第17章 代数系统

中国海洋大学 计算机系

2.

方法：群的定义

证 $\forall a,b\in G, a\circ b=au^{-1}b\in G$,运算o封闭.

$\forall a,b,c\in G$, $(a\circ b)\circ c=(au^{-1}b)\circ c=(au^{-1}b)\,u^{-1}c=au^{-1}(bu^{-1}c)$

$=au^{-1}(b\circ c)=a\circ(b\circ c)$,满足结合律.

$a\circ u=au^{-1}u=a=uu^{-1}a=u\circ a$，$u$是关于运算o的单位元.

设a^{-1} 是群G中a的逆元,e是群G的单位元,则对于运算o有

$a\circ(ua^{-1}u)=au^{-1}(ua^{-1}u)=u$， $(ua^{-1}u)\circ a=(ua^{-1}u)\,u^{-1}a=u$

因此G中任意元素a关于运算o的逆元是$ua^{-1}u$.

故<G, o>是群.

Exercise 3

3. 设G是整数加群<Z,+>,在G内定义°运算如下:

$\forall a,b,c\in G, a\circ b=a+b-2$,证明G关于°运算构成群.

证: $\forall a,b,c\in G, a\circ b\in G$,

显然运算°在G上封闭。

$(a\circ b)\circ c=(a+b-2)+c-2=a+(b+c-2)-2=a\circ(b\circ c)$,

运算°满足结合律。

$a\circ 2=a+2-2=a$, $2\circ a=2+a-2=a$.所以2是运算°的单位元。

$a\circ(4-a)=a+4-a-2=2$, $(4-a)\circ a=4-a+a-2=2$.所以$a^{-1}=4-a$.

综上所述<G, °>是群。

Exercise 4

证 设群G的单位元是e,元素x的逆元是x^{-1}.

$\forall a,b\in G, a*b=ba\in G$,因此运算*在G上封闭.

$\forall a,b,c\in G, (a*b\ )*c=(ba)*c=cba=a*(cb)=a*(b*c)$

因此运算*在G上满足结合律.

$\forall a\in G, a*e=ea=a,\ e*a=ae=a$,所以运算*在G上的单位元是$e$.

$a*a^{-1}=e,\ a^{-1}*a=e$,所以G中任意元素a关于运算*的逆元是a^{-1}.

总上所述,<G,*>是群.

Exercise 6

- 证明 $(ab)^2=a(ba)b=aabb$

因为群满足消去律，所以有$ba=ab$.

9

方法：$|a|=r,|b|=k,|a|=|b| \Leftrightarrow r|k,k|r \Leftrightarrow a^k=e,\ a^r=e$

证 (1) 设$|b^{-1}ab|=r,|a|=k$

$(b^{-1}ab)^k=b^{-1}a^kb=e$,因此$r|k$

$a=(b^{-1})^{-1}(b^{-1}ab)b^{-1}$,故$k|r$.

因此有$|b^{-1}ab|=|a|$.

