M'39 sans étape 2, lemme 2, csqce — n' faire vite

THÉORÈME DE STRUCTURE DES GROUPES ABÉLIENS FINIS.

Colmez p252

Prérequis : • décomposit° en premiers, écriture des ppcm, associativité du ppcm, $a \mid d$ $b \mid d \Rightarrow$ ppcm $\mid d$.

• $|G| = |\hat{G}|$

• Les caractères forment une b.o.n de $\mathbb{C}[G]$ ~~pour~~ G abélien

• un sg cycliq d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$

• un sg de U_n est de la forme U_d où $d \mid n$.

• caractérisat° du produit direct

Rappel : Si G est un groupe abélien fini, on note son groupe dual $\hat{G}$, c'est l'ensemble des morphismes de groupes de G dans $\mathbb{C}^*$, muni de la multiplication. Les éléments de $\hat{G}$ sont appelés caractères linéaires. Les caractères linéaires sont les représentations de degré 1 (et aussi les caractères car deg = 1) ce sont donc des représentat° irréductibles (et ce sont les seuls car G est abélien). On a donc $\hat{G} = \mathrm{Irr}(G)$ et $|G| = |\hat{G}|$. car G abélien $\Rightarrow |G| = |\mathrm{Conj}(G)|$

Def : L'exposant d'un groupe abélien fini G est le plus petit N tq $\forall g \in G$ $g^N = e$.

Lemme 1 Soit G un groupe abélien fini. Son exposant est égal à $\underset{g\in G}{\mathrm{ppcm}}\, o(g)$. De plus il existe un élément de cet ordre dans G.

Dém : On note N l'exposant de G.

• Soit $g \in G$, on a $g^N = e$ d'où $o(g) \mid N$ d'où $\underset{g\in G}{\mathrm{ppcm}}(o(g)) \mid N$

or $g^{\mathrm{ppcm}\, o(g)} = e$ d'où $N \leq \mathrm{ppcm}\, o(g)$ Donc $\mathrm{ppcm}(o(g)) = N$

Etape 1 : Pour $x, y \in G$ d'ordre respectif n et m, on va montrer qu'il existe $z \in G$ tel que $o(z) = \mathrm{ppcm}(n, m)$.

Posons $k = \prod_{\substack{p \mid n \\ \nu_p(n) \geq \nu_p(m)}} p^{\nu_p(n)}$ et $\ell = \prod_{\substack{p \mid m \\ \nu_p(m) > \nu_p(n)}} p^{\nu_p(m)}$ alors k et ℓ n'ont aucun facteur premier commun par construction, donc k et ℓ sont premiers entre eux.

De plus pour p premier, $\nu_p(k\ell) = \begin{cases} \nu_p(n) & \text{si } \nu_p(n) \geq \nu_p(m) \\ \nu_p(m) & \text{sinon} \end{cases} = \max(\nu_p(n), \nu_p(m))$

donc $k\ell = \mathrm{ppcm}(n, m)$.

Comme $k \mid n$, on peut écrire $x' = x^{n/k}$, de même $\ell \mid m$ d'où on pose $y' = y^{m/\ell}$

Ainsi construit, x' est d'ordre k : on a $x'^k = x^n = e$ d'où $o(x') \mid k$ or s'il existait $k' < k$ tq $o(x') = k'$ alors $e = x'^{k'} = x^{n\frac{k'}{k}}$ d'où $o(x) \leq n\frac{k'}{k} < n$ ↯

Donc $o(x') = k$ et de la même manière y' est d'ordre ℓ.

Comme $k \wedge \ell = 1$, on est ramené à étudier le cas $n \wedge m = 1$.

On va montrer que $x'y'$ est d'ordre $k\ell = \mathrm{ppcm}(n, m)$ ce qui conclura l'étape.

1'20 Etape 2 : Soit x d'ordre n et soit y d'ordre m avec $n \wedge m = 1$. Alors $o(xy) = nm$.

• $(xy)^{nm} \underset{G \text{ abélien}}{=} x^{nm} y^{nm} = (x^n)^m (y^m)^n = e^m e^n = e$ d'où $o(xy) \mid nm$.

