近世代数习题作业 3

1．设 R 为实数集，$S=\{(a,b)|a\neq 0,a,b\in R\}$。在 S 上利用通常的加法和乘法定义二元运算"$\circ$"如下：$\forall (a,b),(c,d)\in S$，$(a,b)\circ(c,d)=(ac,ad+b)$

验证：$(S,\circ)$ 是群。

证明：由二元运算"$\circ$"的定义知其为 $(S,\circ)$ 上的二元代数运算。

1) 结合律：显然；

2) 单位元：$e=(1,0)$；

3) 逆元：对 $\forall (a,b)\in S$，$(\frac{1}{a},-\frac{b}{a})\circ(a,b)=(1,0)$

综上 $(S,\circ)$ 是群。

$//f(x)=ax+b,g(x)=cx+d,f\circ g(x)=acx+(ad+b)$

2．设 a 和 b 是群 G 的两个元素。如果 $(ab)^2=a^2b^2$，试证：$ab=ba$

3．设 G 是群。如果 $\forall a\in G$，$a^2=e$，试证：G 是交换群。

证明：由 $\forall a\in G$，$a^2=e\Rightarrow$ 对 $\forall a\in G$ 有 $a=a^{-1}$。从而对 $\forall a,b\in G$，$ab=(ab)^{-1}$

$=b^{-1}a^{-1}=ba$。

4．证明四阶群是交换群。

证明：设 $G=\{e,a,b,c\}$，$(G,\circ)$ 为群。其乘法表为：

$\bullet$	e	a	b	c
e	e	a	b	c
a	a	aa	ab	ac
b	b	ba	bb	bc
c	c	ca	cb	cc

验证交换性只须验证乘法表中的矩阵的对称性即可，即只须验证：

1）ab 与 ba：显然 $ab\neq a,b$，故 $ab=e,c$

若 $ab=e$，即 a 与 b 互逆，则必有 $ba=e$，从而 $ab=ba$；

若 $ab=c$，则 $ba=c$，否则若 $ba=e$，则必有 $ab=e$，从而 $c=e$ 矛盾。

综上 $ab=ba$。

同理可得：$ac=ca$，$bc=cb$。

5．证明：在任一阶大于 2 的非交换群里必有两个非单位元 a 和 b，使得 $ab=ba$。

证明：设 $(G,\circ)$ 为非交换群，且 $|G|>2$（注：不一定为有限群），只需到元素 $a\in G$，且 $a^{-1}\neq a$ 即可。即只需在 G 中找到一个元素，其阶大于 2 即可。若 G 中不存在这样的元素，即对 $\forall a\in G$ 均有 $a^2=e$，则由前面 3 题的结论知 G 为交换群，矛盾。故 $\exists a\in G$，其阶大于 2，即 $a^{-1}\neq a$，从而令 $b=a^{-1}$，显然有 $b\neq a$，但 $ab=ba$。

6． 有限群里阶大于 2 的元素的个数必为偶数。

证明：设 $(G,\circ)$ 为有限群，$|G|=n$，对 $\forall a\in G$，若 a 的阶为 r 且 $r>2$，即 $a^r=e$，则 a^{-1} 的阶也为 r（参见课堂上的思考题结论），即 $(a^{-1})^r=e$，且 $a^{-1}\neq a$，从而阶大于 2 的元素成对出现，故阶大于 2 的元素个数必为偶数。

7．证明：偶数阶群里阶为 2 的元素的个数必为奇数。

证明：设 $(G,\circ)$ 为有限群，$|G|=2n$，设元素阶为 2 的个数为 m，元素阶大于 2 的个数为 $2k$，元素阶为 1 仅有单位元，则有：$1+m+2k=2n$，所以 m 必为奇数。

8． 偶数阶群里至少有一个阶为 2 的元素。

9．设 $a_1,a_2,\cdots,a_n$ 为 n 阶群 G 中的 n 个元素（它们不一定各不相同）。证明：存在整数 p 和 q（$1\le p\le q\le n$），使得 $a_p a_{p+1}\cdots a_q=e$.

证明：考查元素序列：e，a_1，a_1a_2，$a_1a_2a_3$，$\cdots$，$a_1a_2\cdots a_n\in G$，而 $|G|=n$

故上述 $n+1$ 个元素中至少有两个元素相同，若其中一个为 e，则有：$a_1a_2\cdots a_i=e$

此时令 $p=1,q=i$ 即可；若两个元素均不为 e，则存在 $i,j\in[1,n]$，不妨设 $i<j$，使得 $a_1a_2\cdots a_i=a_1a_2\cdots a_j=a_1a_2\cdots a_ia_{i+1}\cdots a_j$，由消去律得：$a_{i+1}\cdots a_j=e$，此时令 $p=i+1,q=j$ 即可。

10. 设a和b为群G的两个元素，$ab = ba$，a的阶为m，b的阶为n。试证：ab的阶为m与n的最小公倍数的约数。何时ab的阶为mn？

证明： 设$[m,n]=p,(m,n)=d$, 则$m|p,n|p$。

$\because (ab)^p = a^p b^p = e$

$\therefore$ ab的阶为m与n的最小公倍数的约数。

设ab的阶为r，则由$r|p$知$\exists t \in Z, p = tr$, 即$[m,n]=tr=tmn$。

又$[m,n]=\frac{mn}{d}$, 从而$\frac{mn}{d}=tmn$, 所以$td=1$,

则有$d=1$，即m与n互质。