GROUPES

PLAN

I : Propriétés usuelles

1– Loi de composition interne

a) Définition :
Soit E un ensemble. On appelle loi de composition interne de E, notée par exemple $*$, une opération qui permet d'associer, à deux éléments quelconques de E a et b, un troisième élément noté $a * b$.

Exemples : Les lois de compositions internes les plus courantes sont :

- $+$ dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.
- $-$ dans les mêmes ensembles.
- $\times$ dans les mêmes ensembles.
- $/$ dans $\mathbb{Q}^*$, $\mathbb{R}^*$, ou $\mathbb{C}^*$.
- div (division entière) dans $\mathbb{N}^*$ ou $\mathbb{Z}^*$.
- $\circ$ dans l'ensemble des applications de E dans E.
- $\cap$ dans l'ensemble $E = \mathcal{P}(\Omega)$ des parties d'un ensemble Ω.
- $\cup$ dans l'ensemble des parties d'un ensemble.

b) Associativité :
Soit E *un ensemble muni d'une loi de composition interne notée* $*$. *Cette loi est dite associative si :*

$\forall\, a \in E, \forall\, b \in E, \forall\, c \in E, (a * b) * c = a * (b * c)$

L'intérêt d'une telle notion est que les parenthèse deviennent inutiles, la notation $a * b * c$ valant indifféremment l'une ou l'autre des expressions. Les lois suivantes, dans les ensembles du paragraphe précédent, sont associatives : +, ×, o, ∩, ∪. Les lois suivantes ne le sont pas : –, /, div.

On notera que l'absence de parenthèses dans l'écriture :

$$7 - 5 - 1 = 1$$

signifie implicitement qu'une convention est adoptée pour distinguer entre $(7 - 5) - 1$ et $7 - (5 - 1)$, la convention étant ici *que le calcul se fait de gauche à droite*, mais rien ne nous aurait empêché de prendre la convention inverse : faire les calculs de droite à gauche. Ce qui aurait conduit au résultat, qui nous paraît faux : $7 - 5 - 1 = 3$!!
Quant à la notation *a*/*b*/*c*, elle est à éviter, aucune convention n'ayant été définie à son sujet.

c) Commutativité :
Soit E *un ensemble muni d'une loi de composition interne notée* $*$. *Cette loi est dite commutative si :*

$$\forall\, a \in \mathrm{E},\ \forall\, b \in \mathrm{E},\ a * b = b * a$$

L'intérêt d'une telle notion est que l'ordre dans lequel les éléments sont placés est indifférent. Les lois suivantes, dans les ensembles du paragraphe précédent, sont commutatives : +, ×, ∩, ∪. Les lois suivantes ne le sont pas : o (sauf si les fonctions sont définies sur un ensemble possédant un seul élément), –, /, div.

Dans le cas d'une loi $*$ commutative et associative, l'expression suivante possède un sens :

$$\mathop{\Large *}_{i \in \mathrm{I}} x_i$$

où I est un ensemble fini d'indices. Par exemple, si I = {1,...,*n*}, l'expression précédente est égale à $x_1 * x_2 * \ldots * x_n$, l'ordre des termes étant indifférent.

Exemples :

$\sum_{i=1}^{n} x_i$ désigne la somme des éléments x_i

$\prod_{i=1}^{n} x_i$ désigne le produit des éléments x_i

$\bigcap_{i \in \mathrm{I}} \mathrm{A}_i$ désigne l'intersection des parties A_i

$\bigcup_{i \in \mathrm{I}} \mathrm{A}_i$ désigne la réunion des parties A_i

On notera, que, si I et J sont deux ensembles disjoints d'indices, on a :

$$\mathop{\Large *}_{i \in \mathrm{I} \cup \mathrm{J}} x_i = \mathop{\Large *}_{i \in \mathrm{I}} x_i * \mathop{\Large *}_{i \in \mathrm{J}} x_i \qquad \text{(i)}$$

Quelle formule donner si I et J ne sont pas disjoints ? Si l'un des ensembles est vide ? Où retrouve–t–on des conventions analogues (penser à 0! par exemple) ?

d) Elément neutre :
Soit E *muni d'une loi interne* $*$. *On dit que e est élément neutre de la loi* $*$ *si :*

$\forall\, a \in \mathrm{E},\ a * e = e * a = a$

EXEMPLES :
Le neutre de + est 0. Celui de $\times$ est 1. Celui de $\circ$ est Id. Celui de $\cap$ est Ω (l'ensemble entier). Celui de $\cup$ est $\varnothing$. – et / n'ont pas d'éléments neutres. Si $*$ est associative, commutative, et admet un élément neutre *e*, alors la formule (i) nous conduit à poser :

$$\mathop{\Large *}_{i \in \varnothing} x_i = e$$

Le neutre, s'il existe est unique. En effet, si *e* et *e*' sont deux neutres, on a :
$e * e' = e$ car *e*' est neutre
$e * e' = e'$ car *e* est neutre
donc $e = e'$.

e) Elément symétrique :
Soit E *muni d'une loi* $*$*, et d'un élément neutre e. On appelle symétrique d'un élément x un élément x' tel que* :
$x * x' = x' * x = e$

EXEMPLES :
Le symétrique de *x* pour + est $-x$ (appelé opposé de x).
Le symétrique de *x* non nul pour $\times$ est $\frac{1}{x}$ (appelé inverse de *x*)
Le symétrique de *f* bijective pour $\circ$ est f^{-1} (appelé réciproque)

Il n'y a en général pas de symétrique pour $\cap$ et $\cup$.

