1. 证：是二元运算

因为 对任意〈a，b〉∈R×R，通过加法可唯一确定一个实数c ＝a＋b，故加法是R×R到R的映射；

1. 证：不是二元运算

某些实数对〈a，b〉不能通过除法唯一确定一个与之相应的实数（比如，2 / 0无意义

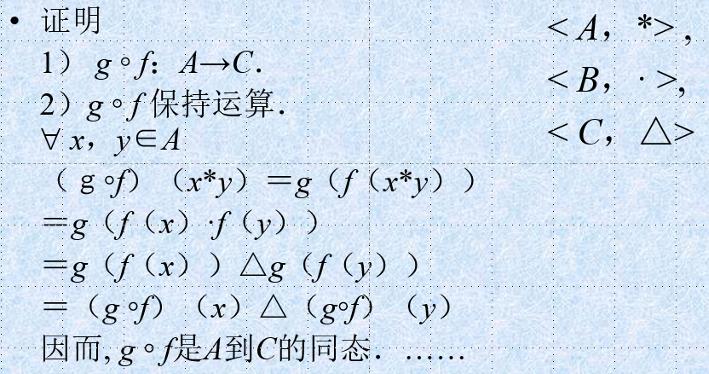
1. 证：代数系统〈*A*，◦〉中既有左单位元*el*，又有右单位元*er*，则 *el*＝*er*．
2. 证：如果单位元存在，则必唯一

因*el*为左单位元，故*el er* ＝ *er* ，又因*er*为右单位元，故*el er* ＝ *el* ，所以*el* ＝ *er*.

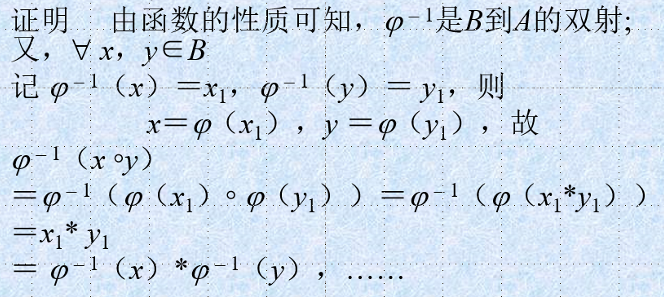
1. 证：设e是代数系统〈A，\*〉单位元， \* 满足结合律，如果a∈A的左逆元b及右逆元c均存在，则b ＝ c．
2. 证：逆元存在则必唯一

b ＝ b e ＝ b（ac）＝（ba）c ＝ ec ＝ c.

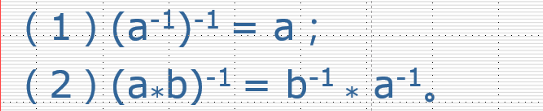
1. 证：f是<A,x>--<B,/>,g是<B,/>--<C,+>,证明:f,g分别是单同态，满同态，同构时，g\*f也必为单同态，满同态，同构



1. 证：代数系统AB在f下同构，则BA在f^(-1)下同构



1. 证：两个代数系统AB同态，A的运算满足结合律/交换律，则B的运算也满足结合律/交换律
2. 证：两个代数系统AB满同态，e是A的单位元/逆元/幂等元，则f(e)为B的单位元/逆元/幂等元、
3. 证：<S,\*>是独异点，如果a,b∈S，有逆元存在



(ab)^-1 = (ab)^-1\*(aa^-1)=(ab)^-1\*(a\*b\*b^-1\*a^-1)=e\*(b^-1\*a^a-1)

1. 证：任何群都没有零元

反证法：零元\*零元的逆元=？

1. 证：设〈G，\*〉为群，则G中消去律成立.

左乘逆元证明左消去律，右乘逆元证明右消去律

1. 证：设〈G，\*〉为群，则单位元e是G中唯一幂等元．

假设a是幂等元，(a^-1) \* a^n = e，

1. 证：设〈G，\*〉，〈H，◦〉是群，f 是G到H的同态．若e 为G的单位元,则 f（e）为H的单位元，且对任意a∈G，有f（a）-1＝ f（a-1 ）．

∵ f（e）◦ f（e）＝ f（e \* e）＝ f（e）.

