Algebra

中国科学技术大学代数讲义群论作业

我真的不懂忧郁

Delft University of Technology

TU Delft

Algebra

中国科学技术大学代数讲义群论作业

by

我真的不懂忧郁

Student Name	Student Number
First Surname	1234567

Instructor:	I. Surname
Teaching Assistant:	I. Surname
Project Duration:	Month, Year - Month, Year
Faculty:	Faculty of Aerospace Engineering, Delft

Preface

A preface...

我真的不懂忧郁

Delft, August 2024

Summary

A summary...

目录

Nomenclature

If a nomenclature is required, a simple template can be found below for convenience. Feel free to use, adapt or completely remove.

Abbreviations

Abbreviation	Definition
ISA	International Standard Atmosphere
...	

Symbols

Symbol	Definition	Unit
V	Velocity	[m/s]
...		
ρ	Density	[kg/m^3]
...		

Chapter 1

Group theory

1.1. 回顾

1. **群的定义**: 由一个集合以及其上的一个二元运算 $(G, \cdot)$ 构成，运算满足结合律，并存在单位元和逆元；
$$(G, \cdot) \xrightarrow{\text{结合律}} semigroup \xrightarrow{\text{单位元}} monoid \xrightarrow{\text{逆元}} Group \tag{1.1}$$
2. **有限群**：群的元素个数有限，其元素个数称为群的**阶**；
3. **交换群/*Abelian* 群**：群上运算满足交换律；
4. **循环群**：循环群是由单个元素生成的群，由 $< g >$ 表示，其中每个元素都是 g 的整数次幂。g 称为循环群的**生成元**。
5. **生成元的阶**：元素 g 的阶 n 是循环了多少次幂回到单位 e，$g^n = e$；
6. **最大公约数条件**：元素 g 是 G 的生成元，当且仅当 $gcd(k, n) = 1$，其中 k 满足 $g = g^k$，n 为生成元阶数。
7. **无限循环群**：$\mathbb{Z}$ 是一个无限循环群，生成元为 1 或者 -1

1.2. 模 m 剩余群

模 m 剩余类是将所有的整数根据 m 取模后的结果进行分类。每个整数 a 可以对应一个剩余类

$$[a]_m := \{x \in \mathbb{Z} \mid x \equiv a \mod m\} \tag{1.2}$$

换句话说，整数 x 和 a 同余于模 m，如果他们的差值能被 m 整除，即 $x - a = km, \exists k \in \mathbb{Z}$。模 m 剩余类可以定义乘法

$$[a]_m \times [b]_m = [a \times b]_m \tag{1.3}$$

模 m 剩余群是由模 m 剩余类中与 m 互素的整数在乘法下构成的群。即

$$\mathbb{Z}_m^\times = \{\ [a] \mid 1 \leqslant a < n, gcd(a, m) = 1\} \tag{1.4}$$

为什么要求互素呢？因为根据群要求，群中的元素必须存在逆元。如果 a 与 m 不互素，

$$gcd(a,m) > 1 \tag{1.5}$$

假设 $[a]$ 的逆元为 $[b]_m \in \mathbb{Z}_m^\times$

$$[a]_m \times [b]_m = [a \times b]_m = [1]_m \tag{1.6}$$

即

$$a \times b \equiv 1 \mod m \tag{1.7}$$

即

$$\begin{aligned} & a \times b = sm + 1 \\ & 1 = tm + 1 \\ & \Rightarrow (a \times b) = km + 1 \end{aligned} \tag{1.8}$$

也就是要找到 (b,k) 使得上式子成立，稍微做变化

$$a \times b + (-k) \times m = 1 \tag{1.9}$$

这说明了 $gcd(a,m) = 1$，才能找到 (b,k)[1]。但是假设是不互素，因此该方程是无解的。

1.3. Exescrise 1

parctice 2.1： 证明 $Map(A,G)$ 是群。

1. 结合律：$(fg)h(\alpha) = f(\alpha)g(\alpha)h(\alpha) = f(\alpha)gh(\alpha)$;
2. 单位元：如果存在单位元 $1 \in M(A,G)$，则 $\forall f \in M(A,G)$，$1 \cdot f = f$，令 $\forall \alpha \in A$，$1(\alpha) = e$，其中 e 是群 G 的单位元，所以 $\forall \alpha \in A$，

$$1 \cdot f(\alpha) = 1(\alpha)f(\alpha) = e \cdot f(\alpha) = f(\alpha) \tag{1.10}$$

