Les Groupes Gauches

1) ***Groupe produit*** : Soit (A, •) et (B, •) deux groupe et E leur produit artésien E = A×B, on peut définir ***canoniquement*** sur E une structure de groupe dite produit :

$\forall$ (a, b) $\in$E, $\forall$ (a', b') $\in$E,

On pose: (a, b)•(a', b') = (a•a', b•b')

Il est clair que (E, •) est un groupe dont le neutre $e_E = (e_A, e_B)$

Et dont le symétrique : $sym_E((a, b)) = (sym_A(a), sym_B(b))$

N.B. les correspondances :

$$p_A : E \longrightarrow A, (a, b) \longmapsto a, \text{ et } p_B : E \longrightarrow B, (a, b) \longmapsto b,$$

Sont des applications surjectives, et de plus sont des morphismes de groupes, il sont dits ***épimorphismes*** canoniques, ou les projections canoniques.

De même nous pouvons généraliser à plusieurs à un produit cartésien de plusieurs groupes (un nombre fini de groupes)

N.B. Pour une famille infini de groupes $\{A_i \mid i \in I\}$ nous pouvons définir le groupe de leur produit cartésien $\prod_{i\in I} A_i$, et aussi, nous pouvons définir le ***sous-groupe*** de $\prod_{i\in I} A_i$ formé par les éléments à support fini (leurs coordonnées qui ne sont pas neutres sont en nombre fini) ce sous-groupes peut être appelé somme directe ou produit faible, noté $\coprod_{i\in I} A_i$

2) ***Théorème*** : Soit G un groupe et A, B des sous groupes de G :
Les ***morphismes*** canoniques :

$p_1 : A\times B \longrightarrow G , (a, b) \longmapsto a,$ et $p_2 : A\times B \longrightarrow G , (a, b) \longmapsto b,$
Nous avons :

$$\textbf{\textit{Ker}}(p_1) = \{e_A\}\times B, \text{ et } \textbf{\textit{Ker}}(p_2) = A\times\{e_B\}$$

Tous les deux des sous-groupes distingués de A×B.

Et enfin $[G \cong A\times B] \Leftrightarrow$

$$[\, G = AB, AB = \{e_G\}, A \lhd G \text{ et } B \lhd G] \Leftrightarrow$$

$$[\forall (a, b)\in A\times B, ab = ba \text{ dans G, et } \forall x\in G, x = ab \text{ d'une façon unique}]$$

3) ***Commutateur d'un couple*** : Soit (a, b) un élément de G×G

On appelle commutateur de ce couple l'élément c de G tel que ab = ba.c, ce commutateur se note c = [a, b]

N.B. si a et b commutent leur commutateur $[a,b] = e_G$. Et le commutateur de (a,b) est l'inverse du commutateur de (b,a).
Pourtant le produit de deux commutateurs n'est pas forcément un commutateur.

4) ***Théorème*** : Soit f : A $\longrightarrow$ B un morphisme de groupes, alors l'image du commutateur d'un couple est le commutateur du couple d'images :

$$f([a,b]) = [f(a),f(b)]$$

5) ***Le groupe dérivé de G*** : Soit (G, e_G) un groupe on appelle sous-groupe dérivé de G, le sous-groupe de G engendré par les commutateurs dans G. On le notera ***D***(G).
Nous pouvons itérer cette opération et avoir

$$\{0\} \leq \ldots \leq \boldsymbol{D}^3(G) \leq \boldsymbol{D}^2(G) \leq \boldsymbol{D}(G) \leq G$$

N.B. Si G est commutatif ***D***(G) = {0}

6) ***Les automorphismes intérieurs de G*** : Soit (G, e_G), et $a \in G$
On construit la correspondance :

$$\varphi_a : G \longrightarrow G,\ x \longmapsto a^{-1}x.a$$

φ_a est un morphisme bijectif (dit automorphisme intérieur de G par l'élément a)

Nous noterons ***Aut***(G) l'ensemble des automorphismes de G, et ***Int***(G) l'ensemble des automorphismes intérieurs de G.

