UNIVERSITE SIDI MOHAMED BEN ABDELLAH

FACULTE DES SCIENCES ET TECHNIQUES

DEPARTEMENT DE MATHEMATIOUES

LICENCE SCIENCES ET TECHNIQUES (LST)

CALCUL SCIENTIFIQUE ET APPLICATION (CSA)

MEMOIRE DE FIN D'ETUDES

Pour L'obtention Du Diplôme De Licence Sciences Et Techniques :

LES STRUCTURES ALGEBRIQUES

Présenté par :

MOHAMED EL KHATTABI

Sous la direction de :

PR.NAJIB MAHDOU (FSTF)

Soutenu le 12 juin 2013 devant le jury composé par :

Année Universitaire : 2012 /2013

FACULTE DES SCIENCES ET TECHNIQUES FES – SAISS
B.P. 2202 – Route d'Imouzzer – FES
212 (0)5 35 61 16 86 – Fax : 212 (0)5 35 60 82 14

Remerciement :

Je tiens à exprimer ma gratitude et présenter mes chaleureux remerciements à :

- *Mr. Najib Mahdou mon encadrant pour sa gentillesse et ses précieux conseils.*
- *Les membres du jury qui ont accepté d'évaluer ce travail.*
- *Toute personne ayant contribué de près ou de loin à l'élaboration de ce modeste travail.*

Dédicace :

Je dédie ce travail l'esprit de ma sœur Majda décédée le 6 /06/ 2009, à mes parents pour leur soutien et leur Sacrificatrices.

A Mes Sœurs Bouchra, Maria, et Naima.

A mes meilleurs amis : Al-Arabi Bayad, Brahim Lakrini, Arssalan Abdrafie , Farah Et Najwa Zineddine.

A tous mes amis qui m'ont accompagné pendant la durée de mes études.

Table des matières

CHAPITRE I : PRELIMINAIRES

1-Loi de composition interne :

Définition : Une loi de composition interne notée T sur un ensemble E est une application de $E \times E$ dans E.

$$E \times E \longrightarrow E$$

$$(x, y) \longrightarrow xTy$$

La notation (E, T) signifie que E est un ensemble muni de la loi de composition interne T.

Notation: Tout couple $(E,*)$ signifié que E est un ensemble et $*$ une loi de composition interne dans E.

2-Propriétés spéciales:

Assoc0iativité :

Définition : Soit $*$ une loi de composition interne dans E. La loi $*$ est dite associative si :

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

Exemple :

1) L'addition et la multiplication dans $\mathbb{N}$ ou $\mathbb{Z}$ sont associatives.

2) La réunion et l'intersection dans $\mathcal{P}(E)$ sont associative.

Commutativité :

Définition : Soit $*$ une loi de composition interne dans E. La loi $*$ est dite commutative si :

$$\forall\, a, b \in E\,, a * b = b * a$$

Exemple :

1) L'addition et la multiplication dans $\mathbb{N}$ sont commutatives.

2) La réunion et l'intersection dans $\mathcal{P}(E)$ sont commutatives.

3) La soustraction dans $\mathbb{C}$ n'est pas commutative.

Elément neutre :

Définition : Soit $*$ une loi de composition interne dans E.

On dit qu'un élément $e \in E$ est neutre pour la loi $*$ si : $\forall a \in E, a * e = e * a = a$

Alors on dit que le couple $(E,*)$ est unifère(ou bien unitaire).

Proposition : Si e et e' sont deux éléments neutres pour $*$ dans E, alors $e = e'$.

Preuve : Supposons que $*$ ait deux éléments neutres e et e' dans E.

Alors puisque e est l'élément neutre et $e' \in E, e' * e = e * e' = e'$.

Et puisque e' est l'élément neutre et $e \in E, e * e' = e' * e = e$.

Donc $e = e'$.donc l'élément neutre est unique.

Exemple :

1) L'addition dans $\mathbb{N}$ possède l'élément neutre 0. La multiplication a l'élément neutre 1.

2) La réunion dans $\mathcal{P}(E)$ a l'élément neutre $\emptyset$: $(\forall A \in \mathcal{P}(E), A \cup \emptyset = A)$.

3) L'intersection dans $\mathcal{P}(E)$ a l'élément neutre E : $(\forall\, A \in \mathcal{P}(E), A \cap E = A)$.

Extension :

Définition : Soient X un ensemble, $*$ une loi de composition interne dans E. On peut munir E^X d'une loi de composition interne noté $*$, définie par : $\forall\, f, g \in E^X, \forall x \in X, (f * g)(x) = f(x) * g(x)$.
Et appelée extension à E^X de la loi $*$ de E.

Exemple : Si $f, g: \mathbb{R} \longrightarrow \mathbb{R}$ alors $f + g: \mathbb{R} \xrightarrow[x \longmapsto f(x)+g(x)]{} \mathbb{R}$

Stabilité :

Définition : Soit $*$ une loi de composition interne dans E. Une partie A de E est dite stable pour $*$ si et seulement si, $A * A \subset A$ c.à.d. $\forall (x, y) \in A \times A, x * y \in A$.

Si A est une partie stable de E pour $*$, la loi de composition dans A définie par : $A \times A \xrightarrow[(x,y) \longmapsto x*y]{} A$ est appelée loi de composition interne induite sur A par $*$ de E, et encore notée $*$.

Loi produit :

Définition : On appelle produit de deux couples (E, T), $(F, \perp)$ le couple $(E \times F, *)$ tel que :

$\forall (x, y), (x', y') \in E \times F, \quad (x, y) * (x', y') = (x\, T\, x', y \perp y')$.

Exemple : $\mathbb{R}^2$, muni de la loi de composition interne $+$ définie par :

$\forall\, (x, y), (x', y') \in \mathbb{R}^2, \quad (x, y) + (x', y') = (x + x', y + y')$ est le produit du $(\mathbb{R}, +)$ par lui-même.

Eléments réguliers :

Définition : Soit $*$ une loi de composition interne dans E.

1) On dit qu'un élément $a \in E$ est régulier à gauche si : $\forall\, b, c \in E, a * b = a * c \Longrightarrow b = c$.
2) On dit que a est régulier à droite si : $\forall\, b, c \in E, b * a = c * a \Longrightarrow b = c$.
3) On dit que a est régulier pour $*$ si et seulement si a est régulier à gauche et à droite.

Exemple :

1) Tout nombre naturel est régulier pour l'addition : $\forall\, x \in \mathbb{N}, a + x = b + x \Longrightarrow a = b$.

2) Tout nombre naturel, sauf 0 est régulier pour la multiplication : $\forall\, x \in \mathbb{N}^*, ax = bx \Longrightarrow a = b$.

Elément symétriques :

Définition : Soit $*$ une loi de composition interne dans E admet un élément neutre.

1) On dit qu'un élément $a \in E$ est symétrisable à droite, s'il existe un élément a' de E tel que $a * a' = e$.
2) On dit qu'un élément $a \in E$ est symétrisable à gauche, s'il existe un élément a' de E tel que $a' * a = e$.
3) On dit que a est symétrisable s'il admet un même symétrique a' à droite et à gauche.

Proposition : Si $x_1, \ldots\ldots\ldots\ldots, x_n$ sont des élément inversible de $(E,\times)$, alors $x_1, \ldots\ldots\ldots\ldots, x_n$ est inversible d'inverse $x_n^{-1}, \ldots\ldots\ldots x_1^{-1}$.

Preuve : Comme $\times$ est associative,

$$(x_1, \ldots., x_n)(x_n^{-1}, \ldots\ldots.., x_1^{-1}) = (x_1, \ldots.., x_{n-1})(x_n x_n^{-1})(x_{n-1}^{-1}, \ldots., x_1^{-1})$$

$$\ldots$$

$$= x_1 x_1^{-1} = e$$

De même on a $(x_n^{-1}, \ldots\ldots.., x_1^{-1})(x_1, \ldots., x_n) = e$

D'où$(x_1, \ldots., x_n)^{-1} = (x_n^{-1}, \ldots\ldots.., x_1^{-1})$.

Proposition : Soit $*$ une loi de composition interne dans E. Si la loi $*$ est associative et E admet un élément neutre alors :

Tout élément symétrisable est régulier.

Preuve : Soient $*$ une loi associative dans E, et E admet un élément neutre et a un élément symétrisable de E. Donc $\exists\, a' \in E$.

Alors $\forall b, c \in E,\quad (b * a) = (c * a) \Longrightarrow (b * a) * a' = (c * a) * a'$

$$b * (a * a') = c * (a * a')$$

$$b * e = c * e \quad \text{donc} \quad b = c\ .$$

De même on montrer que a est régulier à gauche.

Notation : Si la loi est notée additivement, le symétrique d'un élément a se nomme l'opposé de a et se note $(-a)$. Si la notation est multiplicative, il se nomme l'inverse de a et se note a^{-1} .

