(Autour du théorème de
Structure des groupes abéliens finis)

Notations :

G groupe (neutre $e, \varepsilon, 1, 0$) ; G_1, G_2 gpes ; H s/s-gpe de G
$n \in \mathbb{N}^*$ $\qquad$ $\mathrm{Hom}_{gpe}(G_1,G_2)$, $\mathrm{Isom}_{gpe}(G_1,G_2)$
pr $g \in G$ $o(g)$ = ordre de g

Prérequis

- déf de groupe, sous-groupe, distingué ;
  $\cap$ s/s gpes ; s/s-gpe engendré, description int. et ext.
  (iso) morphisme de groupe
  images directe et réciproque d'un s/s gpe par un morphisme de groupes
  image réc. d'un sous-gpe distingué " " "
  image directe " " " " " surjectif
  noyau, image d'un morphisme de groupe

- G fini : Lagrange ; réciproques partielles, contre-exemples
  ordre d'un élément, conservation par inverse, conjugaison
  lemme de Cauchy ($\exists$ élt d'ordre p)

- Groupes cycliques :
  déf, isom ssi même ordre
  s/s-gpes, quotients
  générateurs, ordre d'un élément
  ex (racines de l'unité)

- Thm d'iso

...

I Exposant d'un groupe

Déf : • G est dit d'exposant fini s'il vérifie : $\exists\, m \in \mathbb{N}^*,\ \forall g \in G\ \ g^m = e$
• Pour G d'exposant fini, on note
$\exp(G) = \min\{m \in \mathbb{N}^* / \forall g \in G,\ g^m = e\}$ (existe (partie $\neq \emptyset$ de $\mathbb{N}^*$), $\in \mathbb{N}^*$; est un exposant)
et on l'appelle "exposant de G"

Rmq : • Si G d'exposant fini, tt g ds G est d'ordre fini et $o(g) \mid \exp G$ (en particulier, $\{o(g), g \in G\}$ borné)
$g^m = e \Leftrightarrow o(g) \mid m$ ($\Rightarrow o(g) \leq m$) divisibilité + forte que ordre
Exo : trouver G tq $\forall g \in G\ o(g) < \infty$ et G pas d'exposant fini $\mathbb{Q}/\mathbb{Z}$
• Par Lagrange : G fini $\Rightarrow$ G d'exposant fini et alors $\exp G \leq |G|$ (en fait $\mid$)
mots-clés : écrit, développement, repose question.
Exo : trouver G infini d'exposant fini $\mathbb{F}_2[X]$, $\mathbb{F}_2^{\mathbb{N}}$, $\{-1; 1\}^{\mathbb{N}}$

Prop : On supp G d'exposant fini. On a $\exp G = \text{ppcm}\{o(x), x \in G\}$

D/ Soit $m \in \mathbb{N}^*$. On a
$\forall g \in G, g^m = e \Leftrightarrow \forall g \in G,\ o(g) \mid m \Leftrightarrow \text{ppcm}\{o(g), g \in G\} \mid m$
(ts les $o(g)$ finis ; bien déf car borné)
Dc $\exp G = \text{ppcm}\{o(g), g \in G\}$ ■

Corollaire : Si G fini, $\exp G \mid |G|$ (Lagrange)

Prop : On supp. G abélien et d'exposant fini. Alors : $\exists\, g \in G,\ o(g) = \exp G$.

D/ (i) $\exp G = 1 \Leftrightarrow G = \{e\}$ dc o.p.s. $\exp G \geq 2$.
On écrit $m := \exp G = p_1^{m_1} \cdots p_r^{m_r}$ avec $r \in \mathbb{N}^*$, $p_1, \dots, p_r$ premiers 2 à 2 $\neq$, $(m_1, \dots, m_r) \in (\mathbb{N}^*)^r$

(ii) Soit $i \in [\![1, r]\!]$: $\exists\, g_i \in G$ tq $p_i^{m_i} \mid o(g_i)$
En effet, on a $m = \text{ppcm}\{o(g), g \in G\} = \prod_{p \in \mathcal{P}} p^{\max\{v_p(o(g)),\ g \in G\}}$ (m_i pr $p = p_i$)

