

Group Theory

Jianfeng He

第一章 Basic Conception of Group

§ 1.1 群及其乘法表

1.1.1 群的基本概念

Concept 1.1 (对称变换) 保持系统不变的变换称为 **对称变换**.

Definition 1.1 (群) 在规定了元素的乘法后, 元素的集合 G 若满足下面四条公理, 则这个集合可被称为 **群**:

1). **封闭性**: 任意两元素的乘积仍然属于这个集合. 亦即:

$$RS \in G, \quad \forall R, S \in G \quad (1.1)$$

2). **结合律**: 乘积满足结合律, 亦即:

$$R(ST) = (RS)T, \quad \forall R, S, T \in G \quad (1.2)$$

3). **存在单位元**: 存在一个被称为单位元的元素 E , 用它左乘任意元素, 该元素均保持不变. 亦即:

$$ER = R, \quad \forall R \in G \quad (1.3)$$

4). **任何元素存在逆元**: 任意元素 R 均存在对应的逆元 R^{-1} , 其定义为:

$$R^{-1}R = E \quad (1.4)$$

亦即元素与其逆元的乘积等于单位元.

可以看到, 在对单位元及逆元进行定义的时候, 只定义了左乘, 那么单位元右乘或逆元右乘时, 还会有相同的性质吗? 实际上, 从基本定义出发, 可以得到以下推论:

Property 1.1 (恒元及逆元的右乘)

1). **恒元右乘**: 恒元右乘时, 同样保有恒元的性质, 亦即:

$$RE = R \quad (1.5)$$

2). **逆元右乘**: 逆元右乘时, 还是得到恒元. 换言之, 逆元 R^{-1} 的逆, 恰是 R 自身:

$$RR^{-1} = E \quad (1.6)$$

$$(R^{-1})^{-1} = R \quad (1.7)$$

可以看见, 对于恒元及逆元, 其运算是可交换的, 这个性质对所有群均成立. 由于恒元及逆元在乘法运算上的对称性, 在之后讨论或证明相关性质时, 可以只考虑一个方向上的乘法. 由恒元及逆元的右乘的性质出发, 不难得出恒元及逆元的唯一性:

Property 1.2 (恒元及逆元的唯一性)

恒元的唯一性: 若 $TR = R$ 或 $RT = R$, 则 $T = E$.

逆元的唯一性: 若 $TR = E$ 或 $RT = E$, 则 $T = R^{-1}$.

一般而言, 除了恒元及逆元外, 一般元素之间的乘法是不可对易的, 但也存在如实数加法群这样的乘法可对易的群, 于是有了 **阿贝尔群** 的概念:

Concept 1.2 (阿贝尔群) 元素乘积都可对易的群称为 **阿贝尔群**.

按照群元素的数目, 可以定义 **群的阶数**:

Definition 1.2 (群的阶数) 群 G 的群元素的个数 g 称为群 G 的阶数.

还可以对群的阶数进行更细致的讨论:

Concept 1.3 (无限群) 群元数目无限多的群称为 **无限群**.

Concept 1.4 (连续群) 若可以建立群元到一组连续参数的一一映射, 则这样的群称为 **连续群**.

连续群的一个例子是之后将要接触到的 **李群**.

对于有限群, 由于群元素的有限性, 群中任一元素的幂次足够高时, 其总会回归到自身. 如: 对于 6 阶群 G_6 , 其只有 6 个不同的元素. 设 $R \in G_6$, 对于 R^n , 在 $n > 6$ 之前, 一定会出现 $R^n = R$ 的情形, 因为 6 阶群不可能有 7 个不同元素. 由此可以引出 **群元素的阶数** 的定义:

Definition 1.3 (群元素的阶数) 若群 G 中的群元 R 满足:

$$R^a = E, \quad a \in \mathbb{Z}^+ \quad (1.8)$$

则称 a 为群元素 R 的阶数

群论中有一个名为 **重排定理** 的基本定理, 为更方便地对其进行表述, 首先引入 **复元素** 的概念:

Concept 1.5 (复元素) 在群 G 中选取一个子集 R , 将该子集 R 称为群 G 的一个复元素.

从定义可以发现, 复元素的本质是一个集合, 因此满足集合的 **无序性**, **确定性**, **互异性** 等基本性质. 此外, 两复元素 R_1, R_2 相等的充要条件是它们所包含的元素完全相同. 这一点和一般的集合相等是完全一致的. 在有了复元素的基本概念之后, 需要考虑的是如何定义复元素与普通元素的乘法:

Definition 1.4 (复元素与普通元素的乘法) 复元素乘上普通元素仍然得到一个复元素, 该复元素由该普通元素分别与原本复元素的每一元素相乘得到. 亦即, 若 $R = \{r_i\}$, s 为一普通元素, 则:

$$sR := \{sr_i\}, Rs := \{r_is\} \quad (1.9)$$

复元素也可与复元素相乘, 其结果是所有乘积组合形成的新集合, 即:

