书面作业6.2 参考解答或提示

第1部分 基础

第2部分 理论

T1 f是群G到群H的同态映射，e_G、e_H为G、H的单位元，请证明：

（1）$f(e_G) = e_H$.

（2） 任意$x \in G$, $f(x^{-1}) = f(x)^{-1}$.

（3） 任意$x \in G$, $f(x^n) = f(x)^n (n \in Z)$.

（1）由$e_Ge_G = e_G$ 有 $f(e_G)f(e_G) = f(e_G)=f(e_G)e_H$. 在群H中，消去等式中的$f(e_G)$ 得到： $f(e_G) = e_H$.

（2） 由 $xx^{-1} = e_G$ 有 $f(x)f(x^{-1}) = f(e_G) = e_H$. 类似有$f(x^{-1})f(x) = e_H$，于是 $f(x)$为$f(x^{-1})$的逆元，即：$f(x^{-1}) = f(x)^{-1}$.

或类似1): 由$f(x)f(x^{-1}) = f(e_G) = e_H=f(x) f(x)^{-1}$，在群H中，消去等式中的$f(x)$记得: $f(x^{-1}) = f(x)^{-1}$.

（3）1) 当$n \geq 1$时, 利用同态方程可得 $f(x^n) = f(x)^n$，但严格证明需要用数学归纳法：

当 $n = 1$，显然 $f(x^n) = f(x)^n$.

假设 $k \geq n \geq 1$时，$f(x^n) = f(x)^n$, 对于$n=k+1$时，

于是，$f(x^{k+1}) = f(x^kx) = f(x^k)f(x) = f(x)^kf(x) = f(x)^{k+1}$，即$n=k+1$, $f(x^n) = f(x)^n$;

2）当$n = 0$ 时，$f(x^n) = f(x)^n$ 即：$f(e_G) = e_H$, 1)中已证明;

3）当$n < 0$, 令$n = -N$（$N \geq 1$）. 于是，

$f(x^n) = f(x^{-N})$

$= f((x^N)^{-1})$（注意负指数的含义——n个x运算再取逆：$(xxx...xx)^{-1}=x^{-1}x^{-1}...x^{-1}x^{-1}x^{-1}=x^{-n}$）

$= f(x^N)^{-1}$（x^N为G中一个元素，于是根据2）可得此等式）

$= (f(x)^N)^{-1}$（上式利用前述归纳证明结果）

$= f(x)^{-N} = f(x)^n$.

综上，得证.

T2 针对下列具体的群之间同态关系，写出上一题中3个性质的具体形式（（1）（2）小题），或利用相关性质证明结论（第（3）小题）：

（1）f为群$<R; +>$到群$<R_+;*>$的同态映射：$f(x)=a^x$，$a>0$，+，*为一般的加法、乘法.

1) $f(0)=a^0=1$; 2) $f(x^{-1})=(a^x)^{-1}$即$f(-x)=a^{-x}$; 3)$f(x^n)=(a^x)^n$即$f(nx)=a^{nx}$.

（2）f为群$<R_+;*>$到群$<R; +>$的同态映射：$f(x)=\log_a x$，$a>0$，+，*为一般的加法、乘法.

1) $f(1)=\log_a 1=0$; 2) $f(x^{-1})=(\log_a x)^{-1}$即$f(1/x)=-\log_a x$; 3)$f(x^n)=(\log_a x)^n$，即$f(x^n)=n\log_a x$.

注意区分加运算、乘运算的表示.

（3）证明：f为群G到群H的同态映射，$x \in G$，若$|x|=n$, 则 $|f(x)|$ 整除n.

由$|x|=n$, 有$x^n=e_G$，于是$f(x)^n=f(x^n)=f(e_G)=e_H$，故 $|f(x)|$ 整除n.

T3 证明单位半群G的所有可逆元素的集合H，对于G的运算*，能够构成群.

