Ensembles

Objet : Un objet est un être, de toute nature, qui est représenté par un ***symbole***, on peut le dupliquer en tant que symbole, et aussi le mettre dans plusieurs groupements.

Ensemble : Un ensemble est un rassemblement ou ***collection*** d'objets, éventuellement vide.

Mode de définition d'un ensemble : On peut définir un ensemble en faisant l'inventaire des objets qui le constituent, en entourant cette liste par des accolades pour le délimiter. Ce mode est appelé en extension.. Par ailleurs on peut nommer un ensemble par un quelconque des symboles.

$$A = \{1, <, w, 5\}$$

N.B. $\{1, <, w, 5\}$ est l'ensemble, A un nom qui le représente dans les calculs.

N.B. := signifie que ce qui est à gauche est le nom de ce qui est à droite

N.B. Tous les ensembles vides sont identiques et sont représentés par $\{\}$ ou $\varnothing$

On peut donner une propriété commune des objets collectés (mode en compréhension) :

$$D = \{* \mid * \text{ est un chiffre décimal}\}$$

En extension $D = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

N.B. L'ensemble de tous les ***objets*** n'a pas de sens. Car un ensemble est un objet. et un objet ne peut pas être élément de lui-même.

N.B. L'ensemble de tous les ***ensembles*** n'a pas de sens. Car un ensemble ne peut pas être élément de lui-même.

Pour éviter ce blocage, l'ensemble de tous les ensembles n'étant pas un ensemble, on l'appelle $0-$***Classe*** de tous les ensembles, on désigne cette classe par Ens.

N.B. Les ensembles et les $0-$***Classe*** sont des collections d'objets.

N.B. La $0-$***Classe*** de toutes les $0-$***Classe*** n'a pas de sens. Can une $0-$***Classe*** ne peut pas être élément d'elle-même.

Pour éviter ce blocage, on l'appelle $1-$***Classe*** de toutes les $0-$***Classes***, et ceci suppose que celle-ci n'est pas une $0-$***Classe***.

On remarque la rupture entre une catégorie et une suivante, on peut continuer à définir sans arrêt : $2-$***Classe*** collection de toutes les $1-$***Classe*** etc.

Le but de ce travail est d'étudier les ensembles et la classe Ens.

Ensemble fini : Un ensemble E est fini, si on peut compter ses éléments, dans ce cas ce nombre sera noté #E (le cardinal de E)

La Collection des ensembles finis : la collection des ensembles finis est notée $\mathcal{Ens}_0$

Théorème : $\mathcal{Ens}_0$ est un ensemble. (Démonstration ici-bas)

Relations sur les ensembles :

Elément d'un ensemble : Un objet x dans un ensemble A s'appelle ***élément*** de cet ensemble on note $x \in A$.

N.B. $x \in \{\}$ est une assertion fausse.

Égalité de deux ensembles : Soit A et B deux ensembles, on dit qu'ils sont égaux ssi :

$$\text{(Pour tout objet } x\text{)} : \quad x \in A \iff x \in A$$

Inclusion : soit A et B des ensembles, on dit que A est inclus dans B (ou B contient A) et on note :

$$A \subset B \text{ ou } B \supset A$$

Ssi : (pour tout objet x): $x \in A \implies x \in A$

N.B. on remarque : $(A \subset B \text{ et } A \supset B) \iff A = B$

N.B. Si $A \subset B$ on dit que A est une ***partie*** de B. ou que A est un ***sous-ensemble*** de B.

Opérations sur les ensembles :

Intersection : soit A et B des ensembles, on appelle intersection de A et B, l'ensemble des :
Objets x tels que :

$$x \in A \text{ et } x \in B$$

On note cet ensemble : $A \cap B$, donc : $A \cap B = \{x \mid x \in A \text{ et } x \in B\}$

Réunion : Soit A et B des ensembles, on appelle réunion de A et B, l'ensemble des :
Objets x tels que :

$$x \in A \text{ ou } x \in B$$

(Ce ***ou*** est un ***ou*** inclusif)

On note cet ensemble : $A \cup B$, donc : $A \cup B = \{x \mid x \in A \text{ ou } x \in B\}$

