第一次作业 2.28 解答

1. 下面的集合 A 和集合 B 是否相等？

（3） $A = \{1,2,4\}, B = \{1,2,2,4\}$

解：根据集合相等的定义，A 中的元素都是 B 中的元素，而且 B 中的元素都是 A 中的元素，所以 A=B

【错误情况】这道题有些同学认为 B 不符合互异性，所以认为 B 不是一个集合。

2. 已知 $A \subseteq B, B \subset C$, 证明 $A \subset C$。

证明：由 $A \subseteq B$, 则 $\forall x \in A, x \in B$

而 B⊂C, 则 x∈C

同时，由于 $B \subset C, \exists c \in C, c \notin B$

所以，$c \notin A$, 则 $A \subset C$

【错误情况】不证明“真包含”，只证明包含就打止

3. 下面的等式是否成立？

（1） $\{0\} = \emptyset$ -> 不成立

（2） $\emptyset = 0$ -> 不成立

（3） $\{\emptyset\} = \emptyset$ -> 不成立

（4） $\emptyset = \{x | x \neq x\}$ ->成立

（5） $\emptyset = \{B | B \subseteq A \text{ 且 } |B| = 0\}$ ->不成立

（6） $\mathcal{P}(\emptyset) = \emptyset$ -> 不成立

4. 下列命题是否成立？

（1） 如果 $A \neq B, B \neq C$, 则 $A \neq C \rightarrow$ 不成立

（2） 如果 $\alpha \notin A, A \supseteq B$, 则 $\alpha \notin B \rightarrow$ 成立

（3） $|\mathcal{P}(A)| > 1$ 推出 $A \neq \emptyset \rightarrow$ 成立，因为 A 中必然有元素，否则 $|\mathcal{P}(A)| = 1$

6. 证明下列命题

（2） $A \subseteq C, B \subseteq C \Rightarrow (A \cup B) \subseteq C$

证明：对$\forall x \in (A \cup B), x \in A$ 或 $x \in B$

$\Rightarrow x \in C$

$\Rightarrow (A \cup B) \subseteq C$

7. 用归纳法定义如下集合

（1）十进制无符号整数，它应该包括 4, 167, 0012 等。

解：设上题所求集合为 E

1. （基础语句）令$D = \{0,1,2,3,4,5,6,7,8,9\}$，若 $x \in D$，则 $x \in E$。

2. （归纳语句）如果$x \in E, y \in E$，则 x 与 y 的连接 $xy \in E$。

3. （终结语句）一个数$\in E$，当且仅当它是有限次使用 1、2 得到的。

【错误情况】n+1，10x+a，等等做法不能得到前面有 0 的数

P41 3,7 上交作业参考答案

1 证明

(1)若 a|b ， a＞0，则 （a，b）＝ a ；

解法一：

$\because a \mid b$

$\therefore \exists k \in Z$，使得 b ＝ ka；

$\therefore$（a，b）＝（a，ka）＝ a（1，k）＝ a

得证

解法二：

$\because \quad a \mid b，\ a \mid a$

$\therefore \quad a$是 a和 b的公约数

由最大公约数定义知 a ≤ （a，b）

又 a ＞ 0

$\therefore (a,b) \leq |a| \leq a$(正数的因子最大为本身)

综上，（a，b）＝ a，得证。

(2)（（a，b），b）＝（a，b）

解法很多，一是利用前一问结论

解法一：

易知（a，b）＞ 0，且（a，b）|b

所以由(1)知，（（a，b），b）＝（a，b）

得证

二是利用 将 b 用（a，b）表示

证明：

令（a, b）= c,

易知（a, b）|b, 所以b = kc，$k\in Z$

$\therefore$((a, b), b) = (c, kc)

= c(1, k)=c=(a, b) 得证！

2 （1）证明对所有的 n > 0，有 （n， n+1）= 1 成立。

解法也很多，最简单最经典的有辗转相除求最大公约数法。

解法一：

证明：

n+1 = n * 1 + 1;

n = 1 * n

$\therefore$ (n+1, n) = 1(其中a=n+1, b=n, q_0=1, r_0=1, q_1=n)

得证！

以及利用 mx + ny 集合

解二：

证明：

(n, n+1) 是

集合 $S = \{nx+(n+1)y \mid x, y \in Z\}$ 中的最小正整数

令 $x = -1$, $y = 1$

则 $nx+(n+1)y=1$

$\therefore (n, n+1) \le 1$

又易知 $(n, n+1) > 0$

$\therefore (n, n+1) = 1$ 得证！

3 求得 x 和 y 使得 $314x + 159y = 1$

此题，按理应是求整数 x，y，但未说明，所以非整数 x，y 的也没算错。求整数 x，y 可用辗转相除法

解： $\because (314,159)|1 \therefore$ 方程有解

由辗转相除法可求：

314 = 159 ＊ 1 + 155

159 = 155 ＊ 1 + 4

155 = 4 ＊ 38 + 3

4 = 3 ＊ 1 + 1

3 = 1 ＊ 3

反推，有

1 = 4 － 3 ＊ 1 = 4 － （155 － 4 ＊ 38）＊ 1

= 4 ＊ 39 － 155 = （159 － 155 ＊ 1）＊ 39 － 155

= 159 ＊ 39 −155 ＊ 40

= 159 ＊ 39 － （314 － 159 ＊1）＊ 40

= 159 ＊ 79 － 314 ＊ 40

∴ x = −40 ， y = 79

部分同学 前面算对了，但是，最后 x 和 y 的值写成 x = 79 y = -40，还有部分同学干脆算错了。

5 证明：若对于某个 m 有 10|（3^m+1），则对所有的 n ＞ 0 ，有 10 |（3^{m+4*n} + 1）

证明，大概分为两种思路

一是利用二次展开式

解：

$3^{m+4*n}+1=3^{m}*3^{4*n}+1$

$=(3^{m}+1)*3^{4*n}-3^{4*n}+1$

$=(3^{m}+1)*3^{4*n}-9^{2*n}+1$

$=(3^{m}+1)*3^{4*n}-(10-1)^{2*n}+1$

$=(3^{m}+1)*3^{4*n}-\sum_{i=0}^{2*n}10^{i}*(-1)^{2*n-i}*C(2*n,i)+1$

（二项式展开所得， C (n, m)表示组合数）

$=(3^{m}+1)*3^{4*n}-\sum_{i=1}^{2*n}10^{i}*(-1)^{2*n-i}*C(2*n,i)-1+1$

$=(3^{m}+1)*3^{4*n}-\sum_{i=1}^{2*n}10^{i}*(-1)^{2*n-i}*C(2*n,i)$

由题意知$10\mid(3^{m}+1),\therefore 10\mid(3^{m}+1)*3^{4*n}$

且易知减号后部$10\mid\sum_{i=1}^{2*n}10^{i}*(-1)^{2*n-i}*C(2*n,i)$

$\therefore 10\mid(3^{m+4*n}+1)$ ，得证。

二是利用同余式求

解：

$\because 3^4 \equiv 1(\bmod 10)$ （1）

$\therefore 3^{4*n} \equiv 1(\bmod 10)$（性质4, n个（1）式相乘） （2）

$\because 10 \mid (3^m + 1)$

$\therefore 3^m \equiv (-1)(\bmod 10)$ （3）

$\therefore 3^{m+4*n} \equiv (-1)(\bmod 10)$（性质4,（2）式和（3）式相乘）

$\therefore 10 \mid (3^{m+4*n} + 1)$，得证。

同学犯得典型错误是

由$3^{4n} \equiv 1(\bmod 10)$直接代替

推出$3^{m+4*n} + 1 \equiv 3^m * 3^{4n} + 1 \equiv 3^m * 1 + 1 \equiv 0(\bmod 10)$

另外，还可以讨论尾数以及用数学归纳法证明，不作详细解答。

8 令 $n = 5! + 1$,证明 $n + 1, n + 2, n + 3, n + 4$ 均为合数。

解：

此题显而易见, 可直接求出他的非本身和非1因子

另外还可如下证明

$\because n = 5! + 1 = 5*4*3*2*1 + 1$

$\therefore 2 \mid n+1，\ 2 \mid n+3，\ 3 \mid n+2，\ 5 \mid n+4$

$\therefore n+1, n+2, n+3, n+4$都存在非本身和非1因子，是合数。

9 求解方程组的所有整数解

（2）$2*x + y = 2$

解：

∵（2，1）=1，1|2∴方程有解

观察得知 $x=1$，$y=0$是他的一组特解

∴由定理2.6知通解为

$$\begin{cases} x = 1 + t \\ y = -2t \end{cases}, \quad t \in Z$$

部分同学算错了。

10 若$k \equiv 1 \pmod 4$，问$6*k+5$模4同余几

解：题目问同余几，有部分同学就是求出一个特定的数值，还有另外一部分同学是求出一个表达式，两种都正确，下面给出第二种解法

∵ $k \equiv 1 \pmod 4$ ∴ $k = 4*m+1$ $(m \in Z)$

设$6*k+5$模4同余r，

则$6*k+5 = 4*n + r$（$n \in Z$）

∴ $6*(4*m+1)+5 = 4*n + r$

∴ $r = 4*(6*m - n + 2) +3$

∴$r = 4*t + 3$ $(t \in Z)$

代数结构第三次习题答案

高玲玲 llinggao@mail.ustc.edu.cn

14.证明：每个大于3的素数模6同余1或同余5.

(法一)证明：(1)首先，任何大于3的素数必为奇数,而奇数模6余数只能为1，3，5.

(2)其次，假设素数y＝6x＋3（余数为3）即y＝3（2x＋1）这表明y有约数为3，所以y不可能是素数。

得证。

(法二)证明：由于任一大于3的素数均与6互素，故这些素数属于与6互素的同于类，而与6互素的同余类只有A1，A5，故这些素数模6或同余1或同余5.

