Les groupes (Révisions et Compléments)

Pascal DELAHAYE - d'après le cours de David Delaunay

17 septembre 2024

Les groupes constituent la première structure, après les ensembles, qui présente pour nous un intérêt théorique.
Dans ce chapitre, nous allons en particulier nous intéresser :

- Aux notions de "groupe" et de "sous-groupe" en général.
- Plus particulièrement aux groupes $(\mathbb{Z},\ +)$, $(S_n,\ \circ)$, mais surtout $(\mathbb{Z}/n\mathbb{Z},\ +)$.
- A la notion de "morphisme de groupe" mais surtout d' "isomorphisme de groupe" qui permet de considérer certains groupes comme un seul et même groupe.
- Aux groupes engendrés par un seul élément que l'on appelle des "groupes monogènes".
  Nous montrerons en particulier, grâce à des isomorphismes de groupes bien choisis, que leur structure est la même que :
  - $\rightarrow$ celle de $(\mathbb{Z},+)$ dans le cas d'un groupe monogène infini
  - $\rightarrow$ celle de $(\mathbb{Z}/n\mathbb{Z},+)$ dans le cas d'un groupe monogène fini.
- A la notion d'*ordre d'un élément* d'un groupe avec, en particulier, une version faible du **théorème de Lagrange**.

Questions de cours à maîtriser pour les colles :

1. Les sous-groupes de $(\mathbb{Z},\ +)$
2. Le groupe $(\mathbb{Z}/n\mathbb{Z},+)$ et ses éléments générateurs
3. Le groupe $(S_n,\ o)$: Décomposition d'une permutation, calcul de l'ordre, de la signature...
4. Savoir prouver la CNS pour que la réunion de 2 sous-groupes soit un sous-groupe
5. Les deux structures possibles pour un groupe monogène
6. Ordre d'un élément : définition, propriétés lorsque le groupe est fini
   Démonstration du théorème de Lagrange dans le cas d'un groupe commutatif

Table des matières

1 L'ensemble $\mathbb{Z}/n\mathbb{Z}$ **2**

2 Structure de Groupe **6**

3 Sous-groupes **11**

4 Morphismes de groupes **15**

5 Une classification des groupes **20**

6 Etude des groupes monogènes **20**

7 Ordre d'un élément dans un groupe **24**

8 Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ (HP) **28**

1 L'ensemble $\mathbb{Z}/n\mathbb{Z}$

1. Relation d'équivalence

Préliminaire hors-programme

DÉFINITION : **Relation d'équivalence**

- Une *relation* sur un ensemble E est une partie de $E \times E$.
- Une *relation d'équivalence* sur un ensemble E est un ensemble $\mathcal{C} \subset E \times E$ tel que :

$$\begin{cases} \forall x \in E,\ (x,\ x) \in \mathcal{C} \\ (x,\ y) \in \mathcal{C} \Rightarrow (y,\ x) \in \mathcal{C} \\ (x,\ y), (y,\ z) \in \mathcal{C} \Rightarrow (x,\ z) \in \mathcal{C} \end{cases}$$

On abandonne cependant volontiers la notation $\mathcal{C}$ au profit de $\mathcal{R}$ telle que :

$$x \mathcal{R} y \iff (x, y) \in \mathcal{C}$$

Les 3 propriétés qui définissent une relation d'équivalence se reformulent alors de la façon suivante :

- Réflexivité : $\forall x \in E, \quad x\ \mathcal{R}\ x$
- Symétrie : $\forall x,\ y \in E, \quad x\ \mathcal{R}\ y \Rightarrow y\ \mathcal{R}\ x$
- Transitivité : $\forall x,\ y,\ z \in E, \quad \begin{cases} x\ \mathcal{R}\ y \\ y\ \mathcal{R}\ z \end{cases} \Rightarrow x\ \mathcal{R}\ z$

Exemples de relations d'équivalence :

- $a = b$,
- $P \iff Q$,
- $u_n \sim v_n$,
- H est isomorphe à G,
- A est équivalente à B,
- A est semblable à B,
- x a la même image par f que y,
- $(a,\ b)\ R\ (a',\ b')$ définie par $ab' = a'b$.

Remarque : On peut voir une relation d'équivalence comme une égalité « MODULO certains critères ».

Complément : Relation d'ordre

Définition : On dit que $\mathcal{R}$ est une *relation d'ordre* lorsque $\mathcal{R}$ est $\begin{cases} \text{réflexive} \\ \text{anti-symétrique} : \begin{cases} x\mathcal{R}y \\ y\mathcal{R}x \end{cases} \Rightarrow x = y \\ \text{transitive} \end{cases}$.

Exemples : Vérifier que

- $\leq$ est une relation d'ordre sur $\mathbb{R}$.
- l'ordre lexicographique est une relation d'ordre sur l'ensemble des mots.
- $\subset$ est une relation d'ordre sur $\mathcal{P}(E)$.

DÉFINITION : **Classe d'équivalence**

Soit une relation d'équivalence $\mathcal{R}$ sur E.
La classe d'équivalence d'un élément $x \in E$ est l'ensemble des $y \in E$ tels que $x\ \mathcal{R}\ y$.

$$\bar{x} = \{y \in E \mid x\ \mathcal{R}\ y\}$$

$x\ \mathcal{R}\ y$ peut donc également se lire « y est dans la classe d'équivalence de x ».

Notations usuelles : $\bar{x}$, $\hat{x}$... ou parfois tout simplement x s'il n'y a pas d'ambigüité

Exemples :

- Une fraction $\frac{a}{b}$ est une classe d'équivalence pour la relation $ab' = a'b$ sur $\mathbb{Z} \times \mathbb{N}^*$.
- Une fraction rationnelle $\frac{P}{Q}$ est une classe d'équivalence pour la relation $PQ' = P'Q$ sur $\mathbb{K}[X] \times \mathbb{K}[X]\backslash\{0\}$.
- Une orbite d'une permutation σ est une classe d'équivalence pour la relation $a\ \mathcal{R}\ b \iff \exists k \in \mathbb{N},\ b = \sigma^k(a)$

Exercice : Soit $f : E \to F$.

- Montrer que la relation $\mathcal{R}$ définie par $a\ \mathcal{R}\ b \iff f(a) = f(b)$ est une relation d'équivalence sur E.

- Montrer que les images peuvent être considérées comme les différentes classes d'équivalences de $\mathcal{R}$.

PROPOSITION :

- $x \in \bar{x}$
- $y \in \bar{x} \iff x \in \bar{y} \iff \bar{x} = \bar{y}$

  Un élément quelconque de la classe d'équivalence détermine celle-ci et est appelé un "représentant de la classe d'équivalence".

- L'ensemble des classes d'équivalence de E pour une relation $\mathcal{R}$ forme une partition de E.

DÉFINITION : **Ensemble Quotient**

$E/\mathcal{R}$ désigne l'ensemble des classes d'équivalence de E pour la relation $\mathcal{R}$.

C'est par définition un ensemble de parties de E.

Exemples :

- $\mathbb{Q}$, $\mathbb{K}(X)$.
- $\mathfrak{M}_{n,p}(\mathbb{K})/\mathcal{R}$ où $\mathcal{R}$ est la relation "...est équivalente à ..."

