Conjugaison, Sous-groupe normal, Normalisateur, Centre

$(G,\cdot)$ groupe quelconque de neutre e, $H\leq G$ sous-groupe.

Action de conjugaison : C'est l'action de G *sur lui-même* définie par

$$\begin{array}{rcl} \mathrm{conj} : G\times G & \longrightarrow & G \\ (g,h) & \longmapsto & ghg^{-1} \end{array}$$

Soit $g\in G$. Le sous-groupe conjugué de H par g est isomorphe à H : $\boxed{H\cong gHg^{-1}}$. En particulier, $|gHg^{-1}|=|H|$ si H fini.
En effet, $H\to gHg^{-1} : h\mapsto ghg^{-1}$ est un morphisme, d'inverse $gHg^{-1}\to H : ghg^{-1}\mapsto h$ bien défini car

$$\forall h_1,h_2,\quad gh_1g^{-1}=gh_2g^{-1} \implies gh_1g^{-1}g=gh_2g^{-1}g \implies gh_1=gh_2 \implies h_1=h_2$$

H sous-groupe **distingué/normal dans G** $\overset{\text{def}}{\Leftrightarrow}$ H est (globalement) stable par l'action de conjugaison :

$$\mathrm{Orb}_{\text{conj}}(H)=G\,\mathrm{conj}\,H\subset H \quad\Leftrightarrow\quad \boxed{H\trianglelefteq G \overset{\text{def}}{\Leftrightarrow} \forall g\in G,\ gHg^{-1}\subset H} \quad\Leftrightarrow\quad \forall g\in G,\ \forall h\in H,\ ghg^{-1}\in H$$

$$\Leftrightarrow\quad \forall g\in G,\ gH=Hg \quad\Leftrightarrow\quad \forall g\in G,\ gHg^{-1}=H$$

On note $H\triangleleft G$ lorsque H est un sous-groupe strict.

L'**intersection** de deux sous groupes normaux est normale : $\forall H,K\leq G$ sous-groupes,

$$\boxed{H\trianglelefteq G\ \wedge\ K\trianglelefteq G \quad\implies\quad H\cap K\trianglelefteq G}$$

En effet, $\forall g\in G,\ \forall h\in H\cap K,\ ghg^{-1}\in H$ (car $H\trianglelefteq G$) et $ghg^{-1}\in K$ (car $H\trianglelefteq G$) donc $ghg^{-1}\in H\cap K$.

Si $\varphi\in\mathrm{Hom}((G,\cdot),(G',\cdot'))$ est un **morphisme** de groupes, alors $\boxed{H\trianglelefteq G\Rightarrow f(H)\trianglelefteq f(G)}$ et $H'\trianglelefteq G'\Rightarrow f^{\leftarrow}(H')\trianglelefteq G$.
De plus, son noyau est toujours normal : $\boxed{\mathrm{Ker}\,\varphi\ \trianglelefteq\ G}$

Tout sous-groupe d'un groupe abélien est normal : $\boxed{G \text{ abélien et } H\leq G \quad\implies\quad H\trianglelefteq G}$

car alors $\forall g\in G,\ \forall h\in H,\ ghg^{-1}=gg^{-1}h=e\,h=h\in H$ puisque G est abélien.

Quotient par un sous-groupe normal

To do

Groupe simple

Le sous-groupe trivial $\{e\}$ et G sont toujours distingués dans G. Un **groupe simple** est un groupe n'ayant pas de sous-groupes stricts normaux non triviaux :

$$G \text{ simple} \overset{\text{def}}{\Leftrightarrow} \big(H\triangleleft G \Rightarrow H=\{e\}\big)$$

Groupes abéliens simples : Si G est abélien simple, il est monogène, et même **cyclique** (donc *fini* !) d'ordre premier :

$$\boxed{G \text{ abélien simple} \quad\implies\quad \exists p\in\mathbb{P}\ :\ G\cong \mathbb{Z}/_{p\mathbb{Z}}}$$

Démonstration Si $G=\{e\}$, c'est gagné. Sinon, montrons que G ne **possède pas de sous-groupe strict non trivial**.

