Théorème de structure des g.a.f. (existence)

Leçons : 102, 104, 107, 120 (Lemme + existence), 142 (existence + unicité)

Réf. : Berhuy - Algèbre : Le grand combat p 347 et p 358 (2e édition)
(lemme X) (Th. g.a.f.)

Lemme : (prolongement des caractères linéaires)

Soit G un groupe abélien et H un sous groupe de G.

Alors $\rho_H : (\widehat{G}, .) \longrightarrow (\widehat{H}, .)$ est un morphisme de groupes (de noyau $\widehat{G/H}$)
$\chi \longmapsto \chi_{|H}$

De plus, si $[G:H]$ est fini, alors ρ_H est surjectif.

Th. : (structure des groupes abéliens finis)

Soit G un groupe abélien fini tq $|G| \geq 2$.

Alors il existe des entiers $d_1, \dots, d_s \geq 2$ vérifiant $d_s \mid d_2 \mid \dots \mid d_1$

tels que $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$

De plus, $d_1 \dots d_s$ sont uniques et ne dépendent que de la classe d'isomorphisme de G.

Lemme :

Méthode : récurrence sur $[G:H]$

ρ_H morphisme de groupes : c'est clair

Soit $n \in \mathbb{N}^*$. On considère la proposition suivante :

(H_n) : $\forall H \leq G$ tq $[G:H] \leq n$, ρ_H est surjective

- $n = 1$: si $[G:H] = 1$, alors $H = G$ donc (H_1) est vérifiée.

- Soit $n \in \mathbb{N}^*$. OSP (H_n) vérifiée. Montrons que (H_{n+1}) est alors vérifiée

Soit $H \leq G$ tq $[G:H] \leq n+1$. Si $[G:H] \leq n$, alors on peut appliquer l'hypothèse de récurrence, donc OPS $[G:H] = n+1$

Idée: Construire $H' \leq G$ tq $H \subsetneq H'$ et tel qu'on sache prolonger "à la main" $\chi \in \hat{H}$ en $\chi' \in \hat{H'}$.

Comme $H \subsetneq H'$, $[G:H'] < [G:H]$ et on peut utiliser l'hyp. de récurrence pour prolonger χ' (donc χ) en $\chi'' \in \hat{G}$

$[G:H] \geq 2$ donc $H \neq G$ donc il existe $g \in G \setminus H$

On pose $H' = \langle H, g \rangle$

Alors $H \subsetneq H'$ et

$\forall h' \in H', \exists h \in H, \exists n \in \mathbb{Z} \;/\; h' = h g^n$ (car Gabélien)

$g \notin H$ donc $\overline{g} \neq \overline{1}$ dans G/H (qui est fini), donc $\overline{g}$ est d'ordre $d \geq 1$.

On a alors $\overline{g}^d = \overline{g^d} = \overline{1}$ donc $g^d \in H$.

Soit $\chi \in \hat{H}$

$g^d \in H$ donc $\chi(g^d) \in \mathbb{C}^*$ est bien défini.

Soit $\zeta \in \mathbb{C}^*$ une racine d-ième de $\chi(g^d)$

On pose alors pour $h' \in H'$: $\chi'(h') = \chi(h)\,\zeta^n$.

Si χ' est "bien défini", alors il est clair que $\chi' \in \hat{H'}$ et prolonge χ.

Il q. χ' ne dépend pas de la décomposition de h' choisie.

Soient $h_1, h_2 \in H$, $n_1, n_2 \in \mathbb{Z}$ tels que $h' = h_1 g^{n_1} = h_2 g^{n_2}$

On a alors $g^{n_2 - n_1} = h_1 h_2^{-1} \in H$

donc $\overline{g^{n_2-n_1}} = \overline{1}$ donc $d \mid n_2 - n_1$.

Il existe $k \in \mathbb{Z}$ tq $n_2 - n_1 = kd$.

On a alors $\chi(h_1)\,\zeta^{n_1} = \chi(h_2\, g^{n_2-n_1})\,\zeta^{n_1}$

$= \chi(h_2\,(g^d)^k)\,\zeta^{n_1}$

$= \chi(h_2)\,(\chi(g^d))^k\,\zeta^{n_1}$

$= \chi(h_2)\,\zeta^{dk}\,\zeta^{n_1}$

$\chi(h_1)\,\zeta^{n_1} = \chi(h_2)\,\zeta^{n_2}$ donc χ' est bien défini.

Enfin, $H \subsetneq H'$ donc $[G:H'] < [G:H] = n+1$

donc $[G:H'] \leq n$, et par hypothèse de récurrence, il existe $\chi'' \in \hat{G}$ prolongeant χ', donc prolongeant χ.

Th. (récurrence sur $|G|$) **Existence**

Méthode: en notant $e = \exp(G)$, on construit $\chi : G \twoheadrightarrow \mathbb{U}_e$ surjectif et on obtient alors une suite exacte courte $1 \to H \hookrightarrow G \twoheadrightarrow \mathbb{U}_e \to 1$ où $H = \ker \chi$.

On a alors $G \simeq H \times \mathbb{U}_e \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}$ par hyp. de récurrence. Reste à m.q. $d_s \mid e$.

Soit $n \in \mathbb{N}$, $n \geq 2$. On considère la proposition :

(H_n) : la partie existence est vraie pour tout g.a.f. G tq $|G| \leq n$.

. **$n = 2$:** alors $G \simeq \mathbb{Z}/2\mathbb{Z}$ donc (H_2) est vérifiée.

. Soit $n \geq 2$. OSP (H_n) vérifiée. M.q. (H_{n+1}) est alors vérifiée.

Soit G un groupe abélien fini tq $2 \leq |G| \leq n+1$.

