2.6 Classification of finite groups

Theorem: Suppose $|G| = pq$, where p, q are prime and $qn \neq p-1 \quad \forall n \in Z$.

Then $G \cong Z_{pq}$.

pf : $|Sylp(G)| = kp+1 \,|\, q \Rightarrow |Sylp(G)| = 1$

Say $H \in Sylp(G)$, then $H \lhd G$.

Also, $|Sylq(G)| = kq+1 \,|\, p \Rightarrow |Sylq(G)| = 1, q+1, 2q+1.....$

The assumption $qn \neq p-1 \quad \forall n \in Z$ implies $|Sylq(G)| = 1$.

Say $K \in Sylq(G)$.

Note : $H \cap K = \langle e \rangle$, since $(p,q) = 1$.

Hence $G = H \times K \cong Z_P \times Z_q \cong Z_{pq}$.

Suppose $q < p$ primes and $q \,|\, p-1$.

Fix $2 \leq s \leq p-1$, $s^q \equiv 1 \mod p$,

Set $:= \{a^i b^j \,|\, 0 \leq i \leq p-1, 0 \leq j \leq q-1\} \cong Z_p \nabla_s Z_q$,

where $a^p = b^q = e$, $ba = a^s b$, $(\langle a \rangle \lhd K)$

Theorem: Suppose $|G| = pq$, $q < p$ primes and $q \,|\, p-1$. Suppose G is not abelian. Then $G \cong K$.

pf : As before $|Sylp(G)| = 1$. Hence $H \in Sylp(G) \Rightarrow H \lhd G$.

Assume $H = \langle a \rangle$ foe some $a \in G$ with $|a| = |h| = p$.

Pick any $b_1 \in G - \langle a \rangle$. Then $b_1 a b_b^{-1} = a^k$ for some $1 \le k \le p-1$

If $k = 1$ then $b_1 a = a b_1$, and note that $\langle a \rangle \cap \langle b_1 \rangle = \langle e \rangle$,

hence $\left| \langle a \rangle \langle b_1 \rangle \right| = \dfrac{|\langle a \rangle||\langle b \rangle|}{|\langle a \rangle \cap \langle b_1 \rangle|} \ge \dfrac{pq}{1}$

Then $G = \langle a \rangle \langle b_1 \rangle$ is abelian. $\rightarrow\leftarrow$

Hence $k \ne 1$, note $$b_1 a b_b^{-1} = \left(\left(\left(\left(a^k \right)^k \right)^k \right)^{k^{\cdot^{\cdot^{\cdot}}}} \right)^k = a^{k^t}$$

Note $|b_1| = q$. Hence $a = b_1^q a b_1^{-q} = a^{k^q}$ and $a \ne a^{k^i}$ for $1 \le i \le q-1$, otherwise G is abelian. $\left(a = b_1^t a b_1^{-t} \Leftrightarrow a b_1^t = b_1^t a \right)$

Hence $p \mid k^q - 1$, but $pn \ne k^i - 1 \quad \forall n \in N$ for $1 \le i \le q-1$.

Then k is a "primitive" root of $x^q = 1$ in Z_p.

i.e. $\{ k, k^2, k^3, k^4 \ldots k^q = 1 \}$ is the set of all root of $x^q = 1$ in Z_p.

(Here "all" is related to ① U_p is cyclic

② $\{ a \in Z_p \mid a^q = 1 \}$ is a subgroup of U_p

③ A subgroup of cyclic group is cyclic)

Since $s^q = 1$, we have $k^i = s$ for some $1 \le i \le q$

Choose $b = b^i$. Then $bab^{-1} = b_1^i a b_1^{-i} = a^{k^i} = a^s$.

Thus $G = \langle a \rangle \langle b \rangle = k$.