Soit $H\leq G$ un sous groupe non trivial et $g\in H\backslash\{e\}$. Alors le sous-groupe $\langle g\rangle$ engendré par g est normal car G est abélien. Or G est simple, donc par définiton $\langle g\rangle=G$ ou $\{e\}$, donc $\langle g\rangle=G=H$ puisque $g\neq e$. On voit aussi que G est **monogène**.

De plus, G est **fini**. En effet, si ce n'était pas le cas, alors $\mathrm{ord}(g)=\infty$ donc $\langle g^2\rangle$ ($\cong 2\mathbb{Z}$) serait un sous-groupe strict non trivial de $G=\langle h\rangle$ ($\cong\mathbb{Z}$), ce qui est impossible. Ainsi, G est **cyclique**, c'est à dire que $G\cong \mathbb{Z}/_{|G|\mathbb{Z}}$ avec $|G|=\mathrm{ord}(g)$.

Enfin, soit $d\in\mathrm{Div}(|G|)$ un diviseur de l'ordre. Alors G possède un sous-groupe G_d d'ordre d (par exemple $G/_{\langle g^{|G|/d}\rangle}$ par le théorème de Lagrange). Comme G est simple, on a vu que $G_d\in\{G,\{e\}\}$, donc $d\in\{|G|,1\}$. Donc $|G|\in\mathbb{P}$. $\square$

Normalisateur

Normalisateur de H dans G : C'est le sous-groupe qui stabilise (globalement) H par l'opération de conjugaison :

$$\boxed{\mathrm{N}_G(H) := \{g\in G : gHg^{-1}=H\}} = \{g\in G : gH=Hg\}$$

- Dit autrement, c'est le sous-groupe stabilisateur du point $H\in X$:

$$\mathrm{Stab}_\star(H) = \mathrm{N}_G(H)$$

par l'opération de conjugaison de G sur l'ensemble $X=\{gHg^{-1} : g\in G\}$ des conjugués de H dans G, définie par $\forall g\in G$, $\forall xHx^{-1}\in X,\ g\star(xHx^{-1}):=gxHx^{-1}g^{-1}$.

- C'est un **sous-groupe** de G qui contient H :
  - H est un groupe donc $\forall h\in H,\ hHh^{-1}\subset H$ et $\forall h'\in H,\ h'=h\overbrace{h^{-1}h'h}^{\in H}h^{-1}\in hHh^{-1}$ donc $hHh^{-1}=H$. Donc $H\subset\mathrm{N}_G(H)$, qui est donc non vide (ou encore $\ni e$).
  - $\forall g_1,g_2\in\mathrm{N}_G(H)$, $(g_1g_2)H(g_1g_2)^{-1}=g_1\underbrace{g_2Hg_2^{-1}}_{=H}g_1^{-1}=g_1Hg_1^{-1}=H$ donc $g_1\,g_2\in\mathrm{N}_G(H)$.

- ⚠ En général, le normalisateur $\mathrm{N}_G(H)$ n'est *pas* distingué dans G. Par contre, ***H* y est distingué** par définition.

Ainsi, $$\boxed{H \trianglelefteq \mathrm{N}_G(H) \leq G}$$

On dit que $\mathrm{N}_G(H)$ **normalise** H. C'est même le plus **grand sous-groupe** de G qui normalise H. En particulier :

- De plus, par définition, puisque $H\trianglelefteq G \Leftrightarrow \forall g\in G,\ gH=Hg \Leftrightarrow \forall g\in G,\ gHg^{-1}=H$,

$$\boxed{H\trianglelefteq G \Leftrightarrow \mathrm{N}_G(H)=G}$$

Centralisateur, Centre

Centralisateur de H dans G Ensemble des éléments de G qui commutent avec tous les éléments de H :

$$\boxed{\mathrm{C}_G(H) := \{g\in G : \forall h\in H,\ \underbrace{gh=hg}_{\substack{\Leftrightarrow\, ghg^{-1}=h \\ \not\Leftrightarrow\, ghg^{-1}\in H}}\}}$$

