Chapitre 2

Groupes finis

Dans toute la suite du cours, on désigne par $\#E$ le nombre des éléments d'un ensemble fini E. Si G est un groupe fini, on rappelle que l'entier $\#G$ est appelé **ordre** de G.

2.1 Les groupes quotients $\mathbb{Z}/n\mathbb{Z}$

Définition 2.1 *Soit n un entier positif. On dit que deux entiers a et b sont* ***congrus modulo*** *n si leur différence $(b-a)$ est multiple de n, c'est à dire si $(b-a) \in n\mathbb{Z}$. Cette relation est notée*

$$a \equiv b \pmod{n}.$$

La notion de congruence modulo n a été introduite par Gauss.

Proposition 2.1 *Soit n un entier positif. La congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$. Soit $a \in \mathbb{Z}$, la classe d'équivalence $\overline{a}$ de a modulo n est appelée* ***classe de a modulo*** *n, et on a*

$$\overline{a} = \{a + nk \mid k \in \mathbb{Z}\}.$$

Preuve : On retrouve la relation d'équivalence associée au sous-groupe $n\mathbb{Z}$. (Cf. page 12). □

Proposition 2.2 *Soit n un entier positif et soit $a \in \mathbb{Z}$. Le reste r de la division euclidienne de a par n est le seul entier vérifiant*

$$(1) \qquad \begin{cases} r \equiv a \pmod{n}, \\ 0 \leq r < n. \end{cases}$$

Il en résulte que deux entiers a et b sont congrus modulo n si et seulement si le reste de la division euclidienne de a par n est égal au reste de la division euclidienne de b par n.

Preuve : Il est clair que $r \equiv a \pmod{n}$. Soit r_1 un entier vérifiant (1), alors $r - r_1$ est multiple de n et $|r - r_1| < n$, ce qui montre que $r - r_1 = 0$. □

Rappelons que l'addition du groupe quotient $\mathbb{Z}/n\mathbb{Z}$ est définie, si a et b sont deux entiers, par

$$\overline{a} + \overline{b} = \overline{a+b}.$$

Proposition 2.3 *Le groupe $\mathbb{Z}/n\mathbb{Z}$ est d'ordre n, plus précisément, on a*

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{(n-1)}\}.$$

Preuve : Soit $a \in \mathbb{Z}$, il résulte de la proposition 2.2 que $\overline{a} \in \{\overline{0}, \overline{1}, \ldots, \overline{(n-1)}\}$ et que les classes $\overline{0}$, $\overline{1}$, ..., $\overline{(n-1)}$ sont toutes distinctes. On remarque que $\overline{n} = \overline{0}$, $\overline{(n+1)} = \overline{1}$, etc. □

Proposition 2.4 *Le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique (additif), engendré par $\overline{1}$.*

Preuve : Conséquence directe de la définition de l'addition de $\mathbb{Z}/n\mathbb{Z}$. □

2.2 Généralités sur les groupes finis

Du théorème 0.11 (page 12), on déduit une propriété essentielle des groupes finis :

Théorème 2.5 (Lagrange) *Dans un groupe fini, l'ordre d'un sous-groupe divise l'ordre du groupe.*

Preuve : Soit G un groupe fini et H un sous-groupe de G. On sait d'après le théorème 0.11 (page 12) que les classes d'équivalence modulo H possèdent toutes le même nombre d'éléments que H et constituent une partition de G. L'ensemble G étant fini, il n'y a qu'un nombre fini m de classes, on en déduit que l'ordre de G est égal à m fois l'ordre de H. □

L'étude d'un groupe comporte l'étude de tous ses sous-groupes, le théorème précédent permet de cerner la recherche des sous-groupes, un groupe d'ordre 8 par exemple ne possédera pas de sous-groupe d'ordre 3, 5 ou 7. De même qu'un groupe d'ordre premier ne possédera que ses deux sous-groupes triviaux.

Définition 2.2 *Soit G un groupe fini et soit $x \in G$. On appelle* ***ordre de*** *x l'ordre du sous-groupe $\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$ de G engendré par x.*

Notons que le seul élément de G d'ordre 1 est l'unité 1.

