《离散数学教程》[1]
习题解答[2]

(*beta 16.11*)[3]

SOLVED AND TEXIFIED

BY

肖新攀[4]

新版本下载、考研相关问题讨论

请到计算机科学论坛—计算机考研交流版

(`http://www.ieee.org.cn/list.asp?boardid=67`)

---

[1]《离散数学教程》，耿素云、屈婉玲、王捍贫，北京大学出版社，2002年6月第1版，2003年1月第2次印刷

[2]此“习题解答”系个人作品，仅供学习交流之用，可以自由复制、打印和传播，但不得用作商业用途。如发现解答有错误，烦请告知作者(E-mail: xiaoxinpan@163.com)。

[3]版本号的整数部分表示该版本所包含答案的章数。发布日期：2006 年 11 月 1 日。完成度(已完成题数/总题数)：60.17%

[4]由衷感谢 xbz 网友完成并制作本“习题解答”第十章和第十四章的全部内容、仔细检查其它各章节并提出众多修改意见和新的证明方法。感谢南京大学计算机系胡海星大侠长期以来给予我热情的鼓励和无私的帮助。感谢南京大学 02 计算机系赖江山同学提出各种建议和证明思路。感谢北京大学计算机系刘田教授给予我的帮助和鼓励。感谢 chouxiaoya、tedy、akaru、yitianxing、xuening、ourszf、ushing、pizzamx、datoubaicai、echoqing、soup1122、lycool、hamletyj、leejunner、zliner、sunbird2002、zhaoming169、zqliu、qiushuitian1111、tcschen、Supremgoooo、Smilingface、yangling_1985、jianzhentianxia、ouyangj0、kylinwang、赵现刚、熊亮等网友提出大量修改意见和新的证明方法。谢谢你们!

目录

第一编

集合论

第一章　集合

1.1

(1)　$\{2\}$；

(2)　$\{1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196\}$；

(3)　$\{1, 8, 27, 64\}$；

(4)　$\{0, 1, 2, \cdots\}$；

(5)　$\{2, 3\}$；

(6)　$\{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z, A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z\}$。

1.2

(1)　$\{(x, y) \mid x, y \in \mathbb{R} \land x^2 + y^2 < 1\}$；

(2)　$\{\theta \mid \exists k(k \in \mathbb{Z} \land \theta = \dfrac{\pi}{4} + k\pi)\}$；

(3)　$\{x \mid x \in \mathbb{N} \land x < 8\}$；

(4)　$\{(x, y, z) \mid x, y, z \in \mathbb{N} \land x^2 + y^2 = z^2\}$；

(5)　$\{x \mid x \in \mathbb{R} \land x^2 + 5x + 6 = 0\}$。

1.3　(1), (4), (5), (6), (8), (9) 正确，其余不正确。

1.4

(1)　成立。

证明:

$$\begin{aligned}
& A \in B \land B \subseteq C \\
\Longleftrightarrow\ & A \in B \land \forall x(x \in B \to x \in C) && \text{(子集关系定义)} \\
\Longrightarrow\ & A \in B \land (A \in B \to A \in C) && \text{(x/A)} \\
\Longrightarrow\ & A \in C && \text{(假言推理)}
\end{aligned}$$

□

(2)　不成立。举反例如下：令 $A = \{a\}, B = \{\{a\}\}, C = \{\{a\}, \{b\}\}$，则有 $A \in B \land B \subseteq C$，但 $A \nsubseteq C$。

(3)　不成立。举反例如下：令 $A = \{a\}, B = \{a, b\}, C = \{\{a, b\}, \{b, c\}\}$，则有 $A \subseteq B \land B \in C$，但 $A \notin C$。

(4)　不成立。举反例如下：令 $A = \{a\}, B = \{a, b\}, C = \{\{a, b\}, \{b, c\}\}$，则有 $A \subseteq B \land B \in C$，但

$A \nsubseteq C$。

1.5 令 $A = \{a\}, B = \{\{a\}\}, C = \{\{\{a\}\}\}$，则有 $A \in B \wedge B \in C$，但 $A \notin C$。

1.6

(1) 0 元集：$\varnothing$
1 元集：$\{a\}, \{b\}, \{c\}$
2 元集：$\{a, b\}, \{a, c\}, \{b, c\}$
3 元集：$\{a, b, c\}$
幂集：$\{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$

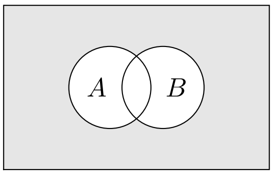
(2) 0 元集：$\varnothing$
1 元集：$\{1\}, \{\{2, 3\}\}$
2 元集：$\{1, \{2, 3\}\}$
幂集：$\{\varnothing, \{1\}, \{\{2, 3\}\}, \{1, \{2, 3\}\}\}$

(3) 0 元集：$\varnothing$
1 元集：$\{\varnothing\}, \{\{\varnothing\}\}$
2 元集：$\{\varnothing, \{\varnothing\}\}$
幂集：$\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}$

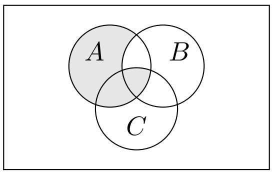
(4) 0 元集：$\varnothing$
1 元集：$\{\{1, 2\}\}$
幂集：$\{\varnothing, \{\{1, 2\}\}\}$

(5) 0 元集：$\varnothing$
1 元集：$\{\{\varnothing, 1\}\}, \{1\}$
2 元集：$\{\{\varnothing, 1\}, 1\}$
幂集：$\{\varnothing, \{\{\varnothing, 1\}\}, \{1\}, \{\{\varnothing, 1\}, 1\}\}$

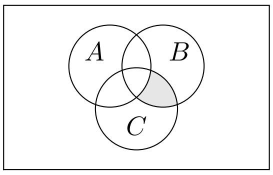
1.7



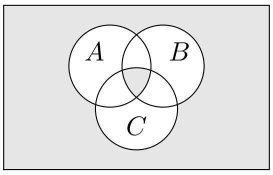
$\sim(A \cup B)$



$A \cap (\sim B \cup C)$



$\sim A \cap (B \cap C)$



$(A \cap B \cap C) \cup \sim(A \cup B \cup C)$

1.8

(1) $\{4\}$；
(2) $\{1, 3, 5\}$；

(3) $\{2,3,4,5\}$；

(4) $\{2,3,4,5\}$；

(5) $\{\varnothing,\{4\}\}$；

(6) $\{\{1\},\{1,4\}\}$。

1.9

(1) $\{-7,-6,-5,-4,-3,-2,-1,0,1,2,3,4,5,6,7,8,9,12,15,16,18,21,24,27,30,32,64\}$；

(2) $\varnothing$；

(3) $\{-7,-6,-5,-4,-3,-2,-1,4,5\}$；

(4) $\{-7,-6,-5,-4,-3,-2,-1,0,3,4,5,6,9,12,15,18,21,24,27,30\}$。

1.10 因为 $\mathcal{P}(A)=\{\varnothing,\{a\}\}$，$\mathcal{P}\mathcal{P}(A)=\{\varnothing,\{\varnothing\},\{\{a\}\},\{\varnothing,\{a\}\}\}$，故 (1), (2), (4), (5) 成立，其余不成立。

1.11

证明: 必要性：

若 $A-B=A$，则有：

$$\begin{aligned}
A\cap B &= (A-B)\cap B && (A-B=A)\\
&= (A\cap\sim B)\cap B && (\text{补交转换律})\\
&= A\cap(\sim B\cap B) && (\text{结合律})\\
&= A\cap\varnothing && (\text{矛盾律})\\
&= \varnothing && (\text{零律})
\end{aligned}$$

充分性：

若 $A\cap B=\varnothing$，则有：

$$\begin{aligned}
A &= A\cap E && (\text{同一律})\\
&= A\cap(B\cup\sim B) && (\text{排中律})\\
&= (A\cap B)\cup(A\cap\sim B) && (\text{分配律})\\
&= \varnothing\cup(A\cap\sim B) && (A\cap B=\varnothing)\\
&= A\cap\sim B && (\text{同一律})\\
&= A-B && (\text{补交转换律})
\end{aligned}$$

综合得：$A-B=A\Leftrightarrow A\cap B=\varnothing$。 □

1.12 先证一个引理：

引理 1.1 对任意集合 A 和 B，有 $A-B=\varnothing\Leftrightarrow A\subseteq B$。

证明:

$$\begin{aligned}
A-B=\varnothing &\iff \neg\exists x(x\in(A-B)) && (\varnothing\ \text{定义})\\
&\iff \forall x\neg(x\in(A-B)) && (\text{量词否定等值式})\\
&\iff \forall x\neg(x\in A\wedge x\notin B) && (\text{相对补定义})\\
&\iff \forall x\neg(x\in A\wedge\neg x\in B) && (\notin\ \text{定义})\\
&\iff \forall x(\neg x\in A\vee x\in B) && (\text{命题逻辑德·摩根律})\\
&\iff \forall x(x\in A\to x\in B) && (\text{蕴涵等值式})\\
&\iff A\subseteq B && (\text{子集关系定义})
\end{aligned}$$

□

(1) 答：$(A-B)\cup(A-C)=A$ 当且仅当 $A\cap B\cap C=\varnothing$ 。

证明:

$$\begin{aligned}(A-B)\cup(A-C)=A &\iff A-(B\cap C)=A && \text{(德·摩根律)}\\ &\iff A\cap(B\cap C)=\varnothing && \text{(习题 1.11 结论)}\\ &\iff A\cap B\cap C=\varnothing && \text{(结合律)}\end{aligned}$$

□

(2) 答：$(A-B)\cup(A-C)=\varnothing$ 当且仅当 $A\subseteq(B\cap C)$。

证明:

$$\begin{aligned}(A-B)\cup(A-C)=\varnothing &\iff A-(B\cap C)=\varnothing && \text{(德·摩根律)}\\ &\iff A\subseteq(B\cap C) && \text{(引理 1.1)}\end{aligned}$$

□

(3) 答：$(A-B)\cap(A-C)=\varnothing$ 当且仅当 $A\subseteq(B\cup C)$。

证明:

$$\begin{aligned}(A-B)\cap(A-C)=\varnothing &\iff A-(B\cup C)=\varnothing && \text{(德·摩根律)}\\ &\iff A\subseteq(B\cup C) && \text{(引理 1.1)}\end{aligned}$$

□

(4) 答：$(A-B)\cap(A-C)=A$ 当且仅当 $A\cap(B\cup C)=\varnothing$。

证明:

$$\begin{aligned}(A-B)\cap(A-C)=A &\iff A-(B\cup C)=A && \text{(德·摩根律)}\\ &\iff A\cap(B\cup C)=\varnothing && \text{(习题 1.11 结论)}\end{aligned}$$

□

1.13

(1) 先证两个引理：

引理 1.2 对任意集合 A 和 B，有：$A\cap B\subseteq A$ 和 $A\cap B\subseteq B$。

证明: $\forall x$，

$$\begin{aligned}x\in A\cap B &\iff x\in A\wedge x\in B && \text{(集合交定义)}\\ &\implies x\in A && \text{(命题逻辑化简律)}\end{aligned}$$

故有，$A\cap B\subseteq A$。同理可证：$A\cap B\subseteq B$。 □

引理 1.3 对任意集合 A 和 B，有：$A\subseteq A\cup B$ 和 $B\subseteq A\cup B$

证明: $\forall x$，

$$\begin{aligned}x\in A &\implies x\in A\vee x\in B && \text{(命题逻辑附加律)}\\ &\iff x\in A\cup B && \text{(集合并定义)}\end{aligned}$$

故有，$A\subseteq A\cup B$。同理可证：$B\subseteq A\cup B$。 □

再证原题：

证明:

$$\begin{aligned}(A-B)-C &= (A\cap\sim B)\cap\sim C && \text{(补交转换律)}\\ &\subseteq A\cap\sim B && \text{(引理 1.2)}\end{aligned}$$

$$
\begin{aligned}
&\subseteq (A\cap\sim B)\cup(A\cap C) && \text{(引理 1.3)}\\
&= A\cap(\sim B\cup C) && \text{(分配律)}\\
&= A\cap\sim(B\cap\sim C) && \text{(德·摩根律)}\\
&= A-(B-C) && \text{(补交转换律)}
\end{aligned}
$$

□

(2) 答：当且仅当 $A\cap C=\varnothing$ 时，(1) 中等号成立。

证明： 先证充分性。当 $A\cap C=\varnothing$ 时：

$$
\begin{aligned}
(A-B)-C &= (A\cap\sim B)\cap\sim C && \text{(补交转换律)}\\
&= (A\cap\sim C)\cap\sim B && \text{(结合律、交换律)}\\
&= (A-C)\cap\sim B && \text{(补交转换律)}\\
&= A\cap\sim B && \text{(习题 1.11 结论)}\\
&= (A\cap\sim B)\cup\varnothing && \text{(同一律)}\\
&= (A\cap\sim B)\cup(A\cap C) && (A\cap C=\varnothing)\\
&= A\cap(\sim B\cup C) && \text{(分配律)}\\
&= A\cap\sim(B\cap\sim C) && \text{(德·摩根律)}\\
&= A-(B-C) && \text{(补交转换律)}
\end{aligned}
$$

再证必要性。若不然，则存在 x，使得 $x\in A\wedge x\in C$。此时，无论 x 是否属于 B，均有 $x\notin(A-B)-C$ 和 $x\in A-(B-C)$。这与假设：$(A-B)-C=A-(B-C)$ 矛盾。 □

1.14

证明：

$$
\begin{aligned}
B &= E\cap B && \text{(同一律)}\\
&= (A\cup\sim A)\cap B && \text{(排中律)}\\
&= (A\cap B)\cup(\sim A\cap B) && \text{(分配律)}\\
&= (A\cap C)\cup(\sim A\cap C) && \text{(前提)}\\
&= (A\cup\sim A)\cap C && \text{(分配律)}\\
&= E\cap C && \text{(排中律)}\\
&= C && \text{(同一律)}
\end{aligned}
$$

□

1.15 $A=B=D=G$，$C=F=H$。

1.16

(1) $\{3,4,\{3\},\{4\}\}$；

(2) $\varnothing$；

(3) $\{\varnothing,\{\varnothing\}\}$。

1.17

(1) $\{\varnothing,\{\{\varnothing\}\},\{\{\{\varnothing\}\}\},\{\{\varnothing\},\{\{\varnothing\}\}\}\}$；

(2) $\{\varnothing,\{\varnothing\},\{\{\varnothing\}\},\{\varnothing,\{\varnothing\}\}\}$；

(3) $\{\{\varnothing\},\{\{\varnothing\}\}\}$。

1.18

(1) $\{\varnothing,1,2,3\}$；

(2) $\varnothing$；

(3) $\varnothing$；

(4) $\varnothing$。

1.19

(1) $A\cup B$；

(2) A；

(3) B。

1.20 先证两个引理。

引理 1.4 对任意集合 A,B,C,D，有 $A\subseteq B\wedge C\subseteq D\Rightarrow A\cup C\subseteq B\cup D$

证明: $\forall x$，

$$\begin{aligned}
x\in A\cup C &\iff x\in A\vee x\in C && \text{(集合并定义)}\\
&\iff (x\in A\vee x\in C)\wedge\\
&\qquad (x\in A\rightarrow x\in B\wedge x\in C\rightarrow x\in D) && \text{(前提、子集关系定义)}\\
&\implies x\in B\vee x\in D && \text{(构造性二难)}\\
&\iff x\in B\cup D && \text{(集合并定义)}
\end{aligned}$$

□

引理 1.5 对任意集合 A,B,C,D，有 $A\subseteq B\wedge C\subseteq D\Rightarrow A\cap C\subseteq B\cap D$

证明: $\forall x$，

$$\begin{aligned}
x\in A\cap C &\iff x\in A\wedge x\in C && \text{(集合交定义)}\\
&\implies x\in B\wedge x\in C && \text{(前提、子集关系定义)}\\
&\implies x\in B\wedge x\in D && \text{(前提、子集关系定义)}\\
&\iff x\in B\cap D && \text{(集合交定义)}
\end{aligned}$$

□

再证原题。

证明:

$$\begin{aligned}
A &= A\cap E && \text{(同一律)}\\
&= A\cap(C\cup\sim C) && \text{(排中律)}\\
&= (A\cap C)\cup(A\cap\sim C) && \text{(分配律)}\\
&\subseteq (B\cap C)\cup(B\cap\sim C) && \text{(题设、引理 1.4)}\\
&= B\cap(C\cup\sim C) && \text{(分配律)}\\
&= B\cap E && \text{(排中律)}\\
&= B && \text{(同一律)}
\end{aligned}$$

□

1.21

(1) 答：$A\cap B=A$ 当且仅当 $A\subseteq B$。

证明:

$A \cap B = A$

$\iff \forall x((x \in A \land x \in B) \leftrightarrow x \in A)$ (外延原则、集合交定义)

$\iff \forall x(((x \in A \land x \in B) \to x \in A) \land (x \in A \to (x \in A \land x \in B)))$ (等价联结词定义)

$\iff \forall x((\neg(x \in A \land x \in B) \lor x \in A) \land (\neg x \in A \lor (x \in A \land x \in B)))$ (蕴涵等值式)

$\iff \forall x((\neg x \in A \lor \neg x \in B \lor x \in A) \land (\neg x \in A \lor (x \in A \land x \in B)))$ (命题逻辑德·摩根律)

$\iff \forall x((\neg x \in A \lor x \in A \lor \neg x \in B) \land (\neg x \in A \lor (x \in A \land x \in B)))$ (命题逻辑交换律)

$\iff \forall x((\neg x \in A \lor x \in A \lor \neg x \in B) \land$

$((\neg x \in A \lor x \in A) \land (\neg x \in A \lor x \in B)))$ (命题逻辑分配律)

$\iff \forall x((1 \lor \neg x \in B) \land (1 \land (\neg x \in A \lor x \in B)))$ (命题逻辑排中律)

$\iff \forall x(1 \land (1 \land (\neg x \in A \lor x \in B)))$ (命题逻辑零律)

$\iff \forall x(\neg x \in A \lor x \in B)$ (命题逻辑同一律)

$\iff \forall x(x \in A \to x \in B)$ (蕴涵等值式)

$\iff A \subseteq B$ (子集关系定义)

□

(2) 答：$A \cup B = A$ 当且仅当 $B \subseteq A$。

证明:

$A \cup B = A$

$\iff \forall x((x \in A \lor x \in B) \leftrightarrow x \in A)$ (外延原则、集合并定义)

$\iff \forall x(((x \in A \lor x \in B) \to x \in A) \land (x \in A \to (x \in A \lor x \in B)))$ (等价联结词定义)

$\iff \forall x((\neg(x \in A \lor x \in B) \lor x \in A) \land (\neg x \in A \lor x \in A \lor x \in B))$ (蕴涵等值式)

$\iff \forall x(((\neg x \in A \land \neg x \in B) \lor x \in A) \land (\neg x \in A \lor x \in A \lor x \in B))$ (命题逻辑德·摩根律)

$\iff \forall x(((\neg x \in A \lor x \in A) \land (\neg x \in B \lor x \in A)) \land$

$(\neg x \in A \lor x \in A \lor x \in B))$ (命题逻辑分配律)

$\iff \forall x((1 \land (\neg x \in B \lor x \in A)) \land (1 \lor x \in B))$ (命题逻辑排中律)

$\iff \forall x((1 \land (\neg x \in B \lor x \in A)) \land 1)$ (命题逻辑零律)

$\iff \forall x(\neg x \in B \lor x \in A)$ (命题逻辑同一律)

$\iff \forall x(x \in B \to x \in A)$ (蕴涵等值式)

$\iff B \subseteq A$ (子集关系定义)

□

(3) 答：$A \oplus B = A$ 当且仅当 $B = \varnothing$。

证明: 充分性。若 $B = \varnothing$，则：

$A \oplus B = A \oplus \varnothing$ ($B = \varnothing$)

$= A$ (教材例 1.7(4))

必要性。若 $A \oplus B = A$，则：

$B = \varnothing \oplus B$ (教材例 1.7(4))

$= (A \oplus A) \oplus B$ (教材例 1.7(5))

$$\begin{aligned}
&= A \oplus (A \oplus B) && \text{(教材例 1.7(2))}\\
&= A \oplus A && (A \oplus B = A)\\
&= \varnothing && \text{(教材例 1.7(5))}
\end{aligned}$$

□

(4) 答：$A \cap B = A \cup B$ 当且仅当 $A = B$。

证明： 充分性。若 $A = B$，则：

$$\begin{aligned}
A \cap B &= A \cap A && (A = B)\\
&= A && \text{(幂等律)}\\
&= A \cup A && \text{(幂等律)}\\
&= A \cup B && (A = B)
\end{aligned}$$

必要性。若 $A \cap B = A \cup B$，则：

$$\begin{aligned}
A &= A \cup (A \cap B) && \text{(吸收律)}\\
&= A \cup (A \cup B) && (A \cap B = A \cup B)\\
&= (A \cup A) \cup B && \text{(结合律)}\\
&= A \cup B && \text{(幂等律)}\\
&= A \cup (B \cup B) && \text{(幂等律)}\\
&= (A \cup B) \cup B && \text{(结合律)}\\
&= (A \cap B) \cup B && (A \cap B = A \cup B)\\
&= B && \text{(吸收律)}
\end{aligned}$$

□

1.22

(1) 即为引理 1.4 和引理 1.5。

(2) 答：不一定。令 $A = \{a\}, C = \{b\}, B = D = \{a, b\}$，则有 $A \subset B \wedge C \subset D$，但 $A \cup B \not\subset C \cup D$。又令 $A = C = \{a, b\}, B = \{a, b, c\}, D = \{a, b, d\}$，则有 $A \subset B \wedge C \subset D$，但 $A \cap B \not\subset C \cap D$

1.23

证明： 若不然，则存在 $x \in B \wedge x \notin C$ 或 $x \notin B \wedge x \in C$。不妨设 $x \in B \wedge x \notin C$，此时，若 $x \in A$ 则有 $x \notin A \oplus B$ 和 $x \in A \oplus C$，这与前提：$A \oplus B = A \oplus C$ 矛盾。若 $x \notin A$ 则有 $x \in A \oplus B$ 和 $x \notin A \oplus C$，这同样与前提：$A \oplus B = A \oplus C$ 矛盾。

对 $x \notin B \wedge x \in C$ 的情况亦有类似讨论。 □

1.24 先证：$(A - B) - C = (A - C) - B$。

证明：

$$\begin{aligned}
(A - B) - C &= (A \cap \sim B) \cap \sim C && \text{(补交转换律)}\\
&= A \cap (\sim B \cap \sim C) && \text{(结合律)}\\
&= A \cap (\sim C \cap \sim B) && \text{(交换律)}\\
&= ((A \cap \sim C) \cap \sim B) && \text{(结合律)}\\
&= (A - C) - B && \text{(补交转换律)}
\end{aligned}$$

□

再证：$(A-B)-C=A-(B\cup C)$。

证明:

$$\begin{aligned}
(A-B)-C &= (A\cap\sim B)\cap\sim C && \text{(补交转换律)}\\
&= A\cap(\sim B\cap\sim C) && \text{(结合律)}\\
&= A\cap\sim(B\cup C) && \text{(德·摩根律)}\\
&= A-(B\cup C) && \text{(补交转换律)}
\end{aligned}$$

□

最后证：$(A-B)-C=(A-C)-(B-C)$。

证明:

$$\begin{aligned}
(A-B)-C &= (A\cap\sim B)\cap\sim C && \text{(补交转换律)}\\
&= (A\cap\sim B\cap\sim C)\cup\varnothing && \text{(同一律)}\\
&= (A\cap\sim B\cap\sim C)\cup(A\cap\varnothing) && \text{(零律)}\\
&= (A\cap\sim B\cap\sim C)\cup(A\cap\sim C\cap C) && \text{(矛盾律)}\\
&= (A\cap\sim C\cap\sim B)\cup(A\cap\sim C\cap C) && \text{(交换律)}\\
&= (A\cap\sim C)\cap(\sim B\cup C) && \text{(分配律)}\\
&= (A\cap\sim C)\cap\sim(B\cap\sim C) && \text{(德·摩根律)}\\
&= (A-C)-(B-C) && \text{(补交转换律)}
\end{aligned}$$

□

1.25

(1) A；

(2) $A-B$；

(3) $B-A$。

1.26

(1)

证明: 先证必要性。

若已知 $A\subseteq C\wedge B\subseteq C$，则 $\forall x$，

$$\begin{aligned}
x\in A\cup B &\iff x\in A\vee x\in B && \text{(子集关系定义)}\\
&\iff (x\in A\vee x\in B)\wedge\\
&\qquad (x\in A\to x\in C)\wedge(x\in B\to x\in C) && \text{(前提、子集关系定义)}\\
&\Longrightarrow (x\in C)\vee(x\in C) && \text{(构造性二难)}\\
&\Longrightarrow x\in C && \text{(命题逻辑幂等律)}
\end{aligned}$$

再证充分性。

若已知 $A\cup B\subseteq C$，则 $\forall x$，

$$\begin{aligned}
x\in A &\Longrightarrow x\in A\vee x\in B && \text{(命题逻辑附加律)}\\
&\Longrightarrow x\in C && \text{(前提、子集关系定义)}
\end{aligned}$$

于是有 $A\subseteq C$。同理可证：$B\subseteq C$。 □

(2)

证明: 先证必要性。

若已知 $C \subseteq A \wedge C \subseteq B$，则 $\forall x$，

$$\begin{aligned}
x \in C &\iff (x \in C) \wedge (x \in C) && \text{(命题逻辑幂等律)}\\
&\implies (x \in A) \wedge (x \in B) && \text{(前提、子集关系定义)}\\
&\iff x \in A \cap B && \text{(集合交定义)}
\end{aligned}$$

再证充分性。

若已知 $C \subseteq A \cap B$，则 $\forall x$，

$$\begin{aligned}
x \in C &\implies x \in A \cap B && \text{(前提、子集关系定义)}\\
&\iff x \in A \wedge x \in B && \text{(集合交定义)}
\end{aligned}$$

□

1.27

证明: 对于任意集合 A，有：

$$\begin{aligned}
&\varnothing \subseteq A && \text{(教材定理 1.1)}\\
\iff &\varnothing \in \mathcal{P}(A) && \text{(幂集定义)}\\
\iff &\{\varnothing\} \subseteq \mathcal{P}(A) \wedge \varnothing \subseteq \mathcal{P}(A) && \text{(子集关系定义、教材定理 1.1)}\\
\iff &\{\varnothing\} \in \mathcal{P}\mathcal{P}(A) \wedge \varnothing \in \mathcal{P}\mathcal{P}(A) && \text{(幂集定义)}\\
\iff &\{\varnothing, \{\varnothing\}\} \subseteq \mathcal{P}\mathcal{P}(A) && \text{(子集关系定义)}\\
\iff &\{\varnothing, \{\varnothing\}\} \in \mathcal{P}\mathcal{P}\mathcal{P}(A) && \text{(幂集定义)}
\end{aligned}$$

于是得到，$\{\varnothing, \{\varnothing\}\} \in \mathcal{P}\mathcal{P}\mathcal{P}(A)$。

由于上述证明中的 A 为任意集合，只需将 A 替换成 $\mathcal{P}(A)$，则证明的倒数第二行即为待证的第二部分：$\{\varnothing, \{\varnothing\}\} \subseteq \mathcal{P}\mathcal{P}\mathcal{P}(A)$。 □

1.28 下面依次证 $(1) \Leftrightarrow (2), (1) \Leftrightarrow (3), (1) \Leftrightarrow (4), (1) \Leftrightarrow (5)$。

先证：$(1) \Leftrightarrow (2)$，即 $A \subseteq B \Leftrightarrow {\sim}B \subseteq {\sim}A$。

证明:

$$\begin{aligned}
A \subseteq B &\iff \forall x(x \in A \to x \in B) && \text{(子集关系定义)}\\
&\iff \forall x(\neg(x \in B) \to \neg(x \in A)) && \text{(命题逻辑假言易位)}\\
&\iff \forall x(x \notin B \to x \notin A) && (\notin \text{ 定义)}\\
&\iff \forall x(x \in {\sim}B \to x \in {\sim}A) && \text{(绝对补定义)}\\
&\iff {\sim}B \subseteq {\sim}A && \text{(子集关系定义)}
\end{aligned}$$

□

再证：$(1) \Leftrightarrow (3)$，即 $A \subseteq B \Leftrightarrow {\sim}A \cup B = E$。

证明:

$$\begin{aligned}
A \subseteq B &\iff \forall x(x \in A \to x \in B) && \text{(子集关系定义)}\\
&\iff \forall x(\neg(x \in A) \vee (x \in B)) && \text{(蕴涵等值式)}\\
&\iff \forall x(x \notin A \vee x \in B) && (\notin \text{ 定义)}\\
&\iff \forall x(x \in {\sim}A \vee x \in B) && \text{(绝对补定义)}\\
&\iff \forall x(x \in {\sim}A \cup B) && \text{(集合并定义)}\\
&\iff {\sim}A \cup B = E && \text{(全集定义)}
\end{aligned}$$

□

下面证[1] $(1) \Leftrightarrow (4)$，即 $A \subseteq B \Leftrightarrow A - B \subseteq {\sim}A$。

证明:

$$
\begin{aligned}
A - B \subseteq {\sim}A &\iff \forall x(x \in A - B \to x \in {\sim}A) && \text{(子集关系定义)}\\
&\iff \forall x((x \in A \wedge x \notin B) \to x \in {\sim}A) && \text{(相对补定义)}\\
&\iff \forall x(\neg(x \in A \wedge x \notin B) \vee x \in {\sim}A) && \text{(蕴涵等值式)}\\
&\iff \forall x((\neg x \in A \vee \neg x \notin B) \vee x \in {\sim}A) && \text{(命题逻辑德·摩根律)}\\
&\iff \forall x((\neg x \in A \vee \neg x \notin B) \vee x \notin A) && \text{(绝对补定义)}\\
&\iff \forall x((\neg x \in A \vee \neg\neg x \in B) \vee \neg x \in A) && \text{(}\notin\text{ 定义)}\\
&\iff \forall x((\neg x \in A \vee x \in B) \vee \neg x \in A) && \text{(命题逻辑双重否定律)}\\
&\iff \forall x(\neg x \in A \vee \neg x \in A \vee x \in B) && \text{(命题逻辑结合律、交换律)}\\
&\iff \forall x(\neg x \in A \vee x \in B) && \text{(命题逻辑幂等律)}\\
&\iff \forall x(x \in A \to x \in B) && \text{(蕴涵等值式)}\\
&\iff A \subseteq B && \text{(子集关系定义)}
\end{aligned}
$$

□

最后证：$(1) \Leftrightarrow (5)$，即 $A \subseteq B \Leftrightarrow A - B \subseteq B$。

证明:

$$
\begin{aligned}
A - B \subseteq B &\iff \forall x(x \in A - B \to x \in B) && \text{(子集关系定义)}\\
&\iff \forall x((x \in A \wedge x \notin B) \to x \in B) && \text{(相对补定义)}\\
&\iff \forall x(\neg(x \in A \wedge x \notin B) \vee x \in B) && \text{(蕴涵等值式)}\\
&\iff \forall x((\neg x \in A \vee \neg x \notin B) \vee x \in B) && \text{(命题逻辑德·摩根律)}\\
&\iff \forall x((\neg x \in A \vee \neg\neg x \in B) \vee x \in B) && \text{(}\notin\text{ 定义)}\\
&\iff \forall x((\neg x \in A \vee x \in B) \vee x \in B) && \text{(命题逻辑双重否定律)}\\
&\iff \forall x(\neg x \in A \vee x \in B) && \text{(命题逻辑结合律、幂等律)}\\
&\iff \forall x(x \in A \to x \in B) && \text{(蕴涵等值式)}\\
&\iff A \subseteq B && \text{(子集关系定义)}
\end{aligned}
$$

□

1.29

证明: $\forall x$，

$$
\begin{aligned}
& x \in (\cap\mathscr{A}) \cap (\cap\mathscr{B}) && \\
\iff & x \in (\cap\mathscr{A}) \wedge x \in (\cap\mathscr{B}) && \text{(集合交定义)}\\
\iff & \forall z(z \in \mathscr{A} \to x \in z) \wedge \forall z(z \in \mathscr{B} \to x \in z) && \text{(广义交定义)}\\
\iff & \forall z((z \in \mathscr{A} \to x \in z) \wedge (z \in \mathscr{B} \to x \in z)) && \text{(量词分配等值式)}\\
\implies & \forall z(z \in \mathscr{A} \to x \in z) && \text{(命题逻辑化简律)}\\
\implies & \forall z((z \in \mathscr{A} \to x \in z) \vee (z \in \mathscr{B} \to x \in z)) && \text{(命题逻辑附加律)}\\
\iff & \forall z((\neg(z \in \mathscr{A}) \vee (x \in z)) \vee (\neg(z \in \mathscr{B}) \vee (x \in z))) && \text{(蕴涵等值式)}
\end{aligned}
$$

---

[1] 感谢北大未名BBS的chouxiaoya网友提供 $(1) \Leftrightarrow (4)$ 和 $(1) \Leftrightarrow (5)$ 的形式化证明。

$\iff \forall z((\neg(z \in \mathscr{A}) \vee \neg(z \in \mathscr{B})) \vee (x \in z) \vee (x \in z))$ (命题逻辑结合律、交换律)

$\iff \forall z((\neg(z \in \mathscr{A}) \vee \neg(z \in \mathscr{B})) \vee (x \in z))$ (命题逻辑幂等律)

$\iff \forall z(\neg(z \in \mathscr{A} \wedge z \in \mathscr{B}) \vee x \in z)$ (命题逻辑德·摩根律)

$\iff \forall z(z \in \mathscr{A} \wedge z \in \mathscr{B} \to x \in z)$ (蕴涵等值式)

$\iff \forall z(z \in \mathscr{A} \cap \mathscr{B} \to x \in z)$ (集合交定义)

$\iff x \in \cap(\mathscr{A} \cap \mathscr{B})$ (广义交定义)

□

1.30

(1)

证明: $\forall x$，

$x \in \mathcal{P}(A) \cap \mathcal{P}(B)$

$\iff x \in \mathcal{P}(A) \wedge x \in \mathcal{P}(B)$ (集合交定义)

$\iff x \subseteq A \wedge x \subseteq B$ (幂集定义)

$\iff x \subseteq A \cap B$ (习题 1.26(2) 结论)

$\iff x \in \mathcal{P}(A \cap B)$ (幂集定义)

□

(2)

证明: $\forall x$，

$x \in \mathcal{P}(A) \cup \mathcal{P}(B)$

$\iff x \in \mathcal{P}(A) \vee x \in \mathcal{P}(B)$ (集合并定义)

$\iff x \subseteq A \vee x \subseteq B$ (幂集定义)

$\iff \forall y(y \in x \to y \in A) \vee \forall y(y \in x \to y \in B)$ (子集关系定义)

$\implies \forall y((y \in x \to y \in A) \vee (y \in x \to y \in B))$ (一阶谓词推理定律)

$\iff \forall y((\neg y \in x \vee y \in A) \vee (\neg y \in x \vee y \in B))$ (蕴涵等值式)

$\iff \forall y(\neg y \in x \vee (y \in A \vee y \in B))$ (命题逻辑交换律、结合律、幂等律)

$\iff \forall y(y \in x \to (y \in A \cup B))$ (蕴涵等值式、集合并定义)

$\iff x \subseteq A \cup B$ (子集关系定义)

$\iff x \in \mathcal{P}(A \cup B)$ (幂集定义)

□

1.31 193。

1.32 10。

1.33 收敛。$\varlimsup\limits_{k\to\infty} A_k = \varliminf\limits_{k\to\infty} A_k = [0,1]$。

1.34 $\varlimsup\limits_{k\to\infty} B_k = [0,1]$, $\varliminf\limits_{k\to\infty} B_k = \varnothing$。

1.35 $\varlimsup\limits_{k\to\infty} A_k = [0,\infty]$, $\varliminf\limits_{k\to\infty} A_k = \{0\}$。

1.36 先证一个引理。

引理 1.6 对任意谓词公式 F 和 G，有:

$$\begin{aligned}
&\exists n_0(n_0 \in \mathbb{N}_+ \land \forall k(k \in \mathbb{N}_+ \land k \geq n_0 \to (F(k) \land G(k))))\\
\iff &\exists n_1(n_1 \in \mathbb{N}_+ \land \forall k(k \in \mathbb{N}_+ \land k \geq n_1 \to F(k)))\\
&\ \land \exists n_2(n_2 \in \mathbb{N}_+ \land \forall k(k \in \mathbb{N}_+ \land k \geq n_2 \to G(k)))
\end{aligned}$$

证明: 必要性：由一阶谓词推理规则 $\exists x(A(x) \land B(x)) \implies \exists x A(x) \land \exists x B(x)$ 和变元换名规则立即可得。

充分性：令 $n_0 = \max(n_1, n_2)$，则有 $\forall k(k \in \mathbb{N}_+ \land k \geq n_0 \to (k \geq n_1 \land k \geq n_2))$。再由“假言三段论”推理规则，即可得证。 □

再证原题：

(1) 先证第一个包含关系：

$$\varliminf_{k\to\infty} A_k \cup \varliminf_{k\to\infty} B_k \subseteq \varliminf_{k\to\infty} (A_k \cup B_k)$$

证明: $\forall x$，

$$\begin{aligned}
&x \in \varliminf_{k\to\infty} A_k \cup \varliminf_{k\to\infty} B_k\\
\iff &\exists n_0(n_0 \in \mathbb{N}_+ \land \forall k(k \in \mathbb{N}_+ \land k \geq n_0 \to x \in A_k)) \lor\\
&\exists n_0(n_0 \in \mathbb{N}_+ \land \forall k(k \in \mathbb{N}_+ \land k \geq n_0 \to x \in B_k)) && \text{(集合并定义、下极限定义)}\\
\iff &\exists n_0((n_0 \in \mathbb{N}_+ \land \forall k(k \in \mathbb{N}_+ \land k \geq n_0 \to x \in A_k)) \lor\\
&\quad (n_0 \in \mathbb{N}_+ \land \forall k(k \in \mathbb{N}_+ \land k \geq n_0 \to x \in B_k))) && \text{(量词分配等值式)}\\
\iff &\exists n_0(n_0 \in \mathbb{N}_+ \land (\forall k(k \in \mathbb{N}_+ \land k \geq n_0 \to x \in A_k)) \lor\\
&\qquad\qquad (\forall k(k \in \mathbb{N}_+ \land k \geq n_0 \to x \in B_k))) && \text{(命题逻辑分配律)}\\
\implies &\exists n_0(n_0 \in \mathbb{N}_+ \land \forall k((k \in \mathbb{N}_+ \land k \geq n_0 \to x \in A_k) \lor\\
&\qquad\qquad (k \in \mathbb{N}_+ \land k \geq n_0 \to x \in B_k))) && \text{(一阶谓词推理定律)}\\
\iff &\exists n_0(n_0 \in \mathbb{N}_+ \land \forall k(\neg(k \in \mathbb{N}_+ \land k \geq n_0) \lor x \in A_k) \lor\\
&\qquad\qquad (\neg(k \in \mathbb{N}_+ \land k \geq n_0) \lor x \in B_k)) && \text{(蕴涵等值式)}\\
\iff &\exists n_0(n_0 \in \mathbb{N}_+ \land \forall k(\neg(k \in \mathbb{N}_+ \land k \geq n_0) \lor (x \in A_k \lor x \in B_k))) && \text{(结合、交换、幂等)}\\
\iff &\exists n_0(n_0 \in \mathbb{N}_+ \land \forall k(k \in \mathbb{N}_+ \land k \geq n_0 \to (x \in A_k \lor x \in B_k))) && \text{(蕴涵等值式)}\\
\iff &x \in \varliminf_{k\to\infty} (A_k \cup B_k) && \text{(集合并定义、下极限定义)}
\end{aligned}$$

□

再证第二个包含关系：

$$\varliminf_{k\to\infty} (A_k \cup B_k) \subseteq \varliminf_{k\to\infty} A_k \cup \varlimsup_{k\to\infty} B_k$$

和

$$\varliminf_{k\to\infty} (A_k \cup B_k) \subseteq \varlimsup_{k\to\infty} A_k \cup \varliminf_{k\to\infty} B_k$$

证明: $\forall x \in \varliminf\limits_{k\to\infty} (A_k \cup B_k)$，只有下面两种可能:

(1) x 属于几乎所有的 A_k，即存在 $n_0(x)$，使得当 $k \geq n_0(x)$ 后，$x \in A_k$，于是 $x \in \varliminf\limits_{k\to\infty} A_k$

(2) 当 (1) 不成立时，必有无限个 $\{A_k\}$ 中的集合不含 x，但由于 $x \in \underline{\lim}_{k\to\infty}(A_k \cup B_k)$，即，只有有限个k，使得 $x \notin (A_k \cup B_k)$，于是，必有无限个 k，使得 $x \in B_k$，即有 $x \in \overline{\lim}_{k\to\infty} B_k$。

综合得：

$$\underline{\lim}_{k\to\infty}(A_k \cup B_k) \subseteq \underline{\lim}_{k\to\infty} A_k \cup \overline{\lim}_{k\to\infty} B_k$$

同理可证：

$$\underline{\lim}_{k\to\infty}(A_k \cup B_k) \subseteq \overline{\lim}_{k\to\infty} A_k \cup \underline{\lim}_{k\to\infty} B_k$$

□

由引理 1.4 和教材定理 1.4(1) 立即有：

$$\underline{\lim}_{k\to\infty} A_k \cup \overline{\lim}_{k\to\infty} B_k \subseteq \overline{\lim}_{k\to\infty} A_k \cup \overline{\lim}_{k\to\infty} B_k$$

和

$$\overline{\lim}_{k\to\infty} A_k \cup \underline{\lim}_{k\to\infty} B_k \subseteq \overline{\lim}_{k\to\infty} A_k \cup \overline{\lim}_{k\to\infty} B_k$$

最后，只需证：

$$\overline{\lim}_{k\to\infty}(A_k \cup B_k) = \overline{\lim}_{k\to\infty} A_k \cup \overline{\lim}_{k\to\infty} B_k$$

即可完成本小题。

证明：先证：

$$\overline{\lim}_{k\to\infty}(A_k \cup B_k) \subseteq \overline{\lim}_{k\to\infty} A_k \cup \overline{\lim}_{k\to\infty} B_k$$

用反证法。由上极限定义可知，对任意 $x \in \overline{\lim}_{k\to\infty}(A_k \cup B_k)$，必存在无限多个 k，使得 $x \in A_k \vee x \in B_k$。若 $x \notin \overline{\lim}_{k\to\infty} A_k \cup \overline{\lim}_{k\to\infty} B_k$，即 $x \notin \overline{\lim}_{k\to\infty} A_k \wedge x \notin \overline{\lim}_{k\to\infty} B_k$，则 $\{A_k\}$ 和 $\{B_k\}$ 中都至多只有有限个集合，使得 $x \in A_k \vee x \in B_k$。这与 $x \in \overline{\lim}_{k\to\infty}(A_k \cup B_k)$ 矛盾。故有：

$$\overline{\lim}_{k\to\infty}(A_k \cup B_k) \subseteq \overline{\lim}_{k\to\infty} A_k \cup \overline{\lim}_{k\to\infty} B_k$$

再证：

$$\overline{\lim}_{k\to\infty} A_k \cup \overline{\lim}_{k\to\infty} B_k \subseteq \overline{\lim}_{k\to\infty}(A_k \cup B_k)$$

$\forall x$，

$$\begin{aligned}
& x \in \overline{\lim}_{k\to\infty} A_k \cup \overline{\lim}_{k\to\infty} B_k \\
\iff & \forall n(n \in \mathbb{N}_+ \to (\exists k(k \in \mathbb{N}_+ \wedge k \geq n \wedge x \in A_k))) \vee \\
& \forall n(n \in \mathbb{N}_+ \to (\exists k(k \in \mathbb{N}_+ \wedge k \geq n \wedge x \in B_k))) && \text{(集合并定义、上极限定义)} \\
\implies & \forall n(n \in \mathbb{N}_+ \to (\exists k(k \in \mathbb{N}_+ \wedge k \geq n \wedge x \in A_k) \vee \\
& \qquad \exists k(k \in \mathbb{N}_+ \wedge k \geq n \wedge x \in B_k))) && \text{(一阶谓词推理定律)} \\
\iff & \forall n(n \in \mathbb{N}_+ \to \exists k((k \in \mathbb{N}_+ \wedge k \geq n \wedge x \in A_k) \vee \\
& \qquad (k \in \mathbb{N}_+ \wedge k \geq n \wedge x \in B_k))) && \text{(量词分配等值式)} \\
\iff & \forall n(n \in \mathbb{N}_+ \to \exists k(k \in \mathbb{N}_+ \wedge k \geq n \wedge (x \in A_k \vee x \in B_k))) && \text{(命题逻辑分配律)} \\
\iff & x \in \overline{\lim}_{k\to\infty}(A_k \cup B_k) && \text{(集合并定义、上极限定义)}
\end{aligned}$$

□

(2) 先证：

$$\varliminf_{k\to\infty} A_k \cap \varliminf_{k\to\infty} B_k = \varliminf_{k\to\infty}(A_k \cap B_k)$$

证明： $\forall x$，

$$\begin{aligned}
& x \in \varliminf_{k\to\infty} A_k \cap \varliminf_{k\to\infty} B_k \\
\Longleftrightarrow\ & \exists n_1(n_1 \in \mathbb{N}_+ \wedge \forall k(k \in \mathbb{N}_+ \wedge k \geq n_1 \to x \in A_k))\wedge \\
& \exists n_2(n_2 \in \mathbb{N}_+ \wedge \forall k(k \in \mathbb{N}_+ \wedge k \geq n_2 \to x \in B_k)) && \text{(集合交定义、下极限定义)} \\
\Longleftrightarrow\ & \exists n_0(n_0 \in \mathbb{N}_+ \wedge \forall k(k \in \mathbb{N}_+ \wedge k \geq n_0 \to x \in A_k \wedge B_k)) && \text{(引理 1.6)} \\
\Longleftrightarrow\ & x \in \varliminf_{k\to\infty}(A_k \cap B_k) && \text{(集合交定义、下极限定义)}
\end{aligned}$$

□

由引理 1.5 和教材定理 1.4(1) 立即有：

$$\varliminf_{k\to\infty} A_k \cap \varliminf_{k\to\infty} B_k \subseteq \varliminf_{k\to\infty} A_k \cap \varlimsup_{k\to\infty} B_k$$

和

$$\varliminf_{k\to\infty} A_k \cap \varliminf_{k\to\infty} B_k \subseteq \varlimsup_{k\to\infty} A_k \cap \varliminf_{k\to\infty} B_k$$

下面证：

$$\varliminf_{k\to\infty} A_k \cap \varlimsup_{k\to\infty} B_k \subseteq \varlimsup_{k\to\infty}(A_k \cap B_k)$$

和

$$\varlimsup_{k\to\infty} A_k \cap \varliminf_{k\to\infty} B_k \subseteq \varlimsup_{k\to\infty}(A_k \cap B_k)$$

证明： $\forall x \in \varliminf_{k\to\infty} A_k \cap \varliminf_{k\to\infty} B_k$，由 $x \in \varliminf_{k\to\infty} A_k$ 知，存在 $n_0 \in \mathbb{N}_+$，使对所有满足 $k \geq n_0$ 的自然数 k 都有 $x \in A_k$。对任意给定的 $n \in \mathbb{N}_+$，我们令 $n' = \max(n, n_0)$，由于 $x \in \varliminf_{k\to\infty} B_k$，故存在 $k \in \mathbb{N}_+ \wedge k \geq n'$，使 $n \in B_k$。由 n' 的选择知，$k \geq n' \geq n_0$，因此必有 $x \in A_k$，从而有 $x \in A_k \cap B_k$。这就证明了：

$$\varliminf_{k\to\infty} A_k \cap \varlimsup_{k\to\infty} B_k \subseteq \varlimsup_{k\to\infty}(A_k \cap B_k)$$

同理可证：

$$\varliminf_{k\to\infty} A_k \cap \varlimsup_{k\to\infty} B_k \subseteq \varlimsup_{k\to\infty}(A_k \cap B_k)$$

□

最后证：

$$\varlimsup_{k\to\infty}(A_k \cap B_k) \subseteq \varlimsup_{k\to\infty} A_k \cap \varlimsup_{k\to\infty} B_k$$

证明： $\forall x$，

$$\begin{aligned}
& x \in \varlimsup_{k\to\infty}(A_k \cap B_k) \\
\Longleftrightarrow\ & \forall n(n \in \mathbb{N}_+ \to \exists k(k \in \mathbb{N}_+ \wedge k \geq n \wedge x \in A_k \wedge x \in B_k)) && \text{(上极限定义、集合交定义)} \\
\Longleftrightarrow\ & \forall n(n \in \mathbb{N}_+ \to \exists k(k \in \mathbb{N}_+ \wedge k \geq n \wedge x \in A_k \wedge
\end{aligned}$$

$$\begin{aligned}
&\qquad\qquad k \in \mathbb{N}_+ \wedge k \geq n \wedge x \in B_k)) && \text{(命题逻辑幂等律、交换律)}\\
&\Longrightarrow \forall n(n \in \mathbb{N}_+ \to (\exists k(k \in \mathbb{N}_+ \wedge k \geq n \wedge x \in A_k)\wedge\\
&\qquad\qquad \exists k(k \in \mathbb{N}_+ \wedge k \geq n \wedge x \in B_k))) && \text{(一阶谓词推理定律)}\\
&\Longleftrightarrow \forall n(\neg n \in \mathbb{N}_+ \vee (\exists k(k \in \mathbb{N}_+ \wedge k \geq n \wedge x \in A_k)\wedge\\
&\qquad\qquad \exists k(k \in \mathbb{N}_+ \wedge k \geq n \wedge x \in B_k))) && \text{(蕴涵等值式)}\\
&\Longleftrightarrow \forall n((\neg n \in \mathbb{N}_+ \vee \exists k(k \in \mathbb{N}_+ \wedge k \geq n \wedge x \in A_k))\wedge\\
&\qquad\qquad (\neg n \in \mathbb{N}_+ \vee \exists k(k \in \mathbb{N}_+ \wedge k \geq n \wedge x \in B_k))) && \text{(命题逻辑分配律)}\\
&\Longleftrightarrow \forall n(\neg n \in \mathbb{N}_+ \vee \exists k(k \in \mathbb{N}_+ \wedge k \geq n \wedge x \in A_k))\wedge\\
&\qquad \forall n(\neg n \in \mathbb{N}_+ \vee \exists k(k \in \mathbb{N}_+ \wedge k \geq n \wedge x \in B_k)) && \text{(量词分配等值式)}\\
&\Longleftrightarrow \forall n(n \in \mathbb{N}_+ \to \exists k(k \in \mathbb{N}_+ \wedge k \geq n \wedge x \in A_k))\wedge\\
&\qquad \forall n(n \in \mathbb{N}_+ \to \exists k(k \in \mathbb{N}_+ \wedge k \geq n \wedge x \in B_k)) && \text{(蕴涵等值式)}\\
&\Longleftrightarrow x \in \varlimsup_{k\to\infty} A_k \cap \varlimsup_{k\to\infty} B_k && \text{(上极限定义、集合交定义)}
\end{aligned}$$

□

(3)

证明： 令 $E = \bigcup\limits_{k\in\mathbb{N}_+}(A_k \cup B_k)$ 为全集，则有：

$$\begin{aligned}
\varlimsup_{k\to\infty}(A_k - B_k) &= \varlimsup_{k\to\infty}(A_k \cap {\sim}B_k) && \text{(补交转换律)}\\
&\subseteq \varlimsup_{k\to\infty} A_k \cap \varlimsup_{k\to\infty}({\sim}B_k) && \text{(第 (1) 小题结论)}\\
&= \varlimsup_{k\to\infty} A_k \cap \varlimsup_{k\to\infty}(E - B_k) && \text{(绝对补定义)}\\
&= \varlimsup_{k\to\infty} A_k \cap (E - \varliminf_{k\to\infty} B_k) && \text{(教材定理 1.5(1))}\\
&= \varlimsup_{k\to\infty} A_k \cap ({\sim}\varliminf_{k\to\infty} B_k) && \text{(绝对补定义)}\\
&= \varlimsup_{k\to\infty} A_k - \varliminf_{k\to\infty} B_k && \text{(补交转换律)}
\end{aligned}$$

□

(4)

证明： 令 $E = \bigcup\limits_{k\in\mathbb{N}_+}(A_k \cup B_k)$ 为全集，则有：

$$\begin{aligned}
\varliminf_{k\to\infty}(A_k - B_k) &= \varliminf_{k\to\infty}(A_k \cap {\sim}B_k) && \text{(补交转换律)}\\
&= \varliminf_{k\to\infty} A_k \cap \varliminf_{k\to\infty}({\sim}B_k) && \text{(第 (2) 小题结论)}\\
&= \varliminf_{k\to\infty} A_k \cap \varliminf_{k\to\infty}(E - B_k) && \text{(绝对补定义)}\\
&= \varliminf_{k\to\infty} A_k \cap (E - \varlimsup_{k\to\infty} B_k) && \text{(教材定理 1.5(2))}\\
&= \varliminf_{k\to\infty} A_k \cap ({\sim}\varlimsup_{k\to\infty} B_k) && \text{(绝对补定义)}\\
&= \varliminf_{k\to\infty} A_k - \varlimsup_{k\to\infty} B_k && \text{(补交转换律)}
\end{aligned}$$

□

第二章　二元关系

2.1　$\langle a,b,c\rangle = \langle\langle a,b\rangle,c\rangle = \{\{\{\{a\},\{a,b\}\}\},\{\{\{a\},\{a,b\}\},c\}\}$。

2.2

(1) $\langle a,b\rangle \cup \langle c,d\rangle = \{\{a\},\{a,b\}\} \cup \{\{c\},\{c,d\}\} = \{\{a\},\{a,b\},\{c\},\{c,d\}\}$；

(2) $\langle a,b\rangle \cap \langle c,d\rangle = \{\{a\},\{a,b\}\} \cap \{\{c\},\{c,d\}\} = \varnothing$；

(3) $\langle a,b\rangle \oplus \langle c,d\rangle = \{\{a\},\{a,b\}\} \oplus \{\{c\},\{c,d\}\} = \{\{a\},\{a,b\},\{c\},\{c,d\}\}$；

(4) $\cap\,\langle a,b\rangle = \cap\{\{a\},\{a,b\}\} = \{a\} \cap \{a,b\} = \{a\}$；

(5) $\cap\,\{\langle a,b\rangle\} = \langle a,b\rangle = \{\{a\},\{a,b\}\}$；

(6) $\cap\,\langle a,b,c\rangle = \cap\langle\langle a,b\rangle,c\rangle = \{\langle a,b\rangle\} = \{\{\{a\},\{a,b\}\}\}$；

(7) $\cap\cap\{\langle a,b\rangle\} = \cap\langle a,b\rangle = \{a\}$；

(8) $\cap\cap\cap\,\{\langle a,b\rangle\}^{-1} = \cap\cap\cap\{\langle b,a\rangle\} = \cap\cap\,\langle b,a\rangle = \cap\{b\} = b$。

2.3　不成立。

$\langle a,\langle b,c\rangle\rangle = \{\{a\},\{a,\{\{b\},\{b,c\}\}\}\} \neq \langle a,b,c\rangle = \{\{\{\{a\},\{a,b\}\}\},\{\{\{a\},\{a,b\}\},c\}\}$。

2.4　因为 $\langle\varnothing,\varnothing\rangle = \{\{\varnothing\},\{\varnothing,\varnothing\}\} = \{\{\varnothing\}\}$，$\langle a,\{a\}\rangle = \{\{a\},\{a,\{a\}\}\}$，故 (3), (5), (7) 成立，其余不成立。

2.5

(1) $A = \varnothing \vee B = \varnothing$；

(2) $A = B \vee A = \varnothing \vee B = \varnothing$；

(3) $A = \varnothing \vee B = \varnothing \vee C = \varnothing$。

2.6

(1)

证明:

$$\begin{aligned}
&\forall x, y\\
&\langle x,y\rangle \in (A\times C)\cup(B\times D)\\
\iff& (x\in A\wedge y\in C)\vee(x\in B\wedge y\in D) && \text{(卡氏积定义、集合并定义)}\\
\iff& (x\in A\vee x\in B)\wedge(x\in A\vee y\in D)\wedge\\
&(y\in C\vee x\in B)\wedge(y\in C\vee y\in D) && \text{(命题逻辑分配律)}\\
\Longrightarrow& (x\in A\vee x\in B)\wedge(y\in C\vee y\in D) && \text{(命题逻辑化简律)}\\
\iff& x\in(A\cup B)\times(C\cup D) && \text{(集合并定义、卡氏积定义)}
\end{aligned}$$

故有：$(A\times C)\cup(B\times D) \subseteq (A\cup B)\times(C\cup D)$。 □

(2)

证明:

$$\begin{aligned}
& \forall x, y \\
& \langle x, y\rangle \in (A-B)\times(C-D) \\
\Longleftrightarrow\ & x \in A \land x \notin B \land y \in C \land y \notin D && \text{(卡氏积定义、相对补定义)} \\
\Longleftrightarrow\ & x \in A \land y \in C \land x \notin B \land y \notin D && \text{(命题逻辑交换律)} \\
\Longrightarrow\ & x \in A \land y \in C \land x \notin B && \text{(命题逻辑化简律)} \\
\Longrightarrow\ & (x \in A \land y \in C \land x \notin B) \lor (x \in A \land y \in C \land y \notin D) && \text{(命题逻辑附加律)} \\
\Longleftrightarrow\ & (x \in A \land y \in C) \land (x \notin B \lor y \notin D) && \text{(命题逻辑分配律)} \\
\Longleftrightarrow\ & (x \in A \land y \in C) \land (\neg(x \in B) \lor \neg(y \in D)) && \text{($\notin$ 定义)} \\
\Longleftrightarrow\ & (x \in A \land y \in C) \land \neg(x \in B \land y \in D) && \text{(命题逻辑德·摩根律)} \\
\Longleftrightarrow\ & (\langle x, y\rangle \in A \times C) \land \neg(\langle x, y\rangle \in B \times D) && \text{(卡氏积定义)} \\
\Longleftrightarrow\ & (\langle x, y\rangle \in A \times C) \land (\langle x, y\rangle \notin B \times D) && \text{($\notin$ 定义)} \\
\Longleftrightarrow\ & \langle x, y\rangle \in (A \times C) - (B \times D) && \text{(相对补定义)}
\end{aligned}$$

故有：$(A-B)\times(C-D) \subseteq (A\times C)-(B\times D)$。 □

2.7

(1)

证明:

$$\begin{aligned}
& \forall x, y \\
& \langle x, y\rangle \in (A-B)\times C \\
\Longleftrightarrow\ & x \in (A-B) \land y \in C && \text{(卡氏积定义)} \\
\Longleftrightarrow\ & x \in A \land x \notin B \land y \in C && \text{(相对补定义)} \\
\Longleftrightarrow\ & x \in A \land \neg x \in B \land y \in C && \text{($\notin$ 定义)} \\
\Longleftrightarrow\ & (x \in A \land \neg x \in B \land y \in C) \lor 0 && \text{(命题逻辑同一律)} \\
\Longleftrightarrow\ & (x \in A \land \neg x \in B \land y \in C) \lor (x \in A \land 0) && \text{(命题逻辑零律)} \\
\Longleftrightarrow\ & (x \in A \land \neg x \in B \land y \in C) \lor (x \in A \land \neg y \in C \land y \in C) && \text{(命题逻辑矛盾律)} \\
\Longleftrightarrow\ & (x \in A \land y \in C) \land (\neg x \in B \lor \neg y \in C) && \text{(命题逻辑分配律)} \\
\Longleftrightarrow\ & (x \in A \land y \in C) \land \neg(x \in B \land y \in C) && \text{(命题逻辑德·摩根律)} \\
\Longleftrightarrow\ & (\langle x, y\rangle \in A \times C) \land \neg(\langle x, y\rangle \in B \times C) && \text{(卡氏积定义)} \\
\Longleftrightarrow\ & (\langle x, y\rangle \in A \times C) \land (\langle x, y\rangle \notin B \times C) && \text{($\notin$ 定义)} \\
\Longleftrightarrow\ & \langle x, y\rangle \in (A \times C) - (B \times C) && \text{(相对补定义)}
\end{aligned}$$

故有：$(A-B)\times C = (A\times C)-(B\times C)$。 □

(2)

证明:

$$\begin{aligned}
(A \oplus B) \times C =& ((A-B) \cup (B-A)) \times C && \text{(对称差性质)} \\
=& ((A-B)\times C) \cup ((B-A)\times C) && \text{(卡氏积性质)} \\
=& ((A\times C)-(B\times C)) \cup ((B\times C)-(A\times C)) && \text{(第 (1) 小题结论)}
\end{aligned}$$

$=(A \times C) \oplus (B \times C)$ (对称差性质)

注：证明中所述“性质”均出现在课本中相关的“定义”之后。形式化证明略。 □

2.8 当 $A=\varnothing \vee B=\varnothing$ 时，有 $A \times B \subseteq A$。当 $A=\varnothing$ 时，等号成立。

2.9 由于 A 到 B 的一个二元关系就是 $A \times B$ 的一个子集。故，从 A 到 B 上不同二元关系的数量就是 $A \times B$ 上不同的子集的数量。即为 $2^{|A \times B|}=2^{mn}$ 个。

从 A 到 B 的关系有：

$R_1=\varnothing$；

$R_2=\{\langle a,1\rangle\}$；

$R_3=\{\langle b,1\rangle\}$；

$R_4=\{\langle c,1\rangle\}$；

$R_5=\{\langle a,1\rangle,\langle b,1\rangle\}$；

$R_6=\{\langle a,1\rangle,\langle c,1\rangle\}$；

$R_7=\{\langle b,1\rangle,\langle c,1\rangle\}$；

$R_8=\{\langle a,1\rangle,\langle b,1\rangle,\langle c,1\rangle\}$；

从 B 到 A 的关系有：

$R_1^{-1}=\varnothing$；

$R_2^{-1}=\{\langle 1,a\rangle\}$；

$R_3^{-1}=\{\langle 1,b\rangle\}$；

$R_4^{-1}=\{\langle 1,c\rangle\}$；

$R_5^{-1}=\{\langle 1,a\rangle,\langle 1,b\rangle\}$；

$R_6^{-1}=\{\langle 1,a\rangle,\langle 1,c\rangle\}$；

$R_7^{-1}=\{\langle 1,b\rangle,\langle 1,c\rangle\}$；

$R_8^{-1}=\{\langle 1,a\rangle,\langle 1,b\rangle,\langle 1,c\rangle\}$。

2.10[1]

证明:

$$\forall a \in \cup\cup R$$

$$\iff \exists S(S \in \cup R \wedge a \in S) \qquad \text{(广义并定义)}$$

$$\iff \exists S'\exists S(S' \in R \wedge S \in S' \wedge a \in S) \qquad \text{(广义并定义)}$$

$$\iff \exists\{\{x\},\{x,y\}\}\exists S(\{\{x\},\{x,y\}\} \in R \wedge S \in \{\{x\},\{x,y\}\} \wedge a \in S) \qquad \text{(R 是二元关系)}$$

$$\iff \exists\{\{x\},\{x,y\}\}\exists S(\{\{x\},\{x,y\}\} \in R \wedge (S=\{x\} \vee S=\{x,y\}) \wedge a \in S) \qquad \text{($\in$ 性质)}$$

$$\iff \exists\{\{x\},\{x,y\}\}(\{\{x\},\{x,y\}\} \in R \wedge (S=\{x\} \wedge a \in S) \vee (S=\{x,y\} \wedge a \in S)) \qquad \text{(命题逻辑德·摩根律)}$$

$$\iff \exists\{\{x\},\{x,y\}\}(\{\{x\},\{x,y\}\} \in R \wedge (a=x \vee (a=x \vee a=y))) \qquad \text{($\in$ 性质)}$$

$$\iff \exists\{\{x\},\{x,y\}\}(\{\{x\},\{x,y\}\} \in R \wedge (a=x \vee a=y)) \qquad \text{(命题逻辑结合律、幂等律)}$$

$$\iff a \in \operatorname{dom} R \vee a \in \operatorname{ran} R \qquad \text{(定义域、值域定义)}$$

$$\iff a \in \operatorname{fld} R \qquad \text{(域定义)}$$

故有 $\operatorname{fld} R=\cup\cup R$。 □

---

[1] 感谢南京大学计算机系胡海星(starfish@lilybbs.us)大侠给出此题的形式化证明。

2.11

(1) $R_1 \cup R_2 = \{\langle a, b\rangle, \langle a, c\rangle, \langle b, d\rangle, \langle c, c\rangle, \langle c, d\rangle, \langle d, b\rangle, \langle d, d\rangle\}$；

$R_1 \cap R_2 = \{\langle b, d\rangle\}$；

$R_1 \oplus R_2 = (R_1 \cup R_2) - (R_1 \cap R_2)\{\langle a, b\rangle, \langle a, c\rangle, \langle c, c\rangle, \langle c, d\rangle, \langle d, b\rangle, \langle d, d\rangle\}$；

(2) $\operatorname{dom} R_1 = \{a, b, c\}$；

$\operatorname{dom} R_2 = \{a, b, d\}$；

$\operatorname{dom}(R_1 \cup R_2) = \operatorname{dom} R_1 \cup \operatorname{dom} R_2 = \{a, b, c, d\}$；

(3) $\operatorname{ran} R_1 = \{b, c, d\}$；

$\operatorname{ran} R_2 = \{b, c, d\}$；

$\operatorname{ran} R_1 \cap \operatorname{ran} R_2 = \{b, c, d\}$；

(4) $R_1 \upharpoonright A = \{\langle a, b\rangle, \langle c, c\rangle, \langle c, d\rangle\}$；

$R_1 \upharpoonright \{c\} = \{\langle c, c\rangle, \langle c, d\rangle\}$；

$(R_1 \cup R_2) \upharpoonright A = \{\langle a, b\rangle, \langle a, c\rangle, \langle c, c\rangle, \langle c, d\rangle\}$；

$R_2 \upharpoonright A = \{\langle a, c\rangle\}$；

(5) $R_1[A] = \{b, c, d\}$；

$R_2[A] = \{c\}$；

$(R_1 \cap R_2)[A] = \varnothing$；

(6) $R_1 \circ R_2 = \{\langle a, c\rangle, \langle a, d\rangle, \langle d, d\rangle\}$；

$R_2 \circ R_1 = \{\langle a, d\rangle, \langle b, b\rangle, \langle b, d\rangle, \langle c, b\rangle, \langle c, d\rangle\}$；

$R_1 \circ R_1 = \{\langle a, d\rangle, \langle c, c\rangle, \langle c, d\rangle\}$。

2.12

(1) $R^{-1} = \{\langle\{\varnothing, \{\varnothing\}\}, \varnothing\rangle, \langle\varnothing, \{\varnothing\}\rangle, \langle\varnothing, \varnothing\rangle\}$；

(2) $R \circ R = \{\langle\varnothing, \varnothing\rangle, \langle\varnothing, \{\varnothing, \{\varnothing\}\}\rangle, \langle\{\varnothing\}, \varnothing\rangle, \langle\{\varnothing\}, \{\varnothing, \{\varnothing\}\}\rangle\}$；

(3) $R \upharpoonright \varnothing = \varnothing$；

$R \upharpoonright \{\varnothing\} = \{\langle\varnothing, \{\varnothing, \{\varnothing\}\}\rangle, \langle\varnothing, \varnothing\rangle\}$；

$R \upharpoonright \{\{\varnothing\}\} = \{\langle\{\varnothing\}, \varnothing\rangle\}$；

$R \upharpoonright \{\varnothing, \{\varnothing\}\} = R = \{\langle\varnothing, \{\varnothing, \{\varnothing\}\}\rangle, \langle\{\varnothing\}, \varnothing\rangle, \langle\varnothing, \varnothing\rangle\}$；

(4) $R[\varnothing] = \varnothing$；

$R[\{\varnothing\}] = \{\{\varnothing, \{\varnothing\}\}, \varnothing\}$；

$R[\{\{\varnothing\}\}] = \{\varnothing\}$；

$R[\{\varnothing, \{\varnothing\}\}] = \operatorname{ran} R = \{\{\varnothing, \{\varnothing\}\}, \varnothing\}$；

(5) $\operatorname{dom} R = \{\varnothing, \{\varnothing\}\}$；

$\operatorname{ran} R = \{\{\varnothing, \{\varnothing\}\}, \varnothing\}$；

$\operatorname{fld} R = \operatorname{dom} R \cup \operatorname{ran} R = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$。

2.13

(1)

证明： 由 R 是二元关系易知，$R \cup R^{-1}$ 也是二元关系。

由引理 1.3 知，$R \subseteq R \cup R^{-1}$，即 $R \cup R^{-1}$ 包含 R。

而对任意 $\langle x, y\rangle$，有：

$\langle x, y\rangle \in R \cup R^{-1}$

$\iff \langle x, y\rangle \in R \vee \langle x, y\rangle \in R^{-1}$ (集合并定义)

$\iff \langle y, x\rangle \in R^{-1} \vee \langle y, x\rangle \in R$ (逆关系定义)

$\Longleftrightarrow \langle y,x\rangle \in R^{-1}\cup R$ (集合并定义)

$\Longleftrightarrow \langle y,x\rangle \in R\cup R^{-1}$ (交换律)

从而 $R\cup R^{-1}$ 是对称的。

对任意包含 R 的对称二元关系 R'，有：

$\forall\langle x,y\rangle$

$\langle x,y\rangle \in R\cup R^{-1}$

$\Longleftrightarrow \langle x,y\rangle \in R\vee \langle x,y\rangle \in R^{-1}$ (集合并定义)

$\Longleftrightarrow \langle x,y\rangle \in R\vee \langle y,x\rangle \in R$ (逆关系定义)

$\Longrightarrow \langle x,y\rangle \in R'\vee \langle y,x\rangle \in R'$ ($R\subseteq R'$)

$\Longleftrightarrow (\langle x,y\rangle \in R'\wedge \langle x,y\rangle \in R')\vee(\langle y,x\rangle \in R'\wedge \langle y,x\rangle \in R')$ (命题逻辑幂等律)

$\Longleftrightarrow (\langle x,y\rangle \in R'\wedge \langle x,y\rangle \in R'\wedge 1)\vee(\langle y,x\rangle \in R'\wedge \langle y,x\rangle \in R'\wedge 1)$ (命题逻辑同一律)

$\Longleftrightarrow (\langle x,y\rangle \in R'\wedge(\langle x,y\rangle \in R'\wedge(\langle x,y\rangle \in R'\to\langle y,x\rangle \in R')))\vee$

$(\langle y,x\rangle \in R'\wedge(\langle y,x\rangle \in R'\wedge(\langle y,x\rangle \in R'\to\langle x,y\rangle \in R')))$ (R' 是对称的)

$\Longrightarrow (\langle x,y\rangle \in R'\wedge \langle y,x\rangle \in R')\vee(\langle x,y\rangle \in R'\wedge \langle y,x\rangle \in R')$ (假言推理)

$\Longleftrightarrow \langle x,y\rangle \in R'\wedge \langle y,x\rangle \in R'$ (命题逻辑幂等律)

$\Longrightarrow \langle x,y\rangle \in R'$ (命题逻辑化简律)

即有 $R\cup R^{-1}\subseteq R'$。

综上所述，$R\cup R^{-1}$ 是包含 R 的最小的对称二元关系。 □

(2)

证明： 由 R 是二元关系易知，$R\cap R^{-1}$ 也是二元关系。

由引理 1.2 知，$R\cap R^{-1}\subseteq R$，即 $R\cap R^{-1}$ 含于 R。

而对任意 $\langle x,y\rangle$，有：

$\langle x,y\rangle \in R\cap R^{-1}$

$\Longleftrightarrow \langle x,y\rangle \in R\wedge \langle x,y\rangle \in R^{-1}$ (集合并定义)

$\Longleftrightarrow \langle y,x\rangle \in R^{-1}\wedge \langle y,x\rangle \in R$ (逆关系定义)

$\Longleftrightarrow \langle y,x\rangle \in R^{-1}\cap R$ (集合并定义)

$\Longleftrightarrow \langle y,x\rangle \in R\cap R^{-1}$ (交换律)

从而 $R\cap R^{-1}$ 是对称的。

对任意含于 R 的对称二元关系 $R'\subseteq R$，有：

$\forall\langle x,y\rangle$

$\langle x,y\rangle \in R'$

$\Longleftrightarrow \langle x,y\rangle \in R'\wedge \langle y,x\rangle \in R'$ (R' 是对称的)

$\Longrightarrow \langle x,y\rangle \in R\wedge \langle y,x\rangle \in R$ ($R'\subseteq R$)

$\Longleftrightarrow \langle x,y\rangle \in R\wedge \langle x,y\rangle \in R^{-1}$ (逆关系定义)

$\Longleftrightarrow \langle x,y\rangle \in R\cap R^{-1}$ (集合交定义)

即有 $R'\subseteq R\cap R^{-1}$。

综上所述，$R\cap R^{-1}$ 是含于 R 的最大的对称二元关系。 □

2.14

(1) $R = \{\langle 1,2\rangle, \langle 2,3\rangle\}$；

(2)

证明:

$$
\begin{aligned}
& R^2 \cap R = \varnothing && \\
\iff & \neg\exists x\exists z(\langle x,z\rangle \in R^2 \land \langle x,z\rangle \in R) && (\varnothing\ \text{定义}) \\
\iff & \forall x\forall z\neg(\langle x,z\rangle \in R^2 \land \langle x,z\rangle \in R) && (\text{量词否定等值式}) \\
\iff & \forall x\forall z(\neg\langle x,z\rangle \in R^2 \lor \neg\langle x,z\rangle \in R) && (\text{命题逻辑德·摩根律}) \\
\iff & \forall x\forall z(\neg(\exists y(\langle x,y\rangle \in R \land \langle y,z\rangle \in R)) \lor \neg\langle x,z\rangle \in R) && (\text{关系合成定义}) \\
\iff & \forall x\forall z(\forall y(\neg(\langle x,y\rangle \in R \land \langle y,z\rangle \in R)) \lor \neg\langle x,z\rangle \in R) && (\text{量词否定等值式}) \\
\iff & \forall x\forall z\forall y(\neg(\langle x,y\rangle \in R \land \langle y,z\rangle \in R) \lor \neg\langle x,z\rangle \in R) && (\text{量词辖域扩张等值式}) \\
\iff & \forall x\forall y\forall z(\neg(\langle x,y\rangle \in R \land \langle y,z\rangle \in R) \lor \neg\langle x,z\rangle \in R) && (\text{全称量词交换律}^{2}) \\
\iff & \forall x\forall y\forall z((\langle x,y\rangle \in R \land \langle y,z\rangle \in R) \to \neg\langle x,z\rangle \in R) && (\text{蕴涵等值式}) \\
\iff & R\ \text{是反传递的。} && (\text{反传递定义})
\end{aligned}
$$

$\square$

2.15

若 A 非空，则：

R 有如下性质：非自反：对任意 x，有 $x \not\subset x$，故 $\langle x,x\rangle \notin R$。
反自反：对任意 x，有 $\langle x,x\rangle \notin R$。
非对称：不存在 $\varnothing, A \in \mathcal{P}(A) \land \varnothing \subset A$ 但 $A \not\subset \varnothing$。
反对称：由于不存在 $x, y \in \mathcal{P}(A)$ 使得 $\langle x,y\rangle \in R \land \langle y,x\rangle \in R$，故 $\langle x,y\rangle \in R \land \langle y,x\rangle \in R \to x = y$ 恒成立。
传递：真子集性质。

S 有如下性质：

非自反：由于 A 非空，则故有 $A \in \mathcal{P}(A) \land A \neq \varnothing$，于是 $A \cap A = A \neq \varnothing \Rightarrow \langle A,A\rangle \notin S$。
非反自反：$\varnothing \in \mathcal{P}(A) \land \varnothing \cap \varnothing = \varnothing \Rightarrow \langle \varnothing,\varnothing\rangle \in S$。
对称：集合交性质。
非反对称：有 $\langle \varnothing,A\rangle \in S \land \langle A,\varnothing\rangle \in S$，但 $A \neq \varnothing$。
非传递：有 $\langle A,\varnothing\rangle \in S \land \langle \varnothing,A\rangle \in S$，但 $\langle A,A\rangle \notin S$。

T 有如下性质：

非自反：有 $\langle \varnothing,\varnothing\rangle \notin T$。
非反自反：有 $A \in \mathcal{P}(A) \land A \cup A = A \Rightarrow \langle A,A\rangle \in T$。
对称：集合并性质。
非反对称：有 $\langle \varnothing,A\rangle \in T \land \langle A,\varnothing\rangle \in T$，但 $A \neq \varnothing$。
非传递：有 $\langle \varnothing,A\rangle \in T \land \langle A,\varnothing\rangle \in T$，但 $\langle \varnothing,\varnothing\rangle \notin T$。

若 A 为空，则：

---

[2] 参见教材例 27.8。

R 有如下性质：

非自反：$\varnothing \not\subset \varnothing$。
反自反：不存在 x，使 $\langle x,x\rangle \in R$。
对称：不存在 $x,y \in \mathcal{P}(A)$ 使得 $\langle x,y\rangle \in R$，故 $xRy \to yRx$ 恒成立。
反对称：由于不存在 $x,y \in \mathcal{P}(A)$ 使得 $\langle x,y\rangle \in R \wedge \langle y,x\rangle \in R$，故 $\langle x,y\rangle \in R \wedge \langle y,x\rangle \in R \to x = y$ 恒成立。
传递：因为 $\varnothing$ 有真子集，故 R 为空关系。故不存在 x,y,z，使得 $\langle x,y\rangle \in R \wedge \langle y,z\rangle \in R$。所以蕴涵式：$\langle x,y\rangle \in R \wedge \langle y,z\rangle \in R \to \langle x,z\rangle \in R$ 永真。

S 有如下性质：

自反：$\langle\varnothing,\varnothing\rangle \in S$。
非反自反：$\langle\varnothing,\varnothing\rangle \in S$。
对称：集合交性质。
反对称：$\forall x\forall y(\langle x,y\rangle \in S \wedge \langle y,x\rangle \in S \Rightarrow x = \varnothing \wedge y = \varnothing \Rightarrow x = y)$。
传递：$\forall x\forall y\forall z(\langle x,y\rangle \in S \wedge \langle y,z\rangle \in S \Rightarrow x = \varnothing \wedge y = \varnothing \wedge z = \varnothing \Rightarrow \langle x,z\rangle \in S)$。

T 有如下性质：

自反：$\varnothing \cup \varnothing = \varnothing = A \Rightarrow \langle\varnothing,\varnothing\rangle \in T$。
非反自反：$\langle\varnothing,\varnothing\rangle \in T$。
对称：集合并性质。
反对称：$\forall x\forall y(\langle x,y\rangle \in T \wedge \langle y,x\rangle \in T \Rightarrow x = \varnothing \wedge y = \varnothing \Rightarrow x = y)$
传递：$\forall x\forall y\forall z(\langle x,y\rangle \in T \wedge \langle y,z\rangle \in T \Rightarrow x = \varnothing \wedge y = \varnothing \wedge z = \varnothing \Rightarrow \langle x,z\rangle \in T)$。

2.16

(1) $R = \{\langle 0,10\rangle, \langle 1,9\rangle, \langle 2,8\rangle, \langle 3,7\rangle, \langle 4,6\rangle, \langle 5,5\rangle, \langle 6,4\rangle, \langle 7,3\rangle, \langle 8,2\rangle, \langle 9,1\rangle, \langle 10,0\rangle\}$；
$S = \{\langle 0,4\rangle, \langle 3,3\rangle, \langle 6,2\rangle, \langle 9,1\rangle, \langle 12,0\rangle\}$。
(2)

R 有如下性质：

非自反：$\langle 0,0\rangle \notin R$。
非反自反：使 $\langle 5,5\rangle \in R$。
对称：加法性质。
非反对称：$\langle 0,10\rangle \in R \wedge \langle 10,0\rangle$，但 $0 \neq 10$。
非传递：$\langle 0,10\rangle \in R \wedge \langle 10,0\rangle$，但 $\langle 0,0\rangle \notin R$。

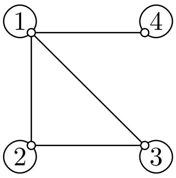
S 有如下性质：

非自反：$\langle 0,0\rangle \notin S$。
非反自反：$\langle 3,3\rangle \in S$。
非对称：$\langle 0,4\rangle \in S$，但 $\langle 4,0\rangle \notin S$。
反对称：不存在 $x,y \in A$ 使得 $\langle x,y\rangle \in S \wedge \langle y,x\rangle \in S$。

非传递：$\langle 12,0\rangle \in S \wedge \langle 0,4\rangle \in S$，但 $\langle 12,4\rangle \notin S$。

2.17

$$M(R)=\begin{pmatrix}1&1&1&1\\1&1&1&0\\1&1&1&0\\1&0&0&1\end{pmatrix}$$



$G(R)$

R 有如下性质：

自反：定义。
非反自反：有 $\langle 1,1\rangle \in R$。
对称：定义。
非反对称：有 $\langle 1,2\rangle \in R \wedge \langle 2,1\rangle \in R$ 但 $1 \neq 2$。
非传递：有 $\langle 2,0\rangle \in R \wedge \langle 0,3\rangle \in R$ 但 $\langle 2,3\rangle \notin R$。

2.18 $R_1=\{\langle a,a\rangle,\langle a,b\rangle,\langle b,b\rangle,\langle c,b\rangle,\langle c,c\rangle\}$；
$R_2=\{\langle a,b\rangle,\langle b,c\rangle\}$；
$R_3=\{\langle a,b\rangle,\langle a,c\rangle,\langle c,a\rangle,\langle c,b\rangle\}$；
$R_4=\{\langle a,a\rangle,\langle b,b\rangle,\langle c,c\rangle\}$。

$$M(R_1)=\begin{pmatrix}1&1&0\\0&1&0\\0&1&1\end{pmatrix},M(R_2)=\begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix},M(R_3)=\begin{pmatrix}0&1&1\\0&0&0\\1&1&0\end{pmatrix},M(R_4)=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$$

R_1 的性质：

自反：易于验证。
非反自反：$\langle a,a\rangle \in R_1$。
非对称：$\langle a,b\rangle \in R_1$，但 $\langle b,a\rangle \notin R_1$。
反对称：易于验证。
传递：易于验证。

R_2 的性质：

非自反：$\langle a,a\rangle \notin R_2$
反自反：易于验证。
非对称：$\langle a,b\rangle \in R_2$，但 $\langle b,a\rangle \notin R_2$。
反对称：易于验证。
非传递：$\langle a,b\rangle \in R_2 \wedge \langle b,c\rangle \in R_2$，但 $\langle a,c\rangle \notin R_2$。

R_3 的性质：

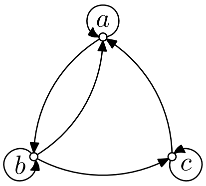
非自反：$\langle a,a\rangle \notin R_3$
反自反：易于验证。
非对称：$\langle a,b\rangle \in R_3$，但 $\langle b,a\rangle \notin R_3$。

非反对称：$\langle a,c\rangle \in R_3 \wedge \langle c,a\rangle \in R_3$，但 $a \neq c$
非传递：$\langle a,c\rangle \in R_3 \wedge \langle c,a\rangle \in R_3$，但 $\langle a,a\rangle \notin R_3$。

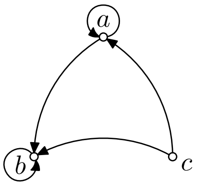
R_4 的性质：

自反：易于验证。
非反自反：$\langle a,a\rangle \in R_4$。
对称：易于验证。
反对称：易于验证。
传递：易于验证。

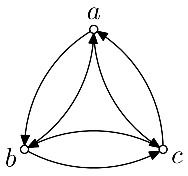
2.19 $R_1 = \{\langle a,a\rangle, \langle a,b\rangle, \langle b,a\rangle, \langle b,b\rangle, \langle b,c\rangle, \langle c,a\rangle, \langle c,c\rangle\}$；
$R_2 = \{\langle a,a\rangle, \langle a,b\rangle, \langle b,b\rangle, \langle c,a\rangle, \langle c,b\rangle\}$；
$R_3 = \{\langle a,b\rangle, \langle a,c\rangle, \langle b,a\rangle, \langle b,c\rangle, \langle c,a\rangle, \langle c,b\rangle\}$；
$R_4 = \{\langle a,a\rangle, \langle a,b\rangle, \langle a,c\rangle, \langle b,c\rangle, \langle c,a\rangle\}$。



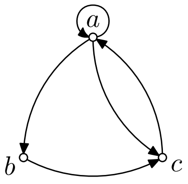
$G(R_1)$



$G(R_2)$



$G(R_3)$



$G(R_4)$

R_1 的性质：

自反：易于验证。
非反自反：$\langle a,a\rangle \in R_1$。
非对称：$\langle c,a\rangle \in R_1$，但 $\langle a,c\rangle \notin R_1$。
非反对称：$\langle a,b\rangle \in R_1 \wedge \langle b,a\rangle \in R_1$，但 $a \neq b$
非传递：$\langle c,a\rangle \in R_1 \wedge \langle a,b\rangle \in R_1$，但 $\langle c,b\rangle \notin R_1$。

R_2 的性质：

非自反：$\langle c,c\rangle \notin R_2$
非反自反：$\langle a,a\rangle \in R_2$
非对称：$\langle a,b\rangle \in R_2$，但 $\langle b,a\rangle \notin R_2$。
反对称：易于验证。
传递：易于验证。

R_3 的性质：

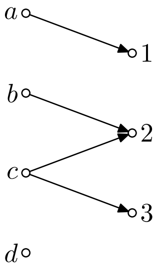
非自反：$\langle a,a\rangle \notin R_3$
反自反：易于验证。
对称：易于验证。
非反对称：$\langle a,b\rangle \in R_3 \wedge \langle b,a\rangle \in R_3$，但 $a \neq b$
非传递：$\langle a,b\rangle \in R_3 \wedge \langle b,a\rangle \in R_3$，但 $\langle a,a\rangle \notin R_3$。

R_4 的性质：

非自反：$\langle b,b\rangle \notin R_4$。
非反自反：$\langle a,a\rangle \in R_4$。
非对称：$\langle a,b\rangle \in R_4$，但 $\langle b,a\rangle \notin R_4$。
非反对称：$\langle a,c\rangle \in R_4 \wedge \langle c,a\rangle \in R_4$，但 $a \neq c$
非传递：$\langle c,a\rangle \in R_4 \wedge \langle a,b\rangle \in R_4$，但 $\langle c,b\rangle \notin R_4$。

2.20

$$M(R_1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$



$G(R_1)$

2.21

$$M(R_1) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad M(R_2) = \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$M(R_2 \circ R_1) = M(R_1) \cdot M(R_2) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

得：$R_2 \circ R_1 = \{\langle 1,\beta\rangle\}$。

2.22

证明： 由 R 的自反性和教材定理 2.19(1) 知，$R = r(R) = R \cup I_A$。从而：

$$\begin{aligned} R &\subseteq (R \circ R) \cup R && \text{(引理 1.3)} \\ &= (R \circ R) \cup (R \circ I_A) && (R \circ I_A = R) \\ &= R \circ (R \cup I_A) && \text{(教材定理 2.6(1))} \\ &= R \circ R && (R = R \cup I_A) \end{aligned}$$

而由 R 的传递性和教材定理 2.14 知，$R \circ R \subseteq R$。

从而有 $R \circ R = R$。 □

举反例证明逆定理不成立。

证明： 令 $A = \{a,b\}$，$R = \{\langle a,a\rangle\}$，则有 $R \circ R = \{\langle a,a\rangle\} = R$，但 $\langle b,b\rangle \notin R$，因而 R 不是自反的。

故有：$R \circ R = R \nRightarrow (R\text{是自反的} \wedge R\text{是传递的})$。 □

2.23

证明： 先证必要性。

若 $R \circ S$ 具有对称性，则：

$\forall x,y$

$\langle x,y\rangle \in R \circ S$

$\Longrightarrow \langle y,x\rangle \in R\circ S$ ($R\circ S$ 是对称的)

$\Longleftrightarrow \exists z(\langle y,z\rangle \in S \wedge \langle z,x\rangle \in R)$ (合成运算定义)

$\Longrightarrow \exists z(\langle z,y\rangle \in S \wedge \langle x,z\rangle \in R)$ (R 和 S 都是对称的)

$\Longleftrightarrow \exists z(\langle x,z\rangle \in R \wedge \langle z,y\rangle \in S)$ (命题逻辑交换律)

$\Longleftrightarrow \langle x,y\rangle \in S\circ R$ (合成运算定义)

于是有 $R\circ S \subseteq S\circ R$。

同理可证：$S\circ R \subseteq R\circ S$。

于是证得：若 $R\circ S$ 具有对称性，则 $R\circ S = S\circ R$。

下面证充分性。

若 $R\circ S = S\circ R$，则：

$\forall x, y$

$\langle x,y\rangle \in R\circ S$

$\Longleftrightarrow \langle x,y\rangle \in S\circ R$ ($R\circ S = S\circ R$)

$\Longleftrightarrow \exists z(\langle x,z\rangle \in R \wedge \langle z,y\rangle \in S)$ (合成运算定义)

$\Longrightarrow \exists z(\langle z,x\rangle \in R \wedge \langle y,z\rangle \in S)$ (R 和 S 都是对称的)

$\Longleftrightarrow \exists z(\langle y,z\rangle \in S \wedge \langle z,x\rangle \in R)$ (命题逻辑交换律)

$\Longleftrightarrow \langle y,x\rangle \in R\circ S$ (合成运算定义)

充分性得证。

综合即得原题。 □

2.24 $R_1 = \varnothing$；

$R_2 = \{\langle 1,1\rangle\}$；

$R_3 = \{\langle 2,2\rangle\}$；

$R_4 = \{\langle 1,2\rangle\}$；

$R_5 = \{\langle 2,1\rangle\}$；

$R_6 = \{\langle 1,1\rangle, \langle 1,2\rangle\}$；

$R_7 = \{\langle 1,1\rangle, \langle 2,1\rangle\}$；

$R_8 = \{\langle 1,1\rangle, \langle 2,2\rangle\}$；

$R_9 = \{\langle 1,2\rangle, \langle 2,1\rangle\}$；

$R_{10} = \{\langle 1,2\rangle, \langle 2,2\rangle\}$；

$R_{11} = \{\langle 2,1\rangle, \langle 2,2\rangle\}$；

$R_{12} = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 2,1\rangle\}$；

$R_{13} = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 2,2\rangle\}$；

$R_{14} = \{\langle 1,1\rangle, \langle 2,1\rangle, \langle 2,2\rangle\}$；

$R_{15} = \{\langle 1,2\rangle, \langle 2,1\rangle, \langle 2,2\rangle\}$；

$R_{16} = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 2,1\rangle, \langle 2,2\rangle\}$；

其中：

$R_8, R_{13}, R_{14}, R_{16}$ 是自反的。

R_1, R_4, R_5, R_9 是反自反的。

$R_1, R_2, R_3, R_8, R_9, R_{12}, R_{15}, R_{16}$ 是对称的。

$R_1, R_2, R_3, R_4, R_5, R_6, R_7, R_8, R_{10}, R_{11}, R_{13}, R_{14}$ 是反对称的。

$R_1, R_2, R_3, R_4, R_5, R_6, R_7, R_8, R_{10}, R_{11}, R_{13}, R_{14}, R_{16}$ 是传递的。

R_1 是空关系，R_8 是恒等关系，R_{16} 是全域关系，R_{13} 是小于等于关系，R_4 是小于关系，R_{14} 是大于等于关系，R_5 是大于关系，R_{13} 是整除关系。

2.25

先证：$I_{\operatorname{dom} R} \subseteq R^{-1} \circ R$。

证明:

$\forall x, y$

$\langle x, y\rangle \in I_{\operatorname{dom} R}$

$\iff x = y \land x \in \operatorname{dom} R$ (恒等关系定义)

$\iff x = y \land \exists z(\langle x, z\rangle \in R)$ (定义域定义)

$\iff x = y \land \exists z(\langle x, z\rangle \in R \land \langle z, x\rangle \in R^{-1})$ (逆关系定义)

$\iff x = y \land \langle x, x\rangle \in R^{-1} \circ R$ (合成运算定义)

$\iff \langle x, y\rangle = \langle x, x\rangle \land \langle x, x\rangle \in R^{-1} \circ R$ (教材定理 2.1)

$\implies \langle x, y\rangle \in R^{-1} \circ R$ (等号性质)

□

再证：$I_{\operatorname{ran} R} \subseteq R \circ R^{-1}$。

证明:

$\forall x, y$

$\langle x, y\rangle \in I_{\operatorname{ran} R}$

$\iff x = y \land x \in \operatorname{ran} R$ (恒等关系定义)

$\iff x = y \land \exists z(\langle z, x\rangle \in R)$ (值域定义)

$\iff x = y \land \exists z(\langle z, x\rangle \in R \land \langle x, z\rangle \in R^{-1})$ (逆关系定义)

$\iff x = y \land \exists z(\langle x, z\rangle \in R^{-1} \land \langle z, x\rangle \in R)$ (命题逻辑交换律)

$\iff x = y \land \langle x, x\rangle \in R \circ R^{-1}$ (合成运算定义)

$\iff \langle x, y\rangle = \langle x, x\rangle \land \langle x, x\rangle \in R \circ R^{-1}$ (教材定理 2.1)

$\implies \langle x, y\rangle \in R \circ R^{-1}$ (等号性质)

□

2.26

(1)

$$M(R) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad M(R^2) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad M(R^3) = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

得：$R^2 = \{\langle a, a\rangle, \langle a, c\rangle, \langle b, b\rangle, \langle b, d\rangle\}$，$R^3 = \{\langle a, b\rangle, \langle a, d\rangle, \langle b, a\rangle, \langle b, c\rangle\}$。

(2) $m = 2, n = 4$；

(3) 注意到：$R^2 = R^4$ 并不意味着 $R^1 = R^3$ 或 $R^2 = I_A$。这一结论可以表述成：在半群(和独异点)上，消去律不一定成立。另外，当 A 为无穷集时，未必存在满足第 (2) 小题的 m 和 n。例

如，我们可以 $\mathbb{N}$ 上定义一个关系 $R_1 = \{\langle x, y\rangle \mid x, y \in N \wedge y = x+1\}$。注意到，对任意 $k \in \mathbb{N}$，$R_1^k = \{\langle x, y\rangle \mid x, y \in N \wedge y = x+k\}$，从而不存在 $m, n \in \mathbb{N}$，使得 $m \neq n \wedge R_1^m = R_1^n$。

2.27 先证两个引理。

引理 2.1 对任意二元关系 R_1, R_2，有：$\operatorname{dom}(R_1 \circ R_2) \subseteq \operatorname{dom} R_2$ 和 $\operatorname{ran}(R_1 \circ R_2) \subseteq \operatorname{ran} R_1$。特别地，对所有 $m \in \mathbb{N}_+$，有 $\operatorname{dom}(R_1^m) \subseteq \operatorname{dom} R_1$ 和 $\operatorname{ran}(R_1^m) \subseteq \operatorname{ran} R_1$。

证明：

$$\forall x, y$$

$$
\begin{aligned}
& \langle x, y\rangle \in R_1 \circ R_2 \\
\Longleftrightarrow\ & \exists z(\langle x, z\rangle \in R_2 \wedge \langle z, y\rangle \in R_1) && \text{(合成运算定义)} \\
\Longrightarrow\ & \exists z(\langle x, z\rangle \in R_2) \wedge \exists z(\langle z, y\rangle \in R_1) && \text{(一阶谓词推理定律)} \\
\Longleftrightarrow\ & x \in \operatorname{dom} R_2 \wedge y \in \operatorname{ran} R_1 && \text{(dom、ran 定义)}
\end{aligned}
$$

这就证明了 $\operatorname{dom}(R_1 \circ R_2) \subseteq \operatorname{dom} R_2$ 和 $\operatorname{ran}(R_1 \circ R_2) \subseteq \operatorname{ran} R_1$。

令 $R_2 = R_1$ 并对 m 作归纳即得此引理的特殊情况：$\forall m \in \mathbb{N}_+, \operatorname{dom}(R_1^m) \subseteq \operatorname{dom} R_1 \wedge \operatorname{ran}(R_1^m) \subseteq \operatorname{ran} R_1$。 □

引理 2.2 对任意二元关系 R_1, R_2，若 $\operatorname{fld} R_1 \cap \operatorname{fld} R_2 = \varnothing$，则 $\forall m, n \in \mathbb{N}_+ (R_1^m \circ R_2^n = \varnothing)$。

证明： 先证：$\forall R_1, R_2((\operatorname{fld} R_1 \cap \operatorname{fld} R_2 = \varnothing) \Rightarrow (R_1 \circ R_2 = \varnothing))$。

若不然，就有 $\langle x, y\rangle \in (R_1 \circ R_2)$。由合成运算定义知，$\exists z(\langle x, z\rangle \in R_2 \wedge \langle z, y\rangle \in R_1)$。从而有 $z \in \operatorname{ran} R_2 \subseteq \operatorname{fld} R_2$ 和 $z \in \operatorname{dom} R_1 \subseteq \operatorname{fld} R_1$，于是有 $z \in \operatorname{fld} R_1 \cap \operatorname{fld} R_2$，与前题矛盾。

这就证明了：$\forall R_1, R_2((\operatorname{fld} R_1 \cap \operatorname{fld} R_2 = \varnothing) \Rightarrow (R_1 \circ R_2 = \varnothing))$。

下面证原命题。

由引理 2.1 知，$\operatorname{dom}(R_1^m) \subseteq \operatorname{dom} R_1$ 且 $\operatorname{ran}(R_1^m) \subseteq \operatorname{ran} R_1$，从而有：

$$
\begin{aligned}
\operatorname{fld}(R_1^m) &= \operatorname{dom}(R_1^m) \cup \operatorname{ran}(R_1^m) && \text{(fld 定义)} \\
&\subseteq \operatorname{dom} R_1 \cup \operatorname{ran} R_1 && \text{(引理 2.1、引理 1.4)} \\
&= \operatorname{fld} R_1 && \text{(fld 定义)}
\end{aligned}
$$

同理可得 $\operatorname{fld}(R_2^n) \subseteq \operatorname{fld} R_2$。从而有：

$$
\begin{aligned}
\operatorname{fld}(R_1^m) \cap \operatorname{fld}(R_2^n) &\subseteq \operatorname{fld} R_1 \cap \operatorname{fld} R_2 && \text{(引理 1.5)} \\
&= \varnothing && \text{(题设)}
\end{aligned}
$$

使用本证明前半部分的结论，就有：$R_1^m \circ R_2^n = \varnothing$。 □

下面证原题。

证明： 用归纳法证明。

当 $m = 0$ 时：

由于 $R_1 \cup R_2$ 仍是 A 上的二元关系。故有：

$$
\begin{aligned}
(R_1 \cup R_2)^0 &= I_A && \text{(幂运算定义)} \\
&= I_A \cup I_A && \text{(幂等律)} \\
&= R_1^0 \cup R_2^0 && \text{(幂运算定义)}
\end{aligned}
$$

设 $m = k$ 时 ($k \in \mathbb{N}$)，等式成立，即有：$(R_1 \cup R_2)^k = R_1^k \cup R_2^k$。

则，当 $m = k+1$ 时：

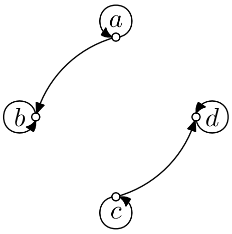
$$
\begin{aligned}
(R_1 \cup R_2)^{k+1} &= (R_1 \cup R_2)^k \circ (R_1 \cup R_2) && \text{(幂运算定义)} \\
&= (R_1^k \cup R_2^k) \circ (R_1 \cup R_2) && \text{(归纳前提)} \\
&= (R_1^k \cup R_2^k) \circ R_1 \cup (R_1^k \cup R_2^k) \circ R_2 && \text{(教材定理 2.6(1))}
\end{aligned}
$$

$$\begin{aligned}
&= (R_1^k \circ R_1) \cup (R_2^k \circ R_1) \cup (R_1^k \circ R_2) \cup (R_2^k \circ R_2) && (\text{教材定理 2.6(2)}) \\
&= R_1^{k+1} \cup (R_2^k \circ R_1) \cup (R_1^k \circ R_2) \cup R_2^{k+1} && (\text{幂运算定义}) \\
&= R_1^{k+1} \cup \varnothing \cup \varnothing \cup R_2^{k+1} && (\text{引理 2.2}) \\
&= R_1^{k+1} \cup R_2^{k+1} && (\text{同一律})
\end{aligned}$$

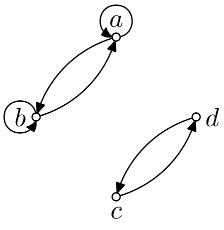
□

2.28 $m = 0, n = 15$。[3]

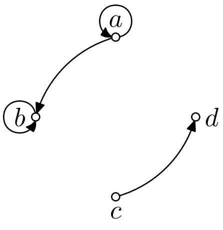
2.29 $r(R) = \{\langle a,a\rangle, \langle a,b\rangle, \langle b,b\rangle, \langle c,c\rangle, \langle c,d\rangle, \langle d,d\rangle\}$；
$s(R) = \{\langle a,a\rangle, \langle a,b\rangle, \langle b,a\rangle, \langle b,b\rangle, \langle c,d\rangle, \langle d,c\rangle\}$；
$t(R) = \{\langle a,a\rangle, \langle a,b\rangle, \langle b,b\rangle, \langle c,d\rangle\}$。



$r(R)$



$s(R)$



$t(R)$

2.30

(1)

证明： 由传递闭包的定义知，$R^+ = t(R)$ 是传递的。又由教材定理 2.19(3) 知，$(R^+)^+ = t(R^+) = R^+$。 □

(2)

证明： 由教材定理 2.22 和 2.24 知，$R^\oplus = rt(R)$。又由教材定理 2.25(3) 知，$R^\oplus$ 是自反的和传递的。再由教材定理 2.19(3) 知，$trt(R) = rt(R)$。最后由教材定理 2.19(1) 和 2.25(3) 知，$rtrt(R) = trt(R)$。于是，$(R^\oplus)^\oplus = rtrt(R) = trt(R) = rt(R) = R^\oplus$。 □

(3)

证明：

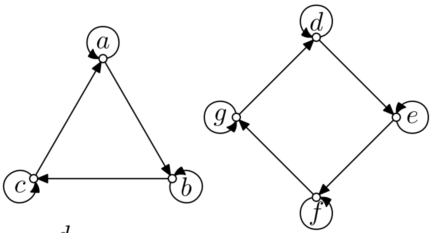
$$\begin{aligned}
R \circ R^\oplus &= R \circ \bigcup_{i=0}^{\infty} R^i && (\text{定义}) \\
&= \bigcup_{i=0}^{\infty} R \circ R^i && (\text{教材定理 2.6(1)}) \\
&= \bigcup_{i=0}^{\infty} R^{i+1} && (\text{教材定理 2.17(1)}) \\
&= \bigcup_{i=1}^{\infty} R^i && (i := i+1) \\
&= t(R) && (\text{教材定理 2.24}) \\
&= R^+ && (\text{定义})
\end{aligned}$$

同理可证：$R^+ = R^\oplus \circ R$。 □

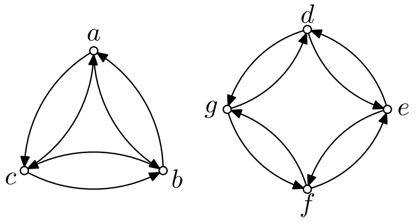
---

[3] 题目中"最小的自然数 $m, n(m \leq n)$"应改为"最小的自然数 $m, n(m < n)$"。否则取 $m = n = 0$ 即可。

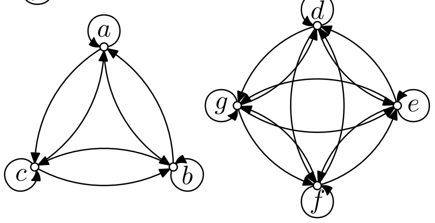
2.31



$r(R)$



$s(R)$



$t(R)$

2.32

证明: 由 $A = I \cdot A \cdot I$ 可得三种关系的自反性。

分别由 $B = P \cdot A \cdot Q \to A = P^{-1} \cdot B \cdot Q^{-1}$、$B = P \cdot A \cdot P^{-1} \to A = P^{-1} \cdot B \cdot (P^{-1})^{-1}$ 和 $B = P \cdot A \cdot P^T \to A = P^{-1} \cdot B \cdot (P^T)^{-1} = P^{-1} \cdot B \cdot (P^{-1})^T$，得三种关系的对称性。

再由 $B = P_1 \cdot A \cdot Q_1 \land C = P_2 \cdot B \cdot Q_2 \to C = P_2 \cdot P_1 \cdot A \cdot Q_1 \cdot Q_2$、$B = P \cdot A \cdot P^{-1} \land C = Q \cdot B \cdot Q^{-1} \to C = Q \cdot P \cdot A \cdot P^{-1} \cdot Q^{-1} = Q \cdot P \cdot A \cdot (Q \cdot P)^{-1}$ 和 $B = P \cdot A \cdot P^T \land C = Q \cdot B \cdot Q^T \to C = Q \cdot P \cdot A \cdot P^T \cdot Q^T = Q \cdot P \cdot A \cdot (Q \cdot P)^T$，得三种关系的传递性。

综上所述，三种关系皆为等价关系。 □

2.33

证明: 自反性。对任意 $a + bi \in \mathbb{C}^*$，由 a 是实数和 $a \neq 0$ 得：$a^2 > 0$。从而有 $\langle a + bi, a + bi \rangle \in R$。

对称性。对任意 $\langle a + bi, c + di \rangle \in R$，由定义得：$a + bi \in \mathbb{C}^* \land c + di \in \mathbb{C}^* \land ac > 0$，由逻辑与运算交换律和实数乘法交换律得：$c + di \in \mathbb{C}^* \land a + bi \in \mathbb{C}^* \land ca > 0$，于是得 $\langle c + di, a + bi \rangle \in R$。