• Notons $q = o(xy)$. On a $(xy)^q = e$.

Supposons par l'absurde que $n \nmid q$ et $m \nmid q$ alors $x^q \neq e$ d'où $y^q = (x^q)^{-1} \in \langle x \rangle \cap \langle y \rangle$.

or $\langle x \rangle \cap \langle y \rangle = \{e\}$ car $n \wedge m = 1$. d'où $y^q = e$ d'où $m = o(y) | q$. ↯.
Donc $n | q$ ou $m | q$.
Supposons (le 2ᵉ cas est symétrique) que $n | q$ alors $x^q = e$ d'où $y^q = e$ d'où $m | q$ or $n \wedge m = 1$ d'où $nm | q$.
Donc $o(xy) = nm$.

Etape 3 : Conclusion :

On a montré que pour tout $x, y \in G$ d'ordre respectif n et m, il existe $z \in G$ d'ordre $\mathrm{ppcm}(n,m)$. En réitérant ce procédé, comme G est fini et comme le ppcm est associatif, on montre qu'il existe un élément d'ordre $\mathrm{ppcm}_{g \in G}\, o(g)$. (ou par récurrence)

L

Lemme 2 : Si G est un groupe abélien fini, $i : G \to \hat{\hat{G}}$, $g \mapsto ev_g : \left| \begin{array}{l} \hat{G} \to \mathbb{C}^\times \\ \chi \mapsto \chi(g) \end{array} \right.$ ~~est un isomorph.~~ un morphisme injectif de groupes.

Dém : ~~Comme G et $\hat{\hat{G}}$ ont même cardinal, il suffit de montrer que i est injectif.~~

Soit $g \in G$ tel que $i(g) = e_{\hat{\hat{G}}}$. alors $\forall \chi \in \hat{G}$, $\chi(g) = 1$.

Or les éléments de $\hat{G} = \mathrm{Irr}(G)$ forment une b.o.n. de l'espace des fonctions centrales de G dans $\mathbb{C}$. En particulier,
C'est une fonction centrale car G est abélien !
$\mathbb{1}_g = \sum_{\chi \in \hat{G}} \langle \mathbb{1}_g, \chi \rangle \chi$. Or pour tout $\chi \in \hat{G}$, $\langle \mathbb{1}_g, \chi \rangle = \frac{1}{|G|} \sum_{h \in G} \overline{\mathbb{1}_g}(h)\, \chi(h)$
d'où $\langle \mathbb{1}_g, \chi \rangle = \frac{\chi(g)}{|G|} = \frac{1}{|G|}$ par hypothèse.
D'où $\mathbb{1}_g(e) = \sum_{\chi \in \hat{G}} \frac{1}{|G|} \chi(e) = 1$ donc $g = e$.

L

Conséquence : G et $\hat{G}$ ont même exposant : Notons N l'exposant de G et M celui de $\hat{G}$,

* on a $\forall \chi \in \hat{G}$ $\chi^M = 1$ donc $\forall g \in G$ $\forall \chi \in \hat{G}$ $\chi(g^M) = \chi^M(g) = 1$ d'où $g^M = 1$ car i est injectif. donc $N \leq M$
* Soit $\chi \in \hat{G}$, $\chi^N(g) = \chi(g^N) = \chi(1) = 1$ et ce pour tout $g \in G$. donc $\forall \chi \in \hat{G}$ $\chi^N = 1$ d'où ~~d'où~~ $M \leq N$. Donc $N = M$.

Thm : Soit G un groupe abélien fini. On note N_1 son exposant, alors il existe $N_r | \dots | N_2 | N_1$ tels que $G \simeq \mathbb{Z}/N_1\mathbb{Z} \times \dots \times \mathbb{Z}/N_r\mathbb{Z}$.

Dém : On va montrer le théorème par récurrence sur $|G|$.

* Pour $|G| = 1$, avec $N_1 = 1$ c'est ok.
* Soit $|G| > 1$. On suppose le résultat vrai pour tout groupe de cardinal inférieur.

