抽象代数

学习辅导

孟道骥　陈良云
徐丽媛　李小蓉　编著

科学出版社

抽象代数学习辅导

孟道骥　陈良云
徐丽媛　李小蓉　编著

科学出版社

内 容 简 介

抽象代数(或近世代数)是数学的一个基础学科，也是数学及相关专业的基础课程. 南开大学抽象代数课程的改革是陈省身先生生前倡导的南开大学数学专业教学改革的一部分，该课程是国家精品课程. 该课程的教材《代数学基础》修订、补充而成《抽象代数 I——代数学基础》. 内容包括基本概念、环、域、群、模和 Galois 理论六部分. 本书给出《抽象代数 I——代数学基础》习题的全部解答，也给出在教学中积累的许多重要、有趣的题目的解答. 有的题目给出多种解答，有的题目给出一些注解.

本书可作为抽象代数课程的辅助教材.

图书在版编目(CIP)数据

抽象代数学习辅导/孟道骥等编著. —北京：科学出版社，2013
ISBN 978-7-03-036792-1

Ⅰ. 抽… Ⅱ. 孟… Ⅲ. 抽象代数—高等学校—教学参考资料
Ⅳ. O153

中国版本图书馆 CIP 数据核字(2013) 第 037831 号

责任编辑：王 静／责任校对：鲁 素
责任印制：阎 磊／封面设计：陈 敬

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

北京市文林印务有限公司 印刷
科学出版社发行 各地新华书店经销
*
2013 年 3 月第 一 版 开本：720×1000 B5
2013 年 3 月第一次印刷 印张：13 1/2
字数：263 000

定价：33.00 元

(如有印装质量问题，我社负责调换)

前　言

1986 年南开大学数学试点班建立后, 在陈省身先生的指导下, 学校对试点班的教学进行了改革和建设. 我有幸为试点班讲授抽象代数课, 能自由地按照自己的一些想法授课, 并将讲稿整理为讲义. 后来我又去给试点班讲授微分几何、高等代数与解析几何以及其他课程. 抽象代数课程的教材《代数学基础》出版后我再也没有教过这门课程, 也没有用这本书上过课. "不在其位, 不谋其政." 话虽如此, 但仍有同学来问问题, 其中有的问题据说是 "没意义的" 而没有被留为作业的题. 当然问过了也就过去了. 近几年, 在读者和陈良云、史毅茜和白瑞蒲老师敦促下将《代数学基础》进行较大修订, 改版为由本人、陈良云、史毅茜和白瑞蒲合著的《抽象代数 I—— 代数学基础》, 在科学出版社重新出版. 有不少读者希望该书配套习题解答, 而且有老师告诉我在网上有《代数学基础》的习题解答, 有的还说是我写的.

首先, 我要感谢写过解答的朋友对此书的关注和为解答习题所付出的劳动; 其次, 我也不敢, 也不应该冒领这些朋友们的功劳.

我看了一些解答, 感觉有的解答太过简单, "显然", "容易证明", "同理可证" 等词语相当多, 读起来较费解; 有的题没有解答; 个别解答还有待商榷.

为答谢各位的关怀, 也因为退休后时间比较充裕, 更主要是在陈良云教授敦促下, 我决定做做这些习题, 并公诸于众, 以飨读者. 虽退休后时间较多, 但精力不如以前, 这是不必讳言的事实. 要如年轻人一样来做习题是相当困难的. 苍天有眼, 陈良云、徐丽媛和李小蓉三位老师愿意同我合作来完成我的这个心愿.

当然, 学习不能只限于书本的知识和完成书本上的习题, 因此我除给出教材中的习题的解答外, 还给出一些补充题. 补充题可以扩展书本知识的不足, 激发学习的热情, 培养数学研究的能力. 例如, 在 3.6 节代数学基本定理中原来没有安排习题, 我们在补充题中介绍用复变函数的观点证明此定理的方法. 又如在 4.9 节点群中原先也没有安排习题, 我们在补充题中介绍关于点群应用的几个题目.

衷心感谢帮助过我们的许多老师和同学以及我们所在单位对我们的大力支持.

虽然我们尽了很大努力编写本书, 但一则由于水平所限, 二则数学的教学总是在不断发展, 因而本书的欠缺和不足肯定存在, 诚恳希望大家不吝指正.

