# Préliminaires

On suppose connues les propriétés élémentaires sur les ensembles ($\cup\ \cap\ \subset\ \supset\ \in\ \ldots$).

**Définition 1 (Relation d'équivalence)** *Soit $E$ un ensemble, et soit $\mathcal{R}$ une relation définie sur $E \times E$. $\mathcal{R}$ est une relation d'équivalence lorsqu'elle vérifie les trois points suivants :*

- $\forall a \in E \quad \mathcal{R}(a,a)$
- $\forall (a,b) \in E^2 \quad \mathcal{R}(a,b) \Rightarrow \mathcal{R}(b,a)$
- $\forall (a,b,c) \in E^3 \quad \mathcal{R}(a,b)$ *et* $\mathcal{R}(b,c) \Rightarrow \mathcal{R}(a,c)$

**Exemple :** Dans le plan orienté et muni d'un point $O$, on peut définir $\mathcal{R}$ de la façon suivante : deux points $M$ et $N$ sont en relation s'il existe une rotation de centre $O$ pour laquelle $N$ est l'image de $M$ (action du groupe des rotations sur le plan).

**Définition 2 (Classe d'équivalence)** *Soit $E$ un ensemble et $\mathcal{R}$ une relation d'équivalence définie sur $E \times E$. On appelle classe d'équivalence de $x \in E$, et on la note usuellement $\dot{x}$ , l'ensemble des éléments en relation avec $x$ :*

$$\dot{x} = \{y \in E / \mathcal{R}(x,y)\}$$

**Proposition 1** *Les classes d'équivalences forment une partition de $E$, c'est à dire qu'elles sont disjointes et que leur réunion est égale à $E$ :*

$$\forall (x,y) \in E^2 \quad \dot{x} = \dot{y} \text{ ou } \dot{x} \cap \dot{y} = \emptyset$$
$$\bigcup_{x \in E} \dot{x} = E$$

**Exercice 1 :** Quelles sont les classes d'équivalence dans l'exemple précédent ?

# 1 Groupes, sous-groupes

**Définition 3** *Soit $G$ un ensemble muni d'une loi interne $*: G \times G \to G$. On dit que $(G,*)$ est un groupe lorsqu'il vérifie les trois propriétés suivantes :*

- *$*$ est associative*
- *Il existe un élément neutre $e$ dans $G$ tel que $\forall a \in G \quad a * e = e * a = a$*
- *Tout élément $a$ de $G$ a un symétrique $b$ dans $G$, souvent noté $a^{-1}$ et qui vérifie $a * b = b * a = e$.*

**Notation :** Par convention, on dit que $a^0 = e$ et pour tout $n \in \mathbb{N}^*$, on a $\underbrace{a * a * \ldots * a}_{n \text{ fois}} = a^n$ et $a^{-n} = (a^n)^{-1}$.

**Remarque :** Si $*$ est commutative, on dit que $G$ est commutatif ou abélien, et on peut utiliser d'autres conventions d'écriture : $+$ au lieu de $*$, $-a$ au lieu de $a^{-1}$, $na$ au lieu de $a^n \ldots$

**Exemples :** (bijections de $E$ dans $E, \circ$), $(\mathbb{C}, +)$, $(\mathbb{C}^*, \times)$, $(\mathcal{L}(E,F), +)$, $(U_n = \{z / z^n = 1\}, \times)$, l'ensemble des isométries conservant un polygone régulier à $n$ côtés : $(D_n, \circ)$.

**Exercice 2 :** Soit $E = (\mathbb{C}^*, \mathbb{C})$ un ensemble sur lequel on définit une loi * :

$$\forall ((a,b),(a',b')) \in E^2 \quad (a,b) * (a',b') = (aa', ab' + b)$$

Montrer que $(E,*)$ est un groupe. À quel groupe connu en géométrie peut-on l'assimiler ?