得证。

当然，也可以像有些同学那样，对于模6同余0到5，逐个分析讨论，得出只能同余1或5。甚至有些同学还举例7、5这两个素数同余1或5，证明了存在性，很好。

18(2).解同余方程：$3x\equiv 6 \pmod{18}$

解：∵$(3,18)=3$且$3\mid 6$,由定理2.8知该同余方程由3个模18不同余的解。

∴该方程有通解$x=x_0+6t \pmod{18}$，其中$0\leqq t\leqq 2$,

x_0 是同余方程$x\equiv 2 \pmod 6$的特解，易知 $x_0=2$，

该同余方程的解为 $x=2$，$8,14 \pmod{18}$.

典型错误：$3x\equiv 6 \pmod{18}$ 等价于 $x\equiv 2 \pmod 6$

$x = 2$ 即为方程的解。

部分同学在给出 $x=2+6t \pmod{18}$，其中 $0\leqq t\leqq 2$。就打住。

19(3).求解同余方程组：

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 1 \pmod 3 \\ x \equiv 6 \pmod 7 \end{cases}$$

解：令$M=2\cdot 3\cdot 7=42$，$M_1=21, M_2=14, M_3=6$

$21b_1\equiv 1 \pmod 2$

$14b_2\equiv 1 \pmod 3$

$6b_3\equiv 1 \pmod 7$

解得：$b_1=1$，$b_2=2$，$b_3=6$

∴$x=21\cdot 1\cdot 1+14\cdot 2\cdot 1+6\cdot 6\cdot 6=265\equiv 13 \pmod{42}$ 是方程组的解

19（4）解下列同余方程组

$$\begin{cases} 2x \equiv 1 \pmod 5 \\ 3x \equiv 2 \pmod 7 \\ 4x \equiv 1 \pmod{11} \end{cases}$$

解：
由(2,5)=1 可知：2x≡1≡6（mod5）等价于x≡3（mod 5）。
由(3,7)=1 可知：3x≡2≡9（mod7）等价于x≡3（mod 7）。
由(4,11)=1 可知：4x≡1≡12（mod11）等价于x≡3（mod 11）。
令M=5 • 7 • 11=385，M1=77，M2=55,M3=35
11b1≡1（mod 5）
55b2≡1（mod 7）
35b3≡1（mod 11）
b1=3，b2=6，b3=6
∴x=77 • 3 • 3+55 • 6 • 3+35 • 6 • 3=2313≡3 (mod 385) 是方程组的解

典型错误： 这两道题一定要注意，x=$\Sigma M_j b_j a_j$，有些同学带错a_j的值。红色标记的才是a_j。

22: 计算$\phi(42),\phi(420),\phi(4200)$.
解：

$$42 = 2\times 3\times 7$$
$$420 = 2^2\times 3\times 5\times 7$$
$$4200 = 2^3\times 3\times 5^2\times 7$$
$$\phi(42) = 42\times(1-1/2)(1-1/3)(1-1/7) = 12$$
$$\phi(420) = 420\times(1-1/2)(1-1/3)(1-1/5)(1-1/7) = 96$$
$$\phi(4200) = 4200\times(1-1/2)(1-1/3)(1-1/5)(1-1/7) = 960$$

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

解：设$m = p_1^{l_1}p_2^{l_2}\dots p_k^{l_k}p^{l_0}, n = q_1^{t_1}q_2^{t_2}\dots q_n^{t_n}p^{t_0}$

因为(m,n)=p;故 l_0, t_0 中一个为1.另一个大于等于1.且$p_1 \dots p_k$ $q_1 \dots q_n$ p 两两互素。

$$\phi(mn) = mn\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_k}\right)\left(1-\frac{1}{q_1}\right)\dots\left(1-\frac{1}{q_n}\right)\left(1-\frac{1}{p}\right)$$

$$\phi(m) = m\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_k}\right)\left(1-\frac{1}{p}\right)$$

$$\phi(n) = n\left(1-\frac{1}{q_1}\right)\dots\left(1-\frac{1}{q_n}\right)\left(1-\frac{1}{p}\right)$$

故，$\phi(mn)\left(1-\frac{1}{p}\right) = \phi(m)\phi(n)$

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

简单点：
解：因为(m,n)=p,不妨设$m = m'p^k, n = n'p$,k≥ 1； 且m' n' p 两两互素
从而$\phi(mn) = \phi(m'n'p^{k+1}) = \phi(m')\phi(n')\phi(p^{k+1}) = \phi(m')\phi(n')p^k(p-1)$
$\phi(m) = \phi(m')\phi(p^k) = \phi(m')p^{k-1}(p-1)$
$\phi(n) = \phi(n')\phi(p) = \phi(m')(p-1)$

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

典型错误： m=xp,n=yp

$\phi(mn) = \phi(xyp^2) = \phi(x)\phi(y)\phi(p^2) = \phi(x)\phi(y)p(p-1)$

$\phi(m) = \phi(xp) = \phi(x)\phi(p) = \phi(x)(p-1)$

$\phi(n) = \phi(yp) = \phi(y)\phi(p) = \phi(y)(p-1)$

$\phi(mn) = \dfrac{p}{p-1}\,\phi(m)\phi(n)$

虽然也得出了正确结论，但是这是非常错误的。因为我们用 $\phi(mn) = \phi(m)\phi(n)$这个公式的前提是m n互素。以上解法不能保证x y p三者之间互素，所以这样做很不正确。虽然有些同学和这不完全相同，但本质是相同。我们可以举个最简单的例子，m=p ,n=p^2 代入下，看看自己每一步有问题否。

26.（1） 验证略。

（2） $\frac{n}{2}\phi(n)$等于所有不超过n且与n互素的正整数的和，其中n≥3且n∈Z

或：$\frac{n}{2}\phi(n)$等于n的缩系中所有元素之和

（3） 若（d,n）=1,则（n-d,n）=1;

故不超过n且与n互素的数总是成对出现，且其和为n；共$\frac{1}{2}\phi(n)$对。

故所有不超过n且与n互素的正整数的和为$\frac{n}{2}\phi(n)$

典型错误： 有些同学没有认真读题，未能观察出各等式左边到底是哪些数，误以为若n为奇数，则是1~n-1，n为偶数，就是小于自己的奇数和。其实不然，注意等式1+5=$\frac{6}{2}\phi(6)$，这里不是1+3+5，而是1+5.从而得出错误结论。

小窍门：以后做题之前思考下自己这章学习了什么内容，为何出此题。奇数偶数问题恐怕不是这章的学习重点。所以以后就不会犯这种错误了。当然，一定要注意审题，细心读题。

29. p为素数，证明：对非负整数k，$(k+1)^p - k^p \equiv 1(\mathrm{mod}\ p)$,并由此推出费尔马定理。

证明：$(k+1)^p - k^p - 1 = \sum_{m=1}^{p-1} C_p^m\, k^{p-m}$

$C_p^m = \frac{P(p-1)\ldots(p-m+1)}{m!}$,即m! | p(p-1)….(p-m+1)，$(1\leq m < p)$

而p为素数，故（m!,p）=1,又因C_p^m为整数，故m! | (p-1)….(p-m+1)得证p | C_p^m $(1\leq m < p)$

所以$(k+1)^p - k^p \equiv 1(\mathrm{mod}\ p)$。

从以上证明过程来看，k可以为任意整数，而不一定要求是非负整数。

下面证费尔马定理：

$\because (k+1)^p - k^p \equiv 1(\mathrm{mod}\ p)$

$k^p - (k-1)^p \equiv 1(\mathrm{mod}\ p)$

…………

$2^p - 1^p \equiv 1(\text{mod p})$

$1^p - 0^p \equiv 1(\text{mod p})$

以上各式相加后，得出：$(\text{k} + 1)^p \equiv \text{k} + 1(\text{mod p})$

即：$a^{p-1} \equiv 1(\text{mod p})$ p为素数。

因此，当（a,p）=1时，即p不能整除a时，得$a^{p-1} \equiv 1(\text{mod p})$.得证。

当然有些同学通过数学归纳法给出了证明。

典型解法：

对于任意a，都有：$a^p \equiv \text{a}(\text{mod p})$，其中p为素数。

从而：$(k+1)^p \equiv \text{k} + 1(\text{mod p})$

$k^p \equiv \text{k}(\text{mod p})$，

从而：$(k+1)^p - k^p \equiv 1(\text{mod p})$ 轻松得证。个人觉得这样做并不妥，因为如果既然已知$a^p \equiv \text{a}(\text{mod p})$何必要再证明一个结论，再用这个结论去证明费马定理。所以，个人觉得出题的出发点不在此。

当然，有些同学通过分情况讨论，当(k+1,p)=1,且（k,p）=1时运用欧拉定理，当p|k 或者p|k+1 再做处理，这样更加复杂。虽然都正确，个人觉得这样处理不是很妥。

典型错误：

从$a^p \equiv \text{a}(\text{mod p})$往$a^{p-1} \equiv 1(\text{mod p})$推的时候，很多同学并没有注明：是在当（a,p）=1时，即p不能整除a时，得出结论。注意费尔马定理的条件！

代数结构第四次作业解答（3.21）

Edit by 伍浩铖（James Wu）　有错误请联系 ustcwhc@mail.ustc.edu.cn

第二章 35 题 若 n 为偶完全数，n>6，证明$\mathbf{n \equiv 1 (mod\ 9)}$

证明：根据定理 2.15，可知，对于偶完全数 n，必有形式

$n = 2^{p-1}(2^p - 1)$

其中 p 和$2^p - 1$都是素数

由于 n>6，则$p \geq 3$

由于 p 是素数，则分三种情况讨论

① P = 3

则$n = 2^2(2^3 - 1) = 28 \equiv 1\ (\mathrm{mod}\ 9)$

② p = 3k + 1，其中 k 是偶数

则$n = 2^{3k}\left(2^{3k+1} - 1\right) = 8^k\left(2 * 8^k - 1\right) \equiv (-1)^k[2 * (-1)^k - 1]$

由于 k 是偶数

则$n \equiv 1 * (2 * 1 - 1) = 1\ (\mathrm{mod}\ 9)$

③ p = 3k + 2，其中 k 是奇数

则$n = 2^{3k+1}\left(2^{3k+2} - 1\right) = 2 * 8^k\left(4 * 8^k - 1\right) \equiv 2 * (-1)^k[4 * (-1)^k - 1] = 8 - 2 * (-1)^k$

