-

Algebre I

0.1 Introduction

L'algèbre classique est l'étude de la résolution d'équation : $\mathrm{x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0}$ *ou x est l'inconnue : une équation polynomial de degrés n*

$$\mathrm{n = 1}: \textit{équation linéaire} \quad \mathrm{x + a_0 = 0 \Leftrightarrow x = -a_0}$$

L'étude de la résolution d'un système linéaire est dit l'algèbre linéaire, vu au 1er semestre

$$\mathrm{n = 2}: \textit{equation quadrilatique} \quad \mathrm{x^2 + a_1x + a_0 = 0 \Leftrightarrow x = -\frac{a_1}{2} \pm \sqrt{(\frac{a_1}{2})^2 - a_0}}$$

Connue dès le IX dans le traité "al-jabr" du savant perce al-Kwarizmi (algèbre linéaire)

$$\mathrm{n = 3}: \textit{équation cubique} \quad \mathrm{x^3 + a_2x^2 + a_1x + a_0 = 0}$$

$\mathrm{x + \frac{a_2}{3} := u \dashrightarrow u^3 + au = b \Rightarrow u = \sqrt[3]{\frac{b}{2} + \sqrt{(\frac{b}{2})^2 + (\frac{a}{3})^3}} + \sqrt[3]{\frac{b}{2} - \sqrt{(\frac{b}{2})^2 + (\frac{a}{3})^3}}}$

-del Ferro 1515, Cardano 1545

$$\mathrm{n = 4}: \textit{équation quatique} \quad \textit{(il existe aussi une solution en degre } n \leq 3$$

-Ferrari 1540

Conclusion : Pour n$\leq$ 4, on peut ecrire les solution de l'equation polynomial de degres n a partir des coeficient, via des addition, soustraction, multiplication, division, et racines : cette equation est dit "resoluble par radicaux"

Question : et degre n$\geq$ 5, Reponse : l'equation de degre n$\geq$ 5 n'est pas resoluble par radicaux

— Galois (1832) : *caracterisation des equations resoluble par radicaux*

Ces résultat ont nescessité l'introduction d'outils d'un type nouveau : des "structure lgébriques abstraites", dont l'étude est le sujet de ce cours

Plan :

- Chapitre I : Groupe
- Chapitre II : Anneaux et Corps
- Chapitre III : Algebre Lineaire

- le n gone regulier est constructible a la regle et au compas $\Leftrightarrow$ *la décomposition de n est de la forme* $\mathrm{n} = 2^{\mathrm{n}}\mathrm{p1}, ..., \mathrm{p_r}$*, avec* $\mathrm{p_i} \neq \mathrm{p_j}$ *pour* $\mathrm{i} \neq \mathrm{j}$*, et les pi des premier de la forme :* $\mathrm{p} = 2^{2^{\nu}} + 1$ *("premier de Fermat")*

P ex : n=3,4,5,6,7,8...,12 est constructible ? ; V, V, V, V, X, V, X, V, X, V

Théoreme des nombres :

- Si p est premier et a un entier non divisible par, p, alors $\mathrm{a}^{\mathrm{p}-1} - 1$ est multiple de p
- il n'existe pas d'entier non nul x,y,z tq $\mathrm{x}^{\mathrm{n}} + \mathrm{y}^{\mathrm{n}} = \mathrm{z}^{\mathrm{n}}$ pour n> 2

L'algèbre moderne s'enseigne dans un ordre anti chronologique

Historiquement :

$\boxed{\text{probleme concret}} \rightarrow \boxed{\text{tente de resoudre}} \rightarrow \boxed{\text{Theorie formelle}}$

Pedagogiquement :

$\boxed{\text{Theorie formelle}} \rightarrow \boxed{\text{application a la resoltuion}}$

Consequence : *La théorie est assez arride et abstraite*
Un des but : *entammer la deduction logique le raisonnement formel, la redaction preuve rigoureuse*

1 Chapitre I : Groupes

La structure de groupe est simple (une loi 3 axiome), mais les concept les plus importants sont deja presents

1.1 Groupe : axiomes et exemples :

Définitions : *Soit G un ensembles muni d'une loi de composition, c a d, une application qui à deux élléments de G associe un troisieme élément de g noté :* $\mathrm{G} \times \mathrm{G} \to \mathrm{G}$

G est appele un groupe si il satisfait les 3 axiomes suivants :

(G1) $\mathrm{g} * (\mathrm{h} * \mathrm{k}) = (\mathrm{g} * \mathrm{h}) * \mathrm{k}, \quad \forall \mathrm{g}, \mathrm{h}, \mathrm{k} \in \mathrm{G}$ *(Associativité)*
(G2) $\exists\ \mathrm{e} \in \mathrm{G} \quad \mathrm{tq} : \mathrm{e} * \mathrm{g} = \mathrm{g} * \mathrm{e} = \mathrm{g}, \quad \forall \mathrm{g} \in \mathrm{G}$ *(éléments neutre)*
(G3) $\forall \mathrm{g} \in \mathrm{G}, \exists \mathrm{g}' \in \mathrm{G} \quad \mathrm{tq} : \mathrm{g} * \mathrm{g}' = \mathrm{g}' * \mathrm{g} = \mathrm{e}$ *(Inverse)*

Si de plus, G satisfait :

$$\mathrm{g} * \mathrm{h} = \mathrm{h} * \mathrm{g} \quad \forall \mathrm{g}, \mathrm{h} \in \mathrm{G}$$

Le groupe G est dit abéliens (ou comutatif)

La cardinalite de G noté $\mid \mathrm{G} \mid$, est appele l'ordre de G

Remarques et notation :

1. Formellement, un groupe est donc la donné d'une pair (G, *) , avec G un ensemble et * une loi de composition. Mais on le note habituellement G.
   -De meme, on notera habituellement $\mathrm{g} * \mathrm{h} := \mathrm{gh}$
   -Dans le cas abelien, on notera souvent $\mathrm{g} * \mathrm{h} := \mathrm{g} + \mathrm{h}$

2. (G1) signifie que l'on a pas a se soucier des parenthese p ex :
   $$((\mathrm{g}_1, \mathrm{g}_2)\mathrm{g}_3)\mathrm{g}_4 = (\mathrm{g}_1(\mathrm{g}_2\mathrm{g}_3))\mathrm{g}_4 = \mathrm{g}_1((\mathrm{g}_2\mathrm{g}_3)\mathrm{g}_4) = \mathrm{g}_1(\mathrm{g}_2(\mathrm{g}_3\mathrm{g}_4))$$
   qu'on notera simplement : $(\mathrm{g}_1\mathrm{g}_2\mathrm{g}_3\mathrm{g}_4)$

3. Lélément neutre est unique :

en effet : *Soit* $\mathrm{e}_1; \mathrm{e}_2 \in \mathrm{G}$ *deux éléments neutre. Alors :*

$$\mathrm{e}_2 = \mathrm{e}_1 * \mathrm{e}_2 = \mathrm{e}_1 \quad \square$$

On le note habituellement $\mathrm{e}, \mathrm{e}_\mathrm{g}, 1, 1_\mathrm{G}$ *ou* $0, 0_\mathrm{G}$ *dnas le cas abelien.*

Remarques :

4. L'égalité g'g = e fait de g' un inverse à gauche de g et gg" = e fait de g" un inverse à droite de g
   Si les deuxs coïncident :

$$\mathrm{g}' \overset{(\mathrm{G2})}{=} \mathrm{g}'\mathrm{e} = \mathrm{g}'(\mathrm{gg}") \overset{(\mathrm{G1})}{=} (\mathrm{g}'\mathrm{g})\mathrm{g}" = \mathrm{eg}" \overset{(\mathrm{G2})}{=} \mathrm{g}"$$

Dans un groupe, (G3) stipule l'existence pour tout g ∈ G d'un inverse (=inverse à gauche et inverse a droite) :
Il est donc unique !

— On le note habituellement g^{-1}, ou -g dans le cas abélien.
— On note aussi g+(-h) := g-h

On obtient donc :

$$gg^{-1} = g^{-1}g = 1, \quad \text{et} \quad g - g = 0 \quad \textit{Dans le cas abéliens}$$

5. Etant donné g∈ G et n∈ $\mathbb{Z}$, la n-ième puissance de g est l'élément $g^n \in G$ défini par :

$$g^n := \begin{cases} g * g * ... * g \text{ (n fois)} & \text{si } n > 0 \\ e & \text{si } n = 0 \\ g^{-1} * ... * g^{-1} \ (\mid n \mid) & \text{si } n < 0 \end{cases}$$

On le montre formelement (ex2, S1) Les règle de calcul :

i) $\forall x, g, h \in G, \quad xg = xh \to g = h\,; \quad \text{et} \quad gx = hx \to g = h$

ii) $\forall g, h \in G, \quad g^{-1})^{-1} = g; \quad \text{et} \quad (gh)^{-1} = h^{-1}g^{-1}$

iii) $\forall g \in G, \forall n, m \in /Z, \quad g^n g^m = g^{n+m}\,; \quad \text{et} \quad (g^n)^m = g^{n \times m}$

Questions : $(gh)^n = g^n h^n$ *?*

6. Attention : *Pour verifier que (G, *) est un groupe il faut montrer (G1),(G2),(G3), mais aussi verifier que la loi est "interne",* $g, h \in G \Rightarrow g * h \in G$
Par exemple : $G = \{-1, ., 1\}$, *muni de l'addition*

Exemple :

1. $\mathbb{Z} := \{..., -2, -1, 0, 1, 2, ...\}$ muni de l'addition (+)

est un groupe abélien d'ordre infini.

De même, $(\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ sont des groupes abéliens d'ordre infini.
$\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$ *muni de la multiplication est un groupe abélien d'ordre* ∞, *de même que* $\mathbb{R}^*, \mathbb{C}^*$

Par contre : $\mathbb{N} := \{0, 1, 2, ...\}$ satisfait (G1), (G2), mais pas (G3) : ce n'est pas un groupe -(on parle de monnïde)

2. Si E est un K-espace vectoriel (K = $\mathbb{R}$ ou $\mathbb{C}$), alors (E, +) est un groupe abélien :

Ce sont les axiomes (A1)-(A4) d'un espace vectoriel

3. Pour tout $n \geq 1$, l'ensemble GL(n ;K) := $\{M \in M_n(K) \mid \det(M) \neq 0\}$

Est un groupe pour la multiplication matricielle (K = $\mathbb{R}$ *ou* $\mathbb{C}$) :
Le groupe général linéaire de degrés n sur K

Demonstration :

◊ Si $M_1, M_2 \in GL(n; k)$, alors $\det(M_1, M_2) = \det M_1 \det M_2 \quad \neq 0$

On a donc bien :

G1. $M_1(M_2M_3) = (M_1M_2)M_3 \quad (\forall M_1, M_2, M_3 \in M_n(K))$: vu en algebre linéaire

G2. $e = I_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} : \quad I_n \cdot M = M \cdot I_n = M \quad (\forall M \in M_n(K))$

G3. $M \in GL(n,k) \Rightarrow \det M \neq 0 \Rightarrow \exists M^{-1} \quad tq \quad MM^{-1} = M^{-1}M = I_n$

De plus :

$$1 = \det(I_n) = \det(M^{-1}M) = \det(M^{-1}) \cdot \det(M) \Rightarrow \det(M^{-1}) \neq 0 \Leftrightarrow M^{-1} \in GL(n,k)$$

Par exemple, pour n=1, on obtient à nouveau $GL(n,K) = K^*$ *avec la multiplication*

Mais GL(n,K) n'est pas abélien pour $n > 1$ $\square$

4. Dans le même genre : $K = \mathbb{R}$ ou $\mathbb{C}$, $n \geq 1$

$$SL(n,K) := \{M \in M_n(K) \mid \det M = 1\}$$

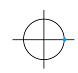
Est un groupe pour la multiplication matricielle : le groupe spécial linéaire de degrés n sur K (facile)
Par exemple, si n=1, SL(1,K) $=\{(1)\}$: *Une des incarnations du groupe trivial*

5. L'ensemble $S^1 := \{z \in \mathbb{C} \mid \quad \| Z \| = 1\}$ est un groupe abéliens pour la multiplication complexe. (facile)

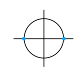
6. Pour $n \geq 1$, l'ensemble des racine n-ième de l'unité :

$$\mu_n(\mathbb{C}) := \{z \in \mathbb{C} \mid z^n = 1\}$$

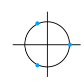
est un groupe abéliens d'ordre n pour la multiplication complexe (facile)
Exemple :



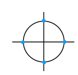
n=1 $\quad \mu_1(\mathbb{C}) = \{1\}$, le groupe trivial



n=2 $\quad \mu_2(\mathbb{C}) = \{-1, 1\}$



n=3



n=4 $\quad \mu_4(\mathbb{C}) = \{1, 2, -1, -2\}$

etc.. $\quad \mu_n(\mathbb{C})$ *est l'une des incarnation du groupe cyclique d'ordre n*

7. Soit X un ensemble non vide quelcquonque,

Posons :

$$S(X) := \{f(: X \to X \mid f \textit{ bijective}\}$$

C'est un groupe par la composition des application c'est le groupe symétrique sur X

Demo :

— f,g : $X \to X$ *bijective* $\Rightarrow f \circ g$ *est bijective*
— f,g,h : $X \to X, f \circ (g \circ h) = (f \circ g) \circ h$
— $id_x : X \to X \quad tq \quad id_x \circ f = f \circ id_x = f \quad (\forall f : X \to X)$
— $f : X \to X$ bijective $\Rightarrow \exists g : X \to X \quad tq \quad f \circ g = g \circ f = id_x$

(vu en logique et théorie des ensembles)

Si $X = \{1, 2, ..., n\}$, alors S(X) est noté Sn :
C'est le groupe des permutations de n objet

Un éléments $\sigma \in \mathrm{S_n}$ est souvent noté $\begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}$

Exemples :

n=1 $\quad \mathrm{S_1} = \{\mathrm{id}\}$, *Le groupe initial*

n=2 $\quad \mathrm{S_2} = \{\mathrm{id}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\}$

n$\geq 3 \neq \mathrm{S_n}$ *n'est pas abélien*

8. Si (G,*) et ($\mathrm{G_2}$, $\circ$) sont deux groupes, alors le produit cartésiens $\mathrm{G_1} \times \mathrm{G_2} := \{(g_1, g_2) \mid g_1 \in G, g_2 \in G_2\}$ est un groupe pour :
$(g_1, g_2) \cdot (h_1, h_2) := (g_1 * h1, g_2 \cdot h_2)$ (facile)

C'est le produit direct de $\mathrm{G_1}$ et $\mathrm{G_2}$

Plus généralement, pour $g_1, G_2, ..., G_n$ *des groupes, le produit* $G_1 \times G_2 \times ... \times G_n$ *est un groupe pour la loi :*

$$(g_1, ..., g_n)(h_1, ..., h_n) := (g_1h_1, ..., g_nh_n)$$

Exemples : $(\mathbb{R}^n, +)$ est le groupe donné par le produit direct de n copies de $(\mathbb{R}, +)$

— G := $\{-1, 1\} \times \{-1, 1\}$ est appelé le groupe de Klein

$$G_1 \times G_2 \textit{est abéliens} \Leftrightarrow G_1 \textit{ et } G_2 \textit{sont abéliens.}$$

9. (moin formel, voir Geo I pour les details)

Soit $P \subset \mathbb{R}^n$, Alors, l'ensemble Sym(P) := $\{f : \mathbb{R}^n \to \mathbb{R}^n \mid$ f est une isometrie, f(P) =P $\}$
est un groupe par la composition de sapplication.
- C'est le groupe symétrique de P dans $\mathbb{R}$*

"Nombre measure sire, groupe measure symmetry"

Exemple : pour n=2, les isomerie du plan $\mathbb{R}^2$ sont des composition de translation et de réfléxions par des droites :

— P =  $=\mathbb{R}^2$. sym(P) ={id} groupe trivial

— P = une droite ——— P
Sym(P) contient en particulier toute les transitions parrallèles a P

1.2 Sous groupe

Définition : Soit G un groupe. Un sous ensemble H de G est appelé sous-groupe de G, noté H< G, si H est un groupe pour la restriction de la loi de composition sur G

Concretement il faut verifier :
1. $(\forall h_1, h_2 \in H) \quad h_1, h_2 \in H$
2. $e_G \in H$
3. $(\forall h \in H) \quad h^{-1} \in H$

Mais en fait ces trois condition sont équivalente a une seule :

Proposition I.1 : Soit G un groupe, et H⊂ G un sous ensemble non vide. Alors,

$$H \text{ est un sous-groupe de } G \Leftrightarrow (\forall h_1, h_2 \in H) \quad \text{on a : } h_1 h_2^{-1} \in H$$

Preuve : $\Rightarrow$: Soit donc $h_1, h_2 \in H$. On a $h_2 \in H \Rightarrow h_2^{-1} \in H$
On a donc $h_1 \in H, h_2^{-1} \in H \Rightarrow h_1 h_2 \in H$

$\Leftarrow$: On a $H \neq \emptyset \Rightarrow \exists h \in H$; $\Rightarrow h \cdot h^{-1} \in H \Leftrightarrow e \in H$; ((2) ok)
(pour vérifier (3), fixons $h \in H$ et appliquons l'hypothese a ; $h_1 = e \in H, h_2 = h$
On a donc ; $e \cdot h^{-1} = h^{-1} \in H$; ce qui montre (3) ; Pour verifier (1), fixons $h_1, h_2 \in H$;
on sait que ; $h_2^{-1} \in H$ Par notre hypothese, on a donc ; $h_1(h_2^{-1})^{-1} = h_1 h_2 \in H$; ce qui montre (1) et conclut la preuve

Attention : Il faut vérifier que $H \neq \emptyset$ (revient a verifier $e \in H$)

Exemples de sous groupes : -

1. Tout groupe G admet $H= \{e\}$ et H=G comme sous groupe. Un sous groupe de G qui n'est pas de cette forme est dit sous-groupe propre
2. On a la chaine de sous groupe (propre) suivante :
   $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$
3. De même, on a : $(\mathbb{Q}*, \cdot) < (\mathbb{R}*, \cdot) < (\mathbb{C}*, \cdot)$
4. Si F est un sous ensemble vectoriel d'un espace vectoriel E, alors $(F,+) < (E, +)$
5. SL(n,K) $<$ GL(n,K)
6. Pour tout n, $(\mu(\mathbb{C}), \cdot) < (S^1, \cdot)$
7. Pour $X \neq \emptyset$ un ensemble , et $A \subset C$ un sous ensemble $\{f \in S(X) | f(A) = A\}$ et
   $\{f \in S(X) | f(a) = a \quad \forall a \in A\}$ est un sous-groupe de S(X).
8. Pour tout $n \in \mathbb{Z}$, le sous ensemble $n\mathbb{Z} := \{n \cdot m | m \in \mathbb{Z}\}$ des multiple de n est un sous groupe de $\mathbb{Z}$ (ex 1,2)

Fait ce sont les seul

9. Soit G un groupe quelqconque . Alors, $Z(G) := \{h \in G | gh = hg \quad \forall g \in G\}$ est un sous groupe de G, appelé le centre de G

Demo :
Vérifions (1), (2), (3)

(2) $\forall g \in G$, on a $ge=eg \; (=g) \Rightarrow e \in Z(G)$

(1) Soient $h_1, h_2 \in Z(G)$; on veut verifier $h_1, h_2 \in Z(G)$: $\forall g \in G$ on a :
$g(h_1, h_2) = (gh_1)h_2 = (h_1 g)h_2 = h_1(gh_2) = h_1(h_2 g) = (h_1 h_2)g$

(3) Soit $h \in Z(G)$; on veut voir $h^{-1} \in Z(G)$
$\forall g \in G$, on a $gh = hg \Rightarrow h^{-1} \cdot (gh) \cdot h^{-1} = h^{-1}(hg)h^{-1} \Rightarrow h^{-1} \in Z(G)$

10. Soit G un groupe quelcconque, et g$\in$ G fixé Alors :
$Z_g(g) := \{h \in G | gh = hg\}$ est un sous groupe de G le centralisateur de g dans G

Remarque : Pour G un groupe fixé, voici une nouvelle méthode pour construire des sou-groupe :

Fixons E$\neq \emptyset$ un sous ensemble de G, et posons :

$$H =< E >:= \{g_1 g_2 ... g_n \in G | n \geq 1, \forall i, g_i \in E \textit{ ou } g_i^{-1} \in E\} \cup \{e_g\}$$

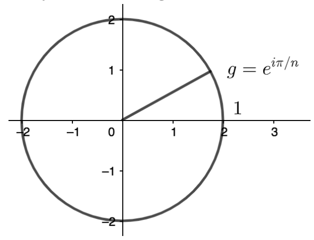
C'est un sous groupe de G, appelé le sous groupe engendré par E.
On dit que E est un systeme de générateur de H

Finalement : s'il existe $g \in G$. tq G=< g >, alors on dit que G est un groupe cyclique. Cela signifie que tous les élements de G sont de la fomre $g^n, n \in \mathbb{Z}$

Exemples de groupes cyclique :

1. G=$(\mathbb{Z}, +)$ est cyclique (d'ordre infin), engendre par g = + 1
   En effet $\forall n \in \mathbb{Z}$, on peut écrire
$$n = \begin{cases} \underbrace{1 + 1 + ... + 1}_{n\,\text{fois}} & \text{si } n > 0 \\ 0 & \text{si } n = 0 \\ \underbrace{(-1) + ... + (-1)}_{n\,\text{fois}} & \text{si } n < 0 \end{cases}$$
2. $\forall n \geq 1$, G=$\mu(\mathbb{C})$ est cyclique engendré par $g = e^{2i\pi/n}$ tout élément de $\mu_n(\mathbb{C})$ est de la forme :

$e^{2i\pi/n \cdot k} = g^k$



Terminologie : Soit g$\in$ G. Alors $o(g) := |< g >|$ *Est appelé l'ordre de $g \in G$*

Ainsi :
— si o(g)=∞, on a $g^n \neq e$ $\forall n \neq 0$
— si $o(g) = n < \infty$, cela signifie $< g >= \{e, g, g^2, ...?g^{n-1}\}$ et $g^n = e$
Ainsi o(g) = n est la plus petite puissance (positive) de g qui donne e

Exemples : -

1. $o(g) = 1 \Leftrightarrow g = e$
2. Dans G=$(\mathbb{Z}, +)$ but éléent m$\neq$ 0 a ordre $o(m) = \infty$
3. Dans $G = \mu(\mathbb{C})$, l'élement $g = e^{2i\pi/n}$ a ordre $o(g) = n$
4. Dans V=$\{-1, 1\} \cdot \{-1, 1\}$, les 3 élement $\neq e = (1, 1)$ ont ordre

1.3 Homomorphisme de Groupe

Définition : Une application $\varphi : G \to G'$ entre deux groupe est appel" un homomorphisme (de groupe) si il satisfait une unique condition :

$$\boxed{\forall G_1, G_2 \in G, \quad \textit{on a} \quad \varphi(G_1, G_2) = \varphi(G_1)\varphi(G_2)}$$

Remarques :

1. Il serait naturel de demander d'avoir aussi :

$$\varphi(e_g)e'_g \quad et \quad \varphi(g^{-1}) = \varphi(g)^{-1} \quad \forall g \in G$$

Ce sont en fait des consequence de la définition :

Demo $\varphi(e_g)\varphi(e_g) = \varphi(e_g e_g) = \varphi(e_g) = \varphi(e_g)e'_g \Rightarrow \varphi(e_g) = e'_g$; $(\forall g \in G)$, $\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e_g) = e'_g$;
de même $\varphi(g^{-1})\varphi(g) = e'_g \Rightarrow \varphi(g^{-1}) = \varphi(g)^{-1}$

2. Si : $\varphi : G \to G'$ et $G' \to G"$ sont des homomorphisme, alors $(\varphi \circ \varphi)(g_1, g_2) = \varphi(\varphi(g_1 g_2)) = \varphi(\varphi(g_1)\varphi(g_2))$ $=\varphi(\varphi(g_1))\varphi(\varphi(g_2)) = (\varphi \circ \varphi)(g_1)(\varphi \circ \varphi)(g_2)$

Rappel : $(G, *), (G', \cdot)$ groupe

$\varphi : G \to G$*est un homomorphisme si :*$\forall g_1, g_2 \in G$, $\varphi(g_1, *g_2) = \varphi(g_1) \cdot \varphi(g_2)$

Terminologie : Soit $\varphi : G \to G'$ un homomorphisme :
- Son noyau est défini par $\mathrm{Ker}(\varphi) := \{g \in G | \varphi(g) = e'_G\} \subset G$
- Son image est défini par $\mathrm{Im}(\varphi) := \{\varphi(g) | g \in G\} \subset G'$

Proposition I.2 :

i) $\mathrm{Ker}(\varphi)$ est un sous groupe de G et $\mathrm{Ker}(\varphi) = \{e_G\} \Leftrightarrow \varphi$*injectif*
ii) $\mathrm{Im}(\varphi)$ est un sous groupe de G', et $\mathrm{Im}(\varphi) = G' \Leftrightarrow \varphi$ *surjectif*

Preuve :

i) On a : $\varphi(e_G) = e_{G'} \Rightarrow$ $e_G \in \mathrm{Ker}(\varphi)$ *qui est donc non vide*;
Pour vérifier que $\mathrm{Ker}(\varphi) < G$; *il suffit par Prop I.1 de voir :* $g_1, g_2 \in \mathrm{Ker}(\varphi) \Rightarrow g_1, g_2 \in \mathrm{Ker}(\varphi)$: Soient donc $g_1, g_2 \in \mathrm{Ker}(\varphi)$; *calculons :* $\varphi(g_1, g_2)^{-1}) = \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1}$;
d'ou : $g_1 g_2^{-1} \in \mathrm{Ker}(\varphi)$ $e_{G'}(e_{G'}^{-1} = e_{G'}$

Montrons : $\mathrm{Ker}(\varphi) = \{e_g\} \Leftrightarrow \varphi$ *injectif*
$\Leftarrow$: *Supposons* φ *injectif, et montrons* $\mathrm{Ker}(\varphi) \subset \{e_G\}$

Soit donc g$\in \mathrm{Ker}(\varphi)$; *on a :* $\varphi(g) = e_{G'} = \varphi(e_G) \Rightarrow g = e_G$
$\Rightarrow$: *Supposons :* $\mathrm{Ker}(\varphi) = \{e_G\}$, *et posons :* $g_1, g_2 \in G$ tq $\varphi(g_1) = \varphi(g_2)$; A voir : $g_1 = g_2$
Calculons : $\varphi(g_1, g_2) = \varphi(g_1)\varphi(g_2) = \varphi(g_1) \cdot \varphi(g_1)^{-1} = e_G \Rightarrow g_1 g_2^{-1} \in \mathrm{Ker}(\varphi) = \{e_G\}$ *On a donc :* $g_1 g_2^{-1} = e_G$ *d'ou* $g_1 = g_2$
(ii) Ex5, S2 $\Box$

Exemple d'homomorphisme :

1. Pour tout groupe G, id :$G \to G$ est un homomorphisme $\mathrm{Ker}=\{e\}, \mathrm{Im} = G)$
2. Pour tout sous-groupe H<G, l'inclusion H$\to$ G est un homomorphisme h$\to$ h
3. Pour tout groupe G,G', on a l'homo; $G \to G', g \to e_{G'}$ *c'est l'homomorphisme trivial* (Ker=G, Im=$\{e_{G'}\}$)
4. Soit G un groupe et g$\in$ G; Alors l'application : $\varphi : \mathbb{Z} \to G, \varphi(n) = g^n$ est un homomorphisme : $\varphi(n+m) = g^{n+m} = g^n \cdot g^m = \varphi(n)\varphi(m)$; Par Définition, Im$\varphi$=$< g >$, et $\mathrm{Ker}\varphi = \begin{cases} o(g)\mathbb{Z} & \mathrm{si}\, o(g) < \infty \\ \{0\} & \mathrm{si}\, o(g) = \infty \end{cases}$

5. Notons que $\mathbb{R}^*+ := (0,\infty)$ est un groupe pour la multiplication réelle : L'application $(\mathbb{C}^*,\cdot) \to \mathbb{R}^*+,\cdot)$, $z \to |z|$ est un homomorphisme ($|z\cdot w| = |z|\cdot|w|$) de noyau S^1, et d'image $\mathbb{R}^*+$

6. det :GL(n,K) $\to$ K* est un homomorphisme (car $\det(M_1M_2) = \det M_1 \cdot \det M_2$) de noyau SL(n,K), et d'im age K*

7. Une application linéaire f :E$\to$ E' est un homomorphisme de (E,+) à (E',+)

8. L'application exponentielle $\varphi : (\mathbb{R},+) \to (\mathbb{C}^*,\cdot)$, $\varphi(x) = e^{i\pi}$ est un homomorphisme (car : $e^{i(x+y)} = e^{ix}\cdot e^{iy}$; d'image S^1, et de noyau $2\pi\mathbb{Z} := \{2\pi\cdot K | k \in \mathbb{Z}\}$

9. soit $m \in \mathbb{Z}$ ($m \neq 0$). Alors la multiplication par m $\mathbb{Z} \to \mathbb{Z}, n \to m\cdot n$ est homomorphisme (car $m(n_1+n_2) = mn_1 + mn_2$), de noyau $\{0\}$ et d'image $m\mathbb{Z}$

10. L'applciation sgn : $(\mathbb{R}^*,\cdot) \to \{-1,1\}$, $\operatorname{sgn}(x) = \begin{cases} +1 & \text{si } x > 0 \\ -1 & \text{si } x < 0 \end{cases}$ est un homomorphisme, de noyau $\mathbb{R}^*+$, et d'image $\{-1,1\}$

Définition : -
Un homomorphisme $\varphi : G \to G'$ *est appelé un isomorphisme s'il existe un homomorphisme* $\pitchfork : G' \to G$ *tel que* $\varphi\circ\pitchfork = id_{G'}$ *et* $\pitchfork\circ\varphi = id_G$ *s'il existe un tel isomorphisme, on dit que G et G' sont isomorphe, noté* $G \cong G'$

Remarque : 1. Un homo $\varphi : G \to G'$ est un isomorphisme $\Leftrightarrow$ φ est un homomorphisme bijectif

$\Rightarrow$: φ isomorphisme $\Rightarrow$ φ *est homomorphisme et* $\exists$ $\pitchfork$ tq $\varphi\circ\pitchfork = id(\Rightarrow \varphi\,\text{surj})$; *et* $\pitchfork\circ\varphi = id(\Rightarrow \varphi\,\text{inj})$ *d'ou* φ bijectif

$\Leftarrow$: *Si* φ *est bijectif, alors*; $\exists \pitchfork : G' \to G$ tq $\varphi\circ\pitchfork = id$ et $\pitchfork\circ\varphi = id$ *Reste a voir :*
$\pitchfork$ *est un homomorphisme En effet : soient* $g_1', g_2' \in G'$: $\pitchfork(g_1',g_2') = \pitchfork(\varphi(\pitchfork(g_i))\cdot\varphi(\pitchfork(g_2'))) = \pitchfork(\varphi(\pitchfork(g_i)\cdot\pitchfork(g_2')))$

2. $id_a : G \to G$ est un isomorphisme
   $\varphi : G \to G', \pitchfork : G' \to G"$ *isom* $\Rightarrow$ $\pitchfork\circ\varphi : G \to G"$ *est un isomorphe*
   $\varphi : G \to G'$ *isomorphe* $\Rightarrow \varphi^{-1} : G' \to G$ *isomorphe* $\Rightarrow$ *"est isom" est une relation d'équivalence*

3. On a tendence à identifer 2 groupe isomorph, de la même manière qu'on identifie 2 ensemble en bijection en th-des-ensemble, et 2 esp vectoriel isomorphe en algebre linéaire

4. Toutes les propriété étudier en th-des-groupe sont invarient par isomorphisme
   p ex : si $G \cong G'$, alors $|G| = |G'|$, G abélien $\Leftrightarrow$ G' abélien, G a un encadement 2 éléments d'ordre 3 $\Leftrightarrow$ G'a ...