Différence : Soit A et B des ensembles, on appelle différence de A et B, l'ensemble des :
Objets x tels que :

$$x \in A \text{ et } x \notin B$$

On note cet ensemble : $A \setminus B$, donc : $A \setminus B = \{x \mid x \in A \text{ et } x \notin B\}$

Différence symétrique : Soit A et B des ensembles, on appelle différence symétrique de A et B, l'ensemble des objets x tels que :

$$(x \in A \text{ et } x \notin B) \text{ ou } (x \in B \text{ et } x \notin A)$$

On note cet ensemble : $A \Delta B$, donc : $A \Delta B = \{ x \mid (x \in A \text{ et } x \notin B) \text{ ou } (x \in B \text{ et } x \notin A)\}$

Exercice : fonction caractéristique d'une partie d'un ensemble :
Soit A et B des parties de E : On définit l'application (la définition d'une application viendra plus tard) de E dans {0 ;1}

$$\chi_A : E \longrightarrow \{0 ; 1\}, x \in A \longmapsto 1, x \in E \setminus A \longmapsto 0.$$

Propriétés : $(\chi_A)^2 = \chi_A$

$\chi_{A \cap B} = (\chi_A).(\chi_B) = \boldsymbol{min}\{\chi_A , \chi_B\}$
$\chi_{A \setminus B} = (\chi_A).(1 - \chi_A)$
$\chi_{A \cup B} = (\chi_A).(1 - \chi_A) + (1 - \chi_A).(\chi_A) - (\chi_A).(\chi_B)$
$\chi_{A \Delta B} = (\chi_A).(1 - \chi_A) + (1 - \chi_A).(\chi_A)$
$\chi_{\{\}} = 0$
$\chi_E = 1$
$A = B \iff \chi_A = \chi_B.$
$A \subset B \iff \chi_A \leq \chi_B.$

Avec ces propriétés démontrer :

$A \cap E = A$, $A \cap \{\} = \{\}$, $A \cap A = A$, $A \cap B = B \cap A$, $A \cap (B \cap C) = (B \cap A) \cap C$

$A \cup E = E$, $A \cup \{\} = A$, $A \cup A = A$, $A \cup B = B \cup A$, $A \cup (B \cup C) = (B \cup A) \cup C$

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

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

$A \setminus B = A \cap (E \setminus B)$

$A \Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$

$A \Delta (B \Delta C) = (B \Delta A) \Delta C$

$A \Delta (B \cap C) = (A \Delta B) \cap (A \Delta C)$

Ensemble des parties d'un ensemble : Soit E un ensemble, on note par 2^E l'ensemble de toutes les parties de E (2^E puisque si E est fini à n éléments l'ensemble de ses parties est à 2^n éléments), des fois on a besoin des parties finies de E, l'ensemble de ces paries finies de E sera noté $2^{(E)}$, si E est fini $2^{(E)} = 2^E$. Plus tard on définira les ensembles infinis.

Couple ordonné de deux objets : un ***couple ordonné*** (a, b) de deux objets a et b peut être défini de plusieurs façons, une desquelles est : $(a, b) = \{a, \{a, b\}\}$, par cette définition on remarque que $(a, b) = (a', b')$ équivaut à $\{a, \{a, b\}\}, \{a', \{a', b'\}\}$ donc équivaut à : $a = a'$ et $b = b'$. Cette dernière serait comme une condition caractéristique d'un couple ordonné.

Produit cartésien de deux ensembles : Soit E, F deux ensembles.

On définit le ***produit cartésien*** $E\times F$ comme étant l'ensemble $\{(a, b) \mid a \in E \text{ et } b \in F\}$, $E\times F$ est vide si l'un de E ou F est vide.

Nuplet ordonné de plusieurs objets : une ***suite ordonnée*** de n objets ou ***nuplet*** : $(a_1, a_2, a_3,\ldots, a_n)$ par la propriété caractéristique $(a_1, a_2, a_3,\ldots, a_n) = (b_1, b_2, b_3,\ldots, b_n)$ équivaut à n égalités simultanées : $a_1= b_1$, $a_2 = b_2$, $a_3 = b_3,\ldots, a_n = b_n$, une autre possibilité de définition est par récurrence sur le nombre d'objets dans cette suite ordonnée : $(a_1, a_2, a_3,\ldots, a_{n+1}) = ((a_1, a_2, a_3,\ldots, a_n), a_{n+1})$, pour n plus que 2, cette définition vérifie bien la propriété caractéristique, a_j sera appelé la j-ème projection de la suite $(a_1, a_2, a_3,\ldots, a_n)$,