$$\longrightarrow \quad \mathrm{C}_G(H)\neq\mathrm{N}_G(H) \quad ⚠$$

- Un élément du centre respecte une condition bien plus forte que juste normaliser H : il stabilise localement H par l'opération de conjugaison, c'est à dire que $\forall h\in H,\ \mathrm{C}_G(H)\subset\mathrm{Stab}_{\mathrm{conj}}(h)$. Réécrit différemment,

$$\mathrm{C}_G(H)=\bigcap_{h\in H}\mathrm{Stab}_{\mathrm{conj}}(h)$$

- C'est un sous-groupe **distingué dans le normalisateur** (⚠ mais pas dans G en général) :
  - $e\in\mathrm{C}_G(H)$ donc $\mathrm{C}_G(H)$ est non vide. De plus $\forall g_1,g_2\in\mathrm{C}_G(H)$, $\forall h\in H$, $(g_1g_2^{-1})h=g_1hg_2^{-1}=h(g_1g_2^{-1})$ car g_1 et g_2 (donc g_2^{-1}) commutent avec h. Donc $g_1\,g_2^{-1}\in\mathrm{C}_G(H)$. Donc $\mathrm{C}_G(H)$ est un sous-groupe de G.
  - Il est immédiat que $\mathrm{C}_G(H)\subset\mathrm{N}_G(H)$. De plus, $\forall g\in\mathrm{N}_G(H)$, $\forall x\in\mathrm{C}_G(H)$, $gxg^{-1}\in\mathrm{N}_G(H)$ car

$$gxg^{-1}H(gxg^{-1})^{-1}=gx\overbrace{g^{-1}Hg}^{=H}x^{-1}g^{-1}=g\overbrace{xHx^{-1}}^{=H}g^{-1}=\overbrace{gHg^{-1}}^{=H}=H \quad \text{car} \quad g,g^{-1}\in\mathrm{N}_G(H)\supset\mathrm{C}_G(H)\ni x$$

Ainsi, $$\boxed{\mathrm{C}_G(H) \trianglelefteq \mathrm{N}_G(H) \leq G}$$

- En général, $H\not\subset\mathrm{C}_G(H)$! Par contre, on a par définition d'un groupe abélien que

$$\boxed{H \text{ abélien} \iff H\leq\mathrm{C}_G(H)}$$

Centre de G

Ce sont les éléments de G qui commutent avec tous les autres éléments; c'est le centralisateur de G :

$$\boxed{\mathrm{Z}(G) \;:=\; \mathrm{C}_G(G) \;=\; \big\{g\in G : \forall x\in G,\; gx=xg\big\}}$$

- C'est aussi l'ensemble des points fixes de l'action de G sur $X=G$ lui même par conjugaison (mais ⚠, ça ne se généralise pas à $\mathrm{C}_G(H)$ pour l'action de G sur un sous-groupe H, ce n'est valable qu'ici) :

$$\boxed{\mathrm{Z}(G) \;=\; \mathrm{Fix}_{\mathrm{conj}\,:\,G\times G\to G} \;=\; \big\{x\in G : |\mathrm{Orb}_{\mathrm{conj}}(x)|=1\big\}}$$

  En effet, par le théorème orbite-stabilisateur, $\forall x\in G,\ |G|=|\mathrm{Stab}_{\mathrm{conj}}(x)|\times|\mathrm{Orb}_{\mathrm{conj}}(x)|$ donc

$$\begin{aligned} x\in\mathrm{Z}(G) \;\Leftrightarrow\; \forall g\in G,\; g\,\mathrm{conj}\,x=gxg^{-1}=x \;&\Leftrightarrow\; \mathrm{Stab}_{\mathrm{conj}}(x)=G \;\Leftrightarrow\; |\mathrm{Stab}_{\mathrm{conj}}(x)|=|G| \;\Leftrightarrow\; |\mathrm{Orb}_{\mathrm{conj}}(x)|=1 \\ &\Leftrightarrow\; x\in\mathrm{Fix}_{\mathrm{conj}} \end{aligned}$$

