群 论　习题解答提示

1 仅平凡群{e}有零元，独异点（单位半群）的幂等元不一定惟一，但群的幂等元惟一。

3.1 原题表述为：

证明：　半群<G;o>是群的充要条件是满足如下两个条件：

1）G 中有左单位元 e_1;

2）对$\forall a\in G$,有元素 $a^{-1}\in G$,使得 $a^{-1}oa=e_1$

提示：

注意：这里的 a^{-1} 仅表示与 a 相关的一个元素，并不是群中 a 的逆元之意。

注意到，$(a^{-1})^{-1}a^{-1}=e_1$,于是

$ae_1=e_1ae_1=(a^{-1})^{-1}a^{-1}ae_1=(a^{-1})^{-1}(a^{-1}a)e_1$

$=(a^{-1})^{-1}e_1e_1=(a^{-1})^{-1}(e_1e_1)=(a^{-1})^{-1}e_1$

$=(a^{-1})^{-1}(a^{-1})a=((a^{-1})^{-1}(a^{-1}))a=e_1a=a.$

从而，为 G 之单位元。进而易证 a^{-1} 即为 a 的逆元。

3.2 由于变换（映射）的复合运算o是可以结合的，恒等变换 $I=f_{1,0}\in G$,显然 I 为 G 单位元。下面只证明复合运算o在 G 上是封闭的，且 G 中每个元素有逆元。

事实上，$a,b,c,d\in Q$,且 $a,c\neq 0$,对于 $x\in Q$,有

$(f_{ab}of_{cd})(x)=f_{ab}(f_{cd}(x))=a(cx+d)+b=acx+(ad+b)$,

又 $ac\neq 0$, $ac,ad+b\in Q$,故$=f_{ac,ad+b}\in G$，所以，复合运算在 G 上是封闭的。

$f_{a,b}\in G$，$a\neq 0$，$a,b\in Q$，取 $f_{1/a,-b/a}\in G$,有

$f_{a,b}of_{1/a,-b/a}=f_{a(1/a),a(-b/a)+b}=f_{1,0}$

所以，f_{ab} 存在逆元 f。

综上，G 关于变换的复合运算o构成群。

4 首先要说明 H 能构成代数结构（$b^{-1}a^{-1}$ 为 ab 的逆元，二者均在 H 中，所以 a，b 在 H 中，则 ab 也在 H 中，H 上运算满足封闭性）。注意到，H 中，运算结合律继承成立，单位元可逆，其在 H 中，可逆元素亦可逆。

6 注意消去律的应用。解为 $a^{-1}bca^{-1}b^{-1}$

7 必要性显然。下面证明充分性。

设$|G|=n$, $G=\{a_1,a_2,\cdots,a_n\}$。

任意 a，$b\in G$，令 $G'=\{aa_1,aa_2,\cdots,aa_n\}$,于是，$G'\subseteq G$，且由 G 满足消去律易得 G’中元素两两不等，有$|G'|=|G|$,于是 $G'=G$，b 从而 $b\in G$。于是，有 $aa_i\in G'$（$1\le i\le n$）使得 $aa_i=b$,即方程 ax=b 在 G 中有解。

同理，方程 ya=b 在 G 中也有解。

所以，根据例 8.4 的结论知，G 作成群。

9 首先构造出 3 阶群的运算表，再讨论。

10 任意 $a\in G$,则在序列 $a,a^2,a^3,\ldots,a^{|G|+1}$ 中至少有两个元素相同,不妨设 $a^r=a^s$（$1\leqslant s<r\leqslant |G|+1$）。

于是，$a^{r-s}=e$

所以，元素 a 的阶数至多为 $r-s\leqslant|G|$。

若元素 $a\in G$，$|a|=|G|$，则 G 中元素可以列举出来：设$|a|=n$.