传递性。对任意 $\langle a_1 + b_1 i, a_2 + b_2 i \rangle, \langle a_2 + b_2 i, a_3 + b_3 i \rangle \in R$，推得 $a_1 + b_1 i \in \mathbb{C}^* \land a_3 + b_3 i \in \mathbb{C}^* \land a_1 a_2 > 0 \land a_2 a_3 > 0$。由乘法性质知，$ab > 0 \Leftrightarrow \mathrm{sgn}(a) = \mathrm{sgn}(b)$，[4] 于是有：

$$
\begin{aligned}
& a_1 a_2 > 0 \land a_2 a_3 \\
\iff & \mathrm{sgn}(a_1) = \mathrm{sgn}(a_2) \land \mathrm{sgn}(a_2) = \mathrm{sgn}(a_3) && \text{(乘法性质)} \\
\implies & \mathrm{sgn}(a_1) = \mathrm{sgn}(a_3) && \text{(等号传递性)} \\
\iff & a_1 a_3 > 0 && \text{(乘法性质)}
\end{aligned}
$$

故有 $\langle a_1 + b_1 i, a_3 + b_3 i \rangle \in R$。

综合得，R 是等值关系。 □

$\mathbb{C}^*/R = \{\{a + bi \mid a + bi \in \mathbb{C}^* \land a > 0\}, \{a + bi \mid a + bi \in \mathbb{C}^* \land a < 0\}\}$；

R 可以看作复平面内一切与 y 轴没有公共点的有向线段的集合。$\mathbb{C}^*/R$ 的性质则说明：一个有向线段与 y 轴没有公共点当且仅当线段的两个端点皆在 y 轴的同一侧。

2.34

(1) 不是。

---

[4] sgn 是“符号函数”(signum)，定义为 $\mathrm{sgn}(x) = \begin{cases} -1 & x < 0 \\ 0 & x = 0 \\ 1 & x > 0 \end{cases}$。

证明： 由等价关系定义知 $\forall x(x \in A \to \langle x,x\rangle \in R_1)$，由绝对补运算定义可知，$\forall x(x \in A \to \langle x,x\rangle \notin {\sim}R_1)$。而 A 非空，即存在 $x \in A$ 但 $\langle x,x\rangle \notin {\sim}R_1$，于是 ${\sim}R_1$ 不是自反关系，因而也不是等价关系。 □

(2) 不是。

证明： 由等价关系定义知 $\forall x(x \in A \to (\langle x,x\rangle \in R_1 \wedge \langle x,x\rangle \in R_2))$，由相对补运算定义可知，$\forall x(x \in A \to \langle x,x\rangle \notin R_1 - R_2)$。而 A 非空，即存在 $x \in A$ 但 $\langle x,x\rangle \notin R_1 - R_2$，于是 $R_1 - R_2$ 不是自反关系，因而也不是等价关系。

同理，$R_2 - R_1$ 也不是等价关系。 □

(3) 不一定。

证明： 反例：令 $A = \{a,b,c\}, R_1 = E, R_2 = \{\langle a,c\rangle, \langle c,a\rangle\} \cup I_A$，易见 R_1 和 R_2 都是等价关系。但对 $r(R_1 - R_2) = \{\langle a,b\rangle, \langle b,a\rangle, \langle b,c\rangle, \langle c,b\rangle\} \cup I_A$，有 $\langle a,b\rangle \in r(R_1 - R_2) \wedge \langle b,c\rangle \in r(R_1 - R_2)$，但 $\langle a,c\rangle \notin r(R_1 - R_2)$。$r(R_1 - R_2)$ 不是传递的，因而不是等价关系。由对称性可证：$r(R_2 - R_1)$ 的情况。

“正例”：令 $R_1 = R_2 = I_A$，则 $R_1 = R_2 = r(R_1 - R_2) = r(R_2 - R_1) = I_A$ 都是等价关系。

可见，当 R_1 和 R_2 都是等价关系时，$r(R_1 - R_2)$ 或 $r(R_2 - R_1)$ 不一定是等价关系。 □

(4) 不一定。

证明： 反例：令 $A = \{a,b,c\}, R_1 = \{\langle a,b\rangle, \langle b,a\rangle\} \cup I_A, R_2 = \{\langle a,c\rangle, \langle c,a\rangle\} \cup I_A$，易见 R_1 和 R_2 都是等价关系。但 $R_1 \circ R_2 = \{\langle a,b\rangle, \langle a,c\rangle, \langle b,a\rangle, \langle c,a\rangle, \langle c,b\rangle\} \cup I_A$ 不是对称的(有 $\langle c,b\rangle \in R_1 \circ R_2$ 但 $\langle b,c\rangle \notin R_1 \circ R_2$)，因而不是等价关系。由对称性可证：$R_2 \circ R_1$ 的情况。

“正例”：令 $R_1 = R_2 = I_A$，$R_1 = R_2 = R_1 \circ R_2 = R_2 \circ R_1 = I_A$ 都是等价关系。

可见，当 R_1 和 R_2 都是等价关系时，$R_1 \circ R_2$ 或 $R_2 \circ R_1$ 不一定是等价关系。 □

2.35

证明： 先证 R 是对称的。

$\forall x, y \in A$

$\langle x,y\rangle \in R$

$\iff \langle x,y\rangle \in R \wedge 1$ (命题逻辑同一律)

$\iff \langle x,y\rangle \in R \wedge \langle x,x\rangle \in R$ (R 是自反的)

$\implies \langle y,x\rangle \in R$ (题设 (2))

再证 R 是传递的。

$\forall x, y, z \in A$

$\langle x,y\rangle \in R \wedge \langle y,z\rangle \in R$

$\implies \langle y,x\rangle \in R \wedge \langle y,z\rangle \in R$ (R 是对称的)

$\implies \langle x,z\rangle \in R$ (题设 (2))

由题设，R 是自反的。从而 R 是 A 上的等价关系。 □

2.36

证明： (1) 由 B_{i_k} 的选择方式知 $\varnothing \notin \pi_2$。

(2) 对任意 $j, k \in \{1, 2, \ldots, m\} \wedge j \neq k$，有：

$B_{i_j} \cap B_{i_k} = (A_{i_j} \cap B) \cap (A_{i_k} \cap B)$ (定义)

$= A_{i_j} \cap A_{i_k} \cap B \cap B$ (结合律、交换律)

$$\begin{aligned}
&= \varnothing \cap B \cap B && (\pi_1\text{ 是划分})\\
&= \varnothing && (\text{零律})
\end{aligned}$$

(3)

$$\begin{aligned}
A \cap B &= \cup\pi_1 \cap B && (\pi_1\text{ 是 }A\text{ 的划分})\\
&= \left(\bigcup_{i=1}^{n} A_i\right) \cap B && (\text{广义并定义})\\
&= \bigcup_{i=1}^{n} (A_i \cap B) && (\text{分配律})\\
&= \bigcup_{k=1}^{m} (A_{i_k} \cap B) && (A_i \cap B\text{ 中有 }m\text{ 个非空的})\\
&= \bigcup_{k=1}^{m} B_{i_k} && (\text{定义})\\
&= \cup\pi_2 && (\text{广义并定义})
\end{aligned}$$

综上所述，π_2 满足划分的全部条件。因此 π_2 是 $A \cap B$ 的一个划分。 □

2.37

证明: 由模运算性质立即得证。 □

$$A/R = \{\{1,6,11,16\},\{2,7,12,17\},\{3,8,13,18\},\{4,9,14,19\},\{5,10,15,20\}\}。$$

2.38

证明: (1) 由 $\mathscr{A}$ 的定义知，$\varnothing \notin \mathscr{A}$。

(2) $\forall A_{i_1} \cap B_{j_1}, A_{i_2} \cap B_{j_2} \in \mathscr{A}$，

$$\begin{aligned}
& A_{i_1} \cap B_{j_1} \cap A_{i_2} \cap B_{j_2} \neq \varnothing &&\\
\Longleftrightarrow\ & \exists x(x \in A_{i_1} \cap B_{j_1} \cap A_{i_2} \cap B_{j_2}) && (\varnothing\text{ 定义})\\
\Longleftrightarrow\ & \exists x(x \in A_{i_1} \wedge x \in B_{j_1} \wedge x \in A_{i_2} \wedge x \in B_{j_2}) && (\text{交集定义})\\
\Longleftrightarrow\ & \exists x(x \in A_{i_1} \wedge x \in A_{i_2} \wedge x \in B_{j_1} \wedge x \in B_{j_2}) && (\text{命题逻辑交换律})\\
\Longrightarrow\ & \exists x(x \in A_{i_1} \wedge x \in A_{i_2}) \wedge \exists x(x \in B_{j_1} \wedge x \in B_{j_2}) && (\text{一阶谓词推理定律})\\
\Longleftrightarrow\ & \exists x(x \in A_{i_1} \cap A_{i_2}) \wedge \exists x(x \in B_{j_1} \cap B_{j_2}) && (\text{交集定义})\\
\Longleftrightarrow\ & A_{i_1} \cap A_{i_2} \neq \varnothing \wedge B_{j_1} \cap B_{j_2} \neq \varnothing && (\varnothing\text{ 定义})\\
\Longrightarrow\ & A_{i_1} = A_{i_2} \wedge B_{j_1} = B_{j_2} && (\pi_1, \pi_2\text{ 是划分})\\
\Longrightarrow\ & A_{i_1} \cap B_{j_1} = A_{i_2} \cap B_{j_2} && (\text{交集定义、外延原则})
\end{aligned}$$

可见，对任意 $A_{i_1} \cap B_{j_1}, A_{i_2} \cap B_{j_2} \in R$，若 $A_{i_1} \cap B_{j_1} \neq A_{i_2} \cap B_{j_2}$，则 $A_{i_1} \cap B_{j_1} \cap A_{i_2} \cap B_{j_2} = \varnothing$。

(3)

$$\begin{aligned}
A &= A \cap A && (\text{幂等律})\\
&= (\cup\pi_1) \cap (\cup\pi_2) && (\pi_1, \pi_2\text{ 是划分})\\
&= \left(\bigcup_{i=1}^{m} A_i\right) \cap \left(\bigcup_{j=1}^{n} B_j\right) && (\pi_1, \pi_2\text{ 定义})\\
&= \bigcup_{\substack{1\le i\le m\\ 1\le j\le n}} (A_i \cap B_j) && (\text{分配律})\\
&= \cup\mathscr{A} && (\mathscr{A}\text{ 定义})
\end{aligned}$$

综上所述，有 $\mathscr{A}$ 是划分。

下面证明 $\mathscr{A}$ 既是 π_1 的加细又是 π_2 的加细。

对任意 $A_i \cap B_j \in \mathscr{A}$，由引理 1.2 知，有 $A_i \cap B_j \subseteq A_i$ 和 $A_i \cap B_j \subseteq B_j$。即，$\mathscr{A}$ 中的每一个划分块都含于 π_1 和 π_2 的某个划分块中。由加细定义知，$\mathscr{A}$ 既是 π_1 的加细又是 π_2 的加细。 $\square$

2.39

(1) $R_\pi = \{\langle 1,2\rangle, \langle 1,3\rangle, \langle 2,1\rangle, \langle 2,3\rangle, \langle 3,1\rangle, \langle 3,2\rangle\} \cup I_A$；

$A/R_\pi = \pi = \{\{1,2,3\},\{4\}\}$；

(2) $\pi_1 = A/R_{\pi_1} = \{\{1\},\{2\},\{3\},\{4\}\}$；

$R_{\pi_1} = I_A$；

$\pi_2 = A/R_{\pi_2} = \{\{1,2\},\{3\},\{4\}\}$；

$R_{\pi_2} = \{\langle 1,2\rangle, \langle 2,1\rangle\} \cup I_A$；

$\pi_3 = A/R_{\pi_3} = \{\{1,3\},\{2\},\{4\}\}$；

$R_{\pi_3} = \{\langle 1,3\rangle, \langle 3,1\rangle\} \cup I_A$；

$\pi_4 = A/R_{\pi_4} = \{\{1\},\{2,3\},\{4\}\}$；

$R_{\pi_4} = \{\langle 2,3\rangle, \langle 3,2\rangle\} \cup I_A$；

$\pi_5 = A/R_{\pi_5} = \pi$；

$R_{\pi_5} = R_\pi = \{\langle 1,2\rangle, \langle 1,3\rangle, \langle 2,1\rangle, \langle 2,3\rangle, \langle 3,1\rangle, \langle 3,2\rangle\} \cup I_A$。

2.40

证明： 必要性：

由加细定义有，$\forall \mathscr{A}(\mathscr{A} \in A/R_1 \rightarrow \exists \mathscr{B}(\mathscr{B} \in A/R_2 \wedge \mathscr{A} \subseteq \mathscr{B}))$，故有：

$$
\begin{aligned}
& \forall x, y \in A \\
& \langle x, y\rangle \in R_1 \\
\Longleftrightarrow\ & \exists \mathscr{A}(\mathscr{A} \in A/R_1 \wedge x \in \mathscr{A} \wedge y \in \mathscr{A}) && \text{(商集定义)} \\
\Longrightarrow\ & \mathscr{A} \in A/R_1 \wedge x \in \mathscr{A} \wedge y \in \mathscr{A} && \text{(}\exists\text{消去)} \\
\Longleftrightarrow\ & \mathscr{A} \in A/R_1 \wedge x \in \mathscr{A} \wedge y \in \mathscr{A} \wedge \exists \mathscr{B}(\mathscr{B} \in A/R_2 \wedge \mathscr{A} \subseteq \mathscr{B}) && \text{(前提)} \\
\Longleftrightarrow\ & \exists \mathscr{B}(\mathscr{A} \in A/R_1 \wedge x \in \mathscr{A} \wedge y \in \mathscr{A} \wedge \mathscr{B} \in A/R_2 \wedge \mathscr{A} \subseteq \mathscr{B}) && \text{(量词辖域扩张等值式)} \\
\Longrightarrow\ & \mathscr{A} \in A/R_1 \wedge x \in \mathscr{A} \wedge y \in \mathscr{A} \wedge \mathscr{B} \in A/R_2 \wedge \mathscr{A} \subseteq \mathscr{B} && \text{(}\exists\text{消去)} \\
\Longrightarrow\ & \mathscr{B} \in A/R_2 \wedge x \in \mathscr{A} \wedge y \in \mathscr{A} \wedge \mathscr{A} \subseteq \mathscr{B} && \text{(命题逻辑化简律、交换律)} \\
\Longrightarrow\ & \mathscr{B} \in A/R_2 \wedge x \in \mathscr{B} \wedge y \in \mathscr{B} && \text{(子集关系定义)} \\
\Longrightarrow\ & \exists \mathscr{B}(B \in A/R_2 \wedge x \in \mathscr{B} \wedge y \in \mathscr{B}) && \text{(}\exists\text{引入)} \\
\Longleftrightarrow\ & \langle x, y\rangle \in R_2 && \text{(商集定义)}
\end{aligned}
$$

充分性：

只需证明 $\forall \mathscr{A} \forall x \forall y(\mathscr{A} \in A/R_1 \wedge x \in \mathscr{A} \wedge y \in \mathscr{A} \rightarrow \exists \mathscr{B}(\mathscr{B} \in A/R_2 \wedge x \in \mathscr{B} \wedge y \in \mathscr{B}))$。

$$
\begin{aligned}
& \forall \mathscr{A}, x, y \\
& \mathscr{A} \in A/R_1 \wedge x \in \mathscr{A} \wedge y \in \mathscr{A} \\
\Longleftrightarrow\ & \langle x, y\rangle \in R_1 && \text{(商集定义)} \\
\Longleftrightarrow\ & \langle x, y\rangle \in R_1 \wedge R_1 \subseteq R_2 && \text{(前提)} \\
\Longrightarrow\ & \langle x, y\rangle \in R_2 && \text{(子集关系定义)} \\
\Longleftrightarrow\ & \exists \mathscr{B}(\mathscr{B} \in A/R_2 \wedge x \in \mathscr{B} \wedge y \in \mathscr{B}) && \text{(商集定义)}
\end{aligned}
$$

□

2.41

证明: 先证：R_3 是自反的。

$$\begin{aligned}
&\forall x, y\\
&\langle x,y\rangle \in A\times B\\
\iff\ & x\in A \land y\in B && (\text{卡氏积定义})\\
\implies\ & \langle x,x\rangle \in R_1 \land \langle y,y\rangle \in R_2 && (R_1, R_2\ \text{是自反的})\\
\iff\ & \langle\langle x,y\rangle,\langle x,y\rangle\rangle \in R_3 && (R_3\ \text{定义})
\end{aligned}$$

再证：R_3 是对称的。

$$\begin{aligned}
&\forall x_1, x_2, y_1, y_2\\
&\langle\langle x_1,y_1\rangle,\langle x_2,y_2\rangle\rangle \in R_3\\
\iff\ & \langle x_1,x_2\rangle \in R_1 \land \langle y_1,y_2\rangle \in R_2 && (R_3\ \text{定义})\\
\implies\ & \langle x_2,x_1\rangle \in R_1 \land \langle y_2,y_1\rangle \in R_2 && (R_1, R_2\ \text{是对称的})\\
\iff\ & \langle\langle x_2,y_2\rangle,\langle x_1,y_1\rangle\rangle \in R_3 && (R_3\ \text{定义})
\end{aligned}$$

最后证：R_3 是传递的。

$$\begin{aligned}
&\forall x_1, x_2, x_3, y_1, y_2, y_3\\
&\langle\langle x_1,y_1\rangle,\langle x_2,y_2\rangle\rangle \in R_3 \land \langle\langle x_2,y_2\rangle,\langle x_3,y_3\rangle\rangle \in R_3\\
\iff\ & \langle x_1,x_2\rangle \in R_1 \land \langle y_1,y_2\rangle \in R_2 \land \langle x_2,x_3\rangle \in R_1 \land \langle y_2,y_3\rangle \in R_2 && (R_3\ \text{定义})\\
\iff\ & \langle x_1,x_2\rangle \in R_1 \land \langle x_2,x_3\rangle \in R_1 \land \langle y_1,y_2\rangle \in R_2 \land \langle y_2,y_3\rangle \in R_2 && (\text{命题逻辑交换律})\\
\implies\ & \langle x_1,x_3\rangle \in R_1 \land \langle y_1,y_3\rangle \in R_2 && (R_1, R_2\ \text{是传递的})\\
\iff\ & \langle\langle x_1,y_1\rangle,\langle x_3,y_3\rangle\rangle \in R_3 && (R_3\ \text{定义})
\end{aligned}$$

故得，R_3 是等价关系。 □

2.42 商集为二元集说明该关系对应的划分有两个划分块。这样的划分有 $\left\{{4 \atop 2}\right\} = 2^3 - 1 = 7$ 个。找出对应的等价关系：

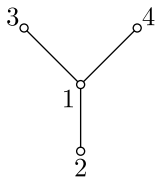
$R_1 = \{\langle b,c\rangle, \langle b,d\rangle, \langle c,b\rangle, \langle c,d\rangle, \langle d,b\rangle, \langle d,c\rangle\} \cup I_A$；
$R_2 = \{\langle a,c\rangle, \langle a,d\rangle, \langle c,a\rangle, \langle c,d\rangle, \langle d,a\rangle, \langle d,c\rangle\} \cup I_A$；
$R_3 = \{\langle a,b\rangle, \langle a,d\rangle, \langle b,a\rangle, \langle b,d\rangle, \langle d,a\rangle, \langle d,b\rangle\} \cup I_A$；
$R_4 = \{\langle a,b\rangle, \langle a,c\rangle, \langle b,a\rangle, \langle b,c\rangle, \langle c,a\rangle, \langle c,b\rangle\} \cup I_A$；
$R_5 = \{\langle a,b\rangle, \langle b,a\rangle, \langle c,d\rangle, \langle d,c\rangle\} \cup I_A$；
$R_6 = \{\langle a,c\rangle, \langle c,a\rangle, \langle b,d\rangle, \langle d,b\rangle\} \cup I_A$；
$R_7 = \{\langle a,d\rangle, \langle d,a\rangle, \langle b,c\rangle, \langle c,b\rangle\} \cup I_A$。

2.43

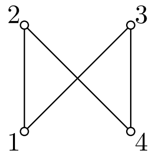
$$\begin{aligned}
\begin{Bmatrix}5\\1\end{Bmatrix} + \begin{Bmatrix}5\\2\end{Bmatrix} + \begin{Bmatrix}5\\3\end{Bmatrix} + \begin{Bmatrix}5\\4\end{Bmatrix} + \begin{Bmatrix}5\\5\end{Bmatrix} &= 1 + (2^4 - 1) + \left(3\begin{Bmatrix}4\\3\end{Bmatrix} + \begin{Bmatrix}4\\2\end{Bmatrix}\right) + C_5^2 + 1\\
&= 1 + (2^4 - 1) + (3 * C_4^2 + 2^3 - 1) + C_5^2 + 1\\
&= 1 + 2^4 - 1 + 3 * 6 + 8 - 1 + 10 + 1\\
&= 52
\end{aligned}$$

2.44

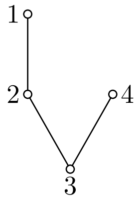
(1)



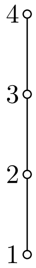
R_1



R_2



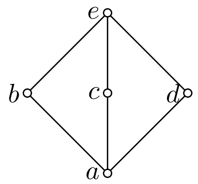
R_3



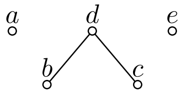
R_4

(2) R_4 是全序关系。

2.45



$\preccurlyeq_1$



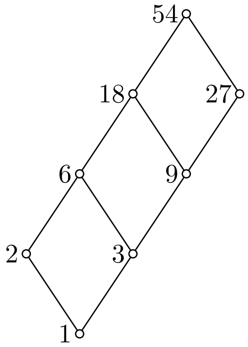
$\preccurlyeq_2$

(1) 对于 $\langle A, \preccurlyeq_1\rangle$，$e$ 是最大元，也是唯一极大元。a 是最小元，也是唯一的极小元。

(2) 对于 $\langle A, \preccurlyeq_2\rangle$，不存在最大元和最小元。$a, d, e$ 是极大元，a, b, c, e 是极小元。

2.46 B 的上界集合为：$\{k * [1, 2, \ldots, 10] \mid k \in \mathbb{N}^+\}$，上确界为 $[1, 2, \ldots, 10] = 2520$。1 是 B 唯一的下界，也是它的下确界。

2.47



$\preccurlyeq$

A 中有四条最长链：

$B_1 = 1, 2, 6, 18, 54$；

$B_2 = 1, 3, 9, 27, 54$；

$B_3 = 1, 3, 6, 18, 54$；

$B_4 = 1, 3, 9, 18, 54$。

由教材定理 2.31(2) 得，A 中元素至少可以划分成 5 个不相交的反链。

由划分定义与反链定义可知，A 中元素至多可以划分成 8 个不相交的反链。

2.48

(1)

证明：先证：$R \upharpoonright B$ 是反自反的。

$\forall x$

$x \in B$

$\Longrightarrow x \in A$ $(B \subseteq A)$

$\Longrightarrow \langle x,x \rangle \notin R$ (R是反自反的)

$\Longleftrightarrow \neg\langle x,x \rangle \in R$ ($\notin$ 定义)

$\Longrightarrow \neg\langle x,x \rangle \in R \vee \neg\langle x,x \rangle \in B \times B$ (命题逻辑附加律)

$\Longleftrightarrow \neg(\langle x,x \rangle \in R \wedge \langle x,x \rangle \in B \times B)$ (命题逻辑德·摩根律)

$\Longleftrightarrow \neg(\langle x,x \rangle \in R \cap B \times B)$ (集合交定义)

$\Longleftrightarrow \neg(\langle x,x \rangle \in R \upharpoonright B)$ ($R \upharpoonright B$ 定义)

$\Longleftrightarrow \langle x,x \rangle \notin R \upharpoonright B$ ($\notin$ 定义)

再证：$R \upharpoonright B$ 是传递的。

$\forall x,y,z$

$\langle x,y \rangle \in R \upharpoonright B \wedge \langle y,z \rangle \in R \upharpoonright B$

$\Longleftrightarrow \langle x,y \rangle \in R \cap B \times B \wedge \langle y,z \rangle \in R \cap B \times B$ ($R \upharpoonright B$ 定义)

$\Longleftrightarrow \langle x,y \rangle \in R \wedge \langle x,y \rangle \in B \times B \wedge$

$\langle y,z \rangle \in R \wedge \langle y,z \rangle \in B \times B$ (集合交定义)

$\Longleftrightarrow \langle x,y \rangle \in R \wedge x \in B \wedge y \in B \wedge$

$\langle y,z \rangle \in R \wedge y \in B \wedge z \in B$ (卡氏积定义)

$\Longleftrightarrow \langle x,y \rangle \in R \wedge \langle y,z \rangle \in R \wedge x \in B \wedge y \in B \wedge z \in B$ (命题逻辑交换律、幂等律)

$\Longrightarrow \langle x,z \rangle \in R \wedge x \in B \wedge y \in B \wedge z \in B$ (R 是传递的)

$\Longrightarrow \langle x,z \rangle \in R \wedge x \in B \wedge z \in B$ (命题逻辑化简律)

$\Longleftrightarrow \langle x,z \rangle \in R \wedge \langle x,z \rangle \in B \times B$ (卡氏积定义)

$\Longleftrightarrow \langle x,z \rangle \in R \upharpoonright B$ ($R \upharpoonright B$ 定义)

综上所述，可知 $R \upharpoonright B$ 是拟序关系。 □

(2)

证明：先证：$R \upharpoonright B$ 是自反的。

$\forall x$

$x \in B$

$\Longleftrightarrow x \in B \wedge x \in B$ (命题逻辑幂等律)

$\Longrightarrow x \in A \wedge x \in B$ $(B \subseteq A)$

$\Longrightarrow \langle x,x \rangle \in R$ (R是自反的)

$\Longleftrightarrow \langle x,x \rangle \in R \wedge \langle x,x \rangle \in B \times B$ (卡氏积定义)

$\Longleftrightarrow \langle x,x \rangle \in R \cap B \times B$ (集合交定义)

$\Longleftrightarrow \langle x,x \rangle \in R \upharpoonright B$ ($R \upharpoonright B$ 定义)

再证：$R \upharpoonright B$ 是反对称的。

$\forall x,y$

$$
\begin{aligned}
& \langle x,y\rangle \in R\upharpoonright B \wedge \langle y,x\rangle \in R\upharpoonright B \\
\Longleftrightarrow\ & \langle x,y\rangle \in R\cap B\times B \wedge \langle y,x\rangle \in R\cap B\times B && (R\upharpoonright B\ \text{定义}) \\
\Longleftrightarrow\ & \langle x,y\rangle \in R \wedge \langle x,y\rangle \in B\times B \wedge \langle y,x\rangle \in R \wedge \langle y,x\rangle \in B\times B && (\text{集合交定义}) \\
\Longleftrightarrow\ & \langle x,y\rangle \in R \wedge x\in B \wedge y\in B \wedge \langle y,x\rangle \in R \wedge y\in B \wedge x\in B && (\text{卡氏积定义}) \\
\Longleftrightarrow\ & \langle x,y\rangle \in R \wedge \langle y,x\rangle \in R && (\text{命题逻辑化简律}) \\
\Longrightarrow\ & x=y && (R\ \text{是反对称的})
\end{aligned}
$$

最后证：$R\upharpoonright B$ 是传递的。(证明同 (1)，略)

综上所述，可知 $R\upharpoonright B$ 是偏序关系。 □

(3)

证明: 由 (2) 知，$R\upharpoonright B$ 是偏序关系。现只需证任意 $x,y\in B$ 在 $R\upharpoonright B$ 下皆可比。

$$
\begin{aligned}
& \forall x,y \\
& x\in B \wedge y\in B \\
\Longleftrightarrow\ & x\in B \wedge y\in B \wedge x\in B \wedge y\in B && (\text{命题逻辑幂等律}) \\
\Longrightarrow\ & x\in A \wedge y\in A \wedge x\in B \wedge y\in B && (B\subseteq A) \\
\Longrightarrow\ & (\langle x,y\rangle \in R \vee \langle y,x\rangle \in R) \wedge x\in B \wedge y\in B && (R\ \text{是全序关系}) \\
\Longleftrightarrow\ & (\langle x,y\rangle \in R \wedge x\in B \wedge y\in B) \vee \\
& (\langle y,x\rangle \in R \wedge y\in B \wedge x\in B) && (\text{命题逻辑分配律、交换律}) \\
\Longleftrightarrow\ & \langle x,y\rangle \in R\upharpoonright B \vee \langle y,x\rangle \in R\upharpoonright B && (R\upharpoonright B\ \text{定义})
\end{aligned}
$$

故有，$R\upharpoonright B$ 是全序关系。 □

(4)

证明: 由 (3) 知，$R\upharpoonright B$ 是全序关系。现只需证明任意 $C\subseteq B$ 在 $R\upharpoonright B$ 下皆有最小元。

对任意 $C\subseteq B$，由 $B\subseteq A$ 和 $\subseteq$ 的传递性可知，$C\subseteq A$。由 R 是 A 上的是良序关系知，$\exists y(y\in C\wedge\forall x(x\in C\wedge\langle y,x\rangle\in R))$。由于 $C\subseteq B$，故对前式中的 x,y 有 $x\in B\wedge y\in B$。于是有 $\langle y,x\rangle\in R\upharpoonright B$。故得，$R\upharpoonright B$ 是 B 上的良序关系。 □

2.49

证明: 先证：R 是反自反的。

$$
\begin{aligned}
& \forall x,y \\
& \langle x,y\rangle \in A\times B \\
\Longleftrightarrow\ & x\in A \wedge y\in B && (\text{卡氏积定义}) \\
\Longrightarrow\ & \neg\langle y,y\rangle \in R_2 \wedge \neg\langle x,x\rangle \in R_1 && (R_1,R_2\ \text{是反自反的}) \\
\Longrightarrow\ & \neg\langle y,y\rangle \in R_2 \wedge (\neg\langle x,x\rangle \in R_1 \vee y=y) && (\text{命题逻辑附加律}) \\
\Longleftrightarrow\ & \neg\langle y,y\rangle \in R_2 \wedge \neg(\langle x,x\rangle \in R_1 \wedge y=y) && (\text{命题逻辑德·摩根律}) \\
\Longleftrightarrow\ & \neg(\langle y,y\rangle \in R_2 \vee (\langle x,x\rangle \in R_1 \wedge y=y)) && (\text{命题逻辑德·摩根律}) \\
\Longleftrightarrow\ & \neg(\langle\langle x,y\rangle,\langle x,y\rangle\rangle \in R) && (R\ \text{定义}) \\
\Longleftrightarrow\ & \langle\langle x,y\rangle,\langle x,y\rangle\rangle \notin R && (\notin\ \text{定义})
\end{aligned}
$$

再证：R 是传递的。

$$\forall x_1,x_2,x_3,y_1,y_2,y_3$$

$$
\begin{aligned}
&\langle\langle x_1,y_1\rangle,\langle x_2,y_2\rangle\rangle\in R\wedge\langle\langle x_2,y_2\rangle,\langle x_3,y_3\rangle\rangle\in R\\
\iff&(\langle y_1,y_2\rangle\in R_2\vee(\langle x_1,x_2\rangle\in R_1\wedge y_1=y_2))\wedge\\
&(\langle y_2,y_3\rangle\in R_2\vee(\langle x_2,x_3\rangle\in R_1\wedge y_2=y_3)) && (R\text{ 定义})\\
\iff&(\langle y_1,y_2\rangle\in R_2\wedge\langle y_2,y_3\rangle\in R_2)\vee\\
&(\langle y_1,y_2\rangle\in R_2\wedge\langle x_2,x_3\rangle\in R_1\wedge y_2=y_3)\vee\\
&(\langle x_1,x_2\rangle\in R_1\wedge y_1=y_2\wedge\langle y_2,y_3\rangle\in R_2)\vee\\
&(\langle x_1,x_2\rangle\in R_1\wedge y_1=y_2\wedge\langle x_2,x_3\rangle\in R_1\wedge y_2=y_3) && (\text{命题逻辑分配律})
\end{aligned}
$$

分别讨论上述 4 种情况。

对第 1 种情况，直接由 R_2 的传递性得 $\langle y_1,y_3\rangle\in R_2$。

对第 2 种情况，由 $\langle y_1,y_2\rangle\in R_2$ 和 $y_2=y_3$ 可得 $\langle y_1,y_3\rangle\in R_2$。

对第 3 种情况，由 $\langle y_2,y_3\rangle\in R_2$ 和 $y_1=y_2$ 可得 $\langle y_1,y_3\rangle\in R_2$。

对第 4 种情况，由 R_1 的传递性和 $=$ 的传递性可得 $\langle x_1,x_3\rangle\in R_1\wedge y_1=y_3$。

可见，由以上 4 种情况都可推出 $\langle\langle x_1,y_1\rangle,\langle x_3,y_3\rangle\rangle\in R$。即，$R$ 的传递性成立。

综上所述，有 R 的拟序关系。 □

2.50

证明: 先证：R 是自反的。

$$
\begin{aligned}
&\forall x,y\\
&\langle x,y\rangle\in A\times B\\
\iff&x\in A\wedge y\in B && (\text{卡氏积定义})\\
\implies&\langle x,x\rangle\in R_1\wedge\langle y,y\rangle\in R_2 && (R_1,R_2\text{ 是自反的})\\
\iff&\langle\langle x,y\rangle,\langle x,y\rangle\rangle\in R && (R\text{ 定义})
\end{aligned}
$$

再证：R 是反对称的。

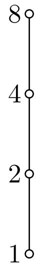
$$
\begin{aligned}
&\forall x_1,x_2,y_1,y_2\\
&\langle\langle x_1,y_1\rangle,\langle x_2,y_2\rangle\rangle\in R\wedge\langle\langle x_2,y_2\rangle,\langle x_1,y_1\rangle\rangle\in R\\
\iff&\langle x_1,x_2\rangle\in R_1\wedge\langle y_1,y_2\rangle\in R_2\wedge\langle x_2,x_1\rangle\in R_1\wedge\langle y_2,y_1\rangle\in R_2 && (R\text{ 定义})\\
\iff&\langle x_1,x_2\rangle\in R_1\wedge\langle x_2,x_1\rangle\in R_1\wedge\langle y_1,y_2\rangle\in R_2\wedge\langle y_2,y_1\rangle\in R_2 && (\text{命题逻辑交换律})\\
\implies&x_1=x_2\wedge y_1=y_2 && (R_1,R_2\text{ 是反对称的})\\
\iff&\langle x_1,y_1\rangle=\langle x_2,y_2\rangle && (\text{教材定理 2.1})\\
\iff&\langle\langle x_1,y_1\rangle,\langle x_2,y_2\rangle\rangle=\langle\langle x_2,y_2\rangle,\langle x_1,y_1\rangle\rangle && (\text{教材定理 2.1})
\end{aligned}
$$

最后证：R 是传递的。

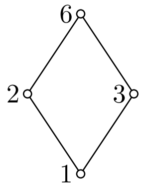
$$
\begin{aligned}
&\forall x_1,x_2,x_3,y_1,y_2,x_3\\
&\langle\langle x_1,y_1\rangle,\langle x_2,y_2\rangle\rangle\in R\wedge\langle\langle x_2,y_2\rangle,\langle x_3,y_3\rangle\rangle\in R\\
\iff&\langle x_1,x_2\rangle\in R_1\wedge\langle y_1,y_2\rangle\in R_2\wedge\langle x_2,x_3\rangle\in R_1\wedge\langle y_2,y_3\rangle\in R_2 && (R\text{ 定义})\\
\iff&\langle x_1,x_2\rangle\in R_1\wedge\langle x_2,x_3\rangle\in R_1\wedge\langle y_1,y_2\rangle\in R_2\wedge\langle y_2,y_3\rangle\in R_2 && (\text{命题逻辑交换律})\\
\implies&\langle x_1,x_3\rangle\in R_1\wedge\langle y_1,y_3\rangle\in R_2 && (R_1,R_2\text{ 是传递的})\\
\iff&\langle\langle x_1,y_1\rangle,\langle x_3,y_3\rangle\rangle\in R && (R\text{ 定义})
\end{aligned}
$$

故得，R 是偏序关系。 □

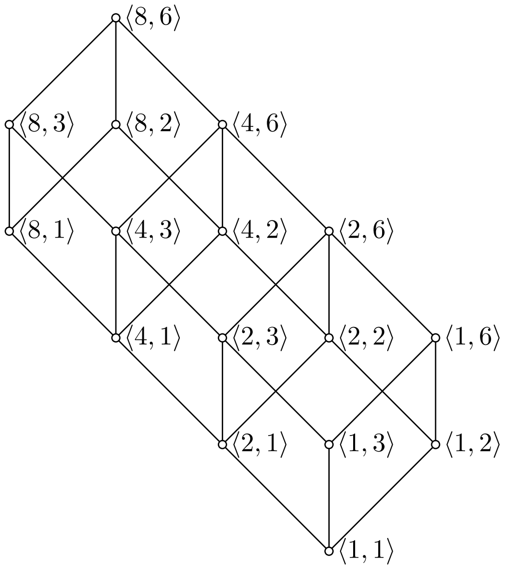
2.51



R_1



R_2



R

2.52 19 个。

2.53

证明: 由习题 2.40 结论知，$\forall x, y \in X(x\text{是}y\text{的加细} \Leftrightarrow R_x \subseteq R_y)$，其中 R_x 和 R_y 分别为 x 和 y 对应的等价关系。令 R_X 为 A 上所有等价关系的集合。由习题 2.40 结论、教材定理 2.28 和子集关系的自反性、反对称性和传递性即证原题。 □

第三章　函数

3.1　$R_2, R_3, R_6, R_7 \in A \mathrel{\ooalign{\hfil$\mapstochar\mkern5mu$\hfil\cr$\to$\cr}} B$，其中 $R_2, R_6 \in A \to B$。

3.2

结论 1：$f \cap g$ 仍是函数。

证明： 由 $f, g \in A \to B$，得：

$$\begin{aligned}
&\forall x, y, z \\
&\langle x, y\rangle \in f \cap g \wedge \langle x, z\rangle \in f \cap g \\
\iff &\langle x, y\rangle \in f \wedge \langle x, y\rangle \in g \wedge \langle x, z\rangle \in f \wedge \langle x, z\rangle \in g && \text{(集合交定义)} \\
\implies &\langle x, y\rangle \in f \wedge \langle x, z\rangle \in f && \text{(命题逻辑化简律)} \\
\implies &y = z && \text{(f 是函数)}
\end{aligned}$$

也即，$f \cap g$ 符合函数的定义，是一个函数。 □

结论 2：$f \cap g \in A \to B$ 当且仅当 $f = g$。

证明： 充分性显然。下面证必要性。

若不然，就有 $\langle x, y\rangle \in f \wedge \langle x, y\rangle \notin g$ 或 $\langle x, y\rangle \notin f \wedge \langle x, y\rangle \in g$。由对称性，不妨设 $\langle x, y\rangle \in f \wedge \langle x, y\rangle \notin g$。

这时，将有 $x \notin \operatorname{dom}(f \cap g)$ (若不然，假设存在 z，使 $\langle x, z\rangle \in f \cap g$，这时由 $\langle x, z\rangle \in g$ 和 $\langle x, y\rangle \notin g$ 可知 $z \neq y$。但 $\langle x, y\rangle \in f$ 且 $\langle x, z\rangle \in f \cap g \subseteq f$。这就使 $y \neq z$ 且 $\langle x, y\rangle \in f \wedge \langle x, z\rangle \in f$，与 f 是函数矛盾)，从而与 $f \cap g$ 是全函数矛盾。

这就证明了必要性。 □

结论 3：$f \cup g$是函数 $\Leftrightarrow f \cup g \in A \to B \Leftrightarrow f = g$。

先证：$f \cup g$是函数 $\Leftrightarrow f \cup g \in A \to B$。

证明： 由全函数定义即得充分性，即：$f \cup g \in A \to B \Rightarrow f \cup g$是函数。

再证必要性。

若 $f \cup g$ 是函数，则：

$$\begin{aligned}
\operatorname{dom}(f \cup g) &= \operatorname{dom} f \cup \operatorname{dom} g && \text{(教材定理 2.3(1))} \\
&= A \cup A && (f, g \in A \to B) \\
&= A && \text{(幂等律)}
\end{aligned}$$

由全函数定义有：$f \cup g \in A \to B$。

故有：$f \cup g$是函数 $\Rightarrow f \cup g \in A \to B$。

综合得：$f \cup g$是函数 $\Leftrightarrow f \cup g \in A \to B$。 □

再证：$f \cup g \in A \to B \Leftrightarrow f = g$。

证明: 充分性显然。

下面证必要性。

若 $f \neq g$，就有 $\langle x,y\rangle \in f \wedge \langle x,y\rangle \notin g$ 或 $\langle x,y\rangle \notin f \wedge \langle x,y\rangle \in g$。由对称性，不妨设 $\langle x,y\rangle \in f \wedge \langle x,y\rangle \notin g$。

由 g 是全函数知，存在 z，使得 $\langle x,z\rangle \in g$。因为 $\langle x,y\rangle \notin g$，所以 $z \neq y$。从而有：$\langle x,y\rangle \in (f \cup g) \wedge \langle x,z\rangle \in (f \cup g)$，且 $z \neq y$。这与 $f \cup g$ 是函数矛盾。

这就证明了必要性。 □

3.3 (1), (2), (6), (10) 是单射。(1), (4), (5), (6), (9), (10) 是满射。(1), (6), (10) 是双射。

3.4 令 $f = \{\langle S, F\rangle \mid \langle S, F\rangle \in \mathscr{A} \times \mathscr{B} \wedge \forall x(x \in A \to (x \in S \leftrightarrow F(x) = 1))\}$。则 f 是 $\mathscr{A}$ 到 $\mathscr{B}$ 的双射，f^{-1} 是 $\mathscr{B}$ 到 $\mathscr{A}$ 的双射。

3.5 先证一个引理。

引理 3.1 $A \to B = \varnothing$ 当且仅当 $A \neq \varnothing \wedge B = \varnothing$。

证明: 由全函数定义即得充分性。

下面证必要性。

若不然，则有 $A = \varnothing \vee B \neq \varnothing$。

分别讨论 $A = \varnothing$ 和 $B \neq \varnothing$ 两种情形。

当 $A = \varnothing$ 时，有 $\varnothing \in A \to B$。即 $A \to B \neq \varnothing$。

当 $B \neq \varnothing$ 时，则存在某个元素 $a \in B$，令 $f = \{\langle x, a\rangle \mid x \in A\}$。这时无论 A 是否为空(当 A 为空时，f 是空函数 $\varnothing$，仍是 A 到 B 的全函数)，皆有 $f \in A \to B$。$A \to B$ 仍然非空。

也即：$A = \varnothing \vee B \neq \varnothing \Rightarrow A \to B \neq \varnothing$。这与前提 $A \to B = \varnothing$ 矛盾。

综上所述，有：$A \to B = \varnothing \Leftrightarrow A \neq \varnothing \wedge B = \varnothing$ □

再证原题。

证明: 由引理 3.1 可知，若 $A \to B = B \to A = \varnothing$，则有：$A \neq \varnothing \wedge B = \varnothing \wedge B \neq \varnothing \wedge A = \varnothing$。矛盾。

故有 $A \to B = B \to A \Rightarrow A \to B \neq \varnothing \wedge B \to A \neq \varnothing$。

故而存在某个 $f \in A \to B$。由 $A \to B = B \to A$ 知，$f \in B \to A$。

于是有：

$$\begin{aligned} A &= \operatorname{dom} f && (f \in A \to B) \\ &= B && (f \in B \to A) \end{aligned}$$

□

3.6

证明:

$$\begin{aligned} &\forall f \\ &f \in C \to A \\ \Longleftrightarrow\ &\forall x \forall y \forall z(x \in \operatorname{dom} f \wedge y \in \operatorname{ran} f \wedge z \in \operatorname{ran} f \wedge xfy \wedge xfz \to y = z) \\ &\wedge \operatorname{dom} f = C \wedge \operatorname{ran} f \subseteq A && \text{(全函数定义)} \\ \Longrightarrow\ &\forall x \forall y \forall z(x \in \operatorname{dom} f \wedge y \in \operatorname{ran} f \wedge z \in \operatorname{ran} f \wedge xfy \wedge xfz \to y = z) \\ &\wedge \operatorname{dom} f = C \wedge \operatorname{ran} f \subseteq B && (A \subseteq B\text{ 、子集关系传递性}) \\ \Longleftrightarrow\ &f \in C \to B && \text{(全函数定义)} \end{aligned}$$

□

3.7 先证一个引理(即为本章第 10 题)。

引理 3.2 设 $f, g \in A \mathrel{+\!\!\!\!\rightarrow} B$，已知 $f \subseteq g$ 且 $\operatorname{dom} g \subseteq \operatorname{dom} f$，则 $f = g$。

证明: 由题设知 $f \subseteq g$，现只需证：$g \subseteq f$。

$$\begin{aligned}
&\forall x, y \\
&\langle x, y\rangle \in g \\
\Longrightarrow\ & x \in \operatorname{dom} g && \text{(dom定义)} \\
\Longrightarrow\ & x \in \operatorname{dom} f && (\operatorname{dom} g \subseteq \operatorname{dom} f) \\
\Longleftrightarrow\ & \exists z(\langle x, z\rangle \in f) && \text{(dom定义)} \\
\Longleftrightarrow\ & \exists z(\langle x, z\rangle \in f \wedge \langle x, z\rangle \in f) && \text{(命题逻辑幂等律)} \\
\Longrightarrow\ & \exists z(\langle x, z\rangle \in f \wedge \langle x, z\rangle \in g) && (f \subseteq g) \\
\Longrightarrow\ & \exists z(\langle x, z\rangle \in f \wedge z = y) && (g\ \text{是函数、}\langle x, y\rangle \in g) \\
\Longrightarrow\ & \langle x, y\rangle \in f && \text{(外延原则)}
\end{aligned}$$

□

由引理 3.2 即证原题。

3.8 由引理 3.2 立即得证。

3.9 令 $A = \mathbb{N}, f : \mathbb{N} \to \mathbb{N}, f(x) = x + 1, g : \mathbb{N} \to \mathbb{N}, g(x) = \lfloor x/2 \rfloor$，则：由加法性质知 f 是单射的，但 f 不是满射的(因为 $0 \in \mathbb{N}$，但 $0 \notin \operatorname{ran} f$)。对任意 $k \in \mathbb{N}$，有 $\langle 2k, k\rangle \in g$，故 g 是满射的，但对任意 $k \in \mathbb{N}$，有 $\langle 2k, k\rangle \in g \wedge \langle 2k + 1, k\rangle \in g \wedge 2k \neq 2k + 1$，故而 g 不是单射的。

3.10 即为引理 3.2。

3.11

证明: 首先证明一个结论。

结论 1：$\forall y(y \in \operatorname{dom} g \to g(y) \neq \varnothing)$。

证明:

$$\begin{aligned}
&\forall y \\
&y \in \operatorname{dom} g \\
\Longleftrightarrow\ & y \in B && (\operatorname{dom} g = B) \\
\Longrightarrow\ & \exists x(x \in A \wedge \langle x, y\rangle \in f) && (f\ \text{是满射}) \\
\Longleftrightarrow\ & \exists x(x \in g(y)) && (g\ \text{定义}) \\
\Longleftrightarrow\ & g(y) \neq \varnothing && (\varnothing\ \text{定义})
\end{aligned}$$

□

下面证明 g 是单射的。

$$\begin{aligned}
&\forall y_1, y_2 \in B, s \in \mathcal{P}(A) \\
&\langle y_1, s\rangle \in g \wedge \langle y_2, s\rangle \in g \\
\Longrightarrow\ & \forall x(x \in s \to \langle x, y_1\rangle \in f) \wedge \forall x(x \in s \to \langle x, y_2\rangle \in f) \wedge s = g(y_1) && (g\ \text{定义}) \\
\Longleftrightarrow\ & \forall x((x \in s \to \langle x, y_1\rangle \in f) \wedge (x \in s \to \langle x, y_2\rangle \in f)) \wedge s = g(y_1) && \text{(量词分配等值式)}
\end{aligned}$$

$$\Longrightarrow \forall x((x \in s \to \langle x, y_1\rangle \in f) \land (x \in s \to \langle x, y_2\rangle \in f)) \land s \neq \varnothing \qquad \text{(结论 1)}$$

$$\Longleftrightarrow \forall x((x \in s \to \langle x, y_1\rangle \in f) \land (x \in s \to \langle x, y_2\rangle \in f)) \land \exists x(x \in s) \qquad (\varnothing\ \text{定义})$$

$$\Longleftrightarrow \forall x((\neg x \in s \lor \langle x, y_1\rangle \in f) \land (\neg x \in s \lor \langle x, y_2\rangle \in f)) \land \exists x(x \in s) \qquad \text{(蕴涵等值式)}$$

$$\Longleftrightarrow \forall x(\neg x \in s \lor (\langle x, y_1\rangle \in f \land \langle x, y_2\rangle \in f)) \land \exists x(x \in s) \qquad \text{(命题逻辑分配律)}$$

$$\Longleftrightarrow \forall x(x \in s \to (\langle x, y_1\rangle \in f \land \langle x, y_2\rangle \in f)) \land \exists x(x \in s) \qquad \text{(蕴涵等值式)}$$

$$\Longrightarrow (\exists x(x \in s) \to \exists x(\langle x, y_1\rangle \in f \land \langle x, y_2\rangle \in f)) \land \exists x(x \in s) \qquad \text{(一阶谓词推理定律)}$$

$$\Longrightarrow \exists x(\langle x, y_1\rangle \in f \land \langle x, y_2\rangle \in f) \qquad \text{(假言推理)}$$

$$\Longrightarrow y_1 = y_2 \qquad (f\ \text{是函数})$$

可见，g 是单根的。故而 g 是单射的。 □

3.12

证明: 对于任意 $x \in \mathbb{R}$，都有 $\langle\langle x, 0\rangle, x\rangle \in f$ 和 $\langle\langle x, 1\rangle, x\rangle \in g$，因此 f, g 都是满射的。

对于任意 $x \in \mathbb{R}$，都有 $\langle\langle x, 0\rangle, x\rangle \in f \land \langle\langle x-1, 1\rangle, x\rangle \in f \land x \neq x-1$ 和 $\langle\langle x, 0\rangle, 0\rangle \in g \land \langle\langle x+1, 0\rangle, 0\rangle \in g \land x \neq x-1$，因此 f, g 都不是单射的。 □

3.13

证明: 令 $f : \mathscr{E} \to \mathscr{F}, f(x) = A/x$。下面证明 $f(x)$ 是双射。

先证 f 是单射。

对 A 上的任意等价关系 $R, S \in \mathscr{E}$，若 $f(R) = f(S)$，则由 f 定义有 $A/R = A/S$。于是:

$$\forall x, y$$

$$\langle x, y\rangle \in R$$

$$\Longleftrightarrow \exists B(x \in B \land y \in B \land B \in A/R) \qquad \text{(商集定义)}$$

$$\Longleftrightarrow \exists B(x \in B \land y \in B \land B \in A/S) \qquad (A/R = A/S)$$

$$\Longleftrightarrow \langle x, y\rangle \in S \qquad \text{(商集定义)}$$

即，$f(R) = f(S) \Rightarrow R = S$，故而 f 是单射的。

再证 f 是满射。

对于A任意划分 $\mathscr{A} \in \mathscr{F}$，令 $R_{\mathscr{A}} = \{\langle x, y\rangle \mid x, y \in A \land \exists B(x \in B \land y \in B \land B \in \mathscr{A})\}$。

下面证明 $R_{\mathscr{A}} \in \mathscr{E}$[1] 且 $f(R_{\mathscr{A}}) = \mathscr{A}$。

先证明 $R_{\mathscr{A}} \in \mathscr{E}$。

自反性:

$$\forall x$$

$$x \in A$$

$$\Longleftrightarrow x \in \cup\mathscr{A} \qquad (\mathscr{A}\ \text{是划分})$$

$$\Longleftrightarrow \exists B(x \in B \land B \in \mathscr{A}) \qquad \text{(广义并定义)}$$

$$\Longleftrightarrow \exists B(x \in B \land x \in B \land B \in \mathscr{A}) \qquad \text{(命题逻辑幂等律)}$$

$$\Longleftrightarrow \langle x, x\rangle \in R_{\mathscr{A}} \qquad (R_{\mathscr{A}}\ \text{定义})$$

对称性:

$$\forall x, y$$

$$\langle x, y\rangle \in R_{\mathscr{A}}$$

---

[1] 即为教材定理 2.28(2)。教材将“本定理证明留读者”，故在此证明。

$\Longleftrightarrow \exists B(x \in B \wedge y \in B \wedge B \in \mathscr{A})$ ($R_{\mathscr{A}}$ 定义)

$\Longleftrightarrow \exists B(y \in B \wedge x \in B \wedge B \in \mathscr{A})$ (命题逻辑交换律)

$\Longleftrightarrow \langle y, x\rangle \in R_{\mathscr{A}}$ ($R_{\mathscr{A}}$ 定义)

传递性：

$\forall x, y, z$

$\langle x, y\rangle \in R_{\mathscr{A}} \wedge \langle y, z\rangle \in R_{\mathscr{A}}$

$\Longleftrightarrow \exists B(x \in B \wedge y \in B \wedge B \in \mathscr{A}) \wedge \exists B(y \in B \wedge z \in B \wedge B \in \mathscr{A})$ ($R_{\mathscr{A}}$ 定义)

$\Longrightarrow x \in B_1 \wedge y \in B_1 \wedge B_1 \in \mathscr{A} \wedge y \in B_2 \wedge z \in B_2 \wedge B_2 \in \mathscr{A}$ ($\exists$消去)

$\Longrightarrow x \in B_1 \wedge B_1 \in \mathscr{A} \wedge z \in B_2 \wedge B_2 \in \mathscr{A} \wedge y \in B_1 \wedge y \in B_2$ (命题逻辑交换律)

$\Longrightarrow x \in B_1 \wedge B_1 \in \mathscr{A} \wedge z \in B_2 \wedge B_2 \in \mathscr{A} \wedge y \in B_1 \cap B_2$ (集合交定义)

$\Longrightarrow x \in B_1 \wedge B_1 \in \mathscr{A} \wedge z \in B_2 \wedge B_2 \in \mathscr{A} \wedge B_1 \cap B_2 \neq \varnothing$ ($\varnothing$ 定义)

$\Longrightarrow x \in B_1 \wedge B_1 \in \mathscr{A} \wedge z \in B_2 \wedge B_2 \in \mathscr{A} \wedge B_1 = B_2$ ($B_1 \cap B_2 \neq \varnothing \rightarrow B_1 = B_2$[2])

$\Longrightarrow x \in B_1 \wedge z \in B_2 \wedge B_1 \in \mathscr{A}$ (外延原则)

$\Longrightarrow \exists B(x \in B \wedge z \in B \wedge B \in \mathscr{A})$ ($\exists$引入)

$\Longleftrightarrow \langle x, z\rangle \in R_{\mathscr{A}}$ ($R_{\mathscr{A}}$ 定义)

于是有 $R_{\mathscr{A}} \in \mathscr{E}$。

由 $R_{\mathscr{A}}$ 和商集定义立即得：$f(R_{\mathscr{A}}) = \mathscr{A}$。

故而 f 是满射的。

综合得，f 是双射的。 □

3.14

证明：先证：S 是自反的。

$\forall f$

$f \in \mathscr{A}$

$\Longrightarrow \forall x(x \in [0,1] \rightarrow (f(x) - f(x)) = 0)$ ($f \in [0,1] \rightarrow \mathbb{R}$)

$\Longrightarrow \forall x(x \in [0,1] \rightarrow (f(x) - f(x)) \geq 0)$ ($\geq$ 定义)

$\Longleftrightarrow \langle f, f\rangle \in S$ (S 定义)

再证：S 是反对称的。

$\forall f, g$

$\langle f, g\rangle \in \mathscr{A} \wedge \langle g, f\rangle \in \mathscr{A}$

$\Longleftrightarrow \forall x(x \in [0,1] \rightarrow (f(x) - g(x)) \geq 0) \wedge$

$\qquad \forall x(x \in [0,1] \rightarrow (g(x) - f(x)) \geq 0)$ (S 定义)

$\Longleftrightarrow \forall x((x \in [0,1] \rightarrow (f(x) - g(x)) \geq 0) \wedge$

$\qquad (x \in [0,1] \rightarrow (g(x) - f(x)) \geq 0))$ (量词分配等值式)

$\Longleftrightarrow \forall x((\neg x \in [0,1] \vee (f(x) - g(x)) \geq 0) \wedge$

$\qquad (\neg x \in [0,1] \vee (g(x) - f(x)) \geq 0))$ (蕴涵等值式)

$\Longleftrightarrow \forall x(\neg x \in [0,1] \vee ((f(x) - g(x)) \geq 0 \wedge (g(x) - f(x)) \geq 0))$ (命题逻辑分配律)

---

[2] 这是划分定义第 (2) 项的逆否命题。由“假言易位”等值式知，它是永真命题。

$\iff \forall x(\neg x \in [0,1] \vee ((f(x)-g(x))=0))$ (等号定义)

$\iff \forall x(x \in [0,1] \to ((f(x)-g(x))=0))$ (蕴涵等值式)

$\iff f = g$ (函数相等定义)

下面证：S 是传递的。

$\forall f, g, h$

$\langle f, g\rangle \in \mathscr{A} \wedge \langle g, h\rangle \in \mathscr{A}$

$\iff \forall x(x \in [0,1] \to (f(x)-g(x)) \geq 0) \wedge$

$\quad \forall x(x \in [0,1] \to (g(x)-h(x)) \geq 0)$ (S 定义)

$\iff \forall x((x \in [0,1] \to (f(x)-g(x)) \geq 0) \wedge$

$\quad (x \in [0,1] \to (g(x)-h(x)) \geq 0))$ (量词分配等值式)

$\iff \forall x((\neg x \in [0,1] \vee (f(x)-g(x)) \geq 0) \wedge$

$\quad (\neg x \in [0,1] \vee (g(x)-h(x)) \geq 0))$ (蕴涵等值式)

$\iff \forall x(\neg x \in [0,1] \vee ((f(x)-g(x)) \geq 0 \wedge (g(x)-h(x)) \geq 0))$ (命题逻辑分配律)

$\iff \forall x(\neg x \in [0,1] \vee ((f(x)-h(x))$

$\quad = (f(x)-g(x)) + (g(x)-h(x)) \geq 0))$ (加法性质)

$\iff \forall x(x \in [0,1] \to ((f(x)-h(x)) \geq 0))$ (蕴涵等值式)

$\iff \langle f, g\rangle \in \mathscr{A}$ (S 定义)

综上所述，有 S 是偏序关系。

下面举反例说明 S 不是全序关系。

令 $f : [0,1] \to \mathbb{R}, f(x) = x$ 和 $g : [0,1] \to \mathbb{R}, g(x) = 1 - x$，则：$0, 1 \in [0,1] \wedge f(0) - g(0) < 0 \wedge g(1) - f(1) < 0$。于是有：$\langle f, g\rangle \notin S \wedge \langle g, f\rangle \notin S$。故 S 不是全序关系。 □

3.15

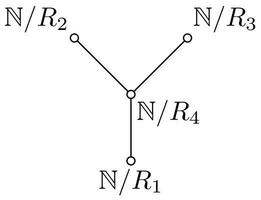
(1) $\mathbb{N}/R_1 = \{\{x\} \mid x \in \mathbb{N}\}$；

$\mathbb{N}/R_2 = \{\{2k + j \mid k \in \mathbb{N}\} \mid j \in \{0, 1\}\}$；

$\mathbb{N}/R_3 = \{\{3k + j \mid k \in \mathbb{N}\} \mid j \in \{0, 1, 2\}\}$；

$\mathbb{N}/R_4 = \{\{6k + j \mid k \in \mathbb{N}\} \mid j \in \{0, 1, 2, 3, 4, 5\}\}$。

(2)



(3) $f_1(H) = H$；

$f_2(H) = \{0\}$；

$f_3(H) = \{0, 1, 2\}$；

$f_4(H) = \{0, 2, 4\}$。

3.16 $g \circ f(x) = x^2 + 2$，既不是满射的也不是单射的。

$f \circ g(x) = x^2 + 4x + 14$，既不是满射的也不是单射的。

f 不是双射，因而没有反函数。g, h 是双射，有反函数。

$g^{-1}(x) = x - 4$; $h^{-1}(x) = \sqrt[3]{x+1}$。

3.17

结论 1：对任意非空集合 A 和 A 上的等价关系 R，自然映射 $f : A \to A/R$ 有反函数当且仅当 $R = I_A$。

证明： 充分性显然。

下面证必要性。

由反函数的定义知，f 有反函数当且仅当 f 是双射的。因此：

$$\begin{aligned}
&\forall x, y \in A \\
&\langle x, y\rangle \in R \\
\Longrightarrow\ & [x]_R = [y]_R && \text{(教材定理 2.27(2))} \\
\Longleftrightarrow\ & f(x) = f(y) && (f\ \text{定义}) \\
\Longleftrightarrow\ & x = y && (f\ \text{是双射}) \\
\Longleftrightarrow\ & \langle x, y\rangle \in I_A
\end{aligned}$$

可知 $R \subseteq I_A$。又由 R 是等价关系知，$I_A \subseteq R$。于是有 $R = I_A$。 □

结论 2：当 $R = I_A$ 时，f 有反函数 $f^{-1} : A/R \to A, f^{-1}([x]) = x$。

证明： 由教材定理 3.9、3.10 和结论 1 立即可得。 □

3.18

(1) $\operatorname{dom} f = \mathbb{R} - \{0\} = (-\infty, 0) \cup (0, +\infty)$；

$\operatorname{ran} f = \mathbb{R} - \{0\} = (-\infty, 0) \cup (0, +\infty)$；

$\operatorname{dom} g = \mathbb{R}$；

$\operatorname{ran} g = \{0\} \cup \mathbb{R}^+ = \mathbb{R} - \mathbb{R}^- = [0, +\infty)$；

$\operatorname{dom} h = \{0\} \cup \mathbb{R}^+ = \mathbb{R} - \mathbb{R}^- = [0, +\infty)$；

$\operatorname{ran} h = \{0\} \cup \mathbb{R}^+ = \mathbb{R} - \mathbb{R}^- = [0, +\infty)$。

(2) 分别令 $\operatorname{dom} f, \operatorname{dom} g, \operatorname{dom} h$ 为 f, g, h 的前域即可。

3.19

(1) $f(A_1) = \{1, 2, 3\}$; $f^{-1}(B_1) = \{0, 4, 5, 6\}$。

(2) $g(A_2) = \mathbb{N}$; $g^{-1}(B_2) = \{2k + 1 \mid k \in \mathbb{N}\} \cup \{6\}$。

(3) f 是双射的，有反函数。g 不是双射的，没有反函数。

3.20

(1)

证明： 由 $f \circ g$ 是单射的和教材定理 3.5(2) 可知，g 是单射的。由题设，g 是满射的。因而，g 是双射的。

由教材定理 3.9、3.10 和 g 是双射的可知，g^{-1} 也是双射的，而且既是 g 的左逆又是 g 的右逆。因此，$f = f \circ I_B = f \circ g \circ g^{-1}$。

因为 $f \circ g$ 和 g^{-1} 都是单射的，由教材定理 3.4(2) 得，$f = f \circ g \circ g^{-1}$ 也是单射的。 □

(2)

证明： 由 $f \circ g$ 是满射的和教材定理 3.5(1) 可知，f 是满射的。由题设，f 是单射的。因而，f 是双射的。

由教材定理 3.9、3.10 和 f 是双射的可知，f^{-1} 也是双射的，而且既是 f 的左逆又是 f 的右

逆。因此，$g = I_B \circ g = f^{-1} \circ f \circ g$。

因为 f^{-1} 和 $f \circ g$ 都是满射的，由教材定理 3.4(1) 得，$g = f^{-1} \circ f \circ g$ 也是满射的。 □

3.21 先证一个引理。

引理 3.3 对任意函数 $f, g \in A \to B$，$f = g$ 当且仅当 $\forall x(x \in A \to f(x) = g(x))$。

证明: 先证必要性。

若 $f = g$，则：

$$\begin{aligned}
&\forall x\\
&x \in A\\
\iff& \exists y(\langle x, y\rangle \in f) && (f \in A \to B)\\
\implies& \langle x, a\rangle \in f && (\exists\text{消去})\\
\iff& f(x) = a && (f(x)\ \text{定义})\\
\iff& f(x) = a \land f(x) = a && (\text{命题逻辑幂等律})\\
\iff& f(x) = a \land \langle x, a\rangle \in f && (f(x)\ \text{定义})\\
\iff& f(x) = a \land \langle x, a\rangle \in g && (f = g)\\
\iff& f(x) = a \land g(x) = a && (g(x)\ \text{定义})\\
\iff& f(x) = g(x) && (\text{等号传递性})
\end{aligned}$$

于是有：$f = g \Rightarrow \forall x(x \in A \to f(x) = g(x))$。

再证充分性。

若 $\forall x(x \in A \to f(x) = g(x))$，则：

$$\begin{aligned}
&\forall x, y\\
&\langle x, y\rangle \in f\\
\iff& f(x) = y && (f(x)\ \text{定义})\\
\iff& g(x) = y && (f(x) = g(x))\\
\iff& \langle x, y\rangle \in g && (g(x)\ \text{定义})
\end{aligned}$$

于是有：$\forall x(x \in A \to f(x) = g(x)) \Rightarrow f = g$。

综合即得原题。 □

再证原题。

证明: 先证：$f \circ h_1 = g \circ h_1$。

由教材定理 3.3 知，$\operatorname{dom}(f \circ h_1) = \operatorname{dom}(g \circ h_1) = \operatorname{dom} h_1 = A$。

由引理 3.3 知，欲证：$f \circ h_1 = g \circ h_1$，只需证：$\forall x(x \in A \to f \circ h_1(x) = g \circ h_1(x))$。

由 A 定义知，对于任意 $x \in A$，有 $x \in X \land f(x) = g(x)$。于是：

$$\begin{aligned}
&\forall x \in A,\\
&f \circ h_1(x) = f(h_1(x)) && (\text{教材定理 3.3})\\
&\qquad\qquad = f(x) && (h_1(x) = x)\\
&\qquad\qquad = g(x) && (f(x) = g(x))\\
&\qquad\qquad = g(h_1(x)) && (h_1(x) = x)\\
&\qquad\qquad = g \circ h_1(x) && (\text{教材定理 3.3})
\end{aligned}$$

从而证得原题。

下面证：$B \subseteq A$。

由引理 3.3 和 $f \circ h_2 = g \circ h_2$ 知，$\forall x(x \in B \to f \circ h_2(x) = g \circ h_2(x))$。于是：

$$\begin{aligned}
&\forall x\\
&x \in B\\
\Longrightarrow\ & f \circ h_2(x) = g \circ h_2(x) \wedge x \in X && \text{(前提)}\\
\Longleftrightarrow\ & f(h_2(x)) = g(h_2(x)) \wedge x \in X && \text{(教材定理 3.3)}\\
\Longleftrightarrow\ & f(x) = g(x) \wedge x \in X && (h_2(x) = x)\\
\Longleftrightarrow\ & x \in A && (A\ \text{定义})
\end{aligned}$$

故有：$B \subseteq A$。□

3.22 先证第一部分，即：$\forall f, g \in (X \to X)(h \circ f = h \circ g \to f = g) \Leftrightarrow h$是单射的。

证明： 先证必要性。

若 h 不是单射的，则存在 $x_1, x_2 \in X$，有 $x_1 \neq x_2 \wedge h(x_1) = h(x_2)$。

令 $f : X \to X, f(x) = x_1$， $g : X \to X, g(x) = x_2$。则 $h \circ f = h \circ g$，但 $f \neq g$。与前提 $h \circ f = h \circ g \to f = g$ 矛盾。故有：$h \circ f = h \circ g \to f = g \Rightarrow h$是单射的。

再证充分性。

若 h 是单射的，则由教材定理 3.10(1) 知，h 存在左逆。令 h' 为 h 的左逆。

对任意函数 $f, g \in (X \to X)$，若 $h \circ f = h \circ g$ 则：

$$\begin{aligned}
f &= I_X \circ f && \text{(教材定理 3.6)}\\
&= h' \circ h \circ f && (h'\ \text{是}\ h\ \text{的左逆})\\
&= h' \circ h \circ g && (h \circ f = h \circ g)\\
&= I_X \circ g && (h'\ \text{是}\ h\ \text{的左逆})\\
&= g && \text{(教材定理 3.6)}
\end{aligned}$$

综合得：对任意的 $f, g \in (X \to X)$，只要 $h \circ f = h \circ g$ 就有 $f = g$ 当且仅当 h 是单射的。□

再证第二部分，即：$\forall f, g \in (X \to X)(f \circ h = g \circ h \to f = g) \Leftrightarrow h$是满射的。

证明： 先证必要性。

若 h 不是满射的，则存在 $a \in X$，有 $\forall x(x \in X \to h(x) \neq a)$ (由此可知，$h(a) \neq a$)。

令 $f : X \to X, f(x) = x$， $g : X \to X, g(x) = \begin{cases} x & x \neq a \\ h(a) & x = a \end{cases}$。则 $f \circ h = g \circ h$，但 $f \neq g$。与前提 $f \circ h = g \circ h \to f = g$ 矛盾。故有：$f \circ h = g \circ h \to f = g \Rightarrow h$是满射的。

再证充分性。

若 h 是满射的，则由教材定理 3.10(2) 知，h 存在右逆。令 h' 为 h 的右逆。

对任意函数 $f, g \in (X \to X)$，若 $f \circ h = g \circ h$ 则：

$$\begin{aligned}
f &= f \circ I_X && \text{(教材定理 3.6)}\\
&= f \circ h \circ h' && (h'\ \text{是}\ h\ \text{的右逆})\\
&= g \circ h \circ h' && (h \circ f = h \circ g)\\
&= g \circ I_X && (h'\ \text{是}\ h\ \text{的右逆})\\
&= g && \text{(教材定理 3.6)}
\end{aligned}$$

综合得：对任意的 $f, g \in (X \to X)$，只要 $f \circ h = g \circ h$ 就有 $f = g$ 当且仅当 h 是满射的。□

3.23 先证一个引理。

引理 3.4 设 A 是一集合，则对任意 $f \in A \to A$，有 $f^n \in A \to A$ $(n \in \mathbb{N})$。

证明： 对 n 作归纳。

若 $n = 0$，则由二元关系幂运算定义知，$f^n = f^0 = I_A \in A \to A$。

设当 $n = k$ $(k \geq 0)$ 时命题成立，则当 $n = k + 1$ 时有：

$$
\begin{aligned}
f^{k+1} &= f^k \circ f && \text{(幂运算定义)} \\
&\in A \to A && \text{(教材定理 3.3)}
\end{aligned}
$$

□

再证原题。

证明： 由 I_A 定义和双射定义易知，I_A 是双射的。

由关系幂运算定义和合成运算结合律有：$f^n = f^{n-1} \circ f = f \circ f^{n-1} = I_A$。

由题设知，n 是正整数，即 $n \geq 1$。因而有 $n - 1 \geq 0$ (且为整数)，即 $(n-1) \in \mathbb{N}$。

因而由引理 3.4 知，$f^{n-1} \in A \to A$。

由 $f^{n-1} \circ f = I_A$ 是双射的和教材定理 3.5(3) 知，f 是单射的。

又由 $f \circ f^{n-1} = I_A$ 是双射的和教材定理 3.5(3) 知，f 是满射的。

综合得，f 是双射的。 □

3.24

证明： 由教材定理 2.9(3) 可知：$f^{-1}(A \cap B) \subseteq f^{-1}(A) \cap f^{-1}(B)$。

下面证明 $f^{-1}(A) \cap f^{-1}(B) \subseteq f^{-1}(A \cap B)$：

$$
\begin{aligned}
& \forall x \\
& x \in f^{-1}(A) \cap f^{-1}(B) \\
\iff & x \in f^{-1}(A) \land x \in f^{-1}(B) && \text{(集合交定义)} \\
\iff & x \in X \land f(x) \in A \land x \in X \land f(x) \in B && \text{(原象定义)} \\
\iff & x \in X \land f(x) \in A \land f(x) \in B && \text{(命题逻辑交换律、幂等律)} \\
\iff & x \in X \land f(x) \in A \cap B && \text{(集合交定义)} \\
\iff & x \in f^{-1}(A \cap B) && \text{(原象定义)}
\end{aligned}
$$

综合得，$f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$。 □

第四章　自然数

4.1

(1) 满足归纳集定义，是归纳集。

(2) $\varnothing$ 不在集合中，此集不是归纳集。

(3) 集合中最后一个元素 $\varnothing^{++++++++}$ 的后继不在集合中，此集不是归纳集。

(4) 若 $a = \varnothing$，则是归纳集。否则，$\varnothing$ 不在集合中，此集不是归纳集。

4.2

(1) $2 \cup 3 = 3$;

(2) $2 \cap 3 = 2$;

(3) $\cup 5 = 4$;

(4) $\cap 6 = 0$;

(5) $\cup \cup 7 = 5$;

4.3

证明: 用数学归纳法证明。

设 $S' = \{n \mid n \in \mathbb{N} \wedge n \neq 0 \wedge \exists m(m \in \mathbb{N} \wedge n = m^+)\}$，再设 $S = S' \cup \{0\}$。下面证明 S 是 $\mathbb{N}$ 的归纳子集。

(1) 由 S 的定义有：$\varnothing = 0 \in S$。

(2) 假设 $n \in S$ (从而由 S 定义有 $n \in \mathbb{N}$)，则由 $\mathbb{N}$ 的定义知，$n^+ \in \mathbb{N}$，又由 $n \in n \cup \{n\} = n^+$ 知，$n^+ \neq 0$。最后由 n^+ 是 n 的后继知，$\exists m(m \in \mathbb{N} \wedge n = m^+)$。因此有 $n^+ \in S' \subseteq S$。

于是，S 是 $\mathbb{N}$ 的归纳子集，因而 $S = \mathbb{N}$。而 $S' = S - \{0\}$，故有，任意非 0 自然数都是某个自然数的后继。 □

4.4

证明: 用数学归纳法证明。

设 $S = \{n \mid \forall m \in \mathbb{N}(m \in m + n^+)\}$。

(1) $0 \in S$。这是因为：$\forall m \in \mathbb{N}, m \in m \cup \{m\} = m^+ = (m+0)^+ = m + 0^+$。

(2) 设 $n \in S$，则 $\forall m \in \mathbb{N}, m \in m + n^+ \subseteq (m + n^+) \cup \{(m + n^+)\} = (m + n^+)^+ = (A_m(n^+))^+ = A_m(n^{++}) = m + (n^+)^+$。即有，$n^+ \in S$。所以，$S = \mathbb{N}$。 □

4.5

证明: 若 A 为传递集，则：

$\forall x$，

$x \in A^+$

$\iff x \in A \cup \{A\}$　(后继函数定义)

$\Longleftrightarrow x \in A \lor x \in \{A\}$ (集合并定义)

$\Longleftrightarrow x \in A \lor x = A$ ($\in$ 性质)

$\Longrightarrow x \subseteq A \lor x = A$ (教材定理 4.10)

$\Longrightarrow x \subseteq A \lor x \subseteq A$ ($x = A \Rightarrow x \subseteq A$)

$\Longleftrightarrow x \subseteq A$ (命题逻辑幂等律)

$\Longrightarrow x \subseteq A \lor x \subseteq \{A\}$ (命题逻辑附加律)

$\Longleftrightarrow x \subseteq A \cup \{A\}$ (集合并定义)

$\Longleftrightarrow x \subseteq A^+$ (后继函数定义)

由教材定理 4.10 知，A^+ 是传递集。 □

4.6

(1)

证明： 若 $\mathscr{A}$ 的每个元素都是传递集，则：

$\forall x$,

$x \in \cup\mathscr{A}$

$\Longleftrightarrow \exists y(y \in \mathscr{A} \land x \in y)$ (广义并定义)

$\Longrightarrow \exists y(y \in \mathscr{A} \land x \subseteq y)$ (y 是传递集、教材定理 4.10)

$\Longrightarrow \exists y(y \subseteq \cup\mathscr{A} \land x \subseteq y)$ (广义并性质)

$\Longrightarrow x \subseteq \cup\mathscr{A}$ (子集关系传递性)

由教材定理 4.10 知，$\cup\mathscr{A}$ 是传递集。 □

(2)

证明： 若 $\mathscr{A}$ 非空，且 $\mathscr{A}$ 的每个元素都是传递集，则：

$\forall x$,

$x \in \cap\mathscr{A}$

$\Longleftrightarrow \forall y(y \in \mathscr{A} \to x \in y)$ (广义交定义)

$\Longrightarrow \forall y(y \in \mathscr{A} \to x \subseteq y)$ (y 是传递集、教材定理 4.10)

$\Longleftrightarrow \forall y(y \in \mathscr{A} \to \forall z(z \in x \to z \in y))$ (子集关系定义)

$\Longleftrightarrow \forall y \forall z(y \in \mathscr{A} \to (z \in x \to z \in y))$ (量词辖域扩张等值式)

$\Longleftrightarrow \forall y \forall z(\neg y \in \mathscr{A} \lor (\neg z \in x \lor z \in y))$ (蕴涵等值式)

$\Longleftrightarrow \forall y \forall z(\neg z \in x \lor (\neg y \in \mathscr{A} \lor z \in y))$ (命题逻辑交换律、结合律)

$\Longleftrightarrow \forall y \forall z(z \in x \to (y \in \mathscr{A} \to z \in y))$ (蕴涵等值式)

$\Longleftrightarrow \forall z(z \in x \to \forall y(y \in \mathscr{A} \to z \in y))$ (量词辖域收缩等值式)

$\Longleftrightarrow \forall z(z \in x \to z \in \cap\mathscr{A})$ (广义交定义)

$\Longleftrightarrow x \subseteq \cap\mathscr{A}$ (子集关系定义)

由教材定理 4.10 知，$\cap\mathscr{A}$ 是传递集。 □

4.7

证明： 令 $S = \{n \mid n \in \mathbb{N} \land \exists m(m \in \mathbb{N} \land m \neq n \land h(m) = h(n))\}$。

注意到，$0 \notin S$。这是因为：若 $0 \in S$，则由集合 S 和函数 h 的定义知，存在 $m \in \mathbb{N}, m \neq 0$，

使得 $h(m) = h(0) = a$。由 $m \neq 0$ 和习题 4.3 结论(任何非 0 自然数都是某个自然数的后继)知，m 是某个自然数 n 的后继。因而 $h(m) = h(n^+) = f(h(n)) = a$，这与题设 $a \in A - \operatorname{ran} f$ 矛盾。故，$0 \notin S$。

若 $S \neq \varnothing$，则依 $\mathbb{N}$ 上的良序定理，S 有最小元 n_0。又由 S 的定义知，存在 $m_0 \in \mathbb{N}, m_0 \neq n_0$，使得 $h(m_0) = h(n_0)$。注意到，对于 m_0 而言，由于有 $n_0 \in \mathbb{N}, n_0 \neq m_0$ 和 $h(n_0) = h(m_0)$，因此有 $m_0 \in S$。

由 $m_0, n_0 \in S$ 和 $0 \notin S$ 知，$m_0 \neq 0, n_0 \neq 0$。再由习题 4.3 结论知，存在 $m_p, n_p \in \mathbb{N}$，使 $m_0 = m_p^+, n_0 = n_p^+$。从而由 h 的定义知：$f(h(m_p)) = h(m_p^+) = h(m_0) = h(n_0) = h(n_p^+) = f(h(n_p))$，由 f 是单射和 $f(h(m_p)) = f(h(n_p))$ 知，$h(m_p) = h(n_p)$。但由教材定理 4.4 和 $m_0 \neq n_0$ 知，$m_p \neq n_p$。这就表明，$n_p \in S$。但 $n_0 = n_p^+ > n_p$，这与 n_0 是 S 最小元矛盾。

因此，S 必为空集。也即，不存在 $n, m \in \mathbb{N}, n \neq m$，使得 $h(n) = h(m)$。这就证明了 h 是单射。 □

第五章　基数（势）

5.1

证明: 取 $f:\mathscr{A}\to\mathscr{B}$，且 $\forall x\in\mathscr{A}, f(x)=x-I_A$。

f 显然是函数。

$\forall R_1,R_2\in\mathscr{A}$，若 $f(R_1)=f(R_2)$，则:

$$\begin{aligned}
&(I_A\subseteq R_1)\land((R_1\cap\sim I_A)\subseteq R_1) && \text{(偏序关系性质、引理 1.2)}\\
\iff&(I_A\subseteq R_1)\land((R_1-I_A)\subseteq R_1) && \text{(补交转换律)}\\
\iff&(I_A\subseteq R_1)\land((R_2-I_A)\subseteq R_1) && (f(R_1)=f(R_2))\\
\Longrightarrow&(I_A\cup(R_2-I_A))\subseteq R_1\cup R_1 && \text{(引理 1.4)}\\
\iff&(I_A\cup(R_2-I_A))\subseteq R_1 && \text{(幂等律)}\\
\iff&(I_A\cup(R_2\cap\sim I_A))\subseteq R_1 && \text{(补交转换律)}\\
\iff&(I_A\cup R_2)\cap(I_A\cup\sim I_A)\subseteq R_1 && \text{(分配律)}\\
\iff&(I_A\cup R_2)\cap E\subseteq R_1 && \text{(排中律)}\\
\iff&(I_A\cup R_2)\subseteq R_1 && \text{(同一律)}\\
\iff&R_2\subseteq R_1 && (I_A\subseteq R_2)
\end{aligned}$$

从而有 $R_2\subseteq R_1$。同理可证 $R_1\subseteq R_2$。故有 $f(R_1)=f(R_2)\Rightarrow R_1=R_2$。即 f 是单射。

对任意 $R'\in\mathscr{B}$，由教材定理 2.29(3) 知，$R'\cup I_A\in\mathscr{A}$。显然有 $f(R'\cup I_A)=R'$。故，f 是满射。

从而 f 是 $\mathscr{A}$ 到 $\mathscr{B}$ 上的双射。由等势定义知，$\mathscr{A}\approx\mathscr{B}$。 □

5.2

(1)　由集合相等关系的自反性、对称性和传递性立即得证。

(2)

证明: 定义函数 $f:((A\to A)/R)\to(\mathcal{P}(A)-\varnothing),\forall x\in(A\to A)/R, f(x)=\operatorname{ran}(x)$。

由 $(A\to A)/R$ 的定义知，f 是函数且为单射。

对任意 $S\in\mathcal{P}(A)-\varnothing$，由于 $\varnothing\notin\mathcal{P}(A)-\varnothing$，故 $S\neq\varnothing$。因而存在元素 $a\in S$。

定义函数 $g:A\to A,\forall x\in A, g(x)=\begin{cases}x, & 若 x\in S\\ a, & 若 x\notin S\end{cases}$。则 $g\in(A\to A)$ 且 $f([g]_R)=S$。因而 f 是满射。

综合知，f 是双射。从而有 $(A\to A)/R\approx\mathcal{P}(A)-\varnothing$。 □

5.3

证明： 由教材定理 5.1 和等势关系的传递性知，$[0,1] \approx \mathbb{R}$。

下面只需证 $[0,1] \approx [a,b]$。

定义 $f : [0,1] \to [a,b], \forall x \in [0,1], f(x) = (b-a)x + a$。

显然，f 是函数且为双射。从而有 $[0,1] \approx [a,b]$。 □

5.4

证明： 由于 I_A 是双射，故 $A \approx A$。

由教材定理 3.9 知，若 $f : A \to B$ 是双射，则 $f^{-1} : B \to A$ 也是双射。从而有 $A \approx B \Rightarrow B \approx A$。

由教材定理 3.4(3) 知，若 $g : A \to B$ 和 $f : B \to C$ 都是双射，则 $f \circ g : A \to C$ 也是双射。故有 $A \approx B \wedge B \approx C \Rightarrow A \approx C$。 □

5.5

证明： 用数学归纳法证明。

令 $S = \{n \mid n \in \mathbb{N} \wedge \forall x(x \subset n \to \exists m(m \in n \wedge x \approx m))\}$。

(1) $0 \in S$。因为对任意 x，$x \subset 0$ 恒为假，故蕴涵式永真。

(2) 设 $n \in S$，对 n^+ 的任意真子集 x，分三种情况讨论：

① 若 $x = n$，就有 $x \approx n \in n^+$。

② 若 $x \subset n$，则依归纳假设，存在 $m \in n \subset n^+$，使 $x \approx m \in n^+$。

③ 若 $n \in x$，则 $x - \{n\} \subset n$（若不然，就有 $n \subseteq x - \{n\}$，于是有 $n^+ = n \cup \{n\} \subseteq x - \{n\} \cup \{n\} = x$，与前提 $x \subset n$ 矛盾）。这时，依归纳假设，存在 $m \in n$，使 $x - \{n\} \approx m$。此时有，$x \approx m^+$（这是因为，对任意函数 $f : x - \{n\} \to m$，令 $g : x \to m^+, \forall y \in x, g(y) = \begin{cases} f(y), & 若 y \neq n \\ m, & 若 y = n \end{cases}$。则 g 是双射当且仅当 f 是双射）。由教材定理 4.4 和 $m \in n$ 知，$x \approx m^+ \in n^+$。

注意到，对任意 $x \subset n^+$，上述三种情况必有一种成立，这是因为：由于 $x \subset n^+ = n \cup \{n\}$，若 $n \notin x$，则 x 的所有元素必然都在 n 里，即有 $x \subseteq n$，这时①和②至少有一种成立。反之，若 $n \in x$，则③成立。而对这三种情况都存在某个集合 $m \in n^+$，使 $x \approx m$。这样就证明了对任意 $n \in S$，有 $n^+ \in S$。从而有 $S = \mathbb{N}$。 □

5.6

证明： 由于 $I_A : A \to A$ 是单射，故 $A \preccurlyeq\cdot A$。

由教材定理 3.4(2) 知，若存在 $g : A \to B, f : B \to C$，且 f 和 g 都是单射，则 $f \circ g : A \to C$ 也是单射。故有 $A \preccurlyeq\cdot B \wedge B \preccurlyeq\cdot C \Rightarrow A \preccurlyeq\cdot C$。 □

5.7

证明： 只需证：A 是无穷可数集当且仅当存在 A 到 $\mathbb{N}$ 的双射。

充分性：

若存在 A 到 $\mathbb{N}$ 的双射，就有 $A \approx \mathbb{N}$。此时，若 A 有穷的，则 A 与一自然数 n 等势，从而由等势关系的传递性知 $\mathbb{N} \approx n$，也即，$\mathbb{N}$ 是有穷的，这与教材定理 5.5 推论 2(2) “$\mathbb{N}$ 是无穷集”矛盾。因此，A 是无穷的。

又由教材定理 5.7 推论 (2) 知，$A \approx \mathbb{N} \implies A \preccurlyeq\cdot \mathbb{N}$。因此，$A$ 是可数的。这就证明了定理的一个方向：若存在 A 到 $\mathbb{N}$ 的双射则 A 是无穷可数集。

必要性：

若 A 是无穷可数集，则由可数集定义知：$A \preccurlyeq\cdot \mathbb{N}$。又由教材定理 5.14 知，$\mathbb{N} \preccurlyeq\cdot A$。从而由 Schröder-Bernstein 定理知，$A \approx \mathbb{N}$。这就证明了定理的另一个方向。 □

5.8 由教材定理 5.17 立即得证。

5.9

证明： 当 $n = 2$ 时，记这两个集合为 A 和 B，设他们的基数分别为：$\kappa = \operatorname{card} A$ 和 $\lambda = \operatorname{card} B$。

由可数集定义知：$\kappa \leq \aleph_0, \lambda \leq \aleph_0$。于是有：

$$\begin{aligned}\kappa \cdot \lambda &\leq \kappa \cdot \aleph_0 && \text{(教材定理 5.22(2))}\\ &= \aleph_0 \cdot \kappa && \text{(教材定理 5.21(1))}\\ &\leq \aleph_0 \cdot \aleph_0 && \text{(教材定理 5.22(2))}\\ &= \aleph_0 && \text{(例 5.9(4))}\end{aligned}$$

因此，$\operatorname{card}(A \times B) = \kappa \cdot \lambda \leq \aleph_0$，是可数集。

设 $n = k(k \geq 2)$ 时命题成立，则当 $n = k + 1$ 时，前 k 个集合的卡氏积 S 为可数集，应用上面 $n = 2$ 时的结论可知，S 与第 $k + 1$ 个集合的卡氏积也是可数集。故，当 $n = k + 1$ 时，命题同样成立。 □

5.10

证明： 若不然，就有 $\mathcal{P}(A)$ 是可数集，即有 $\operatorname{card} \mathcal{P}(A) \leq \aleph_0$，由教材定理 5.11 和 5.14 知：$\aleph_0 \leq \operatorname{card} A \leq \operatorname{card} \mathcal{P}(A) \leq \aleph_0$。由优势关系的传递性，可得：$\aleph_0 \leq \operatorname{card} A \leq \aleph_0$ 和 $\aleph_0 \leq \operatorname{card} \mathcal{P}(A) \leq \aleph_0$。再由 Schröder-Bernstein 定理得，$\operatorname{card} A = \operatorname{card} \mathcal{P}(A) = \aleph_0$，从而有 $A \approx \mathcal{P}(A)$。这与康托定理矛盾。

故，$\mathcal{P}(A)$ 不是可数集。 □

5.11

(1) 取 $f : \mathbb{N} \to A, \forall x \in \mathbb{N}, f(x) = (x + 1)^7$。显然 f 是双射。故 $\operatorname{card} A = \operatorname{card} \mathbb{N} = \aleph_0$。

(2) 取 $f : \mathbb{N} \to B, \forall x \in \mathbb{N}, f(x) = (x + 1)^{109}$。显然 f 是双射。故 $\operatorname{card} B = \operatorname{card} \mathbb{N} = \aleph_0$。

(3) 由教材定理 5.7 和 $\mathbb{N} \approx A \subseteq A \cup B$ 可知，$\mathbb{N} \preccurlyeq\cdot\, A \cup B$。又由 $A \cup B \subseteq \mathbb{N}$ 和教材定理 5.7 推论 (1) 知，$A \cup B \preccurlyeq\cdot\, \mathbb{N}$。从而由 Schröder-Bernstein 定理得：$\operatorname{card}(A \cup B) = \operatorname{card} \mathbb{N} = \aleph_0$。

(4) 令 $C = \{n^{763} \mid n \in \mathbb{N} \wedge n \neq 0\}$，取 $f : \mathbb{N} \to C, \forall x \in \mathbb{N}, f(x) = (x + 1)^{763}$。显然 f 是双射。因此有 $\mathbb{N} \approx C$。再由 $C \subseteq A \cap B$ 和教材定理 5.7 知，$\mathbb{N} \preccurlyeq\cdot\, A \cap B$。又由 $A \cap B \subseteq \mathbb{N}$ 和教材定理 5.7 推论 (1) 知 $A \cap B \preccurlyeq\cdot\, \mathbb{N}$。由 Schröder-Bernstein 定理知，$A \cap B \approx \mathbb{N}$。从而有 $\operatorname{card}(A \cap B) = \operatorname{card} \mathbb{N} = \aleph_0$。

5.12

证明： 由教材定理 5.20 知，$\operatorname{card} \mathcal{P}(A) = 2^{\operatorname{card} A}, \operatorname{card} \mathcal{P}(B) = 2^{\operatorname{card} B}$。

下面证明：$2^{\operatorname{card} A} = 2^{\operatorname{card} B}$。

由 $\operatorname{card} A = \operatorname{card} B$ 和教材定理 5.7 得 $\operatorname{card} A \leq \operatorname{card} B$ 和 $\operatorname{card} B \leq \operatorname{card} A$。对以上两式分别使用教材定理 5.22(4)，就有 $2^{\operatorname{card} A} \leq 2^{\operatorname{card} B}$ 和 $2^{\operatorname{card} B} \leq 2^{\operatorname{card} A}$，由 Schröder-Bernstein 定理即得：$2^{\operatorname{card} A} = 2^{\operatorname{card} B}$。

从而有：$\operatorname{card} \mathcal{P}(A) = 2^{\operatorname{card} A} = 2^{\operatorname{card} B} = \operatorname{card} \mathcal{P}(B)$。 □

5.13

(1)

证明: 对任意自然数 $n \in \mathbb{N}$，取 $S = \{\{\{0\}\}, \{1\}, \{2\}, \ldots, \{n-1\}\}$，则有 $\operatorname{card} S = n, S \cap \mathbb{N} = \varnothing$。

取 $f : \mathbb{N} \to S \cup \mathbb{N}, \forall x \in \mathbb{N}, f(x) = \begin{cases} \{\{0\}\}, & 若x = 0 \\ \{x\}, & 若0 < x < n \\ x - n, & 若x \geq n \end{cases}$。

显然，f 是双射。故有 $n + \aleph_0 = \operatorname{card}(S \cup \mathbb{N}) = \operatorname{card} \mathbb{N} = \aleph_0$。 □

(2)

证明: 对任意非零自然数[1] $n \in \mathbb{N}_+$，令 $S = \{nm \mid m \in \mathbb{N}\}$。

取 $f : \mathbb{N} \to S, \forall x \in \mathbb{N}, f(x) = nx$。$f$ 显然是双射。从而有 $S \approx \mathbb{N}$。

再取 $g : (n \times S) \to \mathbb{N}, \forall \langle x, y \rangle \in (n \times S), g(\langle x, y \rangle) = x + y$，由代余除法的性质知，$g$ 是双射。从而有 $n \times S \approx \mathbb{N}$。

因此：$n \cdot \aleph_0 = \operatorname{card}(n \times S) = \operatorname{card} \mathbb{N} = \aleph_0$。 □

(3)

证明: 由教材例 5.1 知，$\mathbb{N} \approx \mathbb{N}_{偶} \approx \mathbb{N}_{奇}$。显然有 $\mathbb{N}_{偶} \cap \mathbb{N}_{奇} = \varnothing, \mathbb{N}_{偶} \cup \mathbb{N}_{奇} = \mathbb{N}$。于是有 $\aleph_0 + \aleph_0 = \operatorname{card}(\mathbb{N}_{偶} \cup \mathbb{N}_{奇}) = \operatorname{card} \mathbb{N} = \aleph_0$。 □

(4) 由教材定理 5.1(2) 即得。

5.14

(1)

证明: 设 K 为一基数为 κ 的集合，显然有 $\operatorname{card} \varnothing = 0, K \cap \varnothing = \varnothing, K \cup \varnothing = K$。

因此有：$\kappa + 0 = \operatorname{card}(K \cup \varnothing) = \operatorname{card} K = \kappa$。 □

(2)

证明: 设 K 为一基数为 κ 的集合，则有 $K \times \varnothing = \varnothing$。

因此有：$\kappa \cdot 0 = \operatorname{card}(K \times \varnothing) = \operatorname{card} \varnothing = 0$。 □

(3)

证明: 设 K 为一基数为 κ 的集合，则有 $\operatorname{card}(\{\varnothing\}) = 1, K \approx K \times \{\varnothing\}$ (取 $f : K \to K \times \{\varnothing\}, \forall x \in K, f(x) = \langle x, \varnothing \rangle$ 即可)。

故有：$\kappa \cdot 1 = \operatorname{card}(K \times \{\varnothing\}) = \operatorname{card} K = \kappa$。 □

(4)

证明: 设 K 为一基数为 κ 的集合，由全函数定义知：$(\varnothing \to K) = \{\varnothing\}$。

即有：$\kappa \cdot 0 = \operatorname{card}(\varnothing \to K) = \operatorname{card}(\{\varnothing\}) = 1$。 □

(5)

证明: 设 K 为一基数为 κ 的集合，由 $\kappa \neq 0$ 知，$K \neq \varnothing$，全函数定义知：$(K \to \varnothing) = \varnothing$。

故：$\kappa \cdot 1 = \operatorname{card}(\varnothing^K) = \operatorname{card} \varnothing = 0$。 □

(6)

证明: 设 K_1, K_2 为两个基数为 κ 的集合，且 $K_1 \cap K_2 = \varnothing$。由基数定义知，必然存在双射 $f : K_1 \to K_2$。作 $g : K_1 \cup K_2 \to \{K_1, K_2\} \times K_2, \forall x \in K_1 \cup K_2, g(x) = \begin{cases} \langle K_1, f(x) \rangle & 若x \in K_1 \\ \langle K_2, x \rangle, & 若x \in K_2 \end{cases}$。

---

[1] 本小题 n 必须大于 0，否则就有 $\operatorname{card}(\varnothing \times \mathbb{N}) = \operatorname{card} \varnothing = 0 \neq \aleph_0$。

由于 $K_1 \cap K_2 = \varnothing$，所以 g 是函数。

g 显然是满射。

对任意 $x, y \in K_1 \cup K_2, x \neq y$，分三种情况讨论：

(1) 若 $x \in K_1, y \in K_2$ 或 $x \in K_2, y \in K_1$，则由 $K_1 \neq K_2$ 和教材定理 2.1 知，$g(x) \neq g(y)$。

(2) 若 $x, y \in K_1$，则由 f 是双射知，$f(x) \neq f(y)$，从而由教材定理 2.1 知，$g(x) \neq g(y)$。

(3) 若 $x, y \in K_2$，则教材定理 2.1 直接有，$g(x) \neq g(y)$。

因此，g 是单射，从而是双射。从而有 $K_1 \cup K_2 \approx \{K_1, K_2\} \times K_2$。

由此得证：$\kappa + \kappa = \operatorname{card}(K_1 \cup K_2) = \operatorname{card}(\{K_1, K_2\} \times K_2) = 2 \cdot \kappa$。 □

(7)

证明： 设 K 为一基数为 κ 的集合，作 $f : K \to (\{\varnothing\} \to K), \forall x \in K, f(x) = \{\langle \varnothing, x \rangle\}$。显然 f 是双射。

因此有 $K \approx (\{\varnothing\} \to K)$。从而有：$\kappa^1 = \operatorname{card}(\{\varnothing\} \to K) = \operatorname{card} K = \kappa$。 □

(8)

证明： 对任意自然数 $n \in \mathbb{N}$，显然有 $\operatorname{card}(\{n\}) = 1, n \cap \{n\} = \varnothing$。

故有 $n + 1 = \operatorname{card}(n \cup \{n\}) = \operatorname{card}(n^+) = n^+$。 □

第六章　序数*

6.1　若不要求 $\langle A, \prec_A\rangle, \langle B, \prec_B\rangle$ 为拟线序，则第 (1)、(2) 小题的答案都是否定的。举反例如下：

令 $A = \{1, 2, 3, 4, 12\}$，$\prec_A$ 为整除关系，$B = \{1, 2, 3, 4\}$，$\prec_B$ 为小于关系。令 $f(1) = 1, f(2) = f(3) = 2, f(4) = 3, f(12) = 4$。

易于验证，$\langle A, \prec_A\rangle, \langle B, \prec_B\rangle$ 和 f 满足题目中的要求。但 $f(2) = f(3)$，故 f 不是单射。同时，$f(3) \prec_B f(4)$，但 $3 \not\prec_A 4$，因此 $f(x) \prec_B f(y) \nRightarrow x \prec_A y$。

若要求 $\langle A, \prec_A\rangle, \langle B, \prec_B\rangle$ 为拟线序，则 (1)、(2) 的答案都是肯定的。证明如下：

证明： (1)　反设 f 不是单射。则存在 $x, y \in A$，满足 $x \neq y \wedge f(x) = f(y)$。由于 $\langle A, \prec_A\rangle$ 是拟线序，故必有 $x \prec_A y$ 或 $y \prec_A x$。由题设，就有 $f(x) \prec_B f(y)$ 或 $f(y) \prec_B f(x)$。这与假设 $f(x) = f(y)$ 矛盾。故，f 必是单射。

(2)　反设存在 $x, y \in A$，使 $f(x) \prec_B f(y)$，但 $x \not\prec_A y$。由于 $\langle A, \prec_A\rangle$ 是拟线序，所以有 $x = y$ 或 $y \prec_A x$。若 $x = y$，则由 f 是函数可知，$f(x) = f(y)$，这与 $f(x) \prec_B f(y)$ 矛盾。若 $y \prec_A x$，则由题设知，$f(y) \prec_B f(x)$，这同样与前提 $f(x) \prec_B f(y)$ 矛盾。这就证明了 $\forall x, y \in A, x \prec_A y \Leftrightarrow f(x) \prec_B f(y)$。 □

6.2　由拟序关系定义和教材定理 2.15(2)、(5) 立即得证。

6.3

(1)

证明： 由全序定义知，对所有 $x, y \in A$，若 $x \neq y$，则 $\langle x, y\rangle$ 与 $\langle y, x\rangle$ 有且仅有一个属于 R。由于 $x \neq y$，故若 $\langle x, y\rangle$ 或 $\langle y, x\rangle$ 属于 R，则它们也属于 $R - I_A$。由组合数学结论知，这样的 x, y 有 $C_n^2 = n(n-1)/2$ 组。同时，由 $R - I_A$ 的定义知，$R - I_A$ 只有这 $n(n-1)/2$ 个元素。又因为 R 是全序，所以 $I_A \subseteq R$。从而由容斥原理有：$|R| = |I_A| + |R - I_A| - |I_A \cap (R - I_A)| = n + n(n-1)/2 = n(n+1)/2$。 □

(2)　由拟线序定义知，对所有 $x, y \in A$，若 $x \neq y$，则 $\langle x, y\rangle$ 与 $\langle y, x\rangle$ 有且仅有一个属于 R，又由于 $\forall x \in A, \langle x, x\rangle \notin R$，所以：$|R| = C_n^2 = n(n-1)/2$。

6.4　首先证明，良序集定义中的“$\langle A, \prec\rangle$ 为拟全序集”的条件可以弱化为“$\langle A, \prec\rangle$ 为拟序集”。

引理 6.1 *设 $\langle A, \prec\rangle$ 为一个拟序集，若对于 A 的任何非空子集 B 均有最小元，则 $\langle A, \prec\rangle$ 是拟全序集，从而是良序集。*

证明： 反设 $\langle A, \prec\rangle$ 不是拟全序，则存在 $x, y \in A$，使得 $x \neq y \wedge x \not\prec y \wedge y \not\prec x$。这时，取 $B = \{x, y\} \subseteq A$，B 为非空的。但由于 $x \not\prec y \wedge x \neq y$，所以 x 不是的最小元。同理，y 也不是最小元。从而 B 中无最小元，与题设矛盾。

因此 $\langle A, \prec\rangle$ 必是拟全序集。从而由良序定义知，$\langle A, \prec\rangle$ 是良序集。 □

再证原题：

证明： 对任何非空集合 $A \subseteq \mathbb{Z}_+$，令 $B = f(A) = \{f(x) \mid x \in A\}$。则由 f 的定义知，$B \subseteq \mathbb{N}$，由 $\mathbb{N}$ 上的良序定理知，B 中有关于 $<$ 关系的最小元 b。记 $C = A \cap f^{-1}(b) = \{x \mid x \in A \wedge f(x) = b\}$。则 $C \subseteq \mathbb{Z}_+$。从而 C 也有关于 $<$ 的最小元 c。下面证明 c 就是 A 中关于 R 的最小元。

$\forall x \in A$，若 $x \neq c$，则：由 $f(c) = b$ 是 $f(A)$ 中的最小元知，$f(c) < f(x)$ 或 $f(c) = f(x)$。若 $f(c) < f(x)$，则由 R 的定义有 cRx。若 $f(x) = f(c) = b$，则 $x, c \in f^{-1}(b)$，从而由 $x, c \in A$ 知，$x, c \in C = A \cap f^{-1}(b)$。但 c 是 C 中的最小元，且 $x \neq c$，从而必有 $c < x$。于是，由 R 的定义也有 cRx。

这就证明了 c 是 A 中关于 R 的最小元。由 A 的任意性知，$\mathbb{Z}_+$ 中任何非空集合都有最小元。从而由引理 6.1 知，$\langle \mathbb{Z}_+, R \rangle$ 是良序集。 □

6.5

证明： 记 $B = \{x \mid x \in A \wedge f(x) \prec x\}$。只需证明 $B = \varnothing$。

反设 $B \neq \varnothing$，则 B 是良序集 A 的非空子集，从而存在最小元 t。由 B 的定义知，$f(t) \prec t$。由 f 的保序性知，$f(f(t)) \prec f(t)$，从而 $f(t) \in B$。但 $f(t) \prec t$，这与 t 的最小性矛盾。 □

6.6

(1) 由题设知：

$$\begin{aligned}
F(0) &= A \cup (\cup\cup \operatorname{ran}(F \restriction (\operatorname{seg} 0))) && (\gamma\ \text{定义}) \\
&= A \cup (\cup\cup \{F(x) \mid x \in \operatorname{seg} 0\}) && (\text{值域、限制定义}) \\
&= A \cup (\cup\cup \varnothing) && (\operatorname{seg} 0 = \varnothing) \\
&= A \\
F(1) &= A \cup (\cup\cup \operatorname{ran}(F \restriction (\operatorname{seg} 1))) && (\gamma\ \text{定义}) \\
&= A \cup (\cup\cup \{F(x) \mid x \in \operatorname{seg} 1\}) && (\text{值域、限制定义}) \\
&= A \cup (\cup\cup \{F(0)\}) && (\operatorname{seg} 1 = \{0\}) \\
&= A \cup (\cup\cup \{A\}) && (F(0) = A) \\
&= A \cup (\cup A) \\
F(2) &= A \cup (\cup\cup \operatorname{ran}(F \restriction (\operatorname{seg} 2))) && (\gamma\ \text{定义}) \\
&= A \cup (\cup\cup \{F(x) \mid x \in \operatorname{seg} 2\}) && (\text{值域、限制定义}) \\
&= A \cup (\cup\cup \{F(0), F(1)\}) && (\operatorname{seg} 2 = \{0, 1\}) \\
&= A \cup (\cup\cup \{A, A \cup (\cup A)\}) && (F(0) = A, F(1) = A \cup (\cup A)) \\
&= A \cup (\cup(A \cup (A \cup (\cup A)))) && (\text{广义并定义}) \\
&= A \cup (\cup(A \cup (\cup A))) && (\text{同一律}) \\
&= A \cup (\cup A) \cup (\cup\cup A) && (\cup(A \cup B) = (\cup A) \cup (\cup B))
\end{aligned}$$

