近世代数题解

扬州师院数学系代数教研室编

目　录

第一章　基本概念

练　习

§1　集合　子集　集合的运算

1. 设 $A=\{x|x\in\mathbf{R},\ |x|\geqslant 5\}$，$B=\{x|x\in\mathbf{R},\ -6\leqslant x<0\}$，

求$A\cup B$，$A\cap B$，$A\backslash B$，$B\backslash A$，并用图形表示。

解　$A\cup B=\{x|x\in\mathbf{R},\ x<0$ 或 $x\geqslant 5\}$；

$A\cap B=\{x|x\in\mathbf{R},\ -6\leqslant x\leqslant -5\}$；

$A\backslash B=\{x|x\in\mathbf{R},\ x<-6$ 或 $x\geqslant 5\}$；

$B\backslash A=\{x|x\in\mathbf{R},\ -5<x<0\}$。

图形略。

2. 证明：$(A\subset B)\Leftrightarrow(A\cup B=B)\Leftrightarrow(A\cap B=A)$。

证　先证　$A\subset B\Leftrightarrow A\cup B=B$。

若 $A\subset B$，则 $\forall x\in A\cup B$，$x\in B$。$\therefore A\cup B\subset B$；显然 $A\cup B\supset B$，故 $A\cup B=B$。反之，若 $A\cup B=B$，则 $\forall x\in A$，$x\in A\cup B=B$，故 $A\subset B$。　$\therefore A\subset B\Leftrightarrow A\cup B=B$。

次证　$A\subset B\Leftrightarrow A\cap B=A$。

若　$A\subset B$，则$\forall x\in A$，$x\in B$，于是$\forall x\in A$，有 $x\in A\cap B$，$\therefore A\subset A\cap B$，显然 $A\cap B\subset A$，$\therefore A\cap B=A$。反之，若 $A\cap B=A$，则 $\forall x\in A$，$x\in A\cap B$，于是 $\forall x\in A$，有 $x\in B$，故 $A\subset B$。$\therefore A\subset B\Leftrightarrow A\cap B=A$。

综上证得，$A\subset B\Leftrightarrow A\cup B=B\Leftrightarrow A\cap B=A$。

3. 证明：$A=B\Longleftrightarrow A\cup B=A\cap B$.

证 若 $A=B$，则 $A\cup B=A$，$A\cap B=A$，$\therefore A\cup B=A\cap B$. 反之，若 $A\cup B=A\cap B$，则 $\forall x\in A$，有 $x\in A\cup B=A\cap B$，从而 $x\in B$，$\therefore A\subset B$；同理可证 $B\subset A$，故 $A=B$. $\therefore A=B\Longleftrightarrow A\cup B=A\cap B$.

4. 设 $A_n=(n,\infty)$，(n,∞) 表示实数轴上的开区间，即 $(n,\infty)=\{x\mid x\in\mathbf{R},\ n<x<\infty\}$，$n=0,1,2,\cdots$.

求 $\bigcup_{i=0}^{\infty}A_i$. $\bigcap_{i=0}^{\infty}A_i$.

解 $\because A_0\supset A_1\supset A_2\supset\cdots$，$\therefore \bigcup_{i=0}^{\infty}A_i=A_0=(0,\infty)$.

$\because \forall x\in\mathbf{R}$，存在非负整数 n，使 $x\leqslant n$. 于是 $x\overline{\in}A_n$，$x\overline{\in}\bigcap_{i=0}^{\infty}A_i$，$\therefore \bigcap_{i=0}^{\infty}A_i=\phi$.

5. 设 $A=\{x\mid x\in\mathbf{Z}.\ x^2-3x+2=0\}$，写出 2^A.

解 $A=\{1,2\}$，故 $2^A=\{\phi,\{1\},\{2\},\{1,2\}\}$.

6. 设 A，B 是 U 的子集，规定 $A+B=(A\backslash B)\cup(B\backslash A)$，证明：a) $A+B=B+A$ b) $A+\phi=A$，c) $A+A=\phi$.

证 a) $\because$ 集合的并适合交换律，故 $(A\backslash B)\cup(B\backslash A)=(B\backslash A)\cup(A\backslash B)$，即 $A+B=B+A$.

b) $\because A\backslash\phi=A$，$\phi\backslash A=\phi$，

$\therefore (A\backslash\phi)\cup(\phi\backslash A)=A\cup\phi=A$，即 $A+\phi=A$.

c) $\because A\backslash A=\phi$，$\therefore (A\backslash A)\cup(A\backslash A)=\phi$，即 $A+A=\phi$.

§2 映射 映射的合成

1. 对于下面给出的 **Z** 到 **Z** 的映射 f，g，h

$$f:\ x \longmapsto 3x,$$
$$g:\ x \longmapsto 3x+1,$$
$$h:\ x \longmapsto 3x+2;$$

计算 $f\circ g$，$g\circ f$，$g\circ h$，$h\circ g$，$f\circ g\circ h$。

解 $f\circ g:\ x \longmapsto 9x+3$。　$g\circ f:\ x \longmapsto 9x+1$。

$g\circ h:\ x \longmapsto 9x+7$。　$h\circ g:\ x \longmapsto 9x+5$。

$f\circ g\circ h:\ x \longmapsto 27x+21$。

2. 对于上题的 f，g，h 分别求出它们的左逆映射。

解 f 的一个左逆映射为 f_L^{-1}：

$$x \longmapsto \begin{cases} \frac{1}{3}x, & \text{当 } x=3n, \\ x, & \text{当 } x\neq 3n. \end{cases}$$

g 的一个左逆映射为 g_L^{-1}：

$$x \longmapsto \begin{cases} x, & \text{当 } x\neq 3n+1, \\ \frac{1}{3}x-\frac{1}{3}, & \text{当 } x=3n+1. \end{cases}$$

h 的一个左逆映射为 h_L^{-1}：

$$x \longmapsto \begin{cases} x, & \text{当 } x\neq 3n+2, \\ \frac{1}{3}x-\frac{2}{3}, & \text{当 } x=3n+2. \end{cases}$$

其中 n 为任意整数。

3. 对于上题的 f，g，h，找出 f，g，h 的共同的左逆映射，即找出 $\mathbf{Z}$ 到 $\mathbf{Z}$ 的映射 k，使

$$k\circ f=k\circ g=k\circ h=I_{\mathbf{Z}}.$$

解 命 $k:\ \mathbf{Z}\longrightarrow\mathbf{Z}$，

$$x \longmapsto \begin{cases} \frac{1}{3}x, & \text{当 } x=3n, \\ \frac{1}{3}x-\frac{1}{3}, & \text{当 } x=3n+1, \\ \frac{1}{3}x-\frac{2}{3}, & \text{当 } x=3n+2. \end{cases}$$

其中 n 为任意整数。

容易验证，k 是 f，g，h 的一个共同的左逆映射。

4. 对于上题的 f，g，h，找出 **Z** 到 **Z** 的一个映射，使其为 f，g 的共同的左逆映射，但不是 k 的左逆映射。

解 命 k：**Z** $\longrightarrow$ **Z**，

$$x \longmapsto \begin{cases} \frac{1}{3}x, & \text{当 } x=3n, \\ \frac{1}{3}x-\frac{1}{3}, & \text{当 } x=3n+1, \\ x, & \text{当 } x=3n+2. \end{cases}$$

其中 n 为任意整数。

容易验证，k 为满足题中要求的映射。

5. 设 f 是 A 到 B 的映射，g 是 B 到 C 的映射，$g\circ f$ 有左逆映射，能否证明 f，g 都有左逆映射？

解 当 f，g 为题设，且 $g\circ f$ 有左逆映射，可以证明 f 有左逆映射，但 g 未必有左逆映射。

证 f 有左逆映射。

设 $g\circ f$ 有一个左逆映 k，于是对任一 $a\in A$，有 A 到 C 映射 $(k\circ(g\circ f))(a)=a=I_A(a)$。

根据映射合成满足结合律得，$((k\circ g)\circ f)(a)=a$，$\forall a\in A$。故 $k\circ g$ 为 f 的一个左逆映射。

g 未必有左逆映射。例 $A=\{1,2\}$，$B=\{1,2,3\}$，$C=\{1,2\}$，

命 f：$A\longrightarrow B$，　　$x\longmapsto x$，

$$g:\quad B \longrightarrow C. \qquad\qquad i \longmapsto i,\ i=1,2.$$
$$3 \longmapsto 1.$$

容易验证，$g\circ f$ 存在左逆映射，但 g 不存在左逆映射.

6*.设 f 是 A 到 B的单射（满射），g 是 B 到 C 的单射（满射），则 $g\circ f$ 是A 到 C 的单射（满射）.

证 设 f 是 A 到 B 的单射，g 是B到 C 的单射，则对任意 $a_1, a_2\in A$，且 $a_1\neq a_2$，有$f(a_1)\neq f(a_2)$，从而$(g\circ f)(a_1)\neq(g\circ f)(a_2)$，于是 $g\circ f$ 是 A 到 C 的单射.

设 f 是 A 到 B 的满射，则 $f(A)=B$；g 是 B 到 C 的满射，则 $g(B)=C$.

于是 $(g\circ f)(A)=g(B)=C$，$\therefore g\circ f$ 是A 到C 的满射.

7. 设A表示某四年制大学数学系全体学生所成集合，$B=\{1,2,3,4\}$. 对每一 $a\in A$，规定 $f(a)$ 表示 a 所在年级，这个 f 是不是 A 到 B 的映射？是单射？满射？任取 $a\in A$，$f^{-1}(f(a))=?$ 设 $b_1, b_2\in B$，$b_1\neq b_2$，问 $f^{-1}(b_1)\cap f^{-1}(b_2)=?$ $\bigcup\limits_{b\in B} f^{-1}(b)=?$

解 根据题意，任一 $a\in A$，是且仅是某一个年级的学生，故 $f(a)$是B中唯一确定的元素，所以 f 是A到B的映射.

f 未必是满射，因为未必每个年级都有学生；一般说 f 不是单射，因为某年级如有学生，一般不会只有一人.

$f^{-1}(f(a))=\{a$ 所在年级的全体学生$\}$.

当 $b_1, b_2\in B$，$b_1\neq b_2$ 时，$f^{-1}(b_1)\cap f^{-1}(b_2)=\phi$.

$\bigcup\limits_{b\in B} f^{-1}(b)=A$.

8. 设 $A=B=\mathbf{Z}$，m是取定的正整数，对每一 $a\in A$，规

定 $f(a)=r$，此处 r 是 a 被 m 除所得非负余数：$a=qm+r$，$0\leqslant r<m$．f 是不是 A 到 B 的映射，是单射？满射？

若取 $B=\{0,1,2,\cdots m-1\}$，问 $f^{-1}(0)$，$f^{-1}(1)$，$\cdots$，$f^{-1}(m-1)$ 分别由哪些数所组成？设 $i,j\in B$，$i\neq j$，$f^{-1}(i)\cap f^{-1}(j)=?$ $\bigcup\limits_{b\in B} f^{-1}(b)=?$

解 依题意且根据整数的带余除法知，f 是 A 到 B 的映射．f 不是单射，也不是满射．

设 $B=\{0,1,2,\cdots,m-1\}$，则依题意，

$f^{-1}(0)=\{x\mid x=\mathrm{k}\,m,\quad \mathrm{k}=0\pm1,\pm2,\cdots\}$，

$f^{-1}(1)=\{x\mid x=\mathrm{k}\,m+1,\ \mathrm{k}=0,\pm1,\pm2,\cdots\}$，

……

$f^{-1}(m-1)=\{x\mid x=\mathrm{k}\,m+(m-1),\ \mathrm{k}=0,\pm1,\pm2\cdots\}$．

$i,j\in B$，$i\neq j$ 时，$f^{-1}(i)\cap f^{-1}(j)=\phi$．

$\bigcup\limits_{b\in B} f^{-1}(b)=\mathbf{Z}$．

9．设 A 是座标平面上所有点的集合，B 是 x 轴上所有点的集合，对每一 $a\in A$，规定 $f(a)$ 表示 a 向 x 轴作垂线的垂足，这个 f 是不是 A 到 B 的映射？是单射？满射？设 b_1，$b_2\in B$，$b_1\neq b_2$，$f^{-1}(b_1)\cap f^{-1}(b_2)=?$ $f^{-1}(f(a))=?$ $\bigcup\limits_{b\in B} f^{-1}(b)=?$

解 依题意，f 是 A 到 B 的映射，显然 f 是满射，f 不是单射．

设 b_1，$b_2\in B$，$b_1\neq b_2$，则 $f^{-1}(b_1)\cap f^{-1}(b_2)=\phi$．

$f^{-1}(f(a))=\{$通过点 $f(a)$，且平行于 y 轴的直线上的所有点$\}$．

$\bigcup\limits_{b\in B} f^{-1}(b)=A$．

10. 设 f：$A \longrightarrow B$，$S \subseteq A$，证明 $f^{-1}(f(S)) \supseteq S$，举例说明“$=$”不一定成立。

证 设 f：$A \longrightarrow B$，$S \subseteq A$，则对任意 $s \in S$，$f(s) \in f(S)$，$\therefore s \in f^{-1}(f(S))$，$f^{-1}(f(S)) \supseteq S$。

例：取 $A = B = \{0, 1, 2, \cdots\}$，$S = \{0\} \subseteq A$，作 A 到 B 的映射 f：$\forall a \in A$，$f(a) = 0$，显然 $f^{-1}(f(S)) = f^{-1}(0) = A \neq S$。

§3 有限集与可数集

1. 证明，有限集的任一子集都是有限集；无限集的任一扩集都是无限集。

证 设 A 为有限集，若 $A = \phi$，则结论成立。现在设 A 不空，则 A 的元素可以如下列举出来：

$$a_1, a_2, \cdots, a_n.$$

A 的空子集显然是有限集，若 B 是 A 的非空子集，则 B 的元素可以如下列举出来：

$$a_{i_1}, a_{i_2}, \cdots, a_{i_m},\ i_1 < i_2 < \cdots < i_m.$$

于是 B 与自然数集的一个断片 $|1, m| = \{1, 2, \cdots, m\}$ 等浓，B 是有限集。

设 A 为无限集，B 是 A 的任一扩集。若 B 不是无限集，则 B 为有限集，从而由前半部证明，B 的任一子集，特别的 B 的子集 A 为有限集，此与假设不合。$\therefore B$ 是无限集。

2. 证明，一个有限集与一个可数集的并是可数集。

证 设 $A = \{a_1, a_2, \cdots, a_n\}$ 为有限集，$B = \{b_1, b_2, \cdots$

b_n, …} 为可数集，则 $A\cup B=\{a_1, a_2, \cdots, a_n, b_1, b_2, \cdots, b_n, \cdots\}$。

作 f: $A\cup B\longrightarrow \mathbf{Z}^+$,

$$a_i \longmapsto i \quad 1\leqslant i\leqslant n,$$

$$b_j \longmapsto n+j \quad j=1, 2, \cdots.$$

显然 f 是 $A\cup B$ 到 $\mathbf{Z}^+$ 上的一一映射，$\therefore A\cup B$ 与 $\mathbf{Z}^+$ 等浓，从而 $A\cup B$ 为可数集。

3. 找出自然数集 P 的三个与 P 等浓的真子集 A_1, A_2, A_3。

解 设 $P=\{1, 2, 3, \cdots\}$，命 $A_1=\{$全体正奇数$\}$，$A_2=\{$全体正偶数$\}$，$A_3=P\backslash\{1\}$。A_1, A_2, A_3 为 P 的真子集，容易看出存在 $A_i(i=1, 2, 3)$ 到 P 上的一一映射，$\therefore A_i(i=1, 2, 3)$ 与 P 等浓。

4. 证明，坐标平面上所有格子点（即坐标均为整数的点）的集合是可数集。

证 记所有格子点之集为 A，即 $A=\{(a, b)|, a, b\in\mathbf{Z}\}$。可将 A 的元素排成一个方阵，再按下图所予箭头方向给 A 中元素按自然数顺序编号：

$$\begin{array}{ccccccc}
(0,0) & \rightarrow & (0,1) & (0,-1) & \rightarrow & (0,2) & (0,-2)\ \cdots \\
 & \swarrow & & \nearrow & \swarrow & & \nearrow \\
(1,0) & & (1,1) & & (1,-1) & (1,2) & (1,-2)\ \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & \swarrow \\
(-1,0) & & (-1,1) & & (-1,-1) & (-1,2) & (-1,-2)\ \cdots \\
 & \swarrow & & \nearrow & \swarrow & & \nearrow \\
(2,0) & & (2,1) & & (2,-1) & (2,2) & (2,-2)\ \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & \swarrow \\
(-2,0) & & (-2,1) & & (-2,-1) & (-2,2) & (-2,-2)\ \cdots \\
 & \swarrow & & & & & \\
\cdots & & \cdots & & \cdots & \cdots & \cdots\ \cdots
\end{array}$$

这样，A 的元素可利用自然数排列出来，故 A 是可数集。

✓5. 证明，开区间 (a, b) 与闭区间 $[a,b]$ 等浓。

证 映射 f：$x \longmapsto (b-a)x+a$ 显然是 $(0,1)$ 到 (a,b)，$[0,1]$ 到 $[a,b]$ 的双射。由 $P.18$ 例 4 知，$(0,1)$ 与 $[0,1]$ 等浓。设 φ 是 $(0,1)$ 到 $[0,1]$ 的双射，则 $f\varphi f^{-1}$ 是 (a,b) 到 $[a,b]$ 的双射，所以 (a,b) 与 $[a,b]$ 等浓。

也可以用类似 $P.18$ 例 4 的方法，直接做 (a,b) 到 $[a,b]$ 的双射。

6. 利用例 3 的方法，证明全体“自然数的无限序列”作成的集合是不可数集。

证 设 $\{A=X \mid X=(a_1, a_2 \cdots, a_n \cdots), a_i \in \mathbf{Z}^+\}$，显然 A 为无限集。假定 A 为可数集，则 A 的元素可用自然数予以编号，于是 $A=\{X_1, X_2, \cdots, X_n, \cdots\}$，其中

$$X_1=(a_{11}, a_{12}, \cdots, a_{1n}, \cdots)$$
$$X_2=(a_{21}, a_{22}, \cdots, a_{2n}, \cdots)$$
$$\cdots\cdots$$
$$X_n=(a_{n1}, a_{n2}, \cdots, a_{nn}, \cdots)$$
$$\cdots\cdots$$

作自然数的无限序列 $X=(a_1, a_2, \cdots, a_n, \cdots)$，其中 $a_i=a_{ii}$，$i=1, 2, \cdots, n, \cdots$。显然 $X \in A$，但 X 与 $X_1, X_2, \cdots, X_n, \cdots$ 中的任一个都不相同，从而产生矛盾。故 A 为不可数集。

§4 加氏积 二元关系与等价关系

1. 设 $\mathbf{R}^*$ 表示一切非零实数作成的集合，数目的 $+$、$-$、$\times$、$\div$ 是不是 $\mathbf{R}^*$ 的代数运算？为什么？n 次方幂，n

次方根是不是 $\mathbf{R}^*$ 的一元运算？为什么？$\log x$ 是不是一元运算？为什么？构造 $\mathbf{R}^*$ 的两个三元运算。

解 数目的×、÷是$\mathbf{R}^*$的代数运算。$\because \forall a, b \in \mathbf{R}^*\ a \times b$，$a \div b$ 是 $\mathbf{R}^*$ 中唯一确定的元素。数目的＋、－不是 $\mathbf{R}^*$ 的代数运算。$\because\ \forall a \in \mathbf{R}^*, -a \in \mathbf{R}^*$，但 $a+(-a)=0 \bar{\in} \mathbf{R}^*$。$a-a=0 \bar{\in} \mathbf{R}^*$。$n$ 次方幂是 $\mathbf{R}^*$ 的一元运算。$\because a \in \mathbf{R}^*$，$a^n$ 是 $\mathbf{R}^*$ 中唯一确定的元素。当 n 是奇数时，n 次方根是 $\mathbf{R}^*$ 的一元运算。当 n 为偶数时，n 次方根不是 $\mathbf{R}^*$ 的一元运算。$\because$ 负数在实数范围内不能开偶次方。$\log x$ 不是 $\mathbf{R}^*$ 的一元运算。$\because 1 \in \mathbf{R}^*$，而 $\log 1=0 \in \mathbf{R}^*$。构造 $\mathbf{R}^*$ 的两个三元运算 f_1, f_2 如下：

$f_1(x, y, z)=x$，$f_2(x, y, z)=x^2+y^2+z^2$，x, y, z 为 $\mathbf{R}^*$ 中的任意元。

2. 设 $A=\{a, b\}$，$R=\{(a, a)\}$，R 是否具有反身性？对称性？传递性？反对称性？

解 R 不具有反身性，$\because bR'b$。但 R 具有对称性，传递性，反对称性。

3. 设 $A=\{$平面上所有直线$\}$，规定 A 中的二元关系～为：$l_1, l_2 \in A$，$l_1 \sim l_2 \Longleftrightarrow l_1 /\!/ l_2$ 或 $l_1=l_2$。证明，～是 A 的一个等价关系，决定相应的等价类。

证 依题意，$\forall l \in A$，有 $l=l$，故 $l \sim l$。

任意 $l_1, l_2 \in A$，若 $l_1 \sim l_2 \Rightarrow l_1 /\!/ l_2$ 或 $l_1=l_2 \Rightarrow l_2 /\!/ l_1$ 或 $l_2=l_1 \Rightarrow l_2 \sim l_1$。

任意 $l_1, l_2\ l_3 \in A$，若 $l_1 \sim l_2$ 且 $l_2 \sim l_3 \Rightarrow l_1 /\!/ l_2$ 或 $l_1=l_2$ 且 $l_2 /\!/ l_3$ 或 $l_2=l_3 \Rightarrow l_1 /\!/ l_3$ 或 $l_1=l_3 \Rightarrow l_1 \sim l_3$。

可见～具有反身性、对称性、传递性，$\therefore$～是 A 的一个等价关系。

当 $l\in A$ 时，由 l 决定的等价类为：.

直线 $y=\mathrm{k}x=\{l|l\in A$，$l\parallel$ 直线 $y=\mathrm{k}x$，或 l 就是直线 $y=\mathrm{k}x\}$，k 为任意实数，直线 $x=0=\{l|l\in A, l\parallel$ 直线 $x=0$，或 l 就是直线 $x=0\}$.

4. 在复数集 **C** 中，规定二元关系～为：

$a\sim b \Longleftrightarrow a$ 的幅角 $= b$ 的幅角.

证明，～是 **C** 的一个等价关系，决定相应的等价类.

证 $\forall a\in\mathbf{C}$，有 $arga=arga$，故 $a\sim a$.

任意 $a, b\in\mathbf{C}$，若 $arga=argb\Rightarrow argb=arga$，即由 $a\sim b\Rightarrow b\sim a$.

任意 $a, b, c\in\mathbf{C}$，设 $a\sim b$，$b\sim c$，则 $arga=argb$，$argb=argc\Rightarrow arga=argc$，故 $a\sim c$

可见～是 **C** 的一个等价关系.

等价类为：$\bar{a}_\varphi=\{z|z\in\mathbf{C}, argz=\varphi+2\,\mathrm{k}\pi, \mathrm{k}\in\mathbf{Z}\}\ 0\leqslant\varphi<2\pi$；与 $\bar{0}=\{0\}$.

5. 设 $A=\{1,2,3,4\}$，在 2^A 中规定二元关系～：$S\sim T\Longleftrightarrow S, T$ 含有元素个数相同，证明，这是一个等价关系，写出商集 $2^A/\sim$.

证 记 2^A 的元素 S 所含元素个数为 $|S|$. $\forall S\in 2^A$，则 $|S|=|S|$，依题意 $S\sim S$.

对任意的 $S, T\in 2^A$，若 $S\sim T$，则 $|S|=|T|\Rightarrow|T|=|S|$，即 $T\sim S$.

任意的 $S, T, V\in 2^A$，由 $S\sim T$ 和 $T\sim V\Rightarrow |S|=|T|$，$|T|=|V|\Rightarrow |S|=|V|$，即 $S\sim V$.

∴ ～是 2^A 的一个等价关系.

商集 $2^A/\sim=\{\phi, A_1, A_2, A_3, A_4\}$ 其中

$A_1=\{\{1\},\{2\},\{3\},\{4\}\}$,

$A_2=\{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$,

$A_3=\{\{1,2,3\},\{1,3,4\},\{1,2,4\},\{2,3,4\}\}$,

$A_4=A$。

✓6。$(F)_n$ 表示数域F上全部 n 阶方阵的集合，f 是 $(F)_n$ 到 $\{0,1,2,\cdots,n\}$ 上的满射。

$$f:\ (a_{ij})\longmapsto \text{秩}\ (a_{ij})$$

求 f 决定的等价关系，决定等价类。

解 由 f 确定的 $(F)_n$ 中的等价关系为：

$(a_{ij})\sim(b_{ij})\Longleftrightarrow f((a_{ij}))=f((b_{ij}))$，即秩 $(a_{ij})=$ 秩 (b_{ij})。

等价类为：

$\overline{A}_r=\{X\mid X=(x_{ij})\in(F)_n,\ \text{秩}\ X=r\}$，$r=0,1,2,\cdots,n$。

7。设 R_1，R_2 是A的两个等价关系，$R_1\cap R_2$ 是不是A的二元关系？是不是等价关系？为什么？$R_1\cup R_2$ 是不是A的二元关系？

解 集A的二元关系，实际上是 $A\times A$ 的子集，而$A\times A$的两个子集之交、之并仍然是 $A\times A$ 的子集，故 $R_1\cap R_2$，$R_1\cup R_2$ 都是A的二元关系。

若 R_1，R_2 皆A的等价关系，$R_1\cap R_2$ 仍是A的等价关系。事实上，$\forall a\in A$，$(a,a)\in R_1$，$(a,a)\in R_2\Rightarrow(a,a)\in R_1\cap R_2$。

对任意 $a,b\in A$，若 $(a,b)\in R_1\cap R_2\Rightarrow(a,b)\in R_1$，$(a,b)\in R_2$，但 R_1，R_2 为等价关系，故 $(b,a)\in R_1$，$(b,a)\in R_2$，于是 $(b,a)\in R_1\cap R_2$。

同样可证，$R_1\cap R_2$ 具有传递性，所以 $R_1\cap R_2$ 是A的

等价关系。

8. 设 R_1，R_2 是 A 的两个二元关系，规定

$R_1 \circ R_2 = \{(a, b) \mid \exists x \in A:\ (a, x) \in R_1, (x, b) \in R_2\}$。

证明，“$\circ$”是 A 的一切二元关系所成集合 B 的一个二元运算。

证：∵ $R_1 \circ R_2$ 是 $A \times A$ 的一个子集，即 $R_1 \circ R_2$ 确定了 A 的一个二元关系。∴ “$\circ$”：$(R_1, R_2) \longmapsto R_1 \circ R_2$ 是 $B \times B$ 到 B 的一个映射，故它是 B 的一个二元运算。

9. 设 $(\mathbf{R})_n$ 表示实数域 $\mathbf{R}$ 上一切 n 阶方阵的集合。

a) 对于 $A, B \in (\mathbf{R})_n$，规定

$AR_1B \Longleftrightarrow \exists P, Q \in (\mathbf{R})_n, |P| \neq 0, |Q| \neq 0:\ PAQ = B$。

证明，R_1 是 $(\mathbf{R})_n$ 的一个等价关系。等价元素类取怎样的方阵作为代表元，形式最简单？

b) 对于 $A, B \in (\mathbf{R})_n$，规定

$AR_2B \Longleftrightarrow \exists P \in (\mathbf{R})_n, |P| \neq 0:\ PAP^{-1} = B$。

证明，R_2 是 $(\mathbf{R})_n$ 的一个等价关系。等价元素类的代表元是怎样的方阵，形式最简单？

c) 对于 $A, B \in (\mathbf{R})$，规定

$AR_3B \Longleftrightarrow \exists P \in (\mathbf{R})$，$|P| \neq 0:\ PAP' = B$。

证明，R_3 是 $(\mathbf{R})$ 的一个等价关系。等价元素类取怎样的代表元形式最简单？

d) 对于 $A, B \in (\mathbf{R})$，规定

$AR_4B \Longleftrightarrow \exists P \in (\mathbf{R})$，$PP' = I$（单位方阵）：$PAP' = B$。

证明，R_4 是 $(\mathbf{R})$ 的一个等价关系。等价元素类可以取怎样的代表元？

证 由线性代数知识可知，实数域上 n 阶方阵的等价、相似以及实对称矩阵的合同、正交合同皆具有反身性、对称性、传递性，故本题中的 R_1，R_2，R_3，R_4 皆是等价关系。

关于 R_1，等价元素类的代表取如下方阵，形式最简单：

$E_r = diag(\underbrace{1, 1, \cdots 1}_{r}, 0, \cdots, 0)$，$(0 \leqslant r \leqslant n)$

由等价关系 R_2 所划分的等价类，其代表元可取矩阵的有理标准形（详见张远达，熊全淹的《线性代数》第五章）。

关于等价关系 R_3，等价元素的代表可取：

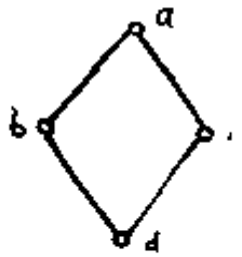
$E_{st} = diag(\underbrace{1, 1, \cdots, 1}_{s}, \underbrace{-1, -1, \cdots, -1}_{t}, 0, \cdots, 0)$，$s$，$t$ 为非负整数，且 $s+t \leqslant n$。

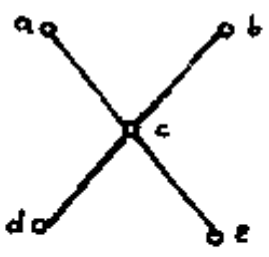
关于等价关系 R_4，等价元素类的代表元可取：

$E_{\lambda_1, \cdots, \lambda_n} = diag(\lambda_1, \lambda_2, \cdots, \lambda_n)$，$\lambda_i \in \mathbf{R}$，且满足 $\lambda_1 \leqslant \lambda_2 \leqslant \cdots \leqslant \lambda_n$。

§5 有序集 Zorn 引理

1. 写出下面图形表示的偏序关系：





指出其极大元，极小元，最大元，最小元。

解 左图表示的偏序关系为：

"$\leqslant$" $=\{(a,a),(b,b),(c,c),(d,d),(d,b),$ $(d,c),(b,a),(c,a),(d,a)\}$。$a$ 为极大元同时亦为最大元，d 为极小元，同时亦为最小元。

右图表示的偏序关系为：

"$\leqslant$" $=\{(a,a),(b,b),(c,c),(d,d),(e,e),$ $(d,c),(e,c),(c,a),(c,b),(d,b),(d,a),(e,b),$ $(e,a)\}$。a,b 为极大元，d,e 为极小元，此偏序关系中无最大元，也无最小元。

2. 举一个偏序集 $(S,\leqslant)$ 但不是有序集的例子。

解 令 $S=\{$数域 P 上的首项系数为1的多项式$\}$，规定：$f(x),g(x)\in S$；$f(x)\leqslant g(x)\Longleftrightarrow f(x)\mid g(x)$。显然可知，依规定"$\leqslant$"具有反身性，反对称性及传递性，故 $(S,\leqslant)$ 是一个偏序集。但 $(S,\leqslant)$ 不是有序集，此因，存在 $f(x),g(x)\in S$，$f(x)\nmid g(x)$，$g(x)\nmid f(x)$，从而既无 $f(x)\leqslant g(x)$，又无 $g(x)\leqslant f(x)$。故"$\leqslant$"不是顺序关系。

3. 举一个有序集 $(S,\leqslant)$ 但不是良序集的例子，并对 S 规定另一偏序关系，使之成为良序集。

解 取 $S=\mathbf{Z}$，"$\leqslant$"表示数目的大小关系，显然 $(S,\leqslant)$ 是有序集，但不是良序集，因为 $(S,\leqslant)$ 中无最小元。

现规定$\mathbf{Z}$的二元关系"$\leqslant'$"：$a\leqslant' b$，如果 $|a|<|b|$；或 $a=b$；或 $a=-b$，且 a 为负数。显然 $(\mathbf{Z},\leqslant')$ 是有序集，下面证明它是良序集。

设 N 是 $\mathbf{Z}$ 的任一非空子集，记 $N'=\{|a|\mid a\in N\}$，因为以数目大小关系为二元关系的非负整数集是良序集，所以 $(N',\leqslant')$ 有最小元 $|a_0|$，如果 $\forall a\in N$，且 $a\neq a_0$，有 $|a|$

$\neq |a_0|$，即 $|a|>|a_0|$，则 a_0 是 $(N,\leqslant')$ 中最小元；如果存在 $a_1\in N$，且 $a_1\neq a_0$，但 $|a_1|=|a_0|$，则 a_1，a_0 中是负数的那一个为 $(N,\leqslant')$ 的最小元，总之，$(N,\leqslant')$ 有最小元。 $\therefore$ $(\mathbf{Z},\leqslant')$ 是良序集。

4．证明，一个偏序集$(S,\leqslant)$若有最大元，则只存在一个。

证 设 $(S,\leqslant)$ 为偏序集，m，n 皆为其最大元，则依定义有 $m\leqslant n$ 和 $n\leqslant m$，由反对称性得$m=n$，所以$(S,\leqslant)$ 若有最大元，只存在一个。

5．证明，有限偏序集的每一个非空子集均含有极小元。

证 设 S 是有限偏序集，T 是 S 的任一非空子集，"$\leqslant$" 为偏序关系。取定$x_0\in T$，考虑$Tx_0=\{x|x\in T,x\leqslant x_0\}$，显然 $x_0\in Tx_0$，若 $Tx_0=\{x_0\}$，则 x_0 为 T 的一个极小元，否则 $\exists x_1\in Tx_0$，$x_1<x_0$。继续考虑 $Tx_1=\{x|x\in T,x\leqslant x_1\}$。若 $Tx_1=\{x_1\}$，则 x_1 是 T 的一个极小元，否则 $\exists x_2\in Tx_1$，$x_2<x_1$。如此继续，我们得到一个链：

$$\cdots x_i<\cdots<x_2<x_1<x_0$$

由于 T 为有限集，此链不可能无限下去，必在有限步后中止，即存在 x_m，使 $Tx_m=\{x|x\in T,x\leqslant x_m\}=\{x_m\}$，从而 $\forall x\in T,x\leqslant x_m$，$x_m$ 为 T 的极小元。

6．举一个含有 $n+1$ 个元的偏序集，使其含有 n 个极大元，一个极小元。

解 令 $S=\{1,p_1,p_2,\cdots,p_n,p_i$ 为互不相同的素数$\}$。定义 S 中的二元关系 "$\leqslant$" 为数的整除关系。显然 $(S,\leqslant)$ 成为一个偏序集。1 是 S 的一个极小元，其余 n 个元皆为极大元。

7. 设 $(Z, \leqslant)$ 是整数集关于整除关系作成的偏序集，$T=\{1, 2, \cdots, 10\}$，求 T 的上界，下界，有没有最小上界？最大下界？与例 6 的区别何在？

解 依题意 T 的上界和下界分别是 1，2，…，10 的公倍数和公约数，而最小上界和最大下界则分别是最小公倍数与最大公约数。所以 T 的最小上界为：$5\cdot7\cdot9\cdot8=2520$，T 的上界为：$2520\,k$，$k\in Z^+$；T 的最大下界为 1，且是 T 仅有的下界。

与例 6 的区别，例 6 讨论的是 T 的最小元，极小元，最大元，极大元，这与上，下界，最大下界，最小上界是不同的概念。对一个偏序集的子集来说，如有最小元，则最小元必是最大下界。如有最大元，则最大元必是最小上界。反之未必。例如本题中的 T，1 是最小元，也是最大下界；2520 是最小上界，但不是 T 的最大元。

8. 设 A 是任意集合，在偏序集 $(2^A, \subseteq)$ 中取其子集的序列 $\{a_1\}, \{a_1, a_2\}, \cdots, \{a_1, a_2, \cdots, a_n\}, \cdots$，它们的并集是不是 2^A 的一个极大元？为什么。

解 题中所言子集序列之并未必是 2^A 的一个极大元。因为该子集序列的并集可能是 A 的真子集，例如当 A 是不可数集时。事实上，$(2^A, \subseteq)$ 中仅有一个极大元，也是最大元 A。

9. 证明，偏序集 $(2^A, \subseteq)$ 既有最大元，也有最小元。$(2^A\backslash\phi, \subseteq)$ 有没有最小元？找出它的极小元。

证 $\because A\in 2^A$，且对所有 $x\in 2^A$，总有 $x\subseteq A$，故 A 是 $(2^A, \subseteq)$ 的最大元；同样，由于 $\phi\in 2^A$，$\forall x\in 2^A$，$\phi\subseteq x$，故 ϕ 是 $(2^A, \subseteq)$ 的最小元。

$(2^A\backslash\phi, \subseteq)$ 没有最小元，其极小元为所有 $\{a\}$，$a\in A$。

10. 设 $S=\mathbf{Z}$，“$m\leqslant n$” 表示 mn 是非负整数，且 $m|n$，证明 $(S, \leqslant)$ 是一个偏序集。S 有没有最大元？最小元？极大元？极小元？

证 对 $\forall x\in S$，恒有 $x\cdot x$ 为非负整数，且 $x|x$，故 $x\leqslant x$。$\forall x, y\in S$，$x\leqslant y$ 且 $y\leqslant x$，则依题意可知 x，y 或同时为 0，或为同号的互相整除的整数，故 $x=y$。$\forall x, y, z\in S$，$x\leqslant y$，且 $y\leqslant z$，则由 $x|y$ 且 $y|z$，推得 $x|z$，再由 xy，yz 非负，可知 xz 非负。所以 $x\leqslant y$。可见 “$\leqslant$” 具有反身性，反对称性，传递性。所以 $(S, \leqslant)$ 是一个偏序集。

显然 0 为 S 的一个最大元，亦是 S 的唯一极大元。S 没有最小元，S 有极小元 1 和 -1。

11. 设偏序集 $(S, \leqslant)$ 有最小元，则 S 有且只有唯一的极小元。

证 首先可知 $(S, \leqslant)$ 的最小元，亦是 S 的一个极小元。所以，当 $(S, \leqslant)$ 有最小元 m 时，S 至少有一个极小元。

设 m' 是 $(S, \leqslant)$ 的任一极小元，$\because$ m 是最小元，$\therefore m\leqslant m'$。$\because m'$ 是极小元，$\therefore$ 由 $m\leqslant m'\Rightarrow m=m'$。

12. 设 A 是一个非空集合，B 是 A 上一切二元关系所组成的集合，对于 B 中元素 R_1，R_2，如果对于 $x, y\in A$，$xR_1y\Rightarrow xR_2y$，那末，就规定 $R_1\leqslant R_2$，则 $(B, \leqslant)$ 作成一个偏序集。

证 依题意，任意 $R\in B$，总有 $R\leqslant R$。设 R_1，$R_2\in B$，且 $R_1\leqslant R_2$ 及 $R_2\leqslant R_1$，则对于 $x, y\in A$，$xR_1y\Rightarrow xR_2y$，及 $xR_2y\Rightarrow xR_1y$，此就是说，当 $(x, y)\in R_1$ 时 $\Rightarrow (x, y)\in R_2$，及 $(x, y)\in R_2\Rightarrow (x, y)\in R_1$。$\therefore$ R_1，R_2 表示 $A\times A$ 的同

一子集合，$R_1 \underset{i}{=} R_2$。设 $R_1, R_2, R_3 \in B$，满足 $R_1 \leqslant R_2$ 且 $R_2 \leqslant R_3$，则对于 $x, y \in A$，$xR_1y \Rightarrow xR_2y$，及 $xR_2y \Rightarrow xR_3y$。从而 $xR_1y \Rightarrow xR_3y$，$\therefore R_1 \leqslant R_3$。可见 B 中的二元关系“$\leqslant$”具有反身性，反对称性，传递性，$\therefore (B, \leqslant)$ 作成一个偏序集。

此外，我们亦可以直接由 $(B, \leqslant) = (2^{A\times A}, \subseteq)$ 得 $(B, \leqslant)$ 是一个偏序集。

习　题

1*。设 $A_n = \{a \mid a \in \mathbf{Z}, (2^n \mid a) \wedge (2^{n+1} \nmid a)\}$

求　$A = \bigcup_{i=1}^{\infty} A_n$

解　$A = \bigcup_{n=1}^{\infty} A = \{2k \mid k \in \mathbf{Z}\}$。

2。设 $A_x = \{y \mid y \in R, 0 \leqslant y < x\}$，

求　$A = \bigcap_{\substack{x\in R \\ x>1}} A_x$。

解　$A = \bigcap_{\substack{x\in R \\ x>1}} A_x = \{y \mid y \in \mathbf{R}, 0 \leqslant y \leqslant 1\}$。

3。设 $A_1, A_2, \cdots$，是集合 E 的可数个子集，命

$$\overline{A} = \bigcap_{m=1}^{\infty} \bigcup_{i=m}^{\infty} A_i, \qquad A = \bigcup_{m=1}^{\infty} \bigcap_{i=m}^{\infty} A_i,$$

证明：① $\overline{A}$ 由一切属于无限多个 A_i 的元所组成；

② A 由一切属于“几乎所有 A_i”的元所组成。（“几乎所有 A_i”指除有限个外的全部 A_i，也说“差不多所有 A_i”。）

证　① 若 x 属于无限多个 A_i，则 $\forall m \geqslant 1$，$A_1 A_2$，$\cdots$，A_{m-1} 是有限个，$\therefore \mathbf{E} m' \geqslant m$，使 $x \in A_{m'}$，于是 $x \in \bigcup_{i=m}^{\infty} A_i$。故 $x \in \overline{A} = \bigcap_{m=1}^{\infty} \bigcup_{i=m}^{\infty} A_i$。

若 x 属于有限个 A_i，不妨设 x 属于 $A_{i_1}, A_{i_2}, \cdots, A_{i_k}$，$i_1 < i_2 < \cdots < i_k$，取 $m > i_k$，$\forall m' \geqslant m$，$x \bar{\in} A_{m'}$，于是 $x \bar{\in} \bigcup_{i=m}^{\infty} A_i$" 故 $x \bar{\in} \overline{A}$。

综上所述，$\overline{A}$ 由一切属于无限多个 A_i 的元所组成。

② 若 $x \in \bigcup_{m=1}^{\infty} \bigcap_{i=m}^{\infty} A_i$，则至少 $\exists m_0$，使 $x \in \bigcap_{i=m_0}^{\infty} A_i$，于是，$x$ 至多不属于 $A_1, A_2, \cdots, A_{m-1}$，即 x 属于 "几乎所有的 A_i"。若 x 属于 "几乎所有的 A_i"，不妨设 x 属于除 $A_{i_1}, A_{i_2}, \cdots, A_{i_k}$ 以外的所有 A_i，取 $m_0 > i_k$，$x \in \bigcap_{i=m_0}^{\infty} A_i$。故 $x \in A = \bigcup_{m=1}^{\infty} \bigcap_{i=m}^{\infty} A_i$。

综上可见，A 由一切属于 "几乎所有 A_i'" 的元所组成。

4. 设 $\{A_i | i \in I\}$ 是集合 E 的子集族，f 是 E 到 B 的映射，证明

① $f(\bigcup_{i=1} A_i) = \bigcup_{i \in I} f(A_i)$，

② $f(\bigcap_{i \in I} A_i) \subset \bigcap_{i \in I} f(A_i)$。

举例说明，② 的 "$\subset$" 可能发生。

证 ① 设 $x' \in f(\bigcup_{i \in I} A_i)$，则 $\exists x \in \bigcup_{i \in I} A_i$，使 $x' = f(x)$，于是 $x \in$ 某一个 A_i，$x' = f(x) \in f(A_i) \subseteq \bigcup_{i \in I} f(A_i)$，$\therefore f(\bigcup_{i \in I} A_i) \subseteq \bigcup_{i \in I} f(A_i)$。

同样可证，$\bigcup_{i \in I} f(A_i) \subseteq f(\bigcup_{i \in I} A_i)$，$\therefore f(\bigcup_{i \in I} A_i) = \bigcup_{i \in I} f(A_i)$。

② 任取 $x' \in f(\bigcap_{i \in I} A_i)$，则 $\exists x \in \bigcap_{i \in I} A_i$，使 $x' = f(x)$，

$\because x\in A_i\ \forall i\in I$，$\therefore f(x)\in f(A_i)$，$\forall i\in I$，即 $x'\in f(A_i)$，$\forall i\in I$。故 $x'\in\bigcap_{i\in I} f(A_i)$，$f(\bigcap_{i\in I} A_i)\subseteq\bigcap_{i\in I} f(A_i)$。

例：取 $E=\mathbf{Q}$，$A_1=\{$非负有理数$\}$，$A_2=\{$非正有理数$\}$，$B=\{0,1\}$。定义

$$f:\quad E\longrightarrow B$$

$$x\longmapsto 0,\ \text{当}\ x=0\ \text{时},$$

$$x\longmapsto 1,\ \text{当}\ x\neq 1\ \text{时}.$$

$\because f(A_1\cap A_2)=\{0\}$，$f(A_1)\cap f(A_2)=\{0,1\}$，

$\therefore f(A_1\cap A_2)\subset\{f(A_1)\cap f(A_2)$。

√5。设 $f:A\twoheadrightarrow A$，且 $f\circ f=f$，则 $f=I_A$。

证 由题设 f 是 A 到 A 的满射，故对 $\forall a\in A$，$\exists a'\in A$，使 $f(a')=a$。又 $\because f\circ f=f$，$\therefore$ 有 $f(a)=f\circ f(a')=f(a')=a$，$\forall a\in A$，$\therefore f=I_A$。

6。找出 $\mathbf{Z}$ 到 $\mathbf{Z}$ 的 $n+1$ 个映射 f_i，$i=1,2,\cdots,n,n+1$ 使 $f_1,f_2,\cdots,f_n$ 有共同的左逆映射 g，但 g 不是 f_{n+1} 的左逆映射。

解 作 $\mathbf{Z}$ 到 $\mathbf{Z}$ 的 $n+1$ 映射如下

$f_i:\ x\longmapsto nx+(i-1)$，$\forall x\in\mathbf{Z}$，$i=1,2,\cdots,n,n+1$。

再命 $g:\ \mathbf{Z}\longrightarrow\mathbf{Z}$

$x\longmapsto\left[\frac{x}{n}\right]$，$\forall x\in\mathbf{Z}$，符号 $[a]$ 表示不超过 a 的最大整数。

容易看出，$\forall x\in\mathbf{Z}$，$(g\circ f_i)(x)=x$，$i=1,2,\cdots,n$。

而 $(g\circ f_{n+1})(x)=x+1\neq x$。

$\therefore g$ 是 $f_1,f_2,\cdots,f_n$ 的共同左逆映射，但不是 f_{n+1} 的左逆映射。

7*. 设A, B, C是集合E的三个子集，且$A=B\cup C$, $B\cap C=\phi$，找出2^A到加氏积$2^B\times 2^C$的一个双射。

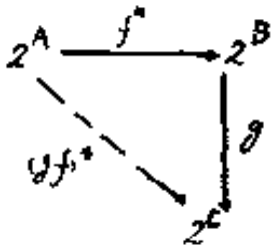
解　作映射f: $2^A\longrightarrow 2^B\times 2^C$

$$A_i\longmapsto (A_i\cap B,\ A_i\cap C),\ \forall A_i\in 2^A.$$

由$(A_i\cap B)\cup(A_i\cap C)=A_i\cap(B\cup C)=A_i\cap A=A_i$，可知$f$是单射。

$\forall B_i\in B$, $C_i\in C$，记$A_i=B_i\cup C_i$, $A_i\in 2^A$。$\because C\cap B=\phi$, $C_i\cap B=\phi$, $\therefore A_i\cap B=(B_i\cup C_i)\cap B=(B_i\cap B)\cup(C_i\cap B)=B_i\cap B=B_i$；同理$A_i\cap C=C_i$。于是$A_i$在映射$f$下的象是$(B, C_i)$，故$f$是满射，从而$f$是双射。

8*.设f是A到B的映射，g是B到C的映射，f^*是2^A到2^B的映射，f^*: $S\longmapsto f(S)$, $\forall S\subseteq A$。g^*是2^B到2^C的映射，g^*: $T\longmapsto g(T)$, $\forall T\subseteq B$，证明下面图形交换：



即 $(gf)^*=g^*\circ f^*$。

证　显然$(gf)^*$, $g^*\circ f^*$都是2^A到2^C的映射。

对$\forall S\subseteq A$，有

$$(gf)^*(S)=(gf)(S)=g(f(S))=g^*(f(S))=g^*(f^*(S))=g^*\circ f^*(S)$$

$\therefore (gf)^*=g^*\circ f^*$。

9. 设 $\mathbf{Z}^+=\{1, 2, \cdots\}$，证明，存在 $\mathbf{Z}^+\times\mathbf{Z}^+$ 到 $\mathbf{Z}^+$ 的双射 ϕ。

证 $\forall p, q\in\mathbf{Z}^+$，$\frac{1}{2}(p+q-2)(p+q-1)+p\in\mathbf{Z}^+$。

命 $\phi: \mathbf{Z}^+\times\mathbf{Z}^+ \longrightarrow \mathbf{Z}^+$

$$(p, q) \longmapsto \frac{1}{2}(p+q-2)(p+q-1)+p,$$

$\forall p, q\in\mathbf{Z}^+$。

则 ϕ 是映射为显然。下面首先证明它是一个满射：

任取 $n\in\mathbf{Z}^+$，$\exists k\in\mathbf{Z}^+$，使得 $\frac{1}{2}k(k+1)\leqslant n<\frac{1}{2}(k+1)(k+2)$。

若 $n=\frac{1}{2}k(k+1)$，则取 $p=k$，$q=1$，有 $\phi(p, q)=n$。

若 $\frac{1}{2}k(k+1)<n<\frac{1}{2}(k+1)(k+2)$，则取 $p=n-\frac{1}{2}k(k+1)$，$q=\frac{1}{2}(k+1)(k+2)-n+1$，有 $\phi(p, q)=n$。

可见对 $\forall n\in\mathbf{Z}^+$，$\exists(p, q)\in\mathbf{Z}^+\times\mathbf{Z}^+$，使 $\phi(p, q)=n$。

再证 ϕ 是单射：设 $(p, q), (m, n)\in\mathbf{Z}^+\times\mathbf{Z}^+$，且 $(p, q)\neq(m, n)$，则 $p\neq m$ 或 $q\neq n$。

若 $p+q=m+n$，则 $p+q-2=m+n-2$，$p+q-1=m+n-1$，且 $p\neq m$，于是

$$\phi(p, q)=\frac{1}{2}(p+q-2)(p+q-1)+p=\frac{1}{2}(m+n-2)(m+n-1)+p\neq\frac{1}{2}(m+n-2)(m+n-1)+m=\phi(m, n).$$

若 $p+q\neq m+n$，不妨设 $p+q>m+n$，于是

$$\frac{1}{2}(p+q-2)(p+q-1)-\frac{1}{2}(m+n-2)(m+n-1)=\frac{1}{2}(p+q-2)\cdot(p+q-1)-\frac{1}{2}(p+q-2)(m+n-1)+\frac{1}{2}(p+q-2)(m+n-1)-\frac{1}{2}(m+n-2)(m+n-1)\geqslant\frac{1}{2}(p+q-2)+\frac{1}{2}(m+n-1)>m-1\geqslant m-p$$

$$\therefore \frac{1}{2}p+q-2)(p+q-1)+p>(m+n-2)(m+n-1)$$

+m即 $\phi(p,q)\neq\phi(m,n)$。故 ϕ 是单射。

从而证得，ϕ 是 $\mathbf{Z}^+\times\mathbf{Z}^+$ 到 $\mathbf{Z}^+$ 的一个双射。

本题也可用练习三第4题的方法证明 $Z^+\times Z^+$ 是可数无限集，从而存在 $Z^+\times Z^+$ 到 Z^+ 的双射。

√ 10. 证明，不存在 A 到 2^A 的双射，此处 $A\neq\phi$。

证　如果存在 A 到 2^A 的双射 φ，则对任意 $a\in A$，不是 $a\in\varphi(a)$ 就是 $a\bar{\in}\varphi(a)$

令 $S=\{a|a\in A, a\bar{\in}\varphi(a)\}$, $S'=\{a|a\in A, a\in\varphi(a)\}$。于是 $A=S\cup S'$，且 $S\cap S'=\Phi$。

$\because S\in 2^A$，$\therefore \exists a_0\in A$，使 $\varphi(a_0)=S$。

若 $a_0\in S$，则因 $\varphi(a_0)=S$，$\therefore a_0\in\varphi(a_0)$，这与 S 的定义矛盾。

若 $a_0\bar{\in}S$，则 $a_0\in S'$，于是根据 S' 的定义，又得到 $a_0\in\varphi(a_0)=S$。产生矛盾，这就证得，不存在 A 到 2^A 的双射。

11. 设 $A=\{1,2,3\}$，f 是 A 到 A 的满射，具有性质 $f(1)=3$，求 f 的个数。

解　由题设，f 是 A 到 A 的一一变换，且限定 $f(1)=3$，于是 f 的个数为2：f_1: $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$; f_2: $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$

12. 设 $A=\{1, 2, \cdots, n\}$，f 是 A 到 A 的满射，具有性质 $f(x_i)=y_i$，$i=1, 2, \cdots, k$，$k<n$，$x_i, y_i \in A$，求 f 的个数。

解 由题设，f 是 A 到 A 的一一变换，今限定 $f(x_i)=y_i$，$i=1, 2, \cdots, k$，$k<n$，则 f 的个数应 $(n-k)$ 个元素的全排列数 $(n-k)!$。

13. A 有 k 个元素，B 有 n 个元素，$k \leqslant n$，求 A 到 B 的单射的个数。

解 若 f 是 A 到 B 的单射，则 $f(A)$ 是由 B 中 k 个不同元素所组成。于是 f 的个数为从 B 中每次取 k 个不同元素进行排列所得到的排列数。因而，A 到 B 的单射个数为

$$A_n^k = \frac{n!}{(n-k)!}.$$

14. $\mathbf{Z}[x]$ 表示一切整数的一元多项式的集合，证明，$\mathbf{Z}[x]$ 是可数集。

✓**证** 显然 $\mathbf{Z}$ 是可数集。由 §3 练习第 4 题知 $\mathbf{Z}\times\mathbf{Z}$ 是可数集，因此 $\mathbf{Z}\times\mathbf{Z}$ 与 $\mathbf{Z}$ 等势，于是利用归纳法可证，有限个 $\mathbf{Z}$ 的加氏积 $\mathbf{Z}\times\mathbf{Z}\times\cdots\times\mathbf{Z}$ 是可数集。

下面证明 $\mathbf{Z}[x]$ 是可数集。$\forall f(x)=a_n x^n+a_{n-1}x^{n-1}+\cdots+a_1 x+a_0 \in \mathbf{Z}[x]$，可由系数的有序数组 $(a_n, a_{n-1}, \cdots, a_1, a_0) \in \underbrace{\mathbf{Z}\times\mathbf{Z}\times\cdots\times\mathbf{Z}}_{n+1}$ 唯一确定。

记 $\mathbf{Z}_n=\{f(x)=\sum_{i=0}^{n} a_i x^i \mid a_i \in \mathbf{Z}\}$

$\because \mathbf{Z}\times\mathbf{Z}\times\cdots\times\mathbf{Z}$ 是可数集，$\therefore \mathbf{Z}_n$ 也是可数集，而 $\mathbf{Z}[x]=\bigcup_{n\in\mathbf{Z}^+}\mathbf{Z}_n$。

用类似的证明方法，可以证明可数个可数集的并集是可数集。

于是得到 $\mathbf{Z}[x]$ 是可数集。

15. 证明 $\mathbf{Q}[x]$ 是可数集。

证 由 $p.40$ 例 4，全体正有理数是可数集，于是存在 $\mathbf{Z}^+$ 到 $\mathbf{Q}^+$ 的双射 φ。作 $\mathbf{Z}$ 到 $\mathbf{Q}$ 的映射 f

$$f:\begin{cases} a \longmapsto \varphi(a), & \text{当 } a \text{ 为正整数时,} \\ a \longmapsto \varphi(-a), & \text{当 } a \text{ 为负整数时,} \\ 0 \longmapsto 0 \end{cases}$$

容易看出，f 是 $\mathbf{Z}$ 到 $\mathbf{Q}$ 的双射，$\mathbf{Z}$ 是可数集，$\therefore \mathbf{Q}$ 也是可数集。

以下仿 14 题的方法，可证得 $\mathbf{Q}[x]$ 是可数集。

16. 证明，$2^{\mathbf{Z}^+}$ 是不可数集。

证 假如 $2^{\mathbf{Z}^+}$ 是可数集，则 $2^{\mathbf{Z}^+}$ 与 $\mathbf{Z}^+$ 等浓，从而存在 $\mathbf{Z}^+$ 到 $2^{\mathbf{Z}^+}$ 的一个双射，这与习题 10 已得结论“不存在 A 到 2^A 的双射”矛盾。$\therefore 2^{\mathbf{Z}^+}$ 是不可数集。

17. 举一个集合的例子，在它上定义一个二元关系，分别适合反身性、对称性、传递性中两个且仅适合两个。

解 设 $A=\mathbf{Z}$。

(1) 在 A 上定义二元关系 R_1 为通常数的整除，即

$$\forall a, b \in A,\ aRb \Longleftrightarrow a \mid b .$$

显然，R 适合且仅适合反射性、传递性，而不适合对称性。

(2) 定义二元关系 R_2：$\forall a, b \in A,\ aR_2b \Longleftrightarrow a=b$，$a \neq 0$。$R_2$ 适合传递性，对称性，但 R_2 不适合反身性，因为 $0R_2'0$。

(3) 定义二元关系 R_3：$\forall a, b \in A$，$aR_3b \Leftrightarrow a$ 与 b 不互素，或者 $a=b=\pm 1$。R_3 适合反身性，对称性，但 R_3 不适合传递性。

例如，取 $a=2$，$b=6$，$c=9$，则 aR_3b，bR_3c，aR'_3c。

18. 设 $A=\mathbf{Z}^+\times\mathbf{Z}^+$，规定 $(m, n)\leqslant(m', n') \Leftrightarrow m\leqslant m'$，$n\leqslant n'$，证明，$(A, \leqslant)$ 是偏序集，并且 A 有最小元。是否 A 的每一个非空子集都有最小元？极小元？

