Théorème (Cauchy) Soit G un groupe fini et $p \in \mathbb{N}$ premier tel que $p \mid |G|$. Alors il existe un élément d'ordre p dans G.

preuve : e = neutre. On pose $X = \{(g_1, \dots g_p) \in G^p \mid g_1 \cdots g_p = e\}$

On fait agir $H = \underbrace{\langle (1 \dots p) \rangle}_{\text{cyclique ordre } p}$ sur X : si $\sigma \in H$, $\sigma \cdot (g_1, \dots g_p) := (g_{\sigma(1)}, \dots g_{\sigma(p)})$ (décalement à gauche)

On remarque une bijection $X \longrightarrow G^{p-1}$, $(g_1, \dots g_p) \longmapsto (g_1, \dots g_{p-1})$ puisque g_p est l'inverse de $g_1 \cdots g_{p-1}$.

donc $\text{card}(X) = |G|^{p-1}$

On pose N le nombre d'orbites distinctes et $\text{orb}(x_1), \dots \text{orb}(x_N)$ ces orbites.
$J := \{i \in [\![1; N]\!],\ \text{orb}(x_i) = \{x_i\}\}$.

On remarque que $\text{orb}(x) = \{x\} \iff x$ est un point fixe sous l'action.
$\iff x = (g_1, \dots g_1)$
en effet si $\forall k \in [\![1; p-1]\!]$ $g_{(1 \dots p)^k(1)} = g_1 \Rightarrow g_{k+1} = g_1$ donc $g_1 = \dots = g_p$.

Par la formule des classes on obtient :

$$\text{card}(X) = |G|^{p-1} = \underbrace{\sum_{i \in J} \text{card}(\text{orb}(x_i))}_{= \text{card}(J)} + \sum_{i \in J^c} \text{card}(\text{orb}(x_i))$$

et il y a une bijection entre I et l'ensemble X^H des points fixes sous l'action :

$J \longmapsto E$, $i \longmapsto x_i$ l'équation devient alors $|G|^{p-1} = \text{card}(X^H) + \sum_{i \in J^c} \overbrace{\text{card}(\text{orb}(x_i))}^{>1}$

De plus, $\forall i \in J^c$, $\text{card}(\text{orb}(x_i)) \cdot |\text{stab}(x_i)| = |H| = p$ en particulier $\forall i \in J^c$, $\text{card}(\text{orb}(x_i)) = p$

en réduisant mod p on obtient $0 \equiv \underbrace{\text{card}(X^H)}_{\geq 1} + 0 \ [p]$ donc $\text{card}(X^H) \geq p$

En remarquant que $x = (g \dots g) \in X^H \iff g^p = e \iff g = e$ ou g est d'ordre p. (p est premier)
$\uparrow$ ordre$(g) \mid p$

on en conclut qu'il existe au moins $p-1$ éléments d'ordre p : donc au moins un. □

Proposition : Soit G un groupe fini et p le plus petit diviseur de $|G|$. Supposons qu'il existe $H < G$ d'indice p. Alors $H \lhd G$.

preuve : On considère l'action $G \xrightarrow{\delta} \text{Bij}(G/H)$, $g \longmapsto \left(\begin{array}{c} G/H \longrightarrow G/H \\ P \longmapsto gP \end{array}\right)$

On pose $K = \ker(\delta) = \{g \in G \mid \forall P \in G/H,\ gP = P\} \lhd G$. et on montre que $H = K$.
si $g \in K$, g stabilise H donc $g \in H$ et $\boxed{K \in H}$

Par le Thm d'iso : $G/K \simeq \text{Im}(\rho)$ et par Lagrange, $|\text{Im}(\rho)| \mid p!$
donc $\frac{|G|}{|K|} \mid p!$: $\exists q \in \mathbb{N}$, $p! \, |K| = |G| \cdot q$ donc $\frac{|G|}{p} \mid (p-1)! \, |K|$ mais $\frac{|G|}{p} \wedge (p-1)! = 1$

car si $\tilde{p}$ premier divise $\frac{|G|}{p}$ et $(p-1)!$ alors $\tilde{p} < p$ et $\tilde{p} \mid \frac{|G|}{p} \mid |G|$ absurde donc par le Lemme de Gauss,

