简明代数学

Eiko (eikochanowo@outlook.com)

本书的目的是带领读者了解并理解群，环，模等代数结构。本书希望以原理性的方式讲述，使读者明白基本的原理，并能理解整个理论，而不是完全的平铺直叙。其中穿插了许多练习，可以帮助读者熟悉概念并检查自己的理解。有一定难度的问题我们用难度星级 ★ 标示出来了，★ 的个数代表它们的难度 (难度分为 0,1,2,3,4,5 星)。0 星的题目都是可以立即想出来的，读者看几眼就能知道答案的那种。看到 0 星题目时一定要立即想一想，这可以用于检查对概念的理解，想不出来就应该回顾前面的内容。有些练习事实上是简单而有一定重要性或有用的结论，读者通过自己的思考，可以对它们有更好的理解和印象。

最后更新：January 23, 2024

Contents

CHAPTER 1

对称现象与群

1. 认识对称

在浩瀚无边的宇宙中，存在着无数缤纷复杂的对称现象。对称这个词我们不陌生，比如我们常说圆既是个轴对称图形，又是个中心对称图形，它还是“旋转”对称的；（等边）三角形是轴对称的，它有三条对称轴，不仅如此，事实上我们感觉到：三角形从三个不同的方向看过去，是一样的，这似乎也是一种对称性……那么什么是对称呢?

我们需要把对称现象作一个高度的概括。不难发现，可以以一种统一的方式来重新理解上面的几个例子：对圆作对称轴反射变换、旋转变换，或者是中心对称变换，即映射 $(x, y) \mapsto (-x, -y)$，整个圆又回到了原来的样子。对（等边）三角形作对称轴反射变换、120 度旋转变换，三角形没有发生变化。

于是我们可以说，所谓某个对象的某种对称，就是指某种变换（映射），它保持整个对象不变。但是一般来说，这种变换要有所限制，通常是只考虑从某个大的比较正常/自然的映射空间中选取一些保持它不变的映射。不能是太烂的映射，要不然可选的映射太多了。对于这整个三角形来说，我们所考虑的仅仅是把它看做不可切割的刚体的变换，那些会割裂三角形的映射按照这种说法也可以看成某种对称，但是我们不予考虑。在这种考虑下，一个（等边）三角形的对称事实上只需要看它的三个顶点 1,2,3 如何运动。比如 $(1, 2, 3) \mapsto (2, 3, 1)$ 的变换就是某种旋转，而 $(1, 2, 3) \mapsto (1, 3, 2)$ 则是某种轴对称。

1.1. 对称的本质属性. 我们现在用数学抽象的记号来书写我们刚才的讨论。我们首先有一个可能具有某些对称性的对象 X，在上面有一些对称，也就是一些变换 $T_1, T_2, \ldots$。它们作用在 X 上使整个 X 不变，也就是说

$$T_i(X) = X.$$

一个自然的道理是任何对象都有一种对称，其实就是啥也不干。这个啥也不干的恒等映射我们记作 1。这是对称的本质属性之一。既然是变换（映射）的话，它们之间必然可以复合，复合运算也必然满足结合律。我们很容易发现，对称之间的复合一定也是对称。用稍微抽象一点的语言来说，这个朴素（这是对称的本质属性之二）的道理就是

$$T_i \circ T_j(X) = T_i(T_j(X)) = T_i(X) = X$$

（后面的大部分时间里，我们将省略复合的符号 $\circ$，直接写成 T_iT_j.）这个简单的式子说明如何用两个对称来“制造”新的对称：把它们复合起来一定还是 X 的对称!作为最简单的例子，我们还是可以考察一下等边三角形。我们知道，旋转 120 度的变换可以作用两次，即 $\sigma \circ \sigma = \sigma^2$，这事实上是某种旋转 240 度的变换。作用三次，这事实上就相当于什么也没干。不妨用 σ 来表示旋转（不妨说是逆时针）120 度的变换，我们已经发现 $\sigma \circ \sigma \circ \sigma = 1$ 即单位映射，这也就是

$$\sigma^3 = 1$$

值得注意的是，就像映射的复合不一定交换一样，没有任何理由表明对称的复合一定会交换，即不一定有 $T_iT_j = T_jT_i$。对称还有一种本质属性。那就是每一种对称变换一定可以反过来进行！也就是任意一种对称 T，有一种对应于它的反对称，我们把它记作 T^{-1}，称它为 T 的逆，使得 $T^{-1} \circ T = 1$。互逆是相互的关系，你是我的逆，我也是你的逆，所以必须也有 $T \circ T^{-1} = (T^{-1})^{-1} \circ T^{-1} = 1$。比如说 σ 的反操作就是顺时针旋转 120 度。而这事实上与 σ^2 无异，这一点可以通过对式子 $\sigma^3 = 1$ 两边同时复合一个 σ^{-1} 看出来：

$$\sigma^{-1}\sigma^3 = \sigma^{-1} = \sigma^2.$$

如果我们用 $S(X)$ 来表示 X 上的所有对称变换的集合的话，以上讨论就是说：

(1) $1 \in S(X)$.
(2) $a, b \in S(X) \Rightarrow ab \in S(X)$.
(3) $a(bc) = (ab)c$.
(4) $a \in S(X) \Rightarrow$ 存在 a 的逆 $b \in S(X), ab = ba = 1$.

事实上，我们把这样一个集合 $S(X)$ 称为**群**，即 X 的对称群。

2. 等边三角形的对称群

等边三角形的对称，有旋转，也有轴对称，事实上它有三种不同的轴对称，不妨记其中以纵轴为对称轴的反射变换是 τ。也有两种不同的旋转 $\sigma, \sigma^2 = \sigma^{-1}$（一个逆时针转 120 度，一个顺时针转 120 度），还有一个啥也不干的对称 1。如前，我们以 1,2,3 记三角形的三个顶点（不妨把等边三角形平放，上面的顶点定为 1，右下的为 2，左下的为 3）。那么每一个对称事实上都是一个从 $\{1,2,3\}$ 到 $\{1,2,3\}$ 的映射 f。别忘了，作为一个对称，f 需要有逆，所以 f 得是单满射。这样的 f 有多少个呢？这只需要决定 $f(1), f(2), f(3)$ 的值就好了。一共有 6 种可能的排列，所以三角形上最多只能有 6 个对称！那实际上它有多少个呢？每一个这样的 f 都是三角形的一个对称吗？的确是！我们将用如下记号

$$\begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix}$$

来表示把 1 映到 a，把 2 映到 b，把 3 映到 c 的映射。很容易发现

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

别忘了我们说过，对称变换可以复合，我们试着复合一下 σ 与 τ，看看会发生什么？通过计算给出

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

有趣的是这次复合没有产生新的东西，$\sigma\tau$ 这个对称是另一种轴对称，保持顶点 2 不变的轴对称。值得注意的是 $\sigma\tau \neq \tau\sigma$，读者可以验证这一点。我们可以验证，整个三角形的对称群有如下 6 个不同的元素：（这刚好构成了 {1,2,3} 到 {1,2,3} 的所有单满射。）

$$1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2$$

这样一个群具有良好的运算性质：有一个恒等元素 1、每个元素都有逆、任何两个元素的复合（也称为元素的乘积）仍然属于这个群，也就是乘法运算具有封闭性。事实上，这个群我们一般记作 D_3，叫做二面体群。二面体群这个词事实上包括了一整个系列的群 D_n，D_n 是指作用在正 n 边形上的所有对称组成的群。（注：有些书上用 D_{2n} 记我们这里的 D_n，这是记号的差别，不幸的是这两种记号都有广泛使用。）

2.1. 另一个简单的但重要的群的例子：置换群. 我们考虑集合 $\{1,2,\dots,n\}$，我们研究这个集合的对称。作用在上面的变换是啥呢？就是从它到它自身的所有单满射（必须是单满射，因为对称变换要求有逆）。这个群我们记作 S_n，叫做 n 元置换群。其间的元素称为置换

$$S_n = \{\text{单满射} f : \{1,2,\dots,n\} \mapsto \{1,2,\dots,n\}\}.$$

容易知道，$|S_n| = n!$。置换群具有基本的重要性，所以对它引入简单而方便的记号是重要的。我们还是以

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$$

表示置换。特别的，我们把如下置换形状的置换

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n & b_1 & \dots & b_k \\ a_2 & a_3 & \dots & a_1 & b_1 & \dots & b_k \end{pmatrix}$$

称为轮换，把它记为 $(a_1a_2a_3\dots a_n)$。可以有长度小于 n 的轮换，比如 (12) 表示把 1 映到 2，把 2 映到 1，其它元素不动的轮换。

2.1.1. *置换的轮换表示.* 一个有趣的事实是每个置换事实上都可以用轮换的乘积（复合）表示出来！为了从一个置换得到它的轮换表示，只需要这样操作：它可能把 a_1 映到 a_2, 把 a_2 映到 a_3，……这样下去直到又把某个 a_k 映回 a_1，我们就找到了一个轮换 $(a_1a_2\dots a_k)$。再从这个轮换没有包含的某一个元素出发，让 f 不停地作用在它身上，直到循环，得到另一个轮换 $(b_1b_2\dots b_l)$，以此类推，我们最终能把该置换的所有元素穷尽，得到

$$f = (a_1a_2\dots a_k)(b_1b_2\dots b_l)\dots$$

并且，表达式中所出现的轮换之间没有公共元素 (故此时这些轮换复合 (乘积) 的顺序不重要)。比如，我们可以得到这个置换的轮换表示：

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23) = (23)(14)$$

只需要发现 $1 \mapsto 4 \mapsto 1$,$2 \mapsto 3 \mapsto 2$.

练习 1.1. 计算 $(12)(34)(13)(24)$，直接将它表为不相交轮换的乘积。

练习 1.2. 将置换

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

写为不相交的轮换乘积。

3. 对称的本质框架：群

一个群本质上是指作用在某种对称物件 X 上的所有对称变换的集合 $S(X)$，这集合满足如下性质

(1) $1 \in S(X)$.
(2) $a, b \in S(X) \Rightarrow ab \in S(X)$.
(3) 乘法满足结合律，$a(bc) = (ab)c$.
(4) $a \in S(X) \Rightarrow$ 存在 a 的逆 $b \in S(X), ab = ba = 1$.

事实上，抽象地考察群，我们可以发现其运算结构与 X 并没有什么关系，其所有运算信息完全包含在了乘法运算里。以上条件是所有对称现象都具有的，为了研究宇宙中所有的对称现象的本质结构，我们不妨去繁就简，作出如下定义

定义 1.1. 一个**群 (Group)** 是指一个集合 G 以及上面附带的一种二元运算 $\cdot : G \times G \to G$ 称为乘法，满足：

(1) $a, b \in G \Rightarrow ab \in G$
(2) 存在一个元素 $e \in G$(称为幺元素)，它满足对任意元素 $a \in G$ 都有 $ea = ae = a$.
(3) 对任意的 $a \in G$，存在 $b \in G$，称为 a 的逆，满足 $ab = ba = e$.
(4) 乘法满足结合律，对任意的 $a, b, c \in G$ 有 $(ab)c = a(bc)$.

特别地，如果这个运算还满足交换律，$ab = ba$，则称它为 **Abel 群 (Abelian Group)**。

练习 1.3. 验证在一个群中，幺元素是唯一的。一个元素的逆也是唯一的。

在这个群的定义里我们没有提到任何对称变换，甚至只看这个定义的话看不出来这是要干什么[1]，还以为这只是某种运算封闭的集合。群确实也可以代表这种运算封闭的集合，比如说全体整数在加法运算下成群。(事实上，这种运算封闭的集合，比如全体整数在加法下成的群，也是某种对称变换：它是作用在整数集上的所有平移变换。) 但请记住群的由来，和群最本质的属性是对称。这样一来，研究了所有群，我们就相当于研究了作用在任何可能的物件/对象上的所有可能的对称。

我们只研究有限群，即元素个数有限的群。我们称一个群的元素个数为这个群的**阶数**。在第二章我们会为大家证明，对于每个有限群，都可以构造一个对象 X，使得这个群恰好是该对象的对称群，也即，每个群都是对称群。所以说群的本质是对称：群即对称，对称即群！

3.0.1. *群的一些例子.* 除了我们已经介绍的 S_n 与 D_n 以外，还有一些简单的群。最简单的群的例子应该是 $\mathbb{Z}$，即全体整数在加法下组成的群，我们可以把这个群想象成全体整数的平移对称群。容易验证，全体偶数在加法下也成群。事实上，全体 n 的倍数在加法下都能组成群（因为 n 的倍数在加法下封闭)。

如果我们把 D_n 中的所有旋转 $\{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$ 拿出来单独组成一团，容易验证这也构成一个群（因为旋转之间的复合还是旋转)，这种群也是最基本的群之一，我们把它记作 $\mathbb{Z}_n$，叫它 n 阶循环群[2]，这是一个 Abel 群。

关于循环群，事实上还有另一种算术的描述：全体整数按照模 n 分成 n 个不同的剩余类，就是按除以 n 之后的余数分别为 $0, 1, 2, \ldots, n-1$ 划分为 n 类。剩余类之间可以进行加法运算，比方说在模 5 下，有 $2 + 4 = 1$. 这样，这些不同的剩余类按加法就组成了一个群，这个群看起来跟之前的 $\mathbb{Z}_n$ 好像是不同的，因为一个是旋转变换 $\{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$，一个是剩余类 $\{0, 1, 2, 3, \ldots, n-1\}$。但是不难看出这两个群在结构上没有什么本质上的区别，也即如果我们把剩余类 k 与 σ^k 等同起来，两边进行的任何群运算都是一样的。这也就是说，在一个对应 f 下

$$\begin{aligned} f : \{0, 1, 2, 3, \ldots, n-1\} &\to \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\} \\ k &\mapsto \sigma^k \end{aligned}$$

左边的各种运算可以与右边对应的元素的对应运算相对应。这时，我们说这两个群**同构**。同构的群没有本质的区别，可以视为同一个。关于同构的具体描述将在下一章给出。

练习 1.4. 考虑由所有 n 次单位根 $\{1, e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, \ldots, e^{\frac{2(n-1)\pi i}{n}}\}$，验证它在通常的复数乘法下组成一个群，也即验证它满足群的定义。这个群跟 $\mathbb{Z}_n$ 同构吗？

---

[1] 一般的书从一开始就只写了这个定义，这对初学者来说容易带来困难，初学者会以为群就是一种集合上面带有一种运算，满足一些不知道为什么的定义，他们需要花很长时间才能认识到群代表的实际上是对称。

[2] 也记为 C_n 或 $\mathbb{Z}/n\mathbb{Z}$.

本章我们用简单的方法探索群[3]的基本结构。

4. 元素上的结构信息

4.1. 元素的阶数. 设 $g \in G$，如果有正整数 n 使得 $g^n = 1$，那么我们说 g 是有限阶的，把最小的这样的正整数 n 称作 g 的阶，否则说它是无限阶的。对于有限群 G 来讲，任一个元素 $g \in G$，不停地作乘法，得到序列 $g, g^2, g^3, \dots$ 由于 G 有限，这个序列一定会重复，不妨设 $g^k = g^l, k > l$，那么有 $g^{k-l} = 1$。也即有限群中任何元素都是有限阶的。

练习 1.5. 设 g 是 G 中的 n 阶元素并且 $g^N = 1$. 证明 N 是 n 的倍数。

命题 1.1. 设 g 是群 G 中的 n 阶元素，那么 g^m 的阶数是 $\frac{n}{(m,n)}$，其中 (m,n) 表示 m, n 的最大公因数。

Proof. 首先由 $(g^m)^{\frac{n}{(m,n)}} = g^{\frac{mn}{(m,n)}} = 1$ 我们知道，g^m 的阶数 $\leq \frac{n}{(m,n)}$. 而若有 $(g^m)^k = 1 = g^{mk}$，则必有 mk 是 n 的倍数，因此 k 必然是 $\frac{n}{(m,n)}$ 的倍数。这就表明了 g^m 的阶数一定是 $\frac{n}{(m,n)}$. □

在 Abel 群中，如果已知 a, b 的阶数，那么 ab 的阶数就被约束住了。

练习 1.6. 设 G 是 *Abel* 群，$a, b \in G$ 阶数分别为 m, n，则 ab 的阶数是 $[m, n]$ 的因数。

练习 1.7 (★). 如上题，若还有 m, n 互素，证明 ab 的阶数就是 mn.

值得注意的是，对于非 Abel 群，仅仅已知 a, b 的阶数是不能得到与 ab 阶数有关的任何信息的，可以证明存在群使得 ab 的阶数取到任意给定的正整数。我们举个例子，在 S_5 中，令 $a = (12)(34), b = (135)$ 则 $ab = (14352)$ 是五阶的。

练习 1.8 (★). 证明，如果一个群中只有 $1, 2$ 阶元素，那么这个群是 *Abel* 群。

练习 1.9 (★). 设 G 是一个偶数阶群，则 $g^2 = 1$ 有偶数个解。由此知群 G 中一定有二阶元素。

5. 子群与商结构

不难发现，D_6，即正六边形的对称群，里面也包含了正三角形的所有对称！比方说旋转 120 度的对称，这个在正六边形的对称群里也有。三角形的三条轴对称也构成正六边形的三条轴对称，当然正六边形有更多轴对称（反射对称）。这种时候我们说 D_3 是 D_6 的子群[4]。数学的历史告诉我们，研究一个结构的子结构是重要的：我们作出如下定义

定义 1.2. 设 G 是一个群，$S \subset G$ 是一个子集，若它在群 G 的乘法下仍然满足群的定义性质，则称 S 是 G 的一个**子群**。记为 $S \leq G$。

我们有很多子群的例子，比方说全体偶数的加法群 $2\mathbb{Z}$ 就是 $\mathbb{Z}$ 的一个子群。再比如说，$\mathbb{Z}_6 = \{1, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\}$ 有子群 $\{1, \sigma^2, \sigma^4\}$ 和子群 $\{1, \sigma^3\}$，其实就是 $\mathbb{Z}_3$ 和 $\mathbb{Z}_2$.

例 1.1. $\{1, (12)(34), (13)(24), (14)(23)\}$ 构成 S_4 的一个子群，叫做 *Klein* 四元群，有时它记作 V 或 $\mathbb{Z}_2^2$. 这个群是 *Abel* 群，但是跟同阶的 *Abel* 群 $\mathbb{Z}_4$ 不同构。

练习 1.10. 证明，子群的 *(任意)* 交仍然是子群。

---

[3]我们基本上只讨论有限群。

[4]严格来说，是 D_3 同构于 D_6 的一个子群

5.1. 陪集与拉格朗日定理. 设 G 是一个群，给定了它的一个子群 $H \leq G$ 后，我们可以在群 G 上规定一个等价关系：

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

由于 H 本身是个群，容易验证这样确实定义了一个等价关系[5]，按照这个等价关系，整个群 G 划分成一些不相交的等价类的并。容易发现，与 b 等价的元素的全体就是 bH，因为 $b \sim a \Leftrightarrow b^{-1}a \in H \Leftrightarrow a \in bH$. 这样，所有的等价类都形如 bH，并且它们的大小相等，都是 $|bH| = |H|$. 我们称形如 bH 这样的子集叫做 G 关于 H 的左陪集，简称陪集[6]。我们以 $[G : H]$ 记这个等价关系下，等价类的个数，也即陪集的个数，称它为子群 H 的**指数 (index)**. 我们有

$$G = \bigcup_{i=1}^{[G:H]} b_i H$$

由于不同的等价类不相交，那么我们已经得到了

定理 1.1 (拉格朗日定理)**.** 设 H 是群 G 的子群，那么

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

通过连续运用陪集分解，我们可以得到

练习 1.11 (★)**.** 设 $A \leq B \leq G$. 则有 $[G : A] = [G : B][B : A]$.

这个定理还表明，子群的阶数一定是 $|G|$ 的因数。比方说，借助拉格朗日定理，我们就能知道 12 阶群一定没有 5 阶子群。

例 1.2. 对于群

$$D_3 = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$$

以及它的子群 $H = \{1, \sigma, \sigma^2\}$，我们有如下陪集分解：

$$D_3 = H \cup \tau H.$$

此时有 $[D_3 : H] = 2$.

练习 1.12. 设 $H \leq G$. 证明 $g \in H \Leftrightarrow gH = H$，从而得知 $a \sim b \Leftrightarrow aH = bH$.

定理 1.2. 设 $g \in G$ 是有限群 G 中的一个 n 阶元素，那么 n 是 $|G|$ 的因数。

Proof. 由于 g 是 n 阶元素，我们很容易验证，$H = \{1, g, g^2, \ldots, g^{n-1}\}$ 构成 G 的一个 n 阶子群，因而由拉格朗日定理知一定有 n 是 $|G|$ 的因数。 □

5.2. 商群与正规子群. 就像线性空间 (向量空间) 可以对子空间构作商空间一样，群也存在商结构。

给定 $H \leq G$，我们试图把陪集集合 $G/H = \{H, b_1H, \ldots, b_{k-1}H\}$ 看成一个群，我们所期望的群运算是这样的：

$$\forall a, b \in G \quad (aH)(bH) = (ab)H$$

不幸的是，对于某些子群 H，这个等式不成立。也就是说，不是所有子群都可以用来构作商群 G/H。我们作如下推理：$(aH)(bH) = (ab)H \Leftrightarrow HbH = bH \Leftrightarrow (b^{-1}Hb)H = H \Leftrightarrow b^{-1}Hb \subset H$，而对所有 b 都满足 $b^{-1}Hb \subset H$ 等价于对所有 b 都满足 $b^{-1}Hb = H$. 所以，若要构作商群 G/H，子群 H 必须满足条件：$\forall b \in G, b^{-1}Hb = H$，这引出如下定义：

---

[5]一个关系 $\sim$ 称作等价关系，如果它满足自反性 $a \sim a$，对称性 $a \sim b \Leftrightarrow b \sim a$ 和传递性 $a \sim b, b \sim c \Rightarrow a \sim c$.

[6]也可以定义右陪集。但为了方便，本书统一使用左陪集。

定义 1.3. 设 $N \leq G$，若

$$\forall g \in G \quad g^{-1}Ng = N$$

则称 N 是 G 的**正规子群**，记作 $N \triangleleft G$. 如果一个群 G 除了 1 和 G 以外没有别的正规子群，则称 G 为**单群**。

例 1.3. 若 G 是 *Abel* 群，则 G 的任何子群都是正规子群。

例 1.4. 我们有 $\mathbb{Z}_3 \triangleleft D_3$，这只需验证 $\tau^{-1}\sigma\tau = \sigma^{-1}$. 容易看出 $\{1, \tau\}$ 是 D_3 的子群，但 $\{1, \tau\}$ 并不是 D_3 的正规子群，因为 $\sigma^{-1}\tau\sigma = \sigma^2\tau \notin \{1, \tau\}$.

例 1.5. 我们有 $\{1, (12)(34), (13)(24), (14)(23)\} = V \triangleleft S_4$. 这一点在我们谈到置换群的共轭概念后大家能马上得到。

值得注意的是，正规子群不具有传递性，即 $A \triangleleft B \triangleleft C$ 推不出 $A \triangleleft C$. 反例将在后面的学习中给出。

练习 1.13. 设 $N \leq H \leq G$ 并且 $N \triangleleft G$. 证明 $N \triangleleft H$.

练习 1.14. 证明：$N \triangleleft G$ 等价于说对任意的 $g \in G$ 有 $Ng = gN$.

练习 1.15 (★). 设 $M, N \triangleleft G$ 且 $M \cap N = \{1\}$，证明 M 和 N 之间的元素可交换。即 $\forall m \in M, n \in N$ 有 $mn = nm$.

练习 1.16 (★). 设 $H \leq G$ 且 $[G : H] = 2$. 证明 $H \triangleleft G$.

练习 1.17 (★). 找出所有的有限交换单群。

5.3. 子群之间的乘积. 设 $N, H \leq G$. 我们记集合

$$NH = \{nh | n \in N, h \in H\} \subset G.$$

这个集合在大群 G 赋予的运算下，能成一个群吗? 答案是不一定。但是当 N 或 H 至少有一个是正规子群时这是对的。不妨设 $N \triangleleft G$，我们计算

$$n_1h_1n_2h_2 = n_1(h_1n_2h_1^{-1})h_1h_2 \in NH$$
$$(n_1h_1)^{-1} = (h_1^{-1}n_1^{-1}h_1)h_1^{-1} \in NH$$
$$1 \in NH$$

而群 NH 的结合律也以从大群中的结合律遗传过来，因而此时 NH 构成子群。

另外，就算 N,H 中没有一个是正规子群，通过运用陪集分解的方法我们仍然能够计算集合 NH 中的元素个数。

命题 1.2. 设 $A, B \leq G$, 则有

$$|AB| = \frac{|A||B|}{|A \cap B|}$$

Proof. 显然，AB 可以写成一些不相交的关于 B 的陪集的并 (尽管 AB 可能不是子群), 我们有

$$AB = \bigcup_{a \in A} aB$$

另外，对 A 作关于子群 $A \cap B$ 的陪集分解有

$$A = \bigcup_{a \in A} aA \cap B$$

我们发现，

$$a_1B = a_2B \Leftrightarrow a_1^{-1}a_2 \in B \Leftrightarrow a_1^{-1}a_2 \in A \cap B \Leftrightarrow a_1A \cap B = a_2A \cap B$$

也就是说，AB 关于 B 的陪集个数等于 A 关于 $A\cap B$ 的陪集个数，所以有

$$\frac{|AB|}{|B|}=\frac{|A|}{|A\cap B|}.$$

(这个等式与线性代数中的第二同构定理是否很相似？) □

练习 1.18 (★★)**.** 设 $A,B\leq G$. 证明

$$[G:A\cap B]\leq[G:A][G:B].$$

特别的，如果 $[G:A]$ 与 $[G:B]$ 互素，证明等号一定成立，并且有 $G=AB$.

练习 1.19 (★★)**.** 设 $A,B\subset G$ 是子集 (注意，没说是子群)，如果 $|A|+|B|>|G|$，证明一定有 $G=AB$.

6. 群映射

线性空间之间的映射一般只考虑与其线性结构有关的线性映射。而群与群之间的映射也是这样，一般只考虑与其群结构有关的群映射，我们要找的这群映射便是群同态。

定义 1.4 (群同态)**.** 设 G,H 都是群，$f:G\to H$ 是映射，若

$$f(ab)=f(a)f(b)$$

则称 f 是**群同态**或**群映射**，简称同态。若 f 是单射，则称它为单同态。若 f 是满射，则称满同态。若 f 既是单同态又是满同态，则称 f 是一个**同构**，称 G 和 H 是**同构**的，记作 $G\cong H$.

值得注意的是，在等式 $f(ab)=f(a)f(b)$ 中，ab 所用的是群 G 中的乘法运算，而 $f(a)f(b)$ 处所用的是群 H 中的乘法运算。

例 1.6. 如第一章，通过对三角形顶点编号，我们发现事实上有 $S_3\cong D_3$. 对于 $n>3$，S_n 与 D_n 并不相同。

例 1.7. 一个群同构于它自身。这只需要取 $f(g)=g$ 即可。有趣的是一个群可以有不同于恒等映射的同构映射，比如

$$\begin{aligned}f:\mathbb{Z}_3&\to\mathbb{Z}_3\\ g&\mapsto g^2\end{aligned}$$

就是一个同构映射，但它不同于恒等映射，我们把它们 (包括 1) 称为 $\mathbb{Z}_3$ 的自同构。事实上，这种 (非平凡) 同构映射的存在说明了群 G 的结构本身具有某种对称性，而群 G 的所有自同构，也就是作用在 G 上的所有对称变换，也构成一个群，称为 G 的自同构群，记作 $\mathrm{Aut}(G)$.

练习 1.20. 验证同态一定把 G 中的 1 对应到 H 中的 1, 把 g^{-1} 对应到 $f(g)^{-1}$，也就是说 $f(1)=1$ 以及 $f(g^{-1})=f(g)^{-1}$.

练习 1.21. 验证 $\mathbb{Z}_4$ 有一个二阶子群，并证明它对这个二阶子群的商群同构于 $\mathbb{Z}_2$.

练习 1.22. 设 g 是 n 阶元素，证明 $f(g)$ 必是有限阶元素，而且阶数是 n 的因数。

练习 1.23. 求出 $\mathrm{Aut}(\mathbb{Z}_4)$.

定义 1.5 (核与像)**.** 设有群同态 $f: G \to H$，我们称集合

$$\ker f = f^{-1}(1) = \{g \in G | f(g) = 1\}$$

为 f 的核，集合

$$\mathrm{Im} f = \{f(g) | g \in G\}$$

为 f 的像。

值得注意的是 $\ker f$ 和 $\mathrm{Im} f$ 分别是 G 和 H 的子群，而且事实上有 $\ker f \triangleleft G$.

练习 1.24. 证明

(1) $\ker f = \{1\} \Leftrightarrow f$是单射。
(2) $\ker f \triangleleft G$.

练习 1.25 (★)**.** 找出所有的阶数 ≤ 5 的群。包含只有一个元素的平凡群在内，阶数不超过 5 的群一共有 6 个。*(*同构的群视为同一个*)*

6.1. 简单重要而典型的群映射.

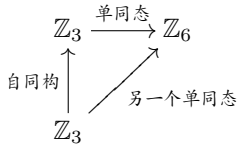
6.1.1. 单同态. 最简单的群映射应该属于单同态。一个单同态 $f: H \to G$ 本质上是把 H 给对应到了 G 中的一个子群 $f(H) \leq G$，而 $f(H)$ 与 H 是同构的。换而言之，单同态就是把 H 以同构的方式“塞”进了 G.

例 1.8. 考虑群的单同态

$$f: \mathbb{Z}_3 = \{1, a, a^2\} \to \mathbb{Z}_6 = \{1, b, b^2, b^3, b^4, b^5\}$$

容易发现，这个同态完全被 $f(a)$ 的值确定下来了，因为 $f(1) = 1$ 而 $f(a^2) = f(a)^2$. 由于 a 是 3 阶元素，$f(a)$ 必须是 1 或 3 阶元素。$\mathbb{Z}_6$ 中的三阶元素只有 b^2, b^4。因此我们知道，$f(a)$ 只可能取 $1, b^2, b^4$。由于我们只考虑单同态，可能的选择只剩下两个：$f(a) = b^2$ 或 $f(a) = b^4$.

如果 $f(a) = b^2$，那么就有 $f(a^2) = b^4$，整个群 $\mathbb{Z}_3 = \{1, a, a^2\}$ 被映射成了 $\{1, b^2, b^4\}$。如果选择 $f(a) = b^4$，那么就有 $f(a^2) = (b^4)^2 = b^8 = b^2$，整个群 $\mathbb{Z}_3 = \{1, b^4, b^2\}$. 我们知道 $\{1, b^2, b^4\}$ 是 $\mathbb{Z}_6$ 的同构于 $\mathbb{Z}_3$ 的子群，但是却有两种不同的将 $\mathbb{Z}_3$ 嵌入到 $\mathbb{Z}_6$ 的方式。但在任何一种方式下，这个单同态都建立了 H 与 $f(H)$ 的同构。尽管 $G = \mathbb{Z}_6$ 中只有一个子群同构于 $H = \mathbb{Z}_3$，但之所以会有多种不同的将 H 嵌入到 $f(H)$ 的方式，是因为存在从 H 到 H 的自同构 $(1, a, a^2) \mapsto (1, a^2, a)$. 换而言之，这种现象发生是因为 H 自身具有的对称性导致的。



6.1.2. 投射与同态的分解. 另一种简单而重要的映射是投射。我们说过，对于群 G 的正规子群 N，可以构作商群 G/N. 我们可以考虑一种把 G 中的元素 g 对应到 G/N 中 g 所在的陪集的自然的映射

$$p: G \to G/N$$
$$g \mapsto gN$$

这个映射显然是同态，因为 $p(ab) = abN = aNbN = p(a)p(b)$. 而且还是满同态。那它的核是什么呢？回忆商群 G/N 中的单位元素就是 N，也即 G 中的单位元素所在的陪集，因此 $p(a) = aN = N \Leftrightarrow a \in N$，我们得出 $\ker p = N$.

投射的重要性和基本性在于，对于任何同态 $f: G \to H$ 我们去考虑这个同态的 $\ker f$. 一件值得注意的事情是，$a^{-1}b \in \ker f$ 等价于说 $f(a^{-1}b) = 1 \Leftrightarrow f(a) = f(b)$.

换而言之，若是把 G 对 $\ker f$ 作商群 (也即陪集分解)，每个陪集 $b\ker f$ 的中的元素都被 f 映射到同一个 $f(b)$，而不同的陪集一定被映射到了不同的元素 (因为只要两个陪集 $a\ker f$ 和 $b\ker f$ 被映射到了相同的元素，就有 $f(a^{-1}b) \in \ker f \Leftrightarrow a\ker f = b\ker f$). 既然 $a\ker f$ 中所有元素都被映为同一个 $f(a)$(给我们一种浪费的感觉)，不如定义一个新映射，把 $a\ker f$ 视为商群中 $G/\ker f$ 的一个元素，让它对应到 $f(a)$.

换而言之，我们发现，任何具有 $\ker f$ 的同态 $f : G \to H$ 都可以分解成两个映射的复合：

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \downarrow{\scriptstyle p} & \nearrow & \\ G/\ker f & & \end{array}$$

这个图的意思就是我们可以将映射 $a \mapsto f(a)$ 对应成两步：$a \mapsto a\ker f \mapsto f(a)$. 第一步是将 a 对应到它所在的陪集 $a\ker f$(即从 G 向 $G/\ker f$ 的自然投射)，第二步是将 $a\ker f$ 映射到 $f(a)$. 唯一可能存在的问题是第二步映射是不是一个同态？答案是是。验证这一点是极为容易的。任何群映射可以分解成两种基本映射的复合：即一个投射，和一个单同态的复合。顺便，事实上我们可以在这个基础上再加一步，也是最水的一步：$a \mapsto a\ker f \mapsto f(a) \mapsto f(a)$, 也即先将 $f(a)$ 映入 H 的子群 $\mathrm{Im}f$，再将 $\mathrm{Im}f$ 通过平凡单射对应到 H.