孟道骥

2012 年冬于南开大学西南村

目　录

第1章　基本概念

1.1　二元运算与同余关系

习题 1　试问下列关系是否为等价关系, 并验证:

1) 在 $\mathbf{R}$ 中, $x\,R\,y$, 若 $x \geqslant y$;

2) 在 $\mathbf{R}$ 中, $x\,R\,y$, 若 $|x| = |y|$;

3) 在 $\mathbf{R}$ 中,$x\,R\,y$, 若 $|x - y| \leqslant 3$;

4) 在 $\mathbf{Z}$ 中,$x\,R\,y$, 若 $x - y$ 为奇数;

5) 在 $\mathbf{C}^{n\times n}$(复数域 $\mathbf{C}$ 上 n 阶方阵的集合) 中, $\boldsymbol{A}\,R\,\boldsymbol{B}$, 若有可逆矩阵 $\boldsymbol{P},\boldsymbol{Q}$, 使 $\boldsymbol{A} = \boldsymbol{PBQ}$;

6) 在 $\mathbf{C}^{n\times n}$ 中, $\boldsymbol{A}\,R\,\boldsymbol{B}$, 若有矩阵 $\boldsymbol{P},\boldsymbol{Q}$, 使 $\boldsymbol{A} = \boldsymbol{PBQ}$;

7) 在 $\mathbf{C}^{n\times n}$ 中, $\boldsymbol{A}\,R\,\boldsymbol{B}$, 若有可逆矩阵 $\boldsymbol{P}$, 使 $\boldsymbol{A} = \boldsymbol{P}^{-1}\boldsymbol{BP}$.

解　1) 不是. $3\,R\,2$, 但 $2\not R\,3$.

2) 是.

3) 不是. $|3 - 0| = 3$, $|6 - 3| = 3$, 但 $|6 - 0| = 6 > 3$.

4) 不是. $x - x = 0$ 不是奇数. $x - y$, $y - z$ 是奇数, 则 $x - z$ 是偶数.

5) 是.

6) 不是. $\boldsymbol{O} = \boldsymbol{OAO}$, $\forall \boldsymbol{A} \in \mathbf{C}^{n\times n}$. 但 $\boldsymbol{A} \neq \boldsymbol{O}$ 时, $\boldsymbol{A} \neq \boldsymbol{POQ}$.

7) 是. □

习题 2　假设 R 是非空集合 A 中的一个关系, 且有对称性和传递性. 有人断定 R 是一个等价关系, 其推理如下:

"对 $a,b \in A$, 从 $a\,R\,b$ 得 $b\,R\,a$, 又从传递性得 $a\,R\,a$, 因而 R 有自反性, 故为等价关系."

他的推理对吗?

解　其推理是不对的. 因为可能存在元素 a_0 使得 $\forall a \in A$, $a_0\not R\,b$. 此时就得不到 $a_0\,R\,a_0$. 例如, 在 $\mathbf{C}$ 上定义 $a\,R\,b$ 为 $ab \neq 0$, 此时 $0\not R\,0$. □

注　如果在这两个条件之外, 再加上条件: $\forall a \in A$, 存在 $a' \in A$ 使得 $a\,R\,a'$, 就可得到 R 为等价关系.

习题 3　设 R 是非空集合 A 中任一关系, 再定义 A 中关系 R_1,R_2 分别为

xR_1y, 当 $x = y$, $x\,R\,y$ 与 $y\,R\,x$ 三者之一成立;

$x\,R_2\,y$, 若有 $x_0, x_1, \cdots, x_n$ 使 $x_0 = x$, $x_n = y$ 且

$$x_0\,R_1\,x_1,\ x_1\,R_1\,x_2,\ \cdots,\ x_{n-1}\,R_1\,x_n.$$

1) 证明 R_2 是一个等价关系;

2) 证明若 R 是等价关系, 则 $R_2 = R$, 即 $x\,R_2\,y$ iff $x\,R\,y$;

3) 令 $A = \mathbf{Z}$, n 为一固定整数,R 定义为 $x\,R\,y$, 当 $x - y = n$. 求关系 R_1 与 R_2.

证　1) 因为 $x = x$, 于是 xR_1x. 又取 $n = 1$, 由 $x = x_0 = x_1 = x$, 于是 xR_2x.

注意, 由 aR_1b, 有或 $a = b$, 或 aRb, 或 bRa. 于是 bR_1a.

因此, 若 $x\,R_2\,y$ 即有 $x_0, x_1, \cdots, x_n$, 使 $x_0 = x$, $x_n = y$, 且

$$x_0\,R_1\,x_1,\ x_1\,R_1\,x_2,\ \cdots,\ x_{n-1}\,R_1\,x_n,$$

则有 $y = x_n\,R_1\,x_{n-1},\ x_{n-1}\,R_1\,x_{n-2},\ \cdots,\ x_1R_1\,x_0 = x$, 故 $y\,R_2\,x$.

