普通高等教育“十一五”国家级规划教材辅导用书

近世代数
习题解答

韩士安　林　磊　编著

科学出版社
www.sciencep.com

普通高等教育“十一五”国家级规划教材辅导用书

近世代数习题解答

韩士安　林　磊　编著

科学出版社

北京

内 容 简 介

本书是普通高等教育“十一五”国家级规划教材《近世代数(第二版)》(韩士安，林磊编著，科学出版社)的配套教学辅导用书. 本书提供了该教材的全部习题解答，习题量大、内容丰富、解答详尽，力求在提供解答时能尽可能多地渗透代数学的重要思想方法及证明的基本技巧，以帮助读者更好地掌握教材内容，同时也是对教材内容的有益补充.

本书可作为高等院校数学专业本科生的参考用书，也可供备考硕士研究生的学生参考使用.

图书在版编目(CIP)数据

近世代数习题解答/韩士安，林磊编著. —北京：科学出版社，2010

普通高等教育“十一五”国家级规划教材辅导用书

ISBN 978-7-03-026865-5

Ⅰ. 近… Ⅱ. ①韩… ②林… Ⅲ. 抽象代数-高等学校-解题 Ⅳ. O153-44

中国版本图书馆 CIP 数据核字 (2010) 第 033664 号

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

新蕾印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2010 年 3 月第 一 版 开本：B5(720×1000)

2010 年 3 月第一次印刷 印张：13 3/4

印数：1—3 500 字数：277 000

定价：22.00 元

(如有印装质量问题，我社负责调换)

前　言

本书是与华东师范大学数学系教师编写、由科学出版社出版的国家理科基地教材《近世代数 (第二版)》(已列入普通高等教育 "十一五" 国家级规划教材) 配套的教学辅导用书.

《近世代数》教材自 2004 年面世以来, 承蒙大家的厚爱, 已经被许多高校选为同名课程的教材. 近世代数是数学专业一门重要的专业基础课, 但是其概念抽象, 证明题多且难以下手, 这使很多学生对学习这门课程产生了畏难情绪. 因此, 他们迫切希望能有一本与教材相配套的教学辅导书, 帮助他们学好这门课程, 本书正是为了满足这一需求而编写的. 本书虽然仅仅对该教材的所有习题给出了解答, 但是在提供解答时力求能尽可能多地渗透代数学的一些重要思想方法, 并介绍多种基本技巧. 希望通过这些做法, 能为学习本课程有一定困难的学生以及想在代数学方面继续深造的学生提供帮助.

由于教材的第二版对第一版进行了适当的修改, 每节后的习题也作了小规模的调整: 有个别章节次序作了改动, 同时增添了一些章节, 相应地也新增了一些习题, 所以本书的习题解答是与第二版教材相配套的. 不过习题的调整范围很小, 使用第一版教材的读者大可不必担心.

在此还需要对本书的使用做些说明. 本书是一本教学辅导书, 不是教材. 因此大家在学习近世代数课程时, 如遇到不会做的习题, 首先应该仔细阅读教材, 将教材中相应的概念、结论弄明白, 将相应的对此类问题的处理方法搞清楚, 然后再尝试做习题. 做完以后再来阅读本书的解答, 比较两者的差异, 看看哪个解答更合理. 当然我们在为教材配备习题时有两种目的: 一是为教材的内容服务, 通过配套习题的练习, 帮助读者更好地掌握教材内容; 二是教材受教学课时的限制, 内容不可能安排过多, 但是有些内容本身是非常有趣、非常重要的, 因此通过安排相应的习题, 来介绍这些内容, 作为对教材内容的补充. 这部分习题主要是为那些学有余力, 并对代数学比较感兴趣的学生安排的. 对于这些习题, 因为内容比较陌生, 读者做起来可能比较困难, 大家可以通过本书, 了解这些习题的解答, 从而扩大知识面, 丰富自己的知识积累.

虽然本书是与相应教材配套的辅导书, 但不使用该教材的读者也完全可以阅读本书. 因为本书中包含的习题量较大, 内容丰富, 解答详尽, 从中可以学到很多代数学的思想方法和证明技巧. 同时相信它对备考硕士研究生的读者也会大有帮助.

