Algèbre Linéaire Avancée (1er Semestre)[1]

Philippe Michel

[1]Monday 14$^{\text{th}}$ September, 2020, 13:00

Table des matieres

Introduction 5

Chapitre 1. Le language des ensembles 7
1. Ensembles 7
2. Operations sur les ensembles 9
3. Applications entre ensembles 10
4. Cardinal d'un ensemble 16

Chapitre 2. Groupes 19
1. Le cas du groupe symetrique 19
2. Groupes abstraits 21
3. Sous-groupes 24
4. Morphismes de groupes 27

Chapitre 3. Anneaux et Corps 33
1. Anneaux 33
2. Corps 33
3. Module sur un anneau 33

Chapitre 4. Espaces vectoriels 35

Introduction

Le terme "Algebre" est derive du mot arabe *al-jabr* tire du titre dun ouvrage

Kitab al-mukhtasar fi hisab al-jabr wa-l-muqabala

("Abrege du calcul par la restauration et la comparaison"), du mathematicien d'origine persane Al-Khwarizmi et redige vers 825 (source wikipedia). L'ouvrage fournissait des procedures generales de calcul pour resoudre des problemes pratiques lies aux actes legaux (partage lors d'un heritage, subdivision de terrains et calculs d'aires) qui conduisaient a resoudre des equations lineaires ou quadratiques. Le nom "Al-Khwarizmi" a d'ailleurs donne naissance au mot "Algorithme".

De nos jours le terme "Algebre" designe plutot l'etude et la classification de structures mathematiques formelles liees aux operations. l'*Algebre Lineaire* se concentre plus particulierement sur l'etude des "espaces vectoriels". Cependant avant d'arriver a cette notion, nous auront besoin d'introduire d'autre structures algebrique plus generales,

- Les "groupes",
- les "anneaux"
- et les "corps" (qui sont des anneaux particuliers) ainsi que
- les "modules" sur les anneaux, les espaces vectoriels sont des modules sur des corps.

L'etude des premiers releve de la "theorie des groupes" (qui sera developpee plus en details dans le cours MATH-113) et celle des trois au tres releve de "l'algebre commutative" (qui sera discutee en deuxieme annee) cependant, comme on va le voir, tous ces sujets sont intimement connectes et il est impossible de traiter l'un de ces sujets sans avoir recours aux autres.

Avant cela nous aurons besoin d' introduire le language des *ensembles*.

CHAPITRE 1

Le language des ensembles

Quelques abbreviations:

$$\exists : \text{"il existe"};\ \forall : \text{"quelque soit" ou bien "pour tout"};$$

$$\Longrightarrow: \text{"implique"};\ \Longleftrightarrow \text{ ou } ssi : \text{"equivaut a, si et seulement si"};\ \mid \text{ ou } \ t.q. : \text{"tel que"}$$

$$spdg,\ wlog : \text{"sans perte de generalite " ou "without loss of generality"}$$

$$ops, wma : \text{"on peut supposer " ou "we may assume"}$$

$$spdgops,\ wlogwma : \cdots$$

1. Ensembles

Une definition rigoureuse de la notion d'ensemble et des ensembles de base (comme les entiers naturels) necessiterait au prealable d'introduire de developper *le calcul des predicats du premier ordre* puis une theorie des ensembles munie d'une axiomatique convenable (la plupart du temps ZFC). Comme il ne s'agit pas du sujet du cours, nous ne le ferons pas et nous en remettons a l'intuition du lecteur. Pour un traitement plus complet, nous referons le lecteur au debut du cours "Structures Algebriques" MATH-113 et plus tard au cours de "logique mathematique" MATH-381.

1.1. Un *ensemble* E est une collection d'objets appeles elements de E. Si e est un element de E (e appartient a E), on note cette relation

$$e \in E.$$

Exemple 1.1. Quelques ensembles

- Il existe un (unique) ensemble ne contenant aucun elements:*l'ensemble vide* que l'on notera
$$\emptyset.$$
- $\mathbb{N}$ est l'ensemble des entiers naturels:
$$\mathbb{N} = \{0, 1, 2, 3, \cdots\}.$$
- $\mathbb{Z}$ est l'ensemble des entiers relatifs:
$$\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}.$$
- $\mathbb{Q}$ est l'ensemble des nombres rationels:
$$\mathbb{Q} = \{\frac{p}{q},\ p, q \in \mathbb{Z},\ q \neq 0\}.$$
- $\mathbb{R}$ designera l'ensemble des nombres *reels*. Cet ensemble sera construit rigoureusement dans le cours d'analyse.
- $\mathbb{C}$ designera l'ensemble des nombres *complexes*. Cet ensemble sera construit rigoureusement dans le cours (en admettant l'existence de $\mathbb{R}$).

On designera un ensemble et les elements qu'il contient par la notation "crochets":

$$E = \{\cdots\}.$$

Entre ces crochets $\{\cdots\}$ on mettra soit

- La liste des elements de l'ensembles (si c'est possible) separes par des virgules: on enumere les elements de l'ensemble.
- une formule indiquant qu'on considere les element d'un autre ensemble (disons F) qui verifient une certaine propriete P codee par une formule logique:
  - $\{0, 1, 2, 3\} = \{m \in \mathbb{N},\ m \leqslant 3\}$.
  - $\mathbb{N} = \mathbb{Z}_{\geqslant 0} = \{m \in \mathbb{Z},\ m \geqslant 0\}$.
  - $\mathcal{P} =$ Ensemble des nombres premiers $= \{p \in \mathbb{N},\ d|p \Longrightarrow d = 1 \text{ ou } p\}$.
  - Soit E-EPFL l'ensemble des etudiants de l'EPFL.

$$A := \{e \in \text{E-EPFL},\ 3|\text{SCIPER}(e)\},$$
$$B := \{e \in \text{E-EPFL},\ 3|\text{SCIPER}(e) - 1\},$$
$$C := \{e \in \text{E-EPFL},\ 3|\text{SCIPER}(e) - 2\}.$$

1.2. Sous-ensemble. Etant donne un ensemble E, un *sous-ensemble* de E est un ensemble A tel que tout element de A est contenu dans E: on note cette relation

$$A \subset E.$$

On dit egalement que A est *contenu* (*inclu*) dans E ou que A est une *partie* de E. Si $e \in E$ est un element de E, on note

$$\{e\} \subset E$$

le sous-ensemble de E dont l'unique element est e (le *singleton* e).

Par exemple, on a la chaine d'inclusions

$$\{1\} \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Si A n'est pas contenu dans E, on le notera

$$A \not\subset E.$$

Notons que l'ensemble vide est un sous-ensemble de tout ensemble E:

$$\emptyset \subset E.$$

Deux ensemble sont *egaux* si ils ont les *memes* elements. On a donc l'equivalence

$$E = F \Longleftrightarrow E \subset F \text{ et } F \subset E.$$

En d'autre termes pour montrer que deux ensemble sont egaux il faut et il suffit de montrer que l'un est inclu dans l'autre et l'autre dans le premier: c'est la methode de la *double-inclusion.*

L'ensemble des sous-ensembles de E est note

$$\mathscr{P}(E) = \{A \text{ ensemble},\ A \subset E\}.$$

REMARQUE 1.1. *L'ensemble de tous les ensembles* ENS n'est PAS un ensemble: en effet si c'etait le cas, on pourrait considerer (Russell) l'ensemble de tous les ensembles *ne se contenant pas eux-meme*

$$\text{Ncont} = \{E \text{ ensemble},\ E \not\in E\}$$

et se poser la question de savoir si

$$\text{Ncont} \in \text{Ncont ou bien Ncont} \not\in \text{Ncont}.$$

Pour resoudre ce probleme, on est amene a introduire une notion plus souple que celle d'ensemble appelle *categorie*: l'ensemble de tous les ensembles ENS forme une categorie.

2. Operations sur les ensembles

2.1. Union, intersection. On defini les operations suivante sur l'ensemble $\mathscr{P}(E)$ des parties d'un ensemble: soient $A, B \subset E$

– la reunion de A et B,
$$A \cup B = \{e \in E | e \in A \text{ ou } e \in B\} \subset E.$$
– l'intersection de A et B,
$$A \cap B = \{e \in E | e \in A \text{ et } e \in B\} \subset E.$$
– la difference de A et B,
$$A - B = A \backslash B = \{a \in A | a \notin B\} \subset E.$$
– la difference symetrique de A et B,
$$A \Delta B = A \backslash B \cup B \backslash A \subset E.$$
– Si $A \cap B = \emptyset$, on dit que A et B sont disjoints.

Plus generalement si on dispose de $n \geqslant 2$ sous-ensembles $E_1, \cdots, E_n \subset E$ on note
$$\bigcap_{i=1}^{n} E_i = E_1 \cup \cdots \cup E_n = E_1 \cup (E_2 \cup \cdots \cup E_n) = \{e \in E | \text{ il existe } i \leqslant n,\ e \in E_i\},$$
$$\bigcup_{i=1}^{n} E_i = E_1 \cap \cdots \cap E_n = E_1 \cap (E_2 \cap \cdots \cap E_n) = \{e \in E | \text{ pour tout } i \leqslant n,\ e \in E_i\}.$$

Exercice 1.1. Montrer que
$$A \Delta B = A \cup B - A \cap B.$$

2.2. Produit cartesien. Etant donne deux ensemble A, B leur *produit cartesien* $A \times B$ est l'ensemble des *couples ordonnes* (a, b) avec a un element de A et b un element de B:
$$A \times B = \{(a, b),\ a \in A, b \in B\}.$$
Si un des facteurs est l'ensemble vide le produit cartesien est vide: on a
$$\emptyset \times B = A \times \emptyset = \emptyset.$$

Remarque 2.1. Noter que les ensembles $A \times B$ et $B \times A$ sont distincts sauf si $A = B$ ou A ou B est l'ensemble vide. Si $A = B \neq \emptyset$ et $a \neq a'$, on a
$$(a, a') \neq (a', a).$$

Si on dispose de n ensembles $A_1, \cdots, A_n$ le produit
$$A_1 \times \cdots \times A_n$$
est l'ensemble des n-uples (ordonnes)
$$(a_1, \cdots, a_n),\ a_1 \in A_1, \cdots a_n \in A_n.$$
Si $A_1 = \cdots = A_n = A$ on note ce produit A^n.