Théorème 2.6 *Soit G un groupe fini, soit $x \in G$ et soit m l'ordre de x. Alors*

1. *m divise l'ordre de G.*
2. *m est le plus petit entier positif tel que $x^m = 1$.*
3. *Les éléments $1, x, x^2, \ldots, x^{m-1}$ sont tous distincts dans G.*
4. *$\langle x \rangle = \{1, x, x^2, \ldots, x^{m-1}\}$.*

Preuve :

1. Résulte du théorème de Lagrange.
2. Si $m = 1$, c'est évident. On suppose $m \geq 2$, la démonstration se fait en deux étapes.
   (a) On montre qu'il existe au moins un entier ℓ, $1 \leq \ell \leq m$ tel que $x^\ell = 1$.

   Soit $$A = \{x, x^2, \ldots, x^m, x^{m+1}\} \subseteq \langle x \rangle,$$

   comme l'ordre de $\langle x \rangle$ est égal à m, il existe au moins deux éléments égaux dans A,

   $$\exists k,\ \exists \ell,\ \ 1 \leq k \leq m,\ \ 1 \leq k + \ell \leq m+1 \text{ vérifiant } x^k = x^{k+\ell},$$

   on en déduit $$1 \leq \ell \leq m \quad \text{et} \quad x^\ell = 1.$$

   (b) Soit n le plus petit entier positif tel que $x^n = 1$, il résulte de (a) que $(n \leq \ell \leq m)$. Montrons que $\langle x \rangle \subseteq \{1, x, x^2, \ldots, x^{n-1}\}$. Soit en effet $k \in \mathbb{Z}$, la division euclidienne de k par n s'écrit $k = nq + r$, $\ 0 \leq r \leq n-1$, ce qui donne

   $$x^k = x^{nq}x^r = (x^n)^q x^r = 1^q x^r = x^r \in \{1, x, x^2, \ldots, x^{n-1}\},$$

   il en résulte $m = \#\langle x \rangle \leq \#\{1, x, x^2, \ldots, x^{n-1}\} \leq n$, c'est-à-dire , en vertu de (a),

   $$m = \#\langle x \rangle = \#\{1, x, x^2, \ldots, x^{m-1}\} = n.$$

   Cela démontre 2. et 4.
3. Résulte de l'égalité $m = \#\{1, x, x^2, \ldots, x^{m-1}\}$. □

Il découle du théorème 2.6 un chapelet de corollaires tous aussi importants les uns que les autres.

Corollaire 2.7 *Soit G un groupe fini d'ordre n, alors on a $x^n = 1$ pour tout $x \in G$.*

Preuve : Soit m l'ordre de x, et soit $k \geq 1$ l'entier tel que $n = mk$, alors

$$x^n = x^{mk} = (x^m)^k = 1^k = 1. \qquad \square$$

Corollaire 2.8 *Tout groupe fini G d'ordre premier p est cyclique et engendré par l'un quelconque de ses éléments distincts de 1.*

Preuve : Soit $x \in G$, $x \neq 1$. Comme $x \in \langle x \rangle$ et $1 \in \langle x \rangle$, l'ordre m de x est ≥ 2 et divise p, d'où $m = p$, c'est-à-dire $\langle x \rangle = G$. $\square$

Corollaire 2.9 *Soit G un groupe d'ordre n. Pour chaque entier positif k, soit $\alpha_G(k)$ le nombre des éléments d'ordre k de G, alors on a*

$$n = \sum_{d/n} \alpha_G(d).$$

Preuve : On sait que si k ne divise pas n, on a $\alpha_G(k) = 0$. Si d divise n, soit $\Omega_G(d)$ l'ensemble des éléments d'ordre d de G, alors $\alpha_G(d) = \#\Omega_G(d)$ et tout élément de G appartient à un $\Omega_G(d)$ et un seul. $\square$

Le théorème suivant est très utile pour déterminer l'ordre des éléments d'un groupe fini.

