第二章 数论

1. 整除运算 |

①a|a ②a|a∧b|a => a=±b ③a|b∧b|c => a|c ④a|b => a|(bc)

⑤a|b∧a|c => a|(bx+cy) ⑥a, b>0∧a|b => a≤b

1. 最大公因子(a,b)；集合及d=(a,b)的相关证明
   1. m(a,b)=(ma,mb) ②(a,m)=(b,m)=1 => (ab,m)=1 ③(a,b)=(a,b+ax)

④c|ab∧(c,b)=1 => c|a

1. 转相除法
2. 最小公倍数[a,b]
3. 一个重要结论[a,b](a,b)
4. 素因子分解唯一性定理
5. 线性不定方程

ax+by=n有解⬄ (a,b)|n.

通解：

1. 同余和线性同余方程

定义2.4后面的性质

1° (a,有解⬄(a,m)|b.

2° 通解：

其中

3° 孙子定理

1. 完系，缩系

(a,m)=1,则完系（缩系）每个数\*a还是完系（缩系）

1. 欧拉定理，费马定理，欧拉函数

费马取m为素数即可

* 1. p为素数时， ②(m,n)=1时，φ(mn)= φ(m) φ(n)

1. 威尔逊定理

p为素数⬄(p-1)! -1(mod p)

1. σ，d和完全数

完全数：σ(n)=2n

若p和为素数，则是完全数p和为素数

偶完全数n，必有n=，p和均为素数

1. 原根指数

① n次整系数多项式f(x)，则f(x) 0（mod p）至多有n个解

② n≥1,则

③ p为素数，l|(p-1). 那么mod p阶为l的数恰好有φ（l）个

④ m有原根⬄m=2，4，p^k, 2·p^k

**习题**

1. 整除，公因子公倍数，素数：1，2，4，5，6，7，8
2. 同余相关的简单题：13，14，15，16，17，27，28
3. 特殊函数φ，σ，d：22，24，25，26，31，32，33，36
4. 完系缩系：23
5. 欧拉费马的应用：29，30，39
6. 完全数：34，35
7. 解不定方程：3，9，10，11，12，20
8. 解一元一次同余方程：18.(3)，38.(2)
9. 解多元一次同余方程组：19.(2)，21
10. 解一元多次同余方程：38.(3)
11. 阶原根指数：37，38，40，41，42

第五章

1. 群：①封闭，②结合，③单位元，④逆元
2. 半群：封闭，结合
3. 带1半群：封闭，结合，单位元
4. 阿贝尔群：交换
5. 群的阶：有限群G的阶为|G|,

群里元素的阶：满足a^n=e的最小正整数n…………6

1. 群的其他定义：
   1. ①+②+右单位元+右逆
   2. ①+②+（a\*x=b和y\*a=b在G中有解）
   3. ①+②+左右消去+G是有限集合——每行每列出现一次克莱因群(K4)
2. 子群：
   1. 子群也是群
   2. 封闭+有逆， 或直接证明a\*b’属于G…………10
   3. 如果H是G的有限非空子集，只需要封闭
   4. 生成子群——怎么生成…………<2,3>
3. 循环群
   1. 存在g属于G，使G={g^n|n为整数}
   2. g是群<G,\*>中k阶元，H={g^r|r为整数}，那么<H,\*>是<G,\*>的一个k阶子群
   3. 循环群的子群是循环群
   4. G是n阶循环群，G=<a>且|G|=n，H≤G，H=<b>且b=a^s,则|H|=n/(n, s)
4. 置换群

n元集合A上全体置换构成集合在合成运算下构成一个群，阶为n！

* 1. 对称群：集合A上的双射全体对于映射合成运算构成群
  2. 置换群：对称群的子群

N次对称群(Sn), N次二面体群(Dn)

1. 群同构——26

两群间存在保持运算的双射

① 是G1->G2的同态映射,e1和e2是G1和G2的单位元，必有，并且对任何G1中元素a，

② 群G到集合G’存在保持运算的双射，则G’对于对应运算也是群，且G和G’同构

③ 任何一个群都与一个置换群同构

**习题**

1. 证明是否是群或子群或特殊群：1，2，3，4，9，10，11，13，14，17
2. 证明除了群以外的一些性质：5，6，7，8，16，18，21，25（21我也不会）
3. 寻找子群：12，15，19，20，24
4. 同构：22，23，26

第六章 商群

1. 同余

a\*b’属于H≤G，称a与b模H同余，记作a≡b(mod H)

1. 陪集

Ha={h\*a|h属于H}，为G中右陪集，元素a是陪集Ha的代表元

* 1. He=H
  2. a≡b (mod H) ⬄Ha≡Hb
  3. a属于H ⬄ Ha=H
  4. 左右陪集等势

1. 指数

群G关于它子群H的左（右）陪集个数叫H在G中的指数，记为[G:H]

拉格朗日定理： G有限，H≤G，则|G|=[G:H]|H| （用陪集分解证明）

推论：

1. 有限群G中元素的阶是|G|的因子
2. 素数阶群都是循环群
3. 正规子群

正规子群定义1：H≤G，对所有G中元素g和H中元素h都有g’\*h\*g属于H，则称H是G的正规子群，记为H◁G

正规子群定义2：H≤G，H是G的正规子群⬄对G中任意元素g，Hg=gH

1. 商群

定义集合的乘法A·B={a\*b | a属于A，b属于B}

N是群G的正规子群，<{Ng|g属于G}, ·>是群，称为G模N的商群，记为G/N

1. 群同态

存在f:G1->G2的保持运算的满射（单射，双射）f，则称f是满同态映射（单一同态映射，同构映射）

核：Ker f = {a | a属于G1, f(a)=e2}

1. Ker f是群G1的正规子群
2. f为单射⬄Ker f = {e1}

群同态基本定理

群G1的任何商群都是G1的同态像。若G2是G1的同态像，则G1/Ker f和G2同构

G/H和(G/K)/(H/K)同构

**习题**

1. 证明陪集及相关性质：1，7
2. 指数，阶数：4，5，6
3. 陪集分解和商群：3，8，13
4. 正规子群：9，10，11，12，19，20
5. 群同态：14，15，16，17，18

第七章 环和域

各种定义和性质

**习题**

1. 证是环或特殊环或子环：1，3，5，8
2. 求相关性质：2，4，6，7