Chapitre 1

Les groupes

1.1 Définitions et premières conséquences

1.1.1 Définitions

On appelle groupe, tout couple $(G, \bullet)$ constitué par un ensemble non vide G, et d'une loi de composition interne $\bullet$ vérifiant :

G_1 : $\bullet$ est associative *ie* : $x \bullet (y \bullet z) = (x \bullet y) \bullet z$ pour tous $x, y, z \in G$.

G_2 : Il existe $e \in G$ élément neutre *ie* tel que :

$$e \bullet x = x \bullet e \text{ pour tout } x \in G$$

G_3 : Quel que soit x élément appartenant à G, il existe $x^{-1} \in G$ vérifiant :

$$x \bullet x^{-1} = x^{-1} \bullet x = e$$

Remarque : On notera par la suite indifféremment $x \bullet y = x \cdot y = xy$.

1.1.2 Sous-groupe

Ceci étant acquis, une partie H non vide d'un groupe G est dite *sous-groupe* de G si elle est stable pour la loi $\bullet$ et si le couple $(H, \bullet)$ est un groupe.

On peut démontrer :

Proposition 1 : Si H est une partie non vide du groupe $(G, \bullet)$ les énoncés suivants sont équivalents :

(i) H est un sous-groupe de G.
(ii) $\forall (x, y) \in H \times H, \ \ x^{-1}y \in H$

1.1.3 Groupe engendré

Si A est une partie non vide d'un groupe G, on appelle *sous-groupe engendré par* A le plus petit (au sens de l'inclusion) des sous-groupes de G contenant A ; c'est bien évidemment l'intersection de tous les sous-groupes de G contenant A et il est noté traditionnellement $[A]$; on peut alors démontrer facilement :

Proposition 2 : Si A est une partie non vide d'un groupe G, les énoncés suivants sont équivalents :

(i) $x \in [A]$

(ii) Il existe un entier naturel n, $n \geq 1, a_1, a_2, ..., a_n$ appartenant à $A \bigcup A^{-1}$ ($A^{-1} = \{a^{-1}, a \in A\}$) de sorte que :

$$x = a_1 \cdot a_2 \cdot ... \cdot a_n$$

Il s'ensuit alors le :

Corollaire : Si G est un groupe et si a est élément de G, le sous-groupe de G engendré par cet élément, *ie* $[a]$, est exactement l'ensemble des a^n, n décrivant $\mathbb{Z}$.

1.1.4 Morphisme de groupe

Etant donnés deux groupes $(G, \bullet)$ et $(G', \bullet)$, une application f de G dans G' est dite *morphisme de groupe* si et seulement si :

$$\forall x, y \in G, \quad f(x \cdot y) = f(x) \cdot f(y)$$

Alors on peut énoncer :

Proposition 3 : Si $f : (G, \bullet) \longrightarrow (G', \bullet)$ est un morphisme :

(i) $f(G)$ est un sous-groupe de G'.

(ii) $Ker(f) = \{x \in G : f(x) = f(e) = e'\}$ (e neutre de G, e' neutre de G') est un sous-groupe distingué de G qui est réduit à $\{e\}$ si et seulement si f est injectif.

Tout est quasiment évident dans l'énoncé de cette proposition, et la notion de sous-groupe distingué d'un groupe G est détaillée dans le paragraphe suivant.

1.2 Relations d'équivalence associées à un sous-groupe : applications

1.2.1 Définitions

Classe résiduelle

Soient $(G, \bullet)$ un groupe et H un sous-groupe de G. Dans $G \times G$ on peut définir les deux relations binaires R_1 et R_2 :

$$R_1(x,y) \Longleftrightarrow x^{-1} \cdot y \in H \;\; ; \;\; R_2(x,y) \Longleftrightarrow x \cdot y^{-1} \in H$$

On constate alors aisément que R_1 et R_2 sont des relations d'équivalence dans G, et on a :

Proposition 4 : Si x appartient à G, la classe de x dans G modulo R_1 (*resp.* modulo R_2) est l'ensemble xH (*resp.* l'ensemble Hx) ; on l'appelle la *classe résiduelle de x modulo H à droite* (resp. *à gauche).*