由于 k 是奇数

则$n \equiv 8 + 2 \equiv 1\ (\mathrm{mod}\ 9)$

综上可知不论 p 取什么样的素数（$\mathrm{p} \geq 3$），皆有$\mathbf{n \equiv 1 (mod\ 9)}$

【错误情况】很多人考虑 p=6k+1, p=6k+5，却忘记了 p=3 的情况

第二章 38 题

（1）算出关于原根 2 的最小指数表(mod 29)

（2）利用此表解$\mathbf{9x \equiv 2\ (mod\ 29)}$

（3）利用此表解$\boldsymbol{x^9 \equiv 2\ (\mathrm{mod}\ 29)}$

解：(1)既然已经被告知 2 是原根，所以根 2 的指数表这么计算：

如下表：

	29
1	0
2	1
…	…
n	k

对于指数表中的第一列中的数 n，其在指数表中对应的数 k 是满足下面关系式的最小整数：

$2^k \equiv n\ (mod\ 29)$

计算满足下面关系式的最小整数k_n

$2^{k_1} \equiv 1\ (mod\ 29)$,

$2^{k_2} \equiv 2\ (mod\ 29)$,

$2^{k_3} \equiv 3\ (mod\ 29)$,

$2^{k_4} \equiv 4\ (mod\ 29)$,

$2^{k_5} \equiv 5\ (mod\ 29)$,

$2^{k_6} \equiv 6\ (mod\ 29)$,

$2^{k_7} \equiv 7\ (mod\ 29)$,

$2^{k_8} \equiv 8\ (mod\ 29)$,

$2^{k_9} \equiv 9\ (mod\ 29)$,

$2^{k_{10}} \equiv 10\ (mod\ 29)$,

$2^{k_{11}} \equiv 11\ (mod\ 29)$,

$2^{k_{12}} \equiv 12\ (mod\ 29)$,

$2^{k_{13}} \equiv 13\ (mod\ 29)$,

$2^{k_{14}} \equiv 14\ (mod\ 29)$,

$2^{k_{15}} \equiv 15\ (mod\ 29)$,

$2^{k_{16}} \equiv 16\ (mod\ 29)$,

$2^{k_{17}} \equiv 17\ (mod\ 29)$,

$2^{k_{18}} \equiv 18\ (mod\ 29)$,

$2^{k_{19}} \equiv 19\ (mod\ 29)$,

$2^{k_{20}} \equiv 20\ (mod\ 29)$,

$2^{k_{21}} \equiv 21\ (mod\ 29)$,

$2^{k_{22}} \equiv 22\ (mod\ 29)$,

$2^{k_{23}} \equiv 23\ (mod\ 29)$,

$2^{k_{24}} \equiv 24\ (mod\ 29)$,

$2^{k_{25}} \equiv 25\ (mod\ 29)$,

$2^{k_{26}} \equiv 26\ (mod\ 29)$,

$2^{k_{27}} \equiv 27\ (mod\ 29)$,

$2^{k_{28}} \equiv 28\ (mod\ 29)$,

可以分别计算2^0至$2^{29-2} = 2^{27}$，然后模 29，对号入座看其余数是多少，作好记录

k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}
0	1	5	2	22	6	12	3	10	23
k_{11}	k_{12}	k_{13}	k_{14}	k_{15}	k_{16}	k_{17}	k_{18}	k_{19}	k_{20}
25	7	18	13	27	4	21	11	9	24
k_{21}	k_{22}	k_{23}	k_{24}	k_{25}	k_{26}	k_{27}	k_{28}		
17	26	20	8	16	19	15	14		

（2）看书上的例题 2

由$9x \equiv 2\ (\mathrm{mod}\ 29)$，以及 29 的最小原根为 2，知

$ind_2 9 + ind_2 x = ind_2 2\ (mod\ 28)$

查询$ind_2 9 = k_9 = 10$，$ind_2 2 = k_2 = 1$，代入上式得到$ind_2 x = -9 \equiv 19 \pmod{28}$
再查表得$k_{26} = 19$，则
$x \equiv 19 \pmod{29}$

（3）看书上的例题 1
根据同余式$x^9 \equiv 2 \pmod{29}$，以及 29 的最小原根为 2，知
$9 * ind_2 x = ind_2 2\ (mod\ 28)$
查询$ind_2 2 = k_2 = 1$，代入上式得到$9 * ind_2 x = 1 \pmod{28}$
$9 * ind_2 x \equiv 1 + 28 * 8 = 225 \pmod{28}$
此同余方程有一个解
$ind_2 x = 25 \pmod{28}$
查表得$k_{11} = 25$
则$x \equiv 11 \pmod{29}$
【错误情况】很多人直接列出了表，不知道是真会了还是照抄书上的表，我还是给判的对的
【错误情况】$ind_2 x = 25 \pmod{28}$，直接得到$x \equiv 25 \pmod{29}$

第二章 10 题

求 37 的 12 个原根

解：
① **首先说明为什么会有 12 个原根。**
$\because \phi(37) = 36$

$\therefore$ 作为 37 的原根，必须阶 $= 36$

根据定理 2.10，p 为素数，$m \mid (p-1)$，那么模 p 阶为m的数恰好有$\phi(m)$个
取 m=36，所以 37 的原根个数$= \phi(36) = \phi(2^2)\phi(3^2) = 2(2-1) * 3(3-1)$

② **再计算这 12 个原根**
因为$(2,37) = 1$，所以首先看 2 是否是一个原根

因为$2^{36} \equiv 1\ (mod\ 37)$，根据阶的性质，知 2 的阶必然是 36 的因子

36 的因子 $= 1,2,3,4,6,9,12,18,36$

经计算：
$2^1 \equiv 2 \pmod{37}, 2^2 \equiv 4 \pmod{37}, 2^3 \equiv 8 \pmod{37}, 2^4 \equiv 16 \pmod{37}$
$2^6 \equiv 27 \pmod{37}, 2^9 \equiv 31 \pmod{37}, 2^{12} \equiv 26 \pmod{37}, 2^{18} \equiv 36 \pmod{37}$

所以只有$2^{36} \equiv 1\ (mod\ 37)$，则 2 是 37 的原根

则$\{2^0，2^1，2^2，\dots，2^{\phi(37)-1}\}$构成了模 37 的缩系。也就是说，若 2 是 37 的原根，

每个与 m 互素的 a 均与且仅与某个2^i模 m 同余，其中$0 \le i \le \phi(37) - 1$。这表示模

m 的原根都在$\{2^0，2^1，2^2，…，2^{\phi(37)-1}\}$中。

根据推论 2.7：若$(a,m)=1$，s 为 a 模 m 的阶，则a^i模m的阶为$\frac{s}{(s,i)}$。

这里取 a=2，m=37，$s=\phi(37)=36$，要使2^i也是 37 的阶，则 i 需要与$s=36$互素，使得$\frac{s}{(s,i)}=\frac{36}{(36,i)}=36$，其中$0\le i\le\phi(37)-1$

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

经计算：

$2^1\equiv 2\ (mod\ 37), 2^5\equiv 32\ (mod\ 37), 2^7\equiv 17\ (mod\ 37), 2^{11}\equiv 13\ (mod\ 37),$
$2^{13}\equiv 15\ (mod\ 37), 2^{17}\equiv 18\ (mod\ 37), 2^{19}\equiv 35\ (mod\ 37), 2^{23}\equiv 5\ (mod\ 37),$
$2^{25}\equiv 20\ (mod\ 37), 2^{29}\equiv 24\ (mod\ 37), 2^{31}\equiv 22\ (mod\ 37), 2^{35}\equiv 19\ (mod\ 37)$

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

第二章 41 题

证明：若 p，q 为奇素数，$q|(a^p+1)$，则有$q|(a+1)$或$q|(2kp+1)$，其中 K 为某个整数

证明：

$q|(a^p+1)\Rightarrow a^p\equiv -1\ (mod\ q)\Rightarrow -a^p\equiv 1\ (mod\ q)\Rightarrow (-a)^p\equiv 1\ (mod\ p)$

设$(-a)$模 q 的阶为 d，则$d|p$，则$d=1$ 或 $d=p$.

① 若$d=1$

则$-a\equiv 1\ (mod\ q)\Rightarrow a+1\equiv 0\ (mod\ q)\Rightarrow q|(a+1)$

② 若$d=p$

$\because (-a)^p\equiv 1\ (mod\ p)$

$\therefore p|\phi(q)$

$\therefore p|(q-1)$

因为 p 为奇，$(q-1)$为偶

$\therefore 2p|(q-1)$

$\therefore q-1=2kp$，k 为某个整数

$\therefore q=2kp+1$，蕴含了 $q|(2kp+1)$，证毕

第二章 42 题

证明：若 a 模 p 的阶为 3，则 a+1 模 p 的阶为 6。（这里默认有条

件：素数 p）

证明：6 的正因子为 1,2,3,6

所以只需要证明四个结论：

$(\mathrm{a}+1) \not\equiv 1(\bmod \mathrm{p})$

$(\mathrm{a}+1)^2 \not\equiv 1(\bmod \mathrm{p})$

$(\mathrm{a}+1)^3 \not\equiv 1(\bmod \mathrm{p})$

$(\mathrm{a}+1)^6 \equiv 1(\bmod \mathrm{p})$

由题可知：

$\because (\mathrm{a},\mathrm{p})=1$

$\therefore (\mathrm{a}+1) \not\equiv 1(\bmod \mathrm{p})$

由$a^3 \equiv 1\ (mod\ p)$，且 $\mathrm{a} \not\equiv 1\ (\bmod \mathrm{p})$，$a^2 \not\equiv 1\ (mod\ p)$