2.2.1. *Relation binaire.* Une *relation* (binaire) $\mathcal{R}$ entre (les elements de) deux ensembles A, B est un sous-ensemble
$$\mathcal{R} \subset A \times B.$$
On dit alors que a, b sont *lies par la relation* $\mathcal{R}$ si
$$(a, b) \in \mathcal{R}$$
ce que l'on ecrit
$$a \sim_{\mathcal{R}} b \text{ ou bien } a\mathcal{R}b.$$
Si le sous-ensemble $\mathcal{R}$ a des proprietes supplementaires on dira que la relation a certaines proprietes.

Par exemple si $B = A$ on a les definitions suivantes: soit $\mathcal{R} \subset A \times A$ une relation de A sur lui-meme

– $\mathcal{R}$ est reflexive si
$$\forall a \in A, a\mathcal{R}a$$
(cad $(a, a) \in \mathcal{R}$). En d'autre termes $\Delta A \subset \mathcal{R}$ ou $\Delta A = \{(a, a),\ a \in A\}$ est la diagonale de A.

– $\mathcal{R}$ est symetrique si
$$\forall a, a' \in A,\ a\mathcal{R}a' \Longleftrightarrow a'\mathcal{R}a.$$
En d'autre termes $\mathcal{R}$ est invariant par la symetrie par rapport a la diagonale ΔA
$$s_\Delta : (a, a') \in A \times A \mapsto (a', a) \in A \times A$$
, c'est a dire
$$s_\Delta(\mathcal{R}) = \mathcal{R}.$$

– $\mathcal{R}$ est transitive si
$$\forall a, a', a'' \in A,\ a\mathcal{R}a' \text{ et } a'\mathcal{R}a'' \Longleftrightarrow a\mathcal{R}a''.$$

– $\mathcal{R}$ est une relation d'equivalence si elle est reflexive, symetrique et transitive.

3. Applications entre ensembles

Soient X et Y des ensembles. Une application (egalement fonction) f de X vers Y est la donnee pour tout $x \in X$ d'un unique element $f(x) \in Y$; l'element $f(x)$ est *l'image* de x par f. Une application est notee
$$f : X \mapsto Y.$$

3.1. Graphe d'une application.

Se donner une application
$$f : X \mapsto Y$$
est equivalent a se donner un sous-ensemble
$$\Gamma \subset X \times Y$$
ayant la propriete suivante:

Graphe: Pour tout $x \in X$ le sous-ensemble Γ_x des elements de Γ qui sont de la forme (x, y) pour $y \in Y$,
$$\Gamma_x = \{(x, y) \in \Gamma\},$$
possede un unique element.

Un tel ensemble s'appelle un *graphe*. Le graphe associe a f est le sous ensemble
$$\Gamma(f) = \{(x, f(x)),\ x \in X\} \subset X \times Y.$$

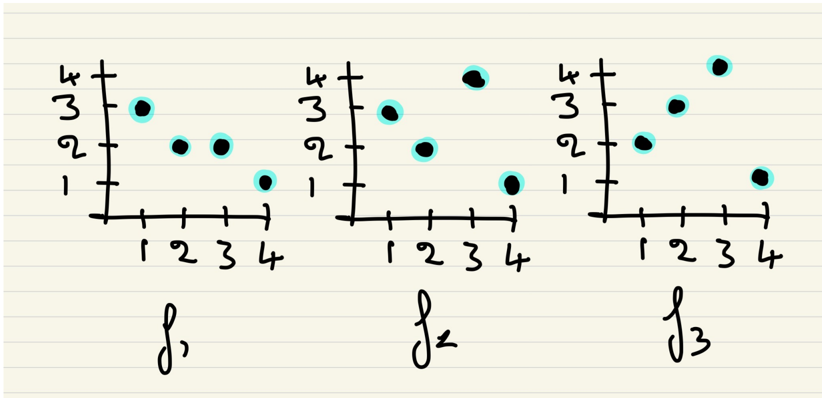

FIGURE 1. Graphes de f_1, f_2, f_3.

En particulier l'ensemble des applications entre X et Y est un ensemble (on l'identifie avec le sous-ensemble de tous les graphes dans $X \times Y$).

NOTATION 1.1. *On note*

$$\mathrm{Hom}_{ENS}(X, Y) \text{ ou encore } \mathcal{F}(X, Y) \text{ ou encore } Y^X$$

l'ensemble des applications de X vers Y 8ou des fonctions de X a valeurs dans Y).

3.1.1. *Exemples.* Soit $y \in Y$, application constante de valeur y est l'application

$$\underline{y} : x \in X \mapsto y \in Y.$$

Son graphe est

$$\Gamma(\underline{y}) = \{(x, y),\ x \in X\} \subset X \times Y.$$

Quand $X = Y$, une autre application importante est *l'identite* de X: c' est l'application

$$\mathrm{Id}_X : x \in X \mapsto x \in X.$$

Son graphe est

$$\Gamma(\mathrm{Id}_X) = \Delta(X) = \{(x, x),\ x \in X\} \subset X \times X$$

et s'appelle la diagonale de $X \times X$.

Soit $X = Y = \{1, 2, 3, 4\}$ et posont

$$f_1 : 1 \mapsto 3,\ 2 \mapsto 2,\ 3 \mapsto 2,\ 4 \mapsto 1$$

$$f_2 : 1 \mapsto 3,\ 2 \mapsto 2,\ 3 \mapsto 4,\ 4 \mapsto 1$$

$$f_3 : 1 \mapsto 2,\ 2 \mapsto 3,\ 3 \mapsto 4,\ 4 \mapsto 1.$$

Les graphes de ces applications sont donnees par les dessins ci-dessus.

Projection. Soit $A_1, \cdots A_n$ des ensemble et

$$\prod_{i=1}^{n} A_i$$

leur produit cartesien. Pour $i = 1, \cdots, n$ la *projection sur le i-eme facteur* est l'application

$$\pi_i : \begin{array}{ccc} \prod_{i=1}^{n} A_i & \mapsto & A_i \\ (a_1, \cdots, a_n) & \mapsto & a_i \end{array}$$

qui a un n-uple associe la i-eme coordonnee.

3.2. Image, preimage. Une application

$$f : X \mapsto Y$$

induit naturellement deux applications entre les ensembles des parties de X et Y:

– L'image

$$\mathrm{Im}(f) : \mathscr{P}(X) \mapsto \mathscr{P}(Y)$$

qui a un sous-ensemble $A \subset X$ associe son image:

$$\mathrm{Im}(f)(A) = \{f(x),\ x \in A\} \subset Y.$$

On notera plus simplement l'image par

$$f(A) = \mathrm{Im}(f)(A).$$

On notera egalement

$$\mathrm{Im}(f) = \mathrm{Im}(f)(X)$$

l'image par f de tout l'ensemble de depart X qu'on appellera l'image de f.

– La preimage

$$\mathrm{preIm}(f) : \mathscr{P}(Y) \mapsto \mathscr{P}(X)$$

qui a un sous-ensemble $B \subset Y$ associe sa preimage:

$$\mathrm{preIm}(f)(B) = \{x \in X,\ f(x) \in B\} \subset Y.$$

On notera plus simplement la preimage par

$$f^{-1}(B) = \mathrm{preIm}(f)(B).$$

Remarque 3.1. On dit quelquefois que la preimage de B est l'ensemble des *antecedents* des element de B par l'application f.

Exemple 3.1. Pour $X = Y = \{1, 2, 3, 4\}$

$$\mathrm{Im}(f_1) = \{1, 2, 3\},\ \mathrm{Im}(f_2) = \{1, 2, 3, 4\},\ \mathrm{Im}(f_3) = \{1, 2, 3, 4\}$$

$$\mathrm{Im}(f_1)(\{2, 3\}) = \{2\},\ \mathrm{Im}(f_2)(\{2, 3\}) = \{2, 4\},\ \mathrm{Im}(f_3)(\{2, 3\}) = \{3, 4\}$$

$$f_1^{-1}(\{2, 4\}) = \{2, 3\},\ f_2^{-1}(\{2, 4\}) = \{2, 3\},\ f_3^{-1}(\{2, 4\}) = \{1, 3\}.$$

Exercice 1.2. Montrer que pour $A \subset X$, on a

$$A \subset f^{-1}(f(A)).$$

Montrer par un exemple qu'en general on n'a pas l'egalite

$$A = f^{-1}(f(A)).$$

Soit $B \subset Y$, existe-t-il des relations d'inclusion entre B et $f(f^{-1}(B))$?

3.3. Injectivite, surjectivite, application reciproque.

- Une application $f : X \mapsto Y$ est *injective* (f est une injection) si pour tout $y \in Y$, $f^{-1}(\{y\})$ (l'ensemble des antecedents de y par f) ne possede pas plus d'un element. On note l'injectivite par
$$f : X \hookrightarrow Y.$$
- Une application $f : X \mapsto Y$ est *surjective* (f est une surjection) si pour tout $y \in Y$, $f^{-1}(\{y\})$ (l'ensemble des antecedents de y par f) possede au moins un element. On note l'injectivite par
$$f : X \twoheadrightarrow Y.$$
- Une application $f : X \mapsto Y$ est *bijective* (f est une bijection) si elle est *injective* et *surjective* : cad si pour tout $y \in Y$, $f^{-1}(\{y\})$ (l'ensemble des antecedents de y par f) possede exactement un element. On note la bijectivite par
$$f : X \xrightarrow{\sim} Y \text{ ou } f : X \simeq Y.$$

Remarque 3.2. Notons qu'une application $f : X \mapsto Y$ est tautologiquement surjective sur son image $\mathrm{Im}(f)$:
$$f : X \twoheadrightarrow \mathrm{Im}(f) \subset Y.$$
En particulier une application injective $f : X \hookrightarrow Y$ defini une bijection
$$f : X \simeq \mathrm{Im}(f).$$
On peut alors identifier les element de X a certains elements de Y via cette bijection.