2. L'ensemble $\mathbb{Z}/n\mathbb{Z}$:

Point clé : La relation « ... est congru à ... modulo n » est une relation d'équivalence sur $\mathbb{Z}$.

DÉFINITION : **Classe de a modulo n**

Un entier $n \in \mathbb{N}^*$ étant fixé, on notera pour tout $a \in \mathbb{Z}$:

$$\bar{a} = \{b \in \mathbb{Z} \mid b \equiv a[n]\} = a + n\mathbb{Z}$$

Il s'agit de la classe d'équivalence de a pour la relation « ... est congru à ... modulo n ».

Exemple : Lorsque $n = 3$, on a $\bar{4} = \{\cdots, -2, 1, 4, 7, \cdots\}$

Remarque : Pour éviter des confusions entre classes modulo n, m... on pourra utiliser les notations : $\hat{a}$, $\mathring{a}$...

THÉORÈME : **Equivalence**
On note $\bar{x}$ de x modulo n.

$$\bar{a} = \bar{b} \iff a \equiv b\ [n]$$

Immédiat !

Exemple : En prenant $n = 11$, on a $\begin{cases} x + y \equiv 3\ [11] \\ x - y \equiv 7\ [11] \end{cases} \iff \begin{cases} \overline{x+y} = \bar{3} \\ \overline{x-y} = \bar{7} \end{cases} \iff \cdots$ (voir plus loin...)

PROPOSITION : **Meilleur représentant d'une classe**

Si r est le reste de la division euclidienne de a par n, on a alors : $\bar{a} = \bar{r}$
Pour simplifier les expressions, il sera donc plus judicieux de remplacer $\bar{a}$ par $\bar{r}$.

♡ *On simplifie systématiquement les classes d'équivalence en choisissant pour représentant de chaque classe, le reste de la division euclidienne par n.*

Exemple : Lorsque $n = 6$ on a $\bar{8}$ sera plutôt noté $\bar{2}$ car la division euclidienne de 8 par 6 est : $8 = 1 \times 6 + 2$.

DÉFINITION : $\mathbb{Z}/n\mathbb{Z}$

Pour tout $n \in \mathbb{N}^*$, on note :

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{a} \mid a \in \mathbb{Z}\} \quad \text{où} \quad \bar{a} \text{ représente la classe de } a \text{ modulo } n$$

Compte-tenu de la proposition précédente : $\mathbb{Z}/n\mathbb{Z} = \{\bar{0},\ \bar{1},\ \ldots,\ \overline{n-1}\}$.

Remarque : $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble quotient $\mathbb{Z}/\mathcal{R}$ où : $a\ \mathcal{R}\ b \iff a \equiv b\ [n]$.

DÉFINITION : **LCI sur $\mathbb{Z}/n\mathbb{Z}$:**

Sur $\mathbb{Z}/n\mathbb{Z}$, on peut définir les deux LCI $+$ et $\times$ par : $\begin{cases} \bar{a} + \bar{b} = \overline{a+b} \\ \bar{a} \times \bar{b} = \overline{a \times b} \end{cases}$

⚠ *Attention à la confusion possible sur le sens des symboles $+$ et $\times$.*

Preuve : Ces définitions n'ont de sens que si $\overline{a+b}$ et $\overline{a \times b}$ sont indépendants des représentants choisis pour $\bar{a}$ et $\bar{b}$. On vérifie facilement que c'est le cas.

Exemples de calculs : Dans $\mathbb{Z}/6\mathbb{Z}$ on a $\begin{cases} \bar{3} + \bar{5} = \bar{8} = \bar{2} \\ \bar{3}.\bar{5} = \overline{15} = \bar{3} \end{cases}$.

Et dans $\mathbb{Z}/4\mathbb{Z}$?

PROPOSITION : **Reformulation des relations de congruences**

Dans $\mathbb{Z}/n\mathbb{Z}$, on a : $\begin{cases} a \equiv b\ [n] \iff \bar{a} = \bar{b} \\ a + b \equiv c\ [n] \iff \bar{a} + \bar{b} = \bar{c} \\ a.b \equiv c\ [n] \iff \bar{a}.\bar{b} = \bar{c} \end{cases}$.

« *Principe du parapluie* » *: On transforme un problème de congruence en un problème algébrique sur $\mathbb{Z}/n\mathbb{Z}$.*

.

Exemple : Résoudre $2\bar{x} = \bar{3}$ dans $\mathbb{Z}/4\mathbb{Z}$.

- Méthode 1 : On teste chacune des 4 valeurs possibles

- Méthode 2 : On remarque que $2\bar{x} = \bar{x} + \bar{x} = \overline{x+x} = \overline{2x} = \bar{2}.\bar{x}$.
  L'idée est alors de multiplier l'équation par l'inverse de $\bar{2}$... (Vu dans le chapitre sur les anneaux)

2 Structure de Groupe

1. Définition :

Cf cours MPSI (A revoir en autonomie !)

DÉFINITION : $(G,\ \star)$ est un groupe lorsque $\begin{cases} \star \text{ lci} \\ \star \text{ est associative} \\ \star \text{ admet un élément neutre dans } G \\ \text{tout élément de } G \text{ est symétrisable dans } G \end{cases}$.

Attention : Lorsque $\star$ n'est pas commutative

- $(a \star b)^{-1} = b^{-1} \star a^{-1}$
- Vérification de l'élément neutre : e est l'éléments neutre ssi $\begin{cases} x \star e = x \\ e \star x = x \end{cases}$ pour tout $x \in G$
- Vérification du symétrique : y est le symétrique de x ssi $\begin{cases} x \star y = e \\ y \star x = e \end{cases}$.

Exemples : Les groupes encadrés ont seulement la structure de groupe.

- Nombres : $(\mathbb{Z},\ +)$, $(\mathbb{Q},\ +)$, $(\mathbb{R},\ +)$ et $(\mathbb{C},\ +)$, $(\mathbb{Q}^*,\ \times)$, $(\mathbb{R}^*,\ \times)$ et $(\mathbb{C}^*,\ \times)$.
- Ensembles : $(\mathbb{Z}/n\mathbb{Z},\ +)$
- Fonctions : $(\mathcal{F}(A, \mathbb{K}),\ +)$, $\boxed{(\mathcal{S}_n, \circ),\ (\mathrm{GL}(\mathbb{E}),\ \circ),\ (\mathrm{O}(E),\ \circ),\ (\mathrm{SO}(E),\ \circ)}$.
- Matrices : $(\mathfrak{M}_n(\mathbb{R}), +)$, $\boxed{(\mathrm{GL}_n(\mathbb{R}), \times),\ (\mathrm{O}_n(\mathbb{R}), \times),\ (\mathrm{SO}_n(\mathbb{R}), \times)}$.

Groupe additif : il s'agit d'un groupe commutatif (abélien) pour lequel la loi est noté $+$.

- Le symétrique de x est alors noté $-x$
- L'élément neutre est alors noté 0_G

Groupe multiplicatif : il s'agit d'un groupe pour lequel la loi n'est pas notée $+$: $*$, ., $\star$, $\circ$, ...

- Le symétrique de x est alors noté x^{-1}
- L'élément neutre est alors noté 1_G ou e_G

Itérés d'un élément :

- Définition : Pour $n \in \mathbb{N}^*$ et pour $a \in G$.