∴故f（e）是H的幂等元，从而是单位元.

又∵ a∈G

f（a）◦ f（a-1）＝ f（a \* a-1 ）＝ f（e）,

f（ a-1 ）◦ f（a）＝ f（ a-1 \* a）＝ f（e）.

故f（a-1 ）为f（a）的逆，即f(a)-1 = f(a-1)

1. 证：设〈G，\*〉是群，〈H，◦〉是任意代数系统，若存在G到H的满同态, 则<H，◦>必为群．

设 f：G～H，则由满同态的性质知，H中运算 ◦ 满足结合律，

且G的单位元e的象f（e）是H的单位元，

又f为满射，y∈H，x∈G使y ＝ f（x），

y-1＝ f（x）-1＝f（x-1）

所以，〈H，◦〉是群．

1. 证：设〈G，\*〉是一个半群，且
   1. G中有一左单位元 e，使e a ＝ a,a ∈G.
   2. G中任一元素a，均有一“左逆元” ，a-1，使 a-1a＝e.则G为群．

则

a/“左逆元” 也是 “右逆元”；

b/左单位元 也是 右单位元故知Ｇ为群

a/“左逆元” 也是 “右逆元”

a∈G，有 a-1∈G 使a-1a ＝ e，

又对a-1 ∈G，有(a-1)-1 ∈G使(a-1)-1 a-1 ＝ e，

因此，

a a-1 ＝ e（a a-1 ）

＝（（ a-1 ）-1 a-1 ）（a a-1）

＝（ a-1）-1（ a-1 a）a-1

＝（ a-1）-1e a-1

＝（ a-1）-1a-1

＝ e

b/左单位元 也是 右单位元

" a∈G，

a e

＝a（a-1a）

＝（aa-1）a

＝ ea

＝ a.

故e确为右单位元．

1. 证：设〈G，\*〉是半群，如果a，b∈G，方程ax＝b，ya＝b在G中总有解，则G是群．

证G有左单位元、每个元素有“左逆元”。

任取 b∈G 令 y b＝b 的一个解为e，则e b ＝ b．

a∈G，设b x ＝ a的解为c， 即 bc＝a

则 e a ＝ e（bc）＝（e b）c ＝ bc＝a ；

2) 任取a∈G，y a＝e有解，设a' 为一解，则a'a＝e，

由定理４可知，G是群.

1. 证：〈G，\*〉是有限群，则其运算表中每一行（列）都是G中元素的一个全排列．

设 G ＝｛a1，a2，…，an｝，

则其运算表中第i行为

aia1，aia2，…，aian

这是G中元素的一个全排列(只需证明其中任意两项必不相同)：若aiaj＝aiak，j≠k，

则由消去律得aj＝ak，矛盾。

1. 证：有限半群，如果消去律成立则必为群

因为G有限,设G={a1,...,an},任取a,b∈G,只需证明ax=b和xa=b有解即可.  
因为半群对运算封闭,所以aa1,...,aan∈G.这n个元素必然两两不等,否则若aai=aaj(i≠j),根据消去律,ai=aj,矛盾.  
所以aa1,...,aan是a1,...,an的一个排列,而b∈G,所以必存在一个ai(1≤i≤n),使得aai=b,所以ax=b有解,同理xa=b有解

1. 证：设〈G，\*〉，〈H，◦〉为两个群，f是G到H的同态，A是G的子群，则f（A）是H的子群．

y１，y２∈f（A），x１，x２∈A，使

f（x1）＝ y2，f（x2）＝ y2

故 y1◦ y2＝ f（x1）◦ f（x2）＝ f（x1\* x2）∈ f（A）.

