101. Groupes monogènes, groupes cycliques. Exemples.

I Groupes monogènes.

Définition 1

Un groupe $(G,\cdot)$ est dit *monogène* si et seulement si

$$\exists x \in G,\ G = \{x^n \mid n \in \mathbb{Z}\}.$$

Remarques.

1. Autrement dit les éléments de G peuvent tous s'exprimer comme une puissance d'un certain élément x de G.
2. Nous dirons dans ce cas que G est engendré par x ou que x est un générateur de G.
3. Si de plus G est fini nous dirons de G qu'il est *cyclique*.
4. L'habitude a consacré l'expression « ordre » du groupe pour parler de son cardinal.
5. Tout élément x d'un groupe engendre un sous-groupe que nous noterons $\langle x\rangle = \{x^n \mid n \in \mathbb{Z}\}$.
6. L'ordre d'un élément d'un groupe désigne l'ordre du sous-groupe engendré par cet élément.

Exemples.

1. $(\mathbb{Z},+)$ est un groupe monogène engendré par 1.
2. $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe cyclique engendré par $\overline{1}$.
3. Tous les groupes ne sont pas cycliques. Ainsi le groupe de Klein$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},+)$, n'est pas cyclique comme le montre la table de Pythagore de sa loi.

Proposition 1

Tout groupe monogène est abélien.

Démonstration 1

Un élément de G commute avec lui même donc avec ses puissances. Par conséquent un groupe monogène est abélien.

Remarques.

1. En particulier les sous-groupes d'un groupe monogène sont donc distingués, ce qui permet de considérer des groupes obtenus par passage au quotient.

2. La contraposée de cette proposition est intéressante : un groupe qui n'est pas abélien n'est pas monogène.

Exemples.

1. $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ sont abéliens.
2. Tout les groupes abéliens (finis) ne sont pas monogènes. Ainsi le groupe de Klein est abélien mais pas monogène.

Théorème 1 - Sous-groupe cyclique engendré

Soient :
. $(G,\cdot)$ un groupe fini,
. $x \in G$.

(i) $|\langle x\rangle|$ divise $|G|$.
(ii) $|\langle x\rangle| = \min\{n \in \mathbb{N}^* \mid x^n = 1\}$ et $\langle x\rangle = \{e,x,\dots,x^{|\langle x\rangle|-1}\}$.

Démonstration 2

(i) Application directe du théorème de Lagrange.

(ii) Comme x est d'ordre fini nécessairement il existent $r < s$ des entiers naturels tels que $x^r = x^s$ donc $x^{s-r} = e$. Par conséquent il existe $m = \min\{n \in \mathbb{N}^* \mid x^n = e\}$.

Démontrons que $\langle x\rangle \subset \{e,x,\dots,x^{m-1}\}$.
Soit $t \in \mathbb{Z}$. Démontrons que $x^t \in \{e,x,\dots,x^{|\langle x\rangle|-1}\}$.
Il existe q et r dans $\mathbb{N}$ tels que $t = qm + r$ avec $0 \leqslant r < m$. Donc : $x^t = (x^m)^q x^r = x^r$. Ainsi $x^t \in \{e,x,\dots,x^{m-1}\}$.
Par conséquent $\langle x\rangle \subset \{e,x,\dots,x^{m-1}\}$.

Démontrons que $\{e,x,\dots,x^{m-1}\} \subset \langle x\rangle$.
Soient s et t deux entiers naturels tels que $0 \leqslant s,t < m$. Par construction de m, si $x^s = x^t$ alors $s = t$. Autrement dit les x^k, $k \in [\![0,m]\!]$ sont distincts deux à deux et donc $\{e,x,\dots,x^{m-1}\} \subset \langle x\rangle$.

Ainsi $\{e,x,\dots,x^{m-1}\} = \langle x\rangle$ et donc $|\langle x\rangle| = m$.

Corollaire 1

Soient :
. $(G,\cdot)$ un groupe fini,
. $x \in G$.

(i) $x^{|\langle x \rangle|} = e$.
(ii) Si $|G|$ est un nombre premier alors G est cyclique et G est engendré par tous ses éléments hormis le neutre.
(iii) $x^m = e$ si et seulement si $|\langle x \rangle|$ divise m.

II Classification des groupes monogènes et leurs sous-groupes.

Groupes monogènes infinis.

Théorème 2

(i) Les sous-groupes de $(\mathbb{Z},+)$ sont les $(n\mathbb{Z},+)$ pour $n \in \mathbb{N}$.
(ii) Si $(G,\cdot)$ est un groupe monogène infini alors G est isomorphe à $(\mathbb{Z},+)$.

