Théorème de structure des groupes abéliens finis

Dorian Cacitti-Holland

2020-2021

Références.

1. Eléments d'analyse et d'algèbre de Pierre Colmez

Leçons.

1. 102 Groupe des nombres complexes de module 1, sous-groupes des racines de l'unité, applications
2. 104 Groupes abéliens et non abéliens finis, exemples et applications
3. 107 Représentations et caractères d'un groupe fini sur un $\mathbb{C}$-espace vectoriel
4. 120 Anneaux $\mathbb{Z}/n\mathbb{Z}$, applications
5. 142 PGCD et PPCM, algorithmes de calcul, exemples

Proposition. Soit G un groupe abélien fini, alors il existe $g \in G$ d'ordre l'exposant de G (le plus petit multiple commun des ordre des éléments de G).

Démonstration.
Etape 1 : Soit $x, y \in G$ d'ordre a, b premiers entre eux, alors xy est d'ordre ab
On a par caractère abélien $(xy)^{ab} = x^a y^b = 1$, donc

$$o(xy) \mid ab$$

Réciproquement soit $n \in \mathbb{N}$ tel que $(xy)^n = 1$, alors $y^{an} = (xy)^{an} = 1$ et $x^{bn} = (xy)^{bn} = 1$.
Donc $b \mid an$ et $a \mid bn$, d'où, comme a et b sont premiers entre eux, $b \mid n$ et $a \mid n$ puis $ab \mid n$.
En particulier pour $n = o(ab)$,

$$ab \mid o(xy)$$

Par conséquent $ab = o(xy)$.
Etape 2 : Soit $x, y \in G$ d'ordre a, b, alors il existe $z \in G$ d'ordre $PPCM(a, b)$
On considère

$$k = \prod_{p \in \mathcal{P}, \nu_p(a) > \nu_p(b)} p^{\nu_p(a)}, l = \prod_{p \in \mathcal{P}, \nu_p(a) \leq \nu_p(b)} p^{\nu_p(b)}$$

Alors $kl = PPCM(a, b)$ et k, l sont premiers entre eux.
Donc $x' := x^{\frac{a}{k}}$ et $y' := y^{\frac{b}{l}}$ sont d'ordres respectifs k et l, d'où, d'après ce qui précède, $z := x'y'$ est d'ordre $kl = PPCM(a, b)$.
Etape 3 : Il existe $g \in G$ d'ordre $N(G)$

Par conséquent, comme $N(G) = PPCM(o(h), h \in G)$, par itérations successives finies car G fini, il existe $g \in G$ tel que

$$o(G) = PPCM(o(h), h \in G) = N(G)$$

□

Théorême. Soit G groupe abélien fini, alors il existe $r \in \mathbb{N}$ et $(d_1, ..., d_r) \in \mathbb{N}^r$ tel que

$$\forall i \in [\![1, r-1]\!], d_{i+1} \mid d_i$$

Et

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times ...\mathbb{Z}/d_r\mathbb{Z}$$

avec $d_1 = N(G)$.

Démonstration.
On raisonne par récurrence sur $n = |G| \in \mathbb{N}^*$:

— Pour $n = 1$: Si $|G| = 1$ alors

$$G = \{1\} \simeq \mathbb{Z}/1\mathbb{Z}$$

D'où $r = 1$ et $d_1 = 1$.

— On suppose le résultat vrai pour tout groupe H tel que $|H| < |G| = n$.
On a $N(G) = N(\hat{G})$, donc, d'après la proposition précédente, il existe $\chi \in \hat{G}$ tel que

$$o(\chi) = N(\hat{G} = N(G)$$

Or pour tout $x \in G$, $\chi(x)$ est une racine $N(G)$-ième de l'unité, ainsi $\chi(G)$ est un sous-groupe de $\mathbb{U}_{N(G)}$.
On suppose par l'absurde que $d := |\chi(G)| < N(G)$, dans ce cas

$$\forall g \in G, \chi^d(g) = \chi(g)^d = 1$$

Ce qui contredit le fait que $o(\chi) = N(G) > d$.
Par conséquent

$$\chi(G) = \mathbb{U}_{N(G)}$$

Il existe donc $g \in G$ tel que

$$\chi(g) = e^{i\frac{2\pi}{N(G)}}$$

Donc $o(\chi(g)) = N(G)$, puis, comme précédement,

$$o(g) = N(G)$$

Ainsi $G' = \langle g \rangle$ est cyclique d'ordre $N(G)$, d'où

$$G' \simeq \mathbb{Z}/N(G)\mathbb{Z}$$

De plus on a

$$G \simeq ker(\chi) \oplus G'$$

En effet :

