{Z}$-模），那么 $S_k(X)$ 的每个子群都是自由的交换群。

证明： 考虑下面的集合：

$$\mathcal{J}=\left\{\left(J,\{f_k\}_{k\in K(J)}\right)\middle|J\subset I, M_J\cap N\text{是自由 }A\text{-模且 }\{f_k\}_{k\in K(J)}\text{ 为一组基}\right\}.$$

我们定义 $\mathcal{J}$ 上的偏序：对任意的 $\left(J,\{f_k\}_{k\in K(J)}\right),\left(J',\{f'_{k'}\}_{k'\in K(J')}\right)\in\mathcal{J}$，$J_1\preceq J_2$ 指的是

$$J\subset J'\text{ 且 }\{f_k\}_{k\in K(J)}\subset\{f'_{k'}\}_{k'\in K(J')}.$$

对任意的 $s=\left(J,\{f_k\}_{k\in K(J)}\right)$，令 $\pi_1(s)=J$，$\pi_2(s)=\{f_k\}_{k\in K(J)}$。对任意的全序子集 $S\subset\mathcal{J}$，令

$$J=\bigcup_{s\in S}\pi_1(s)\subset I,\ \mathbf{b}=\bigcup_{s\in S}\pi_2(s).$$

由于对每个 $s\in S$，$\pi_2(s)\subset N\cap M_{\pi_1(s)}\subset\bigcup_{s\in S}M_{\pi_1(s)}\cap N$，所以，$\mathbf{b}\subset\bigcup_{s\in S}M_{\pi_1(s)}\cap N$。现在证明 $\mathbf{b}$ 为 $\bigcup_{s\in S}M_{\pi_1(s)}\cap N$ 的基（从而，$\bigcup_{s\in S}M_{\pi_1(s)}\cap N$ 是自由 A-模）：

- 任选 $x\bigcup_{s\in S}M_{\pi_1(s)}\cap N$，则存在 $s_0\in S$，使得 $x\in M_{\pi_1(s_0)}\cap N$。此时，$\pi_2(s_0)$ 是 $M_{\pi_1(s_0)}\cap N$ 的基，所以存在 $e_1,\cdots,e_n\in\pi_2(s_0)$ 和 $a_1,\cdots,a_n\in A$，使得 $x=\sum_{i=1}^n a_ix_i$。由于 $\pi_2(s_0)\subset\mathbf{b}$，这表明 $\mathbf{b}$ 生成 $\bigcup_{s\in S}M_{\pi_1(s)}\cap N$。
- $\mathbf{b}$ 中的元素是 A-线性无关的：对任意的 $e_1,\cdots,e_n\in\mathbf{b}$，存在 $s_1,\cdots,s_n\in S$，使得 $e_i\in\pi_2(s_i)$。由于 S 是全序子集，不妨假设 $s_n=\max(s_1,\cdots,s_n)$，那么，$e_1,\cdots,e_n\in\pi_2(s_n)$。由于 $\pi_2(s_n)$ 是 M 的某子模的基，所以它们 A-线性无关。

综合上述，$(J,\mathbf{b})\in\mathcal{J}$ 并且 J 是 S 的上界。根据 Zorn 引理，S 有极大元 (J)。令 $\pi_1(s_*)=J$，那么，$J=I$：否则，任选 $i_0\neq I-J$，$J'=J\cup\{i_0\}$，根据上一引理，$M_{J'}\cap N$ 是自由 A-模并且有一组基 $\mathbf{b}'$ 包含 $\pi_2(s_*)$。所以，$(J',')\in\mathcal{J}$ 且比 s_* 更大，矛盾！ □

4.5.2 主理想整环上有限生成模的分类定理

A 是交换环，p,q 是正整数，用 $\mathbf{M}_{p,q}(A)$ 表示 A 系数 $p\times q$ 的矩阵全体。当 $p=q=n$ 时，令 $\mathbf{M}_n(A)=\mathbf{M}_{n,n}(A)$，那么 $\mathbf{M}_n(A)$ 在矩阵乘法下是环（当 $p\geqslant 2$ 时，这个环不交换）。

在 $\mathbf{M}_n(A)$ 上，我们有经典的行列式映射：

$$\det:\mathbf{M}_n(A)\to A,\quad A\mapsto\sum_{\sigma\in\mathfrak{S}_n}\varepsilon(\sigma)a_{1\sigma(1)}a_{2\sigma(2)}\cdots a_{n\sigma(n)}.$$

其中，$A=(a_{ij})_{i,j\leqslant n}$。特别地，对任意的 $M,M'\in\mathbf{M}_n(A)$，有

$$\det(M\cdot M')=\det(M)\det(M').$$

实际上，以上公式的证明只需要用到 A 中的乘法，所以在线性代数课程中的证明仍然成立。我们可以通过如下 Cauchy-Binet 公式的证明来验证这里的逻辑：

例子 4.32 (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，$m\leqslant n$。对任意的 $1\leqslant j_1<j_2<\cdots<j_m\leqslant n$，我们定义 $M_{\underline{j}}$ 为 M 的第 $j_1,j_2,\cdots,j_m$ 列（按照既定的顺序）给出的 $m\times m$ 的矩阵，$N_{\underline{j}}$ 为 N 的第 $j_1,j_2,\cdots,j_m$ 行（按照既定的顺序）给出的 $m\times m$ 的矩阵，其中，$\underline{j}=(j_1,\cdots,j_m)$。

对于 $m\times m$ 的矩阵 M，其行列式为

$$\det(M)=\sum_{\sigma\in\mathfrak{S}_m}\varepsilon(\sigma)M_{1\sigma(1)}M_{2\sigma(2)}\cdots M_{m\sigma(m)}.$$

我们来证明著名的 **Cauchy-Binet 公式**：

$$\det(M\cdot N)=\sum_{\underline{j}}\det(M_{\underline{j}})\det(N_{\underline{j}}). \tag{4.4}$$

直接计算给出

$$\begin{aligned}\det(M\cdot N)&=\sum_{\sigma\in\mathfrak{S}_m}\varepsilon(\sigma)(M\cdot N)_{1\sigma(1)}(M\cdot N)_{2\sigma(2)}\cdots(M\cdot N)_{m\sigma(m)}\\&=\sum_{\sigma\in\mathfrak{S}_m}\sum_{k_1=1}^{n}\sum_{k_2=1}^{n}\cdots\sum_{k_m=1}^{n}\varepsilon(\sigma)M_{1k_1}N_{k_1\sigma(1)}M_{2k_2}N_{k_2\sigma(2)}\cdots M_{1k_m}N_{k_m\sigma(m)}\\&=\sum_{k_1,\cdots,k_m=1}^{n}M_{1k_1}M_{2k_2}\cdots M_{mk_m}\sum_{\sigma\in\mathfrak{S}_m}\varepsilon(\sigma)N_{k_1\sigma(1)}N_{k_2\sigma(2)}\cdots N_{k_m\sigma(m)}.\end{aligned}$$

令 $N_{\underline{k}}$ 为 $N_{\underline{j}}$ 为 N 的第 $k_1,k_2,\cdots,k_m$ 行给出的 $m\times m$ 的矩阵，其中，$k_1,k_2,\cdots,k_m$ 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 $k_1,k_2,\cdots,k_m$ 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，$1\leqslant j_1<j_2<\cdots<j_m\leqslant n$ 是对 $k_1,\cdots,k_m$ 的重新排序。所以，

$$\begin{aligned}\det(M\cdot N)&=\sum_{\underline{k}\in\mathfrak{S}_m}\varepsilon(\underline{k})M_{1k_1}M_{2k_2}\cdots M_{mk_m}\det(M_{\underline{j}})\\&=\det(N_{\underline{j}})\det(M_{\underline{j}}).\end{aligned}$$

当 $m=n$ 时，Cauchy-Binet 公式给出 $\det(M\cdot N)=\det(M)\det(N)$。

给定 $M\in\mathbf{M}_n(A)$，用 M^{ad} 表示其伴随矩阵（由余子式构成的矩阵）。类似地，我们仍然有

$$M\cdot{}^tM^{\mathrm{ad}}={}^tM^{\mathrm{ad}}\cdot M=\det(M)\cdot I,$$

其中，I 是 $n\times n$ 的单位矩阵。

现在考虑环 $\mathbf{M}_n(A)$ 的可逆元：

$$\mathbf{GL}(n;A)=\mathbf{M}_n(A)^\times,$$

这是 $n\times n$ 的可逆矩阵所构成的群。根据上述 M 与其伴随矩阵相乘的公式，我们有如下结论：

引理 64. $\mathbf{GL}(n;A)=\left\{M\in\mathbf{M}_n(A)\middle|\det(M)\in A^\times\right\}$。

我们要用矩阵来研究主理想整环上的有限生成模，其基本的思想就是研究群 $\mathbf{GL}(p;A)\times\mathbf{GL}(q;A)$ 在 $\mathbf{M}_{p,q}(A)$ 上的作用，它是线性代数中通过左右乘以矩阵将给定矩阵变成对角矩阵的推广。

我们定义群的作用：

$$\big(\mathbf{GL}(p;A)\times\mathbf{GL}(q;A)\big)\times\mathbf{M}_{p,q}(A)\to\mathbf{M}_{p,q}(A),\quad\big((P,Q),M\big)\mapsto P\cdot M\cdot Q^{-1}.$$

给定 $M\in\mathbf{M}_{p,q}(A)$，目标是在 M 的轨道中选形式尽可能简单的代表元。

定理 65 (Smith 正规型)**.** *A 是主理想整环，$M\in\mathbf{M}_{p,q}(A)$，不妨 $p\leqslant q$，$r=\min(p,q)=q$。那么，M 的轨道中有如下形式的矩阵：*

$$P\cdot M\cdot Q^{-1}=\left(\begin{array}{cccc|c}a_1&&&&\\&a_2&&&\\&&\ddots&&\mathbf{0}\\&&&a_r&\end{array}\right)$$

其中，$a_1,\cdots,a_r$ 是仅有的可能非零的元，$(a_1)\supset(a_2)\supset\cdots\supset(a_r)$。进一步，对每个 $i\leqslant r$，a_i 在伴随的意义下唯一。

存在性部分的证明. 对 $p+q$ 进行归纳。当 $p+q=2$ 时，命题明显成立。我们做如下的归纳假设：对 $k\geqslant3$，对任意 $p+q<k$，命题成立。以下证明当 $p+q=k$ 时，该命题仍然出成立。

对 $a\in A$，由于 A 是主理想整环，a 可以写成 $a=up_1^{e_1}\cdots p_k^{e_k}$，其中，$u\in A^\times$ 而 p_i 为不可约元，其中，$e_i\geqslant1$。令 $F(a)=e_1+\cdots+e_k$，这是 a 的不可约因子的个数（算重数）。我们注意到初等矩阵均为 $\mathbf{GL}(p;A)$ 或者 $\mathbf{GL}(q;A)$ 中的元素（因为它们的系数均为整数）。对给定的矩阵 $M=(m_{i,j})_{i\leqslant p,j\leqslant q}$，通过对 M 的左右乘初等矩阵来实现调换两行或者两列，我们不妨假设 $F(m_{1,1})=\min\limits_{i,j}F(m_{i,j})$。我们还定义 $F(M)=\min\limits_{i,j}F(m_{i,j})$。

现在考察 M 的第一行中的元素 $m_{1,j}$ 和第一列中的元素 $m_{i,1}$，其中，$i,j\geqslant2$。分两种情况讨论：

(1) 存在某个 $m_{1,j}$ 或 $m_{i,1}$ 不被 $m_{1,1}$ 整除。

通过对 M 的左右乘初等矩阵，不妨设 $m_{1,2}\notin(m_{1,1})$。考虑 $m_{1,1}$ 和 $m_{1,2}$ 在 A 中生成的理想 $(m_{1,1},m_{1,2})$，由于 A 是主理想整环，所以存在 $d\in A$，使得 $(m_{1,1},m_{1,2})=(d)$。特别地，$d\mid m_{1,1}$ 且 $(m_{1,1})\neq(d)$（否则 $m_{1,2}\in(m_{1,1})$）。据此，必然有 $F(d)<F(m_{1,1})$。根据 $(m_{1,1},m_{1,2})=(d)$，存在 $a,b\in A$，使得

$$am_{1,1}+bm_{1,2}=d.$$

令 $x=\frac{m_{1,1}}{d}$，$y=\frac{m_{1,2}}{d}$，那么

$$ax+by=1.$$

我们构造分块对角的 $q\times q$ 矩阵[21]：

$$Q'=\begin{pmatrix}a&-y&&&\\b&x&&&\\&&1&&\\&&&\ddots&\\&&&&1\end{pmatrix}$$

[21]这里要求 $q\geqslant2$。当 $q=1$ 时，命题显然成立。

根据 $ax+by=1$，$Q'\in\mathbf{GL}(n;A)$。所以，$M\cdot Q'$ 的第一行第一列的位置为 $am_{1,1}+bm_{1,2}=d$。此时，$F(d)<F(m_{1,1})$，此时，新得到的 M' 满足 $F(M')<F(M)$。

再通过调整行和列的位置，我们还可假设 $F(m'_{1,1})=F(M')$，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第一行和第一列的数，使得 M 形如：

$$M=\begin{pmatrix} a_1 & 0 & 0 & 0\\ 0 & * & * & *\\ \cdots & \cdots & \cdots & \cdots\\ 0 & * & * & * \end{pmatrix}$$

我们注意到，通过上述操作，以上矩阵中所有 $*$ 均为 a_1 的倍数：若不然，可以将这一行加到第一行，再次进行情形 (1) 的操作，这样 $F(m_{11})$ 可以进一步减小。如此往复，一直到所有 $*$ 均为 a_1 的倍数即可。对 $*$ 构成的矩阵可以提出因子 a_1，然后使用归纳假设即可。

特别地，以上的证明还给出了具体 P 和 Q 的算法。 □

我们引入如下工具来证明唯一性：

引理 66. 给定 $M\in M_{p,q}(A)$，对 $1\leqslant k\leqslant\min(p,q)$，令 $c_k(M)\subset A$ 为 M 的所有 k 阶子式所生成的理想。当 $k\leqslant 0$ 时，令 $c_k(M)=A$；当 $k>\min(p,q)$ 时，令 $c_k(M)=0$。

对任意的 $k\in\mathbb{Z}$，对任意的 $P\in\mathbf{GL}(p;A),Q\in\mathbf{GL}(q;A)$ 和 $M\in\mathbf{M}_{p,q}(A)$，如下等式成立：

$$c_k(M)=c_k(P\cdot M\cdot Q).$$

证明：首先证明 $c_k(M\cdot Q)\subset c_k(M)$。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，$Q(k)$ 为 Q 的前 k 列所构成的 $q\times k$ 的矩阵，根据 Cauchy-Binet 公式，上述余子式为

$$\det(M(k)\cdot Q(k))=\sum_{\underline{j}}\det(M(k)_{\underline{j}})\det(Q(k)_{\underline{j}})\subset c_k(M).$$

对于 $M\cdot Q$ 的其它余子式也可类似讨论，这就证明了 $c_k(M\cdot Q)\subset c_k(M)$。由于 Q 是可逆矩阵，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 自然可以同样讨论。 □

Smith 标准型唯一性的证明. 对于

$$P\cdot M\cdot Q^{-1}=\left(\begin{array}{cccc|c} a_1 & & & & \\ & a_2 & & & \\ & & \ddots & & \mathbf{0}\\ & & & a_r & \end{array}\right)$$

我们显然有 $c_k(P\cdot M\cdot Q^{-1})=(a_1\cdots a_k)=c_k(M)$，这表明 $a_1a_2\cdots a_k$ 完全被 M 决定。由于每个主理想的生成元在伴随的意义下唯一，所以 $a_1,a_1a_2,\cdots,a_1a_2\cdots a_r$ 被唯一决定。通过相除，$a_1,a_2,\cdots,a_r$ 是唯一的。 □

推论 67 (线性映射版本)**.** *A 是主理想整环，M 和 N 是有限生成的自由 A-模，$\varphi : M \to N$ 是 A-模同态并且 $M \simeq A^q, N \simeq A^p$。那么，存在 M 的基 $u_1, \cdots, u_q$ 和 N 的基 $v_1, \cdots, v_p$ 以及 $a_1, \cdots, a_r \in A$，其中，$r \leqslant \min(p, q)$，使得*

$$(a_1) \supset (a_2) \supset \cdots \supset (a_r), \quad \varphi(u_i) = \begin{cases} a_i v_i, \ i \leqslant r; \\ 0, \ i > r. \end{cases}$$

证明： 任选 M 和 N 的基 $e_1, \cdots, e_q$ 和 N 的基 $f_1, \cdots, f_p$，在这组基下模同态 φ 的矩阵可以表示为 M。则存在 $(P, Q) \in \mathbf{GL}(p; A) \times \mathbf{GL}(q; A)$，使得

$$P \cdot M \cdot Q^{-1} = \left(\begin{array}{cccccc|c} a_1 & & & & & & \\ & \ddots & & & & & \\ & & a_r & & & & \\ & & & 0 & & & \mathbf{0} \\ & & & & \ddots & & \\ & & & & & 0 & \end{array}\right)$$

其中，不妨假设 $p \leqslant q$。那么，

$$\{v_1 = Q \cdot e_1, \cdots, v_q = Q \cdot e_q\}, \ \{v_1 = P \cdot f_1, \cdots, v_p = P \cdot f_p\}$$

为所求的基。 □

命题 68 (主理想整环上自由模的子模)**.** *A 为主理想整环，$M \simeq A^n$ 是有限生成的自由 A-模，$N \subset M$ 为其子模，则 N 是自由的 A-模。进一步，存在 M 的基 $\{e_1, \cdots, e_n\}$,$r \leqslant n$ 和 $a_1, \cdots, a_r \in A$，使得 $(a_1) \supset (a_2) \supset \cdots \supset (a_r)$ 并且 $a_1 e_1, \cdots, a_r e_r$ 是 N 的基。*

证明： 根据命题60以及注记4.29，N 是有限生成的 A-模，所以存在 $m \leqslant n$ 以及 A-模同态

$$\varphi : A^m \twoheadrightarrow N \subset M \simeq A^n,$$

其中，$\mathrm{Im}(\varphi) = N$。对 φ 用上一推论，则存在 A^m 的基 $u_1, \cdots, u_m$ 和 M 的基 $v_1, \cdots, v_n$ 以及 $a_1, \cdots, a_r$，其中，$r \leqslant \min(p, q)$，使得

$$(a_1) \supset (a_2) \supset \cdots \supset (a_r), \quad \varphi(u_i) = \begin{cases} a_i v_i, \ i \leqslant r; \\ 0, \ i > r. \end{cases}$$

此时，$\{a_1 v_1, \cdots, a_r v_r\}$ 是 N 的基。 □

定理 69 (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，则存在 $r, s \in \mathbb{Z}_{\geqslant 0}$ 和 $a_1, \cdots, a_s \in A$，使得 $(a_1) \supset (a_2) \supset \cdots \supset (a_s)$ 并且*

$$M \simeq A^r \oplus {}^{A}\!\diagup\!_{(a_1)} \oplus {}^{A}\!\diagup\!_{(a_2)} \oplus \cdots \oplus {}^{A}\!\diagup\!_{(a_s)}.$$

进一步，以上的 $a_1, \cdots, a_s$ 在伴随的意义下唯一。

注记 4.31. 我们称 r 为 M 的**秩**并记作 $\mathrm{rank}(M)$。

证明: 由于 M 是有限生成的，所以存在满射的 A-模同态 $\varphi: N \to M$，其中，N 是有限成的自由 A-模。特别地，$M \simeq {}^{N}\!/_{\mathrm{Ker}(\varphi)}$。根据命题68，存在 N 的基 $e_1, \cdots, e_n$，使得

$$\mathrm{Ker}(\varphi) \simeq A \cdot a_1 e_1 \oplus \cdots \oplus A \cdot a_s e_s,$$

其中，$s \leqslant n$ 并且 $(a_1) \supset (a_2) \supset \cdots \supset (a_s)$，并且 $a_s \neq 0$。令 $r = n - s$，那么，

$$M \simeq {}^{A^n}\!/_{A \cdot a_1 e_s \oplus \cdots \oplus A \cdot a_s e_s} \simeq A^r \oplus {}^{A}\!/_{(a_1)} \oplus {}^{A}\!/_{(a_2)} \oplus \cdots \oplus {}^{A}\!/_{(a_s)}.$$

着给出了主理想整环上有限生成模的结构定理的存在性部分的证明。 □

注记 4.32. 现在证明唯一性部分，即若有 $r', s' \in \mathbb{Z}_{\geqslant 0}$ 和 $a'_1, \cdots, a'_{s'} \in A$，使得 $(a'_1) \supset \cdots \supset (a'_{s'})$ 且

$$M \simeq A^{r'} \oplus {}^{A}\!/_{(a'_1)} \oplus \cdots \oplus {}^{A}\!/_{(a'_{s'})}.$$

那么，$r = r', s = s'$ 且 a_i 与 a'_i 伴随。

$x \in M$，如果存在 $a \in A - \{0\}$，使得 $a \cdot x = 0$，就称 x 是**挠元素**。不难看出，挠元素的全体 $T(M)$ 是 M 的子模。特别地，根据以上两个关于 M 的分解，我们有

$$T(M) \simeq {}^{A}\!/_{(a_1)} \oplus \cdots \oplus {}^{A}\!/_{(a_s)}, \quad T(M) \simeq {}^{A}\!/_{(a'_1)} \oplus \cdots \oplus {}^{A}\!/_{(a'_{s'})},$$

以及

$$A^r \simeq {}^{M}\!/_{T(M)}, \quad A^{r'} \simeq {}^{M}\!/_{T(M)}.$$

从而，$A^r \simeq A^{r'}$。根据命题61，$r = r'$。

通过考虑 $T(M)$ 的分解，我们以下假设 $r = r' = 0$。对于任意 $a \in A$，假设

$$a = u p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad \alpha_i \geqslant 1, u \in A^{\times},$$

为其素因子的分解，其中，$p_1, \cdots, p_k$ 为两两不同的不可约元素。那么，理想 $\left\{(p_u^{\alpha_i})\right\}_{1 \leqslant i \leqslant k}$ 两两互素。根据中国剩余定理，就有

$${}^{A}\!/_{(a)} \simeq {}^{A}\!/_{(p_1^{\alpha_1})} \times \cdots \times {}^{A}\!/_{(p_k^{\alpha_k})}.$$

以上是环同构，它自然给出了 A-模的同构:

$${}^{A}\!/_{(a)} \simeq {}^{A}\!/_{(p_1^{\alpha_1})} \oplus \cdots \oplus {}^{A}\!/_{(p_k^{\alpha_k})}.$$

据此，我们对 $M \simeq {}^{A}\!/_{(a_1)} \oplus {}^{A}\!/_{(a_2)} \oplus \cdots \oplus {}^{A}\!/_{(a_s)}$ 和 $M \simeq {}^{A}\!/_{(a'_1)} \oplus {}^{A}\!/_{(a'_2)} \oplus \cdots \oplus {}^{A}\!/_{(a'_{s'})}$ 的每个直和分量进行分解，得到

$$M \simeq \bigoplus_{i=1}^{m} \left(\bigoplus_{j=1}^{n_i} {}^{A}\!/_{(p_i^{d_{i,j}})} \right), \quad M \simeq \bigoplus_{i=1}^{m'} \left(\bigoplus_{j=1}^{n'_i} {}^{A}\!/_{(q_i^{d'_{i,j}})} \right)$$

我们证明 $m = m'$，（通过调整顺序）p_i 与 q_i 伴随，$n_i = n'_i$，$d_{i,j} = d'_{i,j}$。由于 a_i 与 a'_i 可由 $p_i, q_i, d_{i,j}$ 与 $d'_{i,j}$ 唯一决定[22]，这就将完成唯一性部分的证明。

首先证明 $m = m'$ 且 p_i 与 q_i 伴随，其中，$i = 1, \cdots, m$。实际上，对给定的不可约元 p，令

$$M_p := \left\{ x \in M | \text{存在 } k \geqslant 0, \text{ 使得} p^k x = 0, \right\}.$$

[22]请参考注记3.29中的证明

对任意的不可约元素 q，如果 p 与 q 不伴随，那么，对 $k,d\geqslant 1$，存在 $a,b\in A$，使得 $ap^k+bq^d=1$，从而，

$$A/(q^d)\to A/(q^d),\quad x\mapsto p^kx,$$

是双射：其逆映射为 $x\mapsto bx$。据此，根据分解 $M\simeq\bigoplus_{i=1}^m\left(\bigoplus_{j=1}^{n_i}A/(p_i^{d_{i,j}})\right)$，我们有

$$M_{p_1}=\bigoplus_{j=1}^{n_1}A/(p_1^{d_{1,j}}).$$

利用第二个分解，必然存在某个（不妨设为）q_1，使得

$$M_{q_1}=\bigoplus_{j=1}^{n_1'}A/(p_1^{d_{1,j}'}).$$

这表明，$q_1=p_1$。利用归纳法，不难看出 $m=m'$ 且 p_i 与 q_i 伴随。

最终，我们假设

$$M\simeq\bigoplus_{j=1}^{n}A/(p^{d_j}),\quad M\simeq\bigoplus_{j=1}^{n'}A/(p^{d_j'}).$$

其中，$d_1\leqslant\cdots\leqslant d_n,d_1'\leqslant\cdots\leqslant d_{n'}'$ 只要证明 $n=n',d_j=d_j'$ 即可。

不妨假设 $l=d_n=\cdots=d_{k+1}>d_k\geqslant\cdots\geqslant d_1$ 并且 $d_n\geqslant d_n'$。注意到映射

$$A/(p)\to p^{s-1}A/(p^sA),\quad x\mapsto p^{s-1}x$$

是同构。所以，

$$p^{l-1}M\simeq\bigoplus_{j=1}^{n}p^lA/(p^{d_j})\simeq\bigoplus_{j=k+1}^{n}p^{l-1}A/(p^l)\simeq\bigoplus_{j=k+1}^{n}A/(p).$$

由于 $A/(p)$ 是域，通过考察 $\dim_{A/(p)}p^{l-1}M$，$d_{n'}'=d_n$ 并且它们在 $\{d_j\}$ 与 $\{d_j'\}$ 中出现的次数一样多。通过对 M 的子模

$$M'=\{x\in M|p^lM=0\}$$

进行讨论，我们就可以用归纳法完成证明。

注记 4.33. 由于交换群可被视为 $\mathbb{Z}$-模，以上定理重新给出有限生成交换群的结构定理，请参考定理34。

应用 (矩阵的标准型)**.** K 是域，V 是有限维 K-线性空间，$T\in\mathrm{End}_K(V)$ 是 K-线性映射，则 V 可被视为 $K[X]$-模：

$$K[X]\times V\to V,\quad (P(X),v)\mapsto P(T)v,$$

即对 $P(X)=a_nX^n+\cdots+a_1X+a_0\in K[X]$, $a_0,\cdots,a_n\in K$，定义

$$P(X)\cdot v=a_nT^n(v)+\cdots+a_1T(v)+a_0v.$$

由于 $\dim_K V<\infty$，这显然是有限生成的 $K[X]$-模。根据分类定理69，存在非零的首一多项式 $P_1,\cdots,P_s\in K[X]$，使得 $(P_1)\supset(P_2)\supset\cdots\supset(P_s)$ 并且

$$V\simeq K[X]/(P_1(X))\oplus K[X]/(P_2(X))\oplus\cdots\oplus K[X]/(P_s(X)).$$

我们需要强调的是以上分解为 $K[X]$-模的直和，也是 K-线性空间的直和。

以上分解没有自由的部分，即 $r=0$：根据 Hamilton-Cayley 定理，$P_T(T)=0$，其中，$P_T(X)\in K[X]$ 是 T 的特征多项式，从而 $P_T(X)$ 乘任何 v 都为 0；我们还可以计算线性空间的维数，若 $r\geqslant 1$，则 $\dim_K K[X]=\infty$，与 $\dim_K V<\infty$ 矛盾。

对于每个 $P_i(X)$，将它分解为不可约首一的多项式之积 $P_i(X)=p_1(X)^d\cdots p_n(X)^{d_n}$。根据中国剩余定理，我们有

$$K[X]\big/_{(P_1(X))}\simeq K[X]\big/_{(p_1(X)^{d_1})}\times\cdots\times K[X]\big/_{(p_n(X)^{d_n})}.$$

这是环同构，也可被视作 $K[X]$-模之间的同构：

$$K[X]\big/_{(P_1(X))}\simeq K[X]\big/_{(p_1(X)^{d_1})}\oplus\cdots\oplus K[X]\big/_{(p_n(X)^{d_n})}.$$

这自然是 K-线性空间之间的同构。

考虑一个因子 $f(X)=p_i(X)^{d_i}$，假设

$$f(X)=X^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0.$$

那么，$K[X]\big/_{(f(X))}$ 作为线性空间的维数为 n 并且 $1,X,\cdots,X^{n-1}$ 为一组基。此时，映射 T 对应着

$$T:K[X]\big/_{(f(X))}\to K[X]\big/_{(f(X))},\ \ Q(X)\mapsto XQ(X).$$

从而，

$$T:1\mapsto X,X\mapsto X^2,\cdots,X^{n-2}\mapsto X^{n-1},\ X^{n-1}\mapsto -a_0-a_1X\cdots-a_{n-1}X^{n-1}.$$

这个分量对应的矩阵为

$$\begin{pmatrix}0&&&&-a_0\\1&0&&&-a_1\\&1&&&-a_2\\&&\ddots&&\vdots\\&&&1&-a_{n-1}\end{pmatrix}$$

以上是所谓的 Frobenius 标准型。

如果 $K=\mathbb{C}$（或更一般地假设 K 为代数封闭域），根据代数基本定理，$\mathbb{C}[X]$ 中每个不可约多项式均形如 $X-\lambda$，其中，$\lambda\in\mathbb{C}$。以上的分解就给出了如下的直和：

$$V\simeq\prod_{\text{有限和}}\mathbb{C}[X]\big/_{\left((X-\lambda)^d\right)}.$$

我们现在研究 T 在一个直和项上的作用：

$$T:\mathbb{C}[X]\big/_{\left((X-\lambda)^d\right)}\to\mathbb{C}[X]\big/_{\left((X-\lambda)^d\right)},\ \ Q(X)\mapsto X\cdot Q(X).$$

此时，我们选取 $1,X-\lambda,\cdots,(X-\lambda)^{d-1}$ 作为 $\mathbb{C}$-线性空间 $\mathbb{C}[X]\big/_{\left((X-\lambda)^d\right)}$ 的基：这 d 个向量显然张成 $\mathbb{C}[X]\big/_{\left((X-\lambda)^d\right)}$；它们是线性无关的：否则，存在 $a_0,\cdots,a_{d-1}$ 使得在 $\mathbb{C}[X]\big/_{\left((X-\lambda)^d\right)}$ 中

$$a_0+a_1(X-\lambda)+\cdots+c_{d-1}(X-\lambda)^{d-1}=0,$$

即

$$a_0+a_1(X-\lambda)+\cdots+c_{d-1}(X-\lambda)^{d-1}\in\left((X-\lambda)^d\right).$$

所以，$(X-\lambda)^d$ 整除 $a_0+a_1(X-\lambda)+\cdots+c_{d-1}(X-\lambda)^{d-1}$。通过观察次数，我们得到 $a_0=\cdots=a_{d-1}=0$。在这组基 $\{e_1=1,e_2=X-\lambda,\cdots,e_d=(X-\lambda)^{d-1}\}$ 下，此时，T 的作用为

$$X\cdot e_1=e_2+\lambda e_1,\quad X\cdots e_2=e_3+\lambda e_2,\cdots,X\cdot e_d=\lambda e_d.$$

它对应的矩阵是

$$\begin{pmatrix}\lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & & \\ & & & \lambda & 1 \\ & & & & \lambda\end{pmatrix}$$

以上是所谓的 Jordan 标准型。

4.6 习题

4.6.1 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，

1. 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：$\{1,f,f^2,\cdots\}$，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）。

2. 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 $\frac{s'a}{s's}=\frac{a}{s}$。

3. 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：

   $$\iota:A\to A_S,\ a\mapsto\frac{a}{1}.$$

   我们把 A_S 称作是 A 对乘性子集 S 的**局部化**。

4. 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 $\iota:A\to A_{S_0}$ 是单射并且此时 $\frac{a}{s}=\frac{a'}{s'}$ 当且仅当 $as'=a's$。

5. 给定乘性子集 $S\subset A$。证明，$\mathrm{Ker}(\iota)=\{a\in A|$存在 $s\in S$, 使得$as=0\}$。进一步证明，ι 为单射当且仅当 $S\subset S_0$。

6. （局部化的泛性质）A, S, A_S 和 $\iota : A \to A_S$ 如上述。试验证，$\iota(S) \subset (A_S)^\times$。

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \downarrow{\scriptstyle \iota} & \nearrow_{\psi} & \\ A_S & & \end{array}$$

证明，对任意的环 B 和环同态 $\varphi : A \to B$，如果 $\varphi(S) \subset B^\times$，则存在唯一的环同态 $\psi : A_S \to B$，使得 $\psi \circ \iota = \varphi$。

7. A, S, A_S 和 $\iota : A \to A_S$ 如上述，$\widehat{S} = \{a \in A | \text{存在 } b \in A, \text{ 使得 } ab \in S\}$。证明，$\widehat{S} = \iota^{-1}\left((A_S)^\times\right)$。进一步证明环同构 $A_S \xrightarrow{\simeq} A_{\widehat{S}}$，其中，$\frac{a}{1}$ 的像是 $\frac{a}{1}$。

8. A 和 B 是交换环，$\varphi : A \to B$ 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 $\psi : A_S \to B_T$，使得如下图表交换[23]：

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota} \\ A_S & \xrightarrow{\psi} & B_T \end{array}$$

9. （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，$\left(\iota^{-1}(J)\right)_S = J$。

10. （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。

11. $\mathfrak{p} \subset A$ 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。

12. （局部化与商可交换）$I \subset A$ 是理想，$S \subset A$ 是乘性子集，$\pi : A \to A/I$ 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

$$\left(A/I\right)_{\pi(S)} \xrightarrow{\simeq} A_S/I_S.$$

13. 给定 $f \in A$，$S = \{1, f, f^2, \cdots\}$，记 $A_f = A_S$。证明，我们有环同构

$$A[X]/(1 - fX) \xrightarrow{\simeq} A_f, \quad X \mapsto \frac{1}{f}.$$

4.6.2 $\mathbb{Z}\left[\sqrt{d}\right]^\times$ 与 Pell 方程，$d \neq \square, d > 0$

假设 $d \in \mathbb{Z}$ 不是完全平方数。令

$$\mathbb{Z}\left[\sqrt{d}\right] = \{x + y\sqrt{d} | x, y \in \mathbb{Z}\}, \quad \mathbb{Q}\left[\sqrt{d}\right] = \{x + y\sqrt{d} | x, y \in \mathbb{Q}\}.$$

[23] 请查阅图表交换的含义

1. 证明，$\mathbb{Z}\left[\sqrt{d}\right]$ 是环而 $\mathbb{Q}\left[\sqrt{d}\right]$ 为其分式域。

2. 证明，如果 $d<0$，$\mathbb{Z}\left[\sqrt{d}\right]$ 是 $\mathbb{C}$ 中的格点（从而是离散的）；如果 $d>0$，$\mathbb{Z}\left[\sqrt{d}\right]$ 在 $\mathbb{R}$ 中稠密。

3. 对任意的 $z=x+y\sqrt{d}\in\mathbb{Q}\left[\sqrt{d}\right]$，我们定义 $\overline{z}=x-y\sqrt{d}$（请注意，如果 $d>0$，这不是复共轭）。证明，环 $\mathbb{Z}\left[\sqrt{d}\right]$ 的自同构群 $\mathbf{Aut}\big(\mathbb{Z}\left[\sqrt{d}\right]\big)$ 恰有 2 个元素。

4. 对任意的 $z\in\mathbb{Q}\left[\sqrt{d}\right]$，我们定义 $N(z)=z\cdot\overline{z}$。证明，对任意的 $a,b\in\mathbb{Q}\left[\sqrt{d}\right]$，$N(a\cdot b)=N(a)\cdot N(b)$ 并且 $N(\mathbb{Z}\left[\sqrt{d}\right])\subset\mathbb{Z}$。据此证明：$\mathbb{Z}\left[\sqrt{d}\right]^{\times}=\big\{z\in\mathbb{Z}\left[\sqrt{d}\right]\big|N(z)=\pm1\big\}$。

5. 对于 $d<0$，试计算 $\mathbb{Z}\left[\sqrt{d}\right]^{\times}$。

当 $d>0$ 时，$\mathbb{Z}\left[\sqrt{d}\right]^{\times}$ 的结构要复杂的多。实际上，

$$N(z=x+y\sqrt{d})=\pm1\quad\Leftrightarrow\quad x^2-dy^2=\pm1.$$

上述方程通常被称作是 Pell 方程。研究 $\mathbb{Z}\left[\sqrt{d}\right]^{\times}$ 可以给出以上方程所有的整数解。

1. 证明，$\mathbb{Z}\left[\sqrt{2}\right]^{\times}\cap(1,3)=\{1+\sqrt{2}\}$。

2. 证明，$\mathbb{Z}\left[\sqrt{2}\right]^{\times}=\{\pm\big(1+\sqrt{2}\big)^k\big|k\in\mathbb{Z}\}$ 并给出群同构 $\mathbb{Z}\left[\sqrt{2}\right]^{\times}\simeq\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$。

3. 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 $d>0$。

1. 证明，有序列 $\{z_n\}_{n\geqslant1}\subset\mathbb{Z}\left[\sqrt{d}\right]^{\times}$，使得 $\lim\limits_{n\to\infty}z_n=0$ 而 $\{N(z_n)\}_{n\geqslant1}$ 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 $q\leqslant M$，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）

2. 证明，存在上述序列的子序列 $\{w_n\}_{n\geqslant1}$ 以及整数 k，使得对任意的 $n,m\geqslant1$，我们有 $N(w_n)=k$ 并且 $w_n\overline{w}_m\in k\mathbb{Z}\left[\sqrt{d}\right]$。（提示：考虑 w_n 在 $\mathbb{Z}\left[\sqrt{d}\right]/k\mathbb{Z}\left[\sqrt{d}\right]$ 中的像）

3. 证明，$\mathbb{Z}\left[\sqrt{d}\right]^{\times}$ 是无限集。

4. 证明，$\mathbb{Z}\left[\sqrt{d}\right]^{\times}\cap(0,\infty)$ 是乘法群 $(0,\infty)$ 的离散子群，即对任意的 $0<a<b<\infty$，$\mathbb{Z}\left[\sqrt{d}\right]^{\times}\cap(a,b)$ 是有限的。

5. 证明，存在 $\eta_d\in(1,\infty)$（被称作是**基本单位**），使得 η_d 生成了 $\mathbb{Z}\left[\sqrt{d}\right]^{\times}\cap(0,\infty)$。特别地，$\mathbb{Z}\left[\sqrt{d}\right]^{\times}\simeq\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$。

（注意到：对任意的 $u\in\mathbb{Z}\left[\sqrt{d}\right]^{\times}-\{\pm1\}$，四个点 $\pm u,\pm\overline{u}$ 在区间 $(-\infty,-1),(-1,0),(0,1),(1,\infty)$ 中各有一个）

4.6.3 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）。

1. （最大公约数与最小公倍数的概念）A 是整环，$a_1,\cdots,a_n\in A$。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 $a_1,\cdots,a_n$ 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 $a_1,\cdots,a_n$ 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。

2. 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。[24]
   - 证明，$(2,\sqrt{-4})$ 不是 $\mathbb{Z}[\sqrt{-4}]$ 中的主理想。[25]
   - 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 $N(x)\leqslant 4$ 的元素只有 $\pm1,\pm2$，其中，$d<-4$）

3. 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。

4. 当 $d=-1,-2,2$ 时，$\mathbb{Z}[\sqrt{d}]$ 是 Euclid 整环，其中，我们取范数[26]为 $\|z\|=|N(z)|=\left|z\cdot\overline{z}\right|$。

   （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 $q\in\mathbb{Z}[\sqrt{-1}]$，使得

   $$|\mathrm{Re}(q)-\mathrm{Re}(\frac{a}{b})|<\frac{1}{2},\ \ |\mathrm{Im}(q)-\mathrm{Im}(\frac{a}{b})|<\frac{1}{2}.$$

   此时，如果令 $r=a-qb$，$N(r)<N(b)$。）

[24] 实际上，通过研究 $2\cdot2=(1+\sqrt{3})(1-\sqrt{3})$，我们知道 $\mathbb{Z}[\sqrt{-3}]$ 不是唯一分解整环。

[25] 实际上，通过研究 $-2\cdot2=\sqrt{-4}\cdot\sqrt{-4}$，我们知道 $\mathbb{Z}[\sqrt{-4}]$ 不是唯一分解整环。

[26] 按定义，对于 $z=x+y\sqrt{d}$，$\overline{z}=y-y\sqrt{d}$，这未必是复共轭。

5. (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 $(x, y) = (3, \pm 5)$。

6. 试求 $y^2 = x^3 - 1$ 的所有整数解。

4.6.4 分圆多项式

对于 $n \geqslant 1$，令 $\xi_n = e^{\frac{1}{n}2\pi i}$，那么，$\{\xi_n^k\}_{0 \leqslant k \leqslant n-1}$ 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

$$\Phi_n(X) = \prod_{(k,n)=1, 1 \leqslant k \leqslant n} \big(X - \xi_n^k\big).$$

这个 $\Phi_n(X) \in \mathbb{C}[X]$ 被称作是**n-次分圆多项式**。

1. 证明，$\prod\limits_{d|n} \Phi_d(X) = X^n - 1$。(请参考第一次作业)
2. 计算 $\Phi_1(X)$ 和 $\Phi_p(X)$，其中，p 为素数。
3. 通过对 n 归纳证明，$\Phi_n(X) \in \mathbb{Z}[X]$。
4. 假设 $z_0 \in \mathbb{C}$。证明，$I_{z_0} = \{Q(X) \in \mathbb{Q}[X] | Q(z_0) = 0\}$ 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 $I_{z_0} = \big(P\big)$ 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**。
5. ζ 是一个本原的 n-次单位根，证明，其极小多项式 $P(X) \in \mathbb{Z}[X]$。
6. 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，$\mathbb{Z}[\zeta] = \Big\{ \sum\limits_{\text{有限和}} a_k \zeta^k \big| a_k \in \mathbb{Z}, k = 1, 2, \cdots \Big\}$ 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。
7. 证明，$\Phi_n(X)$ 在 $\mathbb{Q}[X]$ 不可约。(提示：研究 P 与 Φ_n 的关系)

注记 4.34. 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。

4.6.5 用模的观点看线性代数

K 是域，$n \geqslant 1$，V 是 n 维 K-线性空间，$T \in \mathbf{End}_K(V)$ 是 V 到自身的 K-线性映射。那么，V 可以被视为 $K[X]$-模：

$$K[X] \times V \to V, \quad P(X) \mapsto \ (v \mapsto P(T)v).$$

根据主理想整环 $K[X]$ 上的有限生成模的分类定理，存在唯一的首一多项式 $P_1, \cdots, P_s \in K[X]$，使得 $P_1 \mid P_2, P_2 \mid P_3, \cdots, P_{s_1} \mid P_s$ 并且有如下 $K[X]$-模的分解：

$$V \simeq {K[X]}\big/{(P_1(X))} \oplus {K[X]}\big/{(P_2(X))} \oplus \cdots \oplus {K[X]}\big/{(P_s(X))}.$$

我们称 $P_1, \cdots, P_s$ 为 T 的**不变因子**。

1. 证明，$\left\{P \in K[X] \middle| P(T) = 0\right\}$ 为 $K[X]$ 的理想并且由其中唯一的首一且次数最低的多项式 $m_T(X)$ 生成。这个多项式被称作是 T 的**极小多项式**。

2. 证明，$m_T(X) = P_s(X)$。

3. 令 $p_T(X)$ 为 T 的特征多项式。证明，

$$p_T(X) = P_1(X)P_2(X)\cdots P_s(X).$$

4. 给定 V 的一组基 $\{e_i\}_{1 \leqslant i \leqslant n}$，用 $A = (a_{ij})_{1 \leqslant i,j \leqslant n} \in \mathbf{M}_n(K)$ 表示 T 对应的矩阵，其中，$a_{ij} \in K$；I 为 $n \times n$ 的单位矩阵。令 $L = X \cdot I - A = \begin{pmatrix} X - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & X - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & X - a_{nn} \end{pmatrix} \in \mathbf{M}_n(K[X])$。我们考虑 $K[X]$-模之间的同态：

$$L : K[X]^n \to K[X]^n, \begin{pmatrix} F_1(X) \\ F_2(X) \\ \vdots \\ F_n(X) \end{pmatrix} \mapsto \begin{pmatrix} X - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & X - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & X - a_{nn} \end{pmatrix} \begin{pmatrix} F_1(X) \\ F_2(X) \\ \vdots \\ F_n(X) \end{pmatrix}$$

以及

$$\pi : K[X]^n \to V, \begin{pmatrix} F_1(X) \\ F_2(X) \\ \vdots \\ F_n(X) \end{pmatrix} \mapsto \sum_{i=1}^{n} F(T) \cdot e_i.$$

证明，我们有 $K[X]$-模之间的正合列：

$$K[X]^n \xrightarrow{L} K[X]^n \xrightarrow{\pi} V \to 0,$$

即证明 $\mathrm{Ker}(\pi) = \mathrm{Im}L$ 并且 $V \simeq {K[X]^n}\big/{\mathrm{Im}L}$。

如果存在可逆的 $P \in \mathbf{End}_K(V)$，使得 $P \circ S \circ P^{-1} = T$，就称 S 与 T 是（通过 P）**相似的**。

$$\begin{array}{ccc} V & \xrightarrow{S} & V \\ {\scriptstyle P}\downarrow & & \downarrow{\scriptstyle P} \\ V & \xrightarrow[T]{} & V \end{array}$$

另外，根据 S 和 T 可分别在 V 上定义出（两个）$K[X]$-模的结构。第一个记作 V_S：

$$K[X]\times V\to V,\ \ P(X)\mapsto\ (v\mapsto P(S)v);$$

第二个记作 V_T：

$$K[X]\times V\to V,\ \ P(X)\mapsto\ (v\mapsto P(T)v).$$

5. 证明，若 S 与 T 是通过 P 相似的，则以下映射是 $K[X]$-模同构：

$$V_S\longrightarrow V_T,\ \ v\mapsto P(v).$$

6. 证明，S 与 T 与 P 相似当且仅当 $K[X]$-模 V_S 与 V_T 同构。

7. 证明，S 与 T 与 P 相似当且仅当 S 与 T 具有同样的不变因子。

8. 给定 V 一组基使得 S 和 T 可以用矩阵表示（仍然记作 S 和 T）证明，S 与 T 与 P 相似当且仅当 $X\cdot I-S$ 与 $X\cdot I-T$ 在 $\mathbf{M}_n(K[X])$ 中共轭，即存在 $P\in\mathbf{GL}(n;K[X])$，使得 $P\cdot(X\cdot I-S)\cdot P^{-1}=X\cdot I-T$。

9. 应用：试计算 $\mathbf{GL}(2;\mathbb{F}_3)$ 的共轭类的个数。

10. 应用：给定域扩张 L/K 以及 $A,B\in\mathbf{M}_n(K)$。证明，若存在 $P\in\mathbf{GL}(n;L)$ 使得 $PAP^{-1}=B$，则存在 $Q\in\mathbf{GL}(n;K)$ 使得 $QAQ^{-1}=B$。

    （提示：参考 Smith 标准型唯一性的证明）

11. 给定 $\lambda\in K$。证明，λ 是特征值等价于 $X-\lambda\mid p_T(\lambda)$，即 λ 为 $p_T(\lambda)$ 的根。令 V_λ 为 λ 对应的特征子空间（若 λ 不是特征值，则 $V_\lambda=0$）。令 $\mu_a(\lambda)$ 为 λ 作为 $p_T(\lambda)$ 的根的重数，我们称它为 λ 的**代数重数**；令 $\mu_g(\lambda)=\dim_K V_\lambda$，我们称它为 λ 的**几何重数**。

12. 证明，$\mu_g(\lambda)=\big|\{i\big|X-\lambda\text{乘除}P_i(X)\}\big|$，其中，$\{P_i\}_{i\leqslant s}$ 为 T 的不变因子。

    （提示：可以将 $K[X]$-模 V 进一步分解为

$$V\simeq\left(\bigoplus_{\text{有限}}K[X]/(X-\lambda)^e\right)\oplus\left(\bigoplus_{\text{有限和，}Q\text{ 不可约，}Q(\lambda)\neq 0}K[X]/(Q(X))^e\right)$$