受作者经验和水平的限制, 书中难免出现一些疏漏及不足, 恳请读者批评指正. 至于作者编写风格不尽相同所造成的缺点, 就只能请读者谅解了. 我们的 E-mail 地址是: llin@math.ecnu.edu.cn (林磊); sahan@math.ecnu.edu.cn (韩士安).

作　者

2009 年 5 月

于华东师范大学闵行校区樱桃河畔

目　录

第 1 章　群……1
习题 1-1　等价关系与集合的分类……1
习题 1-2　群的概念……6
习题 1-3　子群……14
习题 1-4　群的同构……21
习题 1-5　循环群……30
习题 1-6　置换群与对称群……39
习题 1-7　置换在对称变换群中的应用……52
第 2 章　群的进一步讨论……59
习题 2-1　子群的陪集……59
习题 2-2　正规子群与商群……64
习题 2-3　群的同态和同态基本定理……72
习题 2-4　群的直积……81
习题 2-5　群在集合上的作用……87
习题 2-6　西罗定理……95
第 3 章　环……101
习题 3-1　环的定义与基本性质……101
习题 3-2　整环、域与除环……117
习题 3-3　理想与商环……127
习题 3-4　环的同态……135
习题 3-5　素理想与极大理想……145
习题 3-6　环的特征与素域……154
第 4 章　环的进一步讨论……156
习题 4-1　多项式环……156
习题 4-2　整环的商域……161
习题 4-3　唯一分解整环……163
习题 4-4　主理想整环与欧几里得整环……174
习题 4-5　唯一分解整环上的多项式环……181

第 5 章　域的扩张 ····· 184
习题 5-1　向量空间 ····· 184
习题 5-2　扩域 ····· 191
习题 5-3　代数扩张 ····· 195
习题 5-4　多项式的分裂域 ····· 203
习题 5-5　有限域 ····· 206
习题 5-6　几何作图 ····· 210

第1章　群

习题 1-1　等价关系与集合的分类

1. 试分别举出满足下列条件的关系：

(1) 有对称性, 传递性, 但无反身性;

(2) 有反身性, 传递性, 但无对称性;

(3) 有反身性, 对称性, 但无传递性.

解　(1) $S=\mathbf{R}$, 对任意的 $a,b\in S$, 规定：$a\sim b \iff ab>0$.

(a) 如果 $ab>0$, 则显然有 $ba>0$, 因此 $\sim$ 有对称性;

(b) 如果 $ab>0$, $bc>0$, 则显然有 $ac>0$, 因此 $\sim$ 有传递性;

(c) 由于 $0\cdot 0=0$, 因此 $0\nsim 0$, 因此 $\sim$ 无反身性.

(2) $S=\mathbf{R}$, 对任意的 $a,b\in S$, 规定：$a\sim b \iff a\geqslant b$.

(a) 对任意的 $a\in S$, 则显然有 $a\geqslant a$, 因此 $\sim$ 有反身性;

(b) 如果 $a\geqslant b$, $b\geqslant c$, 则显然有 $a\geqslant c$, 因此 $\sim$ 有传递性;

(c) 由于 $2\geqslant 1$, 但 $1\ngeqslant 2$, 这说明 $\sim$ 无对称性.

(3) $S=\mathbf{Z}-\{1,-1\}$, 对任意的 $a,b\in S$, 规定：$a\sim b \iff (a,\,b)\neq 1$.

(a) 对任意的 $a\in S$, 由于 $a\neq\pm 1$, 因此 $(a,\,a)=|a|\neq 1$, 从而 $a\sim a$, 这说明 $\sim$ 具有反身性;

(b) 设 $a,b\in S$, 如果 $a\sim b$, 则 $(a,\,b)\neq 1$, 于是 $(b,\,a)=(a,\,b)\neq 1$, 从而 $b\sim a$, 这说明 $\sim$ 具有对称性;

(c) 取 $2,3,6\in S$, 则 $(2,\,6)=2,(6,\,3)=3,(2,\,3)=1$, 于是 $2\sim 6$, $6\sim 3$, 但 $2\nsim 3$, 这说明 $\sim$ 无传递性.