证 对任意 $(m, n)\in\mathbf{Z}^+\times\mathbf{Z}^+$，总有 $m\leqslant m$，$n\leqslant n$，故 $(m, n)\leqslant(m, n)$；设 (m_1, n_1)，(m_2, n_2) 是 A 中任意两个元素，满足 $(m_1, n_1)\leqslant(m_2, n_2)$ 且 $(m_2, n_2)\leqslant(m_1, n_1)$，则显然可得 $m_1=m_2$，$n_1=n_2$，$\therefore (m_1, n_1)=(m_2, n_2)$。又设 (m, n)，(l, k)，(s, t) 是 A 中任意三个元素，满足：$(m, n)\leqslant(l, \mathrm{k})$，$(l, \mathrm{k})\leqslant(s, t)$，则由 $m\leqslant l$，$l\leqslant s$ 得 $m\leqslant s$；$n\leqslant \mathrm{k}$，$\mathrm{k}\leqslant t$，得 $n\leqslant t$，$\therefore (m, n)\leqslant(s, t)$。

综上可见“$\leqslant$”满足反身性、反对称性及传递性，$\therefore (A, \leqslant)$ 是偏序集。

由于 $(1, 1)\in A$，且 $\forall(m, \mathrm{n})\in A$，均有 $(1, 1)\leqslant(m, n)$，故 $(1, 1)$ 是 A 的最小元。

A 的每一非空子集未必有最小元，例如 A 的子集 $\{(1,2), (2, 1)\}$。但 A 的每一非空子集都有极小元。

19. 设 $(A, \leqslant)$，$(B, \leqslant)$ 是两个偏序集，规定 $A\times B$ 的字典排法偏序关系为：$(a_1, b_1)\leqslant(a_2, b_2) \Leftrightarrow a_1<a_2$ 或 $a_1=a_2$，$b_1\leqslant b_2$，证明，$(A\times B, \leqslant)$ 是偏序集。若 $(A, \leqslant)$，$(B, \leqslant)$ 均为有序集，是否有：$(A\times B, \leqslant)$ 是有序集？

证 由于 A，B 皆偏序集，故对 $\forall(a, b)\in A\times B$，总有

$a=a$, $b \leqslant b$; $\therefore (a, b) \leqslant (a, b)$。设 (a, b), (c, d), (e,f) 是 $A\times B$中任意三个元满足 $(a, b)\leqslant(c, d)$, $(c, d)\leqslant(e,f)$, 于是由 $a \prec c$ 或 $a=c$, $b \leqslant d$; $c \prec e$ 或 $c=e$, $d \leqslant f$, 得到 $a \prec e$ 或 $a=e$, $b \leqslant f$, $\therefore (a, b) \leqslant (e, f)$。又若 (a,b), $(c, d)\in A\times B$, 且 $(a, b) \leqslant (c, d)$, $(c, d) \leqslant (a, b)$, 那么 $(a,b)\leqslant(c,d)\Rightarrow a \leqslant c$, $(c,d)\leqslant(a,b)\Rightarrow c \leqslant a$, $\therefore a=c$。再由 $(a, b) \leqslant (c, d)$, $a=c \Rightarrow b \leqslant d$; $(c, d) \leqslant (a, b)$, $c=a \Rightarrow d\leqslant b$。$\therefore b=d$, 故 $(a, b)=(c, d)$。综上可见 $(A\times B, \leqslant)$ 是一个偏序集。

假设 $(A, \leqslant)$, $(B, \leqslant)$ 是有序集，则 $(A\times B, \leqslant)$ 亦是有序集。事实上，任取 (a, b), $(c, d)\in(A\times B, \leqslant)$, $\therefore (A, \leqslant)$ 是有序集，则 $a \prec c$; $c \prec a$; $a=c$, 有且仅一种情况出现。

若 $a \prec c$, 则 $(a, b) \leqslant (c, d)$;

若 $c \prec a$, 则 $(c, d) \leqslant (a, b)$;

若 $a = c$, $\because (B, \leqslant)$ 是有序集, $\therefore$ 必有 $b \leqslant d$ 或 $d \leqslant b$。当 $b \leqslant d$ 时, $(a, b) \leqslant (c, d)$; 当 $d \leqslant b$ 时, $(c, d) \leqslant (a, b)$。总之 $\forall (a, b), (c, d)\in A\times B$, 均有 $(a,b) \leqslant (c,d)$ 或者 $(c,d)\leqslant(a,b)$。故 $(A\times B, \leqslant)$ 是一个有序集。

20。给出复数集C的两种顺序关系，使之成为有序集。与“复数无大小”的概念是否矛盾？

解 任一复数 $y=a+bi$ 决定一对有序实数 (a, b), $\forall a+bi, c+di\in \mathbf{C}$, 定义：$a+bi \leqslant_1 c+di \Leftrightarrow a \prec c$ 或 $a=c$, $b \leqslant d$, 其中“$\leqslant$”为通常数目的大小关系，由于 $(R, \leqslant)$ 是有序集，故由前题证明“$\leqslant_1$”成为C上的一个顺序关系，故使 $(\mathbf{C}, \leqslant_1)$ 成为有序集。

又任一复数都可以唯一地表成一个三角函数式：

$$z=r(\cos\alpha+i\sin\alpha)\qquad 0\leqslant\alpha<2\pi.$$

定义：$r_1(\cos\alpha+i\sin\alpha)\leqslant_2 r_2(\cos\beta+i\sin\beta)\Longleftrightarrow\alpha<\beta$ 或 $\alpha=\beta$，$r_1\leqslant r_2$，其中“$\leqslant$”为数目的大小关系。$\forall r_1(\cos\alpha+i\sin\alpha), r_2(\cos\beta+i\sin\beta)\in\mathbf{C}$

同样地可知，“$\leqslant_2$”是 $\mathbf{C}$ 上的一个顺序关系。于是 $(\mathbf{C},\leqslant_2)$ 成为有序集。

我们这里给出的 $\mathbf{C}$ 上的两种顺序关系与“复数无大小”是不矛盾的。通常的数的大小关系，不仅是一种顺序关系，而且还要满足阿基米德公理，乘法单调性。但我们在这里给出的两种顺序是不具有这些性质的：不能用来比较复数的大小。

21. 设 $(A,\leqslant)$ 是偏序集，对任意的 $a\in A$，命 $f(a)=\{x|x\in A, x\leqslant a\}$，证明，$f$ 是 A 到 2^A 的一个单射，并且，f 保持 $(A,\leqslant)$，$(2^A,\subseteq)$ 的偏序关系，即当 $a\leqslant b$ 时，有 $f(a)\subseteq f(b)$。

证 f 为映射显然，仅证 f 是单射。

设 $f(a)=S$，$f(b)=T$，且 $S=T$，由于 A 是偏序集，故 $a\leqslant a$，$\therefore a\in S$，但 $S=T$，$\therefore a\in T$，于是 $a\leqslant b$。同样可得，$b\leqslant a$。$\therefore a=b$，f 是 A 到 2^A 的一个单射。

若 $a\leqslant b$，则 $\forall x\in f(a)$，$x\leqslant a$。于是，$x\leqslant b$，$\therefore x\in f(b)$，即 $f(a)\subseteq f(b)$。

可见 f 保持 $(A,\leqslant)$，$(2^A,\subseteq)$ 的偏序关系。

22. 设 $(A,\leqslant)$ 是偏序集，T 是 $(2^A,\subseteq)$ 的一个子集，命 $\overline{T}=\{y|y\in 2^A, y\subseteq t, t\in T\}$，则 T 与 $\overline{T}$ 有相同的极大元。

证 根据 T 与 $\overline{T}$ 的定义，显然有 $T\subseteq\overline{T}$。若 x 是 T 的一个极大元，证明 x 是 $\overline{T}$ 的一个极大元。如若不然，则 $\exists y\in\overline{T}$，

使 $x \subset y$，由于 $y \in \overline{T}$，于是 $\exists t \in T$，满足 $y \subseteq t$，从而 $x \subset t$，这与 x 是 T 的极大元矛盾。这就证明了凡 T 的极大元，必是 $\overline{T}$ 的极大元。反之，若 y 是 $\overline{T}$ 的一个极大元，则由于 $y \in \overline{T}$，$\therefore$ $\exists t \in T$，使 $y \subseteq t$，但 $T \subseteq T$，$\therefore$ $t \in T$，故 $y = t \in T$，即 y 是 T 的极大元。这就证明了凡 $\overline{T}$ 的极大元必是 T 的极大元。

23*. 设 $(S, \leqslant)$ 是有序集，则 $(S, \leqslant)$ 是良序集的充要条件是：对任意 $a \in S$，$S_a = \{x \mid x \in S, x < a\}$ 是良序集。

证 若 $(S, \leqslant)$ 是良序集，则对任意 $a \in S$，S_a 必是良序集。这是因为 S_a 的任一非空子集必是 S 的非空子集，从而有最小元。

反之，若对任意 $a \in S$，S_a 是良序集，证明 $(S, \leqslant)$ 是良序集。设 M 是 S 的一个非空子集，任取 $m_0 \in M$，记 $M' = \{m \mid m \in M, m < m_0\}$。如果 m_0 不是 M 的最小元，M' 非空，$\because$ M' 是 S_{m_0} 的子集，$\therefore$ M' 有最小元 m'，易知 m' 也是 M 的最小元。从而证得 $(S, \leqslant)$ 是良序集。

✓ 24. 设 $(S, \leqslant)$ 是偏序集，如果 S 中每一非空子集 M 均有极大元，那么 S 中任意递增序列

$$a_1 < a_2 < \cdots < a_n < \cdots$$

必终止于有限项。并且，反之亦然。

证 设 $a_1 < a_2 < \cdots < a_n < \cdots$ 是 S 中任一无限递增序列，则 S 的非空子集 $\{a_1, a_2, \cdots, a_n, \cdots\}$ 没有极大元，与题没矛盾，故递增序列 $a_1 < a_2 < \cdots < a_n < \cdots$ 必终止于有限项。

反之，设 S 中任意递增序列终止于有限项，证明 S 的每一个非空子集皆有极大元。设 M 是 S 的任一非空子集。如果 M 无极大元，任取 $a_1 \in M$，$\exists a_2 \in M$，使 $a_1 < a_2$；同样 $\exists a_3 \in M$，

使 $a_2 \prec a_3$。以此类推，取定 $a_n \in M$ 后，因 a_n 不是 M 的极大元，故 $\exists a_{n+1} \in M$，使 $a_n \prec a_{n+1}$，这样就得到 S 中的一个无限递增序列

$$a_1 \prec a_2 \prec \cdots \prec a_n \prec a_{n+1} \prec \cdots$$

与 S 中任意递增序列终止于有限项矛盾。此矛盾表明 M 有极大元。

25*。设 $(\mathbf{Z}^+, \preccurlyeq)$ 是整数集关于整除关系作成的偏序集，证明，$(\mathbf{Z}^+, \preccurlyeq)$ 中存在无穷递增序列

$$a_1 \prec a_2 \prec \cdots \prec a_n \prec \cdots$$

$(\mathbf{Z}^+, \preccurlyeq)$ 中是否存在无穷递降序列。

证 对任意 $a \in \mathbf{Z}^+$，且 $a \neq 1$，有 $a \mid a^2$，$a^2 \mid a^3$，$\cdots$，$a^n \mid a^{n+1}$，$\cdots$，故有 $a \prec a^2 \prec a^3 \prec \cdots \prec a^n \prec a^{n+1} \prec \cdots$，即 $(\mathbf{Z}^+, \preccurlyeq)$ 中存在无穷递增序列。

在 $(\mathbf{Z}^+, \preccurlyeq)$ 中，不存在无穷递降序列。这是因为对任意 $a \in \mathbf{Z}^+$，a 的约数只有有限多个。

26。有人说，$\bigcap\limits_{i \in \phi} A_i = U$（见 § 1 末）不应该规定，而是可以证明，即：假定 $\bigcap\limits_{i \in \phi} A_i \neq U$，则 $\bigcap\limits_{i \in \phi} A_i \subset U$，于是，存在 $x \in U$，$x \notin \bigcap\limits_{i \in \phi} A_i$，从而，存在 $j \in \phi$，$x \notin A_j$，与 ϕ 是空集矛盾。此矛盾表明 $\bigcap\limits_{i \in \phi} A_i = U$。

你以为如何？

答：上面证明过程是错误的。“$x \notin \bigcap\limits_{i \in \phi} A_i$，从而存在 $j \in \phi$，$x \notin A_j$”，这是根据 $\bigcap\limits_{i \in I} A_i = \{x \mid \in U, \forall i \in I, x \in A_j\}$ 得到的，而后者作为定义，其前提条件要求 I 非空，故当 $I = \phi$ 时，不能应用该定义。

第二章 群

练习

§1 定义及基本性质

1. (a)设S表示平面上所有点的集合，任取$a,b\in S$，规定$a\circ b$表示线段a,b的中点，问“$\circ$”是不是S的一个二元运算？$(S,\circ)$是不是一个半群？(b)设S表示集合A的一切二元关系所成集合，证明S关于二元关系的合成“$\circ$”(见第一章 练习四、8题) 作成一个有单位元的半群。

解 (a) 依定义“$\circ$”是S的一个二元运算。由于“$\circ$”不满足结合律，所以$(S,\circ)$不是半群

证(b)：由第一章练习四、8题，S关于“$\circ$”是封闭的。今任取$(a,b)\in(R_1\circ R_2)\circ R_3$，则$\exists x\in A$，使$(a,x)\in(R_1\circ R_2)$，$(x,b)\in R_3$；再由$(a,x)\in R_1\circ R_2$，知$\exists y\in A$，使$(a,y)\in R_1$，$(y,x)\in R_2$，于是我们得到：$(a,y)\in R_1$，$(y,b)\in R_2\circ R_3$，从而推得$(a,b)\in R_1\circ(R_2\circ R_3)$，所以$(R_1\circ R_2)\circ R_3\subseteq R_1\circ(R_2\circ R_3)$同样可证$(R_1\circ R_2)\circ R_3\subseteq R_1\circ(R_2\circ R_3)$

$\therefore(R_1\circ R_2)\circ R_3=R_1\circ R_3)$，结合律成立。

令$e=\{(a,a)\mid\forall a\in A\}$，则$e\in S$，且对任意$R\in S$：$e\circ R=R\circ e=R$，$e$是$(S,\circ)$的单位元。所以$(S,\circ)$作成一个有单位元的半群。

2. 设$(S,\circ)$是一个半群，证明，$S\times S$对于下面规定的结合“$\circ$”作成一个半群：

$$(a_1,a_2)\circ(b_1,b_2)=(a_1\circ b_1,a_2\circ b_2)$$

当S有单位元时，证明，$S\times S$也有单位元；当S是群时，$S\times S$也是群。

证 设 $(S,\circ)$是半群，则对任意的$a,b\in S$，$a\circ b\in S$，故题设的结合法"$\circ$"为$S\times S$的一个二元运算。

任取 $(a_1,a_2),(b_1,b_2),(c_1,c_2)\in S\times S$。

则 $\left[(a_1,a_2)\circ(b_1,b_2)\right]\circ(c_1,c_2)=(a_1\circ b_1,a_2\circ b_2)\circ(c_1,c_2)$

$=\left((a_1\circ b_1)\circ c_1,(a_2\circ b_2)\circ c_2\right)$。$(a_1,a_2)\circ\left[(b_1,b_2)\circ(c_1,c_2)\right]=(a_1,a_2)\circ(b_1\circ c_1,b_2\circ c_2)=\left(a_1\circ(b_1\circ c_1),a_2\circ(b_2\circ c_2)\right)$。

由于$(S,\circ)$是半群，$(a_1\circ b_1)\circ c_1=a_1\circ(b_1\circ c_1)$。$(a_2\circ b_2)\circ c_2=a_2\circ(b_2\circ c_2)$，$\therefore\left[(a_1,a_2)\circ(b_1,b_2)\right]\circ(c_1,c_2)=(a_1,a_2)\circ\left[(b_1,b_2)\circ(c_1,c_2)\right]$，$S\times S$对"$\circ$"满足结合律，故$(S\times S,\circ)$是一个半群。

若$(S,\circ)$有单位元e，则$(e,e)\in(S\times S,\circ)$，且易知$(e,e)$是$(S\times S,\circ)$的单位元。

若$(S,\circ)$是群，则$(S\times S,\circ)$也是群。事实上，设a,b是$(S,\circ)$的任意元，它们有逆元a^{-1},b^{-1}，于是可知，(a^{-1},b^{-1})是(a,b)的逆元。

3．设$A=\{1,2\}$，写出半群$(A^A,\circ)$的乘法表。

解 A^A的元素为，e：$1\longmapsto1$，$2\longmapsto2$；a：$1\longmapsto2$，$2\longmapsto1$；b：$1\longmapsto1$，$2\longmapsto1$；c：$1\longmapsto2$，$2\longmapsto2$；

A^A的乘法表为

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	b	b	b
c	c	c	c	c

4. 设$A=\{1,2,3\}$，写出A^A的所有一一变换，并列出其乘法表。

解 A^A的一一变换为：$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$，$a=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$，$b=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ $c=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$，$d=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$，$f=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$

A^A的一一变换关于映射合成的乘法表为：

$\circ$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	f	d	c	b
b	b	d	e	f	a	c
c	c	f	d	e	b	a
d	d	b	c	a	f	e
f	f	c	a	b	e	d

5. 设S是一个半群，且左、右消去律成立，证明S是交

换半群的充要条件是，$\forall a,b\in S$：$(ab)^2=a^2b^2$。

证 若S是交换半群，则$\forall a,b\in S$，有$ab=ba$，$\therefore (ab)^2=(ab)(ab)=a(ba)b=a(ab)b=a^2b^2$。反之，$S$满足左、右消去律，且$\forall a,b\in S$：$(ab)^2=a^2b^2$。则 $(ab)(ab)=a^2b^2$，由左消去律成立得：$(ba)b=ab^2$，再由右消去律成立得：$ba=ab$ 所以S是交换半群。

6. 设S是一个有单位元的半群，$a,b\in S$，b是正则元，且$ab=ba$，证明 $ab^{-1}=b^{-1}a$。

证 设e是S的单位元，b为正则元，则$b^{-1}\in S$，由 $ab=ba$，有 $b^{-1}(ab)b^{-1}=b^{-1}(ba)b^{-1}$，即 $(b^{-1}a)(bb^{-1})=(b^{-1}b)(ab^{-1})$ $b^{-1}a=ab^{-1}$。

7*. 适合消去律的有限半群一定是群。

证 设 $G=\{a_1,a_2\cdots,a_n\}$ 是一个适合消去律的有限半群。任取$a\in G$，考虑集合$N=\{aa_1,aa_2,\cdots,aa_n\}$。由于$G$为半群，$\therefore aa_i\in G,i=1,2,\cdots n$，则$N\subseteq G$。再由$G$中消去律成立，可知$i\neq j$时$aa_i\neq aa_j$，又$G$为有限集，$\therefore N=G$。于是任一$b\in G$，$\exists a_i\in G$，使$aa_i=b$，即方程$ax=b$在$G$中有解，同样可证，方程$ya=b$在$G$中有解。 $\therefore G$是群。

8. 命$G=\{rm\mid r\in \mathbf{Z}\}$，$m$是取定的自然数，证明$(G,+)$是一个群。

证 “+”是G的二元运算为显然。设lm，km，tm是G中任意元，则$(lm+km)+tm=(l+k+t)m=lm+(k+t)m=lm+(km+tm)$。$G$对“+”满足结合律。

由于$o\in G$，且易知o是$(G,+)$的单位元。 $\forall km\in G$，有$(-k)m\in G$，$-km$是km在G中的逆元素。$(G,+)$是一个群。

9。$G=\{a+bi \mid a,b\in \mathbf{Z}, i$是虚数单位$\}$，证明，$(G,+)$是一个群。

证 “$+$”是G的一个二元运算为显然，且结合律成立，0是$(G,+)$的单位元；$\forall a+bi\in G$，有$(-a)+(-b)i\in G$，且易知$(-a)+(-b)i$是$a+bi$在G中的逆元素。$\therefore (G,+)$是一个群。

10。设G是一个群，$a,b,c\in G$，证明

$$xaxba=xbc$$

在G中有且仅有一个解。

证 $\because G$是群，$\therefore \forall a,b\in G$，有$a^{-1},b^{-1}\in G$。

命$x=a^{-1}bca^{-1}b^{-1}$，直接验证可知$a^{-1}bca^{-1}b^{-1}$是方程$xaxba=xbc$的一个解。反之，若x_0是方程$xaxba=xbc$在G中的一个解，则由$x_0ax_0ba=x_0bc\Longrightarrow ax_0ba=bc\Longrightarrow x_0=a^{-1}bca^{-1}b^{-1}$。$\therefore xaxba=xbc$在$G$中有且仅有一个解。

11。设G是一个群，$x,y\in G$，证明

$$(x^{-1}yx)^k=x^{-1}yx\Longleftrightarrow y^k=y。$$

证 $(x^{-1}yx)^k=(x^{-1}yx)\cdot(x^{-1}yx)\cdots\cdots(x^{-1}yx)=x^{-1}yx\cdot$由群中乘法消去律成立得 $x^{-1}y^kx=x^{-1}yx\Longleftrightarrow y^k=y$。

12。设G是一个群，u是在G中取定的元，在G中规定结合法“$\circ$”。

$$a\circ b=au^{-1}b$$

证明，$(G,\circ)$是一个群。

证 “$\circ$”是G中二元运算为显然。设a,b,c为G中任意元。则 $(a\circ b)\circ c=(au^{-1}b)\circ c=(au^{-1}b)u^{-1}c=au^{-1}(bu^{-1}c)$

$=au^{-1}(b\circ c)=a\circ(b\circ c)$，“$\circ$”满足结合律。

易知，u是$(G,\circ)$的单位元。对$\forall a\in G$，直接验证可知，

$ua^{-1}u$是a的逆元，$\therefore (G,\circ)$是一个群.

13. 设$G=(\mathbf{z},+)$，对G规定结合法"$\circ$"

$$a\circ b=a+b-2$$

证明 $(G,\circ)$是一个群.

证 "$\circ$"为G的一个二元运算显然，设a,b,c是G中任意三个元，$(a\circ b)\circ c=(a+b-2)\circ c=(a+b-2+c)-2$
$=a+(b-2+c)-2=a\circ(b+c-2)=a\circ(b\circ c)$. G中结合法"$\circ$"满足结合律. 又$2\in G$，易知2是$(G,\circ)$的单位元. $\forall a\in G$，直接验算得$4-a$是a在$(G,\circ)$中的逆元. $\therefore (G,\circ)$是一个群.

14. 在例9中，写出G的乘法表，并找出G的所有子群.

解 G含有六个元素I,R,R^2,A,AR,AR^2. 其中R表示△依顺时针方向旋转120°，A表示以△的顶点垂直于底的垂线的翻折.

G的乘法表为：

$\cdot$	I	R	R^2	A	AR	AR^2
I	I	R	R^2	A	AR	AR^2
R	R	R^2	I	AR	AR^2	A
R^2	R^2	I	R	AR^2	A	AR
A	A	AR	AR^2	I	R	R^2
AR	AR	AR^2	A	R	R^2	I
AR^2	AR^2	A	AR	R^2	I	R

注意到$AR=RA$. 由乘法表得看出G的所有子群为：
$\{I\}$ $\{I,R,R^2\}$ $\{I,A\}$ G.

15. 在例8中，证明 $H=\{f_{1,b}\mid b\in\mathbf{Q}\}$是$G$的子群.

证 $\because f_{1,0}\in H,\therefore H$非空.

任取 $f_{1,b}$, $f_{1,c}\in H$, 则易知$f_{1,b}\circ f_{1,c}=f_{1,b+c}\in H$。

$\forall f_{1,b}\in H$， $f_{1,b}$在G中的逆元$f_{1,-b}\in H$， 所以H是G的子群。

16*. 设G是一个群，S是G的子群，命$N(S)=\{x\mid x\in G, xSx^{-1}=S\}$则$N(S)$是$G$的子群。$N(S)$叫做$S$的正规化子。$S$的中心化子$C(S)$与$N(S)$有何不同?

证 显然对$\forall x\in S$ $xSx^{-1}=S$。 $\therefore S\subseteq N(S)$, $N(S)$非空。任取$x,y\in N(S)$，则$(xy)S(xy)^{-1}=x(ySy)x^{-1}=xSx^{-1}=S$。 $\therefore xy\in N(S)$。

$\forall x\in N(S)$， $\because$ $S=xSx^{-1}$， $\therefore x^{-1}Sx=x^{-1}(xSx^{-1})x=S$， $\therefore x^{-1}\in N(S)$。 $N(S)$是G的子群。

S的中心化子 $C(S)=\{x\mid x\in G,$ $\forall a\in S, xax^{-1}=a\}$ $\therefore C(S)\subseteq N(S)$， 但$N(S)$中元未必属于$C(S)$。

17. 设$a\in G$，则a与a^{-1}有相同的周期。

证 设$a\in G$，a的周期为m，则$a^m=e$，e是G的单位元。于是$(a^{-1})^m=(a^m)^{-1}=e^{-1}=e$。 a^{-1}的周期$n\mid m$。同样当a^{-1}的周期为n时，可证a的周期$m\mid n$。由此可知，若a与a^{-1}中有一个的周期为有限，则另一个的周期也为有限，且两个元的周期相等；若a与a^{-1}中有一个的周期为无限，则另一个的周期也为无限。

18. $G=\{2^m3^n\mid m,n\in\mathbf{Z}\}$，证明，$G$对于数目乘法作成群。

证 设2^m3^n，$2^l3^k\in G, m, n, l, k\in\mathbf{Z}$，则 $(2^m3^n)\cdot(2^l3^k)=2^{m+l}3^{n+k}\in G$，$G$对乘法封闭。结合律显然成立。

易知 $1=2^0\cdot3^0\in G$，是$(G,\cdot)$的单位元。

任$-2^m3^n\in G$，它在$(G,\cdot)$中有逆元$2^{-m}3^{-n}$。所以$(G,\cdot)$

是一个群。

19。 设$(S,\circ)$是一个有单位元e的半群。$G=S^S$，对G规定二元运算。 $f,g\in G$，$f\cdot g$：$x\longmapsto f(x)\circ g(x)$。
证明，$(G,\cdot)$是一个有单位元的半羣。

证 任取$f,g\in G$，则$f(x),g(x),f(x)\circ g(x)\in S$。故$f\cdot g\in G$。

今取G中任意元g，f，h，由$(S,\circ)$是半群可知
$(f\cdot g)\cdot h=f\cdot(g\cdot h)$，所以$(G,\cdot)$满足结合律。

显然，S的变换φ：$x\longmapsto e$。$\forall x\in S$，是$(G,\cdot)$的单位元。所以$(G,\cdot)$是一个有单位元的半群。

✓20。设S是一个半群，$G=\{f_a\mid a\in S,\ f_a:\ x\longmapsto ax\}$，
证明 $(G,\circ)$是$(S^S,\circ)$的一个子半群。G与S^S的单位元是否相同？

证 设 $f_a,f_b\in G$，则对所有$x\in S$，有 $f_a\circ f_b$：$x\longmapsto abx$。
即 $f_a\circ f_b=f_{ab}\in G$。

显然 $G\subseteq S^S$，所以$(G,\circ)$是$(S^S,\circ)$的一个子半群。

S^S的单位元为1_S ：$a\longmapsto a$ $\forall a\in S$ 若S有左单位之e，则$1_S=f_e\in G$，且是G的单位元；若S无左单位元，则 $1_S\in G$，此时，即使G有单位元也与1_S不同。

21。设 $G=(\mathbb{Z},+)$是整数加法群，$S=\{2,3\}$，向S生成的子群$(S)=?$ 命$S_1=\{3,5\}$，$(S_1)=?$

解 $\because 1=2\cdot 2-3\cdot 1\in(S)$，

$\therefore$ $(S)=G$。

同理 $1=3\cdot 2-5\cdot 1\ \in(S_1)$，$\therefore(S_1)=G$。

22。设G是一个群，G不是交换群，$[G:1]>2$，证明G中存在a,b：$ab=ba$，且a,b都不是单位元。

证 根据例17，若G除单位元以外的每一个元的阶都为

2，则G是交换群。故由G不是交换群知，G中必存在阶不等于2的非单位元a，令$b=a^{-1}\in G$，显然，a,b皆不是单位元，$b\neq a$，且$ab=ba$。

23。设S是任意集合，$(G,+)$是一个加群，命$A=G^S$，即A是S到G的所有映射所成集合，对A规定二元运算：$f,g\in A$，规定$f+g$：$x\longmapsto f(x)+g(x)$，证明$(A,+)$作成一个加群。

证 任取$f,g\in A$，则由$(G,+)$是加群，可知：$f(x)+g(x)\in G$，$\forall x\in S$，即$f+g\in A$，且$f+g=g+f$。

再由G是群，可知：

$$\Big(f(x)+g(x)\Big)+h(x)=f(x)+\Big(g(x)+h(x)\Big),\quad \forall x\in S,$$

即$(f+g)+h=f+(g+h)$。 $(A,+)$满足结合律。

易知，S到G的映射φ：$x\longmapsto o$ $\forall x\in S$，o是$(G,+)$的零元，是$(A,+)$的单位元。

且，$\forall f\in A$，映射 $-f$：$x\longmapsto -f(x)$，$\forall x\in S$，是f的逆元。

所以$(A,+)$是一个加群。

§2 循环群与变换群，群的同构

1。证明循环群是可换群。

证 设$G=(a)$为循环群，$\forall x\in G$，有$x=a^m$，$m\in Z$。

任取$x,y\in G$，设$x=a^m$，$y=a^k$，$m,k\in Z$，

则 $xy=a^m\cdot a^k=a^k\cdot a^m=yx$。$\therefore G$为可换群。

2。设G是6阶循环群，找出G的一切生成元，并找出G的所有子群。

解 设$G=(a)=\{e=a^0,a^1,a^2,a^3,a^4,a^5\}$为6阶循环

群。

G有两个生成元a, a^5， G的子群有四个：

$\{e\}$， $\{e, a^3\}$， $\{e, a^2, a^4\}$， $\{e, a, a^2, a^3, a^4, a^5\}$。

3。 找出S_3的所有子群。

解 $S_3 = \{(1), (12), (13), (23), (123), (132)\}$ 其子群为：$H_1 = \{(1)\}$， $H_2 = \{(1), (12)\}$， $H_3 = \{(1), (13)\}$， $H_4 = \{(1), (23)\}$， $H_5 = \{(1), (123), (132)\}$， $H_6 = S_3$。

4。证明整数加群$\mathbf{Z}_+$与偶数加群同构。

证 命 σ $\mathbf{Z} \to E$，E为全体偶数集。

$$n \longmapsto 2n \quad \forall n \in \mathbf{Z}$$

显然，σ是$\mathbf{Z}$到E点的一一映射。

任取$n_1, n_2 \in \mathbf{Z}$，则有$\sigma(n_1 + n_2) = 2(n_1 + n_2) = 2n_1 + 2n_2 = \sigma(n_1) + \sigma(n_2)$。 $\therefore \sigma$是$\mathbf{Z}+$到 $(E, +)$的同构映射，故$\mathbf{Z}_+ \cong (E, +)$。

5。写出A_4的所有元素。

解 A_4的所有元素为： (1) ，(12)(34)，(13)(24)，(14)(23)，(123)，(124)，(132)，(142)，(143)，(234)，(243)，(134)，

6。设$B_4 = \{e, a, b, ab\}$，乘法表为

$\circ$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

所定义的群叫$KLein$ 四元群，或简称四元群。

(1)找出B_4的所有子群。 (2)找出与 B_4同构的S_4的子群。

解 (1)由乘法表可知"e"为 B_4的单位元，a,ab,b皆为二阶元，故它们的逆元各为其自身。于是B_4的子群有：

$\{e\}$, $\{e,a\}$, $\{e,b\}$, $\{e,ab\}$, $\{e,a,b,ab\}$

(2) 取S_4 的一个子集$H=\{(1),(12),(34),(12)(34)\}$做$B_4$到$H$上的双射 f: $e\longmapsto(1)$, $a\longmapsto(12)$,$b\longmapsto(34)$, $b\longmapsto(12)(34)$。容易验证 f 保持运算，故H是S_4的子群，且 $B_4\cong H$。

7。证明S_4有生成元素 $\{(12),(13),(14)\}$

此题系下一题的特例，证法相同：

8。证明 S_n有生成元素$\{(12),(13)\cdots,(1n)\}$

证 S_n中每一个元都可表成不相交的轮换的乘积，而对每一个轮换又都可以表成若干对换之积：$(l_1l_2\cdots l_k)=(l_1l_k)(l_1l_{k-1})\cdots(l_1l_3)(l_1l_2)$。故$S_n$由一切对换$(lj)$生成。$1\leqslant l,\ j\leqslant n$。但 $(lj)=(1l)(1j)(1l)$，所以S_n由(12)，(13)，$\cdots$，$(1n)$生成。

9。证明 S_4有生成元素$\{(1234),(12)\}$。

证 设$H=\big((1234),(12)\big)$是由(1234)，(12)生成的S_4的子群。

$\because$ $(1234)^{-1}=(1432)\in H$。 $\therefore$ $(1432)(12)(1234)=(14)\in H$。 又 $(1234)(12)(1432)=(23)\in H$，$\therefore$ $(23)(14)(1234)=(13)\in H$。于是由第7题结果，$H=S_4$。

10。证明 S_n有生成元素$\{(1234\cdots n),(12)\}$。

证 对n用数学归纳法。

设 $H=\big((12\cdots n),(12)\big)$，$H\subseteq S_n$。当$n=2$时结论显然成立。假设$n-1$时，结论成立。即$S_{n-1}$有生成元素$\{(12\cdots n-1),12)\}$。由第8题知

$$\big((12\cdots n-1),\ (12)\big)=\big((12),(13),\cdots,(1n-1)\big).$$

现在考虑n的情形。

$\because\ (12\cdots n)^{-1}=(12\cdots n)^{n-1}=(1n\ \ n-1\cdots 2)\in H.$

$(12)(12\cdots n)=(23\cdots n)\in H.$

$(1n\ \ n-1\cdots 32)(23\cdots n)=(1n)\in H.$

又$(1n)(12\cdots n)=(12\cdots n-1)\in H.$

因此，由$\big((12\cdots n-1),(12)\big)\subseteq H\Rightarrow\big((12),\cdots,(1n-1)\big)\subseteq H$

从而$\big((12),\cdots,(1n-1),(1n)\big)\subseteq H$，由第8题结果$H=S_n$。

11. 证明，无限循环群的子群除$\{e\}$外均为无限循环群。

证 设$G=(a)$为无限循环群，设H是G的任一不等于单位元群的子群。则H亦为循环群。若H为有限阶循环群，不妨设H由$n>1$阶元b生成。由于$b\in H\subseteq G$。故$\exists m\in\mathbf{z}$，使$b=a^m$。$\because b^n=e$。$\therefore (a^m)^n=a^{mn}=e$，这与$G$为无限循环群矛盾，所以$H$为无限循环群。

12. 设$A=(a^s)$，$B=(a^t)$是$G=(a)$的两个子群，证明。$A\cap B=(a^d)$，此处d是s,t的最小公倍数。

证 $\forall x\in A\cap B$，$\exists m\in\mathbf{z}$，使$x=a^m$。由于$a^m\in A\Longrightarrow s\mid m$，$a^m\in B\Longrightarrow t\mid m$，所以$d\mid m$，$x=a^m=a^{dk}\in(a^d)$ 即$A\cap B\subseteq(a^d)$另一方面显然有$(a^d)\subseteq A$，$(a^d)\subseteq B$，$\therefore(a^d)\subseteq A\cap B$。从而证得 $A\cap B=(a^d)$。

13. 设f是集合$S=\{1,2,\cdots,m\}$上的一个置换，规定S中元素的一个二元关系$\sim$：$a\sim b\Longleftrightarrow\exists n\in\mathbf{Z}$，$f^n(a)=b$，证明，$\sim$是$S$的一个等价关系，称$S/\sim$的元为$f$的轨道。设$S$含有10个元，$f=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\3&4&2&10&6&5&8&9&7&1\end{pmatrix}$，求$f$的轨道。

证 把f表成不相交的循环之积，对任一$a\in S$。若a所在循环的长度为k，则$f^k(a)=a$，$\therefore a\sim a$；

设a,b是S中任意二元，且$a\sim b$，即$\exists n\in\mathbf{Z}$，使$f^n(a)=b$，于是，显然有$f^{-n}(b)=a$，$\therefore b\sim a$；设a,b,c是S中任意三个元，满足$a\sim b,b\sim c$，即$\exists n_1,n_2\in\mathbf{Z}$，使$f^{n_1}(a)=b$，

$f^{n_2}(b)=c$，从而$f^{n_1n_2}(a)=c$。$\therefore a\sim b$。

故“$\sim$”是S的一个等价关系。

如题设$f=(1\,3\,2\,4\,10)(5\,6)(7\,8\,9)$。容易看出，将$f$写成不相交的循环积，当且仅当同一循环因子中的数码是等价的，故f的轨道有三个：

$S/\sim$：$\{1,3,2,4,10\}$，$\{5,6\}$，$\{7,8,9\}$。

§3 不变子群与商群

1. 设H是G的子群，$a,b\in G$。证明，以下六个条件是等价的：

1) $b^{-1}a\in H$，　2) $a^{-1}b\in H$，　3) $b\in aH$，

4) $a\in bH$，　5) $aH=bH$，　6) $aH\cap bH\neq\phi$。

证 设H是G的子群，$a,b\in H$。

则$b^{-1}a\in H\Longrightarrow(b^{-1}a)^{-1}\in H$　即$a^{-1}b\in H\Rightarrow\exists h\in H$，使$a^{-1}b=h$　即　$b=ah$，$b\in aH\Rightarrow b=ah$，$a=bh^{-1}\in bH\Rightarrow$

$aH\subseteq bH$和$b=ah, bH\subseteq aH\Rightarrow aH=bH\Rightarrow$至少有$a$，$b\in aH\cap bH$，$\therefore aH\cap bH\neq\phi$

这就证明了 1)⇒ 2)⇒ 3)⇒ 4)⇒ 5)⇒ 6)

若 $aH\cap bH\neq\phi$，则可设$x\in aH\cap bH$，于是$x=ah_1=bh_2$，$h_1, h_2\in H$，⇒ $b^{-1}a=h_2h_1^{-1}\in H$，这就证明了6)⇒1)。

故题中六个条件是等价的。

2. 写出A_4关于$H=\{(1),(12)(34),(13)(24),(14)(32)\}$的左陪集分解以及右陪集分解。$H$是不是$A_4$的不变子群？

解 $(1)H=H$，$(12)H=\{(12),(34),(1423),(2413)\}$，$(13)H=\{(13),(24),(1234),(1432)\}$，所以$A_4$关于$H$的左陪集分解为：$A_4=H\cup(12)H\cup(13)H$，

同样可得A_4的互异右陪集为：$H(1)=H$，$H(12)=\{(12),(34),(1423),(2413)\}$，$H(13)=\{(13),(24),(1234),(1432)\}$所以$A_4$关于$H$的右陪集分解为：$A_4=H\cup H(12)\cup H(13)$。显然$H$是$A_4$的不变于群。

3. 对于例3的G，具体描述G/H的运算，$\frac{1}{2}+H$，与$\frac{5}{7}+H$，的和是什么？证明，G/H中每一元的周期都为有限。G/H是不是有限群？

解 对G/H中任意元$\frac{q}{p}+H$，$\frac{s}{r}+H$，其中$\frac{q}{p}$，$\frac{s}{r}$为正的既约真分数或零，$\left(\frac{q}{p}+H\right)+\left(\frac{s}{r}+H\right)=\frac{f}{e}+H$

如果$\frac{q}{p}+\frac{s}{r}\equiv\frac{f}{e}(mod\,H)$，且$\frac{f}{e}$为正的既约真分数或零。

$$\left(\frac{1}{2}+H\right)+\left(\frac{5}{7}+H\right)=\frac{17}{14}+H=\frac{3}{14}+H.$$

$(G/H,+)$的单位元为H。对G/H中任一非单位元$\frac{q}{p}+H$，其中$\frac{q}{p}$为正的既约真分数。$p\cdot\left(\frac{q}{p}+H\right)=H$，

$\therefore$ $\frac{q}{p}+H$的周期为 p。

同样，由例3知，G/H中含有无限多元素，故G/H为无限群。

4．对于例10的G，决定G关于K的左陪集分解。

解 例10中的 $G=\left\{\begin{pmatrix}r & s\\ 0 & 1\end{pmatrix}\middle|\ r,s\in\mathbf{Q},r\neq 0\right\}$，

$K=\left\{\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}\middle|\ n\in\mathbf{Z}\right\}$。 $\forall\begin{pmatrix}r & s\\ 0 & 1\end{pmatrix}\in G$，

$\begin{pmatrix}r & s\\ 0 & 1\end{pmatrix}K=\left\{\begin{pmatrix}r & rn+s\\ 0 & 1\end{pmatrix}\middle|\ n\in\mathbf{Z}\right\}$。容易看出，若$r_1\neq r_2$，则$\begin{pmatrix}r_1 & s\\ 0 & 1\end{pmatrix}$，$\begin{pmatrix}r_2 & t\\ 0 & 1\end{pmatrix}\in K$的同一左陪集，这里$s,t\in\mathbf{Q}$。取定$r\neq 0\in\mathbf{Q}$，若$s_1,s_2\in\mathbf{Q},s_1\neq s_2,0\leqslant s_1,s_2<r$，则$\begin{pmatrix}r & s_1\\ 0 & 1\end{pmatrix}$，$\begin{pmatrix}r & s_2\\ 0 & 1\end{pmatrix}$也不属于$K$的同一左陪集。这是因为，当$0\leqslant s_1<r$时，$\forall n\in\mathbf{Z}^*,0\leqslant rn+s_1<r$不成立，$\therefore\forall n\in\mathbf{Z}$，$rn+s_1\neq s_2$。

另一方面，对任一$\begin{pmatrix}r & t\\ 0 & 1\end{pmatrix}\in G,\exists k\in\mathbf{Z}$，使$kr\leqslant t<(k+1)r$，

命 $s=t-kr$，则 $0\leqslant s<r$。

于是$\begin{pmatrix}r & s\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}=\begin{pmatrix}r & t\\ 0 & 1\end{pmatrix}$，即$\begin{pmatrix}r & t\\ 0 & 1\end{pmatrix}\in\begin{pmatrix}r & t\\ 0 & 1\end{pmatrix}K$，

故$\left\{\begin{pmatrix}r & s\\ 0 & 1\end{pmatrix}K\middle|\ r\in\mathbf{Q}^*,s\in\mathbf{Q},0\leqslant s<r\right\}$给出$G$关于$K$的所有左陪集。

5. 设H是G的不变子群，a,b属于H的同一陪集，记为$a\equiv b(mod\ H)$，称作a,b关于模H同余(或合同)。证明，若$a\equiv b(mod\ H)$，$c\equiv d(mod\ H)$，则$ac\equiv bd(mod\ H)$

证 由$a\equiv b(mod\ H)\Rightarrow b\in aH, c\equiv d(mod\ H)\Rightarrow d\in cH$。$\therefore bd\in aH\cdot cH=acH$，$ac\equiv bd(mod\ H)$。

6. 在上题中，H是G的子群，未必是不变子群，仍用符号$a\equiv b(mod\ H)$表示a,b属于H的同一左陪集，是否还有$a\equiv b$，$c\equiv d\Rightarrow ac\equiv bd(mod\ H)$？$H$是不变子群这一条件在哪一步起作用？

解 若H仅是G的子群，未必是不变子群，则当$a\equiv b$，$c\equiv d$一般不能推出$ac\equiv bd\ (mod\ H)$。例如，取$G=S_3$，$H=\{(1),(1,2)\}$，则$(13)\equiv(123)\ (mod\ H)$，$(23)\equiv(132)\ (mod\ H)$，$(13)(23)=(132)$，$(123)(132)=(1)$，但$(132)\not\equiv(1)(mod\ H)$。

H是G的不变子群这一条件在于保证，$\forall x,y\in G$，

$xH\cdot yH=xyH$。

7*. 设A,B都是G的不变子群，则$AB,A\cap B$都是G的不变子群。

证 根据定理5，AB是G的子群，$A\cap B$显然是G的子群。

对$\forall x\in G, x(A\cap B)x^{-1}\subseteq(xAx^{-1})\cap(xBx^{-1})=A\cap B$。

$x(AB)x^{-1}=(xAx^{-1})(xBx^{-1})=AB$。

$\therefore AB,A\cap B$都是G的不变子群。

8. 设A,B是G的子群，则AB是G的子群的充分必要条件是：$AB=BA$。

证 设AB是G的子群，则$\forall ab\in AB$，

有$(ab)^{-1}=b^{-1}a^{-1}\in AB$. 但$b^{-1}a^{-1}\in BA$, $\therefore$ $AB\subseteq BA$. 同样$BA\subseteq AB$. $\therefore AB=BA$. 反之, $AB=BA$, 任取$ab\in AB$, $a\in A, b\in B$, 有$(ab)^{-1}=b^{-1}a^{-1}\in BA=AB$, $\forall ab, a'b'\in AB$, $a, a'\in A, b, b'\in B$, $\because ba'\in BA=AB$, $\therefore$ $\exists a''\in A, b''\in B$, 使$ba'=a''b''$, 于是$(ab)(a'b')=a(ba')b'=a(a''b'')b'=(aa'')(b''b')\in AB$. $\therefore AB$是G的子群.

9. 设A, B, C是G的子集(群), 下面命题中哪些是正确的? 给出证明或举出反例.

1) $A\cup B=A\cup C\Rightarrow B=C$;

2) $A\cap B=A\cap C\Rightarrow B=C$.

3) $AB=AC\Rightarrow B=C$; 4) $A(B\cup C)=AB\cup AC$.

解 命题1)不正确. 例如取$G=S_3$, $A=S_3$, $B=\{(1)\}$. $C=\{(1),(12)\}$. 显然$A\cup B=A\cup C=S_3$, 但$B\neq C$.

命题2)不正确. 例如取$G=S_3$, $A=\{(1),(12)\}$ $B=\{(1),(13)\}$. $C=\{(1),(23)\}$ 显然$A\cap B=A\cap C=\{(1)\}$. 但$B\neq C$.

命题3)不正确. 例如取$G=S_3$, $A=S_3$, $B=\{(1),(12),$ $C=\{(1)\}$, 显然$AB=AC=G$, 但$B\neq C$.

命题4)是正确的. 因为$\forall x\in A(B\cup C)$, 有$x=ay$, 其中$a\in A$. $y\in B$或$y\in C$. 若$y\in B$则$x=ay\in AB$, 如果$y\in C$, 则$x=ay\in AC$, 总之$x\in AB\cup AC$; 反之, $\forall x\in AB\cup AC$, 则$x\in AB$或$x\in AC$, 若$x\in AB$, 则有$x=ab, a\in A, b\in B$, $\therefore b\in B\cup C$, $\because$ $x=ab\in A(B\cup C)$, 同理由$x\in AC$也可得$x\in A(B\cup C)$. 综上所述, 证得 $A(B\cup C)=AB\cup AC$.

10. 设A, B是G的子群, C表示$A\cup B$生成的子群, 证明$[C:A]\geqslant[B:A\cap B]$.

证 设B关于$A\cap B$的所有不同左陪集为：$x_i(A\cap B)$，$i\in I$。这里$x_i\in B$，且当$x_i\neq x_j$时，$x_i^{-1}x_j\notin A\cap B$。我们证明当$x_i\neq x_j$时，$x_iA\neq x_jA$。否则，由$x_iA=x_jA\Rightarrow x_i^{-1}x_j\in A$，又$x_i^{-1}x_j\in B$，故$x_i^{-1}x_j\in A\cap B=D$，引出矛盾，所以，$x_iA$，$i\in I$，是$C$关于$A$的不同左陪集，从而证得$C$关于$A$的左陪集数不小于$B$关于$A\cap B$的左陪集数。即$[C:A]\geqslant[B:A\cap B]$。

11。设A,B是G的子群，$(|A|,|B|)=1$，

则 $|AB|=|A|\cdot|B|$。

证 设A,B是G的子群，则$A\cap B$是A,B的子群，因此，$|A\cap B|\,\big|\,|A|$，$|A\cap B|\,\big|\,|B|$，$\Rightarrow|A\cap B|\,\big|\,(|A|,|B|)=1$。$\Rightarrow|A\cap B|=1$，即 $A\cap B=\{e\}$。根据定理6推论得

$|AB|=|A|\cdot|B|$。

12 设A是G的子群，$N(A)$表示A的正规化子（见练习一，16题）证明，A是G的不变子群的充要条件是：$G=N(A)$。

证 根据正规化子的定义：$N(A)=\{x|x\in G,xAx^{-1}=A\}$ 因此，$G=N(A)\Longleftrightarrow\forall x\in G.\ xAx^{-1}=A\Longleftrightarrow A\lhd G$。

13。设G是整数加群，$H=\{mk|k\in z\}$，商群G/H含有哪些元？G/H的零元是什么？G/H中运算是怎样的？

解 $G/H=\{\overline{0},\overline{1},\cdots,m-1\}$，其中$\overline{r}=\{mk+r|k\in z\}$。$r=0,1,\cdots,m-1$。$G/H$的零元是$\overline{0}=H$。

设 $\overline{x}$，$\overline{y}\in G/H$，则$\overline{x}$，$\overline{y}$的和为：$\overline{x}+\overline{y}=\overline{x+y}=\overline{j}$。其中$o\leqslant x,y\leq m-1$，$o\leqslant j\leq m-1$，且$j\equiv x+y(m\circ dm)$

14。设G是循环群，A,B,C是G的子群，

证明 $A\cap\big((B\cup C)\big)=\big((A\cap B)\cup(A\cap C)\big)$，即$A$与$B\cup C$生成的子群的交等于$A\cap B$，$A\cap C$所生成的子群。以$B_4$为例，

说明上述命题对非循环群不成立。

证 设$G=(a)$， $A=(a^m)$， $B=(a^k)$， $C=(a^t)$ 其中$m,k,t\in Z^+$。

i)首先可证：若 $(k,t)=d$,则$((a^k)\cup(a^t))=(a^d)$ 事实上，由$(a^t)\subseteq(a^d),(a^k)\subseteq(a^d)\Rightarrow((a^k)\cup(a^t))\subseteq(a^d)$ 另一方面，$\exists\ n_1,n_2\in Z$，使 $n_1t+n_2k=d$。$\therefore$ $a^d\in((a^k)\cup(a^t))$ 从而$(a^d)\subseteq((a^k)\cup(a^t))$。$\therefore$ $((a^k)\cup(a^t))=(a^d)$

ii) 若$[m,d]=q$， $[m,k]=q_1$ $[m,t]=q_2$。
则由练习2，12题得$(a^m)\cap(a^d)=(a^q),(a^m)\cap(a^k)=(a^{q_1})$ $(a^m)\cap(a^t)=(a^{q_2})$于是由*i*)。 $((A\cap B)\cup(A\cap C))=((a^{q1})\cup(a^{q2}))=(a^{q'})$这里$q=(q_1,q_2)$。这样，我们已经证得：$A\cap((B\cap C))=(a^q)$， $((A\cap B)\cup(A\cap C))=(a^{q'})$

iii) 下面证明$q=q'$。

设 $m=p_1^{\alpha 1}\cdots p_r^{\alpha r}$， $k=p_1^{\gamma 1}\cdots p_r^{\gamma r}$， $t=p_1^{\beta 1}\cdots p_r^{\beta r}$ 其中$p_1,\cdots,p_r$为互不相同的素数，α_i，β_i，γ_i 为非负整数，于是$[m,\ k]=\prod_{i=1}^{r}p_i^{max(\alpha_i,\gamma_i)}$， $[m,t]=\prod_{i=1}^{r}p_i^{max(\alpha_i,\beta_i)}$

$$(t,k)=\prod_{i=1}^{r}p_i^{min(\beta_i,\gamma_i)}$$

所以 $q=[m,d]=[m,(t,k)]=\prod_{i=1}^{r}p_i^{max(\alpha_i,min(\beta_i,\gamma_i))}$

$$q'=([m,k],[m,t])=\prod_{i=1}^{r}p_i^{min(max(\alpha_i,\beta_i),max(\alpha_i,\gamma_i))}$$

但明显的 $max(\alpha_i,min(\beta_i,\gamma_i))=min(max(\alpha_i,\beta_i),max(\alpha_i,\gamma_i))$

故 $q=q'$

综上可知$A\cap((B\cup C))=((A\cap B)\cup(A\cap C))$。

再看 $B_4=\{e,a,b,ab\}$。令$A=\{e,a\}$。$B=\{e,b\}$。$C=\{e,ab\}$。 则 $A\cap((B\cup C))=A$。

$((A\cap B)\cup(A\cap C))=\{e\}\neq A\cap((B\cup C))$。所以上述命题对非循环群不成立。

15* 设A,B是G的子群，C是由$A\cup B$生成的子群，若B是C的不变子群，则$C=AB$。

证 因为B是C的不变子群，A是C的子群，由定理5，AB是C的子群，又$\because A\cup B\subseteq AB$。$\therefore$ AB是包含由$A\cup B$生成的子群C，故$C=AB$。

16。设H_1,H_2,N是G的不变子群，且$H_1\subset H_2$则H_1N是H_2N的不变子群。

证 由第7题，H_1N,H_2N皆是G的不变子群。

$\because$ $H_1\subset H_2$， $\therefore$ $H_1N\subset H_2N$，于是由H_1N是G的不变子群，得H_1N是H_2N的不变子群。

17。设G含8个元：$\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}$，$\pm\begin{pmatrix}1&0\\0&-i\end{pmatrix}$，$\pm\begin{pmatrix}0&1\\-1&0\end{pmatrix}$，$\pm\begin{pmatrix}0&1\\i&0\end{pmatrix}$。$(i^2=-1)$，证明，$G$关于方阵乘法作成一个群，并且$G$的每一个子群都是不变子群。

证 记 $e=\begin{pmatrix}1&0\\0&1\end{pmatrix}$， $a_1=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$， $a_2=\begin{pmatrix}1&0\\0&-i\end{pmatrix}$

$a_3=\begin{pmatrix}-1&0\\0&i\end{pmatrix}$， $a_4=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$， $a_5=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$

$a_6=\begin{pmatrix}0&1\\i&0\end{pmatrix}$， $a_7=\begin{pmatrix}0&-1\\-i&0\end{pmatrix}$，

G的乘法表为：

$\cdot$	e	a_1	a_2	a_3	a_4	a_5	a_6	a_7
e	e	a_1	a_2	a_3	a_4	a_5	a_6	a_7
a_1	a_1	e	a_3	a_2	a_5	a_4	a_7	a_6
a_2	a_2	a_3	a_1	e	a_6	a_7	a_5	a_4
a_3	a_3	a_2	e	a_1	a_7	a_6	a_4	a_5
a_4	a_4	a_5	a_7	a_6	a_1	e	a_2	a_3
a_5	a_5	a_4	a_6	a_7	e	a_1	a_3	a_2
a_6	a_6	a_7	a_4	a_5	a_3	a_2	a_1	e
a_7	a_7	a_6	a_5	a_4	a_2	a_3	e	a_1

由乘法表显然可见，G中乘法封闭。因为方阵乘法适合结合律，所以G中乘法也适合结合律，于是$(G,\cdot)$成为有限半群，又G中每一元都在表的各行、各列中无重复、无遗漏地出现，故G中乘法适合消去律，于是$(G,\cdot)$是一个群。

由乘法表可见G的子群有，$H_1=\{e\}$，$H_2=\{e,a_1\}$，$H_3=\{e,a_1,a_2,a_3\}$，$H_4=\{e,a_1,a_4,a_5\}$，$H_5=\{e,a_1,a_6,a_7\}$。$H_6=G$。H_1,H_6显然是G的不变子群。因为指数为2的子群必为不变于群，故H_3,H_4是G的不变子群。$\forall a_i\in G$，有$a_ia_1a_i^{-1}=e\in H_2$，$\therefore$ H_2是G的不变子群。

18*. 设$G=\{B\mid B\in(\mathbf{Q})_n,\ |B|\neq 0\}$，$H=\{A|,A\in G,\ |A|=1\}$。 证明，$H$是$G$的不变子群。

证 H为G的子群是显然的。今任取$X\in G, A\in H$，则

$|XAX^{-1}| = |X|\cdot|A|\cdot|X|^{-1} = 1$。 $\therefore$ $XAX^{-1}\in H$，

即 $XHX^{-1}\subseteq H$，故H是G的不变子群。

✓19。设H是G的不变子群，R是H确定的G的等价关系：$aRb\Longleftrightarrow ab^{-1}\in H$，试用$G\times G$的子集表示$R$。

解 $R=\{(a,b)\mid a,b\in G, ab^{-1}\in H\}$。

注，这里只要求H是G的子群，无需H是G的不变子群。

20。$G=\{f\mid f:\mathbf{z}\to\mathbf{z}/(2)\}$，$f,g\in G$，

规定：$(f+g)(x)=f(x)+g(x)$，证明，G是一个加群，且每一非零元的周期均为2。

证 $\because \mathbf{z}/(2)$是加群， $\therefore$ $\forall f,g,h,\in G$，有

$f+g=g+f,\in G$， $(f+g)+h=f+(g+h)$

令 φ：$x\longmapsto\overline{0}$，$\forall x\in\mathbf{z}$，显然$\varphi\in G$，且对任一 $f\in G$ 有

$\varphi+f=f+\varphi=f$，故φ是G的零元。

又$f\in G$。$(f+f)(x)=f(x)+f(x)=\overline{i}+\overline{i}=\overline{0}$，$\forall x\in\mathbf{z}$。

即 $f+f=\varphi$， $\therefore f$是f的负元。

故G是一个加群。从上面的证明还可看出G的每一非零元的周期均为2。

21。设U表示一切单位根作成的乘群，证明$Q/\mathbf{z}$与U同构。

证

$$U=\{e^{\frac{2k\pi}{n}i}\mid k=0,1,\cdots,n-1,\quad n\in\mathbf{z}^{+}\}$$

$$Q/\mathbf{z}=\{\overline{0},\ \overline{\frac{1}{2}},\ \overline{\frac{1}{3}},\ \cdots,\ \overline{\frac{q}{p}},\ \cdots\}$$

$\frac{q}{p}$为正的真既约分数。

令 $\eta: U \to Q/z$

$$e^{\frac{2k\pi}{n}i} \longmapsto \frac{\overline{k}}{n}, \quad k=0,1,\cdots,n-1, \quad n\in Z^+.$$

η是U到Q/z的映射，且显然是满射。

若 $\dfrac{\overline{k_1}}{n_1}=\dfrac{\overline{k_2}}{n_2}$ 则 $\dfrac{k_1}{n_1}-\dfrac{k_2}{n_2}=m\in z$。

$$\therefore \quad e^{\frac{2k_1\pi}{n_1}i} = e^{\frac{2k_2\pi}{n_2}i}$$

故η是单射

$$\forall\ e^{\frac{2k\pi}{n}i}, \quad e^{\frac{2l\pi}{m}i} \in U:$$

$$\eta\left(e^{\frac{2k\pi}{n}i}\cdot e^{\frac{2l\pi}{m}i}\right)=\eta\left(e^{\frac{2(km+l)\pi}{mn}i}\right)$$

$$=\eta\left(e^{\frac{2s\pi}{mn}i}\right)=\frac{\overline{s}}{mn}$$

其中 $km+ln=lmn+s$。 $0\le s<mn$。

$$\because \quad \frac{\overline{k}}{n}+\frac{\overline{l}}{m}=\frac{\overline{km+ln}}{mn}=\frac{\overline{s}}{mn}. \qquad \therefore \eta\left(e^{\frac{2k\pi}{n}i}\cdot e^{\frac{2l\pi}{m}i}\right)=\frac{\overline{s}}{mn}=\frac{\overline{k}}{n}+\frac{\overline{l}}{n}=\eta\left(e^{\frac{2k\pi}{n}i}\right)\cdot\eta\left(e^{\frac{2l\pi}{m}i}\right)$$

η是U到Q/z的同构映射。

$\therefore \quad U\cong Q/z$。

§4 群的同态、同态基本定理

1. 设$G=(\mathbf{R}^*, \times)$，即一切非零实数作成的乘法群，下列规则f，哪些是G到G的同态映射？

$a)$ $x\longmapsto|x|$，　$b)$ $x\longmapsto 2x$，　$c)$ $x\longmapsto x^2$

$d)$ $x\longmapsto\frac{1}{x}$　$e)$ $x\longmapsto -x$　$f)$ $x\longmapsto -\frac{1}{x}$

对于同态映射f，找出$f(G)$，$Kerf$

解 $a)$ $x\longmapsto|x|$是G到G的同态映射，$f(G)$ = 全体正实数集.$kerf=\{1,-1\}$

$b)$ $x\longmapsto 2x$，不是G到G的同态映射.