Proposition : Soit $*$ une loi de composition interne dans E. Si la loi $*$ est associative et E admet un élément neutre. Tout élément dans E symétrisable admet un symétrique unique.

Preuve : Supposons que a ait deux symétriques $a' \; et \; a''$ dans $(E,*)$.

Alors $a' * a = a'' * a = e$, et comme a est régulier ,on obtient $a' = a''$.

Morphisme :

Définition : Soit $(G_1,*)$ et (G_2,T) . Un homomorphisme de G_1 dans G_2 est une application $f: G_1 \longrightarrow G_2$ tel que $\forall \, x,y \in G_1, \quad f(x * y) = f(x) \; T \; f(y)$.

Proposition :

1) Si $f: (E,*) \longrightarrow (F,T)$ et $g: (F,T) \longrightarrow (G,\perp)$ sont deux morphismes, alors $g \circ f: E \longrightarrow G$ est un morphisme de $(E,*)$ dans $(G,\perp)$.

2) Pour tout $(E,*), Id_E: E \underset{x \longrightarrow x}{\longrightarrow} E$ est un automorphisme de $(E,*)$.

3) Si l'application $f: (E,*) \longrightarrow (F,T)$ est un isomorphisme, alors $f^{-1}: F \longrightarrow E$ est un isomorphisme du (F,T) dans $(E,*)$.

Preuve :

1) $\forall \, x,y \in E, (g \circ f)(x * y) = g\big(f(x) \; T \; f(y)\big) = (g \circ f)(x) \perp (g \circ f)(y)$.

2) Evident.

3) Puisque f est bijective, l'application réciproque $f^{-1}: F \longrightarrow E$ existe, et on a,

$\forall \, x,y \in F: xTy = f\big(f^{-1}(x)\big)Tf\big(f^{-1}(y)\big) = f(f^{-1}(x) * f^{-1}(y))$.

D'où $f^{-1}(xTy) = f^{-1}(x) * f^{-1}(y)$

2-Groupe:

Définition :

1) Soit G un ensemble muni d'une loi de composition interne $*$. On dit que cette loi détermine sur G une structure de groupe ou que G est un groupe si les trois axiomes suivantes sont vérifiés :
   - i) La loi $*$ est associative. C.à.d. que,$\forall \, x,y,z \in G, (x * y) * z = x * (y * z)$.
   - ii) La loi $*$ admet un élément neutre.
     C'est-à-dire. $\exists \; e \in G \; tel \; que \; \forall \, x \in G, x * e = e * x = x$
   - iii) Tout élément $x \in G$ admet un symétrique $x' \in G \; pour \; la \; loi \; *$.
     C à d $\forall \, x \in G, \exists \, x' \in G \; tel \; que \; x * x' = x' * x = e$.
2) Si de plus, la loi $*$ est commutative c.à.d. $\forall \, x,y \in G, x * y = y * x$, On dit que le groupe $(G,*)$ est commutatif ou abélien.

Exemple :

$(\mathbb{Z},+)$, $(\mathbb{R},+) \; et \; (\mathbb{C},+)$ Sont des groupes commutatifs.

$(\mathbb{C}^*,\times), (\mathbb{R}^*,\times) \; et \; (\mathbb{Q}^*,\times)$ Sont des groupes commutatifs.

Conséquences : Soit $(G,*)$ un groupe, alors :

Tout élément de G est régulier à gauche et à droite pour la loi $*$.

c à d que $\forall\, a \in G, \forall\, x, y \in G$:

$$\begin{cases} a * x = a * y \Longrightarrow \ x = y \\ x * a = y * a \Longrightarrow \ x = y \end{cases}$$

Preuve :

$\forall\, x, y, z \in G$

$$x * y = x * z \Longrightarrow x^{-1} * (x\ * y) = x^{-1} * (x * z)$$
$$\Longrightarrow (x^{-1} * x) * y = (x^{-1} * x) * z \Longrightarrow y = z.$$

De même pour $y * x = z * x$.

3-Morphismes de groupes :

Définition : Soient $(G_1,*)$ et (G_2,T) deux groupes. Un homomorphisme de $G_1\ dans\ G_2$ est une application $f: G_1 \longrightarrow\ G_2, tel\ que\ f(x * y) = f(x)\ T\ f(y)$

- ✓ Si de plus f est bijective, on dit que f est un isomorphisme de $G_1\ dans\ G_2$ ou que $G_1\ et\ G_2$ sont isomorphe et on note $G_1 \simeq G_2$.
- ✓ Un endomorphisme du groupe G_1 est un homomorphisme de G_1 dans lui-même.
- ✓ Un automorphisme de G_1 est un isomorphisme de G_1 sur lui-même.

Exemple : La fonction exponentielle est un homomorphisme du groupe $(\mathbb{R}, +)$ dans le groupe $(\mathbb{R}^*, \times)$

Car $e^{x+y} = e^x \times e^y$

Proposition : Soient $(G_1,*)$ et (G_2,T) deux groupes d'éléments neutres respectifs $e_1\ et\ e_2$ et soit $f: G_1 \longrightarrow G_2$ Un homomorphisme, alors :

1) $f(e_1) = e_2$
2) $\forall\, x \in G_1, \quad f(x^{-1}) = (f(x))^{-1}$

Preuve :

1) $f(e_1)\ T\ f(e_1) = f(e_1 * e_1) = f(e_1) = f(e_1)\ T\ e_2$
   D'où $f(e_1) = e_2\ car\ f(e_1)\ est\ régulier.$
2) $\begin{cases} f(x)\ T\ f(x^{-1}) = f(x * x^{-1}) = f(e_1) = e_2 \\ f(x^{-1})\ T\ f(x) = f(x^{-1} * x) = f(e_1) = e_2 \end{cases}$ $\Longrightarrow$ D'où $f(x^{-1}) = (f(x))^{-1}$

Définition : Soient $(G_1,*)$ et (G_2,T) deux groupes et f un homomorphisme de G_1 dans G_2 tel que, $f: G_1 \longrightarrow G_2$. Si e_2 désigne l'élément neutre du groupe (G_2,T) :

- ❖ Le noyau de f notée $\ker f$ est donné par :

$$\ker f = \{\, x \in G_1 \,/\ f(x) = e_2\} = f^{-1}(\{e_2\})$$

❖ L'image de f notée $Im\ f$ est donnée par :

$$Im\ f = \{f(x)\ \ /\ \ x \in G_1\}$$

Proposition : Soit f un homomorphisme du groupe$(G_1,*)\ \ dans\ (G_2,T)$.

Alors si $f\ \ est\ injective \iff \ker f = \{e_1\}$. Où e_1 est l'élément neutre du groupe G_1.

Preuve : (⇒) Supposons que f est injective, et soit $x \in \ker f$.

$f(x) = e_2 = f(e_1)$, d'où puisque f est injective : $x = e_1. Ainsi: \ker f = \{e_1\}$

(⇐)Supposons que $\ker f = \{e_1\}$. Soient $x, y \in G_1,\ tel\ que\ \ f(x) = f(y)$

Donc $f(x)\ T\ (f(y))^{-1} = e_2$

C.à.d. que $(x * y^{-1}) = e_2 = f(e_1) \implies x * y^{-1} \in \ker f$.

$Car\ f\ est\ un\ morphisme$, est par conséquent $x * y^{-1} = e_1$

D'où $x = y \implies f\ est\ injectif$.

Proposition :*(Transfert De La Structure De Groupe*)

Soient$(G,*)$ un groupe, T une loi de composition interne sur E((E,T)) . S'il existe un isomorphisme de $(G,*)$ sur (E,T) . Alors (E,T) est un groupe isomorphe au groupe $(G,*)$ et on note $G \simeq E$.

Preuve : Supposons qu'il existe un isomorphisme de $f: (G,*) \longrightarrow (E,T)$. $(e\ le\ neutre\ de\ G)$

Soient $x, y, z \in E,\ \ X = f^{-1}(x),\quad Y = f^{-1}(y),\ \ Z = f^{-1}(z)$

1) $(x\ T\ y)\ T\ z = \big(f(X)\ T\ f(Y)\big)\ T\ f(Z) = f(X * Y)\ T\ f(Z)$

$= f\big((X * Y) * Z\big) = f(X * (Y * Z))$

$= f(X)\ T\ f(Y * Z) = f(X)\ T\ (f(Y)\ T\ f(Z))$

$= x\ T\ (y\ T\ z). Donc\ T\ est\ associative\ dans\ E.$

2) $\begin{cases} x\ T\ f(e) = f(X)\ T\ f(e) = f(X * e) = f(X) = x \\ f(e)\ T\ x = f(e)\ T\ f(X) = f(e * X) = f(X) = x \end{cases}$ $\quad Donc\ f(e)\ est\ neutre\ pour\ T\ dans\ E.$

3) $\begin{cases} x\ T\ f(X^{-1}) = f(X)\ T\ f(X^{-1}) = f(X * X^{-1}) = f(e) \\ f(X^{-1})\ T\ x = f(X^{-1})\ T\ f(X) = f(X^{-1} * X) = f(e) \end{cases}$

$$Donc\ x\ admet\ un\ symétrique\ \ pour\ T\ dans\ E.$$

4-Groupe produit :

Définition : Le groupe $G \times G'$ est appelé le produit direct de groupe G par G'.

