HW1 参考答案

Ch1

4(3)

> $|\mathcal{P}(A)| > 1$推出$A \neq \varnothing$ 是否成立?

- 成立。反设$A = \varnothing$，则$\mathcal{P}(A) = \mathcal{P}(\varnothing) = \{\varnothing\}$，故$|\mathcal{P}(A)| = 1$，矛盾。

> 注：反证，空集的幂集是只包含空集的集合，元素个数为1

7(3)

> 用归纳法定义集合：不以0打头的二进制偶整数，它应该包括0，110，1010等

1. $0, 10 \in E$
2. 如果$1x0 \in E$且$a \in E$，则将a插在x后，$1xa0 \in E$
3. 集合E只包含有限次使用1，2所得到的元素

> 注：
>
> 1. 基础语句；归纳语句；终结语句。找到集合的基础元素再选用合适的方法进行归纳
> 2. 尽可能使用字符串的方式构造集合，而不是借助这些数之间的代数关系。所以，如果定义的过程中用到加法、乘法等运算是不合适的，有的同学就是不断+2进行归纳

Ch2

1

> 证明：
>
> 1. 若$a|b, a > 0$，则$(a, b) = a$
> 2. $((a, b), b) = (a, b)$

1. 由于$a|a$且$a|b$，故$a|(a, b)$，又$(a, b)|a$，**结合$\boldsymbol{a > 0}$，$\boldsymbol{(a, b) > 0}$**，知$(a, b) = a$
2. 由1.中的结论即可得证

> 证明两数相等，可以证明两数相互整除；类似的证明集合相等，可以证明两集合相互包含

2(1)

> 证明：对所有$n > 0$成立$(n, n+1) = 1$

- 假设$(n, n+1) = d$，则$d|n$且$d|(n+1)$，故$d|[(n+1) - n] \Rightarrow d|1 \Rightarrow d = 1$

3(1)

> 求x和y使得：$314x + 159y = 1$

- 因为$(314, 159) = 1$，所以可以参照**例2.1**，求解x和y

$$314 = 159 * 1 + 155$$
$$159 = 155 * 1 + 4$$
$$155 = 4 * 38 + 3$$
$$4 = 3 * 1 + 1$$
$$3 = 1 * 3$$

反推回去

$$1 = 4 - 3 * 1 = 4 - (155 - 4 * 38)$$
$$= 4 * 39 - 155$$
$$= (159 - 155 * 1) * 39 - 155$$
$$= 159 * 39 - 155 * 40$$
$$= 159 * 39 - (314 - 159 * 1) * 40$$
$$= 159 * 79 - 314 * 40$$
$$\text{故} x = -40, y = 79$$

> 注：对于形如ax+by=(a,b)的不定方程都可以利用辗转相除法的逆过程求解

6

> 求2345和3456两个数的素数分解式

1. $2345 = 5 \times 7 \times 67$
2. $3456 = 2^7 \times 3^3$

HW 10

7.11

> 求出环$\mathbb{Z}_6$的所有理想

解：$\mathbb{Z}_6=\{[0],[1],[2],[3],[4],[5]\}$，若
I是$\mathbb{Z}_6$的理想，则I一定是加群$<\mathbb{Z}_6,+>$的一个子群，由于加群$<\mathbb{Z}_6,+>$是循环群，所以I也一定是循环群

接下来，我们首先求出$<\mathbb{Z}_6,+>$的所有循环子群：

$$G_1=([0])=\{[0]\}$$
$$G_2=([1])=([5])=<\mathbb{Z}_6,+>$$
$$G_3=([2])=([4])=\{[0],[2],[4]\}$$
$$G_4=([3])=\{[0],[3]\}$$

通过验证G_1,G_2,G_3,G_4均是$\mathbb{Z}_6$的理想

> 先求出所有循环子群，再逐一验证是否为理想

7.12

> 若I_1和I_2是环R的理想，则$I_1\bigcap I_2$，$I_1\bullet I_2$，I_1+I_2都是R的理想，并且$I_1\bullet I_2\subseteq I_1\bigcap I_2$

1. $I_1\bigcap I_2$
   - $I_1\bigcap I_2$是环的非空子集
   - 对$\forall x,y\in I_1\bigcap I_2,\forall r\in R$
     - 减法封闭性
       - $x,y\in I_1\Rightarrow x-y\in I_1$
       - $x,y\in I_2\Rightarrow x-y\in I_2$
       - 故$x-y\in I_1\bigcap I_2$
     - 乘法封闭性
       - $x\in I_1\Rightarrow x\bullet r\in I_1$且$r\bullet x\in I_1$
       - $x\in I_2\Rightarrow x\bullet r\in I_2$且$r\bullet x\in I_2$
       - 故$x\bullet r\in I_1\bigcap I_2$且 $r\bullet x\in I_1\bigcap I_2$
2. $I_1\bullet I_2$
   - $I_1\bullet I_2$是环的非空子集
   - 对$\forall x,y\in I_1\bullet I_2,\forall z\in R$

     不妨设

$$x=\sum_{k=1}^{n_1}a_{1k}a_{2k}\quad(a_{1k}\in I_1,a_{2k}\in I_2)$$
$$y=\sum_{i=1}^{n_2}b_{1i}b_{2i}\quad(b_{1i}\in I_1,b_{2i}\in I_2)$$

     - 减法封闭性

$$
\begin{aligned}
x-y &= \sum_{k=1}^{n_1} a_{1k}a_{2k} - \sum_{i=1}^{n_2} b_{1i}b_{2i} \\
&= \sum_{k=1}^{n_1} a_{1k}a_{2k} + \sum_{i=1}^{n_2} (-b_{1i})b_{2i} \\
&= \sum_{j=1}^{n_1+n_2} l_{1j}l_{2j} \in I_1 \bullet I_2
\end{aligned}
$$

$$
l_{1j} = \begin{cases} a_{1j}, & 1 \le j \le n_1 \\ -b_{1(j-n_1)}, & n_1+1 \le j \le n_1+n_2 \end{cases}
$$

$$
l_{2j} = \begin{cases} a_{2j}, & 1 \le j \le n_1 \\ b_{2(j-n_1)}, & n_1+1 \le j \le n_1+n_2 \end{cases}
$$

- 乘法封闭性

$$
x \bullet z = (\sum_{k=1}^{n_1} a_{1k}a_{2k}) \bullet z = \sum_{k=1}^{n_1} a_{1k}(a_{2k} \bullet z) = \sum_{k=1}^{n_1} a_{1k}\tilde{a}_{2k}
$$

$$
z \bullet x = z \bullet (\sum_{k=1}^{n_1} a_{1k}a_{2k}) = \sum_{k=1}^{n_1} (z \bullet a_{1k})a_{2k} = \sum_{k=1}^{n_1} \tilde{a}_{1k}a_{2k}
$$

$$
\text{其中}\tilde{a}_{2k} = a_{2k} \bullet z \in I_2, \tilde{a}_{1k} = z \bullet a_{2k} \in I_1, \text{因此} x \bullet z \in I_1 \bullet I_2, z \bullet x \in I_1 \bullet I_2
$$

3. $I_1 + I_2$
   - $I_1 + I_2$是环的非空子集
   - 对$\forall x, y \in I_1 + I_2, \forall z \in R$

     不妨设

$$
\begin{aligned}
x &= a + b(a \in I_1, b \in I_2) \\
y &= c + d(c \in I_1, d \in I_2)
\end{aligned}
$$

   - 减法封闭性
     - $x - y = (a+b) - (c+d) = (a-c) + (b-d)$
     - $a - c \in I_1, b - d \in I_2$
     - 故$x - y \in I_1 + I_2$
   - 乘法封闭性
     - $x \bullet z = (a+b) \bullet z = az + bz$
     - $z \bullet x = z \bullet (a+b) = za + zb$
     - 因为I_1, I_2都是理想，所以$az, za \in I_1; bz, zb \in I_2$，进而推出 $x \bullet z \in I_1 + I_2 \text{且} z \bullet x \in I_1 + I_2$
4. $I_1 \bullet I_2 \subseteq I_1 \bigcap I_2$
   - 对$\forall r_1 \in I_1, \forall r_2 \in I_2$，因为 $I_1, I_2 \text{均为理想，所以} r_1 \bullet r_2 \in I_1; r_1 \bullet r_2 \in I_2 \Rightarrow r_1 \bullet r_2 \in I_1 \bigcap I_2$

     而对$\forall x \in I_1 \bullet I_2, \text{设} x = \sum_{k=1}^{n} r_{1k}r_{2k}$，由上可知 $r_{1k} \bullet r_{2k} \in I_1 \bigcap I_2, \text{而} < I_1 \bigcap I_2, + > \text{是群，}$

     $\text{由封闭性可知} x \in I_1 \bigcap I_2$，故$I_1 \bullet I_2 \subseteq I_1 \bigcap I_2$

> 注:
>
> 1. 证明理想的步骤
>   - I是环R的非空子集

> - 减法封闭性
> - 乘法封闭性
> 2. $I_1 \bullet I_2$的定义

7.13

> 证明$I=\left\{\begin{pmatrix}0 & 2x\\0 & 0\end{pmatrix}\ \middle|\ x\in\mathbb{Z}\right\}$是$R=\left\{\begin{pmatrix}a & b\\0 & c\end{pmatrix}\ \middle|\ a,b,c\in\mathbb{Z}\right\}$的理想。商环$R/I$是由哪些元素构成的？