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \downarrow{\scriptstyle p} & & \uparrow{\scriptstyle i} \\ G/\ker f & \xrightarrow{\cong} & \mathrm{Im}f \end{array}$$

这样，第二步 $G/\ker f \to a\ker f \mapsto f(a)$ 就是一个同态且是单满射，因此是同构。于是我们得出，我们得出了如下重要的定理：

定理 1.3 (同态基本定理)**.** *若 $f : G \to H$ 是同态，那么 $\ker f \triangleleft G$,$\mathrm{Im}f \leq H$ 且有同构*

$$G/\ker f \cong \mathrm{Im}f$$

Proof. 如上，构作映射

$$\begin{aligned} h : G/\ker f &\to \mathrm{Im}f \\ a\ker f &\mapsto f(a) \end{aligned}$$

易验证这个映射的定义是良好的，因为只要 $b\ker f = a\ker f$ 就有 $f(b) = f(a)$. 现在来证明这是同态：

$$h((a\ker f)(b\ker f)) = h(ab\ker f) = f(ab) = f(a)f(b)$$

第一个等号是因为 $\ker f$ 正规。h 是单射，因为 $h(a\ker f) = f(a) = 1 \Leftrightarrow a \in \ker f$. 另外，$h$ 显然是满射，故 h 是同构。 □

7. 同构定理

同态基本定理又叫第一同构定理。由同态基本定理我们很容易导出许多同构定理，它们和我们在线性代数中学过的同构定理是类似的。

定理 1.4 (第二同构定理)**.** *设 $N \triangleleft G$ 且 $H \leq G$. 则有 $N \triangleleft NH$ 且 $N \cap H \triangleleft H$ 并且有*

$$NH/N \cong H/N \cap H$$

Proof. 由于 $N \triangleleft G$ 以及 $N \leq NH \leq G$ 容易得出 $N \triangleleft NH$. 对任意的 $n \in N \cap H, h \in H$ 有

$$h^{-1}nh \in N \cap H$$

故 $N \cap H \triangleleft H$. 现在，构作映射

$$f : H \to NH/N$$
$$h \mapsto hN$$

先证明这个映射是同态。因为 $N \triangleleft NH$, 我们有

$$f(ab) = abN = aNbN = f(a)f(b).$$

这显然是个满同态。现在我们计算 $\ker f$，设 $h \in \ker f$，则

$$hN = N \Leftrightarrow h \in N \Leftrightarrow h \in N \cap H$$

故 $\ker f = N \cap H$. 现在同态基本定理给出

$$H/N \cap H \cong NH/N.$$

□

下面的这个对应定理是基本的，它描述了 G/N 的子群与 G 的包含了 N 的子群存在着对应关系

定理 1.5 (对应定理)**.** *设 $N \triangleleft G$，记 $\rho : G \to G/N$ 是自然投射，则有如下从所有 G 中包含 N 的子群到所有 G/N 的子群的一一对应*

$$H \mapsto \rho(H) = H/N \subset G/N$$

即把 H 映射到所有形如 hN 的陪集集合。其逆映射为 $T \mapsto \rho^{-1}(T)$, 这里 T 是 G/N 的子群。

Proof.
- 注意到 $H \to G \to G/N$ 的像就是 H/N, 因而是同态的像，故为一个 G/N 的子群。同理对任意子群 $T \leq G/N$，原象 $\rho^{-1}(T)$ 也是一个子群。
- 现在只需验证这两个映射互为逆映射,即验证 $\rho^{-1}(\rho(H)) = H$ 和 $\rho(\rho^{-1}(T)) = T$. 后者是显然的，因为 ρ 是满射。对于前者，设有陪集分解 $H = \cup hN$, 则

$$\rho^{-1}(\rho(H)) = \rho^{-1}\left(\bigcup \rho(h)\right) = \bigcup hN = H.$$

□

8. 循环群，生成元与群的表现

循环群是最简单、最基本的一类群，但仍然十分重要。循环群 $\mathbb{Z}_n$ 有多种描述方法，比如可以描述成正 n 边形的旋转变换群，也可以描述成模 n 的余数类的加法群。循环群的本质特点是，它可以仅由一个元生成。这就是说，可以找到其中一个元素 a，通过不断的作逆 a^{-1} 和乘法 $1, a, a^2, a^3, \ldots$ 可以得到群 G 中的所有元素。我们把话说得更明白一点：

定义 1.6. 设 G 是一个群，$S \subset G$ 是 G 的一个子集。则 G 中所有包含 S 的子群的交，也即包含 S 的最小子群，称为由 S 生成的子群，记为 $\langle S \rangle$. 如果 $G = \langle S \rangle$，则称 G 是由 S 生成的群，称 S 是 G 的一组**生成元**。若一个群可由其中一个元素生成，即存在 $a \in G$ 使得 $G = \langle a \rangle$，就称 G 是**循环群**。

按照这个定义，除了有限循环群 $\mathbb{Z}_n$ 以外，可以有无限循环群，而那本质上就是 $\mathbb{Z}$.

于是，循环群 $\mathbb{Z}_n$ 可以想象成一个由抽象字母 a 生成的，满足关系 $a^n = 1$ 的群，这种用生成元与约束关系描述群的方法叫做**群的表现**，这个例子我们记作

$$\mathbb{Z}_n = \langle a | a^n = 1 \rangle.$$

例 1.9. 类似的，我们容易想象，群 D_3 可以抽象地描述成由抽象字母 σ 和 τ 生成，满足约束关系 $\sigma^3 = \tau^2 = 1$ 以及 $\sigma\tau = \tau\sigma^{-1}$ 的群。我们可以试试列出一系列这两个字母生成的元素

$$1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2$$

在群 D_3 这个特例中，任何抽象字母生成的元素，比如 $\sigma\tau\sigma^2$，都可以写成上面的形式，也即 $\tau^i\sigma^j$ 的形式。这是因为

$$\sigma\tau\sigma^2 = \tau\sigma^{-1}\sigma^2 = \tau\sigma.$$

我们把这记为

$$D_3 = \langle \sigma, \tau | \sigma^3 = \tau^2 = (\sigma\tau)^2 = 1 \rangle$$

(条件 $\sigma\tau = \tau\sigma^{-1}$ 可以简化为 $(\sigma\tau)^2 = 1$). 这容易推广成一般的 D_n 的定义

$$D_n = \langle \sigma, \tau | \sigma^n = \tau^2 = (\sigma\tau)^2 = 1 \rangle.$$

这个定义是抽象的，它完全没有涉及对称，却把群的结构简单明了地确定下来了！

练习 1.26. 接上例，请计算

$$\sigma\tau\sigma^{-1}\tau\sigma\tau^{-1}.$$

本节的描述算是启发性，非正式的。我们今后会严格地对待这种群的表示方法。

n 阶循环群有多少个生成元? 问题的答案是明显的，设 a 是一个生成元，则 a^i 是生成元当且仅当 i 与 n 互质。也就是说，一共有 $\varphi(n)$ 个生成元，这里 $\varphi(n)$ 表示 1 到 n 中与 n 互素的数的个数，也即数论中的欧拉函数。关于这个欧拉函数，有一个有趣的恒等式

$$\sum_{d|n} \varphi(d) = n$$

其中符号 $d|n$ 表示 d 整除 n, 求和号 $\sum_{d|n}$ 表示对 n 的所有正因数 d 求和。这个等式可以由如下观察得出：对于每一个 $d|n$, 循环群 $\mathbb{Z}_n$ 中有且仅有一个 d 阶子群，而这 d 阶子群的生成元有 $\varphi(d)$ 个。每个 $g \in \mathbb{Z}_n$ 都恰好是某一个 $\mathbb{Z}_d$ 的生成元。

关于循环群，有一个刻画了循环群的性质的重要命题：

定理 1.6. 设 G 是有限群。若对 $n = |G|$ 的任何因数 d，G 中至多只有一个 d 阶子群，则 G 是循环群，反之显然也成立。

Proof. 注意到，任何 $g \in G$ 都有一个由它生成的循环子群 $\langle g \rangle$。由假设，这个阶数的子群至多只有一个。对于 $d|n$ 若有一个 d 阶循环子群，则记它的生成元集合为 $\mathrm{gen}(d)$，若没有，则令 $\mathrm{gen}(d)$ 表空集。由于任何 $g \in G$ 都是某个 d 阶循环群的生成元，我们有

$$G = \bigcup_{d|n} \mathrm{gen}(d)$$

而 d 阶循环群有 $\varphi(d)$ 个生成元，因此

$$n \le \sum_{d|n} |\mathrm{gen}(d)| \le \sum_{d|n} \varphi(d) = n$$

我们发现等号成立，故对每个 $d|n$ 它恰有一个 d 阶循环子群，这对 $d = n$ 也是对的，因此它是循环群。 □

练习 1.27 (★). *(没有听说过域的可以跳过)* 证明, 域 F 的乘法群 $F^\times = F\backslash\{0\}$ 的任何有限子群必是循环群。

9. 置换群与共轭

置换群是有限群中最重要的一类群，说是最基本也不为过，原因是：置换群事实上包含了所有的有限群，即任何有限群都是置换群的某个子群！(这一点我们将在后面给出)

9.1. 置换的结构与共轭. 置换群的基本要素当然是置换。对于置换来说，置换的 (不相交的) 轮换分解最能体现出它的结构。我们知道，每个置换都有一个不相交轮换的乘积分解，而且可以有很多轮换分解，但事实上，其中那个置换的不相交轮换分解在不记轮换之间的次序之下是唯一的。这一点比较直觉，证明只需用归纳法，没有太多可说的。

命题 1.3. *每个 $\alpha \in S_n$ 都有不相交的轮换 $\beta_1, \dots, \beta_k$ 使得*

$$\alpha = \beta_1 \dots \beta_k.$$

而且这种分解是唯一的，在不记次序的情况下。

Proof. 设 α 有两个不相交的轮换分解

$$\alpha = (\alpha_{11} \dots \alpha_{1k_1})(\alpha_{21} \dots \alpha_{2k_2}) \dots$$

$$\alpha = (\beta_{11} \dots \beta_{1l_1})(\beta_{21} \dots \beta_{2l_2}) \dots$$

如果 α 移动了 α_{11}, 那么 α_{11} 就会出现在另一个轮换分解式中的某个轮换中，不妨设 $\beta_{11} = \alpha_{11}$. 让 α 不停地作用在 α_{11} 上，依次得到 $\alpha_{11} = \beta_{11}$,$\alpha_{12} = \beta_{12} \dots$ 显然必然有这两个分解式的第一个轮换相等。两个式子同时乘以该轮换的逆，我们得到一个轮换个数更少的式子。重复这个过程，不难得到命题。 □

于是每个置换都有一种唯一的轮换结构，比如说 (123)(45) 和 (234)(15) 具有相同的轮换结构，只是数字不同而已。我们说它们的轮换结构是 $2 \cdot 3$. 类似的，设 α 的轮换分解中长度为 k 的轮换有 m_k 个，则我们说它的轮换结构是 $2^{m_2} \cdot 3^{m_3} \dots k^{m_k}$.

具有相同的轮换结构就像是矩阵具有完全相同的约当块一样，可以通过 “换基” 来实现 “相似”，比如

$$(123)(45) = \sigma^{-1}(234)(15)\sigma$$

其中 $\sigma = (14)$. 这种现象我们称之为共轭：

定义 1.7. 对于 $a, b \in G$, 若有 $g \in G$ 使得

$$a = g^{-1}bg$$

我们称 a 与 b 在 G 中共轭。易验证共轭是一个等价关系。只与自己共轭的元素[7]我们称为中心元素，所有中心元素记为 $C(G)$ 或 $Z(G)$, 称为群 G 的中心.

练习 1.28. *证明群 G 的共轭类个数等于 $|G|$ 当且仅当 G 是 Abel 群。*

练习 1.29. *设 $g \in G$ 是某个固定的元素，验证，共轭映射*

$$f_g(a) = gag^{-1}.$$

是群 G 的自同构。

[7]也即与其它所有元素都交换的元素

练习 1.30 (★). 接上一题，我们于是有从 G 到 $\mathrm{Aut}(G)$ 的映射

$$i : G \to \mathrm{Aut}(G)$$
$$g \mapsto f_g$$

验证这也是一个群同态。证明 $\ker i = Z(G)$ 从而得知 $Z(G)$ 是 G 的正规子群。记 $\mathrm{Im}i = \mathrm{Inn}(G) \leq \mathrm{Aut}(G)$, 称它为群 G 的内自同构群，于是由同态基本定理

$$\mathrm{Inn}(G) \cong G/Z(G).$$

作为给大家看的一个例子，我们证明一个有用的命题。

命题 1.4. *若 $G/Z(G)$ 是循环群，则 G 是 Abel 群。*

Proof. 设 a 是循环群 $G/Z(G)$ 的一个生成元在 G 中的原象，可作 G 关于 $Z(G)$ 的陪集分解

$$G = \bigcup_{i=0}^{n-1} a^i Z(G)$$

故每个元素形如 $a^i z$，显然有 $a^i z_1 a^j z_2 = a^j z_2 a^i z_1$. □

练习 1.31 (★). 证明，若 $\mathrm{Aut}(G)$ 是循环群，则 G 是 *Abel* 群。

练习 1.32 (★). 设 $|G| = p^2$, 其中 p 是素数，证明 G 是 *Abel* 群。

练习 1.33 (★★★★). 设 $\alpha \in \mathrm{Aut}(G)$，令 $I = \{g \in G | \alpha(g) = g^{-1}\}$. 证明：若

$$|I| > \frac{3}{4}|G|$$

则 G 是 *Abel* 群。

那么，既然共轭是一个群上的等价关系，群中的元素自然就会划分为一些等价类，这些等价类就称作共轭类。一般来说，群的共轭类的情况比较复杂，但是对于 S_n 情况比较简单。

练习 1.34 (★). 求 D_5 的共轭类个数。

练习 1.35 (★★★). 设 $p > 2$ 是素数，求 D_p 的共轭类个数。

定理 1.7. 两个置换 $\alpha, \beta \in S_n$ 在 S_n 中是共轭的，当且仅当它们具有相同的轮换结构。

Proof. 设有两个具有相同轮换结构的置换

$$\alpha = (\alpha_{11} \dots \alpha_{1k_1})(\alpha_{21} \dots \alpha_{2k_2}) \dots$$
$$\beta = (\beta_{11} \dots \beta_{1k_1})(\beta_{21} \dots \beta_{2k_2}) \dots$$

显然可作置换 σ 使得 $\sigma(\alpha_{ij}) = \beta_{ij}$. 则有

$$\alpha = \sigma^{-1} \beta \sigma.$$

这等式可用下图[8]表示 (其中若 $j = k_i$，下标 $i(j+1)$ 应理解为 $i1$.)

$$\begin{array}{ccc} \alpha_{ij} & \xrightarrow{\alpha} & \alpha_{i(j+1)} \\ {\scriptstyle\sigma}\downarrow & & \uparrow{\scriptstyle\sigma^{-1}} \\ \beta_{ij} & \xrightarrow{\beta} & \beta_{i(j+1)} \end{array}$$

[8]这种用交换图来表达等式的方式非常直观，在代数学中会经常用到。

由共轭推出轮换结构相同也是简单的，设 α 定义如上，则有

$$\gamma\alpha\gamma^{-1} = (\gamma(\alpha_{11})\dots\gamma(\alpha_{1k_1}))(\gamma(\alpha_{21})\dots\gamma(\alpha_{2k_1}))\dots.$$

□

容易看出，一个群 G 的子群 H 若是正规子群的话，那 H 一定是由一些完整的共轭类拼成的。反之，把一些共轭类拼起来，如果恰好也成一个子群的话，这个子群就是正规子群。

练习 1.36. 好好想一想上面那句话，并证明

$$\{1, (12)(34), (13)(24), (14)(23)\} \lhd S_4.$$

练习 1.37 (★). 观察

$$\{1, (12)(34), (13)(24), (14)(23)\} \lhd S_4.$$

试说明正规子群不具有传递性。

练习 1.38 (★). 我们称 $H \leq G$ 是 G 的特征子群，如果每一个 G 的自同构 α 都将 H 中的元素映到 H 中。证明，若 $H \leq N \lhd G$ 并且 H 是 N 的特征子群，则 $H \lhd G$. 即，正规子群的特征子群还是正规子群。

练习 1.39 (★). 设 p 是 $|G|$ 的最小素因子。证明若有 p 阶子群 $A \lhd G$, 则必有 $A \leq Z(G)$.

9.2. 置换的奇偶性. 置换有奇置换和偶置换之分，用符号 $\mathrm{sgn}\sigma$ 来表示：奇置换是 -1, 偶置换是 1. 置换的符号 $\mathrm{sgn}\sigma$ 我们并不陌生，在线性代数中已经碰过了，它可以定义为 -1 的逆序数次方，也可以定义为使如下等式成立的函数。

$$\prod_{1\leq i\leq j\leq n}(X_{\sigma(j)} - X_{\sigma(i)}) = \mathrm{sgn}\sigma \prod_{1\leq i\leq j\leq n}(X_j - X_i).$$

任何置换都可以分解成对换的乘积，这是因为任何轮换都能分解成对换的乘积，即 $(12\dots k) = (1k)(1, k-1)\dots(13)(12)$，我们还可以定义置换的符号为可分解成的对换的个数的奇偶性，可以证明，置换的任何对换分解的对换的个数的奇偶性不变。按照这种说法，一个对换 (12) 是奇置换，奇数长度的对换如 (123), (12345) 都是偶置换。

我们将给出另外一种定义，我们先解释一下这个定义是怎么来的。我们知道，每个置换 $\sigma \in S_n$ 都有一个唯一的不相交轮换分解，如果把被它固定的元素 c 视为长度为 1 的轮换 (c)，我们以 t 记该置换的不相交轮换分解中轮换的个数，包括长度 1 的轮换。那么定义

$$\mathrm{sgn}\sigma = (-1)^{n-t}.$$

首先，对恒等置换，$t = n$，因此 $\mathrm{sgn}1 = 1$. 对于轮换 $(12\dots k)$，$t = n - k + 1$, 故 $\mathrm{sgn}(12\dots k) = (-1)^{k-1}$. 而 $n - t$ 事实上是对每一个轮换的长度 l 减去 1 后再求和，其奇偶性将与轮换分解中奇置换的个数有关。麻烦的地方是，我们需要证明这是一个同态。直接证明并不容易，所以我们走稍微简单一点的路线：即证明对任意对换 τ 有 $\mathrm{sgn}(\tau\sigma) = \mathrm{sgn}(\tau)\mathrm{sgn}(\sigma) = -\mathrm{sgn}(\sigma)$.

引理 1.1. 对任何对换 τ 有 $\mathrm{sgn}(\tau\sigma) = \mathrm{sgn}(\tau)\mathrm{sgn}(\sigma) = -\mathrm{sgn}(\sigma)$.

Proof. 若 $\tau = (ab)$ 与 σ 的不相交轮换分解的任何一个轮换不相交，等式是显然的。否则若有一个相交元素，容易计算出

$$(ab)(ac..d) = (ac..db)$$

$(ac..db)$ 的长度相对 $(ac..d)$ 增加了 1，故符号改变了。若有两个相交元素，考虑

$$(ab)(abc..d) = (ac..d)$$

计算轮换的长度减 1 之和，右边比左边的 $(abc..d)$ 少 1. 对于另一种情况

$$(ab)(ac..dbe..f) = (ac..d)(be..f)$$

计算轮换的长度减 1 之和，右边比左边的 $(ac..dbe..f)$ 少 1. 故我们立即得出命题。 □

定理 1.8. $\mathrm{sgn} : S_n \to \{1, -1\} \cong \mathbb{Z}_2$ 是一个同态。

Proof. 由第一章，可设 $\alpha = \tau_1\tau_2 \dots \tau_k$ 是 α 的对换分解，则

$$\begin{aligned}
\mathrm{sgn}(\alpha\beta) &= \mathrm{sgn}(\tau_1\tau_2 \dots \tau_k\beta) \\
&= \mathrm{sgn}(\tau_1)\mathrm{sgn}(\tau_2 \dots \tau_k\beta) \\
&\dots \\
&= \mathrm{sgn}(\tau_1) \dots \mathrm{sgn}(\tau_{k-1})\mathrm{sgn}(\tau_k)\mathrm{sgn}(\beta) \\
&= \mathrm{sgn}(\tau_1) \dots \mathrm{sgn}(\tau_{k-1}\tau_k)\mathrm{sgn}(\beta) \\
&\dots \\
&= \mathrm{sgn}(\tau_1\tau_2 \dots \tau_k)\mathrm{sgn}(\beta) \\
&= \mathrm{sgn}(\alpha)\mathrm{sgn}(\beta).
\end{aligned}$$

□

同态 sgn 的核我们记作 A_n, 称作 n 元**交错群**，也就是全体偶置换组成的群。作为一个推论，$A_n \lhd S_n$.

练习 1.40. 确定置换 $(132)(421)(12345)$ 和置换

$$\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ n & n-1 & \dots & 2 & 1 \end{pmatrix}$$

的奇偶性。

练习 1.41. 证明一个置换的阶等于它的不相交轮换分解中的所有轮换长度的最小公倍数。

练习 1.42 (★). 对 S_4 中所有的元素进行共轭类分类，并找出它所有的正规子群。

练习 1.43 (★★). 证明 A_{2n} 有子群同构于 S_n.

10. 直积

我们可以用老群来构造新的群，一种非常简单的构造就是直积。设 G_1, G_2 都是群，我们要赋予笛卡尔乘积 $G_1 \times G_2$ 群的结构，最简单的方法就是把它的乘法定义为分量乘法，即

$$(g_1, g_2)(h_1, h_2) := (g_1h_1, g_2h_2).$$

这样一来群中的幺元素就是 $(1, 1)$,(g, h) 的逆就是 (g^{-1}, h^{-1}). 这个群我们就记作 $G_1 \times G_2$. 如果 G_1, G_2 都是 Abel 群，有时这个构造记为直和 $G_1 \oplus G_2$，群运算用加号代替。

练习 1.44. 研究群 $\mathbb{Z}_2 \times \mathbb{Z}_2$(也即群 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$) 并证明它同构于

$$V = \{1, (12)(34), (13)(24), (14)(23)\}.$$

练习 1.45 (★★)**.** 证明有

$$D_6 \cong D_3 \times \mathbb{Z}_2.$$

事实上，当 n 是奇数时都有

$$D_{2n} \cong D_n \times \mathbb{Z}_2.$$

练习 1.46 (★)**.** 证明当 m, n 互质时有

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$$

CHAPTER 2

群的作用

1. 基本术语

群本质上是对称群/变换群/作用群的抽象结构。本章我们就来研究群的作用，即将抽象的群的元素实现为具体的变换/作用。比方说，循环群这种对称结构如何作用在各种对象上？我们知道，它可以实现为正多边形的旋转，即有群同态

$$\mathbb{Z}_n \to \{\text{正 } n \text{ 边形的旋转群}\}$$

其中 $\mathbb{Z}_n$ 的生成元被映射到某个单位旋转。也可以这样描述这种作用：将正 n 边形的旋转理解为顶点集 $\{1, 2, \ldots, n\}$ 上的一个置换，从而得到 (单) 同态

$$\mathbb{Z}_n \to S_n$$

其中 $\mathbb{Z}_n$ 的生成元被映射到轮换 $(123\ldots n)$. 我们研究群的尽可能广泛的作用，就是考虑群 G 到尽可能大的一类变换群的同态。一般考虑的大的一类变换群主要是两类：置换群和矩阵群。研究到矩阵群的同态的是群的线性表示论 (简称群表示论)。我们研究群在集合上的作用时，就主要是研究的到置换群的同态。以 $\mathrm{Sym}(X)$ 记集合 X 上的所有置换[1]，即所有单满映射，称之为 X 的对称群。那么我们称群 G 在集合 X 上的一个作用就是指一个同态 (不要求是单同态或满同态)

$$\alpha : G \to \mathrm{Sym}(X).$$

这也称为群 G 的一个置换表示，简称表示。也就是说，$\alpha(g)$ 将成为集合 X 上的一个变换 (置换)，单满射，即 $\alpha(g) : X \to X$. 这个变换可以作用在 $x \in X$ 上得到 $\alpha(g)(x)$。这种记号比较严格，但过于冗长，给定了同态 α 后不妨把 G 想象为一堆“算子”，直接用 gx 表示 $\alpha(g)(x)$.

我们先来给出群作用基本的术语。如果 α 是单同态，就称这个作用是**忠实的 (faithful)**，也就是说，这个作用不会把群中的两个不同元素变成相同的变换。对于 $x \in X$，集合

$$Gx = \{gx | g \in G\}$$

称为 x 的**轨道 (Orbit)**。容易证明，a, b 属于同一个轨道，也就是存在 g 使得 $a = gb$, 是一个等价关系，这一点与 G 是群密切相关。如此而来，X 中的元素划分为一些不相交的等价类的并，也就是不相交的轨道的并。如果 X 只有一个轨道，我们就称这个作用是**传递的 (transitive)**，这也就是说，任何一个 x 都可以被 G 中的某一个作用映到任何一个给定的 y.

1.1. 轨道公式.

定义 2.1. 给定了群 G 在集合 X 上的作用，我们用

$$\mathrm{Stab}(x) = \{g \in G | gx = x\}$$

记 G 中所有保持 x 不动的变换。这是 G 的一个子群，称之为 x 的**稳定化子 (Stabilizer)**.

[1]有些书也记为 S_X

练习 2.1 (★)**.** 有一个比传递更强的概念，叫**双传递 (doubly-transitive)**，它是指对任意的 $x \neq y, z \neq w$, 存在 $g \in G$ 使得

$$(gx, gy) = (z, w).$$

证明：G 在 X 上是双传递的当且仅当对所有的 $x \in X$ 都有 $\mathrm{Stab}(x)$ 在 $G\backslash\{x\}$ 上是传递的。

既然 $\mathrm{Stab}(x)$ 是个子群，我们就可以作陪集分解

$$G = \bigcup_i g_i \mathrm{Stab}(x)$$

其中，每个陪集在 x 上的作用全部一致，都是 $g_i x$. 并且不同的陪集显然给出在 x 上不同的作用，否则 $ax = bx \Leftrightarrow a^{-1}b \in \mathrm{Stab}(x) \Leftrightarrow a\mathrm{Stab}(x) = b\mathrm{Stab}(x)$. 我们立马得到了如下简单而基本的轨道公式 (计算轨道长度)

定理 2.1 (轨道公式)**.**

$$|Gx| = [G : \mathrm{Stab}(x)]$$

由于 X 划分为一些轨道，我们以 x_i 记每个轨道的代表元素，则显然必须有

$$|X| = \sum |\text{轨道}| = \sum_i [G : \mathrm{Stab}(x_i)].$$

不要小瞧这个轨道公式，有了它，我们就有了计算一些对称群的阶数的方法，因为 $|G| = |Gx||\mathrm{Stab}(x)|$.

例 2.1. 我们计算 $|D_n|$. 取正 n 边形的某一个顶点 x, 由于作用是传递的，$|Gx| = n$. 而 D_n 中只有两个变换保持 x 不变，平凡变换和某个反射 (轴对称) 变换。故

$$|D_n| = |Gx||\mathrm{Stab}(x)| = 2n.$$

练习 2.2 (★)**.** 计算正四面体的对称群的阶数。

例 2.2. 设 $H, K \leq G, a \in G$, 我们计算如下双陪集集合的元素个数

$$HaK = \{hak | h \in H, k \in K\}.$$

考虑 $H \times K$ 在 G 上的如下作用：

$$\begin{aligned} \rho : H \times K &\to \mathrm{Sym}(G) \\ (h, k) &\mapsto (g \mapsto hgk^{-1}) \end{aligned}$$

不难看出，HaK 就是 a 在该作用下的轨道。于是根据轨道公式，

$$|HaK| = [H \times K : \mathrm{Stab}(a)].$$

我们考虑 $(h, k) \in \mathrm{Stab}(a) \Leftrightarrow hak = a \Leftrightarrow h = ak^{-1}a^{-1} \in H \cap aKa^{-1}$. 于是

$$|HaK| = \frac{|H||K|}{|H \cap aKa^{-1}|}.$$

另外，我们马上能得到如下计算轨道个数的公式，对 G 的任何子集 $S \subset G$ 我们引入记号

$$X^S = \{\text{被所有 } S \text{ 中元素固定的 } x \in X\}.$$

则我们有

定理 2.2 (Burnside)**.** 轨道的个数 N 有如下公式[2]

$$N = \frac{1}{|G|}\sum_{g\in G}|X^g|.$$

Proof.

$$N = \sum_{x\in X}\frac{1}{|Gx|} = \sum_{x\in X}\frac{|\mathrm{Stab}(x)|}{|G|} = \frac{1}{|G|}\sum_{x\in X}\sum_{g\in G}1_{gx=x} = \frac{1}{|G|}\sum_{g\in G}\sum_{x\in X}1_{gx=x}.$$

□

练习 2.3 (★)**.** 设 G 传递地作用在 X 上，$|X|>1$. 则一定存在一个 $g\in G$ 没有不动点。

练习 2.4 (★)**.** 设 G 是一个阶数为 p^k 的群。证明若 G 作用在集合 X 上，则有

$$\left|X^G\right| \equiv |X| \mod p.$$

1.2. 表示的核. 我们来求 $\ker\alpha$，这一般是重要的，因为这样，由同态基本定理，$G/\ker\alpha$ 同构于置换群 $\mathrm{Sym}(X)$ 的某个子群。

$\ker\alpha$ 是什么呢？就是那些固定所有元素的 g, 因此

$$\ker\alpha = \bigcap_{x\in X}\mathrm{Stab}(x).$$

如果这个作用是传递的，就有

$$\ker\alpha = \bigcap_{g\in G}\mathrm{Stab}(gx).$$

$\mathrm{Stab}(x)$ 与 $\mathrm{Stab}(gx)$ 有自然的关系。固定 x 的那些变换，稍微改一改，也可以拿去固定 gx. 这只需要先复合一个 g^{-1}, 再施加 $\mathrm{Stab}(x)$, 再复合 g. 换而言之我们发现

$$g\mathrm{Stab}(x)g^{-1}\subset\mathrm{Stab}(gx).$$

反过来一样有

$$g^{-1}\mathrm{Stab}(gx)g\subset\mathrm{Stab}(x).$$

因此我们发现

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

因而，在作用是传递的时，有

$$\ker\alpha = \bigcap_{g\in G}g\mathrm{Stab}(x)g^{-1}.$$

这是一个正规子群。这事实上也启示我们如下平凡的命题：设 $H\le G$，则

$$\bigcap_{g\in G}gHg^{-1}\triangleleft G$$

2. 常见的作用（表示）

群不光可以作用在其它对象上，它很多时候可以自然地作用在自己的某些结构上。在群论的研究中，这是一种极为重要，朴素而强大的方法。我们举几个简单的例子。

[2]据说 Frobenius 早在 Burnside 之前发现了这个结果

2.1. 共轭作用. 群 G 以共轭作用作用在群 G 上，也即

$$\begin{aligned}\alpha : G &\to \mathrm{Sym}(G)\\ x &\mapsto (g \mapsto xgx^{-1})\end{aligned}$$

练习 2.5 (★). 能否将共轭作用定义为

$$\begin{aligned}\alpha : G &\to \mathrm{Sym}(G)\\ x &\mapsto (g \mapsto x^{-1}gx)\end{aligned}$$

为什么这样定义不行？

关于这个作用的轨道就是共轭类，容易看出，作用的核 $\ker\alpha = Z(G)$. 对于 $g \in G$, 其稳定化子 $\mathrm{Stab}(g)$ 我们记作 $C_G(g) = \{h \in G | gh = hg\}$[3], 这是 G 的一个子群。我们把这个情形下的轨道方程

$$|G| = \sum_i [G : C_G(g_i)]$$

称之为群 G 的**类方程**。值得注意的是，有些元素 $g \in G$ 可能轨道长度为 1，也就是只与自己共轭的，中心元素，$Z(G)$. 如果设 $|G| = p^n$，其中 p 是某个素数，则有

$$p^n = |Z(G)| + \sum_{i, g_i \notin Z(G)} [G : C_G(g_i)]$$

易知 $[G : C_G(g_i)]$ 必是 p 的倍数。故此时的 $|Z(G)|$ 必须是 p 的倍数，因此 $|Z(G)| > 1$. 换而言之我们得到了结论

命题 2.1. 设 $|G| = p^n, n > 1$，则 G 有非平凡的中心 $Z(G)$.

练习 2.6 (★). 若以 $c(G)$ 记群 G 的共轭类的个数，证明，有

$$c(G \times H) = c(G) \cdot c(H).$$

练习 2.7 (★★★). 记号如上，本题中设 G 是非 *Abel* 群，证明有

$$c(G) \leq \frac{5}{8}|G|$$

等号能取到吗？进一步，证明，若 p 是 $|G|$ 最小的素因子，则有

$$c(G) \leq \frac{p^2 + p - 1}{p^3}|G|$$

练习 2.8 (★★★★★). 上题中最后的不等式，对任意素数 p, 等号能取到吗？

2.2. 正则表示 (作用). 群 G 以 (左)[4]乘法作用在群 G 上，也即

$$\begin{aligned}\alpha : G &\to \mathrm{Sym}(G)\\ g &\mapsto (a \mapsto ga)\end{aligned}$$

即将 g 自然地视为一个 G 上的置换 $\alpha(g)$. 这是一个忠实表示。

练习 2.9. 证明这是一个忠实、传递的作用。

---

[3]对于 $S \subset G$, 我们以记号 $C_G(S)$ 表示 $\{g \in G | gs = sg, \forall s \in S\}$, 称为 S 的**中心化子**。

[4]也可以定义右正则表示

$$\begin{aligned}\alpha : G &\to \mathrm{Sym}(G)\\ g &\mapsto (a \mapsto ag^{-1})\end{aligned}$$

我们马上得出 Cayley 定理：每个群都同构于某个置换群的子群。这看起来似乎弱智无比，但是就是这样朴素的观点我们可以得到非平凡的结论，我们举一个例子。

命题 2.2. *设 G 是 $4k+2$ 阶群，那么它一定有一个指数为 2 的正规子群。*

Proof. 考虑群的左正则作用

$$\alpha : G \to \mathrm{Sym}(G)$$

由于这是忠实表示，我们可以把 G 与 $\alpha(G)$ 等同起来。那么，每个 $\alpha(g)$ 都是一个 G 上的置换，由于群乘法具有逆的原因，除非 $g = 1$, 这个置换不可能固定任何群中的元素 ($ga = a \Leftrightarrow g = 1$.) 因此可以将 $\alpha(g)$ 写为一些长度大于 1 的不相交轮换的乘积。现取 g 为群中的一个二阶元素，由前面的习题我们知道在偶数阶群中这是一定可以取到的。因此，$\alpha(g)$ 分解成 $2n+1$ 个不相交的对换的乘积，因而是奇置换。于是我们证明了 G 中有奇置换，因而 G 中的所有偶置换构成一个指数为 2 的正规子群。 □

推论 2.1. *设 $k \geq 1$, 则 $4k+2$ 阶群一定不是单群。*

2.3. 诱导表示 (陪集上的表示/作用). 给定了群 G 的一个子群 H 后，有 (左) 陪集集合 G/H，群 G 可以自然地作用在 G/H 上。

$$\begin{aligned} \alpha : G &\to \mathrm{Sym}(G/H) \\ g &\mapsto (aH \mapsto gaH) \end{aligned}$$

这称为 (左) 诱导表示[5]。它显然是传递的。它的核是

$$\ker \alpha = \bigcap_{g \in G} gHg^{-1}$$

并注意事实上有 $\ker \alpha \lhd H$. 运用这个表示可以得到很多厉害 (其实很简单) 的结论。

例 2.3. *设 H 是无限群 G 的一个具有有限指数的真子群，那么 G 一定有一个具有有限指数的真正规子群。*

Proof. 考虑 G 在陪集 G/H 上的诱导表示

$$\rho : G \to \mathrm{Sym}(G/H)$$

由于 $[G : \ker \rho] \leq |\mathrm{Sym}(G/H)| = [G : H]!$ 是有限的，我们完成了命题的证明。 □

以下是另外一个典型的应用

命题 2.3. *设 p 是 $|G|$ 最小的素因子，那么若 $H \leq G$ 且 $[G : H] = p$ 则有 $H \lhd G$.*

Proof. 考虑在陪集集合 G/H 上的诱导表示

$$\alpha : G \to \mathrm{Sym}(G/H)$$

由于有 $G/\ker \alpha$ 同构于 $\mathrm{Sym}(G/H)$ 的一个子群，因而必须有 $|G/\ker \alpha|$ 是 $[G : H]!$ 的因数。现在由于 $\ker \alpha \leq H$, 我们有

$$|G/\ker \alpha| = \frac{|G|}{|\ker \alpha|} = \frac{|G|}{|H|}[H : \ker \alpha]$$

[5]称它为诱导表示，是因为它实际上是 $\mathrm{Ind}_H^G V_0 = \bigoplus_{g \in G/H} gV_0$，其中 V_0 是 H 的一维平凡表示。

是 $[G:H]=p$ 的倍数。由于 p 是 $|G|$ 的最小素因子，我们知道 $[H:\ker\alpha]$ 是 1 或 p 的倍数。若不是 1，必有 $p^2|p!$，这不可能，故

$$H=\ker\alpha\lhd G.$$

□

练习 2.10 (★★)**.** 设 G 是大于 3 阶的单群，$H\leq G$, 证明 $[G:H]>4$.