- Le centre est un sous-groupe **abélien** par définition : $\forall g,g'\in\mathrm{Z}(G),\ g\,g'=g'\,g$ car $g\in\mathrm{Z}(G)$.
- On a vu que $\boxed{G \text{ abélien} \;\Leftrightarrow\; G=\mathrm{Z}(G)}$
- C'est un sous-groupe **distingué dans G** : $\boxed{\mathrm{Z}(G)\;\trianglelefteq\;G}$

  En effet, $\forall g\in G,\ \forall x\in\mathrm{Z}(G),\ gxg^{-1}\in\mathrm{Z}(G)$ car $\forall y\in G,\ (gxg^{-1})\,y=gg^{-1}xy=xy=yx=yxgg^{-1}=y\,(gxg^{-1})$ car x commute avec tout le monde.

Tout p-groupe fini non trivial possède un centre non trivial

Soit $p\in\mathbb{P}$ et G un **p-groupe fini non trivial**. Alors $\exists n\in\mathbb{N}^* : |G|=p^n$. L'équation aux classes de l'action de conjugaison de G sur lui-même, avec Ω_{conj} l'ensemble des orbites que l'on sépare en orbites de cardinal 1 (points fixes) et de cardinal >1, donne :

$$|G| \;=\sum_{O\in\Omega_{\mathrm{conj}}}|O| \;=\; |\mathrm{Z}(G)|+\sum_{\substack{O\in\Omega_{\mathrm{conj}}\\|O|\neq1}}|O| \qquad \text{car} \qquad \mathrm{Z}(G)\;=\;\big\{x\in G : |\mathrm{Orb}_{\mathrm{conj}}(x)|=1\big\}$$

De plus, $\forall O\in\Omega_{\mathrm{conj}} : |O|\neq1$, comme $|O|\,\mathrm{div}\,|G|=p^n$ (OST), $\exists m\in\mathbb{N}^* : |O|=p^m$, donc $p\,\mathrm{div}\,|O|$. Enfin, $p\,\mathrm{div}\,|G|$, donc

$$p\ \mathrm{div}\ \ |G|-\sum_{\substack{O\in\Omega_{\mathrm{conj}}\\|O|\neq1}}|O| \;=\; |\mathrm{Z}(G)| \quad \text{donc} \quad \boxed{p\,\mathrm{div}\,|\mathrm{Z}(G)| \quad \text{et} \quad \mathrm{Z}(G)\neq\{e\}}$$ □

Note : Et alors $G/\mathrm{Z}(G)$, donc $\mathrm{Inn}(G)$, est encore un p-groupe, plus petit que G.

Si $G/\mathrm{Z}(G)$ est cyclique, G est abélien

Soit $(G,\cdot)$ un groupe **fini** tel que $G/\mathrm{Z}(G)$ est cyclique. Soit donc $g_0\in G$ tel que $\big\langle g_0 \bmod \mathrm{Z}(G)\big\rangle = G/\mathrm{Z}(G)$.
Ainsi, $\forall g\in G,\ \exists k\in\mathbb{N} : g \bmod \mathrm{Z}(G)=(g_0 \bmod \mathrm{Z}(G))^k=g_0^k \bmod \mathrm{Z}(G)$, c'est à dire que $g_0^{-k}\,g\in\mathrm{Z}(G)$, c'est à dire que

$$\forall x\in G,\quad g_0^{-k}\,g\,x=x\,g_0^{-k}\,g \quad (1) \qquad \text{et en particulier pour } x=g_0^k, \qquad g=g_0^{-k}\,g\,g_0^k \quad (2)$$