3. 逆元：$e \in G$ 是群 G 的单位元，对于所有的 $x \in G$，存在逆元 $x^{-1} \in G$，设 $f(\alpha) = x$，$g(\alpha) = -x$，

$$f(\alpha) \cdot g(\alpha) = fg(\alpha) = x \cdot x^{-1} = e \tag{1.11}$$

所以 g 和 f 互为逆元。

lemma 1.3.1: 保距映射的逆映射也是保距映射

proof. 如果 $f : X \to Y$ 是保距映射，$d_X : X \times X \to \mathbb{R}$ 是 X 上的度量，$d_Y : Y \times Y \to \mathbb{R}$ 是 Y 上的度量。

$$d_X(\alpha,\beta) = d_Y(f(\alpha), f(\beta)),\ \forall \alpha,\beta \in X \tag{1.12}$$

[1]这里只说明了必要性，充分性是如果方程有解，则 $gcd(a,m) = 1$，如果方程有解但是 a 和 m 不互素，那么就会有 $k_1a + k_2m = d$ 是最大公约数，由于 $ba + km = 1$ 满足，这说明了 d 必然是 1 的约数，但是 1 的约数只能是 1

若 $f^{-1}: Y \to X$ 是 f 的逆映射，对于 $\forall\, f(\alpha), f(\beta) \in Y$

$$d_Y(f^{-1}f(\alpha), f^{-1}f(\beta)) = d_X(\alpha, \beta) \tag{1.13}$$

所以逆映射也保距。

parctice 2.2 证明保距映射都是双设，且所有保距映射在函数复合意义下都构成群。

假设 $d_X(\cdot,\cdot)$ 是 X 上的度量，$f: X \to Y$ 是 X 上的保距映射，$d_Y(\cdot,\cdot)$ 是 Y 上的度量，意思是 $\forall\, x, y \in X$，$d_X(x, y) = d_Y(f(x), f(y))$

1. 证明 f 是单射；

   如果 f 是单射，即 $\forall f(x_1) = f(x_2)$，$x_1 = x_2$。由于 $d_Y(f(x_1), f(x_2)) = 0 \to d_X(x_1, x_2) = 0 \to x_1 = x_2$。

2. 证明 f 是满射，即对于任意的 $y \in Y$，存在至少一个 $x \in X$，使得 $f(x) = y$。

   假设存在一点 $y_0 \in Y$，使得对于所有的 $x \in X$，$f(x) \neq y_0$。由于 f 是保距映射，所以 $f(X) \in Y$，对于所有的 $y \in f(X)$，使得 $\exists x \in X, f(x) = y$，度量为

   $$d_Y(y, y_0) \tag{1.14}$$

   由于保距映射的逆映射也是保距映射，所以必存在一点 $x_0 \in X$，使得

   $$d_X(x, x_0) = d_Y(y, y_0) \tag{1.15}$$

   这假设矛盾。故 f 是满射。

综上所述，f 是双射。

parctice 2.3. G 是群，$x, y \in G$

1. 证明 $(x^{-1})^{-1} = x$，设 $e \in G$ 是单位元

$$\begin{aligned} &(x^{-1}) \cdot (x^{-1})^{-1} = e \\ &\Rightarrow x \cdot x^{-1} \cdot (x^{-1})^{-1} = x \\ &\Rightarrow e \cdot (x^{-1})^{-1} = x \\ &\Rightarrow (x^{-1})^{-1} = x \end{aligned} \tag{1.16}$$

2. 证明 $(xy)^{-1} = y^{-1}x^{-1}$

$$\begin{aligned} &(xy)^{-1}(xy) = e \\ &(xy)^{-1}xyy^{-1} = y^{-1} \\ &(xy)^{-1}xe = y^{-1} \\ &(xy)^{-1}x = y^{-1} \\ &(xy)^{-1} = y^{-1}x^{-1} \end{aligned} \tag{1.17}$$

parctice 2.6. 证明如果 A 是 $(G, \cdot)$ 的子群，B 是 $(H, +)$ 的子群，则 $A \times B$ 是 $G \times H$ 的子群，但是不是所有 $\mathbb{Z} \times \mathbb{Z}$ 的子群都能如此得到。

1. 证明 $A \times B$ 是 $G \times H$ 的子群。定义群运算为 $\times = (x_1 \cdot x_2, y_1 + y_2)$

   (a) 封闭性：取 $(a_1, b_1), (a_2, b_2) \in A \times B$，其中 $a_1, a_2 \in A$，$b_1, b_2 \in B$，由于 A 和 B 是 G 和 H 的子群，所以

$$\begin{aligned} &a_1 \cdot a_2 \in A \\ &b_1 + b_2 \in B \end{aligned} \tag{1.18}$$