2. 找出下列证明中的错误：

有人断言, 若 S 的关系 $\mathcal{R}$ 有对称性和传递性, 则必有反身性. 这是因为, 对任意的 $a\in S$, 由对称性得, 如果 $a\mathcal{R}b$, 则 $b\mathcal{R}a$. 再由传递性, 得 $a\mathcal{R}a$, 所以 $\mathcal{R}$ 有反身性.

解　有可能在 S 中, 不存在元素 $b\in S$, 使 $a\mathcal{R}b$, 这样, 就不能由反身性和传递性推出 $a\mathcal{R}a$. 具体的例子可参见第 1(1) 题.

3. 证明：在数域 F 上全体 n 阶方阵的集合 M 中, 矩阵的等价、相合和相似都是等价关系.

证明　分别以 $\sim$, $\approx$, $\simeq$ 表示矩阵的等价、相合和相似关系.

(1) 设 $A,B,C\in M$, 则

(a) 因为 $\operatorname{rank}A=\operatorname{rank}A$, 所以 $A\sim A$, 于是 $\sim$ 具有反身性;

(b) 如果 $A\sim B$, 则 $\operatorname{rank}A=\operatorname{rank}B$, 于是 $\operatorname{rank}B=\operatorname{rank}A$, 从而 $B\sim A$, 这说明 $\sim$ 具有对称性;

(c) 如果 $A\sim B$, $B\sim C$, 则 $\operatorname{rank}A=\operatorname{rank}B$, $\operatorname{rank}B=\operatorname{rank}C$, 于是 $\operatorname{rank}A=\operatorname{rank}C$, 从而 $A\sim C$, 这说明 $\sim$ 具有传递性.

这就证明了矩阵的等价是集合 M 的一个等价关系.

(2) 设 $A,B,C\in M$, E 为单位矩阵, 则

(a) 因为 $E^{\mathrm{T}}AE=A$, 所以 $A\approx A$, 于是 $\approx$ 具有反身性;

(b) 如果 $A\approx B$, 则存在可逆矩阵 $P\in M$, 使 $P^{\mathrm{T}}AP=B$, 于是 $(P^{-1})^{\mathrm{T}}BP^{-1}=A$, 从而 $B\approx A$, 这说明 $\approx$ 具有对称性;

(c) 如果 $A\approx B$, $B\approx C$, 则存在可逆矩阵 $P,Q\in M$, 使 $P^{\mathrm{T}}AP=B$, $Q^{\mathrm{T}}BQ=C$, 于是 $(PQ)^{\mathrm{T}}A(PQ)=C$, 从而 $A\approx C$, 这说明 $\approx$ 具有传递性.

这就证明了矩阵的相合是集合 M 的一个等价关系.

(3) 设 $A,B,C\in M$, E 为单位矩阵, 则

(a) 因为 $E^{-1}AE=A$, 所以 $A\simeq A$, 于是 $\simeq$ 具有反身性;

(b) 如果 $A\simeq B$, 则存在可逆矩阵 $T\in M$, 使 $T^{-1}AP=B$, 于是 $(T^{-1})^{-1}BT^{-1}=A$, 从而 $B\simeq A$. 这说明 $\simeq$ 具有对称性;

(c) 如果 $A\simeq B$, $B\simeq C$, 则存在可逆矩阵 $T,S\in M$, 使 $T^{-1}AT=B$, $S^{-1}BS=C$, 于是 $(TS)^{-1}A(TS)=C$, 从而 $A\simeq C$, 这说明 $\simeq$ 具有传递性.

这就证明了矩阵的相似是集合 M 的一个等价关系.

4. 设 ϕ 是集合 A 到 B 的映射, $a,b\in A$, 规定关系 "$\sim$":

$$a\sim b\iff\phi(a)=\phi(b).$$

证明: $\sim$ 是 A 的一个等价关系, 并求其等价类.

证明　设 $a,b,c\in A$, 则

(a) 因为 $\phi(a)=\phi(a)$, 所以 $a\sim a$, 于是 $\sim$ 具有反身性;

(b) 如果 $a\sim b$, 则 $\phi(a)=\phi(b)$, 于是 $\phi(b)=\phi(a)$, 从而 $b\sim a$, 这说明 $\sim$ 具有对称性;

(c) 如果 $a\sim b$, $b\sim c$, 则 $\phi(a)=\phi(b)$, $\phi(b)=\phi(c)$, 从而 $\phi(a)=\phi(c)$, 这说明 $\sim$ 具有传递性.