Proposition : Soit $(G,*)$ un groupe d'élément neutre e.

On définit une loi $*$ sur $G \times G$ on posant :$(a,b) * (c,d) = (a * c, b * d)$.

Muni de cette loi, $G \times G$ est un groupe :

- Le neutre est (e,e).
- L'inverse de (a,b) est (a^{-1}, b^{-1}).

Preuve : Soient $a,b,c,d,x,y \in G$,

Alors $((a,b) * (c,d)) * (x,y) = (a * c, b * d) * (x,y)$

$$=\big((a * c) * x, (b * d) * y\big)$$

$$=\big(a * (c * x), b * (d * y)\big) = (a,b) * (c * x, d * y)$$

$$=(a,b) * \big((c,d) * (x,y)\big)$$

D'où la loi $*$ est associative.

Cette loi admet (e,e) comme un élément neutre et pour tout $(a,b) \in \mathrm{G} \times \mathrm{G}$, l'inverse de

$(a,b)\ \ est\ (a^{-1}, b^{-1})$. Donc $G \times G$ est un groupe.

5-Ordre d'un groupe fini :

Définition : On dit qu'un groupe $(G,*)$ est fini si le cardinal de l'ensemble G est fini

Exemple : $((\mathbb{Z}/7\mathbb{Z})^*, \times)$ est un groupe fini son cardinal est 6.

Définition : Soit $(G,*)$ un groupe fini, le cardinal de l'ensemble G est appelé l'ordre du groupe et on le note $ord(G)$.

Exemple : $((\mathbb{Z}/4\mathbb{Z}), +)$ est un groupe fini d'ordre 4.

6-Sous –groupe :

Définition : Soient $(G,*)$ un groupe, et H une partie de G. On dit que H est un sous-groupe de $(G,*)$ si et seulement si :

i) $\forall x,y \in H, \quad x*y \in H \ (H \text{ est stable pour la loi } *)$
ii) $e \in H \qquad (e \text{ le neutre de } G)$
iii) $\forall x \in H, \ on\ a, \quad x^{-1} \in H. (x^{-1} \text{ le symétrique de } x \text{ dans } G)$

Proposition : Soit $(G,.)$ un groupe d'élément neutre e . Pour qu'une partie H de G soit un sous-groupe de G, il faut et il suffit que :

i) $H \neq \emptyset$.
ii) $\forall x,y \in H, \qquad xy^{-1} \in H.$

Preuve :

La condition nécessaire : si H est un sous-groupe, l'inverse $y^{-1}\ de\ y$ et le produit $xy^{-1}\ de\ x\ et\ de\ y^{-1}$ appartiennent à H.

La condition est aussi suffisante :

On a $x \in H \implies xx^{-1} = e \in H$

$x \in H \implies (e,x) \in H^2 \implies ex^{-1} = x^{-1} \in H$

$x,y \in H \implies (x,y^{-1}) \in H^2 \implies x(y^{-1})^{-1} = xy \in H$

C.à.d. que H est stable pour la loi produite .

D'où $(H,.)$ est un sous groupe G.

Proposition : Soit $(G,*)$ un groupe. $(H_i)_{i\in I}$ une famille de sous-groupe de G.
Alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.

Preuve : Soit $H = \bigcap_{i\in I} H_i$

1) $\forall x,y \in G, \forall x,y \in H \implies (\forall i \in I, x \in H_i \ et\ y \in H_i) \implies (\forall i \in I, x*y \in H_i) \implies x*y \in H$
2) $(\forall\ i \in I, e \in H_i), alors\ e \in H$
3) $\forall x \in G\ , x \in H \implies (\forall i \in I, x \in H_i) \implies (\forall\ i \in I, x^{-1} \in H_i) \implies x^{-1} \in H.$

Définition : Soit $(G,*)$ un groupe. A une partie de G, l'intersection de tous les sous-groupes de G contenant A est un sous-groupe de G . Appelé sous-groupe engendré par A et noté $< A >$.

Ainsi $< A >= \bigcap_{H\ s.g\ de\ G, A\subset H} H$ et $\forall\ a \in G$ on peut noter $< a>$ au lieu $< \{\ a\} >$.

Proposition : Soient $(G,*)$ un groupe, A une partie de G. $< A >$ est le plus petit sous-groupe de G contenant A.

Preuve : On a $< A >= \bigcap_{H.s,g\ de\ G, A \subset H} H$

Donc d'après la proposition précédente $< A >$ est un sous-groupe de G contenant A.

D'autre part, soit H un sous-groupe de G contenant . Par définition de $< A >$, on a : $< A > \subset H$

Ainsi $< A >$ est inclus dans tout sous-groupe de G contenant A.

Donc $< A >$ est le plus petit sous-groupe de G contenant A.

Théorème : Le noyau d'un morphisme $f: (G_1, *) \longrightarrow (G_2, T)$ de groupes est un sous-groupe de G_1.

Preuve : $\forall\ x, y \in \ker f$

$f(x * y^{-1}) = f(x)\ T\ f(y^{-1}) = f(x)\ T\ (f(y))^{-1} = e_1 T e_1 = e_1$. Donc $x * y^{-1} \in \ker f$.

Et puisque $e_1 \in \ker f$ donc $\ker f \neq \emptyset$ et $\forall\ x, y \in \ker f \implies x * y^{-1} \in \ker f$.

Alors $\ker f$ est un sous-groupe de G_1.

Proposition : L'image d'un morphisme $f: A \longrightarrow B$ de groupes est un sous-groupe de B

Tel que : $Im\ f = \{b \in B, \exists a \in A\ tel\ que\ f(a) = b\}$.

Preuve : Soit $a \in A$, alors $f(a) = f(0_A + a) = f(0_A) + f(a)$

Donc $f(a) - f(a) = f(0_A) + f(a) - f(a) \Longrightarrow 0_B = f(0_A)$.

Soient $b_1, b_2 \in Im\ f$ et $a_1, a_2 \in A$ avec $f(a_1) = b_1\ , f(a_2) = b_2$

Alors $b_1 - b_2 = f(a_1) - f(a_2) = f(a_1 - a_2) \in Imf$.

Donc Imf est un sous groupe de B.

Définition :

1) On dit qu'une partie A d'un sous-groupe de G est un ensemble ou système de générateur de G ou que G est engendre par A, si $< A >= G$.
2) Un groupe monogène G est un groupe engendré par un seul élément.
   C'est-à-dire $\exists\ x \in G, tel\ que\ G =< x >$. Si de plus $|G|$ est fini, on dit que G est un groupe cyclique.

Notation :

Soit H un sous-groupe de G. On dit que x est congru à y modulo H et on note :

$x \equiv y\ (H)\ si\ xH = yH$. On note par $\bar{x} = xH = Hx = la\ classe\ de\ x\ modulo\ H$. Notamment, toute intersection de sous-groupe de G est un sous-groupe de G.

7-Groupe Quotient :

Théorème : Soit H un sous-groupe de G . L'ensemble quotient $G\ /\ H$ est un groupe pour la loi $(\bar{x},\bar{y}) \longrightarrow \overline{xy}, \bar{z}$ désignant la classe d'un élément z de G.

Preuve :

1) la correspondance : $(G/H)^2 \xrightarrow[(\overline{x},\overline{y})\to\overline{xy}]{} G/H$ est bien une application.

Soient $x' et\ y'$ tels que $x' \equiv x(H)\ et\ y' \equiv y(H)$

Donc $x' \equiv x(H) \Longrightarrow x'x^{-1} \in H$

$$\Longrightarrow x'y'y'^{-1}x^{-1} \in H$$
$$\Longrightarrow x'y'(xy')^{-1} \in H$$
$$\Longrightarrow x'y' \equiv xy'(H).$$

De même on a : $y' \equiv y(H) \Longrightarrow y'y^{-1} \in H$

$$\Longrightarrow y'xx^{-1}y^{-1} \in H$$

$$\Longrightarrow y'x(yx)^{-1} \in H$$

$$\Longrightarrow y'x \equiv yx(H) \Longrightarrow xy' \equiv xy(H).$$

D'où on a : $x'y' \equiv xy(H)$ c'est-à-dire que : $\overline{x'y'} = \overline{xy}$.

2) L'associativité : Si $\overline{z}$ est une troisième classe, on a :

$\overline{x}(\overline{y}\,\overline{z}) = \overline{x}(\overline{yz}) = \overline{x(yz)} = \overline{(xy)z} = (\overline{xy})\overline{z} = (\overline{x}\,\overline{y})\overline{z}.$

L'élément neutre est $\overline{1} \in H$. L'inverse de la classe de x est la classe de x^{-1}.