Sous-groupe distingué

Un sous-groupe H du groupe G est dit *distingué dans* G si, par définition :

$$(\forall x \in G)(x \cdot H = H \cdot x), ie$$

$$(\forall x \in G)(\forall h \in H)(x \cdot h \cdot x^{-1} \in H).$$

Alors on a :

Proposition 5 : Si H est un sous-groupe distingué du groupe G, l'ensemble G/H des classes résiduelles dans G modulo H est un groupe pour la loi $\bullet$ définie par :

$$(\bar{x}, \bar{y}) \in G/H \times G/H \longrightarrow \bar{x} \bullet \bar{y} = \overline{x \bullet y} \in G/H$$

En particulier, par utilisation de la proposition 3, il s'ensuit que si f est un morphisme du groupe $(G, \bullet)$ dans le groupe $(G', \bullet)$, le groupe $f(G)$ est isomorphe au groupe quotient $G/Kerf$ ce qu'on écrira :

$$f(G) \cong G/Kerf$$

Tout dans l'énoncé de cette proposition se vérifie aisément et est, de ce fait, laissé aux soins du lecteur.

1.2.2 Application : le théorème de Lagrange

Proposition 6 : Si $(G, \bullet)$ est un groupe fini, et si H est un sous-groupe de G, le cardinal de H divise celui de G.

En effet, utilisons par exemple la relation d'équivalence R_1 définie sur G par : $xR_1y \Longleftrightarrow x^{-1}y \in H$.

Chaque classe possède exactement $card\ H$ éléments, et s'il y en a p on a donc, puisque les diverses classes d'équivalence forment une partition de G :

$$card\ G = p \cdot card\ H$$

Ce qui achève la preuve.

Corollaire : Si a est un élément d'un groupe $(G, \bullet)$ ayant n éléments, on a toujours la relation :

$$a^n = e$$

où e est l'élément neutre de $(G, \bullet)$.

En effet, désignons par H le sous-groupe de G engendré par l'élément a ; si q est le nombre d'éléments de H on a donc : $[a] = \{e, a, ..., a^{q-1}\}$ et $a^q = e$; comme n est un multiple de l'entier q il s'ensuit $a^n = e$ ce qui achève la démonstration.

1.3 Groupes monogènes - Groupes cycliques

1.3.1 Définitions

a) Un groupe $(G, \bullet)$ est dit *monogène* s'il existe a dans G vérifiant : $G = [a]$, *ie* si et seulement si :

$$G = \{a^n, n \in \mathbb{Z}\}$$

b) Un groupe $(G, \bullet)$ est dit *cyclique* s'il est monogène et fini.

Proposition 7 : Soit $(G, \bullet)$ un groupe monogène.
Si G est infini, il est isomorphe au groupe $(\mathbb{Z}, +)$.
Si G est fini et possède n éléments, il est isomorphe au groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$ des classes résiduelles modulo n dans $\mathbb{Z}$.

En effet, soit a un générateur de $(G, \bullet)$; l'application : $q \in \mathbb{Z} \longrightarrow a^q \in G$ est manifestement un morphisme surjectif du groupe $(\mathbb{Z}, +)$ dans le groupe $(G, \bullet)$; son noyau est un sous-groupe additif de $\mathbb{Z}$; il est donc de type $n\mathbb{Z}$; si $n = 0$, G est infini et isomorphe à $(\mathbb{Z}, +)$ sinon il est, pour $n \geq 1$, isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$ par application immédiate de la proposition 5.

Ainsi si G est un groupe cyclique, G est du type $G = \{e, a, ..., a^{n-1}\}$ et on a : $a^m = e$ si et seulement si m est un multiple de l'entier n (appelé parfois *ordre* du groupe cyclique G).

1.3.2 Quelques propriétés des groupes cycliques

Sous-groupes d'un groupe cyclique

Proposition 8 : Soit $(G, \bullet)$ un groupe cyclique ayant n éléments, alors :

(i) Tout sous-groupe H de G est lui aussi cyclique.
(ii) Si p est un diviseur de l'entier n, il existe un et un seul sous-groupe de G ayant p éléments.