这就证明了 $\sim$ 是集合 A 的一个等价关系.

此等价关系的全体等价类为

$$A/\sim=\{[a]\,|\,a\in A\},$$

其中

$$[a]=\{x\in A\,|\,\phi(x)=\phi(a)\}.$$

5. 设 $A=\{1,2,3,4\}$, 在 $\mathcal{P}(A)$ 中规定关系 "$\sim$":

$$S_1\sim S_2 \iff S_1 \text{ 与 } S_2 \text{ 含有相同个数的元素.}$$

证明: $\sim$ 是 $\mathcal{P}(A)$ 的一个等价关系, 并求商集 $\mathcal{P}(A)/\sim$.

证明　以 $|S|$ 表示集合 S 所含元素的个数. 设 $P,Q,S\in\mathcal{P}(A)$, 则

(a) 因为 $|P|=|P|$, 所以 $P\sim P$, 于是 $\sim$ 具有反身性;

(b) 如果 $P\sim Q$, 则 $|P|=|Q|$, 于是 $|Q|=|P|$, 从而 $Q\sim P$, 这说明 $\sim$ 具有对称性;

(c) 如果 $P\sim Q$, $Q\sim S$, 则 $|P|=|Q|$, $|Q|=|S|$, 于是 $|P|=|S|$, 从而 $P\sim S$, 这说明 $\sim$ 具有传递性.

这就证明了 $\sim$ 是集合 $\mathcal{P}(A)$ 的一个等价关系.

相应的商集

$$\mathcal{P}(A)/\sim=\{[\varnothing],[\{1\}],[\{1,2\}],[\{1,2,3\}],[\{1,2,3,4\}]\},$$

其中

$$\begin{aligned}
&[\{1\}]=\{\{1\},\{2\},\{3\},\{4\}\},\\
&[\{1,2\}]=\{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\},\\
&[\{1,2,3\}]=\{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}\},\\
&[\{1,2,3,4\}]=\{\{1,2,3,4\}\}.
\end{aligned}$$

6. 在有理数集 $\mathbf{Q}$ 中, 规定关系 "$\sim$":

$$a\sim b \iff a-b\in\mathbf{Z}.$$

证明: $\sim$ 是 $\mathbf{Q}$ 的一个等价关系, 并求出所有的等价类.

证明　设 $a,b,c\in\mathbf{Q}$, 则

(a) 因为 $a-a=0\in\mathbf{Z}$, 所以 $a\sim a$, 于是 $\sim$ 具有反身性;

(b) 如果 $a\sim b$, 则 $a-b\in\mathbf{Z}$, 于是 $b-a\in\mathbf{Z}$, 从而 $b\sim a$, 这说明 $\sim$ 具有对称性;

(c) 如果 $a\sim b$, $b\sim c$, 则 $a-b\in\mathbf{Z}$, $b-c\in\mathbf{Z}$, 于是 $a-c=(a-b)+(b-c)\in\mathbf{Z}$, 从而 $a\sim c$, 这说明 $\sim$ 具有传递性.

这就证明了 $\sim$ 是 $\mathbf{Q}$ 的一个等价关系.

此等价关系的全体等价类为

$$\mathbf{Q}/\sim=\{[r]\,|\,r\in\mathbf{Q}\ \text{且}\ 0\leqslant r<1\},$$

其中

$$[r]=\{r+z\,|\,z\in\mathbf{Z}\}.$$

7. 在复数集 $\mathbf{C}$ 中, 规定关系 "$\sim$":

$$a\sim b\Longleftrightarrow|a|=|b|.$$

证明: $\sim$ 是 $\mathbf{C}$ 的一个等价关系, 试确定相应的商集 $\mathbf{C}/\sim$, 并给出每个等价类的一个代表元素.

证明　设 $a,b,c\in\mathbf{C}$, 则

(a) 因为 $|a|=|a|$, 所以 $a\sim a$, 于是 $\sim$ 具有反身性;

(b) 如果 $a\sim b$, 则 $|a|=|b|$, 于是 $|b|=|a|$, 从而 $b\sim a$, 这说明 $\sim$ 具有对称性;

(c) 如果 $a\sim b$, $b\sim c$, 则 $|a|=|b|$, $|b|=|c|$, 于是 $|a|=|c|$, 从而 $a\sim c$, 这说明 $\sim$ 具有传递性.

