先说“计数”这章。3.1.2的 **乘积法则** 和 **求和法则** 是重点，这俩也挺简单了，看了就会，这个分不拿可惜吖~~~ 3.1.4的**容斥原理**是重点，这个也挺简单的，基本也属于看了就会。作为能考到**世界一流大学**的学生，我相信你们的智商~！！！ 3.2的 **鸽巢原理** 是重点，以及 3.2.2 的定理2的 **广义鸽巢原理** 也要看的，至少要记住公式和怎么用吧，那个定理里的那个比较不常用的符号是 **向上取整** 的意思。3.1.5树图不考，例19要看，例20和例21不用看。到3.3.3，首先要明白什么是**r排列，定理1，推论1，定理2** 都是要好好看看的，后面的定义，定理以及推广都要看看，都不难的。这个，大家都看看吧...真心都不难...实在有愧于大家...再之后，回到我的笔记，回到P131的例5，老师着重讲了讲，这个要弄会滴~~~例6不用看。P132的表格大家看看。之后是具有重复元素的全排列，大家好好看看哟~~~P133的例9和P135.8题要看，例10和例11不用看。再到后面，3.6不用看。**（页数是根据薄版的离散书写的，厚版的离散书同学们自己找一下页数。我写完才发现这个问题，实在抱歉。）**

总的来说，第三章很简单，就算之前没上过课，在图书馆高效率看上两个小时也绝对可以搞定。

第四章高级计数技术，**兔子和斐波那契数**和**汉诺塔**很简单，好好看看，4.2是大重点，6个定理一定要会，这个稍有难度，不过相信世界一流大学的孩子们的智商~！！！4.3不考，分治算法什么的，是数据结构的内容。4.4**生成函数**要看，P178页定理1要会证。P180例1要看。

至此这本书结束。

下面是薄本的《离散数学代数结构》，这本书是我自己根据上课老师说的重点整理的，兼顾参考我们班两位学霸—王楚天小童鞋和刘旸小童鞋的笔记整理的，特别鸣谢一下~啦啦啦~~~

第四章代数系统，从头开始认真看吧，都不难，就是概念理解记住就好。我就补充一下老师上课的笔记吧**（工作量猛增吖（用忧桑的蓝色字体吧...）...T T...**哪位好心人请我吃顿好吃的抚慰一下我的幼小心灵...）。一直从头看到P70，这里有老师上课讲的一道题我记下来了：判断真假之**“若<A,\*>有两个不同的左单位元，则无右单位元”**，这句话为**真**。证明很简单，我说一下思路：**反证法，如果有两个不同的左单位元，且有右单位元，则根据定理1，必有左单位元和右单位元相等，又根据定义3，这个相等的左右单位元称为单位元，又根据定理1的推论，则这个单位元唯一，与题设矛盾，故得证（这个命题的证明当时我没做笔记，是整理时根据上课的回忆来证明的，不严谨的地方请谅解。其实我觉得自己证得挺严密的，哈哈~~~）**可能很多同学迷惑了，根据定理1和推论，这个“若”就有问题吖~~~请自行翻看定义3。下面是我说一下关于如何构造有两个右单位元的例子。下面请看一个例子。（学无余力同学自行跳过即可，弄不懂也没关系）

**若环R恰有一个右单位元,则R必有单位元（判断正误，并说明理由）**

构造环如下  
{0，e，f，e+f}   
乘法定义为  
e\*f=e  
e\*e=e  
f\*f=f  
f\*e=f  
加法定义为  
e+e=0  
f+f=0  
-----以上给了两个有两个右单位元的例子   
  
下面我们证明  
如果右单位元是唯一的，那么它是单位元。  
设e是右单位元   
若存在r使得   
er!=r  
那么  
er-r+e是右单位元，并且不是e，矛盾   
故e是单位元   
还有加性可测是函数必连续的解答在周民强的实变函数中是找的到。

接着回到课本P70，还要记住“**不是所有的代数系统都有单位元，如<E，\*>，其中E代表偶数。**”

P71的**定理2，推论，定义5**都是重点啊啊啊啊。

注意P71的中间部分定义5下面的一句话“**任意代数系统如果存在则必为幂等元**。”同义转述就是“**单位元一定是幂等元。**”不过，**“幂等元不一定是单位元。**”举例：<Q，\*>中的0是幂等元，但不是单位元。

