第二次习题课:

一、(1)

封闭性: $\forall a,b\in S$, 若 $a*b=-1 \Rightarrow a+b+ab=-1$.

$\Rightarrow (a+1)(b+1)=0 \Rightarrow a=-1$ 或 $b=-1$, 与 $a,b\in S$ 矛盾.

单位元: $a*b=a \Rightarrow a+b+ab=a \Rightarrow b(a+1)=0$.

$\Rightarrow b=0$. $\quad 0*a=a*0=a$.

逆元: $\forall a\in S$, $a*b=a+b+ab=0$.

则 $b=-\frac{a}{a+1}\neq -1$.

结合律: $(a*b)*c=(a+b+ab)*c$

$$=a+b+ab+c+ac+bc+abc.$$

$$a*(b*c)=a*(b+c+bc)$$

$$=a+b+c+ab+ac+bc+abc.$$

(2) $2*x*3=2+x+3+2x+3x+6+6x$

$$=11+12x. =7.$$

$$\therefore x=-\frac{1}{3}.$$

二、Z_{mn} 是 mn 阶循环群, 在 $Z_m\times Z_n$ 中寻找 $m\cdot n$ 阶元素

$(Z_m\times Z_n,+)=\{(\bar{i},\bar{\bar{j}})\mid \bar{i}\in Z_m, \bar{\bar{j}}\in Z_n\}$.

考虑元素 $(\bar{1},\bar{\bar{1}})$, 其中 $\bar{1}$ 是 m 阶. $\bar{\bar{1}}$ 是 n 阶.

$$(\bar{1},\bar{\bar{1}})^{mn}=(\bar{1},\bar{\bar{1}})+\cdots+(\bar{1},\bar{\bar{1}})$$

$$=(\overline{m\cdot n},\overline{\overline{m\cdot n}})=(\bar{0},\bar{\bar{0}})$$

设 $(\bar{1},\bar{\bar{1}})$ 的阶为 t, 则有 $t\mid mn$, 我们要证 $mn\mid t$.

由于 $(\bar{1},\bar{\bar{1}})^t=(\bar{t},\bar{\bar{t}})=(\bar{0},\bar{\bar{0}})$.

$\Rightarrow \bar{t}=\bar{0}=\bar{1}^t\ \bar{\bar{t}}=\bar{\bar{0}}=\bar{\bar{1}}^t$.

而 $\bar{1}$ 的阶为 m. $\bar{\bar{1}}$ 的阶为 n

$\Rightarrow m|t$. $n|t$ 而 $(m,n)=1$

$\Rightarrow mn|t$.

三,

"$\Rightarrow$" 若G是交换群,则

$(a*b)^2=a*b*a*b=a*a*b*b=a^2*b^2$.

"$\Leftarrow$" 若 $(a*b)^2=a^2*b^2$,则.

$$a*b*a*b=a*a*b*b.$$

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

$$\Rightarrow b*a=a*b.$$

四,先证明 $H\cap K$ 也是正规子群.

① 封闭性,对 $\forall m_1,m_2\in H\cap K$,则 $\begin{cases}m_1\in H, m_2\in H\\ m_1\in K, m_2\in K.\end{cases}$

$\Rightarrow \begin{cases}m_1*m_2\in H\\ m_1*m_2\in K.\end{cases} \Rightarrow m_1*m_2\in H\cap K.$

② 逆元. $\forall m\in H\cap K$,则 $\begin{cases}m\in H\\ m\in K\end{cases} \Rightarrow \begin{cases}m^{-1}\in H\\ m^{-1}\in K\end{cases} \Rightarrow m^{-1}\in H\cap K$

由①② $H\cap K$ 是一个群.

Date

对 $\forall m\in H\cap K$，$g\in G$.

又 $g^{-1}mg\in H$，$g^{-1}mg\in K$.

$\Rightarrow g^{-1}mg\in H\cap K$.

$\Rightarrow H\cap K$ 为正规子群.

由 G/H，G/K 为交换群. $\forall g_1,g_2\in G$ 有 $\begin{cases} Hg_1\cdot Hg_2=Hg_2\cdot Hg_1 \\ Kg_1\cdot Kg_2=Kg_2\cdot Kg_1 \end{cases}$.

$\Rightarrow \begin{cases} Hg_1\cdot g_2=Hg_2\cdot g_1 \\ Kg_1\cdot g_2=Kg_2\cdot g_1 \end{cases}$.

$\Rightarrow \begin{cases} g_1\cdot g_2(g_2\cdot g_1)^{-1}\in H \\ g_1\cdot g_2\cdot(g_2\cdot g_1)^{-1}\in K \end{cases} \Rightarrow$ 即 $g_1\cdot g_2(g_2\cdot g_1)^{-1}\in H\cap K$.

