Structure des groupes abéliens finis

Dans son rapport 2017, le jury de l'agrégation indique que pour de la session 2018, l'intitulé de la leçon 110 :

Caractères d'un groupe abélien fini et transformée de Fourier discrète. Applications

évoluera pour devenir

Structure et dualité des groupes abéliens finis. Applications.

Il écrit ensuite : *« Le théorème de structure des groupes abéliens finis a une place de choix dans cette leçon, et la dualité des groupes abéliens finis doit être détaillée. Comme application, la cyclicité du groupe multiplicatif d'un corps fini est tout à fait adaptée »*. Rappelons l'énoncé du théorème de structure des groupes abéliens finis.

Théorème. *Soit G un groupe abélien fini non nul. Alors il existe des entiers $r \geqslant 1$ et $1 < d_1|d_2|\dots|d_r$ et un isomorphisme $G \simeq (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_r\mathbb{Z})$. De plus, les entiers r et d_i sont uniques avec ces propriétés Les d_i sont appelés les* facteurs invariants *de G.*

Le jury parle de la dualité car pour montrer que le dual $\widehat{G}$ est isomorphe à G (non canoniquement !), on utilise le théorème de structure. En fait, il suffit de savoir que G est produit de groupes cycliques, et les conditions de divisibilité ne sont pas utiles. Le jury parle de la cyclicité du groupe multiplicatif d'un corps fini, car celle-ci est également un corollaire du théorème de structure. En fait, ici encore un énoncé plus faible que le théorème de structure suffit, précisément, le fait que tout groupe abélien fini possède un élément d'ordre égal à son exposant (voir Lemme 2 ci-dessous). Dans cette note, nous nous proposons d'exposer cet énoncé plus faible, de montrer comment en déduire la cyclicité du groupe multiplicatif d'un corps fini (voir Application ci-dessous), puis de montrer comment le théorème de structure des groupes abéliens finis peut à son tour être démontré à partir de l'énoncé faible... qui finalement n'est pas si faible que ça !

1 Exposant d'un groupe abélien fini

Nous commençons par quelques rappels classiques. Pour tout élément g d'un groupe G, on note $\langle g\rangle$ le sous-groupe engendré par g et $\mathrm{o}(g) = \mathrm{card}\langle g\rangle$ l'ordre (éventuellement infini) de g. Pour commencer, rappelons un fait archi-classique.

Lemme 1. *Soit G un groupe et x, y deux éléments qui commutent, d'ordres finis premiers entre eux. Alors xy est d'ordre fini égal au produit des ordres.*

Démonstration : Comme x et y commutent, pour tout k on a $(xy)^k = x^k y^k$. Notant $m = \mathrm{o}(x)$ et $n = \mathrm{o}(y)$, on déduit que $(xy)^{mn} = 1$ donc xy est d'ordre fini. Supposons que $(xy)^k = 1$ pour un entier k. Alors $x^k = y^{-k}$ qui est un élément de $H := \langle x\rangle \cap \langle y\rangle$. Comme sous-groupe de $\langle x\rangle$, resp. de $\langle y\rangle$, le groupe H est fini d'ordre diviseur de m, resp. de n. Comme m et n sont premiers entre eux on obtient $H = \{1\}$ donc $x^k = y^{-k} = 1$. Il en découle que $k|m$ et $k|n$ donc $k|mn$. □

Dans la suite, on considère des groupes abéliens, pour lesquels on utilise une écriture additive : le produit xy est noté $x+y$ et la puissance x^k est notée kx.

On rappelle que l'*exposant* d'un groupe fini G est le plus petit entier $n>1$ tel que $g^n=1$ pour tout $g\in G$. C'est aussi le ppcm des ordres de ses éléments. L'énoncé plus faible dont nous parlions ci-dessus est le suivant.