下面证明，$\forall n \in \mathbb{N}, F(n^+) = A \cup (\cup F(n))$。

证明： 用强数学归纳法证明：$\forall n \in \mathbb{N}$，有 $F(n^+) = A \cup (\cup F(n))$ 和 $F(n) \subseteq F(n^+)$。

令 $S = \{x \mid x \in \mathbb{N} \wedge F(x^+) = A \cup (\cup F(x)) \wedge F(x) \subseteq F(x^+)\}$。

由于 $F(0) = A \subseteq A \cup (\cup A) = A \cup (\cup F(0)) = F(1)$，所以 $0 \in S$。

对任何 $n \in \mathbb{N}$，$n \geq 1$，若 $\forall x \in \mathbb{N}, x < n \Rightarrow x \in S$，则：

$$F(n^+) = A \cup (\cup\cup \operatorname{ran}(F \restriction (\operatorname{seg}(n^+)))) \qquad (\gamma\ \text{定义})$$

$$\begin{aligned}
&= A\cup(\cup\cup\{F(x)\mid x\in \operatorname{seg}(n^+)\}) && (\text{值域、限制定义})\\
&= A\cup(\cup\cup\{F(0),F(1),\cdots,F(n)\}) && (\operatorname{seg}(n^+)=\{0,1,\cdots,n\})\\
&= A\cup(\cup(F(0)\cup F(1)\cup\cdots\cup F(n))) && (\text{广义并定义})\\
&= A\cup(\cup(F(n))) && (\text{归纳假设：}F(0)\subseteq F(1)\subseteq\cdots\subseteq F(n))
\end{aligned}$$

这就证明了：$F(n^+)=A\cup(\cup F(n))$。

注意到，由于 $n\geq 1$，所以总有 $n-1\in\mathbb{N}$。由归纳假设知：$n-1\in S$。从而 $F(n)=A\cup(\cup F(n-1))$ 且 $F(n-1)\subseteq F(n)$。由教材例 1.8(1) 知，$F(n-1)\subseteq F(n)\Rightarrow \cup F(n-1)\subseteq\cup F(n)$。从而 $F(n)=A\cup(\cup F(n-1))\subseteq A\cup(\cup F(n))=F(n^+)$。

这就证明了：$\forall x\in\mathbb{N},x<n\Rightarrow x\in S\Rightarrow n^+\in S$。由 $\mathbb{N}$ 上的强归纳原则知，$S=\mathbb{N}$。

因此，对一切 $n\in\mathbb{N}$，都有 $F(n^+)=A\cup(\cup F(n))$。 □

(2)

证明： 由第 (1) 小题结论知，$F(n^+)=A\cup(\cup F(n))$。从而：

$$\begin{aligned}
a\in F(n) &\implies a\subseteq\cup F(n) && (\text{教材例 1.8(2)})\\
&\implies a\subseteq A\cup(\cup F(n)) && (F(n)\subseteq A\cup(\cup F(n)))\\
&\implies a\subseteq F(n^+) && (F(n^+)=A\cup(\cup F(n)))
\end{aligned}$$

□

(3)

证明： 因为 $\operatorname{ran}F=\{F(0),F(1),F(2),\cdots\}$，所以 $B=\cup\operatorname{ran}F=\bigcup\limits_{n\in\mathbb{N}}F(n)$。

因此，对任意 $x\in B$，必存在 $n\in\mathbb{N}$，使得 $x\in F(n)$。由第 (2) 小题结论知，$x\subseteq F(n^+)$。而 $F(n^+)\in\operatorname{ran}F$，从而 $x\subseteq F(n^+)\subseteq\cup\operatorname{ran}F=B$。也即，对任意的 $x\in B$，有 $x\subseteq B$。由教材定理 4.10 知，B 是传递集。

又因为 $A=F(0)\in\operatorname{ran}F$，所以有 $A\subseteq\cup\operatorname{ran}F=B$。 □

6.7

(1)

证明： $\prec$ 显然是拟序。

对 $\mathbb{Z}$ 的任意非空子集 A，作 $S=A\cap\mathbb{N}$。

若 $S\neq\varnothing$，则由 $\mathbb{N}$ 上的良序定理知，S 有最小元 s。对所有 $x\in A$，若 $x\in S$，则由最小元定义知，$x\preccurlyeq s$，若 $x\notin S$，则 $x\in\mathbb{Z}-\mathbb{N}$ 且 $s\in\mathbb{N}$，由 $\prec$ 的定义知，$s\prec x$。从而 s 是 A 的最小元。

若 $S=\varnothing$。则 $A\subseteq(\mathbb{Z}-\mathbb{N})$，作 $f:(\mathbb{Z}-\mathbb{N})\to\mathbb{N},\forall -x\in(\mathbb{Z}-\mathbb{N}),f(-x)=x$。由 $\mathbb{Z}$ 和 $\prec$ 定义知，f 是单射且 $x\prec y\Leftrightarrow f(x)<f(y)$。从而由 $\mathbb{N}$ 上的良序定理和教材定理 6.3(3) 知，$\langle\mathbb{Z}-\mathbb{N},\prec\rangle$ 是良序，从而 $A\subseteq(\mathbb{Z}-\mathbb{N})$ 有最小元。

这就证明了 $\mathbb{Z}$ 的每个非空子集都有关于 $\prec$ 的最小元。由引理 6.1 知，$\langle\mathbb{Z},\prec\rangle$ 是良序集。 □

(2) $E(3)=\{0,1,2\}$;　$E(-1)=\mathbb{N}$;　$E(-2)=\mathbb{N}\cup\{-1\}$;　$E(-n)=\mathbb{N}\cup\{-m\mid m\in\mathbb{N}_+\wedge m<n\},\ \forall n\in\mathbb{N}$。

6.8

证明： 设 $f,g:A\to B$ 都是 $\langle A,\prec_A\rangle$ 到 $\langle B,\prec_B\rangle$ 的同构。由同构的定义知，f,g 是双射。从而由教材定理 3.9 知，$f^{-1}:B\to A$ 也是一个双射函数，且有 $f\circ f^{-1}=I_B$。从而：

$\forall x,y\in A$,

$$x\prec_A y\iff g(x)\prec_B g(y)\qquad(g\text{ 是同构})$$

$$\begin{aligned}
&\iff I_B \circ g(x) \prec_B I_B \circ g(y) && (\text{教材定理 3.6})\\
&\iff (f \circ f^{-1}) \circ g(x) \prec_B (f \circ f^{-1}) \circ g(y) && (f \circ f^{-1} = I_B)\\
&\iff f(f^{-1} \circ g(x)) \prec_B f(f^{-1} \circ g(y)) && (\text{教材定理 2.5、教材定理 3.3})\\
&\iff f^{-1} \circ g(x) \prec_A f^{-1} \circ g(y) && (f\ \text{是同构})
\end{aligned}$$

从而有 $\forall x, y, x \prec_A y \Rightarrow f^{-1} \circ g(x) \prec_A f^{-1} \circ g(y)$。由习题 6.5 的结论知，对任意 $x \in A$，有 $x \preccurlyeq_A f^{-1} \circ g(x)$，于是有 $f(x) \preccurlyeq_B f(f^{-1} \circ g(x)) = g(x)$。同理可证，$g(x) \preccurlyeq f(x), \forall x \in A$。这就证明了 $f(x) = g(x), \forall x \in A$，也即，$f = g$ 是 $\langle A, \prec_A\rangle$ 到 $\langle B, \prec_B\rangle$ 上唯一的同构。 □

6.9[1]

证明： 由定义知，F 是函数，且为满射。

对任意 $a, b \in A$，若 $a \neq b$，分两种情况讨论：

情况一：若 $a \prec b$ (或 $b \prec a$)，则有 $a \in F(b)$ (或 $b \in F(a)$)，但 $b \notin F(a)$ (或 $a \notin F(b)$)，从而有 $F(a) \neq F(b)$。

情况二：若既无 $a \prec b$ 也无 $b \prec a$，则 $a \in F(a)$ 但 $b \notin F(a)$，从而也有 $F(a) \neq F(b)$。

这就证明了 F 是单射，从而是双射。

同时，对任意 $a, b \in A$，若 $a \prec b$，则：

$\forall x$，

$$\begin{aligned}
x \in F(a) &\iff x \prec a \vee x = a && (F(a)\ \text{定义})\\
&\implies x \prec b && (a \prec b\text{、拟序关系传递性})\\
&\implies x \in F(b) && (F(b)\ \text{定义})
\end{aligned}$$

从而 $F(a) \subseteq F(b)$。注意到，由于 $b \in F(b) \wedge b \notin F(a)$，所以 $F(a) \subset F(b)$。

反之，若 $F(a) \subset F(b)$，则由于 $a \in F(a) \subset F(b)$，所以有 $a \preccurlyeq b$。同时，由于 F 是单射，所以 $F(a) \subset F(b) \Rightarrow F(a) \neq F(b) \Rightarrow a \neq b$。这就证明了 $a \prec b$。

从而 $a \prec b \Leftrightarrow F(a) \subset F(b)$。由同构定义知，$F$ 是 $\langle A, \prec\rangle$ 到 $\langle S, \subset\rangle$ 上的同构。 □

6.10

证明： 若不然，由序数的三歧性就有 $\alpha \in \beta$。又由于序数是传递集，所以有 $\alpha \subseteq \beta$。

记 $\langle A, \prec\rangle$ 到 $\langle \alpha, \in_\alpha\rangle$ 的同构为 $f : A \to \alpha$，记 $\langle B, \prec^0\rangle$ 到 $\langle \beta, \in_\beta\rangle$ 的同构为 $g : B \to \beta$。注意到，因为 $B \subseteq A$，所以有 $g^{-1} : \beta \to A$。同理，由于 $\alpha \subseteq \beta$，所以有 $f : A \to \beta$。从而有 $f \circ g^{-1} : \beta \to \beta$。容易证明 $f \circ g^{-1}$ 是保序的：

$\forall x, y \in \beta$，

$$\begin{aligned}
x \in y &\iff I_\beta(x) \in I_\beta(y) && (I_\beta\ \text{是恒等函数})\\
&\iff g \circ g^{-1}(x) \in g \circ g^{-1}(y) && (g \circ g^{-1} = I_\beta)\\
&\iff g(g^{-1}(x)) \in g(g^{-1}(y)) && (\text{教材定理 3.3})\\
&\iff g^{-1}(x) \prec^0 g^{-1}(y) && (g\ \text{是同构})\\
&\implies g^{-1}(x) \prec g^{-1}(y) && (\prec^0 \subseteq \prec)\\
&\iff f(g^{-1}(x)) \in f(g^{-1}(y)) && (f\ \text{是同构})
\end{aligned}$$

这就证明了 $f \circ g^{-1}$ 的保序性。

由习题 6.5 的结论应有 $x \underline{\in} f \circ g^{-1}(x), \forall x \in \beta$。又由于 $\alpha \in \beta$，所以应有 $\alpha \underline{\in} f \circ g^{-1}(\alpha)$。但由 g^{-1} 的定义知，$g^{-1}(\alpha) \in B \subseteq A$，由 f 的保序性知，$f \circ g^{-1}(\alpha) \in \alpha$。矛盾。 □

---

[1] 题目中"证明 F 是 $\langle A, \prec\rangle$ 与 $\langle S, \subseteq\rangle$ 之间的同构"应为"证明 F 是 $\langle A, \prec\rangle$ 与 $\langle S, \subset\rangle$ 之间的同构"。否则一个是拟序，一个是偏序，不同构。

第二编

图论

第七章　图

7.1　由图论基本定理知，该图所有顶点度数之和应为 $2 * 16 = 32$。已知的 7 个顶点度数和为 24。由题设，其余各顶点的度数至多为 2，故至少还要有 4 个顶点才能使顶点度数之和等于 32。即，G 中至少有 11 个顶点。

7.2　由图论基本定理知，图中必有偶数个奇度顶点。结合题设可知，只可能有如下几种情况：

(1)　9 个 6 度顶点；
(2)　7 个 6 度顶点和 2 个 5 度顶点；
(3)　5 个 6 度顶点和 4 个 5 度顶点；
(4)　3 个 6 度顶点和 6 个 5 度顶点；
(5)　1 个 6 度顶点和 8 个 5 度顶点。

逐一验证即证原题。

7.3　将每个面看作顶点，将相邻两面的棱看作边。由图论基本定理即证原题。

7.4　先证一个引理。

引理 7.1　(**a**) *设 G 为一个无向简单图，则 G 的每一个非平凡(顶点数大于 1)的连通分支 G_i 中必存在顶点 $v_i, v_j \in V(G_i) \wedge v_i \neq v_j \wedge d(v_i) = d(v_j)$。* (**b**) *若 $|V(G)| \geq 2$，则 G 中必存在 $v_i, v_j \in V(G) \wedge v_i \neq v_j \wedge d(v_i) = d(v_j)$。*

证明： 先证 (a)。

对 G 的任意一个非平凡的连通分支 G_i，设 $|V(G_i)| = n_i$。

由 G 是简单图知，$\forall v \in V(G_i), d(v) \leq n_i - 1$。又由于 G_i 是连通的和非平凡的，所以有：$d(v) \geq 1$。从而 $\forall v \in V(G_i)$，$d(v)$ 只能有 $n_i - 1$ 种取值。但 G_i 有 n_i 个顶点，由鸽巢原理可知 (a) 成立。

再证 (b)。

若 G 中存在非平凡的连通分支，则由 (a) 知，命题成立。若不然，则 G 的每个连通分支都是平凡的，从而每个连通分支中只有一个顶点，且度数为 0。由于 G 为非平凡的，所以 G 中至少有两个这样的顶点，命题同样成立。 □

再证原题。

证明：

证法一： 将选手看作图的顶点，将“u 与 v 下一盘棋”看作边 (u, v)，则每名选手所下的盘数即为该顶点的度。易于验证所构成的图是无向简单图，由引理 7.1 即证原题。

证法二：[1]将每位选手抽象为一个顶点，令两个顶点相邻当且仅当它们对应的选手之间下过一盘

---

[1] 感谢 xbz 网友给出这一证法。

棋。易于验证，所构成的图 G 是无向简单图。

反设各顶点的度数皆不相同，记其度数列(按降序排列)为 $d_n, d_{n-1}, \cdots, d_2, d_1$。则由题设有 $1 \leq d_1$，从而由 $1 \leq d_1 < d_2 < \cdots < d_n$ 和 $d_i(i = 1, 2, \cdots, n)$ 是整数可知 $d_n \geq n$。这与 G 是无向简单图矛盾。 □

7.5 G 有 2 种非同构的情况。证明如下。

先证两个引理。

引理 7.2 对任意简单图 G_1, G_2，有 $G_1 \cong G_2$ 当且仅当 $\overline{G}_1 \cong \overline{G}_2$。

证明: 选用同一个同构映射函数 f，由同构和同构映射函数定义立即得证。 □

引理 7.3 给定 r 个整数 $n_1, n_2, \ldots, n_r (r \geq 1)$，则在同构意义下，完全 r 部图 $K_{n_1,n_2,\ldots,n_r}$ 是唯一的。

证明: 任意两个完全 r 部图 $G = \langle V_1, V_2, \ldots, V_r, E\rangle$ 和 $G' = \langle V_1', V_2', \ldots, V_r', E\rangle$，若满足 $|V_i| = |V_i'| = n_i(i = 1, 2, \ldots, r)$，则由集合等势的定义和性质知，存在双射 $f : V(G) \to V(G')$，满足 $f(x) \in V_i' \leftrightarrow x \in V_i(i = 1, 2, \ldots, r)$。易于验证，这样的 f 满足同构映射的定义，故有，$G \cong G'$。

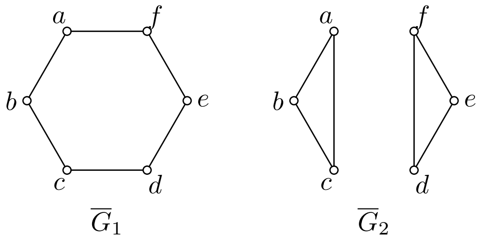
由 G 和 G' 选择的任意性知，当 $n_1, n_2, \ldots, n_r$ 确定时，所有完全 r 部图 $K_{n_1,n_2,\ldots,n_r}$ 皆同构。也即，在同构意义下，完全 r 部图 $K_{n_1,n_2,\ldots,n_r}$ 是唯一的。 □

再证原题。

由图论基本定理和 G 是 3-正则图知：$2m = 3n$。代入原式，解得 $n = 6$。

由引理 7.2 可知，要考虑 G 的同构情况，可以考虑 G 的补图的同构情况。

由于 G 是 6 阶 3-正则图，G 的补图必为 6 阶 2-正则图。下面证明任意 6 阶 2-正则图必与以下两个图之一同构，从而证明任意 6 阶 3-正则图必与以下两个图的补图(即 G_1 和 G_2)之一同构。



证明: 以上两图显然互不同构。

对任意 6 阶 2-正则图 G'：

情况一：若 G' 是连通的，则任取一个顶点 $v_1 \in V(G')$，令 $f(v_1) = a$，并从 v_1 的任意一条边出发，沿通路(由 G' 为 2 正则图知，这样的通路是唯一的)依次将通路上的顶点映射为 b, c, d, e, f。易于验证，$G' \cong \overline{G}_1$。

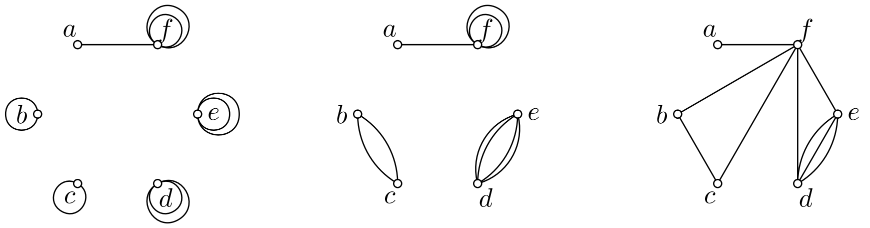
若 G' 不是连通的，则它至少有两个连通分支。又由于 G' 是简单图且每个顶点的度为 2 知，每个连通分支至少有 3 个顶点。结合 $|V(G)| = 6$，得，G' 有且仅有两个连通分支，且这两个连通分支都是 K_3。由引理 7.3 和这两个连通分支的对称性易知，$G' \cong \overline{G}_2$。

综上所述，我们有：任意 6 阶 3-正则图的补图必为 6 阶 2-正则图，任意 6 阶 2-正则图必与 $\overline{G}_1$ 和 $\overline{G}_2$ 之一同构。由引理 7.2 可知，任意 6 阶 3-正则图必与 G_1 或 G_2 同构。 □

7.6

(1) 度数和为偶数，可图化。

(2) 度数和为奇数，不可图化。



G_1 G_2 G_3

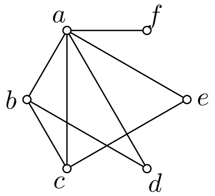
题7.6 (1)图

7.7

(1) $(6,6,5,5,3,3,2) \Leftrightarrow (5,4,4,2,2,1) \Leftrightarrow (3,3,1,1,0) \Leftrightarrow (2,0,0,0)$，不可简单图化。

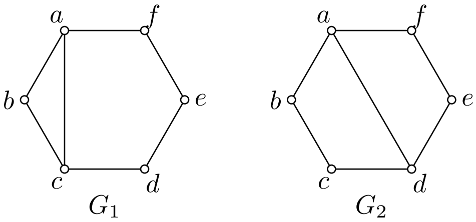
(2) $(5,3,3,2,2,1) \Leftrightarrow (2,2,1,1,0) \Leftrightarrow (1,0,1,0) \Leftrightarrow (1,1,0,0)$，可简单图化(且在同构意义下，这样的图是唯一的)。

(3) $(3,3,2,2,2,2) \Leftrightarrow (2,1,1,2,2) \Leftrightarrow (2,2,2,1,1) \Leftrightarrow (1,1,1,1)$，可简单图化。



G

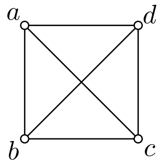
题7.7(2)图



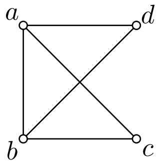
G_1 G_2

题7.7(3)图

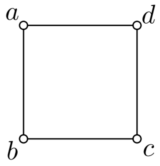
7.8



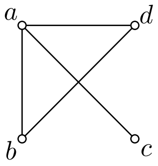
G_1



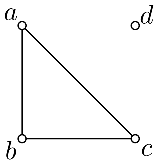
G_2



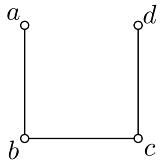
G_3



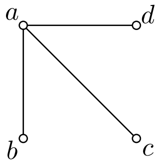
G_4



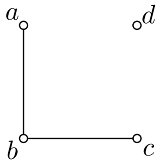
G_5



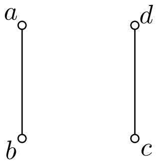
G_6



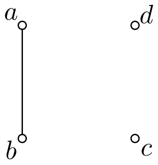
G_7



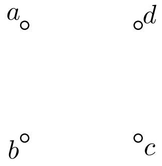
G_8



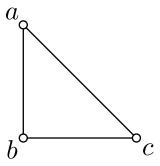
G_9



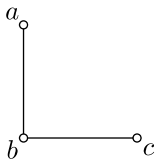
G_{10}



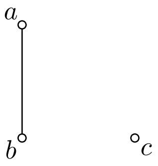
G_{11}



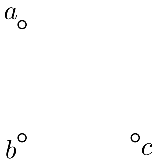
G_{12}



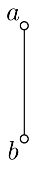
G_{13}



G_{14}



G_{15}



G_{16}

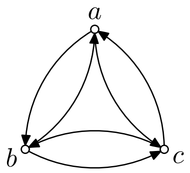
G_{17}

G_{18}

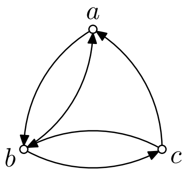
G_{19}

其中 G_1 到 G_{11} 是 K_4 的生成子图。G_6, G_{18}, G_{19} 是自补图。

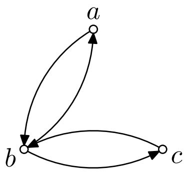
7.9



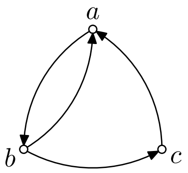
G_1



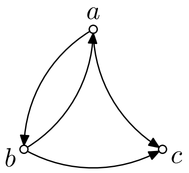
G_2



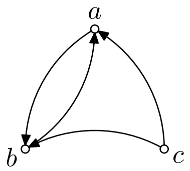
G_3



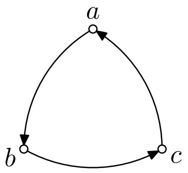
G_4



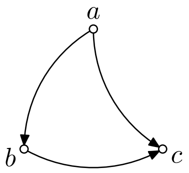
G_5



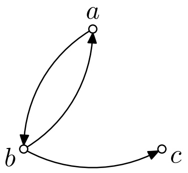
G_6



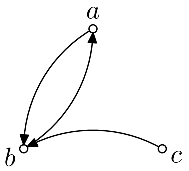
G_7



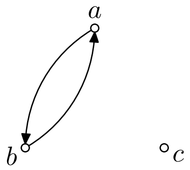
G_8



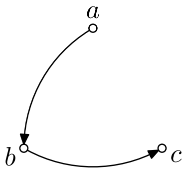
G_9



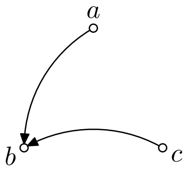
G_{10}



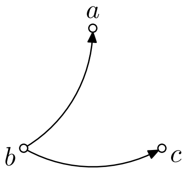
G_{11}



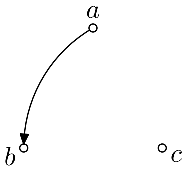
G_{12}



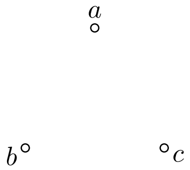
G_{13}



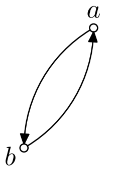
G_{14}



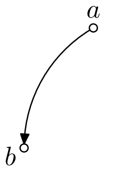
G_{15}



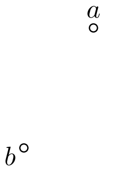
G_{16}



G_{17}



G_{18}



G_{19}

G_{20}

G_{21}

其中 G_1 到 G_{16} 是生成子图。$G_7, G_9, G_{10}, G_{18}, G_{20}, G_{21}$ 是自补图。

7.10

证明: 习题 7.8 中已经列出了 3 个边数为 3 且互不同构 4 阶简单无向图 G_5, G_6, G_7。下面证明，在同构意义下，边数为 3 的 4 阶无向简单图只有上述 3 个。

设 G 为任意边数为 3的 4 阶无向简单图。

(1) 若 $\delta(G) \geq 1$。则 G 的(非增序)度数列只能有：$3, 1, 1, 1$ 和 $2, 2, 1, 1$ 两种。对这两种情况，只需按对应的度数选择同构映射即可证明，它们分别同构于 G_7 和 G_6。

(2) 若 $\delta(G) = 0$。则 G 的(非增序)度数列只能是：$2, 2, 2, 0$。此时，G 同构于 G_5。

因此，在同构意义下，边数为 3 的 4 阶简单无向图只有 G_5, G_6, G_7 三个。由鸽巢原理知，5 个这样的图中必有两组同构(有可能是 $G_i \cong G_j \cong G_k$ 的形式，也可能是 $G_i \cong G_j \wedge G_k \cong G_m$ 的形式，其中 i, j, k, m 是小于等于 5 的互异正整数)。 □

7.11

证明: 设无向图[2] G 是一自补图。由自补图定义知，$|E(\overline{G})| = |E(G)|$ 且 $|E(\overline{G})| + |E(G)| = |E(K_n)| = n(n-1)/2$。解得 $|E(G)| = n(n-1)/4$。

由 $|E(G)|$ 是整数知，$4 \mid n(n-1)$。由于 n 和 $n-1$ 中必有一个是奇数，故 4 整除另一个数，即有 $4 \mid n$ 或 $4 \mid n-1$。从而有：$n = 4k$ 或 $n = 4k+1$。 □

7.12

证明: 从 G 中任选一个顶点，记为 v_1。由鸽巢原理知，G 的其它 5 个顶点中，要么至少有 3 个与 v_1 相邻，要么至少有 3 个与 v_1 不相邻(即，在 $\overline{G}$ 中 v_1 与它们相邻)。

由对称性，不妨设至少有 3 个顶点在 G 中与 v_1 相邻，将这 3 个顶点分别记为 v_2, v_3, v_4。

(1) 若这 3 个顶点互不相邻，则这 3 个顶点在 $\overline{G}$ 中就是彼此相邻的 3 个顶点。所证命题成立。

(2) 若这 3 个顶点中有相邻的顶点，则这对相邻的顶点与 v_1 一起就构成了 G 中彼此相邻的 3 个顶点，命题同样成立。 □

7.13

证明: 反设 G 中仅有的两个奇度顶点分属的 G 的两个不同的连通分支 G_1 和 G_2，那么 G_1 中只有一个奇度顶点，从而 $\sum\limits_{v \in G_1} d(v)$ 是奇数，与图论基本定理矛盾。 □

7.14 首先证明：

引理 7.4 *对任意图(有向或无向) G，若有*

$$\forall u, v, w \in V(G)((u,v),(v,w) \in E(G) \Rightarrow (u,w) \in E(G))$$

(若为有向图，则将引理中的无序对换成有序对即可)，则该图的每一个(强)连通分支都是完全图。

证明: 只需证：$\forall (u, v \in V(G), u \neq v \wedge u \sim v \to (u,v) \in E(G))$ 为永真即可。

设 $\Gamma = w_0 w_1 \cdots w_{k-1} w_k$ 是 u 到 v 的一条最短通路 (其中 $w_0 = u$，$w_k = v$)。由于 $(u,v) \notin E(G)$，所以 $k \geq 2$。反设 $\forall u, v, w \in V(G)((u,v),(v,w) \in E(G) \implies (u,w) \in E(G))$。则由 $(w_0, w_1), (w_1, w_2) \in E(G)$ 就可推出 $(w_0, w_2) \in E(G)$，从而 $\Gamma' = w_0 w_2 \cdots w_{k-1} w_k$ 是一条更短的通路。矛盾。

上述证明中并未用到无序对的可交换性。因此，该证明对有向图的情形同样有效。 □

再证原题。

证明: 若不然，由 G 是连通图和引理 7.4 可知，G 是完全图，矛盾。 □

7.15

证明: 构造一“极大路径” $\Gamma = v_0, v_1, \ldots, v_l$。由 Γ 是极大路径知，v_0 的所有邻接点都在 Γ 上。由 $\delta(G)$ 定义知，至少存在 $\delta(G)$ 个顶点 $v_{i_1}, v_{i_2}, \ldots, v_{i_{\delta(G)}} (i_1 < i_2 < \ldots < i_\delta(G))$ 与 v_0 相邻。且由 $\delta(G) \geq 2$ 知，$\delta(G) \neq 1$。从而由 Γ 是初级通路知，$v_{i_1} \neq v_{i_{\delta(G)}}$。于是有 $(v_{i_{\delta(G)}}, v_0)$ 不在 Γ 上。因此，$v_0, v_1, \ldots, v_{i_{\delta(G)}}, v_0$ 即为一个长度大于等于 $\delta(G)+1$ 的圈。 □

7.16

证明: 构造一个“极大路径” $\Gamma = v_0, v_1, \ldots, v_l$。

由 Γ 是极大路径知，v_0 的所有邻接点都在 Γ 上。

由 $\delta(G) \geq 3$ 可知，除 v_1 外，至少还有两个顶点 $v_i, v_j (2 \leq i < j \leq l)$ 与 v_0 相邻。

---

[2] 本题中的 G 必须是无向图。当 G 为有向图时，上述结论不成立。第 9 题中的 3 阶有向自补图 G_7 和 2 阶有向自补图 G_{18} 便是反例。

于是，$v_0, v_1, \ldots, v_i, v_0$ 是一个长度为 $i+1$ 的圈，$v_0, v_1, \ldots, v_j, v_0$ 是一个长度为 $j+1$ 的圈，$v_0, v_i, \ldots, v_j, v_0$ 是一个长度为 $j-i+2$ 的圈。

令 d 为 G 中各圈长度的最大公约数。则有 $d \mid i+1$、$d \mid j+1$ 和 $d \mid j-i+2$，于是有 $d \mid (i+1)+(j-i+2)-(j+1)=2$ (d 的倍数的和、差仍是 d 的倍数)。

由 $d \mid 2$ 和因子的定义可知 d 等于 1 或 2。 □

7.17

证明： 若 G 不连通，则由定义知 $\kappa(G)=0$。由习题 7.18 第 (1) 小题结论可知，$n-2 \le \delta(G) < \dfrac{n}{2}$，从而有 $2n-4<n$，即 $n<4$。由于 G 不连通，所以 $p(G) \ge 2$。

反设 G 中没有孤立顶点，则 G 的每个连通支都将有 2 个或 2 个以上顶点，从而 $n \ge 2p(G) \ge 4$，这与 $n<4$ 矛盾。这就是说，G 中必有孤立顶点。从而 $\delta(G)=\kappa(G)=0$。命题成立。

若 G 为连通图，则由简单图性质知，$\delta(G) \le \Delta(G) \le n-1$。结合题设可知，$\delta(G)$ 只有两个可能的取值：$n-1$ 和 $n-2$。

当 $\delta(G)=n-1$ 时，易证 G 是完全图。由定义知，$\kappa(G)=\delta(G)=n-1$。命题成立。

当 $\delta(G)=n-2$ 时，由教材定理 7.10 知 $\kappa(G) \le \delta(G) = n-2$，又由教材定理 7.13 知 $\kappa(G) \ge 2\delta(G)-n+2=n-2$，综合即得 $\kappa(G)=\delta(G)=n-2$。命题依然成立。 □

7.18

(1)

证明： 注意到，对任意 $v \in V(G)$，v 所在的连通分支至少有 $d(v)+1 \ge \delta(G)+1$ 个顶点。若 G 不连通，则 G 至少有 $p(G)=k \ge 2$ 个连通分支 $V_1, V_2, \cdots, V_k$，从而

$$\begin{aligned}
|V(G)| &= \sum_{i=1}^{k}|V_i| && \text{(连通分支是 } V(G) \text{ 的划分)}\\
&\ge k(\delta(G)+1) && (|V_i| \ge \delta(G)+1)\\
&\ge k(\frac{n}{2}+1) && \text{(题设)}\\
&\ge 2(\frac{n}{2}+1) && (k \ge 2\text{、}\frac{n}{2}+1 \ge 0)\\
&= n+2 && \text{(乘法分配律)}\\
&> n
\end{aligned}$$

矛盾。从而必有 $k=1$，G 是连通图。 □

(2)

证明： 设 V_1 是 G 的最小点割集，记 $t=|V_1|$。

注意到，由于 G 是简单图，所以从 G 中每删去一个顶点，最多使 G 中剩余各顶点的度数减 1。从而

$$\delta(G-V_1) \ge \delta(G)-|V_1| \ge \frac{n+k-1}{2}-t$$

另一方面，由 $G-V_1$ 不连通和第 (1) 小题结论应有

$$\delta(G-V_1) < \frac{|V(G-V_1)|}{2} = \frac{n-t}{2}$$

综合两式可得：

$$\frac{n+k-1}{2}-t < \frac{n-t}{2}$$

即，$t>k-1$，$t \ge k$。由定义知，G 是 k-连通图。 □

7.19[3]

(1)

证明: 任取 $v_1 \in V(G)$，再取 $v_2 \in N_G(v_1)$ 。则 $N_G(v_1) \cap N_G(v_2) = \varnothing$ (若不然，则它们交集中的顶点将与 v_1 和 v_2 构成一个长度为 3 的圈，这与 G 的围长是 4 矛盾)，而 $|N_G(v_1)| = |N_G(v_2)| = k$，故 G 中至少有 $|N_G(v_1) \cup N_G(v_2)| = |N_G(v_1)| + |N_G(v_2)| - |N_G(v_1) \cap N_G(v_2)| = 2k$ 个顶点。 □

(2)

证明: 先证明 G 是完全二部图 $K_{k,k}$。

按 (1) 中所述的方法选择 v_1, v_2 并构造 $N_G(v_1), N_G(v_2)$。

用 (1) 的结论，我们知道，$N_G(v_1) \cap N_G(v_2) = \varnothing$ 且 $|N_G(v_1)| = |N_G(v_2)| = k$，于是有 $|N_G(v_1) \cup N_G(v_2)| = |N_G(v_1)| + |N_G(v_2)| = 2k = |V(G)|$。也即，$N_G(v_1) \cup N_G(v_2)$ 包括了 G 中所有顶点。

现在证明，在同一顶点集中的两个顶点不相邻。

若不然，则有两个相邻的 u_1, u_2 属于同一个 $N_G(v_i)(i = 1, 2)$。由对称性，不妨设 $u_1, u_2 \in N_G(v_1)$，则由它们在 $N_G(v_1)$ 知它们都与 v_1 相邻，而它们之间也相邻，则 v_1, u_1, u_2, v_1 就是一个长度为 3 的圈，这与 G 的围长为 4 矛盾。

可见，同一个 $N_G(v_i)(i = 1, 2)$ 都不相邻。但由 G 是 k-正则图知，每个顶点都有 k 个邻接点，结合上述两个条件知，$N_G(v_1)$ 中的每一个顶点都是 $N_G(v_2)$ 中的每一个顶点相邻，反之亦然。

由上述论证可知，G 是完全二部图 $K_{k,k}$。再由引理 7.3 知，这样的 G 在同构意义下是唯一的。 □

7.20

证明: 令 v 是 G 中度最大的顶点。

由 $\Delta(G) = n - 2$ 知，G 中有一个顶点与 v 不相邻，将这个顶点记作 u。

由 $d(G) = 2$ 知，G 中的任何一个顶点，至多只需途经一个顶点就可以到达 u。而途经的这一个顶点不可能是 v (因为 u 与 v 之间没有边)。也就是说，$V(G) - \{u, v\}$ 中的任何一个顶点都可以不经过 v 而到达 u。

令 $G' = G - v$，则 G' 是连通的 (因为 $V(G') - \{u\}$ 中所有的顶点都有到达 u 的通路)，由教材定理 7.9 可知，$|E(G')| \geq |V(G')| - 1 = n - 2$，而 G' 比 G 少 $n - 2$ 条边。于是有 $m = |E(G)| = E(G') + n - 2 \geq 2n - 4$。 □

7.21 先证一个引理。

引理 7.5 *若一个 n 阶无向图 G 不含圈，则必有 $|E(G)| = n - p(G)$，其中 $p(G)$ 是 G 中的连通分支数。*

证明: 对 n 做归纳。

当 $n = 1$ 时，命题显然成立。

设 $n = i$ 时，命题成立，下面证明 $n = i + 1$ 时命题也成立。

设 $|V(G)| = i + 1$，且 G 不含圈。令 $x = |E(G)| + p(G)$，下面证明 $x = i + 1$。

任取一个顶点 $v \in V(G)$，令 $G' = G - I_G(v)$。由 G 中无圈和教材定理 7.18 知，G 中任何一条边都是桥，因此，删去的边数恰好等于增加的连通分支数。从而有

$$x = |E(G)| + p(G) = |E(G')| + p(G')$$

令 $G'' = G' - v$。注意到，v 在 G' 中是孤立顶点。从而有 $p(G'') = p(G') - 1$ 和 $|E(G'')| = |E(G')|$。注意到，$|V(G'')| = i$。由归纳假设知 $E(G'') = i - p(G'')$。代入前式即得 $x = |E(G')| +$

---

[3] 感谢南京大学02级计算机系赖江山同学给出第 19、20 题的证明。

$p(G') = |E(G'')| + p(G'') + 1 = i + 1$，也即 $|E(G)| = (i+1) - p(G)$。这就证明了，当 $n = i + 1$ 时命题同样成立。 □

再证原题。

证明: 若 G 为空图，则命题显然成立。若 G 非空，则至少存在一个连通分支，由引理 7.5 可知，G 中若不含圈，则至多有 $n-1$ 条边，即有 $m < n$，这与题设 $m \geq n$ 矛盾。故，G 中必含圈。 □

7.22

证明: 由块的定义知，顶点数为 2 的块只有 K_2。

对任意顶点数大于或等于 3 的块 B，由教材定理 7.20 知，B 中有圈 C。下面证明 B 的所有顶点和所有边都在 C 上。

若 B 中存在边 $e' = (u', v') \notin E(C)$，则任取 C 中一边 $e = (u, v) \in E(C)$，由教材定理 7.20 知，存在一个过 e 和 e' 的圈 C'。由于 $(u, v) \in E(C) \cap E(C')$，故 $|V(C) \cap V(C')| \geq 2$。从 e' 出发，分别向 C' 两侧扩展，直到遇到第一个属于 $V(C) \cap V(C')$ 的顶点，分别记它们为 s 和 t (每侧一个，且必有 $s \neq t$，否则将与 $|V(C) \cap V(C')| \geq 2$ 矛盾)。如此，得到 C' 上的一条路径 $\Gamma = s \cdots t$。注意到，Γ 与 C 无公共边。而 s 和 t 将 C 分成两段，记为 Γ_1 和 Γ_2。由题设，G 中无偶圈，故 $|E(\Gamma_1)| + |E(\Gamma_2)| = |E(C)|$ 为奇数。从而 $|E(\Gamma_1)|$ 与 $|E(\Gamma_2)|$ 的奇偶性不同。令 $C_1 = \Gamma_1 \cup \Gamma, C_2 = \Gamma_2 \cup \Gamma$，则它们是奇偶性不同的两个圈。这与 G 中无偶圈矛盾。故，B 中所有的边都在 C 上。

又由块的连通性知，若存在不在 C 上的点 v，则必有与 v 相邻的边 e'，且 $e' \notin C$，与上面的结论矛盾。

由此知，$V(B) = V(C), E(B) = E(C)$，即有 $B = C$，是奇圈。 □

7.23 令 $n = 4r, \delta = s, \lambda = r, \kappa = 1$，则由教材定理 7.14(1) 立即得证。

7.24

(1) 将习题 7.12 的 G 和 $\overline{G}$ 换成红、蓝两色边即可得证。

(2) 直接利用习题 7.12 的结论即可。

(3)

证明: 将这个“与 6 条或更多条红色边关联”的顶点记作 v_1，这 6 条边的另一端所连接的 6 个顶点构成 K_n 的一个 6 阶子图 H。显然，$H \cong K_6$。

由 (1) 的结论知，H 中必有红色的 K_3 或蓝色的 K_3。

若存在蓝色的 K_3，则命题成立。

若存在红色的 K_3，则这 3 个顶点与 v_1 就构成了红色的 K_4，命题同样成立。 □

7.25

证明: 由引理 7.4 知，若 D 是强连通的，则 D 是有向完全图。这与题设“D 为竞赛图”矛盾。故得，原命题成立。 □

第八章　欧拉图与哈密顿图

8.1

证明: 由于 G 是欧拉图，所以存在欧拉回路 $C = e_{i_1}e_{i_2}\cdots e_{i_m}$。由定义，$G$ 中所有顶点都在 C 上，且对任意 $e \in E(G)$，存在唯一的 $1 \le k \le m$，使得 $e_{i_k} = e$。从 C 中删除 e_{i_k} 后，得到一条通过所有顶点的通路 $\Gamma = e_{i_{k+1}}\cdots e_{i_m}e_{i_1}\cdots e_{i_{k-1}}$。显然，这条通路在 $G - e$ 中，从而 $G - e$ 是连通图。由 e 的任意性可知 $\lambda(G) \ge 2$，从而 G 是 2 边-连通的。 □

8.2　先证明一些有关“块”的性质。

引理 8.1 设 G 为无向连通图，$\mathscr{B} = \{B_1, B_2, \cdots, B_k\}$ 为 G 中所有不同的块的集合，记 $V_i = V(B_i)$，$E_i = E(B_i)$，$i = 1, 2, \cdots, k$。设 $B_i, B_j \in \mathscr{B}$，$B_i \ne B_j$ 是 G 的两个不同的块，则

(1)　$B_i = G[V_i]$;

(2)　$V_i \nsubseteq V_j$;

(3)　$|V_i \cap V_j| \le 1$;

(4)　对 G 的任意阶数不小于 2 的子图 $H = \langle V', E' \rangle$，若 H 中不含割点，则 H 必被包含于唯一的一个块中。

(5)　$E_i \cap E_j = \{(v, v) \mid v \in V_i \cap V_j \wedge (v, v) \in E(G)\}$;

(6)　$G = \cup\mathscr{B}$。

证明:

(1)　当顶点集不变的情况下，向一个图中加入新边不会降低图的连通度，从而由块的极大性即可得证。

(2)　反设 $V_i \subseteq V_j$，则由结论 (1) 可知，$B_i = G[V_i] \subseteq G[V_j] = B_j$，又由于 $B_i \ne B_j$，所以有 $B_i \subset B_j$，即，B_j 是比 B_i 更大的 2-连通子图，这与 B_i 的极大性矛盾。

(3)　若不然，不妨设 $v_1, v_2 \in V_i \cap V_j$，$v_1 \ne v_2$。此时，对任意 $u \in V_i - \{v_1, v_2\}$ 和 $w \in V_j - \{v_1, v_2\}$，必存在从 u 到 w 且不经过 v_1 的通路 Γ_1 和从 u 到 w 且不经过 v_2 的通路 Γ_2。这是因为，由教材定理 7.20 (注意到，教材定理 7.20 的前提“$|V_i| \ge 3$”和“$|V_j| \ge 3$”必然成立。否则，不妨设 $|V_i| \le 2$，则由假设 $|V_i \cap V_j| \ge 2$ 就可推出 $V_i = V_i \cap V_j \subseteq V_j$，这与结论 (2) 矛盾)可知，在 B_i 中存在由 u 到 v_2 而不过 v_1 的通路，在 B_j 中存在由 v_2 到 w 而不经过 v_1 的通路，连接两段通路即得 Γ_1，同理可以得到 Γ_2。因此，$B_i \cup B_j$ 是 2-连通的(因为从 $B_i \cup B_j$ 删除任意顶点后，B_i 和 B_j 内部必然仍是连通的，而由于 v_1 和 v_2 不可能同时被删去，所以 B_i 和 B_j 之间仍有通路，从而 $B_i \cup B_j$ 仍是连通的)。但由结论 (2) 可知，V_i 和 V_j 都是 $V_i \cup V_j$ 的真子集(由习题 1.32 第 (2) 小题可知，$V_i \cup V_j = V_i$ 当且仅当 $V_j \subseteq V_i$，$V_i \cup V_j = V_j$ 当且仅当 $V_i \subseteq V_j$，而由结论 (2) 可知，以上两种情况都不可能出现)，从而 $B_i \cup B_j$ 是比 B_i 和 B_j 都大的 2-连通子图，这与 B_i, B_j 的极大性矛盾。

(4)　由于 H 中不含割点，所以由 H 的顶点集导出的子图 $G[V']$ 也不含割点。如果存在某个顶点 $v \in V(G) - V'$，使得 $G[V' \cup \{v\}]$ 仍无割点，则将 v 加入 V' 中，直止不再存在这样的 v。此时，$G[V']$ 就是 G 的一个块且 $H \subseteq G[V']$，记 $B_s = G[V']$。

反设还存在另一个块 $B_t \in \mathscr{B}$，$B_t \neq B_s$ 且 $H \subseteq B_s \cap B_t$，则由 $|V(H)| \geq 2$ 可知，$|V(B_s) \cap V(B_t)| \geq 2$。这与结论 (3) 矛盾。这就是说，$H$ 只会被包含在唯一的一个块中。

(5) 对任意 $e = (x, y) \in E_i \cap E_j$，应有 $x, y \in V_i \cap V_j$，但由结论 (3) 可知，$V_i \cap V_j$ 中至多有 1 个顶点。所以就有 $x = y$。也即，$e = (x, x)$ 是环。反过来，设 $v \in V_i \cap V_j$，由结论 (1) 可知，若 $(v, v) \in E(G)$，则有 $(v, v) \in E_i \cap E_j$。

(6) $\cup\mathscr{B} \subseteq G$ 是显然的。下面证 $G \subseteq \cup\mathscr{B}$。

首先证明 G 中每一条非环的边都在 $\cup\mathscr{B}$ 中。对任意非环的边 $e = (u, v) \in E(G)$，$u \neq v$，由 (u, v) 导出的子图 $H = G[\{(u, v)\}$ 是 2 阶图，且没有割点，从而由结论 (4) 可知，H 在 G 的某个块 B_s 中，从而 $e \in E(B_s) \subseteq E(\cup\mathscr{B})$。

下面证明 $V(G) \subseteq V(\cup\mathscr{B})$。由于 G 是连通图，所以 G 中每个顶点 v 至少与一个非环的边相关联，而前面已经证明，每条非环的边都在 $\cup\mathscr{B}$ 中，从而 v 也在 $\cup\mathscr{B}$ 中。这就证明了 $V(G) \subseteq V(\cup\mathscr{B})$。

最后说明，G 中的每一个环也在 $\cup\mathscr{B}$ 中。设 $(v, v) \in E(G)$ 是 G 中任意一个环。前面已知，$v \in V(\cup\mathscr{B})$，也即，存在某个 $B_s \in \mathscr{B}$，使得 $v \in V(B_s)$。由结论 (1) 即有，$(v, v) \in E(B_s) \subseteq E(\cup\mathscr{B})$。。

这就证明了 $G \subseteq \cup\mathscr{B}$，从而有 $G = \cup\mathscr{B}$。 □

再证原题。

证明： 充分性。

不妨设 G 中共有 k 个块，分别是 $B_1, B_2, \cdots, B_k$。若 G 的每个块都是欧拉图，则由教材定理 8.1 可知，对 G 的每一个块 B_i，都存在若干个边不重的圈 $S_i = \{C_{i_1}, C_{i_2}, \cdots, C_{i_{n_i}}\}$，使得 $B_i = \cup S_i$。令 $S = \bigcup\limits_{i=1}^{n} S_i$，由引理 8.1(6) 可知，$G = \cup S$。下面证明，$S$ 中的各圈也是边不重的。

设 $C_{i_j}, C_{s_t} \in S$，$C_{i_j} \neq C_{s_t}$ 是 S 中两个不同的圈。若 $i = s$，则 C_{i_j} 和 C_{s_t} 同属一个块，而由前提，它们应该是边不重的。若 $i \neq s$，则由引理 8.1(5) 可知，若它们有公共边，则公共边只能是环。但，如果一个圈 C' 中含有环 (x, x)，则 C' 只能是环本身，即 $C' = (x, x)$ (否则，x 将在 C' 中连续出现两次，这与圈的定义矛盾)。这就是说，如果 C_{i_j} 与 C_{s_t} 有公共边 e，则 $e = (x, x)$ 必为环，且 $C_{i_j} = C_{s_t} = G[\{e\}]$。这与前提 $C_{i_j} \neq C_{s_t}$ 矛盾。

这就证明了 $G = \cup S$ 是若干个边不重的圈的并，从而由教材定理 8.1 可知，G 是欧拉图。

必要性。

若 G 是欧拉图，则由教材定理 8.1 可知，G 是若干个边不重的圈的并，记这些圈为 $S = \{C_1, C_2, \cdots C_r\}$。设 B_i 为 G 的任意一个块，令 $S_i = \{C_j \mid C_j \in S \wedge E(C_j) \cap E(B_i) \neq \varnothing\}$。显然，$S_i$ 中的圈都是边不重的。下面证明 $B_i = \cup S_i$。

首先证明 $B_i \subseteq \cup S_i$。这是因为，B_i 的每条边 $e \in E(B_i)$ 都在某个圈 C_j 中(因为 $G = \cup S$)，而由定义有 $C_j \in S_i$。所以有 $e \in E(C_j) \subseteq E(\cup S_i)$。这就是说，$E(B_i) \subseteq \cup S_i$。而 B_i 是连通的，所以每个顶点 v 至少关联于一条边 $e \in E(B_i) \subseteq E(\cup S_i)$，从而有 $v \in V(\cup S_i)$。也即 $V(B_i) \subseteq V(\cup S_i)$。这就证明了 $B_i \subseteq \cup S_i$。

下面证明 $\cup S_i \subseteq B_i$。若不然，就存在 $C_j \in S_i$，且 $C_j \nsubseteq B_i$。由 S_i 的定义，应当存在某条边 $e = (u, v) \in E(C_j) \cap E(B_i)$。注意到 e 不可能是环(因为如果 e 是环，则必有 $C_j = e$。从而由 $C_j \cap B_i \neq \varnothing$ 可知，$e \in E(B_i)$，$\{e\} = C_j \subseteq B_i$，矛盾)，所以必有 $u \neq v$。由引理 8.1(6) 可知，C_j 应当在某个块 B_s 之中(显然，$B_s \neq B_i$)，从而有 $(u, v) \in E(B_i) \cap E(B_s)$，$u, v \in V(B_i) \cap V(B_s)$，而这与引理 8.1(3) 矛盾。

这就证明了 $B_i = \cup S_i$ 是若干个不相交的圈的并。由 B_i 的任意性和教材定理 8.1 可知，G 的每一个块都是欧拉图。 □

8.3

证明： 记这 $2k$ 个奇数度顶点为 $v_1, v_2, \cdots, v_{2k}$，令 $E' = \{(v_{2i-1}, v_{2i}) \mid i = 1, 2, \cdots, k\}$，$G' = G \cup E'$。注意到，$G'$ 是连通图且每个顶点都是偶数度，由教材定理 8.1，G' 中存在欧拉回路 C'。从 C' 中删去 E'，则 C' 将被划分为 k 段(由于可能出现 E' 中的两条边在 C' 中相邻的情况，所以这 k 段中可能存在“空段”)，设其中有 t 个“非空段” $P_1, P_2, \cdots, P_t$ $(1 \leq t \leq k)$。显然，它们是 t 条边不重的简单通路，且 $E(G) = \bigcup\limits_{i=1}^{t} E(P_i)$。注意到，对任意一条简单通路 P_i，若它的长度为 n_i，则对任意正整数 $1 \leq s \leq n_i$，可以将 P_i 分割成 s 条边不重简单通路(将 P_i 的前 $s-1$ 条边看成 $s-1$ 条简单通路，剩下的 $n-s+1$ 条边看成第 s 条简单通路即可)。从而上述 t 条简单通路可以根据需要被分割成 $s(t \leq s \leq m)$ 条边不重的简单通路，其中 m 是 G 的边数。由于 G 是连通的，且 G 中至少有 $2k$ 个顶点，$k \geq 1$，所以 $m \geq n-1 \geq 2k-1 \geq k$。因此，总能将上述 t 条简单通路分割成 k 条边不重的简单通路 $P'_1, P'_2, \cdots, P'_k$，且有 $E(G) = \bigcup\limits_{i=1}^{k} E(P'_i)$。 □

8.4 首先注意到下述事实。

引理 8.2 设 G 是一个无向图，$G_1 = G[V_1]$ 是 G 的一个连通分支，则对任意 $v \in V_1$，有 $d_{G_1}(v) = d_G(v)$。

证明： 由于 $E(G_1) \subseteq E(G)$，所以显然有 $d_{G_1}(v) \leq d_G(v)$。假设 $d_{G_1}(v) < d_G(v)$，则存在某条边 $(u, v) \in E(G)$，使得 $(u, v) \notin E(G_1)$。但由于 u 与 v 之间有通路且 $v \in V_1$，所以应有 $u \in V_1$。又因为 $G_1 = G[V_1]$ 是由 V_1 生成的子图，所以应有 $(u, v) \in E(G_1)$，矛盾。 □

再证原题。

证明： 必要性。

反设 $G - v_0$ 中有圈，我们将证明 v_0 不是可以任意行遍的。

首先，由于 G 是欧拉图，由教材定理 8.1 可知，G 中每个顶点都是偶数度的。假设 $G - v_0$ 中有圈 C_0，则令 $G' = G - E(C_0)$。注意到，圈中每个顶点都是 2 度的。所以，对任意 $v_i \in V(G)$，若 $v_i \in V(C_0)$，则 v_i 在 G' 中的度数 $d_{G'}(v_i) = d_G(v_i) - 2$。若 $v_i \notin V(C_0)$，则 $d_{G'}(v_i) = d_G(v_i)$。总之，G' 中的每个顶点仍为偶数度的。特别地，由于 $v_0 \notin V(C_0)$，所以 $d_{G'}(v_0) = d_G(v_0) > 0$。

设 G_1 是 v_0 在 G' 中所处的连通分支。由引理 8.2，G_1 中每个顶点仍是偶数度的。由教材定理 8.1 可知，G_1 是欧拉图。记 C_1 是 G_1 中的一条欧拉回路，注意到，C_1 中包含了所有与 v_0 关联的边。

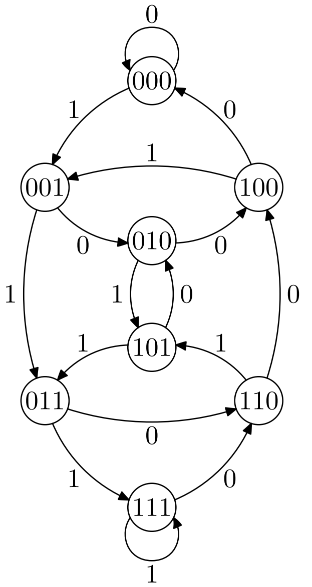
若在 G 中，从 v_0 出发，按 C_1 的轨迹进行行遍，则当 C_1 行遍完成，回到 v_0 时，已无可行遍的边。注意到，此时 G 中还有未被行遍的边(例如 C_0 中的边)，这就是说，按此方法行遍，得到的回路 C_1 不是 G 的一条欧拉回路。从而 v_0 不是可以任意行遍的。

充分性。

假若 v_0 不是可以任意行遍的，我们将证明，$G - v_0$ 中有圈。

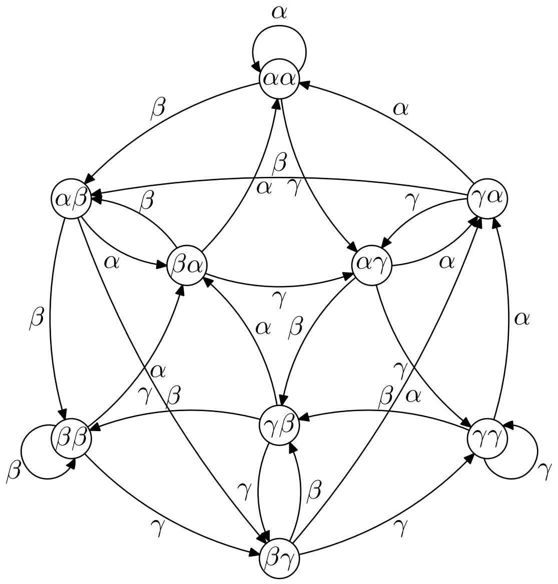
由于 v_0 不是可以任意行遍的，所以存在某条行遍路线，使得行遍过程终止于顶点 v_0 (行遍过程必然终止于 v_0。若不然，假设停在某个顶点 $v_i \neq v_0$ 上，则这个行遍路线将是一条从 v_0 到 v_i 的简单路径 Γ，设 v_i 在路径上共出现过 t 次，则前 $t-1$ 次出现中，每次出现会使 v_i 在 Γ 中的度数加 2，最后一次出现则仅使 v_i 在 Γ 中的度数加 1，从而 v_i 在 Γ 中的度数是奇数。这就是说，$E(G)$ 中还有与 v_i 关联且未被行遍的边，这与行遍过程的终止条件矛盾)，构成一个简单回路 C，且 $G' = G - E(C)$ 中仍有边。注意到，G' 中各顶点的度数仍为偶数。设 G_1 是 G' 中某个非平凡的(即，有边的)连通分支，由引理 8.2，G_1 中各顶点的度数也是偶数。从而教材定理 8.1可知，G_1 是若干个边不重的圈(不妨记为 $C_1, C_2, \cdots C_k$)的并。任取一个圈 C_1，注意到，v_0 不在 C_1 中(因为 v_0 在 G' 中是孤立点)，从而 $C_1 \subseteq G - v_0$。 □

8.5　按教材示例构造状态转移图如下(为方便起见，在图中只写每条边编号中的最后一位，如边 1110 在图中记成 0)：



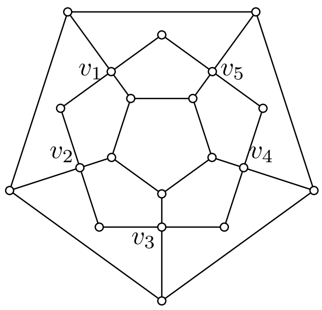
任取一条欧拉回路，如(从顶点 000 开始，仍只写边的最后一位) 0100110101111000。它所对应的就是一个可行的排列方案。

8.6　按教材示例构造状态转移图如下：

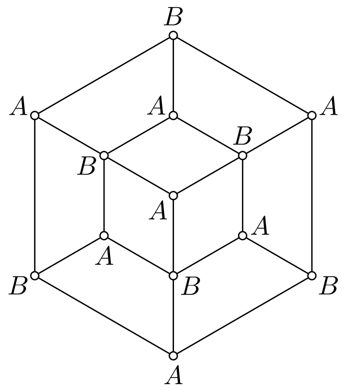


任取一条欧拉回路，如(从顶点 $\alpha\alpha$ 开始) $\alpha\beta\gamma\alpha\beta\alpha\gamma\beta\alpha\beta\beta\beta\alpha\alpha\gamma\gamma\gamma\beta\beta\gamma\beta\gamma\gamma\alpha\gamma\alpha\alpha$。它所对应的就是一个可行的排列方案。

8.7



(a)



(b)

证明:

(a) 删除图中所有的 4 度顶点(即上图中标记为 $v_1, v_2, \cdots, v_5$ 的顶点)，则原图将成为一个有 7 个连通分支的非连通图。由教材定理 8.6 可知，此图不是哈密顿图。

(b) 令 X 为上图中所有标记为 A 的顶点构成的集合，令 Y 为图中所有标记为 B 的顶点构成的集合。易见，$G = \langle X, Y, E\rangle$ 是一个二部图。注意到，G 中共有 13 个顶点。反设 G 是哈密顿图，则图中存在一个长度为 13 的圈，这与教材定理 7.8 矛盾。 □

8.8 证明繁琐，暂略。

8.9

证明: 设 G 为 n 阶无向简单图，边数 $m = \frac{1}{2}(n-1)(n-2)+2$。首先由于 G 是简单图，所以有 $\frac{1}{2}(n-1)(n-2)+2 = m \le \frac{1}{2}n(n-1)$，解得，$n \ge 3$。

下面证明，对 G 中任意两个不相邻的顶点 $u, v \in V(G)$，$u \ne v$，$(u,v) \notin E(G)$，必有 $d(u)+d(v) \ge n$。

若不然，就有 $d(u)+d(v) \le n-1$。注意到，在 K_n 中，与 u 或 v 相关联的边总共有 $2n-3$ 条。若 $d(u)+d(v) \le n-1$，则这 $2n-3$ 条边中，至少有 $(2n-3)-(n-1) = n-2$ 条边不在图 G 中。从而 $m \le |E(K_n)|-(n-2) = \frac{1}{2}n(n-1)-(n-1)+1 = \frac{1}{2}(n-1)(n-2)+1 < \frac{1}{2}(n-1)(n-2)+2$，矛盾。

这就是说，$|G| \ge 3$ 且对 G 中任意两个不相邻的顶点 u, v 都有 $d(u)+d(v) \ge n$。从而由教材定理 8.7 推论 1 可知，G 是哈密顿图。 □

当 $m = \frac{1}{2}(n-1)(n-2)+1$ 时 G 不一定是哈密顿图。反例如下：取 $n = 3$，则 $m = \frac{1}{2}(n-1)(n-2)+1 = 2$。此时，令 $G = T$ 为任意 3 阶树。由于树中无圈，所以也不会有哈密顿圈。此时，G 不是哈密顿图。

再举一个 $m = \frac{1}{2}(n-1)(n-2)+1$ 时 G 是哈密顿图的例子：取 $n = 4$，则 $m = \frac{1}{2}(n-1)(n-2)+1 = 4$。此时令 $G = C$ 为一个 4 阶圈。显然，G 本身就是一个哈密顿圈，从而 G 是哈密顿图。

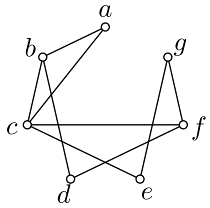
总之，当 $m = \frac{1}{2}(n-1)(n-2)+1$ 时，G 未必是哈密顿图。

8.10

证明: 反设 $C = v_{i_1}v_{i_2}\cdots v_{i_k}$ 不是哈密顿回路，则 $V(G)-V(C) \ne \varnothing$。这时，考虑 C 的邻域 $N(C) = \{v_s \mid v_s \in V(G)-V(C) \wedge \exists v_{i_j}(v_{i_j} \in V(C) \wedge (v_{i_j}, v_s) \in E(G))\}$。$N(C)$ 必不空(若 $N(C)$ 为空，则 $V(C)$ 与 $V(G)-V(C)$ 的顶点之间没有通路，从而与前提“G 是连通图”矛盾)。任取 $v_s \in N(C)$，由 $N(C)$ 定义知，存在 $v_{i_j} \in V(C)$，使得 $(v_{i_j}, v_s) \in E(G)$。这时，

$\Gamma = v_{i_{j+1}} \cdots v_{i_k} v_{i_1} \cdots v_{i_j} v_s$ 是一条长度为 k 的路径，而从 C 中删除 $(v_{i_j}, v_{i_{j+1}})$ 后，得到的只是一条长度为 $k-1$ 的路径 $\Gamma' = v_{i_{j+1}} \cdots v_{i_k} v_{i_1} \cdots v_{i_j}$，不是 G 中的最长路径。矛盾。 □

8.11 构造以 $\{a, b, c, d, e, f, g\}$ 中顶点集的无向图，在能互相交谈的人所对应的顶点间添加边，得到下图：



易见，$C = abdfgec$ 是一个哈密顿回路，从而按此方式安排座位可以使每个人都能与他身边的人交谈。

8.12 建立一个有 $2k$ 个顶点的无向图 $G = \langle V, E \rangle$，其中 $V = \{v_1, v_2, \cdots, v_{2k}\}$ 中每个顶点对应一个人，在能组成小组的人之间加入边。由于 $k \geq 2$，所以 $|G| = 2k \geq 4$。由题设，对任意 $v_i \in V$，有 $d(v_i) = k$。由教材定理 8.7 推论 2 可知，G 中存在哈密顿回路 $C = v_{i_1} v_{i_2} \cdots v_{i_{2k}}$。对所有 $j = 1, 2, \cdots, k$，将 $v_{i_{2j-1}}$ 和 $v_{i_{2j}}$ 分在一组，则可以组成 k 个小组，每个小组都能完成一项该组成员共同熟悉的任务。

8.13

证明: 将 n 个人抽象为 n 阶无向图 G 中的 n 个顶点，在互相认识的人之间添加边。

首先证明，对任意 $v_i \in V(G)$，$d(v_i) \geq n-2$。这是因为，假设 $d(v_i) \leq n-3$，则除 v 自身外，G 中至少还存在两个顶点 $v_j, v_k \in V(G)$，使得 $(v_i, v_j), (v_i, v_k) \notin E(G)$，从而 v_j 和 v_k 合起来不能认识 v_i。这与题设矛盾。

当 $n \geq 3$ 时，任取 $v_i, v_j \in V(G)$，有 $d(v_i) + d(v_j) \geq 2n-4 \geq n-1$，由教材定理 8.7，$G$ 中存在哈密顿通路 Γ，按顶点在 Γ 中出现的顺序将这 n 个人排成一列，则中间任何人都认识两旁的人，而两头的人认识左边(或右边)的人。

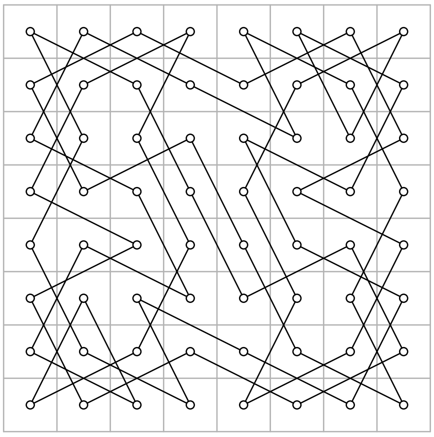
当 $n \geq 4$ 时，对任意 $v_i \in V(G)$，有 $d(v_i) \geq n-2 \geq \dfrac{n}{2}$，由教材定理 8.7 推论 2，$G$ 中存在哈密顿回路 C，按顶点在 C 中出现的顺序将这 n 个人排成一圈，则每个人都认识两旁的人。 □

8.14 将棋盘上的格子抽象为无向图 G 的顶点，对任意顶点 $v_i, v_j \in V(G)$，令 $(v_i, v_j) \in E(G)$ 当且仅当马能从 v_i 所对应的格子直接跳到 v_j 所对应的格子。显然，“马能在棋盘上经过每个格一次且仅一次，最后回到出发点”当且仅当 G 是哈密顿图。

考虑下图中分别被标记为 a, b, c, d 的 4 个方格。注意到，如果从 G 中删除 c, d 所对应的顶点(不妨记为 v_c 和 v_d)，则 a, b 所对应的顶点将成为孤立点。从而 $G - \{v_c, v_d\}$ 中至少有 3 个连通分支。由教材定理 8.6 可知，G 不是哈密顿图。从而题目所述要求无法办到。

			b
	c		
		d	
a			

8.15 可以。下图[1]所示即为一种可行的方案：



50	11	24	63	14	37	26	35
23	62	51	12	25	34	15	38
10	49	64	21	40	13	36	27
61	22	9	52	33	28	39	16
48	7	60	1	20	41	54	29
59	4	45	8	53	32	17	42
6	47	2	57	44	19	30	55
3	58	5	46	31	56	43	18

分析[2]：

以国际象棋棋盘上的每个格为 1 个顶点，若两个顶点间相差一个马步，则连一条边，作无向图 G，如图 1 所示。G 中顶点的度数如图 2 所示。

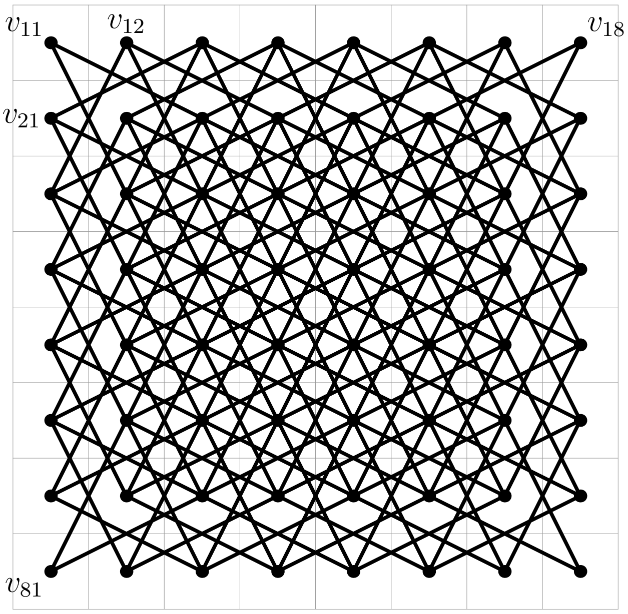
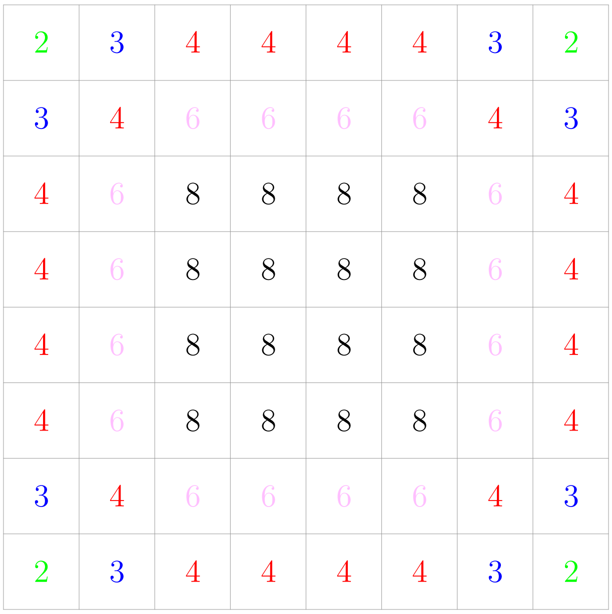


图 1

---

[1] 摘自《图论及其算法》(王树禾，中国科学技术大学出版社，1990)第 68 页。

[2] 感谢 xbz 网友给出本题的详细分析。



2	3	4	4	4	4	3	2
3	4	6	6	6	6	4	3
4	6	8	8	8	8	6	4
4	6	8	8	8	8	6	4
4	6	8	8	8	8	6	4
4	6	8	8	8	8	6	4
3	4	6	6	6	6	4	3
2	3	4	4	4	4	3	2

图 2

假设 G 是 $Hamilton$ 图，则存在 $Hamilton$ 回路 C，由 $d(v_{11}) = 2$ 知，C 中与 v_{11} 相邻的两个顶点为 v_{23} 和 v_{32} 。如果从 v_{11} 开始进行遍历，其过程一定是 $v_{11}, v_{23} \cdots v_{32}, v_{11}$，则 $G - v_{11}$ 中必然存在 v_{23} 到 v_{32} 的 $Hamilton$ 通路。由 v_{18}, v_{81}, v_{88} 和 v_{11} 具有相同的性质可知，$C - \{v_{11}, v_{18}, v_{81}, v_{88}\}$ 会产生 4 条互不相交的路径。而这些路径的起始点只能是 $\{v_{23}, v_{26}, v_{32}, v_{37}, v_{62}, v_{67}, v_{73}, v_{76}\}$ 中的点。

由图 1 和图 2 可以看出，G 有“旋转对称性”（即将 G 顺时针旋转 $90°, 180°, 270°$ 后，仍与 G 重合）。不妨提出猜想：$C - \{v_{11}, v_{18}, v_{81}, v_{88}\}$ 产生的 4 条路径也具有“旋转对称性”（一个依据：C 中已经确定下来的 8 条边具有“旋转对称性”）。如果猜想成立，那么只需求出一条路径，通过旋转就可以得到其它 3 条。

$G - \{v_{11}, v_{18}, v_{81}, v_{88}\}$ 中有 60 个顶点，由猜想知 4 条路径长度相同，可以进行分组，每组 15 个点，例如将 v_{21} 顺时针旋转 $90°, 180°, 270°$ 后，得到 v_{17}, v_{78} 和 v_{82}，则这 4 个点属于同一组。给每个组编一个号，如图 3 所示。

	3_2						
3_1	4_5						
4_1	6_1	8_1					
4_2	6_2	8_2	8_4				
4_3	6_3	8_3					
4_4	6_4						

图 3

图 3 中组编号 a_b的含义：a 代表组中顶点在 G 中的度数，b 只是用来计数。如 6_3 表示组中顶点在 G 中是 6 度的，这是第 3 个 6 度组。这些编号是位置无关的，虽然编号 3_1 放在了顶点 v_{21} 的位置上，它并不只代表 v_{21} 。

由于路径的起始点只能是 6_1 或 6_4 类的点，不妨设由 6_1 出发到 6_4 。以这 15 个编号为顶点，它们代表的顶点若在 G 中相邻，则在两个编号之间连边。作无向图，如图 4 所示。

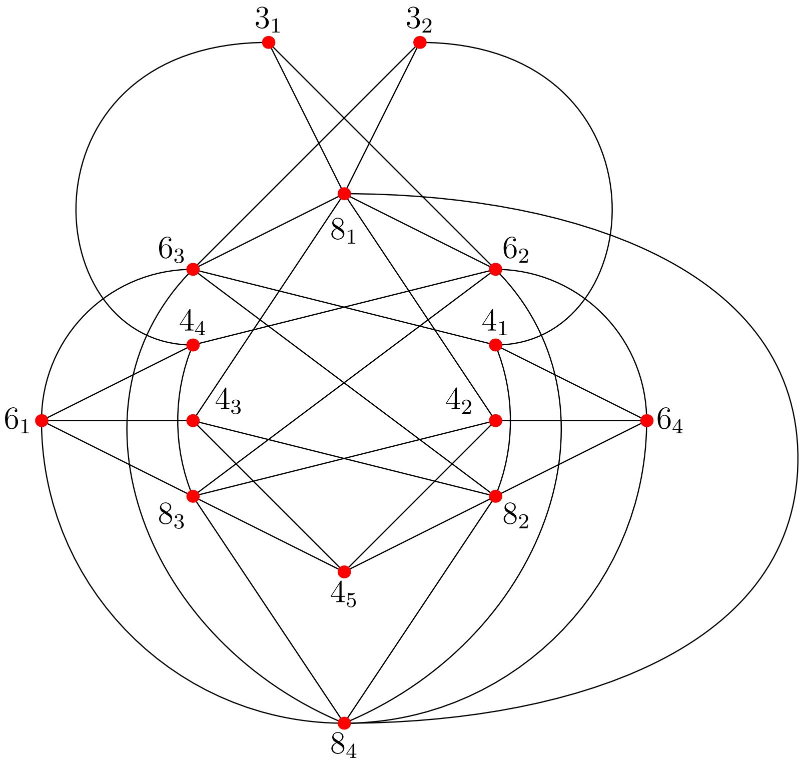


图 4

此时，问题就简化为：在一个 15 个顶点，37 条边构成的图中，寻找一条 6_1 到 6_4 的 *Hamilton* 通路。

寻路时需要注意，当有多种选择时，选择度数最低的顶点。

用深度优先法很容易就可以找到一个解，即 $\{6_1, 4_3, 4_5, 4_2, 8_3, 4_4, 3_1, 6_2, 8_1, 3_2, 4_1, 6_3, 8_2, 8_4, 6_4\}$，如图 5 所示（若第一步不走 4_3 走 4_4 的话，需要回退几次，但也并不复杂）。

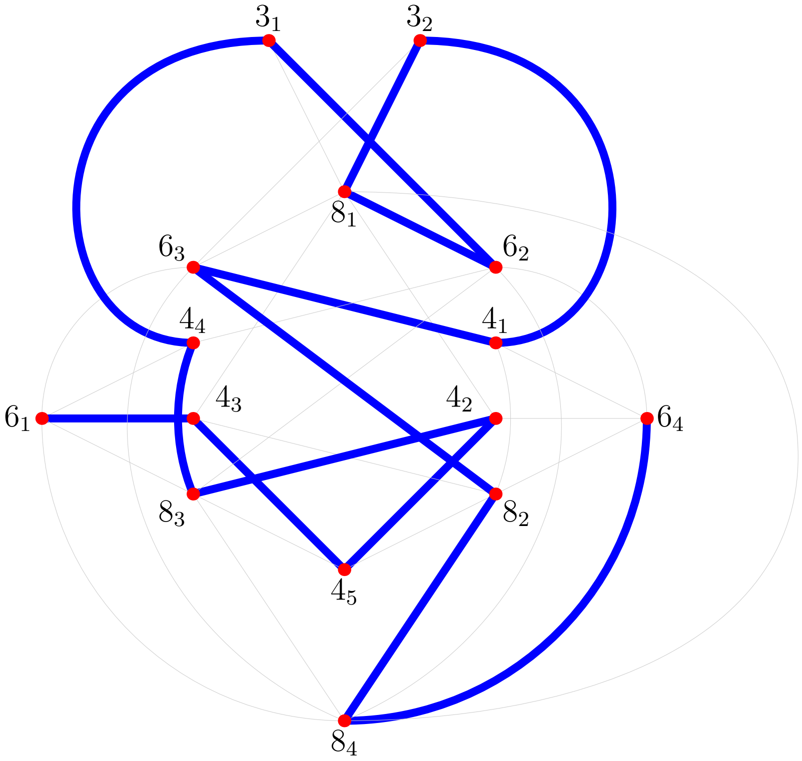


图 5

有了 6_1 到 6_4 的 *Hamilton* 通路，就可以实例化了，如图 6 所示。

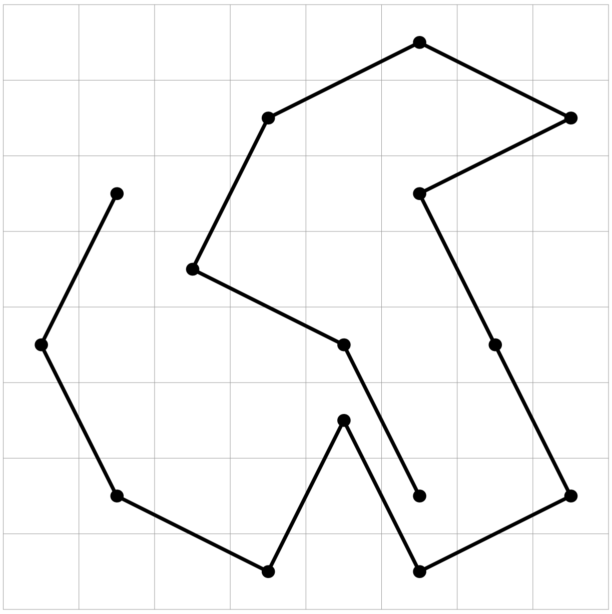


图 6

将此路径顺时针旋转 $90°, 180°, 270°$ 即可得到其它 3 条路径。把 $v_{11}, v_{18}, v_{81}, v_{88}$ 连上去，会产生 2 条回路 C_1, C_2，如图 7 所示（虽然这个结果和我们的预期还有差距，不过已经很接近了）。

解决方案：找两条边，$(w_{11}, w_{12}) \in C_1, (w_{21}, w_{22}) \in C_2$ 且 $(w_{11}, w_{21}) \in G, (w_{12}, w_{22}) \in G$，则 $(C_1 - (w_{11}, w_{12})) \cup (C_2 - (w_{21}, w_{22})) \cup (w_{11}, w_{21}) \cup (w_{21}, w_{22})$ 即为所得，图 8 为一个解。

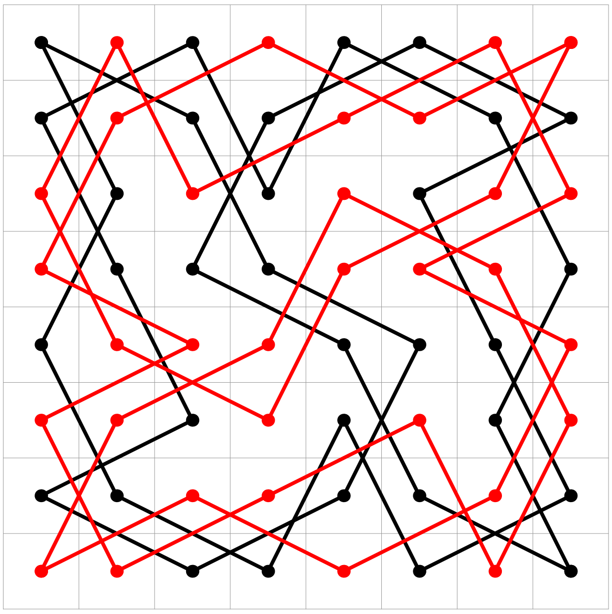


图 7

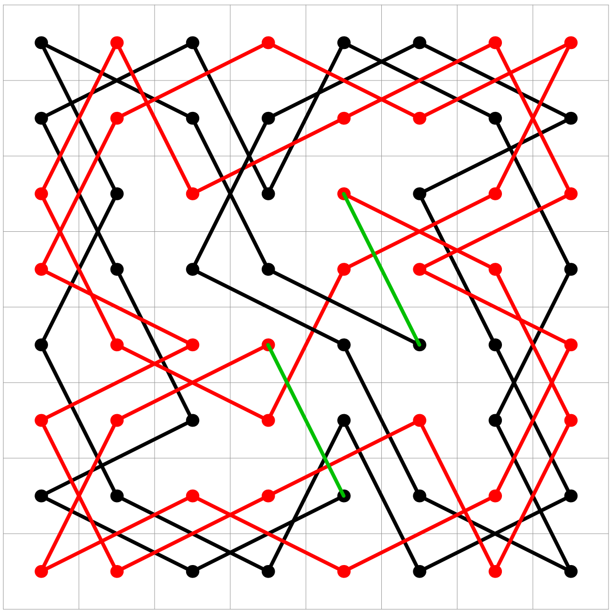


图 8

8.16

证明: 必要性是显然的。下面证充分性。

反设 G 不是哈密顿图。由于 $G \cup (u, v)$ 是哈密顿图，所以存在哈密顿回路 $C \subseteq G \cup (u, v)$。显然，$(u, v) \in E(C)$ (否则就有 $C \subseteq G$，与假设“G 不是哈密顿图”矛盾)。从 C 中删除边 (u, v)，得到一条哈密顿通路 $\Gamma = v_1 v_2 \cdots v_n$，不妨设 $u = v_1, v = v_n$。注意到，对任意 $v_i (2 \leq i \leq n-1)$，若 v_i 与 u 相邻，则 v_{i-1} 必不与 v 相邻(否则，$v_1 v_2 \cdots v_{i-1} v_n v_{n-1} \cdots v_i$ 就是 G 中的一条哈密顿

回路，与假设矛盾)。因此，设 u 共与 $d(u)$ 个顶点相邻(由于 $(u,u),(u,v)\notin E(G)$，所以这 $d(u)$ 个顶点必然都在 $v_2,v_3,\cdots,v_{n-1}$ 中)，则 v 与这 $d(u)$ 个顶点左侧的 $d(u)$ 个顶点都不相邻。注意到，这 $d(u)$ 个顶点不包括 v 本身。因此，加上 v 本身，v 至少与 $d(u)+1$ 个顶点不相邻。这就是说，$d(v)\le n-(d(u)+1)$，即 $d(u)+d(v)\le n-1$。这与题设 $d(u)+d(v)\ge n$ 矛盾。 □

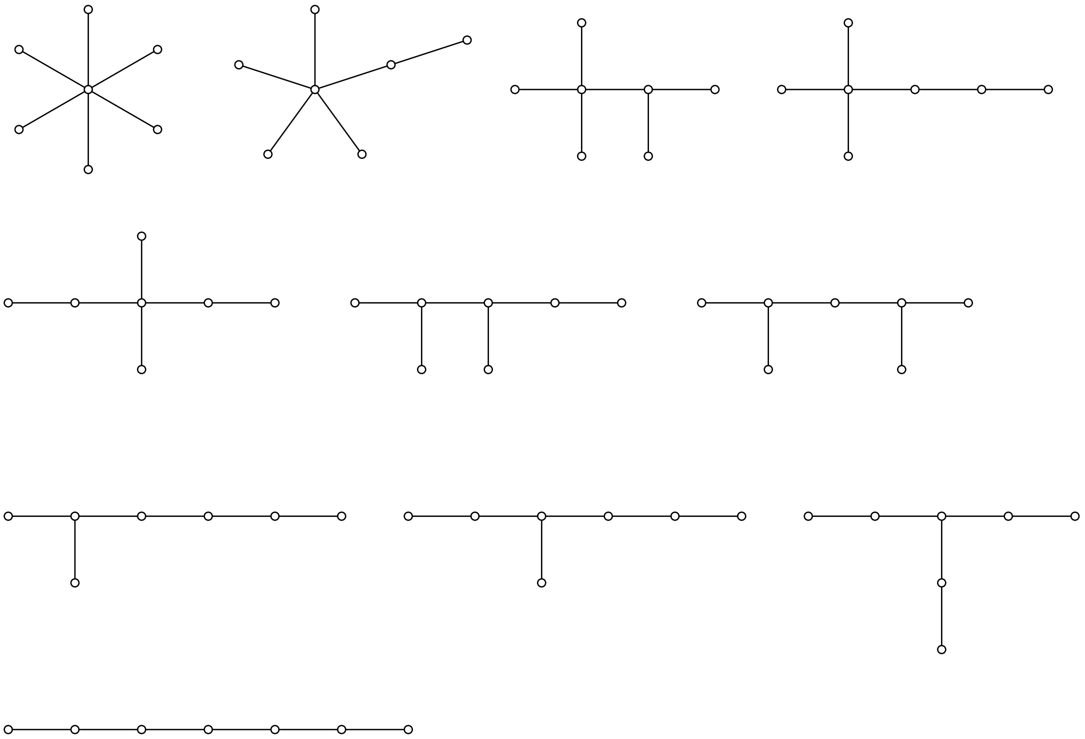
8.17 证明繁琐，暂略。

第九章　树

9.1　可行的度数分配方案有：

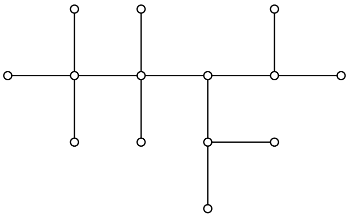
(1)	6	1	1	1	1	1	1
(2)	5	2	1	1	1	1	1
(3)	4	3	1	1	1	1	1
(4)	4	2	2	1	1	1	1
(5)	3	3	2	1	1	1	1
(6)	3	2	2	2	1	1	1
(7)	2	2	2	2	2	1	1

其中方案 (4)、(5) 各自可以生成 2 棵非同构的树，方案 (6) 可以生成 3 棵非同构的树，其余方案均只能生成 1 棵非同构的树。全部 11 棵非同构的树为：

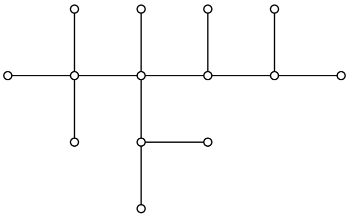


9.2　设 T 中共有 x 个 4 度顶点，则由题设和图论基本定理应有 $2(9+3+x-1) = 2(n-1) = 2m = \sum\limits_{v\in V(T)} d(v) = 9+3\cdot 3+4x$，解得 $x=2$。从而度数列为 4 4 3 3 3 1 1 1 1 1 1 1 1 1。

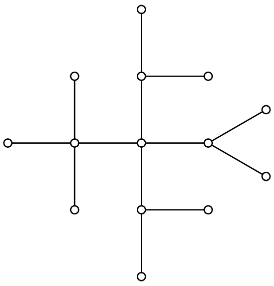
根据两个 4 度顶点之间的距离(它们之间要么直接连接，要么用一个或多个 3 度顶点进行连接)和其余 3 度顶点的分布方式，可以确定以下 14 种构形，每种构形对应一个非同构的无向树：



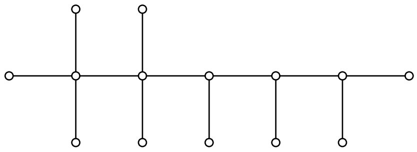
$\begin{array}{ccccccc}4&-&4&-&3&-&3\\&&&&|&&\\&&&&3&&\end{array}$



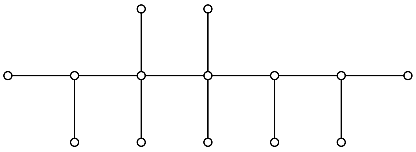
$\begin{array}{ccccccc}4&-&4&-&3&-&3\\&&|&&&&\\&&3&&&&\end{array}$



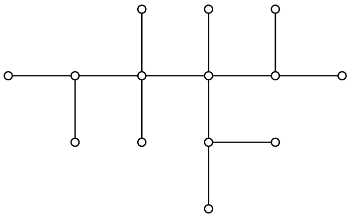
$\begin{array}{ccccc}&&3&&\\&&|&&\\4&-&4&-&3\\&&|&&\\&&3&&\end{array}$



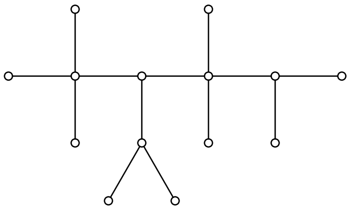
$4-4-3-3-3$



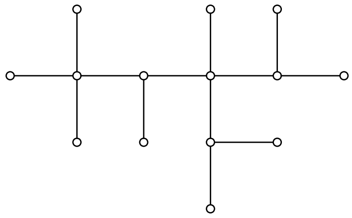
$3-4-4-3-3$



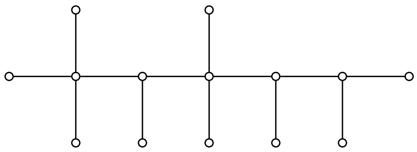
$\begin{array}{ccccccc}3&-&4&-&4&-&3\\&&&&|&&\\&&&&3&&\end{array}$



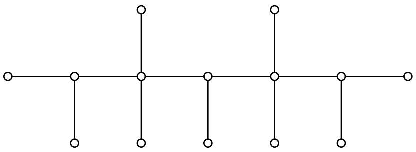
$\begin{array}{ccccccc}4&-&3&-&4&-&3\\&&|&&&&\\&&3&&&&\end{array}$



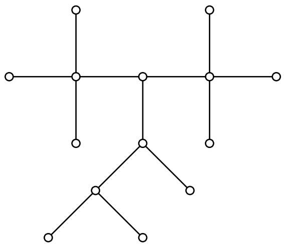
$\begin{array}{ccccccc}4&-&3&-&4&-&3\\&&&&|&&\\&&&&3&&\end{array}$



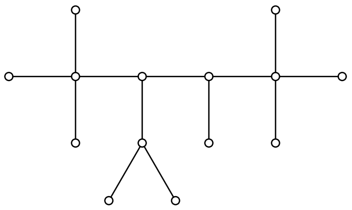
$4-3-4-3-3$



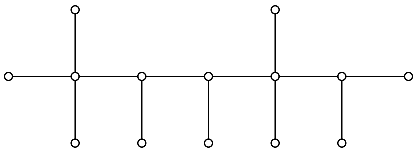
$3-4-3-4-3$



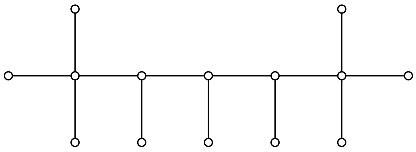
$\begin{array}{ccccc}4&-&3&-&4\\&&|&&\\&&3&&\\&&|&&\\&&3&&\end{array}$



$\begin{array}{ccccccc}4&-&3&-&3&-&4\\&&|&&&&\\&&3&&&&\end{array}$



$4-3-3-4-3$



4 − 3 − 3 − 3 − 4

9.3 设 T 有 n_1 片树叶，则由树的性质和图论基本定理有：

$$2\cdot\sum_{i=1}^{k}n_i-2=2(n-1)=2m=\sum_{i=1}^{k}i\cdot n_i$$

解得：

$$n_1=\sum_{i=2}^{k}(i-2)n_i+2$$

注意到，当 $i=2$ 时，$(i-2)n_i=0$，因此，上式可以改写成

$$n_1=\sum_{i=3}^{k}(i-2)n_i+2$$

这一公式说明，无向树中树叶的个数由 3 度及 3 度以上顶点的个数唯一确定，与树的结构和 2 度顶点的个数无关。

9.4

证明: 对 k 作归纳。

当 $k=1$ 时，T 即为 K_2。$\delta(G)\geq 1$，从而 G 中有边，任取边 $e\in E(G)$，则由 $\{e\}$ 导出的子图 $G[\{e\}]$ 即为与 T 同构的子图。命题成立。

设 $k=t(t\geq 1)$ 时，命题成立。当 $k=t+1$ 时，设 $v\in V(T)$ 是 T 中某片树叶，且 $u\in V(T)$ 为 T 中(唯一)与 v 相邻的顶点。令 $T'=T-v$。由归纳假设，G 中存在与 T' 同构的子图 H'。设同构函数为 $\overline{\varphi}:V(T')\to V(H')$，并记 $u'=\overline{\varphi}(u)$。注意到，u' 在 $V(G)-V(H')$ 中必然还有邻接点(若不然，则 u' 的所有邻接点都在 $V(H')$ 中，从而由 $u'\in V(H')$ 和 H' 是简单图可知，$d(u')\leq|V(H')|-1=t<t+1=\delta(G)$，矛盾)，设 $v'\in V(G)-V(H')$ 就是一个与 u' 相邻且不在 $V(H')$ 中的顶点。

令 $H=\langle V(H')\cup\{v'\},E(H')\cup\{(u',v')\}\rangle$，取 $\varphi:V(T)\to V(H)$，$\forall x\in V(T)$，

$$\varphi(x)=\begin{cases}\overline{\varphi}(x), & 若\ x\in V(T')\\ v', & 若\ x=v\end{cases}$$

易见，φ 是从 T 到 H 的同构。从而当 $k=t+1$ 时，命题同样成立。 □

9.5

证明: T_3 中显然无简单回路 (否则这一回路也将出现在 T 中，这与 T 是树矛盾)。下面只需证 T_3 是连通的。对任意 $u,v\in V(T_3)$，有 $u,v\in V(T_1)$ 和 $u,v\in V(T_2)$，由于 T_1 和 T_2 都是树，所以在中 T_1 和 T_2 中分别有唯一的路径 Γ_1 和 Γ_2 连接 u,v。注意到，Γ_1 和 Γ_2 都在 T 中，而 T 也是树，由 T 中路径的唯一性可知，$\Gamma_1=\Gamma_2\subseteq T_1\cap T_2$。从而 $\Gamma_1\subseteq T_3$。这就是说，u,v 在 T_3 中也是连通的。由 u,v 的任意性可知，T_3 是连通的，从而是树。 □

9.6

证明: 反设 G 和 $\overline{G}$ 中都无圈，则由引理 7.5 有 $|E(G)|=n-p(G)\leq n-1$ 和 $|E(\overline{G})|=n-p(\overline{G})\leq n-1$。从而有 $\dfrac{n(n-1)}{2}=|E(K_n)|=|E(G\cup\overline{G})|\leq 2n-2$。即 $n^2-5n+4\leq 0$，解得 $1\leq n\leq 4$。与题设 $n\geq 5$ 矛盾。 □

9.7 即为引理 7.5。

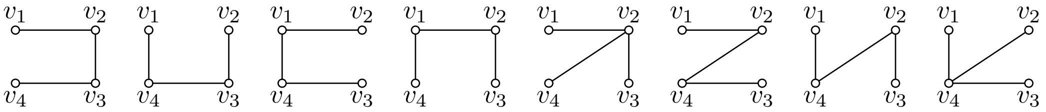
9.8

证明: 对 n 作归纳。

当 $n=2$ 时，必有 $d_1=d_2=1$，命题显然成立。

设 $n=t(t\geq 2)$ 时命题成立。当 $n=t+1$ 时，由于 $n\geq 3$，所以有 $n<\sum\limits_{i=1}^{n} d_i=2n-2<2n$，从而由鸽巢原理可知，必然存在 $1\leq i,j\leq n$，满足 $d_i>1$ 和 $d_j<2$，也即 $d_i\geq 2$ 和 $d_j=1$。不失一般性，不妨设 $i=1$，$j=n$。考虑如下 t 个正整数：$d_1-1,d_2,\cdots,d_t$，它满足条件 $\sum\limits_{i=1}^{t} d_i=2t-2$，从而由归纳假设，存在一个以 $d_1-1,d_2,\cdots,d_t$ 为度数列的无向树 T。向 T 中添加一个新顶点 v，并令 v 与 T 中度数为 d_1-1 的顶点相邻。易见，如此得到的新图 T' 也是树，且以 $d_1,d_2,\cdots,d_n$ 为度数列。这就证明了，当 $n=t+1$ 时，命题同样成立。 □

9.9 $\tau(G)=8$，全体不同的生成树为：



9.10 基本回路有：$C_a=aegdj,C_b=bgdji,C_c=cdg,C_f=fge,C_h=hij$。

基本回路系统为 $\{C_a,C_b,C_c,C_f,C_h\}$。

基本割集有：$S_d=\{a,b,c,d\},S_e=\{a,e,f\},S_g=\{a,b,c,f,g\},S_i=\{b,h,i\},S_j=\{a,b,h,j\}$。

基本割集系统为 $\{S_d,S_e,S_g,S_i,S_j\}$。

9.11

证明: 由题设，存在 $v\in V(T)$，满足 $d(v)\geq k$。设 T 中共有 t 片树叶。则 T 中除树叶和 v 外，其它 $n-t-1$ 个顶点的度数都不小于 2。从而由图论基本定理知：$2n-2=2m=\sum\limits_{v_i\in V(G)} d(v_i)\geq k+2(n-t-1)+t=2n+k-t-2$。解得 $t\geq k$。 □

9.12 首先证明下述结论：

引理 9.1 设无向图 G 中共有 k 个连通分支 $G_1,G_2,\cdots,G_k(k\geq 1)$，$u\in V(G_i)$，$v\in V(G_j)$，$(1\leq i,j\leq k)$，$e=(u,v)\notin E(G)$，$G'=G\cup e$，则

(1) 若 $i=j$，则 $p(G')=p(G)$，且 G' 的连通分支为 $G_1,G_2,\cdots,G_i\cup e,\cdots,G_k$;

(2) 若 $i\neq j$，则 $p(G\cup e)=p(G)-1$，且 G' 的连通分支为 $G_i\cup G_j\cup e,G_1,G_2,\cdots,G_{i-1},G_{i+1},\cdots,G_{j-1},G_{j+1},\cdots,G_k$。

证明: 对任意 $x,y\in V(G)$，分两种情况：

情况一：若 x,y 在 G 中连通，则它们显然在 G' 中也连通。

情况二：若 x,y 在 G 中不连通，则它们属于 G 的两个不同的连通分支。下面证明，x,y 在 G' 中连通，当且仅当 $x\in V(G_i)\wedge y\in V(G_j)$ 或者 $x\in V(G_j)\wedge y\in V(G_i)$。

如果 $x\in V(G_i)\wedge y\in V(G_j)$ 或者 $x\in V(G_j)\wedge y\in V(G_i)$，则 x,y 在 G' 中显然是连通的。

反过来，如果 x,y 在 G' 中连通，则存在通路 $\Gamma=v_0v_1v_2\cdots v_t\subseteq G'$，其中 $v_0=x,v_t=y$。并且必有 $e\in E(\Gamma)$ (否则这个通路将同样出现在 G 中，矛盾)。由于 e 可能在 Γ 中多次出现，因此，假设 e 在 Γ 中的第一次出现和最后一次出现分别为 (v_r,v_{r+1}) 和 (v_s,v_{s+1})，其中 $0\leq r\leq s\leq t-1$ (若 e 只出现一次，则 $r=s$)。考虑 $\Gamma_1=v_0v_1\cdots v_r$，$\Gamma_2=v_{s+1}v_{s+2}\cdots v_t$，注意到，$\Gamma_1$ 和 Γ_2 中都不含 e，从而它们都在 G 中。而 v_r 和 v_{s+1} 都是 e 的端点，所以取值只能是 u 或 v，而且

必然一个是 u，另一个是 v (若不然，就有 $v_r = v_{s+1}$，则 $\Gamma_1\Gamma_2$ 就是 G 中一个从 x 到 y 的通路，矛盾)。这就是说，在 G 中存在 x 到 u (或 v)的通路 Γ_1 和从 y 到 v (或 u) 的通路 Γ_2。从而必有 $x \in V(G_i) \wedge y \in V(G_j)$ 或者 $x \in V(G_j) \wedge y \in V(G_i)$。这就证明了命题的另一个方向。

由上面的讨论可知：

(1) 当 $i = j$ 时，x, y 在 G' 中连通当且仅当它们在 G 中连通。从而连通分支数量不变(只是 G_i 中增加了一条新边 e)。

(2) 当 $i \neq j$ 时，x, y 在 G' 中连通当且仅当它们在 G 连通，或者它们在 G 中分别属于 G_i 和 G_j 这两个连通分支。从而边 e 将把 G_i 与 G_j 连接成一个新的连通分支，而其它的连通分支保持不变。 □

推论 设 E' 为图 G 的一个割集，则 $p(G - E') = p(G) + 1$。

证明: 设 E' 为 G 的任意割集，反设 $p(G-E') \geq p(G)+2$，则任取 $e \in E'$，令 $E'' = E'-\{e\} \subset E'$，则有 $p(G-E'') = p((G-E')\cup e)$，而由引理 9.1 可知，$p((G-E')\cup e) \geq p(G-E')-1 \geq p(G)+1$。这与割集的定义矛盾。 □

引理 9.2 设 C 为无向图 G 中的一个圈，$S \subseteq E(G)$ 为 G 中任意边割集，若 $S \cap E(C) \neq \varnothing$，则 $|S \cap E(C)| \geq 2$。

证明: 若不然，就有 $|S \cap E(C)| = 1$，即，存在唯一的 $e = (u, v) \in S \cap E(C)$。记 $G' = G - S$，$S' = S - \{e\}$，由割集的定义可知，$p(G') > p(G' \cup e) = p(G - S') = p(G)$。这就是说，向 G' 中加入边 e 会使连通分支数减少，从而由引理 9.1可知，u 和 v 在 G' 中属于两个不同的连通分支。然而，由于 u, v 在圈 C 上，而 $C - e$ 是一条从 u 到 v 的通路。而由前提，e 是 $S \cap E(C)$ 中唯一的元素，这就是说，C 中其它的边都在 G' 中，也即 $C - e \subseteq G'$。这就是说，u 与 v 在 G' 中是连通的。矛盾。 □

再证原题。

证明: 设 C 所在的连通分支为 G_1。令 $C' = C - e_1$。显然，C' 中无圈。由教材例 9.1 可知，存在 G_1 的一棵生成树 T，使得 $C' \subseteq T$。考虑由 T 的树枝 e_2 产生的基本割集 S_{e_2}。因为 $e_2 \in S_{e_2} \cap E(C)$，从而由引理 9.2 可知，$S_{e_2}$ 与 C 至少还应有一条公共边 e。注意到，S_{e_2} 是基本割集，因此，除了 e_2 之外，其余的边都只能是 T 的弦，也即，$e \notin E(T)$，而由于 $C' \subseteq T$，因此，满足 $e \in E(C)$，$e \notin E(T)$ 的只有 e_1。从而必有 $e_1 = e \in S_{e_2}$。这就是说，S_{e_2} 即为题中要求的割集。 □

9.13 首先证明下述结论。

引理 9.3 设 G_1、G_2 是 G 的两个子图，满足 $V(G_1) = V(G_2) = V'$ 和 $E(G_1) \subseteq E(G_2)$，则

(1) 设 $\sim_1, \sim_2 \subseteq V' \times V'$ 分别是 G_1 与 G_2 中的“连通关系”，则 $V'/{\sim_1}$ 是 $V'/{\sim_2}$ 的加细。

(2) $p(G_2) \leq p(G_1)$。

证明: 由于 G_2 可以通过向 G_1 中反复新边得到，而由引理 9.1，加入新边要么不改变各连通分支所对应的顶点集，要么使两个连通分支合并为一个，从而使连通分支数减少。对 $|E(G_2) - E(G_1)|$ 作归纳即得原题。 □

引理 9.4 对 G 的任意割集 $E' \subseteq E(G)$，任取 $e = (u, v) \in E'$，设 $G_1 \subseteq G - E'$ 是 $G - E'$ 中 u 所在的连通分支，则 $E' = (V(G_1), \overline{V(G_1)})$ 是一个断集。

证明: 记 $G' = G - E'$，$S = (V(G_1), \overline{V(G_1)})$。设 G_2 为 $G - E'$ 中 v 所在的连通分支。显然有 $G_1 \neq G_2$ (否则由引理 9.1 可知，在 G' 中加入 (u, v) 不会影响其连通分支数，从而与 E' 是割集矛盾)。下面证明，$E' = S$。

首先，显然有 $S \subseteq E'$。若不然，设 $(x, y) \in S$，但 $(x, y) \notin E'$，则，依照定义，有 $x \in G_1$，$y \notin G_1$，且 $(x, y) \in E(G')$。由于 $x \in G_1$ 且 x 与 y 在 G' 中连通，所以 y 也应在连通分支 G_1 中，

这与 $(x,y)\in S$ (从而有 $y\notin G_1$)矛盾。

其次，有 $E'\subseteq S$。这是因为，若不然，则存在边 $(x,y)\in E'$ 满足条件：

(1) $x,y\in V(G_1)$，或者

(2) $x,y\notin V(G_1)$。

然而，情况 (1) 不可能成立，因为按引理 9.1，如果 $x,y\in V(G_1)$，则 $p(G-(E'-\{(x,y)\}))=p((G-E')\cup\{(x,y)\})=p(G-E')<p(G)$，这与 E' 是割集矛盾。