(2) 设$|ab|=r,|ba|=k$

$(ab)^{k+1}=a(ba)^kb=ab$，由消去律得$(ab)^k=e$,所以$r|k$

$(ba)^{r+1}=b(ab)^ra=ba$，由消去律得$(ba)^r=e$,所以$k|r$

故$|ab|=|ba|$

(3)设$|abc|=r$，$|bca|=s$，$|cab|=t$

$(abc)^{s+1}=a(bca)^{s}bc=abc \Rightarrow (abc)^{s}=e$，故$r|s$

$(bca)^{r+1}=bc(abc)^{r}a=bca \Rightarrow (bca)^{r}=e$，故$s|r$

所以$|abc|=|bca|$

$(bca)^{t+1}=b(cab)^{t}ca=bca \Rightarrow (bca)^{t}=e$，故$s|t$

$(cab)^{s+1}=ca(bca)^{s}b=cab \Rightarrow (cab)^{s}=e$，故$t|s$

所以$|bca|=|cab|$

(4) $a^{m}b^{n-2}=(a^{m}b^{n})b^{-2}=bab^{-2}$,

由(1)知，$| a^{m}b^{n-2}|=|bab^{-2}|=|b^{-1}(ba\, b^{-2})b|=|ab^{-1}|$

(或者由(2)知，$| a^{m}b^{n-2}|=|bab^{-2}|=| (ab^{-2})b|=|ab^{-1}|$

$a^{m-2}b^{n}=a^{-2}(a^{m}b^{n}) = a^{-2}ba$,

由(2)知，$| a^{m-2}b^{n}|= |a^{-2}ba|=|a(a^{-2}b)|=| a^{-1}b|$

11

设G是非交换群,则G中存在者非单位元a和b,$a \neq b$且$ab=ba$.

证 非交换群中必存在阶大于2的元素。

否则群中所有元素的阶都小于等于2,即$\forall x \in G$,$x^2=e$,从而群必然是交换群,矛盾.

设$|c|>2$,又因为$x^2=e \Leftrightarrow x=x^{-1}$,

有$c^2 \neq e \Leftrightarrow c \neq c^{-1}$,且$cc^{-1}= c^{-1}c$,

令$a=c$,$b=c^{-1}$,即得。

11

设G是非交换群,则G中存在者非单位元a和b,$a\neq b$且$ab=ba$.

证 只需要证明存在元素a,$a\neq a^{-1}$.

假设任意元素x,都有$x=x^{-1}$,则$x^2=e\Leftrightarrow x=x^{-1}$,即G是交换群,与已知矛盾.

所以存在元素a,$a\neq a^{-1}$,且$aa^{-1}= a^{-1}a$, 令$b=a^{-1}$,即得

11.

解 任取$<a,b> \in Q\times Q, <c,d> \in Q\times Q, <e,f> \in Q\times Q$

$<a,b>\circ<c,d>=<ac,ad+b>$, $<c,d>\circ<a,b>=<ca,cb+d>$

由于$<ac,ad+b>\neq<ca,cb+d>$,故运算$\circ$不满足交换律.

$(<a,b>\circ<c,d>)\circ<c,d>=<ac,ad+b>\circ<c,d>=<acc,acd+ad+b>$

$<a,b>\circ(<c,d>\circ<c,d>)=<a,b>\circ<cc,cd+d>=<acc,a(cd+d)+b>$

$=<acc,acd+ad+b>$

故满足结合律.

令$<a,b>\circ<x,y>=<a,b>\Rightarrow<ax,ay+b>=<a,b>\Rightarrow a=ax,b=ay+b$

$\Rightarrow x=1,y=0$

$<a,b>\circ<1,0>=<a,b>=<1,0>\circ<a,b>$

所以$<1,0>$是单位元.

11 (续)

令$\langle a,b\rangle \circ \langle x,y\rangle=\langle x,y\rangle \Rightarrow \langle ax,ay+b\rangle=\langle x,y\rangle$

$\Rightarrow ax=x, ay+b=y \Rightarrow x=1$, y是a,b的函数

所以不存在零元.

令$\langle a,b\rangle$的逆元是$\langle x,y\rangle$,有

$\langle a,b\rangle \circ \langle x,y\rangle=\langle 1,0\rangle \Rightarrow \langle ax,ay+b\rangle=\langle 1,0\rangle$

$\Rightarrow ax=1, ay+b=0 \Rightarrow x=1/a, y=-b/a$

$\langle 1/a,-b/a\rangle \circ \langle a,b\rangle=\langle 1,0\rangle$

故当$a \neq 0$时,$\langle a,b\rangle$可逆,逆元是$\langle 1/a,-b/a\rangle$.

13

分析：判定封闭性、单位元、逆元

解 (1) 构成子群；

(2) 构成子群

(3) 不能构成群，因为不封闭

(4) 构成子群

Exercise 14

14.设G是群,$a\in$G且$a^2=e$,令H=$\{x|x\in G\wedge xa=ax\}$,
证明H是G的子群.

证 设群G的单位元是e,元素x的逆元是x^{-1}.

