第 4-1 讲: 群论初步

姓名： 林凡琪　　**学号：** 211240042

评分： ______　　**评阅：** ______

2024 年 1 月 28 日

请独立完成作业，不得抄袭。
若得到他人帮助, 请致谢。
若参考了其它资料，请给出引用。
鼓励讨论，但需独立书写解题过程。

1　作业 (必做部分)

题目 1 (TJ 3-3)
Wrte out Cayley tables for groups formed by the symmetries of a rectangle and for $(\mathbb{Z}_4, +)$. How many elements are in each group? Are the groups the same? Why or why not?

解答：
Te symmetries of a rectangle with centroid at the origin and sides parallel to the coordinate axes are generated by reflections σ_x in the x-axis and σ_y in the y-axis.
Their square is identity e and their product (in either order) is the rotation ρ of $\pi/2$ about the origin.
$\rho \circ \sigma_y = (\sigma_x \circ \sigma_y) \circ \sigma_y = \sigma_x \circ (\sigma_y \circ \sigma_y) = \sigma_x \circ e = \sigma_x$
Cayley tables:

$\circ$	e	σ_x	σ_y	ρ
e	e	σ_x	σ_y	ρ
σ_x	σ_x	e	ρ	σ_y
σ_y	σ_y	ρ	e	σ_x
ρ	ρ	σ_y	σ_x	e

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

These groups are not the same. While each symmetry has square the identity e; the square of 1 and 3 is 2; which is not the identity 0.

题目 2 (TJ-3-7)

Let S = $\mathbb{R}$ {-1} and define a binary operation on S by $a * b = a + b + ab$. Prove that$(S, *)$ is an abelian group.

解答:

To proof $(S, *)$ is a group, we must show that $(S, *)$ have the proposition of group.
Closure:if $a, b \in S$, then $a * b \in S$.
We prove the contrapositive: if $a * b \notin S$, either $a \notin S$ or $b \notin S$.
If $a * b \notin S$, then $a * b = a + b + ab = -1$
Adding 1 to both sides:
$1 + a + b + ab = (1 + a)(1 + b) = 0$
So $a = -1 \notin S$ or $b = -1 \notin S$
Associativity:
$a, b, c \in S, (a * b) * c = (a * b) + c + (a * b)c = (a + b + ab) + c + (a + b + ab)c = a + (b + c + bc) + a(b + c + bc) = a + (b * c) + a(b * c) = a * (b * c)$
Identity element:0;
$a \in S, a * 0 = a + 0 + a \times 0 = a$
Inverse:
For $a \in S$, the inverse element is $\frac{-a}{a+1}$
$a * \left(\frac{-a}{a+1}\right) = a + \frac{-a}{a+1} + a\left(\frac{-a}{a+1}\right) = \frac{a(a+1)-a-a^2}{a+1} = 0$
So $(S, *)$ is a group.
Commutativity:
$\forall a, b \in S, a * b = a + b + ab$
exchange the position of a, b.
for addition and multipliation on $mathbbR$ is commutative, so $\rightarrow b * a = b + a + ba = a + b + ab = a * b$
So $(S, *)$ is an abelian group.

题目 3 (TJ 3-39)

Let $\mathbb{T} = \{z \in \mathbb{C}^* : |z| = 1\}$. Prove that $\mathbb{T}$ is a subgroup of $\mathbb{C}^*$.

解答:

According to proposition 3.30:
1.Identity:
The identity of $\mathbb{C}^*$ is 1. And for $z \in \mathbb{T}$, we can suppose that $z = \cos x + i \sin x \rightarrow 1 \times z = 1 \times (\cos x + i \sin x) = \cos x + i \sin x = z$
So the identity of $\mathbb{T}$ is also 1.
2.We can suppose that $z_1, z_2 \in \mathbb{T}, z_1 = \cos x + i \sin x, z_2 = \cos y + i \sin y$
$z_1 z_2 = \cos x \cos y - \sin x \sin y + i(\cos x \sin y + \sin x \cos y) = \cos(x + y) + i \sin(x + y) =$

$z_3 \wedge |z_3| = 1 \to z_3 \in \mathbb{T}$
3.We can suppose that $z \in \mathbb{T}, z = \cos x + i \sin x$
$z^{-1} = \frac{\cos x - \sin xi}{\cos^2 x + \sin^2 x}$
$zz^{-1} = (\cos x + i \sin x)(\frac{\cos x - i \sin x}{\cos^2 x + \sin^2 x}) = \frac{\cos^2 x + \sin^2 x}{\cos^2 x + \sin^2 x} = 1$
$|z^{-1}| = \sqrt[2]{(\frac{\cos x}{\cos^2 x + \sin^2 x})^2 + (\frac{-\sin xi}{\cos^2 x + \sin^2 x})^2} = 1$
So $z^{-1} \in \mathbb{T}$.