$G=\{a^0,a^1,a^2,\cdots,a^{n-1}\}$。注意到，G 显然非空。 且 g 中任意 n 个元素是互异的，否则，假设 $a^i=a^j(0\leqslant i<j<n)$，则 $a^{j-i}=e$, $j-i<n$,与$|a|=n$ 矛盾。

11（1）设$|a|=|a^{-1}|=r_1$(可根据教材证明$|a|=|a^{-1}|$)，

令$|b^{-1}*a*b|= r_2$，则$(b^{-1}*a*b)^{r1}$

$=(b^{-1}*a*b)*(b^{-1}*a*b)*\cdots*(b^{-1}*a*b)$

$=b^{-1}*a*(b*b^{-1})*a*(b*b^{-1})*\cdots*(b*b^{-1})*a*b$

$= b^{-1}*a^{r1}*b= b^{-1}*e*b=e$

故 $r_2 \mid r_1$ (1)

又$(b^{-1}*a*b)^{r2}=\cdots= b^{-1}* a^{r2}*b=e$

于是，$a^{r2}=b* b^{-1}=e$

故 $r_1 \mid r_2$ (2)

于是由(1)(2)知 $r_1= r_2$,

即 a，a^{-1}和 $b^{-1}*a*b$ 的周期相同。

(2) 设$|ab|=r_1$,令$|ba|= r_2$

则$(ab)^{r2}=\cdots=a(ba)^{r2-1}b=a(ba)^{r2}(ba)^{-1}b=\cdots=e$。

从而，$r_1|r_2$,

……。

（3）类似地，可以证明。

12 （1）注意到周期大于 2 的元素及其逆元是成对出现（不相等），因此，其个数为偶。

（2）注意到仅单位元 e 周期为 1，去除同期大于 2 的元素个数，余下即为周期为 2 的元素个数，并结合（1）易得结论。

13 设<G,*>是一个群,e 为单位元,则

$\forall a\in G$，若 $a\neq e$，则 $a\neq a^{-1}$,

若 $a=a^{-1}$ 则 $a_2=e$，于是<{a,e},*>是<G,*>的阶为 2 的子群

由拉格朗日定理:$2 \mid |G|$，即群 G 阶数为偶数，矛盾.

所以，$\forall a\in G$，若 $a\neq e$,a、a^{-1}总是成对出现，

于是,G 可以表示为：$\{e,a_1,a_1^{-1},a2,a_2^{-1},\ldots,a_n,a_n^{-1}\}$，其中 $a_i\neq a_i^{-1}$

故 $e*a_1* a_1^{-1}*\ldots* a_n * a_n^{-1}=e*e*\cdots*e=e$.

15 易证明‹H∩K；*›是 G 之子群：当 a，b∈H∩K，即 a，b∈H，且 a，b∈K，于是有 $ab^{-1}\in H$，$ab^{-1}\in K$，从而 $ab^{-1}\in H\cap K$；但 H∪K 不是，当当 a，b∈H∪K 时不能确定 $ab^{-1}\in H\cup K$。

17 思路：显然 $C\subseteq A$,需要证明

对$\forall x,y\in C, xy^{-1}\in C$,

即 $f(xy^{-1})=g(xy^{-1})$

亦即 $f(x)f(y^{-1})=g(x)g(y^{-1})$ (*)

$f(x)=g(x)$是显然的，需要证明 $f(y^{-1})=g(y^{-1})$.

又由 ee=e，有 f(ee)=f(e),f(e)f(e)=f(e)e’,从而 f(e)=e’，类似地，g(e)=e’，其中 e’为 B 的单位元。

由 f(e)=g(e)=e’,有 $f(yy^{-1})=g(yy^{-1})$，亦即 $f(y)f(y^{-1})=g(y)g(y^{-1})$,

而 f(y)=g(y)是显然的,

于是由群的消去律可得 $f(y^{-1})=g(y^{-1})$。

综上，命题得证。

18 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$(xy^{-1})H(xy^{-1})^{-1}=x(y^{-1}H(y^{-1})^{-1})x^{-1}=x(y^{-1}Hy)x^{-1}=xHx^{-1}=H$.