**Définition 4** *Soit $(G,*)$ un groupe et $H \subset G$. On dit que $H$ est un sous-groupe de $G$ (sous-entendu pour la loi $*$) lorsque $(H,*)$ est un groupe. Ce qui est vérifié dès que :*

- *$H \neq \emptyset$*
- *$*$ est stable dans $H$*
- *$\forall a \in H \quad a^{-1} \in H$*

**Exemple :** Dans le groupe des bijections du plan : groupe des applications affines, groupe des isométries, groupe des similitudes, des similitudes directes, des homothéties-translations, des rotations-translations (isométries directes), des homothéties de centre $O$, des rotations de centre $O$, des translations ...

**Définition 5 (Ordre, cardinal)** *Lorsqu'un groupe $G$ a un nombre fini d'élément, on dit qu'il est fini et son nombre d'éléments est appelé indifféremment ordre ou cardinal.*

**Définition 6 ( et proposition)** *Soit $(G,*)$ un groupe et $A \subset G$, le sous-groupe $H$ de $G$ engendré par la partie $A$ est l'ensemble défini par une des deux égalités équivalentes :*

$$H = \bigcap_{\substack{A \subset G' \subset G \\ G' \text{ ss groupe de } G}} G' \quad \text{ou bien} \quad H = \left\{ a_1^{n_1} * a_2^{n_2} * \dots a_p^{n_p} \text{ avec } (a_1, \dots a_p) \in A^p \text{ et } n_i \in \mathbb{Z} \right\}$$

**Notation :** Le sous-groupe engendré par $A$ est noté $\langle A \rangle$
**Exemple :** Groupe du Rubik's cube
**Exercice 3 :** Dans le plan orienté soit $\Delta$ et $\Delta'$ deux droites parallèles distinctes. Quel est le sous-groupe des transformations du plan engendré par $\{S_\Delta ; S_{\Delta'}\}$ ?

# 2 morphismes

**Définition 7** *Soit $(G,*)$ et $(H,\star)$ deux groupes. On appelle morphisme de groupe toute application $\phi : G \to H$ qui vérifie :*

$$\forall (a,b) \in G^2 \quad \phi(a*b) = \phi(a) \star \phi(b)$$

**Exercice 4 :** Montrer que $\phi(e_G) = e_H$ où $e_G$ et $e_H$ sont les éléments neutres respectifs de $G$ et $H$. Montrer que l'image de l'inverse est l'inverse de l'image.

**Proposition 2** *Soit $\phi : G \to H$ un morphisme de groupes. Le noyau $\ker\phi = \{x \in G / \phi(x) = e_H\}$ et l'image de $\phi$ : $Im\,\phi = \{y \in H / \exists x \in G \text{ tel que } y = \phi(x)\}$ sont des sous-groupes respectivement de $G$ et $H$.*

**Exercice 5 :** Le démontrer

**Proposition 3** *Soit $\phi$ un morphisme de groupe. $\phi$ est injective ssi $\ker\phi = \{e\}$.*

**Définition 8 (Sous-groupe distingué)** *Soit $(G,*)$ un groupe et $H$ un sous groupe de $G$. On dit que $H$ est un sous-groupe distingué de $G$, et on note $H \triangleleft G$, lorsqu'il vérifie :*

$$\forall x \in G, \forall h \in H \quad xhx^{-1} \in H$$

**Exemples :** $\{e\}$, $G$, tous les sous-groupes d'un groupe abélien.

**Proposition 4** *Tout noyau d'un morphisme de groupe est distingué, et réciproquement tout sous groupe distingué peut être considéré comme un noyau de morphisme de groupe.*

**Exercice 6 :** Dans le groupe des similitudes directes, quels sont, parmi les sous-groupes connus déjà cités, les sous-groupes distingués ?