情况 (2) 也不可能成立。若不然，考虑 $G''=G'\cup\{(x,y)\}$，因为 $E'-\{(x,y)\}\subset E'$，按割集定义，应当有 $p(G'')=p(G'\cup\{(x,y)\})=p(G-(E-\{(x,y)\}))=p(G)$。但由于 x,y 都不在 G_1 中，由引理 9.1 可知，G_1 在 G'' 中仍是一个独立的连通分支。这时，再向 G'' 中加入 $e=(u,v)$。注意到，$E(G''\cup\{e\})=E(G)-(E'-\{(u,v),(x,y)\})\subseteq E(G)$，由引理 9.3 应有 $p(G''\cup\{e\})\geq p(G)$。然后，由引理 9.1，却有 $p(G''\cup\{(u,v)\})=p(G'')-1=p(G)-1<p(G)$。矛盾。

这就证明了 $E'\subseteq S$。从而 $E'=S$ 是一个断集。 □

再证原题。

证明: 考虑关于由 T_1 的树枝 e_1 产生的基本割集 S_{e_1}。设 $e_1=(u,v)$ 且 u 在 $G-S_{e_1}$ 中所在的连通分支为 V_1。由引理 9.4 可知，$S_{e_1}=(V_1,\overline{V}_1)$。我们注意到，$T_1[V_1]$ 和 $T_1[\overline{V}_1]$ 是 T_1-e_1 中仅有的两个连通分支(这是因为，$E(T_1-e_1)\subseteq E(G-S_{e_1})$，从而由引理 9.3 知，$T_1[V_1]$ 和 $T_1[\overline{V}_1]$ 之间是不连通的，而因为 $p(T_1)=1$，所以由引理 9.1 可知，$p(T_1-e_1)\leq 2$。也即，$T_1[\overline{V}_1]$ 恰是 T_1-e_1 的另一个连通分支)。由于 S_{e_1} 是割集，所以由教材定理 9.13，S_{e_1} 至少包含 T_2 中的一个树枝，设 $e_2\in S_{e_1}\cap E(T_2)$ 就是这样的一个树枝。注意到，$e_2\neq e_1$ (因为 $e_1\notin E(T_2)$)，从而有 $e_2\notin E(T_1)$ (因为由基本割集定义，S_{e_1} 中只有 e_1 是 T_1 的树枝)。注意到，由于 $e_2\in S_{e_1}=(V_1,\overline{V}_1)$，所以 e_2 的两端分别在 V_1 和 $\overline{V}_1$ 中(从而在 $T_1[V_1]$ 和 $T_1[\overline{V}_1]$ 中)。从而由引理 9.1 可知，$p((T_1-e_1)\cup\{e_2\})=p(T_1-e_1)-1=1$，从而是 $(T_1-e_1)\cup\{e_2\}$ 是连通的。再由 T_1 是树可知 $|(T_1-e_1)\cup\{e_2\}|=|T_1|-1+1=|T_1|=n-1$，从而根据教材定理 9.1，$(T_1-e_1)\cup\{e_2\}$ 是树(自然也就是 G 的生成树)。同理可证 $(T_2-e_2)\cup\{e_1\}$ 是 G 的生成树。 □

9.14

证明: 考虑标定图 $G=K_n$ 和 $H=G-e$ (其中 $e\in E(G)$)。注意到，G 的一棵生成树 $T\subseteq G$ 是 H 的生成树当且仅当 $e\notin E(T)$。因此，$\tau(H)$ 即为 G 中不含 e 的生成树数量。

由教材定理 9.7 可知，G 共有 n^{n-2} 棵不同的生成树。每棵生成树中有 $n-1$ 条边，从而 G 中的边在各生成树中出现的次数之和为 $(n-1)n^{n-2}$。由对称性，G 中的每一条边在 K_n 的生成树中出现的总次数是相同的。因此，e 在所有生成树中出现的总次数应为 $\dfrac{(n-1)n^{n-2}}{n(n-1)/2}=2n^{n-3}$。而 e 在每棵生成树中至多只出现一次，从而 G 中共有 $2n^{n-3}$ 棵含 e 的生成树。这就是说，$\tau(H)=\tau(G)-2n^{n-3}=n^{n-2}-2n^{n-3}=(n-2)n^{n-3}$。 □

9.15

证明: 对任意 $G_i,G_j\in\Omega$，$a,b\in\{0,1\}$：

(1) 由定义显然有 $G_i\oplus G_j\in\Omega$。从而环和运算对 Ω 是封闭的。

(2) 由环和运算定义和教材例 1.7 可知，环和运算满足结合律和交换律。

(3) $\varnothing\in\Omega$，且 $\varnothing\oplus G_i=G_i\oplus\varnothing=G_i$，从而 Ω 中有单位元 $\varnothing$。

(4) 由环和运算定义和教材例 1.7 可知，$G_i\oplus G_i=\varnothing$。从而 Ω 中每个元素都有逆元。

(5) 若 $a=b=1$，则 $(ab)G_i=1\cdot G_i=1\cdot(1\cdot G_i)=a(b\cdot G_i)$，若 $a=0\vee b=0$，则 $(ab)G_i=0\cdot G_i=\varnothing=a(b\cdot G_i)$，从而数乘运算满足结合律。

(6) 由定义，有 $1\in\{0,1\}$ 且 $1\cdot G_i=G_i$，从而 1 是关于数乘运算的单位元。

(7) 若 $a+b=1$，则有 $a=1\wedge b=0$ 或 $a=0\wedge b=1$，从而 $(a+b)G_i=1\cdot G_i=\varnothing\oplus 1\cdot G_i=0\cdot G_i\oplus 1\cdot G_i=a\cdot G_i\oplus b\cdot G_i$。若 $a+b=0$，则有 $a=b$。从而有 $(a+b)G_i=0\cdot G_i=\varnothing=a\cdot G_i\oplus a\cdot G_i=a\cdot G_i\oplus b\cdot G_i$。从而数乘对 F 上的加法满足分配律。

(8) 若 $a=1$，则 $a(G_i\oplus G_j)=G_i\oplus G_j=a\cdot G_i\oplus a\cdot G_j$；若 $a=0$，则 $a(G_i\oplus G_j)=\varnothing=\varnothing\oplus\varnothing=a\cdot G_i\oplus a\cdot G_j$。从而数乘对环和运算满足分配律。

这就证明了 Ω 对环和运算和数乘运算构成 $\{0,1\}$ 上的线性空间。

M 中各元素的独立性是显然的。而对任何 $G_i=G[\{e_{i_1},e_{i_2},\cdots,e_{i_t}\}]\in\Omega$，易见，$G_i=g_{i_1}\oplus g_{i_2}\oplus\cdots\oplus g_{i_t}$。从而 M 是 Ω 的生成元集。 □

9.16 任取一棵生成树 T，例如，取 $T=G[\{a,f,g,b\}]$，则

T 对应的基本回路有：$C_c=acbgf, C_d=adbgf, C_e=efg$。

$C_{基}=\{C_c,C_d,C_e\}$。

$C_c\oplus C_d=cd$；

$C_c\oplus C_e=acbe$；

$C_d\oplus C_e=adbe$；

$C_c\oplus C_d\oplus C_e=cd\cup C_e$；

$C_{环}=\{\varnothing,C_c,C_d,C_e,cd,acbe,adbe,cd\cup C_e\}$。

T 对应的基本割集为 $S_a=\{a,c,d\}, S_b=\{b,c,d\}, S_f=\{c,d,e,f\}, S_g=\{c,d,e,g\}$。

$S_a\oplus S_b=\{a,b\}$；

$S_a\oplus S_f=\{a,e,f\}$；

$S_a\oplus S_g=\{a,e,g\}$；

$S_b\oplus S_f=\{b,e,f\}$；

$S_b\oplus S_g=\{b,e,g\}$；

$S_f\oplus S_g=\{f,g\}$；

$S_a\oplus S_b\oplus S_f=\{a,b,c,d,e,f\}$；

$S_a\oplus S_b\oplus S_g=\{a,b,c,d,e,g\}$；

$S_a\oplus S_f\oplus S_g=\{a,c,d,f,g\}$；

$S_b\oplus S_f\oplus S_g=\{b,c,d,f,g\}$；

$S_a\oplus S_b\oplus S_f\oplus S_g=\{a,b,f,g\}$；

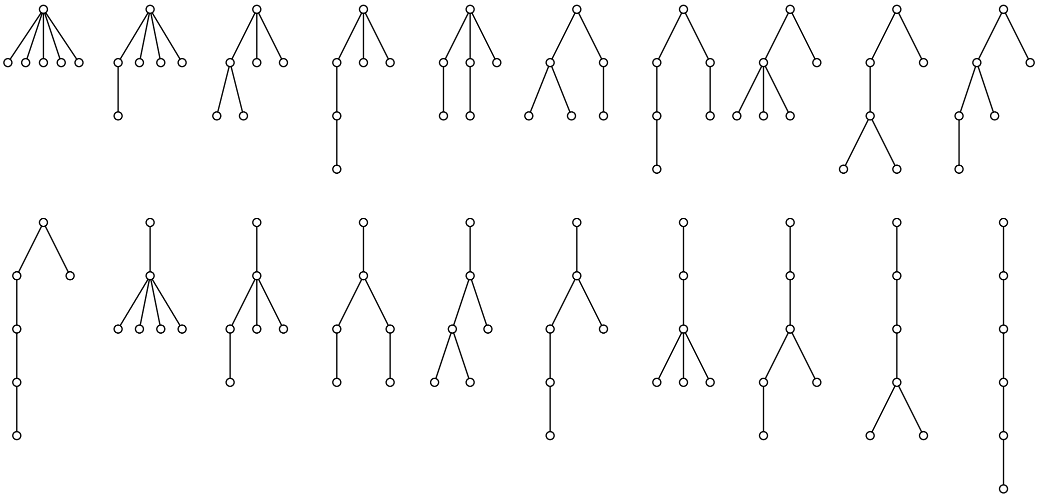
$S_{断}=\{\varnothing,S_a,S_b,S_f,S_g,S_a\oplus S_b,S_a\oplus S_f,S_a\oplus S_g,S_b\oplus S_f,S_b\oplus S_g,S_f\oplus S_g,S_a\oplus S_b\oplus S_f,S_a\oplus S_b\oplus S_g,S_a\oplus S_f\oplus S_g,S_b\oplus S_f\oplus S_g,S_a\oplus S_b\oplus S_f\oplus S_g\}$。

9.17

证明: 必要性是显然的。下面证充分性。

设 $V(T)=\{v_1,v_2,\cdots,v_n\}$，其中 $d^-(v_1)=0$。只需证 $d^-(v_i)=1(i=2,3,\cdots,n)$ 即可。注意到，由题设，v_1 是唯一入度为 0 的顶点，而任何顶点的入度都不可能小于 0。因此，对所有 $i=2,3,\cdots,n$，必有 $d^-(v_i)\geq 1$。反设除 v_1 外，还有其它入度不为 1 的顶点(不妨设为 v_2)，则必有 $d^-(v_2)\geq 2$。从而 $m=\sum\limits_{i=1}^{n}d^-(v_i)=d^-(v_1)+d^-(v_2)+\sum\limits_{i=3}^{n}d^-(v_i)\geq 0+2+(n-2)=n$。然而 T 是树，所以应有 $m=n-1<n$，矛盾。 □

9.18 共 20 棵。见下图：



9.19 首先证明如下结论：

引理 9.5 设 T 为 k 叉正则树 $(k \geq 1)$，且 T 中有 t 片树叶和 i 个分支点，则

$$t = (k-1)i + 1.$$

证明: 由题设可知，T 中各顶点出度之和为 ki，各顶点入度之和为 $t+i-1$。从而由图论基本定理有

$$ki = \sum_{v_i \in V(T)} d^+(v_i) = \sum_{v_i \in V(T)} d^-(v_i) = t + i - 1$$

整理得 $t = (k-1)i + 1$。 □

再证原题。

证明: 对 T 的高度 k 作归纳。

当 $k = 0$ 时，$L = I = 0$。命题成立。

设对所有 $k < t (t \geq 1)$，命题都成立。当 $k = t$ 时，对任意高度为 k 的 2 叉正则树 T，设 v_0 是 T 的树根且 T 中共有 l 片树叶，T_1 和 T_2 分别是 v_0 的两个子顶点导出的子树。i_1, l_1, I_1, L_1 和 i_2, l_2, I_2, L_2 分别是 T_1 和 T_2 中的分支点数、树叶数、各分支点的层数之和以及各树叶的层数之和。由归纳假设，有 $L_1 = I_1 + 2i_1$ 和 $L_2 = I_2 + 2i_2$。

注意到，除 v_0 外，T 中的每一个分支点都在 $V(T_1) \cup V(T_2)$ 中，且 $V(T_1) \cap V(T_2) = \varnothing$。所以应有 $i = i_1 + i_2 + 1$。由于 T 的高度 $t \geq 1$，所以 v_0 不可能是树叶。因此，T 的树叶全都在 $V(T_1) \cup V(T_2)$ 中。所以有 $l = l_1 + l_2$。另一方面，$V(T_1) \cup V(T_2)$ 中每一个顶点相对 T_1 (或 T_2)的层数这一顶点相对于 T 的层数少 1，且 v_0 在 T 中的层数为 0。因此有 $I = I_1 + i_1 + I_2 + i_2$ 和 $L = L_1 + l_1 + L_2 + l_2$。

从而有：

$$\begin{aligned}
L &= L_1 + l_1 + L_2 + l_2 \\
&= (I_1 + 2i_1) + l_1 + (I_2 + 2i_2) + l_2 && \text{(归纳假设)} \\
&= I + i_1 + i_2 + l_1 + l_2 && (I = I_1 + I_2 + i_1 + i_2) \\
&= I + i_1 + i_2 + l && (l = l_1 + l_2) \\
&= I + i_1 + i_2 + i + 1 && \text{(引理 9.5)} \\
&= I + 2i && (i = i_1 + i_2 + 1)
\end{aligned}$$

这就证明了当 $k = t$ 时，命题也成立。 □

9.20

证明: 由 2 叉正则树定义可知，T 中共有 $n = t + i$ 个顶点。由引理 9.5 可知，$t = i + 1$，也即 $i = t - 1$。从而有

$$\begin{aligned} m &= n - 1 && (T \text{ 是树}) \\ &= t + i - 1 && (n = t + i) \\ &= t + (t - 1) - 1 && (i = t - 1) \\ &= 2t - 2 \end{aligned}$$

□

9.21 波兰符号法：$+\div-+a{*}{*}bcde+fg{*}{*}hij$。

逆波兰符号法：$abc{*}d{*}+e-fg+\div hi{*}j{*}+$。

第十章　图的矩阵表示

10.1

(**a**)

$$\begin{bmatrix} -1 & 1 & 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 1 \end{bmatrix}$$

(**b**)

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

10.2　e_6 为桥，易知 G 的生成树必含 e_6。因此只需求出 $G - e_6$ 的生成树。

$G - e_6$ 的关联矩阵为 $M = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$

以 v_4 为参考点，得基本关联矩阵为 $M_f = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$

求 M_f 的所有 3 阶子方阵的行列式，要求计算结果属于 $F = \{0, 1\}$，
子方阵的个数为 $C_5^3 = 10$，它们的行列式依次为：

$$(1)\ \begin{bmatrix}1&0&0\\0&1&1\\0&0&1\end{bmatrix}=1 \qquad (2)\ \begin{bmatrix}1&0&1\\0&1&1\\0&0&0\end{bmatrix}=0 \qquad (3)\ \begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}=1$$

$$(4)\ \begin{bmatrix}1&0&0\\0&1&0\\0&1&1\end{bmatrix}=1 \qquad (5)\ \begin{bmatrix}1&1&0\\0&1&0\\0&0&1\end{bmatrix}=1 \qquad (6)\ \begin{bmatrix}1&0&1\\0&1&1\\0&1&0\end{bmatrix}=-1=1 \pmod 2$$

$$(7)\ \begin{bmatrix}0&0&1\\1&1&1\\0&1&0\end{bmatrix}=1 \qquad (8)\ \begin{bmatrix}0&0&0\\1&1&0\\0&1&1\end{bmatrix}=0 \qquad (9)\ \begin{bmatrix}0&1&0\\1&1&0\\0&0&1\end{bmatrix}=-1=1 \pmod 2$$

$$(10)\ \begin{bmatrix}0&1&0\\1&1&0\\1&0&1\end{bmatrix}=-1=1 \pmod 2$$

在所有的 3 边组合中，除 e_1, e_2, e_4 和 e_2, e_3, e_5 的导出子图不是 $G-e_6$ 的生成树外，其它的导出子图均为 $G-e_6$ 的生成树。$G-e_6$ 的生成树加上 e_6 后，即为 G 的生成树。

10.3 完全图 K_4 的关联矩阵为 $M=\begin{bmatrix}1&0&0&1&1&0\\1&1&0&0&0&1\\0&1&1&0&1&0\\0&0&1&1&0&1\end{bmatrix}$

以v_1为参考点，得基本关联矩阵为$M_f=\begin{bmatrix}1&1&0&0&0&1\\0&1&1&0&1&0\\0&0&1&1&0&1\end{bmatrix}$

求 M_f 的所有 3 阶子方阵的行列式，要求计算结果属于 $F=\{0,1\}$，子方阵的个数为 $C_6^3=20$，它们的行列式依次为：

$$(1)\ \begin{bmatrix}1&1&0\\0&1&1\\0&0&1\end{bmatrix}=1 \qquad (2)\ \begin{bmatrix}1&1&0\\0&1&0\\0&0&1\end{bmatrix}=1 \qquad (3)\ \begin{bmatrix}1&1&0\\0&1&1\\0&0&0\end{bmatrix}=0$$

$$(4)\ \begin{bmatrix}1&1&1\\0&1&0\\0&0&1\end{bmatrix}=1 \qquad (5)\ \begin{bmatrix}1&0&0\\0&1&0\\0&1&1\end{bmatrix}=1 \qquad (6)\ \begin{bmatrix}1&0&0\\0&1&1\\0&1&0\end{bmatrix}=-1=1 \pmod 2$$

$$(7)\ \begin{bmatrix}1&0&1\\0&1&0\\0&1&1\end{bmatrix}=1 \qquad (8)\ \begin{bmatrix}1&0&1\\0&0&0\\0&1&1\end{bmatrix}=0 \qquad (9)\ \begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix}=-1=1 \pmod 2$$

(10) $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = 1$ (11) $\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = 1$ (12) $\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} = -1 = 1 \pmod 2$

(13) $\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} = 1$ (14) $\begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} = 1$ (15) $\begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = -1 = 1 \pmod 2$

(16) $\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = 1$ (17) $\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} = 0$ (18) $\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = 2 = 0 \pmod 2$

(19) $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} = -1$ (20) $\begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} = -1 = 1 \pmod 2$

在所有的 3 边组合中，除 e_1, e_2, e_5；e_1, e_4, e_6；e_3, e_4, e_5 和 e_2, e_3, e_6 的导出子图不是 K_4 的生成树外，其它 3 条边的导出子图均为 K_4 的生成树。

10.4

$$A^1 = \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \qquad A^2 = \begin{bmatrix} 1 & 2 & 2 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

$$A^3 = \begin{bmatrix} 3 & 2 & 2 & 2 \\ 1 & 2 & 1 & 0 \\ 2 & 2 & 2 & 1 \\ 1 & 2 & 1 & 0 \end{bmatrix} \qquad A^4 = \begin{bmatrix} 5 & 6 & 4 & 2 \\ 2 & 2 & 2 & 1 \\ 4 & 4 & 3 & 2 \\ 2 & 2 & 2 & 1 \end{bmatrix}$$

(1) v_1 到 v_4 长度为 1 的通路有 0 条；
v_1 到 v_4 长度为 2 的通路有 0 条；
v_1 到 v_4 长度为 3 的通路有 2 条；
v_1 到 v_4 长度为 4 的通路有 2 条。

(2) v_1 到 v_4 长度小于等于 3 的通路有 2 条。

(3) v_1 到 v_1 长度为 1 的回路有 1 条；
v_1 到 v_1 长度为 2 的回路有 1 条；
v_1 到 v_1 长度为 3 的回路有 3 条；
v_1 到 v_1 长度为 4 的回路有 5 条。

(4) v_4 到 v_4 长度小于等于 3 的回路有 1 条。

(5) D 中长度为 4 的通路（不含回路）有 33 条。

(6) D 中长度为 4 的回路有 11 条。

(7) D 中长度小于等于 4 的通路有 88 条；
D 中长度小于等于 4 的回路有 22 条。

(8) $P(D) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$

10.5

$$A^1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \qquad A^2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{bmatrix} \qquad A^3 = \begin{bmatrix} 0 & 2 & 0 \\ 2 & 0 & 2 \\ 0 & 2 & 0 \end{bmatrix}$$

$$A^4 = \begin{bmatrix} 2 & 0 & 2 \\ 0 & 4 & 0 \\ 2 & 0 & 2 \end{bmatrix} \qquad A^5 = \begin{bmatrix} 0 & 4 & 0 \\ 4 & 0 & 4 \\ 0 & 4 & 0 \end{bmatrix} \qquad A^6 = \begin{bmatrix} 4 & 0 & 4 \\ 0 & 8 & 0 \\ 4 & 0 & 4 \end{bmatrix}$$

……

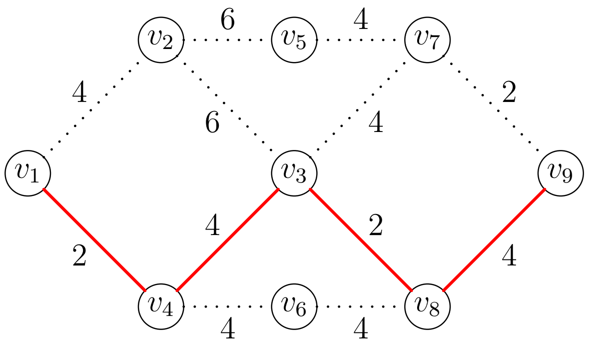
当 k 为奇数时，$a_{22}^{(k)} = 0$；
当 k 为偶数时，$a_{22}^{(k)} = 2^{k/2}$。

第十四章　带权图及其应用

14.1

	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9
0	$\boxed{0}$	4	∞	2	∞	∞	∞	∞	∞
1		4	6	$\boxed{2}$ $/v_1$	∞	6	∞	∞	∞
2		$\boxed{4}$ $/v_1$	6		10	6	∞	∞	∞
3			$\boxed{6}$ $/v_4$		10	6	10	8	∞
4					10	$\boxed{6}$ $/v_4$	10	8	∞
5					10		10	8	12
6					$\boxed{10}$ $/v_2$		10		12
7							$\boxed{10}$ $/v_3$		12
8									$\boxed{12}$ $/v_8$
	0	4	6	2	10	6	10	8	12

由上表可以看出：v_1 到 v_9 的最短路径为 $v_1v_4v_3v_8v_9$，如下图红色路径所示，其权为 12。



14.2

	v_1	v_2	v_3	v_4	v_5	v_6
0	$\boxed{0}$	1	4	∞	∞	∞
1		$\boxed{1}$ $/v_1$	3	8	6	∞
2			$\boxed{3}$ $/v_2$	8	4	∞
3				7	$\boxed{4}$ $/v_3$	10
4				$\boxed{7}$ $/v_5$		9
5						$\boxed{9}$ $/v_4$
	0	1	3	7	4	9

由上表可以看出：

v_1 到 v_2 的最短路径为 v_1v_2，其权为 1。

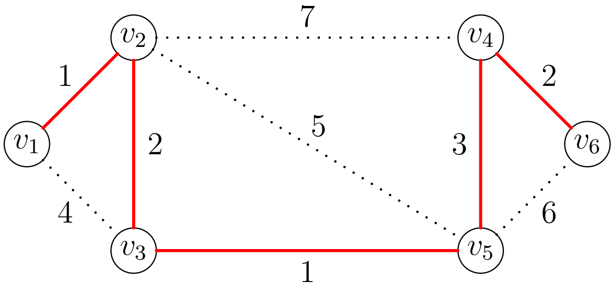
v_1 到 v_3 的最短路径为 $v_1v_2v_3$，其权为 3。

v_1 到 v_4 的最短路径为 $v_1v_2v_3v_5v_4$，其权为 7。

v_1 到 v_5 的最短路径为 $v_1v_2v_3v_5$，其权为 4。

v_1 到 v_6 的最短路径为 $v_1v_2v_3v_5v_4v_6$，其权为 9。

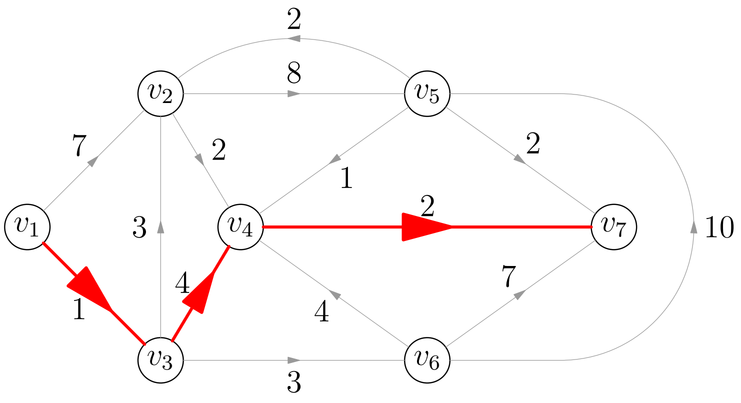
最短路径如下图红色路径所示。



14.3

	v_1	v_2	v_3	v_4	v_5	v_6	v_7
0	$\boxed{0}$	7	1	∞	∞	∞	∞
1		4	$\boxed{1}$ $/v_1$	5	∞	4	∞
2		$\boxed{4}$ $/v_3$		5	12	4	∞
3				5	12	$\boxed{4}$ $/v_3$	11
4				$\boxed{5}$ $/v_3$	12		7
5					12		$\boxed{7}$ $/v_4$
6					$\boxed{12}$ $/v_2$		
	0	4	1	5	12	4	7

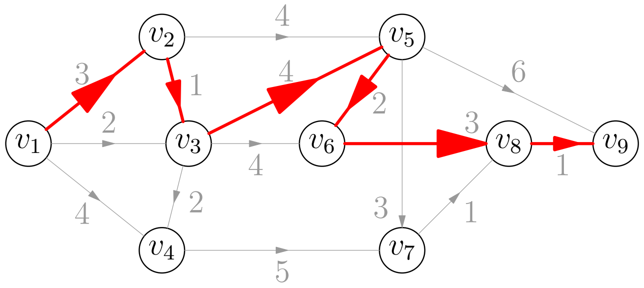
由上表可以看出：v_1 到 v_7 的最短路径为 $v_1v_3v_4v_7$，如下图红色路径所示，其权为 7。



14.4

v_i	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9
$TE(v_i)$	0	3	4	6	8	10	11	13	14
$TL(v_i)$	0	3	4	7	8	10	12	13	14
$TS(v_i)$	0	0	0	1	0	0	1	0	0

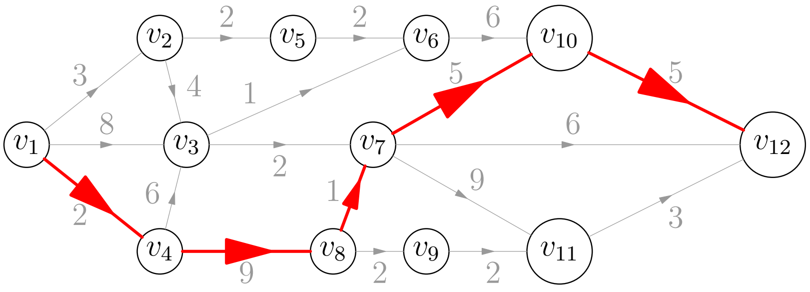
由上表可以看出：关键路径为 $v_1v_2v_3v_5v_6v_8v_9$，下图中的红色路径即为关键路径。



14.5

v_i	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9	v_{10}	v_{11}	v_{12}
$TE(v_i)$	0	3	8	2	5	9	12	11	13	17	18	22
$TL(v_i)$	0	6	10	2	9	11	12	11	17	17	19	22
$TS(v_i)$	0	3	2	0	4	2	0	0	4	0	1	0

由上表可以看出：关键路径为 $v_1v_4v_8v_7v_{10}v_{12}$，下图中的红色路径即为关键路径。



14.6

证明: 用反证法。

假设不存在这样的 u，使得 u 的先驱元集中的元素均在 P_E 中。即 $\forall u \in T_E, \exists w(u \neq w)$ 使得 $w \in T_E$ 且 $w \in \Gamma^-(u)$。

由教材定义 14.1(2) 知，D 中有一个入度为 0 的顶点 v_1，而 v_1 在 P_E 中，即 T_E 中的点的先驱元集均不为空，由于 $T_E \neq \varnothing$，在 T_E 中任取一点，记为 u_1，由假设知 $\exists u_2(u_2 \neq u_1)u_2 \in T_E$ 且 $u_2 \in \Gamma^-(u_1)$。由假设知，$\exists u_3(u_3 \neq u_2)$，由 D 中无回路知：$u_3 \neq u_1, u_3 \in T_E$ 且 $u_3 \in \Gamma^-(u_1)$。由 D 是 n 阶图知，D 是有限图，$|T_E|$ 是有限值。继续直到 u_{T_E}，由假设知 $u_{|T_E|+1}$，$u_{|T_E|+1} \in T_E$，由抽屉原则知，$u_{|T_E|+1}$ 必为 $u_1 \cdots u_{|T_E|}$ 中的一个。推出 D 中有回路，与教材定义 14.1 矛盾，假设错误，即存在这样的 u。 □

14.7

证明: 用反证法。

假设不存在这样的 u，使得 u 的后继元集中的元素均在 P_L 中。即 $\forall u \in T_L, \exists w(u \neq w)$ 使得 $w \in T_L$ 且 $w \in \Gamma^+(u)$。

由 V_n 在 P_L 中且 D 中有一个顶点出度为 0 知，存在这样的 w。在 T_L 中任取一点 u_1，由假设知：$\exists u_2(u_2 \neq u_1)$ 使得 $u_2 \in T_L$ 且 $u_2 \in \Gamma^+(u_1)$。继续构造 $u_3, u_4, \cdots$，新点不能与已构造序列中的任何一点相同，否则会产生回路。而由 D 是有限图知，T_L 为有限值，当构造完 $u_{|T_L|}$ 时，由抽屉原则知，$u_{|T_L|+1}$ 必与 $u_1, u_2, \cdots u_{|T_L|}$ 中的某一点重合，产生回路，与教材定义 14.1(1) 相矛盾。故假设错误，即存在这样的 u。 □

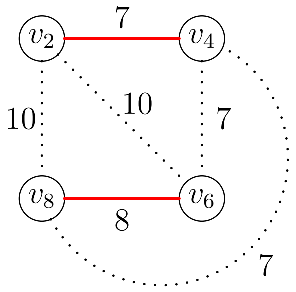
14.8 奇度顶点集 $V' = \{v_2, v_4, v_6, v_8\}$，$|V'| = 4$。用 $Dijkatra$ 算法容易求出：

v_2 到 v_4 的最短路径为 $v_2v_1v_4$，其权为 7；v_2 到 v_6 的最短路径为 $v_2v_5v_6$，其权为 10；

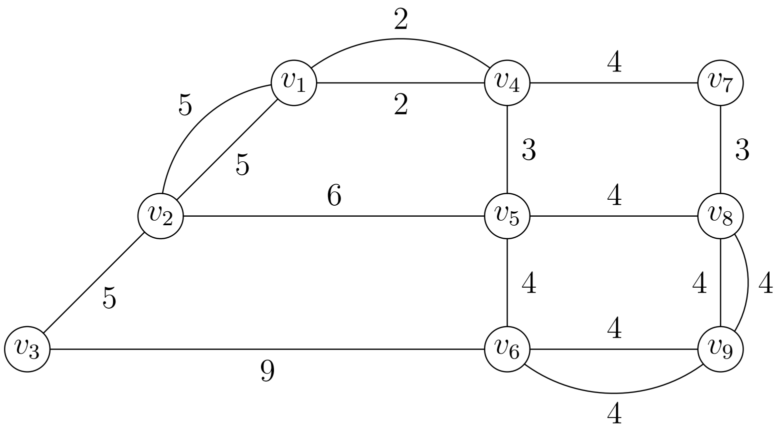
v_2 到 v_8 的最短路径为 $v_2v_5v_8$，其权为 10；v_4 到 v_6 的最短路径为 $v_4v_5v_6$，其权为 7；

v_4 到 v_8 的最短路径为 $v_4v_5v_8$，其权为 7；v_6 到 v_8 的最短路径为 $v_6v_5v_8$，其权为 8。

这 4 个顶点所对应的完全图 K_4 如下图所示。图中两条红色路径为最小完美匹配 $M = \{(v_2, v_4), (v_6, v_8)\}$。



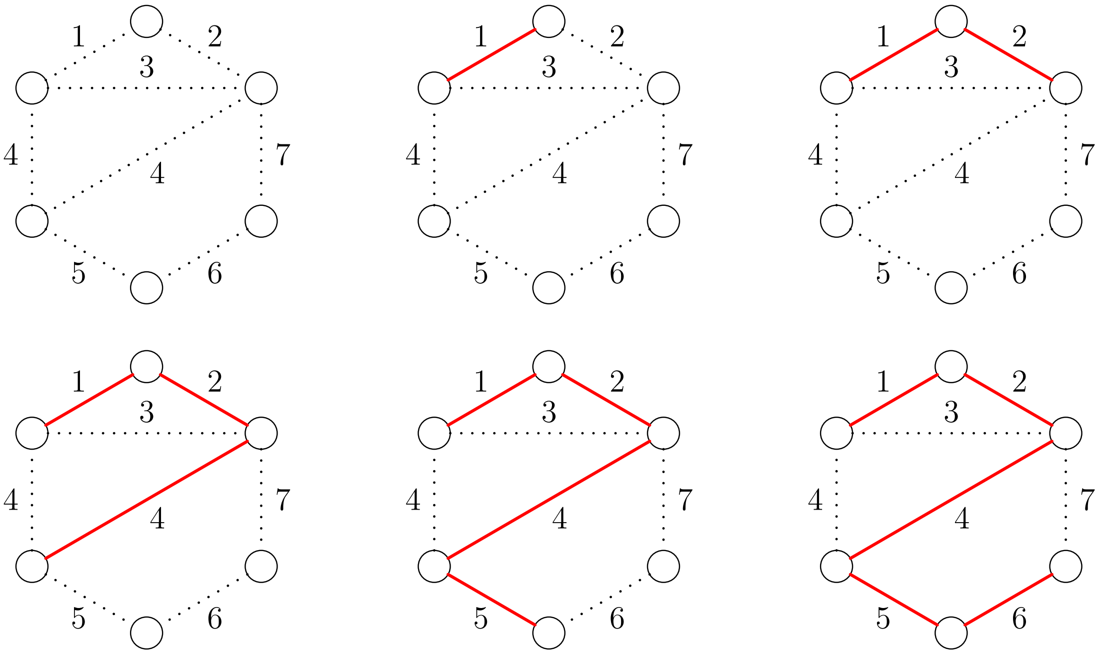
在题图中，将 K_4 中 v_2v_4 和 v_6v_8 对应的最短路径上的各边重复一次所得到的欧拉图如下图所示。



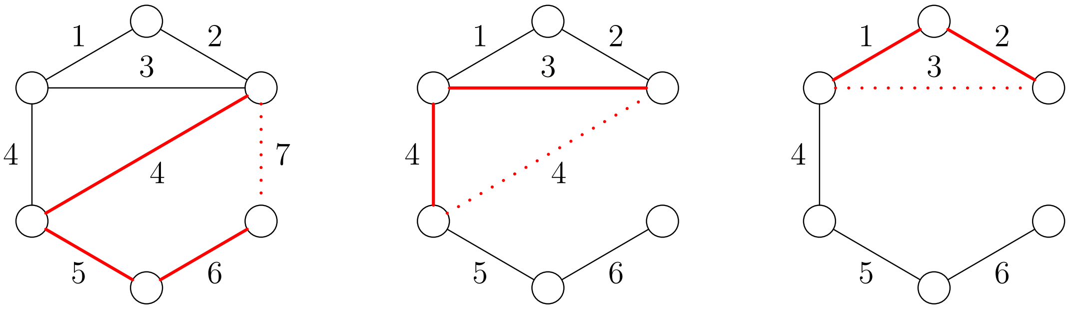
最优投递路线的一个解为：$v_2v_1v_4v_7v_8v_5v_8v_9v_6v_5v_6v_3v_2v_5v_4v_1v_2$，其权为68。

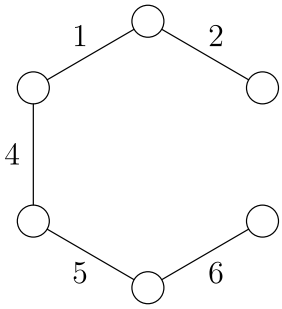
14.9

(1) 避圈法：

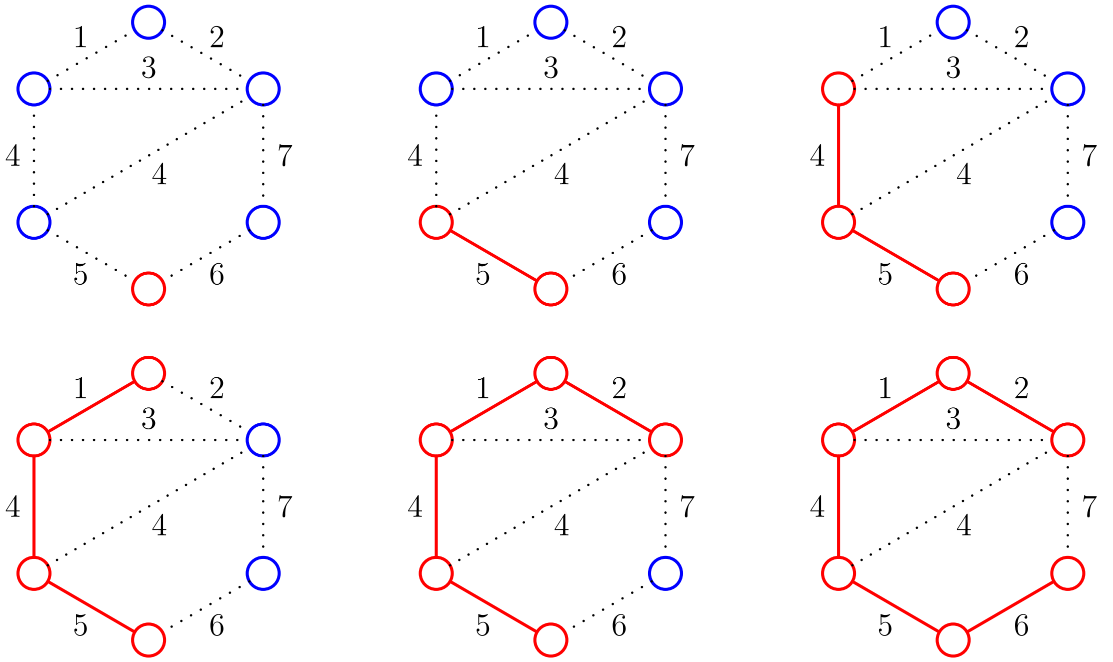


(2) 破圈法：

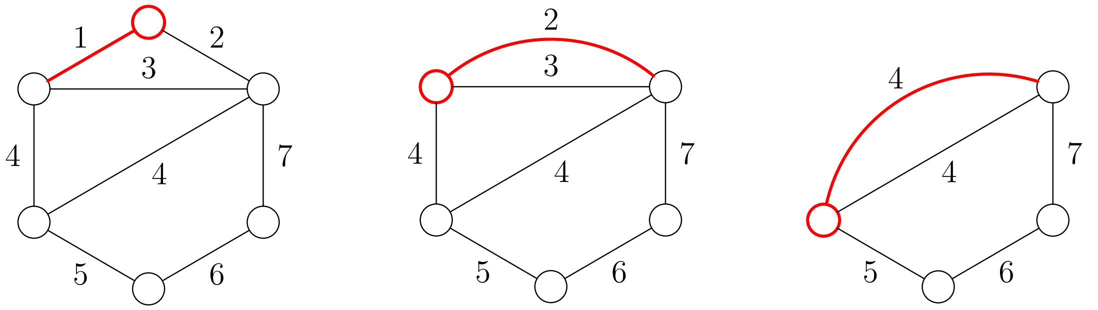


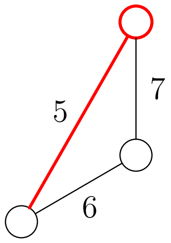


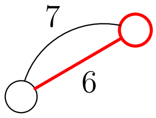
(3) 断集法：

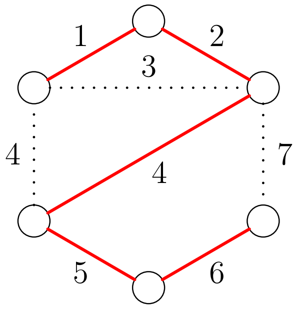


(4) 逐步短接法：







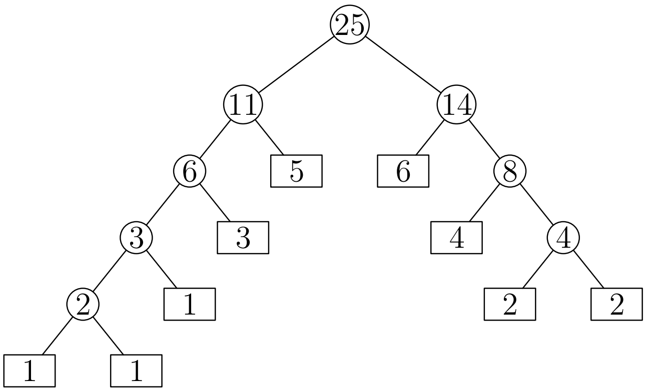


14.10

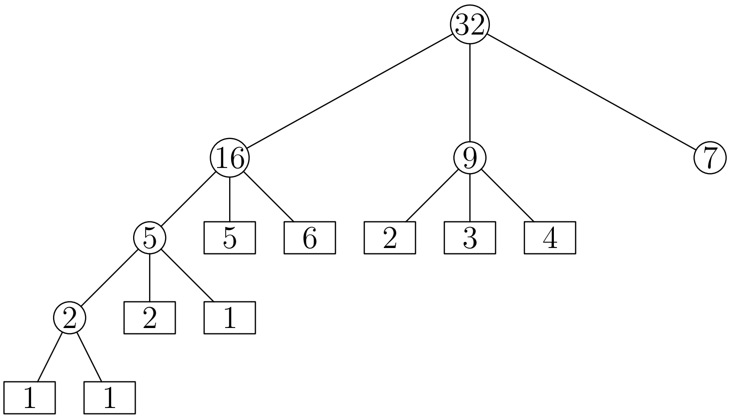
证明： 由题设知，$m = i * r$ 和 $n = i + t$；由教材定理 9.1知，$m = n - 1$。解之，$(r-1)i = t-1$。□

14.11

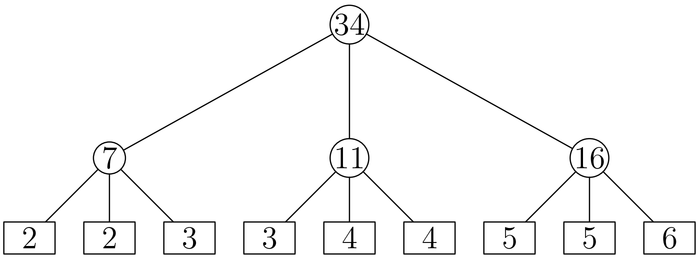
(1) 最优二叉树如下图所示，其权为 73。



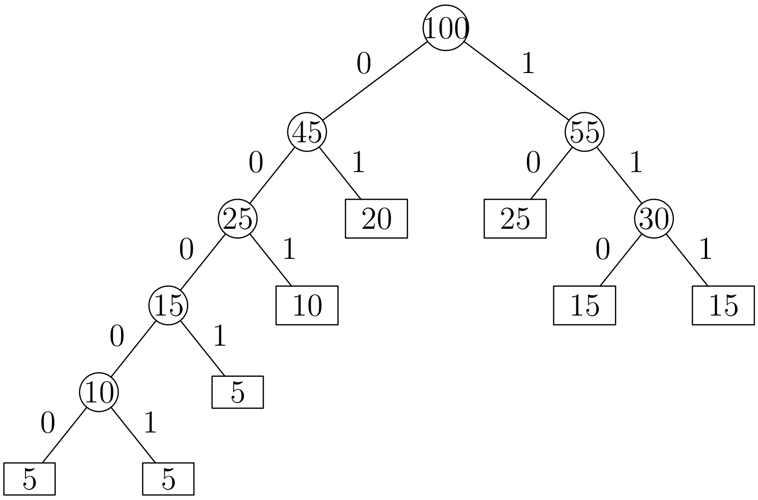
(2) 权所对应的最优 3 叉树不是正则的，最优 3 叉树如下图所示，其权为 64。



(3) 权所对应的最优 3 叉树是正则的，最优 3 叉树如下图所示，其权为 68。



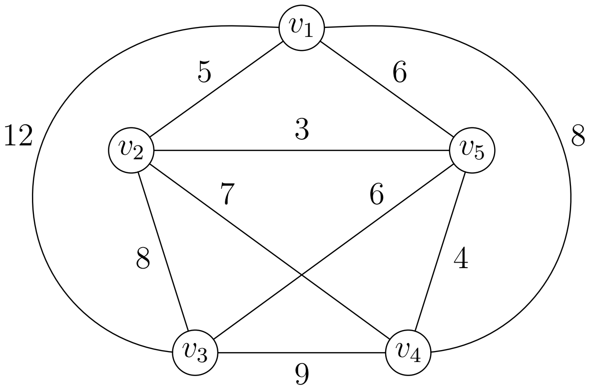
14.12 $w_i = 100p_i, i = a, b, c, d, e, f, g, h$，按从小到大的顺序为 $5 \leq 5 \leq 5 \leq 10 \leq 15 \leq 15 \leq 20 \leq 25$，所对应的最优树如下图所示。



a, b, c, d, e, f, g, h 对应的前缀码为：

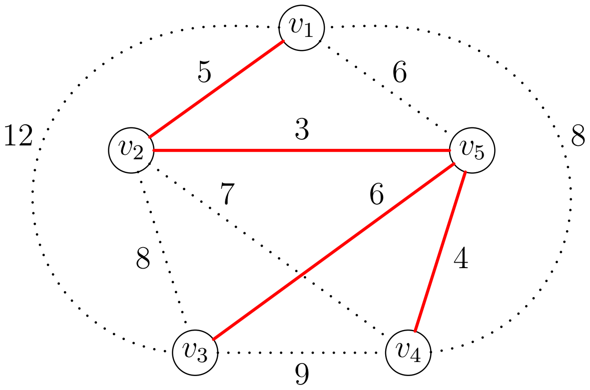
$a - 10$	$b - 01$
$c - 110$	$d - 111$
$e - 001$	$f - 0001$
$g - 00000$	$h - 00001$

14.13 题图如下图所示。

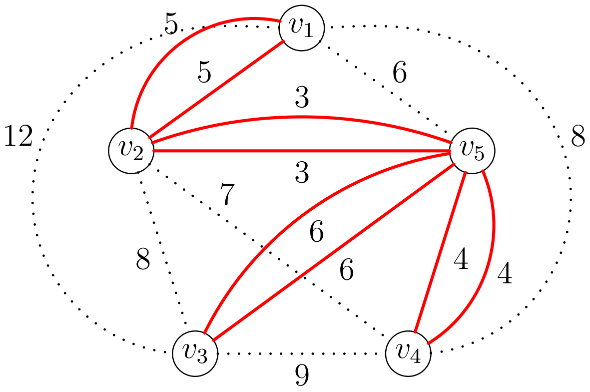


(1) 始于 v_1 的哈密顿回路为：$v_1v_2v_5v_4v_3v_1$，其权为 33。

(2) 第一步：求最小生成树 T，如下图所示。



第二步：将 T 中的各边加平行边，如下图所示。



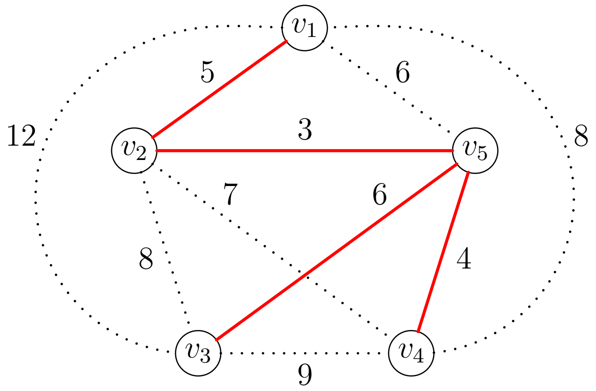
第三步：从 v_1 出发的欧拉回路有 2 条：

$E_{v_1,1} = v_1v_2v_5v_3v_5v_4v_5v_2v_1$，$H_{v_1,1} = v_1v_2v_5v_3v_4v_1$，$W(H_{v_1,1}) = 31$；

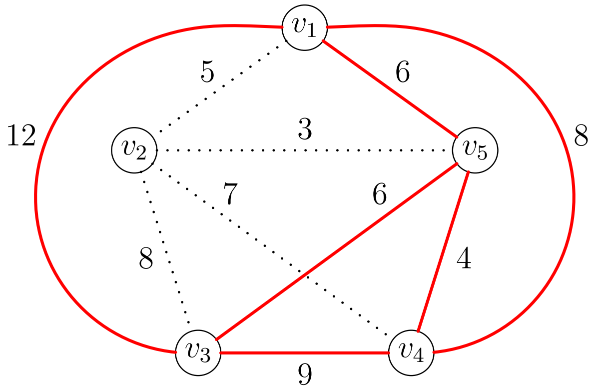
$E_{v_1,2} = v_1v_2v_5v_4v_5v_3v_5v_2v_1$，$H_{v_1,2} = v_1v_2v_5v_4v_3v_1$，$W(H_{v_1,2}) = 33$。

从 v_2 出发的欧拉回路有 4 条：

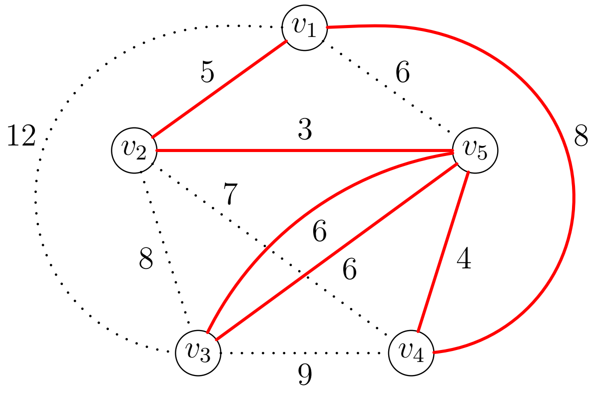
$E_{v_2,1} = v_2v_1v_2v_5v_4v_5v_3v_5v_2$，$H_{v_2,1} = v_2v_1v_5v_4v_3v_2$，$W(H_{v_2,1}) = 32$；
$E_{v_2,2} = v_2v_1v_2v_5v_3v_5v_4v_5v_2$，$H_{v_2,2} = v_2v_1v_5v_3v_4v_2$，$W(H_{v_2,2}) = 33$；
$E_{v_2,3} = v_2v_5v_3v_5v_4v_5v_2v_1v_2$，$H_{v_2,3} = v_2v_5v_3v_4v_1v_2$，$W(H_{v_2,3}) = 33$，
$E_{v_2,4} = v_2v_5v_4v_5v_3v_5v_2v_1v_2$，$H_{v_2,4} = v_2v_5v_4v_3v_1v_2$，$W(H_{v_2,4}) = 33$。
(3) 第一步：求最小生成树 T，如下图所示。



第二步：T 中奇度顶点集合 $V' = \{v_1, v_3, v_4, v_5\}$。$G[V']$ 如下图所示。



最小权完美匹配 $M = \{(v_1, v_4), (v_3, v_5)\}$，将 M 中的边加到 T 上所得欧拉图 G^* 如下图所示。



第三步：从 v_1 出发的欧拉回路有 2 条：
$E_{v_1,1} = v_1v_2v_5v_3v_5v_4v_1$，$H_{v_1,1} = v_1v_2v_5v_3v_4v_1$，$W(H_{v_1,1}) = 31$；

$E_{v_1,2} = v_1v_4v_5v_3v_5v_2v_1$，$H_{v_1,2} = v_1v_4v_5v_3v_2v_1$，$W(H_{v_1,2}) = 31$。

(4) 遍历。共 12 条哈密顿回路，分别为：

$v_1v_2v_3v_4v_5v_1$，其权为 32；$v_1v_2v_3v_5v_4v_1$，其权为 31；

$v_1v_2v_4v_3v_5v_1$，其权为 33；$v_1v_2v_4v_5v_3v_1$，其权为 34；

$v_1v_2v_5v_3v_4v_1$，其权为 31；$v_1v_2v_5v_4v_3v_1$，其权为 33；

$v_1v_3v_2v_4v_5v_1$，其权为 37；$v_1v_3v_2v_5v_4v_1$，其权为 35；

$v_1v_4v_2v_3v_5v_1$，其权为 35；$v_1v_4v_2v_5v_3v_1$，其权为 36；

$v_1v_5v_2v_3v_4v_1$，其权为 34；$v_1v_5v_2v_4v_3v_1$，其权为 37。

综上，最优解有 2 个。$v_1v_2v_3v_5v_4v_1$ 和 $v_1v_2v_5v_3v_4v_1$，权为 31。

第三编

代数结构

第十五章　代数系统

15.1

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

15.2　A 上的函数共有 4 个。分别是：

$f_1 = \{\langle 0,0\rangle, \langle 1,1\rangle\}$；
$f_2 = \{\langle 0,1\rangle, \langle 1,0\rangle\}$；
$f_3 = \{\langle 0,0\rangle, \langle 1,0\rangle\}$；
$f_4 = \{\langle 0,1\rangle, \langle 1,1\rangle\}$。

其中 f_1 是恒等函数，是关于 $\circ$ 运算的单位元。f_3 和 f_4 是常数函数，是关于 $\circ$ 运算的左零元。

运算表为：

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_3	f_3	f_3
f_4	f_4	f_4	f_4	f_4

15.3

i	1	2	3	4	5
$\tau(i)$	2	3	4	5	1

注：题中 τ 的计算公式应为 $\tau(i) = (i \bmod n) + 1$，否则运算对 A 不封闭。

15.4

集合	运算	封闭	交换	结合	幂等	消去	分配	吸收	单位元	零元
$\mathbb{Z}$	普通减法	是	否	否	否	是	—	—	无	无
$\mathbb{Z}^*$	普通乘法	是	是	是	否	是	—	—	1	无
$\mathbb{N}_{奇}$	普通加法	否	—	—	—	—	—	—	—	—
	普通乘法	是	是	是	否	是	—		1	无
$M_n(\mathbb{R})$	矩阵加法	是	是	是	否	是	否	否	全 0 矩阵	无
	矩阵乘法	是	否	是	否	否	对加法		单位矩阵	全 0 矩阵
$GL_n(\mathbb{R})$	矩阵加法	否	—	—	—	—	—	—	—	—
	矩阵乘法	是	否	是	否	是	—		单位矩阵	无
$n\mathbb{Z}$	普通加法	是	是	是	否	是	否	否	0	无
	普通乘法	是	是	是	否	是	对加法		无^{注}	0
$\mathbb{R}^+$	$ab-a-b$	否	—	—	—	—	—	—	—	—
$\{a_i\}$	$a \circ b = b$	是	否	是	是	否	—	—	无	无
$R(A)$	关系合成	是	否	是	否	否	—	—	I_A	$\varnothing$
$\mathbb{Z}^+$	$\gcd(a,b)$	是	是	是	是	否	对 lcm	是	无	1
	$\mathrm{lcm}(a,b)$	是	是	是	是	否	对 gcd		1	无

注：仅当 $n=1$ 时，$n\mathbb{Z}$ 有乘法单位元 1。

15.5

(1) 不能，除非允许 a,b,c 全等(此时令 $a=b=c=0$ 即可)。

(2) 能。令 $A=\{-1,0,1\}$ 即可。

15.6

(1) 构成代数系统。运算适合交换律、结合律。单位元是取值恒为 0 的常数函数，无零元。

(2) 构成代数系统。运算不适合交换律，也不适合结合律。无单位元(取值恒为 0 的常数函数是右单位元)，无零元。

(3) 构成代数系统。运算适合交换律、结合律。单位元是取值恒为 1 的常数函数，零元是取值恒为 0 的常数函数。

(4) 不构成代数系统。当 $g(x)$ 取值为 0 时，函数 $f/g \notin S$。故运算在 S 上不封闭。

15.7

(1) 构成代数系统。运算适合交换律、结合律、幂等律。单位元是 1，无零元。

(2) 构成代数系统。运算适合交换律、结合律、幂等律。零元是 1，无单位元。

(3) 构成代数系统。运算不适合交换律、结合律或幂等律。1 是左零元和右单位元。运算无右零元和左单位元，因而没有零元和单位元。

(4) 不构成代数系统。当 $ab \nmid a+b$ 时，函数 $a/b+b/a \notin \mathbb{Z}^+$。故运算在 $\mathbb{Z}^+$ 上不封闭。

15.8

结论 1：运算满足交换律当且仅当 $p=q$。

证明： 充分性显然。下面证必要性：

取 $a=1, b=0$，若运算满足交换律，则有：

$$a \circ b = b \circ a$$

$$\iff pa+qb+r = qa+pb+r \qquad (\circ\ \text{运算定义})$$

$$\iff p+r = q+r \qquad (a=1, b=0)$$

$$\iff p=q \qquad (\text{加法消去律})$$

必要性得证。 □

结论 2：运算满足结合律当且仅当 $p, q \in \{0,1\} \wedge (p = q \vee r = 0)$。

证明：

$$\forall a, b, c \in \mathbb{R}$$

$$(a \circ b) \circ c = a \circ (b \circ c)$$

$$\iff p(pa + qb + r) + qc + r = pa + q(pb + qc + r) + r \qquad (\circ \text{运算定义})$$

$$\iff p^2a + pqb + pr + qc + r = pa + pqb + q^2c + qr + r \qquad (\text{乘法分配律})$$

$$\iff p^2a + qc + pr = pa + q^2c + qr \qquad (\text{加法消去律})$$

由 a, c 取值的任意性知，上面的等式成立当且仅当 $p^2 = p \wedge q^2 = q \wedge pr = qr$。

又因为 $p^2 = p \wedge q^2 = q$ 成立当且仅当 $p, q \in \{0,1\}$，而 $pr = qr$ 成立当且仅当 $p = q$ 或 $r = 0$，从而得证原题。 □

结论 3：运算满足幂等律当且仅当 $p + q = 1 \wedge r = 0$。

证明：充分性显然。下面证必要性：

若运算满足幂等律，则有：

$$\forall x \in \mathbb{R}$$

$$a \circ x = x$$

$$\iff (p + q)x + r = x \qquad (\circ \text{运算定义})$$

解得：$p + q = 1$ 和 $r = 0$。 □

结论 4a：运算有左单位元当且仅当 $q = 1 \wedge (p \neq 0 \vee r = 0)$。

证明：充分性显然。下面证必要性：

若运算有左单位元 e_l，则：

$$\forall x \in \mathbb{R}$$

$$e_l \circ x = x$$

$$\iff pe_l + qx + r = x \qquad (\circ \text{运算定义})$$

解得：$q = 1, pe_l + r = 0$。

当 $p \neq 0 \vee r = 0$ 时方程 $pe_l + r = 0$ 有解(当 $p = r = 0$ 时，方程有无穷多个解)。 □

结论 4b：运算有右单位元当且仅当 $p = 1 \wedge (q \neq 0 \vee r = 0)$。

证明：与 4a 类似。 □

结论 4c：运算有单位元当且仅当 $p = q = 1$。

证明：充分性：易于验证，当 $p = q = 1$ 时，$-r$ 是单位元。

必要性：综合结论 4a 和 4b 即得。 □

结论 5a：运算有左零元当且仅当 $q = 0 \wedge ((p = 1 \wedge r = 0) \vee p \neq 1)$。

证明：充分性：易于验证，当 $p = 1, q = r = 0$ 时，任何元素都是左零元。当 $q = 0, p =\neq 1$ 时，$r/(1 - p)$ 是左零元。

必要性：

若运算有左零元 θ_l，则：

$$\forall x \in \mathbb{R}$$

$$\theta_l \circ x = \theta_l$$

$\iff p\theta_l + qx + r = \theta_l$ （$\circ$ 运算定义）

解得 $q = 0, p\theta_l + r = \theta_l$。

当 $r = 0$ 时，有 $p = 1$，θ_l 为任意实数。当 $p \neq 1$ 时，有 $\theta_l = r/(1-p)$。

当 $r \neq 0, p = 1$ 时，方程无解。 □

结论 $5b$: 运算有右零元当且仅当 $p = 0 \land ((q = 1 \land r = 0) \lor q \neq 1)$。

证明: 与 $5a$ 类似。 □

结论 $5c$: 运算有零元当且仅当 $p = q = 0$。

证明: 充分性：易见，当 $p = q = 0$ 时，r 是零元。

必要性：由结论 $5a$ 和 $5b$ 即得。 □

15.9 适合交换律、结合律，不适合幂等律。单位元是 0。零元是 1。除 1 以外的有理数 x 都有逆元 $x^{-1} = x/(x-1)$。

15.10

一元运算有 4 个：

x	a	b
$\Delta_1 x$	a	a

x	a	b
$\Delta_2 x$	a	b

x	a	b
$\Delta_3 x$	b	a

x	a	b
$\Delta_4 x$	b	b

二元运算有 16 个：

$\circ_1$	a	b
a	a	a
b	a	a

$\circ_2$	a	b
a	a	a
b	a	b

$\circ_3$	a	b
a	a	a
b	b	a

$\circ_4$	a	b
a	a	a
b	b	b

$\circ_5$	a	b
a	a	b
b	a	a

$\circ_6$	a	b
a	a	b
b	a	b

$\circ_7$	a	b
a	a	b
b	b	a

$\circ_8$	a	b
a	a	b
b	b	b

$\circ_9$	a	b
a	b	a
b	a	a

$\circ_{10}$	a	b
a	b	a
b	a	b

$\circ_{11}$	a	b
a	b	a
b	b	a

$\circ_{12}$	a	b
a	b	a
b	b	b

$\circ_{13}$	a	b
a	b	b
b	a	a

$\circ_{14}$	a	b
a	b	b
b	a	b

$\circ_{15}$	a	b
a	b	b
b	b	a

$\circ_{16}$	a	b
a	b	b
b	b	b

其中 $\circ_3, \circ_5, \circ_{11}, \circ_{12}, \circ_{13}, \circ_{14}$ 是既不可交换也不可结合的。

15.11 不适合交换律。例如，$\langle 1,2\rangle \circ \langle 3,4\rangle = \langle 1*3, 1*4+2\rangle = \langle 3,6\rangle$，而 $\langle 3,4\rangle \circ \langle 1,2\rangle = \langle 3*1, 3*2+4\rangle = \langle 3,10\rangle$，也即 $\langle 1,2\rangle \circ \langle 3,4\rangle \neq \langle 3,4\rangle \circ \langle 1,2\rangle$。

适合结合律。因为 $(\langle a,b\rangle \circ \langle c,d\rangle) \circ \langle e,f\rangle = \langle ac, ad+b\rangle \circ \langle e,f\rangle = \langle ace, acf+ad+b\rangle$，同时，$\langle a,b\rangle \circ (\langle c,d\rangle \circ \langle e,f\rangle) = \langle a,b\rangle \circ \langle ce, cf+d\rangle = \langle ace, acf+ad+b\rangle$，即对任意 $\langle a,b\rangle, \langle c,d\rangle, \langle e,f\rangle \in A$，有 $(\langle a,b\rangle \circ \langle c,d\rangle) \circ \langle e,f\rangle = \langle a,b\rangle \circ (\langle c,d\rangle \circ \langle e,f\rangle)$。

易于验证，$\langle 1,0\rangle$ 是 $\circ$ 运算的单位元，$\langle 0,x\rangle$ 为左零元(其中 $x \in \mathbb{Q}$ 为任意有理数)。$\circ$ 运算无右零元，因为由加法性质知，不存在 d，满足 $\forall a,b \in \mathbb{Q}, ad+b = d$。

对任意 $\langle a,b\rangle \in A$，当 $a \neq 0$ 时，有逆元 $\langle 1/a, -b/a\rangle$ (代入即证)。当 $a = 0$ 时无逆元，因为不存在一个 c，使得 $0c = 1$。

15.12

(1) 注意到，若令 $\varphi: A \to \mathbb{Z}_3, \varphi(a) = 0, \varphi(b) = 1, \varphi(c) = 2$，则 $\langle A, \circ, a\rangle \overset{\varphi}{\cong} \langle \mathbb{Z}_3, \oplus, 0\rangle$，其中 $\oplus$ 是

模 3 加法。从而由模 3 加法的性质知，$\circ$ 满足交换律和结合律，不满足幂等律。a是单位元。无零元。

(2) 由运算表显然有：$x \circ y = y, \forall x, y \in A$。易见，$\circ$ 满足结合律和幂等律，但不满足交换律。A 中每一个元素都是左单位元和右零元。无右单位元和左零元。

(3) 易于验证，若令 $\varphi : A \to \mathbb{Z}_3, \varphi(a) = 1, \varphi(b) = 2, \varphi(c) = 0$，则 $\langle A, \circ, a \rangle \overset{\varphi}{\cong} \langle \mathbb{Z}_3, \otimes, 1 \rangle$，其中 $\otimes$ 是模 3 乘法。从而由模 3 乘法的性质可知，$\circ$ 满足交换律和结合律。$b \circ b = a$，不满足幂等律。a 是单位元。c 是零元。

(4) 考虑代数系统 $\{B, \otimes, 1\}$，其中 $B = \{1, 4, 6\}$，$\otimes$ 是模 10 乘法。易于验证，若令 $\varphi : A \to B, \varphi(a) = 1, \varphi(b) = 6, \varphi(c) = 4$，则 $\langle A, \circ, a \rangle \overset{\varphi}{\cong} \langle B, \otimes, 1 \rangle$。从而由模 10 乘法的性质可知，$\circ$ 满足交换律和结合律。$c \circ c = b$，不满足幂等律。a 是单位元。无零元。

15.13

证明: 由 θ_l 是左零元可知，$\theta_l \circ \theta_r = \theta_l$。又由 θ_r 是右零元可知，$\theta_l \circ \theta_r = \theta_r$。

于是有：$\theta_l = \theta_l \circ \theta_r = \theta_r$。也即，左零元等于右零元。

假设 θ' 也是 $\circ$ 的一个左(右)零元，则由 θ' 是左(右)零元知，$\theta' \circ \theta = \theta'$ (或 $\theta \circ \theta' = \theta'$)，又由 θ 是零元知，$\theta' \circ \theta = \theta \circ \theta' = \theta$。

从而有：$\theta' = \theta' \circ \theta = \theta$ (或 $\theta' = \theta \circ \theta' = \theta$)。

即，若 $\circ$ 同时有左、右零元，则它的左零元等于右零元，是 $\circ$ 唯一的零元。 □

15.14 $V_1 = \langle \mathbb{Z}_6, \oplus \rangle$ 也就是 V 本身，是 V 的平凡子代数。

$V_2 = \langle \{0, 2, 4\}, \oplus \rangle$ 是 V 的真子代数。

$V_3 = \langle \{0, 3\}, \oplus \rangle$ 是 V 的真子代数。

$V_4 = \langle \{0\}, \oplus \rangle$ 是 V 的真子代数。

15.15

(1) 记 $V_1 \times V_2$ 为 $\langle \{\langle 1, 5 \rangle, \langle 1, 6 \rangle, \langle 2, 5 \rangle, \langle 2, 6 \rangle, \langle 3, 5 \rangle, \langle 3, 6 \rangle\}, \triangle, \langle 1, 6 \rangle \rangle$。

$\triangle$ 的运算表如下：

$\triangle$	$\langle 1,5 \rangle$	$\langle 1,6 \rangle$	$\langle 2,5 \rangle$	$\langle 2,6 \rangle$	$\langle 3,5 \rangle$	$\langle 3,6 \rangle$
$\langle 1,5 \rangle$	$\langle 1,5 \rangle$	$\langle 1,5 \rangle$	$\langle 2,5 \rangle$	$\langle 2,5 \rangle$	$\langle 3,5 \rangle$	$\langle 3,5 \rangle$
$\langle 1,6 \rangle$	$\langle 1,5 \rangle$	$\langle 1,6 \rangle$	$\langle 2,5 \rangle$	$\langle 2,6 \rangle$	$\langle 3,5 \rangle$	$\langle 3,6 \rangle$
$\langle 2,5 \rangle$	$\langle 2,5 \rangle$	$\langle 2,5 \rangle$	$\langle 2,5 \rangle$	$\langle 2,5 \rangle$	$\langle 3,5 \rangle$	$\langle 3,5 \rangle$
$\langle 2,6 \rangle$	$\langle 2,5 \rangle$	$\langle 2,6 \rangle$	$\langle 2,5 \rangle$	$\langle 2,6 \rangle$	$\langle 3,5 \rangle$	$\langle 3,6 \rangle$
$\langle 3,5 \rangle$	$\langle 3,5 \rangle$	$\langle 3,5 \rangle$	$\langle 3,5 \rangle$	$\langle 3,5 \rangle$	$\langle 3,5 \rangle$	$\langle 3,5 \rangle$
$\langle 3,6 \rangle$	$\langle 3,5 \rangle$	$\langle 3,6 \rangle$	$\langle 3,5 \rangle$	$\langle 3,6 \rangle$	$\langle 3,5 \rangle$	$\langle 3,6 \rangle$

其中 $\langle 1, 6 \rangle$ 是 $\triangle$ 的单位元。$\langle 3, 5 \rangle$ 是 $\triangle$ 的零元。所有元素都是幂等元。除 $\langle 1, 6 \rangle$ 外，其它元素皆无逆元。

(2) $V_1 = \langle \{1, 2, 3\}, \circ, 1 \rangle$ 就是 V 自身，是 V 的平凡子代数。

$V_2 = \langle \{1, 2\}, \circ, 1 \rangle$ 是 V 的真子代数。

$V_3 = \langle \{1, 3\}, \circ, 1 \rangle$ 是 V 的真子代数。

$V_4 = \langle \{1\}, \circ, 1 \rangle$ 是 V 的平凡真子代数。

15.16

(1) 记 $V_1 \times V_2$ 为 $\langle \mathbb{Z}_3 \times \mathbb{Z}_2, \circ \rangle$。

$\circ$ 的运算表如下：

$\circ$	$\langle 0,0\rangle$	$\langle 0,1\rangle$	$\langle 1,0\rangle$	$\langle 1,1\rangle$	$\langle 2,0\rangle$	$\langle 2,1\rangle$
$\langle 0,0\rangle$	$\langle 0,0\rangle$	$\langle 0,1\rangle$	$\langle 1,0\rangle$	$\langle 1,1\rangle$	$\langle 2,0\rangle$	$\langle 2,1\rangle$
$\langle 0,1\rangle$	$\langle 0,1\rangle$	$\langle 0,0\rangle$	$\langle 1,1\rangle$	$\langle 1,0\rangle$	$\langle 2,1\rangle$	$\langle 2,0\rangle$
$\langle 1,0\rangle$	$\langle 1,0\rangle$	$\langle 1,1\rangle$	$\langle 2,0\rangle$	$\langle 2,1\rangle$	$\langle 0,0\rangle$	$\langle 0,1\rangle$
$\langle 1,1\rangle$	$\langle 1,1\rangle$	$\langle 1,0\rangle$	$\langle 2,1\rangle$	$\langle 2,0\rangle$	$\langle 0,1\rangle$	$\langle 0,0\rangle$
$\langle 2,0\rangle$	$\langle 2,0\rangle$	$\langle 2,1\rangle$	$\langle 0,0\rangle$	$\langle 0,1\rangle$	$\langle 1,0\rangle$	$\langle 1,1\rangle$
$\langle 2,1\rangle$	$\langle 2,1\rangle$	$\langle 2,0\rangle$	$\langle 0,1\rangle$	$\langle 0,0\rangle$	$\langle 1,1\rangle$	$\langle 1,0\rangle$

(2) $V_1 \times V_2$ 的单位元是 $\langle 0,0\rangle$。$\mathbb{Z}_3 \times \mathbb{Z}_2$ 中每一个元素都有逆元。

其中：$\langle 0,0\rangle$ 与 $\langle 0,0\rangle$ 互逆。$\langle 0,1\rangle$ 与 $\langle 0,1\rangle$ 互逆。$\langle 1,0\rangle$ 与 $\langle 2,0\rangle$ 互逆。$\langle 1,1\rangle$ 与 $\langle 2,1\rangle$ 互逆。

15.17 由积代数定义和教材定理 2.1 立即得证。

15.18

证明: 将复数加法运算和乘法运算分别记作 $+_{\mathbb{C}}$ 和 $\cdot_{\mathbb{C}}$。

作 $\varphi : \mathbb{C} \to B, \forall a+bi \in \mathbb{C}, \varphi(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$，显然 φ 是双射。

下面证 φ 是同态映射。

$\forall a+bi, c+di \in \mathbb{C}$，

$$\begin{aligned}
\varphi((a+bi) +_{\mathbb{C}} (c+di)) &= \varphi((a+c)+(b+d)i) && \text{(复数加法定义)} \\
&= \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} && (\varphi\ \text{定义}) \\
&= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & b \end{pmatrix} && \text{(矩阵加法定义)} \\
&= \varphi(a+bi) + \varphi(c+di) && (\varphi\ \text{定义}) \\
\varphi((a+bi) \cdot_{\mathbb{C}} (c+di)) &= \varphi((ac-bd)+(bc+ad)i) && \text{(复数乘法定义)} \\
&= \begin{pmatrix} ac-bd & bc+ad \\ -(bc+ad) & ac-bd \end{pmatrix} && (\varphi\ \text{定义}) \\
&= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & b \end{pmatrix} && \text{(矩阵乘法定义)} \\
&= \varphi(a+bi) \cdot \varphi(c+di) && (\varphi\ \text{定义})
\end{aligned}$$

这就证明了 φ 是 $\langle \mathbb{C}, +_{\mathbb{C}}, \cdot_{\mathbb{C}}\rangle$ 到 $\langle B, +, \cdot\rangle$ 的同态映射，且为双射。

从而有：$\langle \mathbb{C}, +_{\mathbb{C}}, \cdot_{\mathbb{C}}\rangle \overset{\varphi}{\cong} \langle B, +, \cdot\rangle$。 □

15.19

证明: 将积代数 $V_1 \times V_2$ 和 $V_2 \times V_1$ 分别记为 $\langle A \times B, *_1, *_2\rangle$ 和 $\langle B \times A, \bar{*}_1, \bar{*}_2\rangle$。

作 $\varphi : A \times B \to B \times A, \forall \langle x,y\rangle \in A \times B, \varphi(\langle x,y\rangle) = \langle y,x\rangle$。显然 φ 是双射。

下面证 φ 是同态映射。

$\forall \langle x_1,y_1\rangle, \langle x_2,y_2\rangle \in A \times B, \forall i \in 1,2$，

$$\varphi(\langle x_1,y_1\rangle *_i \langle x_2,y_2\rangle) = \varphi(\langle x_1 \circ_i x_2, y_1 \circ_i y_2\rangle) \qquad \text{(积代数定义)}$$

$$\begin{aligned}
&= \langle y_1 \circ_i y_2, x_1 \circ_i x_2 \rangle && (\varphi\text{ 定义}) \\
&= \langle y_1, x_1 \rangle \overline{*}_i \langle y_2, x_2 \rangle && (\text{积代数定义}) \\
&= \varphi(\langle x_1, y_1 \rangle) \overline{*}_i \varphi(\langle x_2, y_2 \rangle) && (\varphi\text{ 定义})
\end{aligned}$$

这就证明了 φ 是 $V_1 \times V_2$ 到 $V_2 \times V_1$ 的同态映射，且为双射。

从而有：$V_1 \times V_2 \overset{\varphi}{\cong} V_2 \times V_1$。 □

15.20 先证一个引理。

引理 15.1 对任意全函数 $f, g : A \to B$，若 $|B| = 2$，则有：$f = g$ 当且仅当 $\exists b_0(b_0 \in B \land \forall x(x \in A \to (f(x) = b_0 \leftrightarrow g(x) = b_0)))$。

证明: 必要性显然。下面证充分性：

反设 $f \neq g$，则存在 $x \in A$，使 $f(x) \neq g(x)$。由 $|B| = 2$ 和 $f(x) \neq g(x)$ 知，$f(x)$ 和 $g(x)$ 中有且仅有一个等于 b_0，这与条件 $\forall x(x \in A \to (f(x) = b_0 \leftrightarrow g(x) = b_0))$ 矛盾。 □

再证原题。

证明: 由命题逻辑矛盾律和排中律知，φ 是全函数(即，对任何 $x \in \mathcal{P}(\{a, b\})$，$a \in x$ 和 $a \notin x$ 有且仅有一个成立)。

由 $\{a\} \in \mathcal{P}(\{a, b\}), \varphi(\{a\}) = 1$ 和 $\{b\} \in \mathcal{P}(\{a, b\}), \varphi(\{b\}) = 0$ 知，φ 是满射。

下面验证 φ 是同态映射。

$\forall x, y \in A$，

$$\begin{aligned}
\varphi(x \cup y) = 1 &\iff a \in x \cup y && (\varphi\text{ 定义}) \\
&\iff a \in x \lor a \in y && (\text{集合并定义}) \\
&\iff \varphi(x) = 1 \lor \varphi(y) = 1 && (\varphi\text{ 定义}) \\
&\iff \varphi(x) + \varphi(y) = 1 && (\text{布尔加定义})
\end{aligned}$$

注意到，可以将 $\varphi(x \cup y)$ 和 $\varphi(x) + \varphi(y)$ 看成两个从 $\mathcal{P}(a, b)$ 到 $\{0, 1\}$ 的函数。再由 $|\{0, 1\}| = 2, 1 \in \{0, 1\}$ 和引理 15.1 可知：$\forall x, y \in A, \varphi(x \cup y) = \varphi(x) + \varphi(y)$。

$\forall x, y \in A$，

$$\begin{aligned}
\varphi(x \cap y) = 1 &\iff a \in x \cap y && (\varphi\text{ 定义}) \\
&\iff a \in x \land a \in y && (\text{集合交定义}) \\
&\iff \varphi(x) = 1 \land \varphi(y) = 1 && (\varphi\text{ 定义}) \\
&\iff \varphi(x) \cdot \varphi(y) = 1 && (\text{布尔乘定义})
\end{aligned}$$

从而有：$\forall x, y \in A, \varphi(x \cap y) = \varphi(x) \cdot \varphi(y)$。

$\forall x \in A$，

$$\begin{aligned}
\varphi({\sim}x) = 1 &\iff a \in {\sim}x && (\varphi\text{ 定义}) \\
&\iff a \notin x && (\text{绝对补定义}) \\
&\iff \varphi(x) = 0 && (\varphi\text{ 定义}) \\
&\iff -\varphi(x) = 1 && (\text{布尔补定义})
\end{aligned}$$

从而有：$\forall x \in A, \varphi({\sim}x) = -\varphi(x)$。

由于 $a \notin \varnothing, a \in \{a, b\}$，从而有 $\varphi(\varnothing) = 0, \varphi(\{a, b\}) = 1$。

这就证明了 φ 是 V_1 到 V_2 的同态映射。再由 φ 是满射知，φ 是 V_1 到 V_2 的满同态。 □

15.21

(1)

证明: ① 若 $\circ_i$ 是可交换的，则：任取 $x, y \in B$，因 φ 是满射，所以存在 $a, b \in A$，使 $\varphi(a) = x, \varphi(b) = y$。从而有：

$$\begin{aligned}
x\overline{\circ}_i y &= \varphi(a)\overline{\circ}_i\varphi(b) && (\varphi(a) = x, \varphi(b) = y) \\
&= \varphi(a \circ_i b) && (\varphi \text{ 是同态映射}) \\
&= \varphi(b \circ_i a) && (\circ_i \text{ 是可交换的}) \\
&= \varphi(b)\overline{\circ}_i\varphi(a) && (\varphi \text{ 是同态映射}) \\
&= y\overline{\circ}_i x && (\varphi(a) = x, \varphi(b) = y)
\end{aligned}$$

因此 $\overline{\circ}_i$ 也是可交换的。

② 若 $\circ_i$ 是可结合的，则：任取 $x, y, z \in B$，因 φ 是满射，所以存在 $a, b, c \in A$，使 $\varphi(a) = x, \varphi(b) = y, \varphi(c) = z$。从而有：

$$\begin{aligned}
(x\overline{\circ}_i y)\overline{\circ}_i z &= (\varphi(a)\overline{\circ}_i\varphi(b))\overline{\circ}_i\varphi(c) && (\varphi(a) = x, \varphi(b) = y, \varphi(c) = z) \\
&= (\varphi(a \circ_i b))\overline{\circ}_i\varphi(c) && (\varphi \text{ 是同态映射}) \\
&= \varphi((a \circ_i b) \circ_i c) && (\varphi \text{ 是同态映射}) \\
&= \varphi(a \circ_i (b \circ_i c)) && (\circ_i \text{ 是可结合的}) \\
&= \varphi(a)\overline{\circ}_i\varphi(b \circ_i c) && (\varphi \text{ 是同态映射}) \\
&= \varphi(a)\overline{\circ}_i(\varphi(b)\overline{\circ}_i\varphi(c)) && (\varphi \text{ 是同态映射}) \\
&= x\overline{\circ}_i(y\overline{\circ}_i z) && (\varphi(a) = x, \varphi(b) = y, \varphi(c) = z)
\end{aligned}$$

因此 $\overline{\circ}_i$ 也是可结合的。

③ 若 $\circ_i$ 是幂等的，则：任取 $x \in B$，因 φ 是满射，所以存在 $a \in A$，使 $\varphi(a) = x$。从而有：

$$\begin{aligned}
x\overline{\circ}_i x &= \varphi(a)\overline{\circ}_i\varphi(a) && (\varphi(a) = x) \\
&= \varphi(a \circ_i a) && (\varphi \text{ 是同态映射}) \\
&= \varphi(a) && (\circ_i \text{ 是幂等的}) \\
&= x && (\varphi(a) = x)
\end{aligned}$$

因此 $\overline{\circ}_i$ 也是幂等的。 □

(2)

证明: 若 $\circ_i$ 对 $\circ_j$ 是可分配的，则：任取 $x, y, z \in B$，因 φ 是满射，所以存在 $a, b, c \in A$，使 $\varphi(a) = x, \varphi(b) = y, \varphi(c) = z$。从而有：

$$\begin{aligned}
x\overline{\circ}_i(y\overline{\circ}_j z) &= \varphi(a)\overline{\circ}_i(\varphi(b)\overline{\circ}_j\varphi(c)) && (\varphi(a) = x, \varphi(b) = y, \varphi(c) = z) \\
&= \varphi(a)\overline{\circ}_i\varphi(b \circ_j c) && (\varphi \text{ 是同态映射}) \\
&= \varphi(a \circ_i (b \circ_j c)) && (\varphi \text{ 是同态映射}) \\
&= \varphi((a \circ_i b) \circ_j (a \circ_i c)) && (\circ_i \text{ 对 } \circ_j \text{ 是可分配的}) \\
&= \varphi(a \circ_i b)\overline{\circ}_j\varphi(a \circ_i c) && (\varphi \text{ 是同态映射}) \\
&= (\varphi(a)\overline{\circ}_i\varphi(b))\overline{\circ}_j(\varphi(a) \circ_i \varphi(c)) && (\varphi \text{ 是同态映射}) \\
&= (x\overline{\circ}_i y)\overline{\circ}_j(x\overline{\circ}_i z) && (\varphi(a) = x, \varphi(b) = y, \varphi(c) = z)
\end{aligned}$$

同理可证 $(y\overline{\circ}_j z)\overline{\circ}_i x = (y\overline{\circ}_i x)\overline{\circ}_j(z\overline{\circ}_i x)$。

从而 $\overline{\circ}_i$ 对 $\overline{\circ}_j$ 也是可分配的。 □

(3)

证明: 若 $\circ_i, \circ_j$ 是可吸收的，则：由吸收律定义知， $\circ_i$ 和 $\circ_j$ 满足交换律，从而由第 (1) 小题

结论知，$\bar{\circ}_i$ 和 $\bar{\circ}_j$ 也满足交换律。同是，任取 $x, y \in B$，因 φ 是满射，所以存在 $a, b \in A$，使 $\varphi(a) = x, \varphi(b) = y$。从而有：

$$\begin{aligned}
x\bar{\circ}_i(x\bar{\circ}_j y) &= \varphi(a)\bar{\circ}_i(\varphi(a)\bar{\circ}_j\varphi(b)) && (\varphi(a) = x, \varphi(b) = y)\\
&= \varphi(a)\bar{\circ}_i\varphi(a \circ_j b) && (\varphi \text{ 是同态映射})\\
&= \varphi(a \circ_i (a \circ_j b)) && (\varphi \text{ 是同态映射})\\
&= \varphi(a) && (\circ_i, \circ_j \text{ 是可吸收的})\\
&= x && (\varphi(a) = x)
\end{aligned}$$

同理可证 $x\bar{\circ}_j(x\bar{\circ}_i y) = x$。

从而 $\bar{\circ}_i, \bar{\circ}_j$ 也是可吸收的。 □

(4)

证明： ① 若 e 是 V_1 中关于 $\circ_i$ 是单位元，则：任取 $x \in B$，因 φ 是满射，所以存在 $a \in A$，使 $\varphi(a) = x$。从而有：

$$\begin{aligned}
x\bar{\circ}_i\varphi(e) &= \varphi(a)\bar{\circ}_i\varphi(e) && (\varphi(a) = x)\\
&= \varphi(a \circ_i e) && (\varphi \text{ 是同态映射})\\
&= \varphi(a) && (e \text{ 是关于 } \circ_i \text{ 是单位元})\\
&= x && (\varphi(a) = x)
\end{aligned}$$

同理可证 $\varphi(e)\bar{\circ}_i x = x$。

从而 $\varphi(e)$ 是的 V_2 中关于 $\bar{\circ}_i$ 单位元。

② 若 θ 是 V_1 中关于 $\circ_i$ 是零元，则：任取 $x \in B$，因 φ 是满射，所以存在 $a \in A$，使 $\varphi(a) = x$。从而有：

$$\begin{aligned}
x\bar{\circ}_i\varphi(\theta) &= \varphi(a)\bar{\circ}_i\varphi(\theta) && (\varphi(a) = x)\\
&= \varphi(a \circ_i \theta) && (\varphi \text{ 是同态映射})\\
&= \varphi(\theta) && (\theta \text{ 是关于 } \circ_i \text{ 是零元})
\end{aligned}$$

同理可证 $\varphi(\theta)\bar{\circ}_i x = \theta$。

从而 $\varphi(\theta)$ 是的 V_2 中关于 $\bar{\circ}_i$ 零元。 □

(5)

证明： 设 x^{-1} 是 x 关于 $\circ_i$ 的逆元，则：

$$\begin{aligned}
\varphi(x)\bar{\circ}_i\varphi(x^{-1}) &= \varphi(x \circ_i x^{-1}) && (\varphi \text{ 是同态映射})\\
&= \varphi(e) && (x^{-1} \text{ 是 } x \text{ 的逆元})
\end{aligned}$$

由第 (4) 小题结论知，$\varphi(e)$ 是 V_2 中关于 $\bar{\circ}_i$ 单位元。从而知 $\varphi(x^{-1})$ 是 $\varphi(x)$ 关于 $\bar{\circ}_i$ 的右逆元。同理可证 $\varphi(x^{-1})$ 也是 $\varphi(x)$ 关于 $\bar{\circ}_i$ 的左逆元。因此，$\varphi(x^{-1})$ 是 $\varphi(x)$ 关于 $\bar{\circ}_i$ 的逆元。 □

15.22

证明： 由教材定理 3.3 知，$\varphi_2 \circ \varphi_1 : A \to C$ 且 $\forall x \in A, \varphi_2 \circ \varphi_1(x) = \varphi_2(\varphi_1(x))$。

因此，$\forall x, y \in A$，

$$\begin{aligned}
\varphi_2 \circ \varphi_1(x \circ y) &= \varphi_2(\varphi_1(x \circ y)) && (\text{教材定理 } 3.3)\\
&= \varphi_2(\varphi_1(x) * \varphi_1(y)) && (\varphi_1 \text{ 是 } V_1 \text{ 到 } V_2 \text{ 的同态})\\
&= \varphi_2(\varphi_1(x)) \cdot \varphi_2(\varphi_1(y)) && (\varphi_2 \text{ 是 } V_2 \text{ 到 } V_3 \text{ 的同态})\\
&= \varphi_2 \circ \varphi_1(x) \cdot \varphi_2 \circ \varphi_1(y) && (\text{教材定理 } 3.3)
\end{aligned}$$

从而 $\varphi_2 \circ \varphi_1$ 是 V_1 到 V_3 的同态。 □

15.23

(1)

证明： 记 V_1 的载体为 A，则 I_A 显然是 V_1 到 V_1 的同态且为双射，所以有 $V_1 \cong V_1$。 □

(2)

证明： 记 $V_1 = \langle A, \circ_1, \circ_2, \ldots, \circ_k \rangle, V_2 = \langle B, \bar{\circ}_1, \bar{\circ}_2, \ldots, \bar{\circ}_k \rangle$。

由同构定义知，存在双射 $\varphi : A \to B$，使得对所有的运算 $\circ_i, \bar{\circ}_i$ 都有：

$$\varphi(\circ_i(x_1, x_2, \ldots, x_{k_i})) = \bar{\circ}_i(\varphi(x_1), \varphi(x_2), \ldots, \varphi(x_{k_i})), \quad \forall x_1, x_2, \ldots, x_{k_i} \in A$$

从而由教材定理 3.9 知 $\varphi^{-1} : B \to A$ 也是双射的，且对所有的运算 $\circ_i, \bar{\circ}_i$ 都有：

$$\begin{aligned}
&\forall y_1, y_2, \ldots, y_{k_i} \in B, \\
&\varphi^{-1}(\bar{\circ}_i(y_1, y_2, \ldots, y_{k_i})) \\
=&\varphi^{-1}(\bar{\circ}_i(\varphi(\varphi^{-1}(y_1)), \varphi(\varphi^{-1}(y_2)), \ldots, \varphi(\varphi^{-1}(y_{k_i})))) && (\varphi \circ \varphi^{-1} = I_B) \\
=&\varphi^{-1}(\varphi(\circ_i(\varphi^{-1}(y_1), \varphi^{-1}(y_2), \ldots, \varphi^{-1}(y_{k_i})))) && (\varphi \text{ 是 } V_1 \text{ 到 } V_2 \text{ 的同态}) \\
=&\circ_i (\varphi^{-1}(y_1), \varphi^{-1}(y_2), \ldots, \varphi^{-1}(y_{k_i})) && (\varphi^{-1} \circ \varphi = I_A)
\end{aligned}$$

从而证明了 φ^{-1} 是 V_2 到 V_1 同态。又由于 φ^{-1} 是双射，所以就有 $V_2 \cong V_1$。 □

(3)

证明： 记 $V_1 = \langle A, \circ_1, \circ_2, \ldots, \circ_k \rangle, V_2 = \langle B, \bar{\circ}_1, \bar{\circ}_2, \ldots, \bar{\circ}_k \rangle, V_3 = \langle C, \circ'_1, \circ'_2, \ldots, \circ'_k \rangle$。

由同构定义知，存在双射 $\varphi_1 : A \to B$ 和 $\varphi_2 : B \to C$，使得对所有的运算 $\circ_i, \bar{\circ}_i, \circ'_i$ 都有：

$$\varphi(\circ_i(x_1, x_2, \ldots, x_{k_i})) = \bar{\circ}_i(\varphi(x_1), \varphi(x_2), \ldots, \varphi(x_{k_i}), \quad \forall x_1, x_2, \ldots, x_{k_i}) \in A$$

$$\bar{\circ}_i(\varphi(y_1), \varphi(y_2), \ldots, \varphi(y_{k_i}) = \varphi(\circ'_i(y_1, y_2, \ldots, y_{k_i})), \quad \forall y_1, y_2, \ldots, y_{k_i}) \in B$$

从而由教材定理 3.4(3) 知，$\varphi_2 \circ \varphi_1 : A \to C$ 也是双射的，且对所有的运算 $\circ_i, \bar{\circ}_i, \circ'_i$ 都有：

$$\begin{aligned}
&\forall x_1, x_2, \ldots, x_{k_i} \in A, \\
&\varphi_2 \circ \varphi_1(\circ_i(x_1, x_2, \ldots, x_{k_i})) \\
=&\varphi_2(\varphi_1(\circ_i(x_1, x_2, \ldots, x_{k_i}))) && (\text{教材定理 } 3.3) \\
=&\varphi_2(\bar{\circ}_i(\varphi_1(x_1), \varphi_1(x_2), \ldots, \varphi_1(x_{k_i}))) && (\varphi_1 \text{ 是 } V_1 \text{ 到 } V_2 \text{ 的同态}) \\
=&\circ'_i (\varphi_2(\varphi_1(x_1)), \varphi_2(\varphi_1(x_2)), \ldots, \varphi_2(\varphi_1(x_{k_i}))) && (\varphi_2 \text{ 是 } V_2 \text{ 到 } V_3 \text{ 的同态}) \\
=&\circ'_i (\varphi_2 \circ \varphi_1(x_1), \varphi_2 \circ \varphi_1(x_2), \ldots, \varphi_2 \circ \varphi_1(x_{k_i})) && (\text{教材定理 } 3.3)
\end{aligned}$$

从而证明了 $\varphi_2 \circ \varphi_1$ 是 V_1 到 V_3 同态。又由于 $\varphi_2 \circ \varphi_1$ 是双射，所以就有 $V_1 \cong V_3$。 □

15.24

(1) 不是同态。

证明： 由于 $1 \in \mathbb{C}$，但 $\varphi(1 \cdot 1) = \varphi(1) = |1| + 1 = 2$，而 $\varphi(1) \cdot \varphi(1) = 2 \cdot 2 = 4$，从而 $\varphi(1 \cdot 1) \neq \varphi(1) \cdot \varphi(1)$。这就证明了 φ 不是同态。 □

(2) 是同态，同态像是 $\langle \mathbb{R} - \mathbb{R}^-, \cdot \rangle$。

证明： $\forall a_1 e^{i\theta_1}, a_2 e^{i\theta_2} \in \mathbb{C}$，

$$\begin{aligned}
\varphi(a_1 e^{i\theta_1} \cdot a_2 e^{i\theta_2}) &= \varphi(a_1 a_2 e^{i(\theta_1 + \theta_2)}) && (\text{复数乘法定义}) \\
&= |a_1 a_2 e^{i(\theta_1 + \theta_2)}| && (\varphi \text{ 定义}) \\
&= a_1 a_2 && (\text{模运算定义}) \\
&= |a_1 e^{i\theta_1}| \cdot |a_2 e^{i\theta_2}| && (\text{模运算定义}) \\
&= \varphi(a_1 e^{i\theta_1}) \cdot \varphi(a_2 e^{i\theta_2}) e && (\varphi \text{ 定义})
\end{aligned}$$

□

(3) 是同态，同态像是 $\langle\{0\},\cdot\rangle$。

证明： $\forall x, y \in \mathbb{C}$，

$$\begin{aligned}
\varphi(x\cdot y) &= 0 && (\varphi \text{ 定义})\\
&= 0\cdot 0 && (0\cdot 0 = 0)\\
&= \varphi(x)\cdot\varphi(y) && (\varphi \text{ 定义})
\end{aligned}$$

□

(4) 不是同态。

证明： 由于 $1\in\mathbb{C}$，但 $\varphi(1\cdot 1) = \varphi(1) = 2$，而 $\varphi(1)\cdot\varphi(1) = 2\cdot 2 = 4$，从而 $\varphi(1\cdot 1)\neq\varphi(1)\cdot\varphi(1)$。这就证明了 φ 不是同态。 □

15.25 显然 I_A 是 V 的一个自同构。下面证明，V 上不存在其它的自同构。

证明： 设 $\varphi : A\to A$ 是 V 的一个自同态且 $\varphi(5^1) = \varphi(5^k)$。则 $\varphi(5^2) = \varphi(5^1\cdot 5^1) = 5^k\cdot 5^k = 5^{2k}$。对 n 施归纳可证，$\forall n\in\mathbb{Z}^+, \varphi(5^n) = \varphi(5^{kn})$。此时 V 在 φ 下的同态像是 $\langle\{5^{kn} \mid n\in\mathbb{Z}^+\},\cdot\rangle$。若 $k\notin\mathbb{Z}^+$，则 $\varphi(A)\nsubseteq A$，与 $\varphi : A\to A$ 矛盾。若 $k = 1$，则 $\varphi = I_A$，是恒等函数。若 $k > 1$，则 $5^1\notin\{5^{kn}\mid n\in\mathbb{Z}^+\}$，从而 φ 不是满射，也就不是同构。

这就证明了 I_A 是 V 上唯一的自同构。 □

15.26

证明： 显然，φ 是函数，且为满射。下面证明 φ 是同态。

$\forall x, y\in\mathbb{Z}^+, \varphi(x\cdot y)$，

$$\begin{aligned}
\varphi(x\cdot y) = 1 &\iff x\cdot y = 1 && (\varphi \text{ 定义})\\
&\iff x = 1\wedge y = 1 && (\text{非负整数性质})\\
&\iff \varphi(x) = 1\wedge\varphi(y) = 1 && (\varphi \text{ 定义})\\
&\iff \varphi(x)\cdot\varphi(y) = 1 && (\text{非负整数性质})
\end{aligned}$$

从而由 $1\in\mathbb{Z}_2, \forall x, y\in\mathbb{Z}^+(\varphi(x\cdot y) = 1\Leftrightarrow\varphi(x)\cdot\varphi(y) = 1)$ 和引理 15.1 有：$\forall x, y\in\mathbb{Z}^+(\varphi(x\cdot y) = \varphi(x)\cdot\varphi(y))$。

这就证明了 φ 是 V_1 到 V_2 的满同态。 □

15.27

(1) 不是。例如 $(-1)R(-3)\wedge 2R2$，但 $(-1+2)\not R(-3+2)$。

(2) 不是。因为 R 不具有传递性(例如 $1R5$，$5R9$，但 $1\not R9$)，所以不是等价关系。

(3) 不是。例如 $(-1)R1\wedge 1R1$，但 $(-1+1)\not R(1+1)$。

(4) 不是。因为 R 不是等价关系。

15.28

证明： 由教材定理 15.11 知，自然映射 $g : A\to A/\!\sim, g(a) = [a], \forall a\in A$ 是从 V 到 $V/\!\sim$ 上的同态映射。又由等价类的定义知，g 是满射。从而 g 是 V 到 $V/\!\sim$ 的满同态。再利用教材定理 15.8 即证原题。 □

15.29

(1)

证明: φ 显然是函数。

由同余运算性质知，$\forall x, y \in \mathbb{Z}, (x+y) \bmod 2 = ((x \bmod 2) + (y \bmod 2)) \bmod 2$。从而有：

$\forall x \in \mathbb{Z}$，

$$\begin{aligned}
\varphi(\triangle x) &= \varphi(x+1) && (\triangle\ \text{定义}) \\
&= (x+1) \bmod 2 && (\varphi\ \text{定义}) \\
&= ((x \bmod 2) + (1 \bmod 2)) \bmod 2 && (\text{同余运算性质}) \\
&= ((x \bmod 2) + 1) \bmod 2 && (1 \bmod 2 = 1) \\
&= (\varphi(x) + 1) \bmod 2 && (\varphi\ \text{定义}) \\
&= \overline{\triangle}\varphi(x) && (\overline{\triangle}\ \text{定义})
\end{aligned}$$

这就证明了 φ 是 V_1 到 V_2 的同态。 □

(2) $\{\{2k \mid k \in \mathbb{Z}\}, \{2k+1 \mid k \in \mathbb{Z}\}\}$。

15.30

(1)

证明: φ 显然是单值的。$\forall x \in A_k$，由 A_k 定义知，$x \geq k$，由题设 $nk \geq m$，从而有 $nx \geq nk \geq m$。这就证明了 φ 确实是 A_k 到 A_m 的函数。

$\forall x, y \in A_k$，

$$\begin{aligned}
\varphi(x+y) &= n(x+y) && (\varphi\ \text{定义}) \\
&= nx + ny && (\text{乘法分配律}) \\
&= \varphi(x) + \varphi(y) && (\varphi\ \text{定义})
\end{aligned}$$

这就证明了 φ 是 V_1 到 V_2 的同态。 □

(2) 分两种情况讨论：

① $n \neq 0$。注意到，由乘法消去律知，此时的 φ 是单射。从而 $\forall x, y \in A_k, \varphi(x) = \varphi(y) \Rightarrow x = y$。因此，$\sim = I_{A_k}$，$A_k/\!\sim = \{\{x\} \mid x \in A_k\}$。于是有：$V_1/\!\sim = \langle\{\{x\} \mid x \in A_k\}, \odot\rangle$，其中 $\odot$ 的定义为：$\{x\} \odot \{y\} = \{x+y\}, \forall x, y \in A_k$。

② $n = 0$。此时，$\varphi(x) = 0, \forall x \in A_k$。从而有 $\sim = E_{A_k}$，$A_k/\!\sim = \{A_k\}$。这时就有 $V_1/\!\sim = \langle\{A_k\}, \odot\rangle$，由于载体 $\{A_k\}$ 只有一个元素，$\odot$ 的运算表只能是：$A_k \odot A_k = A_k$。

15.31

(1) 共有 13 个自同态。

证明: 注意到，b 是幂等元，因此对 V 的任意自同态 φ，都有：

$$\begin{aligned}
\varphi(b) \circ \varphi(b) &= \varphi(b \circ b) && (\varphi\ \text{是同态}) \\
&= \varphi(b) && (b \circ b = b)
\end{aligned}$$

从而 $\varphi(b)$ 也是幂等元。而 A 中唯一的幂等元只有 b，所以对 V 的任何自同态 φ，必有 $\varphi(b) = b$。

同时，又有：

$$\begin{aligned}
\varphi(a) \circ b &= \varphi(a) \circ \varphi(b) && (\varphi(b) = b) \\
&= \varphi(a \circ b) && (\varphi\ \text{是同态}) \\
&= \varphi(a) && (a \circ b = a)
\end{aligned}$$

从而 $\varphi(a) \circ b = \varphi(a)$。而 A 中满足这一条件的元素只有 a 和 b。因而 $\varphi(a)$ 只能是 a 或 b。

下面分 $\varphi(a) = a$ 和 $\varphi(a) = b$ 两种情况讨论。

① 当 $\varphi(a)=a$ 时，由于：

$$\begin{aligned}\varphi(c)\circ b &= \varphi(c)\circ\varphi(b) && (\varphi(b)=b)\\ &= \varphi(c\circ b) && (\varphi\text{ 是同态})\\ &= \varphi(b) && (c\circ b=b)\\ &= b && (\varphi(b)=b)\end{aligned}$$

从而 $\varphi(c)$ 不能等于 a (因为 $a\circ b=a\neq b$)。同样，由于：

$$\begin{aligned}a\circ\varphi(c) &= \varphi(a)\circ c && (\varphi(a)=a)\\ &= \varphi(a\circ c) && (\varphi\text{ 是同态})\\ &= \varphi(b) && (a\circ c=b)\\ &= b && (\varphi(b)=b)\end{aligned}$$

所以 $\varphi(c)$ 不能等于 b (因为 $a\circ b=a\neq b$)。

对于 $\varphi(d)$ 进行类似的讨论也可证明 $\varphi(d)$ 不能等于 a 或 b。

而由于 c 和 d 的运算表完全一致，又不属于 $\circ$ 运算的值域，因此对它们进行任何形式的置换都不影响结果。如此，我们就得到了 4 个满足 $\varphi(a)=a,\varphi(b)=b$ 的自同态：

$\varphi_1(a)=a,\varphi_1(b)=b,\varphi_1(c)=c,\varphi_1(d)=d$；

$\varphi_2(a)=a,\varphi_2(b)=b,\varphi_2(c)=d,\varphi_2(d)=c$；

$\varphi_3(a)=a,\varphi_3(b)=b,\varphi_3(c)=c,\varphi_3(d)=c$；

$\varphi_4(a)=a,\varphi_4(b)=b,\varphi_4(c)=d,\varphi_4(d)=d$；

② 当 $\varphi(a)=b$ 时，上面关于 $\varphi(c)$ 和 $\varphi(d)$ 不能等于 a 的论证依然成立，但关于 $\varphi(c)$ 和 $\varphi(d)$ 不能等于 b 的论证不再成立。这是因为 $\varphi(a)=b$，从而 $\varphi(a\circ c)=\varphi(a)\circ\varphi(c)=b\circ\varphi(c)$，即使 $\varphi(c)=b$ 也不会破坏 φ 同态的性质。

下面说明，只要 $\varphi(a)=\varphi(b)=b$，且 $\varphi(c)$ 和 $\varphi(d)$ 都不等于 a，则 φ 必是同态。

因为 $\varphi(a)=\varphi(b)=b$ 且 $\varphi(c)$ 和 $\varphi(d)$ 都不等于 a，从而 $a\notin\operatorname{ran}(\varphi)$。这样，唯一一组使 $\circ$ 运算结果不为 b 的运算数 a,b 就不会出现同态像中。从而得到：$\forall x,y\in A,\varphi(x)\circ\varphi(y)=b$。而由于 $\varphi(a)=\varphi(b)=b$，从而：

$\forall x,y\in A$，

$$\begin{aligned}\varphi(x\circ y) &= \begin{cases}\varphi(a), & \text{若 } x=a\wedge y=b\\ \varphi(b), & \text{其它}\end{cases} && (\circ\text{ 定义})\\ &= b && (\varphi(a)=\varphi(b)=b)\end{aligned}$$

