近世代数课后习题作业 1 部分参考解答

3.

证明：只须证：对 $\forall x,y\in S$，若有 $(a\circ b)\circ x=(a\circ b)\circ y$，则必有 $x=y$。

由结合律知 $(a\circ b)\circ x=a\circ(b\circ x)$，$(a\circ b)\circ y=a\circ(b\circ y)$，从而 $a\circ(b\circ x)=a\circ(b\circ y)$，又 a 为左消去元，故有 $b\circ x=b\circ y$，而 b 也为左消去元，所以有 $x=y$。

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

4.

证明：由普通加法和乘法满足交换律知所定义的二元运算"$\circ$"满足交换律。

1）证 $(M,\circ)$ 为幺半群

①由定义知二元运算"$\circ$"显然为 M 上的一个二元代数运算，即 $(M,\circ)$ 为一代数系；

②又对 $\forall(x_1,y_1),(x_2,y_2),(x_3,y_3)\in M$ 有：

$((x_1,y_1)\circ(x_2,y_2))\circ(x_3,y_3)=(x_1,y_1)\circ((x_2,y_2)\circ(x_3,y_3))$，即满足结合律。

③单位元：对 $\forall(x,y)\in M$ 有 $(1,0)\circ(x,y)=(x,y)\circ(1,0)=(x,y)$

2）左消去元

由 $(x_1,x_2)\circ(y_1,y_2)=(x_1y_1+2x_2y_2,x_1y_2+x_2y_1)$

$(x_1,x_2)\circ(z_1,z_2)=(x_1z_1+2x_2z_2,x_1z_2+x_2z_1)$

若 $(x_1y_1+2x_2y_2,x_1y_2+x_2y_1)=(x_1z_1+2x_2z_2,x_1z_2+x_2z_1)$，则：

$x_1(y_1-z_1)+2x_2(y_2-z_2)=0$

$x_1(y_2-z_2)+x_2(y_1-z_1)=0$

可得：$2x_2^{\,2}(y_2-z_2)=x_1^{\,2}(y_2-z_2)$，即 $(x_1^{\,2}-2x_2^{\,2})(y_2-z_2)=0$

因为 $x_1^{\,2}-2x_2^{\,2}\neq 0$ 所以 $y_2-z_2=0$，从而 $y_1-z_1=0$

//

5.

推理不正确：由 $x^{2(n-k)}x^k = x^n$ 推不出 $x^{2(n-k)} = x^{n-k}$，这里看不出满足右消去律。

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

6.

证明：设 $(S,\circ)$ 为有限半群，且 $|S| = n$。设 $b \in S$，则可得：$b^1, b^2, \cdots, b^n, b^{n+1} \in S$

则由 S 的有限性知，$\exists i, j \in [1, n+1]$ 使得 $b^j = b^i$，不妨设 $j > i$，即 $j = i + k$，$k > 0$。

从而有：$b^i \circ b^k = b^i$，则两边同时连续左乘 b 可得 $b^p \circ b^k = b^p$，且满足 $p = q \cdot k$，

从而运用递归调用可得 $b^p = b^p \circ b^{2k} = \cdots = b^p \circ b^{qk}$，即 $b^p \circ b^p = b^p$，令 $a = b^p$ 即可。

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

7.

证明：

I. 证 $(M,*)$ 为半群：

1）由"*"定义知满足封闭性；

2）显然"*"满足结合律。

II. 设 e' 为 $(M,*)$ 的单位元，则对 $\forall a \in M$，有 $a * e' = e' * a = a$，即 $a \circ m \circ e' = a$，

$e' \circ m \circ a = a$，由结合律：$a \circ (m \circ e') = a$，$(e' \circ m) \circ a = a$，由 a 的任意性知 $m \circ e'$

与 $e' \circ m$ 为 M 关于"$\circ$"运算的左右单位元，而 $(M,\circ,e)$ 为幺半群，故有 $m \circ e' = e$，

$e' \circ m = e$，则由逆元素的定义知 e' 为 m 关于"$\circ$"运算的逆元素，即为 m 满足的条件。

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

8.