2.4. 循环群的作用：Cauchy 定理. 本节我们看一个群作用的强大威力的例子，我们证明如下的柯西定理：

定理 2.3 (Cauchy)**.** 设 p 是 $|G|$ 的一个素因数，则 G 中有 p 阶元素。

在开始看证明之前我们来理解一下思路。$p=2$ 的情形已经作为一道练习题做过了，还记得做法吗？大家的做法，估计就是对 G 中的元素配对，g 和 g^{-1} 配一对，二阶元素 g 和 g^{-1} 是相同的，就无法配对，最后因为群的阶数是 2 的倍数，配了对的元素个数也是 2 的倍数，我们得出满足 $x^2=1$ 的元素个数有偶数个。由于 $1^2=1$，我们知道一定有二阶元素。

不过，这个证明初看起来似乎并不能推广到 $p>2$ 的情形。但是，如果你用群与对称的观点重新叙述上面的证明，你马上就可以看出如何作推广。我们要将上述证明中出现的现象理解为一种对称性，那么就一定要有对称变换。我们观察到的现象是什么呢？那就是在所有的有序对 $X=\{(g,g^{-1})|g\in G\}$ 集合上，有一种对称变换 $(x,y)\mapsto(y,x)$. 这就是群 $\mathbb{Z}_2$ 在该集合上的作用。那么 X 拆分为一些轨道的并。而在该作用下轨道的长度为 1 等价于说 $g=g^{-1}$ 也就是 $g^2=1$, 由轨道方程

$$|X|=|\{(g,g)|g^2=1\}|+\sum|\text{其它长为 2 的轨道}|$$

轨道公式表明轨道的长度只能是 1 或 2, 我们立刻得出 $|\{g|g^2=1\}|$ 是 2 的倍数。现在，我想，如何推广这个证明已经至为显然。

Proof. 设 $X=\{(g_1,g_2,\dots,g_p)|g_1g_2\dots g_p=1\}$, 并设 a 是群 $\mathbb{Z}_p$ 的生成元，考虑群 $\mathbb{Z}_p$ 在 X 上的如下作用

$$\begin{aligned}\alpha:\mathbb{Z}_p&\to\mathrm{Sym}(X)\\ a&\mapsto f\end{aligned}$$

其中 $f:X\to X$ 是把 $(g_1,g_2,\dots,g_p)$ 映到 $(g_2,g_3,\dots,g_p,g_1)$ 的映射。

我们需要验证 $g_2g_3\dots g_pg_1=1$, 这可由 $ab=1\Leftrightarrow ba=1$ 得到。现在由轨道方程

$$|G|^{p-1}=|X|=|\{g\in G|g^p=1\}|+\sum|\text{其它长为 }p\text{ 的轨道}|$$

我们立得 $|\{g\in G|g^p=1\}|$ 是 p 的倍数，由 $1^p=1$ 立即知道群 G 中存在 p 阶元素，而且至少有 $p-1$ 个。事实上，可以得到更强的结论：(p 阶元素个数 $+1$) 是 p 的倍数。 □

练习 2.11 (★★)**.** 设 $|G|=mp, 1<m<p$, 其中 p 是素数。证明 $\mathbb{Z}_p\lhd G$.

练习 2.12 (★)**.** 设 G 是 6 阶 *Abel* 群，按如下提示，证明 $G\cong\mathbb{Z}_6$.*(由柯西定理，G 中有 2,3 阶元素。从而 $G\cong\mathbb{Z}_2\times\mathbb{Z}_3\cong\mathbb{Z}_6$.)*

练习 2.13 (★★)**.** 设 G 是 6 阶非 *Abel* 群。按如下提示，证明有 $G\cong S_3$, 从而只有两个 6 阶群：$\mathbb{Z}_6$ 和 S_3.

(1) 先证明 $Z(G)=1$.

(2) 证明 G 中必恰有 3 个 2 阶元素。

(3) 考虑 G 在集合 $X=\{a,b,c\}$ 上的共轭作用，其中 a,b,c 都是 2 阶元素。(需先证明这是 X 上的作用。)
(4) 证明 $\{a,b,c\}$ 能生成群 G，由此证明上述作用是忠实的。同态基本定理给出 $G\cong S_3$.

2.5. 在子群上的共轭作用. 设 $A\leq G$ 是一个子群，容易发现，$g^{-1}Ag$ 也是一个子群。因为映射 $x\mapsto g^{-1}xg$ 是自同构，而自同构限制在子群上还是同构，其像必然为群。我们称子群 A 与 B 共轭，如果 $A=g^{-1}Bg$. 那么容易看出，G 可以以共轭作用作用在它的一些子群上。容易看出，一个子群可以有很多个共轭子群，而 G 的正规子群就是那些在 G 的共轭作用下不变的子群，也就是只与自己共轭的子群，这时它单独组成一个共轭类。

对于 $S\subset G$, 我们以记号 $N_G(S)$ 表示 $\{g\in G|gS=Sg\}$, 称为 S 的**正规化子**。容易看出，$A\leq G$ 的稳定化子是 $N_G(A)$，从而有共轭类的大小为

$$[G:N_G(A)].$$

练习 2.14 (★). 设 $|G|=p^n$，证明 G 的非正规子群个数是 p 的倍数。

3. 群在计数问题中的应用

如果要给一个立方体的两个面涂上红色，有多少种涂法呢？初看起来似乎有

$$\binom{6}{2}=\frac{6\times 5}{2}=15$$

种涂法，但是事实上很多种涂法都是相同的，它们之间只是差一个旋转而已。换而言之我们发现在对称的物件上涂色，只需考虑该物件的对称群，并让这个群作用在所有可能的涂色集合上。想知道两种涂法是不是一样的，只需看它们在不在一个轨道里。故，若要知道本质上不同的涂色有多少种，只需数轨道的个数就可以了！而 Burnside 定理提供了一种方案。

我们举一个简单的例子来说明这个方法。考虑这样一个计数问题：在长度为 n 的圆圈形项链上染色，有 c 种不同的颜色可用。两种染色如果在旋转，翻转 (轴对称) 下是相同的，则视为一种染色。有多少种不同的染色呢？我们考虑群作用的空间

$$X=\{(a_1,a_2,\dots,a_n)|a_i\text{是 } c \text{ 种颜色之一}\}$$

并让 D_n 以如下方式定义作用在该空间上：

(1) $\sigma(a_1,a_2,\dots,a_{n-1},a_n)=(a_2,a_3,\dots,a_n,a_1)$
(2) $\tau(a_1,a_2,\dots,a_{n-1},a_n)=(a_n,a_{n-1},\dots,a_2,a_1)$.

容易看出由于 D_n 中的元素都能表示为 $\sigma^i\tau^j$ 的形式，只需定义 σ,τ 在 X 上的作用即可。不难验证上述定义确实给出了 D_n 在 X 上的一个作用 (需要验证 $\sigma^n=\tau^2=(\sigma\tau)^2=1$ 的作用是平凡的)。那么现在我们的问题就等价于计算 X 中的轨道数目 N，由 Burnside 定理，

$$N=\frac{1}{|D_n|}\sum_{g\in D_n}|X^g|.$$

现在来考虑 X^g 的大小。首先 D_n 可视为 S_n 的子群，它事实上是以下标置换的方式作用在 X 上。于是可设 $g\in D_n$ 在 S_n 中的不相交轮换分解：

$$g=c_1c_2\dots c_k=(c_{11}c_{12}\dots c_{1l_1})(c_{21}c_{22}\dots c_{2l_2})\dots$$

其中 $c_i=(c_{i1}c_{i2}\dots c_{il_i})$ 是一些不相交的轮换，长度为 l_i. 比如 $\sigma=(123\dots n)$, $\tau=(1,n)(2,n-1)\dots$.

如果 g 要固定一个 $x \in X$, 即 $gx = x$, 我们可以得到

$$x = (a_1, a_2, \ldots, a_n) = (a_{g(1)}, a_{g(2)}, \ldots, a_{g(n)})$$

即 $a_i = a_{g(i)}$. 由 $gx = x$ 自然有 $g^k x = x$, 从而 $a_{c_{11}} = a_{c_{12}} = \cdots = a_{c_{1l_1}}$. 这表明在轮换 c_1 的所有分量中对应的位置必须为相同的涂色。类似的，在所有轮换上都能得到相同的结果，从而 $|X^g| = c^{g\text{的轮换个数}}$, 注意考虑轮换时要包含 1 轮换.

注意到在 D_n 的同一个共轭类中的元素的轮换分解形状是相同的，一般来说只需要找出 D_n 中所有共轭类并将其轮换分解算出即可。在本例中，我们可以考虑

$$D_n = \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau\sigma, \tau\sigma^2, \ldots, \tau\sigma^{n-1}\}$$

注意到 $\sigma^j(\tau\sigma^i)\sigma^{-j} = \sigma^j\tau\sigma^{i-j} = \tau\sigma^{i-2j}$, 因此当 n 为奇数时，所有 $\tau\sigma^i$ 都是共轭的，于是与 τ 一样，形如

$$\tau = (1, n)(2, n-1)\ldots\left(\frac{n-1}{2}, \frac{n+3}{2}\right)\left(\frac{n+1}{2}\right)$$

都有 $\frac{n-1}{2} + 1 = \frac{n+1}{2}$ 个轮换。当 n 为偶数时可能分为两个共轭类 $\tau\sigma^{2k+1}$ 和 $\tau\sigma^{2k}$, 分别与 $\tau\sigma$ 和 τ 一样，分别具有 $\frac{n}{2}$ 和 $\frac{n}{2} + 1$ 个轮换。

对于 $\mathbb{Z}_n \leq D_n$ 中的元素，σ^k 在 k 与 n 互素时都是长度为 n 的轮换。当他们的最大公因数 $(k, n) = d$ 时，是 d 个长度为 $\frac{n}{d}$ 的轮换之积。回忆我们之前在循环群一节说过对于 n 的因子 d, $\frac{n}{d}$ 阶子群 $d\mathbb{Z}_n \leq \mathbb{Z}_n$ 的生成元，也就是满足 $(k, n) = d$ 的元素 σ^k 的个数为欧拉函数 $\varphi\left(\frac{n}{d}\right)$，于是现在我们可以得出 N 的计算公式

$$\begin{aligned} N &= \frac{1}{|D_n|}\sum_{g\in D_n}|X^g| \\ &= \frac{1}{2n}\left(\sum_{k=1}^{n} c^{(k,n)} + 1_{2|n}\frac{n}{2}c^{\frac{n}{2}} + 1_{2|n}\frac{n}{2}c^{\frac{n}{2}+1} + 1_{2|n+1}nc^{\frac{n+1}{2}}\right) \\ &= \frac{1}{2n}\sum_{d|n}\varphi\left(\frac{n}{d}\right)c^d + 1_{2|n}\frac{c^{\frac{n}{2}}(c+1)}{4} + 1_{2|n+1}\frac{c^{\frac{n+1}{2}}}{2}. \end{aligned}$$

练习 2.15 (★★)**.** 假定在长度为 $2n$ 的项链上，要求只用两种颜色且每种颜色必须恰好使用 n 个珠子。有多少种不同的染色方法？

4. Sylow 定理

Sylow(西罗) 定理可能是初等群论中最重要的一个定理，它也是群的作用的一个精妙的应用。

定理 2.4 (Sylow)**.** *设 G 是群，$|G| = mp^n$, 素数 $p \nmid m$. 那么有:*

(1) *存在 p^n 阶的子群 $P \leq G$, 称为 G 的 Sylow-p 子群。*

(2) *以 $N(p^r)$ 记 G 的 p^r 阶子群的个数，$r \leq n$，有*

$$N(p^r) \equiv 1 \mod p.$$

(3) *所有 Sylow-p 子群互相共轭，因而有 $N(p^n) = [G : N_G(P)]$.*

值得注意的是，一般的 p 子群未必是互相共轭的。

Proof. 令 $|G| = np^r$(没有要求 n 与 p 互素，即不要求 r 是极大的)，我们来考虑 G 中所有 p^r 元子集，其全体记为 X，有 $|X| = \binom{np^r}{p^r}$. 现在可以考虑 G 在 X

上的左乘作用：

$$\begin{aligned}\rho : G &\to \mathrm{Sym}(X)\\ g &\mapsto (S \mapsto gS)\end{aligned}$$

我们将 X 拆分为一些轨道的并

$$X = \bigcup_{i=1}^{m} X_i$$

并有 $|X_i| = [G : \mathrm{Stab}(S_i)]$. 由于 $\mathrm{Stab}(S_i)S_i = S_i$ 我们可以分解

$$S_i = \bigcup_{j=1}^{k_i} \mathrm{Stab}(S_i)g_{ij}$$

于是有 $k_i|\mathrm{Stab}(S_i)| = p^r$ 以及 $|X_i| = nk_i$. 注意到 k_i 一定形如 p 的某个次方，并且 $k_i = 1$ 当且仅当 S_i 形如 Pg, 其中 $P \le G$ 是 G 的一个 p^r 阶子群, $g \in G$. 于是 $k_i = 1$ 当且仅当 T_i 中恰好包含了一个 p^r 阶子群，这表明

$$|X| = \binom{np^r}{p^r} = \sum_{i=1}^{m} nk_i \equiv n \sum_{k_i=1} 1 \mod np.$$

于是

$$\frac{1}{n}\binom{np^r}{p^r} \equiv N(p^r) \mod p.$$

现在只需计算左边的数模 p 的余数。首先它等于 $\binom{np^r-1}{p^r-1}$，于是等于表达式 $(1+x)^{np^r-1}$ 第 p^r-1 次的系数。在模 p 的形式幂级数环 $\mathbb{Z}_p[\![x]\!]$ 中考虑该表达式，有

$$\frac{(1+x)^{np^r}}{1+x} = \frac{(1+x^{p^r})^n}{1+x} = (1+nx^{p^r}+\dots)(1-x+\dots+(-1)^{p^r-1}x^{p^r-1}+\dots)$$

我们得出所求系数模 p 为 $(-1)^{p^r-1} \equiv 1$, 于是我们得到所需命题。当然，也可以用其它方法算出该数，比如直接计算，或者考虑 G 为循环群的特殊情形，我们知道此时必有 $N(p^r) = 1$，但等式左边的数与群无关，只与群的阶数有关，这就直接给出了所需结果。

现在我们来证明所有 Sylow-p 子群是互相共轭的。首先，G 在所有 Sylow-p 子群上有共轭作用，并且每个轨道的阶数 $[G : N_G(P)]$ 必然与 p 互素。取 P 是 G 的一个 Sylow-p 子群，考虑 P 在全体 Sylow-p 子群上的共轭作用。于是 Q 在 P 的作用下不动等价于说 $P \le N_G(Q)$. 此时考虑投射 $P \to N_G(Q) \to N_G(Q)/Q$，由于商群 $N_G(Q)/Q$ 的阶数里没有 p，而 P 中的元素都是 p^k 阶的，我们知道这个投射的像必然是 1，于是得到 $P \le Q$，因此 $P = Q$. 这表明只有 P 自己在该共轭作用下不动，其它轨道都是长度为 p 的次方。但是 G 的共轭作用下每个轨道都不被 p 整除，因而其每个轨道限制在 P 上作用时，必然出现长度为 1 的轨道，而我们已经证明只有 P 自己在共轭作用下不动，于是只能有一个 G-轨道。 □

推论 2.2. *如果 $|G| = np^r$, n 与 p 互素，且有唯一的一个 Sylow-p 子群，则这个子群是正规子群。*

推论 2.3. *如果 $|G| = np^r$, n 与 p 互素，则 $N = N(p^r) = [G : N_G(P)]$ 是 n 的因数且形如 $pk+1$.*

例 2.4. 我们来证明，15 阶群一定是循环群。根据 *Sylow* 定理可以考虑 G 的两个分别为 3 和 5 阶的 *Sylow* 子群 P_3 和 P_5. 并且有 $N(3) \equiv 1 \mod 3$ 并且 $N(3)$ 是 5 的因数。但满足同余式的数只有 1. 同理我们发现 $N(5) = 1$，因此对 $|G|$ 的所有因数 d 都只有一个 d 阶子群，它必然是循环群。

练习 2.16. 设 G 是 40 阶群。证明它有一个正规的 5 阶子群。

练习 2.17 (★★). 设 P 是 G 的一个 *Sylow-p* 子群，证明，若 $N \triangleleft G$ 或者 $P \triangleleft G$, 则 $N \cap P$ 是 N 的一个 *Sylow-p* 子群。

练习 2.18 (★★★★). 证明，若 $H \leq G$, P 是 G 的一个 *Sylow-p* 子群，则存在 $g \in G$ 使得 $H \cap gPg^{-1}$ 是 H 的一个 *Sylow-p* 子群。

练习 2.19. 找出 S_3 的所有 *Sylow*-2 子群和 *Sylow*-3 子群。

练习 2.20 (★★★). 试找出 S_4 的所有 *Sylow* 子群。

就像我们已经看到的那样，Sylow 定理经常和共轭作用联合使用，这是因为它们之间有天然的关系：Sylow-p 子群是互相共轭的。除了 Sylow 定理最常见的数字上的应用必须熟练掌握以外，和共轭作用联合使用往往能得出非平凡的结论。

4.1. 运用 Sylow 定理寻找正规子群. 寻找正规子群很重要，通常可以用来分类群的结构/证明一个群不是单群。而 Sylow 定理一个常见的应用是用 Sylow 定理来寻找正规子群，以下是利用 Sylow 定理寻找正规子群的常见的方法。

- 取 $|G| = np^r$ 使 p 与 n 互素, 计算 Sylow-p 子群 P 的可能个数 N, 它满足
$$\begin{cases} N \equiv 1 \mod p \\ N\text{是 } |G| \text{ 的因数} \end{cases}$$
- 如果 $N = 1$，则由 Sylow 定理我们知道 $P \triangleleft G$.
- 若 $r = 1$, 则可考虑对每个 $r = 1$ 的素数 p, 对应的所有 P 所占的元素个数至少为 $N(p-1)+1$, 有可能利用这一点说明不可能有这么多 Sylow 子群。
- 若 $r = 2$, 还可考虑两个 Sylow 子群的交 $H = P_1 \cap P_2$, 如果 $|P|^2 > |G|$ 则一定有 $|H| = p$(因为 $|P_1P_2| = |P|^2/|P_1 \cap P_2|$), 并且有 $P_1, P_2 \leq N_G(H)$ 从而 $G = N_G(H)$, $H \triangleleft N_G(H) = G$.
- 还可考虑群 G 在 $X = \{P_1, P_2, \ldots, P_N\}$ 上的共轭作用 $\rho : G \to \mathrm{Sym}(X)$, 其核 $\ker\rho$ 可能为 G 的非平凡正规子群。

例 2.5. 我们证明，36 阶群不是单群。考虑它的 9 阶子群的个数 N, 有 $N = 1$ 或 4. 若 $N = 4$，考虑 G 在这四个 *Sylow*-3 子群上的共轭作用

$$\rho : G \to S_4$$

而 $|S_4| = 24$ 因此 ρ 不可能是单射，并且由 *Sylow* 子群在 G 的共轭作用下传递我们知道上述作用不是平凡作用，于是 $\ker\rho \triangleleft G$ 构成了 G 的一个非平凡正规子群。

还有另一种证明，若 $N = 4$, 考虑 $H = P_1 \cap P_2$. 由于 $36 \geq |P_1P_2| = 81/|H|$ 我们知道必然有 $|H| = 3$. 但是 $P_1, P_2 \leq N_G(H)$，于是有 $N_G(H)$ 包含了 P_1, P_2 生成的群，故而 $G = N_G(H) \triangleright H$ 是 G 的非平凡正规子群。

练习 2.21 (★). 证明 150 阶群不是单群。

4.2. 运用 Sylow 定理与共轭作用. 如何来综合运用 Sylow 定理与共轭作用呢? 如下引理描述了共轭作用如何与 Sylow 子群相互作用。

引理 2.1. 设 H 是某个 p 子群，作用在所有的 *Sylow-p* 子群上，则 P_i 单独组成一个轨道 $\Leftrightarrow H \leq P_i$

Proof. 有一边是显然的，我们来证明另一边。设 $a^{-1}Pa = P$ 且 a 是 p^k 阶元素，则 $a \in N_G(P)$. 由于 $P \triangleleft N_G(P)$, 考虑 a 在投射

$$N_G(P) \to N_G(P)/P$$

下的像，由于 $|N_G(P)/P|$ 显然与 p 互素，其像只能为单位元，故 $a \in P$. 这足以证明命题。 □

命题 2.4. *G 的每个 p 方幂阶的子群 H 被某个 Sylow-p 子群包含。*

Proof. 考虑用 H 共轭作用在 G 的所有 Sylow-p 子群上，则其轨道长度为 1 或 p 的倍数。由于 Sylow-p 子群的个数是 $\equiv 1 \mod p$, 我们知道一定有一个 P 单独组成一个轨道，因而由引理 $H \leq P$. □

命题 2.5. *设 H 是一个 p 子群，则包含它的 Sylow-p 子群的个数 $a \equiv 1 \mod p$.*

Proof. 让 H 作用在所有 Sylow-p 子群上，$H \leq P$ 等价于 P 的轨道长度为 1. 由于所有 Sylow-p 子群的个数 $\equiv 1 \mod p$, 我们有

$$a \equiv a + \text{其它轨道} = N \equiv 1 \mod p.$$

□

5. 有限生成 Abel 群的结构

我们来研究所有能被有限个元素生成的 Abel 群的结构。注意不是所有 Abel 群都是有限生成的，比如 $\mathbb{Q}$ 就无法被其中有限个元素生成。最简单的有限生成 Abel 群的例子是所谓 n 元自由 Abel 群 $\mathbb{Z}^n = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$，其由 n 个元素生成: $e_1 = (1, 0, \ldots, 0), e_2 = (0, 1 \ldots, 0), \ldots, e_n$. 它也可以称为自由 $\mathbb{Z}$ 模: $\mathbb{Z}$ 模和 Abel 群是同一个概念。

设 Abel 群 G 能被其中有限个元素 $g_1, \ldots, g_n \in G$ 生成，那么可以定义如下群的满同态

$$\varphi : \mathbb{Z}^n \to G$$
$$\sum_{i=1}^{n} a_i e_i \mapsto \sum_{i=1}^{n} a_i g_i.$$

那么，根据同态基本定理，就有 $G \cong \mathbb{Z}^n / \ker \varphi$. 于是，我们的目标便在于研究，$\mathbb{Z}^n$ 的所有子群长什么样，由此我们可以知道所有可能的商群。

先看 $n = 1$ 的简单情形，我们知道 $\mathbb{Z}$ 的子群只有 0 和 $n\mathbb{Z}$ 而已，$n \geq 1$. 于是 $\mathbb{Z}$ 的非平凡子群都是同构于 $\mathbb{Z}$ 的。

我们将在第四章证明如下 (本质是线性代数) 的重要结果

定理 2.5. *$\mathbb{Z}^n$ 的子群一定是自由 Abel 群，即同构于 $\mathbb{Z}^m$ 并且有 $m \leq n$. 事实上，设 $H \leq \mathbb{Z}^n$ 则有一组 $\alpha_i \in G$ 以及一组非负整数 d_i 使得 $d_i | d_{i+1}$ 且*

$$H = \mathbb{Z}d_1\alpha_1 \oplus \mathbb{Z}d_2\alpha_2 \oplus \ldots \mathbb{Z}d_n\alpha_n.$$

推论 2.4. *所有的有限生成 Abel 群都同构于某种*

$$\mathbb{Z}^m \oplus \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \cdots \oplus \mathbb{Z}_{d_k}.$$

推论 2.5. *所有有限 Abel 群都是有限循环群的直和。*

6. 半直积

半直积是一个群论中常用的重要概念。如果 $N \triangleleft G$, 则可以构作商群 $Q = G/N$. 我们可能会想，会不会有 $G \cong N \times Q$ 成立? 对于绝大部分情形，这是不成立的。例如，读者可以考虑 $G = \mathbb{Z}_4, N = 2\mathbb{Z}_4$ 的情形，显然 $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$.

如果 Q 能够自然的实现为 G 的一个子群, 即存在 $Q \leq G$ 在自然投射 $G \to G/N$ 下刚好是同构的，即合成

$$Q \to G \to G/N$$

是同构映射的话，我们可以断言一个稍弱的命题：G 是 N 和 Q 的半直积，即 $G \cong N \ltimes Q$. 让我们来说明这一点，我们可以从 N 和 Q 把 G 重新构造出来：每个 $g \in G$ 在 Q 中有一个像 q, 那么 $gq^{-1} \in N$, 也就是说，$g = nq$，显然这样的表示法是唯一的. 由于 $N \triangleleft G$, $G = NQ$ 上的乘法运算也可以由 Q 在 N 上的共轭作用恢复出来：

$$(n_1q_1)(n_2q_2) = n_1q_1n_2q_1^{-1}(q_1q_2).$$

这启发我们从 N 和 Q 以及 (共轭作用) 同态 $\theta : Q \to \mathrm{Aut}(N)$ 在集合 $N \times Q$ 上定义一个如下的群结构：

$$(n_1, q_1)(n_2, q_2) = (n_1\theta_{q_1}(n_2), q_1q_2).$$

群中的幺元是 $(1, 1)$，逆元是 $(\theta_{q^{-1}}(n^{-1}), n^{-1})$. 可以验证这样的定义满足结合律，于是 $N \times Q$ 在上述乘法下构成一个群，我们记作 $N \rtimes_\theta Q$，称作 N 和 Q 的半直积。

练习 2.22 (★). 验证上述定义中的结合律。

例 2.6. $G = \mathbb{Z}_3 \rtimes_\theta \mathbb{Z}_2$ 根据 $\theta : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$ 的选取有两种可能：

(1) 若 $\theta = 1_{\mathbb{Z}_3}$ 为常单位值同态，则 $G = \mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$.
(2) 若 θ 为将 $\theta(1)$ 映射到 $\alpha \in \mathrm{Aut}(\mathbb{Z}_3)$ 中唯一非平凡的自同构 $\alpha(a) = a^{-1}$ 的同态，则有

$$G = \langle a, b | a^3 = b^2 = 1, bab^{-1} = a^{-1} \rangle \cong D_3.$$

练习 2.23. 验证 $D_n \cong \mathbb{Z}_n \rtimes_\theta \mathbb{Z}_2$, 同态 θ 是什么？

我们给出下面一个简单的判别法

命题 2.6. 若 $N \triangleleft G$，$Q \leq G$ 并且 $G = NQ$ 以及 $N \cap Q = 1$ 则有

$$G \cong N \rtimes_\theta Q$$

其中 θ 就是 Q 在 N 上的共轭作用。

Proof. 从 $G = NQ$ 以及 $N \cap Q = 1$ 可以看出每一个元素 $g \in G$ 都可以唯一的表示成 nq 的形式。因此由半直积的构造我们知道，可以定义明显的同态

$$G \to N \rtimes_\theta Q$$

它显然是单满射。 □

练习 2.24 (★). 验证 $G = N \rtimes H$ 中，$N \triangleleft G$.

值得注意的是，虽然在半直积 $N \rtimes_\theta Q$ 中，θ 的选取有很多种可能，但是不同的选取可能作出同构的群。(事实上，同一个群也有可能有不同的半直积表示。) 为了应用中方便看出这些同构的群, 我们给出以下两个判别法来判断 $N \rtimes_\theta Q \cong N \rtimes_{\theta'} Q$.

命题 2.7 (N 的对称)**.** 如果存在 $\alpha \in \mathrm{Aut}(N)$ 使得对所有的 n, q 都有

$$\theta_q(n) = \alpha^{-1}(\theta'_q(\alpha(n)))$$

或者等价的说，有交换图表

$$\begin{array}{ccc} N & \xrightarrow{\alpha} & N \\ {\scriptstyle \theta_q}\downarrow & & \downarrow{\scriptstyle \theta'_q} \\ N & \xrightarrow{\alpha} & N \end{array}$$

那么就有 $N \rtimes_\theta Q \cong N \rtimes_{\theta'} Q$.

Proof. 构作同态 $\varphi : N \rtimes_\theta Q \to N \rtimes_{\theta'} Q$

$$\varphi(n, q) := (\alpha(n), q).$$

首先验证它是一个同态，我们有

$$\begin{aligned} \varphi((n_1, q_1)(n_2, q_2)) &= \varphi(n_1\theta_{q_1}(n_2), q_1q_2) \\ &= (\alpha(n_1)\alpha(\theta_{q_1}(n_2)), q_1q_2) \\ &= (\alpha(n_1)\theta'_{q_1}(\alpha(n_2)), q_1q_2) \\ &= \varphi(n_1, q_1)\varphi(n_2, q_2). \end{aligned}$$

它显然是单满射。 □

完全类似的我们有如下命题

命题 2.8 (Q 的对称)**.** 如果存在 $\beta \in \mathrm{Aut}(Q)$ 使得对所有的 n, q 都有

$$\theta_q(n) = \theta'_{\beta(q)}(n)$$

或者等价的说，有交换图表

$$\begin{array}{ccc} Q & \xrightarrow{\theta} & \mathrm{Aut}(N) \\ \downarrow{\scriptstyle \beta} & & \\ Q & \xrightarrow{\theta'} & \mathrm{Aut}(N) \end{array}$$

那么就有 $N \rtimes_\theta Q \cong N \rtimes_{\theta'} Q$.

练习 2.25 (★)**.** 证明上述命题。

练习 2.26 (★)**.** 证明群同构

$$\langle a, b | a^3 = b^7 = 1, aba^{-1} = b^2 \rangle \cong \langle a, b | a^3 = b^7 = 1, aba^{-1} = b^4 \rangle.$$

练习 2.27 (★★★)**.** 找出所有 pq 阶群，p, q 都是素数。证明最多只有两个不同的同构类。

练习 2.28 (★★★)**.** 若 $G = \mathbb{Z}_p \rtimes_\theta \mathbb{Z}_n$，其中 p 是一个素数，证明 G 的共轭类个数 $c(G)$ 满足

$$c(G) = n\left(1 + \frac{p-1}{h^2}\right).$$

其中 h 表示 θ 的阶，即使 $\theta^h = 1$ 的最小数。

练习 2.29 (★★★)**.** 若 Q 是循环群，并且 $\theta(Q)$ 与 $\theta'(Q)$ 在 $\mathrm{Aut}(N)$ 中共轭，证明

$$N \rtimes_\theta Q \cong N \rtimes_{\theta'} Q.$$

(提示：证明有 $\alpha \in \mathrm{Aut}(N), \beta \in \mathrm{Aut}(Q)$ 使 $\alpha^{-1} \circ \theta_q \circ \alpha = \theta'_{\beta(q)}$.)