这就证明了 $\forall x,y\in A,\varphi(x\circ y)=\varphi(x)\circ\varphi(y)$，从而说明 φ 是同态。

如此，我们就得到了 9 个满足 $\varphi(a)=\varphi(b)=b$ 的自同态：

$\varphi_5(a)=b,\varphi_5(b)=b,\varphi_5(c)=b,\varphi_5(d)=b$；

$\varphi_6(a)=b,\varphi_6(b)=b,\varphi_6(c)=b,\varphi_6(d)=c$；

$\varphi_7(a)=b,\varphi_7(b)=b,\varphi_7(c)=b,\varphi_7(d)=d$；

$\varphi_8(a)=b,\varphi_8(b)=b,\varphi_8(c)=c,\varphi_8(d)=b$；

$\varphi_9(a)=b,\varphi_9(b)=b,\varphi_9(c)=c,\varphi_9(d)=c$；

$\varphi_{10}(a)=b,\varphi_{10}(b)=b,\varphi_{10}(c)=c,\varphi_{10}(d)=d$；

$\varphi_{11}(a)=b,\varphi_{11}(b)=b,\varphi_{11}(c)=d,\varphi_{11}(d)=b$；

$\varphi_{12}(a)=b,\varphi_{12}(b)=b,\varphi_{12}(c)=d,\varphi_{12}(d)=c$；

$\varphi_{13}(a)=b,\varphi_{13}(b)=b,\varphi_{13}(c)=d,\varphi_{13}(d)=d$；

从前面的论证中可知，这些便是 V 上所有的自同态。 □

(2) 根据教材定理 15.10 我们知道，对 V 上的任何同态导出的等价关系都是 V 的同余关系。容易证明：

引理 15.2 对任意代数系统 $V = \langle A, \circ_1, \circ_2, \cdots, \circ_n \rangle$，$V$ 上的每一个同余关系都可以由 V 的某个自同态导出。

证明： 设 $\sim$ 是 V 上的一个同余关系，作自然映射 $g : A \to A/{\sim}, \forall x \in A, g(x) = [x]$。由教材定理 15.11 可知，$g$ 是从 V 到 $V/{\sim}$ 的同态。同时，根据选择公理，存在函数 $f : A/{\sim} \to A$，使得 $\forall x \in A/{\sim}, f(x) \in x$。由商代数的定义立即有：$f$ 是 $V/{\sim}$ 到 V 的同态。从而由同态关系的传递性(证明见习题 5.23)知：$f \circ g : A \to A$ 是 V 的一个自同态。再由 f 和 g 的定义知，$\sim$ 正是 $f \circ g$ 导出的等价关系。如此就证明了：V 上的每一个同余关系都可以由 V 的某个自同态导出。 □

利用这个引理，我们知道，要找出 V 上的所有同余关系，只需逐一检查前面找到的 13 个自同态即可。

记 $\sim_i$ 为 φ_i 在 A 上导出的等价关系，则：

① $\sim_1 = \sim_2 = I_A$，是 A 上的恒等关系。

② $\sim_3 = \sim_4 = \{\langle c, d\rangle, \langle d, c\rangle\} \cup I_A$，对应于划分 $\{\{a\}, \{b\}, \{c, d\}\}$。

③ $\sim_5 = E_A$，是 A 上的全域关系。

④ $\sim_6 = \sim_7 = \{\langle a, b\rangle, \langle a, c\rangle, \langle b, a\rangle, \langle b, c\rangle, \langle c, a\rangle, \langle c, b\rangle\} \cup I_A$，对应于划分 $\{\{a, b, c\}, \{d\}\}$。

⑤ $\sim_8 = \sim_{11} = \{\langle a, b\rangle, \langle a, d\rangle, \langle b, a\rangle, \langle b, d\rangle, \langle d, a\rangle, \langle d, b\rangle\} \cup I_A$，对应于划分 $\{\{a, b, d\}, \{c\}\}$。

⑥ $\sim_9 = \sim_{13} = \{\langle a, b\rangle, \langle b, a\rangle, \langle c, d\rangle, \langle d, c\rangle\} \cup I_A$，对应于划分 $\{\{a, b\}, \{c, d\}\}$。

⑦ $\sim_{10} = \sim_{12} = \{\langle a, b\rangle, \langle b, a\rangle\} \cup I_A$，对应于划分 $\{\{a, b\}, \{c\}, \{d\}\}$。

从而得知，V 上共有 7 个同余关系。

15.32

证明： 记 $V_1 \times V_2 = \langle A \times B, \otimes, \Delta', \langle k, \overline{k}\rangle\rangle$。

作 $\varphi : A \times B \to A, \forall \langle a, b\rangle \in A \times B, \varphi(\langle a, b\rangle) = a$。由定义显然有，$R$ 是 φ 导出的 A 上的等价关系。下面只要证明 φ 是同态映射，就可以分别由教材定理 15.10 和同态基本定理得证：R 是 $V_1 \times V_2$ 上的同余关系和 $V_1 \times V_2 \big/ R \cong V_1$。

φ 显然是函数。

$\forall \langle a, b\rangle, \langle c, d\rangle \in A \times B$，

$$\begin{aligned}
\varphi(\langle a, b\rangle \otimes \langle c, d\rangle) &= \varphi(\langle a * c, b \circ d\rangle) && \text{(积代数定义)}\\
&= a * c && (\varphi\ \text{定义})\\
&= \varphi(\langle a, b\rangle) * \varphi(\langle c, d\rangle) && (\varphi\ \text{定义})\\
\varphi(\Delta'\langle a, b\rangle) &= \varphi(\langle \Delta a, \overline{\Delta} b\rangle) && \text{(积代数定义)}\\
&= \Delta a && (\varphi\ \text{定义})
\end{aligned}$$

这就证明了 φ 是 $V_1 \times V_2$ 到 V_1 的同态。

从而由 R 是 φ 在 A 上导出的等价关系和教材定理 15.10 得到：R 是 $V_1 \times V_2$ 上的同余关系。

又由于 B 是非空的(由代数系统定义，代数系统的载体是非空集合)，因而对任意 $a \in A$，都有 $b \in B$，使得 $\langle a, b\rangle \in A \times B, \varphi(\langle a, b\rangle) = a$。这就证明了 $\varphi(A \times B) = A$，从而 V_1 就是 $V_1 \times V_2$ 在 φ 下的同态像。由同态基本定理知，$V_1 \times V_2 \big/ R \cong V_1$。 □

第十六章　半群与独异点

16.1

(1)

证明：由普通加法和乘法的性质知，$\circ$ 对 $\mathbb{R}$ 是封闭的。

$\forall a, b, c \in \mathbb{R}$，

$$\begin{aligned}(a \circ b) \circ c &= (a+b+ab) \circ c && (\circ \text{ 定义})\\ &= (a+b+ab)+c+(a+b+ab)c && (\circ \text{ 定义})\\ &= a+b+c+ab+ac+bc+abc && (\text{加法交换律、结合律、乘法分配律})\\ &= a+(b+c+bc)+a(b+c+bc) && (\text{加法交换律、结合律、乘法分配律})\\ &= a \circ (b+c+bc) && (\circ \text{ 定义})\\ &= a \circ (b \circ c) && (\circ \text{ 定义})\end{aligned}$$

这就证明了 $\langle \mathbb{R}, \circ \rangle$ 是半群。 □

(2)

证明：由第 (1) 小题已知 $\langle \mathbb{R}, \circ \rangle$ 是半群。而：

$\forall a \in \mathbb{R}$，

$$\begin{aligned}a \circ 0 &= a+0+a \cdot 0 && (\circ \text{ 定义})\\ &= a+0+0 && (0 \text{ 是乘法零元})\\ &= a && (0 \text{ 是加法单位元})\\ 0 \circ a &= 0+a+0 \cdot a && (\circ \text{ 定义})\\ &= 0+a+0 && (0 \text{ 是乘法零元})\\ &= a && (0 \text{ 是加法单位元})\end{aligned}$$

这就证明了 0 是 $\circ$ 运算的单位元。从而证明了 $\langle \mathbb{R}, \circ \rangle$ 是独异点。 □

16.2

证明：首先取 $x = a$。由题设，存在 $u_0, v_0 \in S$，满足：$a * u_0 = v_0 * a = a$。

下面证明 v_0 是关于 $*$ 运算的左单位元：

由题设，$\forall x \in S$，有 $u, v \in S$，使得 $a * u = v * a = x$。从而：

$$\begin{aligned}v_0 * x &= v_0 * a * u && (a * u = x)\\ &= a * u && (v_0 * a = a)\\ &= x && (a * u = x)\end{aligned}$$

这就证明了 v_0 是关于 $*$ 运算的左单位元。同理可证 u_0 是关于 $*$ 运算的右单位元。从而由教材定理 15.2 知，$u_0 = v_0 = e$ 是单位元。

这就证明了 V 是独异点。 □

16.3

(1)

证明: $\forall x, y, z \in S$，

$$\begin{aligned}(x \circ y) \circ z &= x \circ z && (\circ\text{ 定义})\\ &= x && (\circ\text{ 定义})\\ &= x \circ (y \circ z) && (\circ\text{ 定义})\end{aligned}$$

从而 $\langle S, \circ \rangle$ 是半群。 □

(2) 令 $S' = S \cup \{e\}$，$\circ' : S' \times S' \to S', x \circ' y = \begin{cases} y, & \text{若} x = e \\ x, & \text{否则} \end{cases}$，依教材定理 16.2，$\langle S', \circ', e \rangle$ 是一个独异点。

16.4

证明:

$$\begin{aligned}(a \circ b) \circ c &= a \circ (b \circ c) && (\text{结合律})\\ &= a \circ (c \circ b) && (b, c\text{ 可交换})\\ &= (a \circ c) \circ b && (\text{结合律})\\ &= (c \circ a) \circ b && (a, c\text{ 可交换})\\ &= c \circ (a \circ b) && (\text{结合律})\end{aligned}$$

□

16.5

(1)

证明:

$$\begin{aligned}a * b &= a * (a * a) && (a * a = b)\\ &= (a * a) * a && (\text{结合律})\\ &= b * a && (a * a = b)\end{aligned}$$

□

(2)

证明: 由于 V 的载体 $\{a, b\}$ 只有 a, b 两个元素，故分 $a * b = a$ 和 $a * b = b$ 两种情况讨论。

① 若 $a * b = a$，则:

$$\begin{aligned}b * b &= (a * a) * b && (a * a = b)\\ &= a * (a * b) && (\text{结合律})\\ &= a * a && (a * b = a)\\ &= b && (a * a = b)\end{aligned}$$

② 若 $a * b = b$，则:

$$\begin{aligned}b * b &= (a * a) * b && (a * a = b)\\ &= a * (a * b) && (\text{结合律})\\ &= a * b && (a * b = b)\end{aligned}$$

$$= b \qquad\qquad (a * b = b)$$

因此，无论对于何种情况，都有 $b * b = b$。 □

16.6

(1)

证明: 由题设，若 $a \circ a \neq a$，就有 $a \circ (a \circ a) \neq (a \circ a) \circ a$。与 V 是半群矛盾。 □

(2)

证明: 由题设，若 $a \circ b \circ a \neq a$，就有 $a \circ (a \circ b \circ a) \neq (a \circ b \circ a) \circ a$。但:

$$\begin{aligned} a \circ (a \circ b \circ a) &= (a \circ a) \circ (b \circ a) && \text{(结合律)} \\ &= a \circ (b \circ a) && \text{(第 (1) 小题结论)} \\ &= a \circ (b \circ a \circ a) && \text{(第 (1) 小题结论)} \\ &= (a \circ b \circ a) \circ a && \text{(结合律)} \end{aligned}$$

矛盾。 □

(3)

证明: 由题设，若 $a \circ b \circ a \neq a \circ c$，就有 $(a \circ c) \circ (a \circ b \circ c) \neq (a \circ b \circ c) \circ (a \circ c)$。但:

$$\begin{aligned} (a \circ c) \circ (a \circ b \circ c) &= (a \circ c \circ a) \circ (b \circ c) && \text{(结合律)} \\ &= a \circ (b \circ c) && \text{(第 (2) 小题结论)} \\ &= a \circ (b \circ (c \circ a \circ c)) && \text{(第 (2) 小题结论)} \\ &= (a \circ b \circ c) \circ (a \circ c) && \text{(结合律)} \end{aligned}$$

矛盾。 □

16.7

证明: 由于 V 是可交换半群，故 $*$ 运算满足交换律和结合律。从而:

$$\begin{aligned} (a * b) * (a * b) &= a * (b * a) * b && \text{(结合律)} \\ &= a * (a * b) * b && \text{(交换律)} \\ &= (a * a) * (b * b) && \text{(结合律)} \\ &= a * b && (a, b \text{ 是幂等元}) \end{aligned}$$

□

16.8

证明: $\forall x, y \in S$，

$$\begin{aligned} (x \circ \theta_l) \circ y &= x \circ (\theta_l \circ y) && \text{(结合律)} \\ &= x \circ \theta_l && (\theta_l \text{ 是左零元}) \end{aligned}$$

□

16.9

证明: 将这个半群记为 $V = \langle S, * \rangle$，由于 S 是非空的，故存在元素 $a \in S$。又由于 S 是有限的，由鸽巢原理知，存在 $i, j \in \mathbb{N}_+, i < j$，使得 $a^i = a^j$。记 $p = j - i$。

注意到，因为 $a^i = a^j = a^{i+p}$，所以有 $a^{i+2p} = a^{j+p} = a^j * a^p = a^i * a^p = a^j = a^i$。对 n 作归纳可证：$\forall n \in \mathbb{N}, a^{i+np} = a^i$。于是有 $a^{i+ip} = a^i$，而 $(a^{ip}) * (a^{ip}) = a^{2ip} = a^{(i+ip)+(ip-i))} = a^{i+ip} * a^{ip-i} = a^i * a^{ip-i} = a^{ip}$。

从而 a^{ip} 就是关于 $*$ 运算的一个幂等元。 □

16.10 由于 $2 \otimes 2 = 0, 3 \otimes 3 = 1$。因此，含有 2 的子半群必含 0，含有 3 的子半群必含 1。由于 0 是零元，1 是单位元，它们的加入显然不改变一个子半群的封闭性(即，若 $\langle S, \otimes\rangle$ 是 V 的一个子半群，则 $\langle S \cup \{0\}, \otimes\rangle$ 和 $\langle S \cup \{1\}, \otimes\rangle$ 也是 V 的子群)。而 $2 \otimes 3 = 2$，这一结果对子半群的封闭性也没有影响(因为若这一运算能够在某个子半群中出现，说明运算数 2 和 3 都在这个子半群中，从而运算结果 2 自然在这个子半群中)。从而 V 的子半群有：

$V_1 = \langle\{0\}, \otimes\rangle$;
$V_2 = \langle\{1\}, \otimes\rangle$;
$V_3 = \langle\{0, 1\}, \otimes\rangle$;
$V_4 = \langle\{0, 2\}, \otimes\rangle$;
$V_5 = \langle\{1, 3\}, \otimes\rangle$;
$V_6 = \langle\{0, 1, 2\}, \otimes\rangle$;
$V_7 = \langle\{0, 1, 3\}, \otimes\rangle$;
$V_8 = V = \langle\mathbb{Z}_4, \otimes\rangle$;

由于 1 是单位元，因此所有含有 1 的子半群都是 V 的子独异点。此外，由于 V_1 中只有一个元素，它自然也是独异点[1]，但它不是 V 的子独异点，这是因为：按子独异点的定义，只有 $\langle Z_4, \otimes, 1\rangle$ 的子代数系统才是“V 的子独异点”。而 V_1 对 $\langle Z_4, \otimes, 1\rangle$ 中的代数常数 1 不封闭，因而不是 V 的子独异点。而 $2 \otimes 2 = 2 \otimes 0 = 0$，从而 V_4 无单位元，不是独异点。

因此，上面 7 个子半群中，除 V_4 外，都是独异点。除 V_1 和 V_4 外，都是 V 的子独异点。

16.11

$\overline{*}$	$[a]$	$[b]$
$[a]$	$[a]$	$[b]$
$[b]$	$[b]$	$[a]$

16.12

(1)

证明: $\forall a, b, c, d \in S, aRc \wedge bRd$，分两种情况讨论：

① 若 $a, b, c, d \notin I$，则由 R 的定义有：$a = c \wedge b = d$。从而有 $a \circ b = c \circ d$，由 R 的定义可知：$(a \circ b)R(c \circ d)$。

② 若不然，则 a, c 和 b, d 至少有一组在 I 中。若 $a, c \in I$，则由 $IS \subseteq I$ 知，$a \circ b \in I \wedge c \circ d \in I$。若 $b, d \in I$，则由 $SI \subseteq I$ 知，$a \circ b \in I \wedge c \circ d \in I$。

因此，无论在哪种情况下都有：$aRc \wedge bRd \Rightarrow (a \circ b)R(c \circ d)$。

这就证明了 R 是 V 上的同余关系。 □

(2) 由 R 的定义知，I 中所有元素构成一个等价类，$S - I$ 中每一个元素单独构成一个等价类。从而 $S/R = \{I\} \cup \{\{x\} \mid x \in S - I\}$。而由 I 的性质知，$I \bar{\circ} x = x \bar{\circ} I = I, \forall x \in S/R$。对于其它元素 $[x], [y] \in (S/R - \{I\})$，$\{x\} \bar{\circ} \{y\} = [x \circ y] = \begin{cases} \{x \circ y\}, & \text{若 } x \circ y \notin I \\ I, & \text{若 } x \circ y \in I \end{cases}$。而前一种情况可以统一于后者(因为对任意 $[x], [y] \in S/R$，若 $x \in I \vee y \in I$，则必有 $x \circ y \in I$，从而 $[x] \bar{\circ} [y] = I$)。

---

[1] 对任意含有一个二元运算的代数系统 $\langle S, *\rangle$，若 S 中只有一个元素 a，则由运算封闭性知，$a * a = a$，从而 a 满足条件 $\forall x \in S (a * x = x * a = x)$，是单位元。因此，任何含一个二元运算和一个元素的代数系统必是独异点(而且也是群)。

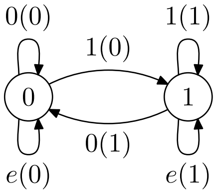
$$从而\ V/R = \langle S/R, \bar{\circ} \rangle, [x]\bar{\circ}[y] = \begin{cases} \{x \circ y\}, & 若\ x \circ y \notin I \\ I, & 否则 \end{cases} \quad \forall [x],[y] \in S/R。$$

16.13 $Q = \Gamma = \{0, 1\}$; $\Sigma = \{0, 1, e\}$;

δ	0	1	e
0	0	1	0
1	0	1	1

λ	0	1	e
0	0	0	0
1	1	1	1

状态图：



16.14 $Q = \{1, 2, 3\}$; $\Sigma = \{a, b\}$; $\Gamma = \{x, y\}$;

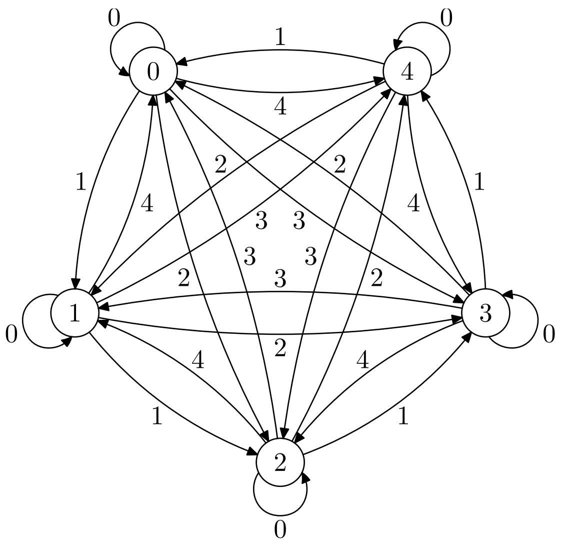
δ	a	b
1	1	3
2	1	2
3	1	2

λ	a	b
1	y	x
2	x	x
3	x	y

16.15

δ	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

状态图：



16.16 由运算表显然有 $q_0 \sim q_1, q_2 \sim q_3, q_4 \sim q_5$。

注意到，虽然 $\forall x \in \Sigma, \lambda(q_0, x) = \lambda(q_2, x)$，但 $\lambda * (q_0, 00) = \lambda(q_0, 0)\lambda(q_1, 0) = 00$，而 $\lambda * (q_2, 00) = \lambda(q_2, 0)\lambda(q_4, 0) = 01$，所以 $q_0 \nsim q_2$。

从而：$Q/{\sim} = \{\{q_0, q_1\}, \{q_2, q_3\}, \{q_4, q_5\}, \{q_6\}\}$。

$\overline{\delta}$	0	1
$[q_0]$	$[q_0]$	$[q_6]$
$[q_2]$	$[q_4]$	$[q_0]$
$[q_4]$	$[q_4]$	$[q_2]$
$[q_6]$	$[q_0]$	$[q_4]$

$\overline{\lambda}$	0	1
$[q_0]$	0	0
$[q_2]$	0	0
$[q_4]$	1	0
$[q_6]$	0	1

第十七章　群

17.1

证明: 易于验证，$\langle G, *, \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), ^{-1}\rangle$ 同构于 Klein 四元群 $\langle G', \circ, e, ^{-1}\rangle$。从而由教材定理 15.8 知，$G$ 关于矩阵乘法构成一个群。 □

17.2

证明: 由群内乘法运算的封闭性知，$\forall a, b \in G, a \circ b = au^{-1}b \in G$，从而 $\circ$ 运算是封闭的。

由群内乘法运算的结合律知，$\forall a, b, c \in G, (a \circ b) \circ c = au^{-1}bu^{-1}c = a \circ (b \circ c) \in G$，从而 $\circ$ 运算是结合的。

对任意 $a \in G$，$u \circ a = uu^{-1}a = a$，$a \circ u = au^{-1}u = a$。从而 $\circ$ 运算有单位元 u。

对任意 $a \in G$，$(ua^{-1}u) \circ a = ua^{-1}uu^{-1}a = u$，$a \circ (ua^{-1}u) = au^{-1}ua^{-1}u = u$，从而 G 中所有元素都有关于 $\circ$ 运算的逆元。

这就证明了 G 关于 $\circ$ 运算构成群。 □

17.3　取 $u = 2$，利用上题结论即得。

17.4

证明: 由群内乘法运算的封闭性和结合律可得 $*$ 运算的封闭性和结合律。

G 中的单位元显然也是 $*$ 运算的单位元。$\forall x \in G$，$x * x^{-1} = x^{-1}x = e, x^{-1} * x = xx^{-1} = e$，从而 G 中每个元素对 $*$ 运算均有逆元。

由群的定义知，$\langle G, * \rangle$ 是群。 □

17.5

证明: 封闭性易于验证。

由矩阵乘法的性质可知结合律成立，且 $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ 是单位元。

易于验证，$\left(\begin{smallmatrix}w&0\\0&w^2\end{smallmatrix}\right)$ 与 $\left(\begin{smallmatrix}w^2&0\\0&w\end{smallmatrix}\right)$ 互逆，$\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&w^2\\w&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&w\\w^2&0\end{smallmatrix}\right)$ 是 2 阶元。从而每个元素都有逆元。

由群的定义知，以上 6 个方阵对矩阵乘法构成群。 □

17.6

证明:

$$
\begin{aligned}
& (ab)^2 = a^2b^2 \\
\Longleftrightarrow\ & abab = aabb && \text{(幂运算定义)} \\
\Longrightarrow\ & ba = ab && \text{(消去律)}
\end{aligned}
$$

□

17.7

证明: 首先，用归纳法证明：$\forall k \in \mathbb{Z}^+, (x^{-1}yx)^k = x^{-1}y^kx$。

当 $k = 1$ 时，命题显然成立。

设当 $k = m$ 时，命题成立。则当 $k = m + 1$ 时：

$$\begin{aligned}
(x^{-1}yx)^{m+1} &= (x^{-1}yx)^m(x^{-1}yx) && \text{(幂运算定义)} \\
&= x^{-1}y^mx(x^{-1}yx) && \text{(归纳假设)} \\
&= x^{-1}y^myx && (xx^{-1} = e) \\
&= x^{-1}y^{m+1}x && \text{(幂运算定义)}
\end{aligned}$$

从而证明了 $\forall k \in \mathbb{Z}^+, (x^{-1}yx)^k = x^{-1}y^kx$。由此式和消去律可证原命题的必要性，由此式和代入规则即可得证充分性。 □

17.8

(2)

证明: $\forall a, b \in G$，

$$\begin{aligned}
b^{-1}a^{-1}ab &= b^{-1}b && (a^{-1}a = e) \\
&= e && (b^{-1}b = e) \\
abb^{-1}a^{-1} &= aa^{-1} && (b^{-1}b = e) \\
&= e && (a^{-1}a = e)
\end{aligned}$$

由逆元的唯一性得：$(ab)^{-1} = b^{-1}a^{-1}$。 □

(4) 首先证明 $(ab)^{-1} = b^{-1}a^{-1}$ 的推广形式：

引理 17.1 设 G 为群，对任意正整数 k，有 $\forall a_1, a_2, \cdots, a_k \in G$，$(a_1a_2\cdots a_k)^{-1} = a_k^{-1}\cdots a_2^{-1}a_1^{-1}$。特别地，$\forall k \in \mathbb{Z}^+, \forall a \in G, (a^k)^{-1} = (a^{-1})^k$。

证明: 当 $k = 1$ 时，命题显然成立。

若 $k = t$ 时命题成立。则当 $k = t + 1$ 时：

$$\begin{aligned}
(a_1a_2\cdots a_ta_{t+1})^{-1} &= a_{t+1}^{-1}(a_1a_2\cdots a_t)^{-1} && \text{(教材定理 17.2(2))} \\
&= a_{t+1}^{-1}a_t^{-1}\cdots a_2^{-1}a_1^{-1} && \text{(归纳假设)}
\end{aligned}$$

这就证明了上述引理。令 $a_1 = a_2 = \cdots = a_k = a$，即得该引理的特殊情况 $(a^k)^{-1} = (a^{-1})^k$。 □

再证原题。

证明: 由幂运算定义易知，若 m, n 中有一者为 0，则 $(a^n)^m = a^{nm} = e$。命题成立。

下面分四种情况讨论：

① 若 $m > 0$ 且 $n > 0$，则由教材定理 16.1(2) 即知，等式成立。

② 若 $m > 0$ 且 $n < 0$，令 $t = -n$，则有：

$$\begin{aligned}
(a^n)^m &= (a^{-t})^m && (n = -t) \\
&= ((a^{-1})^t)^m && \text{(幂运算定义)} \\
&= (a^{-1})^{tm} && \text{(教材定理 16.1(2))} \\
&= a^{-tm} && \text{(幂运算定义)} \\
&= a^{nm} && (n = -t)
\end{aligned}$$

③ 若 $m < 0$ 且 $n > 0$，令 $s = -m$，则有：

$$\begin{aligned}
(a^n)^m &= (a^n)^{-s} && (m = -s) \\
&= ((a^n)^{-1})^s && \text{(幂运算定义)}
\end{aligned}$$

$$\begin{aligned}
&= ((a^{-1})^n)^s && \text{(引理 17.1)}\\
&= (a^{-1})^{ns} && \text{(教材定理 16.1(2))}\\
&= a^{-ns} && \text{(幂运算定义)}\\
&= a^{nm} && (m = -s)
\end{aligned}$$

④ 若 $m < 0$ 且 $n < 0$，令 $s = -m, t = -n$，则有：

$$\begin{aligned}
(a^n)^m &= (a^{-t})^{-s} && (m = -s, n = -t)\\
&= (((a^{-1})^t)^{-1})^s && \text{(幂运算定义)}\\
&= (((a^t)^{-1})^{-1})^s && \text{(引理 17.1)}\\
&= (a^t)^s && \text{(教材定理 17.2(1))}\\
&= a^{ts} && \text{(幂运算定义)}\\
&= a^{nm} && (ts = nm)
\end{aligned}$$

这就证明了 $\forall m, n \in \mathbb{Z}, (a^n)^m = a^{nm}$。 □

(5)

证明： 首先用归纳法证明 $n \in \mathbb{N}$ 的情况。

当 $n = 0$ 时，等式显然成立。

若 $n = k$ 时，等式成立，则当 $n = k + 1$ 时：

$$\begin{aligned}
(ab)^{k+1} &= (ab)^k ab && \text{(幂运算定义)}\\
&= a^k b^k ab && \text{(归纳假设)}\\
&= a^k a b^k b && (G\ \text{是 Abel 群})\\
&= a^{k+1} b^{k+1} && \text{(幂运算定义)}
\end{aligned}$$

从而证明了：$\forall n \in \mathbb{N}, (ab)^n = a^n b^n$。

对于 $n < 0$ 的情况，令 $t = -n$，则 $t > 0$，且：

$$\begin{aligned}
(ab)^n &= (ab)^{-t} && (n = -t)\\
&= ((ab)^{-1})^t && \text{(幂运算定义)}\\
&= (b^{-1}a^{-1})^t && \text{(教材定理 17.2(2))}\\
&= (b^{-1})^t (a^{-1})^t && (\forall n \in \mathbb{N}, (ab)^n = a^n b^n)\\
&= b^{-t} a^{-t} && \text{(幂运算定义)}\\
&= b^n a^n && (n = -t)\\
&= a^n b^n && (G\ \text{是 Abel 群})
\end{aligned}$$

这就证明了原命题。 □

17.9

(1)

证明： $\forall k \in \mathbb{Z}$，

$$\begin{aligned}
& (b^{-1}ab)^k = e\\
\iff & (b^{-1}ab)^{k+1} = (b^{-1}ab) && \text{(代入规则、消去律)}\\
\iff & a^{k+1} = a && \text{(习题 17.7 结论)}\\
\iff & a^k = e && \text{(代入规则、消去律)}
\end{aligned}$$

这就证明了 $\{k \mid k \in \mathbb{Z}^+ \land (b^{-1}ab)^k = e\} = \{k \mid k \in \mathbb{Z}^+ \land a^k = e\}$，从而它们的最小元也是

相同的。由“阶”的定义知，$|b^{-1}ab| = |a|$。 □

(2)

证明： 由归纳法易证：对群中任意元素 $a, b \in G$，有 $(ab)^k a = a(ba)^k, \forall k \in \mathbb{Z}$。

从而，$\forall k \in \mathbb{Z}$，

$$
\begin{aligned}
& (ab)^k = e \\
\iff & (ab)^k a = a && \text{(代入规则、消去律)} \\
\iff & a(ba)^k = a && ((ab)^k a = a(ba)^k) \\
\iff & (ba)^k = e && \text{(代入规则、消去律)}
\end{aligned}
$$

这就证明了 $\{k \mid k \in \mathbb{Z}^+ \wedge (ab)^k = e\} = \{k \mid k \in \mathbb{Z}^+ \wedge (ba)^k = e\}$，从而它们的最小元也是相同的。由“阶”的定义知，$|ab| = |ba|$。 □

(3) 利用第 2 小题结论立即得证。

17.10

证明： 设 $|G| = 2k$。作图 $H = \langle V, E \rangle$，其中 $V = G$，为 G 中所有元素，令 $E = \{(x, y) \mid x, y \in G \wedge xy = e\}$。由逆元的唯一性知，$\forall x \in G$，存在唯一的 y，使 $(x, y) \in E$。从而，对 $V = G$ 中的一切顶点 x，顶点的度 $d_H(x) = \begin{cases} 2, & \text{若} x^{-1} = x; \\ 1, & \text{否则.} \end{cases}$。注意到，$d_H(e) = 2$。若 G 中不存在二阶元，则 e 是 H 中唯一的 2 度顶点。从而 H 中有 $|G| - 1 = 2k - 1$ 个奇数度顶点。这与图论基本定理矛盾。 □

17.11

证明： 若不然，由习题 16.6 结论就有 $\forall a \in G, aa = a$。由消去律得：$\forall a \in G, a = e$。也就是说，$G = \{e\}$ 是平凡群。然而，平凡群是交换群。这与题设“G 是非交换群”矛盾。 □

17.12

证明： 由于 $(p, q) = 1$，故存在 $m, n \in \mathbb{Z}$，使得 $mp + nq = 1$，也即，$mp = -nq + 1$。从而有：

$$
\begin{aligned}
& u_1^{mp} = u_2^{mp} = v_1^{-nq} = v_2^{-nq} = e && (e^m = e, e^n = e) \\
\Longrightarrow\ & u_1^{mp} v_1^{-nq} = u_2^{mp} v_2^{-nq} = e && (ee = e) \\
\iff & u_1 u_1^{-nq} v_1^{-nq} = u_2 u_2^{-nq} v_2^{-nq} = e && (mp = -nq + 1) \\
\iff & u_1 (u_1 v_1)^{-nq} = u_2 (u_2 v_2)^{-nq} && (u_1 v_1 = v_1 u_1\ \text{、}\ u_2 v_2 = v_2 u_2) \\
\iff & u_1 = u_2 && (u_1 v_1 = u_2 v_2\ \text{、消去律})
\end{aligned}
$$

□

17.13

(1) 构成群。由定义易于验证。

(2) 构成群。由定义易于验证。

(3) 不构成群。记 $S \subseteq M_n(\mathbb{R})$ 为全体行列式 ≥ 0 的矩阵集合，令 $A = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \multicolumn{4}{c}{\cdots\cdots\cdots\cdots} \\ 0 & 0 & \cdots & 1 \end{pmatrix}$ 和

$B = \begin{pmatrix} -2 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \hdotsfor{4} \\ 0 & 0 & \cdots & 0 \end{pmatrix}$。则 $|A| = 1, |B| = 0$，$A, B \in S$，但 $|A+B| = \left| \begin{pmatrix} -1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \hdotsfor{4} \\ 0 & 0 & \cdots & 1 \end{pmatrix} \right| = -1$，从而 $A + B \notin S$。S 对矩阵加法不封闭。

(4) 构成群。由定义易于验证。

17.14 本题即为教材定理 17.29。证明如下：

证明： 由于 $ea = ae = a$，因此 $e \in H$，H 非空。

$\forall x, y \in H$，

$$xya = xay \tag{$ya = ay$}$$

$$= axy \tag{$xa = ax$}$$

因此，$xy \in H$。

$\forall x$，

$$x \in H$$

$$\iff xa = ax \tag{H 定义}$$

$$\iff x^{-1}xa = x^{-1}ax \tag{两边左乘 x^{-1}}$$

$$\iff x^{-1}xax^{-1} = x^{-1}axx^{-1} \tag{两边右乘 x^{-1}}$$

$$\iff ax^{-1} = x^{-1}a \tag{$xx^{-1} = x^{-1}x = e$}$$

$$\iff x^{-1} \in H \tag{H 定义}$$

由子群判定定理一知，H 是 G 的子群。 □

17.15

(1) 由于对任何群 G，$\{e\}$ 和 G 本身都是 G 的子群。故，G 只有一个子群当且仅当 $G = \{e\}$。

(2) 由 Lagrange 定理可知，所有素数阶循环群都有且仅有两个子群：$\{e\}$ 和 G 本身。

(3) 由 Lagrange 定理和教材定理 17.13 可知，对所有素数 p，若 G 为 p^2 阶循环群，则 G 必有且仅有 3 个群：$\{e\}$ 、G 和一个 p 阶子群。

17.16

证明： 充分性：

若 $H_1H_2 = H_2H_1$，则：由于 H_1, H_2 都是子群，所以 $e \in H_1, e \in H_2$，从而 $e = ee \in H_1H_2$。这就是说，H_1H_2 是非空的。又由 H_1H_2 的定义知，H_1H_2 中的任意元素均可写成 ab 的形式，其中 $a \in H_1, b \in H_2$。因此，任取 $x, y \in H_1H_2$，将他们写成：$x = ab, y = cd$，其中 $a, c \in H_1, b, d \in H_2$。从而 $xy^{-1} = ab(cd)^{-1} = abd^{-1}c^{-1}$。由于 $b, d \in H_2$，且 H_2 是群，故 $bd^{-1} \in H_2$。于是 $abd^{-1} \in H_1H_2 = H_2H_1$，这就是说，存在 $h_2 \in H_2, h_1 \in H_1$，使得 $abd^{-1} = h_2h_1$。又由于 $h_1, c \in H_1$ 且 H_1 是群，所以 $h_1c^{-1} \in H_1$。从而 $xy^{-1} = abd^{-1}c^{-1} = h_2h_1c^{-1} \in H_2H_1 = H_1H_2$。由子群判定定理二知，$H_1H_2$ 是 G 的子群。

必要性：

若 H_1H_2 是子群，则：由于 $\forall x \in H_1H_2$，存在 $a \in H_1, b \in H_2$，使得 $x = ab$，故：

$$x \in H_1H_2$$

$$\implies x^{-1} \in H_1H_2 \tag{H_1H_2 是群}$$

$$\iff \exists a \exists b (a \in H_1 \land b \in H_2 \land x^{-1} = ab) \tag{H_1H_2 定义}$$

$\Longrightarrow \exists a \exists b(a^{-1} \in H_1 \wedge b^{-1} \in H_2 \wedge x^{-1} = ab)$ (H_1, H_2 是群)

$\Longrightarrow \exists a \exists b(b^{-1}a^{-1} \in H_2H_1 \wedge x^{-1} = ab)$ (H_2H_1 定义)

$\Longleftrightarrow \exists a \exists b((ab)^{-1} \in H_2H_1 \wedge x^{-1} = ab)$ (教材定理 17.2(2))

$\Longrightarrow \exists a \exists b((x^{-1})^{-1} \in H_2H_1)$ ($x^{-1} = ab$)

$\Longleftrightarrow \exists a \exists b(x \in H_2H_1)$ (教材定理 17.2(1))

这就证明了 $H_1H_2 \subseteq H_2H_1$。再证 $H_2H_1 \subseteq H_1H_2$ (由于题设不保证 H_2H_1 为群，故 $H_2H_1 \subseteq H_1H_2$ 的证明方法略有不同)：

$\forall x$，

$x \in H_2H_1$

$\Longleftrightarrow \exists a \exists b(a \in H_1 \wedge b \in H_2 \wedge x = ba)$ (H_2H_1 定义)

$\Longrightarrow \exists a \exists b(a^{-1} \in H_1 \wedge b^{-1} \in H_2 \wedge x = ba)$ (H_1, H_2 是群)

$\Longrightarrow \exists a \exists b(a^{-1}b^{-1} \in H_1H_2 \wedge x = ba)$ (H_1H_2 定义)

$\Longleftrightarrow \exists a \exists b((ba)^{-1} \in H_1H_2 \wedge x = ba)$ (教材定理 17.2(2))

$\Longrightarrow \exists a \exists b((x)^{-1} \in H_1H_2)$ ($x = ba$)

$\Longrightarrow \exists a \exists b(((x)^{-1})^{-1} \in H_1H_2)$ (H_1H_2 是群)

$\Longleftrightarrow \exists a \exists b(x \in H_1H_2)$ (教材定理 17.2(1))

这就证明了 $H_2H_1 \subseteq H_1H_2$。从而证明了 $H_1H_2 = H_2H_1$。[1] □

17.17

证明: 先证 $H_1H_2 \cap H_1' \cap H_2' \subseteq (H_1 \cap H_2')(H_1' \cap H_2)$。对左边集合中的任意元素 x，都存在 $h_1 \in H_1, h_2 \in H_2$，使得 $x = h_1h_2 \in (H_1' \cap H_2')$。注意到，$h_2 \in H_2 \subseteq H_2'$，从而 $h_2^{-1} \in H_2'$。从而 $h_1 = (h_1h_2)h_2^{-1} \in H_2'$。这样就证明了 $h_1 \in H_1 \cap H_2'$。同理可证 $h_2 \in H_1' \cap H_2$。从而有 $x = h_1h_2 \in (H_1 \cap H_2')(H_1' \cap H_2)$。

再证 $(H_1 \cap H_2')(H_1' \cap H_2) \subseteq H_1H_2 \cap H_1' \cap H_2'$。对任意元素 $x \in (H_1 \cap H_2')(H_1' \cap H_2)$，存在 $a \in H_1 \cap H_2', b \in H_1' \cap H_2$，使得 $x = ab$。注意到，$a \in H_1, b \in H_2$，所以显然有 $x = ab \in H_1H_2$。同时，由于 $H_1 \subseteq H_1', H_2 \subseteq H_2'$。所以有 $a, b \in H_1' \cap H_2'$。已知 H_1', H_2' 都是子群，则由教材例 17.12 知，$H_1' \cap H_2'$ 也是子群。从而得：$x = ab \in H_1' \cap H_2'$。这就证明了 $(H_1 \cap H_2')(H_1' \cap H_2) \subseteq H_1H_2 \cap H_1' \cap H_2'$。

综上所述，有 $H_1H_2 \cap H_1' \cap H_2' = (H_1 \cap H_2')(H_1' \cap H_2)$。 □

17.18

(1) 由于 G 同构于 Klein 四元群，故 G 的子群和子群格与教材例 17.14 类似。

G 的子群有：

$H_1 = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\}$;

$H_2 = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\}$;

$H_3 = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\}$;

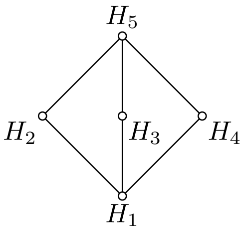
$H_4 = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\}$;

$H_5 = G$.

子群格如下：

---

[1] 注意到，按照 H_1H_2 的定义，对任意 $x, y \in G$， $xy \in H_1H_2$ 只能推出存在两个元素 $h_1 \in H_1, h_2 \in H_2$，使得 $xy = h_1h_2$。而不能直接由 $xy \in H_1H_2$ 推出 $x \in H_1 \wedge y \in H_2$。因此，本题的必要性部分不可以这样证：$\forall a \in H_1, b \in H_2$，$ab \in H_1H_2 \Longleftrightarrow (ab)^{-1} \in H_1H_2 \Longleftrightarrow b^{-1}a^{-1} \in H_1H_2 \Longleftrightarrow b^{-1} \in H_1 \wedge a^{-1} \in H_2 \Longleftrightarrow b \in H_1 \wedge a \in H_2 \Longleftrightarrow ab \in H_2H_1$。因为 $b^{-1}a^{-1} \in H_1H_2$ 不能推出 $b^{-1} \in H_1$ 和 $a^{-1} \in H_2$。



(2) 易于验证，以下 6 个是 G 的子群：

$H_1 = \{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\}$;

$H_2 = \{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)\}$;

$H_3 = \{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&w^2\\w&0\end{smallmatrix}\right)\}$;

$H_4 = \{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&w\\w^2&0\end{smallmatrix}\right)\}$;

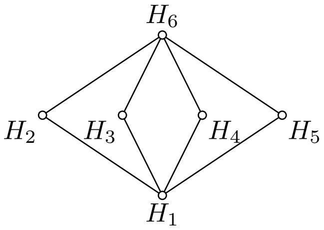
$H_5 = \{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}w&0\\0&w^2\end{smallmatrix}\right), \left(\begin{smallmatrix}w^2&0\\0&w\end{smallmatrix}\right)\}$;

$H_6 = G$.

下面证明 G 只有以上 6 个子群。

由 Lagrange 定理可知，G 的非平凡子群只能是 2 阶或 3 阶的。再由 Lagrange 定理推论 1 知，除单位元外，2 阶群的元素只能是 2 阶或 3 阶群的元素只能是 3 阶元。而 G 中共有 3 个 2 阶元，它们分别与单位元构成 H_2 、H_3 和 H_4。两个 3 阶元由于互为逆元，故必须同时出现。因此，它们能组成的非平凡子群只有 H_5。这就证明了上述 6 个子群是 G 的所有子群。

子群格如下：



17.19

(1) 由教材定理 17.12(2) 知，G 的生成元有 $a, a^2, a^4, a^7, a^8, a^{11}, a^{13}, a^{14}$。

(2) 由教材定理 17.13(3) 和 Lagrange 定理知，G 除了两个平凡子群外，还有一个 3 阶子群和一个 5 阶子群。故，G 的子群包括：

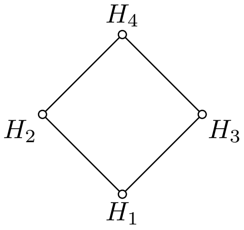
$H_1 = \{e\}$;

$H_2 = \langle a^5 \rangle = \{e, a^5, a^{10}\}$;

$H_3 = \langle a^3 \rangle = \{e, a^3, a^6, a^9, a^{12}\}$;

$H_4 = \langle a \rangle = G$.

子群格如下：



17.20

证明： 若不然，则存在 $c \in \langle a\rangle \cap \langle b\rangle$，$c \neq e$。考虑 $\langle c\rangle$。由于 $c \neq e$ 且 $c, e \in \langle c\rangle$，故 $|\langle c\rangle| > 1$。又由于 $c \in \langle a\rangle$，且 $\langle a\rangle$ 是群，故由 $\langle c\rangle$ 的定义知：$\langle c\rangle \leqslant \langle a\rangle$。从而由 $|\langle a\rangle| = |a| = p$ 是素数和 Lagrange 定理可知，$|\langle c\rangle| = |\langle a\rangle|$。结合 $\langle c\rangle \subseteq \langle a\rangle$ 就有，$a \in \langle c\rangle = \langle a\rangle$。这就是说，存在是 $k \in \mathbb{Z}$，使得 $c^k = a$。从而由 $\langle b\rangle$ 是群和 $c \in \langle b\rangle$ 可知，$a = c^k \in \langle b\rangle$。这与题设 $a \notin \langle b\rangle$ 矛盾。 □

17.21

证明： $H_1H_2 \subseteq G$ 是显然的。

设 $G = \langle a\rangle$。由教材定理 17.13(3) 可知，$H_1 = \langle a^s\rangle, H_2 = \langle a^r\rangle$。由于 $(r, s) = 1$。故存在 $m, n \in \mathbb{Z}$，使得 $mr + ns = 1$。对任意 $x \in G$，设 $x = a^t$，则有 $x = a^{tmr+tns} = a^{s(tm)}a^{r(tn)} \in H_1H_2$。从而有 $G \subseteq H_1H_2$。

综合即有：$G = H_1H_2$。 □

17.22

证明： 记 $H = H_1 \cap H_2$。由定义有，$a^d \in H$。对由教材例 17.12(1) 知，$H \leqslant G$。从而有 $\langle a^d\rangle \subseteq H$。

下面证明 $H \subseteq \langle a^d\rangle$。分两种情况讨论：

情况一：若 G 是无限群，则对任意 $a^t \in H$，由于 $H = H_1 \cap H_2$，故 $a^t \in H_1$，$a^t \in H_2$，由定义知，存在 $k_1, k_2 \in \mathbb{Z}$，使得 $a^{k_1r} = a^{k_2s} = a^t$。由于 G 是无限阶的，所以必有 $k_1r = t$ 和 $k_2s = t$ (否则，不妨设 $k_1r \neq t$，则由消去律知 $a^{k_1r-t} = 0$ 和 $k_1r - t \neq 0$，从而 $|G| = |a| \mid k_1r - t$，这与 G 是无限阶群矛盾)，从而有 $r \mid t$，$s \mid t$，由最小公倍数的性质知 $d = [r, s] \mid t$，从而有 $a^t \in \langle a^d\rangle$。由 a^t 的任意性知，$H \subseteq \langle a^d\rangle$。

情况二：若 G 是 n 阶有限群，则由教材例 17.12 和子群定义知，$H \leqslant H_1$ 且 $H \leqslant H_2$。从而由 Lagrange 定理知和教材例 17.16 知，$|H| \mid |H_1| = \dfrac{n}{(n, r)}$，$|H| \mid |H_2| = \dfrac{n}{(n, s)}$。从而 $(n, r) \mid n|H|$，$(n, s) \mid n|H|$，$[(n, r), (n, s)] \mid n|H|$，也即 $|H| \mid \dfrac{n}{[(n, r), (n, s)]}$。另一方面，由教材例 17.16 知，$|\langle a^d\rangle| = |\langle a^d\rangle| = \dfrac{n}{(n, d)} = \dfrac{n}{(n, [r, s])}$。

下面只需证明 $(n, [r, s]) = [(n, r), (n, s)]$，就可得到 $|H| \mid |\langle a^d\rangle|$，进而由 $\langle a^d\rangle \subseteq H$ 可得 $|\langle a^d\rangle| \leq |H|$，综合得 $|\langle a^d\rangle| = |H|$。再由 $H \subseteq G$ 是有限群和教材定理 5.5 推论就有 $\langle a^d\rangle = H$。

在证明 $(n, [r, s]) = [(n, r), (n, s)]$ 之前，注意到如下事实：

引理 17.2 对任意 $x, y, z \in \mathbb{R}$，有 $\min(x, \max(y, z)) = \max(\min(x, y), \min(x, z))$。

证明： 分两种情况考虑。

若 $x \leq \max(y, z)$，则 $\min(x, \max(y, z)) = x$，而对 y, z 中较大者(不妨设为 y)，则有 $\min(x, y) = x$，而 $\min(x, z) \leq x$。从而 $\max(\min(x, y), \min(x, z)) = x$。等式成立。

若 $x > \max(y, z)$，则必有 $x > y$，$x > z$，从而 $\min(x, y) = y$，$\min(x, z) = z$，$\max(\min(x, y), \min(x, z)) = \max(y, z)$。而由于 $x > \max(y, z)$，所以 $\min(x, \max(y, z)) = \max(y, z)$。等式也成立。 □

下面证明 $(n, [r, s]) = [(n, r), (n, s)]$。

设 n, r, s 的素因子分解式分别为 $n = \prod p_i^{a_i}$，$r = \prod p_i^{b_i}$，$s = \prod p_i^{c_i}$。则：

$$\begin{aligned}
(n, [r, s]) &= \prod p_i^{\min(n, \max(r, s))} && (\gcd, \text{lcm 性质}) \\
&= \prod p_i^{\max(\min(n, r), \min(n, s))} && (\text{引理 17.2}) \\
&= [(n, r), (n, s)] && (\gcd, \text{lcm 性质})
\end{aligned}$$

□

17.23

证明: 分两情况讨论:

情况一：若 G 中存在无限阶元 a，则 $\langle a\rangle, \langle a^2\rangle, \cdots, \langle a^k\rangle, \cdots$ $(k \in \mathbb{Z})$都是 G 的子群，且为互不相同的子群。命题成立。

情况二：若 G 中不存在无限阶元，则对任意 $g \in G$，$|\langle g\rangle| = |g|$ 是有限的。作 $S = \{\langle g\rangle \mid g \in G\}$，我们证明 S 是无穷集合，从而证明 G 有无穷多个不同的子群。

注意到，$G = \cup S$。从而：

$$\begin{aligned} |G| &= |\bigcup_{x \in S} x| && (G = \cup S) \\ &\leq \sum_{x \in S} |x| && (\text{容斥原理}) \end{aligned}$$

若 S 是有穷的，则 $\sum\limits_{x \in S} |x|$ 是有限个有限量之和，从而也是有穷的。这与 G 是无限群矛盾。□

17.24

(1) $\sigma\tau = \left(\begin{smallmatrix} 1&2&3&4&5 \\ 3&4&5&2&1 \end{smallmatrix}\right)$, $\quad \tau\sigma = \left(\begin{smallmatrix} 1&2&3&4&5 \\ 2&4&5&1&3 \end{smallmatrix}\right)$, $\quad \sigma^{-1} = \left(\begin{smallmatrix} 1&2&3&4&5 \\ 2&5&4&3&1 \end{smallmatrix}\right)$, $\quad \tau^{-1} = \left(\begin{smallmatrix} 1&2&3&4&5 \\ 3&5&2&1&4 \end{smallmatrix}\right)$;

(2) $\sigma = (152)(34) = (12)(15)(34), \quad \tau = (14523) = (13)(12)(15)(14).$

17.25

证明: 记 $A = \langle\{(12), (13), \cdots, (1n)\}\rangle, B = \langle\{(12), (23), \cdots, (n-1\,n)\}\rangle$。

$B \subseteq S_n$ 是显然的。下面分别证 $S_n \subseteq A$ 和 $A \subseteq B$，从而证明 $S_n = A = B$。

对任意置换 $\sigma \in S_n$，由教材定理 17.16 可知，σ 可以表成若干个轮换之积。下面分两种情况证明每个轮换都是 A 中若干个元素的乘积。从而证明 $\sigma \in A$。

情况一：若轮换 $\tau = (i_1 i_2 \cdots i_k)$ 中含有 1，即，存在 $1 \leq j \leq k$，使得 $i_j = 1$。则由轮换的定义可知：$\tau = (i_j i_{j+1} \cdots i_k i_1 i_2 \cdots i_{j-1})$。再由 $i_j = 1$ 和教材定理 17.17 知，$\tau = (1 i_{j-1}) \cdots (1 i_2)(1 i_1)(1 i_k) \cdots (1 i_{j+1})$。也即，$\tau$ 可以表示成 A 中若干个元素的乘积。

情况二：若轮换 $\tau' = (i_1 i_2 \cdots i_k)$ 中不含 1，即，$i_j \neq 1 (1 \leq j \leq k)$。此时，易于验证，$\tau' = (1 i_2)(1 i_2 \cdots i_k)(1 i_1) = (1 i_2)(1 i_k) \cdots (1 i_2)(1 i_1)$。从而 τ' 亦可表示成 A 中若干元素之积。

这就是说，任意 n 元置换 $\sigma \in S_n$ 都能表示成 A 中若干元素之积。从而由 A 对置换乘法的封闭性知，$\sigma \in A$。这就证明了 $S_N \subseteq A$。

下面证明 $A \subseteq B$：

当 $n = 1, 2$ 时，由定义直接有 $A \subseteq B$。对任意 $n \geq 3$，对 k 作归纳证明：$(1k) = (12)(23) \cdots (k-1\,k)$ $(2 \leq k \leq n)$。

当 $k = 2$ 时，等式自然成立。

若 $k = t$ 时，等式成立。则当 $k = t+1$ 时，由归纳假设有：$(12)(23) \cdots (t-1\,t)(t\,t+1) = (1t)(t\,t+1)$。直接验证 $(1t)(t\,t+1)$ 对 $1, t, t+1$ 的作用可知，$(1t)(t\,t+1) = (1\,t+1)$。

如此，就证明了对任意 $(1k) \in \{(12), (13), \cdots, (1n)\}$，有 $(1k) = (12)(23) \cdots (k-1\,k) \in B$。从而由 A 的定义知，$A \subseteq B$。

综合得 $A = B = S_n$。 □

17.26

(1) $x = \sigma^{-1}\tau = \left(\begin{smallmatrix} 1&2&3&4&5 \\ 4&1&2&5&3 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1&2&3&4&5 \\ 5&3&1&2&4 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1&2&3&4&5 \\ 3&2&4&1&5 \end{smallmatrix}\right)$,

$y = \tau\sigma^{-1} = \left(\begin{smallmatrix} 1&2&3&4&5 \\ 5&3&1&2&4 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1&2&3&4&5 \\ 4&1&2&5&3 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1&2&3&4&5 \\ 2&5&3&4&1 \end{smallmatrix}\right)$;

(2) $|\sigma| = |(12354)| = 5^1, \quad |\tau| = |(15423)| = 5^1.$

17.27 $H = \{(1), (1234), (13)(24), (1432)\}$;

$H(1) = H(1234) = H(13)(24) = H(1432) = H$;

$$\begin{aligned}
&H(12)=H(134)=H(1423)=H(243)=\{(12),(134),(1423),(243)\};\\
&H(13)=H(14)(23)=H(24)=H(12)(34)=\{(13),(14)(23),(24),(12)(34)\};\\
&H(14)=H(234)=H(1243)=H(132)=\{(14),(234),(1243),(132)\};\\
&H(23)=H(124)=H(1342)=H(143)=\{(23),(124),(1342),(143)\};\\
&H(34)=H(123)=H(1324)=H(142)=\{(34),(123),(1324),(142)\}.
\end{aligned}$$

17.28 因为 $\forall r,s,t\in\mathbb{Q},r\neq 0$，$\left(\begin{smallmatrix} r & s\\ 0 & 1\end{smallmatrix}\right)\cdots\left(\begin{smallmatrix} 1 & t\\ 0 & 1\end{smallmatrix}\right)=\left(\begin{smallmatrix} r & rt+s\\ 0 & 1\end{smallmatrix}\right)$，所以 H 全部左陪集的集合为：$\{\{\left(\begin{smallmatrix} r & rt+s\\ 0 & 1\end{smallmatrix}\right)\mid t\in\mathbb{Q}\}\mid r,s\in\mathbb{Q},r\neq 0\}$。

注意到，$r,s\in\mathbb{Q},r\neq 0$ 时，$\{rt+s\mid t\in\mathbb{Q}\}=\mathbb{Q}$。这是因为：由 $r,s,t\in\mathbb{Q}$ 显然有 $rt+s\in\mathbb{Q}$，从而 $\{rt+s\mid t\in\mathbb{Q}\}\subseteq\mathbb{Q}$。而对任意 $t'\in\mathbb{Q}$，令 $t=(t'-s)/r$，则 $t\in\mathbb{Q}$，且 $t'=rt+s\in\{rt+s\mid t\in\mathbb{Q}\}$。这就证明了 $\{rt+s\mid t\in\mathbb{Q}\}=\mathbb{Q}$。从而，$H$ 全部左陪集的集合又可写成：$\{\{\left(\begin{smallmatrix} r & t\\ 0 & 1\end{smallmatrix}\right)\mid t\in\mathbb{Q}\}\mid r\in\mathbb{Q},r\neq 0\}$。

17.29 仿教材定理 17.20 至教材定理 17.24 可证。

17.30

证明： 记 $H=H_1\cap H_2$。显然有 $e\in H$。由教材例 17.12(1) 可知，H 是群，从而也是 H_1 和 H_2 的子群。由 Lagrange 定理知，$|H|\mid r$ 且 $|H|\mid s$，从而 $|H|\mid(r,s)=1$。由 $e\in H$ 和 $|H|\mid 1$ 可知，$H=\{e\}$。 □

17.31

证明：

证法一： 设 G 为 p^m 阶群。对 m 作强数学归纳。

当 $m=1$ 时，G 本身就是 G 的 p 阶子群，命题成立。

若命题对一切正整数 $m<k$ 都成立，则当 $m=k$ 时，由 $|G|=p^k>1$ 知，G 中有非单位元。任取一非单位元 a。若 $|a|=p^k$，则 $|\langle a\rangle|=|a|=p^k=|G|$，从而由 G 有限群、$\langle a\rangle\subseteq G$、$|\langle G\rangle|=|G|$ 和教材定理 5.5 推论可知，$G=\langle a\rangle$ 是循环群。从而由教材定理 17.13(3) 知，G 有 p 阶子群。反之，若 $|a|<p^k$，则由 Lagrange 定理知，$|\langle a\rangle|=|a|=p^t(1\leq t<k)$。由归纳假设知 $\langle a\rangle$ 有 p 阶子群，这样的 p 阶子群显然也是 G 的子群。故，当 $m=k$ 时，命题依然成立。

证法二：[2]设 G 为任意 p^m 阶群。

由题设显然有 $|G|\geq 2$。任取非单位元 $a\in G$。由 $a\neq e$ 和教材定理 17.26 推论 1 可知，$1<|a|\mid p^m$。由于 p 是素数，所以必有 $|a|=p^k$，$k\in\mathbb{Z}^+$。

令 $b=a^{p^{k-1}}$。注意到，$b\neq e$ (否则将与 $|a|=p^k$ 矛盾)，且 $b^p=(a^{p^{k-1}})^p=a^{p^k}=e$。从而有 $1<|b|\mid p$。由素数的性质可知，$|b|=p$。这就证明了 G 中存在 p 阶子群 $\langle b\rangle$。 □

17.32

证明： 因为 G 是有限群，所以 $H\leqslant G$ 也是有限群。故：

$$\begin{aligned}
[G:H]&=\frac{|G|}{|H|} && \text{(Lagrange 定理)}\\
&=\frac{[G:K]|K|}{|K|/[K:H]} && \text{(Lagrange 定理)}\\
&=[G:K][K:H]
\end{aligned}$$

□

17.33

(1)

---

[2] 感谢 sunbird2002 大侠给出这一证法。

证明: 令 $f : A \times B \to AB$，$\forall \langle a, b\rangle \in A \times B$，$f(\langle a, b\rangle) = ab$。

f 显然是满射。从而 $\{f^{-1}[g] \mid g \in AB\}$ 是 $A \times B$ 的一个划分，其中 $f^{-1}[g] = \{\langle a, b\rangle \mid \langle a, b\rangle \in A \times B \wedge f(\langle a, b\rangle) = g\}$ 是 $\{g\}$ 的原象。从而有：

$$\begin{aligned}|A \times B| &= |\bigcup_{g \in AB} f^{-1}[g]| \\ &= \sum_{g \in AB} |f^{-1}[g]|\end{aligned}$$

下面证明对任意 $g \in AB$，有 $|f^{-1}[g]| = |A \cap B|$。

由定义，对任意 $g \in AB$，存在 $a \in A, b \in B$，使得 $g = ab$。取 $S_g = \{\langle ac, c^{-1}b\rangle \mid c \in A \cap B\}$。易见，对 S_g 中的所有元素 $\langle ac, c^{-1}b\rangle$，有 $\langle ac, c^{-1}b\rangle \in A \times B$ 和 $f(\langle ac, c^{-1}b\rangle) = g$，从而有 $S_g \subseteq f^{-1}[g]$。反之，对任意 $\langle x, y\rangle \in f^{-1}[g]$，有：

$$\begin{aligned}& xy = ab && (xy = g = ab) \\ \Longrightarrow\ & x = aby^{-1} && (\text{两边右乘 } y^{-1}) \\ \Longrightarrow\ & xa^{-1} = by^{-1} && (\text{两边右乘 } a^{-1})\end{aligned}$$

令 $c = by^{-1}$，由 $b \in B, y \in B$ 知，$c \in B$。又因为 $c = by^{-1} = xa^{-1} \in A$，所以有 $c \in A \cap B$。从而 $\langle x, y\rangle = \langle ac, c^{-1}b\rangle \in S_g$。这就证明了 $f^{-1}[g] = S_g$。又由消去律知，$\forall c \in A \cap B$，$ac = ac' \Leftrightarrow c = c'$。从而 $|f^{-1}[g]| = |S_g| = |A \cap B|$。

这就是说，$|A||B| = |A \times B| = \sum\limits_{g \in AB} |f^{-1}[g]| = \sum\limits_{g \in AB} |A \cap B| = |AB||A \cap B|$。 □

(2)

证明: 由题设和习题 17.30 结论知，$A \cap B = \{e\}$。再由第 (1) 小题知，$|AB| = |AB||A \cap B| = |A||B|$。 □

17.34 首先证明以下引理：

引理 17.3 设 $\sigma = (i_1 i_2 \cdots i_k)$ 为集合 A 上的任意 k 阶轮换，τ 是 A 上的任意置换，则 $\tau\sigma\tau^{-1} = (\tau(i_1)\tau(i_2)\cdots\tau(i_k))$ 也是 A 上的一个 k 阶轮换。

证明: 对任意 $x \in A$，分两种情况讨论：

情况一：若存在 $i_j \in \{i_1, i_2, \cdots, i_k\}$，使得 $x = \tau(i_j)$，即 $i_j = \tau^{-1}(i_j)$，则：

$$\begin{aligned}\tau\sigma\tau^{-1}(x) &= \tau\sigma(i_j) && (i_j = \tau^{-1}(i_j)) \\ &= \begin{cases}\tau(i_{j+1}), & j < k \\ \tau(i_1), & j = k\end{cases} && (\sigma = (i_1 i_2 \cdots i_k)) \\ &= (\tau(i_1)\tau(i_2)\cdots\tau(i_k))(x) && (\text{轮换定义})\end{aligned}$$

情况二：若不存在 $i_j \in \{i_1, i_2, \cdots, i_k\}$，使得 $x = \tau(i_j)$，即 $\tau^{-1}(x) \notin \{i_1, i_2, \cdots, i_k\}$，从而由轮换定义知，$\sigma(\tau^{-1}(x)) = \tau^{-1}(x)$。因此有：

$$\begin{aligned}\tau\sigma\tau^{-1}(x) &= \tau(\tau^{-1}(x)) && (\sigma(\tau^{-1}) = \tau^{-1}) \\ &= x && (\tau\tau^{-1} = (1)) \\ &= (\tau(i_1)\tau(i_2)\cdots\tau(i_k))(x) && (\text{轮换定义})\end{aligned}$$

□

再证原题：

证明: 只需证明：对任意置换 $\sigma, \tau \in S_n$，$\tau\sigma\tau^{-1}$ 与 σ 具有相同的轮换指数。

设 $\sigma = \sigma_1\sigma_2\cdots\sigma_t$ 是 σ 是不相交轮换的分解式。令 $\sigma_i' = \tau\sigma_i\tau^{-1}, i = 1, 2, \cdots, t$。由引理 17.3 知，对所有 $1 \leq i \leq t$，σ_i' 也是一个轮换，且长度与 σ_i 相同。同时，对任何两个

轮换 $\sigma_j = (i_{j_1} i_{j_2} \cdots i_{j_m})$ 和 $\sigma_k = (i_{k_1} i_{k_2} \cdots i_{k_r})$，$1 \le j < k \le t$，由引理 17.3 知，$\sigma'_j = (\tau(i_{j_1})\tau(i_{j_2})\cdots\tau(i_{j_m}))$，$\sigma'_k = (\tau(i_{k_1})\tau(i_{k_2})\cdots\tau(i_{k_r}))$。由于 τ 是一一映射且 σ_j, σ_k 不相交，所以 σ'_j 与 σ'_k 也不相交。而：

$$\begin{aligned}
\tau\sigma\tau^{-1} &= \tau\sigma_1\sigma_2\cdots\sigma_t\tau^{-1} && (\sigma = \sigma_1\sigma_2\cdots\sigma_t)\\
&= \tau\sigma_1\tau^{-1}\tau\sigma_2\tau^{-1}\cdots\tau\sigma_t\tau^{-1} && (\tau^{-1}\tau = 1)\\
&= \sigma'_1\sigma'_2\cdots\sigma'_t && (\sigma'_i = \tau\sigma_i\tau^{-1})
\end{aligned}$$

由上面的讨论和轮换指数的定义知，$\tau\sigma\tau^{-1}$ 与 σ 具有相同的轮换指数。 □

17.35 $\sigma = (12354)$，轮换指数为 5^1；$\tau = (15423)$，轮换指数也是 5^1。

17.36 见习题 17.14。

17.37 不是。因为共轭关系对群乘法一般不具有置换性质。以 S_3 为例，令 $\sigma_1 = \sigma_2 = \tau_1 = (12), \tau_2 = (13)$。显然，$\sigma_1$ 与 τ_1 共轭，σ_2 与 τ_2 共轭，但 $\sigma_1\tau_1 = (1)$，而 $\sigma_2\tau_2 = (123)$，不是共轭的。

17.38

(1) 由于循环群都是 Abel 群，所以 $\forall x \in G$，都有 $xax^{-1} = xx^{-1}a = a$。这就是说，$\forall x \in G, \overline{x} = \{x\}$。$G$ 的共轭类分别是：$\overline{e} = \{e\}$；$\overline{a} = \{a\}$；$\overline{a^2} = \{a^2\}$；$\overline{a^3} = \{a^3\}$。

(2) Klein 四元群也是 Abel 群，从而也有 $\forall x \in G, \overline{x} = \{x\}$，Klein 四元群的共轭类分别是：$\overline{e} = \{e\}$；$\overline{a} = \{a\}$；$\overline{b} = \{b\}$；$\overline{c} = \{c\}$。

17.39

证明: $\forall y \in G$，

$$\begin{aligned}
& y \in N(x^{-1}ax) && \\
\iff & yx^{-1}ax = x^{-1}axy && (N(x^{-1}ax) \text{ 定义})\\
\iff & yx^{-1}a = x^{-1}axyx^{-1} && (\text{右乘 } x^{-1})\\
\iff & xyx^{-1}a = axyx^{-1} && (\text{左乘 } x)\\
\iff & xyx^{-1} \in N(a) && (N(a) \text{ 定义})\\
\iff & y \in x^{-1}N(a)x && (x^{-1}N(a)x \text{ 定义})
\end{aligned}$$

□

17.40

证明: 由教材定理 17.30 可知，$|\overline{a}| = [G : N(a)]$，$|\overline{a^n}| = [G : N(a^n)]$。由教材定理 17.29 可知，$N(a) \leqslant G$，$N(a^n) \leqslant G$。下面若能证明 $N(a) \subseteq N(a^n)$，就可以证明 $N(a) \leqslant N(a^n) \leqslant G$，从而习题 17.32 结论得证：$|\overline{a^n}| = [G : N(a^n)] \mid [G : N(a^n)][N(a^n) : N(a)] = [G : N(a)] = |\overline{a}|$。

下面对 n 归纳，证明 $\forall n \in \mathbb{N}_+, N(a) \subseteq N(a^n)$。

当 $n = 1$ 时，命题显然成立。

设 $n = k(k \le 1)$ 时命题成立，则当 $n = k + 1$ 时，$\forall x \in N(a)$，

$$\begin{aligned}
xa^{k+1} &= xa^k a && (\text{幂运算定义})\\
&= a^k xa && (\text{归纳假设})\\
&= aa^k x && (xa = ax)\\
&= a^{k+1}x && (\text{幂运算定义})
\end{aligned}$$

从而有 $x \in N(a^{k+1})$。即有：$N(a) \subseteq N(a^{k+1})$。 □

17.41

证明: 由定义显然有 $C \leqslant N(a)$。由教材定理 17.30 和习题 17.32 结论有：$k = [G : N(a)] = [G : N(a)] \mid [G : N(a)][N(a) : C] = [G : C] = \dfrac{n}{c}$。 □

17.42

证明: 由于循环群是 Abel 群，而对于任何 Abel 群 G 及其子群 H，有：$\forall g \in G$，对任何 $x \in gH$，存在 $h \in H$，使 $x = gh$。由于 G 是 Abel 群，故有 $x = hg \in Hg$。从而有 $gH \subseteq Hg$。同理可证 $Hg \subseteq gH$。 □

17.43

证明: 习题 17.28 已经证明，对任意 $g = \left(\begin{smallmatrix} r & s \\ 0 & 1 \end{smallmatrix}\right) \in G$，$gH = \{\left(\begin{smallmatrix} r & t \\ 0 & 1 \end{smallmatrix}\right) \mid t \in \mathbb{Q}\}$。而对于 Hg，有 $Hg = \{\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} r & s \\ 0 & 1 \end{smallmatrix}\right) \mid t \in \mathbb{Q}\} = \{\left(\begin{smallmatrix} r & s+t \\ 0 & 1 \end{smallmatrix}\right) \mid t \in \mathbb{Q}\}$。因为 $s, t \in \mathbb{Q}$，故有 $s + t \in \mathbb{Q}$，因此有 $Hg = \{\left(\begin{smallmatrix} r & s+t \\ 0 & 1 \end{smallmatrix}\right) \mid t \in \mathbb{Q}\} \subseteq \{\left(\begin{smallmatrix} r & t \\ 0 & 1 \end{smallmatrix}\right) \mid t \in \mathbb{Q}\} = gH$。对任意 $\{\left(\begin{smallmatrix} r & t \\ 0 & 1 \end{smallmatrix}\right)\} \in gH$，令 $t' = t - s$，则有 $\{\left(\begin{smallmatrix} r & t \\ 0 & 1 \end{smallmatrix}\right)\} = \{\left(\begin{smallmatrix} r & s+t' \\ 0 & 1 \end{smallmatrix}\right)\} \in Hg$。从而有 $gH = Hg$。由 g 的任意性知，H 是正规子群。 □

17.44

证明: 由题设知，$K \subseteq H$，$N \subseteq H$，从而由 H 对群乘法的封闭性即有 $KN \subseteq H$。

由于 N 是 H 的正规子群，故对所有 $h \in H$，有 $hN = Nh$。从而有 $KN = NK$。由习题 17.16 结论知，KN 是 G 的子群。由生成子群的定义知，$H \subseteq KN$。

这就证明了 $H = KN$。 □

17.45

证明: 由于 $|N| = 2$ 和 $e \in N$，不妨记 $N = \{e, a\}$。

$e \in C$ 是显然的。由 $N \trianglelefteq G$ 和教材定理 17.32 知，$\forall g \in G$，有 $gNg^{-1} = N$，即 $\{geg^{-1}, gag^{-1}\} = \{a, e\}$。而对任意 $g \in G$，都有 $geg^{-1} = gg^{-1} = e$。所以有 $gag^{-1} = a$。即 $ga = ag$。因此有 $a \in C$。这就证明了 $N = \{e, a\} \subseteq C$。 □

17.46

(1)

证明: 对任意 $g \in G, h \in H$，由题设知，$|g| \neq 0, |h| > 0$。注意到，$|ghg^{-1}| = |g||h||g^{-1}| = |g||g^{-1}||h| = |g \cdot g^{-1}||h| = |h| > 0$，从而有 $ghg^{-1} \in H$。由教材定理 17.32 知，$H \trianglelefteq G$。 □

(2) 令 $a = \begin{pmatrix} -1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \hdotsfor{4} \\ 0 & 0 & \cdots & 1 \end{pmatrix}$，显然有 $|a| = -1$，$a^2 = E$。对所有 $h \in H$ 都有 $|ah| = -|h| < 0$，$ah \notin H$。这就是说，$aH \neq H$。

对任意 $g \in G$，若 $g \in H$，则 $gH = H$。反之，若 $g \notin H$，则有 $|g| < 0$，而 $g = a(ag)$，其中 $|ag| = -|g| > 0$，$ag \in H$。也就是说，$gH = aH$。

这就证明了，G 有且仅有 H 和 aH 这两个陪集，从而有 $[G : H] = 2$。

17.47

(1)

证明: 由矩阵乘法的性质知，$\forall a, b \in G_1, \varphi(ab) = |ab| = |a||b| = \varphi(a)\varphi(b)$。从而 φ 是 G_1 到 G_2 的同态。 □

(2) 对任意 $x \in \mathbb{Q}^*$，令 $A = \begin{pmatrix} x & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$，则有 $A \in M_n(\mathbb{Q}), x = \varphi(A) \in \varphi(G_1)$。从而有 $\varphi(G_1) = \mathbb{Q}^*$。

由 φ 定义知，$\ker \varphi = SL_n(\mathbb{Q}) = \{A \mid A \in M_n(\mathbb{Q}) \wedge |A| = 1\}$ 是 $\mathbb{Q}$ 上的特殊线性群。

17.48

证明: 设 $\varphi : \mathbb{Q} \to \mathbb{Z}$ 为 $\langle \mathbb{Q}, + \rangle$ 到 $\langle \mathbb{Z}, + \rangle$ 的任意同态映射。反设存在 $x \in \mathbb{Q}$，使得 $\varphi(x) = n \neq 0$。则令 $m = \varphi(\frac{x}{2n}) \in \mathbb{Z}$。从而有

$$\begin{aligned}
n &= \varphi(x) \\
&= \varphi(\underbrace{\frac{x}{2n} + \frac{x}{2n} + \cdots + \frac{x}{2n}}_{2n\text{ 个}}) && \text{(有理数性质)} \\
&= \underbrace{\varphi(\frac{x}{2n}) + \varphi(\frac{x}{2n}) + \cdots + \varphi(\frac{x}{2n})}_{2n\text{ 个}} && (\varphi\text{ 是同态}) \\
&= \underbrace{m + m + \cdots + m}_{2n\text{ 个}} && (\varphi(\frac{x}{2n}) = m) \\
&= 2nm && \text{(有理数性质)}
\end{aligned}$$

由上式和有理数上的乘法消去律可知，$2m = 1$，即 $m = \frac{1}{2}$。这与 $m = \varphi(\frac{x}{2n}) \in \mathbb{Z}$ 矛盾。 □

17.49

证明: 由教材定理 3.4 知，$\varphi_2 \circ \varphi_1 : G_1 \to G_3$ 是双射。对任意 $x, y \in G_1$，

$$\begin{aligned}
\varphi_2 \circ \varphi_1(xy) &= \varphi_2(\varphi_1(xy)) && \text{(教材定理 3.3)} \\
&= \varphi_2(\varphi_1(x)\varphi_1(y)) && (\varphi_1\text{ 是同态}) \\
&= \varphi_2(\varphi_1(x))\varphi_2(\varphi_1(y)) && (\varphi_2\text{ 是同态}) \\
&= \varphi_2 \circ \varphi_1(x)\varphi_2 \circ \varphi_1(y) && \text{(教材定理 3.3)}
\end{aligned}$$

从而 $\varphi_2 \circ \varphi_1 : G_1 \to G_3$ 是从 G_1 到 G_3 的同构。 □

17.50

证明: 由教材定理 3.9 知，$\varphi^{-1} : G_2 \to G_1$ 是双射。对任意 $x, y \in G_2$，

$$\begin{aligned}
\varphi^{-1}(xy) &= \varphi^{-1}(\varphi(\varphi^{-1}(x))\varphi(\varphi^{-1}(y))) && (\varphi \circ \varphi^{-1} = I_{G_2}) \\
&= \varphi^{-1}(\varphi(\varphi^{-1}(x)\varphi^{-1}(y))) && (\varphi\text{ 是同态}) \\
&= \varphi^{-1}(x)\varphi^{-1}(y) && (\varphi^{-1} \circ \varphi = I_{G_1})
\end{aligned}$$

从而 $\varphi : G_2 \to G_1$ 是从 G_2 到 G_1 的同构。 □

17.51

(1)

证明: 由于 H 为群，所以有 $e_1 \in \varphi^{-1}(e_2) \subseteq \varphi^{-1}(H)$，从而 $\varphi^{-1}(H)$ 非空。

对任意 $a, b \in \varphi^{-1}(H)$，由定义知，$\varphi(a), \varphi(b) \in H$，从而有 $\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} \in H$，所以有 $ab^{-1} \in \varphi^{-1}(H)$。

由子群判定定理二知，$\varphi^{-1}(H) \leqslant G_1$。 □

(2)

证明: 由第 (1) 小题已知 $\varphi^{-1}(H)$ 为群。对任意 $g \in G_1, h \in \varphi^{-1}(H)$，$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) \in H$，所以有 $ghg^{-1} \in \varphi^{-1}(H)$。由教材定理 17.32 知，$\varphi^{-1}(H) \trianglelefteq G_1$。 □

17.52

证明: 必要性。设 φ 是同态，则有 $b^{km} = \varphi(a^m) = \varphi(e_1) = e_2$。由教材定理 17.8(1) 知，$n \mid mk$。

充分性。首先证明，当 $n \mid mk$ 时，φ 是函数。

$$\begin{aligned}
& forall s,t \in \mathbb{Z}, && \\
& a^s = a^t && \\
\Longleftrightarrow\ & a^{s-t} = e_1 && \text{(消去律)} \\
\Longleftrightarrow\ & m \mid s-t && \text{(教材定理 17.8(1))} \\
\Longrightarrow\ & mk \mid ks-kt && \text{(两边乘 } k\text{)} \\
\Longrightarrow\ & n \mid ks-kt && (n \mid mk) \\
\Longleftrightarrow\ & b^{ks-kt} = e_2 && \text{(教材定理 17.8(1))} \\
\Longleftrightarrow\ & b^{ks} = b^{kt} && \text{(两边乘 } b^{kt}\text{)} \\
\Longleftrightarrow\ & \varphi(a^s) = \varphi(a^t) && (\varphi\ \text{定义})
\end{aligned}$$

这就证明了 φ 是函数。而对任意 $a^s, a^t \in G_1$，$\varphi(a^s a^t) = \varphi(a^{s+t}) = b^{k(s+t)} = b^{ks}b^{kt} = \varphi(a^s)\varphi(a^t)$，所以 φ 是同态。 □

17.53 先证一个引理。

引理 17.4 设 φ 是群 G_1 到 G_2 的同态映射，H 是 G_1 的子群。则有

$$|\varphi(H)| \,\big|\, (|G_2|, |H|).$$

证明: 由教材定理 17.35(1) 知，$\varphi(H) \leqslant G_2$。从而由 Lagrange 定理知，$|\varphi(H)| \,\big|\, G_2$。

考虑 $\varphi \restriction H : H \to \varphi(H)$，显然，$\varphi \restriction H$ 也是同态，且为满同态。由群同态基本定理知，$H/\ker(\varphi \restriction H) \cong \varphi(H)$。从而 $|\varphi(H)| = |H/(\ker\varphi \restriction H)| = [H : \ker\varphi] \,\big|\, |H|$。所以有 $|\varphi(H)| \,\big|\, (|H|, |G_2|)$。 □

再证原题。

证明: 由题设和引理 17.4 知，$|\varphi(H)| \,\big|\, (|H|, |G_2|) = 1$，即有 $\varphi(H) = \{e_2\}$。由同态核的定义即有 $H \subseteq \ker\varphi$。 □

17.54

证明: 作自然映射 $\varphi : G \to G/N$，$\forall g \in G$，$\varphi(g) = Ng$。

由引理 17.4 知，$|\varphi(H)| \,\big|\, (|H|, |G/N|) = (|H|, [G : N]) = 1$，$\varphi(H) = \{N\}$。这就是说，$\forall h \in H$，$\varphi(h) = hN = N$，即有 $h \in N, \forall h \in H$。

这就证明了 $H \subseteq N$。 □

17.55 先证一个引理。

引理 17.5 设 φ 是群 G_1 到 G_2 的同态映射，H 是 G_1 的子群，且 $\ker\varphi \subseteq H$。则对任意 $a \in G_1$ 有

$$a \in H \Leftrightarrow \varphi(a) \in \varphi(H).$$

证明: 由定义立即有 $a \in H \Rightarrow \varphi(a) \in \varphi(H)$。

下面证明 $\varphi(a) \in \varphi(H) \Rightarrow a \in H$。

$\varphi(a) \in \varphi(H)$

$$
\begin{aligned}
&\iff \exists b(b \in H \wedge \varphi(a) = \varphi(b)) && (\varphi(H)\ \text{定义})\\
&\iff \exists b(b \in H \wedge a \ker \varphi = b \ker \varphi) && (\text{教材定理 17.36(2)})\\
&\iff \exists b(b \in H \wedge a \in b \ker \varphi) && (\text{教材定理 17.22})\\
&\implies \exists b(b \in H \wedge a \in bH) && (\ker \varphi \subseteq H)\\
&\iff \exists b(b \in H \wedge a \in H) && (b \in H)\\
&\implies a \in H && (\exists\text{消去、命题逻辑化简律})
\end{aligned}
$$

综合得，$a \in H \Leftrightarrow \varphi(a) \in \varphi(H)$。 □

再证原题。

证明: 教材例 17.45 保证了 $G_2/\varphi(N)$ 的合法性。作 G_2 上的自然映射 $f : G_2 \to G_2/\varphi(N)$，$\forall a \in G_2$，$f(a) = \varphi(N)a$。

令 $g = f \circ \varphi : G_1 \to G_2/\varphi(N)$。则 g 是同态，且为满射(因为 φ 和 f 都是满射)。

考虑 $\ker g$，$\forall a \in G_1$，

$$
\begin{aligned}
& a \in \ker g\\
&\iff g(a) = \varphi(N) && (\ker g\ \text{定义})\\
&\iff f(\varphi(a)) = \varphi(N) && (g = f \circ \varphi)\\
&\iff \varphi(a) \in \varphi(N) && (f\ \text{定义})\\
&\iff a \in N && (\text{引理 17.5})
\end{aligned}
$$

从而证明了 $\ker g = N$。由群同态基本定理知，$G_1/N \cong G_2/\varphi(N)$。 □

17.56

证明: 首先，证明 $HK \trianglelefteq G$。对任意 $x \in HK, g \in G$，由定义知，存在 $h \in H, k \in K$，使得 $x = hk$。从而 $gxg^{-1} = ghkg^{-1} = gh(g^{-1}g)kg^{-1} = (ghg^{-1})(gkg^{-1})$，由于 $H, K \trianglelefteq G$，所以 $ghg^{-1} \in H, gkg^{-1} \in K$，从而 $gxg^{-1} = (ghg^{-1})(gkg^{-1}) \in HK$。这就证明了 $HK \trianglelefteq G$，由教材例 17.46(1) 知，$H \trianglelefteq HK$。再由教材例 17.47 结论即证原题。 □

17.57 先证明如下引理。

引理 17.6 *设 G 为群，C 是 G 的中心。若存在 $H \leqslant C$，则:*

(1) $H \trianglelefteq G$;

(2) 若 G/H 为循环群，则 G 是 Abel 群。

证明: (1) 对任意 $g \in G, h \in H$，由于 $h \in H \subseteq C$，所以有 $ghg^{-1} = hgg^{-1} = h \in H$，由教材定理 17.32 知，$H \trianglelefteq G$。

(2) 由于 G/H 是循环群，所以存在 $a \in G$，使得 $G/H = \langle Ha \rangle$。对任意 $x, y \in G$，必有 $m, n \in \mathbb{Z}$，使 $x \in Ha^m, y \in Ha^n$。即，存在 $h_1, h_2 \in H$，使 $x = h_1a^m, y = h_2a^n$。从而有:

$$
\begin{aligned}
xy &= h_1a^mh_2a^n && (x = h_1a^m, y = h_2a^n)\\
&= h_2h_1a^ma^n && (h_2 \in C)\\
&= h_2h_1a^na^m && (a^ma^n = a^{m+n} = a^na^m)\\
&= h_2a^nh_1a^m && (h_1 \in C)\\
&= yx
\end{aligned}
$$

这就证明了 G 是 Abel 群。 □

再证原题。

证明: 只需证 $G=C$。

由于 $C\trianglelefteq G$，所以有 $|C|\mid|G|=p^2$。即，C 的取值只能是 1，p 或 p^2。

由群的分类方程知：

$$|C|=|G|-\sum_{i=1}^{k}[G:N(a_i)]$$

其中 $a_i(i=1,2,\cdots,k)$ 是含有至少两个元素的共轭类的代表元。由于 $2\leq[G:N(a_i)]\mid p^2$ 且 $[G:N(a_i)]<p^2$，所以必有 $[G:N(a_i)]=p$，$i=1,2,\cdots,k$。从而有：

$$|C|=p^2-kp=(p-k)p$$

这就证明了 $|C|\neq 1$。

$|C|$也不可能为 p。因为若 $|C|=p$，就有 $|G/C|=p$，从而 G/C 是循环群。由引理 17.6 知，G 是 Abel 群，$C=G$ 是 p^2 阶群，矛盾。

因此，只能有 $|C|=p^2$。从而 $G=C$ 是 Abel 群。 □

17.58 先证明如下引理。

引理 17.7 *设 G 是循环群，H 是 G 的任意子群，则 G/H 是循环群。*

证明: 由于循环群都是交换的，所以 H 必是正规的。由教材定理 15.11 自然映射是从 G 到 G/H 的满同态。由 G 是循环群和教材定理 17.34 可知，G/H 也是循环群。 □

再证原题。

证明: 由教材例 17.38 知，G 中存在 p 阶元 a 和 q 阶元 b。由教材例 17.6 知，$|ab|=|a||b|=pq$。从而 $G=\langle ab\rangle$ 是循环群。再由引理 17.7 知，G/H 也是循环群。 □

17.59

证明: 设 $G=\{e,a,b,c\}$为 Klein 群，$G'=\{(1),(12)(34),(13)(24),(14)(23)\}\subseteq S_4$。令 $\varphi:G\to G',\varphi(e)=(1),\varphi(a)=(12)(34),\varphi(b)=(13)(24),\varphi(c)=(14)(23)$。易于验证，$\varphi$ 是同构。由于 G 是群，所以 $G'\cong G$ 也是群。

注意到，G' 是 S_4 中的恒等置换和所有轮换指数为 2^2 的置换构成的集合。由习题 17.34 结论知，S_n 中同一共轭类的元素都具有相同的轮换指数，所以对任意$\sigma\in S_4,\tau\in G'$，$\sigma\tau\sigma^{-1}$ 的轮换指数只能是 1 或 2^2。无论对于哪种情况，都有 $\sigma\tau\sigma^{-1}\in G'$。由教材定理 17.32 知，$G'\trianglelefteq S_4$。□

17.60

证明: 由习题 17.23 结论知，G 必为有限群。记 $|G|=n$，由于 φ 是满自同态，故 $\varphi(G)=G$。由群同态基本定理知，$G/\ker\varphi\cong G$。从而由 Lagrange 定理知

$$|\ker\varphi|=\frac{|G|}{[G:\ker\varphi]}=\frac{|G|}{|G|}=1$$

于是有 $\ker\varphi=\{e\}$。从而由教材定理 17.33 知，φ 是单同态，从而是同构。 □

17.61

证明: 充分性。

由群中逆元的唯一存在性和等式 $(x^{-1})^{-1}=x$ 可知，φ 是双射。对任意 $a,b\in G$，

$$\begin{aligned}
\varphi(ab)&=(ab)^{-1} && (\varphi\text{ 定义})\\
&=b^{-1}a^{-1} && (\text{教材定理 17.2(2)})\\
&=a^{-1}b^{-1} && (G\text{ 是交换群})\\
&=\varphi(a)\varphi(b) && (\varphi\text{ 定义})
\end{aligned}$$

这就证明了 φ 是自同态，从而是自同构。

必要性。

若 φ 是自同构，则对任意 $a, b \in G$，

$$\begin{aligned}
ab &= ((ab)^{-1})^{-1} && (\text{教材定理 17.2(1)})\\
&= \varphi((ab)^{-1}) && (\varphi\ \text{定义})\\
&= \varphi(b^{-1}a^{-1}) && (\text{教材定理 17.2(2)})\\
&= \varphi(b^{-1})\varphi(a^{-1}) && (\varphi\ \text{是同构})\\
&= (b^{-1})^{-1}(a^{-1})^{-1} && (\varphi\ \text{定义})\\
&= ba && (\text{教材定理 17.2(1)})
\end{aligned}$$

这就证明了 G 是交换群。 □

17.62

(1)

证明： 由于对任意正整数 n, t 都有 $n \mid nt$。由习题 17.52 知，φ 是自同态。 □

(2)

证明： 充分性。若 $(n, t) = 1$，则存在 $p, q \in \mathbb{Z}$，使 $pn + qt = 1$。从而对任意 $a^i \in G$，有 $a^i = a^{i-ipn} == a^{iqt} = \varphi(a^{iq}) \in \varphi(G)$。从而 φ 是满自同态。再由习题 17.60 结论知，φ 是自同构。

必要性。若 φ 是自同构，则必是满射。因而，存在 $q \in \mathbb{Z}$，使得 $\varphi(a^q) = a^{qt} = a$，即，$qt - 1 \mid n$。从而必有 $k \in \mathbb{Z}$，使得 $qt - 1 = kn$，取 $p = -k \in \mathbb{Z}$，就有 $pn + qt = 1$。从而有 $(n, t) = 1$。 □

17.63

证明： 定义 $f : G \to \operatorname{Inn} G$，$\forall g \in G$，$f(g) = \varphi_g$。显然 f 是函数且为满射。下面证明 f 是同态。

对任意 $x, y, a \in G$，

$$\begin{aligned}
\varphi_{xy}(a) &= xya(xy)^{-1} && (\varphi_{xy}\ \text{定义})\\
&= xyay^{-1}x^{-1} && (\text{教材定理 17.2(2)})\\
&= \varphi_x(yay^{-1}) && (\varphi_x\ \text{定义})\\
&= \varphi_x(\varphi_y(a)) && (\varphi_y\ \text{定义})\\
&= \varphi_x \circ \varphi_y(a) && (\text{教材定理 3.3})
\end{aligned}$$

这就证明了 f 是同态。

下面证明 $\ker f = C$。

$\forall g \in G$,

$$\begin{aligned}
& g \in C\\
\iff & \forall a(a \in G \to ga = ag) && (C\ \text{定义})\\
\iff & \forall a(a \in G \to gag^{-1} = a) && (\text{右乘}\ g^{-1})\\
\iff & \forall a(a \in G \to \varphi_g(a) = a) && (\varphi\ \text{定义})\\
\iff & \varphi_g = I_G && (I_G\ \text{定义})\\
\iff & g \in \ker f && (\ker f\ \text{定义})
\end{aligned}$$

这就证明了 $\ker f = C$。由群同态基本定理就有，$G/C \cong \operatorname{Inn} G$。 □

17.64

证明: 对任意 10 阶群 G，分两种情况讨论：

(1) 若 G 是 Abel 群，则由教材例 17.38 知，G 中存在 2 阶元 a 和 5 阶元 b。由教材例 17.6 知，$|ab| = |a||b| = 10$。从而 $G = \langle ab\rangle \cong \mathbb{Z}_{10}$ 是循环群(易证，任何无限阶循环群都同构于整数加群，任何 n 阶循环群都同构于模 n 加群。所以 n 阶循环群在同构意义下是唯一的)。

(2) 若 G 不是 Abel 群，则存在 5 阶元。这是因为：若不然，则 G 中所有非单位元都是 2 阶元，即，对任意 $x, y \in G$，有

$$\begin{aligned} &(xy)^2 = e = x^2y^2 && (x, y, xy \text{ 都是 2 阶或 1 阶元}) \\ \Longrightarrow\ & xyxy = xxyy && ((xy)^2 = x^2y^2) \\ \Longleftrightarrow\ & yx = xy && (\text{消去律}) \end{aligned}$$

所以 G 是 Abel 群，与前提矛盾。

设 $a \in G$ 是一个 5 阶元，记 $\langle a\rangle = A$。下面证明，除 $a^i(i = 1, 2, 3, 4)$ 外，G 中再无其它 5 阶元。

若不然，设 $b \notin A$ 也是一个 5 阶元，则 $B = \langle b\rangle$ 也是 G 的一个 5 阶子群。令 $H = A \cap B$，则 $H \leqslant A$。由 Lagrange 定理知，$|H| \mid 5$。因为 $a \neq b$，所以 $|H|$ 不可能等于 5，于是必有 $|H| = 1$。由习题 17.33(1) 知，

$$|AB| = \frac{|A||B|}{|A \cap B|} = 25 > 10$$

这与 $AB \subseteq G$ 矛盾。

这就是说，$G - A$ 中所有的元素只能是 2 阶元。

任取一个 2 阶元 b (显然有 $b \notin A$)，则 $G = A \cup Ab$ 是 G 的陪集分解。这就是说，$G = \{e, a, a^2, a^3, a^4, ab, a^2b, a^3b, a^4b\}$。

下面来讨论它们之间的运算规律。注意到，对任意 a^i，$i = 1, 2, 3, 4$，都应有 $(a^ib)^2 = e$。从而有 $a^iba^ib = e$，即 $ba^ib = (a^i)^{-1} = a^{5-i}$。

有了这个公式，就确定了 G 的运算表：G 中每一个元素都可以表示成 a^ib^j 的形式，其中 $i = 0, 1, 2, 3, 4$，$j = 0, 1$。对任意 $a^ib^j, a^kb^r \in G$，可运用上述等式将 $a^ib^ja^kb^r$ 化成 a^sb^t 的形式(反复使用 $ba^ib = (a^i)^{-1} = a^{5-i}$，直至 b^j 一项被消去。若 $r < j$，可以利用 $a^ib^ja^kb^r = a^ib^ja^kb^re^n = a^ib^ja^kb^{r+2n}$，加大 r)。

上述讨论说明，任何非交换的 10 阶群都可以表示成 $G = \{a^ib^j \mid i \in \mathbb{Z}_5, j \in \mathbb{Z}_2\}$ 的形式，且 $|a| = 5, |b| = 2, ba^ib = a^{5-i}$。这就证明了在同构意义下，仅有上述一种形式的 10 阶非交换群。

综上所述，在同构意义下，10 阶群只有两个，一个是 10 阶循环群 $\mathbb{Z}_{10}$，另一个是二面体群 D_5。[3] □

17.65 由习题 17.63 结论知，$|\mathrm{Inn}\, G| = 1$ 当且仅当 $[G : C] = |G/C| = 1$，即有 $C = G$。换言之，$\mathrm{Inn}\, G = \{I_G\}$ 当且仅当 G 为 Abel 群。

17.66

证明: 定义 $\varphi : G_1 \times G_2 \to G_2 \times G_1$，对任意 $\langle g_1, g_2\rangle \in G_1 \times G_2$，令 $\varphi(\langle g_1, g_2\rangle) = \langle g_2, g_1\rangle$。$\varphi$ 显然是双射。由积代数定义易于验证 φ 是同态。从而有 $G_1 \times G_2 \cong G_2 \times G_1$。 □

17.67

---

[3] 正 n 边形的对称群称为**二面体群**(dihedral group)，记作 D_n。它具有结构：$G = \langle \sigma, \tau \mid \sigma^n = \tau^2 = I, \quad \tau\sigma\tau = \sigma^{-1}\rangle$。

证明： 由于 $e_1 \in H_1, e_2 \in H_2$，所以 $\langle e_1, e_2\rangle \in H_1 \times H_2$，$H_1 \times H_2$ 非空。

对任意 $\langle a,b\rangle, \langle c,d\rangle \in H_1 \times H_2$，

$$\begin{aligned}
\langle a,b\rangle\langle c,d\rangle^{-1} &= \langle a,b\rangle\langle c^{-1}, d^{-1}\rangle && \text{(教材定理 15.6(5))}\\
&= \langle ac^{-1}, bd^{-1}\rangle && \text{(积代数定义)}\\
&\in H_1 \times H_2 && (a,c \in H_1,\ b,d \in H_2)
\end{aligned}$$

由子群判定定理二知，$H_1 \times H_2 \leqslant G_1 \times G_2$。 □

17.68

证明： 令 $\varphi : G \to G/H \times G/K$，$\forall g \in G$，$\varphi(g) = \langle Hg, Kg\rangle$。$\varphi$ 显然是函数，且为同态。下面证明 φ 是单射。

对任意 $a, b \in G$，

$$\begin{aligned}
&\varphi(a) = \varphi(b)\\
\iff& \langle Ha, Ka\rangle = \langle Hb, Kb\rangle && (\varphi \text{ 定义})\\
\iff& Ha = Hb \wedge Ka = Kb && \text{(教材定理 2.1)}\\
\iff& ab^{-1} \in H \wedge ab^{-1} \in K && \text{(教材定理 17.22)}\\
\iff& ab^{-1} \in H \cap K && \text{(集合交定义)}\\
\iff& ab^{-1} = e && (H \cap K = \{e\})\\
\iff& a = b && (\text{右乘 } b)
\end{aligned}$$

因此 φ 是 G 到 $\varphi(G)$ 的双射，从而是同构。

由于 G 是群，所以 $\varphi(G) \cong G$ 也是群，且为 $G/H \times G/K$ 的子群。 □

17.69 作 $\varphi_1 : G_1 \times G_2 \to G_1$，$\forall\langle g_1, g_2\rangle \in G_1 \times G_2$，$\varphi_1(\langle g_1, g_2\rangle) = g_1$；$\varphi_2 : G_1 \times G_2 \to G_2$，$\forall\langle g_1, g_2\rangle \in G_1 \times G_2$，$\varphi_2(\langle g_1, g_2\rangle) = g_2$。

φ_1 和 φ_2 显然是同态，且为满同态。取 $N_1 = \ker\varphi_1 = \{\langle e_1, g_2\rangle \mid g_2 \in G_2\}, N_2 = \ker\varphi_2 = \{\langle g_1, e_2\rangle \mid g_1 \in G_1\}$，由群同态基本定理知，$G_1 \times G_2 \big/ N_1$ 和 $G_1 \times G_2 \big/ N_2$ 满足题目要求。

第十八章　环与域

18.1

证明: $\forall a_1, a_2, b_1, b_2 \in A$，

$$\begin{aligned}
&(a_1 * b_1) \circ (a_1 * b_2) \circ (a_2 * b_1) \circ (a_2 * b_2) \\
=&((a_1 * b_1) \circ (a_1 * b_2)) \circ ((a_2 * b_1) \circ (a_2 * b_2)) && (\circ\text{ 可结合}) \\
=&(a_1 * (b_1 \circ b_2)) \circ (a_2 * (b_1 \circ b_2)) && (*\text{ 对 }\circ\text{ 可分配}) \\
=&(a_1 \circ a_2) * (b_1 \circ b_2) && (*\text{ 对 }\circ\text{ 可分配}) \\
=&((a_1 \circ a_2) * b_1) \circ ((a_1 \circ a_2) * b_2) && (*\text{ 对 }\circ\text{ 可分配}) \\
=&((a_1 * b_1) \circ (a_2 * b_1)) \circ ((a_1 * b_2) \circ (a_2 * b_2)) && (*\text{ 对 }\circ\text{ 可分配}) \\
=&(a_1 * b_1) \circ (a_2 * b_1) \circ (a_1 * b_2) \circ (a_2 * b_2) && (\circ\text{ 可结合})
\end{aligned}$$

□

18.2

证明: $\langle \mathbb{Z}[i], + \rangle$ 显然构成一个 Abel 群，其中 $0 = 0 + 0i$ 是加法单位元，对任意 $a + bi \in \mathbb{Z}[i]$，$(-a) + (-b)i \in \mathbb{Z}[i]$ 是加法逆元。

对任意 $a + bi, c + di \in \mathbb{Z}[i]$，$(a + bi)(c + di) = (ac - bd) + (ad + bc)i \in \mathbb{Z}[i]$，从而 $\langle \mathbb{Z}[i], \cdot \rangle$ 构成代数系统。由复数乘法的结合律知，$\langle \mathbb{Z}[i], \cdot \rangle$ 是半群。

最后，由复数运算规律知，复数乘法对复数加法满足分配律。

从而 $\langle \mathbb{Z}[i], +, \cdot \rangle$ 是环。 □

18.3

证明: $\oplus$ 和 $\cap$ 显然都是 $\mathcal{P}(B)$ 上的二元运算。

由教材例 1.7 知，$\oplus$ 满足结合律、交换律，对 $\cap$ 可分配，$\varnothing$ 为加法单位元，所有元素都是自身的负元。

由教材中给出的“集合恒等式”知，$\cap$ 满足结合律和交换律。

从而 $\langle \mathcal{P}(B), \oplus, \cap \rangle$ 是一个可交换环。 □

18.4

证明: $*$ 和 $\circ$ 显然都是 $\mathbb{Z}$ 上的二元运算。

对任意 $a, b, c \in \mathbb{Z}$，

$$\begin{aligned}
(a * b) * c &= (a + b - 1) + c - 1 && (*\text{ 运算定义}) \\
&= a + (b + c - 1) - 1 && (\text{加法交换律、结合律}) \\
&= a * (b * c) && (*\text{ 运算定义}) \\
(a \circ b) \circ c &= (a + b - ab) + c - (a + b - ab)c && (\circ\text{ 运算定义})
\end{aligned}$$

$$\begin{aligned}
&= a+b-ab+c-ac-bc+abc && \text{(乘法分配律)}\\
&= a+b+c-bc-ab-ac+abc && \text{(加法交换律、结合律)}\\
&= a+(b+c-bc)-a(b+c-bc) && \text{(乘法分配律)}\\
&= a\circ(b\circ c) && \text{($\circ$ 运算定义)}\\
a\circ(b*c) &= a\circ(b+c-1) && \text{($*$ 运算定义)}\\
&= a+(b+c-1)-a(b+c-1) && \text{($\circ$ 运算定义)}\\
&= a+b+c-1-ab-ac+a && \text{(乘法分配律)}\\
&= a+b-ab+a+c-ac-1 && \text{(加法交换律)}\\
&= (a+b-ab)*(a+c-ac) && \text{($*$ 运算定义)}\\
&= (a\circ b)*(a\circ c) && \text{($\circ$ 运算定义)}\\
(b*c)\circ a &= (b+c-1)\circ a && \text{($*$ 运算定义)}\\
&= (b+c-1)+a-(b+c-1)a && \text{($\circ$ 运算定义)}\\
&= b+c-1+a-ba-ca+a && \text{(乘法分配律)}\\
&= b+a-ba+c+a-ca-1 && \text{(加法交换律)}\\
&= (b+a-ba)*(c+a-ca) && \text{($*$ 运算定义)}\\
&= (b\circ a)*(c\circ a) && \text{($\circ$ 运算定义)}
\end{aligned}$$

从而两个运算都是可结合的，且 $\circ$ 对 $*$ 是可分配的。

易于验证，1 是 $*$ 运算的单位元，0 是 $\circ$ 运算的单位元。

对任意 $a\in\mathbb{Z}$ 有 $2-a\in\mathbb{Z}$，且 $a*(2-a)=1$，从而 $\mathbb{Z}$ 中任意元素对 $*$ 运算都是可逆的。

$*$ 运算显然是交换的。

从而 $\langle\mathbb{Z},*,\circ\rangle$ 是一个含幺环。 □

18.5 首先证明对任意 $a\in R$，有 $-a=a$。

证明: $\forall a\in R$，

$$\begin{aligned}
-a &= (-a)^2 && \text{(题设)}\\
&= a^2 && \text{(教材定理 18.1(3))}\\
&= a && \text{(题设)}
\end{aligned}$$

□

(1)

证明: 对任何 $a,b\in R$，

$$\begin{aligned}
a+b &= (a+b)^2 && \text{(题设)}\\
&= a^2+ab+ba+b^2 && \text{(分配律)}\\
&= a+ab+ba+b && \text{(题设)}
\end{aligned}$$

从而由消去律知，$ab+ba=0$。即，$ab=-ba$。又由于 $-ba=ba$，所以 $ab=-ba=ba$。 □

(2)

证明: 由于 $\forall a\in R$ 有 $-a=a$，所以 $a+a=a+(-a)=0$。 □

(3)

证明: 由于 $|R| > 2$，任取两个互异的非零元 $a, b \in R - \{0\}$，$a \neq b$，有

$$\begin{aligned}
&ab + ab = 0 && \text{(第 (2) 小题结论)}\\
\Longleftrightarrow\ &a^2b + ab^2 = 0 && (a^2 = a, b^2 = b)\\
\Longleftrightarrow\ &a(ab + b^2) = 0 && \text{(分配律)}\\
\Longleftrightarrow\ &a(a + b)b = 0 && \text{(分配律)}
\end{aligned}$$

由于 $a + b = a - b \neq 0$，所以：若 $a(a + b) = 0$，则 a 为左零因子，$a + b$ 为右零因子。若 $a(a + b) \neq 0$，则 $a(a + b)$ 为左零因子，b 为右零因子。从而 R 中总有零因子，因而不是整环。 □

18.6

(1) 由教材定理 15.6 即可得证。

(2) 由教材定理 15.6 即可得证。

(3) 不一定。取 $R_1 = R_2 = \langle \mathbb{Z}_2, \oplus, \otimes \rangle$，其中 $\oplus$ 和 $\otimes$ 分别是模 2 加法和模 2 乘法。易于验证，它们是整环。但它们的积代数 $\langle \mathbb{Z}_2 \times \mathbb{Z}_2, \overline{\oplus}, \overline{\otimes} \rangle$ 不是整环，因为 $\langle 0, 1 \rangle, \langle 1, 0 \rangle \in \mathbb{Z}_2 \times \mathbb{Z}_2$ 是非零元，但 $\langle 0, 1 \rangle \overline{\otimes} \langle 1, 0 \rangle = \langle 0, 0 \rangle$。