**Définition 9** *Soit $(G,.)$ un groupe et $H$ un sous-groupe de $G$. Alors la relation $\mathcal{R}$ définie par $(x\mathcal{R}y \iff x.y^{-1} \in H)$ est une relation d'équivalence. L'ensemble de ses classes est noté $G/H$*

**Proposition 5** *Soit $(G,.)$ un groupe et $H$ un sous-groupe **distingué** de $G$. Alors :*

$$\forall (x,x') \in G^2, \ \forall y \in G \quad x\mathcal{R}x' \Rightarrow x.y\mathcal{R}x'.y \text{ et } y.x\mathcal{R}y.x'$$

*On peut ainsi définir une loi sur $G/H$ qui lui confère une structure de groupe.*

**Théorème 1 (Lagrange)** *Soit $(G,*)$ un groupe fini et $H$ un sous-groupe de $G$. L'ordre de $H$ divise celui de $G$.*

**Démonstration :** On peut définir comme précédement une relation d'équivalence $\mathcal{R}$ sur $G$ de la façon suivante : $(x\mathcal{R}x'$ ssi $x.x'^{-1} \in H$. On vérifie ensuite que chaque classe d'équivalence a autant d'élément que $H$, et comme ces classes forment une partition de $G$, l'ordre de $H$ divise bien celui de $G$.

**Proposition 6 (fondamentale)** *Soit $\phi : G \to K$ un morphisme de groupe, alors $G/\ker\phi$ est isomorphe à $Im\,\phi$.*

**Exemple :** voir l'exemple précédent. Ou bien $\phi : \mathbb{Z} \to \mathbb{C}^*$, $\phi(n) = i^n$.

# 3 Groupes cycliques

**Définition 10 (Ordre d'un élément)** *Soit $(G, *)$ un groupe d'élément neutre e, et soit $a \in G$. L'ordre de a, s'il existe, est la borne inférieure de l'ensemble $A = \{n \in \mathbb{N}^*,\ a^n = e\}$.*

**Proposition 7** *Dans un groupe fini d'ordre n, tout élément a vérifie $a^n = e$ où e est l'élément neutre.*

**Exemple :** RSA, Zero Knowledge (Fiat-Shamir)
**Exercice 7 :** Trouver un groupe contenant deux éléments $a$ et $b$ d'ordre fini et tels que $ab$ soit d'ordre infini.

**Définition 11 (groupe monogène)** *Un groupe engendré par un seul élément est dit groupe monogène. Si a est cet élément, on le note $< a >$*

**Proposition 8**
1. *$\langle a \rangle = \{a^n,\ n \in \mathbb{Z}\}$*
2. *$\langle a \rangle$ est commutatif*
3. *Si l'ordre de a n'est pas fini alors $\langle a \rangle$ est isomorphe à $(\mathbb{Z}, +)$, sinon $\langle a \rangle$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{N}^*$.*

**Démonstration :** On définit un morphisme de groupe $\phi : (\mathbb{Z}, +) \to \langle a \rangle \ldots$

**Définition 12 (groupe cyclique)** *Les groupes cycliques sont les groupes finis monogènes, autrement dit les groupes $\mathbb{Z}/nZ$ avec $n \in \mathbb{N}^*$*

**Exemple :** Problème du log discret et protocole de Diffie-Hellman
**Exemple :** Dans le groupe des isométries du plan qui laissent invariant un polygone régulier à $n$ côtés centré en O, le sous-groupe des rotations est cyclique.

**Proposition 9** *Tout sous groupe d'un groupe monogène (respectivement cyclique) est monogène (respectivement cyclique)*

# 4 Groupes opérant sur un ensemble

**Définition 13** *Soit $(G, *)$ un groupe et E un ensemble. On dit que G opère sur E lorsqu'on définit une loi externe $. : G \times E \to E$ qui vérifie :*

$$(\forall (a, b) \in G^2\ \forall x \in E \quad (a * b).x = a.(b.x)) \quad (\forall x \in E \quad e.x = x)$$

**Exemple :** Le groupe $D_n$ agit tout naturellement sur les sommets du polygone.

**Définition 14 (orbite)** *Soit $(G, *)$ un groupe opérant sur un ensemble E, l'orbite d'un élément a de E est l'ensemble $O(a) = \{g.a / g \in G\}$*

