Chap 13: Counting cosets.

G: a group, H: a subgroup of G. $\forall a \in G$.

$aH = \{ah : h \in H\}$ left coset of H in G.

$Ha = \{ha : h \in H\}$ right coset of H in G.

(right) coset is a subset of G

$Ha = Hb$: $Ha \subseteq Hb$ and $Hb \subseteq Ha$

<u>Prop</u>: If $a \in Hb$, then $Ha = Hb$.

<u>Pf</u>: $a \in Hb \Rightarrow a = h_1 b$ for some $h_1 \in H$ $\Rightarrow$ $\forall h \in H$ $ha = hh_1 b \in Hb \Rightarrow Ha \subseteq Hb$

$hb = hh_1^{-1}h_1 b = (hh_1^{-1})a \in Ha$

$\Rightarrow Hb \subseteq Ha$

So $Ha = Hb$.

<u>Thm 1</u>: The family of all the cosets Ha, as a ranges over G, is a partition of G.

<u>Pf</u>: (i) $Ha \cap Hb \neq \emptyset \Rightarrow \exists h_1, h_2$ $h_1 a = h_2 b \Rightarrow a = h_1^{-1} h_2 b \Rightarrow Ha = H \cdot h_1^{-1} h_2 b = Hb$

(ii) $\forall c \in G$. $c = e \cdot c \in Hc$

<u>Thm 2</u>: If Ha is any coset of H, there is a one-to-one correspondence from H to Ha.

<u>Pf</u>: $f: H \to Ha$ $h \mapsto ha$

(i) injective: $h_1 a = h_2 a \Rightarrow h_1 = h_2$

(ii) surjective: $\forall h \in H$, $h \mapsto ha \in Ha$

$\Rightarrow f$ is bijective. or one-to-one correspondence from H to Ha

<u>Thm 3</u> (Lagrange's thm) Let G be a finite group, and H any subgroup of G. The order of G is a multiple of the order of H.

<u>Ex</u>: $|G| = 15 \Rightarrow$ a proper subgroup H has either $|H| = 3$ or $|H| = 5$

Thm 4: If G is a group with a prime number p of elements, then G is a cyclic group. Furthermore, any element $a \neq e$ in G is a generator of G.

So there is, up to isomorphism, only one group of any given prime order p.

Thm 5: The order of any element of a finite group divides the order of the group.

Pf: $|\langle a\rangle| = \mathrm{ord}(a)$ $\quad |\langle a\rangle| \,\big|\, |G|$

Def. $H < G$. The index of H in G, denoted by $(G:H)$, is the number of cosets of H in G:

$$(G:H) = \frac{|G|}{|H|}$$

Exer. A.1 $G = S_3$, $H = \{\varepsilon, \beta, \delta\}$ $\quad \beta = \begin{pmatrix} 1&2&3\\3&1&2\end{pmatrix} = (132)$. $\delta = \begin{pmatrix} 1&2&3\\2&3&1\end{pmatrix} = (123)$.

$\varepsilon = \begin{pmatrix} 1&2&3\\1&2&3\end{pmatrix}$. $\alpha = \begin{pmatrix} 1&2&3\\1&3&2\end{pmatrix} = (23)$, $\gamma = \begin{pmatrix} 1&2&3\\2&1&3\end{pmatrix} = (12)$. $\kappa = \begin{pmatrix} 1&2&3\\3&2&1\end{pmatrix} = (13)$.

$H\alpha = \{\alpha, \beta\alpha, \delta\alpha\}$ $\quad \beta\alpha = (132)(23) = (13)(2) = (13) = \kappa$, $\delta\alpha = (123)(23) = (12)(3) = \gamma$

$= \{\alpha, \kappa, \gamma\}$. $\quad$ There are 2 cosets. $\quad (G:H) = 2 = \frac{|G|}{|H|} = \frac{6}{3}$

$H\varepsilon = \{\varepsilon, \beta, \delta\}$

$G = \mathbb{Z}_4$. $H = \{0, 2\}$ $\quad H+0 = \{0,2\}$, $H + \{1\} = \{1, 3\}$ $\quad$ 2 cosets.

B.1. $G = \mathbb{Z}$, $H = \langle 3\rangle$. $\quad H + 0 = \langle 3\rangle$, $H + 1 = \{1 + 3k;\ k\in\mathbb{Z}\}$

$H + 2 = \{2 + 3k;\ k \in \mathbb{Z}\}$.