18.7

(1) 由于 n 不是素数，所以存在正整数 $1 < p, q < n$，使得 $pq = n$。从而 $p \otimes q = q \otimes p = pq \bmod n = 0$，是零因子。

(2)

证明: 令 k 为最小的使 $k \otimes r = 0$ 的正整数，其中 $\otimes$ 为模 n 乘法。显然，$kr = [r, n]$，其中 $[r, n]$ 是 r 和 n 的最小公倍数。从而 $k = \dfrac{[r, n]}{r} = \dfrac{rn}{r \cdot (r, n)} = \dfrac{n}{(r, n)}$。

当 $(r, n) = 1$ 时，$k = n \notin \mathbb{Z}_n$，从而 r 不是右零因子，由乘法交换律知，r 也不是左零因子，从而不是零因子。当 $(r, n) > 1$ 时，$0 < k < n$，$k \in \mathbb{Z}_n$，从而 r 是零因子。 □

(3) $2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16$。

18.8

证明: 对任何 $b \in R$，若有 $ab = 0$，则有 $b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$，从而 a 不是左零因子。同理可证 a 不是右零因子。从而 a 不是零因子。 □

18.9 先证明第 11 小题结论：

引理 18.1 有限整环必是域。[1]

证明: 设 $\langle R, +, \cdot \rangle$ 是有限整环。令 $R^* = R - \{0\}$。

对任意 $a, b \in R^*$，由 R^* 定义有 $a \neq 0$，$b \neq 0$。因为 R 是整环，所以 $ab \neq 0$，从而有 $ab \in R^*$。这就是说，$\cdot$ 是 R^* 上的二元运算，从而 $\langle R^*, \cdot \rangle$ 是有限的代数系统。

由于 $\cdot$ 在 R 上是交换的、结合的，所以 $\cdot$ 在 R^* 也是交换的、结合的。

由于 $1 \in R$ 且 $1 \neq 0$，所以 $1 \in R^*$。

对任何 $a \in R^*$，取 $\varphi_a : R^* \to R^*$，$\forall x \in R^*$，$\varphi_a(x) = ax$。由于 $\cdot$ 在 R 中适合消去律，因此对任何 $x, y \in R^*$，$\varphi_a(x) = \varphi_a(y) \Leftrightarrow x = y$，从而 φ_a 是单射。这就是说，φ_a 是从 R^* 到 $\varphi_a(R^*)$ 的双射。换言之，R^* 与 $\varphi_a(R^*)$ 等势。

由教材定理 5.5 推论 1 知，$\varphi_a(R^*) \not\subset R^*$，但由 $\cdot$ 对 R^* 的封闭性显然有 $\varphi_a(R^*) \subseteq R^*$。从而就有 $\varphi_a(R^*) = R^*$。

因此，对任意 $a \in R^*$ 都有 $1 \in R^* = aR^*$，即存在 $b \in R^*$，使得 $1 = ba = ab \in aR^*$，从而 a

---

[1] 这里按通常的定义，将“含幺”理解成“$1 \in R$ 且 $1 \neq 0$”。否则 1 阶的代数系统也是有限整环(但按教材定义，它不是域)，定理不成立。

是可逆的。由 a 的任意性知，R^* 中任意元素皆可逆。

这就证明了 $\langle R^*, \cdot\rangle$ 是 Abel 群，从而 $\langle R, +, \cdot\rangle$ 是域。 □

再证原题。

证明： 反设存在 pq 阶整环 R，则由引理 18.1 知，R 是域。这与教材定理 18.4 矛盾。 □

18.10

证明： 要证明 $\langle S, \cdot\rangle$ 是子半群，只须证明 S 对 $\cdot$ 运算的封闭性即可。

$\forall a, b \in S, c \in R$，

$$abc = 0 \iff bc = 0 \quad (a \text{ 不是零因子})$$

$$\iff c = 0 \quad (b \text{ 不是零因子})$$

这就证明了对任意 $a, b \in S$，ab 不是左零因子，同理可证 ab 不是右零因子，从而 $ab \in S$。□

$\langle S, +, \cdot\rangle$ 不一定是 $\langle R, +, \cdot\rangle$ 的子环。

反例：由习题 18.7 第 (3) 小题可知，若 $R = \mathbb{Z}_{18}$，则 $S = \{0, 1, 5, 7, 11, 13, 17\}$。然而 $1 + 1 = 2 \notin S$，S 对加法运算不封闭。从而 $\langle S, +, \cdot\rangle$ 不是子环。

“正例”：对任意无零因子环 R，(如 $\langle \mathbb{Z}, +, \cdot\rangle$)，显然有 $S = R$ 是 R 的子环。

18.11 即为引理 18.1。

18.12

证明： 由教材定理 18.3 知，n 是素数。

由二项式定理知，$(a+b)^n = \sum\limits_{i=0}^{n} C_n^i a^{n-i} b^i$。当 $0 < i < n$ 时，C_n^i 的分母中没有 n，而分子中有 n，从而由 n 是素数和 C_n^i 是整数知，$C_n^i = k_i n$，$k_i \in \mathbb{Z}$，$i = 1, 2, \cdots, n-1$。

而对任意 $a \in R, k_i \in \mathbb{Z}$，有 $kna = kn(1 \cdot a) = k(n \cdot 1)a = k(0 \cdot a) = 0$。从而

$$(a+b)^n = \sum_{i=0}^{n} C_n^i a^{n-i} b^i = a^n + b^n + \sum_{i=1}^{n-1} k_i n a^{n-i} b^i = a^n + b^n.$$

□

18.13

证明： 首先证明 $T \subseteq S$。由于 $|T| \geq 2$，所以存在非零元 $a \in T$，$a \neq 0$。对任意 $x \in T$，由于 T 是子环，所以有 $xa \in T$。从而 $x = (xa)a^{-1} \in S$。由 x 的任意性知，$T \subseteq S$。

其次证明 S 是子域。由于 $T \subseteq S$，S 非空，由子域定义和子群判定定理可知，要证 S 是子域，只需证明 $\forall x, y \in S$，有 $x - y \in S$ 和 $xy^{-1} \in S^*$ 即可。

对任意 $x, y \in S$，存在 $a_1, a_2, b_1, b_2 \in T$，b_1, b_2 不为零，使 $x = a_1 b_1^{-1}, y = a_2 b_2^{-1}$。从而：

$$x - y = a_1 b_1^{-1} - a_2 b_2^{-1} \quad (x = a_1 b_1^{-1}, y = a_2 b_2^{-1})$$

$$= a_1 b_2 b_2^{-1} b_1^{-1} - a_2 b_1 b_1^{-1} b_2^{-1} \quad (b_2 b_2^{-1} = b_1 b_1^{-1} = 1)$$

$$= (a_1 b_2 - a_2 b_1)(b_1 b_2)^{-1} \quad (\text{交换律、分配律})$$

因为 T 是子环，所以 $a_1 b_2 - a_2 b_1, b_1 b_2 \in T$，又因为 F 是域且 b_1 和 b_2 都是非零元，所以 $b_1 b_2 \neq 0$。从而有 $x - y = (a_1 b_2 - a_2 b_1)(b_1 b_2)^{-1} \in S$。

对任意 $x, y \in S^*$，存在 $a_1, a_2, b_1, b_2 \in T$，b_1, b_2 不为零，使 $x = a_1 b_1^{-1}, y = a_2 b_2^{-1}$。从而：

$$xy^{-1} = a_1 b_1^{-1} (a_2 b_2^{-1})^{-1} \quad (x = a_1 b_1^{-1}, y = a_2 b_2^{-1})$$

$$= a_1 b_1^{-1} b_2 a_2^{-1} \quad (\text{教材定理 17.2})$$

$$= a_1 b_2 b_1^{-1} a_2^{-1} \quad (\text{乘法交换律})$$

$$= a_1 b_2 (a_2 b_1)^{-1} \quad (\text{教材定理 17.2})$$

注意到，a_2, b_1 都是非零元(否则将与 $x, y \in S^*$ 矛盾)。从而由于 F 是域，有 $a_2 b_1 \neq 0$，而 $a_1 b_2, a_2 b_1 \in T$。所以有 $a_1 b_2 (a_2 b_1)^{-1} \in S$。同样由于 F 是域，所以有 $a_1 b_2 (a_2 b_1)^{-1} \neq 0$，从而 $a_1 b_2 (a_2 b_1)^{-1} \in S^*$。

这就证明了 S 是子域。

最后，设 S_1 是任意包含 T 的子域。则对所有 $a, b \in T \subseteq S_1, b \neq 0$，由于 $b \in S_1^*$，而 S_1^* 是群，所以 $b^{-1} \in S_1^* \subseteq S_1$，从而有 $ab^{-1} \in S_1$，由 a, b 的任意性知，$S \subseteq S_1$。 □

18.14

证明: 记这唯一的右单位元为 a，下面证明它也是左单位元，从而是乘法单位元。

反设 a 不是左单位元，则存在 $b \in R$，使得 $ab \neq b$。从而有 $a + ab - b \neq a$ (否则，由消去律就有 $ab - b = 0$，$ab = b$，矛盾)。记 $c = a + ab - b$，则对任意 $x \in R$，有：

$$\begin{aligned} xc &= x(a + ab - b) && (c = a + ab - b) \\ &= xa + xab - xb && (\text{分配律}) \\ &= x + xb - xb && (xa = x) \\ &= x && (xb - xb = 0) \end{aligned}$$

从而 $c \neq a$ 也是右单位元，与 a 是唯一的右单位元矛盾。这就证明了对所有的 $b \in R$，有 $ab = b$。所以 a 是 R 的左单位元，从而是单位元。 □

18.15

证明: (1) ⇒ (2)。反设 u 是可逆的，即，u 存在左逆元 a_l。则对 u 的任意右逆元 a_r、a_r'，有：

$$\begin{aligned} a_r &= a_l u a_r && (a_l u = 1) \\ &= a_l && (u a_r = 1) \\ &= a_l u a_r' && (u a_r' = 1) \\ &= a_r' && (a_l u = 1) \end{aligned}$$

从而 u 只有一个右逆元。矛盾。

(2) ⇒ (3)。由于 u 有右逆元 a_r，但 u 不可逆，所以 $a_r u \neq 1$，即有 $a_r u - 1 \neq 0$。同时，u 显然不等于 0 (否则就有 $u a_r = 0 a_r = 0 \neq 1$，矛盾)。但

$$\begin{aligned} u(a_r u - 1) &= u a_r u - u && (\text{分配律}) \\ &= u - u && (u a_r = 1) \\ &= 0 \end{aligned}$$

所以 u 是左零因子。

(3) ⇒ (1)。由于 u 是左零因子，所以存在 $b_r \neq 0$，使 $u b_r = 0$。设 a_r 是 u 的一个右逆元，则：

$$\begin{aligned} u(a_r + b_r) &= u a_r + u b_r && (\text{分配律}) \\ &= 1 && (u a_r = 1, u b_r = 0) \end{aligned}$$

从而 $a_r + b_r$ 也是 u 的一个右逆元。由于 $b_r \neq 0$，所以 $a_r + b_r \neq a_r$，从而 u 有多于一个右逆元。 □

18.16

证明: 设 $a \in R$ 是一个幂零元。令 k 为使 $a^k = 0$ 的最小正整数。若 $a \neq 0$，则必有 $k \geq 2$ (否则就有 $k = 1$，$a = a^1 = 0$，矛盾)。从而由 k 的最小性知，$a^1 \neq 0, a^{k-1} \neq 0$，而 $a^k = a^1 a^{k-1} = 0$，从而 a 和 a^{k-1} 是零因子。这与 R 是整环矛盾。 □

18.17 首先证明第 24 题结论：

引理 18.2 设 R 是交换环，D 是 R 的理想，令

$$N(D) = \{x \mid x \in R, \text{存在正整数 } n \text{ 使 } x^n \in D\},$$

则 $N(D)$ 是 R 的理想。

证明： 对任意 $x, y \in N(D)$，有 $m, n \in \mathbb{Z}^+$，使得 $x^m, y^n \in D$。由于 R 是交换环，所以

$$(x-y)^{m+n-1} = \sum_{i=0}^{m+n-1} C_{m+n-1}^{i} x^{m+n-1-i} y^{i} \tag{*}$$

(*) 式的前 n 项中，x 的指数均大于或等于 m。从而 $x^{m+n-1-i}y^i = x^m x^{n-1-i} y^i$。由于 $x^m \in D$，$x^{n-1-i}y^i \in R$，所以 $x^{m+n-1-i}y^i \in D$。(*) 式的其余 m 项中，y 的指数都大于或等于 n，从而 $x^{m+n-1-i}y^i = x^{m+n-1-i}y^{i-n}y^n$。由于 $x^{m+n-1-i}y^{i-n} \in R$，$y^n \in D$，所以 $x^{m+n-1-i}y^i \in D$。由 D 对加法的封闭性知，$(x-y)^{m+n-1} \in D$。从而 $x - y \in N(D)$。

对任意 $x \in N(D), y \in R(D)$，有 $m \in \mathbb{Z}^+$，使得 $x^m \in D$。由于 R 是交换环，所以 $(xy)^m = x^m y^m$。由于 $x^m \in D$，$y^m \in R$，所以 $(xy)^m \in D$。从而就有 $xy = yx \in N(D)$。

这就证明了 $N(D)$ 是理想。 □

再证原题。

证明： 由定义可知，$N(\{0\})$ 即为 R 中全体幂零元构成的集合。而 $\{0\}$ 是 R 的理想。由引理 18.2 可知，$N(\{0\})$ 是 R 的理想，从而自然是 R 的子环。 □

18.18

证明： 由定义可知，$N(\{0\})$ 即为 R 中全体幂零元构成的集合。而 $\{0\}$ 是 R 的理想。从而由引理 18.2 即证原题。 □

18.19

证明： 设 $A, B \subseteq R$ 是 R 的两个理想。

对任意 $x, y \in A \cap B$，有 $x - y \in A$ 和 $x - y \in B$，所以有 $x - y \in A \cap B$。

对任意 $r \in R, x \in A \cap B$，有 $rx, xr \in A$ 和 $rx, xr \in B$。所以有 $rx, xr \in A \cap B$。

从而 $A \cap B$ 也是 R 的理想。 □

18.20

(1)

证明： 对任意 $x, y \in A + B$，存在 $a_1, a_2 \in A, b_1, b_2 \in B$，使 $x = a_1 + b_1, y = a_2 + b_2$。从而 $x - y = a_1 + b_1 - a_2 + b_2 = (a_1 - a_2) + (b_1 - b_2) \in A + B$。

对任意 $r \in R, x \in A + B$，存在 $a \in A, b \in B$，使 $x = a + b$。从而 $rx = r(a + b) = ra + rb$。由于 A, B 是理想，所以 $ra \in A, rb \in B$。从而 $rx = ra + rb \in A + B$，所以有 $r(A + B) \subseteq A + B$。同理可证 $(A + B)r \subseteq A + B$。这就证明了 $A + B$ 是理想。 □

(2) 考虑实数域 $\mathbb{R}$ 和高斯整数环 $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$。由教材例 18.1 和例 18.5 知，他们都是环，且都是复数域 $\mathbb{C}$ 的子环。但 $\mathbb{R} + \mathbb{Z}[i] = \{x + ai \mid x \in \mathbb{R}, b \in \mathbb{Z}\}$ 对乘法不封闭。例如，$\sqrt{2} + i \in \mathbb{R} + \mathbb{Z}[i]$，但 $(\sqrt{2} + i)^2 = 1 + 2\sqrt{2}i \notin \mathbb{R} + \mathbb{Z}[i]$。从而 $\mathbb{R} + \mathbb{Z}[i]$ 不是子环。

18.21

证明： 为方便讨论，用 E_{ij} 表示第 i 行第 j 列为 1，其余各项皆为 0 的矩阵。用 xE_{ij} 表示第 i 行第 j 列为 x，其余各项都为 0 的矩阵，其中 $x \in F$ 是数域中的任意元素。

设 D 是 $M_n(F)$ 上的任意理想，下面证明，若 $D \neq \{(0)\}$，则 $D = M_n(F)$。

由于 D 不是零理想，所以存在 $A \in D$，且 A 中有非零项。不妨设 $a_{kt} \neq 0 (1 \leq k, t \leq n)$。注意到，对任意 $E_{ij}, i, j = 1, 2, \cdots n$，$x \in F$，有：

$$xE_{ij} = (xa_{kt}^{-1}E_{ik})AE_{tj}$$

由于 D 是理想，且 $A \in D$，$E_{tj} \in M_n(F)$，所以 $AE_{tj} \in D$，同理，由于 $xa_{kt}^{-1}E_{ik} \in M_n(F)$，所以 $xE_{ij} = (xa_{kt}^{-1}E_{ik})AE_{tj} \in D$。

而对任意 $B = (b_{ij}) \in M_n(F)$，有 $B = \sum\limits_{1 \le i,j \le n} b_{ij}E_{ij} \in D$。从而 $D = M_n(F)$。 □

18.22 由于理想都是环的加法子群，而 $\langle \mathbb{Z}_5, \oplus \rangle$ 没有非平凡的子群，所以 $\mathbb{Z}_5$ 的理想只有零理想 $\{0\}$ 和 $\mathbb{Z}_5$ 自身。

易于验证，$\{0, 2, 4\}$ 和 $\{0, 3\}$ 都是 $\mathbb{Z}_6$ 的非平凡理想，所以 $\mathbb{Z}_6$ 的理想有：

$H_1 = \{0\}$；
$H_2 = \{0, 3\}$；
$H_3 = \{0, 2, 4\}$；
$H_4 = \mathbb{Z}_6$。

18.23

证明: 首先，由于 $0 \in D$，从而 D 非空。

对任意 $x \in D$，存在 $m \in Z$，使得 $x = 4m = 2(2m) \in A$，所以有 $D \subseteq A$。

对任意 $x, y \in D$，有 $m, n \in \mathbb{Z}$，使得 $x = 4m, y = 4n$，从而 $x - y = 4(m - n) \in D$。

对任意 $a \in A$，$d \in D$，有 $m, n \in \mathbb{Z}$，使得 $a = 2m, d = 4n$，从而 $ad = da = 8mn = 4(2mn) \in D$。

这就证明了 D 是 A 的一个理想。 □

$A/D = \langle \{\bar{0}, \bar{2}\}, +, \cdot \rangle$。其中 $\bar{0}$ 为加法单位元和乘法零元，$\bar{2} + \bar{2} = \bar{2} \cdot \bar{2} = \bar{0}$。

18.24 即为引理 18.2。

18.25

证明: 设 $A^m = \{0\}$，$(R/A)^n = \{\bar{0}\}$，下面证明 $R^{mn} = \{0\}$。

设 $r_{ij} \in R$，$i = 1, 2, \cdots, m$， $j = 1, 2, \cdots, n$。则 $\prod\limits_{ij} r_{ij} = \prod\limits_{i=1}^{m}\prod\limits_{j=1}^{n} r_{ij}$，记 $a_i = \prod\limits_{j=1}^{n} r_{ij}$，$i = 1, 2, \cdots, m$，注意到：

$$\begin{aligned}
\bar{a}_i &= \overline{r_{i1}r_{i2}\cdots r_{in}} && (a_i \text{ 定义}) \\
&= \bar{r}_{i1}\bar{r}_{i2}\cdots\bar{r}_{in} && (\text{商环乘法运算定义}) \\
&= \bar{0} && ((R/A)^n = \{\bar{0}\}) \\
&= A && (\bar{0} = A + 0 = A)
\end{aligned}$$

从而有 $a_i \in A$，$i = 1, 2, \cdots, m$。因此：

$$\begin{aligned}
\prod_{ij} r_{ij} &= \prod_{i=1}^{m}\prod_{j=1}^{n} r_{ij} && (\text{结合律}) \\
&= \prod_{i=1}^{m} a_i && (a_i \text{ 定义}) \\
&= 0 && (A^m = 0)
\end{aligned}$$

这就证明了 $R^{mn} = \{0\}$，R 是幂零环。 □

18.26

证明: 必要性。设 R/H 是域。下面证明，对 R 的任意理想 $D \subseteq R$，若有 $H \subset D$，就有 $D = R$。

由于 $H \subset D$，所以存在 $x \in D - H$。由于 $x \notin H$，所以 $\bar{x} \neq \bar{0} = H$。又因为 R/H 是域，所以存在 $\bar{y} \in R/H$，使得 $xy + H = \bar{x} \cdot \bar{y} = \bar{1} = 1 + H$。从而 $xy \in xy + H = 1 + H$，也即，存在

$h \in H$，使得 $xy = 1 + h$。由于 $x \in D, y \in R$，且 D 是理想，所以 $xy \in D$，又因为 $H \subset D$，所以 $h \in D$，从而 $1 = xy - h \in D$。对任意 $r \in R$，有 $1 \in D$，$r = r \cdot 1 \in D$。从而有 $D = R$。

这就证明了 R 是极大理想。

充分性。设 R 是极大理想。由于 R 是交换含幺环，所以 R/H 也是交换含幺的。要证 R/H 是域，只需证明 $R/H - \{\bar{0}\}$ 中所有元素均可逆。

对任意 $\bar{a} \in R/H$，若 $\bar{a} \neq \bar{0}$，则 $a \notin H$。令 $A = \{h + ax \mid h \in H \wedge x \in R\}$。注意到，对任意 $h \in H$，有 $h = h + a \cdot 0 \in A$，从而有 $H \subseteq A$。又由于 $a = 0 + a \cdot 1 \in A$ 且 $a \notin R$，所以 $H \subset A$。A 自然是非空的。对任意 $h_1 + ax_1, h_2 + ax_2 \in A$，有 $(h_1 + ax_1) - (h_2 + ax_2) = (h_1 - h_2) + a(x_1 - x_2) \in A$。对任意 $h + ax \in H, r \in R$，有 $r(h + ax) = (h + ax)r = (hr) + a(xr) \in A$。所以 A 是 R 的理想，且 A 真包含 H。由于 H 是极大理想，所以 $1 \in A = R$。因此，存在 $h \in H, b \in R$，使得 $1 = h + ab$，从而有 $1 - ab = h \in H$。从而由教材定理 17.25(4) 知，$\overline{ab} = \bar{1}$。$\bar{b}$ 是 $\bar{a}$ 的逆元。由 $\bar{a}$ 的任意性知，$R/H - \{\bar{0}\}$ 中所有元素均可逆。这就证明了 R/H 是域。 □

18.27

证明: 由于 $0 = 0 \cdot x_1 + 0 \cdot x_2 + \cdots + 0 \cdot x_m \in S$，所以 S 非空。

对任意 $r_1 \cdot x_1 + r_2 \cdot x_2 + \cdots + r_m \cdot x_m, r'_1 \cdot x_1 + r'_2 \cdot x_2 + \cdots + r'_m \cdot x_m \in S$，有 $(r_1 \cdot x_1 + r_2 \cdot x_2 + \cdots + r_m \cdot x_m) - (r'_1 \cdot x_1 + r'_2 \cdot x_2 + \cdots + r'_m \cdot x_m) = (r_1 - r'_1) \cdot x_1 + (r_2 - r'_2) \cdot x_2 + \cdots + (r_m - r'_m) \cdot x_m \in S$。

对任意 $a \in R$，$r_1 \cdot x_1 + r_2 \cdot x_2 + \cdots + r_m \cdot x_m \in S$，有 $(r_1 \cdot x_1 + r_2 \cdot x_2 + \cdots + r_m \cdot x_m)a = a(r_1 \cdot x_1 + r_2 \cdot x_2 + \cdots + r_m \cdot x_m) = (ar_1) \cdot x_1 + (ar_2) \cdot x_2 + \cdots + (ar_m) \cdot x_m \in S$。

这就证明了 S 是 R 的理想。 □

18.28 设 $\varphi : \mathbb{Z}_2 \to \mathbb{Z}$ 为同态，则由于 $\mathbb{Z}_2$ 和 $\mathbb{Z}$ 的加法单位元都是 0，所以应有 $\varphi(0) = 0$。同时有 $\varphi(1) + \varphi(1) = \varphi(1 + 1) = \varphi(0) = 0$。而在 $\mathbb{Z}$ 中，$x + x = 0$ 的解只有 $x = 0$，从而应有 $\varphi(1) = \varphi(0) = 0$。

因此，从 $\mathbb{Z}_2$ 到 $\mathbb{Z}$ 的同态只有零同态 $\varphi : \mathbb{Z}_2 \to \mathbb{Z}, \forall x \in \mathbb{Z}_2, \varphi(x) = 0$。

18.29

证明: A 对矩阵加法显然构成 Abel 群。对任意 $a_1, a_2, b_1, b_2, c_1, c_2 \in \mathbb{Z}$，$\left(\begin{smallmatrix} a_1 & b_1 \\ 0 & c_1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} a_2 & b_2 \\ 0 & c_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a_1a_2 & a_1b_2+b_1c_2 \\ 0 & c_1c_2 \end{smallmatrix}\right) \in A$。从而 A 是环。

因为 $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in B$，所以 B 非空。对任意 $x_1, x_2 \in \mathbb{Z}$，有 $\left(\begin{smallmatrix} 0 & 0 \\ 0 & x_1 \end{smallmatrix}\right) - \left(\begin{smallmatrix} 0 & 0 \\ 0 & x_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & x_1-x_2 \end{smallmatrix}\right) \in B$ 和 $\left(\begin{smallmatrix} 0 & 0 \\ 0 & x_1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 0 & 0 \\ 0 & x_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & x_1x_2 \end{smallmatrix}\right) \in B$。从而 B 是 A 的子环。 □

作 $\varphi : A \to B, \forall \left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \in A, \varphi(\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & a \end{smallmatrix}\right)$，易于验证，$\varphi$ 是同态。$\ker \varphi = \{\left(\begin{smallmatrix} 0 & b \\ 0 & c \end{smallmatrix}\right) \mid b, c \in \mathbb{Z}\}$。

18.30

证明: 由多项式加法和乘法原则可知，对任意 $f(x) = a_0 + a_1x + \cdots + a_nx^n, g(x) = b_0 + b_1x + \cdots + b_mx^m \in F[x]$，有 $\varphi(f(x) + g(x)) = a_0 + b_0 = \varphi(f(x)) + \varphi(g(x))$，$\varphi(f(x) \cdot g(x)) = a_0b_0 = \varphi(f(x)) \cdot \varphi(g(x))$。从而 φ 是同态。对任意 $a \in F$，令 $f(x) = a \in F[x]$，则 $\varphi(f(x)) = a$。从而 φ 是满同态。 □

$\ker \varphi = \{a_1x + a_2x^2 + \cdots + a_nx^n \mid n \in \mathbb{N}, a_i \in F, i = 1, 2, \cdots, n\}$。

$F[x]/\ker \varphi = \langle\{\bar{a} \mid a \in F\}, +, \cdot\rangle$，其中 $\bar{a} = \{a + a_1x + \cdots + a_nx^n \mid n \in \mathbb{N}, a_i \in F, i = 1, 2, \cdots, n\}$，对任意 $a, b \in F$，$\bar{a} + \bar{b} = \overline{a + b}$，$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$。

18.31

证明： 由定义显然有 $A/B\subseteq R/B$。

由于 $B\in A/B$，所以 A/B 非空。

对任意 $\bar{x},\bar{y}\in A/B$，有 $x,y\in A$，从而 $x-y\in A$，$\bar{x}-\bar{y}=\overline{x-y}\in A/B$ ($\bar{x}-\bar{y}=\overline{x-y}$ 是因为 $-y\in\overline{-y}$，从而 $0\in\bar{y}+\overline{-y}$，$\bar{y}+\overline{-y}=\bar{0}$。这就是说 $\overline{-y}=-\bar{y}$，从而 $\bar{x}-\bar{y}=\bar{x}+\overline{-y}=\overline{x+(-y)}=\overline{x-y}$)。

对任意 $\bar{x}\in A/B$，$\bar{y}\in R/B$，有 $x\in A,y\in R$，从而有 $xy\in A$ 和 $yx\in A$。因此有 $\bar{x}\cdot\bar{y}=\overline{xy}\in A/B$，$\bar{y}\cdot\bar{x}=\overline{yx}\in A/B$。

这就证明了 A/B 是 R/B 的理想。

作 $\varphi: R/B\to R/A$，$\forall x+B\in R/B$，令 $\varphi(x+B)=x+A$。

首先证明 φ 是函数。对任意 $x,y\in R/B$，

$$\begin{aligned}
&x+B=y+B\\
\iff&-x+y\in B && \text{(教材定理 17.25(4))}\\
\implies&-x+y\in A && (B\subseteq A)\\
\iff&x+A=y+A && \text{(教材定理 17.25(4))}\\
\iff&\varphi(x+B)=\varphi(y+B) && (\varphi\text{ 定义})
\end{aligned}$$

这就证明了 φ 是函数。

对任意 $x+A\in R/A$，有 $x+B\in R/B$，$\varphi(x+B)=x+A$，从而 φ 是满射。

由除环运算定义可知，φ 是同态，且为满同态。

由教材定理 17.25(4) 知，$\varphi(x+B)=x+A=A$ 当且仅当 $x\in A$。从而 $\ker\varphi=\{x+B\mid x\in A\}=A/B$。由环同态基本定理知，$R/B\Big/(A/B)\cong R/A$。 □

18.32

证明： 对任意 $x\in R_1$，

$$\begin{aligned}
&x\in\varphi^{-1}(\varphi(S))\\
\iff&\exists y(y\in\varphi(S)\wedge\varphi(x)=y) && (\varphi^{-1}\text{ 定义})\\
\iff&\exists y\exists z(z\in S\wedge y=\varphi(z)\wedge\varphi(x)=y) && (\varphi(S)\text{ 定义})\\
\implies&\exists z(z\in S\wedge\varphi(x)=\varphi(z)) && \text{(等量代换)}\\
\iff&\exists z(z\in S\wedge x+\ker\varphi=z+\ker\varphi) && \text{(教材定理 17.36(2))}\\
\iff&\exists z(z\in S\wedge x\in z+\ker\varphi) && \text{(教材定理 17.25(4))}\\
\implies&x\in S+\ker\varphi && (S+\ker\varphi\text{ 定义})\\
\iff&x\in\ker\varphi+S && (\ker\varphi\text{ 是正规的})
\end{aligned}$$

这就证明了 $x\in\varphi^{-1}(\varphi(S))\subseteq\ker\varphi+S$。

反之，对任意 $x\in R_1$，

$$\begin{aligned}
&x\in\ker\varphi+S\\
\iff&\exists y\exists s(y\in\ker\varphi\wedge s\in S\wedge x=y+s) && (\ker\varphi+S\text{ 定义})\\
\implies&\exists y\exists s(y\in\ker\varphi\wedge s\in S\wedge\varphi(x)=\varphi(y)+\varphi(s)) && (\varphi\text{ 是同态})\\
\implies&\exists y\exists s(y\in\ker\varphi\wedge s\in S\wedge\varphi(x)=\varphi(s)) && (y\in\ker\varphi)\\
\implies&\exists s(s\in S\wedge\varphi(x)=\varphi(s)) && (\exists\text{消去})\\
\implies&\varphi(x)\in\varphi(S) && (\varphi(S)\text{ 定义})\\
\iff&x\in\varphi^{-1}(\varphi(S)) && (\varphi^{-1}\text{ 定义})
\end{aligned}$$

这就证明了 $\ker\varphi + S \subseteq \varphi^{-1}(\varphi(S))$。从而有 $\varphi^{-1}(\varphi(S)) = \ker\varphi + S$。 □

18.33

证明： 不妨记 $F_1 = \langle A_1, +_1, *_1\rangle$，$F_2 = \langle A_2, +_2, *_2\rangle$。

由教材定理 18.6 知，$\ker\varphi$ 是 F_1 是理想。由教材例 18.11 知，F_1 中的理想只有 $\{0\}$ 和 F_1。由于 $\varphi(F_1) \neq \{0\}$，所以存在 $x \in F_1$，使得 $\varphi(x) \neq 0$，$x \notin \ker\varphi$。从而 $\ker\varphi \neq F_1$。因此，必有 $\ker\varphi = \{0\}$。

注意到，φ 也是群 $\langle A_1, +_1\rangle$ 到群 $\langle A_2, +_2\rangle$ 的同态。由 $\ker\varphi = \{0\}$ 和教材定理 17.33 知，φ 是从 $\langle A_1, +_1\rangle$ 到 $\langle A_2, +_2\rangle$ 的单同态。这就是说，φ 是从 A_1 到 A_2 的单射，从而也是 F_1 到 F_2 的单同态。 □

18.34

证明： 显然，对任何 $f, g \in \operatorname{End} G$，$f+g$ 和 $f \circ g$ 仍是函数。对任意 $x, y \in G$，

$$\begin{aligned}
(f+g)(x+y) &= f(x+y) + g(x+y) && \text{(定义)}\\
&= f(x) + f(y) + g(x) + g(y) && (f, g \text{ 是同态})\\
&= f(x) + g(x) + f(y) + g(y) && (G \text{ 是 Abel 群})\\
&= (f+g)(x) + (f+g)(y) && \text{(定义)}\\
(f \circ g)(x+y) &= f(g(x+y)) && \text{(定义)}\\
&= f(g(x) + g(y)) && (g \text{ 是同态})\\
&= f(g(x)) + f(g(y)) && (f \text{ 是同态})\\
&= (f \circ g)(x) + (f \circ g)(y) && \text{(定义)}
\end{aligned}$$

这就证明了 $f+g$ 和 $f \circ g$ 都是 G 的自同态。从而 $+$ 和 $\circ$ 都是 $\operatorname{End} G$ 上的二元运算。

$+$ 运算显然满足交换律、结合律，且零同态 φ_0 是加法单位元。令 $\varphi : G \to G$，$\forall x \in G$，$\varphi(x) = -x$。由习题 17.61 结论知，φ 是自同构。对任意 $f \in \operatorname{End} G$，显然有 $\varphi \circ f \in \operatorname{End} G$ 和 $f + \varphi \circ f = \varphi_0$。从而 $\operatorname{End} G$ 中每个元素均有加法逆元。因此，$\langle \operatorname{End} G, +\rangle$ 是 Abel 群。

由教材定理 2.5 知，$\circ$ 运算是可结合的。从而 $\langle \operatorname{End} G, \circ\rangle$ 是半群。

对任意 $f, g, h \in \operatorname{End} G$，$x \in G$，

$$\begin{aligned}
(f \circ (g+h))(x) &= f((g+h)(x)) && (\circ \text{ 运算定义})\\
&= f(g(x) + h(x)) && (+ \text{ 运算定义})\\
&= f(g(x)) + f(h(x)) && (f \text{ 是同态})\\
&= (f \circ g)(x) + (f \circ h)(x) && (\circ \text{ 运算定义})\\
((g+h) \circ f)(x) &= (g+h)(f(x)) && (\circ \text{ 运算定义})\\
&= g(f(x)) + h(f(x)) && (+ \text{ 运算定义})\\
&= (g \circ f)(x) + (h \circ f)(x) && (\circ \text{ 运算定义})
\end{aligned}$$

从而 $\circ$ 运算对 $+$ 运算是可分配的。

这就证明了 $\langle \operatorname{End} G, +, \circ\rangle$ 是环。 □

对循环群上的任何自同态 $\varphi : G \to G$，若 $\varphi(a) = ia$，则必有 $\varphi(ka) = k\varphi(a) = kia$，$k, i \in \mathbb{Z}$。从而循环群上的自同态具有 $\varphi_i(ka) = kia, \forall ka \in G$ 的形式。显然，

$$\varphi_i = \varphi_j \iff i \equiv j \pmod{n},$$

从而 $\operatorname{End} G = \{\varphi_i \mid i = 0, 1, \cdots, n-1\}$。

对任意 $\varphi_i, \varphi_j \in \operatorname{End} G$，$a^t \in G$，

$$\begin{aligned}
(\varphi_i + \varphi_j)(ka) &= \varphi_i(ka) + \varphi_j(ka) && (+\ \text{运算定义})\\
&= kia + kja && (\varphi_i, \varphi_j\ \text{定义})\\
&= k(i+j)a && (\text{整数乘法分配律})\\
&= \varphi_{i+j}(ka) && (\varphi_{i+j}\ \text{定义})\\
(\varphi_i \circ \varphi_j)(ka) &= \varphi_i(\varphi_j(ka)) && (\circ\ \text{运算定义})\\
&= kjia && (\varphi_i, \varphi_j\ \text{定义})\\
&= \varphi_{ji}(ka) && (\varphi_{ji}\ \text{定义})
\end{aligned}$$

因此，G 的自同态环为，$\langle \{\varphi_i \mid i = 0, 1, \cdots, n-1\}, +, \circ \rangle$，对所有 $\varphi_i, \varphi_j \in \operatorname{End} G$，$\varphi_i + \varphi_j = \varphi_{(i+j \bmod n)}$，$\varphi_i \circ \varphi_j = \varphi_{(ji \bmod n)}$。

18.35

证明: 仿上题的方法可证，对有理数加法群上的任何自同态 $\varphi : \mathbb{Q} \to \mathbb{Q}$，若 $\varphi(1) = a$，则 $\forall x \in \mathbb{Q}$，$\varphi(x) = ax$。从而 $\operatorname{End} G = \{\varphi_a \mid a \in \mathbb{Q}\}$，其中 φ_a 定义为 $\forall x \in \mathbb{Q}$，$\varphi_a(x) = ax$。

作 $\sigma : \operatorname{End} \mathbb{Q} \to \mathbb{Q}$，$\forall \varphi_a \in \operatorname{End} \mathbb{Q}$，令 $\sigma(\varphi_a) = a$。显然，σ 是双射。下面证 σ 是从 $\langle \operatorname{End} \mathbb{Q}, +, \circ \rangle$ 到 $\langle \mathbb{Q}, +, \cdot \rangle$ 的同态。

对任意 $\varphi_a, \varphi_b \in \operatorname{End} \mathbb{Q}$，$x \in \mathbb{Q}$，

$$\begin{aligned}
(\varphi_a + \varphi_b)(x) &= \varphi_a(x) + \varphi_b(x) && (+\ \text{运算定义})\\
&= ax + bx && (\varphi_a, \varphi_b\ \text{定义})\\
&= (a+b)x && (\text{分配律})\\
&= \varphi_{a+b}(x) && (\varphi_{a+b}\ \text{定义})\\
(\varphi_a \circ \varphi_b)(x) &= \varphi_a(\varphi_b(x)) && (\circ\ \text{运算定义})\\
&= abx && (\varphi_a, \varphi_b\ \text{定义})\\
&= \varphi_{ab}(x) && (\varphi_{ab}\ \text{定义})
\end{aligned}$$

从而有 $\sigma(\varphi_a + \varphi_b) = \sigma(\varphi_{a+b}) = a + b = \sigma(\varphi_a) + \sigma(\varphi_b)$，$\sigma(\varphi_a \circ \varphi_b) = \sigma(\varphi_{ab}) = ab = \sigma(\varphi_a)\sigma(\varphi_b)$。

这就证明了 σ 是同态，从而是同构。于是有 $\langle \operatorname{End} \mathbb{Q}, +, \circ \rangle \cong \langle \mathbb{Q}, +, \cdot \rangle$。 □

18.36

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	x	0
$x+1$	0	$x+1$	0	$x+1$

由于 $x, (x+1) \in F_2[x]/(x+x^2)$，$x \neq 0$，$x+1 \neq 0$，但 $x \cdot (x+1) = 0$，所以 $F[2]/(x+x^2)$ 不是域。

18.37

证明: 对任意次数大于 1 的多项式 $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F_2[x]$，若 $f(x)$ 中有偶数个非零系数，不妨设它们是 $a_{i_1} = a_{i_2} = \cdots = a_{i_k} = 1$，其中 $i_1 < i_2 < \cdots < i_k$，k 为偶数。则

$$f(x) = x^{i_1}(x^{i_2-i_1}+1) + x^{i_3}(x^{i_4-i_3}+1) + \cdots + x^{i_{k-1}}(x^{i_k-i_{k-1}}+1) \qquad (*)$$

注意到，$\forall m \in \mathbb{Z}^+$，有 $x^m+1=(x+1)(x^{m-1}+x^{m-2}+\cdots+x+1)$。所以 $(*)$ 式中的每一项均可被 $(x+1)$ 整除。从而 $(x+1) \mid f(x)$。由于 $x+1$ 的次数为 1，而 $f(x)$ 的次数大于 1，所以 $f(x)$ 是可约的。

这就证明了 $F_2[x]$ 上任何次数大于 1 的不可约多项式都不可能有偶数个(从而必有奇数个)非零系数。 □

18.38 x，$x+1$，x^2+x+1，x^3+x+1，x^3+x^2+1，x^4+x+1，x^4+x^3+1，$x^4+x^3+x^2+x+1$。

18.39 由于 $F_2[x]$ 上次数小于 n 的多项式共有 2^n 个，所以只需取一个 3 次不可约多项式 $f(x)$，就可以使 $F_2[x]/f(x)$ 为 8 阶有限域。由上题结论知，可以令 $f(x)=x^3+x+1$ 或令 $f(x)=x^3+x^2+1$。

当 $f(x)=x^3+x+1$ 时，运算表如下：

$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2+1	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	$x+1$	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	x^2+x+1	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

当 $f(x)=x^3+x^2+1$ 时，加法表不变，乘法表如下：

$\cdot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	x^2+1	x^2+x+1	1	$x+1$
$x+1$	0	$x+1$	x^2+x	x^2+1	1	x	x^2+x+1	x^2
x^2	0	x^2	x^2+1	1	x^2+x+1	$x+1$	x	x^2+x
x^2+1	0	x^2+1	x^2+x+1	x	$x+1$	x^2+x	x^2	1
x^2+x	0	x^2+x	1	x^2+x+1	x	x^2	$x+1$	x^2+1
x^2+x+1	0	x^2+x+1	$x+1$	x^2	x^2+x	1	x^2+1	x

18.40 $x^5-1=(x-1)(x^4+x^3+x^2+x+1)=(x+1)(x^4+x^3+x^2+x+1)$，由习题 18.38 结论知，$x+1$ 和 $x^4+x^3+x^2+x+1$ 都是不可约多项式。

第十九章　格与布尔代数

19.1

(1) 是。

(2) 不是。$\{c, d\}$ 没有最大下界。

(3) 不是。$\{a, b\}$ 没有上界和下界。

(4) 是。

(5) 是。

(6) 不是。$\{d, f\}$ 没有下界。

(7) 不是。$\{c, d\}$ 没有最小上界。

(8) 是。

19.2

(1) 不是。$\{4, 6\}$ 没有上界。

(2) 是。

(3) 是。

(4) 是。

19.3

(1)

证明:

$$\begin{aligned} a \vee b &= b && \text{(教材定理 19.2)} \\ &= b \wedge c && \text{(教材定理 19.2)} \end{aligned}$$

□

(2)

证明:

$$\begin{aligned} (a \wedge b) \vee (b \wedge c) &= a \vee b && \text{(教材定理 19.2)} \\ &= b \wedge c && \text{(第 (1) 小题结论)} \\ &= (a \vee b) \wedge (a \vee c) && \text{(教材定理 19.2)} \end{aligned}$$

□

19.4

(1)

证明: 由教材定理 19.1(1) 知，$a \wedge b \preccurlyeq a$，由教材定理 19.1(2) 知，$a \preccurlyeq a \vee c$。由偏序关系传递性知，$a \wedge b \preccurlyeq a \vee c$。同理可证 $a \wedge b \preccurlyeq b \vee d$。从而由教材定理 19.1(3) 就有 $a \wedge b \preccurlyeq (a \vee c) \wedge (b \vee d)$。同理可证 $c \wedge d \preccurlyeq (a \vee c) \wedge (b \vee d)$。由教材定理 19.1(4) 即得 $(a \wedge b) \vee (c \wedge d) \preccurlyeq (a \vee c) \wedge (b \vee d)$。□

(2)

证明: 由教材定理 19.1 可知，$a \wedge b \preccurlyeq a \preccurlyeq a \vee b$，$a \wedge b \preccurlyeq b \preccurlyeq b \vee c$，$a \wedge b \preccurlyeq a \preccurlyeq c \vee a$，从而由教材定理 19.1(3) 得 $a \wedge b \preccurlyeq (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$。同理可证 $b \wedge c \preccurlyeq (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$ 和 $c \wedge a \preccurlyeq (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$。由教材定理 19.1(4) 即有 $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \preccurlyeq (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$。□

19.5

证明: 充分性显然。下面证必要性。

对任意 $1 \leq i \leq n$，有：

$$\begin{aligned} a_1 \wedge a_2 \wedge \cdots \wedge a_n &\preccurlyeq a_i && \text{(交换律、教材定理 19.1(1))} \\ &\preccurlyeq a_1 \vee a_2 \vee \cdots \vee a_n && \text{(交换律、教材定理 19.1(2))} \\ &= a_1 \wedge a_2 \wedge \cdots \wedge a_n && \text{(前提)} \end{aligned}$$

从而有 $a_i = a_1 \wedge a_2 \wedge \cdots \wedge a_n$。由 i 的任意性可知，$a_1 = a_2 = \cdots = a_n = a_1 \wedge a_2 \wedge \cdots \wedge a_n$。□

19.6

证明: 充分性。

若 a 与 b 不可比，则有 $a \not\preccurlyeq b$ 和 $b \not\preccurlyeq a$。由教材定理 19.2 即有 $a \wedge b \neq a$ 和 $a \wedge b \neq b$。但由定义有 $a \wedge b \preccurlyeq a$ 和 $a \wedge b \preccurlyeq b$，从而有 $a \wedge b \prec a$ 和 $a \wedge b \prec b$。

必要性。

若 $a \wedge b \prec a$，则有 $a \wedge b \neq a$。由教材定理 19.2 即有 $a \not\preccurlyeq b$。同理可证 $b \not\preccurlyeq a$。因此，a 与 b 不可比。□

19.7

(1) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$；

(2) $(a \vee b) \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$；

(3) $(a \vee b) \wedge (c \vee d) \succcurlyeq (a \wedge c) \vee (b \wedge d)$；

(4) $(a \vee b) \wedge (b \vee c) \wedge (c \vee a) \succcurlyeq (a \wedge b) \vee (b \wedge c) \vee (c \wedge a)$；

其中命题 (4) 是自对偶的(若考虑字母间的对称性，则命题 (2) 和 (3) 也是自对偶的)。

19.8 L_1 的三元子格有 $\{a,b,c\}$，$\{a,b,d\}$，$\{a,b,e\}$，$\{a,c,e\}$，$\{a,d,e\}$，$\{b,c,e\}$，$\{b,d,e\}$。

L_1 的四元子格有 $\{a,b,c,e\}$，$\{a,b,d,e\}$，$\{b,c,d,e\}$。

L_1 的五元子格只有 L_1 本身。

L_2 的三元子格有 $\{a,b,e\}$，$\{a,b,g\}$，$\{a,c,f\}$，$\{a,c,g\}$，$\{a,d,e\}$，$\{a,d,f\}$，$\{a,d,g\}$，$\{a,e,g\}$，$\{a,f,g\}$，$\{b,e,g\}$，$\{c,f,g\}$，$\{d,e,g\}$，$\{d,f,g\}$。

L_2 的四元子格有 $\{a,b,c,g\}$，$\{a,b,d,e\}$，$\{a,b,e,g\}$，$\{a,b,f,g\}$，$\{a,c,d,f\}$，$\{a,c,e,g\}$，$\{a,c,f,g\}$，$\{a,d,e,g\}$，$\{a,d,f,g\}$，$\{d,e,f,g\}$。

L_2 的五元子格有 $\{a,b,c,e,g\}$，$\{a,b,c,f,g\}$，$\{a,b,d,e,g\}$，$\{a,c,d,f,g\}$，$\{a,d,e,f,g\}$。

19.9

证明: 对任意 $x,y \in L_1$，由定义有 $x,y \in L$，$x \preccurlyeq a$ 和 $y \preccurlyeq a$。由于 L 是格，所以有 $x \wedge y, x \vee y \in L$。又由教材定理 19.1(1) 有 $x \wedge y \preccurlyeq x \preccurlyeq a$，且由教材定理 19.1(4) 有 $x \vee y \preccurlyeq a$。所以有 $x \wedge y, x \vee y \in L_1$。由定义，$L_1$ 是 L 的子格。

对任意 $x,y \in L_2$，由定义有 $x,y \in L$，$a \preccurlyeq x$ 和 $a \preccurlyeq y$。由于 L 是格，所以有 $x \wedge y, x \vee y \in L$。又由教材定理 19.1(3) 有 $a \preccurlyeq x \wedge y$，且由教材定理 19.1(2) 有 $a \preccurlyeq x \preccurlyeq x \vee y$。所以有 $x \wedge y, x \vee y \in L_2$。由定义，$L_2$ 是 L 的子格。

易见，$L_3 = L_1 \cap L_2$，而若干子格的交仍是子格(这是因为：设 $A = \{L_i \mid i = 1,2,\cdots k\}$ 是

L 的若干个子格的集合，则对所有 $x, y \in \cap A$，由于 x, y 属于 A 中的每一个子格，所以 $x \wedge y$ 和 $x \vee y$ 也属于 A 中的每一个子格，从而 $x \wedge y, x \vee y \in \cap A$，这就是说，$\cap A$ 也是 L 的子格)，从而 L_3 是 L 的子格。 □

19.10 L_1 含有与钻石格同构的子格 $\{d, e, f, g, h\}$，因此不是分配格。但 L_1 不含与五角格同构的子格，因此是模格。

L_2 含有与五角格同构的子格 $\{a, b, c, f, g\}$，因此不是模格，也不是分配格。

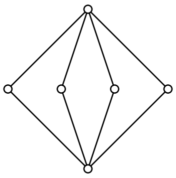
L_3 含有与五角格同构的子格 $\{a, b, d, e, h\}$，因此不是模格，也不是分配格。

L_4 含有与五角格同构的子格 $\{a, b, d, d, e\}$ (书中似有印刷错误，出现了两个 d)，因此不是模格，也不是分配格。

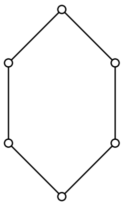
L_5 含有与五角格同构的子格 $\{a, b, c, d, f\}$，因此不是模格，也不是分配格。

19.11 易见，下图中 L_1 是分配格，L_2 是模格但不是分配格，L_3 不是模格。

L_1



L_2



L_3

19.12

证明：必要性。

由教材定理 19.1(2) 知，$a \preccurlyeq a \vee c$。若 L 是模格，则由 $a \preccurlyeq a \vee c$ 和模格定义就有 $a \vee (b \wedge (a \vee c)) = (a \vee b) \wedge (a \vee c)$。

充分性。

若对任意 $a, b, c \in L$ 都有 $a \vee (b \wedge (a \vee c)) = (a \vee b) \wedge (a \vee c)$，则对任意 $x, y, z \in L$，若 $x \preccurlyeq y$，则由教材定理 19.2 就有 $x \vee y = x$，从而

$$\begin{aligned} x \vee (z \wedge y) &= x \vee (z \wedge (x \vee y)) && (x \vee y = x) \\ &= (x \vee z) \wedge (x \vee y) && (\text{前提}) \\ &= (x \vee z) \wedge y && (x \preccurlyeq y\text{、教材定理 19.2}) \end{aligned}$$

由定义知，L 是模格。 □

19.13

证明：必要性。

若 $a \wedge b \preccurlyeq c \preccurlyeq a \vee b$，则由教材定理 19.2 知，$(a \wedge b) \vee c = (a \vee b) \wedge c = c$，从而

$$\begin{aligned} (a \wedge c) \vee (b \wedge c) \vee (a \wedge b) &= ((a \vee b) \wedge c) \vee (a \wedge b) && (\text{分配律}) \\ &= c \vee (a \wedge b) && ((a \vee b) \wedge c = c) \\ &= c && ((a \wedge b) \vee = c) \end{aligned}$$

充分性。

若 $c = (a \wedge c) \vee (b \wedge c) \vee (a \wedge b)$，则

$$\begin{aligned}
a \wedge b &\preccurlyeq ((a \vee b) \wedge c) \vee (a \wedge b) && \text{(教材定理 19.1(2))}\\
&= (a \wedge c) \vee (b \wedge c) \vee (a \wedge b) && \text{(分配律)}\\
&= c && \text{(前提)}\\
&= (a \wedge c) \vee (b \wedge c) \vee (a \wedge b) && \text{(前提)}\\
&= ((a \vee b) \wedge c) \vee (a \wedge b) && \text{(分配律)}\\
&= (a \wedge b) \vee ((a \vee b) \wedge c) && \text{(交换律)}\\
&= (a \wedge b) \vee (c \wedge (a \vee b)) && \text{(交换律)}\\
&= ((a \wedge b) \vee c) \wedge (a \vee b) && (a \wedge b \preccurlyeq a \vee b\text{、}L\text{ 是模格)}\\
&\preccurlyeq a \vee b && \text{(教材定理 19.1(1))}
\end{aligned}$$

□

19.14

(1)

证明:

$$\begin{aligned}
b \wedge (a \vee c) &= (b \wedge (b \vee c)) \wedge (a \vee c) && \text{(吸收律)}\\
&= b \wedge ((b \vee c) \wedge (a \vee c)) && \text{(结合律)}\\
&= b \wedge ((a \vee c) \wedge (b \vee c)) && \text{(交换律)}\\
&= b \wedge ((c \vee a) \wedge (b \vee c)) && \text{(交换律)}\\
&= b \wedge (c \vee (a \wedge (b \vee c))) && (c \preccurlyeq b \vee c\text{、}L\text{ 是模格)}\\
&= b \wedge (c \vee ((a \wedge b) \vee (a \wedge c))) && \text{(题设)}\\
&= b \wedge ((c \vee (a \wedge c)) \vee (a \wedge b)) && \text{(交换律)}\\
&= b \wedge (c \vee (a \wedge b)) && \text{(吸收律)}\\
&= (c \vee (a \wedge b)) \wedge b && \text{(交换律)}\\
&= ((a \wedge b) \vee c) \wedge b && \text{(交换律)}\\
&= (a \wedge b) \vee (c \wedge b) && (a \wedge b \preccurlyeq b\text{、}L\text{ 是模格)}\\
&= (b \wedge a) \vee (b \wedge c) && \text{(交换律)}
\end{aligned}$$

□

(2)

证明:

$$\begin{aligned}
a \vee (b \wedge c) &= (a \vee (b \wedge a)) \vee (b \wedge c) && \text{(吸收律)}\\
&= a \vee ((b \wedge a) \vee (b \wedge c)) && \text{(结合律)}\\
&= a \vee (b \wedge (a \vee c)) && \text{(第 (1) 小题结论)}\\
&= (a \vee b) \wedge (a \vee c) && (a \preccurlyeq a \vee c\text{、}L\text{ 是模格)}
\end{aligned}$$

□

19.15

(1)

证明： 由定义知，$0 \preccurlyeq a$，又由教材定理 19.1(2) 知，$a \preccurlyeq a \vee b = 0$。从而有 $a = 0$。同理可证 $b = 0$。 □

(2)

证明： 由定义知，$a \preccurlyeq 1$，又由教材定理 19.1(1) 知，$1 = a \wedge b \preccurlyeq a$。从而有 $a = 1$。同理可证 $b = 1$。 □

19.16

(1)

证明： 反设 L 中存在以自身为补元的元素 a。则对任意 $x \in L$，有 $x \preccurlyeq 1 = a \vee a = a$ 和 $a = a \wedge a = 0 \preccurlyeq x$，从而有 $x = a$。由 x 的任意性知，$L = \{a\}$，$|L| = 1$，矛盾。 □

(2)

证明： 由于 $|L| \geq 3$，所以存在 $a \in T$，满足 $a \neq 0$ 且 $a \neq 1$。反设 a 有补元 b，则有 $a \vee b = 1$。由于 L 是链，所以 $a \preccurlyeq b$ 和 $b \preccurlyeq a$ 中至少有一式成立。若 $b \preccurlyeq a$，则由教材定理 19.2 有 $a = a \vee b = 1$，与 $a \neq 1$ 矛盾，因此只能有 $a \preccurlyeq b$。然而，若 $a \preccurlyeq b$，则 $a \wedge b = a \neq 0$，这与 b 是 a 的补元矛盾。所以 $a \in L$ 不存在补元，从而 L 不是有补格。 □

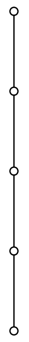
19.17

证明： 由定义，对任意 $a, b \in L_1$，有 $\bar{a}, \bar{b} \in L$，从而 $\bar{a} \wedge \bar{b}, \bar{a} \vee \bar{b} \in L$。而

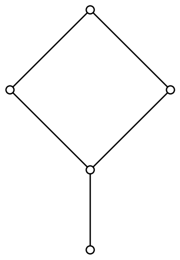
$$\begin{aligned}
(a \vee b) \wedge (\bar{a} \wedge \bar{b}) &= (a \wedge (\bar{a} \wedge \bar{b})) \vee (b \wedge (\bar{a} \wedge \bar{b})) && (\text{分配律})\\
&= ((a \wedge \bar{a}) \wedge \bar{b}) \vee (b \wedge (\bar{b} \wedge \bar{a})) && (\text{交换律})\\
&= ((a \wedge \bar{a}) \wedge \bar{b}) \vee ((b \wedge \bar{b}) \wedge \bar{a}) && (\text{结合律})\\
&= (0 \wedge \bar{b}) \vee (0 \wedge \bar{a}) && (a \wedge \bar{a} = b \wedge \bar{b} = 0)\\
&= 0 \vee 0 && (0 \preccurlyeq \bar{a}\text{、}0 \preccurlyeq \bar{b}\text{、教材定理 19.2})\\
&= 0 && (\text{教材定理 19.3(3)})\\
(a \vee b) \vee (\bar{a} \wedge \bar{b}) &= ((a \vee b) \vee \bar{a}) \wedge ((a \vee b) \vee \bar{b}) && (\text{分配律})\\
&= (\bar{a} \vee (a \vee b)) \wedge (a \vee (b \vee \bar{b})) && (\text{交换律})\\
&= ((\bar{a} \vee a) \vee b) \wedge (a \vee (b \vee \bar{b})) && (\text{结合律})\\
&= (1 \vee b) \vee (a \vee 1) && (\bar{a} \vee a = b \vee \bar{b} = 1)\\
&= 1 \vee 1 && (a, b \preccurlyeq 1\text{、教材定理 19.2})\\
&= 1 && (\text{教材定理 19.3(3)})
\end{aligned}$$

因此 $a \vee b$ 有补元 $\bar{a} \wedge \bar{b} \in L$，从而 $a \vee b \in L_1$。同理可证 $\overline{a \wedge b} = \bar{a} \vee \bar{b} \in L$，从而 $a \wedge b \in L_1$。这就证明了 L_1 是子格。 □

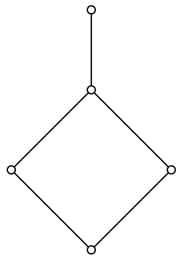
19.18 共有如下 5 个 5 元格。



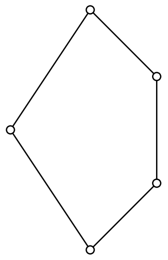
L_1



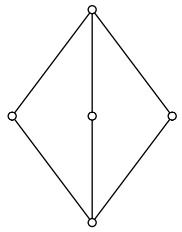
L_2



L_3



L_4



L_5

其中 L_1, L_2, L_3 是分配格，L_4 不是模格，从而也不是分配格，L_5 是模格但不是分配格。只有 L_4 和 L_5 是有补格。

19.19

证明: 对任意 $x \in L$，令 $T(x) = \{y \mid y \in L \text{ 且 } y \preccurlyeq x\}$，$i_x = |T(x)|$。显然，对任意 $x \in L$，有 $1 \le i_x \le t+1$。注意到:

引理 19.1 若 L 是链，则对任意 $x, y \in L$，有

$$x \preccurlyeq y \iff i_x \le i_y.$$

证明: 必要性显然，下面证充分性。

由于 L 是链，所以 $x \preccurlyeq y$ 与 $y \preccurlyeq x$ 至少有一式成立。反设 $x \not\preccurlyeq y$，则必有 $y \preccurlyeq x$。由 $y \preccurlyeq x$ 和偏序关系传递性可知，$T(y) \subseteq T(x)$，但由于 $x \not\preccurlyeq y$，所以 $x \in T(x)$，$x \notin T(y)$，从而 $T(y) \subset T(x)$，$i_y < i_x$，矛盾。 □

作 $\varphi : L \to L(G)$，对任意 $x \in L$，令 $\varphi(x) = \langle a^{p^{t-i_x+1}} \rangle$。$\varphi$ 显然是函数。

对任意 $x, y \in L$，若 $\varphi(x) = \varphi(y)$，则必有 $i_x = i_y$ (这是因为，由 $p^{t-i_x+1}, p^{t-i_y+1} \mid p^t$ 和教材例 17.16 可知，$|\varphi(x)| = p^{i_x-1}$，$|\varphi(y)| = p^{i_y-1}$，若 $i_x \ne i_y$，则 $\varphi(x)$ 与 $\varphi(y)$ 不等势，与 $\varphi(x) = \varphi(y)$ 矛盾)。由引理 19.1 就有 $x \preccurlyeq y$ 和 $y \preccurlyeq x$，从而 $x = y$。这就是说，φ 是单射。

由教材定理 17.13 可知，$L(G) = \{\langle a^{p^i} \rangle \mid i = 0, 1, \cdots, t\}$，下面证明，对任意 $0 \le i \le t$，必然存在一个 $x \in L$，使得 $i = t - i_x + 1$：若不然，则由鸽巢原理可知，存在 $x, y \in L$，使得 $x \ne y$ 且 $i_x = i_y$。但由 $i_x = i_y$ 和引理 19.1 应有 $x = y$，矛盾。这就证明了，对任意 $y \in L(G)$，必然存在 $x \in L$，使得 $\varphi(x) = y$。这就证明了 φ 是满射，从而是双射。

最后证明 $x \preccurlyeq y \Leftrightarrow \varphi(x) \preccurlyeq \varphi(y)$。

充分性。

注意到，对任意 $x, y \in L$，有 $0 \le t - i_x + 1, t - i_y + 1 \le t$，从而由教材例 17.16 可知，$|\langle a^{p^{t-i_x+1}} \rangle| = \dfrac{p^t}{(p^t, p^{t-i_x+1})} = \dfrac{p^t}{p^{t-i_x+1}} = p^{i_x-1}$，$|\langle a^{p^{t-i_y+1}} \rangle| = \dfrac{p^t}{(p^t, p^{t-i_y+1})} = \dfrac{p^t}{p^{t-i_y+1}} = p^{i_y-1}$。因此有，

$$\begin{aligned}
& \varphi(x) \preccurlyeq \varphi(y) && \\
\iff & \langle a^{p^{t-i_x+1}} \rangle \subseteq \langle a^{p^{t-i_y+1}} \rangle && (\varphi \text{ 定义}) \\
\Longrightarrow & |\langle a^{p^{t-i_x+1}} \rangle| \le |\langle a^{p^{t-i_y+1}} \rangle| && (\text{教材定理 5.7 推论}) \\
\iff & p^{i_x-1} \le p^{i_y-1} && (|\langle a^{p^{t-i_x+1}} \rangle| = p^{i_x-1}, |\langle a^{p^{t-i_y+1}} \rangle| = p^{i_y-1}) \\
\iff & i_x \le i_y && (\text{指数函数性质}) \\
\iff & x \preccurlyeq y && (\text{引理 19.1})
\end{aligned}$$

必要性。

$$\begin{aligned}
&\quad x \preccurlyeq y \\
&\iff i_x \leq i_y && (\text{引理 19.1}) \\
&\iff p^{t-i_y+1} \mid p^{t-i_x+1} && (t-i_y+1 \leq t-i_x+1) \\
&\implies \langle a^{p^{t-i_x+1}} \rangle \subseteq \langle a^{p^{t-i_y+1}} \rangle && (\text{生成子群定义}) \\
&\iff \varphi(x) \preccurlyeq \varphi(y) && (\varphi\ \text{定义})
\end{aligned}$$

由教材定理 19.8 知，φ 是同构。 □

19.20

证明： 对任意 $x, y \in L$，有

$$\begin{aligned}
f(x \wedge y) &= (x \wedge y) \vee a && (f\ \text{定义}) \\
&= (x \vee a) \wedge (y \vee a) && (\text{分配律}) \\
&= f(x) \wedge f(y) && (f\ \text{定义}) \\
f(x \vee y) &= (x \vee y) \vee a && (f\ \text{定义}) \\
&= (x \vee y) \vee (a \vee a) && (\text{教材定理 19.3(3)}) \\
&= (x \vee a) \vee (y \vee a) && (\text{结合律、交换律}) \\
&= f(x) \vee f(y) && (f\ \text{定义})
\end{aligned}$$

从而 f 是自同态。同理可证，g 是自同态。 □

由定义，对任意 $x \in f(L)$，存在 $y \in L$，使得 $x = f(y) = y \vee a$。从而由教材定理 19.1(2) 知，$a \preccurlyeq x$。另一方面，对任意 $x \succcurlyeq a$，由教材定理 19.2 有 $f(x) = x \vee a = x$，$x \in f(L)$。这就是说，$f(L) = \{x \mid x \in L \text{ 且 } a \preccurlyeq x\}$。

同理可得，$g(L) = \{x \mid x \in L \text{ 且 } x \preccurlyeq a\}$。

19.21

证明： 由习题 19.9 结论可知，X 和 Y 都是格。

下面证明 f 是 X 到 Y 的双射。

f 显然是函数。对任意 $x_1, x_2 \in X$，

$$\begin{aligned}
&\quad f(x_1) = f(x_2) \\
&\iff x_1 \vee b = x_2 \vee b && (f\ \text{定义}) \\
&\implies a \wedge (x_1 \vee b) = a \wedge (x_2 \vee b) && (x_1 \vee b = x_2 \vee b) \\
&\iff (a \wedge x_1) \vee (a \wedge b) = (a \wedge x_2) \vee (a \wedge b) && (\text{分配律}) \\
&\iff x_1 \vee (a \wedge b) = x_2 \vee (a \wedge b) && (x_1, x_2 \preccurlyeq a\text{、教材定理 19.2}) \\
&\iff x_1 = x_2 && (a \wedge b \preccurlyeq x_1, x_2\text{、教材定理 19.2})
\end{aligned}$$

从而 f 是单射。

对任意 $y \in Y$，由于 $b \preccurlyeq y$，所以 $a \wedge b \preccurlyeq a \wedge y$，又由于 $y \preccurlyeq a \vee b$，所以 $a \wedge y \preccurlyeq a \wedge (a \vee b) = a$。从而 $a \wedge y \in X$。而

$$\begin{aligned}
f(a \wedge y) &= (a \wedge y) \vee b && (f\ \text{定义}) \\
&= (a \vee b) \wedge (y \vee b) && (\text{分配律}) \\
&= (a \vee b) \wedge y && (b \preccurlyeq y\text{、教材定理 19.2}) \\
&= y && (y \preccurlyeq a \vee b\text{、教材定理 19.2})
\end{aligned}$$

这就是说，对任意 $y \in Y$，有 $y = f(a \wedge y) \in f(X)$。因此，$f$ 是满射，从而是双射。

由上题结论可知，f 是 L 上的自同态，从而也是 $X, Y \subseteq L$ 上的同态。

这就证明了 f 是从 X 到 Y 的同构。

注意到，对任意 $x \in X$，有

$$\begin{aligned}
g \circ f(x) &= g(f(x)) && \text{(函数合成运算定义)}\\
&= (x \vee b) \wedge a && (f, g \text{ 定义})\\
&= (x \wedge a) \vee (b \wedge a) && \text{(分配律)}\\
&= x \vee (b \wedge a) && (x \preccurlyeq a\text{、教材定理 19.2})\\
&= x && (b \wedge a \preccurlyeq x\text{、教材定理 19.2})
\end{aligned}$$

这就是说，g 是 f 的左逆。由 f 是双射和教材定理 3.10(4) 可知，$g = f^{-1}$ 是 f 唯一的逆，从而是 Y 到 X 的同构(“同构映射的逆也是同构映射”这一结论的证明见习题 15.23 第 (2) 小题)。□

19.22

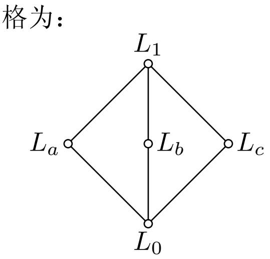
证明: 对任意 $f, g \in A, x, y \in L$，有

$$\begin{aligned}
f \circ g(x \wedge y) &= f(g(x \wedge y)) && \text{(合成运算定义)}\\
&= f(g(x) \wedge g(y)) && (g \text{ 是自同态})\\
&= f(g(x)) \wedge f(g(y)) && (f \text{ 是自同态})\\
&= f \circ g(x) \wedge f \circ g(y) && \text{(合成运算定义)}\\
f \circ g(x \vee y) &= f(g(x \vee y)) && \text{(合成运算定义)}\\
&= f(g(x) \vee g(y)) && (g \text{ 是自同态})\\
&= f(g(x)) \vee f(g(y)) && (f \text{ 是自同态})\\
&= f \circ g(x) \vee f \circ g(y) && \text{(合成运算定义)}
\end{aligned}$$

这就证明了，对任意 $f, g \in A$，有 $f \circ g \in A$。从而 $\circ$ 是 A 上的二元运算。

由于函数合成运算满足结合律，而恒等映射 $I_L \in A$ 是关于函数合成运算的单位元。因此，A 关于合成运算构成独异点。□

19.23 L 的理想有：$L_0 = \{0\}$，$L_a = \{0, a\}$，$L_b = \{0, b\}$，$L_c = \{0, c\}$，$L_1 = \{0, a, b, c, 1\}$。理想格为：



19.24

证明: 作 $\varphi : L \to I_0(L)$，$\forall x \in L$，$\varphi(x) = \{x \mid x \in L \text{ 且 } x \preccurlyeq a\}$。教材定理 19.12 已证明，$\varphi$ 是从 L 到 $I_0(L)$ 的单同态。现在只需证明 $\varphi(L) = I(L)$ 即可。

首先，对任何 $x \in L$，由 φ 定义和教材定理 19.12 有 $\varphi(x) \in I_0(L) = I(L) \cup \{\varnothing\}$，而 $x \in \varphi(x)$，从而 $x \neq \varnothing$。这就是说，$\varphi(x) \in I(L)$。由 x 的任意性知，$\varphi(L) \subseteq I(L)$。

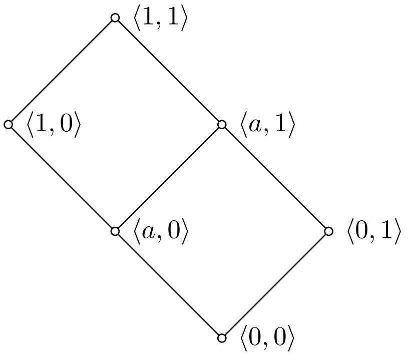
由于 L 是有限格，所以对任意 $I \in I(L)$，$\vee I = \bigvee\limits_{x \in I} x$ 是存在的，记 $a = \vee I$。注意到，由理想对 $\vee$ 运算的封闭性有 $a \in I$。下面证明 $I = \varphi(a) \in \varphi(L)$。

对任何 $x \in I$，显然有 $x \preccurlyeq a$，从而 $x \in \varphi(a)$。也就是说，$I \subseteq \varphi(a)$。

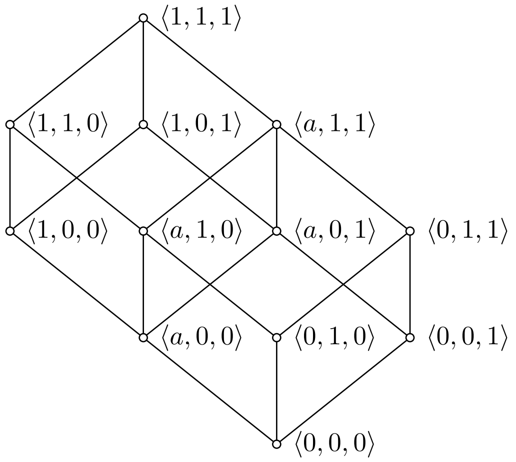
而对任何 $x \in \varphi(a)$，由 $\varphi(a)$ 的定义知，$x \preccurlyeq a$。由于 $x \in L$，$a \in I$，而 I 是理想，所以 $x \in I$。从而有 $\varphi(a) \subseteq I$。也即 $\varphi(a) = I$。

这就证明了 $\varphi(L) = I(L)$，φ 是 L 到 $I(L)$ 的满同态，从而是同构。 □

19.25



$L_1 \times L_2$



$L_1 \times L_2 \times L_2$

19.26

证明: $\forall a, b \in B$，

$$\begin{aligned}
a \vee (\bar{a} \wedge b) &= (a \vee \bar{a}) \wedge (a \vee b) && \text{(分配律)}\\
&= 1 \wedge (a \vee b) && \text{(补元定义)}\\
&= a \vee b && (a \vee b \preccurlyeq 1\text{、教材定理 19.2})\\
a \wedge (\bar{a} \vee b) &= (a \wedge \bar{a}) \vee (a \wedge b) && \text{(分配律)}\\
&= 0 \vee (a \wedge b) && \text{(补元定义)}\\
&= a \wedge b && (a \wedge b \preccurlyeq 0\text{、教材定理 19.2})
\end{aligned}$$

□

19.27 首先证明如下结论:

引理 19.2 设 $\langle B, \wedge, \vee, ^{-}, 0, 1\rangle$ 是布尔代数，则 $\forall a, b \in B$，有

$$\overline{(a \wedge \bar{b}) \vee (\bar{a} \wedge b)} = (\bar{a} \wedge \bar{b}) \vee (a \wedge b).$$

证明:

$$\begin{aligned}
\overline{(a \wedge \bar{b}) \vee (\bar{a} \wedge b)} &= \overline{a \wedge \bar{b}} \wedge \overline{\bar{a} \wedge b} && \text{(教材定理 19.23(2))}\\
&= (\bar{a} \vee \bar{\bar{b}}) \wedge (\bar{\bar{a}} \vee \bar{b}) && \text{(教材定理 19.23(2))}\\
&= (\bar{a} \vee b) \wedge (a \vee \bar{b}) && \text{(教材定理 19.23(1))}\\
&= (\bar{a} \wedge (a \vee \bar{b})) \vee (b \wedge (a \vee \bar{b})) && \text{(分配律)}\\
&= (\bar{a} \wedge a) \vee (\bar{a} \wedge \bar{b}) \vee (b \wedge a) \vee (b \wedge \bar{b}) && \text{(分配律)}\\
&= 0 \vee (\bar{a} \wedge \bar{b}) \vee (b \wedge a) \vee 0 && \text{(补元定义)}\\
&= (\bar{a} \wedge \bar{b}) \vee (b \wedge a) && \text{(0 是全下界、教材定理 19.2)}\\
&= (\bar{a} \wedge \bar{b}) \vee (a \wedge b) && \text{(交换律)}
\end{aligned}$$

□

再证原题。

证明: 由 B 对 $\vee$，$\wedge$ 和求补运算的封闭性可知，$\oplus$ 是 B 上的二元运算。

对任意 $a,b,c\in B$，有

$$\begin{aligned}
(a\oplus b)\oplus c &= (((a\wedge\bar{b})\vee(\bar{a}\wedge b))\wedge\bar{c})\vee(\overline{(a\wedge\bar{b})\vee(\bar{a}\wedge b)}\wedge c) && (\oplus\text{ 运算定义})\\
&= (((a\wedge\bar{b})\vee(\bar{a}\wedge b))\wedge\bar{c})\vee(((\bar{a}\wedge\bar{b})\vee(a\wedge b))\wedge c) && (\text{引理 19.2})\\
&= (a\wedge\bar{b}\wedge\bar{c})\vee(\bar{a}\wedge b\wedge\bar{c})\vee(\bar{a}\wedge\bar{b}\wedge c)\vee(a\wedge b\wedge c) && (\text{分配律})\\
&= (a\wedge\bar{b}\wedge\bar{c})\vee(a\wedge b\wedge c)\vee(\bar{a}\wedge b\wedge\bar{c})\vee(\bar{a}\wedge\bar{b}\wedge c) && (\text{交换律})\\
&= (a\wedge((\bar{b}\wedge\bar{c})\vee(b\wedge c)))\vee(\bar{a}\wedge((b\wedge\bar{c})\vee(\bar{b}\wedge c))) && (\text{分配律})\\
&= (a\wedge(\overline{(b\wedge\bar{c})\vee(\bar{b}\wedge c)}))\vee(\bar{a}\wedge((b\wedge\bar{c})\vee(\bar{b}\wedge c))) && (\text{引理 19.2})\\
&= a\oplus(b\oplus c) && (\oplus\text{ 运算定义})
\end{aligned}$$

从而 $\oplus$ 是可结合的。

由 $\vee$ 和 $\wedge$ 的可交换性立即可得 $\oplus$ 的可交换性。

对任意 $a\in B$，有

$$\begin{aligned}
0\oplus a &= a\oplus 0 && (\oplus\text{ 是可交换的})\\
&= (a\wedge\bar{0})\vee(\bar{a}\wedge 0) && (\oplus\text{ 运算定义})\\
&= (a\wedge 1)\vee(\bar{a}\wedge 0) && (\bar{0}=1)\\
&= a\vee 0 && (0\preccurlyeq\bar{a}\text{、}a\preccurlyeq 1\text{、教材定理 19.2})\\
&= a && (0\preccurlyeq a\text{、教材定理 19.2})
\end{aligned}$$

从而 0 是关于 $\oplus$ 运算的单位元。

对任意 $a\in B$，有 $a\oplus a=(a\wedge\bar{a})\vee(\bar{a}\wedge a)=0\vee 0=0$。从而 B 中所有元素都是自身的逆元。

这就证明了 $\langle B,\oplus\rangle$ 是 Abel 群。 □

19.28

证明: 由上题结论可知，$\langle B,\oplus\rangle$ 构成 Abel 群。

由 B 对 $\wedge$ 运算的封闭性和 $\wedge$ 运算的可结合性可知，$\langle B,\otimes\rangle$ 是半群。

由 $\wedge$ 运算对 $\vee$ 运算的分配律可知，$\otimes$ 运算对 $\oplus$ 运算是可分配的。

这就证明了 $\langle B,\oplus,\otimes\rangle$ 是环。

由教材定理 19.3(3) 可知，对任意 $a\in B$，有 $a\otimes a=a$。从而 $\langle B,\oplus,\otimes\rangle$ 是布尔环。 □

19.29

证明: 充分性显然。下面证必要性。

作 $\varphi: B\to\mathcal{P}(A)$，$\forall x\in B$，$\varphi(x)=\{a\mid a\in B,\ a$ 是原子, $a\preccurlyeq x\}$。由教材定理 19.25 的证明过程可知，φ 是从 B 到 $\mathcal{P}(A)$ 的同构。

注意到，$\varphi(0)=\varnothing$，且对任何原子 $a_i\in A$，有 $a_i\in\varphi(a_i)$。反设 $x\neq 0$，则 $\varphi(x)\neq\varnothing$，从而存在 $a\in A$，使得 $a_i\in\varphi(x)$。于是有 $a\in\varphi(x)\cap\varphi(a)=\varphi(x\wedge a_i)\neq\varnothing$。这与 $\varphi(x\wedge a)=\varphi(0)=\varnothing$ 矛盾。 □

19.30

证明: 对 n 作归纳。

当 $n=1$ 时，命题显然成立。

设 $n=k$ 时，命题成立。则当 $n=k+1$ 时，

$$\overline{a_1\wedge a_2\wedge\cdots\wedge a_k\wedge a_{k+1}}=\overline{a_1\wedge a_2\wedge\cdots\wedge a_k}\vee\bar{a}_{k+1} \qquad (\text{教材定理 19.23(2)})$$

$$= \bar{a}_1 \vee \bar{a}_2 \vee \cdots \vee \bar{a}_k \vee \bar{a}_{k+1} \qquad \text{(归纳假设)}$$

同理可证 $\overline{a_1 \vee a_2 \vee \cdots \vee a_n} = \bar{a}_1 \wedge \bar{a}_2 \wedge \cdots \wedge \bar{a}_n$。 □

19.31

(1)

$$\begin{aligned}
(a \wedge b) \vee (a \wedge \bar{b}) \vee (\bar{a} \vee b) &= (a \wedge (b \vee \bar{b})) \vee (\bar{a} \vee b) && \text{(分配律)}\\
&= (a \wedge 1) \vee (\bar{a} \vee b) && (b \vee \bar{b} = 1)\\
&= a \vee \bar{a} \vee b && (a \preccurlyeq 1\text{、教材定理 19.2})\\
&= 1 \vee b && (a \vee \bar{a} = 1)\\
&= 1 && (b \preccurlyeq 1\text{、教材定理 19.2})
\end{aligned}$$

(2)

$$\begin{aligned}
(a \wedge b) \vee (a \wedge \overline{b \wedge c}) \vee c &= (a \wedge (b \vee \overline{b \wedge c})) \vee c && \text{(分配律)}\\
&= (a \wedge (b \vee (\bar{b} \vee \bar{c}))) \vee c && \text{(教材定理 19.23(2))}\\
&= (a \wedge (1 \vee \bar{c})) \vee c && (\text{结合律、}b \vee \bar{b} = 1)\\
&= (a \wedge 1) \vee c && (\bar{c} \preccurlyeq 1\text{、教材定理 19.2})\\
&= a \vee c && (a \preccurlyeq 1\text{、教材定理 19.2})
\end{aligned}$$

19.32

证明: 对任意 $a, b \in B_1$，由题设已知 $\varphi(a \wedge b) = \varphi(a) \wedge \varphi(b)$，而

$$\begin{aligned}
\varphi(a \vee b) &= \varphi(\overline{\overline{a \vee b}}) && \text{(教材定理 19.23(1))}\\
&= \overline{\varphi(\overline{a \vee b})} && \text{(题设)}\\
&= \overline{\varphi(\bar{a} \wedge \bar{b})} && \text{(教材定理 19.23(2))}\\
&= \overline{\varphi(\bar{a}) \wedge \varphi(\bar{b})} && \text{(题设)}\\
&= \overline{\overline{\varphi(a)} \wedge \overline{\varphi(b)}} && \text{(题设)}\\
&= \overline{\overline{\varphi(a)}} \vee \overline{\overline{\varphi(b)}} && \text{(教材定理 19.23(2))}\\
&= \varphi(a) \vee \varphi(b) && \text{(教材定理 19.23(1))}
\end{aligned}$$

这就证明了 φ 是同态。 □

19.33

证明: 习题 19.9 已经证明，$[a, b]$ 是格 $\langle B, \wedge, \vee \rangle$ 子格。也即，$[a, b]$ 在 $\wedge$ 和 $\vee$ 运算下是封闭的。

由 $\wedge$ 和 $\vee$ 运算在 B 中的分配律可得 $\wedge$ 和 $\vee$ 运算在 $[a, b]$ 中的分配律。

由定义可知，a 是 $[a, b]$ 的全下界，b 是 $[a, b]$ 的全上界。

对任意 $x \in [a, b]$，令 $y = (\bar{x} \vee a) \wedge b$。则：

$$\begin{aligned}
a &= a \wedge b && (a \preccurlyeq b\text{、教材定理 19.2})\\
&\preccurlyeq (\bar{x} \wedge b) \vee (a \wedge b) && \text{(教材定理 19.1(2))}\\
&= (\bar{x} \vee a) \wedge b && \text{(分配律)}\\
&= y && \text{(定义)}\\
&= (\bar{x} \vee a) \wedge b && \text{(定义)}\\
&\preccurlyeq b && \text{(教材定理 19.1(1))}
\end{aligned}$$

因此有 $y \in [a,b]$。而

$$\begin{aligned}
x \wedge y &= x \wedge ((\bar{x} \vee a) \wedge b) && (y = (\bar{x} \vee a) \wedge b)\\
&= (x \wedge (\bar{x} \vee a)) \wedge b && (\text{结合律})\\
&= (x \wedge a) \wedge b && (\text{习题 19.26 第 (2) 小题结论})\\
&= a \wedge b && (a \preccurlyeq x\text{、教材定理 19.2})\\
&= a && (a \preccurlyeq b\text{、教材定理 19.2})\\
x \vee y &= x \vee ((\bar{x} \vee a) \wedge b) && (y = (\bar{x} \vee a) \wedge b)\\
&= (x \vee (\bar{x} \vee a)) \wedge (x \vee b) && (\text{分配律})\\
&= ((x \vee \bar{x}) \vee a) \wedge (x \vee b) && (\text{结合律})\\
&= (1 \vee a) \wedge (x \vee b) && (x \vee \bar{x} = 1)\\
&= 1 \wedge (x \vee b) && (a \preccurlyeq 1\text{、教材定理 19.2})\\
&= x \vee b && (x \vee b \preccurlyeq 1\text{、教材定理 19.2})\\
&= b && (x \preccurlyeq b\text{、教材定理 19.2})
\end{aligned}$$

从而 $y \in [a,b]$ 是 x 在 $[a,b]$ 中的补元。

这就证明了 $[a,b]$ 是布尔代数。 □

由于当 $a \neq 0$ 时，有 $0 \notin [a,b]$，当 $b \neq 1$ 时，有 $1 \notin [a,b]$。因此，除非 $a = 0$， $b = 1$，(此时 $[a,b] = B$，是 B 的平凡子代数)，否则 $[a,b]$ 将不能包括 $\langle B, \wedge, \vee, {}^{-}, 0, 1\rangle$ 中所有的代数常元，从而不是 $\langle B, \wedge, \vee, {}^{-}, 0, 1\rangle$ 的子代数。

19.34

(1)

证明: 对任意 $y \in B_2$，由于 φ 是双射，所以存在唯一的 $x \in B_1$，使得 $y = \varphi(x)$。若 $0 \prec y \preccurlyeq \varphi(a)$，则由教材定理 19.8 有 $0 \prec x \preccurlyeq a$ (这里 $0 \prec x$ 是因为由教材定理 19.24(1) 知， $\varphi(0) = 0$。而 $\varphi(x) \neq 0$，所以 $x \neq 0$。另一方面，由于 0 是全下界，所以有 $0 \preccurlyeq x$。综合就有 $0 \prec x$)。

由于 a 是原子，所以 $x = a$，从而 $y = \varphi(a)$。由 y 的任意性可知， $\varphi(a)$ 是原子。 □

(2)

证明: 由第 (1) 小题结论可知，对任意两个布尔代数 B_1 与 B_2，若 $B_1 \cong B_2$，则 B_1 与 B_2 的原子数量相同。从而，由有限布尔代数的表示定理可知，要证原题，只需证：对任何 n 元集合 A，幂集代数 $\mathcal{P}(A)$ 有且仅有 n 个原子。

首先证明，对任何 $a \in A$， $\{a\} \in \mathcal{P}(A)$ 是原子。这是因为，对任何 $a \in A$， $B \in \mathcal{P}(A)$，若 $0 \prec B \preccurlyeq \{a\}$，则有 $B \neq 0 = \varnothing$，即存在 $x \in B$。而 $x \in B \subseteq \{a\}$，也即 $x \in \{a\}$。由 $\{a\}$ 的描述法定义 $\{x \mid x = a\}$ 可知， $x \in \{a\} \Leftrightarrow x = a$。也即， $B = \{x\} = \{a\}$。这就证明了对所有 $a \in A$，$\{a\}$ 都是原子，从则 $\mathcal{P}(A)$ 中至少有 n 个原子。

反设 $\mathcal{P}(A)$ 中还有其它的原子 $C \notin \{\{x\} \mid x \in A\}$，则由于 $C \neq 0 = \varnothing$，所以存在 $x \in A$，使得 $x \in C$。从而 $0 \prec \{x\} \preccurlyeq C$，而 $\{x\} \neq C$ (否则 $C = \{x\} \in \{\{x\} \mid x \in A\}$，矛盾)，这与 C 是原子矛盾。这就证明了 $\mathcal{P}(A)$ 中有且仅有 n 个原子。 □

19.35

证明:

(1) 由教材定理 19.24(1) 有 $\varphi(0) = 0$，所以有 $0 \in J$。

(2) 由 $0 \preccurlyeq x \preccurlyeq a$ 和教材定理 19.7 可知， $0 = \varphi(0) \preccurlyeq \varphi(x) \preccurlyeq \varphi(a) = 0$，从而有 $\varphi(x) = 0$，

$x \in J$。

(3) 由于 φ 是同态，所以有 $\varphi(a \vee b) = \varphi(a) \vee \varphi(b) = 0 \vee 0 = 0$，$a \vee b \in J$。 □

19.36

(1) 对任意同态 $\varphi : B_1 \to B_2$，由教材定理 19.24(1) 应有 $\varphi(0) = 0$，$\varphi(1) = 1$。从而必有 $\varphi(B_1) = B_2$。

易见，若 $\varphi(a) = \varphi(b) = 0$ (或 $\varphi(a) = \varphi(b) = 1$)，则有 $\varphi(a) \vee \varphi(b) = 0 \neq 1 = \varphi(a \vee b)$ (或 $\varphi(a) \wedge \varphi(b) = 1 \neq 0 = \varphi(a \wedge b)$)，从而 φ 不是同态。而当 $\varphi(a) \neq \varphi(b)$ 时，φ 是同态。

因此，从 B_1 到 B_2 的同态只有 $\varphi_1 = \{\langle 0,0\rangle, \langle a,0\rangle, \langle b,1\rangle, \langle 1,1\rangle\}$ 和 $\varphi_2 = \{\langle 0,0\rangle, \langle a,1\rangle, \langle b,0\rangle, \langle 1,1\rangle\}$。

(2) 对上题中的 φ_1，有 $B_1/\sim = \langle\{\{0,a\},\{b,1\}\}, \wedge, \vee, {}^-, \{0,a\}, \{b,1\}\rangle$。运算表如下：

$\wedge$	$\{0,a\}$	$\{b,1\}$
$\{0,a\}$	$\{0,a\}$	$\{0,a\}$
$\{b,1\}$	$\{0,a\}$	$\{b,1\}$

$\vee$	$\{0,a\}$	$\{b,1\}$
$\{0,a\}$	$\{0,a\}$	$\{b,1\}$
$\{b,1\}$	$\{b,1\}$	$\{b,1\}$

x	$\bar{x}$
$\{0,a\}$	$\{b,1\}$
$\{b,1\}$	$\{0,a\}$

对于 φ_2，只需将上述集合中的 a，b 对换即可。

19.37 注意到：

引理 19.3 *设 A, B 是两个不交的集合，则对任意 $X_1, X_2 \subseteq A$，$Y_1, Y_2 \subseteq B$，有*

$$X_1 \cup Y_1 \subseteq X_2 \cup Y_2 \iff X_1 \subseteq X_2 \text{ 且 } Y_1 \subseteq Y_2.$$

证明： 充分性显然。下面证必要性。

若 $X_1 \cup Y_1 \subseteq X_2 \cup Y_2$，则对任意 $x \in X_1$，有 $x \in X_1 \cup Y_1 \subseteq X_2 \cup Y_2$。由 $x \in A$ 和 $A \cap B = \varnothing$ 可知，$x \notin Y_2 \subseteq B$。从而必有 $x \in X_2$。这就证明了 $X_1 \subseteq X_2$。同理可证 $Y_1 \subseteq Y_2$。 □

再证原题。

证明： 由教材例 19.14 和教材定理 15.6 可知，$\langle \mathcal{P}(A \cup B), \cap, \cup, \sim, \varnothing, A \cup B\rangle$ 和 $\langle \mathcal{P}(A) \times \mathcal{P}(B), \wedge, \vee, -, \langle\varnothing,\varnothing\rangle, \langle A, B\rangle\rangle$ 都是布尔代数。

定义 $\varphi : \mathcal{P}(A) \times \mathcal{P}(B) \to \mathcal{P}(A \cup B)$，$\forall \langle X, Y\rangle \in \mathcal{P}(A) \times \mathcal{P}(B)$，令 $\varphi(\langle X, Y\rangle) = X \cup Y$。$\varphi$ 显然是映射，且为满射。

由引理 19.3 可知，φ 是单射，从而是双射。

由引理 19.3 和教材定理 19.8 可知，φ 是 $\langle \mathcal{P}(A) \times \mathcal{P}(B), \wedge, \vee\rangle$ 到 $\langle \mathcal{P}(A \cup B), \cap, \cup\rangle$ 的同构。也即，对任意 $\langle X_1, Y_1\rangle, \langle X_2, Y_2\rangle \in \mathcal{P}(A \cup B)$，有 $\varphi(\langle X_1, Y_1\rangle \wedge \langle X_2, Y_2\rangle) = \varphi(\langle X_1, Y_1\rangle) \cap \varphi(\langle X_2, Y_2\rangle)$ 和 $\varphi(\langle X_1, Y_1\rangle \vee \langle X_2, Y_2\rangle) = \varphi(\langle X_1, Y_1\rangle) \cup \varphi(\langle X_2, Y_2\rangle)$。

$\forall \langle X, Y\rangle \in \mathcal{P}(A) \times \mathcal{P}(B)$，有

$\varphi(-\langle X, Y\rangle)$

$=\varphi(\langle A - X, B - Y\rangle)$ (− 运算定义)

$=(A - X) \cup (B - Y)$ (φ 定义)

$=(A \cap \sim X) \cup (B \cap \sim Y)$ (补交转换律)

$=((A \cap \sim X) \cup B) \cap ((A \cap \sim X) \cup \sim Y)$ (分配律)

$=(A \cup B) \cap (\sim X \cup B) \cap (A \cup \sim Y) \cap (\sim X \cup \sim Y)$ (分配律)

$=(A \cup B) \cap \sim X \cap \sim Y \cap (\sim X \cup \sim Y)$ ($B \subseteq \sim X$、$A \subseteq \sim Y$、习题 1.21 结论)

$=(A \cup B) \cap \sim X \cap \sim Y$ ($\sim Y \subseteq \sim X \cup \sim Y$、习题 1.21 结论)

$$
\begin{aligned}
&=(A\cup B)\cap\sim(X\cup Y) && \text{(德·摩根律)}\\
&=(A\cup B)-(X\cup Y) && \text{(补交转换律)}\\
&=\sim(X\cup Y) && (E=A\cup B)\\
&=\sim\varphi(\langle X,Y\rangle) && (\varphi\ \text{定义})
\end{aligned}
$$

这就证明了 $\langle\mathcal{P}(A\cup B),\cap,\cup,\sim,\varnothing,A\cup B\rangle\overset{\varphi}{\cong}\langle\mathcal{P}(A)\times\mathcal{P}(B),\wedge,\vee,-,\langle\varnothing,\varnothing\rangle,\langle A,B\rangle\rangle$。 □

19.38

证明: 作 $f:B_1/{\sim}\to B_2$，$\forall[x]\in B_1/{\sim}$，令 $f([x])=\varphi(x)$。

由定义，对任意 $[x],[y]\in B_1/{\sim}$，有

$$
\begin{aligned}
&\ f([x])=f([y])\\
\iff&\ \varphi(x)=\varphi(y) && (f\ \text{定义})\\
\iff&\ x\sim y && (\sim\ \text{定义})\\
\iff&\ [x]=[y] && \text{(教材定理 2.27)}
\end{aligned}
$$

这就证明了 f 是函数，且为单射。

对任意 $y\in B_2$，由于 φ 是满射，所以存在 $x\in B_1$，使 $f([x])=\varphi(x)=y$，所以 f 是满射，从而是双射。

由于 φ 是同态，所以对 B_1 上的任何 k_i 元运算 $\circ_i$ 和任意 $x_1,x_2,\cdots,x_k\in B_1$，有

$$
\begin{aligned}
\circ_i\left(f([x_1]),f([x_2]),\cdots,f([x_{k_i}])\right)&=\circ_i(\varphi(x_1),\varphi(x_2),\cdots,\varphi(x_{k_i})) && (f\ \text{定义})\\
&=\varphi(\circ_i(x_1,x_2,\cdots,x_{k_i})) && (\varphi\ \text{是同态})\\
&=f([\circ_i(x_1,x_2,\cdots,x_{k_i})]) && (f\ \text{定义})
\end{aligned}
$$

上述关于 $\circ_i$ 的证明适用于 B_1 上的所有运算，从而证明了 f 是同构。

对任意 $x\in B_1$，由定义立即有 $f\circ g(x)=f(g(x))=f([x])=\varphi(x)$。这就证明了 f 是一个满足 $f\circ g=\varphi$ 的同构映射。

假设存在另一个同构映射 f'，满足 $f'\circ g=\varphi$。则对任意 $x\in B_1$，有

$$
\begin{aligned}
&\ f'\circ g(x)=\varphi(x) && \text{(前提)}\\
\iff&\ f'([x])=\varphi(x) && (g\ \text{定义})\\
\iff&\ f'([x])=f([x]) && (f[x]=\varphi(x))
\end{aligned}
$$

从而有 $f'=f$。这就证明了 f 是唯一的。 □

19.39 由有限布尔代数的表示定理可知，任何 8 元布尔代数都同构于 3 位逻辑代数 $\langle\{0,1\}^3,\wedge,\vee,-,000,111\rangle$，其中 $\wedge$、$\vee$ 和 $-$ 分别是按位与、按位或和按位非运算。因此，下面只需讨论 $\{0,1\}^3$ 的所有子代数即可。

由于布尔代数的子代数也是布尔代数，从而由教材定理 19.26 可知，$\{0,1\}^3$ 的子代数只能是 1、2、4 或 8 阶的。又由于子代数需要对所有运算(包括代数常元 000 和 111)封闭，所以对 $\{0,1\}^3$ 的任意子代数 B_i，必有 $000,111\in B_i$。这就是说，$\{0,1\}^3$ 不可能有 1 阶的子代数。

显然，$\{0,1\}^3$ 的 8 阶子代数只有它自身，$\{0,1\}^3$ 的 2 阶子代数只有 $\{000,111\}$。

对 $\{0,1\}^3$ 的任意 4 阶子代数 B，若有 $x\in B$，$x\neq000$，$x\neq111$，则由子代数对补运算的封闭性知，$\bar{x}\in B$。由习题 19.16 第 (1) 小题结论可知，$\bar{x}\neq x$，又由分配格的补元唯一性可知，$\bar{x}\neq000$，$\bar{x}\neq111$ (若不然，比如 $\bar{x}=111$，则 111 将有 x 和 000 两个补元，矛盾)。从而有 $B=\{000,x,\bar{x},111\}$。

反之，易于验证(完整证明见下题)，对任意 $x\in\{0,1\}^3$，$\{0,x,\bar{x},1\}$ 都是 $\{0,1\}^3$ 的一个子布尔代数。从而 $\{0,1\}^3$ 的子代数有：

$B_1 = \{000, 111\}$；

$B_2 = \{000, 001, 110, 111\}$；

$B_3 = \{000, 010, 101, 111\}$；

$B_4 = \{000, 011, 100, 111\}$；

$B_5 = \{0, 1\}^3$。

19.40

证明： 令 $X = \{0, x, \bar{x}, 1\}$。对任意 $a, b \in X$，分三种情况讨论：

情况一：若 $a = 0$ (或 $b = 0$)，则有 $a \wedge b = 0 \in X$ 和 $a \vee b = b \in X$ (或 $a \vee b = a \in X$)。

情况二：若 $a = 1$ (或 $b = 1$)，则有 $a \wedge b = b \in X$ (或 $a \wedge b = a \in X$) 和 $a \vee b = 1 \in X$。

情况三：若上述两者都不成立，则必有 $a, b \in \{x, \bar{x}\}$，此时，若 $a = b$，则 $a \wedge b = a \vee b = a = b \in X$。若 $a \neq b$，则必有 $a = \bar{b}$，从而有 $a \wedge b = 0 \in X$ 和 $a \vee b = 1 \in X$。

这就是说，对任意 $a, b \in X$，都有 $a \wedge b \in X$ 和 $a \vee b \in X$。

又因为 0 和 1 互补，x 和 $\bar{x}$ 互补，所以 X 对补运算封闭。

由于 $0, 1 \in X$，所以 X 对零元运算 0 和 1 也封闭。

这就是说，X 对 B 的所有运算都封闭，从而 X 是 B 的子布尔代数。 □

附录一　北京大学计算机系考研真题解答

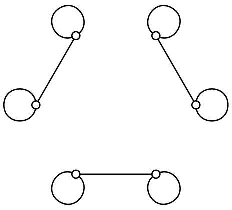
1990 年计算机数学基础

二、

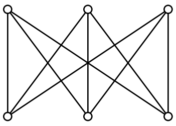
1.

(1) 由图论基本定理和每个顶点度数为 3 可知，$2m = 3n$。由题设有 $2n - 3 = m$。解得，$n = 6, m = 9$。

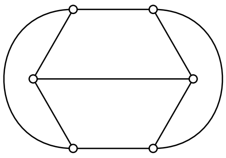
(2) 不是唯一的。例如，以下几个图都满足题目的条件。



G_1



G_2



G_3

G_1 显然与 G_2, G_3 都不同构。G_2 是二部图 $K_{3,3}$ 且不是平面图；G_3 有奇圈，且是平面图。所以 G_2 与 G_3 也不同构。

2.

(1) T 有 3 条弦，因而有 3 个基本回路：$C_b = bade$，$C_c = cde$，$C_g = gef$。

(2) 基本回路系统即为 $\{C_b, C_c, C_g\}$。

(3) 由于任意环路都可表示成基本回路的环和，且基本回路系统是线性独立的，又由于对任意环路 C，有 $C \oplus C = \varnothing$，所以只需考虑每个基本回路在环和运算式中出现 0 次或 1 次的情况即可。

从而 G 中不同的环路有：

$\varnothing$，
$C_b = bade$，
$C_c = cde$，
$C_g = gef$，
$C_b \oplus C_c = bac$，
$C_b \oplus C_g = badgf$，
$C_c \oplus C_g = cdgf$，
$C_b \oplus C_c \oplus C_g = bacegf$。

G 的圈空间(即环路空间)为 $\{\varnothing, C_b, C_c, C_g, C_b \oplus C_c, C_b \oplus C_g, C_c \oplus C_g, C_b \oplus C_c \oplus C_g\}$。

1991 年计算机数学基础

七、

1.

(1) $(A-C)\cup B=A\cup B$ 的充分必要条件是 $A\cap C\subseteq B$。(证明见 1998 年第四题第 1 小题)。

(2) 首先证明如下结论[1]。

结论一：集合 A 满足方程 $\cup A=A$ 的充分必要条件是：A 是传递集且对任意 $x\in A$，存在 $y\in A$，使得 $x\in y$。

证明：必要性。若 $\cup A=A$，则 $\cup A\subseteq A$。由教材定理 4.10 可知，A 是传递集。另一方面，由于 $A=\cup A$，从而对任意 $x\in A$，有 $x\in\cup A$，由 $\cup A$ 定义就有，存在 $y\in A$，使得 $x\in y$。

充分性。若 A 是传递集，则有 $\cup A\subseteq A$。同时，对任意 $x\in A$，由于存在 $y\in A$，使得 $x\in y$，所以有 $x\in\cup A$。由 x 的任意性可知 $A\subseteq\cup A$。从而就有 $\cup A=A$。 □

由结论一可知：

① $A=\varnothing$ 是方程 $\cup A=A$ 的一个解，且方程 $\cup A=A$ 不存在其它有限解。

证明：由定义立即有 $A=\varnothing$ 是方程 $\cup A=A$ 的解。

下面说明，若 A 是 $\cup A=A$ 的解且 $A\neq\varnothing$，则 A 必是无限集。

若 $A\neq\varnothing$，则存在 $x_0\in A$。由结论一可知，存在 $x_1\in A$，使得 $x_0\in x_1$，再由结论一可知，存在 $x_2\in A$，使得 $x_1\in x_2$，从而存在集合列 $x_0,x_1,\cdots$，满足 $x_i\in x_{i+1}\wedge x_i\in A(i=0,1,\cdots)$。由正则公理[2] 可知，这些 x_i 是互异的。这就是说，A 中至少有可数无穷个元素，从而 A 是无穷集。 □

② 若 A 是极限序数，则 A 是方程的一个解(极限序数的定义见教材定义 6.8)。

证明：若 A 为一极限序数，则由序数性质知，A 是传递集，所以有 $\cup A\subseteq A$。下面证明 $A\subseteq\cup A$。

首先证明，对任意 $x\in A$，必有 $x^+\in A$：若不然，由序数三歧性有 $A\in x^+$ 或 $A=x^+$。若 $A\in x^+=x\cup\{x\}$，则有 $A=x$ 或 $A\in x$，这与 $x\in A$ 矛盾。若 $A=x^+$，则与 A 是极限序数矛盾。这就证明了对任意 $x\in A$，有 $x^+\in A$。 另一方面，由 x^+ 定义知，$x\in x^+$，从而对任意 $x\in A$，有 $x\in x^+\in A$，$x\in\cup A$。即 $A\subseteq\cup A$。

综合得，$A=\cup A$。 □

③ 对任意传递集 B，$A=B\cup\{B,\{B\},\{\{B\}\},\cdots\}$ 是方程的一个解。

证明：由结论一立即可得。 □

上面已经给出 $\cup A=A$ 的一些解的形式，但仍不能证明是否 $\cup A=A$ 的所有解都具有上述三种形式的一种。

---

[1] 感谢北京大学计算机系刘田教授给予的提示!

[2] 正则公理可以表述为“若 S 为一个非空集合，则必然存在 $x\in S$，使得 $x\cap S=\varnothing$”。由正则公理可以证明：不存在集合 $x_0,x_1,\cdots,x_n$，满足 $x_0\in x_1\in x_2\in\cdots\in x_n\in x_0$。有关内容详见《公理集合论导引》(张锦文)第一章第11节。

(3) 可以定义 16 个不同的二元关系，其中有 3 个不同的偏序关系，2 个不同的等价关系。

(4) $\operatorname{card} A \leq \operatorname{card} B$。

(5) 满足交换律、结合律和消去律。单位元为 $\varnothing$。

(6) G 共有 4 个子群：

$H_1 = \langle 0 \rangle = \{0\}$；

$H_2 = \langle 4 \rangle = \{0, 4\}$；

$H_3 = \langle 2 \rangle = \{0, 2, 4, 6\}$；

$H_4 = \langle 1 \rangle = G$；

其中平凡的真子群为 $H_1 = \{0\}$。

(7) $a \in I, a \wedge 0 = 0$。

2.