    并研究 $X-\lambda$ 在分量上的作用）

13. 证明，$\mu_g(\lambda)\leqslant\mu_a(\lambda)$ 并且 $\sum\limits_\lambda\mu_g(\lambda)\leqslant\dim_k V$。

14. 证明，T 可被对角化当且仅当其极小多项式 $m_T(X)$ 分裂成一次多项式的乘积。

4.7 练习题

1. A 是环（未必交换）。证明，如果 $a\in A$ 是幂零元[27]，$b\in A^\times$ 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，$1-ba\in A^\times$。

[27]即存在 $n\geqslant 1$，使得 $a^n=0$

3. A 是交换环，$\mathfrak{Nil}(A)=\{a\in A|$存在 $n\geqslant 1$，使得 $x^n=0\}$，$\mathrm{Spec}(A)$ 是 A 的所有素理想的集合。证明，$\mathfrak{Nil}(A)=\bigcap\limits_{\mathfrak{p}\in\mathrm{Spec}(A)}\mathfrak{p}$。

4. A 是交换环，$\mathrm{SpecMax}(A)$ 是其极大理想的集合，其 **Jacobson 根式理想**被定义为 $J(A)=\bigcap\limits_{\mathfrak{m}\in\mathrm{SpecMax}(A)}\mathfrak{m}$。

   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

$$\big\{A\text{ 的左理想 }J\supset I\big\}\xrightarrow{1:1}\big\{{}^{A}\!/\!_{I}\text{ 的左理想}\big\},\quad J\mapsto {}^{J}\!/\!_{I}.$$

6. A 和 B 是交换环，$\varphi:A\to B$ 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，$\varphi:A\to B$ 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 $\mathbb{Z}\to\mathbb{Q}$ 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，$\mathfrak{p}_1,\cdots,\mathfrak{p}_n$ 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，$I_1,\cdots,I_n$ 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 $n\geqslant 1$，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 $T\in\mathrm{End}_K(V)$ 可以给出 V 上的一个 $K[X]$-模的结构：

$$K[X]\times V\to V,\quad (P(X),v)\mapsto P(T)v.$$

    证明，V 上的每一个 $K[X]$-模的结构都恰好有某个 $T\in\mathrm{End}_K(V)$ 唯一决定。

13. $\mathbb{Z}[X]$ 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？

14. 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。

15. 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

$$_{W}J=\big\{\varphi\in\mathbf{End}_K(V)\big|\mathrm{Ker}(\varphi)\supset W\big\},\quad J_{W}=\big\{\varphi\in\mathbf{End}_K(V)\big|\mathrm{Im}(\varphi)\subset W\big\}.$$

    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：

$$\big\{V\text{ 的线性子空间}\big\}\xrightarrow{1:1}\big\{\mathbf{End}_K(V)\text{ 中左理想}\big\},\quad W\mapsto {}_{W}J,$$
$$\big\{V\text{ 的线性子空间}\big\}\xrightarrow{1:1}\big\{\mathbf{End}_K(V)\text{ 中右理想}\big\},\quad W\mapsto J_{W}.$$

16. 环 $\mathbf{M}_n\left(\mathbb{Z}/p\mathbb{Z}\right)$ 中一共有多少个极大的左理想？当 $n=4$ 时，环 $\mathbf{M}_4\left(\mathbb{Z}/p\mathbb{Z}\right)$ 中一共有多少个左理想？

17. A 是交换环，$I\subset A$ 是理想，M 是 A-模。验证，$I\cdot M=\{\sum\limits_{\text{有限和}} a_i\cdot x_i|a_i\in I,x_i\in M\}$ 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。

18. 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

$$\left\{N'\text{ 是 }M\text{ 的子模且 }N'\supset N\right\}\xrightarrow{1:1}\left\{M/N\text{ 的子模}\right\},\quad N'\mapsto N'/N.$$

19. A 是交换环，M',M 和 M'' 是 A-模，假定我们有如下正合列[28]：

$$0\to M'\xrightarrow{\varphi}M\xrightarrow{\psi}M''\to 0.$$

    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 $s:M''\to M$，使得 $\psi\circ c=\mathrm{id}_{M''}$；
    - 存在 A-模同态 $p:M\to M'$，使得 $p\circ\varphi=\mathrm{id}_M$。

    以上发生的话，我们就称改正合列是**分裂的**。

20.（五引理）给定 A-模同态的交换图表：

$$\begin{array}{ccccccccc}
M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 & \longrightarrow & M_5 \\
\downarrow{\scriptstyle\psi_1} & & \downarrow{\scriptstyle\psi_2} & & \downarrow{\scriptstyle\psi_3} & & \downarrow{\scriptstyle\psi_4} & & \downarrow{\scriptstyle\psi_5} \\
N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 & \longrightarrow & N_5
\end{array}$$

    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。

21. A 是交换环，M,M' 和 N 是 A-模，试描述 $\mathrm{Hom}_A(M,N)$ 上自然的 A-模结构。给定 A-模同态 $\varphi:M'\to M$。证明，如下映射

$$\widehat{\varphi}:\mathrm{Hom}_A(M,N)\to\mathrm{Hom}_A(M',N),\quad f\mapsto\varphi g,$$

    和

$$\widehat{\varphi}:\mathrm{Hom}_A(N,M')\to\mathrm{Hom}_A(N,M),\quad g\mapsto\varphi\circ g,$$

    是 A-模同态。进一步证明所谓的 $\mathrm{Hom}_A(\cdot,\cdot)$ 的左正合性：

---

[28]这里指的是 $\varphi:M'\to M$ 是单的 A-模同态，$\psi:M\to M''$ 是满的 A-模同态并且 $\mathrm{Ker}(\psi)=\mathrm{Im}(\varphi)$。

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 $\varphi_j:M_k\to M_{j+1}$ 是 A-模同态并且 $\mathrm{Im}(\varphi_k)=\mathrm{Ker}(\varphi_{k+1})$，其中，$j=1,2,\cdots,n-1$ 而 $k=1,2,\cdots,n-2$。我们还经常省略掉映射而把正合列写成

$$M_1\longrightarrow M_2\longrightarrow\cdots\longrightarrow M_{n-1}\longrightarrow M_n.$$

- 给定 A-模的正合列
$$0 \to M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'',$$
我们有如下 A-模的正合列
$$0 \to \mathrm{Hom}_A(N, M') \xrightarrow{\widehat{\varphi}} \mathrm{Hom}_A(N, M) \xrightarrow{\widehat{\psi}} \mathrm{Hom}_A(N, M'').$$

- 给定 A-模的正合列
$$M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0,$$
我们有如下 A-模的正合列
$$0 \to \mathrm{Hom}_A(M'', N) \xrightarrow{\widehat{\psi}} \mathrm{Hom}_A(M, N) \xrightarrow{\widehat{\varphi}} \mathrm{Hom}_A(M', N).$$

22. 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 $\varphi : M \to N$，证明，有自然的 A-模同态 $T(\varphi) : T(M) \to T(N)$。

- 给定 A-模的正合列
$$0 \to M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'',$$
证明，我们有如下 A-模的正合列
$$0 \to T(M') \xrightarrow{T(\varphi)} T(M) \xrightarrow{T(\psi)} T(M'').$$

- 试构造 A-模的满同态 $M \overset{\psi}{\twoheadrightarrow} M''$，使得 $T(\psi) : T(M) \to T(M'')$ 不是满射。

5 域的扩张

除了常见的域 $\mathbb{Q},\mathbb{R},\mathbb{C}$ 或者 $\mathbb{F}_p$，在后面的章节中我们还会研究**函数域**。给定域 K，$K[X]$ 是 K 上的多项式环，我们定义

$$K(X)=\mathrm{Frac}\big(K[X]\big)=\left\{\frac{P(X)}{Q(X)}\Big|P,Q\in K[X],Q\neq 0\right\}.$$

按照定义，$\frac{P_1}{Q_1}=\frac{P_2}{Q_2}$，其中，$P_1Q_2=P_2Q_1$。我们把 $K(X)$ 称作是 K 上的**（一元）函数域**。

首先引入域的特征的概念。对任意域 K，有自然的环同态

$$\iota:\mathbb{Z}\to K,$$

其中，$\iota(n)=n\cdot 1_K$，这里 1_K 为 K 的单位元。若 ι 为单射，则称 K 的**特征为零**并记作 $\mathrm{char}(K)=0$；否则，存在唯一的素数 p，使得 $\mathrm{Ker}(\iota)=p\mathbb{Z}$，即 $p\cdot 1_K=0$，此时称 K 的**特征为** p 并记作 $\mathrm{char}(K)=p$。很明显，$\mathbb{Q},\mathbb{R},\mathbb{C}$ 是特征为零的域而 $\mathbb{Z}\big/p\mathbb{Z}$ 的特征为 p。

- 如果 $\mathrm{Char}(K)=0$，环同态 $\iota:\mathbb{Z}\to K$ 可以延拓到 $\mathbb{Q}$ 上，即 $\iota\left(\frac{m}{n}\right)=\frac{\iota(m)}{\iota(n)}$，其中，$m,n\in\mathbb{Z}$，即有自然的域同态：
$$\mathbb{Q}\longrightarrow K.$$
所以，K 总（以唯一的方式）包含 $\mathbb{Q}$ 作为其子域。
- 如果 $\mathrm{Char}(K)=p$，环同态 $\iota:\mathbb{Z}\to K$ 给出了域同态
$$\bar{\iota}:\mathbb{F}_p=\mathbb{Z}\big/p\mathbb{Z}\to K,$$
此时 K 总（以唯一的方式）包含 $\mathbb{F}_p$ 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**。本原域在域扩张下不变：

引理 70. *给定域扩张 $L\big/K$，则 $\mathrm{Char}(K)=\mathrm{Char}(L)$。*

证明： 考虑环同态的交换图表：

$$\begin{array}{ccc}\mathbb{Z} & \xrightarrow{\ \iota\ } & L\\ & \searrow^{\iota'} & \uparrow\\ & & K\end{array}$$

因为域扩张映射 $K\to L$ 是单射，所以 $\mathrm{Ker}(\iota)=\mathrm{Ker}(\iota')$。命题得证。 □

例子 5.1. 域 K 的特征为 p，所谓的 Frobenius 映射定义如下：

$$\mathrm{Frob}:K\longrightarrow K,\quad x\mapsto x^p.$$

那么，Frob 是域同态。

实际上，对任意的 $x,y\in K$，我们有

$$\mathrm{Frob}(x+y)=(x+y)^p=x^p+y^p+\sum_{k=1}^{p-1}\binom{p}{k}x^ky^{p-k}.$$

当 $1\leqslant k\leqslant p-1$ 时，$p\mid\binom{p}{k}$，所以上述求和中的项均为 0。从而，

$$\mathrm{Frob}(x+y)=x^p+y^p=\mathrm{Frob}(x)+\mathrm{Frob}(y).$$

这说明 Frob 是域同态。

5.1 代数扩张

定义 5.1. 给定域扩张 L/K 和 L'/K 和域同态 $\varphi: L \to L'$，如果 $\varphi\big|_K = \mathrm{id}_K$，即对任意的 $x \in K$，$\varphi(x) = x$，就称 φ 为**K-同态**。

$$\begin{array}{ccc} L & \xrightarrow{\varphi} & L' \\ | & & | \\ K & \xrightarrow{\mathrm{id}_K} & K \end{array}$$

用 $\mathbf{Hom}_K(L, L')$ 表示所有的 K-同态，用 $\mathbf{End}_K(L)$ 表示所有 L/K 到自身的 K-同态，用 $\mathbf{Aut}_K(L)$ 表示所有 L/K 到自身的 K-同构。

注记 5.1. $\mathbf{Aut}_K(L)$ 配有同态的复合是群。

定义 5.2. 给定域扩张 L/K 和 $x \in L$。如果存在非零的 K-系数多项式 $P(X) \in K[X]$，使得 $P(x) = 0$，就称 x **在 K 上是代数的**。此时，存在唯一[29]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**。

如果以上不成立，即对任意非零 K-系数多项式 $P(X) \in K[X]$，$P(x) \neq 0$，就称x **在 K 上是超越的**。

如果每个 $x \in L$ 在 K 上均为代数的，就称域扩张 L/K 是**代数扩张**。

注记 5.2. 根据极小多项式次数最低的性质，$P(X)$ 是 $K[X]$ 上的不可约多项式。

注记 5.3 (由代数元生成的子域)**.** 给定域扩张 L/K 中的一个代数元 $x \in L$，我们考虑由多项式的取值给出的环同态：

$$\mathrm{ev}_x : K[X] \twoheadrightarrow K[x], \qquad Q(X) \longmapsto Q(x).$$

即将多项式 $Q(X)$ 在 x 处取值。这显然满射。

假设 $P(X)$ 是 x 在 K 上的极小多项式，从而，$P(x) = 0$，所以，$P \in \mathrm{Ker}(\mathrm{ev}_x)$。另外，对于 $Q(X) \in \mathrm{Ker}(\mathrm{ev}_x)$，根据多项式的带余除法，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，我们有

$$R(x) = Q(x) - A(x)P(x) = 0.$$

根据极小多项式次数最低的性质，我们知道 $R = 0$，从而，$Q = AP$。以上推导表明 $\mathrm{Ker}(\mathrm{ev}_x) = \big(P(X)\big)$。根据环同态第一定理，我们得到环同构

$$K[X]/\big(P(X)\big) \xrightarrow{\simeq} K[x] \subset L.$$

另外，$\big(P(X)\big)$ 是极大理想[30]，从而 $K[x]$ 是域。特别地，$K[x]$ 是 L 的子域。

我们进一步说明 $K[x] = K(x)$。根据定义，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，$K[x] = K(x)$。通过 $K(x)$ 的定义中的最小性也可以证明 $K[x] = K(x)$：$K(x)$ 是包含 x 的最小的域，而 $K[x]$ 是域并且包含 x，所以 $K[x] = K(x)$。

命题 71. *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。*

[29] 利用 $K[X]$ 是主理想整环或者辗转相除法

[30] 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 $I \subset \big(P(X)\big)$ 是非平凡理想，那么，$I = \big(P_1(X)\big)$，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 $I = \big(P(X)\big)$。

进一步，$[K(x):K]=\deg P(X)$，其中，$P(X)$ 为 x 的极小多项式而 $1,x,\cdots,x^{\deg(P)-1}$ 是 $K(x)/K$ 的一组基。

我们还有如下域同构的序列：

$$K[X]/\big(P(X)\big)\xrightarrow{\simeq}K[x]\xhookrightarrow{\simeq}K(x).$$

证明：假设 $K(x)/K$ 是有限扩张，那么，（可能）无限个元素 $1,x,\cdots,x^n,\cdots$ 在 K 上线性相关，从而存在 $a_0,\cdots,a_n\in K$，$a_n\neq 0$，使得

$$a_0+a_1x+\cdots+a_nx^n=0\quad\Leftrightarrow\quad P(x)=0,\ P(X)=\sum_{k=0}^{n}a_kX^k\in K[X].$$

这表明 x 在 K 上是代数的。

如果 x 在 K 上是代数的，我们考虑它的极小多项式 $P(X)=X^n+\sum_{k=0}^{n-1}a_kX^k$，其中，$n\geqslant 1$。根据 $P(x)=0$，我们知道 $1,x,\cdots,x^n$ 在 K 上线性相关；根据 P 的最小性，$1,x,\cdots,x^{n-1}$ 在 K 上线性无关，（否则将有次数更低的 K-系数多项式以 x 为根）。这说明 $1,x,\cdots,x^{n-1}$ 是 $K(x)/K$ 的基。

至此，命题中结论均已证明。 □

推论 72. 有限扩张是代数扩张。

证明：对任意给定的有限扩张 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，即 L 中所有元素均为代数的，所以 L/K 是代数扩张。 □

推论 73. 给定域扩张 L/K，如下命题成立：

1) 子集 $M\subset L$ 中的每个元素在 K 上均为代数的，那么，$K(M)/K$ 是代数扩张。进一步，如果 M 还是有限集，那么 $K(M)/K$ 是有限扩张。

2) 令 $K^{\mathrm{alg}}=\big\{x\in L|x\text{ 在 }K\text{ 上是代数的}\big\}$，那么，$K^{\mathrm{alg}}$ 是 L 的子域。特别地，K^{alg}/K 是 L/K 中最大的[31]、代数的中间域。

证明：假设 $M=\{m_1,\cdots,m_k\}\subset L$ 是在 K 上代数的元所构成的有限子集，根据以上命题，$K(m_1)/K$ 是有限扩张；而 m_2 显然在 $K(m_1)$ 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 $K(m_1,\cdots,m_k)/K$ 是有限扩张。

现在仅假设 $M\subset L$ 是由在 K 上代数的元素构成的子集（未必有限）。对任意的 $x\in K(M)$，存在 $m_1,\cdots,m_k\in M$，使得 $x\in K(m_1,\cdots,m_k)$。以上我们已经证明了 $K(m_1,\cdots,m_k)/K$ 是有限扩张，所以，$K(x)/K$ 是有限扩张，即 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^{alg} 是子域，对 $M=K^{\mathrm{alg}}$ 运用上面的结论，从而 $K\left(K^{\mathrm{alg}}\right)$ 中元素均为代数的。根据 K^{alg} 的定义，$K\left(K^{\mathrm{alg}}\right)\subset K^{\mathrm{alg}}$。这表明，$K\left(K^{\mathrm{alg}}\right)=K^{\mathrm{alg}}$ 而 $K\left(K^{\mathrm{alg}}\right)$ 是子域。 □

推论 74. 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：如果 L/K 是代数扩张，很明显 L/E 和 E/K 均为代数扩张。

如果 L/E 和 E/K 均为代数扩张。对任意的 $x\in L$，根据 L/E 是代数扩张的定义，存在正整数 n 和 $e_0,\cdots,e_{n-1}\in E$，使得

$$x^n+e_{n-1}x^{n-1}+\cdots+e_1x+e_0=0.$$

[31]在包含关系下。

这表明 x 在 $K(e_{n-1},\cdots,e_0)$ 上是代数的，从而，$K(e_{n-1},\cdots,e_0,x)/K(e_{n-1},\cdots,e_0)$ 是有限扩张。另外，由于 $e_0,\cdots,e_{n-1}$ 在 K 上是代数的，所以，$K(e_{n-1},\cdots,e_0)/K$ 是有限扩张。综上所述，$K(e_{n-1},\cdots,e_0,x)/K$ 是有限扩张，所以，x 在 K 上是代数的。 □

5.2 代数闭包

命题 75. *K 是域，$P\in K[X]$，则存在有限域扩张 K_P/K，使得 P 在 K_P 中有根，即存在 $y\in K_P$，使得 $P(y)=0$。*

证明： 不妨设 $P(X)$ 不可约，否则考虑 P 的一个不可约因子即可。考虑环同态的复合

$$K\hookrightarrow K[X]\longrightarrow K[X]/(P)=:K_P.$$

这是 K 的有限扩张。记 $\varphi:K[X]\longrightarrow K_P$，记 $X\in K[X]$ 在 K_P 中的像为 y，即 $\varphi(X)=y$。

由于 $P(X)$ 在 $K[X]/(P)$ 中的像为 0，根据 φ 是域同态，有

$$P(\varphi(X))=\varphi(P(X))=0,$$

即 $P(y)=0$。 □

命题 76. *K 是域，则如下性质等价：*

1) 每个次数至少为 1 的多项式 $P\in K[X]$ 在 K 中有根；

2) $K[X]$ 中不可约多项式（默认其次数至少为 1）的均为 1 次多项式；

3) 若 L/K 是代数扩张，则 $L=K$。

*若 K 满足以上性质，则称其为**代数封闭域**。*

证明： 1)$\Leftrightarrow$ 2) 是显然的。先证明 2)$\Rightarrow$ 3)：对任意的 $x\in L$，令 $P\in K[X]$ 为其极小多项式，从而，$P(X)=X-x$，从而，$x\in K$，即 $L\subset K$。

再证 3)$\Rightarrow$ 2)。任选不可约多项式 $P\in K[X]$，则 K_P/K 是代数扩张，从而 $K_P=K$。所以，$\deg(P)=[K_P:K]=1$。 □

定义 5.3. *K 是域，若 Ω/K 为代数扩张且 Ω 是代数封闭域，就称 Ω 为 K 的一个**代数闭包**。*

以下我们证明域 K 具有唯一（在 K-同构的意义下）的代数闭包。

5.2.1 代数闭包的存在性

引理 77. *K 是域，$P(X)\in K[X]$，则存在代数扩张 L/K，使得 P 在 L 中**分裂**，即在 $L[X]$ 中，有*

$$P(X)=a(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n).$$

其中 $a\in K$，$\alpha_1,\cdots,\alpha_n\in L$。

证明： 对 P 的次数进行归纳：当 $\deg(P)\leqslant 1$ 时，命题是平凡的。假设 $\deg(P)\geqslant 2$，根据命题75，$P(X)$ 在代数扩张 K_P/K 中有根 α。将 $P(X)$ 视为 K_P 系数的多项式，则它在 $K_P[X]$ 中分解为

$$P(X)=(X-\alpha)\cdot Q(X),$$

其中，$\alpha\in K_P$ 并且 $\deg(Q)<\deg(P)$。根据归纳假设，存在代数扩张 L/K_P，使得 $Q(X)$ 在 $L[X]$ 中分裂，所以 $P(X)=Q(X)(X-\alpha)$ 也在 $L[X]$ 中分裂。 □

引理 78 (E. Artin)**.** K 是域，则存在域扩张 L/K，使得对任意次数至少为 1 的多项式 $P(X)\in K[X]$，P 在 L 中有根。

证明: 定义由 K 上所有非常数多项式作为不定元生成的多项式环

$$A:=K\left[X_P\middle|P\in K[X],\ \deg(P)\geqslant 1\right]=\bigcup_{\substack{F\subset K[X]-K,\\ |F|<\infty}}K\left[X_P|P\in F\right].$$

令 $\mathfrak{J}$ 为由形如 $P(X_P)$ 的元素所生成的理想，即

$$\mathfrak{J}=\left(P(X_P)\middle|P\in K[X],\ \deg(P)\geqslant 1\right),$$

其中，对 $P(X)=\sum_{i=0}^{n}a_iX^i$，$P(X_P)=\sum_{i=0}^{n}a_iX_P^i\in A$，其中，$a_i\in K$。类似于命题75，对任意的 $P\in K[X]$，P 在 $A/\mathfrak{J}$ 中有根。为了保证得到域扩张，还需要如下的细节:

- $\mathfrak{J}\neq A$。

  若不然，则有 $P_1,\cdots,P_n\in K[X]$ 以及 $Q_1,\cdots,Q_n\in A$，使得

  $$\sum_{k=1}^{n}Q_k\cdot P_k(X_{P_k})=1.$$

  不失一般性，可假设 $Q_k=Q_k(X_{P_1},\cdots,X_{P_n})$。用变元 T_k 表示 X_{P_k}，以上等式表明

  $$\sum_{k=1}^{n}Q_k(T_1,\cdots,T_n)\cdot P_k(T_k)=1. \tag{5.1}$$

  根据引理77，存在域扩张 K'，使得每个 P_k 在 K' 中有根 α_k，其中，$k=1,\cdots,n$。据此，可以构造环同态

  $$K[T_1,\cdots,T_k]\to K',\ \ T_k\mapsto\alpha_k,\ k=1,\cdots,n.$$

  此时，(5.1)的左端的像为 0 而右端的像为 1，矛盾。

- 任选 A 的极大理想 $\mathfrak{m}$，使得 $\mathfrak{m}\supset\mathfrak{J}$ 并定义 $L=A/\mathfrak{m}$。那么，L 是域并且以下复合映射

  $$K\to A/\mathfrak{J}\to A/\mathfrak{m}$$

  给出了域扩张 L/K

根据 $\mathfrak{J}$ 的定义，$P(X_P)$ 在 $A/\mathfrak{J}$ 中为 0，从而在 $A/\mathfrak{m}$ 中为 0，即 $X_P+\mathfrak{m}\in L$ 是多项式 $P(X)$ 的根。 □

注记 5.4. 给定域 K，记以上引理中的 $L=A/\mathfrak{m}$ 为 $E(K)$。我们注意到以上的构造过程不能保证 $E(K)/K$ 为代数扩张。

对 $k\geqslant 1$，我们归纳地定义

$$E^{k+1}(K)=E(E^k(K)).$$

这给出了域扩张的序列:

$$K\ \text{——}\ E(K)\ \text{——}\ E^2(K)\ \text{——}\ \cdots\ \text{——}\ E^k(K)\ \text{——}\ \cdots.$$

令 $E^\infty(K)=\bigcup_{k\geqslant 1}E^k(K)$，则 $E^\infty(K)$ 是域: 因为对任意的 $x\in E^\infty(K)$，则存在 $k\geqslant 1$，使得 $x\in E^k(K)$，从而 $x^{-1}\in E^k(K)\subset E^\infty(K)$。

根据构造，$E^\infty(K)$ 还是代数封闭域: 实际上，对任意 $P(X)\in E^\infty(K)[X]$，存在 $k\geqslant 1$，使得 $P(X)\in E^k(K)[X]$。此时，$P(X)$ 的根均落在 $E^{k+1}(K)\subset E^\infty(K)$ 中。

引理 79. 给定域扩张 L/K，其中 L 是代数封闭域，则

$$\Omega = \{x \in L | x \text{ 在 } K \text{ 上是代数的}\}$$

是 K 的代数闭包。

证明：由于 $\Omega = K(\Omega)$ 是 K 通过添加代数元得到域扩张，所以 Ω/K 是代数扩张。现在证明 Ω 是代数封闭的。任选多项式

$$P(X) = \omega_n X^n + \cdots + \omega_1 X + \omega_0 \in \Omega[X],$$

根据 L 是代数封闭的，对任意 P 的根 $x \in L$，只要证明 $x \in \Omega$ 即可。根据 Ω 的定义，这等价于证明 x 在 K 上是代数的。实际上，由于 $\omega_0, \cdots, \omega_n$ 在 K 上是代数的，x 在 $K(\omega_0, \cdots, \omega_n)$ 上是代数的，所以域扩张

$$K \text{ —— } K(\omega_0, \cdots, \omega_n) \text{ —— } K(\omega_0, \cdots, \omega_n, x)$$

是有限扩张。从而，x 在 K 上是代数的。 □

根据这个引理，我们最终可以完成 K 的代数闭包的构造。定义

$$\Omega = \{x \in E^\infty(K) | x \text{ 在 } K \text{ 上是代数的}\}.$$

由于 $E^\infty(K)$ 是代数封闭的，所以 Ω 是 K 的代数闭包。

5.2.2 域同态扩张的技术引理

给定域扩张 L/K，$x \in L$，$P(X) \in K[X]$ 是 x 的极小多项式，我们有域同构

$$\mathrm{ev}_x : K[X]/(P(X)) \xrightarrow{\simeq} K(x) = K[x] \subset L, \quad Q(X) \mapsto Q(x).$$

特别地，$x \in L$ 定义出 K-同态：

$$\mathrm{ev}_x : K[X]/(P(X)) \longrightarrow L, \quad Q(X) \mapsto Q(x).$$

引理 80. 给定域扩张 L/K 以及不可约多项式[32] $P(X) \in K[X]$，令 $Z_P(L)$ 为 P 在 L 中（不同的）根的集合，即

$$Z_P(L) = \{P(\alpha) = 0 | \alpha \in L\}.$$

那么，我们有如下一一对应：

$$Z_P(L) \xrightarrow{1:1} \mathrm{Hom}_K\left(K[X]/(P(X)), L\right),$$

$$\alpha \longmapsto \mathrm{ev}_\alpha$$

特别地，$\left|\mathrm{Hom}_K\left(K[X]/(P(X)), L\right)\right| \leqslant \deg(P)$。

注记 5.5. 简而言之，不可约多项式 $P(X)$ 在 L 中不同根的个数等于把 $K_P \simeq K[X]/(P(X))$ 到 L 的 K-同态的个数。特别地，重根的出现使得域 K_P 到 L 的 K-同态减少。

[32]默认每个不可约多项式的次数至少是 1

证明: 给定 $\alpha \in Z_P(L)$，由于 P 不可约，在 α 处取值所定义环同态

$$\mathrm{ev}_\alpha : K[X] \to L, \quad Q(X) \mapsto Q(\alpha),$$

的核是 $\big(P(X)\big)$。这就定义了 K-同态：

$$\mathrm{ev}_\alpha : {}^{K[X]}\!/_{(P(X))} \to L, \quad Q(X) \mapsto Q(\alpha).$$

反之，对任意的 K-同态：

$$\varphi : {}^{K[X]}\!/_{(P(X))} \to L,$$

令 $\alpha = \varphi\big(X + (P(X))\big)$。由于 $P(X)$ 的像为 0，所以，

$$P(\alpha) = 0 = P\big(\varphi\big(X + (P(X))\big)\big) = \varphi(P(X)) = 0.$$

这就给出 P 在 L 中的一个根。

不难验证，以上映射互为逆，这就是命题要求的一一对应。

由于 $Z_P(L) \leqslant \deg(P)$，所以 $\left|\mathrm{Hom}_K\left({}^{K[X]}\!/_{(P(X))}, L\right)\right| \leqslant \deg(P)$。 □

注记 5.6. 该引理可以给出 ${}^{K[X]}\!/_{(P(X))}$ 的 K-自同构个数的控制：

$$\begin{aligned}\left|\mathbf{Aut}_K\left({}^{K[X]}\!/_{(P(X))}\right)\right| &= \left|\mathbf{Hom}_K\left({}^{K[X]}\!/_{(P(X))}, {}^{K[X]}\!/_{(P(X))}\right)\right| \\ &= Z_P\left({}^{K[X]}\!/_{(P(X))}\right) \leqslant \deg(P) = [{}^{K[X]}\!/_{(P(X))} : K].\end{aligned}$$

注记 5.7 (多项式系数的扩张)**.** 给定域同态 $\sigma : K \to L$，给定域 K 以及 $P(X) \in K[X]$。通过对系数的作用，多项式 $P^\sigma(X) \in L[X]$ 定义为：

$$P^\sigma(X) = \sum_{k=0}^{n} \sigma(a_k) X^k, \quad \text{其中}, \quad P(X) = \sum_{k=0}^{n} a_k X^k.$$

据此，我们得到环同态：

$$K[X] \longrightarrow L[X], \quad P \mapsto P^\sigma.$$

实际上，$P^\sigma \in \sigma(K)[X] \subset L[X]$。

引理80 在此情形下可以重新表述为如下的一一对应：

$$Z_{P^\sigma}(L) \xrightarrow{1:1} \mathrm{Hom}_\sigma\left({}^{K[X]}\!/_{(P(X))}, L\right).$$

其中，域同态 $\varphi \in \mathrm{Hom}_\sigma\left({}^{K[X]}\!/_{(P(X))}, L\right)$ 指的是对任意的 $k \in K$ 和 $y \in {}^{K[X]}\!/_{(P(X))}$，我们有

$$\varphi(k \cdot y) = \sigma(k)\varphi(y).$$

实际上，给定域扩张 ${}^{L}\!/_{K}, {}^{L'}\!/_{K'}$ 和域同态 $\sigma : K \to K', \varphi : L \to L'$，对任意的 $x \in K$，$\varphi(x) = \sigma(x)$，就称 φ 为**σ-同态**。

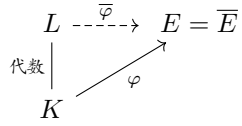
$$\begin{array}{ccc} L & \xrightarrow{\varphi} & L' \\ \big| & & \big| \\ K & \xrightarrow{\sigma} & K' \end{array}$$

我们习惯上用 $\mathbf{Hom}_\sigma(L, L')$ 表示所有的 σ-同态。

当 K 是 L 的子域而 $\sigma = \mathrm{id}$ 为嵌入映射时，引理80时上述一一对应的特例。

我们现在陈述代数封闭域的一种泛性质：

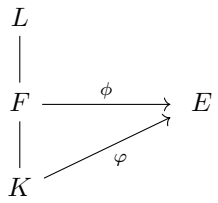
命题 81 (代数扩张的同态延拓)**.** 给定代数扩张 L/K，E 是代数封闭域。对任意的域同态 $\varphi: K \to E$，存在域同态 $\overline{\varphi}: L \to E$，使得 $\overline{\varphi}\big|_K = \varphi$。



注记 5.8. 我们不假设 L/K 是有限扩张。

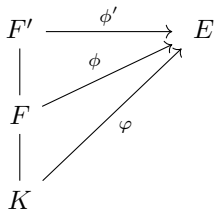
证明: 考虑如下延拓的集合

$$\mathscr{X} = \Big\{(F,\phi)\Big| F \text{ 是 } L/K \text{ 的中间域，} \phi: F \to E \text{ 是域同态并且 } \phi\big|_K = \varphi\Big\}.$$



注意到 $\mathscr{X}$ 是非空的：$(K,\varphi) \in \mathscr{X}$。

我们在 $\mathscr{X}$ 上定义偏序关系：$(F,\phi) \preceq (F',\phi')$，指的是 $F \subset F'$ 且 $\phi'\big|_F = \phi$，即



对 $\mathscr{X}$ 的全序子集 $\{(F_i,\phi_i)\}_{i\in I} \subset \mathscr{X}$，定义

$$F_\infty := \bigcup_{i\in I} F_i, \quad \phi_\infty\big|_{F_i} = \phi_i.$$

这就给出了[33]$\{(F_i,\phi_i)\}_{i\in I}$ 的一个上界 (F_∞,ϕ_∞)。根据 Zorn 引理，$\mathscr{X}$ 中有极大元 (F,ϕ)。如果这可以证明 $F = L$，那么 (F,ϕ) 就是 φ 在 L 上的延拓。

如若不然，任选 $x \in L - F$ 并考虑 x 在 F 上（x 在 F 上仍然是代数）的极小多项式 $P(X)$ 和域同构

$$\mathrm{ev}_x : F[X]/(P(X)) \xrightarrow{\simeq} F(x) \subset L.$$

通过同态 $\phi: F \to E$，我们知道 P^φ 在 E 中有根（因为 E 是代数封闭的）。根据引理80，我们就有域同态

$$\overline{\phi} : F[X]/(P(X)) \longrightarrow E.$$

从而，我们得到域同态

$$\overline{\phi} \circ (\mathrm{ev}_x)^{-1} : F(x) \longrightarrow E.$$

容易看出，$\overline{\phi}\big|_F = \varphi$。由于 $F(x)$ 是严格比 F 大的中间域，这与 F 的极大性矛盾。 □

[33]需要利用良序性验证 F_∞ 是域且 ϕ_∞ 的定义不依赖于 i 的选取，这些细节是平凡的。

5.2.3 代数闭包的唯一性

我们证明代数闭包的唯一性。

引理 82. L/K 是代数扩张，则 $\mathbf{End}_K(L) = \mathbf{Aut}_K(L)$，即代数扩张的 K-自同态必为自同构。

证明: 由于域同态为单射。只要证明任意的 $\varphi \in \mathbf{Hom}_K(L, L)$，$\varphi$ 是满射即可。实际上，对任意的 $x \in L$，令 P 为其极小多项式而 $Z_P(L)$ 为 P 在 L 中根的集合。那么，φ 把 P 的根映射为 P 的根，从而我们有单射:

$$\varphi : Z_P(L) \to Z_P(L).$$

由于多项式根的个数是有限，所以 Z_P 是有限集。那么，$\varphi : Z_P \to Z_P$ 是满射。特别地，存在 $y \in Z_P(L) \subset L$，使得 $\varphi(y) = x$。 □

K 是域，假设 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 $i = 1, 2$。根据命题81，存在域同态

$$\varphi \in \mathrm{Hom}_K(\Omega_1, \Omega_2), psi \in \mathrm{Hom}_K(\Omega_2, \Omega_1).$$

通过复合，我们就有 $\psi \circ \varphi \in \mathrm{End}_K(\Omega_1)$。以上引理表明 $\psi \circ \varphi$ 是 Ω_1 的 K-自同构；类似地，$\varphi \circ \psi$ 是 Ω_2 的 K-自同构。从而，φ 和 ψ 均为同构。综上所述，K 的代数闭包在 K-自同构的意义下是唯一的。

从此往后，对任意域 K，在 K-同构的意义下，我们用 $\overline{K}$ 表示它的代数闭包。如果 K 是代数封闭域，我们自然有 $\overline{K} = K$。

例子 5.2 ($\overline{\mathbb{Q}}$ 的构造)**.** 对 $\mathbb{C}/\mathbb{Q}$ 使用引理79，这表明 $\overline{\mathbb{Q}}$ 就是 $\mathbb{C}$ 中有理系数多项式的根组成的集合:

$$\mathbb{Q} = \big\{ z \in \mathbb{C} \big| \text{存在 } P \in \mathbb{Q}[X], \text{ 使得} P(z) = 0 \big\}.$$

5.3 环的整扩张

与域的代数扩张类似，我们还可以考虑环的整扩张。给定环 B 及其子环 $A \subset B$，我们称 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 $P(x) = 0$，就称 x 在 A 上是**整的**或者说 x 是 A 上的**整元素**。

给定环 A 及其扩张 B，B 中在 x 上的整元素可以用有限生成 A-模来刻画。由于在大部分数论或代数几何的场合，A 都是 Noether 环从而有限生成 A-模为 Noether 模，我们暂且偏离主题引入 Noether 模的概念。

5.3.1 Noether 模

所谓 Noether 环是每个理想均为有限生成的环，其等价定义是上升理想链的稳定条件，即对 A 中任意理想链

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots,$$

存在 $n_0 \geqslant 1$，使得当 $n \geqslant n_0$ 时，$I_n = I_{n_0}$。

定义 5.4. A 是环（不要求 A 是 Noether 环），M 是 A-模。若下述等价条件之一成立:

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 $n_0 \geqslant 1$，使得当 $n \geqslant n_0$ 时，$M_n = M_{n_0}$。

我们称 M 是 **Noether 模**。

注记 5.9. 以上两个条件等价性与 Noether 环情形的证明完全一致，我们留给对此怀疑的同学去验证。

注记 5.10. Noether 环上有限生成模是 Noether 模。

根据命题60，Noether 环上有限生成模的子模是有限生成的，所以定义中的 1) 成立。

引理 83. *给定 A-模的正合列*

$$0 \to M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \to 0,$$

则 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，所以 M' 是 Noether 模；作为 M 的商模，每个 M'' 中的上升子模序列都可以提升为（在 $M \to M''$ 下的逆像）M 中的上升子模序列，即

$$M_1'' \subset M_2'' \subset \cdots \subset M_n'' \subset \cdots$$

为 M'' 中的子模链，那么，

$$\psi^{-1}(M_1'') \subset \psi^{-1}(M_2'') \subset \cdots \subset \psi^{-1}(M_n'') \subset \cdots$$

为 M 中的子模链，从而有 n_0，使得 $n \geqslant n_0$ 时，$\psi^{-1}(M_n'') = \psi^{-1}(M_{n_0}'')$。作用 ψ，就有 $n \geqslant n_0$ 时，$M_n'' = M_{n_0}''$。所以，M'' 为 Noether 模。

假设 M' 和 M'' 为 Noether 模。N 为 M 的子模，则在 $M'' = {}^{M}\!/_{M'}$ 中，N 对应着 ${}^{N}\!/_{N \cap M'}$，即

$$\psi : N \twoheadrightarrow {}^{N}\!/_{N \cap M'} \subset M'' = {}^{M}\!/_{M'}.$$

根据 M'' 的 Noether 性，存在 $x_1, \cdots, x_k \in N$，使得 $\{x_i + M'\}_{i \leqslant k}$ 生成了 ${}^{N}\!/_{N \cap M'}$；根据 M' 的 Noether 性，存在 $y_1, \cdots, y_l \in N \cap M'$，使得 $\{y_j\}_{j \leqslant l}$ 生成了 $N \cap M'$。从而，对任意的 $z \in N$，利用 $\{x_i + M'\}_{i \leqslant k}$，存在 $a_i \in A$，使得 $z - \sum\limits_{i \leqslant k} a_i x_i \in M'$，从而，$z - \sum\limits_{i \leqslant k} a_i x_i \in M' \cap N$；再利用 $\{y_j + M'\}_{j \leqslant l}$，我们就有 $b_j \in A$，使得

$$z - \sum_{i \leqslant k} a_i x_i = \sum_{j \leqslant l} b_j y_j.$$

这表明有限集 $\{x_i\}_{i \leqslant k} \cup \{y_j\}_{j \leqslant l}$ 生成了 N。所以 M 是 Noether 模。 □

注记 5.11. A 是 Noether 环，则对任意自然数 n，A^n 是 Noether 模。实际上，当 $n = 1$ 时，将 A 视作是 A-模，其理想也就是子模均为有限生成的，所以 A 是 Noether 模。考虑自然的正合列

$$0 \to A \longrightarrow A \oplus A^n \longrightarrow A^n \to 0,$$

利用上述引理对 n 进行归纳，则 A^n 是 Noether 模。

由于每个有限生成的 A-模是某个 A^n 的商模，上述引理也可以推出 Noether 环上有限生成模是 Noether 模。

5.3.2 整性的刻画

我们现在研究环扩张中的整元素。

命题 84. *给定环的扩张 $A\subset B$。对 $x\in B$，令 $A[x]=\big\{P(x)\big|P(X)\in A[X]\big\}\subset B$，这是 A-模。则如下三个条件等价：*

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)⇒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 $y\in A[x]$，那么，

$$y=a_0+a_1x+\cdots+a_NX^N,\ \ a_i\in A.$$

凡是 y 的表达式中含有 x 的比 $n-1$ 次更高的次幂，就用 $x^n=-\big(a_{n-1}x^{n-1}+\cdots+a_1x+a_0\big)$ 进行替换。如此反复，一直到 $N<n$ 为止。从而，$1,x,\cdots,x^{n-1}$ 生成了 $A[x]$。

2)⇒3) 是显然的；现在证明 3)⇒1)。假设 $\{x_1,\cdots,x_n\}\subset M$ 生成了 M，则对每个 $i\leqslant n$，$x\cdot x_i\in M$。从而，存在 $\{a_{ij}\}_{1\leqslant i,j\leqslant n}\subset A$，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，以上关系可以用矩阵表达：

$$\big(x\cdot\mathbf{I}-A\big)\begin{pmatrix}x_1\\ \ddots\\ x_n\end{pmatrix}=0.$$

左右两边乘以 $\big(x\cdot\mathbf{I}-A\big)$ 的伴随矩阵 $\big(x\cdot\mathbf{I}-A\big)^*$，我们得到

$$\big(x\cdot\mathbf{I}-A\big)^*\big(x\cdot\mathbf{I}-A\big)\begin{pmatrix}x_1\\ \ddots\\ x_n\end{pmatrix}=\det\big(x\cdot\mathbf{I}-A\big)\cdot\mathbf{I}\begin{pmatrix}x_1\\ \ddots\\ x_n\end{pmatrix}=0.$$

即对任意的 $i\leqslant n$，有 $\det\big(x\cdot\mathbf{I}-A\big)x_i=0$。由于 $1\in M$，从而存在 $b_1,\cdots,b_n$，使得

$$b_1x_1+b_2x_2+\cdots+b_nx_n=1.$$

两边同时乘以 $\det\big(x\cdot\mathbf{I}-A\big)$，就给出了 $\det\big(x\cdot\mathbf{I}-A\big)=0$。将这个行列式按定义展开，就给出了 x 所满足的首一的代数方程。 □

推论 85. *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，所以存在 $m,n\geqslant 1$，使得

$$x^n=a_{n-1}b^{n-1}+\cdots+a_1x+a_0,\ \ y^m=b_{m-1}y^{m-1}+\cdots+b_1y+b_0,$$

其中，系数 $a_i,b_j\in A$。通过以上关系，我们某个 $A[x,y]$ 中元素里的 x^n 和 y^m 替换为较小的次数，所以，$\{x^iy^j\big|0\leqslant i\leqslant n,0\leqslant j\leqslant m\}$ 生成了 $A[x,y]$。根据上述命题，$A[x,y]$ 中的每个元素 z 都满足 $z\cdot A[x,y]\subset A[x,y]$ 而且 $1\in A[x,y]$。所以，z 是整元素。 □

注记 5.12. 类似地，若 $x_1,\cdots,x_k\in B$ 在 A 上是整的，则 $A[x_1,\cdots,x_k]$ 是有限生成 A-模。

根据推论，我们有如下定义

定义 5.5. 给定环的扩张 $A\subset B$，集合

$$\overline{A}:=\{x\in B|x\text{ 在 }A\text{ 上是整的}\}$$

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**。若 $\overline{A}=B$，则称 B 在 A 上是**整的**，即 B 中的每个元素都是 A 上的整元素。

当 A 是整环时，考虑 $K=\mathrm{Frac}(A)$。若 A 在 K 中的整闭包是 A，则称 A 是**整闭的**。

引理 86. 给定环的扩张 $A\subset B\subset C$，若 B 在 A 上是整的，C 在 B 上是整的，则 C 在 A 上是整的。

证明: 对任意的 $x\in C$，存在 $b_1,\cdots,b_{n-1}\in B$，使得

$$x^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0=0.$$

由于 $b_1,\cdots,b_{n-1}$ 在 A 上是整的，所以 $A[b_0,\cdots,b_{n-1}]$ 为有限生成的 A-模。根据上式所提供的代数关系，通过把 x 的高次幂替换成低次幂，$M=A[b_0,\cdots,b_{n-1},x]$ 仍为有限生成的 A-模。特别地，$x\cdot M\subset M$ 并且 $1\in M$。所以，x 在 A 上是整的。 □

引理 87. 唯一分解整环是整闭的。

证明: A 是唯一分解整环，令 $x=\frac{b}{a}\in\mathrm{Frac}(A)$ 是整元素，其中，a 与 b 互素。那么，存在 $a_0,\cdots,a_{n-1}\in A$，使得

$$x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0.$$

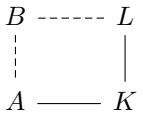
由于 $x=\frac{b}{a}$，对上述方程两边同时乘 a^n 给出：

$$b^n=-\big(a_{n-1}ab^{n-1}+\cdots+a_1a^{n-1}b+a_0a^n\big).$$

令 p 为 a 的一个不可约因子（如果这样的因子不存在，那么 a 为 A 中可逆元，命题自然成立），则 p 整除方程右边的每一项，从而 $p\mid b^n$，所以，$p\mid b$，这和，a 与 b 互素矛盾。从而，$a\in A^\times$，进而 $x\in A$。 □

5.3.3 数域的整数环

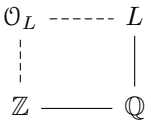
A 是整环，$K=\mathrm{Frak}(A)$ 为其分式域，L/K 为代数扩张。我们最关心如下场景下的整扩张：



其中，B 为 A 在 L 中的整闭包。特别地，B 是 A 的整扩张。

定义 5.6. 所谓的**数域**L，指的是 L 为 $\mathbb{Q}$ 的有限扩张。

例子 5.3. 考虑上述场景在 L 为数域时的情形，即 $A=\mathbb{Z}$，$K=\mathbb{Q}$，L 为 $\mathbb{Q}$ 的有限扩张，$B=\mathcal{O}_L$ 为 $\mathbb{Z}$ 在 L 中的整闭包：



我们将 $\mathcal{O}_L$ 称为数域 L 的**代数整数环**。

引理 88. *A 是整环，$K=\mathrm{Frak}(A)$ 为其分式域，L/K 为代数扩张，B 为 A 在 L 中的整闭包。那么，$\left(A^{\times}\right)^{-1}B=L$。*

证明: 对任意 $x\in L$，由于 L/K 是代数扩张，所以存在 $a_i,b_i\in A$，其中，$i,j\leqslant n-1$ 并且 $b_0,\cdots,b_{n-1}$ 非零，使得

$$x^n+\frac{a_{n-1}}{b_{n-1}}x^{n-1}+\cdots+\frac{a_1}{b_1}x+\frac{a_0}{b_0}=0.$$

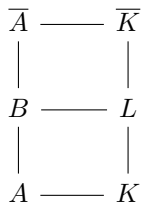
令 $d=b_{n-1}b_{n-2}\cdots b_1b_0\in A$。对上式两边同乘 d^n，得到

$$(d\cdot x)^n+c_{n-1}(d\cdot x)^{n-1}+\cdots+c_1(d\cdot x)+c_0=0,$$

其中，$c_i\in A$。所以，$dx\in B$，即 $x\in\left(A^{\times}\right)^{-1}B$。 □

命题 89. *A 是整环并且 A 是整闭的，$K=\mathrm{Frak}(A)$，L/K 为代数扩张，B 为 A 在 L 中的整闭包。那么，对任意 $x\in B$，其极小多项式 $P(X)\in A[X]$。*

