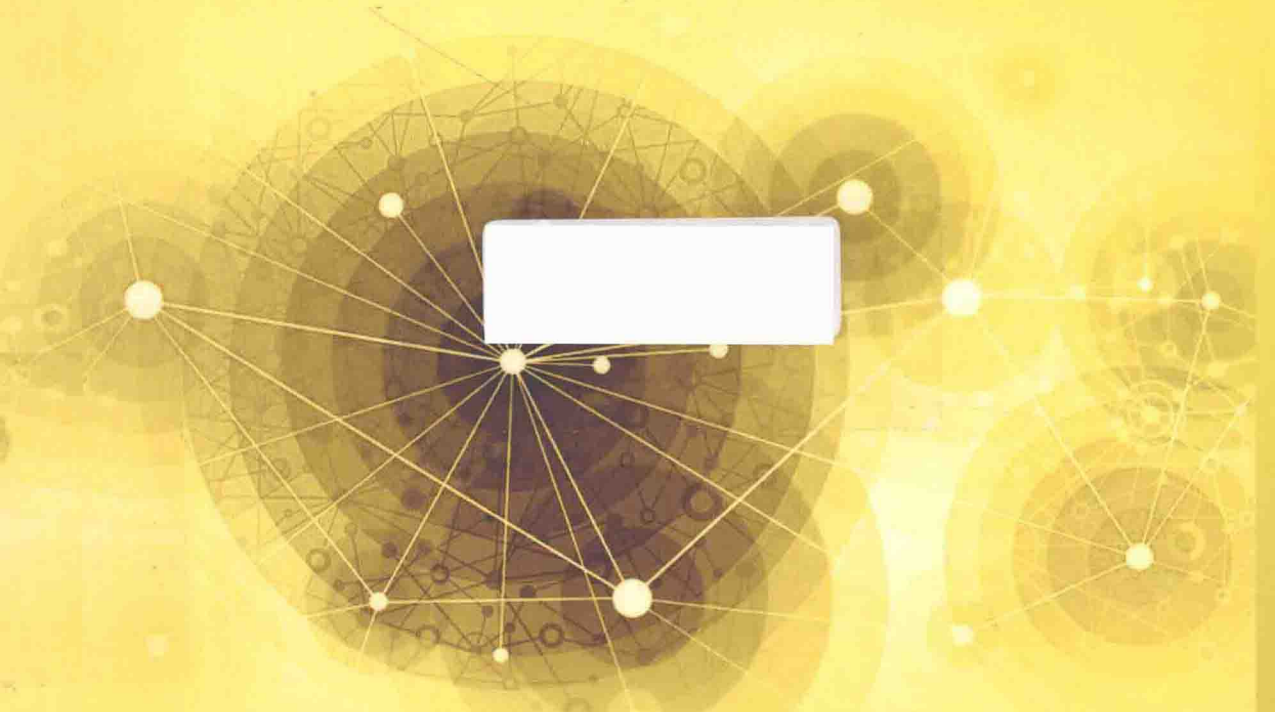
抽象代数的问题和反例

黎永锦　编著



科学出版社

抽象代数的问题和反例

黎永锦　编著

科学出版社

北京

内 容 简 介

本书汇集了抽象代数中的大量问题和反例, 主要内容有群论、环论、域和伽罗瓦理论等. 书中通过例子对抽象代数的基本概念进行了比较仔细的对比, 考虑了很多重要定理在不同条件下是否成立的问题, 给出了抽象代数中很多值得深入思考的问题.

本书可供高年级本科生学习抽象代数和教师教学时参考. 本书比较系统和完整, 也可以看作是一本用来阅读的习题解答.

图书在版编目(CIP)数据

抽象代数的问题和反例/黎永锦编著. —北京：科学出版社, 2015.5

ISBN 978-7-03-044398-4

Ⅰ. ①抽… Ⅱ. ①黎… Ⅲ. ①抽象代数–研究 Ⅳ. ①O153

中国版本图书馆 CIP 数据核字(2015) 第 110938 号

责任编辑：李 欣 / 责任校对：张凤琴

责任印制：张 倩 / 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

三河市骏杰印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2015 年 5 月第 一 版 开本：720 × 1000 1/16

2015 年 5 月第一次印刷 印张：13 1/4

字数：267 000

定价：78.00 元

(如有印装质量问题, 我社负责调换)

前　言

抽象代数是一门比较抽象的数学学科, 因此, 在学习的过程中, 有时候只有形式上的理解, 未能深刻地理解其中很多概念和定理的数学背景, 更难以提出自己的问题.