若 $x\,R_2\,y$, $y\,R_2\,z$, 则有

$$x = x_0\,R_1\,x_1,\ x_1\,R_1\,x_2,\ \cdots,\ x_{n-1}\,R_1\,x_n = y,$$
$$y = y_0\,R_1\,y_1,\ y_1\,R_1\,y_2,\ \cdots,\ y_{m-1}\,R_1\,y_m = z.$$

令

$$\begin{cases} z_i = x_i, & i = 0, 1, \cdots, n, \\ z_{n+j} = y_j, & j = 0, 1, \cdots, m. \end{cases}$$

于是

$$x = z_0\,R_1\,z_1,\ z_1\,R_1\,z_2,\ \cdots,\ z_{n+m-1}\,R_1\,z_{n+m} = z,$$

因此 $x\,R_2\,y$.

故 R_2 是等价关系.

2) 若 R 是等价关系, 显然 $R = R_1$. 因为 $x\,R_1\,y$ 当且仅当 $x\,R\,y$, 所以 $x\,R\,y$, 有 $x\,R_2\,y$. 于是有

$$x = x_0\,R_1\,x_1,\ x_1\,R_1\,x_2,\ \cdots,\ x_{n-1}\,R_1\,x_n = y,$$

即

$$x = x_0\,R\,x_1,\ x_1\,R\,x_2,\ \cdots,\ x_{n-1}\,R\,x_n = y,$$

由 R 是等价关系, 知 $x\,R\,y$, 所以 $R_2 = R$.

3) $a, b \in \mathbf{Z}$, 如果 $a\,R_1\,b$, 则有 $a - b = 0$, 或 $a - b = n$, 或 $a - b = -n$. 故 $x\,R_2\,y$, 即有

$$x = x_0\,R_1\,x_1,\ x_1\,R_1\,x_2,\ \cdots,\ x_{n-1}\,R_1\,x_n = y.$$

当且仅当

$$x-y=(x-x_1)+(x_1-x_2)+\cdots+(x_{n-1}-y)=mn,\quad m\in\mathbf{Z},$$

当且仅当 $n|(x-y)$. □

习题 4 试问下面的二元运算 $*$ 哪些满足交换律, 哪些满足结合律?

1) 在 $\mathbf{Z}$ 中,$a*b=a-b$;

2) 在 $\mathbf{Q}$(有理数的集合) 中, $a*b=ab+1$;

3) 在 $\mathbf{Q}$ 中, $a*b=ab/2$;

4) 在 $\mathbf{N}$ 中,$a*b=2^{ab}$;

5) 在 $\mathbf{N}$ 中,$a*b=a^b$.

解 1) 交换律与结合律都不成立.

2) 交换律成立, 结合律不成立.

3) 交换律与结合律都成立.

4) 交换律成立, 结合律不成立.

5) 交换律与结合律都不成立. □

习题 5 设 $m\in\mathbf{Z}$, $m\neq 0$. 在 $\mathbf{Z}$ 中定义关系 $\sim$, $a\sim b$, 若 $a\equiv b(\mathrm{mod}\, m)$. 将对此关系的商集合记为 $\mathbf{Z}_m$(或 $\mathbf{Z}/m\mathbf{Z}$). 试求:

1) $\mathbf{Z}_m$ 中元素个数;

2) 由 $\mathbf{Z}$ 导出的 $\mathbf{Z}_3$ 的加法和乘法;

3) 由 $\mathbf{Z}$ 导出的 $\mathbf{Z}_6$ 的加法和乘法.

解 1) 由例 1.1.1[①] 知, $\sim$ 对加法、乘法都是同余关系. 对任一 $n\in\mathbf{Z}$, 有

$$n=mq+r,\quad q,r\in\mathbf{Z},\ 0\leqslant r\leqslant m-1.$$

于是 $\mathbf{Z}_m$ 中有 m 个元素.

2) 由 1), $\mathbf{Z}_3$ 有以 0, 1, 2 为代表元的同余类 $\bar{0}$, $\bar{1}$, $\bar{2}$. 易得

$$\bar{0}+\bar{0}=\bar{0},\bar{0}+\bar{1}=\bar{1},\bar{0}+\bar{2}=\bar{2},\bar{1}+\bar{1}=\bar{2},\bar{1}+\bar{2}=\bar{0},\bar{2}+\bar{2}=\bar{1};$$

$$\bar{0}\bar{0}=\bar{0},\ \bar{0}\bar{1}=\bar{0},\ \bar{0}\bar{2}=\bar{0},\ \bar{1}\bar{1}=\bar{1},\ \bar{1}\bar{2}=\bar{2},\ \bar{2}\bar{2}=\bar{1}.$$

3) 由 $\mathbf{Z}$ 导出的 $\mathbf{Z}_6$ 的加法和乘法如下两个表.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

□

①孟道骥, 陈良云, 史毅茜, 白瑞蒲. 2010. 抽象代数 I—— 代数学基础. 北京: 科学出版社

1.2　幺半群　群

习题 1　验证下列集合及所给的二元运算 $*$ 是否合理. 若合理, 问哪些是半群、幺半群、群, 或三种都不是?