Produit cartésien de plusieurs ensembles : On généralise à un produit cartésien d'un nombre fini d'ensembles : $E_1, E_2, E_3,\ldots\ldots, E_n$, en définissant tout d'abord ainsi le produit cartésien $E_1\times E_2\times E_3\times\ldots\ldots\times E_n$, est défini comme étant l'ensemble $\{(a_1, a_2, a_3,\ldots, a_n) \mid (a_1 \in E_1, a_2 \in E_2, a_3 \in E_3,\ldots, a_n \in E_n\}$, et la puissance cartésienne *n*-ème : $E^n = \{(a_1, a_2, a_3,\ldots, a_n) \mid (a_1 \in E, a_2 \in E, a_3 \in E,\ldots, a_n \in E\}$, le produit cartésien peut être étendu à un nombre infini d'ensemble en définissant une suite illimité d'objets. $(a_0, a_1, a_2, a_3,\ldots, a_n, \ldots.)$, et $\left(a_j\right)_{j\in I}$ pour I un ensemble d'indice quelconque. $E^{\mathbb{N}} = \{ (a_0, a_1, a_2, a_3,\ldots, a_n, \ldots.) \mid a_j \in E$, pour tout j de $\mathbb{N}\}$, $E^I = \{ \left(a_j\right)_{j\in I} \mid a_j \in E$, pour tout j de I$\}$.

Relation d'un ensemble dans un autre : Soit E, F deux ensembles, une relation de E dans F est une correspondance qui à un élément de E fait correspondre zéro, un, ou plusieurs éléments de F, si f est cette relation on note $f : E \longrightarrow F$ ou $E \xrightarrow{f} F$, E est appelé ***départ*** de f et F est appelé ***arrivée*** de f, si à x de E correspond y de F, on note $x \longmapsto y$, dit lien de x vers y par f, et on dit y est ***image*** de x par f, ou que x est un ***antécédent*** de y par f., deux relations $f : E \longrightarrow F$ et $f' : E' \longrightarrow F'$ sont dites égale ssi : $E = E'$, $F = F'$ et tout lien $x \longmapsto y$ par f est aussi un lien par f' et réciproquement, on définit le ***graphe*** de cette relation par ***Gr***$(f) = \{(x,y) \in E\times F \mid x \longmapsto y\}$ une partie du produit cartésien $E\times F$, réciproquement, à toute partie C du produit cartésien correspond une relation de E dans F, on notera par $2^{E\times F}$ l'ensemble de toutes les relations de E dans F, et par 2^{E^2} l'ensemble de toutes les relations de E dans E, qui se nomment les relations sur E.

On définit le ***composé*** de deux relations $E \xrightarrow{f} F$ et $H \xrightarrow{g} K$ comme étant une relation $E \longrightarrow K$, par $x \longmapsto k$ si il existe un élément *z* de $F\cap H$ tel que : $x \longmapsto z$ et $z \longmapsto k$, on note cette relation composée par $g\circ f$, cette opération de composition est associative non commutative. La réciproque d'une relation $E \xrightarrow{f} F$, est la relation $F \xrightarrow{f^{-1}} E$ qui renverse les flèches : $x \longmapsto y$ par f, équivaut à : $y \longmapsto x$ par f^{-1}. On définit la restriction de f à une partie A de E, la relation $f_A : A \longrightarrow F$, qui applique la règle f de correspondance : $f_A: x \longmapsto y$ équivaut à $x \in A$ et $f : x \longmapsto y$, on définit la réduite de f à une partie B de F, comme étant la relation $f^B : E \longrightarrow B$, qui applique la

même règle f de correspondance : $f^B : x \longmapsto y$ équivaut à $y \in B$ $f : x \longmapsto y$. On peut combiner la restriction et la réduction : $f_A^B : A \longrightarrow B$

