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 $a\circ(b\circ x)=a\circ(b\circ y)$，由 a 为左消去元，则有 $b\circ x=b\circ y$，又 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：$2{x_2}^2(y_2-z_2)={x_1}^2(y_2-z_2)$，即 $({x_1}^2-2{x_2}^2)(y_2-z_2)=0$

因为 ${x_1}^2-2{x_2}^2\neq 0$（$\sqrt{2}$ 为无理数），所以 $y_2-z_2=0$，同理 $y_1-z_1=0$

从而 $y_2=z_2$，$y_1=z_1$， 即 $(y_1,y_2)=(z_1,z_2)$。

//

5．解：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。

另：作业中证 $x^{2(n-k)}=x^{n-k}$ 的其它**错误**方法如下 $(n>k)$：

由 $x^n=x^k \Rightarrow x^{2(n-k)}=x^{2n-2k}=x^{n+n-2k}=x^n\circ x^{n-2k}=x^k\circ x^{n-2k}$

$$=x^{k+n-2k}=x^{n-k}$$

即：$x^{2(n-k)}=x^{n-k}$

错误原因：这里不能保证 $n-2k>0$，从而在半群中元素 x^{n-2k} 可能无意义，因为不能保证半群中一定有逆元素。

这里解决 $n-2k>0$ 的问题，可以对序列 n，k 采用下面的编码：

设 $|S|=m$，对 $\forall x\in S$：由运算封闭性及结合律均有 $x^{2^0},x^{2^1},x^{2^2},\cdots,x^{2^m}\in S$，从而 $\exists n,k\in[0,m]$（设 $n>k$），使得 $x^{2^n}=x^{2^k}$，则有：

$$x^{2(2^n\text{-}2^k)}=x^{2^n+2^n-2\cdot 2^k}=x^{2^n}\circ x^{2^n-2\cdot 2^k}$$

$$=x^{2^k}\circ x^{2^n-2\cdot 2^k}=x^{2^k+2^n-2\cdot 2^k}=x^{2^n-2^k}$$

即 $x^{2(2^n\text{-}2^k)}=x^{2^n-2^k}$，则有 $x^{(2^n\text{-}2^k)}\circ x^{(2^n-2^k)}=x^{(2^n\text{-}2^k)}$

//这里可以看出当 $n>k$ 时，$2^n-2\cdot 2^k>0$。

//依次类推，当 $n>k$ 时可将底数换为大于 2 的，如：$3^n-2\cdot 3^k>0$，$4^n-2\cdot 4^k>0$ 等。

//

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 $b^p=(b^p\circ b^k)\circ b^k=b^p\circ b^{2k}=\cdots=b^p\circ b^{qk}$，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 $(M,*)$ 为代数系；

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：由"$\circ$"的扩充定义知封闭性满足，而且显然有元素u即为扩充后的单位元，因此只需要验证结合律仍然成立即可。

//

9．证明：显然$(2^s,\Delta)$为代数系：

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。

//

11．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$x*x=x\circ e_1=x$。