Abstract Algebra

陈彦桥
南方科技大学

2025 年 7 月 28 日

目录

第一章 群、环、体、域 **5**

1.1 群 5

1.1.1 群的定义 5

1.1.2 群的基本性质 6

1.1.3 陪集（Coset） 7

1.1.4 正规子群 8

1.2 同态与同构 9

1.2.1 同态与同构的定义与性质 9

1.2.2 群的直积与直和 12

1.3 环 13

1.4 体和域 13

第二章 特殊的群 **15**

第三章 环与数论 **17**

第四章 域扩张与伽罗瓦理论 **19**

第五章 模与格简介 **21**

第一章　群、环、体、域

1.1　群

1.1.1　群的定义

Definition 1.1.1 (群). 若一个集合 G 定义了一个二元运算 $\circ$，满足

- 运算封闭性：若 $a,b \in G$，则 $a \circ b \in G$;
- 结合律：$(a \circ b) \circ c = a \circ (b \circ c)$;
- 单位元：存在 e 使得对于 $a \in G$，有 $e \circ a = a \circ e = a$;
- 逆元：存在 $b := a^{-1}$ 使得对于 $a \in G$，有 $a \circ a^{-1} = e$;

则 G 是一个群。

通常，我们会省略写中间的运算符号，即 $a \circ b = ab$。

Remark 1.1.1. 进一步，若满足交换律 $a \circ b = b \circ a$，则称这个群是阿贝尔群（*Abel Group*）。

对于代数结构没有特别好的一些结构，我们同样予以其命名：

Definition 1.1.2 (半群). 若一个集合 G 定义了一个二元运算 $\circ$，满足

- 运算封闭性：若 $a,b \in G$，则 $a \circ b \in G$;
- 结合律：$(a \circ b) \circ c = a \circ (b \circ c)$;

则 G 是一个半群（*Semigroup*）。

Remark 1.1.2. 进一步，若半群具有单位元，那么称之为幺半群（*Monoid*）

Definition 1.1.3 (阶). 群中元素的数量被称为阶。

1.1.2 群的基本性质

Theorem 1.1.1 (基本性质). 以下的几条定理是不言而喻的：

- 群的单位元唯一。
- 群的任意元素的逆元唯一。
- 群具有消去律。（这由逆元的性质保证）

Definition 1.1.4 (子群). 若集合 H 满足以下性质：

- 群 G 元素构成的集合的子集为 H;
- H 满足 G 中运算的所有性质;

则 H 是 G 的子群，记为 $H \leq G$。

Theorem 1.1.2 (子群的判定定理). 下述三个条件等价：

- $H \leq G$;
- $\forall a, b \in G$，$ab \in H$ 且 $a^{-1} \in H$;（平凡验证封闭性与逆元）
- $\forall a, b \in G$，$ab^{-1} \in H$（或者 $a^{-1}b \in H$）;（实用的推论）

Definition 1.1.5 (群的积). 定义：

$$HK = \{hk | h \in H, k \in K\}$$

将判定定理改述为上述语言得到：

Theorem 1.1.3 (子群的判定定理（改述版本）). 对于 $H \subseteq G, H \neq \emptyset$，下述三个条件等价：

- $H \leq G$;
- $H^2 \subseteq H$ 且 $H^{-1} \subseteq H$;
- $HH^{-1} \subseteq H$（或者 $H^{-1}H \subseteq H$）;

Definition 1.1.6 (平凡子群、真子群、生成群、生成系). 作出如下定义：

- 显然 G 的子群可以为其自身以及 $\{e\}$，$\{e\}$ 被称为 G 的平凡子群。
- 若 $H \leq G$，且 $H \leq G$，则 H 为 G 的真子群。
- 若 $M \subseteq G$，$\forall (M \subseteq H_i\ H_i \leq G)$，$\bigcap_{i=1}^{n} H_i$ 被称为“M 生成的子群”，记为 $\langle M \rangle$。
- 若 $\langle M \rangle = G$，称 M 为 G 的一个生成系。