(1) $f(\mathbb{R}_0(t)) = f(\mathbb{R}) = \{x^2 \mid x \in \mathbb{R}\} = \{x \mid x \in \mathbb{R} \wedge x \geq 0\} = \mathbb{R} - \mathbb{R}^-$。

(2) $f^{-1}(\mathbb{R}_4(t)) = \mathbb{R}_2(t)$。

(3) $f^{-1}(\{(t^2 + 2t + 1)\}) = \{(t + 1)\}$。

(4) $f^{-1}(f(\{(t-1), (t^2-1)\})) = f^{-1}(\{(t^2 - 2t + 1), (t^4 - 2t^2 + 1)\}) = \{(1-t), (t-1), (1-t^2), (t^2-1)\}$。

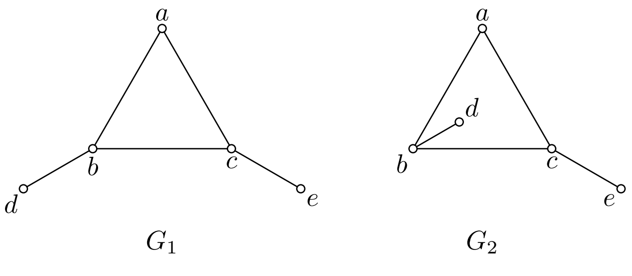
八、

1.

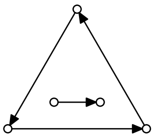
(1) 正确。无回路的连通图是树，树的边数为顶点数减一。

(2) 不正确。当 G 不连通时，G^{**} 是连通的(任何图的对偶图都是连通的)，从而它们不同构。例如：设 G 为 2 阶零图，则 G^* 是 1 阶零图，从而 G^{**} 也是 1 阶零图，与 G 不同构。

(3) 不正确。例如，下图中 $G_1 \cong G_2$，但 G_1^* 的度数列是 7 3，而 G_2^* 的度数列是 5 5，两者显然不同构。



(4) 不正确。反例见下图。



(5) 不正确。$K_{3,3}$ 删除一条边后，只有 8 条边，不满足极大平面图的必要条件 $m = 3n - 6 = 12$。

2.

证明：

证法一：

由于 T 是树，所以 $m = n - 1$。又由于 T 是连通的，所以每个顶点的度数至少为 1。反设 T 中至多有 $k - 1$ 片树叶，则 G 中至少有 $n - k + 1$ 个顶点的度数大于等于 2，且至少有一个顶点的

度数等于 $\Delta(G)$，从而 $2m = \sum\limits_{v \in G} d(v) \geq \Delta(G) + (k-1) + 2(n-k) = 2n-1 > 2n-2$。矛盾。

证法二：

设 v 为 T 中度数最大的顶点，记 v 的邻域 $N(v) = \{v_1, v_2, \cdots, v_k\}$。令 Γ_i 为以 vv_i 为起点的初级路径，朝远离 v 的方向不断扩展此路径，直到无法扩展为止。此时 Γ_i 的终点 v_i' 必是为叶(否则，若 $d(v_i') \geq 2$，则 v_i' 至少与 Γ_i 上的两个顶点相邻，从而可以构成圈，这与 T 是树矛盾)，且对 $1 \leq i, j \leq k$，若 $i \neq j$，则 $v_i' \neq v_j'$ (否则又可以构成圈，矛盾)，从而 T 中至少有 k 片树叶。 □

九、

证明： 取 $\varphi : G \to H/H_1$，$\forall x \in G$，令 $\varphi(x) = H_1\sigma(x)$。

φ 显然函数，且由于 σ 是满同态，所以对任意 $H_1y \in H/H_1$，存在 $x \in G$，使得 $\sigma(x) = y$，于是有 $\varphi(x) = H_1y$。从而 φ 也是满射。

对任意 $a, b \in G$，

$$
\begin{aligned}
\varphi(ab) &= H_1\sigma(ab) && (\varphi \text{ 定义}) \\
&= H_1\sigma(a)\sigma(b) && (\sigma \text{ 是同态}) \\
&= H_1H_1\sigma(a)\sigma(b) && (H_1H_1 = H_1) \\
&= H_1\sigma(a)H_1\sigma(b) && (H_1\sigma(a) = \sigma(a)H_1) \\
&= \varphi(a)\varphi(b) && (\varphi \text{ 定义})
\end{aligned}
$$

从而 φ 是同态，且 $\varphi(G) = H$。

对任意 $x \in G$，

$$
\begin{aligned}
& x \in \ker \varphi \\
\iff & \varphi(x) = H_1 && (\ker \text{ 定义}) \\
\iff & H_1\sigma(x) = H_1 && (\varphi(x) = H_1\sigma(x)) \\
\iff & \sigma(x) \in H_1 && (\text{教材定理 } 17.22) \\
\iff & x \in G_1 && (G_1 = \sigma^{-1}(H_1))
\end{aligned}
$$

从而 $G_1 = \ker \varphi$。由群同态基本定理知，$G/G_1 \cong H/H_1$。 □

1992 年计算机数学基础

11.

(1) $A \oplus A = \varnothing$，$\operatorname{card} A = 2$。

(2) A 上可以定义 16 个二元关系，其中有 4 个自反的关系，4 个反自反的关系，8 个对称的关系，12 个反对称的关系，2 个等价关系，3 个偏序关系。

(3) A^A 中有 4 个函数，其中有 2 个是满射的，2 个是单射的，2 个是双射的。

(4) A 上可以定义 4 个一元运算，16 个二元运算。

(5) 以 A 的元素作为群的元素，可以构成 1 个不同构的群。以 A 的元素作为格的元素，可以构成 1 个不同构的格。

12.

证明: 充分性。首先，由逆元的唯一存在性可知，f 是函数且为单射。又由于 $\forall x \in G, x = (x^{-1})^{-1}$，所以 $x = f(x^{-1}) \in \operatorname{ran} f$，从而 f 是双射。

若 G 是交换群，则对任意 $x, y \in G$，

$$\begin{aligned}
f(xy) &= (xy)^{-1} && (f\text{ 定义})\\
&= y^{-1}x^{-1} && (\text{教材定理 17.2})\\
&= x^{-1}y^{-1} && (G\text{ 是交换群})\\
&= f(x)f(y) && (f\text{ 定义})
\end{aligned}$$

这就证明了 f 是自同构。

必要性。若 f 是自同构，则对任意 $x, y \in G$，

$$\begin{aligned}
xy &= ((xy)^{-1})^{-1} && (\text{教材定理 17.2})\\
&= f((xy)^{-1}) && (f\text{ 定义})\\
&= f(y^{-1}x^{-1}) && (\text{教材定理 17.2})\\
&= f(y^{-1})f(x^{-1}) && (f\text{ 是自同构})\\
&= (y^{-1})^{-1}(x^{-1})^{-1} && (f\text{ 定义})\\
&= yx && (\text{教材定理 17.2})
\end{aligned}$$

从而 G 是交换群。 □

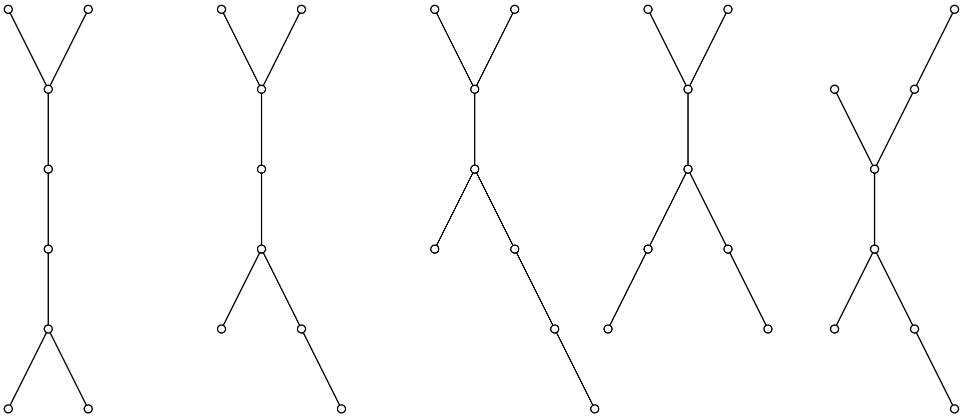
13.

(1) a, c, d 能构成无向图的度数列。

(2) c, d 能构成无向简单图的度数列。

(3) c 能构成无向树的度数列(由于无向树的边数等于顶点数减一，无向树的度数列应满足度数和的一半等于项数减一)。

(4) 以 c 为度数列的树有 5 个：



(5) d 对应的图 G 的圈秩为 $m-n+1=10-10+1=1$，割集秩为 $n-1=9$。

14. G 的对偶图 G^* 为欧拉图当且仅当对 G 中的每个面的次数都是偶数。

证明：

G 中的每个面的次数都是偶数

$\Longleftrightarrow$ G^* 中的每个顶点的次数都是偶数 (教材定理 11.15)

$\Longleftrightarrow$ G^* 中的每个顶点的次数都是偶数 $\wedge 1$ (命题逻辑同一律)

$\Longleftrightarrow$ G^* 中的每个顶点的次数都是偶数 $\wedge$ G^* 是连通的 (对偶图性质)

$\Longleftrightarrow$ G^* 是欧拉图 (教材定理 8.1)

$\square$

1993 年计算机数学基础

四、

1.

(1) K_5 和 K_6 中都有且仅有 2 条边不重的哈密顿回路。

(2) 6 棵(最大度为 $2, 4, 5$ 的各一棵，最大度为 3 的 3 棵)。

(3) 3 个(含 K_5 的 1 个，含 $K_{3,3}$ 的 2 个)。

2.

证明: 考虑 G 的生成树 T，由于任何非平凡的无向树至少有两片树叶，所以 T 中存在树叶 $v_1, v_2 \in V(G)$，$v_1 \neq v_2$。由于 v_1, v_2 是树叶，所以 $T - \{v_1, v_2\}$ 仍是连通的，从而 $G - \{v_1, v_2\}$ 也是连通的。 □

3. 可以安排。

证明: 按如下方式作图 $G = \langle V_1 \cup V_2, E \rangle$：令 $V_1 = \{u_i \mid i = 1, \cdots, 7\}$ 为 7 门课程对应顶点的集合，$V_2 = \{v_i \mid i = 1, \cdots, 7\}$ 为 7 名教员对应顶点的集合。令 $(u_i, v_j) \in E(G)$ 当且仅当 v_j 对应的教员可以教 u_i 对应的课程。

显然，$G = \langle V_1, V_2, E \rangle$ 是二部图。由题设，V_1 中每个顶点至少关联 3 条边，V_2 中每个顶点至多关联 3 条边。由教材定理 13.12 知，G 中存在完美匹配。而 G 中完美匹配所对应的安排方案即为所求。 □

五、

1.

(1) 不正确。(充要条件是 $B \subseteq A$)。

(2) 不正确。($\mathcal{P}(A) - A = \{\{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}$)。

(3) 正确。(令 $R = I_A$ 即可)。

(4) 正确。($\langle 2x + y, 6 \rangle = \langle 5, x + y \rangle$ 当且仅当 $2x + y = 5 \wedge x + y = 6$)。

(5) 不正确。($M_n(\mathbb{R})$ 中有不可逆元)。

(6) 不正确。(A 对乘法不封闭，不构成代数系统)。

(7) 正确。(教材定理 19.21)。

2.

(1) 由于 $0 \in \mathbb{N}$ 但 $0 \notin \operatorname{ran} f$，所以 f 不是满射。由于 $f(\langle 0, 1 \rangle) = f(\langle 1, 0 \rangle) = 2$，所以 f 不是单射。f 自然也不是双射。

$f(\mathbb{N} \times \{1\}) = \{x + 1 + 1 \mid x \in \mathbb{N}\} = \{x + 2 \mid x \in \mathbb{N}\} = \mathbb{N} - \{0, 1\}$。

(2) 由有序对性质知，对任意 $x, y \in \mathbb{N}$，$\langle x, x + 1 \rangle = \langle y, y + 1 \rangle \Rightarrow x = y$，所以 f 是单射。由于

$\langle 0,2\rangle \in \mathbb{N}\times\mathbb{N}$ 但 $\langle 0,2\rangle \notin \operatorname{ran} f$，所以 f 不是满射，从而也不是双射。

$f\restriction\{0,1,2\} = \{\langle 0,\langle 0,1\rangle\rangle,\langle 1,\langle 1,2\rangle\rangle,\langle 2,\langle 2,3\rangle\rangle\}$。

3.

证明： 记 $\kappa = \operatorname{card} B, \mu = \operatorname{card}(A-B)$，由于 $B\cap(A-B)=\varnothing$，所以由基数加法的定义知，$\kappa+\mu = \operatorname{card}(B\cup(A-B)) = \operatorname{card} A = \lambda$。

另一方面，由于 $\kappa \geq \aleph_0$，由教材定理 5.24 知，$\lambda = \kappa+\mu = \max\{\kappa,\mu\}$ (教材定理 5.24 要求“其中较大的为无穷基数”，本题已知 κ 为无穷基数，若 $\mu \leq \kappa$，则 κ 就是“较大的”“无穷基数”，若 $\mu > \kappa$，则 μ 就是“较大的”“无穷基数”，从而定理的前提总成立)。由于已知 $\kappa < \lambda$，从而 $\kappa \neq \max\{\kappa,\mu\} = \lambda$，所以必有 $\operatorname{card}(A-B) = \mu = \max\{\kappa,\mu\} = \lambda$。 □

4. $|x| = 3$。

证明： 首先，由于 y 是二阶元，所以有 $y^{-1} = y$。同时：

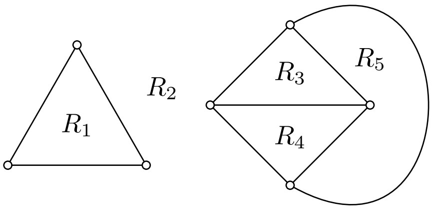
$$
\begin{aligned}
& yxy^{-1} = x^2 \\
\iff & yx = x^2y && \text{(右乘 } y\text{)} \\
\iff & x = y^{-1}x^2y && \text{(左乘 } y^{-1}\text{)} \\
\implies & x^2 = (y^{-1}x^2y)(y^{-1}x^2y) && \text{(两边取平方)} \\
\iff & x^2 = y^{-1}x^4y && (yy^{-1} = e) \\
\iff & x^2 = yx^4y^{-1} && (y = y^{-1})
\end{aligned}
$$

从而有 $yx^4y^{-1} = x^2 = yxy^{-1}$。由消去律知 $x^3 = e$。从而 $|x| \mid 3$。因为 x 不是单位元，所以 $|x| \neq 1$，因此只能有 $|x| = 3$。 □

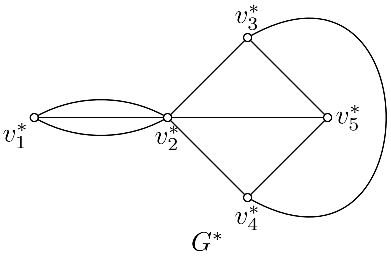
1994 年计算机数学基础

四、

1.　由题意可求得 G 和 G^*。



G



G^*

由于 G^* 中存在奇数度顶点 $v_1^*, v_3^*, v_4^*, v_5^*$，所以 G^* 不是欧拉图。

由于 v_1^* 只与 v_2^* 相邻，所以 v_1^* 若出现在某个回路 C 中，则 v_1^* 的两侧都只能是 v_2^*，当 $|C| > 2$ 时，C 不是圈。从而 G^* 中不可能存在哈密顿圈。(另证：令 $V_1^* = \{v_2^*\}$，则 $p(G^* - V_1^*) = 2 > |V_1^*|$，由教材定理 8.6 知，$G^*$ 不是哈密顿图)。

2.　先求邻接矩阵和 $B_i = \sum\limits_{k=1}^{i} A^k$。

$$A = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$A^2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 2 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & 2 & 0 \end{pmatrix} \qquad A^3 = \begin{pmatrix} 2 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 2 & 0 \\ 2 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 4 \end{pmatrix} \qquad A^4 = \begin{pmatrix} 0 & 4 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 4 \\ 0 & 4 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 4 \\ 4 & 0 & 4 & 0 & 0 \end{pmatrix}$$

$$B_2=\begin{pmatrix}0&1&0&1&2\\1&0&1&0&1\\0&1&0&1&2\\1&0&1&0&1\\1&2&1&2&0\end{pmatrix}\qquad B_3=\begin{pmatrix}2&1&2&1&2\\1&2&1&2&1\\2&1&2&1&2\\1&2&1&2&1\\1&2&1&2&4\end{pmatrix}\qquad B_4=\begin{pmatrix}2&5&2&5&2\\1&2&1&2&5\\2&5&2&5&2\\1&2&1&2&5\\5&2&5&2&4\end{pmatrix}$$

(1) v_2 到 v_5 共有 $b_{25}^{(4)}=5$ 条长度小于等于 4 的通路。

(2) 长度为 3 的通路有 $\sum\limits_{1\le i,j\le 5} a_{ij}^{(3)}=20$ 条，其中有 $\sum\limits_{i=1}^{5} a_{ii}^{(3)}=12$ 条是回路。

(3) 由于 B_3 中每一项皆大于 0，所以 D 是强连通的。

3.

(1)

证明： 反设 G 不连通，则 G 至少有两个连通分支。从而必然有顶点数小于等于 $\dfrac{n}{2}$ 的连通分支 $G[V_i]$。设 $v\in G[V_i]$，则由 G 是简单图和 $d(v)\ge\dfrac{n}{2}$ 知，$|V_i|\ge\dfrac{n}{2}+1$，矛盾。 □

(2)

证明： 由于 G 是简单图，从图中删除一个顶点至多使 G 中其它的顶点减少一度，对任意 $V_1\subseteq V(G)$，若 $|V_1|=k-1$，则 $\delta(G-V_1)\ge\delta(G)-(k-1)=\dfrac{n-k+1}{2}$，而 $|G-V_1|=n-k+1$。由第 (1) 小题结论知，$G-V_1$ 是连通的。从而 $\kappa(G)\ge k$，G 是 k-连通的。 □

五、

1. 不成立。

2. 不成立。(当 $A=\varnothing$ 时，对任意 B,C 都有 $A\times B=A\times C=\varnothing$)。

3. 不成立。(显然对全域关系 E_A 有 $E_A^2=E_A$，但当 $|A|\ge 2$ 时 $E_A\ne I_A$)。

4. 不成立。(f^{-1} 未必是全函数，从而 f^{-1} 未必属于 $B\to A$；若将题中"$f^{-1}:B\to A$"改为"$f^{-1}:B\mathrel{+\!\!\!\!\rightarrow}A$"，则命题成立)。

5. 成立。(同态映射保持运算的交换律)。

6. 成立。

7. 成立。(任何代数系统都是它自身的子代数)。

8. 不成立。(积代数未必保持消去律)。

六、

1.

(1) 不是单射。例如，$f(\langle 1,0\rangle)=f(\langle 0,1\rangle)=1$。

(2) 不是满射。例如，$3\in\mathbb{N}$ 但 $3\notin\operatorname{ran} f$。

(3) $f^{-1}(0)=\{\langle 0,0\rangle\}$。(注意，$f^{-1}(0)$ 是 $\operatorname{dom} f$ 的一个子集而不是一个元素，$f^{-1}(0)=\{\langle 0,0\rangle\}\ne\langle 0,0\rangle$)。

(4) $f\upharpoonright\{\langle 0,0\rangle,\langle 1,2\rangle\}=\{\langle\langle 0,0\rangle,0\rangle,\langle\langle 1,2\rangle,5\rangle\}$。

2.

(1)

证明： 自反性。对任何 $f\in B^A, x\in A$，有 $f(x)\preccurlyeq f(x)$，从而有 fRf。所以 R 是自反的。

传递性。对任何 $f,g,h\in B^A$，若 $fRg\wedge gRh$，则对所有 $x\in A$，有 $f(x)\preccurlyeq g(x)\wedge g(x)\preccurlyeq h(x)$，由 $\preccurlyeq$ 关系的传递性，有 $f(x)\preccurlyeq h(x)$，从而有 fRh。所以 R 是传递的。

反对称性。对任意 $f, g \in B^A$，若 $fRg \wedge gRf$，则对所有 $x \in A$，有 $f(x) \preccurlyeq g(x) \wedge g(x) \preccurlyeq f(x)$，从而有 $f(x) = g(x)$。由 x 的任意性知，$f = g$。所以 R 是反对称的。

这就证明了 R 是偏序关系。 □

(2) $\langle B^A, R\rangle$ 存在最大元当且仅当 $\langle B, \preccurlyeq\rangle$ 存在最大元。若 $\langle B, \preccurlyeq\rangle$ 中存在最大元 m，则常数函数 $f : A \to B, \forall x \in A, f(x) = m$ 就是 $\langle B^A, R\rangle$ 的最大元。

证明： 充分性。若 $\langle B, \preccurlyeq\rangle$ 存在最大元 m，则取 $f : A \to B$，对所有 $x \in A$，令 $f(x) = m$。显然，对任意 $g \in B^A$，$x \in A$，都有 $g(x) \preccurlyeq f(x) = m$，从而有 gRf。因此，$\langle B^A, R\rangle$ 有最大元 f。

必要性。反设 $\langle B, \preccurlyeq\rangle$ 不存在最大元，则对任意 $a \in A, f \in B^A$，必存在 $b \in B$，使得 $b \not\preccurlyeq f(a)$ (否则 $f(a)$ 将成为 B 的最大元)。令 $g : A \to B, \forall x, g(x) = b$，则 $g(a) \not\preccurlyeq f(a)$，从而 $g \not R f$，f 不是最大元。由 f 的任意性知，$\langle B^A, R\rangle$ 无最大元。 □

七、

证明： 充分性。若 G 为素数，则由 Lagrange 定理知，G 没有非平凡的子群。从而 G 是单群。

必要性。设 G 为单群。任取 G 中一个非单位元 $a \in G$ (本题应假定 G 是非平凡的，否则若 $G = \{e\}$，则 G 也是单群，但 $|G| = 1$，不是素数)，则由于 $\langle a\rangle$ 是 G 的正规子群(因为 G 是 Abel 群，所以 G 的一切子群都是正规的)，且 a 不是单位元，所以 $|\langle a\rangle| = |a| > 1$，$\langle a\rangle \neq \{e\}$。由单群定义知，必有 $\langle a\rangle = G$。从而 $G = \{a^k \mid k \in \mathbb{Z}\}$ 是由 a 生成的循环群。假若 G 不是素数阶的，就存在 $k \bigm| |G|, 1 < k < |G|$，而 $1 < |\langle a^k\rangle| = |a^k| = \dfrac{|G|}{k} < |G|$，从而 $\langle a^k\rangle$ 是 G 的一个非平凡的正规子群，矛盾。 □

1995 年计算机数学基础

三、

1.

(1) $\kappa = 2$；

(2) $\lambda = 3$；

(3) $\chi = 4$；

(4) 生成树中有 9 条树枝和 10 条弦。

2. 2 个(由于任何非平凡的树至少有 2 片树叶，而 G 的生成树上的树叶显然都不是割点，所以至少有 2 个非割点。考虑 G 恰为一条初级通路的情况，可知这个下界是 tight 的)。

3. 6 个。

4. 3 个(原式等价于 $(\neg p \vee q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (\neg p \vee \neg q \vee r)$)。

5. $\langle 1, 0 \rangle$。

6.

(1) $P_n^m = \dfrac{n!}{(n-m)!}$ 个。

(2) $n!\left\{ {m \atop n} \right\}$ 个，其中 $\left\{ {m \atop n} \right\}$ 为第二类 Stirling 数。

四、

2.

证明: 由于 $R_1 = R \cap B \times B \subseteq B \times B$，所以 R_1 是 B 上的二元关系。下面证明 R_1 是偏序关系。

自反性。对任意 $b \in B$，有 $\langle b, b \rangle \in R$ 和 $\langle b, b \rangle \in B \times B$，从而有 $\langle b, b \rangle \in R_1$。因此，$R_1$ 是自反的。

传递性。对任意 $\langle a, b \rangle, \langle b, c \rangle \in R_1$，有 $\langle a, b \rangle, \langle b, c \rangle \in R$，从而由 R 的传递性有 $\langle a, c \rangle \in R$，又由 $\langle a, b \rangle, \langle b, c \rangle \in R_1 \subseteq B \times B$ 知 $a, b, c \in B$，从而 $\langle a, c \rangle \in B \times B$。从而有 $\langle a, c \rangle \in R_1$。因此，$R_1$ 是传递的。

反对称性。对任意 $a, b \in A$，若 $\langle a, b \rangle \in R_1 \subseteq R$ 且 $\langle b, a \rangle \in R_1 \subseteq R$，则由 R 的反对称性知，$a = b$。因此，R_1 是反对称的。

这就证明了 R_1 是 B 上的偏序关系。 □

3.

证明: 首先证明存在 $a \in G$，使得 $a^{-1} \neq a$。若不然，则对任意 $a, b \in G$，都有 $a = a^{-1}, b = b^{-1}$，从而：

$$aabb = aa^{-1}bb^{-1} \qquad (a^{-1} = a, b^{-1} = b)$$

$$
\begin{aligned}
&= e && (aa^{-1} = bb^{-1} = e)\\
&= (ab)(ab)^{-1} && ((ab)(ab)^{-1} = e)\\
&= abab && ((ab)^{-1} = ab)
\end{aligned}
$$

由消去律，有 $ab = ba$。由 a, b 的任意性知，G 是交换群。矛盾。

上面证明了存在 $a \in G$，使得 $a^{-1} \neq a$。令 $c = a, d = a^{-1}$，则有 $c \neq d$，但 $cd = dc = e$。 □

4.

证明： 令 $H = G_1 \oplus G_2$，对任意 $v_i \in V(H)$，设 v_i 在 G_1 和 G_2 中的度数分别为 $a_i = |N_{G_1}(v_i)|$ 和 $b_i = |N_{G_2}(v_i)|$。由环和运算的定义和容斥原理知，$d_H(v_i) = |N_H(v_i)| = |N_{G_1}(v_i) \oplus N_{G_2}(v_i)| = a_i + b_i - 2|N_{G_1}(v_i) \cap N_{G_2}(v_i)|$，由于 G_1 和 G_2 是欧拉图，所以 a_i, b_i 是偶数，从而 $d_H(v_i)$ 也是偶数。

设 V_k 是 H 的任意连通分支，下面证明对任意顶点 $v_i \in V_k$ 都有 $d_{H[V_k]}(v_i) = d_H(v_i)$。

若不然，就存在边 $(v_i, v_j) \in E(H)$，但 $(v_i, v_j) \notin E(H[V_k])$，由于 $H[V_k]$ 是由顶点集 V_k 生成的子图，所以仅当 $v_j \notin V_k$ 时才会有这种情况。但由于 v_j 与 v_i 间有边，而 v_i 与 V_k 中其它顶点有通路，所以 v_j 与 V_k 中各顶点都有通路。由连通分支定义应有 $v_j \in V_k$。矛盾。这就证明了对任意 $v_i \in V_k$，都有 $d_{H[V_k]}(v_i) = d_H(v_i)$。

由此可知，对 H 中的任意连通分支 $H[V_k]$，V_k 中每个顶点的度数都是偶数，从而 $H[V_k]$ 是欧拉图。 □

1996 年计算机数学基础

三、

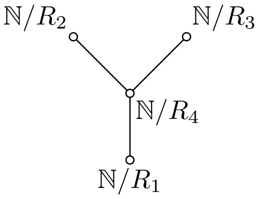
1. $\mathbb{N}/R_1=\{\{n\}\mid n\in\mathbb{N}\}$；

$\mathbb{N}/R_2=\{\{2k\mid k\in\mathbb{N}\},\{2k+1\mid k\in\mathbb{N}\}\}$；

$\mathbb{N}/R_3=\{\{3k+j\mid k\in\mathbb{N}\}\mid j=0,1,2\}$；

$\mathbb{N}/R_4=\{\{6k+j\mid k\in\mathbb{N}\}\mid j=0,1,2,3,4,5\}$。

2.



3. $f_1(H)=H$；

$f_2(H)=\{0\}$；

$f_3(H)=\{0,1,2\}$；

$f_4(H)=\{0,2,4\}$。

五、

1.

(1) $\ker\varphi_1=G$。由于 $|G|\geq 2$，所以 φ_1 既不是单射也不是满射，当然也不是同构。

(2) $\ker\varphi_2=\{0\}$。由于 $1\in\mathbb{Z}$ 但 $1\notin\varphi_2(\mathbb{Z})$，所以 φ_2 不是满射，从而不是同构。

(3) $\ker\varphi_3=\{0\}$。由于指数函数是单射，且对任意 $x\in\mathbb{R}^+$，有 $\ln x\in\mathbb{R}$，且 $x=\varphi_3(\ln x)$，所以 φ_3 是满射，从而是同构映射。

2.

证明： 由于 $e\in A, e\in B$，所以 $e=ee\in AB$，AB 非空。

由于 A 是正规子群，所以对任意 $b\in B$，有 $Ab=bA$。从而 $BA=\{bA\mid b\in B\}=\{Ab\mid b\in B\}=AB$。

对任意 $x,y\in AB$，存在 $a_1,a_2\in A,b_1,b_2\in B$，使 $x=a_1b_1,y=a_2b_2$，从而 $xy^{-1}=a_1b_1(a_2b_2)^{-1}=a_1b_1b_2^{-1}a_2^{-1}$，而 $a_1b_1b_2^{-1}\in AB=BA$，所以存在 $a_3\in A,b_3\in B$，使得 $a_1b_1b_2^{-1}=b_3a_3$。于是有 $xy^{-1}=b_3a_3a_2^{-1}\in BA=AB$。

由子群判定定理二，AB 是 G 的子群。 □

六、

1.

(1) $\kappa = 2$；

(2) $\xi = 5$；

(3) $\alpha_0 = 4$；

(4) $\chi = 3$；

(5) $\beta_1 = 3$。

2.

证明： 反设 G 中不存在度数小于等于 3 的顶点。则由图论基本定理知，$2m = \sum\limits_{i=1}^{n} d(v_i) \geq 4n$，从而有 $m \geq 2n$。

另一方面，由于 G 是平面图，且不含长度为 3 的边，从而 G 中任何面的次数都至少为 4，代入公式 $m \leq \dfrac{l}{l-2}(n-2)$，就有 $m \leq 2n-4$。矛盾。 □

1997 年计算机数学基础

三、

3.　由于 $m=17$，所以树上共有 18 个顶点。题目中已给出 17 个顶点的度数，故，唯一度数未知的顶点即是树根。设树根的度数为 d，则由图论基本定理知 $d+4\cdot 4+1\cdot 3+12=2m=34$，解得，$d=3$。因此，树根的度数为 3。

4.

证明：要证 $\lambda(G^*)\geq 2$，即要证 G^* 中无桥。由于 G 是连通图，所以 G^* 的对偶图 $G^{**}\cong G$。反设 G^* 中有桥 e^*，则由对偶图的性质知，在 G^{**} 中与 e^* 对应的边 e^{**} 是环(这是因为，若 e^* 为桥，则 G^*-e^* 是不连通的，因此，e^* 的两侧都是 G^* 的外部面，而外部面是唯一的，从而 e^{**} 是环)，这与 $G^{**}\cong G$ 是简单图矛盾。这就证明了 G^* 中无桥，从而有 $\lambda(G^*)\geq 2$。

由于极大平面图的每个面的次数皆为 3，所以对任意 $v_i^*\in G^*$，有 $d_{G^*}(v_i^*)=\deg(R_i)=3$。从而 G^* 是 3-正则的。□

四、

1.　$R=\{\langle 0,4\rangle,\langle 3,3\rangle,\langle 6,2\rangle,\langle 9,1\rangle,\langle 12,0\rangle\}$，从而 $R^2=\{\langle 3,3\rangle,\langle 12,4\rangle\}$。

2.　若 A 为无穷集，则 B 中无极大元和最大元，B 中的极小元集合为 $\{x\mid x\in P(A)\wedge|x|=1\}$。若 A 为有穷集，记 $n=|A|$，则 B 中极大元的集合为 $\{x\mid x\in P(A)\wedge|x|=n-1\}$，极小元的集合为 $\{x\mid x\in P(A)\wedge|x|=1\}$，$B$ 中无最大元。

3.　$G(1)=\{1,2\},G(2)=\{3\},G(3)=\varnothing$，可见 G 是单射。但 G 不是满射(例如，$\{1\}\in\mathcal{P}(A)$ 但 $\{1\}\notin\operatorname{ran}G$)，从而不是双射。$\operatorname{ran}G=\{\varnothing,\{1,2\},\{3\}\}$。

4.

证明：由理想的定义可知，I 对 $\vee$ 运算封闭。

对任意 $a,b\in I$，由 $\wedge$ 运算定义有 $a\wedge b\in A$ 且 $a\wedge b\preccurlyeq a$，从而由理想的定义知，$a\wedge b\in I$。所以 I 对 $\wedge$ 运算也封闭。

这就证明了 I 是子格。□

5.

(1)

证明：对任意 $x,y\in G$ 有：

$$
\begin{aligned}
&\quad xax^{-1}=yay^{-1} \\
&\Longleftrightarrow ax^{-1}y=x^{-1}ya &&\text{(左乘 } x^{-1}\text{、右乘 } y\text{)}\\
&\Longleftrightarrow x^{-1}y\in N(a) &&(N(a)\text{ 定义})
\end{aligned}
$$

$\iff N(a)x = N(a)y$ (教材定理 17.22)

从而 H 中不同的元素数恰为 $G/N(a)$ 中不同的陪集数。这就证明了 $|H| = [G : N(a)]$。 □

(2)

证明： 由于 $N(a)$ 和 C 都是群，且 C 是 $N(a)$ 的子群。由 Lagrange 定理知，$|N(a)| = [N(a) : C]|C|$，从而：

$$\begin{aligned}
|H| &= [G : N(a)] && \text{(第 (1) 小题结论)}\\
&= \frac{|G|}{|N(a)|} && \text{(Lagrange 定理)}\\
&= \frac{|G|}{[N(a) : C]|C|} && (|N(a)| = [N(a) : C]|C|)\\
&= \frac{n}{[N(a) : C]m} && (|G| = n, |C| = m)\\
&\mid \frac{n}{m} && \text{(}[N(a) : C]\text{ 是整数)}
\end{aligned}$$

□

1998 年计算机数学基础

三、

3. 首先计算邻接矩阵：

$$A=\begin{pmatrix}1&1&1&0\\1&0&1&0\\0&0&0&1\\1&1&0&0\end{pmatrix},\quad A^2=\begin{pmatrix}2&1&2&1\\1&1&1&1\\1&1&0&0\\2&1&2&0\end{pmatrix},\quad A^3=\begin{pmatrix}4&3&3&2\\3&2&2&1\\2&1&2&0\\3&2&3&2\end{pmatrix}$$

(1) G 中共有 $\sum\limits_{1\leq i,j\leq 4} a_{ij}^{(3)}=35$ 条长度等于 3 的通路，$\sum\limits_{1\leq i} a_{ii}^{(3)}=10$ 条长度等于 3 的回路。

(2) 从 v_1 到 v_3 共有 $a_{13}^{(1)}+a_{13}^{(2)}+a_{13}^{(3)}=6$ 条长度小于等于 3 的通路。

(3) v_1 到自身共有 $a_{11}^{(1)}+a_{11}^{(2)}+a_{11}^{(3)}=7$ 条长度小于等于 3 的回路。

4.

证明: 考虑 G 的对偶图 G^*。由于 $\lambda\geq 2$，所以 G 中有回路，从而 G 中至少有两个面，也即，$|G^*|\geq 2$。另一方面，因为 G 中任意两个面至多有一条共同边，所以 G^* 中任意两个顶点间至多有一条边，从而 G^* 是简单图。因此，要证原命题，只需证：任意 $n(n\geq 2)$ 阶简单图中必有度数相同的顶点(从而 G^* 中有度数相同的顶点 v_i,v_j，而 $\deg(R_i)=d(v_i)=d(v_j)=\deg(R_j)$，即得原题)。

设 G 为任意 $n(n\geq 2)$ 阶简单图。令 $G[V']$ 为 G 中顶点数最多的一个连通分支(若 G 是连通图，则 $V'=V(G)$)。分两种情况讨论：

情况一：若 $|V'|=1$，则 G 为零图。由 $n\geq 2$ 可知，存在 $v_i,v_j\in V(G)$，$v_i\neq v_j$，使得 $d(v_i)=d(v_j)=0$。命题成立。

情况二：若 $|V'|=k\geq 2$，则因为 $G[V']$ 为简单连通图，所以 $\forall v_i\in V'$ 有 $1\leq d(v_i)\leq k-1$。由于 V' 中有 k 个顶点，却仅有 $k-1$ 种可能的取值，由鸽巢原理知，必有 $v_i,v_j\in V'\subseteq V(G)$，$v_i\neq v_j$，使得 $d(v_i)=d(v_j)$。命题依然成立。 □

四、

1. $(A-C)\cup B=A\cup B$ 的充分必要条件是 $A\cap C\subseteq B$。

证明:

$$\begin{aligned}
&(A-C)\cup B=A\cup B\\
\Longleftrightarrow\ &(A\cap\sim C)\cup B=A\cup B && \text{(补交转换律)}\\
\Longleftrightarrow\ &(A\cup B)\cap(\sim C\cup B)=A\cup B && \text{(分配律)}\\
\Longleftrightarrow\ &A\cup B\subseteq\sim C\cup B && (*)
\end{aligned}$$

$\iff \forall x(x \in A \cup B \to x \in {\sim}C \cup B)$ (子集定义)

$\iff \forall x((x \in A \vee x \in B) \to (\neg x \in C \vee x \in B))$ (集合并运算、绝对补运算定义)

$\iff \forall x(\neg(x \in A \vee x \in B) \vee (\neg x \in C \vee x \in B))$ (蕴涵等值式)

$\iff \forall x((\neg x \in A \wedge \neg x \in B) \vee (\neg x \in C \vee x \in B))$ (命题逻辑德·摩根律)

$\iff \forall x((\neg x \in A \vee \neg x \in C \vee x \in B) \wedge (\neg x \in B \vee \neg x \in C \vee x \in B))$ (命题逻辑分配律)

$\iff \forall x((\neg x \in A \vee \neg x \in C \vee x \in B) \wedge 1)$ (命题逻辑排中律、零律)

$\iff \forall x(\neg x \in A \vee \neg x \in C \vee x \in B)$ (命题逻辑同一律)

$\iff \forall x(\neg(x \in A \wedge x \in C) \vee x \in B)$ (命题逻辑德·摩根律)

$\iff \forall x((x \in A \wedge x \in C) \to x \in B)$ (蕴涵等值式)

$\iff \forall x((x \in A \cap C) \to x \in B)$ (集合交定义)

$\iff x \in A \cap C \subseteq B$ (子集定义)

下面证明 $*$，即，对任意集合 A, B，有 $A \cap B = A \Leftrightarrow A \subseteq B$。

若 $A \cap B = A$，则：

$\forall x,$

$x \in A$

$\iff x \in A \cap B$ ($A \cap B = A$)

$\iff x \in A \wedge x \in B$ (集合交定义)

$\implies x \in B$ (命题逻辑化简律)

从而有 $A \cap B = A \Rightarrow A \subseteq B$。

若 $A \subseteq B$，则：

$\forall x,$

$x \in A$

$\implies x \in B$ (子集定义)

$\iff 1 \wedge x \in B$ (命题逻辑同一律)

$\iff x \in A \wedge x \in B$ (前提)

$\iff x \in A \cap B$ (集合交定义)

从而有 $A \subseteq B \Rightarrow A \cap B = A$。

综合得 $A \cap B = A \Leftrightarrow A \subseteq B$。 □

2.

(1) $f(\mathbb{N} \times \{1\}) = \{n \cdot 1 \mid n \in \mathbb{N}\} = \mathbb{N}$。

(2) $f^{-1}(\{0\}) = \{\langle m, n\rangle \mid m, n \in \mathbb{N} \wedge mn = 0\} = \{\langle 0, n\rangle, \langle n, 0\rangle \mid n \in \mathbb{N}\}$。

(3) f 不是单射(例如 $f(\langle 1, 4\rangle) = f(\langle 2, 2\rangle) = 4$，但 $\langle 1, 4\rangle \neq \langle 2, 2\rangle$)，从而也不是双射。

(4) f 是满射，因为对任何 $n \in \mathbb{N}$，有 $\langle n, 1\rangle \in \mathbb{N} \times \mathbb{N}, f(\langle n, 1\rangle) = n$。

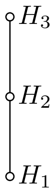
3.

(1) 易知 $\mathrm{Aut}\, G = \{\varphi_i \mid i = 1, 2, 3, 4\}$，其中 $\varphi_i : \mathbb{Z}_5 \to \mathbb{Z}_5 (i = 1, 2, 3, 4)$ 定义为 $\forall x \in \mathbb{Z}_5, \varphi_i(x) = ix \bmod 5$。

运算表如下：

$\circ$	φ_1	φ_2	φ_3	φ_4
φ_1	φ_1	φ_2	φ_3	φ_4
φ_2	φ_2	φ_4	φ_1	φ_3
φ_3	φ_3	φ_1	φ_4	φ_2
φ_4	φ_4	φ_3	φ_2	φ_1

(2) 易于验证，$\mathrm{Aut}\,G$ 中共有 3 个子群：
$H_1=\{\varphi_1\}$；
$H_2=\{\varphi_1,\varphi_4\}$；
$H_3=\mathrm{Aut}\,G$；
从而哈斯图为：



(3) 由于 $|S|<5$，所以 $\langle S,R\rangle$ 是分配格，但因为 H_2 没有补元，所以不是有补格，从而也不是布尔格。(另证：反设 $\langle S,R\rangle$ 是有补格，则 $\langle S,R\rangle$ 是有补分配格，从而是布尔格。但有限阶布尔格都是 $2^k(k\in\mathbb{N})$ 阶的，这与 $|S|=3$ 矛盾。所以 $\langle S,R\rangle$ 必定不是有补格)。

4.

证明：首先证明 G 中无二阶元：若不然，不妨设 $a\in G$ 为二阶元，则 $\langle a\rangle=\{e,a\}$ 是 G 的子群，从而由 Lagrange 定理知，$2=|\langle a\rangle|\mid|G|$。这与 $|G|$ 是奇数阶群矛盾。

令 $\mathscr{A}=\{\{x,y\}\mid x,y\in G\wedge xy=e\}$，则 $\mathscr{A}$ 是 G 的一个划分(因为每个元素均可逆，所以 $\cup\mathscr{A}=G$；又由逆元唯一性和 $(x^{-1})^{-1}=x$ 可知，$\forall A,B\in\mathscr{A},A\cap B\neq\varnothing\to A=B$)。由于 G 中无二阶元，所以 $\forall A\in\mathscr{A}$，若 $A\neq\{e\}$，就必有 $|A|=2$，从而总有 $\prod\limits_{x\in A}x=e$。由于 $\mathscr{A}$ 是 G 的划分，且 G 是 Abel 群，所以：

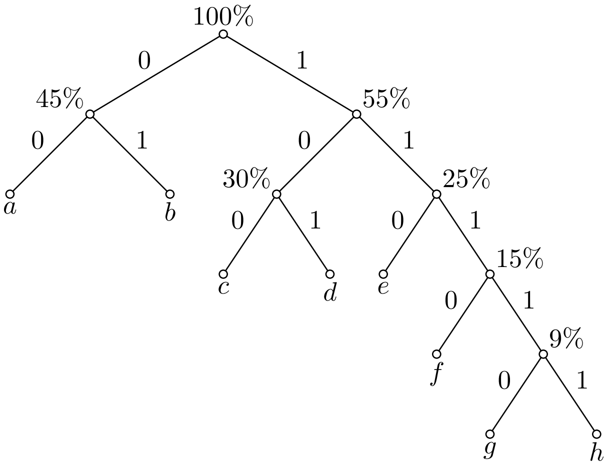
$$\prod_{x\in G}x=\prod_{A\in\mathscr{A}}\prod_{x\in A}x=\prod_{A\in\mathscr{A}}e=e.$$

□

1999 年计算机数学基础

三、

3. 作最优树如下：



得最佳前缀码：

a—00；

b—01；

c—100；

d—101；

e—110；

f—1110；

g—11110；

h—11111；

每传输 100 个字母，需要传输 $25 \cdot 2 + 20 \cdot 2 + 15 \cdot 3 + 15 \cdot 3 + 10 \cdot 3 + 6 \cdot 4 + 5 \cdot 5 + 4 \cdot 5 = 279$ 个二进制位。所以传输 100^n 个按此概率分布的字母需用 $279 \cdot 100^{n-1}$ 个二进制位。

4.

证明： 由于 $\delta^+(D) \geq 1$，所以 D 中有边。在 D 中构造一极大路径 Γ，不妨记 $\Gamma = v_1 v_2 \cdots v_k$。由于 Γ 是极大路径，所以所有邻接于 v_k 的顶点都在 Γ 上。令 $s = \min\{i \mid \langle v_k, v_i \rangle \in E(D)\}$。考虑初级回路 $C = v_k v_s v_{s+1} \cdots v_k$，注意到，由于所有邻接于 v_k 的顶点都在 Γ 上，且 v_s 是所有邻接于 v_k 的顶点中编号最小的一个，所以其它邻接于 v_k 的顶点 v_i 都满足 $s < i < k$，从而都在 C 上。由于 G 中至少有 $\delta^+(D)$ 个顶点邻接于 v_k，而这些顶点，连同 v_k 本身，都在 C 上，所以 C 中至少有 $\delta^+(D) + 1$ 个顶点。 □

5. 不能。假如找到了这样的平面图，就否定地解决了四色猜想。鉴于一百多年来没有人能够否定地解决四色猜想，所以试图在两个小时的考试时间内构造出一个四色猜想的反例必定是徒劳的(事实上，Appel 和 Haken 已经于 1976 年证明了四色猜想，从而确认了不可能有这样的平面图)。

四、

1.

(1) $\mathcal{P}(A)-\{\varnothing\}=\{\varnothing,\{\varnothing\},\{\{\varnothing\}\},\{\varnothing,\{\varnothing\}\}\}-\{\varnothing\}=\{\{\varnothing\},\{\{\varnothing\}\},\{\varnothing,\{\varnothing\}\}\}$。

(2) $\mathcal{P}(A)\oplus A=\{\varnothing,\{\varnothing\},\{\{\varnothing\}\},\{\varnothing,\{\varnothing\}\}\}\oplus\{\varnothing,\{\varnothing\}\}=\{\{\{\varnothing\}\},\{\varnothing,\{\varnothing\}\}\}$。

2.

(1) $R_1=I_A$；

$R_2=I_A\cup\{\langle 1,2\rangle,\langle 2,1\rangle\}$；

$R_3=I_A\cup\{\langle 1,3\rangle,\langle 3,1\rangle\}$；

$R_4=I_A\cup\{\langle 2,3\rangle,\langle 3,2\rangle\}$；

$R_5=E_A$。

(2)

$\cap$	R_1	R_2	R_3	R_4	R_5
R_1	R_1	R_1	R_1	R_1	R_1
R_2	R_1	R_2	R_1	R_1	R_2
R_3	R_1	R_1	R_3	R_1	R_3
R_4	R_1	R_1	R_1	R_4	R_4
R_5	R_1	R_2	R_3	R_4	R_5

(3) R_5 是单位元，R_1 是零元，仅 R_5 为可逆元，它的逆元是它自身。

(4) 由于集合交运算适合结合律，所以 V 是半群，又由于 V 有单位元，所以是独异点。但由于并非所有元素皆可逆，所以 V 不是群。

3.

(1) $$f\circ g(x)=\begin{cases}1, & x=0;\\ 2, & x=2;\\ 0, & x=4;\\ k, & x=2k,k\in\mathbb{N},k\geq 3;\\ 3, & x=2k+1,k\in\mathbb{N}.\end{cases}$$

由于 $f\circ g(4)=0,f\circ g(0)=1,f\circ g(2)=2,f\circ g(2k)=k(k\geq 3)$，所以 $f\circ g$ 是满射。但 $f\circ g(6)=f\circ g(3)=3$，所以 $f\circ g$ 不是单射，从而不是双射。

(2) $f\circ g(A)=\{1,2,3\}$，$f\circ g^{-1}(B)=\{0,4,8\}$。

4.

证明:

$A\subseteq\mathcal{P}(A)$

$\iff\forall x(x\in A\to x\in P(A))$ (子集定义)

$$
\begin{aligned}
&\iff \forall x(x \in A \to x \subseteq A) && \text{(幂集定义)}\\
&\iff \forall x(x \in A \to \forall y(y \in x \to y \in A)) && \text{(子集定义)}\\
&\iff \forall x \forall y(x \in A \to (y \in x \to y \in A)) && \text{(量词辖域扩张等值式)}\\
&\iff \forall x \forall y(\neg x \in A \lor (\neg y \in x \lor y \in A)) && \text{(蕴涵等值式)}\\
&\iff \forall x \forall y(\neg(x \in A \land y \in x) \lor y \in A) && \text{(命题逻辑德·摩根律)}\\
&\iff \forall y(\forall x \neg(x \in A \land y \in x) \lor y \in A) && \text{(量词辖域收缩等值式)}\\
&\iff \forall y(\neg \exists x(x \in A \land y \in x) \lor y \in A) && \text{(量词否定等值式)}\\
&\iff \forall y(\exists x(x \in A \land y \in x) \to y \in A) && \text{(蕴涵等值式)}\\
&\iff \forall y(y \in \cup A \to y \in A) && \text{(广义并定义)}\\
&\iff \cup A \subseteq A && \text{(子集定义)}
\end{aligned}
$$

□

5.

证明：证法一：

$$
\begin{aligned}
&\ g \in Ag && (e \in A)\\
&\iff g \in Bh && (Ag = Bh)\\
&\iff Bg = Bh && \text{(教材定理 17.22)}\\
&\iff Bg = Ag && (Ag = Bh)\\
&\Longrightarrow \forall b(b \in B \to \exists a(a \in A \land bg = ag)) && \text{(陪集定义)}\\
&\Longrightarrow \forall b(b \in B \to \exists a(a \in A \land b = a)) && \text{(消去律)}\\
&\iff \forall b(b \in B \to b \in A) && (b = a)\\
&\iff B \subseteq A && \text{(子集定义)}
\end{aligned}
$$

同理可证 $A \subseteq B$。所以有 $A = B$。 □

2000 年计算机数学基础

三、

1.

(1) $3!\cdot\genfrac{\{}{\}}{0pt}{}{4}{3}=3!\cdot C_4^2=36$。

(2) $\mathrm{card}(A\to B)=\mathrm{card}(\varnothing)=0$。

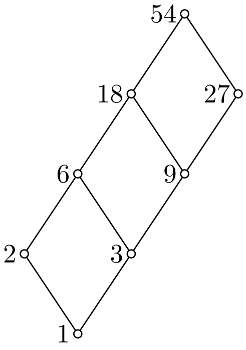
(3) $2n-1$，(考虑有向的星图，可知这个下界是 tight 的)。

(4) $\min\{r,s\}$。

(5) 4。

2.

(1) 哈斯图如下：



(2) $\Pi=\{\{1\},\{2,3\},\{6,9\},\{18,27\},\{54\}\}$。

(3) B 中无最小元，极大元集合为 $\{2,9\}$，最小上界为 18。

3.

证明： 构造一个“极大路径” $\Gamma=v_0,v_1,\ldots,v_l$。

由 Γ 是极大路径知，v_0 的所有邻接点都在 Γ 上。

由 $\delta(G)\geq 3$ 可知，除 v_1 外，至少还有两个顶点 $v_i,v_j(2\leq i<j\leq l)$ 与 v_0 相邻。

于是，$v_0,v_1,\ldots,v_i,v_0$ 是一个长度为 $i+1$ 的圈，$v_0,v_1,\ldots,v_j,v_0$ 是一个长度为 $j+1$ 的圈，$v_0,v_i,\ldots,v_j,v_0$ 是一个长度为 $j-i+2$ 的圈。

倘若 $i+1$ 和 $j+1$ 中有偶数，则命题已经成立。

否则，就有 $i+1$ 和 $j+1$ 都是奇数，从而 $(j+1)-(i+1)=j-i$ 是偶数，所以 $j-i+2$ 是偶数。命题同样成立。 □

四、

1.

(1) 因为 $(b*c)*c=d*c=d\neq b=b*a=b*(c*c)$，所以该运算不满足结合律。

(2) a 是单位元，d 是零元。

(3) 令 $x_1=x_2=y_1=b, y_2=c$，则 x_1Ry_1, x_2Ry_2，但 $x_1*y_1=b*b=a$，$b*c=x_2*y_2=d$，$\langle a,d\rangle\notin R$。从而 R 不是 $\langle A,*\rangle$ 上的同余关系。

2.

证明：注意到，由于 A 是正规子群，所以 $y^{-1}xy\in A$ 且 $x^{-1}\in A$，从而 $x^{-1}y^{-1}xy\in A$。同理，由于 B 是正规子群，所以 $x^{-1}y^{-1}x\in B$ 且 $y\in B$，从而 $x^{-1}y^{-1}xy\in B$。而 $A\cap B=\{e\}$，所以有 $x^{-1}y^{-1}xy=e$。等式两侧依次左乘 x 和 y，即得 $xy=yx$。 □

3.

(1) 可交换的二元关系可以看作是从 $A\&A$ 中一个子集，其中 $A\&A=\{\{x,y\}\mid x,y\in A\}$ 为 A 与自身的无序积。由于这样的无序对有 $C_3^2+3=6$ 个(C_3^2 为从 3 个数中取两个不同的元素的方法数，加 3 是因为可以取相同的元素进行运算)，而由于是自反的，所以有三个无序对必须选择，从而可交换且自反的二元关系有 $2^3=8$ 个。

(2) $A\times A$ 中共有 3 个 $\langle x,x\rangle$ 形式的有序对。对每一个这样的有序对，一个反对称的二元关系可以选择包含它，或不包含它。从而在这一步骤中，共有 2^3 种不同的选法。$A\times A$ 中还有 3 组 $\langle x,y\rangle,\langle y,x\rangle$ 形式的有序对，其中 $x,y\in A, x\neq y$。对每一组这样的有序对，一个反对称的二元关系可以选择不包含任意一个，或包括其中的一个(共计 3 种不同的选择方式)，从而在这一步骤中，共有 3^3 种不同选法。总计就有 $2^3\cdot 3^3=6^3$ 种选法。

(3) 由前两小题的分析易知，对称的二元关系有 2^6 个，反对称的二元关系有 6^3 个，即对称又反对称的二元关系有 2^3 个。A 上的二元关系有 2^9 个。从而由德·摩根律和容斥原理可知，既不对称，也不是反对称的二元关系有 $2^9-2^6-6^3+2^3=240$ 个。

2001 年计算机数学基础

三、

1.

(1) $\cap A = \{\varnothing\} \cap \{\{\varnothing\}\} = \varnothing$。

(2) $\cup A = \{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\}$。

(3) $\cup \cup A = \cup\{\varnothing, \{\varnothing\}\} = \varnothing \cup \{\varnothing\} = \{\varnothing\}$。

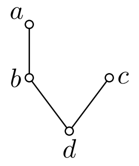
(4) $\cup\mathcal{P}(A) = A = \{\{\varnothing\}, \{\{\varnothing\}\}\}$。

(5) $\mathcal{P}(\cup A) = \mathcal{P}(\{\varnothing, \{\varnothing\}\}) = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}$。

2. 由图论基本定理，$\sum\limits_{v \in V(G)} d(v) = 2m = 42$。12 个 3 度顶点的度数和为 36，因此共有 3 个 2 度顶点。从而 $n = 15$。

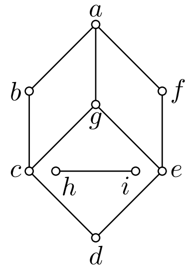
3.

(1) 哈斯图如下：



(2) $C = \varnothing$，无上确界。$D = \{d\}$，下确界为 d。

4. 为顶点作标记如下：



(1) $\kappa = 0$。

(2) $\chi = 2$。事实上，取 $V_1 = \{a, c, e, h\}, V_2 = \{b, d, f, g, i\}$，则 $\langle V_1, V_2, E\rangle$ 为二部图。

(3) $\beta_0 = 5$。$V_2 = \{b, d, f, g, i\}$ 为点独立集，所以 $\beta_0 \geq 5$。而任何点独立集，至多只能从 $\{a, b, c, d, e, f\}$ 中取三个顶点，从 $\{h, i\}$ 中取一个顶点，加上 g，至多有 5 个顶点。所以 $\beta_0 = 5$。

(4) $\beta_1 = 4$。取图中所有水平和竖直的边即得一个 4 阶匹配，而显然有 $\beta_1 \leq 4 = \left\lfloor \dfrac{n}{2} \right\rfloor$。

(5) $\alpha_0 = 4$。$V_1 = \{a, c, e, h\}$ 即是一个 4 阶点覆盖。而 $\alpha_0 \geq \beta_1 = 4$。

5.

证明: 由于 G 中没有长为 3 的圈，所以 G 中面的次数至少为 4 (若 G 中无圈，则 G 中只有一个外部面，由 G 是连通图和 $n \geq 3$ 知，外部面的次数为 $2m \geq 2(n-1) \geq 2(4-1) = 6$)，由教材定理 11.8 有

$$m \leq \frac{l}{l-2}(n-2) \leq 2(n-2) = 2n-4,$$

若 $\delta(G) \geq 4$，则有 $m \geq 2n > 2n-4$，矛盾。 □

四、

1.

(1) 由于整数集对加、减、乘法封闭，所以对 $*$ 运算也封闭。从而 $\langle A, * \rangle$ 是代数系统。对任意 $x, y, z \in A$：

由于 $x * y = x + y - xy = y + x - yx = y * x$，所以运算满足交换律。

由于 $(x * y) * z = x + y + z - xy - xz - yz + xyz = x * (y * z)$，所以运算满足结合律。

由于 $x * x = x + x - x^2$，当 $x \neq 0, 1$ 时，$x * x \neq x$，所以运算不满足幂等律。

由于 $x * 0 = 0 * x = x$，因此有运算有单位元 $0 \in \mathbb{Z}$。

由 $x * y = x + y - xy = 0$ 解得：当 $x = 1$ 时，等式无解。当 $x \neq 1$ 时，$y = \dfrac{x}{x-1}$。因此，仅当 $x = 0, 2$ 时，有 $y = x^{-1} \in \mathbb{Z}$。此时 y 分别为 0 和 2。因此，仅 $0, 2$ 为可逆元，它们的逆元即是它们自身。

(2) 由对称差的性质可知，A 对 $*$ 运算封闭。从而 $\langle A, * \rangle$ 是代数系统。

由对称差的性质知，运算满足交换律、结合律。

对任意 $x \in A$，有 $x * x = x \oplus x = \varnothing$，当 $x \neq \varnothing$ 时，$x * x \neq x$，所以运算不满足幂等律。

显然 $\varnothing$ 是单位元，且所有元素都是自身的逆元。

(3) 当 $|B| \geq 2$ 时，$*$ 运算对 A 不封闭。因为当 $|B| \geq 2$ 时，任取 $a, b \in B, a \neq b$。则 $\{a\}, \{b\} \in A$，但 $\{a\} \cap \{b\} = \varnothing \notin A$。从而当 $|B| \geq 2$ 时，$\langle A, * \rangle$ 不是代数系统。

2. $|x| = 3$。

证明: 首先，由于 y 是二阶元，所以有 $y^{-1} = y$。同时：

$$\begin{aligned}
& yxy^{-1} = x^2 \\
\iff & yx = x^2y && \text{(右乘 } y\text{)} \\
\iff & x = y^{-1}x^2y && \text{(左乘 } y^{-1}\text{)} \\
\implies & x^2 = (y^{-1}x^2y)(y^{-1}x^2y) && \text{(两边取平方)} \\
\iff & x^2 = y^{-1}x^4y && (yy^{-1} = e) \\
\iff & x^2 = yx^4y^{-1} && (y = y^{-1})
\end{aligned}$$

从而有 $yx^4y^{-1} = x^2 = yxy^{-1}$。由消去律知 $x^3 = e$。从而 $|x| \mid 3$。因为 x 不是单位元，所以 $|x| \neq 1$，因此只能有 $|x| = 3$。 □

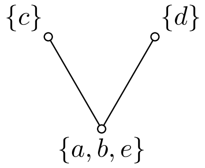
2002 年计算机数学基础

三、

1.

(1) $A/R_1 = \{\{a,b,e\},\{c\},\{d\}\}$。

(2)

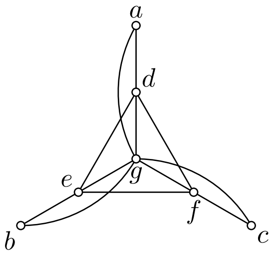


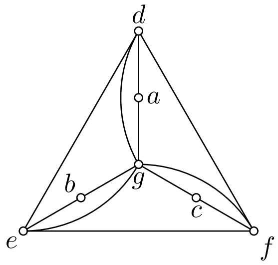
2.

(1) 每个顶点都偶数度的，所以 G 是欧拉图。

(2) G 不是哈密顿图。理由如下：对 G 中顶点进行标号(见下图)，反设存在哈密顿圈 Γ，因为顶点 a 的度为 2，所以它在 Γ 中必与它仅有的两个顶点相邻，也即，g 与 a 在 Γ 中相邻。同理，g 与 b,c 也在 Γ 中相邻。但 g 在 Γ 中只能出现一次，从而至多只能与两个顶点相邻，矛盾。

(3) G 是可平面的。右图是 G 的一个平面嵌入。





3.

(1)

证明： 若不然，则有多于 $\dfrac{n}{2}$ 个顶点的度数大于 $\dfrac{4m}{n}$，从而总度数大于 $\dfrac{4mn}{2n} = 2m$，与图论基本定理矛盾。 □

(2)

证明： 按如下方式构造点独立集 V^*：任取一个度数不超过 $\dfrac{4m}{n}$ 的顶点 v_1 加入 V^*。若 $V(G) - V^*$ 中仍存在度数不超过 $\dfrac{4m}{n}$ 且与 V^* 中任何顶点都不相邻的顶点 v_i，则将 v_i 加入 V^*。重复这一过程直至 G 中不再存在这样的顶点。设 $|V^*| = k$，下面证明 $k \geq \dfrac{n/2}{1+4m/n}$。

考虑 $N_g(V^*) = \{v \mid v \in V(G) \land \exists u(u \in V^* \land (u,v) \in E(G))\}$。由于 V^* 中每一个顶点的度

数都不超过 $\dfrac{4m}{n}$，所以：

$$\begin{aligned}|N_g(V^*)\cup V^*| \leq & |N_g(V^*)|+|V^*| && \text{(容斥原理)}\\ \leq & \frac{4m}{n}k+k && (|V^*|=k)\\ \leq & k(1+4m/n)\end{aligned}$$

反设 $k<\dfrac{n/2}{1+4m/n}$，则有 $|N_g(V^*)\cup V^*|<\dfrac{n}{2}$，由第 (1) 小题结论，$V(G)-V^*$ 中仍有度数不超过 $\dfrac{4m}{n}$ 且与 V^* 中任何顶点都不相邻的顶点。这与 V^* 的选择方式矛盾。 □

四、

1.

证明： $\forall a,b\in G$，

$$\begin{aligned}aba^{-1}b^{-1} \in & Naba^{-1}b^{-1}\\ = & Na\circ Nb\circ Na^{-1}\circ Nb^{-1} && \text{(商群运算定义)}\\ = & Na\circ Na^{-1}\circ Nb\circ Nb^{-1} && (G/N\text{ 是 Abel 群})\\ = & N(aa^{-1}bb^{-1}) && \text{(商群运算定义)}\\ = & Ne && (aa^{-1}bb^{-1}=e)\\ = & N && \text{(陪集定义)}\end{aligned}$$

□

2.

证明： 由鸽巢原理知，存在 $1\leq i,j\leq 8$，使第 i 行各项之和 $S_i\geq 7$，第 j 行各项之和 $S_j\geq 7$，从而第 i 行与第 j 列各项之和等于 $S_i+S_j-a_{ij}\geq 7+7-1=13$。 □

3. 题目中的要求已经决定大多数运算的值，仅有 $a*c=c*a$ 的值是可以自由决定的。这里令 $a*c=c*a=a$，使 c 成为单位元。运算表如下：

$*$	a	b	c
a	a	c	a
b	c	b	b
c	a	b	c

注意到，由于 $ab=ba=cc=c$，所以每个元素都可逆。假设 $*$ 运算是可结合的，则 $\langle A,*\rangle$ 将构成一个 3 阶循环群(素数阶群必是循环群)，而这是不可能的(因为 a,b 都是 2 阶元，不可能是生成元)。所以 $*$ 运算一定不是可结合的(反例如，$(a*a)*b=a*b=c\neq a*(a*b)=a*c=a$)。

4. 根据各数除以 3 所得的余数，将这 20 个数分成 3 类：$S_k=\{3n+k\mid n\in\mathbb{N}\wedge 3n+k\leq 20\}(k=1,2,3)$。显然，$|S_1|=|S_2|=7,|S_3|=6$。而三个数之和为 3 的倍数当且仅当这三个数分别来自 S_1,S_2,S_3 或三个数全部来自同一个 $S_i(1\leq i\leq 3)$。从而共有 $7\cdot 7\cdot 6+2\cdot C_7^3+C_6^3$ 种选法。

2003 年计算机专业基础

三、

1. 条件 I 是条件 II 的充分必要条件。

证明： 充分性。

若存在 $A \subseteq X, B \subseteq Y$，使得 $R = A \times B$，则对任意 $x_1, x_2 \in X, y_1, y_2 \in Y$ 有

$$\langle x_1, y_1 \rangle \in R \wedge \langle x_2, y_2 \rangle \in R$$

$$\Longrightarrow x_1 \in A \wedge y_2 \in B \qquad (R = A \times B)$$

$$\Longrightarrow \langle x_1, y_2 \rangle \in R \qquad (R = A \times B)$$

必要性。

取 $A = \operatorname{dom} R \subseteq X, B = \operatorname{ran} R \subseteq Y$，下面证明对任意 $x \in A, y \in B$ 有 $\langle x, y \rangle \in R$，从而有 $R = A \times B$。

$\forall x \in X, y \in Y$，

$$x \in A \wedge y \in B$$

$$\Longleftrightarrow \exists w(\langle x, w \rangle \in R) \wedge \exists z(\langle z, y \rangle \in R) \qquad (\operatorname{dom}, \operatorname{ran} \text{ 定义})$$

$$\Longleftrightarrow \exists w \exists z(\langle x, w \rangle \in R \wedge \langle z, y \rangle \in R) \qquad (\text{量词辖域扩张等值式})$$

$$\Longleftrightarrow \exists w \exists z(\langle x, y \rangle \in R) \qquad (\text{条件 I })$$

$$\Longrightarrow \langle x, y \rangle \in R \qquad (\exists \text{消去})$$

□

2.

(1) 当且仅当 N 为大于 0 的偶数时，B_N 是欧拉图。

因为 B_N 是 N-正则图。当且仅当 N 为偶数时，B_N 中每个顶点都是偶数度的。

(2) 当且仅当 $N \geq 2$ 时，B_N 为哈密顿图。

用归纳法证明。直接验证可知 B_0, B_1 不是哈密顿图，B_2 是哈密顿图。对任意 $N \geq 2$，若 B_N 是哈密顿图，则可如下构造 B_{N+1} 上的哈密顿圈：先取 B_{N+1} 的一半(正好是一个 B_N)，寻找上面的一个哈密顿圈，从中删去任意一条边，成为哈密顿路，在 B_{N+1} 的另一半上以同样找一个哈密顿圈，删去与之对应的一条边。将两边的哈密顿路拼接成一个 B_{N+1} 上的哈密顿圈即可。

(3) 当且仅当 $N \leq 3$ 时，B_N 为可平面的。

易于验证，B_0, B_1, B_2, B_3 是可平面的。

注意到，由于 B_N 是二部图(这一点将在第 (4) 小题中证明)，因此不存在长度为 3 的圈，由公式 $m \leq \dfrac{l}{l-2}(n-2)$ 知，若 B_N 为平面图则 $m \leq 2n - 4 < 2n = 4 \cdot 2^{N-1}$。另一方面，由图论基本定理知，$2m = N2^N$，$m = N2^{N-1}$。从而由 $N2^{N-1} = m < 4 \cdot 2^{N-1}$ 解得 $N < 4$。

(4) 对所有 $N \geq 1$，B_N 都是二部图。

由 B_N 定义知，B_N 任意两个相邻顶点所对应的 0-1 串中，1 的数量只差一个，从而 1 的数量的奇偶性是不同的。令 V_1 为所有对应的 0-1 串中有奇数个 1 的顶点，V_2 为所有对应的 0-1 串中有偶数个 1 的顶点，则 $B_N = \langle V_1, V_2, E\rangle$ 是二部图。

3. 命题对无向图成立。

证明: 考虑无向图 G的任何一棵生成树 T。以其中一个顶点为根，行遍这棵树(前序、中序、后序皆可)，每访问到一个顶点 v，则检查与这个顶点关联的边中，是否有未曾通过的弦，若有，则从此弦上通过，然后立即回到 v，反复这一过程直至所有与 v 关联的弦都被走过至少一次。按此方法行遍整棵树后，行进的轨迹正好是一个通过图 G 中每个边恰好两次的回路。 □

命题对有向图(即使是强连通的)不成立。反例如下：

考虑一个 $n+2(n \geq 3)$ 阶有向图 D，其中 $V(D) = \{v_i \mid i = 0, 1, 2, \cdots, n, n+1\}$，$E(D) = \{\langle v_0, v_i\rangle, \langle v_i, v_{n+1}\rangle \mid i = 1, 2, \cdots, n\} \cup \{\langle v_{n+1}, v_0\rangle\}$。显然，$D$ 是强连通的。由于 v_{n+1} 的入度为 n，要想通过 D 中所有的边，就必须经过 v_{n+1} 至少 n 次，每次到达 v_{n+1} 后，都必须通过边 $\langle v_{n+1}, v_0\rangle$ 离开。因此，任何一个通过 D 中所有边的回路都将通过边 $\langle v_{n+1}, v_0\rangle$ 至少 n 次。

四、

1.

证明: 反设 $\mathrm{Aut}\, G$ 中只有一个元素(从而只能是恒等映射 I_G)。由 $\mathrm{Inn}\, G \trianglelefteq \mathrm{Aut}\, G = \{I_G\}$ 可知，$\mathrm{Inn}\, G = \{I_G\}$。再由 $\mathrm{Inn}\, G$ 定义知，对所有 $g, h \in G$，有 $ghg^{-1} = \varphi_g(h) = I_G(h) = h$。等式两边右乘 g，就有 $gh = hg$。由 g, h 的任意性知，G 是 Abel 群。矛盾。 □

2.

(1) 由于二元运算即为从 $A \times A$ 到 A 的全函数，故有 $3^{3\cdot 3} = 3^9$ 个。

(2) 可交换的二元运算可以看作是 $A\&A$ 到 A 的全函数，其中 $A\&A = \{\{x, y\} \mid x, y \in A\}$ 为 A 与自身的无序积。由于这样的无序对有 $C_3^2 + 3 = 6$ 个(C_3^2 为从 3 个数中取两个不同的元素的方法数，加 3 是因为可以取相同的元素进行运算)，所以 A 上可交换的二元运算有 $|A|^{|A\&A|} = 3^6$ 个。

(3) 幂等的运算相当于从 $A \times A - \{\langle a, a\rangle, \langle b, b\rangle, \langle c, c\rangle\}$ 到 A 的全函数。故有 $3^{9-3} = 3^6$ 个。

(4) 令 E 为 A 上的所有二元运算，$\mathscr{A}$ 为 A 上可交换的二元运算，$\mathscr{A}$ 为 B 上幂等的二元运算。则 $|{\sim}\mathscr{A} \cap {\sim}\mathscr{B}| = |{\sim}(\mathscr{A} \cup \mathscr{B})| = |E| - |\mathscr{A} \cup \mathscr{B}|$ 即为 A 上既不可交换，也不是幂等的二元运算数。由容斥原理，$|\mathscr{A} \cup \mathscr{B}| = |\mathscr{A}| + |\mathscr{B}| - |\mathscr{A} \cap \mathscr{B}|$。而 $|\mathscr{A} \cap \mathscr{B}|$ 相当于 $A\&A$ 到 A 的全函数的个数，等于 3^3。从而 A 上既不可交换，也不是幂等的二元运算共有 $3^9 - 2\cdot 3^6 + 3^3 = 3^3(3^3 - 1)$ 个。

2004 年计算机专业基础

二、

1.

(1) A 上共有 2^{n^2} 个二元关系，共有 n^n 个一元(全)函数。

(2) A 上共有 5 个等价关系，19 个偏序关系。

(3) $\cup\cup\{1,2\} = \cup(1\cup 2) = \cup 2 = 1$，$\cap\cap\{2,3\} = \cap(2\cap 3) = \cap 2 = \varnothing$。

(4) $\mathrm{card}(\mathbb{Z}\times\mathbb{Z}) = \aleph_0$，$\mathrm{card}\,A = \aleph = 2^{\aleph_0}$。

2. 命题 (1) 成立。

证明： $\forall x$，

$$
\begin{aligned}
& x \in \cap(A\cup B) & \\
\Longleftrightarrow\ & \forall S(S \in A\cup B \to x \in S) & \text{(广义交定义)} \\
\Longleftrightarrow\ & \forall S((S \in A \vee x \in B) \to x \in S) & \text{(集合并定义)} \\
\Longleftrightarrow\ & \forall S(\neg(S \in A \vee x \in B) \vee x \in S) & \text{(蕴涵等值式)} \\
\Longleftrightarrow\ & \forall S((\neg S \in A \wedge \neg x \in B) \vee x \in S) & \text{(命题逻辑德·摩根律)} \\
\Longleftrightarrow\ & \forall S((\neg S \in A \vee x \in S) \wedge (\neg x \in B \vee x \in S)) & \text{(命题逻辑分配律)} \\
\Longleftrightarrow\ & \forall S((S \in A \to x \in S) \wedge (x \in B \to x \in S)) & \text{(蕴涵等值式)} \\
\Longleftrightarrow\ & \forall S(S \in A \to x \in S) \wedge \forall S(S \in B \to x \in S) & \text{(量词分配等值式)} \\
\Longleftrightarrow\ & x \in \cap A \wedge x \in \cap B & \text{(广义交定义)} \\
\Longleftrightarrow\ & x \in (\cap A) \cap (\cap B) & \text{(集合交定义)}
\end{aligned}
$$

□

3.

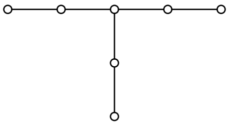
(1) 当 r 和 s 皆为偶数时，G 为欧拉图。

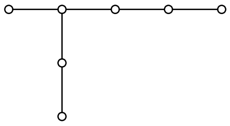
(2) 当 $r = s \geq 2$ 时，G 为哈密顿图。

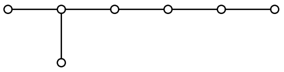
(3) 当 $r \leq 2$ 或 $s \leq 2$ 时，G 为平面图。

(4) 轮图是自对偶的，所以 $\chi^* = \chi = 4$。

4. 考虑 3 度顶点所对应的 3 个分支中 2 度顶点的数量，由于总计有且仅有 3 个 2 度顶点，故，这些 2 度顶点的分布只能有 $\{0,0,3\},\{0,1,2\},\{1,1,1\}$ 这三种可能。显然，两棵满足题目要求的无向树是同构的当且仅当它们 2 度顶点在分支中的分布方式相同。因此，在同构意义上，共有三棵满足要求的无向树：







5.

(1)

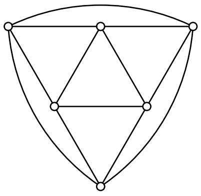
证明: 反设 G 中不存在度数小于等于 3 的顶点，则由图论基本定理可知 $2m = \sum\limits_{v\in G} d(v) \geq \sum\limits_{v\in G} 4 = 4n$，即 $m \geq 2n$。又由于 G 中不存在长度为 3 或 4 的圈，所以 G 中每个面的次数至少为 5。

从而有：

$$\begin{aligned} m &\leq \frac{5}{5-2}(n-2) && \text{(教材定理 11.9)} \\ &= 2n - \frac{n+10}{3} \\ &< 2n \end{aligned}$$

矛盾。 □

(2) 不成立。举 6 阶反例如下：



三、

1. $V/\sim = \langle \mathbb{N}/\sim, \oplus \rangle$，其中 $\mathbb{N}/\sim = \{2\mathbb{N}, \{1\}, \{3\}, \{5\}, \cdots\}$，$2\mathbb{N} = \{2n \mid n \in \mathbb{N}\}$。$\oplus$ 的运算表为：$\forall x, y \in \mathbb{N}/\sim$，$x \oplus y = \begin{cases} 2\mathbb{N}, & \text{当 } x = 2\mathbb{N} \text{ 或 } y = 2\mathbb{N}; \\ \{mn\}, & \text{当 } x = \{m\}, y = \{n\}, m, n \in \mathbb{N}. \end{cases}$

2.

证明: 由于 xH 是 G 的子群，所以 $e \in xH$。即，$\exists y \in H$，使得 $xy = e$。由消去律知，$y = x^{-1} \in H$。由 $x^{-1} \in H$ 和 H 是群知，$x = (x^{-1})^{-1} \in H$。 □

2005 年计算机数学基础

1. 对任意集合 A,B 有：$A\cup(A\cap B)=A$ 和 $A\cap(A\cup B)=A$。

证明： $\forall x$，

$x\in A$

$\Longrightarrow x\in A\vee x\in A\cap B$ (命题逻辑附加律)

$\Longleftrightarrow x\in A\cup(A\cap B)$ (集合并定义)

从而有 $A\subseteq A\cup(A\cap B)$。

$\forall x$，

$x\in A\cup(A\cap B)$

$\Longleftrightarrow x\in A\vee x\in A\cap B$ (集合交定义)

$\Longleftrightarrow x\in A\vee(x\in A\wedge x\in B)$ (集合交定义)

$\Longleftrightarrow (x\in A\vee x\in A)\wedge(x\in A\vee x\in B)$ (命题逻辑分配律)

$\Longrightarrow x\in A\vee x\in A$ (命题逻辑化简律)

$\Longrightarrow x\in A$ (命题逻辑同一律)

从而有 $A\cup(A\cap B)\subseteq A$。

综合得 $A\cup(A\cap B)=A$。 □

2. 二个元素集合上共有 4 个不同有序对，从而有 $2^4=16$ 个不同的二元关系。不妨记这个集合为 $A=\{a,b\}$。A 上的等价关系只有两个，一个是恒等关系 I_A，一个是全域关系 E_A。

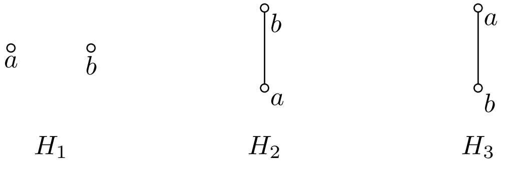
偏序关系有：

$H_1=I_A$；

$H_2=I_A\cup\{\langle a,b\rangle\}$；

$H_3=I_A\cup\{\langle b,a\rangle\}$；

哈斯图分别为：



全函数共有 4 个：

$f_1=\{\langle a,a\rangle,\langle b,a\rangle\}$；

$f_2=\{\langle a,a\rangle,\langle b,b\rangle\}$；

$f_3=\{\langle a,b\rangle,\langle b,a\rangle\}$；

$f_4=\{\langle a,b\rangle,\langle b,b\rangle\}$。

3. 等价。

证明: 将一个人抽象为一个顶点，在能直接对话的人所对应的顶点间添加边。则题中两个条件的等价性可以描述成：一个有限阶无向简单图 G 是连通的当且仅当对 $V(G)$ 的任意二阶划分 $\{V_1, V_2\}$，存在 $u \in V_1, v \in V_2$ 使得 $(u, v) \in E(G)$。

下面证明这一命题。

必要性。若不然，则存在划分 $\{V_1, V_2\}$，使 V_1, V_2 之间无边。从而不存在 V_1 中顶点到 V_2 中顶点的通路。这与 G 的连通性矛盾。

充分性。对任意顶点 $v \in V(G)$，令 $N_G^{(k)}(v)$ 为与 v 的距离小于等于 k 的顶点的集合，$N_G^{(0)}(v) = \{v\}$。对任意 $k \in \mathbb{N}$，显然有 $v \in N_G^{(k)}(v)$，从而 $N_G^{(k)}(v)$ 非空。若 $N_G^{(k)}(v) \neq V(G)$，则 $\{N_G^{(k)}(v), V(G)-N_G^{(k)}(v)\}$ 是 $V(G)$ 的一个划分，从而由条件二可知，存在 $N_G^{(k)}(v)$ 到 $V(G)-N^{(k)}$ 的边，而 $V(G)-N^{(k)}$ 中与这些边关联的顶点将属于 $N_G^{(k+1)}(v)$。从而 $N_G^{(0)}(v) \subset N_G^{(1)}(v) \subset \cdots \subset N_G^{(k)}(v) \subset N_G^{(k+1)}(v) \subset \cdots \subseteq G$。由于 G 是有限图，所以一过程必将在有限步后结束(事实上，当 $N_G^{(k)}(v) \neq V(G)$ 时，$N_G^{(k+1)}(v)$ 至少比 $N_G^{(k)}(v)$ 多一个顶点，从而 $|N_G^{(k)}(v)| \geq k$，当 $k \geq n$ 时，必有 $N_G^{(k)}(v) = V(G)$)。这就是说，v 与 G 中的每一个顶点之间都有通路。由 v 的任意性知，G 是连通图。 □

4. 不存在。

证明: 反设存在这样的 5 个国家。考虑地图的对偶图 G^*。由于地图是平面图，所以地图的对偶图也是平面图。又由于每个国家都是一块连通的区域，所以每个国家在对偶图中恰好对应一个顶点。若任何两个国家都相邻，则这 5 个国家在对偶图中所对应的顶点将构成 K_5，从而有 $K_5 \subseteq G^*$，G^* 不是平面图。矛盾。 □

5. 不可能。

证明: 以这 $3 \times 3 \times 3$ 个小块为顶点集 $V(G)$，在两个顶点间添加边当且仅当它们所对就的小块有公共的侧面。若在老鼠起点所在的角和立方体的中心之间再添一条边，则题目的问题等价于：G 中是否存在 27 阶圈(哈密顿回路)?

注意到，若令 V_1 为大立方体的 8 个角对应的顶点和大立方体 6 个侧面中央的 6 个小立方体所对应的顶点。令 V_2 为 G 中其余的顶点(即，12 个侧棱中段所对应的顶点和大立方体中心所对应的顶点)，则 $G = \langle V_1, V_2, E\rangle$ 是一个二部图。而二部图中无奇圈，从而不可能存在 27 阶的圈。□

6.

(1) 由于整数集对加、减、乘法封闭，所以对 $*$ 运算也封闭。从而 $\langle A, *\rangle$ 是代数系统。对任意 $x, y, z \in A$：

由于 $x * y = x + y - xy = y + x - yx = y * x$，所以运算满足交换律。

由于 $(x * y) * z = x + y + z - xy - xz - yz + xyz = x * (y * z)$，所以运算满足结合律。

由于 $x * x = x + x - x^2$，当 $x \neq 0, 1$ 时，$x * x \neq x$，所以运算不满足幂等律。

由于 $x * 0 = 0 * x = x$，因此有运算有单位元 $0 \in \mathbb{Z}$。

由 $x * y = x + y - xy = 0$ 解得：当 $x = 1$ 时，等式无解。当 $x \neq 1$ 时，$y = \dfrac{x}{x-1}$。因此，仅当 $x = 0, 2$ 时，有 $y = x^{-1} \in \mathbb{Z}$。此时 y 分别为 0 和 2。因此，仅 $0, 2$ 为可逆元，它们的逆元即是它们自身。

(2) 由于实数集对减法和绝对值运算封闭，所以对 $*$ 运算也封闭。从而 $\langle A, *\rangle$ 是代数系统。对任意 $x, y, z \in A$：

由于 $x * y = |x - y| = |y - x| = y * x$，所以运算满足交换律。

令 $x = 2, y = z = 1$，则 $(x * y) * z = ||x - y| - z| = 0 \neq 2 = |x - |y - z|| = x * (y * z)$，所以

运算不满足结合律。

由于 $x * x = |x - x| = 0$，当 $x \neq 0$ 时，$x * x \neq x$，所以运算不满足幂等律。

由于对所有 $x, y \in A$，若 $x < 0$，则有 $0 \leq x * y \neq x$，从而 $\langle A, * \rangle$ 没有单位元。

(3) 由于 n 的倍数的乘积仍是 k 的倍数，所以 $A = n\mathbb{Z}$ 对 $*$ 运算封闭。从而 $\langle A, * \rangle$ 是代数系统。

由乘法性质知，$*$ 运算满足交换律和结合律，不满足幂等律。

当 $n = 1$ 时，A 中有单位元 1，1 和 -1 $n \neq 1$ 时，无单位元。

(4) 由对称差的性质可知，A 对 $*$ 运算封闭。从而 $\langle A, * \rangle$ 是代数系统。

由对称差的性质知，运算满足交换律、结合律。

对任意 $x \in A$，有 $x * x = x \oplus x = \varnothing$，当 $x \neq \varnothing$ 时，$x * x \neq x$，所以运算不满足幂等律。

显然 $\varnothing$ 是单位元，且所有元素都是自身的逆元。

(5) 首先证明封闭性。

若 R_1, R_2 是两个等价关系，则 $R_1 \cap R_2$ 显然是自反的(因为对任意 $x \in B$，都有 $\langle x, x \rangle \in R_1, \langle x, x \rangle \in R_2$，所以有 $\langle x, x \rangle \in R_1 \cap R_2$)。对任意 $x, y, z \in B$，若 $\langle x, y \rangle, \langle y, z \rangle \in R_1 \cap R_1$，则由 R_1, R_2 的传递性知，$\langle x, z \rangle \in R_1, \langle x, z \rangle \in R_2$，从而有 $\langle x, z \rangle \in R_1 \cap R_2$，$R_1 \cap R_2$ 是传递的。对任意 $x, y \in B$，若 $\langle x, y \rangle \in R_1 \cap R_2$，则由 R_1, R_2 的对称性知，$\langle y, x \rangle \in R_1, \langle y, x \rangle \in R_2$，从而 $\langle y, x \rangle \in R_1 \cap R_2$，$R_1 \cap R_2$ 是对称的。这就证明了对证明 B 上的等价关系 $R_1, R_2 \in A$，有 $R_1 \cap R_2 \in A$。从而 $\langle A, * \rangle$ 是代数系统。

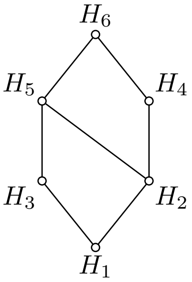
由集合交的性质知，$*$ 运算满足交换律、结合律和幂等律。

B 上的全域关系 E_B 是单位元。除 E_B 外，其它元素无逆元。

7. 因为 $\langle \mathbb{Z}_{12}, \oplus \rangle$ 是循环群，面循环群的子群都是 $\langle a^n \rangle$ 的形式。所以 G 的子群为：

$H_1 = \langle 0 \rangle = \{0\}$；
$H_2 = \langle 6 \rangle = \{0, 6\}$；
$H_3 = \langle 4 \rangle = \{0, 4, 8\}$；
$H_4 = \langle 3 \rangle = \{0, 3, 6, 9\}$；
$H_5 = \langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$；
$H_6 = \langle 1 \rangle = G$；

子群格如下：



易于验证，$L(G)$ 中没有与五角格或钻石格同构的子格，所以 $L(G)$ 是模格，也是分配格。

由于 H_2 和 H_5 没有补元，所以 $L(G)$ 不是有补格，从而不是布尔代数。

8.

证明： 对任意 $g \in G, h \in N$，有

$$\begin{aligned} f(ghg^{-1}) &= f(g)f(h)f(g)^{-1} && (f\ \text{是同态}) \\ &= f(g)f(g)^{-1}f(h) && (G_2\ \text{是交换群}) \\ &= f(h) && (f(g)f(g)^{-1} = e_2) \end{aligned}$$

由于 $f(ghg^{-1}) = f(h) \Leftrightarrow ghg^{-1}\ker f = h\ker f$。而 $h\ker f \subseteq hN = N$，且 $e_1 \in \ker f$。从而 $ghg^{-1} = ghg^{-1}e_1 \in ghg^{-1}\ker f \subseteq N$。这就证明了 $\forall g \in G, \forall h \in N, ghg^{-1} \in N$，从而证明了 N 是 G 的正规子群。 □

2006 年计算机数学基础

二、集合论与图论部分

1. 是。

证明： 首先证明对任何集合 X, Y，有 $Y = (X \cup Y) - (X - Y)$。这是因为：

$$\begin{aligned} Y &= \varnothing \cup Y && \text{(同一律)} \\ &= (X \cap \sim X) \cup Y && \text{(矛盾律)} \\ &= (X \cup Y) \cap (\sim X \cup Y) && \text{(分配律)} \\ &= (X \cup Y) \cap \sim(X \cap \sim Y) && \text{(德·摩根律)} \\ &= (X \cup Y) - (X - Y) && \text{(补交转换律)} \end{aligned}$$

由题设和上述结论可知，$B = (A \cup B) - (A - B) = (A \cup C) - (A - C) = C$。 □

2.

(1) 无解。反设存在集合 $X = \mathcal{P}(X)$，则由等势的性质有 $X \approx \mathcal{P}(X)$。这与康托定理矛盾。

(2) 有解。$A = \varnothing$ 即为一个解。[1]

3. 由 $R^7 = R^{15}$ 和教材定理 2.18(2) 可知，$R^{2006} = R^{7+249*8+7} = R^{7+7} = R^{14}$。

4. t 的最大值为 k。

证明： 为表述方便，对任意一个由 k 个初级回路(有向或无向)组成的图，记这 k 个初级回路为 $C_1, C_2, \cdots, C_k$。对任意给定的 k，令 $S_k = \{G \mid G \text{ 是由 } k \text{ 个初级回路组成的图}\}$。对任意 $G \in S_k$，令 $f(G)$ 为"使 G 成为欧拉图所应添加的最少边数"(从而 f 是从 S_k 到自然数集的函数)，则题目所求即为 $t_{max} = \max f(S_k)$。

下面首先证明，对任意给定的 k，存在 $G \in S_k$，使得 $f(G) = k$ (从而有 $t_{max} \geq k$)。

考虑这样的 $G \in S_k$，它所对应的初级回路组 $C_1, C_2, \cdots, C_k$ 中，任何两个不同的初级回路 $C_i, C_j (i \neq j)$ 间都没有公共顶点。显然，这样的 G 有且仅有 k 个连通分支，这 k 个连通分支恰为上述 k 个初级回路。由初级回路的性质可知，G 中每个顶点的度数皆为偶数。设 E' 是一个使 $G' = G \cup E'$ 成为欧拉图的最小边集，$H = \langle V', E' \rangle$ 是 E' 的导出子图，则：

(1) 要将两个连通分支连接起来，就需要添加一条横跨两个连通分支的边，所以 H 中的边必须覆盖到 G 的每一个连通分支(即，对每个连通分支 G_i，都存在某条边 $e_j \in E'$，使得 e_j 的某个端点在 G_i 中)，否则，若某个 G_i 中不含 E' 的任何端点，则在 G' 中，$V(G_i)$ 与 $V(G) - V(G_i)$ 间仍然没有边，这与 G' 是连通图矛盾。由于各连通分支间没有公共顶点，所以 H 覆盖 k 个连通分支意味着 H 中至少有 k 个不同的顶点，即 $|V'| \geq k$。

(2) 由于 $G \cup H = G \cup E' = G'$ 是欧拉图，所以 $G \cup H$ 中各顶点仍是偶数。又因为 G 与

---

[1] 可以证明，除空集外，任意有限集合都不是方程 $A = \cup A$ 的解。对于无限的情形则有许多解。详细分析见 1990 年离散真题七 1(2) 的解答。

H 没有公共边，所以对任意 $v \in V(G)$，有 $d_{G\cup H}(v) = d_G(v) + d_H(v)$。因为 $d_G(v)$ 是偶数，所以 $d_H(v)$ 也应是偶数。这就是说，对任意顶点 $v \in V'$ (注意到，由于 H 是一个由边集导出的子图，所以 $v \in V'$ 意味着 v 必与 E' 中的某条边关联，从而 $d_H(v) \geq 1$)，有 $d_H(v) \geq 2$。

综合上述两个条件可知，$2|E'| = \sum\limits_{v\in V'} d(v) \geq 2|V'| \geq 2k$，即 $f(G) = |E'| \geq k$。

这就证明了 $t_{max} \geq k$ (注意到，由于有向图中顶点度数的定义为出度与入度之和，所以若有向图 D 为欧拉图，D 中各顶点的度数也是偶数，上述证明对有向图同样有效)。

下面证明 $t_{max} \leq k$。

对任意给定的图 $G \in S_k$，易见，G 的连通分支数 $p \leq k$。从每个连通分支中各取一个顶点，依次记为 $v_1, v_2, \cdots, v_p$。由于不同的连通分支间不会有公共顶点，所以 $v_1, v_2, \cdots, v_p$ 是互异的。向 G 中添加 p 条边：$\langle v_1, v_2\rangle, \langle v_2, v_3\rangle, \cdots, \langle v_{p-1}, v_p\rangle, \langle v_p, v_1\rangle$ (若 G 为无向图，则将上述 p 条边改为无向边)，易见，得到的新图 G' 是连通的。令 $C_{k+1} = v_1v_2\cdots v_pv_1$，则 $G' = G \cup C_{k+1} = C_1 \cup C_2 \cup \cdots \cup C_k \cup C_{k+1}$。注意到，由于 $v_1, v_2, \cdots, v_p$ 分属 G 的不同连通分支(而不同连通分支间不会有边)，所以 C_{k+1} 的每一条边都不在 G 中。这就是说，C_{k+1} 与 $C_1, C_2, \cdots, C_k$ 没有公共边。从而 G' 是连通的且为 $k+1$ 个边不重的初级回路的并，所以 G' 是欧拉图。这就证明了，对任意 $G \in S_k$，有 $f(G) \leq p \leq k$。由 G 的任意性可知 $t_{max} \leq k$。

综合得，$t_{max} = k$。 □

5.

(1) 2 种。

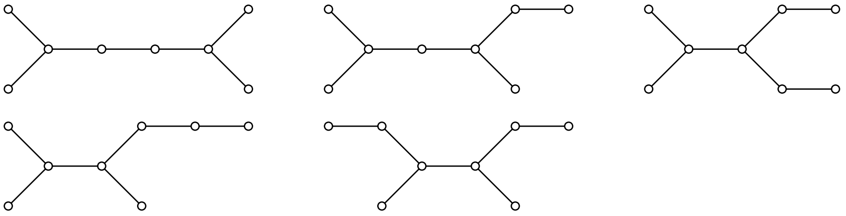
证明： 首先，由于 1-色图只有零图，而零图是平面图，所以给极小非平面图着色至少需要 2 种颜色。另一方面，由于 $K_{3,3}$ 是极小非平面图，且 $\chi(K_{3,3}) = 2$，从而极小非平面图点色数的最小值为 2。 □

(2) 5 种。

证明： 设 G 是 n 阶极小非平面图，$e \in E(G)$ 是 G 中任意一条边。令 $H = G - e$，则 H 是平面图。由教材定理 11.10 可知，$|E(H)| \leq 3n - 6$。从而 $|E(G)| = |E(H)| + 1 \leq 3n - 5$。即 $\sum\limits_{v_i\in V(G)} d(v_i) = 2|E(G)| \leq 6n - 10$。由鸽巢原理可知，$G$ 中存在度数小于等于 5 的顶点 v。易见，$G - v$ 是平面图，从而由 Heawood 定理可知，$G - v$ 是 5-可着色的。仿照 Heawood 定理证明中的换色方法可知，G 也是 5-可着色的。这就是说，极小非平面图的点色数不超过 5。[2]

另一方面，由于 K_5 是极小非平面图，且 $\chi(K_5) = 5$，所以极小非平面图点色数的最大值即为 5。 □

6. 是 3 3 2 2 1 1 1 1。对应的 5 棵非同构的无向树为：



三、代数结构部分

1.

---

[2] 若利用四色定理则可直接证明极小非平面图的点色数不超过 5。

证明： 对任意 $x \in \mathbb{Z}$，分两种情况：

情况一：若 $x = 2k(k \in \mathbb{Z})$ 为偶数，则 $f(\triangle x) = f(2k+1) = (2k+1) \bmod 2 = 1$，而 $\diamond f(x) = \diamond(2k \bmod 2) = \diamond 0 = 1 \bmod 2 = 1$，从而有 $f(\triangle x) = \diamond f(x)$。

情况二：若 $x = 2k+1(k \in \mathbb{Z})$ 为奇数，则 $f(\triangle x) = f(2k+2) = (2k+2) \bmod 2 = 0$，而 $\diamond f(x) = \diamond(2k+1 \bmod 1) = \diamond 1 = 2 \bmod 2 = 0$，从而也有 $f(\triangle x) = \diamond f(x)$。

这就是说，对任意 $x \in \mathbb{Z}$，都有 $f(\triangle x) = \diamond f(x)$，从而 f 是同态。 □

由于 $f(0) = 0, f(1) = 1$，所以 f 是满同态。又由于 $f(2) = f(0) = 0$，所以 f 不是单同态，从而不是同构。

2.

(1)

证明： 对任意 $x, y \in L$，有：

$$\begin{aligned}
f_a(x \vee y) &= (x \vee y) \wedge a && (f_a \text{ 定义}) \\
&= (x \wedge a) \vee (y \wedge a) && (L \text{ 是分配格}) \\
&= f_a(x) \vee f_a(y) && (f_a \text{ 定义}) \\
f_a(x \wedge y) &= (x \wedge y) \wedge a && (f_a \text{ 定义}) \\
&= (x \wedge y) \wedge (a \wedge a) && (a \wedge a = a) \\
&= (x \wedge a) \wedge (y \wedge a) && (\text{交换律、结合律}) \\
&= f_a(x) \wedge f_a(y) && (f_a \text{ 定义})
\end{aligned}$$

这就证明了 f_a 是自同态。同理可证 g_a 是自同态。 □

(2) 由幂集格定义知，对任意 $x \in L$，$x \in f_{\{1\}}(L)$ 当且仅当 $x \subseteq \{1\}$ (充分性：若 $x \subseteq \{1\}$，则 $x = x \cap \{1\} = f_{\{1\}}(x) \in f_{\{1\}}(L)$。必要性：若 $x \in\in f_{\{1\}}(L)$，则 $x = f_{\{1\}}(y) = y \cap \{1\} \subseteq \{1\}$)。从而 $f_{\{1\}}(L) = \{\varnothing, \{1\}\}$，$f_{\{1\}}$ 的同态像为 $\langle \{\varnothing, \{1\}\}, \wedge, \vee \rangle$。

同理可知，对任意 $x \in L$，$x \in g_{\{1\}}(L)$ 当且仅当 $\{1\} \subseteq x$。从而 $g_{\{1\}}(L) = \{\{1\}, \{0,1\}, \{1,2\}, \{0,1,2\}\}$，$g_{\{1\}}$ 的同态像为 $\langle \{\{1\}, \{0,1\}, \{1,2\}, \{0,1,2\}\}, \wedge, \vee \rangle$。

3.

证明： 充分性。若 G 为素数，则由 Lagrange 定理知，G 没有非平凡的子群(从而也没有非平凡的正规子群)，所以 G 是单群。

必要性。设 G 为单群。任取 G 中一个非单位元 $a \in G$ (本题应假定 G 是非平凡的，否则若 $G = \{e\}$，则 G 也是单群，但 $|G| = 1$，不是素数)，则由于 $\langle a \rangle$ 是 G 的正规子群(因为 G 是 Abel 群，所以 G 的一切子群都是正规的)，且 a 不是单位元，所以 $|\langle a \rangle| = |a| > 1$，$\langle a \rangle \neq \{e\}$。由单群定义知，必有 $\langle a \rangle = G$。从而 $G = \{a^k \mid k \in \mathbb{Z}\}$ 是由 a 生成的循环群。下面证明 G 是素数阶的。

反设 G 不是素数阶的，则分两种情况讨论。

情况一：若 G 是无限阶的，则 a 也是无限阶的，从而 $a^2 \neq e, a^2 \neq a$。这就是说，$\langle a^2 \rangle \neq G$ (因为 $a \notin \langle a^2 \rangle$) 且 $\langle a^2 \rangle \neq \{e\}$ (因为 $a^2 \in \langle a^2 \rangle$)，从而 $\langle a^2 \rangle$ 是 G 的一个非平凡的正规子群，这与 G 是单群矛盾。

情况二：若 G 是有限阶的且 $|G|$ 不是素数，则存在 $k \mid |G|, 1 < k < |G|$，而 $1 < |\langle a^k \rangle| = |a^k| = \dfrac{|G|}{k} < |G|$，从而 $\langle a^k \rangle$ 是 G 的一个非平凡的正规子群，矛盾。 □

附录二　教材定理汇总

第一章　集合

定理 1.1 空集是一切集合的子集.

推论 空集是惟一的.

定理 1.2 设 A 的元素个数 $|A| = n$ (n 为自然数), 则 $|\mathcal{P}(A)| = 2^n$.

定理 1.3 (容斥原理) 设 $A_1, A_2, \cdots, A_n$ 为 n 个集合，则

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n}|A_i| - \sum_{i<j}|A_i \cap A_j| + \sum_{i<j<k}|A_i \cap A_j \cap A_k| - \cdots + (-1)^{n-1}|A_1 \cap A_2 \cap \cdots \cap A_n|.$$

定理 1.4 设 $\{A_k\}$ 为集合列，则

$$(1)\quad \underline{\lim_{k\to\infty}} A_k \subseteq \overline{\lim_{k\to\infty}} A_k; \qquad (2)\quad \overline{\lim_{k\to\infty}} A_k = \bigcap_{n=1}^{\infty}\bigcup_{k=n}^{\infty} A_k; \qquad (3)\quad \underline{\lim_{k\to\infty}} A_k = \bigcup_{n=1}^{\infty}\bigcap_{k=n}^{\infty} A_k.$$

定理 1.5 设 $\{A_k\}$ 为集合列，B 为一集合，则

$$(1)\quad B - \overline{\lim_{k\to\infty}} A_k = \underline{\lim_{k\to\infty}}(B - A_k); \qquad (2)\quad B - \underline{\lim_{k\to\infty}} A_k = \overline{\lim_{k\to\infty}}(B - A_k).$$

定理 1.6 设 $\{A_k\}$ 为一个集合列，令 $E = \bigcup\limits_{k\in\mathbb{N}_+} A_k$ 为全集，$B_k = \sim A_k, k = 1, 2, \cdots$，则 $\{B_k\}$ 也是一个集合列，且 $E = \underline{\lim_{k\to\infty}} A_k \cup \overline{\lim_{k\to\infty}} B_k = \overline{\lim_{k\to\infty}} A_k \cup \underline{\lim_{k\to\infty}} B_k$.

第二章　二元关系

定理 2.1 $\langle a, b\rangle = \langle c, d\rangle$ 的充要条件是 $a = c$ 且 $b = d$.

定理 2.2 $\langle a_1, a_2, \cdots, a_n\rangle = \langle b_1, b_2, \cdots, b_n\rangle$ 当且仅当 $a_i = b_i, i = 1, 2, \cdots, n$.

定理 2.3 设 F, G 为二集合，则

(1) $\operatorname{dom}(F \cup G) = \operatorname{dom} F \cup \operatorname{dom} G$;　(2) $\operatorname{ran}(F \cup G) = \operatorname{ran} F \cup \operatorname{ran} G$;

(3) $\operatorname{dom}(F \cap G) \subseteq \operatorname{dom} F \cap \operatorname{dom} G$;　(4) $\operatorname{ran}(F \cap G) \subseteq \operatorname{ran} F \cap \operatorname{ran} G$;

(5) $\operatorname{dom} F - \operatorname{dom} G \subseteq \operatorname{dom}(F - G)$;　(6) $\operatorname{ran} F - \operatorname{ran} G \subseteq \operatorname{ran}(F - G)$.

定理 2.4 设 F 为任一集合，则

(1) $\operatorname{dom} F^{-1} = \operatorname{ran} F$;

(2) $\operatorname{ran} F^{-1} = \operatorname{dom} F$;

(3) $(F^{-1})^{-1} \subseteq \operatorname{dom} F$，当 F 为关系时，等号成立.

定理 2.5 设 R_1, R_2, R_3 为三个集合，则

$$(R_1 \circ R_2) \circ R_3 = R_1 \circ (R_2 \circ R_3).$$

定理 2.6 设 R_1, R_2, R_3 为三个集合，则

(1) $R_1 \circ (R_2 \cup R_3) = R_1 \circ R_2 \cup R_1 \circ R_3$;　(2) $(R_1 \circ R_2) \cup R_3 = R_1 \circ R_3 \cup R_2 \circ R_3$;

(3) $R_1 \circ (R_2 \cap R_3) = R_1 \circ R_2 \cap R_1 \circ R_3$;　(4) $(R_1 \circ R_2) \cap R_3 = R_1 \circ R_3 \cap R_2 \circ R_3$.

定理 2.7 设 F, G 为二集合，则

$$(F \circ G)^{-1} = G^{-1} \circ F^{-1}.$$

定理 2.8 设 $R, S, A, B, \mathscr{A}$ 为集合，$\mathscr{A} \neq \varnothing$，则

(1) $R \upharpoonright (A \cup B) = (R \upharpoonright A) \cup (R \upharpoonright B)$;　(2) $R \upharpoonright \cup\mathscr{A} = \cup\{R \upharpoonright A \mid A \in \mathscr{A}\}$;

(3) $R \upharpoonright (A \cap B) = (R \upharpoonright A) \cap (R \upharpoonright B)$;　(4) $R \upharpoonright \cap\mathscr{A} = \cap\{R \upharpoonright A \mid A \in \mathscr{A}\}$;

(5) $(R \circ S) \upharpoonright A = R \circ (S \upharpoonright A)$.

定理 2.9 设$R, S, A, B, \mathscr{A}$ 为集合，$\mathscr{A} \neq \varnothing$，则

(1) $R[A \cup B] = R[A] \cup R[B]$;　(2) $R[\cup\mathscr{A}] = \cup\{R[A] \mid A \in \mathscr{A}\}$;

(3) $R[A \cap B] = R[A] \cap R[B]$;　(4) $R[\cap\mathscr{A}] = \cap\{R[A] \mid A \in \mathscr{A}\}$;

(5) $R[A] - R[B] \subseteq R[A - B]$;　(6) $(R \circ S)[A] = R[S[A]]$.