Notation 1.2. *On note*
$$\mathrm{Inj}(X, Y),\ \mathrm{Surj}(X, Y),\ \mathrm{Bij}(X, Y) \subset \mathrm{Hom}_{ENS}(X, Y)$$
les ensemble d'applications, injective, surjectives et bijectives de X vers Y.

Exemple 3.2. On a:
(1) f_1 n'est ni injective ($f_1^{-1}(\{2\}) = \{2, 3\}$) ni surjective ($4 \notin \mathrm{Im}(f_1)$). f_2 et f_3 sont bijectives.
(2) L'application $n \in \mathbb{Z} \mapsto 2n \in \mathbb{Z}$ est injective mais pas surjective.
(3) L'application $n \in \mathbb{N} \mapsto [n/2] \in \mathbb{N}$ est surjective mais pas injective ($[x]$ designe la partie entiere d'un nombre rationnel x, cad le plus grand entier $\leqslant x$).
(4) L'application polynomiale
$$C : (m, n) \mapsto ((m + n)^2 + m + 3n)/2$$
et une bijection entre $\mathbb{N}^2$ et $\mathbb{N}$ (Cantor).
(5) L'application
$$(m, n) \mapsto m + (n + [(m + 1)/2])^2$$
et une bijection entre $\mathbb{N}^2$ et $\mathbb{N}$.

Exercice 1.3. Demontrer (4). Pour cela
(1) Commencer a verifier qu'on a bien une application de $\mathbb{N}^2$ vers $\mathbb{N}$.
(2) Calculer les valeurs $C(m, n)$ pour $(m, n) \leqslant 5$ et les reporter sur le plan (m, n).

(3) Pour montrer l'injectivite et la surjectivite on pourra etudier l'application $(m, n) \mapsto C(m, n)$ quand on la restreint au sous-ensemble

$$D_k = \{(m, n) \in \mathbb{N}^2,\ m + n = k\}$$

pour $k \geqslant 0$ un entier et regarder les valeurs que prend cette fonction sur ces ensembles.

Dans le cas des ensembles finis dont on connait le nombre d'element on a les proprietes suivantes liant injectivite, surjectivite, bijectivite au nombres d'elements, tres utilie pour demontrer la bijectivite.

Proposition 1.1. *Soient X et Y des ensembles finis possedant respectivement $|X|$ et $|Y|$ elements et $f : X \mapsto Y$ une application entre ces ensembles. On a les proprietes suivantes*

- *Si $f : X \hookrightarrow Y$ est injective alors $|X| \leqslant |Y|$.*
- *Si $f : X \twoheadrightarrow Y$ est surjective alors $|X| \geqslant |Y|$.*
- *Si $f : X \hookrightarrow Y$ est injective et $|X| \geqslant |Y|$ alors $|X| = |Y|$ et f est bijective.*
-
- *Si $f : X \twoheadrightarrow Y$ est surjective et $|X| \leqslant |Y|$ alors $|X| = |Y|$ et f est bijective.*

3.3.1. *Application reciproque d'une bijection.* Soit $f : X \xrightarrow{\sim} Y$ une bijection, alors pour tout $y \in Y$, $f^{-1}(\{y\}) \subset X$ est un element a un seul element

$$f^{-1}(\{y\}) = \{x\},$$

a savoir l'unique element x de X tel que $f(x) = y$, ie. l'unique solution de l'equation dont l'inconnue est a valeur dans X

$$f(X) = y.$$

On peut donc definir une application (l'application *reciproque* de f)

$$f^{-1} : Y \to X$$

definie par

$$f^{-1}(y) = x.$$

Remarque 3.3. On prendra garde que l'on utilise la meme notation pour l'application reciproque d'une application bijective $f^{-1} : Y \xrightarrow{\sim} X$ (qui n'existe que si f est bijective) et l'application *preimage* (qui existe tout le temps)

$$\mathrm{preIm}(f) = f^{-1} : \mathscr{P}(Y) \mapsto \mathscr{P}(X).$$

Meme si les notations sont les memes (par commodite) le contexte devrait etre suffisant pour identifie la signification de la notation.

Exemple 3.3. On a

$$\mathrm{Id}_X^{-1} = \mathrm{Id}_X.$$

3.4. Composition d'applications. Soit X, Y, Z des ensembles et $f : X \mapsto Y$ et $g : Y \mapsto Z$ des applications, a f et g on associe la *composee* de f et g

$$g \circ f : X \mapsto Z$$

est l'application qui va de X a Y via f et de Y a Z via g:

$$\begin{tikzcd} & Y \arrow[dr, "g"] & \\ X \arrow[ur, "f"] \arrow[rr, "g\circ f"] & & Z \end{tikzcd}$$

Elle est definie par

$$x \in X \mapsto g \circ f(x) := g(f(x)) \in Z.$$

En d'autre termes ona une application (dite de composition)

$$(3.1) \qquad \circ : \begin{array}{ccc} \mathrm{Hom}_{ENS}(X,Y) \times \mathrm{Hom}_{ENS}(Y,Z) & \mapsto & \mathrm{Hom}_{ENS}(X,Z) \\ (f,g) & \mapsto & g \circ f \end{array}$$

La composition a les proprietes suivantes:

– Associativite: soient $f : X \mapsto Y$, $g : Y \mapsto Z$, $h : Z \mapsto W$,

$$h \circ (g \circ f) = (h \circ g) \circ f$$

de sorte que la composee des trois applications s'ecrit simplement

$$h \circ g \circ f.$$

– Simplification: soit $f : X \xrightarrow{\sim} Y$ une bijection,

$$f \circ f^{-1} = \mathrm{Id}_X,\ f^{-1} \circ f = \mathrm{Id}_Y.$$

En particulier

$$\mathrm{Id}_X \circ \mathrm{Id}_X = \mathrm{Id}_X.$$

Lemme 1.1. *Soient des applications $f : X \mapsto Y$ et $g : Y \mapsto Z$. Si*

(1) *Si f et g sont injectives, $g \circ f$ est injective.*
(2) *Si f et g sont surjectives, $g \circ f$ est surjective.*
(3) *Si f et g sont bijectives, $g \circ f$ est bijective et*

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Preuve: Exercice. □

Exercice 1.4. Soient des applications $f : X \mapsto Y$ et $g : Y \mapsto Z$. Montrer que si

(1) Si $g \circ f$ est injective alors f est injective.
(2) Si $g \circ f$ est surjective alors g est surjective.

Montrer par des exemples que dans le premier cas g n'est pas forcement injective et que dans le second cas f n'est pas forcement surjective.

On suppose que $g \circ f$ est bijective, que peut on dire (ou ne pas dire) de f et de g ?

Exercice 1.5. Soit $f : X \mapsto Y$ une application.

– Qu'il existe $g : Y \mapsto X$ telle que $g \circ f = \mathrm{Id}_X$ et $f \circ g = \mathrm{Id}_Y$. Montrer qu'alors f est bijective et que g est sa reciproque.
– Montrer que ce n'est pas forcement vrai si on a seulement que $g \circ f = \mathrm{Id}_X$.

3.5. Unions et intersections generalises. On peut generaliser maintenant l'intersection et l'union de sous-ensembles: soit X un ensemble, I un autre ensemble (qu'on suppose non vide) et

$$f : I \mapsto \mathscr{P}(X)$$

une application de I a valeurs dans l'ensemble des sous-ensemble de X. On notera alors pour tout $i \in I$

$$f(i) =: X_i$$

et on notera l'application f sous la forme

$$(X_i)_{i\in I}$$

et on dira que $(X_i)_{i\in I}$ est une *collection* ou un *famille* de sous-ensembles de X indexee par I. On peut alors former les sous-ensembles "union" et "intersection" des $(X_i)_{i\in I}$

$$\bigcup_{i\in I} X_i = \{x \in X, \ \text{ il existe } i \in I, \ x \in X_i\} \subset X$$

$$\bigcap_{i\in I} X_i = \{x \in X, \ \text{ pour tout } i \in I, \ x \in X_i\} \subset X.$$

3.6. Produits cartesiens generalises. De meme on definit le produit cartesien associes a une famille d'ensembles $(X_i)_{i\in I}$ (ou l'on suppose que les X_i sont contenus dans un ensemble d'ensemble:

$$\prod_{i\in I} X_i = \{(x_i)_{i\in I}, \ \forall i \in I, x_i \in X_i\}.$$

Si l'un des $X_i = \emptyset$ alors $\prod_{i\in I} X_i = \emptyset$.

Supposons que tous les X_i soient non-vides. Si I est un ensemble fini (I est en bijection alrs un ensemble de la forme $\{1, \cdots, n\}$, $n \geqslant 1$) alors le produit est non-vide. En revanche si I n'est pas fini, le fait que le produit est *toujours* non-vide est ce qu'on appelle *l'axiome du choix* que l'on peut decider (ou pas) d'inclure dans la theorie axiomatique que l'on se donne au depart.

4. Cardinal d'un ensemble

Définition 1.1. *Soient X et Y deux ensembles. Si il existe une bijection $f : X \xrightarrow{\sim} Y$, on dit que X et Y ont le meme cardinal et on le note*

$$|X| = |Y|.$$

Proposition 1.2. *La relation "avoir le meme cardinal" a la proprietes suivantes*

(1) *Reflexivite:* $|X| = |X|$
(2) *Symetrie:* $|X| = |Y| \Longrightarrow |Y| = |X|$,
(3) *Transitivite:* $|X| = |Y|$ *et* $|Y| = |Z| \Longrightarrow \ |X| = |Z|$.

Preuve: Pour la reflexivite, il suffit de prendre Id_X. Pour la Symetrie, si $f : X \simeq Y$ est une bijection, sa reciproque $f^{-1} : Y \simeq X$ est une bijection. Pour la Transitivite, si $f : X \simeq Y$ et $g : Y \simeq Z$ sont des bijections alors $g \circ f : X \mapsto Z$ est encore une bijection. $\square$

Définition 1.2. *Un ensemble X est fini si il est soit vide, soit en bijection avec un ensemble de la forme $\{1, \cdots, n\}$ pour $n \in \mathbb{N}$ un entier $\geqslant 1$. On ecrit alors*

$$|\emptyset| = 0, \ |X| = n.$$

Un ensemble est infini sinon.