– et /, n'ayant aucune propriété particulière, apparaissent ici comme symétrisations des opérations + et $\times$. On ne les considère donc plus comme des lois.

Le symétrique, s'il existe, et si la loi est associative, est unique. En effet, si *x*' et *x*'' sont deux symétriques de *x*, alors on a :
$x' * x * x'' = (x' * x) * x'' = e * x'' = x''$
$= x' * (x * x'') = x' * e = x'$.
donc $x' = x''$. Ce symétrique est souvent noté x^{-1}.

EXERCICE : Si $*$ est associative, commutative, admet un élément neutre *e*, et si tout élément admet un symétrique, alors on a, avec I et J quelconques :

$$\mathop{\Large *}_{i \in I \cup J} x_i = \mathop{\Large *}_{i \in I} x_i * \mathop{\Large *}_{i \in J} x_i * \left(\mathop{\Large *}_{i \in I \cap J} x_i\right)^{-1}$$

2– Définition d'un groupe
Un ensemble (G,$*$) *est un groupe si* :
i) G *est non vide.*
ii) $*$ *est une loi de composition interne.*
iii) $*$ *est associative.*
iv) $*$ *admet un élément neutre e.*

v) *tout x de e admet un symétrique x'*.

Si, en outre, $*$ est commutative, le groupe est dit commutatif ou abélien (Niels Abel, mathématicien norvégien, 1802 – 1829).

On note parfois la loi du groupe multiplicativement (ab au lieu de $a * b$) ou additivement ($a + b$ au lieu de $a * b$), mais la notation additive est réservée aux groupes commutatifs. $a * a * ... * a$ est alors noté a^n dans le cas multiplicatif ou na dans le cas additif.

Les axiomes des groupes permettent de simplifier les équations. Ainsi :

$a * x = a * y \Rightarrow x = y$ (composer à gauche par le symétrique de a)

$x * a = y * a \Rightarrow x = y$ (composer à droite par le symétrique de a)

3– Exemples de groupes

On peut citer le groupe des complexes de module 1, le groupe des racines $n^{ème}$ complexes de l'unité, le groupe des similitudes directes du plan, le groupe symétrique. Voici d'autres exemples.

EXEMPLE 1 :

Voici quelques groupes à deux éléments :

{σ,Id} où σ est une symétrie, muni de la loi o.

$U_2 = \{+1,-1\}$ muni du produit (groupe des racines carrées de l'unité, ou règle des signes).

$\mathbb{Z}/2\mathbb{Z} = \{0,1\}$ muni de la loi +. Dans cet ensemble, on pose 1 + 1 = 0.

S_2, groupe symétrique à deux éléments, muni de la loi o

{Croissance, Decroissance} muni de la loi o, et de la règle donnant le sens de variation de la composée de deux fonctions monotones.

{true,false} (en programmation), muni de la loi xor (ou exclusif).

Tous ces groupes sont en fait identiques au suivant :

Groupe à deux éléments $\{a,e\}$. La table de Pythagore de ce groupe est :

*	*a*	*e*
a	*e*	*a*
e	*a*	*e*

On a nécessairement $a^2 = e$ car si $a^2 = a$, en simplifiant par a, on obtient $a = e$.

La correspondance se fait de la façon suivante :

Groupe	*	*a*	*e*
{σ,Id}	o	σ	Id
{+1,–1}	×	–1	+1
$\mathbb{Z}/2\mathbb{Z}$	+	1	0
{Croissance, Décroissance}	o	Decroissante	Croissante
{true,false}	xor	true	false

Tous ces groupes sont dits isomorphes. Un théorème démontré pour l'un d'entre eux l'est pour tous.

Par exemple : la valeur d'un produit en fonction de la parité du nombre de a est a si ce nombre est impair, e si ce nombre est pair. Ce résultat se traduit de la façon suivante dans quelques situations courantes :

$\sigma^{2p} = Id$ et $\sigma^{2p+1} = \sigma$ pour une symétrie σ

Le produit d'un nombre pair de termes négatifs est positif, le produit d'un nombre impair de termes négatifs est négatif.

La composée d'un nombre pair de fonctions décroissantes et d'un nombre quelconque de fonctions croissantes est croissante ; La composée d'un nombre impair de fonctions décroissantes et d'un nombre quelconque de fonctions croissantes est décroissante.