CHAPITRE II : ANNEAUX

1-Distributivité :

1) On dit que la loi $*$ est distributive à gauche pour la loi T si :

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

2) On dit que la loi $*$ est distributive à droite pour la loi T si : $(b\ T\ c) * a = (b * a) T (c * a)$.

3) On dit que T est distributive sur $*$ si et seulement si T est distributive à gauche et à droite sur $*$.

Exemple :

1) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

2) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Définition :

1) On dit qu'un ensemble A muni de deux lois de compositions internes notée $+ et\ \times$ est un anneau si :
   - i) $(A, +)$ est un groupe commutatif.
   - ii) La loi $\times$ est associative. C.à.d. que : $\forall\, x,y,z \in A, on\ a: x \times (y \times z) = (x \times y) \times z$
   - iii) La loi $\times$ admet un élément neutre noté 1. (Dans ce cas on dit que A est un anneau unitaire)
   - iv) La loi $\times$ est distributive par rapport à la loi $+$. C à d que :

     $$\forall\, x,y,z \in A\ on\ a \begin{cases} x \times (y+z) = x \times y + x \times z \\ (x+y) \times z = x \times z + y \times z \end{cases}$$

2) On dit que l'anneau $(A, +, \times)$ est commutatif si de plus la loi $\times$ est commutative.

Exemple :

1) $(\mathbb{Z}, +, \times), (\mathbb{R}, +, \times)\ et\ (\mathbb{C}, +, \times)$ sont des anneaux commutatifs et unitaires.
2) Soit $(A, +, \times)$ un anneau et E un ensemble. Alors l'ensemble $F(E, A)$ des applications de $E \longrightarrow A$ muni des deux lois :

$$(f,g) \longrightarrow f+g \qquad (f,g) \longrightarrow f \times g$$

$$x \longrightarrow f(x) + g(x) \qquad x \longrightarrow f(x) \times g(x)$$

Est un anneau unitaire.

2-Anneau produit:

Définition : Soient $(A, +, \times)$ et $(A', +, \times)$ deux anneaux. On définit des lois $+ et \times\ \ sur\ A \times A'$ en posant :

$\forall\, a,b \in A;\ \forall\, c,d \in A'$

- $(a,b) + (c,d) = (a+c, b+d)$.

- $(a,b)\times(c,d)=(a\times c,b\times d)$.

3-Règles de calcul dans un anneau:

Soit $(A,+,\times)$ un anneau.
On note : 0 est l'élément neutre pour $+, et\ 1$ le neutre pour $\times$.

$\forall\,(a,b,c)\in A^3$ On a:

1) $a\times 0=0\times a=0$ (0 est absorbant pour la multiplication)
2) $(-1)\times a=a\times(-1)=-a$
3) $\begin{cases}(-a)\times b=a\times(-b)=-ab\\(-a)\times(-b)=a\times b=ab\end{cases}$
4) $\begin{cases}(a-b)\times c=a\times c-b\times c\\c\times(a-b)=c\times a-c\times b\end{cases}$
5) $\forall\, n\in\mathbb{N}^*\ (1-a)\sum_{k=0}^{n-1}a^k=(\sum_{k=0}^{n-1}a^k)(1-a)=1-a^n$
6) $(1+a)\sum_{k=0}^{2p}(-1)^k a^k=(\sum_{k=0}^{2p}(-1)^k a^k)(1+a)=1+a^{2p+1}$
7) $\forall\, n\ \in\ \mathbb{N}^*\ \forall\,(x_1,\dots,x_n)\in A^n$
$$\sum_{i=1}^{n}a\,x_i=a\sum_{i=1}^{n}x_i$$
$$\sum_{i=1}^{n}x_i a=(\sum_{i=1}^{n}x_i)a$$
8) $\forall\, n,p\in\mathbb{N}^*,\forall\,(x_1,\dots\dots.,x_n)\in A^n,\forall\big(y_1,\dots\dots,y_p\big)\in A^p.$
$$\sum_{i=1}^{n}(\sum_{j=1}^{p}x_i y_j)=\sum_{j=1}^{p}\big(x_i y_j\big)=(\sum_{i=1}^{n}x_i)(\sum_{j=1}^{p}y_j)$$
9) $a^{n+1}-b^{n+1}=(a-b)\sum_{k=0}^{n}a^{n-k}b^k$

Proposition :(*FORMULE DU BINOME DE NEWTON*)

Soit $(A,+,\times)$ un anneau. $n\in\mathbb{N}, x,y\in A\ tel\ que\ x\times y=y\times x.$

On a: $(x+y)^n=\sum_{k=0}^{n}c_n^k x^k y^{n-k}$

Où par convention $x^0=y^0=1_A$.

Preuve :(*Par récurrence*)

Pour $n=0\ la\ formule\ est\ vraie$

Supposons la formule est vraie pour n , et montrons que la formule est vraie pour $n+1$.

$On\ a\ (x+y)^{n+1}=(x+y)^n(x+y)$

$=(\sum_{k=0}^{n}c_n^k x^k y^{n-k})\,(x+y)$

$=(\sum_{k=0}^{n}c_n^k x^k y^{n-k})x+(\sum_{k=0}^{n}c_n^k x^k y^{n-k})y$

$=\sum_{k=0}^{n}c_n^k x^{k+1}y^{n-k}+\sum_{k=0}^{n}c_n^k x^k y^{n+1-k}$

$$= \sum_{k=1}^{n+1} c_n^{k-1} x^k y^{n+1-k} + \sum_{k=0}^{n} c_n^k x^k y^{n+1-k} \quad (avec\ k = k+1)$$

$$= x^{n+1} + \sum_{k=1}^{n} c_n^{k-1} x^k y^{n+1-k} + y^{n+1} + \sum_{k=1}^{n} c_n^k x^k y^{n+1-k}$$

$$= c_{n+1}^{n+1} x^{n+1} y^{(n+1)-(n+1)} + c_{n+1}^{0} x^0 y^{(n+1)} + \sum_{k=1}^{n} (c_n^{k-1} + c_n^k) x^k y^{n+1-k}$$

$$= \sum_{k=0}^{n+1} c_{n+1}^k x^k y^{n+1-k} \quad (\ avec\ c_n^k = c_{n-1}^k + c_{n-1}^{k-1})$$

4-SOUS –ANNEUX ET IDEAUX :

4-1-Sous-anneau :

Définition : Soient $(A, +, \times)$ un anneau, B une partie de A. On dit que B est un sous-anneau de$(A, +, \times)$ si et seulement si :

- Muni des lois induites $(B, +, \times)$ possède lui-même une structure d'anneau.

Exemple :

1) $(\mathbb{Z}, +, \times)$ est un sous-anneau de l'anneau $(\mathbb{Q}, +, \times)$
2) $(\mathbb{Q}, +, \times)$ est un sous-anneau de $(\mathbb{R}, +, \times)$

Proposition :(*Caractéristique d'un sous-anneau*)

Soient $(A, +, \times)$ un anneau, B une partie de A. Pour que B soit un sous-anneau de A, il faut et il suffit que :

- ✓ $1_A \in B$.
- ✓ $\forall (a, b) \in B^2, \quad a - b \in B$
- ✓ $\forall (a, b) \in B^2, \quad ab \in B$

Exemple : Le seul sous-anneau de $(\mathbb{Z}, +, \times)\ est\ (\mathbb{Z}, +, \times)$ lui-même.

Proposition : Soit $(A, +, \times)$ un anneau. Soit $(B_i)_{i \in I}$ une famille non vide de sous-anneaux de A, alors $\bigcap_{i \in I} B_i$ est un sous-anneau de A.

Preuve : $\forall\ i \in I$, B_i est un sous-groupe de A donc $\bigcap_{i \in I} B_i$ est un sous-groupe de A.

Stable par multiplication

$$x, y \in \bigcap_{i \in I} B_i \Leftrightarrow \forall i \in I, x \in B_i\ et\ y \in B_i$$

$$\Longrightarrow \forall i \in I, x \times y \in B_i$$

$$\Longrightarrow x \times y \in \bigcap_{i \in I} B_i$$

$\forall\ i \in I,\ 1_A \in I$ donc $1_A \in \bigcap_{i \in I} B_i$.

4-2-IDEAUX :

Définition : Soit $(A,+,\times)$ un anneau commutatif. Soit I une partie de A .
On dit que I est un idéal de A si :

- $(I,+)$ est un sous-groupe de $(A,+)$.
- $\forall x \in I, \forall y \in A, on\ a : xy \in I$

Tout idéal qu'est à la fois idéal à gauche et idéal à droite de A est appelé idéal bilatère de A, c'est-à-dire :

1) $\forall a \in A, \forall i \in I, \Longrightarrow\ a \times i \in I.$
2) $\forall a \in A, \forall i \in I, \Longrightarrow i \times a \in I.$

Exemple :

$\{0\}$ et A sont deux idéaux de A dit idéaux impropre.