$ea=e=ae \Rightarrow e\in H \Rightarrow H\neq\varnothing$

$\forall x,y\in H,\ a^2=a \Rightarrow a^{-1}=a$

$a(xy^{-1})=(ax)y^{-1}=(xa)y^{-1}=x(ay^{-1})=x(ya^{-1})^{-1} = x(ya)^{-1}$

$= x(ay)^{-1}= x(y^{-1}a^{-1}) = x(y^{-1}a) = (xy^{-1})a$

所以$xy^{-1}\in H$

所以H是G的子群.

Exercise 15

解 只有一个子群的： $<\{e\},*>$

只有两个子群的：素数阶循环群，

$<Z_3,+_3>$; 子群是$\{0\},Z_3$

只有三个子群的：p^2阶循环群，p为素数，

$<Z_4,+_4>$; 子群是$\{0\},<2>,Z_3$

16

证 必要性.

任取$xy\in H_1H_2$，$(xy)^{-1}\in H_1H_2$，令$(xy)^{-1}=x'y'$，

$xy=(x'y')^{-1}=y'^{-1}x'^{-1}\in H_2H_1$.

所以$H_1H_2\subseteq H_2H_1$.

任取$yx\in H_2H_1$，$(yx)^{-1}=x^{-1}y^{-1}\in H_1H_2$，

$yx=(x^{-1}y^{-1})^{-1}\in H_1H_2$

所以$H_2H_1\subseteq H_1H_2$.

综上, $H_1H_2=H_2H_1$.

充分性.

$\forall\ h_1h_2 \in \mathrm{H_1H_2},\ h_3h_4 \in \mathrm{H_1H_2},\ h_4^{-1} \in \mathrm{H_2},\ h_3^{-1} \in \mathrm{H_1}$

$(h_1h_2)(h_3h_4)^{-1}=(h_1h_2)(h_4^{-1}h_3^{-1})$,

$h_4^{-1}h_3^{-1} \in \mathrm{H_2H_1},\ \mathrm{H_1H_2}=\mathrm{H_2H_1} \Rightarrow h_4^{-1}h_3^{-1} \in \mathrm{H_1H_2}$

令$h_5\ h_6= h_4^{-1}\ h_3^{-1} \in \mathrm{H_1H_2}$，

$(h_1h_2)(h_3h_4)^{-1}=(h_1h_2)(h_5\ h_6) =h_1(h_2h_5)\ h_6$

$h_2h_5 \in \mathrm{H_2H_1} \Rightarrow \mathrm{h_2h_5} \in \mathrm{H_1H_2}$，令$h_7h_8= h_2h_5 \in \mathrm{H_1H_2}$

$(h_1h_2)(h_3h_4)^{-1}= h_1(h_7h_8)\ h_6= (h_1h_7)\ (h_8\ h_6)$

$h_1h_7 \in \mathrm{H_1}$，$\mathrm{h_8h_6} \in \mathrm{H_2}$，

所以$(h_1h_2)(h_3h_4)^{-1} \in \mathrm{H_1H_2}$.

因此$\mathrm{H_1H_2}$是G的子群.

或者

$\forall\ h_1h_2 \in H_1H_2,\ h_3h_4 \in H_1H_2,\ h_4^{-1} \in H_2,\ h_3^{-1} \in H_1$

$(h_1h_2)(h_3h_4)^{-1} = (h_1h_2)(h_4^{-1}h_3^{-1}) = h_1h_2h_4^{-1}h_3^{-1},$

$h_2h_4^{-1} \in H_2,\ h_2h_4^{-1}h_3^{-1} \in H_2H_1,$

$H_1H_2 = H_2H_1 \Rightarrow h_2h_4^{-1}h_3^{-1} \in H_1H_2$

令$h_5\, h_6 = h_2h_4^{-1}h_3^{-1} \in H_1H_2,$

$(h_1h_2)(h_3h_4)^{-1} = h_1h_5h_6$

令$h_1h_5 = h_7 \in H_1,\ h_7h_6 \in H_1H_2$

所以$(h_1h_2)(h_3h_4)^{-1} \in H_1H_2$.

因此H_1H_2是G的子群.