$\because$ $\exists x, y\in G, f(xy)=2xy\neq(2x)(2y)=f(x)\cdot f(y)$

$c)$ $x\longmapsto x^2$是G到G的同态映射，$f(G)$ = 全体正实数集，$ker=\{1,-1\}$

$d)$ $x\longmapsto\frac{1}{x}$，是G到G的同态映射，$f(G)=G, kerf=\{1\}$

$e)$ $x\longmapsto -x$不是G到G的同态映射.

$\because$ $\forall x,y\in G$，$f(xy)=-xy\neq(-x)(-y)=f(x)\cdot f(y)$

$f)$ $x\longmapsto -\frac{1}{x}$，不是$G$到$G$的同态映射. 理由同上.

2. 设$G=\{2^m3^n\mid m,n\in Q\}$，关于数目乘法作成群，$f$：$2^m3^n\longmapsto 2^m$，证明$f$是$G$到$G$的同态映射，找出$f(G)$，$kerf$.

证 若$2^m3^n=2^{m'}3^{n'}$，$m,m',n,n'\in Q$，则$m=m'$，$n=n'$.

$\therefore$ f：$2^m3^n\longmapsto 2^m$是G到G的映射，任取G中两元2^m3^n，2^l3^t，

则 $f\left((2^m3^n)(2^l3^t)\right)=f(2^{m+l}3^{n+t})=2^{m+l}=2^m2^l$

$=f(2^m3^n)\cdot f(2^l3^t)$，　∴ f是同态映射。

$f(G)=\{2^m\mid m\in Q\}$，　$kerf=\{3^n\mid n\in Q\}$

3．$G=\{A\mid A\in(Q)_n,|A|\neq 0\}$，$G$对方阵乘法作成群，证明$f:A\longmapsto|A|$是$G$到$(\mathbf{R}^*,\cdot)$的同态映射。找出$f(G)$，$kerf$

证　$\forall A\in G$，$|A|\in\mathbf{R}^*$，　∴f：$A\longmapsto|A|$是G到$\mathbf{R}^*$的映射，任取A，$B\in G$，有$f(AB)=|AB|=|A|\cdot|B|$

$=f(A)\cdot f(B)$ 所以f是G到$(\mathbf{R}^*,\cdot)$的同态映射。

$f(G)=(Q^*,\cdot)$，$kerf=\{A\mid A\in G,|A|=1\}$

4．$G=\{A\mid A\in(\mathbf{Q})_2,\ |A|\neq 0\}$$G$对方阵乘法作成群，$A\in G,|A|=2^{n(A)}\frac{q}{p}$，$p,q\in\mathbf{Z}$　p,q为奇数，命φ：$A\longmapsto\begin{pmatrix}1 & n(A)\\ 0 & 1\end{pmatrix}$，证明$\varphi$是$G$的一个自同态，找出$I_m\varphi$，$ker\varphi$

证　$\forall A\in G$，可将$|A|$唯一地表示成$2^{n(A)}\frac{q}{p}$，p，$q\in\mathbf{Z}$，p,q为奇数的形式。　∴φ是G到自身的映射．若$|A|=2^{n(A)}\frac{q}{p}$，$|B|=2^{n(B)}\frac{q'}{p'}$，$p,q,p',q'\in\mathbf{Z}$，且均为奇数，那么$|AB|=|A|\cdot|B|=2^{n(A)+n(B)}\frac{qq'}{pp'}$，其中$pp',qq'\in\mathbf{Z}$，且皆为奇数。

∴ 有$n(AB)=n(A)+n(B)$。因此，$\varphi(AB)=\begin{pmatrix}1 & n(AB)\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & n(A)+n(B)\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & n(A)\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & n(B)\\ 0 & 1\end{pmatrix}=\varphi(A)\varphi(B)$ 所以φ是G的自同态映射。

$I_m\varphi=\left\{\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\mid a\in\mathbf{Z}\right\}$　$ker\varphi=\{A\mid A\in G,|A|=\frac{q}{p}$

$p,q\in\mathbf{N}$, p,q为奇数}

5. G是正有理数作成的乘法群，$a\in G$，$a=2^n\frac{q}{p}$，p,q是奇数，命φ：$a\longmapsto n$，证明，φ是G到$(\mathbf{Z},+)$的同态映射。找出$Im\varphi$ $ker\varphi$。

证 $\forall a\in G$，可将a唯一地表成$a=2^n\frac{q}{p}$，p,q是奇数的形式

$\therefore$显然φ是G到$\mathbf{Z}$的映射。任取$a,b\in G$，设$a=2^n\frac{q}{p}$，$b=2^m\frac{q'}{p'}$，$m,n\in\mathbf{Z}$，p,q,p',q'皆奇数。则$ab=2^{m+n}\frac{qq'}{pp'}$，$m+n\in\mathbf{Z}$，$pp',qq'$为奇数。而$\varphi(ab)=n+m=\varphi(a)+\varphi(b)$

$\therefore$ φ是G到$(\mathbf{Z},+)$的同态映射。

$$I_m\varphi=(\mathbf{Z},+),\quad ker\varphi=\left\{\frac{q}{p}\mid p,q\text{为奇数}\right\}$$

6. 设G是可换群，k是取定的正整数，命f：$a\longmapsto a^k$，证明，f是G的自同态映射。找出Imf，$kerf$。

证 显然f是G到自身的映射。任取$a,b\in G$，因为G可换，所以有$f(ab)=(ab)^k=a^kb^k=f(a)f(b)$，$f$是$G$的自同态映射。

$Imf=\{a^k\mid a\in G\}$，$kerf=\{x\mid x\in G,x^k=e\}$

7. 设$G\overset{f}{\sim}G'$，$kerf=K$，H是G的子群，证明$f^{-1}\left(f(H)\right)=HK$

证 $\because f(HK)=f(H)\cdot f(K)=f(H)$，

$\therefore$ $HK\subseteq f^{-1}\left(f(H)\right)$，任取$y\in f^{-1}\left(f(H)\right)$，则$f(y)\in f(H)$，$\exists h\in H$，使$f(y)=f(h)$，于是$f(h^{-1}g)=f(h)^{-1}f(y)=e'$，$e'$是

G'的单位元。$\Rightarrow h^{-1}y\in K, y\in hK\subseteq HK$，故$f^{-1}\Big(f(H)\Big)\subseteq HK$

$\therefore\ f^{-1}\Big(f(H)\Big)=HK$

8．设H,K是G的子群，且K是$H\cup K$生成子群的不变子群，证明：

a) $(HUK)=HK$；　　*b*) $H\cap K$是H的不变子群；

c) 命φ：$aK\longmapsto a(H\cap K)$，则φ是HK/K到$H/H\cap K$的同构映射。

证　*a*) 见练习三，15题。

b) $H\cap K$是H的子群显然。$\forall h\in H$，有$hHh^{-1}\subseteq H$，$hKh^{-1}\subseteq K$，这是因为K是$(H\cup K)$的不变子群。

$\therefore\ h(H\cap K)h^{-1}\subseteq H\cap K$　$\therefore$ $H\cap K$是H的不变子群。

c) 首先证明$\varphi: aK\longmapsto a(H\cap K), \forall a\in H$，是$HK/K$到$H/H\cap K$ 的映射。事实上，若$aK=bK$，　$a,b\in H$，则$a^{-1}b\in K$　$a^{-1}b\in H\cap K$，　$\therefore a(H\cap K)=b(H\cap K)$，　故$\varphi$是映射，且显然是满射。　若$a(H\cap K)=b(H\cap K)$，$a$，$b\in H$，则$a^{-1}b\in H\cap K$，$a^{-1}b\in K$　故φ是单射。

$\because\ K\lhd(HUK)$，　$H\cap K\lhd H$

$\therefore\ \forall\ a,b\in H$，　$aK\cdot bK=abK\longmapsto ab(H\cap K)$

$=a(H\cap K)\cdot b(H\cap K)$$\varphi$保持运算。　因此$\varphi$是$HK/K$到$H/H\cap K$的同构映射。

9．设G是群，$a,b\in G$，若存在$\sigma_x\in I(G)$，使$b=\sigma_x(a)$，则说a,b共轭。证明，共轭关系是G的一个等价关系．找出S_3的共轭类。

证　$\forall a\in G$　$a=aaa^{-1}=\sigma_a(a)$，　a与a共轭，

若$a,b\in G$　a与b共轭：$b=\sigma_x(a)$，则$a=\sigma_{x^{-1}}(b)$，b与a

共轭。又设 $a,b,c\in G$，　$b=\sigma_x(a)$，　$c=\sigma_y(b)$，则$c=\sigma_{yx}(a)$ 故共轭关系是G的一个等价关系。

S_3的共轭元素类为：{(1)}，{(12)，(13)，(23)}，{(123)，(132)}。

10，找出$Klein$四元群B_4的内自同构群。

解　$B_4=\{e,a,b,ab\}$ 由于B_4是可换群，故$\forall\sigma_x\in I(B_4)$：$a\longmapsto xax^{-1}=a$　$\forall a\in B_4$；　σ_x是恒等自同构，所以$I(B_4)$是单位元群。

11．找出$Klein$四元群的自同构群。

解　$Klein$四元群的保持单位元不变的双射有以下六个：

$$\begin{pmatrix}e & a & b & ab\\ e & a & b & ab\end{pmatrix},\ \begin{pmatrix}e & a & b & ab\\ e & b & a & ab\end{pmatrix},\ \begin{pmatrix}e & a & b & ab\\ e & a & ab & b\end{pmatrix},$$

$$\begin{pmatrix}e & a & b & ab\\ e & ab & b & a\end{pmatrix},\ \begin{pmatrix}e & a & b & ab\\ e & b & ab & a\end{pmatrix},\ \begin{pmatrix}e & a & b & ab\\ e & ab & a & b\end{pmatrix},$$

根据练习二，6题B_4的乘法表知，a,b,ab中任意二元的乘积等于第三元，　∴上面六个双射都是同构映射。由于同构映射将单位元变成单位元，∴ $Klein$四元群的自同构群恰有上面六个元素组成，故是对称群S_3。

12．设G是单群(即不变子群只有$\{e\}$及本身)，且不是交换群，证明，$G\cong I(G)$。

证　令　$\eta:\ G\longrightarrow I(G)$

$$a\longmapsto\sigma_a$$

则η是G到$I(G)$的满射。　显然$\forall a,b\in G,\sigma_{ab}=\sigma_a\sigma_b$。

∴ $\eta(ab)=\eta(a)\eta(b)$，η是G到$I(G)$上的同态映射。

∵ $Ker\eta$是G的不变子群，故由题设$Ker\eta=\{e\}$，或$Ker\eta=G$若$Ker\eta=G$，则$\forall a\in G$，　σ_a是G的恒等映射，即$\forall b\in G$，$aba^{-1}=b,ab=ba$，这与G是不可换群矛盾，　∴ $Ker\eta=\{e\}$，

于是η是同构映射。即$G\cong I(G)$。

13*。设n是取定的自然数，$n>1$，命

$$M_n=\{[a,b]\mid a,b\in\mathbf{Z},\ (a,n)=1\},$$

规定$[a,b]=[a_1,b_1]\Longleftrightarrow a\equiv a_1(mod n),b\equiv b_1(mod n)$，

$$[a,b][b,d]=[ac,bc+d]$$

证明，M_n作成群。

命 $\mathbf{Z}_n'=\{\overline{a}\mid \overline{a}\in\mathbf{Z}_n,(a,n)=1\}$，证明，$\mathbf{Z}'_n$关于运算$\overline{a}\cdot\overline{b}=\overline{a\ b}$作成一个群。

命 φ：$[a,b]\longmapsto\overline{a}$，证明$\varphi$是$M_n$到$\mathbf{Z}_n'$的满同态，求$Ker\varphi$。

证 $\forall[a,b],[c,d]\in M_n$，如果$[a,b]=[a',b']$，$[c,d]=[c',d']$，那么$a\equiv a'(mod n),b\equiv b'(mod n),c\equiv c'(mod n),d\equiv d'(mod n)$。于是，$ac\equiv a'c'(mod n)$，$bc+d\equiv b'c'+d'(mod n)$。$[ac,bc+d]=[a'c',b'c'+d']$，$[a\ ,b][c,d]=[ac,bc+d]\in M_n$，故"$\cdot$"确是$M_n$的一个二元运算。

$\forall[a,b],[c,d],[e,f]\in M_n$，$([a,b]\cdot[c,d])\cdot(e,f)=[ac,bc+d]\cdot[e,f]=[(ac)e,(bc+d)e+f]=[ace,bce+de+f]$；$[a,b]\cdot([c,d]\cdot[e,f])=[a,b]\cdot[ce,de,+f]=[a(ce)b(ce)+de+f]=[ace,bce+dec+f]$ $\therefore([a,b]\cdot[c,d])\cdot(e,f)=[a,b]\cdot([c,d]\cdot[e,f])$，乘法结合律成立。

$\because(1,0)=1$，$\therefore[1,0]\in M_n$，且$\forall[a,b]\in M_n$，$[1,0][a,b]=[a,b][1,0]=[a,b]$，故$[1,0]$是$M_n$的单位元。

$\forall[a,b]\in M_n$，$\because(a,n)=1$，$\therefore\exists s,t\in\mathbf{Z}$，使$as+nt=1$，$as\equiv1(mod n)$，且$(s,n)=1$，于是$[a,b][s,n-bs]=[as,n]=[1,0]$；$[s,n-bs][a,b]=[as,an-abs+b]=[1,0]$，$\therefore[a,b]$在$M_n$中有逆元，$M_n$作成一个群。

下面证明$\mathbf{Z}_n'$关于运算$\bar{a}\cdot\bar{c}=\overline{ab}$成群。

$\forall\ \bar{a},\ \bar{b}\in\mathbf{Z}_n^1$，如果$\bar{a}=\overline{a'}$，$\bar{b}=\overline{b'}$，那么$a\equiv a'(mod\ n)$，$b\equiv b'(mobn)$，于是$ab\equiv a'b'(modn)$，

$\therefore\ \overline{ab}=\overline{a'b'}$，即$\bar{a}\cdot\bar{b}=\overline{a'}\cdot\overline{b'}$。

当$\bar{a}$，$b\in\mathbf{Z}_n'$，即$(a,n)=1$，$(b,n)=1$，那么$(ab,n)=1$，

$\therefore\ \overline{ab}\in\mathbf{Z}_n'$故结合法"$\cdot$"确是$\mathbf{Z}'_n$的一个二元运算，显然，乘法适合结合律，$\bar{1}$为$\mathbf{Z}_n'$的单位元。

$\forall\ \bar{a}\in\mathbf{Z}_n'$，$(a,n)=1$，$\exists s,t\in\mathbf{Z}_n'$，使$as+tn=1$，且$(s,n)=1$　　$\therefore\ \bar{a}\cdot\bar{s}=\bar{s}\cdot\bar{a}=\bar{1}$，$\bar{a}$在$\mathbf{Z}_n'$中有逆元，$\mathbf{Z}_n'$作成一个群。

令　φ：　　$M_n\longrightarrow\mathbf{Z}_n'$

$$[a,b]\longmapsto\bar{a}$$

φ是满射。

任取$[a,b],[c,d]\in M_n$，则$\varphi([a,b]\cdot[c,d])=\varphi[ac,bc+d]=\overline{ac}=\bar{a}\cdot\bar{c}=\varphi[a,b]\varphi[c,d]$　　$\therefore$　φ是M_n到$\mathbf{Z}_n'$的一个同态映射。

$Ker\varphi=\{[a,b]\mid a,b\in\mathbf{Z},\ a\equiv1(modn)\}$

14．设$G=(\mathbf{Z},+)$，$G'=(a)$是6阶循环群，　命φ：$n\longmapsto a^n$，则φ是G到G'的满同态，找出G的所有子群，在φ下的象为(a^2)．找出G的所有子群，在φ下的象为(a^3)。

解　$H_t=\{(6t+2)m\mid m\in\mathbf{Z}\}$，$t=0,\ \pm1,\pm2,\cdots$，是在$\varphi$下的象为$(a^2)$的$G$的所是子群。

$H_s=\{(6s+3)m\mid m\in\mathbf{Z}\}$，$s=o,\ 1,2,\cdots$，是在$\varphi$下的象为$(a^3)$的$G$的所有子群。

15．设G是一个可换群，$E=EndG$，任取f，$g\in\in E$，规定，$(f+g)(x)=f(x)+g(x)$，证明，$(E,+)$作成一个可换群。

证 设$f,g\in E,x,y\in G$,根据$f+g$的定义和G可换，

$\therefore\quad (f+g)(x+y)=f(x+y)+g(x+y)=(f(x)+f(y))+(g(x)+g(y)=(f(x)+g(x))+(f(y)+g(y))=(f+g)(x)+(f+g)(y)\qquad \therefore\ f+g\in E$,且易知$f+g=g+f$

又设f,g,h为E中任三个元，$\forall x\in G$，$((f+g)+h)(x)=(f+g)(x)+h(x)=(f(x)+g(x))+h(x)=f(x)+(g(x)+h(x))=f(x)+(g+h)x=(f+(g+h))(x)$。即$(f+g)+h=f+(g+h)$。

G的零同态φ（将G中任一元皆变成零元的变换）是$(E,+)$的单位元素。

对$\forall f\in E$，作 f'：$x\longmapsto -f(x)$，$\forall x\in G$,则可知,$f'\in E$,且 $f+f'=f'+f=\varphi\qquad \therefore$ f在E中有负元素，故$(E,+)$作成一个可换群。

16。设G是一个群，G的子群仅有有限个。f是G到自身的一个满同态。证明，f是G的一个自同构，（提示，利用定理6）

证 设$Kerf=K$。令$A=\{G$的所有包含K的子群$\}$，$A'=\{G$的所有子群$\}$。显然$A\subseteq A'$根据定理6,A与A'间有一个双射。但A与A'皆为有限集，故$A=A'$。从而$\{e\}\in A$，$K\subseteq\{e\}$，于是$K=\{e\}$，f是G的一个自同构。

§5 直　　积

1。设 $G=G_1\times G_2\times\cdots\times G_n$，证明

$$\varphi_i:\quad (a_1,a_2,\cdots,a_n)\longmapsto a_i$$

是G到G_i的满同态。

证 显然a_i是由$(a_1,a_2,\cdots,a_n)$中第i个元素唯一确定。

∴ φ_i是G到G_i的一个映射。

任取 $b_i\in G_i$，$\exists(b_1,b_2,\cdots,b_i\cdots,b_n)\in G$，使得$\varphi(b_1,b_2,\cdots,b_i,\cdots,b_n)=b_i$，　∴ φ_i是G到G_i的满射。

另外 $\varphi_i((a_1,\cdots,a_i,\cdots,a_n)(b_1,\cdots,b_i,\cdots,b_n))=\varphi_i(a_1b_1,a_2b_2,\cdots,a_ib_i,\cdots,a_nb_n)=a_ib_i=\varphi_i(a_1,\cdots,a_i,\cdots,a_n)\cdot\varphi_i(b_1,\cdots,b_i,\cdots,b_n)$。　∴ φ_i是G到G_i的一个满同态。

2. 设 $G=G_1\times G_2\times\cdots\times G_n$，证明

$$E_i:(a_1,a_2,\cdots,a_n)\longmapsto(e_1,\cdots,e_{i-1},a_i,e_{i+1},\cdots,e_n)$$

是G的一个自同态，我们用 0 表示把G的每一个元皆映射于G的单位元，则有

$$E_i\circ E_i=E_i;\quad E_i\circ E_j=0,\ \text{当}i\neq j\text{时}.$$

证 显然，E_i是G到G的一个映射，设$E_i(a_1,a_2,\cdots,a_n)=(e_1,e_2,\cdots,e_{i-1},a_i,e_{i+1}\cdots,e_n)$，$E_i(b_1,b_2,\cdots,b_n)=(e_1,e_2,\cdots,e_{i-1},b_i,e_{i+1},\cdots,e)$，则 $E_i((a_1,a_2,\cdots,a_i)(b_1,b_2,\cdots,b_i))=E_i(a_1b_1,a_2b_2,\cdots,a_ib_i)=(e_1,e_2,\cdots,e_{i-1},a_ib_i,\cdots,e_n)=E_i(a_1,a_2,\cdots,a_i)E_i(b_1,b_2,\cdots,b_i)$。

∴ E_i是G到G的一个自同态。

任取$(a_1,a_2,\cdots,a_i)\in G$，则$(E_i\circ E_i)(a_1,a_2,\cdots,a_n)=E_i(E_i(a_1,a_2,\cdots,a_i))=E_i(e_1,e_2,\cdots,e_{i-1},a_i,e_{i+1},\cdots,e_n)=(e_1,e_2,\cdots,e_{i-1},a_i,e_{i+1},\cdots,e_i)=E_i(a_1,a_2,\cdots,a_i)$。

∴ $E_i\circ E_i=E$。

当$i\neq j$时，$(E_i\circ E_j)(a_1,a_2,\cdots,a_i)=E_i(E_j(a_1,a_2,\cdots a_i))=E_i(e_1,e_2,\cdots,e_{j-1},e_j,a_{j+1},\cdots,e_i)=(e_1,e_2,\cdots,e_i)$。

∴ $E_i\circ E_j=0$，当$i\neq j$时。

3. 设 G_1,G_2是G的两个不变子群，且$G\approx(G_1,G_2)$，

$G_1 \cap G_2 = \{e\}$，证明，$G = G_1 \times G_2$

证 ∵ $G_1 \lhd G$，$G_2 \lhd G$，∴ $G_1 \cdot G_2$是G的子群 $\Rightarrow G = (G_1, G_2) = G_1 \cdot G_2$，即$\forall g \in G$，有$g = ab, a \in G_1, b \in G_2$。如果还有$g = a'b'$，$a' \in G, b' \in G_2$。则$ab = a'b' \Rightarrow (a')^{-1}a = b'b^{-1} \in G_1 \cap G_2 = \{e\}$，$\therefore a' = a$，$b' = b$。这就是说，将$G$的每一个元表示为$G_1, G_2$的元素的积，其表示式唯一，因此$G$是$G_1, G_2$的内直积。

√ 4．设G_1, G_2是两个群，证明$G_1 \times G_2$是交换群的充要条件是G_1, G_2均为交换群。

证 $G_1 \times G_2$是交换群$\Longleftrightarrow (a_1, a_2)(b_1, b_2) = (b_1, b_2)(a_1, a_2)$，$\forall a_i, b \in G$，$i = 1, 2$。即$(a_1 b_1, a_2 b_2) = (b_1 a_1, b_2 a_2)$ $\Longleftrightarrow a_1 b_1 = b_1 a_1$；$a_2 b_2 = b_2 a_2$，$\forall a, b \in G$，$i = 1, 2$，$\Longleftrightarrow G_1, G_2$是交换群。

5．证明，$Z/(6) \cong Z/(2) \oplus Z/(3)$。

证 $Z/(6)$是由$1 + (6)$生成的6阶循环群，而$Z/(2) \oplus Z/(3)$共有6个元素：$\{(0+(2), 0+(3)), (0+(2), 1+(3)), (0+(2), 2+(3)), (1+(2), 0+(3)), (1+(2), 1+(3)), (1+(2), 2+(3))\}$。易知$(1+(2), 1+(3))$的周期为6，

∴ $Z/(2) \oplus Z/(3)$是$(1+(2), 1+(3))$生成的6阶循环群。

∴ $Z/(6) \cong Z/(2) \oplus Z/(3)$。

6．设B_4表示*Klein*四元群。下面的直积中哪些是同构的？$C_4 \times C_3, C_6 \times C_2, B_4 \times C_3, S_3 \times C_2$。

证 显然$C_4 \times C_3, C_6 \times C_2, B_4 \times C_3, S_3 \times C_2$都是12阶的群。由于$S_3$不是可换群，所以$S_3 \times C_2$也不是可换群。而$C_4 \times C_3, C_6 \times C_2, B_4 \times C_3$都是可换群，因此$S_3 \times C_2$与$C_4 \times C_3, C_6 \times C_2, B_4 \times C_2$都不同构。又∵$(4, 3) = 1$，

∴ $C_4\times C_3=C_{12}$是12阶循环群，而$C_6\times C_2, B_4\times C_3$中元素的最大周期为6，它们都不是循环群，所以$C_4\times C_3$，与$C_6\times C_2$，$B_4\times C_3$也都不同构。我们可以证明，$C_6\times C_2\cong B_4\times C_3$。为此，首先证明：$C_2\times C_2\cong B_4$。

设$C_2=(d)=\{e,d\}$。则$C_2\times C_2=\{(e,e),(e,d),(d,e),(d,d)\}$，$B_4=\{e,a,b,ab\}$，作$C_2\times C_2$到$B_4$的映射$\varphi$：$(e,e)\longmapsto e$，$(e,d)\longmapsto a$，$(d,e)\longmapsto b$，$(d,d)\longmapsto ab$。不难直接验证，$\varphi$是一个同构映射。由上题的证明可知$C_6\cong C_3\times C_2$。所以$C_6\times C_2\cong C_3\times C_2\times C_2\cong C_2\times C_2\times C_3\cong B_4\times C_3$。

7. 设G_1,G_2是两个群，证明

$$G_1\times G_2\cong G_2\times G_1.$$

证 设 $\varphi: G_1\times G_2\longrightarrow G_2\times G_1$

$$(a,b)\longmapsto(b,a),\quad \forall a\in G_1, b\in G_2.$$

显然φ是$G_1\times G_2$到$G_2\times G_1$的一个映射，且是满射。

设 $(a,b)\neq(c,d)$，则至少$a\neq c$或$b\neq d$，

于是$\varphi(a,b)\neq\varphi(c,d)$，　∴ φ是一个双射。

又 $\varphi((a,b)(c,d))=\varphi(ac,bd)=(bd,ac)=(b,a)(d,c)=\varphi(a,b)\varphi(c,d)$。因此 $G_1\times G_2\cong G_2\times G_1$。

8. 设 $G=G_1\times G_2$，证明 $G/G_1\cong G_2$，$G/G_2\cong G_1$。

证 不妨认为G_1,G_2是G的子群，G是G_1,G_2的内直积。于是$G=G_1G_2$，G_1,G_2都是G的不变子群，且$G_1\cap G_2=\{e\}$，那么根据§4定理7，有$G/G_2=G_1G_2/G_2\cong G_1/G_1\cap G_2=G_1/\{e\}$。显然$G_1/\{e\}\cong G_1$　∴　$G/G_2\cong G$。同理可证，$G/G_1\cong G_2$。

9. 设 $G=G_1\times G_2$，H是G_1的不变子群，证明，H也是G的不变子群。

证 不妨认为G_1, G_2是G的子群，G是G_1, G_2的内直积。于是，$G = G_1G_2$，且$\forall a \in G_1$，$\forall b \in G_2$，有$ab = ba$，特别$aH = Ha$。又∵ $H \lhd G_1$。 ∴ $\forall b \in G_2$，有$Hb = bH$。任取$g \in G$，则$g = ab$，$a \in G_1, b \in G_2, gH = abH = aHb = Hab = Hg$， ∴ H也是G的不变子群。

10. 设G是其子群A，B的直积(内部)，N是A的不变子群，证明，$G/N \cong A/N \times B$。

证 ∵ G是子群A, B的内直积， ∴ $\forall g \in G$，有唯一分解表达式$g = ab, a \in A, b \in B$。且$\forall a \in A$，$\forall b \in B$，有$ab = ba$。

令： ϕ： $G/N \longrightarrow A/N \times B$

$gN \longmapsto (aN, b)$，$\forall g \in G, g = ab, a \in A, b \in B$。

设 $g' = a'b'$，$a' \in A, b' \in B$。则$g'N \longmapsto (a'N, b')$，若$gN = g'N \Rightarrow g^{-1}g' \in N$，$b^{-1}a^{-1}a'b' = a^{-1}a'b^{-1}b' \in N \subseteq A$。∴ $b^{-1}b' \in A \cap B = \{e\}$，$b^{-1}b' = e$，$e$是$G$中单位元，于是$b = b'$，从而$a^{-1}a' \in N$，$a' \equiv a (mod N)$。故 $(aN, b) = (a'N, b')$，ϕ确是映射，显然ϕ是满射。

若 $(aN, b) = (a'N, b')$，则$b = b'$，$aN = a'N$，$a' \equiv a (mod N)$。于是$a'b' \equiv ab (mnd N)$。故 $gN = g'N$，∴ϕ是单射。ϕ还是G/N到$A/N \times B$的同构映射，这是因为，$gN \cdot g'N = gg'N = (ab \cdot a'b')N = (aa'bb')N \longmapsto (aa'N, bb') = (aN, b)(a'N, b')$， ∴ $G/N \cong A/N \times B$。

11. 设A, B是G的正规子群，且$G = AB$。证明

$$G/A \cap B \cong A/A \cap B \times B/A \cap B.$$

证 首先不难验证$A \cap B$是G, A, B的正规子群。

∵ $G = AB$，$\forall g \in G$，有$g = ab, a \in A, b \in B$。

因此$g(A \cap B) = ab(A \cap B) = a(A \cap B)b(A \cap B)$。

$\therefore$ $G/A\cap B=A/A\cap B\cdot B/A\cap B$。

又$\because$ $A\lhd G, B\lhd G$，容易看出$A/A\cap B, B/A\cap B$是$G/A\cap B$的正规子群。

任取$g(A\cap B)\subset(A/A\cap B)\cap(B/A\cap B)$，则$g(A\cap B)\in A/A\cap B\Rightarrow g\in A$，又$g(A\cap B)\in B/A\cap B\Rightarrow g\in B$。

$\therefore$ $g\in A\cap B\Rightarrow g(A\cap B)=A\cap B$，因此$(A/A\cap B)\cap(B/A\cap B)=A\cap B$是商群$G/A\cap B$的单位元。从而将$G/A\cap B$中每一个元表为$A/A\cap B, B/A\cap B$的元的积，其表示式唯一，$\therefore$ $G/A\cap B\cong A/A\cap B\times B/A\cap B$。

12．设A, B, C是三个群，且

$$A\times B\cong A\times C$$

是否有 $B\cong C$。

解 一般得不出$B\cong C$。例如取$A=\mathbf{Z}\oplus\mathbf{Z}\oplus\cdots$，可数个无限循环群的直和，$B=\mathbf{Z}$，$C=(0)$。显然

φ: $(a_1, a_2, \cdots, a_i, \cdots)\longmapsto((a_2, a_3, \cdots, a_i, \cdots), a_1)$，$a_i\in\mathbf{Z}$，是$A$到$A\times B$的同构映射。$A\cong A\times B$。又$A\cong A\times C$。于是$A\times B\cong A\times C$，但$B$与$C$不同构。

习 题

1．设$H\leq K\leq G$，证明：

$$[G:H]=[G:K][K:K]$$

证 显然，当$[G:K]$、$[K:H]$中有一个为无限时，$[G:H]$也是无限。

下面考虑$[G:K]$、$[K:H]$都是有限的情形。设$[G:K]=s$，$[K:H]=r$，且G关于K的s个左陪集为a_1K，$a_2K, \cdots, a_sK$；K关于H的r个左陪集为$b_1H, b_2H, \cdots, b_rH$。为此，我们只需证明a_ib_jH，$i=1, 2, \cdots, s$；$j=1, 2, \cdots, r$，是

G关于H的所有不同的左陪集。

首先，对G中任一元g，有$g=a_ik$，其中$k\in K$；而对于k，又有$k=b_jh$，其中$h\in H$。所以，$g=a_ib_jh\in a_ib_jH$。

其次，当$i\neq i'$或$j\neq j$时，有$a_ib_jH\cap a_{i'}b_{j'}H=\phi$。

若$i\neq i'$，因为$a_ib_jH\subset a_iK$，$a_{i'}b_{j'}H\subset a_{i'}K$，而$a_iK\cap a_{i'}K=\phi$，故$a_ib_jH\cap a_{i'}b_{j'}K=\phi$。

若$i=i'$，而$j\neq j$时，如果存在G中元x，$x\in a_ib_jH\cap a_ib_{j'}H$$\Rightarrow a_i^{-1}x\in b_jH\cap b_{j'}H$，这与$b_jH\cap b_{j'}H=\phi$矛盾。

综上所述，G关于H的左陪集恰为sr个，即$[G:H]=[G:K][K:H]$。

2* 设$G=(a)$是n阶循环群，$G'=(b)$是m阶循环群。证明，当且仅当$m|nk$时，存在G到G'的同态映射φ，具有性质$\varphi(a)=b^k$。

设$nk=mt$，证明，上述φ是单一同态映射的充要条件是$(n,t)=1$。

证 若存在G到G'的同态映射φ，具有性质$\varphi(a)=b^k$，那么$\varphi(e)=\varphi(a^n)=b^{nk}=e'$，所以$m|nk$。

反之，若$m|nk$，定义G到G'的映射φ：$a^p\longmapsto b^{kp}$。为了说明φ的确是一个映射，只要证明当$a^p=a^q$时，$b^{kp}=b^{kq}$。事实上，由$a^p=a^q$，得$n|p-q$，于是$nk|kp-kq$，$m|kp-kq\Rightarrow b^{kp}=b^{kq}$。显然，如此定义的映射$\varphi$是$G$到$G'$的同态映射。

下面设$nk=mt$，证明上述φ是单一同态映射的充要条件是$(n,t)=1$。

若$(n,t)=1$。设$\varphi(a^p)=b^{kp}=e'$，则$m|kp$，$mt|kpt$。于是，$nk|kpt$，$n|pt\Rightarrow n|p$，即$a^p=e$，$Ker\varphi=\{e\}$，故φ是单射，从而是单一同态映射。

反之，若$(n,t)\neq 1$。令$d=(n,t)$，则有$n=n'd, t=t'd$，其中$0<n'<n$，由$nk=mt\Rightarrow n'k=mt'$，所以$\varphi(a^{n'})=b^{kn'}=b^{mt'}=e'$，但$a^{n'}\neq e$，故$\varphi$不是单射，从而不是单一同态映射。

3*。设f是群G到群G'的同态映射，$a\in G$，a的周期为r，是否有$f(a)$的周期必定是r？二者之间有何关系？

解 $f(a)$的周期未必是r。由$[f(a)]^r=f(a^r)=f(e)=e'$，其中，e是G中单位元，e'是G'中单位元，可知，$f(a)$的周期整除a的周期r。

4．证明，复数加群$(\mathbf{C},+)$不含指数有限的真子群。

证 设H是G的真子群，且$[G:H]=m$，因为G是交换群，$\therefore H\lhd G$，对任意$x\in G$，$\frac{x}{m}\in G$，由第二章例题1知，$m\left(\frac{x}{m}\right)\in H$，即$x\in H$，$H=G$。这与$H$是$G$的真子群矛盾，故$[G:H]$不能是有限的。

5．证明，非零复数乘群$G=(\mathbf{C}^*,\cdot)$不含指数有限的真子群。

证 设H是G的真子群，且$[G:H]=m$，因为G是交换群，$\therefore H\lhd G$，对任意$x\in G$，有$y\in G$，使得$y^m=x$。由第二章例题1知，$y\in G\Rightarrow y^m\in H$，即$x\in H$，$H=G$，与$H$是$G$的真子群矛盾，故$[G:H]$不能是有限的。

6．设G是可换群，对集合G^G规定二元运算：$f,g\in G^G$，命$(f\cdot g)(x)=f(x)\cdot g(x)$，$\forall x\in G$。证明，$(G^G,\cdot)$是一个有单位元的可换半群，是不是群？

证 设$f,g,h\in G^G$，$((f\cdot g)\cdot h)(x)=(f\cdot g)(x)\cdot h(x)=(f(x)\cdot g(x))\cdot h(x)$，$\forall x\in G$。 $(f\cdot(g\cdot h))(x)=f(x)\cdot(g\cdot h)$

$(x)=f(x)\cdot(g(x)h(x))$，$\forall x\in G$。 ∵ G是群， ∴$(f(x)g(x))h(x)=f(x)(g(x)h(x))$，$\forall x\in G$。故$(f\cdot g)\cdot h=f\cdot(g\cdot h)$。又因为$G$是可换群，所以$f(x)g(x)=g(x)f(x)$，$\forall x\in G\Rightarrow f\cdot g=g\cdot f$。显然，映射$\varphi$：$\varphi(x)=e$，$\forall x\in G$，其中$e$是$G$的单位元，是$(G^G,\cdot)$的单位元，这就证得$(G^G,\cdot)$是一个有单位元的可换半群。

$(G^G,\cdot)$是一个群，因为对任何的$f\in G^G$，令g：$g(x)=f(x)^{-1}$ $\forall x\in G$，则可知g是f在$(G^G,\cdot)$中的逆元。

7．设H是含于G的中心的子群，则H是G的正规子群。若G/H是循环群，则G是可换群。

证 因为H含于G的中心，H中的元与G中的任意元可换，所以，$\forall a\in G, aHa^{-1}=H$，$H\lhd G$。

若G/H是循环群，设aH是其生成元，则对G中任意两个元g_1,g_2，有$g_1=a^{t1}h_1$，$g_2=a^{t2}h_2$，其中$h_1,h_2\in H$。注意到H中的元与G中元可换，且a^{t1}与a^{t_2}可换，于是$g_1g_2=a^{t1}h_1\cdot a^{t2}h_2=a^{t2}h_2a^{t1}h_1=g_2g_1$。故$G$是可换群。

8．设G是一个群，$a,b\in G$，符号$[a,b]$表示G中元素$a^{-1}b^{-1}ab$，称之为G的换位元，证明

① G的一切有限个换位元的乘积所成的集合G'是G的一个不变子群。

② G/G'是可换群。

③ 若N是G的不变子群，且G/N可换，则$N\geqslant G'$。

证 ①显然，G'是G的子群，对任意$[a\ b]$和G中元g，$g^{-1}[a,b]g=g^{-1}a^{-1}b^{-1}abg=(ag)^{-1}b^{-1}agb\cdot b^{-1}g^{-1}bg=[ag,b][b,g]\in G'$。一般地，对$G'$中任一元$[a_1b_1][a_2,b_2]\cdots[a_n,b_n]$，$g^{-1}[a_1,b_1][a_2,b_2]\cdots[a_n,b_n]g=(g^{-1}[a_1,b_1]g)$

$(g^{-1}[a_2, b_2]g)\cdots(g^{-1}[a_s, b_s]g) \in G'$，故$g^{-1}G'g \in G'$，$G' \lhd G$。

②对G/G'中任意二个元aG'，bG'，因为$(ab)^{-1}(ba) = b^{-1}a^{-1}ba \in G'$，所以，$abG' = baG'$，从而$aG' \cdot bG' = bG' \cdot aG'$，$G/G'$是可换群。

③要证$N \geqslant G'$，只要证明$[a,b] \in N$，$\forall a,b \in G$。因为G/N可换，所以$abN = aN \cdot bN = bN \cdot aN = baN \Rightarrow (ba)^{-1} \cdot ab = a^{-1}b^{-1}ab \in N$。即$[a,b] \in N$。

9。$H \lhd G$，$K \lhd G$，且G/H，G/K是可换群，则$G/H \cap K$是可换群。

证 设G'是G中换位元生成的子群，因为G/H，G/K是可换群，由第8题③得$H \geqslant G'$，$K \geqslant G' \Rightarrow H \cap K \geqslant G'$，于是$\forall a,b \in G$，由$a^{-1}b^{-1}ab \in H \cap K \Rightarrow ab(H \cap K) = ba(H \cap K)$，$\therefore a(H \cap K) \cdot b(H \cap K) = ab(H \cap K) = ba(H \cap K) = b(H \cap K) \cdot (aH \cap K)$，即$G/H \cap K$是可换群。

10。设$A_1 \subseteq A_2 \subseteq \cdots \subseteq A_n \subseteq \cdots$是$G$的不变子群的链，证明$A = \bigcup_{i=1}^{\infty} A_i$是$G$的不变子群。

证 由第二章§1例13知，A是G的子群，对A中任意元a，存在A_j，使$a \in A_j$，因为A_j是G的不变子群，所以，对G中任意元g，$gag^{-1} \in gA_jg^{-1} \subseteq A_j \subset A$，即$gAg^{-1} \subseteq A$，$A$是$G$的不变子群。

11。设$H < G$，$K < G$，且$|H| = n$，$|K| = m$，$(m,n) = 1$，则$H \cap K = \{e\}$。

证 因为$H \cap K$既是H又是K的子群，设$|H \cap K| = p$，则$p|n$，$p|m$，由$(m,n) = 1 \Rightarrow p = 1$，故$H \cap K = \{e\}$。

12．证明，阶数为10的可换群是循环群．

证 设群G是阶数为10的可换群，如果G中有周期为10的元素，则G为循环群，否则G中除单位元外的元素的周期只能是2和5，但不能都是2，反之，G中有四阶子群$K=\{e, a, b, ab\}$，$[K:1]=4\Rightarrow 4|10$，矛盾．于是G中必有周期是5的元a，令$H=\{e,a,a^2,a^3,a^4\}$，它是G的5阶不变子群，商群G/H是二阶的，设$G/H=\{H, bH\}$，那么$bH\cdot bH=b^2H=H\Rightarrow b^2\in H$．如果$b$的周期也是5，则$b=b^6=(b^2)^3\in H$，矛盾．所以$b$的周期为2，但这样一来，由于$G$是可换群，而$(5,2)=1$，$\therefore$ ab是G中周期为10的元素，与G中无周期为10的元素不合，从而证得G是循环群．

13．证明，设p,q是互异素数，$|G|=pq$，G是可换群，证明，G是循环群．

证 群G是pq阶可换群，显然G中至少有一个周期为p或q的元，不妨设a是G中周期为p的元．令$H=(a)$，H是G的p阶不变子群，商群G/H是q阶群，$\because$ q是素数，$\therefore G/H$是q阶循环群．设G/H的生成元为bH，那么$(bH)^q=b^qH=H\Rightarrow b^q\in H$．$b$的周期不能为$p$，因为由$b^p=e\in H$，$b^q\in H$，$(p,q)=1\Rightarrow b\in H$，矛盾．故$b$的周期只可能为$pq$或$q$，若$b$的周期为$pq$，$G$是循环群；若$b$的周期为$q$，则$ab$的周期为$pq$，$G$是循环群．

14．设p,q是互异素数，$|G|=pq$，$p<q$，证明，G的q元子群是不变子群．

证 我们首先证明G中不可能有两个不同的q元群．如若G中有两个不同的q元子群H_1, H_2，$\because$ $H_1\cap H_2$是G的子群，其阶数整除q，$\therefore$ $H_1\cap H_2=\{e\}$．令$S=\{h_1h_2, h_1\in H_1, h_2\in H_2\}$．若$h_1h_2=h_1'h_2'$，那么$(h_1')^{-1}h_1=h_2'h_2^{-1}$

$\in H_1 \cap H_2, (h_1')^{-1}h_1 = h_2' h_2^{-1} = e$，即$h_1 = h_1'$，$h_2 = h_2'$，所以$S$恰含$q^2$个元素。但$S \subseteq G$，这与$|G| = pq < q^2$矛盾。

现设H是G的q元子群，$\forall a \in G, aHa^{-1}$也是$G$的$q$元子群，$\therefore aHa^{-1} = H$，$H$是不变子群。

15. 设p, q是互异素数，$|G| = pq$，证明，G中存在q元子群。

证 我们先证明这样一个结论：如果可换群G的阶被素数q整除，那么G中必存在周期为q的元。对$|G|$用归纳法。当$|G| = q$时结论成立，假定结论对$|G| < m$成立，现证结论对$|G| = m$成立，任取G中非单位元a，a的周期为$r \neq 1$。如果$q | r, r = qr'$，那么$a^{r'}$的周期为q，如果$q \nmid r$，那么$G/(a)$的阶为$m/r < m$，且$q | \frac{m}{r}$，由归纳假定必存在$b(a)$，它在$G/(a)$中的周期为q。设b在G中周期为s，由$(b(a))^s = b^s(a) = (a) \Rightarrow q | s$，$s = gs'$，于是$b^{s'}$的周期为$q$。

下面设$|G| = pq, \forall a \in G$，令$N_a = \{x | x \in G, xax^{-1} = a\}$，则$N_a$是$G$的一个子群。用$\overline{a}$表示元素$a$在群$G$中的共轭类，即$\overline{a} = \{gag^{-1}, g \in G\}$，则$|\overline{a}| = [G : N_a]$，这是因为$gag^{-1} = g'ag'^{-1} \Longleftrightarrow g'^{-1}gag^{-1}g' = a \Longleftrightarrow g'^{-1}g \in N_a \Longleftrightarrow g'N_a = gN_a$。易见共轭关系是$G$中元素的一个等价关系。将$G$中元素按共轭关系分类，$G = \bigcup_a \overline{a}$，$a$遍历共轭类的代表元。于是$|G| = \sum_a |\overline{a}| = \sum_a [G : N_a] = |C| + \sum_{a \notin C} [G : N_a]$，其中$C$表示$G$的中心。如果存在一个$N_a$，其阶为$q$，命题得证；如果，$\forall a \notin C, |N_a| \neq q$，那么$|N_a| = p$，$[G : N_a] = q \Rightarrow q | |c|$，$\because C$是可换群，应用前面所证明的结论知，在$C$中，从而在$G$

中存在a元子群。

16. 证明$f: x \longmapsto x^{-1}$是G的一个自同构的充要条件是：G是可换群。

证 显然f是G到G的双射。如果G是可换群，对G中任意元x, y，有$xy \longmapsto (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}$，所以$f$是$G$的一个自同构。如果$f$是一个自同构，那么对$G$中任意二个元$x, y$，由$x^{-1} \longmapsto x, y^{-1} \longmapsto y \Rightarrow x^{-1}y^{-1} \longmapsto xy$，同时又有$x^{-1}y^{-1} = (yx)^{-1} \longmapsto yx$，故$xy = yx$，所以$G$是可换群。

17. 设$H \leq G$，$K \leq G$，利用H，K规定G的元素间的一个二元关系：$a, b \in G, a \sim b \Longleftrightarrow \exists h \in H, k \in K$：$b = hak$，证明

① "$\sim$"是G的一个等价关系，

② $a \in G$，a所在的等价元素类，

$$\overline{a} = \{x \mid x \in G, x \sim a\} = HaK,$$

③ $b \in \overline{a} \Rightarrow Hb \subseteq \overline{a}$，$bK \subseteq a$，

④ $bK \cap Ha \neq \phi \Longleftrightarrow bK \subseteq a$，

⑤ 命$D = a^{-1}Ha \cap K$，C表示在HaK中出现的H在G中的所有右陪集，则

$$\varphi: Dk_0 \longmapsto Hak_0$$

是K到C的一一映射。

C中含有的右陪集个数与D在K中的指数有何关系？

证 ①②③显然（略）。

④ $bK \cap Ha \neq \text{中} \Longleftrightarrow \exists k \in K, h \in H$，使$bk = ha \Longleftrightarrow \exists k \in K$，$h \in H$，使$b = hak^{-1} \Longleftrightarrow b \in \overline{a} \Longleftrightarrow bK \subseteq \overline{a}$。

⑤ D是K的子群，若$Dk_1 = Dk_2$，则$k_1k_2^{-1} \in D \subseteq a^{-1}Ha$，$(ak_1)(ak_2)^{-1} \in H \Rightarrow Hak_1 = Hak_2$，所以$\varphi$是$D$到$C$的映射，且易见，$\varphi$是满射。

如果$Hak_1 = Hak_2 \Rightarrow (ak_1)(ak_2)^{-1} \in H \Rightarrow k_1k_2^{-1} \in a^{-1}Ha$，又$k_1k_2^{-1} \in K$，于是$k_1k_2^{-1} \in a^{-1}Ha \cap K = D \Rightarrow Dk_1 = Dk_2$，$\varphi$是$D$到$C$的一一映射。

C中含有的右陪集个数等于$[K : D]$。

18. 设$G=(a)$，$H<G$，$[G : H]=m$，则G/H是m阶循环群，且$e, a\cdots, a^{m-1}$可取作H的陪集的代表。

证 循环群的子群是循环群，设$H=(a^t)$，易知H，aH，$\cdots$，$a^{t-1}H$是G关于H的所有不同陪集。 $\because [G : H]=m$，$\therefore t=m$，于是e，a，$\cdots$，a^{m-1}可取作H的陪集的代表，从而G/H是由aH生成的m阶循环群。

19. 设G是可换群，证明，G中一切有限阶元素所成的集合T是G的一个子群，并且G/T除单位元外不含有限阶元素。

证 设$a \in T$，a是m阶元素，则a^{-1}也是m阶元素，$\therefore a^{-1} \in T$。又$b \in T$，b是n阶元素，则$(ab)^{mn} = a^{mn}b^{mn} = e \Rightarrow ab \in T$。故$T$是$G$的子群。

对G/T中任意元aT，如果aT的阶有限，为k，则$(aT)^k = a^kT = T \Rightarrow a^k = b \in T$。命$b$的阶为$h$，于是$a^{kh} = b^h = e$，$a \in T$，故$aT = T$是$G/T$中单位元，$G/T$中除单位元外不含有限阶元素。

20. $H<G$，$K<G$，$D = H \cap K$，证明

① 若$k_1, k_2 \in K$，且k_1, k_2属于D的两个不同右陪集，则$Hk_1 \cap Hk_2 = \phi$

② 设H、K是G的有限子群，$[K : D]=d$，且$K = \bigcup_{i=1}^{d} Dk$，则$HK = \bigcup_{i=1}^{d} Hk_i$

由①，②，关于$|HK|$与$|D|$，你能得出怎样的结论？

证 ①若$Hk_1 \cap Hk_2 \neq \phi$，则$k_1k_2^{-1} \in H$，又$k_1k_2^{-1} \in K \Rightarrow$

$k_1k_2^{-1}\in H\cap K=D$，从而$Dk_1=Dk_2$，矛盾，　∴ $Hk_1\cap Hk_2=\phi$。

②由$K=\bigcup_{j=1}^{d}Dk_j$，得 $HK=\bigcup_{i=1}^{d}HDk_i=\bigcup_{i=1}^{d}Hk_i$。

由①，②，$|HK|=|H|\cdot d=\frac{|H|\,|K|}{|D|}$。

21. 设G是有限群，H是G的子群，$a\in G$，证明，存在最小正整数m，$a^m\in H$，并且，m是a的周期n的因数。

证　∵ G是有限群，　∴ $\forall a\in G$，a的周期有限。设a的周期为n，于是$a^n=e\in H$，故存在最小正整数m，使$a^m\in H$。命$n=km+t$，$0\leq k<m$，则$a^t=a^na^{-km}=(a^m)^{-k}\in H$，$t$必为零，否则与$m$的最小性矛盾，故$m$是$n$的因数。

22. 设S是G的一个子群，$\{S_\alpha\mid\alpha\in A\}$是$G$中与$S$共轭的所有子群的集合，证明，$N=\bigcap_{\alpha\in A}S_\alpha$是$G$的不变子群。

证　对G中任意元a，及S_α，$\alpha\in A$，$aS_\alpha a^{-1}$是S的一个共轭子群。另一方面，对任一S_β，$\beta\in A$，存在S的一个共轭子群$S_\beta'=a^{-1}S_\beta a$，使$S_\beta=aS_\beta'a^{-1}$，于是$\{aS_\alpha a^{-1}\mid\alpha\in A\}$也是$G$中与$S$共轭的所有子群的集合。∴ $aNa^{-1}=\bigcap_{\alpha\in A}aS_\alpha a^{-1}=\bigcap_{\alpha\in A}S_\alpha=N$，$N$是$G$的不变子群。

23. 设G是有限群，证明，G中与子群S共轭的子群的个数等于$[G:N(S)]$。此处$N(S)=\{x\mid x\in G,xSx^{-1}=S\}$。

证　由练习一，16题，$N(S)$是G的子群，对G中任意元x，y，$xSx^{-1}=ySy^{-1}\Longleftrightarrow y^{-1}xSx^{-1}y=S\Longleftrightarrow y^{-1}x\in N(S)\Rightarrow xN(S)=yN(S)$。故$S$在$G$中的共轭子群的个数等于$[G:N(S)]$。

24. 设G是有限群，$S_1,\cdots,S_k$是与S共轭的全部子群，

证明$\bigcup_{i=1}^{k} S_i$是G的一个真子集。

证 记$N(S)=\{x \mid x\in G, xSx^{-1}=S\}$，显然$S\trianglelefteq N(S)$，$\therefore |N(S)|\geqslant |S|$。于是，由上题$[G:N(S)]=k$，$\therefore |G|=|N(S)|[G:N(S)]\geqslant |S|\cdot[G:N(S)]=k|S|$。∵单位元是$S_i$中的公共元，$\therefore |\bigcup_{i=1}^{k} S_i|<k|S_i|=k|S|\leq G$，从而得到$\bigcup_{i=1}^{k} S_i$是$G$的真子集。

25. 证明，就同构的意义来说，10个元的群只有两个。

证 由第15题知，在10元群G中存在一个5元子群H，H是5阶循环群。设$H=\{e,a,a^2,a^3,a^4\}$，同时G中也必有周期为2的元素，设为b，于是，

$$G=H\cup Hb=\{e,a,a^2,a^3,a^4,b,ab,a^2b,a^3b,a^4b\}$$

(1) 如果$ba=ab$，那么G是交换群，由13题知，G是10阶循环群。

(2) 如果$ba\neq ab$，当然$ba\neq e$，否则$b=a^4$，b的周期为5，矛盾。因此，还有以下三种可能，$ba=a^4b$，$ba=a^2b$，$ba=a^3b$。

我们指出，$ba=a^2b$不可能，反之，有$a=b^2a=b(ba)=b(a^2b)=a^4$，矛盾。同样$ba=a^3b$也不可能。

而当$a^5=e$，$b^2=e$，$ba=a^4b$时，元素a，b的确生成一个10阶非交换群，这只要验证它与S_5中由(12345)，(25)(34)生成的子群同构。

故就同构的意义来说，10个元的群只有两个。

26. 证明，阶数为素数幂的群的中心不仅含有单位元。

证 由第15题知，将G中元素按共轭关系分类，$G=\bigcup_{a}\bar{a}$，a遍历共轭类的代表元。于是，$|G|=\sum_{a}|\bar{a}|=\sum_{a}[G:N_a]$

$=|C|+\sum_{a\notin C}[G:N_a]$，其中$C$表示$G$的中心，$N_a=\{x|x\in G, xax^{-1}=a\}$。当$a\notin C$时，$N_a$是$G$的真子群。设$|G|=p^r$，$p$是素数，那么$N_a$的阶为$p^{r'}$，$0<r'<r$，故$p|[G:N_a]$，所以$p|C|$，这说明$G$的中心不仅含有单位元。

27. 证明，阶数为p^2(p素数)的群是可换群。

证 设群G的阶为p^2，G的中心为C，C是G的不变子群，由上题知$|C|>1$。若$|C|=p^2$，则G是可换群；若$|C|=p$，那么G/C是阶数为素数p的群，从而是循环群，由第7题得G是可换群，这与$|C|=p$矛盾。

28. 设G是群，$a,b\in G$，a,b在G中共轭，证明，$C_a=\{x|x\in G, xa=ax\}$与$C_b=\{x|x\in G, xb=bx\}$是共轭子群。

证 因为a,b在G中共轭，$\exists d\in G$，使$a=dbd^{-1}$。$\forall x\in C_a$，$x=axa^{-1}$，于是$x=axa^{-1}=dbd^{-1}xdb^{-1}d^{-1}$，$d^{-1}xd=b(d^{-1}xd)b^{-1}$，$(d^{-1}xd)b=b(d^{-1}xd)$，所以$d^{-1}xd\in C_b$，$d^{-1}C_ad\subseteq C_b$。同理由$b=d^{-1}ad$，得$dC_bd^{-1}\subseteq C_a$，$d^{-1}C_ad\supseteq C_b$，故$d^{-1}C_ad=C_b$，$C_a$与$C_b$是共轭子群。

29. $H\lhd G$，$K\lhd G$，且$H\cap K=\{e\}$，证明G与$G/H\times G/K$的一个子群同构。

证 作G到$G/H\times G/K$的映射φ：$a\longmapsto(aH, aK)$，$\forall a\in G$，容易论证φ是G到$G/H\times G/K$的群同态映射。且若，$a\longmapsto(aH,aK)=(H,K)$，$(H,K)$是$G/H\times G/K$中单位元，那么$aH=H$，$aK=K\Rightarrow a\in H\cap K=\{e\}$，$a=e$，即$Ker\varphi=\{e\}$。所以$G$与其同态象，$G/H\times G/K$的一个子群同构。