$\therefore\ a^3-1=(a-1)(a^2+a+1) \equiv 0\ (mod\ p)$

$\because \mathrm{p} \nmid (\mathrm{a}-1)$且 p 为素数

$\therefore \mathrm{p}|(a^2+\mathrm{a}+1)$

$\therefore (\mathrm{a}+1)^2=a^2+a+1 \equiv a \not\equiv 1\ (mod\ p)$

$\therefore\ (a+1)^3 \equiv a(a+1) \equiv -a^3 \equiv -1 \not\equiv 1\ (mod\ p)$

$\therefore (a+1)^6 \equiv 1\ (mod\ p)$

证毕

【错误情况】很多人不考虑证明$(a+1)^i \not\equiv 1\ (mod\ p), \mathrm{i}=1,2,3$

代数结构第五次作业解答 （3.28）

Edit by 贺国超 有错误请联系 hgc@mail.ustc.edu.cn

第三章 第 3 题

（3） f(n)是双射函数 g(n)也是双射函数

（5） 都不是。

举反例。易知 $f(j) = j^2+2j-15 = (j+1)^2 -16 >= -16$ 所以小于-16 的数没有对应的原象，不是满射。 另外对于 0 ，它对应于两个原象 3 和 5，所以不是单射。所以也不是双射。

典型错误：部分同学推出是单射和满射，还有部分同学说不是映射，都是对映射定义不清晰的原因。另外很多同学把第二问的 R-》R 写成了 N-》N。

第三章 第 6 题

证明：

方法同例4，先证满射。

任取S(B)的一个元素s=$(bi_1,bi_2,\ldots,bi_n)$ $bi_j \in$ B,$1 \le j \le n$。因为F是A到B的映射全体，那么F中一定会存在一个映射f, 使得$f(a_j)=bi_j$，即

$s=(f(a_1),f(a_2),\ldots,f(a_n))=g(f)$

也就是说f是s的原象，由任意性知，g是满射。

再证单射。

设f_1，f_2都是s=$(bi_1, bi_2,\ldots, bi_n)$的原象。那么，我们可以知道$f_1(a_j)=bi_j$

$=f_2(a_j)$ $1\le j \le n$，即对于任意的$a_j \in$ A，有$f_1(a_j)=f_2(a_j)$，由映射相等的定义知$f_1=f_2$，也就是说对于$S(B)$中的任意一个元素s只有一个原象, 即g是单射。

综上得知, g是从F到$S(B)$的双射。

由组合排列的知识，我们很容易知道集合B的元素构成的全体有序n数组的个数是m^n，即$|S(B)|=m^n$.由定理3.4知, 形成双射的两个有限集合的元素个数相等，所以$|F|=|S(B)|=m^n$。

得证。

典型错误：部分同学的证明太简单，直接给出结论。

第三章 第 7 题

证明：

（1）证两集合A，B相等一般的方法：任取元素a在A中，证明a也在B中，然后再任取元素b在B中，证明b也在A中。

令M ＝ $a(A\cup B)$ ， N = $a(A)\cup a(B)$ 。

任取$x\in$M，则一定存在一个原象$s\in A\cup B$，使得$x=a(s)$，由$s\in A\cup B$知$s\in A$或者$s\in B$ 。由此可继续推得$a(s)\in a(A)$ 或者$a(s)\in a(B)$ ，必有$a(s)\in a(A)\cup a(B)$ ，即$x\in$N 。

同理，任取 $y\in$N，即 $y\in a(A)\cup a(B)$ ，所以 $y\in a(A)$ 或者 $y\in a(B)$ ，则一定存在一个原象$s\in A$或者 $s\in B$，使得 $y=a(s)$，由$s\in A$或者 $s\in B$知$s\in A\cup B$，必有$a(s)\in a(A\cup B)$，即 $y\in$M

综上所述M＝N，得证。

（2）证集合A$\subseteq$B的一般方法：任取元素a在A中，证明a也在B中即可。

令M ＝ $a(A\cup B)$ ， N = $a(A)\cup a(B)$

任取$x\in$M，则一定存在一个原象$s\in A\cap B$，使得$x=a(s)$，由$s\in A\cap B$知$s\in A$且$s\in B$ 。由此可继续推得$a(s)\in a(A)$ 且$a(s)\in a(B)$ ，必有$a(s)\in a(A)\cap a(s)$，即 $x\in$N 。

由任意性知，M$\subseteq$N，得证。

反例：S＝{-1, 0, 1}，$a(s)$ ＝ s^2。取A={-1，0}，B={1，0}，知$a(A\cap B)$ ={0}$\neq$\{0,1\}$=a(A)\cap a(s)$.

错误情况：部分同学直接用的其他说明方法，欠详尽的过程和严谨。

第三章 第 9 题

因为 f，g，h 都是从 Z 到 Z 的映射，所以可以直接求得

$f\circ g=f\circ g(x)=f(3x+1)$ =9x+3，同理可求

$g\circ f$ =9x+1

$g\circ h$ =9x+7

$h\circ g$ =9x+5

$f\circ g\circ h$ =27+21

第三章 第 11 题

令$f(n)=\begin{cases} n/2, & \text{n 为偶} \\ (n+1)/2, & \text{n 为奇,} \end{cases}$ g (n)= 2n

$\therefore f\circ g(n)=f(2\text{n})=n \quad \therefore f\circ g=I_s$

$\therefore \text{g}\circ f(n)=\begin{cases} n & \text{n 为偶} \\ n+1 & \text{n 为奇} \end{cases} \therefore g\circ f\neq I_s$

若f是双射，由定理3.2知 f^{-1}也是双射，则$f\circ f^{-1}=I_s$.假设存在不同的映射g也满足$f\circ g=I_s$.$\therefore$对于任意n，有 $f\circ f^{-1}(\text{n})=f\circ g(n)=n$,

$\therefore$ 对于任意n，$f(f^{-1}(\text{n}))=f(g(n))$。

$\because$ f是双射，每个象都有唯一的原象

$\therefore$对于任意n，$f^{-1}(\text{n})=g(n)$。 $\therefore f^{-1}=g$

$\therefore$满足$f\circ g=I_s$的映射有且只有一个f^{-1}。

有结论$f\circ g=I_s$且$g\circ f=I_s$

错误情况:

没有对 f^{-1}有是唯一满足的 g 进行说明。

第三章 第 14 题 （2）

根据定义，易求:

$\begin{pmatrix} 12345678 \\ 36418257 \end{pmatrix}=(134)(26)(587)$

第三章 第 16 题

证明：

对于任意n元置换$\sigma=\begin{pmatrix}1 & 2 & 3\dots n\\ a_1 a_2 a_3\dots a_n\end{pmatrix}$，我们可以使用如何方法从$\sigma_1$构造：

考虑第一个位置，σ_I与对换$(1\ \ a_1)$相乘得到$\sigma_1=(1\ \ a_1)\sigma_I=\begin{pmatrix}1 & 23\dots a_1\dots n\\ a_1 & 23\dots 1\dots a_n\end{pmatrix}$，

σ_1的第一个位置与σ相等。同理，可以用$(2\ a_2)$与σ_1相乘得到σ_2，σ_2的第一个和第二个位置都与σ相等。继续使用$(3\ \ a_3)(4\ \ a_4)$　σ_i与　相乘，直到最后得到σ。而我们知道,$(i，a_i)$可以表示成对换$(i\,i+1)(i+1\,i+2)\cdots(a_{i-1}\ \ a_i)$的乘积。所以，$\sigma$可以表示成若干个形如$(i\,i+1)$对换的乘积。

得证。

很多同学用的归纳法，但是归纳假设过程比较不清晰。

第三章 第 18 题 （2）

证明： $\because f+g=g$

$\therefore \bar{f}+g=\bar{f}+f+g$

$\because \bar{f}+f=1$

$\therefore \bar{f}+g=1+g=1$

得证

部分同学 由 f+g = g 推出 f = 0

代数结构第六次作业

llinggao@mail.ustc.edu.cn 高玲玲

Chapter3.P.65

19.写出下列 2 元开关函数的小项表达式。

(1)恒为 1 的函数

(2)当且仅当两个变量取值相同时函数值为 1.

解：

（1）
$$f(x_1,x_2)=(x_1+\bar{x}_1)(x_2+\bar{x}_2)$$
$$=x_1x_2+x_1\bar{x}_2+\bar{x}_1x_2+\bar{x}_1\bar{x}_2$$

（2）
$$\begin{aligned} f(x_1,x_2) &= f(0,0)x_1^0x_2^0+f(0,1)x_1^0x_2^1+f(1,0)x_1^1x_2^0+f(1,1)x_1^1x_2^1 \\ &= 1*x_1^0x_2^0+0*x_1^0x_2^1+0*x_1^1x_2^0+1*x_1^1x_2^1 \\ &= x_1x_2+\bar{x}_1\bar{x}_2 \qquad (1) \end{aligned}$$

Chapter4.P.90

2.在整数集合 Z 上给出三个关系，它们分别具有如下性质：

(1) 自反，对称，但不是传递的。

解一：关系 R 为：xy≥0

自反性：xx≥0，故(x,x) ∈ R

对称性：若 xy≥0，则 yx≥0，即若(x,y) ∈ R，则(y,x) ∈ R

不传递性：若 x=-1，y=0，z=1，可知(x,y) ∈ R，(y,z) ∈ R 但(x,z) ∉ R

解二：定义关系 R 为：（|x|+2,|y|+2）≠ 1

自反性：（|x|+2,|x|+2）=|x|+2≠ 1, (x,x) ∈ R

对称性：显然。

不传递性：x=3，y=8，z=10 显然，(x,y) ∈ R，(y,z) ∈ R 但(x,z) ∉ R

解三：关系 R 为：|x-y|≤3

自反性：|x-x|=0≤3，(x,x) ∈ R

对称性：显然。

不传递性：x=3，y=6，z=9，则(x,y) ∈ R，(y,z) ∈ R 但(x,z) ∉ R

解四：定义关系 R 为：x 与 y 中有相同的数字

典型错误：

关系 R 为： （x，y）≠1，即 x，y 不互素

但(1,1)∉R，从而 R 不是自反的。

而对于关系：x，y 有公约数。虽然是自反的，且对称，但由于 1 是任意两个整数的公约数，从而满足传递关系。所以 x，y 有公约数这个关系也不能成为本题的答案。对于这种有公约