7. $|G| \leq 15$ 的所有群

这一节将包含相当多的例子：我们将分类所有阶数不超过 15 的群，即在此中找出所有不同构的群。首先，应当注意到，p 是素数时，p 阶群仅有 p 阶循环群 $\mathbb{Z}_p$ 这一个。于是还剩下 $n = 4, 6, 8, 9, 10, 12, 14, 15$ 这些阶数。我们已经证明 p^2 阶群只有两个，$\mathbb{Z}_{p^2}$ 和 $\mathbb{Z}_p^2$. 现在考虑如下命题

命题 2.9 ($|G| = pq$ 的情况)**.** *设 $1 < p < q$ 是两个素数，G 是 pq 阶群，则*

(1) *若 $p|q-1$, 则 $G \cong \mathbb{Z}_{pq}$ 或 $G \cong \mathbb{Z}_q \rtimes \mathbb{Z}_p$.*
(2) *若 $p \nmid q-1$, 则 $G \cong \mathbb{Z}_{pq}$.*

Proof. 由 Sylow 定理指出 q 阶循环子群，记为 $\mathbb{Z}_q$，是 G 的正规子群。取 $\mathbb{Z}_p$ 是 G 的一个 Sylow-p 子群，由于显然 $|\mathbb{Z}_q \cap \mathbb{Z}_p| = 1$ 以及 $G = \mathbb{Z}_p\mathbb{Z}_q$ 我们得到 $G = \mathbb{Z}_q \rtimes_\theta \mathbb{Z}_p$, 其中

$$\theta : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_q) \cong \mathbb{Z}_{q-1}.$$

这表明，若 $p \nmid q-1$, 上述映射必然是平凡的，于是 $G \cong \mathbb{Z}_q \times \mathbb{Z}_p \cong \mathbb{Z}_{pq}$. 若 $p|q-1$, 考虑非平凡 θ 的选取，这样 θ 就成了单同态。但 $\mathbb{Z}_p$ 在 $\mathbb{Z}_{q-1}$ 中的嵌入像只有一个，于是这些非平凡态射之间只差 $\mathbb{Z}_p$ 的一个自同构。于是使用 Q 的对称引理告诉我们它们导出的群都是同构的。 □

于是要讨论的主要难点集中在 $n = 8, 12$ 这两个阶数上。

7.1. 8 阶群的分类. 交换的 8 阶群只有 $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ 以及 $\mathbb{Z}_2^3$. 下面我们来研究非交换的 8 阶群。由 Sylow 定理可知 G 有 $2k+1$ 个 4 阶子群。不可能有 5 个，否则将至少占用 $5 \times (4-2) + 2 = 12$ 个元素。因此只能有 1 个或者 3 个。

如果只有一个 4 阶子群 $H \lhd G$, 必然有 $H \cong \mathbb{Z}_4$, 否则若 $H \cong \mathbb{Z}_2^2$, G 中将没有 4 阶元素，推出 G 的元素都是 $1, 2$ 阶于是 G 是 Abel 的，这与我们讨论的情况无关。那么现在 $H = \mathbb{Z}_4$. 设 $a \in G - H$, 则必然有 $G = \langle a \rangle H \cong \mathbb{Z}_4 \rtimes \mathbb{Z}_2 \cong D_4$, 共轭作用的非平凡选择只有一种。但实际上 D_4 有 3 个 4 阶子群 $\langle \sigma \rangle, \langle \sigma^2, \tau \rangle, \langle \tau\sigma, \sigma^2 \rangle$.

如果有 3 个 4 阶子群，注意指数为 2 的子群都是正规的。由柯西定理我们任意取一个 2 阶元素 b，如果它不属于某一个 4 阶子群，G 必然是半直积，于是可能为 $\mathbb{Z}_4 \rtimes \mathbb{Z}_2$，这就是上面的 D_4. 如果是 $\mathbb{Z}_2^2 \rtimes \mathbb{Z}_2 = \langle a, b, c | a^2 = b^2 = (ab)^2 = c^2 = 1, cac^{-1} = b \rangle$ 的情况，取 $a = \tau\sigma, b = \tau\sigma^3, c = \tau$ 我们发现这还是 D_4.

现在设所有二阶元素 b 都属于所有 4 阶子群，由于这些 4 阶子群中至少有一个是 $\mathbb{Z}_4$(否则 G 中只有二阶元素就 Abel 了)，我们推出只有一个二阶元素 $b \in G$. 这将表明所有 4 阶子群都是形如 $\mathbb{Z}_4$ 的。设 i, j, k 是它们分别的生成元，则有 $i^2 = j^2 = k^2 = b$. 现在考虑元素 ij, 它不可能属于 $\langle i \rangle$ 或 $\langle j \rangle$, 否则若 $ij = i^k$ 就能推出 $j \in \langle i \rangle$，这将表明 $\langle i \rangle = \langle j \rangle$，这不可能。于是必有 $ij \in \langle k \rangle - \{b\}$, 如果 $ij = k$ 则有 $ijk = b$. 如果 $ij = k^{-1} = kb$，通过重新选择 k 为 k^{-1} 我们可以化归到上一种情况。这些关系已经决定了群 G, 我们记这个群为 Q_8，称为四元数群。事实上，这个群正是由四元数体中的 $\{i, j, k\}$ 所生成的

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}.$$

现在我们来说明 Q_8 不同构于 D_4，这只需注意到 Q_8 中有 1 个二阶元而 D_4 中有 5 个。

7.2. 12 阶群的分类. 对于 12 阶群，Abel 群容易看出只有 $\mathbb{Z}_{12}, \mathbb{Z}_2 \times \mathbb{Z}_6$ 这两个。现在只需考虑非 Abel 群的情形。对 G 用 Sylow 定理可知，G 有 1 个或 3 个正规的四阶子群 H, 还有 1 个或 4 个三阶子群 K. 现在可以看出 $G = H \rtimes K \cong H \rtimes_\theta \mathbb{Z}_3$, 其中 $H \cong \mathbb{Z}_4$ 或者 $\mathbb{Z}_2^2$ 并且 $\theta : \mathbb{Z}_3 \to \mathrm{Aut}(H)$ 考虑为非平凡同态 (平凡同态则得到直积，就是我们提到的两个 Abel 群了)。

先假设它有一个正规的 4 阶子群 H. 若 $H = \mathbb{Z}_4$, 考虑 $\theta : \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$, 则 θ 必然是平凡的。

若 $H = \mathbb{Z}_2 \times \mathbb{Z}_2$, 我们知道 $\mathrm{Aut}(H) \cong S_3$ 是 H 中 3 个 2 阶元的置换群，则考虑映射 $\theta : \mathbb{Z}_3 \to \mathrm{Aut}(H) = S_3$ 映到 S_3 的唯一一个三阶子群 $A_3 \cong \mathbb{Z}_3$. 于是 θ 可看成 $\mathbb{Z}_3 \to A_3 \cong \mathbb{Z}_3$ 的同构，从而不同的 θ 选取只差一个 $\mathrm{Aut}(\mathbb{Z}_3)$ 中的元素，由 Q 的对称引理可知它们导出的群 $G = \mathbb{Z}_2^2 \rtimes \mathbb{Z}_3$ 是同构的。事实上，这个群并不是陌生的新群。

练习 2.30 (★)**.** 看出上述群就是 A_4.

现在来考虑它有 3 个 4 阶子群的情形，由于这 3 个四阶子群必定占掉 $(4-2) \times 3 + 1 = 7$ 个元素，因此不可能有 4 个 3 阶子群，因为 4 个 3 阶子群将至少占去 $(3-1) \times 4 + 1 = 9$ 个元素。我们推出此时只能有一个 3 阶子群 K，因而它是正规的。若 $H = \mathbb{Z}_4$, 只有一种非平凡的半直积 $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$.

如果 $H = \mathbb{Z}_2^2$, 那么 $\theta : \mathbb{Z}_2^2 \to \mathrm{Aut}(Z_3) \cong \mathbb{Z}_2$. 容易看出只有三种非平凡的映射 θ 可以选取。但这三种选取只相差 $\mathbb{Z}_2^2$ 的一个自同构，于是决定了相同的群 $\mathbb{Z}_3 \rtimes \mathbb{Z}_2^2$. 事实上它就是 D_6.

练习 2.31 (★)**.** 证明它是 D_6.

现在我们来证明 $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ 既不是 D_6 也不是 A_4. 由于 A_4 中没有 3 阶的正规子群，$\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ 不可能同构于 A_4. 而 D_6 中没有 4 阶元素，所以也不可能同构于它。

7.3. 小阶群表. 将我们的讨论以表格的形式总结起来，我们有如下所有不超过 15 阶的群的表格

阶数	Abel	非 Abel
2	$\mathbb{Z}_2$	
3	$\mathbb{Z}_3$	
4	$\mathbb{Z}_4, \mathbb{Z}_2^2$	
5	$\mathbb{Z}_5$	
6	$\mathbb{Z}_6$	S_3
7	$\mathbb{Z}_7$	
8	$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2^3$	D_4, Q_8
9	$\mathbb{Z}_9, \mathbb{Z}_3^2$	
10	$\mathbb{Z}_{10}$	D_5
11	$\mathbb{Z}_{11}$	
12	$\mathbb{Z}_{12}, \mathbb{Z}_2^2 \times \mathbb{Z}_3$	$A_4, D_6, \mathbb{Z}_3 \rtimes \mathbb{Z}_4$
13	$\mathbb{Z}_{13}$	
14	$\mathbb{Z}_{14}$	D_7
15	$\mathbb{Z}_{15}$	

CHAPTER 3

环与域

1. 定义和例子

从运算的角度讲，群是一个带有“乘法运算”的集合。当这个群是交换群时，这个运算通常写作加法。如果我们在集合上考虑加法与乘法两种运算呢？比如 $\mathbb{Z}$ 在加法下是一个 Abel 群，但同时还有乘法的结构。这是一种新的代数结构，叫做环。当然环上的加法和乘法不能随便给定，它们需要互相兼容，满足一些合理的运算性质。完整的定义如下

定义 3.1 (环)**.** 一个集合 R 附带两种运算 $(+)$ 和 $(\cdot)$ 叫做**环 (ring)**，如果 R 在 $+$ 运算下构成一个 Abel 群，并且对任意的 $a, b, r \in R$ 满足

(1) (结合律) $(ab)r = a(br)$
(2) (分配率) $r(a+b) = ra + rb$, $(a+b)r = ar + br$
(3) 存在乘法幺元 $1 \in R$ 满足 $r1 = 1r = r$.

这里像通常一样约定了乘法的运算优先级高于加法，并且省略了字母之间的乘号。在环中，我们用 0 表示加法幺元，1 表示乘法幺元。

值得注意的是在环的定义中我们不要求乘法一定是交换的，我们只要求加法一定是交换的。如果乘法还具有交换律，我们就把 R 称为交换环。

定义 3.2 (域)**.** 如果 R 是一个环，并且任意非 0 元素 $r \in R$ 在 R 中都有乘法逆 $r^{-1} \in R$ 满足

$$r^{-1}r = rr^{-1} = 1$$

则我们称 R 是一个**体**。如果 R 的乘法交换，则称 R 是一个**域**。

在环中，非零元素不一定有乘法逆。如果非零元素 $r \in R$ 有乘法逆，我们就称 r 是**单位**。

练习 3.1. 找出环 $\mathbb{Z}$ 中所有单位。

环与域的概念在代数中有很多的例子，我们举几个常见的例子

例 3.1. 全体整数 $\mathbb{Z}$ 在通常的加法和乘法下构成一个环。

例 3.2. 全体有理数 $\mathbb{Q}$, 实数 $\mathbb{R}$, 复数 $\mathbb{C}$ 在通常的运算下都构成域。

例 3.3. 以整数为系数的所有 x 的多项式构成的集合

$$\mathbb{Z}[x] := \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 | a_i \in \mathbb{Z}, n \geq 0\}$$

在通常的多项式乘法和加法下构成一个环。类似的可以定义任何一个环 R 上的多项式环

$$R[x] := \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 | a_i \in R, n \geq 0\}$$

这也是一个环，其加法按通常的定义给出，乘法按

$$\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{j=0}^{n} b_j x^j\right) = \sum_{k=0}^{m+n}\left(\sum_{i+j=k} a_i b_j\right) x^k$$

定义。容易验证其满足结合律，分配率。

例 3.4. 设 S 是由所有有限字符串组成的集合，定义 $\mathbb{Z}[S]$ 是这样一个环，它由所有字符串 *(*还有 $\mathbb{Z}$*)* 的有限形式和组成，比如

$$5 + 2hello - 3world \in \mathbb{Z}[S]$$

加法按自然的方式给出，乘法由字符串的连接给出：

$$abc \cdot adc = abcadc$$

$$(2a + 3b)(2a - 3b) = 4aa - 6ab + 6ba - 9bb.$$

在这个定义下，$\mathbb{Z}[S]$ 构成了一个非交换环，例如 $a \cdot b = ab$ 而 $b \cdot a = ba$.

练习 3.2. 全体自然数 $\mathbb{N} = \{0, 1, 2, \dots\}$ 在通常整数运算下构成一个环吗？

练习 3.3 (★). 验证集合 $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$ 在通常运算下构成一个环。

练习 3.4 (★). 考虑集合

$$\mathbb{Z}_{(2)} := \left\{ \frac{a}{b} \in \mathbb{Q} \,\middle|\, \text{作为既约分数，其分母}b\text{是奇数} \right\}.$$

它是一个环吗？是一个域吗？

练习 3.5 (★★). 设 $\mathbb{H} = \{a + bi + cj + dk | a, b, c, d \in \mathbb{R}\}$ 是由如下规则定义的一个环，其乘法由

$$ij = k, jk = i, ki = j$$

$$ji = -k, kj = -i, ik = -j$$

$$i^2 = j^2 = k^2 = -1$$

确定。称 $\mathbb{H}$ 为四元数代数，请你验证它是一个体。*(*提示：考虑 $(a+bi+cj+dk)(a-bi-cj-dk)$*)*

类似的，我们也需要研究环与环之间的关系，就像群同态一样，可以定义环的同态和域的同态，它们需要保持运算结构和幺元。

定义 3.3 (环同态)**.** 一个环之间的映射 $f : R \to S$ 称为环同态，如果 f 满足

(1) (Abel 群同态) $f(a + b) = f(a) + f(b)$
(2) (保持乘法) $f(ab) = f(a)f(b)$
(3) (保持幺元) $f(1) = 1, f(0) = 0$.

如果 f 还是单射，则称为单同态。如果 f 还是满射，称为满同态。如果 f 有一个同态逆，则称 f 为同构。域同态也按环之间的同态来理解。

例 3.5. 设 K 是一个域，$x_0 \in K$, 可以定义一个多项式赋值同态

$$\begin{aligned} f : K[x] &\to K \\ p(x) &\mapsto p(x_0) \end{aligned}$$

将多项式 $p(x)$ 映射到它在 $x = x_0$ 处的值 $p(x_0)$.

练习 3.6. 验证这是环同态并且还是满同态。

2. 理想

理想这个概念最初是 Kummer 提出的。提出这个概念是为了挽救在许多数论中考虑的环里面，没有像整数一样优美的唯一分解律：任何整数都可以唯一分解为一些素数的乘积。在一般的环中，素分解不一定是唯一的。Kummer 发现，如果引入“理想数”的概念，理想的乘积仍然可能满足唯一分解律。

简单地来说，理想就是倍数集合。比如对于素数 $p \in \mathbb{Z}$ 可以考虑 p 的所有倍数构成的集合 $(p) := \{kp | k \in \mathbb{Z}\}$, 叫做 p 生成的理想。这个倍数集合最本质的特点是具有倍数的“吸收性”，即对任何 $r \in \mathbb{Z}, i \in (p)$ 都有 $ri \in (p)$. 这就引出了如下理想的概念

定义 3.4 (理想)**.** 环 R 的一个 Abel 子群 I 叫做左理想, 如果对任何 $r \in R, i \in I$ 都有 $ri \in I$. 如果条件改成 $ir \in I$，则称为右理想。如果 I 既是左理想又是右理想，则称为双边理想。注意到在交换环中，不需要考虑左右理想的概念，所有理想都是双边的，于是在交换环中左，右理想都简称为理想。R 本身是一个理想，称为平凡理想，不等于 R 的理想则称为真理想。

理想的一个重要用途就是可以用来构作**商环**，就像定义商群一样，给定环 R 和一个双边理想 I 我们可以定义陪集集合

$$R/I = \{r + I | r \in R\}.$$

这首先是一个 Abel 群 R 对于子群 I 的商群，其元素为陪集 $r + I$ 或理解为 R 在 I 所确定的等价关系的一个代表元。其乘法只需要从大环 R 遗传过来就可以了，即规定 R/I 中的乘法为

$$(r + I)(s + I) = rs + I.$$

容易验证由于理想的吸收律，作为 R 中的子集，乘积 $(r + I)(s + I) \subset rs + I$. 故上述乘法是定义良好的 (不依赖于代表元的选取)。

例 3.6. 考虑环 $\mathbb{Z}$ 的理想 $n\mathbb{Z} = \{nk | k \in \mathbb{Z}\}$, 关于这个理想作的商环为所谓模 n 的剩余类环

$$\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} | a \in \mathbb{Z}\} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}.$$

作为加法群，这是一个 n 阶循环群。作为环这是一个有限的环，其中加法幺元素为 $n\mathbb{Z}$, 乘法幺元素为 $1 + n\mathbb{Z}$. 这个环的数论含义是所有整数在模 n 意义下的 n 个剩余类构成的环。值得注意的是，当 n 为素数 p 时，$\mathbb{Z}/p\mathbb{Z}$ 事实上是一个由 p 个元素构成的有限域。

练习 3.7. 对于一列理想 I_λ 我们可以定义它们的和：$\Sigma_\lambda I_\lambda$ 为如下理想

$$\left\{ \text{所有有限和} \sum_\lambda a_\lambda i_\lambda | a_\lambda \in R, i_\lambda \in I_\lambda \right\}.$$

证明这是一个理想。对于有限个理想 $I_1, \ldots, I_n$ 我们可以定义它们的积 $J = I_1 \ldots I_n$ 为

$$J = \{i_1 \ldots i_n | i_k \in I_k\}.$$

证明这也是一个理想。

练习 3.8. 按如下步骤，证明数论中的费马小定理

(1) 设 $0 \neq a \in \mathbb{Z}/p\mathbb{Z}$. 证明对任意 k, $a^k \neq 0$.
(2) 由此得出 a 有乘法逆，即 $\mathbb{Z}/p\mathbb{Z}$ 是域，有时记为 $\mathbb{F}_p$, 称作 p 元有限域。
(3) 证明 $\mathbb{F}_p^\times := \mathbb{Z}/p\mathbb{Z} - \{0\}$ 是一个乘法群，从而对任意 $a \in \mathbb{F}_p^\times$, $a^{p-1} = 1$.

2.1. 素理想. 理想这个概念是从数论里面得到的，那么自然的，它就会和许多算术概念产生联系。在数论中，用来证明自然数分解成素因子的乘积的唯一分解律的最重要的一步是证明素数具有如下称为欧几里得引理的性质：设 p 是一个素数，如果 $p|ab$, 那么 $p|a$ 和 $p|b$ 至少有一个成立。从理想的角度讲，$(p) = p\mathbb{Z} \subset \mathbb{Z}$ 是 p 的倍数集合，它是 $\mathbb{Z}$ 的一个理想。这时有

$$ab \in (p) \Rightarrow a \in (p)\text{或者}b \in (p).$$

我们可以把这个概念推广到任何一个环，如果环 R 的一个**真理想**$I \in R$ 满足上面的性质，就把 I 称为**素理想**。即，如果

$$ab \in I \Rightarrow a \in I\text{或者}b \in I$$

那么 I 就叫素理想。对于一个交换环 R, 它的所有素理想构成的集合一般记为 $\mathrm{Spec}(R)$. 注意平凡理想不是素理想，这一点属于约定，原因和约定 1 不是素数类似，1 这种可逆元应该叫做单位，而不适合叫做素数。

练习 3.9 (★). 我们称环 R 是整环，如果在 R 内 $ab = 0$ 能推出 $a = 0$ 或 $b = 0$. 证明：设 I 是 R 的一个双边理想，证明 R/I 是整环当且仅当 I 是素理想。

练习 3.10. 设有环同态 $f : R \to S$, 证明，素理想的原象一定是素理想。即若 $P \subset S$ 是 S 的一个素理想，那么 $f^{-1}(S)$ 是 R 的素理想。

另一个有用的概念是**极大理想**，环 R 的一个真理想 I 是极大理想 (左, 右, 双边) 是指，环 R 中没有包含 I 的更大的真理想 (左, 右, 双边). 我们说明几个极大理想的简单性质

命题 3.1 (极大理想必为素理想)**.** 设 I 是 R 的一个极大理想 *(双边)*，则 I 也是 R 的一个素理想 *(双边)*。

Proof. 否则，可设 $ab \in I$ 但 $a, b \notin I$. 考虑

$$((a) + I)((b) + I) = (ab) + I \subset I$$

由于 $(a) + I, (b) + I$ 严格大于 I，根据假定它们只能等于平凡理想 R。于是得到

$$R = R \cdot R \subset I$$

这与 I 是极大理想 (根据定义一定是真理想) 矛盾。 □

命题 3.2. 任意非单位元 $a \in R$ 必然被包含在某个极大理想中。

Proof. 考虑由 a 生成的 (左) 理想 Ra, 由 a 非单位，我们知道 $Ra \neq R$. 于是 Ra 是真理想，对包含它的所有理想的集合用 Zorn 引理[1]那么可得它被包含在某个极大 (左) 理想之中。 □

练习 3.11 (★). 证明：设 I 是 R 的一个双边理想，证明 R/I 是域当且仅当 I 是极大理想。

练习 3.12 (★). 设 a 被包含在所有极大理想之中，证明 $a + 1$ 是单位。

---

[1]Zorn 引理是指：如果带有偏序的集合 S 上的任意升链都在 S 中有上界，那么 S 存在极大元。该引理是集合论的结果，等价于选择公理。这里包含 I 的任意理想的升链 $I_1 \subset I_2 \subset \dots$ 的上界是理想的并 $\bigcup_{i=1}^{\infty} I_i$, 容易证明它也是一个理想因此属于 S 从而可以用 Zorn 引理。

2.2. 同态的核与像. 就如同群同态的核与像，对于一个环同态 $f : R \to S$, 我们可以定义

$$\ker(f) := \{r \in R | f(r) = 0\}$$

以及

$$\mathrm{Im}(f) := \{f(r) | r \in R\}.$$

练习 3.13. 验证核是 R 中的双边理想，像是 S 中的一个子环。

我们有显然的同构定理

定理 3.1 (第一同构定理)**.** 给定一个环同态 $f : R \to S$，它将诱导一个环的同构

$$\overline{f} : R/\ker(f) \to \mathrm{Im}(f)$$

Proof. 这个同构由

$$r + \ker(f) \mapsto f(r)$$

定义。它显然是良好定义的，因为 $\ker(f)$ 的像是 0. 如果 $f(r) = 0$, 那么 $r \in \ker(f)$, 故它是单射。满射也是显然的。 □

定理 3.2 (对应定理)**.** 设 I 是一个双边理想，$p : R \to R/I$ 是自然的投射，那么 R/I 的所有理想与 R 中包含 I 的理想一一对应。

练习 3.14. 证明，域的理想只有平凡理想和零理想 $(0) := \{0\}$. 说明从域到任意环的同态只能是单同态或者零同态。

3. Noether 性质

如果环 R 中所有理想都是有限生成的，即任何理想 $I \subset R$ 都可以表示为

$$I = Ra_1 + Ra_2 + \cdots + Ra_n$$

的形式 (右理想则换成 $a_1R + \cdots + a_nR$)，这里 $a_i \in R$, 则我们说 R 是一个 Noether 环 (左, 右, 双边)，这是环论中一个重要而基本的性质，我们研究的大部分环都是 Noether 的。关于 Noether 性质，有如下经典的等价表述

定理 3.3 (Noether 性质)**.** 以下三条等价 *(关于左, 右, 双边各有一个本定理，不再赘述)*

(1) R 是 *Noether* 环
(2) R 的任何理想的上升链

$$I_1 \subset I_2 \subset \ldots$$

必然停止，即存在 n 使得 $I_n = I_{n+1} = I_{n+2} = \ldots$.
(3) R 的任意由理想组成的非空集合 S 必有极大元，即存在 $I \in S$ 使得 $I \subset J \in S \Rightarrow I = J$

Proof. (1) ⇒ (2) :
设 $I = \bigcup_{i=1}^{\infty} I_i$, 容易证明这是一个理想。于是 I 是有限生成的，设它由 $a_1, \ldots, a_m$ 生成，由定义，可设 $a_i \in I_{n_i}$, 那么当 $n \geq \max(n_1, \ldots, n_m)$ 时，$I_n = I$, 故升链在此停止。

(2) ⇒ (3) :
否则，存在一个严格递增的无穷长升链，与 (2) 矛盾。

(3) ⇒ (1) :
令 I 是任意理想，设 S 是所有有限生成的被包含在 I 内的理想组成的集合，那么可以取出极大元 $J \in S$. 如果 $J \neq I$, 存在 $a \notin J$ 但是 $a \in I$, 考虑 $J + Ra$ 是一个有限生成的理想，它严格比 J 大，这与 J 的定义矛盾。因此 $J = I$. □

练习 3.15. 证明，一个有限环必然是 *Noether* 的。

练习 3.16. 证明，如果 R 是 *Noether* 的，那么 R/I 也是，这里 I 是一个双边理想。从而得出 R 的任何同态像也是 *Noether* 的。

下面的一个基本定理说明了很多环都是 Noether 的。

定理 3.4 (Hilbert 基定理)**.** 如果 R 是 *Noether* 的，那么 $R[x]$ 也是。

Proof. 设 I 是 $R[x]$ 中一个 (不妨设为左理想) 理想，那么记

$$J_m = \{r \in R | r\text{出现在某个 } m \text{ 次多项式 } f(x) \in I \text{ 的首系数中}\} \cup \{0\}.$$

显然有一个理想的上升链

$$J_0 \subset J_1 \subset J_2 \dots$$

根据 R 的 Noether 性，J_i 全都是有限生成的，并且这个升链必然停止。设 $J_n = J_{n+1} = \dots$ 那么取出 $J_0, \dots, J_n$ 的生成元对应的多项式 $f_{i,j}(x) \in R[x]$, $\deg(f_{i,j}) = i \le n$ 我们证明 $\forall g_0 \in I$ 都能由 $\{f_{i,j}\}$ 生成。设它的头系数出现在 f_{n_1,j_1} 中，$n_1 \le \deg(g_0)$, 有

$$g_1 = g - f_{n_1,j_1} x^{\deg(g)-n_1}$$

次数严格小于 $\deg(g_0)$. 如果它不为 0, 可继续取出某个 f_{n_2,j_2}, $n_2 \le \deg(g_1)$，使得

$$g_2 = g_1 - f_{n_2,j_2} x^{\deg(g_1)-n_2}$$

次数严格小于 $\deg(g_1)$. 如果它不为 0, 这个过程还可以继续。但由于次数是一个非负整数，这个过程必然停止，最终可以得到

$$g_0 = \sum_k f_{n_k,j_k} x^{\deg(g_{k-1}-n_k)}$$

这便证明了命题。 □

4. 主理想整环中的算术

这一节我们假定所有的环都是交换环。此时不需要再区分左右理想和双边理想，统称为理想。设 $a_1, \dots, a_n \in R$, 我们定义理想记号

$$(a_1, \dots, a_n) := Ra_1 + Ra_2 + \dots + Ra_n$$

表示由 $a_1, \dots, a_n$ 生成的理想。如果一个理想 I 可以由一个元 $a \in R$ 生成，即 $I = (a)$，那么我们称它为**主理想** (principal ideal)。如果有一个整环 R 的所有理想都是主理想，那么我们称它为主理想整环 (principal ideal domain)，简称为 PID.

定理 3.5 (最大公因数理论)**.** $\mathbb{Z}$ 是 *PID*。

Proof. 设 I 是 $\mathbb{Z}$ 的一个非零理想，并设 $0 < a \in I$, 如果 $I = (a)$, 证明完成。否则设 $0 < b \in I$ 使得 a 不整除 b, 那么考虑带余数的除法

$$b = aq + r, \quad 0 < r < a$$

由此得到 $r = b - aq \in I$. 如果 I 内元素全部能被 r 整除，那么 $I = (r)$ 我们完成证明，否则可以继续取出一个不被 r 整除的元素并重复这一过程，得到一个比 r 更小的正整数属于 I. 但 r 是正整数，这个过程无法无限进行下去，一定会有一步的 r 使得 $r \in I$ 且所有 I 中的元素都能被 r 整除。由此得到 I 是主理想。 □

推论 3.1. 设 d 是 $a_1, \dots, a_n \in \mathbb{Z}$ 的最大公因数，那么存在整数 $x_1, \dots, x_n \in \mathbb{Z}$ 使得

$$d = a_1 x_1 + \dots + a_n x_n.$$

PROOF. 根据定理，$I = (a_1, \dots, a_n) = (r)$ 是主理想。显然 $d|r = r_1a_1 + \cdots + r_na_n$。但是由 $a_i \in (r)$ 同样有 $r|a_i$, 于是 r 整除 a_i 的最大公因数 $r|d$. 这表明 $r = \pm d$ 故 $d \in (d) = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_n$, 存在 $x_i \in \mathbb{Z}$ 使得

$$d = a_1x_1 + \cdots + a_nx_n.$$

□

设 R 是一个一般的整环，就像我们定义素数一样，我们称一个非单位元 $a \in R$ 是**不可约元**，如果 $a = bc$ 只能推出 b, c 至少有一个是单位。而我们称 $p \in R$ 是**素元**，如果 (p) 是素理想，即 $p|ab \Rightarrow p|a$ 或 $p|b$. 我们知道，在整数环 $\mathbb{Z}$ 的情形，不可约元和素元是等价的，但在一般的整环中这是未必等价的。有趣的是，在 PID 中这是成立的。

练习 3.17 (★)**.** 证明，在 *PID* 中不可约元和素元等价。

我们来说明主理想整环在算术上具有非常良好的性质：

定理 3.6 (PID⇒UFD)**.** 我们称一个整环 R 是唯一分解整环 *(Unique Factorization Domain),* 简称 *UFD,* 如果其中每一个非零元素都可以以唯一的方式写成**不可约元**的乘积 *(*在不记顺序，单位的前提下*).* 我们有：R 是 *PID*⇒ R 是 *UFD.* 作为一个推论，*UFD* 中不可约元和素元也等价。

我们先证明一个引理，它等价于分解的存在性

引理 3.1. *Noether* 环中，对任意非零理想 I，存在有限个非零素理想 P_i 使得 $I \supset P_1 \dots P_n$.

PROOF. 令 S 是使命题不成立的理想的集合，则取出极大元 $J \in S$, 那么 J 不是素理想，否则 $J \supset J$ 是一个命题所需的分解。故存在 $xy \in J$ 使得 $x, y \notin J$, 有

$$((x) + J)((y) + J) = (xy) + J \subset J$$

注意到 $(x) + J, (y) + J$ 严格大于 J, 根据 J 的定义，它们存在分解，于是它们的乘积也存在分解，由此得出 J 也存在分解，这与 J 的定义矛盾。故 S 为空集。 □

现在我们来证明唯一分解定理

PROOF. 由引理我们知道，设 $a \in R$, 那么

$$(a) \supset (p_1) \dots (p_n)$$

这里 (p_i) 是一些非零素理想。由于 $p_1 \dots p_n \in (p_1) \dots (p_n) \in (a)$, 这表明存在 b 使得

$$ab = p_1 \dots p_n.$$

对于每一个 p_i, 由于 $(p_i) \supset (p_1 \dots p_n) = (ab) \ni ab$, 得到 $(p_i) \ni a$ 或者 $(p_i) \ni b$. 我们将所有满足 $(p_i) \ni b$ 的 p_i 逐个约去，直到所有的 $(p_i) \not\ni b$, 重新编号，可以写

$$ab' = p_1 \dots p_m$$

如果 b' 不是单位，那么它被一个极大理想 (是素理想) 包含 $(p) \ni b' \Rightarrow (p) \ni ab' = p_1 \dots p_m$ 推出 (p) 要包含 p_i 中的某一个，即 $(p) \supset (p_i)$ 但是由于 (p_i) 是素理想，p_i 必然是不可约元，因此 p 与 p_i 相差一个单位，$(p) = (p_i) \ni b'$, 这与 b' 的定义相矛盾。故 b' 不被任何极大理想包含，它只能是单位。这就证明了分解的存在性。

至于唯一性，我们可以假定有两种分解

$$a = up_1 \dots p_m = vq_1 \dots q_n$$

这里 u, v 是单位，$(p_i), (q_j)$ 是素理想。我们可以从 $(p_i) \ni vq_1 \dots q_n$ 得出 $(p_i) \ni q_j \Rightarrow (p_i) = (q_j)$ 那么它们相差一个单位从而将其从两边约去。重复此过程直到某

一边变成一个单位，另一边自然也不可能还留有素元。这证明了 $m = n$ 并且分解中出现的素因子在相差排序和单位的意义下完全相同。 □

推论 3.2. $\mathbb{Z}$ 是 *UFD.*

练习 3.18 (★)**.** 试说明 *PID* 中，非零素理想都是极大的。

注意，虽然唯一分解性质看起来像是显然的，你可能会以为它在所有环中成立，但这是不对的。例如在 $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$ 中，有

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

这是 6 的两种本质不同的分解。有趣的地方是，它们的分解中出现的因子是不可约元但不是素元。

练习 3.19 (★★)**.** 证明，$2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ 是 $\mathbb{Z}[\sqrt{-5}]$ 中的不可约元，但不是素元。从而唯一分解定理在 $\mathbb{Z}[\sqrt{-5}]$ 中不成立。

4.1. 有趣案例：高斯整环. 所谓高斯整环是指 $R = \mathbb{Z}[i] = \{a + bi | a, b \in\}$. 我们将用类似于 $\mathbb{Z}$ 的方法证明 $\mathbb{Z}[i]$ 是一个 PID 从而是一个 UFD. 我们定义环 $\mathbb{Z}[i]$ 中的范数:

$$N(a + bi) := a^2 + b^2$$

它描述了环中元素的' 大小'。容易看出这个范数具有乘性，即 $N(\alpha\beta) = N(\alpha)N(\beta)$. 而这在算术上也有所含义

练习 3.20. 证明，如果 n, m 都能写成两个整数的平方之和，那么 nm 也能。

练习 3.21. 证明，在 $\mathbb{Z}[i]$ 中，$N(\alpha) = 1$ 当且仅当 α 是单位。

引理 3.2 (高斯整环中的欧几里得除法)**.** 设 $\alpha, \beta \in \mathbb{Z}[i]$, 那么存在 $\gamma, \delta \in \mathbb{Z}[i]$ 使得

$$\alpha = \beta\gamma + \delta$$

并且 $0 \leq N(\delta) < N(\beta)$.