DÉFINITION 1.3. *Un ensemble X est denombrable si il est fini ou a meme cardinal que $\mathbb{N}$. Un ensemble est indenombrable sinon.*

EXEMPLE 4.1. (1) Pour tout ensemble X, $|\mathscr{P}(X)| = |\{0,1\}^X|$.
(2) Si $|X| = n \in \mathbb{N}$, $|\mathscr{P}(X)| = 2^n$.
(3) $|\mathbb{Z}|$ est denombrable.
(4) $\mathbb{Q}$ est denombrable.
(5) $|X| = |Y| = |\mathbb{N}| \Longrightarrow |X| \times |Y| = |\mathbb{N}|$.
(6) (Cantor) Si X est denombrable et infini alors $\mathscr{P}(X)$ n'est pas denombrable.
(7) $\mathbb{R}$ nest pas denombrable (c'est un corollaire du point precedent).

On va demontrer (6) qui est du a G. Cantor.

Preuve: Si X denombrable infini alors on a une identification $X \xrightarrow{\sim} \mathbb{N}$ et donc

$$\mathscr{P}(X) \xrightarrow{\sim} \mathscr{P}(\mathbb{N}) \xrightarrow{\sim} \{0,1\}^{\mathbb{N}}.$$

Il suffit donc de montrer que ce dernier ensemble n'est pas denombrable.

Une application $f : n \in \mathbb{N} \mapsto f(n) \in \{0,1\}$ est simplement une *suite* a valeurs dans $\{0,1\}$. Supposons que l'on ait une bijection

$$\mathbb{N} \xrightarrow{\sim} \{0,1\}^{\mathbb{N}}.$$

Ainsi, a tout entier k on associe la suite $f_k = (f_k(n))_{n \geqslant 0}$ et par hypothese, toute suite f est de la forme f_k pour un certain k. Soit f_C la suite definie par

$$f_C(n) = \begin{cases} 0 & \text{si } f_n(n) = 1 \\ 1 & \text{si } f_n(n) = 0. \end{cases}$$

Alors $f_C = f_{k_0}$ pour un certain $k_0 \geqslant 0$. quelle est la valeur de $f_C(k_0)$? Il y a deux possibilites 0 ou 1:

- Si $f_C(k_0) = 0$ alors $f_{k_0}(k_0) = 1$ par definition de f_C mais alors $0 = f_C(k_0) = f_{k_0}(k_0) = 1$, contradiction.
- Si $f_C(k_0) = 1$ alors $f_C(k_0) = 0$ par definition de f_C mais alors $1 = f_C(k_0) = f_{k_0}(k_0) = 0$, contradiction.

Donc $\{0,1\}^{\mathbb{N}}$ n'est pas denombrable. Cet argument s'appelle l'argument de *la diagonale de Cantor*. □

EXERCICE 1.6. Deduire (7) de (6) (utiliser le developpement binaire d'un nombre reel dans $[0,1[$ masi faire attention que par convention un developpement binaire ne se termine pas par une suite constante de 1 (heureusement l'ensemble des suites a valeurs dans $\{0,1\}$ qui sont ultimement constantes egales a 1 est "petit".

4.1. Le Theoreme de Cantor-Bernstein-Schroeder. On peut raffiner la notion d'egalite des cardinaux:

DÉFINITION 1.4. *Soient X et Y deux ensembles. Si il existe une application injective entre X et Y, $\phi : X \hookrightarrow Y$, on dit que le cardinal de X est plus petit que celui de Y et on note cette relation $|X| \leqslant |Y|$. Si de plus $|X| \neq |Y|$, on le note $|X| < |Y|$.*

Bien evidemment si les ensembles sont finis cette definition correspond a la notion habituelle de cardinal comme etant le nombre d'elements.

EXERCICE 1.7. Montrer la transittivite de cette relation:

$$|X| \leqslant |Y| \text{ et } |Y| \leqslant |Z| \Longrightarrow |X| \leqslant |Z|.$$

En pensant au cas des ensembles finis il est tres tentant de penser que

$$|X| \leqslant |Y| \text{ et } |Y| \leqslant |X| \Longrightarrow |X| = |Y|.$$

Eh bien c'est vrai et c'est le theoreme suivant dont la preuve est donnee en exercice du cours "Structures Algebriques":

THÉORÈME (Cantor-Bernstein-Schroeder). *Soit X et Y deux ensembles (pas necessairement finis). Si il existe une injection $\phi : X \hookrightarrow Y$ et une injection $\psi : Y \hookrightarrow X$ alors il existe une bijection $\varphi : X \simeq Y$. En d'autre termes*

$$|X| \leqslant |Y| \textit{ et } |Y| \leqslant |X| \Longleftrightarrow |X| = |Y|.$$

CHAPITRE 2

Groupes

1. Le cas du groupe symetrique

Soit X un ensemble, on note

$$\mathrm{Bij}(X) = \mathfrak{S}(X) = \mathrm{Aut}_{ENS}(X) = \mathrm{Bij}(X,X) \subset \mathrm{Hom}_{ENS}(X,X)$$

l'ensemble des bijections de X vers lui-meme.

Si X est fini non-vide (on peut alors supposer que $X = \{1, \cdots n\}$) pour $n \geqslant 1$ une tell bijection s'appelle alors une *permutation* de X sur lui-meme.

Cet ensemble admet des structures supplementaires

(1) $\mathrm{Bij}(X)$ est non-vide: $\mathrm{Id}_X \in \mathrm{Bij}(X)$,

(2) $\mathrm{Bij}(X)$ est stable par composition des applications (3.1): soient $f : X \xrightarrow{\sim} X$, $g : X \xrightarrow{\sim} X$ des bijections alors l'application composee, $f \circ g : X \to X$ est encore une bijection (la composee d'applications injectives est injective et la composee d'applications surjectives est surjective). On dispose donc d'une application (de composition):

$$\circ : \begin{array}{ccc} \mathrm{Bij}(X) \times \mathrm{Bij}(X) & \mapsto & \mathrm{Bij}(X) \\ (f,g) & \mapsto & f \circ g \end{array}.$$

(3) La composition est associative:

$$\forall f, g, h \in \mathrm{Bij}(X),\ (f \circ g) \circ h = f \circ (g \circ h) =: f \circ g \circ h.$$

(4) L'identite Id_X a la propriete de *neutralite*:

$$\forall f \in \mathrm{Bij}(X),\ f \circ \mathrm{Id}_X = \mathrm{Id}_X \circ f = f.$$

(5) L'application reciproque $f \mapsto f^{-1}$ envoie $\mathrm{Bij}(X)$ sur $\mathrm{Bij}(X)$

$$.^{-1} : \begin{array}{ccc} \mathrm{Bij}(X) & \mapsto & \mathrm{Bij}(X) \\ f & \mapsto & f^{-1} \end{array}$$

et on a

$$\forall f \in \mathrm{Bij}(X),\ f \circ f^{-1} = f^{-1} \circ f = \mathrm{Id}_X.$$

Ces proprietes font de l'ensemble $\mathrm{Bij}(X)$ un *groupe* qu'on appelle le *groupe symetrique de* X.

1.1. Exemple: les permutations d'un ensemble fini. Considerons le cas ou X est un ensemble fini, non-vide de cardinal $n \geqslant 1$; on peut alors supposer que $X = \{1, \cdots n\}$. On note souvent ce groupe Σ_n.

On rappelle qu'alors $\mathrm{Bij}(X)$ est fini de cardinal

$$|\,\mathrm{Bij}(X)| = n!$$

avec

$$n! = 1.2. \cdots .n,\ n \geqslant 1,\ 0! = 1.$$

Preuve: En effet pour definir une bijection $\sigma : \{1, \cdots n\} \xrightarrow{\sim} \{1, \cdots n\}$. On choist $\sigma(1)$ parmi n elements, puis $\sigma(2)$ parmi les $n-1$ element restants,... Le mieux est de demontrer cette egalite une recurrence sur n. □

On peut representer une permutation par un tableau a deux lignes et n colonnes

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

Ainsi l'identite est ainsi codee par

$$\mathrm{Id}_X = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Par exemple, pour $n = 4$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

est la permutation qui envoie

$$1 \mapsto 3,\ 2 \mapsto 2,\ 3 \mapsto 4,\ 4 \mapsto 1$$

et si on compose σ avec elle-meme on obtient

$$\sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix},$$

qui envoie

$$1 \mapsto 3, 2 \mapsto 2, 3 \mapsto 4, 4 \mapsto 1;$$

iterant une fois de plus, on a

$$\sigma \circ \sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \mathrm{Id}_X.$$

1.1.1. *Cycles.* Un autre exemple est la permutation cyclique

$$\sigma_{+1} = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}$$

qui envoie

$$1 \mapsto 2,\ 2 \mapsto 3, \cdots,\ k \mapsto k+1, \cdots, n \mapsto 1.$$

Pour les permutations cycliques telle que celle ci-dessus, une autre notation (plus compacte) est tres utile: pour $1 \leqslant k \leqslant n$, on se donne

$$\{a_1, \cdots, a_k\} \subset \{1, \cdots n\}$$

des elements *distincts* et on pose

$$(a_1 a_2 \cdots a_k)$$

la permutation qui envoie

$$a_1 \mapsto a_2,\ a_2 \mapsto a_2, \cdots, a_k \mapsto a_1$$

et qui envoie chacun des $n-k$ elements de $\{1, \cdots n\} - \{a_1, \cdots, a_k\}$ sur lui meme: la permutation $(a_1 a_2 \cdots a_k)$ est appellee *cycle de longueur k*.

Par exemple

$$\sigma_{+1} = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix} = (12 \cdots n)$$

est un cycle de longueur n et

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (134)$$

est un cycle de longueur 3.

