群与 Galois 理论

清华大学, 2024 年秋季学期

于 品

2024 年 9 月 30 日

摘要

通过这份讲义，您什么也学不到。

目录

1 域扩张与经典几何问题 **4**
1.1 域与线性空间 4
1.2 域扩张 7
1.3 应用：三等分已知角 10

2 群、环和模的定义 **14**
2.1 群的定义和例子 14
2.1.1 补充：正二十面体的对称 17
2.2 群同态 19
2.3 正规子群与商群 20
2.4 环的定义 23
2.5 模的定义 26
2.6 对称群 $\mathfrak{S}_n$ 27
2.7 习题 34
2.7.1 A. 乘积结构 34
2.7.2 B. 域的有限乘法子群是循环群 35
2.7.3 C. 线性群中元素的阶的几个命题 36
2.7.4 D. 有限群乘积的消去定理 36
2.7.5 练习题（不提交） 37
2.7.6 较难问题提示与解答 39

3 群与群作用 **40**
3.1 基本定义 40
3.2 群作用的基本例子 42
3.2.1 几何上的例子 42
3.2.2 群作用在由自身所构造的对象上的例子 44
3.3 群作用的应用举例 46
3.3.1 双传递性与单群的 Iwasawa 判定 46
3.3.2 Burnside 引理 50

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），我们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)，我们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

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

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 $X = u + v$。

[1] $k = 0$ 所对应的求根公式最早由 del Ferro 发现。

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

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

从而，

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

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

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

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，$\overline{k} = \{m \in \mathbb{Z} | m \equiv k \ (\mathrm{mod} p)\}$，$k = 0, \cdots, p-1$。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 $m \equiv n \ (\mathrm{mod} p)$，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 $|\mathbb{F}_p| = p$。

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

$$v_1 + v_2 = v_2 + v_1.$$

[2]如果域 K 的元素个数是有限的，就称 K 是有限域。

– 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

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

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 $v = k_0 e_0 + k_1 e_1 + \cdots + k_n e_n \in V^\times$，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

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

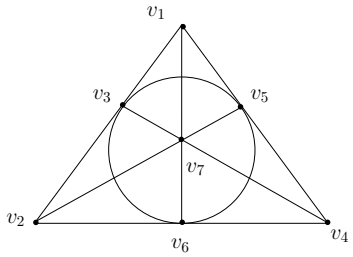
（这个等式被称作是 q-二项式展开，将 q 看作是变量，试考虑 $q \to 0$ 的极限。）

例子 1.5. 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 $\mathbf{P}^2(\mathbb{F}_2)$：

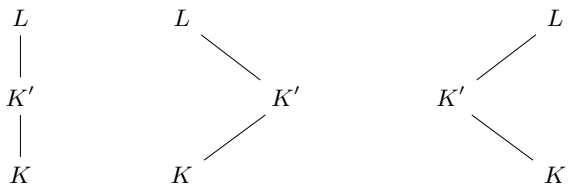


以上图中有 6 条直线段，每条这样的线段上的三个点都是共线的；图中圆形所经过的三个点也是共线的。

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 $\bigcap_{i\in I} K_i'$ 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

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

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

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

[3]在包含关系下

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 $\sum\limits_i x_iv_i = x$；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：

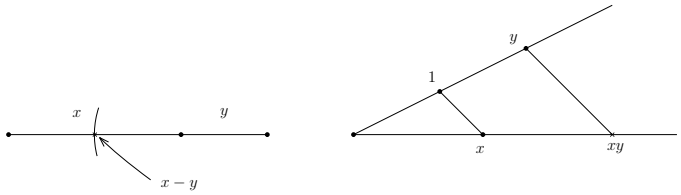
- P 是两条 $\mathscr{S}$-直线的唯一交点；
- P 是一条 $\mathscr{S}$-直线和一个 $\mathscr{S}$-圆的交点；
- P 是两个 $\mathscr{S}$-圆的交点；

