Chapitre 1

Groupes monogènes. Groupes cycliques. Exemples

Pré-requis

1. Généralités sur les groupes.
2. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
3. Théorème de Lagrange pour les groupes.
4. Définition d'un nombre premier.
5. P.G.C.D. de deux entiers naturels.
6. Lemme de Gauss en arithmétique.
7. Notion de corps.

1.1 Groupes monogènes

Définition 1. Soit $(G, .)$ un groupe. $(G, .)$ est dit monogène s'il existe un élément x tel que pour tout élément y de $(G, .)$, il existe un entier relatif k tel que $y = x^k$. On note alors $G = \langle x \rangle$ et l'on dit que $(G, .)$ est engendré par x ou encore que x est un générateur de $(G, .)$. Si de plus, $(G, .)$ est d'ordre fini, on dit que $(G, .)$ est cyclique.

Exemples. 1. $(\mathbb{Z}, +)$ est monogène infini engendré par 1 ou -1.

2. Pour tout entier naturel non nul n, $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique d'ordre n.

3. Pour tout entier naturel non nul n, $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ est un groupe cyclique d'ordre $n-1$.

4. Pour tout entier naturel non nul n, $\left(\mathbb{U}_n = \left\{e^{\frac{2ik\pi}{n}},\, k \in [\![0; n-1]\!]\right\}, \times\right)$ est un groupe cyclique d'ordre n.

Remarque. Tout groupe monogène est abélien. Attention, la réciproque est fausse : le groupe de Klein est abélien mais non cyclique.

Définition 2. Soit $(G,.)$ un groupe fini. Soit a un élément de G. On appelle ordre de a l'ordre du sous-groupe $\langle a\rangle = \{a^k,\ k \in \mathbb{Z}\}$ engendré par a.

Théorème 3. *Soit $(G,.)$ un groupe fini. Soit a un élément de G. Soit m l'ordre de a. Alors :*

1. *m divise l'ordre de G.*
2. *m est le plus petit entier naturel non nul tel que $a^m = 1$.*
3. *Les éléments 1, a, a^2, ..., a^{m-1} sont tous distincts dans G. De plus, $\langle a\rangle = \{1; a; a^2; ...; a^{m-1}\}$.*

Démonstration. 1. C'est le théorème de Lagrange.

2. Si $m = 1$, c'est évident. Si $m \geqslant 2$. On démontre que $A = \{a; a^2; a^3; ...; a^{m+1}\}$ possède au moins deux éléments égaux. Ainsi, il existe un entier l compris entre 1 et m tel que $a^l = 1$. Soit $s = \min\{k \in \mathbb{N}^*,\ a^k = 1\}$. On a $s \leqslant m$. Soit $k \in \mathbb{Z}$. On a $k = sq + r$ avec $0 \leqslant r \leqslant s-1$ donc $a^k = a^r$ et par conséquent $a^k \in \{1; a; a^2; ...; a^{s-1}\}$. Ainsi, $\langle a\rangle \subset \{1; a; ...; a^{s-1}\}$ et $m \leqslant s$. D'où $m = s$.

3. $\{1; a; ...; a^{m-1}\} \subset \langle a\rangle$ est évident. De plus, $|\langle a\rangle| = m$, d'où l'égalité. □

Corollaire 4. *Soit $n \in \mathbb{N}$. Soit $(G,.)$ un groupe fini d'ordre n. Alors, pour tout $x \in G$, $x^n = 1$.*

Démonstration. Soit m l'ordre de x. D'après le théorème 3, m divise n. Donc il existe un entier relatif k tel que $n = mk$. D'où $x^n = x^{mk} = (x^m)^k = 1^k = 1$. □

Corollaire 5. *Tout groupe $(G,.)$ d'ordre p premier est cyclique et engendré par l'un quelconque de ses éléments distincts de 1.*

Démonstration. Soit a un élément de G distinct de 1. Alors 1 et a appartiennent à $\langle a\rangle$. Donc $|\langle a\rangle| \geqslant 2$. De plus, $|\langle a\rangle|$ divise p d'après 1. du théorème 3. p étant premier, nécessairement $|\langle a\rangle| = p$ et par conséquent $G = \langle a\rangle$. □

Corollaire 6. *Soit $(G,.)$ un groupe fini. Soit $a \in G$. Soit m l'ordre de a. Alors pour tout entier naturel k, $\left(a^k = 1\right) \Leftrightarrow (m|k)$.*

Démonstration. $\Leftarrow$: Il existe un entier relatif k' tel que $k = mk'$. Ainsi, d'après le théorème 3 :

$$a^k = a^{mk'} = (a^m)^{k'} = 1^{k'} = 1$$

$\Rightarrow$: Division euclidienne de k par m : $k = mq + r$ avec $0 \leqslant r < m$. D'où :

$$a^k = a^{mq+r} = a^{mq}a^r = a^r = 1$$

Ce qui entraîne $r = 0$ d'après le théorème 3. Ainsi, $m|k$. □

Remarque. Attention, $a^k = 1$ n'implique pas que k est l'ordre de a mais simplement que l'ordre de a divise k.