解:

1. 证明I是R的理想
   - I是R的非空子集
   - 对$\forall\begin{pmatrix}0 & 2x\\0 & 0\end{pmatrix}$，$\begin{pmatrix}0 & 2y\\0 & 0\end{pmatrix}\in I;\begin{pmatrix}a & b\\0 & c\end{pmatrix}\in R$
     - $\begin{pmatrix}0 & 2x\\0 & 0\end{pmatrix}-\begin{pmatrix}0 & 2y\\0 & 0\end{pmatrix}=\begin{pmatrix}0 & 2(x-y)\\0 & 0\end{pmatrix}\in I$
     - $\begin{pmatrix}0 & 2x\\0 & 0\end{pmatrix}\begin{pmatrix}a & b\\0 & c\end{pmatrix}=\begin{pmatrix}0 & 2xc\\0 & 0\end{pmatrix}\in I$
     - $\begin{pmatrix}a & b\\0 & c\end{pmatrix}\begin{pmatrix}0 & 2x\\0 & 0\end{pmatrix}=\begin{pmatrix}0 & 2xa\\0 & 0\end{pmatrix}\in I$
   - 综上I是R的理想
2. 商环R/I是由哪些元素构成的？
   - 商环R/I中的等价类满足$\begin{pmatrix}a_1 & b_1\\0 & c_1\end{pmatrix},\begin{pmatrix}a_2 & b_2\\0 & c_2\end{pmatrix}\in R,\begin{pmatrix}a_1 & b_1\\0 & c_1\end{pmatrix}-\begin{pmatrix}a_2 & b_2\\0 & c_2\end{pmatrix}=\begin{pmatrix}a_1-a_2 & b_1-b_2\\0 & c_1-a_2\end{pmatrix}\in I$。即$a_1=a_2;c_1=c_2;b_1,b_2$同奇偶
   - 则$R/I=\left\{\begin{pmatrix}a & 0\\0 & c\end{pmatrix}+I\ \middle|\ a,c\in\mathbb{Z}\right\}\bigcup\left\{\begin{pmatrix}a & 1\\0 & c\end{pmatrix}+I\ \middle|\ a,c\in\mathbb{Z}\right\}$

> 1. 求商环，就是找等价类，等价类中的任意元素相减属于I，从而确定等价类满足的性质
> 2. 商环的每个元素是一个等价类，是一个集合

第11次作业答案

7.14

> 在高斯整数环$\mathbb{Z}[i]=\{a+bi|a,b\in\mathbb{Z}\}$中,$I=(2+i)$含有哪些元素？$\mathbb{Z}[i]/(2+i)$含有哪些元素?

$I=(2+i)=\{(a+bi)(2+i)|a+bi\in Z[i]\}=\{(2a-b)+(a+2b)i|a,b\in Z\}$

方法1：取I中极小元进行分析

由于$(2+i)(2-i)=5,(2+i)(1+2i)=5i$可知，$5,5i\in I$,从而将Z[i]的实部虚部分割成5的同余类$a+bi,a\in\{[0],[1],[2],[3],[4]\},b\in\{[0],[1],[2],[3],[4]\}$,

再考虑到$2+i\in I$,针对$Z[i]=\{x+yi|x,y\in Z\}$中每个元素，在2+i模的意义下又可以将其分割成5组，如下图所示

	y=[0]	y=[1]	y=[2]	y=[3]	y=[4]
x=[0]	0	3	1	4	2
x=[1]	1	4	2	0	3
x=[2]	2	0	3	1	4
x=[3]	3	1	4	2	0
x=[4]	4	2	0	3	1

方法二

$I=(2+i)=\{(a+bi)(2+i)|a+bi\in Z[i]\}=\{(2a-b)+(a+2b)i|a,b\in Z\}$

显然$0\in I$,当$x+yi\in I$时，$x+yi-0\in I$

若$x+yi\notin I$方程组
$\begin{cases}2a-b=x\\a+2b=y\end{cases}$

无整数解,

解得

$$\begin{cases}a=\dfrac{2x+y}{5}\\b=\dfrac{2y-x}{5}\end{cases}$$

从而$x-2y=r\equiv 1,2,3,4\pmod 5$

有$(x-r)+yi\in I$ 其中$r\equiv 1,2,3,4\pmod 5$

而对$x+yi\in I$ 有$r\equiv 0\pmod 5$

这样就将Z中元素分成5个同余类，分别为

$I,1+I,2+I,3+I,4+I$

7.17

> $F[x]$是数域F上的多项式环。在$F[x]$上定义运算$f(x)\cdot g(x)=f(g(x))$. 则 $<F[x],x,\cdot>$ 是否是环？为什么？

不是环，不满足分配律，可以任意举例

$$f(x)=x^2,g(x)=1,h(x)=1$$
$$f(x)(g(x)+h(x))=f(g(x)+h(x))=f(2)=4$$
$$f(x)g(x)+f(x)h(x)=f(g(x))+f(h(x))=2$$

两者不相等，故不是环

7.22

> 证明：$(3)/(6)$是$\mathbb{Z}/(6)$的理想，并且
>
> $$\frac{\mathbb{Z}/(6)}{(3)/(6)}\cong\mathbb{Z}/(3)$$

$\forall x,y\in(3),r\in Z$，因为$(3)=\{3k|k\in Z\}$,设$m=3k_1,n=3k_2\in(3)(k_1,k_2\in Z)$,则

$m-n=3(k_1-k_2)\in(3)$，由于Z中乘法可交换，任取$r\in Z$所以$rm=3rk_1=3k_1r=mr\in(3)$

所以(3)是Z的理想，同理(6)是Z的理想，又因为$(6)\subseteq(3)$，所以根据电子版书定理7.17得证

7.24

> 令ϕ: $R[x]\to R,\phi(f(x))=\phi(a_0+a_1x+\ldots+a_nx^n)=a_0$.
>
> (1)证明ϕ是从环$R[x]$到环R的满同态映射
>
> (2)求$Ker\phi$，并找出与$R[x]/Ker\phi$同构的环。

1

令$f(x)=\sum_{i=0}^n a_ix^i,g(x)=\sum_{i=0}^n b_ix^i$

则$\phi(f(x)+g(x))=\phi(\sum_{i=0}^n(a_i+b_i)x^i)=a_0+b_0=\phi(f(x))+\phi(g(x))$

由由于$\phi(f(x)g(x))=\phi(a_0b_0+(a_1b_0+a_0b_1)x\ldots)=a_0b_0=\phi(f(x))\phi(g(x))$

在$R[x]$中,$1_R=1+\sum_{i=1}^n a_ix^i$,因此有$\phi(1_R)=1$

同时对$\forall a_0\in R$,总有$f(x)=a_0+\sum_{i=1}^n a_ix^i$,$\phi(f(x))=a_0$所以$\phi$是$R[x]\to R$的满同态映射

2

$Ker\phi=\{f(x)|\phi(f(x))=0\}=\{\sum_{i=1}^n a_ix^i|a_1\ldots a_n\in R\}$

所以由环同态基本定理

$R[x]/Ker\phi\cong R$

> 注意：满同态映射单位元不要忘记

HW12 参考答案

ch8

1

`*`是$min\{x_1, x_2\}$,⊕是$max\{x_1, x_2\}$

证明：

$\forall x_1, x_2 \in R, min\{x_1, x_2\} \leq x_1, min\{x_1, x_2\} \leq x_2$

故$min\{x_1, x_2\}$为x_1, x_2的下界。

若c是x_1, x_2的下界，则$c \leq x_1, c \leq x_2$而$min\{x_1, x_2\}$为x_1或x_2

故$c \leq min\{x_1, x_2\}$

因此$min\{x_1, x_2\}$为x_1, x_2的最大下界。

同理$max\{x_1, x_2\}$为x_1, x_2的最小上界。

故$< R_1, \leq >$是格。

4

由定义可得,$a * b = a, a * c = a, b * c = b, a \oplus b = b, a \oplus c = c, b \oplus c = c$

将上式代入(1)(2)可得等式显然成立。

12

充分性:

$$(a \oplus b) * (b \oplus c) * (c \oplus a) = (((a \oplus b) * b) \oplus ((a \oplus b) * c)) * (c \oplus a) = (b \oplus a * c \oplus b * c) * (c \oplus a)$$
$$= b * c \oplus b * a \oplus a * c \oplus a * c \oplus b * c \oplus b * c * a = (b * c) \oplus (b * a) \oplus (a * c)$$

必要性:

$(\Leftarrow)$：格中任意元素 a,b,c

令 $\begin{cases} a' = (a*b)\oplus(a*c) \\ b' = b*c \\ c' = a \end{cases}$

a',b',c' 仍在格中

且有 $(a'*b')\oplus(b'*c')\oplus(c'*a') = (a'\oplus b')*(b'\oplus c')*(c'\oplus a')$ $(*)$