Ou encore : $\forall g \in G\ o(g) \mid m$ dc $v_{p_i}(o(g)) \leq v_{p_i}(m) = m_i$; si $<$ $\forall g \in G$, $v_{p_i}(\text{ppcm}) \leq m_i - 1$

(iii) Soit $i \in [\![1, r]\!]$ g_i c ci-dessus, $o(g_i) = p_i^{m_i} q_i$, $\gamma_i = g_i^{q_i}$ est d'ordre $p_i^{m_i}$ (Gr cyclique)

(iv) On pose $\gamma = \gamma_1 \cdots \gamma_r$
Les $\gamma_1, \dots, \gamma_r$ commutent 2 à 2 car G abélien
Ordre 2 à 2 premiers entre eux
dc Exo $o(\gamma) = p_1^{m_1} \cdots p_r^{m_r} = m$

$\gamma_1\gamma_2$ d'ordre $p_1^{m_1} p_2^{m_2}$, commute à γ_3, $\wedge = 1$
$\gamma_1\gamma_2\gamma_3$ — $p_1^{m_1} p_2^{m_2} p_3^{m_3}$
(récurrence propre) ■

Exo : ctre-ex si G non abélien.

II Caractères linéaires - groupe dual

non lin ∃ (cf Repr)

← notion cruciale et transverse, // ev

Prop-déf: On note $\hat{G} = \mathrm{Hom}_{gpe}(G, \mathbb{C}^\times)$, appelé dual de G. (str mult) (groupe)

L'application $\hat{G} \times \hat{G} \longrightarrow \hat{G}$ munit $\hat{G}$ d'une structure de gpe abélien

$(\chi_1, \chi_2) \longmapsto \begin{array}{l} G \to \mathbb{C}^\times \\ g \mapsto \chi_1(g)\chi_2(g) \end{array}$

Mult° "pt par pt" "à l'arrivée"

Rmq: neutre, inverse

Interlude groupe dérivé :

Déf: $D(G) = \langle ghg^{-1}h^{-1}, (g,h) \in G^2 \rangle$ est appelé sous-groupe dérivé de G (important)

Rmq: G abélien $\Leftrightarrow D(G) = \{e\}$ la taille de $D(G)$ mesure la non abélianité de G

Prop: (i) Si H distingué ds G et G/H abélien, alors $D(G) \subseteq H$.

(ii) Si $D(G) \subseteq H$, alors H distingué ds G et G/H abélien.

(iii) $D(G) = \bigcap_{\substack{H \triangleleft G \\ G/H \text{ ab}}} H$

Déf: $G/D(G)$ est noté G^{ab} et appelé abélianisé de G. "plus gros quotient abélien de G"

Fin interlude

Prop: On note π^{ab} la projection canonique de G ds G^{ab}. L'application $\widehat{G^{ab}} \longrightarrow \hat{G}$, $\chi \longmapsto \chi \circ \pi^{ab}$ est un isomorphisme (de groupes).

DI (Étapes):

bien défini $G \xrightarrow{\pi^{ab}} G^{ab} \xrightarrow{\chi} \mathbb{C}^\times$ — $\hat{G}$ ne voit que l'abélianisé de G (car $\mathbb{C}^\times$ abélien) ↳ On peut penser G abélien ds la suite

morphisme de groupes car loi à l'arrivée et on compose au départ

injectif par surjectivité de π^{ab}

surjectif
$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi^{ab}"'] & \mathbb{C}^\times \\ G^{ab} \arrow[ur, dashed, "\chi"'] & \end{tikzcd}$$
$H := \mathrm{Ker}\,\varphi \triangleleft G$, $G/H \hookrightarrow \mathbb{C}^\times$ abélien, dc $D(G) \subseteq H$ dc factorisation (donc aussi unicité) $\blacksquare$

Interlude factorisation

Soient φ ds $\mathrm{Hom}_{gpe}(G_1, G_2)$, H_1 s/s gpe de G_1, π projection de G_1 sur G_1/H_1.