Théorème 7. *1. Tout groupe monogène infini est isomorphe au groupe $(\mathbb{Z}, +)$.*
2. Tout groupe cyclique d'ordre $n \in \mathbb{N}^*$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Démonstration. 1. Soit $(G, .)$ est un groupe monogène infini engendré par un élément g. Considérons l'application $f : (\mathbb{Z}, +) \to (G, .)$ définie par $f(k) \coloneqq g^k$. Il est clair que f est un morphisme. De plus $(G, .)$ étant monogène engendré par g, par définition, pour tout élément x de G, il existe un entier relatif k tel que $x = g^k$. Ainsi f est donc un épimorphisme. Enfin, si $g^r = g^s$, alors $g^{r-s} = 1$ et par conséquent $r = s$, ce qui prouve que f est un monomorphisme. f est donc un isomorphisme.

2. Soit $(G, .)$ un groupe cyclique d'ordre n engendré par g.

Considérons $f : (\mathbb{Z}/n\mathbb{Z}, +) \to (G, .)$ définie par $f(\overline{k}) \coloneqq g^k$. Alors f est clairement un isomorphisme. □

1.2 Sous-groupes d'un groupe monogène

1.2.1 D'un groupe monogène infini

Proposition 8. *Soit $(G, .)$ un groupe monogène infini. Si $(H, .)$ est un sous-groupe de $(G, .)$, alors il existe un entier naturel n tel que $(H, .)$ est isomorphe à $(n\mathbb{Z}, +)$.*

Démonstration. Soit $(G, .)$ un groupe monogène infini. Alors, d'après le théorème 7, il est isomorphe à $(\mathbb{Z}, +)$. Soit $(H, +)$ un sous-groupe de $(\mathbb{Z}, +)$. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Sinon, il existe un élément strictement positif dans H. Soit m le plus petit des éléments strictement positifs de H. Comme $m \in H$, naturellement, $m\mathbb{Z} \subset H$. Soit $h \in H$. Effectuons la division euclidienne de h par m : il existe un entier relatif q et un entier naturel r tels que :

$$\begin{cases} h = mq + r \\ 0 \leqslant r < m \end{cases}$$

Or, $r = h - mq \in H$. Comme $r < m$, alors nécessairement, $r = 0$. D'où $h = mq \in m\mathbb{Z}$. Ainsi, $H \subset m\mathbb{Z}$. □

1.2.2 D'un groupe cyclique

Définition 9. On appelle fonction indicatrice d'Euler la fonction définie sur $\mathbb{N}^*$ à valeurs dans $\mathbb{N}$ qui, à chaque entier naturel non nul n, associe le nombre d'entiers compris entre 1 et n premiers avec n.

Exemples. On a : $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$ et $\varphi(8) = 4$.

Remarque. La fonction indicatrice d'Euler n'est pas croissante sur $\mathbb{N}^*$ car $\varphi(9) = 6$ et $\varphi(10) = 4$.

Théorème 10. *(Description des groupes cycliques) Soit $n \in \mathbb{N}^*$. Soit G un groupe cyclique d'ordre n. Soit a un générateur de G.*

1. *Tout sous-groupe de $\langle a \rangle$ est cyclique.*
2. *Pour tout entier naturel k, $\left|\langle a^k \rangle\right| = \frac{n}{n \wedge k}$.*
3. *Si d divise n, alors $\langle a \rangle$ contient $\varphi(d)$ éléments d'ordre d.*
4. *$\langle a \rangle$ contient $\varphi(n)$ générateurs. Ce sont les a^k tels que $n \wedge k = 1$.*
5. *Si d divise n, alors l'ensemble $E_d = \{x \in \langle a \rangle,\ x^d = 1\}$ est l'unique sous-groupe de $\langle a \rangle$ d'ordre d, de plus il est cyclique.*