提示：需要证明结合律成立：即a，b∈ H，则$(a*b)^{-1} \in H$.

T4 设$<G;o>$是半群，若∀ a,b∈ G，方程$a*x=b$，$y*a=b$有解，则称$<G;*>$是可解的，

（1）证明：可解半群G是群；

（2）G是有限半群，G为群当且仅当G中消去律成立.

提示：（1）需要首先利用方程有解以及单位元的性质，将"右单位元"e_1表示出来，再利用另外一个方程进行运算判断此e_1满足左单位元的要求，类似地，证明右单位元e_2也存在，从而二者相等即为单位元；再进一步，证明元素可逆.（2）对于充分性，可利用消去律证明半群G也是可解半群.

（1）首先证G有单位元.
根据题意，方程$a*x=a$（$a\in G$）有解，设它的一个解为$e\in G$，则有$a*e=a$.
对于任意$b\in G$，
方程$y*a=b$有解，设解为c，则有$c*a=b$.
于是，$b*e=(c*a)*e=c*(a*e)=c*a=b$.
因此e为G的右单位元.
类似地，方程$y*a=a$，$a\in G$有解.设它的一个解为$e'\in G$，则有$e'*a=a$.对于任意$b\in G$，方程$a*x=b$有解，设解为c，则有$a*c=b$.于是，$e'*b=e'*(a*c) =(e'*a)*c=a*c=b$.因此$e'$为G的左单位元.
所以，G有左单位元也存在右单位元，$e=e'$，从而G存在单位元，不妨设为e.
进一步，证明G的每一个元素存在逆元.
对任意$a\in G$，方程$a*x=e$有解c，则c即为a的右逆元，同样地，方程$x*a=e$有解c'，则c即为a的左逆元.由于*在G上满足结合律，于是，$c=c*e=c*(a*c')=(c*a)*c'=e*c'=c'$，a存在逆元c.
综上，半群$<G;*>$存在单位元，且G中每一个元素可逆，故G是一个群.
（2）必要性显然.下面证明充分性.
设$|G|=n,G=\{a_1,a_2,\ldots,a_n\}$.
任意a，$b\in G$，由G满足消去律易得
$b\in\{a*a_1,a*a_2,\ldots,a*a_n\}$,即$b\in G$.
于是，在G中必存在$a*a_i=b$（$1\le i\le n$）,即方程$a*x=b$在G中有解.
同理，方程$y*a=b$在G中也有解.
所以，根据（1）知，G作成群.
T5 设$<H;*>$是群$<G;*>$的子群，令$A=\{x|x\in G，x*H*x^{-1}=H\}$，证明：$<A;*>$是$<G;*>$的一个子群.
显然A非空且$A\subseteq G$,需要证明对$\forall x,y\in A,xy^{-1}\in A$.
对$\forall x,y\in A$,有$xHx^{-1}=H$, $yHy^{-1}=H$.
由$yHy^{-1}=H$可得$y^{-1}Hy=H$.
于是$(xy^{-1})H(xy^{-1})^{-1}=x(y^{-1}H(y^{-1})^{-1})x^{-1}$
$=xHx^{-1}=H$.
因此，$xy^{-1}\in A$，故$<A;*>$是$<G;*>$的一个子群.
T6 设$<H;*>$和$<K;*>$均是群$<G;*>$的子群，设$HK=\{h*k \mid h\in H，k\in K\}$，证明$<HK;\cdot>$是$<G;\cdot>$的子群的充要条件是$HK=KH$.
1）HK显然非空.
必要性
对$\forall h*k\in HK,h\in H,k\in K$，有$h^{-1}\in H$，$k^{-1}\in K$，且
有$(h*k)^{-1} =k^{-1}*h^{-1}\in KH$.
从而有$h*k=((h*k)^{-1})^{-1}\in KH$ (KH为子群)
故$HK\subseteq KH$
类似地可以证明$KH\subseteq HK$.
综上两方面，知$KH=HK$.
2）充分性
显然$HK\subseteq G$,需要证明对$\forall h_1*k_1,h_2*k_2\in HK,h_1*k_1(h_2*k_2)^{-1}\in HK$,其中$h_1,h_2\in H,k_1,k_2\in K$.
而$h_1*k_1(h_2*k_2)^{-1}=h*k_1*k_2^{-1}*h_2^{-1}=h_1*k'*h_2^{-1}$,其中$k'=k_1*k_2^{-1}$.
由$HK=KH$，必存$h_3\in H,k_3\in K$在使得$k'*h_2^{-1}=h_3*k_3$.
于是$h_1*k_1(h_2*k_2)^{-1}=h_1*h_3*k_3=h_4*k_3\in HK$，其中$h_4=h_1*h_3$.
充分性得证.
综上1）、2）,命题得证.