  → Dans un groupe multilicatif l'itéré $a \star a \star ... \star a$ est noté a^n.
  a^{-n} représente le symétrique de a^n.
  Par convention $a^0 = 1_G$.

  → Dans un groupe additif, l'itéré $a + ... + a$ est noté na.
  $-na$ représente le symétrique de na.
  Par convention $0a = 0_G$.

- ⚠ Attention : Lorsque le groupe $(G, \star)$ n'est pas commutatif : $(a \star b)^n \neq a^n \star b^n$

Exercice : 1

(∗) Montrer que si G est un groupe tel que tout éléments $a,\ b \in G$ vérifie $(ab)^2 = a^2b^2$, alors G est commutatif.

2. Le groupe $(\mathbb{Z}/n\mathbb{Z},\ +)$:

La loi + sur $\mathbb{Z}/n\mathbb{Z}$ a été définie précédemment.

THÉORÈME : $(\mathbb{Z}/n\mathbb{Z},\ +)$ est un groupe commutatif tel que $\begin{cases} \text{élément neutre : } \bar{0} \\ \text{opposé de } \bar{a} : -\bar{a} = \overline{-a} \end{cases}$.

Preuve :

- Associativité :
- Commutativité :
- Elément neutre :
- Symétrique :

Formule : $k.\bar{a} = \overline{ka}$ pour tout $k \in \mathbb{Z}$.

Preuve :

- Par récurrence lorsque $k \in \mathbb{N}$.
- On se ramène au cas précédent lorsque $k \in \mathbb{Z}\backslash\mathbb{N}$

Exemples : Présentation des lois + de $\mathbb{Z}/2\mathbb{Z}$ et de $\mathbb{Z}/3\mathbb{Z}$ sous forme de tableau.

♡ Chaque ligne et colonne contient tous les éléments du groupe.

Cette propriété provient de la bijectivité de $f_a : \begin{array}{ccc} G & \longrightarrow & G \\ x & \mapsto & x \star a \end{array}$ et de $g_a : \begin{array}{ccc} G & \longrightarrow & G \\ x & \mapsto & a \star x \end{array}$.

Preuve :

(a) Le groupe symétrique :

Cf cours MPSI (A revoir en autonomie !)

Notations :

- $\mathcal{S}_E$ est l'ensemble des bijections de E dans E
- $\mathcal{S}_n$ est l'ensemble des bijections de $[\![1, n]\!]$ dans $[\![1, n]\!]$.

Cardinal : La groupe symétriques S_n a pour caldinal $n!$

Définitions et Notations :

- Permutation de $\mathcal{S}_n$
- Notation usuelle/orbitale d'une permutation
- Support d'une permutation
- Orbite d'un élément pour une permutation
- Ordre d'une permutation
- Inversion dans une permutation
- Signature d'une permutation

Exemple : Etudier la permutation suivante : $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 3 & 7 & 2 & 10 & 8 & 4 & 6 & 9 & 1 \end{smallmatrix}\right)$.

Exemples d'éléments + propriétés + notations

Dans S_n :

- **Les cycles** :

  Un cycle est une permutation dont une seule orbite peut contenir plus d'un élément.
  On utilise une notation spécifique pour les cycles de S_n : $c = (x_1\ x_2\ \dots\ x_p)$
  Lorsque cette orbite admet p éléments, on dit que c est un p-cycle et on a $c^p = \mathrm{id}$.
  Les cycles commutent si et seulement si ils sont à supports disjoints.

- **Les transpositions** : Un 2-cycle τ est appelé une transposition : on a $\tau^2 = \mathrm{id}$.

- **Les permutations circulaires** :

  Dans $\mathcal{S}_n$, un n-cycle c est appelé une permutation circulaire et $c^n = \mathrm{id}$.

Rappels des théorèmes de décomposition :

- Décomposition commutative d'une permutation en produit de cycles à supports disjoints (unique à l'ordre près !).

Exercice : 2
(∗) Déterminer les permutations d'ordre 2 de $\mathcal{S}_n$.

- Décomposition non commutatif d'un cycle en produit de transpositions.

- Décomposition non commutative d'une permutation en produit de transpositions (non unique mais parité unique du nombre de transpositions).

Exemple : Décomposer une permutation de S_{12} choisie au hasard.

Méthode pour calculer la composée de permutations

On détermine les images de chacun des éléments de $[\![1, n]\!]$.

Exercice : 3

(∗) Justifier que deux permutations à supports disjoints sont commutatives.

Exercice : 4

(∗) Dans le groupe symétrique S_n, calculer $\sigma^k \tau \sigma^{-k}$ pour tout $k \in [\![0, n-2]\!]$ lorsque $\begin{cases} \tau = (1\ 2) \\ \sigma = (1\ 2\ \dots\ n) \end{cases}$.

3. Produit fini de groupes :

Cf cours MPSI (A revoir en autonomie !)

DÉFINITION : **Groupe produit**

Soit $(G_1, \star_1), \dots, (G_n, \star_n)$ des groupes.

Sur $G_1 \times G_2 \times \cdots \times G_n$ on définit la lci $\star$ par $(x_1, \dots, x_n) \star (y_1, \dots, y_n) = (x_1 \star_1 y_1, \dots, x_n \star_n y_n)$.

$(G_1 \times G_2 \times \cdots \times G_n, \star)$ est un groupe appelé *groupe produit*

Preuve : On vérifie facilement que c'est un groupe avec :

- l'élément neutre : $(e_1, e_2, \dots, e_n)$
- le symétrique d'un élément $(x_1^{-1}, x_2^{-1}, \dots, x_n^{-1})$.
- la commutativité si et seulement si tous les groupes sont commutatifs.

Exemples : G^n, $\mathbb{Z}^2$, $\mathbb{R}^{+*} \times \mathbb{R}$ et $(\mathbb{Z}/2\mathbb{Z})^n$ sont des groupes produits pour des lois à préciser...

Exercice : 5

(∗) Soit G un groupe tel que tout élément g vérifie $g^2 = e_G$.

1. Montrer que G est commutatif.
2. Montrer que $(\mathbb{Z}/2\mathbb{Z})^2$ vérifie cette propriété.

3 Sous-groupes

1. Définition et exemples :

Cf Cours MPSI (A revoir en autonomie !)

DÉFINITION : H est un sous-groupe de $(G,\ \star)$ lorsque $\begin{cases} H \subset G \\ e_G \in H \quad (\text{ou } H \neq \emptyset) \\ H \text{ stable par } \star \text{ et par symétrisation} \end{cases}$.

Un sous-groupe H du groupe G est un groupe inclus dans G de loi identique à que celle G.
H admet alors le même élément neutre que G et les symétriques dans H sont les mêmes que dans G.

Méthode : Pour montrer la stabilité par symétrisation

⚠ Il s'agit de montrer une stabilité et non une existence !