**下面再补充一个我笔记上的老师上课讲的概念！！！课本没有！！！**

**模n的同余关系Rn**

如n=3， 2 Rn 5。

再来，例如n=3 ，｛[0],[1],[2]｝=Z3，叫做**模3剩余类集**，同理有**模n剩余类集**。

下面是第三小节同态与同构，自己看书，仔细看。

对于基础不太好的同学，我在此补充两个概念。

**对于A到B的f映射，**

**单射：A中集合a、b，有a ≠ b → f(a) ≠ f(b)**

**满射：对于任意a∈B，都在A中有原象**

**双射：既是单射，又是满射**

例3，例4，定理2神马的，都要看啊。定理3到定理7全都要看。

（现在是七点五十，写了一个半小时了，累死我了...55555...乃们！一定要请我吃好吃的~55555...现在舍友开始陆陆续续有起床的了）

**再补充一道题！！！老师上课讲的！！！**

**设<S，\*>是一个半群，且消去律成立，证明：S是可交换半群的充分必要条件是对∀ a，b∈S /\*居然打不出倒写的A，QQ拼音输入法有待改进吖...\*/ ，有（ab）²=a2b² 。**

**证明：由（ab）²=a²b² 得出abab = aabb ,等式两边分别消去第一个a和第四个b，则有ab=ba，故得证。**

第四小节同余关系与商代数不用看。第五小节直积不用看。

下面进入第五章**群**，加油哟~~~希望就在前方 ^0^ ~~~~

定义神马的都先自觉看一遍，一直到P82。

书都没自己看过一遍的，请自行关闭此网页...书都没看过，有什么资格参加世界一流大学的期末考试！！！

**下面列一下概念，看看你能不能都迅速说出其含义和区别：**

**半群，可交换半群，Abel群，群，幺半群，子半群，子幺半群，子群，群的阶。**

**P83的半群构成群的定理不讲。**

**同态一定要考。**

（八点啦~~~啦啦啦~~~太阳公公出来啦~~~我的小台灯也该歇歇啦~~~真心不建议小台灯看书，从早上六点多到现在看得我眼睛有点痛...）

**号外号外~~~！！！**[**http://wenku.baidu.com/view/42e0e47c27284b73f24250cf.html**](http://rrurl.cn/6BAlaw)

**亲们！！！我找到可以打出那些奇奇怪怪数学字符的好东东了~~~详见上面的网址~~~下面我的特殊数学符号都是这么打出来的~~~**

额，好饿，早饭没时间吃了，只吃了一个苹果充饥，后来刷了三个单元读写译上机，还剩三个单元，舍友以斌小童鞋帮我刷的，在此表示感谢~~~以斌奋力帮我刷读写译的时候，我出去匆匆吃了油条和豆腐脑，饿死了...不过外面的雪景真的很漂亮~~~赶紧吃完直接埋葬我大洪楼图书馆，看到十一点半还差四个小节没有看完，果断回宿舍了。出图书馆的时候头一阵阵发晕...天旋地转啊...

继续学术~！

先指出立勋同学对于课本P83的定理2证明的一点看法。

立勋同学觉得，证明中**“f(e)是 H的幂等元，从而是单位元**。”这句话欠妥，在这句话前面加上一句“**∀ x∈G , 有f(e)·f(x)=f(e·x)=f(x)”**

**下面再补充上课老师讲的一道重点题！！！是例题！！！**

**求证：<G，\*>，<H,△>为群，f是G到H的同态，A⊆G，<A，\*>是<G，\*>的子群，证<f(A),△>是<H,△>的子群。**

**证明：只需证 ① f(A)⊆ H，② f(A)≠φ ，③ f(A) 对于△封闭。下面证③：**

**∀y₁，y₂∈f(A) ; ∃ x₁,x₂∈A ； y₁△ y₂=f(x₁)△f(x₂) = f(x₁\*x₂) ；**

**∵x₁\*x₂∈A ∴ f(x₁\*x₂)∈f(A) 故得证 ，再证<f(A),△>是群（证是群的这步此处省略！那些恶心的符号我快疯了...证是群只需用定义的那三个条件即可！！！ 抱歉真的不想写了...）**

**第三节“子群与元素的周期”，这里会出大题！！！**

定义神马的，各位自己看~~~**例4**就是上面补充的那道题，要看。

现在是下午六点，好饿，上次吃饭还是早上的油条豆腐脑。

以下内容难度突然增大，我睡了午觉之后又看了将近两个小时才把下面的六道题看懂。

**下面这六道题，特！别！重！要！！！**

**❶P87例4**

**❷P88定理2 及证明 及推论。**

**❸P89定理3的证明（注意先分两种情况讨论，即周期是有限还是无限；再用“带余式除法”——这个技巧很重要！！！）（元素周期肯定考）**

**❹P90例10，这个往年考过**

**❺P90习题8.书上没有解答，下面给出解答（又是虐心的敲字...T T）：**

**证明：分两种情况，周期有限和周期无限。周期无限很容易证明，只要你智商不捉急就应该会，略。下面证周期有限的。**

**假设|a|=n , 往证|f(a)|=n ,即证**

**(f(a))ⁿ = f(e) → f(a)f(a)f(a)···f(a) = f(e) → f(aⁿ) = f(e)**

**而aⁿ=e ，∴成立**

**假设 存在 0<x<m 使得(f(a))^x = f (e)**

**若(f(a))^x = f(a^x) =f(e) 则 a^x = e ,则|a|≠n，矛盾。**

**❻证明：素数阶循环群中每一个非单位元的元素都是其生成元。（必须会！！！）**

**证明：设G是一个素数阶循环群，其生成元为a，|a|=n（n为素数），e是G的单位元。**

**假设b∈G ，b≠e , (b)≠G ,进一步，设|b|=m , 1＜m＜n ,**

**b^m=e , ∵a为G的生成元，则 ∃ i∈Z , a^i =b (1≤i≤n) ,**

**∴(a^i)^m = e, 即a^im = e ∴n|im**

**又n是素数，∴n|im 不成立。**

**最后一章——环与域，加油！！！！**

**我！要！疯！了！！！**

为了这个离散复习整理，我从早上六点十分忙到现在下午六点半...现在处于崩溃边缘...T T ...

首先，把课本通读一遍，定义神马的都看懂，这个不难。其中，性质的前12条讲了，13-15没讲。

**要明白环的单位元，逆元是谁的单位元和逆元，不会的看P112的中间部分。**

**有个地方容易被忽略，可能导致同学误解，即零元和单位元的区别。注意：在环<R,+,·>中，在<R,+>的单位元中叫零元，在<R,·>中的单位元叫单位元，只是在不同的环境中叫法不一样，实质是一样的。（换个马甲而已...）**

**P113的习题7很可能考，这是最后一节课老师唯一讲的一道题。这道题是道绝对大综合，包括了前面所有的知识！！！**

**我写一下思路(不会画那种｛列出的层次，所以就用编程的思想来表达，即缩进的格数)：**

**❶环**

**①<R，+>为abel群**

**⒈半群**

**⒉幺半群**

**⒊群**

**⒋可交换**

**②<R,x>为半群 → x满足结合律**

**③x对+可分配**

**❷有单位元**

第二小节 整环 除环 域 不是很重要

**零因子是重点，往年总考。要仔仔细细看定义1和例1。(本来到此就应该结束了，不过立勋整理笔记时脑海里闪过了一丝记忆。大家是不是想起了什么？？？请翻回P70！！！倒数第二行！！！P70说情况复杂，留在以后讨论，就是这里！！！零因子！！！)例2也要看。**

至于定义2和定义3，老师说，了解，不考。

**全面结束！！！现在是晚上七点五十，午饭没吃，晚饭没吃，就弄这么个东西，早上六点十分搞到现在...洗澡吃饭~~~！！！啦啦啦啦好开心~~~~**

下面有四个附件，对我的帮助是极大的。**特别感谢梦迪姐的帮助~~！！！**附件2有删节，否则整篇文章超过3万字了...