Démonstration. 1. Soit H un sous-groupe de $\langle a \rangle$. Si $H = \{1\}$, il est évidemment cyclique. Si $H \neq \{1\}$, alors il existe un entier naturel non nul l tel que $a^l \in H$. Ainsi, $\{k \in \mathbb{N}^*,\ a^k = 1\}$ est non vide et minoré par 0 donc admet un minimum. Soit $d \coloneqq \min\{k \in \mathbb{N}^*,\ a^k = 1\}$. $(H, .)$ étant un groupe, $\langle a^d \rangle \subset H$. Soit $a^k \in H$. Effectuons la division euclidienne de k par d : $k = dq + r$ avec $0 \leqslant r < d$. Ainsi, $(a)^k(a^{-dq}) = a^r \in H$ car H est un groupe. Ceci contredit la minimalité de d sauf si $r = 0$. D'où $a^k = (a^d)^q \in \langle a^d \rangle$. Ainsi, $H = \langle a^d \rangle$.

2. D'après le théorème 3, on a :

$$\begin{aligned} \left|\langle a^k \rangle\right| &= \min\{m \in \mathbb{N}^*,\ (a^k)^m = 1\} \\ &= \min\{m \in \mathbb{N}^*,\ a^{km} = 1\} \\ &= \min\{m \in \mathbb{N}^*,\ n | km\} \end{aligned}$$

Soit $d \coloneqq n \wedge k$. Il existe alors deux entiers naturels n' et k' tels que $n = dn'$ et $k = dk'$ et $n' \wedge k' = 1$. Ainsi, $n|km$ est équivalent à $dn'|dk'm$ et à $n'|m$ car $n' \wedge k' = 1$. Or, le plus petit entier $m \in \mathbb{N}^*$ tel que $n'|m$ est n', c'est-à-dire $\frac{n}{n \wedge k}$. D'où

$$\left|\langle a^k \rangle\right| = \frac{n}{n \wedge k}$$

3. d divise n donc il existe un entier naturel q tel que $n = dq$. Soit a^k un élément de

$\langle a\rangle$, on a :

$$\begin{aligned}\left|\langle a^k\rangle\right| = d &\Leftrightarrow \frac{n}{n\wedge k} = d\\ &\Leftrightarrow \frac{dq}{n\wedge k} = d\\ &\Leftrightarrow \frac{q}{n\wedge k} = 1\\ &\Leftrightarrow n\wedge k = q\end{aligned}$$

Or il existe un entier naturel k' tel que $k = qk'$. Ainsi :

$$\left(\left|\langle a^k\rangle\right| = d\right) \Leftrightarrow (dq \wedge qk' = q) \Leftrightarrow (d \wedge k' = 1)$$

Or, des entiers k' premiers avec d, il y en a $\varphi(d)$.

4. a^k engendre $\langle a\rangle$ si, et seulement si, a^k est d'ordre n. Or a^k est d'ordre $\frac{n}{n\wedge k}$. Donc a^k engendre $\langle a\rangle$ si, et seulement si, $n \wedge k = 1$. Il y en a bien $\varphi(n)$ d'après la définition de la fonction indicatrice d'Euler.

5. $E_d = \{x \in \langle a\rangle,\, x^d = 1\}$ est clairement un sous-groupe de $\langle a\rangle$, ce dernier étant abélien. De plus, d'après 1., il est cyclique. D'après le corollaire 4, il contient tout sous-groupe de $< a >$ d'ordre d. Soit g un générateur de E_d. Pour tout entier naturel non nul r, on a $(g^r)^d = 1$ qui est équivalent à n divise rd. Or d divise n, donc il existe un entier relatif k tel que $n = dk$. Mais alors, $(g^r)^d = 1$ est équivalent à k divise r. Ainsi, les éléments de E_d sont : g^k, g^{2k}, ..., $g^{dk} = g^n = 1$. Ils sont clairement tous distincts et il y en a donc d. E_d est donc engendré par g^k. Comme tout groupe cyclique d'ordre d, il possède $\varphi(d)$ générateurs. D'après 4., ce sont les g^{kr} avec $r \wedge d = 1$. □

Remarque. On peut synthétiser ce théorème ainsi :

Soit G un groupe cyclique d'ordre n. Alors, pour chaque diviseur d de n, l'ensemble $E_d = \{x \in G,\, x^d = 1\}$ est l'unique sous-groupe d'ordre d de G. Il est cyclique et possède exactement $\varphi(d)$ éléments d'ordre d. Ces éléments sont les générateurs de E_d et s'écrivent sous la forme : $x^{\frac{n}{d}r}$ avec $1 \leqslant r \leqslant d$ et $r \wedge d = 1$.