证明: 由于 $x\in B$，存在 $P_0(X)\in A[X]\subset K[X]$ 并且 $P_0(X)$ 是首一的多项式，使得 $P_0(x)=0$。特别地，$P(X)\mid P_0(X)$。我们在 K 的代数封闭域中讨论。根据命题81，即代数扩张的同态延拓的性质，不妨假设 $L\subset\overline{K}$ 并且 $\overline{A}$ 为 A 在 $\overline{K}$ 中的整闭包。根据定义，我们自然有 $B\subset\overline{A}$：



令 $Z(P_0)$ 和 $Z(P)$ 分别为 $P_0(X)$ 和 $P(X)$ 在 $\overline{K}$ 中的根的集合。根据 $P(X)\mid P_0(X)$，$Z(P)\subset Z(P_0)$。由于 $P_0(X)\in A[X]$ 是首一的，所以对任意 $y\in Z(P_0)$，y 在 A 上是整的，即 $Z(P_0)\subset\overline{A}$。从而，$Z(P)\subset\overline{A}$。根据 Vieta 定理，$P$ 的系数均为 $Z(P)$ 中元的整系数对称多项式而 $\overline{A}$ 是环，所以 $P(X)\in\overline{A}[X]$，进而 $P(X)\in\overline{A}[X]\cap K[X]$。根据 A 的整闭性，$P\in A[X]$。 □

注记 5.13 (B 作为 A-模的有限性)**.** 假设 A 是整闭的 Noether（整）环，$K=\mathrm{Frak}(A)$，L/K 为有限可分扩张，B 为 A 在 L 中的整闭包，则 B 是有限生成的 A-模。特别地，若 A 是主理想整环，则 B 是自由 A-模并且其秩为 $[L:K]$。

我们之后将证明这个命题。

- 数域的情形

例子 5.4. 考虑 L 是数域的情形：

$$\begin{array}{ccc} \mathcal{O}_L & \text{------} & L \\ \vdots & & | \\ \mathbb{Z} & \text{——} & \mathbb{Q} \end{array}$$

我们将证明，$L/\mathbb{Q}$ 总是可分扩张。此时，$A=\mathbb{Z}$ 是主理想整环，$\mathcal{O}_L$ 为数域 L 的代数整数环。特别地，$\mathcal{O}_L$ 是秩为 $[L:\mathbb{Q}]$ 的自由交换群。

- 函数域的情形

例子 5.5. $\mathbb{F}_q$ 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：

$$\begin{array}{ccc} B & \text{----------} & L \\ \vdots & & | \\ \mathbb{F}_q[X] & \text{——} & \mathbb{F}_q(X) \end{array}$$

在此情形下，并不需要假设 $L/\mathbb{F}_q(X)$ 是可分的[34] 此时，$\mathbb{F}_q[X]$ 是主理想整环，B 是有限生成的 $\mathbb{F}_q[X]$-模。特别地，B 是自由的 $\mathbb{F}_q[X]$ 模且其秩为 $[L:\mathbb{F}_q(X)]$。

例子 5.6 (二次数域的整数环)**.** d 是不包含任何平方因子的整数，$K=\mathbb{Q}(\sqrt{d})$。那么，K 中的元素均形如 $x=a+b\sqrt{d}\in K$，其中，$a,b\in\mathbb{Q}$。此时，$[\mathbb{Q}(\sqrt{d}):\mathbb{Q}]=2$，所以 $\mathbb{Q}(\sqrt{d})$ 被称作是二次数域。我们计算 $\mathcal{O}_K=\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$。

考虑 $x=a+b\sqrt{d}\in K$ 的极小多项式，由于

$$x^2-2ax+a^2-b^2d=0,$$

所以 $x\in\mathcal{O}_K$ 等价于 $2a\in\mathbb{Z}, a^2-b^2d\in\mathbb{Z}$。特别地，我们有

$$(2a)^2-(2b)^2d\in\mathbb{Z}\ \Rightarrow\ (2b)^2d\in\mathbb{Z}.$$

由于整数 d 没有平方因子，所以，$2b\in\mathbb{Z}$（d 不能抵消 b 的 $(2b)^2$ 分母）。作为总结，$x\in\mathcal{O}_K$ 的一个必要条件为

$$2a,2b\in\mathbb{Z}.$$

特别地，$\mathbb{Z}+\mathbb{Z}\sqrt{d}\subset\mathcal{O}_K$。这是 $\mathcal{O}_K$ 的子环。

以下对 a 分情况讨论：

- $a\in\mathbb{Z}$。类似地讨论给出 $a,b\in\mathbb{Z}$。
- $a=\frac{1}{2}a'$，其中，$a'\in\mathbb{Z}$ 为奇数。

  根据 $a^2-b^2d\in\mathbb{Z}$，$b\notin\mathbb{Z}$。所以，$b=\frac{1}{2}b'$，其中，$b'\in\mathbb{Z}$ 为奇数。那么，

  $$a^2-b^2d\in\mathbb{Z}\ \Rightarrow\frac{1}{4}\big(a'^2-b'^2d\big)\in\mathbb{Z}.$$

  由于 $a'^2\equiv b'^2\equiv 1 \mod 4$，所以上式等价于 $d\equiv 1 \mod 4$。

[34]证明该结论要先研究 L/K 是纯不可分的情形，由于此结论与课程主旨并不直接关联，我们在讲义中不给出其细节。

综上所述，我们有

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})}=\begin{cases} m+n\sqrt{d},\ \ m,n\in\mathbb{Z} & d\equiv 2,3 \mod 4;\\ \frac{1}{2}(m+n\sqrt{d}),\ \ m,n\in\mathbb{Z}, a\equiv b \bmod 2, & d\equiv 1 \mod 4.\end{cases}$$

其中，d 是不包含任何平方因子的整数。

例子 5.7. $\mathbb{Z}[\sqrt{5}]$ 不是整闭的。

$$\begin{array}{ccc} \mathcal{O}_{\mathbb{Q}(\sqrt{5})} & \text{——} & \mathbb{Q}(\sqrt{5}) \\ | & & | \\ \mathbb{Z}[\sqrt{5}] & & | \\ | & & | \\ \mathbb{Z} & \text{————} & \mathbb{Q} \end{array}$$

实际上，$x=\frac{1}{2}(-1+\sqrt{5})\in\mathbb{Q}(\sqrt{5})=\mathrm{Frac}(\mathbb{Z}[\sqrt{5}])$ 在 $\mathbb{Z}[\sqrt{5}]$ 上是整的，但是 $x\notin\mathbb{Z}[\sqrt{5}]$。

5.4 分裂域与正规扩张

定义 5.7. 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，即对任意 $i\in I$，存在 $\alpha_{i,j}\in L$ 以及 $a_i\in K$，使得

$$P_i(X)=a_i(X-\alpha_{i,1})(X-\alpha_{i,2})\cdots(X-\alpha_{i,n_i}).$$

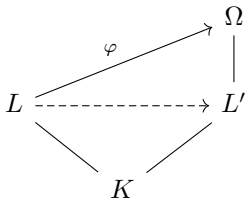
2) $L=K(\{\alpha_{i,j}\}_{i\in I,j\leqslant n_i})$。

我们称 L 是 K 的（由 $\{P_i(X)\}_{i\in I}$ 给出的）一个**分裂域**。

注记 5.14. 分裂域 L 是 K 的代数扩张，因为它是由 K 添加代数元得到的。

注记 5.15. 在 $\overline{K}$ 中考虑，只要（只能）把 $\{P_i(X)\}_{i\in I}$ 的根都添加到 K 中就得到分裂域 $K(\{\alpha_{i,j}\}_{i\in I,j\leqslant n_i})$。换而言之，$K$ 的（一个）分裂域就是把一些多项式的（所有）根添加到 K 中。

命题 90 (分裂域的唯一性)**.** *K 是域，$\{P_i(X)\}_{i\in I}$ 是 $K[X]$ 中一族多项式，L 和 L' 均为 K 的由 $\{P_i(X)\}_{i\in I}$ 定义的分裂域并且 L' 落在某个代数封闭域 Ω 中。那么，对任意的 $\varphi\in\mathrm{Hom}_K(L,\Omega)$，都有 $\varphi(L)\subset L'$，即 $\varphi\in\mathrm{Hom}_K(L,L')$。*



特别地，分裂域在 K-同构意义下唯一。

证明: 通过两种方式来计算 P_i^{φ}，其中 $i\in I$，请参考注记5.7。由于 $P_i(X)$ 是 K-系数的多项式，所以 $P_i^{\varphi}=P_i$。在代数封闭域 Ω 中，P_i 均分裂，所以

$$P(X)=P_i^{\varphi}(X)=a_i(X-\varphi(\alpha_{i,1}))(X-\varphi(\alpha_{i,2}))\cdots(X-\varphi(\alpha_{i,n_i})),$$

其中，$a_i \in K, \alpha_{i,j} \in \Omega$。

根据上一注记，$L' = K(\{\varphi(\alpha_{i,j})\}_{i\in I, j\leqslant n_i})$。然而，

$$\varphi(L) = \varphi\big(K(\{\alpha_{i,j}\}_{i\in I, j\leqslant n_i})\big) = K(\{\varphi(\alpha_{i,j})\}_{i\in I, j\leqslant n_i}),$$

所以，$\varphi(L) \subset L'$，即 $\varphi \in \mathrm{Hom}_K(L, L')$。

现在证明分裂域在 K-同构意义下的唯一性：考虑 K 的两个（关于同一族多项式的）分裂域 L 和 L'。先将 L' 放到代数封闭域 Ω（比如选 $\Omega = \overline{L'}$）中，由于 L/K 是代数扩张，再根据命题81选 $\varphi \in \mathrm{Hom}_K(L, \Omega)$。应用以上结论就得到了域同态 $\varphi : L \to L'$；类似地，还可以构造域同态 $\psi : L' \to L$。所以，$\psi\circ\varphi \in \mathrm{Hom}_K(L, L)$。根据引理82，$\psi \circ \varphi$ 是同构，所以 ψ 和 φ 均为 K-同构。从而，L 与 L' 同构。 □

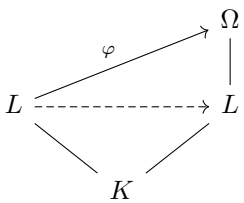
注记 5.16. 分裂域的定义不要求多项式族 $\{P_i(X)\}_{i\in I}$ 的指标集是有限集。若 I 有限，我们可以考虑 $P(X) = \prod_{i\in I} P_i(X)$，则 P 的分裂域与 $\{P_i(X)\}_{i\in I}$ 的分裂域相同。特别地，此时分裂 L 是 K 的有限扩张。

我们以下关于正规性的定义不需要有限性假设，只要求 L/K 是代数扩张。

定理 91 (正规性的定义)**.** *给定代数扩张 L/K，下面四个叙述等价：*

1) L 是 $K[X]$ 中一族多项式 $\{P_i(X)\}_{i\in I}$ 的分裂域；

2) 对任意域扩张 Ω/L，其中 Ω 是代数封闭域，对任意 $\varphi \in \mathrm{Hom}_K(L, \Omega)$，均有 $\varphi(L) \subset L$；



3) 存在某个域扩张 Ω/L，其中 Ω 是代数封闭域，使得对任意 $\varphi \in \mathrm{Hom}_K(L, \Omega)$，均有 $\varphi(L) \subset L$；

4) 对任意不可约多项式 $P(X) \in K[X]$，若 $P(X)$ 在 L 中有根，则 $P(X)$ 在 $L[X]$ 中分裂。

*满足以上条件的代数扩张 L/K 被称为***正规扩张***。*[35]

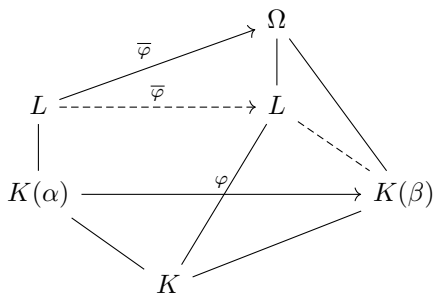
注记 5.17. 在流行的教科书中，人们通常采取 4) 作为正规扩张的定义并证明 1) 与之等价。

证明： 2) ⇒ 3) 显然；命题90给出 1) ⇒ 2)。

证明 2) ⇒ 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 $\varphi : K(\alpha) \to K(\beta)$。由于 L 是 K 的代数扩张，利用命题81，可以把 φ 延拓成 $\overline{\varphi} : L \to \Omega$，即



[35]我们默认正规扩张是代数扩张。

根据 2)，$\overline{\varphi}(L)\subset L$，从而

$$K(\beta)=\varphi\big(K(\alpha)\big)=\overline{\varphi}\big(K(\alpha)\big)\subset L.$$

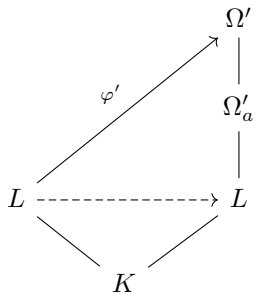
特别地，$\beta=\varphi(\alpha)\in L$。

证明 4) ⇒ 1)。考虑多项式族：

$$\{P_i\}_{i\in I}=\Big\{P_x(X)\text{是 }x\text{ 的极小多项式}\Big|x\in L\Big\}.$$

我们注意到每个 P_i 均为不可约多项式。根据 4)，P_i 在 L 中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）生成，从而 L 是 K 的分裂域。

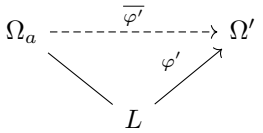
最后证明 3) ⇒ 2)（相对困难）。Ω 已经由 3) 给定。我们考虑另一个代数封闭的 Ω' 以及 $\varphi'\in\mathrm{Hom}_K(L,\Omega')$，即下图



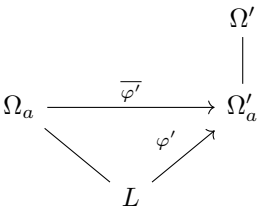
我们选取 Ω'_a 为 Ω' 中的那些在 K 上的代数的元所构成的子域。根据引理79，Ω'_a 同构于 K 的代数闭包 $\overline{K}$，它也是 L 的代数闭包（因为 L 在 K 上是代数的）。类似地，我们构造 Ω_a 为 Ω 中在 K 上的代数元所构成的子域，它也同构于 K 的代数闭包 $\overline{K}$。

$$K\text{ —— }L\text{ —— }\Omega_a\text{ —— }\Omega.$$

根据命题81，我们可以对 $\varphi':L\to\Omega'$ 进行延拓：



注意 $\overline{\varphi'}$ 是 L-同态。根据代数闭包的唯一性以及 $\overline{\varphi'}$ 把 K-系数多项式的根映射为 K-系数多项式的根，我们实际上还有如下的图表：



以上 $\overline{\varphi'}$ 是代数封闭域之间的 L-同构。从而，$\overline{\varphi'}^{-1}\circ\varphi':L\to\Omega$。根据 3)，$\overline{\varphi'}^{-1}\circ\varphi':L\to L$，所以，$\varphi':L\to L$。 □

注记 5.18. 以上最后一个交换图表明 $\varphi(L)\subset\Omega'_a$。所以，我们不妨假设 Ω 和 Ω' 均为 $\overline{K}$（差一个同构的意义下）。此时，命题明显成立。

例子 5.8. L/K 是域扩张并且 $[L:K]=2$，那么，L/K 是正规扩张。

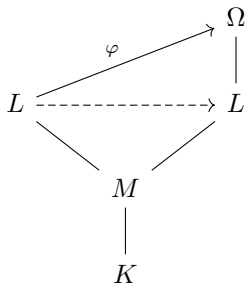
不妨假设 $L\subset\overline{K}$。对任意的 $\alpha\in L-K$，其极小多项式 $P(X)$ 为二次多项式，即 $P(X)=X^2+aX+b$，其中，$a,b\in K$。那么，$P(X)=(X-\alpha)(X+a+\alpha)$。从而，$L=K(\alpha)=K(\alpha,a+\alpha)$ 是 P 的分裂域。

命题 92. *L/K 是正规扩张，那么对任意的中间域 M，L/M 也是正规扩张。*

证明： 可用 1) 来证明：L 是一族 K-系数多项式 $\{P_i(X)\}_{i\in I}$ 的分裂域，自然是一族 M-系数多项式 $\{P_i(X)\}_{i\in I}$ 的分裂域。

也可用 4) 来证明：假设 $P(X)$ 是 $M[X]$ 中的不可约多项式并且对于 $\alpha\in L$，$P(\alpha)=0$。考虑 α 在 K 上的极小多项式 $Q(X)$：在 $M[X]$ 中，$P\mid Q$（因为 $Q(\alpha)=0$ 而 Q 只是在 $K[X]$ 中不可约）。由于 L/K 是正规扩张并且 $Q(\alpha)=0$，所以 Q 在 L 中分裂，即 Q 的所有根都在 L 中。那么，P 的所有根也都在 L 中，即 P 在 L 中也分裂。

还可用 2) 来证明：对任意域扩张 Ω/L，其中 Ω 是代数封闭的，对任意 $\varphi\in\mathrm{Hom}_M(L,\Omega)$，



只要证明 $\varphi(L)\subset L$ 即可。这是显然的，因为 φ 可被视作 $\mathrm{Hom}_K(L,\Omega)$ 中的映射。 □

注记 5.19. M/K 未必是正规的。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：$\sqrt[4]{2}$ 是不可约多项式 X^4-2 的根，但是根 $\sqrt[4]{2}i\notin\mathbb{R}\supset\mathbb{Q}(\sqrt[4]{2})$。

注记 5.20. 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

$$\mathbb{Q}\longrightarrow\mathbb{Q}(\sqrt{2})\longrightarrow\mathbb{Q}(\sqrt[4]{2}).$$

例子 5.9. 令 $K=\mathbb{Q}\left(\sqrt{2}i,\sqrt[4]{2}(1-i)\right)$，以下每个扩张的次数均为 2：

$$\mathbb{Q}\xrightarrow{2}\mathbb{Q}(\sqrt{2}i)\xrightarrow{2}\mathbb{Q}\left(\sqrt{2}i,\sqrt[4]{2}(1-i)\right)=K.$$

所以，$[K:\mathbb{Q}]=4$。现在来说明 $K/\mathbb{Q}$ 不是正规扩张。

注意到 $\alpha=\sqrt[4]{2}(1-i)$ 是多项式 X^4+8 的根，其中，X^4+8 在 $\mathbb{Q}[X]$ 中不可约[36]，令 L 为 X^4+8 的分裂域，即添加 $\mathbb{Q}$ 上添加 X^4+8 的所有根得到的域，这是 K 的扩张（可能相同）。由于 X^4+8 是实系数的多项式，$\overline{\alpha}$ 也是它的根，所以 $\overline{\alpha}\in L$。特别地，

$$\sqrt[4]{2}=\frac{1}{2}(\alpha+\overline{\alpha})\in L.$$

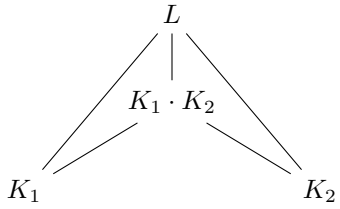
[36]通过待定系数法直接计算即可证明

据此，$i \in L$。从而，$L = \mathbb{Q}(\sqrt[4]{2}, i)$。通过考虑

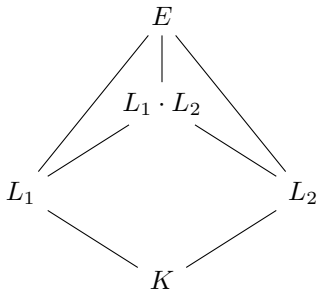
$$\mathbb{Q} \text{ —— } \mathbb{Q}(\sqrt[4]{2}) \text{ —— } \mathbb{Q}(\sqrt[4]{2}, i)$$

可以看出 $[L : \mathbb{Q}] = 8$。特别地，$K \neq L$，从而 $K/\mathbb{Q}$ 不正规。

L 是域，K_1, K_2 为其子域，我们记 $K_1 \cdot K_2 := K_1(K_2) = K_2(K_1)$ 并称之为 K_1 和 K_2（在 L 中）的**复合域**。



命题 93. 给定域扩张 E/K，L_1 和 L_2 是中间域。若 L_1/K 和 L_2/K 是正规扩张，



则 $L_1 \cdot L_2/K$ 也正规。

证明: 利用正规扩张定义的 1) 来证明：L_1 和 L_2 分别是 K 添加了所有 $\{P_i\}_{i\in I}$ 的根和所有 $\{Q_j\}_{j\in J}$ 的根所得的分裂域，从而 $L_1 \cdot L_2$ 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。

还可利用 2) 来证明: 对任意的域扩张 $\Omega/L_1 \cdot L_2$, 其中 Ω 是代数封闭的, 对任意的 $\varphi \in \mathrm{Hom}_K(L_1 \cdot L_2, \Omega)$, 通过到 L_1 的限制，我们可将 φ 视为

$$\varphi : L_1 \to \Omega.$$

从而，由于 L_1/K 正规，所以 $\varphi : L_1 \to L_1 \subset L_1 \cdot L_2$。类似地，$\varphi : L_2 \to L_2 \subset L_1 \cdot L_2$。所以，$\varphi : L_1 \cdot L_2 \to L_1 \cdot L_2$。 □

注记 5.21. 给定代数扩张 L/K 以及其一族中间域 $\{M_i\}_{i\in I}$。如果对每个 $i \in I$，M_i/K 均为正规扩张，则它们的交 $\bigcap_{i\in I} M_i$ 也是 K 的正规扩张。

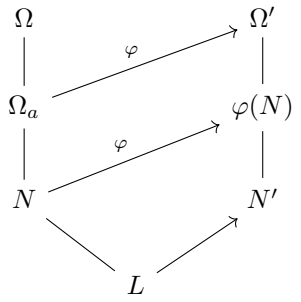
实际上，根据正规扩张的定义 4)，以上性质是显然的。据此，我们可以定义正规闭包。

定理 94. 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[37]、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' 类似地构造，那么有 K-同构 $N \simeq N'$。

在同构的意义下，我们称 N 为 L/K 的**正规闭包**。

[37]在包含关系下

证明: 根据上面的注记，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，它自然在包含关系下最小。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 $L\subset\Omega'$ 以及有关代数扩张同态延拓的命题81，我们固定一个 $\varphi:\Omega_a\to\Omega'$，使得上图交换。域扩张 $\varphi(N)/K$ 是正规的，所以 $\varphi(N)\supset N'$（根据 N' 的最小性）。考虑 $\varphi^{-1}(N')\subset N$，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，P 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 $N\simeq_K N'$ □

注记 5.22. 由于 L/K 是代数的，所以 L 是 K 添加上 K-系数多项式 $\{P_i\}_{i\in I}$ 的**某些**根得到的。为了得到正规闭包 N，我们需要把 $\{P_i\}_{i\in I}$ 的所有根都添加到 K 中即可。

比如说，$\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ 不是正规的，通过添加 X^4-2 的根 $\pm i\sqrt[4]{2}$，我们得到它的正规闭包

$$N=\mathbb{Q}(\pm\sqrt[4]{2},\pm i\sqrt[4]{2})=\mathbb{Q}(\sqrt[4]{2},i).$$

5.5 可分扩张

定义 5.8. K 是域，$P\in K[X]$ 是 K-系数多项式。如果 P 在 $\overline{K}$ 中没有重根，就称 P 是**可分的**；否则称之为**不可分的**。

L/K 是代数扩张，对于 $x\in L$，如果其极小多项式是可分的，就称 x 为**可分的**；否则称之为**不可分的**。若每个 $x\in L$ 均可分，则称代数扩张 L/K 是**可分的**；否则称之为**不可分的**。

注记 5.23 (判断多项式的可分性)**.** 根据注记4.21, 多项式 P 可分等价于 $\mathrm{Disc}(P)\neq 0$。另外, 由于 $\mathrm{Disc}(P):=\mathrm{Res}(P,P')$，所以多项式 P 可分等价于 $(P,P')=1$。

特别地，若 $P\in K[X]$ 是不可约多项式，则 P 可分等价于 $P'\neq 0$：实际上，若 P 可分，则 $(P,P')=1$，这显然说明 $P'\neq 0$；反之，$P'\neq 0$ 并且 $\deg(P')<\deg(P)$，根据 P 不可约，只能有 $(P,P')=1$。

注记 5.24 (不可分的不可约多项式)**.** 假设 $P\in K[X]$ 是不可约多项式，记 $P(X)=a_nX^n+\cdots+a_1X+a_0$，其中 $a_n\neq 0$。那么，

$$P'(X)=\sum_{k=1}^{n}ka_kX^{k-1}=na_nX^{n-1}+\cdots.$$

若 P 是不可分的，则 $P'=0$，从而，$n\cdot a_n=0$，所以，在 K 中 $n=0$。这表明 $\mathrm{Char}(K)=p$ 并且 $p\mid n$，其中 p 是素数。

利用 $\mathrm{Char}(K)=p$ 重新计算 $P'(X)$：

$$P'(X)=\sum_{p\nmid k}ka_kX^{k-1}=0.$$

所以，当 $p \nmid k$ 时，$a_k = 0$。这表明

$$P(X) = \sum_{p|k} a_k X^k = Q(X^p).$$

其中，$Q(X)$ 的定义如下：

$$Q(X) = \sum_{p|k} a_k X^{\frac{k}{p}}.$$

由于 P 不可约，根据 $P(X) = Q(X^p)$，$Q(X)$ 也不可约。特别地，如果 P 不可约并且不可分，则 $\deg(P) \geqslant p$。

另外，当 $\mathrm{Char}(K) = p$ 时，我们注意到形如 $Q(X^p)$ 的多项式的导数为 0。

注记 5.25. 在特征零情形下，不可约多项式都是可分多项式。特别地，如果 $\mathrm{Char}(K) = 0$，那么，任意的代数扩张 L/K 均为可分扩张。

例子 5.10. 令 $K = \mathbb{F}_p(T) = \mathrm{Frac}(\mathbb{F}_p[T])$。根据 Eisenstein 判别法，多项式

$$P(X) = X^{p^2} + TX^p + T$$

在 $\mathbb{F}_p[T][X]$ 中不可约。根据 Gauss 引理，$P(X)$ 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 是可分的多项式。

5.5.1 完美域

当 $\mathrm{Char}(K) = p$ 时，我们有 Frobenius 同态：

$$\mathrm{Frob} : K \to K, \quad x \mapsto x^p.$$

特别地，对任意的 $x, y \in K$，$(x+y)^p = x^p + y^p$。

引理 95. *若 $\mathrm{Char}(K) = p$，则对任意 $a \in K - K^p$，$X^p - a$ 在 $K[X]$ 中不可约并且不可分。*

证明： 由于 K 的特征为 p，$X^p - a$ 显然是不可分的。现在证明 $X^p - a$ 不可约。

我们在 $\overline{K}$ 中考虑 $X^p - a$ 的分解。注意到存在唯一的 $b \in \overline{K}$，使得 $b^p = a$：若有另一个 $b' \in \overline{K}$，使得 $b'^p = a$，则 $(b - b')^p = b^p - b'^p = 0$，从而 $b = b'$。

所以，$X^p - a$ 在 $\overline{K}$ 中恰有一个（p-重）根，即

$$X^p - a = (X - b)^p \in \overline{K}[X].$$

如果 P 是可约，即 $P(X) = P_1(X) \cdot P_2(X)$，其中 $P_1, P_2 \in K[X]$。上述在 $\overline{K}[X]$ 中的分解给出：

$$X^p - a = \underbrace{(X-b)^k}_{P_1(X)} \cdot \underbrace{(X-b)^l}_{P_2(X)}.$$

根据假设，$b \notin K$。所以，$k, l \neq 1$，即 $k, l \geqslant 2$。据此，P_1 和 P_2 均有重根从而是不可分。根据之前的讨论，P_1 和 P_2 次数至少是 p，所以 $X^p - a$ 的次数至少是 $2p$，矛盾。 □

引理 96. *域 K 的特征为 p，$P \in K[X]$，$\deg(P) \geqslant 2$，P 不可约。若 P 在 $\overline{K}$ 中只有一个根，则*

$$P(X) = X^{p^n} - a, \quad a \notin \mathrm{Im}(\mathrm{Frob}) = K^p.$$

证明: 在 $\overline{K}$ 中，我们可以分解 P:

$$P(X) = (X-b)^m = (X-b)^{p^n \cdot l} = (X^{p^n} - b^{p^n})^l,$$

其中，$m \geqslant 2, m = p^n \cdot l$ 并且 $(l,p) = 1$。所以，

$$P(X) = Q(X^{p^n}),$$

其中，$Q(X) = (X - b^{p^n})^l$。根据这个表达式，我们注意到 $Q \in K[X]$。由于 P 不可约，所以 Q 也不可约。另外，由于 P 在 $\overline{K}$ 中只有一个根，所以 Q 也只有一个根。若 $l \geqslant 2$，Q 只有一个根，所以 Q 不可分。据此，$\deg(Q) = l$ 为 p 的倍数，这与 $(p,l) = 1$ 矛盾。所以，$l = 1$。从而，

$$P(X) = X^{p^n} - b^{p^n} = X^{p^n} - a.$$

如果 $a \in \mathrm{Im}(\mathrm{Frob})$，即 $a = c^p$，其中，$c \in K$，则

$$P(X) = X^{p^n} - c^p = (X^{p^{n-1}} - c)^p$$

是可约的，矛盾。所以，$a \notin \mathrm{Im}(\mathrm{Frob})$。 □

定义 5.9. K 是域，若每个不可约多项式 $P(X) \in K[X]$ 均可分，则称 K 是**完美的** (perfect)。

注记 5.26. 特征为零的域是完美域。

注记 5.27. K 是完美的，L/K 是代数扩张，则 L/K 可分。

命题 97. *K 是特征为 p 的域，那么，K 是完美的当且仅当 $\mathrm{Frob}: K \to K$ 是满射。*

证明: 若 Frob 不是满射，根据引理95，选 $a \in K - K^p$，即 $a \notin \mathrm{Frob}(K)$。那么，$X^p - a$ 不可约也不可分。从而，域 K 不完美。

若 Frob 是满射，对任意不可约多项式 $P(X)$，如果 $P(X)$ 不可分，我们来推出矛盾: 此时，$P'(X) = 0$，从而，

$$P(X) = \sum_{p|m} a_m X^m = \sum_k a_{kp} X^{kp}.$$

由于 Frob 是满射，对每个 k，存在唯一的 $b_k \in K$，使得 $\mathrm{Frob}(b_k) = a_{kp}$。那么，

$$P(X) = \big(\sum_k b_k X^k\big)^p.$$

这与 $P(X)$ 不可约矛盾。 □

例子 5.11. $\mathbb{F}_p(T) = \mathrm{Frac}(\mathbb{F}_p[T])$ 不是完美域。

根据 Eisenstein 判别，$X^p - T \in K[X]$ 是不可约多项式并且不可分: 实际上，不存在 $\frac{P(T)}{Q(T)} \in \mathbb{F}_p(T)$，使得 $\left(\frac{P(T)}{Q(T)}\right)^p = T$，否则

$$\left(\frac{P(T)}{Q(T)}\right)^p = \frac{P(T^p)}{Q(T^p)} = T.$$

这表明

$$P(T^p) = Q(T^p) \cdot T.$$

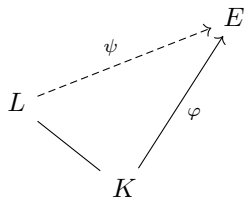
对 T 求导，左边为 0 而右边为 $Q(T^p)$，矛盾。所以，$\mathbb{F}_p(T)$ 不是完美的。

5.5.2 可分次数

用所谓的可分次数可以刻画代数扩张是否是可分。给定代数扩张 L/K，任选域同态 $\varphi : K \to E$，其中，E 是代数封闭域。令

$$\mathrm{Ext}_{L/K}(E,\varphi) = \left\{\psi \in \mathrm{Hom}(L,E) \middle| \psi|_K = \varphi\right\}.$$

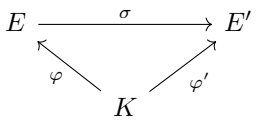
这是 φ 到 L 上所有可能的扩张所构成的集合。



考虑对另一个可能的域同态 $\varphi' : K \to E'$，其中，E' 是代数封闭域。我们有集合之间的双射：

$$\mathrm{Ext}_{L/K}(E,\varphi) \xrightarrow{1:1} \mathrm{Ext}_{L/K}(E',\varphi').$$

实际上，通过选取 $\varphi(K)$ 在 E 中的代数闭包 $\overline{\varphi(K)}$，由于 $\psi(L) \subset \overline{\varphi(K)}$，我们不妨假设 $E = \overline{\varphi(K)}$；类似地，不妨假设 $E' = \overline{\varphi'(K)}$。根据代数闭包的唯一性，存在 K-同构 $\sigma : E \to E'$，使得 $\psi' = \psi \circ \sigma$：



据此，我们可以构造双射

$$\mathrm{Ext}_{L/K}(E,\varphi) \longrightarrow \mathrm{Ext}_{L/K}(E',\varphi'), \quad \overline{\varphi} \mapsto \sigma \circ \overline{\varphi}.$$

其逆为 $\overline{\varphi'} \mapsto \sigma^{-1} \circ \overline{\varphi}$。特别地，$|\mathrm{Ext}_{L/K}(E,\varphi)|$ 只依赖于 L/K。

定义 5.10. 对任意的代数扩张 L/K，任意选定域同态 $\varphi : K \to E$，其中，E 是代数封闭域。我们定义 L/K 的**可分次数**为

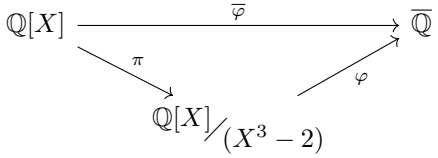
$$[L:K]_s := \left|\mathrm{Ext}_{L/K}(E,\varphi)\right|.$$

如果选取 $E = \overline{K}$，$[L:K]_s$ 就是把 L 嵌入到 $\overline{K}$ 的同态的个数。

注记 5.28. 如果 L/K 是有限扩张，我们将证明 $[L:K]_s \leqslant [L:K]$ 并且 L/K 可分当且仅当 $[L:K]_s = [L:K]$。

例子 5.12. $[\mathbb{C}:\mathbb{R}]_s = 2$。

例子 5.13. 令 $K = \mathbb{Q}$，$L = \mathbb{Q}[X]/(X^3 - 2)$。此时，$L/\mathbb{Q}$ 是 3 次扩张并且 $[L:K]_s = 3$。实际上，L 到 $\overline{\mathbb{Q}}$ 的像被 X 在 $\overline{\mathbb{Q}}$ 的像 $\alpha = \overline{\varphi}$ 决定：



我们注意到 α 只能取 $X^3 - 2$ 的某个根，所以一共有 3 个这样 φ。

例子 5.14. 令 $L=\mathbb{F}_p(T)=\mathrm{Frac}(\mathbb{F}_p[T])$，$K=\mathbb{F}_p(T^p)=L^p=\mathrm{Frob}(L)$。此时，$K$ 是 L 的子域并且 $[L:K]=p$：实际上，$L=K(T)$ 并且 $T^p\in K$，所以 $T\in L$ 的极小多项式是 $X^p-T^p\in K[X]$。此时，$L={}^{K[X]}\!/_{(X^p-T^p)}$，从而 $[L:K]=p$。

我们注意到 X^p-T^p 在 $\overline{K}$ 中只有一个根（p 重根），从而，${}^{K[X]}\!/_{(X^p-T^p)}$ 到 $\overline{K}$ 的嵌入必须把 X 映射成这个根。所以，$[L:K]_s=1$。按后面的定义，${}^{\mathbb{F}_p(T)}\!/_{\mathbb{F}_p(T^p)}$ 是纯不可分的扩张。

给定代数扩张 ${}^{L}\!/_{K}$ 和中间域 $K\subset M\subset L$，把某个同态 $\varphi:K\to E$ 延拓到 L 上等价于可以先将它延拓到 M 上然后再延拓到 L 上，即

$$\mathrm{Ext}_{{}^{L}\!/_{K}}(E,\varphi)=\coprod_{\psi\in\mathrm{Ext}_{{}^{M}\!/_{K}}(E,\varphi)}\mathrm{Ext}_{{}^{L}\!/_{M}}(E,\psi).$$

这个集合的划分表明：

命题 98. *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，如下公式成立*

$$[L:K]_s=[L:M]_s[M:K]_s.$$

推论 99 (纯不可分扩张的刻画)**.** *${}^{L}\!/_{K}$ 是代数扩张，对 $x\in L$，若 $[K(x):K]_s=1$，即 ${}^{K(x)}\!/_{K}$ 到 $\overline{K}$ 只有唯一的 K-同态，就称 x 是***纯不可分的***。若每个 $x\in L$ 均为纯不可分的，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： 若 $[L:K]_s=1$，对任意的 $x\in L$，考虑中间域 $K(x)\subset L$。根据命题98，$[K(x):K]_s\leqslant[L:K]_s=1$。所以，$[K(x):K]_s=1$，即 x 是纯不可分的。

若 ${}^{L}\!/_{K}$ 是纯不可分的，那么每个 $x\in L$ 都是纯不可分的，即 $[K(x):K]_s=1$。考虑一个 K-同态 $\varphi:L\to\overline{K}$。由于 ${}^{K(x)}\!/_{K}$ 到 $\overline{K}$ 的扩张是唯一的，从而 $\varphi\big|_{K(x)}$ 把 x 映射到 $\overline{K}$ 的像是唯一的。据此，所有 $x\in L$ 的像都被唯一决定了，这就决定了 φ，即 $\left|\mathrm{Ext}_{{}^{L}\!/_{K}}(E,\varphi)\right|=1$。这表明 $[L:K]_s=1$。 □

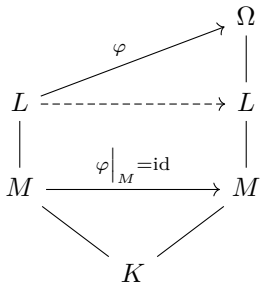
推论 100. *给定代数扩张 ${}^{L}\!/_{K}$ 和中间域 $K\subset M\subset L$。那么，${}^{L}\!/_{K}$ 是纯不可分的当且仅当 ${}^{L}\!/_{M}$ 和 ${}^{M}\!/_{K}$ 是纯不可分的。*

证明： 这由命题98中的公式立得。 □

注记 5.29. 纯不可分的扩张是正规扩张。

我们证明一个略强的结论：给定代数扩张 ${}^{L}\!/_{K}$ 和中间域 M，若 ${}^{L}\!/_{M}$ 是正规而 ${}^{M}\!/_{K}$ 是纯不可分的，则 ${}^{L}\!/_{K}$ 是正规的。

令 $\Omega=\overline{L}$。对任意的 K-同态 $\varphi:L\to\Omega$，我们要证明 $\varphi(L)\subset L$。实际上，由于 ${}^{M}\!/_{K}$ 是纯不可分的，即 $[M:K]_s=1$，所以，$\varphi\big|_{M}=\mathrm{id}$。



此时，φ 为 M-同态。由于 ${}^{L}\!/_{M}$ 是正规的，所以 $\varphi(L)=L$。

命题 101. ${}^{L}\!/_{K}$ 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: 证明的想法与推论99一致。对每个 $x \in M$，$[K(x):K]_s = 1$，从而 x 在到某个代数封闭域 E 的像都被唯一决定了，进一步每个 $K(M)$ 中元素到该代数封闭域 E 的像也被唯一确定。这表明只存在唯一的扩张，即 $\left|\mathrm{Ext}_{K(M)/K}(E,\varphi)\right| = 1$。 □

为了进一步刻画 $[L:K]$ 和 $[L:K]_s$ 之间的关联，首先研究**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。给定代数封闭域 Ω，根据引理80，我们有双射:

$$Z_P(\Omega) \xrightarrow{1:1} \mathrm{Hom}_K\left({}^{K[X]}\!/_{(P(X))}, \Omega\right).$$

其中，$Z_P(\Omega)$ 为 P 在 Ω 中的（不同）根的集合。利用 Ω 的代数封闭性，我们得到如下重要结论:

注记 5.30. $[K(x):K]_s$ 恰好是 x 极小多项式 $P(X)$（在某个代数封闭域中）的不同根的个数。特别地，$P(X)$ 的重根越多，$[K(x):K]_s$ 越小。

- $\mathrm{Char}(K) = 0$。此时，由于 P 不可约，所以，P 无重根，所以其根的个数为 $\deg(P)$。据此，

  $$[K(x):K]_s = [K(x):K] = \deg(P).$$

- $\mathrm{Char}(K) = p$。此时，存在 $Q(X) \in K[X]$，使得 $P(X) = Q(X^{p^n})$ 并且 n 是**最大的**这样的指标。那么，

  $$[K(x):K] = p^n[K(x):K]_s.$$

  实际上，由于 n 是最大的并且 Q 是不可约的，所以，$Q' \neq 0$（否则 $Q = Q_1(X^p)$，那么 $P(X) = Q_1(X^{p^{n+1}})$）。此时，Q 有 d 个不同的根且无重根，从而 P 也有 d 个不同的根（从而 $[K(x):K]_s = d$）但每个根的重数均为 p^n。此时，$\deg(P) = p^n \cdot d$，所以，$[K(x):K] = p^n \cdot d$。这就给出了上述公式。

  我们有时也称 n 为 x 在 K 上**不可分次数**。

注记 5.31. 上述推理表明，当 $\mathrm{Char}(K) = p$ 时，$x \in K(x) \subset L$ 是可分的（当且仅当 $n = 0$）当且仅当 $[K(x):K] = [K(x):K]_s$。

定理 102. *假设域 K 的特征为 p，${}^{L}\!/_{K}$ 是有限扩张，则存在非负整数 $n \geqslant 0$（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: 由于 ${}^{L}\!/_{K}$ 是有限扩张，我们可以选取 $x_1, \cdots, x_k \in L$，使得 $L = K(x_1, \cdots, x_k)$。令 $K_0 = K$，$K_i = K(x_1, \cdots, x_i)$，其中，$i = 1, \cdots, k$。特别地，$K_i = K_{i-1}(x_i)$。根据以上关于单代数扩张情形的讨论，我们有

$$[K_i : K_{i-1}] = p^{n_i}[K_i : K_{i-1}]_s.$$

根据命题98中的公式，对上式 $i = 1, \cdots, k$ 取乘积并令 $n = \sum_{i=1}^{k} n_i$。这就证明了定理中的公式 $[L:K] = p^n[L:K]_s$。

若 ${}^{L}\!/_{K}$ 是可分扩张，则每个 x_i 在 K_{i-1} 上也可分，从而，$n_i = 0$。据此，$n = \sum_{i=1}^{k} n_i = 0$，所以 $[L:K] = [L:K]_s$。

若 L/K 不是可分的，在选择 $x_1,\cdots,x_k$ 使得 $L=K(x_1,\cdots,x_k)$ 的构造中，我们总可以要求 x_1 为不可分元，即 $n_1>0$。此时，$n=\sum_{i=1}^{k}n_i>0$。 □

推论 103. 若 L/K 是有限的纯不可分扩张，则 $[L:K]$ 是 p 的幂，其中 $p=\mathrm{Char}(K)$。

推论 104. 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: 对任意给定的 $x\in K(M)$，存在 $x_1,\cdots,x_k\in M$，使得 $x\in K(x_1,\cdots,x_k)$。定理102的证明过程表明 $K(x_1,\cdots,x_k)/K$ 是可分的。从而，$x\in K(x_1,\cdots,x_k)$ 可分。 □

推论 105. 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。

对任意的 $x\in L$，x 在 K 上的极小多项式没有重根。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），x 在 M 上的极小多项式也是没有重根的，从而 x 在 M 上可分。这说明 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。特别地，$x\in K(a_0,\cdots,a_{n-1},x)$。我们令

$$K_i=K(a_0,\cdots,a_i),\ K_n=K(a_0,\cdots,a_{n-1},x),\quad i=0,\cdots,n-1.$$

重复定理102证明过程，此时每个 n_i 均为 0，这说明 $K(a_0,\cdots,a_{n-1},x)/K$ 是可分的。特别地，x 在 K 上可分，从而 L/K 是可分的。 □

推论 106. 给定代数扩张 L/K，存在唯一的最大的[38]中间域 $\overline{L}^s$（被称作是 K 在 L 中的**可分闭包**），使得 $\overline{L}^s/K$ 是可分扩张。此时，$L/\overline{L}^s$ 是纯不可分的，即 $[L:\overline{L}^s]_s=1$。

$$\begin{array}{c} L \\ \Big|\ \text{纯不可分} \\ \overline{L}^s \\ \Big|\ \text{（极大）可分} \\ K \end{array}$$

进一步，如果 $[L:K]_s<\infty$，那么，

$$[L:K]_s=[\overline{L}^s:K]_s=[\overline{L}^s:K].$$

证明: 因为在 K 上添加可分元得到的扩张还是可分的，我们就把 L 中所有可分元素都添加到 K 中，这就给出了 $\overline{L}^s$ 的构造（同时也给出了最大性和唯一性）。

剩下还需要证明 $[L:\overline{L}^s]_s=1$。根据推论99，我们要证明对任意的 $x\in L$，$[\overline{L}^s(x):\overline{L}^s]_s=1$，这等价于证明 x 在 $\overline{L}^s$ 上的极小多项式 $P(X)\in\overline{L}^s[X]$ 只有一个根。此时，存在 $n\geqslant 1$，使得 $P(X)=Q(X^{p^n})$ 并且

[38]在包含关系下

$Q' \neq 0$（Q 不可约从而是可分的）。那么，x^{p^n} 是 Q 的根，从而 x^{p^n} 是可分的（因为 Q 是可分的）。根据 $\overline{L}^s$ 的定义方式，$x^{p^n} \in \overline{L}^s$，所以 $P(X) \mid X^{p^n} - x^{p^n} \in \overline{L}^s[X]$。然而 $X^{p^n} - x^{p^n}$ 只有一个根，所以 $P(X)$ 也只有一个根。

如果 $[L:K]_s < \infty$，那么，

$$[L:K]_s = [L:\overline{L}^s]_s[\overline{L}^s, K]_s = [\overline{L}^s, K]_s.$$

这就给出了 $[L:K]_s = [\overline{L}^s : K]_s = [\overline{L}^s : K]$。 □

例子 5.15. 假设 k 为特征为 2 的域，$K = k(x,y)$ 为二元函数域（即 $\mathrm{Frac}\big(k[X,Y]\big)$）。假设 α 是 $T^2+T+x \in K[T]$ 的一个根，$M = K(\alpha)$。由于 T^2+T+x 在 $K[T]$ 中不可约，所以 $[M:K] = 2$ 并且是可分扩张。实际上，由于 $k[x]$ 是唯一分解整环，所以，$k[x,y] = k[x][y]$ 也是。根据 Gauss 引理，T^2+T+x 在 $K[T]$ 中不可约等价于它在 $k[x,y][T]$ 中不可约。据此，可以假设

$$T^2+T+x = \big(T+f(x,y)\big)\big(T-f(x,y)+1\big) \quad \Rightarrow f(x,y)(1-f(x,y)) = x.$$

其中，$f(x,y) \in k[x,y]$，这与 x 是 $k[x,y]$ 中的不可约元矛盾。

假设 β 是 $T^2 - \alpha y \in M[T]$ 的一个根，令 $L = M(\beta)$，我们来说明 $[L:M] = 2$。若不然，存在 $f(x,y) + g(x,y)\alpha \in M$（因为 $\dim_K M = 2$），其中，$f, g \in K$，使得

$$\big(f(x,y)+g(x,y)\alpha\big)^2 = \alpha y \quad \Leftrightarrow \quad f(x,y)^2 + g(x,y)^2\alpha^2 = \alpha y.$$

利用 $\alpha^2 = \alpha + x$ 替换 α，我们有

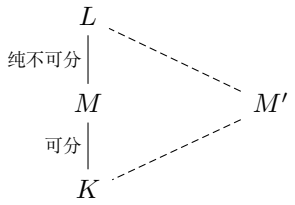
$$f(x,y)^2 + g(x,y)^2 x + \big(g(x,y)^2 - y\big)\alpha = 0.$$

根据 $1, \alpha$ 在 K 上的无关性，我们有

$$f(x,y)^2 + g(x,y)^2 x = 0, \;\; g(x,y)^2 = y.$$

然而，$g(x,y)^2 = g(x^2,y^2) = y$ 是不可能的。

我们注意到 $T^2 - \alpha y \in M[T]$ 不可分。此时，我们显然有



现在证明 L 在 K 上没有纯不可分的元素。假设存在中间域 M'，使得 M'/K 是纯不可分的，那么，对任意的 $\gamma \in M'$，我们有 $\gamma^2 = j(x,y) \in K$。利用 L/K 的基，我们有

$$\gamma = f(x,y) + g(x,y)\alpha + h(x,y)\beta + i(x,y)\alpha\beta.$$

从而，

$$\gamma^2 = j(x,y) \quad \Leftrightarrow \quad f(x,y)^2 + g(x,y)^2\alpha^2 + h(x,y)^2\beta^2 + i(x,y)^2\alpha^2\beta^2 = j(x,y)^2.$$