B.2: $G = \mathbb{R}$, $H = \mathbb{Z}$. $\quad \forall a \in [0,1)$. $H + a = \{a + k;\ k \in \mathbb{Z}\}$.

cosets: $\{H + a;\ a \in [0,1)\} \cong S^1$.

B.4. $G = \mathbb{R}^*$, $H = \langle \frac{1}{2}\rangle = \{2^k;\ k\in\mathbb{Z}\} = \langle 2\rangle$

Cosets: $\{H\cdot a;\ a \in (\frac{1}{2}, 1] \cup [-1, -\frac{1}{2})\} \cong S^1 \times \mathbb{Z}_2$.

C.2 $|G|=pq$ $\underset{\neq e}{a}\in G \Rightarrow |\langle a\rangle| \mid pq \Rightarrow |\langle a\rangle| = p$, or q, or pq

If $|\langle a\rangle|=pq$, then $G=\langle a\rangle$.

D.6 G abelian $|G|=n$. $(m,n)=1$. $f: G\to G$ $x\mapsto x^m$.

f is a homomorphism: $f(xy)=(xy)^m=x^m y^m=f(x)f(y)$.

need to show that f is a bijection. Because G is finite, enough to show that f is injective. If $f(x)=f(y)$, then $x^m=y^m \Rightarrow (xy^{-1})^m=e$

$\Rightarrow |\langle xy^{-1}\rangle| \mid m$. By lagrange thm, $|\langle xy^{-1}\rangle| \mid n$

So $|\langle xy^{-1}\rangle| \mid \gcd(m,n)$. m,n relatively prime $\Rightarrow |\langle xy^{-1}\rangle|=e$

$\Rightarrow xy^{-1}=e \Rightarrow x=y$. So f is injective $\Rightarrow$ bijective

E.6 Φ. $\{\text{right cosets}\} \longrightarrow \{\text{left cosets}\}$.

$$Ha \mapsto a^{-1}H$$

well-defined: $Ha=Hb \Leftrightarrow ab^{-1}\in H \Leftrightarrow b^{-1}\in a^{-1}H \Leftrightarrow b^{-1}H=a^{-1}H$

injective: $a^{-1}H=b^{-1}H \Leftrightarrow a^{-1}\in b^{-1}H \Leftrightarrow ba^{-1}\in H \Leftrightarrow b\in Ha$
$\Leftrightarrow Ha=Hb$

surjective: $\forall\, bH$. $Hb^{-1}\mapsto bH$.

So Φ is a bijection.

Cauchy's theorem: If G is a finite group, and p is a prime divisor of $|G|$, then G has an element of order p.

F. $|G|=6$. By Cauchy's thm, $\exists$ an element a of order 2 and an element of order 3.

$G=\{e, a, b, b^2, ab, ab^2\}$.

Chap 10. E3 : $ord(a)=m$, $ord(b)=n$, $gcd(m,n)=1 \Rightarrow \{a^i b^j ;\ 0\le i\le m-1,\ 0\le j\le n-1\}$ consists of distinct elements.

Pf. $a^{i_1}b^{j_1}=a^{i_2}b^{j_2} \Rightarrow a^{i_1-i_2}=b^{j_2-j_1}$

$ord(a^{i_1-i_2}) \mid m$, $ord(a^{i_1-i_2}) = ord(b^{j_2-j_1})$, $ord(b^{j_2-j_1}) \mid n$ and $gcd(m,n)=1 \Rightarrow ord(a^{i_1-i_2})=ord(b^{j_2-j_1})=1$

$\Rightarrow a^{i_1-i_2}=b^{j_2-j_1}=e \Rightarrow m \mid i_1-i_2$, $n \mid j_2-j_1$.

Case 1: $ab=ba$: $ord(ab) \overset{\Uparrow}{=} lcm(m,n)=mn$

because $gcd(m,n)=1$: ($\cdot\ ord(ab)\le lcm(m,n) \Leftarrow (ab)^{lcm(m,n)}=e$

$\cdot\ (ab)^k=e \Rightarrow a^k=b^{-k} \Rightarrow ord(a^k) \mid m$, $ord(a^k)=ord(b^{-k})$, $ord(b^{-k}) \mid n$

$\Downarrow$

$ord(a^k)=ord(b^{-k})=1$

$\Downarrow$

$a^k=b^{-k}=e \Rightarrow m \mid k$, $n \mid k$

$\Rightarrow lcm(m,n) \mid k$)

$\Rightarrow G=\langle ab\rangle$ is cyclic $\begin{pmatrix} m=2 \\ n=3 \end{pmatrix}$.

Case 2: $ba=ab^2$: $G\cong S_3$.

a: a reflection, b: a rotation