Fonction d'un ensemble dans un autre : Soit $f : E \longrightarrow F$ une relation, on dit que c'est une fonction si tout x de E a au plus une image par f, l'ensemble des x de E qui ont des images dans F se note ***Dom***(f) domaine de définition de f, si y de F est image de x de E on note $y = f(x)$, les y de F qui ont des antécédents par f se note $f<E>$ ou ***Im***(f). On notera par $\mathcal{Fonc}$(E, F) l'ensemble des fonctions de E dans F, nous avons :

$$\mathcal{Fonc}(E, F) \subset 2^{E \times F}$$

Application d'un ensemble dans un autre : Soit $f : E \longrightarrow F$ une relation, on dit que c'est une application ssi c'est une fonction avec ***Dom***(f) = E, bref à tout x de E correspond par f un et un seul élément de F, nous noterons $\mathbf{F^E}$, l'ensemble de toutes les applications de E dans F. Une application f est dite ***injective*** si deux éléments différents x_1 et x_2 de E leurs images $y_1 = f(x_1)$ et $y_2 = f(x_2)$ sont différents. Une application f est dite ***surjective*** si tout élément y de F possède au moins un antécédent (ou image réciproque) x de E : $y = f(x)$. Une application qui est à la fois injective et surjective est dite ***bijective***, ou permutation de E, nous noterons par **E!** L'ensemble de toutes les applications bijectives de E sur E, et la relation réciproque *correspondante* est nécessairement une application, qui est de nouveau bijective. L'image d'une partie A de E se note ***f<A>*** qui est l'ensemble de toutes les images des éléments de A par f, de même si B est une partie de F, l'image réciproque de B par f se note $\boldsymbol{f^{-1}<B>}$, (la puissance -1 ne signifie pas forcément que f est bijective), c'est l'image réciproque de tous les éléments de B par f. Le plus simple des applications est l'application identique, c'est celle qui à tout x de E fait corresponde x lui-même, on note l'application identique de E dans E (ou sur E) par $\boldsymbol{Id}_E : E \longrightarrow E$.

Relation d'un ensemble dans lui-même : Soit $\mathcal{R} : E \longrightarrow E$, une relation de E dans F (qui n'est autre que E), on peut dire R est une relation sur E. Son graphe est une partie de E^2. Un lien $x \longmapsto y$. par $\mathcal{R}$ sera noté pour simplifier $x\mathcal{R}\,y$, une relation est dite ***réflexive*** si tout élément de E est relié à lui-même par $\mathcal{R}$, une relation $\mathcal{R}$ est dite ***symétrique*** si tout lien $x\mathcal{R}y$ exige le lien $y\mathcal{R}\,x$, une relation $\mathcal{R}$ est dite ***antisymétrique*** si les liens $x\mathcal{R}\,y$ et $y\ \mathcal{R}\,x$, exigent $x = y$, une relation $\mathcal{R}$ sera dite ***transitive*** si les liens $x\mathcal{R}\,y$ et $y\mathcal{R}\,z$, exigent le lien $x\ \mathcal{R}\ z$. Une relation $\mathcal{R}$ sera dite ***antiréflexive*** si on n'a aucun lien $x\mathcal{R}\,x$.

Relation d'équivalence sur un ensemble : Soit $\mathcal{R} : E \longrightarrow E$, une relation sur E, on dit que c'est une ***relation d'équivalence*** sur E, si elle est réflexive, symétrique et transitive. On notera $\mathcal{Equi}$(E) l'ensemble de toutes les relations d'équivalence sur E.

Classe d'équivalence : On note $\bar{x}$ l'ensemble $\{x' \in E \mid x'\mathcal{R}x\}$ dit classe d'équivalence de x par $\mathcal{R}$, tout élément de cette classe peut représenter cette classe.

Ensemble quotient : l'ensemble de toutes les classes d'équivalence est l'ensemble quotient de E par R noté $E/\mathcal{R} = \{\bar{x} \mid x \in E\} = \{\{x' \in E \mid x'\mathcal{R}\,x\} \mid x \in E\}$

Relation d'ordre sur un ensemble : Soit $\mathcal{R}$: E ⟶ E, une relation sur E, on dit que c'est une ***relation d'ordre*** sur E, si elle est réflexive, antisymétrique et transitive. On notera par Ord€ l'ensemble de toutes les relations d'ordres sur E.