1) $\mathbf{Z}$, $a*b=ab$;

2) $\mathbf{Z}$, $a*b=a-b$;

3) $\mathbf{R}^+=\{x\in\mathbf{R}|x>0\}$, $a*b=ab$;

4) $\mathbf{Q}\setminus\{0,1\}$, $a*b=ab$;

5) $[0,1]$, $a*b=\delta_{1a}b+\delta_{1b}a-\delta_{1a}\delta_{1b}$. 其中,

$$\delta_{1a}=\begin{cases}0, & a\neq 1,\\ 1, & a=1.\end{cases}\qquad \delta_{1b}=\begin{cases}0, & b\neq 1,\\ 1, & b=1.\end{cases}$$

6) $\mathbf{Z}$, $a*b=a+b-ab$.

解　1) 以 1 为幺元的幺半群, 而不是群, 因为 0 不可逆.

2) 运算定义合理, 但不是半群, 因结合律不成立.

3) 以 1 为幺元的群.

4) 运算定义不合理, 因为 $2*\dfrac{1}{2}\notin\mathbf{Q}\setminus\{0,1\}$.

5) 注意

$$0*b=b*0=0,\quad 1*b=b*1=b,$$
$$a*b=b*a=\delta_{1b}a,\quad a\neq 0,1.$$

于是 $b*c=1$ 当且仅当 $b=c=1$, 由此可得

$$0*(b*c)=(0*b)*c=0,\quad 1*(b*c)=(1*b)*c=b*c.$$

当 $a\neq 0,1$ 时,

$$a*(b*c)=\delta_{1\,b*c}a=\delta_{1\,b}\delta_{1\,c}a,\quad (a*b)*c=\delta_{1\,b}\delta_{1\,c}a,$$

因此 $([0,1],*)$ 是以 1 为幺元的交换幺半群, 但不是群.

6) 设 $a,b,c\in\mathbf{Z}$, 于是

$$(a*b)*c=(a*b)+c-(a*b)c=a+b+c-(ab+bc+ac)+abc,$$
$$a*(b*c)=a+(b*c)-a(b*c)=a+b+c-(ab+bc+ac)+abc,$$
$$0*a=0+a-0a=a,$$
$$1*a=1+a-1a=1,$$

因此 $(\mathbf{Z},*)$ 是以 0 为幺元的交换幺半群, 但不是群. □

习题 2 在 $\mathbf{Z}\times\mathbf{Z}$ 中定义乘法为

$$(x_1,x_2)(y_1,y_2)=(x_1y_1+2x_2y_2,\ x_1y_2+x_2y_1).$$

证明:

1) $\mathbf{Z}\times\mathbf{Z}$ 对此乘法为交换幺半群;

2) 当 $(x_1,x_2)\neq(0,0)$ 时, 则由

$$(x_1,x_2)(y_1,y_2)=(x_1,x_2)(z_1,z_2),$$

可得 $(y_1,y_2)=(z_1,z_2)$.

证 1) 由于

$$(x_1,x_2)(y_1,y_2)=(x_1y_1+2x_2y_2,\ x_1y_2+x_2y_1)=(y_1,y_2)(x_1,x_2),$$

$$((x_1,x_2)(y_1,y_2))(z_1,z_2)=(x_1y_1+2x_2y_2,\ x_1y_2+x_2y_1)(z_1,z_2)$$

$$=(x_1y_1z_1+2x_2y_2z_1+2x_1y_2z_2+2x_1y_2z_2,\ x_1y_1z_2+2x_2y_2z_2+x_1y_2z_1+x_2y_1z_1),$$

$$(x_1,x_2)((y_1,y_2)(z_1,z_2))=(x_1,x_2)(y_1z_1+2y_2z_2,\ y_1z_2+y_2z_1)$$

$$=(x_1y_1z_1+2x_2y_2z_1+2x_2y_2z_2+2x_1y_2z_2,\ x_1y_1z_2+2x_2y_2z_2+x_1y_2z_1+x_2y_1z_1),$$

$$(1,0)(y_1,y_2)=(y_1,y_2),$$

因此 $\mathbf{Z}\times\mathbf{Z}$ 对此乘法为交换幺半群.

2) 当 $(x_1,x_2)\neq(0,0)$ 时, 则由

$$(x_1,x_2)(y_1,y_2)=(x_1,x_2)(z_1,z_2),$$

可得

$$\begin{cases} x_1(y_1-z_1)+2x_2(y_2-z_2)=0, \\ x_2(y_1-z_1)+x_1(y_2-z_2)=0. \end{cases}$$

由于 $x_1,x_2\in\mathbf{Z}(x_1,x_2)\neq(0,0)$, 故 $x_1^2-2x_2^2\neq0$. 由此可得 $(y_1,y_2)=(z_1,z_2)$. □

习题 3 在 $S=\{x|x\in\mathbf{R},x\neq-1\}$ 中定义运算 $*$ 为 $a*b=a+b+ab$. 试证 S 对 $*$ 是一个群. 并求方程 $2*x*3=7$ 的解.