- On considère $x \in H$ et son symétrique x^{-1} dans G.
- On montre alors que $x^{-1} \in H$

Exemples :

- Nombres :
  → $(U,\ \times)$, $(U_n,\ \times)$ sont des sous-groupes de $(\mathbb{C}^*,\ \times)$
  → $(n\mathbb{Z},\ +)$ est un sous-groupe de $(\mathbb{Z},\ +)$

- Fonctions :
  → $(\mathrm{GL}(\mathbb{E}),\ \circ)$, $(\mathrm{SO}(E),\ \circ)$ sont des sous-groupes de $(\mathcal{B}(E),\ \circ)$
  → Le groupe des fonctions polynômiales $(\mathbb{R}_n[x],\ +)$ est un sous-groupe de $(\mathcal{F}(\mathbb{R},\ \mathbb{R}),\ +)$
  → Le groupe alterné $\mathcal{A}_n$ des permutations de signature $+1$ est un sous-groupe de $\mathcal{S}_n$

- Matrices : $(\mathrm{O}_n(\mathbb{R}),\ \times)$, $(\mathrm{SO}_n(\mathbb{R}),\ \times)$, $(SL_n(\mathbb{R}),\ \times)$ sont des sous-groupes de $(\mathrm{GL}_n(\mathbb{R}),\ \times)$.

Méthode : Pour montrer que $(H,\ \star)$ est un groupe

- On peut utiliser la définion d'un groupe,
- ♡ On peut montrer que $(H,\ \star)$ est un sous-groupe d'un groupe $(G,\ \star)$ connu. (si c'est possible !)

Exercice : 6

(∗) Montrer que $H = \{x + y\sqrt{3} \mid x \in \mathbb{N},\ y \in \mathbb{Z},\ x^2 - 3y^2 = 1\}$ est un sous-groupe de $(\mathbb{R}^{+*},\ \times)$

On remarquera que pour tout $x + y\sqrt{3} \in H$, on a $x \geq \sqrt{3}|y|$.

PROPOSITION : **Intersection et Réunion de sous-groupes**

- L'intersection d'une famille (finie ou infinie) de sous-groupes est un sous-groupe.
- ⚠ La réunion d'une famille (finie ou infinie) de sous-groupes N'EST en général PAS un sous-groupe.

Preuve :

- Intersection :

- Réunion :

Exercice : 7

(♡) Soient H et K deux sous-groupes d'un groupe G.
Montrer que $H \cup K$ est un sous-groupe de G ssi $H \subset K$ ou $K \subset H$.

Ces propriétés sur l'intersection et la réunion sont également vraies pour les sev d'un $\mathbb{K}$-ev

Exercice : 8

(∗) Montrer que $\left(\bigcup_{n\in\mathbb{N}^*} \mathbb{U}_n,\ \times\right)$ est un groupe.

PROPOSITION : **Somme de deux sous-groupes**

Soient F et H deux sous-groupes d'un groupe additif (et donc abélien) G.

$$F + H = \{f + h \mid f \in F,\ h \in H\} \quad \text{est un sous-groupe de } G$$

D/ Aucune difficulté.

Remarque : $F + H$ est le plus petit sous-groupe de G qui contient F et H.

2. Sous-groupe engendré par une partie :

DÉFINITION : **Sous-groupe engendré par une partie**

Soit A une partie non vide d'un groupe G.
Le sous-groupe engendré par A, noté $< A >$ est :

- l'ensemble des éléments obtenus en composant autant de fois voulu un nombre fini d'éléments de A et leurs symétriques entre eux.
- l'intersection de tous les sous-groupes de G contenant A.
- le plus petit sous groupe de G contenant A.

Les trois définitions précédentes sont bien entendue équivalentes entre elles.

Mq l'intersection de tous les sg de G contenant A est le plus petit sous groupe de G contenant A.

Notation : Le sous-groupe engéndré par $\{a\}$ est noté $< a >$.

Méthode pour montrer que $\text{Vect}(A) = H$

On procède par double inclusion en montrant que :

- $\text{Vect}(A) \subset H$ (ou seulement $A \subset H$ si on sait que H est un groupe)
- $H \subset \text{Vect}(A)$ (en montrant que tout élément de H se décompose en puissances d'éléments de A)

Exemples :

- $G =< a >$ est appelé un *groupe monogène* et a est un *générateur* de G.
- Cas d'une partie de $(G,\ .)$ à deux éléments : $\begin{cases} < \{a,b\} >= \{a^n b^m \mid n,\ m \in \mathbb{Z}\} & \text{si } ab = ba \\ < \{a,b\} >= \{a^{n_1} b^{m_1} \dots a^{n_p} b^{m_p} \mid p \in \mathbb{N},\ ...\} & \text{sinon} \end{cases}$.
- S_n est engendré par :
  → L'ensemble des transpositions
  → L'ensemble des cycles
  → L'ensemble des transpositions de la forme $(1\ i)$. D/ $(i\ j) = (1\ i)(1\ j)(1\ i)$
- Dans $(\mathbb{Z}^2, +)$: $< \{(a,\ b),\ (c,\ d)\} >= \{k(a,\ b) + h(c,\ d) \mid k, h \in \mathbb{Z}\}$
- $F + H =< F \cup H >$

$\subset$

$\supset$

Exercice : 9

$(*)$ Déterminer le sous-groupe de $\mathcal{B}(\mathbb{R}\backslash\{0,\ 1\},\ \mathbb{R}\backslash\{0,\ 1\})$ engendré par f et g définies par $\begin{cases} f(x) = 1 - x \\ g(x) = \frac{1}{x} \end{cases}$.

On constate que $\begin{cases} f^2 = \text{id} \\ g^2 = \text{id} \end{cases}$ et que parmi les autres composées possibles, on ne trouve que $\begin{cases} f \circ g \\ g \circ f \\ f \circ g \circ f \end{cases}$.

Exercice : 10

(♡) Dans le groupe symétrique S_n, on considère les permutations : $\begin{cases} \tau = (1\ 2) \\ \sigma = (1\ 2\ \dots\ n) \end{cases}$.

On rappelle que pour tout $k \in [\![0, n-2]\!]$, on a $\sigma^k \tau \sigma^{-k} = (k+1\ k+2)$. *(Vu précédemment en exo)*

1. Soit $i < j \in [\![1, n]\!]$.
   Calculer $(i\ i+1)(i+1\ i+2)\dots(j-2\ j-1)(j-1\ j)(j-2\ j-1)\dots(i+1\ i+2)(i\ i+1)$.
   En déduire que S_n est engendré par l'ensemble des transpositions de la forme $(k\ k{+}1)$ avec $k \in [\![1, n{-}1]\!]$.

2. En déduire que S_n est engendré par la famille $(\tau,\ \sigma)$.

3. Les sous-groupes de $\mathbb{Z}$:

Proposition : Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$ où $n \in \mathbb{N}$.

Preuve :

- Analyse : Soit H un sous-groupe de $\mathbb{Z}$ non réduit à 0.
  On considère $n = \min H \cap \mathbb{N}^*$ et on montre que $n\mathbb{Z} \subset H$, puis que $H \subset n\mathbb{Z}$ par division euclidienne.

- Synthèse : On a vu précédemment que les $n\mathbb{Z}$ sont bien des sous-groupes de $(\mathbb{Z},\ +)$.

Il faux retenir le principe de cette démonstration car il est utilisé dans d'autres démonstrations.

Remarque : Ce résultat permet de redéfinir $\begin{cases} \text{le PGCD : } a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z} \\ \text{le PPCM : } a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z} \end{cases}$ (Voir le cours sur les anneaux !)

