Groups

Revisited With Examples From Number Theory

宦皓然

致理书院

2022 年 6 月 3 日

1. Lagrange 定理
2. Cayley 定理
3. 乘法循环群

简单的群：$(\mathbb{Z},+)$ 和 $(n\mathbb{Z},+)$

- 我们已经知道，$(\mathbb{Z},+)$ 是一个群。
- 这是一个循环群，生成元是 1 ，从而也是交换群。
- 我们来看它的一个子群，$(n\mathbb{Z},+)$。其中

$$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\} = \{0, n, -n, 2n, -2n, \dots\}$$

- 对这个子群用 Lagrange 定理，得到 $|\mathbb{Z}| = [\mathbb{Z} : n\mathbb{Z}]\,|n\mathbb{Z}|$
- 这带来两个问题：
  1. $[\mathbb{Z} : n\mathbb{Z}]$ 是什么？
  2. 如何理解无限群使用 Lagrange 定理？

理解陪集

- 下面来讨论 $[\mathbb{Z}:n\mathbb{Z}]$，也就是 $\mathbb{Z}$ 关于 $n\mathbb{Z}$ 的陪集个数。
- 由于我们在交换群上工作，不用区分左右陪集。
- 容易看出，

$$\begin{aligned} x+n\mathbb{Z} &= \{x+nk : k \in \mathbb{Z}\} \\ &= \{y \in \mathbb{Z} : y \equiv x \pmod n\} \end{aligned}$$

- 这是一个具体的陪集的例子：模 n 同余的那些数，构成一个陪集。
- 由此得到 $[\mathbb{Z}:n\mathbb{Z}]=n$。

无限群上的 Lagrange 定理

- 带回 $|\mathbb{Z}| = [\mathbb{Z} : n\mathbb{Z}]\,|n\mathbb{Z}|$，我们得到 $|\mathbb{Z}| = n\,|n\mathbb{Z}|$。
- 可以取 $|\cdot|$ 为集合的势，那么这就得到 $\aleph_0 = n\aleph_0$。
- 这确实是一个正确的式子……但是没什么意义？
- 事实上，对于 Lagrange 定理 $|G| = |H|\,[G : H]$，可以通过构造 $\{xH : x \in G\} \times H \to G$ 的双射，证明 Lagrange 定理对无穷群也成立。
- 课本中为了证明左陪集与右陪集"数量相等"，在两者间构造了双射，从而课本对于左右陪集数量相等的定理没有做有限群的限制。

Cayley 定理

- 下面我们在 $\mathbb{Z}_p = \mathbb{Z}/n\mathbb{Z}$ 上解释 Cayley 定理。
- Cayley 定理：群 G 同构于某个交换群。
- 定义：由 1-1 映射（置换、排列+）构成的群叫做交换群。
- 注意到，
$$\{x + \mathbb{Z}_p : x \in \mathbb{Z}_p\} = \mathbb{Z}_p$$
- 或者说，$f_x : \mathbb{Z}_p \to \mathbb{Z}_p, y \mapsto y + x$ 是一个双射。
- 这就表明，f_x 是一个 $\mathbb{Z}_p$ 上的置换。
- 然后验证这些置换构成群（封闭性、结合律、单位元、逆元）……

Cayley

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$$0 \mapsto \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \end{pmatrix}$$
$$1 \mapsto \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{pmatrix}$$
$$2 \mapsto \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix}$$
$$3 \mapsto \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 1 & 2 \end{pmatrix}$$

- 由列看：+2 这个操作，把 $\{0, 1, 2, 3\}$ 变成 $\{2, 3, 0, 1\}$，只是交换了他们的顺序。
- 我们把第一行的 0,1,2,3 理解成元素，把第一列的+0,+1,+2,+3 看作对于元素的置换，就得到了 Cayley 定理。
- $\{+0, +1, +2, +3\}$ 是群，其中元素是对 $\{1, 2, 3, 4\}$ 的一个置换；也就是右边的置换。这就是同构。

Cayley

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$$0 \mapsto \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \end{pmatrix}$$
$$1 \mapsto \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{pmatrix}$$
$$2 \mapsto \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix}$$
$$3 \mapsto \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 1 & 2 \end{pmatrix}$$