利用 $\alpha^2 = \alpha + x$ 和 $\beta^2 = \alpha y$，经过化简，我们得到

$$\big[f(x^2,y^2) + \boxed{g(x^2,y^2)x} + i(x^2,y^2)xy + j(x^2,y^2)\big] + \big[g(x^2,y^2) + \boxed{h(x^2,y^2)y} + i(x^2,y^2)xy + \boxed{i(x^2,y^2)y}\big]\alpha = 0.$$

通过通分，除了框内的两项，我们得到的多项式为偶数次的，从而，

$$g(x^2,y^2)=0,\ h(x^2,y^2)+i(x^2,y^2)=0.$$

从而，$g=0,h=i$。据此，我们可以化简上述长等式为

$$\begin{cases} f(x^2,y^2)+j(x^2,y^2)=i(x^2,y^2)xy, \\ i(x^2,y^2)=0. \end{cases}$$

只有 $f=j$，这表明 $\gamma\in K$。这说明 L 中在 K 上没有纯不可分的元素，我们也说 K 在 L 中是纯不可分封闭的。

例子 5.16. 在 $\mathbb{F}_p(T)[X]$ 中考虑多项式

$$P(X)=X^2+TX+T,\ \ Q(X)=X^{2p}+TX^p+T=P(X^p).$$

$P(X)$ 在 $\mathbb{F}_p(T)[X]$ 中是不可约的（根据 Gauss 引理和 Eisenstein 判别法），α,α 为 P 在 $\overline{\mathbb{F}_p(T)}$ 中的根。那么，$\mathbb{F}_p(T)(\alpha)/\mathbb{F}_p(T)$ 的次数为 2，这是可分的（因为 $P'\neq 0$）也是正规的。在 $\overline{\mathbb{F}_p(T)}[X]$ 中，我们有

$$P(X)=(X-\alpha)(X-\alpha'),\ \ \alpha,\alpha'\in\overline{\mathbb{F}_p(T)}.$$

$Q(X)$ 在 $\mathbb{F}_p(T)[X]$ 中是不可约的（根据 Gauss 引理和 Eisenstein 判别法）。令 β 为 Q 在 $\overline{\mathbb{F}_p(T)}$ 中的一个根，$P(\beta^p)=0$，我们不妨假设 $\beta^p=\alpha$。我们再选取 $\beta'\in\overline{\mathbb{F}_p(T)}$，使得 $\beta'^p=\alpha'$。此时，

$$Q(X)=(X^p-\alpha)(X^p-\alpha')=(X-\beta)^p(X-\beta')^p.$$

由于 $Q(X)$ 在 $\mathbb{F}_p(T)[X]$ 中不可约，所以 $[\mathbb{F}_p(T)(\beta):\mathbb{F}_p(T)]=2p$。

$$\begin{array}{c} \mathbb{F}_p(T)(\beta) \\ \text{纯不可分}\big| \\ \mathbb{F}_p(T)(\alpha) \\ \text{可分}\big| \\ \mathbb{F}_p(T) \end{array}$$

很明显，$\mathbb{F}_p(T)(\beta)/\mathbb{F}_p(T)(\alpha)$ 是纯不可分的。特别地，$[\mathbb{F}_p(T)(\beta),\mathbb{F}_p(T)]_s=2$。

例子 5.17 (最基础的例子)**.** 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，x^{p^n} 在 K 上是可分的。进一步，K 的可分闭包为 $K(x^{p^n})$，即

$$\begin{array}{c} K(x) \\ \text{纯不可分}\big| \\ K(x^{p^n}) \\ \text{可分}\big| \\ K \end{array}$$

实际上，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，我们可以给出可分闭包 $\overline{K(x)}^s=K(x^{p^n})$。

例子 5.18 (可分闭包的具体构造)**.** L/K 是代数扩张。根据上一例子，对任意的 $x\in L$，令 n_x 为其不可分次数。那么，$\left\{x^{p^{n_x}}\middle|x\in L\right\}$ 是 L 中所有可分元素。所以，

$$\overline{L}^s=K\left(\left\{x^{p^{n_x}}\middle|x\in L\right\}\right).$$

5.5.3 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 107. *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，由于 L/K 是有限扩张，L 也是有限域。此时，$L^\times$ 是有限循环群，那么，选这个循环群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。我们总可以把 L 写成 $L = K(x_1, \cdots, x_d)$ 的形式，只要对 $d = 2$ 证明该扩张为单扩张即可。现在，我们令 $L = K(x_1, x_2)$。由于 K 是无限域而 L/K 只有有限个中间域，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，

$$(a - b)x_2 = (x_1 + ax_2) - (x_1 + bx_2) \in M \quad \Rightarrow \quad x_2 \in M.$$

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 $P_M \mid P$。令

$$P_M(x) = X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0, \quad a_i \in M.$$

很显然，$K(a_0, \cdots, a_m) \subset M$。特别地，

$$[K(x) : K(a_0, \cdots, a_m)] \geqslant [L : M].$$

另外，我们还有：

$$[K(x) : K(a_0, \cdots, a_m)] \leqslant \deg(P_M) = [L : M],$$

从而，$M = K(a_0, \cdots, a_m)$。

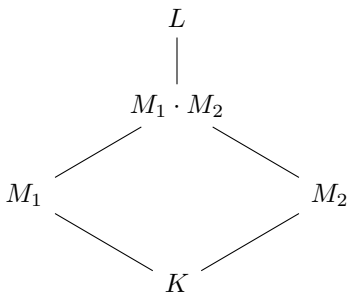
综合上面的讨论，中间域 M 完全由 P_M（的系数）决定。由于 P 的首一的因子 P_M 只有有限个，所以，L/K 只有有限个中间域。 □

推论 108 (本原元素定理)**.** *有限可分扩张是单扩张，即对于有限可分扩张 L/K，存在 $x \in L$，使得 $L = K(x)$。*

证明： 令 $\Omega = \overline{K}$；令 $\mathcal{P}$ 为 $\mathrm{Hom}_K(L, \Omega)$ 的子集所组成的集合（这是有限集）；令 $\mathcal{M}$ 为 L/K 的中间域所组成的集合。根据上一个命题，我们只要证明如下映射为单射即可：

$$\Psi : \mathcal{M} \longrightarrow \mathcal{P}, \quad M \mapsto \mathrm{Hom}_M(L, \Omega).$$

假设 $\Psi(M_1) = \Psi(M_2)$，即 $\mathrm{Hom}_{M_1}(L, \Omega) = \mathrm{Hom}_{M_2}(L, \Omega)$，我们考虑如下图表：



$\mathrm{Hom}_{M_1}(L,\Omega)=\mathrm{Hom}_{M_2}(L,\Omega)$ 表明 $\mathrm{Hom}_{M_1}(L,\Omega)\subset\mathrm{Hom}_{M_1\cdot M_2}(L,\Omega)$，所以，

$$|\mathrm{Hom}_{M_1\cdot M_2}(L,\Omega)|\geqslant|\mathrm{Hom}_{M_1}(L,\Omega)|.$$

由于 L/K 可分，所以，$L/M_1\cdot M_2$ 和 L/M_1 都可分，从而，

$$|\mathrm{Hom}_{M_1\cdot M_2}(L,\Omega)|=[L:M_1\cdot M_2]\leqslant[L:M_1]=|\mathrm{Hom}_{M_1}(L,\Omega)|.$$

结合以上两个不等式，我们有 $[L:M_1\cdot M_2]=[L:M_1]$，从而，$M_1\cdot M_2=M_1=M_2$，所以 Ψ 为单射。特别地，

$$|\mathcal{M}|\leqslant|\mathcal{P}|<\infty,$$

即 L 只有有限个中间域。从而，L/K 是单扩张。 □

例子 5.19. K 的特征为 p，考虑域扩张 $K(X,Y)/K(X^p,Y^p)$。我们注意到 $\{X^iY^j\}_{1\leqslant i,j\leqslant p-1}$ 是该扩张的一组基，从而 $[K(X,Y):K(X^p,Y^p)]=p^2$。另外，X 的极小多项式为 $T^p-X^p=0$（不可分），从而，X（类似地 Y）在 $K(X^p,Y^p)$ 上纯不可分。根据命题101，$K(X,Y)/K(X^p,Y^p)$ 是纯不可分的（从而不满足本原元素定理关于可分性的要求）。

现在说明 $K(X,Y)/K(X^p,Y^p)$ 有无限多个中间域。实际上，我们可以考虑如下中间域：

$$M_n:=K(X^p,Y^p,X+Y^{pn+1}),\quad n=1,2,\cdots.$$

我们注意到 $X+Y^{pn+1}\notin K(X^p,Y^p)$ 而 $\left(X+Y^{pn+1}\right)^p\in K(X^p,Y^p)$，所以，$[M_n:K(X^p,Y^p)]=p$。由于 $[K(X,Y):K(X^p,Y^p)]=p^2$，为了证明 $\{M_n\}_{n\geqslant1}$ 两两不同，只要证明

$$M=K(X^p,Y^p,X+Y^{pn+1},X+Y^{pm+1})=K(X,Y),\quad m\neq n,$$

即可。由于 $X+Y^{pn+1},X+Y^{pm+1}\in M$，所以，

$$Y\left((Y^p)^n-(Y^p)^m\right)=\left(X+Y^{pn+1}\right)-\left(X+Y^{pm+1}\right)\in M.$$

从而，$Y\in M$。进一步，$X\in M$。这说明 $M=K(X,Y)$。特别地，这表明 $K(X,Y)/K(X^p,Y^p)$ 不是单扩张。

现在还可直接证明 $K(X,Y)/K(X^p,Y^p)$ 不是单扩张。如若不然，假设 $K(X,Y)=K(X^p,Y^p,f(X,Y))$。由于 $f^p(X,Y)=f(X^p,Y^p)$（利用 K 的特征为 p），所以，$f^p\in K(X^p,Y^p)$。据此，f 的极小多项式 P 整除 T^p-a，其中，$a\in K(X^p,Y^p)$。特别地，$\deg(P)\leqslant p$，从而，

$$[K(X^p,Y^p,f(X,Y)):K(X^p,Y^p)]\leqslant p<p^2.$$

这和 $K(X,Y)=K(X^p,Y^p,f(X,Y))$ 矛盾。

5.5.4 迹与范数映射

对于有限扩张 L/K，对任意的 $x\in L$，考虑乘法映射：

$$m_x:L\to L,\quad y\mapsto x\cdot y.$$

这是 K-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：

$$\mathrm{Tr}_{L/K}(x)=\mathrm{Tr}(m_x),\ \mathrm{N}_{L/K}(x)=\det(m_x),\quad P_{L/K,x}(X)=\det(X\cdot I-m_x).$$

很明显，x 为 m_x 在域 L 上的特征值，从而，$P_{L/K,x}(x)=0$。

注记 5.32. 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 $e_1,\cdots,e_m$ 为 $K(x)/K$ 的基，$f_1,\cdots,f_n$ 为 $L/K(x)$ 的基。那么，$\{e_if_j\}_{i\leqslant m,j\leqslant n}$ 为 L/K 的基。考虑 $m_x:K(x)\to K(x)$ 的矩阵表示 M，我们有 $\det(X\cdot I-M)=P(x)$（只要选取 $1,x,\cdots,x^{m-1}$ 作为 $e_1,\cdots,e_m$ 进行计算即可，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

$$\begin{pmatrix}M&0&\cdots&0\\0&M&\cdots&0\\&&\ddots&0\\0&0&\cdots&M\end{pmatrix}.$$

这就给出了以上公式。

命题 109. *以下映射为群同态：*

$$\mathrm{Tr}_{L/K}:(L,+)\to(K,+),\quad \mathrm{N}_{L/K}:(L^\times,\cdot)\to(K^\times,\cdot).$$

如果 $M\subset L$ 是中间域，那么，

$$\mathrm{Tr}_{L/M}\circ\mathrm{Tr}_{M/K}=\mathrm{Tr}_{L/K},\quad \mathrm{N}_{L/M}\circ\mathrm{N}_{M/K}=\mathrm{N}_{L/K}.$$

证明： 群同态的性质根据定义立得。关于迹 Tr 以及范数 N 映射的复合性质请参考习题5.11.1。 □

定理 110. *L/K 为有限可分扩张，E/K 为域扩张并且 $|\mathrm{Hom}_K(L,E)|=[L:K]$。那么，对任意的 $x\in L$，*

$$\mathrm{Tr}_{L/K}(x)=\sum_{\sigma\in\mathrm{Hom}_K(L,E)}\sigma(x),\ \mathrm{N}_{L/K}(x)=\prod_{\sigma\in\mathrm{Hom}_K(L,E)}\sigma(x),$$

以及

$$P_{L/K,x}(X)=\prod_{\sigma\in\mathrm{Hom}_K(L,E)}\big(X-\sigma(x)\big).$$

证明： 证明请参考习题5.11.1。 □

关于迹与可分性的最重要结论是如下的定理：

定理 111. *L/K 是有限扩张。那么，L/K 是可分的等价于二次型*

$$L\times L\longrightarrow K,\quad (x,y)\mapsto\mathrm{Tr}_{L/K}(x\cdot y).$$

非退化。

证明： 证明请参考习题5.11.1。 □

注记 5.33. 当 $\mathrm{Char}(K)=0$ 时，L/K 是可分扩张。此时，对任意的 $x\in L$，令 $y=x^{-1}$，则

$$\mathrm{Tr}_{L/K}(x\cdot y)=\mathrm{Tr}_{L/K}(1)=[L:K]\neq 0.$$

进一步，如果 $[L:K]$ 与 $\mathrm{Char}(K)$ 互素，则二次型 $(x,y)\mapsto\mathrm{Tr}_{L/K}(x\cdot y)$ 非退化。特别地，此时 $[L:K]$ 是可分的。

注记 5.34. 给定有限可分的扩张 L/K，二次型 $\mathrm{Tr}_{L/K}(x\cdot y)$ 给出了 L（作为 K-线性空间）到其对偶 L^* 之间一个自然的同构：

$$L\xrightarrow{\simeq}L^*,\quad x\mapsto\Big(y\mapsto\mathrm{Tr}_{L/K}(x\cdot y)\Big).$$

据此，对任意的基 $\{e_1,e_2,\cdots,e_n\}$，我们可以定义其对偶基 $\{e_1^*,e_2^*,\cdots,e_n^*\}$，使得

$$\mathrm{Tr}_{L/K}(e_i\cdot e_j^*)=\begin{cases}1,\ i=j;\\0,\ i\neq j.\end{cases}$$

我们考虑单代数扩张的例子，$L=K(x)$，x 在 K 上可分，令 $P(X)$ 为 x 的极小多项式，$d=\deg(P)=[K(x):K]$。在 $L[X]=K(x)[X]$ 中，$P(X)$ 可以被写作

$$P(X)=(X-x)\left(b_{d-1}X^{d-1}+b_{d-2}X^{d-2}+\cdots+b_1X+b_0\right),,$$

其中，$b_k\in K(x)$ 并且 $b_{d-1}=1$。我们选取 $e_1=1,e_2=x,\cdots,e_d=x^{d-1}$ 作为 L 的基，现在来计算 $\{e_1^*,e_2^*,\cdots,e_d^*\}$。实际上，

$$e_k^*=\frac{b_{k-1}}{P'(x)},\ k=1,2\cdots,d.$$

在上式中，$P'(x)=\sum_{k=0}^{d-1}b_kx^k$。

我们要证明 $\mathrm{Tr}_{L/K}\left(x^j\cdot\frac{b_i}{P'(x)}\right)=\delta_i^j$，其中，$0\leqslant i,j\leqslant d-1$。固定 j，考虑多项式

$$Q(X)=\sum_{i=0}^{d-1}\mathrm{Tr}_{L/K}\left(x^j\cdot\frac{b_i}{P'(x)}\right)X^i.$$

只要证明 $Q(X)=X^j$ 即可。我们有

$$\begin{aligned}Q(X)&=\sum_{i=0}^{d-1}\sum_{\sigma\in\mathbf{Hom}_K(K(x),\overline{K})}\sigma\left(x^j\cdot\frac{b_i}{P'(x)}\right)X^i=\sum_{i=0}^{d-1}\sum_{\sigma\in\mathbf{Hom}_K(K(x),\overline{K})}\sigma\left(x^j\right)\frac{\sigma(b_i)}{P'\big(\sigma(x)\big)}X^i\\&=\sum_{\sigma\in\mathbf{Hom}_K(K(x),\overline{K})}\left[\left(\sum_{i=0}^{d-1}\sigma(b_i)X^i\right)\frac{\sigma\left(x^j\right)}{P'\big(\sigma(x)\big)}\right]\\&=\sum_{\sigma\in\mathbf{Hom}_K(K(x),\overline{K})}\frac{P(X)}{X-\sigma(x)}\frac{\sigma\left(x^j\right)}{P'\big(\sigma(x)\big)}\end{aligned}$$

根据 Lagrange 插值公式，上式为 X^j。

5.6 Galois 理论

5.6.1 Galois 对应

给定正规扩张 L/K，记 $\mathrm{Gal}(L/K)=\mathrm{Aut}_K(L)$ 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，就称 L/K 为 **Galois 扩张**。对任意的子群 $H<\mathrm{Gal}(L/K)$，定义

$$L^H:=\big\{x\in L\big|g(x)=x,\forall g\in H\big\}.$$

引理 112. *L/K 是有限正规扩张，则*

$$[L:K]_s=\big|\mathrm{Gal}(L/K)\big|.$$

特别地，若 L/K 是 Galois 扩张，那么

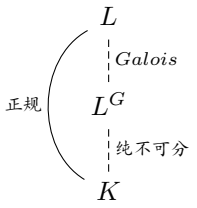
$$[L:K]=\big|\mathrm{Gal}(L/K)\big|.$$

证明：我们选定域扩张 Ω/L，其中，Ω 是代数封闭的。那么，

$$[L:K]_s = \left|\mathrm{Ext}_{L/K}(\Omega, \mathrm{id})\right| \overset{\text{正规}}{=} \left|\mathrm{Ext}_{L/K}(L, \mathrm{id})\right| = \left|\mathrm{Gal}(L/K)\right|.$$

如果 L/K 是 Galois 扩张，则 $[L:K]_s = [L:K]$，所以 $[L:K] = \left|\mathrm{Gal}(L/K)\right|$。 □

命题 113. L/K 是正规扩张，$G = \mathrm{Gal}(L/K)$。



那么，L^G/K 是纯不可分的，L/L^G 是 *Galois* 扩张并且

$$\mathrm{Gal}(L/L^G) = G.$$

进一步，我们有 $\overline{L}^s \cdot L^G = L$，$\overline{L}^s \cap L^G = K$。

证明：选定 $\Omega = \overline{K}$。根据正规性的定义，我们有（先将每个 $\mathrm{Ext}_{L^G/K}(\Omega, \mathrm{id})$ 中的映射延拓到 L 上）

$$\mathrm{Ext}_{L^G/K}(\Omega, \mathrm{id}) = \mathrm{Ext}_{L^G/K}(L, \mathrm{id}).$$

根据 L^G 的定义，对于每个 $\varphi \in \mathrm{Ext}_{L^G/K}(L, \mathrm{id})$，它被延拓到成 L 上的自同构（从而落在 G 中）之后在 L^G 上是单位映射。所以上式右边集合只有一个元素。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。因为 L/L^G 是正规的，所以 P 的所有根都在 L 中，令 $x_1, \cdots, x_m$ 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，

$$0 = P(x_i) = P^\sigma(x_i) = \big(\prod_{\text{所有根}} (X - \alpha)\big)^\sigma = \prod_{\text{所有根}} (X - \sigma(\alpha)).$$

这表明 x_i 形如 $\sigma(\alpha)$，其中，α 也是根，即 $\sigma^{-1}(x_i)$ 仍然是 P 的根。从而，我们得到了群作用：

$$\mathrm{Gal}(L/K) \times \{x_1, \cdots, x_m\} \to \{x_1, \cdots, x_m\}.$$

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，$P \mid Q$ 而 Q 无重根，所以 P 是可分的。

最后来说明 $\mathrm{Gal}(L/L^G) = G$。根据定义，$\mathrm{Gal}(L/L^G) < \mathrm{Gal}(L/K)$。另外，对任意的 $g \in \mathrm{Gal}(L/K)$，按定义，g 在 L^G 上的作用是平凡的，从而，$g \in \mathrm{Gal}(L/L^G)$，即 $\mathrm{Gal}(L/K) < \mathrm{Gal}(L/L^G)$。

我们注意到 $\overline{L}^s \cap L^G/K$ 是 L^G 的中间域，所以是纯不可分的，它也是 $\overline{L}^s$ 的中间域，所以是可分的，从而，$\overline{L}^s \cap L^G = K$；$\overline{L}^s \cdot L^G$ 是 $L/\overline{L}^s$ 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，$\overline{L}^s \cdot L^G = L$。 □

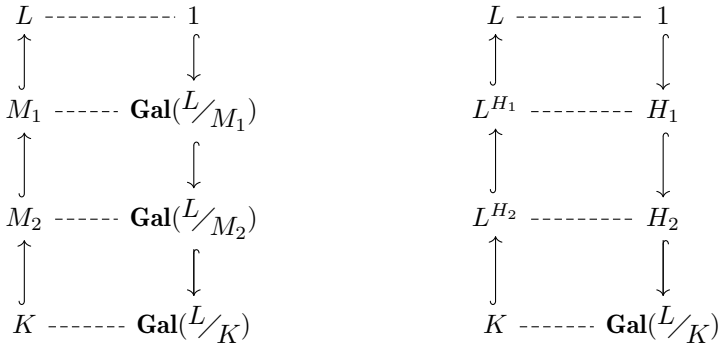
注记 5.35. 证明过程中利用 G 在根上的作用是 Galois 理论中最典型的推理方法（群作用）。

定理 114 (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：

$$\mathcal{M}=\big\{K\subset M\subset L\big|M\text{是中间域}\big\},\quad \mathcal{S}=\big\{H<\mathbf{Gal}(L/K)\text{是子群}\big\},$$

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）：

$$\mathcal{M}\xrightarrow{1:1}\mathcal{S},\quad M\mapsto\mathbf{Gal}(L/M),\quad L^H\hookleftarrow H.$$

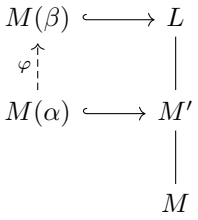


进一步，扩张 M/K 是正规扩张[39]当且仅当 $\mathbf{Gal}(L/M)\lhd\mathbf{Gal}(L/K)$ 是正规子群并且在此情形下，我们有

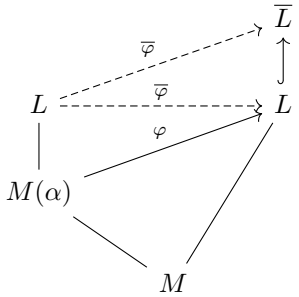
$$\mathbf{Gal}(M/K)=\mathbf{Gal}(L/K)\Big/\mathbf{Gal}(L/M).$$

证明: 我们用 $\Phi:\mathcal{M}\to\mathcal{S}$ 和 $\Psi:\mathcal{S}\to\mathcal{M}$ 表示上述对应映射。我们证明 $\Psi\circ\Psi=\mathrm{id}_{\mathcal{M}}$，即对给定的 $M\in\mathcal{M}$，证明 $L^{\mathbf{Gal}(L/M)}=M$：

令 $M'=L^{\mathbf{Gal}(L/M)}$，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，$\deg(P)\geqslant 2$。



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 $\varphi\in\mathrm{Hom}_M\big(M(\alpha),M(\beta)\big)$，从而，$\varphi\in\mathrm{Hom}_M\big(M(\alpha),L\big)$。



此时，φ 可以被扩张成 $\overline{\varphi}:L\to\overline{L}$。由于 L/M 是正规扩张，所以，$\overline{\varphi}:L\to L$，即 $\overline{\varphi}\in\mathbf{Gal}(L/M)$。然而，对于 $\alpha\in M'$，$\overline{\varphi}(\alpha)=\beta\neq\alpha$，矛盾。

[39]从而是 Galois 扩张

注记 5.36. 在以上证明 $\Psi\circ\Psi=\mathrm{id}_{\mathcal{M}}$ 的过程中，我们并不需要假设 $L\big/K$ 是有限扩张。作为应用，我们考虑 $\overline{\mathbb{Q}}\big/\mathbb{Q}$，这是 Galois 扩张。对任意的 $\alpha\in\overline{\mathbb{Q}}$，$\alpha\in\mathbb{Q}$ 当且仅当对任意的 $\sigma\in\mathbf{Gal}(\overline{\mathbb{Q}}\big/\mathbb{Q})$，$\sigma(\alpha)=\alpha$。

我们现在证明 $\Psi\circ\Phi=\mathrm{id}_{\mathcal{S}}$，即对给定的 $H\in\mathcal{S}$，证明 $\mathbf{Gal}(L\big/L^H)=H$。根据定义 $H<\mathbf{Gal}(L\big/L^H)$，特别地，我们有

$$|H|\leqslant\mathbf{Gal}(L\big/L^H)=[L:L^H].$$

由于 $L\big/L^H$ 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

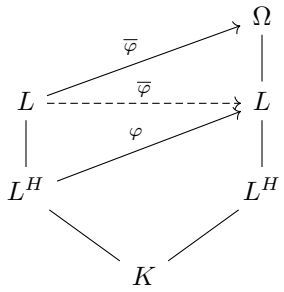
$$Q(X)=\prod_{h\in H}\big(X-h(\alpha)\big).$$

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 $Q\mid P$。特别地，

$$|H|=\deg(Q)\geqslant\deg(P)=[L^H(\alpha):L^H]=[L:L^H].$$

综合以上不等式，我们就证明了 $H=\mathbf{Gal}(L\big/L^H)$。

假设 $H\lhd\mathbf{Gal}(L\big/K)$，为了说明 $L^H\big/K$ 是正规扩张，任意选取 $\varphi\in\mathrm{Hom}_K(L^H,\Omega)$，其中，$\Omega=\overline{L}\supset L$，我们证明 $\varphi(L^H)=L^H$：

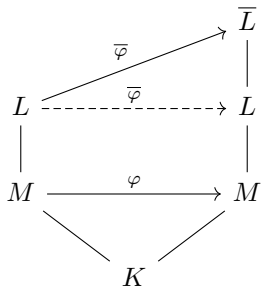


首先把 φ 延拓成 $\overline{\varphi}\in\mathrm{Hom}_K(L,\Omega)$，由于 $L\big/L^H$ 是正规扩张，所以，$\overline{\varphi}\in\mathrm{Hom}_K(L,L)$，从而，$\overline{\varphi}\in\mathbf{Gal}(L\big/K)$。为了证明 $\varphi(L^H)\subset L^H$，我们任选 $x\in L^H$，只要证明对任意的 $h\in H$，$h\big(\overline{\varphi}(x)\big)=\overline{\varphi}(x)$ 即可。这等价于 $\big(\overline{\varphi}^{-1}\cdot h\cdot\overline{\varphi}\big)(x)=x$。由于 $H\lhd\mathbf{Gal}(L\big/K)$，$\overline{\varphi}^{-1}\cdot h\cdot\overline{\varphi}\in H$ 而 $x\in L^H$，以上等式是显然的。

假设 $M\big/K$ 是正规扩张，那么，对任意的 $\varphi\in\mathbf{Gal}(L\big/K)$，我们有 $\varphi(M)\subset M$。通过 φ 在 M 上的限制，我们有群同态：

$$\mathrm{Res}:\mathbf{Gal}(L\big/K)\to\mathbf{Gal}(M\big/K).$$

另外，对每个 $\varphi\in\mathbf{Gal}(M\big/K)$，我们总能将它延拓成 $\mathbf{Gal}(L\big/K)$ 中的元素 $\overline{\varphi}$：



所以，以上的限制映射是满射：

$$\mathrm{Res}:\mathbf{Gal}(L\big/K)=\mathrm{Hom}_K(L,\overline{L})\twoheadrightarrow\mathrm{Hom}_K(M,\overline{L})=\mathbf{Gal}(M\big/K).$$

按照定义，$\mathrm{Ker}(\mathrm{Res}) = \mathbf{Gal}(L/M)$，即

$$1 \longrightarrow \mathbf{Gal}(L/M) \xrightarrow{\subset} \mathbf{Gal}(L/K) \xrightarrow{\mathrm{Res}} \mathbf{Gal}(M/K) \longrightarrow 1.$$

这就完成了整个证明。 □

例子 5.20 (二面体群在 Riemann 球面上的作用)**.** 考虑 $\mathbb{C}$ 上的一元函数域 $L = \mathbb{C}(T)$。令 ξ 为某个本原的 n-次单位根（比如选取 $\xi = e^{\frac{2\pi}{n}i}$），我们研究如下的自同构 $\mathbf{Aut}_{\mathbb{C}}(L)$：

$$\sigma(T) = \xi \cdot T, \quad \tau(T) = T^{-1}.$$

由于 $\sigma^n = \tau^2 = \mathrm{id}$ 并且 $\sigma\tau\sigma = \tau$，所以，$G = \langle \sigma, \tau \rangle < \mathbf{Aut}_{\mathbb{C}}(L)$ 同构于二面体群 $\mathfrak{D}_n$。令 $K = L^G$，我们来证明 $L^G = K := \mathbb{C}(T^n + T^{-n})$。很明显，我们有 $K \subset L^G$。令 $M = \mathbb{C}(T^n)$，那么，

$$\begin{array}{c} L = \mathbb{C}(T) \\ | \\ M = \mathbb{C}(T^n) \\ | \\ K = \mathbb{C}(T^n + T^{-n}) \end{array}$$

对于扩张 M/K 而言，T^n 在 K 上的极小多项式为 $X^2 - (T^n + T^{-n})X + 1$；对于扩张 L/M 而言，T^n 在 K 上的极小多项式为 $X^n - T^n$。据此，我们知道

$$[L : K] = [L : M][M : K] = 2n$$

上面的观察还告诉我们 $\mathbb{C}(T)$ 是 $X^{2n} - (T^n + T^{-n})X^n + 1$ 在 $\mathbb{C}(T^n + T^{-n})$ 上的分裂域（它的 $2n$ 个根恰好为 $\xi^i T^{\pm 1}, i = 1, \cdots, n$）。所以，$L/K$ 是正规扩张，从而是 Galois 扩张。

由于 $K \subset L^G$ 并且 $[L : L^G] = |G| = 2n$，以上关于次数的计算表明 $K = L^G$。

注记 5.37. 如果 L/K 是有限正规扩张，我们还有

$$[L : L^G] = [L : K]_s = \mathrm{Gal}(L/K), \quad [L^G : K] = \frac{[L : K]}{[L : K]_s} = L/K \text{ 的不可分次数.}$$

根据 Galois 对应，$L^{\mathbf{Gal}}(L/K) = K$，我们形象地说如果 $x \in L$ 在 $\mathbf{Gal}(L/K)$ 下作用不变，那么它可以下降到 K 中。对于线性空间，我们也有类似的 Galois 下降：

命题 115. *给定有限维 Galois 扩张 L/K 和 n-维 L-线性空间 L^n 是，其中，$e_1 = (1, 0, \cdots, 0), \cdots, e_n = (0, \cdots, 0, 1)$ 是它的标准的基。对任意的 $x = (x_1, \cdots, x_n) \in L^n$ 和 $\sigma \in \mathbf{Gal}(L/K)$，我们定义*

$$\sigma(x) = \big(\sigma(x_1), \cdots, \sigma(x_n)\big).$$

假设 $V \subset L^n$ 是 V 的 d-维 L-线性子空间并且在 $\mathbf{Gal}(L/K)$ 作用下不变，即对任意的 $v \in V$ 和 $\sigma \in \mathbf{Gal}(L/K)$，有 $\sigma(v) \in V$。那么，存在 V 的基 $v_1 = (v_{11}, \cdots, v_{1n}), \cdots, v_d = (v_{d1}, \cdots, v_{dn})$，使得 $v_{ij} \in K$，其中，$1 \leqslant i \leqslant d, 1 \leqslant j \leqslant n$。

证明: 任选 $v_1,\cdots,v_d$ 作为 V 的基，把每个 v_i 看作是行向量并排成一列，我们得到如下的 $d\times n$ 矩阵，通过对 v_i 做线性组合，我们总可以把这个矩阵调成如下的形式：

$$\begin{pmatrix} 0 & \cdots & 0 & 1 & * & 0 & 0 & * & \cdots & * \\ 0 & \cdots & \cdots & 0 & 0 & 1 & 0 & * & \cdots & * \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0 & 0 & \cdots & 0 & 0 & 0 & 1 & * & \cdots & * \end{pmatrix}$$

其中，每一行都是从 1 作为开始项（前面为 0）、每行的 1 都严格在前一行的 1 之后并且每个开始的 1 之上都是 0。

我们现在考虑 $\sigma(v_i)\in V$，即

$$\sigma(v_i)=c_1v_1+\cdots+c_iv_i+\cdots+c_dv_d.$$

由于 σ 作用在每个分量上，根据以上表达式以及上述矩阵每行的 1 都严格在前一行的 1 之后均为 0，$c_1,\cdots,c_{i-1}=0$ 而 $c_i=1$，即

$$\sigma(v_i)=v_i+c_{i+1}v_{i+1}\cdots+c_dv_d.$$

再利用每个开始的 1 之上都是 0，我们就有 $c_{i+1}=\cdots=c_d=0$。据此，$\sigma(v_i)=v_i$，即其每个分量都在 $\mathbf{Gal}(L/K)$ 作用下不变，从而落在 K 中。 □

注记 5.38. 以上命题使得我们可以定义一个 L-线性空间的 K-线性子空间。

5.6.2 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 $Z_P(L)=\{\alpha_1,\cdots,\alpha_d\}$ 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 $L=K(\alpha_1,\cdots,\alpha_d)$。

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

$$\mathbf{Gal}(L/K)\times Z_P(L)\longrightarrow Z_P(L),\ \ (\sigma,\alpha)\mapsto\sigma(\alpha).$$

由于对任意的 $\sigma_1,\sigma_2\in\mathbf{Gal}(L/K)$，我们显然有 $\sigma\big(\sigma_2(\alpha)\big)=(\sigma_1\cdot\sigma_2)(\alpha)$，以上映射给出了 Galois 群 $\mathbf{Gal}(L/K)$ 在根的集合 $Z_P(L)$ 上的作用 $\mathbf{Gal}(L/K)\curvearrowright Z_P(L)$。根据群作用的定义，我们有群同态

$$\mathbf{Gal}(L/K)\longrightarrow\mathfrak{S}_{Z_P(L)}.$$

由于 $L=K(\alpha_1,\cdots,\alpha_d)=K\big(Z_P(L)\big)$，所以，如果 $\sigma\in\mathrm{Ker}\big(\mathbf{Gal}(L/K)\to\mathfrak{S}_{Z_P(L)}\big)$，那么，$\sigma$ 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

$$\mathbf{Gal}(L/K)\longrightarrow\mathfrak{S}_{Z_P(L)}$$

是单同态。

定理 116. K 是域，$P \in K[X]$ 为可分的多项式，L 是 P 的分裂域。那么，$\mathbf{Gal}(L/K)$ 在根的集合上的作用 $Z_P(L)$ 是忠实的：

$$1 \to \mathbf{Gal}(L/K) \longrightarrow \mathfrak{S}_{Z_P(L)}.$$

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，

$$\mathbf{Gal}(L/K) \times Z_{P_1}(L) \longrightarrow Z_{P_1}(L).$$

对 $Z_{P_2}(L)$，以上仍然成立。所以，$\mathbf{Gal}(L/K) \curvearrowright Z_P(L)$ 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 $\mathbf{Gal}(L/K) \curvearrowright Z_P(L)$ 是传递的：假设 $\{\alpha_1, \cdots, \alpha_{d'}\}$ 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 $\sigma \in \mathbf{Gal}(L/K)$，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 $K = L^{\mathbf{Gal}(L/K)}$，$Q(X) \in K[X]$。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：

注记 5.39. 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

$$P(X) = P_1(X)P_2(X) \cdots P_m(X),$$

那么，$\mathbf{Gal}(L/K) \curvearrowright Z_P(L)$ 具有 m 个轨道并且每个轨道都对应着某个 $P_i(X)$ 的根。

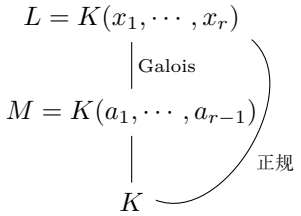
例子 5.21. K 是域，L 是多项式 $P(X) \in K[X]$ 的分裂域，其中，

$$P(X) = (X - x_1)^{n_1} \cdots (X - x_r)^{n_r}, \quad x_i \in L.$$

此时，L/K 是有限正规扩张，$\mathbf{Gal}\left(L/K\right)$ 是 L/K 的 K-自同构群（定义）。令

$$Q(X) = (X - x_1) \cdots (X - x_r) = X^r + a_{r-1}X^{r-1} + \cdots + a_1X + a_0.$$

并令 $M = K(a_0, \cdots, a_{r-1})$。此时，$L$ 是 M 的分裂域并且 $L = M(x_1, \cdots, x_r)$。由于 $x_1, \cdots, x_r$ 在 $Q(X)$ 中没有重根，所以，在 M 上可分，从而，L/M 是可分的。据此，L/M 是 Galois 扩张。



我们自然有（作为子群）：

$$\mathbf{Gal}\left(L/M\right) \longrightarrow \mathbf{Gal}\left(L/K\right).$$

另外，对任意的 $\sigma \in \mathbf{Gal}\left(L/K\right)$，由于 a_i 是 $x_1, \cdots, x_r$ 的对称多项式，所以，$\sigma(a_i) = a_i$，从而，$\sigma\big|_M = \mathrm{id}$，从而，上述映射是满的。据此，我们得到等式

$$\mathbf{Gal}\left(L/M\right) = \mathbf{Gal}\left(L/K\right).$$

例子 5.22. 考虑域扩张 $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$，我们来计算其 Galois 群 $G = \mathbf{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$。

利用中间域

$$\mathbb{Q} \text{ —— } \mathbb{Q}(\sqrt{2}) \text{ —— } \mathbb{Q}(\sqrt{2},\sqrt{3}),$$

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

$$G \hookrightarrow \mathfrak{S}_{\left\{\sqrt{2},-\sqrt{2},\sqrt{3},-\sqrt{3}\right\}} \simeq \mathfrak{S}_4$$

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 $G \simeq \mathbb{Z}/4\mathbb{Z}$，由于其生成元对应着 4-循环，那么它的作用只能有 1 个轨道）。在以上 $\mathfrak{S}_{\left\{\sqrt{2},-\sqrt{2},\sqrt{3},-\sqrt{3}\right\}} \simeq \mathfrak{S}_4$ 的等同中，我们要求 $1 \leftrightarrow \sqrt{2}$, $2 \leftrightarrow -\sqrt{2}$, $3 \leftrightarrow \sqrt{3}$, $4 \leftrightarrow -\sqrt{3}$。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

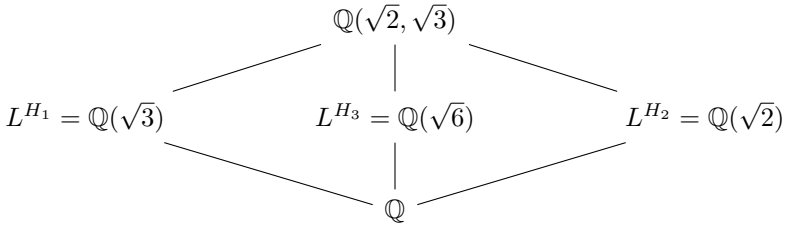
$$G = \langle (1,2), (3,4) \rangle.$$

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[40]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：



例子 5.23（利用 Galois 群决定域扩张）**.** 若 $\mathrm{Char}(K) \neq 2$，L/K 是 4 次 Galois 扩张并且 $\mathbf{Gal}\left(L/K\right) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$。那么，存在 $a,b \in L$，使得 $L = K(\sqrt{a},\sqrt{b})$。

实际上，当 $\mathrm{Char}(K) \neq 2$ 时，对任意的 2 次扩张 M/K，必然存在 $a \in K, x \in M$，使得 $x^2 = a$ 并且 $M = K(x)$（此时，我们记 $x = \sqrt{a}$，当然，x 不唯一）。任选 $y \in M - K$，由于 $[L:K] = 2$，$1, y, y^2$ 是 K-线性相关的。从而，存在 $b,c \in K$，使得

$$y^2 + by + c = 0 \quad \Rightarrow \quad \big(y + \frac{b}{2}\big)^2 = \frac{b^2}{4} - c.$$

[40]我们只要考虑 $H < G$ 使得 $H \neq G$，$H \neq 1$。

以上，我们用到了 $\mathrm{Char}(K)\neq 2$。此时，$x=y+\frac{b}{2}, a=\frac{b^2}{4}-c$。

考虑 $\mathbf{Gal}\left(L/K\right)\simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ 的两个不同的 2 阶子群 H_1,H_2。根据 Galois 对应，L^{H_1}/K 和 L^{H_2}/K 是两个不同的 2 次中间域。所以，存在 $a,b\in L$，使得

$$L^{H_1}=K(\sqrt{a}),\quad L^{H_a}=K(\sqrt{b}).$$

那么，$L\supset K(\sqrt{a},\sqrt{b})$。通过考虑次数易见，$L=K(\sqrt{a},\sqrt{b})$。

例子 5.24. 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，

$$G\hookrightarrow \mathfrak{S}_3,$$

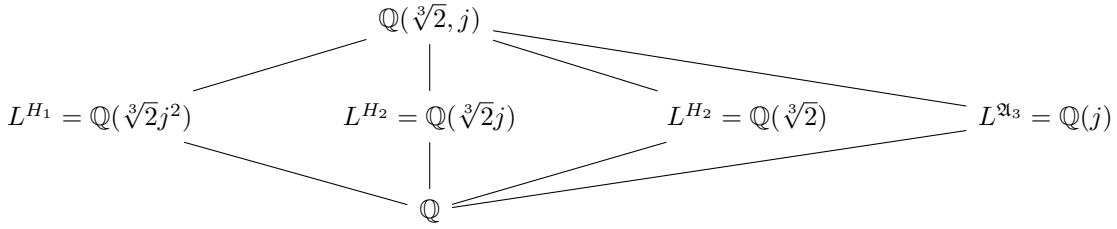
其中，$G=\mathbf{Gal}(\mathbb{Q}(\sqrt[3]{2},j))$。根据中间域

$$\mathbb{Q}\ \text{——}\ \mathbb{Q}(\sqrt[3]{2})\ \text{——}\ \mathbb{Q}(\sqrt[3]{2},j),$$

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 $z\mapsto\overline{z}$ 是 G 中的元，它对应着对换 $(2,3)$。我们还知道 $\mathfrak{S}_3$ 有 4 个非平凡的子群：

$$H_1=\langle(1,2)\rangle,\ H_2=\langle(1,3)\rangle,\ H_3=\langle(2,3)\rangle,\ \mathfrak{A}_3=\langle(1,2,3)\rangle.$$

它们所对应的中间域为



以上，$\mathfrak{A}_3\lhd\mathfrak{S}_3$ 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。

例子 5.25. 令 L 为多项式 $P(X)=X^5-6X+3$ 在 $\mathbb{Q}$ 上的分裂域。根据 Eisentein 判别法 $(\mathrm{mod}\ 3)$，$P(X)$ 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 $x_5=\overline{x_4}$。特别地，我们知道复共轭映射 $z\mapsto\overline{z}$ 是 $G=\mathbf{Gal}(L/\mathbb{Q})$ 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)。根据习题3.6.1的第二问，一个对换和 5-循环可以生成 $\mathfrak{S}_5$，从而，$\mathbf{Gal}(L/\mathbb{Q})\simeq\mathfrak{S}_5$。特别地，$[L:\mathbb{Q}]=120$。

由于 $\mathbf{Gal}(L/\mathbb{Q})\simeq\mathfrak{S}_5$ 中有唯一的指标为 2 的子群 H，它同构于 $\mathfrak{A}_5$。那么，$L^H=E$ 是唯一的 2 次中间域。此时，$E=\mathbb{Q}(\sqrt{d})$，这里，d 是某个无平方因子的整数。我们现在计算 d 的数值。

根据例子4.22，我们考虑多项式 $P(X)=X^n+aX+b$，此时，$n=5,a=-6,b=3$。令 $\Delta=\prod_{i<j}(x_i-x_j)$ 为其判别式，则

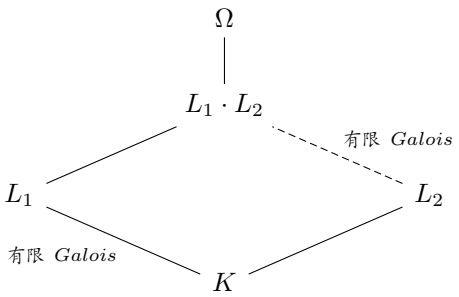
$$\mathrm{Disc}(P):=\Delta^2=\prod_{i<j}(x_i-x_j)^2=(-1)^{\frac{n(n-1)}{2}}\prod_{i\neq j}(x_i-x_j)=n^nb^{n-1}+(-1)^{n-1}(n-1)^{n-1}a^n.$$

由于 Δ^2 是 P 的系数的多项式，所以 $\Delta^2 \in \mathbb{Q}$。我们也可以使用 Galois 理论证明这一点：Δ^2 在 $\mathbf{Gal}(L/\mathbb{Q})$ 的作用下不变，从而 $\Delta^2 \in \mathbb{Q}$。利用上述公式，我们计算

$$\Delta^2 = 5^5 \times 3^4 - 4^4 \times 6^5 = 3^4 \times (-21451).$$

根据定义，Δ 在 $\mathfrak{A}_5$ 作用下不变而 $L^{\mathfrak{A}_5}$ 对应着 $\mathbb{Q}$ 的二次扩张 E，其中，$\Delta \in E$。特别地，$E = \mathbb{Q}(\sqrt{-21351})$。

命题 117 (域的复合)**.** *给定域扩张 Ω/K 以及中间域 L_1, L_2，$L_1 \cdot L_2$ 为它们的复合。如果 L_1/K 是有限 Galois 扩张，那么，$L_1 \cdot L_2/L_2$ 也是有限 Galois 扩张。*



通过在 L_1 上的限制，我们有单的群同态：

$$\mathrm{Res} : \mathbf{Gal}\left(L_1 \cdot L_2/L_2\right) \longrightarrow \mathbf{Gal}\left(L_1/K\right), \quad \sigma \mapsto \sigma\big|_{L_1},$$

并且其像为 $\mathbf{Gal}\left(L_1/L_1 \cap L_2\right)$。特别地，我们有 $\mathbf{Gal}\left(L_1 \cdot L_2/L_2\right) \simeq \mathbf{Gal}\left(L_1/L_1 \cap L_2\right)$。

进一步，我们还有 $[L_1 : K] = [L_1 \cdot L_2 : L_2][L_1 \cap L_2 : K]$。特别地，如果 L_2/K 是有限扩张并且 $L_1 \cap L_2 = K$，那么，$[L_1 \cdot L_2 : K] = [L_1 : K][L_2 : K]$。

证明: 由于 L_1 在 K（从而在 L_2）上是可分的，所以，$L_1 \cdot L_2 = L_2(L_1)$ 在 L_2 上也是可分的；由于 L_1 在 K 上是正规的，那么，L_2 是 K 通过添加一族 K-系数多项式 $\{P_i\}_{i \in I}$ 的所有根而得到的，所以 $L_1 \cdot L_2$ 是 L_2 通过添加 $\{P_i\}_{i \in I}$ 的所有根而得到，从而，$L_1 \cdot L_2/L_2$ 是正规的。以上证明了 $L_1 \cdot L_2/L_2$ 是 Galois 扩张（显然是有限的）。

对任意的 $\sigma \in \mathbf{Gal}\left(L_1 \cdot L_2/L_2\right)$，它的限制给出了

$$\sigma\big|_{L_1} : L_1 \longrightarrow L_1 \cdot L_2.$$

由于 L_1/K 是正规的，从而，

$$\sigma\big|_{L_1} : L_1 \longrightarrow L_1.$$

这就定义出

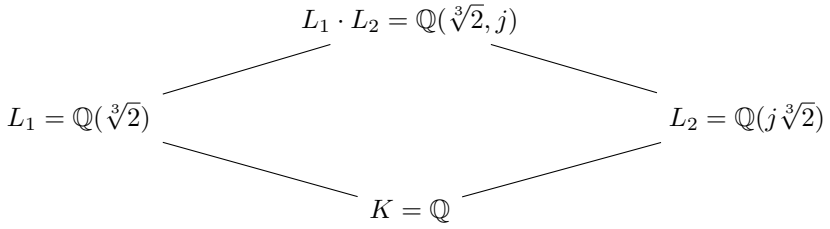
$$\mathrm{Res} : \mathbf{Gal}\left(L_1 \cdot L_2/L_2\right) \longrightarrow \mathbf{Gal}\left(L_1/K\right).$$