Démonstration : Ecrivons $G = \{e, a, ..., a^{n-1}\}$ et soit $H \neq \{e\}$ un sous-groupe de G ; notons $r = \min\{q \in \{1, 2, ..., n-1\}, a^q \in H\}$; alors H est le sous-groupe de G engendré par $b = a^r$; en effet soit $x = a^q \in H$; par division euclidienne on a :

$$q = rs + t \quad \text{où} \quad 0 \leq t \leq r - 1$$

Alors : $x = a^q = a^{rs} \cdot a^t$; il s'ensuit que $a^t = x \cdot a^{-rs}$ appartient à H, ce qui impose $t = 0$ et prouve bien (i).

Pour démontrer l'assertion (ii) écrivons : $n = pq$ et notons $b = a^q$; si H est le sous-groupe engendré par b, H contient les p éléments : $e, b, b^2, ..., b^{p-1}$ qui sont deux à deux distincts ; comme $a^n = e$ il vient $b^p = e$ ce qui prouve que H possède exactement p éléments ; reste à prouver l'unicité du sous-groupe H.

Soit donc H' un sous-groupe de G ayant p éléments ; H' est cyclique ; désignons par b' un générateur de H'. On peut donc trouver un entier q' de $\{1, 2, ..., n-1\}$ tel que $a^{q'}$ engendre H' ; comme H' a p éléments, on doit avoir : $a^{pq'} = e$ ce qui impose pq' multiple de n. Ainsi on peut écrire :

$$q' = k'q \quad \text{avec } k' \text{ entier}$$

De ce fait : $a^{q'} = (a^q)^{k'}$ appartient à H et on a donc l'inclusion $H' \subset H$ et comme H et H' ont le même nombre d'éléments, il reste $H = H'$, ce qui achève la démonstration.

Générateurs d'un groupe cyclique - Indicatrice d'Euler - Formule de Möbius

On peut énoncer :

Proposition 9 : Soit $G = \{e, a, ..., a^{n-1}\}$ un groupe cyclique d'ordre $n \geq 2$. $b = a^i, 1 \leq i \leq n-1$ est un générateur de G si et seulement si $i \wedge n = 1$ *ie* si et seulement si i et n sont premiers entre eux.

En effet, $[a^i] = G$ si et seulement si :

$$\exists k \in \mathbb{Z} : a^{ik} = a \; ie \; ssi : a^{ik-1} = e \; ie \; ssi : ik - 1 \in n\mathbb{Z} \; ie \; ssi : i \wedge n = 1$$

Le nombre de générateurs de G ne dépend que de n et il est égal au nombre, noté $\varphi(n)$, d'entiers $i \in \{1, 2, ..., n\}$ et premiers avec n. On l'appelle *l'indicateur d'Euler* de l'entier n ; on convient que $\varphi(1) = 1$.

Corollaire : On a la formule, dite de Möbius :

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

$d|n$ veut dire d divisant n, $d \geq 1$

En effet, soit $\mathcal{D} = \{d \in \{1, ..., n\} : d|n\}$.

Si $d \in \mathcal{D}$ il existe H_d unique, sous-groupe de G, ayant d éléments. H_d admet exactement $\varphi(d)$ générateurs ; autrement dit il existe $\varphi(d)$ éléments de G d'ordre d exactement ; d'où la formule.

Remarque : On peut aussi démontrer cette égalité comme il suit :
posons :

$$K_n(X) = \prod_{\substack{k \wedge n = 1 \\ 1 \leq k \leq n}} (X - e^{\frac{2ik\pi}{n}}) \quad et \quad K_1(X) = X - 1; \; deg \; K_n(X) = \varphi(n)$$

Dans $\mathbb{C}[X]$:

$$X^n - 1 = \prod_{1 \leq k \leq n} (X - e^{\frac{2ik\pi}{n}}) = \prod_{d \in \mathcal{D}} \left[\prod_{k \wedge n = d} (X - e^{\frac{2ik\pi}{n}}) \right]$$

or :

$$\prod_{k \wedge n = d} (X - e^{\frac{2ik\pi}{n}}) = \prod_{k' \wedge \frac{n}{d} = 1} (X - e^{\frac{2ik'\pi}{n'}})$$

où $n' = \frac{n}{d}$ et $k' \wedge n' = 1$. Donc :

$$X^n - 1 = \prod_{d \in \mathcal{D}} K_{\frac{n}{d}}(X) = \prod_{d \in \mathcal{D}} K_d(X)$$