EXEMPLE 2 :
L'exemple suivant n'est pas un groupe :

*	*a*	*e*
a	*a*	*a*
e	*a*	*e*

On trouve cependant cette situation dans les cas suivants :

{*a*, *e*}	*	*a*	*e*
$\mathbb{Z}/2\mathbb{Z}$	×	0	1
{*f* paire, *f* impaire}	o	paire	impaire
{true, false}	or	true	false
{false, true}	and	false	true
{Ω, ∅}	∩	∅	Ω
{∅, Ω}	∪	Ω	∅

Ici, *a* est dit absorbant.

EXEMPLE 3 : Groupes à trois éléments :
Quels sont les groupes à trois éléments ?
Il n'y en a qu'un :

*	*a*	*b*	*e*
a	*b*	*e*	*a*
b	*e*	*a*	*b*
e	*a*	*b*	*e*

Pour le remplir, on remarque que, pour chaque élément *y*, l'application : $x \in G \rightarrow yx \in G$ est bijective. Chaque élément du groupe apparaît donc une fois et une seule dans chaque ligne *y*. De même, l'application $x \rightarrow xy$ est bijective, donc chaque élément du groupe apparaît une fois et une seule dans chaque colonne *y*. En outre $ab = b$ est impossible car cela implique, en simplifiant par *b*, que $a = e$. De même $ab = a$ est impossible, donc $ab = e$, etc... Il est alors facile de compléter le tableau.

Tous les groupes à trois éléments sont donc isomorphes. En voici quelques exemples :

G	*	*a*	*b*	*e*
$U_3 = \{1, j, j^2\}$	×	*j*	j^2	1

où *j* est une racine cubique complexe de l'unité. U_3 est le groupe des racines cubiques de l'unité.

$\{1, \sigma, \sigma^2\}$	o	σ	σ^2	Id

où σ est une rotation de $2\pi/3$

$\mathbb{Z}/3\mathbb{Z}$	+	1	2	0

constitué des éléments {0,1,2} où le calcul se fait modulo 3

A_3	o	(1 2 3)	(1 3 2)	Id

groupe dit alterné des permutations paires de trois éléments

EXEMPLE 4 :
Quels sont les groupes à 4 éléments ?
On n'en trouve que deux :

*	*a*	*b*	*c*	*e*
a	*e*	*c*	*b*	*a*
b	*c*	*a*	*e*	*b*
c	*b*	*e*	*a*	*c*
e	*a*	*b*	*c*	*e*

*	*a*	*b*	*c*	*e*
a	*e*	*c*	*b*	*a*
b	*c*	*e*	*a*	*b*
c	*b*	*a*	*e*	*c*
e	*a*	*b*	*c*	*e*

Le premier, avec l'isomorphisme suivant, n'est autre que $(\mathbb{Z}/4\mathbb{Z},+)$, c'est à dire le groupe des éléments {0,1,2,3} où les calculs se font modulo 4, ou d'autres groupes isomorphes :

G	*	*c*	*a*	*b*	*e*
$U_4 = \{1,-1,i,-i\}$	$\times$	i	-1	$-i$	1

groupe des racines quatrième de l'unité.

$\mathbb{Z}/4\mathbb{Z}$	+	1	2	3	0

Le second, avec l'isomorphisme suivant, est $(\mathbb{Z}/2\mathbb{Z})^2$:

G	*	*a*	*b*	*c*	*e*
$(\mathbb{Z}/2\mathbb{Z})^2$	+	(1,0)	(0,1)	(1,1)	(0,0)

Ce dernier groupe se trouve également dans la situation suivante : considérons un matelas. Il peut être laissé dans la position initiale (Id). On peut le tourner dans le sens de la longueur (σ). On peut le tourner dans le sens de la largeur (θ). On peut lui faire un demi–tour à plat (φ). {Id, σ, θ, φ} n'est autre que le second groupe.

EXEMPLE 5 :

U_n groupe des racines $n^{\text{ème}}$ de l'unité dans $\mathbb{C}$, muni du produit

$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, ..., n-1\}$ où les calculs se font modulo n. Plus précisément, $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble quotient de $\mathbb{Z}$ par la relation d'équivalence de congruence modulo n :

$$x \equiv y \bmod n \Leftrightarrow \exists\, p \in \mathbb{Z},\ x - y = pn \Leftrightarrow \exists\, p \in \mathbb{Z},\ p \mid x - y$$

On définit sur $\mathbb{Z}/n\mathbb{Z}$ une addition de la façon suivante :
Soient $C(x)$ et $C(y)$ deux classes. On pose : $C(x) + C(y) = C(x+y)$. Il faut réaliser que la valeur trouvée dépend a priori du choix fait de x et de y dans chacune des classes. Il est nécessaire de montrer que cette valeur ne dépend que des classes, et non des représentants x et y de chaque classe.

$$\begin{cases} C(x) = C(x') \\ C(y) = C(y') \end{cases} \Leftrightarrow \begin{cases} x \equiv x' \\ y \equiv y' \end{cases} \Rightarrow x+y \equiv x'+y' \Rightarrow C(x+y) = C(x'+y')$$

La possibilité d'une addition repose donc sur la compatibilité de la loi + dans $\mathbb{Z}$ avec la relation de congruence.