5. pour montrer que G,G' sont isomorphes, il faut mexhiber un isomophisme G$\to$ G' pour montrer que G,G' ne sont pas isomorphe, il faut trouver une propriété invariante que G a mais pas G'

Exemples d'isomorphismes :

1. Tous les groupe d'ordre 1 sont isomorphe (c'est le groupe trivial)

2. Tous les groupe d'ordre 2 sont isomorphe (en particulier : $\mu_2(\mathbb{C}) \cong S_2$)

Demo :
En effet soit G un groupe d'ordre 2, Alors, on a ; G={e, g} avec ee=e, eg=ge=g, et ; gg=e (inverse)

.	e	g
e	e	g
g	g	e

Soient donc G=$\{e, g\}$, et G'=$\{e', g'\}$ 2 groupe ; L'app $\varphi : G \to G'$, $\begin{matrix} e & \to e' \\ g & \to g' \end{matrix}$, est un isomorphisme

3. Tous les groupe d'ordre 3 sont isomorphe
4. Tous les groupe d'ordre 4 ne sont pas isomorphe : $\mu_4(\mathbb{C}) \ncong \{-1,1\} \cdot \{-1,1\} := V$
   En effet i$\in \mu_4(\mathbb{C})$ est d'ordre 4, alors que les éléments de V sont d'orde 1 ou 2
5. L'application $\varphi : (\mathbb{R}, +) \to (\mathbb{R}^*+, \cdot)$,$\varphi(x) = e^x$ est un isomorphisme
   ($e^{x+y} = e^x \cdot e^y$, bijectif d'inverse log : $\mathbb{R}^*+ \to \mathbb{R}$)
6. Si f :X $\to$ Y est une bijection, alors $\varphi : S(X) \to S(Y), \varphi(\sigma) = f \circ \sigma \circ f^{-1}$ est un isomorphisme (exercice)

Terminologie : Un isomorhisme $\varphi : G \to G$ est appelé un automorhisme de G

Remarque : L'ensemble Aut(G) des automorphisme de G, est un sous groupe pour la composition des applications (Remarque 2 ci dessus)

Retour en arriere :

* $H < G \Leftrightarrow$ H est un groupe pour * restreinte a H ; $\Leftrightarrow$ (1) $h_1, h_2 \in H \Rightarrow h_1, h_2 \in H$;
(2) eg $\in H$; (3) $h \in H \Rightarrow h^{-1} \in H$

$\Leftarrow$: ✓ ; $\Rightarrow$: H est un groupe pour * ; $\Rightarrow \exists e_H \in H$ tq $e_H \cdot H = h \cdot e_H = h \quad \forall h \in H$

a voir : $e_H = e_G$; en effet : $e_H \cdot e_H = e_H = e_H \cdot e_G$; $e_H = e_G$

* question sur $o(g) := | < g > | \to ex1, S3$

* etre isomorphe est une relation d'équivalence : Attention la classe de tous les groupes n'est pas un ensemble

Rappel : G groupe ; Aut(G) = $\{\varphi : G \to G \| \varphi \textit{isomorphisme}\}$

Exemple d'isomorphisme : -

1. Déterminons Aut($\mathbb{Z}$) ; Remarquons d'abord que tout homo $\varphi : \mathbb{Z} \to \mathbb{Z}$ est donné par la multiplication par n=$\varphi(1) \in \mathbb{Z}$

En effet : pour n> 0, on a ; $\varphi(n) = \varphi(\underbrace{1 + ... + 1}_{n}) = \varphi(1) + ... + \varphi(1) = \varphi(1) \cdot n$

pour n< 0 : $\varphi(n) = \varphi((-1) + ...) = (-1) \cdot \varphi(-1)$; $= (-n)(-\varphi(1)) = \varphi(1) \cdot n$

pour n=0, $\varphi(0) = 0$; $= \varphi(1) \cdot 0$

on a en fait : $(\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}), \circ)$ est isomorphe a $(\mathbb{Z}, \cdot)$ comme monoïdes , via; $\varphi \to \varphi(1) \in \mathbb{Z}$ *ainsi Aut($\mathbb{Z}$) est donné par les éléments inversible de Hom($\mathbb{Z}, \mathbb{Z}$) $\cong \mathbb{Z}$,r par* $\{-1, 1\}$; On a donc : $\boxed{\mathrm{Aut}(\mathbb{Z}) \cong \{-1, 1\}}$

2. Pour G un groupe quecquonque, et g$\in$ G l'application tq : G$\to \iota$, $\iota_g(x) = gxg^{-1}$ *est un automorphimse de G appele la conjugaison par g ($\iota_g = \mathrm{id}_G$ si G est abélien)*

Demo : $\forall x, y \in G, \iota_g(xy)$; $= g(xy)g^{-1}$; $= gx(g^{-1}g)yg^{-1}$; $= (gxg^{-1})(gyg^{-1})$; $\iota_g(x)\iota_g(y)$; $\Rightarrow \iota_g$ est un homorphisme

De plus : $\iota_g^{-1}(\iota_g(x)); \quad = g^{-1}(gxg^{-1})g; \quad = x \Rightarrow \iota_g^{-1} \circ \iota_g = id_G$; de meme , $\iota_g \circ \iota_g^{-1} = id_G \Rightarrow \iota_g \in Aut(G)$

De plus : l'application z :$G \to Aut(G), g \to \iota_g$ est un homomorphisme de noyau Z(G). Son image notée Int(G) est formé des automorphisme intérieur de G :

Demo : $\forall g, h \in G, \forall x \in G : \iota_g(\iota_h(x)); \quad = g(hxh^{-1})g^{-1}; \quad = (gh)x(gh)^{-1}; \quad = \iota_{gh}(x) \Rightarrow \iota_g \circ \iota_{gh}; \quad g \in Ker(r) \Leftrightarrow \iota_g = id_G \Leftrightarrow \iota_g(x) = x \, \forall x \in G \Leftrightarrow gxg^{-1} = x \, \forall x \in G \Leftrightarrow gx = xg (\forall x \in G) \Leftrightarrow g \in Z(G)$

1.4 Théoreme de Lagrange sous groupe normaux et groupe quotients :

Notation : Pour des sous ensemble $X, y \subset G$ et $g \in G$, on note :

— $gX := \{gx | x \in X\}$
— $Xg := \{xg | x \in X\}$
— $XY := \{xy | x \in X, y \in Y\}$
— $X^{-1} = \{x^{-1} | x \in X\}$

Terminologie :
— Soit H un sous groupe d'un groupe G,
Un sous ensemble de la forme gH est appelé une classe a gauche (resp classe a droite) modulo H dans G
— L'ensemble des classe a gauche est noté $G/H := \{gH | \; g \in G\}$
— Le cardinal de G/H est appelé l'indice de H dans G, noté [G,H]

Remarque : - L'application $G \to G, g \to g^{-1}$ induit une bijection :

$$f : G/H := \{gH | g \in G\} \to H \backslash G := \{Hg | g \in G\}$$

Demo : En effet : $f(gH) = (gH)^{-1} = H^{-1}g^{-1} = Hg^{-1}$
Cette application est bijective, d'inverse $Hg \to g^{-1}H$; ainsi $[G,H] = |G/H| = |H \backslash G|$

Théoreme de Lagrange : -

$$\boxed{\textit{Si H est un sous groupe d'un groupe fini G, alors : } |G| = [G : H] \cdot |H|}$$

Preuve : Soit G un groupe et $H < G$ pour $g_1, g_2 \in G$, notons $g_1 \sim g_2 \Leftrightarrow g_2^{-1}g_1 \in H$

Vérifions que c'est une relation d'équivalence sur G :

- Réfléxive : $g \sim g \Leftrightarrow g^{-1}g \in H \Leftrightarrow e \in H$ ✓
- Symétie : $g_1 \sim g_2 \Leftrightarrow g_2^{-1}g_1 \in H \Rightarrow (g_2^{-1}g_1)^{-1}; \quad = g_1^{-1}g_2 \in H \Leftrightarrow: g_2 \sim g_1$
- Trnasitivité : $g_1 \sim g_2$ et $g_2 \sim g_3$; $\Leftrightarrow g_2^{-1}g_1 \in H$ et $g_3^{-1}g_2 \in H$; $\Rightarrow \underbrace{(g_3^{-1}g_2)(g_2^{-1}g_1)}_{g_3^{-1}g_1} \in H$

  $\Leftrightarrow g_1 \sim g_3$

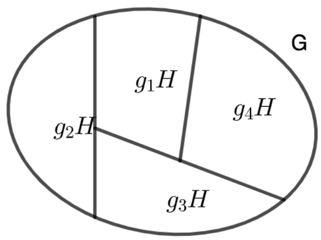
(3 axiome pour relation d'équialence $\leftrightarrow$ 3 axiome pour $H < G$)

Les classes d'équivalence correspondantes sont : -

$$[g]_H := \{g' \in G | g' \sim g\} = \{g' \in G | g^{-1}g^{-1} \in G\} = \{g' \in G | g' \in gH\} = gH$$

(Les classes a gauche !)

Ainsi les classes sa gauche partitionnent G, par défiition, on a [G :H] classes a gauche



Finalement, $\forall$g $\in$ G *on a une bijection :* $\begin{cases} \mathrm{H} \to \mathrm{gH} \\ \mathrm{h} \to \mathrm{gh} \end{cases}$

- Surjectif par définition de gH
- injectif : $gh_1 = gh_2; \quad \Rightarrow h_1 = h_2$: ✓

Ainsi on a G qui est partitionner en :[G :H] sous ensemble tous de cardinal |H| donc si G est fini $|G| = [G : H] \cdot |H|$ ☐

Corrolaire I.3 : Si H < G fini, alors |H| divise |G| et [G : H] donne |G| ☐

Corrolaire I.4 : Pour tout g $\in$ G avec G fini o(g) donne |G|
preuve : Appliquer I.3 a H=< g > ☐

Corrolaire I.5 : Si G est un groupe d'ordre premier, alors il est cyclique, et tout g$\in$ G$, g \neq$ e engendre G

Preuve : Soit donc G un groupe avec |G| premier ; et

(g$\in$ G , g$\neq$ e ; g $\neq$ e $\Leftrightarrow$ o(g) $\geq$ 2 $\oplus$ ParI.4, o(g)$|$ |G| $\Rightarrow$ o(g) = |G|) $\Rightarrow$< g >= G ☐

Corrolaire I.6 : Si G est fini alors $g^($|G|) = e($\forall$g $\in$ G)

Preuve : Pour tout g$\in$ G on a que o(g) $|$ |G| par I.4 donc $\exists$n $\in \mathbb{Z}$ tq |G| = o(g) $\cdot$ n
On a donc : $g^{|G|} = g^{o(g)\cdot n} = (g^{o(g)})^n = e^n = e$ ☐

Remqarque : On verra des conséquence de cet énoncé en th des nombre

Exemple : -

1. Pour G fini quelcquonque, et H= {e}; Les classe a gauche sont g $\cdot$ H = {g}, les élément de G
   On a : [G :H] =|G| ; d'ou |G| = |G| $\cdot$1

2. Pour G fini quelcquonque, et H=G $(g' \in G, g' = g(g^{-1}g' \in gG)$
   Les classe a gauche sont : gH = gG = G
   $\Rightarrow$ on a une unique classe a gauche, d'ou [G : G] = 1; on a l'équation |G|=1$\cdot$|G|

3. Pour G = Sn , posons H :=$\{\sigma \in S_n | \sigma(n) = n\} \cong S_{n-1}$ Calculons [G :H] dans ce cas en reprenant les notations de la preuve de Lagrange ; Pour $\sigma_1, \sigma_2 \in S_n$ on a : $\sigma_1 \sim \sigma_2 \Leftrightarrow \sigma_2^{-1}\sigma_1 \in H \Leftrightarrow \sigma_2^{-1}(\sigma_1(n)) = n; \quad \Leftrightarrow \sigma_1(n) = \sigma_2(n) \in \{1, 2, 3, ..., n\}$

   Ainsi le nombre d'équivalence correspondante est égale a :
   $|\{1, 2, ..., n\}|$ = n ; on a donc : [G :H] =n
   Par Lagrange on obtient : |Sn| = |G| = [G :H] $\cdot$|H| = n $\cdot$ $|S_{n-1}|$; Par notation : |Sn| = n(n-1)(n-2)...2$\cdot$1 = n ! ; comme il se dit

Question : -
Quand la loi de composition dans G induit - elle une structure de groupe sur G/H ? (via $(g_1, H)\cdot(g_2 H) := g_1 g_2 H$, ou $[g_1]_H \cdot [g_2]_H := [g_1 g_2]_H$)

Définition : Un sous groupe N< G est dit normal (on dit aussi distingué) dans G si :

$$\forall g \in G; \quad gNg^{-1} = N \quad \textit{ceci est noté } : N \triangleleft G$$

Proposition I.7 : - Si N◁ G, alors G/N est un groupe pour la loi de composition :

$$G/N \times G/N \to G/N, \quad (g_1 N, g_2 N) \to g_1 g_2 N$$

de plus : la projection canonique $\pi : G \to G/N$, $\pi(g) = gN$ est un homomorphisme surjectif de noyau N.

Preuve : -

- Vérifions que la loi de composition sur G/N est bien défini :
  Soit $g_1 h_1, g_2 h_2 \in G$ tq $h_1 N = h_1 N$ et $g_2 N = h_2 N$; on veut voir : $g_1 h_1 N = g_2 h_2 N$

On a : $\left.\begin{array}{l} g_1 N = N \Leftrightarrow g_1 \in N \overset{N \triangleleft G}{\Rightarrow} g_2^{-1}(h_1^{-1} g_1) g_2 \in N \\ g_2 N = h_2 N \Leftrightarrow h_2^{-1} g_2 \in N \end{array}\right\} = h_2^{-1} g_2 g_2^{-1} h_1^{-1} g_1 g_2 \in N \Leftrightarrow (h_1 h_2)^{-1} g_1 g_2 \in N \Leftrightarrow h_1 h_2 N = g_1 g_2 N$

- $\left.\begin{array}{l} \text{L'associativité découle de celle dans G} \\ \text{Le neutre est } e_{G/N} = [e]_N = eN = N \end{array}\right\}$ G/N est un groupe

l'inverse de gN est $g^{-1}N$

- Par définition $\pi(g_1 g_2) = g_1 g_2)N = g_1 N) = \pi(g_1)\pi(g_2)$: c'est un homomorphisme π est surjectif par définition de G/N et $Ker(\pi) = \{g \in G | \pi(g) = e_{G/N}\} = \{g \in G | gN = N\} = \{g \in G | g \sim_N e\} = \{g \in G | e^{-1} g \in N\} = N$ □

Terminologie : - G/N est appellé le groupe quotient (de G par N)

Remarque :

1. $N \triangleleft G \Leftrightarrow \forall g \in G, gNg^{-1} = N$
   $\Leftrightarrow \forall g \in G, gN = Ng \Leftrightarrow$ *les classes a gauche et a droite coincident*

2. $N \triangleleft G \Leftrightarrow \forall g \in G, \forall x \in N$, on a : $gxg^{-1} \in N$

Exemple : -

1. On a toujours $N=\{e\} \triangleleft G$ ($\forall g \in G$ on $geg^{-1} = e \in N$)

2. on a toujours $N=G \triangleleft G$ ($\forall g_1 x g^{-1} \in G$)

3. Si G est abéilen, alors tout sous groupe est normal ($\forall g \in G, \forall x \in N$, on a $gxg^{-1} = gg^{-1}x = x \in N$)

4. On a $Z(G) \triangleleft G$ (meme preuve)

5. $\varphi : G \to G'$ est un homomorphisme, alors $Ker(\varphi) \triangleleft G$

<u>preuve</u> : - Soit donc x∈ $Ker(\varphi)$ et g∈ G a voir : $gxg^{-1} \in Ker(\varphi)$; $\varphi(gxg^{-1})\varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(g)e \cdot \varphi(g)^{-1} = e$ □

Par I.7 : - réciproquemeny tout N$\triangleleft$

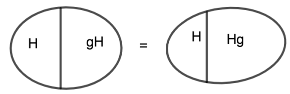
6. SL(n,K) $\triangleleft$GL(n, K) (car SL(n,K) = Ker(det : GL(n,K) $\to$ K*)

7. Pour tout groupe G, Int(G)$\triangleleft$Aut(G) (ex5, s3)

8. tout sous groupe et indice 2 est normal

Preuve : Soit H< G avec 2=[G :H] = |G/H| = |H\G| $\Rightarrow$ on a les partitions :

$$G = H \sqcup gH(g \notin H), \quad \text{et}\, G = H \sqcup Hg(g \notin H)$$



$$\left.\begin{array}{l} \textit{on a donc que :}\ gH = Hg \forall g \notin H \\ \textit{Pour :}\ g \in H, \textit{on a :} gH = Hg = H \end{array}\right\} \Leftrightarrow \forall g \in G, gH = Hg \Leftrightarrow H \triangleleft G \quad \square$$

9. Dans G=S3 , posons H = $\left\{ \mathrm{id}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$. Alors H $\ntriangleleft$ G

En effet, pour x=$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\in$ H et. g=$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, on a : $gxg^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \notin H$

Définition :

$\boxed{\text{Un groupe est dit simple si il n'as pas de sous groupe normal propre (ie , N} \neq \{e\}, G)}$

Exemple : - Si G est d'orre premier, alors G est simple (par lagrange)
(On verra : ce sont les seul groupe simple abélien)

Proposition I.8 : - Soit G un groupe N$\triangleleft$G , et :

$\varphi : G \to G'$ *un homomorphisme tq :*N $\subset$ Kerφ
Alors il existe un unique homomorphisme
$\overline{\varphi} : G/N \to G'$ tq$\overline{\varphi} \circ \pi = \varphi$

Terminologie : -

- Un tel énoncé est une "propriété universelle"
- On dit que 'φ passe au quotient"

Preuve : -

— $\overline{\varphi}(gN) = \overline{\varphi}(\pi(g)) = (\overline{\varphi} \circ \pi)(g) = \varphi(g)$ (en notation $[g]_N$, on a : $\overline{\varphi}([g]_N) = \varphi(g)$)

— $\overline{\varphi}$ est bien défini (ie : existe) : soient $g_1, g_2 \in G$ tq $g_1N = g_2N$
$\Leftrightarrow g_2^{-1}g_1 \in N \subset \mathrm{Ker}\varphi \Rightarrow e = \varphi(g_1^{-1}g_1) = \varphi(g_2)^{-1}\varphi(g_1) \Leftrightarrow \varphi(g_2) = \varphi(g_1)$

Ainsi $\overline{\varphi}$ est bien défini

— $\overline{\varphi}$ homomorphisme : $\overline{\varphi}((g_1N)(g_2N)) = \overline{\varphi}(g_1g_2N) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \overline{\varphi}(g_1N)\overline{\varphi}(g_2N)$

Proposition I.9 : - Soit $\varphi : G \to G'$ un homomorphisme

Alors φ *definit un homomorphisme* $\boxed{\overline{\varphi} : G/\mathrm{Ker}\varphi \to \mathrm{Im}(\varphi)}$

Exemple : -

1. L'homomorphisme trivial $\varphi : \begin{matrix} G \to G' \\ g \to e_{G'} \end{matrix}$ reduit l'isomorphisme $G/G \cong \{e\}$

2. L'homomorphisme $id_G : G \to G$ reduit l'isomorphisme $G/\ \{e\} \cong G$

3. l'homomorhpisme det : $GL(n,K) \to K^*$ reduit l'iso : $GL(n,K)\ /\ SL(n,K) \cong K^*$

4. L'homomorphisme $\varphi : (\mathbb{C}, +) \to (C^*, \cdot)$, $\varphi(z) = e^{2\pi iz}$ a image $\mathbb{C}^h$ et noyau Z, d'ou l'isomorphisme : $\mathbb{C}/\mathbb{Z} \cong \mathbb{C}^*$ La restriction de φa $(\mathbb{R}, +)$ a image $(S^1, \cdot)$ et noyau $\mathbb{Z}$ d'ou : $\mathbb{R}/\mathbb{Z} \cong S^1$

5. L'homomorphisme $\iota : G \to Aut(G)$ a image Int(G) et noyau Z(G), d'ou l'iso $G/Z(G) \cong Int(G)$

1.5 Groupes cycliques

Considérons l'exemple de $G = (\mathbb{Z}, +)$.
Pour tout $n \in \mathbb{N}$, on a le sous-groupe $H = n\mathbb{Z} = \{\ldots, -2n, n, 0, n, 2n, \ldots\}$
La partition de $\mathbb{Z}$ en classes modulo H est $\mathbb{Z} = n\mathbb{Z} \sqcup (1 + n\mathbb{Z}) \sqcup (2 + n\mathbb{Z}) \sqcup \ldots \sqcup ((n-1) + n\mathbb{Z})$
$H \lhd \mathbb{Z}$ car $\mathbb{Z}$ est abélien.

$$\frac{\mathbb{Z}}{H} = \frac{\mathbb{Z}}{n\mathbb{Z}} = \{[0], [1], [2], \ldots, [n-1]\},\ \text{n classes d'équivalences}$$

pour la relation : $[a] = [b] \iff a - b \in n\mathbb{Z} \overset{not.}{\iff} a \equiv b \mod n$, a congrue à b modulo n.

$\frac{\mathbb{Z}}{n\mathbb{Z}}$ est appelé le groupe des <u>entiers modulo n</u>.
La loi : $[a] + [b] = [a + b]$, rete de la division par n.

Par exemple pour n = 2, on a $\frac{\mathbb{Z}}{2\mathbb{Z}} = \{[0], [1]\}$, avec la loi donnée par la table

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

Pour n = 3, on $\frac{\mathbb{Z}}{3\mathbb{Z}} = \{[0], [1], [2]\}$ et

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

Notons que $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est cyclique pour tout $n \in \mathbb{Z}$.

Démonstration : -

En effet :
— si n = 0, $\frac{\mathbb{Z}}{0\mathbb{Z}} = \mathbb{Z}$, infini cyclique engendré par 1
— si n > 0, $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est engendré par [1], car $[i] = \underbrace{[1] + \cdots + [1]}_{\text{i fois}}$

On verra : tout G cyclique est isomorphe à $\frac{\mathbb{Z}}{n\mathbb{Z}}$ pour un unique $n \in \mathbb{N}$! Pour cela on a besoin

Proposition I.10 Soit H un sous-groupe de $\mathbb{Z}$. Alors, il existe un unique $n \in \mathbb{N} = \{0, 1, 2, \ldots\}$ tel que $H = n\mathbb{Z}$.

Démonstration : -
Soit $H < \mathbb{Z}$. Si $H = \{0\}$, alors $H = o\mathbb{Z}$, trivial.
Supposons donc $H \neq \{0\}$. Dans ce cas, on a $H \cap \{1,2,3,\ldots\} \neq \varnothing$, car $h \in H \implies -h \in H$
Soit n le plus petit élément de $H \cap \{1,2,\ldots\}$.

Affirmation : $H = n\mathbb{Z}$

En effet : $[\supset]$: $n \in H \overset{H \text{ groupe}}{\Longrightarrow} n\mathbb{Z} = \{\ldots, -n-n, -n, 0, n, n+n, \ldots\} \subset H$.

$[\subset]$: Soit $h \in H \subset \mathbb{Z}$. A voir : h est un multiple de n.
Par l'algorithme de division euclidienne : $\exists q \in \mathbb{Z}, r$ avec $0 \leq r < n$ tel que $h = qn + r$. $H < \mathbb{Z}, h \in H, n \in H \implies r = h - qn \in H$. Si $r > 0$, alors $r \in H \cap \{1,2,\ldots\}$, impossible par minimalité de n (et $r < n$). Ainsi on a $r = 0$, d'où $h = qn \in n\mathbb{Z}$

Finalement, n est unique car $|\frac{\mathbb{Z}}{H}| = |\frac{\mathbb{Z}}{n\mathbb{Z}}| = \begin{cases} n & \text{si } n > 0 \\ \infty & \text{si } n = 0 \end{cases}$ donc impossible d'avoir $H = n\mathbb{Z} = m\mathbb{Z}$ avec $n \neq m$

Théorème I.11 : Classification des groupes cycliques Soit G est un groupe cyclique.
Si G est infini, alors $G \cong \mathbb{Z}$. Sinon, $G \cong \dfrac{\mathbb{Z}}{n\mathbb{Z}}$ avec $n = |G|$.

