G: finite. with $|G| = p^e m$ s.t. $\gcd(p, m) = 1$. (Notation: $|G|_p = p^e$)

A Sylow p-subgroup is a subgroup $H \le G$ s.t. $|H| = p^e$.

① existence?

② relations between Sylow p-subgroups?

③ How many Sylow p-subgroups?

Theorem 1 (1st).

Sylow subgroups exist.

Theorem 2. (2nd). Sylow p-subgps of G are all conj. In particular, G has only one Sylow p-subgp $\Leftrightarrow$ the Sylow p-subgp $\lhd G$.

Let P be a Sylow p-subgp and let $H \le G$ s.t. $|H| \mid p^e$. Then H is conjugate to a subgroup of P. In particular, all Sylow p-subgps are conjugate. i.e. G is transitive on $Syl_p(G)$

Proof: Let $\Omega = [G:P] = \{Px \mid x \in G\}$.

Then G acts on Ω by right multiplication. $g: \Omega \to \Omega$, $Px \longmapsto Pxg$. $\forall g, x \in G$

Then the map is a group action of G on Ω,

and is transitive (called a coset action), with $P = G_{w_0}$, where w_0 is the point corresponding to P.

Of course, H acts on Ω, which may be intransitive. The subgp $P \le G$ fixes the point $P \in \Omega$.

$P = w_0 \in \Omega$. $w_0^x = Px = P = w_0$ for $x \in P$.

$\Rightarrow P \le G_{w_0}$.

The size of $|\Omega| = \dfrac{|G|}{|P|} = m. = \sum |Orb(Px)|$.

For $x \in G_{w_0}$, $\underset{Px}{\underset{\parallel}{w_0^x}} = w_0 = P \Rightarrow x \in P$.

Each orbit of H on Ω has size dividing $|H|$.

So there is an orbit of H which is of size equal to 1, namely, H fixes a point $w \in \Omega$.

Now $G_w = \{g \in G \mid w^g = w\}$ is conjugate to $P = G_{w_0}$.

by an elt. y s.t. $w^y = w_0$.

Since H fixes w, we have $H \le G_w = y^{-1} G_{w_0} y = y^{-1} P y$. $\square$

$g^{-1} G_\alpha g = G_{\alpha g}$

$x \in g^{-1} G_\alpha g \Leftrightarrow x = g^{-1} h g$ for some $h \in G_\alpha$

$\Leftrightarrow g x g^{-1} = h \in G_\alpha \Leftrightarrow \alpha^{g x g^{-1}} = \alpha$

$\Leftrightarrow (\alpha^g)^x = \alpha^g \Leftrightarrow x \in G_{\alpha g}$.

Theorem 3. (3rd).

Let n_p be the # of Sylow p-subgps, then $n_p \mid m$ and $n_p \equiv 1 \pmod p$.

$P \lhd N \le G$.

Proof: Let $P \in Syl_p(G)$, and let $N = N_G(P) = \{g \in G \mid g^{-1} P g = P\}$. called the $\boxed{\text{normalizer}}$ of P in G.

Then $m = \dfrac{|G|}{|P|}$, $n_p = |Syl_p(G)|$. By theorem 2, G is transitive on $Syl_p(G)$, with a stablizer $N_G(P)$. so that $|Syl_p(G)| = \dfrac{|G|}{|N_G(P)|}$.

Observe $n_p \cdot \frac{|N_G(P)|}{|P|} = \frac{|G|}{|N_G(P)|} \cdot \frac{|N_G(P)|}{|P|} = \frac{|G|}{|P|} = m$. So $n_p \mid m$.

by right multiplication.

$\Omega = [G:P]$, $\Delta = Syl_p(G)$. Then G is transitive on Ω with a stab. P.

transitive on Δ with a stab. $N_G(P)$

by conjugation.

Since $P \le N_G(P)$, we have $\underset{n_p}{\underset{\shortparallel}{|\Delta|}} \Big| \underset{m.}{\underset{\shortparallel}{|\Omega|}}$

Recall $\Delta = Syl_p(G)$, size n_p.

Now, P acts on Δ by conjugation.

Then each orbit of P has size dividing $|P|$. As $g.c.d.(n_p, p) = 1$,

There is $\boxed{\text{exactly one}}$ obit which of size 1. $\to$ P only fixes P in Δ.

$n_p = |\Delta| = |\Delta_1| + |\Delta_2| + \cdots + |\Delta_t| = 1 + |\Delta_2| + \cdots + |\Delta_t| \equiv 1 \pmod p$. $\square$

Let $P, Q \in Syl_p(G)$

Then by conjugation, P fixes Q

iff $x^{-1}Qx = Q \quad \forall x \in P$.

So $x \in N_G(Q) \geq P, Q$.

Since $Q \lhd N_G(Q)$, $y^{-1}Qy = Q$, $\forall y \in N_G(Q)$.

But P, Q conjugate, $P = \underset{Q.}{\underset{\shortparallel}{y^{-1}Qy}}$ for some y

$\Rightarrow N_G(Q)$ only has only one Sylow p-subgp.

Conj. Let n be an integer which is not a power of a prime,

Then there exists a gp G of order divisible by n

s.t. G does not have a subgroup of order n.

Ex. If a group G is of order $2p$ with p prime, then $G = C_{2p}$ or D_{2p}.

Proof: If $p = 2$, the $|G| = 4$. $G = C_4$ or $C_2 \times C_2 = D_4$.

Let p be an odd prime, then $n_p \mid 2$, $n_p = 1 \pmod p$. $\Rightarrow n_p = 1$.

and so $\overset{C_p \cong}{P} \lhd G$. Write $P = \langle g \rangle$. Let Q be a Sylow 2-subgp.

Then $g^x \in \langle g \rangle$, and $g^x = g^i$ for some integer $i \in \{1, 2, \cdots, p-1\}$.

Noticing that $g^x = x^{-1}gx = g^i$. $(\underset{g}{\underset{\shortparallel}{x^{-1}gx}})^x = (g^x)^x = (g^i)^x = g^{i^2}$. we have $i^2 \equiv 1 \pmod p$.

So $i = 1$ or -1 and $G = \langle g, x \mid g^p = 1 = x^2, g^x = \overset{\text{abelian.}}{g} \text{ or } \underset{\text{dihedral.}}{g^{-1}} \rangle = C_{2p}$ or D_{2p}. $\square$

Ex. Let $|G| = pq$, where $p > q$ are primes, then $G_p \lhd G$, i.e. $n_p = 1$,

and G is cyclic or $q \mid (p-1)$.

Proof: $n_p \mid q$ and $n_p = kp + 1 \mid q$ for some k $\Rightarrow$ $k = 0$ and $n_p = 1$. i.e. $G_p \lhd G$.

Next, $n_q = kq + 1 \mid p$, so $kq + 1 = 1$ or $kq + 1 = p$. $\Rightarrow n_q = 1$ or $kq = p - 1$

$\Rightarrow G \underset{?}{=} G_p \times G_q = C_{pq}$ or $\underline{q \mid p-1}$. $\square$

$M, N \lhd G \underset{?}{\Rightarrow} M \cap N = \{1\}$.

$g^x = g^i$ for some integer i.

$G = G_p : G_q = \langle g \rangle : \langle x \rangle = C_p : C_q$.