近世代数课后习题作业 4 参考解答

1．证明：显然对 $\forall f \in G$， f 为双射。

1）封闭性：对 $\forall f, g \in G$，设 $f(x)=ax+b$， $g(x)=cx+d$， $a \neq 0, c \neq 0$，

则 $f \circ g(x)=f(g(x))=f(cx+d)=a(cx+d)+b=(ac)x+ad+b$，所以 $f \circ g \in G$

2）结合律：映射的复合满足结合律。

3）单位元： $I_e(x)=x$

4）逆元：显然对 $\forall f \in G$，由 f 为双射，故 f 可逆，且 $f^{-1}(x)=\dfrac{1}{a}x-\dfrac{b}{a}$，则 $f^{-1} \in G$ 。

///////////////////////////

2．证明：

1）由 φ 的构造知 φ 为双射。

2）同构方程：对 $\forall x, y \in R^{+}$，$\varphi(x \times y)=\log_p(x \times y)=\log_p x+\log_p y=\varphi(x)+\varphi(y)$ 。

///////////////////////////

3. 证明：记 $U_n=\{x \mid x^n=1\}$，对 $\forall x_k \in U_n$，$x_k=\cos\dfrac{2k\pi}{n}+i\sin\dfrac{2k\pi}{n}$，$k=0,1,\cdots,n-1$ 。

由前面的习题作业知其为群，且有 $U_n=(x_1)$， 其中 $x_1=\cos\dfrac{2\pi}{n}+i\sin\dfrac{2\pi}{n}$，

$x_k=\cos\dfrac{2k\pi}{n}+i\sin\dfrac{2k\pi}{n}=(\cos\dfrac{2\pi}{n}+i\sin\dfrac{2\pi}{n})^k=(x_1)^k$ 。

///////////////////////////

4．解：$(Z_{12},\oplus)$ 为模 12 的同余类加群， $Z_{12}=(a)=([1])$，其非平凡真子群如下：

1） $S_1=(2a)=\{[0],[2],[4],[6],[8],[10]\}$

2） $S_2=(3a)=\{[0],[3],[6],[9]\}$

3） $S_3=(4a)=\{[0],[4],[8]\}$

4） $S_4=(6a)=\{[0],[6]\}$

///////////////////////////

5．证明：由 $(n,r)=1 \Rightarrow \exists k_1, k_2 \in Z$， $k_1 \cdot n+k_2 \cdot r=1$，则有：

$a^1=a^{k_1 \cdot n+k_2 \cdot r}=a^{k_1 \cdot n}a^{k_2 \cdot r}=ea^{k_2 \cdot r}=(a^r)^{k_2}$，即 $a=(a^r)^{k_2}$，则 G 的生成元 a 可由 a^r 生

成，故有：$(a^r)=G$。

///////////////////////////

6. 证明：设 a^r 的阶为 k，则 $(a^r)^k=e$，即 $a^{rk}=e$。又 $a^n=e$，所以 $n|rk$，又 $(r,n)=d$，

则有：$\frac{n}{d}|\frac{r}{d}k$，而 $(\frac{n}{d},\frac{r}{d})=1$，所以 $\frac{n}{d}|k$。

又由 $(a^r)^{\frac{n}{d}}=a^{\frac{nr}{d}}=(a^n)^{\frac{r}{d}}=e^{\frac{r}{d}}=e$ 得：$k|\frac{n}{d}$，从而 $k=\frac{n}{d}$

///////////////////////////

7．证明：设 $(G,\circ)$ 为六阶群。则对 $\forall x\in G(x\neq e)$，其阶只能为 2，3，6。

1）若 $\exists a\in G$，且 a 的阶为 6，即 $a^6=e$，则 $G=(a)$，则由循环群的子群知存在

三阶子群为：$S=\{e,a^2,a^4\}$

2）若 $\exists a\in G$，且 a 的阶为 3，即 $a^3=e$，此时显然有三阶子群为：$S=\{e,a^1,a^2\}$

3）若不存在 $a\in G$，使得 a 的阶为3或6，则对 $\forall a\in G$ 有 $a^2=e$，从而此时群 $(G,\circ)$

为交换群。令 $A=\{a,b\}$，其中 $a,b\in G$ 且均不为单位元。则 $(A)=\{e,a,b,ab\}$，

$|(A)|=4\nmid 6$ 矛盾。

///////////////////////////

8．证明：设 $(G,\circ)$ 为群，$|G|=p^m$。取 $a\in G(a\neq e)$，设其阶为 r，则 $r\,|\,p^m$，

由 p 为素数得：$r=p^k$，$k\geq 1$。

1）若 $k=1$，则群 G 的一个 p 阶子群为 $H=(a)$；

2）若 $k>1$，取 $b=a^{p^{k-1}}\in G$，设 b 的阶为 q，即 $b^q=e$。由 $b^p=(a^{p^{k-1}})^p=a^{p^k}=e$

$\Rightarrow q\,|\,p$，又 $b^q=(a^{p^{k-1}})^q=a^{qp^{k-1}}=e$，则有 $r\,|qp^{k-1}$，即：$p^k\,|qp^{k-1}$，从而 $p\,|\,q$，

所以 $q=p$。此时群 G 的一个 p 阶子群为 $H=(b)$。

///////////////////////////

11．证明：只需在 S_l 与 S_r 之间找到一个双射即可。

定义 $\varphi:S_l\to S_r$，且对 $\forall aH\in S_l$，有 $\varphi(aH)=Ha^{-1}$，下证 φ 为双射。

满射：显然。

单射：对 $\forall aH, bH \in S_l$，若 $aH \neq bH$，下证 $\varphi(aH) \neq \varphi(bH)$。

若 $\varphi(aH) = \varphi(bH)$，则有 $Ha^{-1} = Hb^{-1}$，从而 $Ha^{-1}b = H$，由定理 12.6.1 知 $a^{-1}b \in H$，从而 $aH = bH$，矛盾。