19

解（1）与15互质的所有正整数为1,2,4,7,8,11,13,14

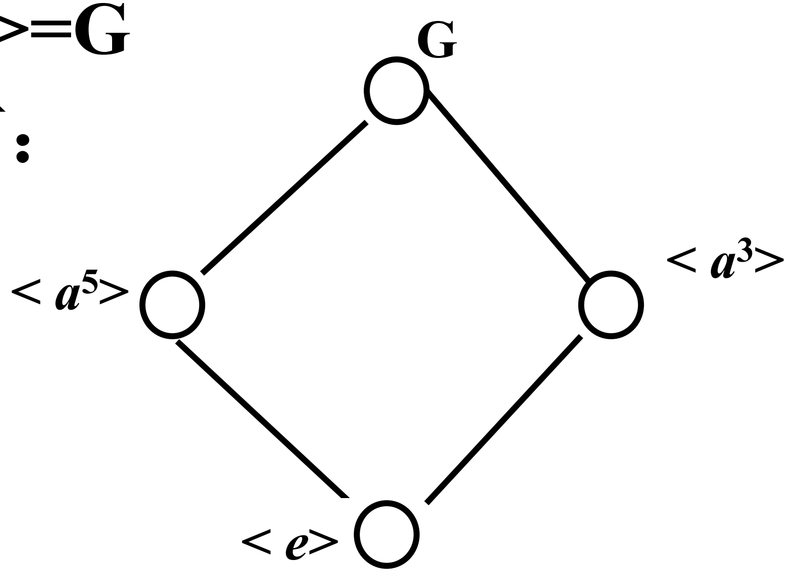
所有生成元是$a, a^2, a^4, a^7, a^8, a^{11}, a^{13}, a^{14}$.

（2）15的正整数因子有1,3,5,15.

$a^{15}=e, a^{15/3}= a^5, a^{15/5}= a^3, a^{15/15}= a,$

子群有$<e>=\{e\}$，$<a^5>=\{ e, a^5, a^{10}\}, <a^3>=\{ e, a^3, a^6, a^9, a^{12}\}$，$<a>=G$

子群格如下：



20

证 因为$<a>$,$<b>$是G的子群，故$e\in<a>\cap<b>$.

假设存在$x\in<a>\cap<b>$, $x\neq e$, 因为$|a|=p$是素数，所以$|<a>|=p$为素数, 故x是子群$<a>$的生成元，设$a=x^t$。

又$x\in<b>$, 由于$<b>$是群, 运算封闭, 故$a=x^t\in<b>$，这与已知矛盾。

分析：$|a|=p$,p为素数，那么$<a>$中的所有非单位元都是生成元。这是因为：对于任何小于p且与p互质的数n，都有a^n是$<a>$的生成元。又p是素数，所以n可以是小于p的所有正整数。因此a^n（$1\leq n\leq p$）是$<a>$的生成元。

24.

解：

（1）$\sigma\tau=(135)(24)$, $\tau\sigma=(124)(35)$, $\sigma^{-1}=(125)(34)$

$\tau^{-1}=(13254)$

（2）$\sigma=(152)(34)=(12)(15)(34)$

$\tau=(14523)=(13)(12)(15)(14)$

26.

- 解：

（1）$\sigma=(12354)$, $\sigma^{-1}=(14532)$,$\tau=(15423)$

则方程$\sigma x=\tau$的解是$x=\sigma^{-1}\tau＝(134)$

方程$y\sigma=\tau$的解是$y=\tau\sigma^{-1}=(125)$

(2) S_5的单位元是恒等函数(1)，又因为$\sigma^2=(13425)$, $\sigma^3=(15243)$, $\sigma^4=(14532)$, $\sigma^5=(1)$,所以$|\sigma|=5$。

$\tau^2=(14352)$, $\tau^3=(12534)$, $\tau^4=(13245)$, $\tau^5=(1)$,所以$|\tau|=5$

27.

27. 在S_4中取子群H=<(1234)>,写出H在S_4中的全部右陪集.