Transpositions. Un classe particulierement importante de cycle sont ceux de longueur 2, $(a_1 a_2)$, $a_1 \neq a_2$ qu'on les appelle *transpositions*: explicitement $(a_1 a_2)$ echange a_1 et a_2 et envoie tous les autres elements sur eux-meme.

Dans le cours MATH-113 vous demontrerez le theorem de decomposition suivant

THÉORÈME 2.1. *Soit* $\mathfrak{S}_n = \mathrm{Bij}(\{1, \cdots, n\})$ *le groupe de permutations de* n *elements alors*

(1) *Toute permutation s'ecrit comme une composee de cycles,*
(2) *tout cycle s'ecrit comme compose de tranpositions,*
(3) *et donc toute permutation s'ecrit comme compose de tranpositions.*

Par exemple

$$\sigma = (134) = (34) \circ (14)$$

et (le demontrer)

$$(12 \cdots n) = (2n) \circ (23) \circ \cdots \circ (k-1, k) \circ \cdots \circ (n-2, n-1) \circ (1n)$$

2. Groupes abstraits

DÉFINITION 2.1. *Un groupe* $(G, \star, e_G, \cdot^{-1})$ *est la donnee d'un quadruple forme de*

– *d'un ensemble* G *non-vide,*
– *d'une application (appelee loi de composition interne)*

$$\star : \begin{array}{ccc} G \times G & \mapsto & G \\ (g, g') & \mapsto & \star(g, g') =: g \star g' \end{array}$$

– *d'un element* $e_G \in G$ *(appele element neutre),*
– *d'une application (appele inversion)*

$$\cdot^{-1} : \begin{array}{ccc} G & \mapsto & G \\ g & \mapsto & g^{-1} \end{array}$$

ayant les proprietes suivantes:

– *Associativite:* $\forall g, g', g'' \in G,\ (g \star g') \star g'' = g \star (g' \star g'')$.
– *Neutralite de* e_G*:* $\forall g \in G,\ g \star e_G = e_G \star g = g$.
– *Inversibilite:* $\forall g \in G,\ g^{-1} \star g = g \star g^{-1} = e_G$.

REMARQUE 2.1. Par soucis de concision on omettra l'element neutre et l'inversion (voire de la loi de groupe) dans les donnees: notera souvent un groupe par G ou $(G, \star)$.

REMARQUE 2.2. La propriete d'associativite est indispensable et par ailleurs extremement utile: si l'on se donne 3 elements

$$g_1, g_2, g_3 \in G$$

dont on veut former le produit (dans cet ordre): pour cela on calcule $g_{12} = g_1 \star g_2$ puis le produit $g_{12} \star g_3 = (g_1 \star g_2) \star g_3$ et l'associativite nous dit qu'au lieu de cela on aurait pu commencer par calculer $g_{23} = g_2 \star g_3$ et faire le produit

$$g_1 \star g_{23} = g_1 \star (g_2 \star g_3)$$

et l'associativite nous dit que cela de depend pas de la maniere dont on s'y prend:

$$(g_1 \star g_2) \star g_3 = g_1 \star (g_2 \star g_3)$$

et on peut ecrire sans ambiguite ce produit sans parantheses

$$g_1 \star g_2 \star g_3 = g_1 \star (g_2 \star g_3) = (g_1 \star g_2) \star g_3.$$

Dememe si on dispose de n elements $g_1, \cdots, g_n \in G$, on defini sans ambiguite leur produit

$$g_1 \star \cdots \star g_n = \star_{i=1}^n g_i.$$

Proposition 2.1. *Soit G un groupe. On a*

- *Involutivite de l'inversion: $\forall g,\ (g^{-1})^{-1} = g,\ g^{-1} \star g = e_G$.*
- *Unicite de l'element neutre: soit $e'_G \in G$ tel qu'il existe $g \in G$ verifiant $g \star e'_G = g$ alors $e'_G = e_G$. On a la meme conclusion si il existe g' tel que $e'_G \star g' = e'_G$.*
- *Unicite de l'inverse: si $g' \in G$ verifie $g \star g' = e_G$ alors $g' = g^{-1}$.*
- *On a $(g \star g')^{-1} = g'^{-1} \star g^{-1}$.*

Preuve: Dans l'equation

$$g \star e'_G = g$$

on multiple a gauche par g^{-1} ce qui donne

$$g^{-1} \star g \star e'_G = e_G \star e'_G = e'_G = g^{-1} \star g = e_G.$$

Pour le deuxieme cas on multiplie a droite par g'^{-1}. Pour l'unicite de l'inverse: en multipliant l'egalite $g \star g' = e_G$ a gauche par g^{-1} et en utilisant l'associativite on a

$$g \star g' = e_G \Longrightarrow g^{-1} \star g \star g' = g^{-1} \star e_G$$

et $g^{-1} \star g \star g' = g'$ tandis que $g^{-1} \star e_G = g^{-1}$. En particulier, appliquant ce raisonnement a g^{-1} avec $g' = g$, comme $g \star g^{-1} = e_G$ on obtient que $(g^{-1})^{-1} = g$.

Pour le dernier point on a

$$(g'^{-1} \star g^{-1}) \star (g \star g') = g'^{-1} \star (g^{-1}) \star g) \star g' = g'^{-1} \star e_G \star g' = g'^{-1} \star g' = e_G$$

et donc (par unicite de l'inverse)

$$(g \star g')^{-1} = g'^{-1} \star g^{-1}.$$

2.1. Exemples de groupes.

- Comme on l'a vu $(\mathrm{Bij}(X), \circ, \mathrm{Id}_X, \cdot^{-1})$ muni de la composition des applications , de l'identite Id_X et de la reciproque forme un groupe: le *groupe symetrique de X* ou le groupe des *permutations* de X.
- L'ensemble $(\mathbb{Z}, +, 0, -\cdot)$des entiers relatifs $\mathbb{Z}$ muni de l'addition, du zero 0 et de l'oppose $n \mapsto -n$ forme un groupe.
- En revanche $(\mathbb{Z} - \{0\}, +, 0, -\cdot)$ forme des entiers non-nuls muni des memes structures ne forme pas un groupe (il manque un element neutre et d'ailleurs il n'est pas stable par addition).
- L'ensemble $(\mathbb{Q}, +, 0, -\cdot)$ des entiers relatifs $\mathbb{Z}$ muni de l'addition, du zero 0 et de l'oppose $n \mapsto -n$ forme un groupe.
- L'ensemble $(\mathbb{Q}^\times, \times, 1, 1/\cdot)$ avec $\mathbb{Q}^\times = \mathbb{Q} - \{0\}$ est l'ensemble des nombres rationels non-nuls muni de la multiplication, de l'unite 1 et de l'inversion $\lambda \mapsto 1/\lambda$ forme un groupe,
- de meme que le sous-ensemble $\mathbb{Z}^\times := \{\pm 1\}$ muni des memes structures.

– Groupe produit: soient $(G, \star)$ et $(H, *)$ deux groupes. Le groupe produit $(G \times H, \boxtimes)$ est le groupe associe au produit cartesien
$$G \times H = \{(g, h),\ g \in G,\ h \in H\}$$
muni de la loi de composition interne $\boxtimes$ definie par
$$(g, h) \boxtimes (g', h') := (g \star g', h * h'),$$
d'element neutre
$$e_{G\times H} := (e_G, e_H)$$
et d'inverse
$$(g, h)^{-1} := (g^{-1}, h^{-1}).$$

2.1.1. *Notation exponentielle.* Soit $g \in G$ un element d'un groupe. Pour tout entier $n \geqslant 1$, on forme le produit de g avec lui-meme n fois et on le note
$$g \star g \star \cdots \star g = g^n.$$
On a donc
$$g^{n+1} = g^n \star g = g \star g^n.$$
On pose ensuite
$$g^0 = e_G \tag{2.1}$$
et si $n < 0$ est un entier negatif, on pose
$$g^n = (g^{-1})^{-n} = g^{-1} \star \cdots \star g^{-1} (-n = |n| \text{ fois}).$$
cela defini g^n pour $n \in \mathbb{Z}$ On a alors pour tout $m, n \in \mathbb{Z}$
$$g^{m+n} = g^m \star g^n. \tag{2.2}$$
On a alors defini une fonction
$$\exp_g : \begin{array}{ccc} \mathbb{Z} & \mapsto & G \\ n & \mapsto & \exp_g(n) = g^n \end{array} \tag{2.3}$$
qu'on appelle *exponentielle* de n dans la base g. On dira alors que l'image
$$\mathrm{Im}(\exp_g) = \exp_g(\mathbb{Z}) = \{g^n,\ n \in \mathbb{Z}\}$$
est l'ensemble des puissances de g.

2.2. Groupes commutatifs. A l'exception du tout premier exemple, les autres groupes ont une propriete supplementaire: la *commutativite*

Définition 2.2. *Soit $(G, \star)$ un groupe. Deux elements g, h commutent si*
$$g \star h = h \star g.$$
Un groupe G est abelien (ou commutatif) si toutes les paires d'elements de G commutent:
$$g, h \in G,\ g \star h = h \star g.$$

Exercice 2.1. Montrer que si X possede 2 elements ou moins alors $\mathrm{Bij}(X)$ est commutatif. Montrer que si X possede au moins 3 element il ne l'est pas (pour cela choisir trois elements distincts $x_1, x_2, x_3 \in X$ et trouver des bijections σ, τ qui verifient
$$\forall x \in X - \{x_1, x_2, x_3\}, \sigma(x) = x,\ \tau(x) = x$$
et telles que $\sigma \circ \tau = \tau \circ \sigma$.

2.2.1. *Notation additive.* Si le groupe G est commutatif, sa loi de groupe sera souvent notee (mais pas toujours) par une addition (par exemple $+_G$), l'element neutre par le signe "0" (par exemple 0_G) et l'inversion par $-\cdot$: on ecrira

$$g +_G g', g +_G 0_G = 0_G +_G g = g, g +_G (-g) = 0_G$$

et l'exponentielle d'un entier $n \in \mathbb{Z}$ dans la base un element g sera notee sous forme de multiple: pour $n \geqslant 1$,

$$n.g = g +_G \cdots +_G g,\ (-n).g = (-Gg) +_G \cdots +_G (-_G g)(n \text{ fois}),\ 0.g = 0_G,$$

de sorte que (2.2) devient

$$\forall m, n \in \mathbb{Z},\ (m+n).g = m.g +_G n.g.$$

On dispose alors d'une application (de multiplication par g) de $\mathbb{Z}$ a valeurs dans G:

$$\cdot.g : \begin{array}{ccc} \mathbb{Z} & \mapsto & G \\ n & \mapsto & n.g \end{array}$$

On dira alors que son image

$$\mathbb{Z}.g = \{n.g,\ n \in \mathbb{Z}\} \subset G$$

est l'ensemble des multiples de g.