证 因为 $0*b=b$, 所以 0 为幺元. 又

$$\begin{aligned}(a*b)*c&=(a+b+ab)*c=a+b+ab+c+(a+b+ab)c\\&=a+b+c+ab+ac+bc+abc=a*(b*c),\end{aligned}$$

所以 $(S,*)$ 是交换幺半群. 又对于 $a\neq-1$, 有

$$a*\frac{-a}{1+a}=a-\frac{a}{1+a}-\frac{a^2}{1+a}=0.$$

所以 $(S,*)$ 是交换群.

由 $2*x*3=7$, 知

$$x=\frac{-2}{3}*7*\frac{-3}{4}=\frac{-2}{3}+7+\frac{-3}{4}-\frac{14}{3}+\frac{1}{2}-\frac{21}{4}+\frac{7}{2}=-\frac{1}{3}.$$ □

习题 4　证明若有限半群 G 满足消去律, 即

$$ax=ay\Rightarrow x=y,\quad xa=ya\Rightarrow x=y,$$

则 G 为群.

此结论对无限半群成立吗?

证　设 $G=\{g_1,g_2,\cdots,g_n\}$, $x\in G$. 令 $xG=\{xg_1,xg_2,\cdots,xg_n\}$. 若 $xg_i=xg_j$, 由消去律, $g_i=g_j$, 因而 $G=xG$. 于是有 i (不妨设 $i=1$), 使得 $x=xg_1$. 于是对任何 j, 有 $xg_j=(xg_1)g_j=x(g_1g_j)$. 再由消去律得 $g_1g_j=g_j$. 于是 g_1 是 G 的左幺元. 同样 $Gx=\{g_1x,g_2x,\cdots,g_nx\}=G$. 于是有 $g_kx=g_1$, 即 g_k 是 x 的左逆元, 因而 G 是群.

令 $G=\{2n|n\in\mathbf{N}\}$, 于是 G 对乘法与加法都是半群, 都满足消去律, 但 G 对乘法与加法都不是群. □

习题 5　如果在半群 G 中还有一个"一元运算"(即 G 到 G 的一个映射: $a\to a'$) 且满足

$$a'(ab)=b=(ba)a',\quad \forall a,b\in G.$$

证明此半群必为群.

证　任意取定 $a_0\in G$, 令 $e=a_0'a_0$, 于是 $eb=(a_0'a_0)b=a_0'(a_0b)=b$. 因此 e 为 G 的左幺元. 又由 $b(a_0a_0')=(ba_0)a_0'=b$, 知 a_0a_0' 是右幺元, 还有 $e=a_0a_0'=a_0a_0'$. 又 $b'b$ 也是幺元, 于是 $b'b=e$, 故 b' 是 b 的逆元. 因此 G 是群. □

习题 6　如果半群 G 有左幺元 e, 对 $\forall a\in G$, 有右逆元 (即有 $a'\in G$ 使 $aa'=e$). 问 G 一定是群吗?

解　令 $G=\left\{\left(\begin{smallmatrix}x & y\\ 0 & 0\end{smallmatrix}\right)\middle|\, x,y\in\mathbf{Q},x\neq 0\right\}$. 由

$$\begin{pmatrix}x & y\\ 0 & 0\end{pmatrix}\begin{pmatrix}x_1 & y_1\\ 0 & 0\end{pmatrix}=\begin{pmatrix}xx_1 & xy_1\\ 0 & 0\end{pmatrix},$$

知 G 是以 $\boldsymbol{e}=\left(\begin{smallmatrix}1 & 0\\ 0 & 0\end{smallmatrix}\right)$ 为左幺元的半群. 由

$$\begin{pmatrix}x & y\\ 0 & 0\end{pmatrix}\begin{pmatrix}x^{-1} & 0\\ 0 & 0\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}=\boldsymbol{e},$$

知 $\left(\begin{smallmatrix}x & y\\ 0 & 0\end{smallmatrix}\right)$ 有右逆元. 取 $y\neq 0$, 若有

$$\begin{pmatrix}x_1 & y_1\\ 0 & 0\end{pmatrix}\begin{pmatrix}x & y\\ 0 & 0\end{pmatrix}=\boldsymbol{e},$$

则 $x_1x=1$, $x_1y=0$, 于是 $x_1=\frac{1}{x}, x_1=0$ 这就导出矛盾. 故 G 不是群.

因此, 即使半群 G 有左幺元 e, 对 $\forall a\in G$, 有右逆元, G 也不一定是群. □

习题 7 设 $P(X)$ 为非空集合 X 的幂集 (即 X 的所有子集构成的集合).