Ainsi, en identifiant les degrés il vient :

$$n = \sum_{d \in \mathcal{D}} \varphi(d)$$

1.4 Groupes opérant sur un ensemble - Applications

1.4.1 Définitions

Un groupe G opère sur un ensemble E si on dispose d'une application $*$ de $G \times E$ dans E : $(g, x) \longrightarrow g * x$ vérifiant :

$$\begin{cases} g * (g' * x) = (g \cdot g') * x \\ e * x = x \end{cases} \text{ pour tous } g, g' \in G, \text{ et tout } x \in E$$

De ce fait dans E on peut définir une relation d'équivalence par :

$$(x \sim y) \Longleftrightarrow (\exists g \in G)(y = g * x)$$

La classe de x dans E est appelée alors *l'orbite de x selon G*. C'est l'ensemble $O(x) = \{g * x, g \in G\}$.

Par exemple, si $E = \{1, 2, ..., n\}$ et $G = [\sigma]$ où $\sigma \in S_n$, les orbites, dans E de l'action de $[\sigma]$ définie par :

$$(g, i) \longrightarrow g * i = g(i)$$

correspondent aux divers supports des divers cycles $c_1, c_2, ..., c_q$ dont le produit commutatif constitue la permutation σ.

Proposition 10 : Si le groupe G opère sur l'ensemble E et si x appartient à E, l'orbite $O(x)$ est en bijection avec l'ensemble dans G des classes résiduelles modulo H, où H est le sous-groupe de G des g tels que $g * x = x$, via la relation d'équivalence dans G définie par $g \sim g'$ *ssi* $g'^{-1} \cdot g \in H$

En effet, soit f l'application : $G \longrightarrow O(x)$ définie par :

$$f(g) = g * x$$

f est une surjection et on sait que $f(G) = O(x)$ est en bijection avec l'ensemble $G/\sim$ constitué par les classes dans G via la relation d'équivalence dans G définie par :

$$g \sim g' \; ssi \; f(g) = f(g') \; ie \; ssi : (g'^{-1} \cdot g) * x = x \; ie \; ssi : g'^{-1} \cdot g \in H$$

où H est le sous-groupe de G (ce qui se vérifie aisément) constitué par les $g \in G$ tels que $g * x = x$ et qu'on appelle *stabilisateur de x via l'action de G sur E.*

1.4.2 Applications

Elles peuvent se résumer dans la proposition suivante :

Proposition 11 : Soit G un groupe fini opérant sur un ensemble fini E ; si : $\{O(x_i),\ i \in I\}$ désigne les diverses orbites dans E via l'action de G, on a la relation :

$$card\ E = \sum_{i \in I} \frac{card\ G}{card\ H_i}$$

où H_i est le sous-groupe de G stabilisant $x_i,\ i \in I$.

En particulier, et pour l'exemple, si E est un cube de $\mathbb{R}^3$ et si G est le groupe des rotations le laissant invariant, on peut montrer aisément que l'action de G sur E définie par :

$$(u, M) \in G \times H \longrightarrow u(M) \in E$$

définit une seule orbite dont le stabilisateur associé possède exactement 3 éléments ; il s'ensuit qu'il existe exactement $3 \times 8 = 24$ rotations conservant ce cube.

1.5 Exposant d'un groupe commutatif fini

1.5.1 Définition

Si G est un groupe fini, commutatif ou non, on appelle *exposant de* G le ppcm des ordres des divers éléments de G ; usuellement il est noté $\omega(G)$.

$\omega(G)$ est donc le plus petit entier vérifiant $x^{\omega(G)} = e$ pour tout $x \in G$ et c'est bien sûr un diviseur de l'entier $n = card\ G$ via le théorème de Lagrange.

Cette notion est surtout intéressante lorsque G est un groupe commutatif.

1.5.2 Cas où G est commutatif - Applications

Proposition 12 : Si G est un groupe commutatif il existe toujours au moins un élément de G d'ordre $\omega(G)$.
G est cyclique si et seulement si $\omega(G) = card\ G$

Démonstration :

1er pas : si x et y dans G sont d'ordre p et q avec $p \wedge q = 1$ alors : $z = xy$ est d'ordre $pq = ppcm(p, q)$.