3. Sous-groupes

Avec la notion d'ensemble vient la notion de sous-ensemble. De meme avec la notion de *groupe* vient la notion de *sous-groupe* d'un groupe G: un sous-groupe est un sous-ensemble de G qui herite naturellement des structures additionelles $\star, e_G, \cdot^{-1}$ venant avec la structure de groupe de l'ensemble G.

Définition 2.3. *Soit $(G, \star, e_G, \cdot^{-1})$ un groupe. Un sous-groupe $H \subset G$ est un sous-ensemble de G tel que*

(1) $e_G \in H$.
(2) *H est stable pour la loi de composition interne $\star$:*

$$\forall h, h' \in H,\ h \star h' \in H.$$

(3) *H est stable par l'inversion:*

$$\forall h \in H,\ h^{-1} \in H.$$

Alors si on note $\star_H$ et $\cdot_H^{-1}$ les restrictions de la loi de composition $\star$ et de l'inversion $\cdot^{-1}$ aux sous-ensembles $H \times H$ et H on a

$$\star_H : \begin{array}{ccc} H \times H & \mapsto & H \\ (h, h') & \mapsto & h \star h' \end{array},\quad \cdot_H^{-1} : \begin{array}{ccc} H & \mapsto & H \\ h & \mapsto & h^{-1} \end{array}$$

et $(H, \star_H, e_G, \cdot_H^{-1})$ forme un groupe.

Remarque 3.1. Distinguer les restrictions a H de la loi de composition et de l'inversion est formellement correct mais un peu pedant. La convention universelle est d'omettre cette restriction dans les notations et d'ecrire $(H, \star, e_H = e_G, \cdot^{-1})$ ou plus simplement $(, \star)$.

En fait il n'est pas necessaire de verifer les trois conditions de la definition d'un sous-groupe.

PROPOSITION 2.2 (Critere de sous-groupe). *Pour montrer qu'un sous-ensemble non-vide $\emptyset \neq H \subset G$ est un sous-groupe il suffit de verifier l'un ou l'autre des groupes de proprietes (1) ou (2) ci-dessous:*

(1) (a) $\forall h, h' \in H,\ h \star h' \in H$,
    (b) $\forall h \in H,\ h^{-1} \in H$.
(2) $\forall h, h' \in H,\ h \star h'^{-1} \in H$.

Preuve: On va montrer que si (2) est verifiee alors H est un sous-groupe (le cas (1) est encore plus simple):

(1) En prenant $h' = h$, on a $h \star h^{-1} = e_G \in H$ donc H contient l'element neutre.
(2) En applicant $h \star h'^{-1} \in H$ avec $h = e_G$ on a que si $h' \in H$ alors $h'^{-1} \in H$.
(3) En applicant $h \star h'^{-1} \in H$ avec $h \in H$ et $h'' = h'^{-1}$ et en utilisant que $(h'^{-1})^{-1} = h'$, on a que si $h, h' \in H$ alors $h \star h' \in H$.

□

EXEMPLE 3.1. Voici quelques exemples de sous-groupes:

(1) $\{e_G\} \subset G$ est un sous.-groupe: le sous-groupe trivial.
(2) $G \subset G$ est egalement un sous-groupe.
(3) l'ensemble vide $\emptyset \subset G$ n'est pas un sous-groupe (il lui manque l'element neutre).
(4) $2\mathbb{Z} \subset \mathbb{Z}$ (l'ensemble des entiers pairs) est un sous-groupe.
(5) $1 + 2\mathbb{Z} \subset \mathbb{Z}$ (l'ensemble des entiers impairs) n'est pas un sous-groupe.
(6) Pour tout entier $q \in \mathbb{Z}$,
$$q.\mathbb{Z} = \{q.n, n \in \mathbb{Z}\} \subset \mathbb{Z},$$
l'ensemble des multiples de q est un sous-groupe. Reciproquement, tout sous-groupe de $\mathbb{Z}$ est de la forme $q.\mathbb{Z}$ pour $q \in \mathbb{Z}$.
(7) Pour $g \in G$, l'ensemble des puissance de g
$$\exp_g(\mathbb{Z}) = \{g^n,\ n \in \mathbb{Z}\} \subset G$$
est un sous-groupe commutatif de G.
(8) Si G est commutatif et que la loi de groupe est notee additivement, l'ensemble des multiples de g,
$$\mathbb{Z}.g = \{n.g,\ n \in \mathbb{Z}\} \subset G$$
est un sous-groupe commutatif de G.
(9) Soit X un ensemble $G = \mathrm{Bij}(X)$ et $x \in X$ un element, alors le sous-ensemble
$$\mathrm{Bij}(X)_x = \{\sigma \in \mathrm{Bij}(X),\ \sigma(x) = x\}$$
est un sous-groupe: on l'appelle *le stabilisateur* de x dans $\mathrm{Bij}(X)$.

EXERCICE 2.2. Montrer que tout sous-groupe de $H \subset \mathbb{Z}$ est de la forme $H = q.\mathbb{Z}$ avec $q \in \mathbb{Z}$. Pour cela, on supposera que $H \neq \{0\}$ et on considerera $q > 0$ le plus petit element de H positif et non-nul (on montrera qu'un tel q existe) et que $H = q.\mathbb{Z}$.

Le resultat suivant qu'on demontrera plus tard nous dit que le cas du groupe symetrique est fondamental (voir Exercice 2.5 pour la preuve) :

THÉORÈME 2.2. *Soit G un groupe alors G s'identifie canoniquement a un sous-groupe du groupe $\mathrm{Bij}(G)$ des bijections de G sur lui-meme.*

3.1. Groupe engendre par un ensemble.

Proposition 2.3. *Soit G un groupe et $H_1, H_2 \subset G$ deux sous-groupes alors $H_1 \cap H_2$ est un sous-groupe. Plus generalement soit $H_i, i \in I,\ H_i \in G$ une collection de sous-groupes de G indexes par I alors*

$$\bigcap_{i \in I} H_i$$

est un sous-groupe de G.

Preuve: On utilise le critere de sous-groupe: d'abord $\bigcap_{i \in I} H_i$ est non-vide car il contient l'element neutre e_G. Soient $h, h' \in \bigcap_{i \in I} H_i$ montrons que $h \star h'^{-1} \in \bigcap_{i \in I} H_i$. Il s'agit de montrer que pour tout $i \in I$, $h \star h'^{-1} \in H_i$ mais c'est vrai car H_i est un sous-groupe de G. $\square$Soit

$$\mathcal{G}_A = \{H \subset G \text{ sous-groupe } | A \subset H\}$$

l'ensemble de tous les sous-groupes de G contenant A (cet ensemble est non-vide car G est dedans). Alors l'intersection de ses sous-groupes

$$\bigcap_{H \in \mathcal{G}_A} H$$

est un sous-groupe contenant A et est le plus petit de ces sous-groupes: si H est un sous-groupe H contenant A alors

$$\langle A \rangle \subset H.$$

Définition 2.4. *Le sous-groupe*

$$\langle A \rangle := \bigcap_{H \in \mathcal{G}_A} H$$

s' appelle le sous-groupe engendre par A.

Voici une caracterisation plus constructive de $\langle A \rangle$ (qui justifie la terminologie):

Théorème 2.3. *Soit $A \subset G$ un ensemble, si $A = \emptyset$ alors $\langle A \rangle = \{e_G\}$, sinon on pose*

$$A^{-1} = \{g^{-1},\ g \in A\} \subset G$$

l'image de A par l'inversion, alors

$$\langle A \rangle = \{g_1 \star \cdots \star g_n,\ n \geqslant 1,\ g_i \in A \cup A^{-1}\}.$$

En d'autres termes, $\langle A \rangle$ est l'ensemble des elements de G qu'on peut former en multipliant ensemble des elements de A et de son inverse A^{-1} de toutes les manieres possibles.

Preuve: Si $A = \emptyset$, il est clair que le groupe trivial a les bonnes proprietes. Supposons A non-vide. Il s'agit de montrer que l'ensemble

$$\langle A \rangle' = \{g_1 \star \cdots \star g_n,\ n \geqslant 1,\ g_i \in A \cup A^{-1}\}$$

est un sous-groupe contenant A et qu'il est contenu dans tout sous-groupe $H \supset A$.

Considerant les mots de longueur 1, $g_1,\ g_1 \in A$ on voit que $A \subset \langle A \rangle'$. Soient

$$g_1 \star \cdots \star g_n, g'_1 \star \cdots \star g'_{n'} \in \langle A \rangle'$$

deux tels mots alors

$$g_1 \star \cdots \star g_n \star (g'_1 \star \cdots \star g'_{n'})^{-1} = g_1 \star \cdots \star g_n \star g'^{-1}_{n'} \star \cdots \star g'^{-1}_1 \in \langle A \rangle'.$$

ainsi $\langle A\rangle'$ est un sous-groupe de G contenant A par consequent

$$\langle A\rangle \subset \langle A\rangle'.$$

Enfin, si $A \subset H$ est un autre sous-groupe alors $A^{-1} \in H$ (car H est stable par inversion) et pour tout $n \geqslant 1$ et tout $g_1, \cdots, g_n \in A \cup A^{-1} \subset H$ on a $g_1 \star \cdots \star g_n \in H$ car H est stable par $\star$ et donc $\langle A\rangle' \subset H$ et donc

$$\langle A\rangle' \subset \bigcap_{H \in \mathcal{G}_A} H = \langle A\rangle \subset \langle A\rangle'.$$

□

Exemple 3.2. Soit $g \in G$ alors le sous-groupe engendre par g, $\langle\{g\}\rangle$ vaut

$$\langle\{g\}\rangle = g^{\mathbb{Z}}.$$

4. Morphismes de groupes

Les sous-groupes d'une groupe son les sous-ensemble qui preservent la structur de groupe; les *morphismes* de groupes sont les applications entre deux groupes qui preservent les structures respectives de ces groupes.