证明：

1）结合律：由集合论知识知集合的对称差运算"Δ"满足结合律，故 $(2^S,\Delta)$ 为半群；//这里结合律可以直接调用，不用再验证。

2）单位元：对 $\forall A \in 2^S$ 有 $\phi \Delta A = A \Delta \phi = A$；

3）逆元：对 $\forall A \in 2^S$ 有 $A \Delta A = A \Delta A = \phi$，即为自身。

故 $(2^S,\Delta)$ 为群。

9.

在所有 3 次置换构成的集合 S_3 对置换的乘法构成半群 $(S_3,\circ)$ 中，令 $A=\{(12),(23)\}$，

请给出由 S_3 的子集 A 所生成的子半群 (A)。

解：直接对 A 根据生成迭代算法可得 $(A)=S_3$，即包含 A 的子半群只能是 S_3。

//这里关于置换的复合运算也就是有限集合上的双射复合运算，请大家查阅前面集合论的内容，这个复合运算后面我们经常用到。//

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

10.

证明：主要验证一下结合律，显然。

近世代数课后习题作业 2 参考解答

1.

证明：先证 $x\circ x=x$

由已知得：对 $\forall x\in S$ 有 $x\circ e_1=e_1\circ x=x$， $x*e_2=e_2*x=x$

则有 $x\circ x=(x*e_2)\circ(x*e_2)=x*(e_2\circ e_2)$，下证 $e_2\circ e_2=e_2$

因为 $e_2=e_1\circ e_2=(e_1*e_2)\circ e_2=(e_1\circ e_2)*(e_2\circ e_2)=e_2*(e_2\circ e_2)=e_2\circ e_2$

所以 $x\circ x=x*e_2=x$

再证 $x*x=x$

$x*x=(x\circ e_1)*(x\circ e_1)=x\circ(e_1*e_1)$，下证 $e_1*e_1=e_1$

因为 $e_1=e_2*e_1=(e_1\circ e_2)*e_1=(e_1*e_1)\circ(e_2*e_1)=(e_1*e_1)\circ e_1=e_1*e_1$

所以 $x*x=x\circ e_1=x$。

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

2.

证明：记 $H=\{x\mid\exists a_1,a_2,\cdots,a_n\in A\text{使}x=a_1a_2\cdots a_n,n\geq 1\}$，下证 $(A)=H$

1）先证 H 为包含 A 的子半群。

显然 $A\subseteq H$（令 $n=1$ 即可），且"$\circ$"在 H 上的运算封闭，故 H 为包含 A 的子半群。

2）下证 H 的“最小性”。

设 P 为任意包含 A 的子半群，下证 $H\subseteq P$。

对 $\forall x\in H$ ， $\exists a_1,a_2,\cdots,a_i\in A$ 使得 $x=a_1a_2\cdots a_i$ ，又 $A\subseteq P$ ，所以 $a_1,a_2,\cdots,a_i\in P$，故有 $a_1a_2\cdots a_i\in P$，即 $x\in P$，所以 $H\subseteq P$。

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

3.

证明：令 $P=\{a\mid a\circ a=a,a\in M\}$

① 显然有 $e\in P$，故 $P\neq\phi$，且 $P\subseteq M$；

② 下证封闭性：对 $\forall a,b\in P$，下证 $a\circ b\in P$

因为 $(a\circ b)\circ(a\circ b)=a\circ(b\circ a)\circ b=a\circ(a\circ b)\circ b=(a\circ a)\circ(b\circ b)=a\circ b$ ，故

$a \circ b \in P$。

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

4.

解：不一定。设$G=(a)=\{e,a^1,a^2,a^3,\cdots\}$，$\{e,a^2,a^3,\cdots\}$为$G$的子幺半群，但不是循环幺半群。//成立的正例请大家自己给出。

//

5.

证明：记$S=\varphi^{-1}(e_2)$，则$S=\{x|\varphi(x)=e_2,x\in M_1\}$，显然有$S\subseteq M_1$

①S非空：由$\varphi(e_1)=e_2$知$e_1\in S$。

②封闭性：对$\forall x,y\in S$有：$\varphi(x)=e_2$，$\varphi(y)=e_2$，

则$\varphi(x\circ y)=\varphi(x)*\varphi(y)=e_2*e_2=e_2$，所以$x\circ y\in S$

故S是M_1的一个子幺半群。

若S是M_1的理想，则有$SM_1\subseteq S$，$M_1S\subseteq S$

对$\forall x\in S$，$\forall y\in M_1$，$\varphi(x\circ y)=\varphi(x)*\varphi(y)=e_2*\varphi(y)=\varphi(y)$

同理$\varphi(y\circ x)=\varphi(y)*\varphi(x)=\varphi(y)*e_2=\varphi(y)$

所以如果$\varphi(y)=e_2$，则$x\circ y(y\circ x)\in S$，此时S是M_1的理想，否则不是。

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

6.