4 Morphismes de groupes

1. Définition :

Cf cours MPSI (A revoir en autonomie !)

Définition : Morphismes de groupes

$\varphi : (G,\ \star) \to (H,\ \circ)$ est un morphisme de groupes lorsque :

$$\begin{cases} (G,\ \star) \text{ et } (H,\ \circ) \text{ sont des groupes} \\ \varphi(g_1 \star g_2) = \varphi(g_1) \circ \varphi(g_2) \quad \forall g_1, g_2 \in G \end{cases}$$

Vocabulaire : $\begin{cases} \text{Endomorphisme } (\varphi : G \to G) \\ \text{Isomorphisme } (\varphi \text{ est bijective}) \\ \text{Automorphisme } (\varphi \text{ est un endomorphisme bijectif}) \end{cases}$

Exemples :

- $\varphi : G \to G$ telle que $\varphi(g) = e$
- $\varphi = \mathrm{id}_G$
- $\varphi : \mathbb{Z} \to G$ telle que $\varphi(n) = a^n$
- $\exp : \mathbb{R} \to U$ (morphisme surjectif canonique)
- $\exp : \mathbb{C} \to \mathbb{C}^*$
- $\exp : \mathbb{R} \to \mathbb{R}^{+*}$ et sa bijection réciproque $\ln : \mathbb{R}^{+*} \to \mathbb{R}$
- $m : \mathbb{C}^* \to \mathbb{R}^{+*}$ telle que $m(z) = |z|$
- $c : \mathbb{C} \to \mathbb{C}$ telle que $c(z) = \bar{z}$
- $\det : \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^*$
- $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ telle que $\varphi(k) = \bar{k}$ (morphisme surjectif canonique).

Proposition : Signature d'une permutation

La signature d'une permutation $\varepsilon : \begin{array}{ccccc} (\mathcal{S}_n, \circ) & \longrightarrow & (\{-1,1\}, \times) \\ \sigma & \mapsto & \varepsilon(\sigma) \end{array}$ est un morphisme de groupe.

Exercice : 11

(∗) Quelle est la signature d'un cycle ?
En déduire une nouvelle formule donnant la signature d'une permutation.

Proposition : La composée de deux morphismes est un morphisme.

D/ Facile

Proposition : Calculs avec un morphisme : $\varphi : G \to H$

- $\varphi(e_G) = e_H$
- $\varphi(x)^{-1} = \varphi(x^{-1})$
- $\varphi(x_1 \star \cdots \star x_n) = \varphi(x_1) \circ \cdots \circ \varphi(x_n)$
- $\varphi(a^n) = \varphi(a)^n$

D/ Facile, mais il faut savoir le faire...

PROPOSITION : **Images d'un sous-groupe**

Les images $\left\{ \begin{array}{l} \text{directe} \\ \text{réciproque} \end{array} \right.$ d'un sous-groupe par un morphisme sont des sous-groupes.

D/ Facile, mais il faut savoir le faire...

2. Noyau et Image :

Cf cours MPSI (A revoir en autonomie !)

DÉFINITION : **Noyau et Image d'un morphisme**

Pour un morphisme $\varphi : G \to H$ on définit : $\left\{ \begin{array}{l} \ker \varphi = \{x \in G \mid \varphi(x) = e_H\} \\ \text{Im}\, \varphi = \{\varphi(x) \mid x \in G\} \end{array} \right.$.

- $\ker \varphi$ est un sous-groupe de G
- $\text{Im}\, \varphi$ est un sous-groupe de H

Méthode : Recherche du noyau de $\varphi : G \to H$

On recherche les antécédents de e_H par φ.
Pour cela, on résout l'équation $\varphi(x) = e_H$ dans G.

Méthode : Recherche de l'image de $\varphi : G \to H$

On recherche l'ensemble des images.
Pour cela, on procède par analyse/synthèse...
→ Analyse : Soit $y \in \text{Im}\, \varphi$, alors $y = \varphi(x)$ avec $x \in G$ et ... et donc $y \in \Delta$
→ Synthèse : Soit $y \in \Delta$, vérifions s'il existe $x \in G$ tel que $y = \varphi(x)$...

Exemples : Déterminer

- $\text{Im}\, m$ et de $\ker m$ (m est l'application "module" dans $\mathbb{C}^*$)
- Im(exp) et de ker(exp) (exp est l'exponentielle réelle, puis complexe)
- Im(det) et de ker(det).
- $\text{Im}\, \varepsilon$ et de $\ker \varepsilon$.

Exercice : 12

(∗) Soit $f : \mathbb{R}^* \to \mathbb{R}^*$ définie par $f(x) = x^n$ où $n \in \mathbb{N}^*$.

Montrer que f est un endomorphisme du groupe $(\mathbb{R}^*,\ \times)$.
Déterminer son noyau et son image.

THÉORÈME : **Caractérisation de l'injectivité et de la surjectivité**

- Un morphisme $\varphi : G \to H$ est injectif si et seulement si $\ker \varphi = \{e_G\}$
- Un morphisme $\varphi : G \to H$ est surjectif si et seulement si $\mathrm{Im}\,\varphi = H$ (trivial !)

D/ Pas de difficulté

3. Isomorphisme de groupe :

Cf cours MPSI (A revoir en autonomie !)

DÉFINITION : **Isomorphisme de groupe**

Un isomorphisme de groupe est un morphisme de groupe bijectif.

Exemples à connaître :

- $\ln : \mathbb{R}^{+*} \to \mathbb{R}$
- $\exp : \mathbb{R} \to \mathbb{R}^{+*}$ (réelle)
- $\tau_a : G \to G$ telle que $\tau_a(x) = axa^{-1}$.

PROPOSITION : **Stabilité par composition et par inversion.**

- La composée de deux isomorphismes de groupe est un isomorphisme de groupe.
- La bijection réciproque d'un isomorphisme de groupe est un isomorphisme de groupe.

D/ Facile.

Remarque : L'ensemble des automorphismes de G est un sous-groupe de $\mathcal{B}(G,\ G)$.

Exercice : 13
(♡♡) Soit $p,\ q \in \mathbb{N}^*$ premiers entre eux.

Montrer que $\varphi : \begin{array}{ccc} \mathbb{Z}/pq\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ \bar{k} & \mapsto & (\tilde{k},\ \hat{k}) \end{array}$ est un isomorphisme de groupes.

La démonstration est à connaître !

4. Groupes isomorphes :

DÉFINITION : **Groupes isomorphes**

Soit deux groupes G et H.
On dit que G *est isomorphe à* H lorsqu'il existe un isomorphisme de G vers H.

PROPOSITION : **Nouvelle terminologie**

La relation "... est isomorphe à ..." est une relation d'équivalence sur l'ensemble des groupes.
On dira donc plus simplement que les groupes G et H *sont isomorphes.*

Interprétation : ♡ *Lorsque 2 groupes sont isomorphes, ils peuvent être considérés identiques aux notations des lci et des éléments près. Les isomorphismes permettent ainsi d'identifier les groupes de même nature et de se limiter à l'étude d'un unique groupe représentatif.* ♡

Exemples de groupes isomorphes :

- $(\mathbb{R}, +)$ et $(\mathbb{R}^{+*}, \times)$ via la fonction exp
- $(\mathbb{Z}/4\mathbb{Z}, +)$ et $(U_4, \times)$ en prenant l'isomorphisme φ défini par $\varphi(\bar{k}) = i^k$.