Démonstration : -
Soit donc G un groupe cyclique. Par définition, il existe $g \in G$ tel que $G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$. Cela signifie que l'homomorphisme φ: $\begin{cases} \mathbb{Z} & \to G \\ k & \mapsto g^k \end{cases}$ est surjectif.
Considérons $H = \ker\varphi < \mathbb{Z}$. Par I.10, $\exists n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$

- Si $n = 0$, on a $\ker\varphi = 0\mathbb{Z} = \{0\} \iff \varphi$ injective $\implies \varphi$ iso $\implies G \cong \mathbb{Z}$.
- Si $n > 0$, on a $\ker\varphi = n\mathbb{Z}$, d'où un isomorphisme $\overline{\varphi}$: $\dfrac{\mathbb{Z}}{n\mathbb{Z}} G$ par I.9, d'où $G \cong \dfrac{\mathbb{Z}}{n\mathbb{Z}}$. Finalement $|G| = |\frac{\mathbb{Z}}{n\mathbb{Z}}| = n$.

Exemple

$$\mu_n(\mathbb{C}) \cong \frac{\mathbb{Z}}{n\mathbb{Z}}, \text{via} \exp(\frac{2i\pi k}{n}) \longleftrightarrow [k]$$

Voyons une applicaoin à la théorie des nombres (petit théorème de Fermat). Quelques rappels :

Terminologie

— Pour $a, b \in \mathbb{Z}$, on dit que a divise b, noté $a \mid b$, si $\exists q \in \mathbb{Z}$ tel que $aq = b$.

— Pour $u, v \in \mathbb{Z}$, le plus grand commun diviseur de u et v, noté $\mathrm{pgcd}(u, v)$, est défini par :

$$\mathrm{pgcd}(u,v) := \begin{cases} 0 & \mathrm{si u{=}v{=}0} \\ \max\{n \in \mathbb{N} \mid n|u \text{ et } n|v\} & \text{sinon} \end{cases}$$

— Deux entiers $u, v \in \mathbb{Z}$ sont dits premiers entre eux si $\mathrm{pgcd}(u, v) = 1$

Proposition I.12 Pour $u, v \in \mathbb{Z}$, $\{un + vm \mid n, m \in \mathbb{Z}\} = \mathrm{pgcd}(u, v)\mathbb{Z}$.

Démonstration : -

Soient donc $u, v \in \mathbb{Z}$

Le sous-ensemble $H := \{un + vm \mid n, m \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$.

$H \ni u \cdot 0 + v \cdot 0 = 0 \implies H \neq \varnothing$

$$h_1 = un_1 + vm_1 \quad (n_1, m_1, n_2, m_2 \in \mathbb{Z}) \implies h_1 - h_2 = u(\overbrace{n_1 - n_2}^{\in\mathbb{Z}}) + v(\overbrace{m_1 - m_2}^{\in\mathbb{Z}}) \in H$$

$h_2 = un_2 + vm_2$

Par I.10, $\exists k \in \mathbb{N}$ tel que $H = k\mathbb{Z}$. A voir : $k = \mathrm{pgcd}(u, v) =: j$.

Comme $u, v \in H = k\mathbb{Z}$, on a $k|u$ et $k|v \overset{\text{déf. de pgcd}}{\implies} 0 \leq k \leq j$.

D'autre part, $j|u$ et $j|v \implies$ u et v sont des multiples de j.

$\implies$ tout élément de H est un multiple de j $\overset{k\in H}{\implies}$ k est un multiple de j.

$\implies j \leq k \implies j = k$.

Théorème de Bézout Deux entiers $u, v \in \mathbb{Z}$ sont premiers entre eux si et seulement si il existe $m, n \in \mathbb{Z}$ tels que $um + vm = 1$

Démonstration : -

Par I.12, u, v premiers entre eux $\iff \{un + vm \mid n, m \in \mathbb{Z}\} = \mathbb{Z} \iff \{un + vm \mid n, m \in \mathbb{Z}\} \ni 1$

Revenons à $\frac{\mathbb{Z}}{n\mathbb{Z}}$, avec $n > 0$.

Notation : $(\dfrac{\mathbb{Z}}{n\mathbb{Z}})^* := \{[m] \in \dfrac{\mathbb{Z}}{n\mathbb{Z}} \mid \mathrm{pgcd}(m, n) = 1\}$

Sur $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$, définissons $[m_1] \cdot [m_2] = [m_1 \cdot m_2]$

Affiramation : $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$ est un groupe pour la multiplicaion ci-dessus.

Démonstration : -

Notons d'abord que $\mathrm{pgcd}(m_1, n) = \mathrm{pgcd}(m_2, n) = 1 \implies \mathrm{pgcd}(m_1 \cdot m_2, n) = 1$

De plus, si $[m_1] = [m'_1]$, alors $m'_1 = m_1 + k_1 n \implies m'_1 m'_2 = m_1 m_2 + (k_1 + k_2 + k_1 k_2 n)n$. De même pour $[m_2] = [m'_2]$ ce qui implique $[m'_1 m'_2] = [m_1 m_2]$

Ainsi, la loi est interne et bien définie. Elle est clairement associative le neutre est $[1] \in \frac{\mathbb{Z}}{n\mathbb{Z}}$

Reste à voir : inverse.
Soit $[m] \in \frac{\mathbb{Z}}{n\mathbb{Z}}^*$. Par Bézout, $\exists x, y \in \mathbb{Z}$ tels que $mx + ny = 1 \in \mathbb{Z}$

$$\implies [1] = [mx] + \underbrace{[ny]}_{=0} = [m][x] \implies \text{m a comme inverse } [x]$$

Finalement, $mx + ny = 1 \underset{\text{Bézout}}{\implies}$ x et n sont premiers entre eux $\iff [x] \in \frac{\mathbb{Z}}{n\mathbb{Z}}^*$.

$(\mathbb{Z}/_{n\mathbb{Z}}{}^* := \{[m] \in \mathbb{Z}/_{n\mathbb{Z}} | \mathrm{pgcd}(m,n) = 1\}$ est un groupe pour $[m_1] \cdot [m_2] = [m1 \cdot m_2]$.

Notation : -
Pour $n \in \{1, 2, 3, ...\}$, notons $\varphi(n) := \#\{m \in \{1, 2, 3...\} | \mathrm{pgcd}(m, n) = 1\}$ la fonction phi d'Euler

Exemple : - $\varphi(1) = 1, \quad \varphi(2) = 1, \quad \varphi(4) = 2, \quad \varphi(5) = 4...$

Corrolaire : [Euler] - Soient n$\geq$ 1 un entier, et a$\in \mathbb{Z}$ tq a et n sont premier entre eux : Alors; $a^{\varphi(n)} - 1$ est un multiple de n

Preuve : -
Fixons $n \geq 1$ et $a \in \mathbb{Z}$; Par hypothese, on a : ; $[a] \in (\mathbb{Z}/_{n\mathbb{Z}}) * := G$ *Le groupe G a ordre :*$|G| = \varphi(n)$
Par corrolaire I.6, on a ; $g^{|G|} = e_G$, ie :

$$[1] = [a]^{\varphi(n)} = [a^{\varphi(n)}] \in (\mathbb{Z}/n\mathbb{Z})* \subset (\mathbb{Z}/n\mathbb{Z})* \Leftrightarrow a^{\varphi(n)} - 1 \in n\mathbb{Z} \quad \square$$

Petit Théoreme de Fermat : -

Soit p un premier et a un entier qui n'est pas un multiple de p. Alors, $a^{p-1} - 1$ est un multiple de p

Preuve : - C'est Cor I.12 dans le cas n=p $\square$

Exemple : -

⊙ p=2 : a impair ⇒ a-1 pair
⊙ p=3 : a pas un multiple de 3 ⇒ $a^2 - 1$ est multiple de 3
⌜ a=3k+i, $i \in \{1, 2\} \Rightarrow a^2 = 9k^2 + 6ki + (2^2 - 1)$ un multiple de 3 ⌟

1.6 Commutateur, abélisé, groupe résoluble

Terminologie : - Soit G un groupe, et g,h $\in$ G Le commutateur g et h est $[g,h] := ghg^{-1}h^{-1} \in G$

Remarque : -

1. $[g,h] = e \Leftrightarrow ghg^{-1}h^{-1} = e \Leftrightarrow gh = hg \Leftrightarrow$ g et h commutent
   En partivulier, G est abélien $\Leftrightarrow [g, h] = e \quad (\forall g, h \in G)$

2. Si $\varphi : G \to G'$ est un homomorphisme, alors :

$$\varphi([g, h]) = \varphi(ghg^{-1}h^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1} = [\varphi(g), \varphi(h)]$$

3. $[g,h]^{-1} = (ghg^{-1}h^{-1})^{-1} = hgh^{-1}g^{-1} = [h, g]$

4. $[e,g] = [g,e] = e \quad (\forall g \in G)$

5. *Mais le produit de 2 commutent n'est en général pas un commutateur !*

On définit donc :

Terminologie : - Soit G un groupe. Le groupe dérivié de G est le sous groupe de G engendré par le commutateur :

$$[\mathrm{G},\mathrm{G}] := \langle\{[\mathrm{g},\mathrm{h}]|\mathrm{g},\mathrm{h}\in\mathrm{G}\}\rangle < \mathrm{G}$$

6. par rem 3, tout éléments de [G,G] est un produit de commutateur

7. Par rem 2, si $\varphi : \mathrm{G}\to\mathrm{G}'$ est un homomorphisme ; $\varphi([\mathrm{G},\mathrm{G}])\subset[\varphi(\mathrm{G}),\varphi(\mathrm{G})]$

Exemple : -

1. G abélien $\Leftrightarrow$ [G,G] $=\{e\}$ par rem 1

2. Pour $\mathrm{G}=\mathrm{S}_3$, on a $[\mathrm{S}_3,\mathrm{S}_3]$ est le sous groupe d'ordre de S_3 engendrer par $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ [ex, 6,5,4]

3. Pour n$\geq$ 1 et K$=\mathbb{R},\mathbb{C}$ on a $\boxed{[\mathrm{GL}(\mathrm{n},\mathrm{K}),\mathrm{GL}(\mathrm{n},\mathrm{K})]=\mathrm{SL}(\mathrm{n},\mathrm{k})}$

$[\subset]$: clair car $\det(\mathrm{M}_1,\mathrm{M}_2,\mathrm{M}_1^{-1},\mathrm{M}_2^{-1}) = \det\mathrm{M}_1\cdot\det\mathrm{M}_2(\det\mathrm{M}_1)^{-1}(\det\mathrm{M}_2)^{-1} = 1\checkmark$

$[\supset]$: Trivial si n=1 car SL(n,K) $=\{1\}$ mais pas facile pour n$>$ 1! Voici li'dée :

Si $\mathrm{n}\geq 3$, alors on peut montrer (dur) que SL(n,K) est engendrer par les matrices $\mathrm{t}_{\mathrm{i},\mathrm{j}}(\lambda) := \begin{pmatrix}1 & & \mathrm{j}\\ & \ddots & \lambda\\ & & \lambda\end{pmatrix}\mathrm{i}$

avec i$\neq$ j et $\lambda\in\mathrm{K}$

Ensuite pour n$\geq$ 3 on isole la relation : $\mathrm{t}_{\mathrm{ij}}(\lambda)\mathrm{t}_{\mathrm{kj}},(1)\mathrm{t}_{\mathrm{ik}}(\lambda)^{-1}\mathrm{t}_{\mathrm{kj}}(-1)^{-1}\begin{cases}\mathrm{i}\neq\mathrm{j},\mathrm{j}\neq\mathrm{k}\\ \mathrm{i}\neq\mathrm{k}\end{cases}$

Cela implique : SL(n,K) $\subset[\mathrm{SL}(\mathrm{n},\mathrm{K}),\mathrm{SL5n},\mathrm{K})]\subset[\mathrm{GL}(\mathrm{n},\mathrm{K}),\mathrm{GL}(\mathrm{n},\mathrm{K})]$

(pour n=2 une autre relation est utilisé, qui donne aussi SL(2,K) $\subset$ [SL(2,K),SL52,K)])

Notons que pour n$\geq$ 2 on a : [SL(n,K),SL(n,K)]=SL(n,K)

Théoreme I.13 : - Soit G un groupe quelqconque. Alors :

(i) [G,G] $\lhd$G

(ii) Le quotient G/[G,G] $:=\mathrm{G}_{\mathrm{ab}}$ est abélien

(iii) On a la propriété universelle suivante : Pour tout homo : $\varphi\mathrm{G}\to\mathrm{A}$ avec A abélien, il existe un unique homo $\overline{\varphi}:\mathrm{G}_{\mathrm{ab}}\to\mathrm{A}$ tq $\overline{\varphi}\cdot\pi=\varphi$

$$\begin{array}{ccc}\mathrm{G} & \overset{\forall\varphi}{\to} & \mathrm{A}\\ \downarrow & & \\ & \nearrow & \\ \mathrm{G}_{\mathrm{a,b}} & & \end{array}$$

Remarque : -

1. G_{ab} est appelé l'abélianisé de G
2. La prop univ signifie : le quotient G$\to\mathrm{G}_{\mathrm{ab}}$ est la manière la plus économe de rendre un groupe abélien : on "tue" les commutateur

Preuve : -

(i) Soit g$\in$ G quelqconque, et rg la conj par g Comme rg est un hom la remarque 7 donne :
$g[G,G]g^{-1} = rg([G,G]) \subset [rg(G), rg(G)] \subset [G,G]$ donc ; N$=[G,G]$ est un sous groupe normal

(ii) Par rem 1 $G_{ab} = G/N$ est abélien $\Leftrightarrow$ tout commutateur dans G/N est trivial
A voir donc : ($\forall g, h \in G$, on a : $[gN, hN] = e_{G/N}$, avec N $=$ [G,G]
En notant $\pi : G \to G_{ab} = G/N$; La projection on a ; $[gNhN]{=}[\pi(g), \pi(h)] = \pi([g,h]) = e_{G/N}$
car $[g,h] \in [G,G] = N = \mathrm{Ker}\pi$

(iii) Soit donc $\varphi G \to A$ un homo avec A groupe abélien ; Verifions N$=$[G,G] $\subset \mathrm{Ker}\varphi$, pour conclure a l'aide de Prop I.8

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & A \\ \pi \downarrow & & \\ & \nearrow & \exists' \overline{\varphi} \\ G/N = & G_{a,b} & \end{array}$$

En effet ; $\varphi([G,G]) \subset [\varphi(G), \varphi(G)] \subset [A,A] = \{o_A\}$ car A abélien
Ainsi on obtient ; $N \subset \mathrm{Ker}\varphi$ $\square$

Exemple : -

1. G abélien $\Leftrightarrow$ [G,G] $= \{e\} \Leftrightarrow G_{ab} = G$

2. Comme $|[S_3, S_3]|$ on a $(S_3)_{ab} \cong \mathbb{Z}/2\mathbb{Z}$ On remarque que $(\forall n \geq 2)(S_n)_{ab} = Sn\,/[Sn, Sn] \cong \mathbb{Z}/2\mathbb{Z}$ section (I.7)

3. $GL(n,K)_{ab} \cong GL(n,K)/SL(n,K) \cong K^*$

Terminologie : -
Pour un groupe G notons G$=G^{(0)}$; $G^{(1)} := [G^{(0)}, G^{(0)}]$; $G^{(2)} := [G^{(1)}, G^{(1)}, ..., G^{(k+1)} = [G^{(k)}, G^{(k)}], ...$
On obtient une suite dérivé de G

Définitions : -

$\boxed{\text{G est dit résoluble s'il existe } k \geq 0 \text{ tq } G^{(k)} = \{e\}}$

Exemple : -

1. G abélien $\Leftrightarrow G^{(1)} = \{e\} \Rightarrow$ G résoluble

2. Si S_2 sont abélien $\Rightarrow$ résoluble
S_3 pas abélien mais $[S_3, S_3]$ abélien $\Rightarrow (S_3)^{(2)} = \{e\} \Rightarrow S_3$ résoluble
S_4 est aussi résoluble (section I.7)
on verra S_n pas résoluble pour $n \geq 5$

3. GL(n,K) $=$ K* abélien $\Rightarrow$ résoluble GL(n,K) pas résoluble pour $n \geq 2$, car $G^{(1)} = SL(n,K), G^{(2)} = SL(n,K)$, etc
$G^{(k)} = SL(n,K) \quad \forall k \geq 1$

1.7 Groupe symétriques :

Rappel : X un ensemble ($\neq \emptyset$) , $S(X) := \{f : X \to X | f \text{ bijective}\}$ est un groupe
Si X et Y sont en bijection, alors $S(X) \cong S(Y)$ (serie 2)
S X est fini, disons $n = |X|$, alors $S(X) := S_n$ <u>Le groupe symetrique d'indice n</u>
$\sigma \in S_n$ est appelé une permutation (de n objets)

Ces groupe sont d'une grande importance, on particulier a cause de :

Théoreme de Cayley : -

$$\boxed{\text{Tout groupe est isomorphe a un sous groupe d'un groupe symétrique}}$$

Preuve : - Soit donc G un groupe quelconque

Posons : $X = G$ et $\varphi : \begin{array}{ll} G & \to S(G) \\ g & \to \varphi(g) \end{array}$ définie par $\varphi(g) : \begin{array}{ll} G & \to G \\ h & \to gh \end{array}$

$$\text{A voir : } \left.\begin{array}{ll} (1) & \varphi(g) \in S(G) \\ (2) & \varphi \text{ homomorphisme} \\ (3) & \varphi \text{ injective} \end{array}\right\} \Rightarrow \varphi \text{ définit un homomorphisme } G \overset{\cong}{\to} \operatorname{Im}(\varphi) < S(G), \text{ et } \checkmark$$

$$(1) \quad (\varphi(g) \circ \varphi(g^{-1}))(h); \quad = \varphi(g)(\varphi(g^{-1})(h)) = \varphi(g)(g^{-1}h) = g(g^{-1}h) = h$$
$$= id_G(h) \quad \forall h \in G$$

$$\left.\begin{array}{l} \Rightarrow \varphi(g) \circ \varphi(g^{-1}) = id_G \\ \text{De meme} \quad : \varphi(g^{-1}) \circ \varphi(g) = id_G \end{array}\right\} \Rightarrow \varphi(g) \text{ est bijective : d'inverse } \varphi(g^{-1}) \Rightarrow \varphi(g) \in S(G)$$

(2) Soient $g_1, g_2 \in G$; a voir : $\varphi(g_1) \circ \varphi(g_2) \in S(G)$

$\forall h \in G : \quad \varphi(g_1, g_2)(h) = (g_1 g_2) \cdot h = g_1 \cdot (g_2 h) = \varphi(g_1)(g_2 h) = \varphi(g_1)(\varphi(g_2)(h))$

$= (\varphi(g_1) \cdot \varphi(g_2)(h)$

(3) $g \in Ker(\varphi) \Leftrightarrow \varphi(g) = id_G \Leftrightarrow \varphi(g)(h) = h \quad \forall h \in G \Leftrightarrow gh = h \quad \forall h \in G \Rightarrow g = e_G$

$Ker\varphi = \{e_G\} \Leftrightarrow \varphi$ injective $\square$

Remarque : - Si G et fini, disons $|G| = n$ alors on obtient $G \cong \operatorname{Im}(\varphi) < S_n$
Si G est infini on n'a pas de $G <$ de S_n)

Dès a présent on se restreint a X fini, et l'on étudie donc :

$$S_n = S(\{1, 2, ..., n\}), \quad n \geq 1$$

Notation et terminologie : -

— Soit $1 \leq r \leq n$ Une permutation $\sigma \in S_n$ est un r-cycle si :
$$\exists \{x_1, ..., x_r\} \subset \{1, 2, 3, ..., n\} \text{ tq } \sigma(x_i) = x_{i+1}$$

Pour i=1,...,r-1 $\quad \sigma(x_r) = x_1$ et $\sigma(y) = y \ \forall y \in \{1, 2, 3, ..., n\} \backslash \{x_1, ..., x_r\}$ On note $\boxed{\sigma = (x_1, ..., x_r)}$

— Un 2 cycle est appellé une transposition (1-cycle est l'identité)
— On notera $\sigma \circ \tau := \sigma\tau \in S_n, \quad \sigma, \tau \in S_n$

Exemple : - D ans S_3 la permutation notée $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ en algebre linéaire

De meme $\tau \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ est notée $\tau = (2\ 3) = (3\ 2)$

Calculons $\sigma\tau = (1\ 2)(2\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3) \in S_3$

et $\tau\sigma = (2\ 3)(1\ 2) = (3\ 2\ 1)$ et l'on voit que S_3 n'est pas abélien :

Dernier calcul : $\tau\sigma\tau^{-1} = (2\ 3)(1\ 2)(2\ 3) = (1\ 3)$

Cela montrer meme que H=$< \sigma >= \{id, \sigma\}$ n'est pas normal dans S_3

proposition I.14 : - Soit $(x_1, x_2, ..., x_r)$ un cycle dans S_n

i) $(x_1x_2, ..., x_r) = (x_2x_3, ..., x_rx_1) \in S_n$

ii) $(x_1x_2...x_r) = (x_1x_2...x_j)(x_jx_{j+1}...x_r) \in S_n \quad \forall 1 \leq j \leq r$

iii) $L'\text{ordre de}\,(x_1, x_2, ..., x_r)$ dans S_n est r

iv) Pour tout $\tau \in S_n$ on a : $\tau(x_1, x_2, ...x_r)\tau^{-1} = (\tau(x_1)\tau(x_2)...\tau(x_r))$

v) Deux cycles a support disjoint commutent

Preuve : - i), ii) évident

iii) Par définition pour $\sigma = (x_1x_2...x_r)$, on a :

$$o(\sigma) = |<\sigma>| = \min\{k|\sigma^k = id\} = r$$

Preuve : - iv)

Supposons $r = 2, r : \sigma = (x_1x_2) := (i, j)$, Calculons :

$$\tau(i, j)\tau^{-1} \quad : k \to \begin{cases} \tau(j) & \text{si } k = \tau(i) \\ \tau(i) & \text{si } k = (\tau(i)\ , \quad c'\text{est } \tau(i)\tau(j) \\ \tau(\tau^{-1}(k)) = k, & \text{sinon} \end{cases}$$

$*$ pour le cas général on utilise ii) (et une recurence) pour obtenir :

$$\begin{aligned} \tau(x_1x_2...x_r)\tau^{-1} &= \tau(x_1x_2)...(x_{r-1}x_r)\tau^{-1} \\ &= \tau(x_1x_2)\tau^{-1}\tau(x_2x_3)\tau^{-1}...\tau(x_{r-1}x_r)\tau^{-1} \\ &= (\tau(x_1)\tau(x_2))(\tau(x_2)\tau(x_3))...(\tau(x_1.)\tau(x_r)) = (\tau(x_1)\tau(x_2).\tau(x_r)) \end{aligned}$$

v) Si $\sigma(x_1x_2..x_r)$ et $\tau = (y_1y_2...y_5)$ avec $\quad x_i \neq y_i \quad \forall i, j|$ alors $\sigma\tau = \tau\sigma$
est donné par $:\in S_n$ $\square$

Théoreme I.15 : -

$$\boxed{\text{Toute permutation est le produit de cycle a support disjoint}}$$

Preuve : - L'idée est clair : $1 \to \sigma(1) \to \sigma^2(1)... \to \sigma^r(1) = 1 \to$ un cycle
et on continue avec $i \notin \{i, \sigma(i)...\sigma^{r-1}(1)\}$ etc.

$*$ voici une preuve plus formelle :

Fixons $\sigma \in S_n$ une fois pour toute Sur $\{1, 2, ...n\}$ posons $i\sim j \Leftrightarrow \exists m \in \mathbb{Z}$ tq $i = \sigma^m(j)$

C'est une relation d'equivalence : $-i \sim i$ car $i = \sigma^0(i), \quad o \in \mathbb{Z})$

$-i \sim j \Leftrightarrow i =\sim^m (j) \Leftrightarrow j = \sigma^{-m}(i) \Rightarrow j \sim i \quad (m \in \mathbb{Z} \Rightarrow -m \in \mathbb{Z})$

$-i \sim j$ et $j \sim k \Leftrightarrow \exists m, l \in \mathbb{Z}$ tq $i = \sigma^m(j)$ et $j = \sigma^e(k)$

$\Rightarrow i = \sigma^m(\sigma^l(k)) = \sigma^{m+e}(k) \Rightarrow i \sim k \begin{pmatrix} m, e \in \mathbb{Z} \\ m + e \in \mathbb{Z} \end{pmatrix}$

Ainsi on obtient une partition : $\{1, 2, 3..., n\} = B_1 \sqcup B_2 \sqcup ... \sqcup B_k$ une classe d'équivalence

On verifie que $\forall s = 1, ..., k$ et $\forall i \in B_5$ on a : $\begin{array}{l} B_5 = \{i, \sigma(i), \sigma^2, ..., \sigma^{5-1}(i)\} \\ \text{ou } r := |B_5| \end{array}$

Si l'on pose $\sigma_5 := (i,\sigma(2), \sigma^2(i)...\sigma^{r-1}(i))$ pour s=1...k,
On obtient $\sigma = \sigma_1\sigma_2...\sigma_k$, avec support$(\sigma_5) = B_5$, et donc disjoint $\square$

Exemple : - $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 4 & 2 & 3 \end{pmatrix} \in S_6$

$\Rightarrow \sigma = (1\ 5\ 2)(6\ 3)$

Remarque : -
La décomposition d'une permutation en produit de cycle a support disjoint est unique à :

$$\left.\begin{array}{ll} 1) & \text{permutation des cycles [I.14, v)]} \\ 2) & \text{permutation cyclique de chaque cycle[I.14, i)]} \\ 3) & \text{1-cycle} \end{array}\right\} \quad \text{près}$$

Corollaire I.16 : - Toute permutation est produit de transposition

Preuve : - Soit $\sigma \in S_n$ par I.15 σ est produit de cycle ParI.14 chaque cycle est produit de transposition □ (voir ex6, serie 5)

Définition : -

La signatur d'une permutation $\sigma \in S_n$ est $\varepsilon(\sigma) := \prod_{1 \le i \le j \le n} \frac{\sigma(i) - \sigma(j)}{i - j} \in \mathbb{Q}^*$

Exemple : -

1. $\sigma = id \Rightarrow \varepsilon(id) = \prod_{i \le j} \frac{i-j}{i-j} = 1$
2. $\sigma = (1\ 2) \in S_3 \Rightarrow \varepsilon(\sigma) = \frac{2-1}{1-2} \cdot \frac{1-3}{2-3} \cdot \frac{2-3}{1-3} = -1$

Proposition I.17 : - La signatur prend ces valeur dans ±1 et défini un homomorphisme

$$\varepsilon : S_n \longrightarrow \{-1; 1\}$$

Preuve : - Notons d'abord que $\varepsilon\ (\sigma) = \prod_{\{i,j\} \subset \{1,\ldots,n\} i \ne j} \frac{\sigma(i) - \sigma(j)}{i - j}$

Idee de la preuve :

$$\left.\begin{array}{l} (1)\ \varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau) \\ (2)\ \text{si}\ \sigma\ \text{est une transposition alors,}\ \varepsilon(\sigma) = -1 \end{array}\right\} \Rightarrow \text{Par I.16 on a terminer}$$

(1) Pour $\sigma, \tau \in \mathrm{S_n}$ calculons :

$$\varepsilon(\sigma\tau) = \prod_{\{i,j\}} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{i - j} = \prod_{\{i,j\}} \left(\frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \cdot \frac{\tau(i) - \tau' j'}{i - j} \right)$$

$$= \prod_{\{i,j\}} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \cdot \underbrace{\prod_{\{i,j\}} \frac{\tau(i) - \tau' j'}{i - j}}_{=\varepsilon(\tau)}; \quad = \varepsilon(\sigma)\varepsilon(\tau)$$

$$= \prod_{\{k,l\}} \frac{\sigma(k) - \sigma(l)}{k - l} = \varepsilon(\sigma); \quad = \varepsilon(\tau) \quad \text{Cela demontre (1)}$$

(2) Soit $\sigma(u, v)$ une transposition quelconque. Calculons :

$$\varepsilon(\sigma) = \prod_{\{i,j\}} \frac{\sigma(i) - \sigma(j)}{i - j} = \underbrace{\left(\prod_{\substack{\{i,j\} \cap \{u,v\} \\ = \emptyset}} \frac{\sigma(i) - \sigma(j)}{i - j} \right)}_{=1} \cdot \underbrace{\left(\prod_{\substack{i=u \\ j \neq u,v}} \frac{\sigma(i) - \sigma(j)}{i - j} \right) \cdot \left(\prod_{\substack{i=v \\ j \neq u,v}} \frac{\sigma(i) - \sigma(j)}{i - j} \right)}_{=1} \cdot \left(\frac{\sigma(u) \cdot \sigma(v)}{u - v} \right)$$

□

Remarque : -

1. ainsi, $\sigma \in \mathrm{S_n}$ a $\varepsilon(\sigma) = 1 \quad (\text{resp} - 1) \Leftrightarrow$ *s'écrit comme produit d'un nb impair de transposition notons que ce produit n'est pas unique :*
   par exemple : $(1\ 3) = (2\ 3)(1\ 2)(2\ 3)$
   Mais la prop I.17 montre que la partie du nombre de transposition dans la decomposition d'une permutation donné est fixe !

