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。
   $(b*a)^{n+1} = b*(a*b)^n*a =$ 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。

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)∀g∈G, a ∗ e = e ∗ a, ∴ e∈H, H ≠ ∅

(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：

$H \leq G, K \leq G$

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

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

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

$\therefore H \cap K$ 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$e, g^1, \ldots, g^{n-1}$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'。