抽象代数入门

咕咕嘎嘎

目录

第 1 章 群环域模初识

内容提要

- 群环域模的定义
- 同构
- 子结构

1.1 群环域模的基本结构

1.1.1 群

群是一种最基本的代数结构，它只规定了对象和对象间的运算及运算法则. 群是一个非空集合 G 和在上面定义的运算的整体 $(G,\cdot)$.

定义 1.1 (群)

G 是非空集合，$e\in G$ 并且 G 上配有乘法：

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

满足如下性质

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

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

笔记 群的运算 (这里姑且称其为乘法) 要求满足结合律、有乘法单位元 (identity)，逆元 (inverse). 其中并不要求所有群中的元素都是可交换的，而只是要求单位元、逆元可交换 (事实上存在更普遍的群结构，使得这里的条件可以再减弱至只有左或者右元存在).

群的乘法单位元和逆元都是唯一的. 事实上，设有单位元 ee_1,e_2, 则有 $e_1\cdot e_2=e_1=e_2$. 另一方面，设 a 有逆元 s,t, 则 $s\cdot a\cdot s=s\cdot a\cdot t=s=t$.

群上定义的乘法是 $G\times G\to G$ 的映射.

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

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

若对任意 $g_1,g_2\in G$，$g_1\cdot g_2=g_2\cdot g_1$，就称 $(G,\cdot)$ 是**交换群**或 **Abel 群**。若 $|G|$ 有限 (集合 G 的元素个数有限)，就称 G 是**有限群**并把 $|G|$ 称作是群的**阶**；否则称 G 为**无限群**。

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

定义 1.2 (循环群)

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

例题 1.1 令 $G=\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C},g_1,g_2\in G$，定义 $g_1\cdot g_2=g_1+g_2$，其中 $+$ 是 G 自然的加法运算。那么，G 是交换群，0 是单位元。

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

例题 1.2 域上的一般线性群 K 是域，$G=\mathbf{GL}(n;K)$ 是 K 上 $n\times n$ 可逆矩阵的集合，令 $\cdot$ 为矩阵的乘法，e 为单位矩阵，$\mathbf{GL}(n;K)$ 是群（被称为**一般线性群**）。如果 $n\geqslant 2$，$\mathbf{GL}(n;K)$ 不是交换群。

例题 1.3 二面体群 二面体群 $\mathfrak{D}_n$, 详情参照讲义.

对称群具有重要的地位. 在本章后续部分会讨论对称群的构成.

定义 1.3 (集合的对称群)

X 是集合，$X \neq \emptyset$，$\mathfrak{S}_X$ 为 X 到自身的双射的集合。对任意 $g_1, g_2 \in \mathfrak{S}_X$，令 $g_1 \cdot g_2$ 为 g_1 与 g_2 的复合，即

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

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

定义 1.4 (子群)

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

笔记 在子群上使用群的乘法，子群也是群. 因为子群 H 满足结合律 (继承于 G 的结合律)，有逆元 (子群定义)，有单位元 ($h \cdot h^{-1} = 1$, 子群对取逆、乘法封闭).

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

例题 1.4 $\mathbb{C}^\times$ 为全体非零复数，其群乘法为复数的乘法，这是群。尽管 $\mathbb{C}^\times \subset \mathbb{C}$, 但是 $(\mathbb{C}^\times, \cdot)$ 不是 $(\mathbb{C}, +)$ 的子群. 因为两个群定义的乘法不同.

命题 1.1 (由子集生成的子群)

G 是群。

1. 假设 $\{G_i\}_{i \in I}$ 是 G 的一族子群，那么，$\bigcap_{i \in I} G_i$ 是子群。
2. 子集 $S \subset G$ 并且 $S \neq \emptyset$，根据上述，存在唯一的、包含 S 的、最小的（在包含关系下）子群，它被称作是由 S **生成的子群**并记作 $\langle S \rangle$。实际上，$\langle S \rangle$ 是包含 S 的所有子群之交 (类比集生成的 σ 代数)。
3. $S \subset G$，那么，$\langle S \rangle$ 具有如下描述：

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

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

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

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

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

我们还有

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

这表明 $\langle S \rangle$ 对取逆封闭。

换句话说，由子集 S 生成的子群是由 S 中元素构成的群乘法组合.