Proof. 考虑复数的商 $\frac{\alpha}{\beta} = x + iy$, 分别取 a, b 为最接近 x, y 的两个整数。于是

$$\alpha = \beta(x + iy) = \beta(a + bi + E) = \beta(a + bi) + \delta$$

其中 $\delta = \alpha - \beta(a + bi) \in \mathbb{Z}[i]$, 并且

$$N(E) = |E|^2 \leq \frac{1}{4} + \frac{1}{4} < 1$$

故

$$N(\delta) = N(\beta)|E|^2 < N(\beta).$$

□

推论 3.3. $\mathbb{Z}[i]$ 是 *PID,* 从而也是 *UFD.*

Proof. 仿照 $\mathbb{Z}$ 是 PID 的证明，任取非零非单位元 $a \in I$, 如果 $(a) \neq I$, 可以取出 $b \in I - (a)$ 并不断使用欧几里得除法使得余数 $r = a - bq$ 的范数越来小，而这是一个正整数，这个过程必然停止，最终可以得到 $r \in I$ 且 I 中所有元素被 r 整除。 □

我们来看 $\mathbb{Z}[i]$ 是 UFD 这个事实的强大应用

命题 3.3. 我们证明，方程

$$y^2+1=x^3$$

只有 $(x,y)=(1,0)$ 这唯一一组整数解。

PROOF. 在 $\mathbb{Z}[i]$ 中考虑该方程，分解为

$$(y+i)(y-i)=x^3$$

设 $(d)=(y+i,y-i)$ 是它们在 $\mathbb{Z}[i]$ 中的最大公因数，有 $d|y+i,d|y-i\Rightarrow d|y+i-(y-i)=2i$. 容易将 $2i$ 分解为 $2i=(1+i)(1-i)i$ 这里 i 是单位而 $(1+i),(1-i)$ 是不可约元从而是素元。如果 d 包含 $(1+i)$ 或者 $(1-i)$ 作为素因子，那么 $(y-i)(y+i)$ 就会是一个偶数，从而 x^3 被 8 整除，得到 y^2 是一个 $8k+7$ 形状的数字，这是不可能的，因为任何整数的平方除以 8 的余数只可能是 $0,1,4$. 因此 d 是单位，即 $y+i$ 与 $y-i$ 互素。在 UFD 中，两个互素的数的乘积等于一个立方可以推出这两个数在相差单位的意义下都是立方，即可设

$$y+i=u(a+bi)^3$$

$$y-i=\overline{u}(a-bi)^3$$

这里 $u\in\mathbb{Z}[i]^\times$ 是单位。由于 $\mathbb{Z}[i]$ 中的单位只有 $\pm1,\pm i$, 而 $\pm1=(\pm1)^3$, $\pm i=(\mp i)^3$, 我们可以将 u 乘进立方的括号里面，故可以假定 $u=1$. 此时

$$y+i=a^3-3b^2a+(-b^3+3a^2b)i$$

因此必有 $-b^3+3a^2b=b(-b^2+3a^2)=1$ 这表明 $b=\pm1$, 故 $-b^2+3a^2=3a^2-1|1$, 只能是 $a=0,b=-1$. 故 $y=0,x=1$ 是方程唯一的整数解。 □

练习 3.22 (★★). 证明 $\mathbb{Z}[\sqrt{-2}]$ 是 *PID.*

练习 3.23 (★★★★). 找出

$$y^2+2=x^3$$

的所有整数解。

练习 3.24 (★★★). 证明 $\mathbb{Z}[\sqrt{-3}]$ 不是 *UFD,* 但是比它大一点的环 $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ 却是 *PID.*

4.2. 域上的多项式环是 PID. 这个结论非常经典而重要，我们在这里还是给出它的证明。事实上这个证明仍然是类似的，由欧几里得除法给出

定理 3.7. 设 $a,b\in K[x]$ 是两个多项式，其中 b 的次数 $\deg(b)>0$, 那么存在多项式 $q,r\in K[x]$ 使得

$$a=bq+r$$

这里 $\deg(r)<\deg(b)$.

PROOF. 设 $a(x)=a_0x^n+a_1x^{n-1}+\ldots$, $b(x)=b_0x^m+b_1x^{m-1}+\ldots$. 那么取

$$q_0(x)=\frac{a_0}{b_0}x^{n-m}$$

我们有

$$a-bq_0=0x^n+\ldots$$

它的 n 次项被抵消了。如果它的次数不低于 b 的次数，设 $a_0'x^{n_1}$ 是它的下一个最高次非零项，可以取

$$q_1=q_0+\frac{a_0'}{b_0}x^{n_1-m}$$

我们有

$$a - bq_1 = 0x^n + 0x^{n_1} + \dots$$

如果它的次数不低于 b 的次数，我们可以继续取下去，直到它的次数低于 b 的次数为止，此时的 $a - bq$ 记为 r. □

推论 3.4. *$K[x]$ 是 PID.*

练习 3.25 (★). 由 x, y 两个变量生成的多项式环 $K[x, y]$ 还是 *PID* 吗？为什么？

5. 环的分式化和分式域

本节讨论的都是交换环。对于一个整环 R, 我们可以取一个乘性子集 $S \subset R$, 即一个子集满足 $a \in S, b \in S \Rightarrow ab \in S$. 不失一般性可假设 $1 \in S$, 定义环 R 对于 S 的分式化为

$$S^{-1}R := \left\{ \frac{r}{s} | r \in R, s \in S \right\}$$

这个集合可以自然的赋予加法和乘法结构

$$\frac{r}{s} + \frac{r'}{s'} := \frac{rs' + sr'}{ss'} \in S^{-1}R$$

$$\frac{r}{s} \cdot \frac{r'}{s'} := \frac{rr'}{ss'} \in S^{-1}R.$$

两个分式 $r/s, r'/s'$ 视作等同当且仅当 $rs' - r's = 0$. 容易验证它构成了一个环。如果取 $S = R\backslash\{0\}$, 则把得到的分式化记作 $\mathrm{Frac}(R)$, 称作 R 的分式域。

定义 3.5 (整闭)**.** 设有整环 R, 记 $K = \mathrm{Frac}(R)$, 如果存在 K 中的元素 $x \in K$ 满足一个首系数为 1 的 R 中的多项式方程

$$x^n + r_1 x^{n-1} + \cdots + r_{n-1}x + r_n = 0$$

则称 x 在 R 上整。所有 K 中在 R 上整的元素叫做 R 在 K 中的整闭包，简称 R 的整闭包，记作 $\overline{R}$. 如果环 R 在 K 中的整闭包就是 R, 称 R 为整闭 (integrally closed) 的，也叫正规 (normal) 的。

例 3.7. $\mathbb{Z}$ 在 $\mathbb{Q}$ 中的整闭包就是 $\mathbb{Z}$, 这是因为，如果 $\frac{x}{y}$ 是一个既约分数满足一个首一 $\mathbb{Z}$ 系数方程，可以乘掉分母得到

$$x^n + r_1 y x^{n-1} + \cdots + r_n y^n = 0$$

可得 y 的每一个素因子 p 都整除 x. 由既约的假定，y 只能没有素因子，即 y 是单位，$\frac{x}{y}$ 是整数。故 $\mathbb{Z}$ 是整闭的。

例 3.8. 设 d 是一个无平方因子数，则

$$\mathrm{Frac}(\mathbb{Z}[\sqrt{d}]) = \mathbb{Q}(\sqrt{d}) := \{x + y\sqrt{d} | x, y \in \mathbb{Q}\}.$$

这是因为，

$$\frac{r + s\sqrt{d}}{a + b\sqrt{d}} = \frac{(r + s\sqrt{d})(a - b\sqrt{d})}{(a + b\sqrt{d})(a - b\sqrt{d})} = \frac{ra - sbd}{a^2 - b^2 d} - \frac{rb + sa}{a^2 - b^2 d}\sqrt{d}$$

其分母 $a^2 - b^2 d$ 不为 0, 因为 d 是无平方因子的。

练习 3.26. 证明 *UFD* 都是整闭的。

练习 3.27. 验证 $\frac{1+\sqrt{-7}}{2}$ 在 $\mathbb{Z}$ 上整，从而证明 $\mathbb{Z}[\sqrt{-7}]$ 不是 *UFD.*

练习 3.28 (★★). 找出 $\mathbb{Z}[\sqrt{5}]$ 的整闭包。

练习 3.29 (★★). 我们来考察一个分式化对素理想影响的例子。

(1) 对于环 $\mathbb{Z}$, 列出它的所有素理想。
(2) 取 $S = \{1, 2, 4, 8, 16, \dots\}$, 考虑环的分式化 $S^{-1}\mathbb{Z}$, 列出它的所有素理想。
(3) 取素理想 $(2) \subset \mathbb{Z}$, 设 $S = \mathbb{Z}\backslash(2)$, 证明这是一个乘性子集，并列出 $S^{-1}\mathbb{Z}$ 中的所有素理想。

练习 3.30 (★★★). 可按如下提示，证明 $K[x, y]$ 是 *UFD*. 从而得出 *UFD* 不一定是 *PID*.

(1) 设 $K(x)$ 是 $K[x]$ 的分式域，那么 $K(x)[y]$ 是域 $K(x)$ 上的多项式环，从而是 *PID*
(2) 将任意多项式 $f(x, y) \in K[x, y]$ 放入 $K(x)[y]$ 中得到一个因子分解
(3) 在某些 $(K[x]/(p(x)))[y]$ 中考察该分解，这里 $p(x) \in K[x]$ 是某些不可约多项式，注意到 $K[x]/(p(x))$ 是域，$(K[x]/(p(x)))[y]$ 也是一个 PID.
(4) 证明 $K[x, y]$ 是 *UFD*.

6. 初等数论在密码学中的应用

$\mathbb{Z}/n = \mathbb{Z}_n$ 是一个阿贝尔群，它代表了模 n 的 n 个剩余类，并且在加法下构成一个群。如果我们考虑 $\mathbb{Z}_n^\times = (\mathbb{Z}/n)^\times$，即所有与 n 互素的剩余类构成的集合，这个集合在乘法下构成一个群，并且其阶数为 $\varphi(n)$. 根据拉格朗日定理，对任意 $a \in \mathbb{Z}_n^\times$ 都有 $a^{\varphi(n)} = 1$, 即对任意与 n 互素的整数 a 都有

$$a^{\varphi(n)} \equiv 1 \mod n.$$

这便是初等数论中的 Euler-Fermat 定理。这一定理在现代密码学中有着有趣的应用.

在公钥密码学中，人们希望实现如下目标:

- 我们需要在一个通信质量可靠，但信息安全不可靠的信道中通信。
- 我们希望只有发件人和收件人能解读信息的内容，任何在信道中窃听的第三方只能获得密文，而无法获得明文。
- 我们还希望这套加密通信体系不需要事先进行密钥分发。

以往古典密码学的最安全的加密方法是一次性密钥密码，即通信的双方事先准备好一串只有双方知道的超长的随机字符串 $k \in \mathbb{Z}_n^m$ 作为一次性密钥，在通信前将密钥 k 加到明文 x 上去得到密文 $x + k$. 由于 k 是完全随机的并且与 x 独立，$x + k$ 的分布也是完全随机的，即其概率分布是平凡的均匀分布。故任何只获得了 $x + k$ 而不知道 k 的人无法了解到关于 x 的任何信息。收件方只需要计算 $(x + k) - k = x$ 即可。但是这个密钥只能使用一次，因为 x 具有非平凡的概率分布，这导致多次使用同一个密钥是不安全的。因此双方事实上需要准备大量的一次性密钥，用完即扔。这样不仅不方便，而且密钥分发也是一个很难的问题：用完了一次性密钥之后你很难确保密钥能安全的 (通过信道或线下分发) 分发到对方手中。

现代密码学的开端，RSA 公钥加密体系通过引入初等数论的方法和非对称加密体系的概念解决了这一问题。考虑一个由两个大质数乘起来的大整数 $n = pq$，那么 $\mathbb{Z}_n^\times$ 是一个阶数为 $\varphi(n) = (p - 1)(q - 1)$ 的群。即对 $a \in \mathbb{Z}^\times$ 都有 $a^{(p-1)(q-1)} = 1$. 事实上，对应的同余式

$$a^{\varphi(pq)} \equiv 1 \mod pq$$

对 $a \in \mathbb{Z} - (pq)\mathbb{Z}$ 都成立。这表明，如果我们取一对指数 (e, d) 使得 $ed \equiv 1 \mod \varphi(pq)$, 就会有

$$(x^e)^d \equiv x^{eq} \equiv x \mod n$$

对所有 x 成立。于是我们可以用 e 来加密信息 $x \in \mathbb{Z}/n$, 得到密文 $x^e \in \mathbb{Z}/n$，然后用 d 来解密，得到 $x^{ed} = x \in \mathbb{Z}/n$. 注意这里加密用的密钥和解密用的密钥是不同

的，并且它们之间的联系需要通过求解 $ed = 1 \in \mathbb{Z}/(p-1)(q-1)$ 来得到。(根据理想理论，只需保证 e 和 $(p-1)(q-1)$ 互素即可存在 $ex + (p-1)(q-1)y = 1$). 如果 p, q 很大，n 将变得难以分解，而不分解 n 就无从知道 $(p-1)(q-1)$ 的取值 (容易证明，在给定 n 的前提下，知道 $(p-1)(q-1)$ 等价于知道 p 和 q)。于是我们可以构造出如下的不需要密钥分发的加密体系：

(1) 首先生成两个随机的，巨大的素数 p, q,
(2) 计算 $n = pq, m = (p-1)(q-1)$,
(3) 随机生成与 m 互素的整数 e，并利用 Euclid 除法计算得到 d 满足 $ed \equiv 1 \mod m$,
(4) 向外公布 (n, e) 作为你的公钥，将 d 保留为私密 (私钥) 信息，p, q, m 等信息保留或丢弃。
(5) 当有人需要向你发送加密信息 $x \in \mathbb{Z}/n$ 时，他可以计算 $x^e \in \mathbb{Z}/n$，并通过信道发送给你。
(6) 获得 x^e 的第三方由于不知道 d，也不能分解 n，无法得知 x。
(7) 你只需要计算 $(x^e)^d = x \in \mathbb{Z}/n$ 就可以解密出原始的信息。

CHAPTER 4

模与线性代数

1. 模的基本知识

模可以说是现代代数学里面最广泛和最重要的一种代数结构了。它可以视为所谓线性代数的自然推广，但所蕴含的现象远远超过了域上的向量空间。就像群可以以群作用一样作用在集合上，我们也可以让环作用在一个集合上。但我们希望环的加法，乘法都能自然地作用在这样的集合上。如果把环里面的乘法看成作用的复合，那我们还不清楚环的加法如何与这个作用配合，因此我们还需要一个加法的结构。于是这引出了模的定义：

定义 4.1 (R 模，多模，双边 R 模)**.** 设 R 是一个环，一个 R-模 M 是指一个阿贝尔群，并且定义了 R 在 M 上的一个 (左) 作用，即对 $r \in R, m \in M$ 可以定义出一个作用后的元素 $rm \in M$. 并且这个作用满足

(1) (幺律) $1m = m$
(2) (结合律) $(r'r)m = r'(rm)$
(3) (R 的分配律) $(r' + r)m = r'm + rm$
(4) (M 的分配律) $r(m + m') = rm + r'm$

我们就说 M 是一个**左 R-模**，也记为 ${}_RM$. 类似的，如果 M 定义了一种右作用 $mr \in M$, 满足类似的性质，注意此时结合律应该换为 $m(r'r) = (mr')r$. 我们就说 M 是一个**右 R-模**，也记为 M_R.

如果一个 Abel 群 M 上定义了多种模结构，对一族环 $\{A_i\}$ 定义了左模的结构，并且对另一族环 $\{B_j\}$ 定义了右模的结构，那么我们称它们的作用可交换，或者说它们的作用是兼容的，是指 $a_j(a_im) = a_i(a_jm)$, 以及 $(a_im)b_j = a_i(mb_j)$ 和 $(mb_i)b_j = (mb_j)b_i$. 如果这些模结构是互相兼容的，那么我们称 M 是一个**多模**，具体的可以记成 $(\{A_i\};\{B_j\})$-模，或者 $(A_i|B_j)$-模，或者写成 ${}_{(A_i)}M_{(B_j)}$, 有时我们也写成 $M_{A_i|B_j}$. 如果 M 是一个 $(R|R)$ 多模，即既是 R 左模又是 R 右模并且两种模结构互相兼容，即 $(rm)r' = r(mr')$, 则称 M 为**双边 R-模**. 在 R 是交换环的情形，左 R-模和右 R-模统称为 R-模。

练习 4.1. 验证，环 R 在自己身上的左乘可以看做一个左 R-模。类似的右乘是一个右 R-模，于是 R 是双边 R 模。

练习 4.2. 设 I 是 R 的一个双边理想，验证，R/I 在自然的左乘右乘作用下是一个双边 R-模。

练习 4.3. 说明每一个 *Abel* 群都是 $\mathbb{Z}$-模，而 $\mathbb{Z}$-模自然也是 *Abel* 群。说明这两个概念的等价性。

练习 4.4. 说明对于交换环 R, 一个左 R 模 M 可以按如下方式定义出右 R 模的结构

$$mr := rm$$

为什么这个定义在 R 不是交换环时不成立？

环可以很复杂，环上的模自然也可以很复杂，但有两类比较经典的模我们重点讨论，域上的模 (向量空间)，以及主理想整环上的 (有限生成) 模。

1.1. 模的同态.

定义 4.2. 设 M, N 是两个 R-模，那么我们说一个 R-模同态 $\varphi : M \to N$ 是指一个 Abel 群同态并且满足 $\varphi(rm) = r\varphi(m)$. 对于右模的同态则修改为 $\varphi(mr) = \varphi(m)r$. R-模同态也叫 R-线性映射。

对于多模同态，则需要 φ 与所有模结构兼容。

单同态，满同态，同构的含义是明显的，不再赘述。如果存在模同构态射 $\varphi : M \to N$，我们称 M, N 同构，记作 $M \cong N$. 由于右模的理论完全是类似的，以下大部分时候我们默认考虑左模。

对于 M 的子集 $N \subset M$, 如果它满足 $RN \subset N$ 我们称 N 是 M 的子模。对于任何子模我们可以构作商模 M/N, 其元素为陪集 $m + N$, 作用定义为

$$r(m + N) := rm + N$$

容易验证该定义不依赖于陪集代表元的选取，并且满足 R-模的定义。

练习 4.5. 设 $\varphi : M \to N$ 是一个 R-模同态，证明 $\ker\varphi := \{m \in M | \varphi(m) = 0\}$ 是一个 M 的子模，$\mathrm{Im}\varphi$ 是 N 的子模。证明第一同构定理

$$\overline{\varphi} : M/\ker\varphi \cong \mathrm{Im}\varphi.$$

练习 4.6. 设 $\{M_i\}_{i\in I}$ 是 M 的一族子模，证明

$$\sum_{i\in I} M_i = \{\text{所有有限和 } m_{i_1} + \cdots + m_{i_n} | m_{i_1} \in M_{i_1}, \ldots, m_{i_n} \in M_{i_n}, \{i_1, \ldots, i_n\} \subset I\}$$

和 $\bigcap_{i\in I} M_i$ 都是 M 的子模。

以下两个定理与群论中的同构定理证明基本相同。

定理 4.1 (第二同构定理)**.** 设 M, N 都是某个 R-模的子模, 则 $M+N$ 和 $M\cap N$ 也是子模并且

$$(M + N)/N \cong M/M \cap N.$$

定理 4.2 (对应定理)**.** 设 $N \subset M$ 是 M 的子模，则 M/N 的子模与介于 $M \supset L \supset N$ 之间的子模 L 一一对应。

1.2. 正合序列. 当我们有一系列模和模的同态时

$$M \xrightarrow{f} N \xrightarrow{g} L$$

如果 $\ker(g) = \mathrm{Im}(f)$, 我们说这个序列在 N 处正合。如果一个模的映射序列在每一处 (除了最左边和最右边的端点) 都正合，我们说它是一个正合序列。

练习 4.7.

$$0 \longrightarrow M \xrightarrow{f} N$$

是正合序列当且仅当 f 是单同态。

练习 4.8.

$$M \xrightarrow{f} N \longrightarrow 0$$

是正合序列当且仅当 f 是满同态。

例 4.1.

$$0 \longrightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

是一个 $\mathbb{Z}$ 模的正合序列，其中 2 是乘以 2 的映射，p 是投射。这里 $\ker(p) = 2\mathbb{Z} = \mathrm{Im}(2)$.

2. 模的基本构造

本节我们来讨论如何从已有的模构造出新的模。我们已知的方法有，商模，模的交，模的和。

2.1. Hom **函子.** 给定两个左 R-模 M, N，我们可以将所有 R-模同态 $M \to N$ 组成的集合记为 $\mathrm{Hom}_R(M,N)$. 对于 $((A_i)|(B_j))$ 多模同态构成的集合则记为 $\mathrm{Hom}_{(A_i)|(B_j)}(M,N)$. 如果我们要区分模同态的方向，有时候我们用这个记号，将左 R 模同态的集合写成 $\mathrm{Hom}_{R|}(M,N)$. 对于两个同态 $f: M \to N$, $g: M \to N$, 容易定义它们的和为

$$(f+g)(m) := f(m) + g(m)$$

这显然也是一个同态，故 $f+g \in \mathrm{Hom}_R(M,N)$, 这说明 $\mathrm{Hom}_R(M,N)$ 是一个 Abel 群。值得注意的是，如果 M, N 都是左 R 模或者都是右 R 模，没有多模的结构，那么它们的 $\mathrm{Hom}_R(M,N)$ 并没有自然的 R 模结构，仅仅是 Abel 群 ($\mathbb{Z}$-模) 而已。但如果 M, N 至少有一个具有多模的结构的话，Hom 函子可以被自然的赋予模结构，我们来说明这一点。

2.1.1. Hom 的模结构. 以下 R, S 是两个环，如果 M 具有左 R 模结构和右 S 模的多模结构，当我们需要明确标明模的结构时我们写为 ${}_RM_S$.

我们来举例说明 $\mathrm{Hom}_R({}_RM_S, {}_RN)$ 具有左 S 模的结构。这是因为我们可以对 $f \in \mathrm{Hom}(M,N)$,$s \in S$ 定义

$$(sf)(m) := f(ms)$$

那么 (sf) 显然是一个左 R 模同态 (这里需要用到多模的定义：多个环的模结构需要互相兼容)。我们需要验证 $\mathrm{Hom}_R(M,N)$ 满足左 S 模的定义，其它性质都是显然的，唯一需要仔细检查的是结合律

$$(s's)f = s'(sf)$$

左边的同态是 $m \mapsto f(ms's)$, 右边的同态是 $s'(m \mapsto f(ms)) = m \mapsto f(ms's)$, 因此这是成立的，即 $\mathrm{Hom}_R(M,N)$ 在这个定义下成为一个左 S-模。

类似的一共有八种情况，我们将所有情况列出如下表格

群	自然的模结构	S 模结构的定义
$\mathrm{Hom}_{R\|}({}_RM, {}_RN)$ $\mathrm{Hom}_{\|R}(M_R, N_R)$	$\mathbb{Z}$ 模	none
$\mathrm{Hom}_{R\|}({}_RM_S, {}_RN)$ $\mathrm{Hom}_{\|R}(M_{S,R}, N_R)$	左 S 模	$(sf)(m) := f(ms)$
$\mathrm{Hom}_{R\|}({}_{S,R}M, {}_RN)$ $\mathrm{Hom}_{\|R}({}_SM_R, N_R)$	右 S 模	$(fs)(m) := f(sm)$
$\mathrm{Hom}_{R\|}({}_RM, {}_RN_S)$ $\mathrm{Hom}_{\|R}(M_R, N_{S,R})$	右 S 模	$(fs)(m) := f(m)s$
$\mathrm{Hom}_{R\|}({}_RM, {}_{R,S}N)$ $\mathrm{Hom}_{\|R}(M_R, {}_SN_R)$	左 S 模	$(sf)(m) := sf(m)$

总结来说，就是 N 有哪个方向的 S 模结构，$\mathrm{Hom}_R(M,N)$ 就会具有哪个方向的 S 模结构。如果双模结构出现在 M 上，作用会被函数从里向外复合反过来乘法的方向，导致模的方向发生改变。

练习 4.9 (★). 确认你弄明白了表格中的所有情况。

2.1.2. 自同态环. 当 $M = N$ 时, $\mathrm{Hom}_R(M, M)$ 记作 $\mathrm{End}_R(M)$, 此时它具有自然的环结构, 乘法是 $M \to M$ 的同态的复合。

练习 4.10 (★). 证明, M 是 R 模, 那么它具有自然的左 $R, \mathrm{End}_R(M)$ 多模结构。

2.1.3. Hom 的函子性. 我们说 Hom 函子是什么意思呢? 所谓**函子**是现代数学范畴论中的一个抽象概念, 它描述不同范畴之间的对象如何对应起来。它需要

(1) 将物件 A 对应于物件 $F(A)$
(2) 将映射 $f : A \to B$ 对应于另一个映射 $F(f) : F(A) \to F(B)$ 或者 $F(f) : F(B) \to F(A)$. 满足前者的称为协变函子, 后者称为反变函子。
(3) 函子必须保持复合, 即 $F(f \circ g) = F(f) \circ F(g)$.
(4) 我们还要求函子将恒等映射对应到恒等映射, 即 $F(1_A) = 1_{F(A)}$.

作为例子, 我们详细来说明 Hom 如何构成函子。

- 对于一个固定的 R 模 N, 我们发现 $M \mapsto \mathrm{Hom}_R(M, N)$ 是一个反变函子, 有时记为 h_N. 这个函子将 R 模 M 对应到 Abel 群 $\mathrm{Hom}_R(M, N)$, 并且将 R 模同态 $f : M' \to M$ 对应到阿贝尔群的同态

  $$\mathrm{Hom}(f, N) := \mathrm{Hom}(M, N) \to \mathrm{Hom}(M', N) : h \mapsto h \circ f.$$

  显然它保持复合和恒等映射。
- 类似的, 对于固定的模 M, 我们发现 $N \mapsto \mathrm{Hom}_R(M, N)$ 是一个协变函子, 它将模同态 $g : N' \to N$ 对应到阿贝尔群同态

  $$\mathrm{Hom}(M, g) := \mathrm{Hom}(M, N') \to \mathrm{Hom}(M, N) : h \mapsto g \circ h.$$

  显然它也保持复合和恒等映射。

2.2. 直和. 给定两个左 R-模 M, N, 定义它们的直和 $M \oplus N$ 是集合 $M \times N = \{(m, n) | m \in M, n \in N\}$ 作为 Abel 群的直和, 加法为分量相加, R 的作用定义为

$$r(m, n) := (rm, rn)$$

容易验证这个定义给出了一个 R-模结构。直和不仅仅限于有限直和, 对任意一族由集合 I 编号的 R 模 $\{M_\lambda\}$ 我们可以定义直和

$$\bigoplus_{\lambda \in I} M_\lambda := \left\{ (m_\lambda) \in \prod_{\lambda \in I} M_\lambda | \text{至多有有限个 } m_\lambda \text{ 不为 } 0 \right\}.$$

如果对一列相同的模 $M_\lambda = M$ 作直和, 这个直和我们记作 $M^{(I)}$.

练习 4.11 (★). 验证, 如果 M, N 是 L 的两个子模, 满足

$$M \cap N = 0$$

那么证明有同构 $M + N \cong M \oplus N$. 此时我们把 $M + N$ 称作 M, N 的内直和。

练习 4.12. 证明我们有如下明显的正合列

(1)
$$0 \to M \to M \oplus N \to N \to 0$$
(2) 这里设 $M' \subset M$ 是子模, 那么
$$0 \to M' \to M \to M/M' \to 0$$
是自然的正合列。

2.3. 直积. 与直和类似，一族模 M_λ 的直积是由集合 $\prod_\lambda M_\lambda$ 赋予自然的模结构得出的。区别在于直积中，我们不要求每一个元素的分量只有有限多个不为 0，任意序列 $(m_\lambda) \in \prod M_\lambda$ 都是允许的元素。类似的，如果对一列相同的模 $M_\lambda = M$ 作直积，这个直积我们记作 M^I.

例 4.2. *考虑 $F = \oplus_{i=0}^{\infty}\mathbb{Z}$, 而 $G = \prod_{i=0}^{\infty}\mathbb{Z}$ 是两个 $\mathbb{Z}$ 模, 那么 $(1,2,3,4,\dots) \in G$ 是 G 中的一个元素，但在 F 中没有这个元素。有自然的包含 $F \subset G$,F 是 G 的一个子模。*

练习 4.13. *模的有限直和与有限直积同构。*

练习 4.14. *证明如下称为直和的 universal property，以及直积的 universal property 的自然同构*

$$\mathrm{Hom}_R\left(\bigoplus_{\lambda\in I} M_\lambda, N\right) = \prod_{\lambda\in I}\mathrm{Hom}_R(M_\lambda, N).$$

$$\mathrm{Hom}_R\left(M, \prod_{\lambda\in I} N_\lambda\right) = \prod_{\lambda\in I}\mathrm{Hom}_R(M, N_\lambda).$$

说明它们与这两句话等价

- *对任意映射 $h_\lambda : M_\lambda \to N$, 存在唯一的映射 $(\oplus h_\lambda) : \bigoplus_\lambda M_\lambda \to N$ 使得 $h_\lambda = (\oplus h_\lambda) \circ \iota_\lambda$. 这里 $\iota_\lambda : M_\lambda \to \oplus M_\lambda$ 是自然的含入映射。*
- *对任意映射 $g_\lambda : P \to N_\lambda$, 存在唯一的映射 $(\prod p_\lambda) : P \to \prod M_\lambda$ 使得 $g_\lambda = \mathrm{pr}_\lambda \circ (\prod p_\lambda)$. 这里 $\mathrm{pr}_\lambda : \prod M_\lambda \to M_\lambda$ 是到分量的投射。*

2.4. 自由模. 由 R 的任意数量个直和 (可能是无限的) 得到的模，或者与之同构的模称为自由 R 模。比如 $R^n = R \oplus R \oplus \cdots \oplus R$($n$ 个 R 的直和). 自由模的重要性在于它有如下好性质，任意从 R^n 出发的模的同态 $f : R^n \to M$ 都可以很容易被确定下来，只需要确定每个 $e_i = (0,\dots,0,1,0,\dots,0) \in R^n$(第 i 位是 1) 被映射到哪里去，整个模的同态就完全确定下来了。因为 R^n 中每一个元素 $(r_1,\dots,r_n)$ 都可以写成

$$(r_1,\dots,r_n) = \sum r_i e_i$$

因此

$$f((r_1,\dots,r_n)) = \sum f(r_i e_i) = \sum r_i f(e_i).$$

值得注意的是，$f(e_i)$ 的值怎么选取没有任何限制。即 f 的确定完全取决于 $f(e_i)$ 这 n 个值的任意选取，或者说，取决于一个任意元素 $(f(e_1), f(e_2),\dots,f(e_n)) \in M^n$. 这给出了如下自然同构

$$\mathrm{Hom}_R(R^n, M) = M^n.$$

练习 4.15. *证明自由模的基本性质*

$$\mathrm{Hom}_R\left(R^{(I)}, M\right) = M^I$$

注意 I 可能是无限的，并且注意直和与直积的区别。

2.5. 生成元与基. 对于一个 (左)R 模 M, 我们选取了一族元素 $(m_i)_{i\in I\in M^I}$ 之后，由 $\mathrm{Hom}_R(R^{(I)},M)=M^I$ 可以定义出一个映射 $\oplus(r\mapsto rm_i):R^{(I)}\to M$, 暂时记为 ρ. 这个映射的像称之为 m_i 的 R-**线性组合**. 我们说 $\{m_i\}_{i\in I}\subset M$ 是 M 的一组**生成元**，是指由 $\rho:R^{(I)}\to M$ 是满射。即，任意 $m\in M$ 都可以写成某个有限的 m_i 的线性组合

$$m=r_1m_{i_1}+\cdots+r_nm_{i_n}.$$

如果存在一族有限的 m_i 是 M 的一组生成元, M 称作**有限生成**的。我们说 $\{m_i\}_{i\in I}$ 是一组 R-**线性无关组**, 简称无关组，是指它对应的映射 $\rho:R^{(I)}\to M$ 是单射。即如果 m_i 之间有任何有限个元素 $m_{i_1},\dots,m_{i_n}$ 有任何 R 线性关系

$$r_1m_{i_1}+\cdots+r_nm_{i_n}=0$$

那么所有系数 $r_1=r_2=\cdots=r_n=0$. 如果一组元素 $\{m_i\}$ 既是 M 的生成元，又是 M 的线性无关组，这组元素就叫 M 的一组**基**.

练习 4.16. 说明，M 有一组基等价于 M 与某个自由模同构。

练习 4.17. 给出一个非自由模的例子，于是它没有任何基，尽管它一定有生成元，但它们一定不是线性无关的。

2.6. 标量限制. 当我们有环同态 $f:A\to B$ 和一个 B 模 M 时，我们可以通过 f 自然的在 M 上获得 A 模的结构，即定义

$$am:=f(a)m.$$

这样的一个模结构叫做通过 f 的标量限制，记作 $f_*(M)$, 或者 $M_{[A]}$, 或者 Res^B_AM. 注意一般获得的 A 模结构与原有的 B 模结构并不一定兼容，因此不能说这是一个左 A,B 多模。但当 $f(A)$ 与 B 交换时，这是对的。

练习 4.18 (★). 设 M 是左 B 模, $f:A\to B$ 是上述同态。证明 $\mathrm{Hom}_B({}_BB_A,M)$ 给出的左 A 模就是 $f_*(M)$.

练习 4.19 (★). 设 $f:A\to B$, M,N 是两个 B 模，证明有一个自然同态

$$\mathrm{Hom}_B(M,N)\to\mathrm{Hom}_A(f_*M,f_*N).$$

3. 向量空间

考虑 $R=k$ 是一个域，由于域 k 是交换环，k 模不分左右，我们把域 k 模统称为k-**向量空间**或者k-**线性空间**。它们之间的 k-模同态称之为k-**线性映射**或者k-**线性变换**。

3.1. 向量空间的基. 线性空间最好的一点是，它一定有一组基，于是所有线性空间都同构于某个自由 k 模。这使得线性空间非常好研究，我们来说明这一点。接下来我们设 V 是一个 k-向量空间。

定理 4.3 (基扩张定理)**.** 设 F 是 V 的一组无关组，G 是 V 的一组生成元，满足 $F\subset G$, 那么存在 V 的一组基 B 使得 $F\subset B\subset G$.

Proof. 如果有一列递增的无关组 B_i 使得 $F\subset B_i\subset G$, 那么显然 $\cup_iB_i$ 也是无关组并且满足 $F\subset\cup_iB_i\subset G$. 于是由 Zorn 引理存在一个极大的无关组 B 满足 $F\subset B\subset G$. 我们来证明 B 能生成 V, 即对应的映射 $\rho_B:k^{(B)}\to V$ 是同构。否则，存在 $v\in V$ 不能表示成 B 内元素的线性组合, 那么由于 G 是生成元组，有一个有限和 $v=\rho_G(a)=\sum_{g\in G'}a_gg$, 这里 G' 是有限集。于是一定有一个 $g\in G'$ 与 B 无关，否则所有 $g\in G'$ 都与 B 线性相关，由于 B 是无关组，可以得到 $g\in G'$ 都能由 B 生成，从而得到 v 也能由 B 生成，这是不可能的。但这样的话 $\{g\}\cup B$ 就是

一个在 $F \subset \{g\} \cup B \subset G$ 里面的更大的无关组，这与 B 的设定矛盾。故 B 是一组基。 □

例 4.3. 考虑 $k = \mathbb{R}$, $M = \mathbb{R}^2 = \{(x, y)\}$ 相当于平面上所有向量的集合，在分量的加法下构成 *Abel* 群。那么 M 在 k 的乘法下自然的构成一个 k 向量空间

$$a(x, y) := (ax, ay) \in M.$$

容易验证这个 M 在该作用下满足 k 向量空间 *(k* 模*)* 的四条定义。$\{(0, 1), (1, 0)\}$ 是它的一组基.