数,互素 等关系，一定要考虑到 0，1 等的特殊情况。当然部分同学意识到这个问题后，利用解二的方法给出正确答案。

(2) 自反传递但不是对称的

解一：定义关系 R 为：x≥y

自反性：x≥x，即(x,x) ∈ R

传递性：若 x≥y，y≥z，则 x≥z

不对称性：若 x=3，y=2，则(x,y) ∈ R 但(y,x) ∉ R

解二：定义关系 R 为：x≤y

典型错误：

定义关系 R 为：x 为 y 的倍数。显然（0,0）∉ R，即 R 不具有自反性，故不能作为本题的答案。

(3) 对称传递但不是自反的

解一：关系 R 为空关系

易知，R 对称、传递，但不自反：比如（1,1）∉ R

因为对称、传递都是有前提的，而空关系不能满足前提，也就不违背对称、传递性了。但违背自反性。

解二：关系 R 为：x，y 有公约数 2

易证，R 对称、传递，但不自反：（1,1）∉ R

解三：关系 R 为：xy≠0

对称性：显然。

传递性：若 xy≠0，yz≠0，则 x，y，z 皆不为 0，则 xz≠0

非自反性：（0,0）∉ R

解四：关系 R 为：xy>0 或 $\frac{x}{y}=1$,由于（0,0）∉ R，所以有非自反性，对称性和传递性可以验证。

典型错误：

(一）有同学认为，即对称又传递，但是不是自反的关系是不存在的，并给出证明：

任取 xRy，由对称性得 yRx，再有传递性得 xRx， 即若 R 即具有对称性又具有传递性，则必有自反性。

这个证明看上去貌似很正确，然而并没有思考清楚。这是因为，如果 xRy，即(x,y) ∈ R，才会有(x,x) ∈ R，而若，(x,y) ∉ R，即 x，y 本来就不属于这个关系 R，显然就不会有 xRx。而对于自反性的定义，我们是要求对于所有的元素 x，均有 xRx。

（二）关系 R 为，x y 存在大于 1 的公约数

因为（1,1）=1，所以（1,1）∉ R，从而不是自反的。

但是因为 2R6,6R3,但（2,3）∉ R，从而也不传递！

当然，对于这三道题，有些同学通过枚举法来给出关系 R，不能算错，但题目要求是在整数集合 Z 上的，所以枚举可能不是题目的本意。

解答如下：

令 $Ix=\{(x,x),x\notin Z\}$

(1) $R1=Ix \cup \{(1,3),(3,1),(1,4),(4,1)\}$

(2) $R2=Ix \cup \{(0,1)\}$

(3) $R3=\{(1,1)\}$

第七次作业解答

助教：伍浩铖
如有疑问请联系：ustcwhc@mail.ustc.edu.cn

第四章 第 3 题

令$\mathbf{A}=\{\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d}\}$，$\boldsymbol{R_1}$和$\boldsymbol{R_2}$是A上的关系，其中

$$\boldsymbol{R_1}=\{(\boldsymbol{a},\boldsymbol{a}),(\boldsymbol{a},\boldsymbol{b}),(\boldsymbol{b},\boldsymbol{d})\},$$

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

求$\boldsymbol{R_1}\circ\boldsymbol{R_2},\boldsymbol{R_2}\circ\boldsymbol{R_1},\boldsymbol{R_1^2},\boldsymbol{R_2^3}$。

解：

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

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

③ $R_1^2=\{(a,a),(a,d),(a,b)\}$

④ $\because R_2^2=\{(\mathrm{b},\mathrm{b}),(\mathrm{c},\mathrm{c}),(\mathrm{c},\mathrm{d})\}$

$\therefore R_2^3=\{(b,c),(b,d),(c,b)\}$

第四章 第 5 题

证明：$\boldsymbol{R}'=\boldsymbol{I_A}\cup\boldsymbol{R}$是R的自反闭包

证：证明 R’=IAUR,是R 的自反闭包。

证.对任意x∈ A,因（x,x）∈IA,故（x,x）∈ R’，即R’在A 上是自反的。

又 R⊆ IAUR=> R ⊆ R’.

若有自反关系R”且R” ⊇ R,因R” 是自反的=> R” ⊇ IA,于是R” ⊇ IAUR= R’。

R’ 是包含 R 的最小自反关系。

第四章 第 7 题

令$\mathbf{A}=\{\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{4}\}$.在$\boldsymbol{\mathcal{P}}(\mathbf{A})$中定义关系 ~：

$$\mathbf{S}\sim\mathbf{T}\Leftrightarrow|\mathbf{S}|=|\mathbf{T}|$$

证明~ 是$\boldsymbol{\mathcal{P}}(\mathbf{A})$上的等价关系，并写出它的商集$\boldsymbol{\mathcal{P}}(\mathbf{A})/\sim$

证明：

1) 对所有 m∈p(A),有|m|=|m|=>m~m=>~是自反的.

2) 若 p,q∈p(A),且p~q

则|p|=|q|=>|q|=|p|=> q~p=>~是对称的.

3) 若 e,f,g∈p(A),且e~f, f~g

则|e|=|f|,|f|=|g|=>|e|=|g||=>e~g=>~是传递的.

4) 由 1）2）3）知~是 p(A)上的等价关系。

它的商集即是由模不同的元素集合组成的集合，可以写成：

① {[ϕ], [{1}], [{1,2}], [{1,2,3}], [{1,2,3,4}]}或
② {{ϕ}, {{1}, {2}, {3}, {4}}, {{1,2}, … , {3,4}}, {{1,2,3}, … , {2,3,4}}, {{1,2,3,4}}}

第四章 第 8 题

R^*为非零实数集合，$x, y \in R^*$, 定义R^*上的关系ρ

$$x\rho y \Leftrightarrow x \cdot y > 0$$

证明：ρ是R^*上的等价关系，列出所有等价类的代表元

证：1）对所有a∈R*,因a≠0=>a•a>0=>aρa=>ρ 是自反的.

2) 若x,y∈R*,xρy=>x•y>0=>y•x>0=>yρx=>ρ 是对称的.

3) 若x,y,z∈R*, xρy, yρz=> x•y>0, y•z >0=>x与y 同号，y与z 同号=> x与z 同号 => x•z>0=> xρz=>ρ是传递的.

由1）2）3）知ρ 是R*上的等价关系。

两个等价类为正实数集和负实数集，代表元为某一正实数和某一负实数。

第四章 第 9 题

R 为实数集合，在 R 上定义关系 ρ，$x, y \in R$

$$x\rho y \Leftrightarrow x与y相差一个整数$$

证明：ρ 是 R 上的等价关系，写出全部等价类的代表元。

证：

1）对所有x∈R,有x-x=0∈Z=> xρ x=>ρ 是自反的.

2) 若x,y∈R,

xρ y=>x-y=k1(k1∈Z) => y-x= -k1(-k1∈Z) =>yρ x=>ρ 是对称的.

3) 若x,y,z∈R,

xρ y, y ρ z => x-y=k1(k1∈Z),y-z=k2(k2∈Z) =>x-z=k1+k2=k3(k3∈Z) => x ρ z=>ρ 是传递
的.

由1）2）3）知ρ 是R 上的等价关系。

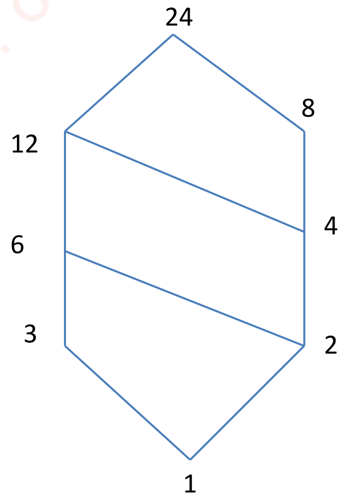
代表元为[0,1).

第四章 第 12（1）题

画出 Hasse 图

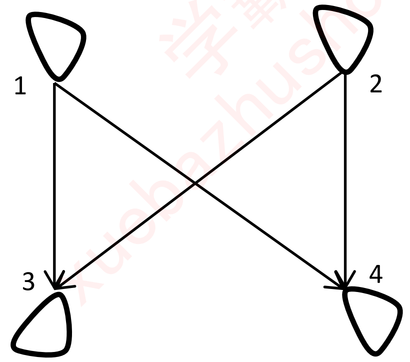
（1）,{1, 2, 3, 4, 6, 8, 12, 24}

解：

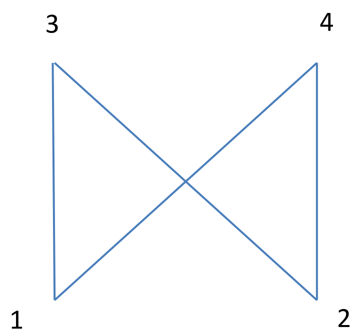


第四章 第 13（2）题

画出图中关系的 **Hasse** 图



解：



第四章 第 15 题

Z 为整数集合，在$Z^* = Z - \{0\}$上定义≤ 关系，$m, n \in Z^*$

$$m \le n \Leftrightarrow m \cdot n > 0且m|n.$$

证明：$< Z^*, \le >$是部分序集。它是否存在最大元，最小元，极大元，极小元？

证明：首先证明$< Z^*, \le >$是部分序集

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

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

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

其次，有结论：$< Z^*, \le >$ 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$k \le 2k$，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 $p \le m$，而不存在 $n \in Z^*$，$n \ne p$，$n \cdot p > 0, n|p$，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，所以不存在极大元

第四章 第 16 题

A 是任意集合，在部分序集$< \mathcal{P}(A), \subseteq >$中取子集序列$\{a_1\}, \{a_1, a_2\}, \dots, \{a_1, a_2, \dots, a_n, \dots\}, \dots$,它们的并集是否是$\mathcal{P}(A)$的一个极大元？为什么？