♡ *Deux groupes finis sont isomorphes lorsqu'ils ont le même nombre d'éléments et si leur loi peut être représentée par une même table.*

Méthode : Pour montrer que deux groupes ne sont pas isomorphes

On montre que deux groupes G et H ne sont pas isomorphes en procédant par l'absurde et en montrant que deux équations équivalentes via un isomorphisme n'ont pas le même nombre de solutions.

En pratique, on considère souvent les équations $\begin{cases} x^2 = 1_G \text{ lorsque } G \text{ et multiplicatif} \\ 2x = 0_G \text{ lorsque } G \text{ est additif} \end{cases}$.

Preuve :

- On suppose qu'il existe un isomorphisme $\varphi : G \to H$.
- On considère (E_G) une équation d'inconnue $x \in G$.
- En transformant (E_G) par l'isomorphisme φ, on obtient :

$$x \in G \text{ solution de } (E_G) \iff \varphi(x) \text{ solution de } (E_H)$$

- Si $\text{Card}(\mathcal{S}_G) > \text{Card}(\mathcal{S}_H)$ alors φ n'est pas injective et on obtient une contradiction.
  Si $\text{Card}(\mathcal{S}_H) > \text{Card}(\mathcal{S}_G)$, on fait le même raisonnement avec φ^{-1}.

- $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \times)$.

On considère l'équation $x^2 = 1$ dans $\mathbb{R}^*$.

- $H = ((\mathbb{Z}/2\mathbb{Z})^2, +)$ n'est pas isomorphe à $(\mathbb{Z}/4\mathbb{Z},\ +)$. (et donc à $(U_4,\ \times)$)

On considère l'équation $2\bar{x} = \bar{1}$ dans $\mathbb{Z}/4\mathbb{Z}$.

5 Une classification des groupes

	Groupes infinis	Groupes finis
Groupes monogènes	$(\mathbb{Z},\ +) =< 1 >$	$(U_n, \times) =< e^{i2\pi/n} >$ (Groupes cycliques)
Groupes non monogènes	$(\mathbb{R}^*,\ \times)$	$(S_n,\ \circ)$ pour $n \geq 3$

6 Etude des groupes monogènes

DÉFINITION : **Groupe monogène**

On dit qu'un groupe G est monogène lorsqu'il est engendré par un seul élément.
C'est à dire, s'il existe $a \in G$ tel que :

$$G =< a >= \{a^k \mid k \in \mathbb{Z}\} \quad \text{ou} \quad G =< a >= \{ka \mid k \in \mathbb{Z}\}$$

"a" est appelé un *élément générateur* (ou un générateur) de G.

Exemples de groupes monogènes :

- $\mathbb{Z} =< 1 >$ (additif)
- $U_n =< e^{i2\pi/n} >$ (multiplicatif)
- $\mathbb{Z}/n\mathbb{Z} =< \bar{1} >$ (additif)
- $G =< (1\ 2\ 3) >$ dans $\mathcal{S}_n$ (multiplicatif)

Contre-exemple : $(\mathbb{R}, +)$ n'est pas monogène.

1. Commutativité :

PROPOSITION : Un groupe monogène est un groupe commutatif.

D/ Facile

Méthode 1 : Pour montrer qu'un groupe n'est pas monogène

On peut :

- soit montrer qu'il n'est pas commutatif (car tout groupe monogène est commutatif)
- soit procéder par l'absurde (Supposons que $G =< a >$) et montrer que $G \not\subset < a >$.

Exemples de groupes non monogènes :

- S_n n'est pas monogène pour $n \geq 3$
- $\mathrm{GL}_n(\mathbb{K})$ n'est pas monogène pour $n \geq 2$

Preuve : Ces deux groupes ne sont pas commutatifs.

(a) Eléments générateurs : *Que dire des éléments générateurs d'un groupe monogène ?*

Réponse : Un groupe monogène peut admettre plusieurs générateurs.

Exemples : Donner les générateurs de $\mathbb{Z}/14\mathbb{Z}$ et $< (1\ 2\ 3) >$.

2. Description des groupes monogènes (finis ET infinis) :

THÉORÈME FONDAMENTAL : **Typologie des groupes monogènes**

Les groupes MONOGENES sont :

- soit isomorphes à $(\mathbb{Z},\ +)$, lorsque le groupe est de cardinal infini.
- soit isomorphes à $(\mathbb{Z}/n\mathbb{Z},\ +)$, lorsque le cardinal est fini et vaut n. *(groupe cyclique)*

Preuve : Soit $G =< a >$ monogène.
On considère $\varphi : \mathbb{Z} \to G$ définie par $\varphi(p) = a^p$ (morphisme surjectif !).
Son noyau vaut $n\mathbb{Z}$.

- Si $n = 0$ alors φ isomorphisme.
- Si $n > 0$, on considère $\bar{\varphi} : \mathbb{Z}/n\mathbb{Z} \to G$ telle que $\bar{\varphi}(\bar{k}) = a^k$ en prenant $k \in [\![0, n-1]\!]$
  Cette application est bien définie et c'est un isomorphisme.

Par exemple : $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{U}_n$ sont isomorphes via l'application $\varphi(\bar{k}) = (e^{2i\pi/n})^k = e^{2ik\pi/n}$.

Remarque : ♡ Les groupes monogènes sont donc de la même nature que $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$.

A retenir sur les groupes monogènes

En adoptant la notation multiplicative et en prenant $a \in G$.

- Si Card$(< a >) = +\infty$: $< a >$ et $\mathbb{Z}$ sont isomorphes via $\varphi(k) = a^k$.

  Cela signifie que, si $< a >$ est infini, alors :

  $$\boxed{< a >= \{\ldots,\ a^{-2},\ a^{-1},\ 1_G,\ a,\ a^2,\ \ldots\}} \quad \text{éléments 2 à 2 distincts}$$

- Si Card$(< a >) = n \in \mathbb{N}^*$: $< a >$ et $\mathbb{Z}/n\mathbb{Z}$ sont isomorphes via $\varphi(\bar{k}) = a^k$.

  Cela signifie que, si $< a >$ est fini de cardinal n, alors :

  $$\boxed{< a >= \{1_G,\ a,\ a^2,\ \ldots,\ a^{n-1}\} \quad \text{avec} \quad a^n = e} \quad \text{éléments 2 à 2 distincts}$$

Remarque : Avec la notation additive, on obtient

$$< a >= \{\ldots,\ -2a,\ -a,\ 0,\ a,\ 2a,\ \ldots\} \quad \text{ou} \quad < a >= \{0,\ a,\ 2a,\ \ldots,\ (n-1)a\}$$

Exemples :

- $n\mathbb{Z}$ est monogène infini engendré par n donc : $n\mathbb{Z} = \{\cdots,\ -2.1,\ -1.1,\ 0,\ 1,\ 2.1, \ldots\}$
- U_5 est monogène de cardinal 5 engendré par $e^{i\frac{2\pi}{5}}$ donc : $U_5 = \{1,\ e^{i\frac{2\pi}{5}},\ (e^{i\frac{2\pi}{5}})^2,\ (e^{i\frac{2\pi}{5}})^3,\ (e^{i\frac{2\pi}{5}})^4\}$

3. Les générateurs d'un groupe monogène

On commence par étudier les générateur de $\mathbb{Z}/n\mathbb{Z}$.