$$\begin{tikzcd} G_1 \arrow[r, "\varphi"] \arrow[d, "\pi"'] & G_2 \\ G_1/H_1 \arrow[ur, dashed, "\psi"'] & \end{tikzcd}$$

(i) $\exists\, \psi \in \mathrm{Hom}_{gpe}(G_1/H_1, G_2)$ tq $\varphi = \psi \circ \pi \Leftrightarrow H_1 \subseteq \mathrm{Ker}\,\varphi$

(ii) Si la condition (i) est réalisée :

- ψ est unique
- $\mathrm{Im}\,\psi = \mathrm{Im}\,\varphi$
- $\mathrm{Ker}\,\psi = \mathrm{Ker}\,\varphi / H_1$
- ψ inj $\Leftrightarrow H_1 = \mathrm{Ker}\, H_1$

corollaire

Fin interlude

Ex: $\hat{\mathbb{Z}} \longrightarrow \mathbb{C}^\times$, $\varphi \longmapsto \varphi(1)$ est un isom de gpes

morph de gpes (cf déf str gpe sur $\mathbb{C}^\times$)

inj car $\mathbb{Z} = \langle 1 \rangle$

surj : construire explicitement

Rmq : Im d'un car lin est tjs cyclique

Ex : $\widehat{\mathbb{Z}/n\mathbb{Z}} \longrightarrow \mu_n(\mathbb{C})$ est un isom

$\chi \longmapsto \chi(\bar 1)$

$\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^\times \longleftarrow \zeta$

$\bar k \mapsto \zeta^k$

bien défini $\chi(n.\bar 1) = \chi(\bar 0) = 1 = \chi(\bar 1)^n$
morph gpe
inj car $\langle \bar 1 \rangle = \mathbb{Z}/n\mathbb{Z}$
surj par factorisation de $\mathbb{Z} \to \mathbb{C}^\times$
$k \mapsto \zeta^k$

Important

Csq: $\boxed{\widehat{\mathbb{Z}/n\mathbb{Z}} \simeq \mathbb{Z}/n\mathbb{Z}}$ Non canonique (doublement)

// ev

Propriétés : (i) Pour tout φ est ds $\mathrm{Isom}_{gpe}(G_1, G_2)$, $\begin{matrix}\widehat{G_2} \to \widehat{G_1} \\ \chi \mapsto \chi\circ\varphi\end{matrix}$ est un isom de gpes

En général : $\varphi : G_1 \to G_2$ induit $\hat\varphi : \widehat{G_2} \to \widehat{G}$ (morph de gpes)

(ii) On note $\iota_1 : G_1 \hookrightarrow G_1 \times G_2$, $p_1 : G_1\times G_2 \to G_1$, de même ι_2 et p_2.
$g_1 \mapsto (g_1, e_{G_2})$ $\quad (g_1, g_2) \mapsto g_1$

L'appl° $\widehat{G_1 \times G_2} \longrightarrow \widehat{G_1} \times \widehat{G_2}$ est un isom de gpes
$\chi \longmapsto (\chi\circ\iota_1, \chi\circ\iota_2)$
$(\chi_1\circ p_1)(\chi_2\circ p_2) \longleftarrow (\chi_1, \chi_2)$

on grossit le gpe

Thm (inflation-restriction) : Soit G gpe abélien, H s/s-gpe de G (distingué), π la projection de G ds G/H.

(i) L'appl° $\mathrm{inf}_H^G : \widehat{G/H} \longrightarrow \widehat{G}$ est un morphisme de gpes injectif, d'image $H^\perp = \{\varphi \in \widehat{G} / \varphi_{|H} \equiv 1\}$
$\chi \mapsto \chi\circ\pi$

analogie ev

(ii) L'appl° $\mathrm{res}_H^G : \widehat{G} \longrightarrow \widehat{H}$ est un morphisme de gpe de noyau $H^\perp$.
$\chi \mapsto \chi_{|H}$

(ii') Si $[G:H]$ est fini, res_H^G est surjectif. En fait tjrs vrai ?