— Soit $h \in ker(\chi) \cap G'$, alors $\chi(h) = 1$ et $h = g^k$ avec $k \in [\![1, N(G)]\!]$, d'où $\chi(g)^k = 1$, ainsi $k = N(G)$ et $h = 1$, ce qui montre bien

$$ker(\chi) \cap G' = \{1\}$$

— Ainsi $\chi : G' \longrightarrow \mathbb{U}_{N(G)}$ est un isomorphisme de groupes par égalité des cardinaux, on note $\alpha : \mathbb{U}_{N(G)} \longrightarrow G'$ son inverse.
Soit $x \in G$, on pose $a = \alpha(\chi(x)) \in G'$ et $b = a^{-1}x \in ker(\chi)$, d'où

$$x = ab \in ker(\chi) \times G'$$

Par conséquent

$$G \simeq ker(\chi) \oplus G' \simeq ker(\chi) \times G' \simeq ker(\chi) \times \mathbb{Z}/N(G)\mathbb{Z}$$

Puis, soit $G = G' \simeq \mathbb{Z}/N(G)\mathbb{Z}$, soit $G' \neq G$, dans ce cas, comme $|G'| = N(G)$

$$|ker(\chi)| = \frac{|G|}{N(G)} < |G|$$

D'où par hypothèse de récurrence il existe $r \in \mathbb{N}^*$ et $(d_2, ..., d_r) \in \mathbb{N}^{r-1}$ tel que

$$\forall i \in [\![2, r-1]\!], d_{i+1} \mid d_i$$

Et

$$ker(\chi) \simeq \mathbb{Z}/d_2\mathbb{Z} \times ... \times \mathbb{Z}/d_r\mathbb{Z}$$

On a

$$d_2 = N(ker(\chi)) \mid N(G) =: d_1$$

Et

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_r\mathbb{Z}$$

Le principe de récurrence permet donc de conclure.

□

Lemme. (S'il reste du temps) Soit G un groupe abélien fini alors G le groupe des caractères $\hat{G}$ de G ont le même exposant, ie le plus petit entier $k \in \mathbb{N}^*$ tel que

$$\forall g \in G, g^n = 1$$

Démonstration.
Soit H un groupe abélien fini et $N(H)$ son exposant, alors pour tout $\chi \in \hat{H}$,

$$\forall x \in H, \chi^{N(H)}(x) = \chi(x)^{N(H)} = \chi(x^{N(H)}) = \chi(1) = 1$$

D'où $\chi^{N(H)} = 1$.
Ainsi $N(\hat{H}) \mid N(H)$.
En particulier on a avec le lemme suivant,

$$N(G) = N(\hat{\hat{G}}) \mid N(\hat{G}) \mid N(G) \text{ ie } N(G) = N(\hat{G})$$

□

Lemme. (S'il reste encore du temps) Soit G un groupe abélien fini, alors

$$i : \begin{array}{ccc} G & \longrightarrow & \hat{\hat{G}} \\ g & \longmapsto & \left[\begin{array}{ccc} \hat{G} & \longrightarrow & \mathbb{C} \\ \varphi & \longmapsto & \varphi(g) \end{array} \right] \end{array}$$

Est un isomorphisme de groupes.

Démonstration.
Etape 1 : i est bien définie
Soit $g \in G$, alors

$$i(g)(\mathbb{1}_{triv}) = 1, \forall (\chi_1, \chi_2) \in \hat{G}^2, i(g)(\chi_1\chi_2) = (\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g) = i(g)(\chi_1)i(g)(\chi_2)$$

D'où $i(g) \in \hat{\hat{G}}$.
Etape 2 : i est un morphisme de groupes
Soit $(g_1, g_2) \in G^2$, alors

$$\forall \varphi \in \hat{G}, i(g_1g_2)(\varphi) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = (i(g_1)i(g_2))(\varphi)$$

D'où i est un morphisme de groupes.
Etape 3 : i est injectif
Soit $g \in G$ tel que

$$\forall \chi \in \hat{G}, 1 = i(g)(\chi) = \chi(g)$$

Or $\delta_g = \sum_{\chi \in \hat{G}} \langle \delta_g, \chi \rangle \chi$ avec

$$\forall \chi \in \hat{G}, \langle \delta_g, \chi \rangle = \frac{1}{|G|} \sum_{h \in G} \delta_g(h) \overline{\chi(h)} = \frac{\overline{\chi(g)}}{|G|} = \frac{1}{|G|}$$

En particulier pour $h = 1$, on obtient

$$\delta_g(1) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(1) = \frac{|\hat{G}|}{|G|} = 1$$

Ce qui montre bien que $g = 1$ et que i est injectif.
Etape 4 : i est bijectif
$|G| = |\hat{G}|$ car, comme G est abélien, $|G| = |Conj(G)| = |Irr(G)| = |\hat{G}|$ et de même $|\hat{G}| = |\hat{\hat{G}}|$.
Par conséquent i est un isomorphisme de groupes. □