PROPOSITION : **Générateurs de $\mathbb{Z}/n\mathbb{Z}$**

Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les $\bar{p}$ avec $p \in [\![1, n-1]\!]$ et $p \wedge n = 1$

Preuve :

DÉFINITION : **Indicatrice d'Euler**

Le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$ est noté $\varphi(n)$ et $\varphi : \mathbb{N}^* \to \mathbb{N}$ est appelée l'*indicatrice d'Euler*.

$\varphi(n)$ *est donc* $\begin{cases} \textit{le nombre de générateurs de } \mathbb{Z}/n\mathbb{Z} \\ \textit{le nombre de nombres de } [\![1,n]\!] \textit{ premiers avec } n \end{cases}$.

Exemple : Calculer $\varphi(3)$ et $\varphi(4)$.

Nous savons désormais qu'un groupe monogène peut admettre plusieurs générateurs...
Mais quels sont-ils exactement ?

PROPOSITION : **Correspondance des générateurs**

Soit G et H deux groupes isomorphes via un isomorphisme $\varphi : G \to H$.
On a alors :

Les générateurs de H sont les images par φ des générateurs de G

Preuve : On procède par double inclusion.

COROLLAIRE : **Générateurs d'un groupe monogène**

- Lorsque $< a > \approx \mathbb{Z}/n\mathbb{Z}$: Les générateurs de $< a >$ sont : $\{a^p \mid p \in [\![1,n]\!],\ p \wedge n = 1\}$

  Il y en a $\varphi(n)$ *(indicatrice d'Euler !)*

- Lorsque $< a > \approx \mathbb{Z}$: Les générateurs de $< a >$ sont : a et a^{-1}.

4. Etude des groupes cycliques : $\left(\approx \mathbb{Z}/n\mathbb{Z} \right)$

DÉFINITION : **Groupe cyclique**

- Un groupe monogène et FINI est appelé un *groupe cyclique*.
- Un groupe cyclique de cardinal $n \in \mathbb{N}^*$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
- 2 groupes cycliques de même cardinal sont isomorphes.

Exemples :

- $\mathbb{Z}/n\mathbb{Z}$ est cyclique engendré par $\bar{1}$.
- $\mathbb{U}_n$ est cyclique engendré par $e^{\frac{2i\pi}{n}}$.
- Tout sous-groupe monogène d'un groupe fini est cyclique : $< (1\ 2\ 5) >$, $< e^{i3\pi/5} >$

Exemple : $< (1\ 5\ 4\ 2) >$ et U_4 sont isomorphes car ils sont tous les deux monogènes de cardinal 4.

D/ Ils sont tous les deux isomorphes à $\mathbb{Z}/2\mathbb{Z}$.

Contre-exemple

⚠ deux groupes finis de même cardinal ne sont pas forcément isomorphes.

Bien que de même cardinal, nous savons que $(\mathbb{Z}/2\mathbb{Z})^2$ et $\mathbb{Z}/4\mathbb{Z}$ ne sont pas isomorphes.
On en déduit qu'au moins l'un des deux (ici $(\mathbb{Z}/2\mathbb{Z})^2$) n'est pas monogène.

Méthode 2 : Pour montrer qu'un groupe FINI n'est pas monogène

On peut montrer :

- qu'il n'est pas commutatif

  ou
- qu'il n'est pas isomorphe à $\mathbb{Z}/n\mathbb{Z}$. *On utilise pour cela l'équation* $2x = 1$ *ou* $x^2 = 1$.

PROPOSITION : Générateurs de $G =< a >$ cyclique de cardinal n.

Les générateurs de G sont les a^k où $k \wedge n = 1$.
Il y en a $\varphi(n)$.

Preuve : Déjà vu !

Exemples : Déterminer les générateurs de $\mathbb{U}_1$, $\mathbb{U}_2$, $\mathbb{U}_3$ et $\mathbb{U}_{24}$.

7 Ordre d'un élément dans un groupe

1. Définition et propriétés :

DÉFINITION : **Ordre d'un élément** $a \in G$

- Lorsqu'il existe $n \in \mathbb{N}^*$ tel que $a^n = e_G$ on dit que a est *d'ordre fini.*
- Le plus petit $n \in \mathbb{N}^*$ qui convient est appelé *l'ordre* de a et est noté $\mathcal{O}(a)$.

Remarque : ⚠ En notation additive, l'ordre de a est la plus petit $n \in \mathbb{N}^*$ tel que $na = 0_G$.

Exemples :

- L'élément neutre est le seul élément d'ordre 1.
- i est d'ordre 4 et j est d'ordre 3 dans $\mathbb{U}$.
- 2 n'est pas d'ordre fini dans les groupes $(\mathbb{R}^*, \times)$ et $(\mathbb{R}, +)$.
- Les p-cycles sont d'ordre p et les transpositions sont d'ordre 2.
- Les permutations sont d'ordre le PPCM des cardinaux des différentes orbites de la permutation.
- Dans un groupe cyclique de cardinal n, un générateur est d'ordre n.

Exercice : Donner les ordres des éléments de $\mathbb{Z}/8\mathbb{Z}$. Que constatez-vous ?

DÉFINITION : **Ordre d'un groupe**

Dans le cas des groupes finis, le cardinal d'un groupe est également appelé l'*ordre* du groupe.

Exemples : $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{U}_6$ et S_3 sont des groupes d'ordre 6.

LEMME : a est d'ordre n si et seulement si $< a > \approx \mathbb{Z}/n\mathbb{Z}$

Preuve : En reprenant l'application $\varphi : \mathbb{Z} \to < a >$ définie par $\varphi(k) = a^k$.
$\Rightarrow$ Dans ce cas $n \in \ker\varphi \neq \{0\}$ et donc $\ker\varphi = p\mathbb{Z}$, puis par définition de n, $\ker\varphi = n\mathbb{Z}$.
$\Leftarrow$ Dans ce cas on a $\ker\varphi = n\mathbb{Z}$.

THÉORÈME FONDAMENTAL : **Caractérisations de l'ordre d'un élément**

Soit $a \in G$ et $n \in \mathbb{N}^*$.
Les propositions suivantes sont équivalentes.

- a est d'ordre n
- $< a > \approx \mathbb{Z}/n\mathbb{Z}$
- $\mathrm{Card}(< a >) = n$
- $< a >= \{e,\ a,\ a^2,\ \ldots,\ a^{n-1}\}$ distincts 2 à 2

Preuve : Conséquences du lemme précédent.

COROLLAIRE : IMPORTANT !
Si a est d'ordre n alors :

$$\boxed{a^m = e_G \iff m \equiv 0\ [n]}$$

On en déduit alors que : $a^l = a^k \iff l \equiv k\ [n]$.

Preuve : On utilise le fait que $\ker\varphi = n\mathbb{Z}$.
On peut également prouver directement ce résultat par division euclidienne.