$\{+0, +1, +2, +3\}$ 是群，其中元素是对 $\{1, 2, 3, 4\}$ 的一个置换；也就是右边的置换。这就是同构。

进一步，如果把左侧“44 加法表”的所有位置全都替换成置换，这个加法表仍然成立，其中加法的意思改成置换的复合。

把"2"理解成"+2"，"+2"是一个置换。

$(\mathbb{Z}_n, \cdot)$ 不是群

- 下面我们考虑乘法，$(\mathbb{Z}_n, \cdot)$ 是不是一个群？
- 我们沿用刚才的想法，注意到 $0\mathbb{Z}_n = \{0\}$，“$\times 0$” 不是置换。这就说明 $(\mathbb{Z}_n, \cdot)$ 不是一个群。
- 我们继续看，对于 $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$，我们有

$$
\begin{aligned}
4\mathbb{Z}_6 &= \{0, 4, 8, 12, 16, 20\} \\
&= \{0, 4, 2, 0, 4, 2\} \\
&= \{0, 2, 4\} \\
&\neq \mathbb{Z}_6
\end{aligned}
$$

- 我们需要去掉 $\mathbb{Z}_6$ 中的一些元素得到 $\mathbb{Z}_6^*$ 使之在乘法下是群。下面分析如何得到这一个乘法群。

$(\mathbb{Z}_{12}, \times)$

×	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

- 其中，只有第 $\{1, 5, 7, 11\}$ 行的元素构成排列。

收缩之后得到群 $(\mathbb{Z}_{12}^*, \times)$

$\times$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

- 注意到事实上我们挑选的条件是 $5\mathbb{Z}_{12} = \mathbb{Z}_{12}$，而不只是 $5\{1, 5, 7, 11\} = \{5, 1, 11, 7\} = \{1, 5, 7, 11\}$。
- 现在我们看这些 $1, 5, 7, 11$ 具体是怎么选出来的，它们满足了什么条件。
- 构成排列：$5y \equiv 5z \pmod{12} \Leftrightarrow y \equiv z \pmod{12}$。

乘法群 $(\mathbb{Z}_n^*, \cdot)$

- 假设我们可以选取 $\mathbb{Z}_n^* \subseteq \mathbb{Z}_n$ 是一个乘法群。
- 我们希望 $x\mathbb{Z}_n^* = \mathbb{Z}_n^*$。
- 这也就是说，对于 $x \in \mathbb{Z}_n^*$，有 $xy \equiv xz \pmod n \Leftrightarrow y \equiv z \pmod n$。
- 对应到课本上的群的定义，这也就是消去律，或者说逆元的存在性。
- 下面对于 $a \in \mathbb{Z}_n$，方程 $ax \equiv 1 \pmod n$ 解的存在性。
- 这个方程可以化为 $ax = 1 + ny$，或者 $ax - ny = 1$。
- Bézout 定理：整数不定方程 $ax + by = 1$ 有解，当且仅当 a, b 互质。

乘法群 $(\mathbb{Z}_n^*, \cdot)$

- Bézout 定理：整数不定方程 $ax + by = 1$ 有解，当且仅当 a, b 互质。
- $ax = 1 + ny$，或者 $ax - ny = 1$，有解当且仅当 a, n 互质。
- $ax \equiv 1 \pmod{n}$ 有解，当且仅当 a, n 互质。
- 所以应该取 $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n : (x, n) = 1\}$，这是 $\mathbb{Z}_n$ 的子集中最大的乘法群。
- 这个乘法群有多大？
- 课上提到，$\{0, 1, 2, \dots, n-1\}$ 中与 n 互质的数的个数，记为 $\varphi(n)$，也就是欧拉函数。
- 一些例子：
  1. $\mathbb{Z}_6^* = \{1, 5\}$
  2. $\mathbb{Z}_{18}^* = \{1, 5, 7, 11, 13, 17\}$
  3. $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

1. Lagrange 定理
2. Cayley 定理
3. 乘法循环群

原根

- $(\mathbb{Z}_n^*, \cdot)$ 是交换群，那它是不是循环群？
- 定理：$(\mathbb{Z}_n^*, \cdot)$ 是循环群，当且仅当 n 形如 $2, 4, p^k, 2p^k$，其中 p 是奇素数，$k \geq 1$。
- 循环群 $(\mathbb{Z}_n^*, \cdot)$ 的生成元，称作原根。
- 例子：对于 $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$
  - $1 = 1$
  - $2 = 2, 2^2 = 4, 2^3 = 1, 2^4 = 2$
  - $3 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1, 3^7 = 3$
- 所以 3 是生成元。事实上，我们可以写 $\log_3 1 = 0, \log_3 3 = 1, \log_3 6 = 2$（在某种意义下成立）。
- 思考：如果 $(\mathbb{Z}_n^*, \cdot)$ 是循环群，它有 $\varphi(\varphi(n))$ 个原根（生成元）。

Thanks!