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**。

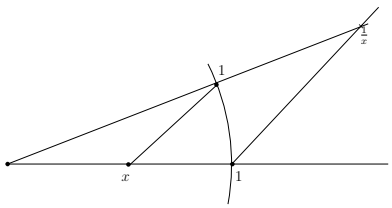
$\mathbb{R}$ 中尺规可作的数满足如下三条性质：

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：



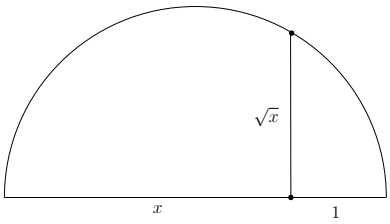
其中，右图中需要做过 y 点的平行线。

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，

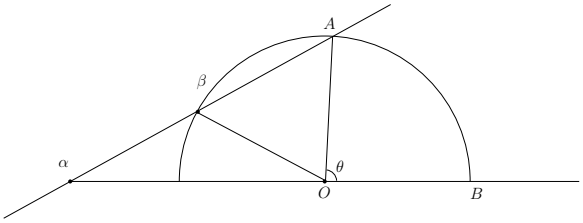
$$4x^3 - 3x - \frac{1}{2} = 0.$$

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

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

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

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

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：

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

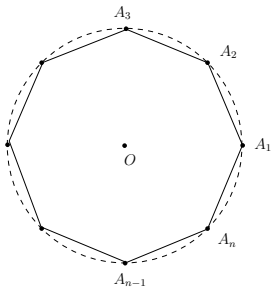
令 $r = \rho_1$，那么，$\rho_k = r^k$。

- 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_kA_{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）：

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



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，

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

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 $x=r^ks$，$y=r^ls^b$，其中，$b=0$ 或 1（若 $x=r^k$，显然 $xy\in\mathfrak{D}$）。根据 $srs=r^{-1}$，我们有

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

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 ${s'}_1^{n'_1}\cdots {s'}_{k'}^{n'_{k'}}$，它们相乘得

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

如果 $s_k={s'}_1$，我们可以将采取上述替换，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。

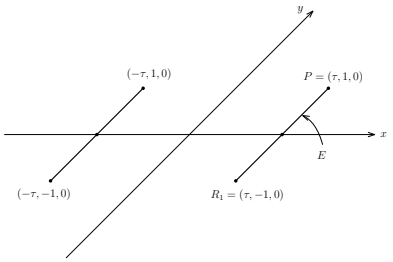
G 的**中心**Z(G) 是群中与所有元素均交换的元素组成的子群，按定义，我们有

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

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。

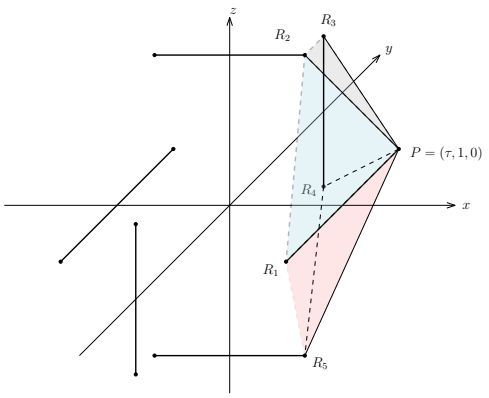
考虑三维空间 $\mathbb{R}^3$。在 $z = 0$ 定义的平面上放置两条线段：线段 E 与 y-轴平行，端点为 $P = (\tau, 1, 0)$ 和 $R_1 = (\tau, -1, 0)$，其中点落在 x 轴上；第二条线段与 E 关于 y 轴对称，其端点为 $(-\tau, 1, 0)$ 和 $(-\tau, -1, 0)$。



对以上四个端点 $(\pm\tau, \pm 1, 0)$ 的 x, y, z 坐标进行轮换可以得到 12 个点：

$$\{(\pm\tau, \pm 1, 0),\ (\pm 1, 0, \pm\tau\},\ (0, \pm\tau, \pm 1)\}$$

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 $2\times10=20$ 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 $1\times15=15$ 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。

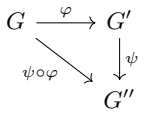
注记 2.10. 若有 G_1 到 G_2 的群同构，就称它们是**同构的**并记作是 $G_1\simeq G_2$。注意到这个符号并不精确，因为没说明 φ 是如何定义的。实际上，群 G_1 和 G_2 同构而它们之间的同构映射 φ 可能不唯一。

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，$\mathrm{Ker}(\log)=\{1\}$。
- $\mathrm{mod}\ n$ 映射。考虑除 n 的余数给出自然的群同态
$$\mathbb{Z}\xrightarrow{\mathrm{mod}\ n}\mathbb{Z}/n\mathbb{Z},\qquad k\mapsto\overline{k}.$$
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：

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

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：

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

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。*

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

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

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

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 $\mathbb{Z}/n\mathbb{Z}$ 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，$\mathbb{Z}/n\mathbb{Z} \simeq \langle g\rangle$。 □