D) (i) Comme avec $H = D(G)$

+ généralement $\varphi : G_1 \to G_2$ induit adjoint $\widehat{G_2} \to \widehat{G_1}$
$\chi \mapsto \chi\circ\varphi$

Morphisme de gpes : à vérifier
Injectif par surjectivité de π
Image $= \{\varphi \in \widehat{G} / H \leq \mathrm{Ker}\,\varphi\}$ thm de factorisation

(ii) Morph de gpes ✓ ; $\mathrm{Ker} = H^\perp$ par déf°

Toute se joue sur la première récurrence — pose $\mathcal{H}(n\in?)$ — initialise — hérédité — ccl

(ii') Par récurrence forte sur $[G:H]$.
Pour r ds $\mathbb{N}^*$, on pose $(\mathcal{H}_r)$: si $[G:H] = r$, alors res_H^G est surjectif

(I) Si $r = 1$ $G = H$, $\mathrm{res}_H^G = \mathrm{id}_{\widehat{G}}$ surj.

(H) On fixe r ds $\mathbb{N}_{\geq 2}$ tq $\forall k \in [\![1; r-1]\!]$, $\mathcal{H}_k$ vraie. On veut MQ $\mathcal{H}_r$ vraie : on supp $[G:H] = r$. Soit $\chi \in \widehat{H}$

- Cstr° d'un s/s gpe intermédiaire. Comme $r \geq 2$, on a $G \neq H$. On fixe $g \in G\setminus H$ et on pose $N = \langle H, g\rangle$
On a $H \leq N \neq H$ et $N = \{ \underset{\text{non unique}}{hg^m}, h\in H\ m\in\mathbb{Z}\}$

S/s gpe engendré - produit de s/s gpe

• Extension de χ à N : $\tilde{\chi}_{|H} = \chi$; choisir $\chi(g)$, de manière compatible (on peut avoir $g^m \in N$)

$[G:H] < \infty$ → On note $d = o(\pi(g))$ (fini car G/H fini) ; pr $k \in \mathbb{Z}$ on a : $d \mid k \Leftrightarrow \pi(g)^k = e_{G/H} \Leftrightarrow g^k \in H$

$\mathbb{C}$ alg clos → On fixe ζ ds $\mathbb{C}^\times$: $\zeta^d = \chi(g^d)$ ← du sens car $g^d \in H$

: L'appl° $N \xrightarrow{\tilde{\chi}} \mathbb{C}^\times$, $hg^m \mapsto \chi(h)\zeta^m$ est bien définie

Soient (h, h', m, m') ds $H^2 \times \mathbb{Z}^2$ tq $hg^m = h'g^{m'}$. MQ $\chi(h)\zeta^m = \chi(h')\zeta^{m'}$

On a $h'h^{-1} = g^{m-m'}$ dc $g^{m-m'} \in H$ dc $d \mid m-m' = dk$, $k \in \mathbb{Z}$

On a donc $\chi(h'h^{-1}) = \chi(g^{dk}) = \chi(g^d)^k = \zeta^{dk} = \zeta^{m-m'} = \chi(h')\chi(h)^{-1}$ ✓

: C'est un morph. de gpes : $\tilde{\chi}(hg^m h'g^{m'}) = \tilde{\chi}(hh'g^{m+m'}) = \chi(h)\chi(h')\zeta^{m+m'} = \tilde{\chi}(hg^m)\tilde{\chi}(h'g^{m'})$

: $\tilde{\chi}_{|H} = \chi$ par construction

• Conclusion $H \subsetneq N$ dc $[G:N] < r$ dc par HR : $\exists \hat{\chi} \in \hat{G}$ tq $\hat{\chi}_{|H} = \tilde{\chi}_{|H} = \chi$

(c) $\mathcal{H}_r$ vraie pr tt r ds $\mathbb{N}^*$. ■

Corollaire : Soit G abélien fini. On a $|G| = |\hat{G}|$. Plus tard : en fait $G \simeq \hat{G}$

D) (Idées) Récurrence sur $|G|$. Vrai si G cyclique (ex).