另外，根据上面的推理，如果 $\sigma\big|_{L_1} = \mathrm{id}_{L_1}$，它在 $\{P_i\}_{i \in I}$ 的所有根上的作用都是不动的，从而，在 $L_2(L_1) = L_1 \cdot L_2$ 上的作用也是不动的。这就表明上述限制映射 Res 是单射。

令 $H := \mathrm{Im}(\mathrm{Res}) < \mathbf{Gal}\left(L_1/K\right)$，根据 Galois 对应，只要证明 $L_1^H = L_1 \cap L_2$ 即可。由于 Res 是单射，对任意的 $x \in L_1$，$x \in L_1^H$ 等价于 x 作为 $L_1 \cdot L_2$ 中的元素在 $\mathbf{Gal}\left(L_1 \cdot L_2/L_2\right)$ 作用下不变，即等价于 $x \in L_2$。据此，$H = \mathbf{Gal}\left(L_1/L_1 \cap L_2\right)$。

其余的结论都是简单的推论，我们略去证明。 □

注记 5.40. 如果 L_1/K 不是 Galois 扩张，以上命题的结论不成立。实际上，令 $j = e^{\frac{2}{3}\pi i}$，我们考虑如下域的复合：

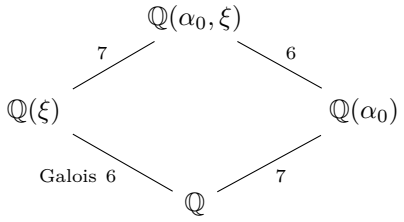


那么，$[L_1 : K] = 3$ 而 $[L_1 \cdot L_2 : L_2] = 2$，所以，$[L_1 \cdot L_2 : L_2]$ 不整除 $[L_1 : K]$。

练习 5.1. 给定域扩张 Ω/K 以及中间域 L_1, L_2，$L_1 \cdot L_2$ 为它们的复合，假设 L_1/K 是有限正规扩张而 L_2/K 是有限扩张。证明，如果 L_1/K 或 L_2/K 是可分的，那么，$[L_1 \cdot L_2 : L_1] = [L_1 : L_1 \cap L_2]$。

例子 5.26. K 为 $X^7 - 8$ 在 $\mathbb{Q}$ 上的分裂域，我们来计算 $\mathbf{Gal}\left(K/\mathbb{Q}\right)$。

$X^7 - 8$ 在 $\mathbb{Q}$ 上不可约。令 $\xi = e^{\frac{2\pi}{7}i}$ 为 7 次单位根，$\alpha_0 = 8^{\frac{1}{7}}$。容易看出，$\xi, \alpha_0 \in K$ 并且 $K = \mathbb{Q}(\alpha_0, \xi)$，从而，



从而，$[K : \mathbb{Q}] = 42$。中间域 $\mathbb{Q}(\xi)$ 对应着一个 7 阶子群 $\mathbf{Gal}\left(K/\mathbb{Q}(\xi)\right)$，从而，$\mathbf{Gal}\left(K/\mathbb{Q}\right)$ 中有一个 7 阶元 σ_1；中间域 $\mathbb{Q}(\alpha_0)$ 对应着一个 6 阶子群，根据命题117，我们有 $\mathbf{Gal}\left(K/\mathbb{Q}(\alpha_0)\right) \simeq \mathbf{Gal}\left(\mathbb{Q}(\xi)/\mathbb{Q}\right) = \mathbb{Z}/6\mathbb{Z}$，从而，$\mathbf{Gal}\left(K/\mathbb{Q}\right)$ 中有一个 6 阶元 σ_2。所以，$\mathbf{Gal}\left(K/\mathbb{Q}\right) = \langle \sigma_1, \sigma_2 \rangle$ 是 42 阶循环群，实际上，

$$\mathbf{Gal}\left(K/\mathbb{Q}\right) = \mathbf{Gal}\left(K/\mathbb{Q}(\xi)\right) \times \mathbf{Gal}\left(K/\mathbb{Q}(\alpha_0)\right).$$

5.6.3 有限 Galois 扩张的正规基

命题 118. *假设域 K 中有无限多个元素，L/K 是 n-次 Galois 扩张并且 $\mathbf{Gal}\left(L/K\right) = \{\sigma_1, \cdots, \sigma_n\}$。那么，对任意的非零多项式 $P \in K[X_1, \cdots, X_n]$，存在 $x \in L$，使得*

$$P\big(\sigma_1(x), \sigma_2(x), \cdots, \sigma_n(x)\big) \neq 0.$$

注记 5.41. 由于 $|K| = \infty$，则对任意非零多项式 $P \in K[X_1, \cdots, X_n]$，存在 $x_1, \cdots, x_n \in K$，使得 $P(x_1, \cdots, x_n) \neq 0$。

我们可以对 n 归纳来证明这个性质。当 $n = 1$ 时，使得 $P(x_1) = 0$ 的 x_1 不超过 $\deg(P)$ 个，所以，存在 $x \in K$，使得 $P(x) = 0$。假设当 $n - 1$ 时，命题成立。如果 $P(X_1, \cdots, X_n)$ 不含 X_n 变量，则根据归纳假设 P 在某个位置处不为 0。否则，我们可以把 P 写成

$$P(X_1, \cdots, X_n) = P_d(X_1, \cdots, X_{n-1})X_n^d + P_{d-1}(X_1, \cdots, X_{n-1})X_n^{d-1} + \cdots + P_0(X_1, \cdots, X_{n-1})$$

并且 $P_d(X_1, \cdots, X_{n-1})$ 非零。根据归纳假设，先选 $x_1, \cdots, x_{d-1}$，使得 $P_d(x_1, \cdots, x_{n-1}) \neq 0$。此时，$P(x_1, \cdots, x_{n-1}, X_n)$ 是关于 X_n 的非零多项式，由 $n = 1$ 的结论，存在 x_n 使得 $P(x_1, \cdots, x_{n-1}, x_n) \neq 0$。

命题的证明. 任选 L/K 的一组基 $e_1,\cdots,e_n$。对任意 $x\in L$，它可以被写成

$$x=x_1e_1+x_2e_2+\cdots+x_ne_n,$$

其中，$x_i\in K$ 并且

$$P\big(\sigma_1(x),\sigma_2(x),\cdots,\sigma_n(x)\big)=0.$$

从而，

$$P\big(\sum_{i=1}^n x_i\sigma_1(e_i),\cdots,\sum_{j=1}^n x_j\sigma_n(e_j)\big)=0.$$

令

$$Q(X_1,\cdots,X_n)=P\big(\sum_{i=1}^n X_i\sigma_1(e_i),\cdots,\sum_{j=1}^n X_j\sigma_n(e_j)\big).$$

根据前面注记，$Q(X_1,\cdots,X_n)=0$。根据注记5.51 给定有限 Galois 扩张 L/K，矩阵 $\big(\sigma_i(e_j)\big)_{1\leqslant i,j\leqslant n}$ 可逆，令 $(A_{ij})\in\mathbf{GL}(L;n)$ 为其逆。所以，

$$P(X_1,\cdots,X_n)=Q\big(\sum_{i=1}^n A_{1i}X_i,\cdots,\sum_{j=1}^n A_{nj}X_j\big)=0.$$

所以 P 为零。 □

注记 5.42. 若 K 是有限域,则存在非零多项式 $P(X_1,\cdots,X_n)$,使得对任意 $x_1,\cdots,x_n\in K$,有 $P(x_1,\cdots,x_n)=0$。比如说

$$P(X_1,\cdots,X_n)=\big(X_1^q-X_1\big)\big(X_2^q-X_2\big)\cdots\big(X_n^q-X_n\big),$$

其中，$q=|K|$。

定理 119 (有限 Galois 扩张的正规基定理)**.** L/K 是有限 *Galois* 扩张。那么，存在 $x\in L$，使得 $\big\{\sigma(x)\big|\sigma\in\mathbf{Gal}\left(L/K\right)\big\}$ 是 L 的一组基（作为 K-线性空间）。我们把这种基称作是 L/K 的**正规基**。

证明: 假设 K 中元素个数是无限的，考虑多项式环 $K\left[X_\sigma\big|\sigma\in\mathbf{Gal}\left(L/K\right)\right]=K[\sigma_1,\cdots,\sigma_n]$ 中的多项式

$$P(X_{\sigma_1},\cdots,X_{\sigma_n})=\det\left(X_{\sigma_i^{-1}\cdot\sigma_j}\right)_{1\leqslant i,j\leqslant n}.$$

不妨设 $\sigma_1=\mathrm{id}$，那么，$P(X_{\sigma_1},\cdots,X_{\sigma_n})=1$（它对应的矩阵是单位矩阵)。根据上一命题，存在 $x\in L$，使得

$$P(\sigma_1(x),\cdots,\sigma_n(x))=\pm\det\left(X_{\sigma_i^{-1}\cdot\sigma_j}\right)_{1\leqslant i,j\leqslant n}\neq 0.$$

我们现在说明 $\{\sigma(x_1),\cdots,\sigma(x_n)\}$ 是 L 的一组基础：假设 $a_1,\cdots,a_n\in K$，使得

$$a_1\sigma_1(x)+a_2\sigma_2(x)+\cdots+a_n\sigma_n(x)=0,$$

那么，对任意的 $i=1,\cdots,n$，我们有

$$\sigma_i^{-1}\left(\sum_{j=1}^n a_j\sigma_j(x)\right)=0.$$

即

$$\sum_{j=1}^n(\sigma_i^{-1}\cdot\sigma_j)(x)a_j=0.$$

由于 $\det\left(X_{\sigma_i^{-1}\cdot\sigma_j}\right)_{1\leqslant i,j\leqslant n}\neq 0$，我们有 $a_1=\cdots=a_n=0$，这说明 $\{\sigma(x_1),\cdots,\sigma(x_n)\}$ 线性无关，从而是 L 的一组基。 □

注记 5.43. 我们将利用 Artin 的引理123 来证明有限域的情形。

5.6.4 有限域

K 是有限域，$\mathrm{char}(K)=p$，我们有自然的域同态：

$$\mathbb{F}_p \longrightarrow K.$$

据此，我们知道 $|K|=p^n$，其中，$n=[K:\mathbb{F}_p]$。

定理 120. *p 是素数。对任意的 $n\geqslant 1$，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。*

注记 5.44. 假设 q 为素数的幂，我们用将 $\mathbb{F}_q$ 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

$$K:=\left\{x\in\overline{\mathbb{F}_p}\middle|x^{p^n}-x=0\right\}.$$

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 121. *对于 $q=p^n$，$\mathbf{Gal}({}^{\mathbb{F}_q}\!/_{\mathbb{F}_p})$ 是 n 阶循环群并且其生成元为*

$$\mathrm{Frob}:\mathbb{F}_q\to\mathbb{F}_q,\quad x\mapsto x^p.$$

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，$\mathbf{Gal}({}^{\mathbb{F}_{p^n}}\!/_{\mathbb{F}_{p^m}})$ 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，$\mathbf{Gal}({}^{\mathbb{F}_q}\!/_{\mathbb{F}_p})$ 有 n 个元素。我们自然有 $\mathrm{Frob}\in\mathbf{Gal}({}^{\mathbb{F}_q}\!/_{\mathbb{F}_p})$。另外，$\mathrm{Frob}^n=x^{p^n}=x^q$，对于循环群的生成元 $\xi\in\mathbb{F}_q^\times$，$\mathrm{Frob}^k(\xi)=\xi$ 当且仅当 $n-1\mid k-1$，从而，$\mathrm{Frob}^k\neq 1$，其中，$1\leqslant k\leqslant n-1$。据此，$\mathbf{Gal}({}^{\mathbb{F}_q}\!/_{\mathbb{F}_p})=\{\mathrm{Frob}^k|0\leqslant k\leqslant n-1\}$，所以，

$$\mathbf{Gal}({}^{\mathbb{F}_q}\!/_{\mathbb{F}_p})=\langle\mathrm{Frob}\rangle.$$

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，$m\mid n$，并且 m 阶子群是唯一的，所以，Galois 对应定理保证了上述给出了所有的中间域。由于 Frob^m 固定 $\mathbb{F}_{p^m}$ 中的所有元素并且其阶为 $\frac{n}{m}$，所以

$$\mathbf{Gal}({}^{\mathbb{F}_{p^n}}\!/_{\mathbb{F}_{p^m}})\simeq\langle\mathrm{Frob}^m\rangle.$$

这就完成了证明。 □

注记 5.45. 对任意的 p 的幂 q，$\mathbf{Gal}(\mathbb{F}_{q^l}/\mathbb{F}_q)$ 是 l 阶循环群。

例子 5.27. K 是有限域（特征为 p），L/K 是有限扩张，则 $\mathrm{N}_{L/K}: L^\times \to K^\times$ 是满射。

假设 $|L| = q^l, |K| = q$，x 为 $L^\times$（循环群）的生成元。此时，$\sigma \in \mathbf{Gal}\left(L/K\right)$ 的作用为

$$\sigma(x) = x^q.$$

所以，

$$\mathrm{N}_{L/K}(x) = \prod_{j=0}^{l-1} \sigma^j(x) = x^{1+q+\cdots+q^{l-1}} = x^{\frac{q^l-1}{q-1}}.$$

在循环群 $L^\times$ 中，x 的阶为 $q^l - 1$，上式表明 $\mathrm{N}_{L/K}(x)$ 阶为 $q - 1 = |K^\times|$。所以，$\mathrm{N}_{L/K}(x)$ 为 $K^\times$ 的生成元：首先，注意到 x 是 $X^q - X$ 的根；另外，K 中的每个元素都是该多项式的根并且这个多项式一共有 q 个根。所以，$x \in K$。

5.6.5 分圆扩张

对任意的域 K 和正整数 $n \geqslant 1$，定义 K 中 n-次单位根的集合：

$$\mu_n(K) = \left\{x \in K \middle| x^n - 1 = 0\right\}.$$

由于 n 次多项式至多有 n 个（不同的）根，所以，$|\mu_n(K)| \leqslant n$。

注记 5.46. 当 $\mathrm{char}(K) = p$ 时，令 $n = mp^k$，其中，$p \nmid m$。此时，$x^n - 1 = 0$ 等价于 $(x^m - 1)^{p^k} = 0$，从而，$\mu_n(K) = \mu_m(K)$。

注记 5.47 (循环群结构)**.** 对任意的 $\xi, \xi' \in \mu_n(K)$，显然有 $\xi^{-1}, \xi \cdot \xi' \in \mu_n(K)$，所以 $\mu_n(K)$ 是 $K^\times$ 的子群。

- 由于 $K^\times$ 的有限子群为循环群，所以 $\mu_n(K)$ 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**。
- 如果 $n_1 \mid n_2$，$\mu_{n_1}(K) < \mu_{n_2}(K)$ 是子群。
- $|\mu_n(K)| \big| n$，这是因为对任意的 $x \in \mu_n(K)$，总有 $x^n = 1$。

现在研究**分圆多项式**。对任意的 $n \geqslant 1$，令

$$\Phi_n(X) := \prod_{\substack{\xi \in \mu_n(\overline{\mathbb{Q}}), \\ \xi \text{ 本原}}} (X - \xi).$$

考虑 $\mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 对 Φ_n 的作用。每一个 $\sigma \in \mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 把 n-次本原根映射成 n-次本原根，从而，$\Phi_n^\sigma = \Phi_n$。据此，$\Phi_n(X) \in \mathbb{Q}[X]$。另外，将 n-次单位根根据其阶分类，我们得到如下公式

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

我们回忆 Gauss 引理，对唯一分解整环 A 及其分式域 $K = \mathrm{Frac}(A)$，若在 $K[X]$ 中有 $P(X) = P_1(X)P_2(X)$，其中，$\deg(P_i) \geqslant 1$，则存在 $k \in K^\times$，使得 $kP_1(x), k^{-1}P_2(X) \in A[X]$。由于上式中 $X^n - 1$ 以及分圆多项式 Φ_d 均为首一多项式，所以，$\Phi_n(X) \in \mathbb{Z}[X]$。

注记 5.48. 分圆多项式有一系列有趣的性质，我们用习题的形式呈现给大家：

- 假设 $n \geqslant 2$。证明，$\Psi_n(X) = X^{\deg(\Psi_n)}\Psi_n(X^{-1})$。
- 证明，$\Psi_{2n}(X) = \begin{cases} \Psi_n(-X), & 2 \nmid n; \\ \Psi_n(X^2), & 2 \mid n. \end{cases}$。
- 证明，若 p 是素数且 $p \nmid n$，则 $\Psi_{pn}(X) = \frac{\Psi_n(X^p)}{\Psi_n(X)}$。
- $n = p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$ 是 n 的素因数分解。证明，$\Psi_n(X) = \Psi_{p_1\cdots p_k}(X^{p_1^{r_1-1}p_2^{r_2-1}\cdots p_k^{r_k-1}})$。

通过研究所谓的分圆域，我们可以证明分圆多项式 $\Phi_n(X)$ 是不可约多项式。

定义 5.11 (分圆域)**.** K 是域，$n \geqslant 1$，ξ 是 $\overline{K}$ 中的一个 n-次本原单位根；当 $\mathrm{char}(K) = p$ 时，还进一步要求 $(p, n) = 1$。我们称 $K(\xi) \subset \overline{K}$ 是 K 的**n-次分圆域**或者**n-次分圆扩张**。

注记 5.49. $K(\xi)$ 不依赖于 n-次本原单位根的选取，因为 $K(\xi) = K(\mu_n(\overline{K}))$。

对任意的域 K，存在唯一的环同态 $\iota : \mathbb{Z} \to K$。通过对系数作用，我们可以将每个 $\mathbb{Z}[X]$ 中的多项式 $P(X)$ 视作 $K[X]$ 中的多项式 $P^K(X)$，即对于 $P(X) = \sum_{i=0}^{d} a_i X^i$，定义 $P^K(X) = \sum_{i=0}^{d} \iota(a_i)X^i$。特别地，我们得到 $\Phi_n^K(X) \in K[X]$。

定理 122. *$K(\xi)/K$ 是 K 的 n-次分圆扩张[41]，$P(X)$ 是 ξ 在 K 上的极小多项式。那么，$K(\xi)/K$ 是 Galois 扩张，$P(X) \mid \Phi_n^K(X)$ 并且如下群同态是单射：*

$$\mathbf{Gal}(K(\xi)/K) \longrightarrow \left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}, \quad \sigma \mapsto k_\sigma,$$

其中，$\sigma(\xi) = \xi^{k_\sigma}$。

证明： $K(\xi)$ 是 $X^n - 1$ 的分裂域，从而 $K(\xi)/K$ 是正规扩张；$\left(X^n - 1\right)' = nX^{n-1} \neq 0$（因为当 $\mathrm{char}(K) = p$ 时，$(p, n) = 1$），所以 $X^n - 1$ 是可分的多项式，从而 $K(\xi)/K$ 是可分扩张。这就说明了 $K(\xi)/K$ 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 $d = n$：如若不然，$\Phi_d^K(\xi) = 0$，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 $\overline{K}$ 中，由于 $(p, n) = 1$，我们恰有 n 个根）。

由于 $\sigma \in \mathbf{Gal}(K(\xi)/K)$ 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，$(k_\sigma, n) = 1$。此时，$\sigma \mapsto k_\sigma$ 显然是群同态。这就定义出定理中的群同态。由于 $K(\xi)$ 是单扩张，这个群同态是单的。 □

注记 5.50. $|\mathbf{Gal}(K(\xi)/K)| = [K(\xi) : K]$ 整除 $\varphi(n)$。

例子 5.28. 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 $\mathbf{Gal}\left(\mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q}\right) \to \left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$ 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。

[41] 当 $\mathrm{char}(K) = p$ 时，总假设 $(p, n) = 1$。

为了说明 $\mathbf{Gal}(K(\xi)/K) \to \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ 是满射，这要证明对任意的 $l \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$，存在 $\sigma \in \mathbf{Gal}(K(\xi)/K)$，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 $P \mid \Phi_n$，$\mathbf{Gal}(K(\xi)/K)$ 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

$$Q(X)^l = P(X)A(X) \mod l.$$

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。

例子 5.29. 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，$\mathbf{Gal}(\mathbb{F}_q(\xi)/\mathbb{F}_q)$ 是循环群并且

$$\mathbf{Gal}(\mathbb{F}_q(\xi)/\mathbb{F}_q) = \left\langle \sigma : x \mapsto x^q \right\rangle.$$

从而，$\mathrm{Im}\big(\mathbf{Gal}(\mathbb{F}_q(\xi)/\mathbb{F}_q) \to \left(\mathbb{Z}/n\mathbb{Z}\right)^\times\big)$ 由 σ 的像生成，它把 ξ 映射成 ξ^q。从而，σ 在 $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ 中恰好是 $q \mod n$。特别地，$[\mathbb{F}_q(\xi) : \mathbb{F}_q]$ 恰好是 q 在 $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ 的阶。

例子 5.30 (Galois 反问题)**.** 对任意的有限交换群 A，存在数域[42] $K/\mathbb{Q}$，使得 $\mathbf{Gal}(K/\mathbb{Q}) \simeq A$。特别地，任意的有限交换群 A 都可以实现为 $\mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 的商群。

根据有限生成交换群的分类定理，存在 $d_1, \cdots, d_s \in \mathbb{Z}_{\geqslant 2}$，使得

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

并且 $d_1 \mid d_2, d_2 \mid d_3, \cdots, d_{s-1} \mid d_s$。根据 Dirichlet 定理[43]，对每个 $i = 1, \cdots, s$，我们选取素数 p_i，使得 $p_i \equiv 1 \mod d_i$。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，

$$\mathbf{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \simeq \left(\mathbb{Z}/n\mathbb{Z}\right)^\times \simeq \prod_{i=1}^{s} \left(\mathbb{Z}/p_i\mathbb{Z}\right)^\times \simeq \prod_{i=1}^{s} \mathbb{Z}/(p_i - 1)\mathbb{Z}.$$

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：

$$1 \to d_i\mathbb{Z}/(p_i - 1)\mathbb{Z} \to \mathbb{Z}/(p_i - 1)\mathbb{Z} \to \mathbb{Z}/d_i\mathbb{Z} \to 1.$$

从而，A 是 $\mathbf{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ 的商群，即有 $H \simeq \prod_{i=1}^{s} d_i\mathbb{Z}/(p_i - 1)\mathbb{Z}$，使得 $\mathbf{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})/H \simeq A$。此时，根据 Galois 对应，$K = \mathbb{Q}(\xi)^H$ 的 Galois 群为 A。

[42] 数域就是 $\mathbb{Q}$ 的有限扩张

[43] 参见习题5.11.8

5.6.6 Hilbert 90 与循环扩张的 Kummer 理论

给定 Galois 扩张 L/K。若 $\mathbf{Gal}(L/K)$ 是循环群，则称 L/K 是**循环扩张**；若 $\mathbf{Gal}(L/K)$ 是交换群，则称 L/K 是 **Abel 扩张**。

引理 123 (特征的线性无关性, E. Artin)**.** *G 是群，K 是域，$\mathrm{Funt}(G,K)$ 是 G 上 K-值函数的 K-线性空间，$\chi_1,\cdots,\chi_k\in\mathrm{Hom}(G,K^\times)$ 是群同态（被称作是特征）。那么，$\chi_1,\cdots,\chi_k$ 在 $\mathrm{Funt}(G,K)$ 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，现在考虑如下的线性关系：

$$a_1\chi_1(g)+\cdots+a_k\chi_k(g)+a_{k+1}\chi_{k+1}(g)=0,\ \ \forall g\in G,$$

其中，$a_1,\cdots,a_{k+1}\in K$。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

$$a_1\chi_1(h)\chi_1(g)+\cdots+a_k\chi_k(h)\chi_k(g)+a_{k+1}\chi_{k+1}(h)\chi_{k+1}(g)=0,\ \ \forall g\in G.$$

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

$$a_1(\chi_1(h)-\chi_k(h))\chi_1(g)+\cdots+a_{k-1}(\chi_{k-1}(h)-\chi_k(h))\chi_{k-1}(g)+a_{k+1}(\chi_{k+1}(h)-\chi_k(h))\chi_{k+1}(g)=0,\ \ \forall g\in G.$$

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。 □

注记 5.51. 给定有限 Galois 扩张 L/K,令 $\mathbf{Gal}\left(L/K\right)=\{g_1,\cdots,g_n\}$,那么,对任意 L/K 的基 $e_1,\cdots,e_n\in L$，矩阵 $\left(g_i(e_j)\right)_{1\leqslant i,j\leqslant n}\in\mathbf{GL}(n;L)$。

如若不然，则存在不全为 0 的 $c_1,\cdots,c_n\in L$，使得对任意的 $1\leqslant j\leqslant n$，有

$$c_1g_1(e_j)+c_2g_2(e_j)+\cdots+c_ng_n(e_j)=0.$$

由于 $e_1,\cdots,e_n\in L$ 是 L/K 的基，所以对任意的 $x\in L$，由

$$c_1g_1(x)+c_2g_2(x)+\cdots+c_ng_n(x)=0.$$

将每个 g_i 视作是 $L^\times$ 上的特征 $g_i:L^\times\to L^\times$，则它们线性相关，这与引理123矛盾。

例子 5.31. 给定有限 Galois 扩张 L/K，令 $\mathbf{Gal}\left(L/K\right)=\{g_1,\cdots,g_n\}$，再任选 L/K 的基 $x_1,\cdots,x_n\in L$，其中 $x_1=1$。

考虑 n-维 L-线性空间 V 并假设 G 可以线性作用在 V 上并且对任意的 $g\in\mathbf{Gal}(L/K)$ 和 $v,w\in V,\lambda\in L$，有

$$g(v+w)=g(v)+g(w),\ \ g(\lambda\cdot v)=g(\lambda)g(v).$$

令

$$V^{\mathbf{Gal}(L/K)}=\left\{v\in V\middle|g(v)=v,\text{ 对任意 }g\in\mathbf{Gal}(L/K)\right\}.$$

由于对任意的 $k\in K,v\in V^{\mathbf{Gal}(L/K)}$，$g(kv)=g(k)g(v)=kv$，所以 $V^{\mathbf{Gal}(L/K)}$ 是 K-线性空间。用平均值应该在群作用下不变的想法可以构造 $V^{\mathbf{Gal}(L/K)}$ 中的元素：对任意的 $v\in V$，则

$$\sum_{i=1}^m g_i(v)\in V^{\mathbf{Gal}(L/K)}.$$

特别地，

$$v(j) := \sum_{i=1}^{m} g_i(e_j \cdot v) = \sum_{i=1}^{m} g_i(e_j) g_i(v) \in V^{\mathbf{Gal}(L/K)}.$$

由于 $\big(g_i(e_j)\big)_{1\leqslant i,j\leqslant n}$ 可逆，所以，$g_i(v)$ 是 $v(j)$ 的 L-线性组合。若取 $g_i = g_1 = 1$，那么，每个 $v \in V$ 均为 $V^{\mathbf{Gal}(L/K)}$ 中元素的 L-线性组合，即 $\mathrm{span}_L V^{\mathbf{Gal}(L/K)} = V$。据此，我们得到 L-线性空间之间的满同态：

$$\varphi : V^{\mathbf{Gal}(L/K)} \otimes_K L \twoheadrightarrow V, \quad v \otimes \lambda \mapsto \lambda \cdot v.$$

以上还是 $\mathbf{Gal}(L/K)$ 作用之间的同态。我们现在证明该同态实际上是满射。若不然，则存在 $\sum_{i=1}^{m} v_i \otimes \lambda_i \in \mathrm{Ker}(\varphi)$，即 $\sum_{i=1}^{m} \lambda_i v_i = 0 \in V$。我们假设 m 是使得上述成立的最小的非零整数。我们注意到存在某个 $\lambda_i \notin K$：否则

$$\sum_{i=1}^{m} v_i \otimes \lambda_i = \left(\sum_{i=1}^{m} \lambda_i v_i \right) \otimes 1 = 0.$$

不妨假设 $\lambda_m \notin K$，则存在 $g \in \mathbf{Gal}(L/K)$，使得 $g(\lambda_m) \neq \lambda_m$。由于

$$g\left(\sum_{i=1}^{m} v_i \otimes \lambda_i \right) \in \mathrm{Ker}(\varphi) = \sum_{i=1}^{m} v_i \otimes g(\lambda_i).$$

所以，

$$\lambda_m g\left(\sum_{i=1}^{m} v_i \otimes \lambda_i \right) - g(\lambda_m) \sum_{i=1}^{m} v_i \otimes \lambda_i \in \mathrm{Ker}(\varphi)$$

即

$$\sum_{i=1}^{m-1} v_i \otimes \big(\lambda_m g(\lambda_i) - g(\lambda_m)\lambda_i \big) \in \mathrm{Ker}(\varphi).$$

我们不妨设 $\lambda_1 = 1$，由 m 的最小性，上式中 $i = 1$ 时意味着 $g(\lambda_m) = \lambda_m$，矛盾。

综上所述，我们有 G-作用间的同构

$$V^{\mathbf{Gal}(L/K)} \otimes_K L \xrightarrow{\sim} V, \quad v \otimes \lambda \mapsto \lambda \cdot v.$$

注记 5.52 (有限域上（循环扩张上）正规基的构造)**.** K 是有限域，L/K 是有限扩张（从而是 Galois 扩张），σ 为 K 上的 Frobenius 同构，即 $\sigma(x) = x^q$，其中，$x \in L, |q| = |K|$。此时，$\mathbf{Gal}\left(L/K\right) = \langle \sigma \rangle$ 是有限群。

1) K 上的 Frobenius 同构 σ 定义了 L 是上的一个有限生成的 $K[X]$-模结构，即对任意的 $P(X) = \sum_{i=0}^{d} a_i X^i \in K[X]$（其中 $a_i \in K$）和 $x \in L$，定义 $P(X) \cdot x := \sum_{i=0}^{d} a_i \sigma^i(x)$。

2) 作为 K-线性映射 $\sigma \in \mathbf{End}_K(L)$，$\sigma$ 的极小多项式为 $X^n - 1$。

   实际上，$\sigma^n = 1$，从而其极小多项式整除 $X^n - 1$。如果这个极小多项式的次数小于 n，那么，就存在 $a_0, \cdots, a_d \in K$（某些非零），$d < n$，使得

   $$a_0 + a_1\sigma + \cdots + a_d\sigma^d = 0.$$

   这和 Artin 的特征不相关性引理矛盾（在 Artin 的定理123中取 $G = L^\times, K = L$，此时，$\mathbf{Gal}\left(L/K\right)$ 中的元素为特征）。

   特别地，作为 K-线性映射 $\sigma \in \mathbf{End}_K(L)$，$\sigma$ 的极小多项式恰为其特征多项式（因为前者整除后者并且有相同的维数）。

3) 对 $K[X]$-模 L 用主理想整环上有限生成模的分类定理，从而存在首一多项式 $P_1,\cdots,P_s\in A$，使得 $(P_1)\supset(P_2)\supset\cdots\supset(P_s)$ 并且

$$L\simeq K[X]\big/(P_1(X))\oplus K[X]\big/(P_2(X))\oplus\cdots\oplus K[X]\big/(P_s(X)).$$

我们强调上面的分解是 $K[X]$-模的直和。特别地，$P_1(\sigma)=0$（因为 $P_1|P_2|\cdots|P_s$）。从而，$X^n-1\mid P_1$。由于 $\dim_K L=n$，所以，$s=1$ 并且 $P_1(X)=X^n-1$。从而，作为 $K[X]$-模，我们有同构

$$K[X]\big/(X^n-1)\xrightarrow{\simeq}L.$$

此时，作为 K-线性空间，上式左边有一组自然的基 $\{1,X,\cdots,X^{n-1}\}$。根据上述同构，这组基对应了 L 中的基

$$\big\{g\in\mathbf{Gal}\left(L\big/K\right)\big|g\cdot x\big\}=\{x,\sigma(x),\cdots,\sigma^{n-1}(x)\}.$$

这是 $L\big/K$ 的正规基。

引理 124 (Hilbert 90)**.** [44] *$L\big/K$ 是次数为 n 的循环扩张，$\sigma\in\mathbf{Gal}(L\big/K)$ 是生成元，$x\in L$。那么，*

$$\begin{cases}\mathrm{N}_{L/K}(x)=1 & \Leftrightarrow \text{ 存在 } y\in L,\text{ 使得 } x=\frac{y}{\sigma(y)};\\ \mathrm{Tr}_{L/K}(x)=0 & \Leftrightarrow \text{ 存在 } y\in L,\text{ 使得 } x=y-\sigma(y).\end{cases}$$

证明： 假设 $\mathbf{Gal}(L\big/K)=\langle\sigma\rangle=\{1,\sigma,\sigma^2,\cdots,\sigma^{n-1}\}$。

如果 $x=\frac{y}{\sigma(y)}$，那么，

$$\mathrm{N}_{L/K}(x)=\prod_{k=0}^{n-1}(\sigma^k(x))=\frac{\prod_{k=0}^{n-1}(\sigma^k(y))}{\prod_{k=0}^{n-1}(\sigma^{k+1}(y))}=1.$$

反之（E. Artin），$\mathrm{N}_{L/K}(x)=1$，即 $x\sigma(x)\cdots\sigma^{n-1}(x)=1$。我们考虑 L 到自身的 K-线性映射：

$$\psi=\mathrm{id}+x\sigma+(x\sigma(x))\sigma^2+\cdots+\big(x\sigma(x)\cdots\sigma^{n-2}(x)\big)\sigma^{n-1}.$$

这是 n 个特征的线性组合[45]，根据 Artin 引理，存在 $y\in L$，使得 $\psi(y)\neq0$。我们计算 $\sigma(\psi(y))$：

$$\begin{aligned}\sigma(\psi(y))=&\sigma(y)+\sigma(x)\sigma^2(y)+\sigma(x)\sigma^2(x)\sigma^3(y)\\&+\cdots+\sigma(x)\sigma^2(x)\cdots\sigma^{n-2}(x)\sigma^{n-1}(y)+\underbrace{\sigma(x)\sigma^2(x)\cdots\sigma^{n-1}(x)}_{=x^{-1}}y\\=&x^{-1}\big[x\sigma(y)+x\sigma(x)\sigma^2(y)+x\sigma(x)\sigma^2(x)\sigma^3(y)+\cdots+x\sigma(x)\sigma^2(x)\cdots\sigma^{n-2}(x)\sigma^{n-1}(y)+y\big]\\=&x^{-1}\psi(y).\end{aligned}$$

所以，$x=\frac{\psi(y)}{\sigma(\psi(y))}$。

如果 $x=y-\sigma(y)$，那么，

$$\mathrm{Tr}_{L/K}(x)=\sum_{k=0}^{n-1}(\sigma^k(x))=\sum_{k=0}^{n-1}\sigma^k(y)-\sum_{k=0}^{n-1}\sigma^{k+1}(y)=0.$$

[44] 这是 Hilbert 著名的 Zahlbericht 中的第九十个定理。

[45] 以上 ψ 的构造是自然的：为了找到 y，使得 $x=\frac{y}{\sigma(y)}$，即 $x\sigma(y)=y$，定义映射 $f(y)=x\sigma(y)$。那么，y 是 f 的不动点。据此，我们取 y 在 f 下的平均 $\frac{1}{n}\sum_{k=0}^{n-1}f^k(y)$，这与 ψ 的形式基本一致。

反之，$\mathrm{Tr}_{L/K}(x)=0$，即 $x+\sigma(x)+\cdots+\sigma^{n-1}x=0$。由于 L/K 是可分的，根据习题5.11.1，二次型

$$\mathrm{Tr}_{L/K}: L\times L\to K,\ \ (x_1,x_2)\mapsto \mathrm{Tr}_{L/K}(x_1x_2),$$

是非退化的。特别地，存在 $z\in L$，使得 $\mathrm{Tr}_{L/K}(z)\neq 0$。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，

$$\begin{aligned}\sigma(y)=&\sigma(x)\sigma^2(z)+(\sigma(x)+\sigma^2(x))\sigma^2(z)+\cdots+\underbrace{(\sigma(x)+\sigma^2(x)\cdots+\sigma^{n-1}x)}_{=-x}z\\ =&-xz+(x+\sigma(x))\sigma^2(z)+(x+\sigma(x)+\sigma^2(x))\sigma^2(z)+\cdots\\ &-x(\sigma^2(z)+\sigma^2(z)+\cdots+\sigma^{n-1}(z))\\ =&y-x(z+\sigma(z)+\sigma^2(z)+\sigma^2(z)+\cdots+\sigma^{n-1}(z))=y-x\mathrm{Tr}_{L/K}(z).\end{aligned}$$

从而，$x=\frac{1}{\mathrm{Tr}_{L/K}(z)}(y-\sigma(y))$。 □

注记 5.53 (一般形式的 Hilbert 90)**.** 给定有限的 Galois 扩张 L/K，当 $\mathbf{Gal}\left(L/K\right)$ 不再是循环群时，我们也有类似的结论。

考虑函数 $f:\mathbf{Gal}\left(L/K\right)\to L^\times$。那么，如下两个陈述等价：

a) 对任意的 $g,h\in\mathbf{Gal}\left(L/K\right)$，$f(gh)=g(f(h))f(g)$；

b) 存在 $x\in L$，使得对任意的 $g\in\mathbf{Gal}\left(L/K\right)$，$f(g)=\frac{x}{g(x)}$。

只要证明 $a)\Rightarrow b)$ 即可。令 $x=\sum_{h\in\mathbf{Gal}(L/K)}f(h)h(y)$，其中，根据引理123，我们可以选取 y，使得 $x\neq 0$。对任意的 $g\in\mathbf{Gal}\left(L/K\right)$，我们计算

$$\begin{aligned}g(x)=&\sum_{h\in\mathbf{Gal}(L/K)}g(f(h))g(h(y))=\sum_{h\in\mathbf{Gal}(L/K)}f(g)^{-1}f(g\cdot h)(g\cdot h)(y)\\ \overset{gh=k}{=}&f(g)^{-1}\sum_{k\in\mathbf{Gal}(L/K)}f(k)k(y)=f(g)^{-1}x.\end{aligned}$$

从而，$f(g)=\frac{x}{g(x)}$。

例子 5.32. 利用 Hilbert 90，我们可以找出所有满足勾股定理的整数解。为此，我们考虑域扩张 $\mathbb{Q}(i)/\mathbb{Q}$，此时，其 Galois 群是 2-阶循环群并且其非平凡自同构为 $\sigma: x+yi\mapsto x-yi$。为了找到所有的 $x,y,z\in\mathbb{Z}$，使得 $x^2+y^2=z^2$，我们注意到这个式子等价于 $\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}\left(\frac{x}{z}+\frac{y}{z}i\right)=1$。根据 Hilbert 90，以上等价于存在 $q_1+q_2i\in\mathbb{Q}(i)$，使得

$$\frac{x}{z}+\frac{y}{z}i=\frac{\sigma(q_1+q_2i)}{q_1+q_2i}=\frac{q_1-q_2i}{q_1+q_2i}.$$

通过约去因子，我们可以假设 $q_1=m,q_2=n$ 是整数，从而，

$$\frac{x}{z}+\frac{y}{z}i=\frac{m-ni}{m+ni}=\frac{m^2-n^2}{m^2+n^2}-\frac{2mn}{m^2+n^2}i.$$

这表明（通过调整 m 的符号）(x,y,z) 与 $(m^2-n^2,2mn,m^2+n^2)$ 成比例。

例子 5.33 (解 Pell 方程)**.** 假设 $d \in \mathbb{Z}_{\geqslant 1}$ 不是完全平方数，我们要找如下 Pell 方程

$$x^2 - dy^2 = 1$$

的所有有理数解。为此，考虑 2-次域扩张 $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$，其 Galois 群是 2-阶循环群并且其非平凡自同构为 $\sigma : x + y\sqrt{d} \mapsto x - y\sqrt{d}$。此时，

$$\mathrm{N}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}\left(x + y\sqrt{d}\right) = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2.$$

所以，Pell 方程等价于 $\mathrm{N}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}\left(x + y\sqrt{d}\right) = 1$。根据 Hilbert 90，这等价于存在 $m, n \in \mathbb{Z}$，使得

$$x + y\sqrt{d} = \frac{m - n\sqrt{d}}{m + n\sqrt{d}} = \frac{m^2 + dn^2}{m^2 - dn^2} - \frac{2mn}{m^2 - dn^2}\sqrt{d}.$$

从而，

$$x = \frac{m^2 + dn^2}{m^2 - dn^2},\ y = \frac{2mn}{m^2 - dn^2}\sqrt{d},\ m, n \in \mathbb{Z}$$

给出了 Pell 方程的通解。

例子 5.34. K 是有限域，L/K 是 n-次有限扩张，$q = |K|$。范数映射 $\mathrm{N}_{L/K} : L^\times \to K^\times$ 是群同态，我们来计算 $\left|\mathrm{Ker}(\mathrm{N}_{L/K})\right|$，即范数为 1 的元素的个数。有限域的扩张是循环扩张，其生成元为 Frobenius 同态 Frob。根据 Hilbert 90，我们知道

$$\left|\mathrm{Ker}(\mathrm{N}_{L/K})\right| = \left\{\frac{\mathrm{Frob}(x)}{x} \middle| x \in L^\times\right\} = \mathrm{Im}(\psi),$$

其中，群同态 ψ 定义为：

$$\psi : L^\times \to L^\times,\ x \mapsto \frac{\mathrm{Frob}(x)}{x}.$$

从而，

$$\left|\mathrm{Ker}(\mathrm{N}_{L/K})\right| = \frac{|L^\times|}{\left|\mathrm{Ker}(\psi)\right|}.$$

根据定义，

$$\mathrm{Ker}(\psi) = \left\{x \in L^\times \middle| \mathrm{Frob}(x) = x\right\} = K^\times.$$

所以，

$$\left|\mathrm{Ker}(\mathrm{N}_{L/K})\right| = \frac{|L^\times|}{\left|K^\times\right|} = \frac{q^n - 1}{q - 1}.$$

特别地，这个计算表明 $\mathrm{N}_{L/K} : L^\times \to K^\times$ 是满同态，请参考例子5.27。

例子 5.35 (Hilbert 90 与 Galois 下降)**.** 给定有限 Galois 扩张 L/K，那么，$\mathbf{Gal}(L/K)$ 可以自然地作用在射影空间 $\mathbf{P}^n(L)$ 上。实际上，对任意的 $[x_0 : x_1 : \cdots : x_n] \in \mathbf{P}^n(L)$ 和 $g \in \mathbf{Gal}(L/K)$，我们定义

$$g[x_0 : x_1 : \cdots : x_n] = [g(x_0) : g(x_1) : \cdots : g(x_n)].$$

这个定义显然不依赖于 $\mathbf{P}^n(L)$ 点的齐次坐标的选取。

另外，$\mathbf{P}^n(K)$ 可以自然地被视作是 $\mathbf{P}^n(L)$ 的子集：

$$\mathbf{P}^n(K) \hookrightarrow \mathbf{P}^n(L),\ [x_0 : x_1 : \cdots : x_n] \mapsto [x_0 : x_1 : \cdots : x_n],$$

其中，$x_0, \cdots, x_n \in K$。那么，我们有

$$\mathbf{P}^n(L)^{\mathbf{Gal}(L/K)} = \mathbf{P}^n(K),$$

其中，$\mathbf{P}^n(L)^{\mathbf{Gal}(L/K)} = \{p \in \mathbf{P}^n(L) | g \cdot p = p, \text{ 对任意 } g \in \mathbf{Gal}(L/K)\}$。

我们现在直接证明上述论断。考虑如下交换图：

$$\begin{array}{ccc} K^{n+1} & \xrightarrow{\subset} & L^{n+1} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathbf{P}^n(K) & \xrightarrow{\subset} & \mathbf{P}^n(L) \end{array}$$

不难看出，以上映射与 Galois 群 $\mathbf{Gal}(L/K)$ 的作用相符，即每个箭头对对应着 G-作用的态射，请参考定义3.6。对任意的 $p \in \mathbf{P}^n(L)^{\mathbf{Gal}(L/K)}$，$\pi^{-1}(p)$ 是 $\mathbf{P}^n(L)$ 中的 1 维线性子空间并且在 $\mathbf{Gal}(L/K)$ 的作用下不变。根据命题115，存在 $(x_0, \cdots, x_n) \in L^{n+1}$，使得 $(x_0, \cdots, x_n)$ 张成 $\pi^{-1}(p)$ 并且 $x_0, \cdots, x_n \in K$。这表明，$p = [x_0 : x_1 : \cdots : x_n] \in \mathbf{P}^n(K)$。

我们还可以用 Hilbert 90 的一般形式证明 $\mathbf{P}^n(L)^{\mathbf{Gal}(L/K)} = \mathbf{P}^n(K)$：给定 $p \in \mathbf{P}^n(L)^{\mathbf{Gal}(L/K)}$，任选非零的 $(x_0, \cdots, x_n) \in \pi^{-1}(p) \subset L^{n+1}$。按定义，对任意 $g \in \mathbf{Gal}(L/K)$，$g(x_0, \cdots, x_n) \in \pi^{-1}(p)$，所以存在函数

$$f : \mathbf{Gal}(L/K) \to \mathbf{Gal}(L/K),$$

使得

$$g(x_0, \cdots, x_n) = \big(g(x_0), \cdots, g(x_n)\big) = \big(f(g) \cdot x_0, \cdots, f(g) \cdot x_n\big).$$

对任意的 $g, h \in \mathbf{Gal}(L/K)$，我们计算 $f(gh)$：

$$\begin{aligned} f(gh)(x_0, \cdots, x_n) &= (g \cdot h)(x_0, \cdots, x_n) = g\big(h(x_0, \cdots, x_n)\big) \\ &= g\big(f(h) \cdot x_0, \cdots, f(h) \cdot x_n\big) = \Big(g\big(f(h) \cdot x_0\big), \cdots, g\big(f(h) \cdot x_n\big)\Big) \\ &= \Big(g\big(f(h)\big) \cdot g(x_0), \cdots, g\big(f(h)\big) \cdot g(x_n)\Big) = g\big(f(h)\big)\big(g(x_0), \cdots, g(x_n)\big) \\ &= g\big(f(h)\big) f(g)\big(x_0, \cdots, x_n\big). \end{aligned}$$

所以，$f(gh) = g\big(f(h)\big) f(g)$。根据 Hilbert 90 的一般形式，存在 $x \in L^\times$，使得 $f(g) = \frac{x}{g(x)}$,。从而，

$$g(x_0, \cdots, x_n) = (\frac{xx_0}{g(x)}, \cdots, \frac{xx_n}{g(x)}),$$

即 $g(x_i) = \frac{xx_i}{g(x)}$，从而对任意的 $g \in \mathbf{Gal}(L/K)$，$g(x \cdot x_i) = x \cdot x_i$。所以，$x \cdot x_i \in K$。我们只要选取如下 p 的如下齐次坐标即可：

$$p = [x \cdot x_0 : x \cdot x_1 : \cdots : x \cdot x_n].$$

定理 125 (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；[46]

2) 存在 $a \in K$，对任意的 $d > 1, d \mid n$，$a \notin K^d$，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 是该多项式的某个根。

证明: 首先证明 1)⇒2)。

[46]按定义，循环扩张是 Galois 扩张。

令 σ 为 $\mathbf{Gal}(L/K)$ 的某个生成元，ξ 为 K 中的某个 n-次本原单位根。由于 $\mathrm{N}_{L/K}(\xi^{-1})=1$，根据 Hilbert 90，存在 $\alpha\in L$，使得 $\xi^{-1}=\frac{\alpha}{\sigma(\alpha)}$，从而，

$$\sigma(\alpha)=\xi\cdot\alpha,\ \ \sigma^k(\alpha)=\xi^k\cdot\alpha,\ k=0,1,\cdots,n-1.$$

