Structure des groupes abéliens finis

Théorème (Structure des groupes abéliens finis)**.** *Soit G un groupe abélien fini non réduit à un l'élément neutre. Alors il existe $d_1/d_2/\ldots/d_n$ dans $\mathbb{N}\setminus\{0,1\}$ tels que*

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}.$$

De plus la suite finie des facteurs $d_1, d_2, ..., d_n$ est l'unique suite vérifiant ces propriétés. On appelle ces facteurs, les facteurs invariants *de G.*

Notons qu'en particulier tout groupe abélien fini est isomorphe à un produit direct de groupes cycliques.

Pour définir le groupe abélien isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ vous pouvez entrer

```
A = AbelianGroup(3,[4,7,6],names='uvw')
A
```

Vous remarquez que les groupes abéliens finis sont notés multiplicativement en `SAGE`. L'argument `names='uvw'` est facultatif, il permet de donner les noms que vous souhaitez aux générateurs canoniques associés à votre définition de `A`. Afin de considérer des éléments de `A` en fonction de ces générateurs, on utilise la commande `C.gens()` qui retourne ceux-ci :

```
u,v,w = A.gens()
y = u^2*v^4*w^3
y
```

L'élément `y` de `A` correspond à l'élément $(2, 4, 3)$ de $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Calculer son ordre. Que vaut `y^2` ?

La méthode `elementary_divisors()` donne la liste des facteurs invariants :

```
A.elementary_divisors()
```

Exercice 1. *On considère les deux groupes abéliens*

$$G_1 = \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/35\mathbb{Z}$$
$$G_2 = \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/63\mathbb{Z}$$

Calculer l'ordre de G_1 et de G_2.
Calculer l'exposant de G_1 et de G_2.
Les groupes G_1 et G_2 sont-ils isomorphes ?

Exercice 2. *On considère les trois groupes abéliens*

$$M_1 = \mathbb{Z}/180\mathbb{Z} \times \mathbb{Z}/600\mathbb{Z}$$
$$M_2 = \mathbb{Z}/360\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$$
$$M_3 = \mathbb{Z}/240\mathbb{Z} \times \mathbb{Z}/450\mathbb{Z}$$

Calculer le ordres de M_1, M_2, M_3.
Pourquoi M_3 n'est-il isomorphe ni à M_1, ni à M_2 ?
Montrer que les groupes M_1 et M_2 sont isomorphes.

1 Unicité de la structure des groupes abéliens

Le but de cette partie est d'étudier une preuve de l'unicité.

Soit G un groupe abélien fini noté multiplicativement. Supposons que G est isomorphe à

$$\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$$

avec $d_1/d_2/.../d_n$. Il s'agit de montrer que $d_1, ..., d_n$ sont uniques vérifiant ces propriétés.

Nous noterons $x_1, ..., x_n$ les générateurs de G obtenu canoniquement via l'isomorphisme ci-dessous (les $x_1, x_2, ..., x_n$ correspondent via l'isomorphisme aux éléments $(1, 0, 0, ..., 0), (0, 1, ..., 0), ..., (0, 0, 0, ..., 1)$ de $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$). Pour chaque i, $\langle x_i \rangle$ est un sous-groupe cyclique d'ordre d_i de G et G est isomorphe aux produits directs de ces sous-groupes.

Cas des p-groupes

On montre tout d'abord le résultat pour les p-groupes par récurrence sur l'ordre des groupes. Le résultat est évident pour le groupe trivail. Supposons donc que p est un nombre premier et que G est isomorphe à

$$\mathbb{Z}/p^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/p^{\alpha_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\alpha_n}\mathbb{Z}$$

tel que $1 \leq \alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_n$.

Voici un exemple :

```
p = 3
A = AbelianGroup(5,[p,p,p^2,p^2,p^3],names='xyztu')
x1,x2,x3,x4,x5 = A.gens()
```

Exercice 3. *1. Former l'ensemble E des éléments de A d'ordre p. Combien E a-t-il d'éléments ?*

2. La commande suivante permet de définir le sous-groupe B de A engendré par $x_1, x_2, x_3^p, x_4^p, x_5^{p^2}$.

```
B = A.subgroup([x1,x2,x3^p,x4^p,x5^(p^2)])
```

Calculer son ordre.