2. .[Lien avec Alg I]
   Graphiquement : $\varepsilon(\sigma) = (-1)$
   p ex : $\sigma(1\ 2\ \ 3\ 4\ 5) \Rightarrow$
   $\varepsilon(\sigma) = (-1)^4 = 1$
   Cela decoule des fait suivant :
   (A)$(-1)^{\#\text{pts double}}$ est invarient par mouvement et donc bien défini
   (B) Pour $\sigma = (ij)$ # pts double est impair
   (C) Le nombre de point double est additif par composition des permutation

Terminologie : - Une permutation $\sigma \in \mathrm{S_n}$ est dite paire si $\varepsilon(\sigma) = +1 \quad (\text{resp} - 1)$

Définition : -

Le sous-groupe $\mathrm{A_n} := \mathrm{Ker}(\varepsilon) \triangleleft \mathrm{S_n}$ des permutation paires est appelé le groupe alterné de degré n

Remarque : - Si n 1 alors : $\varepsilon : \mathrm{S_n} \to \{-1, 1\}$ est surjective $\Rightarrow \mathrm{S_n}/\mathrm{A_n} \cong \{-1, 1\} \Rightarrow$

2. $= |\mathrm{S_n}/\mathrm{A_n}| = [\mathrm{S_n} : \mathrm{A_n}] = \frac{|\mathrm{S_n}|}{|\mathrm{A_n}|} \Rightarrow \boxed{|\mathrm{A_n}| = \frac{n!}{2}}$ pour n≥ 1

Exemple : -

$n = 1 \quad A_1 = S_1 = \{id\}$

$n = 2 \quad A_2 = \{id\} \triangleleft \{id, (1\ 2)\} = S_2$

$n = 3 \quad A_3 = \{id, (1\ 2\ 3), (1\ 3\ 2)\} \triangleleft S_3$

$*$ Un r-cycle a signatur $(-1)^{r-1}$, en particulier, les 3-cycle sont des A_n

Proposition I.18 : - Le groupe A_n est engendre par les 3 cycle :

Preuve : - Comme tout éléments de A_n est produit de nombre pair de transposition, il suffit de vérifier que tout produit de 2 transposition est produit de 3-cycle
Soient donc : (x_1, x_2) et (x_3, x_4) des transposition dans S_n

Cas1 : $\{x_1, x_2\} = \{x_3, x_4\} \Rightarrow (x_1, x_2)(x_3, x_4) = (x_1 x_2)(x_1 x_2) = id$ rien a verifier

Cas2 : $|\{x_1 x_2\} \cap \{x_3 x_4\}| = 1$, disons $x_1 = x_3$ et $x_2 \neq x_4$

Alors :

$$(x_1 x_2)(x_3 x_4) = (x_1 x_2)(x_1 x_4) = (x_2 x_1)(x_1 x_4) = (x_2 x_1 x_4)$$

Cas3 : $\{x_1, x_2\} \cap \{x_3 x_4\} = \emptyset \Rightarrow (x_1 x_2)(x_3 x_4) = (x_1 x_2 x_3)(x_2 x_3 x_4)$ □

Voici une serie de resultat qui illustrent beaucoup de concept vu au cours de ce chapitre

$\boxed{\text{La relation } \triangleleft \text{ n'est pas transitive}}$ (voir ex3 srie 3)

Posons $N_2 := \{\sigma \in A_4 | \sigma^2 = id\}$ et $N_1 = \{id, \alpha\}$ pour : $\alpha \in N_1 \backslash \{id\}$

$-N_2 \triangleleft A_4$: soit $\sigma \in N_2, \tau \in A_4$ Alors $\tau\sigma\tau^{-1} \in A_4$, et
$(\tau\sigma\tau^{-1})^2 = \quad (\tau\sigma\tau^{-1}) = \tau\sigma^2\tau^{-1} = \tau id\, \tau^{-1} = id \Rightarrow \tau\sigma\tau^{-1} \in N_2$

$-N_1 \triangleleft N_2$: : tous les elements de N_2 soit d'ordre 2 $\Rightarrow N_2$ abélien
$\Rightarrow$ tout sous groupe est normal

$-$Mais$N_1 \ntriangleleft A_4$: pex si $\alpha = (1\ 2)(3\ 4)$ et $\tau(1\ 2\ 3) \in A_4$
alors $\tau\alpha\tau^{-1} = (2\ 3)(1\ 4) \notin N_1$

$\boxed{[S\_n,S\_n] = A_N \quad \forall\ n}$

$\subset$: $\forall \sigma\tau \in S_n \quad \varepsilon([\sigma, \tau]) = [\varepsilon(\sigma), \varepsilon(\tau)] = 1$ car $\{-1, 1\}$ est abélien

$\Rightarrow [\sigma, \tau] \in A_n \Rightarrow [S_N, S_n] \subset A_n$

$\supset$: tout 3 cycle est un commutateur : $(x_1 x_2 x_3) = [(x_2 x_3)(x_1 x_2)]$ et on conclut □

$\boxed{\text{Pour } n \geq s, \quad [A_n, A_n] = A_n}$ $(\Rightarrow (A_n)_{ab} = \{1\} \quad \forall n \geq 5)$

$\subset$: ✓

$\supset$: Soit (i, j, k) un 3 cycle dans A_n : $n \geq 5$

$\Rightarrow \exists l, m \in \{1, ..., n\}$ tq $|\{i, j, k, l, m\}| = 5$

$\Rightarrow (i, l, k), (k, j, m)] =; \quad \underbrace{(i\ l\ k)(k\ j\ m)(i\ l\ k)^{-1}}_{=(i\ j\ m)}(kjm)^{-1} = (i\ j\ k)$

$\Rightarrow (i\ j\ k) \in [A_n, A_n]$ et l'on conclut par I.18 $\square$

$\boxed{S_n \text{ est resoluble} \Leftrightarrow n \in \{1, 2, 3, 4\}}$

— $S_1 = S_1^o = \{id\}$

— S_2 est abélien $\Rightarrow S_2^{(1)} := [S_2, S_2] = \{id\} \Rightarrow S_2$ résoluble

— $S_3^{(1)} = [S_2, S_3] = A_3$ abélien $\Rightarrow S_3^{(2)} = A_3^{(1)} = \{id\} \Rightarrow S_3$ résoluble

— $S_4^{(1)} = [S_4, S_4] = A_4, S_4 = [A_4, A_4] \cong \mathbb{Z}/2\mathbb{Z}$ abélien $\Rightarrow S_4^{(3)} = \{id\} \Rightarrow S_4$ résoluble

Pour $n \geq 5, S_n^{(1)}[S_n, S_n] = A_n \quad S_n^{(1)} = [A_n, A_n] = A_n \Rightarrow S_n = A_n \neq \{id\} \quad \forall k \geq \Rightarrow S_n$ n'est pas abélien !

$\boxed{\text{Pour tout } n > 2 \quad Z(S_n) := \{\sigma \in S_n | \sigma\tau = \sigma\tau \quad \forall \tau \in S_n\} \text{ est tivial}}$

Preuve : - Soit $\sigma \in S_n$ $(n \geq 3)$, $\sigma \neq id$

A voir : $\exists \tau \in S_n$ tq $\tau \circ \tau^{-1} \neq \sigma (\Rightarrow \tau\sigma \neq \sigma\tau \Rightarrow \sigma \notin Z(S_n))$

Par I.15 On peut ecrire $\sigma = \sigma_1\sigma_2...\sigma_s$ cycle a support disjoint
Notons R la longueur maximal de ces cycles, on a : $r \geq 2$ car sinon $\sigma = id$

Srlg Supposons que $\sigma_1 = (x_1, x_2, ..., x_r)$ avec $r \geq 2$

Cas 1 : $r \geq 3$
Dans ce cas prenons $\tau := (x_1, x_2) \in S_n$ Calculons :
$\tau\sigma\tau^{-1} = \tau\sigma_1\sigma_2...\sigma_5\tau^{-1} = \tau\sigma_1\tau^{-1}\sigma_2...\sigma_S = (x_2, x_1, x_3, ..., x_r)\sigma_2...\sigma_S (\neq \sigma...\sigma_S = \sigma)$

$\neq$ car $(x_2, x_1, ..., x_r) \neq (x_1, x_2, ...x_r)$ puisque $r \geq 3$

Cas 2 : $r = 2$ tous les cycles $\sigma_1, \sigma_2, ..., \sigma_S$ sont de longueur 1 ou 2
Comme $\sigma_1 = (x_1, x_2)$ et $n \geq 3$ $\quad \exists y \in \{1, ..., n\} \backslash \{x_1, x_2\}$ Posons $\tau := (x_1, y) \in S_n$

Calculons : $\tau\sigma\tau^{-1} = \tau\sigma_1...\sigma_S\tau^{-1} = \underbrace{(\tau\sigma_1\tau^{-1})}_{=(y, x_2)}...\underbrace{(\tau\sigma_S\tau^{-1})}_{\sigma'} = (y_1x_2) \cdot \sigma' \neq (x_1x_2) \cdot \sigma_2...\sigma_S = \sigma$

$(x_2 \to y) \quad (x_2 \to x_1)$

Cela conclut la preuve $\square$

Theoreme I.19 : -

$\boxed{\text{Pour tout } n \geq 5\ A_n \text{ est simple}}$

Remarque : -

1. Cela implque que $[A_n, A_n] = A_n$ pour $n \geq 5$ (deja vu)

$$\text{soit } N := [A_n, A_n] \triangleleft A_n\,; \quad A_n \text{ simple} \Rightarrow \left.\begin{array}{ll} N = \{id\} & \text{ou } N = A_n \\ \Updownarrow & \\ A_n \text{ abélien} & \text{faux pour } n \geq 4 \end{array}\right\} \Rightarrow N = A_n$$

2. A_4 n'est pas simple ($[A_4, A_4]$ est un n-groupe normal propre de A_n, voir serie 5)

Lemme I.20 : - Pour $n \geq 5$ tous les 3-cycle sont conjugué dans A_n

Preuve : - Soit donc (i, j, k) un 3-cycle quelqconque dans A_n , $n \geq 5$

Soit $\sigma \in S_n$ tq $\sigma(i) = 1, \sigma(j) = 2, \sigma(k) = 3$ on a : $\sigma(i, j, k)\sigma^{-1} = (1, 2, 3)$
— si $\sigma \in A_n$ on a terminer
— si $\sigma \notin A_n$, alors $\sigma^1 := (4, 5) \cdot \sigma \in A_n$ car $n \geq 5$ On a :

$$(\sigma)(i, j, k)(\sigma^{-1}) = (4, 5)(4, 5)(1, 2, 3)(4, 5) = (1, 2, 3) \quad \square$$

Preuve du Théoreme I.19 : -

Soit $N \triangleleft A_n$ ($n \geq 5$) $N \neq \{id\}$ A voir : $N = A_n$

Affirmation	N continet un 3-cycle
Cela implqie le theorme	Si N contient un 3-cycle comme $N \triangleleft A_n$ et $n \geq 5$
	N contient tout les 3-cycle par I.20
Par I.18	on aura $N \supset A_n$ d'ou $N = A_n$

Preuve de l'affirmation : - Comme $N \neq \{id\}$ on a $x \neq id$ Ecrivons $x = \sigma_1\sigma_2 ... \sigma_S \neq id$

Cas 1	cycle a longueur > 3 disons $\sigma_1 = (i, j, k, l, ...)$
	Posons $y := (i, j, k) \in A_n$
	$x \in N \Rightarrow x^{-1} \in N \overset{N \triangleleft A_n}{\Rightarrow} yx^{-1}y^{-1} \in N \overset{x \in N}{\Rightarrow} xyx^{-1}y^{-1} \in N$
Calculons	$xyx^{-1}y^{-1} = \underbrace{\sigma_1 y \sigma_1^{-1}}_{(jkl)} y^{-1} = (j\ k\ l)(i\ k\ j)$
	$(i\ l\ j) \in N$ donc ok

Cas 2, Cas 3 : on se ramene au cas 1, deja traité (sans détail ici) $\square$

1.8 Classification :

- (pour votre culture général **pas a l'examen**)
Classifier les groupes abélien n'est pas dur (voir Alg II) :

Theorme : -

> Soit G un groupe abélien fini. Alors, il existe une unique suite d'entier $m_1, m_2, ... m_S \geq 2$ ($S \geq 0$) tq $m_i | m_{i+1}$ $\forall i = 1, ..., S - 1$ et $G \cong \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_S\mathbb{Z}$

Remarque : - On montre facilement que si pgcd(m,n)=1 alors $Z : m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$

Exemple : - Classifier a iso pres tous les groupes abélien d'ordre $36 = 2 \cdot 2 \cdot 3 \cdot 3$

$$36 = 2 \cdot 19 = 3 \cdot 12 = 6 \cdot 6$$

Donc G abélien d'ordre 36 est isomorphe a exactement un groupe parmis :

$\mathbb{Z}/36\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

Par exemple : $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ par la remarque

le cas général (non-abélien) est infiniment plus dur
Mas les groupe finis simple peuvent etre considére comme les "brique" de base pour construire tous les groupe finis. Et on connait tous les groupes finis simple

Théoreme : - Tout les groupe finis simple est isomorphe a exactement un groupe parmi :

— $\mathbb{Z}/p\mathbb{Z}$ avec p premier

— A_n pour $n \geq 5$

— Les "groupe calssique" (typiquement des groupze de matrice sur un corp fini)

— 27 groupe "sporadique" (le plus grand a $8 \cdot 10^{53}$ éléments)

Qutient : -
X ensemble, $x \sim y$ est une relation d'équivalence sur X si :

$R-\ x \sim x$		On pose $[x] := \{y \in X \vert x \sim y\}$
$S-\ x \sim y \Rightarrow y \sim x$	$\forall x, y, z \in X$	la classe d'équivalence de $x \in X$
$T - x \sim y,\ y \sim z \Rightarrow x \sim z$	On note $X/\sim$ l'ensemble des classes d'équivalence, et	$\begin{cases} \pi : X \to X/\sim \\ \pi(x) = [x] \end{cases}$

Remarque : - Les classes d'équivalence forment une partition de X et :

$\forall x \in X$ x appartient a une unique classe d'équivalence

$x \in [x]$ par R
$x \in [y] \cap [z] \Leftrightarrow x \sim y,\ x \sim z \Leftrightarrow [y] = [z]$

Une application : f :X→ Y passe au quotient si $\boxed{x \sim y \Rightarrow f(x) = f(y)}$

On peut alors defini $\overline{f} : X/\sim \to Y$, $\overline{f}([x]) = f(x) (\Leftrightarrow \overline{f}(\pi(x) = f(x) \Leftrightarrow \overline{f} \circ \pi = f)$

Exemple : - X ={population mondiale} x∼ y ⇔ meme date de naissance
$X/\sim = \{date\}$

f :X ⇒ $\{0, 1, 2, ...,\}$
f(x) = l'age de x en annés, passe au Quotient $\overline{f} : \{dates\} \to \{0, 1, 2\}$
g(x) = nombre d'enfant : ,ne passe pas au quotient !

Exemple : - G groupe quelqconque , H< G
$g_1 \sim g_2 \Leftrightarrow g_2^{-1} g_1 \in H$: relation d'équivalence sur G (cf parmi)
$[g] = gH$, classe a gauche module H

2 Chapitre II : Anneaux et corps

2.1 Anneaux et corp axiome exemples

Cours "logique" : arithétique sur $\mathbb{Z}$

— "a divise b" dans $\mathbb{Z}$ si $\exists c \in \mathbb{Z}$ tq b=ac

— le pgcd de a et b : $d \geq 0$ tq $\begin{cases} d|a, \ d|b \\ \text{si } c|a \ c|b \end{cases}$ alors $c|d$

— $a,b \in \mathbb{Z}$, $b > 0$ $\quad \exists q, r \in \mathbb{Z}$ tq $\quad a=qb+r$ avec $0 \leq r < b$

— Theoreme fondamental de l'arithmétique :
tout $n > 1$ *s'écrit de façon unique comme produit de premier*

$\sim$

L ecadre formel ou cette théorie se generalise est celui des anneux 'euclidien) l'exemple dondamental est $\mathbb{Z}$ *mais on a aussi* $\mathbb{R}[X], \mathbb{Z}([i],...$ *C'est l'objjjet du Chap II*

II.1 Anneaux et corp : axiome et exemple

Définitions : - *un anneux est un ensemble A muni de deux loi de composition* :

$$+ : \begin{array}{ccc} A \times A & \to & A \\ (a,b) & \to & a+b \end{array}$$

$$\cdot : \begin{array}{ccc} A \times A & \to & A \\ (a,b) & \to & a \cdot b \end{array}$$

(A1)	$(A, +)$ est un groupe abélien
(A2)	$(a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall\, a, b, c \in A$
(A3)	$\exists 1 \in A \quad$ tq $\quad 1 \cdot a = a \cdot 1 = a \quad \forall a \in A$
(A4)	$a \cdot (b+c) = a \cdot b + a \cdot c$ et $(b+c) \cdot a = b \cdot a + c \cdot a \quad \forall\, a, b, c \in A$

Remarque et terminologie : -

1. La loi + est appelée l'addition. Le neutre dans (A,+) est notée $0=0_A$ et l'inverse de a dans (A,+) est noté -a
2. La loi $\cdot$ est appelée la multiplication. On notera suovent $a \cdot b := ab$
   (A2) (A3) signifient que $(A, \cdot)$ est un monoïde
   En particulier, le neutre $1=1_A$ est unique (voir Chap I)
3. L'axiome (A') est un axiome de distibutivité
   Formellement, on aurait du l'écrire : $\quad a \cdot (b+c) = (a \cdot b) + (a \cdot c) \quad (\neq a \cdot (b+a) \cdot c)$
4. on a les regle de calcul suivante, $\quad \forall a, b \in A$:

(i) $a \cdot 0 = 0 \cdot a = 0$

(ii) $a(-b) = (-a)b = -(ab)$

(iii) $(-a)(-b) = ab$

(iv) $(-A)a = -a$

(v) $(-1)(-1) = 1$

En effet : -

i) $a \cdot 0 \overset{A1}{=} a(0+0) \overset{A4}{=} a \cdot 0 + a \cdot 0$

$\Rightarrow 0 = a \cdot 0 = -(a0) = a0 + a0 - a0 = a0$

ii) $ab + a(-b) \overset{A4}{=} a(b-b) = a \cdot 0 \overset{i}{=} 0$

$\Leftrightarrow$ a(−b) est l'inverse additif. de ab $\Leftrightarrow a(-b) = -(ab)$

(ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (v) : facile

5. On a bien sur $a+b = a+c \Rightarrow b = c$ car(A,+) est un groupe
   En revanche , $a \cdot b = a \cdot c \not\Rightarrow b = c$!!
6. L'ensemble A= $\{0\}$ est un anneau (trivialement) appelé l'anneau nul noté $A = 0$
   NotonsqueA $= 0 \Leftrightarrow 0 = 1$
   $\Rightarrow$ (trivial) $\Leftarrow$ Si 0=1 alors $\forall a \in A$, on a : $a = a \cdot 1 = a \cdot 0$, d'ou A=$\{0\}$
7. Pour a$\in$ A et n$\in \mathbb{Z}$ on note : $na := \begin{cases} \underbrace{a + ... + a}_{n} & \text{si } n > 0 \\ 0 & \text{si } n = 0 \\ (-a) + ... + (-a) & \text{si } n < 0 \end{cases}$

Par les ex 2,3 Serie 1 on a : (n+m)a=na+na

$(nm)\cdot a = n(ma) \quad \forall a, b \in A$

$n(a+b)=na+nb \quad \forall n, m \in \mathbb{Z}$

Mais on a de plus n(ab)=(na)b=a(nb)

En efet pour $n > 0$: $n(ab) = \underbrace{ab + ... + ab}_{n} = \underbrace{a + ... + a)}_{n}b = (na) \cdot b$

n(ab) =ab+...+ab = a(b+...+b)=a(nb)

Exemple d'anneaux : -

1. $(\mathbb{Z}, +, \cdot)$ est un anneaux commutatif
   De meme $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des anneaux commutatif
2. Si K=$\mathbb{R}$ou$\mathbb{C}$ et n ≥ 1 alors A$M_n(K)$ est un anneau pour l'addition et la multiplication matricielle
   (Cela decoule des resultat de l'algebre lineaire)
   Pour n=1, on a $M_n(K)$ commutatif Mais $M_n(K)$ n'est pas commutatif des que $n > 1$
3. A={f : $\mathbb{R} \to \mathbb{R}$|f differentiable } est un anneau commutatif
   (f,g diff $\Rightarrow$ -f,f+g,f·g diff -f(x) = 0 $\forall$x et g(x)=1 $\forall$x sont diff)
   De meme pour {f : $\mathbb{R} \to \mathbb{R}$|f continue)
4. Soit (G,+) un groupe abélien. Alors l'ensemble des endomorphisme de G :
   $$\mathrm{End(G)} := \{\varphi : \mathrm{G} \to \mathrm{G} | \varphi \ \textit{endomorphisme}\}$$
   est un anneau pour $(\varphi + \psi)(g) := \varphi(g) + \psi(g)$ et $(\varphi \cdot \psi)(g) := \varphi(\psi(g)) \quad \forall g \in G$
5. Pour tout n$\geq$ 1 $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], ..., [n-1]\}$ est un anneau pour :
   $$[a] + [b] := [a+b] \quad \text{et} \quad [a] \cdot [b] := [ab]$$

ou [ ] designe la classe d'équivalenc emodulo $n\mathbb{Z}$ $(a \sim b \Leftrightarrow a - b \in n\mathbb{Z})$

Preuve : -

- $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abéloine ; découle de la theorie general vue au chap I
- Verifions que la mutliplication est bien definie :
  $$[a] = [a'], [b] = [b'] \Rightarrow [ab] = [a'b']$$

En effet : -

[a]=[a'] $\Leftrightarrow$ a'-a $\in n\mathbb{Z} \Leftrightarrow \exists k \in \mathbb{Z}$ tq a'-a =kn
$[b] = [b'] \Leftrightarrow$ b'-b $\in n\mathbb{Z} \Leftrightarrow \exists l \in \mathbb{Z}$ tq b'-b =ln

Calclons a'b' -ab =(a+kn)(b+ln)-ab

On a donc a'b' -ab $\in n\mathbb{Z}$ = ab +aln + knb + kln^2 -ab = $n\underbrace{al + bk + kln)}_{\in\mathbb{Z}}$ et donc [ab]=[a'b']

Le reste est automatiquement hérité de $\mathbb{Z}$ par exemple :

(A4) $[a] \cdot ([b] + [c]) = [a] \cdot [b + c] = [a(b + c)] + [ab + ac] = [ab] + [ac] = [a][b] + [a][b]$

Par exemple on a la table de multiplication suivante dans $\mathbb{Z}/n\mathbb{Z}$:

·	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

6. Si A_1, A_2 sont deux anneaux alors $A_1 \times A_2$ est un anneau pour
   $(a_1, a_2) + (b_1 b_2) := (a_1 + b_1, a_2 + b_2)$ $\forall a_1 b_1 \in A \ a_2 b_2 \in A_2$
   $(a_1, a_2) \cdot (b_1 b_2) := (a_1 b_1, a_2 b_2)$

Terminologie : - Soit A un anneau

— B est un sous-anneau de A si $1_A \in B$, et $a, b \in B \Rightarrow$ a+b,-a,a·b $\in$ B
— a $\neq 0 \in$ A est un diviseur s'il existe b$\neq 0 \in$ A tq ab=0 ou ba = 0
— A est integre si A est commutatif A $\neq 0$ est sans diviseur de 0 (ie : ab=0 $\Rightarrow$ a=0 ou b=0)

On note $A^* := \{a \in A | \exists b \in A \text{ avec } ab=ba = 1\}$ l'ensemble des unité de A

Notons que $(A^*,\cdot)$ est un groupe
De plus si $A \neq 0$ alors $0 \notin A^*$ $(0 \cdot b = b \cdot = 0 \neq 1)$
Aisin on a $A^* \subset A - \{0\}$

Définition : -

$$\boxed{\text{Un anneau } K \neq 0 \text{ commutatif est un corp si } K^* = K \setminus \{0\}}$$

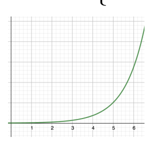
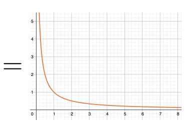
Ainsi un corp est un anneau commutatif non-nul tq : $\forall a \neq 0 \in K,\ \exists b \in K \text{ tq } ab = 1_A$

Remarque : - Un corp K est un anneau integre

Si : $ab = 0$ avec $a \neq 0$ $\exists a^{-1} \in K$ tq $aa^{-1} = 1 \Rightarrow 0 = a^{-1} \cdot 0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b$

On a donc : $b = 0$ et donc pas de diviseur de zero dans K

Exemple : -

1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ est une suite de sous-anneaux tous integre
   $(ab = 0 \Rightarrow a = 0 \text{ ou } b = 0)$
   $\mathbb{Z}^* = \{-1, 1\}$
   $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$
2. Soit $K = \mathbb{R}$ ou $\mathbb{C}$ $\quad n \geq 1$ et $A = M_n(K)$ $\qquad$ Si $n = 1$ $\quad M_1(K) = K$ est un corp
   Si $n \geq 2$ $M_n(K)$ possede des diviseur de 0 $\left[a \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, ab = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right]$
   $\Rightarrow$ pas integre $\Rightarrow$ pas un corp)
   $M_n(K)^* = \{M \in M_n(K) | \exists N \in M_n(K) \text{ avec } MN = NM = I\} = GL(n, K)$
3. $\{f, \mathbb{R} \to \mathbb{R} | f \text{ derivable}\}$ est un sous-aneaux de $\{f : \mathbb{R} \to \mathbb{R} |\ f \text{ continue}\}$
   Ces anneaux ne sont pas integre : f =  g = 
   $f \neq 0, g \neq 0$ mais $f \cdot g = 0$ $\qquad \begin{cases} (f+g)(x) := f(x) + g(x) \\ (f \cdot g)(x) := f(x) \cdot g(x) \end{cases}$
   $\{f | f \text{ continue}\} = \{f | f \text{ continue}, \ , f(x) \neq 0\ \forall x \in \mathbb{R}\}$ $\qquad$ (f cont $f(x) \neq 0\ \forall x \Rightarrow \frac{1}{f}$ est continue)
4. $(G, +)$ gr − ablien $A = End(G)$ $\quad$ En général End(G)adesdiviseurde0
   $A^* = End(G)^* = Aut(G)$
   ∗Remarque : Au 1.3 on avait calculé $Aut(\mathbb{Z}) = \{-1, 1\}$ En fait on avait commencer par montrer que $End(\mathbb{Z}) \cong \mathbb{Z}$ d'ou la conclusion : $Aut(\mathbb{Z}) = End(\mathbb{Z})^* \cong \mathbb{Z}^* = \{-1, 1\}$
5. Conclusion $n \geq 1$ et $A = \mathbb{Z}/n\mathbb{Z}$
   ∗Affirmation : $\mathbb{Z} : n\mathbb{Z}$ integre $\Leftrightarrow$ n est premier

Preuve : -

$\Rightarrow$: Par la contraposé supposons n non-premier

Donc il existe $1 < r, s < n$ tq $r \cdot s = n$
On a donc $a := [r] \neq 0 \in \mathbb{Z}/n\mathbb{Z}, b := [s] \neq 0 \in \mathbb{Z}/n\mathbb{Z}$
Mais $a \cdot b = [r] \cdot [s] = [rs] = [n] = [0] = 0 \in \mathbb{Z}/n\mathbb{Z}$ Ainsi $\mathbb{Z}/n\mathbb{Z}$ n'est pas integre

$\Leftarrow$: Peut se demontrer directement mais découle aussi de l'affirmation suivante
$*$**Affirmation** $(\mathbb{Z}/\mathbf{n}\mathbb{Z})^* = \{[m] \in \mathbb{Z}/n\mathbb{Z} | \mathrm{pgcd}(m, n) = 1\}$