故，f（A）对 ◦ 是封闭的，〈f（A），◦〉是代数系统．

由于

f |A：A～f（A）

由上节定理３[1]，〈f（A），◦〉是群。

从而f（A）是H的子群．

1. 证：设G是群，C＝｛a|a∈G， "x∈G：ax＝xa｝，则C为G的子群，（称为群G的中心）

x∈G，e x ＝ x e，故 e∈C，即C非空．设a，b∈C，则 x∈G，

（a b）x＝a(bx)=a(xb)=(ax)b ＝(xa)b ＝ x（a b）.即a b∈C.

又设a∈C，则 x∈G，a x＝x a，两边左乘a –1 ，得x ＝ a–1xa，两边再右乘a–1 ，得 x a –1 ＝ a –1 x. 从而得知a -1 ∈C．故C是子群

1. 证：设H是群〈G，\*〉的非空子集，则

H是G的子群，**当且仅当**

（1）a，b∈H 有a \* b∈H.

（2）a∈H ，a在G中的逆元a–1 ∈H.

必要性: 设H是G的子群，则由定义知（１）必成立．又由定理１知，a在G中的逆元a–1 ∈H．

充分性：设（１）、（２）成立，则由（１）知H 为半群．H 非空，取a∈H，由（２），a–1 ∈H，由（１），a \* a–1 ＝ e∈H，显然，e是H的单位元．

又，a∈H， a–1 ∈H必是a在H中的逆元．故H是子群．

1. 证：设*G*是群，*a*∈*G*，令（*a*）＝｛ *a i* | *i*∈**Z** ｝, 则（*a*）是*G*的子群，（称为由*a* 生成的循环子群．）

显然（a）非空，又 ai，aj∈(a)，

ai aj ＝ ai+j ∈ (a)；

又，a i∈（a）由指数律

( a i ) –1 ＝ a – i ∈（a）

故（a）为G的子群．

1. 证：设H是群G的子群，

1）则H的单位元 e' 就是G的单位元e。

2）对a∈H，a在H中的逆元 a' 就是a在G中的逆元a -1．

1）e'是H的单位元，则e' e' ＝ e' ，故 e' 为G的幂等元，但G的单位元e是唯一幂等元，故e' ＝ e．

2）a∈H， a'为a 在H中的逆元，且e' ＝ e ，故 a' a ＝ a a' ＝ e' ＝ e.

因而，a' 为a在G中的逆元．

1. 证：设〈G，\*〉为群，S是G的非空子集，则

S是G的子群 a，b∈S，a \* b –1 ∈S.

必要性显然；充分性：

S≠∅，取 a∈S，于是, e＝a \* a–1 ∈S. 从而, a ∈S，a –1 ＝ e \* a–1 ∈S.

a , b∈S，由以上所证，b-1 ∈S，故

a \* b ＝ a \* (b–1 )–1 ∈S，

从而S是G的子群．

（用了T23的结论）

1. 证：设*G*是一个群，*a*∈*G*

（1）*a*的周期等于*a*生成的循环子群（*a*）的阶，即| *a* |＝|（*a*）|

（2）若*a*的周期为*n <*∞ ，则*a m* ＝ *e*  *n* | *m*.