将 a',b',c' 代入，

$(a'*b')\oplus(b'*c')\oplus(c'*a')$

$= [(a*b)\oplus(a*c)*(b*c)] \oplus (b*c*a] \oplus [a*((a*b)\oplus(a*c))]$

$\because a*b\le a \quad a*c\le a$

$\therefore (a*b)\oplus(a*c)\le a$

$\therefore a*[(a*b)\oplus(a*c)] = (a*b)\oplus(a*c)$

$\therefore (a'*b')\oplus(b'*c')\oplus(c'*a')$

$= [(a*b)\oplus(a*c)*(b*c)] \oplus (b*(c*a)] \oplus [(a*b)\oplus(a*c)]$

$= [(a*b)\oplus(a*c)*(b*c)] \oplus [(a*b)\oplus(a*c)]$ $(a*b*c\le a*c)$

$= (a*b)\oplus(a*c)$ (1)

同理，$(a'\oplus b')*(b'\oplus c')*(c'\oplus a')$

$= [(a*b)\oplus(a*c)\oplus(b*c)] * [(b*c)\oplus a] * [a\oplus((a*b)\oplus(a*c))]$

$= [(a*b)\oplus(a*c)\oplus(b*c)] * ((b*c)\oplus a] * a$ $(a\ge a*b, a\ge a*c)$

$= [(a*b)\oplus(a*c)\oplus(b*c)] * a$

$= [(a\oplus b)*(a\oplus c)*(b\oplus c)] * a$ (2)

$= a*(b\oplus c)$

由$(*)$(1)(2)，$(a*b)\oplus(a*c) = a*(b\oplus c)$

由对偶性，可证 $(a\oplus b)*(a\oplus c) = a\oplus(b*c)$

$\therefore$ 该格为分配格

15

- 证明f是$A\to B$的映射:

  $(x\oplus a)*b\le b$显然成立。

  $x\oplus a\ge a$显然成立，$a<b$因此$(x\oplus a)*b\ge a$

  综上，f是$A\to B$的映射。

- 证明f是同态映射:

  对于$\forall x,y\in A, f(x),f(y)\in B,$

  $f(x)\oplus f(y)=((x\oplus a)*b)\oplus((y\oplus a)*b)=((x\oplus a)\oplus(y\oplus a))*b=((x\oplus y)\oplus a)*b=f(x\oplus y)$

  $f(x)*f(y)=((x\oplus a)*b)*((y\oplus a)*b)=((x\oplus a)*(y\oplus a))*b=((x*y)\oplus a)*b=f(x*y)$

  证毕。

HW 13

8.18

> 证明：在布尔代数中，$x \preceq y \Leftrightarrow y' \preceq x'$。

解：布尔代数$\langle A, *, \oplus, ', 0, 1\rangle$对应的$\langle A, *, \oplus\rangle$是格布尔格，因此由定理8.2得

- $x \preceq y \Leftrightarrow x * y = x;$
- $y' \preceq x' \Leftrightarrow y' \oplus x' = x'$

因此只需证，$x * y = x \Leftrightarrow y' \oplus x' = x'$，即证$y' \oplus x' = (x * y)'$，

又因为布尔代数满足交换律故即证$x' \oplus y' = (x * y)'$，由定理8.9，即摩根定律可得。

> 注：布尔代数就是由有补分配格(布尔格)诱导出来的代数系统，所以它满足格的性质，同时满足分配律，有界性，有补元

8.19

> $\langle A_1, *, \oplus, ', 0, 1\rangle$与$\langle A_2, \wedge, \vee, ^{-}, \tilde{0}, \tilde{1}\rangle$是两个布尔代数。证明他们的直积$\langle A_1 \times A_2, \tilde{*}, \tilde{\oplus}, ^{\circ}, 0, 1\rangle$是布尔代数

1. 证明交换律：$(a_1, a_2)\tilde{*}(b_1, b_2) = (b_1, b_2)\tilde{*}(a_1, a_2); (a_1, a_2)\tilde{\oplus}(b_1, b_2) = (b_1, b_2)\tilde{\oplus}(a_1, a_2)$
   - $(a_1, a_2)\tilde{*}(b_1, b_2) = (a_1 * b_1, a_2 \wedge b_2) = (b_1 * a_1, b_2 \wedge a_2) = (b_1, b_2)\tilde{*}(a_1, a_2)$
   - 同理可证，$(a_1, a_2)\tilde{\oplus}(b_1, b_2) = (b_1, b_2)\tilde{\oplus}(a_1, a_2)$
2. 证明分配律：$(a_1, a_2)\tilde{*}(b_1, b_2)(\tilde{\oplus}(c_1, c_2)) = [(a_1, a_2)\tilde{*}(b_1, b_2)]\tilde{\oplus}[(a_1, a_2)\tilde{*}(c_1, c_2)]$
   - $(a_1, a_2)\tilde{*}(b_1, b_2)(\tilde{\oplus}(c_1, c_2)) = (a_1 * b_1, a_2 \wedge b_2)\tilde{\oplus}(c_1, c_2) = (a_1 * b_1 \oplus c_1, a_2 \wedge b_2 \vee c_2)$
   - $[(a_1, a_2)\tilde{*}(b_1, b_2)]\tilde{\oplus}[(a_1, a_2)\tilde{*}(c_1, c_2)] = (a_1 * b_1, a_2 \wedge b_2)\tilde{\oplus}(a_1 * c_1, a_2 \wedge c_2) = ((a_1 * b_1) \oplus (a_1 * c_1), (a_2 \wedge b_2) \vee (a_2 \wedge c_2)) = (a_1 * b_1 \oplus$
   - 另一条分配律同理可证
3. $(0, \tilde{0}), (1, \tilde{1}) \in A_1 \times A_2,$ 对于$A_1 \times A_2$中的任意元素(x, y)
   - $(x, y)\tilde{*}(1, \tilde{1}) = (x, y)$
   - $(x, y)\tilde{\oplus}(0, \tilde{0}) = (x, y)$
4. 对于$A_1 \times A_2$中的任意元素$(x, y),$ 存在$(x, y)^{\circ} = (x', \bar{y}) \in A_1 \times A_2,$ 使得$(x, y)\tilde{*}(x', \bar{y}) = (0, \tilde{0}); (x, y)\tilde{\oplus}(x', \bar{y}) = (1, \tilde{1})$
5. 综上直积$\langle A_1 \times A_2, \tilde{*}, \tilde{\oplus}, ^{\circ}, 0, 1\rangle$是布尔代数

> 注：证明布尔代数的步骤：
>
> 1. 证明交换律
> 2. 证明分配律
> 3. 找到乘法单位元和加法单位元
> 4. 找到元素的补元(**注意不是逆元**)

8.22

> $\langle\{1, 2, 3, 4, 6, 12\}, |\rangle$和$\langle\{1, 2, 3, 4, 6, 8, 12, 24\}, |\rangle$是布尔代数吗？

解：

1. 不是。整除关系的$*, \oplus$分别代表着最大公因子和最小公倍数，即$a, b \in A, a * b = (a, b); a \oplus b = [a, b],$ 单位元分别为12和1，但是2没有补元，故不是布尔代数。
2. 不是。同上。

> 对于整除关系来说，$*, \oplus$分别代表着最大公因子和最小公倍数，即最大下界和最小上界

第二次作业答案

负责人：乐之皓

Ch2 9(3)

> 求所有整数解 15x + 16y = 17.

特解

$$\begin{cases} x = -1 \\ y = 2 \end{cases}$$

故所有整数解为

$$\begin{cases} x = x_0 + \dfrac{b}{(a,b)}t = -1 + 16t \\ y = y_0 - \dfrac{a}{(a,b)}t = 2 - 15t \end{cases} (t \in Z)$$

> 注意：这里$t \in Z$不能漏，b和a不要写反了

Ch2 18(2)

> 解线性同余方程 $3x \equiv 6 \pmod{18}$.

因 (3, 18) = 3, 3 | 6, 有 3 个模 18 不同余的解.

考察 x ≡ 2 (mod 6). x ≡ 2 + 6t(mod 18), 0 ≤ t ≤ 2 是所求解, 即解为 x ≡ 2, 8, 14 (mod 18)

Ch2 19(4)

> 解同余方程组:
>
> $$\begin{cases} 2x \equiv 1 \pmod{5} \\ 3x \equiv 2 \pmod{7} \\ 4x \equiv 1 \pmod{11} \end{cases}$$

方程组等价为

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 3 \pmod{11} \end{cases}$$

$$M = 5 \times 7 \times 11 = 385, M_1 = 77, M_2 = 55, M_3 = 35$$

$$77b_1 \equiv 1 \pmod{5} \Rightarrow b_1 = 3$$

$$55b_2 \equiv 1 \pmod{7} \Rightarrow b_2 = 6$$

$$35b_3 \equiv 1 \pmod{11} \Rightarrow b_3 = 6$$

$$\Rightarrow 77 \times 3 \times 3 + 55 \times 6 \times 3 + 35 \times 6 \times 3 \equiv 2313 \equiv 3 \pmod{385}$$

> 注意：步骤过程按照书上例题来

Ch2 22

> 计算 $\phi(42), \phi(420), \phi(4200)$.