爱因斯坦曾说:“提出一个问题往往比解决一个问题更为重要, 因为解决一个问题也许只是一个数学上或实验上的技巧问题. 而提出新的问题、新的可能性, 从新的角度看旧问题, 却需要创造性的想像力, 而且标志着科学的真正进步.”

从能否提出问题可以知道不同学生对数学的理解差异, 发现和提出自己问题的能力是非常重要的, 提出问题可以说是数学学习的核心. 学习抽象代数最好以问题为中心, 通过发现问题、提出问题、探究问题和解决问题来提高对基本概念和重要定理的理解. 教师也应该在教学过程中通过提出问题来启发和引领学生深入思考.

为了减少阅读的困难, 书中选入的例子一般都是比较容易的, 主要取材于有关的书籍、学术论文和网络上的相关资源. 对于一些基本概念和性质, 为了方便阅读, 也作为问题提出, 但这些内容在很多教科书都容易找到, 因此一般不再给出理由和证明. 书中还收录了一些公开问题, 这些问题是比较难的, 有很多数学家都在研究这些问题, 可能读者看到这些问题的时候, 有些已经解决了, 或有了新的进展, 因此, 如果对这些问题有兴趣, 在开展研究前最好查阅一些最新的相关论文.

书中的问题来源于很多不同的渠道, 有些是上课时同学帮忙找到的例子, 因此, 虽然经过了多年的试用和很多同学的阅读, 还是难免有些概念可能不统一, 这样会造成反例的错误, 也可能是我粗心大意造成的, 还请大家耐心指正, 只能在不断修改中完善, 请大家谅解. 最后, 我要感谢对本书的改进和校对做了很多工作和提出了很多建议的同学, 如杨剑锋、苏彦宏、关静怡、王洋、廖鹏程、和炳和黄景灏等. 没有他们的支持和帮忙, 本书是不可能完成的.

黎永锦

2015 年 1 月于中山大学

符 号 表

Q	有理数域
Q^*	非零有理数集合
R	实数域
C	复数域
Z	整数集合, 正负整数, 包含 0
Z^+	正整数集合
N	自然数集
$a \mid b$	a 整除 b
$a \equiv b \pmod{m}$	a 与 b 模 m同余
(a, b)	a 和 b 的最大公因子
$o(a)$	a 的阶
$\|G\|$	群 G 的阶
S_n	n 个字母的对称群
Z_n	模 n 的加法群或环
Z_p	模 p 的加法群或域 (p 为素数)
$\cong$	同构
$\mathrm{Ker}(f)$	同态 f 的核
$< H >$	由集合 H 生成的子群
$< a >$	由元素 a 生成的循环子群
aH, Ha	a 的左陪集和右陪集
$[G : H]$	子群 H 在群 G 中的指数
GH	$\{ab \mid a \in G, b \in H\}$
sgn σ	置换 σ 的符号
A_n	n 个字母的交错群
$C_H(a)$	a 在 H 中的中心化子
$N_G(H)$	H 在 G 中的正规化子群
$C(G)$	G 的中心
G'	G 的换位子群
$G^{(n)}$	G 的第 n 次导群
char R	环 R 的特征
(H)	由 H 生成的理想

(a)	由元素 a 生成的主理想
$F[x]$	F 上的多项式
$F[x_1, x_2, \cdots, x_n]$	F 上 n 个未定元的多项式环
$\deg f$	多项式的次数
$\dim V$	线性空间 V 的维数
G_f	多项式 f 的伽罗瓦群
H^{-1}	$H^{-1} = \{a^{-1} \mid a \in H\}$
$R[a]$	由 R 和 a 生成的环, 包含 R 和 a 的最小环
$F(a)$	域 F 上的单扩张
$[K : F]$	域扩张 K/F 的次数
$G_1 \oplus G_2$	交换群G_1和交换群G_2的直积
$G_1 \times G_2$	群G_1和群G_2的直积
$F \setminus \{a\}$	F除去a的所有元素

目　录

第 1 章　群　　论

群只有一种代数运算, 因此比较容易深入讨论. 群的左右单位元和逆元的相关问题应该仔细讨论, 元素的阶对揭示群的结构起着重要的作用, 通过群的阶可以给出群的一些重要性质, 但一般来说, 两个不同元素的阶无法决定它们的乘积的阶, 元素的阶是研究群的一个重要工具. 子群继承了群的一些重要性质, 通过子群可以了解群的很多性质, 但群与子群的关系是复杂而密切的. 正规子群是一个重要的概念, 具有很好的性质. 对称群是一类性质比较清楚的群, 它给群提供了很多重要而简明的反例. 群的同态和同构让不同的群可以比较, 使得群的分类简单明了.