证明：设$\varphi:(S_1,*)\to(S_2,\bullet)$同态，$\psi:(S_2,\bullet)\to(S_3,\Delta)$同态，记$f=\psi\circ\varphi$，由映射的符合知$f$为$S_1\to S_3$的映射。又对$\forall x,y\in S_1$：

$$f(x*y)=\psi\circ\varphi(x*y)=\psi(\varphi(x*y))=\psi(\varphi(x)\bullet\varphi(y))=\psi(\varphi(x))\Delta\psi(\varphi(y))$$

$$=\psi\circ\varphi(x)\Delta\psi\circ\varphi(y)=f(x)\Delta f(y)$$

所以$f=\psi\circ\varphi$为$S_1\to S_3$的同态，即两个同态的合成还是同态。

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

7.

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

综上$(S,\circ)$是群。

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

8.

证明：

1）封闭性：$(x_i x_j)^n=1$

2）结合律：显然；//复数的乘法。

3）单位元：$e=1$；

4）逆元：$x_k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$，$x_k^{-1}=\cos\frac{2k\pi}{n}-i\sin\frac{2k\pi}{n}$

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

9.

证明：此题中由$\begin{bmatrix}a&0\\0&b\end{bmatrix}\bullet\begin{bmatrix}c&0\\0&d\end{bmatrix}=\begin{bmatrix}ac&0\\0&bd\end{bmatrix}$，其中$ac=\pm1,bd=\pm1$，故$G$对矩阵乘法封闭性显然满足，故构成一个代数系。

1）结合律：矩阵乘法满足结合律；

2）单位元：$e=\begin{bmatrix}1&0\\0&1\end{bmatrix}$；

逆元：$\begin{bmatrix}-1&0\\0&-1\end{bmatrix}^{-1}=\begin{bmatrix}-1&0\\0&-1\end{bmatrix}$，$\begin{bmatrix}1&0\\0&-1\end{bmatrix}^{-1}=\begin{bmatrix}1&0\\0&-1\end{bmatrix}$，$\begin{bmatrix}-1&0\\0&1\end{bmatrix}^{-1}=\begin{bmatrix}-1&0\\0&1\end{bmatrix}$

近世代数课后习题作业 3 参考解答

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

$= b^{-1}a^{-1} = ba$。

//

3．**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。

//

4．**证明**：设 $(G,\circ)$ 为非交换群，且 $|G| > 2$（注：不一定为有限群），只须找到元素 $a \in G$，且 $a^{-1} \neq a$ 即可。

即只须在 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 2 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 $ab = ba$。

//

5．**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。

//

6．**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。

7．**证明**：由上题结论即可知。

//

8．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。

//

9．**证明**：

充分性$\Leftarrow$：由$G_1\subseteq G_2$或$G_2\subseteq G_1\Rightarrow G_1\cup G_2=G_1$或$G_1\cup G_2=G_2$是$G$的子群。

必要性$\Rightarrow$：假设不成立，则由$e\in G_1\cap G_2$知：

至少$\exists a\in G_1\wedge a\notin G_2$，$\exists b\in G_2\wedge b\notin G_1$。

由$a\in G_1\cup G_2$，$b\in G_1\cup G_2$及$G_1\cup G_2$为子群得：$ab\in G_1\cup G_2$，从而$ab\in G_1$或$ab\in G_2$。若$ab\in G_1$，则由$a^{-1}\in G_1$知$a^{-1}(ab)\in G_1\Rightarrow b\in G_1$矛盾；若$ab\in G_2$，则由$b^{-1}\in G_2$知$(ab)b^{-1}\in G_2\Rightarrow a\in G_2$矛盾，故假设不成立。

//

10．**证明**：记$S=\varphi^{-1}(e_2)$，则$S=\{x|\varphi(x)=e_2,x\in G_1\}$，显然$S\subseteq G_1$