分别将42，420，4200分解质因数，代入公式计算即可

$$42 = 2 \times 3 \times 7, 420 = 2^2 \times 3 \times 5 \times 7, 4200 = 2^3 \times 3 \times 5^2 \times 7,$$

$$\phi(42) = \phi(2) * \phi(3) * \phi(7) = 1 * 2 * 6 = 12$$

$$\phi(420) = \phi(2^2) * \phi(3) * \phi(5) * \phi(7) = (2 * 1) * 2 * 4 * 6 = 96$$

$$\phi(4200) = \phi(2^3) * \phi(3) * \phi(5^2) * \phi(7) = (2^2 * 1) * 2 * (5 * 4) * 6 = 960$$

Ch2 24

> p为素数，(m,n) = p, 问$\phi(mn)$与 $\phi(m)\phi(n)$之间有什么关系

设 $m = p_1^{\alpha_1} * p_2^{\alpha_2} \dots p_n^{\alpha_n}$
设 $n = p_1^{\beta_1} * p_2^{\beta_2} \dots p_n^{\beta_n}$，其中$p_i$为素数，$\alpha_i, \beta_i \geq 0$

$(m, n) = p = p_1^{\min(\alpha_1, \beta_1)} * p_2^{\min(\alpha_2, \beta_2)} \dots p_n^{\min(\alpha_n, \beta_n)}$

不妨另$i = l$时，$\min(\alpha_l, \beta_l) = 1$,其他时刻$\min(\alpha_i, \beta_i) = 0$

由于p为素数，$p_l = p$,有

$$\phi(mn) = mn(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_n})$$

$$\phi(m)\phi(n) = mn(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_l})^2 \dots (1 - \frac{1}{p_n})$$

即可得

$$\phi(mn) = \frac{p}{p-1} \phi(m) * \phi(n)$$

Ch2 27

> 314^{159}除以7的余数是多少?

方法一:

$$314 \equiv -1 \pmod 7$$

$$314^{159} \equiv (-1)^{159} \equiv 6 \pmod 7$$

方法二:

即解$314^{159} \equiv x \pmod 7$

由Euler定理，$314^6 \equiv 1 \pmod 7$

$314^{6*26+3} \equiv x \pmod 7$

$314^3 \equiv x \pmod 7$

$(44 * 7 + 6)^3 \equiv x \pmod 7$

$6^3 \equiv x \pmod 7$

$x \equiv 6 \pmod 7$

余数为6

HW3 参考答案

Ch2

30(1)

> 1^{p-1} + 2^{p-1} + ...+ $(p-1)^{p-1} \equiv -1(modp)$

- 由欧拉定理可得$a^{p-1} \equiv 1(modp)$对a = 1,...,p-1成立。故1^{p-1} + 2^{p-1} + ...+ $(p-1)^{p-1} \equiv p-1 \equiv -1(modp)$成立。

35

> 若n为偶完全数，n>6，证明$n \equiv 1(mod9)$

根据定理2.15， n=$2^{p-1}(2^p-1)$其中p和2^p-1都是素数。
由于n>6,则p>=3.

由于p是素数，分三种情况讨论。

1. p=3

   则n=28，满足条件。

2. p=3k+1,其中k为偶数

   则$n=2^{3k}(2^{3k+1}-1)=8^k(2*8^k-1)$

   则$n \equiv (-1)^k(2*(-1)^k-1)(mod9)$

   由于k是偶数，故满足条件。

3. p=3k+2,其中k为奇数

   则$n=2^{3k+1}(2^{3k+2}-1)=2*8^k(4*8^k-1)$

   则$n \equiv 2*(-1)^k(4*(-1)^k-1) \equiv 8+2(mod9)$

   故满足条件。

37

> 求2，4，7，8，11，13，14模15的阶是多少?

由于$\phi(15)=8$,故阶只可能为1，2，4，8.

易得阶依次为4，2，4，4，2，4，2.

38

(1)

k1	k2	k3	k4	k5	k6	k7
0	1	5	2	22	6	12
k8	k9	k10	k11	k12	k13	k14
3	10	23	25	7	18	13
k15	k16	k17	k18	k19	k20	k21
27	4	21	11	9	24	17
k22	k23	k24	k25	k26	k27	k28
26	20	8	16	19	15	14

(2)

由于29的最小原根为2。

故$ind_2 9 + ind_2 x \equiv ind_2 2 (mod 28)$

查表得$ind_2 9 = 10, ind_2 2 = 1$

故$ind_2 x \equiv -9 \equiv 19 (mod 28)$

查表得$x \equiv 26 (mod 29)$

(3)

由于29的最小原根为2。

故$9 * ind_2 x = ind_2 2 (mod 28)$

查表得

$9 * ind_2 x \equiv 1 (mod 28)$

$ind_2 x \equiv 25 (mod 28)$

$x \equiv 11 (mod 29)$

40

由书中表得2是37的最小原根。

则{2^0,2^1,...,$2^{\phi(37)-1}$}构成了模37的缩系，每个与37互素的a均与且仅与某个2^i模37同余。模37的原根都在上述集合中。

要使2^i也是37的原根，则i需要与36互素。

所以$i \in \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$

故37的原根集合为{2,32,17,13,15,18,35,5,20,24,22,19}

HW4 参考答案

Ch3

5

1. 设$f(x)=\sum_{i=0}^{n}a_ix_i$, 则$\frac{d}{dx}f(x)=\sum_{i=1}^{n}i\cdot a_ix^{i-1}\in R[x]$故这是一个从$R[x]$到$R[x]$的映射，故值域是$R[x]$。由于对于值域中的每个元素都可以通
，易证明为满射。由于任意常数项求导后为0，不为单射，所以可知不为双射。
2. 由于$I(f(x))=\int_0^x f(t)dt=\sum_{i=0}^{n}a_i\frac{x^{i+1}}{i+1}\in R[x]$故这是一个从$R[x]$到$R[x]$的映射。值域为除了含有常数项的$R[x]$。并且特别的，$I(0)=0$，因此
也不是双射

> 注：
>
> 1. 映射：像是唯一的
> 2. 单射：所有元素的原像唯一
> 3. 满射：所有元素均有原像
> 4. 双射：即是单射又是满射

12

> 设$\sigma=\begin{pmatrix}1&2&3&4&5&6\\3&1&4&5&6&2\end{pmatrix},\tau=\begin{pmatrix}1&2&3&4&5&6\\2&4&1&3&6&5\end{pmatrix}$。计算$\tau\sigma$、$\tau^2\sigma$、$\sigma\tau^2$、$\sigma^{-1}\tau\sigma$

$$\tau\sigma=\begin{pmatrix}1&2&3&4&5&6\\1&2&3&6&5&4\end{pmatrix}$$
$$\tau^2\sigma=\begin{pmatrix}1&2&3&4&5&6\\2&4&1&5&6&3\end{pmatrix}$$
$$\sigma\tau^2=\begin{pmatrix}1&2&3&4&5&6\\3&6&4&5&1&2\end{pmatrix}$$
$$\sigma^{-1}\tau\sigma=\begin{pmatrix}1&2&3&4&5&6\\2&6&1&5&4&3\end{pmatrix}$$

> 注：置换没有交换性，所以一定要注意计算顺序

14(2)

> 将下列置换表示成不相交的轮换之积：$\begin{pmatrix}1&2&3&4&5&6&7&8\\3&6&4&1&8&2&5&7\end{pmatrix}$

$$\begin{pmatrix}1&2&3&4&5&6&7&8\\3&6&4&1&8&2&5&7\end{pmatrix}=(134)(26)(587)$$

19

> 写出下列二元函数的小项表达式：
>
> 1. 值恒为1的函数
> 2. 当且仅当两个变量取值相同时，函数的值为一

1. 值恒为一，则$f(1,1)=f(1,0)=f(0,1)=f(0,0)=1$，因为
$f(x_1,x_2)=f(1,1)x_1x_2+f(1,0)x_1\bar{x_2}+f(0,1)\bar{x_1}x_2+f(0,0)\bar{x_1}\bar{x_2}$，所以$f(x_1,x_2)=x_1x_2+x_1\bar{x_2}+\bar{x_1}x_2+\bar{x_1}\bar{x_2}$
2. 当且仅当两个变量取值相同时，函数的值为一，则$f(0,0)=1,f(0,0)=1,$其余为0，$f(x_1,x_2)=x_1x_2+\bar{x_1}\bar{x_2}$

> 注：留意p63 n元开关函数的形式

Ch4

1(3)

> 设E是万有集合，在$\mathcal{P}(E)$上定义如下关系，请说明该关系具有什么性质？
>
> - SR_3T，当且仅当$S\subset T$

- 不自反性、传递性、反对称性

> - 关于反对称性的说明：
> R_3的反对称性等价于$\forall S,T\in\mathcal{P}(E)$，$SR_3T\wedge TR_3S\Rightarrow S=T$, 其中前件$SR_3T\wedge TR_3S$恒假, 因此上式恒真，反对称性成立
> - 注意 "不自反性" 和 "不是自反的 / 没有自反性" 的区别. 后者与自反性是互补的，而前者只是后者的一个子集

2(2)