Ordre partiel, Ordre total : Si $x\mathcal{R}y$ on dit que *x* et *y* sont ordonnées, on peut noter cette relation d'ordre par ≤ : cet ordre est ***total*** si chaque deux éléments de E sot reliés par ≤, un ***ordre partiel*** est (E, ≤) dont deux éléments au moins sont non reliés. La relation induite sur toute partie F de E est aussi un ordre sur cette partie,

Ensemble ordonné inductif, ***lemme de Zorn***: (E, ≤) est dit ***inductif*** si toute partie F de E totalement ordonné par l'ordre induit possède un ***premier élément***, c-à-d un plus petit élément, le ***lemme de Zorn*** affirme que tout ensemble (ordonné) inductif, possède un élément maximal. Dans un ensemble ordonné (E, ≤) une ***chaîne*** c'est une partie totalement ordonnée, une ***chaîne maximale*** est une partie totalement ordonnée maximale (qui n'est pas contenue strictement dans une autre partie totalement ordonnée), les chaînes maximales forment une partition de l'ensemble E, ce qui produit un ensemble quotient par la relation d'équivalence associée à cette partition. Cet ensemble quotient muni de l'ordre induit est totalement partiel, c-à-d tout élément n'est relié qu'à lui-même.

La logique bivalente : On considère $\mathcal{Q}$ l'ensemble de toutes les assertions logiques qui affirment et qui sont vraies ou fausses, on note celle qui sont vraies $\mathcal{V}$ et celle qui sont fausses $\mathcal{F}$; et on pose le principe de la ***logique bivalente*** (celle qui gère les raisonnements déployés dans les démonstrations en mathématique) : toute assertion est vraie ou fausse et pas d'autre : $\mathcal{Q} = \mathcal{V} \cup \mathcal{F}$, une assertion ne peut pas être à la fois vraie et fausse : $\mathcal{V} \cap \mathcal{F} = \varnothing$. $\mathcal{Q}$ subit donc une ***partition*** qui conduit à une relation d'équivalence, toutes les assertions vraies sont équivalentes entre elles, toutes les assertions fausses sont équivalentes entre elles, on note **1** la classe des vraies et par **0** la classe des assertions fausses. {**0**, **1**} est ***l'ensemble quotient***, et l'application h : $\mathcal{Q}$ ⟶ {**0**, **1**}, $v \in \mathcal{V} \longmapsto h(v) = \mathbf{1}$, $v \in \mathcal{F} \longmapsto h(v) = \mathbf{0}$, est appelée fonction de valeur ; sur $\mathcal{Q}$ se définit naturellement quatre opérations ***unaires*** : il suffit de les définir sur l'ensemble quotient {**0**, **1**}:

$u_1(\mathbf{0}) = \mathbf{1}$, $u_1(\mathbf{1}) = \mathbf{1}$, $u_2(\mathbf{0}) = \mathbf{0}$, $u_2(\mathbf{1}) = \mathbf{1}$, $u_3(\mathbf{0}) = \mathbf{1}$, $u_3(\mathbf{1}) = \mathbf{0}$, $u_4(\mathbf{0}) = \mathbf{0}$, $u_1(\mathbf{1}) = \mathbf{0}$,

On donne des noms à chacune de ces quatre : u_1 la ***tautologie***, u_2 l'***affirmation***, u_3 la ***négation NON*** ou ¬, u_4 l'***antilogie***.

Sur $\mathcal{A}$ se définit naturellement seize opérations ***binaires*** : il suffit de les définir sur l'ensemble quotient {**0** , **1**}: on donne les plus importants : la ***conjonction ET*** ou ∧ : notation infixe) **0∧0 = 0, 0∧1 = 0, 1∧0 = 0, 1∧1 = 1,** la ***disjonction OU*** ou ∨ : **0∨0 = 0, 0∨1 = 1, 1∨0 = 1, 1∨1 = 1,** le ***conditionnel SIALORS*** ou → : **0→0 = 1,**

0→1 = 1, 1→0 = 0, 1→1 = 1, le ***biconditionnel SSI*** ou ↔ : **0↔0 = 1, 0↔1 = 0, 1↔0 = 0, 1↔1 = 1,**