解 S_4中的全部元素有：

(1), (1 2), (1 3), (1 4), (2 3),(2 4),(3 4), (2 3 4),(2 4 3),

(1 3 4),(1 4 3),(1 2 4),(1 4 2),(1 2 3),(1 3 2), (1 2 3 4),

(1 2 4 3),(1 2)(3 4),(1 3 2 4),(1 3 4 2),(1 3)(2 4),

(1 4)(2 3),(1 4 2 3),(1 4 3 2)

H={(1),(1 2 3 4),(1 3)(2 4),(1 4 3 2)}

H(1 2)={(1 2),(1 3 4),(1 4 2 3),(2 4 3)}

H(1 3)={(1 3),(1 4)(2 3),(2 4),(1 2)(3 4)}

H(1 4)={(1 4),(2 3 4),(1 2 4 3),(1 3 2)}

H(2 3)={(2 3),(1 2 4),(1 3 4 2),(1 4 3)}

H(3 4)={(3 4),(1 2 3),(1 3 2 4),(1 4 2)}

28

解 $\forall \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G, \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} \in G,$ 有 $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix}$

$$= \begin{pmatrix} \frac{a'}{a} & \frac{b'}{a} - \frac{b}{a} \\ 0 & 1 \end{pmatrix} \in H \Leftrightarrow \frac{a'}{a} = 1 \Leftrightarrow a = a'$$

所以 $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} \in H \Leftrightarrow \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} H = \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} H \Leftrightarrow a = a'$

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} H = \{ \begin{pmatrix} a & at+b \\ 0 & 1 \end{pmatrix} \mid t \in Q \} = \{ \begin{pmatrix} a & p \\ 0 & 1 \end{pmatrix} \mid p \in Q \},$$

所以不同的左陪集为

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} H = \{ \begin{pmatrix} a & p \\ 0 & 1 \end{pmatrix} \mid p \in Q \}, \quad a \neq 0, a \in Q$$

30

证 $e \in H_1$, $e \in H_2$,所以有$e \in H_1 \cap H_2$

设$x \in H_1 \cap H_2$,则$|x| \mid r$， $|x| \mid s$

由于$(r,s)=1$,因此$|x|=1$,即$x=e$.

故$H_1 \cap H_2=\{e\}$.

或者:

$e \in H_1$, $e \in H_2$,所以有$e \in H_1 \cap H_2$

$H= H_1 \cap H_2$,显然H是H_1的子群,H也是H_2的子群,

由拉格朗日定理得$|H| \mid r$,$|H| \mid s$,又$(r,s)=1$,所以$|H|=1$,

因此$H=H_1 \cap H_2=\{e\}$.

31.

证 任取$x\in G$，$x\neq e$, $|x|\mid p^m$,$|x|\neq 1$.所以$|x|=p^k$, $1\leq k\leq m$.

若$k=1$,则<x>为p阶子群.

若$k>1$, 令$y=x^{p^{k-1}}$,则

$$y^p=(x^{p^{k-1}})^p=x^{p^k}=e.$$

显然$|y|=p$, <y>是p阶子群。

32.

32.设G是有限群,K是G的子群,H是K的子群.

证明[G:H]=[G:K][K:H]

证 |G|=|K|[G:K]，[G:K]=|G|/|K|

|K|=|H|[K:H], |H|=|K|/[K:H]

由于H≤K, K≤G,易知H≤G,

所以[G:H]=|G|/|H|=[G:K][K:H]

附加题

- 设G＝<Z,+>是整数加群。

  1）说明$3Z=\{3k|k\in Z\}$是G的正规子群；

  2）求<Z/3Z,*>,并运算*的运算表。

1）证 任取$3n_1,3n_2\in 3Z$,

$3n_1+(3n_2)^{-1}=3n_1+(-3n_2)=3(n_1-n_2)\in 3Z$,所以3Z是G的子群。

由于运算+满足交换律，所以3Z是正规子群。

或者：任取$g\in Z$, $3n\in 3Z$,则

$g+(3n)+g^{-1}=g+(3n)+(-g)=3n\in 3Z$，

所以3Z是G的正规子群。

2) $3Z+0=3Z=[0]$, $3Z+1=\{3k+1|k\in Z\}=[1]$,

$3Z+2=\{3k+2|k\in Z\}=[2]$,

$Z/3Z=<\{[0],[1],[2]\},*>$,

运算表如下

*	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

42.