Lemme 2. *Soit G un groupe abélien fini et e son exposant. Alors G possède un élément d'ordre e.*

Démonstration : Soit $x\in G$ un élément d'ordre maximal noté n. Pour montrer que $n=e$ il suffit de montrer que l'ordre m de n'importe quel élément $y\in G$ divise n. Il suffit de montrer que pour tout nombre premier p, on a $v_p(m)\leqslant v_p(n)$ où $v_p(n)$ est la valuation p-adique de n, c'est-à-dire l'exposant de la plus grande puissance de p qui divise n. Écrivons $n=p^ar$ et $m=p^bs$ avec $p\nmid r$ et $p\nmid s$. Alors xp^a est d'ordre r, y^s est d'ordre p^b, et xp^ay^s est donc d'ordre p^br par le lemme 1. Comme n est l'ordre maximal, on déduit $p^br\leqslant n=p^ar$ d'où $b\leqslant a$. □

Ce lemme simple permet d'obtenir facilement la conséquence annoncée :

Application. *Soit G un sous-groupe fini du groupe multiplicatif $K^\times$ d'un corps commutatif K. Alors G est cyclique.*

Démonstration : Notons e l'exposant de G. Tous les éléments g de G vérifient $g^e=1$, donc sont racines du polynôme X^e-1 de sorte que $\operatorname{card}(G)\leqslant \operatorname{card}\operatorname{Rac}(X^e-1)\leqslant e$. Or d'après le lemme 2 il existe un élément $x\in G$ d'ordre e, donc $\operatorname{card}(G)\geqslant e$ et finalement $G=\langle x\rangle$ est cyclique. □

2 Existence

Pour la suite, rappelons qu'il existe une autre décomposition que celle du théorème de structure : la décomposition en composantes primaires, qui consiste à dire qu'un groupe abélien fini G est produit de ses sous-groupes de Sylow. Plus précisément, écrivons la décomposition en facteurs premiers $|G|=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$ et notons $G_i=\{x\in G; p_i^{\alpha_i}x=0\}$ qui est un p_i-groupe. La décomposition en composantes primaires est le fait qu'on a l'isomorphisme de groupes :

$$\begin{aligned} G_1\times\cdots\times G_s &\xrightarrow{\sim} G\\ (g_1,\dots,g_s)&\longmapsto g_1+\cdots+g_s. \end{aligned}$$

La démonstration est moins difficile que celle du théorème de structure : en effet, posons $q_i=\prod_{j\neq i}p_j^{\alpha_j}$ pour $1\leqslant i\leqslant s$; les q_i sont premiers entre eux donc il existe une relation de Bézout $u_1q_1+\cdots+u_sq_s=1$ et on vérifie sans peine que l'application $g\mapsto(u_1q_1g,\dots,u_sq_sg)$ est un isomorphisme inverse.

Ceci étant dit, la partie « existence » dans le théorème de structure découlera du petit ingrédient supplémentaire que voici :

Lemme 3. *Soit G un groupe abélien fini. Soit x un élément d'ordre maximal et $H=\langle x\rangle$. Alors tout élément de G/H peut être relevé dans G en un élément de même ordre.*

Démonstration : Soit $\overline{y}\in G/H$. Pour tout relevé $y\in G$ on a $\mathrm{o}(\overline{y})\,|\,\mathrm{o}(y)$, il nous suffit donc d'en trouver un tel que $\mathrm{o}(y)\,|\,\mathrm{o}(\overline{y})$.

Supposons d'abord que G est un p-groupe. Notons $\mathrm{o}(x)=p^s$ et $\mathrm{o}(\overline{y})=p^t$ avec $t\leqslant s$. Soit $y\in G$ quelconque qui relève $\overline{y}$. Alors $p^ty\in H$, i.e. $p^ty=ax$ pour un certain entier a. Ecrivons $a=p^kb$ avec

$p \nmid b$. Si $k < t$, du fait que $\mathrm{o}(x) = p^s$ on déduit que $\mathrm{o}(ax) = \mathrm{o}(pkbx) = p^{s-k}$ donc $\mathrm{o}(p^t y) = p^{s-k}$ puis $\mathrm{o}(y) = p^{s-k+t} > p^s = \mathrm{o}(x)$ en contradiction avec la maximalité de $\mathrm{o}(x)$. Nous avons donc $k \geqslant t$, et l'égalité $p^t y = ax$ fournit $p^t(y - p^{k-t}bx) = 0$ si bien que $y' := y - p^{k-t}bx$ est un relevé de $\overline{y}$ d'ordre diviseur de p^t.