**[参考资料]**

**附件1：梦迪姐友情提供的往年某离散试卷**

离散试卷

1． 在一棵有2个2度结点，4个3度结点，其余为树叶的树中，应该有几片树叶？

2． 画出图一所示加权图的一棵最小生成树

3． 图一中是否含有Euler回路、Hamilton回路？若有的话，请写出一条相应的回路。

4． 图一中共有几个面？所有面的度数之和是多少？

5． 在图二中，从到共有多少条长度为4的通路？

6． 设<A,\*>到<B,Ñ>是两个代数系统，eÎB是B的单位元。令f:A®B，定义为：对任意的aÎA，f(a)=e。证明A和B两个代数系统同态。

7． 假设T是非平凡的无向树，T中度数最大的顶点有2个，并且它们的度数k大于等于2。证明：T 中至少有片树叶。

8.若G是一个平面图，证明，其中，是G中的顶点数，是G中的边数，是G的面数，是G中的连通分支数。

9.假设A、B、C为任意集合，证明或否定下列命题。

1) 如果，那么B=Æ。

2) 如果A – B = B，那么 A = B = Æ。

3) 如果AB，且BC，则AC。

4) 若A ¹ Æ 并且AB=AC，则B = C。

5) （P(S)表示S的幂集）

1． 假设有如下一个解释：

论域D={1,2}, a = 2, f(x) = x2(mod 2) + 1, P(x,y)：x > y

求在上述解释下公式 "x$y(P(x,a) ®P(f(x),f(y))) 的真值。

2． 证明：(ØP∧(ØQ∧R))∨(Q∧R)∨(P∧R) º R

3． 假设f和g分别是X到Y、Y到Z的函数，并且g°f是一个满射。如果g是一个单射，证明f是一个满射。

4． 符号化下列命题，并证明或否定结论的有效性。所有的年轻人都会操作数据库；所有的老年人都不会操作数据库；有些老年人很爱学习。因此，有些非年轻人很爱学习。（提示：F(x)：x是年轻人；G(x)：x会操作数据库；H(x)：x是老年人I(x)：x很爱学习）

5.设R是集合A上的一个关系，证明：R具有传递性，当且仅当RnÍR，其中n=2,3,4,…。

1、设是自然数集合，定义上的二元关系：

（1）证明是一个等价关系；

（2）求关系的等价类。

2、设、是两个偏序集，定义上的关系如下：

当且仅当且

（1）证明关系是偏序关系。

（2）进一步设，是上的整除关系，，是上的整除关系，画出的Hasse图，并分别列出其极大元、极小元、最大元、最小元。

**附件2：（有删节，否则整篇文章超过3万字了）**

（代数结构部分）

37、设A={2,4,6}，A上的二元运算\*定义为：a\*b=max{a,b}，则在独异点<A,\*>中，单位元是( )，零元是( )。

答：2，6

38、设A={3,6,9}，A上的二元运算\*定义为：a\*b=min{a,b}，则在独异点<A,\*>中，单位元是( )，零元是( )；

答：9，3

（半群与群部分）

39、设〈G,\*〉是一个群，则

(1) 若a,b,x∈G，ax=b，则x=( )；

(2) 若a,b,x∈G，ax=ab，则x=( )。

答： （1） ab （2） b

40、设a是12阶群的生成元， 则a2是( )阶元素，a3是( )阶元素。

答： 6,4

41、代数系统<G,\*>是一个群，则G的等幂元是(　　　　)。

答：单位元

42、设a是10阶群的生成元， 则a4是( )阶元素，a3是( )阶元素。

答：5，10

43、群<G,\*>的等幂元是(　　)，有(　　　)个。

答：单位元，1

44、素数阶群一定是( )群, 它的生成元是( )。

答：循环群，任一非单位元

45、设〈G,\*〉是一个群，a,b,c∈G，则

(1) 若ca=b，则c=( )；(2) 若ca=ba，则c=( )。

答：（1） b (2) b

46、<H,,>是<G,,>的子群的充分必要条件是( )。

答：<H,,>是群 或 " a，b G， abH，a-1H 或" a,b G，ab-1H

47、群＜A,\*＞的等幂元有(　　　)个，是(　　　)，零元有(　　　)个。

答：1，单位元，0

48、在一个群〈G,\*〉中，若G中的元素a的阶是k，则a-1的阶是( )。

答：k

49、在自然数集N上，下列哪种运算是可结合的？（ ）

(1) a\*b=a-b　　(2) a\*b=max{a,b}　(3) a\*b=a+2b　(4) a\*b=|a-b|

答：(2)

50、任意一个具有2个或以上元的半群，它（ ）。

(1) 不可能是群　　(2) 不一定是群

(3) 一定是群 　(4) 是交换群

答：(1)

51、6阶有限群的任何子群一定不是（ ）。

(1) 2阶　　(2) 3 阶 (3) 4 阶 　(4) 6 阶

答：(3)