练习 4.20 (★). 证明，对向量空间来说，以下说法等价

(1) B 是 V 的一组基.
(2) B 是 V 的一个极大无关组.
(3) B 是 V 的一个极小生成元组.

练习 4.21. 设 $k = \mathbb{Q}$, 找出下面哪些是 k^2 的基，哪些不是？

(1) $(1, 2), (3, 4)$
(2) $(-1, 1), (1, -1)$
(3) $(1, 1), (1, 2), (1, 0)$

3.2. 维数理论. 如果 V 有两组不同的基 B_1, B_2, 我们希望证明 B_1 和 B_2 是等势的，即它们之间存在双射。

3.2.1. 有限的情形. 如果 B_1, B_2 都是有限的，设 $m = |B_1|$ 拥有较少的元素。我们对 m 使用归纳法，证明 $|B_2| \leq m$。如果 $m = 1$,$B_1 = \{b\}$, 那么 B_2 中任意元素都可以写为 b 的某个非零 k-系数倍, 它们无法是线性无关的，除非 $|B_2| = 1$.

现在假定命题对于 $|B_1| \leq m$ 都是成立的，我们来考虑 $|B_1| = m + 1$ 的情形。设 $a \in B_2$, 由基扩张定理，存在一组基 $B = \{a\} \cup B'$ 满足 $\{a\} \subset B \subset \{a\} \cup B_1$, 于是 $V \simeq ka \oplus \left(\bigoplus_{b' \in B'} kb'\right)$, 从而 $V' = V/ka$ 以 B'(的投射像) 为一组基, 其元素个数为 m. 同理 V' 也以 $B_2 - \{a\}$ 的投射像作为一组基，于是 $|B_2| - 1 \leq m$.

3.2.2. 无限的情形. 现在假定 V 具有一组无限基 B 从而 $V \cong k^{(B)}$, 如果 C 是另一组基，对于每一个 $c \in C$, 都有某个有限的表达式 $c = \sum_{b \in B} c_b b$ 这里至多有限个 c_b 不为零。那么对任意 $c \in C$, 考虑有限集 $B_c := \{b \in B | c_b \neq 0\}$, 由于 C 能生成整个空间，对每个 b 必有 c 中向量在 b 的系数上不为 0, 我们有

$$\bigcup_{c \in C} B_c = B$$

由于 B 是无限集，这就表明 $|C| \geq |B|$, 于是由 B 是无限的，我们推出两者都是无限的. 于是对 C 用同样的推理可知 $|B| \geq |C|$.

定义 4.3. 我们定义 V 的**维数**$\dim_k V$ 是它的任意一组基 B 的基数 $|B|$.

练习 4.22 (★). 设有一族 k 向量空间的正合列

$$0 \to E \to F \to G \to 0$$

利用基扩张定理，证明

$$\dim E + \dim G = \dim F.$$

由此推出以下维数公式

(1) 设 $f : V \to W$, 则

$$\dim V = \dim \ker f + \dim \mathrm{Im} f.$$

(2) 设 $F \subset E$ 是子向量空间，那么

$$\dim E = \dim(E/F) + \dim F.$$

(3) $\dim(M \oplus N) = \dim M + \dim N$.
(4) 设 $M, N \subset V$ 是两个子空间，那么

$$\dim M + \dim N = \dim(M \oplus N) = \dim(M + N) + \dim M \cap N.$$

4. 交换环上的矩阵

4.1. 有限生成自由模. 我们本节需要假定 R 都是交换环。值得注意的是，自由模 R^m 中，有一组标准基，即每个元素都可以以唯一的方式写为 $a_1e_1 + a_2e_2 + \cdots + a_me_m$ 的形式。

如果一个 R 模 M 同构于 R^n, 我们就说 M 具有秩 n. 但是我们还没有证明秩的唯一性，即需要证明 $R^m \cong R^n \Rightarrow m = n$. 遗憾的是在一般的环中，这不一定是对的。但至少在 PID 上的情形，这是对的。为了证明这一点，我们需要发展一些环上的线性代数的知识。

4.2. 环上的矩阵. 我们考虑自由模 $R^n \to R^m$ 的模同态，由于

$$\mathrm{Hom}_R(R^n, R^m) = (\mathrm{Hom}_R(R, R^m))^n = (R^m)^n = R^{mn}$$

我们知道，确定一个同态 $\varphi : R^n \to R^m$，本质上只需要知道每个 $e_j \in R^n$ 被映到 R^m 中的哪里。我们用 $e'_i \in R^m$ 表示 R^m 中的标准基。如果我们记 e_j 的像在第 i 个位置的分量为 a_{ij}, 那么可以写

$$\varphi(e_j) = \sum_i a_{ij}e'_i$$

这里 $a_{ij} \in R$ 是我们要的 mn 个 R 中的元素。我们可以把这些元素用排成一个矩阵

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix}$$

矩阵一般用大写字母 $A, B, \dots$ 等等来表示。这里我们的矩阵是 φ 的矩阵，我们也记为 A_φ. 当我们需要强调矩阵元素是 a_{ij} 时，我们写 $A = (a_{ij})_{1 \le i \le m, 1 \le j \le n}$. 这个矩阵具有 m 行 n 列，我们说它是一个 R 上的 $m \times n$ 的矩阵，记作 $A \in M_{m \times n}(R)$. 当 $m = n$ 时这个记号简单写为 $M_n(R)$.

练习 4.23. 确认自己理解：给出一个 $m \times n$ 矩阵与给出一个同态 $R^n \to R^m$ 等价。即给出任意一个由 R 中元素构成的矩阵，它都代表了某个同态。于是任意矩阵 A 都能 (唯一的) 写为 A_f 的形式，f 是某个同态。

4.2.1. 映射的复合与矩阵的乘法. 对于 $f, g \in \mathrm{Hom}_R(R^n, R^m)$, 以及 $r \in R$ 我们可以给出同态 rf 和 $f + g$ 的定义。那么类似的定义矩阵的数乘和加法，即定义 r 乘以 A_f 是指映射 rf 所对应的矩阵 B_{rf}

$$rA_f := B_{rf}$$

记 f, g 两个同态对应的矩阵分别为 A_f, B_g, 那么定义 $A + B$ 是映射 $f + g$ 对应的矩阵 C_{f+g}

$$A_f + B_g := C_{f+g}.$$

练习 4.24. 证明 rA 的元素就是 (ra_{ij}), 而 $A + B$ 的元素就是 $(a_{ij} + b_{ij})$. 从而证明 $M_{m \times n}(R)$ 构成一个 R 模。

当我们有同态的复合

$$R^l \xrightarrow{f} R^m \xrightarrow{g} R^n$$

时，可以通过 A_f, B_g 算出 C_{gf}, 我们把这个过程叫做矩阵的乘法，记作

$$B_g \cdot A_f = C_{gf}.$$

具体是怎么操作的呢？我们可以由矩阵 $A_f = (a_{ij}), B_g = (b_{ij})$ 写出

$$f(e_j) = \sum_i a_{ij} e'_i$$

$$g(e'_i) = \sum_k b_{ki} e''_k$$

因此

$$(g \circ f)(e_j) = g(f(e_j)) = g\left(\sum_i a_{ij} e'_i\right) = \sum_k \left(\sum_i b_{ki} a_{ij}\right) e''_k.$$

这表明 $C_{gf} = (c_{ij}) = B \cdot A$ 的系数应该为

$$c_{ij} = \sum_k b_{ik} a_{kj}.$$

这便是矩阵的乘法公式。注意 B 是 $n \times m$ 的，A 是 $m \times l$ 的，而 BA 是 $n \times l$ 的，这表明矩阵乘法给出了一个映射

$$M_{n\times m}(R) \times M_{m\times l}(R) \to M_{n\times l}(R).$$

当 $m = n = l$ 时，这个乘法运算给出了 $M_n(R)$ 上的乘法，从而 $M_n(R)$ 成为一个 (通常非交换) 环。

练习 4.25. 构成环的必要条件是乘法满足结合律。由映射的复合满足结合律这一点，导出矩阵乘法满足结合律。

练习 4.26. 设 $1 : R^n \to R^n$ 是恒等映射，写出它的矩阵，记为 I_n. 这个矩阵称为 n 阶单位阵。它是 $M_n(R)$ 中的乘法幺元。

练习 4.27. 设 $A \in M_{m\times n}(R)$.

(1) 说明，如果我们将 R^n 中的元素看成 $n \times 1$ 的矩阵 *(称之为列向量)*, 那么 A 对应的映射 $R^n \to R^m$ 就是如下矩阵的乘法

$$R^n \to R^m : v \mapsto A \cdot v$$

这里 $v \in M_{n\times 1}(R) = R^n$.

(2) 说明，A 作为线性映射的像 $\mathrm{Im}(A)$ 是 A 的所有列生成的 R^m 的子模。

5. PID 上矩阵的约化理论

本节我们设 R 是一个 PID, 考虑 R 上的 $m \times n$ 矩阵 $M \in M_{m\times n}(R)$. 注意到由矩阵乘法，$M_{m\times n}(R)$ 具有 $(M_m(R), R; M_n(R), R)$ 多模结构，即可以通过 m 阶方阵左乘，n 阶方阵右乘作用在 $m \times n$ 阶矩阵上面。

记环 $M_n(R)$ 中的乘法可逆元构成的群为 $GL_n(R)$, 我们称 $A, B \in M_{m\times n}$ 是**相抵**的，是指存在两个可逆元 $P \in GL_m(R), Q \in GL_n(R)$ 使得 $A = PBQ$. 注意相抵是一个等价关系。

5.1. 矩阵的初等变换. 对于矩阵的乘法 $C = BA$，可以形象的理解为 C 是 B 的列重新组合得到的，也是 A 的行重新组合得到的，而组合的系数由另一个矩阵决定。由矩阵乘法公式

$$c_{ij} = \sum_k b_{ik}a_{kj}$$

可以看出，C 的第 j 列是由 B 的第 1 列乘以 a_{1j} 加上 B 的第二列乘以 a_{2j}，一直加到第 k 列乘以 a_{kj}. 类似的，C 的第 i 行则是 A 的各第 k 行乘以对应的 b_{ik} 再相加。于是，左乘一个矩阵相当于行操作，右乘一个矩阵则相当于列操作。

所谓初等变换，则是指一类简单基本的对矩阵的可逆操作。可以对一个矩阵通过左乘和右乘一些简单的可逆方阵来施行初等变换。一共有这样几类初等变换：

(1) 将矩阵的一行 (或者一列) 乘以 R 中的某个非零元素，然后加到另一行 (对应的，另一列) 上去. 比如将 A 的第 1 行乘以 r 然后加到第 2 行上去

$$\begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ ra_{11}+a_{21} & ra_{12}+a_{22} \end{pmatrix}.$$

(2) 重新排列矩阵的行或者列. 设 $A = (a_{ij}) \in M_{m\times n}(R)$, 如果我们需要用置换 $\sigma \in S_m$ 重新排列矩阵的行，就左乘 m 阶方阵 $P = (\delta_{\sigma(i)j})$. 这里 $\delta_{ij} = 1_{i=j}$ 表示当 $i = j$ 时为 1, 否则为 0 的一个函数。我们有

$$(PA)_{ij} = \sum_k \delta_{\sigma(i)k}a_{kj} = a_{\sigma(i)j}.$$

这样的方阵叫做置换矩阵。类似的，重新排列矩阵的列就右乘一个 n 阶置换矩阵。

(3) 将矩阵的某一行或者一列乘以一个单位 $u \in R^\times$. 这只需要将矩阵左乘或者右乘一个对角矩阵

$$\begin{pmatrix} 1 & & & & \\ & u & & & \\ & & 1 & & \\ & & & \cdots & \\ & & & & 1 \end{pmatrix}.$$

其中 u 所在的行 (列) 就是需要乘以的行 (列)。

(4) 将矩阵的 a 倍的第 i 行 (或者列) 加上 b 倍的第 j 行 (列) 作为新的第 i 行 (列)，原来的 c 倍第 i 行 (列) 加上 d 倍第 j 行 (列) 作为新的第 j 行 (列)，这里 $ad - bc = 1$. 这也是一个可逆的变换，它等价于左乘以下矩阵 (列的情形：改为右乘，并将 b, c 对调位置)

$$\begin{pmatrix} \cdots & & & & \\ & a & & b & \\ & & \cdots & & \\ & c & & d & \\ & & & & \cdots \end{pmatrix}$$

其中省略的部分都是斜对角的 1. 它的逆是

$$\begin{pmatrix} \cdots & & & & \\ & d & & -b & \\ & & \cdots & & \\ & -c & & a & \\ & & & & \cdots \end{pmatrix}.$$

值得注意的是，这些初等变换都是可逆的，并且它们的逆还是初等变换。并且一系列初等变换都可以用左乘一个矩阵和右乘一个矩阵来得到。这是因为，施行一系列行列初等变换，可以视为按一定顺序左乘右乘了一系列 P_i 和 Q_i, 由结合律，可以将结果写成

$$(P_k \dots P_1)A(Q_1 \dots Q_k)$$

当然，这相当于说 $M_{m\times n}(R)$ 是 $(M_m(R); M_n(R))$ 多模。

5.2. 相抵标准型.

定理 4.4 (PID 中的相抵标准型)**.** *设 $A \in M_{m\times n}(R)$, 这里 R 是一个 PID, 那么存在一组唯一 (在相差 R 中单位的意义下) 的 $d_i \in R$, 满足 $d_1|d_2|\dots|d_r$, 使得 A 相抵于如下对角形*

$$\begin{pmatrix} d_1 & & & & \\ & d_2 & & & \\ & & \cdots & & \\ & & & d_r & \\ & & & & O \end{pmatrix}.$$

这里 O 表示某个零矩阵 (可以没有)，空着的位置都是 0. 我们把得到的 r 叫做 A 的秩，记作 $\mathrm{rank}A$.

Proof. • 考虑矩阵左上角 $a = a_{11}$，通过行交换和列交换我们把素因子数最少的元素挪到这个位置，约定 0 有无穷多个素因子。如果整个矩阵都是 0, 证明可以视为完成了。否则，可以设 a_{11} 具有有限个素因子。

- 如果 a_{11} 整除第一列中所有元素，我们可以用第一行的初等变换消去第一列中剩下的所有元素。否则将不被 a_{11} 整除的 a_{i1} 挪到 a_{21} 的位置，考虑 $I = (a_{11}, a_{21}) = (d)$, 我们有 $\alpha a_{11} + \beta a_{21} = d$. 这里一定有 $(\alpha, \beta) = (1)$, 否则若 α, β 都被某个素因子 p 整除，我们有 $(\alpha/p)a_{11} + (\beta/p)a_{21} = d/p \in I = (d)$, 这不可能。因此可以设有 $\delta, \gamma \in R$ 使得 $\alpha\delta - \beta\gamma = 1$. 那么，通过将原来的第一行乘以 α 加上第二行乘以 β 作为新的第一行，并将原来的第一行乘以 γ 加上第二行乘以 δ 作为新的第二行，我们得到左上角的新元素是 d, 它是原来 a_{11} 的真因数，因此具有更少的素因子数量。
- 不断进行这个操作，直到第一列所有元素都被 a_{11} 整除，此时矩阵的第一列的其他元素可以被 a_{11} 通过初等变换消除为 0, 对第一行也进行类似的操作直到除了 a_{11} 都是 0.
- 如果 a_{11} 整除矩阵中所有元素，我们记 $d_1 = a_{11}$, 然后继续对从第二行第二列开始的矩阵部分做上述归纳操作。否则，重复第一步的操作，将矩阵中素因子数最少的元素挪到 a_{11}. 这个操作一定会停止，因为 a_{11} 的素因子个数会不断减少，直到 a_{11} 整除所有矩阵元素或者 a_{11} 被移除了所有素因子然后变成单位，那时它仍然整除所有矩阵元素。
- 如此操作，矩阵最终可以化为我们所需要的形式。

□

练习 4.28 (★). *本题中 R 是 PID. 并将 $A \in M_n(R)$ 视为 $R^n \to R^n$ 的 R-线性变换。按如下提示，发现高斯消元法。*

(1) *证明，$A \in M_n(R)$ 是可逆的当且仅当它相抵于单位矩阵 I_n，从而得出 A 可逆 $\Leftrightarrow \mathrm{rank}A = n$ 且 $d_1 = d_2 = \dots = d_n = 1$.*
(2) *推出任何可逆矩阵都可以写成初等矩阵 (即初等变换中所使用的矩阵) 的乘积。换句话说，初等矩阵构成了 $GL_n(R)$ 的生成元。*
(3) *证明，若 A 可逆，可以只使用行变换将 A 化为相抵标准型，即 I_n.*

(4) 考虑求逆矩阵 A^{-1} 的如下算法，并排写下两个矩阵 $(A|B)$, 这里 B 是一个 $n\times m$ 的矩阵。只使用行变换 (当 B 也是 n 阶方阵时也可改为只使用列变换)，对 A 施行初等变换，并且同时对 B 做相同的操作。证明当 A 化为单位矩阵时，B 就被变成了 $A^{-1}B$.

(5) 分别考虑 $B=I_n$ 和 $B=\beta$ 为一个列矢量的情形，得出求逆矩阵和对于 A 可逆时解方程

$$Ax=\beta$$

的一个算法。这里 $x\in R^n=M_{n\times 1}(R)$ 是一个未知列矢量。

练习 4.29 (★)**.** 本题中的假定与上题相同。

(1) 设 A 不一定是可逆的，证明 A 的核 $\ker A$ 可以由 $Qe_{r+1},\dots,Qe_n$ 生成，这里 Q 是将 A 化为相抵标准型的矩阵 Q,$r=\mathrm{rank}A$ 是非零的 $d_1|\dots|d_r$ 的个数。

(2) 得出计算子模 $\ker A\subset R^n$ 的如下算法：并排写下两个矩阵 $(A|I)$,I 是单位阵，然后对 A 施行初等变换，同时对 I_n 做相同的列操作，但不进行行操作。当 A 化为标准型时，右侧矩阵的后 $n-r$ 列所生成的 R 子模就是 $\ker A$.

练习 4.30 (★)**.** 设 $\varphi: V\to W$ 是一个线性映射，在某组 V 和 W 的基下对应的矩阵是 $A\in M_{m\times n}(k)$. 证明 $\mathrm{rank}A=\dim_k \mathrm{Im}\varphi$.

6. PID 上的有限生成模的结构

利用我们在本章建立的这些结果，我们将证明两个重量级结论，一个是 PID 上的 (有限生成) 自由模的秩是确定的，即 $R^m\cong R^n\Rightarrow m=n$. 另一个是 PID 上有限生成自由模的子模还是有限生成自由模。

6.1. 有限生成自由模的秩. 事实上，这对所有整环成立。

定理 4.5. 若 R 是一个整环，那么 $R^n\cong R^m\Rightarrow n=m$.

Proof. 我们利用整环的分式域 $K=\mathrm{Frac}(R)$, 考虑将这个问题' 向量空间化', 这样我们也许能用向量空间具有确定的维数来证明这个命题。事实上, 从 $R^n\to R^m$ 的映射 f 定义了一个 R 上的 $m\times n$ 矩阵 A, 由于 R 是整环，包含映射 $i: R\to K$ 是一个单射，将 A 视为 K 上的矩阵可以得到一个 K 中的矩阵 A_K, 它定义了一个 $K^n\to K^m$ 的映射，记为 f_K. 由 f 有逆我们看出 f_K 也有逆，从而 f_K 也是同构，那么由向量空间的维数的唯一性，我们得到 $m=n$. □

于是，我们可以定义有限生成自由模的秩 $\mathrm{rank}(R^n)=n$.

6.2. 有限生成自由模的子模.

6.2.1. *Noether* 模. 所谓 **Noether 模**是指这样一类模，它的所有子模都是有限生成的 (那么自然，它自己也得是有限生成的)。

例 4.4. 设 R 是诺特环，那么 R 作为 R 模的子模是它的所有理想，由 *Noether* 性，它们是有限生成的，因此 R 是 *Noether* 模。

和 Noether 环完全类似，我们有如下的等价叙述

定理 4.6. 以下关于 R 模 M 的叙述等价

(1) M 是 *Noether* 模。

(2) M 的任意子模的上升链必然停止。

(3) M 的任意子模构成的子集中存在极大元。

练习 4.31 (★)**.** 仿照 *Noether* 环的证明，说明上述等价关系。

为了说明各类常见的模都是 Noether 模，我们从 R 开始构造出其它 Noether 模。

定理 4.7. (1) *若 M 是 Noether 模，那么所有 M 的同态像也是。*
(2) *若 M 是 Noether 模当且仅当对某个子模 $N \subset M$ 有 N 和 M/N 也是 Noether 模。*
(3) *Noether 模的有限和，以及有限直和都是 Noether 的。*

Proof. (1) 任何同态 $\varphi : M \to N$ 的像都形如 $\mathrm{Im}\varphi \cong M/\ker\varphi$, 由于对应定理，$M/\ker\varphi$ 的所有子模的上升链都可以对应到 M 的子模的上升链，从而必然停止。
(2) ($\Rightarrow$): 显然成立。
($\Leftarrow$): 考虑 M 的一族子模的上升链 M_i, 那么有 $M_i \cap N$ 和 $(M_i+N)/N$ 两列分别是 N 和 M/N 里面的上升链，由于它们 Noether, 这两个序列都会停止，于是只需证明若 $P \subset Q$, $P \cap N = Q \cap N$ 且 $(P+N)/N = (Q+N)/N$ 时 $P = Q$ 即可。设 $q \in Q$, 由于可以找到 $p \in P$ 使得 $q - p \in N$, 于是这个元素 $q - p \in Q \cap N = P \cap N \subset P$, 从而 $q \in P$.
(3) 由 $0 \to M \to M \oplus N \to N \to 0$ 我们看出有限直和都是 Noether 的，而一般的有限和 $\sum M_i \subset M$ 是 $\bigoplus M_i \to \sum M_i \subset M$ 的同态像。
□

作为结论，若 R 是 Noether 环，R^n 是 Noether 的，从而所有有限生成 R 模都是 Noether 的，因为它们都是某个 R^n 的同态像。

6.2.2. *PID 上的有限生成自由模.* 设 R 是一个 PID, 那么 R 显然是 Noether 环，于是 R^n 是 Noether 模从而其子模都是有限生成的。设 $N \subset R^n$ 是一个子模，由于它是有限生成的，可设有满射 $R^m \to N$, 将它与自然映射 $N \to R^n$ 复合可以得到一个映射 $f : R^m \to R^n$, 其像为 N. 于是我们可以将该映射写为一个 $n \times m$ 的矩阵 A, 考虑 A 的相抵标准型，存在可逆 n 阶和 m 阶的方阵 P, Q 使得 $PAQ = D$, 这里 D 是一个对角形的矩阵。翻译回映射的语言，这就是说，存在两个同构映射 $p : R^n \to R^n$ 和 $q : R^m \to R^m$ 使得 $p \circ f \circ q = \delta : R^m \to R^m \to R^n \to R^n$. 那么显然 $\mathrm{Im}(f) = \mathrm{Im}(f \circ q) \cong \mathrm{Im}(p \circ f \circ q) = \mathrm{Im}\delta$, 这里 δ 对应的矩阵是 D, 也就是以下形式

$$\begin{pmatrix} d_1 & & & & \\ & d_2 & & & \\ & & \cdots & & \\ & & & d_r & \\ & & & & O \end{pmatrix}.$$

其中 $d_i \in R$,$r \leq n$. 于是我们知道，存在 R^n 的一组基 $e_1', e_2', \ldots, e_n'$, 使得 $\mathrm{Im}\delta = d_1 R e_1' \oplus d_2 R e_2' \oplus \cdots \oplus d_r R e_r'$, 这里直和是内直和。此处这个 $\mathrm{Im}\delta$ 已经与 N 同构了，如果要换回原来 N 的形式，那么由于 p^{-1} 是同构映射，

$$N = p^{-1}(\mathrm{Im}\delta) = \bigoplus_{i \leq r} d_i R p^{-1}(e_i').$$

这里 $e_i = p^{-1}(e_i')$ 仍然构成 R^n 的一组基，因为 p^{-1} 是同构。于是存在 R^n 的一组基 $e_1, \ldots, e_n$ 使得

$$N = d_1 R e_1 \oplus \cdots \oplus d_r R e_r.$$

推论 4.1. $N \cong R^r$ *并且* $\mathrm{rank} N = r \leq n$.

6.2.3. *PID* 上的有限生成模. 任何有限生成模 M 都是自由模的同态像，从而是自由模关于它某个子模的商。我们知道，PID 上有限生成自由模 R^n 的子模一定形如 $(d_1)e_1 \oplus \cdots \oplus (d_r)e_r$, 这里 e_i 是 R^n 的一组基 (不一定是标准基). 于是在同构 $R^n \cong Re_1 \oplus \dots Re_n$ 下，这个商同构于

$$R/(d_1) \oplus \cdots \oplus R/(d_r) \oplus R^{n-r}$$

定理 4.8. 设 R 是一个 *PID*,M 是一个有限生成 R 模，那么存在一列 R 中的元素 $d_1|d_2|\dots|d_r$ 和非负整数 k 使得

$$M \cong R/(d_1) \oplus \cdots \oplus R/(d_r) \oplus R^k.$$

这称作 M 的'循环分解'.

练习 4.32. 证明，有限生成阿贝尔群都同构于如下形式

$$G \cong \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_r} \oplus \mathbb{Z}^k$$

这里 $d_1|d_2|\dots|d_r$ 是一列整数。

练习 4.33 (★). 利用 *PID* 中的素因子分解，将上述有限生成模的结构定理转化为如下"准素分解"的形式。

(1) 若 $d = up_1^{k_1} \dots p_s^{k_s}$, 这里 u 是单位, p_i 是不同的素数, $k_s \geq 0$ 是非负整数，证明 *(*这可以看作是中国剩余定理的特例。你本质上只需要证明 $d = d_1d_2$, 其中 d_1, d_2 互素的情形*)*

$$R/(d) \cong R/(p_1^{k_1}) \oplus \dots R/(p_s^{k_s}).$$

(2) 说明 $\mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{18} \cong \mathbb{Z}_2^3 \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_9)$.

(3) 证明，所有有限生成 R 模都是形如 $R/(p^k)$ 和 R 的模的直和。准确的说，有如下分解

$$M \cong R^k \oplus \bigoplus_p \left((R/p^{\alpha_{p,1}})^{\beta_{p,1}} \oplus (R/p^{\alpha_{p,2}})^{\beta_{p,2}} \oplus \cdots \oplus (R/p^{\alpha_{p,s_p}})^{\beta_{p,s_p}}\right)$$

其中 $0 \leq \alpha_{p,1} \leq \alpha_{p,2} \leq \dots \alpha_{p,s_p}$, $\beta_{p,i} \geq 0$.

(4) 反过来，说明准素分解如何化为循环分解。

7. 线性映射的标准型

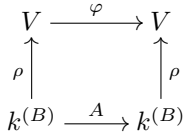
本节我们设 $\varphi : V \to V$ 是一个有限维 k-向量空间上的线性映射。如果我们取 V 的一组基 $B = \{e_1, \dots, e_n\}$ 并将 φ 写成矩阵形式 A, 一个问题出现了，在向量空间 V 和 φ 的定义中，没有明确选择的是哪一个基。事实上，很多线性空间和线性映射都可以在不写出基底和矩阵的情况下定义出来，即不依赖于基底的选取。但是如果我们要将其写成矩阵形式，就一定要人为选取一组基。这就产生了这样几个问题:

(1) 不同的基的选取对矩阵有什么影响?

(2) 有没有一种' 最好' 或者' 很好' 的特殊基，使得矩阵的形式得到简化?

7.1. 相似矩阵. 我们先来看第一个问题。设 $B' = \{e'_1, \dots, e'_n\}$ 是另一组基，其矩阵记作 A'. 所谓矩阵，本质上是 $k^n \to k^n$ 的映射，它与原来的映射的关系可以用基映射 $\rho : k^{(B)} \to V$ 来描述，这里 ρ 是 $\{e_1, \dots, e_n\}$ 所确定的映射，它是一个同

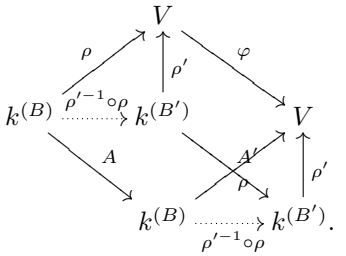
构。将 A 看做 $k^n \to k^n$ 的线性映射，此时我们有 $A = \rho^{-1} \circ \varphi \circ \rho$, 如下交换图所示 (所谓交换图，是指按照不同路线将映射复合起来时，所得的映射一致)



类似的，如果 ρ' 是另一组基所确定的映射，则有 $A' = \rho'^{-1} \circ \varphi \circ \rho'$. 于是

$$A' = \rho'^{-1}\rho A \rho^{-1}\rho' = (\rho'^{-1}\rho)A(\rho'^{-1}\rho)^{-1}$$

这个故事可由如下交换图来表示



注意到这里 $\rho'^{-1} \circ \rho : k^{(B)} \to k^{(B')}$ 也是一个 $n \times n$ 的矩阵并且还是同构 (从而是可逆矩阵). 记该矩阵为 P, 称作坐标转移矩阵。我们得到

$$A' = PAP^{-1}.$$

这样两个来自同一个映射的矩阵就被联系起来了。如果存在可逆矩阵 P 使得两个方阵 A', A 由上述关系联系起来，我们就称这两个矩阵**相似**. 容易验证，相似是 $M_n(k)$ 上的等价关系。

练习 4.34. 设 $V = k^2$, 选取 $\varphi : V \to V$ 为满足 $\varphi(e_1) = e_2$, $\varphi(e_2) = e_1$ 的唯一线性映射。φ 对应的矩阵 A 是什么？如果我们选取一组新的基 $e_1' := (1, 1), e_2' = (1, -1)$, 计算转移矩阵 P 和 A'.

7.2. 相似标准型. 现在我们需要回答，给定两个矩阵 A, B, 如何判断它们是否相似? 这本质上是一个分类问题。一般来讲，我们会从以下几个角度研究这样的问题，一是寻找' **不变量**'，即可以通过矩阵 A 算出来的，在相似变换下不变的量。二是，我们可以在每一个相似等价类中找出一个**代表元**，然后看看矩阵 A 和 B 能否被化为相同的代表元，或者从不变量计算出这些代表元。无论哪一种，都启发我们从不依赖于坐标的角度出发。不妨设我们的矩阵是线性映射 φ 在 V 上的一组基下的矩阵表示，我们发现，V 除了是 k 模以外，还可以把 φ 作用在 V 上。通过重复作用 φ 和它们的线性组合，我们可以将任一个 φ 的 k 多项式 $p(\varphi)$，作用在 V 上，这里 $p(t) \in k[t]$ 是多项式。于是 V 成为一个 $k[t]$ 模，其作用为

$$p(t)v := p(\varphi)v.$$

我们思考，如果我们让 φ 代表矩阵的作用，那么矩阵相似是否和对应的 V 模结构有关? 事实上我们可以发现

引理 4.1. 设 V_A 是 V 在 $t.v := A.v$ 作用下的 $k[t]$ 模结构，V_B 是 V 在 $t.v := B.v$ 作用下的 $k[t]$ 模，那么 A 与 B 相似当且仅当作为 $k[t]$ 模，$V_A \cong V_B$.

PROOF. • 如果 A 与 B 相似，那么转移矩阵 $P : V_A \to V_B$ 就是所需的同构映射，注意它的值域上 t 的作用与定义域上的不同。由于它是可逆矩阵，它显然是 k-模同构，为验证它是 $k[t]$ 模同态，此只需验证它与 t 交换：

$$P(tv) = PAv_a = PAP^{-1}Pv = B(Pv) = t(Pv).$$

注意这里概念上 $(Pv) \in V_B$, 尽管作为向量空间 V_A 和 V_B 完全等同，但它们的 $k[t]$ 模结构不同。

- 反过来，如果存在 $k[t]$ 模同构 $P : V_A \cong V_B$, 我们就有

$$P(tv) = tP(v)$$

而这就是 $PA = BP \Leftrightarrow PAP^{-1} = B$.

□

于是，我们发现，对矩阵或映射作相似分类等价于对 $k[t]$ 模进行分类。注意到 $k[t]$ 是一个 PID, 我们知道，PID 上有限生成模的结构已经被我们完全分类清楚了! 它一定可以写成一些形如 $R/(d)$ 的模或者准素模 $R/(p^k)$ 的直和。一种想法是，我们可以把这样的形式对应的矩阵作为我们的代表元，从而只需要将 V_A 化为这样的形式，就可以将矩阵化为标准型。我们先来讨论标准型到底长什么样。

7.2.1. *有理标准型*. 在 V_A 的循环分解中，我们把得到的 d_i 称之为矩阵 A 或者 φ 的**不变因子**。为了找出更简单的形式，我们将循环分解中的不变因子分解为素因子的乘积，从而变成准素分解，即 V 成为形如 $R/(p^k)$ 的模的直和 (R 不会出现在分解中，因为 V 是有限维 k 向量空间)，这里 $p \in R$ 是 R 上的不可约元素。当我们写出

$$V_A \cong R/(p_1^{k_1}) \oplus \cdots \oplus R/(p_r^{k_r})$$

时 (这里允许序列 p_i 和 k_i 中的元素重复)，我们把所有的这些 $p_i(t)^{k_i}$(可重复) 称为 A 或者 φ 的**初等因子**。容易看出，给出初等因子完全确定了 V_A 的模结构。上述分解不仅是 R 模的直和分解，也是作为 k 模的直和分解。于是我们知道，只需找出 $R/(p_i^{k_i})$ 的一组 k 基，即可找出 V 的一组 k-基。可设 $p_i(t)^{k_i} = t^{d_i} - a_{d_i-1}t^{d_i-1} - \cdots - a_0$ 是首系数为 1 的多项式 (因为在 $k[t]$ 中 $k - \{0\}$ 都是单位), 我们取 $1, t, t^2, \ldots, t^{d_i-1}$ 在 $R/(p_i^{k_i})$ 中的像作为它的一组 k-基。那么 φ 在这组基上的作用就是乘以 t 在这组基上的作用，我们有

$$\begin{gathered} t \cdot 1 = t \\ t \cdot t = t^2 \\ \cdots \\ t \cdot t^{d_i-1} = t^{d_i} = a_{d_i-1}t^{d_i-1} + a_{d_i-2}t^{d_i-2} + \cdots + a_0 \end{gathered}$$

这便给出了在这组基下 φ 在子空间 $R/(p_i^{k_i})$ 上作用的矩阵

$$A_{p_i^{k_i}} = \begin{pmatrix} & & & a_0 \\ 1 & & & a_1 \\ & 1 & & a_2 \\ & & \cdots & \cdots \\ & & 1 & a_{d_i-1} \end{pmatrix}.$$

于是 φ 在这样的基下，其矩阵便是形如这样的矩阵按照对角排列构成的矩阵

$$A = \begin{pmatrix} A_{p_1^{k_1}} & & & \\ & A_{p_2^{k_2}} & & \\ & & \cdots & \\ & & & A_{p_r^{k_r}} \end{pmatrix}.$$

这里矩阵中的所有元素都属于 k, 我们称之为 φ 的**有理标准形**。

练习 4.35 (★). 设 $\varphi: V \to V$ 是 n 维 k 线性空间上的线性变换。从而 φ 使 V 成为一个以 $k[t]$ 模 V_φ.

