13.12将下述置换分解为不含公共元的循环置换，然后再将其分解成对换之乘积。

$$(2)\begin{pmatrix} 3 & 7 & 6 & 5 & 2 & 1 & 4 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

解答：原式$=(3765412)$

$$=(37)(76)(65)(54)(41)(12).$$

(3)$\begin{pmatrix} a & b & c & d & e & f \\ f & a & e & d & c & b \end{pmatrix}$

解答：原式 = (a f b) (c e) = (a f) (f b) (c e).

13.13已知置换**δ** =(1 2 … n), S = (1 2 3)(4 5), T = (1 4)(3 2)(1 6).

求：(1)δ^{-1}

解答：$\because \delta = \begin{pmatrix} 1\,2\,3\cdots n \\ 2\,3\,4\cdots 1 \end{pmatrix}$,

$$\therefore \delta^{-1} = \begin{pmatrix} 2\,3\,4\cdots 1 \\ 1\,2\,3\cdots n \end{pmatrix} = (n\,n-1\cdots 2\,1).$$

(2)$S^2 \cdot T$

解答：$\because S^2 = (123)(45)(123)(45)$

$= (123)(123)(45)(45)$

$= (132).$

$\therefore S^2 \cdot T = (132)(14)(32)(16)$

$= (13)(32)(32)(14)(16)$

$= (31)(14)(16) = (314)(16)$

$= (431)(16) = (4316).$

(3)$(S\cdot T)^{-1}$

解答：$\because S\cdot T=(123)(45)(14)(32)(16)$

$=(12)(23)(32)(54)(41)(16)$

$=(12)(541)(16)=(21)(5416)$

$=(21)(1654)=(21654).$

$\therefore (S\cdot T)^{-1}=(16542)^{-1}$

$=(24561).$

13.18群G, a,b,c是G中的任意元素，证明：
(1)元素ab与ba同阶.

证明：设ab的阶为r,ba的阶为p，

则$(ab)^r=(ba)^p=e.$

$$i.e.\ \overbrace{(ab)(ab)\cdots(ab)}^{r}=e\Rightarrow a\overbrace{(ba)\cdots(ba)}^{r-1}b=e,$$

$$\therefore a(ba)^{r-1}ba=e\cdot a=a\Rightarrow a(ba)^r=a,$$

$\therefore$由消去律，得$(ba)^r=e.$

由定理14.12，得$p\mid r.$

同理，$r\mid p.$

$\therefore p=r.$　即ab与ba同阶.

(2)元素 abc,bca与cab同阶.

证明:$\because a,b,c \in G.$

$\therefore bc \in G.$

由(1)得,$a(bc)$与$(bc)a$同阶,即abc,bca同阶.

同理$b(ca)$与$(ca)b$同阶.

$\therefore abc,bca$与cab同阶.

13.20G为群，a,b∈G,已知ab = ba,a的阶为n，b的阶为m，证明：
(1)(n, m) =1时，ab阶为nm.

证明：设ab的阶为p.

由$ab = ba, a^n = e, b^m = e \Rightarrow (ab)^{nm} = a^{nm}b^{mn} = e.$

$\Rightarrow p \mid nm.$(定理14.12)

$(ab)^p = e \Rightarrow a^p = (b^p)^{-1};$

$a^{pm} = (a^p)^m = (b^p)^{-m} = e \Rightarrow n \mid pm;$

$\because (n,m) = 1 \quad \therefore n \mid p.$

同理，$m \mid p \Rightarrow nm \mid p \Rightarrow p = nm. \therefore ab$阶为$nm.$

(2)(n,m) ≠1,且(a)∩(b)={e}时,ab阶为n,m之最小公倍数LCM(n,m).

证明：设$d=(n,m)\neq 1, l=[n,m]; n=r_1 d, m=r_2 d,$

$(r_1,r_2)=1$,即$l=r_1 r_2 d$;设ab的阶为p.

$(ab)^l=a^l b^l=(a^n)^{r_2}(b^m)^{r_1}=e\Rightarrow p\mid l.$

又$(ab)^p=e$,即$a^p b^p=e$

$a^p b^p=e$,即$a^p=b^{-p}$

$(a)\bigcap(b)=\{e\}\Rightarrow a^i b^j\neq e$,除非$a^i=e, b^j=e;$

$\Rightarrow a^p=e, b^p=e.$

$\therefore n\mid p, m\mid p\Rightarrow l\mid p;$

$\therefore p=l$,即ab的阶为$LCM(n,m)$.

13.25证明：任意无限群必有无限多的子群.

证明：设群为$[G;*]$

(1)若G中有一个元素a的阶为无限，

则令$H_1=\{e,a^1,a^{-1},a^2,a^{-2},\cdots\}$,

$H_2=\{e,a^2,a^{-2},a^4,a^{-4},\cdots\}$,

……

$H_n=\{e,a^n,a^{-n},a^{2n},a^{-2n},\cdots\}$

显然有无限多个子群.

