Exposant d'un groupe :

I Le développement

Le but de ce développement est de redémontrer les propriétés classiques sur l'exposant d'un groupe et d'en déduire un résultat sur les sous-groupes de $\mathbb{K}^\times$ ($\mathbb{K}$ étant un corps commutatif quelconque).

Dans tout ce développement, on considère un groupe $(G,*)$ de neutre noté e_G.

Lemme 1 : [Berhuy, p.344]
Si G est un groupe d'exposant fini, alors $\exp(G) = \text{PPCM}(\{o(x),\ x \in G\})$.
De plus, si G est fini, on a $\exp(G)$ qui divise $\text{Card}(G)$.

Preuve :
$*$ On suppose que G est d'exposant fini.
Pour tout $m \in \mathbb{Z}$, on a :

$$(\forall x \in G,\ x^m = e_G) \iff (\forall x \in G,\ o(x)|m) \iff (\text{PPCM}(\{o(x),\ x \in G\})|m)$$

Or, puisque G est d'exposant fini, la première équation admet au moins une solution strictement positive et les équivalentes précédentes montrent que la plus petite solution strictement positive est alors $\text{PPCM}(\{o(x),\ x \in G\})$.
Donc par définition de l'exposant, on a $\exp(G) = \text{PPCM}(\{o(x),\ x \in G\})$.

$*$ Si de plus G est fini, alors $\text{Card}(G)$ est solution de l'équation précédente, donc on a $\exp(G)$ qui divise $\text{Card}(G)$.

■

Exemple 2 : [Berhuy, p.345]
$*$ Si G est cyclique d'ordre n, alors $\exp(G) = n$.
En effet, on a $\exp(G)$ qui divise n par le lemme précédent et d'autre part, G possède un élément d'ordre n (car cyclique), donc n divise $\exp(G)$ (par définition du PPCM). D'où l'égalité $\exp(G) = n$.

$*$ On a $\exp(D_8) = 4$ puisque les ordres des rotations dans D_8 sont 1,2 ou 4 et que l'ordre des symétries dans D_4 est égal à 2.

$*$ $\exp(\mathfrak{S}_3) = 6$ puisque les éléments de $\mathfrak{S}_3$ sont d'ordre 1,2 ou 3.

Proposition 3 : [Berhuy, p.345]
Si G est un groupe abélien d'exposant fini, alors il existe un élément $x \in G$ d'ordre $\exp(G)$.

Preuve :
On suppose que G est un groupe abélien d'exposant fini.
Écrivons $\exp(G) = \text{PPCM}(\{o(x),\ x \in G\}) = \prod_{i=1}^{r} p_i^{m_i}$ (décomposition en facteurs premiers).

Soit $i \in [\![1;r]\!]$.
Il existe un élément $x_i \in G$ tel que $p_i^{m_i}$ divise $o(x_i)$. En effet, dans le cas contraire, pour tout élément $x \in G$, la plus grande puissance de p_i divisant $o(x)$ serait au plus $p_i^{m_i-1}$. Mais dans ce cas, la puissance de p_i dans la décomposition de $\exp(G)$ serait strictement inférieure à m_i et on aboutit à une contradiction.

Soit $i \in [\![1;r]\!]$.
On choisit $x_i \in G$ un élément tel que $p_i^{m_i}$ divise $o(x_i)$ et écrivons $o(x_i) = p_i^{m_i} q_i$ (décomposition en facteurs premiers). On a alors $o\left(x_i^{q_i}\right) = p_i^{m_i}$ (car p_i et q_i sont premier entre eux) et puisque G est abélien, on a $o\left(x_1^{q_1}...x_r^{q_r}\right) = \prod_{i=1}^{r} p_i^{m_i} = \exp(G)$.

Ainsi, il existe un élément de G d'ordre $\exp(G)$.

■

Corollaire 4 : [Berhuy, p.345]
Si G est un groupe abélien fini, alors on a l'équivalence :

$$(\exp(G) = \text{Card}(G)) \iff (G \text{ cyclique})$$

Preuve :
On suppose que G est un groupe abélien fini.
$*$ Si G est cyclique, alors l'exemple précédent montre que l'on a $\exp(G) = \text{Card}(G)$.

$*$ Réciproquement, supposons que $\exp(G) = \text{Card}(G)$.
Puisque G est fini il est aussi d'exposant fini et comme il est abélien (par hypothèse) on a par la proposition précédente qu'il existe un élément $x \in G$ d'ordre $\exp(G) = \text{Card}(G)$.
Donc on a $< x > \subseteq G$ et $\text{Card}(< x >) = \text{Card}(G)$, d'où $G =< x >$ et le fait que G est cyclique.

On a ainsi démontré l'équivalence voulue.