Dans le cas d'un groupe abélien fini général, utilisons la décomposition en composantes primaires $G = G_1 \times \cdots \times G_m$ où les G_i sont les Sylow de G. On écrit $x = (x_1, \ldots, x_m)$ avec $x_i \in G_i$, et $\overline{y} = (\overline{y}_1, \ldots, \overline{y}_m)$ avec $\overline{y}_i \in G_i/\langle x_i \rangle$. Les ordres $|G_i|$ étant premiers entre eux, pour tout élément $g = (g_1, \ldots, g_m)$ avec $g_i \in G_i$, on a $\mathrm{o}(g) = \mathrm{o}(g_1) \cdots \mathrm{o}(g_m)$; on en déduit que x_i est d'ordre maximal dans G_i. Le cas des p-groupes déjà traité montre qu'il existe $y_i \in G_i$ d'ordre égal à celui de $\overline{y}_i$. Posons $y = (y_1, \ldots, y_m)$, alors $\mathrm{o}(y) = \mathrm{o}(y_1) \cdots \mathrm{o}(y_m) = \mathrm{o}(\overline{y}_1) \cdots \mathrm{o}(\overline{y}_m) = \mathrm{o}(\overline{y})$. □

Théorème de structure, démonstration de l'existence : si $G \neq 1$, on note e_1 l'exposant de G ; d'après le lemme 2, on peut choisir $x_1 \in G$ d'ordre maximal e_1 dans G ; on pose $H_1 = \langle x_1 \rangle$. Par récurrence, tant que $G \neq H_i$, on note e_{i+1} l'exposant de G/H_i ; d'après le lemme 2 il existe un élément $\overline{x}_{i+1} \in G/H_i$ d'ordre e_{i+1} et d'après le lemme 3 on peut choisir $x_{i+1} \in G$ d'ordre e_{i+1} qui relève $\overline{x}_{i+1}$. On pose $H_{i+1} = \langle x_1, \ldots, x_{i+1} \rangle$. Comme G est fini, il existe r tel que $G = H_r = \langle x_1, \ldots, x_r \rangle$. Ceci signifie que le morphisme de groupes $f_0 : \mathbb{Z}^r \to G$, $(n_1, \ldots, n_r) \mapsto n_1 x_1 + \cdots + n_r x_r$ est surjectif. Comme $e_i x_i = 0$ dans G, il y a un morphisme de groupes induit $f : (\mathbb{Z}/e_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/e_r\mathbb{Z}) \to G$ qui est encore surjectif. Montrons que f est injectif. Si $n_1 x_1 + \cdots + n_r x_r = 0$ dans G, alors dans G/H_{r-1} on obtient $n_r x_r = 0$, donc n_r est multiple e_r. Donc $n_r x_r = 0$, ainsi $n_1 x_1 + \cdots + n_{r-1} x_{r-1} = 0$ dans G et en recommençant par récurrence, on montre que e_i divise n_i pour tout i. Ceci prouve que f est injectif, donc un isomorphisme. Une propriété élémentaire est que si $\pi : G \to G'$ est un morphisme surjectif de groupes, l'exposant de G' divise celui de G. Il en découle que $e_r | e_{r-1} | \ldots | e_2 | e_1$ et on obtient donc le résultat en posant $d_i = e_{r+1-i}$. □

3 Unicité

La partie « unicité » découlera du lemme suivant.

Lemme 4. *Soit G un groupe abélien fini. Alors le groupe $\mathrm{Aut}(G)$ agit transitivement sur l'ensemble des éléments de G d'ordre maximal. En particulier, si x, y sont deux éléments d'ordre maximal, les groupes quotients $G/\langle x \rangle$ et $G/\langle y \rangle$ sont isomorphes.*