   所以 $(a_1, b_1) \times (a_2, b_2) = (a_1 \cdot a_2, b_1 + b_2) \in A \times B$

   (b) 单位元：e 是 G 中单位元，0 是 H 中单位元，容易证明 $(e, 0)$。

2. 并未所有的子群都能表示为群的笛卡尔积。例如

$$H = \langle (2, 3) \rangle = \{(2n, 3n) | n \in \mathbb{Z}\} \tag{1.19}$$

practice 2.9 令 G 是 n 阶有限群，$a_1, a_2, \cdots, a_n$ 是群 G 的任意 n 个元素，不一定两两不同，证明：存在整数 p, q，$1 \leqslant p \leqslant q \leqslant n$，使得

$$a_p a_{p+1} \cdots a_q = 1 \tag{1.20}$$

proof. 由于 G 是一个群，因此满足封闭性，1 是其上单位元。令

$$s_k = a_1 a_2 \cdots a_k \tag{1.21}$$

构造出序列 $\{s_k\}$。显然每个 s_k 都属于 G，由于 G 的阶数是 n，因此最多能取 $s_1, s_2, \cdots, s_n$ 共 n 个不同值。又由于单位元 1 占了一个位置，根据**鸽巢原理**，因此必然存在 $1 \leqslant p \leqslant q \leqslant 1$，$s_q = s_p$，即

$$1 = (a_1 a_2 \cdots a_p)^{-1}(a_1 a_2 \cdots a_p) = (a_1 a_2 \cdots a_p)^{-1}(a_1 a_2 \cdots a_q) = a_p a_{p+1} \cdots a_q \tag{1.22}$$

practice 2.10 证明在偶数阶群 G 中，方程 $x^2 = 1$ 总有偶数个解

proof. $x \in G$，1 是 G 中的单位元，所以方程的解满足 $x = x^{-1}$。我们要证明满足方程的解的总数为偶数个。

1. 首先单位元 1 肯定是方程的解：$1^2 = 1$；
2. 如果 $x \neq 1$，那么需要满足 $x = x^{-1}$，这时有两种情况：如果 $x \neq x^{-1}$，则它们成对出现，是为偶数；如果 $x = x^{-1}$，则 $x \neq 1$ 的情况下只能有奇数个这样的 x，因为如果是偶数个，加上 1 一共就会有奇数个，再加上 $x \neq x^{-1}$ 的偶数个，则整个群 G 的阶数就是奇数个，不满足偶数阶群的条件。

综上所述，$x^2 = 1$ 总有偶数个 G 中的解。

parctice 2.13 设 A 和 B 分别是群 G 的两个子群，试证：$A \cup B$ 是 G 的子群当且仅当 $A \leqslant B$ 或 $B \leqslant A$，利用这个事实证明：群 G 不能表为两个真子群的并。

proof. 假设 $A \cup B$ 是 G 的子群，$A \cap B \neq \emptyset$ 但互不存在包含关系，$\forall\, x \in A, y \in B$，$xy \in A \cup B$，我们可以假设 $xy \in B$，因为 $y \in B$，故逆元 $y^{-1} \in B \subseteq A \cup B$

$$B \ni (xy)y^{-1} = xe = x \tag{1.23}$$

这与 $x \in A$ 矛盾。

practice 2.14 设 A, B 是群 G 的两个子群，试证明 AB 是 G 的子群当且仅当 $AB = BA$。

proof. $AB = \{ xy \mid \forall x \in A, \forall y \in B \}$。$A, B$ 是群 G 的子群，则满足结合律，则对于所有的 $xy \in AB$，其中 $x \in A, y \in B$

$$(xy)(xy) \in AB \tag{1.24}$$

所以

$$x(yx)y \in AB \tag{1.25}$$

所以

$$(ex)(yx)(ye) \in AB \tag{1.26}$$

因为 $ex, yx, ye \in BA$，所以

$$(ex)(yx)(ye) \in BA \tag{1.27}$$

所以

$$(xy) \in BA \tag{1.28}$$

由 xy 的选取任意

$$AB = BA \tag{1.29}$$

practice 2.15. 设 A 和 B 是有限群 G 的两个非空子集，如果 $|A| + |B| > |G|$，证明 $G = AB$。特别地，如果 S 是 G 的一个子集，$|S| > |G|/2$，证明 $\forall g \in G$，存在 $a, b \in S$ 使得 $g = ab$。