我们把与 $\mathbb{Z}/n\mathbb{Z}$ 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：

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

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

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

和

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

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 $1_A \cdot g = g \cdot 1_A$；

[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。

3) 乘法分配律成立：对任意的 $a_1, a_2, a_3 \in A$，有

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

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：

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

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 $x=\sum_{g\in G}x_ge_g, y=\sum_{h\in G}y_he_h\in K[G]$（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：
$$x\cdot y=\sum_{g\in G}\sum_{h\in G}x_gy_he_{gh}.$$
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

$$\varphi(a+_1b)=\varphi(a)+_2\varphi(b),\quad \varphi(a\cdot_1b)=\varphi(a)\cdot_2\varphi(b),$$

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

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

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

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

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

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

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

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：

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

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。*

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

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 $\varphi:1\mapsto\overline{0},\ g\mapsto\overline{1}$。

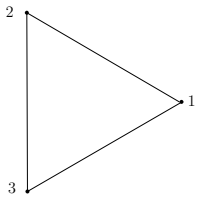
例子 2.35. $\mathfrak{S}_3$ 有 6 个元素，罗列如下：

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

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：

$$\mathrm{Int}(g)(\sigma)=g\sigma_1g^{-1}\cdot g\sigma_2g^{-1}\cdots g\sigma_mg^{-1}.$$

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：

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

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**：

$$\varepsilon:\mathfrak{S}_n\to\{\pm1\},\quad \sigma\mapsto\begin{cases}1, & \sigma\text{ 是偶置换;}\\ -1, & \sigma\text{ 是奇置换.}\end{cases}$$

将 $\{\pm1\}$ 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：

$$\mathfrak{A}_n=\mathrm{Ker}\big(\varepsilon:\mathfrak{S}_n\to\{\pm1\}\big).$$

这是偶置换的集合。

注记 2.29. 我们有如下正合列

$$1\to\mathfrak{A}_n\xrightarrow{\subset}\mathfrak{S}_n\xrightarrow{\varepsilon}\{\pm1\}\to 1.$$

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 $\mathbf{Aut}(\mathfrak{S}_6)\big/\mathrm{Im}(\mathrm{Int})$ 中至多有两个元素。从而，$\mathbf{Out}(\mathfrak{S}_6)=1$ 或者 $\mathbb{Z}\big/2\mathbb{Z}$。

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

2.7 习题

2.7.1 A. 乘积结构

A1) $(G_1, \cdot_1)$ 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**。

A2) 证明，投影映射

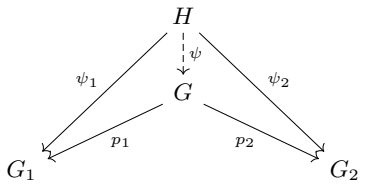
$$\pi_1 : G_1 \times G_2 \to G_1, \quad (g_1, g_2) \mapsto g_1,$$

和

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

是群同态。它们的核是什么?

A3) (泛性质) 给定群 $(G_1, \cdot_1)$ 和 $(G_2, \cdot_2)$。证明, 存在唯一的[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 $p_i \circ \psi = \varphi_i$ $(i = 1, 2)$。



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)

A4) 给定互素的正整数 n_1 和 n_2。利用 A3) 证明，

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

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。

A5) C_1 和 C_2 是两个有限阶的循环群，那么，$C_1 \times C_2$ 是否是循环群?

A6) $(A_1, +_1, \cdot_1)$ 和 $(A_2, +_2, \cdot_2)$ 是环。我们在 $A_1 \times A_2$ 上如下定义加法 $+$ 和乘法 $\cdot$:

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

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

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

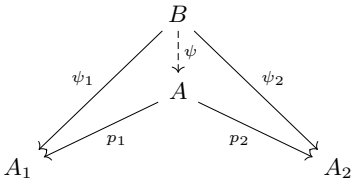
和

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

是环同态。

[7]在同构的意义下

A7)（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 $p_i \circ \psi = \varphi_i$（$i = 1, 2$）。