On vérifie facilement que la loi ainsi définie confère à $(\mathbb{Z}/n\mathbb{Z},+)$ une structure de groupe commutatif. L'élément neutre est $C(0)$, le symétrique de $C(p)$ est $C(-p) = C(n-p)$. Ce groupe est cyclique, engendré par $C(1)$.

EXEMPLE 6 : Voici un exemple d'isomorphisme entre deux groupes, c'est-à-dire d'application bijective compatible avec les lois de chaque groupe :

$(\mathbb{R},+) \to (\mathbb{R}^{+}*,\times)$

$x \to e^{x}$

Cet isomorphisme intervient dans le choix d'échelles logarithmiques, pour exemple pour la mesure du bruit, ou celle des mouvements telluriques.

EXEMPLE 7 : le groupe symétrique S_n des permutations d'un ensemble à n éléments.

Soit G un groupe fini constitué de n élements. Pour tout a de G, considérons l'application σ_a de G dans G, qui à x associe ax. Cette application est bijective, sa réciproque étant $\sigma_{a'}$ où a' est le symétrique de a dans le groupe G. σ_a est donc une permutation de G. En outre, on a :

$\sigma_a \circ \sigma_b = \sigma_{ab}$. (i)

On a donc l'association :

$(G,*) \to (\mathsf{S}_G,\circ)$

$a \to \sigma_a$

qui définit une application Φ, qualifiée de morphisme du fait de la relation (i). Φ est injective. En effet $\sigma_a = \sigma_b \Rightarrow \sigma_a(e) = \sigma_b(e) \Rightarrow a = b$. Φ est surjective sur $\Phi(G) = \{\sigma_a \mid a \in G\}$. $(\Phi(G),\circ)$ est un sous–groupe de S_G, et l'on a montré que tout groupe fini est isomorphe à un sous–groupe d'un groupe symétrique.

II : Sous-Groupes et morphismes de groupes

1– Sous-groupe

Définition : Soit (G,$*$) *un groupe et* G' *une partie de* G. *On dit que* G' *est un sous–groupe de* G *si, muni de la loi* $*$, (G',$*$) *est un groupe*.

Il suffit de vérifier les propriétés suivantes :

- ❑ G' est non vide
- ❑ G' est stable pour $*$ (ce qui signifie que $*$ est une loi interne à G') :

$$\forall x \in G', \forall y \in G', x * y \in G'$$

- ❑ G' est stable par passage au symétrique : $\forall x \in G', x^{-1} \in G'$

Il est inutile de vérifier que G' dispose d'un élément neutre. En effet, si e est le neutre de G, on montre que e est également neutre de G'. En effet :

G' est non vide, donc il existe x élément de G'

$x \in G'$ donc $x^{-1} \in G'$

$x \in G'$ et $x^{-1} \in G'$ donc $x * x^{-1} \in G'$ donc $e \in G'$

$\forall x \in G, e * x = x * e = x$ donc ceci reste vrai a fortiori pour x dans G'

L'associativité étant vraie dans G est a fortiori vraie dans G'. Il en est de même de l'éventuelle commutativité.

On montre aisément que l'intersection de deux ou plusieurs sous-groupes est lui-même un sous-groupe.

2– Exemples de sous-groupes

EXEMPLE 1 : Le groupe alterné A_n des permutations paires est un sous-groupe du groupe symétrique S_n (voir le chapitre GROUPESYM.PDF dans le cours de première année)

EXEMPLE 2 : Dans le plan $\mathbb{R}^2$, considérons les applications qui au vecteur (x,y) associe le vecteur $(x',y') = (ax + by, cx + dy)$, avec $ad - bc \neq 0$, ce qu'on note :

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

L'ensemble de ces applications, muni de la loi de composition $\circ$, forme un groupe appelé groupe linéaire.
L'ensemble des applications pour lesquelles $ad - bc = \pm 1$ en forme un sous-groupe.
L'ensemble des applications orthogonales (rotations et symétries) forme un sous-groupe de ce sous-groupe appelé groupe orthogonal.
L'ensemble des rotations forme lui–même un sous-groupe du groupe orthogonal.

EXEMPLE 3 : l'ensemble des nombres pairs forme un sous-groupe de $(\mathbb{Z},+)$.

3– Morphismes, Exemples

Soit (G,∗) *et* (G',#) *deux groupes. On appelle morphisme (respectivement isomorphisme) de* G *dans* G' *toute application f (respectivement toute application bijective) vérifiant :*

$$\forall x \in G, \forall y \in G, f(x * y) = f(x) \# f(y)$$

EXEMPLE 1 :
L'application du groupe symétrique $(S_n, \circ)$ dans $(\{-1,1\},\times)$ qui, à chaque permutation associe sa signature est un morphisme.

EXEMPLE 2 :
L'application du groupe linéaire dans $\mathbb{R}^*$ qui à toute matrice associe son déterminant est un morphisme.