(2)若所有元素的阶均为有限，

$\because G$无限，$\therefore$ 这些元素的个数无限.

记为$\{a_1, a_2, \cdots, a_n, \cdots\}$，

则$(a_1), (a_2), \cdots, (a_n), \cdots$均为$G$的子群，且个数无限.

综上所述，无限群必有无限多的子群.

补充题：1.群G是阶为偶数的有限群，则G中阶为2的元素个数一定是奇数.证明：

对任意一个阶为2的元素$a \in G, a \cdot a = e$, $\therefore a^{-1} = a$;个数记为p;

而对任意一个阶大于2的元素$b \in G$,必有$b \neq b^{-1}$, $b^{-1} \in G$,即(b, b^{-1})成对出现，这种元素个数为偶数；个数记为2q;

单位元e的阶为1;

$\because$G中元素个数为偶数$= 1 + p + 2q$;

$\therefore$p为奇数，即阶为2的元素个数为奇数.

2.设G是rs阶循环群，H_1和H_2分别为G的r阶和s阶子群，证明：$G=H_1H_2$

证明：设a为G的生成元，$G=(a), a^{rs}=e.$

由13.27(1)和(3)，得

H_1, H_2均为循环群，且$H_1=(a^s), H_2=(a^r).$

(1)显然有$H_1H_2 \subseteq G.$

(2)$\forall x \in G, \because G=(a), \therefore x=a^k.$

$(r, s)=1 \Rightarrow \exists m, n \in \mathbf{Z}, s.t. \quad ns+mr=1,$

$\therefore x=a^k=a^{k(ns+mr)}=(a^s)^{kn}\cdot(a^r)^{km} \in H_1H_2.$

$\therefore H_1H_2 \supseteq G.$

$\therefore H_1H_2=G.$

3.[H1;·] [H2; ·]是[G; ·]的子群，[H1∪H2; ·]是否为群[G; ·]的子群？说明理由.

解答：不一定 .

反例： [G;⊕] 模6同余.

H_1 ={[0], [2], [4]}， H_2 ={[0], [3]} [$H_1 \cup H_2$; ⊕]不是群.

另一方面， [G; ⊕] 模8同余.

H_1 ={[0], [2], [4], [6]}, H_1 ={[0], [4]}

[$H_1 \cup H_2$; ⊕]是[G; ⊕]的子群.

4.设H_1,H_2是G的子群，证明$H_1\cdot H_2$是G的子群当且仅当$H_1H_2=H_2H_1$，其中H_1H_2=$\{h_1h_2|h_1$属于H_1并且h_2属于$H_2\}$，$H_2H_1=\{h_2h_1|h_1$属于H_1并且h_2属于$H_2\}$

证明：(1)必要性.

$\forall h_1h_2\in H_1H_2,\because H_1H_2$为子群，$\therefore (h_1h_2)^{-1}\in H_1H_2$，记为$h_1'h_2'$.

$\because H_1,H_2$为子群，$\therefore h_1h_2=(h_1'h_2')^{-1}=(h_2')^{-1}(h_1')^{-1}\in H_2H_1.$

$\therefore H_1H_2\subseteq H_2H_1.$

$\forall h_2h_1\in H_2H_1,(h_2h_1)^{-1}=(h_1)^{-1}(h_2)^{-1}\in H_1H_2.$

$\because H_1H_2$为子群，$\therefore h_2h_1=((h_2h_1)^{-1})^{-1}\in H_1H_2.$

$\therefore H_1H_2\supseteq H_2H_1$

$\therefore H_1H_2=H_2H_1.$

(2)充分性.

$\forall h_1h_2, h_3h_4 \in H_1H_2,$

$(h_1h_2)(h_3h_4)^{-1} = (h_1h_2)(h_4^{-1}h_3^{-1}) = h_1(h_2h_4^{-1})h_3^{-1},$

$h_2, h_4^{-1} \in H_2 \Rightarrow h_2h_4^{-1} \in H_2,$记为$h_6 \in H_2.$

$\therefore (h_1h_2)(h_3h_4)^{-1} = h_1h_6h_3^{-1}.$

$\because (h_6h_3^{-1}) \in H_2H_1,$且$H_1H_2 = H_2H_1,$

$\therefore (h_6h_3^{-1}) \in H_1H_2,$ 记为$h_7h_8 \in H_1H_2.h_7 \in H_1$

$h_8 \in H_2$

$\therefore (h_1h_2)(h_3h_4)^{-1} = h_1h_7h_8 = (h_1h_7)h_8 \in H_1H_2.$

由定理14.15，H_1H_2为子群.