> 给出整数集合Z上满足如下性质的关系
>
> - 自反的、传递的、但不是对称的

- $x\rho y\Leftrightarrow x\geq y$

> 注：搞清自反、反自反、对称、反对称、传递

第5次作业答案

负责人：乐之皓

Ch4 3

> 设a, b, c, d, R_1, R_2是A上的关系，其中

> $$R_1 = \{(a,a),(a,b),(b,d)\},$$
> $$R_2 = \{(a,d),(b,c),(b,d),(c,b)\}$$

> 求$R_1 \circ R_2, R_2 \circ R_1, R_1^2, R_1^3$

$$1.R_1 \circ R_2 = \{(c,d)\}$$

$$2.R_2 \circ R_1 = \{(a,d),(a,c)\}$$

$$3.R_1^2 = \{(a,a),(a,b),(a,d)\}$$

$$4.R_1^3 = \{(b,c),(b,d),(c,b)\}$$

> 注意：偏序关系是倒着运算的，有些人把R_1^3看成R_1^2

Ch4 4

> R_1是集合B到集合C的关系，R_2与R_3是集合A到集合B的关系。证明：
>
> $$R_1 \circ (R_2 \circ R_3) \subseteq (R_1 \circ R_2) \cap (R_1 \circ R_3)$$

对$\forall (x,y) \in R_1 \circ (R_2 \cap R_3)$均$\exists z \in B$, 使得 $x(R_2 \cap R_3)z$ 且 zR_1y,

所以有 $x(R_2 \cap R_3)z \Rightarrow xR_2z$且$xR_3z$

$xR_2z, zR_1y \Rightarrow (x,y) \in R_1 \circ R_2$

$xR_3z, zR_1y \Rightarrow (x,y) \in R_1 \circ R_3$

所以，$(x,y) \in (R_1 \circ R_2) \cap (R_1 \circ R_3)$

所以，$R_1 \circ (R_2 \circ R_3) \subseteq (R_1 \circ R_2) \cap (R_1 \circ R_3)$

Ch4 5

> 设R是集合A上的二元关系，I_A是A上的恒等关系。证明：$R' = R \cap I_A$是R的自反闭包

- R'具有自反性

  $xR'x \Leftrightarrow xI_Ax$或$xRx$，而$xI_Ax$恒成立
- $R \subseteq R'$显然成立
- 对任意满足P有自反性且$R \subseteq P$的集合P

  $xR'y \Leftrightarrow xI_Ay$或$xRy$

  若xI_Ay, 则$x = y$, 且P有自反性 $\Rightarrow xPy$

  若xRy, 因为$R \subseteq P$，故xPy

  综上两种情况，对任意满足$xR'y$的x，y，都有$xPy \Rightarrow R' \subseteq P$

Ch4 7

> 设$A=1,2,3,4$，在$\mathscr{P}(A)$上定义关系“$\sim$”。任给$S,T\in\mathscr{P}(A)$，
>
> $$S\sim T,\text{当且仅当}|S|=|T|$$
>
> 证明：“$\sim$”是$\mathscr{P}(A)$上的等价关系，并写出他的商集$\mathscr{P}(A)/\sim$

自反性：$\forall S\in\mathscr{P}(A),|S|=|S|$

对称性：$\forall S,T\in\mathscr{P}(A),S\sim T\Rightarrow|S|=|T|\Rightarrow|T|=|S|\Rightarrow T\sim S$

传递性：$\forall S,T,V\in\mathscr{P}(A),S\sim T,T\sim V\Rightarrow|S|=|T|,|T|=|V|\Rightarrow|S|=|V|\Rightarrow S\sim V$

商集：$\{[\phi],[\{1\}],[\{1,2\}],[\{1,2,3\}],[\{1,2,3,4\}]\}$

其中

$[\phi]=\{\phi\}$

$[\{1\}]=\{\{1\},\{2\},\{3\},\{4\}\}$

$[\{1,2\}]=\{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$

$[\{1,2,3\}]=\{\{2,3,4\},\{1,3,4\},\{1,2,4\},\{1,2,3\}\}$

$[\{1,2,3,4\}]=\{\{1,2,3,4\}\}$

Ch4 9

> $\mathbb{R}$是实数集合，在$\mathbb{R}$上定义关系R. 任给$x,y\in\mathbb{R}$
>
> $$xRy,\text{当且仅当}x\text{与}y\text{相差一个整数}$$
>
> 证明：R是$\mathbb{R}$上的等价关系，列出所有等价类的代表元

自反性：$\forall x\in R,x\text{与}x\text{相差}\Rightarrow x\rho x$

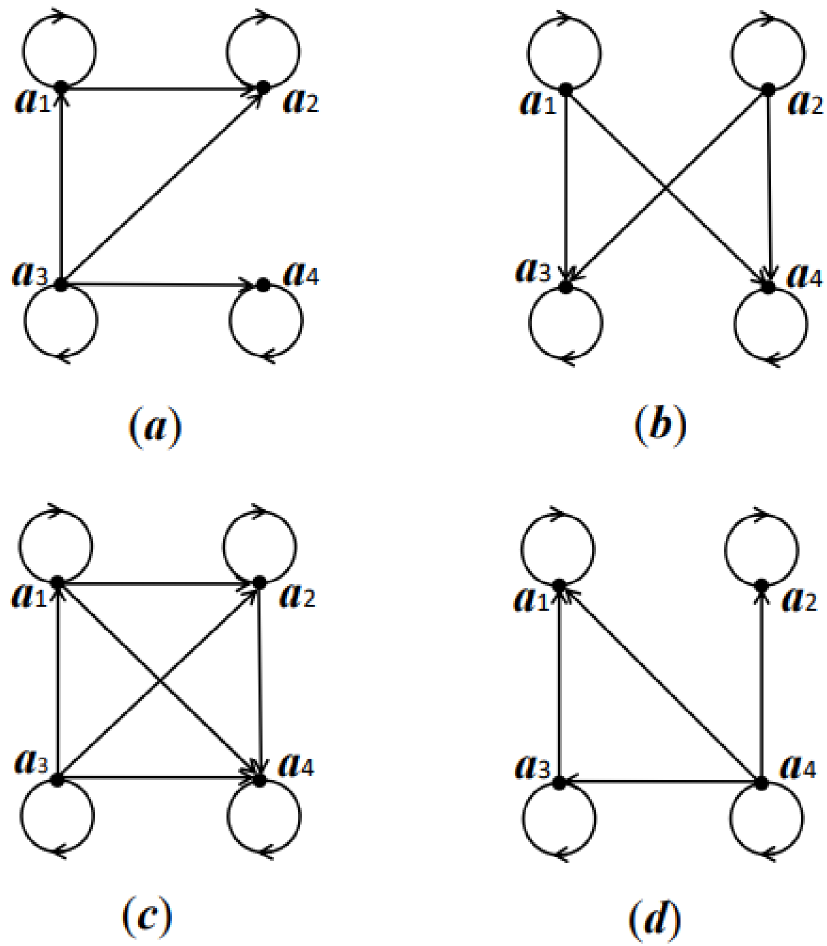
对称性：$\forall x,y\in R,x\rho y\Rightarrow|x-y|=k=|y-x|,k\in\mathbb{N}\Rightarrow y\rho x$

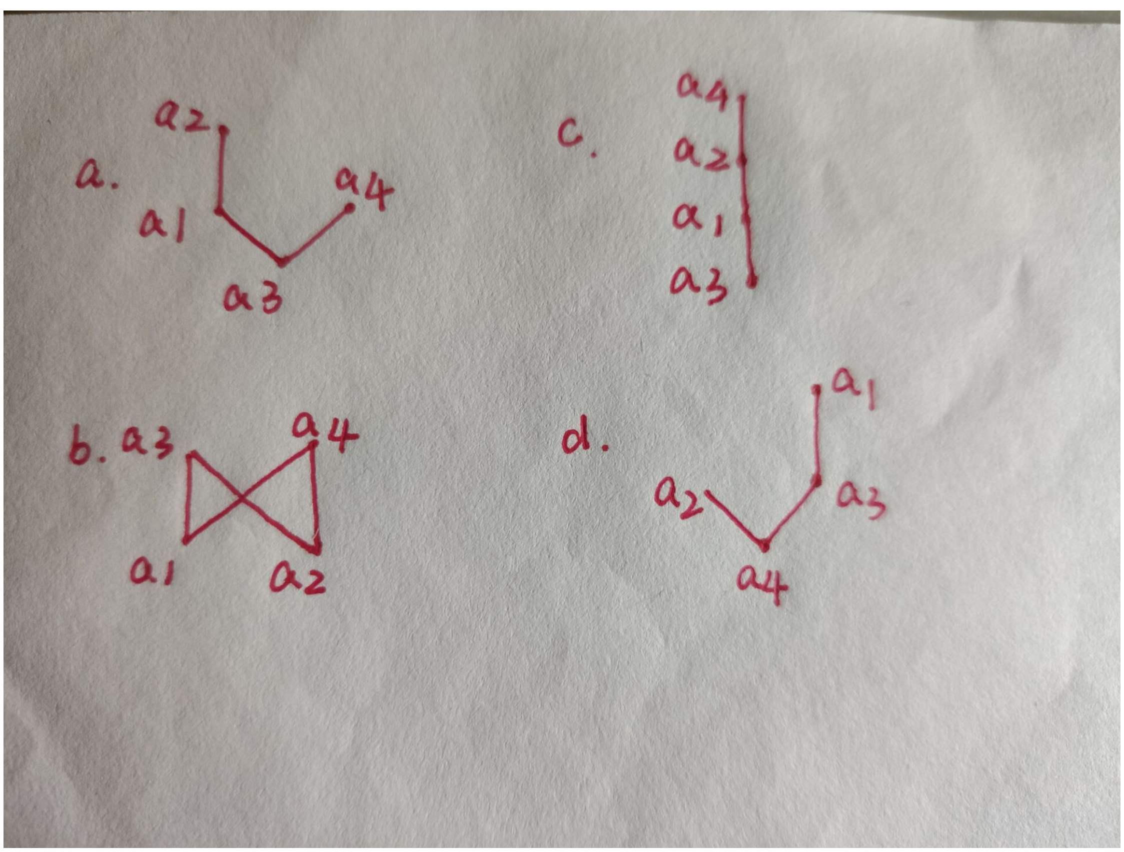
传递性：$\forall x,y,z\in R,x\rho y,y\rho z\Rightarrow x-y=k_1,y-z=k_2(k_1,k_2\in\mathbb{Z})\Rightarrow x-z=k_1+k_2\Rightarrow x\rho z$