Théorème 2.10 *Soit G un groupe fini, soit $x \in G$ et soit m l'ordre de x.*

1. *Pour tout entier positif q, on a l'équivalence*

$$\boxed{(x^q = 1) \iff (m \text{ divise } q).}$$

2. *Pour tout entier positif k,*

$$\boxed{x^k \text{ est d'ordre } m/d, \text{ où } d = \operatorname{pgcd}(m,k).}$$

Preuve :

1. Si m divise q, posons $q = mq'$, alors

$$x^q = x^{mq'} = (x^m)^{q'} = 1^{q'} = 1.$$

   Réciproquement, si $x^q = 1$, soit $q = mq' + r$, $0 \leq r < m$, la division euclidienne de q par m. Alors

$$1 = x^q = x^{mq'+r} = x^{mq'}x^r = x^r.$$

   On déduit du point 2. du théorème 2.6 (page 32) que $r = 0$.

2. On écrit $m = dm'$ et $k = dk'$, de sorte que $\operatorname{pgcd}(m', k') = 1$.

   Soit α l'ordre de x^k, de l'égalité $(x^k)^\alpha = x^{k\alpha} = 1$, on déduit que m divise $k\alpha$, c'est-à-dire dm' divise $dk'\alpha$, d'où m' divise $k'\alpha$ et m' divise α d'après le lemme de Gauss.

   Réciproquement, $(x^k)^{m'} = x^{km'} = x^{dk'm'} = x^{mk'} = (x^m)^{k'} = 1$, donc α divise m' et finalement $\alpha = m'$. $\square$

Attention Bien comprendre le point 1. du théorème 2.10 : si $x \in G$ et si q est un entier > 1,

l'égalité $(x^q = 1)$ n'implique pas que x est d'ordre q
mais seulement que **l'ordre de x divise q.**

En particulier, soit G un groupe d'ordre n ; d'après le corollaire 2.7 ci-dessus, *tous les éléments* de G vérifient $x^n = 1$, mais ces éléments ne sont pas tous *d'ordre n*. Mieux, si G n'est pas cyclique, *aucun* de ses éléments n'est d'ordre n.
L'important corollaire suivant résulte du point 2. du théorème 2.10.

Corollaire 2.11 *Soit G un groupe fini, soit $x \in G$ et soit k un entier positif.*
L'ordre de x^k est égal à l'ordre de x si et seulement si k est premier avec l'ordre de x.

Exercice 20 — Soit G un groupe fini *commutatif* et soit x et y deux éléments de G, d'ordres respectifs p et q. Montrer que

1. Si p et q sont premiers entre eux, le produit $z = xy$ est d'ordre pq et le sous-groupe de G engendré par z contient x et y.
2. Il existe un élément $t \in G$ dont l'ordre est égal au ppcm de p et q.

2.3 Groupes cycliques et indicatrice d'Euler

On rappelle qu'un groupe G est cyclique s'il est fini et s'il existe un élément $g \in G$, appelé générateur de G, tel que $G = \langle g \rangle$, ce qui équivaut à l'égalité

$$(\text{ordre de } g) = (\text{ordre de } G).$$

On rappelle également que *tout groupe cyclique est commutatif.*
L'énoncé suivant est une conséquence directe du théorème 2.6 (page 32).

Théorème 2.12 *Soit G un groupe cyclique d'ordre n, et soit $g \in G$ un générateur de G.*

1. *g est d'ordre n.*
2. *Tous les éléments g^k sont distincts pour $k = 0, 1, \ldots, n-1$.*
3. *$G = \{g^k \mid k \geq 0\} = \{1, g, \ldots, g^{n-1}\}$.*
4. *En notation additive, cela s'écrit $G = \{kg \mid k \geq 0\} = \{0, g, \ldots, (n-1)g\}$.*

Corollaire 2.13 *Deux groupes cycliques de même ordre sont isomorphes.*

Preuve : Soit G_1 et G_2 deux groupes cycliques d'ordre n, de générateurs respectifs g_1 et g_2. L'application u de G_1 sur G_2 définie par

$$\forall k \geq 0, \quad \begin{cases} u(g_1^k) = g_2^k & \text{si } G_1 \text{ et } G_2 \text{ sont multiplicatifs,} \\ u(kg_1) = kg_2 & \text{si } G_1 \text{ et } G_2 \text{ sont additifs,} \\ u(kg_1) = g_2^k & \text{si } G_1 \text{ est additif et } G_2 \text{ multiplicatif,} \end{cases}$$

est un isomorphisme de G_1 sur G_2. $\square$

Corollaire 2.14 *Tout groupe cyclique d'ordre $n \geq 1$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Preuve : On a vu, proposition 2.4 page 31, que le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n. $\square$

Exercice 21 — Montrer que les groupes $\mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ sont commutatifs, d'ordre 4, mais non isomorphes.