Tout idéal I de A différent de $\{0\}$ et A est dit idéal propre de A.

Remarque : Si un idéal I contient un élément inversible $x \in A$. Alors on a : $I = A$.

Preuve :

Soit $x \in I\ , x^{-1} \in A\ donc\ 1 = xx^{-1} \in I$

Soit $a \in A, on\ a : a = \underbrace{a}_{a \in A} . \underbrace{1}_{1 \in I} \in I, d'$où $A = I$.

Proposition : Soient I et J deux idéaux à droite (resp. à gauche) d'un anneau A, alors $I + J$ est un idéal à droite (resp. à gauche) de A.

Preuve : Soit $x, y \in I + J \Longrightarrow \exists\ a, b \in I\ et \exists\ a', b' \in J$ tel que $x = a + a'$ et $y = b + b'$

$$x - y = (a - b) + (a' - b') \in I + J.$$

D'autre part, si $I\ et\ J$ sont deux idéaux à droite

$\forall\ z \in A$, on a $az \in I$ et $a'z \in J$ donc $xz = (a + a')z = az + a'z \in I + J$, d'où la preuve.

5-Générateur d'un idéal :

Définition : L'idéal engendré par une partie F d'un anneau A est le plus petit idéal contenant cette partie. Il est noté $I(F)\ ou\ < F >$.

Proposition : Soit A un anneau commutatif. Pour tout $x \in A$ la partie $xA = Ax = \{ax, a \in A\}$ est un idéal de A appelé idéal engendré par x.

Preuve :

1) $x = 1.x \in Ax$
2) $\forall (a,b) \in A^2, ax + bx = (a + b)x \in Ax$
3) $\forall a \in A, \forall\ b \in A, b(ax) = (ba)x \in Ax.$

Proposition : l'intersection d'une famille d'idéaux est un idéal.

Preuve : Soit $(I_j)_{j\in J}$ une famille d'idéaux d'un anneau $(A,+,\times)$.

$\forall\, j \in J, I_j$ est un sous-groupe de A donc l'intersection $\bigcap_{j\in J} I_j$ est un sous-groupe de A.

Stable par multiplication par un élément de A :

$$x \in \bigcap_{j\in J} I_j \iff \forall\, j \in J\ ,\ x \in I_j$$

$$\Longrightarrow \forall j \in J, \forall a \in A,\ x \times a \in I_J \Longrightarrow x \times a \in \bigcap_{j\in J} I_j$$

Définition :

Soit $(A,+,\times)$ un anneau commutatif.

Un idéal I de A est dit premier si :

- $I \neq A$
- $\forall\, x, y \in A; x \times y \in I \Longrightarrow\ x \in I\ ou\ y \in I$

Un idéal I de A est dit maximal si :

- $I \neq A$
- $\forall\, J\ ideal\ de\ A\ , I \subseteq J \Rightarrow (J = I\ ou\ J = A)$

Un idéal I de A est un idéal principale si :

- $\exists\ a \in I\ tel\ que\ I = Aa = \{xa, x \in A\}$

6-Homomorphismes d'anneaux :

Définition : Soient $(A,+,\times) et\ (B,+,\times)$ deux anneaux. On note $1_A\ et\ 1_B$ les éléments neutres multiplicatifs. On note $0_A\ et\ 0_B$ les éléments neutres additifs. On dit qu'une application $f: A \longrightarrow B$ est un homomorphisme d'anneaux si :

- $f(1_A) = 1_B$.
- $\forall (x,y) \in A^2, f(x+y) = f(x) + f(y)$
- $\forall (x,y) \in A^2, f(xy) = f(x)f(y)$
- Un endomorphisme d'anneaux $(A,+,\times)$ est un homomorphisme d'anneaux de $(A,+,\times)\ dans\ (A,+,\times)$.
- Un isomorphisme d'anneaux est un homomorphisme d'anneaux bijectif.
- Un automorphisme d'anneaux $(A,+,\times)$ est un endomorphisme bijectif dans l'anneau $(A,+,\times)$.

Proposition :

1) $Si\ f: A \longrightarrow B\ et\ g: B \longrightarrow C$ sont des morphismes d'anneaux, alors $g \circ f: A \longrightarrow C$ est un morphisme d'anneaux.
2) $Id_A: A \longrightarrow A$ est un automorphisme de l'anneau$(A,+,\times)$.
3) Si $f: A \longrightarrow B$ est un isomorphisme d'anneaux, alors $f^{-1}: B \longrightarrow A$ est un isomorphe d'anneaux.

Théorème :

1) Le noyau d'un morphisme est un idéal.
2) Un morphisme est injectif si et seulement si son noyau est nul.

Preuve :

1) Soit f un morphisme d'un anneau A dans un anneau B. Le noyau est un groupe additif puisque le morphisme est aussi un morphisme de groupe additif.
   En plus, si $a \in \ker f$ et $b \in A$:
   Alors on a :$f(ab) = f(a) \times f(b) = 0_B \times f(b) = 0_B; donc\ ab \in \ker(f)$.
   Donc le noyau d'un morphisme est un idéal.
2) Si le morphisme est injectif, le zéro a un seul antécédent $\Longrightarrow \ker f = \{0\}$
   Réciproquement ; si $f(x) = f(y) \Longrightarrow f(x - y) = 0$.
   c.à.d. $x - y \in \ker(f) = \{0\}$
   Donc $x = y\ et\ f$ est injective.

Proposition : Pour tout morphisme $f: A \longrightarrow B$ d'anneaux, $\ker f$ est un idéal bilatère de A.

Preuve : On sait que le $\ker f$ est un sous-groupe. Alors soit $x \in \ker f$, et soit $a \in A$

Donc $f(ax) = f(a)f(x) = f(a)0 = 0$

$f(xa) = f(x)f(a) = 0f(a) = 0$. Donc $\ker f$ est un idéal bilatère de A.

Anneau Quotient :

Soit I un idéal d'un anneau commutatif A. On sait que $A\ /\ I$ muni de la loi additive $(\overline{x}, \overline{y}) \longrightarrow \overline{x + y}$ est un groupe commutatif car $(A, +)$ est un groupe commutatif. On définie de même sur $A\ /\ I$ la loi multiplicative suivante : $(\overline{x}, \overline{y}) \longrightarrow \overline{xy}$. En effet :

$\overline{x} = \overline{x'} \Longrightarrow x = x' + u, où\ u \in I$

$\overline{y} = \overline{y'} \Longrightarrow y = y' + v, où\ v \in I$

$\Longrightarrow xy = x'y' + uy' + vx' + uv$

I étant un idéal, alors $uy' + vx' + uv \in$ I et par suite $xy - x'y' \in I$ c'est-à-dire $\overline{xy} = \overline{x'y'}$.

$A\ /\ I$ muni des deux lois citées précédemment est un anneau commutatif unitaire.

On appelle l'anneau quotient de A par I. L'homomorphisme d'anneau $A \longrightarrow A\ /\ I$ est appelé l'homomorphisme canonique.

7-ANNEAUX INTEGRES :

Définition : Soient A un sous anneau, $a \in A$.

1) On dit que a est un diviseur de zéro à gauche dans A si et seulement si :

$$\begin{cases} a \neq 0 \\ \exists\ b \in A, b \neq 0\ et\ ab = 0. \end{cases}$$

2) On dit que a est un diviseur de zéro à droite dans A si et seulement si :

$$\begin{cases} a \neq 0 \\ \exists\, c \in A, c \neq 0 \; et \; ca = 0 \end{cases}$$

3) On dit que a est un diviseur de zéro dans A si et seulement si a est un diseur de zéro à gauche dans A ou un diviseur de zéro à droite dans A.

Exemple :

Soit $f: \mathbb{R} \to \mathbb{R}$ et $g: \mathbb{R} \to \mathbb{R}$

$$x \to \begin{cases} 0 \; si \; x < 0 \\ x \; si \; x \geq 0 \end{cases} \qquad x \to \begin{cases} x \; si \; x \leq 0 \\ 0 \; si \; x > 0 \end{cases}$$

Sont des diviseurs de zéro puisque $f \neq 0, g \neq 0, fg = 0$.

Définition : Un anneau $(A, +, \times)$ est dit intègre si :

- A n'admet aucun diviseur de zéro.

Autrement dit, c'est un anneau vérifiant :

$$\forall\, x, y \in A, x \times y = 0 \Rightarrow x = 0 \; ou \; y = 0.$$

Exemple : L'anneau $\mathbb{Z}$ des entiers est intègre.

Définition : Soient A un anneau intègre,$(x, y) \in A^2$. On dit que x divise y et on note $x|y$ si et seulement si $\exists\, a \in A$ tel que $y = ax$: En d'autre terme $x|y \Leftrightarrow \exists a \in A \,/\, y = ax$.