30. $H\lhd G$，$K\lhd G$，且$HK=G$，$hk=kh$，$\forall h\in H, k\in K$，证明G是$H\times K$的一个同态象。

证 作$H\times K$到G的映射φ：$(h,k)\longmapsto hk$，$\forall h\in H, h\in K$。

$\because G=HK$，$\therefore\varphi$是满射。由$(h,k)(h',k')=(hh',\ kk')\longmapsto hh'kk'=hk\cdot h'k'$，$\forall h,h'\in H,k,k'\in K$，得$\varphi$是$H\times K$到$G$上的群同态映射，　$\therefore G$是$H\times K$的一个同态象。

注：由$HK=G,hk=kh,\ \forall h\in H,k\in K\Rightarrow H\lhd G,K\lhd G$。

31。设G是个群，H是G的子群，$a\in G,a\notin H$，证明，存在G的子群M，具有性质

$a)$ $a\notin M$，　$b)$ $M\supseteq H$，　$c)$真包含M的G的任一子群均含有a。

证　令G中所有包含H，而不含元素a的子群所构成的集合为S。$\because H\in S$，　$\therefore$ S不空，在S中我们规定$K\leqslant N$，当且仅当作为集合有$K\subseteq N$。易知，这样规定的“$\leqslant$”是S的一个偏序关系。设$L=\{A_i,i\in I\}$是S的任一非空有序子集，令$A=\bigcup_{i\in I}A_i$，则A是G的一个包含H的子群。因为$a\notin A_i$，$\forall i\in I$。$\therefore$ $a\notin A$，故$A\in S$，它是L的一个上界，根据$Zorn$引理，S有极大元M。

显然，M具有性质$a)$和$b)$，对任何一个真包含M的G的子群M'，$M'\notin S$，但$M'\supseteq H$，故$a\in M'$，于是M具有性质$c)$。

32* 设G是n个无限循环群的直积：

$$G=(a_1)\times(a_2)\times\cdots\times(a_n)$$

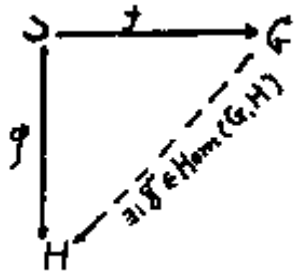
S是含有n个元的集合：

$$S=\{x_1x_2,\cdots,x_n\},$$

f是S到G的映射，f：$x_i\longmapsto(e,\cdots,a_i,\cdots,e)$，$i=1,2,\cdots,n$。证明，对于任意交换群$H$，任一$S$到$H$的映射$\varphi$，均唯一存在$G$到$H$的同态映射$g$，使下图交换：

证　唯一性，如果g是G到H的同态映射，且$\varphi=gf$。于是$g(e,\cdots,a_i,\cdots,e)=gf(x_i)=\varphi(x_i)$，$\forall x_i\in S$，那么对$G$中任

意元 $(a_1^{k1}, a_2^{k2}, \cdots, a_n^{kn})$，$g(a_1^{k1}, a_2^{k2}, \cdots, a_n^{kn}) = [g(a_1, e, \cdots, e)]^{k1} \cdot [g(e, a_2, e, \cdots, e)]^{k2} \cdots [g(e, \cdots, e, a_n)]^{kn} = \varphi(x_1)^{k1}\varphi(x_2)^{k2}\cdots\varphi(x_n)^{kn}$，所以$g$是唯一确定的。



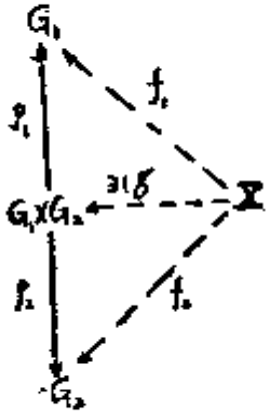
存在性，做G到H的映射$g:(a_1^{k1}, a_2^{k2}, \cdots, a_n^{kn}) \longmapsto \varphi(x_1)^{k1}\varphi(x_2)^{k2}\cdots\varphi(x_n)^{kn}$。 $\because$ (a_i)是无限循环群，$\therefore g$确是G到H的一个映射。$\forall x_i \in S, gf(x_i) = g(e, \cdots, a_i, \cdots, e)$，$\therefore \varphi = gf$。注意到$H$是交换群，易知$g$是$G$到$H$的群同态映射。

33. 叙述并证明上题关于 G 是可数个无限循环群的直积的情形。

用直和代替直积，我们有与上题类似的结论：设G是可数个无限循环群的直和，$G = \sum_{i=1}^{\infty}\oplus(a_i)$。$S$是可数个元素的集合，$S = \{x_1, x_2, \cdots, x_n, \cdots\}$，$f$是$S$到$G$的映射，$f: x_i \longmapsto (e, \cdots, a_i, \cdots)$，$i = 1, 2, \cdots$，证明，对于任意交换群$H$，任一$S$到$H$的映射$\varphi$，均唯一存在$G$到$H$的同态映射$g$，使$\varphi = fg$。

证明与上题相同，从略。

34* 设群G是G_1, G_2的直积：$G = G_1 \times G_2$，π_i是G_i到G的映射，$\pi_1(a_1) = (a_1, e)$，$\pi_2(a_2) = (e, a_2)$，设X是任意可换群，且存在G_i到X的同态映射f_i，$i = 1, 2$，证明，存在唯一同态映射g，使右图交换。即



$$f_1 = g \circ \pi, f_2 = g \circ \pi_2$$

证 唯一性，设g是$G_1 \times G_2$到X的同态映射，且$f_1 = g \circ \pi_1$，$f_2 = g \circ \pi_2$，于是$g(a_1, a_2) = g[(a_1, e)(e, a_2)] = g(a_1, e) \cdot g(e_1, a_2) = (g \circ \pi_1(a_1)(g \circ \pi_2(a_2)) = f_1(a_1) f_2(a_2)$，即$g(a_1, a_2)$是完全确定的，从而证得$g$的唯一性。

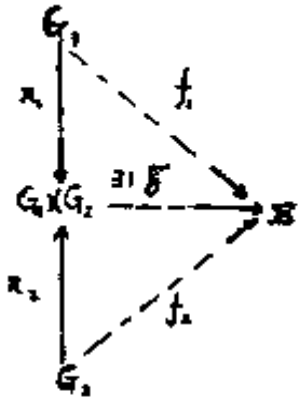
存在性，做$G_1 \times G_2$到X的映射g：$(a_1, a_2) \longmapsto f_1(a_1) f(a_2)$，　$\forall a_1 \in G_1, a_2 \in G_2$。　$\forall a_1 \in G_1$，$g \circ \pi_1(a_1) = g(a_1, e) = f_1(a_1) f_2(e) = f_1(a_1)$。　$\therefore f_1 = g \circ \pi_1$。同理可证，$f_2 = g \circ \pi_2$。下面证明$g$是$G_1 \times G_2$到$X$的群同态映射。

$g[(a_1, a_2)(a_1', a_2')] = g(a_1 a_1', a_2 a_2') = f_1(a_1 a_1') \cdot f_2(a_2 a_2') = f_1(a_1) f_1(a_1') f_2(a_2) f_2(a_2')$，

$g(a_1, a_2) \cdot g(a_1', a_2') = f_1(a_1) f_2(a_2) f_1(a_1') f_2(a_2') = f_1(a_1) f_1(a_1') f_2(a_2) f_2(a_2')$，

$\therefore g[(a_1, a_2)(a_1', a_2')] = g(a_1, a_2) \cdot g(a_1', a_2')$，$\forall a_1, a_1' \in G$，$a_2, a_2' \in G_2$。$g$是$G_1 \times G_2$到$X$的群同态映射。

35。同上题，p_i是G到G_i的射影，f_i是X到G_i的同态映射，$i = 1, 2$。证明，存在唯一同态映射g，使下图交换。即



$f_1 = p_1 \circ g$，$f_2 = p_2 \circ g$

证 类似于上题的方法可以证明，满足条件的X到$G_1 \times G_2$的唯一的同态映射是$g: x \longmapsto (f_1(x), f_2(x))$，$\forall x \in X$。

36。设f是加群G到G'的满同态，并且，存在G'到G的同

态映射g，使$f\circ g$是G'的恒等映射，证明，$G=Img\oplus \mathrm{K}erf$。

证 显然Img、$\mathrm{K}erf$是G的子群。先证$G=Img+\mathrm{K}erf$。$\forall a\in G$，令$f(a)=a'\in G$，那么$a=g(a')+(a-g(a'))$，$g(a')\in Img$。 $\because$ $f(a-g(a'))=f(a)-fg(a')=a'-a'=0$，$\therefore$ $a-g(a')\in \mathrm{K}erf$，因此 $a\in Img+\mathrm{K}erf$，故$G=Img+\mathrm{K}erf$。次证$Img\cap \mathrm{K}erf=\{0\}$。设$a\in Img\cap \mathrm{K}erf$，$\because a\in Img$，$\therefore \exists a'\in G'$，使$a=g(a')$，又$a\in \mathrm{K}erf$，$\therefore f(a)=0$，于是$a'=fg(a')=f(a)=0$，从而$a=g(0)=0$，故$Img\cap \mathrm{K}er_f=\{0\}$，$G=Img\oplus \mathrm{K}erf$。

注：由$f\circ g$是G'的恒等映射得f是G到G'的满映射。

37. 设f是加群G到G'的单一同态，并且，存在G'到G的同态映射g，使$g\circ f$是G的恒等映射，证明$G'=Imf\oplus \mathrm{K}erg$。

证 先证$G'=Imf+\mathrm{K}erg$。 $\forall a'\in G'$，令$a=g(a')$，$a'=f(a)+(a'-f(a))$，$f(a)\in Imf$，$\because g(a'-f(a))=g(a')-gf(a)=a-a=0$，$\therefore a'-f(a)\in \mathrm{K}erg$。于是$a'\in Imf+\mathrm{K}erg$，$G'=Imf+\mathrm{K}erg$。次证$Imf\cap \mathrm{K}erg=\{0\}$，设$a'\in Imf\cap \mathrm{K}erg$，$\because a'\in Imf$，$\therefore$存在$a\in G$，使$a'=f(a)$，又$a'\in \mathrm{K}erg$，$\therefore g(a')=0$，$a=g\cdot f(a)=g(a')=0$，从而$a'=f(0)=0$，故$Imf\cap \mathrm{K}erg=\{0\}$，$G'=Imf\oplus \mathrm{K}erg$。

注：由$g\circ f$是G的恒等映射得f是G到G'的单一映射。

38. 设$f:x\mapsto x^3$是群G到G的单一同态，证明，G是交换群。

证 对G中任意元a,b，$f(ab)=(ab)^3=a^3b^3$，即$abab=a^3b^3$，$(ba)^2=a^2b^2$。同理$(ba)^3=b^3a^3$，$(ab)^2=b^2a^2$。于是$(ba)^4=(a^2b^2)^2=b^4a^4$，而又有$(ba)^4=(ba)^3ba=b^3a^3ba$。由$b^4a^4=b^3a^3ba\Rightarrow ba^3=a^3b$，$\therefore (ab)^3=(ab)^2(ab)=b^2a^2\cdot ab=b^2a^3b=b^2\cdot ba^3=b^3a^3=(ba)^3$，即$f(ab)=f(ba)$。因为$f$是单一同态，所以$ab=ba$，$G$是交换群。

第三章　环与域

练习

§1　定义及基本性质

1．　在环A中，计算$(a+b)^3=?$

解　$(a+b)^3=(a^2+ab+ba+b^2)(a+b)=a^3+aba+ba^2+b^2a+a^2b+ab^2+bab+b^3$。

2．证明$\mathbf{Z}[i]=\{a+bi\mid a,b\in\mathbf{Z},i$是虚数单位$\}$关于数目加法、乘法作成一个环。

证　分别验证环的定义中所须条件成立即可。

3．　证明，任意一个不仅含有一个数的有限数集关于数目的加法和乘法不能作成一个环。

证　用反证法。设R是一个有限数集，R中不只有一个元素，但R作成环。$\because$ R不只含一个元素，$\therefore$必$\exists a\in R,a\neq 0$。作$S=\{na\mid n$为整数$\}$，则$S\subseteq R$。显然，在数集中，由于$a\neq 0$，$\therefore$当$m\neq n$时，$ma\neq na$，$\therefore S$为无限集。这与已知R是有限数集且$S\subseteq R$矛盾。R不能作成一个环。

4．　在$\mathbf{Z}_5$中，找出每一个非零元的逆元。

解　$\bar{1}$的逆元是$\bar{1}$本身；$\bar{2}$和$\bar{3}$互为逆元，$\bar{4}$的逆元是$\bar{4}$本身。

5．　在$\mathbf{Z}_{15}$中，找出方程$x^2-1=0$的全部根。

解　设$\bar{y}\in\mathbf{Z}_{15}$，$\overline{y^2-1}=0$，则$y=0,1,\cdots,14$，$y^2\equiv 1\pmod{15}$。易求得，只有$y=1,4,11,14$。$\therefore$方程$x^2-1=0$在$\mathbf{Z}_{15}$中的全部根是$\bar{1},\bar{4},\overline{11},\overline{14}$。

6. 设 a 是有单位元的环 A 的一个正则元，证明，$-a$ 也是正则元，且 $(-a)^{-1}=-a^{-1}$。

证 ∵ a 是正则元，∴$\exists a^{-1}\in A$，使得 $aa^{-1}=a^{-1}a=1$。∴$(-a)(-a^{-1})=(-a^{-1})(-a)=1$。$-a$ 是正则元，且 $(-a)^{-1}=-a^{-1}$。

7. 设 a,b 是有单位元的环 A 的两个正则元，证明 ab 也是 A 的正则元，且 $(ab)^{-1}=b^{-1}a^{-1}$。

证 ∵ a,b 是 A 的正则元，∴$\exists a^{-1},b^{-1}\in A$，使得 $aa^{-1}=a^{-1}a=1$，$bb^{-1}=b^{-1}b=1$。

∴$(ab)(b^{-1}a^{-1})=a(bb^{-1})a^{-1}=aa^{-1}=1$；$(b^{-1}a^{-1})(ab)=b^{-1}(a^{-1}a)b=b^{-1}b=1$，$ab$ 是 A 的正则元，$(ab)^{-1}=b^{-1}a^{-1}$。

8. 设 A 是有单位元的环，证明，A 中正则元一定不是零因子。

证 用反证法。设 a 是 A 中一个正则元，如果 a 是零因子，则存在 $b\in A$，$b\neq 0$，使得 $ab=0$。但 a 为正则元，有逆元 a^{-1}。于是，$b=a^{-1}(ab)=a^{-1}\cdot 0=0$，与 $b\neq 0$ 矛盾。∴ A 中任一正则元一定不是零因子。

9. A 是所有分母为2的非负整数次方幕的既约分数所成集合，问 A 关于数目加法、乘法是否作成一个环？

解 任取 $a,b\in A$，则必存在整数 k_1,k_2 和非负整数 m_1,m_2，使 $a=\frac{k_1}{2^{m_1}}$，$b=\frac{k_2}{2^{m_2}}$，$a\pm b=\frac{k_1\cdot 2^{m_2}\pm k_2\cdot 2^{m_1}}{2^{m_1+m_2}}$。显然，经过约分之后，$a\pm b$ 仍是分母为2的非负整数次方幕的既约分数，从而 $a\pm b\in A$。同理，$ab=\frac{k_1k_2}{2^{m_1+m_2}}\in A$。

按环的定义，容易证得，A 关于数目加法、乘法作成一

个环。

10. 设 S 表示 A 的一切不是(左零因子，也不是右)零因子的元的集合，证明， S 是 $(A,\cdot)$ 的子半群。

证 任取 $a,b\in S$，今用反证法证明 ab 不是 A 的左零因子。

如若 ab 为 A 的左零因子，则有 $c\in A, c\neq 0$，使得 $(ab)c=0$。

$\therefore a(bc)=(ab)c=0$。但 a 不是 A 的左零因子，$\therefore$ 必有 $bc=0$，但 b 也不是 A 的左零因子，$\therefore$ 必有 $c=0$，与 $c\neq 0$ 矛盾。

$\therefore ab$ 不是 A 的左零因子。同理可证，ab 也不是 A 的右零因子。因此，$ab\in S$，S 对乘法封闭。

又∵结合律显然成立，$\therefore S$ 是 $(A,\cdot)$ 的子半群。

注：原题“设 S 表示 A 的一切不是零因子的元的集合”，这样，按原书关于零因子的定义，A 中就包含是左零因子，而非右零因子的元；也包含是右零因子，而非左零因子的元，那么，题中结论不成立。

例如取 A 为 F 上无穷矩阵环(见第三章习题40)。

$$\text{令 } a=\begin{pmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & \ddots & \ddots \end{pmatrix},\qquad b=\begin{pmatrix} 0 & & & \\ 1 & 0 & & \\ & 1 & \ddots & \\ & & \ddots & \end{pmatrix}$$

1是 F 中单位。由 ab 是 A 的单位元，易证 $a,b\in S$，但 $ba\notin S$。故 S 不是 $(A,\cdot)$ 的子半群。

11. 证明，$B_1=\{3x\mid x\in\mathbf{Z}\}$，$B_2=\{5x\mid x\in\mathbf{Z}\}$ 是整数环 $\mathbf{Z}$ 的两个子环。求 $B_1\cap B_2=?$

解 ① 任取 $a,b\in B_1$，则必存在 $x_1,x_2\in\mathbf{Z}$，使得 $a=3x_1$，$b=3x_2$，$\therefore a-b=3x_1-3x_2=3(x_1-x_2)\in B_1$，$a\cdot b=3x_1\cdot 3x_2=3(3x_1x_2)\in B_1$，$\therefore B_1$ 是 $\mathbf{Z}$ 的子环。同理可证，B_2 是 $\mathbf{Z}$ 的子环。

② 任取 $y\in B_1\cap B_2$，则 $y\in B_1$，$y\in B_2$。由 $y\in B_1$ 知，$3\mid y$，

由$y\in B_2$知，$5|y$，而$(3,5)=1$，$\therefore 3\times 5|y$，即$15|y$，$y=15x\in\{15x|x\in\mathbf{Z}\}$，$B_1\cap B_2\subseteq\{15x|x\in\mathbf{Z}\}$。

但是，显然$B_1\supseteq\{15x|x\in\mathbf{Z}\}$，$B_2\supseteq\{15x|x\in\mathbf{Z}\}$，$\therefore B_1\cap B_2\supseteq\{15x|x\in Z\}$。$\therefore B_1\cap B_2=\{15x|\in\mathbf{Z}\}$。

12. 设E是加群$(G,+)$的自同态环，H是G的一个子群，证明$E_H=\{f|f\in E,f(H)\subseteq H\}$是$E$的一个子环。

证 单位映射$1\in E_H$，$\therefore E_H$非空。任取$f_1,f_2\in E_H$，则$f_1,f_2\in E$，且$f_1(H)\subseteq H$，$f_2(H)\subseteq H$。

$\because E$是环，$\therefore f_1-f_2\in E$，$f_1\cdot f_2\in E$，且$(f_1-f_2)(h)=f_1(h)-f_2(h)\in H$，$\forall h\in H$。$(f_1f_2)(h)=f_1(h)\cdot f_2(h)\in H\cdot H=H$（$\because H$是子群），$\forall k\in H$。$\therefore (f_1-f_2)(H)\subseteq H$，$(f_1f_2)(H)\subseteq H$，$f_1-f_2\in E_H$，$f_1\cdot f_2\in E_H$，$E_H$是$E$的一个子环。

13. 设E是加群$(G,+)$的自同态环，H是G的一个子群，证明$B_H=\{f|f\in E,\forall x\in G:f(x+H)\subseteq f(x)+H\}$是$E$的一个子环。

证 单位映射$1\in B_H$，$\therefore B_H$非空。任取$f_1,f_2\in B_H$，则$f_1,f_2\in E$，且$\forall x\in G$，$f_1(x+H)\subseteq f_1(x)+H$，$f_2(x+H)=f_2(x)+H$。

由$f_1,f_2\in E$，E为环，可知$f_1-f_2\in E$，$f_1f_2\in E$。

$\because H$是G的子群，$f_1(x+H)\subseteq f_1(x)+H$，$f_2(x+H)\subseteq f_2(x)+H$。$\therefore$对$\forall x\in G,h\in H$有：$f_1(x+h)-f_2(x+h)\in f_1(x)-f_2(x)+H$，$f_1(x+h)\cdot f_2(x+h)\in f_1(x)\cdot f_2(x)+H$。$\therefore\forall x\in G$，$h\in H$，$(f_1-f_2)(x+h)=f_1(x+h)-f_2(x+h)\in f_1(x)-f_2(x)+H=(f_1-f_2)(x)+H$，$(f_1\cdot f_2)(x+h)=f_1(x+h)\cdot f_2(x+h)\subseteq f_1(x)f_2(x)+H=(f\cdot f_2)(x)+H$。$\therefore f_1-f_2\in B_H$，$f_1f_2\in B_H$，$B_H$是$E$的一个子环。

14*. 设$(A,+,\cdot)$是一个环，对A^A规定加法与乘法：任取$f,g\in A^A$，$\forall x\in A$，命

$$(f+g)(x)=f(x)+g(x),$$
$$(f\cdot g)(x)=f(x)\cdot g(x);$$

证明，$(A^A,+,\cdot)$是一个环。

命S是A的一个子环，证明

$$B_S=\{f\mid f\in A^A, f(S)\subseteq S\}$$

是$(A^A,+,\cdot)$的一个子环。

证 (1)容易验证，$(A^A,+)$是可换加群，$(A^A,\cdot)$是乘法半群，且对于任意的$f,g,h\in A^A$和任意的$x\in A$，$[f(g+h)](x)=f(x)[(g+h)(x)]=f(x)[g(x)+h(x)]=f(x)g(x)+f(x)h(x)=(fg)(x)+(fh)(x)=(fg+fh)(x)$。$\therefore f(g+h)=fg+fh$。同样，有$(g+h)f=gf+hf$。$\therefore$乘法对加法适合分配律，$(A^A,+,\cdot)$作成一个环。

(2) 显然，零同态（即把A中的任意元素都映射为0的同态）$\in B_S$，$\therefore B_S$非空。任取$f,g\in B_S$，则$f,g\in A^A$，$f(S)\subseteq S$，$g(S)\subseteq S$，而S是A的子环，$\therefore (f-g)(s)=f(s)-g(s)\in S$；$(fg)(s)=f(s)g(s)\in S$，$\forall s\in S$。$\therefore (f-g)(S)\subseteq S$，$(fg)(S)\subseteq S$，$B_S$是$(A^A,+,\cdot)$的一个子环。

15. 设F是数域，$F[x]$是F上未知量x的多项式环，对$F[x]$规定结合法$\circ$：

$$f(x)\circ g(x)=f(g(x))$$

问$(F[x],+,\circ)$是否是一个环？环中哪些算律不成立？

解 $(F[x],+,\circ)$不能作成一个环。例如，命$f(x)=x+1$，$g(x)=h(x)=x$。易知，$[f\circ(g+h)](x)=2x+1$，而$(f\circ g+f\circ h)(x)=2x+2$。$\therefore f\circ(g+h)\neq f\circ g+f\circ h$，左分配律不成立。但是，容

易验证右分配律及乘法结合律成立。

16*。 设 S 是域 F 的一个非零子环，证明，S 是子域的充要条件是：对任意的 $x\in S, x\neq 0$，均有 $x^{-1}\in S$。

证 先证必要性。若 S 是子域，则对于任意的 $x\in S, x\neq 0$，有 $x\in$ 乘法群 S^*，$\therefore$ 必有 $x^{-1}\in S^*\subseteq S$，即 $x^{-1}\in S$。

再证充分性。若对于任意的 $x\in S, x\neq 0$，均有 $x^{-1}\in S$，则显然 $1=xx^{-1}\in S$，且 S 中的非零元全体作成一个乘法群，$\therefore S$ 为除环。但 $S\subseteq$ 域 F，交换律在 S 中成立，$\therefore S$ 是域 F 的子域。

§2 理想与商环

1。 设环 A 有幂等元 e：$e^2=e$，且 $e\neq 0$，则

$$L=\{x-xe\mid x\in A\}$$

是 A 的一个左理想。

证 任取 $a,b\in L$，则有 $x_1,x_2\in A$，使得 $a=x_1-x_1e$，$b=x_2-x_2e$，$\therefore a-b=(x_1-x_1e)-(x_2-x_2e)$

$=(x_1-x_2)-(x_1-x_2)e\in L$。$\therefore L$ 是 $(A,+)$ 的一个加法子群。

再任取 $x\in A$，$xa=x(x_1-x_1e)=xx_1-(xx_1)e\in L$，$\therefore AL=L$，$L$ 是 A 的一个左理想。

注 本题中“e 是幂等元”这一条件是多余的。

2。 找出 $\mathbf{Z}_6$ 的所有理想。

解 $\mathbf{Z}_6=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$。先证明 $\mathbf{Z}_6$ 中的任一理想均为主理想。

在 $\mathbf{Z}_6$ 中，规定 $\bar{0}<\bar{1}<\bar{2}<\bar{3}<\bar{4}<\bar{5}$。设 B 是 $\mathbf{Z}_6$ 的任一理想，$B\neq\{\bar{0}\}$，则 B 中不等于 $\bar{0}$ 的元素中必有一“最小的”，设为 $\bar{a}$，$1\leqslant a\leqslant 5$，则有 $(\bar{a})\subseteq B$。任取 $\bar{b}\in B$，$0\leqslant b\leqslant 5$，设 $b=ag+r$，

$0 \leqslant r < a$, $\bar{r} = \bar{b} - \overline{ag} \in B$. 由$\bar{a}$为$B$中$\neq \bar{0}$的元素中之最小者，可知，$\bar{r} = \bar{0}$，即$r = 0$. $\therefore \bar{b} = \overline{ag} \in (\bar{a})$，那么$(\bar{a}) = B$. 即$\mathbf{Z}_6$中的任一理想都是主理想.

$\therefore \mathbf{Z}_6$中的所有的理想是：$\{\bar{0}\}$，$\mathbf{Z}_6 = (\bar{1}) = (\bar{5})$，$(\bar{2}) = (\bar{4})$，$(\bar{3})$，共有四个不同的理想.

3. 设F是域，问多项式环$F[x]$的主理想(x^2)含有哪些元？$F[x]/(x^2)$含有哪些元？

解 $\because F(x)$是含1的可换环. $\therefore (x^2) = \{f(x) \cdot x^2 \mid f(x) \in F[x]\}$，即$(x^2)$中的元素是$F[x]$中所有次数$\geqslant 2$的多项式，此外还有0.

任取$f(x) \in F[x]$，必有$f(x) = g(x) \cdot x^2 + ax + b$，$\therefore f(x) \equiv ax + b((x^2))$，其中$a, b \in F$. 易知，当且仅当$a_1 = a_2, b_1 = b_2$时，$a_1 x + b_1 \equiv a_2 x + b_2$ $((x^2))$. $\therefore F[x]/(x^2) = \{\overline{ax+b} \mid a, b \in F\}$，其中$\overline{ax+b} = ax + b + (x^2)$.

4. 在实数域上x, y的多项式环$\mathbf{R}[x, y]$中，下面集合哪些是$\mathbf{R}[x, y]$的理想？

a) 一切常数项为零的多项式$f(x, y)$所成集合.

b) 一切不含x的多项式$f(x, y)$所成的集合.

c) 一切$f(x, y)$，其常数项和一次项系数均为零.

d) 一切$f(x, y)$，其二次项系数均为零.

解 *a*) 按理想的定义，易证得，这是$R[x, y]$的理想.

b) 设这个集合为$S = \{f(y) \mid f(y) \in R[y]\}$. 则它不是$R[x, y]$的理想. 因为，取$g(x, y) \in R[x, y]$，$g(x, y)$中含$x$. 取$f(y) \in S$，$f(y) \neq 0$. 则$g(x, y) f(y)$中含$x$，它不属于$S$，$\therefore R[x, y] \cdot S$不属于$S$. S不是$R[x, y]$的理想.

c) 按理想的定义，易证得，它是$R[x, y]$的理想.

d) 设此集合为S，则S不是$R[x,y]$的理想.这是因为，取$x\in S$,及$x\in R[x,y]$,则$x\cdot x=x^2\notin S$.这说明$R[x,y]\cdot S\subseteq S$及$S\cdot R[x,y]\subseteq S$未必成立. $\therefore S$不是$R[x,y]$的理想.

5. 设A_1,B_1是环A的两个理想，证明$A_1\cap B_1$是A的一个理想.设$\{A_\alpha|\alpha\in B\}$是A的理想的族，证明 $\bigcap\limits_{\alpha\in B}A_\alpha$仍是$A$的理想

证 $\because A_1,B_1$是环A的两个理想，$\therefore A_1,B_1$是A的子环，从而$A_1\cap B_1$也是A的子环，而且$A_1A\subseteq A_1$,$AA_1\subseteq A_1$; $B_1A\subseteq B_1$,$AB_1\subseteq B_1$. $\because A(A_1\cap B_1)\subseteq AA_1\subseteq A_1$,$A(A_1\cap B_1)\subseteq AB_1\subseteq B_1$, $\therefore A(A_1\cap B_1)\subseteq A_1\cap B_1$.同理$(A_1\cap B_1)A\subseteq A_1\cap B_1$. $\therefore A_1\cap B_1$是A的一个理想.

$\because\{A_\alpha|\alpha\in B\}$是$A$的理想的族，$\therefore$对于每一个$A_\alpha$，$A_\alpha$是$A$的子环，且$AA_\alpha\subseteq A_\alpha$,$A_\alpha A\subseteq A_\alpha$. 由$A_\alpha$是$A$的子环知$\bigcap\limits_{\alpha\in B}A_\alpha$仍是$A$的子环. 由$AA_\alpha\subseteq A_\alpha$知，$A(\bigcap\limits_{\alpha\in B}A_\alpha)\subseteq AA_\alpha\subseteq A_\alpha$, $\therefore A(\bigcap\limits_{\alpha\in B}A_\alpha)\subseteq\bigcap\limits_{\alpha\in B}A_\alpha$.同理$(\bigcap\limits_{\alpha\in B}A_\alpha)A\subseteq\bigcap\limits_{\alpha\in B}A_\alpha$. $\therefore\bigcap\limits_{\alpha\in B}A_\alpha$是$A$的理想.

6. 设A_i是环A的理想，$i=1,2,3\cdots$并且$A_1\subseteq A_2\subseteq\cdots\subseteq A_n\subseteq\cdots$，证明

$$A'=\bigcup_{i=1}^{\infty}A_i \quad \text{是}A\text{的理想.}$$

证 任取$a,b\in A'=\bigcup\limits_{i=1}^{\infty}A_i$，则必存在正整数$m,n$，使得$a\in A_m,b\in A_n$.取$k=max\{m,n\}$. $\because A_m\subseteq A_k$,$A_n\subseteq A_k$, $\therefore a,b\in A_k$，而A_k是环A的理想，$\therefore a-b\in A_K\subseteq\bigcup\limits_{i=1}^{\infty}A_i=A'$.

任取$a\in A'=\bigcup\limits_{i=1}^{\infty}A_i$, $x\in A$, 必存在正整教m，使得$a\in A_r$,

而A_m是A的理想，$\therefore ax\in A_m\subseteq\bigcup_{i=1}^{\infty}A_i=A'$，$xa\in A_m\subseteq A'$，

故$A'=\bigcup_{i=1}^{\infty}A_i$是$A$的理想。

7. 设A_1，A_2是环A的两个理想，证明，$A_1A_2\subseteq A_1\cap A_2$。举例说明，$A_1A_2$可以真包含于$A_1\cap A_2$中。

证 $\because A_1$和A_2分别是环A的两个理想，$\therefore A_1A_2\subseteq A_2$，$A_1A_2\subseteq A_1$，故$A_1A_2\subseteq A_1\cap A_2$。

A_1A_2可以真包含于$A_1\cap A_2$中。例如，在整数环$\mathbf{Z}$中，$A_1=(2)=\{2x|x\in\mathbf{Z}\}$和$A_2=(4)=\{4x|x\in\mathbf{Z}\}$都是$\mathbf{Z}$的理想，易得出，$A_1A_2=(8)=\{8x|x\in Z\}$，$A_1\cap A_2=(4)=\{4x|x\in\mathbf{Z}\}$。显然，$A_1A_2$真包含于$A_1\cap A_2$。

8. 在例7中，命$A_1=\left\{\begin{pmatrix}0&2x\\0&0\end{pmatrix}\middle|\,x\in\mathbf{Z}\right\}$。证明，$A_1$是$A$的理想。商环$A/A_1$由哪些元素组成？

证 任取$a=\begin{pmatrix}0&2x\\0&0\end{pmatrix}\in A_1$，$b=\begin{pmatrix}0&2y\\0&0\end{pmatrix}\in A_1$。任取$x=\begin{pmatrix}\alpha&\beta\\0&\gamma\end{pmatrix}\in A$。其中$x,y,\alpha,\beta,\gamma\in Z$。则

$$a-b=\begin{pmatrix}0&2x\\0&0\end{pmatrix}-\begin{pmatrix}0&2y\\0&0\end{pmatrix}=\begin{pmatrix}0&2(x-y)\\0&0\end{pmatrix}\in A_1,$$

$$xa=\begin{pmatrix}\alpha&\beta\\0&\gamma\end{pmatrix}\begin{pmatrix}0&2x\\0&0\end{pmatrix}=\begin{pmatrix}0&2(\alpha x)\\0&0\end{pmatrix}\in A_1,$$

$$ax=\begin{pmatrix}0&2x\\0&0\end{pmatrix}\begin{pmatrix}\alpha&\beta\\0&\gamma\end{pmatrix}=\begin{pmatrix}0&2(x\gamma)\\0&0\end{pmatrix}\in A_1.$$

$\therefore A_1$是A的理想。

任取$\begin{pmatrix}\alpha&\beta\\0&\gamma\end{pmatrix}\in A$，其中$\alpha,\beta,\gamma\in\mathbf{Z}$。如果$\beta=2\delta$，$\delta\in\mathbf{Z}$，则

$\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \gamma \end{pmatrix} + \begin{pmatrix} 0 & 2\delta \\ 0 & 0 \end{pmatrix}$，从而$\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \equiv \begin{pmatrix} \alpha & 0 \\ 0 & \gamma \end{pmatrix} (A_1)$；

如果$\beta = 2\delta + 1, \delta \in \mathbf{Z}$，则$\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} = \begin{pmatrix} \alpha & 1 \\ 0 & \gamma \end{pmatrix} + \begin{pmatrix} 0 & 2\delta \\ 0 & 0 \end{pmatrix}$，从而

$\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \equiv \begin{pmatrix} \alpha & 1 \\ 0 & \gamma \end{pmatrix} (A_1)$，显然，若$\alpha \neq \alpha'$，或$\gamma \neq \gamma'$，则$\begin{pmatrix} \alpha & e_1 \\ 0 & \gamma \end{pmatrix} \not\equiv \begin{pmatrix} \alpha' & e_2 \\ 0 & \gamma' \end{pmatrix} (A_1)$，其中$e_1, e_2 = 0, 1$. $\therefore A/A_1 = \left\{ \overline{\begin{pmatrix} \alpha & \varepsilon \\ 0 & \gamma \end{pmatrix}} \middle| \alpha, \gamma \in \mathbf{Z}, e = 0 \text{ 或 } 1 \right\}$，其中$\overline{\begin{pmatrix} \alpha & \varepsilon \\ 0 & \gamma \end{pmatrix}} = \begin{pmatrix} \alpha & \varepsilon \\ 0 & \gamma \end{pmatrix} + A_1$.

9. 设$A = (\mathbf{Z})_3$是整数环$\mathbf{Z}$上3阶方阵环，证明

$$B = \left\{ \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} \middle| a, b, c \in \mathbf{Z} \right\}$$

是A的一个子环. B是不是A的理想？求$B^2 = ?$ $B^3 = ?$

证 任取$\alpha = \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} \in B$和$\beta = \begin{pmatrix} 0 & d & e \\ 0 & 0 & f \\ 0 & 0 & 0 \end{pmatrix} \in B$，则

$$\alpha - \beta = \begin{pmatrix} 0 & a-d & b-e \\ 0 & 0 & c-f \\ 0 & 0 & 0 \end{pmatrix} \in B, \qquad \alpha \cdot \beta = \begin{pmatrix} 0 & 0 & af \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in B,$$

$\therefore B$是A的一个子环.

B不是A的理想. 例如取$x = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \in A$,

$$a = \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} \in B, \text{ 其中 } a \neq 0. \text{ 则}$$

$$xa = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a & b+c \\ 0 & a & b+c \\ 0 & a & b+c \end{pmatrix} \notin B. \text{ 故 } AB \text{ 不属于 } B.$$

∵上面已证得，对于任意的$\alpha,\beta\in B$，

总有$\alpha\beta=\begin{pmatrix}0&0&af\\0&0&0\\0&0&0\end{pmatrix}$，$\therefore B^2\subseteq\left\{\begin{pmatrix}0&0&a\\0&0&0\\0&0&0\end{pmatrix}\middle|a\in\mathbf{Z}\right\}$.

另一方面总有$\begin{pmatrix}0&0&a\\0&0&0\\0&0&0\end{pmatrix}=\begin{pmatrix}0&a&*\\0&0&*\\0&0&0\end{pmatrix}\begin{pmatrix}0&*&*\\0&0&1\\0&0&0\end{pmatrix}\in B^2$.

$$\therefore B^2=\left\{\begin{pmatrix}0&0&a\\0&0&0\\0&0&0\end{pmatrix}\middle|a\in\mathbf{Z}\right\}.$$

任取$\begin{pmatrix}0&0&a\\0&0&0\\0&0&0\end{pmatrix}\in B^2$，$\begin{pmatrix}0&f&g\\0&0&h\\0&0&0\end{pmatrix}\in B$，

$$\begin{pmatrix}0&0&a\\0&0&0\\0&0&0\end{pmatrix}\cdot\begin{pmatrix}0&f&g\\0&0&h\\0&0&0\end{pmatrix}=\begin{pmatrix}0&0&0\\0&0&0\\0&0&0\end{pmatrix}.\quad\therefore B^3=\left\{\begin{pmatrix}0&0&0\\0&0&0\\0&0&0\end{pmatrix}\right\}.$$

10. 举一个环A的例子，A含有子环$B\neq 0$，$B^n\neq 0$，但$B^{n+1}=0$.

解 设$A=(\mathbf{Z})_{n+1}$是整数环$\mathbf{Z}$上$(n+1)$阶方阵环. 命

$$B=\left\{\begin{pmatrix}0&a_{12}&a_{13}&\cdots&a_{1n}&a_{1n+1}\\0&0&a_{23}&\cdots&a_{2n}&a_{2n+1}\\\cdots&\cdots&\cdots&\cdots&\cdots&\cdots\\0&0&0&\cdots\cdots&0&a_{nn+1}\\0&0&0&\cdots\cdots&0&0\end{pmatrix}\middle|\text{其中}a_{ij}\in\mathbf{Z}\right\}$$

容易验证，B是A的子环，$B\neq 0$，$B^n\neq 0$，但$B^{n+1}=0$.

11. 设p,g是两个素数，$(p)\cap(g)$是整数环$\mathbf{Z}$的怎样一个理想？$(p)(g)$是$\mathbf{Z}$的怎样一个理想？

解 当$p=g$时，易证$(p)\cap(g)=(p)$，$(p)(g)=(p^2)$。

若$p\neq g$，任取$x\in(p)\cap(g)$，则$x\in(p)$，$x\in(g)$，$\therefore p|x, g|x$。但$(p,g)=1$，$\therefore pg|x$，$x\in(pg)$。$\therefore(p)\cap(g)\subseteq(pg)$，另一方面，显然$(pg)\subseteq(p)$，$(pg)\subseteq(g)$，$\therefore(pg)\subseteq(p)\cap(g)$。

$\therefore(p)\cap(g)=(pg)$。

任取$x\in(pg)$，$x=a\cdot pg=ap\cdot g\in(p)(g)$，$\therefore(pg)\subseteq(p)(g)$。但由第7题结果知，$(p)(g)\subseteq(p)\cap(g)=(pg)$，

$\therefore(p)\cdot(g)=(pg)$

$\therefore$当$p\neq g$，p,g为素数时，$(p)\cap(g)=(p)\cdot(g)=(pg)$。

12. 设L是环A的一个左理想，证明，L的左零化子$A_1=\{x|x\in A, xL=0\}$是A的一个理想。

证 任取$x,y\in A$，$(x-y)L\subseteq xL-yL=0$，$\therefore x-y\in A_1$，$\forall a\in A$，$(ax)L=a(xL)=a\cdot 0=0$，$\therefore ax\in A_1$，$\therefore L$是环A的一个左理想，$\because$对于任意的$a\in A$，$aL\subseteq L$，于是，$(xa)L=x(aL)\subseteq xL=0$，$xa\in A$。

综上A_1是A的一个理想。

13. 设L是环A的一个左理想，命

$$(L:A)=\{x|x\in A, xA\subseteq L\}。$$

证明$(L:A)$是A的理想，并且，对于A的左理想族$\{L_\alpha|\alpha\in B\}$来说，有 $\left(\bigcap_{\alpha\in B}L_\alpha : A\right)=\bigcap_{\alpha\in B}(L_\alpha:A)$。

证 (1)任取$x,y\in(L:A)$，$xA\subseteq L$，$yA\subseteq L$。$\therefore(x-y)A\subseteq xA-yA\subseteq L$，$x-y\in(L:A)$。

对于任意的$a\in A$，$aL\subseteq L$，$\therefore(ax)A=a(xA)\subseteq aL\subseteq L$；$(xa)A=x(aA)\subseteq xA\subseteq L$。$\therefore ax, xa\in(L:A)$，$(L:A)$是$A$的理想。

(2)任取$x\in(\bigcap\limits_{\alpha\in B}L_\alpha:A)$，　则$x\in A, xA\subseteq\bigcap\limits_{\alpha\in B}L_\alpha$，$\therefore x\in A$，$xA\subseteq L_\alpha, \forall\alpha\in B$，即$x\in(L_\alpha:A), \forall\alpha\in B$，从而，$x\in\bigcap\limits_{\alpha\in B}(L_\alpha:A)$。

$(\bigcap\limits_{\alpha\in B}L_\alpha:A)\subseteq\bigcap\limits_{\alpha\in B}(L_\alpha:A)$。

任取$x\in\bigcap\limits_{\alpha\in B}(L_\alpha:A)$，则$x\in(L_\alpha:A), \forall\alpha\in B$。$\therefore x\in A$，$xA\subseteq L_\alpha, \forall\alpha\in B$。$\therefore x\in A, xA\subseteq\bigcap\limits_{\alpha\in B}L_\alpha$，即$x\in(\bigcap\limits_{\alpha\in B}L_\alpha:A)$。

$\therefore\bigcap\limits_{\alpha\in B}(L_\alpha:A)\subseteq(\bigcap\limits_{\alpha\in B}L_\alpha:A)$。则证得$(\bigcap\limits_{\alpha\in B}L_\alpha:A)=\bigcap\limits_{\alpha\in B}(L_\alpha:A)$。

14。　设$I=\mathbf{Z}\times\mathbf{Z}$。$\mathbf{Z}$为整数环。证明，$A=\{(0,y)\mid y\in\mathbf{Z}\}$是$I$的一个理想。问$A$的左零化子

$$B=\{x\mid x\in A, xA=0\}$$

是怎样一个理想？$A\cap B=?$　$A+B=?$

证　① 任取$(0,x),(0,y)\in A$，则$(0,x)-(0,y)=(0,x-y)\in A$，又任取$(a,b)\in A$，则$(a,b)(0,x)=(0,bx)\in A$，$(0,x)(a,b)=(0,xb)\in A$，$\therefore A$是I的一个理想。

② 任取$x\in B$，则$x\in I, xA=0$。$\because x\in I$，$\therefore x=(x_1,x_2)$，其中$x_1,x_2\in\mathbf{Z}$。$\because xA=0, (0,1)\in A$，$\therefore(x_1,x_2)\cdot(0,1)=(0,0)$，即$(0,x_2)=(0,0)$，$\therefore x_2=0, x=(x_1,0)$，子是$B\subseteq\{(x,0)\mid x\in\mathbf{Z}\}$。然而，显然$(x,0)$是$A$的左零化子，$\{(x,0)\mid x\in\mathbf{Z}\}\subseteq B$。$\therefore A$的左零化子$B=\{(x,0)\mid x\in\mathbf{Z}\}$。

③ 任取$a=(x,y)\in A\cap B$。$\because(x,y)\in A$，$\therefore x=0$，又$\because(x,y)\in B$，因此$y=0$。$\therefore a=(0,0)$，$A\cap B=\{(0,0)\}$。

④ $A+B=\{(x,y)\mid x,y\in\mathbf{Z}\}=A$。

15。　举例说明一个没有零因子的环A，其剩余类环可能有零因子。

解　整数环$\mathbf{Z}$是一个没有零因子的环。取$A=\mathbf{Z}$，

$(15)=\{15n|n\in\mathbf{Z}\}$是它的一个理想。容易知道，$A$关于这个理想的剩余类环$A/(15)=\mathbf{Z}/(15)$就含零因子。例$\bar{3}\cdot\bar{3}+(15)$就是它的一个零因子。

16。 设F是一个域，找出F的所有理想。

解 只含一个零元素的集合$\{0\}$为F的一个理想。

设 B是F的一个理想，$B\neq\{0\}$，则至少有一个元素$b\in B$，而$b\neq 0$，$\because F$是域，$\therefore b^{-1}\in F$，$\because B$是域F的理想，$b^{-1}\in F$，$b\in B$，$b^{-1}b\in B$，即$1\in B$。$\therefore$对于任意的$a\in F$，$a=a\cdot 1\in B$，从而，$B=F$。

$\therefore$域F的理想只有零理想及F本身。

17。 设$(A,+,\cdot)$是一个环，A_1是A的一个理想，命$B=\{f|f\in A^A, f(A_1)\subseteq A_1\}$，证明，$B$是$(A^A,+,\cdot)$（$A^A$的$+,\cdot$的定义见练习（一）第14题）的一个理想。

证 由练习一中的第14题知，B是一个子环。

任取$h\in A^A$，$f\in B$，则$hf\in A^A$，且 $(hf)(a)=h(a)\cdot f(a)\in A\cdot A_1\subseteq A_1$，$\forall a\in A$。$\therefore (hf)(A_1)\subseteq A_1$，$hf\in B$。同样地，$fh\in B$。$\therefore B$是 $(A^A,+,\cdot)$的一个理想。

18。 在高斯整数环$\mathbf{Z}[i]$中，$A=(2+i)$含有哪些元？$\mathbf{Z}[i]/(2+i)$含有哪些元？

解 (1) 设$x=a+bi\in(2+i)$，则$a+bi=(\alpha+\beta i)(2+i)$
$=(2\alpha-\beta)+(\alpha+2\beta)i$。$\therefore a=2\alpha-\beta$，$b=\alpha+2\beta$，而$2a+b=5\alpha$是5的整数倍。$\therefore$ $(2+i)\subseteq\{a+bi|a,b\in\mathbf{Z}$，且$2a+b$是5的整数倍$\}$。

当$2a+b=5k$，k为整数时，$a+bi=a+(5k-2a)i=$
$=[k+(2k-a)i](2+i)\in(2+i)$。$\therefore\{a+bi|a,b\in\mathbf{Z}$，且$2a+b$是5的整数倍$\}\subseteq$ $(2+i)$。

$\therefore A=(2+i)=\{a+bi|a,b\in\mathbf{Z}$，且$2a+b$是5的整数倍$\}$。

(2) 任取$x=a+bi\in\mathbf{Z}[i]$。$\because a+bi=(a-2b)+b(2+i)$
$\therefore a+bi\equiv a-2b(A)$。 设$a-2b=5k+d$,其中$k,d\in\mathbf{Z}$,$0\leqslant d<5$。
$\because 5=(2-i)(2+i)\in A$,$\therefore a-2b\equiv d(A)$, $a+bi\equiv d(A)$, 其中,
$d=0,1,2,3,4$。又$i\neq j(A)$,当$i,j=0,1,2,3,4$,$i\neq j$时。$\therefore \mathbf{Z}[i]/(2+i)=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\}$,其中$\bar{d}=d+(2+i)$,$d=0,1,2,3,4$。

19。 证明, 域F上n阶方阵环$(F)_n$的每一个不是左零因子的方阵均是可逆方阵。

证 设$A=(a_{ij})\in(F)_n$,A不是左零因子。

假如A不是可逆方阵, 则方程组
$a_{i1}x_1+a_{i2}x_2+\cdots+a_{in}x_n=0$,$i=1,2,\cdots,n$, 在域$F$中有非零解。设$\beta_1,\beta_2\cdots,\beta_n$是一个非零解,

取 $B=\begin{pmatrix}\beta_1 & 0 & \vdots & 0\\ \beta_2 & 0 & \vdots & 0\\ \vdots & \vdots & \vdots & \vdots\\ \beta_n & 0 & \vdots & 0\end{pmatrix}$,则$B\neq 0$,但$AB=0$,$\therefore A$是左零因子。与已知$A$不是左零因子矛盾。$\therefore A$必是可逆方阵。

§3 环的同态 同态基本定理

1。 设A是例3给出的环。证明$A_1=\left\{\begin{pmatrix}0 & 0\\ 0 & x\end{pmatrix}\middle| x\in\mathbf{Z}\right\}$是$A$的子环。找出$A$到$A_1$的一个满同态$f$,并求出$\ker f$。

A_1是不是A的理想? 是不是A的右理想?

解 (1) 任取$\begin{pmatrix}0 & 0\\ 0 & x\end{pmatrix}$, $\begin{pmatrix}0 & 0\\ 0 & y\end{pmatrix}\in A_1$, 则$\begin{pmatrix}0 & 0\\ 0 & x\end{pmatrix}-\begin{pmatrix}0 & 0\\ 0 & y\end{pmatrix}$
$=\begin{pmatrix}0 & 0\\ 0 & x-y\end{pmatrix}\in A_1$; $\begin{pmatrix}0 & 0\\ 0 & x\end{pmatrix}\begin{pmatrix}0 & 0\\ 0 & y\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & xy\end{pmatrix}\in A_1$,$\therefore$ A_1是A的子

环。

(2) $f:\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\longmapsto\begin{pmatrix} 0 & 0 \\ 0 & c \end{pmatrix}$。则容易验证，$f$是$A$到$A_1$的一个满同态。

$$\ker f=\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\middle|\ c=0\right\}=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\middle|\ a,b\in\mathbf{Z}\right\}.$$

(3) 任取$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\in A$，$\begin{pmatrix} 0 & 0 \\ 0 & x \end{pmatrix}\in\mathbf{Z}$。

则$\begin{pmatrix} 0 & 0 \\ 0 & x \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & xc \end{pmatrix}\in A_1$。但取$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\in A$，$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\in A_1$。

则$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\notin A_1$。$\therefore A_1$不是$A$的理想，但$A_1$是$A$的右理想。

2。 设A是整数环$\mathbf{Z}$上二阶方阵环。I是元素为偶数的所有二阶方阵所成的集合。证明，I是A的一个理想。问A/I含有多少个元素？

证 (1) $I=\left\{\begin{pmatrix} 2a & 2b \\ 2c & 2d \end{pmatrix}\middle|\ a,b,c,d\in\mathbf{Z}\right\}$，按理想的定义，容易验证$I$是$A$的一个理想。

(2) 记$\overline{a}$是$\mathbf{Z}/(2)$中a所在的剩余类。作f：$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\longmapsto\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$，则容易验证，$f$是环$A$到环$\overline{A}=\left\{\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}\middle|\ \overline{a}$，$\overline{b}$，$\overline{c}$，$\overline{d}$分别是$a,b,c,d$所在的剩余类$\right\}$的满同态，且$\ker f=I$。$\therefore A/I\cong\overline{A}$。 而$Z/(2)$的剩余类只有$\overline{0}$或$\overline{1}$。$\therefore\overline{A}$中的元素个数为16。从而$A/I$含有16个元素。

3*。 设$A=\mathbf{Z}\times\mathbf{Z}$关于以下定义的加法、乘法作成的环：$(a,b)+(c,d)=(a+c,b+d)$，$(a,b)(c,d)=(ac,bd)$，命$f:(a,b)\longmapsto a$，证明，$f$是$A$到$\mathbf{Z}$的一个同态映射，求$\ker f$=？

$A/Kerf$是怎样的一个环?

证 (1) $\because (a,b)\mid\!\!\to a,(c,d)\longmapsto c$, $\therefore f((a,b)+(c,d))$
$=f((a+c,b+d))=a+c=f((a,b))+f((c,d))$.
$f((a,b)\cdot(c,d))=f((ac,bd))=ac=f((a,b))\cdot f((c,d))$.
$\therefore f$是A到Z的一个同态映射(且是满同态).

(2) 容易知道,$kerf=\{(a,b)\mid a=0\}=\{(0,b)\mid b\in\mathbf{Z}\}$,

(3) $A/Kerf$是与环$\mathbf{Z}$同构的一个环.

4. 设A是偶数环,$I=\{4x\mid x\in\mathbf{Z}\}$,证明$I$是$A$的一个理想. A/I是怎样的环? I是否就是(4)? $A/(4)$是不是域?

解 (1) 按照理想的定义,容易验证 I 是A的一个理想.

(2) $\because A=\{2x\mid x\in\mathbf{Z}\}$,当$x$为奇数时,$2x\equiv 2\ (I)$; 当$x$为偶数时,$2x\equiv 0\ (I)$. $\therefore A/I=\{\bar{0},\bar{2}\}$,运算表为

+	$\bar{0}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{2}$
$\bar{2}$	$\bar{2}$	$\bar{0}$

·	$\bar{0}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{2}$	$\bar{0}$	$\bar{0}$

(3) $\because (4)=\{4m+4y\mid m\in\mathbf{Z},y\in A\}$. 任取$4x\in I$,其中$x\in\mathbf{Z}$,则$4x=4x+4\times 0\in(4)$, $\therefore I\subseteq(4)$;任取$4m+4y\in(4)$,其中$m\in\mathbf{Z}$, $y\in A$. 则$4m+4y=4(m+y)\in I$, $(4)\subseteq I$. $\therefore I=(4)$.

(4) $A/(4)=A/I$. 由(2)中运算表可知,A/I有零因子,不成域, 即$A/(4)$不成为域.

5. 证明(3)/(6)是$\mathbf{Z}/(6)$的理想,且$\mathbf{Z}/(6)/(3)/(6)\cong\mathbf{Z}/(3)$

证 命$f:a+(6)\longmapsto a+(3)$, $\forall a\in\mathbf{Z}$. 当$a+(6)=b+(6)$时, $a-b\in(6)\subset(3)$, $a+(3)=b+(3)$. $\therefore f$是$\mathbf{Z}/(6)$到$\mathbf{Z}/(3)$的一个映射, 且是满射. 易证,f是$\mathbf{Z}/(6)$到$\mathbf{Z}/(3)$的满同态映射.