7) ***Théorème*** : (***Aut***(G), $\circ$, Id_G) est un groupe et (***Int***(G), $\circ$, Id_G) est un sous-groupe distingué de (***Aut***(G), $\circ$, Id_G) :

$$(\boldsymbol{Int}(G), \circ, Id_G) \lhd (\boldsymbol{Aut}(G), \circ, Id_G)$$

8) ***Théorème*** : ***D***(G) $\lhd$ G, si bien que G/***D***(G) est un groupe noté G^{ab} dit ***l'abélianisé*** de G.
Cet ***abélianisé*** est une solution d'un problème universel.

Les Groupes Abéliens

1) Groupe abélien engendré par une famille finie : Soit (A, +) un groupe abélien, et B = $\{b_1, b_2, b_3, \ldots, b_{n-1}, b_n\}$ une partie finie de A, (on note $B \in 2^{[A]}$) on dit que B engendre A si :

$\forall\ x \in A,\ \exists\ (\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_{n-1}, \alpha_n) \in \mathbb{Z}^n$,

$$x = \alpha_1 b_1 + \alpha_2 b_2 + \alpha_3 b_3 + \ldots + \alpha_{n-1} b_{n-1} + \alpha_n b_n.$$

N.B. Nous pouvons étendre ceci à un groupe engendré par une partie quelconque I (finie ou infinie) de A :
Dans ce cas :

$\forall\ x \in A, \exists B \in 2^{[A]}$(ensemble des parties finies de A),

$B = \{b_1, b_2, b_3, \ldots, b_{n-1}, b_n\}$,

$\exists (\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_{n-1}, \alpha_n) \in \mathbb{Z}^n$,

$$x = \alpha_1 b_1 + \alpha_2 b_2 + \alpha_3 b_3 + \ldots + \alpha_{n-1} b_{n-1} + \alpha_n b_n.$$

N.B. Dans la notation ***multiplicative*** :

$(A,\times)$ un groupe abélien, et $B=\{b_1,b_2,b_3,\ldots,b_{n-1},b_n\}$ une partie finie de A, (on note $B\in 2^{[A]}$) on dit que B engendre A si :

$\forall x \in A, \ \exists (\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_{n-1}, \alpha_n) \in \mathbb{Z}^n, \ x = b_1^{\alpha_1} \ b_2^{\alpha_2} \ldots \ b_n^{\alpha_n}$.

N.B. On n'affirme pas l'unicité des $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_{n-1}, \alpha_n$.
En effet si les ordres des éléments sont finis :
ord$(b_1) = m_1$, ***ord***$(b_2) = m_2$, ***ord***$(b_3) = m_3, \ldots..$, ***ord***$(b_{n-1}) = m_{n-1}$, ***ord***$(b_n) = m_n$
Signifie :
$m_1 b_1 = 0, \ m_2 b_2 = 0, m_3 b_3 = 0, \ldots, m_{n-1} b_{n-1} = 0, m_n b_n = 0.$
Si on considère les égalités de la division:
$\alpha_1 = m_1 q_1 + r_1, \alpha_2 = m_2 q_2 + r_2, \ldots, \alpha_n = m_n q_n + r_n,$

$$0 \le r_1 < m_1, 0 \le r_2 < m_2, \ldots, 0 \le r_n < m_n,$$

$x = r_1 b_1 + r_2 b_2 + r_3 b_3 + \ldots + r_{n-1} b_{n-1} + r_n b_n.$
Cette écriture est unique sous les conditions

$$0 \le r_1 < m_1, 0 \le r_2 < m_2, \ldots, 0 \le r_n < m_n,$$

Card$(A) \le m_1 \times m_2 \times \ldots \times m_n$.