Définition 2.5. *Soient $(G, \star)$ et $(H, *)$ deux groupes, un morphisme de groupes $\varphi : G \mapsto H$ est une application telle que*

$$\forall g, g' \in G,\ \varphi(g \star g') = \varphi(g) * \varphi(g').$$

Théorème 2.4. *Soit $\varphi : G \mapsto H$ un morphisme de groupes alors*
(1) $\varphi(e_G) = e_H$,
(2) $\forall g \in G,\ \varphi(g^{-1}) = \varphi(g)^{-1}$,
(3) $\forall g, g' \in G,\ \varphi(g \star g') = \varphi(g) * \varphi(g')$.

Preuve: La troisieme identite est juste une repetition de la definition.

Pour la premiere identite, on a

$$\varphi(g) = \varphi(g \star e_G) = \varphi(g) * \varphi(e_G)$$

et donc $\varphi(e_G) = e_H$ par unicite de l'element neutre dans H.

Pour la deuxieme on a pour tout $g \in G$

$$\varphi(g \star g^{-1}) = \varphi(e_G) = e_H = \varphi(g) * \varphi(g^{-1})$$

et donc $\varphi(g^{-1}) = \varphi(g)^{-1}$ par unicite de l'inverse dans H. □

Exemple 4.1. Les applications suivantes sont des morphismes de groupes

– Soit G un groupe (note multiplicativement) et $g \in G$. Montrer que l'application

$$\exp_g : n \in \mathbb{Z} \mapsto g^n \in G$$

est un morphisme de groupe.

– En particulier pour

$$q \in \mathbb{Z},\ [\times q] : \begin{array}{ccc} \mathbb{Z} & \mapsto & \mathbb{Z} \\ n & \mapsto & qn \end{array}$$

est un morphisme de groupes.

– Les fonctions exponentielles et logarithme

$$\exp : \begin{array}{ccc} (\mathbb{R},+) & \mapsto & (\mathbb{R}_{>0},\times) \\ x & \mapsto & \exp(x) \end{array}, \ \log : \begin{array}{ccc} (\mathbb{R}_{>0},\times) & \mapsto & (\mathbb{R},+) \\ x & \mapsto & \log(x) \end{array}.$$

On peut egalement construire des morphismes de groupes a partir d'autres morphismes de groupes:

Proposition 2.4. *Soient $(G,\star),(H,*),(K,\otimes)$ des groupes et $\varphi : G \mapsto H$ et $\psi : H \mapsto K$ des morphismes de groupes alors la composee $\psi \circ \varphi : G \mapsto K$ est un morphisme de groupes.*

Preuve: Soit $g, g' \in G$ alors

$$\psi \circ \varphi(g \star g') = \psi(\varphi(g \star g')) = \psi(\varphi(g) * \varphi(g')) = \psi(\varphi(g)) \otimes \psi(\varphi(g')) = \psi \circ \varphi(g) \otimes \psi \circ \varphi(g').$$

□

Ensuite les morphismes de groupes bijectifs sont stable par l'application reciproque:

Proposition 2.5. *Soit $\varphi : G \mapsto$ un morphisme de groupe bijectif alors l'application reciproque $\varphi^{-1} \in \mathrm{Hom}_{ENS}(H,G)$ est un morphisme de groupe bijectif.*

Preuve: Il faut montrer que pour $h, h' \in H$

$$\varphi^{-1}(h * h') = \varphi^{-1}(h) \star \varphi^{-1}(h').$$

Soit $g = \varphi^{-1}(h),\ g' = \varphi^{-1}(h')$ alors

$$\varphi(g \star g') = \varphi(g) * \varphi(g') = \varphi(\varphi^{-1}(h)) * \varphi(\varphi^{-1}(h')) = h * h'.$$

Ainsi $g \star g' \in \varphi^{-1}(\{h * h'\})$ mais comme φ est bijective $\varphi^{-1}(\{h * h'\})$ ne possede qu'un seul element et comme $\varphi^{-1}(h * h')$ en fait partie (puisque $\varphi(\varphi^{-1}(h * h')) = h * h'$) on a

$$\varphi^{-1}(h) \star \varphi^{-1}(h') = g \star g' = \varphi^{-1}(h * h')$$

□

Notation. On notera

– $\mathrm{Hom}_{Gr}(G,H)$ l'ensemble des morphismes de groupes de G vers H,
– $\mathrm{Inj}_{Gr}(G,H)$ l'ensemble des morphisme injectifs (qu'on appelle egalement monomorphismes de groupes),
– $\mathrm{Surj}_{Gr}(G,H)$ l'ensemble des morphisme surjectifs (qu'on appelle egalement epimorphismes de groupes), et
– $\mathrm{Iso}_{Gr}(G,H)$, l'ensemble des morphisme de groupes bijectifs (qu'on appelle egalement isomorphismes de groupes).
– Si $H = G$, on ecrit notera ces ensembles

$$\mathrm{Hom}_{Gr}(G),\ \mathrm{Inj}_{Gr}(G),\ \mathrm{Surj}_{Gr}(G),\ \mathrm{Iso}_{Gr}(G)$$

et par ailleurs on ecrira egalement

$$\mathrm{Hom}_{Gr}(G) = \mathrm{End}_{Gr}(G)$$

(qu'on appelle egalement endomorphismes de groupe) et

$$\mathrm{Iso}_{Gr}(G) = \mathrm{Aut}_{Gr}(G)$$

(qu'on appelle egalement automorphismes de groupe).

4.1. Noyau, Image. Les morphismes preserve la structure de sous-groupe:

PROPOSITION 2.6. *Soit $\varphi \in \mathrm{Hom}_{Gr}(G, H)$ un morphisme de groupes. Soit $K \subset G$ un sous-groupe alors $\varphi(K) \subset H$ est un sous-groupe. En particulier l'image de φ, $\varphi(G) = \mathrm{Im}(\varphi)$ est un sous-groupe de H.*

Preuve: Soit $h, h' \in \varphi(K)$, on veut montrer que $h * h'^{-1} \in \varphi(K)$. Par definition il existe $k, k' \in K$ tels que $\varphi(k) = h, \varphi(k') = h'$ et

$$h * h'^{-1} = \varphi(k) * \varphi(k')^{-1} = \varphi(k \star k'^{-1}) \in \varphi(K)$$

car $k \star k'^{-1} \in K$ puisque K est un sous-groupe. □

PROPOSITION 2.7. *Soit $\varphi \in \mathrm{Hom}_{Gr}(G, H)$ un morphisme de groupes. Soit $L \subset H$ un sous-groupe de H, alors l'image inverse*

$$\varphi^{-1}(L) = \{g \in G,\ \varphi(g) \in L\} \in G$$

est un sous-groupe de G. En particulier $\varphi^{-1}(e_H)$ est un sous-groupe de G

Preuve: Soit $g, g' \in \varphi^{-1}(L)$ alors montrons que $\varphi(g \star g'^{-1}) \in L$. On a

$$\varphi(g \star g'^{-1}) = \varphi(g) * \varphi(g')^{-1} \in L$$

car $\varphi(g), \varphi(g') \in L$ par definition et L est un sous-groupe. □

DÉFINITION 2.6. *Le sous-groupe $\varphi^{-1}(e_H)$ s'appele le noyau de φ et est note*

$$\ker(\varphi) = \varphi^{-1}(e_H) = \{g \in G,\ \varphi(g) = e_H\}.$$

L'importance du noyan vient du fait qu'il permet de tester facilement si un morphisme est injectif.

THÉORÈME 2.5 (Critere d'injectivite). *Soit $\varphi \in \mathrm{Hom}_{Gr}(G, H)$ un morphisme de groupes alors les proprietes suivantes sont equivalentes*

(1) *φ est injectif,*
(2) $\ker(\varphi) = \{e_G\}$.

Preuve: Supposons φ injectif alors $\ker(\varphi) = \{g \in G,\ \varphi(g) = e_H\}$ possede au plus un element. Mais comme $\varphi(e_G) = e_H$ on a $\ker(\varphi) = \{e_G\}$.

Supposons que $\ker(\varphi) = \{e_G\}$; on veut montrer que pour tout $h \in H$,

$$\varphi^{-1}(h) = \{g \in G,\ \varphi(g) = h\}$$

possede au plus un element. Soient $g, g' \in \varphi^{-1}(h)$ (si l'ensemble est vide on a fini) alors

$$\varphi(g) = \varphi(g') = h$$

et

$$\varphi(g) * \varphi(g')^{-1} = h * h^{-1} = e_H$$

mais

$$e_H = \varphi(g) * \varphi(g')^{-1} = \varphi(g \star g'^{-1})$$

donc $g \star g'^{-1} \in \ker(\varphi) = \{e_G\}$ et

$$g \star g'^{-1} = e_G \Longrightarrow g = g'$$

et donc $\varphi^{-1}(h)$ possede au plus un element. □

Exercice 2.3. Soit $h \in H$ montrer que
$$\varphi^{-1}(\{h\})$$
est soit vide soit qu'il existe $g \in G$ tel que
$$\varphi^{-1}(\{h\}) = g \star \ker(\varphi) = \ker(\varphi) \star g$$
ou
$$g \star \ker(\varphi) = \{g \star k,\ k \in \ker(\varphi)\}$$
et
$$\ker(\varphi) \star g = \{k \star g,\ k \in \ker(\varphi)\}.$$

Exercice 2.4. Dans le cas du morphisme
$$\exp_g : n \in \mathbb{Z} \mapsto g^n \in G,$$
on a donc $\ker(\exp_g) = q.\mathbb{Z}$ avec $q \in \mathbb{N}$ (car tous les sous-groupes de $\mathbb{Z}$ sont de cette forme). Montrer que si $\ker(\exp_g) = \{0\}$ alors $g^{\mathbb{Z}}$ est infini isomorphe a $\mathbb{Z}$ et que si $\ker(\exp_g) = q.\mathbb{Z},\ q > 0$ alors
$$g^{\mathbb{Z}} = \{g^0 = E_G, g, \cdots, g^{q-1}\}$$
est fini de cardinal q.