Exemples. 1. Considérons le groupe cyclique $(\mathbb{Z}/12\mathbb{Z}, +)$. 4 divise 12, donc $E_4 = \{\overline{k} \in \mathbb{Z}/12\mathbb{Z},\, 4\overline{k} = \overline{0}\}$ est l'unique sous-groupe d'ordre 4 de $(\mathbb{Z}/12\mathbb{Z}, +)$. Il est cyclique et possède $\varphi(4) = 2$ éléments d'ordre 4. Ces éléments sont $\overline{3}$ et $\overline{9}$. E_4 contient aussi $\overline{0}$ et $\overline{6}$.

2. Considérons le groupe cyclique $\left(\mathbb{U}_{15} = \left\{e^{\frac{2ik\pi}{15}},\, k \in [\![0; 14]\!]\right\}, \times\right)$. 3 divise 5, donc $E_3 = \left\{e^{\frac{2ik\pi}{15}} \in \mathbb{U}_{15},\, (e^{\frac{2ik\pi}{15}})^3 = 1\right\}$ est l'unique sous-groupe d'ordre 3 de $\left(\mathbb{U}_{15} = \left\{e^{\frac{2ik\pi}{15}},\, k \in [\![0; 14]\!]\right\}, \times\right)$. Il est cyclique et possède $\varphi(3) = 2$ éléments d'ordre 3. Ces éléments sont $e^{\frac{2i\pi}{3}}$ et $e^{\frac{4i\pi}{3}}$. E_3 contient aussi 1.

Théorème 11. *(Formule de Möbius) Pour tout entier naturel non nul n, on a :*

$$n = \sum_{d|n} \varphi(d)$$

Démonstration. Soit $\langle a \rangle$ un groupe cyclique d'ordre n. D'après 3. du théorème 10, pour tout diviseur d de n, $\langle a \rangle$ contient $\varphi(d)$ éléments d'ordre d. Or tout élément de a a un ordre qui divise n d'après le théorème 3. D'où le résultat. □

Théorème 12. *(Caractérisation des groupes cycliques) Soit $(G, .)$ un groupe d'ordre $n \in \mathbb{N}^*$. Soit d un diviseur de n. Notons $E_d = \{x \in G,\ x^d = 1\}$ et $\alpha_G(d)$ le nombre d'éléments d'ordre d de G. Les assertions suivantes sont équivalentes :*

1. *Pour tout diviseur d de n, $|E_d| \leqslant d$.*
2. *Pour tout diviseur d de n, $\alpha_G(d) \leqslant \varphi(d)$.*
3. *Pour tout diviseur d de n, $\alpha_G(d) = \varphi(d)$.*
4. *Le groupe G est cyclique.*
5. *Pour tout diviseur d de n, $|E_d| = d$.*

Démonstration. $1 \Rightarrow 2$: Si $\alpha_G(d) = 0$, c'est évident. Si $\alpha_G(d) \geqslant 1$, alors il existe un élément a de G d'ordre d. Donc $a \in E_d$ et $\langle a \rangle \subset E_d$. Par suite, $|\langle a \rangle| = d \leqslant |E_d|$. Donc, d'après 1., $d = |E_d|$. Par conséquent, $E_d = \langle a \rangle$. Or $\langle a \rangle$ contient $\varphi(d)$ générateurs. Donc ce sont les seuls éléments d'ordre d de G. Par conséquent, $\alpha_G(d) \leqslant \varphi(d)$.

$2 \Rightarrow 3$: Il est clair que $n = \sum_{d|n} \alpha_G(d)$. De plus, $n = \sum_{d|n} \varphi(d)$. Donc, d'après 2., nécessairement, pour tout diviseur d de n, $\alpha_G(d) = \varphi(d)$.

$3 \Rightarrow 4$: Il suffit de prendre $d = n$ dans 3. Ainsi, G possède au moins un élément d'ordre n et est donc cyclique.

$4 \Rightarrow 5$: Découle de 5. du théorème 10.