（半群与群部分）

19、求循环群C12={e,a,a2,…,a11}中H={e,a4,a8}的所有右陪集。

解：

因为|C12|=12，|H|=3，所以H 的不同右陪集有4 个：H，{a,a5,a9},{a2,a6,a10},{a3,a7,a11}。

20、求下列置换的运算：

解：

（1）=

（2）=

==

21、试求出8阶循环群的所有生成元和所有子群。

解：

设G是8阶循环群，a是它的生成元。则G={e,a,a2,..,a7}。由于ak是G的生成元的充分必要条件是k与8互素，故a,a3,a5,a7是G的所有生成元。

因为循环群的子群也是循环群，且子群的阶数是G 的阶数的因子，故G的子群只能是1 阶的、2阶的、4 阶的或8阶的。因为|e|=1,|a|=|a3|=|a5|=8,|a2|=|a6|=8, |a4|=2,且G 的子群的生成元是该子群中a的最小正幂，故G的所有子群除两个平凡子群外，还有{e,a4},{e,a2,a4,a6}。

22、I上的二元运算\*定义为：a,bI，a\*b=a+b-2。试问<I,\*>是循环群吗？解：

<I,\*>是循环群。因为<I,\*>是无限阶的循环群，则它只有两个生成元。1和3是它的两个生成元。因为an=na-2(n-1)，故1n=n-2(n-1)=2-n。从而对任一个kI,k=2-(2-k)=12-k，故1是的生成元。又因为1和3 关于\*互为逆元，故3 也是<I,\*>的生成元。

23、设<G,·>是群，aG。令H={xG|a·x=x·a}。试证：H 是G 的子群。

证明：

c，dH，则对c，dHK，c·a=a·c,d·a=a·d。故(c·d) ·a=c·(d·a)=c·(a·d)=(c·a) ·d=(a·c) ·d=a·(c·d)。从而c·dH。

由于c·a=a·c,且·满足消去律，所以a ·c-1=c-1·a。故c-1H。

从而H 是G的子群。

24、证明：偶数阶群中阶为2 的元素的个数一定是奇数。

证明：

设<G,·>是偶数阶群，则由于群的元素中阶为1 的只有一个单位元，阶大于2 的元素是偶数个，剩下的元素中都是阶为2 的元素。故偶数阶群中阶为2 的元素一定是奇数个。

25、证明：有限群中阶大于2的元素的个数一定是偶数。

证明：

设<G,·>是有限群，则aG，有|a|=|a-1|。且当a 阶大于2时，a-1。故阶数大于2 的元素成对出现，从而其个数必为偶数。

26、试求<N6,+6>中每个元素的阶。

解：

0是<N6,+6>中关于+6的单位元。则|0|=1；|1|=|5|=6，|2|=|4|=3，|3|=2。

27、设<G,·>是群，a,bG，ae，且a4·b=b·a5。试证a·bb·a。

证明：

用反证法证明。

假设a·b=b·a。则a4·b= a3·（a·b）= a3·(b·a)=(a5·b)·a

=(a2·(a·b))·a=（a2·（b·a））·a=((a2·b)·a)·a=(a·(a·b))·(a·a)

=(a·(b·a))·a2=((a·b)·a)·a2 =((b·a)·a)·a2=(b·a2)·a2

=b·(a2·a2)=b·a4。

因为a4·b= b·a5，所以b·a5= b·a4。由消去律得，a=e。

这与已知矛盾。

28、I上的二元运算\*定义为：a,bI，a\*b=a+b-2。试证：<I,\*>为群。

证明：

（1）a,b,cI，(a\*b)\*c=(a\*b)+c-2=(a+b-2)+c-2=a+b+c-4, a\*(b\*c)

=a+(b\*c)-2=a+(b+c-2)-2=a+b+c-4。故(a\*b)\*c= a\*(b\*c)，从而\*满足结合律。

（2）记e=2。对aI，a\*2=a+2-2=a=2+a-2=2\*a.。故e=2是I关于运算\*的单位元。

（3）对aI，因为a\*（4-a）=a+4-a-2=2=e=4-a+a-2=(4-a)\*a。故4-a是a关于运算\*的逆元。

综上所述，<I,\*>为群。

29、设<S,·>为半群，aS。令Sa={ai | iI+ }。试证<Sa,·>是<S,·>的子半群。

证明：

b，cSa，则存在k,lI+，使得b=ak,c=al。从而b·c=ak·al=ak+l。因为k+lI+，所以b·cSa，即Sa关于运算·封闭。故<Sa,·>是<S,·>的子半群。

30、单位元有惟一逆元。

证明：

设<G,>是一个群，e是关于运算的单位元。

若e1,e2都是e的逆元，即e1\*e=e且e2\*e=e。

因为e是关于运算的单位元，所以e1=e1\*e=e=e2\*e=e2。

即单位元有惟一逆元。

31、设e和0是关于A上二元运算\*的单位元和零元，如果|A|>1，则e0。

证明：

用反证法证明。假设e=0。

对A的任一元素a，因为e和0是A上关于二元运算\*的单位元和零元，

则a=a\*e=a\*0=0。即A的所有元素都等于0,这与已知条件|A|>1矛盾。

从而假设错误。即e0。

32、证明在元素不少于两个的群中不存在零元。

证明：（用反证法证明）

设在素不少于两个的群<G,>中存在零元。对aG, 由零元的定义有 a\*=。

<G,>是群，关于\*消去律成立。 a=e。即G中只有一个元素，这与|G|2矛盾。故在元素不少于两个的群中不存在零元。

33、证明在一个群中单位元是惟一的。

证明：

设e1,e2都是群〈G,\*〉的单位元。 则e1=e1\*e2=e2。

所以单位元是惟一的。

34、设a是一个群〈G，\*〉的生成元，则a-1也是它的生成元。

证明：

xG，因为a是〈G，\*〉的生成元，所以存在整数k，使得x=a。

故x=((a))=((a))=(a)。从而a-1也是〈G，\*〉的生成元。

35、在一个偶数阶群中一定存在一个2阶元素。

证明：

群中的每一个元素的阶均不为0 且单位元是其中惟一的阶为1的元素。因为任一阶大于2 的元素和它的逆元的阶相等。且当一个元素的阶大于2 时，其逆元和它本身不相等。故阶大于2 的元素是成对的。从而阶为1的元素与阶大于2 的元素个数之和是奇数。