Proposition : Soient A un anneau intègre, $(x, y) \in A^2$. Alors si $x|y \iff Ay \subset Ax$.

Preuve : Si $x|y$, alors $\exists\, a \in A$ tel que $y = ax$.

Donc $\forall\, \alpha \in A, \alpha y = \alpha(ax) = (\alpha a)x \in Ax$. D'où $Ay \subset Ax$.

Proposition : Soit A un anneau unifére intègre. Alors, tout élément inversible d'un coté est inversible.

Preuve : Soit $a \in A$ inversible à droite, alors $\exists b \in A$ tel que $ab = 1$.

$$ab - 1 = 0 \Longrightarrow b(ab - 1) = bab - b = (ba - 1)b = 0.$$

Puisque A est intègre $b \neq 0$, alors b est régulier

Alors $ba - 1 = 0$. Donc a est aussi inversible à gauche.

Définition :(*Elément nilpotent*)

Soit A un anneau non réduit à $\{0\}$. Soit a un élément non nul de A.

On dit que a est nilpotent s'il existe un entier n tel que $a^n = 0$, avec ces notations $\forall\, p > n, a^p = 0$

Le plus petit entier n tel que $a^n = 0$ est appelé l'indice de nilpotente de a.

8-CORPS :

Définition : Un ensemble K muni de deux lois de compositions internes $+\ et\ \times$. On dit que $(K, +, \times)\ est$ un corps si :

- ✓ $(K, +, \times)\ est\ un\ anneau.$
- ✓ $0_K \neq 1_K. (tout\ corps\ contient\ 1\ et\ 0)$
- ✓ Tout élément de $K \setminus \{0\}$ admet un inverse pour le produit dans K.

Si de plus, $\times$ est commutatif dans K on dit que $(K, +, \times)$ est un corps commutatif.

Exemple :

$(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)\ et\ (\mathbb{C}, +, \times)$ Sont tous des corps commutatifs.

Caractérisation d'un corps : Soit A un anneau non nul. Les assertions suivantes sont équivalentes :

i) $A\ est\ un\ corps$.
ii) $Les\ seuls\ idéaux\ de\ A\ sont\ \{0\}\ et\ A.$
iii) $Tout\ homomorphisme\ non\ nul\ de\ A\ dans\ un\ anneau\ est\ injectif.$

Preuve :

$i) \Rightarrow ii)$ Soit $I \neq \{0\}\ un\ idéal$

Soit $x \neq 0\ et\ x \in I, x^{-1} \in A \implies 1 = xx^{-1} \in I$

Soit $a \in A$, on a : $a = a.1 \in I$, d'où $I = A$.

$ii) \Longrightarrow iii)$, Soit $f: A \longrightarrow B$ un morphisme d'anneau non nul avec $B \neq \{0\}$

C à d :$\exists\ x \in A\ tel\ que\ f(x) \neq 0$. Par suite $x \notin \ker f\ \ et \ker f\ \ est\ un\ idéal.$

Donc d'après $ii)$ on a $\ker f = \{0\}$ et par suite f est injectif.

$iii) \Rightarrow i)$. Soit $x \in A\ et\ x$ non inversible

Comme x est non inversible, alors $B = A\ /\ xA\ (A \neq xA)$

Par suite $f: A \longrightarrow B = A/xA$ où $f(z) = \bar{z} = z + xA$ qu'est non nul car $(B \neq 0)$ est un morphisme qu'est injectif d'après $iii)$. Or $f(0) = \bar{0} = \bar{x} = f(x)$

Donc $x = 0\ \ car\ f\ injectif.$

Remarque : Tout corps commutatif est un anneau intègre.

La réciproque est fausse, $\mathbb{Z}$ est un anneau intègre mais n'est pas un corps.

9-Sous-corps :

Définition : Soient $(K,+,\times)$ un corps, L une partie de K. On dit que L est un sous-corps de K si:

- L est un sous-anneau de K .
- $\forall\, x \in L \setminus \{0\},\ x^{-1} \in L.$

Autrement dit :

- $L \neq \emptyset$.
- $\forall\, x, y \in L \setminus \{0\},\quad xy^{-1} \in L$

Exemple : $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, et $\mathbb{R}$ est un sous-corps de $\mathbb{C}$. (Pour les lois usuelles $+$ et $\times$)

Proposition :(*Caractérisation D'un Sous-Corps*)

L est un sous-corps de $(K,+,\times)$ si et seulement si :

- $1 \in L.$
- $\forall (a,b) \in L^2,\ a-b \in L.$
- $\forall (a,b) \in L^2, avec\quad b \neq 0, ab^{-1} \in L.$

10-Morphisme de corps :

Définition : Soient $(K,+,\times)$ et $(L,+,\times)$ deux corps. On dit qu'une application $f: K \longrightarrow L$ est un morphisme de corps si :

- $f(1_K) = 1_L.$
- $\forall (a,b) \in K^2,\qquad f(a+b) = f(a) + f(b)$
- $\forall (a,b) \in K^2,\qquad f(ab) = f(a)f(b)$

Si de plus f est bijective. On dit que f est un isomorphisme de corps.

Proposition :(*Corps des fractions d'un anneau intègre*)

Soit $(A,+,\times)$ un anneau commutatif.

Si A est un anneau intègre, il existe un corps $(K,+,\times)$ tel que :

- ✓ $(A,+,\times)$ est un sous-anneau de K.
- ✓ $K = \{ab^{-1}, a, b \in A, b \neq 0\}.$
- ✓ Si K' est un corps satisfaisant les deux dernières conditions, alors $K' \simeq K$ (On dit que le corps K est unique à l'isomorphisme prés).

Le corps K s'appelle le corps des fractions de l'anneau A.

Exemple :

$(\mathbb{Q},+,\times)$ est le corps des fraction de l'anneau intègre $(\mathbb{Z},+,\times)$.

Proposition : Soient $A \ et \ B$ deux corps commutatifs et f un homomorphisme de A vers B.
Alors f est injectif.

Preuve :

Soit $x \in \ker f \ tel \ que \ x \neq 0$.

x étant inversible. Donc on a :

$1 = f(1) = f(xx^{-1)} = f(x)f(x^{-1}) = 0$

Ce qui est impossible, donc $\ker f = \{0\} \ et \ f \ est \ injectif$.

CHAPITRE III : LES MODULES

1-Premier pas :

Définition : Soit A un anneau. Un A-module(ou un module sur A) est un groupe abélien M muni d'une application (multiplication externe) $A \times M \xrightarrow[(a,m)\to am]{} M$ vérifiant les propriétés suivantes :

$\forall\, a, b \in A \; et \; \forall m, n \in M$, on a:

1. $(a+b)m = am + bm$ et $a(m+n) = am + an$ (distributivité).
2. $(ab)m = a(bm)$.
3. $1_A m = m$.

Exemple :

1) Un anneau A est un A-module.

2) Un idéal de A est A-module.

Définition : *(Sous-Module)*

Soit A un anneau. Et soit M un A-module, un sous-module est une partie N de M vérifiant :

- N est un sous-groupe abélien de M.
- $\forall\, a \in A$ et $\forall\, m \in N, am \in N$.

Autrement dit : Une partie N de M est un sous-module si et seulement si :

- ✓ $0 \in N$.
- ✓ $\forall\, x, y \in N$ et $\forall \alpha \in A$:
  - $x + y \in N$
  - $\alpha x \in N$

Exemple : Si A est un anneau, les idéaux de A sont les sous- A-modules de A.

Définition : *(Homomorphisme)*

Soit A un anneau, et soit $M \; et \; N$ deux A-modules. Un homomorphisme de M dans N est une application $f: M \longrightarrow N$ tells que, $\forall\, a, b \in A$ et $\forall\, m, n \in M$ on a : $f(am + bn) = af(m) + bf(n)$.

On note $Hom_A(M, N)$ l'ensemble des homomorphismes de M dans N.

Un homomorphisme de M dans M est appelé endomorphisme de M. On note $End_A(M)$ l'ensemble des endomorphismes du A-module M.

Lemme : Soit A un anneau et soit M, N, P trois A-modules. Si $f: M \longrightarrow N$ et $g: N \longrightarrow P$ sont des homomorphismes, leur composé $g \circ f: M \longrightarrow P$ est un homomorphisme de A-modules.

Définition : On dit qu'un morphisme de A-module $f: M \longrightarrow N$ est un isomorphisme s'il existe un homomorphisme $g: N \longrightarrow M$ tel que $f \circ g = Id_N \;\; et \; g \circ f = Id_M$.

Proposition : Un morphisme est un isomorphisme si et seulement si, il est bijectif.

Preuve :

Si $f: M \longrightarrow N$ est un isomorphisme de réciproque g, il est clair que g est la bijection réciproque de f.

Inversement, si $f: M \longrightarrow N$ est un morphisme bijectif, soit g sa bijection réciproque. Alors g est un morphisme.

