Disscusion on Cyclic Groups

OT 2

郑奘巍

zzw@smail.nju.edu.cn

2019 年 3 月 10 日

问题

在二维平面上的“移动”构成循环群吗? 若不是，请改造为循环群。你能找到这个循环群的一些子群吗？他们是循环群吗?

二维平面的“移动”有哪些元素?

定义

$\mathbb{R} * \mathbb{R}$ 二维平面/向量空间

定义

$\{(\theta, r) : \theta \in [0, 360), r \in \mathbb{R}\}$ 极坐标

我们将分别考察他们是否有可能为循环群

定义

同构 (isomorphic)：G 和 G' 为两个群，如果有一个 G 到 G' 的双射 σ 满足 $\forall x, y \in G, \sigma(xy) = \sigma(x)\sigma(y)$, 则称 G 与 G' 同构

同构的群拥有相同的性质。我们将在同构意义下考察循环群。

定义

直和：令 $G = G_1 \times G_2$, G 中乘法定义为 $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$，可证 G 为群（可参考书本第九章）

书中告诉了我们，$\mathbb{Z}$ 是循环群，其子群 $n\mathbb{Z}, n = 0, 1, 2, \cdots$ 也是循环群（且循环群的子群也是循环群）。有没有除此之外的循环群呢?

定理

Infinite cyclic group $G = \langle a \rangle$ *is isomorphic to* $(\mathbb{Z}, +)$

证明.

Define $\phi : \mathbb{Z} \to G : \phi(k) = a^k$.

Discuss homomorphism, surjection, injection respectively. $\square$

定理

Cyclic group of same order are isomorphic to each other.

证明.

$G_1 = \langle a \rangle, G_2 = \langle b \rangle, |a| = |b| = k$. $\phi : G_1 \to G_2 : \phi(a^n) = b^n$.
Discuss homomorphism, surjection, injection respectively. □

引理

平面移动群：$\mathbb{R} * \mathbb{R}$ 二维平面/向量空间

证明.

无限循环群必然可数，故此不为循环群 $\square$

定义

$\{(\theta, r) : \theta \in [0, 360), r \in \mathbb{R}\}$ 极坐标

改造为群:

定义

平面移动群：$G = \mathbb{T} * \mathbb{R}$, $\mathbb{R}$ 为实数加群，$\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ 为圆群

利用 $e^{i\theta}$ 的形式可与 $[0, \frac{2}{\pi})$ 建立对应，从而不可数。也不为循环群

改造为可数。由 Theorem 4.25 知 nth roots of unity 为 $\mathbb{T}$ 的子群，且为循环群，记为 $\mathbb{T}_n$

定义

平面移动群：$\mathbb{Z} \times \mathbb{Z}$

定义

平面移动群：$\mathbb{T}_n \times \mathbb{Z}$

注意：以上两个群是同构的，以下仅讨论 $\mathbb{Z} \times \mathbb{Z}$

定理

$G = \mathbb{Z} \times \mathbb{Z}$ is not a cyclic group

证明.

Suppose to the contrary (a, b) is a generator, since $(1, 0) \in G$, $\exists n, nb = 0$. Thus $b = 0$ but it cannot generate $(0, 1)$. $\square$

注意：直和中只要有一个循环群是无限的，以上论证均成立。

改造为有限：

定义

平面移动群：$\mathbb{Z}_n \times \mathbb{Z}_m$

$Z_2 \times Z_2, Z_2 \times Z_3$

定理

Let G and H both be finite cyclic groups with orders $n = |G| = \langle x \rangle$ and $m = |H| = \langle y \rangle$ respectively. Then $G \times H$ is cyclic if and only if $gcd(n, m) = 1$.

证明.

$" \Leftarrow "$: $|(x, y)| = k \Rightarrow (x, y)^k = e \Rightarrow x^k = e_G, y^k = e_H \Rightarrow n|k, m|k \Rightarrow nm|k$. And $(x, y)^n m = e$. Thus $k|nm$. So $|(x, y)| = nm$ □

$" \Rightarrow "$: $G \times H$ is cyclic, and (x, y) is one generator. First we prove that x generates G. In same way we know y generates H.
Then we prove that $g \in G, |g| = m, h \in H, |h| = n$ then $|(g, h)| = lcm(g, h)$.
Note
$|G \times H| = |G||H| = mn = |\langle x, y\rangle| = lcm(|x|, |y|) = lcm(m, n)$.
Thus $gcd(m, n) = 1$.

最后，我们通过改造得到了两组二维平面移动的循环群（都只能表示部分方向)：

- $Z_n * Z_m, (n, m) = 1$
- $T_n * Z_m, (n, m) = 1$

由于其均同构于 Z_{nm}, 根据书上定理，其共有 $\phi(nm)$ 个生成元。对于 $b = a^k$, 子群 $\langle b \rangle$ 的阶数为 $\frac{n}{gcd(k,mn)}$

定义

直和：令 $G = G_1 \times G_2$, G 中乘法定义为 $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$，可证 G 为群（可参考书本第九章）

问题

在 $Z_3 \times Z_4$ 中，$(1, 2)$ 是生成元吗？若不是，其阶为多少？

问题

$(x, y) \in Z_n \times Z_m$，求 $|\langle(x, y)\rangle|$


Thank
You!