$5 \Rightarrow 1$: Évident. □

1.3 Exemples

1.3.1 Produit de groupes cycliques

Théorème 13. *Soient G_1 et G_2 deux groupes cycliques d'ordres respectifs m et n.*

$$(m \wedge n = 1) \Leftrightarrow (G_1 \times G_2 \text{ cyclique})$$

Démonstration. $\Rightarrow$: G_1 étant cyclique d'ordre m est isomorphe à $(\mathbb{Z}/m\mathbb{Z}, +)$ et G_2 étant cyclique d'ordre n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$. Considérons l'application $f : (\mathbb{Z}/mn\mathbb{Z}, +) \to (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, +)$ qui à $\ddot{k}$ associe $(\overline{k}; \tilde{k})$. f est clairement un morphisme de groupes. Déterminons $\ker(f)$. Supposons que $(\overline{k}; \tilde{k}) = (\overline{0}; \tilde{0})$. Alors m divise k et n divise k. Or m et n sont premiers entre eux, donc mn divise k et par conséquent $\ddot{k} = \ddot{0}$. Ainsi $\ker(f) = \{\ddot{0}\}$ et f est donc un monomorphisme. Le groupe de départ et le groupe d'arrivée ayant le même ordre, f est un isomorphisme.

$\Leftarrow$: Supposons que $G_1 \times G_2$ est cyclique d'ordre mn et raisonnons par l'absurde : supposons que $d \coloneqq m \wedge n \geqslant 2$. Alors il existe deux entiers naturels m' et n' tels que $m = dm'$ et $n = dn'$ avec $m' \wedge n' = 1$. Or :

$$(m \vee n) \times (m \wedge n) = mn$$

D'où : $m \vee n = dm'n' = m'n = mn' < mn$. Soit $(x; y) \in G_1 \times G_2$, on a :

$$(x; y)^{m \vee n} = (x^{m \vee n)}; y^{m \vee n}) = (1; 1)$$

Ainsi, tout élément de $G_1 \times G_2$ a un ordre strictement inférieur à mn. Ce qui est en contradiction avec le fait que $G_1 \times G_2$ est cyclique d'ordre mn. Par conséquent, $m \wedge n = 1$. □

Exemples. Le groupe $((\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/15\mathbb{Z}), +)$ est cyclique car $8 \wedge 15 = 1$. Le groupe de Klein, $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ n'est pas cyclique car $2 \wedge 2 = 2$.

Remarque. Ce théorème permet de décomposer tout groupe cyclique en produit direct de groupes cycliques plus « petits ».

1.3.2 Sur un corps fini

Théorème 14. *Soit $(\mathbb{K}, +, \times)$ un corps fini. Alors $(\mathbb{K}^*, \times)$ est un groupe cyclique.*

Démonstration. Soit $(\mathbb{K}, +, \times)$ un corps fini. Nécessairement, $(\mathbb{K}^*, \times)$ est un groupe. Il s'agit donc de démontrer qu'il est cyclique. Soit d un diviseur de l'ordre de $(\mathbb{K}^*, \times)$. $E_d \neq \varnothing$ car $1 \in E_d$. Puisque $(\mathbb{K}, +, \times)$ est un corps, le polynôme $X^d - 1$ a au plus d racines sur $\mathbb{K}$. Donc $|E_d| \leqslant d$. Ainsi, d'après le théorème 12, $(\mathbb{K}^*, \times)$ est cyclique. □

Corollaire 15. *Soit p un nombre premier. Alors $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ est un groupe cyclique. Il est isomorphe à $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$.*

Démonstration. Soit p un nombre premier. Alors $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps fini. Donc, d'après le théorème 14, $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ est un groupe cyclique. Son ordre étant $p - 1$, d'après le théorème 7, il est isomorphe à $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$. □

Chapitre 2

Permutations d'un ensemble fini, groupe symétrique. Applications

Pré-requis

1. Composition de deux applications.
2. Définition d'une bijection.
3. Notions sur les groupes.
4. Relation d'équivalence sur un ensemble.
5. Division euclidienne.
6. Isométries du plan.

2.1 Permutations d'un ensemble fini

Définition 16. Soit $n \in \mathbb{N}^*$. On appelle permutation de $[\![1;n]\!]$ toute bijection de $[\![1;n]\!]$ dans $[\![1;n]\!]$. L'ensemble des permutations de $[\![1;n]\!]$ est noté $\mathfrak{S}_n$.

Remarque. Notation matricielle d'une permutation σ :

$$\sigma = \begin{pmatrix} 1 & 2 & ... & k & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(k) & ... & \sigma(n) \end{pmatrix}$$

Proposition 17. *Soit $n \in \mathbb{N}^*$.*

1. *$(\mathfrak{S}_n, \circ)$ est un groupe d'ordre $n!$.*
2. *$(\mathfrak{S}_n, \circ)$ est abélien si, et seulement si, $n \leqslant 2$.*