On note N_1 l'exposant de G. On vient de voir que l'exposant de $\hat{G}$ est aussi N_1.

donc par le premier lemme, on sait qu'il existe $\chi_1 \in \widehat{G}$ d'ordre N_1.

$\chi_1(G)$ est un sous groupe de $\mathbb{C}^*$ et plus précisément de $\mathbb{U}_{N_1}$ car

← racines N_1 e de l'unité.

$\forall g \in G \quad \chi_1^{N_1}(g) = 1$. - donc $\chi_1(G)$ est de la forme $\mathbb{U}_\ell$ où $\ell | N_1$ = $\forall g \in G \ \chi_1^{\ell}(g) = 1$

donc $N_1 \leq \ell$

Or χ_1 est d'ordre N_1 donc $\chi_1(G) = \mathbb{U}_{N_1}$.

En particulier, il existe $x_1 \in G$ tel que $\chi_1(x_1) = \exp\left(\frac{2i\pi}{N_1}\right)$.

x_1 est d'ordre N_1 : $N_1 = \underset{g\in G}{\mathrm{ppcm}}(o(g))$ d'où $o(x_1) | N_1$

et de plus $\chi_1^{o(x_1)}(x_1) = \chi_1(x_1^{o(x_1)}) = \chi_1(e) = 1$

$= \exp\left(2i\pi \frac{o(x_1)}{N_1}\right)$

d'où $N_1 | o(x_1)$. Donc $o(x_1) = N_1$.

Ainsi $H_1 = \langle x_1 \rangle$ est un sous groupe cyclique de G d'ordre N_1. (donc isomorphe à $\mathbb{Z}/_{N_1\mathbb{Z}}$).

* Montrons que $G \simeq H_1 \times \ker \chi_1$. $\to |G| = \underbrace{|H_1|}_{>1} |\ker \chi_1| \quad \to |\ker \chi_1| < |G|$

→ $\ker \chi_1 = \{g \in G, \chi_1(g) = \chi_1(e)\} = \ker \rho_1$ sous groupe de G.

→ On a $\chi_{1|H_1} : H_1 \longrightarrow \mathbb{U}_{N_1}$ qui est surjectif : en effet,

$\in \mu_{N_1}^{\times} \cap \chi_1(H$

$\chi_1(H_1)$ est de la forme $\mathbb{U}_d$ où $d | N_1$ (comme avant) or $x_1 \in H_1$ et $\chi_1(x_1)$ est d'ordre N_1 car c'est une racine N_1e de l'unité donc $\chi_1(H_1) = \mathbb{U}_{N_1}$.

Or $|H_1| = N_1 = |\mathbb{U}_{N_1}|$ donc $\chi_{1|H_1}$ est bijectif.

→ $H_1 \cap \ker \chi_1 = \{e\}$ car $\chi_{1|H_1}$ est injectif.

→ $G = H \ker \chi_1$: soit $g \in G$, par surjectivité, il existe $h \in H_1$ tq $\chi_1(g) = \chi_1(h)$ donc $gh^{-1} \in \ker \chi_1$

Comme G est abélien, on a par caractérisat° du produit direct, $G \simeq H_1 \times \ker \chi_1$.

Or $\ker \chi_1$ est un sous groupe de G de cardinal strictement inférieur à $|G|$

donc par hypothèse de récurrence, il existe $N_r | \dots | N_2$ tq $\ker \chi_1 \simeq \mathbb{Z}/_{N_2\mathbb{Z}} \times \dots \times \mathbb{Z}/_{N_r\mathbb{Z}}$.

où N_2 est l'exposant de $\ker \chi_1$ qui est un sous groupe de G. donc $N_2 | N_1$.

D'où le résultat par récurrence.

Si H est un sg de G, il existe $h \in H$ d'ordre exposant de H.

or $o(h) \,|\, \underset{g \in G}{\mathrm{ppcm}}(o(g))$ = exposant de G

exposant de H

$h \in H \subset G$

Tout ne rentre pas, choisir selon leçon