- 若 $|M|=1$ 且 M 为 G 的一个生成系，则 G 为循环群。
- 由有限个元素生成的群为有限生成群。
- 对于任意元素 a，称 $\langle a\rangle$ 的阶为元素 a 的阶，记为 $o(a)$。
- 群中所有元素阶的最小公倍数为群的方次数，记为 $\exp(G)$。

Remark 1.1.3. 实际上,“生成”可以理解为 M 的若干元素包含在若干个封闭的子群中，而这些子群的交恰好就是 M 中元素“能够”通过子群中运算得到的“被生成的元素”。对于这些子群中的其它元素，需要不属于 M 中的元素通过运算生成，因此也就自然不属于 M 的“生成”结果。

1.1.3 陪集（Coset）

接下来，我们进入群理论中第一个非常重要的部分：陪集。

Definition 1.1.7 (右（左）陪关系). 设 $H\leq G$，定义等价关系 $a\overset{l}{\sim}b$ 为

$$\exists h\in H, a=bh.$$

同样地可以定义 $a\overset{r}{\sim}b$

$$\exists h\in H, a=hb.$$

注意到 $a\overset{l}{\sim}b$ 意味着 $a\in bH$，则 bH 为一个等价类。同理可以得到另一个等价类 Hb。

Remark 1.1.4. 事实上，上述的等价关系阐明的是元素之间的转换关系。若一个元素可以通过一次左乘或者右乘某个子群中的元素而变成群中的另一个。由于 a,b 是任意的，我们很容易得出一个直观的结论：H 相当于一个待选的操作集合，而整个群中的某个子集中的元素可以通过这些操作相互转化。一个不太恰当的比喻是，某些场所中的陪酒小姐，她可以只服务某一个人群，我们总能够在这一群小姐中找到一位，服务了 a 以后就去服务 b。这样，我们就建立了一个人群的关系网络。而我们将要介绍的陪集，就是 H 要去陪的那些人。

于是我们可以通过上述等价关系定义陪集：

Definition 1.1.8 (陪集). 若 $H\leq G$，$a\in G$，形如 aH（类似地，Ha）的集合被称为 H 的一个左（右）陪集。

Remark 1.1.5. 我们之前的 *remark* 中的比喻，可以用来解释陪集的定义：若 b 在陪集中，那么他和 a 有过相同的陪酒小姐。这样，他们之间就存在一个中间人的关系。

Remark 1.1.6. 形式上，一个关键洞察是，陪集是对于群结构的一个划分，这个划分由确定的集合决定。群的元素被划分为若干个等价类，从而方便我们进行研究。

左陪集是等价类，因此群可以被分解为左陪集的无交并。

Theorem 1.1.4.

$$G = \dot{\bigcup}_{aH} aH$$

Remark 1.1.7. 这个定理表明，这一群陪酒小姐服务的对象是分成了几个群体的，有一些陪酒小姐服务高端人士，有一些陪酒小姐服务中产阶级，有一些陪酒小姐则服务比较寒酸的人士。他们找的小姐的服务方针是不太一样的。这样，我们就可以通过小姐的档次分出群体中所有人的档次了。