Montrons alors que g commute avec tout élément de G : $\forall x\in G,\ g\,x\overset{(1)}{=}x\,g_0^{-k}\,g\,g_0^k\overset{(2)}{=}x\,g$ donc

$$\boxed{G/\mathrm{Z}(G) \text{ cyclique} \;\Rightarrow\; G \text{ abélien}}$$ □

Théorème N/C

Soit $H\leq G$ un sous-groupe. Puisque $\mathrm{C}_G(H)\trianglelefteq\mathrm{N}_G(H)$, on peut passer au quotient, et alors le groupe quotient est isomorphe à un sous-groupe de $\mathrm{Aut}(H)$:

$$\boxed{\Big(\mathrm{N}(H)/\mathrm{C}(H),\cdot\Big) \;\cong\; \big(\mathrm{Im}(\Phi_H),\circ\big) \;\hookrightarrow\; \big(\mathrm{Aut}(H),\circ\big) \quad \text{avec} \quad \begin{array}{rcl}\Phi_H : \mathrm{N}_G(H) & \longrightarrow & \mathrm{Aut}(H)\\ g & \longmapsto & (h\mapsto ghg^{-1})\end{array}}$$

Démonstration D'abord, $\forall g\in\mathrm{N}_G(H),\ \Phi_H(g)$ est un endomorphisme de H car $\forall x\in H,\ ghg^{-1}\in H$ car $g\in\mathrm{N}_G(H)$, et il est inversible, d'inverse $\Phi_H(g)^{-1}=\Phi_H(g^{-1})$, c'est donc bien un automorphisme (dit **intérieur** à H).

De plus, on vérifie que $\Phi_H \in \mathrm{Hom}\big((\mathrm{N}_G(H),\cdot),(\mathrm{Aut}(H),\circ)\big)$ est bien un **morphisme** : $\forall g,g'\in \mathrm{N}_G(H)$,

$$\Phi(g\,g') \;=\; x\mapsto gg'h(gg')^{-1} \;=\; x\mapsto g(g'hg'^{-1})g^{-1} \;=\; x\mapsto g\,\Phi_H(g')(h)\,g^{-1} \;=\; \Phi_H(g)\circ\Phi_H(g')$$

Calculons son **noyau** : $\forall g\in \mathrm{N}_G(H)$,
$$\begin{aligned} g\in \mathrm{Ker}(\Phi_H) &\iff \Phi_H(g)=h\mapsto ghg^{-1}=e_{(\mathrm{Aut}(H),\circ)}=h\mapsto h\\ &\iff \forall h\in H,\ ghg^{-1}=h\\ &\iff g\in \mathrm{C}(H)=\{g\in G:\forall h\in H,\ gh=hg\}\end{aligned}$$

Donc $\boxed{\mathrm{Ker}(\Phi_H)=\mathrm{C}_G(H)}$. Ainsi, par **factorisation canonique** de Φ par son noyau $\mathrm{C}_G(H)$ distingué dans $\mathrm{N}(H)$, on a :

$$\begin{array}{ccc} \mathrm{N}(H) & \longrightarrow & \mathrm{Aut}(H)\\ \downarrow & & \uparrow\\ {\mathrm{N}(H)}/{\mathrm{C}(H)} & \longleftrightarrow & \mathrm{Im}(\Phi_H)\end{array}$$

□

Conséquence : en prenant $H=G$, et puisque $\mathrm{N}_G(G)=G$ car G est un groupe, et que $\mathrm{C}_G(G)=Z(G)$, on obtient un isomorphisme entre ${G}/{\mathrm{Z}(G)}$ et $\mathrm{Im}(\Phi_G)$, que l'on nomme groupe des **automorphismes intérieurs** de G, noté $\mathrm{Inn}(G)$:

$$\boxed{{G}/{\mathrm{Z}(G)} \;\cong\; \mathrm{Inn}(G) \;:=\; \big\{x\mapsto gxg^{-1} : g\in G\big\} \;\subset\; \mathrm{Aut}(G)}$$

Le nombre d'automorphismes intérieurs est une mesure de la non-commutativité de la loi de $(G,\cdot)$.