结论：不一定，分情况讨论

证明：

（1） 若A 是有限集合，则子集序列的并集是$\mathcal{P}(A)$的极大元。

设 A={a1，a2，…，ak}

则子序列的并集为{a1，a2，…，ak}

$\mathcal{P}(A)$中不存在与{a1，a2，…，ak}不同的M，使{a1，a2，…，ak}⊆M

∴A子集序列的并集是$\mathcal{P}(A)$的极大元。

（2） 若A 是无限集合

a)若A 是可数集，则子集序列的并集不一定是$\mathcal{P}(A)$的极大元。

设A={a1，a2，…，an，…}

若子序列为$\{a_1\}, \{a_1, a_2\}, \dots, \{a_1, a_2, \dots, a_n\}, \dots$,则为极大元

若子序列为$\{a_2\}, \{a_2, a_3\}, \dots, \{a_2, a_3, \dots, a_n\}, \dots$, 则不是极大元

b) A 是不可数集，则子集序列的并集不是P(A)的极大元。

$$\cup_{n=1}^{n=+\infty} \{a_1, a_2, \dots, a_n\} = \{a_1, a_2, \dots, a_n, \dots\}$$

是可数无限集，

而 A 是不可数无限集，则存在真子集关系：

$$\cup_{n=1}^{n=+\infty} \{a_1, a_2, \dots, a_n\} \subset A$$

∴ 则该子序列的并集不是$\mathcal{P}(A)$的极大元

代数结构第八次作业答案参考

edit by 贺国超 如有错误请联系 hgc@mail.ustc.edu.cn

第 4 章

18. 证明一个有限集合与一个可数集合的并是可数集合。

证明：

① 若该可数集合是有限可数集合，则两个有限集合的并还是有限集合，也是可数集合；

② 若该可数集合是无限可数集合，则设可数集合 $A=\{a_1,a_2,\ldots,a_m,\ldots\}$，有限集合 $B=\{b_1,b_2,\ldots,b_n\}$。

令 $C = B - A\cap B = \{c_1, c_2, c_3 \quad c_p$ ，再令 $D = A\cup B$

按照如下方式构造 D， $d_i=\begin{cases} c_i & i\le p \\ a_{i-p} & i> p \end{cases}$，

易知存在一个双射 $f: D\to N$，即 D 与自然数集合 N 等势；

得证！

错误情况：大部分的同学都没有分清楚可数集合和无限可数集合的概念。误认为可数集合就是无限可数集合。

20. 证明 R*R 与 R 等势

证明：证法不唯一。此处证明(R*R)~(R^+*R)~R

对(R*R)上的数对(x,y)，构造函数 f 为直角坐标转换极坐标函数 f(r,a)，其中 r 为坐标(x,y)与极点距离，r>=0;a 为坐标(x,y)和极点连线与 x 轴正半轴夹角，-pi<=a<pi,再利用书上的半圆法将 a 双射到整条实数轴。显然,f 为双射。因此(R*R)~(R^+*R)。

对(R^+*R)上的数对(r,a)，假设 r 的表示形式为$(\ldots000r_mr_{m-1}\ldots r_1\bullet R_1R_{2\ldots}R_n000\ldots)$, a 的表示形式为$(\ldots000a_ja_{j-1}\ldots a_1\bullet.A_1A_{2\ldots}A_k000\ldots)$。构造函数 g(z)，令 z 按照如下方式生成：$(\ldots a_3r_3a_2r_2a_1r_1\bullet R_1 A_1 R_2A_2 R_3 A_3,\ldots)$,z 的符号由 a 唯一确定。Z 是实数。g 也是双射。因此(R^+*R)~R。

根据等势关系的传递性，可得(R*R)~R。

注 1：也可证明(R*R)~((0,1)*(0,1))~(0,1)~R

注 2：也可分别构造(R*R)→R 和 R→(R*R)的单射（满射）

注 3：尽量不可用极限理论证明，用上述插数法证明时，要注意符号，这也是部分同学的错误来源。

第 5 章

1：

（2）是交换群，单位元为 0, a 的逆元为-a；

（3）是交换群，单位元为$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$，A 的逆元是其本身。

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

（5）不是交换群，单位元为 1，a>0 时逆元为 1/a， a<0 时，逆元为 a。

错误情况：部分同学因计算出错，不满足结合律认为不是群。

2：（1）封闭性：a * b = a + b + ab = a（b+1）+b+1-1= (a + 1)(b + 1) − 1，因为 a，b ≠ −1，所以 a * b ≠ −1 ∈ S

结合律：(a * b) * c = （ a + b +ab ） *c =a + b +ab + c + (a + b +ab)c = a(b+c+bc)+a+b+c+bc =a *（ b* c ）

单位元:0

逆元： a^{-1} = -a/(1+a)

（2）2 * x * 3 = 7， ⇒x=-1/3

4: G是交换群⇔ $b*a=a*b$ ⇔ $a*b*a*b=a*a*b*b$ ⇔ $(a*b)^2=a^2*b^2$

代数结构第九次作业答案

llinggao@mail.ustc.edu.cn

6/p.113. a 和 b 是群 G 中的两个任意元素，证明 a*b 与 b*a 是同阶的。

证明：

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。

   $(b*a)^{n+1} = b*(a*b)^n*a = b*a$

   $\therefore (b*a)^n = e$

   ∴ m|n

   同理，n|m

   ∴ 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：

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

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。

10.G 是群，

$$H = \{a|a\epsilon G, \forall g\epsilon G, a*g = g*a\}$$

称为群 G 的中心。证明：<H,*>是<G,*>的子群。

证明：

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

(2)

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

(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. **H, K是群G 的子群，证明 H ∩ K也是G 的子群。H ∪ K是群 G 的子群吗？证明你的结论。**

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！

13. 令 $G = \{f_{a*b}: Q \to Q, f(x) = ax + b, a \neq 0, a, b \epsilon Q\}$，**G 对合成元素构成群。证明** $H = \{f_{1^b} | \, b \epsilon Q\}$**是G的子群。**

证明： $f_{1^b} = x + b$

1. $e = f_{1^0} = x \epsilon H, H \neq \emptyset$
2. $\forall b_1, b_2 \epsilon Q, f_{1^{b_1}} \epsilon H$， $f_{1^{b_2}} \epsilon H$

   $f_{1^{b_1}} * f_{1^{b_2}} = (x + b_2) + b_1 = x + (b_1 + b_2) = f_{1^{b_1 + b_2}}$

3.$\forall f_{1^b} \epsilon H$, 其逆元$f_{1^{-b}} = x - b \epsilon H$

综上，H 是 G 的子群。

典型错误：不说明 H 非空。

代数结构第十次作业解答

伍浩铖 ustcwhc@mail.ustc.edu.cn

第五章 第 15 题

G 是 6 阶循环群，找出 G 的全部生成元并列出 G 的所有子群。

解：$G=\{e,g^1,g^2,g^3,g^4,g^5\}$,考察每个元素，只有 g^1 与 g^5 的指数与 6 互素，所以生成元为 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 $<G,*>$

第五章 第 16 题

G 是 n 阶循环群，d 是 n 的因子，G 存在且仅存在一个 d 阶子群。

证明：

存在性：

设 $G=\{e,g^1,g^2,...,g^{n-1}\}$，且 $n=dm$，则 $K=\{e,g^m,g^{2m},...,g^{(d-1)m}\}$ 就构成了一个 d 阶子群，生成元为 g^m

唯一性：

① d=1，则 $K=\{e,g^m,g^{2m},...,g^{(d-1)m},*\}=\{e\}$，显然每个群只有这么一个子群。

② 若 d>1，设 H 是另外一个 d 阶子群，生成元为 g^s，这里显然 s 为 H 中除了单位元 e 之外的最小阶。设 $n=st+r, 0\le r<s$，则 $g^r=g^{n-st}=g^n g^{-st}=g^{-st}\in H$，所以只能是 $r=0$，则 $s|n$，则 g^s 的阶为 $d=\frac{n}{s}=\frac{n}{m}$，则 $s=m$，即 H 与 K 是同一个子群。

唯一性证毕。

第五章 第 21 题

$Sn(n \ge 2)$ 的每个子群或者全部由偶置换构成，或者其中奇偶置换各占一半

证明：

1. 由于偶置换与偶置换的合成仍为偶置换=>Sn 的某些子群可以全部由偶置换构成。
2. 由于奇置换与奇置换的合成为偶置换，若某子群含有奇置换则必含偶置换。设此子群为

$D = A \cup B = \{p_1, p_2, ..., p_m\} \cup \{q_1, q_2, ..., q_n\}$，

$\{p_1, p_2, ..., p_m\}$ 为奇置换集合 A，$\{q_1, q_2, ..., q_n\}$ 为偶置换集合 B。

因奇置换 p_1 与任意奇置换 p_i 的合成为偶置换=> $p_1 \circ p_i \in B$。由 $p_1 \circ p_i$ 各不相同 =>

$m \le n$

因奇置换 p_1 与任意偶置换 q_j 的合成仍为奇置换=> $p_1 \circ q_j \in A$。由 $p_1 \circ q_j$ 各不相同=>

$m \ge n$

于是 $m = n$，即奇置换与偶置换各占一半。

第五章 第 25 题

证明：无限循环群的子群，除 $\{e\}$ 之外都是无限循环群。

证明：反证法。

设无限循环群为 $G = \{e, g^1, g^2, ...\}$，则不存在 $g^i = e, i \ne 0$

假设其有一个子群 $K \ne \{e\}$，它是一个有限循环群，生成元为 g^k，其阶为 d，则 $g^{k \cdot d} = e$，矛盾。证毕

第五章 第 26 题

在群 $<G,*>$ 中定义新的二元运算 $\bullet$：

$$a \bullet b = b * a$$

证明 $<G,\bullet>$ 是群，并且 $<G,*>$ 与 $<G,\bullet>$ 同构。

证明：

1. 是群：

（封闭性）$\forall a,b \in G, a \bullet b = b * a \in G$

（结合律）$\forall a,b,c \in G, (a \bullet b) \bullet c = (b * a) \bullet c = c * (b * a) =$
$(c * b) * a = (b \bullet c) * a = a \bullet (b \bullet c)$

（单位元）$<G,*>$ 中的单位元 e 可以作为 $<G,\bullet>$ 的单位元，因为

$\forall a \in G, a \bullet e = e * a = a, e \bullet a = a * e = a$

（逆元）$<G,*>$ 中的逆元可以作为 $<G,\bullet>$ 的逆元，因为

$\forall a, a^{-1} \in G, a \bullet a^{-1} = a^{-1} * a = e, a^{-1} \bullet a = a * a^{-1} = e$