$*$Consequence Si n est premier, alors but m=1,2,...n-1 est premier a n
et donc $(\mathbb{Z}/n\mathbb{Z})^* = \mathbb{Z}/n\mathbb{Z}\backslash\{0\}$ et donc est un corp ($\Rightarrow$ integre)

Preuve de l'affirmation :

$(\mathbb{Z}/n\mathbb{Z})^* \overset{\text{def}}{=} \{[m] \in \mathbb{Z}/n\mathbb{Z} | \exists [l] \in \mathbb{Z}/n\mathbb{Z} \text{ tq } [m][l] = [1] \in \mathbb{Z}/n\mathbb{Z}\}$
$\exists [l] \in \mathbb{Z}/n\mathbb{Z}$ tq $[m][l] = [1] \in \mathbb{Z}/n\mathbb{Z} \Leftrightarrow \exists l, k \in \mathbb{Z}$ tq $ml + kn = 1$
$\Leftrightarrow \mathrm{pgcd}(m, n) = 1$ par bezout

En resumer : - Sont equivalent :

(i) $\mathbb{Z}/n\mathbb{Z}$ est integre (i) $\Rightarrow$ (iii) : Aff
(ii) $\mathbb{Z}/n\mathbb{Z}$ est un corp (ii) $\Rightarrow$ (ii) : consequence de Aff
(iii) n est premier (ii) $\Rightarrow$ (i) : toujours vrai

Remarque : - A fini alors A integre $\Rightarrow$ A corps

Faux si A est mutli p.ex A=$\mathbb{Z}$ integre pas un corp

Notation : - si n=p premier on notera $F_p := \mathbb{Z}/p\mathbb{Z}$ le corp de entier modulo p

Exemple : - $F_2 = \{[0], [1]\}$ est un corp a 2 element

6. Si A_1, A_2 sont 2 anneaux non-nul alors $A_1 \times A_2$ n'est pas integre
$(a = (1, 0), b = (0, 1)$ $a \cdot b = (0, 0) = 0_{A \times A}, a \neq 0, b \neq 0$ car $A_1 \neq 0, A_2 \neq 0)$

Finalement $(A_1 \times A_2)^* = {A_1}^* \times {A_2}^*$

Une aplication : Le theoreme de Wiston pour $n \geq 2$ condition $(n-1)!$ modulo n

n	2	3	4	5	6	7	8	9	10	11
(n-1)!	1	2	6	24	120	720	5040	.	.	.
(n-1)! mod n	1	2	2	4	0	6	0	0	0	10

Theoreme de Wilson :

$\boxed{\text{Un entier } n \geq 2 \text{ est premier si et seulement si } (n-1)! \equiv -1 \pmod n}$

Preuve : -

$\Leftarrow$: Soit donc n$\geq$ 2 avec $(n-1)! \equiv -1 \pmod n$ et soit $1 \leq d < n$ tq $d|n$

Avoir : $d = 1$ ($\Rightarrow$ n premier)

On a $(n-1)! \equiv -1 (\mathrm{mod}\ n) \Leftrightarrow \left.\begin{matrix} n|(n-1)!+1 \\ d|n \end{matrix}\right\} \Rightarrow \boxed{d|(n-1)!+1} (*)$

$d \leq n-1 \Rightarrow \boxed{d|(n-1)!} (**)$

$(*)\&(**) \Rightarrow d|((n-1)!+1)-(n-1)!$ ie : $d|1$ et donc $d = 1$

En fait si n> 4 est non premier alors (n-1) ! $\equiv$ 0 (mod n))

$\Rightarrow$: Supposons n=p premier. Si p = 2 ça marche. On peut supposer donc p> 2

On veut le produit de tous les elements de $(\mathbb{Z}/n\mathbb{Z})^*$ (puisque $(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}\backslash\{0\}$)

Dans ce produit chaque a possede un inverse a^{-1} tq $a \cdot a^{-1} = 1$

On obtient : $[(p-1)^{-1}] = \prod_{a \in (\mathbb{Z}/p\mathbb{Z})*} a \overset{aa^{-1}=1}{=} \prod_{\substack{a \in (\mathbb{Z}/p\mathbb{Z})* \\ \text{tq } a=a^{-1}}} a$

Mais dans $\mathbb{Z}/p\mathbb{Z}$, on a $a = a^{-1} \Leftrightarrow a^2 = 1 \Leftrightarrow a^2 - 1 = 0$

$\Leftrightarrow (a+1)(a-1) = 0 \underset{\mathbb{Z}/p\mathbb{Z}}{\Leftrightarrow} a = 1 = 0$ ou $a - 1 = 0 \Leftrightarrow a = -1$ ou $a = +1$

On a donc : $[(p-1)!] = (+1)(-1) = -1 \in \mathbb{Z}/n\mathbb{Z}$ donc $(p-1)! \equiv -1(\mathrm{mod}\ p)$ $\square$

2.2 Homomorphisme d'anneaux

Définition : -

Une application $\varphi : A \to A'$ entre deux anneaux est un homomorphisme d'anneaux si
$\varphi(a+b) = \varphi(a) + \varphi(b)$ $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ $\forall a, b \in A$
$\varphi(1_A) = 1_{A'}$

Rappel et terminologie : -

1. La premiere condition signifie que $\varphi : (A, +) \to (A', +)$ est un homomorphisme de groupe
   En particulier on aura $\varphi(o_A) = o_{A'}$ et $\varphi(-a) = -\varphi(a)$ $\forall a \in A$
2. Les deux premiere condition n'impliquent pas la 3eme en general
   Par exemple : $\varphi(a) = 0$ $\forall a \in A$ $(A' \neq 0)$
3. Si $\varphi : A \to A'$ est un homomorphisme et si a$\in$ A*alors$\varphi(a) \in (A^*)$
   $(a \in A^* \Leftrightarrow \exists b \in A$ tq $ab = ba = 1_A \Rightarrow 1_{A'} = \varphi(1_A) = \begin{cases} = \varphi(ab) = \varphi(a)\varphi(b) \\ = \varphi(ba) = \varphi(b)\varphi(a) \end{cases}$
   $\Rightarrow \varphi(a) \in (A')^*$ avec inverse $\varphi(b)$
   Ainsi , $\varphi|_{A*} : A^* \to (A')^*$ est un homomorphisme de groupe pour la multiplication
4. $\varphi A \to A'$ $\psi : A' \to A''$ homo $\Rightarrow \psi \circ \varphi : A \to A''$ homo
5. On definit le noyau et l'image de $\varphi : A \to A'$ par
   $\mathrm{Ker}\varphi = \{a \in A|\ \varphi(a) = 0\}$ $\mathrm{Im}\varphi = \{\varphi(a)|a \in A\}$
   Par prop I.2 : -Kerφ est un sous groupe de (A,+) φ inj $\Leftrightarrow \mathrm{Ker}\varphi = 0$
   Imφ est un sous groupe de (A',+) φ surj $\Leftrightarrow \mathrm{Im}\varphi\mathrm{Im}\varphi = A'$

En fait : Imφ est un sous-anneaux de A'

$$A_{A'} = \varphi(1_A) \in \mathrm{Im}\varphi$$
$$\varphi(a), \varphi(b) \in \mathrm{Im}\varphi \Rightarrow \varphi(a)\varphi(b) = \varphi(ab) \in \mathrm{Im}\varphi$$

Par contre : - Kerφ n'est pas un sous-anneaux de A !

Car : $1_A \notin \mathrm{Ker}\varphi$ (puisque $\varphi(1_A) = 1_{A'} \neq 0$ sauf $A' = 0$)

6. Un isomorphisme d'anneaux est un homomorphisme $\varphi : A \to A'$ tq
   Il existe homomorphisme $\psi A' \to A$ $\psi \circ \varphi = \mathrm{Id}_A$ $\varphi \circ \psi = \mathrm{Id}_{A'}$
   C'est équivlent à : φ est un homomrphisme biijectif, comme pour les groupes)

Si $\varphi : A \to A'$ est un sous-anneaux alors $\varphi|_{A*} : A^* \to (A')^*$ est un sous groupe
Toute les remarque sur les iso de groupe se transportent aux iso d'anneaux

Exempe d(homomorphisme (d'anneaux) : -

1. $\mathrm{id}_A : A \to A$ est un homomorphimse
2. Si $B \subset A$ est un sous-anneaux, l'inclusion $\varphi \begin{array}{l} : B \to A \\ b \to \varphi(b) = b \end{array}$ est un homomorphisme
   En particulier on a les homomrphisme $\mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C}$ donné par les inclusion
3. $\varphi : \{f : \mathbb{R} \to \mathbb{R} | f \text{ derivable}\} \to \mathbb{R}, \varphi(f) = f(x_0)$ pour $x_0 \in \mathbb{R}$ fini
   φ est un homomorphisme : $-\varphi(f+g) = (f+g)(x_0) = f(x_0) + g(x_0) = \varphi(f) + \varphi(g)$
   idem pour la mutliplication
   $1_A(x) = 1 \quad \forall x \in \mathbb{R} \Rightarrow \varphi(1_A) = 1_A(x_0) = 1$
   Son noyau : $\mathrm{Ker}\varphi = \{f | f(x_0) = 0\}$
4. $A = Mn(K)$ $P \in GL(n,k)$ fini alors $\varphi A \to A$ $\varphi(M) = PMP^{-1}$ *est un homomorphime*
   On dit que φ est un automorphisme de A
5. $\varphi : \begin{array}{l} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \\ a \to [a] \end{array}$ est un homomrphisme d'anneaux $\begin{pmatrix} \varphi(a+b) = [a+b] = [a] + [b] = \varphi[a]\varphi[b] \\ \varphi(a \cdot b) = [a \cdot b] = [a][b] = \varphi(a) \cdot \varphi(b) \\ \varphi(1) = [1] = 1_{\mathbb{Z}/n\mathbb{Z}} \end{pmatrix}$

Proposition : - Pour tout anneaux A, il existe unique homomorphisme d'anneaux $\varphi\mathbb{Z} \to A$

Preuve : - Soit A un anneaux et $\varphi : \mathbb{Z} \to A$ un homomorhpisme

Pour n$\in \mathbb{Z} > 0$ on a $\varphi(n) = \varphi(\underbrace{1 + ... + 1}_{n}) = \underbrace{\varphi(1) + ...\varphi(1)}_{n} = \underbrace{1_A + ... + 1_A}_{n} := n1_A$

Pour n$\in \mathbb{Z} < 0$ on a $\varphi(n) = \varphi(\underbrace{(-1) + ... + (-1)}_{|n|}) = \underbrace{\varphi(-1) + ... + \varphi(-1)}_{|n|} = \underbrace{(-1_A) + ... + (-1_A)}_{|n|}$

Pour n =0 $\varphi(0) = 0_A = 0 \cdot 1_A$

Ainsi si $\varphi : \mathbb{Z} \to A$ est un homomorphisme on a forcement $\boxed{\varphi(n) = n1_A \quad \forall n \in \mathbb{Z}}$

Verifions encore que cette formule definit bien un homomrhisme d'anneaux cela découle de la remarque 7 apres la définition d'un anneaux : $\forall n, m \in \mathbb{Z}$

$$\varphi(n+m) = (n+m) \cdot 1_A = n \cdot 1_A + m1_A = \varphi(n) + \varphi(m)$$
$$\varphi(n \cdot m) = (n \cdot m)1_A = n(m \cdot 1_A) = n\varphi(m) = n \cdot (1_A\varphi(m)) = (n1_A)\varphi(m) = \varphi(n)\varphi(m)$$
$$\varphi(1) = 1 \cdot 1_A = 1_A \qquad \square$$

Ainsi tout anneau A possede un unique homo $\varphi : \mathbb{Z} \to A$ d'ou un noyau $\mathrm{Ker}\varphi < \mathbb{Z}$ uniquement associé a A, d'ou un entier n$\in \{0, 1, 2, ...\}$ uniquement associé a A !

Terminologie : - Cet entier n est appelé la caractéristique de A, noté car(A) en clair :

* $\ast$ car(A)=0 $\Leftrightarrow$ Ker$\varphi = \{0\}$ $\Leftrightarrow$ $\varphi : \mathbb{Z} \to A$ injectif $\Leftrightarrow$ A contient $\mathbb{Z}$ comme sous-anneaux
  Dans ce cas $\underbrace{1_A + ... + 1_A}_{n} \neq 0 \quad \forall n > 0$
* $\ast$ car(A) $= n > 0 \Leftrightarrow 1_A + ... + 1_A =$ pour n = car(A)
  et c'est le plus petit entier tel que c'est le cas

Exemple : -

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ est caractéristique 0
2. $\mathbb{Z}/n\mathbb{Z}$ a caractériqtique n : $\underbrace{[1] + ... + [1]}_{n} = [0]$

Proposition II.2 : - Si A est un anneau integre, alors car(A) est soit nulle soit un nombre premier

Preuve : - Supposons que n=car(A) > 0 mais pas premier
A voir : A pas integre

Si $n > 0$ n est pas premier alors il existe $1 < r, s < n$ tq $r \cdot s = n$; (en effet ; n non premier $\Rightarrow \exists d$ tq $d|n$ $d \neq 1, d \neq n$ choisir $\begin{array}{l} r = d \\ s = \frac{n}{d} \end{array}$

Calculons : $0 = n \cdot 1_A = (r \cdot s)1_A = (\underbrace{1_A + ... + 1_A}_{rs}) = (\underbrace{1_A + ... + 1_A}_{r}) = \underbrace{(r \cdot 1_A)}_{:=a} \cdot \underbrace{(s \cdot 1_A)}_{:=b}$

On a donc $ab = 0$ mais $a \neq 0$ car $r < n$ et n est le puls petit entier tq $n \cdot 1_A = 0$
et $b \neq 0$ pour la meme raison. Donc A n'est pas integre $\square$

Corollaire II.3 : - Un corps a caractérisituqe nulle ou un premier $\square$

Proposition II.4 : - Si $\varphi : A \to A'$ est un homomorphisme d'anneaux, alors la caractéristique de A' divise celle de A

Preuve : - Soit donc $\varphi : A \to A'$ un homomorphisme d'anneaux, et $\varepsilon : \mathbb{Z} \to A, \varepsilon' : \mathbb{Z} \to A'$ les homomorphisme donné en prop II.1

φ et ε sont des homo $\Rightarrow \varphi \circ \varepsilon : \mathbb{Z} \to A'$ est un homo

$\overset{\text{Prop II.1}}{\Rightarrow} \varphi \circ \varepsilon = \varepsilon'$ par unicité

Si l'on note n := car(A), n' = carA' et obtient :

$$n'\mathbb{Z} = \mathrm{Ker}(\varepsilon') = \mathrm{Ker}(\varphi \circ \varepsilon) \supset \mathrm{Ker}(\varepsilon) = n\mathbb{Z}$$

On a donc $n\mathbb{Z} \subset n'\mathbb{Z} \Leftrightarrow \exists k \in \mathbb{Z}$ tq $n = n' \cdot k \Leftrightarrow n'|n$ $\square$

Conséquence : - $A \cong A' \Rightarrow \mathrm{car}(A) = \mathrm{car}(A')$

2.3 Idéaux et anneaux quotients

Au chap I, on a vu que les sous groupe normaux sont important. Ils coincident avec les noyaux d'homo de groupe
Qu'en est il pour les anneaux ? Etudions les noyaux d'homo d'anneaux

Lemme II.5 : - Si $\varphi A \to A'$ est un homo d'anneaux alors I :=Kerφ satisfait :

(i) I est un sous-groupe de (A,+)

(ii) Si x$\in$ I et a$\in$ A alors ax$\in$ I et xa $\in$ I

Preuve : -
(i) vu, découle du Chap I
(ii) Soit x$\in$ I = Kerφ et a$\in$ A : $\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a)\cdot 0 \Rightarrow ax \in I$
et de meme : $xa \in I$ $\square$

On définit donc :

Définition : -

> Soit A un anneaux. Un sous-ensemble I$\subset$ A est appelé un ideal de A si :
> (i) I est un sous-groupe de (A,+)
> (ii) $\forall x \in I, \forall a \in A, \quad ax \in I$ et $xa \in I$

Exemple d'idéaux : -

1. Tout anneaux A possede les idéaux I=$\{0\}$ et I=A
(Un anneau commutatif non-nul est un corp $\Leftrightarrow$ les seul idéaux sont ceux-la)
2. n$\mathbb{Z}$ est un ideal de $\mathbb{Z}$
3. Dans A commutatif $\forall x \in A$ I :=(x) = $\{xa|a \in A\}$ = xA est idéal de A, appelé l'idéal principal engendré par x

(i) $0 = x\cdot 0 \in I$
$x\cdot a, x\cdot b \in I \Rightarrow xa - xb = x(a-b) \in I$

(ii) $xa \in I, a' \in A \Rightarrow a'(xa) = x(a'a) \in I$
(idem) pour $(xa)\cdot a' = x(aa'), \in I$

Par exemple si A=$\mathbb{Z}$ et x=n (x) = n$\mathbb{Z}$ l'exemple 2
Pour x=0 on a (0) = $\{0\}$; pour x=1_A on a (1) = A (exemple 1)

4. Par le lemme II.5 si $\varphi : A \to A'$ est un homo d'anneaux alors I=kerφ est un idéal de A

Remarque : - Attention !

1. Un idéal n'est pas en général un sous-anneaux
2. Un sous anneaux n'est en général pas un idéal
3. Si φ est un homo Im(φ) n'est pas un ideal

$\Big\}$ $\varphi : \mathbb{Z} \to \mathbb{Q}$ l'inclusion
Im(φ = $\mathbb{Z}$ est un sous anneaux
de $\mathbb{Q}$, mais pas un ideal

$\sim$

Comme un idéal $I \subset A$ est un sous-groupe de (A,+) abélien, on a le groupe quotient $A/I := \{a + I|\ a \in A\} = \{[a]|a \in A\}$ ou $a\sim b \Leftrightarrow a - b \in I$

Par la thèse du Chap I, on sait que A/I est un groupe abélien pour [a]+[b] := [a+b], et $\pi : A \to A/I$, $\pi(a) = [a]$ est un homo de groupe
De plus :

Proposition II.6 : - Si I est un idéal de A alors A/I est un anneaux pour [a]+[b] := [a+b] et [a]$\cdot$[b] = [a $\cdot$ b] De plus, $\pi : A \to A/I$ est un homo d'anneaux

Preuve : - Le fait que A/I est un groupe abélien est deja connu mais on a refaire la preuve que + est bien définie :

$$\begin{matrix}[a]=[a'] \\ [b]=[b']\end{matrix} \Leftrightarrow \begin{matrix}a' - a \in I \\ b' - b \in I\end{matrix} \Rightarrow (a' + b') - (a + b) = \underbrace{(a' - a)}_{\in I} + \underbrace{(b - b')}_{\in I} \in I$$

$\Leftrightarrow [a' + b'] = [a + b] \Rightarrow$ $\boxed{[a]+[b] := [a+b] \text{ est bien définie}}$

on obtient maintenant que (A/I, +) est un groupe abélien et π est un homo de groupe

Par exemple : - [a]+[b] = [a+b] = [b+a] = [b]+[a]

Verifions que la multiplication est bine définie :

$$\begin{matrix} [a] = [a'] \\ [b] = [b'] \end{matrix} \Leftrightarrow$$

Remarque : - Les idéaux de A sont exactement les noyaux d'homo d'anneaux A→ A′

Exemple d'anneaux quotient : -

1. $I = \{0\} \subset A \Rightarrow A/I = A/\{0\} = A$
2. I=A $\Rightarrow A/I = A/A = 0$ l'anneau trivial ([a]=[b]$\Leftrightarrow$ $a - b \in A$ toujours vrai)
3. I=n$\mathbb{Z} \subset \mathbb{Z} = A \Rightarrow A/I = \mathbb{Z}/n\mathbb{Z}$ l'anneau des entiers modulo n
4. Plus généralement : si A est commutatif, $x \in A$ I=(x), on obtient l'anneau commutatif A/(x) ou [a]=[b] $\Leftrightarrow$ a=b $\in$ xA

Proposition II.7 : - Soit $\varphi : A \to A'$ un homo d'anneaux I$\subset$ A un idéal

$$\begin{matrix} A & \xrightarrow{\varphi} & A' \\ \downarrow \pi & \nearrow & \\ A/I & & \end{matrix}$$

Tq Ker$\varphi \subset$ I Alors il existe un unique homo d'anneaux
$\overline{\varphi}A/I \to A'$ tq $\overline{\varphi}([a]) = \varphi(a) \quad \forall a \in A$

Preuve : - Par Prop I.8 il existe un unique homo-de-groupe
$\overline{\varphi} : A/I \to A'$ tq $\overline{\varphi}([a]) = \varphi(a)(\Leftrightarrow \overline{\varphi} \circ \pi = \varphi)$
Reste a vérifier que $\overline{\varphi}$ est un homo d'anneaux : $\overline{\varphi}([a] \cdot [b]) = \overline{\varphi}([ab]) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}([a])\overline{\varphi}([b])$

$\overline{\varphi}(1_A/2) = \overline{\varphi}([1_A]) = \varphi(1_A) = 1_{A'}$ □

Proposition II.8 : - Toute homo d'anneaux $\varphi : A \to A'$ définit un isomorphisme d'anneaux

$\boxed{\overline{\varphi} : A/\text{Ker}\varphi \to \text{Im}\varphi}$

Preuve : - Par Prop I.9, on sait que φ definit $\overline{\varphi}$ iso de groupe par Prop II.7, $\overline{\varphi}$ est un homo d'anneaux

$\Rightarrow \overline{\varphi}$ homo d'anneaux bijectif $\Leftrightarrow \overline{\varphi}$ iso d'anneaux □

Exemple : - Soit A un anneaux quelquoncque et $\varphi : \mathbb{Z} \to A$ l'homo donné en prop II.1

* car(A)=0 alors Ker$\varphi = 0 \Rightarrow \varphi$injectif $\Rightarrow\Rightarrow \varphi : \mathbb{Z} \to \varphi(\mathbb{Z})$ est un iso d'anneux
  $\Rightarrow$ A contient un sous-anneaux isomorphe a $\mathbb{Z}$ (le sous-anneaux $\varphi(\mathbb{Z})$)
* si car(A)=n> 0 alors Ker$\varphi = n\mathbb{Z}$ Par la prop II.8 on a un iso d'anneaux $\overline{\varphi} : \mathbb{Z}/n\mathbb{Z} \to \varphi(\mathbb{Z}) = A$
  $\Rightarrow$ A continent un sous-anneaux isomorphe a $\mathbb{Z}/n\mathbb{Z}$

2.4 Corps des fraction d'un anneaux integre

L'anneaux integre A=$\mathbb{Z}$ n'est pas un corp. Mais, il existe un corps K=$\mathbb{Q}$ et un hom d'anneaux injectif $\mathbb{Z} \to \mathbb{Q}$ (l'inclusion) : on parle de plongement : A→ K

Notons qu'il existe un plogement de A dans un corps K, alors A est integre

Et en fait c'est possible des que A est integre

Théoreme II.9 : -

$$\boxed{\text{Tout anneaux integre se plonge dans un corps}}$$

Réléchissons a la construction de $\mathbb{Q}$ a partir de $\mathbb{Z}$ (vu en logique) et tenton de l'étendre :

$$\mathbb{Q} := \mathbb{Z} \times (\mathbb{Z} - \{0\})/\sim \text{ ou } (a,b) \sim (c,d) \Leftrightarrow ad = bc$$

penser a ab comme $\frac{a}{b}$ ($\dfrac{a}{b} = \dfrac{c}{d} \Leftrightarrow ad = bc$) Notons [a,b] la classe de (a,b) (penser a $\frac{a}{b}$)

On définit les opération : [a,b]+[c,d]=[ad+bc,bd]
[a,b]· [c,d] = [ac,bd]
On verifie que c'est bien définie et que cela donne un corp

Preuve du Theoreme : - Soit A un anneau integre. Posons X :=A×(A − {0}) et :

$$\boxed{(a,b) \sim (c,d) \in X \Leftrightarrow ad = bc \in A}$$

C'est un realtion d'équivalence : (a,b) $\sim (a,b) \Leftrightarrow ab = ba \in A$: Ok car A commutatif
(a,b) $\sim$ (c,d) $\Leftrightarrow$ ad=bc équation equi-
(c,d) $\sim$ (a,b) $\Leftrightarrow$ cb=da
valanet dans A commutatif

$$\left.\begin{array}{l} (a,b) \sim (c,d) \Leftrightarrow ad = bc \\ (c,d) \sim (e,f) \Leftrightarrow (cf = de \end{array}\right\} \Rightarrow b(de) = b(cf) = (bc)f = (ad)f$$

$\Leftrightarrow d(be) = d(af) \Rightarrow be = af \Leftrightarrow (a,b) \sim (e,f)$

C'est bien une relation d'equivalence :
Posons Q(A) := X/$\sim$ =$\{[a,b] | W \in X\}$

Theoreme II.9 (precicsion) : - Pour tout anneaux integre A, il existe un corp Q(A) et un homomorphisme d'anneaux injectif

(-plongement) i: A $\rightarrow$ Q(A)

- L'addition dans Q(A) est définie par $\boxed{[a,b]+[c,d] := [ad+bc,\ bd]}$
  C'est bien définie :–$b \neq 0, d \neq 0 \Rightarrow bd \neq 0$ car A est integre

$$\left.\begin{array}{l} [a',b'] = [a,b] \Leftrightarrow a'b = b'a \\ [c',d'] = [c,d] \Leftrightarrow c'd = d'c \end{array}\right\} [a'd' + b'c', b'd'] = [ad + bc, bd]$$

$\Leftrightarrow' a'd' + b'c')bd = b'd'(ad + bc)$

a'd' bd + b'c'bd = (a'b)dd' + (c'd)bb' = (b'a)dd' + (d'c)bb' = b'dad + b'd'bc donc ça marche

(Q(A),+) est un groupe abélien : associativité
— le neutre est 0=[0,1] (=[a,b], $b \neq 0$) : [0,1] + [a+b] + [ab+1a,1b]=[a,b]
— L'indice additif de [a,b] est [-a,b] : [a,b]+[-a,b] = [ab+b(-a),b^2]=[0,b^2]=[0,1]
a,b +[c,d] = [c,d]+[a,b] : par définition

- La multiplication dans Q(A) est définie par $\boxed{[a,b]\cdot[c,d] = [ac,bd]}$

  C'est bien définie : $b\neq 0, d \neq 0 \Rightarrow bd \neq 0$ car A integre

$$\left.\begin{array}{l} [a',b']=[a,b] \Leftrightarrow a'b = b'a \\ [c',d']=[c,d] \Leftrightarrow c'd = d'c \end{array}\right\} \Rightarrow [a'c',b'd']=[ac,bd]$$

$\Leftrightarrow a'c'bd = b'd'ac$

En effet : a'c'bd = (a'b)(c'd) = (b'a)(d'c)=b'd'ac ça marche

Q(A),+,·) est un anneaux (A1) vu :

(A2) découle de (A2) par l'anneau A

(A3) L'unité est $1_{Q(A)} := [1_A, 1_A]$(=[b,b],b±) :[a,b]·[1,1]=[a1,b1]=[a,b]

(A4) découle de (A4) pour A

Commutatif : car A est commutatif

Preuve : - soient a,b ∈ A tq i(a)=i(b)

ie : [a,1] = [b,1] ⇔ a,1,=1,b ⇔ a=b □

c'est un corps : Si [a,b]≠∈ Q(A), cela signifie [a,b]≠ $[0, 1]$

2.5 Anneaux euclidiens

Définition : -

> Un anneau integre A est un anneau euclidien s'il existe une application f :A$\backslash\{0\} \to \{1, 2, 3\}$ tq :
> 1. f(a) ≤ f(ab) $\forall a, b \in A\backslash\{0\}$
> 2. Pour tout a,b ∈ A$\backslash\{0\}$ il existe q,r ∈ A tq a=qb+r avec r=0 ou f(r)< f(b)

Remarque : - Voir ex 6,S8 le point 2 est crucial

Exemple : -

1. A=$\mathbb{Z}$ avec f :$\mathbb{Z}\backslash\{0\} \to \{1, 2, 3\}, f(n) = |n|$
   C'est l'algo de division euclidienne !
2. Si A est un corps, c'est un anneaux euclidien (pour f≡ 1)
   $\forall a, b \in A\backslash\{0\}$ on pose q=ab^{-1} et r=0
3. D'autre exemple plus tard

En prop I.10 on avait utilisé la division euclidienne (dans $\mathbb{Z}$) pour montrer tout sous-groupe de $\mathbb{Z}$ est de la forme n$\mathbb{Z}$ Voici la généralisation (meme preuve)

