P134 #36

$U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$

$o(1) = 1$, $o(3) = 4 = o(7)$, $o(9) = 2$, $o(11) = 2$
$o(13) = 4 = o(17)$, $o(19) = 2$

$U(24) = \{1, 5, 7, 11, 13, 17, 19, 23\}$

$o(1) = 1$, $o(5) = 2$, $o(11) = 2$, $o(13) = 2$, $o(17) = 2$
$o(19) = 2$, $o(23) = 2$

$\therefore$ $U(20) \not\cong U(24)$.

---

Cosets

$G$ group, $H$ subgroup of $G$
For $a \in G$
$Ha = \{ha \mid h \in H\}$ right coset
$aH = \{ah \mid h \in H\}$ left coset

- $aH = bH \iff a^{-1}b \in H$
- $aH = H \iff a \in H$

---

Suppose $G$ abelian. Then $H$ is abelian
$\Rightarrow$ $ha = ah$ $\forall a \in G$, $h \in H$
$\Rightarrow$ $Ha = aH$.

Ex(1) $G = S_3 = \{\underset{\| e}{(1)}, (12), (23), (13), (123), (132)\}$

$H = \langle (123) \rangle = \{(123), (132), (1)\}$

$K = \langle (12) \rangle = \{(12), (1)\}$

$H = H(1)$

$H(12) = \{(123)(12), (132)(12), (1)(12)\}$

$= \{(13), (23), (12)\}$

$\Rightarrow G = H \cup H(12)$

$H = (1)H$

$(12)H = \{(12)(123), (12)(132), (12)(1)\}$

$= \{(23), (13), (12)\}$

$= H(12)$

$K = K(1)$

$K(123) = \{(12)(123), (1)(123)\}$

$= \{(23), (123)\}$

$K(132) = \{(12)(132), (1)(132)\}$

$= \{(13), (132)\}$

$\Rightarrow G = K \cup K(123) \cup K(132)$

$K = (1)K$

$(123)K = \{(123)(12), (123)(1)\}$

$= \{(13), (123)\} \neq K(123)$

$(132)K = \{(132)(12), (132)(1)\}$

$= \{(23), (132)\} \neq K(132)$

$\Rightarrow G = K \cup (123)K \cup (132)K$.

In general, $aH \neq Ha$.

Prop: $G$ group, $H$ a subgroup of $G$ and $|G|/|H| = 2$. Then $aH = Ha \ \forall a \in G$

---

$G$ finite group. Say $|G| = n$

Let $H$ be any subgroup of $G$. Then

$$G = H \cup Ha_1 \cup \cdots \cup Ha_k$$

disjoint union of right cosets. Since $|Ha_i| = |H|$, we have

$$|G| = (k+1)|H|$$

$\Rightarrow |H| \mid |G|$.

Lagrange's Thm: Let $G$ be a finite group and $H$ a subgroup of $G$. Then $|H| \mid |G|$.

Consequences of Lagrange Thm:

(1) Suppose $|G| = p$, $p$ prime

Choose $e \neq a \in G$. Consider $H = \langle a \rangle$. Then $|H| \neq 1$ & $|H| \mid p \Rightarrow H = \langle a \rangle = G$

$\Rightarrow$ $G$ is cyclic.

Remark: Converse of Lagrange Thm is not true.

Example: $G = A_4$, $|G| = |A_4| = \frac{1}{2}(4!) = 12$

$6 \mid |G|$, but $A_4$ does not have a subgroup of order 6.

HW P150 # 1, 3, 5, 7, 9, 15, 16, 17, 22, 39

Lagrange's Thm: $G$ finite group and $H$ subgroup of $G$. Then $|H| \mid |G|$.

Consequences:

(1) $|G| = p$, prime

$\Rightarrow$ $G$ is cyclic.

(2) $|G| = n$ and $a \in G$

Then $o(a) \mid |G|$.

$o(a) = |\langle a \rangle| \mid |G|$

(3) $|G| = n$, $a \in G$

$\Rightarrow a^{|G|} = e$

$o(a) \mid n \Rightarrow n = kl$, $a^k = e$

$a^n = a^{kl} = (a^k)^l = e^l = e$.

(4) $p$, $m \in \mathbb{Z}$, $p$ prime

$\Rightarrow p \mid (m^p - m)$

(Equivalently, $m^p - m \equiv 0 \pmod{p}$)

By division algorithm

$$m = pk + r \quad , \quad 0 \le r < p$$

$$\Rightarrow \quad pk = m - r \Rightarrow p \mid (m-r)$$

$$\Rightarrow \quad m \pmod p = \underbrace{r \pmod p}_{\| \; r}$$

$$\Rightarrow (m \pmod p)^p = (r \pmod p)^p$$

$$m^p \pmod p \qquad r^p \pmod p$$

Suppose $r = 0 \Rightarrow p \mid m \Rightarrow p \mid (m^p - m)$

Assume $r \neq 0 \Rightarrow 1 \le r \le p-1$

$\Rightarrow r \in U(p)$, $|U(p)| = p-1$

$\Rightarrow r^{p-1} = 1 \Rightarrow r^p = r$

$\Rightarrow r^p \pmod p = r \pmod p$

$$m^p \pmod p = m \pmod p$$

$\Rightarrow p \mid (m^p - m)$.