Cœur d'un sous-groupe

Le **cœur normal** du sous-groupe $H\leq G$ est l'intersection des conjugués de H par G :

$$\boxed{\mathrm{Core}_G(H) \;:=\; \bigcap_{g\in G} gHg^{-1}}$$

- Le cœur normal est un sous-groupe (car $\cap$ de sous-groupes) **distingué** dans G : $\forall g\in G,\ \forall x\in \mathrm{Core}(H)$,
  Montrons que $gxg^{-1}\in \bigcap_{y\in G} yHy^{-1}$. Soit $y\in G$. On a que $x\in\bigcap_{z\in G} zHz^{-1}$ donc $\forall z\in G,\ x\in zHz^{-1}$
  Donc en particulier pour $z=g^{-1}y$, on a $x\in g^{-1}yH(g^{-1}y)^{-1}$, d'où $gxg^{-1}\in yHy^{-1}$. Donc $gxg^{-1}\in \mathrm{Core}(H)$.

$$\boxed{\mathrm{Core}_G(H) \;\trianglelefteq\; G}$$

- C'est un sous-groupe de H : $\forall x\in \mathrm{Core}_G(H)$, $\forall g\in G,\ x\in gHg^{-1}$, et en particulier pour $g=e$, $x\in H$. Donc

$$\boxed{\mathrm{Core}_G(H) \;\leq\; H}$$

- C'est même le plus **grand sous-groupe normal de G contenu dans H** : $\boxed{\forall N\trianglelefteq G : N\subset H,\ N\subset \mathrm{Core}_G(H)}$
  En effet, soit $x\in N$. Puisque $N\trianglelefteq G$, on a que $\forall g\in G,\ gxg^{-1}\in N\subset H$, donc $x\in g^{-1}Hg$.
  Donc $x\in \bigcap_{g\in G} gHg^{-1}=\mathrm{Core}_G(H)$ avec $g\leftrightarrow g^{-1}$. Donc $N\subset \mathrm{Core}_G(H)$.
- C'est le **noyau** du morphisme associé à l'action de G sur ${G}/{H}$ définie par $\forall g\in G,\ \forall xH\in {G}/{H},\ g\star(xH):=gxH$:

$$\boxed{\mathrm{Core}_G(H) = \mathrm{Ker}(\Phi) \quad\text{avec}\quad \begin{array}{rcl}\Phi : G & \longrightarrow & \mathfrak{S}({G}/{H})\\ g & \longmapsto & (xH\mapsto gxH)\end{array}}$$

  (⚠ H n'étant pas forcément normal, on ne considère aucune structure de groupe sur ${G}/{H}$)
  C'est un morphisme de $(G,\cdot)$ dans $(\mathfrak{S}({G}/{H}),\circ)$:

$$\forall g,g'\in G,\quad \Phi(g\,g') \;=\; xH\mapsto gg'xH \;=\; (xH\mapsto gxH)\circ(xH\mapsto g'xH) \;=\; \Phi(g)\circ\Phi(g')$$

  Calculons son noyau : $[\ (*) : y\in H \;\Rightarrow\; yH=H \;\Rightarrow\; \forall h\in H,\ yh\in H \;\Rightarrow\; y\in H$ (car sinon $eh\notin H$) donc $y\in H \Leftrightarrow yH=H\ ]$

$$\begin{aligned}\mathrm{Ker}(\Phi) &= \{g\in G : \Phi(g)=e_\circ\} = \{g\in G : xH\mapsto gxH=xH\mapsto xH\}\\ &= \{g\in G : \forall x\in G,\ \underbrace{gxH=xH}_{(*)\ \Leftrightarrow\ x^{-1}gx\in H\ \Leftrightarrow\ g\in xHx^{-1}}\}\\ &= \bigcap_{x\in G}\{g\in G : g\in xHx^{-1}\} = \bigcap_{g\in G} xHx^{-1} = \mathrm{Core}_G(H)\end{aligned}$$

- Ainsi, par **factorisation canonique** de Φ par son noyau, $G/\mathrm{Core}(H)$ est isomorphe à un sous-groupe de $\mathfrak{S}(G/H)$:

$$\left(G/\mathrm{Core}(H),\cdot\right) \cong \left(\mathrm{Im}(\Phi),\circ\right) \longrightarrow \left(\mathfrak{S}(G/H),\circ\right)$$

Application : **Groupe simple admettant un sous-groupe strict d'indice fini**

Supposons que G est **simple**. Alors comme $\mathrm{Ker}(\Phi)=\mathrm{Core}_G(H)\trianglelefteq G$, alors on a deux cas :

- $\mathrm{Core}_G(H)=\{e\}$, et alors (Φ est injective, quoi) $G\cong G/\{e\}=G/\mathrm{Core}_G(H)\cong\mathrm{Im}(\Phi)$, qui est un sous groupe de $\mathfrak{S}(G/H)$. Donc G est isomorphe à un sous-groupe de $\mathfrak{S}(G/H)$.
- $\mathrm{Core}_G(H)=G$, et alors puisque $\mathrm{Core}_G(H)\leq H$, on a que $H=G$.