这就证明了 $\sim$ 是 $\mathbf{C}$ 的一个等价关系.

相应的商集

$$\mathbf{C}/\sim=\{[r]\,|\,r\in\mathbf{R}\ \text{且}\ r\geqslant 0\},$$

其中

$$[r]=\{x\in\mathbf{C}\,|\,|x|=r\}=\{r(\cos\theta+\mathrm{i}\sin\theta)\,|\,\theta\in[0,2\pi)\}.$$

对任意的 $c\in\mathbf{C}$, 等价类 $[c]$ 的代表元素可取作 $|c|$.

8. 设集合

$$S=\{(a,\,b)\ |\ a,b\in\mathbf{Z},b\neq 0\}.$$

在集合 S 中, 规定关系 "$\sim$":

$$(a,\,b)\sim(c,\,d)\iff ad=bc.$$

证明: $\sim$ 是 S 的一个等价关系.

证明　设 $(a,\,b),(c,\,d),(e,\,f)\in S$, 则

(a) 因为 $ab=ba$, 所以 $(a,\,b)\sim(a,\,b)$, 于是 $\sim$ 具有反身性;

(b) 如果 $(a,\,b)\sim(c,\,d)$, 则 $ad=bc$, 于是 $cb=da$, 从而 $(c,\,d)\sim(a,\,b)$, 这说明 $\sim$ 具有对称性;

(c) 如果 $(a,\,b)\sim(c,\,d)$, $(c,\,d)\sim(e,\,f)$, 则 $ad=bc$, $cf=de$, 于是 $adf=bcf=bde$. 由于 $d\neq 0$, 因此 $af=be$, 从而 $(a,\,b)\sim(e,\,f)$, 这说明 $\sim$ 具有传递性.

这就证明了 $\sim$ 是 S 的一个等价关系.

*9. 设 $A=\{a, b, c, d\}$, 试写出集合 A 的所有不同的等价关系.

解　按例 9 中的方法, 可知 A 共有如下 15 个不同的等价关系:

$$\sim_1=\{a\sim a,b\sim b,c\sim c,d\sim d,a\sim b,b\sim a,a\sim c,c\sim a,a\sim d,$$
$$d\sim a,b\sim c,c\sim b,b\sim d,d\sim b,c\sim d,d\sim c\};$$
$$\sim_2=\{a\sim a,b\sim b,c\sim c,d\sim d,b\sim c,c\sim b,b\sim d,d\sim b,c\sim d,d\sim c\};$$
$$\sim_3=\{a\sim a,b\sim b,c\sim c,d\sim d,a\sim c,c\sim a,a\sim d,d\sim a,c\sim d,d\sim c\};$$
$$\sim_4=\{a\sim a,b\sim b,c\sim c,d\sim d,a\sim b,b\sim a,a\sim d,d\sim a,b\sim d,d\sim b\};$$
$$\sim_5=\{a\sim a,b\sim b,c\sim c,d\sim d,a\sim b,b\sim a,a\sim c,c\sim a,b\sim c,c\sim b\};$$
$$\sim_6=\{a\sim a,b\sim b,c\sim c,d\sim d,a\sim b,b\sim a,c\sim d,d\sim c\};$$
$$\sim_7=\{a\sim a,b\sim b,c\sim c,d\sim d,a\sim c,c\sim a,b\sim d,d\sim b\};$$
$$\sim_8=\{a\sim a,b\sim b,c\sim c,d\sim d,a\sim d,d\sim a,b\sim c,c\sim b\};$$
$$\sim_9=\{a\sim a,b\sim b,c\sim c,d\sim d,c\sim d,d\sim c\};$$
$$\sim_{10}=\{a\sim a,b\sim b,c\sim c,d\sim d,b\sim d,d\sim b\};$$
$$\sim_{11}=\{a\sim a,b\sim b,c\sim c,d\sim d,b\sim c,c\sim b\};$$
$$\sim_{12}=\{a\sim a,b\sim b,c\sim c,d\sim d,a\sim b,b\sim a\};$$
$$\sim_{13}=\{a\sim a,b\sim b,c\sim c,d\sim d,a\sim c,c\sim a\};$$
$$\sim_{14}=\{a\sim a,b\sim b,c\sim c,d\sim d,a\sim d,d\sim a\};$$
$$\sim_{15}=\{a\sim a,b\sim b,c\sim c,d\sim d\}.$$

*10. 不用公式 (1.1.1), 直接算出集合 $A=\{1, 2, 3, 4, 5\}$ 的不同的分类数.