Definition 1.1.9 (指数). H 的左陪集的个数被称为 H 在 G 中的指数，记为 $|G:H|$。

注意到，H 与其陪集存在双射，也就是

$$\varphi : H \to aH$$

是双射。H 一旦确定，陪集就是确定的。

Theorem 1.1.5 (拉格朗日定理). G 为有限群，$H \leq G$，则

$$|G| = |G:H||H|$$

这个定理在无交并和双射的前置结论下是显然的。

Theorem 1.1.6. 有限群的任意元素的阶整除群的阶，即 $a^{|G|} = e$。

这里，后面的结论在前面那个条件的结论下显然。但是前面那个条件是为什么呢？根据拉格朗日定理，取 $H = \langle a \rangle$ 即可。

1.1.4 正规子群

在线性代数中，商空间对于我们解决子空间相关的问题至关重要。显然，商空间 $V/W = \{\overline{\alpha} | \overline{\alpha} = \alpha + W, \alpha \in V\}$ 是 W 的一个关于加法的陪集。其中商空间中的运算被定义为 $\overline{\alpha} + \overline{\beta} = \overline{\alpha + \beta}$，也就是 $\alpha + W + \beta + W = (\alpha + \beta) + W$。我们想要将这一思想推广到群中，但是，显然我们必须要解决左陪集和右陪集不同的问题。

Theorem 1.1.7. $H \leq G$，任意两个左陪集相乘仍然为左陪集的充要条件是左右陪集相等。

进一步，为了定义商群，我们定义正规子群

Definition 1.1.10 (正规子群). $H \leq G$，若 $\forall a$，$aH = Ha$，则 H 为 G 的正规子群，记为 $H \trianglelefteq G$。

Remark 1.1.8. 我们继续用不正经的比喻来解释这一定义。首先，我们定义服务 *1* 和服务 *2*（对应左陪和右陪），这样，某一个客人点了不同的服务，小姐的下一个客人是可能不一样的。但是，若这是一个“正规”的场所，那么服务不应该有“不正经”的内容，应该表里如一，因此不论客人点哪个服务，下一位客人都是一样的。

Theorem 1.1.8 (正规子群判定定理). 以下三个条件等价：

- $H \trianglelefteq G$;
- $\forall a \in G, a^{-1}Ha = H$;
- $\forall a \in G, a^{-1}ha \in H$;

其中最后一个条件比较实用。

进一步我们定义商群：

Definition 1.1.11 (商群). 若 $H \trianglelefteq G$，则 H 的陪集在乘法下构成群，称其为 G 关于 H 的商群，记为 G/H。

Remark 1.1.9. 很简单，H 是小姐，拿着一批小姐名单去找人，找到的可不就是客户嘛。所以商群就是小姐的客户。

Remark 1.1.10. 对于陪集，我们可以有一个类比认知：我们小学就学过的除法中，$a/c = b$，其中 b 称为商，我们发现，陪集被定义为 $a = bH$，实际上就是说，H 就是那个除数，它将群元素 a 的其它“结构”除掉，保持最本质的性质。这样，我们就不难理解为什么 H 是商群的单位元了：在同余类中，无论加上模数多少遍，元素仍然保持不变。这恰好就是单位元的性质。我们将这一不变性推广到更广泛的区域上去，就是我们的陪集。

1.2 同态与同构

1.2.1 同态与同构的定义与性质

Definition 1.2.1 (同态). 若映射

$$\varphi : G_1 \to G_2$$

保持运算，即 $\varphi(ab) = \varphi(a)\varphi(b)$，则 φ 是一个同态。若 φ 为单（满）射，则为单（满）同态。若为双射，那么称之为同构，记为 $G_1 \cong G_2$。

Remark 1.2.1. 同态表明，我可以将旧的经验转移到新的情境中，原有的群中的运算，可以分别将运算对象映射到像空间中再利用那里的运算得出结果。相当于运送建材，先在工厂用电钻拆开，然后拿到工地也能拿螺丝刀拧上。这就是同态，一个样。

Definition 1.2.2 (自同态). 若同态 φ 是

$$\varphi : G \to G$$

则称其为自同态，记 G 所有自同态的集合为 $\mathrm{End}(G)$。同理记 $\mathrm{Aut}(G)$ 为 G 全体自同构组成的集合。注意到 $\mathrm{Aut}(G)$ 组成一个群，而 $\mathrm{End}(G)$ 是一个幺半群。这是显然的，因为同态不一定是双射，不一定可逆。