因为该群的阶是偶数，从而它一定有阶为2 的元素。

36、代数系统<G,\*>是一个群，则G除单位元以外无其它等幂元。

证明：

设e是该群的单位元。若a是<G,\*>的等幂元，即a\*a=a。

因为a\*e=a，所以a\*a=a\*e。由于运算\*满足消去律，所以a=e。

即G除单位元以外无其它等幂元。

37、设<G,>是一个群，则对于a,b∈G，必有唯一的x∈G，使得ax=b。

证明：

因为a-1\*b∈G，且a\*(a-1\*b)=(a\*a-1)\*b=e\*b=b，所以对于a,b∈G，必有x∈G，使得ax=b。

若x1,x2都满足要求。即ax1=b且ax2=b。故ax1=ax2。

由于\*满足消去律，故x1=x2。

从而对于a,b∈G，必有唯一的x∈G，使得ax=b。

38、设半群<S,·>中消去律成立，则<S,·>是可交换半群当且仅当a,bS，（a·b）2=a2·b2。

证明：

a,bS，（a·b）2=(a·b)·(a·b)=((a·b)·a)·b

=(a·(a·b))·b=((a·a)·b)·b=(a·a)·(b·b)=a2·b2;

a,bS，因为（a·b）2=a2·b2，所以(a·b)·(a·b)=(a·a)·(b·b)。故a·((b·a)·b)=a·(a·(b·b))。由于·满足消去律，所以(b·a)·b=a·(b·b)，即(b·a)·b=(a·b)·b。从而a·b=b·a。故·满足交换律。

39、设群<G,＊>除单位元外每个元素的阶均为2，则<G,＊>是交换群。

证明：

对任一aG，由已知可得a\*a=e，即a-1=a。

对任一a,bG，因为a\*b=(a\*b)-1=b-1\*a-1=b\*a，所以运算\*满足交换律。

从而＜G,\*＞是交换群。

40、设\*是集合A上可结合的二元运算，且a,bA,若a\*b=b\*a，则a=b。试证明：

（1）aA,a\*a=a，即a是等幂元；

（2） a,bA,a\*b\*a=a;

（3） a,b,cA,a\*b\*c=a\*c。

证明：

（1）aA,记b=a\*a。因为\*是可结合的，故有b\*a=(a\*a)\*a=a\*(a\*a)=a\*b。由已知条件可得a=a\*a。

（2）a,bA,因为由（1），a\*(a\*b\*a)=(a\*a)\*(b\*a)=a\*(b\*a),

(a\*b\*a)\*a=(a\*b)\*(a\*a)=(a\*b)\*a=a\*(b\*a)。

故a\*(a\*b\*a)=(a\*b\*a)\*a，从而a\*b\*a=a。

（3） a,b,cA,（a\*b\*c）\*（a\*c）=（（a\*b\*c）\*a）\*c=(a\*(b\*c)\*a)\*c

且(a\*c)\*(a\*b\*c)=a\*(c\*(a\*b\*c))=a\*(c\*(a\*b)\*c))。

由（2）可知a\*(b\*c)\*a=a且c\*(a\*b)\*c=c，

故（a\*b\*c）\*（a\*c）=(a\*(b\*c)\*a)\*c=a\*c

且(a\*c)\*(a\*b\*c)= a\*(c\*(a\*b)\*c))= a\*c，

即（a\*b\*c）\*（a\*c）=(a\*c)\*(a\*b\*c)。

从而由已知条件知，a\*b\*c=a\*c。

41、设<G,·>是群，作f:GG,aa-1。证明：f是G的自同构G是交换群。

证明：

设f 是G的自同构。对a，bG，a·b=(b-1·a-1)-1=(f(b) ·f(a))-1=(f(b·a))-1=((b·a)-1)-1=b·a。故运算·满足交换律 ，即G是可交换群。

因为当ab时，a-1b-1，即f(a)f(b)，故f是G到G中的一个单一函数。又对aG，有f(a-1)=(a-1)-1=a。故f是G到G上的满函数。从而f是G到G上的自同构。

对a，bG，因为G是可交换群，故f(a·b)=(a·b)-1=(b·a)-1=a-1·b-1=f(a)·f(b)。故f满足同态方程。

从而f是G 的自同构。

42、若群<G,＊>的子群<H,＊>满足|G|＝2|H|，则<H,＊>一定是群<G,＊>的正规子群。

证明：

由已知可知，G关于H 有两个不同的左陪集H，H1和两个不同的右陪集H，H2。因为HH1=且HH1=G，HH2=且HH2=G，故H1=G-H=H2。

对aG，若aH，则aH=H,Ha=H。否则因为aG-H，故aHH,HaH。从而aH=Ha=G-H。故H是G的不变子群。

43、设H和K都 是G的不变子群。证明：HK也是G 的不变子群。

证明：

因为H和K都 是G的不变子群，所以HK是G 的子群。对aG，hHK，有a·h·a-1a·H·a-1，·h·a-1a·K·a-1。因为H和K都 是G的不变子群，所以a·h·a-1H且a·h·a-1K。从而a·h·a-1HK。故HK是G 的不变子群。