命题 1.2 (有限阶)

当 $S = \{g\}$ 只有一个元素时，记它生成的子群为 $\langle g \rangle$。很明显，$\langle g \rangle$ 是循环群并且

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

若有正整数 n，使得 $g^n = 1$，就称 g 是**有限阶的元**（否则称之为**无限阶的元**）并用 $\mathrm{ord}(g)$ 来记最小的这

种整数且称之为g **的阶**。此时，$\langle g\rangle$ 是有限循环群并且 $|\langle g\rangle| = n$。

我们注意到

- 若 g 是有限阶的元，$k,l \in \mathbb{Z}$，则 $g^k = g^l$ 当且仅当 $\mathrm{ord}(g) \mid k-l$。而这就给出了一个等价类，对 m 模同余等价类是一个例子.
- G 是有限群，则所有 $g \in G$ 均为有限阶的。

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

定义 1.5 (中心化子、群的中心)

G 是群，$g \in G$，定义 g 的**中心化子**：

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

这是子群，由群中与 g 交换的元素构成。

容易证明中心化子中的元素对乘法封闭：设 $h_1, h_2 \in \mathrm{C}_g(G)$, 则 $gh_1h_2 = h_1gh_2 = h_1h_2g$.

同时可以证明对取逆封闭：由于 $gh = hg$, 因此两边同时取逆：$h^{-1}g^{-1} = g^{-1}h^{-1}$, 而 $g^{-1} = g' \in G$, 因此 $g'h^{-1} = h^{-1}g', h^{-1} \in \mathrm{C}_g(G)$.

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

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

1.1.2 环

环比群复杂的地方在于，环上定义了两种运算，且乘法没有群的乘法性质良好：环并不要求元素有逆，而是规定了乘法分配律.

定义 1.6 (环)

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

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

和

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

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

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

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

就称 $(A, \cdot, +)$ 或 A 是一个**环**。

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

定义 1.7 (逆)

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

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

用 $A^\times$ 表示环 A 中有逆的元素（即有左逆又有右逆）的元素的集合。增强了环的乘法没有要求存在逆的条件，这让 $(A^\times,\cdot)$ 成为群。

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

例题 1.5 A 是环，$\mathbf{M}_n(A)$ 是环 A 上 $n\times n$ 的矩阵的集合。注意到，矩阵的乘法和加法只用到了分量上的乘法和加法并且不使用乘法的逆或者交换律，所以，在矩阵的加法和乘法下，$\mathbf{M}_n(A)$ 是环，其单位矩阵和零矩阵对应着 $1_{\mathbf{M}_n(A)}$ 和 $0_{\mathbf{M}_n(A)}$。

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

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

对于交换环 A，我们仍然可以定义行列式：

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

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

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

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

例题 1.6 多项式环 A 是环，$A[X]$ 是 A 上以 X 为不定元的多项式的集合，即每个 $P\in A[X]$ 均形如

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

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

另外，我们强调多项式不是多项式函数。

我们有如下简单的性质：

a) 若 A 是交换环，则 $A[X]$ 也是交换环。

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

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

例题 1.7 K-代数 K 是域，A 是环并且是 K-线性空间，如果对任意的 $x,y\in A$ 和 $k\in K$，我们有

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

就称 A 是K**-代数**。

我们有如下三类重要的例子：

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

$$x\cdot y=\sum_{g\in G}\sum_{h\in G}x_gy_he_{gh}.$$

这是一个 K-代数，它的乘法记录了群 G 的乘法。

定义 1.8 (子环)

A 是环，$B\subset A$ 为其加法群的子群。如果 $1_A\in B$ 并且 B 对乘法封闭，即对任意 $a,b\in B$，$a\cdot b\in B$，就称 B 是 A 的**子环**。

使用环 A 的加法和乘法，子环 B 具有自然的环结构。

1.1.3 域

域上也配置了两种运算，但是具有良好性质.