取$x+(6)\in kerf$。则$x+(3)=(3)$，$x\in(3)$，$\therefore kerf\subseteq(3)/(6)$；显然$(3)/(6)\subseteq kerf$，$\therefore kerf=(3)/(6)$。

由同态基本定理知，$(3)/(6)$是$\mathbf{Z}/(6)$的理想，且$\mathbf{Z}/(6)/(3)/(6)\cong\mathbf{Z}/(3)$。

6. 设m,r是取定的正整数，且$r|m$。用符号$\overline{a}$表示$\mathbf{Z}_m$中a所在的剩余类，$[a]$表示$\mathbf{Z}_r$中a所在剩余类，命$f:\ \overline{a}\longmapsto[a]$，证明，$f$是$\mathbf{Z}_m$到$\mathbf{Z}_r$的同态映射，求$kerf=?$ $\mathbf{Z}_m/kerf$是怎样的环？

解 (1) $\because r|m$，$\therefore$任取$x\in(m)$，则$m|x$，从而$r|x$，$x\in(r)$ $\therefore(m)\subseteq(r)$。

$f:\ \overline{a}\longmapsto[a]$。当$\overline{a}=\overline{b}$时，$\overline{a-b}=\overline{0}$，即$a-b\in(m)\subseteq(r)$。$\therefore[a]=[b]$。$\therefore f$是$\mathbf{Z}_m$到$\mathbf{Z}_r$的一个映射，且是满射。

$\because\overline{a}+\overline{b}=\overline{a+b}\longmapsto[a+b]=[a]+[b]$，$\overline{a}\cdot\overline{b}=\overline{ab}\longmapsto[ab]=[a][b]$，$\therefore f$是$\mathbf{Z}_m$到$\mathbf{Z}_r$的同态映射。

(2) $kerf=\{\overline{a}\mid[a]=[0]\}$，而$[a]=[0]\Longleftrightarrow a\in(r)$，$\therefore kerf=\{\overline{a}\mid a\in(r)\}=(r)/(m)$。

(3) 由同态基本定理，$\mathbf{Z}_m/kerf\cong\mathbf{Z}_r$。

7. 设$f(x)\in\mathbf{R}[x]$，$f(x)=a_0+a_1x+\cdots\cdots+a_nx^n$，命

$$f:\ f(x)\longmapsto a_0.$$

证明，f是$\mathbf{R}[x]$到$\mathbf{R}$的满同态，求$kerf=?$ $\mathbf{R}[x]/kerf$与怎样的环同构？

解 (1) 显然，f是$\mathbf{R}[x]$到$\mathbf{R}$的一个满映射。

任取$f(x),g(x)\in\mathbf{R}[x]$，设$f(x)=a_0+a_1x+\cdots+a_nx^n$，$g(x)=b_0+b_1x+\cdots b_nx^m$。则$f(x)+g(x)=(a_0+b_0)+(a_1+b_1)x+\cdots$，$f(x)\cdot g(x)=a_0b_0+(a_0b_1+a_1b_0)x+\cdots$。于是，$f(f(x)+g(x))=a_0+b_0=f(f(x))+f(g(x))$，$f(f(x)g(x))$

$=a_0b_0=f(f(x))\cdot f(g(x))$。$\therefore f$是$\mathbf{R}[x]$到$\mathbf{R}$的一个同态满射。

(2) $kerf=\{a_1x+\cdots+a_nx^n\mid a_i\in\mathbf{R}\}=(x)$。

(3) $\mathbf{R}[x]/kerf\cong\mathbf{R}$。

8。证明，高斯整数环$\mathbf{Z}[i]$同构于$\mathbf{Z}[x]/(x^2+1)$。

证 任取$f(x)\in\mathbf{Z}[x]$，则必存在$g(x)\in\mathbf{Z}[x]$，使得$f(x)=(x^2+1)\cdot g(x)+ax+b$，其中$a,b\in\mathbf{Z}$。

命τ：$\mathbf{Z}[x]\longrightarrow\mathbf{Z}[i]$，$f(x)=(x^2+1)\cdot g(x)+ax+b\longmapsto f(i)=ai+b$。容易知道，$\tau$是$\mathbf{Z}[x]$到$\mathbf{Z}[i]$的一个满射。且$\tau(f(x)+h(x))=f(i)+h(i)=\tau(f(x))+\tau(h(x))$，$\tau(f(x)\cdot h(x))=f(i)h(i)=\tau(f(x))\cdot\tau(h(x))$，$\forall f(y),g(x)\in\mathbf{Z}[x]$。$\therefore\tau$是$\mathbf{Z}[x]$到$\mathbf{Z}[i]$的一个满同态。显然，$ker\tau=(x^2+1)$。从而$\mathbf{Z}[i]\cong\mathbf{Z}[x]/(x^2+1)$。

9。 找出$\mathbf{Z}$到自身的一切同态映射，并找出每一同态的核。

解 设τ是$\mathbf{Z}$到自身的任一同态映射，则$\tau(m)=m\cdot\tau(1)$，$\forall m\in\mathbf{Z}$，且$\tau(1)=\tau(1\cdot1)=\tau(1)\cdot\tau(1)$。由$\tau(1)=\tau(1)\cdot\tau(1)$知$\tau(1)=0$或1。

若$\tau(1)=0$，则$\tau(m)=m\cdot\tau(1)=0$，$\forall m\in\mathbf{Z}$。$\therefore\tau$是零同态，显然，其核为$\mathbf{Z}$。

若$\tau(1)=1$，则$\tau(m)=m\cdot\tau(1)=m$，$\forall m\in\mathbf{Z}$，$\therefore\tau$为恒等同态。显然，其核为$\{0\}$。

$\because\tau$是任取的，$\therefore\mathbf{Z}$到自身的一切同态映射仅此两种：零同态或恒等同态，其核分别为$\mathbf{Z}$或$\{0\}$。

10。 设环A的子环仅有有限个，f是A到自身的满同态，证明，f是A的一个自同构。

证 $\because$当$x\in kerf^1$时，$f^1(x)=0$，$\therefore f^{1+1}(x)=f(0)=0$。

$\therefore x\epsilon kerf^{i+1}, i=1,2,3,\cdots\cdots, kerf\subseteq kerf^2\subseteq\cdots\cdots\subseteq kerf^i\subseteq kerf^{i+1}\subseteq\cdots\cdots$。但是$kerf^i$都是$A$的子环$(i=1,2,\cdots\cdots)$，而由题意，$A$的子环只有有限个。$\therefore$必存在正整数$n$，使得$kerf^n=kerf^{n+1}$。

$\because f$是A到自身的满射，$\therefore f(A)=A$。因而$A=f(A)=f^2(A)=\cdots=f^n(A)=f^{n+1}(A)=\cdots$。考察$A$到$A$的同态$f$的核$kerf$。任取$x\epsilon kerf$，则$x\epsilon A, f(x)=0$。但是$A=f^n(A)$，$\therefore$必存在一个$x'\epsilon A$，使得$x=f^n(x')$，$\therefore f^{n+1}(x')=f(x)=0$，$x'\epsilon kerf^{n+1}$。而$kerf^{n+1}=kerf^n$，$\therefore x'\epsilon kerf^n, f^n(x')=0$，亦即$x=f^n(x')=0$，$kerf=0$。$\therefore f$是$A$的一个自同构。

11. 找出$\mathbf{Z}_2$到$\mathbf{Z}$的一切同态映射。

解 设τ是$\mathbf{Z}_2$到$\mathbf{Z}$的任一个同态映射，并设$\tau(\bar{1})=n\epsilon\mathbf{Z}$。

$\because\tau(\bar{0})=0$，$\therefore\tau(\bar{1})+\tau(\bar{1})=\tau(\bar{1}+\bar{1})=\tau(\bar{0})=0$，$\therefore n+n=0$，$n=0$，即$\tau(\bar{1})=0$。$\therefore\mathbf{Z}_2$到$\mathbf{Z}$的同态映射只有$\tau=0$。

§4 分式环

1. 设A是一个环，命$\overline{A}$为整数环$\mathbf{Z}$与环A的加氏积，$\overline{A}=\mathbf{Z}\times A$，对$\overline{A}$规定加法与乘法：

$$(m,a)+(n,b)=(m+n,a+b),$$

$$(m,a)\cdot(n,b)=(mn,na+mb+ab).$$

证明，$\overline{A}$是一个有单位元的环，且$\overline{A}$含有子环与A同构。

证 (1) 容易验证$(\overline{A},+)$是一个可换加群。

$\because((m,a)(n,b))(g,c)=(mn,na+mb+ab)(g,c)$

$=((mn)g,g(na+mb+ab)+(mn)c+(na+mb+ab)c)$

$= (mng, nga + mgb + mnc + gab + mbc + nac + abc)$,

$(m,a)((n,b)(g,c)) = (m,a)(ng, gb + nc + bc)$

$= (mng, nga + mgb + mnc + gab + mbc + nac + abc)$.

$\therefore ((m,a)(n,b))(g,c) = (m,,a)((n,b),(g,c))$。乘法的结合律成立。

$\because (m,a)[(n,b) + (g,c)] = (m,a)(n+g, b+c)$

$= (mn+mg, mb + mc + na + ga + ab + ac)$,

$(m,a)(n,b) + (m,a)(g,c) = (mn, na + mb + ab)$

$+ (mg, ga + mc + ac) = (mn + mg, na + mb + ab + ga + mc + ac)$。

$\therefore (m,a)[(n,b) + g,c)] = (m,a)(n,b) + (m,a)(g,c)$。左分配律成立。同理可证右分配律成立。综上，$\overline{A}$成为环。

容易知道。$(1,0)$ 是$\overline{A}$中的单位元。

(2)取$A' = \{(0,a) \mid a \in A\}$。$\because (0,a) \pm (0,b) = (0, a \pm b)$，$(0,a)(0,b) = (0,ab)$，$\therefore A'$是$\overline{A}$的一个子环。

作τ：$(0,a) \longmapsto a$。则容易验证，τ是A'到A的一个同构映射。$\therefore \overline{A}$中的子环$A' = \{(0,a) \mid a \in A\}$与环$A$同构。

2。 在上题中，证明，整数环$\mathbf{Z}$可同构嵌入于$\overline{A}$中。

证 命$A'' = \{(m,0) \mid m \in \mathbf{Z}\}$，作$\eta: m \longmapsto (m,0)$。易验证，$\eta$是$\mathbf{Z}$到$A''$的一个同构映射，$Z \cong A''$。$\therefore$整数环$Z$可同构嵌入于$\overline{A}$中。

3。 设A是域，证明，A的分式域就是A本身。

证：设域A的分式域为 $F = \left\{ \frac{a}{b} \middle| a \in A, b \in A^* \right\}$，则$A \subseteq F$；$A = \left\{ \frac{au}{u} \middle| a \in A, u \in A^* \right\}$。任取$\frac{a}{b} \in F$，其中$a \in A$，$b \in A^*$，则有$c \in A$，使$a = cb$，$\frac{a}{b} = \frac{cb}{b} \in A$，$\therefore F \subseteq A$。因此，$F = A$。

4. 设A是一个有单位元1的可换环，S是A的一个有单位元1的乘法半群，$Q=A\times S$。对Q的元$(a,s),(a',s')$，若存在$s_1\in S$使$s_1(s'a-sa')=0$，则规定$(a,s)\sim(a',s')$，证明，$\sim$是Q的一个等价关系。

证 $\because 1\cdot(sa-sa)=0,\therefore(a,s)\sim(a,s)$。

当$(a,s)\sim(a',s')$时，存在$s_1\in S$，使得$s_1(s'a-sa')=0$。$\therefore s_1(sa'-s'a)=0$，$(a',s')\sim(a,s)$。

当$(a,s)\sim(a',s')$，$(a',s')\sim(a'',s'')$时，存在$s_1,s_2\in S$，使得$s_1(s'a-sa')=0$，$s_2(s''a'-s'a'')=0$。而A为可换环，$\therefore s_2s_1s''(s'a-sa')+ss_1s_2(s''a'-s'a'')=0$。整理后，即$s_1s_2s'(s''a-sa'')=0$。而$s_1s_2s\in S$，$\therefore(a,s)\sim(a'',s'')$。

综上，“$\sim$”是Q的一个等价关系。

5. 在上题中，若S含有A的零元，问$Q/\sim$含有几个元素

解 $\because 0\in S,\therefore(0,0)\in Q$。任取$(a,s)\in Q,s_1\in S$，总有$s_1(0\cdot a-s\cdot 0)=0,\therefore(a,s)\sim(0,0)$。$\therefore Q/\sim$只含一个元素$(0,0)$。

6. 在题4中，用记号$S^{-1}A$表示$Q/\sim$。(a,s)所在的类用记号$\frac{a}{s}$表示，规定$\frac{a}{s}\cdot\frac{a'}{s'}=\frac{aa'}{ss'}$。证明，上式定义出$S^{-1}A$的一个乘法，$S^{-1}A$关于这个乘法作成一个有单位元的半群。

证 $\because \frac{a}{s}\cdot\frac{a'}{s'}=\frac{aa'}{ss'}$，$\frac{b}{t}\cdot\frac{b'}{t'}=\frac{bb'}{tt'}$，若$\frac{a}{s}=\frac{b}{t}$，$\frac{a'}{s'}=\frac{b'}{t'}$，则由于$(a,s)\sim(b,t)$，$(a',s')\sim(b',t')$，存在$s_1,s_2\in S$，使得$s_1(ta-sb)=0,s_2(t'a'-s'b')=0$。$\therefore s_1s_2a't'(ta-sb)+s_1s_2bs(t'a'-s'b')=0$。亦即$s_1s_2(tt'aa'-ss'bb')=0$。$\therefore(aa',ss')\sim(bb,'tt')$，$\frac{aa'}{ss'}=\frac{bb'}{tt'}$。这样规定的乘法是

合理的。

$\left(\frac{a}{s}\cdot\frac{a'}{s'}\right)\cdot\frac{a''}{s''}=\frac{aa'}{ss'}\cdot\frac{a''}{ss''}=\frac{aa'a''}{ss's''}=\frac{a}{s}\cdot\frac{a'a''}{s's''}=\frac{a}{s}\cdot\left(\frac{a'}{s'}\cdot\frac{a''}{s''}\right)$，$\therefore S^{-1}A$关于这个乘法成为半群。

对于任意的$t\in S$，$\because 1\cdot(sat-st\cdot a)=0$，

$\therefore\frac{at}{st}=\frac{a}{s}$，即$\frac{a}{s}\cdot\frac{t}{t}=\frac{a}{s}$，$\frac{t}{t}$是$S^{-1}A$中的单位元。$\therefore S^{-1}A$作成一个有单位元$\frac{t}{t}$的乘法半群。

7．在$S^{-1}A$中，规定$\frac{a}{s}+\frac{a'}{s'}=\frac{s'a+sa'}{ss'}$。证明，上式定义出$S^{-1}A$的一个加法，$S^{-1}A$关于这个加法作成一个加群。

证 若$\frac{a}{s}+\frac{a'}{s'}=\frac{s'a+sa'}{ss'}$，$\frac{b}{t}+\frac{b'}{t'}=\frac{t'b+tb'}{tt'}$，而$\frac{a}{s}=\frac{b}{t}$，$\frac{a'}{s'}=\frac{b'}{t'}$时，则由于$(a,s)\sim(b,t)$，$(a',s')\sim(b',t')$，$\therefore$存在$s_1,s_2\in S$，使得$s_1(ta-sb)=0$；$s_2(t'a'-s'b')=0$。$\therefore s_2t's'\cdot s_1(ta-sb)+s_1ts\cdot s_2(t'a'-s'b')=0$。整理后得，$s_1s_2[tt'(s'a+sa')-ss'(t'b+tb')]=0$。

$\therefore(s'a+sa',ss')\sim(t'b+bt',tt')$，$\frac{s'a+sa'}{ss'}=\frac{t'b+tb'}{tt'}$，这样规定的加法是合理的。

$\frac{a}{s}+\frac{a'}{s'}=\frac{s'a+sa'}{s's}=\frac{sa'+s'a}{s's}=\frac{a'}{s'}+\frac{a}{s}$，$\left(\frac{a}{s}+\frac{a'}{s'}\right)+\frac{a''}{s''}=\frac{s''s'a+s''sa'+ss'a''}{ss's''}=\frac{a}{s}+\left(\frac{a'}{s'}+\frac{a''}{s''}\right)$，$\frac{0}{s'}+\frac{a}{s}=\frac{a}{s}+\frac{0}{s}=\frac{a}{s}$，$\frac{0}{s}$为零元，其中$s'\in S$；$\frac{a}{s}$的负元为$\frac{-a}{s}$。$\therefore S^{-1}A$

关于规定的这个加法作成一个加群。

8. 证明，$S^{-1}A$关于第6、7题中所规定的加法、乘法作成一个可换环，并且φ：$a \mapsto \frac{a}{1}$ 是A到$S^{-1}A$的一个同态映射，$\varphi(S)$中任意元在$S^{-1}A$中均可逆。

证 由6、7题知，$S^{-1}A$关于加法成群，关于乘法成半群。

$\because \frac{b}{t} \cdot \left(\frac{a}{s} + \frac{a'}{s'}\right) = \frac{b}{t} \cdot \frac{s'a + sa'}{ss'} = \frac{bs'a + bsa'}{tss'}$，$\frac{b}{t} \cdot \frac{a}{s} + \frac{b}{t} \cdot \frac{a'}{s'} = \frac{ba}{st} + \frac{ba'}{ts'} = \frac{bats' + tsba'}{tsts'} = \frac{t}{t} \cdot \frac{(bs'a + bsa')}{tss'} = \frac{bs'a + bsa'}{tss'}$。$\therefore \frac{b}{t}\left(\frac{a}{s} + \frac{a'}{s'}\right) = \frac{b}{t} \cdot \frac{a}{s} + \frac{b}{t} \cdot \frac{a'}{s'}$。左分配律成立。同理可证右分配律成立。$\therefore S^{-1}A$成为环。

$\because \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} = \frac{ba}{ts} = \frac{b}{t} \cdot \frac{a}{s}$，$\therefore S^{-1}A$是可换环。

$\because \varphi(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \varphi(a) + \varphi(b)$，$\varphi(ab) = \frac{a \cdot b}{1} = \frac{a}{1} \cdot \frac{b}{1} = \varphi(a) \cdot \varphi(b)$。$\therefore \varphi$是$A$到$S^{-1}$的一个同态映射。

任取$s \in S$，则$\varphi(s) = \frac{s}{1}$。容易知道$\frac{1}{s} \in S^{-1}A$。且$\frac{1}{s}\varphi(s) = \frac{1}{s} \cdot \frac{s}{1} = 1$，$\therefore \varphi(s)^{-1} = \frac{1}{s} \in S^{-1}A$。故$\varphi(S)$中任意元在$S^{-1}A$中均可逆。

§5 素理想与极大理想

1. 设$R = \mathbf{Z}[x, y]$，证明，(x, y)，$(x, z, 2)$都是R的素理想

证 容易证明，(x,y)和$(x,y,2)$都是$R=\mathbf{Z}[x,y]$的理想。

作R到$\mathbf{Z}$的的一个映射$\tau: f(x,y)\longmapsto f(0,0)$。易证$\tau$是$R$到$\mathbf{Z}$上的一个满同态映射。易知$f(x,y)\in Ker\tau \Longleftrightarrow \exists g(x,y)$和$h(x,y)\in R$，使得$f(x,y)=x\cdot g(x,y)+y\cdot h(x,y)$。即$Ker\tau=(x,y)$。$\therefore \mathbf{Z}[x,y]/(x,y)\cong\mathbf{Z}$。$\because \mathbf{Z}$是整环，$\therefore \mathbf{Z}[x,y]/(x,y)$是整环，$(x,y)$是$R$的素理想。

作$\mathbf{Z}[x,y]=R$到$\mathbf{Z}/(2)$的映射$\eta: f(x,y)\longmapsto \overline{f(0,0)}\in \mathbf{Z}/(2)$。易证$\eta$是$R$到$\mathbf{Z}/(2)$的满同态。易知，$f(x,y)\in ker\eta \Longleftrightarrow \exists g(x,y),\overline{h(x,y)}\in R, n\in Z$，使得，$f(x,y)=x\cdot g(x,y)+y\cdot h(x,y)+2n$。即$ker\eta=(x,y,2)$。$\therefore R/(x,y,2)\cong\mathbf{Z}/(2)$。$\because \mathbf{Z}/(2)$是整环，$\therefore R/(x,y,2)$也是整环，$(x,y,2)$是$R$的素理想。

2. 在整数环$\mathbf{Z}$中，p是素数，(p^2)是不是素理想？$(2p)$是不是素理想？

解 命$a=b=p$，则$ab-p^2\in(p^2)$，但$a-p\notin(p^2)$，$b-p\notin(p^2)$，$\therefore (p^2)$不是素理想。命$a=2$，$b=p$，则$ab=2p\in(2p)$，但$a=2\notin(2p)$，$b=p\notin(2p)$，$\therefore (2p)$不是素理想。

3. 设R是偶数环，p是素数，$(2p)$是不是极大理想？是不是素理想？

解 (1) 假设$p\neq 2$，(g)是R的一个理想，$(2p)\subsetneq(g)$。则$g\mid 2p$。但p为素数，$(p,g)=1$或$(p,g)=p$。然而当$(p,g)=p$时，$p\mid g$，同时$\because g\in R$，有$2\mid g$，且$p\neq 2$，$\therefore 2p\mid g$，$(g)\subseteq(2p)$。与假设$(2p)\subsetneq(g)$矛盾。$\therefore (p,g)=1$。

于是，由$g\mid 2p$得$g\mid 2$，$(g)=(2)=R$，$\therefore (2p)$是R的极大理想。

若$a,b\in R$，$ab\in(2p)$，则$2p\mid ab$。$\therefore p\mid ab$，但p为素数，$\therefore p\mid a$或$p\mid b$。又$\because a,b$为偶数，$p\neq 2$，$\therefore 2p\mid a$或$2p\mid b$。因此$a\in(2p)$

或$b\in(2p)$，$(2p)$是素理想。

(2)如果$p=2$，则$(2p)=(4)$。若(g)是R的理想，$(g)\supseteq(2p)=(4)$，则$g\mid 4$，不妨认为g是正数，于是，$g=2$或4。当$g=4$时$(g)=(4)=(2p)$；当$g=2$时，$(g)=(2)=R$。$\therefore$ $(2p)$是R的极大理想。但是，取$a=b=2\in R$，$ab=4\in(4)=(2p)$，而$a=2\notin(4)$，$b=2\notin(4)$，$\therefore(2p)=(4)$不是素理想。

4. 在$\mathbf{Z}[x]$中，证明(x,n)是极大理想的充要条件是：n为素数。

证 作$\mathbf{Z}[x]$到$\mathbf{Z}/(n)$的映射η：$f(x)\longmapsto\overline{f(0)}$。容易验证$\eta$是$\mathbf{Z}[x]$到$\mathbf{Z}/(n)$的满同态，且$ker\eta$是$=\{f(x)\mid f(x)\in\mathbf{Z}[x],\overline{f(0)}=\overline{0}\}$。

设$f(x)=a_0+a_1x\cdots+a_nx^n$，则$f(0)=a_0$。易知，$\overline{f(0)}=\overline{0}\Longleftrightarrow a_0\in(n)$。故$ker\eta=(x,n)$。$\mathbf{Z}[x]/(x,n)\cong\mathbf{Z}/(n)$。

$\mathbf{Z}[x]$是有单位元的可换环，(x,n)是$\mathbf{Z}[x]$的极大理想$\Longleftrightarrow\mathbf{Z}[x]/(x,n)$是域，即$\mathbf{Z}/(n)$是域。如果$n$不是素数，有$n=m_1m_2$，$m_1\neq 1$，$m_2\neq 1$。则$m_1$和$m_2$是$\mathbf{Z}/(n)$的零因子，$\mathbf{Z}/(n)$就不是域。如果$n$为素数，$(n)$是$\mathbf{Z}$的极大理想，则$\mathbf{Z}/(n)$为域，$\therefore(x,n)$为$\mathbf{Z}[x]$的极大理想$\Longleftrightarrow n$为素数。

5. 设R是有单位元的环，A是R的真理想，证明，存在R的一个极大理想M，$M\supseteq A$。

证 R是有单位元1的环，命$S=\{H\mid H$是R的理想，$H\supseteq A$，$1\notin H\}$。

$\because A\in S$，$\therefore S$非空，且S依包含关系作成一偏序集。取S的任一非空有序子集$L=\{H_\alpha\mid\alpha\in B\}$。命$H=\bigcup_{\alpha\in B}H_\alpha$，则$H$是$R$的一个理想，$H\supseteq A$，$1\notin H$，从而$H$是$L$的上界。由Zorn引理知$S$有极大元$M$。

若M不是R的极大理想，则存在R的一个真理想M'，$M \subsetneq M'$。$\because M \supseteq A$，$\therefore M' \supseteq A$，且$1 \notin M'$（若$1 \in M'$，易知$M' = R$，与$M'$为$R$的真理想矛盾），$\therefore M' \in S$。而$M \subsetneq M'$，这与$M$是$S$中之极大元矛盾。故$M$是$R$的一个极大理想，且$M \supseteq A$。

6. 命$A = \mathbf{Q} \times \mathbf{Q}$，如下规定$A$的$+$，$\times$：$(a,b)+(c,d) = (a+c, b+d)$，$(a,b)\cdot(c,d) = (0,ac)$。证明，$A$是一个没有单位元的交换环，并且，$A$不含极大理想。

证 按照环的定义，容易验证，$A = \mathbf{Q} \times \mathbf{Q}$是一个交换环。

显然，只要$c \neq 0$，任取$(a,b) \in A$，总有$(a,b)\cdot(c,d) = (0, ac) \neq (c,d)$，$\therefore A$中无单位元。

设B是A的任一真理想，命B_1表示B的第一坐标全体所成的集合，B_2表示B的第二坐标所成的集合。容易验证，B_1和B_2都是$(\mathbf{Q}, +)$的子群。

如若$B_1 = \mathbf{Q}$，则对于任意的$a \in \mathbf{Q}$，有$a \in B_1$，$\therefore (a,0) \in B$，又$\because (1,0) \in A$，$\therefore (a,0)(1,0) = (0,a) \in B$，$a \in B_2$，从而$\mathbf{Q} \subseteq B_2$。但$B_2 \subseteq \mathbf{Q}$，$\therefore B_2 = \mathbf{Q}$，且$(a,0)+(0,a) \in B$，即$(a,a) \in B$，$\forall a \in \mathbf{Q}$。于是，任给$(a,b) \in A$时，由于$(a-b,0)$及$(b,b)$皆$\in B$，故其和$(a,b) \in B$，$\therefore B = A$，与“$B$是$A$的真理想”矛盾。$\therefore B_1 \subsetneq \mathbf{Q}$，$B_1$为$(\mathbf{Q}, +)$的真子群。由原书$p.116$中的例3知，存在$(\mathbf{Q}, +)$的真子群$H_1$，使得$H_1$真包含$B_1$。

作$B' = \{(a,b) \mid a \in H_1, b \in \mathbf{Q}\}$，则由$B_1 \subsetneq H_1$知$B \subsetneq B'$，且易证得$B'$为$A$的理想。但$H_1$是$(\mathbf{Q}, +)$的真子群，$\therefore B'$又是$A$的真理想。

这就证得了，“对于A的任一真理想B，必存在A的真理想B'，使得$B \subsetneq B'$”。$\therefore A$不含极大理想。

§6 单一分解整环

1*. 设S是有单位元1且消去律成立的可换半群，证明p.170相伴$\sim$是一个等价关系，找出1所在的等价类。

证 当$a|b$，且$b|a$时，才记为$a\sim b$。显然，1) $a|a$，$\therefore a\sim a$；2) $\forall a,b\in S$，若$a\sim b$，则$a|b$，$b|a$，$\therefore b\sim a$；3) $\forall a,b,c\in S$，若$a\sim b$，$b\sim c$，则$a|b$，$b|a$，$b|c$，$c|b$，$\therefore a|c$，$c|a$，$a\sim c$。故$\sim$是一个等价关系。

设$1\in$等价类C。任取$x\in C$，由$1\sim x$知$1|x$，$x|1$。而由$x|1$可知，$\exists y\in S$，使得$xy=1$，$\therefore x$为可逆元。若令U为S中全体正则元所成的集合(成可换群)，则$C\subseteq U$；另一方面，任取$x\in U$，有$xx^{-1}=1$，$\therefore x|1$。但$1|x$，$\therefore x\sim 1$，$U\subseteq C$。$\therefore C=U$，即1所在的等价类就是S中全体正则元所成的集合。

2. 在上题中，对商集$S/\sim$如下规定二元关系：对任意$A,B\in S/\sim$，任取$a\in A$，$b\in B$，如果$a|b$，那末，就规定$A\leqslant B$。证明，这样的规定确为$S/\sim$的一个偏序关系。

证 设$A,B\in S/\sim$，若存在$a\in A$，$b\in B$，且$a|b$，由题中所作规定，$A\leqslant B$。这时任取$c\in A$，$d\in B$，由于$a,c\in A$，$b,d\in B$，$\therefore a\sim c$，$b\sim d$，则$c|a$，$b|d$。又$\because a|b$，$\therefore$必有$c|d$。从而可知，题中对于$S/\sim$所作的$A\leqslant B$的规定，是与A,B中的代表元a,b的选取无关。任取$A,B\in S/\sim$。当$a\in A$，$b\in B$时，$a|b$或者$a\nmid b$，两者之中有且仅有一个成立，故"$\leqslant$"确是一个二元关系。

由于：1) $\forall A\in S/\sim$，显然有$A\leqslant A$；2) $\forall A,B\in S/\sim$，当$A\leqslant B$且$B\leqslant A$时，任取$a\in A$，$b\in B$，则有$a|b$及$b|a$，$\therefore a\sim b$，$A=B$；3) $\forall A,B,C\in S/\sim$，当$A\leqslant B$，$B\leqslant C$时，任取$a\in A$，$b\in B$，$c\in C$，则有

$a|b, b|c, \therefore a|c$, $A \leqslant C$. 故 "$\leqslant$" 是$S/\sim$ 的一个偏序关系.

3. 在上题中,找出$(S/\sim, \leqslant)$的最小元素.证明,$(S/\sim, \leqslant)$中除最小元素以外的所有类中的极小者,元其素为S的既约元.

证 任取$A \in S/\sim$, $a \in A$, $\because 1|a$, $\therefore 1$所在的类$U \leqslant A$. $\therefore (S/\sim, \leqslant)$的最小元素为$U$,它由$S$中全体正则元所组成的集合

设A是$(S/\sim, \leqslant)$中除U以外的所有类中的极小者.任取$a \in A$,则$a \notin U$.设$a = bc$,则$b|a$. $\therefore b$所在的类$B \leqslant A$. 但A是除U外之极小者, $\therefore B = U$或$B = A$.当$B = U$时$b \in U$;当$B = A$时$b \sim a$从而$c \in U$.总之,由$a = bc$知$b \in U$或$c \in U$. $\therefore a$是S的一个既约元.

4. 设p是S的素元,$p|a_1 a_2 \cdots a_n$,证明,至小存在一个i,$1 \leqslant i \leqslant n$, $p|a_i$.

证 用数学归纳法.$n = 1$时,由于$p|a_1$, $\therefore$命题已成立.

假设命题在$n-1$时成立.即:如果$p|a_1 a_2 \cdots a_{n-1}$,则至少存在一个i, $1 \leqslant i \leqslant n-1$,使$p|a_i$.

$\because a_1 a_2 \cdots a_n = (a_1 \cdots a_{n-1}) a_n$, $\therefore$由素元的定义知,当$p|(a_1 \cdots a_{n-1}) a_n$时.或者$p|a_1 \cdots a_{n-1}$,或者$p|a_n$.而当$p|a_1 \cdots a_{n-1}$时,由归纳假设,至少存在一个$i$, $1 \leqslant i \leqslant n-1$,使得$p|a_i$. $\therefore$总存在一个i, $1 \leqslant i \leqslant n$,使$p|a_i$.

5. 设R是一切形如$\frac{m}{2^k}$(m是任意整数,k是非负整数)的有理数所成集合,证明,$(R, +, \times)$作成一个有单位元的整环,R的哪些元是单位?哪些元是既约元?

解 按照环的定义,容易验证$(R, +, \times)$为一个可换环,其单位元是$\frac{1}{2^0} = 1$.如果$\frac{m}{2^k} \cdot \frac{m'}{2^{k'}} = 0$,则$mm' = 0$,其中$m$, m'为整数,从而$m = 0$或$m' = 0$, $\therefore$环R中不含非零的零因子.

$(R,+,\times)$作成一个有单位元的整环。

设 $x=\frac{m}{2^k}$是R中之单位，则存在$x'=\frac{n}{2^t}\in R$，使得x

即$\frac{m}{2^k}\cdot\frac{n}{2^t}=1$。$\therefore mn=2^{k+t}$，$m|2^{k+t}$，$m=\pm 2^p$，$p$是非

数。如果$m=\pm 2^p$，p是非负整数，x为单位。显然当且仅当

$\pm 2^p$，p是非负整数，$\frac{m}{2^k}$是R中之单位。

设 $x=\frac{m}{2^k}$是 R中之既约元。$\because x$不是单位。$\therefore m$不是2

幂。将m分解成质因数的积，$m=2^t p_1\cdots p_r$，$r\geqslant 1$，其中 p_1，

是不等于2的素数，允许有相同的。我们可以证明$r=1$

是因为如果 $r>1$，则$x=\frac{m}{2^k}=\frac{2^t p_1}{2^k}\cdot\frac{p_2\cdots p_r}{2^0}$，$\frac{2^t p_1}{2^k}$和$\frac{p_2}{}$

都不是单位，从而与x是既约元矛盾。$\therefore r=1$，$m=2$

$x=\frac{2^t p}{2^k}$。故R中的既约元都是形如$\frac{2^t p}{2^k}$的元素，其中

奇素数。反之任何 $x=\frac{2^t p}{2^k}$，p为奇数数，也确是R的既约

6. 找出高斯整数环的所有单位。

解 $A=\{a+bi\mid a,b\in\mathbf{Z}\}$。设$x=a+bi$是$A$中的单位，

在$x'\in A$，使得$x\cdot x'=1$。直接计算得，$x'=\frac{a}{a^2+b^2}-\frac{b}{a^2+}$

且$\frac{a}{a^2+b^2}$，$\frac{b}{a^2+b^2}$都应该是整数，a，b也是整数，$\therefore$

$a=\pm 1,b=0$或$a=0,b=\pm 1$。易验证，$x=\pm 1$或$\pm i$确是

$\therefore A$中的单位只有$\pm 1,\pm i$。

7. 设z是高斯整数环的既约元，证明，z能整除且仅

除一个素（自然）数p。

证 设$x=a+bi$是高斯整数环A的任一元，约定$\bar{x}=a-bi$。题知，A中单位只有$\pm1,\pm i$，易知，当x不是单位时，$\bar{x}$是单位，反之亦然。

$\because z$是A中既约元，$\therefore \bar{z}$也是A中既约元。此因，首先由z单位可知$\bar{z}$不是单位。其次，若$\bar{z}=\bar{u}\bar{v}$且$\bar{u},\bar{v}$都不是单位，$z=uv$且u,v都不是单位。故由z是既约元得$\bar{z}$是既约元。

命$z\cdot\bar{z}=m$，则$m\neq1$(若$m=1$，则z为单位，与已知矛盾)，且E整数。

若m为素数，则$z\mid m$，$\therefore z$能除尽一个素自然数。

若m不是素（自然）数，则m可分解为素(自然)数的乘积$p_1p_2\cdots p_t$，$t\geqslant2$。由于A是单一分解环，且每个p_i都不是单z每个p_i总可分解成既约元的乘积，$p_i=p_i^{(1)}\cdots p_i^{(r_i)}$，$i=1,2,\cdots,t$，$\therefore m=p_1^{(1)}\cdots p_1^{(r_1)}\cdots p_t^{(1)}\cdots p_t^{(r_t)}$。但$m=z\bar{z}$也约元的分解，它们在相伴意义上是唯一的，$\therefore r_1+r_2+\cdots=2$，$t=2$，$r_1=r_2=1$。从而$m=p_1p_2$，且素数$p_1,p_2$都是$A$的元。$\therefore z\sim p_1$或$z\sim p_2$。从而$z\mid p_1$或$z\mid p_2$，$z$总能除尽一个自然）数。

如果$z\mid p_1,z\mid p_2,p_1,p_2$是素(自然)数，但$p_1\neq p_2$。这时，$\bar{p_1}$，而$\overline{p_1}=p_1$，$\therefore\bar{z}\mid p_1,\bar{z}z\mid p_1^2$。同理$z\bar{z}\mid p_2^2$。$\therefore p_1^2$和$p_2^2$有公因子$z\bar{z}$，且$z\bar{z}=m$为$\neq1$的正整数。然而由$p_1,p_2$是素数，$\neq p_2$可知，$p_1^2$和$p_2^2$互素，从而产生矛盾。　$\therefore p_1=p_2$。

综上，z能整除且只能整除一个素(自然)数。

3.高斯整数环的元素z的范数$v(z)$若为素数(自然数)，则既约元。

证 设$z=a+bi$，$\bar{z}=a-bi$，则$v(z)=z\cdot\bar{z}$为正数或零。若$z=z_1z_2$，则$v(z)=v(z_1)\cdot v(z_2)$，$\therefore$当$v(z)$=素数p时，

$\nu(z_1)\cdot\nu(z_2)=p$，但$\nu(z_1)$和$\nu(z_2)$均为非整数，而素数的非负整数因子只有1和p，∴或者$\nu(z_1)=1$，或者$\nu(z_2)=1$。即$z_1\overline{z_1}=1$或$z_2\overline{z_2}=1$，于是，$z_1\in U$或$z_2\in U$，z为既约元。

9.找出高斯整数环的所有既约元。

解 设D为高斯整数环的所有既约元的集合，$D_1=\{z\mid z\in A$ $\nu(z)$为素数$\}$，$D_2=\{\varepsilon p\mid \varepsilon\in U, p\in \mathbf{Z}, p$为$A$的既约元$\}$。则由第8题知，$D_1\subseteq D$，又 ∵$D_2\subseteq D$， ∴$D_1\cup D_2\subseteq D$。任取$z\in D$，则$\bar{z}\in D$，$z\bar{z}=\bar{\nu}(z)$为一非负整数。如果$\nu(z)$=素数，则$z\in D_1$；如果$\nu(z)$不是素数，则如第7题中证明的那样，$\nu(z)=p_1p_2$为素数的分解，$z\bar{z}=p_1p_2$，且$p_1,p_2$都是$A$中的既约元，故$z\sim p_1$或$z\sim p_2$（实际上，可以证得$p_1\sim p_2$），∴$z\in D_2$。于是，若$z\in D$，则$z\in D_1$或$z\in D_2$，∴$D\subseteq D_1\cup D_2$。从而，$D=D_1\cup D_2$。

10^*。证明，定义6中，R有单位元的条件是多余的。即整环R的每一理想都是主理想，则R有单位元。

证 按题意，即要求证明："设R是整环，如果存在R^*到非负整数集合N里的一个映射ν，适合条件(E)：取定$a\in R^*$，对任一$b\in R$，均存在$q,r\in R$，使$b=qa+r$，此处$r=0$或$u(v)<v(a)$。则R中含单位元e。"

∵非负整数的非空集合N中必有最小数，∴可设有$a\in R^*$，使得$\nu(a)\leqslant\nu(b)$，$\forall b\in R^*$。

任取$b\in R$，总有$q,r\in R$，使得$b=qa+r$，$r=0$或$\nu(r)<\nu(a)$。若$r\neq 0$，则$\nu(r)<\nu(a)$，但这与$\nu(a)$为N中最小数矛盾。∴必$r=0$，$b=qa$。特别地，对于$a\in R$，有$e\in R$，使$a=ea$，从而$be=(qa)e=q(ae)=qa=b$，$\forall b\in R$，∴R中含单位元e。

§7 单一分解整环上的多项式环

1. 设R是单一分解整环，若$f_1(x), f_2(x) \in R[x]$，$f_1(x) \cdot f_2(x)$是本原多项式，则$f_1(x), f_2(x)$都是本原多项式。

证 设$f_1(x) = a_1\bar{f}_1(x)$，$f_2(x) = a_2\bar{f}_2(x)$，其中$a_1, a_2 \in R$，$\bar{f}_1(x), \bar{f}_2(x)$是本原多项式，则$f_1(x)f_2(x) = a_1a_2\bar{f}_1(x) \cdot \bar{f}_2(x)$，且由高斯引理知，$\bar{f}_1(x)\bar{f}_2(x)$是本原多项式。又$\because f_1(x)f_2(x)$也是本原多项式，$\therefore a_1a_2$是$R$的单位，则存在$\beta \in U$，使得$a_1a_2\beta = 1$，即$a_1(a_2\beta) = 1$，$a_2(a_1\beta) = 1$。$\therefore a_1, a_2 \in U$，

由$f_1(x) = a_1\bar{f}_1(x)$，而$a_1 \in U$，$\bar{f}_1(x)$为本原多项式，可知$f_1(x)$为本原多项式。同理，$f_2(x)$也是本原多项式。

2. 设$f(x), g(x) \in R[x]$，$f(x) = af_1(x)$，$g(x) = bg_1(x)$，$f_1(x), g_1(x)$是本原多项式。如果$g(x) \mid f(x)$，那么$b \mid a$，$g_1(x) \mid f_1(x)$。

证 $\because g(x) \mid f(x)$，$\therefore$存在$h(x) \in R[x]$使得$f(x) = g(x) \cdot h(x)$。

设$h(x) = ch_1(x)$，$h_1(x)$是本原多项式，则$af_1(x) = bc \cdot g_1(x)h_1(x)$。由高斯引理知，$g_1(x)h_1(x)$是本原多项式，$\therefore a \sim bc$，$f_1(x) \sim g_1(x)h_1(x)$，故$b \mid a$，$g_1(x) \mid f_1(x)$。

3. 设$f_1(x), f_2(x), \cdots f_i(x), \cdots$是$R[x]$中本原多项式的序列，并且$f_{i+1}(x) \mid f_i(x)$，$i = 1, 2\cdots$证明，这个序列只能含有有限个互不相伴的项。

证 用反证法。假设$f_1(x), f_2(x), \cdots, f_n(x), \cdots$中含无限个互不相伴的项，并设$f_1'(x) = f_1(x), f_2'(x), \cdots, f_n'(x), \cdots$，是其中互不相伴的本原多项式的序列，且$f_{i+1}'(x) \mid f_i'(x)$，

$i=1,2,\cdots$，$deg\ f_1(x)=n$为非负整数。

$\because f'_{i+1}(x)\mid f_i'(x)$，$\therefore$存在$h_{i+1}(x)\in R[x]$，使得$f_i'(x)=f'_{i+1}(x)h_{i+1}(x)$。若$degf'_{i+1}(x)=degf_i'(x)$，则$h_{i+1}(x)=a_{i+1}\in R$，$f_i'(x)=a_{i+1}f'_{i+1}(x)$。$\because f_i'(x)$和$f'_{i+1}(x)$是本原多项式，$\therefore a_{i+1}$是单位，$f'(x)\sim f'_{i+1}(x_1)$，从而与已知互不相伴矛盾。$\therefore degf'_{i+1}(x)\neq degf_i'(x)$。但由$f'_{i+1}(x)\mid f_i'(x)$知$degf_i'(x)\geqslant degf'_{i+1}(x)$。故$degf_i'(x)>degf'_{i+1}(x)$，$i=1,2,\cdots$。

由此，我们可得到一无穷的非负整数序列：$n=degf_1'(x)>degf_2'(x)>\cdots>degf_i'(x)>\cdots\geqslant 0$，而$n$为有限，产生矛盾。$\therefore f_1(x),\cdots,f_i(x),\cdots$中只能含有限个互不相伴的项。

4。设$f(x)$是$\mathbf{Z}[x]$中首项系数为1的多项式，若$f(x)$有有理根a，则a是整数。

证 设$a=\frac{a}{b}$，$a,b\in\mathbf{Z}$，$(a,b)=1$。则$(x-\frac{a}{b})\mid f(x)$，$(bx-a)\mid bf(x)$。因此，存在$g(x)\in\mathbf{Z}[x]$，使得$bf(x)=(bx-a)g(x)$

$\because f(x)$的首项系数为1，比较等式两边的首项系数，容易知道$g(x)$的首项系数为1，$\therefore g(x)$在$\mathbf{Z}[x]$中是本原多项式，$\because (a,b)=1$，$\therefore bx-a$是$\mathbf{Z}[x]$中的本原多项式，而$f(x)$也是本原多项式，$\therefore b$是$\mathbf{Z}$中的单位，即$b=\pm 1$，a为整数。

5*。设R是单一分解整环，P是R的商域，若$f(x)\in R[x]$，$f(x)$在$P[x]$中有真因子，则$f(x)$在$R[x]$也有真因子。

证 若$f(x)$在$P[x]$中有真因子，因为P是域，则有$f(x)=g(x)h(x)$，其中$g(x),h(x)\in P[x]$，$g(x)$，$h(x)$的次数$\geqslant 1$。$\because P$是R的商域，$\therefore$总有$g(x)=a^{-1}g_1(x)$，$h(x)=b^{-1}h_1(x)$，其中$a,b\in R$，$g_1(x),h_1(x)\in R[x]$。$\therefore$在$R[x]$中，$abf(x)=g_1(x)\cdot h_1(x)$。令$f(x)=cf_2(x)$，$g_1(x)=a_1g_2(x)$，$h_1(x)=b_1h_2(x)$，

其中$f_2(x),g_2(x),h_2(x)$是$R[x]$中的本原多项式，则$abcf_2(x)=a_1b_1g_2(x)h_2(x)$，由p.184引理2知，在$R[x]$中$f_2(x)\sim g_2(x)h_2(x)$，∴有$\varepsilon\in U\subseteq R$，使$f_2(x)=\varepsilon\cdot g_2(x)h_2(x)$。$f(x)=c\varepsilon g_2(x)h_2(x)$。 因此，$f(x)$在$R[x]$中有真因子$g_2(x),h_1(x)$。

6. 设R是一个有单位元1的整环，证明，$R[x]$中首项系数为1的多项式能分解成$R[x]$中既约多项式的乘积。

证 对多项式$f(x)$的次数n，用数学归纳法证明之。

当$n=1$时，$f(x)=x+a\in R[x]$。显然，$f(x)$是$R[x]$中的既约多项式。假设次数$<n$的首项系数为1的多项式，都能分解成$R[x]$中既约多项式的乘积。

设$f(x)$的次数$=n$，如果$f(x)$是$R[x]$中既约多项式，则结论已成立。如果$f(x)$不是$R[x]$中的既约多项式，则$f(x)$可以分解成$R[x]$中两个次数较低的多项式的乘积，即，$f(x)=g(x)h(x)$，其中$g(x)$和$h(x)$的次数$<n$。设$g(x)$的首项系数为$a\neq 0$，$h(x)$的首项系数为$b\neq 0$，$a,b\in R$。

比较$f(x)=g(x)h(x)$两边最高项系数可知，$ab=1$。命$g_1(x)=bg(x)\in R[x]$，$h_1(x)=ag(x)\in R[x]$，容易知道，$deg\,g_1(x)=deg\,g(x)<n$，$deg\,h_1(x)=deg\,h(x)<n$，$g_1(x)$，$h_1(x)$的首项系数都为1，且$f(x)=g_1(x)h_1(x)$。根据归纳假设，$g_1(x)$和$h_1(x)$都可分解成$R[x]$中既约多项式的乘积。故$f(x)$可分解成$R[x]$中既约多项式的乘积。

§8 域的扩张

1. 写出$\mathbf{Q}(\sqrt{2},\sqrt{3})$的元素形式，并找出$\mathbf{Q}(\sqrt{2},\sqrt{3})$的所有

子域.

解 由$\mathbf{Q}(\sqrt{2},\sqrt{3})=\mathbf{Q}(\sqrt{2})(\sqrt{3})$，易知$\mathbf{Q}(\sqrt{2},\sqrt{3})=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\mid a,b,c,d\in\mathbf{Q}\}$，且$(\mathbf{Q}(\sqrt{2},\sqrt{3}):\mathbf{Q})=(\mathbf{Q}(\sqrt{2},\sqrt{3}):\mathbf{Q}(\sqrt{2}))\cdot(\mathbf{Q}(\sqrt{2}):\mathbf{Q})=2\cdot2=4$.

设K是$\mathbf{Q}(\sqrt{2},\sqrt{3})$的一个子域，则$(K:\mathbf{Q})=1,2,4$. 当$(K:\mathbf{Q})=1$时，$K=\mathbf{Q}$；当$(K:\mathbf{Q})=4$时，$K=\mathbf{Q}(\sqrt{2},\sqrt{3})$. 此外，$\mathbf{Q}(\sqrt{2})$，$\mathbf{Q}(\sqrt{3})$，$\mathbf{Q}(\sqrt{6})$是$\mathbf{Q}(\sqrt{2},\sqrt{3})$的子域，且是$\mathbf{Q}$的二次扩域. 对于$\mathbf{Q}(\sqrt{2},\sqrt{3})$的任一子域$K$，都可由$\mathbf{Q}$添加一个形为$b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$，其中$b,c,d\in\mathbf{Q}$的元素得到.

如果b,c,d有一个为零，其它两个不为零，不妨设$b,c\neq0$，$d=0$，那末$K=\mathbf{Q}(b\sqrt{2}+c\sqrt{3})$. 于是$(b\sqrt{2}+c\sqrt{3})^2=2b^2+3c^2+2bc\sqrt{6}\in K$，$\sqrt{6}\in K$，$\therefore K\supseteq\mathbf{Q}(\sqrt{6})$，但易知$b\sqrt{2}+c\sqrt{3}\notin\mathbf{Q}(\sqrt{6})$，$\therefore\mathbf{Q}(\sqrt{6})\subsetneq K$，故$(K:\mathbf{Q})=4$，即$K=\mathbf{Q}(b\sqrt{2}+c\sqrt{3})=\mathbf{Q}(\sqrt{2},\sqrt{3})$.

如果b,c,d都不为零，那末$K=\mathbf{Q}(b\sqrt{2}+c\sqrt{3}+d\sqrt{6})$. 于是$(b\sqrt{2}+c\sqrt{3}+d\sqrt{6})^2=2b^2+3c^2+6d^2+2(bc\sqrt{6}+2bd\sqrt{3}+3cd\sqrt{2})\in K$，$3cd\sqrt{2}+2bd\sqrt{3}+bc\sqrt{6}\in K$. $\because\frac{3cd}{b}=\frac{2bd}{c}=\frac{bc}{d}$在$\mathbf{Q}$中不成立，$\therefore$由$b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$，$3cd\sqrt{2}+2bd\sqrt{3}+bc\sqrt{6}\in K$，得知$\exists e,f\in\mathbf{Q}$，$e,f\neq0$，有$e\sqrt{2}+f\sqrt{3}\in K$. 因此$\mathbf{Q}(b\sqrt{2}+c\sqrt{3}+d\sqrt{6})=\mathbf{Q}(e\sqrt{2}+f\sqrt{3})=\mathbf{Q}(\sqrt{2},\sqrt{3})$.

这就说明，除$\mathbf{Q}(\sqrt{2})$，$\mathbf{Q}(\sqrt{3})$，$\mathbf{Q}(\sqrt{6})$外，无其它$\mathbf{Q}$的二次扩域为$\mathbf{Q}(\sqrt{2},\sqrt{3})$的子域. 故$\mathbf{Q}(\sqrt{2},\sqrt{3})$的子域是$\mathbf{Q}$，$\mathbf{Q}(\sqrt{2})$，$\mathbf{Q}(\sqrt{3})$ $\mathbf{Q}(\sqrt{6})$，$\mathbf{Q}((\sqrt{2},\sqrt{3})$.

2. $(\mathbf{Q}(\sqrt{2},\sqrt{3}):\mathbf{Q})=?$

解 由上题知，$(\mathbf{Q}(\sqrt{2},\sqrt{3}):\mathbf{Q})=4$.

3. 求$e^{\frac{2\pi}{5}i}$在$\mathbf{Q}$上的最小多项式，并求出$\mathbf{Q}(e^{\frac{2\pi}{5}i})$在$\mathbf{Q}$上的次

数。

解 命$x=e^{\frac{2\pi}{5}i}$，则$x^5=1$，$\therefore e^{\frac{2\pi}{5}i}$是$x^5-1$的根。但$x^5-1=(x-1)(x^4+x^3+x^2+x+1)$，而$e^{\frac{2\pi}{5}i}$不是$x-1$的根，$\therefore e^{\frac{2\pi}{5}i}$是$g(x)=x^4+x^3+x^2+x+1$的根。

$\because g(x+1)=(x+1)^4+(x+1)^3+(x+1)^2+(x+1)+1=x^4+5x^3+10x^2+10x+5$。由$Eisenstein$判别法知，$g(x)$在$\mathbf{Q}[x]$上是既约的。$\therefore e^{\frac{2\pi}{5}i}$的最小多项式是$g(x)=x^4+x^3+x^2+1$。

$$(\mathbf{Q}(e^{\frac{2\pi}{5}i}):\mathbf{Q})=4.$$

4. 设$F=\mathbf{Z}/(2)$，证明$f(x)=x^3+x+1$是$F[x]$中既约多项式，写出$F[x]/(f(x))$的乘法表，并证明$F[x]/(f(x))$是$f(x)$的分裂域。

证 设$f(x)=g(x)h(x)$，$g(x),h(x)\in F[x]$，$degg(x)\leqslant degh(x)$。$\because degg(x)+degh(x)=degf(x)=3$，$\therefore degg(x)=0$或1。$\because F[x]$中的一次因式只有$x$与$x+1$，而$x\nmid f(x)$，$(x+1)\nmid f(x)$，$\therefore g(x)$不能为一次因式，$degg(x)=0$，$g(x)\in F$。又$F=\mathbf{Z}/(2)$是域，$\therefore g(x)$为正则元，$f(x)$是$F[x]$中的既约多项式。

$\because x^3\equiv x+1((f(x)))$，

$\therefore F[x]/(f(x))=\{\bar{0},\ \bar{1},\overline{x},\ \overline{x+1},\overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1}\}$，其中$\overline{g(x)}=g(x)+(f(x))$。其乘法表为：

×	0	$\overline{1}$	$\overline{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
0	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x^2}$	$\overline{x^2+x}$	$\overline{x+1}$	$\overline{1}$	$\overline{x^2+x+1}$	$\overline{x^2+1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2+x+1}$	$\overline{x^2}$	$\overline{1}$	$\overline{x}$
$\overline{x^2}$	$\overline{0}$	$\overline{x^2}$	$\overline{x+1}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\overline{x}$	$\overline{x^2+1}$	$\overline{1}$
$\overline{x^2+1}$	$\overline{0}$	$\overline{x^2+1}$	$\overline{1}$	$\overline{x^2}$	$\overline{x}$	$\overline{x^2+x+1}$	$\overline{x+1}$	$\overline{x^2+x}$
$\overline{x^2+x}$	$\overline{0}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\overline{1}$	$\overline{x^2+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{x^2}$
$\overline{x^2+x+1}$	$\overline{0}$	$\overline{x^2+x+1}$	$\overline{x^2+1}$	$\overline{x}$	$\overline{1}$	$\overline{x^2+x}$	$\overline{x^2}$	$\overline{x+1}$

$F[x]/(f(x))$是F的扩域，且$\overline{x}$，$\overline{x^2}$，$\overline{x^2+x}$都是$f(x)$的根。又，若H是$F[x]/(f(x))$的子域，且H包含$f(x)$的根，则$H^*=H\backslash\{0\}$是$\{F[x]/(f(x))\}\backslash\{0\}$的子群，而$\{F[x]/(f(x))\}\backslash\{0\}$的阶为7，$\therefore H^*$的阶应是7的因子。显然，$H^*$不是单位元群，于是，$H^*=\{F[x]/(f(x))\}\backslash\{0\}$，$H=F[x]/(f(x))$。$\therefore F[x]/(f(x))$是包含$f(x)$的所有根的最小域，从而，是$f(x)$的分裂域。

5. 设F是一个域，σ是F的一个自同构，证明$L=\{x\mid x\in F,\sigma(x)=x\}$是$F$的一个子域，且含有$F$的最小子域。

证 设e是F的单位元，显然$0,e\in L$，L非空。任取$x,y\in L$，则$\sigma(x-y)=\sigma(x)-\sigma(y)=x-y$，$\sigma(xy)=\sigma(x)\sigma(y)=xy$，且当$x\neq 0$时，$\sigma(x^{-1})=\sigma(x)^{-1}=x^{-1}$，$\therefore x-y,xy,x^{-1}\in L$，$L$是$F$的一个子域。

∵ F的最小子域P是F中一切子域的交，$\therefore L \supseteq P$。

6。证明，$F[x]$中n次多项式$f(x)$在F上的分裂域K关于F的次数$\leqslant n!$

证 对n用数学归纳法。当$n=1$时，命题显然成立。假设对于任何$n-1$次多项式，其分裂域的次数$\leqslant(n-1)!$

设$f(x)$的次数$=n$，在K$[x]$中，$f(x)=(x-\rho_1)(x-\rho_2)\cdots(x-\rho_n)$。设$\rho_1$在$F$上的最小多项式为$g(x)$，$\because f(\rho_1)=0$，$\therefore g(x)\mid f(x)$，$deg\,g(x)\leqslant n$。因此，$(F(\rho_1):F)\leqslant n$。

命$h(x)=(x-\rho_2)\cdots(x-\rho_n)$，则$f(x)=(x-\rho_1)h(x)$，且$deg\,h(x)=n-1$。$\because f(x)\in F[x]\subseteq F(\rho_1)[x]$，$x-\rho_1\in F(\rho_1)[x]$，$\therefore h(x)\in F(\rho_1)[x]$，而$h(x)$在$F(\rho_1)$上的分裂域为$F(\rho_1)(\rho_2,\cdots,\rho_n)=$K。$\therefore$由归纳假设，$(K:F(\rho_1))\leqslant(n-1)!$

$\therefore (K:F)=(K:F(\rho_1))\cdot(F(\rho_1):F)\leqslant(n-1)!\cdot n=n!$

7。设F是特征p的域，$f(x)$是$F[x]$中既约多项式，证明，$f(x)$在F的扩域K中有重根的充要条件是：$f(x)$可表成x^p的多项式。

证 易证，既约多项式$f(x)$在扩域K中有重根$\Leftrightarrow f'(x)=0$。

充分性。设$f(x)=a_0(x^p)^m+a_1(x^p)^{m-1}+\cdots+a_{m-1}x^p+a_m\in F[x]$，则$f'(x)=a_0mpx^{mp-1}+a_1(m-1)px^{(m-1)p-1}+\cdots+a_mpx^{p-1}$。$\because F$的特征是$p$，$\therefore f'(x)=0$。$f(x)$在K中有重根。

必要性。若$f(x)$不可表成x^p的多项式，则在$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$中有一项$a_{m-i}x^i$，$i$不是$p$的倍数，$a_i\neq 0$，于是，$f'(x)$中必有一项$ia_{m-i}x^{i-1}\neq 0$，故$f'(x)\neq 0$，于是，$f(x)$在$K$中无重根。

§9 直　和

1. 设D_1, D_2是两个整环，$D_1 \oplus D_2$是不是整环？

解　$D_1 \oplus D_2$不是整环。∵若取$(a,0),(0,b) \in D_1 \oplus D_2$，其中$a \neq 0$，$b \neq 0$。则$(a,0) \neq (0,0)$，$(0,b) \neq (0,0)$，但$(a,0)\cdot(0,b) = (0,0)$，∴ $D_1 \oplus D_2$不是整环。

2. 设$R = \mathbf{Z}/(2^3 \cdot 3)$，将$R$表成其子环的直和。

解　$R = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{23}\}$，∴$R$含有子环$R_1 = (2^3)/(2^3 \cdot 3) = \{\bar{0}, \bar{8}, \overline{16}\}$，$R_2 = (3)/(2^3 \cdot 3) = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}\}$。易见，$R_1$和$R_2$都是$R$的理想。$R_1 + R_2$是$R$的子环。且∵$\overline{16} \in R_1$，$\bar{9} \in R_2$，$\overline{16} + \bar{9} = \bar{1} \in R_1 + R_2$。∴ $R_1 + R_2 = R$。又$R_1 \cap R_2 = \{\bar{0}\}$。∴ $R = R_1 \oplus R_2$。

3. 设$R = (\mathbf{Z})$，整数环上n阶方阵环，将R表为其左理想的直和。

解　命R_r是R中第r列元素属于$\mathbf{Z}$而其余的元素均为零的矩阵全体所作成的集合，容易验证，R_r是R的左理想，$R_r \cap (R_1 + \cdots + R_{r-1} + R_{r+1} + \cdots + R_n) = \{0\}$，$r = 1, 2, \cdots, n$。且$R = R_1 + R_2 + \cdots + R_n$　∴ $R = R_1 \oplus R_2 \oplus \cdots R_n$。

4. 将$R = (\mathbf{Z})_n$表为其右理想的直和。

解　命R_r'表示R中第r行元素属于$\mathbf{Z}$而其余的元素均为零的矩阵全体所作成的集合，容易验证，R_r'是R的右理想，$R_r' \cap (R_1' + \cdots + R_{r-1}' + R_{r+1}' + \cdots + R_n') = \{0\}$，$r = 1, 2, \cdots, n$。$R = R_1' + R_2' + \cdots + R_n'$，∴$R = R_1' \oplus R_2' \oplus \cdots + R_n'$。

5. 设F_1, F_2是两个域，命$R = F_1 \oplus F_2$，找出R的一切理想。

解 容易证明，仅含一个零元素的子集{0}及R本身，都是R的理想。

设 $B=\{(a_1,a_2)\mid a_1\in F_1, a_2\in F_2\}\neq\{0\}$，是$R$的一个理想。

(1) 若B中元素的第二坐标a_2恒为零。这时，$B\subseteq\{(a_1,0)\mid a_1\in F_1\}$。

$\because$ $B\neq\{0\}$，$\therefore$必存在$(a,0)\in B$，$a\in F_1$，$a\neq 0$。这时，任取$a_1\in F_1$，有$(a_1,0)=(a_1a^{-1},0)\cdot(a,0)\in B$，$\therefore$ $\{(a_1,0)\mid a_1\in F_1\}\subseteq B$。于是$B=\{(a_1,0)\mid a_1\in F_1\}$。