44、设群G的中心为C（G）={aG|xG,a·x=x·a}。证明C（G）是G的不变子群。

证明：

先证C（G）是G的子群。

a,bC（G），对xG,有a·x=x·a ，b·x=x·b。故（a·b）·x= a·(b·x)= a·(x·b)=(a·x)·b=(x·a)·b=x·(a·b), a-1·x=x·a-1。从而a·b，a-1C（G）。 故C（G）是G 的子群。

再证C（G）是G的不变子群。

对aG，hC(G)，记b=a·h·a-1。下证bC(G)。因为hC(G)，所以b=(a·h) ·a-1=（h·a）·a-1=h·(a·a-1)=hC(G)。

故C（G）是G的不变子群。

45、设<G,·>是没有非平凡子群的有限群。试证：G是平凡群或质数阶的循环群。

证明：

若G是平凡群，则结论显然成立。

否则设<G,·>的阶为n。任取aG且ae,记H=（a）(由a生成的G的子群)。显然H{e}，且G没有非平凡子群，故H=G。从而G一定是循环群，且a是G 的生成元。

若n是合数，则存在大于1 的整数k,m，使得n=mk。记H={e,ak,(ak)2,…,(ak)m-1}，易证H是G 的子群，但1<|H|=m<n，故H是G 的非平凡子群。这与已知矛盾。从而n是质数。

故G是质数阶的循环群。

综上所述，G是平凡群或质数阶的循环群。

46、设H和K都是G 的有限子群，且|H|与|K|互质。试证：HK={e}。

证明：

用反证法证明。

若HK{e}。则HK是一个元素个数大于1的有限集。

先证HK也是G的子群，从而也是H和K的子群。

a,b HK,则a,b H且a,bK。因为H和K都 是G的子群，故 a·b,a-1 H且a·b,a-1 K。从而a·b HK,a-1 HK。故HK是G的子群，从而也是H和K的子群。

由拉格朗日定理可知，|HK|是|H|和|K|的因子，这与已知矛盾。

47、素数阶循环群的每个非单位元都是生成元。

证明：

设<G,\*>是p阶循环群，p是素数。

对G中任一非单位元a。设a的阶为k,则k1。

由拉格朗日定理，k是p的正整因子。因为p是素数，故k=p。即a的阶就是p，即群G的阶。故a是G的生成元。

48、若<S,>是可交换独异点，T为S中所有等幂元的集合，则<T,>是<S,>的子独异点。

证明：

ee=e，eT，即T是S的非空子集。

a,bT, <S，>是可交换独异点,

(ab)(ab)=((ab)a)b

=(a(ba))b=（a(ab)）b

=((aa)b)b=(aa)(bb)

=ab,即abT。

故<T,>是<S,>的子独异点。

49、设<G,>是群，且a∈G的阶为n，k∈I，则|ak|＝，其中(k,n)为k和n的最大公因子。

证明：

记p=,q=,｜ak｜＝m。由n和p的定义，显然有(ak)p=e。故mp且m|p。

又由于akm=e，所以由定理5.2.5知，n|km。即p|qm。但p和q 互质，故p|m。

由于p和m都是正整数，所以p=m。即｜ak｜＝。

50、设<G,>是有限群，|G|＝n，则a∈G，|a|n。

证明：

aG，由封闭性及|G|=n可知a,a2,…,an,an+1中必有相同的元素，不妨设为ak=am,k<m。 由消去律得 am-k=e。从而|a|m-kn。

51、设G＝(a)，若G为无限群，则G只有两个生成元a和a-1；

证明：

bG＝(a)，则nI,使b=an。故b=(a-n)-1=(a-1)-n,从而a-1也是G的生成元。

若c是G的生成元，则k,mI，分别满足c=ak和a=cm。从而c= (cm)k= cmk。若km1，则由消去律可知c的阶是有限的，这与|G|无限矛盾。从而km=1，即k=1,m=1或k=-1,m=-1。故c=a或c=a-1。

从而G只有两个生成元a和a-1。

52、设G＝(a)，{e}HG，am是H中a 的最小正幂，则

（1） H＝(am)；

（2） 若G为无限群，则H也是无限群；

证明：

（1）bH, kI, 使得b=ak。令k=mq+r, 0r<m。

则ar=ak-mq=aka-mq=b(am)-q。

因为b,amH, 且HG，所以arH。

由于0r<m，且am是H中a 的最小正幂，故r=0,即k=mq。

从而b=(am)q。故am是H的生成元。

（2）因为{e}H，故H的生成元为am （m0）。因为G是无限群，所以a的阶是无限的，从而am的阶也是无限的，故H也是无限群。

53、设G＝(a)，|G|＝n，则对于n 的每一正因子d，有且仅有一个d阶子群。因此n阶循环群的子群的个数恰为 n的正因子数。

证明：

对n 的每一正因子d，令k=,b=ak, H={e,b,b2,…,bd-1}。

因为|a|=n,所以bd=(ak)d=akd=an=e且|b|=d。

从而H中的元素是两两不同的，易证HG。

故|H|=d。所以是G的一个d阶子群。

设H1是G的任一d阶子群。则由定理5.4.4知，H1＝(am)，其中am是H1中a 的最小正幂，且|H|=。因为|H|=d，所以m==k，即H=H1。从而H是G的惟一d阶子群。

设H是G的惟一的d阶子群。若d=1 ,则结论显然成立。否则H＝(am)，其中am是H中a 的最小正幂。由定理5.4.4知，d=。故d是n的一个正因子。

54、设h是从群<G1,>到<G2,>的群同态，G和G2的单位元分别为e1和e2，则

（1） h(e1)=e2；

（2） aG1，h(a-1)=h(a)-1；

（3） 若HG1，则h(H)G2；

（4） 若h为单一同态，则aG1，|h(a)|=|a|。

证明：

(1) 因为h(e1)h(e1)=h(e1e1)= h(e1)= e2h(e1),所以h(e1)=e2。

(2) a∈G1，h(a)h(a-1)=h(aa-1)= h(e1)= e2,

h(a-1)h(a)=h(a-1a)= h(e1)= e2,故h(a-1)=h(a)-1。

(3) c,d∈h(H),a,b∈H，使得c=h(a),d=h(b)。故cd=h(a)h(b)