On dit alors que g est d'ordre fini et que sont ordre est $\mathrm{ord}(g) = q$ 8et on ecrit $\mathrm{ord}(g) = \infty$ sinon.

4.2. Exemple: la conjugaison dans un groupe. Soit $(G, .)$ un groupe et $g \in G$ un element. La conjugaison par g est l'application
$$\mathrm{Ad}_g : \begin{array}{ccc} G & \mapsto & G \\ h & \mapsto & g.h.g^{-1}. \end{array}$$

Proposition 2.8. *Pour tout g, l'application Ad_g est un morphisme de groupe bijectif et dont l'application reciproque vaut*
$$\mathrm{Ad}_g^{-1} = \mathrm{Ad}_{g^{-1}} : G \xrightarrow{\sim} G.$$
De plus l'application
$$\mathrm{Ad} : \begin{array}{ccc} G & \mapsto & \mathrm{Bij}(G) \\ g & \mapsto & \mathrm{Ad}_g \end{array}$$
est un morphisme de groupes.

Preuve: Calculons (comme $g.g^{-1} = e_G$)
$$\mathrm{Ad}_g(h.h') = g.h.h'.g^{-1} = g.h.e_G.h'.g^{-1} = g.h.g.g^{-1}.h'.g^{-1} = \mathrm{Ad}_g(h).\mathrm{Ad}_g(h').$$
Verifions que Ad_g est injective en calculant son noyau:
$$\ker(\mathrm{Ad}_g) = \{h \in G, g.h.g^{-1} = e_G\}$$
mais
$$g.h.g^{-1} = e_G \Longrightarrow g.h = g \Longrightarrow h = e_G$$
(en multipliant a droite par g et a gauche par g^{-1}. Notons ensuite que pour tout $h' \in G$
$$\mathrm{Ad}_g(g^{-1}.h'.g) = g.g^{-1}.h'.g.g^{-1} = h'$$
donc $h' \in \mathrm{Im}(\mathrm{Ad}_g)$ et l'application est surjective. En fait on a pour tout $h \in G$
$$\mathrm{Ad}_{g^{-1}}(\mathrm{Ad}_g(h)) = h,\ \mathrm{Ad}_g(\mathrm{Ad}_{g^{-1}}(h)) = h$$

de sorte que $\mathrm{Ad}_{g^{-1}}$ est la reciproque de Ad_g. Ainsi $\mathrm{Ad}_g \in \mathrm{Bij}(G)$.

On a pour tout $g, g' \in G$, $h \in G$

$$\mathrm{Ad}_g \circ \mathrm{Ad}_{g'}(h) = g.g'.h.g'^{-1}.g^{-1} = \mathrm{Ad}_{g.g'}(h)$$

de sorte que

$$\mathrm{Ad}_g \circ \mathrm{Ad}_{g'} = \mathrm{Ad}_{g.g'}$$

et l'application $\mathrm{Ad} : G \mapsto \mathrm{Bij}(G)$ est bien un morphisme de groupes (dont l'image est contenue dans $\mathrm{Aut}_{Gr}(G)$). $\square$

Remarque 4.1. Le noyau de Ad est le sous-groupe

$$\ker(\mathrm{Ad}) = \{g \in G,\ \mathrm{Ad}_g = \mathrm{Id}_G\} = \{g \in G,\ \forall h \in G,\ g.h.g^{-1} = h\}$$

$$= \{g \in G,\ \forall h \in G,\ g.h = h.g\}$$

est l'ensemble des elements de G qui commutent avec tous les elements de G, on appelle ce sous-groupe le *centre de* G et on le note

$$Z(G).$$

4.3. Translations dans un groupe. Soit $(G, .)$ un groupe et $g \in G$, l'application de translation a gauche par g est l'application

$$t_g : \begin{array}{ccc} G & \mapsto & G \\ g' & \mapsto & g.g' \end{array}.$$

Cette application n'est PAS un morphisme de groupe en general: elle ne l'est que si $g = e_G$. En effet si $g = e_G$, on a $t_g(g') = e_g.g' = g'$ et $t_{e_G} = \mathrm{Id}_G$. Sinon on a

$$t_g(e_G)0g.e_G = g \neq e_G$$

donc t_g, 'est pas un morphisme de groupes.

En revanche $t_g \in \mathrm{Bij}(G)$. En effet, t_g admet $t_{g^{-1}}$ comme application reciproque:

$$t_{g^{-1}} \circ t_g(g') = g^{-1}.g.g' = g'$$

et donc $t_{g^{-1}} \circ t_g = \mathrm{Id}_G$ et de meme $t_g \circ t_{g^{-1}} = \mathrm{Id}_G$.

Exercice 2.5. Montrer que l'application translation a gauche

$$t_. : \begin{array}{ccc} G & \mapsto & \mathrm{Bij}(G) \\ g & \mapsto & t_g \end{array}$$

est un morphisme de groupes de $(G, .)$ vers $(\mathrm{Bij}(G), \circ)$ qui est injectif. Ainsi

$$G \xrightarrow{\sim} t_G \subset \mathrm{Bij}(G)$$

et donc G est isomorphe a un sous-groupe de $\mathrm{Bij}(G)$: le groupe des translations a gauche sur l'ensemble G.

4.4. Proprietes des ensembles de morphismes. Comme on l'a vu les morphismes sont stables par composition

PROPOSITION. *Soient* $(G,\star),(H,*),(K,\otimes)$ *des groupes et* $\varphi : G \mapsto H$ *et* $\psi : H \mapsto K$ *des morphismes de groupes alors la composee* $\psi\circ\varphi : G \mapsto K$ *est un morphisme de groupes.*

Ainsi que par l'application reciproque:

PROPOSITION. *Soit* $\varphi \in \mathrm{Iso}_{Gr}(G,H)$ *un morphisme de groupe bijectif alors l'application reciproque* $\varphi^{-1} \in \mathrm{Hom}_{ENS}(H,G)$ *est un morphisme de groupe bijectif. Ainsi l'application reciproque* $\cdot^{-1}$ *envoie* $\mathrm{Iso}_{Gr}(G,H)$ *sur* $\mathrm{Iso}_{Gr}(H,G)$*.*

Soient G,H deux groupes tels que $\mathrm{Iso}_{Gr}(G,H)\neq\emptyset$ et il existe donc un isomorphisme de groupes

$$\varphi : G \xrightarrow{\sim} H.$$

On dit alors que G et H sont *isomorphes* et one le note

$$G \simeq_{Gr} H.$$

Si c'est le cas, – pour autant que l'on soit interesse par les structures de groupes – G et H ont exactement les meme proprietes et peuvent etre identifies l'un a l'autre comme groupes via les morphismes φ et φ^{-1}.

EXERCICE 2.6. montrer que la relation pour deux groupes d'etre isomorphes est une relation d'equivalence sur la categorie des groupes (qui n'est pas un ensemble): soient G,H,K des groupes,

(1) on a $G \simeq_{Gr} G$.
(2) Si $G \simeq_{Gr} H$ alors $H \simeq_{Gr} G$,
(3) si $G \simeq_{Gr} H$ et $H \simeq_{Gr} K$ alors $G \simeq_{Gr} K$.

4.5. Le groupe des automorphismes d'un groupe. Regardons maintenant ce qui ce passe si $G = H$.

COROLLAIRE 2.1. *L'ensemble* $\mathrm{Aut}_{Gr}(G) \subset \mathrm{Bij}_{ENS}(G)$ *est un sous-groupe pour la composition* $\circ$*.*

Preuve: On a vu que Id_G est un morphisme de groupes qui est bijectif et de reciproque Id_G de sorte que $\mathrm{Id}_G \in \mathrm{Aut}_{Gr}(G)$. De plus on a vu que si $\varphi\in\mathrm{Aut}_{Gr}(G)$ alors $\varphi^{-1}\in\mathrm{Aut}_{Gr}(G)$. Il suffit alors de montrer que si $\varphi,\psi\in\mathrm{Aut}_{Gr}(G)$, $\varphi\circ\psi\in\mathrm{Aut}_{Gr}(G)$. On a vu que $\varphi\circ\psi\in\mathrm{End}_{Gr}(G)$ et comme la composee de deux applications bijectives est bijective $\varphi\circ\psi\in\mathrm{Aut}_{Gr}(G)$. □

EXERCICE 2.7. Soient G et H deux groupes. On suppose que $\mathrm{Iso}_{Gr}(G,H)\neq\emptyset$. Montrer que pour tout $\varphi\in\mathrm{Iso}_{Gr}(G,H)$,

$$\mathrm{Iso}_{Gr}(G,H) = \varphi\circ\mathrm{Aut}_{Gr}(G) = \mathrm{Aut}_{Gr}(H)\circ\varphi$$

avec

$$\varphi\circ\mathrm{Aut}_{Gr}(G) = \{\varphi\circ\psi,\ \psi\in\mathrm{Aut}_{Gr}(G)\}$$

et

$$\mathrm{Aut}_{Gr}(H)\circ\varphi = \{\psi\circ\varphi,\ \phi\in\mathrm{Aut}_{Gr}(H)\}.$$

CHAPITRE 3

Anneaux et Corps

Un Anneau pour les gouverner tous,
Un Anneau pour les trouver,
Un Anneau pour les amener tous,
Et dans les ténèbres les lier

1. Anneaux

1.1. Sous-anneau.

1.2. Morphismes.

1.3. Noyau, Image.

2. Corps

2.1. Corps des fractions.

2.2. Caracteristique.

2.3. Corps finis.

2.4. Sous-corps premier.

3. Module sur un anneau

3.1. Morphismes.

3.2. Noyau, Image.

3.3. Algebre sur un anneau.

CHAPITRE 4

Espaces vectoriels