D'autres exemples ont été vus dans le paragraphe I-3). L'intérêt d'un isomorphisme est que deux groupes isomorphes sont indiscernables en ce qui concerne leurs propriétés. On les discerne seulement par le *sens* que l'on donne aux éléments du groupe.

EXEMPLE 3 : $\mathbb{Z}/n\mathbb{Z}$ et le groupe U_n des racines $n^{\text{èmes}}$ complexes de 1 sont isomorphes. Il suffit de considérer l'application suivante :

$$\mathbb{Z}/n\mathbb{Z} \to U_n$$
$$p \to \exp(\frac{2ip\pi}{n})$$

p étant défini modulo n, il convient de vérifier que son image ne dépend pas du représentant choisi, ce qui est bien le cas, puisque si, $p \equiv p'$ mod n, on a $\exp(\frac{2ip\pi}{n}) = \exp(\frac{2ip'\pi}{n})$. Autrement dit, l'application est bien définie de $\mathbb{Z}/n\mathbb{Z}$ dans U_n et pas seulement de $\mathbb{Z}$ dans U_n. Il est facile ensuite de vérifier que l'application est bijective et qu'il s'agit d'un morphisme.

4– Propriétés des morphismes

On pourra vérifier les propriétés suivantes sur les exemples de morphismes vus au II-3) et au I-3).

a) Si e est le neutre de G, alors $f(e)$ est le neutre de G'. En effet, si e' est le neutre de G' :

$f(e) = f(e * e) = f(e) \# f(e)$ et d'autre part, $f(e) = f(e) \# e'$

$\Rightarrow$ $f(e) \# f(e) = f(e) \# e'$, et en composant à gauche par $f(e)^{-1}$, on obtient $f(e) = e'$

b) $\forall x \in G$, $f(x^{-1}) = f(x)^{-1}$.
En effet $f(x^{-1}) \# f(x) = f(x^{-1} * x) = f(e) = e'$

c) *Définition :* On appelle noyau de f l'ensemble $\mathrm{Ker}(f) = \{x \mid f(x) = e'\}$. Alors :

i) $\mathrm{Ker}(f)$ est un sous-groupe de G.

ii) f est injective si et seulement si $\mathrm{Ker}(f) = \{e\}$.

Démonstration :
i) est laissé au lecteur. Montrons ii). Si f est injective, alors e' a au plus un antécédent. Or e est un antécédent de e'. Donc $\mathrm{Ker}\, f = \{e\}$. Réciproquement, si $\mathrm{Ker}\, f = \{e\}$, alors :

$f(x) = f(y) \Rightarrow f(x) \# f(y)^{-1} = e' \Rightarrow f(x) \# f(y^{-1}) = e'$

$\Rightarrow$ $f(x * y^{-1}) = e' \Rightarrow x * y^{-1} \in \mathrm{Ker}\, f \Rightarrow x * y^{-1} = e \Rightarrow x = y$.

d) *Définition* : On appelle image de f l'ensemble $\mathrm{Im}(f) = \{y \mid \exists x, f(x) = y\}$. Alors :

i) $\mathrm{Im}\, f$ est un sous-groupe de G'.

ii) f est surjective si et seulement si $\mathrm{Im}(f) = G'$.

5– Sous-groupes engendrés par une partie

Soit $(G,*)$ un groupe et M une partie de G. Considérons G' l'ensemble des produit de la forme $x_1 \ldots x_n$, $n \in \mathbb{N}$, avec $x_i \in M$ ou $x_i^{-1} \in M$. Il est facile de voir que :

i) G' est un sous-groupe de G

ii) Si F est un sous-groupe de G contenant M, alors G' est inclus dans F. G' est donc le plus petit sous-groupe de G contenant M.

iii) G' est égal à l'intersection de tous les sous-groupes contenant M. Cette intersection est en effet un sous-groupe F, et d'après ii), G' est inclus dans F. Inversement, G' est un sous-groupe contenant M donc F est égal à G' intersecté avec les autres sous-groupes contenant M, et est donc inclus dans G'.

On dit que G' est engendré par M ou que M est un système de générateurs de G'.

EXEMPLE 1 : Le groupe symétrique S_n est engendré par l'ensemble des transpositions.

EXEMPLE 2 : $\mathbb{Z}$ est engendré par $\{1\}$.

EXEMPLE 3 : $\mathbb{Z}/n\mathbb{Z}$ est engendré par {1}

6– Groupes monogènes et groupes cycliques

On appelle groupe *monogène* un groupe G engendré par un seul élément *a*. Les éléments du groupe sont donc de la forme a^n, *n* élement de $\mathbb{Z}$ si la loi est notée multiplicativement, ou *na* si elle est notée additivement.

On dispose des règles de calcul suivantes :

$a^n.a^m = a^{n+m}$ pour *n* et *m* éléments de $\mathbb{N}$

$(a^{-1})^n = (a^n)^{-1}$. On notera cette quantité a^{-n}. Dans ce cas, la relation précédente est vraie pour *n* et *m* éléments de $\mathbb{Z}$. On a également :

$(a^n)^m = a^{nm}$ pour *n* et *m* éléments de $\mathbb{Z}$.