Définition 2.3 ***Indicatrice d'Euler*** *(Leonhard Euler, 1707-1783) Soit n un entier positif, l'indicatrice d'Euler de n, notée $\varphi(n)$, est définie comme étant égale au nombre des entiers k vérifiant*

$$(1) \qquad (1 \leq k \leq n) \ \textit{et} \ (\text{pgcd}\,(k,n) = 1).$$

Notons que pour tout entier positif n, on a $\text{pgcd}\,(1,n) = 1$, ce qui fait que $\varphi(n) \geq 1$.

Exemples

1. Il est clair que $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$. Etc.
2. Si $n = 10$, les entiers vérifiant (1) sont 1, 3, 7 et 9, il y en a 4, donc $\varphi(10) = 4$. Remarquons que $\varphi(9) = 6$, la fonction φ n'est pas croissante.

Nous verrons plus loin (page 41), que l'indicatrice d'Euler $\varphi(n)$ se calcule à partir de la décomposition de l'entier n en facteurs premiers. La première étape est le résultat suivant.

Proposition 2.15 *Soit p un nombre premier. Pour tout entier positif n, on a*

$$\varphi(p^n) = p^n - p^{n-1} = (p-1)p^{n-1} = p^n\left(1 - \frac{1}{p}\right).$$

En particulier, $\varphi(p^n)$ est pair dès que $p > 2$.

Preuve : Parmi les p^n entiers k tels que $1 \leq k \leq p^n$, il y a p^{n-1} multiples de p, les autres sont premiers avec p d'après la proposition 1.11 (page 25). □

Théorème 2.16 *Un groupe cyclique G d'ordre n possède $\varphi(n)$ générateurs distincts. Plus précisément, si g est un générateur de G, les $\varphi(n)$ générateurs de G sont les éléments g^k, où $1 \leq k \leq n$ et $\text{pgcd}\,(n,k) = 1$.*

Preuve : Il résulte du théorème 2.12 (page 34) que tous les éléments g^k sont distincts pour $1 \leq k \leq n$, puis du corollaire 2.11 (page 34) que si $k \geq 1$, g^k est générateur de G si et seulement si $\text{pgcd}\,(k,n) = 1$. □

Transcrit en notation additive, le théorème précédent permet de déterminer les générateurs du groupe (additif) $\mathbb{Z}/n\mathbb{Z}$.

Corollaire 2.17 (Générateurs de $\mathbb{Z}/n\mathbb{Z}$) *Les $\varphi(n)$ générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$ sont les classe $\overline{k}$ modulo n, où $1 \leq k \leq n$ et $\text{pgcd}\,(k,n) = 1$.*

Preuve : Résulte du fait que $\overline{1}$ est générateur $\mathbb{Z}/n\mathbb{Z}$. □

Théorème 2.18 *Soit G un groupe cyclique d'ordre n. Pour chaque diviseur d de n, l'ensemble*

$$U_d = \{x \in G \mid x^d = 1\}$$

est un sous-groupe d'ordre d de G. C'est le seul sous-groupe d'ordre d de G. Ce sous-groupe est cyclique. Il en résulte que G possède exactement $\varphi(d)$ éléments d'ordre d, et que tout sous-groupe d'un groupe cyclique est cyclique.