A8) 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）

A9) A 和 B 是环，$A^\times$ 和 $B^\times$ 是它们的乘法可逆元所构成的（乘法）群。证明，我们有群同构

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

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 B. 域的有限乘法子群是循环群

给定正整数 n，Euler 的 ϕ-函数给出 $1, \cdots, n$ 中与 n 互素的数的个数：

$$\phi(n) = \big|\{1 \leqslant k \leqslant n \big| (k, n) = 1\}\big|.$$

B1) 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。

B2) 证明，ϕ 具有如下乘性：对任意互素的正整数 n 和 m，有

$$\phi(nm) = \phi(n)\phi(m).$$

进一步，如果 $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ 是它的素因子分解，其中，p_i 为不同的素数而指标 α_i 均为正整数，证明：

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

B3) 证明，对任意正整数 n，对任意与 n 互素的整数 a，有 $a^{\phi(n)} \equiv 1 \ (\text{mod} n)$。特别地，当 p 为素数时，这给出了 Fermat 小定理。

B4)（有限循环群子群的分类）证明，作为加法群，对每个 n 的因子 d，$\mathbb{Z}/n\mathbb{Z}$ 恰有一个阶为 d 的循环子群 C_d。进一步，$\mathbb{Z}/n\mathbb{Z}$ 的每个子群均形如 C_d，其中，$d|n$。

B5) 证明，对任意的正整数 n，我们有公式

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

B6) K 是域，$G < K^\times$ 是有限群，$|G| = n$。对任意的 $d|n$，令 G_d 为 G 中阶为 d 的元素组成的集合。证明，

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

[8]在同构的意义下

[9]请与 A4) 仔细对比

B7) 证明，G 是循环群。

B8) 证明，$\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ 是循环群，其中，p 是素数。

B9) 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：

- 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 $\overline{l}\in\left(\mathbb{Z}/p^m\mathbb{Z}\right)^\times$，使得 $\langle\overline{l}\rangle=\left(\mathbb{Z}/p^m\mathbb{Z}\right)^\times$。

B10) 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）

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2^{m-2}\mathbb{Z}\longrightarrow\left(\mathbb{Z}/2^m\mathbb{Z}\right)^\times,\quad (a,b)\mapsto(-1)^a5^b \mod 2^m.$$

是群同构。

B11) (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 $\overline{l}$ 都被称为 n 的**原根**。

2.7.3 C. 线性群中元素的阶的几个命题

C1) 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，$\mathbf{GL}(n;\mathbb{Z})=\left\{A\in\mathbf{M}_n(\mathbb{Z})\middle|\det(A)=\pm1\right\}$。
- 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 $\left|\mathrm{ord}(A)\right|\leqslant C_n$。

C2) 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 $P(X)=\sum_{k=0}^{n}a_kX^k$，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 D. 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：

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

D1) 证明如下等式，其中，以下是对所有 G 的正规子群 H 来求和：

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

D2) 证明，对每个 G 的正规子群 H 存在整数 λ_H，使得

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

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

D3) 假设 G_1, G_2, G' 是有限群并且 $G_1 \times G' \simeq G_2 \times G'$。证明，$I(G_1, G') = I(G_2, G')$。

D4)（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 $G_1 \simeq G_2$。

D5) 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（不提交）

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。
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 $K \lhd G$。

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

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：

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

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：

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

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

$$(G/K)/(H/K) \xrightarrow{\simeq} G/H.$$

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

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

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 $G \to G/N$ 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

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

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，$G/K \simeq H$。

35. 请给出 8 阶群（在同构意义下）的清单。

2.7.6 较难问题提示与解答

3 群与群作用

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：

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

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

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

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，

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

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

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

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，

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

是群同态。

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

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

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，

$$g(e_1+e_2)=\lambda_1e_1+\lambda_2e_2=\lambda_1\left(e_1+\frac{\lambda_2}{\lambda_1}e_2\right)$$

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

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

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 $\mathbb{F}_5=(\mathbb{Z}\big/5\mathbb{Z},+,\cdot)$，$\mathbf{P}^1(\mathbb{F}_5)$ 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)**.** 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 $\mathfrak{A}_5$，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 $\mathfrak{S}_Y=\mathrm{Stab}(g_0H)$）。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 ${}^{G\curvearrowright}X$ 是传递的。另外，双传递的定义等价于说 ${}^{G\curvearrowright}(X\times X)$ 恰好有两个轨道 Δ 和 $X\times X-\Delta$。

[11]参见第二次作业的 B5)

练习 3.2. 给定传递的群作用 $^{G}\curvearrowright X$，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。

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

$$t'=gtg^{-1}=gxg^{-1}\cdot gyg^{-1}\cdot\big(gxg^{-1}\big)^{-1}\cdot\big(gyg^{-1}\big)^{-1}.$$

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，

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