■

Remarque 5 : [Berhuy, p.346]
L'exemple de $\mathfrak{S}_3$ montre que les deux résultats précédents sont faux si G n'est pas supposé abélien. En effet, on avait $\exp(\mathfrak{S}_3) = \text{Card}(\mathfrak{S}_3) = 6$ alors que $\mathfrak{S}_3$ ne contient pas d'élément d'ordre 6 et n'est pas cyclique (par la classification des petits groupes).

Théorème 6 : [Berhuy, p.346]
Soit $\mathbb{K}$ un corps commutatif quelconque.
Tout sous-groupe fini de $\mathbb{K}^\times$ est cyclique.

Preuve :
Soit G un sous-groupe fini de $\mathbb{K}^\times$.
On a que G est abélien et on note $e = \exp(G)$.
Ainsi, pour tout $x \in G$, $x^e = 1_\mathbb{K}$ et puisque le polynôme $X^e - 1_\mathbb{K} \in \mathbb{K}[X]$ est de degré e, il possède au plus e racines dans $\mathbb{K}$.
D'autre part, d'après la proposition précédente, il existe un élément $x_0 \in G$ d'ordre e. Et puisque $< x_0 > \subseteq G$ et que $\text{Card}(G) \leq e$, on en déduit finalement que $\text{Card}(G) = e$ et donc que $G =< x_0 >$.

Ainsi, tout sous-groupe fini de $\mathbb{K}^\times$ est cyclique.

■

Remarque 7 : [Berhuy, p.346]
$*$ En particulier, on en déduit que tout sous-groupe de $\mathbb{F}_q^\times$ est cyclique (avec $q = p^n$ où p est un nombre premier et n un entier naturel non nul) puisque $\mathbb{F}_q$ est un corps.
$*$ Si p est un nombre premier, on a alors que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique car les $\mathbb{Z}/p\mathbb{Z}$ sont des corps et puisqu'ils sont finis donc on peut appliquer le théorème précédent avec le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ tout entier.

II Remarques sur le développement

II.1 Résultat(s) utilisé(s)

On a utilisé ici la notion d'exposant dont on rappelle la définition :

Définition 8 : Groupe d'exposant fini [Berhuy, p.344] :
On dit que G est **d'exposant fini** lorsqu'il existe un entier $n \in \mathbb{N}^*$ tel que pour tout $x \in G$, $x^n = e_G$. Dans ce cas, on appelle **exposant de** G le plus petit entier $n \in \mathbb{N}^*$ vérifiant cette propriété et on le note $\exp(G)$.

On rappelle également quelques résultats sur l'ordre d'un élément dans un groupe :

Proposition 9 : [Berhuy, p.151]
Si G est d'ordre $n \in \mathbb{N}^*$, alors pour tout $x \in G$, $x^n = e_G$.

Corollaire 10 : [Berhuy, p.151]
Soit $x \in G$.
$*$ Pour tout $d \in \mathbb{N}^*$, l'élément x^d est d'ordre fini et on a : $o\left(x^d\right) = \frac{o(x)}{\text{PGCD}(d, o(x))}$.
En particulier :
- Si d divise $o(x)$, alors $o\left(x^d\right) = \frac{o(x)}{d}$.
- Si d et $o(x)$ sont premiers entre eux, alors $o\left(x^d\right) = o(x)$.

Proposition 11 : [Berhuy, p.151]
Soient $x, y \in G$ d'ordre fini.
Si x et y commutent, alors xy est d'ordre fini.
De plus, on a les propriétés suivantes :
- Si $< x > \cap < y >= e_G$, alors $o(xy) = \text{PPCM}(o(x), o(y))$.
- Si $o(x)$ et $o(y)$ sont premiers entre eux, alors $o(xy) = o(x)o(y)$.

II.2 Pour aller plus loin...

Il existe des groupes infinis dont les éléments sont tous d'ordre fini ($\mathbb{Q}/\mathbb{Z}$ par exemple) mais sans qu'il soit d'exposant fini.

De même, un groupe d'exposant fini n'est pas forcément fini comme le montre l'exemple de $(\mathbb{Z}/2\mathbb{Z})^\mathbb{N}$. Cependant, on a une réciproque partielle avec le théorème de Burnside :

Théorème 12 : Théorème de Burnside [Francinou, p.353] :
Soit H un sous-groupe de $\text{GL}_n(\mathbb{C})$.
Si H est d'exposant fini, alors il est fini.

II.3 Recasages

Recasages : 104 - 142.

III Bibliographie

— Grégory Berhuy, *Algèbre : le grand combat*.

— Serge Francinou, *Exercices de mathématiques, Oraux X-ENS, Algèbre 2*.