解　设 $A_n=\{1,2,\cdots,n\}$, $B(n)$ 为集合 A_n 的不同的分类数, $B(n,k)$ 为集合 A_n 分划为 k 个不同子集的分类数. 显然有

$$B(n)=\sum_{k=1}^{n}B(n,k).$$

下面给出计算 $B(n,k)$ 和 $B(n)$ 的方法:

为简便起见, 称集合 A_n 分划为 k 个不同子集的任一种分类为集合 A_n 的一个 k 分划. 易知:

(1) 如果 $\{S_1,S_2,\cdots,S_{k-1}\}$ 是 A_{n-1} 的任一个 $k-1$ 分划, 则 $\{S_1,S_2,\cdots,S_{k-1},\{n\}\}$ 就是 A_n 的一个 k 分划.

(2) 如果 $\{S_1,S_2,\cdots,S_k\}$ 是 A_{n-1} 的任一个 k 分划, 则

$$\{S_1 \cup \{n\}, S_2, \cdots, S_k\},$$
$$\{S_1, S_2 \cup \{n\}, S_3, \cdots, S_k\},$$
$$\cdots\cdots$$
$$\{S_1, S_2, \cdots, S_{k-1}, S_k \cup \{n\}\}$$

都是 A_n 的 k 分划.

显然, A_n 的任一个 k 分划都可如此得到. 由此得

$$B(n,k) = kB(n-1,k) + B(n-1,k-1). \tag{1.1.1}$$

由此递推公式, 可得下表:

$B(n,k)$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$\cdots$	B_n
$n=1$	1						1
$n=2$	1	1					2
$n=3$	1	3	1				5
$n=4$	1	7	6	1			15
$n=5$	1	15	25	10	1		52
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$

由表中的第六行, 立即可得 $B(5) = 52$, 即 $A = \{1, 2, 3, 4, 5\}$ 的不同的分类数为 52.

习题 1-2　群 的 概 念

1. 证明: 实数域 $\mathbf{R}$ 上全体 n 阶方阵的集合 $M_n(\mathbf{R})$, 关于矩阵的加法构成一个交换群.

证明　(1) 矩阵的加法显然是 $M_n(\mathbf{R})$ 的代数运算.

(2) 矩阵的加法满足结合律和交换律.

(3) 对任意的矩阵 $A \in M_n(\mathbf{R})$, 有

$$A + 0 = 0 + A = A,$$

所以零矩阵 0 是 $M_n(\mathbf{R})$ 关于加法的零元.

(4) 对任意的 $A \in M_n(\mathbf{R})$, 有 $-A \in M_n(\mathbf{R})$, 且

$$A + (-A) = (-A) + A = 0,$$

所以 $M_n(\mathbf{R})$ 中每个元素关于矩阵的加法都有负元.

由此知, $(M_n(\mathbf{R}), +)$ 构成一个交换群.

2. 证明: 实数域 $\mathbf{R}$ 上全体 n 阶可逆方阵的集合 $GL_n(\mathbf{R})$ 关于矩阵的乘法构成群. 这个群称为 n 阶**一般线性群**.

证明 (1) 设 $A, B \in GL_n(\mathbf{R})$, 则 A, B 可逆, 于是 AB 也可逆, 从而 $AB \in GL_n(\mathbf{R})$, 所以矩阵的乘法是 $GL_n(\mathbf{R})$ 的代数运算.

(2) 因为矩阵的乘法满足结合律, 所以 $GL_n(\mathbf{R})$ 中的乘法运算也满足结合律.

(3) 单位矩阵 $E \in GL_n(\mathbf{R})$, 且对任意的矩阵 $A \in GL_n(\mathbf{R})$, 有

$$EA = AE = A,$$

所以单位矩阵 E 是 $GL_n(\mathbf{R})$ 的单位元.