全部等价类的代表元：[0,1)上的所有实数

Ch4 13

> 画出每个偏序关系的对应的哈希图





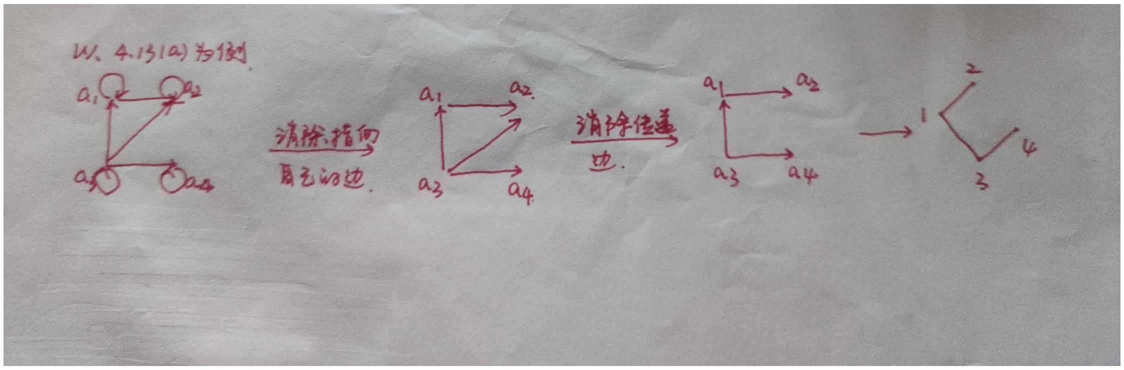
这题错误率比较高，在此给出一些方法：

太长不看版：

第一步：消除指向自己的边

第二步：不断删除走捷径的边，直到不能删除为止

注意:箭头指向控制的元素



在这里copy一下网上正经一点的解法：

[https://www.docin.com/p-598952413.html]:

设集合 $A=\{a_1, a_2, \ldots, a_n\}$，$D_A$ 是在 A 上定义的偏序关系，做<A，D_A>的哈斯图.

首先，　为 A 中的元素定位.

第一步，

令 $R_1=D_A-I_A$

求 $\mathrm{Ran}(R_1)$

求 $A-\mathrm{Ran}(R_1)$

于是，$A-\mathrm{Ran}(R)$中的元素画在哈斯图的第一层(即哈斯图最下面的层);

第二步，

令 R_2={从 R_1 中去掉以第一层的元素为第一元素的有序对，所剩有序对}

求 $\mathrm{Ran}(R_2)$,

求 $\mathrm{Ran}(R_1)\ -\mathrm{Ran}(R_2)$

于是，$\mathrm{Ran}(R_1)\ -\mathrm{Ran}(R_2)$中的元素画在哈斯图的第二层(自下而上).

第三步

令 R_3={从 R_2 中去掉以第二层的元素为第一元素的有序对，所剩有序对}

求 $\mathrm{Ran}(R_3)$,

求 $\mathrm{Ran}(R_2)-\mathrm{Ran}(R_3)$

于是，$\mathrm{Ran}(R_2)-\mathrm{Ran}(R_3)$中的元素画在哈斯图的第三层.

…　…　…　…　…　…　…　…

第 $k-1$ 步

令 R_{k-1}={从 R_{k-2} 中去掉以第 $k-2$ 层的元素为第一元素的有序对，所剩有序对}

求 $\mathrm{Ran}(R_{k-1})$,

求$(R_{k-2})-\mathrm{Ran}(R_{k-1})$

于是，$\mathrm{Ran}(R_{k-2})-\mathrm{Ran}(R_{k-1})$中的元素画在哈斯图的第 $k-1$ 层.

第 k 步，

令 R_k={从 R_{k-1} 中去掉以第 $k-1$ 层的元素为第一元素的有序对，所剩有序对}=∅,

于是将 $\mathrm{Ran}(R_{k-1})$中的元素画在第 k 层(最顶层).

其次，将有遮盖关系的顶点连线，就得到$<A, D_A>$的哈斯图．

注释：设$<A,\preceq>$是偏序集，$x,y \in A$，如果 $x<y$，不存在 $z\in A$，使得 $x<z$ 且 $z<y$，则称 y 遮盖 x．

如，在自然数集合 **N** 上的小于关系"＜"，$<1,2>$，$<2,4> \in <$，2 遮盖 1，因为在 1,2 之间不存在另一个自然数 k，使得 $1<k$ 且 $k<2$．而 4 不能遮盖 2，因为存在 $3\in \mathbf{N}$，使得 $2<3$ 且 $3<4$．

HW6 参考答案

Ch4

15

证明：首先证明$<Z^*,\leq>$是部分序集

① 自反性：$\forall x \in Z^*, x \cdot x > 0, x|x \Rightarrow x \leq x$

② 反对称性：$\forall m,n \in Z^*$,若 $m \leq n, n \leq n \Rightarrow m \cdot n > 0, m|n, n|m \Rightarrow m = n$

③ 传递性：$\forall m,n,p \in Z^*$,若 $m \leq n, n \leq p \Rightarrow mn > 0, np > 0$,则 $mn^2p > 0$，即 $mp > 0$，且 $m|n, n|p$，则 $m|p$，综上$m \leq p$

其次，有结论：$<Z^*,\leq>$ 不存在最大元，最小元，极大元，存在 2 个极小元

① 假设存在极大元 k，则存在$2k \in Z^*$，使得 $2k^2 > 0$，且 $k|2k$，即$k \leq 2k$，矛盾

② 因为没有极大元，所以没有最大元

③ 因为$p = 1$ 与任意 $m \in Z^*, m > 0$，有 $p \cdot m > 0, p|m$，则 $p \leq m$，而不存在 $n \in Z^*$，$n \neq p$，$n \cdot p > 0, n|p$，则$p = 1$ 是极小元，同理，$p = -1$ 也是极小元

4.因为有两个极小元，所以不存在最小元。

19

令A_i={(i,0),(i,1)...} i>=0

A_i显然为可数集
NxN=$A_0 \bigcup A_1 \bigcup A_2 \ldots$
NxN是可数个可数集的并集。
NxN是可数集合。

Ch5

1(4)

是交换群，单位元为γ,$\alpha^{-1} = \delta, \beta^{-1} = \beta, \gamma^{-1} = \gamma, \delta^{-1} = \alpha$

1(6)

是交换群，单位元为1，求解$ax \equiv 1(modp)$可得a的逆元。

3

$\forall a, b \in G, a * b = b^2 * a * b * a^2 = b * (b * a)^2 * a = b * a$

6

1. 当 a*b 与 b*a 均为有限阶时，不妨设 a*b 的阶为 n，b*a 的阶为 m。
   $(\mathrm{b} * \mathrm{a})^{n+1} = b * (a * b)^n * a = \mathrm{b} * \mathrm{a}$
   $\therefore (b * a)^n = e$
   $\therefore$ m|n
   同理，n|m
   $\therefore$ m=n
2. 当 a*b 与 b*a 有一个为无限阶时，另一个定为无限阶。

反证：不妨假设：a*b 为无限阶，b*a 为有限阶，阶数为 k

由 1 中证明知，若 b*a 的阶为 k，则 a*b 的阶与之相等也为 k，这与 a*b 为无限阶矛盾。

Ps：1 中证$(b * a)^n = e$ 时亦可以：

$(b * a)^n = \mathrm{b} * (a * b)^{n-1} * a$

$= \mathrm{b} * (a * b)^{n-1} * a * b * b^{-1}$

$= \mathrm{b} * (a * b)^n * b^{-1}$

$= \mathrm{b} * \mathrm{e} * b^{-1}$

=e

典型错误：

证到$(b * a)^n = e$时即说明两者阶相等。

部分同学未考虑无限阶的情况。

7

a为2阶元,可得$\forall x \in G, x * a * x' * x * a * x' = e$则$x * a * x'$也为二阶元，或一阶元(显然不成立)。