(2) 若B中元素的第一坐标a_1恒为零。这时，和(1)一样，可得$B=\{(0,a_2)\mid a_2\in F_2\}$。

(3) B中元素的第一、二坐标都不恒为零。这时，必有$(a,b)\in B$，其中$a\in F_1, b\in F_2$，a,b皆$\neq 0$。任取$(a_1,a_2)\in R$，则有$(a_1,a_2)=(a_1a^{-1},1)(a,b)(1,b^{-1}a_2)\in B$，$\therefore B=R$。

$\therefore$ R的理想是{0}，R本身，$B_1=\{(a_1 0)\mid a_1\in F_1\}$及$B_2=\{(0,a_2)\mid a_2\in F_2\}$。

注：本题可作为下一题的特例来处理，从而得出上述结果。

6.设R_1,R_2是有单位元的环，A_i是R_i的理想，$i=1,2$，证明，$A_1\oplus A_2$是$R_1\oplus R_2$的理想，且$R_1\oplus R_2$的任一理想均有上述形状。

证 按理想的定义，容易证明，当A_i是R_i的理想$(i=1,2)$时，$A_1\oplus A_2$是$R_1\oplus R_2$的理想。

设 B是$R_1\oplus R_2$的任一理想，命$A_1=B\cap R_1$，$A_2=B\cap R_2$，则容易证明，A_1是R_1的理想，A_2是R_2的理想，$A_1\cap A_2=(B\cap R_1)\cap(B\cap R_2)=B\cap(R_1\cap R_2)=\{0\}$，$\therefore$ $A_1+A_2=A_1\oplus A_2$，$A_1\oplus A_2\subseteq B$。

设 e_i是R_i的单位元，$i=1,2$，则易知，e_1+e_2是$R_1\oplus R_2$的单位元，且因R_i是$R_1\oplus R_2$的理想，故$ae_i\in R_i$，$\forall a\in R_1\oplus R_2$，$i=1,2$。任取$x\in B$，则有$x=xe_1+xe_2$，$xe_i\in R_i$，由$B$是$R_1\oplus R_2$的理想知$xe_i\in B$，$\therefore xe_i\in B\cap R_i=A_i$，$i=1,2$，$x=xe_1+xe_2\in A_1\oplus A_2$，$B\subseteq A_1\oplus A_2$。从而，$B=A_1\oplus A_2$。这就证得，$R_1\oplus R_2$的任一理想均有$A_1\oplus A_2$的形状，其中，$A_i$为$R_i$的理想，$i=1,2$。

7。设A是环R的理想，且A有单位元，证明，R有理想A'存在，使$R=A\oplus A'$。

证 设A中单位元为e，命$A'=\{x-xe\mid x\in R\}$，由原书p。203例3知A'为R的左理想，且$R=A\oplus A$。

任取$r\in R$，$x-xe\in A'$，因$e\in A$，A是R的理想，故$xer\in A$。从而，$xer-(xer)e-x(ere)$，而 $re\in A$，$ere=re$，$\therefore xer=xre$，$(x-xe)r=xr-xer=xr-xre\in A'$，故$A'$为$R$的右理想，从而，$A'$为$R$的理想。命题得证。

8。 设环R可表成其理想A_1，A_2的直和：$R=A_1\oplus A_2$，证明，A_1的任一自同构f均可扩为R到A_1的满同态。

证 $\because R=A_1\oplus A_2$，$\therefore R=\{a_1+a_2\mid a_1\in A_1,a_2\in A_2\}$。

命 $\tau:a_1+a_2\longmapsto a_1^f$，易知，$\tau$是$R$到$A_1$的映射，且$\therefore f$是$A_1$的自同构，$\therefore A_1^f=A_1$，$\tau$是$R$到$A_1$的满射。

$\because \tau(a_1+a_2)=a_1^f,\tau(b_1+b_2)=b_1^f$，$\therefore \tau((a_1+a_2)+(b_1+b_2))=\tau((a_1+b_1)+(a_2+b_2))=(a_1+b_1)^f=a_1^f+b_1^f=\tau(a_1+a_2)+\tau(b_1+b_2)$，$\tau((a_1+a_2)\cdot(b_1+b_2))=\tau(a_1b_1+a_2b_2)=(a_1b_1)^f=a_1^fb_1^f=\tau(a_1+a_2)\cdot\tau(b_1+b_2)$

$\therefore$ τ是R到A_1的满同态，且显然是f的扩充。

9。设A是环R的一个理想，若A的任一自同构均可扩为

R到A的满同态，则R中存在理想A'，使$R=A\oplus A'$。

证 取$f:x^f=x,\forall x\in A$，易知f是A的自同构，故由题设，f可扩为R到A的满同态τ：$x^\tau=x^f=x,\forall x\in A$。

命$A'=\{x|x\in R,x^\tau=0\}=Ker_\tau$，则$A'$为$R$的一个理想。

任取$x\in R,x=x^\tau+(x-x^\tau)$，则$x^\tau\in A,(x-x^\tau)^\tau=x^\tau-(x^\tau)^\tau=x^\tau-x^\tau=0$，$x-x^\tau\in A'$。 $\therefore x\in A+A'$，$R\subseteq A+A'$，但是，$A+A'\subseteq R$，故$R=A+A'$。

任取$y\in A\cap A'$，由$y\in A$知$y^\tau=y$，由$y\in A'$知$y^\tau=0$，$\therefore y=0$，$A\cap A'=\{0\}$，从而证得$R=A\oplus A'$。

习 题

1．设R是可换环，则R中一切幂零元的集合N作成R的一个理想。

证 $\because 0\in N$，$\therefore N$非空。

任取$a,b\in N$，由原书p.207的例1，可知$a-b\in N$。

任取$x\in R,a\in N$，设$a^m=0$，则$(xa)^m=(ax)^m=a^\tau x^m=0$，$\therefore xa\in N,ax\in N$，$\therefore N$是$R$的一个理想。

2．设R是可换环，A是R的理想，命$N(A)=\{x|x\in R,x^n\in A,n$是与$x$有关的自然数$\}$，证明，$N(A)$是$R$的理想。

设$R=\mathbf{Z}$．$A=(4)$，求$N(A)$。

设$R=\mathbf{Z}$．$A=(p^t)$，求$N(A)$。

设$R=\mathbf{Z}$．$A=(p_1^{l_1}p_2^{l_2})$求$N(A)$。

证 (1)任取$x,y\in N(A)$和$a\in R$，则有自然数m,n，使得$x^m\in A,y^n\in A$。 $\because R$是可换环，$\therefore (x-y)^{m+n-1}=\sum_{k=0}^{m+n-1}a_k$，其

中$a_k=(-1)^kC_k^{m+n-1}x^{(m+n-1)-k}y^k$。

若 $k\geqslant n$，则因$y^n\in A$，而A是环R的理想，$\therefore a_k\in A$；若$k<n$，则$(m+n-1)-k\geqslant m$，$\because x^m\in A$，A是R的理想，$\therefore a_k\in A$。因此可得$(x-y)^{m+n-1}\in A$，$x-y\in N(A)$。又 $\because (ax)^m=(xa)^m=a^mx^m\in RA\subseteq A$。$\therefore ax\in N(A)$，$xa\in N(A)$。故$N(A)$是$R$的理想，

(2) 当$R=\mathbf{Z}$，$A=(4)$时，任取$x\in N(A)$，则存在自然n，使$x^n\in(4)$，$\therefore 4\mid x^n$，$2\mid x$，因此$N(A)\subseteq(2)$。然而容易知道，$(2)\subseteq N(A)$。$\therefore N(A)=(2)$。

(3) 当$R=\mathbf{Z}$，$A=(p^t)$时，任取$x\in N(A)$，则存在自然数n，使$x^n\in(p^t)$，$p^t\mid x^n$，由于p是素数，$\therefore p\mid x$，$x\in(p)$，因此，$N(A)\subseteq(p)$。另一方面，任取$x\in(p)$，则 $p\mid x$，$\therefore p^t\mid x^t$，$x^t\in(p^t)=A$，于是 $x\in N(A)$，$(p)\subseteq N(A)$。$\therefore N(A)=(p)$。

(4) 当$R=\mathbf{Z}$，$A=(p_1^{\,l_1}p_2^{\,l_2})$，$p_1$，$p_2$是两个不相同的素数时，用上面同样的方法可以求得$N(A)=(p_1p_2)$。

3。设环R的加群$(R,+)$是循环群，则R是可换环。

证 $\because (R,+)$是循环群，$\therefore$若设$(R,+)$的生成元为a，则$R=\{na\mid n$为整数$\}$。

任取$x,y\in R$，则必存在整数m、n，使得$x=ma$，$y=na$，$\therefore xy=(ma)\cdot(na)=mna^2=(na)\cdot(ma)=yx$，$R$是可换环。

4。设R是可换环，A是R的理想，S是R的子集，命$(A:S)=\{x\mid x\in R,xS\subseteq A\}$。证明，$(A:S)$是$R$的一个理想。

当理想A，B具有关系$A\subseteq B$时，$(A:S)\supseteq(B:S)$。

当集合S，T具有关系$S\subseteq T$时，$(A:S)\supseteq(A:T)$。

证 (1)任取$x,y\in(A:S)$，则$x,y\in R$，xS，$yS\subseteq A$，而A是环R的理想，$\therefore (x-y)S\subseteq xS-yS\subseteq A$，$x-y\in(A:S)$。

$\forall a\in R$，$(ax)S=a(xS)\subseteq aA\subseteq A$，$\therefore ax\in(A:S)$。同样

地，$xa\in(A:S)$，$\therefore(A:S)$是R的一个理想。

(2) $\because A\subseteq B$，$\therefore$任取$x\in(A:S)$，有$xS\subseteq A\subseteq B$，$\therefore x\in(B:S)$，$(A:S)\subseteq(B:S)$。

(3) 任取$x\in(A:T)$，则$xT\subseteq A$，但$S\subseteq T$，$\therefore xS\subseteq xT\subseteq A$，故$x\in(A:S)$，$(A:T)\subseteq(A:S)$，即$(A:S)\supseteq(A:T)$。

5。设A，B，C是可换环R的理想，证明(1)$((A:B):C)=(A:BC)$，(2)$(A:C)\cap(B:C)=((A\cap B):C)$。

证 (1) 任取$x\in((A:B):C)$，则$xC\subseteq(A:B)$，$(xC)B\subseteq A$。$\because R$是可换环，$\therefore x(BC)\subseteq A$，$x\in(A:BC)$，$((A:B):C)\subseteq(A:BC)$。

任取$x\in(A:BC)$，则$xBC\subseteq A$，即$(xC)B\subseteq A$，$\therefore xC\subseteq(A:B)$，$x\in((A:B):C)$，$(A:BC)\subseteq((A:B):C)$。

综上$((A:B):C)=(A:BC)$。

(2) 任取$x\in(A:C)\cap(B:C)$，则$x\in(A:C)$，$x\in(B:C)$。$\therefore xC\subseteq A$，$xC\subseteq B$，$xC\subseteq A\cap B$。于是$x\in(A\cap B:C)$，$(A:C)\cap(B:C)\subseteq(A\cap B:C)$。

任取$x\in(A\cap B:C)$，则$xC\subseteq A\cap B$，$\therefore xC\subseteq A$，$xC\subseteq B$，$\therefore x\in(A:C)$，$x\in(B:C)$，$x\in(A:C)\cap(B:C)$，$(A\cap B:C)\subseteq(A:C)\cap(B:C)$。

综上$(A:C)\cap(B:C)=(A\cap B:C)$。

6。设R是有单位元1的环，$u\in R$，u有右逆元，证明，关于u的下述条件是等价的：(1)u有多于一个的右逆元，(2)u不是单位，(3)u是左零因子。

证 (1)⇒(2)：设u有多于一个的右逆元，则u至少有两个不同的右逆元u_1和u_2，于是$u(u_1-u_2)=uu_1-uu_2=1-1=0$。

如果u是单位，则u有逆元u^{-1}，$\therefore u_1-u_2=u^{-1}\cdot u(u_1-u_2)$
$=u^{-1}\cdot 0=0$，$u_1=u_2$。与已知$u_1\neq u_2$矛盾。$\therefore u$不是单位。

(2) $\Rightarrow$(3)：设u不是单位，且u有右逆元v，则$uv=1$，$vu\neq 1$。于是$u(vu-1)=(uv)u-u=0$，u是左零因子。

(3) $\Rightarrow$(1)：设u是左零因子，且u有一个右逆元v，使得$uv=1$。

$\because$ u是左零因子，$\therefore$存在一个$v'\in R$，$v'\neq 0$，使得$u\cdot v'=0$，于是$u(v+v')=1$，$v+v'$是u的右逆元，且不同于v。

7。设R是有单位元1的环，$u\in R$，u有多于一个的右逆元，证明，u有无限多个右逆元。

证 用反证法：假设u有$n(<\infty)$个右逆元，并设这些右逆元的集合为$S=\{v_1,v_2,\cdots,v_n\}$，则因u有多于一个的右逆元，$\therefore n\geqslant 2$。

令$T=\{v_1+1-v_iu\mid i=1,2,\cdots,n\}$，则因$u(v_1+1-v_iu)$
$=uv_1+u-uv_iu=1+u-u=1(i=1,2,\cdots,n)$，$\therefore T$中的任意一个元素也都是$u$的右逆元。

如果$v_1+1-v_iu=v_1+1-v_ju$，则$v_iu=v_ju$，$\therefore v_iuv_1=v_juv_1$，这就得到，$v_i=v_j$。$\therefore$当$i\neq j$时，由于$v_i\neq v_j$，$v_1+1-v_iu\neq v_1+1-v_ju$。$\therefore T$中的元素各不相同。

$\because S$和T都是u的n个不同的右逆元集合，$\therefore S=T$。
故必存在某个k，使得$v_1=v_1+1-v_ku$，于是得$v_ku=1$，由$uv_k=v_ku=1$，知u是单位。

但是，u有多于一个的右逆元，由第6题知，u不是单位，矛盾。$\therefore u$有无限多个右逆元。

8。设R是一个环，R的非零左理想只有本身，则$R^2=0$或R是除环。

证 任取$a\in R$，易知$Ra=\{xa|x\in R\}$是R的一个左理想。

(1) 若对任何$a\in R, a\neq 0$皆有$Ra\neq\{0\}$，则由题设，$Ra=R$。∴对于任意的$b\in R$，$ya=b$在R中有解，R是除环。

(2) 若至少存在一个$0\neq a\in R$，使$Ra=\{0\}$。作$R'=\{na|n\in\mathbf{Z}\}$，则R'是$(R,+)$的子群，且$R'\neq\{0\}$，而由$Ra=\{0\}$知，$r(na)=0, \forall r\in R$。故R'是R的一个非零左理想，从而$R'=R$。仍由$Ra=\{0\}$，可以得出$(ma)(na)=0$，于是$R^2=R'^2=\{0\}$。

9. 设R是一个单环，L是R的一切非零左理想的交，$L^2\neq 0$，则R有单位元。

证 由原书$p.208$例4可知：存在$e\in L, e\neq 0$，使得$e^2=e$，$Re=L$。

作$B=\{x|x\in R, xe=0\}$，容易知道，B是R的左理想。如果$B\neq\{0\}$，则有$B\supseteq L$，∴$e\in L\subseteq B$，$e\cdot e=0$，与已知$e^2=e\neq 0$矛盾，故$B=\{0\}$。∵$(x-xe)e=xe-xe^2=0, \forall x\in R$，∴$x-xe\in B=\{0\}$，$x-xe=0$，$xe=x$，$\forall x\in R$，即$Re=R$。而$Re=L$，∴$R=L$。

于是对于R的任一非零左理想A，由于$A\supseteq L=R$，$R\supseteq A$，∴$A=R$，即R的非零左理想只有本身，但$R^2=L^2\neq\{0\}$，由上题结论知，R是除环。从而，R有单位元。

注：本题中，“R是单环”这一条件可以省略。

10. 在上题中，证明R是一个除环。

证 上题已证。

11. 设R是一个环，$a\in R, a\neq 0$，证明，存在R的不含a的极大子环M，即M是R的子环，$a\notin M$，而R的任一真包含M的子环均含有a。

证 命$S=\{A|A$是R的子环，$a\notin A\}$，∵$\{0\}\in S$ ∴S非空。

S对于集合的包含关系作成一偏序集。取S的任一非空有序子集$L=\{A_\alpha|\alpha\in B\}$，命$A=\bigcup_{\alpha\in B}A_\alpha$。容易知道 A是R的一个子环，并且$a\notin A$(否则，如果$a\in A$,则存在某一个α,使得$a\in A_\alpha$，这与A_α的选择矛盾)，从而A是L的上界。$\therefore$ S的任一非空有序子集均有上界。故由 $Zorn$ 引理知,S含有一个极大元M，M即为R中不含a的极大子环。

12* 设R是一个环,S是R的子集，A是R的子环，$S\cap A=D$,证明R存在极大子环M,$M\supseteq A$，且$M\cap S=D$。

证 命$L=\{B|B$是R的子环,$B\supseteq A, B\cap S=D\}$,$\because A\in L$,$\therefore L$非空,且按集合包含关系成偏序集。取$L$的任一非空有序子集$L'=\{B_\alpha|\alpha\in I\}$,命$B=\bigcup_{\alpha\in I}B_\alpha$。容易证明，$B$是$R$的子环，且$B\cap S=(\bigcup_{\alpha\in I}B_\alpha)\cap S=\bigcup_{\alpha\in I}(B_\alpha\cap S)=\cup D=D$。$\therefore$ B是L'的上界,即L的任一非空有序子集均有上界，由$Zorn$ 引理，L有极大元M,M即为所求。

13* 设环R的理想I有单位元（即存在$e\in I$,$\forall a\in I$,$ea=ae=a$),A是I的理想，证明,A也是R的理想。

证 $\because$ A是I的理想，$\therefore$ A是R的子环。

设e是I的单位元,当然e也是A的单位元。任取$x\in R$,$a\in A$,有$xa=x(ea)=(xe)a$,$\because xe\in RI\subseteq I$,$\therefore xa=(xe)a\in IA\subseteq A$。同样地,$ax=(ae)x=a(ex)\in AI\subseteq A$,$\therefore A$是$R$的理想。

14 $(R,+,\cdot)$叫做一个弱环，若$(R,+,\cdot)$适合以下条件：

(1) $(R,+)$是一个加群，

(2) $(R,\cdot)$是一个半群，

(3) R中存在固定元素e_1,e_2：

$$\begin{aligned} x(y+z) &= xy+xz-e_1 \\ (y+z)x &= yx+zx-e_2, \end{aligned} \qquad \forall x,y,z\in R.$$

证明 $a)$ $e_1=e_2(=e)$;

$b)$ $xe=ex=e$, $\forall x\in R$;

$c)$ $x0=0x=e$;

$d)$ $x(y-z)=xy-xz+e$,

$(y-z)x=yx-zx+e$;

$e)$ $A=\{x\mid x\in R, xr=rx=e, \forall r\in R\}$是$R$的一个加法子群.

证 $a)$令 $x=y=z=0$, 则 $0(0+0)=0\cdot0+0\cdot0-e_1$, $(0+0)0=0\cdot0+0\cdot0-e_2$. $e_1=e_2=0^2$.

$b)$这里用 $c)$的结论: $\because xe=x0^2=(x0)0=e0=e$, $ex=0^2x=0(0x)=0e=e$, $\therefore$ $xe=ex=e$.

$c)$取$y=e, z=0$, 则, $xe=x(e+0)=xe+x0-e$, $ex=(e+0)x=ex+0x-e$, $\therefore x0=0x=e$.

$d)$ $\because xy=x(z+(y-z))=xz+x(y-z)-e$, $\therefore x(y-z)=xy-xz+e$.

同样可证: $(y-z)x=yx-zx+z$.

$e)$首先可知, $0\in A$, 故A非空. 任取$x,y\in A$, $\because xr=rx=e, yr=ry=e, \forall r\in R$, $\therefore (x-y)r=xr-yr+e=e-e+e=e$, $r(x-y)=rx-ry+e=e-e+e=e$.

故$(x-y)\in A$, A是R的加法子群.

15 举出一个弱环的例子.

解 设$R=\{0,x,y,e\}$, 规定$+$, $\cdot$如下表,

则$(R,+,\cdot)$成一弱环.

+	0	x	y	e
0	0	x	y	e
x	x	0	e	y
y	y	e	0	x
e	e	y	x	0

·	0	x	y	e
0	e	e	e	e
x	e	0	0	e
y	e	0	0	e
e	e	e	e	e

16 设R的理想A为幂零理想(即存在 n, $A^n=0$)且R/A为幂零环，证明R是幂零环。

证 因为R/A是幂零环，所以存在m，使$\prod_{i=1}^{m}\overline{a_i}=\overline{0}$，

$\forall\overline{a_i}\in R/A, i=1,2,\cdots,m$，即$\prod_{i=1}^{m}a_i\in A, \forall a_i\in R$。于是对$R$中任意$mn$个元$x_i$，$i=1,2,\cdots mn$，易知$\prod_{i=1}^{mn}x_i=0$，即$R^{mn}=0$，$R$是幂零环。

17. 设A,B是环R的幂零理想，证明$A+B$是R的幂零理想。

证 显然$A+B$是R的理想，由题设存在m,n，使$A^m=0$，$B^n=0$。而$(A+B)^{m+n}$的展开式中任意一项T_K必是s个A和t个B的乘积，且$s+t=m+n$。于是$T_K\subseteq A^s\cap B^t$，但$s\geqslant m, t\geqslant n$必有一成立，$\therefore T_K=0$，因此，$(A+B)^{m+n}=0$，$A+B$是$R$的幂零理想。

18. 设L是环R的一个幂零左理想，证明，R中存在幂零理想$A,B\supseteq L$。

证 设$L^r=\{0\}$。命$A=L+LR$，则有$A\supseteq L$，显见A是R

的理想。

用数学归纳法可证，$A^r=(L+LR)^r=L^r+L^rR$。事实上，假设$(L+LR)^{r-1}=L^{r-1}+L^{r-1}R$，则$(L+LR)^r=(L+LR)^{r-1}\cdot(L+LR)=(L^{r-1}+L^{r-1}R)(L+LR)=L^r+L^{r-1}RL+L^rR+L^{r-1}RLR\subseteq L^r+L^rR$。$\because L^r=\{0\}$，$\therefore A^r=0$，$A$是幂零理想。

19。设环R中任意两个非零理想A，B的积AB均不等于零，　证明，R的任意两个非零左理想L，M的积LM也不等于零。

证　命$A=L+LR$，$B=M+MR$，则由上题知A，B是R的两个非零理想，且由$RM\subseteq M$，有

$$AB=(L+LR)(M+MR)\subseteq LM+(LM)R$$

故若$LM=\{0\}$，将导致$AB=\{0\}$，与题设矛盾。$\therefore LM\neq\{0\}$。

20。设环R中任意两个非零左理想的积均不等于零，若对R中元素x，有$RxR=0$。则$x=0$。

证　显然当$R=\{0\}$时，$x=0$必成立，故不妨设$R\neq\{0\}$。

$\because Rx$与R是R的两个左理想，而$RxR=0$，$R\neq 0$，$\therefore$由题设可知$Rx=0$。由此可知，x生成的理想$(x)=\{xr+nx\mid r\in R,n\in\mathbf{Z}\}$，且$R\cdot(x)=0$。$\therefore(x)=0$，从而$x=0$。

21。　设R是可换环，P是R的一个理想，若对于R的任意理想A,B，$AB\subseteq P\Rightarrow A\subseteq P$或$B\subseteq P$则$P$是素理想。

证　设$x,y\in R$，且$xy\in P$。$\because P$是R的一个理想，$\therefore P\supseteq(xy)$。$\because R$是可换环，易知$(xy)=(x)(y)$，从而$(x)(y)\subseteq P$，由题设$(x)\subseteq P$或$(y)\subseteq P$，故$x\in P$或$y\in P$，$\therefore P$是素理想。

22。设R是有单位元$1\neq 0$的可换环，S是R的不含零元的乘法半群，P是R的与S的交为空集的极大理想，证明，P是素理想。

证 设$x,y\in R$,且$xy\in P$.如$x\notin P,y\notin P$,则由x,P生成的理想$(x,P)\supset P$.$\therefore (x,P)\cap S\neq\phi$.同理$(y,P)\cap S\neq\phi$.由于$S$是$R$的不含零元的乘法半群，可知,$((x,P)(y,P))\cap S\neq\phi$.

R是有单位元的可换环,从而$(x,P)(y,P)\subseteq(xy,P)=P$
$\therefore P\cap S\neq\phi$矛盾。$\therefore x,y$至少有一个属于$P$,$P$是素理想。

23. 设R是主理想整环，p是素元,证明(p)是素理想.

证 设 $a,b\in R,ab\in(p)$,则$ab=cp$,从而$p\mid ab$,$\because p$是素元,
$\therefore p\mid a$或$p\mid b$,即$a\in(p)$或$b\in(p)$,(p)是素理想.

24. 设R是主理想整环,证明，R中任意元a,b均有最大公约元d存在，并且，d 可表成 $ax+by$的形式,$x,y\in R$.

证 设a,b是R中任意元,显见$(a)+(b)$是R的一个理想，
$\because R$是主理想整环，$\therefore$存在$d\in R$,使$(a)+(b)=(d)$.$\because$ $a\in(d)$
$\therefore d\mid a$.同理$d\mid b$.又如$c\in R,c\mid a$, $c\mid b$,则$a\in(c),b\in(c)$,从而$(a)+(b)\subseteq(c)$, $\therefore d\in(c)$, $c\mid d$.因此,d是a,b的最大公约元.且
$\because d\in(a)+(b)$, 有$d=ax+by$,其中$x,y\in R$.

25. 设R是整数环$\mathbf{Z}$的同态像，证明，R的每一子环都是理想.

证 设 $\mathbf{Z}\overset{f}{\sim}R$, A是R的一个子环.于是,$f^{-1}(A)$是$\mathbf{Z}$的一个子环.但整数环$\mathbf{Z}$的子环都是$\mathbf{Z}$的理想，$\therefore f^{-1}(A)$是$\mathbf{Z}$的理想.从而,$A=f(f^{-1}(A))$是R的一个理想.

26. 设$R\overset{f}{\sim}R'$,L是R的极大理想,$f(L)=L'$，问L'是否是R'的极大理想?设$f(L)=L'$,L'是R'的极大理想，是否有L是R的极大理想?

解 L'不一定是R'的极大理想.

例如：命$R=\mathbf{Z}$,$R'=\mathbf{Z}/(3)$, $f:\begin{matrix}R\to R'\\ a\to\overline{a}\end{matrix}$, $R\overset{f}{\sim}R'$,

取$L=(2)$，则L是R的极大理想，但$L'=f(L)\neq R'$。$\therefore L'$不是R'的极大理想。

同样，L也不一定是R的极大理想。

例如：命f是整数环$\mathbf{Z}$到一个二元域$P=\{0,1\}$的同态，满足：$f(2n)=0, f(2n+1)=1, \forall n\in\mathbf{Z}$，则$(4)$是$\mathbf{Z}$的一个理想，$f((4))=(0)$是$P$的极大理想，而$(4)$显见非$\mathbf{Z}$的极大理想。

27．证明，不存在整环R，R含有6个元。

证 设整环R含有6个元，则$(R,+)$是6阶加群。由原书$P121$第13题知，$(R,+)$是6阶循环群。故可设$R=\{0, a, 2a, 3a, 4a, 5a\}$。则$a^2\in R$，$6a^2=6a\cdot a=0$。于是，$2a\cdot 3a=6a^2=0$，而$2a\neq 0$，$3a\neq 0$，这与$R$是整环矛盾。所以不存在仅含6个元的整环。

28．设R是有单位元的环，R含有子域F。R，F有共同单位元，证明，R的任一非零同态象均含有与F同构的子域。

证 设f是R的任一非零同态映射，显然$F\sim f(F)$。如果F与$f(F)$不同构，则存在$a,b\in F, a\neq b$，而$f(a)=f(b)$。

命$x=a-b$，则$x\in F$，$x\neq 0$，$f(x)=f(a)-f(b)=0$，因而$x\in kerf$。设x^{-1}是x的逆元素，由于$kerf$是R的理想，故$e=x^{-1}x\in kerf$。任取$y\in R$，则$y=ye\in kerf$，故$f(y)=0, \forall y\in R$。但这时f是零同态，矛盾。故有$F\simeq f(F)$。

29．设f是域F到域F'的同态映射，且$f(F)\neq 0$，则f是单一同态。

证 $kerf$是F的理想。而F是域，其理想只有0和F本身。由$f(F)\neq 0$，知$kerf\neq F$，$\therefore kerf=0$，f是单一同态。

本题也可利用上题结论，令$R=F$，由于$f(R)=f(F)\neq 0$，故$F\simeq f(F)$，所以f是单一同态。

30．在 $\mathbf{Z}[\sqrt{-x}]$中分解21为既约元的乘积。

解 设$R=\mathbf{Z}[\sqrt{-5}]$，命S表示乘法半群$(R,\cdot)$，由原书P．171例1知，S中的单位只有±1。

设$21=(a+b\sqrt{-5})(c+d\sqrt{-5})=ac-5bd+(bc+ad)\sqrt{-5}$，

则 $$bc+ad=0,\quad ac-5bd=21$$

解之得 $$c=\frac{21a}{a^2+5b^2},\qquad d=-\frac{21b}{a^2+5b^2},$$

由于d是整数，故当$b\neq0$时，$5b^2\leqslant a^2+5b^2\leqslant|21b|$，因而$-4\leqslant b\leqslant4$。

由于a,b,c,d都是整数，故b仅能为$0,\pm1,\pm2$。故求得：

(甲)$21=3\cdot7=(4+\sqrt{-5})(4-\sqrt{-5})=(1+2\sqrt{-5})(1-2\sqrt{-5})$

及(乙)$21=(-3)(-7)=(-4+\sqrt{-5})(-4-\sqrt{-5})=(-1+2\sqrt{-5})(-1-2\sqrt{-5})$

由于S中的单位仅有±1，故(甲)中各分解式是不同的分解，(乙)中的分解式分别与(甲)中相应的分解式相伴。现在证明(甲)中各因子，从而(乙)中各因子都是$\mathbf{Z}[\sqrt{-5}]$中的既约元。

如果素数p不是既约元，设$p=(a+b\sqrt{-5})(c-d\sqrt{-5})$是$p$的一个真分解，则$b\neq0,d\neq0$，且$(a,b)=1,(c,d)=1$。

由于$p=(a+b\sqrt{-5})(c-d\sqrt{-5})=ac+5bd+(bc-ad)\sqrt{-5}$，故$p=ac+5bd$，$bc=ad$。由$b\mid ad$，$(a,b)=1$，知$b\mid d$。由$d\mid bc$，$(c,d)=1$，知$d\mid b$。故$d=\pm b$，$c=\pm a$（同时取“+”号或“−”号），$p=\pm(a^2+5b^2)$。因为$p>0$，故$p=a^2+5b^2$。即存在整数$a,b$，使$p=a^2+5b^2$。当$p=3$及$p=7$时，$p=a^2+5b^2$无整数解，故3和7是$\mathbf{Z}[\sqrt{-5}]$中既约元。

如果$x+y\sqrt{-5}$不是既约元，设$x+y\sqrt{-5}=(a+b\sqrt{-5})$

$(c+d\sqrt{-5})$是一个真分解，这时，$x-y\sqrt{-5}=(a-b\sqrt{-5})(c-d\sqrt{-5})$，$x^2+5y^2=(x+y\sqrt{-5})(x-y\sqrt{-5})=(a+b\sqrt{-5})(c+d\sqrt{-5})(a-b\sqrt{-5})(a-b\sqrt{-5})=(a^2+5b^2)(c^2+5d^2)$。这时，$a^2+5b^2$和$c^2+5d^2$都不是既约元，即整数$x^2+5y^2$可分解成两个非既约的整数的乘积。由于21仅能分解成3和7的乘积，而3和7都是既约元，因此(甲)中各因子都是既约元。

31. $R=\mathbf{Z}[i]$(高斯整环)，下列理想，哪些是素理想？

(5)，(9)，(11)，(3)。

解 由于$2+i\overline{\in}(5)$，$2-i\overline{\in}(5)$，而$(2+i)(2-i)=5$，故$(2+i)(2-i)\in(5)$，因此(5)不是素理想。

由于$3\overline{\in}(9)$，$3^2\in(9)$，故(9)不是素理想。

设p是一个素数，如果$(a+bi)(c+di)\in(p)$，则$(a+bi)(c+di)=p(m+ni)$。又$(a-bi)(c-di)=p(m-ni)$，故$(a^2+b^2)(c^2+d^2)=p^2(m^2+n^2)$。因而$p$必整除整数$a^2+b^2$和$c^2+d^2$中的一个。不妨设$p\mid(a^2+b^2)$，即$a^2+b^2\equiv0(mod\,p)$。

取$p=11$，由于对于任意整数x，$x^2\equiv0,1,3,4,5,9(mod\,11)$，而1，3，4，5，9中任意两数之和皆不被11整除，故由$a^2+b^2\equiv0(mod\,11)$，必得$a^2\equiv0(mod\,11)$，且$b^2\equiv0(mod\,11)$，故$11\mid a$，$11\mid b$，$a+bi\in(11)$，故(11)是素理想。

当$p=3$时，由于对于任意整数x，$x^2\equiv0,1(mod\,3)$，而$1+1=2$不被3整除，故由$a^2+b^2\equiv0(mod\,3)$，必得$a^2\equiv0$，$(mod\,3)$，$b^2\equiv0(mod\,3)$。故$3\mid a$，且$3\mid b$，$a+bi\in(3)$，故(3)是素理想。

32. 设R是一个环，$R^*=R\backslash\{0\}$作成的乘法半群，并且，对R中任一非零元r，存在非负整数$\nu(r)$具有性质：对任意$a,b\in R$，$a\neq0$，存在q_1,q_2,r_1,r_2，使

$b=q_1a+r_1, r_1=0$或$v(r_1)<v(a)$，

$b=aq_2+r_2, r_2=0$或$v(r_2)<v(a)$。

证明，R有单位元，并且R中任意两个元均存在左边的以及右边的最大公约元。

证 因为非负整数的非空集合有最小数，故可设$a\in R$，使$v(a)$最小。由于对任意$0\neq r\in R$，总有$v(r)\geqslant v(a)$，故对任意$b\in R$，存在q_1, q_2，使得$b=q_1a=aq_2$。对a本身也存在e, e'，使$a=ea=ae'$。由$ea=a$可知$eaq_2=aq_2$，即$eb=b$。由$ae'=a$可知，$q_1ae'=q_1a$，即$be'=b$。因此e是R的左单位元，e'是R的右单位元。故$e'=ee'=e$，所以e是R的单位元。

任取$x, y\in R$，并设$x\neq 0$，则根据已知条件有以下等式：

$$y=q_1x+r_1$$

$$x=q_2r_1+r_2$$

$$r_1=q_3r_2+r_3$$

$$\cdots\cdots\cdots$$

因为$v(r_1)>v(r_2)>v(r_3)>\cdots$，故经过有限步后，必有

$$r_{n-1}=q_{n+1}r_n+r_{n+1}$$

$$r_n=q_{n+2}r_{n+1}$$

故 $r_{n-1}=q_{n+1}r_n+r_{n+1}=q_{n+1}q_{n+2}r_{n+1}+r_{n+1}=(q_{n+1}q_{n+2}+e)r_{n+1}$，因此$r_{n+1}$是$r_{n-1}$的一个右约元。由$r_{n+1}$是$r_{n-1}$和$r_n$的右约元，可推出$r_{n+1}$是$r_{n-2}$的右约元，因而$r_{n+1}$是$x$和$y$的一个右边的公约元。任取$x$和$y$的一个右边的公约元$a$，则$a$也是$r_1$的右约元。由于$a$是$x$和$r_1$的右约元，故$a$也是$r_2$的右约元，由此类推，可知$a$是$r_{n+1}$的右约元，故$r_{n+1}$是$x$和$y$的一个右边的最大公约元。同理可知，存在$x$和$y$的左边的最大公约元。

33. 设 $R=\{a+b\sqrt{-2}\mid a, b\in\mathbf{Z}\}$, $\alpha=a+b\sqrt{-2}$, 规定 $\nu(\alpha)=a^2+2b^2$.

证明, R 是欧氏环.

证 显然, R 是含单位元的整环. 我们注意到上面定义的 $\nu(\alpha)=a^2+2b^2$, 实际上就是复数 $\alpha=a+b\sqrt{-2}$ 的范数, 故对任何复数有定义. 并且, 只要 $\alpha\neq 0$, 就有 $\nu(\alpha)$ 是正实数, 而且对任意 α,β, 均有 $\nu(\alpha\beta)=\nu(\alpha)\nu(\beta)$.

对 $\alpha\in R^*$, $\beta\in R$, 设 $\alpha^{-1}\beta=k+l\sqrt{-2}$, 其中 k,l 是有理数. 取 k', l' 分别为最接近 k, l 的整数, 于是有 $|k-k'|\leqslant\frac{1}{2}$, $|l-l'|\leqslant\frac{1}{2}$. 命 $\gamma=k'+l'\sqrt{-2}$, 则

$$\nu(\alpha^{-1}\beta-\gamma)=(k-k')^2+(2l-l')^2\leqslant\frac{1}{4}+\frac{1}{2}=\frac{3}{4}$$

命 $\delta=\beta-\alpha\gamma$, 则 $\gamma,\delta\in R$, 且 $\beta=\alpha\gamma+\delta$. 若 $\delta\neq 0$, 则

$$\nu(\delta)=\nu(\beta-\alpha\gamma)=\nu(\alpha)\nu(\alpha^{-1}\beta-\gamma)\leqslant\frac{3}{4}\nu(\alpha)<\nu(\alpha),$$

故 R 是欧氏环.

34. 设 R 是欧氏环, p 是 R 中素元, 证明 $R/(p)$ 是域.

证 因为 R 是欧氏环, 故 R 的任一理想都是主理想. 今设 $(p)\subsetneqq(a)$, 则 $p\in(a)$, 故存在 $x\in R$, 使得 $p=ax$. 因为 p 是素元, 当然是既约元, 故 a,x 中必有一个是单位. 如果 x 是单位, 则 $a=px^{-1}\in(p)$, 从而 $(a)\subseteq(p)$, 与 $(p)\subsetneqq(a)$ 矛盾. 故 a 是单位, 这时 $(a)=R$, 因此 (p) 是极大理想. 由于 R 是含单位元的可换环, (p) 是极大理想, 故 $R/(p)$ 是域.

35. 在主理想整环 R 中, a,b 说是互素的, 如果 $(a,b)=R$. 证明, R 中与取定元素 a 互素的元所组成的模 (a) 的剩余类作成乘法群.

$R=\mathbf{Z}$，a-7，$\mathbf{Z}$中与7互素的整数所组成的模(a)的剩余类作成的乘法群含有几个元，$a=8$的情形如何？

证 首先，如果a,b互素，则对于任意$x\in b+(a)$，a,x互素。这是因为由a,b互素可知，$(a,b)=R$，所以单位元$e\in(b,a)$，故存在$h,k\in R$，使$e=ah+bk$，因为$x\in b+(a)$，故可设$x=b+ay$，即$b=x-ay$，因而$e=ah+bk=ah+(x-ay)k=a(h-yk)+xk\in(a,x)$，故$(a,x)=R$，所以$a,x$互素。设 $S=\{b+(a)\mid b\in R,(a,b)=R\}$，则$S\subseteq R/(a)$。任取 $b+(a)\in S,c+(a)\in S$，由于$e\in(a,b),e\in(a,c)$，故可设$e=ah+bk,e=ax+cy$，则

$$e=(ah+bk)(ax+cy)=a(ahx+bkx+chy)+bc(ky)\in(a,bc)。$$

因此，$(b+(a))(c+(a))=bc+(a)\in S$，$S$是一个乘法半群。并且由于$e=ah+bk\in(a,k)$，故$k+(a)\in S$，而

$$(b+(a))(k+(a))=bk+(a)=bk+ah+(a)=e+(a)。$$

所以，对于任意$b+(a)\in S$，存在逆元素$k+(a)\in S$，因而S对乘法作成群。

当$R=\mathbf{Z},a=7$时，S含有6个元$\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6}$。

当$R=\mathbf{Z},a=8$时，S含有4个元$\overline{1},\overline{3},\overline{5},\overline{7}$。

36. 找出$\mathbf{Z}/(8)$的一切非零理想，它们的交是什么？

解 $\mathbf{Z}/(8)$的任一理想都是$A/(8)$，其中A是$\mathbf{Z}$的理想，且$A\supseteq(8)$。由于$\mathbf{Z}$是主理想整环，故存在$a\in\mathbf{Z}$，使$A=(a)$。由于$(a)\supseteq(8)$，所以$8\in(a)$，故$a\mid 8$。反之，对于任意整数a，如果$a\mid 8$，则$(a)\supseteq(8)$。因而$\mathbf{Z}/(8)$的非零理想有且仅有$\mathbf{Z}/(8)$，$(2)/(8),(4)/(8)$。由于$\mathbf{Z}\supset(2)\supset(4)$，故$\mathbf{Z}/(8)\supset(2)/(8)\supset(4)/(8)$，因而它们的交为$(4)/(8)$。

37. 证明，$\mathbf{Z}/(p^n)$（此处p是素数）的一切非零理想的交是

一个非零理想。

证 仿上题易知$\mathbf{Z}/(p^n)$的一切非零理想为$\mathbf{Z}/(p^n)$，$(p_n)/(p^n)\cdots$，$(p^{n-1})/(p^n)$。并且$\mathbf{Z}/(p^n)\supset(p)/(p^n)\supset\cdots\supset(p^{n-1})/(p^n)$。故$\mathbf{Z}/(p^n)$的一切非零理想的交是$(p^{n-1})/(p^n)$，它是$\mathbf{Z}/(p^n)$的一个非零理想。

38. 设$P_1\supseteq P_2\supseteq\cdots$是可换环$R$中素理想的降链，证明$P=\bigcap_{i=1}^{\infty}P_i$是$R$的素理想。

证 显然，P是R的一个理想。任取$a,b\in R$，如果$ab\in P$，则对任意α，$ab\in P_\alpha$。假设$a\overline{\in}P$，则必存在α，使$a\overline{\in}P_\alpha$，由于这是一个降链，故$a\overline{\in}P_\beta$，$\forall\beta\geqslant\alpha$。由于$P_\beta$是素理想，而$ab\in P_\beta$，且$a\overline{\in}P_\beta$，因而$b\in P_\beta$，$\forall\beta\geqslant\alpha$。当$\beta<\alpha$时，由于$P_\beta\supseteq P_\alpha$，$\therefore b\in P_\beta$，因而对一切$\beta$均有$b\in P_\beta$，从而$b\in P$，故$P$是$R$的素理想。

39. 设F是域，$F\langle x\rangle$表示一切形式幂级数

$f=a_0+a_1x+\cdots+a_nx^n+\cdots=\sum_{i=0}^{\infty}a_ix^i$关于下面的加乘作成的环：

$$\sum a_ix^i+\sum b_ix^i=\sum(a_i+b_i)x^i$$

$$\sum a_ix^i\cdot\sum b_ix^i=\sum_{k=1}^{\infty}\Big(\sum_{i+j=k}a_ib_j\Big)x^k$$

证明 $F\langle x\rangle$只有一个极大理想。

证 任取$f=a_0+a_1x+\cdots+a_nx^n+\cdots\in F\langle x\rangle$，其中$a_0\neq0$。

命$h=b_0+b_1x+\cdots+b_nx^n+\cdots$，

其中$b_0=a_0^{-1}$，$b_n=-a_0^{-1}\Big(\sum_{i=0}^{n-1}a_{n-i}b_i\Big)$，$n=1,2,3,\cdots$。

则$fh=e$。

所以f是$F\langle x\rangle$中的单位。设I是$F\langle x\rangle$的任意一个真理想，则任取$f=a_0+a_1x+\cdots+a_nx^n+\cdots\in I$时，必有$a_0=0$。因为否则$I$中含有单位，因而$I=F\langle x\rangle$，与$I$是真理想矛盾。设$S=\{f|=a_0+a_1x+\cdots+a_nx^n+\cdots\in F\langle x\rangle, a_0=0\}$，则$S$包含$F\langle x\rangle$的一切真理想，且显然$S$是$F\langle x\rangle$的一个真理想。设$M$是$F\langle x\rangle$的任一极大理想。由于$M$是真理想，故$S\supseteq M$，由于$M$是极大理想，故$S=M$，即$S$是$F\langle x\rangle$的唯一的极大理想。

40。设F是域，$(F)_\infty$表示F上所有矩阵。

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & \cdots \\ a_{21} & a_{22} & \cdots & a_{2n} & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{pmatrix}$$

的集合，但每一列中只有有限个元素不等于零，证明，$(F)_\infty$关于矩阵的$+,\times$作成一个环。

证 任取$A,B\in(F)_\infty$，设A的第i列有h_i个元素不等于零，B的第i列有k_i个元素不等于零，则$A+B$的第i列至多有h_i+k_i个元素不等于零，即只有有限个元素不等于零。现在讨论AB的第i列的元素。设B的第i列中最后一个不为零的元素在第k_i行。因为A的每一列的非零元素的个数有限，故A的前k_i列中非零元素的个数有限。设这些元素分布在前h_i行，则对任意$m>h_i$，由于A的第m行元素中前k_i个元素均为零，而在B的第i列中仅有前k_i个元素可能不等于零，故在AB的第i列中，第m个元素必为零，即只有前h_i个元素可能不为零，故AB的每一列中只有有限个元素不等于零。因而$(F)_\infty$对$+,\times$运算封闭。容易验证$(F)_\infty$作成一个环。

41. 设A是一个不含零因子的环，证明$(A,+)$中每一元皆有相同周期.

证　如果$(A,+)$中所有非零元具有无限周期，则可认为周期相同. 今设$a\in(A,+)$，且$a\neq 0$，并设a具有有限周期m，则$ma=0$. 任取$b\in(A,+)$，且$b\neq 0$. 由于$0=(ma)b=m(ab)=a(mb)$，而A无零因子，且$a\neq 0$，故$mb=0$，即b有有限周期. 设b的周期为n，则$n\mid m$. 同理可知，$m\mid n$，因而$m=n$. 故A中所有非零元具有相同周期m.

42. 设f是环R到R'的满同态，$K=\ker f$，证明$R[x]/k[x]\cong R'[x]$.

证　对于任意$a_0+a_1x+a_2x^2+\cdots+a_nx^n\in R[x]$.

命φ：$a_0+a_1x+\cdots+a_nx^n\longmapsto f(a_0)+f(a_1)x+\cdots+f(a_n)x^n$

容易验证，φ是环$R[x]$到$R'[x]$的满同态，且$K\ker\varphi=K[x]$. 故$R[x]/K[x]\simeq R'[x]$.

43. 找出$\mathbf{Z}[x]$的一切同态象.

解　任取一个非负整数n，并设a是环$\mathbf{Z}/(n)$上超越元或代数元. 命

$$\varphi:\ \mathbf{Z}[x]\longrightarrow\mathbf{Z}/(n)[a]$$
$$f(x)\longmapsto\overline{f}(a)$$

其中$\overline{f}(x)$是将$f(x)$中的系数$a\in\mathbf{Z}$换成$a+(n)\in\mathbf{Z}/(n)$而得到的多项式. 易知φ是满同态映射. 故$\mathbf{Z}[x]\sim\mathbf{Z}/(n)[a]$.

反之，设环R'是环$\mathbf{Z}[x]$的同态象，则可设ψ是环$\mathbf{Z}[x]$到环R'的满同态映射. 命$a=\psi(x)$，则有$R'=\psi(Z)[a]$. 但$\mathbf{Z}\sim\psi(\mathbf{Z})$，故有非负整数$n$使$\psi(\mathbf{Z})\cong\mathbf{Z}/(n)$，$\therefore R'\cong\mathbf{Z}/(n)[a]$.

故$\mathbf{Z}[x]$的一切同态象是$\mathbf{Z}/(n)[a]$，其中n是非负整数，a是环$\mathbf{Z}/(n)$上超越元或代数元.

第四章　格

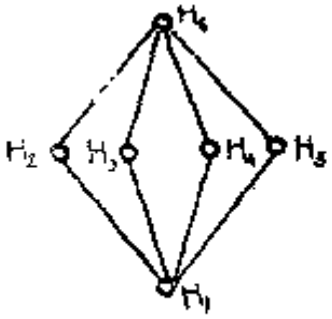
练习

§1　定义及基本性质

1．设$G=S_3$，作$L(G)$的图形．

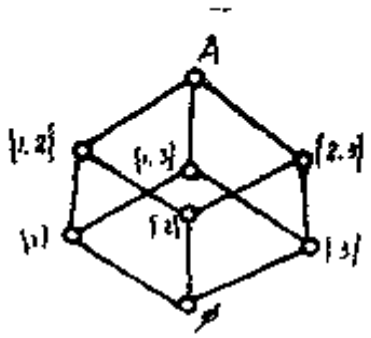
解　$G=S_3=\{(1),(12),(13),(23),(123),(132)\}$．$G$的所有子群如下：

$H_1=\{(1)\}$，$H_2=\{(1),(12)\}$，$H_3=\{(1),(13)\}$．$H_4=\{(1),(23)\}$，$H_5=\{(1),(123),(132)\}$．$H_6=\{(1),(12),(13),(23),(123),(132)\}$．则得$L(G)$的图形如右图．



2．设$A=\{1,2,3\}$，作出A的幂集格$(2^A,\subseteq)$的图形．

解　由$A=\{1,2,3\}$可得$2^A=\{\phi,\{1\},\{2\},(3),\{1,2\},\{1,3\},\{2,3\},A\}$则得$(2^A,\subseteq)$的图形如右图．

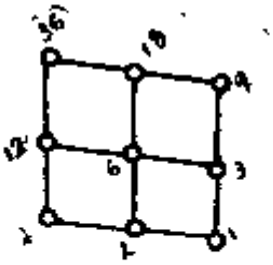


3．设$S=\{1,2,3,4,6,9,12,18,36\}$，当$a|b$时规定$a\leqslant b$．

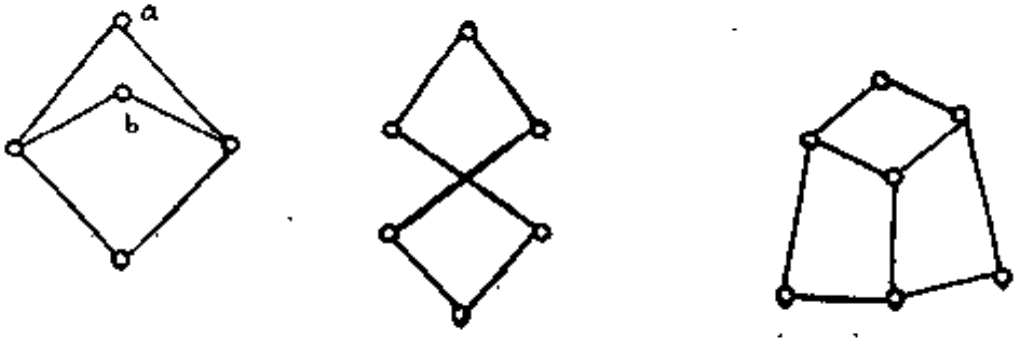
证明，$(S,\subseteq)$是一个格，作出S的图形．

证　显见S是由36的一切正约数组成的，S对于所规定

的“$\leqslant$”是偏序集．任取$a,b\in S$，易知$a\cap b=(a,b)$，$a\cup b=[a,b]$．而且，$\because a\mid 36, b\mid 36$，$\therefore (a,b)\mid 36$，$[a,b]\mid 36$，$\therefore a\cup b$，$a\cap b$皆$\in S$，$\therefore$ $(S,\subseteq)$是一个格．S的图形如右图．



4. 下面图形给出的偏序集，哪一个是格？



解 中图、右图是格，左图中$\{a,b\}$没有最小上界，故不是格．

5. 设φ是格S到S'的满同态，S有零元和单位元，证明，S'也有零元和单位元．

证 设0，1分别是S的零元和单位元，当然$\varphi(0)\in S'$，$\varphi(1)\in S'$．$\because \varphi$是格S到S'的满同态，$\therefore$ S'的任意元可写成$\varphi(a)$，其中$a\in S$．而$\varphi(a)\cup\varphi(0)=\varphi(a\cup 0)=\varphi(a)$，$\varphi(a)\cap\varphi(1)=\varphi(a\cap 1)=\varphi(a)$，$\therefore \varphi(0)$、$\varphi(1)$即为$S'$的零元和单位元．

6．设S是一个格，A是S的所有自同态的集合，证明，A关于变换的合成作成一个有单位元的半群．

证 任取$\varphi_1,\varphi_2,\varphi_3\in A$.则有:$\varphi_i(a\cup b)=\varphi_i(a)\cup\varphi_i(b)$, $\forall a,b\in S,i=1,2,3$,及$\varphi_i(a\cap b)=\varphi_i(a)\cap\varphi_i(b)$, $\forall a,b\in S,i=1,2,3$. $\therefore$ $(\varphi_1\varphi_2)(a\cup b)=\varphi_1(\varphi_2(a\cup b))=\varphi_1(\varphi_2(a)\cup\varphi_2(b))=\varphi_1(\varphi_2(a))\cup\varphi_1(\varphi_2(b))=(\varphi_1\varphi_2)(a)\cup(\varphi_1\varphi_2)(b)$. 同样有: $(\varphi_1\varphi_2)(a\cap b)=(\varphi_1\varphi_2)(a)\cap(\varphi_1\varphi_2)(b)$, $\therefore\varphi_1\varphi_2\in A$. $\therefore$ A是半群.令φ是S的恒等变换, 即$\varphi(a)=a$, $\forall a\in S$,则 $\varphi(a\cup b)=a\cup b=\varphi(a)\cup\varphi(b)$,$\varphi(a\cap b)=a\cap b=\varphi(a)\cap\varphi(b)$, $\therefore$ $\varphi\in A$. $\therefore$ A是一个有单位元的半群.

7. 设A,B是两个集合, f是A到B的映射, 证明, $S=\{f(x)\mid x\in 2^A\}$是$(2^B,\subseteq)$的一个子格.

证 显见$S\subseteq 2^B$.任取$f(x_1),f(x_2)\in S$, $\because$ $x_1,x_2\in 2^A$, $\therefore$ $x_1\cup x_2$, $x_1\cap x_2\in 2^A$. $\therefore f(x_1\cup x_2)$, $f(x_1\cap x_2)\in S$,而$f(x_1\cup x_2)=f(x_1)\cup f(x_2)$,$f(x_1\cap x_2)=f(x_1)\cap f(x_2)$, $\therefore S$对$\cap$, $\cup$封闭,S是$(2^B,\subseteq)$的一个子格.

8. 证明, 在任意格 $(S,\cup,\cap)$中, 均有 $a\cup(b\cap c)\leqslant(a\cup b)\cap(a\cup c)$,$(a\cap b)\cup(a\cap c)\leqslant a\cap(b\cup c)$.

证 $\because a\cup b\geqslant a, a\cup b\geqslant b\geqslant b\cap c$, $\therefore a\cup b\geqslant a\cup(b\cap c)$.又$a\cup c\geqslant a, a\cup c\geqslant c\geqslant b\cap c$, $\therefore a\cup c\geqslant a\cup(b\cap c)$. $\therefore a\cup(b\cap c)\leqslant(a\cup b)\cap(a\cup c)$.对它应用对偶原理即得:$(a\cap b)\cup(a\cap c)\leqslant a\cap(b\cup c)$.

9. 设L_1,L_2是两个格,证明,加氏积$L_1\times L_2$对下面规定的$\cup$,$\cap$作成一个格.$(a_1,a_2)\cup(b_1,b_2)=(a_1\cup b_1,a_2\cup b_2)$, $(a_1,a_2)\cap(b_1,b_2)=(a_1\cap b_1,a_2\cap b_2)$.

若L_1,L_2都有单位元和零元, 证明, $L_1\times L_2$也有单位元和零元.

证 $\because a_i,b_i\in L_i,i=1,2$; $\therefore a_i\cup b_i,a_i\cap b_i\in L_i,i=1,2$.

$\therefore (a_1 \cup b_1,\ a_2 \cup b_2), (a_1 \cap b_1, a_2 \cap b_2) \in L_1 \times L_2$. 易知$\cup$, $\cap$适合算律L_1-L_4. $\therefore (L_1 \times L_2, \cup, \cap)$作成一个格. 设$0_i, 1_i$为$L_i (i=1,2)$的零元和单位元. 当然$(0_1,0_2), (1_1,1_2) \in L_1 \times L_2$, 对任意$(a_1, a_2) \in L_1 \times L_2$, $\because (a_1,a_2) \cup (0_1,0_2) = (a_1 \cup 0_1, a_2 \cup 0_2) = (a_1,a_2)$ $(a_1,a_2) \cap (1_1,1_2) = (a_1 \cap 1_1, a_2 \cap 1_2) = (a_1,a_2)$, $\therefore (0_1,0_2)$, $(1_1,1_2)$为$L_1 \times L_2$的零元和单位元.

10. 设 0 , I是格S的零元和单位元, 证明 $x \cup y = 0 \Rightarrow x = y = 0$, $x \cap y = I \Rightarrow x = y = I$, 此处$x, y$是$S$的任意元.

证 因为0, I 是格 S 的零元和单位元, 则: $a \cup 0 = a$, $\forall a \in S$; $a \cap I = a$, $\forall a \in S$. $\because a \cup 0 \geqslant 0$, $a \cap I \leqslant I$, $\therefore a \geqslant 0$, $a \leqslant I$, $\forall a \in S$, 由$x \cup y \geqslant x$及$x \cup y = 0$即得$0 \geqslant x$, 但$x \geqslant 0$, 从而$x = 0$, 同样$y = 0$. 又由$x \cap y \leqslant x$及$x \cap y = I$即得$I \leqslant x$, 但$x \leqslant I$, 从而$x = I$, 同样$y = I$.