(4) 对任意的 $A \in GL_n(\mathbf{R})$, 则 A 可逆, 于是 A^{-1} 存在且可逆, 从而 $A^{-1} \in GL_n(\mathbf{R})$, 且

$$A \cdot A^{-1} = A^{-1} \cdot A = E,$$

所以 $GL_n(\mathbf{R})$ 中每个元素在 $GL_n(\mathbf{R})$ 中都可逆.

由此知, $(GL_n(\mathbf{R}), \cdot)$ 构成一个群.

3. 证明: 实数域 $\mathbf{R}$ 上全体 n 阶正交矩阵的集合 $O_n(\mathbf{R})$, 关于矩阵的乘法构成一个群. 这个群称为 n 阶**正交群**.

证明 (1) 设 $A, B \in O_n(\mathbf{R})$, 则 A, B 为正交矩阵, 于是 AB 也是正交矩阵, 从而 $AB \in O_n(\mathbf{R})$, 所以矩阵的乘法是 $O_n(\mathbf{R})$ 的代数运算.

(2) 因为矩阵的乘法满足结合律, 所以 $O_n(\mathbf{R})$ 中的乘法运算也满足结合律.

(3) 单位矩阵 $E \in O_n(\mathbf{R})$, 且对任意的矩阵 $A \in O_n(\mathbf{R})$, 有

$$EA = AE = A,$$

所以单位矩阵 E 是 $O_n(\mathbf{R})$ 的单位元.

(4) 对任意的 $A \in O_n(\mathbf{R})$, 则 A 是正交矩阵, 于是 A^{-1} 存在且是正交矩阵, 从而 $A^{-1} \in O_n(\mathbf{R})$, 且

$$A \cdot A^{-1} = A^{-1} \cdot A = E,$$

所以 $O_n(\mathbf{R})$ 中每个元素在 $O_n(\mathbf{R})$ 中都可逆.

由此知, $(O_n(\mathbf{R}), \cdot)$ 构成一个群.

4. 证明: 所有行列式等于 1 的 n 阶整数矩阵组成的集合 $SL_n(\mathbf{Z})$, 关于矩阵的乘法构成群.

证明 (1) 设 $A, B \in SL_n(\mathbf{Z})$, 则 A, B 都是行列式为 1 的整数矩阵, 于是 AB 也是整数矩阵且 $|AB| = 1$, 从而 $AB \in SL_n(\mathbf{Z})$, 所以矩阵的乘法是 $SL_n(\mathbf{Z})$ 的代数运算.

(2) 因为矩阵的乘法满足结合律, 所以 $SL_n(\mathbf{Z})$ 中的乘法运算也满足结合律.

(3) 单位矩阵 $E \in SL_n(\mathbf{Z})$, 且对任意的矩阵 $A \in SL_n(\mathbf{Z})$, 有

$$EA = AE = A,$$

所以单位矩阵 E 是 $SL_n(\mathbf{Z})$ 的单位元.

(4) 对任意的 $A \in SL_n(\mathbf{Z})$, 则 A 是整数矩阵且 $|A| = 1$, 于是 A 的伴随矩阵 A^* 也是整数矩阵且 $|A^*| = 1$, 从而 $A^* \in SL_n(\mathbf{Z})$, 且

$$A \cdot A^* = A^* \cdot A = |A|E = E,$$

所以 $SL_n(\mathbf{Z})$ 中每个元素在 $SL_n(\mathbf{Z})$ 中都可逆.

由此知, $(SL_n(\mathbf{Z}), \cdot)$ 构成一个群.

5. 在整数集 $\mathbf{Z}$ 中, 规定运算 "$\oplus$" 如下:

$$a \oplus b = a + b - 2, \qquad \forall a, b \in \mathbf{Z}.$$

证明: $(\mathbf{Z}, \oplus)$ 构成群.

证明　(1) 显然 $\oplus$ 为 $\mathbf{Z}$ 的代数运算.

(2) 对任意的 $a, b, c \in \mathbf{Z}$, 有

$$a \oplus b = a + b - 2 = b + a - 2 = b \oplus a,$$

所以交换律成立.

(3) 对任意的 $a, b, c \in \mathbf{Z}$, 有

$$\begin{aligned}(a \oplus b) \oplus c &= (a + b - 2) \oplus c = (a + b - 2) + c - 2 \\ &= a + (b + c - 2) - 2 = a + (b \oplus c) - 2 \\ &= a \oplus (b \oplus c),\end{aligned}$$

所以结合律成立.