Proposition II.10 - Soit I un idéal dans un anneaux euclidien A, Alors il existe x∈ A tq I=(x) := $\{xa|a \in A\}$

Preuve : - Soit donc I⊂ A un idéal Si I=$\{0\}$ on choisit x=0, ok

On suppose donc : I ≠ $\{0\}$

Choisissons x∈ I$\backslash\{0\}$ qui minimise f sur I$\backslash\{0\}$ ($\forall y \in I\backslash\{0\} f(x) \leq f(y)$)

Affirmation I=(x)

En effet : [⊃] : x∈ I ⇒ xa ∈ I ∀a ∈ A ⇒ (x) ⊂ I

[⊂] : Soit donc y ∈ I y≠ , Par l'axiome 2 d'un anneau euclidien

$$x \in I, q \in A \Rightarrow \left.\begin{matrix} qx \in I \\ y \in I \end{matrix}\right\} \Rightarrow r = y - qx \in I \Rightarrow r = 0, \text{ car } f(r) < f(x) \text{ est impossible par minimalité}$$

Ainsi r=0 ⇒ y = qx, et donc y∈ (x)

Remarque : - Un anneaux integre tq tout idéal de la forme (x) est un anneau principale

Ainsi cette proposition dit : A euclidien $\Rightarrow$ A principale

(On verra un anneau non-principale en fin du Chap II)

On va généraliser et étudier les notions suivantes :

(A) divisibilité
(B) pgcd
(C) éléments premier

(A) Terminologie : Soient a,b avec A commutatif On dit que a divise b noté $a|b$ s'il existe $c \in A$ tq$b=ac$

Dans le cas contraire, on note $a \nmid b$

Exemple : -

1. Dans $A=\mathbb{Z}$ on a :$2 \nmid 3$ car il n'existe pas $n\in \mathbb{Z}$ tq $3=2n$
   mais dans $A=\mathbb{Q}$ on a $2|3$
2. Si $A = K$ est un corps, alors tout $a \neq$ divise tout b ! on pose $c=a^{-1}b$

Remarque : -

1. $a|b$, $b|c \Rightarrow a|c$
2. $a|b$, $a|c \Rightarrow a|(b+c)$
3. $a|b \Rightarrow a|bx \quad \forall x \in A$
4. $a|b$, $u\in A^* \Rightarrow au|b$
5. $a|b \Leftrightarrow (b)\subset (a)$

Proposition II.11 : - Pour $a,b \in A$ avec A integre les énoncé suivant sont équivalents :

(i) $a|b$ et $b|a$
(ii) $(a)=(b)$
(iii) $\exists u \in A^*$ tq $b=ax$

Preuve : - (i) $\Leftrightarrow$ (ii) par la remarque 5 ci dessus

(iii) $\Rightarrow$ (i) supposons $b=a\cdot u$ avec $u\in A^*$ Alors $a|b$ par définition et $a=b\cdot u^{-1} \Rightarrow b|a$

(i)$\Rightarrow$ (iii) supposons $a|b$ et $b|a$ donc $\exists$ $c,d \in A$ tq $b=ac$ et $a=bd$

$\Rightarrow a = bd = (ac)d \Rightarrow 0 = a - acd = a(1-cd)$

A integre $\Rightarrow$ soit $a=0$ et alors $b=0$ et (iii) est infinie

Soit $1\text{-}cd =0$, et alors $cd=1$ d'ou $c,d\in A^*$
d'ou $b=ac$ avec $c\in A^*$ et (ii) est vérifier $\square$

Exemple : -

1. Dans $A=\mathbb{Z}$ m,n sont associé $\Leftrightarrow m=\pm n$
2. Dans A=K corps

(B) Terminologie : - Si on a deux éléments $a,b \in A$ anneaux commutatif, alors un plus grand commun diviseur de a et b, noté pgcd de (a,b) est un élément $d\in A$ tq

— $d|a$ et $d|b$
— Si $c\in A$ est tq $c|a$ et $c|b$ alors $c|d$

Remarque : -

1. Si d est un pgcd de a et b, alors du aussi $\forall u \in A^*$

⌜ - $d|a, d|b$ u$\in A^* \Rightarrow du|a, du|b$

- si $c \in A$ tq $c|a, c|b \Rightarrow c|d \Rightarrow c|du$ ⌟

2. Réciproquement si A est intègre alors deux pgcd d et d' de a et b sont forcément associés ($\exists u \in A^*$ tq $d' = d \cdot u$)

⌜

$$\left.\begin{array}{l} d|a, d|b \Rightarrow d|d' \\ d'|a, d'|b \Rightarrow d'|d \end{array}\right\} \Rightarrow \text{d et d' sont associé}$$

⌞

Exemple : - Dans $\mathbb{Z}$ 2 pgcd de a,b $\in \mathbb{Z}$ fixé sont égaux a multiplication par élément de $\mathbb{Z}^*=\{-1,1\}$ près au signe pres!

Dans ce cas il est naturel de définit le pgcd comme celui qui est ≥ 0

Mais cela ne fait pas de sens sur A quelqconque d'ou "un" pgcd

Qu'en est-il de l'éxistence d'un pgcd?
Dans un anneaux euclidien on a la généralisation suivante de I.12 (Bézout) :

Proposition II.12 - Soit A un anneau euclidien et a,b $\in$ A fixé

Alors il existe pgcd d$\in$ A de a et b

De plus il existe $\lambda, \mu \in A$ tq d=$\lambda a + \mu b$

Preuve : - Soient donc a,b $\in$ A fixé Considérons :

$$I := \{ra + s \cdot b | r, s \in A\} \subset A$$

C'est un idéal de A :

- $0 = 0 \cdot a + a \cdot b \in I$ d'ou I$\neq \emptyset$
- $\begin{array}{l} ra+sb \in I \\ r'a+s'b \in I \end{array} \Rightarrow (ra + sb) - (r'a + sb) = (\underbrace{r - r}_{\in A})a + (\underbrace{s - s'}_{\in A})b \in I$

Ainsi I< (A, +))

- si ra+sb $\in$ I et x$\in$ A alors $x \cdot (ra + sb) = (\underbrace{xr}_{\in A})a + (\underbrace{xs}_{\in A})b \in I$

C'est donc bien un idéal de A. comme A est euclidien par Prop II.10 il existe d$\in$ A tq I=(d)=$\{xd|x \in A\}$
Je prétend que d est un pgdc de a et b

$$\left.\begin{array}{l} - \begin{array}{ll} a=1\cdot a + 0 \cdot b & \in I = (d) \Rightarrow d|a \\ b=0 \cdot a + 1 \cdot b & \in I = (d) \Rightarrow d|b \end{array} \\ \text{- soit } c \in A \text{ tq } c|a \text{ et } c|b \Rightarrow c|(ra + sb)\ \forall r, s \in A \Rightarrow c|x\ \forall x \in I \Rightarrow c|d \end{array}\right\} \text{d est un pgcd de a et b}$$

Finalement $d \in (d) = I = \{ra + sb|r, s \in A\} \Rightarrow \exists\ \lambda, \mu \in A$ tq d=$\lambda a + \mu b$ □

(C) Terminologie : - Soit A un anneaux integre et p$\in$ A $p \neq 0$, $p \notin A^*$

- p est irréductible dans A si p=$a \cdot b$ avec a,b$\in$ A $\Rightarrow a \in A^*$ ou b$\in A^*$
- p est premier dans A si p|ab avec a,b $\in$ A $\Rightarrow$ p|a ou p|b

Exemples : -

1. Dans $\mathbb{Z}$ p$\in \mathbb{Z}$ -$\{-1,0,1\}$ est premier $\Leftrightarrow$ p est irresuctible $\Leftrightarrow$ Les diviseur de p sont ± 1 et $\pm p$
   Ainsi ces notions sont des générateurs naturelles de la notion de "nb premier" dans $\mathbb{Z}$
2. Dans un corps, comme $A^* \cup \{0\}$ = A on a aucun éléments premier / irreductible

Proposition II.13 : - si p$\in$ A est premier, alors p est inrréductible
Réciproquement si A est euclidien, alors p irréductible $\Rightarrow$ p premier

Remarque : - Voir ex7 série 9

Preuve : - Soit donc p$\in$ A p$\neq$ 0 p$\notin$ A avec p premier :
Soient a,b $\in$ tq p=ab A voir :a$\in$ A* ou b$\in$ A*
On a $p|p = ab \Rightarrow$ p|a ou p|b suppososn srlg que p|a : donc $\exists c \in$ A tq a= pc
$\Rightarrow a = pc = (ab)c = a(bc) \Rightarrow 1 + bc \Rightarrow b \in A^*$

Cela montrer que p est irréductible

Réciproquement supposons p$\in$ A irréductible, avec euclidien
Soient a,b $\in$ A tq p|ab $\in$ A tq p|ab
A voir : p|a ou p|b

Supposons srlg $p\nmid$ a. Alors tout pgcd de a et p est une unité

Soit donc d$\in$ A tq d|a et d|p Donc $\exists c \in$ A tq p=dc $\Rightarrow$ c$\in$ A* ou d$\in$ A*
Si c$\in$ A* alors d=pc^{-1} donc p|d $\underset{d|a}{\Rightarrow}$ p|a une contrdiction

On a donc bien d$\in$ A*

Comme A abélien par Prop II.12 $\exists \lambda, \mu \in A$ tq $\lambda a + \mu p = 1$
Ecrivons b=1b $= (\lambda a + \mu p) \cdot b = \lambda ab + \mu pb$

$$p|ab \Rightarrow \left.\begin{matrix} p|\lambda ab \\ p|\mu pb \end{matrix}\right\} \Rightarrow p|(\lambda ab + \mu pb) = b \text{ d'ou } p|b \qquad \square$$

<u>But :</u>- La généralistion du Theoreme fondamental de l'arithmétique aux anneaux-euclidiens

Lemme II.14 : - Dans un anneaux euclidien la fonction f :A-$\{0\} \Rightarrow \{1, 2, ...\}$ satisfait
f(a,b)> f(a) $\quad \forall a, b \in A - \{0\}$ et b$\notin$ A*

Preuve : - Par le premier condition dans la def d'un anneau euclidien on a f(a)$\leq$ f(ax) $\quad \forall a, x \neq 0$
Fixons a$\neq$ 0 $\in$ A On a donc si l'on pose I :=(a) , f(a) = min$\{f(ax)|x \in A - \{0\}\}$
i.e : $\boxed{f(a) = \min\{f(y)|y \in I, y \neq 0}$
Comme ab $\in$ I on a f(a)$\leq$ f(ab) Supposons par l'absurde que f(a)=f(ab)

Donc on a : f(ab)=f(a) = min $\{f(y)|\ y \in I - \{0\}\}$
Par l'arguement dans la preuve de la proposition II.10 : I=(ab)
On a donc (a)=(ab) $\Rightarrow \exists x \in A$ tq $a = abx \Rightarrow bx = 1$
$\Rightarrow b \in A^*$ une contradiction

Théoreme II.15 : -

> Soit A un anneaux euclidien, et soit a$\in$ A , a$\neq$ 0 et a $\notin$ A*. Il existe des éléments irréductibles $p_1, ..., p_n \in A$ tq a=$p_i ... p_n$. De plus si a=$p_1, ..., p_n = q_i ... q_n$ avec p_i, p_j irréductible, alors m=n et pour tout i=1,...,n p_i est arrivé a $q_{\sigma(i)}$ par une permutation

Exemple : - A=$\mathbb{Z}$ On obtient :
tout n> 1 est produit de nombre premier produit unique a l'ordre des facteurs pres

Preuve : - Soit donc a$\in$ A a$\neq 0$ a$\in$ A* A euclidien

- L'éxistence d'une décoposition découle immédiatement de :

  Affirmation Tout a$\in A - \{0\}$ est soit une unité soit le produit d'un nombre fini d'élément irréductible dans A

  En effet : on démontrer l'affirmation par récurrence sur f(a)$\in \{1, 2, ...\}$
  - supposons f(a)=1. Alors a$\in$ A* en effet si a$\notin$ A* alors par Lemme II.14
  f(a)=f($1 \cdot$ a) $\underset{\text{II.14}}{<}$ f(1) $\geq 1 \Rightarrow$ f(a) > 1 On a donc a$\in$ A* $\Rightarrow$ f(a) > 1
  ce qui est équivalent à f(a)=1 $\Rightarrow$ a $\in$ A*
  - supposons l'affirmation vraie pour tout a$\in A - \{0\}$ tq f(a')< f(a)
  Si a est une unité ou a un élément irréductible, on a fini !
  On peut donc supposer a$\notin$ A* a non-irréductible
  Ainsi il existe b,c $\in A - \{0\}$ tq a=bc et b$\notin$ A*,c$\notin$ A*
  Par Lemme II.14 on a f(b)<f(a), f(c)<f(a); Par Hypothese de récurence b et c sont produit d'irréductible
  Ainsi a=bc est aussi produit d'irréductible

- Pour l'unicité supposons a=$p_1, ..., p_n$ =$q_1, ..., q_n$ avec p_i et q_j sont irréductible et donc premier
  Considérons $p_1 | p_1 ... p_n = q_1 ... q_m \Rightarrow \exists$j tq $p_1 | q_j \Rightarrow \exists$ $u_1 \in$ A tq $q_j = u_1 p_1$
  q_j irrductible $\Rightarrow p_1 \in$ A* ou $u_1 \in$ A* $p_i \notin$ A et donc $u_i \in$ A*
  Ainsi p_i est associé a $q_j = q_{\sigma(i)}$
  On a : $p_1 ... p_n = q_1 ... q_{j-1} u p_1 q_{j+1} ... q_m \Rightarrow p_2 p_3 ... p_n = u_1 q_1 ... q_{j-1} q_{j+1} ... q_n$
  On continue : $p_2 = u_2 q_{\sigma(2)}$, $u_2 \in$ A*, $p_3 = ...$etc
  Comme m$\geq$ n on finit avec :
  $\Rightarrow q_{je} \in$ A* impossible $\Rightarrow$ m-n = 0 ie : m=n
  On a donc m=n et $p_i = u_i q_{\sigma(1)}$ $\forall$i = 1...n, avec $u_1 \in A^n, \sigma \in S_n$ $\square$

Théoreme : - dec en produit irréductible, dans A euclidien

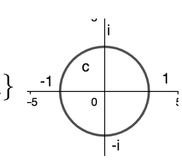
Remarques : -

1. Un anneau integre dans lequel THII.15 est valide s'appelle un anneau factoriel.
   Ainsi ce THéoreme dit : A euclidien $\Rightarrow$ A factoriel
2. En fait le theoreme plus général suivant est valide :
   A principale $\Rightarrow$ A factoriel
   On a donc les inclusions suivantes :
   {corps} $\subsetneq$ {anneaux euclidiens} $\subsetneq$ {anneaux} $\subsetneq$ {anneaux factoriel} $\subsetneq$ {anneaux integres}

2.6 Les entiers de Gauss

Soit $\mathbb{Z}[i] :=\{x + iy | x, y \in \mathbb{Z}\} \subset \mathbb{C}$

Par l'ex 7 serie 9 : c'est un sous-anneau de $\mathbb{C}$ dans un anneau integre et $\mathbb{Z}[i]^* = \{1, i, -1, -i\}$



C'est l'anneau de Gauss

Théoreme II.16 : -

$$\boxed{\text{L'anneau } \mathbb{Z}[i] \text{ est euclidien}}$$

Preuve : -Posons f $:\mathbb{Z}[i]-\{0\} \to \{1,2,3,...,\}$, $f(x+iy)=||x+iy||^2=x^2+y^2$

On a biien f(x+iy)$\geq 1 \quad \forall x+iy \neq 0$

De plus pour a,b $\in \mathbb{Z}[i]-\{0\}$ f(ab)=$||ab||^2=||a||^2\cdot||b||^2=f(a)f(b)\geq f(a)$ ce qui vérifie le premier point. Voyons le second

Fixons a,b $\in \mathbb{Z}[i]-\{0\}$; on veut trouver q,r$\in \mathbb{Z}[i]$ tq a=qb+r et f(r)< f(b) ou r=0

On a a,b $\in (\mathbb{Z}[i]-\{0\})\subset \mathbb{C}^*$ considérons $\frac{a}{b}\in \mathbb{C}^*$

$\frac{a}{b}=u+iv$ avec $u,v\in\mathbb{R}$

u$\in \mathbb{R} \Rightarrow \exists x\in\mathbb{Z}$ tq $(x-u)\leq \frac{1}{2}$; $\quad v\in\mathbb{R}\Rightarrow \exists y\in Z$ tq $|y-v|\leq\frac{1}{2}$

<u>Posons </u> q :=x+iy $\in \mathbb{Z}[i]$ et r :=a-qb $\in \mathbb{Z}[i]$

r=$a-qb=b\left(\frac{a}{b}-q\right)=b((u+iv)-(x+iy))=b(u-x+i(v-y))\Rightarrow$ soit r=0 soit :

$$f(r) \quad f(b)\cdot f((u-x)+i(v-y))$$
$$f(b)\cdot(\underbrace{u-x}_{\leq\frac{1}{4}})^2+(\underbrace{r-y}_{\leq\frac{1}{4}})^2)\leq\frac{1}{2}f(b)<f(b) \quad \square$$

Conséquence : - Tout les §II.5 s'applique a A=$\mathbb{Z}[i]$

Cela implique une preuve d'un théoreme de Fermat - on a besoin du Lemme :

Lemme II 17 : - Soit p un premier de la forme p=4n+1, n$\in\mathbb{N}$
Alors il existe m$\in\mathbb{Z}$ tq $m^2=-1(\text{mod } p)$

Preuve : - Soit donc p$\in\mathbb{N}$ un premier de la forme p=4n+1, et posons m $:=\left(\frac{p-1}{2}\right)!\in\mathbb{Z}$ Notons que $\frac{p-1}{2}$ est un entier pair :

$$\text{Calculons} \quad m^2 \quad = 1\cdot 2\cdot 3...\frac{p-1}{2}\cdot(-1)(-2)...\left(\frac{-p-1}{2}\right)$$
$$\equiv 1\cdot2\cdot3...\left(\frac{p-1}{2}\right)(p-1)(p-2)(p-3)...\left(\underbrace{p-\left(\frac{p-1}{2}\right)}_{\frac{p+1}{2}=\left(\frac{p-1}{2}+1\right)}\right)(\text{mod } p)$$
$$=1\cdot2\cdot3...\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}+1\right)....(p-3)(p-2)(p-1)=(p-1)!$$
$$=(-1)\text{ mod } p \quad \textit{par Wilson puisque p est premier} \quad \square$$

Théoreme des deux carré de Fermats : -

$$\boxed{\text{Un premier impair de deux carré si et seulement si il est congru à 1 modulo 4}}$$

Exemple : -

Preuve : -

$\Rightarrow$ tres facile exo

$\Leftarrow$ preuve de Dedekind 1894
Soit donc p un premier; $p \equiv 1(4)$
A voir; $\exists x, y \in \mathbb{Z}$ tq $p = x^2 + y^2$
Par Lemme II.17 il existe $m \in \mathbb{Z}$ tq $p | m^2 + 1$ dans $\mathbb{Z}$

Dans $\mathbb{Z}[i]$ on a :$m^2 + 1 = (m + i)(m - i)$
On a $p | (m^2 + 1) = (m + i)(m - i) \in \mathbb{Z}[i]$; mais $p \nmid m + i$, $p \nmid m - i$
$(p | m + i \Rightarrow \exists x, y \in \mathbb{Z}$ tq $m + i = p(x + iy) \Rightarrow \pm 1 = py$ impossible)
Cela signifie que $p \in \mathbb{Z}[i]$ *n'est pas premier* ($\Leftrightarrow$ pas irreductible, car $\mathbb{Z}[i]$ euclidien)
$\mathbb{Z}[i]$ euclidien $\Rightarrow$ on peut appliquer le Th II.15 a l'élément $p \in \mathbb{Z}[i]$

Ainsi il existe $p_1, ..., p_n \in \mathbb{Z}[i]$ irreductible tq $p = p_1 p_2 ... p_n$ $n \geq 2$
Appliquon f à cette égalité :

$p^2 = f(p) = f(p_1 ... p_n) = f(p_1) ... f(p_n) \in \mathbb{Z}$

de plus $f(p_i) > 1$ $\forall i$; car $f(p_i) = 1 \Rightarrow p_i \in \mathbb{Z}[i]^*$ impossible car p est premier

Comme $p \in \mathbb{Z}$ est premier, l'unicité de la décomposition en premier dans $\mathbb{Z}$ implique $\boxed{n \leq 2}$ On a donc n=2
$f(p_1) = f(p_2) = p$
$p_1 = x + iy \Rightarrow p = f(p_1) = x^2 + y^2$ $\square$

2.7 Anneaux de polynome

Dans tout ce paragraph, A est un anneaux commutatif
Notons A[X] l'ensemble des symbole $P = a_0 + a_1 X + a_2 X^2 + ... + a_n X^n$, avec $a_i \in A$
avec $P = a_0 + a_1 X + ... + a_n X^n$ et $Q = b_0 + b_1 X + ... + b_m X^m$ qui coïncide ssi $a_i = b_i$; $\forall i \geq 0$
• Sur A[X] on définit une addition comme suit :

$$P = \sum_{i \geq 0} a_i X^i; \quad Q = \sum_{i \geq 0} b_i X^i; \quad \Rightarrow P + Q = \sum_{i \geq 0} c_i X^i \text{ avec : } \quad c_i = a_i + b_i$$

• Sur A[X] on définit une multiplication :

$$P = \sum_{i \geq 0} a_i X^i; \quad Q = \sum_{j \geq 0} b_j X^j; \quad \Rightarrow P \cdot Q = \sum_{k \geq 0} c_k X^k \text{ avec } \quad c_k = \sum_{i+j=k} a_i b_j$$

Exemple : - $P = 2 + 3X - X^2$
$Q + 1 + 4X + X^2$

$$\begin{aligned} P \cdot Q &= (2 + 3X - X^2)(1 + 4X + X^2) = (2 \cdot 1) + (3 \cdot 1 + 2 \cdot 4) \cdot X + (2 \cdot 1 + 3 \cdot 4 + (-1) \cdot 1) \cdot X^2 \\ &+ (3 \cdot 1 + (-1) \cdot 4) X^3 + ((-1) \cdot 1) X^4 \\ &= 2 + 11 \cdot X + 13 \cdot X^2 - X^3 - X^4 \end{aligned}$$

Fait (A[X],+,·) est un anneau commutatif

Définition : - L'anneau A[X] est l'anneaux des polynome (en X) a coefficiant dans A

Terminologie : -

- Si $P = a_0 + a_1 X + ... + a_n X^n$ avec $a_n \neq 0$
  On dit que deg(P)=n (si P = 0 deg(P)=$-\infty$)
- Le coeficiant a_n est appelé le coeficiant dominant de P

Remarque : -

1. a est un sous-anneaux de A[X] via : $\begin{array}{ll} A\to & A[X] \\ a\to & P(A)=a \text{ polynome de degre } 0\end{array}$

   d'ou : - A^* est un sous-groupe de $A[X]^*$
   - A[X] integre $\Rightarrow$ A integre

2. $\deg(P+Q) \leq \max\{\deg P, \deg Q\}$

3. $\deg(P\cdot Q) \leq \deg(P) + \deg(Q)$ (Dans $\mathbb{Z}_4[X], P = [2]X = Q,\ \deg P = \deg Q = 1$
   mais $P\cdot Q = [2][2]\cdot X^2 = 0$

Proposition II.18 : - Soit A un anneaux integre. Alors :

(i) $A[X]^* = A^*$

(ii) A[X] est integre

(iii) $\deg(P\cdot Q) = \deg(P)+\deg(Q)$

Preuve : -

(iii) Soient $P=\sum_{i=0}^{n}, a_n \neq 0,\ Q = \sum_{j=0}^{m}, b_n \neq 0$

$PQ=\sum_{k\geq 0} c_k X^k$ avec $c_k = \sum_{i+j=k} a_i b_j$

$\Rightarrow$ $c_{n+m} = a_n \cdot b_m$ car $a_i = 0\ \forall i > n\ b_j = 0\ \forall j > n$

$a_n \neq 0, b_m \neq 0$, A integre $\Rightarrow c_{n+m} \neq 0 \Rightarrow \deg(P\cdot Q) \geq n+m = \deg(P)+\deg(Q)$

Comme $\deg(P\cdot Q) \leq \deg(P)+\deg(Q)$ on a gagne

(ii) Soient $P,Q \in A[X]$ avec $P \neq 0$ et $Q \neq 0$

$\Rightarrow$ $\deg(P) \geq 0$, $\deg(Q) \geq 0$

$\Rightarrow$ $\deg(PQ)=\deg(P)+\deg(Q) \geq 0 \Rightarrow PQ \neq 0$

(i) On a toujours $A^* \subset A[X]^*$ voyons l'autre inclusion

Soit $P \in A[X]^*$; il existe donc $Q \in A[X]$ tq $P\cdot Q = 1$

On a donc $0=\deg(1)=\deg(P)+\deg(Q) \Rightarrow \deg(P)=\deg(Q)=0$

$\to$ $P,Q \in A$ tq $PQ=1 \Rightarrow P \in A^*$

Conséquence : -

1. Si A est integre A[X] est integre
   Par II.4 on a A[X] se plonge dans son corp des fractions Q(A[X]) :
   Le corps des fonction rationnelles (a coef dans A)

2. Si a=K est un corps alors : $K[X]^*$: $K^*=K^*\backslash\{0\}$ les polynome de degre 0
   Ainsi tout polynome de degres 1 dans K[X] est irréductible

Preuve : -

<u>En effet</u> Si $P \in K[X]$; $\deg P = 1$, et $P=Q\cdot T$ alors :

$1=\deg P=\deg(Q\cdot T) = \deg Q + \deg T \Rightarrow \deg Q = 0$ ou $\deg T = 0$

$\Leftrightarrow Q \in K[X]^*$ ou $T \in K[X]^*$ . . Ainsi P est irréductible

Faux dans $\mathbb{Z}[X]$: $P=2X$

Théoreme II.19 : -

Si K est un corps alors l'anneau K[X] est euclidien pour degre :$K[X]\setminus\{0\} \to \{0,1,2\}$

Preuve : -

Pour P,Q $\in K[X]\setminus\{0\}$ deg(PQ)=deg P+$\underbrace{\text{deg Q}}_{\geq 0}$ $\geq$ deg P

Soient P,Q $\in P, Q \in K[X]\setminus\{0\}$
on doit trouver T,R $\in K[X] \text{tq} P = T \cdot Q + R$ avec R=0 ou deg R< deg Q
Fixons :

$$Q = \sum_{j=0}^{n} b_j X^j \textit{ avec } b_m \neq 0 \qquad \text{d'ou deg } Q = m \geq 0$$

Procédons par récurrence sur n=deg P ≥ 0

- Si $n < m$ *alors on pose* $T = 0\ R = P$
  Cela donne le départ de la récurrence sauf si m=0 auquel cas on a
  $Q = b_0 \in K^*$, *et l'on pose* $R = 0\ T = P \cdot b_0^{-1}$
- *Soit* $P = \sum_{i=0}^{n} a_i X^i$ avec $a_n \neq 0$ et supposons $n \geq m$
  posons $P_1 := P - a_n \cdot \underbrace{b_m^{-1}}_{b_m \in K\setminus\{0\}=K^*} X^{n-m}Q$
  Ainsi deg P $<$ n = deg P
  Par hypothèse de récurence $\exists T_1, R \in K[X]$ tq $P_1 = T_1Q + R$, $R = 0$ ou deg $R <$ deg Q

$\Rightarrow$ $P = P_1 + a_n b_m^{-1} X^{n-m} \cdot Q = (T_1Q + R) + a_n b_m^{-1} X^{n-m} Q = (\underbrace{T_1 + a_n b_m^{-1} X^{n-m}}_{:=T})Q + R$ $\square$

Remarque : -

1. C'est faux si A n'est pas un corps (en général)
   Par exemple $\mathbb{Z}[X]$ n'est pas euclidien
2. En fait la preuve montre que la division euclidienne est possible dans A[X] des que le coefficient dominant de Q est inversible ($b_m \in A^*$)