=h(ab)。因为HG，所以ab ∈H ，故cd∈h(H)。又c-1=(h(a))-1=h(a-1)且a-1∈H，故c-1∈h(H)。由定理5.3.2知h(H)G2。

(4) 若|a|=n,则an=e1。故(h(a))n=h(an)=h(e1)=e2。从而h(a)的阶也有限，且|h(a)|n。

设|h(a)|=m,则h(am)= (h(a))m= h(e1)=e2。因为h是单一同态，所以am=e1。即|a|m。

故|h(a)|=|a|。

若a的阶是无限的，则类似于上述证明过程可以得出，h(a)的阶也是无限的。

故结论成立。

55、有限群G的每个元素的阶均能整除G的阶。

证明：

设|G|=n，aG，则|a|=m。令H={e,a,a2,…,am-1}。

则H是G的子群且|H|=m。由Lagrange定理知|H|能整除|G|，故a的阶能整除G的阶。

56、证明：在同构意义下，只有两个四阶群，且都是循环群。

证明：

在4阶群 G中，由Lagrange定理知，G中的元素的阶只能是1，2或4。阶为1 的元素恰有一个，就是单位元e.

若G有一个4阶元素，不妨设为a，则G=（a）,即G是循环群 ，从而是可交换群。

若G没有4阶元素，则除单位元e外，G的其余3个阶均为2。不妨记为a,b,c。因为a,b,c的阶均为2，故a-1=a,b-1=b,c-1=c。从而aba, abb, abe,故ab=c。同理可得ac=ca=b, cb=bc=a, ba=c。

57、在一个群<G,\*>中，若G中的元素a的阶是k，即|a|=k，则a-1的阶也是k。

证明：

因为| a |=k，所以ak=e。即（a-1）k=(ak)-1=e。

从而a-1的阶是有限的，且|a-1|k。

同理可证，a的阶小于等于|a-1|。

故a-1的阶也是k。

58、在一个群<G,\*>中，若A和B 都是G的子群。若AB=G，则A=G或B=G。

证明：

用反证法证明。

若AG且BG，则有aA,aB且bB,bA。因为A，B都是G的子群，故a,bG，从而a\*bG。

因为aA,所以aA。若a\*bA,则b= a\*(a\*b)A，这与aB矛盾。从而a\*bA。

同理可证a\*bB。

综合可得a\*bAB=G，这与已知矛盾。从而假设错误，得证A=G或B=G。

59、设e是奇数阶交换群<G,\*>的单位元，则G的所有元素之积为e。

证明：

设G=<{e,a,a,…,a},\*>，n为正整数。

因为G的阶数为奇数2n+1，所以由拉格朗日定理知G中不存在2 阶元素，即除了单位元e以外，G的所有元素的阶都大于2。故对G中的任一非单位元a，它的逆元a不是它本身，且G中不同的元素有不同的逆元。

由此可见，G中的2n个非单位元构成互为逆元的n对元素。因为G 是交换群，故G的所有元素之积可变成单位元和n对互为逆元的元素之积的积，从而结果为e。

60、设S=QQ，Q为有理数集合，\*为S上的二元运算：对任意(a,b)，(c,d)S,有

(a,b)\*(c,d)=(ac,ad+b),

求出S关于二元运算\*的单位元，以及当a0时，(a,b)关于\*的逆元。

解：

设S关于\*的单位元为(a,b)。根据\*和单位元的定义，对(x,y)S,有

(a,b)\*(x,y)=(ax,ay+b)=(x,y), (x,y)\*(a,b)=(ax,xb+y)=(x,y)。

即ax=x,ay+b=y,xb+y=y对x,yQ都成立。解得a=1,b=0。

所以S关于\*的单位元为(1,0)。

当a0时，设(a,b)关于\*的逆元为(c,d)。根据逆元的定义，有

(a,b)\*(c,d)= (ac,ad+b)=(1,0)

(c,d)\*(a,b)= (ac,cb+d)=(1,0)

即ac=1,ad+b=0,cb+d=0。解得c=,d=-。

所以(a,b)关于\*的逆元为(,-)。

61、设<G,\*>是一个群，H、K是其子群。定义G上的关系R：对任意a,b∈G，aRb ó存在 h∈H,k∈K, 使得b=h\*a\*k，则R是G上的等价关系。

证明：

a∈G，因为H、K是G的子群，所以e∈H且e∈K。令h=k=e,则a=e\*a\*a=h\*e\*k,从而aRa。即R是自反的。

a,b∈G，若aRb，则存在 h∈H，k∈K, 使得b=h\*a\*k。因为H、K是G的子群，所以h-1∈H且k-1∈K。故a=h-1\*a\*k-1,从而bRa。即R是对称的。

a,b,c∈G，若aRb,bRc,则存在 h,g∈H，k,l∈K, 使得b=h\*a\*k，c=g\*b\*l。所以c=g\*b\*l=g\*(h\*a\*k)\*l=(g\*h)\*a\*(k\*l)。因为H、K是G的子群，所以g\*h∈H且k\*l∈K。从而aRc。即R是传递的。