- 证明 设G=<a>是循环群，H是G的子群，所以H是循环群，令H的生成元为a^k,k是H中最小的幂指数。

  任取$a^s \in$G,$a^{kt} \in$H,则$a^s a^{kt}(a^s)^{-1}=a^{s+kt-s}=a^{kt} \in$H,

所以H是G的正规子群，由于H的任意性，得证。

提示：由正规子群的判定定理得证

46.

(1) 证 先证H是G的子群.

单位矩阵I,$|I|=1>0$,所以$I\in H$, 因此$H\neq\varnothing$.

任取$x,y\in H$, $|x|>0,|y|>0$, 因此$|xy^{-1}|=|x|/|y|>0$, 所以H是G的子群。

再证明H是G的正规子群.

任取$g\in G,n\in H$,有$|n|>0,|gng^{-1}|=|g||n|/|g|=|n|>0$. 故而$gng^{-1}\in H$,因此H是G的正规子群。

(2) 当$a\in H$时，$Ha=H$

任取$a,b\in G-H$,$|a|<0,|b|<0$,有 $|ab^{-1}|=|a|/|b|>0$,所以$ab^{-1}\in H\Leftrightarrow Ha=Hb=G-H$,所以$G/H=\{H,G-H\}$, $[G:H]=2$

47.

（1）证明 $\forall A,B\in G_1, \varphi(AB)=|AB|=|A||B|=\varphi(A)\,\varphi(B)$

所以φ是G_1到G_2的同态映射。

（2）因为A是n阶有理数矩阵，所以$|A|$是非零有理数，故$\varphi(G_1)=Q-\{0\}$

G_1的单位元是n阶单位阵I，G_2的单位元是1，

$\ker\varphi=\{A|A\in G_1, \varphi(A)=|A|=1\}$

Exercises 48

证: 设V_1=<Q,+>,V_2=<Z,+>,假设f是从V_1到V_2的非零同态, 则有

存在$x\in Q$,使$f(x)=y\neq 0, y\in Z$

取$m\in Z^+$,m不整除y

$y=f(x)=f(m(x/m))=f(x/m)+f(x/m)+\ldots f(x/m)$

$=mf(x/m)$

则有$f(x/m)=y/m\notin Z$,与f的值域是Z矛盾。

Exercises 48

或者

证 设$V_1=<Q,+>$,$V_2=<Z,+>$,假设f是从V_1到V_2的非零同态, 则有

存在$x\in Q$,使$f(x)=y\neq 0,y\in Z$

若$y>0$,令$t=f(x/2y)$,则$t\in Z$,且

$y=f(x)=f(x/2y)+f(x/2y)+\ldots f(x/2y)=2yt$

所以$t=1/2$,与$t\in Z$矛盾.

若$y<0$,令$m=-y$,$m\in Z^+$,$m=-f(x)=f(-x)$.令$t=f(-x/2m)$,同样可以得到$t=1/2$,与$t\in Z$矛盾.

Exercises 49

49. 设φ_1是群G_1到G_2的同构,设φ_2是群G_2到G_3同构,证明$\varphi_2\circ\varphi_1$是群G_1到G_3的同构.

证明 显然$\varphi_2\circ\varphi_1$是从G_1到G_3的双射函数.

$\forall x,y\in G_1$, $\varphi_2\circ\varphi_1(xy)=\varphi_2(\varphi_1(xy))=\varphi_2(\varphi_1(x)\ \varphi_1(y))$

$$=\varphi_2(\varphi_1(x))\ \varphi_2(\varphi_1(y))=\varphi_2\circ\varphi_1(x)\ \varphi_2\circ\varphi_1(y)$$

因此$\varphi_2\circ\varphi_1$是群G_1到G_3的同构.