特别地，由于 ξ 是本原的，所以，以上 $\{\sigma^k(\alpha)|k=0,\cdots,n-1\}$ 两两不同。以上等式应该被视作是 $\mathbf{Gal}(L/K)$ 在根上的作用。此时，

$$P(X)=\prod_{k=0}^{n-1}(X-\sigma^k(\alpha))\in K[X]$$

是 α 的极小多项式，从而是不可约的。特别地，$[K(\alpha):K]=\deg(P)=n$，所以 $L=K(\alpha)$。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，$1<d\mid K$。否则，$b^d=a$，其中 $b\in K$。从而，

$$P(X)=\left(X^{\frac{n}{d}}\right)^d-b^d=(X^{\frac{n}{d}}-b)Q(X)$$

是可约的，矛盾。

其次证明 2)⇒1)。

假设存在 $a\in K$，对任意 $d>1,d\mid n$，$a\notin K^d$，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，根据 $|\mu_n(K)|=n$，则 X^n-a 的所有根恰为是 $\{\alpha,\xi\alpha,\cdots,\xi^{n-1}\alpha\}$ 并且该集合中的元素两两不同，其中 ξ 是 K 中的 n-次本原单位根。这表明 X^n-a 可分，所以 L/K 是可分扩张。综合上述，L/K 是 Galois 扩张。另外，考虑 $\mathbf{Gal}(L/K)$ 在以上多项式的根上的作用，我们得到单的群同态：

$$\mathbf{Gal}(L/K)\longrightarrow\mu_n(K),\ \ g\mapsto\zeta_g,\ \ \text{其中 } g(\alpha)=\zeta_g\alpha.$$

所以，$\mathbf{Gal}(L/K)$ 是循环群。以下证明

$$X^n-a=\prod_{k=0}^{n-1}(X-\xi^k\alpha)$$

是不可约的。如果这一点成立，由于 $\mathbf{Gal}(L/K)$ 在根上的作用传递，通过考虑元素个数，我们就有 $\mathbf{Gal}(L/K)\simeq\mu_n(K)$ 是 n 阶循环群。假设 $Q\mid P$ 并且是首一的多项式，则 $Q(X)=(X-\xi^{i_1}\alpha)\cdots(X-\xi^{i_m}\alpha)$，其中，$1\leqslant m<n$。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 $d=(n,m)<n$，有 $\alpha^d\in K$。此时，$d\mid n$。所以，$a=\alpha^n=\left(\alpha^d\right)^{\frac{n}{d}}\in K^{\frac{n}{d}}$，与所给假设相抵触。 □

例子 5.36. K 为域，$P(X)=X^n-a\in K[X]$，$n\geqslant 2$，$a\in K^\times$，L 为 P 的分裂域。令 $\xi\in\mu_n(\overline{K})$ 为 n-次本原单位根。我们未必有 $\xi\in K$ 但是 $\xi\in L$。

现在证明 $\mathbf{Gal}(L/K)$ 是 $\mathbf{Aff}_1\left(\mathbb{Z}/n\mathbb{Z}\right)$ 的子群，其中，

$$\mathbf{Aff}_1\left(\mathbb{Z}/n\mathbb{Z}\right)=\left\{g_{u,b}:x\mapsto ux+b\middle|u\in\left(\mathbb{Z}/n\mathbb{Z}\right)^\times,b\in\mathbb{Z}/n\mathbb{Z}\right\}.$$

请参考例子3.8。

任选 α 为 P 在 L 中的根，则对任意的 $g \in \mathbf{Gal}(L/K)$，存在唯一的 $u \in \left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$ 和 $b \in \mathbb{Z}/n\mathbb{Z}\}$，使得

$$g(\xi) = \xi^u, \quad g(\alpha) = \xi^b \cdot \alpha.$$

那么，$g \mapsto g_{u,b}$ 给出了单的群同态：

$$\mathbf{Gal}(L/K) \hookrightarrow \mathbf{Aff}_1\left(\mathbb{Z}/n\mathbb{Z}\right).$$

给定素数 p，当 $K = \mathbb{Q}, a \notin \mathbb{Q}^p$ 时，易见 $[L : K] = p(p-1)$ 而 $\left|\mathbf{Aff}_1\left(\mathbb{F}_p\right)\right| = p(p-1)$，此时，

$$\mathbf{Gal}(L/\mathbb{Q}) \xrightarrow{\simeq} \mathbf{Aff}_1\left(\mathbb{F}_p\right).$$

特别地，$\mathbf{Aff}_1\left(\mathbb{F}_p\right)$ 可以实现为数域的 Galois 群。

5.7 群论的补充：可解群

5.7.1 滤链

定义 5.12. G 是群。假设 G 的子群序列 $(G_i)_{0\leqslant i\leqslant n}$ 满足

$$1 = G_n \lhd G_{n-1} \lhd G_{n-2} \lhd \cdots \lhd G_1 \lhd G_0 = G, \tag{5.2}$$

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 $\left(\mathrm{gr}_i(G) = G_i/G_{i+1}\right)_{i\leqslant n-1}$ 称作是该滤链的**分次化**并记作 $\mathrm{gr}(G)$，其中，每个 $\mathrm{gr}_i(G)$ 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**。

注记 5.54. 我们强调，以上定义中仅要求 $G_i \lhd G_{i-1}$ 而 G_i 可能在 G_{i-2} 中不再是正规子群，其中，$i = 1, \cdots, n-1$。

注记 5.55. 给定子群 $H < G$，我们定义

$$H_i = G_i \cap H.$$

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

注记 5.56. 给定正规子群 $N \lhd G$，那么，$G_i \cap N \lhd G_i$。令

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

由于 $G_i \lhd G_{i-1}$，根据练习题2.7.5一节中的子群对应定理，$\left(G/N\right)_i \lhd \left(G/N\right)_{i-1}$。这表明，滤链 (G_i) 诱导出商群 G/N 上的滤链 $\left(G/N\right)_i$。

注记 5.57. 给定群同态的正合列

$$1 \to N \to G \to G/N \to 1.$$

根据以上两个注记，我们有

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

也就是说

$$1 \to \mathrm{gr}_i(N) \to \mathrm{gr}_i(G) \to \mathrm{gr}_i\left(G/N\right) \to 1. \tag{5.3}$$

定义 5.13. 给定群 G 的滤链 $(G_i)_{0\leqslant i\leqslant n}$，如果每个 $\mathrm{gr}_i(G)$ 都是单群，其中，$0\leqslant i\leqslant n-1$，我们就称这个滤链为 **Jordan-Hölder 滤链**。

命题 126. *有限群 G 必有 Jordan-Hölder 滤链。*

证明： 如果 $G=1$，我们在(5.2)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，G/N 为单群。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 $(G,N_0,N_1,\cdots)$ 作为 G 的 Jordan-Hölder 滤链。证毕。 □

注记 5.58. 无限群未必有 Jordan-Hölder 滤链。

实际上，$\mathbb{Z}$ 没有 Jordan-Hölder 滤链。因为它的每个有限指标的子群都同构于 $\mathbb{Z}$，所以其 Jordan-Hölder 滤链不会在有限步停止。

定理 127 (Jordan-Hölder)**.** *任意给定群 G 的 Jordan-Hölder 滤链 $(G_i)_{0\leqslant i\leqslant n}$，其因子群的集合 $\{\mathrm{gr}_i(G)\}$（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，则约定其长度为 ∞。*

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

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

$$1\to N\to G\to G/N\to 1,$$

以及滤链对此整合列所诱导的滤链的整合列(5.3)。由于 (G_i) 为 Jordan-Hölder 滤链，所以，$\mathrm{gr}_i(G)$ 均为单群，其正规子群 $\mathrm{gr}_i(N)$ 只能是 1 或 $\mathrm{gr}_i(G)$。据此，我们可以把集合 $I=\{0,\cdots,n-1\}$ 分划为两部分

$$I_1=\big\{i\big|\mathrm{gr}_i(N)=\mathrm{gr}_i(G)\big\},\ I_2=\big\{i\big|\mathrm{gr}_i(N)=1\big\}.$$

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 $n\big(N,(N_i)_{i\in I_1},S\big)$ 和 $n\big(G/N,\big(G/N\big)_{i\in I_2},S\big)$ 与滤链的选取无关。又因为

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

所以，$n(G,(G_i),S)$ 也与滤链的选取无关。 □

推论 128. *对任意的正规子群 $N\lhd G$，我们有*

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

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 $\ell(G)=\ell(N)+\ell\big(G/N\big)$ 仍然成立。 □

例子 5.37. 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。

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：

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

作为因子群，$\mathbb{Z}/n\mathbb{Z}$ 在 $\mathrm{gr}G$ 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。

例子 5.38. （$\mathfrak{S}_3$ 的滤链）$\mathfrak{A}_3 \lhd \mathfrak{S}_3$ 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：

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

这个滤链的长度为 2，其因子群为 2 阶和 3 阶的循环群。

例子 5.39. （$\mathfrak{S}_4$ 的滤链）$\mathfrak{A}_3 \lhd \mathfrak{S}_3$ 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，$D \lhd \mathfrak{A}_4$ 是正规子群。对每个 i，我们都有如下的 Jordan-Hölder 滤链：

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

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。

例子 5.40. （$\mathfrak{S}_n$ 的滤链，$n \geqslant 5$）根据习题3.6.2，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，所以 $\mathfrak{S}_n$ 只有有唯一一个 Jordan-Hölder 滤链：

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

该滤链的因子群分别为 $\mathfrak{A}_n$ 和 2 阶循环群。

5.7.2 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[47]

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

$H < G$ 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 $\mathbf{D}(G)$。

注记 5.59. $\mathbf{D}(G) \lhd G$ 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（不仅是内同构）$\varphi \in \mathrm{Aut}(G)$，$\varphi\big(\mathbf{D}(G)\big) = \mathbf{D}(G)$。

命题 129. *$H < G$ 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。

[47]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。

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，$H \lhd G$。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。 □

注记 5.60. 要得到 G 的一个交换的商群，以上命题表明至少要商掉 $\mathbf{D}(G)$。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 $G \to G^{\mathrm{ab}}$ 上去，这可以用如下的交换图来表示：

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & A \\ \downarrow & \nearrow_{\overline{\varphi}} & \\ G^{\mathrm{ab}} & & \end{array}$$

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

例子 5.41. 假设 $n \geqslant 2$，那么，$\mathfrak{S}_n^{\mathrm{ab}} \simeq \mathbb{Z}/2\mathbb{Z}$。

$n = 2$ 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，$\mathbf{D}(\mathfrak{S}_n) \lhd \mathfrak{A}_n$。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 $i, j, k \leqslant n$，我们有

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

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，

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

例子 5.42. $n \geqslant 2$，K 是域，$G = \mathbf{GL}(n; K)$，则 $\mathbf{D}(G) = \mathbf{SL}(n; K)$。这是线性代数中的一个经典结论。很明显，$\mathbf{D}\big(\mathbf{GL}(n; K)\big) < \mathbf{SL}(n; K)$。我们证明反过来的包含关系。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，则有如下经典公式：

$$e_{ij} \cdot e_{kl} = \delta_{jk} e_{il}, \tag{5.4}$$

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(5.4)，我们有

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

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 $\lambda \in K$，$E_{ij}(\lambda) \in \mathbf{D}\big(\mathbf{GL}(n; K)\big)$（实际上，我们证明了 $E_{ij}(\lambda) \in \mathbf{D}\big(\mathbf{SL}(n; K)\big)$）。

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

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

然后计算下面乘积的非对角线项：

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

我们令以上两个系数为 0，这就给出了如下待定的方程：

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

这等价于

$$\begin{cases}\beta+\nu+\beta\mu\nu=0,\\ \alpha+\mu+\alpha\beta\mu+\lambda+\mu\nu\lambda=0.\end{cases}\tag{5.5}$$

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，(5.5)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

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

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 $1+\nu\neq0$（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，$D\in\mathbf{D}\big(\mathbf{SL}(n;K)\big)$。

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 $A\in\mathbf{D}\big(\mathbf{SL}(n;K)\big)$。

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

注记 5.61. 以上证明实际给出了 $\mathbf{D}\big(\mathbf{SL}(n;K)\big)=\mathbf{SL}(n;K)$。

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

$$\mathbf{D}^0G=G,\ \mathbf{D}^1G=\mathbf{D}G,\ \mathbf{D}^nG=\mathbf{D}(\mathbf{D}^{n-1}G)=(\mathbf{D}^{n-1}G,\mathbf{D}^{n-1}G),\ n\geqslant1.$$

我们显然有

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

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

$$\mathbf{D}^\infty G=\bigcap_{n\geqslant1}\mathbf{D}^nG.$$

定义 5.14. 如果存在正整数 n，使得 $\mathbf{D}^n G = 1$，我们就称 G 为**可解群**[48]。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**。

注记 5.62. 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 $d\ell(H) \leqslant d\ell(G)$；对于商群 G/N 而言，我们有满射 $G \to G/N$，那么，$\mathbf{D}G \to \mathbf{D}\left(G/N\right)$ 也是满射，从而，$1 = \mathbf{D}^n G \to \mathbf{D}^n\left(G/N\right)$ 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。

命题 130. *G 是群，$N \lhd G$ 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*

$$d\ell(G) \leqslant d\ell(N) + d\ell\left(G/N\right).$$

证明： 令 $i = d\ell(N)$，$j = d\ell\left(G/N\right)$。那么，$\mathbf{D}^j G \subset N$，$\mathbf{D}^i N = 1$。所以，$\mathbf{D}^{i+j} G = \mathbf{D}^i(\mathbf{D}^j G) = 1$。 □

注记 5.63. $d\ell(G) = 0$ 等价于 G 是平凡群；$d\ell(G) \leqslant 1$ 等价于 G 是交换群。特别地，交换群是可解群。

注记 5.64. 有两个关于可解群的大定理，它们的证明困难，但其叙述简洁。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 131. *给定群 G 和正整数 n, 如下命题等价*

(1) G 是可解群并且 $d\ell(G) \leqslant n$。

(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 $0 \leqslant i \leqslant n-1$。

(2') G 有滤链 $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = 1$，使得 G_{i+1} 是 G_i 的正规子群并且 G_i/G_{i+1} 交换，其中 $0 \leqslant i \leqslant n-1$。

(3) G 有交换的特征子群 A，使得 G/A 可解并且 $d\ell\left(G/A\right) \leqslant n-1$。

证明： (1)⇒(2)：取 $G_i = \mathbf{D}^i G$；(2)⇒(2')：显然；(2')⇒(1)：根据命题 129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)⇒(3)：取 $A = \mathbf{D}^{n-1} G$，由于 $\mathbf{D}A = 1$，所以，A 是交换群。另外，$\mathbf{D}^{n-1}\left(G/A\right) \subset \mathbf{D}^{n-1} G/A = 1$。

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

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

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

推论 132 (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 $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = 1$，使得 G_{i+1} 是 G_i 的正规子群并且 G_i/G_{i+1} 交换，其中 $0 \leqslant i \leqslant n-1$。

(3) G 有滤链 $G = H_0 \rhd H_1 \rhd \cdots \rhd H_m = 1$，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 $0 \leqslant i \leqslant m-1$。

[48]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。

证明：只要证明 (2)⇒(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 $G_i \rhd G_i^1 \rhd G_i^2 \rhd \cdots \rhd G_i^l \rhd G_{i+1}$，使得

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

并且

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

是循环群。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 133 (有限可解群的另一个等价定义)**.** *G 是有限群，$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = 1$ 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 $0 \leqslant i \leqslant n-1$。*

证明：如果 G_i/G_{i+1} 为素数阶循环群，根据推论132中的 (3)，G 可解；反之，如果 G 可解，其商群与子群均可解，所以 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。 □

例子 5.43. 1) G 是非交换单群。那么，$\mathbf{D}(G) = G$，从而 G 不可解。据此，当 $n \geqslant 5$ 时，$\mathfrak{S}_n$ 不可解，因为它包含了 $\mathfrak{A}_n$ 这个不可解的子群。

2) 当 $n \leqslant 4$ 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：

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

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 $\dim_K(V_i) = n - i$，$i = 0, \cdots, n$。定义[49]

$$G = \big\{ s \in \mathbf{GL}(V) \big| s : V_i \to V_i, \ \ 0 \leqslant i \leqslant n \big\}.$$

以及其子群序列 $(B_i)_{0 \leqslant i \leqslant n}$：

$$B_i = \big\{ s \in G \big| (s-1)V_j \subset V_{i+j}, 0 \leqslant j \leqslant n-i \big\}.$$

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 $j + k \leqslant n$，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 $v \in V_{i+k}, w \in V_{i+j}$，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 $0 \leqslant i \leqslant n$，$(B_0, B_i) \subset B_i$，所以 B_i 是 $G = B_0$ 的正规子群。
- 对 $1 \leqslant i \leqslant n$，$(B_i, B_i) \subset B_{2i} \subset B_{i+1}$，所以 B_i/B_{i+1} 是交换群（$i \leqslant n-1$）。

据此，滤链 $(B_i)_{0 \leqslant i \leqslant n}$ 满足命题131的 (2)，所以 G 是可解群。

[49]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。

5.8 Galois 理论的经典应用

5.8.1 尺规作图

根据 Wantzel 的结论，即定理3，$x \in \mathbb{R}$ 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 $[K_i : K_{i-1}] = 2$ $(i = 1, \cdots, m)$ 并且 $x \in K_m$。通过添加 i 以及考虑 z 的实部和虚部，那么，$z \in \mathbb{C}$ 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 $[K_i : K_{i-1}] = 2$ $(i = 1, \cdots, m)$ 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 $\mathbb{Q}[X]/(P) \simeq \mathbb{Q}(z) \subset K_m$ 是 K_m 的子域，所以 $\deg(P)$ 是 2 的幂。

定理 134. *$z \in \mathbb{C}$ 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，L 为 $P(X)$ 在 $\mathbb{Q}$ 上的分裂域。那么，z 是尺规可作的当且仅当 $[L : K]$ 为 2 的幂。*

引理 135. *G 是 p-群，即 $|G| = p^n$，p 为素数，则存在滤链 $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = 1$，使得*

$$G_{i-1}/G_i \simeq \mathbb{Z}/p\mathbb{Z}, \quad i = 1, \cdots n.$$

证明: 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，根据命题19，G 的中心 $\mathrm{Z}(G)$ 非平凡，所以可以选取 $G_{n-1} < \mathrm{Z}(G)$，使得 $G_{n-1} \simeq \mathbb{Z}/p\mathbb{Z}$。我们还有 $G_{n-1} \lhd G$。那么，G/G_{n-1} 是阶为 p^{n-1} 群。根据归纳假设，存在 G 的子群 G_i，其中，$i = 1, \cdots, n-2$，使得

$$G/G_{n-1} \rhd G_1/G_{n-1} \rhd \ldots G_{n-2}/G_{n-1} \rhd 1,$$

并且

$$G_i/G_{i+1} \simeq \frac{G_i/G_{n-1}}{G_{i+1}/G_{n-1}} \simeq \mathbb{Z}/p\mathbb{Z}.$$

那么，$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = 1$ 为所求的滤链。 □

定理的证明. 假设 L 为 P 的分裂域，$z = z_1, \cdots, z_n$ 为 P 在 L 中所有的根。

如果 z 是尺规可作的，则有域扩张的序列

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

使得 $[K_i : K_{i-1}] = 2$ $(i = 1, \cdots, m)$ 并且 $z \in K_m$。选取 Galois 扩张 $M/\mathbb{Q}$，使得 $M \supset K_m \cup L$。由于 P 是不可约多项式，对每个根 z_j，存在 $g \in \mathbf{Gal}\left(M/\mathbb{Q}\right)$，使得 $g(z) = z_i$。实际上，由于 $L/\mathbb{Q}$ 是 Galois 扩张，所以存在 $\sigma \in \mathbf{Gal}\left(L/\mathbb{Q}\right)$，使得 $g(z) = z_i$。另外，$\mathbf{Gal}\left(L/\mathbb{Q}\right)$ 是 $\mathbf{Gal}\left(M/\mathbb{Q}\right)$ 的商群，所以以上陈述成立。

根据上面的讨论，对任意的 i，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 $[g(K_i) : g(K_{i-1})] = 2$ $(i = 1, \cdots, m)$ 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 $L = \mathbb{Q}(z_1, \cdots, z_n)$，所以 L 中的元素都是尺规可作的。

由于 $L/\mathbb{Q}$ 是有限可分扩张，根据本原元素定理，即推论108，存在 $\xi \in L$，使得 $L = \mathbb{Q}(\xi)$。由于 ξ 是尺规可作的，所以，ξ 落在 $\mathbb{Q}$ 的某个扩张 M' 中，其中，$[M' : \mathbb{Q}] = 2^m$ 而 $L = \mathbb{Q}(\xi) \subset M'$，所以，$[L : \mathbb{Q}]$ 为 2 的幂。

最后证明若 $[L : \mathbb{Q}] = 2^m$，那么，L 中的元素是是尺规可作的。此时，$\mathbf{Gal}(L/\mathbb{Q})$ 是 2-群。根据上一引理，存在滤链 $\mathbf{Gal}(L/\mathbb{Q}) = G_0 \rhd G_1 \rhd \cdots \rhd G_n = 1$，使得

$$G_{i-1}/G_i \simeq \mathbb{Z}/2\mathbb{Z}, \quad i = 1, \cdots n.$$

根据 Galois 对应，存在中间域 $\mathbb{Q} = M_0 \subset M_1 \subset \cdots \subset M_n = L$，使得 $[M_i : M_{i-1}] = 2$，其中，$i = 1, \cdots, n$。根据 Wantzel 的定理，每个 M_i 中的元素都是尺规可作的。 □

令 $F_m = 2^{2^m} + 1$，其中，$m = 1, 2, \cdots$。如果 F_m 是素数，就称之为 **Fermat 素数**。我们可以计算

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537.$$

前 4 个数是素数而 $641 \mid F_5$。

注记 5.65. 若 $2^n + 1$ 是素数，则 n 为 2 的幂。

实际上，可以假设 $n = 2^l m$，其中，m 是奇数。若 $m > 1$，则

$$2^n + 1 = \left(2^{2^l}\right)^m + 1 = (2^{2^l} + 1) \sum_{k=0}^{m-1} (-1)^k \left(2^{2^l}\right)^k$$

是合数。

定理 136. *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: 我们有两个基本的观察:

- 若正 n 边形可作，由于可以二等分已知角，从而正 $2n$ 边形也可作;
- 若可以做正 n 边形和正 m 边形，其中，n 和 m 互素，则可以做出正 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，

  $$e^{\frac{1}{mn}2\pi i} = e^{\frac{a}{m}2\pi i} \cdot e^{\frac{b}{n}2\pi i}$$

  也是尺规可作的。

根据这两个性质，只要对奇素数 p 证明如下两条即可:

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，其分裂域为 $\mathbb{Q}(e^{\frac{2\pi i}{p}})$ 并且 $[\mathbb{Q}(e^{\frac{2\pi i}{p}}) : \mathbb{Q}] = p - 1$。从而，正 p 边形尺规可作当且仅当 $p - 1$ 是 2 的幂，这也等价于 p 为 Fermat 素数。

另外，对于素数 $p > 2$，正 p^2 边形尺规可作当且仅当 $e^{\frac{2\pi i}{p^2}}$ 是尺规可作的，其在 $\mathbb{Q}$ 上的分裂域的次数为 $\varphi(p^2) = p(p-1)$，这显然不是 2 的幂。所以正 p^2-边形不是尺规可作的。 □

例子 5.44. 我们考虑多项式 $P(X)=X^4+X^3-X^2-X+1$ 的根是否是尺规可作的，这等价于研究它在 $\mathbb{Q}$ 上的分裂域 $L/\mathbb{Q}$。

首先证明 $P(X)$ 是 $\mathbb{Q}[X]$ 上的不可约多项式。我们用 mod 2 的方法。在 $\mathbb{F}_2[X]$ 中，$P(X)$ 对应着多项式 $\overline{P}(X)=X^4+X^3+X^2+X+1$，它显然在 $\mathbb{F}_2$ 中没有根。反设 $P(X)$ 可约，则其根是某个二次不可约多项式的根，从而落在 $\mathbb{F}_4$ 中。令 $\mathbb{F}_4=\mathbb{F}_2(a)$，此时，$a$ 在 $\mathbb{F}_2$ 上的极小多项式为 X^2+X+1，则 $\mathbb{F}_4=\{0,1,a,a+1\}$。直接计算，可以给出 $\overline{P}(a)=a+1,\overline{P}(a+1)=a$，它们均非零，矛盾。所以，$\overline{P}$ 是不可约的，进而 P 在 $\mathbb{Q}[X]$ 中不可约。

由于 $P(X)$ 是实系数多项式，在 $\mathbb{C}[X]$ 中，它可以被写成

$$P(X)=(X^2+aX+b)(X^2+\overline{a}X+\overline{b}).$$

据此，

$$\begin{cases} a+\overline{a}=1, \\ a\overline{a}+b+\overline{b}=-1, \\ a\overline{b}+b\overline{a}=-1, \\ b\overline{b}=1. \end{cases}$$

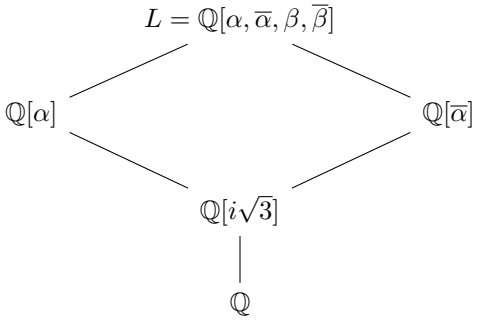
当 $b=\overline{b}=-1$ 时，第一个与第三个方程一样，此时可以解出 a，从而，

$$P(X)=(X^2+\frac{1+i\sqrt{3}}{2}X-1)(X^2+\frac{1-i\sqrt{3}}{2}X-1).$$

任意选取 α 为 $P(X)$ 的根。根据以上因式分解，$\frac{1+i\sqrt{3}}{2}$ 或 $\frac{1-i\sqrt{3}}{2}$ 在 $\mathbb{Q}(\alpha)$ 中，即 $i\sqrt{3}\in\mathbb{Q}(\alpha)$，从而，我们有域扩张

$$\mathbb{Q} \text{ —— } \mathbb{Q}(i\sqrt{3}) \text{ —— } \mathbb{Q}(\alpha)$$

不妨假设 α 是 $X^2+\frac{1+i\sqrt{3}}{2}X-1$ 的根而另一个根是 $\beta=\alpha^{-1}$，则 $X^2+\frac{1+i\sqrt{3}}{2}X-1$ 的根是 $\overline{\alpha}$ 和 $\overline{\beta}$。此时，我们有域扩张的图表：



以上每个相邻中间域的扩张次数均为 2，所以 $[L:\mathbb{Q}]=8$。这表明 $P(X)$ 的所有根都是尺规可作的。

以下我们计算 $\mathbf{Gal}(L/\mathbb{Q})$。由于 $P(X)$ 不可约，所以 $\mathbf{Gal}(L/\mathbb{Q})$ 在根 $\{\alpha,\beta,\overline{\alpha},\overline{\beta}\}$ 上的作用是传递的。受此启发，先考虑如下群论的问题：

注记 5.66. 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，$4\,||H|$ 并且 $|H|\,|\,24$，所以，$|H|=4,8,12$ 或者 24。

- $|H|=24$，则 $H=\mathfrak{S}_4$。

- $|H|=12$，则 $H=\mathfrak{A}_4$。

  实际上，该群的指标为 2，从而 $H\lhd\mathfrak{S}_4$。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，通过共轭可以假设 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 群只能是 $\mathfrak{D}_4$。

5.8.2 多项式的根式解

在这一节中，为了避免过多的技术负担，我们只讨论特征为 0 的域。假设 K 为特征零的域，$P\in K[X]$，如果 P 在 $\overline{K}$ 的每个根都可以通过有限步如下的操作得到：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 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，这可以用域的语言来表达：

定义 5.15. 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 $i=1,\cdots,m$，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 $x_i^{d_i}\in K_{i-1}$，就称 L/K 是**根式扩张**。换而言之，L 是通过对 K 添加有限个 d_i 次方根得到的。

对于多项式 $P(X)\in K[X]$，若存在根式扩张 L/K，使得 P 在 L 中分裂，则称$P(X)$ **在 K 上有根式解**。

注记 5.67. 给定域扩张 L/K 及中间域 $K\subset M\subset L$，若 L/M 和 M/K 是根式扩张，则 L/K 也是。

引理 137 (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 $\overline{K}$ 中的正规闭包 N 也是 K 的根式扩张。*

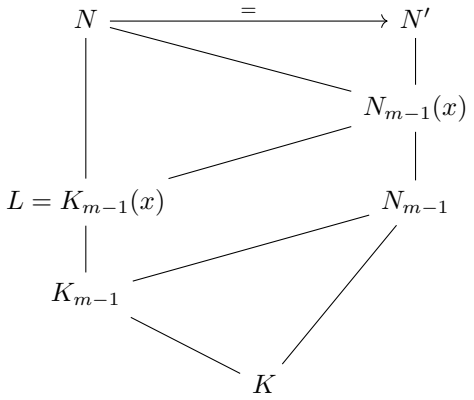
注记 5.68. L 由 K 添加上 $P(X)\in K[X]$ 的某些根生成。现在把 $P(X)$ 的所有根都添到 K 中就得到了 L 在 $\overline{K}$ 中的正规闭包 N。

证明： L/K 是根式扩张，所以存在中间域的序列：

$$K=K_0\subset K_1\subset\cdots\subset K_m=L$$

使得对任意的 $i=1,\cdots,m$，存在 $x_i\in K_i$ 以及正整数 d_i，$K_i=K_{i-1}(x_i)$ 并且 $x_i^{d_i}\in K_{i-1}$。对 m 进行归纳

来证明该命题，其中 $m=0$ 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 $\overline{K}$ 中的正规闭包；令 N 为 $K_m=L$ 在 $\overline{K}$ 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 $x_1,\cdots,x_l$。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 138 (Galois)**.** *域 K 的特征为零，L/K 是有限的 Galois 扩张，则如下等价：*

1) 存在 K 的根式扩张 M，使得 $K\subset L\subset M$；

2) $\mathbf{Gal}(L/K)$ *是可解群。*

我们首先做一些准备工作：

注记 5.69. 在研究 Kummer 理论时，我们有如下结论：K 是域并且 $|\mu_n(K)|=n$，L 是 X^n-a 在 K 上的分裂域，则 $\mathbf{Gal}(L/K)$ 是 $\mu_n(K)$ 的子群，它通过

$$\mathbf{Gal}(L/K)\longrightarrow\mu_n(K),\quad g\mapsto\zeta_g,\quad \text{其中 } g(\alpha)=\zeta_g\alpha.$$

来实现。

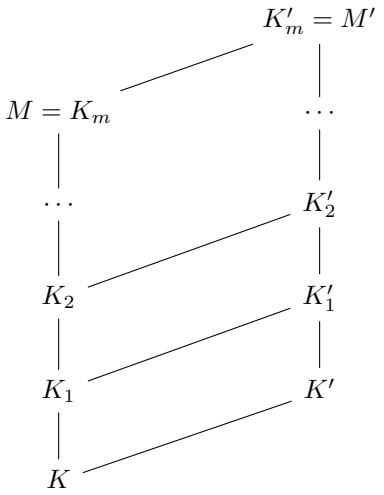
注记 5.70. 以下我们主要用到如下关于可解群的性质：可解群的子群和商群都是可解的；对于群 G 及其正规子群 $N\lhd G$，若 N 和 G/N 可解，则 G 可解。另外，对有限群 G 而言，可解等价于以下任何一条：

- G 有滤链 $G=G_0\rhd G_1\rhd\cdots\rhd G_n=1$，使得 G_{i+1} 是 G_i 的正规子群并且 G_i/G_{i+1} 交换，其中 $0\leqslant i\leqslant n-1$。
- G 有滤链 $G=H_0\rhd H_1\rhd\cdots\rhd H_m=1$，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 $0\leqslant i\leqslant m-1$。

证明： 1)⇒2)。根据上述技术性引理，选取 M' 为 M 在 $\overline{K}$ 中的正规闭包，那么，M'/K 也是根式扩张。通过把 M 替换为 M'，我们不妨假设 M/K 是根式扩张也是 Galois 扩张。因为 $\mathbf{Gal}(L/K)$ 为 $\mathbf{Gal}(M/K)$ 的商群，只要证明 $\mathbf{Gal}(M/K)$ 是可解群即可。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 $x_i^{d_i} \in K_{i-1}$，$1 \leqslant i \leqslant m$。为了应用 Kummer 理论的想法，令 K_i' 为 K_i 上在 $\overline{K}$ 中）添加上 $X^{d_1 d_2 \cdots d_m} - 1$ 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，这因为 $M = K_m$ 是 K 上某个多项式 $P(X)$ 的分裂域，所以 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：

$$1 \to \mathbf{Gal}(M'/K') \to \mathbf{Gal}(M'/K) \to \mathbf{Gal}(K'/K) \to 1.$$

根据分圆域的理论，$\mathbf{Gal}(K'/K)$ 是交换群从而是可解的。所以，只要证明 $\mathbf{Gal}(M'/K')$ 是可解群即可。

通过以上讨论，我们不妨设 K 中含所有 $d_1 d_2 \cdots d_m$ 次单位根。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 $\mathbf{Gal}(M/K_i)$ 是 $\mathbf{Gal}(M/K_{i-1})$ 的正规子群。如果令 $G_i = \mathbf{Gal}(M/K_i)$，我们就得到滤链：

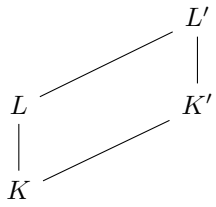
$$G_0 \rhd G_1 \rhd \cdots G_{m-1} \rhd 1,$$

并且

$$G_{i-1}/G_i = \mathbf{Gal}(M/K_{i-1})/\mathbf{Gal}(M/K_i) \simeq \mathbf{Gal}(K_i/K_{i-1})$$

是循环群。从而，$G_0 = \mathbf{Gal}(M/K)$ 是可解群。

2)⇒1)。假设 $\mathbf{Gal}(L/K)$ 可解，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 $[L : K]!$ 次的所有单位根所得到的域，即



类似于前面的讨论，L'/K 是 Galois 扩张。另外，L/K 是 Galois 扩张，从而，$\mathbf{Gal}(L'/L) \lhd \mathbf{Gal}(L'/K)$。另外，分圆扩张 L'/L 是 Abel 扩张而 $\mathbf{Gal}(L/K)$ 是可解群，从而 $\mathbf{Gal}(L'/K)$ 是可解群，所以其子群 $\mathbf{Gal}(L'/K')$ 也是可解群。另外，$[L' : K'] \leqslant [L : K]$：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 $\deg(P)$。此时，K' 包含了所有有 $[L' : K']!$ 次单位根。由于 K' 为 K 添加了一个本原单位根，所以 K'/K 是根式扩张。于是，只要对 L'/K' 证明即可。

综上所述，我们不妨设 K 包含了所有的 $[L : K]!$ 次单位根。由于 $\mathbf{Gal}(L/K)$ 可解，所以存在滤链

$$\mathbf{Gal}(L/K) = G_0 \rhd G_1 \rhd \cdots G_{m-1} \rhd G_m = 1,$$

使得 G_{i-1}/G_i 是循环群，其中，$i = 1, 2, \cdots, m$。令 $K_i = L^{G_i}$，根据 Galois 对应，我们有域扩张的序列：

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = L,$$

由于 $G_1 \lhd G_0$，所以，K_1/K_0 是 Galois 扩张；由于 $G_2 \lhd G_1$，所以，K_2/K_1 是 Galois 扩张；以此类推，K_i/K_{i-1} 为 Galois 扩张，其 Galois 群为 $[K_i : K_{i-1}]$ 阶循环群。由于 $[K_i : K_{i-1}] \mid [L : K]$，$K_{i-1}$ 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 $x_i^{[K_i:K_{i-1}]} \in K_{i-1}$。所以，$L/K$ 是根式扩张。

至此，我们完整地证明了 Galois 的定理。 □

例子 5.45. 多项式 $X^5 - 6X + 3 \in \mathbb{Q}[X]$ 的分裂域的 Galois 群为 $\mathfrak{S}_5$。$\mathfrak{S}_5$ 是不可解群，所以 $X^5 - 6X + 3 = 0$ 在 $\mathbb{Q}$ 上不能通过根式求解。

例子 5.46 (三次方程)**.** 假设 $\mathrm{Char}(K) = 0$ 并且包含一个三次本原单位根 ξ，$P(X) = X^3 + aX + b \in K[X]$ 是不可约多项式，L 为 P 在 K 上的分裂域。$\alpha, \beta, \gamma \in L$ 为 P 的三个根。此时，$[L : K] = 3$ 或 6 而 $\mathbf{Gal}\left(L/K\right) \simeq \mathfrak{A}_3$ 或 $\mathfrak{S}_3$。

令 $H < G$ 为其唯一的 3 阶子群，$\sigma \in H$ 为其生成元并不妨假设 $\sigma(\alpha) = \beta, \sigma(\beta) = \gamma, \sigma(\gamma) = \alpha$。定义 Lagrange 解式

$$z = \alpha + \xi\beta + \xi^2\beta^3,\ z' = \alpha + \xi^2\beta + \xi\beta^3.$$

由于 $\sigma(z) = z, \sigma(z') = z'$，所以，$z, z' \in L^H$。

现在考虑 Galois 对应：

$$\begin{array}{ccc} L & \text{----------} & 1 \\ | & & \downarrow \\ L^H = K(\Delta) & \text{----------} & H \\ | & & \downarrow \\ K & \text{----------} & \mathbf{Gal}(L/K) \end{array}$$

那么，$[L^H : K] = 1$ 或 2。无论何种情形，我们都有 $L^H = K(\Delta)$，其中，

$$\Delta = (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma).$$

另外，对于 $P(X) = X^3 + aX + b$ 而言，

$$\mathrm{Disc}(P) = (-1)^{\frac{3(3-1)}{2}}\Delta^2 = 4a^3 + 27b^2.$$

所以，理论上 z^3, z'^3 可以用 $K(\sqrt{-4a^3 - 27b^2})$ 元素表达，所以可以用系数 a, b 的根式表达。通过开三次方，z, z' 用系数的根式表达，在与 $\alpha + \beta + \gamma = 0$ 联立，这就给出了求根公式。

我们现在给出具体的计算。根据

$$(\alpha^2\beta+\beta^2\gamma+\gamma^2\alpha)-(\alpha^2\gamma+\beta^2\alpha+\gamma^2\beta)=\Delta,$$
$$(\alpha^2\beta+\beta^2\gamma+\gamma^2\alpha)+(\alpha^2\gamma+\beta^2\alpha+\gamma^2\beta)=3b$$

我们可以计算

$$\begin{aligned}z^3&=\alpha^3+\beta^3+\gamma^3+3\xi(\alpha^2\beta+\beta^2\gamma+\gamma^2\alpha)+3\xi^2(\alpha^2\gamma+\beta^2\alpha+\gamma^2\beta)+6\alpha\beta\gamma\\&=\frac{3}{2}(\xi-\xi^2)\Delta-\frac{27}{2}b,\end{aligned}$$

以及

$$z'^3=-\frac{3}{2}(\xi-\xi^2)\Delta-\frac{27}{2}b.$$

进一步，

$$\begin{cases}3\alpha=\alpha+\beta+\gamma+z+z',\\3\beta=\alpha+\beta+\gamma+\xi^2z+\xi z',\\3\gamma=\alpha+\beta+\gamma+\xi z+\xi^2z'.\end{cases}$$

这就可以给出 Cardanno 的公式。

例子 5.47 (四次方程)**.** 假设 $\mathrm{Char}(K)=0$ 并且包含一个三次本原单位根 ξ，$P(X)=X^4+aX^2+bX+c\in K[X]$ 是不可约多项式，M 为 P 在 K 上的分裂域。$\alpha,\beta,\gamma,\delta\in M$ 为 P 的四个根。此时，$\mathbf{Gal}\left(L/K\right)<\mathfrak{S}_4$。

令 $H:=\{1,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$ 为 $\mathfrak{S}_4$ 中的双置换给出的 4 阶子群。我们有 $H\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$。考虑下述 Galois 对应：

$$\begin{array}{ccc}M & \text{----------} & 1\\ \big| & & \big\downarrow\\ L^{H\cap\mathbf{Gal}(L/K)} & \text{------} & H\cap\mathbf{Gal}\left(L/K\right)\\ \big| & & \big\downarrow\\ K & \text{----------} & \mathbf{Gal}(L/K)\end{array}$$

令 $u=(\alpha+\beta)(\gamma+\delta),v=(\alpha+\gamma)(\beta+\delta),w=(\alpha+\delta)(\beta+\gamma)$。问题的关键在于注意到 $u,v,w\in L^{H\cap\mathbf{Gal}(L/K)}$。此时，$[L:K]=2,3$ 或 6，所以，u,v,w 理论上是某个 3 次多项式的根，从而可以被解出来。实际上，根据对称性，我们计算

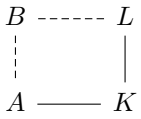
$$(X-u)(X-v)(X-w)=X^3-2aX^2+(a^2-4c)X+b^2\in K[X].$$

所以，我们可以利用 Cardanno 的结果来计算 u,v,w。另外，根据 $\alpha+\beta+\gamma+\delta=0$ 以及 $u=(\alpha+\beta)(\gamma+\delta)$，我们可以解出 $\alpha+\beta$ 和 $\gamma+\delta$；类似地，我们可以解出 $\{\alpha,\beta,\gamma,\delta\}$ 中任意两个数的和，从而解出所有的根。

5.9 mod p 的理论

5.9.1 代数整数环的有限性

我们现在利用5.3一节关于整扩张的概念来研究 mod p 约化的理论。我们回忆以下关于整扩张的图像：



A 是整环，$K=\mathrm{Frak}(A)$ 为其分式域，L/K 为代数扩张，B 为 A 在 L 中的整闭包。

注记 5.71. 根据命题89，对任意的 $x\in B$，其极小多项式 $P(X)\in A[X]$。我们回忆 $\mathrm{Tr}_{L/K}$ 和 $\mathrm{N}_{L/K}$ 的定义[50]。给定 $x\in L$，对乘法定义的线性映射：

$$m_x: L\longrightarrow L,\quad y\mapsto x\cdot y.$$

其迹、行列式和特征多项式给出了 $\mathrm{Tr}_{L/K}$ 和 $\mathrm{N}_{L/K}$：

$$\mathrm{Tr}_{L/K}(x)=\mathrm{Tr}(m_x),\ \mathrm{N}_{L/K}(x)=\det(m_x),\quad P_{L/K,x}(X)=\det(X\cdot I-m_x).$$

其中，

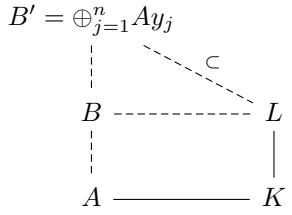
$$P_{L/K,x}(X)=P(X)^{[L:K(x)]}.$$

从而，$P_{L/K,x}(X)\in A[X]$。特别地，$\mathrm{Tr}_{L/K}(x),\mathrm{N}_{L/K}(x)\in A$。

命题 139 (有限性)**.** *假设 A 是整闭的 Noether 环，$K=\mathrm{Frak}(A)$，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，若 A 是主理想整环，则 B 是自由 A-模且其秩为 $[L:K]$。

证明: 作为 K-线性空间，我们可以选取 L 的一组基 $\{x_1,\cdots,x_n\}$，使得 $\{x_1,\cdots,x_n\}\subset B$。这是因为 $L=\left(A^\times\right)^{-1}B$。



由于 L/K 可分，非退化的双线性型

$$L\times L\longrightarrow K,\quad (x,y)\mapsto \mathrm{Tr}_{L/K}(x\cdot y),$$

给出 K-线性空间的同构：

$$L\longrightarrow L^*,\quad x\mapsto \left(y\mapsto \mathrm{Tr}_{L/K}(x\cdot y)\right).$$

据此，选取 $\{y_i\}_{1\leqslant i\leqslant n}\subset L$ 为 $\{x_1,\cdots,x_n\}$ 的对偶基，即

$$\mathrm{Tr}_{L/K}(x_i\cdot y_j)=\delta_i^j,\quad 1\leqslant i,j\leqslant n.$$

[50]参考作业5.11.1

定义 B 的对偶模:

$$B' = \{x \in L | \mathrm{Tr}_{L/K}(x \cdot x_j) \in A, 1 \leqslant j \leqslant n\}.$$

这显然是 A-模并且 $B \subset B'$。另外，对任意的 $x \in B'$，我们有

$$x = \sum_{j=1}^{n} \mathrm{Tr}_{L/K}(x \cdot x_j) y_j.$$

这表明 B' 是有限生成的 A-模，其中 $\{y_i\}_{1 \leqslant i \leqslant n}$ 是生成元。由于 A 是 Noether 环，所以 B' 是 Noether 模，进而其子模 B 是有限生成的。

若 A 是主理想整环，由于 $B \subset L$ 是无挠的，主理想整环上有限生成模的分类定理表明 B 是自由 A-模。再令 $B'' := \oplus_{j=i}^{n} A x_i$，则

$$B'' \subset B \subset B'.$$

由于 B'' 和 B' 都是秩为 $[L : K]$ 的自由模，所以 B 也是。 □

注记 5.72 (数域的扩张)**.** 考虑 $\mathbb{Q}$ 的有限扩张 K，令 $\mathcal{O}_K$ 为 K 的整数环；L 为 K 的有限扩张，$\mathcal{O}_L$ 为 $\mathcal{O}_K$ 在 L 中的整闭包。从而，$\mathcal{O}_L$ 也是 $\mathbb{Z}$ 在 L 中的整闭包，即 $\mathcal{O}_L$ 为 L 所对应的**代数整数环**。

$$\begin{array}{ccc} \mathcal{O}_L & \text{------} & L \\ \vdots & & | \\ \mathcal{O}_K & \text{------} & K \\ \vdots & & | \\ \mathbb{Z} & \text{———} & \mathbb{Q} \end{array}$$

根据以上命题，$\mathcal{O}_L$ 是秩为 $[L : \mathbb{Q}]$ 的自由交换群。

例子 5.48 ($\mathbb{Q}(e^{\frac{2\pi i}{p}})$ 的整数环，p 是素数)**.** 令 $\xi = e^{\frac{2\pi i}{p}}$，$L = \mathbb{Q}(e^{\frac{2\pi i}{p}})$，$\xi$ 在 $\mathbb{Q}$ 上的极小多项式为

$$X^{p-1} + \cdots + X + 1.$$

特别地，$\xi \in \mathcal{O}_L$ 并且 $\bigoplus_{j=0}^{p-2} \mathbb{Z} \cdot \xi^j \subset \mathcal{O}_L$。

容易看出，

$$\mathrm{Tr}_{L/\mathbb{Q}}(\xi^k) = \begin{cases} p, & k = 0; \\ -1, & 1 \leqslant k \leqslant p-1. \end{cases}$$

我们现在证明

$$\mathrm{N}_{L/\mathbb{Q}}(1 - \xi) = (-1)^{p-1} p.$$

我们可以利用 $1, \xi, \cdots, \xi^{p-2}$ 为 $L/\mathbb{Q}$ 的基对 m_ξ 所对应的矩阵直接计算行列式；也可以对 $1 - \xi$ 在 Galois 群作用下的像取乘积。根据

$$P(X) = X^{p-1} + \cdots + X + 1 = \frac{X^p - 1}{X - 1},$$

我们考虑

$$Q(X) = P(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \cdots + p.$$

那么，$\xi - 1$ 是 $Q(X)$ 的根，从而，

$$\mathrm{N}_{L/\mathbb{Q}}(\xi - 1) = \prod_{\sigma \in \mathbf{Gal}(L/\mathbb{Q})} \sigma(\xi - 1) = p.$$

特别地，上述计算给出

$$\mathrm{N}_{L/\mathbb{Q}}(\xi-1)=(-1)^{p-1}\prod_{k=1}^{p-1}(1-\xi^k)=(-1)^{p-1}p.$$

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 $\sigma\in\mathbf{Gal}(L/\mathbb{Q})$，$\sigma(x)\in\mathcal{O}_L$（它们满足同一个首一整系数多项式）。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，

$$\mathrm{Tr}_{L/\mathbb{Q}}\big(x\cdot(1-\xi)\big)=\sum_{\sigma\in\mathbf{Gal}(L/\mathbb{Q})}\sigma(x\cdot(1-\xi))\in\mathcal{O}_L\cdot(1-\xi).$$

另一方面，$\mathrm{Tr}_{L/\mathbb{Q}}\big(x\cdot(1-\xi)\big)\in\mathbb{Z}$。从而，

$$\mathrm{Tr}_{L/\mathbb{Q}}\big(x\cdot(1-\xi)\big)\in p\mathbb{Z},\quad\forall x\in\mathcal{O}_L.$$