1.1　群 的 定 义

1.1.1　二元运算

问题 1.1.1　*二元运算是什么?*

从 $S \times S$ 到 S 的一个映射 $\cdot$ 称为 S 上的一个二元运算.

问题 1.1.2　*$S \times S$ 上的映射 $\cdot$ 都是 S 上的一个二元运算吗?*

不一定. 设 $S = \{(a_1, a_2, a_3) \mid a_1, a_2, a_3$ 都是实数$\}$是 3 维欧氏空间, 则内积不再是向量, 因此内积不是二元运算.

1.1.2　群的定义

问题 1.1.3　*什么是群?*

设 G 是一个非空集合, 若在 G 上定义一个二元运算 $\cdot$, 满足

(1) 结合律: 对任何 $a, b, c \in G$, 有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, 则称 G 是一个半群 (semigroup), 记作 $(G, \cdot)$. 若 $(G, \cdot)$ 还满足

(2) 存在单位元 $e \in G$, 使对任何 $a \in G$ 有 $e \cdot a = a \cdot e = a$.

(3) 对任何 $a \in G$, 有 $a^{-1} \in G$, 使得 $a^{-1} \cdot a = a \cdot a^{-1} = e$, 则称 $(G, \cdot)$ 是一个群 (group).

如果半群中也有单位元, 则称为幺半群 (monoid).

如果群 $(G, \cdot)$ 适合交换律: 对任何 $a, b \in G$ 有 $a \cdot b = b \cdot a$, 则称 G 为交换群或 Abel 群.

群中的乘法运算一般简记为 ab.

问题 1.1.4　什么是群的可逆元?

如果 $ab = ba = e$, 那么就称 a 为一个可逆元 (invertible element), 并称 b 为 a 的逆元 (inverse element). 可逆元 a 的逆元通常记作 a^{-1}.

问题 1.1.5　从 $S \times S$ 到 S 的二元运算都满足结合律吗?

不一定. 取 S 为实数全体所构成的集合, 将映射 $\cdot$

$$\cdot : S \times S \to S$$

定义为

$$a \cdot b = a + b^2,$$

则二元运算 $\cdot$ 不满足结合律.

问题 1.1.6　若 $S \times S$ 到 S 的二元运算满足交换律, 则它一定满足结合律吗?

不一定. 设 R 为实数, 在 $R \times R$ 上, 定义

$$\cdot : (a,\ b) \quad \mapsto \quad |a\ -\ b|,$$

则运算 $\cdot$ 满足交换律, 但它不满足结合律.

问题 1.1.7　幺半群一定是群吗?

不一定. 整数集 Z 对于乘法是一个幺半群, 但它不是群.

问题 1.1.8　什么是左单位元和右单位元?

设 G 是一个半群, 若存在 $a \in G$, 使对任何 $c \in G$ 有 $ac = c$, 则称 a 为 G 的左单位元.

设 G 是一个半群, 若存在 $b \in G$, 使对任何 $c \in G$ 有 $cb = c$, 则称 b 为 G 的右单位元.

问题 1.1.9　半群 G 的左单位元一定是半群 G 的右单位元吗? 若半群 G 有左单位元和右单位元, 则它们一定相等吗?

左单位元不一定是半群 G 的右单位元, 若半群 G 有左单位元和右单位元, 则它们也不一定相等.

设 $G = \{a, b\}, a \neq b$, 定义 $aa = a, ab = b, ba = a, bb = b$, 则 G 是一个半群, 并且 a 是 G 的左单位元, 但 $ba \neq b$, 因此 a 不是 G 的右单位元. 明显地, b 是 G 的右单位元.

问题 1.1.10　什么是左逆元和右逆元?