1）S非空：对$\forall y\in G_2$，由φ为满射，则$\exists x\in G_1$，使得$y=\varphi(x)$，从而$\varphi(e_1)*y=\varphi(e_1)*\varphi(x)=\varphi(e_1\circ x)=\varphi(x)=y$，同理有$y*\varphi(e_1)=\varphi(x)=y$，即有：$\varphi(e_1)*y=y*\varphi(e_1)=y$，从而$\varphi(e_1)=e_2$，故有$e_1\in S$。

2）封闭性：对$\forall x,t\in S$，有$\varphi(x)=e_2$，$\varphi(t)=e_2$，则$\varphi(x\circ t)=\varphi(x)*\varphi(t)=e_2$，

所以 $x \circ t \in S$。

3）结合律：显然。

4）单位元：$e_1 \in S$。

5）逆元：对 $\forall x \in S$，有 $\varphi(x) = e_2$，则：$e_2 = \varphi(e_1) = \varphi(x \circ x^{-1}) = \varphi(x) * \varphi(x^{-1})$

$= e_2 * \varphi(x^{-1}) = \varphi(x^{-1})$，即 $\varphi(x^{-1}) = e_2$，所以 $x^{-1} \in S$。

//

11. **解**：$(S_1) = Z$，$(S_2) = \{3k | k \in Z\}$

//请大家自己对照生成算法给出生成过程。第一个由 5，7 很快能生成 Z 出的生成元“1”来。第二个由生成算法能很快看出其规律，新加入的元素为它们公因子 3 的倍数。//

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 $f^{-1}(x) = \frac{1}{a}x - \frac{b}{a}$，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 $\forall x_k \in U_n$，$x_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$，$k = 0,1,\cdots,n-1$。

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

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

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

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：

$a^1 = a^{k_1 \cdot n + k_2 \cdot r} = a^{k_1 \cdot n} a^{k_2 \cdot r} = e a^{k_2 \cdot r} = (a^r)^{k_2}$，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。

近世代数课后习题作业5参考解答

1.

证明：设 $H=A\bigcap B$，则由定理知 H 仍为群 G 的子群，则由拉格朗日定理得：$|B|=|H|\cdot[B:H]$，记 $j=[B:H]=\frac{|B|}{|H|}$，则 $B=Hb_1\bigcup Hb_2\bigcup\cdots\bigcup Hb_j$，$b_i\in B(i=1,.\cdots,j)$ 其中 $Hb_i(i=1,\cdots,j)$ 为互不相同的右陪集。则 $AB=AHb_1\bigcup AHb_2\bigcup\cdots\bigcup AHb_j$，又 $AH=A$，所以 $AB=Ab_1\bigcup Ab_2\bigcup\cdots\bigcup Ab_j$，又 $Ab_i\bigcap Ab_l=\phi$，否则，若 $Ab_i\bigcap Ab_l\neq\phi$，则由陪集的性质得：$Ab_i=Ab_l$，从而 $b_ib_l^{-1}\in A$，又 $b_ib_l^{-1}\in B$，所以 $b_ib_l^{-1}\in A\bigcap B$，即 $b_ib_l^{-1}\in H$，所以 $Hb_i=Hb_l$，矛盾。因此根据容斥原理有：$|AB|=|Ab_1|+|Ab_2|+\cdots+|Ab_j|=j\cdot|A|$

即 $|AB|=\frac{|B|}{|H|}\cdot|A|=\frac{|A\|B|}{|A\bigcap B|}$

2.

证明：假设不成立，则 $\exists a\in G$，使得 $a^{-1}Ha\bigcap H=\{e\}$，记 $P=a^{-1}Ha$，由 H 为 G 的子群易知 P 也为 G 的子群，且 $|P|=|H|=n$（由映射 $\varphi(h)=a^{-1}ha$ 为单射），则由1题的结论：$|PH|=\frac{|P\|H|}{|P\bigcap H|}=\frac{n\cdot n}{1}=n^2$，又 $PH\subseteq G$，$|G=n^2$，所以 $PH=G$，则由教材中的例题结论知 $P\bigcap H=H\neq\{e\}$，矛盾。

3.