Si $A \to [[0;m_1 -1]] \times [[0;m_1 -1]] \times \ldots.. \times [[0;m_1 -1]]$;

$x = r_1 b_1 + r_2 b_2 + r_3 b_3 + \ldots. + r_{n-1} b_{n-1} + r_n b_n \mapsto (r_1, r_2, \ldots, r_{n-1}, r_n)$ est bijective ***Card***$(A) = m_1 \times m_2 \times \ldots \times m_n$.

Notons $B_1 =$ ***gp***(b_1), $B_2 =$ ***gp***$(b_2), \ldots, B_n =$ ***gp***(b_n), les groupes ***cycliques*** engendrés par $b_1, b_2, \ldots, b_n$.

$$A = B_1 \oplus B_2 \oplus \ldots \oplus B_n. \quad \textbf{\textit{Somme directe}}.$$

2) Eléments de torsion : un élément de torsion dans A est tout éléments x d'ordre fini :

$\exists \alpha \in \mathbb{N}^*, \alpha x = 0.$
On note **T**(A) l'ensemble de tous les éléments de torsion de A.

T$(A) \le A$. (**T**(A) est un ***sous groupe*** de A)

N.B. Si **T**$(A) = 0$ on dit que A est ***sans torsion***.

N.B. Si A est fini, de cardinal n, tout élément x de A est d'ordre $\le n$, il est de torsion, donc **T**$(A) = A$ on dit que A est ***de torsion***.

N.B. **F**$(A) = A \backslash$ **T**(A) est l'ensemble des éléments ***sans torsion*** de A.
F(A) est vide ou infini.

3) Groupe abélien libre : un groupe abélien (A, +) est dit libre sur B = {b_1, b_2, b_3,…b_{n-1}, b_n} si tout élément x de A s'écrit d'une façon unique de la forme :

$$x = \alpha_1 b_1 + \alpha_2 b_2 + \alpha_3 b_3 + \ldots + \alpha_{n-1} b_{n-1} + \alpha_n b_n.$$

(α_1, α_2, α_3,…, α_{n-1}, α_n) unique $\in \mathbb{Z}^n$,
Dans ce cas B doit être une partie sans torsion de A.

N.B. B étant fini, A est ***libre de type fini***.

Si (A,+) est de type fini engendré par B = {b_1, b_2, b_3,…, b_{n-1}, b_n} avec b_1, b_2,…, b_{m-1}, b_m de torsion et b_{m+1}, b_{m+2},…, b_{n-1}, b_n sans torsion, alors $\mathbf{T}(A) = \boldsymbol{gp}(b_1) \oplus \boldsymbol{gp}(b_2) \oplus \ldots \oplus \boldsymbol{gp}(b_m)$ le groupe quotient A/$\mathbf{T}$(A) est sans torsion et

$\mathbf{F}(A) = \boldsymbol{gp}(b_{m+1}) \oplus \boldsymbol{gp}(b_{m+2}) \oplus \ldots \oplus \boldsymbol{gp}(b_m)$ est ***isomorphe*** à A/$\mathbf{T}$(A)

$$A = \mathbf{F}(A) \oplus \mathbf{T}(A)$$

$\mathbf{F}$(A) est un sous groupe sans torsion (infini) mais de type fini, $\mathbf{T}$(A) est un sous groupe de torsion (fini) et de type fini.

4) Théorème : Si (A, +) est un groupe de type fini, alors :

A est libre ***ssi*** A sans torsion.