设 G 是一个有单位元的半群, 若 $a, b \in G$, 满足 $ab = e$, 则称 b 为 a 的右逆元, a 为 b 的左逆元.

问题 1.1.11 *若 G 是一个有单位元的半群, 则 G 的左逆元一定是右逆元吗?*

不一定. 设 G 是所有正整数 Z^+ 到 Z^+ 的映射, 则在复合作为乘法的运算下, G 是一个半群, 并且单位元 e 为恒等映射, 令 $a: Z^+ \to Z^+$ 为 $a(n) = 2n$, 定义 Z^+ 到 Z^+ 的映射 b 为: 当 n 为偶数时, $b(n) = \dfrac{n}{2}$; 当 n 为奇数时, $b(n) = 1$, 则容易验证 $ba = e$; 但 ab 不等于 e, 因此, a 的左逆元 b 不是它的右逆元.

问题 1.1.12 *若 G 是一个有单位元的半群, 若 $a \in G$ 的左逆元 b 和右逆元 c 都存在, 则 a 的逆元一定存在吗?*

是的. 若 $a \in G$ 的左逆元 b 和右逆元 c 都存在, 则 $ba = e$, $ac = e$, 因此, $(ba)c = ec = c$, 并且 $(ba)c = b(ac) = be = b$, 故 $b = c$, 所以, a 的逆元为 b.

问题 1.1.13 *若 G 是一个有单位元的半群, 则 $a \in G$ 有右逆元 b 和左逆元 c, 则 a 一定是可逆元吗?*

是的. 由于 $ab = e$, 所以, $c(ab) = ce = c$, 故 $(ca)b = eb = b$, 从而 $b = c$, 因此, a 是可逆元.

问题 1.1.14 *若半群 G 有左单位元 e, 并且任意 $a \in G$, 存在 $b \in G$, 使得 $ab = e$, 则 G 一定是群吗?*

不一定. 设 $G = \{e, a\}, e \neq a$, 定义 $ea = a, ae = e, aa = a, ee = e$, 则 G 是半群, e 是左单位元, 并且 $ee = e$, $ae = e$, 但 a 没有左逆元, 否则的话, 由 $aa = a$ 可得 $a = e$, 矛盾. 所以, G 不是群.

问题 1.1.15 *若半群 G 有右单位元 e, 并且任意 $a \in G$, 存在 $b \in G$, 使得 $ab = e$, 则 G 一定是群吗?*

是的. 存在 $e \in G$, 使得对任意 $a \in G$, 有 $ae = a$. 对于 $a \in G$, 有 $b \in G$, 使得 $ab = e$. 对 $b \in G$, 存在 $c \in G$, 使得 $bc = e$, 因此 $bab = be = b$, 故 $ba = (ba)e = (ba)(bc) = (bab)c = e$. 另外, $ea = (ab)a = a(ba) = ae = a$, 因此, e 是 G 的单位元, 并且 b 是 a 的逆元, 所以, G 是群.

问题 1.1.16 *若半群 G 有右单位元 e, 并且任意 $a \in G$, 存在 $b \in G$, 使得 $ba = e$, 则 G 一定是群吗?*

不一定. 设 $G = \{e, a\}, e \neq a$, 定义 $ae = a, ea = e, aa = a, ee = e$, 则 G 是半群, e 是右单位元, 但 a 没有右逆元, 否则的话, 由 $aa = a$ 可得 $a = e$, 矛盾. 所以, G 不是群.

问题 1.1.17 *若半群 G 有左单位元 e, 并且任意 $a \in G$, 存在 $b \in G$, 使得 $ba = e$, 则 G 一定是群吗?*

是的. 证明与前面问题类似.

容易知道, 若 e 是群 G 的单位元, 则 $e^2 = e$.

问题 1.1.18　设 G 是群, $a \in G$, 满足 $a^2 = a$, 则 a 一定是单位元吗?

是的. 由于 $a^2 = a$, 故 $a^{-1}a^2 = a^{-1}a = e$, 所以, $a = e$.

问题 1.1.19　设 G 是半群, 若对于任意 $a, b \in G$, 都存在 $x, y \in G$, 使得 $xay = b$, 则 G 一定是群吗?