Sinon, pr $g \in G \setminus \{e\}$, $H = \langle g \rangle$, on a $|\hat{G}| = |H^\perp| |\hat{H}| = |\widehat{G/H}| |\hat{H}| \overset{\text{hyp réc}}{=} |G/H| |H| = |G|$ ■

Prop : L'appl° $ev : G \to \hat{\hat{G}}$, $g \mapsto (\hat{G} \to \mathbb{C}^\times, \chi \mapsto \chi(g))$ est (bien définie) un isom. de gpes

bidual !

Canonique, // ev

D) • bien définie : pr g fixé ds G $\forall (\chi_1, \chi_2) \in \hat{G}^2$ $ev_g(\chi_1\chi_2) \overset{\text{déf loi gpe sur } G}{=} (\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g) = ev_g(\chi_1)\, ev_g(\chi_2)$

dc $ev_g \in \hat{\hat{G}}$

• morph. de gpes $\forall (g_1, g_2) \in G^2$, on a : $\forall \chi \in \hat{G}$ $ev_{g_1g_2}(\chi) = \chi(g_1g_2) \overset{\chi \text{ hom}}{=} \chi(g_1)\chi(g_2) = ev_{g_1}(\chi)\, ev_{g_2}(\chi)$

dc $ev_{g_1g_2} = ev_{g_1} ev_{g_2}$ $= (ev_{g_1} ev_{g_2})(\chi)$ ds $\hat{\hat{G}}$

• $|\hat{\hat{G}}| = |\hat{G}| = |G|$ donc il suffit de montrer injectivité

Soit g ds $G \setminus \{e\}$ MQ $ev_g \neq 1_{\hat{G}}$ ie $\exists \chi \in \hat{G}$ tq $\chi(g) \neq 1$

$\langle g \rangle \neq \{e\}$ dc $\widehat{\langle g \rangle} \neq \{1\}$ (m̂ ordre) : soit $\chi \in \widehat{\langle g \rangle}$, $\chi \neq 1_{\langle g \rangle}$

On a $\chi(g) \neq 1$ sinon $\chi = 1_{\langle g \rangle}$

Soit $\tilde{\chi}$ ds $\hat{G}$ tq $\tilde{\chi}_{|\langle g \rangle} = \chi$. On a $ev_g(\tilde{\chi}) = \tilde{\chi}(g) = \chi(g) \neq 1$ ■

Lien avec décomposition de Frobenius

Thm (Structure des groupes abéliens finis) : Soit G groupe abélien fini.

(i) Il existe s dans $\mathbb{N}$ et $(d_1,..,d_s) \in \mathbb{N}_{\geq 2}^s$ tq : $d_1 | \dots | d_s$ et $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$

(ii) L'entier s et la famille $(d_1,..,d_s)$ satisfaisant (i) sont uniques (et ne dépendent que de la classe d'iso de G)

Rmq :
- $d_i \geq 2$ nécessaire pr unicité
- $s = 0 \iff G = \{e\}$
- $d_1 \dots d_s = |G|$ et $d_s = \exp(G)$ $\exists$ él^t d'ordre d_s de $d_s | \exp G$; $d_1|..|d_s \Rightarrow G$ de d_s-torsion $\Rightarrow d_s \geq \exp G$

⚠ pas unicité de l'iso, ni des s/s gpes cycliques ds la décomposition cf exo

D/ Existence : par récurrence (forte) sur $n = |G|$; pr $n \in \mathbb{N}^*$, on pose $(\mathcal{H}_n)$: pr tt G g.a.f tq $|G| = n$, (i) est vraie.

