DEF. A group whose order is p^b for some prime p and integer $b \geq 0$ is a p-group.

NOTATION. Given an action of a group G on a set X, we say an element $x \in X$ is fixed by the action, and write $x \in X^G$, if $gx = x$ for all $g \in G$.

THM A. For each action of a p-group P on a finite set X,

$$|X| \equiv |X^P| \bmod p \quad *)$$

(For $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$, we write $a \equiv b \bmod m$ if $m \mid a-b$.)

Proof. The orbit sizes are divisors of $|P|$, hence they are of the form p^c with $c \geq 0$. The orbits of size 1 make up X^P. Therefore $X - X^P$ is a disjoint union of orbits of sizes p^c with $c > 0$. Each such size is divisible by p, so $p \mid |X| - |X^P|$.

THM B. Each nontrivial p-group has nontrivial center.

Proof. Let P be a p-group. In the action of P on P by conjugation, the elements fixed by the action make up the center $Z(P)$ of P. By THM A,

$$|P| \equiv |Z(P)| \bmod p.$$

If P is a nontrivial p-group, then $p \mid |P|$, so $p \mid |Z(P)|$, so $Z(P) \neq 1$.

LEMMA. Let G be a group. If $G/Z(G)$ is cyclic, then G is abelian.

Proof. If $G/Z(G) = \langle gZ(G) \rangle$, then each element of G is of the form $g^k z$ for some $k \in \mathbb{Z}$ and some $z \in Z(G)$. If $g^{k'} z'$ is another such element

$$g^k z \cdot g^{k'} z' = g^{k+k'} zz' = g^{k'+k} z'z = g^{k'} z' \cdot g^k z,$$

showing G is abelian.

COR. For prime p,

(1) Each group of order p^2 is abelian (& $G \cong C_{p^2}$ or $C_p \times C_p$).

(2) Each nonabelian group P of order p^3 has $|Z(P)| = p$ and $P/Z(P) \cong C_p \times C_p$.

Proof. Let P be a nonabelian p-group. Then $P/Z(P)$ is not cyclic, by the Lemma, but $Z(P) \neq 1$, by THM B. If $|P| = p^2$ this is impossible, proving (1). If $|P| = p^3$, the lemma implies $|Z(P)| = p$ and $|P/Z(P)| = p^2$ and not cyclic ... .

THM C Let G be a finite group, P a p-subgroup, H a subgroup of index not divisible by p. Then P is contained in a conjugate $H^g = gHg^{-1}$ of H.

Proof. G acts on G by left translation and therefore on $S(G)$, the set of all subsets of G. Since $g_1 g' H = gg' H$, it follows that G stabilizes G/H (the set of all left cosets of H in G). Therefore G, and also P, acts by left translation on G/H. By THM A,

$$|G/H| \equiv |(G/H)^P| \mod p.$$

Since $p \nmid |G/H|$, it follows that $p \nmid |(G/H)^P|$, so $(G/H)^P \neq \phi$, ie P fixes some left H-coset in G: $PgH = gH$, so $PgH \subset gH$, so $PgHg^{-1} = H^g$.

DEF Let G be a finite group, and let p be a prime. A <u>Sylow</u> p-subgroup of G is a p-subgroup S of G whose index is not divisible by p, ie a subgroup S of G whose order is the highest power of p dividing $|G|$.

EXAMPLE If $|G| = 12$, then a Sylow 2-(or 3-or 5-)subgroup of G would have order 4 (or 3 or 1).

The next three results were conjectured by Sylow (18 =) in 1862 and proved in 1872.

THM D Each finite group G has at least one Sylow p-subgroup, for each prime p. In fact, the number $s_p(G)$ of Sylow p-subgroups of G satisfies

$$\boxed{s_p(G) \equiv 1 \bmod p.}$$

LEMMA. If H_1 & H_2 are subgroups of G and $H_1 g_1 = H_2 g_2$ for some $g_1, g_2 \in G$, then $H_1 = H_2$.

Proof $H_1 g_1 = H_2 g_2 \Rightarrow H_1 = H_2 g$ (with $g = g_2 g_1^{-1}$), so $1 \in H_2 g$ so $H_2 g = H_2$, so $H_1 = H_2$

Proof of Thm D. Let $|G| = p^q m$ with $p \nmid m$. We have an action of G by left translation on the set $\mathcal{A}$ of all subsets $A \subset G$ with $|A| = p^q$.

For $A \in \mathcal{A}$, if G_A is the stabilizer of A, then $G_A A = A$, so A is a union of some right cosets of G_A. Therefore $|G_A|$ divides p^q.

If $|G_A| = p^q$, then G_A is a Sylow p-subgroup of G and A is a right coset of G_A. Conversely, for each Sylow p-subgroup S of G each right coset Sg is fixed by S ($S \cdot Sg = Sg$), so S is the stabilizer of Sg.
By the Lemma, the number of $A \in \mathcal{A}$ with $|G_A| = p^q$ is therefore $s_p(G) \cdot m$.

If $|G_A|$ divides p^{q-1}, then A belongs to an orbit of size divisible by p.
The number of such A is therefore divisible by p.

It follows that

$$\checkmark \qquad |\mathcal{A}| \equiv s_p(G) m \bmod p.$$

If we now replace G by a cyclic group of the same order, then $\mathcal{A}$ & m are unchanged!

$$\checkmark\!\checkmark \qquad |\mathcal{A}| \equiv s_p(C) m \bmod p.$$

By $\checkmark$ & $\checkmark\!\checkmark$, since $p \nmid m$ we conclude that

$$* \qquad s_p(G) \equiv s_p(C) \bmod p$$

But C has exactly one subgroup of order p^q, & $s_p(C) = 1$.

THM E For each finite group G and each prime p, the Sylow p-subgroups are all conjugate to each other, so $s_p(G) = |G/N_G(S)|$, for each Sylow p-subgroup S of G, where $N_G(S) = \{g \in G : S^g = S\}$ (the normalizer of S in G, a subgroup of G). Therefore

$$\boxed{s_p(G) \text{ divides } |G/S|}.$$

THM F Let G be a finite group and p a prime. Then each p-subgroup of G is contained in a Sylow p-subgroup of G

Proofs of Theorems E and F. Let P be a p-subgroup of G and let S be a Sylow p-subgroup of G. Since $p \nmid |G/S|$, Thm C implies $P \subset S^g$ for some $g \in G$. Since $|S^g| = |S|$ it follows that S^g is also a Sylow p-subgroup of G. In particular if P is a Sylow p-subgroup of G, so $|P| = |S|$, then $P = S^g$.

Since the Sylow p-subgroups are all conjugate, i.e. make a single orbit in the action of G by conjugation on $\mathcal{S}(G)$, it follows that $s_p(G)$ is the index of the stabilizer, i.e. normalizer, of any one of them.

COR 1. (Cauchy) If G is a finite group and p is any prime divisor of $|G|$, then G has at least one element of order p.

Proof. Let S be a Sylow p-subgroup of G. Then $|S| = p^a$ for some $a \geq 1$. Let s be an element $\neq 1$ in S. Then s has order p^b for some $b \geq 1$, so $s^* = s^{p^{b-1}} \neq 1$ but $s^{*p} = 1$, i.e. s^* has order p.

EXERCISE 1. Let G be a group of order $p^a m$ with $p \nmid m$. Prove that if m has no divisor $d > 1$ with $d \equiv 1 \bmod p$, then a Sylow p-subgroup of G is normal.

EXERCISE 2. Let G be a finite group, $K \lhd G$, P a Sylow subgroup of K, $H = N_G(P)$. Prove $G = HK$.