50

- 证 因为φ是从G_1到G_2的同构，所以φ^{-1}是从G_2到G_1的双射。

任取$x,y\in G_2$,必存在$a,b\in G_1$,使得$\varphi(a)=x$, $\varphi(b)=y$,

所以$\varphi^{-1}(x)=a$, $\varphi^{-1}(y)=b$,

$\varphi^{-1}(xy)=\varphi^{-1}(\varphi(a)\ \varphi(b))=\varphi^{-1}(\varphi(ab))=ab=\varphi^{-1}(x)\ \varphi^{-1}(y)$

令e_1,e_2分别是G_1和G_2的单位元，$\varphi(e_1)=e_2$,所以$\varphi^{-1}(e_2)=e_1$.

$\varphi^{-1}(x^{-1})=\varphi^{-1}(\varphi(a)^{-1})=\varphi^{-1}(\varphi(a^{-1}))=a^{-1}=\varphi^{-1}(x)^{-1}$.

总上所述, φ^{-1}是从G_2到G_1的同构

Exercises 51

51. 设φ是群G_1到G_2的同态映射,证明

（1）若H是G_2的子群,则$\varphi^{-1}(H)$是G_1的子群.

（2）若H是G_2的正规子群,则$\varphi^{-1}(H)$是G_1的正规子群.

证 (1) 设G_1和G_2的单位元分别为e_1, e_2,显然$e_2 \in H$,

$\varphi(e_1)=e_2 \in H \Rightarrow e_1 \in \varphi^{-1}(e_2) \land \varphi^{-1}(e_2) \subseteq \varphi^{-1}(H)$,故$\varphi^{-1}(H) \neq \varnothing$.

$\forall x,y \in \varphi^{-1}(H)$, $\exists s,t \in H$,使得$s=\varphi(x)$, $t=\varphi(y)$

$\varphi(xy^{-1})= \varphi(x)\ \varphi(y^{-1})=st^{-1} \in H$

所以$xy^{-1} \in \varphi^{-1}(H)$，因此$\varphi^{-1}(H) \leq G_1$.

(2) 由(1)知, $\varphi^{-1}(H)\le G_1$.下面证$\varphi^{-1}(H)$是G的正规子群.

$\forall g\in G_1, n\in\varphi^{-1}(H)$,

令$m=\varphi(n)\in H, t=\varphi(g)\in G_2$,有

$\varphi(gng^{-1})=\varphi(g)\varphi(n)\varphi(g^{-1})=tmt^{-1}$,

因为H是G_2的正规子群,故

$tmt^{-1}\in H\Rightarrow \varphi(gng^{-1})\in H\Rightarrow gng^{-1}\in\varphi^{-1}(H)$

得证.

53.

证 H_1是G_1的子群,所以$\varphi(H)$是G_2的子群.根据Lagrange定理有$|\varphi(H)| \mid G_2$.

根据同态基本定理有

$$\varphi(H) \cong H/\ker(\varphi\restriction H) \Rightarrow |\varphi(H)| = |H/\ker(\varphi\restriction H)|$$

$$= [H:\ker(\varphi\restriction H)] = |H|/|\ker(\varphi\restriction H)|$$

所以$|\varphi(H)| \mid |H|$.

由于 $(|H|,|G_2|)=1$,因此$|\varphi(H)|=1$,即$\varphi(H)=\{e\}$.

故而,$H \subseteq \ker\varphi$.

Exercises 55

55. 设φ是群G_1到G_2的满同态,N是G_1的正规子群,且$\ker\varphi\subseteq N$.证明$G_1/N\cong G_2/\varphi(N)$.

证明 方法一：利用同态基本定理

因为N是G_1的正规子群,所以$\varphi(N)$是G_2的正规子群.

令$f:G_1\to G_2/\varphi(N)$, $f(x)=\varphi(N)\varphi(x)$

下面证明f是G_1到$G_2/\varphi(N)$的满同态.

$\forall\, x,y\in G_1$, $f(xy)=\varphi(N)\varphi(xy)=\varphi(N)\varphi(x)\varphi(y)$

$=(\varphi(N)\varphi(x))(\varphi(N)\varphi(y))=f(x)\,f(y)$

因此f是G_1到$G_2/\varphi(N)$的同态.

$\forall\varphi(N)y\in G_2/\varphi(N)$, $y\in G_2$,因为φ是群G_1到G_2的满同态,

所以$\exists x, x\in G_1$,使得$\varphi(x)=y$,即$\varphi(N)y=\varphi(N)\varphi(x)=f(x)$.