L'implication directe $\Rightarrow$ est utilisée pour déterminer l'ordre d'un élément.

2. Exercices

Méthode : Pour prouver que deux éléments a et b ont le même ordre

- On note p l'ordre de a et q l'ordre de b.
- On montre alors que $\begin{cases} a^q = e_G \\ b^p = e_G \end{cases}$

Exemple : Soit x un élément d'ordre fini. Montrer que x et x^{-1} ont le même ordre.

Méthode : Pour déterminer l'ordre d'un élément $a \in G$

- Si c'est possible : on calcule a^2, a^3 ... etc ...jusqu'à obtenir $a^p = e_G$
- Plus généralement : on procède par Analyse/Synthèse :
  - → Analyse : Soit r l'ordre de a, alors ... On trouve un ensemble de valeurs possibles.
  - → Synthèse : On vérifie alors si la plus petite de ces valeurs convient.

Exercice : 14

(∗) Si a est d'ordre n alors a^k est d'ordre $\dfrac{n}{n \wedge k}$.

Preuve :

- Analyse : Soit m l'ordre a^k. On a alors $a^{km} = e$ et donc $mk \equiv 0\ [n]$.
  On constate que mk est alors multiple commun à m et n.
  mk est donc un multiple de $m \vee n$.
- Synthèse : On vérifie que le plus petit élément trouvé en analyse (cad $m \vee n$) convient.

Exercice : 15

(∗) Montrons que si $\begin{cases} h \text{ est d'ordre } n \\ k \text{ est d'ordre } m \end{cases}$ alors $(k,\ h) \in G^2$ est d'ordre $n \vee m$.

Preuve :

- Analyse : Soit p l'ordre de (h, k), alors $(h,\ k)^p = (e_H,\ e_K)$ et donc $\begin{cases} n \mid p \\ m \mid p \end{cases}$.
  p est alors un multiple du PPCM.
- Synthèse : Le PPCM convient !

Exercice : 16

(∗∗) On suppose $H =< h >$ et $K =< k >$ cycliques d'ordres respectifs n et m.

Montrer que $H \times K$ est cyclique ssi $n \wedge m = 1$.

On utilisera le résultat de l'exercice précédent.

Preuve :

$\Rightarrow$ Supposons que $(h_0,\ k_0)$ est générateur de $H \times K$, alors $\begin{cases} h_0 \text{ est générateur de } H \\ k_0 \text{ est générateur de } K \end{cases}$.
Donc h_0 est d'ordre n et k_0 est d'ordre m.
$(h_0,\ k_0)$ est ainsi à la fois d'ordre $n \vee m$ (cf exo précédent) et d'ordre nm (le cardinal du groupe).
Ainsi, $n \vee m = nm$ et donc $n \wedge m = 1$.

$\Leftarrow$ Supposons que $n \wedge m = 1$. Alors $(h,\ k)$ est d'ordre $n \vee m = nm$ égal au cardinal de $H \times K$.
Donc $(h,\ k)$ est générateur du groupe $H \times K$.

3. Eléments d'un groupe fini :

On se demande ici ce que l'on peut dire de l'ordre des éléments d'un groupe fini.

PROPOSITION : Les éléments d'un groupe fini sont d'ordre fini et leur ordre est inférieur à l'ordre du groupe.

Preuve : Immédiat car $< a > \subset G$ qui est fini.

Exercice : 17

(**) Déterminer le nombre d'éléments de $\mathcal{S}_5$ qui sont d'ordre 6.

Preuve : On recherche ces éléments sous la forme de produits de cycles disjoints sachant qu'un cycle de longueur p est d'ordre p et qu'un produit de cycles disjoints est d'ordre le PPCM des ordres des cycles.

THÉORÈME FONDAMENTAL : **LAGRANGE**

Soit G un groupe de cardinal fini $n \in \mathbb{N}^*$.

- Tout élément $a \in G$ vérifie $a^n = e$.
- L'ordre des éléments de G divisent n.

Preuve :

- A connaître dans le cas où le groupe est commutatif.

  On considére $P = \prod_{x \in G} x$ et la bijection $\tau_a : \begin{array}{ccc} G & \longrightarrow & G \\ x & \mapsto & a \star x \end{array}$.

  Nous avons alors $\prod_{x \in G} x = \prod_{x \in G} \tau_a(x)$...
- Immédiat d'après le lemme.

Une version plus générale du théorème de Lagrange dit que le cardinal d'un sous-groupe d'un groupe fini divise l'ordre du groupe.

A retenir !

Lorsque G est un groupe et $a \in G$, l'application $\varphi_a : \begin{array}{ccc} G & \longrightarrow & G \\ x & \mapsto & ax \end{array}$ est bijective.
On en déduit alors l'égalité d'ensembles suivante, utilisée dans certains raisonnements :

$$\{ax \mid x \in G\} = \{x \mid x \in G\}$$

Exemples :

- Dans un groupe à 8 éléments (par exemple U_8), les éléments ne peuvent être que d'ordre 1, 2, 4 ou 8.
- Dans $\mathbb{Z}/6\mathbb{Z}$, donner les ordres des différents éléments.

Exercice : 18
(∗) Montrer que les sous-groupes finis de $\mathbb{U}$ sont les $\mathbb{U}_n$.

COROLLAIRE : Tout groupe fini de cardinal p premier est cyclique. (et donc commutatif !)

Preuve : Les éléments sont d'ordre fini divisant p.
Or, seul e est d'ordre 1 donc les autres éléments sont d'ordre p et engendrent donc le groupe.

8 Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ (HP)

Khûbes

Nous cherchons dans cette partie à déterminer la nature des sous-groupes d'un groupe cyclique.
Par isomorphisme, cela revient à nous intéresser aux sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

THÉORÈME : Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques de cardinal un diviseur de n.

Preuve : Soit H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$.
On considère $a \in [\![1, n-1]\!]$ le plus petit élément tel que $\bar{a} \in H$.
On montre alors en s'inspirant de la démonstration sur les sous-groupes de $\mathbb{Z}$ que $H =< a >$.
Le cardinal de $< a >$ étant l'ordre de a, c'est un diviseur de n.

PROPOSITION : **Réciproquement**

Pour tout $d > 0$ divisant n, $\mathbb{Z}/n\mathbb{Z}$ admet un (unique) sous-groupe de cardinal d.

Preuve : Soit $d \mid n$, on prend $c = n/d$. DESSIN !

- Existence : On montre facilement que $< \bar{c} >= \{\bar{0},\ \bar{c},\ 2\bar{c}, \ldots,\ (d-1)\bar{c}\}$.
- Unicité : Soit H de cardinal d. Montrons que tout $\bar{x} \in H$ est de la forme $\bar{x} = k\bar{c}$.
  Tout élément de H est d'ordre divisant d et donc $\forall \bar{x} \in H$:

  $$d.\bar{x} = \bar{0} \quad \text{donc} \quad n \mid dx \quad \text{donc} \quad c \mid x \quad \text{et donc} \quad H \subset \{\bar{0},\ \bar{c},\ 2\bar{c}, \ldots,\ (d-1)\bar{c}\}$$

  L'égalité s'obtient avec les cardinaux.

Par isomorphisme, le résultat que nous venons de démontrer est vrai pour tous les groupes cycliques.