Definition 1.2.3 (同态的像与核). 定义 $\varphi(G)$ 为 φ 的像，记为 $\mathrm{im}\varphi$ 而单位元对应的原像定义为核，也就是

$$\ker\varphi := \{a|\varphi(a) = e\}$$

不难发现，商群的单位元就是 H，因此若要验证一个同态是单的，只需要任取 H 中的元素，验证其被映射到像空间的单位元，并且验证对于任意原空间中的元素，若其被映射到单位元，可以推出其属于 H，就可以验证其单射性质；若要验证其满射，只需要取像空间中任意元素，说明其在同态下存在原像（被作用的元素属于原空间）即可。

同态是单射并不好验证，但是我们可以通过以下的等价条件进行验证：

Theorem 1.2.1. $\ker\varphi = \{e\} \Leftrightarrow \varphi$ 单

接下来我们将要介绍同构中非常关键且基础的一个定理：

Theorem 1.2.2 (同构基本定理). 设 φ 是群同态，则

$$G/\ker\varphi \cong \mathrm{im}\varphi$$

Definition 1.2.4 (平移). 定义 G 上的变换

$$L(a) : G \to G$$

称 $L(a)$ 为由 a 引起的左平移，同理可以定义右平移。

Theorem 1.2.3 (凯莱定理). 任一群同构于某一集合上的变换群。

Theorem 1.2.4 (凯莱定理（有限群）). 任一群 G 同构于对称群 $S_{|G|}$ 的某个子群。

Proof. 设 $L(G)$ 是左平移的全体构成的 G 的全变换群 $S(G)$ 的子集，定义

$$L : G \to S(G)$$

对于任意 $a, b, g \in G$

$$L(ab)g = (ab)g = a(bg) = L(a)(bg) = (L(a)L(b))g$$

因此 L 是群同态。注意到 $\mathrm{im}L = L(G)$，对于 L 而言，$L(a) = \mathrm{id}$ 当且仅当 $a = e$，因此 $\ker L = \{e\}$，因此由同态基本定理得到

$$G \cong L(G)$$

得证. □

Remark 1.2.2. 凯莱定理事实上阐述了这样一件事情：任何抽象的群与某个置换群同构。这使得我们能够具体地研究群的内部结构。由于变换群可以由具体的自然数的置换表示，我们的研究就会更加简单和容易。因此我们将 $L(G)$ 称为 G 的左正则表示，对应地，$R(G)$ 被称为右正则表示。

实际上，在范畴论中，我们有更广泛的结论：

Theorem 1.2.5 (米田引理). 设 $\mathcal{C}$ 为局部小范畴，$X \in \mathcal{O}b$。设 F 为从任意 $\mathcal{C}$ 到 $\mathbb{SET}$ 的函子，存在从 $Nat(h_X, F)$ 到集合 $F(X)$ 的双射。且该双射为

$$\alpha \mapsto \alpha_X(\mathrm{id}_X)$$

其逆映射把 $u \in F(X)$ 映射到自然变换 β，使得对于任意的 $T \in \mathcal{O}b(\mathcal{C})$，都有

$$\beta_Y : Hom_{\mathcal{C}}(X, Y) \to F(Y)$$

我们不会深入这一结论，因为这远远超出了本笔记的叙述“范畴”。

回到正题，我们直觉上愿意定义所谓的“典范”，以便于我们进行群结构的研究，因此我们将从原群到商群的同态记为：

Definition 1.2.5 (典范同态). 若 $H \trianglelefteq G$，则易得

$$\pi : G \to G/H$$

是同态。这一同态被称为从 G 到 G/H 的典范同态。

Remark 1.2.3. 容易发现，由于 H 是正规子群，因此商群存在。典范同态保证从原来的群转换为商群的过程中保持运算，使得商群的结构是良定义的。

Theorem 1.2.6 (第一同构定理). $H \trianglelefteq G$，在 G 到 G/H 典范同态下

- G 的包含 H 的子群与 G/H 的子群在典范同态下一一对应;
- 上述一一对应下，正规子群对应正规子群;
- 若 $K \trianglelefteq G$ 且 $K \supseteq H$，则