$\frac{|G|}{p} = |H| \mid |K|$ donc $H = K \lhd G$. □

Le sommaire : 101 : groupe opérant sur un ensemble
104 : groupes finis

Remarque : un tel sous groupe n'existe pas forcément :

Si G est simple et $|G| \neq p$ si $\exists H$ d'indice p on aurait $H \lhd G \Rightarrow$ $H = \{e\}$ (impossible car $|G| \neq p$) ou $H = G$ (impossible car indice $p \neq 1$)

On prend l'exemple de A_5 :
A_5 simple, $|A_5| = 60 = 2 \times 30$ mais $\exists H < A_5$ tq $|H| = 30$ (i.e $[A_5 : H] = 2$) car A_5 est simple.

une application sans la Théorie des Sylow :

Soit G un groupe d'ordre 15 : $G \simeq \mathbb{Z}/15\mathbb{Z}$.

En effet par le Théorème de Cauchy, il existe H, K sous groupes d'ordre respectifs 5 et 3. Puisque $[G:H] = 3$ Par la proposition $H \lhd G$. De plus par Lagrange $H \cap K = \{e\}$ il vient que $G = H.K$ et $G \simeq \mathbb{Z}/5\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$

où $\varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$ est un morphisme. Comptons le nb de φ possibles :

$\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z}) \simeq \mathbb{Z}/4\mathbb{Z}$ donc cela revient à compter le nb de morphismes $\mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z}$: 1 seul puisque

si $x \in \mathbb{Z}/3\mathbb{Z} \setminus \{0\}$ on a $\varphi(x)$ d'ordre un diviseur de 3 et de 4 : 1 donc $\varphi(x) = 0$.

Donc φ est le morphisme trivial : $G \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/15\mathbb{Z}$

---

questions posées : groupes d'ordre 15. (Je m'y attendais...)

$\exists |H| = 5$, $|K| = 3$ et on a $H \lhd G$. K agit sur H par conjugaisons
formule des classes :
$5 = \sum_{i=1}^{N} \underbrace{|\mathrm{orb}(x_i)|}_{1 \text{ ou } 3}$ si une seule d'ordre 1 : $5 \equiv 1 [3]$: Absurde

soit donc $h \in H \setminus \{1\}$, $|\mathrm{orb}(h)| = 1$ alors $\forall g \in K$, $gh = hg$. H est cyclique engendré par h donc les éléments de H commutent avec ceux de K. De plus, $G = H.K$ (cardinaux)
donc $G \simeq H \times K \simeq \mathbb{Z}/15\mathbb{Z}$.

d'ordre p^2 : analogue

—

donner un sous groupe de S_n d'indice $n-1$: $\underbrace{\{\sigma \in S_n \mid \sigma(i) = i\}}_{H_i}$ d'ordre $(n-1)!$ donc indice n.
est-il distingué ? Non : si $\tau = (12)$, H_1 : $\tau H_1 \tau^{-1} = H_2 \not\subset H_1$ donc pas distingué.
soit $h \in H_1$, $\tau h \tau^{-1}(2) = 2$ donc $\tau H_1 \tau^{-1} \subset H_2$
si $h \in H_2$, $h = \tau \underbrace{\tau^{-1} h \tau}_{\in H_1 ?} \tau^{-1}$ $\quad \tau^{-1} h \tau(1) = \tau^{-1} h(2) = \tau^{-1}(2) = 1$

—

que dire du Thm de cauchy si p pas premier ? Faux en général : S_3 pas cyclique mais pour les $p^{v_p(m)}$ où $|G| = m$ c'est vrai : Thm de Sylow.

À quoi servent les sous gpe distingués ?

A avoir une structure de groupe du quotient tel que la proj canonique soit un morphisme.

Est ce équivalent ?

oui $p : G \to G/H$ est un morphisme ss: $H \lhd G$.