Exemple : -

$$\begin{array}{r|l} x^5 + 3x^4 + x^3 - 6x^2 - x + 1 & x^3 + 2x^2 + x - 1 \\ \hline -x^5 - 2x^4 - x^3 + x^2 & x^2 + x - 2 := T \\ -2x^2 + 2x - 1 = R & \end{array} \Rightarrow P = (x^2 + x - 2)Q + (-2x^2 + 2x - 1)$$

Si Y est un ensemble quelquconque et A un anneau alors :

$$A^Y = \{f : Y \to A\} \quad \textit{est un anneau pour :} \begin{array}{l} (f+g)(x)=f(x)+g(x) \\ f(\cdot\ g)(x)=f(x)g(x) \end{array}$$

En particulier $A^A = \{f : A \to A\}$ est un anneau

Tout P=$\sum_{i\geq 0} a_i X^i \in A[X]$ définit $\overline{P} : A \to A$ $\overline{P}(x) := \sum_{i\geq 0} a_i x^i$; l'application polynomial associé

De plus l'app $\varphi : A5X] \to A^A$ $\varphi(P) = \overline{P}$ est un homo d'anneaux

Terminologie : - a$\in$ A est un anneaux de P$\in$ A[X] $\Leftrightarrow$ (x-a)|P dans A[X]

Preuve : - $\Leftarrow$ (x-a)|P $\Leftrightarrow$ $\exists$ T$\in$ A[X] tq P=T$\cdot$$(x-a)$
Comme P$\to$ $\overline{P}$ est un hom $\overline{P} = \overline{T}\overline{(x-a)} \Rightarrow \overline{P}(a) = \overline{T}(a)\cdot(a-a) = \overline{T}(a)\cdot 0 = 0 \Leftrightarrow$ a est racine de P

$\Rightarrow$ Supposons a $\in$ A racine de P ie : $\overline{P}(a) = 0$
Faisons la division euclidienne de P par Q :=x-a $\in$ A[X] (ok car coef =1)
Donc $\exists$ T,R$\in$ A[X] tq P=T $\cdot$ Q + R R=0 ou deg R< deg Q = 1 $\Rightarrow$ R $\in$ A (R=0 ou deg R=0)
Comme P$\to$ $\overline{P}$ est un homo on a : $\overline{P} = \overline{T}\cdot\overline{Q} + \overline{R}$ R$\in$ A
Par hypothese : $O = \overline{P}(a) = \overline{T}(a)\cdot\underbrace{\overline{Q}(a)}_{=0} + \overline{R}(a) \Rightarrow R = 0 \Rightarrow P = T\cdot Q$ donc Q|P $\square$

Exemple : - Les éléments irréductible ($\Leftrightarrow$ premier) de $\mathbb{C}$[X] sont les polynome de degrés 1
Par conséquent tout P$\in$ $\mathbb{C}$[X] irréductible est associé a un unique X-$\lambda \in \mathbb{C}$[X]

On a deja vu :	P$\in$ $\mathbb{C}$[X] deg P=1 $\Rightarrow$ P irréductible
<u>reste a voir</u>	deg P$\neq$ 1$\Rightarrow$ P non irreductible
	-deg P = 0 $\Leftrightarrow$ P$\in$ $\mathbb{C}[X]^*$ $\Rightarrow$ P pas irréductible
	-deg P$\geq$ 2 $\Rightarrow$ P admet au moin une racine a$\in$ $\mathbb{C}$
	$\Rightarrow (x-a)\|P \Rightarrow \exists T \in \mathbb{C}[X]$; tq $P = (x-a)T,\ \deg T, = \deg P - 1 \geq 1$
	$\Rightarrow$ P pas irréductible
<u>Par consequent</u>	P$\in$ $\mathbb{C}$[X] irreductible $\Leftrightarrow$ deg P = 1
	deg P =1 $\Leftrightarrow$ $P = a_0 + a_1x,\ a_1 \neq 0 \Rightarrow$ P est associé a x+$(a_1)^{-1}a_0 := x - \lambda$

La

décomposition en irréductible de P$\in$ $\mathbb{C}$[X] est P=a(x-λ_1)$(x-\lambda_2)...(x-\lambda_n)$
ou a $\in \mathbb{C}^*$ est le coeff dominant de P, et $\lambda_1, ..., \lambda_n$ sont les racines

3 Chapitre III Espace vectoriels et modules

3.1 Espaces vectoriel et application linéaires

Définition : - Soit K un corps. un ensemble E muni de deux lois :
$+ : \mathrm{E} \times \mathrm{E} \to \mathrm{E}$ et $\cdot \mathrm{K} \times \mathrm{E} \to \mathrm{E}$
est appellé un espaces vectoriel sur K si

(E1)	est un groupe abélien
(E2)	$\lambda(\mu \mathrm{v}) = (\lambda\mu) \cdot \mathrm{v}$
(E3)	$(\lambda + \mu)\mathrm{v} = \lambda \mathrm{v} + \mu \mathrm{v}$
(E4)	$\lambda(\mathrm{v} + \mathrm{w}) = \lambda \mathrm{v} + \lambda \mathrm{w}$
(E5)	$1_{\mathrm{K}} \cdot \mathrm{v} = \mathrm{v}$

Remarque/Terminologie : -

1. Les éléments de K sont appelé des scalaires et ceux de E des vecteurs
2. C'est la def de 1 semestre mais avec K un corps quelqconque pex $\mathrm{K}=\mathbb{R}, \mathbb{C}$ $\mathrm{K}=\mathbb{Q}$ $\boxed{\mathrm{K}=\mathbb{Z}/\mathrm{p}\mathbb{Z} := \mathbb{F}}$ $\mathrm{K}=\mathrm{Q}(\mathbb{Z}[\mathrm{X}])$
3. On a les regle de calcul suivantes :
   (i) $\mathrm{O}_{\mathrm{K}} \cdot \mathrm{v} = \mathrm{O}_{\mathrm{E}} \quad \forall \mathrm{v} \in \mathrm{E}$
   (ii) $\lambda \cdot \mathrm{O}_{\mathrm{E}} = \mathrm{O}_{\mathrm{E}} \quad \forall \lambda \in \mathrm{K}$
   (iii) $\lambda \mathrm{v} = 0 \Rightarrow \lambda = \mathrm{O}_{\mathrm{K}}$ ou $\mathrm{v} = \mathrm{O}_{\mathrm{E}}$
   (iv) $(-\lambda)\mathrm{v} = -(\lambda \mathrm{v})$ qu'on note $-\lambda \mathrm{v}$

Exemple d'espace vectoriels : -

1. Un $\mathbb{F}_2$ -espace vectoriel est exactement un groupe abélien ou tout élément non-trivial est d'ordre 2.
2. Soit K un sous-espace d'un corps L K sous-anneaux de L
   Alors L est un sous-espace vectoriel sur K :
   (E1) $\Leftrightarrow$ (A1)
   (E2) $\Leftrightarrow$ (A2)
   (E3)(E4) $\Leftrightarrow$ (A3)
   (E5) $\Leftrightarrow$ (A4)
   $\mathbb{C}$ est un $\mathbb{R}$-espace vectoriel R est un $\mathbb{Q}$ espace vectoriel
   tout corps de caractéristiques 0 est un $\mathbb{Q}$ esapce vectoriel
   tout corps de caractéristiques P est un $\mathbb{F}$ espace vectoriel
   En particulier K est un K-espace vectoriel
3. $E{=}K^n = \underbrace{K \times ... \times K}_{n}$ ($n \geq 1$) est un esp vectoriel pour :
   $(x_1, ..., x_n + (y_1, ..., y_n) = (x_1 + y_1 + ... + x_n + y_n) \quad \lambda(x_1, ..., x_n)$
4. Pour K un corps E=K[X] est un espaces vectoriel sur K
   via $P + Q$ et $\lambda \cdot P = \lambda(\sum a_i x^i) = \sum(\lambda a_i)x^i$
   De meme $K_n[X] := \{P \in K[X] | \deg P < n\}$ est un K esp vectoriel
5. Pour K un corps et $n \geq 1$ L'ensemble $M_n(K)$ des matrices $n{\times}n$ a coeff dans K est un K-espace vectoriel
6. Si $E_1, .., E_n$ sont des K-espaces vectoriels alors :
   $E := E_1 \times ... \times E_n$ est un K-esp vectoriel via : $\begin{array}{l}(v_1, v_n) + (w_1...w_n) = (v_1 + w_1..v_n + w_n) \\ \lambda(v_1..v_n) = (\lambda v_1..\lambda v_n)\end{array}$
   On le note $E{=}E_1 \oplus ... \oplus E_n$ appelé
   la somme directe de $E_1...E_n$ par exemples si $E_1 = ...E_n$ on retourne $E{=}K^n$

Terminologie : - Un sous-ensemble non-vide $F \neq \emptyset$ d'un espace vectoriel E est appellé un sous-espace vectoriel de E si :

- $v, w \in F \Rightarrow v + w \in F; \quad \lambda \in K, v \in F \Rightarrow \lambda \cdot v \in F$
  (equiv *f est un esp vectoril pour la restriction des 2 lois de E a F)*

Exemple : -

1. Tout espace vectoriel E admets les sou-espaces vectoriel $F{=}\{0\}$ et F=E
2. Si on a une suite de sous-corps $K \subset L \subset M$ alors L et M sont des K-espaces vectoriels et L est un sous-espace vectoriel de M
3. $K_n[X] := \{P \in K[X] \mid \deg P < n\}$ est un sous-espace vectoriel de $K_m[X]$ $\forall m \geq n$ et de K[X]
4. Si on a F_1 F_2 sous-espace vectoriel de E $\Rightarrow F_1 \cap F_2$ est aussi un sous-esapce vectoriel
5. Si on a F_1 F_2 sous-espace de E alors $F_1 + F_2 = \{v_1 + v_2 \mid v_1 \in F_1 \; v_2 \in F_2\}$
   est aussi un sous-espace vectoriel

Définition : - Soit E E' deux espace vectoriel sur un même corps K. Une application $f : E \to E'$ est dite linéaire (ou K linéaire) si :

- $f(v{+}w){=}f(v){+}f(w) \quad \forall v, w \in E$
- $f(\lambda v) = \lambda f(v) \quad \forall v \in E$

Remarque et Terminologie : -

1. On note habituellement $L(E, E') \quad (= L_k(E, E'))$ l'ensemble linéaire
2. Comme d'habitude on peut considérer $Ker(f) = \{v \in E \mid f(v) = 0\} \subset E$ et $Im(f) \subset E'$
   Ce sont des sous-espace vectoriel
   On a toujours : $Ker(f) = \{0\} \Leftrightarrow f$ est injective
3. $\left.\begin{array}{lll} f: & E \to E' & \textit{linéaire} \\ g: & E' \to E" & \textit{linéaire} \end{array}\right\} \Rightarrow g \circ f : E \to E"$ *est linéaire*
4. Un isomorphisme (linéaire au isomohpsiem d'espace vectoriel) est une application linéaire
   $f : E \to E'$ bijective (d'inverse linéaire mais c'est une séquence)
5. F_1, F_2 sous-espace vectoriel alors $F_1 + F_2 := \{v_1 + v_2 \mid v_1 \in F_1, v_2 \in F_2\}$ est ou sous-esapce de E

Exemple d'application linéaire : -

1. L'application nulle $f : E \to E'$ $f('v) = 0 \quad \forall v \in E$ est linéaire (avec Ker(f)=E et$Im(f) = \{0\}$)
2. Si F est un sous-espace vectoriel de E, alors l'inclusion $f : F \to E$ $f(v) = v$ est linéaire
   avec Ker(f)=$\{0\}$ (f inj) et Im(f)=F)
   en particulier $f = Id_E$ est linéaire
3. Pour $\lambda \in K$ l'application $ev_\lambda : K[X] \to K$
   définie par $ev_\lambda \; (\sum_i a_i X^i) = \sum_i a_i x^i$ est linéaire
   $(Ker(ev_\lambda) = \{P \in K[X] \mid \lambda$ *est racine de* $P\} \quad Im(ev_\lambda) = K)$

Terminolgie : - Soit E un sous-espace vectoriel et $F_1, ..., F_n$ des sous-espace vectoriel de E
On dit que E est la somme directe (interne) de $F_1, .., F_n$ si tout v$\in$ E s'écrit de maniere unqieu $v = V_1 + ... + v_N \quad v_i \in F_i \forall i = 1, ..., n$

Remarque : - E est somme directe interne de $F_1, ..., F_u$ si et seulement si :

$$E = F_1 + ... + F_n \text{ et } F_i \cap F_j = \{0\} \quad \forall i \neq j$$

(Tout éléments r$\in$ E s'écrit $v = v_1 + ... + v_N$ $v_I \in F_i \Leftrightarrow E = F_1 + ... F_n$
L'unicité de l'écriture $\Leftrightarrow F_i \cap F_j = \{0\} \quad \forall i \neq j$)

Proposition III.1 : - Si E est somme directe (interne) de $F_1 \ldots F_n \subset E$ alors $E \cong F_1 \oplus ... \oplus F_n$ E est isomorphe a la somme directe (externe) des espaces vectoreils $F_1, ..., F_n$

Preuve : - Soit E somme directe (interne) de $F_1, ..., F_n$

Posons $f : F_1 \oplus ... \oplus F_n \to E$ définie par $f(v_1, ..., v_n) = v_1 + ... + v_n$

f est linéaire :

$$\begin{aligned} f((v_1, ..., v_n) + (w_1, ..., w_n) &= f(v_1 w1, ..., v_n w_n) = (v_1 + w_1) + ... + (v_n + w_n) \\ &= (v_1 + ... + v_n) + (w_1 + ... + w_n) = f(v_1 ... v_n) + f(w_1 ... w_n) \end{aligned}$$

$$f(\lambda(v_1..v_n)) = f(\lambda v_1..\lambda v_n) = \lambda v_1 + .. + \lambda v_n = \lambda(v_1 + ... + v_n) = \lambda f(v_1..v_n)$$

$$\left.\begin{array}{l} \text{Donc f linéaire} \\ \text{Finalement f est surjective} \\ \text{car tout v} \in \text{E s'écrit } v = v_1 + .. + v_n) \text{ avec } v_i \in F_i \\ \text{et f est injective car cette écriture est unique} \\ \text{(par def de somme directe interne)} \end{array}\right\} \Rightarrow \text{f isomorphisme} \quad \square$$

Remarque : -

Si F est un sous-espace vectoriel de E alors (F,+) est un sous-groupe (E,+) et on peut donc considérer le groupe quotient E/F muni de l'addition $[v] + [w] := [v + w]$

De plus on peut munir E/F d'une loi $K \times E/F \to E/F$ via :

$$\lambda \in K \ [v] \in E/F \quad \Longrightarrow \quad [v]\lambda \cdot [v] = [\lambda v]$$

Cela munit E/F d'une structure d'espace vectoriel et tous les resultats vu au chap I s'étendent)

3.2 Indépendance linéaire base, dimension

Terminologie : -

- Si E est un K espace vectoriel et $v_1..v_n \in E$ alors tout $v = \lambda_1 v_1 + .. + \lambda_n v_n \in E$
  Avec $\lambda_i \in K$ est une combinaison linéaire de $v_1..v_n$
- Pour $\emptyset \neq S \subset E$ un sous-ensemble non-vide de E on pose
  $L(S) :=\{$*combinaison linéaire d'un nombre fini d'éléments de S*$\} = \{\lambda_1 v_1 + .. + \lambda_n v_n \mid \begin{matrix} n \geq 0, \ \lambda_i \in K \\ v_i \in S \end{matrix}$
- Par convention $L(\emptyset)=\{0\}$ L(S) est le sous-espace vetoriel engendré par S

Lemme III.2 -

(i) L(S) est un sous-espace vectoriel de E, le plus petit contenant S (d'ou le nom)

(ii) $S \subset T \subset E \Rightarrow L(S) \subset L(T)$

(iii) $L(S \cup T) = L(s) + L(T)$ pour $S,T \subset E$

Preuve : -

(ii) trivial

(i) Si $v,w \in L(s)$ alors $v = \lambda_1 v_1 + .. + \lambda_n v_n \quad w = \mu_m w_m \begin{matrix} v_i w_j \in S \\ \lambda_i \mu_j \in K \end{matrix}$

$\Rightarrow v+w = \lambda_1 v_1 + ..\lambda_n v_n + \mu_1 w_1 + .. + \mu_m w_m \in L(S)$
et $\lambda \cdot v = \lambda(\lambda_1 v_1 + .. + \lambda_n v_N \mid \ = (\lambda\lambda_1)v_1 + ... + (\lambda\lambda_n)v_N \in L(S)$
Soit finalement $F \subset E$ un sous-espace vectoriel avec $F \supset S$

$F \supset S \quad \mathrm{F\ sous-espzce\ vectoriel} \Rightarrow F \supset \{\lambda \cdot v \mid \lambda \in K, v \in S\}$
$\quad \mathrm{F\ sous-espace\ vectoriel} \Rightarrow F \supset \{\mathrm{somme\ de}\ \lambda_i v_i \ \lambda_i \in K \ v_i \in S\} = L(S)$

Ainsi L(S) est le plus petit sous-espace vectoriel de E contenant S $\square$

Terminologie : - Un espace vectoriel E est dit de-dimension-fini sur K s'il existe S fini $\subset E$ tq $E = L(S)$

Exemple : -

1. $\mathbb{C} = L(\{1, 2, \})$ est de-dimension-fini sur $\mathbb{R}$
2. $K^n = L(\overbrace{(1, 0, .., 0)}^{=e_1}, ..., \overbrace{(0, ..., 0, 1)}^{=e_n}\ )$ est de-dim-fini sur K
3. $K_n[X] = L(\{1, x, x^2, x^3, .., x^{n-1}\})$ est de-dim-fini sur F $\forall n$
4. K[X] n'est pas de dimension fini sur K

Si $S \subset K[X]$ est fini L(S) ne contient que des polynome de degres$\leq \max\{\deg \mid P \in S\}$
d'ou : $L(S) \neq K[X]$

Définition : -

Soit E un espace vectoriel sur K et $v_1,..,v_n \in Z$ On dit que $v_1,..,v_n$ sont linéairement indépandant si :

$$\lambda_1 v_1 + .. + \lambda_n v_n = \quad \lambda_1..\lambda_n \in K \Rightarrow \lambda_1 = .. = \lambda_n = 0$$

Sinon il sont dit linéairement dépendant

Exemple : -

1. $\{1,2\} \subset \mathbb{C}$ est une famille libre sur $\mathbb{R}$ mais liée sur $\mathbb{C}$
2. $e_1,..,e_n \in K^n$ sont linéairement indépandant sur K
3. $\{1,x,..,x^{n-1}\}$ est dit libre de $K_n[X]$ sur K

Remarque : - Si $v_1,..,v_n \in E$ est une famille libre, alors tout éléments de $L(\{v_1,..,v_n\})$ s'écrit de manière unique comme combinaison linéaire des $v_1,..,v_n$

<u>En effet</u> si $v = \lambda_1 v_1 + ... + \lambda_n v_n = \lambda'_1 + v_1 + ... + \lambda'_n v_n \quad \lambda_i, \lambda'_i \in K$

$\Rightarrow$ 0=v-v=$(\lambda_1 v + ... + \lambda_n v_n) - (\lambda_1 v_1 + ... + \lambda_n v_n)) - (\lambda'_1 v_1 + .. + \lambda'_n v_n) = (\lambda_1 - \lambda'_1)v_1 + ...$

Comme $v_i,..,v_n$ est libre on a : $\lambda_i - \lambda'_i = 0 \quad \forall i$ dans $\lambda_i = \lambda'_i$

Proposition III.3 : - Soit $v_1,..,v_n \in E$ une famille liée
Alors il existe j$\in \{1,..,n\}$ tq v_j est combinaison lin de $v_1..v_{j-1}$

Preuve : - Par hypothèse il existe $\lambda_1..\lambda_n \in K$ non-tous nuls, tq ; $\lambda_1 v_1 + ... + \lambda_n v_n = 0$

<u>Posons</u> j :=max$\{i \mid \lambda_i \neq 0\}$ $\quad 0 = \lambda_1 v_1 + ..\lambda_n v_N = \lambda_1 v_1 + ..\lambda_j v_j$ car ; $i > j \Rightarrow \lambda_i = O$

$$\lambda_j v_j = -(\lambda_1 v_1 + .. + \lambda_j v_j) \underset{\lambda_j \neq 0}{\Rightarrow} v_j = ((-\lambda_j)^{-1}\lambda_1)v_1 + ... + ((-\lambda_j)^{-1}\lambda_{j-1})v_{j-1} \qquad \square$$

Corrolaire III.4 : - Soient $v_1..v_N \in E$ avec $v_1..v_k$ linéairement indépendant (k$\in \{0,1..n\}$)

<u>Alors</u> il existe $\{i_1,...i_r\} \subset \{k+1..n\}$ tq $v_1..v_k, v_{i1}..v_{ir}$ est linéairemeny indéperndant et :

$$L(\{v_1..v_n, v_{i1}..v_{ir}\}) = L(\{v_1..v_n\})$$

Preuve : - soit donc $S := \{v_1..v_n\} \subset E$, avec $v_1..v_k$ linéairement indépendant

Supposons qu'il n'existe pas de $v_j \in S$ combinaison linéaire des $v_1..v_{j-1}$
Dans ce cas par la contrapos" de la prop 4 , la famille S est libre

Dans ce cas onpose $\{i,..,ir\} = \{k+1..n\}$ il n'y a rien a faire

dans le cas contraire : il existe v_j combinaison linéaire de $v_i..v_{j-1}$ Prenons le plus grand tel j, et posons S'=S-$\{v_j\} = \{v_1..v_k, v_{k+1}..v_{j-1}, v_{j+1}..v_n\}$
notons que $j > k$ car $v_1..v_k$ est libre)
on a : L(S') = L(S) : $S' \subset S \Rightarrow L(S') \subset L(S)$
$L(S) \subset L(S')$: car v_j est combinaison linéaire des $v_i..v_{j-1}$

On recommence : supposons qu'aucun $v_l \in S'$ n'est combinaison linéaire des précédent

Par propostion 4 S' est libre et L(S') est libre et L(S') = L(S) On pose $\{i..i_r\} = \{k+1..n\} \backslash \{j\}$ Sinon on enleve le plus grand $v_l \in S'$ combinaison linéaire des précédents

On continue cette procédure jusqu'a obtenir : T=$\{v_1..v_k, v_{i1}..v_{il}\} \subset S$ tq L(T) =L(S)

et aucun éléments n'est combinaison linéaire des précédent et par Prop 4 cette famille est libre $\square$

Définition. : - Soit S$\subset$ E un espace vectoriel L ensemble S est une base de E si :

(i) L(S) = E

(ii) toute famille finie $\{v_1..v_n\} \subset S$ est libre

Remarque : -

De manière équivalente : toute éléments de E s'écrit de facon unique comme combinaison linéaire d'éléments de S

Théoreme : -

tout espacr vectoriel de-dimension-fini admet une base

Preuve : -

soit E un espace de dimension fini Donc il existe S :=$\{v_1..v_n\} \subset$ E tq E=L(S) Appliquons CorIII.4 dans le cas k=0 :

$\exists\{i_1..i_r\} \subset \{1..n\}$
tq $v_i..v_{ir}$ est libre et $L5\{v_{i1}..v_{ir}) = L(S) = E$ donc $v_{i1}..v_{ir}$ est une base $\square$

Exemple de base : -

1. $\{1, i\}$ est u n base de $\mathbb{C}$ ou $\mathbb{R}$
2. $\{e_1..e_n\}$ est une base de K^n (ou $e_j := (0, ..0, 1, 0, .., 0)$)
3. $\{1, x, x^2, .., x^{n-1}\}$ est une base de $K_n[X]$
4. $\{1, x, x^2, x^3..\}$ est une base de K[X]

Remarque : -

tout espace vectoriel admet une base
Mais la preuve repose sur "le lemme de Zorm" (axiome du choix), et n'est donc pas constructible (voir exo 7 serie 11)

Lemme III.6 : - Si $v_1..v_n$ engendre l'espace vectoriel E et $w_1..w_m$ sont linéairement indépendant alors $m \leq n$

preuve : -

Soit donc $v_1..v_n \in E$ qui engendrent E et $w_1..w_n \in E$ lineairement indépendant
<u>A voir</u> $m \leq n$

considérons la famille $w_m, v_1..v_n$ cette famille engendre E mais est liée car $v_1..v_n$ engendrent E
Appliquons cor.4 à : $w_m v_1..v_n$ en utilisant (w_m est libre) :

$$\exists\{i_1..i_r\} \subset \{1..n\} \text{ avec } r \leq n-1 \text{ tq } w_m, v_{i1}..v_{ir} \textit{ est une base de E}$$

On recomence avec $w_{m-1}, w_m, v_{i1}..v_{ir}$ engendrent E mais liée comme avant
On applique a nouveau cor.4 à $w_{m-1}, w_m, v_{i1}..v_{ir}$ (w_{m-1}, w_m libre) :

$$\exists\{j_1..j_s\} \subset \{i_1..i_r\} \text{ avec } s \leq r-1 \leq n-2 \text{ tq } w_{m-1}, w_m\ v_{j1}..v_{js} \text{ est une base}$$

Etc... apres m_1 itération de ce processus on obtient une base de E de la forme $w_2..w_n\ v_k\ v_{kl}$ avec l$\leq n-(m-1) = n-m+1$

<u>finalement</u> comme $w_1 \in E$ w_1 est combinaison linéaire de $w_2..w_m\ v_{k1}\ v_{kl}$ et comme $w_1..w_m$ est libre un des v_{kj} apparait dans cette combinaison linéaire
Cela donne donc l≥ 1

On obtient ainsi : $n-m+1 \geq l \geq 1 \Rightarrow m \leq n$ $\square$

Théoreme III.7 : -

deux lois pour un espace vectoriel de-dimension-fini ont meme cardinal

Preuve : - Soient $\{v_1..v_n\}$ et $\{w_1..w_m\}$ deux base pour E

Comme $v_1..v_n$ engendrent E et $w_1..w_m$ est libre on a :
On échangent les rôle : $n \leq m$ Ainsi m=n □

Définition : -

Soit E un espace vectoriel de-dimension-fini. La dimension de E notée dim(E) est le nombre déléments d'une base quelconque de E

Remarque : -

1. Ainsi si E est de-dilension-finie on a que dim(E) est finie
   Cela justifie la terminologie et l'on peut abandonné les tirets
2. Ce théoreme est valable pour tout espace vectoriel et l'on peut donc définir la dimension de E comme le cardinal (peut etre infin) d'une base quelcconque de E

Exemple : -

1. $\dim_{\mathbb{R}} (\mathbb{C})=2$
2. $\dim(K^n)=n$
3. $\dim(K_n[x]) = n$

Théoreme III.8 : -
Deux espaces vectoriels de dimension finie E et E' sont isomorphe si et seulement si dim(E)=dim(E')

Preuve : -

$\Leftarrow$ Soit E de dimension n. On va montrer que $E \cong K^n$ Du coup si E' est un autre espace vectoriel de dim n on a $E' \cong K^n$ d'ou $E \cong E'$ et on a fini

soit donc E de dim n. Il existe donc une base $v_1..v_n$ de E
Soit :

$$f : K^n \to E \quad f(x_1..x_n) = x_1v_1 + .. + x_nv_n \left(= \sum_{i=1}^{n} x_iv_i\right)$$

f est linéaire : $f((x_1..x_n) + (y_1..y_n)) = f(x_1 + y_1 + .. + x_n + y_n) = \sum_{i=1}^{n}(x_i + y_i) = \sum_{i=1}^{n} x_iv_i + \sum_{i=1}^{n} y_iv_i$

$$f(\lambda(x_1.x_n)) = f(\lambda x_1..\lambda x_n) = \sum_{i=1}^{n}(\lambda x_i)v_i = \sum_{i=1}^{n} \lambda(x_iv_i) = \lambda \sum_{i=1}^{n} x_iv_i = \lambda f(x_1..x_n)$$

f est surjective car : $v_1..v_n$ engendre E ; f injective $\Leftrightarrow$ Ker f = 0 $\Leftrightarrow$ $v_1..v_n$ linéairement indépendant

$\Rightarrow$ Soit f :E$\to E'$ un isomorphisme et soit S une base de E.
On va montrer que f(S) est une base de E'
(Du coup f :S $\to$ f(S) est une bijection on aura : dim(E)=#S = #f(S) = dim(E') et on aura fini)