Démonstration 3

1. Évidemment les $n\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$.
Démontrons que réciproquement tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$.
Tout d'abord $\{0\} = 0\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Soit $(H,+)$ un sous-groupe de $\mathbb{Z}$ non réduit à 0.
$H \cap \mathbb{N}^*$ est non vide (quitte à considérer un opposé). Donc $H \cap \mathbb{N}^*$ admet un minimum n.
Remarquons qu'en particulier $n\mathbb{Z} \subset H$.
Démontrons que $H \subset n\mathbb{Z}$. Autrement dit montrons que $H \cap \mathbb{N} \subset n\mathbb{N}$.
Soit $h \in H \cap \mathbb{N}$.
Par divisions euclidienne il existe $q \in \mathbb{N}$ et $r \in [\![0,n-1]\!]$ tels que : $h = qn + r$.
Puisque $qn \in n\mathbb{Z} \subset H$, $h - qn \in H$ et donc nécessairement $r \in H$. Le fait que n soit un minimum impose donc : $r = 0$. Et par conséquent $h = qn \in n\mathbb{Z}$.
Nous avons démontré que $H \subset n\mathbb{Z}$.

2. Notons $\varphi : \left\{ \begin{array}{ccc} \mathbb{Z} & \to & G \\ n & \mapsto & g^n \end{array} \right.$. φ est clairement un morphisme de groupes. Par définition des groupes monogènes φ est surjective.

Supposons qu'il existe $n \in \mathbb{N}^*$ tel que $g^n = e$. Alors G serait isomorphe à $\mathbb{Z}/n\mathbb{Z}$ donc serait fini, ce qui est impossible. Nécessairement $n = 0$. Donc $\ker(\varphi) = \{0\}$ et $\mathbb{Z}$ est isomorphe à G.

Groupes cycliques.

Théorème 3

Soient :

. $n \in \mathbb{N}^*$,

. $(G,\cdot)$ un groupe cyclique d'ordre n,

. g un générateur de G.

(i) Si $(G,\cdot)$ est cyclique d'ordre n alors G est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$.

(ii) Si d est un diviseur de n alors $\langle g^{\frac{n}{d}} \rangle$ est l'unique sous-groupe d'ordre d de G.

(iii) Les générateurs de G sont les g^k avec $k \wedge n = 1$.

Démonstration 4

1. Notons $\varphi : \left\{ \begin{array}{ccc} \mathbb{Z} & \to & G \\ k & \mapsto & g^k \end{array} \right.$. φ est clairement un morphisme de groupes. Par définition des groupes monogènes φ est surjective.
   Soit $k \in \mathbb{Z}$ tel que $g^k = e$. D'après le (iii) du corollaire sur les sous-groupes engendrés, ceci équivaut à dire que l'ordre de g divise k, ce qui équivaut encore à : $k \in n\mathbb{Z}$. par conséquent : $\ker(\varphi) = n\mathbb{Z}$.
   Finalement $G \sim \mathbb{Z}/n\mathbb{Z}$.

2. * Montrons que $\langle x^{\frac{n}{d}} \rangle$ est sous-groupe cyclique de G.

   Clairement $\langle g^{\frac{n}{d}} \rangle$ est un sous-groupe monogène de G.

   $\langle g^{\frac{n}{d}} \rangle$ est d'ordre inférieur à d puisque $\left(g^{\frac{n}{d}}\right)^d = e$.

   De plus s'il existait un entier naturel $k < d$ tel que $\left(g^{\frac{n}{d}}\right)^k = e$ ceci contredirait le fait que $\langle g^{\frac{n}{d}} \rangle$ est d'ordre d (caractère minimal de l'ordre du groupe). Donc nécessairement $g^{\frac{n}{d}}$ est d'ordre au moins d.
   Finalement $\langle g^{\frac{n}{d}} \rangle$ est d'ordre d.

   * Montrons l'unicité de $\langle g^{\frac{n}{d}} \rangle$.

   Soit H un sous-groupe de G d'ordre d.

Puisque H et $\langle g^{\frac{n}{d}} \rangle$ ont même ordre il suffit de montrer que $H \subset \langle g^{\frac{n}{d}} \rangle$ ce que nous allons faire.
Le cas $H = \{e\}$ étant d'étude triviale soit $h \in H \setminus \{e\}$. Puisque $H \subset G$: $\exists k \in \mathbb{N}^*$, $g^k = h$. Puisque H est d'ordre d, $\left(g^k\right)^d = e$ et donc n divise kd.
Autrement dit : il existe $t \in \mathbb{N}$ tel que $kd = nt$.
Nous en déduisons que $g^k = g^{\frac{n}{d}t} = \left(g^{\frac{n}{d}}\right)^t \in \langle g^{\frac{n}{d}} \rangle$.
Et donc $h \in \langle g^{\frac{n}{d}} \rangle$ puis $H \subset \langle g^{\frac{n}{d}} \rangle$.