证明：由前面的习题结论知六阶群中一定有三阶子群，假设不唯一，设 A,B 为六阶群 G 两个不同的三阶子群。不妨设 $A=\{e,a,b\}$，$B=\{e,c,d\}$，则 $A\bigcap B=\{e\}$。从而 $|AB|=\frac{|A\|B|}{|A\bigcap B|}=9>6$ 矛盾。

4.

证明：设 H 为群 G 的子群，且有 $[G:H]=2$，则其左陪集构成的划分为：H,aH $(a\notin H)$，其右陪集构成的划分为：$H,Ha(a\notin H)$，从而 $aH=G\setminus H$

$Ha = G \setminus H$，所以 $aH = Ha$。

5.

证明：设 H_1, H_2 为群 G 的两个正规子群，记 $H = H_1 \bigcap H_2$。则对 $\forall a \in G, h \in H$，由 H_1, H_2 为群 G 的两个正规子群得：$aha^{-1} \in H_1$，$aha^{-1} \in H_2$，所以 $aha^{-1} \in H_1 \bigcap H_2$，即 $aha^{-1} \in H$，故 H 是 G 的正规子群。

6.

证明：对 $\forall a, b \in NH$，则 $\exists n_1, n_2, h_1, h_2 \in NH$, 使得 $a = n_1 h_1, b = n_2 h_2$，则 $ab^{-1} = n_1 h_1 h_2^{-1} n_2^{-1}$。又由 N 是 G 的正规子群，则对 $\forall x \in G$，$xN = Nx$。故 $\exists n_3 \in N$ 使得 $h_2^{-1} n_2^{-1} = n_3 h_2^{-1}$，则 $ab^{-1} = n_1 h_1 n_3 h_2^{-1}$，同理 $\exists n_4 \in N$，使得 $h_1 n_3 = n_4 h_1$，从而 $ab^{-1} = n_1 n_4 h_1 h_2^{-1} = (n_1 n_4)(h_1 h_2^{-1}) \in NH$，则由子群的判定定理知 NH 是 G 的子群。

7.

证明：设 G 为群且 $|G| = 2n$，则由前面习题作业结论知偶数阶群 G 中一定存在一个阶为 2 元素，即 $\exists a \in G$，$a^2 = e$，从而 $H = (a) = \{e, a\}$。由 G 为交换群，则对 $\forall x \in G$，$xH = Hx = \{x, ax\} = \{x, xa\}$，故 H 为群 G 的一个 2 阶正规子群，根据拉格朗日定理以及正规子群和商群的关系知 G 必有一个 n 阶商群。

8.

证明：

必要性 $\Rightarrow$：对 $\forall a, b \in G$，由 H 为 G 的正规子群可得：$aH \cdot bH = a(Hb)H = a(bH)H = abHH = abH$，仍为 H 的左陪集。

充分性 $\Leftarrow$：由已知可得：对 $\forall a \in G$，$aH \cdot a^{-1}H = cH$，因为 $e \in aH \cdot a^{-1}H$，从而 $e \in cH$，；又 $e \in H$，即 $e \in cH \bigcap H$，则由左陪集的性质得：$cH = H$，所以 $aH \cdot a^{-1}H = H$，则对 $\forall h \in H$，$\exists h_1, h_2 \in H$，使得 $aha^{-1}h_1 = h_2 \Rightarrow aha^{-1} = h_2 h_1^{-1} \in H$

9.

证明：由 H 是群 G 的 2 阶正规子群可设 $H = \{e, a\}$，且对 $\forall x \in G$，$xH = Hx$，即 $\{x, xa\} = \{x, ax\}$，所以 $xa = ax$，故 $a \in C$，从而 $H \subseteq C$

近世代数课后习题作业 6 参考解答

1.

证明：必要性$\Rightarrow$：设 $\varphi: G \to \overline{G}$ 的满同态，根据群同态基本定理有：$G/Ker\,\varphi \cong \overline{G}$，

则 $|G/Ker\,\varphi| = |\overline{G}| = n$，又根据拉格朗日定理得：$|G/Ker\,\varphi| = \frac{|G|}{|Ker\,\varphi|} = \frac{m}{|Ker\,\varphi|}$，

即 $m = n \cdot |Ker\,\varphi|$，所以 $n \mid m$。

充分性$\Leftarrow$：设 $G = (a), a^m = e$，$\overline{G} = (b), b^n = \bar{e}$，$\varphi: G \to \overline{G}$，且对 $\forall a^k \in G$，