En particulier, si G admet un sous-groupe $H<G$ **strict d'indice fini** $n=\mathrm{ind}_G(H)=\left|G/H\right|$, alors G est **isomorphe** à un sous-groupe de $\mathfrak{S}_n\cong\mathfrak{S}(G/H)$, et en particulier G est **fini**, et H aussi. Et par le théorème de Lagrange, $\mathrm{Im}(\Phi)$ étant un sous-groupe de $\mathfrak{S}_n$, $|G|=|\mathrm{Im}(\Phi)|\,\mathrm{div}\,|\mathfrak{S}_n|=n!$, donc l'**ordre de G divise $\mathrm{ind}_G(H)!$**, ainsi que $\mathrm{ind}_G(\mathrm{Core}_G(H))$.

Et par contraposée, si G est **infini** et admet un **sous-groupe strict d'indice fini**, alors G n'est **pas simple** : il admet alors un sous-groupe strict normal non-trivial.

Tout sous-groupe d'indice $\min(\mathrm{Div}\mathbb{P}(|G|))$ est normal

Soit $(G,\cdot)$ un groupe fini et $H\leq G$ un sous groupe (si il en existe) d'indice $\mathrm{ind}_G(H)=p:=\min(\mathrm{Div}\mathbb{P}(|G|))$, le plus petit diviseur premier de l'ordre de G. Montrons que H est distingué dans G, en montrant que le cœur de H vaut tout H.
$G/\mathrm{Core}(H)$ est isomorphe à un sous-groupe de $\mathfrak{S}(G/H)$, donc par la théorème de Lagrange,

$$\mathrm{ind}_G(\mathrm{Core}_G(H)) = \left|G/\mathrm{Core}(H)\right| \,\mathrm{div}\, \left|\mathfrak{S}(G/H)\right| = |\mathfrak{S}_p| = p! = \prod_{n=1}^{p} n$$

De plus, encore par le théorème de Lagrange, $\left|G/\mathrm{Core}(H)\right|=|G|/|\mathrm{Core}(H)|$ et comme $p:=\min(\mathrm{Div}\mathbb{P}(|G|))$, $\forall n<p$, $|G|$, donc $|G|/|\mathrm{Core}(H)|$, donc $\left|G/\mathrm{Core}(H)\right|$ n'admet pas n comme facteur. Donc nécessairement

$$\mathrm{ind}_G(\mathrm{Core}_G(H))\in\{1,p\}$$

Si $H=G$, c'est gagné. Sinon $\mathrm{Core}(H)\leq H<G$, donc $\left|G/\mathrm{Core}(H)\right|\neq 1$ donc $\mathrm{ind}_G(\mathrm{Core}_G(H))=p=\mathrm{ind}_G(H)$ donc, comme $\mathrm{Core}(H)$ est un sous-groupe de H toujours distingué dans G, on a $H=\mathrm{Core}_G(H)\trianglelefteq G$. Ainsi,

$$\boxed{\mathrm{ind}_G(H)=\min(\mathrm{Div}\mathbb{P}(|G|)) \implies H\trianglelefteq G}$$ □

Démonstration par action de H sur G/H

On considère le morphisme associé à l'action de $H\leq G$ sur G/H définie par $\forall h\in H,\ \forall xH\in G/H,\ h\star(xH):=hxH$:

$$\begin{array}{rccc} \star: & H\times G/H & \longrightarrow & G/H \\ & (h,xH) & \longmapsto & hxH \end{array}$$

Montrons que $\star$ agit trivialement, c'est à dire que tous les points sont fixes. Notons que $e \bmod H=eH=H$ en est un.