综上所述，f是G_1到$G_2/\varphi(N)$的满同态.

下面证明ker$f$=N.

$G_2/\varphi(N)$的单位元是$\varphi(N)$.

$\ker f=\{x|f(x)=\varphi(N)\varphi(x)=\varphi(N)\}=\{x|\varphi(x)\in\varphi(N)\}$

下面证明$x\in N$.假设$x\notin N$且$\varphi(x)\in\varphi(N)$,

则$\exists y, y\in N$, $\varphi(x)=\varphi(y) \in\varphi(N), Ny=N$

因为$\varphi(N)$是G_2的正规子群,所以

$\varphi(x)\varphi(y)^{-1}=e_2\Rightarrow \varphi(xy^{-1})=e_2\Rightarrow xy^{-1}\in\ker\varphi\Rightarrow xy^{-1}\in N$

$\Rightarrow x\in Ny\Rightarrow x\in N$,与$x\notin N$矛盾.

因此$\ker f=\{x|f(x)=\varphi(N)\} =\{x|\varphi(x)\in\varphi(N)\}=\{x|x\in N\}=N$

由同态基本定理可知：$G_1/\ker f\cong f(G_1)$，其中

$\mathrm{Ker}f=N, f(G_1)=G_2/\varphi(N)$,所以$G_1/N\cong G_2/\varphi(N)$.

方法二

构造函数 f: $G_1/N \to G_2/\varphi(N)$,

$\forall x \in G_1, f(Nx)=\varphi(N)\varphi(x)$

证明f是良定义的、是双射函数、是同态.

Exercises 56

证：H,K是G的正规子群,易证HK也是G的正规子群.

先证HK=KH.

$\forall x\mathrm{K},\ x\mathrm{K}\in \mathrm{HK}\Rightarrow x\mathrm{K}=\mathrm{K}x \Rightarrow x\mathrm{K}\in \mathrm{KH}$,所以$\mathrm{HK}\subseteq \mathrm{KH}$

$\forall x\mathrm{H},\ x\mathrm{H}\in \mathrm{KH}\Rightarrow xH=Hx \Rightarrow xH\in HK$,所以$KH\subseteq HK$

由习题16可知,HK是G的子群

$\forall g\in \mathrm{G}, xy\in \mathrm{HK}$,所以有$gxg^{-1}\in \mathrm{H},\ gyg^{-1}\in \mathrm{K}$,

$gxyg^{-1}=(gxg^{-1})(gyg^{-1})\in \mathrm{HK}$,所以HK是G的正规子群.

设$f: G/H \to G/HK$, $\forall Hx \in G/H, f(Hx)=HKx$

先证f是良定义的.

$Hx=Hy \Leftrightarrow xy^{-1} \in H \Rightarrow xy^{-1} \in HK \Leftrightarrow HKx=HKy \Leftrightarrow f(Hx)=f(Hy)$

再证f是满同态的.显然f是满射,$f(G/H)=G/HK$

$\forall Hx, Hy \in G/H$,

$f(HxHy)=f(Hxy)=HK(xy)=(HKx)(HKy)=f(Hx)f(Hy)$

最后证$\ker f=HK/H$.

令$f(Hx)=HKx=HK \Rightarrow x \in HK$,

$\ker f=\{Hx|x \in HK\}=HK/H$

由群同态基本定理知， $G/HK \cong (G/H)/(HK/H)$

- 证 由Lagrange推论,G中存在元素a且$|a|=p$,存在元素b,且$|b|=q$.由于$(p,q)=1$,且$ab=ba$,故$|ab|=pq$.令$t=pq$,于是$G=\langle t\rangle$.

设H是G的子群,对于任意$Hx\in G/H$,有$x\in$G,$x=t^i$,i为整数.则

$Hx=Ht^i=(Ht)^i\in\langle Ht\rangle$

因此$G/H\subseteq\langle Ht\rangle$.

显然$\langle Ht\rangle\subseteq G/H$.从而$G/H=\langle Ht\rangle=\langle Hab\rangle$.