(I) $n = 1$ $G = \{e\}$ $s = 0$, famille vide conviennent $n=2$ aussi, $n=3$ si vs préférez

(H) Soit n ds $\mathbb{N}_{\geq 2}$ tq $\mathcal{H}_k$ vraie pr tt k ds $[\![1; n-1]\!]$. Soit G g.a.f d'ordre n

- Candidat pr le dernier facteur : seule info "intrinsèque" $d_s = \exp G$ dc dernier facteur engendré par él^t d'ordre $\exp G$

  On note $d = \exp G$. On a $|G| = n \geq 2$ dc $d \geq 2$. * Soit γ ds G d'ordre d

  * = utilisation d'un résultat précédent

- Construction d'un "supplémentaire" (⚠ $\nexists$ tjs pr grpe qcq).

  Si $\exists$, = noyau de la projection sur $\langle \gamma \rangle$, dc d'un morph de gpe ds $\langle \gamma \rangle \simeq \mathbb{Z}/d\mathbb{Z} \simeq \mu_d(\mathbb{C})$

  Soit χ un isom de gpe de $\langle \gamma \rangle$ ds $\mu_d(\mathbb{C})$. ex $\mathbb{Z}/d\mathbb{Z} \xrightarrow{\sim} \langle g \rangle \xrightarrow{\sim} \mu_d(\mathbb{C})$ $\zeta \in \mu_d^*(\mathbb{C})$

  $\bar{k} \mapsto \gamma^k \mapsto \zeta^k$

  * Soit $\tilde{\chi} \in \hat{G}$ prolongeant χ et $H = \ker \tilde{\chi}$

- $H \times \langle \gamma \rangle \xrightarrow{\sim} G$ est (bien défini) un morphisme de gpes car G abélien

  $(h, g) \mapsto hg$

  Injective : $hg = e \Rightarrow \tilde{\chi}(hg) = 1 \overset{H = \ker\tilde{\chi},\ \tilde{\chi}_{|\langle\gamma\rangle} = \chi}{\Rightarrow} \chi(g) = 1 \Rightarrow g = e$ car χ inj.

  Surjectif : Soit x ds G. $\tilde{\chi}(x)$ $(\in \mu_d(\mathbb{C}) = \langle \zeta \rangle)$ est de la forme $\zeta^k = \chi(\gamma)^k = \tilde{\chi}(\gamma^k)$ pr un $k \in \mathbb{Z}$

  alors $x\gamma^{-k} \in \ker \tilde{\chi} = H$ ✓

- Appl^o de l'HR à H On a $|\langle \gamma \rangle| \geq 2$ dc $|H| = |G|/|\langle\gamma\rangle| \in [\![1; n-1]\!]$ $H = \{e\}$ ok

  Par HR, $\exists$ $s \in \mathbb{N}$, $(d_1,..,d_s) \in \mathbb{N}_{\geq 2}^s$ tq $d_1 | \dots | d_s$ et $H \simeq \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$

- Ccl : reste à montrer $d_s | d$ H a un él^t d'ordre d_s, dc G aussi dc $d_s | \mathrm{ppcm}(o(x), x \in) = d$.

(C) $\mathcal{H}_n$ vraie pr tt n ds $\mathbb{N}^*$.

Unicité : pr s ds $\mathbb{N}$ on pose $\mathcal{H}_s$: pr ts $t \in [\![0; s]\!]$ et $d_1,..,d_s, c_1,..,c_t$ ds $\mathbb{N}_{\geq 2}$ tq $d_1 | \dots | d_s$, $c_1 | \dots | c_t$ et $\prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z} \simeq \prod_{i=1}^{t} \mathbb{Z}/c_i\mathbb{Z}$, on a $t = s$ et $(d_1,..,d_s) = (c_1,..,c_s)$

Si $\mathcal{H}_s$ vraie pr tt s ds $\mathbb{N}$, c'est OK. Récurrence forte

(I) Pr $s=0$ Tt t ds $\mathcal{H}_s$ est $=0$ ✓

(H) Soit $s \in \mathbb{N}^*$ tq $\mathcal{H}_t$ vraie pr tt $t \in [\![0;s-1]\!]$. Soient $t, d_1, .., d_s, c_1, .., c_t$ comme ds $\mathcal{H}_s$