$\varphi(a^k) = b^k$

1）φ 为映射：若 $a^k = a^l$，则 $a^{k-l} = e$，又 $a^m = e$，所以 $m \mid (k-l)$，又 $n \mid m$，所以 $n \mid (k-l)$，而 $b^n = \bar{e}$，所以 $b^{k-l} = \bar{e}$，则 $b^k = b^l$，即 $\varphi(a^k) = \varphi(a^l)$。

2）同态方程：对 $\forall a^k, a^l \in G$，$\varphi(a^k \cdot a^l) = \varphi(a^{k+l}) = b^{k+l} = b^k b^l = \varphi(a^k)\varphi(a^l)$。

综上 $G \sim \overline{G}$。

//

2.

证明：设 $G = (a)$，由 H 为循环群(为交换群)的子群，故 H 为正规子群，且 H 为商群 G/H 的单位元，对 $\forall bH \in G/H (b \in G)$，$bH = a^k H = (aH)^k$，因此 $G/H = (aH)$

//

3.

1）$(Z(\sqrt{2}), +)$ 为 Abel 群：

①封闭性：对 $\forall m_1 + n_1\sqrt{2}, m_2 + n_2\sqrt{2} \in Z(\sqrt{2})$，有：

$$(m_1 + n_1\sqrt{2}) + (m_2 + n_2\sqrt{2}) = (m_1 + m_2) + (n_1 + n_2)\sqrt{2} \in Z(\sqrt{2})$$

②结合律：显然。

③单位元：$e = 0$。

④逆元：对 $\forall m + n\sqrt{2}, \in Z(\sqrt{2})$，$(m + n\sqrt{2}) + ((-m) + (-n\sqrt{2})) = 0 \in Z(\sqrt{2})$

⑤交换律：显然。

2）$(Z(\sqrt{2}), *)$ 为半群：

①封闭性：对 $\forall m_1 + n_1\sqrt{2}, m_2 + n_2\sqrt{2} \in Z(\sqrt{2})$，有：

$(m_1+n_1\sqrt{2})*(m_2+n_2\sqrt{2})=(m_1m_2+2n_1n_2)+(m_2n_1+m_1n_2)\sqrt{2}\in Z(\sqrt{2})$

②结合律：显然。

3）分配律：显然。

//

4.

证明：$(Z(i),+)$为 Abel 群，$(Z(i),*)$为半群，且分配律显然成立。

//

5.

证明：$Q(\sqrt[3]{2})$对乘法不封闭。

假设 $Q(\sqrt[3]{2})$对乘法封闭，则由$\sqrt[3]{2}\in Q(\sqrt[3]{2})\Rightarrow(\sqrt[3]{2})^2\in Q(\sqrt[3]{2})$，设 $(\sqrt[3]{2})^2=a+b\sqrt[3]{2}$，

$\Rightarrow 2=a\sqrt[3]{2}+b(\sqrt[3]{2})^2\Rightarrow 2=a\sqrt[3]{2}+b(a+b\sqrt[3]{2})\Rightarrow 2=ab+(a+b^2)\sqrt[3]{2}$

$\Rightarrow\sqrt[3]{2}=\frac{2-ab}{a+b^2}$，而 $\frac{2-ab}{a+b^2}$为有理数，$\sqrt[3]{2}$为无理数，故矛盾。

注：证$\sqrt[3]{2}$为无理数

假设$\sqrt[3]{2}$为有理数，则有：$\sqrt[3]{2}=\frac{q}{p}$，$(p,q)=1$。

从而 $q^3=2p^3\Rightarrow p^3\mid q^3\Rightarrow(p^3,q^3)=p^3$，又由$(p,q)=1$可得：

$1=(p,q(p,q))=((p,pq),q^2)=(p,q^2)=\cdots=(p^3,q^3)$，从而 $p^3=1\Rightarrow p=1$，所以

$\sqrt[3]{2}=q$，即$\sqrt[3]{2}$为整数，而$1<\sqrt[3]{2}<2$，矛盾。

//

6.

证明：$(Q(\sqrt[3]{2},\sqrt[3]{4}),+)$为 Abel 群，$(Q(\sqrt[3]{2},\sqrt[3]{4})\setminus\{0\},*)$为 Abel 群，且分配律显然成立。

//

7.