因此，$xy^{-1}\in A$，故<A；*>是<G；*>的一个子群.

19 HK 显然非空.

1）必要性

对$\forall hk\in HK, h\in H, k\in K$，有$h^{-1}\in H$，$k^{-1}\in K$，且

有$(hk)^{-1}=k^{-1}h^{-1}\in KH$.

从而有$hk=((hk)^{-1})^{-1}\in KH$（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$\forall h_1k_1, h_2k_2\in HK, h_1k_1(h_2k_2)^{-1}\in HK$,其中$h_1, h_2\in H, k_1, k_2\in K$.

而$h_1k_1(h_2k_2)^{-1}=hk_1k_2^{-1}h_2^{-1}=h_1k'h_2^{-1}$,其中$k'=k_1k_2^{-1}$.

由 HK=KH，必存$h_3\in H, k_3\in K$在使得$k'h_2^{-1}=h_3k_3$.

于是$h_1k_1(h_2k_2)^{-1}=h_1h_3k_3=h_4k_3\in HK$，其中$h_4=h_1h_3$.

充分性得证.

综上 1）、2）, 命题得证.

20

需要证明如下三个性质：

1)自反性：对于$\forall s\in S_n$,有$I^{-1}sI=s$,其中$I\in G$,为 G 的单位元(即恒等变换). 因此有 sRs.

2)对称性：对于$\forall s, t\in S_n$,若$(s,t)R$,即存在$g\in G$,使得$s=g^{-1}tg$.

由可得,$t=gsg^{-1}=(g^{-1})^{-1}sg^{-1}$,其中$g^{-1}\in G$. 故 tRs.

3)传递性：可以类似地证明.

21 S_3的二阶子群有$\{P_1, P_2\}$，$\{P_1, P_3\}$. $\{P_1, P_4\}$，其中

$$P_1=\begin{pmatrix}123\\123\end{pmatrix}, P_2=\begin{pmatrix}123\\213\end{pmatrix}, P_3=\begin{pmatrix}123\\321\end{pmatrix}, P_4=\begin{pmatrix}123\\132\end{pmatrix}\quad P_5=\begin{pmatrix}123\\231\end{pmatrix}\quad P_6=\begin{pmatrix}123\\312\end{pmatrix}.$$

22 可以由 Burnside 定理计算得到：(6+2+0+0)/4=2 个等价类（轨道）

23 请参考例 8.30

24 1）是，-1，1 为其生成元。

2）不是。

3）是，其中一个生成元为$e^{(2\pi/n)i}$ 即 $\cos(2\pi/n)+i\sin(2\pi/n)$ 。

4）是，生成元为 m，或-m。

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

26 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 $H=\{a^0, a^1, a^2, \cdots, a^{n-1}\}$可以构成 G 的子群且 H 为循环群，G=H 为循环群.

27 根据例 8.14 可以判定 G 的生成元有$a^1, a^2, a^4, a^7, a^8, a^{11}, a^{13}, a^{14}$

根据例 8.16 可以得到 G 的所有子群为$\langle e\rangle, \langle a\rangle, \langle a^3\rangle, \langle a^5\rangle$

28 下面仅分析 2)、4）的证明思路：

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 $ab^{-1}=h\in H$。

29 1) $\langle 3\rangle=\{0,3,6,9\}$,其不同的子陪集有 3 个：

$0+\langle 3\rangle=3+\langle 3\rangle=\langle 3\rangle=\{0,3,6,9\}$

$1+\langle 3\rangle=4+\langle 3\rangle=7+\langle 3\rangle=10+\langle 3\rangle=\{1,4,7,10\}$

$2+\langle 3\rangle=5+\langle 3\rangle=8+\langle 3\rangle=11+\langle 3\rangle=\{2,5,8,10\}$

2) $\{f_1,f_2\}$有 3 个不同的左陪集：

$f_1\{f_1,f_2\}=\{f_1,f_2\}$， $f_3\{f_1,f_2\}=\{f_3,f_5\}$，$f_4\{f_1,f_2\}=\{f_4,f_6\}$.