11*. 设S是一个格, S的非空子集J说是S的一个理想, 如果以下条件被满足:

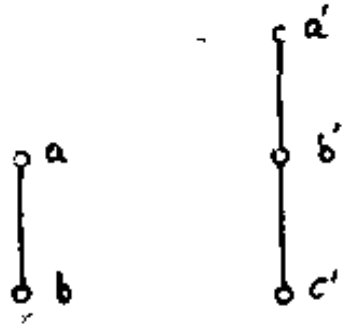
①$\forall a, b \in J$: $a \cup b \in J$

②$\forall a \in J$, $x \in S$: $a \cap x \in J$.

证明, a) 理想J是S的子格, 而S的子格不一定是理想. b) 设φ是格S到S'的同态映射, A是S的子格, J是S的理想, 则$\varphi(A)$是$\varphi(S)$的子格, $\varphi(J)$是$\varphi(S)$的理想, c) $\varphi(A)$是不是S'的子格? $\varphi(J)$是不是S'的理想?

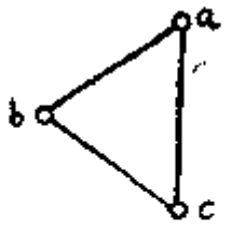
证 a) 任取$a, b \in J$则$a \cup b \in J$. 又$b \in J \subseteq S \therefore a \cap b \in J$. $\therefore J$是S的子格. 又如S是含有零元 0 和单位元1的n元格 ($n \geqslant 3$). 则$\{0,1\}$显然是S的一个子格, 设$a \in S$, 且$a \neq 0$、1, 由$1 \cap a = a \in \{0,1\}$, 可知$\{0,1\}$非S的理想. b) 任取$\varphi(a)$, $\varphi(b) \in \varphi(A)$, $\because a, b \in A \therefore a \cup b$, $a \cap b \in A$, $\therefore \varphi(a \cup b), \varphi(a \cap b) \in \varphi(A)$, 即$\varphi$

$(a)\cup\varphi(b),\varphi(a)\cap\varphi(b)\in A$. $\therefore\varphi(A)$是$\varphi(S)$的子格. 任取$\varphi(a),\varphi(b)\in\varphi(J),\varphi(x)\in\varphi(S)$. $\because J$是S的理想, $\therefore a\cup b\in J$, $a\cap x\in J$, $\varphi(a\cup b)\in J,\varphi(a\cap x)\in J$,即: $\varphi(a)\cup\varphi(b)\in\varphi(J)$, $\varphi(a)\cup\varphi(x)\in\varphi(J)$. $\therefore\varphi(J)$是$\varphi(S)$的理想. c)显然$\varphi(A)$是S'的子格. 当φ是满同态映射, 即$\varphi(S)=S'$时,$\varphi(J)$是S'的理想,反之$\varphi(J)$可以不是S'的理想. 例如在右图中$S=\{a,b\}$, $S'=\{a',b',c'\}$. 令: $\varphi(a)=a'$, $\varphi(b)=b'$. 易知φ是格S到S'的同态映射. 取$J=S$. 显见J是S的理想. 而$\varphi(J)=\{a',b'\}$不是S'的理想, $\because a'\in\varphi(J),c'\in S'$. 而$a'\cap c'=c'\overline{\in}\varphi(J)$.



12. 证明,n元格的图形中不可能出现以三个元为顶点而边上没有元的三角形.

证 用反证法. 如出现这样的三角形如右图,则一方面,$\because$ $\overline{a\ \ c}$ 边上没有元, 即表示不存在满足$a>x>c$的元x. 另方面由图中可知$a>b>c$.故得矛盾.



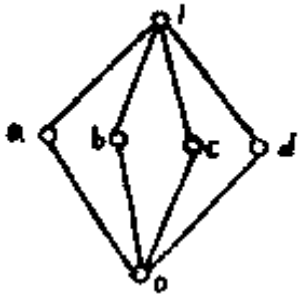
13. 设S是一个格,S的元$x_1,x_2,\cdots,x_n$经$\cup$, $\cap$用各种方式连结起来的式子叫做格多项式,记为$f(x_1,x_2,\cdots,x_n)$.设$x_i\leqslant y_i$, $i=1,2,\cdots,n$, 证明对任意格多项式f, 均有$f(x_1,x_2,\cdots,x_n)\leqslant f(y_1,y_2,\cdots y_n)$.

证 记f中出现$\cup$,$\cap$的次数为m. 当$m=0$时, 结论显然成立. 以下对$m\geqslant 1$的情形用归纳法:
当$m=1$时.即证$x_1\cup x_2\leqslant y_1\cup y_2$,$x_1\cap x_2\leqslant y_1\cap y_2$.

$\because y_1 \cup y_2 \geqslant y_1 \geqslant x_1, y_1 \cup y_2 \geqslant y_2 \geqslant x_2 \therefore x_1 \cup x_2 \leqslant y_1 \cup y_2$。同样可得 $x_1 \cap x_2 \leqslant y_1 \cap y_2$。设 $m \leqslant K$ 时，结论成立，则当 $m = K+1$ 时。将 $f(x_1, x_2, \cdots, x_n)$ 按最后一次 $\cup$ 或 $\cap$ 分成两个格多项式，即 $f(x_1, x_2, \cdots, x_n) = f_1(x_1, x_2, \cdots, x_n) \cup f_2(x_1, x_2, \cdots, x)$ 或 $f(x_1, x_2, \cdots, x_n) = f_1(x_1, x_2, \cdots, x_n) \cap f_2(x_1, x_2, \cdots, x_n)$，则 f_1, f_2 中出现 $\cup$，$\cap$ 的次数 $\leqslant K$，由归纳假设应有 $f_1(x_1, x_2, \cdots, x_n) \leqslant f_1(y_1, y_2, \cdots y_n)$，$f_2(x_1, x_2, \cdots, x_n) \leqslant f_2(y_1, y_2, \cdots, y_n)$。应用前面 $m = 1$ 时的同样方法可得 $f_1(x_1, x_2, \cdots, x_n) \cup f_2(x_1, x_2, \cdots x_n) \leqslant f_1(y_1, y_2, \cdots y_n) \cup f_2(y_1, y_2, \cdots, y_n)$，$f_1(x_1, x_2, \cdots, x_n) \cap f_2(x_1, x_2, \cdots x_n) \leqslant f_1(y_1, y_2, \cdots, y_n) \cap f_2(y_1, y_2, \cdots, y_n)$，即：$f(x_1, x_2, \cdots, x_n) \leqslant f(y_1, y_2, \cdots, y_n)$

§2 Dedekind 格

1. 举出两个仅含有6个元的格，一个是分配格，另一个不是分配格。



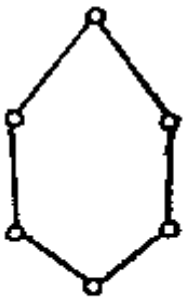
解 令：$S_1 = \{1, 2, 3, 4, 5, 6\}$，$\leqslant$ 表示普通数的大小，因为任一有序集都是分配格，故 $(S_1, \leqslant)$ 成一分配格。(参见本章后面的习题中第一题)

S_2 为右图所示的格，由图可知：$a \cap (b \cup c) = a \cap 1 = a$，而 $(a \cap b) \cup (a \cap c) = 0 \cup 0 = 0$，$\therefore a \cap (b \cup c) \neq (a \cap b) \cup (a \cap c)$，$S_2$ 不是分配格。

2. 举出两个仅含有6个元的格，一个是 *Dedekind* 格，另

一个不是*Dedekind*格。

解 首先我们证明这样一个命题："格L不是模格的充要条件是存在$x,y,z\in L$满足：$x>z, x\cup y=z\cup y, x\cap y=z\cap y$"。先证必要性：设$L$不是模格则有$a,b,c\in L$满足$a\geqslant c$而$a\cap(b\cup c)>(a\cap b)\cup c$。令：$x=a\cap(b\cup c), z=(a\cap b)\cup c, y=b$。则易验证$x,y,z$适合：$x>z$，$x\cup y=b\cup c=z\cup y, x\cap y=a\cap b=z\cap y$。再证充分性：如$L$中存在适合命题条件的$x$，$y$，$z$。则：$x>z, x\cap(y\cup z)=x\cap(x\cup y)=x, (x\cap y)\cup z=(z\cap y)\cup z=z$。$\therefore x\cap(y\cup z)>(x\cap y)\cup z$。即$x,y,z$不适合模律。当然$L$不是模格，故命题得证。利用反证法易知上面命题中蕴含着y和x,z皆不可比。此时x，$y,z,x\cap y$，$x\cap y$构成L的一个五边形子格。由此可得与上面命题等价的一个命题："L是模格的充要条件为：L不含有五边形子格。"根据此命题易知：左图是六个元的模格。右图是六个元的非模格。



3. 设S是分配格，a是S的固定元。

$$\varphi:\ x\longmapsto x\cap a,\qquad \psi:\ x\longmapsto x\cup a,$$

证明φ,ψ是S的两个自同态，找出$\varphi(S),\psi(S)$。

证 任取x，$y\in S$。则$\varphi(x\cup y)=(x\cup y)\cap a=(x\cap a)\cup(y\cap a)=\varphi(x)\cup\varphi(y)$，$\varphi(x\cap y)=(x\cap y)\cap a=(x\cap a)\cap(y\cap a)=\varphi(x)\cap\varphi(y)$。$\therefore\varphi$是$S$的自同态。同样可证$\psi$也是$S$的自同态。又由：$\varphi(x)=x\cap a\leqslant a, \forall x\in S$，及任意$x\leqslant a$都有$x=x\cap a$，从而

$\varphi(x)=x$，可知：$\varphi(S)=\{x|x\in S, x\leqslant a\}$，同样可得：$\psi(S)=\{x|x\in S, x\geqslant a\}$。

4. 设φ是格S到S'的同态映射，证明，$\varphi(S)$是S'的子格。

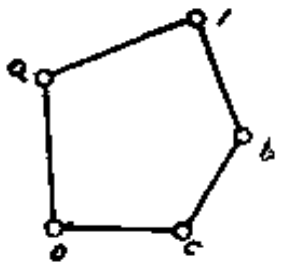
证 本题是§1.练习，第11题c)的特殊情形，即取$A=S$即得本题结论。

5. 设S是$Dcdekind$格，$x,y,a\in S$，$x\neq y$，x复盖a，y也复盖a，证明，$x\cup y$复盖x，并复盖y。

证 $\because x>a, y>a$. $\therefore x\cap y\geqslant a$. $x\geqslant x\cap y\geqslant a$, $y\geqslant x\cap y\geqslant a$. 如$x\cap y\neq a$，则由$x$，$y$皆复盖$a$得到$x\cap y=x=y$与$x\neq y$矛盾。$\therefore x\cap y=a$，$\because$ S是$Dedekind$格。$\therefore x\cup y/x$与$y/x\cap y$同构。从而$x\cup y/x$与y/a同构。$\because y$复盖a，$\therefore$ $x\cup y$复盖x。又由$x\cup y/y$与x/a同构。$\because x$复盖a，$\therefore x\cup y$复盖y。

6. 举例说明，在不是$Dedekind$格的格S中，存在x到0的两个极大链，具有不同的长度。

解 设S是右图所示的格。$\because b>c$而$b\cap(a\cup c)=b\cap 1=b$，$(b\cap a)\cup c=0\cup c=c$，$\therefore b\cap(a\cup c)\neq(b\cap a)\cap c$，$S$不是$Dedekind$格。



$1>a>0$与$1>b>c>0$显然是1到0的两个长度不同的极大链。

7. 设φ是格S到S'的同态映射，考虑集合S关于映射φ的商集$S/\varphi=\{\bar{a}|a\in S\}$，此处$\bar{a}=\{x|x\in S, \varphi(x)=\varphi(a)\}$。在$S/\varphi$中规定二元运算$\cup$，$\cap$：

$\forall\ \overline{a}, \overline{b}\in S/\varphi$：$\overline{a}\cup\overline{b}=\overline{a\cup b}$，$\overline{a}\cap\overline{b}=\overline{a\cap b}$。

证明，$\cup$，$\cap$确是S/φ的两个二元运算，且$(S/\varphi, \cup, \cap)$是一

个格。命$\varphi_*: \overline{a} \longmapsto \varphi(a)$，则$\varphi_*$是$S/\varphi$到$\varphi(S)$的同构映射。

证 任取$\overline{a}$，$\overline{b}$，$\overline{c}$，$\overline{d} \in S/\varphi$。若$\overline{a}=\overline{c}$，$\overline{b}=\overline{d}$。则易得$\varphi(a)=\varphi(c)$，$\varphi(b)=\varphi(d)$，$\therefore \varphi(a\cup b)=\varphi(a)\cup\varphi(b)=\varphi(c)\cup\varphi(d)=\varphi(c\cup d)$，$\varphi(a\cap b)=\varphi(a)\cap\varphi(b)=\varphi(c)\cap\varphi(d)=\varphi(c\cap d)$，从而$\overline{a\cup b}=\overline{c\cup d}$，$\overline{a\cap b}=\overline{c\cap d}$，$\therefore \cup, \cap$确是$S/\varphi$的两个二元运算，容易验证$\cup, \cap$适合算律$L_1-L_4$。$\therefore (S/\varphi, \cap, \cap)$是一个格。$\because \varphi_*(\overline{a})=\varphi(a)$，$\therefore \varphi_*(\overline{a})\cup\overline{b})=\varphi_*(\overline{a\cup b})=\varphi(a\cup b)=\varphi(a)\cup\varphi(b)=\varphi_*(\overline{a})\cup\varphi_*(\overline{d})$。$\forall \overline{a}, \overline{b} \in S/\varphi$同样有：$\varphi_*(\overline{a}\cap\overline{b})=\varphi_*(\overline{a})\cap\varphi_*(\overline{b})$。$\therefore \varphi_*$是$S/\varphi$到$\varphi(S)$的同态映射。易知$\varphi_*$是满射。又由$\varphi(a)=\varphi(b)$可得$\overline{a}=\overline{b}$。$\therefore \varphi_*$是单射。$\therefore \varphi_*$是$S/\varphi$到$\varphi(S)$的同构映射。

8.（此题与§1练习第6题相同）

9. 设S是一个分配格，a，$b \in S$，且$a<b$。证明，$\varphi: x \longmapsto (x\cup a)\cap b$是$S$到$b/a$的一个同态映射。

证 首先可知φ是S到自身的一个映射。又对于任意$x \in S$，$(x\cup a)\cap b \leqslant b$，$\because a \leqslant x\cup a$，$a<b$，$\therefore a \leqslant (x\cup a)\cap b$。$\therefore \varphi$是$S$到$b/a$的一个映射，又对于任意$x, y \in S$。

$$\varphi(x\cup y)=((x\cup y)\cup a)\cap b=((x\cup a)\cup(y\cup a))\cap b=((x\cup a)\cap b)\cup((y\cup a)\cap b)=\varphi(x)\cup\varphi(y)$$

$$\varphi(x\cap y)=((x\cap y)\cup a)\cap b=((x\cup a)\cap(y\cup a))\cap b=((x\cup a)\cap b)\cap((y\cup a)\cap b)=\varphi(x)\cap\varphi(y)$$

$\therefore \varphi$是S到b/a的一个同态映射。

10. 指出下面证明中的错误，并举出反例。

设S是任意格，$x \in S$，x到0的极大链的最大长度为d，则x到0的任一极大链的长均为d。

证　设x到0的长度为d的极大链为：

$x=x_0>x_1>\cdots>x_n=0$。

$x=x_0>y_1>\cdots>y_s=0$

是x到0的任一极大链，我们用数学归纳法，证明$d=s$。当$d=1$时，因x复盖0，故$y_1=0$，即$s=1$，命题成立。假定命题对$d-1$成立，即任意y，只要y到0的极大链的最大长度为$d-1$，则y到0的任一极大链的长度均为$d-1$。我们看d的情形。由于x复盖y_1，故y_1到0的极大链的最大长度为$d-1$，由归纳假定，$s-1=d-1\Rightarrow s=d$，即命题对任意d都成立。

解　错误在于“由于x复盖y_1，故y_1到0的极大链的最大长度为$d-1$”。因为由x复盖y_1，只能得到y_1到0的极大链的最大长度$\leqslant d-1$。事实上当S不是 *Dedekind* 格时y_1到0的极大链的最大长度可以小于$d-1$。

前面第6题解中的格即是一个反例。在那里取$x=1$，则x到0的极大链的最大长度为3，$x>a>0$是x到0的另一极大链其长为2，但a到0的极大链的最大长度为$1<3-1$。可知证明中这一断言是错误的。

§3　布尔代数

1．设f是布尔代数$(S,\cup,\cap,',0,I)$到布尔代数S'的同态映射，证明：$f(S)$是S'的子代数。

证　设$a,b\in S$，$\because f(0)=f(a\cap a')=f(a)\cap f(a')$
$=f(a)\cap(f(a))'$，

$f(1)=f(a\cup a')=f(a)\cup f(a')=f(a)\cup(f(a))'$

$\therefore f(0), f(1)$即S'的零元和单位元，且属于$f(S)$。

任取$f(a), f(b) \in f(S)$。$\because (f(a))' = f(a') \in f(S)$。

$f(a) \cup f(b) = f(a \cup b) \in f(S)$。

$f(a) \cap f(b) = f(a \cap b) \in f(S)$　$\therefore f(S)$是S'的子代数。

2．设f是布尔代数S到S'的同态映射，S表示集合S关于映射f的商集：$\overline{S} = S/f = \{\overline{a} \mid a \in S\}$，$\overline{a} = \{x \mid x \in S, f(x) = f(a)\}$

如下规定$\overline{S}$的运算：对任意$\overline{a}$，$\overline{b} \in S$

$\overline{a} \cup \overline{b} = \overline{a \cup b}$，$\overline{a} \cap \overline{b} = \overline{a \cap b}$，$\overline{a}' = \overline{a'}$。证明，$\overline{S}$作成一个布尔代数，($\overline{S}$叫做$S$关于$f$的商代数)。

证　因为布尔代数S, S'首先都是格，f首先是格S到格S'的同态映射，故由§2练习中的第7题即可知$(\overline{S}, \cup, \cap)$是一个格。$\because S$是分配格，$\therefore a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$ $\forall a, b, c \in S$，于是$\overline{a} \cap \overline{(b \cup c)} = \overline{(a \cap b)} \cup \overline{(a \cap c)}$

即$\overline{a} \cap (\overline{b} \cup \overline{c}) = (\overline{a} \cap \overline{b}) \cup (\overline{a} \cap \overline{c})$ $\forall \overline{a}, \overline{b}, \overline{c} \in S$，$\therefore \overline{S}$是分配格，容易验证所定义的$\overline{a}'$由$\overline{a}$唯一确定。又$\overline{a} \cup \overline{0} = \overline{a \cup 0} = \overline{a}$，$\overline{a} \cap \overline{1} = \overline{a \cap 1} = \overline{a}$ $\therefore \overline{0}$，$\overline{1}$即$\overline{S}$的零元和单位元，且易验证$\overline{a}'$是$\overline{a}$的补元。$\therefore \overline{S}$是一个布尔代数。

3．同上题，命$J = f^{-1}(0) = \{x \mid x \in S, f(x) = 0(S'$中零元$)\}$证明，$J$具有性质：

①$0 \in J$。

②设$a \in J$，则对一切$x \leqslant a$，均有$x \in J$。

③$\forall a, b \in J \Rightarrow a \cup b \in J$。

(具有性质②③的子集叫做S的一个理想)。

证　①由第1题可知$f(0)$是S'的零元。$\therefore 0 \in J$。②$a \in J$，

$x \leqslant a$，　$\therefore$　$f(a)=0, x=x\cap a$。$\therefore f(x)=f(x\cap a)=f(x)\cap f(a)=f(x)\cap 0=0$。$\therefore x\in J$。③由$a,b\in J$得$f(a)=f(b)=0$，$\therefore f(a\cup b)=f(a)\cup f(b)=0\cup 0=0$，$\therefore a\cup b\in J$。

4。设f是布尔代数S到S'的满同态，φ是S到$\overline{S}=S/f$的映射：φ：$a\longmapsto\overline{a}$，证明，φ是布尔代数S到$\overline{S}$的满同态映射（称φ为自然同态）。

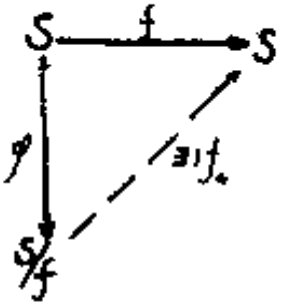
证　显见φ是S到$\overline{S}$的满射。任取$a,b\in S$。

$\varphi(a\cup b)=\overline{a\cup b}=\overline{a}\cup\overline{b}=\varphi(a)\cup\varphi(b)$

$\varphi(a\cap b)=\overline{a\cap b}=\overline{a}\cap\overline{b}=\varphi(a)\cap\varphi(b)$

$\varphi(a')=\overline{a'}=(\overline{a})'=(\varphi(a))'$，$\therefore\varphi$是$S$到$\overline{S}$的满同态映射。　〔注：此题无需$f$是“满”的。因为无论$f$是否“满”，总有$\varphi$是“满”的。〕

5。设S,S'是布尔代数，f是S到S'的满同态，φ是S到S/f的自然同态，证明，存在唯一的同构映射f_*使右面图形交换：



证　命f_*：$\overline{a}\longmapsto f(a)$，由练习第7题即知$f_*$是格$S/f$到$f(S)$的同格映射，再利用$f$是$S$到$S'$的满同态。就有$f(S)=S'$，故$f_*$是格$S/f$到$S'$的同构映射。

又$\because f_*(\overline{a}')=f_*(\overline{a'})=f(a')=(f(a))'=(f_*(\overline{a}))'$

$\therefore f_*$是布尔代数S/f到S'的同构映射。显见$f_*\varphi(a)=f_*(\overline{a})=f(a)$　$\forall a\in S$。　$\therefore f_*\varphi=f$，f_*使题中图形交换，由原书$P.27$定理2。即得f_*唯一。

6。找出8元布尔代数的所有子代数。

解　设S是8元布尔代数，由本节定理2，$S\cong(2^A,\subseteq)$，其

中$A=\{a,b,c\}$.从而S的所有子代数与$(2^A, \subseteq)$的所有子代数同构.

由于含有限个元的布尔代数的元数是2的正整数次幂，从而易知：$A_1=\{A,\phi\}$,

$A_2=\{A,\{a,b\},\{c\},\phi\}$,

$A_3=\{A,\{a,c\},\{b\},\phi\}$,

$A_4=\{A,\{b,c\},\{a\},\phi\}$,

$A_5=\{A,\{a,b\},\{a,c\},\{b,c\},\{c\},\{b\},\{a\},\phi\}$.

为$(2^A,\subseteq)$的所有子代数. 而S的所有子代数与以上子代数同构.

7. 设A,B是两个集合，$A\cap B=\phi$,任取$S\subseteq A$, $T\subseteq B$. 命$f: S\cup T\longmapsto(S, T)$, 证明:$f$是布尔代数$(2^{A\cup B}, \subseteq)$到$2^A\times 2^B$的同构映射.

证 首先证明,对于任意的$S\in 2^A, T\in 2^B$有$S\cap T=\phi$.

$\because S\subseteq A, T\subseteq B, \therefore S\cap T\subseteq A\cap B=\phi, \therefore S\cap T=\phi$.下证$f$是$2^{A\cup B}$到$2^A\times 2^B$的一个映射.设$S_1\cup T_1=S_2\cup T_2$,则$A\cap(S_1\cup T_1)=A\cap(S_2\cup T_2)$. 即$(A\cap S_1)\cup(A\cap T_1)=(A\cap S_2)\cup(A\cap T_2)$, $S_1\cup\phi=S_2\cup\phi, S_1=S_2$同样有$T_1=T_2$. $\therefore f$是一个映射.易知f既是单射又是满射.

任取$S_i\cup T_i\in 2^{A\cup B}, i=1,2$. $f((S_1\cup T_1)\cup(S_2\cup T_2))=f((S_1\cup S_2)\cup(T_1\cup T_2))=(S_1\cup S_2, T_1\cup T_2)=(S_1,T_1)\cup(S_2,T_2)=f(S_1\cup T_1)\cup f(S_2\cup T_2)$.

$f((S_1\cup T_1)\cap(S_2\cup T_2))=f((S_1\cap(S_2\cup T_2))\cup(T_1\cap(S_2\cup T_2)))=f(((S_1\cap S_2)\cup(S_1\cap T_2))\cup((T_1\cap S_2)\cup(T_1\cap T_2)))=f((S_1\cap S_2)\cup(T_1\cap T_2))=(S_1\cap S_2, T_1\cap T_2)=(S_1,T_1)\cap(S_2,T_2)=$

$f(S_1 \cup T_1) \cap f(S_2 \cup T_2)$。

$\because (S'_1 \cup T_1') \cup (S_1 \cup T_1) = (S'_1 \cup S_1) \cup (T'_1 \cup T_1) = A \cup B = 1$, $(S'_1 \cup T_1') \cap (S_1 \cup T_1) = (S'_1 \cap S_1) \cup (T'_1 \cap T_1) = \phi \cup \phi = 0$。

$\therefore (S_1 \cup T_1)' = S_1' \cup T_1'$, $\therefore f((S_1 \cup T_1)') = f(S_1' \cup T_1') = (S_1', T_1') = (S_1, T_1)' = (f(S_1 \cup T_1))'$。

$\therefore f$是布尔代数 $(2^A, \subseteq)$到$2^A \times 2^B$的同构映射。

8. 设S是元数大于2的布尔代数，任取$a \in S$, $a \neq I$, $a \neq o$ 证明$T = \{o, I, a, a'\}$是S的一个子代数。

证 结论是显然的。

9. 证明二元布尔代数是一个域。

证 设$S = \{o, I\}$是一个二元布尔代数，则由S确定的布尔环是有单位元的可换环，而S仅含两个元，即可知此布尔环必是域。

10. 设J是布尔代数S的理想，则J也是布尔环$(S, +, \cdot)$的理想。反之亦然。

证 设J是布尔代数S的理想。任取$a, b \in J$。则$a + b = (a \cap b') \cup (a' \cap b)$，利用分配律可得：$a + b = (a' \cup b') \cap (a \cup b)$，$\therefore a + b \leqslant a \cup b \in J$，从而$a - b = a + b \in J$。$\therefore J$是布尔环$(s, +, \cdot)$的加法子群。任取$a \in J$, $x \in S$。$\because J$是布尔代数S的理想。$\because x \cap a \leqslant a \therefore x \cap a \in J$即$x \cdot a \in J$，$\therefore J$是布尔环$(s, +, \cdot)$的理想。反之，设$J$是布尔环$(s, +, \cdot)$的理想，则对$a \in J$及一切$x \leqslant a$, $\because x \cdot a \in J$, $\therefore x \cap a \in J$，即$x \in J$。任取$a, b \in J$。$\because J$是布尔环$(s, +, \cdot)$的理想，$\therefore a + b + ab \in J$，即$a \cup b \in J$，$\therefore J$是布尔代数$S$的理想。

习题

1. 证明，任一有序集都是分配格。

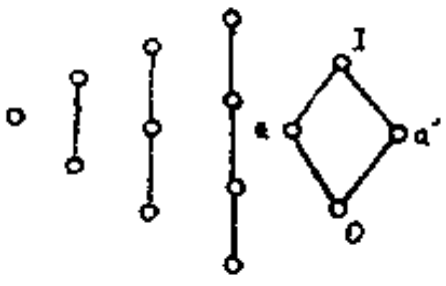
证 设S是有序集，易知S必是格。任取$a,b,c\in S$，不妨认为$a\geqslant b\geqslant c$，则：1) $a\cap(b\cup c)=a\cap b=b$，$(a\cap b)\cup(a\cap c)=b\cup c=b$，$\therefore a\cap(b\cup c)=(a\cap b)\cup(a\cap c)$。2) $b\cap(a\cup c)=b\cap a=b$，$(b\cap a)\cup(b\cap c)=b\cup c=b$，$\therefore b\cap(a\cup c)=(b\cap a)\cup(b\cap c)$。3) $c\cap(a\cup b)=c\cap a=c$，$(c\cap a)\cup(c\cap b)=c\cup c=c$。$\therefore c\cap(a\cup b)=(c\cap a)\cup(c\cap b)$。$\therefore a,b,c$适合分配律，$S$是分配格。

2*. 证明，格S是有序集的充要条件是：S的每一非空子集都是子格。

证 设格S是有序集，A是S的任一非空子集。任取$a,b\in A$，$\because S$是有序集，不妨设$a\geqslant b$，则$a\cup b=a$，$a\cap b=b$，$\therefore a\cup b,a\cap b\in A$，$\therefore A$是子格。又如格$S$的每一非空子集皆子格，则任取$a,b\in S$，$\because\{a,b\}$是子格，$\therefore a\cup b,a\cap b\in\{a,b\}$。如$a\cup b=a$，则$a\geqslant b$。如$a\cup b=b$，则$b\geqslant a$。$\therefore S$是有序集。

3. 决定所有元数$\leqslant 4$的格，并证明它们都是分配格。

证 元数$\leqslant 4$的格如右图所示。有序集当然是分配格。所以只须对$\{0,I,a,a'\}$验证它是分配格就可以了，而这也是容易直接验证的。



4. 设G是P^n阶循环群，P是素数，证明，$L(G)$是

分配格。

证 设$G=(a), a^{p^n}=e$。令：$G_i=(a^{p^i})$, $i=0,1,\cdots,n$。易知G_i为G的所有子群，且有：$G=G_0\supset G_1\supset\cdots\supset G_n=(e)$。$\therefore L(G)$ 成有序集，由第1题可知$L(G)$ 是分配格。

5。证明，格S是分配格的充要条件是：$\forall x,y,z\in S$：

$(x\cap y)\cup(y\cap z)\cup(z\cap x)=(x\cup y)\cap(y\cup z)\cap(z\cup x)$。

证 设格S是分配格，则对任意$x,y,z\in S$

$(x\cap y)\cup(y\cap z)\cup(z\cap x)=(x\cap y)\cup(z\cap(x\cup y))$

$=((x\cap y))\cup z)\cap((x\cap y)\cup(x\cup y))$

$=(x\cup z)\cap(y\cup z)\cap(x\cup y)$。反之设$S$是格，$\forall x,y,z\in S$，有

$(x\cap y)\cup(y\cap z)\cup(z\cap x)=(x\cup y)\cap(y\cup z)\cap(z\cup x)$。(1)

则对于任何$a,b,c\in S$若$a\geqslant c$，则显见$a\cup b\geqslant c\cup b, a\cap b\geqslant c\cap b$。

于是 $(a\cap b)\cup(b\cap c)\cup(c\cap a)=(a\cap b)\cup c$,

$(a\cup b)\cap(b\cup c)\cap(c\cup a)=(b\cup c)\cap a$。由 (1) 可知：

$a\cap(b\cup c)=(a\cap b)\cup c$ (2) 又由 (1) 式可知：

$x\cap((x\cap y)\cup(y\cap z)\cup(z\cap x))=x\cap((x\cup y)\cap$

$(y\cup z)\cap(z\cup x))=x\cap(x\cup y)\cap(y\cup z)\cap(z\cup x)=x\cap(z\cup x)$

$\cap(y\cup z)=x\cap(y\cup z)$。

$\because x\geqslant x\cap y, x\geqslant z\cap x$。$\therefore x\geqslant(x\cap y)\cup(z\cap x)$,

令 $a=x, b=y\cap z, c=(x\cap y)\cup(z\cap x)$，则$a\geqslant c$，代入 (2)式，即得：$x\cap((x\cap y)\cup(y\cap z)\cup(z\cap x))=(x\cap(y\cap z))$

$\cup((x\cap y)\cup(z\cap x))=((x\cap y)\cap z)\cup(x\cap y)\cup(z\cap x)$

$=(x\cap y)\cup(z\cap x)$。$\therefore x\cap(y\cup z)=(x\cap y)\cup(x\cap z)$。

$\therefore S$是分配格。

6。设$(R,+,\cdot)$是一个环。命S表示 $(R,+)$ 的所有子加群所成集合，$a,b\in S$，规定$a\cap b$表示子加群的交，$a\cup b$ 表示

子加群a,b的和。证明，

$(S,\cup,\cap)$ 作成一个格。L(R)表示环$(R,+,\cdot)$ 的子环格，证明，就集合来说，$L(R)\subseteq S$。L (R)是不是S的子格？

证 $(S,\cup,\cap)$即$(R,+)$的子群格。任取$(R_0,+,\cdot)\in L(R)$，$\because(R_0,+,\cdot)$ 是 $(R,+,\cdot)$的子环。显然 $(R_0,+)$是$(R,+)$的子加群$\therefore(R_0,+)\in S$，$\therefore$就集合来说$L(R)\subseteq S$。$L(R)$不一定是S的子格。例如：取环 $(R,+,\cdot)$为一个二元布尔环，易知此时$L(R)=S$。$\therefore$ $L(R)$是S的子格。 又如：取$R=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\mid a,b,c,d\in\mathbf{Q}\}$，则 $(R,+,\cdot)$是一个环，易知：$R_1=\{a+b\sqrt{2}\mid a,b\in\mathbf{Q}\}$和$R_2=\{a+b\sqrt{3}\mid a,b\in\mathbf{Q}\}$对$+,\cdot$构成$R$的子环。即$R_1,R_2\in L(R)$ 而对S中的$\cup$有$R_1\cup R_2=\{a+b\sqrt{2}+c\sqrt{3}\mid a,b,c\in\mathbf{Q}\}$
易知$R_1\cup R_2$不是环$(R,+,\cdot)$的子环。$\therefore$ $L(R)$不是S的子格 。

7。设G是一个群，$L(G)$表示G的子群格，N (G) 表示G的正规子群格，证明N (G) 是$L(G)$的子格。

证 显然$N(G)\subseteq L(G)$。任取$A,B\in N(G)$，因为$A\cap B,A\cup B$仍是G的正规子群，$\therefore$ $A\cap B,A\cup B\in N(G)$，$\therefore$ $N(G)$是$L(G)$的子格。

8。设A是任意集合，S是A的一切二元关系作成的集合，规定S中的$\cup,\cap$如下：
$\forall a,b\in A,R_1,R_2\in S$：$a(R_1\cap R_2)b\Longleftrightarrow aR_1b$并且$aR_2b$；
$a(R_1\cup R_2)b\Longleftrightarrow aR_1b$或$aR_2b$。
证明，$(S,\cup,\cap)$作成一个格。S是否有单位元？是否有零元？

证 易知$R_1\cap R_2,R_1\cup R_2$仍是A的二元关系，且$\cap,\cup$

适合算律L_1-L_4，$\therefore (S,\cup,\cap)$作成一个格。

令$R=A\times A$，$R_0=\phi$，则$\forall a,b\in A$有aRb，$aR_0{}'b$，可知R，$R_0\in S$。任取$R_1\in S$，$\because\ a(R_0\cup R_1)b\Longleftrightarrow aR_0b$或$aR_1b\Longleftrightarrow aR_1b$，$a(R\cap R_1)b\Longleftrightarrow aRb$并且$aR_1b\Longleftrightarrow aR_1b$，$\therefore\ R_0\cup R_1=R\cap R_1=R_1$。$\therefore\ R_0,R$即$S$的零元和单位元。

9. 设$(S,\subseteq)$是有零元的格，如果S中任一非空子集的并均属于S，那末S是完全格。

证 只证S中任意非空子集A的交$\bigcap\limits_{a\in A}a$均属于S即可。命$M=\{x\mid x\in S,\forall a\in A:\ x\leqslant a\}$，$\because\ O\in M$，$\therefore\ M$非空。

令$l=\bigcup\limits_{x\in M}x$，由题设$l\in S$。下证$l=\bigcap\limits_{a\in A}a$。

任取$a\in A$，由M的定义知a是M的一个上界，从而$l\leqslant a$即l是A的一个下界。设$s\in S$，且s是A的一个下界，则$s\in M$。从而$s\leqslant l$，即l是A的最大下界，$\therefore\ l=\bigcap\limits_{a\in A}a$，$\therefore S$是完全格。

10. 设格$(S,\leqslant)$中不存在单位元，证明，S中存在递增的无穷序列：$x_0<x_1<x_2<\cdots<x_n<\cdots$。

证 任取$x_0\in S$，$\because\ x_0\neq 1$，故不能对子所有$y\in S$，均有$x_0\cup y=x_0$，于是存在$y_0\in S$，$x_0\cup y_0\neq x_0$，从而$x_0\cup y_0>x_0$。命$x_1=x_0\cup y_0$，则$x_0<x_1$。假定在S中存在x_2，……，x_n，使$x_0<x_1<x_2<\cdots<x_n$。$\because x_n\neq 1$，对x_n进行如对x_1同样的讨论可得：有$x_{n+1}\in S$，使$x<x_{n+1}$，即S中存在递增的无穷序列。

11. 证明，Q关于数目大小“$\leqslant$”作成一个格，$(Q,\leqslant)$是否有单位元？是否有零元？

证 $\because$ Q关于$\leqslant$成有序集，$\therefore$显然是一个格，Q没有零元和单位元。$\because$ 如a是Q的零元，则有$x\cup a=x$，$\forall x\in Q$。而$\because\ a\in Q$是有理数，$\therefore$ 必有$x<a$且$x\in Q$，此时$x\cup a=a\neq x$，$\therefore$Q没有零元。类似的讨论可证Q没有单位元。

12．将$-\infty$添加到格（$\mathbf{Q}$，$\leqslant$）中，并将例6的证明步骤用于（$\mathbf{Q}$，$\leqslant$），说明这个过程恰好是由有理数建立实数的*Dedekind*分划的步骤．

证 记$\mathbf{Q}'=\mathbf{Q}\cup\{-\infty\}$，其中$-\infty$是一个记号．规定$-\infty<a$，$\forall a\in\mathbf{Q}$．则易知$(\mathbf{Q}',\leqslant)$成为格，且有零元$-\infty$．

由原书*P*．252例5知：$\mathbf{Q}'$中一切具有以下性质的子集A全体所成集合$\overline{\mathbf{Q}'}$关于集合的包含关系作成一个完全格$(\overline{\mathbf{Q}'},\subseteq)$：

①$A\neq\phi$．　②$a\in A,x\leqslant a\Rightarrow x\in A$．　③$A$的任意非空子集$N$，当$N$的最小上界在$\mathbf{Q}'$中存在时，一定属于$A$．

当$A\in\overline{\mathbf{Q}'}$且$A\neq\{-\infty\}$时，命$A'$是$A$在$\mathbf{Q}'$中的余集，即$A'=\mathbf{Q}'-A=\{x\mid x\in\mathbf{Q}',x\notin A\}$，则有$\mathbf{Q}'=A\cup A'$，且因$a\in A'\Rightarrow a\notin A\Rightarrow a\not\leqslant b,\forall b\in A$，又有$a>b,\forall a\in A',b\in A$．故$A\mid A'$成为有理数的一个*Dedekind*分划（按理应在A中去掉$-\infty$，为避免符号复杂，仍记A）．是即$\overline{\mathbf{Q}'}$中每一个$A\neq\{-\infty\}$确定一个*Dedekind*分划$A\mid A'$（约定当A'中有最小数时，此数归到A中）．反之，每给一个*Dedekind*分划（约定同上），则其下部添加$-\infty$后所成之集A必$\in\overline{\mathbf{Q}'}$，且$A\neq\{-\infty\}$，并且上部恰是$A$在$\mathbf{Q}'$中的余集．又易知，当$A$，$B\in\overline{\mathbf{Q}'}$，$A\neq\{-\infty\}$，$B\neq\{-\infty\}$，且$A\neq B$时，$A$，$B$按上法确定的*Dedekind*分划$A\mid A'$及$B\mid B'$不同．由于全体*Dedekind*分划所成之集即全体实数之集，故视$A=A\mid A'$时，$\overline{\mathbf{Q}'}$即是全体实数之集（按理应在$\overline{\mathbf{Q}'}$中去掉$\{-\infty\}$，为简单起见，仍记$\overline{\mathbf{Q}'}$，）

由原书*P*.253例6知：φ：$\mathbf{Q}'\to\overline{\mathbf{Q}'}$

$$a\longmapsto(a)=\{x\mid x\in\mathbf{Q}'x\leqslant a\}$$

将格$(\mathbf{Q}',\leqslant)$同构嵌入于完全格$(\overline{\mathbf{Q}'},\subseteq)$，是即，当视$(a)=a$时，有理数集$\subseteq$实数集．当$A\in\overline{\mathbf{Q}'}$，$A\neq\{-\infty\}$，且$A$在$\mathbf{Q}'$中

有最小上界a时，由规定A时所给条件中的第三个条件知$a\in A$，从而a是A中最大数，故由A确定的$Dedekind$分划$A|A'$的下部A中有最大数a。反之，若$A\in\overline{\mathbf{Q}'}$，$A\neq\{-\infty\}$，且$A$确定的$Dedekind$分划$A|A'$的下部$A$中有最大数$a$，则易知$a$就是$A$在$\mathbf{Q}'$中的最小上界。用$Dedekind$分划建立实数时，若分划$A|A'$的下部$A$有最大数$a$，则$A|A'$确定的实数应该就是$a$。因为当下部$A$有最大数$a$时，有$A=(a)$。而此处将有理数嵌入实数集时是视$(a)=a$的，故两者一致，由例6知：

$a\leqslant b\Longleftrightarrow\varphi(a)\leqslant\varphi(b)$，故 $a\leqslant b\Longleftrightarrow(a)\subseteq(b)$。

因此，有理数在实数集$\overline{\mathbf{Q}'}$中的大小顺序和有理数在$\mathbf{Q}'$中的大小顺序一致。设$\alpha=A|A'=A$，$\beta=B|B'=B$，故在$\overline{Q}'$中有

$\alpha=\beta\Longleftrightarrow A=B$。 $\alpha>\beta\Longleftrightarrow A\supset B$。

这和用$Dedekind$分划建立实数的大小顺序是一致的。综上所述，例6的过程用于$(\mathbf{Q},\leqslant)$恰好是由有理数建立实数的$Dedekind$分划的步骤。

13. 设S是模格，证明，S中不含与五边形格同构的子格。

证 参见§2练习第2题解。

14. 设$(S,\cup,\cap,',0,I)$是一个布尔代数，x，$y\in S$，证明$x\leqslant y\Longleftrightarrow x'\geqslant y'$，

并且$x\leqslant y\Longleftrightarrow x\cap y'=O\Longleftrightarrow x'\cup y=I$

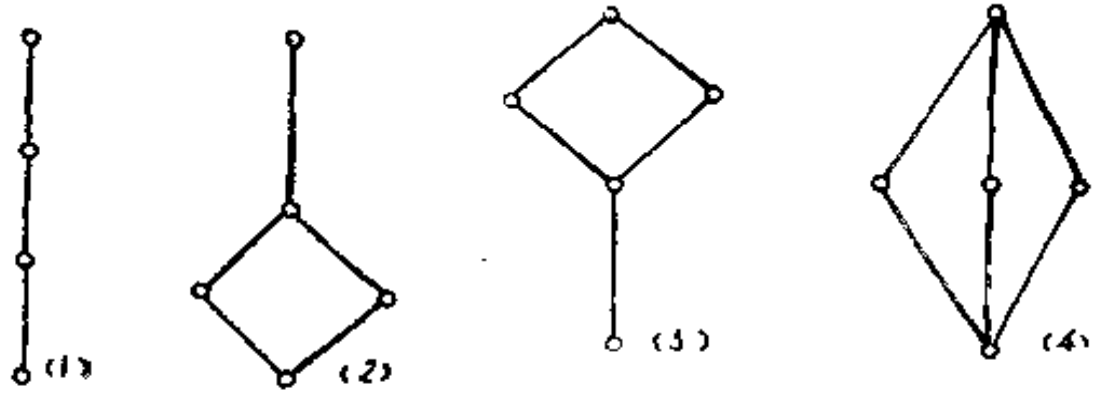
证 由$x\leqslant y$，可知$x\cup y=y$，$\therefore y'=(x\cup y)'=x'\cap y'$，$\therefore x'\geqslant y'$。反之$x'\geqslant y'$则由前面结论$(x')'\leqslant(y')'$即$x\leqslant y$。又由$x\leqslant y$可知$x\cap y=x$。$\therefore x\cap y'=(x\cap y)\cap y'=x\cap o=O$。反之如$x\cap y'=0$，则$y=y\cup o=y\cup(x\cap y')=(y\cup x)\cap(y\cup y')=y\cup x$，$\therefore x\leqslant y$。而$x\cap y'=0\Longleftrightarrow(x\cap y)'=0'$，即$x'\cup y=I$。

15. 设G，G'是两个群，φ是G到G'的满射，$ker\varphi=K$。

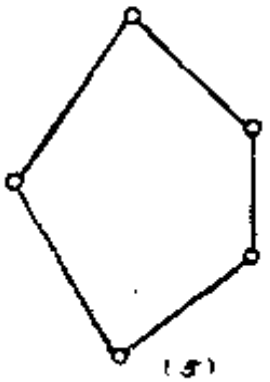
证明，$S=\{H \mid H \leqslant G, H \supseteq K\}$ 是$L(G)$ 的子格，并且S 与 $L(G')$同构。〔註：原题如此，这里 φ 应为满同态〕

证 显见$S \subseteq L(G)$。任取$H_1, H_2 \in S$，则$H_i \supseteq K$，$i=1,2$。$\therefore H_1 \cap H_2 \supseteq K$，$H_1 \cup H_2 \supseteq K$。从而$H_1 \cap H_2$，$H_1 \cup H_2 \in S$。$\therefore$ S是$L(G)$ 的子格，作对应$H \longmapsto \varphi(H)$，由原书$P.100$ 定理 6 可知它是S到$L(G')$的双射，且保持偏序关系“$\subseteq$”，即$H_1 \subseteq H_2 \Rightarrow \varphi(H_1) \subseteq \varphi) H_2)$，此时易推知：$\varphi(H_1 \cap H_2)=\varphi(H_1) \cap \varphi H_2)$，$\varphi(H_1 \cup H_2)=\varphi(H_1) \cup \varphi(H_2)$。$\therefore S \overset{\varphi}{\cong} L(G')$。

16。证明，五个元的格只有以下五种：



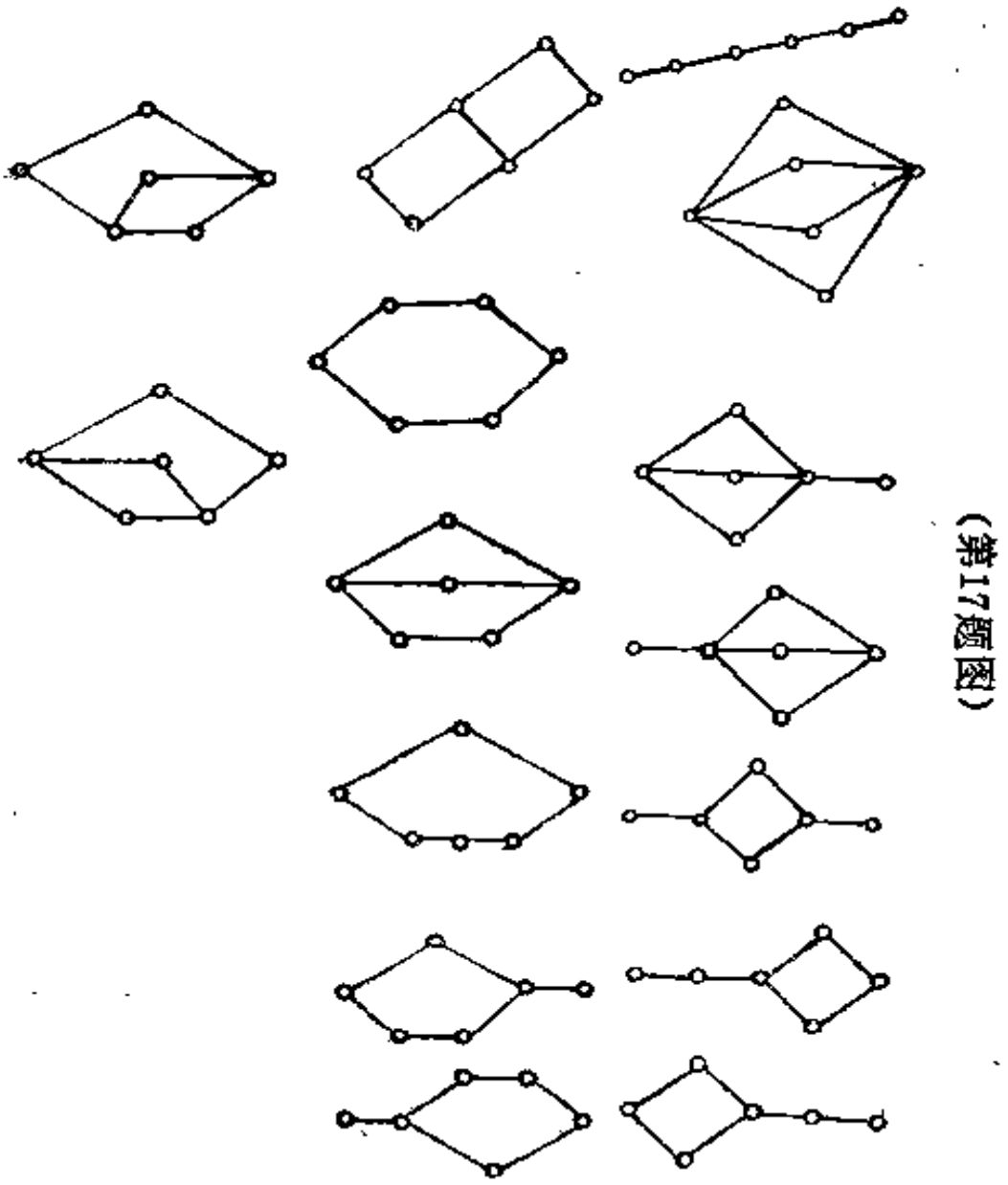
证 设S是个五元格，显然$0,1 \in S$。设其他三个元为a,b,c，则有以下几种情况：①如a,b,c有序，则得图(1)。②如a,b,c中无两个元有关系“$<$”，则得图(4)。③如a,b,c中只有两个元有关系“$<$”则得图(5)。④如$a>b, a>c$，b,c不可比，则成图(2)。⑤如$a<b, a<c$。



b,c不可比则成图（3）.所以五元格只有这五种.

17. 找出所有六个元的格.