假设 $x=a_0+a_1\xi+\cdots+a_{p-2}\xi^{p-2}\in\mathcal{O}_L$，其中，$a_0,\cdots,a_{p-2}\in\mathbb{Q}$。那么，

$$\begin{aligned}\mathrm{Tr}_{L/\mathbb{Q}}\big(x\cdot(1-\xi)\big)&=\mathrm{Tr}_{L/\mathbb{Q}}\big(a_0(1-\xi)+\sum_{i=1}^{p-2}a_i\xi^i-\sum_{i=1}^{p-2}a_i\xi^{i+1}\big)\\&=\mathrm{Tr}_{L/\mathbb{Q}}\big(a_0(1-\xi)\big)+\sum_{i=1}^{p-2}a_i\xi^i-\sum_{i=1}^{p-2}a_i\xi^{i+1}\\&=pa_0.\end{aligned}$$

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，

$$a_1+a_2\xi+\cdots+a_{p-2}\xi^{p-2}=(x-a_0)\cdot\xi^{-1}\in\mathcal{O}_L.$$

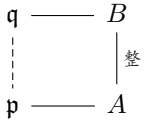
从而，$a_1\in\mathbb{Z}$。重复这个过程，我们得到 $a_i\in\mathbb{Z}$，$i=0,\cdots,p-2$。最终，我们证明

$$\mathcal{O}_{\mathbb{Q}(\xi)}=\mathbb{Z}[\xi],\quad\xi=e^{\frac{2\pi i}{p}}.$$

5.9.2 素理想与 Galois 群

我们研究 A 与其整扩张 B 的素理想之间的关联。我们不加证明的引用如下定理：

定理 140 (Cohen-Seidenberg)**.** 给定环的整扩张 $A\subset B$，$\mathfrak{p}\subset A$ 是素理想。



那么，存在素理想 $\mathfrak{q}\subset B$，使得 $\mathfrak{q}$ 在 $\mathfrak{p}$ 之上，即 $\mathfrak{q}\cap A=\mathfrak{p}$。

注记 5.73. Cohen-Seidenberg 定理的证明并不困难，自然的想法是对 $\mathfrak{p}$ 的局部化。这个证明与课程的主旨关联不大，所以略去。

注记 5.74. 在 Cohen-Seidenberg 定理中，$\mathfrak{p}$ 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 $a_0, \cdots, a_{n-1} \in A/\mathfrak{p}$，其中，$a_0 \neq 0$，使得

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \ \Rightarrow \ x \cdot a_0^{-1}(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) = 1.$$

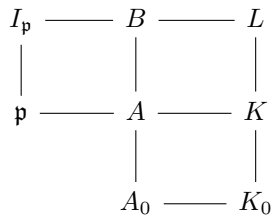
这说明 x 有逆，从而，$B/\mathfrak{q}$ 是域，所以，$\mathfrak{q}$ 是极大理想。

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 $a_0, \cdots, a_{n-1} \in A/\mathfrak{p}$，其中，$a_0 \neq 0$，使得

$$x^{-n} + a_{n-1}x^{1-n} + \cdots + a_1 x^{-1} + a_0 = 0 \ \Rightarrow \ x^{-1} = -\big(a_{n-1} + \cdots + a_1 x^{n-2} + a_0 x^{n-1}\big) \in A/\mathfrak{p}.$$

所以，$A/\mathfrak{p}$ 是域，即 $\mathfrak{p}$ 是极大理想。

假设 $K_0 = \mathbb{Q}$ 的有限扩张 K，令 A 为 $A_0 = \mathbb{Z}$ 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。[51]



令 $I_\mathfrak{p} = \{\mathfrak{q} \subset B | \mathfrak{q} \text{ 是素理想并且在 } \mathfrak{p} \text{ 之上}\}$。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

$$I_\mathfrak{p} = \{\mathfrak{q} \subset B | \mathfrak{q} \text{ 是素理想并且在 } \mathfrak{p} \text{ 之上}\} = \{\mathfrak{q} \supset \mathfrak{p} \cdot B | \mathfrak{q} \text{ 是素理想}\}.$$

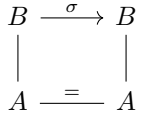
注记 5.75 (有限性)**.** 根据 A 和 B 是 Noether 环，我们可以证明 $I_\mathfrak{p}$ 为有限集。以下只对 L/K 是 Galois 扩张的情形证明此结果（据此也能推出一般的结论）。

定理 141. *A, B, K, L 和 $\mathfrak{p}$ 如上所述，进一步假设 L/K 是 Galois 扩张。那么，$\mathbf{Gal}(L/K)$ 可以传递地作用在 $I_\mathfrak{p}$ 上：*

$$\mathbf{Gal}(L/K) \times I_\mathfrak{p} \to I_\mathfrak{p}, \ \ (\sigma, \mathfrak{q}) \mapsto \sigma(\mathfrak{q}).$$

特别地，$|I_\mathfrak{p}| \leqslant |\mathbf{Gal}(L/K)|$。

注记 5.76 (Galois 群对素理想的作用)**.** 对于 $x \in B$，x 是 A-系数的首一多项式的根，所以对任意的 $\sigma \in \mathbf{Gal}(L/K)$，$\sigma(x)$ 也是该方程的根。从而，$\sigma(x) \in B$。这就给出了环同构：



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 $\sigma|_A = \mathrm{id}$，所以 $\mathfrak{q}$ 仍在 $\mathfrak{p}$ 之上。这就给出了定理中的群作用。

[51] 在函数域的情形，我们会考虑 $K_0 = \mathbb{F}_q(X)$。

证明: 现在证明 $\mathbf{Gal}(L/K)$ 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 $\mathfrak{q} \notin \{\sigma(\mathfrak{q}')|\sigma \in \mathbf{Gal}(L/K)\}$。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，

$$\pi : B \to B/\mathfrak{q} \times \prod_{\sigma\in\mathbf{Gal}(L/K)} B/\sigma(\mathfrak{q}')$$

是满射，从而，存在 $x \in B$，使得

$$\begin{cases} x \equiv 0 \mod \mathfrak{q}; \\ x \equiv 1 \mod \sigma(\mathfrak{q}'),\ \ \forall\, \sigma \in \mathbf{Gal}(L/K). \end{cases}$$

根据范数映射的定义及上面第一个同余式，$\mathrm{N}_{L/K}(x) \in \mathfrak{q} \cap A = \mathfrak{p}$；根据第二个同余式，对任意的 $\sigma \in \mathbf{Gal}(L/K)$，$\sigma(x) \equiv 1 \mod \mathfrak{q}'$，从而，$\mathrm{N}_{L/K}(x) = \prod_{\sigma\in\mathbf{Gal}(L/K)} \sigma(x) \notin \mathfrak{q}'$，特别地，$\mathrm{N}_{L/K}(x) \notin \mathfrak{q}' \cap A = \mathfrak{p}$，矛盾。 □

定义 5.16. 任意给定 $\mathfrak{q} \in I_{\mathfrak{p}}$，定义 $\mathfrak{q}$ 的**分解群**为以上作用在 $\mathfrak{q}$ 出的稳定化子：

$$\mathfrak{D}_{\mathfrak{q}} := \big\{\sigma \in \mathbf{Gal}(L/K)\big|\sigma(\mathfrak{q}) = \mathfrak{q}\big\}.$$

注记 5.77. 对其他 $g(\mathfrak{q}) \in I_{\mathfrak{p}}$，其中，$g \in \mathbf{Gal}(L/K)$，有

$$G_{g(\mathfrak{q})} = g\mathfrak{D}_{\mathfrak{q}}g^{-1}.$$

从而，每个 $\mathfrak{q} \in I_{\mathfrak{p}}$ 定义的分解群均同构。

给定 $\sigma \in \mathfrak{D}_{\mathfrak{q}}$，根据 $\sigma : B \to B$ 和 $\sigma : \mathfrak{q} \to \mathfrak{q}$，我们有域同构 $\overline{\sigma} : B/\mathfrak{q} \to B/\mathfrak{q}$。

$$\begin{array}{ccc} B & \xrightarrow{\ \sigma\ } & B \\ \downarrow & & \downarrow \\ B/\mathfrak{q} & \overset{\overline{\sigma}}{\dashrightarrow} & B/\mathfrak{q} \end{array}$$

另外，$\overline{\sigma} : A/\mathfrak{p} \to A/\mathfrak{p}$ 是单位映射 id。从而，

$$\begin{array}{ccc} B/\mathfrak{q} & \xrightarrow{\qquad\overline{\sigma}\qquad} & B/\mathfrak{q} \\ & \searrow \quad \swarrow & \\ & A/\mathfrak{p} & \end{array}$$

注记 5.78. 当 $A = \mathbb{Z}$ 且 $\mathfrak{p} = (p)$ 为素数 p 的素理想时，由于 B 为有限生成 $\mathbb{Z}$-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。

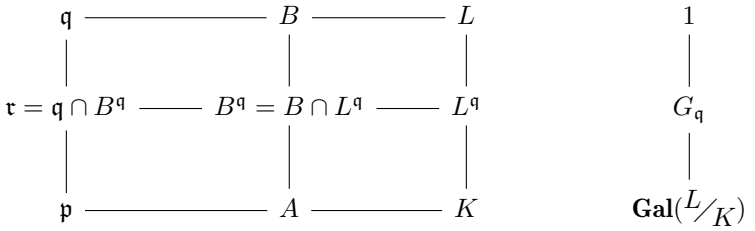
以上讨论给出了群同态

$$\mathrm{Res}_{\mathfrak{q}} : \mathfrak{D}_{\mathfrak{q}} \longrightarrow \mathbf{Gal}\big(^{B/\mathfrak{q}}/_{A/\mathfrak{p}}\big).$$

由于 $^{B}\!/_{\mathfrak{q}}/^{A}\!/_{\mathfrak{p}}$ 是有限域的有限扩张，$\mathbf{Gal}(^{B}\!/_{\mathfrak{q}}/^{A}\!/_{\mathfrak{p}})$ 是循环群。我们称以上同态的核 $\mathfrak{I}_{\mathfrak{q}}$ 为 $\mathfrak{q}$ 的**惯性群**：

$$\mathfrak{I}_{\mathfrak{q}} := \mathrm{Ker}\Big(\mathrm{Res}_{\mathfrak{q}} : \mathfrak{D}_{\mathfrak{q}} \longrightarrow \mathbf{Gal}(^{B}\!/_{\mathfrak{q}}/^{A}\!/_{\mathfrak{p}})\Big).$$

我们现在对 $^{L}\!/_{K}$ 使用 Galois 理论。根据 Galois 对应，令 $L^{\mathfrak{q}}$ 为 $G_{\mathfrak{q}}$ 的中间域，即



令 $B^{\mathfrak{q}} = B \cap L^{\mathfrak{q}}$，这是 A 在 $L^{\mathfrak{q}}$ 中的整闭包；令 $\mathfrak{r} = \mathfrak{q} \cap B^{\mathfrak{q}}$，这是 $B^{\mathfrak{q}}$ 的素理想，它在 $\mathfrak{p}$ 之上。那么，$\mathfrak{q}$ 是唯一一个在 $\mathfrak{r}$ 上的理想：实际上，$\mathbf{Gal}(^{L}\!/_{L^{\mathfrak{q}}}) = G_{\mathfrak{q}}$ 在 $\mathfrak{r}$ 上的素理想集上的作用传递，根据 $G_{\mathfrak{q}}$ 的定义，只有一个这样的 $\mathfrak{q}$。

引理 142. *域扩张 $^{A}\!/_{\mathfrak{p}}/^{B^{\mathfrak{q}}}\!/_{\mathfrak{r}}$ 是平凡的，即 $^{A}\!/_{\mathfrak{p}} = ^{B^{\mathfrak{q}}}\!/_{\mathfrak{r}}$。*

证明： 对 $x \in B^{\mathfrak{q}}$，我们构造 $z \in A$，使得 $z \equiv x \mod \mathfrak{r}$：根据中国剩余定理，存在 $y \in B^{\mathfrak{q}}$，使得

$$\begin{cases} y \equiv x & \mod \mathfrak{r}; \\ y \equiv 1 & \mod \sigma^{-1}(\mathfrak{q}) \cap B^{\mathfrak{q}}, \ \ \forall\, \sigma \in \mathbf{Gal}(^{L}\!/_{K}) - \mathfrak{D}_{\mathfrak{q}}. \end{cases}$$

以上，我们用到了 $\mathfrak{q}$ 为 $\mathfrak{r}$ 上唯一的素理想，从而，$\sigma^{-1}(\mathfrak{q}) \cap B^{\mathfrak{q}} \neq \mathfrak{r}$。根据以上同余关系，我们有

$$\begin{cases} y \equiv x & \mod \mathfrak{r}; \\ \sigma(y) \equiv 1 & \mod \mathfrak{r}, \ \ \forall\, \sigma \in \mathbf{Gal}(^{L}\!/_{K}) - \mathfrak{D}_{\mathfrak{q}}. \end{cases}$$

从而，$z = \mathrm{N}_{^{L^{\mathfrak{q}}}\!/_{K}}(y) \equiv x \mod \mathfrak{r}$。 □

定理 143. *$\mathrm{Res}_{\mathfrak{q}}$ 为满的群同态。*

证明： 根据上述讨论，可以假设 $L^{\mathfrak{q}} = K$。令 $K_{\mathfrak{p}} = ^{A}\!/_{\mathfrak{p}}, L_{\mathfrak{q}} = ^{B}\!/_{\mathfrak{q}}$，那么，存在 $x \in B$，使得它在 $L_{\mathfrak{q}}$ 中的像 $\overline{x}$ 满足 $L_{\mathfrak{q}} = K_{\mathfrak{p}}(\overline{x})$（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 $\overline{x}$ 在 $K_{\mathfrak{p}}$ 上的极小多项式。通过 $\mod \mathfrak{p}$，我们有 $\overline{P}(X) \in K_{\mathfrak{p}}[X]$ 并且 $Q(X) \mid \overline{P}(X)$，这是因为 $\overline{x}$ 是 $\overline{P}(X)$ 的根。

对任意的 $\overline{\sigma} \in \mathbf{Gal}(^{L_{\mathfrak{q}}}\!/_{K_{\mathfrak{p}}})$，$\overline{\sigma}$ 完全由 $\overline{\sigma}(\overline{x})$ 决定。另外，$\overline{\sigma}(\overline{x})$ 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 $y = \overline{\sigma}(\overline{x}) \mod \mathfrak{q}$。先选定 $\sigma' \in \mathrm{Hom}_K(K(x), L)$，使得 $\sigma'(x) = y$，再将 σ' 扩张成 $\sigma \in \mathrm{Hom}_K(L, L)$。这个 σ 给出了 $\overline{\sigma}$。 □

注记 5.79. 令 $K_{\mathfrak{p}} = ^{A}\!/_{\mathfrak{p}}, L_{\mathfrak{q}} = ^{B}\!/_{\mathfrak{q}}$，我们有如下正合列：

$$1 \to \mathfrak{I}_{\mathfrak{q}} \longrightarrow \mathfrak{D}_{\mathfrak{q}} \longrightarrow \mathbf{Gal}(^{L_{\mathfrak{q}}}\!/_{K_{\mathfrak{p}}}) \to 1.$$

命题 144. *假设 $L = K(x)$，$P(X)$ 为 x 在 K 上的极小多项式。若 $\overline{P}(X) \in K_{\mathfrak{p}}[X] = ^{A}\!/_{\mathfrak{p}}[X]$ 可分，则惯性群 $\mathfrak{I}_{\mathfrak{q}}$ 是平凡的。特别地，我们有群同构*

$$\mathfrak{D}_{\mathfrak{q}} \xrightarrow{\simeq} \mathbf{Gal}(^{L_{\mathfrak{q}}}\!/_{K_{\mathfrak{p}}}).$$

证明: $P(X)$ 在 L 中分裂，即 $P(X)=(X-x_1)\cdots(X-x_n)$，其中，$x_1=x,x_2,\cdots,x_n\in L$。通过 $\bmod \mathfrak{q}$，在 $L_\mathfrak{q}$ 中，我们有

$$\overline{P}(X)=(X-\overline{x_1})\cdots(X-\overline{x_n}),\ \ \overline{x_i}\neq\overline{x_j},\ 1\leqslant i<j\leqslant n.$$

根据惯性群的定义，对任意的 $\sigma\in\mathfrak{I}_\mathfrak{q}$，$\overline{\sigma}(\overline{x_i})=\overline{x_i}$。由于 $L=K(x)$，为了决定 $\sigma\in\mathfrak{I}_\mathfrak{q}$，我们只要考虑 $\sigma(x)=x_j$。根据 $\overline{\sigma}(\overline{x_1})=\overline{x_1}$，$j=1$，从而 $\sigma(x)=x$。这表明 $\sigma=1$。 □

用同样的想法也可以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 145. $P(X)$ 为 $A[X]$ 中首一不可约多项式，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。

若 $\overline{P}(X)$ 可分，则 $L_\mathfrak{q}$ 是 $\overline{P}$ 在 $K_\mathfrak{p}$ 上的分裂域并且 $\mathfrak{D}_\mathfrak{q}\simeq\mathbf{Gal}(L_\mathfrak{q}/K_\mathfrak{p})$。

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 $\bmod\mathfrak{q}$ 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 $\sigma\in\mathfrak{D}_\mathfrak{q}$ 和 $i\leqslant l$，$\sigma(Z_i)=Z_i$。

注记 5.80. $\overline{P}$ 是可分的，所以 $\overline{P}$ 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，$x_1,x_2,\cdots,x_n\in L$。通过 $\bmod\mathfrak{q}$，在 $L_\mathfrak{q}$ 中，我们有

$$\overline{P}(X)=(X-\overline{x_1})\cdots(X-\overline{x_n}),\ \ \overline{x_i}\neq\overline{x_j},\ 1\leqslant i<j\leqslant n.$$

其中，$x_i\equiv\overline{x_j}\bmod\mathfrak{q}$ 并且 $\overline{x_j}\in L_\mathfrak{q}$。我们考虑 $L_\mathfrak{q}/K_\mathfrak{p}$ 的中间域:

$$\begin{array}{ccc}L_\mathfrak{q} & & 1\\ | & & |\\ K_\mathfrak{p}(\overline{x_1},\cdots,\overline{x_n}) & & \mathbf{Gal}(L_\mathfrak{q}/K_\mathfrak{p}(\overline{x_1},\cdots,\overline{x_n}))\\ | & & |\\ K_\mathfrak{p} & & \mathbf{Gal}(L_\mathfrak{q}/K_\mathfrak{p})\end{array}$$

对任意的 $\sigma\in\mathfrak{D}_\mathfrak{q}$，$\sigma$ 把 P 的根映射成 P 的根，所以 σ 把每个 $\overline{x_i}$ 映射成某个 $\overline{x_j}$。据此，我们有群同态

$$\mathfrak{D}_\mathfrak{q}\longrightarrow\mathbf{Gal}(K_\mathfrak{p}(\overline{x_1},\cdots,\overline{x_n})/K_\mathfrak{p}),\ \ \sigma\mapsto\overline{\sigma}.$$

由于 $\{\overline{x}_i\}_{i\leqslant n}$ 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 对应以及 $\mathrm{Res}_\mathfrak{q}$ 为满射，我们有如下交换图表:

$$\begin{array}{ccc}\mathfrak{D}_\mathfrak{q} & \xrightarrow{\mathrm{Res}_\mathfrak{q}} & \mathbf{Gal}(L_\mathfrak{q}/K_\mathfrak{p})\\ & \searrow^{\text{单}} & \downarrow{\scriptstyle \text{满}}\\ & & \mathbf{Gal}(K_\mathfrak{p}(\overline{x_1},\cdots,\overline{x_n})/K_\mathfrak{p})\end{array}$$

所以，所有的映射均为双射，进而 $K_{\mathfrak{p}}(\overline{x_1},\cdots,\overline{x_n})=L_{\mathfrak{q}}$ 并且 $\mathfrak{D}_{\mathfrak{q}}\simeq \mathbf{Gal}\left(L_{\mathfrak{q}}/K_{\mathfrak{p}}\right)$。

以下，假设 $\overline{P}(X)=\overline{P_1}(X)\overline{P_2}(X)\cdots\overline{P_l}(X)$ 是 $\overline{P}$ 在 $K_{\mathfrak{p}}[X]$ 中的不可约分解，我们证明对任意的 $\sigma\in\mathfrak{D}_{\mathfrak{q}}$ 和 $i\leqslant l$，$\sigma: Z_i\to Z_i$。实际上，对 σ 在 $\mathbf{Gal}\left(L_{\mathfrak{q}}/K_{\mathfrak{p}}\right)$ 中的像 $\overline{\sigma}$ 而言，我们显然有 $\overline{\sigma}:\overline{Z_i}\to\overline{Z_i}$，这里，$\overline{Z_i}$ 为 Z_i 中的元素 $\bmod\mathfrak{q}$ 之后的像，从而只能有 $\sigma: Z_i\to Z_i$。 □

作为推论，我们就得到了如下的著名定理：

定理 146 (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 $\mathbf{Gal}(L/\mathbb{Q})$ 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 $i=1,\cdots,l$，$\deg(\overline{P_i})=n_i$。那么，存在 $(n_1,\cdots,n_l)$-型的 $\sigma\in\mathbf{Gal}(L/\mathbb{Q})<\mathfrak{S}_n$（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 $A=\mathbb{Z},K=\mathbb{Q},\mathfrak{p}=(p)$。此时，$\mathfrak{D}_{\mathfrak{q}}\simeq\mathbf{Gal}\left(L_{\mathfrak{q}}/\mathbb{F}_p\right)$。由于 $\mathbf{Gal}\left(L_{\mathfrak{q}}/\mathbb{F}_p\right)$ 是循环群，我们选取 $\sigma\in\mathfrak{D}_{\mathfrak{q}}<\mathbf{Gal}(L/\mathbb{Q})<\mathfrak{S}_n$，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。 □

例子 5.49. 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 $\mathbf{Gal}(L/\mathbb{Q})$。

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，$\mathbf{Gal}(L/\mathbb{Q})$ 中有 4-循环。

在 $\mathbb{F}_3$ 中考虑，我们有 $\overline{P}(X)=X^4+X^3+2X^2+1$。容易看出，$\overline{P}$ 在 $\mathbb{F}_3$ 恰有一个根 -1。从而，

$$\overline{P}(X)=(X+1)(X^3-X+1).$$

并且 X^3-X+1 是不可约的。据此，$\mathbf{Gal}(L/\mathbb{Q})$ 中有 3-循环。

以上表明 $|\mathbf{Gal}(L/\mathbb{Q})|\geqslant 3\times 4=12$，所以，$\mathbf{Gal}(L/\mathbb{Q})$ 为 $\mathfrak{S}_4$ 或者 $\mathfrak{A}_4$。

在 $\mathbb{F}_5$ 中考虑，我们有 $\overline{P}(X)=X^4-X^3+2X^2-2X$，从而，

$$\overline{P}(X)=X(X-1)(X^2+2).$$

此时，X^2+2 在 $\mathbb{F}_5[X]$ 上不可约。据此，$\mathbf{Gal}(L/\mathbb{Q})$ 中有对换。从而，$\mathbf{Gal}(L/\mathbb{Q})\neq\mathfrak{A}_4$。

综上所述，$\mathbf{Gal}(L/\mathbb{Q})\simeq\mathfrak{S}_4$。

练习 5.2. 令 K 为 $P(X)=X^4+2X^2+X+3$ 在 $\mathbb{Q}$ 上的分裂域，计算 $\mathbf{Gal}\left(K/\mathbb{Q}\right)$。进一步，不用计算给出 $P(X)=X^4+2X^2-59X-27$ 在 $\mathbb{Q}$ 上的分裂域的 Galois 群。

引理 147. *G 是 $\mathfrak{S}_n$ 的子群，考虑 $\mathfrak{S}_n$ 在 $\{1,\cdots,n\}$ 上的自然作用并假设 G 的作用是传递的。如果 G 包含一个对换和一个 $(n-1)$-循环，那么 $G=\mathfrak{S}_n$*

证明： 不妨设 $\sigma=(2,3,\cdots,n)\in G$ 以及 $(a,b)\in G$。由于 G 的作用传递，通过选取 $g\in G$ 使得 $g(a)=1$，则 $g(a,b)g^{-1}=(1,g(b))$。所以，我们不妨设 $(1,b)\in G$。据此，

$$\sigma^k(1,b)\sigma^{-k}=(\sigma^k(1),\sigma^k(b))=(1,\sigma^k(b)).$$

所以，$(1,2),(1,3),\cdots,(1,n)\in G$，从而 $G=\mathfrak{S}_n$。 □

例子 5.50. 令 K 为 $P(X)=X^6+22X^5+6X^4+12X^3-52X^2-14X-30$ 在 $\mathbb{Q}$ 上的分裂域, 计算 $\mathbf{Gal}\left(K/\mathbb{Q}\right)$。

通过 $\mod 2$ 以及 Eisenstein 判别法，P 不可约。这表明 $\mathbf{Gal}\left(K/\mathbb{Q}\right)$ 是 $\mathfrak{S}_6$ 的一个传递的子群。

在 $\mathbb{F}_3[X]$ 中，$P(X)=X^6+X^5-X^2+X=X(X^5+X^4-X+1)$。然而，在 $\mathbb{F}_3[X]$ 中 X^5+X^4-X+1 不可约（利用 $X^2+1, X^2\pm X-1$ 是唯一的二次不可约多项式），从而 $\mathbf{Gal}\left(K/\mathbb{Q}\right)$ 包含 5-循环。

在 $\mathbb{F}_5[X]$ 中，

$$P(X)=X^6+2X^5+X^4+2X^3-2X^2+X=X(X-1)(X+1)(X+2)(X^2+2).$$

在 $\mathbb{F}_5[X]$ 中 X^2+2 不可约，从而 $\mathbf{Gal}\left(K/\mathbb{Q}\right)$ 包含一个对换。

根据上述引理，$\mathbf{Gal}\left(K/\mathbb{Q}\right)\simeq\mathfrak{S}_6$。

练习 5.3. 令 K 为多项式 $P(X)=X^6+22X^5-9X^4+12X^3-37X^2-29X-15$ 在 $\mathbb{Q}$ 上的分裂域，试计算 $\mathbf{Gal}\left(K/\mathbb{Q}\right)$。

练习 5.4. 令 K 为多项式 $P(X)=X^6+18X^5+12X^4-6X^3+32X^2+13X+45$ 在 $\mathbb{Q}$ 上的分裂域，试计算 $\mathbf{Gal}\left(K/\mathbb{Q}\right)$。

5.10 Galois 群计算举例

例子 5.51. 令 K 为 $P(X)=X^4+4$ 在 $\mathbb{Q}$ 上的分裂域，计算 $\mathbf{Gal}\left(K/\mathbb{Q}\right)$。

我们观察到 $P(X)=(X^2+2i)(X^2-2i)$, 所以 P 的根为 $\{\pm\sqrt{\pm 2i}\}$。再注意到 $\sqrt{2i}=\sqrt{2}\cdot\frac{\sqrt{2}}{2}(1+i)=1+i$, 所以，这个根的极小多项式是二次的，即 P 是可约的。实际上，

$$P(X)=(X^4+4X^2+4)-4X^2=(X^2+2X+2)(X^2-2X+2).$$

我们可以把 P 的根都写成 $\{\pm 1\pm i\}$，所以，$K=\mathbb{Q}(i)$，从而 $\mathbf{Gal}\left(K/\mathbb{Q}\right)\simeq\mathbb{Z}/2\mathbb{Z}$。

例子 5.52. 令 K 为 $P(X)=X^3-3X+1$ 在 $\mathbb{Q}$ 上的分裂域，计算 $\mathbf{Gal}\left(K/\mathbb{Q}\right)$。

$P(X)=X^3-3X+1$ 在 $\mathbb{Z}[X]$ 上不可约，所以，$\mathbf{Gal}\left(K/\mathbb{Q}\right)\simeq\mathfrak{A}_3$ 或 $\mathfrak{S}_3$。我们计算其判别式

$$\mathrm{Disc}(P)=-4(-3)^3-27\cdot 1^2=81=9^2.$$

所以，$\mathbf{Gal}\left(K/\mathbb{Q}\right)\simeq\mathfrak{A}_3$。

例子 5.53. 令 K 为 $P(X)=X^3-3TX-T-T^2$ 在 $\mathbb{C}(T)$ 上的分裂域，计算 $\mathbf{Gal}\left(K/\mathbb{C}(T)\right)$。

首先，根据 Eisenstein 判别法以及考察 $\mathbb{C}[T]$ 的素理想 (T)，我们知道 $P(X)$ 在 $\mathbb{C}[T]$ 上不可约，从而 $P(X)$ 在 $\mathbb{C}(T)=\mathrm{Frac}\big(\mathbb{C}[T]\big)$ 上不可约，所以 $\mathbf{Gal}\left(K/\mathbb{C}(T)\right)\simeq\mathfrak{A}_3$ 或 $\mathfrak{S}_3$。我们计算其判别式

$$\mathrm{Disc}(P)=-4(-3T)^3-27(-T-T^2)^2=-108T^2(T-1)^2=\big(\sqrt{-108}T(T-1)\big)^2.$$

所以，$\mathbf{Gal}\left(K/\mathbb{Q}\right)\simeq\mathfrak{A}_3$。

例子 5.54. 令 K 为 $P(X)=X^{2^m}-1$ 在 $\mathbb{Q}$ 上的分裂域，其中，$m\geqslant 2$，计算 $\mathbf{Gal}\left(K/\mathbb{Q}\right)$。

根据分圆扩张的理论，$\mathbf{Gal}\left(K/\mathbb{Q}\right)\simeq\left(\mathbb{Z}/2^m\mathbb{Z}\right)^\times$。我们使用习题2.7.2的结论，即存在群同构：

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2^{m-2}\mathbb{Z}\longrightarrow\left(\mathbb{Z}/2^m\mathbb{Z}\right)^\times,\quad(a,b)\mapsto(-1)^a5^b\mod 2^m.$$

所以，$\mathbf{Gal}\left(K/\mathbb{Q}\right)\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2^{m-2}\mathbb{Z}$。

例子 5.55. 令 K 为 $P(X)=X^4-5$ 在 $\mathbb{Q}$ 上的分裂域，计算 $\mathbf{Gal}\left(K/\mathbb{Q}\right)$。

考虑域扩张的序列 $\mathbb{Q}\subset\mathbb{Q}(5^{\frac{1}{4}})\subset K=\mathbb{Q}(5^{\frac{1}{4}},i)$，我们知道 $[K:\mathbb{Q}]=8$。

根据例子5.36，$\mathbf{Gal}(L/K)$ 是 $\mathbf{Aff}_1(\mathbb{Z}/4\mathbb{Z})$ 的子群。然而，$|\mathbf{Aff}_1(\mathbb{Z}/4\mathbb{Z})|=8$，所以，

$$\mathbf{Gal}(L/K)\simeq\mathbf{Aff}_1(\mathbb{Z}/4\mathbb{Z}).$$

另外，$\mathbf{Aff}_1(\mathbb{Z}/4\mathbb{Z})\simeq\mathfrak{D}_4$。实际上，$\mathbf{Aff}_1$ 中的元素

$$x\mapsto 3x,\quad x\mapsto x+1$$

恰好对应着 $\mathfrak{D}_4$ 中的一个反射与一个旋转。

例子 5.56. 令 K 为 $P(X)=X^6-2$ 在 $\mathbb{Q}$ 上的分裂域，计算 $\mathbf{Gal}\left(K/\mathbb{Q}\right)$。

根据例子5.36，$\mathbf{Gal}(L/K)$ 是 $\mathbf{Aff}_1(\mathbb{Z}/6\mathbb{Z})$ 的子群。另外，由于 $|(\mathbb{Z}/6\mathbb{Z})|=2$，所以，$|\mathbf{Aff}_1(\mathbb{Z}/6\mathbb{Z})|=12$ 并且 $\mathbf{Aff}_1(\mathbb{Z}/6\mathbb{Z})\simeq\mathfrak{D}_6$。实际上，$\mathbf{Aff}_1$ 中的元素

$$x\mapsto 5x,\quad x\mapsto x+1$$

对应 $\mathfrak{D}_6$ 中的一个反射与一个旋转。

另外，域扩张的序列 $\mathbb{Q}\subset\mathbb{Q}(2^{\frac{1}{6}})\subset K=\mathbb{Q}(2^{\frac{1}{6}},\xi_6)$ 表明 $[K:\mathbb{Q}]\geqslant 12$。所以，

$$\mathbf{Gal}(L/K)\simeq\mathbf{Aff}_1(\mathbb{Z}/6\mathbb{Z})\simeq\mathfrak{D}_6.$$

例子 5.57. 令 L 为 $P(X)=X^n-T$ 在 $K=\mathbb{C}(T)$ 或 $K=\mathbb{R}(T)$ 上的分裂域，计算 $\mathbf{Gal}\left(L/K\right)$。

根据 Eisenstein 判别法，$P(X)$ 在这两个域上均为不可约多项式。当 $K=\mathbb{C}(T)$ 时，由于 $\mathbb{C}(T)$ 上包含所有 n-次单位根，根据 Kummer 理论，$\mathbf{Gal}\left(L/K\right)\simeq\mathbb{Z}/n\mathbb{Z}$。

当 $K=\mathbb{R}(T)$，我们仍然有 $L=\mathbb{C}(\sqrt[n]{T})=\mathbb{R}(T)(\sqrt[n]{T},i)$，即 $\mathbb{R}(T)\subset\mathbb{R}(T)(\sqrt[n]{T})\subset\mathbb{R}(T)(\sqrt[n]{T},i)$，所以，$[L:K]=2n$。另外，仿照例子5.36，对任意 $g\in\mathbf{Gal}\left(L/K\right)$，通过考虑 g 在 i 和 $\sqrt[n]{T}$ 的作用，我们知道 $\mathbf{Gal}\left(L/K\right)$ 是由映射

$$\{(i,\sqrt[n]{T})\mapsto(\pm i,\xi_n^k\sqrt[n]{T})\}$$

构成的群的子群。容易看出，这是 $\mathfrak{D}_n$。由于 $\mathbf{Gal}\left(L/K\right)$ 恰有 $2n$ 个元素，所以，$\mathbf{Gal}\left(L/K\right)\simeq\mathfrak{D}_n$。

例子 5.58. 令 K 为 $P(X)=X^6+3$ 在 $\mathbb{Q}$ 上的分裂域，计算 $\mathbf{Gal}\left(K/\mathbb{Q}\right)$。

根据 Eisenstein 判别法，P 是不可约多项式，从而，$6\mid[K:\mathbb{Q}]$。注意到 $\alpha=i\sqrt[6]{3}$ 是 P 的根并且 K 包含 6 次单位根 ξ_6，从而，$K=\mathbb{Q}(\alpha,\xi_6)$。

根据例子5.36，$\mathbf{Gal}(L/K)$ 是 $\mathbf{Aff}_1(\mathbb{Z}/6\mathbb{Z})$ 的子群。然而，$|\mathbf{Aff}_1(\mathbb{Z}/6\mathbb{Z})|=12$，所以，$[K:\mathbb{Q}]=6$ 或 12。通过考虑 $\mathbf{Gal}(L/K)$ 对 α 和 ξ_6 的作用，我们来证明吧 $[K:\mathbb{Q}]=6$。

给定 $g\in\mathbf{Gal}(L/K)$，由于 ξ_6 和 ξ_6^{-1} 是仅有的 6 次本原单位根，所以

$$g(\xi_6)=\xi_6^a,\quad g(\alpha)=\xi_6^b\cdot\alpha,$$

其中，$a=\pm1$，$b=0,1,\cdots,5$ 并且 a,b 的值决定了 g。由于 $\xi_6=\frac{1}{2}+\frac{i\sqrt{3}}{2}$，所以，$\xi_6$ 在 g 下的像由 $g(i\sqrt{3})$ 决定，即 $g(i\sqrt{3})=a\cdot i\sqrt{3}$。另外，$-\alpha^3=i\sqrt{3}$，从而，

$$a=i\sqrt{3}=g(-\alpha^3)=-g(\alpha)^3=-\xi_6^{3b}\alpha^3=\xi_6^{3b}\cdot i\sqrt{3}.$$

所以，$a=\xi_6^{3b}$。当 $a=1$ 时，$b=0,2,4$；当 $a=-1$ 时，$b=1,3,5$。所以，这样的 (a,b) 的个数不超过 6。据此，$[K:\mathbb{Q}]=6$。实际上，以上运算表明 $\alpha^3=i\sqrt{3}$，从而 $\xi_6=\frac{1}{2}-\frac{\alpha^3}{2}$，这就直接证明了 $K=\mathbb{Q}(\alpha,\xi_6)=\mathbb{Q}(\alpha)$。

令 $X=\Big\{\{\alpha,-\alpha\},\{\xi_6\alpha,-\xi_6\alpha\},\{\xi_6^2\alpha,-\xi_6^2\alpha\}\Big\}$ 为根的集合的一个分拆，不难看出，$\mathbf{Gal}(L/K)$ 作用在 X 上，这就给出了 $\mathbf{Gal}(L/K)\simeq\mathfrak{S}_3$。

例子 5.59. 令 L 为 $P(X)=(X^5-2)(X^5-3)$ 在 $\mathbb{Q}$ 上的分裂域，计算 $\mathbf{Gal}\left(L/\mathbb{Q}\right)$。

首先考虑 $K=\mathbb{Q}(\xi_5,\sqrt[5]{2})$，这是 X^5-2 的分裂域。由于 K 有 4 次中间域 $\mathbb{Q}(\xi_5)$ 和 5 次中间域 $\mathbb{Q}(\sqrt[5]{2})$，所以，$[K:\mathbb{Q}]=20$。根据例子5.36，$\mathbf{Gal}(K/\mathbb{Q})$ 是 $\mathbf{Aff}_1\big(\mathbb{Z}/5\mathbb{Z}\big)$ 的子群，其中，$|\mathbf{Aff}_1\big(\mathbb{Z}/5\mathbb{Z}\big)|=20$，所以，$\mathbf{Gal}(K/\mathbb{Q})\simeq\mathbf{Aff}_1\big(\mathbb{Z}/5\mathbb{Z}\big)$。给定 $g\in\mathbf{Gal}(K/\mathbb{Q})$，它由以下 a,b 决定：

$$g(\xi_5)=\xi_5^a,\quad g(\sqrt[5]{2})=\xi_5^b\cdot\sqrt[5]{2},\quad 1\leqslant a\leqslant 4,0\leqslant b\leqslant 4.$$

我们现在证明 X^5-3 在 $K=\mathbb{Q}(\xi_5,\sqrt[5]{2})$ 上不可约：

- X^5-3 在 K 上没有根。

  我们注意到 $\mathbb{Q}(\xi_5^b\cdot\sqrt[5]{2})$ 是 K 的 5 个不同的 5 次中间域，其中，$b=0,1,\cdots,5$（如果有两个相同，则 ξ_5 和 $\sqrt[5]{2}$ 都在这个中间域中），它们对应着 $\mathbf{Gal}(K/\mathbb{Q})$ 的 5 个子群。由于 20 阶的群的 Sylow 2-子群最多有 5 个，所以，这是 K 的所有 5 次中间域。

  如果 $\sqrt[5]{3}\in K=\mathbb{Q}(\xi_5,\sqrt[5]{2})$，则 $\mathbb{Q}(\sqrt[5]{3})$ 为一个 5 次中间域并且落在 $\mathbb{R}$ 中，这表明 $\mathbb{Q}(\sqrt[5]{3})=\mathbb{Q}(\sqrt[5]{2})=M$。据此，由于 $\{(\sqrt[5]{2})^b\}_{b=0^4}$ 是 $M/\mathbb{Q}$ 的基，所以，存在 $l_0,\cdots,l_4\in\mathbb{Q}$，使得

  $$\sqrt[5]{3}=l_0+l_1\sqrt[5]{2}+l_2(\sqrt[5]{2})^2+l_3(\sqrt[5]{2})^3+l_4(\sqrt[5]{2})^4.$$

  通过取迹 $\mathrm{Tr}_{M/\mathbb{Q}}$，则 $l_0=0$。此时，考虑

  $$\sqrt[5]{3}(\sqrt[5]{2})^4=l_1+l_2\sqrt[5]{2}+l_3(\sqrt[5]{2})^2+l_4(\sqrt[5]{2})^3.$$

  那么，$\beta=\sqrt[5]{3}(\sqrt[5]{2})^4=\sqrt[5]{3\cdot 2^4}$ 满足 $\beta^5-3\cdot 2^4=0$，从而，$1,\beta,\cdots,\beta^4$ 也是 $M/\mathbb{Q}$ 的基，从而，取迹 $\mathrm{Tr}_{M/\mathbb{Q}}$ 给出 $l_1=0$。以此类推，$l_0=\cdots=l_4=0$，矛盾。

- X^5-3 在 K 上不能分解成一个二次与一个三次不可约多项式的乘积。

  如若不然，根据上述，$X^5-3=P(X)Q(X)$，其中，$P(X),Q(X)\in K[X]$ 并且 P,Q 是首一的并且是不可约的。那么，对任意的 $\sigma\in\mathbf{Gal}(K/\mathbb{Q})$，我们有

  $$X^5-3=(X^5-3)^\sigma=P^\sigma(X)Q^\sigma(X).$$

  此时，$P^\sigma(X),Q^\sigma(X)$ 均为首一不可约多项式。根据 $K[X]$ 是唯一分解整环以及 P 与 Q 的次数为 2 和 3，我们必有 $P^\sigma(X)=P(X),Q^\sigma(X)=Q(X)$，其中，$\sigma\in\mathbf{Gal}(K/\mathbb{Q})$。这说明 $P,Q\in\mathbb{Q}[X]$，矛盾。

综上所述，我们得到 $[L:\mathbb{Q}]=100$，其中，$L=K(\sqrt[5]{3})=\mathbb{Q}(\xi_5,\sqrt[5]{2},\sqrt[5]{3})$。

我们现在将 $\mathbf{Gal}(L/\mathbb{Q})$ 实现为 $\mathbf{Aff}_2\big(\mathbb{Z}/5\mathbb{Z}\big)$ 的子群，

$$\mathbf{Aff}_2\big(\mathbb{Z}/5\mathbb{Z}\big)=\big\{f_{A,b}:\mathbb{F}_5^2\to\mathbb{F}_5^2\big|\text{对任意 }x\in\mathbb{F}_5^2,\ f_{A,b}(x)=A\cdot x+b,A\in\mathbf{GL}(2;\mathbb{F}_5),b\in\mathbb{F}_5^2\big\}$$

$\mathbf{Gal}(K/\mathbb{Q})\simeq\mathbf{Aff}_1\big(\mathbb{Z}/5\mathbb{Z}\big)$。给定 $g\in\mathbf{Gal}(K/\mathbb{Q})$，它由以下 a,b_1,a_2 决定：

$$g(\xi_5)=\xi_5^a,\ g(\sqrt[5]{2})=\xi_5^{b_1}\cdot\sqrt[5]{2},\ g(\sqrt[5]{3})=\xi_5^{b_2}\cdot\sqrt[5]{3},\ 1\leqslant a\leqslant 4,0\leqslant b_1,b_2\leqslant 4.$$

按照定义，令 $A=\begin{pmatrix}a&0\\0&a\end{pmatrix}, b=\begin{pmatrix}b_1\\b_2\end{pmatrix}$，定义

$$\varphi:\mathbf{Gal}(L/\mathbb{Q})\mapsto\mathbf{Aff}_2(\mathbb{Z}/5\mathbb{Z}),\ g\mapsto\left(\begin{pmatrix}x_1\\x_2\end{pmatrix}\mapsto\begin{pmatrix}a&0\\0&a\end{pmatrix}\begin{pmatrix}x_1\\x_2\end{pmatrix}+\begin{pmatrix}b_1\\b_2\end{pmatrix}\right)$$

这样的元素恰好有 100 个。

特别地，$\mathbf{Aff}_2(\mathbb{Z}/5\mathbb{Z})$ 的子群

$$\left\{f_{A,b}:\mathbb{F}_5^2\to\mathbb{F}_5^2\middle|A\in\mathbf{GL}(2;\mathbb{F}_5)\text{且是对角阵},b\in\mathbb{F}_5^2\right\}$$

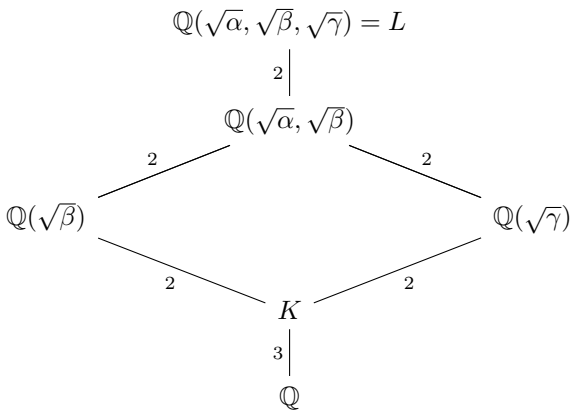
是可解群。实际上，100 阶的群的 Sylow 5-子群都是正规子群。由于 5-群均可解，所以每个 100 阶的群都是可解群。

例子 5.60. 令 L 为 $P(X)=X^6-3X^2+1$ 在 $\mathbb{Q}$ 上的分裂域，计算 $\mathbf{Gal}\left(L/\mathbb{Q}\right)$。

令 $Q(X)=X^3-3X^2+1$，则 Q 是不可约多项式并且有三个实根依次记作 $\alpha<0<\beta<\gamma$。令 K 为 $Q(X)$ 在 $\mathbb{Q}$ 上的分裂域，由于 $\Delta(Q)=81=9^2$，所以 $\mathbf{Gal}\left(K/\mathbb{Q}\right)\simeq\mathfrak{A}_3$，选取生成元 $\sigma\in\mathbf{Gal}\left(K/\mathbb{Q}\right)$，使得 $\sigma(\alpha)=\beta,\sigma(\beta)=\gamma,\sigma(\gamma)=\alpha$。由于 $[K:\mathbb{Q}]=3$，我们还有 $K=\mathbb{Q}(\alpha)=\mathbb{Q}(\beta)=\mathbb{Q}(\gamma)$。

由于 $P(X)=Q(X^2)$，所以，$L=K(\sqrt{\alpha},\sqrt{\beta},\sqrt{\gamma})=\mathbb{Q}(\sqrt{\alpha},\sqrt{\beta},\sqrt{\gamma})$。由于 $\sqrt{\alpha}\notin\mathbb{R}$，所以，$[L:K(\sqrt{\beta},\sqrt{\gamma})]=2$。

由于 $\mathbf{Gal}\left(L/\mathbb{Q}\right)\xrightarrow{\text{Res}}\mathbf{Gal}\left(K/\mathbb{Q}\right)$ 是满射，任选 $\overline{\sigma}$ 为 σ 在 $\mathbf{Gal}\left(L/\mathbb{Q}\right)$ 中的延拓。那么，$\overline{\sigma}(\sqrt{\alpha})=\pm\sqrt{\beta},\overline{\sigma}(\sqrt{\beta})=\pm\sqrt{\gamma},\overline{\sigma}(\sqrt{\gamma})=\pm\sqrt{\alpha}$。利用 $\overline{\sigma}$，我们可以看出 $[K(\sqrt{\beta}):K]=2$：否则 $\sqrt{\beta}\in K$ 而 $\overline{\sigma}(K)\subset K$，所以，$\overline{\sigma}^2(\sqrt{\alpha})=\pm\gamma\in K$，这与 $K\subset\mathbb{R}$ 矛盾。类似地，$[K(\sqrt{\gamma}):K]=2$。



利用 $\overline{\sigma}$，我们证明 $\mathbb{Q}(\sqrt{\beta})\neq\mathbb{Q}(\sqrt{\gamma})$：若不然，令 $\mathbb{Q}(\sqrt{\beta})=\mathbb{Q}(\sqrt{\gamma})=M$ 由于 $\overline{\sigma}(\sqrt{\beta})=\pm\sqrt{\gamma}$，所以 $\overline{\sigma}(M)\subset M$，从而，$\overline{\sigma}^2(\sqrt{\beta})=\pm\sqrt{\alpha}\in M$，这与 $M\subset\mathbb{R}$ 矛盾。综合上述讨论，我们得到上述扩张的图表。

由于 L/K 是 $(X^2-\alpha)(X^2-\beta)(X^2-\gamma)$ 分裂域，其 Galois 群的 8 个元素可以罗列如下：

$$\left\{\alpha\mapsto\pm\sqrt{\alpha},\ \beta\mapsto\pm\sqrt{\beta},\ \gamma\mapsto\pm\sqrt{\gamma}\right\}.$$

所以，$\mathbf{Gal}\left(L/K\right)\simeq\left(\mathbb{Z}/2\mathbb{Z}\right)^3$。特别地，我们有

$$1\longrightarrow\left(\mathbb{Z}/2\mathbb{Z}\right)^3\longrightarrow\mathbf{Gal}\left(L/K\right)\longrightarrow\mathbb{Z}/3\mathbb{Z}\longrightarrow1.\tag{5.6}$$