分两种情况证明| *a* |＝|（*a*）|

（i）*a*的周期*n*为有限数，往证 （*a*）＝｛*a*0，*a*1，…，*an* -1｝ 且 *a*0，*a*1，…，*an* -1 互不相同．

"*a i*∈（*a*），令*i* ＝ *kn*＋*r*,*k*，*r*∈**Z**，０≤*r*＜*n*

则 *ai* ＝ *a kn+r* ＝ *akn ar* ＝ *ar*

故 *ai*∈｛ *a*0，*a*1，…，*an* -1 ｝

因此 （*a*）Í｛ *a*0，*a*1，…，*an* -1 ｝

又显然｛ *a*0，*a*1，…，*an* -1 ｝Í（*a*），

所以 （*a*）＝｛ *a*0，*a*1，…，*an* -1｝．

下面说明 *a*0，*a*1，…，*an* -1互不相同

若 *a i* ＝ *a j*０≤*i*，*j*＜*n*，*i*≠*j*

不妨设*i*＞*j*，则 *a i – j* ＝ *e*，０＜*i*－*j*＜*n*，与*a*的周期为*n*矛盾．

所以 *a*0，*a*1，…，*an* -1互不相同，

从而 |（*a*）|＝ *n*，即有 | *a*|＝|（*a*）|

（ii）*a*的周期为∞，这时

*a* 1，*a* 2，…，*a i* …

互不相同，故|（*a*）|＝∞，

因此也有| *a* |＝|（*a*）|．

总之，| *a* |＝|（*a*）|成立．

（２）设*a m* ＝ *e*，令

*m* ＝ *kn*＋*r*，　０≤*r*＜*n*

则 *a m* ＝ *a kn+r* ＝ *a kn a r* ＝ *a r*

因此 *a r* ＝ *e*，０≤*r*＜*n*

由于*a*的周期为*n*，故必有*r*＝０，即*n*|*m*．

反之，若*n*|*m*，显然*a m* ＝ *e*.

————————————————————————————————————————————————————————————

1. 证：设〈*G*，\*〉是一个循环群，

1）若*G*是无限群，则〈*G*，\*〉〈**Z**，＋〉

2）若*G*是*n*阶群，则 〈*G*，\*〉  〈**Z***n*，＋*n*〉

１）设*G*是无限循环群，设*a*为其生成元，

*G* ＝（*a*）＝｛…，*a–*2 ，*a*–1 ，*a*0，*a*1，*a*2，…｝

令 *f*：**Z**→*G*，定义如下：

*f* (*i* ) = *a i*,*i*∈**Z .**

显然*f*为满射．下证*f*为单射，*i*，*j*∈**Z** 若 *f*（*i*）＝ *f*（*j*），即*a i* ＝ *a j*，要证 *i*＝*j*．若*i*≠*j*，不妨设*i*＞*j*，则

*a i – j*＝ *e*,*i*－*j*＞０

因此*a*必有有限周期，从而*G*＝（*a*）为有限群，矛盾．所以，*i*＝*j*，从而*f*为单射．总之*f*是双射．

又 *i*，*j*∈**Z，***f*（*i*＋*j*）＝*a i+j*＝*a i* \* *a j* ＝ *f*（*i*）\* *f*（*j*）

即*f*保持运算，从而*f*：**Z** *G*.

２）设*G*为*n*阶循环群，*a*为其生成元，则|*a|=n*，且

*G*＝｛*a*0，*a*1，*a*2，…，*an* -1 ｝

其中*a*0，*a*1，*a*2，…，*an* -1互不相同，令

*f* （［*i*］）= *a i*，［*i*］∈**Z***n*

则显然 *f* 是 **Z***n* 到*G*的满射，又设

*f*（［*i*］）＝*f*（［*j*］），即*a i*＝*a j*，则*a i – j* ＝ *e*，

由周期的性质可知，*n* | *i*－*j* 即*i* ≡ *j* mod *n*.

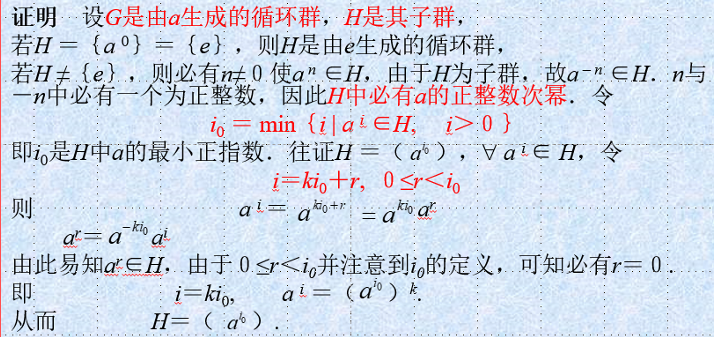
因此［*i*］＝［*j*］. 从而知 *f* 是单射．总之*f*是双射．

下证*f*是同态．［*i*］，［*j*］∈**Z***n*，

*f*([*i*]＋*n*[*j*])＝ *f*([*i*＋*j*])＝*a i+j* ＝ *a i* \* *a j*＝*f*([*i*]) \* *f*([*j*])

因此*f*：**Z***n*  *G*．

1. 证：循环群的子群必为循环群



1. 证：设〈*G*，\*〉是*n*阶循环群，*m*是正整数且 *m* | *n*，则*G*中存在唯一一个*m*阶子群．

由于*m*|*n*，设*n* ＝ *dm*，则（*a d*）*m*＝*a d m* ＝ *a n* ＝*e*.