3. Si $k \wedge n = 1$ alors l'ordre du sous-groupe divisant l'ordre du groupe nécessairement $\langle g^k \rangle = G$.
Réciproquement si g^k est un générateur de G alors nécessairement $k \wedge n = 1$ car dans le cas contraire $\left(g^k\right)^{\frac{n}{k}} = e$ donc le sous-groupe engendré par g^k serait d'ordre au plus $\frac{n}{k}$ et ne pourrait égaler G.

Remarques.

1. Le groupe réduit au neutre (d'ordre 0) est aussi un groupe cyclique mais son étude est triviale.
2. En particulier, d'après (ii), tous les sous-groupes d'un groupe cyclique sont cycliques.
3. Le (i) autorise à limiter toutes les démonstrations à $\mathbb{Z}/n\mathbb{Z}$ même si ce n'est pas le choix retenu ici.
4. Les points (ii) et (iii) recensent tous les sous-groupes de G.

Corollaire 2

Soient :
. $n \in \mathbb{N}^*$,
. $(G,\cdot)$ un groupe cyclique d'ordre n,
. g un générateur de G,
. φ l'indicatrice d'Euler.

(i) Les sous-groupes de G sont isomorphes aux groupes $\mathbb{Z}/d\mathbb{Z}$ avec d parcourant l'ensemble des diviseurs de n.
(ii) G admet $\varphi(n)$ générateurs.

Démonstration 5

Découle du précédent théorème.

Remarques.

1. L'indicatrice d'Euler désigne la fonction $\varphi : \mathbb{N}^* \to \mathbb{N}$ qui à tout $n \in \mathbb{N}$ associe le nombre de d'entiers naturel non plus petits que n qui soient premiers à n.

Proposition 2 - Formule de Moëbius

Notons φ l'indicatrice d'Euler.

$$\forall n \in \mathbb{N}^*,\ n = \sum_{d|n} \varphi(d).$$

Démonstration 6

Soit G un groupe cyclique d'ordre $n \in \mathbb{N}^*$.
Puisque l'ordre d'un élément g de G divise celui de G :

$$|G| = \sum_{d|n} \text{card}\{g \in G \mid \langle g \rangle = d\}$$

Et puisque G admet exactement $\varphi(d)$ éléments d'ordre d :

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

III Exemples.

Les racines de l'unité.

Définition 2

Soient :

1. $n \in \mathbb{N}^*$,

Nous appellerons groupe des racines n-ième de l'unité le sous groupe de $(\mathbb{C}^*, \cdot)$ défini par

$$\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}.$$

Remarques.

1. Cette définition nécessite la vérification que $\mathbb{U}_n$ ainsi défini est effectivement un sous-groupe.

Produit de groupes cycliques.

Théorème 4

Soient :

. G et H deux groupes cycliques.

. n et m les ordres respectifs de G et H.

$(G \times H, \cdot)$ est cyclique si et seulement $n \wedge m = 1$.

Démonstration 7

* Supposons que $n \wedge m = 1$.
g et h des générateurs respectivement de G et H.
Démontrons que (g,h) est d'ordre nm dans $G \times H$.

Alors $(g,h)^{nm} = (g^{nm}, h^{nm}) = (e_G; e_H) = e$. Donc l'ordre de (g,h) divise nm.
Soit p l'ordre de (g,h), alors, de $g^p = e_G$ et $h^p = e_H$ nous déduisons $n|p$ et $m|p$ et puisque $n \wedge m = 1$, nécessairement $nm|p$.

(g,h) est un élément dont l'ordre égale celui du groupe auquel il appartient donc il est générateur et $G \times H$ est par conséquent cyclique.

* Réciproquement supposons que $G \times H$ est cyclique.
Soit donc $(g,h) \in G \times H$ un générateur de $G \times H$ (qui est donc d'ordre nm).
Démontrons, en raisonnant par l'absurde, que nécessairement n et m sont premiers.

Supposons qu'il existe $d > 1$ diviseur commun à n et m : $n = n'd$ et $m = m'd$.
Alors $n'm'd < nm$ et pourtant $(g,h)^{n'm'd} = e$ ce qui contredit le fait que $G \times H$ est cyclique d'ordre nm.

Ainsi si $G \times H$ est cyclique, nécessairement $n \wedge m = 1$.

Remarques.

1. Ce résultat réclame de savoir ce qu'est un groupe produit.
2. Il réclame également de savoir que l'ordre d'un groupe produit est le produit des ordres des groupes le composant.
3. Ce résultat est extrêmement précieux puisqu'il permet de décomposer un groupe cyclique en un produit de sous-groupes cycliques d'ordres plus petits.

Sur un corps fini.