证明：设$(S,+,\circ)$为环，记其唯一的左单位元为e_1，即对 $\forall a\in S$，$e_1a=a$，下证

$ae_1=a$，只须证：$ae_1-a=0$。因为$(e_1+ae_1-a)a=e_1a+(ae_1)a-aa=a$，所以

e_1+ae_1-a也为一左单位元，故$e_1+ae_1-a=e_1$，所以 $ae_1-a=0$，即 $ae_1=a$。

8.

证明：由 $(a-b^{-1})b=ab-1\Rightarrow a-b^{-1}=(ab-1)b^{-1}$，则 $(a-b^{-1})^{-1}=b(ab-1)^{-1}$。

又 $(a-b^{-1})((a-b^{-1})^{-1}-a^{-1})=1-(1-b^{-1}a^{-1})=b^{-1}a^{-1}$，则：

$((a-b^{-1})^{-1}-a^{-1})=(a-b^{-1})^{-1}b^{-1}a^{-1}=b(ab-1)^{-1}b^{-1}a^{-1}$，

从而 $((a-b^{-1})^{-1}-a^{-1})^{-1}=ab(ab-1)b^{-1}=aba-a$。

//

9.

证明：设 $(S,+,\circ)$ 为环，单位元为 1，　$\forall a\in S$，且 a 为非零的零因子。下设 a 存在逆元素，记为 a^{-1}，则有： $a^{-1}a=1$

由 a 为非零的零因子，则 $\exists b\in S\wedge b\neq 0$，使得 $ab=0$，又由 $a^{-1}a=1\Rightarrow a^{-1}(ab)=b$ $\Rightarrow b=0$，矛盾。

//

10.

证明：设 $(S,+,\circ)$ 为交换环，则 $\forall a,b\in S$，　$ab=ba$

1）当 $n=0,1$ 时显然成立。当 $n=2$ 时：

$(a+b)^2=(a+b)(a+b)=(a+b)a+(a+b)b=a^2+ba+ab+b^2=a^2+2ab+b^2$。

2）假设当 $n=k$ 时成立，即：

$(a+b)^k=a^k+C_k^1a^{k-1}b+C_k^2a^{k-2}b^2+\cdots+C_k^kb^k$

则当 $n=k+1$ 时：

$(a+b)^{k+1}=(a+b)^k(a+b)=(a^k+C_k^1a^{k-1}b+C_k^2a^{k-2}b^2+\cdots+C_k^kb^k)(a+b)$

$=a^{k+1}+C_k^1a^kb+C_k^2a^{k-1}b^2+\cdots+C_k^kab^k$

$+a^kb+C_k^1a^{k-1}b^2+C_k^2a^{k-2}b^3+\cdots+C_k^kb^{k+1}$

$=a^{k+1}+(C_k^1+1)a^kb+(C_k^2+C_k^1)a^{k-1}b^2+\cdots+(C_k^k+C_k^{k-1})ab^k+b^{k+1}$

$=a^{k+1}+C_{k+1}^1a^{k+1-1}b+C_{k+1}^2a^{k+1-2}b^2+\cdots+C_{k+1}^kab^k+b^{k+1}$

（$C_k^{i+1}+C_k^i=C_{k+1}^{i+1}$）

11.

证明：设 a_l 为 a 的左逆元，由 $a_l a = 1 \Rightarrow aa_l aa_l = aa_l$，由于 R 为无零因子环满足消去律，则得： $aa_l = 1$。

//

12.

证明：

1） $a(-b) = -(ab) = -(ba) = (-b)a$

2） $a(-ab) = (-a)(ab) = (-a)(ba) = -(aba) = (-ab)a$

3） $a(b+c) = ab + ac = ba + ca = (b+c)a$

4） $a(a+c) = aa + ac = aa + ca = (a+c)a$

//

13.