Démonstration : Supposons d'abord que G est un p-groupe. D'après la partie existence du théorème de structure, on peut supposer que $G = (\mathbb{Z}/p^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_r}\mathbb{Z})$ avec $a_1 \leqslant \cdots \leqslant a_r$. Notons $C_i = \mathbb{Z}/p^{a_i}\mathbb{Z}$ le i-ème facteur dans le produit, et k le nombre des a_i (les derniers de la liste) qui sont égaux à a_r. Un élément $x = (x_1, \ldots, x_r)$ est d'ordre maximal dans G, égal à p^{a_r}, si et seulement si l'une de ses k dernières composantes x_i engendre $C_i = \mathbb{Z}/p^{a_r}\mathbb{Z}$, c'est-à-dire n'est pas multiple de p. Par exemple, l'élément $x_0 = (0, \ldots, 0, 1)$ est d'ordre maximal, et il suffit de trouver un automorphisme φ tel que $\varphi(x_0) = x$. Quitte à renuméroter les facteurs, on peut supposer dans la suite que x_r engendre C_r. Notons $H = C_1 \times \cdots \times C_{r-1}$ vu comme le sous-groupe de G où la dernière composante s'annule, et $C'_r = \langle x \rangle$. Comme $x_r \neq 0$ on a $H \cap C'_r = \{0\}$, et comme x_r engendre le facteur C_r on a $H + C'_r = G$. Ceci montre que le morphisme $\lambda : H \times C'_r \to G$, $(h, c) \mapsto h + c$ est injectif et surjectif, donc un isomorphisme. Compte tenu de l'isomorphisme $\mu : C_r = \mathbb{Z}/p^{a_r}\mathbb{Z} \xrightarrow{\sim} C'_r$, $\ell \mapsto \ell x_r$ on obtient un *auto*morphisme :

$$\varphi : G = H \times C_r \xrightarrow{\mathrm{Id} \times \mu}{}^{\sim} H \times C'_r \xrightarrow{\lambda}{}^{\sim} G.$$

Comme $\mu(1) = x_r$, on voit que $\varphi(x_0) = x$.

Dans le cas général, écrivons la décomposition en composantes primaires $G = G_1 \times \cdots \times G_m$, et $x = (x_1, \ldots, x_m)$, $y = (y_1, \ldots, y_m)$. Pour tout i les éléments x_i et y_i sont d'ordre maximal dans G_i. D'après ce qui précède, il existe $\varphi_i : G_i \to G_i$ tel que $\varphi(x_i) = y_i$. Alors l'application $\varphi : G \to G$ défini par $\varphi(g) = (\varphi_1(g_1), \ldots, \varphi_m(g_m))$ est un automorphisme qui envoie x sur y.

Pour conclure, on choisit φ tel que $\varphi(x) = y$, alors $\varphi(\langle x \rangle) \subset \langle y \rangle$ et $\varphi^{-1}(\langle y \rangle) \subset \langle x \rangle$ donc φ induit un isomorphisme $G/\langle x \rangle \xrightarrow{\sim} G/\langle y \rangle$. □

Théorème de structure, démonstration de l'unicité : Supposons que l'on a deux isomorphismes :

$$(\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_r\mathbb{Z}) \simeq G \simeq (\mathbb{Z}/d'_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d'_s\mathbb{Z})$$

avec $1 < d_1 | d_2 | \ldots | d_r$ et $1 < d'_1 | d'_2 | \ldots | d'_s$. En particulier les deux groupes ont même exposant, c'est-à-dire $d_r = d'_s$. Choisissons l'élément d'ordre maximal $x = (0, \ldots, 0, 1)$ qui engendre $\mathbb{Z}/d_r\mathbb{Z}$ à gauche, et l'élément d'ordre maximal $x' = (0, \ldots, 0, 1)$ qui engendre $\mathbb{Z}/d'_s\mathbb{Z}$ à droite. D'après le lemme 4, en prenant les quotients on obtient un isomorphisme :

$$(\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_{r-1}\mathbb{Z}) \simeq (\mathbb{Z}/d'_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d'_{s-1}\mathbb{Z}).$$

En itérant ce raisonnement par récurrence, on montre que $d_i = d'_i$ pour tout i et que $r = s$. □

Remarques.

1) Le lemme 3 est inspiré de Lang, *Algèbre* (Dunod), lemme 1.8.3 (c'est-à-dire chapitre 1, lemme 8.3). La décomposition en composantes primaires y est invoquée ; on peut se reporter au livre Berhuy, *Modules, Théorie, pratique, et un peu d'arithmétique*, Calvage et Mounet, chap. VIII, th. 3.29. (Le théorème de structure des groupes abéliens finis y figure également, en chap VIII, cor. 3.2 et th. 3.9.)

2) Le théorème de structure des groupes abéliens finis se déduit assez facilement du théorème de structure des *p-groupes* abéliens finis. Il est donc tout à fait légitime et intéressant de se limiter à démontrer ce cas particulier ; on fait alors l'économie de l'argument qui utilise la décomposition en composantes primaires.

3) Je remercie Émeline Luirard et Bérenger Hug dont une question est à l'origine de cette note.