首先解决第一个证明：

1. $AB \subset G$ 是明显的，因为如果存在 $x \in AB, x \notin G$, 则存在 $a, b \in G$，$ab = x \notin G$，这就不满足群的封闭性。
2. 下面证明 $G \subset AB$。

   $\forall x \in G$，$x \notin AB$，$ab = x \notin AB$，$a, b \in G$, $a, b \notin A, B$，就是说 a, b 只能在 $G - (A \cup B)$ 中。又由于

$$|A| + |B| > |G| \tag{1.30}$$

   所以 $G - (A \cup B) = \emptyset$，所以有矛盾。

综上所述，$G = AB$。

在解决第二个：
如果 S 是 G 的一个子集，对 $\forall g \in G$，由第一个证明，$G = S^2$，所以存在 $a, b \in S$，$g = ab$

parctice 2.16. 确定 $\mathbb{Z}$ 的所有子群

整数群 Z 是一个无限的循环群，其生成元为 $\{1\}$ 者 $\{-1\}$ 整数群的子群具有非常规整的结构：每一个子群都是由某个整数生成的。

所以任意 $\{n\mathbb{Z}|n \in \mathbb{N}\}$ 和 $\{0\}$ 都是 $\mathbb{Z}$ 的子群。

Question 1: 证明循环群的最大公约数条件。

1. 充分性：$gcd(k, n) = 1 \Rightarrow g^k$ 是生成元；

$$g^1 = g^{\alpha k + \beta n} = (g^k)^\alpha (g^n)^\beta = \underbrace{g^\alpha \cdots g^\alpha}_{k} \cdot e = (g^k)^\alpha \tag{1.31}$$

即 g 是 g^k 的某个幂次，所以 g^k 是生成元。

2. 必要性：g^k 是生成元 $\Rightarrow gcd(k, n) = 1$；

如果 g^k 是生成元，$g^n = e$，所以 $g^{n+1} = g$，所以 $\forall\, s \in \mathbb{N}$，$k = sn + 1$，$g^k = g$，

$$gcd(k, n) = gcd(sn + 1, n) = 1 \tag{1.32}$$

parctice 2.17. 证明：映射 $f : G \to G, a \to a^{-1}$ 是 G 的自同构当且仅当 G 是 $Abelian$ 群。

$\forall\, a, b \in G$，

$$f(ab) = (ab)^{-1} = b^{-1}a^{-1} \tag{1.33}$$

根据群同态的定义

$$f(ab) = f(a)f(b) = a^{-1}b^{-1} \tag{1.34}$$

上面两式要相等当且仅当

$$a^{-1}b^{-1} = b^{-1}a^{-1} \tag{1.35}$$

即 G 是 $Abelian$ 群。

parctice 2.19. 对于下面的每一种情形，确定 G 是否同构于 H 和 K 的积

注意群同构的要求是群同态的同时并且是满射。

1. $G = \mathbb{R}^\times$，$H = \{\pm 1\}$，$K = \mathbb{R}^\times_+$，其中 $\mathbb{R}^\times_+$ 为正实数构成的乘法群；

设 $f : H \times K \to G$，$\forall\, (h, k) \in H \times K, h \in H, k \in K$，

$$f((h, k)) := h \times k \in G \tag{1.36}$$

证明 $f((h_1, k_1)(h_2, k_2)) = f((h_1, k_1))f((h_2, k_2))$。假设已经定义了 $H \times K$ 中运算使得下面运算合理

$$f((h_1, k_1)(h_2, k_2)) = f((h_1h_2, k_1, k_2)) = h_1h_2 \times k_1k_2 \tag{1.37}$$

由于 G 是 $Abelian$ 群，所以

$$h_1h_2 \times k_1k_2 = (h_1 \times k_1) \times (h_2 \times k_2) = f((h_1, k_1))f((h_2, k_2)) \tag{1.38}$$

即 f 是群同态。由于 $f((-1,0))$ 和 $f((1,0))$ 映射到 G 中的值都是 0，因此不是双射，所以不是群同构。

2. $G = B_n(F)$，$H = Diag_n(F)$，$K = T_n(K)$；
3. $G = \mathbb{C}^\times$，$H = S^1$，$K = \mathbb{R}_+^\times$

parctice 2.20. 证明有理数加法群 $\mathbb{Q}$ 和乘法群 $\mathbb{Q}^\times$ 不同构

parctice 2.21.

parctice 2.22.