证明：设 $(F,+,\circ)$ 为域。

1）由 $|F| = 4$，故 $(F,+)$ 的特征数只能是 1，2，4（关于加法群的阶，根据拉格朗日定理可得），又 F 为域，则其特征数为素数，所以 F 的特征数是 2。

2）由已知可设 $F = \{0, e, a, a^{-1}\}$（因为出了零元素外，剩余 3 元素也构成群），且 $a^2 = a^{-1}$（因为 $F \setminus \{0\}$ 为三阶群，由于阶为素数故 $F \setminus \{0\}$ 为循环群，即 $a^3 = e$）。

① 当 $x = a$ 时，显然有 $a + e = 0$ 或 a^{-1}，

若 $a + e = 0 \Rightarrow e + a^{-1} = 0 \Rightarrow a = a^{-1}$，矛盾。

故只能有 $a + e = a^{-1}$，即 $a + e = a^2$，满足方程 $x^2 = x + e$

② 当 $x = a^{-1}$ 时，显然有 $a^{-1} + e = 0$ 或 a，

若 $a^{-1} + e = 0 \Rightarrow e + a = 0 \Rightarrow a = a^{-1}$，矛盾。

故只能有 $a^{-1} + e = a \Rightarrow a^{-1} + e = a^{-2} = (a^{-1})^2$，满足方程 $x^2 = x + e$

//

14.

解：不是。如 $p = 6$，则 $[2] \neq [0]$， $[3] \neq [0]$，但 $[2][3] = [6] = [0]$，与域为无零因子环矛盾。

15．设域F的特征为有限数p，a与b及a_i均在F里。证明：

$$(a\pm b)^{p^n}=a^{p^n}\pm b^{p^n}$$

$$(a_1+a_2+\cdots+a_n)^p=a_1^p+a_2^p+\cdots+a_n^p$$

证明：先证$(a\pm b)^{p^n}=a^{p^n}\pm b^{p^n}$

1）当$n=1$时，由定理知成立。

2）假设当$n=k$时也成立，即$(a\pm b)^{p^k}=a^{p^k}\pm b^{p^k}$

则当$n=k+1$时，$(a\pm b)^{p^{k+1}}=((a\pm b)^{p^k})^p=(a^{p^k}\pm b^{p^k})^p$，又根据已证定理可得：$(a^{p^k}\pm b^{p^k})^p=(a^{p^k})^p\pm(b^{p^k})^p=a^{p^{k+1}}\pm b^{p^{k+1}}$，即$(a\pm b)^{p^{k+1}}=a^{p^{k+1}}\pm b^{p^{k+1}}$。

再证$(a_1+a_2+\cdots+a_n)^p=a_1^p+a_2^p+\cdots+a_n^p$

$(a_1+a_2+\cdots+a_n)^p=((a_1+a_2+\cdots+a_{n-1})+a_n)^p=(a_1+a_2+\cdots+a_{n-1})^p+a_n^p$

$=(a_1+a_2+\cdots+a_{n-2})^p+a_{n-1}^p+a_n^p=\cdots=a_1^p+a_2^p+\cdots+a_{n-2}^p+a_{n-1}^p+a_n^p$。

//

16.

证明：

1）$E=\{2k\mid k\in Z\}$, 对$\forall 2k_1,2k_2\in E$，$2k_1-2k_2=2(k_1-k_2)\in E$；

又$2k_1\cdot 2k_2=2(2k_1k_2)\in E$，所以$E$是$Z$的一个子环。

2）对$\forall r_1,r_2\in E$，$4r_1-4r_2=4(r_1-r_2)\in N$，$r_1\cdot 4r=4(r_1r)\in N$，故$N$是的$E$理想。

3）$N\neq(4)$，因为$4\in(4)$，但显然$4\notin N$。

//

17.

证明：由 3 与 7 互质，则$k_1,k_2\in Z$，使得$k_1\cdot 3+k_2\cdot 7=1$，即$1\in(3,7)$，而$Z=(1)$，

所以$(3,7)=Z$，同理$(13,10)=Z$

//

18.

证明：

1）对$\forall n_1+h_1,n_2+h_2\in N+H$，$(n_1+h_1)-(n_2+h_2)=(n_1-n_2)+(h_1-h_2)$，

又$(n_1-n_2)\in N,(h_1-h_2)\in H$，所以$(n_1+h_1)-(n_2+h_2)\in N+H$。

2）对 $\forall r \in R$，$n+h \in N+H$，$r(n+h)=rn+rh$，$(n+h)r=nr+hr$，而 $rn \in N, nr \in N$，$rh \in H, hr \in H$，所以 $r(n+h) \in N+H$，$(n+h)r \in N+H$。

综上 $N+H$ 也是 R 的理想。