- S/s-gpe des m-itérés - comparaison des cardinaux : "On va se débarasser de d_1"

  pr G, G_1, G_2 gpe ab., on a $\begin{array}{c} G \to G \\ m \mapsto m.g \end{array}$ morph. de gpe $(m \in \mathbb{N}^*)$

  Not° add. pr $m \in \mathbb{N}^*$ $\quad$ $G_1 \simeq G_2$ induit $m.G \simeq m.G_2$

  $G \geq m.G = \{m.g, g \in G\}$ $\quad$ $m(G \times G_2) = m.G_1 \times m.G_2$

  On a $d_1 \left(\prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z} \right) \simeq d_1 \left(\prod_{i=1}^{t} \mathbb{Z}/c_i\mathbb{Z} \right)$

  $\prod_{i=1}^{s} d_1\mathbb{Z}/d_i\mathbb{Z} \overset{*}{\simeq} \prod_{i=1}^{t} d_1\mathbb{Z}/c_i\mathbb{Z}$

  Où $\forall (d,c) \in \mathbb{N}_{\geq 2}$ $\quad d\mathbb{Z}/c\mathbb{Z} = d \cdot (\mathbb{Z}/c\mathbb{Z}) = \{d\bar{k}, \bar{k} \in \mathbb{Z}/c\mathbb{Z}\} = \langle \bar{d} \rangle_{\mathbb{Z}/c\mathbb{Z}} = d\mathbb{Z}+c\mathbb{Z}/c\mathbb{Z} = (d \wedge c)\mathbb{Z}/c\mathbb{Z}$

  ordre $\frac{c}{c \wedge d}$

  $d_1 | d_i$

  D'où $\prod_{i=1}^{s} \frac{d_i}{d_1} = \prod_{i=1}^{t} \frac{c_i}{c_i \wedge d_1}$ et $d_1^s = \prod_{i=1}^{t} (c_i \wedge d_1) \overset{*}{\leq} d_1^t$ $\quad \prod d_i = \prod c_i$

- Comme $d_1 \geq 2$ on a $s \leq t$ dc $s = t$ ($t \leq s$ par hyp)

- Si $\exists i \in [\![1,s]\!]$ tq $c_i \wedge d_1 < d_1$ alors $*$ donne $d_1^s < d_1^s$ dc $\forall i \in [\![1,s]\!]$ $d_1 | c_i$

- S/s-gpe des c_1 multiples : $c_1^s = \prod_{i=1}^{s} (d_i \wedge c_1) \leq c_1^s$ donne $c_1 | d_1$ dc (≥ 0) $c_1 = d_1$

- $*$ donne $\prod_{i=1}^{s} \mathbb{Z}/\left(\frac{d_i}{d_1}\right)\mathbb{Z} \simeq \prod_{i=1}^{s} \mathbb{Z}/\left(\frac{c_i}{c_1}\right)\mathbb{Z}$ $\quad$ $d_{i+1} = m_{i+1}d_i = u_{i+1}d_1 = m_i u_i d_1$

  $d_i = u_i d_1$

  avec $\frac{d_2}{d_1} | \dots | \frac{d_s}{d_1}$ et $\frac{c_2}{c_1} | \dots | \frac{c_s}{c_1}$

  Par HR pr $m = \max \{ s - |\{i \in [\![1,s]\!], d_i = d_1\}|, \text{idem pr } c \} < s$ on a $\forall i \in [\![1,s]\!]$

  entiers sont égaux

  $\frac{d_i}{d_1} = \frac{c_i}{c_1}$ dc $d_i = c_i$

(C) $\forall s \in \mathbb{N}$ $\mathcal{H}_s$ vraie.

Corollaire : Pr G g.a.f, on a $G \simeq \hat{G}$ (non canoniquement)

Généralisations possibles :

- Décomposition en $\times$ p-Sylow, p^∞-torsion.
- Grpes abéliens de type fini
- Produit semi-direct (D_n, $\mathfrak{S}_n$, GL_n ...)
- Grpes d'ordre pq
- Classification des gpes d'ordre ≤ 11
- $(\mathbb{Z}/n\mathbb{Z})^\times$ cyclique $\Leftrightarrow$?