L'application de $(\mathbb{Z},+)$ dans G qui à *n* associe a^n est un morphisme de groupe surjectif. Il y a alors deux cas :

❑ Ce morphisme est aussi injectif, ce qui signifie que :

$\forall\, n \in \mathbb{Z}^*,\ a^n \neq e$

$\forall\, n \in \mathbb{Z},\ \forall\, m \in \mathbb{Z},\ n \neq m \Rightarrow a^n \neq a^m$

Dans ce cas, G est infini et isomorphe à $\mathbb{Z}$

❑ Ce morphisme n'est pas injectif. Dans ce cas, il existe *n* tel que $a^n = e$. Soit *n* le plus petit entier strictement positif vérifiant cette relation. Nous allons prouver que G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

soit $\Phi : \mathbb{Z}/n\mathbb{Z} \rightarrow G$

$p \rightarrow a^p$

p est en fait défini modulo *n*. a^p est cependant parfaitement défini sans ambiguïté car $a^{p+kn} = a^p.(a^n)^k = a^p.e^k = a^p$.

Φ est un morphisme.

Φ est injective. En effet, soit *p* tel que $a^p = e$. Divisons *p* par *n*. On a : $p = qn + r$ avec $0 \leq r < n$. Donc $e = a^p = a^{qn+r} = a^r$. Or, par définition de *n*, $a^r = e \Rightarrow r = 0$ puisque *n* est le plus petit entier strictement positif tel que $a^n = e$, que $0 \leq r < n$ et que $a^r = e$. Donc $p = qn \equiv 0 \bmod n$ et $\mathrm{Ker}\Phi = \{0\}$.

Φ est surjective. a^p est l'image de *p*.

En particulier, G est constitué de *n* éléments. $G = \{e, a, a^2, ..., a^{n-1}\}$. On dit que G est un groupe *cyclique* d'ordre *n*, et que *a* est un élément d'ordre *n*.

Les groupes monogènes sont donc tous isomorphes à $\mathbb{Z}$ ou à $\mathbb{Z}/n\mathbb{Z}$

Un sous-groupe H d'un groupe monogène G est lui–même monogène. En effet, soit *a* générateur de G, et soit *p* la plus petite puissance positive telle que a^p soit élément de H. Alors a^p est générateur de H. En effet, si a^m est élément de H, a^{-m} aussi, et on peut supposer *m* positif. Divisons *m* par *p*.

$m = pq + r$ avec $0 \leq r < p$.

On a alors $a^r = a^{m-pq} = a^m.(a^p)^{-q}$ élément de H. Or $0 \leq r < p$ et *p* est la plus petite puissance positive telle que a^p soit élément de H. Donc $r = 0$ et a^m est une puissance de a^p.

7– Groupes finis

a) Soit G un groupe fini. Le nombre d'éléments de G s'appelle l'ordre du groupe et est noté Card(G) ou $|G|$. On appelle également ordre d'un élément l'ordre du sous-groupe engendré par cet élément.

Dans la recherche sur la classification des groupes finis simples, on a mis en évidence des groupes dit sporadique. L'un d'eux est un groupe d'ordre

$$2^{46} \times 3^{20} \times 5^9 \times 7^6 \times 11^2 \times 13^3 \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71$$
$$= 808017424794512875886459904961710757005754368000000000$$

Ce groupe s'appelle *Le Monstre* !! Le premier groupe simple sporadique, découvert en 1861, est le groupe de Mathieu M_{11}, composé de 7920 éléments. Il s'agit du sous-groupe de S_{11}, engendré par les permutations (1 2 3 4 5 ... 10 11) et (5 6 4 10)(11 8 3 7).

THEOREME DE LAGRANGE :
Soit H *un sous-groupe de* G. *Alors, l'ordre de* H *divise l'ordre de* G.

Pour tout x élément de G, on note $xH = \{xy \mid y \in H\}$. L'application qui à y associe xy étant une bijection, xH et H sont en bijection, et tous les ensemble xH ont même nombre d'éléments que H.

La relation binaire définie par :

$$x \mathcal{R} x' \Leftrightarrow xH = x'H$$

est clairement une relation d'équivalence. Montrons que la classe d'équivalence de x est précisément xH. Il faut donc montrer l'équivalence entre :

i) $xH = x'H$ ($x \mathcal{R} x'$)

ii) $x' \in xH$ (x' appartient à la classe de x)

Supposons i). Alors x' est élément de x'H, puisque $x' = x'e$ et que e est élément de H. Comme $x'H = xH$, on en déduit que x' est élément de xH.
Supposons ii). il existe h élément de H tel que $x' = xh$. Dans ce cas, x'H est l'ensemble des éléments de la forme $x'y$, $y \in$ H, donc de la forme xhy, avec y et h et donc yh éléments de H. Ce sont donc des éléments de xH. Ainsi x'H est inclus dans xH. Inversement, xH est l'ensemble des éléments de la forme xy, $y \in$ H, donc de la forme $x'h^{-1}y$. Ces éléments sont bien dans x'H car $h^{-1}y$ est élément de H.