由于二阶元唯一，所以$x * a * x' = a$

得$x * a = a * x$

9

充分性：

$\forall\ a,b\in H$， $a*b'\in H$

则

$a\in H\Rightarrow a*a'=e\in H$

$e,a\in H\Rightarrow e*a'=a'\in H$

$a,b\in H\Rightarrow a,b'\in H\Rightarrow a*(b')'=a*b\in H$

$\therefore <H,*>$ 是 $<G,*>$ 的子群。

必要性：

$<H,*>$ 是 $<G,*>$ 的子群

则

$\forall\ a,b\in H\Rightarrow a,b'\in H\Rightarrow a*b'\in H$ 。

10

证明：

(1)$\forall g\epsilon G, a*e=e*a, \therefore e\epsilon H, H\neq\emptyset$

(2)

$$\forall a,b\in H,\quad \begin{aligned}&(a*b)*g=a*(b*g)=a*(g*b)\\&=(a*g)*b=(g*a)*b=g*(a*b)\end{aligned},\quad \therefore a*b\in H$$ 。

(3)

$$\forall a\in H,\quad a*g=g*a\Rightarrow g'*a'=a'*g',\quad \therefore a'\in H$$

综上，<H,*>是<G,*>的子群。

典型错误：不说明 H 非空。

定义 5.5 中定义子群的概念的时候的前提就是 H 是 G 的非空子集。故在证明子群的时候，一定要说明 H 非空。即证明子群的三要素：1.非空 2.封闭 3.逆元存在。

11

证明：

$H \le G, K \le G$

$e \in H, e \in K \Rightarrow e \in H \cap K$

$a \in H \cap K \Rightarrow a \in H, a \in K \Rightarrow a' \in H, a' \in K \Rightarrow a' \in H \cap K$

$a, b \in H \cap K \Rightarrow a * b \in H, a * b \in K \Rightarrow a * b \in H \cap K$

$\therefore H \cap K$ 是 G 的子群。

$H \cup K$ 不一定是 G 的子群。

当 $H \subseteq K$ 或 $H \supseteq K$ 时，$H \cup K$ 为 K 或 H，是 G 的子群。

否则，不一定，例如取 a，b 使 $a \in H, a \notin K, b \notin H, b \in K$

不能确定 $a * b \in H \cup K$ 是否成立。

当然，遇到这种问题，我们可以举反例说明即可：

令$G = \{[0], [1], [2], [3], [4], [5]\}$(mod 6 的同余类), $< G, * >$ 为群，$*$ 为同余类加法

易知 H={[3]} k={[0],[2],[4]}

<H,*> <k,*> 为<G,*>的子群。

H ∪ K ={ [0],[2],[3],[4]}

而[2]*[3]不属于H ∪ K，即H ∪ K不满足封闭性，从而不是 G 的子群。

典型错误：

1. 不说明H ∩ K非空。
2. 证明H ∪ K 不是 G的子群时候举例如下：

   <G,*>为Z^+上的乘法群。

   令$H = \left\{1,2,\frac{1}{2}\right\}, K = \left\{1,3,\frac{1}{3}\right\}$

   然后说明 2*3=6 不属于H ∪ K。

   注意，这里的 H，K 根本就不是一个子群！因为他本身就不满足封闭性！

   2*2=4 并不属于 H！

15

$G = \{e, g^1, g^2, g^3, g^4, g^5\}$

G的生成元为g^1和g^5

G的子群为：一阶$< \{e\}, * >$,二阶$< \{e, g^3\}, * >$,三阶$< \{e, g^2, g^4\}, * >$,六阶$< G, * >$

17

由于g是n阶的，则$e, g^1, ..., g^{n-1}$是两两互不相同的元素，且均是群G的元素。由于G的阶数为n,则G不包含上述元素外的任意元素，综上，G是由g生成的循环群。

18

- 存在性

  设g为G的生成元，g^n=e,由于d为n的因子，a= $g^{\frac{n}{d}}$ 为G中的d阶元，由定理5.10，G存在一个由a=$g^{\frac{n}{d}}$生成的一个d阶循环子群H。

- 唯一性

  假设G中存在另一个d阶子群H'，生成元为b=g^r，则b^d=e,即g^{rd}=e,n|rd,可得$r = m * \frac{n}{d}$,则该循环群中的任意元素b^i=g^{ri}=$g^{m*i*n/d}$均为H中的元素。又H‘与H均为d阶子群，则H=H'。

HW 7

5.25

> 证明：无限循环群的子群，除{e}以外都是无限循环群

解：设$G=\langle a\rangle$是无限循环群，H是G的子群，因为循环群的子群还是循环群，若$H\neq\{e\}$,则$H=\langle a^m\rangle$,其中a^m为H中最小正方幂元。假如H是有限设$|H|=t$，则$|a^m|=t$,即$a^{mt}=e$。这与a为无限阶元矛盾。

> 注：循环群的子群还是循环群

5.26

> 在群$\langle G,*\rangle$中定义新的二元运算$\bullet$, $a\bullet b=b*a$。证明：$\langle G,\bullet\rangle$是群，并且$\langle G,*\rangle$与$\langle G,\bullet\rangle$同构

解：定义映射$f:G\to G, f(x)=x'$，注意此处的逆在*运算意义下，首先由于群逆元的存在唯一性，得知f是一个映射；另外对于$\forall a,b\in G$,若有$f(a)=f(b)\Leftrightarrow a'=b'$,则有$e=b'*a\Rightarrow b=a$，故知$f$是单射，另外对$\forall a\in G, f(a')=(a')'=a$，所以$f$是满射。综上$f$是双射。

进一步地，对$\forall a,b\in G$，有$f(a*b)=(a*b)'=b'*a'=a'\bullet b'=f(a)\bullet f(b)$，故$f$保持运算。

综上，由定理5.15，$\langle G,\bullet\rangle$是群，并且$\langle G,*\rangle$与$\langle G,\bullet\rangle$同构，同构映射是f。

> 利用定理5.15求解，主要是找到G到G的双射，并且保持运算，及同构映射。观察到$a\bullet b=b*a; a,b$位置交换，考虑逆运算

6.3

> 写出A_4中关于$H=\{e,(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$的左陪集分解和右陪集分解。

解：
$A_4=\{e,(123),(132),(124),(142),(134),(143),(234),(243),(12)(34),(13)(24),(14)(23)\}$共可以分解成$\frac{|A_4|}{|H|}=3$个陪集

左陪集分解：

$$\begin{aligned} eH=H&=\{e,(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}\\ (123)H&=\{(123),(134),(243),(142)\}\\ (132)H&=\{(132),(124),(143),(234)\}\end{aligned}$$

右陪集分解：

$$\begin{aligned} He=H&=\{e,(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}\\ H(123)&=\{(123),(134),(243),(142)\}\\ H(132)&=\{(132),(124),(143),(234)\}\end{aligned}$$

> 注：
>
> 1. 陪集的个数：拉格朗日定理，确定个数后尝试求出三个不同的陪集即可
> 2. 左陪集等于右陪集

6.4

> H是群G的指数为2的子群。证明：对于G的任何元素a必有$a^2\in H$，若H的指数为3，是否对G的任意元素a有$a^3\in H$?证明你的断言。

1. 若$a\in H$，由于H是子群，所以$a^2=a*a\in H$；

   若$a\notin H$,则$a'\notin H$,否则$a=(a')'\in H$,由于H的指数为2，所以a,a'都属于H的另一个右陪集，也即$a\equiv a'(mod\ H)$，也即$a*(a')'=a^2\in H$成立
2. 否。反例如下：

   $S_3=\{I,(123),(132),(12),(13),(23)\}$

   $H=\{I,(12)\}$

   $a=(13)$时$,a^3=(13)\notin H$

> 注：以a是否属于H分类讨论

6.5

> H,K是G的两个子群，$[G:H]=m,[G:K]=n,$证明子群$H\bigcap K$在G中的指数$\leq m\bullet n$

1. 法一

   考虑陪集交$Ha\bigcap Kb,$其中a,b任意，若他不为空，则对$\forall x\in Ha\bigcap Kb$有$Ha=Hx,Kb=Kx$成立(等价类性质)，所以$\forall y\in Ha\bigcap Kb=Hx\bigcap Kx,\exists h\in H,k\in K,y=h*x=k*x,$于是$h=k=y*x'$成立，所以$h=k\in H\bigcap K$成立,也即$y\in(H\bigcap K)x$。另一方面，对于$y\in(H\bigcap K)x$而言，有$z\in H\bigcap K,y=z*x$，于是显然$y\in Hx,y\in Kx$成立，也就是$y\in Ha,y\in Kb$，也就是$y\in Ha\bigcap Kb$。

   所以说存在映射g对于每一个非空的陪集交$Ha\bigcap Hb$，一定可以映射到一个子群$H\bigcap K$的陪集且g是满射(参见上面证明中的"另一方面"部分)，而非空的陪集交至多有mn个，所以子群$H\bigcap K$的陪集至多有mn个(此时$Ha\bigcap Hb$对任意a,b非空且映射g为单射)，于是有原命题成立。

2. 法二

本题有同学使用公式$|HK|=\frac{|H||K|}{|H\bigcap K|}$进行证明，这个公式书上并没有，考试也不能直接使用，这里给出一个简单证明：

$该公式要求H,K都是有限阶的,设|H|=n,|K|=m。HK=\{h*k|h\in H,k\in K\}=h_1K\bigcup h_2K\bigcup...\bigcup h_nK$，也就是说$HK$是$K$的若干陪集之交，那么现在考察$h_1K\bigcup h_2K\bigcup...\bigcup h_nK$中哪些项是相同的？