T7 设f、g是从群$<A;*>$到群$<B;o>$的同态，$C=\{x|x\in A且f(x)=g(x)\}$, 请证明：$<C;*>$是$<A;*>$的子群.

提示：按照判定定理来证明，并注意利用同态映射以及T1中的有关结论.

设A、B的单位元分别为e，e′，f是从群$<A;*>$到群$<B;o>$的同态，

有$f(e)of(e)=f(e*e)=f(e)=f(e)oe'$，在B中消去等式中的f(e)得$f(e)=e'$.

类似地，$g(e)=e'$，故$f(e)=g(e)$. 并有：$e\in C$，C非空.

对任意$x, y\in C$，

有$x, y\in A$，且$f(x)=g(x), f(y)=g(y)$. 现在需要证明$x*y^{-1}x\in C$.

由$y\in A$有$y^{-1}\in A$，从而，$x*y^{-1}\in A$.

下面证明$f(x*y^{-1})=g(x*y^{-1})$.

f、g是从群$<A;*>$到群$<B;o>$的同态，由同态方程，上述等式转化为$f(x)of(y^{-1})=g(x)og(y^{-1})$，

而$f(x)=g(x)$，故仅需证明$f(y^{-1})=g(y^{-1})$.

由$f(e)=g(e)$，以及f、g下的同态方程有$f(y*y^{-1})=g(y*y^{-1})$，即$f(y)of(y^{-1})=g(y)og(y^{-1})$，由$f(y)=g(y)$得$f(y^{-1})=g(y^{-1})$.

(本等式的证明还可以直接利用T1中的有关结论）.

综上，对任意$x, y\in C$，有$x*y^{-1}x\in C$，故$<C;*>$是$<A;*>$的子群.

T8 证明：（1）有限群G中的任何元素a的阶可整除|G|.

设$|a|=n$, 则$\{ a^0,a^1,a^2,\ldots,a^{n-1}\}$可以构成G的n阶子群，再由拉格朗日定理可知，$|a| \mid |G|$.

（2）质数阶的群G没有非平凡子群(G除外)，且为循环群.

由拉格朗日定理易判定质数阶群G的子群要么是{e}，要么是其自身，没有其它子群.

设$|a|=n>1$, 则$H=\{a^0,a^1,a^2,\ldots,a^{n-1}\}$可以构成G的子群且H为循环群，因此G=H.

（3）设G和H分别是m阶与n阶群，若G到H存在单同态，则$m|n$.

设G到H的同态映射为g，易得g是G到$g(G)\subseteq H$的双射关系，同态方程显然是成立的，从而G与g(G)之间同构，$|g(G)|=|G|=m$.

设G、H的单位元分别为e，e′，有$g(e)g(e)=g(ee)=g(e)=g(e)e'$，在H中消去g(e)得$g(e)=e'$.

又对任意$x\in G$，$g(x)g(x)^{-1}=e'=g(e)=g(xx^{-1})=g(x)g(x^{-1})$, 在H中消去等式中的g(x)得$g(x)^{-1}=g(x^{-1})$.