Preuve : Le groupe G étant commutatif, U_d est un sous-groupe de G. Il résulte ensuite du corollaire 2.7 (page 33) que tout sous-groupe d'ordre d de G est contenu dans U_d.
Posons $n = dn'$ et soit g un générateur de G, on a l'équivalence, pour tout entier $k \geq 1$,

$$\left((g^k)^d = g^{kd} = 1\right) \iff (kd \text{ est multiple de } n = dn') \iff (k \text{ est multiple de } n').$$

Les éléments de U_d sont donc $g^{n'}$, $g^{2n'}, \ldots, g^{dn'} = g^n = 1$.
Ces éléments sont tous distincts car $in' \leq n$ pour tout $i = 1, \ldots, d$.
Le sous-groupe U_d est donc cyclique d'ordre d, engendré par $g^{n'}$, il possède par conséquent $\varphi(d)$ générateurs qui sont les seuls éléments d'ordre d de U_d donc de G.
D'après le corollaire 2.11 (page 34), ces éléments sont les $g^{n'k}$, où k est premier avec d. □

Exercice 22 — Déterminer les éléments d'ordre 8 du groupe $\mathbb{Z}/32\,\mathbb{Z}$.

Exercice 23 — **Contrexemple** Soit G le groupe (additif) $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$.

1. Quel est l'ordre de G?
2. Déterminer $U_3 = \{x \in G \mid 3x = 0\}$.
3. Déterminer l'ensemble des éléments d'ordre 3 de G. En déduire que les conclusions du théorème 2.18 ci-dessus ne s'appliquent pas à un groupe non cyclique, même s'il est commutatif.

Corollaire 2.19 *Pour chaque entier positif n, on a*

$$(1) \qquad n = \sum_{d/n} \varphi(d).$$

Preuve : Résulte du théorème 2.18 appliqué au groupe $\mathbb{Z}/n\mathbb{Z}$, et du corollaire 2.9 (page 33). □

Le théorème suivant donne une **caractérisation** très pratique des groupes cycliques, dont nous ferons usage au chapitre 5.

Théorème 2.20 *Soit G un groupe d'ordre n. Pour chaque diviseur d de n, soit*

$$\begin{cases} U_d = \{x \in G \mid x^d = 1\}, \\ \alpha_G(d) \textit{ le nombre d'éléments d'ordre } d \textit{ de } G. \end{cases}$$

Les conditions suivantes sont équivalentes.

1. *Pour chaque diviseur d de n, $\#U_d \leq d$.*
2. *Pour chaque diviseur d de n, $\alpha_G(d) \leq \varphi(d)$.*
3. *Pour chaque diviseur d de n, $\alpha_G(d) = \varphi(d)$.*
4. *G est cyclique.*
5. *Pour chaque diviseur d de n, $\#U_d = d$.*

Preuve : Notons que si G n'est pas commutatif, U_d n'est pas nécessairement un sous-groupe.
$1 \Longrightarrow 2$. Si $\alpha_G(d) \geq 1$, il existe un élément $x \in G$ d'ordre d, donc $x \in U_d$, et il résulte du théorème 2.7 (page 33) que $\langle x \rangle \subseteq U_d$, d'où $\#\langle x \rangle = d \leq \#U_d$. Sous l'hypothèse 1., on en déduit $d = \#U_d$, donc $\langle x \rangle = U_d$.
Le sous-groupe $\langle x \rangle$ possède $\varphi(d)$ générateurs d'après le théorème 2.16 (page 35), et l'égalité $\langle x \rangle = U_d$ implique que ce sont les seuls éléments d'ordre d de G. On en déduit $\alpha_G(d) = \varphi(d)$.
Autrement dit, ou bien $\alpha_G(d) = 0$ ou bien $\alpha_G(d) = \varphi(d)$, d'où $\alpha_G(d) \leq \varphi(d)$.
$2 \Longrightarrow 3$. Le corollaire 2.9 (page 33) et le corollaire 2.19 ci-dessus impliquent l'égalité

$$n = \sum_{d/n} \alpha_G(d) = \sum_{d/n} \varphi(d).$$

De cette égalité et de la condition 2., on déduit que pour tout diviseur d de n, on a

$$\alpha_G(d) = \varphi(d).$$

$3 \Longrightarrow 4$. Pour $d = n$, on déduit de 3. que $\alpha_G(n) = \varphi(n) \geq 1$, le groupe G possède donc un élément d'ordre n, il est cyclique.
$4 \Longrightarrow 5$. C'est le théorème 2.18 (page 35).
$5 \Longrightarrow 1$. Évident. □