---

Defn: $G$ finite group, $H$ subgroup

(# of distinct cosets of $H$ in $G$) $= i_G(H)$

called "index of $H$" in $G$.

P152 #39

$H$, $K$ subgroups of a group $G$.

$|H| = 24$, $|K| = 20$.

$H \cap K$ subgroup of $G$

$H \cap K \subset H$, $H \cap K \subset K$

$\Rightarrow |H \cap K| \mid |H| = 24$, $|H \cap K| \mid |K| = 20$

$\Rightarrow |H \cap K| \mid \underbrace{\gcd(24, 20)}_{= 4}$

$\Rightarrow |H \cap K| = 1, 2, \text{ or } 4$

$|H \cap K| = 1 \Rightarrow H \cap K = \{e\}$ abelian

$|H \cap K| = 2$, prime $\Rightarrow H \cap K$ cyclic

$\Rightarrow H \cap K$ abelian.

$|H \cap K| = 4$. $e \neq a \in H \cap K$

$o(a) \mid 4$

If $a \in H \cap K$ and $o(a) = 4$, then $H \cap K$ cyclic, hence abelian.
If $H \cap K$ does not have any elements of order 4, then all nonidentity elements have order 2, Hence $H \cap K$ is abelian.

Test 2, Oct 18 Wednesday
Chaps 3, 4, 5, 6, 7

P152 #39

$|H| = 24, \quad |K| = 20$

$H \cap K$ subgroup
$H \cap K \subset H \Rightarrow |H \cap K| \mid |H| = 24$
$H \cap K \subset K \Rightarrow |H \cap K| \mid |K| = 20$
$\Rightarrow |H \cap K| \mid \gcd(24, 20) = 4$
$\Rightarrow |H \cap K| = 1, 2 \text{ or } 4$

$|H \cap K| = 1 \Rightarrow H \cap K = \{e\}$ abelian
$|H \cap K| = 2$ prime $H \cap K$ cyclic $\Rightarrow$ abelian

$|H \cap K| = 4$:
Suppose $H \cap K$ contains $x \in H \cap K$ such that $o(x) = 4$. Then $H \cap K$ is cyclic, hence abelian.
If not, all nonidentity elements in $H \cap K$ has order 2.
Suppose $a, b \in H \cap K$, $a \neq e$, $b \neq e$, $b \neq a^{-1}$
$o(a) = 2 \Rightarrow a = a^{-1}$, $o(b) = 2 \Rightarrow b = b^{-1}$
$o(ab) = 2 \Rightarrow (ab)^{-1} = ab$
$b^{-1}a^{-1} = ba$ $\Rightarrow H \cap K$ abelian.

P151 #16 $\{e\} \neq K \subsetneq H \subsetneq G$

$|K| = 42$ , $|G| = 420$

$|H| = ?$

$|K| \mid |H|$ , $|H| \mid |G|$

$\|$ 42 $\|$ 420

$|H| = 84$ or $210$.

P150 #7.

$o(a) = 30$ , $G = \langle a \rangle$

$H = \langle a^4 \rangle = \{a^4, a^8, a^{12}, a^{16}, a^{20}, a^{24}, a^{28}, a^2, a^6, a^{10}, a^{14}, a^{18}, a^{22}, a^{26}, e\}$

The distinct cosets are:

$H = He$ , $Ha = aH$

$\|$

$eH$

P132 #12 $G$ group

$\alpha : G \longrightarrow G$ , $\alpha(g) = g^{-1}$

$\alpha$ is clearly 1-1 and onto.

Suppose $\alpha$ is a hom.

$\forall\ g_1, g_2 \in G$

$$\alpha(g_1 g_2) = \alpha(g_1)\alpha(g_2)$$

$$\| \qquad\qquad \| \qquad\qquad \|$$

$$(g_1 g_2)^{-1} = g_1^{-1} g_2^{-1}$$

$$\Rightarrow \quad g_1 g_2 = (g_1^{-1} g_2^{-1})^{-1} = g_2 g_1$$

$\Rightarrow$ $G$ abelian.

Suppose $G$ abelian

$\forall\ g_1, g_2 \in G$

$$\alpha(g_1 g_2) \stackrel{?}{=} \alpha(g_1)\alpha(g_2)$$

$$\| \qquad\qquad \|$$

$$(g_1 g_2)^{-1} \qquad g_1^{-1} g_2^{-1}$$

$$\| \qquad\qquad \| \qquad \text{since } G \text{ abelian}$$

$$g_2^{-1} g_1^{-1}$$

$\therefore$ $\alpha$ is an automor.

P133 #32

$\varphi : \mathbb{Z}_{50} \longrightarrow \mathbb{Z}_{50}$, $\varphi(7) = 13$

automorphism

$\varphi(x) = ?$ for any $x \in \mathbb{Z}_{50}$.

$\mathbb{Z}_{50} = \langle 1 \rangle$, $\varphi(1) = ?$

$$\varphi(1) = -\varphi(-1) = -\varphi(49)$$

$$= -\varphi(\underbrace{7+\cdots+7}_{7 \text{ times}}) = -(\underbrace{13+\cdots+13}_{7 \text{ times}})$$

$$= -41 = 9$$

$$\Rightarrow \varphi(x) = 9x .$$