Definition 1.5 (复元素与复元素相乘) 若 $R = \{r_i\}$, $S = \{s_i\}$, 则:

$$RS := \{r_is_j\}, SR := \{s_ir_j\} \quad (1.10)$$

接下来正式介绍重排定理:

Theorem 1.1 (重排定理) 用 G 表示群中所有元素构成的复元素, G^{-1} 表示群中所有元素的逆元素构成的复元素, T 为群中任一普通元素, 于是:

$$TG = GT = G^{-1} = G \quad (1.11)$$

对于有限群, 可以把群中每一对乘积得到的结果都列出来形成一张表, 由此引出 **乘法表** 的概念:

Concept 1.6 (乘法表) 对于有限群, 在行与列都填满该群中的所有元素. 若记 $R = \{r_i\}$ 在第 i 行第 j 列的位置, 填上元素 r_i 右乘 r_j 的结果 $r_i r_j$, 由此形成的表称为乘法表.

可以预见, 对于阿贝尔群, 乘法表是关于对角线对称的.

Definition 1.6 (群的同构) 若存在一个从群 G 到群 G' 的一一映射 f :

$$f: G \rightarrow G', R \mapsto R' \quad (1.12)$$

若 $\forall R, S \in G, R' = f(R), S' = f(S)$, 满足:

$$F(R, S) = F'(R', S') \quad (1.13)$$

即称 G 与 G' 同构, 记为 $G \approx G'$. 其中 F, F' 分别表示两群的群乘法.

Notation :

- 1). 对于奇数阶群, 因为单位元自身是自身的逆元. 因而此时除了单位元以外的元素为偶数个, 从而可以成对地提取出元素以及它的逆元; 对于偶数阶群, 由于除了单位元外的元素为奇数个, 因此必然有元素其逆元是自身, 也就是说, 偶数阶群必然存在二阶元素.
- 2). 不难证明: 若一个群 G 中含有二阶元素, 则该二阶元素与么元素构成该群的一个子群

1.1.2 群的生成元与秩

前面提到过, 有限群的元素有阶数的概念. 也就是说: 或许可以只用很少的几个元素以及它们的幂来构造出该群的所有元素, 这就涉及到下面将介绍的 **生成元** 的概念:

Definition 1.7 (循环群与生成元) 由一个元素 R 及其幂次构成的有限群称为由 R 生成的循环群, 记为 C_n . n 称为 **循环群的阶**, R 称为 **循环群的生成元**. 一般地, 循环群 C_n 可以被描述为:

$$C_n = \{E, R, R^1, R^2, \dots, R^{n-1}\}, R^n = E \quad (1.14)$$

对于 n 阶循环群, 其阶数等于其生成元的阶数. 此外, 不难得知:

$$R^{-1} = R^{1-n} \quad (1.15)$$

更一般地, 若用记号 $j \bmod N$ 来表示 j 整除 N 后的余数, 则对于 n 阶循环群 C_n , 有:

$$R^a = R^{a \bmod N} \quad (1.16)$$

于是可以从循环的角度来理解模运算: $j \bmod N$ 表示将取值相差 N 的两个 j 看成相同的.

以上只讨论了对于循环群如何定义阶数, 那么, 对任一有限群, 能否定义阶数以及生成元呢? 答案是肯定的, 由此还能引出有限群的秩的概念:

Definition 1.8 (有限群的生成元与秩) 对于群 G , 任取一个元素 R_1 , 若其幂次构成的集合尚无法填满整个群, 那么再取下一个元素 R_2 , 并考虑 R_2 的幂次构成的集合. 如此反复操作, 直至由取出的元素的幂次构成的元素集合的并集能够填满整个群为止, 将这些基本元素的集合 $\{R_i\}$ 称为群 G 的 **生成元**, 集合 $\{R_i\}$ 中元素的数目称为该群的 **秩**.

生成元的概念在之后学习李群时可以做进一步推广, 这一点可以做如下理解: 在经典的微积分理论中, 任一种变换可以进行泰勒展开, 而泰勒展开本质上是一系列的幂次相加, 这些幂次就有点类似这里介绍的生成元. 也就是说, 连续群也可以找到一些基本元素, 由这些基本元素的运算来得到整个连续群的性质.

§ 1.2 群的各种子集

1.2.1 子群

Definition 1.9 (子群) 若群 G 的一个子集 H , 按照原本的群乘法规则仍然构成群, 则称其为群 G 的一个子群.

Definition 1.10 (循环子群) 群 G 中任一元素的幂次构成的群称为群 G 的一个循环子群.

不难得知, 循环子群同构于相同阶数的循环群.

Notation :

- 1). 按照之前关于复元素的定义, 可知: 子群本身也是一种复元素. 这为之后介绍陪集的概念带来了方便.

1.2.2 陪集和不变子群