我们也可以将 $\mathbf{Gal}\left(L/\mathbb{Q}\right)$ 的元素全部罗列出来：

$$\left\{\begin{array}{l}\alpha\mapsto\pm\sqrt{\alpha},\\ \beta\mapsto\pm\sqrt{\beta},\\ \gamma\mapsto\pm\sqrt{\gamma}.\end{array}\right.,\quad\left\{\begin{array}{l}\alpha\mapsto\pm\sqrt{\beta},\\ \beta\mapsto\pm\sqrt{\gamma},\\ \gamma\mapsto\pm\sqrt{\alpha}.\end{array}\right.,\quad\left\{\begin{array}{l}\alpha\mapsto\pm\sqrt{\gamma},\\ \beta\mapsto\pm\sqrt{\alpha},\\ \gamma\mapsto\pm\sqrt{\beta}.\end{array}\right.$$

这自然给出了 $\mathbf{Gal}\left(L/\mathbb{Q}\right)$ 的群结构。

我们现在用矩阵群或者更为熟悉的群来表示 $\mathbf{Gal}\left(L/\mathbb{Q}\right)$。实际上，我们有

$$\mathbf{Gal}\left(L/\mathbb{Q}\right)=\left\{\begin{pmatrix}\pm1&0&0\\0&\pm1&0\\0&0&\pm1\end{pmatrix},\begin{pmatrix}0&\pm1&0\\0&0&\pm1\\\pm1&0&0\end{pmatrix},\begin{pmatrix}0&0&\pm1\\\pm1&0&0\\0&\pm1&0\end{pmatrix}\right\}.$$

另外，根据正合列(5.6)，$\mathbf{Gal}\left(L/\mathbb{Q}\right)$ 中有 3 阶子群 $H\simeq\langle\overline{\sigma}\rangle$（可能要重选 $\overline{\sigma}$），其像为 $\mathbf{Gal}\left(K/\mathbb{Q}\right)$；$\mathbf{Gal}\left(L/\mathbb{Q}\right)$ 中有同构于 $\mathbb{F}_2^3$ 的 8 阶子群 N。由于它们的阶互素，所以，$\mathbf{Gal}\left(L/\mathbb{Q}\right)\simeq N\rtimes_\varphi H$，其中，作用 φ 由如下映射给出：

$$\varphi(\overline{\sigma}):(x_1,x_2,x_3)\mapsto(x_2,x_3,x_1),\quad\forall(x_1,x_2,x_3)\in N\simeq\mathbb{F}_2^3.$$

以上给出了

$$\mathbf{Gal}\left(L/\mathbb{Q}\right)\simeq\left(\mathbb{Z}/2\mathbb{Z}\right)^3\rtimes_\varphi\mathbb{Z}/3\mathbb{Z}.$$

我们还可以证明

$$\mathbf{Gal}\left(L/\mathbb{Q}\right)\simeq\mathfrak{A}_4\times\mathbb{Z}/2\mathbb{Z}.$$

首先观察到 H 在 $N=\mathbb{F}_3^2$ 上的作用有一个 1 维不变子空间：

$$V=\mathbb{F}_2\cdot(1,1,1)=\{(0,0,0),(1,1,1)\}\subset\mathbb{F}_3^2.$$

注意到 V 在 $\mathbb{F}_3^2$ 中有一个 2 维的补空间 W，它由 $(1,1,0),(1,0,1)$ 和 $(0,1,1)$ 张成。实际上，

$$W=\left\{(x_1,x_2,x_2)\in\mathbb{F}_2^3\middle|x_1+x_2+x_3=0\right\}.$$

此时，$\mathbb{F}_3^2=V\oplus W$ 并且 W 在 H 的作用下也不变。此时，我们有

$$\mathbb{F}_2^3\rtimes_\varphi H\simeq(V\times W)\rtimes_\varphi H\simeq V\times\left(W\rtimes_\varphi H\right)\simeq\mathbb{Z}/2\mathbb{Z}\times\left(W\rtimes_\varphi H\right).$$

将 W 等同于 $\mathfrak{A}_4$ 中的 $\{1,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$ 而 H 等同于某个 3-循环生成的子群，容易看出，$\mathfrak{A}_4\simeq W\rtimes_\varphi H$，这就完成了计算。

5.11 习题

5.11.1 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：

$$m_x:L\longrightarrow L,\quad y\mapsto x\cdot y.$$

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：

$$\mathrm{Tr}_{L/K}(x)=\mathrm{Tr}(m_x),\ \mathrm{N}_{L/K}(x)=\det(m_x),\quad P_{L/K,x}(X)=\det(X\cdot I-m_x).$$

1. 假设 $x \in K$，试计算 $\mathrm{Tr}_{L/K}(x), \mathrm{N}_{L/K}(x)$ 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。

2. 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

$$\mathrm{Tr}_{L/K}(x) = 2a = x + \sigma(x),\ \mathrm{N}_{L/K}(x) = a^2 - db^2 = x \cdot \sigma(x),\ P_{L/K,x}(X) = (X - x)(X - \sigma(x)).$$

3. 证明，以下映射为群同态：

$$\mathrm{Tr}_{L/K} : (L, +) \to (K, +),\quad \mathrm{N}_{L/K} : (L^\times, \cdot) \to (K^\times, \cdot).$$

4. （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 $\{e_i\}_{i \leqslant m}$ 和 $\{f_j\}_{j \leqslant n}$ 分别为 M/K 和 L/M 的基，此时 $\{e_i f_j\}_{i \leqslant m, j \leqslant n}$ 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）

5. 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 $\{e_i\}_{i \leqslant m}$ 和 $\{f_j\}_{j \leqslant n}$ 分别为 $K(x)/K$ 和 $L/K(x)$ 的基，此时 $\{e_i f_j\}_{i \leqslant m, j \leqslant n}$ 为 L/K 的基）

6. 对于 $x \in L$，$P_{\min}(X)$ 为其在 K 上的极小多项式，$x_1, x_2, \cdots, x_d$ 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，

$$\mathrm{Tr}_{L/K}(x) = [L : K(x)]\big(\sum_{i=1}^{d} x_i\big),\quad \mathrm{N}_{L/K}(x) = \big(\prod_{i=1}^{d} x_i\big)^{[L:K(x)]}.$$

7. 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 $x \in L$，

$$\mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(x),\ \mathrm{N}_{L/K}(x) = \prod_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(x),$$

以及

$$P_{L/K,x}(X) = \prod_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \big(X - \sigma(x)\big).$$

8. L/K 为有限扩张，Ω/K 如上。那么，对任意的 $x \in L$，

$$\mathrm{Tr}_{L/K}(x) = p^n \sum_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(x),\ \mathrm{N}_{L/K}(x) = \big(\prod_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(x)\big)^{p^n},$$

其中，$p^n = \frac{[L,K]}{[L,K]_s}$ 为扩张的不可分次数。

9. (迹和范数的传递性) 如果 $K \subset M \subset L$ 是中间域。证明,

$$\mathrm{Tr}_{M/K} \circ \mathrm{Tr}_{L/M} = \mathrm{Tr}_{L/K}, \quad \mathrm{N}_{M/K} \circ \mathrm{N}_{L/M} = \mathrm{N}_{L/K}.$$

(为简单起见, 你可以只对可分情形进行证明)

10. 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 $\overline{K}$ 中的一个根。证明,

$$\mathrm{Disc}(P) = (-1)^{\frac{1}{2}d(d-1)} \mathrm{N}_{K(\alpha)/K}(P'(\alpha)).$$

以上, $\mathrm{Disc}(P) := \prod_{i<j}(\alpha_i - \alpha_j)^2$, 其中, $\{\alpha_i\}$ 为 P 在 $\overline{K}$ 中的所有根 (包括重根)。

11. L/K 为有限扩张, $x \in L$ 在 K 上不可分。证明, $\mathrm{Tr}_{L/K}(x) = 0$。

12. L/K 为有限扩张并且不是可分的。证明, $\mathrm{Tr}_{L/K} \equiv 0$。

13. 考虑对称 K-双线性的二次型

$$L \times L \longrightarrow K, \quad (x, y) \mapsto \mathrm{Tr}_{L/K}(x \cdot y).$$

对任意的 $x \in L^\times$, 存在 $y \in L$, 使得 $\mathrm{Tr}_{L/K}(x \cdot y) \neq 0$, 我们就称这个二次型是**非退化的**, 否则是**退化的**。证明, 如果 $\mathrm{char}(K) = 0$, 以上二次型非退化; 如果 L/K 不是可分的, 以上二次型退化。

14. 假设 L/K 是可分的, 从而, $L = K(x)$, $n = [L : K]$。证明, $\mathrm{Tr}_{L/K}(x^k)$ 中至少有一个非零, 其中, $k = 0, 1, \cdots, n-1$.

15. 证明, L/K 是可分的等价于二次型

$$L \times L \longrightarrow K, \quad (x, y) \mapsto \mathrm{Tr}_{L/K}(x \cdot y).$$

非退化。

5.11.2 关于多项式的一个命题

K 是域, $P \in K[X]$ 并且 $\deg(P) = p$ 是素数。假设 P 满足如下性质: 对任意的域扩张 L/K, 如果 P 在 L 中有根, 那么 P 在 $L[X]$ 中可以分裂成一次多项式的乘积。证明, 以下两种可能必居其一 (可以同时发生):

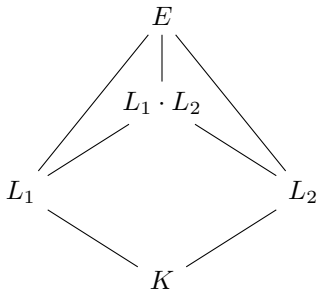
- P 在 $K[X]$ 中不可约;
- P 在 K 上有根。

证明, 在以下情形下, P 均满足上述的性质:

1. $\mathrm{Char}(K) = p$, $P(X) = X^p - a$, $a \in K$;
2. $\mathrm{Char}(K) = p$, $P(X) = X^p - X - a$, $a \in K$;
3. $\mathrm{Char}(K) \neq p$, $P(X) = X^p - a$, $a \in K$ 并且存在 $\xi \in K$ 使得 $\xi^p = 1$ 但是 $\xi \neq 1$。

5.11.3 关于域扩张的一个命题

给定域扩张 E/K，L_1 和 L_2 是中间域并且 $[L_1:K]<\infty,[L_2:K]<\infty$。



1. 证明，$[L_1\cdot L_2:L_1]\leqslant[L_2:K]$。
2. 证明，$[L_1\cdot L_2:K]\leqslant[L_1:K][L_2:K]$。
3. 证明，如果 $[L_1:K]$ 与 $[L_2:K]$ 互素，那么 $[L_1\cdot L_2:K]=[L_1:K][L_2:K]$。
4. 证明，如果 $[L_1\cdot L_2:K]=[L_1:K][L_2:K]$，那么 $L_1\cap L_2=K$。
5. 上一命题的逆命题不成立：假设 $\alpha,\beta\in\mathbb{C}$ 是 X^3-2 的两个不同的根，证明，$\mathbb{Q}(\alpha)\cap\mathbb{Q}(\beta)=\mathbb{Q}$ 但是 $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]<[\mathbb{Q}(\alpha):\mathbb{Q}][\mathbb{Q}(\beta):\mathbb{Q}]$。

5.11.4 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 $|F|<\infty$。

1. 令 $Z=\{x\in F|$对任意的 $y\in F$，有 $xy=yx\}$ 为 F 的中心。证明，Z 是域。令 $q=|Z|$，证明，存在 $n\geqslant 0$，使得 $|F|=q^n$。
2. 对任意的 $x\in F$，令 $C_x=\{y\in F|xy=yx\}$。证明，C_x 是 F 的子环并且存在整数 n_x 使得 $|C_x|=q^{n_x}$。
3. 对于 $x\in F^\times$，令 $\mathrm{Conj}(x)=\{yxy^{-1}|y\in F^\times\}$。证明，$|\mathrm{Conj}(x)|=\frac{q^n-1}{q^{n_x}-1}$ 并证明 $n_x\mid n$。
4. 证明，如果 $x\notin Z$，那么，$\Phi_n(q)$ 整除 $|\mathrm{Conj}(x)|$，其中，$\Phi_n(X)$ 为第 n 个分圆多项式。
5. 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）

5.11.5 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。

1. 证明，如果 $x\in L$ 是 P 的根，那么，

$$P(X)=\big(X-x\big)\big(X-(x+1)\big)\cdots\big(X-(x+p-1)\big).$$

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。
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

$$\mathrm{Gal}(L/K) \longrightarrow \mathbb{F}_p, \quad g \mapsto g(x) - x$$

是群同构。特别地，$\mathrm{Gal}(L/K) \simeq \mathbb{Z}/p\mathbb{Z}$。

B) K 是特征为 p 的域，L/K 是 Galois 扩张并且 $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/p\mathbb{Z}$，$\sigma$ 是 $\mathrm{Gal}(L/K)$ 的一个生成元。

1. 证明，存在 $y \in L$，使得 $\sum_{k=0}^{p-1} \sigma^k(y) = -1$。
2. 令 $x = \sum_{k=0}^{p-1} k\sigma^k(y)$，证明，$\sigma(x) = x + 1$。
3. 证明，$P(X) = \prod_{k=0}^{p-1} \big(X - \sigma^k(x)\big)$ 是 x 的极小多项式并且 $a = x^p - x \in K$。
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)+B)，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（$m \geqslant 2$）。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）。

C) K 是特征为 p 的域，L/K 是阶为 p^m 的循环扩张，σ 是 $\mathrm{Gal}(L/K)$ 的一个生成元，$\tau = \sigma^{p^{m-1}}$，$M = L^{\langle\tau\rangle}$。

1. 证明，存在 $\lambda \in M$，$P(X) = X^p - X - \lambda$ 在 L 中有根 θ 并且 $L = M(\theta)$，$\tau(\theta) = \theta + 1$。
2. 证明，存在 $\beta \in M$，使得 $\sigma(\theta) = \theta + \beta$。
3. 证明，$K(\theta) = L$。
4. 证明，$\sigma(\lambda) - \lambda = \beta^p - \beta$ 并且 $\mathrm{Tr}_{M/K}(\beta) = 1$。

D) K 是特征为 p 的域，M/K 是阶为 p^{m-1} 的循环扩张（$m \geqslant 2$），σ 是 $\mathrm{Gal}(M/K)$ 的一个生成元。假设 $\beta \in M$ 并且 $\mathrm{Tr}_{M/K}(\beta) = 1$。[52]

1. 证明，存在 $\lambda \in M$，使得 $\sigma(\lambda) - \lambda = \beta^p - \beta$。（提示：使用 Hilbert 90）
2. $P(X) = X^p - X - \lambda$ 是 $M[X]$ 中的不可约多项式。
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 $\overline{\sigma} \in \mathrm{Gal}(L/K)$ 使得 $\overline{\sigma}$ 生成了 $\mathrm{Gal}(L/K)$ 并且 $\overline{\sigma}(\theta) = \theta + \beta$。

5.11.6 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。

1. 证明，通过对 $X^{17} - 1$ 的根的作用，我们有群同构

$$\mathrm{Gal}(L/K) \xrightarrow{\simeq} \left(\mathbb{Z}/17\mathbb{Z}\right)^\times$$

并且 $\sigma : \xi \mapsto \xi^3$ 是 $\mathrm{Gal}(L/K)$ 的一个生成元。

2. 以下是 $H_0 = \mathrm{Gal}(L/K)$ 的一个 Jordan-Hölder 滤链：

$$H_0 \rhd H_1 \rhd H_2 \rhd H_3 \rhd H_4 = 1,$$

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。

[52]根据 M/K 是有限可分的以及 $\mathrm{Tr}_{M/K} : M \times M \to K$ 是非退化的，这种 β 总是存在。

3. 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。

4. 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。

5. 令 $c_j=\sum_{k=0}^{1}\sigma^{8k+j}(\xi)$，其中，$j=0,1,\cdots,7$。计算 c_0+c_4 和 $c_0\cdot c_4$ 并证明

$$\cos(\frac{2\pi}{17})=\frac{1}{16}\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+\sqrt{68+12\sqrt{17}-4\sqrt{34-2\sqrt{17}}-8\sqrt{34+2\sqrt{17}}}\right).$$

5.11.7 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。

1. 证明，每个奇数次的实系数多项式在 $\mathbb{R}$ 上总有根。

2. 证明，每个 $\mathbb{R}(i)$ 系数的二次多项式的根都在 $\mathbb{R}(i)$ 中。

3. 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。

4. 令 H 为 $\mathrm{Gal}(L/\mathbb{R})$ 的 Sylow 2-子群，证明，$L^H=\mathbb{R}$。据此证明 $\mathrm{Gal}(L/\mathbb{R})$ 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）

5. 证明，存在子群 $H'<\mathrm{Gal}(L/\mathbb{R})$，其指标为 2 并进一步证明 $L^{H'}=\mathbb{R}(i)$。

6. 证明代数基本定理。

5.11.8 Dirichlet 定理的特例

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 $p\equiv b \mod a$。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。

1. 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：

$$\{d\in\mathbb{Z}|d\geqslant 0,\text{存在非负整数 } n,\text{ 使得 } d\mid P(n)\}.$$

2. 令 $P(X)=\dfrac{X^a-1}{\Phi_a(X)}$。证明，存在素数 p 和整数 n，使得 $p\mid\Phi_a(n)$ 但是 $p\nmid P(n)$。

   （提示：在 $\mathbb{Q}[X]$ 中，存在 $U(X),V(X)$，使得 $U(X)P(X)+V(X)\Phi_a(X)=1$）

3. 计算 n 在 $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ 中的阶。

4. 证明，存在素数 p，使得 $p\equiv 1 \mod a$。

5. 证明，存在无限个素数 p，使得 $p\equiv 1 \mod a$。（提示：对合适的 a 使用 D4) 的结论）

5.11.9 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 $\left(\dfrac{x}{p}\right)$ 的定义如下：

$$\left(\frac{x}{p}\right)=\begin{cases}1, & x \text{ 是 } \mathbb{F}_p \text{ 中的完全平方}^{53}\\ -1, & x \text{ 不是 } \mathbb{F}_p \text{ 中的完全平方。}\end{cases}$$

1. 证明，映射 $\left(\mathbb{F}_p\right)^\times\to\{\pm1\}$，$x\mapsto\left(\dfrac{x}{p}\right)$ 是满的群同态并且 $\left(\dfrac{x}{p}\right)=x^{\frac{p-1}{2}}$（在 $\mathbb{F}_p$ 中计算）。特别地，我们得到 $\left(\dfrac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$。

2. 利用 Galois 理论计算 $\left(\dfrac{2}{p}\right)$。令 ζ 为 $\overline{\mathbb{F}_p}$ 中 8 次本元单位根。

   - 证明，$(\zeta+\zeta^{-1})^2=2$。
   - 证明，$\left(\dfrac{2}{p}\right)=1$ 当且仅当 $\mathrm{Frob}(\zeta+\zeta^{-1})=\zeta+\zeta^{-1}$。
   - 证明，$\left(\dfrac{2}{p}\right)=(-1)^{\frac{(p-1)(p+1)}{8}}$。

3. $\ell>2$ 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 $S^2=\displaystyle\sum_{x\in\mathbb{F}_\ell^\times}\sum_{y\in\mathbb{F}_\ell^\times}\left(\frac{xy}{\ell}\right)\xi^{x+y}=\sum_{x\in\mathbb{F}_\ell^\times}\sum_{z\in\mathbb{F}_\ell^\times}\left(\frac{x^2z}{\ell}\right)\xi^{x+zx}$）

4. 证明，$S\in\mathbb{F}_p$ 等价于 $\left(\dfrac{p}{\ell}\right)=1$。

5. 证明**二次互反律**：

   $$\left(\frac{p}{\ell}\right)\left(\frac{\ell}{p}\right)=(-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}.$$

5.11.10 一个 6 次多项式分裂域的 Galois 群的计算

1. 证明，X^2+X+1 是 $\mathbb{F}_2[X]$ 中唯一一个二次不可约多项式。

2. 证明，$\mathbb{F}_2[X]$ 中每个三次不可约多项式都整除 X^8+X。

3. 证明，在 $\mathbb{F}_2[X]$ 中，在 $\mathbb{F}_2[X]$ 中，X^2+X+1 乘除 X^8+X+1。计算 $P_2(X)=\frac{X^8+X+1}{X^2+X+1}$ 并证明 $P_2(X)$ 是不可约的。

4. 令 $T(X)=X^2+1\in\mathbb{Z}[X]$，$F_0(X)=X$，$F_n(X)=T\big(F_{n-1}(X)\big)$，其中，$n\geqslant 1$。证明，在 $\mathbb{Z}[X]$ 中，$T(X)-X$ 整除 $F_n(X)-F_{n-1}(X)$，其中，$n\geqslant 1$；进一步证明，在 $\mathbb{Z}[X]$ 中，$T(X)-X$ 整除 $F_3(X)-X$。

5. 证明，在 $\mathbb{Z}[X]$ 中，计算 $P(X)=\frac{F_3(X)-X}{T(X)-X}$（你可以用 $P(10)=1143745$ 来检验答案的正确性）并证明 $P(X)$ 是 $\mathbb{Z}[X]$ 中的不可约多项式。

6. 令 $\mathcal{R}=\left\{x\in\overline{\mathbb{Q}}\middle|P(x)=0\right\}$ 为 P 根的集合，L 为 P 在 $\mathbb{Q}$ 上的分裂域（不妨假设 $L\subset\overline{Q}\subset\mathbb{C}$），$G:=\mathrm{Gal}(L/\mathbb{Q})$ 为其 Galois 群。证明，$\mathcal{R}$ 可以如下描述：

$$\mathcal{R}=\left\{x\in\overline{\mathbb{C}}\middle|T(T(T(x)))=x,\text{但是 }T(x)\neq x\right\}.$$

7. 证明，对任意的 $x\in\mathcal{R}$，我们有 $T(x)\in\mathcal{R}$，从而，以下映射是良好定义的：

$$T:\mathcal{R}\longrightarrow\mathcal{R}.$$

8. 证明，$|\mathcal{R}|=6$ 并且可以将 $\mathcal{R}$ 中的元素记作是

$$\mathcal{R}=\{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6\}=\underbrace{\{\alpha_1,\alpha_3,\alpha_5\}}_{\mathcal{R}_1}\cup\underbrace{\{\alpha_2,\alpha_4,\alpha_6\}}_{\mathcal{R}_2}.$$

使得 $T(\alpha_1)=\alpha_3,T(\alpha_3)=\alpha_5,T(\alpha_5)=\alpha_1$ 而 $T(\alpha_2)=\alpha_4,T(\alpha_4)=\alpha_6,T(\alpha_6)=\alpha_2$。特别地，如果将 $\mathfrak{S}_{\mathcal{R}}$ 与 $\mathfrak{S}_6$ 等同，其中，$\alpha_i\in\mathcal{R}$ 对应着指标 i，那么，T 可以被视作是 $(1,3,5)(2,4,6)\in\mathfrak{S}_6$。

9. 令 $C_T=\left\{g\in\mathfrak{S}_6|g\cdot T=T\cdot g\right\}$ 为 T 在 $\mathfrak{S}_6$ 中的中心化子。证明，对任意的 $g\in C_T$，我们有 $g(\mathcal{R}_1)=\mathcal{R}_1,g(\mathcal{R}_2)=\mathcal{R}_2$ 或者 $g(\mathcal{R}_1)=\mathcal{R}_2,g(\mathcal{R}_2)=\mathcal{R}_1$。据此，证明以下映射是**满的**群同态：

$$\varepsilon:C_T\to\{\pm1\},\ \ \varepsilon(g)=\begin{cases}1, & \text{如果 } g(\mathcal{R}_1)=\mathcal{R}_1;\\ -1, & \text{如果 } g(\mathcal{R}_1)=\mathcal{R}_2.\end{cases}$$

其中，$\{\pm1\}$ 是 2 阶循环群。

10. 证明，$|C_T|=18$。

11. 我们可以将 $G:=\mathrm{Gal}(L/\mathbb{Q})$ 视作是 $\mathfrak{S}_{\mathcal{R}}=\mathfrak{S}_6$ 的子群。证明，$G<C_T$，$\varepsilon\big|_G:G\to\{\pm1\}$ 也是满射并且 $|G|=6$ 或 18。

12. 令 $\xi=\alpha_1+\alpha_3+\alpha_5,\eta=\alpha_2+\alpha_4+\alpha_6$，证明，$Q(X)=(X-\xi)(X-\eta)\in\mathbb{Q}[X]$。注意，不能使用本题后面的结论。

13. 证明，$Q(X)=X^2+X+3\in\mathbb{Z}[X]$。

14. 令 $H:=\mathrm{Ker}\big(\varepsilon\big|_G:G\to\{\pm1\}\big)$，证明，$L^H$ 是 $L/\mathbb{Q}$ 的唯一 2 次的中间域。进一步给出整数 d，使得该中间域为 $\mathbb{Q}(\sqrt{d})$。

15. 利用 GaloisGPT 软件，得到 P 的判别式 $\mathrm{Disc}(P)=-33$，请问它的结果是否正确并给出理由。

16. 令

$$\begin{cases}\gamma_1 &=\alpha_1\alpha_2+\alpha_3\alpha_4+\alpha_5\alpha_6,\\ \gamma_2 &=\alpha_1\alpha_4+\alpha_3\alpha_6+\alpha_5\alpha_2,\\ \gamma_3 &=\alpha_1\alpha_6+\alpha_3\alpha_2+\alpha_5\alpha_4,\end{cases}\quad\begin{cases}\delta_1 &=\alpha_1\alpha_2+\alpha_3\alpha_6+\alpha_5\alpha_4,\\ \delta_2 &=\alpha_1\alpha_4+\alpha_3\alpha_2+\alpha_5\alpha_6,\\ \delta_3 &=\alpha_1\alpha_6+\alpha_3\alpha_4+\alpha_5\alpha_2.\end{cases}$$

令 $A(X)=(X-\gamma_1)(X-\gamma_2)(X-\gamma_3)$，$B(X)=(X-\delta_1)(X-\delta_2)(X-\delta_3)$。证明，$A(X),B(X)\in\mathbb{Q}[X]$。注意，不能使用本题后面的结论。

利用 Mathematica 软件可以算得（正确的结果）

$$A(X)=X^3-3X^2-6X-28,\ \ B(X)=X^3-3X^2-6X-1.$$

17. 证明，$\mathrm{Disc}(A) = -2^2 \cdot 3^6 \cdot 11$ 而 $\mathrm{Disc}(B) = 3^6$。我们可以利用如下公式：对于多项式 $X^3 + aX + b$，$\mathrm{Disc}(X^3 + aX + b) = -4a^3 - 27b^2$

18. 证明，$G \simeq C_T$。

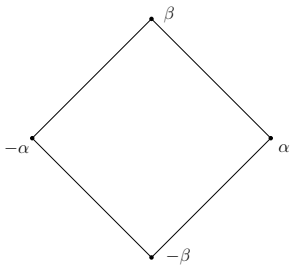
5.11.11 偶四次多项式的分裂域：Kaplansky 定理

$P(X) = X^4 + aX^2 + b \in \mathbb{Q}[X]$ 是不可约多项式，$\{\alpha, -\alpha, \beta, -\beta\} \subset \overline{\mathbb{Q}}$ 为其根，K 为 P 在 $\mathbb{Q}$ 上的分裂域，$G = \mathbf{Gal}\left(K/\mathbb{Q}\right)$。

这个题目的目标是证明 Kaplansky 定理：

$$G \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & \text{若 } b \in \mathbb{Q}^2; \\ \mathbb{Z}/2\mathbb{Z}, & \text{若 } b(a^2 - 4b) \in \mathbb{Q}^2; \\ \mathfrak{D}_4, & \text{其余情形.} \end{cases}$$

我们考虑如下的正方形：



1. 将 $\mathfrak{D}_4$ 视为上述正方形的对称群。令 r 为绕其中心的对称，s 为保持顶点 β 与 $-\beta$ 的反射，那么，$\mathfrak{D}_4$ 的 8 个元素由如下映射给出：

$$(*)\cdots\cdots \begin{cases} 1 : \alpha \mapsto \alpha,\ \beta \mapsto \beta; \quad r : \alpha \mapsto \beta,\ \beta \mapsto -\alpha; \quad r^2 : \alpha \mapsto -\alpha,\ \beta \mapsto -\beta; \quad r^3 : \alpha \mapsto -\beta,\ \beta \mapsto \alpha; \\ s : \alpha \mapsto -\alpha,\ \beta \mapsto \beta; \quad sr : \alpha \mapsto \beta,\ \beta \mapsto \alpha; \quad sr^2 : \alpha \mapsto \alpha,\ \beta \mapsto -\beta; \quad sr^3 : \alpha \mapsto -\beta,\ \beta \mapsto -\alpha. \end{cases}$$

   证明，$\mathfrak{D}_4$ 的 4 阶子群如下：

$$\{1, \sigma, \sigma^2, \sigma^3\}, \{1, s, sr^2, r^2\}, \{1, sr, sr^3, r^2\},$$

   其中，后两个子群共轭。

2. 证明，$\mathfrak{S}_4$ 的 Sylow 2-子群与 $\mathfrak{D}_4$ 同构。

3. 证明，$\mathbf{Gal}\left(K/\mathbb{Q}\right)$ 只能是 $\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 或 $\mathfrak{D}_4$。

4. 证明，$\mathbf{Gal}\left(K/\mathbb{Q}\right)$ 在 $\{\alpha, \beta, -\alpha, -\beta\}$ 上的作用可以被视作是 $(*)$ 中作用的子群。

5. 证明，$\alpha^2 - \beta^2 \notin \mathbb{Q}$。

6. 证明，$\mathbf{Gal}\left(K/\mathbb{Q}\right) \simeq \mathbb{Z}/4\mathbb{Z}$ 当且仅当 $\frac{\alpha}{\beta} - \frac{\beta}{\alpha} \in \mathbb{Q}$。

7. 证明，$\mathbf{Gal}\left(K/\mathbb{Q}\right) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 当且仅当 $\alpha\beta \in \mathbb{Q}$。

8. 证明 Kaplansky 定理。

9. 计算下列多项式的根并给出它们在 $\mathbb{Q}$ 上的分裂域的 Galois 群：

   - $X^4 - 4X^2 - 1$；
   - $X^4 - 6X^2 + 4$；
   - $X^4 + 5X^2 + 5$；
   - $X^4 - 7X^2 + 10$，此多项式与上述多项式有何不同?

5.11.12 Galois 扩张的正规基定理（无限域的情形）

假设 L/K 是有限 Galois 扩张，$P \in K[X]$ 是首一、可分的 n 次多项式，$\alpha \in L$ 为 P 的根并且 $L = K(\alpha)$（根据本原元素定理）。令 $\mathbf{Gal}\left(L/K\right) = \{g_1, \cdots, g_n\}$ 并且规定 $g_1 = 1$。令 $\alpha_i = g_i(\alpha)$，其中，$i = 1, \cdots, n$。

1. （Lagrange 插值公式）令 $Q_i(X) = \dfrac{P(X)}{P'(\alpha_i)(X - \alpha_i)} \in L[X]$。证明，
$$Q_1(X) + Q_2(X) + \cdots + Q_n(X) = 1.$$

2. 证明，当 $i \neq j$ 时，$P \mid Q_iQ_j$；当 $i \neq j$ 时，$P \mid Q_iQ_j - Q_i$。

3. 证明，$L[X]$ 系数的矩阵 $A = \left(\sigma_i\sigma_j(Q_1)\right)_{1 \leqslant i,j \leqslant n}$，满足
$$^tA \cdot A = \mathbf{I} \mod P,$$
其中，$\mathbf{I}$ 是单位矩阵。以上，对于 $Q \in L[X]$ 和 $\sigma \in \mathbf{Gal}\left(L/K\right)$，$\sigma(Q)$ 是对其系数进行作用。

4. 以下假设 K 是无限域。证明，存在 $\beta \in L$，使得 $\det\left[\sigma_i\sigma_j\big(g_1(\beta)\big)\right] \neq 0$。

5. 证明，存在 $\beta \in L$，$\{g_1(\beta), g_2(\beta), \cdots, g_n(\beta)\}$ 是 Galois 扩张 L/K 的基。

练习 5.5. p 是素数，$l \geqslant 2$（还是要求 l 是偶数?），$q = p^l$，$K = \mathbb{F}_q(T)$。给定 α 和 β 分别为 $P(X) = X^{p^2} - TX + T$ 和 $Q(X) = X^{p^2-1} - T$ 在 $\overline{K}$ 中的根。

1) 证明，P 和 Q 在 $K[X]$ 中不可约。（提示：对 $Q(X + T)$ 用 Eisenstein 判别法）

2) 证明，P 的所有根为 $\{\alpha, \alpha + \beta' | Q(\beta') = 0\}$。

3) 证明，$K(\beta)/K$ 为 Galois 扩张并计算其 Galois 群。

4) 令 L 为 P 在 K 上的分裂域。证明，$L = K(\alpha, \beta)$，$K(\beta)/K$ 为 Galois 扩张并且其 Galois 群为 $p^2(p^2 - 1)$ 阶的。

5) 证明，$\mathbf{Gal}\left(L/K(\beta)\right) \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$。（提示：利用 2) 说明该群中的元素的阶至多为 p）。

6) 证明，L/K 是可解的（能否进一步写出 P 的根的具体表达式?）。

5.11.13 练习题

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 $f : K \to L$ 都是多项式，即证明对任意的 $x \in K$，
$$f(x) = \sum_{a \in K} \big(f(a)(1 - (x-a)^{q-1})\big).$$

2. K 是域，考虑如下的域扩张：
$$\begin{array}{c} L = K(X) \\ | \\ M = K\left(\frac{X^3}{X+1}\right) \\ | \\ K \end{array}$$
   1) 证明，$M \neq L$。
   2) 令 $f(X) = \frac{X^3}{X+1}$，证明，$M[T]$ 中的多项式 $T^3 - f \cdot T - f$ 不可约。
   3) 计算 $[L : M]$。

3. 试找出域扩张 $\mathbb{Q}(\sqrt[4]{7})/\mathbb{Q}$ 所有的中间域。

4. 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。

5. 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。

6. 计算 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ 在 $\mathbb{Q}$ 上的极小多项式。

7. p 是奇素数，试计算 $\mathbb{Q}(\cos(\frac{2\pi}{p}))/\mathbb{Q}$ 的扩张次数。

8. 给定单代数扩张 $K(x)/K$。证明，如果 $[K(x) : K]$ 是奇数，那么，$K(x) = K(x^2)$。

9. 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）

10. 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。

11. K 是域，$P \in K[X]$ 并且 $\deg(P) = n$，L 是由 $P(X)$ 给出的一个分裂域。证明，$[L : K] \mid n!$。

12. K 是域并且是可数的。证明，$K[X]$ 也是可数的。我们记 $K[X] = \{P_1, P_2, \cdots, P_n, \cdots\}$ 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，$L := \bigcup_{n \geqslant 1} K_n$ 是 K 的一个代数闭包。

13. 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。[54]

14. K 是域，$P(X) \in K[X] - K$，L 为 K 的分裂域。证明，$[L : K] \mid n!$，其中，$d = \deg(P)$。

15. 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 $\alpha \in \overline{\mathbb{F}}$ 是 P 的根，那么，对任意的 $a \in \mathbb{F}_p$，$\alpha + a$ 也是根）

16. 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 $\sigma \in \mathrm{Aut}_K(L)$，使得 $P_1^\sigma = P_2$。

17. 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。

18. L/K 是正规扩张，$P(X) \in K[X]$ 是不可约多项式，$Q_1(X), Q_2(X)$ 是 $P(X)$ 在 $L[X]$ 中的两个首一的不可约因子。证明，存在 $\sigma \in \mathbf{Aut}_K(L)$，使得 $(Q_1)^\sigma = Q_2$。请进一步给出反例：如果 L/K 不是正规扩张，那么结论并不成立。

19. L/K 是代数扩张，那么 L/K 是正规的等价于对任意的不可约多项式 $P(X) \in K[X]$，$P(X)$ 在 $L[X]$ 中的所有不可约因子的次数均相等。

20. 考虑如下扩张：

$$\mathbb{Q} \text{ —— } \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \text{ —— } \mathbb{C}.$$

试计算 $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})/\mathbb{Q}$ 在 $\mathbb{C}$ 中的正规闭包 N 并计算 $[N : \mathbb{Q}]$。证明，$N/\mathbb{Q}(\sqrt{2})$ 是正规扩张并给出所有 $\mathbf{Aut}_{\mathbb{Q}(\sqrt{2})}(N)$ 中的元素。

21. 域 K 的特征为 p，L/K 是有限扩张并且 $L^p \subset K$。

1) 证明，L/K 是纯不可分扩张。

2) 如果存在 $\{x_1, \cdots, x_n\} \subset L$，使得

$$K \subsetneq K(x_1) \subsetneq K(x_1, x_2) \subsetneq \cdots \subsetneq K(x_1, x_2, \cdots, x_{n-1}) \subsetneq K(x_1, x_2, \cdots, x_{n-1}, x_n) = L,$$

那么，$[L : K] = p^n$。特别地，满足以上条件的 $\{x_1, \cdots, x_n\}$ 的元素个数由 L/K 决定。

---

[54] 令 $K = K_1 \cap K_2$。对任意首一的、不可约多项式 $P(X) \in K[X]$，假设 $\alpha \in L$ 为 P 的一个根，为了证明 P 的所有根均在 L 中，我们对 $P(X)$ 在 $L[X]$ 中进行因式分解：

$$P(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_m) \cdot Q(X),$$

其中，$\alpha_1 = \alpha, \cdots, \alpha_m \in L$ 并且 $Q(X) \in L[X]$ 在 L 中没有根。以上分解显然是唯一的，剩下只要说明 $Q(X) = 1$ 即可。

我们在 $K_1[X]$ 中分解 $P(X)$ 为首一的不可约多项式之积：

$$P(X) = R_1(X)^{\alpha_1} \cdots R_l(X)^{\alpha_l} Q_1(X)^{\beta_1} \cdots Q_k(X)^{\beta_k},$$

其中，$R_1(X), \cdots, R_l(X), Q_1(X)^{\beta_1}, Q_k(X)$ 均为 $K_1[X]$ 中首一的不可约多项式，指标 $\alpha_1, \cdots, \alpha_l$ 和 $\beta_1, \cdots, \beta_k$ 均大于 0 并且 $R_1, \cdots, R_l$ 在 L 中有根但是 $Q_1, \cdots, Q_k$ 在 L 中没有根。根据 L/K_1 是正规扩张，则 $R_1(X)^{\alpha_1} \cdots R_l(X)^{\alpha_l}$ 在 L 中分裂但是 $Q_1(X)^{\beta_1} \cdots Q_k(X)^{\beta_k}$ 在 L 中没有根。利用以上 P 在 $L[X]$ 中进行因式分解的唯一性，我们得到

$$Q(X) = Q_1(X)^{\beta_1} \cdots Q_k(X)^{\beta_k} \in K_1[X].$$

类似的，$Q(X) \in K_2[X]$，从而，$Q(X) \in K[X]$。若 $Q \neq 1$，则 $Q \mid P$，这与 P 是 $K[X]$ 中的不可约多项式矛盾。

22. K 是特征为 p 的完美域，$f \in K(X)$ 并且 $f \notin K$。证明，$K(X)/K(f)$ 是可分的当且仅当 $f \notin K^p$。

23. 域 K 的特征为 p，扩张 L/K 是纯不可分的并且 $[L:K] = p^n$。证明，对任意的 $x \in L$，$x^{p^n} \in K$。

24. 给定域 K 和多项式 $P(X) \in K[X]$，L 为其分裂域，试计算 $L, [L:K]$ 和 $|\mathbf{Aut}_K(L)|$，其中

    1) $K = \mathbb{F}_3, P(X) = X^3 + 2X + 1$;

    2) $K = \mathbb{F}_p, P(X) = X^{p^8} - 1$;

    3) $K = \mathbb{F}_3(T), P(X) = X^3 - T$。

25. 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。

26. 证明，$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5})$。（提示：先计算 $\mathbf{Gal}\left(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}\right)$）

27. 给定域扩张 $\mathbb{Q} \subset K \subset \mathbb{C}$，$K/\mathbb{Q}$ 是 Galois 扩张。证明，K 在复共轭下不变。

28. 给定 Galois 扩张 L/K，M 为其中间域，N 为 M 在 L 中的正规闭包[55]证明，

$$\mathbf{Gal}\left(L/N\right) = \bigcap_{\sigma \in \mathbf{Gal}\left(L/K\right)} \sigma \cdot \mathbf{Gal}\left(L/M\right) \cdot \sigma^{-1}.$$

29. 给定 Galois 扩张 $L/\mathbb{K}$，M 为其中间域，H 为其在 Galois 对应下所对应的 $\mathbf{Gal}\left(L/K\right)$ 的子群，即 $M = L^H$。令 $\mathrm{N}_{\mathbf{Gal}\left(L/K\right)}(H)$ 为 H 在 $\mathbf{Gal}\left(L/K\right)$ 中的正规化子，$M_0 = L^{\mathrm{N}_{\mathbf{Gal}\left(L/K\right)}(H)}$。证明，$M/M_0$ 为 Galois 扩张。进一步证明，若 $M' \subset M$ 为 M/K 的中间域并且 M/M' 为 Galois 扩张，则 $M' \supset M_0$。

30. L/K 是有限正规扩张。如果除了 L 和 K 之外，该扩张没有其它的中间域，证明，$[L:K]$ 是素数。

    给定某个 4-次 $\mathbb{Q}$-系数不可约多项式 $P(X)$，使得其分裂域 $L/\mathbb{Q}$ 的 Galois 群同构于 $\mathfrak{S}_4$。证明，存在其中间域 M，使得 $[M:K] = 4$ 并且 M/K 没有非平凡的中间域。

31. K 是有限域。证明，对任意的 $n \geqslant 1$，存在 n-次不可约多项式。

32. $\mathbb{F}_q$ 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）

33. 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 $\mathrm{Gal}(L/K)$ 中的一个 p 阶元 σ，使得

$$P(X) = \big(X - \alpha\big)\big(X - \sigma(\alpha)\big) \cdots \big(X - \sigma^{p-1}(\alpha)\big).$$

    进一步证明，如果存在 P 的另一个根 $\beta \in K(\alpha)$，那么，$L = K(\alpha)$。

34. $L/\mathbb{Q}$ 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，$4 \nmid [L:\mathbb{Q}]$。

[55]这是 L 中包含 M 并且在 K 上正轨的最小子域，它由 K 添加上 M 中元素的在 K 上的极小多项式的所有根生成。

35. K 是域，$P \in K[X]$ 是 n 次可分多项式，L 为 P 在 K 上的分裂域。通过对 P 的根的作用，我们将 $\mathbf{Gal}(L/K)$ 视为 $\mathfrak{S}_n$ 的子群。证明，

$$\mathrm{Gal}(L/K) < \mathfrak{A}_n \quad \Leftrightarrow \quad \mathrm{Disc}(P) \in K^2.$$

36. 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，

$$\mathrm{Gal}(L/K) = \begin{cases} \mathfrak{A}_3, & \text{如果 } \mathrm{Disc}(P) \text{ 是 } K \text{ 中的完全平方;} \\ \mathfrak{S}_3, & \text{如果 } \mathrm{Disc}(P) \text{ 不是 } K \text{ 中的完全平方.} \end{cases}$$

37. L/K 是有限 Galois 扩张并且 $\mathrm{Gal}(L/K) \simeq \mathfrak{S}_n$，其中，$n \geqslant 5$。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 $\deg(P) \geqslant n$。如果 $n = 4$，是否有反例?

38. 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 $\mathrm{Gal}(L/K)$ 为交换群，$x \in L$ 为 P 的一个根。证明，$L = K(x)$。

39. 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) $3X^5 - 12X^3 + 12X - 1$;

40. $p_1, p_2, \cdots, p_d$ 是 d 个不同的素数，$L = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \cdots, \sqrt{p_d})$。证明，$L/\mathbb{Q}$ 是 Galois 扩张并计算其 Galois 群。据此证明，$\sqrt{15} \notin \mathbb{Q}(\sqrt{10}, \sqrt{42})$。

A 有关集合的回顾

A.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 $\overline{a}$（或者 $[a]$）表示

$$\overline{a}=[a]=\big\{b\in A|b\sim a\big\}\subset A.$$

我们将这样的一个集合称作是 $\sim$ 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，$a\in\overline{a}$；如果 $a\sim b$，则 $\overline{a}=\overline{b}$；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：

$$A=\coprod\overline{a}.$$

反之，假设 $A=\coprod_{i\in I}A_i$ 是 A 的一个划分，即 $\bigcup_i A_i=A$ 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 148. *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

$$A\big/_{\sim}=\big\{\overline{a}\mid a\in A\big\}.$$

我们有自然商映射：

$$\pi:A\to A\big/_{\sim},\quad a\mapsto\pi(a)=\overline{a}.$$

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 149 (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 $f:A\to B$，存在映射 $\widetilde{f}:A\big/_{\sim}\to B$ 使得如下图表交换（即 $f=\widetilde{f}\circ\pi$）*

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & B \\ \downarrow{\scriptstyle\pi} & \nearrow{\scriptstyle\widetilde{f}} & \\ A\big/_{\sim} & & \end{array}$$

当且仅当对任意的 $a\sim a'$，我们有 $f(a)=f(a')$。

证明： 假设 $f=\widetilde{f}\circ\pi$。对于 $a\sim a'$，按定义，$\pi(a)=\pi(a')$，所以，$\widetilde{f}(\pi(a))=\widetilde{f}(\pi(a'))$，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 $\overline{a}\in A\big/_{\sim}$，我们令 $\widetilde{f}(\overline{a})=f(a)$。容易看出 $\widetilde{f}$ 是良好定义的并且满足要求。 □

注记 A.1. 满足命题要求的 $\widetilde{f}$ 是唯一的。这个命题会始终贯穿我们的课程（用来构造映射）。

A.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 $a\preceq b$，并且如下的性质成立：

1)（自反性）对任意的 $a\in A$，$a\preceq a$（或者对任意的 $a\in A$，$(a,a)\in\mathcal{O}$）；

2)（传递性）如果 $a\preceq b$，$b\preceq c$，那么，$a\preceq c$（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 $a\preceq b$，$b\preceq a$，那么，$a=b$（或者如果 $(a,b),(b,a)\in\mathcal{O}$，那么，$a=b$。

注记 A.2. 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 $a\preceq b$ 和 $b\preceq a$ 可能都不成立。如果对任意的 $a,b\in A$，$a\preceq b$ 和 $b\preceq a$ 至少一者成立，我们称之为**全序集**。

给定偏序集 $(A,\preceq)$ 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 $s\preceq a$，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 $(A,\preceq)$，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 150 (超限归纳法)**.** $(A,\preceq)$ 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 $x\prec a$ 可以推出 $x\in S$，那么，这样的 $a\in S$。那么，$S=A$。

注记 A.3. 符号 $x\prec a$ 指的是 $x\preceq a$ 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 $x\preceq a_0$（$x\neq a_0$），由于 x_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 $(A,\preceq)$，$I\subset A$ 是子集，如果对任意 $x\in I$，对任意的 $y\preceq x$，都有 $y\in I$，我们就称 I 是一个**左半轴**。如果 $\preceq$ 是全序，对任意的 $x\in A$，$A_x=\{y\in A|y\prec x\}$ 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 $s\preceq s'$，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 151 (Zorn 引理)**.** $(A,\preceq)$ 是偏序集，如果任意全序子集[56]$S\subset X$ 都有上界，那么，A 有极大元。

证明: 用反证法，假设 A 中无极大元。令 $\mathcal{S}=\big\{S\subset A\big|S\text{是全序子集}\big\}$。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

$$\mathcal{T}=\big\{(S,b)\big|S\in\mathcal{S},\ b\text{ 是 }S\text{ 的上界并且 }b\notin S\big\}.$$

我们考虑满射

$$\pi:\mathcal{T}\to\mathcal{S},\quad (S,b)\mapsto S.$$

根据选择公理[57]，存在映射 $\ell:\mathcal{S}\to\mathcal{T}$，使得 $\ell\circ\pi=\mathrm{id}_{\mathcal{S}}$，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：

[56]即在 S 我们仍然使用 A 的偏序，此时对 S 而言它是全序集

[57]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 $f(x)\in F(x)$。

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 $\mathfrak{I} = \left\{ I \subset W \cap W' \middle| I \text{ 是 } W \text{ 中的左半轴也是 } W' \text{ 中的左半轴} \right\}$，很明显，$J = \cup_{I \in \mathfrak{I}} I \in \mathfrak{I}$ 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，$J \cup \{w\} \in \mathfrak{I}$，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，$x \preceq v$。

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 $y \in W$，$y \prec x$，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。 □