解 设S是六元格.除有序集的情况外它至少含有一个四边形的子格，（即$\{a,b,a\cup b,a\cap b\}$），如此四边形子格的边上还有其他元，则S就有五边形子格，这样的S是非模格，共有7种，反之S是模格，有8种.故六元格S有以下15种，（前面8种是模格，后面7种是非模格.）



（第17题图）

第五章　群的进一步讨论

§1　Sylow 子 群

1. 写出三种 12 阶的不交换群的乘法表，找出其共轭的 *Sylow* 子群。

解　根据例 3 给出的关系，可直接写出群 G 的乘法表。

(1) $H_1=\{e, a, a^2, a^3\}$ 是 G 的一个子群，$C_3=\{e, c, c^2\}$ 是 G 的一个正规子群。并由关系 $ac=c^2a$，得出乘法表如下：（见表一）

由乘法表可知与 H_1 共轭的另外两个Sylow 子群是 $H_2=c^2H_1c=\{e, ca, a^2, ca^3\}$ 及 $H_3=cH_1c^2=\{e, c^2a, a^2, c^2a^3\}$。

(2) $H_1=\{e, a, b, ab\}$ 是 G 的一个子群，$C_3=\{e, c, c^2\}$ 是 G 的一个正规子群，并有关系 $ac=ca, bc=c^2b$。首先，我们减少生成元素的个数。命 $x=ac$，因 a 的周期为 2，c 的周期为 3，而 $ac=ca$，故 x 的周期为 6。因为 $a=a^2c^3=x^3$，$c=a^4c^4=x^4$，所以 G 由 x 和 b 生成。因为 $xbx=(ac)b(ac)=ac(ba)c=ac(ab)c=a(ac)bc=a^2cbc=c(bc)=c(c^2b)=b$，所以存在关系 $bx=x^5b$。反过来，用 $x^6=e$，$b^2=e$，$bx=x^5b$，命 $x^3=a, x^4=c$，可以推出原来的全部关系，即 $a^2=e, b^2=e$，$c^3=e$，$ab=ba$，$ac=ca$，$bc=c^2b$。因此，这两组关系等价。我们可以得到乘法表如下：（见表二）

此时，$H_1=\{e, x^3, b, x^3b\}$，$C_3=\{e, x^4, x^2\}$。则与 H_1 共轭的另外两个 *Sylow* 子群是 $H_2=x^2H_1x^4=\{e, x^3, x^4b, xb\}$，$H_3=x^4H_1x^2=\{e, x^3, x^2b, x^5b\}$。

(3) $B_4=\{e, a, b, ab\}$ 是 G 的一个正规子群，$C_3=\{e,$

$c, c^2\}$ 是 G 的一个子群，并有关系 $ca = bc$, $cb = (ab)c$, $c(ab) = ac$。（见表三）

（表一）

	e	c	c^2	a	ca	c^2a	a^2	ca^2	c^2a^2	a^3	ca^3	c^2a^3
e	e	c	c^2	a	ca	c^2a	a^2	ca^2	c^2a^2	a^3	ca^3	c^2a^3
c	c	c^2	e	ca	c^2a	a	ca^2	c^2a^2	a^2	ca^3	c^2a^3	a^3
c^2	c^2	e	c	c^2a	a	ca	c^2a^2	a^2	ca^2	c^2a^3	a^3	ca^3
a	a	c^2a	ca	a^2	c^2a^2	ca^2	a^3	c^2a^3	ca^3	e	c^2	c
ca	ca	a	c^2a	ca^2	a^2	c^2a^2	ca^3	a^3	c^2a^3	c	e	c^2
c^2a	c^2a	ca	a	c^2a^2	ca^3	a^2	c^2a^3	ca^3	a^3	c^2	c	e
a^2	a^2	ca^2	c^2a^2	a^3	ca^3	c^2a^3	e	c	c^2	a	ca	c^2a
ca^2	ca^2	c^2a^2	a^2	ca^3	c^2a^3	a^3	c	c^2	e	ca	c^2a	a
c^2a^2	c^2a^2	a^2	ca^2	c^2a^3	a^3	ca^3	c^2	e	c	c^2a	a	ca
a^3	a^3	c^2a^3	ca^3	e	c^2	c	a	c^2a	ca	a^2	c^2a^2	ca^2
ca^3	ca^3	a^3	c^2a^3	c	e	c^2	ca	a	c^2a	ca^2	a^2	c^2a^2
c^2a^3	c^2a^3	ca^3	a^3	c^2	c	e	c^2a	ca	a	c^2a^2	ca^2	a^2

（表二）

	e	x	x^2	x^3	x^4	x^5	b	xb	x^2b	x^3b	x^4b	x^5b
e	e	x	x^2	x^3	x^4	x^5	b	xb	x^2b	x^3b	x^4b	x^5b
x	x	x^2	x^3	x^4	x^5	e	xb	x^2b	x^3b	x^4b	x^5b	b
x^2	x^2	x^3	x^4	x^5	e	x	x^2b	x^3b	x^4b	x^5b	b	xb
x^3	x^3	x^4	x^5	e	x	x^2	x^3b	x^4b	x^5b	b	xb	x^2b
x^4	x^4	x^5	e	x	x^2	x^3	x^4b	x^5b	b	xb	x^2b	x^3b
x^5	x^5	e	x	x^2	x^3	x^4	x^5b	b	xb	x^2b	x^3b	x^4b
b	b	x^5b	x^4b	x^3b	x^2b	xb	e	x^5	x^4	x^3	x^2	x
xb	xb	b	x^5b	x^4b	x^3b	x^2b	x	e	x^5	x^4	x^3	x^2
x^2b	x^2b	xb	b	x^5b	x^4b	x^3b	x^2	x	e	x^5	x^4	x^3
x^3b	x^3b	x^2b	xb	b	x^5b	x^4b	x^3	x^2	x	e	x^5	x^4
x^4b	x^4b	x^3b	x^2b	xb	b	x^5b	x^4	x^3	x^2	x	e	x^5
x^5b	x^5b	x^4b	x^3b	x^2b	xb	b	x^5	x^4	x^3	x^2	x	e

(表三)

	e	c	c^2	a	ac	ac^2	b	bc	bc^2	ab	abc	abc^2
e	e	c	c^2	a	ac	ac^2	b	bc	bc^2	ab	abc	abc^2
c	c	c^2	e	bc	bc^2	b	abc	abc^2	ab	ac	ac^2	a
c^2	c^2	e	c	abc^2	ab	abc	ac^2	a	ac	bc^2	b	bc
a	a	ac	ac^2	e	c	c^2	ab	abc	abc^2	b	bc	bc^2
ac	ac	ac^2	a	abc	abc^2	ab	bc	bc^2	b	c	c^2	e
ac^2	ac^2	a	ac	bc^2	b	bc	c^2	e	c	abc^2	ab	abc
b	b	bc	bc^2	ab	abc	abc^2	e	e	c^2	a	ac	ac^2
bc	bc	bc^2	b	c	c^2	e	ac	ac^2	a	abc	abc^2	ab
bc^2	bc^2	b	bc	ac^2	a	ac	abc^2	ab	abc	c^2	e	c
ab	ab	abc	abc^2	b	bc	bc^2	a	ac	ac^2	e	c	c^2
abc	abc	abc^2	ab	ac	ac^2	a	c	c^2	e	bc	bc^2	b
abc^2	abc^2	ab	abc	c^2	e	c	bc^2	b	bc	ac^2	a	ac

与C_3共轭的另外3个Sylow子群是$aC_3a=\{e,abc,bc^2\}$，$bC_3b=\{e,ac,abc^2\}$，$(ab)C_3(ab)=\{e,bc,ac^2\}$。

2. 写出10阶的非交换群的乘法表，找出其共轭的Sylow子群。

解 因为$|G|=10$，所以G的2－Sylow子群是2阶循环群C_2，G的5－Sylow子群是5阶循环群C_5。5－Sylow子群的个数$k_5=5l+1$，$k_5|10$，所以$k_5=1$，C_5是G的正规子群。2－Sylow子群的个数$k_2=2l+1$，$k_2|10$，所以，$k_2=1,5$。如果$k_2=1$，则$G=C_2\times C_5=C_{10}$，是10阶循环群，所以$k_2=5$。

设$H_1=\{e,a\}$是G的一个子群，$C_5=\{e,c,c^2,c^3,c^4\}$是G的正规子群。设$a^{-1}ca=c^i$，则$c=a^{-2}ca^2=a^{-1}c^ia=c^{i^2}$。因此$i^2\equiv 1(mod\ 5)$，$i=1,4$。如果$i=1$，则$ac=ca$，$G$是可换群，因此$i=4$，有关系$ac=c^4a$，$G$是10阶二面体群。乘法表如下：

	e	c	c^2	c^3	c^4	a	ca	c^2a	c^3a	c^4a
e	e	c	c^2	c^3	c^4	a	ca	c^2a	c^3a	c^4a
c	c	c^2	c^3	c^4	e	ca	c^2a	c^3a	c^4a	a
c^2	c^2	c^3	c^4	e	c	c^2a	c^3a	c^4a	a	ca
c^3	c^3	c^4	e	c	c^2	c^3a	c^4a	a	ca	c^2a
c^4	c^4	e	c	c^2	c^3	c^4a	a	ca	c^2a	c^3a
a	a	c^4a	c^3a	c^2a	ca	e	c^4	c^3	c^2	c
ca	ca	a	c^4a	c^3a	c^2a	c	e	c^4	c^3	c^2
c^2a	c^2a	ca	a	c^4a	c^3a	c^2	c	e	c^4	c^3
c^3a	c^3a	c^2a	ca	a	c^4a	c^3	c^2	c	e	c^4
c^4a	c^4a	c^3a	c^2a	ca	a	c^4	c^3	c^2	c	e

与 H_1 共轭的Sylow子群为 $H_2=c^4H_1c=\{e, c^3a\}$，$H_3=c^3H_1c^2=\{e, ca\}$，$H_4=c^2H_1c^3=\{e, c^4a\}$，$H_5=cH_1c^4=\{e, c^2a\}$。(根据乘法表对角线上的 e，可得到 G 的5个周期为2的元素，从而即可得到全部2-Sylow子群。)

3. 设 A 是有限群 G 的子集，证明，G 中与 A 共轭的子集的个数等于 $[G:N(A)]$。

证 由 P. 261 引理3可知，G 中与 A 共轭的子集的个数等于 $[G, G\cap N(A)]$，是即 $[G:N(A)]$。

4. 设 P 是 G 的 p-Sylow 子群，H 是 G 的正规子群，且 $[G:H]$ 与 p 互素，证明 $P\subseteq H$。

证 设 $|G|=p^rm$，$p\nmid m$。因为 $p\nmid[G:H]$，所以 $p^r\mid|H|$，H 的 p-Sylow 子群 P' 是 p^r 阶子群，因而是 G 的 p-Sylow子群，P' 与 P 在 G 中共轭，$xP'x^{-1}=P$。但由于 H 是 G 的正规子群，$xP'x^{-1}\subseteq xHx^{-1}=H$，所以 $P\subseteq H$。

5. 证明35阶的群一定是循环群。

证 设 $|G|=35$，因 $35=5\cdot7$，故 G 的 5-Sylow 子群为5阶循环群 C_5，G 的 7-Sylow 子群为 C_7。5-Syloy 子群的个数 $k_5=5l+1$，$k_5\mid35$，故 $k_5=1$。7-Sylow 子群的个数 $k_7=7l+1$，$k_7\mid35$，故 $k_7=1$。C_5 和 C_7 都是 G 的正规子群，故 $G=C_5\times C_7=C_{35}$ 是循环群。

6. 设有限群 G 的阶数为 np，p 是素数，$n<p$。证明，G 含有阶数 p 的不变子群。

证 因为 $p^2\nmid np$，故 G 的 p-Sylow 子群是 p 阶循环群 C_p。p-Sylow 子群的个数 $k_p=pl+1$，$k_p\mid nP$，即 $(pl+1)\mid nP$。但由于 $(pl+1, p)=1$，所以 $(pl+1)\mid n$，由于 $n<p$，故 $l=0$，$k_p=1$，因而 C_p 是 G 的正规子群。

§2 有限交换群

1. 利用数学归纳法证明定理2（两个有限交换群同构的充分必要条件是有相同的初等因子组）。

证 充分性：设A，B是两个有限交换群，具有相同的初等因子组$\{p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots, p_s^{\alpha_s}\}$，则$A=(a_1)\times(a_2)\times\cdots\times(a_s)$，$B=(b_1)\times(b_2)\times\cdots\times(b_s)$，位里$a_m$和$b_m$的周期都是$p_m^{\alpha_m}$，$m=1, \cdots, s$。

命φ：$a_1^{i_1}a_2^{i_2}\cdots a_s^{i_s}\longmapsto b_1^{i_1}b_2^{i_2}\cdots b_s^{i_s}$，$0\leqslant i_m<p_m^{\alpha_m}$，$m=1, \cdots, s$。显然$\varphi$是$A$到$B$的一个双射。

任取$x_1=a_1^{i_1}a_2^{i_2}\cdots a_s^{i_s}$，$x_2=a_1^{j_1}a_2^{j_2}\cdots a_s^{j_s}$，设$x_1x_2=a_1^{k_1}a_2^{k_2}\cdots a_s^{k_s}$，位里$0\leqslant i_m, j_m, k_m<p_m^{\alpha_m}$，$m=1, 2, \cdots, s$，显然$i_m+j_m\equiv k_m(mod\ p_m^{\alpha_m})$，$m=1, 2, \cdots, s$。

显然$\varphi(x_1)=b_1^{i_1}b_2^{i_2}\cdots b_s^{i_s}$，$\varphi(x_2)=b_1^{j_1}b_2^{j_2}\cdots b_s^{j_s}$，$\varphi(x_1x_2)=b_1^{k_1}b_2^{k_2}\cdots b_s^{k_s}$。因为$b_m$的周期是$p_m^{\alpha_m}$，而$i_m+j_m\equiv k_m(mod\ p_m^{\alpha_m})$，所以$\varphi(x_1)\varphi(x_2)=\varphi(x_1x_2)$，$A$和$B$同构。

必要性：设有限交换群A和B同构，A具有初等因子组$\{p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots, p_s^{\alpha_s}\}$，今对初等因子的个数用归纳法加以证明。

当$s=1$时，A是$p_1^{\alpha_1}$阶循环群，由于同构关系，B也是$p_1^{\alpha_1}$阶循环群，因而B和A具有相同的初等因子组$\{p_1^{\alpha_1}\}$。

假定对于初等因子的个数$<s$的有限交换群，必要性成立，今设$A=(a_1)\times(a_2)\times\cdots\times(a_s)$，令$A_1=\{a_1\}$，$A_2=\{a_2\}\times\{a_3\}\times\cdots\times\{a_s\}$，则$A=A_1\times A_2$。设$B_1$，$B_2$分别为

A_1 和 A_2 在 B 中的同构象，显然，$A=A_1\times A_2$ 在 B 中的同构象是 $B_1\times B_2$。因此，$B=B_1\times B_2$，由于 A_1 和 A_2 的初等因子的个数小于 s，根据归纳假设可知，B_1 和 A_1 有相同的初等因子组，B_2 和 A_2 有相同的初等因子组。故 $B_1=(b_1)$，$B_2=(b_2)\times(b_3)\times\cdots\times(b_s)$，并且 b_m 的周期和 a_m 相等，等于 $p_m^{\alpha_m}$，$m=1,2,\cdots,s$。

因而 $B=B_1\times B_2=(b_1)\times(b_2)\times\cdots\times(b_s)$。这意味着 B 和 A 有相同的初等因子组$\{p_1^{\alpha_1},p_2^{\alpha_2},\cdots,p_s^{\alpha_s}\}$。定理得到证明。

2。设 $G=(a)\times(b)$，$|a|=8$，$|b|=4$，命 $c=ab$，$d=a^4b$，证明 $G=(c)\times(d)$

证 用 $[m,n]$ 表示非负整数 m 和 n 的最小公倍数。因为 a，b 分属于 G 的两个不同的直积因子，所以 $|c|=[|a|,|b|]=[8,4]=8$，$|d|=[|a^4|,|b|]=[2,4]=4$，故 (c) 是 8 阶循环群，(d) 是 4 循环群。任取 $x\in(c)\cap(d)$，则 $x=(ab)^i=(a^4b)^j$，即 $x=a^ib^i=a^{4j}b^j$。由于 $G=(a)\times(b)$，故 $i=4j(mod\ 8)$，$i\equiv j(mod\ 4)$。由此可知 $j\equiv0(mod\ 4)$，因而 $x=a^{4j}b^j=e$，即 $(c)\cap(d)=\{e\}$，$(c)\times(d)$ 是 G 的 32 阶子群，由于 $G=(a)\times(b)$ 是 32 阶群，所以 $G=(c)\times(d)$。

3。写出 45 阶交换群的一切可能类型。

解 因为 $45=5\times3^2$，初等因子组有两种 $\{5,3,3\}$，$\{5,3^2\}$，因而 45 阶交换群仅有两种类型：$C_5\times C_3\times C_3$，$C_5\times C_9$。

4。写出 108 阶交换群的一切可能类型。

解 108阶交换群的初等因子组有：$\{2,2,3,3,3\}$，$\{2,2,3,3^2\}$，$\{2,2,3^3\}$，$\{2^2,3,3,3\}$，$\{2^2,3,3^2\}$，$\{2^2,3^3\}$。故108阶交换群有 6 种：$C_2\times C_2\times C_3\times C_3\times C_3$，

$C_2\times C_2\times C_3\times C_9, C_2\times C_2\times C_{27}, C_4\times C_3\times C_3\times C_3, C_4\times C_3\times C_9, C_4\times C_{27}$。

5. 设 G 是 2^n 阶交换群，G 中指数为 2 的子群仅存在一个，证明，G 是循环群。

证 由 p.259 定理 2 知 G 是 2 群。故由 p·274 例 6 知 G 是循环群 $(p=2)$。

6. 设交换群 G 的初等因子组为 $\{p^3, p^2\}$，求 G 中阶数为 p^2 的子群的个数。

解 G 的 p^2 阶子群的初等因子组可能是 $\{p,p\}$ 和 $\{p^2\}$。

令 $G_p=\{x|x\in G, x^p=e\}$, $G_{p^2}=\{x|x\in G, x^{p^2}=e\}$ 容易验证，G_p 和 G_{p^2} 都是 G 的子群，并且 G_p 包含 G 的初等因子组为 $\{p,p\}$ 的一切子群，G_{p^2} 包含 G 的一切 p^2 阶子群。易知 $|G_p|=p^2$，故 G_p 的初等因子组是 $\{p,p\}$，因而 G_p 是 G 的初等因子组为 $\{p,p\}$ 的唯一的子群。

现在考虑 G 的 p^2 阶循环子群的个数。因为 p^2 阶循环群 (c) 中，元素 $c^i(0\leqslant i\leqslant p-1)$ 是 p^2 阶元素，当且仅当 $p\nmid i$，故 G 中 p^2 阶元素的个数等于 $|G_{p^2}|-|G_p|=p^4-p^2$，而每个 p^2 阶元素属于且仅属于一个 p^2 阶循环群，每个 p^2 阶循环群含有 p^2-p 个 p^2 阶元素，因此 G 的 p^2 阶循环子群的个数等于 $(p^4-p^2)/(p^2-p)=p^2+p$，故 G 的 p^2 阶子群的个数为 p^2+p+1。

7. 写出 144 阶交换群的一切可能的类型。

解 初等因子组有：$\{3,3,2,2,2,2\}$, $\{3,3,2^2,2,2\}$, $\{3,3,2^2,2^2\}$, $\{3,3,2^3,2\}$, $\{3,3,2^4\}$, $\{3^2,2,2,2,2\}$, $\{3^2,2^2,2,2\}$, $\{3^2,2^2,2^2\}$, $\{3^2,2^3,2\}$, $\{3^2,2^4\}$。

对应的不变因子组为 $\{2,2,6,6\}$，$\{2,6,12\}$，$\{12,12\}$，$\{6,24\}$，$\{3,48\}\}$，$\{2,2,2,18\}$，$\{2,2,36\}$，$\{4,36\}$，$\{2,72\}$，$\{144\}$。

144阶交换群有十种：$C_2\times C_2\times C_6\times C_6$，$C_2\times C_6\times C_{12}$，$C_{12}\times C_{12}$，$C_6\times C_{24}$，$C_3\times C_{48}$，$C_2\times C_2\times C_2\times C_{18}$，$C_2\times C_2\times C_{36}$，$C_4\times C_{36}$，$C_2\times C_{72}$，$C_{144}$。

8. 证明，对任意素数 $p_1, p_2, \cdots, p_r$，任意自然数 $\alpha_1, \alpha_2, \cdots, \alpha_r$，存在交换群 G，其初等因子组为

$$\{p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots, p_r^{\alpha_r}\}$$

证 $G=C_{p_1^{\alpha_1}}\times C_{p_2^{\alpha_2}}\times\cdots\times C_{p_r^{\alpha_r}}$ 就是所要求的交换群。

§3 具有有限生成元的交换群

1. 利用数学归纳法，写出定理 2 的末一部分证明。

证 设 A，B 是两个同构的交换群：

$$A=(a_1)\times(a_2)\times\cdots\times(a_h)\times(u_1)\times\cdots\times(u_t),\quad n\geqslant 1$$

$$B=(b_1)\times(b_2)\times\cdots\times(b_k)\times(v_1)\times\cdots\times(v_m),\quad m\geqslant 0$$

此处 $|(a_i)|$ 为有限，$i=1,2,\cdots,h$；且 $|(a_{i-1})|\,\big|\,|(a_i)|$，$i=2,3,\cdots,h$；$(u_i)$ 是无限循环群，$i=1,2,\cdots,u$；$|(b_j)|$ 有限，$j=1,2,\cdots,k$；且 $|(b_{j-1})|\,\big|\,|(b_j)|$，$j=2,3,\cdots,k$；$(v_j)$ 是无限循环群，$j=1,2,\cdots,m$。今对 n 用归纳法证明 $h=k$，$m=n$，且 $(a_i)\cong(b_i)$，$i=1,2,\cdots,h$。

由于 $n\geqslant 1$，故首先可知必 $m\geqslant 1$，当 $n=1$ 时，由 p.273 引理 2 知：

$(a_1)\times\cdots\times(a_h)\cong(b_1)\times\cdots\times(b_k)\times(v_1)\times\cdots\times(v_{m-1})$，

故 $m-1=0$，且

$(a_1)\times\cdots\times(a_h)\cong(b_1)\times\cdots\times(b_k)$

由§2中的定理4知 $h=k$，且 $(a_i)\cong(b_i)$，$i=1,2,\cdots,h$，故当 $n=1$ 时命题成立。

假定命题对 $n-1$ 成立，则由

$(a_1)\times\cdots\times(a_h)\times(u_1)\times\cdots\times(u_{n-1})\cong(b_1\times\cdots\times(b_k)\times(v_1)\times\cdots\times(v_{m-1})$

可知 $h=k$，$n-1=m-1$，且 $(a_i)\cong(b_i)$，$i=1,2,\cdots,h$。故命题对 n 也成立。

命 $A=B=G$，就得到定理2的末一部分的证明。

2。利用数学归纳法证明定理3（两个有限生成元的自由交换群同构的充要条件是生成元的个数相同）。

证 设 A，B 是两个有限生成的自由交换群，生成元的个数分别为 n 和 m，则

$$A=(a_1)\times(a_2)\times\cdots\times(a_n)$$

$$B=(b_1)\times(b_2)\times\cdots\times(b_m)$$

若 $m=n$，命 $\varphi:\ a_1^{i_1}a_2^{i_2}\cdots a_n^{i_n}\longmapsto b_1^{i_1}b_2^{i_2}\cdots b_n^{i_n}$，容易验证 $A\cong B$。

必要性。当 $n=1$ 时，$A=\{e\}\times(a_1)$，由引理2可知 $\{e\}\cong(b_1)\times(b_2)\times\cdots\times(b_{m-1})$，因而 $B=(b_m)$，$m=1$。

当 $n>1$ 时，由引理2可知，$(a_1)\times(a_2)\times\cdots\times(a_{n-1})\cong(b_1)\times(b_2)\times\cdots\times(b_{m-1})$，但此时根据归纳假定可知 $m-1=n-1$，因而 $m=n$，定理得到证明。

3。设 G 是无限循环群，找出 G 的所有基。

解 根据书中关于基的定义，命题应仅限于不含单位元

e 的基。设 $G=(a)$，显然 $\{a\}$ 是 G 的一个基。今设 S 是 G 的任一个基，我们证明 S 是一个元素的集合。否则，任取 S 的两个不同的元素 s_1，s_2，则存在整数 m_1，m_2，使得 $s_1=a^{m_1}$，$s_2=a^{m_2}$。显然 $S_1{}^{m_2}S_2{}^{m_1}=(a^{m_1})^{m_2}(a^{m_2})^{-m_1}=e$。因为 $s_1\in S$，$s_2\in S$，故 $s_1\neq e$，$s_2\neq e$，$m_1\neq 0$，$m_2\neq 0$，又因为 a 的周期无限，所以 $s_1^{m_2}=(a^{m_1})=a^{m_1m_2}\neq e$，这与基的定义相矛盾，故 S 中仅含有一个元，从而是 G 的生成元。因此 $\{a\}$ 及 $\{a^{-1}\}$ 就是 G 的所有的基。

4. 设 $a_1, a_2, \cdots, a$ 是自由交换群 F_n 的一个基，证明对任意整数 k，$a_1a_2^k, a_2, \cdots, a_n$ 仍是 F_n 的一个基。

证 因为 $a_1^{i_1}a_2^{i_2}a_3^{i_3}\cdots a_n^{i_n}=(a_1a_2^k)^{i_1}a_2^{i_2-i_1k}a_3^{i_3}\cdots a_n^{i_n}$，所以 $a_1a_2^k, a_2, \cdots, a_n$ 是 F_n 的一个生成元系。

设 $(a_1a_2^k)^{i_1}a_2^{i_2}a_3^{i_3}\cdots a_n^{i_n}=e$，即 $a_1^{i_1}a_2^{i_2+i_1k}a_3^{i_3}\cdots a_n^{i_n}=e$，由于 $a_1, a_2, \cdots, a_n$ 是 F_n 的一个基，故 $i_1=i_2+i_1k=i_3=\cdots=i_n=0$，即 $i_1=i_2=i_3=\cdots=i_n=0$，因而 $a_1a_2^k, a_2, \cdots, a_n$ 仍是 F_n 的一个基。

5. 证明，F_n 的任一基都含有 n 个元素。

证 按原书对于基的定义，此处应限于不含单位元 e 的基，故下面只考虑不含单位元 e 的基。

首先可以证明 F_n 没有无限基。因若 $F_n=(a_1)\times\cdots\times(a_n)$ 有一基 S 含无限个元，则可取 $n+1$ 个元。

$b_1, b_2, \cdots, b_{n+1}\in S$。

设 $b_i=a_1^{\alpha_{1i}}a_2^{\alpha_{2i}}\cdots a_n^{\alpha_{ni}}$，$i=1, 2, \cdots, n+1$，其中 α_{1i}，$\alpha_{2i}, \cdots, \alpha_{ni}$ $(i=1, 2, \cdots, n+1)$ 都是整数。

易知整系数齐次线性方程组

$$\sum_{j=1}^{n+1}\alpha_{ij}x_j=0,\quad i=1, 2, \cdots, n \qquad (甲)$$

有非零有理数解。从而有非零整数解。设 $(x_1, x_2, \cdots, x_{n+1})$ 是（甲）的一个非零整数解，则有

$$b_1^{x_1} b_2^{x_2} \cdots b_{n+1}^{x_{n+1}} = e .$$

从而应有 $b_i^{x_i} = e$, $i = 1, 2, \cdots, n+1$，于是有

$$a_1^{\alpha_{1i} x_i} a_2^{\alpha_{2i} x_i} \cdots a_n^{\alpha_{ni} x_i} = e .$$

从而应有 $a_k^{\alpha_{ki} x_i} = e$, $k = 1, 2, \cdots, n$，于是有

$$\alpha_{ki} x = 0 , \quad k = 1, 2, \cdots, n .$$

但 $b_i \neq e$，故 α_1, α_2, $\cdots$, α_{n+1} 不全为 0，故

$$x = 0 , \quad i = 1, 2, \cdots, n+1 .$$

这与“$(x_1, x_2, \cdots, x_{n+1})$ 是（甲）的一个非零整数解”矛盾。故 F_n 没有无限基。

用完全同样的方法可以证明，若 $\{b_1, b_2, \cdots, b_s\}$ 及 $\{c_1, c_2, \cdots, c_t\}$ 是 F_n 的任意两个基，则必 $t \leqslant s$，从而又有 $s \leqslant t$，故必 $s = t$。

令 F_n 已有一基 $\{a_1, a_2, \cdots, a_n\}$ 恰含 n 个元，故 F_n 的任一基都恰含 n 个元。

6. 指出引理 2 的证明中哪几步利用 A 是交换群的条件。

解 (5) 式 $K = (u) \times (K \cap H_1)$ 的成立需要 A 是交换群的条件。因为虽然已有 $(u) \cap (K \cap H_1) = \{e\}$, $(u)(K \cap H_1) = K$, $K \cap H_1$ 是 K 的正规子群。但 (5) 式的成立，仍需要 (u) 是 K 的的正规子群。而 B（从而 A）是交换群的条件保证了 (5) 式的成立。同样 (6) 式 $H_1 = (V) \times (K \cap H_1)$ 也需 B（从而 A）是交换群这一条件。

习　题

1．设 S_p 是有限群 G 的 $p-$Sylow 子群，N 是 G 的不变子群，证明，S_pN/N 是 G/N 的 $p-$Sylow 子群。

证　设 $|G|=p^\alpha mn$，$|N|=p^\beta n$，$(p, mn)=1$，则 $|S_p|=p^\alpha$，可知 $|S_p\cap N|=p^\gamma$，$\gamma\leqslant\beta$。故 $|S_pN/N|=|S_p/S_p\cap N|=\dfrac{|S_p|}{|S_p\cap N|}=p^{\alpha-\gamma}$，$\alpha-\gamma\geqslant\alpha-\beta$。而 $|G/N|=p^{\alpha-\beta}m$，故 $|S_pN/N|=p^{\alpha-\beta}$，所以 S_pN/N 是 G/N 的一个 $p-$Sylow 子群。

2．设 S_p 是有限群 G 的 $p-$Sylow 子群，$N(S_p)$ 表示 S_p 的正规化子，证明：

① 含于 $N(S_p)$ 的 S_p 的共轭子群只有一个。

② $N(S_p)=N(N(S_p))$。

证　① 设 S_p' 是 $N(S_p)$ 中的在 G 中与 S_p 共轭的一个子群，则 S_p' 和 S_p 同是 $N(S_p)$ 的 $p-$Sylow 子群，因而在 $N(S_p)$ 中共轭，但 S_p 是 $N(S_p)$ 的正规子群，故 $S_p'=S_p$。

② 显然 $N(S_p)\subseteq N(N(S_p))$，任取 $x\in N(N(S_p))$，则由于 $S_p\subseteq N(S_p)$，故 $x^{-1}S_px\subseteq x^{-1}N(S_p)x=N(S_p)$。由①可知 $x^{-1}S_px=S_p$，故 $x\in N(S_p)$，所以 $N(S_p)\supseteq N(N(S_p))$，即 $N(S_p)=N(N(S_p))$。

3．设 S_p 是有限群 G 的 $p-$Sylow 子群，K, L 是 S_p 的子集，适合下面条件：

i) $\forall a\in S_p$：$a^{-1}Ka=K$，$a^{-1}La=L$，

ii) $\exists b\in G$：$L=b^{-1}Kb$，

证明 $\exists c\in N(S_p)$：$L=c^{-1}Kc$。

证 设 $N(K)$，$N(L)$ 分别是 K 和 L 在 G 中的正规化子，则 $S_p\subseteq N(K)$，$S_p\subseteq N(L)$，由 $b^{-1}Kb=L$，容易推得 $b^{-1}N(K)b=N(L)$，故 $b^{-1}S_pb\subseteq b^{-1}N(K)b\subseteq N(L)$，因此 $b^{-1}S_pb$ 和 S_p 是 $N(L)$ 的两个 Sylow 子群，故存在 $x\in N(L)$，使 $x^{-1}(b^{-1}S_pb)x=S_p$，令 $c=bx$，则 $c\in N(S_p)$，且 $c^{-1}Kc=x^{-1}(b^{-1}Kb)x=x^{-1}Lx=L$。

4．设 K 是有限群 G 的子群，H 是 K 的子群，且 K 中与 H 同构的子群均与 H 在 K 中共轭，

证明，$N(K)=(N(H)\cap N(K))K$。

证 由于 K 是 $N(K)$ 的正规子群，$N(H)\cap N(K)$ 是 $N(K)$ 的子群，故 $(N(H)\cap N(K))K$ 是 $N(K)$ 的子群。任取 $x\in N(K)$，由于 $K\supseteq H$，故 $K\supseteq x^{-1}Hx$。根据条件，$x^{-1}Hx$ 和 H 在 K 中共轭，故存在 $b\in K$，使得 $b(x^{-1}Hx)b^{-1}=H$，令 $a=xb^{-1}$，则 $a\in N(H)\cap N(K)$，而 $x=ab$，$x\in(N(H)\cap N(K))K$，所以，$N(K)\subseteq(N(H)\cap N(K))K$，即 $N(K)=(N(H)\cap N(K))K$。

5．设 G 不是循环群，$|G|=p^2$，证明，G 可分解成两个 p 阶循环群的直积。

证 由 G 不是循环群可知，G 中任意元素，除 e 外，周期均等于 p。任取 G 中 p 阶元素 a，则 (a) 是 p 阶循环群，由例 6 可知，(a) 是 G 的正规子群。任取 $b\in G$，$b\bar{\in}(a)$，则 (b) 是 p 阶循环群，是 G 的正规子群。由于 $b\bar{\in}(a)$，故 $(b)\supset(a)\cap(b)$，因而 $(a)\cap(b)=\{e\}$。所以 $(a)\times(b)$ 是 G 的 p^2 阶子群，即 $G=(a)\times(b)$。

6．设有限交换群 G 的阶数被任一素数的平方都除不尽，

则G是循环群。

证设G的不变因子组为$\{h_1, h_2, \cdots, h_n\}$，任取$h_1$的素因子$p$，则有$p|h_i$，$i=1, 2, \cdots, n$，因而$p^n||G|$。由于$p^2 \nmid |G|$，故$n=1$，$G$的不变因子组为$\{h\}$，因而$G$是循环群。

7. 设G是p群，$|G|=p^m$，则G至少含有$p-1$个周期p的元，属于G的中心。

证设C是G的中心，N_a是a在G中的正规化子，$\sum$表示对共轭元素类的代表元求和。根据群的类方程

$$|G| = |C| + \sum_{a \notin C} [G : N_a].$$

$p||C|$，因而C中至少含有1个周期为p的元素，设为a则$C \supseteq (a)$，(a)为p阶循环群，故C至少含有$p-1$个周期为p的元素。

8. 设G是p群，且G含有指数p的循环子群，则G是不可分解的，或G是交换群。

证设(a)是G的指数为p的循环子群，a的周期为p^m，则$|G|=p^{m+1}$。若G中含有周期为p^{m+1}的元素，则G是p^{m+1}阶循环群，不可分解。今设G可分解，则G中元素周期最大值为p^m。

设$G=H\times K$，H中元素周期最大值为p^i，K中元素周期最大值为p^j，$i \geqslant j$，则$a^{p^i}=e$，$\therefore i \geqslant m$，但显然$i \leqslant m$，故$i=m$，$p^m||H|$，因为$K \neq \{e\}$，所以H是p^m阶循环群，K是p阶循环群，因此$G=H\times K$是交换群。

9. 设p，q是素数，且$p<q$，p，q适合何种条件时，pq元群一定是循环群？你找出的这个条件是不是必要的？

解设G是pq元群，则G存在p-Sylow子群C_p，

$q-$Sylow 子群 C_q，且 G 中 $q-$Sylow 子群的个数 $k_q=ql+1$，$k_q|pq$。由于 $(ql+1, q)=1$，故 $k_q|p$，由于 $p<q$，故 $k_q=1$，C_q 是 G 的正规子群。同样可知，G 中 $p-$Sylow 子群的个数 $k_p=pl+1$；$k_p|q$。如果对于任意自然数 l：$(pl+1)\nmid q$，则 $k_p=1$，C_p 是 G 的正规子群，因而 $G=C_p\times C_q=C_{pq}$ 是循环群。条件不是必要的，因为命 $G=C_p\times C_q$，且 $(pl+1)\nmid q$，$\forall$自然数 l，则 G 仍是循环群。例如 $G=C_{35}$。

10. 证明，n 个生成元的自由交换群的子群仍是自由交换群。

证 此处所说子群应 $\neq\{e\}$，其中 e 是群的单位元

设 $F_n=(a_1)\times\cdots\times(a_n)$，并设 V 是 F_n 的任意子群，但 $V\neq\{e\}$。对于 $e\neq x\in F_n$，有唯一表示式

$$x=a_1^{k_1}a_2^{k_2}\cdots a_n^{k_n}，\text{其中 } k_1，\cdots，k_n \text{ 不全为 } 0。$$

若 $k_n\neq 0$，而 $k_{m+1}=\cdots=k_n=0$，则称 x 的长度是 m，记作 $l(x)=m$，并称 k_m 是 x 的最后指数；可知有

$$1\leqslant l(x)\leqslant n，\ \forall e\neq x\in F_n。$$

再规定 $l(x)=0\Longleftrightarrow x=e$。

我们先证明存在 $b_1\in V$ 满足

① (b_1) 是无限循环群，

② $V\supseteq(b_1)$

③ 当 $v\in V$，并 $l(v)\leqslant l(b_1)$ 时，必有 $v\in(b_1)$。

设 V 中 $\neq e$ 的元的长度中最小者是 m，易知 V 中有长度是 m 且最后指数是正整数的元，这种元中总有一个元 b_1 其最后指数为最小，设

$$b_1=a_1^{k_1}\cdots a_{m-1}^{k_{m-1}}a_m^{k}。$$

当然 $V\supseteq(b_1)$，且因 $k>0$，可知 (b_1) 是无限循环群。当

$v\in V$，且 $l(v)\leqslant l(b_1)$ 时，若 $l(v)<l(b_1)$，则可知 $v=e\in(b_1)$。若 $l(v)=l(b_1)$，则可设

$$v=a_1^{L1}\cdots a_{m-1}^{Lm-1}a_m^{L}$$

设 $l=kq+r$，$0\leqslant r<k$，则有

$vb_1^{-q}=a_1^{q1}\cdots a_{m-1}^{am-1}a_m^{r}\in V$，$\alpha_1\cdots\alpha_{m-1}$ 是整数，由 b_1 的选法知 r 不能 >0。故 $r=0$，于是 $l(vb_1^{-q})<m$，从而 $vb_1^{-q}=e$，故 $v=b_1^{q}\in(b_1)$。

今设已有 $b_1, b_2, \cdots, b_s\in V$，满足

$$\begin{cases}①\ (b_i)\text{ 是无限循环群，}i=1,2,\cdots,s,\text{ 且}\\ \quad l(b_1)<l(b_2)<\cdots<l(b_s),\\ ②\ V\supseteq(b_1)\times\cdots\times(b_s),\\ ③\ \text{当 }v\in V,\text{且}l(v)\leqslant l(b_s)\text{时，必有}v\in(b_1)\times\cdots\times(b_s).\end{cases}$$

这里 $s\geqslant 1$。

若 $V=(b_1)\times\cdots\times(b_s)$，则 V 即是自由交换群。

若 $V\supset(b_1)\times\cdots\times(b_s)$，记 $V'=(b_1)\times\cdots\times(b_s)$，则 $V-V'\neq\phi$，且 $V-V'$ 中有 $\neq e$ 的元。

设 $V-V'$ 中 $\neq e$ 的元的长度中最小者是 r，则可知 $r>l(b_s)$，又易知 $V-V'$ 中有长度为 r 且最后指数是小正整数的元，这种元中总有一个元 b_{s+1}，其最后指数最小，

设 $b_{s+1}=a_1^{k1}\cdots a_{r-1}^{kr-1}a_r^{k}$

可知 (b_{s+1}) 是无限循环群，且 $l(b_s)\leqslant l(b_{s+1},)$ 又 $V\supseteq(b_{s+1})$。

当 $x\in((b_1)\times\cdots\times(b_s))\cap(b_{s+1})$ 时，易知必 $x=e$，故有直积 $(b_1)\times\cdots\times(b_s)\times(b_{s+1})$，且当然

$$V\supseteq(b_1)\times\cdots\times(b_s)\times(b_{s+1}).$$

当 $v\in V$，且 $l(v)\leqslant lb_{s+1})$ 时，若 $l(v)<l(b_{s+1})$，则当 $v=e$ 时，有 $v\in(b_1)\times\cdots\times(b_s)\times(b_{s+1})$，而当 $v\neq e$ 时，据

b_{s+1}^{-q} 的选法可知 $v\in V-V'$。但 $v\in V$，故 $v\in V'$，从而 $v\in(b_1)\times\cdots\times(b_s)\times(b_{s+1})$。

若 $l(v)=l(b_{s+1})$，设 $v=a_1^{j_1}\cdots a_{r-1}^{j_{r-1}}a_r^{j_r}$，则设 $l=qk+h$，$0\leqslant h<k$ 时，有 $vb_{s+1}^{-q}=a_1^{\alpha_1}\cdots a_{r-1}^{\alpha_{r-1}}a_r^{h}\in V$，若 $h>0$，则 $l(vb_{s+1}^{-q})=r$，由 b_{s+1} 的选法知 $vb_{s+1}^{-q}\in V'$，故 $v\in(b_1)\times\cdots\times(b_s)\times(b_{s+1})$。若 $h=0$，则 $vb_{s+1}^{-p}=a_1^{\alpha_1}\cdots a_{r-1}^{\alpha_{r-1}}$，故 $l(vb_{s+1}^{-q})<r=l(b_{s+1})$，因此 $vb_{s+1}^{-q}=e$，或 $vb_{s+1}^{-q}\in V'$，总之有 $v\in(b_1)\times\cdots\times(b_s)\times(b_{s+1})$。

由于 $l(b_1)<l(b_2)<\cdots<l(b_s)<l(b_{s+1})<n$，而 n 是定自然数，诸 $l(b_i)$ 是正整数，故此过程不能无限继续，是即总有正整数 m 使

$$V=(b_1)\times\cdots\times(b_m)$$

而 (b_1)，…，(b_m) 都是无限循环群，故 V 是自由交换群。

11. 证明，n 个生成元的交换群一定是 n 个生成元的自由交换群的同态象。

证设 $F_n=(a_1)\times(a_2)\times\cdots\times(a_n)$ 是自由交换群，B 是由 $\{b_1,b_2,\cdots,b_n\}$ 生成的交换群。

命 φ：$a_1^{j_1}a_2^{j_2}\cdots a_n^{j_n}\longmapsto b_1^{j_1}b_2^{j_2}\cdots b_n^{j_n}$。

容易验证 φ 是 F_n 到 B 的同态满射，故 B 是 F_n 的的同态象。

12. 设 G 是交换群，$G=A\times(a)=B\times(b)$，此处 (a)，(b) 是 p 阶循环群，p 是素数。

① 证明，存在 p 阶循环群 $(c)\subseteq G$，使

$$G=A\times(c)=B\times(c)$$

② 证明，$A\cong B$。

③ 举例说明，$A\times(c)=B\times(c)$ 未必有 $A=B$。

证：① 如果 $a\overline{\in}B$，则 $(a)\supset B\cap(a)$，从而 $B\cap(a)=$

$\{e\}$. $G \supseteq B\times(a)\supset B$. 因为 B 在 G 中的指数 p 是素数，故 $G=B\times(a)=A\times(a)$. 同样可以证明，如果 $b\bar{\in}A$，则 $G=A\times(b)=B\times(b)$. 今设 $a\in B$, $b\in A$, 因为 $a\bar{\in}A$，故 $ab\bar{\in}A$，否则就要推出 $a\in A$. 显然 ab 的周期为 p，是个素数，因而 $A\cap(ab)=\{e\}$，由 A 在 G 中的指数为素数，所以 $G=A\times(ab)$，同样可知 $G=B\times(ab)$.

② 由 $G=A\times(c)=B\times c$，可知 $A\cong G/(c)\cong B$.

③ 设 $G=(a)\times(b)$，(a)，(b) 都是 p 阶循环群. 显然 $ab\bar{\in}(b)$，因为 ab 的周期为 p 是素数，故 $(b)\cap(ab)=\{e\}$，由于 G 的阶数是 p^2，因而 $G=(ab)\times(b)=(a)\times(b)$，显然 $(ab)\neq(a)$.

13. 设 G 是交换群，$G=A\times(a)=B\times(b)$，此处 (a)，(b) 是 p^n 阶循环群，p 是素数. 证明 $A\cong B$.

证 我们讨论以下三种情形：

① $A\cap(b)=\{e\}$.

此时，$A\times(b)$ 是 G 的子群，即 $G\supseteq A\times(b)\supset A$，因而 $[G:A]=[G:A\times(b)][A\times(b):A]$，由于 $[G:A]=p^n=[A\times(b):A]$，故 $[G:A\times(b)]=1$，因而 $G=A\times(b)=B\times(b)$，$A\cong G/(b)\cong B$.

② $B\cap(a)=\{e\}$.

与情形①相同，可知 $A\cong B$.

③ $A\cap(b)\neq\{e\}$，且 $B\cap(a)\neq\{e\}$.

由于 $A\cap(b)\neq\{e\}$，而 $A\cap(b)$ 是 (b) 的子群，可知 $A\cap(b)$ 是 p^k 阶循环群，$1\leqslant k\leqslant n$. 故 $A\cap(b)=(b^{p^{n-k}})$，所以 $b^{p^{n-1}}=(b^{p^{n-k}})^{k-1}\in A$. 由于 $a^{p^{n-1}}\bar{\in}A$，故 $(ab)^{p^{n-1}}\bar{\in}A$. 当然有 $(ab)^{p^{n-1}}\neq e$. 由于 a, b 的周期都是 p^n，故 ab 的周

期是 p^n 的一个约数。但 $(ab)^{p^{n-1}} \neq e$，故 ab 的周期是 p^n，(ab) 是 p^n 阶循环群。如果 $A \cap (ab) \neq \{e\}$，则必有 $(ab)^{p^{n-1}} \in A$，现在已经证明 $(ab)^{p^{n-1}} \bar{\in} A$，故 $A \cap (ab) = \{e\}$，$A \times (ab)$ 是 G 的一个子群。由于 $[A \times (ab) : A] = p^n$，故 $G = A \times (ab)$。同理可知，$G = B \times (ab)$，因而

$$A \cong G/(ab) \cong B.$$

14. 证明，阶数为 255 的群一定是循环群。

证 因为 $255 = 3 \times 5 \times 17$，故 255 阶群 G 含有 3－Sylow子群 C_3，5－Sylow 子群 C_5，17－Sylow子群 C_{17}。设这些Sylow子群的个数分别为 k_3, k_5, k_{17}。由 $k_3 = 3l + 1$，$k_3 | 255$，得 $k_3 = 1, 85$，同理可得 $k_5 = 1, 51$，$k_{17} = 1$。下面分四种情形讨论。

① $k_3 = 85$，$k_5 = 51$，$k_{17} = 1$。此时周期为 3 的元素有 $85 \times 2 = 170$个，周期为 5 的元素有 $51 \times 4 = 204$ 个。但 $107 + 204 = 374 > 255$，此种情形不能存在。

② $k_3 = 85$，$k_5 = 1$，$k_{17} = 1$。C_3 的正规化子在 G 中的指数 $k_3 = 85$，故 C_3 的正规化子是 3 阶循环群，因此，设 $C_3 = (a)$，$C_5 = (b)$ 时，必有 $ba \neq ab$，因为否则 b 将属于 C_3 的正规化子，而这不可能，由于 $k_5 = 1$，故 C_5 在 G 中正规。因此可设 $a^{-1}ba = b^i$，于是有 $b = a^{-3}ba^3 = b^{i^3}$，故 $i^3 \equiv 1 \pmod 5$ 但此时得出 $i = 1$，从而 $a^{-1}ba = b$，即 $ba = ab$。导出矛盾。

③ $k_3 = 1$，$k_5 = 51$，$k_{17} = 1$。同情形 ② 一样导出矛盾。

④ $k_3 = 1$，$k_5 = 1$，$k_{17} = 1$。此时 C_3, C_5, C_{17} 均是 G 的正规子群，且是阶数两两互素的循环群，因而 $G = C_3 \times C_5 \times C_{17} = C_{255}$。所以阶数为 255 的群必定是循环群。

15. 证明，阶数为 45 的群一定是交换群。

证 设 $|G|=45$，则 G 的 3－Sylow 子群 K 是一个 9 阶群，G 的 5－Sylow 子群是 5 阶循环群 C_5。设 3－Sylow 子群的个数为 k_3，5－Sylow 子群的个数为 k_5。则 $k_3=3l+1$，$k_3|45$；$k_5=5l+1$，$k_5|45$，因此 $k_3=k_5=1$，K 和 C_5 都是 G 的正规子群。显然 $K\cap C_5=\{e\}$，故 $G=K\times C_5$。

由第 5 题可知，9 阶群 K 或者是 9 阶循环群，或者是两个 3 阶循环群的直积。在这两种情形下，K 都是交换群。由于 K 和 C_6 都是交换群，故 $G=K\times C_5$ 是交换群。

16。决定所有 18 阶的群。

解 设 $|G|=18$，因为 $18=2\times3^2$，故 G 的 2－Sylow 子群是 C_2，G 的 3－Sylow 子群是 9 阶群，故有两种可能，C_9 或 B_9（两个 3 阶循环群的直积）。2－Sylow 子群的个数 $k_2=2l+1$，$k_2|18$。故 $k_2=1$，3，或 9。3－Sylow 子群的个数 $k_3=3l+1$，$k_3|18$，故 $k_3=1$。故 G 只能有以下三种情形：① 一个 2－Sylow 子群，一个 3－Sylow 子群；② 3 个 2－Sylow 子群，一个 3－Sylow 子群；③ 9 个 2－Sylow 子群，一个 3－Sylow 子群。

情形 1。G 含有不变子群 C_2，又含有不变子群 C_9 或 B_9。此时，G 有两种情形，$G=C_2\times C_9=C_{18}$，或 $G=C_2\times B_9$，二者都是可换群。

情形 2。G 含有三个共轭的 2 阶子群和一个 9 阶不变子群（C_9 或 B_9）。这四个子群两两交成 $\{e\}$，因此这四个子群共含有 12 个元素，即 G 中尚有 6 个元素不属于任何 Sylow 子群。任取一个这样的元素 x，则 x 的周期只能为 6。令 $a=x^2$，$c=x^3$，则 a 的周期为 3，c 的周期为 2，且 $ac=ca$。我们证明 G 的唯一的 3－Sylow 子群不能是 C_9。因为假定它

是 $C_9=(b')$，则因 a 的周期是3，由第二Sylow定理可知 $a\in C_9$，从而又可知 $a=b'^3$ 或 $a=b'^6$。当 $a=b'^3$ 时，命 $b=b'$；当 $a=b'^6$ 时，命 $b=b'^2$，则 $C_9=(b)$，$a=b^3$。设 $c^{-1}bc=b^i$，则 $i^2\equiv 1(mod\ 9)$，$i=1$ 或 8。当 $i=1$ 时，$bc=cb$，而 b 的周期9和 c 的周期2互素，故 bc 的周期为18，从而 G 是18阶循环群，与 G 含有三个共轭的2－Sylow子群矛盾。当 $i=8$ 时，$c^{-1}ac=c^{-1}b^3c=(c^{-1}bc)^3=b^{24}=b^6=a^2$，但 $ac=ca$，即 $c^{-1}ac=a$，故有 $a=a^2$，这与 $a\neq e$ 矛盾。故 G 的唯一的3－Sylow子群不能是 C_9，从而是 B_9。此时 $a\in B_9$。设 N_a 是 a 在 G 中的正规化子，由于 B_9 是交换群，$a\in B_9$，故 $N_a\supseteq B_9$。由于 $ac=ca$，故 $C\in N_a$，但 c 的周期是2，故 $c\overline{\in}B_9$，因此，$N_a\supset B_9$。由于 $[G:B_9]=2$，故 $[G:N_a]=1$，从而 $G=N_a$。设 G 的中心为 C，则 $a\in C$。任取 $d\in B_9$，但 $d\overline{\in}(a)$，由于 B_9 是交换群，而 $d\in B_9$，故 d 在 G 中的正规化子 $N_d\supseteq B_9$。若 $N_d=G$，则 $d\in C$，从而 $B_9=(a)\times(d)\subseteq C$。再由 $[G:B_9]=2$，易知 G 应为交换群，矛盾。因此 $N_d\neq G$，故 $N_d=B_9$，从而 $[G:N_d]=[G:B_9]=2$，即 d 共有两个共轭元，故 G 中全部8个周期为3的元中，除 a 和 a^2 外，其余6个周期为3的元两两共轭。设这6个元素为 u，u^2，v，v^2，w，w^2。如果 u 与 v 共轭，则必 u^2 与 u^2 共轭，这时必 w 与 w^2 共轭。同样，如果 u 与 w 共轭，则必 u^2 与 w^2 共轭，这时 v 与 v^2 共轭。因此，在 u，v，w 中至少有一个元与自己的平方共轭。设此元是 g，则 (g) 是 G 的正规子群，而且 $B_9=(a)\times(g)$。g 在 G 中的正规化子 $N_g=B_9$。设 $c^{-1}gc=g^i$ 则 $i^2\equiv 1(mod\ 3)$，故 $i=1,2$。若 $i=1$，则有 $gc=cg$，$c\in N_g$，这与 $N_g=B_9$ 矛盾，故 $i=2$，$c^{-1}gc=g^2$。故 G 是由关系式

$a^3=e$, $g^3=e$, $c^2=e$, $ag=ga$, $ac=ca$, $gc=cg^2$ 所决定的18阶群. 为了证明这个乘法表确实是群的乘法表, 命 $a\mapsto((1),(123))$, $g\mapsto((123),(1))$, $c\mapsto((12),(1))$, 则 $\{((1),(123)),((123),(1)),((12),(1))\}$ 在 $S_3\times C_3$ 中生成的子群 $S_3\times C_3$ 恰好与 G 同构.

情形3. G 含有9个共轭的2阶子群和一个9阶不变子群 (C_9 或 B_9). 设 G 含有 C_2 和 C_9, 并设 $C_2=(c)$, $C_9=(a)$. 因为 C_9 是 G 的不变子群, 设 $c^{-1}ac=a^i$, 则 $i\equiv1(mod\ 9)$, 故 $i=1$ 或 8. 但当 $i=1$ 时, G 含有周期为18的元素 ac, 这不可能. 故 $i=8$, 即 $c^{-1}ac=a^8$. 因而由关系 $a^9=e$, $c^2=e$, $ac=ca^8$ 定义群 G. 为了证明这个乘法表确实是群的乘法表, 命 $a\mapsto(1\,2\,3\,4\,5\,6\,7\,8\,9)$, $c\mapsto(19)(28)(37)(46)$, 则 $\{(1\,2\,3\,4\,5\,6\,7\,8\,9),(19)(28)(37)(46)\}$ 在 S_9 中生成的子群恰好与 G 同构. 这样, 就证明了群 G 存在, G 是18阶二面体群.

设 G 含有 C_2 和 B_9. 由于 G 中含有9个共轭的2阶子群和一个9阶不变子群. 而这些子群两两交成 $\{e\}$, 共有18个元, 因而 G 中只有周期为1, 2及3的元素, 因此不存在周期为6的元素, 故周期为3的元素和周期为2的元素不能交换, 因而 G 的中心 $C=\{e\}$. 设 $B_9=(a)\times(b)$, 任取 $c\in G$, 但 $c\bar{\in}B_9$, 因而 c 的周期为2. 由于 $a\in B_9$, 而 B_9 是 G 的正规子群, 故 $c^{-1}ac\in B_9$. 命 $x=a(c^{-1}ac)$, 则 $x\in B_9$. 且因 B_9 是交换群, 有 $a(c^{-1}ac)=(c^{-1}ac)c$, 于是 $c^{-1}xc=c^{-1}(ac^{-1}ac)c=c^{-1}acc^{-1}(c^{-1}ac)c=c^{-1}ac(c^{-2}ac^2)=(c^{-1}ac)a=a(c^{-1}ac)=x$. 因为 $x\in B_9$, 而 B_9 是交换群, 故 x 在 G 中的正规化子 $N_x\supseteq B_9$. 由于 $c^{-1}xc=x$, 故 $c\in N_x$, 但 $c\bar{\in}B_9$, 故 $N_x\supset B_9$,

从而 $N_x=G$，因而 $x\in C$，但 $c=\{e\}$，故 $x=e$，即 $ac^{-1}ac=e$，$c^{-1}ac=a^2$。同理可得 $c^{-1}bc=b^2$，故 G 由关系 $a^3=e$，$b^3=e$，$c^2=e$，$ab=ba$，$ac=ca^2$，$bc=cb^2$ 所确定。命 $\mapsto(123)$，$b\mapsto(456)$，$c\mapsto(12)(45)$，则由 $\{(123),(456),(12)(45)\}$ 在 S_6 中生成的子群与 G 同构。这就证明了 G 的存在性。

由以上讨论可知，18 阶的群，就同构的意义来讲，共有五个，其中两个是交换群，三个是非交换群。

17．决定所有 20 阶的群。

解 设 $|G|=20$，由于 $20=2^2\times5$，故 G 的 $2-$Sylow 子群为 4 阶，存在两种可能 C_4 或 B_4（*Klein* 四元群），G 的 $5-$Sylow 子群为 5 阶循环群 C_5。$2-$Sylow 子群的个数 $k_2=2l+1$，$k_2|20$，故 $k_2=1$ 或 5。$5-$Sylow 子群的个数 $k_5=5l+1$，$k_5|20$，故 $k_5=1$。

情形 1。G 含有不变子群 C_4 或 B_4，又含有不变子群 C_5。此时，G 有两种情形，$G=C_4\times C_5=C_{20}$，或 $G=B_4\times C_5$。二者都是可换群。

情形 2。G 含有不变子群 C_5 和五个共轭的 4 阶子群。此时又可分为两种情形。

① G 含有 C_4。设 $C_4=(a)$，$C_5=(c)$。因为 C_5 是 G 的正规子群，故可设 $a^{-1}ca=c^i$，$i^4\equiv1(mod\ 5)$，可知 $i=1,2,3$ 或 4。当 $i=1$ 时，ac 的周期为 20，G 为循环群，与 G 含有五个共轭的 $2-$Sylow 子群相矛盾。故 $i=2,3$ 或 4。

当 $i=2$ 时，$a^{-1}ca=c^2$，G 由关系 $a^4=e$，$c^5=e$，$ca=ac^2$ 所定义。命 $a\mapsto(1243)$，$c\mapsto(12345)$，则 $\{(1243),(12345)\}$ 在 S_5 中生成的子群与 G 同构，这就证明了 G 的存在性。

当 $i=3$ 时，$a^{-1}ca=c^3$。但这时 $a^{-3}ca^3=c^{3^3}=c^{27}=c^2$，

而 $c_4=(a)=(a^3)$，因此同 $i=2$ 时一样。

当 $i=4$ 时，$a^{-1}ca=c^4$，G 由关系 $a^4=e$，$c^5=e$，$ca=ac^4$ 所定义。命 $a\mapsto((15)(24),(1234))$，$c\mapsto((12345),(1))$，则 $\{((15)(24),(1234)),((12345),(1))\}$ 在 $s_5\times c_4$ 中生成的子群与 G 同构，这就证明了 G 的存在性。

② G 含有 B_4。设 $C_5=(c)$，任取 $x\in B_4$，由于 C_5 是 G 的正规子群，故可设 $x^{-1}cx=c^i$，从而 $i^2\equiv 1\pmod 5$，得 $i=1$ 或 4。我们证明 B_4 中必存在周期为 2 的元素和 c 可交换。首先可以设 B_4 中周期为 2 的元素是 x，y，xy。若 x，y 与 c 不可换，则 $x^{-1}cx=c^4$，$y^{-1}cy=c^4$，故 $(xy)^{-1}c(xy)=y^{-1}(x^{-1}cx)y=y^{-1}c^4y=(y^{-1}cy)^4=c^{16}=c$，所以 $(xy)c=c(xy)$。这就证明了 B_4 中存在周期为 2 的元素和 c 可交换。设该元素为 a，并设 N_a 是 a 在 G 中的正规化子。因为 B_4 是交换群，而 $a\in B_4$，故 $N_a\supseteq B_4$。又因为 $ac=ca$，故 $c\in N_a$，但 $c\bar{\in}B_4$，故 $N_a\supset B_4$。再由 $5=[G:B_4]=[G:N_a][N_a:B_4]$ 及 $[N_a:B_4]>1$，可知 $N_a=G$，故 a 在 G 的中心 C 中。任取 $b\in B_4$，$b\bar{\in}(a)$，则 $B_4=(a)\times(b)$。如果 $b^{-1}cb=c$，则同样由 $N_b\supseteq B_4$，及 $c\in N_b$，而 $c\in B_4$，就有 $N_b\supset B_4$，从而 $N_b=G$，于是有 $b\in C$。而已有 $a\in C$，故 $B_4=(a)\times(b)\subseteq C$。这样，$B_4$ 在 G 中正规，这与 G 含有 5 个共轭的 4 阶子群相矛盾。因而，$b^{-1}cb=c^4$。故 G 由关系 $a^2=e$，$b^2=e$，$c^5=c$，$ab=ba$，$ac=ca$，$cb=bc^4$ 所定义。命 $a\mapsto((12),(1))$，$b\mapsto((1),(15)(24))$，$c\mapsto((1),(12345))$，则 $\{((12),(1)),((1),(15)(24)),((1),(12345))\}$ 在 $C_2\times S_5$ 中生成的子群与 G 同构，并可知 G 是一个 20 阶二面体群。

由以上讨论，知 20 阶的群，就同构意义讲，共有五个，

其中两个是交换群，三个是非交换群。

18. 设G的阶数为p^2q，p，q是互异素数，证明，G含有个不变子群H，且H是Sylow子群。

证：① 设$p>q$，G的$p-$Sylow子群的个数$k_p=pl+1$，$k_p|p^2q$。由于$(pl+1,p^2)=1$，故$(pl+1)|q$。由$p>q$，故$l=0$，$k_p=1$。因而G的$p-$Sylow子群是不变子群。

② 设$p<q$，G的$q-$Sylow子群的个数$k_q=ql+1$，$k_q|p^2q$。由于$(ql+1,q)=1$，故$(ql+1)|p^2$。如果$l=0$，则$k_q=1$，G的$q-$Sylow子群是不变子群。如果$l\neq 0$，由于$p<q$，故$p<ql+1\leqslant p^2$。由于p是素数，$(ql+1)|p^2$，故$ql+1=p^2$，$ql=p^2-1=(p+1)(p-1)$。p^2-1中的任意素因子不大于$p+1$，故p^2-1中不大于p的素因子的唯一可能是$p+1$，因而$q=p+1$。但由于p，q都是素数，故$p=2$，$q=3$。G为12阶群。如果$3-$Sylow子群在G中不正规，则$3-$Sylow子群的个数$k_3=3l+1=4$。则G含有四个共轭的3阶循环群。显然这四个3阶循环群两两交成$\{e\}$，故G中至少有8个周期为3的元素。这些元素当然不能属于$2-$Sylow子群。但G必含有4阶的$2-$Sylow子群，故另外4个元素组成唯一的$2-$Sylow子群，是G的不变子群。

综上所述，G的Sylow子群中，必有一个是G的不变子群。

19. 证明阶数是200的群必含有不变子群H，且H是Sylow子群。

证 设$|G|=200$，G的$5-$Sylow子群的个数为$k_5=5l+1$，$k_5|200$。由于$200=8\times 25$，$(5l+1,25)=1$，故$(5l+1)|8$，由此可得$l=0$，$k_5=1$，G的$5-$Sylow子群是

G的不变子群。

20。设G是一个群，$a\in G$，$a\neq e$，证明，G中存在不含a的极大子群M。即M具有性质：1) M是G的不含a的子群，2) M_1是G的子群，$M_1\supset M$，则$a\in M_1$。

证 命$S=\{K|K$是G的子群，$a\bar{\in}K\}$。由于$\{e\}\in S$，故S不空。其次，S关于包含关系“$\subseteq$”作成一个偏序集。易知S中任一有序子集$T=\{K_\alpha|\alpha\in J\}$的并$\bigcup_{\alpha\in J}K_\alpha$仍在$S$中。故由$Z_{orn}$引理知，$S$含有极大元$M$，$M$就是$G$中不含$a$的极大子群。

21。设H是G的子群，S是G的子集，且$H\cap S=D$。证明，存在G的极大子群M，M含有H，且与S的交为D。

证 命$\sum=\{K|K$是G的子群，$K\supseteq H$，$K\cap S=D\}$。

因为$H\in\sum$，故$\sum$不空。并且$\sum$关于包含关系“$\subseteq$”作成一偏序集合。设$T=\{K_\alpha|\alpha\in J\}$是$\sum$中任一有序子集，易知$\bigcup_{\alpha\in J}K_\alpha$是$G$的子群，且$\supseteq H$，再由$(\bigcup_{\alpha\in J}K_\alpha)\cap S=\bigcup_{\alpha\in J}(K_\alpha\cap S)=D$，可知$\bigcup_{\alpha\in J}K_\alpha\in\sum$。故由$Z_{orn}$引理知$\sum$含有极大元素$W$，$M$即为所求的极大子群。

22。设R是一个环，$a\in R$，$a\neq 0$，证明R中存在不含a的极大理想I。

证 命$S=\{K|K$是R的理想，$a\bar{\in}K\}$。显然零理想属于S，故S不空。且S关于包含关系“$\subseteq$”成一偏序集。对于S的任一有序子集$T=\{K_\alpha|\alpha\in J\}$，容易验证$\bigcup_{\alpha\in J}K_\alpha$是$R$的理想，且$a\bar{\in}\bigcup_{\alpha\in J}K_\alpha$，故$\bigcup_{\alpha\in J}K_\alpha\in S$。于是由$Z_{orn}$引理可知，$S$有极大元$I$，$I$即为所求的极大理想。

编　后

本题解是根据吴品三副教授所编《近世代数》一书编写的，解答了书中全部练习和习题。题解中所用名词、符号与该书一致。根据原书作者所做的勘误，我们对书中的练习和习题进行了校正，凡属修改过的题目，都在标号的右上角注上了“*”号。此外，由于排印条件的限制，对原书第三章题目中少数使用德文字母的地方做了更动。

题解工作是由我室部分同志分别完成的，由于水平所限，加之时间仓促，错误和不妥之处可能不少，诚恳希望同志们批评指正。

最后，我们对北京师范大学吴品三副教授，李天林同志所给予的关心和支持表示感谢。

扬州师院数学系代数教研室

一九八一年一月