又,*h*∈**Z**，若０＜*h*＜*m*，则０＜*d h*＜*n*，故由周期的定义,

（*a d*）*h* ＝ *a d h* ≠ *e*.

从而*a d*的周期为*m*，因此，*a d* 生成的循环子群*A*＝（*a d*）是*G*的*m*阶子群．

下面再证*G*中*m*阶子群是唯一的. 在*G*中任取一*m*阶子群*H*，由定理２知，*H*是循环群，设*H*的生成元为*a i* ，即 *H* ＝（*a i*），则 *a i* 的周期为*m*，因此

*a i m*＝（*a i*）*m* ＝ *e*.

所以*n* | *im* ，即 *md* | *im*，可见 *d* | *i*，不妨设*i*＝*kd*，则

*a i* ＝ *a kd* ＝（*ad*）*k*

因此，*a i*∈*A*. 从而，对任何*j*∈**Z**，（*ai*）*j*∈*A*，因而*H**A*，又*H*与*A*＝（*a d*）均有*m*个元素，所以有*H* ＝（*a d*），这样就证明了*G*中有唯一的*m*阶子群．

1. 证：设*R*为有单位元的环，且不只含一个元素，则１≠０．

若１＝０，则 *a* ∈*R*，

*a = a*·１＝ *a*·０＝０.

故*R*只含一个元素０，矛盾．

以后提到有单位元的环时，总指非零环．因此１≠０总成立．

当环*R*的乘法运算满足交换律，即〈*R*，· 〉为（可）交换半群时，称*R*为（可）交换环．

1. 证：对于剩余环〈**Z***n*，＋*n*，×*n* 〉，若*n*不是素数，则**Z***n*中必存在零因子．

**Z***n*中的零元为［０］．因为*n*不是素数，故存在整数*n*1，*n*2，使

*n*＝*n*1*n*2，１＜*n*1≤*n*2＜*n*

因此 ［*n*1］≠［０］，［*n*2］≠［０］，

但 ［*n*1］×*n*［*n*2］＝［０］. 即［*n*1］，［*n*2］是**Z***n*的一对零因子．

1. 证：若环*R*无零因子，则乘法消去律成立．反之亦然．

设*R*中无零因子， *a*≠0, ， 如果 *ab*＝*ac*，则 *ab*－*ac*＝０， *a*（*b*－*c*）＝０. 由于*a*≠０，*R*中无零因子，故 *b*－*c*＝０,即*b* ＝ *c*.

同理*ba*＝*ca*  *b*＝*c* ;

反之，设环*R*中乘法消去律成立，若*R*中有零因子*a*，*b*，使得 *ab*＝０＝ *a*０，由消去律得 *b*＝０，矛盾．故*R*中必无零因子．

1. 证：若*p*是一个素数，则〈**Z***p*，＋*p*，×*p* 〉是一个整环．

若［*i*］×*p*［*j*］=［０］，则

［*ij*］＝［０］，因而 *p*｜*ij*．故*p*｜*i* 或 *p*｜*j*，［*i*］＝［０］ 或 ［*j*］＝［０］

〈**Z***n*，＋*n*，×*n* 〉是整环 *n*为素数

1. 证：设*R*是一个无零因子的有限环，且｜*R*｜≥２，则*R*必为除环．

需要证明〈*R*-{0}，· 〉为群．

由于｜*R*｜≥２，故*R*-{0}非空，又，*R*中不含零因子，故*R*-{0}对 · 封闭，从而〈 *R*-{0} ，· 〉必构成半群，且由定理１知，在该半群中消去律成立，从而〈 *R*-{0} ，· 〉是一个满足消去律的有限半群，故必为群．