综上，$<G,\bullet>$ 是一个群。

2. $<G,*>$ 与 $<G,\bullet>$ 同构：

在群 $<G,*>$ 和 $<G,\bullet>$ 定义映射 $f(a) = a^{-1}$．以下证明 $f: G \to G$ 是双射且满足

$f(a * b) = f(a) \bullet f(b)$

1. $f(a * b) = (a * b)^{-1} = b^{-1} * a^{-1} = a^{-1} \bullet b^{-1} = f(a) \bullet f(b)$

2. f 是满射：对于 G 中的任一元素 a 都能在 G 中找到 a^{-1} 使得 $f(a^{-1}) = (a^{-1})^{-1} = a$，

f 是单射，对于 $a \neq b$,若 $f(a) = f(b)$,则 $a^{-1} = b^{-1} \Rightarrow a = b$ 矛盾

综上，$<G,*>$ 与 $<G,\bullet>$ 同构

第六章 第 1 题

H 是交换群 G 的子群，证明 H 的每个左陪集也是一个右配集

证明：$aH = \{a * h \mid h \in H\} = \{h * a \mid h \in H\} = Ha$

第六章 第 3 题

写出 A_4 关于 $H = \{e, (12)(34), (13)(24), (14)(23)\}$ 的左陪集分解与右配集分解。

解：A_4 是指所有四元偶置换。若一个轮换中的数字有偶（奇）数个，则表示奇（偶）轮换，奇轮换与奇轮换的组合是偶置换。所以

$$A_4=\{e,(12)(34),(13)(24),(14)(23),(243),(234),(123),(124),(132),(134),(142),(143)\}$$

左陪集分解可以这么做，首先计算左陪集的个数$=|A_4|/|H|=3$

1. $eH=H$ 是分解后的第一个集合
2. 取剩下的第一个元素的左陪集 $(243)H=\{(123),(134),(142),(243)\}$ 作为第二个集合
3. 取剩下的第一个元素的左陪集 $(234)H=\{(124),(134),(143),(234)\}$

则 $A_4=H\cup\{(123),(134),(142),(243)\}\cup\{(124),(134),(143),(234)\}$

右配集的分解也可以用同样的方法得到：

$$A_4=H\cup\{(123),(134),(142),(243)\}\cup\{(124),(134),(143),(234)\}$$

第六章 第五题

H,K 是 G 的两个子群，$[G:H]=m,[G:K]=n$，证明子群 $H\cap K$ 在 G 中的指数 $[G:H\cap K]\le mn$

证明：将 G 按照 H,K 的左陪集分解为：

$$G=H_1\cup H_2\cup\ldots\cup H_m$$
$$G=K_1\cup K_2\cup\ldots\cup K_n$$

任取 H_i,K_j，若 $H_i\cap K_j\ne\varnothing$，则下面来看一下 $H_i\cap K_j$ 是个什么东西

将 H_i,K_j 中的元素列出来，$H_i=\{h_{i1},h_{i1},\ldots h_{is}\},K_i=\{k_{j1},k_{j1},\ldots k_{jt}\}$

由于 H_i,K_j 是 G 关于 H,K 的左陪集，则 H_i,K_j 中的任何一个元素都可以当做代表元

由于 $H_i\cap K_j\ne\varnothing$，则可取一元素 $a\in H_i\cap K_j$，则 $H_i=aH,K_j=aK$

下面证明 $H_i\cap K_j=aH\cap aK=a(H\cap K)$，即 $H_i\cap K_j\ne\varnothing$ 是 $H\cap K$ 的一个左陪集

1. $$\begin{aligned}&\forall b\in aH\cap aK,\exists x\in H\ and\ x\in K,b=ax\\&\Rightarrow x\in H\cap K,b=ax\in a(H\cap K)\\&\Rightarrow aH\cap aK\subseteq a(H\cap K)\end{aligned}$$

$\forall c \in a(H \cap K), \exists y \in H \cap K, c = ay$

2. $\Rightarrow y \in H \; and \; y \in K, c = ay \in aH \cap aK$

$\Rightarrow a(H \cap K) \subseteq aH \cap aK$

所以$\varnothing \neq H_i \cap K_j = aH \cap aK = a(H \cap K)$是$H \cap K$的一个左陪集

而$H_i \cap K_j \neq \varnothing$的情况最多有$mn$个，则$[G : H \cap K] \leq mn$

第六章 第 7 题

H是G的正规子群。如果a,b属于H的同一个陪集中，c,d属于H的同一个陪集中，那么$a*c$和$b*d$属于H的同一个陪集中

证明：要证明属于同一个陪集，只要证明了$\exists h \in H, (a*c)*h = b*d$就行，或者$(a*c)*(b*d)^{-1} \in H$亦可，我们采用后一种思路。

$(a*c)*(b*d)^{-1} = a*c*d^{-1}*b^{-1} = a*h_1*b^{-1}, (h_1 = c*d^{-1} \in H)$

因为H是G的正规子群，所以$b*h_1*b^{-1} = h_2 \in H$

$a*h_1*b^{-1} = a*b^{-1}*b*h_1*b^{-1} = a*b^{-1}*h_2 = h_3*h_2 \in H, (h_3 = a*b^{-1} \in H)$

所以$(a*c)*(b*d)^{-1} \in H$，即$a*c$和$b*d$属于H的同一个陪集中。

第六章 第 10 题

H_1和H_2是G的正规子群，证明：$H_1 \cap H_2, H_1 * H_2$也是 G的正规子群

证明：

1. $H_1 \cap H_2$

① 先证明是子群

（封闭性）$\forall a,b \in H_1 \cap H_2, a*b \in H_1, a*b \in H_2 \Rightarrow a*b \in H_1 \cap H_2$

（逆元）$\forall a \in H_1 \cap H_2, a^{-1} \in H_1, a^{-1} \in H_2 \Rightarrow a^{-1} \in H_1 \cap H_2$

所以$H_1 \cap H_2$是子群

② 再证明是正规子群

由于 H_1 是正规子群，所以 $\forall g \in G, \begin{cases} h_1 \in H_1, g*h_1*g^{-1} \in H_1 \\ h_2 \in H_2, g*h_2*g^{-1} \in H_2 \end{cases}$

也就有 $\forall g \in G, h \in H_1 \cap H_2, g*h*g^{-1} \in H_1 \cap H_2$

所以 H_1 是正规子群

2. $H_1 * H_2$

① 先证明是子群

$$\begin{aligned} &\forall a_1, a_2 \in H_1, b_1, b_2 \in H_2, a_1*b_1 \in H_1*H_2, a_2*b_2 \in H_1*H_2 \Rightarrow \\ \text{（封闭性）}&(a_1*b_1)*(a_2*b_2) = a_1*(b_1*a_2*b_2) = a_1*(b_1*a_2*b_1^{-1}*b_1*b_2) = \\ &a_1*(a_3*b_1*b_2) = (a_1*a_3)*(b_1*b_2) = a_4*b_3 \in H_1*H_2 \end{aligned}$$

（逆元） $\forall a \in H_1, b \in H_2, a*b \in H_1*H_2, (a*b)*(a*b)^{-1}=e$，则 $(a*b)^{-1}$ 是其逆元，下面证明 $(a*b)^{-1} \in H_1*H_2$

$(a*b)^{-1} = b^{-1}*a^{-1} = a^{-1}*(a*b^{-1}*a^{-1}) = a^{-1}*b_1 \in H_1*H_2$

所以 H_1*H_2 是一个子群

② 在证明 H_1*H_2 是正规子群

$$\begin{aligned} &\forall g \in G, h_1 \in H_1, h_2 \in H_2, g*(h_1*h_2)*g^{-1} = (g*h_1*g^{-1})*(g*h_2*g^{-1}) = \\ &h_3*h_4 \in H_1*H_2, \\ &\text{其中} g*h_1*g^{-1}=h_3 \in H_1, g*h_2*g^{-1}=h_4 \in H_2 \end{aligned}$$

所以 H_1*H_2 是正规子群

第六章 第 12 题

H, K 都是群 G 的正规子群并且 $H \cap K = \{e\}$。证明：对任意 $h \in H, k \in K$，都有 $h*k = k*h$

证明：

$$\left.\begin{aligned} &h*k*(k*h)^{-1} = h*k*h^{-1}*k^{-1} = (h*k*h^{-1})*k^{-1} = k_1*k^{-1} \in K \\ &h*k*(k*h)^{-1} = h*k*h^{-1}*k^{-1} = h*(k*h^{-1}*k^{-1}) = h*h_1 \in H \\ &H \cap K = \{e\} \end{aligned}\right\} \Rightarrow$$

$h*k*(k*h)^{-1} = e \Rightarrow h*k = k*h$

第六章 第 14 题

在非零实数乘法群中，如下定义的映射 f 中，那些是同态映射，并且找出它的同态核。

同态映射的关键是要有一个映射满足 $f(a*b)=f(a)\bullet f(b)$

同态核就是映射到单位元的集合

（1） $f_1(x)=|x|$ $\Rightarrow$同态映射，Ker f={±1}

（2） $f_2(x)=2x$ $\Rightarrow$非同态映射

（3） $f_3(x)=x^2$ $\Rightarrow$同态映射，Ker f={±1}

（4） $f_4(x)=\dfrac{1}{x}$ $\Rightarrow$同态映射, Ker f={1}

（5） $f_5(x)=-x$ $\Rightarrow$非同态映射

（6） $f_6(x)=-\dfrac{1}{x}$ $\Rightarrow$非同态映射

第十一次作业答案参考

——贺国超，有疑问请发邮件给 hgc@mail.ustc.edu.cn

第 6 章

定理 6.74 后半部分：

证明：定义$F: G_1/f^{-1}(H_2) \longrightarrow f(G_1)/H_2, F(af^{-1}(H_2)) = f(a)H_2$

首先要说明F是映射。

如果$a_1f^{-1}(H_2) = a_2f^{-1}(H_2)$，那么$a_1'*a_2 \in f^{-1}(H_2)$，$f(a_1'*a_2) \in H_2$