$$G/K \cong (G/H)/(K/H)$$

Remark 1.2.4. 这个定理表明，商运算保持正规性，低阶商群可以通过高阶商群构造。这一性质进一步强调了正规性的重要性。

Theorem 1.2.7 (第二同构定理). 设 G 是群，$H \trianglelefteq G$，$K \leq G$，那么以下结论成立：

- $HK \leq G, H \cap K \trianglelefteq K$;
- $(HK)/H \cong K/(K \cap H)$

Remark 1.2.5. 这一定理的证明是不难的。首先，只需要通过判定定理验证 HK 是子群，然后通过正规子群判定定理老老实实验证正规子群。证明同构还是四步法：证明 *Well-Defined*（证明运算性质与代表元选取无关，常见手法是通过选取两个假设相等的元素，验证其像是否一定相等）、证明为群同态（保持运算）、证明单（核空间只有单位元）、证明满（每个像对应原像）。这些基本的定理基本上都按照以上步骤进行，这是基本功。

Remark 1.2.6. 定理显然表明，积运算不保持正规性，交运算保持正规性；同时，子群积对正规子群的商同构于子群对子群交的商。

1.2.2 群的直积与直和

新群的构造可以通过简单的复合进行：

Definition 1.2.6 (直和). 设群 G_1, G_2，由笛卡尔积得群 $G_1 \times G_2$，该集合在运算

$$(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$$

下保持群结构。称为群的（外）直和，记为 $G_1 \oplus G_2$，G_1 和 G_2 称为 $G_1 \oplus G_2$ 的直和因子。

我们常常反过来考虑：是否可以将一个群分解为多个群的直和？我们给出如下的等价判定条件：

Theorem 1.2.8 (群的直和分解判定). 设 G 是群，$H, K \trianglelefteq G$，$G = HK$，那么以下结论等价：

- 映射

$$\sigma : H \oplus K \to G$$

  是同构;

- G 的任意元素唯一表示为 H 和 K 元素的乘积;
- G 的单位元唯一表示为 H 和 K 元素的乘积;
- $H \cap K = \{e\}$;

Remark 1.2.7. 判定内容是直观的，这表明两个群负责不同维度的内容而不存在交集。事实上，从第四个结论就可以联想到线性代数中的直和分解的内容，这在群中也是相同的。事实上，这与实际我们人工智能的分类也有很大关系：若一个事物的描述是可分的，那么它一定是若干直和的结果。

满足如上性质的 G 被称为 H 和 K 的（内）直和，记号相同。对于多个群的直和，我们同样可以证明上述四个定理，只需要使用归纳法进行验证即可。其中注意，第四个定理为 $\forall i, H_i \cap (H_1 \cdots \hat{H}_i \cdots H_n) = \{e\}$，其中 $\hat{H}_i$ 表示去掉 H_i。

Definition 1.2.7 (直积). 设 G 是群，I 为集合的指标集（可以是无穷集合）。记

$$\prod_{i \in I} G_i$$

为（外）直积。同样为集合的笛卡尔积，运算同样为按分量运算。显然，若 I 有限，其与直和无区别。但是在无限集情况下，二者不同。该集合的一个自然的子集为 $\{(\cdots, a_i, \cdots) | a_i \in G_i, \forall j \neq i, a_j = e_j\}$。

存在一个映射将任一群映射到直积群中，当指标集有限，直和的任意元素都可以唯一地表示为像空间中的和（线性代数中，这被称为正交基），而无限集中则没有如上性质。

终于，我们结束了群的内容，接下来我们了解环的内容。事实上，环的内容有很多与群是类似的。

1.3 环

1.4 体和域

第二章　特殊的群

第三章　环与数论

第四章　域扩张与伽罗瓦理论

第五章　模与格

第六章　群表示论