1) 试证 $P(X)$ 对于对称差 $\triangle$,

$$A\triangle B=(A\setminus B)\cup(B\setminus A),\quad \forall A,B\in P(X),$$

构成一个群, 每个非幺元的阶为 2;

2) 试求 $P(X)$ 的阶.

证 1) 设 $A,B,C\in P(X)$. 首先, 有

$$\varnothing\triangle A=A\triangle\varnothing=A,\quad A\triangle A=\varnothing.$$

其次, 若 $x\in A\triangle B$, 如 $x\in A\setminus B$, 于是 $x\in A$, 但 $x\notin B$, 故 $x\notin A\cap B$, 即 $x\in(A\cup B)\setminus(A\cap B)$. 反之, 若 $x\in(A\cup B)\setminus(A\cap B)$, 则有 $x\in A\cup B$, $x\notin(A\cap B)$. 例如, $x\in A$, 则 $x\notin B$, 即 $x\in(A\setminus B)\subseteq(A\triangle B)$, 因而

$$A\triangle B=(A\cup B)\setminus(A\cap B).$$

由此可得

$$A\triangle(B\triangle C)=(A\cup B\cup C)\setminus((A\cap B)\cup(A\cap C)\cup(B\cap C))=(A\triangle B)\triangle C,$$

结论成立.

2) 若 X 是无限集, 则 $P(X)$ 的阶为无限. 若 X 的元素个数为 n, 则 $P(X)$ 的阶为 $\sum\limits_{k=0}^{n}\mathrm{C}_n^k=2^n$. □

习题 8 设群 G 中每个非幺元的阶为 2. 试证 G 为 Abel 群.

证 设 e 为 G 的幺元. 于是 $\forall a\in G$, $a^2=e$. 因此 $a^{-1}=a$. 于是 $\forall a,b\in G$, $ab=(ab)^{-1}=b^{-1}a^{-1}=ba$. 因此 G 为 Abel 群. □

习题 9 确定 S_5 中元素 $\sigma\tau$, $\sigma^{-1}\tau\sigma$, σ^2, σ^3, 其中,

$$\sigma=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix},\quad \tau=\begin{pmatrix}1&2&3&4&5\\3&4&1&5&2\end{pmatrix}.$$

解 所求元素如下:

$$\sigma\tau=\begin{pmatrix}1&2&3&4&5\\1&5&2&4&3\end{pmatrix},\quad \sigma^{-1}\tau\sigma=\begin{pmatrix}1&2&3&4&5\\5&3&2&1&4\end{pmatrix},$$

$$\sigma^2=\begin{pmatrix}1&2&3&4&5\\3&1&2&4&5\end{pmatrix},\quad \sigma^3=\begin{pmatrix}1&2&3&4&5\\1&2&3&5&4\end{pmatrix}.$$ □

习题 10　列出 S_3 的群表.

解　记

$$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad (1\,2\,3)=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad (1\,3\,2)=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},$$

$$(1\,2)=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\quad (1\,3)=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad (2\,3)=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}.$$

则下表

	e	$(1\,2)$	$(2\,3)$	$(1\,3)$	$(1\,2\,3)$	$(1\,3\,2)$
e	e	$(1\,2)$	$(2\,3)$	$(1\,3)$	$(1\,2\,3)$	$(1\,3\,2)$
$(1\,2)$	$(1\,2)$	e	$(1\,2\,3)$	$(1\,3\,2)$	$(2\,3)$	$(1\,3)$
$(2\,3)$	$(2\,3)$	$(1\,3\,2)$	e	$(1\,2\,3)$	$(1\,3)$	$(1\,2)$
$(1\,3)$	$(1\,3)$	$(1\,2\,3)$	$(1\,3\,2)$	e	$(1\,2)$	$(2\,3)$
$(1\,2\,3)$	$(1\,2\,3)$	$(1\,3)$	$(1\,2)$	$(2\,3)$	$(1\,3\,2)$	e
$(1\,3\,2)$	$(1\,3\,2)$	$(2\,3)$	$(1\,3)$	$(1\,2)$	e	$(1\,2\,3)$

是 S_3 的群表. □

习题 11　$\mathbf{N}$[①] 的所有变换组成的幺半群 $M(\mathbf{N})$ 中元素 f 定义为

$$f(n)=n+1,\quad \forall n\in\mathbf{N}.$$

证明 f 有无穷多个左逆元, 但无右逆元.

证　设 $m\in\mathbf{N}$, 定义 $g_m\in M(\mathbf{N})$ 如下:

$$g_m(n)=n-1,\quad n\neq 1,\qquad g_m(1)=m.$$

于是

$$g_m f(n)=g_m(n+1)=n,\quad \forall n\in\mathbf{N}.$$

所以 f 有无穷多个左逆元.