$\Rightarrow (H\cap K)\cdot g_1g_2=(H\cap K)g_2\cdot g_1$.

$\Rightarrow G/H\cap K$ 为交换群.

五、自反性：令 $\varphi_1:G\to G$，$\varphi_1(g)=g$，φ_1 为双射.

$\Rightarrow \varphi_1(g_1\cdot g_2)=g_1\cdot g_2=\varphi_1(g_1)\cdot\varphi_1(g_2)$.

$\Rightarrow G$ 与 G 同构.

对称性：$\langle G_1,*\rangle$，$\langle G_2,\cdot\rangle$ 是群. 假设 $\langle G_1,*\rangle\cong\langle G_2,\cdot\rangle$.

则 $\exists\varphi_2:G_1\to G_2$. 是双射，满足.

$\forall g_1,g_2\in G_1$，有 $\varphi_2(g_1*g_2)=\varphi_2(g_1)\cdot\varphi_2(g_2)$.

φ_2^{-1} 也是双射.

$\forall g_3,g_4\in G_2$. $\exists a,b\in g_1$ 满足 $g_3=\varphi_2(a)$，$g_4=\varphi_2(b)$.

则 $\varphi_2^{-1}(g_3\cdot g_4)=\varphi_2^{-1}(\varphi_2(a)\cdot\varphi_2(b))=\varphi_2^{-1}(\varphi_2(a*b))$

$=a*b=\varphi_2^{-1}(g_3)*\varphi_2^{-1}(g_4)$

传递性：若 $\langle G_1,*\rangle \cong \langle G_2,\cdot\rangle$，$\langle G_2,\cdot\rangle \cong \langle G_3,\circ\rangle$.

令 $\varphi_1: G_1\to G_2$，$\varphi_2: G_2\to G_3$.

由 φ_1,φ_2 是双射，则 $\varphi_2\varphi_1$ 也是双射.

对 $\forall$ ~~[illegible]~~ $a,b\in G_1$.

有 $\varphi_2\varphi_1(a*b)$

$=\varphi_2(\varphi_1(a)\cdot\varphi_1(b))$

$=\varphi_2\varphi_1(a)\circ\varphi_2\varphi_1(b)$.

$\Rightarrow \langle G_1,*\rangle \cong \langle G_3,\circ\rangle$

则同构是等价关系.

六.(1) 设 $G=(a)$. M 是 G 的子集，

若 $M=\{\varepsilon\}$，则 M 是循环群.

若 M 不仅包含单位元.则由 M 是 G 的子群，M 中所有元素都可以写成 a^m，设 i 是使 $a^i\in M$ 中最小的数.

下面证明: $M=(a^i)$.

设 $\forall a^t\in M$，$t\geq i$，$\exists q,r$ s.t $t=q\cdot i+r$，$0\leq r<i$.

$\Rightarrow a^t=a^{qi+r}=a^{qi}a^r$

$\Rightarrow a^r\in M \Rightarrow r=0$.

$\Rightarrow M=(a^i)$.

(2) $d\mid n$. 设 $d=nk$. $G=(a)$.

存在性: a^k 的阶是 d. 则 $\langle a^k\rangle$ 符合条件

唯一性：设 H 是 G 的一个 d 阶子群，

由(1)知 $H=\langle a^m\rangle$，且 $n=qm$.　　　这种说法可能有点问题.

$a^n=a^{mq}=(a^m)^q=e$.

$\therefore d=|H|=q=\frac{n}{m}$.　$\Rightarrow m=\frac{n}{d}=k$.

$\Rightarrow H=\langle a^k\rangle$，所以 d 阶子群唯一.

G 是 n 阶循环群，$G=\langle a\rangle$，且 $|G|=n$，H 是 G 的一个子群.

$H=\langle b\rangle$，$b=a^s$，则 $|H|=\frac{n}{(n,s)}$.

证：设 $m=|H|$，m 是使 $b^m=e$ 的最小整数，$b^m=a^{sm}=e$

$\Rightarrow n\mid sm$，设 $(n,s)=d$，$n=dn_0$，$s=ds_0$，且 $(n_0,s_0)=1$.

$\Rightarrow n_0\mid s_0m$，又由 m 最小

$\Rightarrow n_0=m=\frac{m}{(n,s)}$.

设 $H=\langle a^m\rangle$，且 $|H|=d$.

$\Rightarrow d=\frac{n}{(n,m)}$

$\Rightarrow (n,m)=k$

$\Rightarrow k\mid m$.

$\Rightarrow H\subset\langle a^k\rangle$.

而 $|H|=|\langle a^k\rangle|=d$

$\Rightarrow H=\langle a^k\rangle$.