Si $|G| \leq n$, on peut appliquer l'hyp. de récurrence, donc OPS $|G| = n+1$

1) "χ_0"

Soit $e = \exp(G)$. $|G| \geq 2$ donc G est non trivial d'où $e \geq 2$.

Soit $x_0 \in G$ tq $o(x_0) = e$

Alors $\langle x_0 \rangle$ est cyclique d'ordre e, donc il existe un isomorphisme $\chi_0 : \langle x_0 \rangle \xrightarrow{\sim} \mathbb{U}_e$

où $\mathbb{U}_e = \{\zeta \in \mathbb{C}^*,\ \zeta^e = 1\}$.

2) Prolongement à G

$\langle x_0 \rangle \leq G$ et $x_0 \in \widehat{\langle x_0 \rangle}$ donc par le lemme de prolongement des caractères, il existe $\chi : G \to \mathbb{C}^*$ un caractère de G prolongeant χ_0.

On a alors $\mathbb{U}_e \subset \operatorname{Im} \chi$.

On a, $\forall x \in G$, $x^e = 1$ donc $\chi(x)^e = 1$ donc $\boxed{\operatorname{Im} \chi = \mathbb{U}_e}$.

On a donc $\boxed{\chi : G \twoheadrightarrow \mathbb{U}_e \text{ et } \chi \text{ est surjectif.}}$

3) Suite exacte courte

L'isomorphisme $\chi_0^{-1} : \mathbb{U}_e \xrightarrow{\sim} \langle x_0 \rangle$ se prolonge en un morphisme $s : \mathbb{U}_e \to G$ tel que $\chi \circ s = id_{|\mathbb{U}_e}$.

Par conséquent, en posant $H = \ker \chi$, la suite exacte courte

$$1 \to H \xrightarrow{i} G \underset{s}{\overset{\chi}{\rightleftarrows}} \mathbb{U}_e \to 1$$

est scindée car s est une section de χ.

On a donc $\boxed{G \simeq H \times \mathbb{U}_e}$

- si $|H| = 1$, alors on a $G = \langle x_0 \rangle$ donc $G \simeq \mathbb{U}_e$ soit $G \simeq \mathbb{Z}/e\mathbb{Z}$
- si $|H| \leq 2$, comme $|G| = |H| \times e$, $2e \leq |H| \leq n$

et par hyp. de récurrence,

$$\exists\, d_1 \dots d_s \geq 2 \;/\; H \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z} \text{ et } d_1 | \dots | d_s.$$

d'où $\boxed{G \overset{\varphi}{\simeq} \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}}$

4) $\Pi_g \cdot d_s | e$

Soit $y = (\bar{0}, \dots, \bar{0}, \bar{1}, \bar{0}) \in \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}$.

Alors, $o(y) = d_s$, et φ étant un isomorphisme,

$x = \varphi^{-1}(y)$ est d'ordre d_s.

$x \in G$ donc $x^e = 1$ donc $\boxed{d_s | e}$

Unicité

Rappel : Soit $d \geq 1$, alors $\overline{d}$ est d'ordre $\frac{n}{\text{pgcd}(d,n)}$ dans $\mathbb{Z}/n\mathbb{Z}$.

En effet, soit $c = \text{pgcd}(d,n)$.

On a $d = cd'$ où $d' \wedge n' = 1$
$n = cn'$

$k\overline{d} = \overline{0} \iff n \mid kd$

$\iff cn' \mid kcd'$

$\iff n' \mid kd'$ (lemme de Gauss)

$\iff n' \mid k$

donc $o(\overline{d}) = n' = \frac{n}{\text{pgcd}(d,n)}$

On suppose $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z} \simeq \mathbb{Z}/d'_1\mathbb{Z} \times \dots \times \mathbb{Z}/d'_t\mathbb{Z}$

où $2 \leq d_1 \mid \dots \mid d_s$ et $2 \leq d'_1 \mid \dots \mid d'_t$.

Sans perte de généralité, OPS que $s \geq t$.

On a $d_1 G \simeq d_1\mathbb{Z}/d_1\mathbb{Z} \times \dots \times d_1\mathbb{Z}/d_s\mathbb{Z} \simeq d_1\mathbb{Z}/d'_1\mathbb{Z} \times \dots \times d_1\mathbb{Z}/d'_t\mathbb{Z}$

On, $\forall\, d, n \geq 1$, $d\mathbb{Z}/n\mathbb{Z} = \langle \overline{d} \rangle$ donc

$$|d_1 G| = \frac{d_1}{\text{pgcd}(d_1,d_1)} \times \dots \times \frac{d_s}{\text{pgcd}(d_1,d_s)} = \frac{|G|}{d_1^s} \quad \text{car } d_1 \mid d_i \ \forall 1 \leq i \leq s$$

et $$|d_1 G| = \frac{|G|}{\prod_{i=1}^{t} \text{pgcd}(d_1, d'_i)}$$

Donc $$d_1^s = \prod_{i=1}^{t} \text{pgcd}(d_1, d'_i) \leq d_1^t$$

$d_1 \geq 2$, donc $s \leq t$ donc $\boxed{s = t}$

Si $\text{pgcd}(d_1, d'_1) < d_1$, alors $\prod_{i=1}^{t} \text{pgcd}(d_1, d'_i) < d_1^t = d_1^s$

absurde

donc $\text{pgcd}(d_1, d'_1) = d_1$ donc $\boxed{d_1 \mid d'_1}$.

On a $s = t$ donc d_1 et d'_1 jouent des rôles symétriques donc $\boxed{d'_1 \mid d_1}$

On a donc $\boxed{d_1 = d'_1}$, et en itérant le procédé $\boxed{d_i = d'_i \quad \forall\, 1 \leq i \leq s = t}$.