若 g 是 f 的右逆元, 于是有

$$n=fg(n)=g(n)+1,\quad \forall n\in\mathbf{N}.$$

因而

$$g(n)=n-1,\quad \forall n\in\mathbf{N}.$$

但 $g(1)=1-1=0\notin\mathbf{N}$, 故 f 无右逆元. □

①$\mathbf{N}=\{1,2,\cdots\}$ 为自然数的集合, 或正整数的集合

习题 12 设 M 为幺半群, e 为其幺元. M 的元素 a 称为可逆的, 如果 M 有中元素 a^{-1} 使得

$$a^{-1}a = aa^{-1} = e.$$

试证下列命题:

1) 若 $a \in M$ 且有 $b, c \in M$ 使得

$$ab = ca = e,$$

则 a 可逆, 且 $a^{-1} = b = c$;

2) $a \in M$ 可逆, 则 $b = a^{-1}$ 当且仅当

$$aba = a, \quad ab^2a = e;$$

3) M 的子集 G 为群的充分必要条件是 G 中每个元素可逆, 且 $\forall g_1, g_2 \in G$, 有 $g_1^{-1}g_2 \in G$;

4) M 中所有可逆元素构成一群.

证 1) 由

$$c = ce = c(ab) = (ca)b = eb = b,$$

于是 $ba = ab = e$, 因此 $a^{-1} = b = c$.

2) 若 $b = a^{-1}$, 则 $aa^{-1}a = a$, $a(a^{-1})^2a = e$.

反之, $e = ab^2a = (ab^2)a = a(b^2a)$, 于是由结论 1), a 可逆, 且 $a^{-1} = ab^2 = b^2a$.

再由 $aba = a$, 于是有 $ba = a^{-1}aba = a^{-1}a = e$, 因而 $a^{-1} = b$.

3) G 为群, 故 G 中每个元素 g 可逆, 且 $g^{-1} \in G$. 又已知 G 对乘法封闭, 于是 $\forall g_1, g_2 \in G$, 有 $g_1^{-1}g_2 \in G$.

反之, $g \in G$, g 可逆, 于是取 $g_1 = g_2 = g$, 因而 $e = g_1^{-1}g_2 \in G$. 又 $g_1, g_2 \in G$, 因此 $g_1^{-1} = g_1^{-1}e \in G$, $g_1g_2 = (g_1^{-1})^{-1}g_2 \in G$. 显然结合律成立, 因而 G 是群.

4) 记 M 中所有可逆元素的集合为 U, 显然 U 中任何元素可逆. 设 $g_1, g_2 \in U$, 由

$$(g_1^{-1}g_2)(g_2^{-1}g_1) = (g_2^{-1}g_1)(g_1^{-1}g_2) = e,$$

知 $g_1^{-1}g_2 \in U$, 故 U 构成一群. □

习题 13 设 M 为幺半群,$m \in M$. 在 M 中另定义乘法 "$*$": $a * b = amb$.

1) 试证 M 对 $*$ 为半群;

2) 试问在什么情况下, M 对 $*$ 为幺半群?

证 1) 设 $a, b, c \in M$. 于是

$$(a * b) * c = (amb) * c = ambmc, \quad a * (b * c) = am(b * c) = ambmc = (a * b) * c,$$

于是 $(M,*)$ 是半群.

2) 设 1 为 M 的幺元, a 为 $(M,*)$ 的幺元, 则有

$$1 = a*1 = am1 = am, \quad 1 = 1*a = 1ma = ma.$$

于是 m 是可逆元, 且 $a = m^{-1}$. 反之, 若 m 可逆, 于是有

$$m^{-1}*b = m^{-1}mb = b, \quad b*m^{-1} = bmm^{-1} = b.$$

因此 $(M,*)$ 为幺半群, 当且仅当 m 是可逆元. □

1.3　子群与商群

习题 1　设 H 是群 G 的子群. 证明 $\{Ha\}$ 是 G 的分划, 且对应的等价关系 R_1 为

$$a\,R_1\,b, \quad \text{当 } ba^{-1} \in H.$$

证　设 $a,b \in G$, 而 $Ha \cap Hb \neq \varnothing$. 于是有 $h_1,h_2 \in H$ 使得 $h_1a = h_2b$. 记 $h_0 = h_2^{-1}h_1$, 于是 $h_0a = b$, $a = h_0^{-1}b$. 因而 $\forall h \in H$, 有 $ha = hh_0^{-1}h_0a = hh_0^{-1}b \in Hb$. $hb = hh_0h_0^{-1}b = hh_0a \in Ha$. 所以 $Ha = Hb$. $\{Ha\}$ 是 G 的分划.