(⇒) Si A est libre sur B, B engendre A comme A de type fini, B est fini, soit B = {b_1, b_2, b_3,…., b_{n-1}, b_n} soit
$x = \alpha_1 b_1 + \alpha_2 b_2 + \alpha_3 b_3 + \ldots + \alpha_{n-1} b_{n-1} + \alpha_n b_n$. est un élément de A, si x est de torsion, il existe un entier β non nul tel que $\beta x = 0 = 0b_1 + 0b_2 + 0b_3 + \ldots + 0b_{n-1} + 0b_n$.
et $\beta x = \beta\alpha_1 b_1 + \beta\alpha_2 b_2 + \beta\alpha_3 b_3 + \ldots + \beta\alpha_{n-1} b_{n-1} + \beta\alpha_n b_n$.
L'unicité de l'expression de βx dans B (à cause de la liberté de A sur B) exige :
$\beta\alpha_1 = 0$, $\beta\alpha_2 = 0$, $\beta\alpha_3 = 0$,…; $\beta\alpha_{n-1} = 0$, $\beta\alpha_n = 0$,
Comme β non nul :
$\alpha_1 = 0$, $\alpha_2 = 0$, $\alpha_3 = 0$,…; $\alpha_{n-1} = 0$, $\alpha_n = 0$,
D'où x = 0.
Il en résulte que 0 est le seul élément de torsion de A. A est donc sans torsion.
Contredisant la liberté de A.

(⇐)
Supposons maintenant que A est de type fini, et sans torsion, montrons qu'alors il est libre.
Supposons que A (étant de type fini) est engendré par B = {b_1, b_2, b_3,…, b_{n-1}, b_n}. Par récurrence sur le cardinal #B de B, commençons avec #B =1, B = {b_1}, tout x de A s'écrit $x = \alpha_1 b_1$ comme b_1 sans torsion, donc tous les n.b_1 sont distincts et alors, A contient alors un nombre infini d'éléments, A est infini, engendré par un seul élément, et tout élément de B s'exprimera d'une façon unique par rapport à B, il donc libre.
Supposons que tout groupe abélien de type fini, qui est libre sur n-1 éléments distincts est sans torsion, et soit la combinaison linéaire nulle :
$\alpha_1 b_1 + \alpha_2 b_2 + \alpha_3 b_3 + \ldots + \alpha_{n-1} b_{n-1} + \alpha_n b_n = 0$

Les coefficients peuvent être considérés premiers entre eux dans leur ensemble, si non ils aurons un ***pgcd*** non nul d et alors :

$$d\beta_1 b_1 + d\beta_2 b_2 + d\beta_3 b_3 + \ldots + d\beta_{n-1} b_{n-1} + d\beta_n b_n = 0$$

En factorisant par d non nul,

$$d(\beta_1 b_1 + \beta_2 b_2 + \beta_3 b_3 + \ldots + \beta_{n-1} b_{n-1} + \beta_n b_n) = 0$$

Comme le groupe A est supposé sans torsion :

$(\beta_1 b_1 + \beta_2 b_2 + \beta_3 b_3 + \ldots + \beta_{n-1} b_{n-1} + \beta_n b_n) = 0$

Avec des coefficients $\beta_1, \beta_2, \beta_3, \ldots \beta_{n-1}, \beta_n$ sans diviseur commun. (premiers entre eux dans leur ensemble).

1° si $\beta_n = 1$: nous aurons

$$\beta_1 b_1 + \beta_2 b_2 + \beta_3 b_3 + \ldots + \beta_{n-1} b_{n-1} + b_n = 0$$
$$b_n = -(\beta_1 b_1 + \beta_2 b_2 + \beta_3 b_3 + \ldots + \beta_{n-1} b_{n-1})$$
$$b_n = -\beta_1 b_1 - \beta_2 b_2 - \beta_3 b_3 - \ldots - \beta_{n-1} b_{n-1}$$

Ainsi A sera engendré par $\{b_1, b_2, b_3, \ldots, b_{n-1}\}$, on appliquera donc l'hypothèse de la récurrence.

2° si $\beta_n = -1$: nous aurons

$$\beta_1 b_1 + \beta_2 b_2 + \beta_3 b_3 + \ldots + \beta_{n-1} b_{n-1} - b_n = 0$$
$$b_n = (\beta_1 b_1 + \beta_2 b_2 + \beta_3 b_3 + \ldots + \beta_{n-1} b_{n-1})$$
$$b_n = +\beta_1 b_1 + \beta_2 b_2 + \beta_3 b_3 + \ldots + \beta_{n-1} b_{n-1}$$

et A sera engendré par $\{b_1, b_2, b_3, \ldots, b_{n-1}\}$, on appliquera aussi l'hypothèse de la récurrence.