从而，对任意$a',b'\in g(G)$，有$a,b\in G$,使得$g(a)=a', g(b)=b'$,

于是，$a'b'^{-1}=g(a)g(b)^{-1}=g(a)g(b^{-1})=g(ab^{-1})\in g(G)$,

由子群判定定理有：g(G)是H之子群.

从而，由拉格朗日定理，$|g(G)|\,|\,|H|$,即$m|n$.

T9 证明右陪集的如下性质：

1) $a\in Ha$； 2) $b\in Ha\Leftrightarrow Ha=Hb$； 3) $a\in H\Leftrightarrow Ha=H$； 4)$Ha=Hb\Leftrightarrow ab^{-1}\in H$.

下面仅分析2)、4）的证明思路,1)、3）可以类似证明：

2) 必要性 对于任意$b\in Ha$，不妨设$b=h_1a$，$h_1\in H$.于是，对于任意$hb\in Hb$，有

$hb=h(h_1a)=(hh_1)a$

由于H是群，所以$hh_1\in H$.于是

$hb=(hh_1)a\in Ha$,

故$Hb\subseteq Ha$

同理可证：$Ha\subseteq Hb$，于是$Hb=Ha$.

充分性 略

4) 充分性 若$ab^{-1}\in H$，则存在$h_1\in H$，使得

$h_1=ab^{-1}$.于是，有 $a=h_1b\in Hb$.

又据2)可知：Ha=Hb.

必要性 若Ha=Hb，则有

$a\in Ha=Hb$.于是存在$h\in H$，使$a=hb$.所以 $ab^{-1}=h\in H$.

T10

1) 设G为模12加群，求<3>在G中所有的左陪集.

2) $X=\{x|x\in R, x\neq 0,1\}$，在X上定义如下6个函数，则$G=\{f_1,f_2,f_3,f_4,f_5,f_6\}$关于函数的复合运算构成群，求子群$\{f_1,f_2\}$的所有的陪集.

$f_1(x)=x$，$f_2(x)=1/x$，$f_3(x)=1-x$，$f_4(x)=1/(1-x)$，$f_5(x)=(x-1)/x$，$f_6(x)=x/(x-1)$.

1) <3>={0,3,6,9}, 其不同的左陪集有3个：

0+<3>=3+<3>=<3>={0,3,6,9}

1+<3>=4+<3>=7+<3>=10+<3>={1,4,7,10}

2+<3>=5+<3>=8+<3>=11+<3>={2,5,8,11}

2)$\{f_1, f_2\}$有3个不同的左陪集：$f_1\{f_1,f_2\}=\{f_1,f_2\}$，$f_3\{f_1,f_2\}=f_5\{f_1,f_2\}=\{f_3,f_5\}$，$f_4\{f_1,f_2\}=f_6\{f_1,f_2\}=\{f_4,f_6\}$.

3个右陪集：$\{f_1, f_2\}f_1=\{f_1,f_2\}$，$\{f_1,f_2\}f_3=\{f_1,f_2\}f_4=\{f_3,f_4\}$，$\{f_1,f_2\}f_5=\{f_1,f_2\}f_6=\{f_5,f_6\}$.

第3部分 综合应用

T1 某通讯编码由4个数据位x1、x2、x3、x4和3位校验位x5、x7、x8构成，它们的关系如下：

$x5=x1\oplus x2\oplus x3$

$x6=x1\oplus x2\oplus x4$

$x7=x1\oplus x3\oplus x4$

其中，⊕为异或运算.若S为满足上述关系的码字的集合，且当$x,y\in S$时有$x\oplus y=x1\oplus y1,\ldots,x7\oplus y7$.

（1）<S;⊕>是群，试证明之；

（2）**(选做)** 查阅资料分析、证明上述纠错码（群码）的纠错能力.

提示：在S上满足封闭性，上述异或运算是满足结合律的，0000000是单位元，S中元素的x存在逆元x. 故<S;⊕>是群.