3. Vérifier que tous les éléments de E sont dans B. Qu'en déduit-on ?

De manière générale on peut vérifier que l'ensemble

$$H = \{g \in G : g^p = 1\}$$

est le sous-groupe de G engendré par $x_1^{p^{\alpha_1 - 1}}, x_2^{p^{\alpha_2 - 1}}, ..., x_n^{p^{\alpha_n - 1}}$ et est donc isomorphe à $(\mathbb{Z}/p\mathbb{Z})^n$. Ce sous-groupe est donc d'ordre p^n et donc n est uniquement déterminé par G.

Exercice 4. *1. Combien l'ensemble $F = \{a^p : a \in A\}$ a-t-il d'éléments ? (On pourra utiliser la commande* `set` *pour définir F).*

2. Calculer l'ordre du sous-groupe C de A engendré par $x_1^p, x_2^p, x_3^p, x_4^p, x_5^p$.

3. Vérifier que tous les éléments de F sont dans C. Qu'en déduit-on ?

De manière générale on vérifie que l'ensemble

$$G_1 = \{g^p : g \in G\}$$

est le sous-groupe de G engendré par $x_1^p, x_2^p, ..., x_5^p$ et est donc isomorphe à

$$\mathbb{Z}/p^{\alpha_i - 1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\alpha_n - 1}\mathbb{Z}$$

où i est le plus petit indice tel que $\alpha_i \geq 2$. Si G est par ailleurs isomorphe à

$$\mathbb{Z}/p^{\beta_1}\mathbb{Z} \times \mathbb{Z}/p^{\beta_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\beta_n}\mathbb{Z}$$

avec $1 \leq \beta_1 \leq \beta_2 \leq \cdots \leq \beta_n$ alors G_1 est isomorphe à

$$\mathbb{Z}/p^{\beta_j - 1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\beta_n - 1}\mathbb{Z}$$

où j est le plus petit indice tel que $\beta_j \geq 2$. Par hypothèse de récurrence on conclut que $i = j$ et que $\alpha_k = \beta_k$ pour chaque k.

Cas général

Revenons maintenant au cas général d'un groupe abélien fini G isomorphe à

$$\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$$

avec $d_1/d_2/.../d_n$.

Exercice 5. *1. Considérer l'exemple $A = \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/840\mathbb{Z}$ avec pour générateurs x_1, x_2, x_3. Quel est l'exposant de A ?*

2. Déterminer l'ensemble E des éléments d'ordres une puissance de 2. Combien E a-t-il d'éléments ?

3. Calculer l'ordre du sous-groupe B de A engendré par $x_1^3, x_2^{15}, x_3^{105}$?

4. Montrer que tous les éléments de E sont dans B. Qu'en déduit-on ?

Revenons au groupe G. On remarque tout d'abord que d_n est à égal à l'exposant de G. Maintenant pour déterminer les d_i il suffit de déterminer pour chaque nombre premier p divisant d_n et pour chaque i le facteur $p^{\alpha_{i,p}}$ de d_i (c'est-à-dire $d_i = p^{\alpha_{i,p}} d_i'$ avec p ne divisant pas d_i'). Pour chaque p divisant d_n on considère l'ensemble H_p des éléments de G d'ordre une puissance de p. On vérifie alors que H_p est le sous-groupe de G engendré par $x_1^{d_1'}, .., x_n^{d_n'}$ qui est isomorphe à

$$\mathbb{Z}/p^{\alpha_{1,p}}\mathbb{Z} \times \mathbb{Z}/p^{\alpha_{2,p}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\alpha_{n,p}}\mathbb{Z}$$

avec $\alpha_{1,p} \leq \alpha_{2,p}... \leq \alpha_{n,p}$. Par ce qui précède on déduit que tous les $\alpha_{i,p}$ sont uniquement déterminés.

2 Existence de la structure des groupes abéliens

Soit G un groupe abélien fini. Dans cette partie on étudie une preuve de l'existence d'une suite $d_1/d_2/.../d_n$ telle que G est isomorphe à

$$\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}.$$

Un élément d'ordre l'exposant du groupe

Rappelons tout d'abord que l'on peut montrer facilement que G possède toujours un élément d'ordre l'exposant de G. La preuve a été faite en exercice à partir des remarques suivantes :

- Si a et b sont deux éléments de G d'ordre m et n premiers entre-eux alors ab est d'ordre mn.
- Pour tout p^α divisant l'exposant de G il existe a d'ordre kp^α pour un certain k et alors a^k est d'ordre p^α.