En effet : Si $n, n' \in N \; et \; a, a' \in A$ on a :

$$f\big(ag(n) + a'g(n')\big) = af\big(g(n)\big) + a'f\big(g(n')\big) = an + a'n' .$$

Donc $ag(n) + a'g(n') = g(an + a'n')$. Ce qui établit la linéarité de g.

Définition : (Noyau)

Soit $f: M \longrightarrow N$ un morphisme de A-modules. On appelle noyau de f, noté $\ker f$, l'ensemble des $m \in M$ tels que $f(m) = 0. En\ d'autre\ terme\ \ker f = \{\forall m \in M \ / f(m) = 0\}$.

Proposition : Soit $f: M \longrightarrow N$ un homomorphisme de A-module. Si M' est un sous-module de M, $f(M')$ est un sous-module de N. Si N' est un sous-modules N, alors $f^{-1}(N')$ est un sous-module de M.

En particulier, le noyau $\ker f$ et l'image $Imf = f(M)$ de f sont des sous-modules de M et N respectivement.

Preuve :

Montrons que $f(M')$ est un sous-module de N.

Comme $f(0_M) = 0_N$ et $0_M \in M'$ et $0_N \in f(M')$. D'autre part, si $n \; et \; n' \in f(M')$

$\exists \; m \; et \; m' \in M'$ tel que $n = f(m)$ et $n' = f(m')$

$$\Longrightarrow n + n' = f(m) + f(m') = f(m + m') \in f(M')$$

Enfin, si $n = f(m) \in f(M')$ et si $a \in A, an = af(m) = f(am) \in f(M')$ puisque $am \in M'$.

Montrons que $f^{-1}(N)$ est un sous-module de M.

Comme $f(0_M) = 0_N \in N', 0_M \in f^{-1}(N')$, d'autre part, si $m \; et \; m' \in f^{-1}(N')$ et si $a, b \in A$

On a : $f(am + bm') = af(m) + bf(m') \in N'$. Puisque $f(m) \; et \; f(m')$ appartiennent à N' et que

N' est un sous-module de N ; Donc $am + bm' \in f^{-1}(N')$.

2-Operations sur les Modules :

Proposition : Soit A un anneau, soit M un A-module et soit $(N_s)_{s \in S}$ une famille de sous-modules de M. Alors l'intersection $N = \bigcap_s N_s$ est un sous-module de M.

Preuve :

Comme $0 \in N_s \ \forall s, \ donc \ 0 \in N$.

Soient m, n deux éléments de N, $\forall s \ \ m \ et \ n$ appartiennent au sous-module de N_s. Donc $m+n$ aussi et $m+n$ appartiennent à leur intersection N .

Enfin, soit $m \in N$ et $a \in A. \forall \ s, \ m \in N_s \ donc \ am \in N_s$ et finalement $am \in N$.

ainsi N est un sous-A-module de M.

Définition : Soit A un anneau, M un A-module et soit $(M_s)_{s \in S}$ une famille de sous-modules de M. la somme des M_s, $\sum_s M_s$, est le sous-module de M engendré par la réunion $\bigcup_s M_s$ des M_s.

C'est aussi l'ensemble des combinaisons linéaires $\sum_s m_s$ où $(m_s)_s$ est une famille presque nulle d'élément de M tel que $m_s \in M_s \ \ \forall s$.

Définition : Soit A un anneau, M un A-module et I un idéal de A. On définit le sous-module IM de M comme l'ensemble des combinaisons linéaires $\sum_i a_i m_i$. Où $\forall \ i, a_i \in I$ et $m_i \in M$.

Proposition : Soit M un A-module. Soit $(N_s)_{s \in S}$ une famille quelconque de sous-modules de M et P_1 et P_2 deux sous-modules de M.

Si $P_1 \cup P_2$ est un sous-module de M, alors, $P_1 \subset P_2$ ou $P_2 \subset P_1$.

Preuve : On suppose P_1 et P_2 ne sont pas inclus l'un dans l'autre.

Alors il existe $p_1 \in P_1$ et $p_2 \in P_2$ tel que $p_1 \notin P_2$ et $p_2 \notin P_1$. Puisque les P_i sont des sous modules il vient $p_1 + p_2 \notin P_1$ et $p_1 + p_2 \notin P_2$.

Alors que $p_1, p_2 \in P_1 \cup P_2$.

Définition : Soit A un anneau. Et soit (M_s) une famille de A-modules le produit des M_s est l'ensemble $\prod_s M_s$ des lois :

- ✓ $(m_s)_s + (n_s)_s = (m_s + n_s)_s$
- ✓ $a(m_s)_s = (am_s)_s$

Qui en font un A-module

La somme directe des M_s est le sous-module $\oplus_s M_s$ de $\prod M_s$ formé des éléments $(m_s)_s$ tel que : $\forall s$ sauf pour un nombre fini $m_s = 0$.

3-Noyau et image :

Proposition : Soit $f : M \longrightarrow N$ un morphisme de A-modules (en particulier un morphisme de groupe additif)

1. Le noyau de f , $\ker f = \{m \in M; f(m) = 0\}$ est un sous-module de M.
2. L'image de f, $Imf = \{\forall n \in N, \exists m \in M; f(m) = n\}$ est un sous-module de N.

Preuve :

1) On sait que $\ker f$ est un sous-groupe de M.
   Soit $x \in \ker f$ et soit $\alpha \in A$, alors on a : $f(\alpha x) = \alpha f(x) = \alpha 0 = 0$.
   Donc $\alpha x \in \ker f$, ce qui montre que $\ker f$ est un sous-module de M.
2) On sait que Imf est un sous-groupe de N.
   Soit $x \in Imf$ et $\alpha \in A$.
   Comme $x \in Imf$. Il existe un antécédent $y \in M$ de x. C'est-à-dire $f(y) = x$.
   Alors par linéarité de f, αy est un antécédent de $\alpha x \in Imf$.
   Cela montre que Imf est un sous-module de N.

4-Générateurs, Bases, Modules libres :

Définition : Soit A un anneau. Et soit M un A-module. On dit qu'une famille $(m_i)_{i\in I}$ d'éléments de M est :

- Génératrice : Si le sous-module de M engendré par les m_i est égal à M.
- Libre : Si pour toute familles presque nulles $(a_i)_{i\in I}$ d'éléments de A,
  La relation $\sum_i m_i a_i = 0 \Longrightarrow a_i = 0, \forall i \in I$.
- Une Base de M : C'est un système libre de générateurs, c'est-à-dire pour tout élément m de M, il existe une unique famille presque nulle $(a_i)_{i\in I}$ dans A telle que $m = \sum m_i a_i$.

Proposition : Soit A un anneau, M un A-module et S une partie de M.

Soit φ_s l'homomorphisme canonique : $A^S \longrightarrow M$, $(a_s)_{s\in S} \longrightarrow \sum_s a_s s$.

Alors :

1) φ_s est injectif si et seulement si S est libre.
2) φ_s est surjectif si et seulement si S est génératrice.
3) φ_s est isomorphisme si et seulement si S est une base.

Preuve :

Le noyau de φ_s est l'ensemble des familles (a_s). Telle que $\sum_s a_s s = 0$, dire que S est libre équivaut donc à dire que $\ker \varphi_s = \{0\}$. C'est-à-dire que φ_s est injectif.

L'image de φ_s est l'ensemble des combinaisons linéaires d'éléments de S.

Par suite $Im\varphi_s =< S >$ et φ_s est surjectif si et seulement si S est génératrice.

Enfin, la définition de fait que S est une base revient exactement à dire que φ_s est bijectif, donc un isomorphisme.

5-Annulateur,Modules monogénes :

Définition : On dit qu'un élément x d'un A-module M est annulé par le scalaire $a \in A$ si $ax = 0$.
L'ensemble des éléments de A qui annulent x est un idéal de A appelé annulateur de x (on écrit $Ann(x)$).

L'annulateur d'un sous-module N est l'ensemble des éléments de A qui annulent tout élément de N, i.e. $Ann(N) = \bigcap_{x\in N} Ann(x)$ qui aussi un idéal de A.

L'annulateur du module M est évidemment $\bigcap_{x\in M} Ann(x)$. Si $Ann(M) = \{0\}$, on dit que M est fidèle. L'annulateur d'un module libre est toujours nul.

Si $Ann(x) \neq \{0\}$, on dit que x est un élément de torsion.

Module monogéne :

Définition : Un module est dit monogène s'il est engendré par un seul élément, il est isomorphe à A/I où I est son annulateur.

6-Suites exactes :

Définition : Une suite d'applications linéaires : …. $\longrightarrow M_{i-1} \overset{f_i}{\to} M_i \overset{f_{i+1}}{\longrightarrow} M_{i+1}$ … …

Est dite exacte si pour chaque i, $Imf_i = \ker f_{i+1}$.