**Proposition 10** *Les orbites forment une partition de E.*

**Exercice 8 :** Comment fait-on agir le groupe des translations-homothéties sur les droites du plan affine ? Quelle est l'orbite d'une droite ?
**Exercice 9 :** (difficile) Montrer que si $G$ est fini, chaque orbite a un cardinal qui divise l'ordre de $G$

**Définition 15 (conjugaison)** *On dit que G opère par conjugaison sur un de ses sous-groupes distingués H lorsque la loi externe est définie ainsi :*

$$\forall a \in G,\ \forall b \in H \quad a.b = a * b * a^{-1}$$

*Deux éléments d'une même orbite sont alors dit éléments conjugués.*

**Exercice 10 :** Dans le groupe des similitudes, on considère le sous-groupe distingué des isométries. Quelles sont les orbites d'une translation et d'une rotation ?

# 5 Groupe des permutations

**Définition 16 (permutation)** *On appelle permutation d'un ensemble fini $E$, toute application bijective de $E$ dans lui même. On note l'ensemble des bijections $\mathfrak{S}_E$ ou $\mathfrak{S}_n$ si $n$ est le cardinal de $E$.*

**Notation :** Si on considère $E = \{1; 2; 3; 4\}$, la permutation $\sigma$ qui envoie 1 sur 2, 2 sur 3, 3 sur 4 et 4 sur 1 est notée $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

**Proposition 11** *On sait que $\mathfrak{S}_E$ muni de la loi de composition est un groupe fini d'ordre $n!$*

**Programmation :** On peut simuler facilement une permutation d'un ensemble fini à $n$ éléments si on dispose d'une calculatrice qui manipule les matrices. On considère, dans $\mathbb{R}^n$ le sous ensemble $E$ constitué des vecteurs de la base canonique. Les matrices de changement de base, si on impose à la nouvelle base d'être encore une fois la base canonique mais pas forcément dans le même ordre, sont justement des permutations de $E$. Composer des permutations revient alors à multiplier des matrices, ce qui est facile.

**Exemple :** Pour la permutation citée en exemple, on pourrait mettre en mémoire la matrice $\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

**Définition 17 (transposition)** *Une transposition est une permutation qui inverse uniquement deux éléments $a$ et $b$ de $E$. On la note $\tau_{ab}$.*

**Proposition 12** *Toute permutation d'un ensemble $E$ peut s'écrire comme composée de transpositions, autrement dit l'ensemble des transpositions engendre le groupe des permutations.*

**Démonstration :** Il suffit de faire une récurrence sur le cardinal de $E$.

**Définition 18 (cycle)** *Un cycle est une permutation dont les éléments non invariants sont en permutation circulaire. L'ensemble des éléments non invariants est appelé le support du cycle, et le cardinal du support est la longueur du cycle (qui peut être nulle).*

**Notation :** Le cycle du premier exemple est noté tout simplement $(1 \quad 2 \quad 3 \quad 4)$.

**Exercice 11 :** $\begin{pmatrix} a & b & c & d & e & f & g \\ c & b & e & d & a & f & g \end{pmatrix}$ et $\begin{pmatrix} a & b & c & d & e & f & g \\ c & b & f & e & d & a & g \end{pmatrix}$ sont-ils des cycles ?

**Exercice 12 :** Soit $\sigma$ une permutation d'un ensemble $E$. Le groupe cyclique $< \sigma >$ opère alors naturellement sur $E$. Quelle condition doivent vérifier les classes d'équivalence des orbites pour que $\sigma$ soit un cycle ?