Exercice 6. *Soient les permutations $\sigma = (1,6,4,11,8,10)(2,3)(7,9)$ et $\tau = (2,9,3,7)$ de S_{11}. Soit G le groupe engendré par ces deux permutations.*

1. *Vérifier que G est abélien.*
2. *Quel est l'ordre de G ? Quel est son exposant ?*
3. *Soit $\pi = \sigma\tau$. Quel est l'ordre de π ?*
4. *Définir une fonction* `element_ordre_exposant` *qui prend en argument un groupe G et qui retourne un élément d'ordre l'exposant de G s'il existe, qui retourne $False$ sinon.*
5. *Tester cette fonction sur G et sur S_3.*

Morphisme et produit direct

On considère x un élément d'ordre l'exposant de G. Alors $\langle x\rangle$ est un sous-groupe de G. On va montrer qu'alors il existe un sous-groupe K de G tel que G est isomorphe au produit direct de K et $\langle x\rangle$. Alors l'exposant de K divise celui de G et on peut conclure par récurrence sur l'ordre des groupes.

On peut vérifier facilement que l'existence d'un tel K est équivalent à l'existence d'un morphisme ϕ de G sur $\langle x\rangle$ tel que ϕ est égale à l'identité sur $\langle x\rangle$.

On reprend l'exemple de l'exercice précédent et considère H le sous-groupe engendré par π. Un morphisme de G sur H est définit par les images de générateurs de G. (Attention tout choix d'images de générateurs ne permet pas d'étendre une application en un morphisme). Voici un exemple qui envoie π sur π et τ sur π^3. :

```
H = PermutationGroup([pi])
phi = PermutationGroupMorphism_im_gens(G,H,(pi,tau),(pi,pi^3))
phi
```

Exercice 7. *Soit K le noyau de ϕ. Vérifier que G est isomorphe $K \times H$.*

Caractères d'un groupe abélien

Afin de montrer qu'il existe toujours un tel morphisme ϕ, on utilise le prolongement des caractères. Un *caractère* de G est un morphisme de G dans le groupe $(\mathbb{U}, \times)$ des complexes de module 1.

Lemme. *Soient G un groupe abélien fini et H un sous-groupe de G. Si ϕ est un caractère de H alors il existe ψ un caractère de G qui prolonge ϕ.*

Démonstration. On prolonge par récurrence ϕ à G de la façon suivante. Supposons que $H \neq G$. Soit $a \in G \setminus H$ et H_1 le sous-groupe de G engendré par H et a. On considère k le plus petit entier $i > 0$ tel que $a^i \in H$ (il suit que $a^i \in H$ si et seulement si i est multiple de k). On choisit alors $\gamma \in \mathbb{U}$ tel que $\gamma^k = \phi(a^k)$ et on définit ψ de H_1 dans $\mathbb{U}$ par $\psi(a^i h) = \gamma^i \phi(h)$ pour tout i et tout $h \in H$. On vérifie que ψ ets bien définie et que c'est un morphisme de groupe. □

Lemme. *Soient G un groupe abélien fini et x un élément d'ordre l'exposant de G. Posons H le sous-groupe engendré par x. Alors il existe un morphisme ϕ de G vers H qui vaut l'identité sur H.*

Démonstration. Soit m l'exposant de G. On considère l'isomorphisme ψ de H vers $\mathbb{U}$ qui envoie x sur $e^{2i\pi/m}$. Ce caractère se prolonge en caractère de G qui est à valeur dans $\mathbb{U}_m$ car tous les éléments de G sont d'ordre divisant m. On obtient ϕ en composant ce caractère par ψ^{-1}. □

Exercice 8. *Soient les permutations $\sigma = (2,6,11)(3,8,9,5)$, $\tau = (1,7,10,4)(2,11,6)(3,9)(5,8)$ et $\pi = (1,10)(4,7)(12,13,14)$ de S_{14} ; Soit G le sous-groupe de S_{14} engendré par les permutations.*

1. *Vérifier que G est abélien. Quels sont l'ordre et l'exposant de G.*
2. *Vérifier que σ est d'ordre l'exposant de G.*
3. *Soit H le sous-groupe engendré par σ et H_1 le sous-groupe engendré par σ et τ. Définir un morphisme $\phi_1$de H_1 vers H qui prolonge l'identité sur H.*
4. *Définir un morphisme ϕ qui prolonge ϕ_1 à G. Vérifier que son noyau est cyclique. En déduire que G est isomorphe à $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.*

Exercice 9. *Ecrire un programme qui prend en entrée un groupe de permutations et qui donne ses facteurs invariants si ce groupe est abélien.*