(1) 证明, φ 的不变因子中的 d_n 就是所有初等因子的最小公倍数。
(2) 对于一个环 R 上的模 M, 定义

$$\mathrm{ann}(M) := \{r \in R | rM = 0\}$$

称之为 M 的零化子, 证明它是 R 的一个理想。
(3) 得出 φ 存在最小多项式, 即 $\mathrm{ann}(V_\varphi) = (m(t))$ 并且该多项式就是 $m(t) = d_n(t)$, 其次数 $\leq n$.

7.2.2. *Jordan* 标准型. 如果我们的域 k 是代数闭域, 即所有 k 上的多项式都在 k 上有根, 即可以分解为一次式的乘积 (比如 $k = \mathbb{C}$), 那么矩阵还能化归为更简单的形式。这时, $k[t]$ 上的不可约多项式都形如一次式 $(t-a)$, 于是 $p_i^{k_i}$ 一定形如 $(t-\lambda_i)^{k_i}$. 我们考虑 $R/((t-\lambda_i)^{k_i})$ 的一个形式更简便的 k-基: $(t-\lambda)^{k_i-1}, (t-\lambda)^{k_i-2}, \ldots, 1$, 在这组基下, t 的作用如下

$$t \cdot (t-\lambda)^{k_i-1} = \lambda \cdot (t-\lambda)^{k_i-1} + 0$$

$$t \cdot (t-\lambda)^{k_i-2} = \lambda \cdot (t-\lambda)^{k_i-2} + (t-\lambda)^{k_i-1}$$

$$\cdots$$

$$t \cdot 1 = \lambda \cdot 1 + (t-\lambda)$$

这表明, 在这组基下, φ 在这个子空间上具有如下矩阵表示

$$J_{p_i^{k_i}} = \begin{pmatrix} \lambda_i & 1 & & & \\ & \lambda_i & 1 & & \\ & & \lambda_i & 1 & \\ & & & \cdots & 1 \\ & & & & \lambda_i \end{pmatrix}.$$

这里矩阵是 $k_i \times k_i$ 的大小。于是 φ 在 V 这样选取的基下具有如下矩阵表示

$$A = \begin{pmatrix} J_{p_1^{k_1}} & & & \\ & J_{p_2^{k_2}} & & \\ & & \cdots & \\ & & & J_{p_r^{k_r}} \end{pmatrix}.$$

这称为 φ 的 **Jordan 标准型**。特别的, 如果 $k_i = 1$, 那么 $J_{(x-\lambda_i)} = (\lambda_i)$ 是一个只有对角线的一阶矩阵。

练习 4.36. 证明, A 在域 k 上可对角化当且仅当所有初等因子都是一次的。于是等价于 A 的最小多项式能在 k 上分解成一次式的乘积并且无重根。

练习 4.37 (★★★). 设 $k = \mathbb{F}_p$ 是有限域, 那么 $M_2(k)$ 中有多少个 k-相似等价类 ?

7.2.3. *自由化解*. 虽然我们已经知道了所有映射的矩阵都可以化为标准型，即 V_A 模可以分解为结构定理中所叙述的形式，但是，我们要怎么具体来确定 V_A 的模结构呢? 在模的理论中，有一个方法是所谓的' 模的化解'。就像 Taylor 展开一样，对于一个一般的 R 模 M, 在了解了它的生成元之后，可以定义一个生成映射 $R^{(I)} \to M$. 那么这个 $R^{(I)}$ 就可以视为 M 的' 一阶近似', 它包含了所有生成元，但是生成元之间却没有任何线性关系。这些关系事实上就是 $R^{(I)} \to M$ 的核，记为 K。如果我们再找出 K 的一组生成元，就可以得到一个正合列

$$R^{(I_2)} \to R^{(I_1)} \to M \to 0.$$

如果此时左边映射已经是单射，我们的逼近就结束了，否则还可以继续不停的在左边重复这个操作，得到一个很长的正合列，这个正合列就叫 M 的**自由化解序列**。注意这样的序列未必是唯一的。

练习 4.38 (★). *证明，对于 PID 上的有限生成模 M, 总可以构造出自由化解序列形如*

$$0 \to R^{(I_2)} \to R^{(I_1)} \to M \to 0.$$

即，它的' 自由模逼近' 在至多两项之后就可以停止了。

7.2.4. *V 的 $k[t]$ 化解*. 本节记 $R = k[t]$. 我们要如何给定一个 R^n 到 V 的满射? 或者说，怎么找出一组生成元? 事实上，当我们给定一组 V 的基 $\alpha_1, \dots, \alpha_n$ 之后，φ 具有矩阵表示 A，并且 $\alpha_1, \dots, \alpha_n$ 是 V 的一组 k 生成元，自然也是一组 R-生成元。于是我们考虑由 $\alpha_1, \dots, \alpha_n \in V$ 确定的 R-满射

$$\rho : R^n \to V.$$

现在要为这个映射找出核，我们考虑矩阵表示 A, 显然有

$$x_i := te_i - (a_{1i}e_1 + \cdots + a_{ni}e_n) \in \ker \rho.$$

这里 $e_i \in R^n$ 是标准基，这就找出了 $\ker \rho$ 的 n 个生成元 $x_1, \dots, x_n$. 于是我们可以作出映射 $R^n \to R^n$ 使它的像对应到 x_i, 事实上, 该映射刚好由矩阵 $tI - A \in M_n(R)$ 所描述。由于 $te_i = x_i + (a_{1i}e_1 + \dots)$, 我们发现 $N = \sum Rx_i + \sum ke_i$ 是 R^n 的一个 R-子模。于是对任意 $x = \sum p_i(t)e_i \in \ker \rho$, 它都属于 N, 从而可以写成

$$x = \sum q_i(t)x_i + \sum c_i e_i.$$

注意到 $0 = \rho(x) = \sum c_i \alpha_i$, 我们知道所有 $c_i = 0$. 这表明 x 是 x_i 的 R-线性组合，我们证明了 x_i 确实构成了 $\ker \rho$ 的一组生成元。

我们还需证明 $R^n \to R^n$ 是单射, 即 x_i 是 R-线性无关组。为此, 设 $\sum q_i(t)x_i = 0$, 我们有

$$\sum_i q_i(t)te_i - \sum_{i,j} q_j a_{ij} e_i = \sum_i \left(q_i t - \sum_j q_j a_{ij} \right) e_i = 0$$

这表明 $tq_i = \sum_j a_{ij} q_j$. 那么我们发现，$(q_1, \dots, q_n) = \sum Rq_i \subset \sum kq_i$. 由于 R 是 PID, 左边的理想是主理想，设它等于 (d). 若 $d \neq 0$, 由于 R 是整环，(d) 应当是包含了任意次数的多项式，但右边 $\sum kq_i$ 是有限维 k-空间，且仅包含有限次数的多项式，这不可能。于是 $d = 0$, 我们知道 $q_1 = q_2 = \cdots = q_n = 0$.

推论 4.2. *我们有如下 R-模的短正合列*

$$0 \to R^n \to R^n \to V_A \to 0.$$

其中 $R^n \to R^n$ 是由 $tI - A \in M_n(R)$ 确定的映射。

有了这个基本的正合列之后，我们来考察怎么具体将 V_A 的模结构计算出来。注意到 $tI-A$ 是 PID 上的矩阵，于是存在可逆矩阵 $P,Q\in M_n(R)$ 使得

$$P(tI-A)Q=D=\mathrm{diag}(d_1,\dots,d_r,0,\dots,0)$$

这里 $d_1|\dots|d_r$, diag 表示以这些元素为对角线，其它地方为 0 的对角矩阵。那么我们有这样一个交换图

$$\begin{array}{ccccccccc}
0 & \longrightarrow & R^n & \xrightarrow{tI-A} & R^n & \longrightarrow & V_A & \longrightarrow & 0\\
 & & \downarrow{\scriptstyle Q^{-1}} & & \downarrow{\scriptstyle P} & & \vdots{\scriptstyle q} & & \\
0 & \longrightarrow & R^n & \xrightarrow{D} & R^n & \longrightarrow & V' & \longrightarrow & 0
\end{array}$$

这里我们需要以下一个简单的引理

引理 4.2. *设 R 是一个 (未必交换) 环，M' 等都是 (不妨设) 左 R 模，如果给定了如下的关于 R 模和 R 模同态的交换图 (除了 γ 以外的部分)*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0\\
 & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \vdots{\scriptstyle \gamma} & & \\
0 & \longrightarrow & N' & \xrightarrow{f'} & N & \xrightarrow{g'} & N'' & \longrightarrow & 0
\end{array}$$

并且两个行都是正合的，那么可以唯一的构造出一个 R 模同态 γ, 使得整个图都交换。另外，如果 α,β 还是同构映射，那么 γ 也是。(本质上，这个同态 γ 是由 β 诱导的。)

Proof. 事实上，取 $m''\in M''$, 考虑它在 M 中的一个原象 m, 将其映射到 $g'\circ\beta(m)$, 我们定义 $\gamma(m'')=g'\circ\beta(m)$. 那么需要验证这个定义不依赖于原象 m 的选取，事实上，另一个原象只与 m 相差一个 $\ker(g)$ 的元素，即相差一个 $\mathrm{Im}f$ 的元素，故记另一个原象为 $m+f(m')$, 它在 N'' 中的像是 $g'(\beta(m))+g'(\beta(f(m')))=g'(\beta(m))+g'(f'(\alpha(m')))=g'(\beta(m))$, 于是 γ 的定义不依赖于原象 m 的选取。这里用到了交换性。容易验证 γ 确实是一个 R 模同态。唯一性是显然的，因为 γ 就是由图的交换性唯一确定的。

现在来考虑 α,β 是同构时，γ 为何是同构映射。事实上，我们作出 α^{-1},β^{-1}, 然后定义出这样一个交换图

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0\\
 & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \vdots{\scriptstyle \gamma} & & \\
0 & \longrightarrow & N' & \xrightarrow{f'} & N & \xrightarrow{g'} & N'' & \longrightarrow & 0\\
 & & \downarrow{\scriptstyle \alpha^{-1}} & & \downarrow{\scriptstyle \beta^{-1}} & & \vdots{\scriptstyle \gamma'} & & \\
0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0
\end{array}$$

那么由引理的前一部分，可以唯一的构造出 γ' 与图交换。注意到 $1_{M''}:M''\to M''$ 显然是一个与第一行和第三行交换的映射，于是由唯一性，$\gamma'\circ\gamma=1_{M''}$, 从而 γ 是同构。 □

现在，由于 P,Q 可逆，Q^{-1},P 显然定义出了同构映射。由这个引理我们知道可以构造出 V_A 到 V' 的同构，这里

$$V'\cong R^n/DR^n=R/(d_1)\oplus\cdots\oplus R/(d_r)\oplus R^{n-r}.$$

注意到 $V' \cong V_A$ 作为 R 模同构自然也是 k 模同构，并且是一个有限维 k 向量空间，但是 R 并不是有限维 k 向量空间，于是 $n = r, d_1|d_2|\dots|d_n$ 是 R 中的非零元素使得

$$V_A \cong V' \cong R/(d_1) \oplus \cdots \oplus R/(d_n).$$

当然，判断出 V_A 同构于上述形式并不需要前面的论证，只需要使用有限生成 R 模的结构定理即可。但是上述过程给出了一个利用 A 的形式将 V_A 化为结构定理中的标准型的明确计算方式。

练习 4.39 (★). 证明，当给出了如下 R 模同态的交换图之后 (这里行都是短正合列)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0 \end{array}$$

可以唯一的构造映射 α 使图交换。如果 β, γ 都是同构，那么 α 也是。

练习 4.40 (★★). 设 $K \subset L$ 是两个域，K 是 L 的子域。证明 $A, B \in M_n(K)$ 在 K 上相似当且仅当它们在 L 上相似。

7.2.5. 特征向量与根子空间. 本节我们通过特征空间理论的讨论如何实际的得到转移矩阵 P 使得 $P^{-1}AP = D$ 为我们的标准型，或者等价的说，$AP = DP$. 假定 k 是一个使 φ 的初等因子都是形如一次式的乘积 $(x - \lambda_i)^{k_i}$ 的域 (比如说，代数闭域，如 $k = \mathbb{C}$)，我们将此时的初等因子中出现的 λ 称作 φ 的**特征值**. 按照特征值排列准素因子我们有

$$V_\varphi \cong \bigoplus_\lambda \left(\bigoplus_k (R/(t-\lambda)^k)^{n_k} \right).$$

对于每个特征值 λ,$\bigoplus_k (R/(t-\lambda)^k)^{n_k}$ 在同构下对应的 V_φ 的子空间称为关于特征值 λ 的**根子空间**，它等于

$$R_\lambda := \bigcup_k \ker(\varphi - \lambda)^k.$$

而子空间 $\ker(\varphi - \lambda)$ 称之为关于 λ 的**特征子空间**，记为 V_λ, 其中的向量叫做 φ 的**特征向量**，它显然是对应特征值的根子空间的子空间。注意到我们前面讨论 Jordan 标准型时对形如 $R/((t-\lambda)^k)$ 的子模的基的 k-基的选取，我们知道 $1 \in R$ 在该模中的投射像生成了这个模，即它有一组基 $(t-\lambda)^{k-1}, \dots, (t-\lambda), 1$, 这里我们的基需要按这样的顺序排列以保证 φ 的矩阵是之前所描述的 Jordan 形式。那么如果我们找出了 $1 \in R/((x-\lambda)^k)$ 到 V_φ 的同构下的像，不妨记为 α，该子空间对应的一组 k-基就可以写成 $(\varphi - \lambda)^{k-1}\alpha, \dots, (\varphi - \lambda)\alpha, \alpha$.

如果 φ 是可对角化的，那么所有初等因子都是一次式，此时根子空间就等于特征子空间。只要求出特征向量，就能得到 P. 对于一般的 φ 我们需要求出根子空间的基 $\ker(\varphi - \lambda)^k$. 下面我们举几个例子来说明

例 4.5. 我们考虑域 $k = \mathbb{Q}$ 上的如下矩阵

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, tI - A = \begin{pmatrix} t-1 & -2 \\ -3 & t-4 \end{pmatrix}.$$

那么我们对 $tI - A$ 做初等变换，得到

$$\Rightarrow \begin{pmatrix} -2 & t-1 \\ t-4 & -3 \end{pmatrix} \Rightarrow \begin{pmatrix} -2 & 0 \\ t-4 & \frac{(t-4)(t-1)}{2} - 3 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & t^2 - 5t - 2 \end{pmatrix}.$$

于是 A 在 $\mathbb{Q}$ 上的有理标准型为 $\begin{pmatrix} 0 & 2 \\ 1 & 5 \end{pmatrix}$. 即，存在 $\mathbb{Q}$ 上的可逆矩阵，使 A 相似于上述形式。如果我们考虑 $k=\mathbb{R}$ 或者 $k=\mathbb{C}$(事实上，只需要 $k=\mathbb{Q}(\sqrt{33})$ 即可), 那么从 $t^2-5t-2=\left(t-\frac{5+\sqrt{33}}{2}\right)\left(t-\frac{5-\sqrt{33}}{2}\right)$ 我们得到它的初等因子，从而它在 k 上相似于如下对角阵

$$A'=\begin{pmatrix} \frac{5+\sqrt{33}}{2} & 0 \\ 0 & \frac{5-\sqrt{33}}{2} \end{pmatrix}.$$

这就是它在任意包含了 $\mathbb{Q}(\sqrt{33})$ 的域 k 上的的 *Jordan* 标准型。

为求出 P, 考虑它对这两个特征值 $\lambda_1=\frac{5+\sqrt{33}}{2}, \lambda_2=\frac{5-\sqrt{33}}{2}$ 的特征子空间 $V_{\lambda_1}=\ker(A-\lambda_1 I)$ 和 $V_{\lambda_2}=\ker(A-\lambda_2 I)$. 利用前几节描述的 ker 的算法对 $\ker(A-\lambda I)$ 进行计算 (或者直接解方程) 我们可以计算出这两个空间的生成元，即特征向量是 $\begin{pmatrix} 2 \\ \lambda-1 \end{pmatrix}$, 这里令 $\lambda=\lambda_1,\lambda_2$ 分别得到对应特征值的特征向量。于是 (注意，P 不需要是唯一的。)

$$P=\begin{pmatrix} 2 & 2 \\ \frac{3+\sqrt{33}}{2} & \frac{3-\sqrt{33}}{2} \end{pmatrix}$$

满足 $AP=PA'$, 即 $P^{-1}AP=A'$.

例 4.6. 考虑如下 $\mathbb{Q}$ 上的矩阵，将其化为 *Jordan* 标准型 J，并找出对应的 P 使得 $P^{-1}AP=J$.

$$A=\begin{pmatrix} 2 & 1 & 2 & 1 \\ 1 & 2 & 2 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

通过对 $tI-A$ 的初等变换，我们可以计算出它的不变因子

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & (t-1) & 0 \\ 0 & 0 & 0 & (t-1)^2(t-3) \end{pmatrix}$$

从而得出初等因子是 $(t-1),(t-1)^2$ 和 $(t-3)$. 于是我们先计算 $\ker(A-1\cdot I)^2$, 得到了根子空间 R_1 如下的一组基 (基并非唯一，大家算出来的可能不同)

$$v_1=\begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, v_2=\begin{pmatrix} -2 \\ 0 \\ 1 \\ 0 \end{pmatrix}, v_3=\begin{pmatrix} -2 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

对上述向量分别作用 $A-I$，我们发现前两个向量落入了 $\ker(A-I)$, 而最后一个 $(A-I)v_3=-e_1-e_2+e_3$ 从而属于 $\ker(A-I)^2-\ker(A-I)$. 于是令 $\alpha_2=v_3$, 这个向量就对应了 $R/((t-1)^2)$ 中的生成元 1, 它的 *Jordan* 块对应的基是 $(A-I)\alpha_2,\alpha_2$. 那么我们还需要一个不属于 $k[\varphi]\alpha_2$ 生成的空间的特征向量来对应到另一个初等因子 $(t-1)$, 显然可以取 $\alpha_1=v_1$.

最后通过简单的对特征向量 $\ker(A-3I)$ 的计算，我们找到一个特征值为 3 的特征向量

$$\beta = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

将它们以 $\alpha_1, (A-I)\alpha_2, \alpha_2, \beta$ 的顺序排列进矩阵 P, 我们就得到了所需的转移矩阵

$$P = \begin{pmatrix} -1 & -1 & -2 & 1 \\ 1 & -1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, P^{-1}AP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

练习 4.41 (★★). 事实上，在上述例子的 P 的计算过程中，我们还可以用以下手段降低计算量。

(1) 设 $\varphi : V \to V$ 是一个一般的 n 维空间上的线性映射，它的极小多项式形如 $(t-\lambda_1)^{k_1}(t-\lambda_2)^{k_2}$, 这里两个特征值不相同。证明

$$\mathrm{Im}(\varphi-\lambda_1)^{k_1} = \ker(\varphi-\lambda_2)^{k_2}$$

$$\ker(\varphi-\lambda_1)^{k_1} = \mathrm{Im}(\varphi-\lambda_2)^{k_2}.$$

(2) 这里 A 回到上一个例子中的 A. 通过计算矩阵 $(A-3I)$ 和 $\ker(A-3I)$, 找出 $\lambda = 3$ 的特征向量，并利用 $\ker(A-I)^2 = \mathrm{Im}(A-3I)$, 说明 $\ker(A-I)^2$ 直接由 $A-3I$ 的列生成，从而无需计算 $(A-I)^2$ 和它的核。

练习 4.42 (★). *Fibonacci* 序列是所谓由初始条件 $F_1 = 1, F_2 = 1$ 以及递推式

$$F_{n+2} = F_{n+1} + F_n$$

所确定的唯一正整数序列。我们可以将上述递推式转化为矩阵形式

$$\begin{pmatrix} F_{n+2} \\ F_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix}.$$

记其矩阵为 A. 通过将上述矩阵化为 $k = \mathbb{C}$ 上的 *Jordan* 标准型，我们可以轻松的计算 A^n，并从其中导出 F_n 的通项公式。

练习 4.43 (★★). 是否存在矩阵 X 使得

$$X^2 = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}?$$

7.3. 线性映射的不变量. 所谓不变量，是指，要么这个量的定义不依赖于基的选取，要么对任意基的选取，这个量都是不变的 (即所谓相似不变量). 本节我们来看线性映射的几个经典的不变量。

7.3.1. 行列式. 考虑一个 n 维 k-向量空间 V 和其上的一个线性映射 $\varphi : V \to V$. 我们考虑 V 上的一个 n-线性交错函数

$$D(v_1, v_2, \ldots, v_n) : V \times V \times \cdots \times V \to k.$$

所谓 n-线性是指，D 对每个变量 v_i 都是线性的，即固定其它元素时，

$$v_i \mapsto D(v_1, \ldots, v_i, \ldots, v_n) : V \to k$$

是一个 k 线性映射。而交错则是指，如果有两个向量相同，比如 $v_i = v_j = v$，那么函数的值为 0.

$$D(v_1, \dots, v, \dots, v, \dots, v_n) = 0.$$

作为推论，这表明当我们交换两个向量 v_i, v_j 的位置时，函数值会变为原来的相反数

$$D(v_1, \dots, v_i, \dots, v_j, \dots, v_n) = -D(v_1, \dots, v_j, \dots, v_i, \dots, v_n).$$

这是因为 $D(\dots, v_i + v_j, \dots, v_i + v_j, \dots) = 0$, 利用 n-线性展开可得上述推论。那么首先我们要问了，我们加了这么多奇怪的条件，这样的函数还能存在吗？我们考虑引入 V 的一组基 $e_1, \dots, e_n$, 并考虑 v_i 在基底下的分解

$$v_i = \sum a_{ji} e_j.$$

那么由 n 线性我们有

$$\begin{aligned} D(v_1, \dots) &= \sum_{j_1} a_{j_1 1} D(e_{j_1}, \dots) \\ &= \sum_{j_1} \sum_{j_2} a_{j_1 1} a_{j_2 2} D(e_{j_1}, e_{j_2}, \dots) \\ &= \dots \\ &= \sum_{j_1, \dots, j_n} a_{j_1 1} \dots a_{j_n n} D(e_{j_1}, \dots, e_{j_n}) \end{aligned}$$

由于 $D(e_{j_1}, \dots, e_{j_n})$ 中需要没有重复元素才能不为 0, 我们只需要考虑 $k \mapsto j_k$ 刚好构成 $\{1, \dots, n\}$ 的一个置换的情形。不妨记这个置换为 σ, 此时置换 σ 又可以分解为一系列对换的乘积，而每一个对换对 D 来说刚好产生一个负号，从而

$$D(e_{\sigma(1)}, \dots, e_{\sigma(n)}) = \operatorname{sgn}(\sigma) D(e_1, \dots, e_n)$$

故

$$D(v_1, \dots, v_n) = \left(\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n} \right) D(e_1, \dots, e_n).$$

容易验证上述表达式定义的函数确实满足 n-线性性和交错性，于是我们想要的函数 D 确实存在，但其定义似乎依赖于 $D(e_1, \dots, e_n)$ 值的选取和 V 的一组基的选取。为了避免无意义的 0 函数，我们选取 $D(e_1, \dots, e_n) \neq 0$, 对任意映射 φ, 考虑

$$\det(\varphi) := \frac{D(\varphi(e_1), \dots, \varphi(e_n))}{D(e_1, \dots, e_n)}$$

称为 φ 的**行列式**，如果我们写出矩阵分解 $\varphi(e_i) = \sum a_{ji} e_j$, 根据上面的公式，我们知道这个定义不依赖于 $D(e_1, \dots, e_n)$ 的值的选取 (只要不为 0), 从而可以写出对于矩阵 A 的行列式的定义

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} \dots a_{\sigma(n)n}.$$

这相当于假定 $D(e_1, \dots, e_n) = 1$ 时，$D(\alpha_1, \dots, \alpha_n)$ 的值，这里 α_i 是 A 的列。神奇的是，事实上 φ 的行列式的定义也不依赖于基 $e_1, \dots, e_n$ 的选取！为此我们只需证明相似的矩阵行列式相同。而这是因为行列式是一个乘法同态：

定理 4.9 (行列式是乘法同态)**.** *固定向量空间 V 的一组基的选取，设 $A, B \in M_n(k)$ 是两个矩阵，那么*

$$\det(AB) = \det(A) \det(B).$$

PROOF. 设 A 的列从左到右分别是 $\alpha_1, \ldots, \alpha_n$, 那么 AB 的第 j 列就是 $b_{1j}\alpha_1 + \cdots + b_{nj}\alpha_n$. 设, 通过类似于前面的交错和展开，我们有

$$\begin{aligned}\det(AB) &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) b_{\sigma(1)1}\ldots b_{\sigma(n)n} D(\alpha_1, \ldots, \alpha_n)\\ &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) b_{\sigma(1)1}\ldots b_{\sigma(n)n} \det(A)\\ &= \det(A)\det(B).\end{aligned}$$

□

很容易看出，$\det(I) = 1$, 因此对于可逆矩阵 P 有

$$\det(PP^{-1}) = \det(P)\det(P^{-1}) = 1 \Rightarrow \det(P^{-1}) = (\det P)^{-1}.$$

那么，两个相似的矩阵 $A' = PAP^{-1}$ 的行列式就一定是相同的

$$\det(A') = \det(P)\det(A)(\det P)^{-1} = \det(A).$$

事实上，行列式有着明显的含义，n-线性交错函数某种意义上就是 n-维空间中的一种带符号的体积函数，它描述了向量 $v_1, \ldots, v_n$ 张成的平行多面体的体积。而这个体积的定义最终还需依赖' 基础体积'$D(e_1, \ldots, e_n)$ 的值。那么，φ 的行列式就是 φ 把这个基构成的平行多面体映射成的新平行多面体的体积' 放大的倍数', 这个倍数却不依赖于' 基础体积' 的值. 即，它描述了线性映射 φ 的带符号的' 大小'. 这个大小是不依赖于基的选取的。

练习 4.44. 说明，行列式事实上可以对 $M_n(R)$ 中的矩阵定义，这里 R 是一个交换环。

练习 4.45 (★). 本题中设 $A \in M_n(R)$ 是 *PID* 上的矩阵。

(1) A 是可逆矩阵当且仅当 $\det(A) \in R^\times$ 是单位。
(2) A 定义了一个单射当且仅当 $\det(A) \neq 0$.
(3) $\operatorname{rank} A < n$ 当且仅当 $\det(A) = 0$.

练习 4.46 (★). 设 $\varphi : V \to V$ 是一个 n 维向量空间上的 k-线性映射，A 是它在某一组基下的矩阵，证明下列说法的等价性。

(1) $\operatorname{rank} A = \dim V$.
(2) A 的列能生成 $\dim V$.
(3) $\ker\varphi = 0$, 即 φ 是单射。
(4) $\det\varphi \neq 0$.
(5) 0 不是 φ 的特征值。
(6) $Ax = 0$ 没有非零解。
(7) A 是可逆矩阵，φ 是同构。

练习 4.47 (★★). 设 $\varphi : V \to V$ 是域 k 上 n 维向量空间上的线性映射，定义多项式 $p_\varphi(t) = \det(t1_V - \varphi)$.

(1) $p_\varphi(t)$ 是 φ 的一个相似不变量，它的根都是 φ 的特征值，因此称为 φ 的特征多项式。
(2) 证明 $p_\varphi(t)$ 等于 φ 的所有不变因子的乘积，也即所有初等因子的乘积。
(3) 证明 *Cayley-Hamilton* 定理 $p_\varphi(\varphi) = 0$.

8. 张量积

设 M 和 N 分别是左 A 模和右 A 模，我们可以定义一个阿贝尔群 $M \otimes_A N$，其中的元素都是由形如 $m \otimes n$ 的符号生成的，其 0 元素为 $0 \otimes 0$，并且满足以下三条约束

(1) (系数平衡) $(ma) \otimes n = m \otimes (an)$,
(2) (左线性) $(m + m') \otimes n = m \otimes n + m' \otimes n$,
(3) (右线性) $m \otimes (n + n') = m \otimes n + m \otimes n'$.

即，要求这个符号 $\otimes$ 具有双线性性，并且 A 中的元素可以自由的穿过该符号。严格来说，这个定义是指，$M \otimes_A N$ 是一个由所有符号 $m \otimes n$ 生成的自由 $\mathbb{Z}$ 模，商掉所有形如 $(ma) \otimes n - m \otimes (an), (m + m') \otimes n - m \otimes n - m' \otimes n$ 等关系元素生成的子模。当我们不写出 A 的时候，要么从上下文是明确对哪一个基环取张量积，要么我们是在对 $A = \mathbb{Z}$ 取张量积。由于任何模都是阿贝尔群因此可以视为双边 $\mathbb{Z}$ 模，故 $\otimes_{\mathbb{Z}}$ 总是可以定义出来的。

例 4.7. 设 $M = \mathbb{Z}/2$, $N = \mathbb{Z}/3$ 是两个 $\mathbb{Z}$ 模，那么考虑 $T = M \otimes_{\mathbb{Z}} N = \mathbb{Z}/2 \otimes \mathbb{Z}/3$. 这个群是由所有形如 $\overline{m} \otimes \overline{n}$ 的符号生成的，这里 $\overline{m} \in \mathbb{Z}/2$ 表示整数 m 所在的剩余类。

(1) 当 $\overline{m} = \overline{0}$ 时，$\overline{0} = \overline{0} \cdot 0$ 因此 $\overline{0} \otimes \overline{n} = (\overline{0} \cdot 0) \otimes \overline{n} = \overline{0} \otimes (0 \cdot \overline{n}) = \overline{0} \otimes \overline{0} = 0$, 这个元素是 T 中的 0 元素。
(2) 同理当 $\overline{n} = \overline{0}$ 时，$\overline{m} \otimes \overline{0} = 0$.
(3) 当 $\overline{m} = \overline{1}$ 时，我们有 $\overline{1} = 3 \cdot \overline{1}$，因此 $\overline{1} \otimes \overline{n} = (\overline{1} \cdot 3) \otimes \overline{n} = \overline{1} \otimes (3 \cdot \overline{n}) = \overline{1} \otimes \overline{0} = 0$.

因此在这个例子中，张量积 $(\mathbb{Z}/2) \otimes_{\mathbb{Z}} (\mathbb{Z}/3) = 0$. 事实上对 $(m, n) = 1$ 互素都有 $(\mathbb{Z}/m) \otimes_{\mathbb{Z}} (\mathbb{Z}/n) = 0$.

练习 4.48. 观察上述例子，回答：在 $M \otimes_A N$ 中，$m \otimes n = 0$ 是否等价于 m, n 中有至少一个是 0？

虽然一般来说我们定义出的 $M \otimes_A N$ 只是一个 Abel 群，但类似于 Hom, 当 M 或 N 至少有一个具有双边模的结构时，可以将 $M \otimes_A N$ 赋予模结构。我们来举例说明 ${}_S M_R \otimes_R {}_R N$) 具有左 S 模的结构。这是因为我们可以对,$s \in S$ 定义

$$s(m \otimes n) := (sm) \otimes n.$$

类似的一共有四种情况，我们将所有情况列出如下表格

群	自然的模结构	S 模结构的定义
$M_R \otimes_R N$	$\mathbb{Z}$ 模	none
${}_S M_R \otimes_R N$ $M_R \otimes_{S,R} N$	左 S 模	$s(m \otimes n) := (sm) \otimes n$ $s(m \otimes n) := m \otimes (sn)$
$M_{S,R} \otimes_R N$ $M_R \otimes_R N_S$	右 S 模	$(m \otimes n)s := (ms) \otimes n$ $(m \otimes n)s := m \otimes (ns)$

练习 4.49. 确认你弄明白了表格中的所有情况。

例 4.8. 设 M 是一个左 A 模，同时有一个系数扩张同态 $\rho : A \to B$, 这里你可以把 B 理解为一个更大系数的环，比如 $\mathbb{Q} \to \mathbb{C}$. 那么由于 B 此时可以视作一个左 B 右 A 模，我们可以利用张量积，将 M 的 A 系数扩张为 B 系数，得到一个左 B 模:

$$N = B \otimes_A M$$

这里平衡关系可以理解为 $b \otimes (am) = (b\rho(a)) \otimes m$, 因为 B 的右 A 模结构是由 ρ 给出的。

练习 4.50. 设 M 是一个左 A 模, A 显然是一个双边 A 模, 证明 $A\otimes_A M\cong M$ 是一个左 A 模, 同构于 M.