(4) 对任意的 $a \in \mathbf{Z}$, 因为

$$a \oplus 2 = a + 2 - 2 = a = 2 \oplus a,$$

所以零元为 $2 \in \mathbf{Z}$.

(5) 对任意的 $a \in \mathbf{Z}$, 因为

$$a \oplus (-a + 4) = a + (-a + 4) - 2 = 2 = (-a + 4) \oplus a,$$

所以 a 的负元为 $-a + 4$.

由此知, $(\mathbf{Z}, \oplus)$ 构成群.

6. 分别写出下列各群的乘法表.

(1) 例 6 中的群;　(2) 群 U_7;　(3) 群 $\mathbf{Z}_7^*$;　(4) 群 $U(18)$.

解　(1)

	1	−1	i	−i
1	1	−1	i	−i
−1	−1	1	−i	i
i	i	−i	−1	1
−i	−i	i	1	−1

(2) 记 $\omega = \cos\dfrac{2\pi}{7} + \mathrm{i}\sin\dfrac{2\pi}{7}$.

	1	ω	ω^2	ω^3	ω^4	ω^5	ω^6
1	1	ω	ω^2	ω^3	ω^4	ω^5	ω^6
ω	ω	ω^2	ω^3	ω^4	ω^5	ω^6	1
ω^2	ω^2	ω^3	ω^4	ω^5	ω^6	1	ω
ω^3	ω^3	ω^4	ω^5	ω^6	1	ω	ω^2
ω^4	ω^4	ω^5	ω^6	1	ω	ω^2	ω^3
ω^5	ω^5	ω^6	1	ω	ω^2	ω^3	ω^4
ω^6	ω^6	1	ω	ω^2	ω^3	ω^4	ω^5

(3)

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

(4)

	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

注　表中的 a 表示 $\bar{a}$.

7. 设 $G = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \middle| a \in \mathbf{R}, a \neq 0 \right\}$. 证明: G 关于矩阵的乘法构成群.

证明　(1) 设 $A=\begin{pmatrix} a & a \\ a & a \end{pmatrix}, B=\begin{pmatrix} b & b \\ b & b \end{pmatrix} \in G$, 则 $AB=\begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix} \in G$, 所以矩阵的乘法是 G 的代数运算.

(2) 因为矩阵的乘法满足结合律, 所以 G 的乘法也满足结合律.

(3) 因为 $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \in G$, 且对任意的 $A=\begin{pmatrix} a & a \\ a & a \end{pmatrix} \in G$, 有

$$\begin{pmatrix} a & a \\ a & a \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} a & a \\ a & a \end{pmatrix} = \begin{pmatrix} a & a \\ a & a \end{pmatrix},$$

所以单位元为 $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$.

(4) 对任意的 $A=\begin{pmatrix} a & a \\ a & a \end{pmatrix} \in G$, 有 $B=\begin{pmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{pmatrix} \in G$, 且

$$\begin{pmatrix} a & a \\ a & a \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{pmatrix} = \begin{pmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{pmatrix} \cdot \begin{pmatrix} a & a \\ a & a \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix},$$

即 $B=\begin{pmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{pmatrix}$ 为 G 的逆元, 所以 G 的每个元素都可逆.

这就证明了 G 关于矩阵的乘法构成群.

8. 证明: 所有形如 $2^m3^n(m,n\in\mathbf{Z})$ 的有理数的集合关于数的乘法构成群.

证明　设 $G=\{2^m3^n \mid m,n\in\mathbf{Z}\}$.

(1) 对任意的 $x=2^{m_1}3^{n_1}, y=2^{m_2}3^{n_2} \in G$,

$$xy=2^{m_1}3^{n_1}2^{m_2}3^{n_2}=2^{m_1+m_2}3^{n_1+n_2}\in G,$$

所以数的乘法是 G 的代数运算.

(2) 因为数的乘法满足结合律和交换律, 所以 G 的乘法也满足结合律和交换律.

(3) 因为 $1=2^03^0\in G$, 且对任意的 $x=2^m3^n\in G$,

$$1\cdot x=x\cdot 1=x=2^m3^n,$$