由同态定义知$(f(a_1))' \bullet f(a2) = f(a_1'*a_2) \in H_2$，则$f(a_1)$与$f(a_2)$模$H_2$同余

则$f(a_1)H_2 = f(a_2)H_2$，即映射F与代表元选取无关。

再说明双射。

任取y = f（a）H_2，则F[$af^{-1}(H_2)$] = y,即$af^{-1}(H_2)$是y的一个原象，即满射。

又若$a_1f^{-1}(H_2)$和$a_2f^{-1}(H_2)$都是y原象，即$f(a_1)H_2 = f(a_2)H_2$，

则有$(f(a_1))' \bullet f(a_2) = f(a_1'*a_2) \in H_2$，

故$a_1'*a_2 \in f^{-1}(H_2)$，$a_1f^{-1}(H_2) = a_2f^{-1}(H_2)$，所以F是双射。

另外有：

F[$af^{-1}(H_2) \bullet bf^{-1}(H_2)$] = F[$(a*b)f^{-1}(H_2)$]

$= f(a*b)H_2 = [f(a) \bullet f(b)]H_2 = f(a)H_2 \bullet f(b)H_2 = F[af^{-1}(H_2)] \bullet F[bf^{-1}(H_2)]$

综上所述，F为群同构映射，故$G_1/f^{-1}(H_2) \cong f(G_1)/H_2$

第 16 题

对任意a，b$\in$G， $(a*b)=(a*b)^k=\underbrace{(a*b)*\quad\quad *(a*b)}_{k个(a*b)相乘}$

$\because G$是交换群

$\therefore f(a*b)=\underbrace{(a*b)*\cdots\cdots*(a*b)}_{k个(a*b)相乘}=a^k*b^k=f(a)\bullet f(b)$

$\therefore$ f是同态映射。

且易求得f(G)={a^k|k$\in$G}，Ker f = {a|a^k=e，a$\in$G}。

第 19 题

证明：

对$\forall g_1\in G$，$\forall g_2\in G$ ，

$\because H$和K是交换群

$\therefore Hg_1\bullet Hg_2=Hg_1*g_2=Hg_2*g_1=Hg_2\bullet Hg_1$

$\therefore (g_1*g_2)\equiv(g2*g1)(\bmod H)$,即$(g_1*g_2)'*(g2*g1)\in H$

同理$(g_1*g_2)'*(g2*g1)\in K$

$\Rightarrow (g_1*g_2)'*(g2*g1)\in(H\cap K)$

$\Rightarrow (g_1*g_2)\equiv(g2*g1)(\bmod(H\cap K))$

$\Rightarrow (H\cap K)g_1*g_2=(H\cap K)g_2*g_1$

$\Rightarrow (H\cap K)g_1\bullet(H\cap K)g_2=(H\cap K)g_2\bullet(H\cap K)g_1$

$\therefore G/(H\cap K)$是交换群，得证！

第七章

第 2 题

（1）$\{1,-1\}$
（2）$\{x \mid x \in Q, x \neq 0\}$
（3） $\{[1],[3]\}$
（4）$\{[1],[5]\}$

第 3 题

证明：设<R,+>的生成元为r, 任取a，$b \in R$，
设$a = r^m$，　$b = r^n$
$$a \bullet b = r^m \bullet r^n = \underbrace{(r+r+\cdots\cdots+r)}_{m个r} \bullet \underbrace{(r+r+\quad+r)}_{n个r} = mnr^2$$
$$b \bullet a = r^n \bullet r^m = \underbrace{(r+r+\cdots\cdots+r)}_{n个r} \bullet \underbrace{(r+r+\quad+r)}_{m个r} = mnr^2$$
于是$a \bullet b = b \bullet a$,<R,+,•>是交换环， 得证！

第 5 题

解：(1)：非整环，非域
(2)：　整环，非域
(3)：　整环，　域

第 7 题

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。

代数结构第 12 次习题答案

高玲玲 llinggao@mail.ustc.edu.cn

Chapter7 环和域

8 page153

证。（1）对 $f,g \in E_H$， $x\in H$有 $(f+g)(x)=f(x)+g(x) \in H$=> $(f+g)(H) \subseteq H$
=> E_H对加法封闭

（2）$x\in H$令 $f_0(x)= O_H$ => $f_0(H) =\{O_H\}\subseteq H$=> $f_0\in E_H$.

对 任 $x\in H$，$f \in E_H$ 有 $(f+ f_0)(x)= f(x)+ f_0(x)= f(x)+ O_H= f(x)$ 同理$(f_0+ f)(x)= f(x)$
=> f_0 是E_H. 的 加法幺元（零元）。

令 $f'(x)=-f(x)$; 对 任 $x\in H$ $(f'+f)(x)= O_H= f_0(x)$ => f'是 f的 逆元。

因 $f(x) \in H$ ， $-f(x)$ 是 $f(x)$的加法逆元 =>$-f(x) \in H$

从而， 对$f \in E_H$ 有逆元存在。

（1）（2）=>$< E_H , +>$ 是 $<E , +>$ 的 子群。

（3）对 $x\in H, f , g \in E_H$， 有 $(f \bullet g)(x)= f(g(x)) \in H$ => E_H 对乘法封闭。

（4）令 $f_1 (x)=x$, $(f_1 \bullet g)(x)= f_1 (g(x))= g(x)$ => f_1是乘法幺元。

由（1）（2）（3）（4）=>E_H是E的子环。

个人意见：

证明子群、子环等概念时，先交代下 单位元（乘法幺元）属于这个集合，从而说明其非空。另外，在证明过程中，有条理地交代下所证的结论，比如，对加法封闭、零元、逆元等关键点。

典型错误：

第一点：H 是 G 的子群。

注意，要证的是 E_H 是 E 的子环，所以应该证明 E_H是 E 的子群。

10 page153

证。(1) $f((a,b)+ (c,d))=f(a+c, b+d)=a+c=f(a,b)+f(c,d)$

(2) $f((a,b)\bullet (c,d))=f(ac, bd)= ac= f(a,b) \bullet f(c,d)$

(3) $f(1,1)=1$, $(1,1)$ 是 $Z\times Z$ 的 单位元， 1 是 Z 的 单位元.

=>f 是同态映射。

令 $f(a,b)=0$=> $a=0$ => $\ker f=\{(0,b)| b\in H\}$

典型错误：

$\text{Kerf}=\{(1,b) | b\in Z\}$

课本 7.6 节：环的同态映射中，同态核为像为 R_2零元的集合。

18 page153

$f(x)+g(x)=-1+4x$, $f(x) \bullet g(x)=-5+5x-5x^2 +3x^4+5x^6$

典型错误：
不进行化简。注意，这是 Z_7 上的运算。

P153——19
f(x)=1+x+x2+…+xn 有因子 1+x 当且仅当 $f(-1)=0_R$

$$f(-1)=\begin{cases}0 & n\text{为奇数}\\1 & n\text{为偶数}\end{cases}$$

∴1+x+x2+…+xn 有因子 1+x 当且仅当 n 为奇数

Chapter8 格与布尔代数

8.1 证明：1.定义证明<R1,≤>是部分序集
2.再证 * 是 min 运算，⊕ 是 max 运算。

8.2 证明：（1）从含义入手，a*b 表示{a,b} 的最大下界，b*a 表示{b,a} 的最大下界，由于集合的无序性，两者相同。从而 a*b=b*a
同理，a⊕b=b⊕a
当然，也可以利用课本中证明定理 8.1 的方法证明。
（2）因 a⊕ 是 max 运算 a⊕b，a≤a
故 a≤a*(a⊕b)
又因为 a≥a*(a⊕b)
故 a=a*(a⊕b)

同理证 a⊕(a*b)=a

典型错误
受第一题的影响，简单认为 * 就是 min 运算，⊕ 是 max 运算
得出 a*b=min{a,b}=b*a
大错特错!! 我快崩溃!
注意，a*b 永远只能表示 a 和 b 的最大下界，而不是简单的 min 运算。
题 1 中之所以有这样的结论，是因为小于等于关系是一个线性序，即任何两个元素都可比较，或者说都有一个大小关系在里面。
但是，这里的前提是：A 是一个格。格是部分序。所谓部分序，就是部分有序，不是所有元素之间都有可比较关系。{1,3,5,15}上的整除关系是一个部分序，3 和 5 之间就不存在大小关系!
这也是部分同学分情况讨论：若 a≤b，怎么样；若 b≤a 怎么样。 错误的原因。

4.证明：（1）a⊕b=b=b*c
（2）(a*b)⊕(b*c)=a⊕b=b
(a⊕b)*(a⊕c)=b*c=b
故（a*b)⊕(b*c)=b=(a⊕b)*(a⊕c)
证毕

5. （1）证明在格中$(a*b)\oplus(c*d)\le(a\oplus c)*(b\oplus d)$

证明：　$a*b\le a, c*d\le c$

所以　$(a*b)\oplus(c*d)\le a\oplus c$

同理，$(a*b)\oplus(c*d)\le b\oplus d$

由于$(a\oplus c)*(b\oplus d)$是最大下界，

所以$(a*b)\oplus(c*d)\le(a\oplus c)*(b\oplus d)$

（2）证明$(a*b)\oplus(b*c)\oplus(c*a)\le(a\oplus b)*(b\oplus c)*(c\oplus a)$

证明：$(a*b)\oplus(b*c)\le b$

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

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

同理：$(a*b)\oplus(b*c)\oplus(c*a)\le a\oplus c$

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

故命题得证。

8-8 设 S={1,3,5,15,25,75},<S,|>是格，请列出互补元素。

解：最小元=1，最大元=75，

1 与 75 互补

3 与 25 互补

典型错误：

5 和 15 互补

8.10 具有三个或更多元素的线性序集不是补格

线性序有三个或更多元素

则存在 a，且 $a\ne 0$，1

对 a，存在 b，使得 $a*b=0$，有 $b=0$

又 $a\oplus b=1$,则 $a=1$，与 $a\ne 1$ 矛盾

得出此线性序不是有补格