8.1. 张量积的 Universal Property. 相比于直和或者直积分别代表多个物件指向一个物件, 和一个物件指向多个物件, 张量积的一个重要含义是, 它代表了多线性属性。什么意思呢? 我们说 $B:M\times N\to P$ 是一个 $\mathbb{Z}$-多线性映射, 是指 B 的两个变量都是 $\mathbb{Z}$ 线性的。如果还要求 B 是 A-平衡的, 即 $B(xa,y)=B(x,ay)$, 那么 B 本质上是定义在 $M\otimes_A N$ 上的线性映射。即, 双线性映射不过是一类特殊空间上的线性映射。

定理 4.10 (张量积的 Universal 性质)**.** (1) 设 M,N 是两个 $\mathbb{Z}$ 模, 那么任意一个双线性映射 $B:M\times N\to P$ 都可以分解为映射的复合

$$\begin{array}{ccc} M\times N & & \\ \downarrow{\scriptstyle\varphi} & \searrow{\scriptstyle B} & \\ M\otimes N & \xrightarrow{B'} & P \end{array}$$

其中 $\varphi(m,n)=m\otimes n$ 是一个与 B 无关, 只与 M,N 有关的的典范映射, 也叫 $M\otimes N$ 的结构映射, $B':M\otimes N\to P$ 是一个使上图交换的唯一的映射。

(2) 设 M,N 分别具有右, 左 A 模结构, 那么类似的, 任意一个 A 平衡的 $\mathbb{Z}$ 双线性映射 $B:M\times N\to P$ 都可以唯一的分解为 $B'\circ\varphi:M\times N\to M\otimes_A N\to P$.

Proof. 根据定义, $M\otimes N=F/I$, 这里

$$F=\bigoplus_{(m,n)\in M\times N}\mathbb{Z}(m\otimes n)$$

是所有抽象符号 $m\otimes n$ 生成的自由模, I 则是由所有双线性关系生成的子模,

$$I=\langle (m+m')\otimes n-m\otimes n-m'\otimes n, m\otimes(n+n')-m\otimes n-m\otimes n'\rangle_{m,n}.$$

给定了一个双线性映射 $B:M\times N\to P$ 之后, 我们可以定义一个 $\mathbb{Z}$ 线性映射

$$f\in \mathrm{Hom}_{\mathbb{Z}}(F,P)=\prod_{M\times N}\mathrm{Hom}(\mathbb{Z}(m\otimes n),P)$$

为满足 $m\otimes n\mapsto B(m,n)$ 的唯一映射。其存在性是自由模的性质保证的。由于 B 是双线性的, 显然有 $f(I)=0$(因为 f 在 I 的所有生成元上是 0, 有 $I\subset\ker f$), 因此可以作出商映射 $\overline{f}:F/I\to P:a+I\mapsto f(a)$, 这便是我们需要的 $B':M\otimes N\to P$. 命题的第二部分也是类似的, 只需作简单修改即可。 □

推论 4.3.

$$\mathrm{Hom}_{\mathbb{Z}}(M\otimes_A N,P)=\mathrm{Hom}_{|A}(M,\mathrm{Hom}_{\mathbb{Z}}(N,P))$$

这里左边对应的就是命题中的 B', 右边对应的是 A 平衡双线性映射 $B:M\times N\to P$。

引理 4.3. 如果 V,W 是 k 线性空间, 那么在 $V\otimes_k W$ 中, $v\otimes w=0\Leftrightarrow v=0$ 或 $w=0$.

Proof. ($\Leftarrow$) 为显然, 对于 ($\Rightarrow$), 如果 v,w 都不为 0, 可以构造 k 线性函数 $f:V\to k, g:W\to k$ 使得 $f(v),g(w)\neq 0$. 那么容易验证, $B(x,y):=f(x)g(y)$ 是一个 k 平衡双线性映射, 因此可以分解为 $B=B'\circ\varphi:V\times W\to V\otimes_k W\to k$. 但是 $B(v,w)=f(v)g(w)$ 不为 0, 因此 $\varphi(v,w)=v\otimes w\neq 0$. □

练习 4.51. 将上述命题推广到 M,N 分别是右，左 A 模的情形。这里需要添加适当的假设：M 和 N 满足，任意非零元素都存在 A 线性函数在该元素上不取零。

例 4.9. 设 k 是一个域，V,W 是两个 k 向量空间。显然它们是两个双边 k 模，因此可以定义出 k-线性空间 $V\otimes_k W$. 如果 V,W 分别是由基底 $\{e_i\},\{f_j\}$ 生成的，那么 $V\otimes_k W$ 由基底 $e_i\otimes f_j$ 生成。该基底能生成整个 $V\otimes W$ 是显然的，难点在于说明 $\{e_i\otimes f_j\}\subset V\otimes W$ 线性无关。假设有一个有限和

$$x=\sum a_{ij}e_i\otimes f_j=0$$

那么这表明，对任意 k 平衡双线性映射 $B:V\times W\to k$，都有 $B'(x)=0$. 由于 $(v,w)\mapsto e_i^*(v)f_j^*(w)$ 显然是一个 k 平衡双线性映射，这里 e_i^* 代表在基底 e_i 上取值为 1，其他基底上取值为 0 的唯一线性函数 $e_i^*:V\to k$. 将该函数作用在 x 上我们得到 $a_{ij}=0$，而 i,j 是任意的，因此这表明 x 的所有系数都是 0.

练习 4.52. 说明，$\dim_k(V\otimes_k W)=\dim V\cdot\dim W$.

练习 4.53 (★). (1) 如果有两个线性映射 $f:V'\to V,g:W'\to W$，能否自然的定义出一个线性映射 $f\otimes g:V'\otimes W'\to V\otimes W$？

(2) 设 V',V,W',W 分别有一组基底 e_i',e_i,f_j',f_j，而 f,g 在基底下有矩阵表示 $A=(a_{ij}),B=(b_{ij})$. 求在 $V'\otimes W'$,$V\otimes W$ 自然的基底 $\{e_i'\otimes f_j'\},\{e_i\otimes f_j\}$ 下，$f\otimes g$ 的矩阵表示 $A\otimes B$. 在适当的基底排列顺序下，你应该可以得出如下形式

$$\begin{pmatrix} a_{11}B & \dots & a_{1m'}B \\ \vdots & \vdots & \vdots \\ a_{m1}B & \dots & a_{mm'}B \end{pmatrix}.$$

而如果你把基底的排列换一种方式，你可以得出如下矩阵形式

$$\begin{pmatrix} b_{11}A & \dots & b_{1n'}A \\ \vdots & \vdots & \vdots \\ b_{n1}A & \dots & b_{nn'}A \end{pmatrix}.$$

作为推论，这两个矩阵一定是相似的。通常我们将前者约定为矩阵 $A\otimes B$.

9. 对偶空间

CHAPTER 5

域扩张和伽罗瓦理论

CHAPTER 6

群表示论

本章节需要大家具有线性代数和张量积的基础知识。从某种意义上说，群表示论是线性代数的延伸。想想一个线性空间 V 和其上的一个线性算子 $\sigma : V \to V$, 那么我们可以把 v 自然的作用在 V 上，于是可以得出一系列 $v, \sigma v, \sigma v^2, \ldots$. 如果 σ 还是可逆的，我们相当于可以把 σ^k 这一系列算子都作用在 V 上，不难发现，这本质上可以视作群 $\mathbb{Z}$ 在线性空间 V 上的作用。更一般的我们可以考虑群 G 在 V 上的作用。群的线性表示是指群以线性变换的方式作用在线性空间上，即给出一个群同态 $\rho : G \to \mathrm{GL}(V)$. 或者等价的说，给 F-向量空间 V 一个 FG 模结构 (简称为 G 模)：FG 是由 G 中元素构成的所有线性组合，它们是所有 “算子”，可以自然的作用在 V 上，并且满足对于 $\forall g, h \in G$ 以及 $\forall \lambda, \mu \in F$,

(1) $1v = v$.
(2) $h(gv) = (hg)v$.
(3) $g(\lambda v + \mu w) = \lambda gv + \mu gw$.

1. 基本概念

设 G 是一个群，V 是域 F 上的向量空间。如果有同态

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

则我们称 (V, ρ) 是一个 G 的**F-线性表示**，在不引起混淆时我们直接称 V 或者 ρ 为 G 的一个线性表示。如果 $\dim V < \infty$, 我们说 $\dim V$ 是表示的次数，记作 $\deg \rho$. 我们只涉及有限维的表示。

我们可以定义 $\ker \rho := \{g \in G : \rho(g) = 1_V\}$, 称作表示 ρ 的核。如果 $\ker \rho = \{1\}$ 我们说表示 ρ 是忠实的。

一个表示就是给了 G 在线性空间 V 上的一个 (以可逆线性变换的方式) 作用。V 可以等价的说成一个 G-模。所有 $\rho(g)$ 都是 $V \to V$ 的一个可逆线性变换。

例 6.1. *考虑由 G 的元素张成的线性空间 FG, G 在其上以左乘的方式有一个可逆线性变换的作用 (置换它的基)。这称为 G 的正则表示，记为 (FG, ρ_{reg})*

1.1. 子表示和商表示. 设 V 是一个 G 表示，$U \subset V$ 是一个子空间。我们称 U 是一个**子表示** 如果 $\rho(g)U \subset U (\forall g \in G)$, 也即 U 在 G 的作用下是封闭的。在这种情形下我们还可以给商空间一个自然的作用，获得所谓的商表示

$$g(v + U) := gv + U.$$

如果 U 是 V 的一个子表示, 适当的取 V 的一组基 $v_1, \ldots, v_m, \ldots, v_n$ 使得 $v_1, \ldots, v_m$ 构成 U 的一组基，则用矩阵的语言我们有对所有 $g \in G$,

$$\rho_V(g) = \begin{pmatrix} \rho_U(g) & * \\ & \rho_{V/U}(g) \end{pmatrix}.$$

例 6.2. *正则表示 FG 有一个一维子表示 $U = F(\sum_{g \in G} g)$.*

1.2. 表示的同态. 设 (V_1,ρ_1) 和 (V_2,ρ_2) 是两个表示. 如果有线性映射 $f\in \mathrm{Hom}FV_1,V_2$ 满足 $\rho_2(g)\circ f=f\circ\rho_1(g)$ 即 $gf(v)=f(gv)$, 或者说有如下交换图表

$$\begin{array}{ccc} V_1 & \xrightarrow{f} & V_2 \\ {\scriptstyle \rho_1(g)}\downarrow & & \downarrow{\scriptstyle \rho_2(g)} \\ V_1 & \xrightarrow{f} & V_2 \end{array}$$

则我们称 f 是一个 G 表示的同态，或者说是一个 G 模同态。全体 G-模同态的空间记作 $\mathrm{Hom}GV_1,V_2$.

1.3. 反轭表示. 当 V 是一个 G 表示时, 我们也可以自然地把 $V^*=\mathrm{Hom}FV,F$ 看成一个 G 表示

$$\left(\rho^*(g)f\right)(v):=f(g^{-1}v)$$

我们把这个表示称作 V 的**反轭表示**。在选取了 V 的一组基 B，以及 V^* 的一组对偶基 B^* 之后，我们有

$$\rho^*_{B^*}(g)=\left(\rho_B(g)^T\right)^{-1}.$$

读者可能会奇怪，为何反轭表示里，$gf(v)$ 定义为 $f(g^{-1}v)$ 而不是 $f(gv)$? 这是因为群的作用需要满足结合律，也即需要满足

$$(gh)f=g(hf).$$

但是注意到映射 f 的合成会把乘法的顺序反过来

$$g(hf)=g(f(h^{-1}\cdot))=f(h^{-1}g^{-1}\cdot)=f((gh)^{-1}\cdot)$$

因此需要引入逆将乘法的顺序再反过来，这是唯一合理的定义。

1.4. 张量积表示. 对于给定的两个表示 V 和 U, 我们可以在张量积空间 $V\otimes U$ 上定义一个自然的作用使其成为一个 G 表示

$$\begin{aligned}\rho_V\otimes\rho_U:G&\to \mathrm{GL}(V\otimes U)\\ g&\mapsto \rho_V(g)\otimes\rho_U(g).\end{aligned}$$

称之为张量积表示。通过张量积表示，我们可以将空间 $\mathrm{Hom}FV,U$ 自然地视作一个 G 模。这是因为，$\mathrm{Hom}FV,U$ 可以自然的视作 $V^*\otimes_F U$，于是在其上的张量积表示可以给出

$$(gf)(v):=g(f(g^{-1}v)).$$

在这个定义下，$\mathrm{Hom}GV,U$ 成为 $\mathrm{Hom}FV,U$ 的子表示。

命题 6.1. 我们有如下 G 模同构

$$V^*\otimes U\cong_{FG}\mathrm{Hom}FV,U.$$

Proof. 取 U 的一组基 u_i 以及 V 的一组基 v_i 和对偶基 v^i, 考虑从 $\mathrm{Hom}FV,U$ 到 $V^*\otimes U$ 的一个对应

$$f\mapsto\sum_{i,j}v^i(f(u_j))\cdot v^i\otimes u_j.$$

容易看出这是线性空间的同构。由定义知它们在 G 的作用下是相同的。 □

1.5. 表示的直和. 我们可以将两个表示 V_1 和 V_2 直和起来，得到一个新的 G 表示 $V_1 \oplus V_2$

$$\begin{aligned} \rho_1 \oplus \rho_2 : G &\to \mathrm{GL}(V_1 \oplus V_2) \\ g &\mapsto \rho_1(g) \oplus \rho_2(g). \end{aligned}$$

也即

$$g(v_1, v_2) = (gv_1, gv_2).$$

从矩阵的观点来看，令 B_i 是 V_i 的一组基，则我们有

$$\rho_V(g) = \begin{pmatrix} \rho_{V_1}(g) & & \\ & \cdots & \\ & & \rho_{V_n}(g) \end{pmatrix}.$$

1.6. 表示的外张量积. 给了一个 G_1 的表示和 G_2 的表示之后，我们可以构造一个 $G_1 \times G_2$ 的表示

$$\begin{aligned} \rho_1 \# \rho_2 : G_1 \times G_1 &\to \mathrm{GL}(V_1 \otimes V_2) \\ (g_1, g_2) &\mapsto \rho_1(g_1) \otimes \rho_2(g_2) \end{aligned}$$

称作表示 ρ_1 和 ρ_2 的外张量积。

2. 不可约表示

我们现在将要研究将表示拆分成一些更小的表示，以及无法再分解的基本的表示：不可约表示。一个表示 V 叫做**不可约** 如果它没有非平凡的子表示。叫做**不可分解**，如果它不能分解成两个非平凡的子表示的直和。显然不可约模一定是不可分解的。我们称一个表示是完全可约的，如果它能分解成不可约模的直和。显然我们讨论的有限维表示都可以分解为不可分解表示的直和，但不可分解模不一定是不可约模。但是，我们将证明，对于 $\mathrm{char}F \nmid |G|$ 的情形，有限维表示都是完全可约的。

我们今后将完全限于 $\mathrm{char}F \nmid |G|$ 的情形 (称之为常表示论)，读者完全可以假设 $F = \mathbb{C}$ 而不失任何关键信息。$\mathrm{char}F \| |G|$ 的情形非常复杂，属于模表示论的范畴。

引理 6.1. *设 $f : V \to U$ 是 G-模同态，则 $\ker f \subset V$ 和 $\mathrm{Im}f \subset U$ 都是子表示。*

Proof. 若 $v \in \ker f$ 则有 $f(gv) = gf(v) = 0$, 因此 $gv \in \ker f$, 即 $\ker f$ 是 V 的子表示。类似可证 $\mathrm{Im}f$. □

下面的引理是简单而重要的：两个不同构的不可约表示之间没有非平凡的同态。

引理 6.2 (Schur)**.** *设 V_1 和 V_2 是两个 G 表示，则有*

(1) *若 f 是任一个非平凡 G-模映射，那么 f 只能是同构。因此，若 $\rho_1 \ncong \rho_2$，则 $\mathrm{Hom}GV_1, V_2 = 0$.*
(2) *$\mathrm{Hom}GV_1, V_1$ 是一个包含 F 的除环.*
(3) *若 F 是代数闭域, 那么 $\mathrm{Hom}GV_1, V_1 \cong F1_{V_1} \cong F$.*

Proof. 若 f 是一个 G-模映射，$W = \ker f$ 是 V_1 的子表示，由于 V_1 是不可约的，必然有 $W = V_1$ 或者 $W = 0$. 若假设 f 非平凡，必有 $W = 0$ 从而 f 是单射。同理我们必有 $\mathrm{Im}f = V_2$, 故 f 也是满射，因此是一个同构。

对于第二个命题，只需注意到 $\mathrm{Hom}GV_1, V_1$ 中的任意非零元素都是同构因而是可逆的。

最后，如果 F 是代数闭域，我们可以考虑 f 的特征值 λ 和特征向量 v. 注意到由 Gv 张成的空间构成 V_1 的子表示，故它等于 V_1. 因此任何 $x \in V$ 可以写成

$$x = \sum_{g \in G} x_g gv, \quad x_g \in F.$$

必然有

$$f(x) = \sum_{g\in G} x_g g\lambda v = \lambda x.$$

这表明 $f = \lambda 1_{V_1}$. □

2.1. Maschke 定理. 我们即将开始看到 $\mathrm{char}F \nmid |G|$ 起到什么样的作用。Maschke 定理描述了在这种情形下，每个子表示都有直和补表示，这将表明不可分解模是不可约的，从而我们研究的有限维表示都可以分解为不可约表示的直和。

定理 6.1 (Maschke)**.** *令 V 是一个 F-表示, $\mathrm{char}F \nmid |G|$，那么 V 的任意子表示 U 都有直和补表示。*

Proof. 我们首先可以找到 U 的一个补空间 (不要求该补空间是子表示)，设 $V = U \oplus W$，考虑 $p : V \to U$ 是该直和分解附带的投射，我们只需证明存在一个 G-模投射 $p' : V \to U$，这样的话 $V = U \oplus \ker p'$，而 $\ker p'$ 则自动是子表示。

做法是考虑 p 的平均化：

$$\begin{aligned} p' : V &\to U \\ v &\mapsto \frac{1}{|G|}\sum_{g\in G} g^{-1}p(gv). \end{aligned}$$

容易验证它确实是 G-模同态

$$p'(gv) = \frac{1}{|G|}\sum_{h\in G} h^{-1}p(hgv) = \frac{1}{|G|}\sum_{h\in G} (hg^{-1})^{-1}p((hg^{-1})gv) = gp'(v).$$

□

2.2. 正则表示的分解. 正则表示 FG 具有基本的重要性，因为每个不可约表示都是 FG 的直和项。这是因为，如果我们把 FG 分解成某些不可约表示的直和

$$FG = \bigoplus_{i=1}^{m} V_i^{\oplus n_i}$$

设 V 是任意一个不可约表示，则有

$$\mathrm{Hom}GFG, V = \bigoplus_{i=1}^{m} \mathrm{Hom}GV_i, V^{\oplus n_i}.$$

于是由 Schur 引理，若 V 没有出现在 FG 的分解中，上述空间 $= 0$. 如果 $V = V_j$, 则 $n_j \dim \mathrm{Hom}GV_j, V_j = \mathrm{Hom}GFG, V$. 但是我们知道，可以实际的计算空间 $\mathrm{Hom}GFG, V$. 事实上，其中的元素 $f \in \mathrm{Hom}GFG, V$ 完全由 $f(1) \in V$ 值所决定，反过来任给一个 $v \in V$ 可以作出映射 f 使得 $f(1) = v$. 于是有线性空间的同构

$$\begin{aligned} \varphi : \mathrm{Hom}GFG, V &\to V \\ f &\mapsto f(1). \end{aligned}$$

于是我们得出如下重要命题

定理 6.2 (正则表示的分解)**.** *任何不可约表示都是正则表示 FG 的直和项。如果 If $V_1, \ldots, V_k$ 是所有的互不同构的不可约表示，那么*

$$FG \cong \bigoplus_{i=1}^{k} V_i^{\oplus d_i}.$$

其中

$$d_i = \frac{\dim V_i}{\dim \mathrm{Hom}GV_i, V_i}.$$

特别的，如果 $F = \mathbb{C}$, $d_i = \dim V_i$.

Proof. 考虑

$$V_i = \mathrm{Hom}GFG, V_i = \mathrm{Hom}GV_i, {V_i}^{\oplus d_i}.$$

计算两边的维数即得结论。 □

推论 6.1. 设 $F = \mathbb{C}$，并且 $n_1, n_2 \ldots, n_k$ 是所有不可约表示的次数，那么我们有 $|G| = n_1^2 + \cdots + n_k^2$.

3. 特征标理论

特征表理论是群表示论的核心部分之一：它是表示的重要不变量。给定一个表示 (V, ρ)，我们可以联系一个表示的特征标 $\chi = \chi_\rho : G \to F$，定义为 g 作为线性变换的迹

$$\begin{aligned} \chi_\rho : G &\to F \\ g &\mapsto \mathrm{tr}\rho(g). \end{aligned}$$

引理 6.3. 设 $F = \mathbb{C}$, 则 $\rho(g) : V \to V$ 作为矩阵是可对角化的，并且其特征值都是单位根。

Proof. 这是因为 $g \in G$ 有阶数 $g^n = 1$, 这表明 $\rho(g)^n = 1$，满足该方程的矩阵必然是可对角化的，并且特征值为 n 的单位根。 □

命题 6.2 (特征标的基本性质)**.** 特征标 χ_ρ 具有如下基本性质

(1) $\chi(1) = \deg \rho$
(2) $\chi(ghg^{-1}) = \chi(h)$
(3) 设 $F = \mathbb{C}$, 则 $\chi(s^{-1}) = \overline{\chi(s)}$.

Proof. 由于 $1 \in G$ 的作用必然是恒等作用，它的迹当然是 V 的维数。第二条是由于矩阵的相似不改变迹。第三条是因为 $\rho(s^{-1})$ 与 $\rho(s)$ 互为逆矩阵，故它们对应的特征值之和分别为 $\sum \lambda_i$ 和 $\sum \lambda_i^{-1} = \sum \overline{\lambda_i}$. 这里用到了 $|\lambda_i| = 1$. □

3.1. Properties. The sum, or product, of two characters of G, is still a character of G, since the sum is the character of the direct sum of the two representations, and the product is the character of the tensor product of the two representations.

3.2. Orthogonal Relations. If $\mathrm{char}F \nmid |G|$, for two F-valued functions χ_1, χ_2 on G, define

$$(\chi_1, \chi_2) := \frac{1}{|G|} \sum_{g \in G} \chi_1(g)\chi_2(g^{-1}).$$

We have the following

定理 6.3 (First Orthogonal Relation)**.** $\mathrm{char}F \nmid |G|$, *if* χ_1 *and* χ_2 *are characters of two irreducible* F *representations* V_1, V_2 *of* G, *then*

$$(\chi_1, \chi_2) = \begin{cases} 0, & \rho_1 \ncong \rho_2 \\ \dim(\mathrm{Hom}GV_1, V_1)1_F, & \rho_1 \cong \rho_2 \end{cases}$$

引理 6.4. $\mathrm{char}F \not| |G|$, *let* χ *be the character of an* F*-representation* V, χ' *be the character of the sub* F*-representation* $\mathrm{Inv}_G(V) = \{v | gv = v, \forall g \in G\}$. *Then*

$$\frac{1}{|G|}\sum_{g\in G}\chi(g) = \frac{1}{|G|}\sum_{g\in G}\chi'(g).$$

Proof.

$$\frac{1}{|G|}\sum_{g\in G}\chi(g) = \mathrm{tr}\left(\frac{1}{|G|}\sum_{g\in G}\rho(g)\right) = \mathrm{tr}z$$

where z is a linear map indicated by the context. Note that $gz = zg = z$ therefore z is an G-module map and $z^2 = z$. □

Proof of the theorem.

$$\begin{aligned}
\frac{1}{|G|}\sum_{g\in G}\chi_{V_1}(g)\overline{\chi_{V_2}(g)} &= \frac{1}{|G|}\sum_{g\in G}\chi_{V_1}(g)\chi_{V_2^*}(g)\\
&= \frac{1}{|G|}\sum_{g\in G}\chi_{V_1\otimes V_2^*}(g)\\
&= \frac{1}{|G|}\sum_{g\in G}\chi_{\mathrm{Hom}FV_2,V_1}(g)\\
&= \frac{1}{|G|}\sum_{g\in G}\chi_{\mathrm{Inv}_G(\mathrm{Hom}FV_2,V_1)}(g)\\
&= \frac{1}{|G|}\sum_{g\in G}\chi_{\mathrm{Hom}GV_2,V_1}(g)\\
&= \begin{cases} (\dim \mathrm{Hom}GV_1, V_1)1_F & \rho_1 \cong \rho_2\\ 0 & \rho_1 \ncong \rho_2. \end{cases}
\end{aligned}$$

□

推论 6.2. *If* $V \cong n_1V_1 \oplus \cdots \oplus n_kV_k$, *where* $V_1, \ldots, V_k$ *are distinct irreducible representations, then*

$$(\chi, \chi_i) = n_i \dim \mathrm{Hom}GV_i, V_i.$$

If $\mathrm{char}F = 0$ *and* F *is the splitting field of* G, *then* $(\chi, \chi) = 1$ *if and only if* V *is irreducible.*

The first orthogonal relation can also be stated as follows

$$\frac{1}{|G|}\sum_{t=1}^{s} h_t\chi_i(g_t)\chi_j(g_t^{-1}) = \delta_{ij}\dim \mathrm{Hom}GV_i, V_i$$

where $\{g_1, \ldots, g_s\}$ is a set of representatives of the s conjugate classes of G. $h_1, \ldots, h_s$ are the sizes of each conjugate class. In particular, if $F = \mathbb{C}$ and denote $\chi_{ij} = \chi_i g_j$, one has

$$\frac{1}{|G|}\sum_{t=1}^{s} h_t\chi_{it}\overline{\chi_{jt}} = \delta_{ij}$$

using matrix notations, this is

$$X H \overline{X}^T = |G| I$$

where $X = (\chi_{ij}), H = \mathrm{diag}\{h_1, \ldots, h_s\}$. It is easy to see that we have

$$\overline{X}^T X = |G| H^{-1}$$

or written explicitly

$$\sum_{t=1}^{s} \overline{\chi_{ti}} \chi_{tj} = \frac{|G|}{h_i} \delta_{ij} = |C_G(g_i)| \, \delta_{ij}$$

this is called the second orthogonal relation or column orthogonal relation.

3.3. 置换特征标. Let $G \leq S_n$ acts on $\{x_1, \ldots, x_n\}$, we obtain easily a representation of G on

$$V = \langle x_1, \ldots, x_n \rangle_F$$

thus $|\mathrm{Fix}(g)| = \mathrm{tr}\rho(g)$ is a character. Since

$$U = F(x_1 + \cdots + x_n) = Fz$$

is a subrepresentation or a sub-FG-module of V, one can construct the quotient representation V/U, and obviously

$$\chi_\rho = \chi_U + \chi_{V/U} = 1 + \chi_{V/U}.$$

Which gives another useful character χ of G

$$\chi = |\mathrm{Fix}(g)| - 1.$$

21

3.4. Tensor Product.

$$V \otimes V \cong \mathrm{Sym}^2(V) \oplus \mathrm{Alt}^2(V)$$

$$\chi^2 = \chi_S + \chi_A$$

$$\chi_S = \frac{1}{2}\left(\chi^2(g) + \chi(g^2)\right)$$

$$\chi_A = \frac{1}{2}\left(\chi^2(g) - \chi(g^2)\right)$$

3.5. Powers of Irreducible Character.

定理 6.4. *Let χ be an irreducible character taking r different values. Then any irreducible character is a component of one of the r characters $1, \chi, \chi^2, \ldots, \chi^{r-1}$.*

3.6. Character Table : Examples. We give some examples of calculating the character table of a given group G.

例 6.3. *To calculate the character table of S_3, first note that it is easy to obtain the character table of S_2*

S_2	1	1
	(1)	(12)
χ_1	1	1
χ_2	1	-1

then, via the homomorphism

$$\sigma : S_3 \to S_3/A_3 \cong S_2$$

we lift two characters of S_2 to characters of S_3

S_3	1	3	2
	(1)	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	n_3	a	b

since $6 = 1^2 + 1^2 + 2^2$*, we have* $n_3 = 2$*. Moreover by the second orthogonal relation we have*

$$1 \times 1 + 1 \times (-1) + 2a = 0$$
$$1 \times 1 + 1 \times 1 + 2b = 0$$

therefore $a = 0, b = -1$*. Thus*

S_3	1	3	2
	(1)	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

例 6.4. *We wish to calculate the* $\mathbb{C}$ *character table of* A_5*, which does not have a nontrivial normal subgroup. First we identify the conjugate classes of* A_5*. Note that*

$$[A_5 : C_{A_5}(g)] = [S_5 : C_{S_5}(g)] \frac{[C_{S_5}(g) : C_{A_5}(g)]}{[S_5 : A_5]}$$

the quotient $\frac{[C_{S_5}(g):C_{A_5}(g)]}{[S_5:A_5]}$ *is either* $\frac{1}{2}$ *or* 1 *depending on whether* $C_{S_5}(g) \subset A_5$*.*

3.7. Integrality.

引理 6.5. *Let* $g \in G$ *is an element of order* m*, then* $\chi(g)$ *is a sum of* $\deg \rho$ m*-th root of units. In particular, this is true for all* g *if* m *is the l.c.m. of all orders of elements in* G*.*

Proof. If $g^m = 1$, then $\rho(g)^m = 1$, the eigenvalues of $\rho(g)$ will all be m-th unit roots. □

推论 6.3. *Let* χ *be a complex character, then* $\chi(g)$ *is an algebraic integer.*

推论 6.4. $|\chi_\rho(g)| \leq \chi_\rho(1)$*, with equality holds if and only if* $\rho = \omega 1_V$*.*

Proof. Under certain basis, $\rho(g)$ will be a diagonal matrix, whose diagonal elements are m-th unit roots. Therefore

$$|\chi_\rho(g)| = |\omega_1 + \cdots + \omega_n| \leq \chi_\rho(1)$$

with equality holds if and only if $\omega_1 = \cdots = \omega_n$, in which case $\rho(g) = \omega 1_V$. □

定理 6.5. *Let* χ *be an irreducible complex character, then*

$$\frac{[G : C_G(g)]\chi(g)}{\chi(1)}$$

is an algebraic integer.

Proof. Let $\phi = \sum_{h \in C_g} \rho(h)$ be a linear transform from V to V. Clearly it is also a G-module map. Now Schur's Lemma gives $\phi = \lambda 1_V$. Taking tr we have

$$\mathrm{tr}\phi = \lambda\chi(1) = \sum_{h \in C_g} \chi(g) = [G : C_G(g)]\chi(g)$$

thus

$$\lambda = \frac{[G : C_G(g)]\chi(g)}{\chi(1)}.$$

Now, to show that λ is an algebraic integer, note that ϕ is the restriction of $\psi = \sum \rho_{\mathrm{reg}}(h)$ on V. An eigenvalue of ϕ will also be the eigenvalue of ψ. Since λ is the eigenvalue of ϕ, it is the root of the polynomial $\det(\lambda I - M)$ with M being the matrix of ψ which is an polynomial of integral coefficients. □

推论 6.5. *$\chi(1)$ must be a divisor of $|G|$.*

Proof.

$$\frac{|G|}{\chi(1)} = \sum_{g\in G} \frac{1}{\chi(1)}\chi(g)\overline{\chi(g)} = \sum_{i=1}^{s} \frac{[G : C_G(g)]\chi(g_i)}{\chi(1)}\overline{\chi(g_i)}$$

which is an algebraic integer and also a rational, which must be an integer. □

3.8. Burnside's Theorem.

引理 6.6. *Let α be a sum of n unit roots, with $\frac{\alpha}{n}$ being an algebraic integer. Then $\alpha = 0$ or $\frac{\alpha}{n}$ is a unit root.*

Proof. Let $f(x)$ be the minimal polynomial for $\beta_1 = \alpha/n$ over $\mathbb{Q}$, $\beta_2, \ldots, \beta_k$ be its conjugates. The Galois group $\mathrm{Gal}(f)$ acts transitively on them, let $\sigma_i \in \mathrm{Gal}(f)$ be the one such that $\sigma_i(\beta_1) = \beta_i$. The number

$$c = \prod \beta_i \in \mathbb{Q}$$

is also an algebraic integer since σ_i permutes the roots of f, we conclude that c is an integer. Now we wishes to prove that $|\beta_i| = 1$, to do so, note that $|\beta_1| \leq 1$. In order to establish similar inequalities for each i, one needs to consider the field $\mathbb{Q}(\epsilon)$, where F is the splitting field for f and ϵ is some unit root such that $\alpha \in \mathbb{Q}(\epsilon)$. Since $\mathbb{Q}(\epsilon)/\mathbb{Q}$ is normal, $F \subset \mathbb{Q}(\epsilon)$, $\mathbb{Q}(\epsilon)$ is actually a splitting field for $x^m - 1$ over F. We extend every σ_i to an automorphism of $\mathbb{Q}(\epsilon)$, which sends unit roots in $\mathbb{Q}(\epsilon)$ to unit roots in it. Therefore we have $|\beta_i| \leq 1$ for each i, consequently $|c| \leq 1$ and so $|c| = 1 = |\beta_i|$. □

4. 诱导表示

我们通常希望用更小的群的表示来描述一个群 G 的表示。这方面，最简单的考虑是所谓膨胀 (Inflation).

4.1. 膨胀. 当 $N \lhd G$，我们可以通过投射 $G \to G/N$ 将 G/N 的表示拉回为 G 的表示：

$$G \to G/N \to \mathrm{GL}(V).$$

这个操作称为膨胀

$$\inf : \mathrm{Rep}(G/N) \to \mathrm{Rep}(N)$$

并且我们有 inf 是一个忠实函子。这是一个常用的获得较为简单的 G 表示的手段。

4.2. 限制. 当有子群 $H \leq G$ 时，我们可以将 G 的一个表示 V 直接视为 H 的表示，即通过合成

$$H \to G \to \mathrm{GL}(V)$$

定义 H 的作用。这个操作称作限制 (Restriction)

$$\mathrm{Res}^G_H : \mathrm{Rep}(G) \to \mathrm{Rep}(H).$$

从特征标的角度来看，限制不改变特征标：只需将 χ 限制在子群 $H \leq G$ 上取值即可。

4.3. 诱导表示. 诱导这个操作则是要从 H 的表示 V 构造出一个 G 的表示来，也即把 H 模 V 变为一个 G 模。这个构造比限制要复杂，但是想法是简单的：利用双边 G 模 FG 和我们的胶水：张量积，我们将为 V 配上一个 G 系数，考虑如下的张量积

$$V' = \mathrm{Ind}^G_H(V) = FG \otimes_{FH} V$$

则 V' 由于 FG 可视为左 G 右 H 模的结构，具有 G 的左乘作用

$$g(g_0 \otimes_H v) := (gg_0) \otimes_H v$$

V' 于是成为一个 G 表示。可以这样来想象 $\mathrm{Ind}^G_H V$, 我们取一组陪集代表元 G/H, 那么