30 设 g 为 G 到 H 的单同态映射，则 g 的同态象 g(G)是 H 的子群，g 为 G 到 g(G)的双射，g(G)为 m 阶群，从而知 m|n.

31 有 4 个左陪集：H, cH, c^2H, c^3H.

33 设 e 为 G 上之单位元，e' 为 G' 上之单位元，

由题设 $H\subseteq G$，$e'\in H'$，易得 $f(e)=e'$，

故 $e\in H$ 从而 $H\neq\phi$.

下面首先证明 H 为 G 子群，之后证明其为 G 之正规子群。

对$\forall a,b\in H$,有 $a', b'\in H'$，

使得 $a'=f(a)\in H'$，$b'=f(b)\in H'$,且$(f(b))^{-1}\in H'$，

又由 $f(b)\circ f(b)^{-1}=e'=f(e)=f(b*b^{-1})=f(b)\circ f(b^{-1})$，有 $f(b)^{-1}=f(b^{-1})$

于是,由 $f(a*b^{-1})=f(a)\circ f(b^{-1})=f(a)\circ f(b)^{-1}\in H'$ (H' 为 G' 之子群)

故 $a*b^{-1}\in H$ 所以 H 为 G 之子群。

进一步，类似地，对$\forall h\in H$,有 $a\in G$，有 $a'\in G'$，$h'\in H'$，

使得 $a'=f(a)\in G'$，$h'=f(h)\in H'$,且 $f(h)^{-1}\in H'$，

于是 $f(a*h*a^{-1})=f(a)\circ f(h)\circ f(a^{-1})=f(a)\circ f(h)\circ f(a)^{-1}\in H'$ (H' 为 G' 之正规子群).

从而 $a*h*a^{-1}\in H$.

所以 H 为 G 之正规子群.

36. （注：为简便考虑，下面的证明过程忽略了运算符号）

首先，证明 N 为 G 正规子群：即 34 题证明过程

其次，构造以 G/N 到 G'/N' 的双射 f：

$\forall xN\in G/N$，$x\in G$，$f(xN)=f(x)N'$

下面首先证明 f 为双射，其次证明满足同态方程。

显然，$xN\in G/N$ 有像 $f(x)N'\in G'/N'$。

又对$\forall x_1, x_2\in G$，

有 $x_1N=x_2N$

$\Leftrightarrow x_1x_2^{-1}\in N$

$\Leftrightarrow f(x_1x_2^{-1})\in N'$

$\Leftrightarrow f(x_1)f(x_2)^{-1}\in N'$

$\Leftrightarrow f(x_1)N'=f(x_2)N'$

从而知，若 $x_1N=x_2N$ 则 $f(x_1)N'=f(x_2)N'$，故 是从 G/N 到 G'/N' 的函数。

且若 $f(x_1)N'=f(x_2)N'$ 则 $x_1N=x_2N$，故 是从 G/N 到 G'/N' 的单射。

又 f 是满射，

故 对$\forall x'N' \in G'/N'$（$x' \in G'$）

存在$x \in G$（$f(x)= x'$），$xN \in G/N$使f（xN）$= f(x)N'$

故f是满射。

所以f为双射。

下面证明f满足同态方程：

对 $\forall x_1$，$x_2 \in G$，

有 f（x_1Nx_2N）

$= f$（x_1x_2N）（N为正规子群）

$= f$（x_1x_2）N'

$= f$（x_1）f（x_2）N'

$= f$（x_1）N' f（x_2）N' （N' 为正规子群）

$= f$（x_1N）f（x_2N）

从而同态方程满足.

综上，$\langle G/N; *\rangle$与$\langle G'/N'; o\rangle$同构.