3° si $\beta_n = 0$: $\beta_1 b_1 + \beta_2 b_2 + \beta_3 b_3 + \ldots + \beta_{n-1} b_{n-1} = 0$. On applique l'hypothèse de récurrence sur $\{b_1, b_2, b_3, \ldots, b_{n-1}\}$,

4° si aucun coefficient n'est pas 0 ou +1 ou –1 :

On cherchera un autre ensemble générateur dont l'un des coefficient de x dans cet ensemble sera +1 ou –1, ceci consiste à diminuer la valeur absolue des coefficients, jusqu'à arriver à un qui est +1 ou -1 :

Supposons $|\beta_1| > |\beta_2| > 0$

pour s entier, on peut écrire : $\beta_1 b_1 + \beta_2 b_2 + \beta_3 b_3 + \ldots + \beta_{n-1} b_{n-1} + \beta_n b_n = 0$

Sous la forme

$\beta_1 b_1 - s\beta_2 b_1 + \beta_2 b_2 + s\beta_2 b_1 + \beta_3 b_3 + \ldots + \beta_{n-1} b_{n-1} + \beta_n b_n = 0$

$(\beta_1 - s\beta_2) b_1 + \beta_2 (b_2 + s b_1) + \beta_3 b_3 + \ldots + \beta_{n-1} b_{n-1} + \beta_n b_n = 0$

La division euclidienne de $\beta_1 - s\beta_2$ par β_2 donne le meilleur s pour que $|\beta_1 - s\beta_2| < |\beta_2|$, en posant $\beta'_1 = \beta_1 - s\beta_2$ et $b'_2 = b_2 + s b_1$. Nous aurons

$\beta'_1 b_1 + \beta_2 b'_2 + \beta_3 b_3 + \ldots + \beta_{n-1} b_{n-1} + \beta_n b_n = 0$.

En répétant ceci, nous sommes sure d'arriver à un des coefficients 0 +1 ou –1 nous appliquerons un des cas précédents.

5) Conséquence : Tout groupe abélien de type fini qui n'est pas de torsion, est somme directe d'un fini et d'un groupe libre (infini)

En effet si A = T(A), et de type fini, il est fini.

Si non T(A) étant le sous-groupe de torsion, A/T(A) est sans torsion, non réduit au neutre, donc il est infini, et libre, A/T(A) est de type fini aussi, on applique le théorème, et on trouvera une base $\{b_1, b_2, b_3,\ldots,b_n\}$de A/T(A), si $\{a_1, a_2, a_3,\ldots,a_n\}$est un choix transversal d'antécédents, $\{a_1, a_2, a_3,\ldots,a_n\}$ est un ensemble générateur d'un sous-groupe L libre de A. et il est clair(à expliquer en remarquant que A/T(A) est isomorphe à L) que A est somme directe de T(A) et de L :

$$A = L \oplus T(A)$$

6) Corollaire : Tout groupe abélien A de type fini, est somme directe de groupe fini et d'un groupe libre.

N.B. Le théorème affirme A de type fini : $A = L \oplus T(A)$ avec T(A) et L de type fini tous les deux, L libre et de type fini sa structure est évidente :

$$L = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \ldots \oplus \mathbb{Z}e_s$$

T(A) est de torsion, de type fini et fini, il a plusieurs structures possibles.
Pour étudier les groupes abéliens de type fini, Il suffit donc d'étudier seulement les groupes abéliens finis. (Qui sont évidement de torsion), ces groupes se décomposent en une somme directe finie de groupes cycliques (finis)

N.B. Posons $\mathfrak{C}_n$ le groupe additif $\mathbb{Z}/n\mathbb{Z}$ et $(\mathbf{F}_p)^\times$ le groupe multiplicatif $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$. ($\mathbf{F}_p$ étant le corps premier d'ordre p, qui est par ailleurs isomorphe à $\mathbb{Z}/p\mathbb{Z}$).
Nous avons :

$\mathfrak{C}_2 \oplus \mathfrak{C}_3$ isomorphe à $\mathfrak{C}_6$ mais $\mathfrak{C}_3 \oplus \mathfrak{C}_3$ non isomorphe à $\mathfrak{C}_9$.