不一定. 设 $G = \{e, a\}, e \neq a$, 定义 $ea = a, ae = e, aa = a, ee = e$, 则 G 是半群, 存在 a, e, 使得 $aae = e$, 并且 $eaa = a, aea = a, eee = e$, 但 a 没有逆元, 否则的话, 由 $aa = a$ 可得 $a = e$, 矛盾. 所以, G 不是群.

问题 1.1.20　设 G 是半群, 若对于任意 $a, b \in G$, 方程 $xa = b, ay = b$ 都有解, 则 G 一定是群吗?

是的. 取定 $a \in G$, 则由 $ay = a$ 有解可知存在 $e_1 \in G$, 使得 $ae_1 = a$. 对于任意 $b \in G$, 由 $xa = b$ 有解可知存在 $g \in G$, 使得 $ga = b$, 故 $be_1 = (ga)e_1 = g(ae_1) = ga = b$ 对任意 $b \in G$ 成立, 因此 e_1 为 G 的右单位元.

类似地, 由 $xa = a$ 有解可知存在 $e_2 \in G$, 使得 $e_2a = a$. 对于任意 $b \in G$, 由 $ay = b$ 有解可知存在 $g \in G$, 使得 $ag = b$, 故 $e_2b = e_2(ag) = (e_2a)g = ag = b$ 对任意 $b \in G$ 成立, 因此 e_2 为 G 的左单位元. 从而, 由 $e_2e_1 = e_1, e_2e_1 = e_2$ 可知 e_1 为 G 的单位元, 不妨记 $e = e_1 = e_2$.

对于任意 $a \in G$, 由方程 $xa = e, ay = e$ 都有解, 可得 $x = xe = x(ay) = (xa)y = ey = y$, 因此, $x = y$, 从而 x 是 a 的逆元, 所以, G 是群.

明显地, 在交换群中, 对于 $a, b \in G$, $(ab)^n = a^nb^n$ 是一定成立的.

问题 1.1.21　设 G 是群, $a, b \in G$, 则 $(ab)^n = a^nb^n$ 一定成立吗?

不一定. 在非交换群 S_3 中, 设 $a = (12), b = (123)$, 则 $ab = (12)(123) = (23)$, 故 $(ab)^2 = (23)(23) = (1)$, 并且 $a^2b^2 = (12)^2(123)^2 = (1)(132) = (132)$, 因此, $(ab)^2 \neq a^2b^2$.

问题 1.1.22　存在 1, 2, 3 阶的非循环交换群吗?

不存在. 设 $K_4 = \{e, a, b, c\}$, 乘法表为

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

则 K_4 是克莱因四元群 (Klein four-group), K_4 是阶最小的非循环交换群.

1.1.3 群的性质

问题 1.1.23 *群中的消去律成立吗?*

成立. 设群 G 中的元素 a, b, c 满足 $ab = ac$ 或 $ba = ca$, 则 $b = c$.

问题 1.1.24 *若 G 是一个半群, 并且在 G 中消去律成立, 则 G 一定是群吗?*

不一定. 设 G 为所有非零整数, 则 G 在整数的乘法下是一个半群, 并且在 G 中消去律成立, 但 G 的元素不一定有逆元, 因此 G 不是群.

问题 1.1.25 *若 G 是一个有单位元的有限半群, 并且在 G 中消去律成立, 则 G 一定是群吗?*

是的. 对于任意 $a \in G$, 由于 G 是有限的, 故一定存在正整数 $m > n > 0$, 使得 $a^m = a^n$, 故由 $a^{m-n}a^n = a^m = a^n = ea^n$ 可得 $a^{m-n} = e$, 因而, $a^{-1} = a^{m-n-1}$, 所以, G 是群.

问题 1.1.26 *群中的元素 a, b 的乘积的逆是什么?*

设 a, b 是群 G 中的两个元素, 则 $(ab)^{-1} = b^{-1}a^{-1}$.

明显地, 若 G 是交换群, 则对任意 $a, b \in G$, 都有 $(ab)^{-1} = a^{-1}b^{-1}$.

问题 1.1.27 *若群 G 中的任意两个元素 $a, b \in G$, 都有 $(ab)^{-1} = a^{-1}b^{-1}$, 则 G 一定是交换群吗?*

是的. 对任意 $a, b \in G$, 都有 $(a^{-1}b^{-1})^{-1} = (a^{-1})^{-1}(b^{-1})^{-1} = ab$, 另外, 由 $(a^{-1}b^{-1})^{-1} = (b^{-1})^{-1}(a^{-1})^{-1} = ba$, 可知 $ab = ba$ 对任意 $a, b \in G$ 都成立, 因此, G 一定是交换群.