**Proposition 13 (commutativité de cycles disjoints)** *Si $\sigma_1$ et $\sigma_2$ sont deux cycles de supports disjoints, alors ils commutent : $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.*

**Proposition 14** *Toute permutation $\sigma$ d'un ensemble $E$ peut s'écrire comme une composition de cycles disjoints (donc qui commutent).*

**Démonstration :** Il suffit de considérer les cycles liés à chaque orbite.

**Proposition 15 (signature)** *Soit $n \in \mathbb{N}^*$, l'application $\epsilon : (\mathfrak{S}_n, \circ) \to (\{-1, 1\}, \times)$ telle que :*

$$\forall \sigma \in \mathfrak{S}_n \quad \epsilon(\sigma) = \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i}$$

*est un morphisme de groupe.*

**Remarque :** $\epsilon(\sigma) = (-1)^{\text{nombre d'inversions dans } \sigma}$

**Définition 19** *$\epsilon(\sigma)$ est appelé signature de $\sigma$*

**Définition 20 (groupe alterné)** *Le noyau de la signature (ensemble des permutations paires) est un sous-groupe de $\mathfrak{S}_n$ appelé groupe alterné et noté $\mathfrak{A}_n$.*

**Exercice 13 :** Décomposer $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 6 & 7 & 1 & 5 & 2 & 9 & 8 \end{pmatrix}$. Signature ? Ordre de $\sigma$ ? À quel groupe est isomorphe le groupe engendré par $\sigma$ ?

**Exercice 14 :** Soit $h = (1\,2)(3\,7)(2\,4)(1\,3)(5\,8)$, calculer $h^{2772}$.

**Exercice 15 :** Déterminer un sous-groupe de $\mathfrak{S}_3$ isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

**Exercice 16 :** Montrer que, bien que 15 divise 5!, il n'existe pas d'élément de $\mathfrak{S}_5$ d'ordre 15.

**Exercice 17 :** Quel est le nombre minimum de permutations nécéssaires pour engendrer $\mathfrak{S}_n$ $(n \in \mathbb{N}^*)$ ?

**Exercice 18 :** Un groupe $G$ est donné par la table suivante :

| * | a | b | c | d | e | f |
|---|---|---|---|---|---|---|
| a | e | f | d | c | a | b |
| b | c | e | a | f | b | d |
| c | b | d | f | a | c | e |
| d | f | c | b | e | d | a |
| e | a | b | c | d | e | f |
| f | d | a | e | b | f | c |

Construire un isomorphisme entre $G$ et un groupe connu.

**Exercice 19 :** Donner une interprétation géométrique du groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

On note $\mathbb{U}$ le groupe multiplicatif des complexes de module 1.

**Exercice 20 :** Parmi les groupes suivants, quel est l'intrus ?

— $(\{z \in \mathbb{U} \,/\, z^6 = 1\}, \times)$
— $(\mathbb{Z}/6\mathbb{Z}, +)$
— $(\mathbb{Z}/7\mathbb{Z})^*, \times)$
— $\mathcal{S}_3$
— Groupe des isométries positives laissant invariant un hexagone
— $\langle\,(1\,2\,3\,4\,5\,6)\,\rangle$

**Exercice 21 :**

1. Vrai ou Faux ? $a = e^{i\theta} \in \mathbb{U}$, $< a >$ fini $\iff \frac{\theta}{\pi} \in \mathbb{Q}$
2. $(\mathbb{Q}, +)$ est-il monogène ?
3. $(\{z \in \mathbb{U} \,/\, \exists n \in \mathbb{N},\, z^n = 1\}, \times)$ est il un groupe ? Si oui, est-il monogène ?

**Exercice 22 :** $(p, q) \in \mathbb{N}^{*2}$. $((\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/q\mathbb{Z}), +)$ est-il cyclique ? (DELCOURT 2.13/2.14)

**Exercice 23 :** Vrai/Faux ? $\langle a \rangle$ et $\langle b \rangle$ cycliques (finis) $\Longrightarrow \langle ab \rangle$ cyclique. (penser à des groupes géométriques)

**Exercice 24 :** Soit $E$ un e.v. de dimension finie et $f$ un endomorphisme bijectif de $E$.
Montrer que $\langle f \rangle$ fini $\Longrightarrow \det f = \pm 1$
Réciproque ? (Toujours la géométrie ...)