定义 1.9 (域)

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

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

和

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

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

1. $(K,+)$ 是交换群.
2. $(K,\cdot)$ 是交换群.
3. 乘法和加法满足乘法分配律：对任意的 $a_1,a_2,a_3 \in K$，有

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

就称 $(K,\cdot,+)$ 或 K 是一个**域**。

例题 1.8 p 是素数。我们用 $\mathbb{Z}/p\mathbb{Z}$ 表示整数集除 p 的同余类，即

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

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

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

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

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

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

1.1.4 模

和前几种代数结构不同，模是两个不同集合生成的映射. 模可以被视作是环上的线性空间：

定义 1.10 (模)

A 是环，$(M,+)$ 是交换群。如果存在映射

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

使得对任意 $a,a' \in A, m,m' \in M$，有

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

就称 $(M,+)$ 或 M 是 **(左)A-模**。

定义 1.11 (子模)

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

例题 1.9 K 是域，则 K-模是 K-线性空间。

例题 1.10 K 是域，$A=K[X]$ 为 K 上的多项式环，V 是 K-线性空间。给定线性映射 $T\in \mathrm{End}_K(V)$，这定义出 V 上的 $K[X]$-模的结构：

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

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

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

很显然，我们有

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

这是最重要的一类 $K[X]$-模（由线性映射 T 决定）。

1.2 同态

1.2.1 群同态

定义 1.12 (群同态)

$(G_1,\cdot_1)$ 和 $(G_2,\cdot_2)$ 是群，$\varphi\colon G_1\to G_2$ 是映射。如果 φ 将 G_1 中的乘法保持到 G_2 上，即对任意 $g,h\in G_1$，有

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

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

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

笔记 在群同构之前，群中的元素存在一一对应 (集合的同构：对称群). 进一步地，群同构保持了群之间的乘法结构.

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

这就是说，群同态保留了单位元.

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

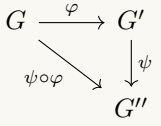
假设 G_1 和 G_2 均为 $(\mathbb{C}^\times,+)$，对任意的 $\lambda\in\mathbb{C}^\times$，映射 $z\mapsto\lambda\cdot z$ 均为 G_1 到 G_2 的同构。

命题 1.3 (同态的复合)

群同态的复合仍为群同态，即有映射

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

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



♠

定义 1.13 (自同构)

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

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

♣

研究映射的一个必不可缺的话题就是映射的核与像.

定义 1.14 (群同态的像与核)

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

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

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

注意到 φ 是单射当且仅当 $\mathrm{Ker}(\varphi) = \{1\}(\varphi(x) = 1 \Rightarrow x = 1)$；$\varphi$ 是满射当且仅当 $\mathrm{Im}(\varphi) = G_2$。在群论中常用的一个结论是为说明 φ 是单射只要验证 $1 \in G_2$ 的原像唯一。

实际上，如果 $\mathrm{Ker}(\varphi) = \{1\}$，假设 $g, h \in G_2$ 使得 $\varphi(g) = \varphi(h)$，那么，$\varphi(gh^{-1}) = \varphi(g)\varphi(h)^{-1} = 1$，即 $gh^{-1} \in \mathrm{Ker}(\varphi)$。这表明 $gh^{-1} = 1$，即 $g = h$。所以，φ 是单射。

♣

例题 1.11 G 是群，$g \in G$，则映射

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

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

定义 1.15 (共轭映射)

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

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

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

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

对任意 $h, g_1, g_2 \in G$，我们有

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

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

♣

1.2.2 环同态

同态是相对于运算而言的，因此环同态具有两个因子：乘法和加法.

定义 1.16 (环同态)

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

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

并且 $\varphi(1_{A_1})=1_{A_2}$，就称 φ 是从 A_1 到 A_2 的**环同态**。我们用 $\mathrm{Hom}(A_1,A_2)$ 表示从 A_1 到 A_2 的环同态的集合。如果环同态 φ 是双射，就称 φ 是从 A_1 到 A_2 的一个**环同构**；如果 A_1 与 A_2 之间存在环同构，就称这两个环是**同构的**并记作是 $A_1\simeq A_2$。

笔记 和群同态一样，环同态保持了乘法单位元.

给定从 A_1 到 A_2 的环同构 φ，它的逆

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

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

定义 1.17 (核)

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

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

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

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

笔记 应该注意，环同态的核把环内的元素映为加法单位元 0_{A_2}.

引理 1.1

K 是域，A 是环，$\varphi\colon K\to A$ 是环同态，则 φ 是单射。

证明 实际上，对任意 $k\in K^\times$，有

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

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

1.2.3 模同态

命题 1.4

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

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

定义 1.18 (A-模同态)

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

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

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

定义 1.19 (核)

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

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

这是 M_1 的子模。

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

1.2.4 正规子群和商结构

定义 1.20 (左陪集)

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

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

在陪集概念下，可以定义等价类：

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

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

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

定义 1.21 (商集和指标)

我们定义左陪集的集合

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

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

事实上也可以定义右陪集，但是二者实质上没有区别.