由6.2题的结论可得，
$h_iK=h_jK\Leftrightarrow h_i'*h_j\in K；又因为H是群，所以h_i'*h_j\in H成立。故h_i'*h_j\in H\bigcap K,也就是说h_i(H\bigcap K)=h_j(H\bigcap K)$，上面推导的每一步都是等价的，即$h_iK=h_jK\Leftrightarrow h_i(H\bigcap K)=h_j(H\bigcap K)$，而模
$H\bigcap K左不同余的元素在H中有[H:H\bigcap K]=\frac{|H|}{|H\bigcap K|}个，所以h_1K$
$\bigcup h_2K\bigcup...\bigcup h_nK中不同的陪集有\frac{|H|}{|H\bigcap K|}个,故|HK|=|h_1K\bigcup h_2K\bigcup...\bigcup h_nK|=\frac{|H||K|}{|H\bigcap K|}$

下面利用该公式证明题6.5

$由[G:H]=m,[G:K]=n得|G|/|H|=m,|G|/|K|=n,而[G:H\bigcap K]=\frac{|G|}{|H\bigcap K|},由如上证明的公式得[G:H\bigcap K]=\frac{|G|}{|H\bigcap K|}=\frac{|G||HK|}{|H||K|}$
$\frac{|G|^2}{|H||K|}=mn$

> 注：该公式要求H,K是有限的，但是题目并没有给出这样的条件，因此使用该公式证明是不完备的！

第8次作业答案

ch6

6.9

> 如果群G中含有一个某阶子群，那么该群必是正规子群。

对于任意$g \in G$考虑集合$g'Hg$，首先由封闭性，$g'Hg \subseteq G$成立，另外对任意$g'hg \in H$，有$g'h'g \in H$且$g'h'g * g'hg = g'hg * g'h'g = e$成立，所以$g'Hg$是子群，另外对于$h_1, h_2 \in H$，有$g'h_1g = g'h_2g \Rightarrow h_1 = h_2$，所以定义$f: H \to g'Hg$满足$f(h) = g'hg$，则$f$是双射（满射性显然），所以$|H| = |g'Hg|$，即$g'Hg$与$H$同阶，由于$H$唯一，得到$H = g'Hg$，于是对任意$g \in G, h \in H$有$g'hg \in g'Hg = H$，所以$H$是正规子群。

6.13

> 在$G = \{f | f : Z \to Z/(2)\}$ 上定义运算+.
>
> $$(f+g)(x) = f(x) + g(x).$$

> 证明：<G,+>是交换群，并且非零元素的阶为2.

对$\forall f, g \in G,$满足对$x \in Z, (f+g)(x) = f(x) + g(x) \in Z/(2),$有封闭性

对$\forall f, g, h \in G, (f + (g+h))(x) = f(x) + (g(x) + h(x)) = (f(x) + g(x)) + h(x)) = ((f+g)+h)(x),$满足结合律

存在单位元e，满足对任意$x \in Z, e(x) = [0],$有对任意$a \in G, e(x) + a(x) = a(x) + e(x)$

对$\forall f \in G$存在逆元为其本身，使得$(f+f)(x) = 2f(x) = [0] = e(x)$

同时又有$(f+g)(x) = f(x) + g(x) = g(x) + f(x) = (g+f)(x)$

所以$<G, +>$为交换群，由逆元的性质可知，非零元素的阶为2

> 注意：证明交换群之前先需要证明群

6.15

> 令$G = \{A | A \in (Q)_n, |A| \neq 0\}$, G对于矩阵乘法构成群. $f: G \to R^*, f(A) = |A|$.证明：f是从群G到非零实数乘群R^*的同态映射。求$f(G)$和$Ker f$。

由线性代数知识知：$\forall A, B \in G, |AB| = |A||B|,$即$\forall f(AB) = f(A)f(B),$故$f$为同态映射.

$$f(G) = \mathbb{Q}^*$$

$$Ker\ f = \{A \in G |\ |A| = 1\} = SL_n(\mathbb{Q})$$

注：$f(G)$指f的值域，以及不要像“$\{|A| \mid A \in (\mathbb{Q})_n, |A| \neq 0\}$”一样把值域的定义抄一遍，而是要计算出来。

6.17

> $G=<a>$ 是n阶循环群，$G^{'}=<b>$ 是m阶循环群，证明：
>
> $m|nk \leftrightarrow \exists\phi: G\to G^{'}$ 是同态映射并且$\phi(a)=b^k$.

"$\Leftarrow$"：
若$\exists\varphi: G\to G'$是同态映射且$\varphi(a)=b^k$,则

$$b^{nk}=(\varphi(a))^n=\varphi(a^n)=\varphi(e_G)=e_{G'}$$

而m为循环群$G'=\langle b\rangle$的阶,故$m|nk$
"$\Rightarrow$"：
若$m|nk$,则取$\varphi: G\to G', \varphi(a^i)=b^{ik}$, $i=0,1,...,n-1$,由于

$$\forall a^i,a^j\in G, \varphi(a^i*a^j)=\varphi(a^{i+j})=b^{(i+j)k}=b^{ik}*b^{jk}=\varphi(a^i)*\varphi(a^j)$$

故φ即为所求同态映射.

6.20

> 在群G中，a,b是G中的元素，称$a'*b'*a*b$为G的换位元。证明：
>
> (1)G中的所有有限个换位元乘积构成G'，G'是G的正规子群；
>
> (2)G/G'是交换群；
>
> (3)若N是G的正规子群并且G/N是交换群，那么G'是N的子群.

(1)由于有限个换位元乘积的乘积仍为有限个换位元的乘积,故G'关于G中运算具有封闭性，且$\forall \prod_{i=1}^{n}(a_i'*b_i'*a_i*b_i)\in G'$,有

$$(\prod_{i=1}^{n}(a_i'*b_i'*a_i*b_i))'=\prod_{j=n}^{1}(b_j'*a_j'*b_j*a_j)\in G'$$

故$G'\leq G$.

又由于$\forall g\in G, \prod_{i=1}^{n}(a_i'*b_i'*a_i*b_i)\in G'$,都有

$$g'*(\prod_{i=1}^{n}a_i'*b_i'*a_i*b_i)*g=\prod_{i=1}^{n}((g'*a_i*g)'*(g'*b_i*g)'*(g'*a_i*g)*(g'*b_i*g))\in G'$$

故$G'\lhd G$.
(2)即需证明$\forall g,h\in G, gG'\cdot hG'=hG'\cdot gG'$,即只需证明$g*h\in(h*g)G'$.事实上,由于$g'*h'*g*h\in G'$且$g*h=(h*g)*(g'*h'*g*h)$,上式成立.
(3)由于G'由换位元生成，只需证明符合条件的N包含G的所有的换位元：因为G/N为交换群，所以$\forall a,b\in G,(a*b)N=(b*a)N$,故$a'*b'*a*b=(b*a)'*(a*b)\in N$,证毕.

注：这题有些同学误以为(1)中的子集G'是换位元的集合(然后封闭性当然没法证了……)；以及老师上课强调过要证正规子群首先需要证明它是一个子群。

HW9 参考答案

Ch7

1(3)

非环，因为<R,`*`>中不含单位元e(无法保证a`*`e = |a|·e = a等式成立)。

2(4)

{[1],[5]}

3

证明：设<R,+>的生成元为r, 任取a，b$\in$R，

设a = r^m ， b = r^n

$$a\bullet b = r^m \bullet r^n = \underbrace{(r+r+\cdots\cdots+r)}_{m个r} \bullet \underbrace{(r+r+\qquad+r)}_{n个r} = mnr^2$$

$$b\bullet a = r^n \bullet r^m = \underbrace{(r+r+\cdots\cdots+r)}_{n个r} \bullet \underbrace{(r+r+\qquad+r)}_{m个r} = mnr^2$$

于是a•b =b• a,<R,+,•>是交换环， 得证！

5(3)

对于$\forall a_1,a_2,b_1,b_2\in\mathbb{Q}$，若$(a_1+b_1\sqrt{3})\cdot(a_2+b_2\sqrt{3})=0$，则有$a_1=a_2=b_1=b_2=0$，则没有零因子，是整环；

又对于$\forall a_1,a_2,b_1,b_2\in\mathbb{Q}$，若$(a_1+b_1\sqrt{3})\cdot(a_2+b_2\sqrt{3})=1$，则$a_2=\frac{a_1}{a_1^2-3b_1^2},b_2=\frac{b_1}{3b_1^2-a_1^2}$，又$a_1+b_1\sqrt{3}$是非零元素，则有$a_1^2\neq 3b_1^2$，则一定有$a_2,b_2\in\mathbb{Q}$，即环的所有非零元素都有逆元，是域。

7

证明：a*b 是零因子，且环是交换环,存在非零 c,d

所以由 c*(a*b)=0 且(a*b)*d=0

可以推出 a*(c*b)=0 且(b*d)*a=0。

反证，若 a 与 b 都不是零因子，则有 c*b 和 b*d 都不为零，则与上式 a*(c*b)=0 且(b*d)*a=0 矛盾。所以或者 b 是零因子。

证毕。