明显地, 若 G 是交换群, 则对任意 $a, b \in G$, 都有 $(ab)^n = a^n b^n$, 反过来呢?

问题 1.1.28 *若群 G 中的任意两个元素 $a, b \in G$, 都有 $(ab)^2 = a^2b^2$, 则 G 一定是交换群吗?*

是的. 由于 $(ab)^2 = a^2b^2$, 并且 $(ab)^2 = abab$, 故 $a^2b^2 = abab$, 所以, $ab = ba$ 对任意 $a, b \in G$ 成立, 所以, G 是交换群.

问题 1.1.29 *若群 G 中的任意两个元素 $a, b \in G$, 都有 $(ab)^3 = a^3b^3$ 和 $(ab)^5 = a^5b^5$, 则 G 一定是交换群吗?*

是的. 由 $(ab)^3 = a^3b^3$ 可知 $ababab = aaabbb$, 故 $baba = aabb$. 类似地, 由 $(ab)^5 = a^5b^5$ 知道 $abababbabb = aaaaabbbbb$, 故 $babababa = aaaabbbb$, 因此, $(baba)(baba) = (aabb)(aabb)$, 因而, $bbaa = aabb$, 再根据 $baba = aabb$ 可知 $bbaa = baba$, 所以, 对于任意 $a, b \in G$, 都有 $ba = ab$.

问题 1.1.30　若群 G 中的任意两个元素 $a,b\in G$, 都有 $(ab)^3=a^3b^3$, 则 G 一定是交换群吗?

不一定. 设 G 为所有满足 $a_{ii}=\bar{1}$, 当 $i<j$ 时, 有 $a_{ij}=0$, $a_{ij}\in Z_3$ 的 3×3 矩阵, 则容易验证, 对于任意 $a\in G$, 有 $a^3=e$ 是单位矩阵, 因此, 对于任意 a, $b\in G$, 都有 $(ab)^3=a^3b^3$, 但 G 不是交换群.

问题 1.1.31　设 G 是群, 若任意非单位元 $a\in G$, a 的阶都是 2, 则 G 一定是交换群吗?

是的. 由于 $a^2=e$, 故 $a^{-1}=a$ 对于任意 $a\in G$ 都成立. 因此对于任意 $a,b\in G$, 有 $ba=(ba)^{-1}=a^{-1}b^{-1}=ab$, 所以, G 是交换群.

问题 1.1.32　设 G 是群, 若任意非单位元 $a\in G$, a 的阶都是 3, 则 G 一定是交换群吗?

不一定. 设 $x,y,z\in Z_3$, 则所有形如

$$a=\begin{bmatrix}1 & x & y\\ 0 & 1 & z\\ 0 & 0 & 1\end{bmatrix}$$

的矩阵在矩阵乘法下构成一个 27 阶的群 G, 并且对于任意 $a\in G$, a 的阶都是 3, 但对于

$$b=\begin{bmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix},\quad c=\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 1\\ 0 & 0 & 1\end{bmatrix},$$

则

$$bc=\begin{bmatrix}1 & 1 & 1\\ 0 & 1 & 1\\ 0 & 0 & 1\end{bmatrix},\quad cb=\begin{bmatrix}1 & 1 & 0\\ 0 & 1 & 1\\ 0 & 0 & 1\end{bmatrix},$$

故 $bc\neq cb$, 所以, G 不是交换群.

问题 1.1.33　元素个数最少的非交换群是什么?

容易验证, 1, 2, 3, 4, 5 阶群都一定是交换群, 对称群 S_3 是 6 阶的非交换群, 因此阶最小的非交换群的阶是 6.

问题 1.1.34　设 G 是群, $a,b\in G$, 若 $a^2=b^2$, 则 $a=b$ 一定成立吗?

不一定. 在克莱因四元群 $K_4=\{e,a,b,ab\}$ 中, $a^2=b^2=e$, 但 $a\neq b$.

问题 1.1.35　设 G 是群, $a\in G$, a 一定有平方根吗? 即一定存在 $b\in G$, 使得 $a=b^2$ 吗?