命题 1.5 (左陪集的元素个数)

对任意的 gH 和 $g'H$，如下映射为双射：

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

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

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

定理 1.1 (Lagrange)

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

定义 1.22 (正规子群)

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

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

例题 1.12 G 是交换群，其所有子群都是正规子群。

例题 1.13 群同态的核是正规子群，即若 $\varphi\colon G \to G'$ 是群同态，则 $\mathrm{Ker}(\varphi) \lhd G$。

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

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

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

定义 1.23 (正规化子)

*H 是群 G 的子群，定义 H 在 G 中的*正规化子*为：*

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

容易验证 $\mathrm{N}_G(H)$ 是 G 的子群。按定义，我们有

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

这是 G 的使得 H 在其中为正规子群的最大子群。

♣

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

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

我们必须验证以上是良好定义的（乘法在等价类上一致）。假设 $g_1' = g_1h$，其中，$h \in H$，那么，$g_1H = g_1'H$。所以，上述直观的定义还应该给出

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

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

有了陪集上的良好定义的乘法，我们可以定义群到陪集的群同态：商映射.

定理 1.2 (商映射)

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

$$\pi \colon G \longrightarrow G/H$$

是群同态。另外，$\mathrm{Ker}(\pi) = H$。

实际上，左陪集的乘法定义为 $g_1H \cdot g_2H = g_1g_2H$, 当 H 正规，这个乘法是良好定义的.

♡

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

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

此时，

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

所以，π 是群同态。

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

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

这表明群的乘法结构由同态决定。

定理 1.3 (群同态基本定理)

G 是群，$H \lhd G$ 是正规子群，$\varphi \colon G \to G'$ 是群同态。若 $H < \mathrm{Ker}(\varphi)$，则存在唯一的群同态 $\overline{\varphi} \colon G/H \to G'$，

使得 $\overline{\varphi}\circ\pi=\varphi$，其中，$\pi\colon G\to G/H$ 是自然的同态。

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

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

♡

证明 对任意的左陪集 gH，定义

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

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

选取 $H=\mathrm{Ker}(\varphi)$，我们显然有满射

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

另一方面,$\overline{\varphi}(a)=\overline{\varphi}(b)\Leftrightarrow\overline{\varphi}(a)\overline{\varphi}(b)^{-1}=1\Leftrightarrow\overline{\varphi}(ab^{-1})=1\Leftrightarrow ab^{-1}\in\mathrm{Ker}\overline{\varphi}\Leftrightarrow a\mathrm{Ker}\overline{\varphi}=b\mathrm{Ker}\overline{\varphi}$，所以该同态是单射，从而为同构。

推论 1.1 (循环群的结构)

G 是群，$g\in G$，那么 $\langle g\rangle$ 要么与 $\mathbb{Z}$ 同构，要么与 $\mathbb{Z}/n\mathbb{Z}$ 同构，其中，$n=\mathrm{ord}(g)$。

♡

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

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

定义 1.24 (商模)

给定 A-模 M 及其子模 N，我们可以构造其**商模** M/N。

首先将 M 视为交换群，其所有子群均为正规子群，从而，我们可以定义商群：

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

这自然也是交换群，其 A-模结构由如下公式给出：

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

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

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

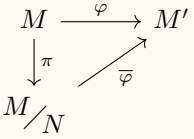
这个同态是满射。

♣

定理 1.4 (线性代数基本定理)

M 和 M' 是 A-模，$N\subset M$ 是子模，$\varphi\colon M\to M'$ 是 A-模同态。如果 $N\subset\mathrm{Ker}(\varphi)$，那么存在唯一的 A-模

同态 $\overline{\varphi}\colon M/N \to M'$，使得 $\overline{\varphi}\circ\pi=\varphi$，其中，$\pi\colon M\to M/N$ 是自然的同态。



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

♡

证明 对任意 $m+N$，定义

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

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

选取 $N=\mathrm{Ker}(\varphi)$，我们显然有满射

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

根据定义，$\overline{\varphi}(m+N)=0$ 当且仅当 $m\in\mathrm{Ker}(\varphi)$，所以该同态是单射，从而为同构。

第 2 章 群作用