(i) Soit v' $\in E'$ f surjective $\Rightarrow \exists v \in E$ tq $v' = f(v)$
Comme E =L(S) $\exists v_1..v_n \in S \lambda_1..\lambda_n \in K$ tq $v = \lambda_1 v_1 + .. + \lambda_n v_n$
$\Rightarrow \quad v' = f(v) = f(\lambda_1 v_1..\lambda_n v_n) = \lambda_1 f(v_1) + .. + \lambda_n(fv_n)$ avec $f(v) \in f(S)$
On a donc v' $\in L(f(S))$ d'ou E' = L(f(S))

(ii) Soient $v'_1..v'_n \in f(S)$ et $\lambda_1..\lambda_n \in K$ tq $\lambda_1 v'_1 + .. + \lambda_n v'_n = 0$
a voir $\lambda_1 = .. = \lambda_n = 0$
$v'_i \in f(S) \Rightarrow \exists v_i \in S$ tq $v'_i = f(v_2)$
$\Rightarrow \quad 0= \lambda_1 v'_1 + ... + \lambda_n v'_n = \lambda_1 f(v_1) + ... + \lambda_n f(v_N) = f(\lambda_1 v_1 + .. + \lambda_n v_n)$
Come f est injective cela implique $\lambda_1 v_1 + .. + \lambda_n v_n = 0$
Come $v_i \in S$, S base on a $\{v_i..v_n\}$ est libre d'ou $\lambda_1 = .. = \lambda_n = 0$ $\square$

Théoreme : - E$\cong$ E' $\Leftrightarrow$ dim(E) = dim(E')

Exemple -

1) $\mathbb{C} \cong \mathbb{R}^2$
2) $K_n[X] \cong K^n$
3) $\mathbb{R}^n \ncong \mathbb{R}^m$ pour n$\neq$ m

Lemme III.9 : - Soi tE un espace vectoriel de dimension rinie et F un sous-espace de E alors :

- F est de-dimension-finie; $\dim(F) \leq \dim(E)$; $\dim(E/F) = \dim(E) - \dim(F)$

Théoreme III.10 : - (Théoreme du rang) :

Si $f : E \to E'$ *est une application linéaire avec E de dimension finie alors*

$$\boxed{\mathrm{Dim}(E) = \dim(\mathrm{Ker}\ f) + \dim(\mathrm{Im}\ f))}$$

Démonstration : - Soit donc $F : E \to E'$ avec $\dim(E) < \infty$ Cela définit un isomorphisme $E/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$ On a donc :

$\dim(\mathrm{Im}(f))$=$\dim(E/\mathrm{Ker}(f)) \overset{\mathrm{LemmeII.9}}{=} \dim(E) - \dim(\mathrm{Ker}(f))$ $\square$

Preuve du Lemme : - Soit donc E de dim-fini dim(E)=n et F un sous-espace

- Par le Lemme III.6 toute famille s de n+1 éléments de F est liée (contraposé Lemme III.6)

Soit $w_1, ..w_m$ une famille libre de taille maximale dans F on a donc m$\leq$ n

<u>Afiirmation</u> $w_1..w_m$ engendrent F ($\Rightarrow w_1..w_m$un base $\Rightarrow \dim(F) = m \ \leq n = \dim(E)$)

<u>en effet</u> : Soit w$\in$ F un élément quelconque. Par maximalité de $w_1..w_m$ la famille $w_1..w_m$ w est liée Ainsi il existe $\lambda_1..\lambda_m\lambda \in K$ non tous nul tq

$\lambda_1 w_1..\lambda_m w_m + \lambda_m = 0$
On a $\lambda \neq 0$ carr si $\lambda. = 0$ on a. : $\lambda_1..\lambda_m$ non-nul t $\lambda_1 w_1...\lambda_m w_m = 0$; ie : $w_1..w_m$ est liée une contradiction
Ainsi $\lambda \neq 0 \in K$ d'ou $\lambda w = -(\lambda_1 w_1 + .. + \lambda_m w_m) \Rightarrow w = ((-\lambda)^{-1}\lambda_1)w_1 + .. + (-\lambda^{-1}\lambda_m)w_m \in L(\{w_1..w_m\})$, on a fini

- Soit $w_1..w_m$. une base de F. Comme dim E = n il existe une base $v_1..v_n$ de E

Apliquons Le corrolaire III.4 a la famille $w_1..w_m, v_1..v_m$ avec $w_1..w_m$est libre :

$$\textit{il existe } \{i_1..i_r\} \subset \{1..n\} \text{ tq } w_1..w_m, v_{i1}..v_{ir} \textit{ est une base de E} \quad (\text{avec } m + r = n)$$

Affirmation $[V_i]..[V_{ir}] \in E/F$ est une base de E/F ($\Rightarrow (\dim(E/F) = r = n - m = \dim E - \dim F)$
En effet Démontronq les 2 points dans la définiton d'une base

- *un éléments quelconque de E/F est de la forme*$[V] = \pi(v) \in E/F$ *avec* $v \in E$ et $\pi : E \to E/F$
  comme $w_1..w_m, v_{i1}..v_{ir}$ *engendrent E il existe* $\lambda_1..\lambda_m, \mu_1..\mu_r$ tq
  $v = \lambda_1 w_1 + ..\lambda_m v_m + \mu_1 v_1 + ... + \mu_R v_{ir}$ *On applique* π :

$$[v] = \pi(v) = \lambda_1 \underbrace{\pi(w_1)}_{=0} +.. + \lambda_m \underbrace{\pi(w_m)}_{=0} + \mu_1\pi(v_{i1}) + ... + \mu_r\pi(v_{ir}) = \mu_1[v_{i1}] + .. + \mu[v_{ir}]$$

$(w_i \in F = \ker(\pi))$ Donc cette famille engendre E/F

(ii) Soient $\alpha_1..\alpha_r \in K$ tq $\alpha_1[V_{i1}] + ... + \alpha_r[V_{ir}] = 0 \in E/F$
A voir $\alpha_1 = .. = \alpha_r = 0$ est on aura terminer
$\Rightarrow [\alpha_1 v_{i1} + .. + \alpha_r v_{ir}] \in F = L(\{w_1..w_m\})$
Ainsi il existe $\beta_1 \dots \beta_m \in K$ tq $\alpha_1 v_{i1} + ... + \alpha_r v_{ir} = \beta_1 w_1 + ... + \beta_m w_m$
$\Rightarrow 0 = \beta_1 w_1 + ... + \beta_m w_m - \alpha_1 v_{i1} - ... - \alpha_r v_{ir} \Rightarrow \beta_1 = .. = \beta_m = \alpha_1 = .. = \alpha_r = 0$ □

Terminologie : - Une suite $0 \xrightarrow{f_0} E_1 \xrightarrow{f_1} E_2 \xrightarrow{f_2} E_3 \xrightarrow{f_3} ... \xrightarrow{f_{n-1}} E_n \xrightarrow{f_n} 0$
d'application linéaire est dite exacte si $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1}) \quad \forall i$

Corrolaire : - Dans une suite exacted'espace vectoriel de dimension finie on a :

$$\sum_{i=1}^{n} (-1)^i \dim(E_i) = 0$$

Preuve : - Appliquns les th du rang a $f_i : E_i \to E_{i+1}$:

$$\sum_{i=1}^{n} (-1)^i \dim(E_i) = \sum_{i=1}^{n} (-1)^i (\dim(\mathrm{Ker}(f_i)) + \dim(\mathrm{Im}(f_i))$$

$$= \sum_{i=1}^{n} (-1)^i (\dim(\mathrm{Ker}(f_i)) + \dim(\mathrm{Ker}(f_{i+1}))$$

$= - (\dim \mathrm{Ker}(f_i) + \cancel{\dim \mathrm{Ker}(f_2)}) + (\cancel{\dim(\mathrm{Ker}(f_2))} + \cancel{\dim(\mathrm{Ker} f_3)}) + ...+$
$(-1)^n (\cancel{\dim \mathrm{Ker}(f_n)} + \underbrace{\mathrm{Ker}(f_{n+1}}_{=\mathrm{Im}(f_n)=0} = 0$ □

3.3 Application aux polyèdre

On considère un polyèdre. On note : $\begin{cases} S := \#\text{ sommets de } P \\ A := \#\text{ d'arrete de } P \\ F := \#\text{ de face de } P \end{cases}$

Existe il une relation entre S,A et F ?

Exemple : -

	pyra	cube	octa	dodéca	isoca
S	4	8	6	20	12
A	6	12	12	30	30
F	4	6	8	12	20

Euler [1758] Pour tout olyèdre P. on a $S-A+F=2$

Définition : - (Mobius)

Un polyèdre est une collection finie de polygone (face) telle que :

(i) Si deux faces se rencontrent c'est en un sommets ou en une arretes

(ii) Chaque arrête borde exactement 2 faces (3 hors jeu) dite adjacente

(iii) Pour toute paire de face , f,f', il existe des faces $f_1, f_2..f_n$ tq

f=$f..f_N = f'$ et f_{i+1} est adjacente a f_i $\forall$i..(1 et 2 hors jeu)

Mais voici un autre contre-exemple

Théoreme : -

Soit P un polyèdre tq toute boucle forme d'arrête une collection de faces (4) Alors S-A+F = 2

Preliminaire a la preuve : -

- On va appeler un sommet : un o-polytope
  Une arrete : un 1-polytope
  Une face : un polytope 2-polytope
  Un polyèdre : un 3-polytope
- Soit P un polyèdre fixéé pour n= -1, 0, 1, 2, 3 on note $C_n(P)$ le $\mathbb{F}_2$ espace vectoriel de base donné par l'ensemble de n-polytope de P

Exemple : - P $C_0(P) \ni 0, v_1, v_2, v_3, v_4, v_1+v_2, v_3+v_4, v_1+v_2+v_3+v_4...$

$C_{-1}(P) = \{0, \emptyset\}$

$C_3(P) = \{0, P\}$

Remarque : - 2. L'addition dans $C_n(P)$ est donné comme suit :

On additionne Les 2 sommes et on efface chaque éléments qui apparait 2 fois Par exemple $(v_1+v_2)+(v_2+v_3) = v_1+v_3$

- Pour σ un n-polytope on pose $\delta_n(\sigma) \in C_{n-1}(P)$ la somme des (n-1) polytope dans le bord de σ

Cela définit de manière unique une app linéaire $\delta_n : C_n(P) \to C_{n-1}(P)$
via $\delta_n(\sigma_1..\sigma_r) = \delta_n(\sigma_1) + .. + \delta_n(\sigma_r)$

Exemple : -

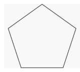
P polyèdre :

* $\delta_1 = v_1 + v_2 \in C_0(P)$
* $\delta_1 = \delta_1(\sigma_1) + \delta_2(\sigma_2) = (v_1+v_2) + (v_2+v_3) = v_1 + v_3$

$C_n(P) :=$ Le$\mathbb{F}_2$ epace-vectoriel $\{n-\text{polytope de P}\}$ n=-1,0,1,2,3 =$\{$somme de n-polytope de P$\}$

$\delta : C_n(P- \to C_{n-1}(P)$ est linéaire

Exemple : -

1) $\delta_0(v) = \emptyset$, $\forall$ sommets; $\delta_0(v_1 + v_2) = \delta_0(v_1) + \delta_0(v_2). = \emptyset\emptyset = 0 \in C_{-1}(P) = \mathbb{F}_2\emptyset$
2) $\delta_1(\sigma_1 + \sigma_2) = \sigma_1(\sigma_1) + \sigma_1(\sigma_2) = (v_1 + v_2) + (v_2 + v_3) = v_1 + v_3$
3) $\delta_1(\square) = 0$
4) $\delta_2(\sigma_1 + \sigma_2) =$ 

On a une suite : $0 \overset{\delta_4}{\to} C_3(P) \overset{\delta_3}{\to} C_2(P) \overset{\delta_2}{\to} C_1(P) \overset{\delta_1}{\to} C_0(P) \overset{\delta_0}{\to} C_{-1}(P) \to 0$ de dimension :
#3 polytope =1

Par le corrlaire II.2 : il reste a voir que la suite est exte et l'on aura : $\begin{cases} 0 = 1 - F + A - S + 1 \\ \Leftrightarrow S - A + F = 2 \end{cases}$

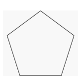
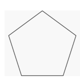
Preuve de l'exactitude : - ($\Rightarrow$ Théoreme III.2)

Notons tout d'abord que$\forall$non a $\delta_{n-1} \circ \delta_n = 0$ Cela implique $\boxed{IM(\delta_N) \subset Ker(\delta_{n-1}) \quad \forall n}$

En effet : si $x \in Im(\delta_n)$; $\exists y$ tq $x = \delta_n(y) \Rightarrow \delta_{n-1}(x) = \delta_{n-1}(\delta_n(y)) = (\delta_{n-1} \circ \delta_n)(y) = 0$
$\Rightarrow x \in Ker(\delta_{n-1}$

Verifion que ; $\delta_{n-1} \circ \delta_n = 0 \quad \forall n$
Il suffit de le voir pour tous les éléments dans la base

— $\delta_0(\delta_1(—) = \delta_0(v_1 + v_2) = \emptyset + \emptyset = 0$ ✓

— $\delta_1(\delta_2($  $) = \delta_1($  $) = 0$ ✓

— $\delta_2(\delta_3(P)) = \delta_2($ somme de toute les faces$) = 2\cdot$ chaque arrete $= 0$

<u>reste a voir</u> : $\boxed{Ker(\delta_{n-1} \subset Im(\delta_n) \quad \forall n}$

• $Ker(\delta_{-1} = C_{-1} = \mathbb{F}_2\emptyset = \{0, \emptyset\} \subset Im(\delta_0)$: ok car $\delta_0(v) = \emptyset$ pour tout sommet v
Donc ça marche car P contient au moin au sommet

• $Ker(\delta_0) \subset Im(\delta_1)$ $\begin{cases} Ker(\delta_0) = \textit{somme d'un nombre pair de sommet} \\ Im(\delta_1) = \textit{bord d'une famille d'arretes} \end{cases}$
Cette notation dite; $\forall v_1, v_2$ sommet il exite un chemin formé d'arrete qui joint v_1 a v_2
C'est une conséquence des points (ii) et (iii) dans la définiton de Mobius

• $Ker(\delta_1) \subset IM(\delta_2) \Leftrightarrow$ *toute boucle formé d'arrete boucle une collection de faces : c'est l'hypothèse du Th !*

• $Ker(\delta_2) \subset Im(\delta_3) = \{0, \textit{somme de toute les face}\}$: cela découle de la condition (iii)

$Ker(\delta_3) \subset Im(\delta_4) = 0 \Leftrightarrow \delta_3$ inj $\Leftrightarrow \delta_3(P) \neq 0$ clair $\square$

3.4 Modules : axiomes et exemple :

Définition : - Soit A un anneau. Un ensemble M muni d'une loi + : $\begin{array}{ll} M \times M & \to M \\ (x,y) & \to x+y \end{array}$

et d'une loi : $\begin{array}{ll} A \times M & \to M \\ (a,x) & \to a \cdot x = ax \end{array}$

(M1)	(M,+) est un groupe abélien
(M2)	a(bx) = (ab) x
(M3)	(a+b)x = ax+bx
(M4)	a(x+y) = ax+ay
(M5)	$1_A \cdot x = x$

Exemples : -

1) Si A = K est un corps, alors un A-module coïncident avec un K-espace vectoriel
⇒ Les modules généralisent les espaces-vectoriels

2) Si A=ℤ alors les ℤ modules coïncident avec les groupes abéliens.
En effet un ℤ moduules est un groupe abélien par (M1)
Réciproquement soit (G,+) un groupe abélien

Il est muni de la loi $\mathbb{Z} \times G \to G$

$$\text{ou } nx := \begin{cases} \overbrace{x + .. + x}^{n} & \text{si } n > 0 \\ 0 & \text{si } n = 0 \\ \underbrace{(-x) + ... + (-x)}_{|n|} & \text{si } n < 0 \end{cases}$$

Et les axiomes sont vérifier :
(M2) : $n \cdot (m \cdot x) = (nm)x$
(M3) : (n+m)x=nx+mx
(M4 : n(x+y) = nx+ny
(M5) : 1x = x par def

Ainsi Les modules génerlaisent les groupes abéliens!

3) Théoreme A est un A-modules ((M1)=(A1), (M2)-(M5) ⇔ (A2)-(A4))
Ainsi les modules généralisnet aussi les anneaux

4) Soit E un espace vectoriel et f :E → E un endomorphisme.
Cela définit une structure de K[X]-module sur E via :

$$P = \sum_{i=1}^{n} \lambda_i X^i \in K[X] \quad \Rightarrow \boxed{P \cdot V := \sum_{i=0}^{n} \lambda_i f^i(v)} \quad \text{ou } f^i := \overbrace{f \circ ..f \circ}^{i}$$

(M1) o, car E espace vectoriel ; (M2) ok par def de PQ ; (M3) Ok par def de P+Q ; (M4) par linéarité de f ; (M5) par def

On obtient donc K[X]-module qui dépend de f on le notera E_f

Reciproquement si M est un module sur K[X] alors M est un K espace vectoriel (restriction de la loi externe a K⊂ K[X]*) et l'application*

f :M→ M f(x) = Xx est linéaire

$$f(x+y) = X(x+y) = Xx+Xy = f(x)+f(y)$$
$$f(\lambda x) = X(\lambda x) = (X\lambda)x = (\lambda X)x = \lambda(Xx) = \lambda f(x)$$

Ainsi les modules généralisent aussi les espaces vectoriels munis d'un endomorphisme !

5) Si $M_1//M_n$sont des A-module alors $M_1 \times .. \times M_n$ est aussi un A-module via :
$(x_1..x_n) + (y_1..y_n) := (x_1 + y_1..x_n + y_n)$
ou $x_iy_i \in M_i \quad \forall i$ $a(x_1..x_n) = (ax_1..ax_n)$ et $a\in A$
Le resultat est noté $M_1 \oplus .. \oplus M_n$est la somme directe de $M_1..M_n$

Remarque : - Comme pour les espaces vectoreile les "regel de calcul" suivantes avec les même preuve :

(i) $O_A \cdot x = O_M \quad \forall x \in M \quad a \cdot O_M = O_M \quad \forall a \in A$

(ii) $(-a)\ x= a(-x) =-(ax) \quad \forall a \in A \quad \forall x \in M$

En revanche l'égalité $a \cdot x = O_M$ avec $a \in A$ $x\in M$ n'implique pas $a= O_A$ ou $x = O_M$

Par exmeple prenons $A=\mathbb{Z}$ et $M= \mathbb{Z}\backslash 2\mathbb{Z}$:
soit $a =2 \in \mathbb{Z}$, $x=[i] \in \mathbb{Z}\backslash 2\mathbb{Z}$ on a $a\neq 0$ $x\neq 0$; mais $a\cdot x = 2 \cdot [i] = [i] + [i] = [0] = 0\mathbb{Z}\backslash 2\mathbb{Z}$

Terminologie : - Un sous-ensemble $N\neq \emptyset$ d'un A module M est un sous-module de M si :

$x,y \in N \Rightarrow x + y \in N;$ et $x \in N a \in A \Rightarrow ax \in N$

Exemple : -

1) Si A=K est un corps c'est la rotation de sous-espace vectoriel

2) Si $A=\mathbb{Z}$ un sous $\mathbb{Z}$-module est un sous-groupe abélien facile

3) Soit A un anneau du module du A-module M=A est un idéal de A

4) Soit E un K-espace vectoriel et $f\in End(E)$
Cela défini une structure de K[X]-module sur E noté Ef. Un sous-module du K[X]-module Ef est un sous-espace $F\subset E$ <u>stable</u> par f ; ie : tel que $f(F)\subset F$

$$F \subset Ef \text{ sous-module} \iff (x,y \in F \Rightarrow x + y \in F \text{ et } x \in F,\ P \in K[X] \ \Rightarrow P \cdot x \in F)$$
$$\Leftrightarrow (x, y \in F \implies x + y \in F; \quad x \in F \implies \lambda \cdot x \in F \quad \forall \lambda \in K \text{ et } X \cdot x \in F$$
$$\Leftrightarrow F\subset E \text{ est un sous-esapce vectoriel et } x\in F \implies X \cdot x = f(x) \in F$$
$$\Leftrightarrow F\subset E \text{ est un sous-espce vectoriel tq } f(F) \subset F$$

5) Si $M_1M_2 \subset M$sont deux sous-ensemble de M, alors $M_1 + M_2 := \{x_1 + X_2 \mid x_i \in M_i\}$ est aussi un sous-module de M

Définition : -

Une application $\varphi : M \to M'$ entre deux module sur A est un homomorphisme de A-module (ou application A-linéaire) si :

$$\boxed{\varphi(x + y) = \varphi(x) + \varphi(y) \qquad \forall x, y \in M; \quad \varphi(a \cdot x) = a \cdot \varphi(x) \begin{cases} \forall a \in A \\ \forall x \in M \end{cases}}$$

Exemple : -

1) Si A=K est corps, c'est la notation d'applciation linéaire

2) Si A=$\mathbb{Z}$ une application $\mathbb{Z}$-linéaire est un homomorphisme de groupe (abéline)

$(\varphi(x+y)=\varphi(x)+\varphi(y) \iff$ homo de groupe et $\varphi(n\cdot x)=\varphi(\overbrace{x+..+x}^{n})=\overbrace{\varphi(x)+...+\varphi(x)}^{n}=n\cdot\varphi(x)$ si $n>0)$

3) Si A=K[X] : soient $E_f, E'_{f'}$ deux $K[X]-$module (avec $f\in End(E)$ $f'\in End(E')$)
Une application $\varphi : E_f \to E'_{f'}$ est $K[X]-$linaire $\iff \varphi$ est K-linéaire et $\varphi\circ f = f'\circ\varphi$

$$\begin{array}{ccc} E & \xrightarrow{f} & E \\ \varphi\downarrow & & \downarrow\varphi \\ E' & \xrightarrow{f'} & E' \end{array}$$

(comme ci-dessus φ est K[X]-linéaire $\iff \begin{cases}\varphi(x+y)=\varphi(x)+\varphi(y)\\ \varphi(\lambda\cdot x)=\lambda\varphi(x)\ \forall\lambda\in K\end{cases}$ et

$$\begin{cases}\varphi(X\cdot x)=X\varphi(x)=f'(\varphi(x)\\ \varphi(f(x)\ \forall x\in E\end{cases}$$

Remarque : - Si M est un A-module et N$\subset$ M un sous-module N est un sous-groupe (abélien) $\Longrightarrow$ on a un groupe abélien quotient pour la loi externe suivante :

$$a\in A[x]\in M/N \Longrightarrow a\cdot[x]:=[a\cdot x] \quad (\text{cf ex5 S}, 11)$$

Comme dans le cas des espaces vectoriel tout se genralise en particulier le Théoreme d'isomorphisme tout $\varphi : M\to M'$ application A-isomérie définit un isomorphisme

$\boxed{\overline{\varphi}\ M/Ker\varphi \to Im(\varphi)}$

FIN

3.5 Classification des modules de génération finie sue un anneau euclidien

Terminologie : - Un A-module M est somme directe (interne) de sous-module $M_1, ..., M_n$ si tout $x \in M$ s'écrit de maniere unique $x = x_1 + ... + x_n$; $x_i \in M_i \forall i$

Remrque : -

1) La prop III.1 s'étent verbatim $M \cong M_1 \oplus .. \oplus M_n$
2) M est somme directe de M_1 et M_2 $\iff$ $M = M_1 + M_2$ et $M_1 \cap M_2 = \{0\}$

Exemle : - Soit Ef un K[X] - module somme directe de $F_1..F_n \subset E_f$

On a donc $Ef \cong F_1 \oplus .. \oplus F_n$ comme K[X]-module Cela signifie :
1) $E \cong F_1 \oplus ... \oplus F_n$ comme K espace vectoriel $\varphi K[X]-$lin
2) $F_i \subset E_f$ sous K[X] module $\implies$ $f(F_i) \subset F_i$

Ainsi dans un base de la forme $S = S_1 \cup ... \cup S_n$ une matrice pour f sera :

$\begin{pmatrix} Ma_{f1} & 0 \\ 0 & Ma_{f_n} \end{pmatrix}$ ou $f_i = f|_{F_i} \in End(F_i)$

Terminologie : - Un A-module M est dit cyclique si : $\exists x_0 \in M$ tq $\forall x \in M$ $x = a \cdot x_0$ pour $a \in A$

Exemple : -

1) Un k-module cyclique est soit $M = \{0\}$ soit M=K
2) Un $\mathbb{Z}-$module cyclique est un groupe cyclique (ie : $\mathbb{Z}/ n\mathbb{Z}$)
3) M=A est un A-module cyclqie (prendre $x_0 = 1_A$). Plus généralement si I est un idéal de A A/I est un A-module cyclique
   (Posons $x_0 = [1_A]$. Tout $x \in A/I$ s'écrit $x = [a]$ par $a \in A$ et on a $x = [a] = [a \cdot 1_A] = a[1_A] = a \cdot x_0$)
   Pour A=K et $\mathbb{Z}$ on retrouve les exemple 1 et 2
   En fait tous les modules cyclique sont de cette forme

Proposition III.12 : - Soit A un anneau commutatif Alors si M est un A-module cyclique il existe un idél $I \subset A$ tq $M \cong A/I$

Preuve : - Soit M un A-module cyclique engendré par $x_0 \in M$

Posons $\varphi : A \to M$ $\varphi(A) = a \cdot x_0$; C'est une application linéaire :

- $\varphi(a + b) = (a + B) \cdot x_0 = a \cdot x_0 + b_0 \cdot x_0 = \varphi(a) + \varphi(b)$
- $\varphi(a \cdot b) = (a \cdot b) \cdot x_0 = a \cdot (b \cdot x_0) = a \cdot \varphi(b)$

De plus φ est un surjective car x_0 engendre M

Finalement Kerφ est un sous-module de A donc un idéal I car A commutatif; Par le théoreme d'isomorphisme on a un iso $\overline{\varphi} : A/I \to M$ $\square$

Corollaire III.13 : - Si A est euclidien tout A-module cyclique est isomorphe a $A/(x)$ pour un certain $x \in A$

Preuve : - découle de prop III.12 et prop II.10 $\square$

Terminologie : - Un A-module M est dit de génération finie s'il existe $x_1..x_n \in M$ tq tout $x \in M$ s'écrit ; $x = a_1x_1 + ... + a_nx_n$ avec $a_i \in A$

Exemple : -

1) Pour A=K un corps un K-espace vectoriel est de génération finie $\iff$ il est de dimension finie
2) Pour A= $\mathbb{Z}$ si un groupe abélien est finie alors il est de génération finie

Théoreme III.14 : -

Soit A un anneau euclidien. Tout A-module de génération finie est somme directe d'un nombre finie de sous-module cyclique

Théoreme II.15 : - Clasification de génération finie sur A euclidien

Soit A un anneau euclidien et M un A-module de génération finie. Alors il existe des entiers r,n ≥ 0 des éléments premier $p_1, ..., p_n$ (pas forcement distinct) et des entiers $\nu_1 ... \nu_n \geq 1$ tq

$$\boxed{M \cong A^r \oplus A/(p_1^{\nu_1}) \oplus ... \oplus A/(p_n^{\nu_n})}$$

Preuve : - Soit donc un M un A-module de génération finie
Par le Théoreme III.14 (A eculidien) il existe $M_1 ... M_n$ sous-module cyclique de M tq M$\cong$ $M_1 \oplus ... \oplus M_n$

Par Corrolaire III.13 (A euclidien) il existe $x_1 ... x_n \in A$ tq $M_i \cong A/(x_i) \forall i$

On a donc ; M$\cong$ $A/(x_1) \oplus ... \oplus A/(x_n)$

- si $x_i = 0$ on a ; $M_i \cong A/(0) = A$ qui contribue a A^r

- si $x_i \in A^*$ on a ; $M_i \cong A/A = \{0\}$ qui ne contribue pas

- si $x \in A$ $x \neq A^*$ $x \neq 0$ alors ; (par le théoreme II.15) A euclidien il existe des premier $p_1 ... p_n$ des entier $\mu_1 ... \mu_l \geq 1$ et $\mu \in A^*$ tq $x = \mu p_1^{\mu_1} ... p_l^{\mu_l}$

$\implies$ $A/(x) \quad = \quad A/(p_1^{\mu_1} ... p_l^{\mu_l}) \cong A/(p_1^{\mu_1}) \oplus ... \oplus A/(p_l^{\mu_l})$ par le th des reste chinois

(vu par l=2 mais le cas général est par induction)

(vu comme isomorphisme d'anneaux mais c'est trivialement un isomorphisme de A-module)