7) Groupe primaire (non nécessairement abélien): Un groupe est dit primaire si tous ses éléments sont d'ordre, une puissance d'un seul nombre premier p.

$$\forall\, x \in A,\ \exists\ r \in \mathbb{N},\ \textbf{\textit{ord}}(x) = p^r.$$

Dans ce cas on dit que A est un ***p-groupe***.

8) Les p-sous groupe de A : On désigne par A_p l'ensemble des éléments x de A tels que $\exists\ r \in \mathbb{N},\ \textbf{\textit{ord}}(x) = p^r$.

$$A_p = \{x \in A \mid \exists\ r \in \mathbb{N},\ \textbf{\textit{ord}}(x) = p^r\}$$

C'est un sous groupe de A, il contient 0, et si $p^r.x = 0$ et si $p^s.y = 0$, et, t le ***pppcm*** de r et s : $p^t.x = 0$ et $p^t.y = 0$, donc

$$p^t.(x - y) = 0 \quad \text{par suite } x - y \in A_p$$

Dans ce cas on dit que A_p est le ***p-sous groupe*** maximal de A.
N.B. Nous remarquons que tous les sous-groupes de A_p sont des ***p-groupes*** (car leur ordre est un diviseur de p^r)

N.B. Nous remarquons aussi que si A est fini, une puissance de p divise l'ordre de A. Nous pouvons imaginer :

$$A = A_{p1} \oplus \ldots \oplus A_{ps}$$

Où $A_{p1}, \ldots, A_{ps}$, sont *les* ***p-sous-groupes*** maximaux de A.

(p_j est un diviseur de #A)

9) Théorème : Tout groupe abélien fini, s'exprime et d'une façon unique comme somme directe de ***p-groupes***.

$$A = A_{p1} \oplus \ldots \oplus A_{ps}$$

Pour des nombres p_j premiers différents
Si $p_1, \ldots, p_s$ sont les premiers divisant #A, alors

$$A = A_{p1} \oplus \ldots \oplus A_{ps}$$

$A_{p1}, \ldots, A_{ps}$ sont les ***p-sous-groupes maximaux*** de A.

10) Théorème : Tout groupe fini est somme directe de groupes cycliques.

11) Conséquence : Tout groupe abélien de type fini est somme directe de groupes cycliques ou monogènes.

Preuve : Nous savons que $A = T(A) \oplus L$ avec T(A) de torsion et de type fini, donc fini soit d'après le théorème précédent ;

$$T(A) = A_{p1} \oplus \ldots \oplus A_{ps}$$

$A_{p1}, \ldots, A_{ps}$ sont des ***p-groupes*** (finis) chacun d'ordre une puissance entière d'un nombre premier. (ce ne sont pas nécessairement des groupes cycliques, mais sont des sommes directes de groupes cycliques (finis))
Et puis, L est déjà libre de type fini :

$$L = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \ldots \oplus \mathbb{Z}e_s$$

$\mathbb{Z}e_1, \mathbb{Z}e_2, \ldots, \mathbb{Z}e_s$ sont des groupes monogènes. (Cycliques infinis)
Ainsi

$$A = T(A) \oplus L = A_{p1} \oplus \ldots \oplus A_{ps} \oplus \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \ldots \oplus \mathbb{Z}e_s$$

N.B. si p est premier et si A est un groupe fini tel que $pA = \{0\}$, A est un ***p-groupe***, on peut considérer A comme un espace vectoriel sur le corps $\mathbf{F}_p = \mathbb{Z}/p\mathbb{Z}$, A est de type fini, il est somme directe de droites vectorielles (dans le groupe ce ne sont que les sous groupes cycliques qui décomposent A.