Ainsi les parties xH, étant des classes d'équivalence, forment une partition de G, et toutes ces parties ont même nombre d'éléments. On a donc :

Card(G) = Card(H) × NbreCl où NbreCl désigne le nombre de classes d'équivalence.
et Card(H) divise Card(G).

b) Conséquences :

❑ L'ordre d'un élément divise l'ordre du groupe. Cela peut également s'exprimer sous la forme :

$\forall x \in G, x^n = e$ où $n = |G|$

Cette dernière relation peut se montrer directement dans un groupe commutatif en constatant que, pour x donné, l'application $y \in G \rightarrow xy \in G$ est bijective et donc que :

$$\prod_{y \in G} y = \prod_{y \in G} xy = \prod_{y \in G} x \prod_{y \in G} y = x^n \prod_{y \in G} y$$

❑ Si G est un groupe d'ordre un nombre premier, alors G est cyclique et engendré par n'importe lequel de ses éléments différents de *e*.
En effet, soit *a* un tel élément et H = $\{a^n \mid n \in \mathbb{Z}\}$. H est un sous-groupe de G comportant au moins deux éléments (*a* et *e*). Card(H) divise Card(G), Card(G) est premier et Card(H) est supérieur ou égal à 2, donc Card(H) = Card(G) donc H = G.

Annexe : Groupes de frises

1– Groupe maximal d'une frise

Une frise est une structure décorative en forme de bande, que nous supposerons infinie, invariante par translation et par certaines isométries du plan.

L'exemple le plus élémentaire de frise que l'on puisse concevoir est formé de points $(A_n)_{n\in\mathbb{Z}}$ équidistants sur un axe. Notons I_n le milieu de $[A_{n-1},A_n]$. Posons : $A_n = O + n\boldsymbol{i}$. Les isométries du plan laissant invariante cette frise sont :
❑ les translations t^n, de vecteurs $n\boldsymbol{i}$, $n \in \mathbb{Z}$
❑ les symétries centrales S_{A_n} de centre A_n et les symétries centrales S_{I_n} de centre I_n, $n \in \mathbb{Z}$
❑ la symétrie axiale δ d'axe $\boldsymbol{i}$
❑ les symétries axiales σ_{A_n} d'axe orthogonal à $\boldsymbol{i}$, passant par A_n, et σ_{I_n} d'axes orthogonales à $\boldsymbol{i}$, passant par I_n.
❑ les symétries glissées $\delta \circ t^n = t^n \circ \delta$, $n \in \mathbb{Z}$.

On pourra prouver les relations suivantes :

$t \circ S_{A_n} = S_{I_{n+1}}$ $\qquad$ $t \circ S_{I_n} = S_{A_n}$
$S_{A_n} \circ t = S_{I_n}$ $\qquad$ $S_{I_n} \circ t = S_{A_{n-1}}$
$t^{2n-1} \circ S_{A_0} = S_{I_n}$ $\qquad$ $S_{A_0} \circ t^{2n+1} = S_{I_{-n}}$
$t^{2n} \circ S_{A_0} = S_{A_n}$ $\qquad$ $S_{A_0} \circ t^{2n} = S_{A^{-n}}$
$t^2 \circ S_{A_n} = S_{A_{n+1}}$ $\qquad$ $S_{A_n} \circ t^2 = S_{A_{n-1}}$

$S_{A_n} \circ S_{A_p} = t^{2(n-p)}$
$S_{I_n} \circ S_{I_p} = t^{2(n-p)}$
$S_{A_n} \circ S_{I_p} = t^{2(n-p)+1}$
$S_{I_p} \circ S_{A_n} = t^{2(p-n)-1}$

$\delta \circ S_{A_n} = \sigma_{A_n} = S_{A_n} \circ \delta$
$\delta \circ S_{I_n} = \sigma_{I_n} = S_{I_n} \circ \delta$
$\delta^2 = \mathrm{Id}$

$t \circ \sigma_{A_n} = \sigma_{I_{n+1}}$ $\qquad$ $t \circ \sigma_{I_n} = \sigma_{A_n}$
$\sigma_{A_n} \circ t = \sigma_{I_n}$ $\qquad$ $\sigma_{I_n} \circ t = \sigma_{A_{n-1}}$
$t^{2n-1} \circ \sigma_{A_0} = \sigma_{I_n}$ $\qquad$ $\sigma_{A_0} \circ t^{2n+1} = \sigma_{I_{-n}}$
$t^{2n} \circ \sigma_{A_0} = \sigma_{A_n}$ $\qquad$ $\sigma_{A_0} \circ t^{2n} = \sigma_{A^{-n}}$
$t^2 \circ \sigma_{A_n} = S_{A_{n+1}}$ $\qquad$ $\sigma_{A_n} \circ t^2 = \sigma_{A_{n-1}}$

S_{A_n} o $\sigma_{A_p} = t^{2(n-p)}$ o δ

Certaines relations sont redondantes. L'ensemble de ces transformations forme un groupe G engendré par $\{t, \delta, S_{A_0}\}$ par exemple.