题目 4 (TJ 3-42)

解答:
1.Identity:
The identity of G is $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
For $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H(a + d = 0)$
$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+0 & b+0 \\ c+0 & d+0 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$
So $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is the identity of H.
2.We can suppose that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Hand \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in H, (a + d = 0 \wedge x + w = 0)$
$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} a+x & b+y \\ c+z & d+w \end{pmatrix}$
We can know that $(a + x) + (d + w) = (a + d) + (x + w) = 0 + 0 = 0$
So $\begin{pmatrix} a+x & b+y \\ c+z & d+w \end{pmatrix} \in H$
3.Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $(a + d = 0)$ denoted by A;
$A^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$
And $\frac{d}{ad-bc} + \frac{a}{ad-bc} = \frac{a+d}{ad-bc} = \frac{0}{ad-bc} = 0$
So $A^{-1} \in H$

题目 5 (TJ 3-49)
Let a and b be elements of a group G. If $a^4b = ba$ and $a^3 = e$, prove that $ab = ba$.

解答:
According to the usual laws of exponents: $a^4 = a^3a$
$\to a^4b = a^3ab = (a^3)ab = eab = ab$
Since $a^4b = ba$, $\to ab = ba$

题目 6 (TJ 3-51)
If $xy = x^{-1}y^{-1}$ for all x and y in G, prove that G must be abelian.

解答:
According to proposition 3.19, $(ab)^{-1} = b^{-1}a^{-1}$
Since $b^{-1}, a^{-1} \in G$ and $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$, $\forall a, b \in G, ab = ba$
So G is abelian.

题目 7 (TJ 4-1)

解答:
(a)False.
Disprove:
According to the corollary 4.14.
The generators of $\mathbb{Z}_n$ are the integers r such that $1 \leq r < n$ and gcd(r,n)=1.
One of the generators is 49, and it is not prime.
(b)False.
Disprove:
The multipliation table for U(8):

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$|1| = 1$; $|3| = |5| = |7| = 2$
1, 3, 5, 7 are all not generator of U(8). (c)False.
We can assume that g is a generator of $\mathbb{Q}$, but it can not generat $g/2$.
(d)False.
Counterexample:S_3
The subgroup of S_3 are all cyclic, but S_3 is not.
(e) True.
Since an infinite group has infinite number of subgroups, we can know a group with a finite number of subgroup is finite.

题目 8 (TJ 4-24)
Let p and q be distinct primes. How many generators does $\mathbb{Z}_{pq}$ have?

解答:
We should find out how many r satisfying corollary 4.14.
因为 p, q 都是 distinct primes, 所以 $\varphi(pq) = \varphi(p)\varphi(q)$, 并且 $\varphi(p) = p-1, \varphi(q) = q-1$
$\varphi(p)\varphi(q) = (p-1)(q-1) = pq - p - q + 1$
(此处算法致谢 $https://blog.csdn.net/AgCl_LHY/article/details/107624346$)

题目 9 (TJ 4-12)
Find a cyclic group with exactly one generator. Can you find cyclic groups with exactly two generators? Four generators? How about n generators?

解答：
1 generator:$\mathbb{Z}_2$:1
2 generators:$\mathbb{Z}_3$:1,2
4 generators:$\mathbb{Z}_5$:1,2,3,4
n generators:
if(n>2 and n=1(mod 2)), then it is impossible.For that, if a is a generator, then a^{-1} must also be a generator.
If (n = 0(mod 2)):$\mathbb{Z}_m, m = \varphi(n)$

题目 10 (TJ 4-32)
Let G be a finite cyclic group of order n generated by x. Show that if $y = x^k$ where $gcd(k, n) = 1$, then y must be a generator of G.

解答：
According to TH 4.13.
The order of y is $n/gcd(k, n) = n$
So y is a generator of G.

---

2 作业（选做部分）

题目 1 (Z_p)
证明：设 p 为素数，则 $Z_p = \{1, 2, ..., p-1\}$ 关于 p **乘法**构成的 $p-1$ 阶循环群。（此处的 $1, 2, ..., p-1$ 是模 p 等价类的代表元）

解答：

题目 2 (SageMath 学习)
安装 SageMath，并学习 TJ 第三章 3.6 节、3.7 节；第四章 4.6 节、4.7 节关于 SageMath 的内容

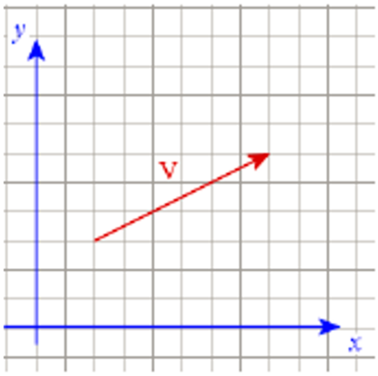
解答：

---

3 Open Topics

在二维平面上的“移动”（例如向东北 30 度移动 9 公里）。你能够以这些“移动”为元素构建一个群吗？

Open Topics 1 (“移动” 群-1)
- 它的几何元素和运算分别是什么？
- 它为什么符合群的定义？
- 它是阿贝尔群吗？为什么？



Open Topics 2 (“移动” 群-2)

- 你能找出它的一些子群吗? 并说明为什么找到的是子群
- 它是循环群吗? 如果是, 生成元是什么? 生成元唯一吗? 如果不是, 如何改造出一个循环群?
- 你能找出这个（改造后的）循环群的一些子群么? 它们是循环群么?

4 反馈