从上面的证明知 $Ha = Hb$ 当且仅当 $ba^{-1} = h_0 \in H$. 于是对应的等价关系 R_1 为 $a\,R_1\,b$, 当且仅当 $ba^{-1} \in H$. □

习题 2　设 H 是 $\mathbf{Z}$ 的一个子群. 证明必有非负整数 m 使 $H = m\mathbf{Z}$.

证　若 $H = \{0\}$, 自然 $H = 0\mathbf{Z}$. 设 $H \neq \{0\}$, 令 $m = \min\{|h| \mid h \in H \setminus \{0\}\}$. 于是 $m\mathbf{Z} \subseteq H$. 若 $k \in H$, 于是有 $k = ml + r$, 其中 $l,r \in \mathbf{Z}$, 且 $0 \leqslant r < m$. 注意 $r = k - ml \in H$, 由 m 的取法, 知 $r = 0$. 因此 $k \in m\mathbf{Z}$, 故 $H = m\mathbf{Z}$. □

习题 3　写出 S_3 的全部子群及其左右陪集, 并指出哪些子群是正规子群.

解　记

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad (1\,2\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad (1\,3\,2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$(1\,2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad (1\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad (2\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

除平凡子群 S_3, $\{e\}$ 外, 非平凡子群及其陪集如下:

子群 $S_2^1 = \langle(1\,2)\rangle$, $S_3 = S_2^1 \cup (1\,3)S_2^1 \cup (2\,3)S_2^1 = S_2^1 \cup S_2^1(1\,3) \cup S_2^1(2\,3)$;

子群 $S_2^2 = \langle(1\,3)\rangle$, $S_3 = S_2^2 \cup (1\,2)S_2^2 \cup (2\,3)S_2^2 = S_2^2 \cup S_2^2(1\,2) \cup S_2^2(2\,3)$;

子群 $S_2^3 = \langle(2\,3)\rangle$, $S_3 = S_2^3 \cup (1\,2)S_2^3 \cup (1\,3)S_2^3 = S_2^3 \cup S_2^3(1\,3) \cup S_2^3(2\,3)$;

子群 $A_3=\langle(1\,2\,3)\rangle$, $S_3=A_3\cup(1\ 2)A_3=A_3\cup A_3(1\ 2)$,
其中 A_3 是正规子群. □

习题 4 设 H 是群 G 的子群且 $[G:H]=2$. 试证 $H\lhd G$.

证 因为 $[G:H]=2$, 所以有 $x\in G\setminus H$ 使得

$$G=H\cup xH=H\cup Hx.$$

由此可知 $\forall h\in H$, $xh\notin H$, 于是 $xh\in Hx$. 因此 $xH=Hx$. 进而 $\forall g\in G$, $gH=Hg$. 于是 $H\lhd G$. □

习题 5 设 H_1,H_2 为群 G 的两个有限子群. 证明

$$|H_1H_2|=[H_1:1][H_2:1]/[H_1\cap H_2:1].$$

证 因为 $H_1H_2=\bigcup\limits_{g\in H_2}H_1g$, 而且 $H_1g\neq H_1g'$ 当且仅当 $H_1g\cap H_1g'=\varnothing$. $H_1g=H_1g'$ 当且仅当 $gg'^{-1}\in H_1$, 即 $gg'^{-1}\in H_1\cap H_2$.

注意 $H_1\cap H_2$ 是 H_2 的子群, 于是

$$H_2=(H_1\cap H_2)g_1\cup(H_1\cap H_2)g_2\cup\cdots\cup(H_1\cap H_2)g_r,\quad r=[H_2:H_1\cap H_2],$$

当 $i\neq j$ 时, $(H_1\cap H_2)g_i\neq(H_1\cap H_2)g_j$, 即 $g_ig_j^{-1}\notin H_1\cap H_2$. 因此

$$H_1H_2=\bigcup_{i=1}^{r}H_1g_i,\qquad i\neq j,\quad H_1g_i\cap H_1g_j=\varnothing.$$

于是

$$|H_1H_2|=[H_1:1][H_2:H_1\cap H_2]=[H_1:1][H_2:1]/[H_1\cap H_2:1].$$ □

习题 6 设 H_1,H_2 为有限群 G 的两个子群且 $H_1\subseteq H_2$. 证明

$$[G:H_1]=[G:H_2][H_2:H_1].$$

证 设

$$G=\bigcup_{i=1}^{s}H_2g_i,\qquad i_1\neq i_2,\ H_2g_{i_1}\cap H_2g_{i_2}=\varnothing,\quad s=[G:H_2];$$

$$H_2=\bigcup_{j=1}^{r}H_1h_j,\qquad j_1\neq j_2,\quad H_1h_{j_1}\cap H_1h_{j_2}=\varnothing,\quad r=[H_2:H_1].$$

于是有

$$G=\bigcup_{i=1}^{s}\bigcup_{j=1}^{r}H_1h_jg_i.$$