Une frise quelconque est associée à un groupe d'isométrie qui la laisse invariante. Ce groupe est nécessairement un sous-groupe de G

2– Les sept groupes de frises :

La recherche de tous les sous-groupes de G contenant des translations, conduit aux sous-groupes suivants :

❑ I – Le groupe complet : F_2^1 ou G

Ex : XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕⊕
⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗⊗

❑ II – Le groupe contient une symétrie centrale et pas de symétries axiales. $F_2 = <t, S_A>$ ou G_c

Ex : SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

❑ III – Le groupe contient une symétrie centrale et des symétries glissées, mais ne contient pas δ. $F_2^2 = <t/2$ o $\delta, S_A>$ ou G_{cg}

Ex : ∧∨ ∧∨∧∨∧∨∧∨∧∨∧∨∧∨∧∨∧∨∧∨∧∨∧∨∧∨∧∨∧∨

❑ IV – Le groupe ne contient pas de symétrie centrale et mais contient plusieurs symétries axiales. $F_1^2 = <t, \sigma_A>$ ou G_s

Ex : VVVVVVVVVVVVVVVVVVVVVVVVVVVVVVV
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
↑↑

❑ V – Le groupe ne contient pas de symétrie centrale et mais contient δ. $F_1^1 = <t, \delta>$ ou G_δ

Ex : DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→

❑ VI – Le groupe ne contient pas de symétrie centrale ni de symétries axiales, mais contient des symétries glissées. $F_1^3 = <t/2$ o $\delta>$ ou G_g

Ex : ⌈⌊

❑ VII – Le groupe ne contient que des translations. $F_1 = <t>$ ou G_t

Ex : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
LLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL
∂∂

Il y a donc 7 groupes de frises en dimension 1. On montre qu'il en existe 17 en dimension 2, 230 en dimension 3, 4783 en dimension 4. Au delà, on ne dispose que de résultats partiels.

Nous conclurons ce chapitre par un extrait du roman de Georges Perec, *La disparition*. Ce roman est entièrement rédigé sans comporter une seule fois la lettre *e*. L'humour de l'extrait ci-dessous ne peut être pleinement apprécié que par ceux qui ont suivi un cours sur les groupes ☺ :

> On groups.
> (Traduction d'un travail dû à Marshall Hall jr L.I.T. 28, folios 5 à 18 inclus).
> La notion-là, qui la conquit, qui la trouva, qui la fournit ? Gauss ou Galois ? L'on n'a jamais su. Aujourd'hui, tout un chacun connaît ça. Pourtant, on dit qu'au fin fond du noir, avant sa mort, dans la nuit, Galois grava sur son pad (Marshall Hall jr, op. cit. fol. 8) un long chaînon à sa façon. Voici :
> $aa^{-1} = bb^{-1} = cc^{-1} = dd^{-1} = ff^{-1} = gg^{-1} = hh^{-1} = ii^{-1} = jj^{-1} = kk^{-1} = ll^{-1} = mm^{-1} = nn^{-1} = oo^{-1} = pp^{-1} = qq^{-1} = rr^{-1} = ss^{-1} = tt^{-1} = uu^{-1} = vv^{-1} = ww^{-1} = xx^{-1} = yy^{-1} = zz^{-1} =$
> Mais nul n'a jamais pu savoir la conclusion à quoi Galois comptait aboutir dans son manuscrit non fini.
> Cantor, Douady, Bourbaki, ont cru, par un, par dix biais (du corps parfait aux topos, du local ring aux C^{star}, du K-functor qu'on doit à Shih aux ❑ du grand Thom, n'oubliant ni distributions, ni involutions, ni convolutions, Schwartz ni Koszul ni Cartan ni Giorgiutti) saisir un vrai fil sûr pour franchir l'abrupt hiatus. Tout fut vain.
> Pontryagin y passa vingt ans, finissant par n'y plus voir du tout.
> Or voici qu'il y a huit mois Kan, travaillant sur un adjoint à lui (voir D. Kan Adjoint Functors Transactions, V, 3, 18) montra par induction, croit-on, (il raisonnait – a-t-il dit à Jaulin – sur un grand cardinal, par "forcing" pour part) la Proposition Soit G soit H soit K ($H \subset G$, $K \subset G$) trois magmas (nous suivons Kuroch) où l'on a $a(bc) = (ab)c$; où, pour tout a, $x \to xa$, $x \to xa$ sont surs, sont monos, alors on a $G \approx H \times K$, si $G = H \cup K$; si H, si K sont invariants ; si H, K n'ont qu'un individu commun $H \cap K$ = Las ! Kan mourut avant d'avoir fini son job. Donc, à la fin, l'on n'a toujours pas la solution.

◆