- Si M' est un sous-module de M, la suite : $0 \longrightarrow M' \overset{i}{\to} M \overset{s}{\to} M/M' \longrightarrow 0$ est exacte.
- Si $M = M_1 \oplus M_2$, la suite $0 \longrightarrow M_1 \overset{i}{\to} M \overset{pr_2}{\longrightarrow} M_2 \longrightarrow 0$ est exacte.
- La suite $0 \longrightarrow M \overset{f}{\to} N$ est exacte si et seulement si f est injective.
- De même la suite $M \overset{g}{\to} N \longrightarrow 0$ est exacte si et seulement si g est surjective.

Suites exactes scindées :

Propositions :

1-a) Une suite exacte $M \overset{g}{\to} N \longrightarrow 0$ est dite scindée s'il existe un homomorphisme $g_1 : N \longrightarrow M$ tel que $g \circ g_1 = Id_N$, dans ce cas $M = \ker g \oplus Img_1$.

Preuve : $\forall\, x \in M$ s'écrit $x = x - g_1\big(g(x)\big) + g_1(g(x))$ avec $g_1(g(x)) \in Img_1$

Et $x - g_1(g(x)) \in \ker g$ puisque $g \circ g_1 = Id_N$,

Par ailleurs, si $x \in Img_1 \cap \ker g$ alors $\exists x_0 \in N$ tel que $x = g_1(x_0)$ et $g(x) = 0$ d'où $0 = (g \circ g_1)(x_0) = x_0$ et $x = g_1(0) = 0$.

1-b) Inversement si $M \overset{g}{\to} N \longrightarrow 0$ est exacte et $\ker g$ est facteur direct de M alors la suite est scindée.

En effet, g étant surjective, $\forall\, y \in N, y = g(m)$ où $m \in M'$ un supplémentaire de $\ker g$ (écrire $y = g(x)\ et\ x = m + n, n \in \ker g, m \in M'$), M est unique car si $m_1 \in M'$ vérifie $y = g(m_1)$,on a $m_1 - m \in \ker g \cap M' = \{0\}$, en posant $g_1(y) = m$. Donc la suite est scindée.

2) D'une manière analogue, on dit que la suite exacte $0 \longrightarrow P \overset{f}{\to} M$ est scindée s'il existe $f_1 : M \longrightarrow P$ tel que $f_1 \circ f = Id_p$; dans ce cas $M = Imf \oplus \ker f_1$. Inversement si Imf est facteur direct de M, la suite est scindée . Dans ce cas, on a aussi $Imf \simeq P$.

On résulte de 1) et 2) la proposition suivante :

Proposition : Pour une suite exacte $0 \longrightarrow P \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$, les conditions suivantes sont équivalentes.

1. $0 \longrightarrow P \xrightarrow{f} M$ est scindée.
2. $M \xrightarrow{g} N \longrightarrow 0$ est scindée.
3. $M \simeq P \oplus N$.

Définition : On dit que la suite $0 \longrightarrow P \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ est scindée, si les trois conditions précédentes sont vérifiées.

CHAPITRE IV : ANNEAUX ET MODULES NOETHERIENS

Définition : Soit A un anneau. On dit qu'un A-module M est de type fini s'il existe une partie fini $S \subset M$ tel que $M =< S >$. c'est-à-dire que $M = Ax_1 + Ax_2 + \ldots\ldots + Ax_n$.

Proposition : Soit A un anneau et soit M un A-module. Les propriétés suivantes sont équivalentes :

a) Tout sous-modules de M est de type fini.
b) Toute suite croissante de sous-modules de M est stationnaire.
c) Toute famille non vide de sous-modules de M admet un élément maximal.

Définition : Un A-module qui vérifié les trois propriétés équivalentes est dit Noethérien.

Preuve :*(De la proposition)*

a)⟹b) : Si $(M_n)_{n\geq 1}$ est une suite croissante de sous-modules de M, la réunion $\bigcup_{n\geq 1} M_n$ est un sous-module de M donc de type fini. Si $m_{i_1}, \ldots\ldots, m_{i_s}$ est un système fini de générateurs de cette réunion avec $m_{i_j} \in M_j$ et $i = \sup\{i_k\}\, 1 \leq k \leq s$, on voit que la suite est stationnaire à partir de i.

b) ⟹ c) Soit $(M_i)_{i\in I}$ une famille non de vide de sous-modules de M et M_j un élément quelconque de cette famille ; si M_j n'est pas maximal alors $M_j \subset M_{j+1}$ où M_{j+1} est un autre élément de cette famille ; si M_{j+1} n'est pas maximal alors $M_{j+1} \subset M_{j+2}$ où M_{j+2} est un élément de la famille, on fabrique ainsi une suite croissante à partir d'un certain M_{j+k} qui sera un élément maximal de la famille $(M_i)_{i\in I}$.

c) ⟹a) :

Soit N un sous-module de M ; la famille des sous-modules de N qui sont de type fini n'est pas vide (si $m \in N, Am$ est un élément de cette famille), elle admet un élément maximal $M' = \sum_{i=0}^{n} Am_i$. On a alors $M' = N$ car si $M' \subsetneq N$ et $m \in N - M'$, le sous-module $M' + Am$ de N est de type fini et contient strictement M' ce qui contredit la maximalité de M'.

Définition : Un anneau A est dit Noethérien s'il est Noethérien en tant que module sur lui-même. Les conditions équivalentes s'énoncent alors :

- Tout idéal de A est de type fini.
- Toute suite croissante d'idéaux de A est stationnaire.
- Toute famille non vide d'idéaux de A admet un élément maximal.

Proposition : Soit A un anneau, M un A-module de type fini. Alors pour tout module Noethérien N, $Hom_A(M, N)$ est un A-module Noethérien.

Preuve : Comme M est de type fini, on peut considérer une famille fini $(m_1, \ldots\ldots, m_n)$ d'éléments de M qui l'engendrent, on a alors un homomorphisme canonique :

$f : Hom_A(M, N) \longrightarrow N^n,\ g \longrightarrow f(g) = (g(m_1), \ldots\ldots, g(m_n))$.

C'est effectivement un homomorphisme car pour tout g et h dans $Hom_A(M, N)$ et $a\ et\ b$ dans A

On a: $f(ag + bh) = ((ag + bh)(m_1), \ldots\ldots\ldots, (ag + bh)(m_n))$

$$= \big(ag(m_1) + bh(m_1), \dots\dots\dots, ag(m_n) + bh(m_n)\big)$$

$$= a\big(g(m_1), \dots\dots\dots, g(m_n)\big) + b\big(h(m_1), \dots\dots\dots, h(m_n)\big)$$

$$= af(g) + bf(g).$$

Il est injectif car si un homomorphisme de M dans N est nul en tous les m_i, il s'annule en toute combinaison linéaire des m_i donc sur M.

Ainsi $Hom_A(M,N)$ est un isomorphisme à un sous-module de N^n. Comme N est un A-module Noethérien, N^n aussi et $Hom_A(M,N)$ est un A-module Noethérien.

Proposition : Soit A un anneau Noethérien, et soit I un idéal de A.

Alors $A\ /\ I$ est Noethérien.

Preuve : On sait que $A/I = \{x + I = \overline{x}\ /\ x \in A\}$

Or les idéaux de $A\ /\ I$ sont de la forme $J\ /\ I$, avec J un idéal de A tel que $J \supseteq I$

Soit $H \subseteq A/I \Longrightarrow H = \sum A/I\,\overline{x_i}$ avec $x_i \in A$

$$= \sum A/I\,(x_i + I)$$

Soit $J = \sum x_i A + I \Longrightarrow J/I = \sum \overline{x_i}\,(A/I) = H$

Alors $H = J\ /\ I$ et $J = \sum_{i=1}^{n} Ax_i$

$H = J/I = \sum_{i=1}^{n}(A/I)\,\overline{x_i}$ Est de type fini. Donc $A\ /\ I$ est Noethérien.

Exemple : $\mathbb{Z}/n\mathbb{Z}$ est Noethérien.

Proposition : $K[X]$ est un anneau Noethérien

Preuve : Soit I un idéal tel que $I \subseteq K[X]$

Soit $P \in I \setminus \{0\}$ de degré minimal et $J = \{d^\circ P\ /P \in I \setminus \{0\}\}$

En suite $P\,K[X] \subseteq I$

Maintenant soit $Q \in I$

Donc $Q = PH + R$ avec $d^\circ R < d^\circ P$

$\begin{cases} R = Q - PH \in I \\ d^\circ R < d^\circ P \end{cases} \Longrightarrow R = 0$ donc $Q = PH \in PA$

Exemple : $\mathbb{Z}$ est un anneau Noethérien.

Définition : Soit $C = A \times B$ avec A et B sont des anneaux.

Un idéal I de C, s'écrit sous la forme : $I = I_1 \times I_2$.

Avec I_1un idéal de A et I_2 un idéal de B