Supposons qu'il existe un point non fixe $g \bmod H=gH\in G/H$. Alors $|\mathrm{Orb}_\star(gH)|\neq 1$. Or $|\mathrm{Orb}_\star(gH)|\,\mathrm{div}\,|H|\,\mathrm{div}\,|G|$ par le théorème orbite-stabilisateur et par le théorème de Lagrange, donc $|\mathrm{Orb}_\star(gH)|\geqslant p$.

C'est strictement impossible car la formule des classe nous donne, en considérant les orbites de gH et eH :

$$p = \left|G/H\right| = \sum_{O\in\Omega_\star}|O| \geqslant |\mathrm{Orb}_\star(gH)|+|\mathrm{Orb}_\star(eH)| = p+1 > p$$

Ainsi, toutes les orbites sont réduites à un point, donc $\forall h\in H,\ \forall x\in G,\ xH=h\star(xH)=hxH$, donc $x^{-1}hxH=H$ donc en particulier pour $e\in H$ et $x=g^{-1}$, $\forall g\in G,\ ghg^{-1}\in H$. Donc $H\trianglelefteq G$. □

Tout sous-groupe d'indice 2 est normal (cas particulier que l'on peut montrer à la main)

Soit $(G,\cdot)$ un groupe, non nécessairement fini, et $H\leq G$ un sous groupe d'indice $\mathrm{ind}_G(H)=2$. Ainsi, G/H ne comporte que 2 classes, dont H. Donc $\forall g\in G$,
- soit $g\in H$ et alors $gH=Hg=H$ car H est un groupe, donc $gHg^{-1}=H$; ou
- soit $g\notin H$ et alors $G/H=\{H,gH\}=\{H,Hg\}$, donc $gH=Hg$ donc on a encore $gHg^{-1}=H$

donc $\boxed{\mathrm{ind}_G(H)=2 \implies H\trianglelefteq G}$ □

Divers

Un groupe fini n'est pas l'union des conjugués d'un sous-groupe propre

Soit $(G,\cdot)$ un groupe **fini** et $H<G$ un sous-groupe propre ($\neq G, \neq\{e\}$). Alors G n'est ***pas*** l'union des conjugués de H.

En effet, $\forall g\in G$, au sein d'une même classe modulo H, $\forall gh=gH,\ ghH(gh)^{-1}=ghHh^{-1}g^{-1}=ghh^{-1}Hg^{-1}=gHg^{-1}$ donc en notant $\bar{g}=g \bmod H$, $\forall x\in\bar{g},\ xHx^{-1}=H$ donc on peut réduire l'union à un système de représentants :

$$\bigcup_{g\in G} gHg^{-1}=\bigcup_{\bar{g}\in G/H} gHg^{-1}$$

$$\begin{aligned}
\left|\bigcup_{g\in G} gHg^{-1}\Big\backslash\{e\}\right|=\left|\bigcup_{g\in G} gHg^{-1}\backslash\{e\}\right| &= \left|\bigcup_{\bar{g}\in G/H} gHg^{-1}\backslash\{e\}\right| \\
&\leqslant \sum_{\bar{g}\in G/H} \underbrace{\left|gHg^{-1}\backslash\{e\}\right|}_{=|H\backslash\{e\}|} \\
(gHg^{-1}\cong H) \qquad &= |H\backslash\{e\}|\times\sum_{\bar{g}\in G/H} 1 \\
(\text{théorème de Lagrange : } |G|=|G/H|\times|H|) \qquad &= (|H|-1)\times\left|G/H\right| = (|H|-1)\times\frac{|G|}{|H|} \\
(|G|\geqslant|H| \text{ car } H \text{ est un groupe strict}) \qquad &= |G|-\frac{|G|}{|H|} \leqslant |G|-1 = |G\backslash\{e\}|
\end{aligned}$$

$$\text{donc} \quad \left|\bigcup_{g\in G} gHg^{-1}\right| \leqslant |G| \quad \text{donc} \quad \boxed{\bigcup_{g\in G} gHg^{-1} \subsetneq G} \qquad \square$$