Question 2: 若 G 为无限群，则 G 的生成元为 g 或者 g^{-1}

proof. g^α 是 G 的生成元当且仅当存在 $\beta \in \mathbb{Z}$，$g = g^{\alpha\beta}$。如果 G 为无限去，则 $\alpha\beta = 1$，故 $\alpha = \pm 1$。

1.4. Exescrise 2: 陪集, 群同态基本定理

1. **指数**：群 G 关于子群 H 的指数 $(G : H)$ 是指 G 关于 H 的陪集代表元的个数；
2. **陪集**：对 $a \in G$，集合 $aH = \{ ah \mid h \in H \}$ 称为 G 关于 H 的**右陪集**，$Ha = \{ ha \mid h \in H \}$ 称为 G 关于 H 的**左陪集**，a 称为 G 的**陪集代表元**。$\{a_i | i \in I\}$ 为陪集代表元系当且仅当

$$G = \bigcup_{i \in I} Ha_i \ (or \bigcup_{i \in I} a_i H) \tag{1.39}$$

为 G 的**分拆**。

Question 3: 设 G 为循环群

1. 如果 G 为有限群，则其阶为 n，则 $G \cong \mathbb{Z}/n\mathbb{Z}$；
2. 如果 G 为无限群，则 $G \cong \mathbb{Z}$

Question 4: 已知循环群 G 的阶和生成元 g，对元素 $a \in G$，如何求 a 关于 g 的离散对数？

lemma 1.4.1: 陪集 aH 和 bH 要么不交，要么重合，且 $aH = bH$ 当且仅当 $b^{-1}a \in H$（或 $a^{-1}b \in H$）。

***proof*.**

只要证明 $\forall\ h \in H$，$ah \in bH$，$bh \in aH$。如果 $aH \cap bH \neq \emptyset$，则存在 $ah_1 = bh_2$，则 $b^{-1}a = h_2h_1^{-1} \in H$，则 $\forall h \in H$

$$\begin{aligned} ah &= ah_1(h_1^{-1}h) = bh_2(h_1^{-1}h) \in bH \\ bh &= bh_2(h_2^{-1}h) = ah_1(h_2^{-1}h) \in aH \end{aligned} \tag{1.40}$$

故 $aH = bH$。引理说明的是右陪集的情形，左陪集也是等价的。

> **theorem 1.4.2:** *(拉格朗日定理).* 如果 G 为有限群，则 $|G| = |H| \cdot (G \cdot H)$

***proof*.**

$$|G| = \sum_{i \in I} |a_i H| = \underbrace{\sum_{i \in I} |H|}_{|I|\text{个}} = (G : H) \cdot |H| \tag{1.41}$$

> **Question 5:** *(费马小定理)* 设 p 是素数，则对所有与 p 互素的整数 a，
>
> $$a^{p-1} \equiv 1 \mod p \tag{1.42}$$

References

[1] I. Surname, I. Surname, and I. Surname. "The Title of the Article". In: *The Title of the Journal* 1.2 (2000), pp. 123–456.

Chapter A

Source Code Example

Adding source code to your report/thesis is supported with the package listings*. An example can be found below. Files can be added using* \lstinputlisting[language=<language>]{<filename>}.

```python
"""
ISA Calculator: import the function, specify the height and it will return a
list in the following format: [Temperature,Density,Pressure,Speed of Sound].
Note that there is no check to see if the maximum altitude is reached.
"""

import math
g0 = 9.80665
R = 287.0
layer1 = [0, 288.15, 101325.0]
alt = [0,11000,20000,32000,47000,51000,71000,86000]
a = [-.0065,0,.0010,.0028,0,-.0028,-.0020]

def atmosphere(h):
    for i in range(0,len(alt)-1):
        if h >= alt[i]:
            layer0 = layer1[:]
            layer1[0] = min(h,alt[i+1])
            if a[i] != 0:
                layer1[1] = layer0[1] + a[i]*(layer1[0]-layer0[0])
                layer1[2] = layer0[2] * (layer1[1]/layer0[1])**(-g0/(a[i]*R))
            else:
                layer1[2] = layer0[2]*math.exp((-g0/(R*layer1[1]))*(layer1[0]-layer0[0]))
    return [layer1[1],layer1[2]/(R*layer1[1]),layer1[2],math.sqrt(1.4*R*layer1[1])]
```

Chapter B

Task Division Example

If a task division is required, a simple template can be found below for convenience. Feel free to use, adapt or completely remove.

表 **B.1:** Distribution of the workload

	Task	Student Name(s)
	Summary	
Chapter 1	Introduction	
Chapter 2		
Chapter 3		
Chapter *		
Chapter *	Conclusion	
	Editors	
	CAD and Figures	
	Document Design and Layout	