综上所述，R是G上的等价关系。

62、设H是G的子群，则下列条件等价：

（1） H是G的不变子群；

（2） a∈G，aHa-1H；

（3） a∈G，a-1HaH；

（4） a∈G，h∈G，aha-1H。

证明：

(1)(2) a∈G，则对h∈H,令h1=aha-1，因为ah aH且Ha=aH，所以h2∈H，使得ah=h2a。故h1=（h2a）a-1=h2H。故 aHa-1H。

(2)(3) a∈G，对h∈H,令h1=a-1ha，则（h1）-1= ah-1a-1。因为h-1∈H，所以（h1）-1= ah-1a-1∈aHa-1。由（2）可知（h1）-1∈H,从而h1H。故a-1HaH 。

(3)(4) 类似于（2）(3)的证明。

(4)(1) a∈G，对b∈aH，则h∈H，使得b=ah。故b=(ah) (a-1a)=(aha-1)a。由于aha-1∈H，所以b∈Ha。即aHHa。

反之对b∈Ha，则h∈H，使得b=ha。故b=(aa-1) (ha)=a(a-1ha)=a(a-1h(a-1)-1)。由于a-1h(a-1)-1∈H，所以b∈aH。即HaaH。

即Ha=aH。从而H是G的不变子群。

63、在半群<G,\*>中，若对a,bG，方程a\*x=b 和y\*a=b都有惟一解，则<G,\*>是一个群。

证明：

任意取定aG，记方程a\*x=a的惟一解为eR。即a\*eR=a。

下证eR为关于运算\*的右单位元。

对bG，记方程y\*a=b的惟一解为y。

<G,\*>是半群，运算\*满足结合律。

b\*eR=(y\*a)\*eR=y\*(a\*eR)=y\*a=b。

类似地，记方程y\*a=a的唯一解为eL。即eL\*a=a。

下证eL为关于运算\*的左单位元。

对bG，记方程a\*x=b的惟一解为x。

<G,\*>是半群，运算\*满足结合律。

eL\*b=eL\*(a\*x)=(eL\*a)\*x=a\*x=b。

从而在半群<G,\*>中, 关于运算\*存在单位元，记为e。

现证G中每个元素关于运算\*存在逆元。

对bG，记c为方程b\*x=e的惟一解。下证c为b关于运算的逆元。记d=c\*b。 则b\*d=(b\*c)\*b=e\*b=b。

b\*e=b,且方程b\*x=b有惟一解，d=e。

b\*c=c\*b=e。从而c为b关于运算的逆元。

综上所述，<G,\*>是一个群。

64、设<G，\*>是群， H和K都是G的子群，令HK={h\*s | s∈K，h∈H}, KH={s\*h |s∈K,h∈H},<HK,\*>，<KH,\*>是G的子群的充分必要条件是HK=KH。

证明：

HK是G的子群。cHK，则c-1HK，故存在aH,bK ,使得c-1=a·b。因为c=（a·b）-1=b-1·a-1。因为H和K都是G 的子群，所以a-1H,b-1K ，即cKH。从而HKKH。 cKH，则存在aH,bK ,使得c=b·a。因为c=（a-1·b-1）-1。因为H和K都是G 的子群，所以a-1H,b-1K ，即a-1·b-1HK。因为HK是G的子群，所以c=（a-1·b-1）-1HK。从而KHHK。

故HK=KH。

HK=KH。对c，dHK，有a1,a2H,b1,b2K ,使得c=a1·b1 ,d=a2·b2。则c·d=( a1·b1)·(a2·b2)=(( a1·b1)·a2)·b2=( a1·(b1·a2))·b2。因为b1·a2KH=KH，所以存在a3H,b3K ,使得b1·a2 =a3·b3。从而c·d=( a1·（b1·a2）·b2=(a1·（a3·b3）)·b2=(a1·a3)·(b3·b2)。因为H和K都是G的子群，故a1·a3H, b3·b2K。从而c·dHK。

又c-1=(a1·b1)-1=b-11·a-11。因为H和K都是G的子群，故a-11H, b-11K。从而c-1KH。因为HK=KH，所以c-1HK。

综上所述，HK是G的子群。

65、设H和K都 是G的不变子群。证明：HK也是G 的不变子群。

证明：

先证HK是G 的子群。

对aHK，有hH，kK，使得a=h·k。因为a=h·k=(h·k·h-1)·h，且K是G 的不变子群，所以h·k·h-1K。故aKH。从而HKKH。

同理可证，KHHK。

故HK=KH。从而HK是G的子群。

下证HK是G的不变子群。

对aG，bHK，有hH，kK，使得b=h·k。故a·b·a-1=a·(h·k)·a-1=(a·h·a-1)·(a·k·a-1)。因为H和K都是G的不变子群，所以a·h·a-1H且a·k·a-1K。从而a·b·a-1HK。故HK是G 的不变子群。

66、设<G,\*>为群，a,b,cG。若a\*b=c\*b\*a,a\*c=c\*a,b\*c=c\*b，且a,b的阶分别为m,n，则c的阶整除m与n的最大公因子(m,n)。

证明：

设c的阶为k。在a\*b=c\*b\*a两边同时右乘b，再由a\*b=c\*b\*a得

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

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

=(c\*b)\*a\*b=…=(c\*b)\*a,

再由b\*c=c\*b及b 的阶为n得

a=a\*b= (c\*b)\*a=(c\*b)\*a=c\*a,

所以c=e。故由元素阶的定义有k|n。

由a\*b=c\*b\*a,a\*c=c\*a,b\*c=c\*b得a\*b=b\*a\*c，两边同时左乘a，再由a\*b=b\*a\*c得

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

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

= a\*b\*(a\*c)=…=b\*(a\*c),

再由a\*c=c\*a及a 的阶为m得

b= a\*b= b\*(a\*c)=b\* a \* c=b\*c,

所以c=e。故由元素阶的定义有k|m。

由此可见，k是m和n的公因子，从而能整除m和n的最大公因子(m,n)。