定理 2.10 设 $R \subseteq A \times A$，则下面的命题是等价的:

(1) R 是自反的;　(2) $I_A \subseteq R$;

(3) R^{-1} 是自反的;　(4) $M(R)$ 主对角线上的元素全为 1;

(5) $G(R)$ 的每个顶点处均有环.

定理 2.11 设 $R \subseteq A \times A$，则下面的命题是等价的:

(1) R 是反自反的;　　(2) $I_A \cap R = \varnothing$;

(3) R^{-1} n是反自反的;　　(4) $M(R)$ 主对角线上的元素全为 0;

(5) $G(R)$ 的每个顶点处均无环.

定理 2.12 设 $R \subseteq A \times A$，则下面的命题是等价的:

(1) R 是对称的;　　(2) $R^{-1} = R$;

(3) $M(R)$ 是对称的;

(4) $G(R)$ 中任何二个顶点之间若有有向边，必有两条相反的有向边.

定理 2.13 设 $R \subseteq A \times A$，则下面的命题是等价的:

(1) R 是反对称的;　　(2) $R \cap R^{-1} \subseteq I_A$;

(3) 在 $M(R)$ 中，若任意的 $r_{ij} = 1 (i \neq j)$，则必有 $r_{ji} = 0$;

(4) 在 $G(R)$ 中，对于任何二个顶点 $x_i, x_j (i \neq j)$，若有有向边 $\langle x_i, x_j \rangle$，则必没有 $\langle x_j, x_i \rangle$.

定理 2.14 设 $R \subseteq A \times A$，则下面的命题是等价的:

(1) R 是传递的;　　(2) $R \circ R \subseteq R$;

(3) 在 $M(R \circ R)$ 中，若任意的 $r'_{ij} = 1$，则 $M(R)$ 中相应的元素 $r_{ij} = 1$;

(4) 在 $G(R)$ 中，对于任何二个顶点 x_i, x_j, x_k，若有有向边 $\langle x_i, x_j \rangle, \langle x_j, x_k \rangle$，则必有有向边 $\langle x_i, x_k \rangle$ (即若从 x_i 到 x_k 有长为 2 的有向通路，则从 x_i 到 x_k 必有长度为 1 的有向通路).

定理 2.15 设 $R_1, R_2 \subseteq A \times A$.

(1) 若 R_1, R_2 是自反的，则 $R_1^{-1}, R_2^{-1}, R_1 \cup R_2, R_1 \cap R_2, R_1 \circ R_2, R_2 \circ R_1$ 也是自反的;

(2) 若 R_1, R_2 是反自反的，则 $R_1^{-1}, R_2^{-1}, R_1 \cup R_2, R_1 \cap R_2, R_1 - R_2, R_2 - R_1$ 也是反自反的;

(3) 若 R_1, R_2 是对称的，则 $R_1^{-1}, R_2^{-1}, R_1 \cup R_2, R_1 \cap R_2, R_1 - R_2, R_2 - R_1, \sim R_1 (= E_A - R_1), \sim R_2$ 也是对称的;

(4) 若 R_1, R_2 是反对称的，则 $R_1^{-1}, R_2^{-1}, R_1 \cap R_2, R_1 - R_2, R_2 - R_1$ 也是反对称的;

(5) 若 R_1, R_2 是传递的，则 $R_1^{-1}, R_2^{-1}, R_1 \cap R_2$ 也是传递的.

定理 2.16 设 A 为含 n 个元素的有穷集合，$R \subseteq A \times A$，则存在自然数 s, t，且满足 $0 \leq s < t \leq 2^{n^2}$，使得 $R^s = R^t$.

定理 2.17 设 $R \subseteq A \times A$，m, n 为任意的自然数，则下面的等式成立:

(1) $R^m \circ R^n = R^{m+n}$;　　(2) $(R^m)^n = R^{mn}$.

定理 2.18 设 $R \subseteq A \times A$，若存在自然数 $s, t (s < t)$，使得 $R^s = R^t$，则下面的等式成立:

(1) $R^{s+k} = R^{s+t}, \forall k \in \mathbb{N}$;

(2) $R^{s+kp+i} = R^{s+i}$，其中 $k, i \in \mathbb{N}, p = t - s$;

(3) 令 $S = \{R^0, R^1, \cdots, R^{t-1}\}$，则对于任意 $q \in \mathbb{N}$，均有 $R^q \in S$.

定理 2.19 设 $R \subseteq A \times A$ 且 $A \neq \varnothing$，则

(1) R 是自反的当且仅当 $r(R) = R$;

(2) R 是对称的当且仅当 $s(R) = R$;

(3) R 是传递的当且仅当 $t(R) = R$.

定理 2.20 设集合 $A \neq \varnothing$，$R_1, R_2 \subseteq A \times A$，且 $R_1 \subseteq R_2$，则

(1) $r(R_1) \subseteq r(R_2)$;　　(2) $s(R_1) \subseteq s(R_2)$;　　(3) $t(R_1) \subseteq t(R_2)$.

定理 2.21 设 $A \neq \varnothing$，$R_1, R_2 \subseteq A \times A$，则下列各式成立：

(1) $r(R_1 \cup R_2) = r(R_1) \cup r(R_2)$;　　(2) $s(R_1 \cup R_2) = s(R_1) \cup s(R_2)$;

(3) $t(R_1) \cup t(R_2) \subseteq t(R_1 \cup R_2)$.

定理 2.22 设 $R \subseteq A \times A$ 且 $A \neq \varnothing$，则

$$r(R) = R \cup I_A.$$

定理 2.23 设 $R \subseteq A \times A$ 且 $A \neq \varnothing$，则

$$s(R) = R \cup R^{-1}.$$

定理 2.24 设 $R \subseteq A \times A$ 且 $A \neq \varnothing$，则

$$t(R) = R \cup R^2 \cup \cdots .$$

推论 设 A 为非空且为有穷集合，$R \subseteq A \times A$，则存在自然数 l，使得

$$t(R) = R \cup R^2 \cup \cdots \cup R^l.$$

定理 2.25 设 $R \subseteq A \times A$ 且 $A \neq \varnothing$，则

(1) 若 R 是自反的，则 $s(R)$ 和 $t(R)$ 也是自反的；

(2) 若 R 是对称的，则 $r(R)$ 和 $t(R)$ 也是对称的；

(3) 若 R 是传递的，则 $r(R)$ 也是传递的.

定理 2.26 设 $R \subseteq A \times A \wedge A \neq \varnothing$，则

(1) $rs(R) = sr(R)$;

(2) $rt(R) = tr(R)$;

(3) $st(R) \subseteq ts(R)$.

定理 2.27 设 R 是非空集合 A 上的等价关系，对于任意的 $x, y \in A$，下面各式成立：

(1) $[x]_R \neq \varnothing$ 且 $[x]_R \subseteq A$;　　(2) 若 $\langle x, y\rangle \in R$，则 $[x]_R = [y]_R$;

(3) 若 $\langle x, y\rangle \notin R$，则 $[x]_R \cap [y]_R = \varnothing$;　　(4) $\cup\{[x]_R \mid x \in A\} = A$.

定理 2.28 设 A 为一个非空集合.

(1) 设 R 为 A 上的任意一个等价关系，则 A 关于 R 的商集 A/R 为 A 的一个划分；

(2) 设 $\mathscr{A}$ 为 A 上的任意一个划分，令 $R_{\mathscr{A}} = \{\langle x, y\rangle \mid x, y \in A \wedge x, y$ 属于 $\mathscr{A}$ 的同一个划分块$\}$，则 $R_{\mathscr{A}}$ 是为 A 上的等价关系.

定理 2.29 设 $\preccurlyeq$ 为非空集合 A 上的偏序关系，$\prec$ 为 A 上的拟序关系. 则

(1) $\prec$ 是反对称的；

(2) $\preccurlyeq - I_A$ 为 A 上的拟序关系；

(3) $\prec \cup I_A$ 为 A 上的偏序关系.

定理 2.30 设 $\prec$ 为非空集合 A 上的拟序关系，则 $\forall x, y \in A$，

(1) $x \prec y, x = y, y \prec x$，三式中至多有一式成立；

(2) 若 $(x \prec y \vee x = y) \wedge (y \prec x \vee x = y)$，则 $x = y$.

定理 2.31 设 $\langle A, \preccurlyeq\rangle$ 为一个偏序集，若 A 中最长链的长度为 n，则

(1) A 中存在极大元；

(2) A 存在 n 个划分块的划分，每个划分块都是反链.

第三章　函数

定理 3.1 设 $f:C\to D$，则 f 为单射的，$\mathscr{C}$ 为 C 的非空的子集族，$C_1,C_2\subseteq C$，则

(1) $f(\cup\mathscr{C})=\cup\{f(A)\mid A\in\mathscr{C}\}$;

(2) $f(\cap\mathscr{C})=\cap\{f(A)\mid A\in\mathscr{C}\}$;

(3) $f(C_1-C_2)=f(C_1)-f(C_2)$.

定理 3.2 设 $f:C\to D$，$D_1,D_2\subseteq D$，$\mathscr{D}$ 是 D 的非空子集族，则

(1) $f^{-1}(\cup\mathscr{D})=\cup\{f^{-1}(D)\mid D\in\mathscr{D}\}$;

(2) $f^{-1}(\cap\mathscr{D})=\cap\{f^{-1}(D)\mid D\in\mathscr{D}\}$;

(3) $f^{-1}(D_1-D_2)=f^{-1}(D_1)-f^{-1}(D_2)$.

定理 3.3 设 $g:A\to B$，$f:B\to C$，则 $f\circ g:A\to C$，且对于任意的 $x\in A$，

$$f\circ g(x)=f(g(x)).$$

定理 3.4 设 $g:A\to B$，$f:B\to C$.

(1) 如果 f 和 g 都是满射的，则 $f\circ g$ 是满射的;

(2) 如果 f 和 g 都是单射的，则 $f\circ g$ 是单射的;

(3) 如果 f 和 g 都是双射的，则 $f\circ g$ 是双射的.

定理 3.5 设 $g:A\to B$，$f:B\to C$.

(1) 如果 $f\circ g$ 是满射的，则 f 是满射的;

(2) 如果 $f\circ g$ 是单射的，则 g 是单射的;

(3) 如果 $f\circ g$ 是双射的，则 g 是单射的，f 是满射的.

定理 3.6 设 $f:A\to B$，I_A,I_B 分别为 A 上和 B 上的恒等函数，则

$$f\circ I_A=I_B\circ f.$$

定理 3.7 设 $f:\mathbb{R}\to\mathbb{R}$，$g:\mathbb{R}\to\mathbb{R}$，已知 f 和 g 按实数集上的“$\leq$”关系都是单调增加的，则 $f\circ g$ 也是单调增加的.

定理 3.8 设 A 为一个集合，A^{-1} 为函数当且仅当 A 为单根的.

推论 设 R 为二元关系，R 为函数当且仅当 R^{-1} 是单根的.

定理 3.9 设 $f:A\to B$，且 f 为双射函数，则 $f^{-1}:B\to A$，且也为双射函数.

定理 3.10 设 $f:A\to B$，且 $A\neq\varnothing$.

(1) f 存在左逆当且仅当 f 是单射的;

(2) f 存在右逆当且仅当 f 是满射的;

(3) f 既有左逆又有右逆当且仅当 f 是双射的;

(4) 如果 f 是双射的，则 f 的左逆与右逆相等.

第四章　自然数

定理 4.1 $\mathbb{N}$ 是归纳集.

定理 4.2 设 $\mathbb{N}$ 为自然数的集合，$\sigma:\mathbb{N}\to\mathbb{N}$，且 $\sigma(n)=n^+$ (称 σ 为后继函数)，则 $\langle\mathbb{N},\sigma,\varnothing\rangle$ 是 Peano 系统.

定理 4.3 任意自然数的元素都是它的子集.

定理 4.4 对于任意的自然数 m,n，则 $m^+\in n^+$ 当且仅当 $m\in n$.

定理 4.5 任何自然数都不是自己的元素.

定理 4.6 空集属于除零外的一切自然数.

定理 4.7 (三歧性定理) 对于任意的自然数 m,n，下面三式中有且仅有一式成立:

$$m\in n, m=n, n\in m.$$

定理 4.8 ($\mathbb{N}$ 上的递归定理) 设 A 为一个集合，且 $a\in A$，$F:A\to A$，则存在惟一的一个函数 $h:\mathbb{N}\to A$，使得 $h(0)=a$，且对于任意 $n\in\mathbb{N}$，

$$h(n^+)=F(h(n)).$$

定理 4.9 设 $\langle M,F,e\rangle$ 为任意一个 Peano 系统，则 $\langle\mathbb{N},\sigma,0\rangle\sim\langle M,F,e\rangle$.

定理 4.10 设 A 为一个集合，则下面的命题是等价的:

(1)　A 是传递集;

(2)　$\cup A\subseteq A$;

(3)　对于任意的 $y\in A$，则 $y\subseteq A$;

(4)　$A\subseteq\mathcal{P}(A)$.

定理 4.11 设 A 为一个集合，则 A 为传递集当且仅当 $\mathcal{P}(A)$ 为传递集.

定理 4.12 设 A 是传递集，则 $\cup(A^+)=A$.

定理 4.13 每个自然数都是传递集.

定理 4.14 自然数集合 $\mathbb{N}$ 是传递集.

定理 4.15 设 $m,n\in\mathbb{N}$，则

$$m+0=m, \tag{加法规则 1}$$
$$m+n^+=(m+n)^+. \tag{加法规则 2}$$

定理 4.16 设 $m,n\in\mathbb{N}$，则

$$m\cdot 0=0, \tag{乘法规则 1}$$
$$m\cdot n^+=m\cdot n+m. \tag{乘法规则 2}$$

定理 4.17 对于任意的自然数 m,n，则

$$m^0=1, \tag{指数运算规则 1}$$
$$m^{n^+}=m^n\cdot m. \tag{指数运算规则 2}$$

定理 4.18 设 $m, n, k \in \mathbb{N}$，则

(1) $m + (n + k) = (m + n) + k$;

(2) $m + n = n + m$;

(3) $m \cdot (n + k) = m \cdot n + m \cdot k$;

(4) $m \cdot (n \cdot k) = (m \cdot n) \cdot k$;

(5) $m \cdot n = n \cdot m$.

定理 4.19 $\underline{\in}_{\mathbb{N}}$ $(\leq_{\mathbb{N}})$ 为 $\mathbb{N}$ 上的线序关系，$\in_{\mathbb{N}}$ $(<_{\mathbb{N}})$ 为 $\mathbb{N}$ 上的拟线序关系.

定理 4.20 设 $m, n, k \in \mathbb{N}$，则

(1) $m \in n \Leftrightarrow (m + k) \in (n + k)$ $(m < n \Leftrightarrow m + k < n + k)$;

(2) $m \in n \Leftrightarrow m \cdot k \in n \cdot k$ $(m < n \Leftrightarrow m \cdot k < n \cdot k), k \neq 0$.

定理 4.21 设 n, m, k 为自然数，

(1) 如果 $m + k = n + k$，则 $m = n$;

(2) 如果 $k \neq 0$，且 $m \cdot k = n \cdot k$，则 $m = n$.

定理 4.22 ($\mathbb{N}$ 上的良序定理) 设 A 为 $\mathbb{N}$ 的非空子集，则存在惟一的 $m \in A$，使得对于一切的 $n \in A$，有 $m \underline{\in} n$ (这样的 m 称为 A 的最小元).

定理 4.23 ($\mathbb{N}$ 上的强归纳原则) 设 A 为 $\mathbb{N}$ 的一个子集，对于任意的 $n \in \mathbb{N}$，如果小于 n 的元素都属于 A，就有 $n \in A$，则 $A = \mathbb{N}$.

第五章　基数(势)

定理 5.1 (1) $\mathbb{Z} \approx \mathbb{N}$; (2) $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$; (3) $\mathbb{N} \approx \mathbb{Q}$; (4) $(0,1) \approx \mathbb{R}$; (5) $[0,1] \approx (0,1)$.

定理 5.2 设 A 为任意的集合，则 $\mathcal{P}(A) \approx (A \to 2)$，其中 $(A \to 2)$ 为 2^A，即 A 到 $2 = \{0,1\}$ 的全体函数.

定理 5.3 设 A, B, C 为任意的集合，则

(1) $A \approx A$;

(2) 若 $A \approx B$，则 $B \approx A$;

(3) 若 $A \approx B$ 且 $B \approx C$，则 $A \approx C$.

定理 5.4 (康托定理)

(1) $\mathbb{N} \not\approx \mathbb{R}$;

(2) 设 A 为任意的集合，则 $A \not\approx \mathcal{P}(A)$.

定理 5.5 不存在与自己的真子集等势的自然数.

推论 1 不存在与自己的真子集等势的有穷集合.

推论 2

(1) 任何与自己的真子集等势的集合都是无穷集.

(2) $\mathbb{N}$ 是无穷集.

推论 3 任何有穷集合都与惟一的自然数等势.

定理 5.6 任何有穷集合的子集仍为有穷集合.

定理 5.7 设 A, B 为任意二集合，则 $A \preccurlyeq\cdot B$ 当且仅当存在 $C \subseteq B$，使得 $A \approx C$.

推论 设 A, B 为二集合.

(1) 若 $A \subseteq B$，则 $A \preccurlyeq\cdot B$;

(2) 若 $A \approx B$，则 $A \preccurlyeq\cdot B$ 且 $B \preccurlyeq\cdot A$.

定理 5.8 设 A, B, C 为三个集合.

(1) $A \preccurlyeq\cdot A$;

(2) 若 $A \approx B$ 且 $B \preccurlyeq\cdot C$，则 $A \preccurlyeq\cdot C$.

定理 5.9 设 A, B, C, D 为 4 个集合，已知 $A \preccurlyeq\cdot B$ 且 $C \preccurlyeq\cdot D$，则

(1) 若$B \cap D = \varnothing$，则 $A \cup C \preccurlyeq\cdot B \cup D$;

(2) $A \times C \preccurlyeq\cdot B \times D$.

定理 5.10 设 A, B, C, D 为 4 个集合，且已知 $\operatorname{card} A = \operatorname{card} C = \kappa, \operatorname{card} B = \operatorname{card} D = \lambda$，则

$$A \preccurlyeq\cdot B \text{ 当且仅当 } C \preccurlyeq\cdot D.$$

定理 5.11 设 A 为任意一个集合，则

$$\operatorname{card} A < \operatorname{card} \mathcal{P}(A).$$

定理 5.12 (Schröder-Bernstein 定理)
(1) 设 A, B 为二集合，若 $A \preccurlyeq\cdot B$ 且 $B \preccurlyeq\cdot A$，则 $A \approx B$；

(2) 设 κ, λ 为二基数，若 $\kappa \leq \lambda$ 且 $\lambda \leq \kappa$，则 $\kappa = \lambda$.

定理 5.13 $\mathbb{R} \approx (\mathbb{N} \to 2)$，其中 $\mathbb{N} \to 2 = 2^{\mathbb{N}}$.

定理 5.14
(1) 设 A 为任意的无穷集合，则 $\mathbb{N} \preccurlyeq\cdot A$；

(2) 设 κ 为任意的无穷基数，则 $\aleph_0 \leq \kappa$.

推论 1 设 κ 为任意的基数，$\kappa < \aleph_0$ 当且仅当 κ 是有穷基数.

推论 2 有穷集合的子集一定是有穷集合.

推论 3 设 A 是 $\mathbb{N}$ 的无穷子集，则 $\operatorname{card} A = \aleph_0$.

定理 5.15 集合 A 是无穷可数集当且仅当 A 可以写成如下形式:

$$\{a_1, a_2, \cdots, a_n, \cdots\}.$$

定理 5.16 可数集的子集是可数集.

定理 5.17 可数个可数集的并集是可数集.

定理 5.18 设 A 为无穷集，则 $\mathcal{P}(A)$ 不是可数集.

定理 5.19 设 K_1, K_2, L_1, L_2 为 4 个集合，若 $K_1 \approx K_2, L_1 \approx L_2$，则
(1) 如果 $K_1 \cap L_1 = K_2 \cap L_2 = \varnothing$，则 $K_1 \cup L_1 \approx K_2 \cup L_2$；

(2) $K_1 \times L_1 \approx K_2 \times L_2$；

(3) $L_1 \to K_1 \approx L_2 \to K_2$.

定理 5.20
(1) 设 A 为一集合，则 $2^{\operatorname{card} A} = \operatorname{card} \mathcal{P}(A)$；

(2) 设 κ 为一基数，则 $\kappa < 2^{\kappa}$.

推论 (1) $\operatorname{card} \mathcal{P}(\mathbb{N}) = 2^{\aleph_0}$； (2) $\operatorname{card} \mathcal{P}(\mathbb{R}) = 2^{\aleph}$； (3) $\aleph = 2^{\aleph_0}$.

定理 5.21 设 κ, λ, μ 是三个任意的基数，则
(1) $\kappa + \lambda = \lambda + \kappa$, $\kappa \cdot \lambda = \lambda \cdot \kappa$； (2) $\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu$, $\kappa \cdot (\lambda \cdot \mu) = (\kappa \cdot \lambda) \cdot \mu$

(3) $\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$； (4) $\kappa^{\lambda+\mu} = \kappa^{\lambda} \cdot \kappa^{\mu}$；

(5) $(\kappa \cdot \lambda)^{\mu} = \kappa^{\mu} \cdot \lambda^{\mu}$； (6) $(\kappa^{\lambda})^{\mu} = \kappa^{\lambda \cdot \mu}$.

推论 设 κ, λ 为任意二基数，则
(1) $\kappa + (\lambda + 1) = (\kappa + \lambda) + 1$； (2) $\kappa \cdot (\lambda + 1) = \kappa \cdot \lambda + \kappa$； (3) $\kappa^{\lambda+1} = \kappa^{\lambda} \cdot \kappa$

定理 5.22 设 κ, λ, μ 为三个基数，若 $\kappa \leq \lambda$，则
(1) $\kappa + \mu \leq \lambda + \mu$； (2) $\kappa \cdot \mu \leq \lambda \cdot \mu$；

(3) $\kappa^{\mu} \leq \lambda^{\mu}$； (4) $\mu^{\kappa} \leq \mu^{\lambda}$，$\kappa, \mu$ 不同时为 0.

定理 5.23 设 κ 为任意的无穷基数，则 $\kappa \cdot \kappa = \kappa$.

定理 5.24 设 κ, λ 为二基数，其中较大的为无穷基数，较小的不为 0，则

$$\kappa + \lambda = \kappa \cdot \lambda = \max\{\kappa, \lambda\}.$$

推论 设 κ 为一无穷基数，则 $\kappa + \kappa = \kappa \cdot \kappa = \kappa$.

定理 5.25 设 κ 为无穷基数，则 $\kappa^{\kappa} = 2^{\kappa}$.

第六章　序数*

定理 6.1 设 $\langle A, \prec\rangle$ 为拟线序集[1]，$\prec$ 为 $A \neq \varnothing$ 上的良序关系，当且仅当不存在函数 $f: \mathbb{N} \to A$，使得对于任意 $n \in \mathbb{N}$，有 $f(n^+) \prec f(n)$.

定理 6.2 设 $\langle A, \prec_1\rangle, \langle B, \prec_2\rangle, \langle C, \prec_3\rangle$ 为三个拟序集，则

(1) $\langle A, \prec_1\rangle \cong \langle A, \prec_1\rangle$;

(2) 若 $\langle A, \prec_1\rangle \cong \langle B, \prec_2\rangle$，则 $\langle B, \prec_2\rangle \cong \langle A, \prec_1\rangle$;

(3) 若 $\langle A, \prec_1\rangle \cong \langle B, \prec_2\rangle$ 且 $\langle B, \prec_2\rangle \cong \langle C, \prec_3\rangle$，则 $\langle A, \prec_1\rangle \cong \langle C, \prec_3\rangle$.

定理 6.3 设 $f: A \to B$ 且为单射，$\prec_B$ 为 B 上的拟序关系，在 A 上定义关系 $\prec_A$ 如下，对于任意的 $x, y \in A$，$x \prec_A y \Leftrightarrow f(x) \prec_B f(y)$，则

(1) $\prec_A$ 为 A 上的拟序关系;

(2) 若 $\prec_B$ 为 B 上的拟线序(拟全序)关系，则 $\prec_A$ 为 A 上的拟线序关系;

(3) 若 $\prec_B$ 为 B 上的良序关系，则 $\prec_A$ 为 A 上的良序关系.

定理 6.4 设 A, B 为二集合，且 $B \subseteq A$.

(1) 若 $\prec_A$ 为 A 上的拟序关系，则 $\prec_A\restriction B$ 为 B 上的拟序关系;

(2) 若 $\prec_A$ 为 A 上的拟线序关系，则 $\prec_A\restriction B$ 为 B 上的拟线序关系;

(3) 若 $\prec_A$ 为 A 上的良序关系，则 $\prec_A\restriction B$ 为 B 上的良序关系.

定理 6.5 (超限归纳原理) 设 $\prec$ 为 A 上的良序，B 是 A 关于 $\prec$ 的归纳子集，则 $B = A$.

定理 6.6 设 $\prec$ 为 A 上的拟线序，如果 A 上任何关于 $\prec$ 的归纳子集都与 A 是相等的，则 $\prec$ 为 A 上的良序.

超限递归定理模式 对于任意的公式 $\gamma(x, y)$，下面叙述的是一条定理:

设 $\prec$ 为集合 A 上良序，若 $\forall f \exists! y \gamma(f, y)$ 成立，则存在惟一的一个以 A 为定义域的函数 F，$\forall t \in A, \gamma(F \restriction \operatorname{seg} t, F(t))$ 成立.

定理 6.7 设 $\langle A, \prec_A\rangle, \langle B, \prec_B\rangle$ 为两个良序集，则下面三种情况至少成立其一:

(1) $\langle A, \prec_A\rangle \cong \langle B, \prec_B\rangle$;

(2) $\langle A, \prec_A\rangle \cong \langle \operatorname{seg} b, \prec_B^0\rangle, b \in B$;

---

[1] 教材中的原文是 "设 $\langle A, \prec\rangle$ 是拟序集"。然而，易于验证，若 $\langle A, \prec\rangle$ 不是拟线序集，上述定理不成立(一个最简单的反例是 $\prec = \varnothing$ 的情况，注意到，$\varnothing$ 是在任何非空集合上都是拟序，但不是拟线序，更不是良序)。为说明 "拟线序" 这一条件的必要性，下面再举一个 nontrivial 的反例: 令 $A = \mathbb{N}, \prec = \{\langle 0, x\rangle \mid x \in \mathbb{N}_+\}$。则 $\langle \mathbb{N}, \prec\rangle$ 显然是拟序集，且 $\operatorname{dom}(\prec) = \{0\}$，$\operatorname{ran}(\prec) = \mathbb{N}_+$，从而 $\operatorname{dom}(\prec) \cap \operatorname{ran}(\prec) = \varnothing$，也即，对任意 $x, y, z \in \mathbb{N}$，若有 $y \prec x$ (从而 $y \in \operatorname{dom}(\prec)$)，则不可能有 $z \prec y$ (因为 $y \notin \operatorname{ran}(\prec)$)。这样一来，就不可能存在定理所描述的 $f: \mathbb{N} \to \mathbb{N}$ (因为无论 $f(1)$ 取何值，$f(1) \prec f(0)$ 和 $f(2) \prec f(1)$ 都不可能同时成立)。所以，$\langle \mathbb{N}, \prec\rangle$ 满足定理所述的条件。但 $\mathbb{N}$ 的非空子集 $\mathbb{N}_+$ 却没有最小元，从而 $\langle \mathbb{N}, \prec\rangle$ 不是良序集。(事实上，教材中此定理证明的充分性部分用到: "任取 $b_0 \in B$，则 b_0 不是 B 的最小元，因而存在 $b_1 \in B$，使得 $b_1 \prec b_0$。" 而 "b_0 不是最小元" 只表明 "存在 $b_1 \in B$，使 $b_0 \neq b_1 \wedge b_0 \nprec b_1$"，若 $\prec$ 不是拟线序，就不能由此推出 $b_1 \prec b_0$。)

(3) $\langle \operatorname{seg} a, \prec_A^0 \rangle \cong \langle B, \prec_B \rangle, a \in A$.

其中，$\prec_A^0$，$\prec_B^0$ 分别为 $\prec_A$ 在 $\operatorname{seg} a$ 上的限制和 $\prec_B$ 在 $\operatorname{seg} b$ 上的限制.

定理 6.8 设 $\prec$ 为集合 A 上的良序，则惟一存在一个以 A 为定义域的函数 E，使得对于任意的 $t \in A$，$E(t) = \operatorname{ran}(E \upharpoonright \operatorname{seg} t) = \{E(x) \mid x \prec t\}$.

定理 6.9 设 $\langle A, \prec \rangle$ 为良序集，E 为前段值域函数，α 是 $\langle A, \prec \rangle$ 的 $\in$-象，则

(1) $\forall t \in A, E(t) \notin E(t)$;

(2) E 为 A 与 α 之间的双射函数;

(3) $\forall s, t \in A, s \prec t \Leftrightarrow E(s) \in E(t)$;

(4) $\alpha = \operatorname{ran} E$ 是传递集.

定理 6.10 两个良序集是同构的当且仅当它们具有相同的 $\in$-象.

定理 6.11 同构的良序集具有相同的序数.

定理 6.12 设 α 按属于关系是良序的，并且 α 是传递集，则 α 是一个序数(即，α 是 $\langle \alpha, \in_\alpha \rangle$ 的 $\in$-象).

定理 6.13 设 α, β, γ 为三个序数，则

(1) α 的元素为序数(即任何序数的元素还是序数);

(2) $\alpha \notin \alpha$ (反自反性);

(3) $\alpha \in \beta \wedge \beta \in \gamma$，则 $\alpha \in \gamma$ (传递性);

(4) $\alpha \in \beta, \alpha = \beta, \beta \in \alpha$ 有且仅有一式成立(序数之间具有三歧性);

(5) 由序数构成的非空集，按属于关系有最小元.

定理 6.14 设 α, β 为任意两个序数，$\alpha < \beta, \alpha = \beta, \alpha > \beta$，三式有且仅有一式成立.

定理 6.15

(1) 任何以序数为元素的传递集合是序数;

(2) 0 是序数;

(3) 若 α 是序数，则 $\alpha^+ = \alpha \cup \{\alpha\}$ 为序数;

(4) 若集合 A 是以序数为元素的集合，则 $\cup A$ 为序数.

定理 6.16

(1) 一切自然数都序数.

(2) 自然数集合 $\mathbb{N}$ 是序数(当 $\mathbb{N}$ 作为序数时，将它记为 ω)，$\omega, \omega^+, \omega^{++}, \omega^{+++}, \cdots$ 是序数.

(3) 设 A 是以序数为元素的集合，则 $\cup A$ 为 A 的关于属于等于关系的最小上界.

(4) 设 α 为一序数，则 α^+ 是大于 α 的最小序数.

(5) 设 α 为一序数，则 $\alpha = \{x \mid x \text{ 是序数 } \wedge x < \alpha\}$.

定理 6.17 (Hartogs 定理) 对于任何集合 A，都存在序数 α，使得 $A \preccurlyeq\cdot\, \alpha$.

定理 6.18 (良序定理) 对于任意的集合 A，都存在 A 上的良序.

定理 6.19 (命数定理) 对于任何集合 A，都存在序数 α，使得 $A \approx \alpha$.

定理 6.20

(1) 对于任意的集合 A 和 B，$\operatorname{card} A = \operatorname{card} B \Leftrightarrow A \approx B$;

(2) 对于任意的有穷集合 A，$\operatorname{card} A$ 是与 A 等势的惟一的自然数.

定理 6.21 设 α 为一序数，则 α 为初始序数当且仅当 α 为一个基数.

第七章　图

定理 7.1 (图论基本定理) 设 $G = \langle V, E \rangle$ 为一个无向图，$V = \{v_1, v_2, \cdots, v_n\}$，$|E| = m$，则

$$\sum_{i=1}^{n} d(v_i) = 2m.$$

定理 7.2 (图论基本定理) 设 $D = \langle V, E \rangle$ 为一个有向图，$V = \{v_1, v_2, \cdots, v_n\}$，$|E| = m$，则

$$\sum_{i=1}^{n} d(v_i) = 2m \text{ 且 } \sum_{i=1}^{n} d^+(v_i) = \sum_{i=1}^{n} d^-(v_i) = m.$$

推论 任何图 G (无向图或有向图)中，奇度数顶点的个数是偶数.

定理 7.3 $\mathbf{d} = (d_1, d_2, \cdots, d_n)$ ($d_i \geq 0$ 且为整数，$i = 1, 2, \cdots, n$)是可图化的当且仅当

$$\sum_{i=1}^{n} d_i = 0 \pmod 2.$$

定理 7.4 设非负整数列 $\mathbf{d} = (d_1, d_2, \cdots, d_n), (n-1) \geq d_1 \geq d_2 \geq \cdots \geq d_n \geq 0$，则 $\mathbf{d}$ 是可简单图化的当且仅当对于每个整数 r，$1 \leq r \leq (n-1)$，

$$\sum_{i=1}^{r} d_i \leq r(r-1) + \sum_{i=r+1}^{n} \min\{r, d_i\} \text{ 且 } \sum_{i=1}^{n} d_i = 0 \pmod 2.$$

定理 7.5 设非负整数列 $\mathbf{d} = (d_1, d_2, \cdots, d_n)$，$\sum\limits_{i=1}^{n} d_i = 0 \pmod 2$ 且 $(n-1) \geq d_1 \geq d_2 \geq \cdots \geq d_n \geq 0$，则 $\mathbf{d}$ 是可简单图化的当且仅当 $\mathbf{d}' = (d_2 - 1, d_3 - 1, \cdots, d_{d_1+1} - 1, d_{d_1+2}, \cdots, d_n)$ 是可简单图化的.

定理 7.6 在 n 阶图 G 中，若从顶点 v_i 到 $v_j (v_i \neq v_j)$ 存在通路，则从 v_i 到 v_j 存在长度小于等于 $n-1$ 的通路.

推论 在 n 阶图 G 中，若从顶点 v_i 到 $v_j (v_i \neq v_j)$ 存在通路，则 v_i 到 v_j 一定存在长度小于等于 $n-1$ 的路径.

定理 7.7 在 n 阶图 G 中，若存在 v_i 到自身的回路，则存在 v_i 到自身长度小于等于 n 的回路.

推论 在一个 n 阶图 G 中，若存在 v_i 到自身的简单回路，则一定存在 v_i 到自身的长度小于等于 n 的初级回路(圈).

定理 7.8 一个图 G 为二部图当且仅当图 G 中无奇圈.

定理 7.9 设 G 为 n 阶无向图，若 G 是连通图，则 G 的边数 $m \geq n-1$.

定理 7.10 (Whitney) 对于任意的图 G，均有下面不等式成立:

$$\kappa \leq \lambda \leq \delta,$$

其中 κ, λ, δ 分别为 G 的点连通度、边连通度和最小度.

推论 若 G 是 k-连通图，则 G 必为 k 边-连通图.

定理 7.11 设 G 是 $n(n \geq 6)$ 阶简单无向连通图，$\lambda(G) < \delta(G)$，则必存在由 K_{n_1}, K_{n-n_1} 及在它们之间适当地连入 $\lambda(G)$ 条边，含 G 作为生成子图的图 G^*，其中 $\lambda(G)+2 \leq n_1 \leq \left\lfloor \frac{n}{2} \right\rfloor$.

推论

(1) $\delta(G) \leq \delta(G^*) \leq n_1 - 1 \leq \left\lfloor \frac{n}{2} \right\rfloor - 1$;

(2) G^* 中存在不相邻的顶点 u, v，使得 $d_{G^*}(u) + d_{G^*}(v) \leq n-2$;

(3) $d(G) \geq d(G^*) \geq 3$.

定理 7.12 设 G 是 $n(n \geq 6)$ 阶连通简单无向图.

(1) 若 $\delta(G) \geq \left\lfloor \frac{n}{2} \right\rfloor$，则 $\lambda(G) = \delta(G)$;

(2) 若对于 G 中任意一对不相邻的顶点 u, v 均有 $d(u) + d(v) \geq n-1$，则 $\lambda(G) = \delta(G)$;

(3) 若 $d(G) \leq 2$，则 $\lambda(G) = \delta(G)$.

定理 7.13 设 G 是 n 阶无向简单连通图，且 G 不是完全图 K_n，则

$$\kappa(G) \geq 2\delta(G) - n + 2.$$

定理 7.14 对于给定的正整数 $n, \delta, \kappa, \lambda$，存在 n 阶简单连通无向图 G，使得 $\delta(G) = \delta$，$\kappa(G) = \kappa$，$\lambda(G) = \lambda$ 的充分必要条件是下列三式之一成立:

(1) $0 \leq \kappa \leq \lambda \leq \delta < \left\lfloor \frac{n}{2} \right\rfloor$;

(2) $1 \leq 2\delta - n + 2 \leq \kappa \leq \lambda = \delta < n-1$;

(3) $\kappa = \lambda = \delta = n-1$.

定理 7.15 (Whitney) 设 G 为 $n(n \geq 3)$ 阶无向连通图，G 为 2-连通图当且仅当 G 中任意两个顶点共圈.

定理 7.16 设 G 为 $n(n \geq 3)$ 阶无向图，G 为 2 边-连通图当且仅当 G 中任何两个顶点共简单回路.

定理 7.17 设 v 为无向连通图 G 中的一个顶点，v 为 G 的割点当且仅当存在 $V(G) - v$ 的一个划分: $V(G) - v = V_1 \cup V_2$，使得对于任意的 $u \in V_1$，任意的 $w \in V_2$，v 在每一条 u 到 w 的路径上.

推论 设 v 为无向连通图 G 中的一个顶点，v 为割点当且仅当存在与 v 不同的两个顶点 u 和 w，使 v 处在每一条从 u 到 v 的路径上.

定理 7.18 设 e 为无向连通图 G 中的一条边，e 是 G 的桥当且仅当 e 不在 G 中的任何圈上.

定理 7.19 设 e 为无向连通图 G 中的一条边，e 为桥当且仅当存在 $V(G)$ 的一个划分: $V(G) = V_1 \cup V_2$ 使得对于任意的 $u \in V_1, v \in V_2$，e 在每一个 u 到 v 的路径上.

定理 7.20 设 G 为 $n(n \geq 3)$ 阶无向简单连通图，则下面命题是等价的:

(1) G 是块;

(2) G 中任意二顶点共圈;

(3) G 中任意一个顶点与任意一条边共圈;

(4) G 中任意两条边共圈;

(5) 任给 G 中两个顶点 u, v 和一条边 e，存在从 u 到 v 经过 e 的路径;

(6) 对于 G 中的任意 3 个顶点中的两个顶点，都存在从一个顶点到另一个顶点且含第 3 个顶点的路径;

(7) 对于 G 中任意 3 个顶点中的任意两个顶点，都存在从一个顶点到另一个顶点而不含第 3 个顶点的路径.

定理 7.21 设 D 为 n 阶有向图，D 是强连通的当且仅当 D 中存在回路，它经过 D 中每个顶点至少一次.

定理 7.22 设 D 为 n 阶有向图，D 是单向连通图当且仅当 D 中存在经过每个顶点至少一次的通路.

第八章　欧拉图与哈密顿图

定理 8.1 设 G 是无向连通图，则下面三个命题是等价的:

(1)　G 是欧拉图;

(2)　G 中所有顶点的度数都是偶数;

(3)　G 是若干个边不重的圈的并.

定理 8.2 设 G 是连通的无向图，G 是半欧拉图当且仅当 G 中恰有两个奇度顶点.

定理 8.3 设 D 是连通的有向图，则下面三个命题是等价的:

(1)　D 是欧拉图;

(2)　$\forall v \in V(D)$，$d^+(v) = d^-(v)$;

(3)　D 为若干个边不重的有向初级回路的并.

定理 8.4 设 D 是连通的有向图，D 是半欧拉图当且仅当 D 中恰有两个奇度顶点，其中一个顶点入度比出度大 1，另一个顶点出度比入度大 1，而其余顶点的入度均等于出度.

定理 8.5 设 G 是无向欧拉图，则 Fleury 算法终止时得到的简单通路是欧拉回路.

定理 8.6 设无向图 $G = \langle V, E\rangle$ 是哈密顿图，则对于 V 的任意非空真子集 V_1 均有

$$p(G - V_1) \leq |V_1|$$

其中，$p(G - V_1)$ 为 $G - V_1$ 的连通分支数.

推论 设无向图 $G = \langle V, E\rangle$ 是半哈密顿图，则对于 V 的任意非空真子集 V_1 均有

$$p(G - V_1) \leq |V_1| + 1.$$

定理 8.7 设 G 是 $n(n \geq 2)$ 阶无向简单图，若对于 G 中任意不相邻的顶点 v_i, v_j 均有

$$d(v_i) + d(v_j) \geq n - 1$$

则 G 中存在哈密顿通路.

推论 1 设 G 是 $n(n \geq 3)$ 阶无向简单图，若对于 G 中任意不相邻的顶点 v_i, v_j 均有

$$d(v_i) + d(v_j) \geq n$$

则 G 中存在哈密顿回路，从而 G 是哈密顿图.

推论 2 设 G 是 $n(n \geq 3)$ 阶无向简单图，若对于任意的 $v \in V(G)$，均有 $d(v) \geq \frac{n}{2}$，则 G 为哈密顿图.

定理 8.8 设 u, v 为无向 n 阶简单图 G 中的两个不相邻的顶点，且 $d(u) + d(v) \geq n$，则 G 为哈密顿图当且仅当 $G \cup (u, v)$ 为哈密顿图.

定理 8.9 设 D 为 $n(n \geq 2)$ 阶竞赛图，则 D 具有哈密顿通路.

推论 设 D 为 n 阶有向图，若 D 含 n 阶竞赛图作为子图，则 D 中具有哈密顿通路.

定理 8.10 强连通的竞赛图为哈密顿图.

推论 设 D 为 n 阶有向图，若 D 含 n 阶强连通的竞赛图作为子图，则 D 是哈密顿图.

定理 8.11 完全图 $K_{2k+1}(k \geq 1)$ 中含 k 条边不重的哈密顿回路，且 k 条边不重的哈密顿回路中含 K_{2k+1} 中的全部边.

推论 $K_{2k}(k \geq 2)$ 中含 $k-1$ 条边不重的哈密顿回路，从 K_{2k} 中删除这 $k-1$ 条边哈密顿回路上所有边后所得的图含 k 条彼此不相邻的边.

第九章　树

定理 9.1 设 $G=\langle V,E\rangle$ 为 n 阶 m 条边的无向图，则下面各命题是等价的:

(1) G 是树(连通无回路);

(2) G 中任二顶点之间存在惟一的一条路径;

(3) G 中没有圈，且 $m=n-1$;

(4) G 是连通的，且 $m=n-1$;

(5) G 是连通的，且 G 中任何边均为桥;

(6) G 中没有圈，但在 G 中任二不同顶点 u,v 之间增添边 (u,v)，所得图含惟一的一个圈.

定理 9.2 设 T 是 n 阶非平凡的无向树，则 T 至少有两个片树叶.

定理 9.3 无向图 G 具有生成树当且仅当 G 是连通的.

推论 1 设 G 为 n 阶 m 条边的无向连通图，则 $m\geq n-1$.

推论 2 设 T 是 n 阶 m 条边的无向连通图 G 的一棵生成树，则 T 的余树 $\overline{T}$ 中含 $m-n+1$ 条边.

推论 3 设 T 是连通图 G 的一棵生成树，$\overline{T}$ 为 T 的余树，C 为 G 中任意一圈，则 $E(\overline{T})\cap E(C)\neq\varnothing$.

定理 9.4 设 T 是无向连通图 G 中的一棵生成树，e 为 T 的任意一条弦，则 $T\cup e$ 中含 G 的只含一条弦，其余边均为树枝的圈，而且不同的弦对应的圈是不同的.

定理 9.5 设 T 是连通图 G 的一棵生成树，e 为 T 的一条树枝，则 G 中存在只含树枝 e，其余元素均为弦的割集. 设 e_1,e_2 是 T 的不同的树枝，则它们对应的只含一条树枝的割集是不同的.

定理 9.6 设 $G=\langle V,E\rangle$ 为 n 阶无向连通标定图($V=\{v_1,v_2,\cdots,v_n\}$)，则对 G 的任意非环边 e 均有 $\tau(G)=\tau(G-e)+\tau(G\backslash e)$.

定理 9.7 $\tau(K_n)=n^{n-2}(n\geq 2)$，其中 K_n 为 n 阶标定完全图.

定理 9.8 Ω 对环和运算及数乘运算: $0\cdot G_i=\varnothing$，$1\cdot G_i=G_i$，$i=1,2,\cdots,2^m$，构成数域 $F=\{0,1\}$ 上的 m 维线性空间，其 M 为生成元集.

定理 9.9 设 T 是 n 阶 m 条边的无向连通图 G 的一棵生成树，C_k 是对应弦 e'_k 的基本回路，$k=1,2,\cdots,m-n+1$，则任意的 $r(1\leq r\leq m-n+1)$ 条弦 $e'_{i_1},e'_{i_2},\cdots,e'_{i_r}$ 均在

$$C_{i_1}\oplus C_{i_2}\oplus\cdots\oplus C_{i_r}$$

中，其中 $\oplus$ 为图之间的环和运算.

定理 9.10 设 C_1 和 C_2 是无向图 G 中的任意两个回路(初级的或简单的)，则环和 $C_1\oplus C_2$ 为 G 中环路.

推论 设 C_1,C_2 为无向图 G 中的任意两个环路，则 $C_1\oplus C_2$ 为 G 中环路(即环路对环和运算是封闭的).

定理 9.11 设 G 为无向连通图，T 为 G 的任意一棵生成树，则 G 中任一回路(初级的或简单的)或为 T 的基本回路或为若干个基本回路的环和.

推论 1 无向连通图 G 中任一环路或为某棵生成树的基本回路，或为若干个基本回路的环和.

推论 2 设 G 为 n 阶 m 条边的无向连通图，设 G 中有 s 个回路(初级的或简单的)，则

$$m-n+1 \le s \le 2^{m-n+1}-1.$$

推论 3 设 G 为 n 阶 m 条边的无向连通图，设 s 是 G 中环路数(含 $\varnothing$)，则

$$S = 2^{m-n+1}.$$

定理 9.12 设 G 为 n 阶 m 条边的无向连通图，设 $C_{环}$ 为 G 中环路(含 $\varnothing$)组成的集合，则 $C_{环}$ 是 Ω 的 $m-n+1$ 维的子空间，其中 Ω 是 G 的所有边导出子图的集合.

定理 9.13 连通图 G 中每个割集至少包含 G 的每个生成树的一个树枝.

定理 9.14 设 G 为 n 阶 m 条边的无向连通图，T 是 G 的一棵生成树，$S_{基}$ 为 T 对应的基本割集系统，则对于任意的 $S_{i_1}, S_{i_2}, \cdots, S_{i_k} \in S_{基}$，必有它们对应的树枝 $e'_{i_1}, e'_{i_2}, \cdots, e'_{i_k}$ 均在

$$S_{i_1} \oplus S_{i_2} \oplus \cdots \oplus S_{i_k}$$

中，其中 $\oplus$ 为对称差运算.

定理 9.15 设 S_1, S_2 为无向图 G 的两个断集，则 $S_1 \oplus S_2$ 为 G 中断集，其中 $\oplus$ 为对称差运算.

定理 9.16 设 G 为无向连通图，T 为 G 的任意一棵生成树，则 G 中任一断集或为 T 的基本割集或为若干个基本割集的对称差集.

定理 9.17 设 G 为 n 阶 m 条边的无向连通图，并设 $S_{断} = \{\varnothing\} \cup \{S' \mid S'$ 是 G 的断集的导出子图$\}$，则 $S_{断}$ 为 Ω 的 $n-1$ 维子空间，其中 Ω 是 G 的所有边导出子集集合.

第十章　图的矩阵表示

定理 10.1 n 阶无向连通图 G 的关联矩阵的秩 $r(M(G))=n-1$.

定理 10.2 n 阶无向连通图 G 的基本关联矩阵的秩 $r(M_f(G))=n-1$.

推论 1 设 n 阶无向图 G 有 p 个连通分支，则 $r(M(G))=r(M_f(G))=n-p$，其中 $M_f(G)$ 是从 $M(G)$ 的每个对角块中删除任意一行而得到的矩阵.

推论 2 G 是连通图当且仅当 $r(M(G))=r(M_f(G))=n-1$.

定理 10.3 设 $M_f(G)$ 是 n 阶连通图 G 一个基本关联矩阵. M_f' 是 $M_f(G)$ 中任意 $n-1$ 列组成的方阵，则 M_f' 中各列所对应的边集 $\{e_{i_1},e_{i_2},\cdots,e_{i_{n-1}}\}$ 的导出子图 $G[\{e_{i_1},e_{i_2},\cdots,e_{i_{n-1}}\}]$ 是 G 的生成树当且仅当 M_f' 的行列式 $|M_f'|\neq 0$.

定理 10.4 设 A 是 n 阶有向标定图 D 的邻接矩阵，A 的 $l(l\geq 2)$ 次幂 $A^l=A^{l-1}\cdot A$ 中元素 $a_{ij}^{(l)}$ 为 v_i 到 v_j 长度的 l 的通路数，$\sum\limits_i\sum\limits_j a_{ij}^{(l)}$ 为 D 中长度为 l 的通路总数，则 $\sum\limits_i a_{ii}^{(l)}$ 为 D 中长度为 l 的回路总数.

推论 设 A 是 n 阶有向标定图 D 的邻接矩阵，B_r 中元素 $b_{ij}^{(r)}$ 为 v_i 到 v_j 长度小于等于 r 的通路数，$\sum\limits_i\sum\limits_j b_{ij}^{(r)}$ 为 D 中长度小于等于 r 的通路总数，而 $\sum\limits_i b_{ii}^{(r)}$ 为 D 中长度小于等于 r 的回路数.

定理 10.5 设 G 是 n 阶无向简单图，$V=\{v_1,v_2,\cdots,v_n\}$，A 是 G 的相邻矩阵，A^k 中元素 $a_{ij}^{(k)}\left(=a_{ji}^{(k)}\right)(i\neq j)$ 为 G 中 v_i 到 v_j (v_j 到 v_i)长度为 k 的通路数. 而 $a_{ii}^{(k)}$ 为 v_i 到 v_j 长度为 k 的回路数.

推论 1 在 A^2 中，$a_{ii}^{(2)}=d(v_i)$.

推论 2 若 G 是连通图，对于 $i\neq j, v_i, v_j$ 之间的矩离 $d(v_i,v_j)$ 为使 A^k 中元素 $a_{ij}^{(k)}\neq 0$ 的最小正整数 k.

第十一章　平面图

定理 11.1 图 G 可嵌入球面当且仅当 G 可嵌入平面.

推论 设 $\tilde{G}$ 与 $\tilde{G}'$ 分别是平面图 G 的球面嵌入和平面嵌入，则 $\tilde{G} \cong \tilde{G}'$.

定理 11.2 平面图 G 中所有面的次数之和等于边数 m 的 2 倍:

$$\sum_{i=1}^{n} \deg(R_i) = 2m.$$

定理 11.3 设 R 是平面图 G 的某个平面嵌入 $\tilde{G}$ 的一个内部面，则存在 G 的平面嵌入 $\tilde{G}_1$ 以 R 为外部面.

定理 11.4 G 为 $n(n \geq 3)$ 阶简单的连通平面图，G 为极大平面图当且仅当 G的每个面的次数均为 3.

定理 11.5 $n(n \geq 4)$ 阶极大平面图 G 中，$\delta(G) \geq 3$.

定理 11.6 对于任意的连通的平面图 G，有

$$n - m + r = 2$$

其中，n, m, r 分别为 G 的阶数、边数和面数.

定理 11.7 对于任何具有 $p(p \geq 2)$ 个连通分支的平面图 G，有

$$n - m + r = p + 1$$

成立，其中 n, m, r 分别为 G 的顶点数，边数和面数.

定理 11.8 设 G 是连通的平面图，且 G 的各面的次数至少为 $l(l \geq 3)$，则 G 的边数 m 与顶点数 n 有如下关系:

$$m \leq \frac{l}{l-2}(n-2).$$

定理 11.9 设 G 是有 $p(p \geq 2)$ 个连通分支的平面图，各面的次数至少为 $l(l \geq 3)$，则边数 m 与顶点数 n 有如下关系:

$$m \leq \frac{l}{l-2}(n-p-1).$$

定理 11.10 设 G 是 $n(n \geq 3)$ 阶 m 条边的简单平面图，则

$$m \leq 3n - 6.$$

定理 11.11 设 G 为 n 阶($n \geq 3$) m 条边的极大平面图，则

$$m = 3n - 6.$$

定理 11.12 设 G 是简单的平面图，则 G 中至少存在一个顶点，其度数小于等于 5.

定理 11.13 图 G 是平面图当且仅当 G 不含与 K_5 同胚的子图，也不含与 $K_{3,3}$ 同胚的子图.

定理 11.14 图 G 是平面图当且仅当 G 中没有可以收缩到 K_5 的子图，也没有可以收缩到 $K_{3,3}$ 的子图.

定理 11.15 设 G^* 是连通平面图 G 的对偶图，n^*, m^*, r^* 和 n, m, r 分别为 G^* 和 G 的顶点数、边数和面数，则

(1) $n^* = r$;　(2) $m^* = m$;　(3) $r^* = n$;

(4) 设 G^* 的顶点 v_i^* 位于 G 的面 R_i 中，则 $d_{G^*}(v_i^*) = \deg(R_i)$.

定理 11.16 设 G^* 是具有 $p(p \geq 2)$ 个连通分支的的对偶图，则

(1) $n^* = r$;　(2) $m^* = m$;　(3) $r^* = n - p + 1$;

(4) 设 v_i^* 位于 G 的面 R_i 中，则 $d_{G^*}(v_i^*) = \deg(R_i)$.

其中 n^*, m^*, r^*, n, m, r 同定理 11.15.

定理 11.17 设 G^* 是某平面图 G 的对偶图，在 G^* 的图形不改变的条件下，$G^{**} \cong G$ 当且仅当 G 是连通图.

定理 11.18 $n(n \geq 4)$ 阶轮图 W_n 是自对偶图.

定理 11.19 所有顶点都在外部面边界上的 $n(n \geq 3)$ 阶外可平面图是极大外可平面图当且仅当 G 的每个内部面的边界都是长为 3 的圈，外部面的边界是一个长为 n 的圈.

推论 对于 n 阶外平面图，总可以用添加新边的方法得到极大外平面图.

定理 11.20 设 G 是所有顶点均在外部面边界上的 $n(n \geq 3)$ 阶极大外平面图，则 G 有 $n-2$ 个内部面.

定理 11.21 设 G 是 $n(n \geq 3)$ 阶极大外平面图，则

(1) $m = 2n - 3$，其中 m 为 G 中边数;

(2) G 中至少有 3 个顶点的度数小于等于 3;

(3) G 中至少有 2 个顶点的度数为 2;

(4) G 的点连通度 $\kappa = 2$.

定理 11.22 一个图 G 是外平面图当且仅当 G 中不含与 K_4 或 $K_{2,3}$ 同胚的子图.

定理 11.23 设 G 是 n 阶简单平面图且是哈密顿图，C 为 G 中一条哈密顿回路. 以 r_i', r_i'' 分别表示在 C 的内部和在 C 的外部的次数为 i 的面数，则

$$\sum_{i=3}^{n}(i-2)(r_i' - r_i'') = 0.$$

定理 11.24 任何 4-连通平面图都是哈密顿图.

第十二章　图的着色

定理 12.1 $\chi(G)=1$ 当且仅当 G 为零图.

定理 12.2 $\chi(K_n)=n$.

定理 12.3 奇圈和奇数阶轮图都是 3-色图，而偶数阶轮图为 4-色图.

定理 12.4 图 G 是 2-可着色的当且仅当 G 为二部图.

推论 1 $\chi(G)=2$ 当且仅当 G 为非零图的二部图.

推论 2 图 G 是 2-可着色的当且仅当 G 中不含奇圈.

定理 12.5 对于任意的图 G，均有

$$\chi(x)\leq\Delta(G)+1.$$

定理 12.6 (Brooks) 设连通图不是完全图 $K_n(n\geq 3)$ 也不是奇圈，则

$$\chi(G)\leq\Delta(G).$$

定理 12.7 对图 G 进行 $\chi(G)$-着色，设

$$V_i=\{v\mid v\in V(G)\text{ 且 }v\text{ 涂颜色 }i\,\},i=1,2,\cdots,\chi(G),$$

则 $\Pi=\{V_1,V_2,\cdots,V_{\chi(G)}\}$ 是 $V(G)$ 的一个划分.

定理 12.7’ 对图 G 进行 $\chi(G)$-着色，设

$$R=\{\langle u,v\rangle\mid u,v\in V(G)\text{ 且 }u,v\text{ 涂一样颜色 }\},$$

则 R 是 $V(G)$ 上的等价关系.

定理 12.8 $f(K_n,k)=k(k-1)\cdots(k-n+1),f(N_n,k)=k^n$，其中 K_n,N_n 分别为 n 阶完全图和 n 阶零图.

推论 $f(K_n,k)=f(K_{n-1},k)(k-n+1),n\geq 2$.

定理 12.9 在无环无向图 G 中，$V(G)=\{v_1,v_2,\cdots,v_n\}$.

(1)　$e=(v_i,v_j)\notin E(G)$，则

$$(G,k)=f(G\cup(v_i,v_j),k)+f(G\backslash(v_i,v_j),k).$$

(2)　$e=(v_i,v_j)\in E(G)$，则

$$(G,k)=f(G-e,k)-f(G\backslash e,k).$$

其中，$G\backslash(v_i,v_j)$ 在这里表示将 v_i,v_j 合并成一个顶点 w_{ij}，使它关联 v_i,v_j 关联的一切边.

推论 $f(G,k)=f(K_{n_1},k)+f(K_{n_2},k)+\cdots+f(K_{n_r},k)$. 且$\chi(G)=\min\{n_1,n_2,\cdots,n_r\}$.

定理 12.10 设 V_1 是 G 的点割集，且 $G[V_1]$ 是 G 的 $|V_1|$ 阶完全子图，$G-V_1$ 有 $p(p\geq 2)$ 个连通分支 $G_1,G_2,\cdots,G_p$，则

$$f(G,k)=\frac{\prod\limits_{i=1}^{p}(f(H_i,k))}{f(G[V_1],k)^{p-1}}.$$

其中，$H_i = G[V_1 \cup V(G_i)], i = 1, 2, \cdots, p$.

定理 12.11 T 是 n 阶树当且仅当 $f(T, k) = k(k-1)^{n-1}$.

定理 12.12 若 G 是 n 阶圈，则

$$f(G, k) = (k-1)^n + (-1)^n(k-1).$$

定理 12.13 地图 G 是 k-面可着色的当且仅当它的对偶图 G^* 是 k-可着色的.

定理 12.14 设 G 是连通的无环的平面图，G^* 是 G 的对偶图，则 G 是 k-可着色的当且仅当 G^* 是 k-面可着色的.

定理 12.15 任何平面图都是 6-可着色的

定理 12.16 (Heawood) 任何平面图都是 5-可着色的.

定理 12.17 (Vizing) 设 G 是简单图，则 $\Delta(G) \leq \chi'(G) \leq \Delta(G) + 1$.

第十三章　支配集、覆盖集、独立集与匹配

定理 13.1 设无向图 G 中无孤立顶点，V_1^* 为 G 的一个极小支配集，则 G 中存在另一个极小支配集 V_2^*，使得 $V_1^* \cap V_2^* = \varnothing$.

定理 13.2 设无向图 G 中无孤立顶点，V^* 为 G 中极大独立集，则 V^* 是 G 中极小支配集.

定理 13.3 设无向图 $G = \langle V, E\rangle$ 中无孤立顶点，$V^* \subset V$，则 V^* 为 G 的点覆盖集当且仅当 $\overline{V}^* = V - V^*$ 为 G 的点独立集.

推论 设 G 是 n 阶无孤立点的无向图. V^* 是 G 的极小(最小)点覆盖集当且仅当 $\overline{V}^* = V(G) - V^*$ 为 G 的极大(最大)点独立集. 从而有

$$\alpha_0 + \beta_0 = n.$$

定理 13.4 设 G 是 n 阶无向图，V^* 为 G 中团当且仅当 V^* 为 $\overline{G}$ 中的独立集.

推论 设 G 是 n 阶无向图，V^* 为 G 中极大(最大)团当且仅当 V^* 为 $\overline{G}$ 中的极大(最大)独立集，从而 $\nu_0(G) = \beta_0(\overline{G})$.

定理 13.5 设 G 为无孤立点的 n 阶无向图.

(1) 设 M 为 G 中一个最大匹配，对于每个 M 非饱和点 v，取一条关联 v 的边组成边集 N，则 $W = M \cup N$ 为 G 中一个最小边覆盖集.

(2) 设 W_1 为 G 中一个最小边覆盖集，若 W_1 中存在相邻的边就移去其中的一条边，继续这一过程，直到无相邻的边为止，设移去的边组成的集合为 N_1，则 $M_1 = W_1 - N_1$ 为 G 中一个最大匹配.

(3) $\alpha_1 + \beta_1 = n$.

推论 设 G 为 n 阶无孤立点的无向图，M 为 G 中一个匹配，W 为 G 中一个边覆盖，则

$$|M| \le |W|.$$

等号成立时，M 为 G 中完美匹配且 W 为 G 中的最小边覆盖.

定理 13.6 设 G 为无孤立点的 n 阶无向图，M 为 G 中一个匹配，N 为 G 中一个点覆盖，Y 为 G 中一个点独立集，W 为 G 中一个边覆盖，则

(1) $|M| \le |N|$,

(2) $|Y| \le |W|$,

等号成立时，M, N, Y, W 分别为 G 中最大匹配、最小点覆盖集，最大点独立集、最小边独立集.

推论 设 G 为无孤立顶点的 n 阶无向图，则

$$\beta_1 \le \alpha_0, \quad \beta_0 \le \alpha_1.$$

定理 13.7 设 M_1, M_2 为 G 中两个不同的匹配，则 $G[M_1 \oplus M_2]$ 的每个连通分支或为由 M_1, M_2 中的边组成的交错圈，或为交错路径.

定理 13.8 设 M 为图 G 中的一个匹配，Γ 为 G 中关于 M 的可增广路径，则 $M' = M \oplus E(\Gamma)$ 仍为匹配，且 $|M'| = |M| + 1$.

定理 13.9 M 为 G 中最大匹配当且仅当 G 中不含 M 可增广路径.

定理 13.10 n 阶无向图 G 具有完美匹配当且仅当对于任意的 $V' \subset V(G)$,

$$p_{奇}(G - V') \le |V'|,$$

其中 $p_{奇}(G - V')$ 表示 $G - V'$ 中奇数阶连通分支数.

推论 任何无桥 3-正则图都有完美匹配.

定理 13.11 (Hall 定理) 设二部图 $G = \langle V_1, V_2, E\rangle$，$|V_1| \le |V_2|$. G 中存在 V_1 到 V_2 的完备匹配当且仅当对于任意 $S \subseteq V_1$，均有 $|S| \le |N(S)|$，其中 $N(S)$ 为 S 的邻域，即

$$N(S) = \bigcup_{v_i \in S} N(v_i).$$

定理 13.12 设 $G = \langle V_1, V_2, E\rangle$ 为二部图，若 V_1 中每个顶点至少关联 $t(t \ge 1)$ 条边，而 V_2 中每个顶点至多关联 t 条边，则 G 中存在 V_1 到 V_2 的完备匹配.

定理 13.13 设 $G = \langle V_1, V_2, E\rangle$ 为 k-正则二部图，则 G 中存在 k 个边不重的完美区配.

推论 $K_{k,k}$ 中存在 k 个边不重的完美匹配.

定理 13.14 设 $G = \langle V_1, V_2, E\rangle$ 为无孤立点的二部图，则 $\alpha_0 = \beta_1$.

第十四章　带权图及其应用

定理 14.1 设 $P_E = \{v \mid TE(v) \text{ 已算出 }\}$，$T_E = V - P_E$，若 $T_E \neq \varnothing$，则存在 $u \in T_E$，使得

$$\Gamma^-(u) \subseteq P_E.$$

定理 14.2 设 $P_L = \{v \mid TL(v)) \text{ 已算出 }\}$，$T_L = V - P_L$，若 $T_L \neq \varnothing$，则存在 $u \in T_L$，使得

$$\Gamma^+(u) \subseteq P_L.$$

定理 14.3 $TS(v_i) = 0$ 当且仅当 v_i 处在关键路径上.

定理 14.4 C 是带正权无向连通图 $G = \langle V, E, W \rangle$ 中的最优投递路线当且仅当对应的欧拉图 G^* 满足:

(1) G 的每条边在 G^* 中至多重复出现一次;

(2) G 的每个圈上 G^* 中重复出现的边的权之和不超过该圈权的一半.

定理 14.5 设带正权无向连通图 $G = \langle V, E, W \rangle$，$V'$ 为 G 中奇度顶点集，设 $|V'| = 2k(k \geq 0)$，$F = \{e \mid e \in E \wedge \text{ 在求 } G \text{ 的最优回路时加了重复边 }\}$，则 F 的导出子图 $G[F]$ 可以表示为以 V' 中顶点为起点与终点的 k 条不交的最短路径之并.

定理 14.6 设 T 是无向连通带权图 $G = \langle V, E, W \rangle$ 中的一棵生成树，则下面命题等价:

(1) T 是 G 中的最小生成树;

(2) 任意的 $e \in E(T)$，设 e 对应的基本割集为 S_e，都有 e 是 S_e 中带权最小的边;

(3) 任意的 $e \in E(\overline{T})$ ($\overline{T}$ 为 T 的余树)，设 C_e 是 e 对应的基本的回路，都有 e 是 C_e 中带权最大的边.

定理 14.7 设 $G = \langle V, E, W \rangle$ 是无向连通带权图，C 为 G 中任意一个圈，e' 是 C 中带权最大的边，则 $G - e'$ 中的最小生成树也是 G 中的最小生成树.

定理 14.8 设 $G = \langle V, E, W \rangle$ 为一个无向连通带权图. $S = (V_1, \overline{V}_1)$ 为 G 中一个断集，$e' \in S$ 且 $W(e') = \min\limits_{e \in S}\{W(e)\}$，设 T' 是以 e' 为树枝的所有生成树中带权最小的，则 T' 是 G 的最小生成树.

定理 14.9 设 $G = \langle V, E, W \rangle$ 为一个无向连通带权图，e 是 G 非环且是带权最小的边. 则 G 中一定存在含 e 作为树枝的最小生成树 T^*.

定理 14.10 设 $G = \langle V, E, W \rangle$ 为一个无向连通带权图，e 是 G 中非环的带权最小的边，设 G' 是 G 中短接 e 的两个端后所得的图，T' 是 G' 中的最小生成树，在 G 中设 $T^* = G[E(T') \cup \{e\}]$，则 T^* 是 G 中的最小生成树.

定理 14.11 在带权为 $w_1 \leq w_2 \leq \cdots \leq w_t$ 的所有最优树中，一定存在以权为 w_1, w_2 的两顶点 v_1, v_2 为兄弟，且 v_1, v_2 的层数都是树高 h 的最优树.

定理 14.12 (Huffman 定理) 设 T' 带权为 $w_1 + w_2, w_3, \cdots, w_t$ 的最优二叉树，其中 $w_1 \leq w_2 \leq \cdots \leq w_t$，如果将 T' 中带权为 $w_1 + w_2$ 的树叶作为分支点，使它带两个儿子，带权分别为 w_1 和

w_2，记所得树为 T^*，则 T^* 是带权为 $w_1, w_2, \cdots, w_t$ 的最优树.

定理 14.13 设 $r(r \geq 2)$ 叉正则树 T 分支点数为 i，树叶数为 t，则 $(r-1)i = t-1$.

定理 14.14 一棵二叉树可以产生一个前缀码.

推论 一棵二叉正则树可以产生唯一的一个前缀码.

定理 14.15 设 $G = \langle V, E, W \rangle$ 是 n 阶完全带权图，各边带的权均为正，并且对于任意的 $v_i, v_j, v_k \in V$，边 $(v_i, v_j), (v_j, v_k,), (v_i, v_k)$ 带的权 w_{ij}, w_{jk}, w_{ik} 满足三角不等式，即

$$w_{ij} + w_{jk} \geq w_{ik},$$

则

$$\frac{d}{d_0} \leq \frac{1}{2}(\lceil \log_2 n \rceil + 1),$$

其中，d_0 是 G 中最短哈密顿回路的权，而 d 是用最邻近法走出的哈密顿回路的权.

定理 14.16 设 $G = \langle V, E, W \rangle$ 为 $n(n \geq 3)$ 阶无向完全带权图，各边的权均大于 0，对任意的 $v_i, v_j, v_k \in V$，边 $(v_i, v_j), (v_j, v_k), (v_i, v_k)$ 的权满足三角不等式：$w_{ij} + w_{jk} \geq w_{ik}$，$d_0$ 是 G 中最短哈密顿回路的权，H 是用最小生成树法走出的 G 的哈密顿回路，其权为 d，则

$$\frac{d}{d_0} < 2.$$

定理 14.17 定理的条件同定理 14.16，则

$$\frac{d}{d_0} < \frac{3}{2}.$$

其中 d_0 是 G 中最短哈密顿回路的权，d 是用最小权匹配法得到的哈密顿回路的权.

第十五章　代数系统

定理 15.1 设 $\circ$ 为 A 上的二元运算，若 $\circ$ 运算适合结合律，则 $\circ$ 运算适合广义结合律.

定理 15.2 设 $\circ$ 为 A 上的二元运算，若存在 $e_l \in A$ 和 $e_r \in A$ 满足 $\forall x \in A$ 有 $e_l \circ x = x$ 和 $x \circ e_r = x$，则 $e_l = e_r = e$，且 e 就是 A 中关于 $\circ$ 运算的惟一的单位元.

定理 15.3 设 $\circ$ 为 A 上的二元运算，若存在 $\theta_l \in A$ 和 $\theta_r \in A$ 使得 $\forall x \in A$ 有 $\theta_l \circ x = \theta_l$ 和 $x \circ \theta_r = \theta_r$，则 $\theta_l = \theta_r = \theta$，且 θ 是 A 中关于 $\circ$ 运算的惟一的零元.

定理 15.4 设集合 A 至少含有两个元素，e 和 θ 分别为 A 中关于 $\circ$ 运算的单位元和零元，则 $e \neq \theta$.

定理 15.5 设 $\circ$ 为 A 上可结合的二元运算且单位元为 e. 对于 $x \in A$ 若存在 $y_l, y_r \in A$，使得 $y_l \circ x = e$ 和 $x \circ y_r = e$，则 $y_l = y_r = y$，且 y 是 x 关于 $\circ$ 运算的惟一的逆元.

定理 15.6 设代数系统 $V_1 = \langle A, \circ_{11}, \circ_{12}, \cdots, \circ_{1r} \rangle, V_2 = \langle B, \circ_{21}, \circ_{22}, \cdots, \circ_{2r} \rangle$ 是同类型的，V 是 V_1 与 V_2 的积代数. 对任意的二元运算 $\circ_{1i}, \circ_{1j}, \circ_{2i}, \circ_{2j}$，
(1) 若 $\circ_{1i}, \circ_{2i}$ 在 V_1 和 V_2 中是可交换的(或可结合的，幂等的)，则 $\circ_i$ 在 V 中也是可交换的(或可结合的，幂等的).
(2) 若 $\circ_{1i}$ 对 $\circ_{1j}$ 在 V_1 上是可分配的，$\circ_{2i}$ 对 $\circ_{2j}$ 在 V_2 上是可分配的，则 $\circ_i$ 对 $\circ_j$ 在 V 上也是可分配的.
(3) 若 $\circ_{1i}, \circ_{1j}$ 在 V_1 上是可吸收的，且 $\circ_{2i}, \circ_{2j}$ 在 V_2 上也是可吸收的，则 $\circ_i, \circ_j$ 在 V 上是可吸收的.
(4) 若 e_1 (或 θ_1)为 V_1 中关于 $\circ_{1i}$ 运算的单位元(或零元)，e_2 (或 θ_2)为 V_2 中关于 $\circ_{12}$ 运算的单位元(或零元)，则 $\langle e_1, e_2 \rangle$ (或 $\langle \theta_1, \theta_2 \rangle$)为 V 中关于 $\circ_i$ 运算的单位元(或零元).
(5) 若 $\circ_{1i}, \circ_{2i}$ 为含有单位元的二元运算，且 $a \in A, b \in B$ 关于 $\circ_{1i}$ 和 $\circ_{2i}$ 运算的逆元分别为 a^{-1}, b^{-1}，则 $\langle a^{-1}, b^{-1} \rangle$ 是 $\langle a, b \rangle$ 在 V 中关于 $\circ_i$ 运算的逆元.

定理 15.7 设 $V_1 = \langle A, \circ_1, \circ_2, \cdots, \circ_r \rangle, V_2 = \langle B, \bar{\circ}_1, \bar{\circ}_2, \cdots, \bar{\circ}_r \rangle$ 是同类型的代数系统，对于 $i = 1, 2, \cdots, r$，$\circ_i, \bar{\circ}_i$ 是 k_i 元运算. $\varphi : A \to B$ 是 V_1 到 V_2 的同态，则 $\varphi(A)$ 关于 V_2 中的运算构成代数系统，且是 V_2 的子代数，称为 V_1 在 φ 下的**同态像**.

定理 15.8 设 $V_1 = \langle A, \circ_1, \circ_2, \cdots, \circ_r \rangle, V_2 = \langle B, \bar{\circ}_1, \bar{\circ}_2, \cdots, \bar{\circ}_r \rangle$ 是同类型的代数系统，$\varphi : A \to B$ 是 V_1 到 V_2 的满同态，$\circ_i, \circ_j$ 是 V_1 中的两个二元运算.
(1) 若 $\circ_i$ 是可交换的(或可结合的，幂等的)，则 $\bar{\circ}_i$ 也是可交换的(或可结合的，幂等的).
(2) 若 $\circ_i$ 对 $\circ_j$ 是可分配的，则 $\bar{\circ}_i$ 对 $\bar{\circ}_j$ 也是可分配的.
(3) 若 $\circ_i, \circ_j$ 是可吸收的，则 $\bar{\circ}_i, \bar{\circ}_j$ 也是可吸收的.
(4) 若 e (或 θ)是 V_1 中关于 $\circ_i$ 运算的单位元(或零元)，则 $\varphi(e)$ (或 $\varphi(\theta)$)是 V_2 中关于 $\bar{\circ}_i$ 运算的单位元(或零元).

(5) 若 $\circ_i$ 是含有单位元的运算，$x^{-1} \in A$ 是 x 关于 $\circ_i$ 的逆元，则 $\varphi(x^{-1})$ 是 $\varphi(x)$ 关于 $\bar{\circ}_i$ 运算的逆元.

定理 15.9 设 $V = \langle A, \circ_1, \circ_2, \cdots, \circ_r \rangle$ 是代数系统，对于 $i = 1, 2, \cdots, r$，$\circ_i$ 是 k_i 元运算. $\sim$ 是 V 上的同余关系，V 关于 $\sim$ 的商代数 $V/\!\sim\, = \langle A/\!\sim, \bar{\circ}_1, \bar{\circ}_2, \cdots, \bar{\circ}_r \rangle$. 令 $\circ_i, \circ_j$ 是 V 中的两个二元运算.

(1) 若 $\circ_i$ 是可交换的(或可结合的，幂等的)，则 $\bar{\circ}_i$ 在 $V/\!\sim$ 中也是可交换的(或可结合的，幂等的).

(2) 若 $\circ_i$ 对 $\circ_j$ 是可分配的，则 $\bar{\circ}_i$ 对 $\bar{\circ}_j$ 在 $V/\!\sim$ 中也是可分配的.

(3) 若 $\circ_i, \circ_j$ 满足吸收律，则 $\bar{\circ}_i, \bar{\circ}_j$ 在 $V/\!\sim$ 中也满足吸收律.

(4) 若 e (或 θ)是 V 中关于 $\circ_i$ 运算的单位元(或零元)，则 $[e]$ (或 $[\theta]$)是 $V/\!\sim$ 中关于 $\bar{\circ}_i$ 运算的单位元(或零元).

(5) 若 $\circ_i$ 为 V 中含有单位元的运算，且 $x \in A$ 关于 $\circ_i$ 的逆元为 x^{-1}，则在 $V/\!\sim$ 中 $[x]$ 关于 $\bar{\circ}_i$ 运算的逆元是 $[x^{-1}]$.

定理 15.10 设 $V_1 = \langle A, \circ_1, \circ_2, \cdots, \circ_r \rangle, V_2 = \langle B, \bar{\circ}_1, \bar{\circ}_2, \cdots, \bar{\circ}_r \rangle$ 是同类型的代数系统，对于 $i = 1, 2, \cdots, r$，$\circ_i, \bar{\circ}_i$ 是 k_i 元运算. 令 $\varphi : A \to B$ 是 V_1 到 V_2 的同态，则由 φ 导出的 A 上的等价关系 $\sim$ 是 V_1 上的同余关系.

定理 15.11 设 $V = \langle A, \circ_1, \circ_2, \cdots, \circ_r \rangle$ 是代数系统，其中 $\circ_i$ 为 k_i 元运算，$i = 1, 2, \cdots, r$. $\sim$ 为 V 上的同余关系，则**自然映射** $g : A \to A/\!\sim, g(a) = [a], \forall a \in A$ 是从 V 到 $V/\!\sim$ 上的同态映射.

定理 15.12 (同态基本定理) 设 $V_1 = \langle A, \circ_1, \circ_2, \cdots, \circ_r \rangle, V_2 = \langle B, \circ'_1, \circ'_2, \cdots, \circ'_r \rangle$ 是同类型的代数系统，对于 $i = 1, 2, \cdots, r$，$\circ_i, \circ'_i$ 是 k_i 元运算. $\varphi : A \to B$ 是 V_1 到 V_2 的同态，关系 $\sim$ 是 φ 导出的 V_1 上的同余关系，则 V_1 关于同余关系 $\sim$ 的商代数同构于 V_1 在 φ 下的同态像，即 $V_1/\!\sim\, \cong \langle \varphi(A), \circ'_1, \circ'_2, \cdots, \circ'_r \rangle$.

第十六章　半群与独异点

定理 16.1 设 $V = \langle S, \circ \rangle$ 是半群，则 $\forall x, y \in S$ 有

(1) $x^n \circ x^m = x^{n+m}$;

(2) $(x^n)^m = x^{nm}$.

定理 16.2 设 $\langle S, \circ \rangle$ 是半群，则可以适当地定义单位元 e，将这个半群扩张为独异点.

定理 16.3 设 S 为半群，V 为独异点，则 S 的任何子半群的非空交集仍是 S 的子半群，V 的任何子独异点的交集仍是 V 的子独异点.

定理 16.4 S 为半群，B 是 S 的非空子集. $\forall n \in \mathbb{Z}^+$，令

$$B^n = \{b_1 b_2 \cdots b_n \mid b_i \in B, i = 1, 2, \cdots, n\},$$

则

$$\langle B \rangle = \bigcup_{n \in \mathbb{Z}^+} B^n.$$

定理 16.5 设 $V = \langle S, * \rangle$ 为半群，$V' = \{S^S, \circ\}$，$\circ$ 为函数的合成运算，则 V' 是半群，且存在 V 到 V' 的同态.

定理 16.6 (独异点的表示定理) 设 $V = \langle S, *, e \rangle$ 是独异点，则存在 $T \subseteq S^S$，使 $\langle T, \circ, I_S \rangle$ 同构于 $\langle S, *, e \rangle$.

定理 16.7 设 $M^* = \langle Q, \Sigma^*, \Gamma^*, \delta^*, \lambda^* \rangle$ 是扩展的有穷自动机，则 $\forall w_1, w_2 \in \Sigma^*$ 有

(1) $\delta^*(q, w_1 w_2) = \delta^*(\delta^*(q, w_1), w_2)$,

(2) $\lambda^*(q, w_1 w_2) = \lambda^*(q, w_1)\lambda^*(\delta^*(q, w_1), w_2)$,

其中 $w_1 w_2$ 是 w_1 与 w_2 的连接.

定理 16.8 设 $M = \langle Q, \Sigma, \delta \rangle$ 是半自动机，$M^* = \langle Q, \Sigma^*, \delta^* \rangle$ 是 M 的扩展. 对任意的 $w \in \Sigma^*$，定义 $f_w : Q \to Q$，$f_w(q) = \delta^*(q, w)$. 令 $S = \{f_w \mid w \in \Sigma^*\}$ 是所有这样定义的函数的集合，$\circ$ 是函数的合成运算，则 $T_M = \langle S, \circ, f_\wedge \rangle$ 是一个独异点，且是 $\langle Q^Q, \circ, I_Q \rangle$ 的子独异点.

定理 16.9 设 $T = \langle S, \cdot, e \rangle$ 是独异点，则存在半自动机 M，且 M 对应的独异点 T_M 同构于 T.

定理 16.10 设 $M_1 = \langle Q_1, \Sigma_1, \Gamma_1, \delta_1, \lambda_1 \rangle$，$M_2 = \langle Q_2, \Sigma_2, \Gamma_2, \delta_2, \lambda_2 \rangle$ 是自动机. 它们分别对应独异点 T_{M_1} 和 T_{M_2}. 若 $M_1 \leq M_2$，则 T_{M_1} 是 T_{M_2} 的同态像.

定理 16.11 设 $M_1 = \langle Q_1, \Sigma, \Gamma, \delta_1, \lambda_1 \rangle$ 是有穷自动机，$M_2 = \langle Q_1/{\sim}, \Sigma, \Gamma, \delta_2, \lambda_2 \rangle$ 是 M_1 的商自动机，则 $M_1 \sim M_2$.

第十七章　群

定理 17.1 设 $\langle G, \circ\rangle$ 是具有一个可结合二元运算的代数系统，若存在 $e \in G$，使得 $\forall a \in G$，有 $a \circ e = a$，且 $\forall a \in G$，存在 $a' \in G$ 满足 $a \circ a' = e$，则 G 是一个群。

定理 17.2 G 为群，$\forall a, b \in G$ 有

(1) $(a^{-1})^{-1} = a$;

(2) $(ab)^{-1} = b^{-1}a^{-1}$;

(3) $a^n a^m = a^{n+m}, \quad m, n \in \mathbb{Z}$;

(4) $(a^n)^m = a^{mn}, \quad m, n \in \mathbb{Z}$;

(5) 若 G 为 Abel 群，$(ab)^n = a^n b^n, \quad n \in \mathbb{Z}$.

定理 17.3 G 为群，$\forall a, b \in G$，方程 $ax = b$ 和 $ya = b$ 在 G 中有解且有惟一解.

定理 17.4 设 G 是具有一个可结合的二元运算的代数系统，如果 $\forall a, b \in G$ 方程 $ax = b$ 和 $ya = b$ 在 G 中有解，则 G 是群.

定理 17.5 群中运算满足消去律.

定理 17.6 设 G 是具有一个二元运算的不含零元的有限代数系统，且该运算适合结合律和消去律，则 G 是一个群.

定理 17.7 设 $G = \{a_1, a_2, \cdots, a_n\}$ 为群，则 G 的运算表的每行每列都是 G 中元素的一个置换.

定理 17.8 G 是群，$a \in G$ 且 $|a| = r$，则

(1) $a^k = e$ 当且仅当 $r \mid k$，$k \in \mathbb{Z}$;

(2) $|a| = |a^{-1}|$;

(3) 若 $|G| = n$ 则 $r \leq n$.

定理 17.9 (子群判定定理一) G 是群，H 是 G 的非空子集，则 H 是 G 的子群当且仅当

(1) $\forall a, b \in H$ 有 $ab \in H$，　(2) $\forall a \in H$ 有 $a^{-1} \in H$.

定理 17.10 (子群判定定理二) G 是群，H 是 G 的非空子集，则 H 是 G 的子群当且仅当 $\forall a, b \in H$ 有

$$ab^{-1} \in H.$$

定理 17.11 (子群判定定理三) G 是群，H 是 G 的有穷非空子集，则 H 是 G 的子群当且仅当 $\forall a, b \in H$ 有

$$ab \in H.$$

定理 17.12 $G = \langle a\rangle$ 是循环群.

(1) 若 G 是无限阶循环群，则 G 的生成元是 a 和 a^{-1}.

(2) 若 G 是 n 阶循环群，则 G 有 $\phi(n)$ 个生成元. 当 $n=1$ 时，$G=\langle e\rangle$ 的生成元是 e，当 $n>1$ 时，对每一个不大于等于 n 的正整数 r，a^r 是 G 的生成元当且仅当 $(n,r)=1$.

定理 17.13 $G=\langle a\rangle$ 是循环群，那么

(1) G 的子群也是循环群;

(2) 若 G 是无限阶的，则 G 的子群除 $\{e\}$ 以外仍是无限阶的;

(3) 若 G 是 n 阶的，则 G 的子群的阶是 n 的因子，对于 n 的每个正因子 d，在 G 中有且仅有一个 d 阶子群.

定理 17.14 设 $E(A)$ 是 A 上的全体一一变换构成的集合，则 $E(A)$ 关于变换的乘法构成一个群.

定理 17.15 设 $\sigma,\tau\in S_n$，若 σ 与 τ 是不相交的，则 $\sigma\tau=\tau\sigma$.

定理 17.16 任何 n 元置换都可以表成不相交的轮换之积，并且表法是惟一的.

定理 17.17 设 $\sigma=(i_1i_2\cdots i_k)$ 是 $A=\{1,2,\cdots,n\}$ 上的 k 阶轮换，$k>1$，则

$$\sigma=(i_1i_k)(i_1i_{k-1})\cdots(i_1i_2).$$

定理 17.18 $\sigma\in S_n$ 且 $\sigma(j)=i_j$，$j=1,2,\cdots,n$，则在 σ 的对换表示中对换个数的奇偶性与排列 $\pi=i_1i_2\cdots i_n$ 中的逆序数的奇偶性一致.

定理 17.19 G 是 n 元置换群.

(1) $\sigma\in G$，$\sigma=(i_1i_2\cdots i_k)$，则 $|\sigma|=k$.

(2) $\tau\in G$，$\tau=\tau_1\tau_2\cdots\tau_l$ 是不相交轮换的分解式，若 τ_i 是 k_i 阶轮换，$i=1,2,\cdots,l$，则 τ 的阶是 $k_1,k_2,\cdots,k_l$ 的最小公倍数，即 $|\tau|=[k_1,k_2,\cdots,k_l]$.

定理 17.20 设 G 是群，H 是 G 的子群，则

(1) $He=H$; (2) $\forall a\in G,a\in Ha$.

定理 17.21 设 G 是群，H 是 G 的子群，则 $\forall a\in G,Ha\approx H$.

定理 17.22 G 是群，H 是 G 的子群，$\forall a,b\in G$ 有

$$a\in Hb\Leftrightarrow Ha=Hb\Leftrightarrow ab^{-1}\in H.$$

定理 17.23 G 是群，H 是 G 的子群，在 G 上定义二元关系 R，$\forall a,b\in G$ 有

$$aRb\Leftrightarrow ab^{-1}\in H,$$

则R为 G 上的等价关系，则 $[a]_R=Ha$.

定理 17.24 G 是群，H 是 G 的子群，则

$$\forall a,b\in G,Ha\cap Hb=\varnothing \text{ 或 } Ha=Hb\text{，且 }\bigcup_{a\in G}Ha=G.$$

定理 17.25 设 G 是群，H 是 G 的子群，则

(1) $eH=H$;

(2) $\forall a\in G,a\in aH$;

(3) $\forall a\in G,aH\approx H$;

(4) $\forall a,b\in G,a\in bH\Leftrightarrow aH=bH\Leftrightarrow a^{-1}b\in H$;

(5) 在 G 上定义二元关系 R，$\forall a,b\in G$，$aRb\Leftrightarrow a^{-1}b\in H$，则 R 为 G 上的等价关系，且 $[a]_R=aH$;

(6) $\forall a,b\in G,aH\cap bH=\varnothing$ 或 $aH=bH$，且 $\bigcup_{a\in G}aH=G$.

定理 17.26 (Lagrange 定理) 设 G 是有限群，H 是 G 的子群，则

$$|G|=[G:H]|H|.$$

推论 1 G 是 n 阶群，则 G 中每个元素的阶是 n 的因子，且 $\forall a\in G$ 有 $a^n=e$.

推论 2 阶为素数的群是循环群.

定理 17.27 群 G 上的共轭关系是 G 上的等价关系.

定理 17.28 G 是群，C 是 G 的中心，则 $\forall a \in G$ 有

$$a \in C \Leftrightarrow \bar{a} = \{a\}.$$

定理 17.29 G 是群，则 $\forall a \in G$，$N(a)$ 是 G 的子群.

定理 17.30 G 是有限群，则 $\forall a \in G$ 有

$$|\bar{a}| = [G : N(a)].$$

定理 17.31 (群的分类方程) G 是有限群，C 是 G 的中心. 设 G 中至少含有两个元素的共轭类有 k 个，且 $a_1, a_2, \cdots, a_k$ 分别为这 k 个共轭类的代表元素，则

$$|G| = |C| + [G : N(a_1)] + [G : N(a_2)] + \cdots + [G : N(a_k)].$$

定理 17.32 N 是群 G 的子群，则下列条件互相等价.

(1) $N \trianglelefteq G$;

(2) $\forall g \in G$ 有 $gNg^{-1} = N$;

(3) $\forall g \in G$，$\forall n \in N$ 有 $gng^{-1} \in N$.

定理 17.33 设 φ 是群 G_1 到 G_2 的同态，则 φ 为单同态当且仅当

$$\ker \varphi = \{e_1\}.$$

定理 17.34 $G_1 = \langle a \rangle$ 是循环群，φ 是 G_1 到 G_2 的满同态，则 G_2 也是循环群.

定理 17.35 设 φ 是群 G_1 到 G_2 的同态.

(1) 若 H 是 G_1 的子群，则 $\varphi(H)$ 是 G_2 的子群.

(2) 若 H 是 G_1 的正规子群，且 φ 是满同态，则 $\varphi(H)$ 是 G_2 的正规子群.

定理 17.36 设 φ 是群 G_1 到 G_2 的同态，则

(1) $\ker \varphi$ 是 G_1 的正规子群; (2) $\forall a, b \in G_1, \varphi(a) = \varphi(b) \Leftrightarrow a \ker \varphi = b \ker \varphi$.

定理 17.37 (群同态基本定理) 设 G 是群，H 是 G 的正规子群，则 G 的商群 G/H 是 G 的同态像. 若 G' 是 G 的同态像，$G \overset{\varphi}{\sim} G'$，则

$$G/\ker \varphi \cong G'.$$

定理 17.38 G 是群，则 $\mathrm{End}\, G$ 关于映射的合成运算构成一个独异点，$\mathrm{Aut}\, G$ 关于映身的合成运算构成一个群.

定理 17.39 G 是群，则 $\mathrm{Inn}\, G \trianglelefteq \mathrm{Aut}\, G$.

定理 17.40 设 G 是群，K 和 L 是 G 的子群，则 $G = K \times L$ 当且仅当下面的条件成立:

(1) $K \trianglelefteq G, L \trianglelefteq G$; (2) $K \cap L = \{e\}$; (3) $G = KL$.

定理 17.41 设 G 是群，$G_1, G_2, \cdots, G_n$ 是 G 的子群，则 $G = G_1 \times G_2 \times \cdots \times G_n$ 当且仅当以下条件成立:

(1) $G_i \trianglelefteq G, i = 1, 2, \cdots, n$;

(2) $G_i \cap G_1 G_2 \cdots G_{i-1} G_{i+1} \cdots G_n = \{e\}, i = 1, 2, \cdots, n$;

(3) $G = G_1 G_2 \cdots G_n$.

定理 17.42 用 r-电路计算一个 m 元函数至少需要 $\lceil \log_r m \rceil$ 个时间单位.

定理 17.43 设 $\langle \mathbb{Z}_n, \otimes \rangle$ 是群，若存在 $a \in \mathbb{Z}_n$，$a \neq 0$，且 a 属于 $\mathbb{Z}_n$ 的每一个非平凡的子群，则对于任意的模 n 加法器 T，总存在着某个输入，使得 T 至少依赖于输入的 $2 \lceil \log_2 n \rceil$ 位.

推论 1 若 $\mathbb{Z}_n$ 中含有一个无所不在的元素，则用 r-电路计算 $\mathbb{Z}_n$ 中的加法至少需要 $\lceil \log_r(2\lceil \log_2 n\rceil)\rceil$ 个时间单位.

推论 2 若 $\mathbb{Z}_n$ 中不存在无所不在的元素，H 是 $\mathbb{Z}_n$ 的子群，H 中存在一个无所不在的元素，则用 r-电路计算 $\mathbb{Z}_n$ 中的加法至少需要 $\lceil \log_r(2\lceil \log_2|H|\rceil)\rceil$ 个时间单位.

定理 17.44 (1) $n = p^i$，p 为素数，i 为正整数，则用 r-电路计算 $\mathbb{Z}_n$ 中的加法至少需要 $\lceil \log_r(2\lceil \log_2 n\rceil)\rceil$ 个时间单位.

(2) $n = p_1^{i_1}p_2^{i_2}\cdots p_k^{i_k}$，是 n 的素因子分解式，则用 r-电路计算 $\mathbb{Z}_n$ 中的加法至少需要 $\lceil \log_r(2\lceil \log_2 t(n)\rceil)\rceil$ 个时间单位，其中 $t(n) = \max\{p_1^{i_1}, p_2^{i_2}, \cdots, p_k^{i_k}\}$.

第十八章　环与域

定理 18.1 设 R 是环，则

(1) $\forall a \in R, a0 = 0a = 0$;

(2) $\forall a, b \in R, (-a)b = a(-b) = -(ab)$;

(3) $\forall a, b \in R, (-a)(-b) = ab$;

(4) $\forall a, b, c \in R$ 有

$$a(b-c) = ab - ac, \qquad (b-c)a = ba - ca;$$

(5) $\forall a_1, a_2, \cdots, a_n, b_1, b_2, \cdots, b_m \in R$ 有

$$\Big(\sum_{i=1}^{n} a_i\Big)\Big(\sum_{j=1}^{m} b_j\Big) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j;$$

(6) $\forall a, b \in R, n \in \mathbb{Z}, (na)b = a(nb) = n(ab)$.

定理 18.2 设 R 是环. R 是无零因子环的充分必要条件是在 R 中乘法适合消去律，即对于任意 $a, b, c \in R, a \neq 0$，若有 $ab = ab$ (或 $ba = ca$)，则有 $b = c$.

定理 18.3 设 F 为有限域，则 F 的特征是素数.

定理 18.4 设 F 为有限域，则存在素数 p，使得 $|F| = p^n$，其中 $n \in \mathbb{Z}^+$.

定理 18.5 环 R 的非空子集 S 是 R 的一个子环的充分必要条件是：对任意 $a, b \in S$ 有

(1) $a - b \in S$;　　(2) $ab \in S$.

定理 18.6 设 $\varphi : R_1 \to R_2$ 是环同态，则 $\ker \varphi$ 是环 R_1 的理想.

定理 18.7 设 $\varphi : R_1 \to R_2$ 是环同态，那么

(1) 若 S 是 R_1 的子环，则 $\varphi(S)$ 是 R_2 的子环;

(2) 若 T 是 R_2 的子环，则 $\varphi^{-1}(T)$ 是 R_1 的子环;

(3) 若 D 是 R_1 的理想，则 $\varphi(D)$ 是 R_2 的理想;

(4) 若 I 是 R_2 的理想，则 $\varphi^{-1}(I)$ 是 R_1 的理想.

定理 18.8 设 D 是环 R 的理想，$g : R \to R/D$，$\forall r \in R$ 有 $g(r) = D + r$，则 g 是 R 到 R/D 的同态，且 $\ker g = D$.

定理 18.9 (环同态基本定理) 环 R 的任何商环 R/D 都是 R 的同态像. 反之，若环 R' 是 R 的同态像，则 $R' \cong R/\ker\varphi$.

定理 18.10 设 $F[x]$ 是有限域 F 上的多项式环，$f(x) \in F[x]$. 在 $F[x]$ 上如下定义二元关系 R，$\forall g(x), h(x) \in F[x]$,

$$g(x)Rh(x) \Leftrightarrow f(x) \mid (g(x) - h(x)),$$

则 R 是 $F[x]$ 上的同余关系.

定理 18.11 设 F 为有限域，环 $F[x]/f(x)$ 是域当且仅当 $f(x)$ 在 $F[x]$ 中是不可约的.

第十九章　格与布尔代数

格的对偶原理 如果命题 P 的对一切格 L 为真，则 P 的对偶命题也对一切格为真.

定理 19.1 设 $\langle S,\preccurlyeq\rangle$ 是格，则 $\forall a,b,c\in S$ 有

(1) $a\wedge b\preccurlyeq a, a\wedge b\preccurlyeq b$;　　(2) $a\preccurlyeq a\vee b, b\preccurlyeq a\vee b$;

(3) $a\preccurlyeq b$ 且 $a\preccurlyeq c\Rightarrow a\preccurlyeq b\wedge c$;　　(4) $a\succcurlyeq b$ 且 $a\succcurlyeq c\Rightarrow a\succcurlyeq b\vee c$.

定理 19.2 设 $\langle S,\preccurlyeq\rangle$ 是格，$\forall a,b\in S$ 有

$$a\preccurlyeq b\Leftrightarrow a\wedge b=a\Leftrightarrow a\vee b=b.$$

定理 19.3 设 $\langle L,\wedge,\vee\rangle$ 是格 L 导出的代数系统，则

(1) $\forall a,b\in L$ 有

$$a\wedge b=b\wedge a, a\vee b=b\vee a;$$

(2) $\forall a,b,c\in L$ 有

$$(a\wedge b)\wedge c=a\wedge(b\wedge c),(a\vee b)\vee c=a\vee(b\vee c);$$

(3) $\forall a\in L$ 有

$$a\wedge a=a, a\vee a=a;$$

(4) $\forall a,b\in L$ 有

$$a\wedge(a\vee b)=a, a\vee(a\wedge b)=a.$$

定理 19.4 设 $\langle S,*,\circ\rangle$ 是具有两个二元运算的代数系统. 若 $*$ 和 $\circ$ 运算服从交换律、结合律和吸收律，则可以适当定义 S 上的偏序 $\preccurlyeq$，使得 $\langle S,\preccurlyeq\rangle$ 构成一个格，且 $\langle S,\preccurlyeq\rangle$ 导出的代数系统 $\langle S,\wedge,\vee\rangle$ 就是 $\langle S,*,\circ\rangle$.

定理 19.5 设 L 是格，则

(1) $\forall a,b,c\in L$ 有

$$a\preccurlyeq b\Rightarrow a\wedge c\preccurlyeq b\wedge c \text{ 且 } a\vee c\preccurlyeq b\vee c;$$

(2) $\forall a,b,c,d\in L$ 有

$$a\preccurlyeq b \text{ 且 } c\preccurlyeq d\Rightarrow a\wedge c\preccurlyeq b\wedge d \text{ 且 } a\vee c\preccurlyeq b\vee d.$$

定理 19.6 设 L 是格，则

(1) $\forall a,b,c\in L$ 有

$$a\vee(b\wedge c)\preccurlyeq(a\vee b)\wedge(a\vee c),\qquad a\wedge(b\vee c)\succcurlyeq(a\wedge b)\vee(a\wedge c);$$

(2) $\forall a,b,c\in L$ 有

$$a\preccurlyeq b\Leftrightarrow a\vee(c\wedge b)\preccurlyeq(a\vee c)\wedge b.$$

定理 19.7 设 φ 是格 $\langle L_1, \wedge, \vee \rangle$ 到 $\langle L_2, \wedge, \vee \rangle$ 的同态映射，则 $\forall a, b \in L_1$ 有

$$a \preccurlyeq b \Rightarrow \varphi(a) \preccurlyeq \varphi(b).$$

定理 19.8 设 L_1, L_2 是格，$\varphi : L_1 \to L_2$ 是双射，则 φ 为 L_1 到 L_2 的同构的充分必要条件是:

$$\forall a, b \in L_1, a \preccurlyeq b \Leftrightarrow \varphi(a) \preccurlyeq \varphi(b).$$

定理 19.9 设 L 是偏序集. 若对任意 $S \subseteq L$ 都有 $\wedge S$ (或 $\vee S$)存在，则 L 是完备格.

定理 19.10 设 L 是格，令

$$I(L) = \{x \mid x \text{ 是 } L \text{ 的理想}\},$$

则 $I(L)$ 关于集合的包含关系构成一个格，称为**格 L 的理想格**.

定理 19.11 对任意格 L，设 $I(L)$ 是 L 的理想格. 令 $I_0(L) = I(L) \cup \{\varnothing\}$，则 $I_0(L)$ 是完备格.

定理 19.12 任意格 L 都可以嵌入到 $I_0(L)$ 中.

推论 任何格都可以嵌入一个完备格.

定理 19.13 一个格 L 是模格当且仅当 L 不含有和五角格同构的子格.

定理 19.14 格 L 是模格充要条件是对 L 中任意 a, b, c，$a \preccurlyeq b$ 有

$$a \vee c = b \vee c \text{ 且 } a \wedge c = b \wedge c \Rightarrow a = b.$$

定理 19.15 设 L 为分配格，则在 L 中成立广义分配律，即 $\forall a, b_i \in L, i = 1, 2, \cdots, n$ 有

(1) $a \vee \left(\bigwedge\limits_{i=1}^{n} b_i \right) = \bigwedge\limits_{i=1}^{n} (a \vee b_i)$; (2) $a \wedge \left(\bigvee\limits_{i=1}^{n} b_i \right) = \bigvee\limits_{i=1}^{n} (a \wedge b_i)$.

定理 19.16 设 L 为分配格，则 $\forall a, b, c \in L$ 有

$$a \wedge c = b \wedge c \text{ 且 } a \vee c = b \vee c \Rightarrow a = b.$$

定理 19.17 分配格一定是模格.

定理 19.18 一个模格 L 是分配格当且仅当 $\forall a, b, c \in L$ 有

$$(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = (a \vee b) \wedge (b \vee c) \wedge (c \vee a).$$

定理 19.19 一个模格是分配格当且仅当它不含有与钻石格同构的子格.

推论 1 格 L 是分配格当且仅当 L 既不含有与五角格同构的子格，也不含有与钻石格同构的子格.

推论 2 每一条链都是分配格.

推论 3 小于五元的格都是分配格.

定理 19.20 格 L 是分配格当且仅当 $\forall a, b, c \in L$ 有

$$a \wedge c = b \wedge c \text{ 且 } a \vee c = b \vee c \Rightarrow a = b.$$

定理 19.21 设 L 是有界分配格，$a \in L$. 若 a 存在补元，则 a 的补元是惟一的.

定理 19.22 设 $\langle B, *, \circ, \triangle, a, b \rangle$ 是代数系统，其中 $*$ 和 $\circ$ 是二元运算，$\triangle$ 为一元运算，$a, b \in B$ 是零元运算. 如果满足以下条件:

(1) $\forall x, y \in B$ 有 $x * y = y * x, x \circ y = y \circ x$; (交换律)

(2) $\forall x, y, z \in B$ 有 $x * (y \circ z) = (x * y) \circ (x * z)$, $x \circ (y * z) = (x \circ y) * (x \circ z)$; (分配律)

(3) $\forall x \in B$ 有 $x * b = x, x \circ a = x$; (同一律)

(4) $\forall x \in B$ 有 $x * \triangle x = a, x \circ \triangle x = b$; (补元律)

则 $\langle B, *, \circ, \triangle, a, b \rangle$ 是布尔格. 若规定 $*$ 为 B 中求最大下界运算，$\circ$ 为求最小上界运算，则 $\triangle$ 为这个布尔格的求补运算且 a 是全下界 0，b 为全上界 1.

定理 19.23 设 $\langle B, \wedge, \vee, {}^{-}, 0, 1 \rangle$ 是布尔代数，则

(1) $\forall a \in B, \bar{\bar{a}} = a$;

(2) $\forall a, b \in B, \overline{a \wedge b} = \bar{a} \vee \bar{b}, \overline{a \vee b} = \bar{a} \wedge \bar{b}$;

(3) $\forall a, b \in B, a \preccurlyeq b \Leftrightarrow a \wedge \bar{b} = 0 \Leftrightarrow \bar{a} \vee b = 1 \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b = b$;

(4) $\forall a, b \in B, a \preccurlyeq b \Leftrightarrow \bar{b} \preccurlyeq \bar{a}$.

定理 19.24 设 B_1, B_2 是布尔代数，$\varphi : B_1 \to B_2$. 若 φ 是同态，则

(1) $\varphi(0) = 0, \varphi(1) = 1$;

(2) $\varphi(B_1)$ 是布尔代数，且是 B_2 的子代数.

定理 19.25 (有限布尔代数的表示定理) 设 B 是有限布尔代数，A 是 B 的全体原子构成的集合，则 B 同构于 A 的幂集代数 $\mathcal{P}(A)$.

定理 19.26 有限布尔代数的基数是 2^n 形式的，其中 $n \in \mathbb{N}$，且任何两个等势的有限布尔代数都是同构的.

定理 19.27 对每个有限布尔代数 B，$B \neq 0$，都存在正整数 n，使得 $B \cong \{0, 1\}^n$.

定理 19.28 设 B 是布尔代数，令

$$F_n(B) = \{f \mid f : B^n \to B\}$$

是 B 上所有 n 元布尔函数的集合. $\forall f, g \in F_n(B)$，如下定义 $f \wedge g$，$f \vee g$，$\bar{f}$，f_0 和 f_1：$\forall x \in B^n$ 有

$$\begin{aligned}
(f \wedge g)(x) &= f(x) \wedge g(x), \\
(f \vee g)(x) &= f(x) \vee g(x), \\
\bar{f}(x) &= \overline{f(x)}, \\
f_0(x) &= 0, \\
f_1(x) &= 1.
\end{aligned}$$

则 $\langle F_n(B), \wedge, \vee, ^{-}, f_0, f_1 \rangle$ 构成布尔代数.