	(0,0)	(0,1)	(1,0)	(1,1)	
v1	**0**	**0**	**0**	**0**	***antilogie***
v2	**0**	**0**	**0**	**1**	***Conjonction*** ∧
v3	**0**	**0**	**1**	**0**	Non ***Conditionnel*** ┐→
v4	**0**	**1**	**0**	**0**	┐←
v5	**1**	**0**	**0**	**0**	Non ***Disjonction*** ┐∨
v6	**0**	**0**	**1**	**1**	
v7	**0**	**1**	**0**	**1**	
v8	**1**	**0**	**0**	**1**	***Biconditionnel*** ↔
v9	**0**	**1**	**1**	**0**	Non ***Biconditionnel*** ┐↔
v10	**1**	**0**	**1**	**0**	
v11	**1**	**1**	**0**	**0**	
v12	**0**	**1**	**1**	**1**	***Disjonction*** ∨
v13	**1**	**0**	**1**	**1**	←
v14	**1**	**1**	**0**	**1**	***Conditionnel*** →
v15	**1**	**1**	**1**	**0**	Non ***Conjonction*** ┐∧
v16	**1**	**1**	**1**	**1**	***tautologie***

Les Structures algébriques:

Ensemble des lois de composition sur E : Soit E un ensemble, une loi de composition sur E est une fonction $\tau : E^2 \longrightarrow E$, de E^2 dans E, si elle n'est pas une application, on l'appelle loi de composition interne non partout définie sur E.

Donc $\mathcal{Fonc}(E, E^2)$ est l'ensemble de toutes les lois de composition sur E.

Ensemble des lois de compositions internes sur E : Soit E un ensemble, une loi de composition sur E est une fonction de E^2 dans E, une loi de composition interne sur E est une application $\tau : E^2 \longrightarrow E$, de E^2 dans E.

Donc $\mathbf{E}^{E^2}$ est l'ensemble de toutes les lois de composition internes sur E.

Rq : $\mathcal{Fonc}(E, E^2) \backslash \mathbf{E}^{E^2}$ est l'ensemble des lois de composition sur E non partout définies

Magma : Soit E un ensemble, et $\tau : E^2 \longrightarrow E$, une loi de composition interne sur E, le couple ordonné (E, τ) est appelé Magma définie sur E par la loi τ.

Morphisme de magma : un ***morphisme*** d'un magma (E, τ) dans un autre (E', τ') est une application $f : E \longrightarrow E'$, qui vérifie : pour tout x_1 et x_2 de E on a $f(x_1 \tau x_2) = f(x_1) \tau' f(x_2)$.

Sous-magma : Un ***sous-magma*** de (E, τ) est une partie A de E tel que la restreinte réduite $\tau_{A^2}^{A}$: $A^2 \longrightarrow A$ (on dit restriction pour simplifier) de τ : $E^2 \longrightarrow E$ à A^2 et A est bien une application (donc une loi de composition interne sur A).

On remarque que l'image d'un sous-magma par un morphisme de magmas est un sous-magma, et que l'image réciproque d'un sous-magma par un morphisme de magma est un sous-magma. Tout magma est sous-magma de lui-même. L'application identique d'un magma dans lui-même est un morphisme de ce magma dans lui-même $x \longmapsto x$. L'application $x \longmapsto a\tau x$ est dite translation à gauche par *a*, et $x \longmapsto x\tau a$ est dite translation à droite par *a*. Un élément *a* d'un magma (E, τ) est dit ***simplifiable à droite*** si : pour tous x et y de E on a : $x\tau a = y\tau a \implies x = y$. (ceci signifie que la translation à droite par a est injective), il est dit ***simplifiable à gauche*** si : pour tous *x* et *y* de E on a : $a\tau x = a\tau y \implies x = y$. (ceci signifie que la translation à gauche par a est injective). Il est dit ***simplifiable*** s'il est simplifiable à gauche et à droite. (Ceci signifie que les translations à droite et à gauche par *a* sont injectives.)
On appelle ***isomorphisme*** d'un magma (E, τ) dans un autre (E', τ'), tout ***morphisme bijectif*** de (E, τ) dans (E', τ'), $\boldsymbol{Id_E}$ est un isomorphisme de (E, τ) dans lui-même, on dit alors que c'est un ***automorphisme*** du magma (E, τ). Soit (E, τ) un magma on dit que la loi est ***associative*** si pour tous *x*, *y* et *z* on a : $(x\tau y)\tau z = x\tau(y\tau z)$.

Semi groupe : Un ***semi-groupe*** est un magma dont la loi est associative, un morphisme de ***semi-groupes*** (E, τ) et (E', τ'), est un morphisme vis-à-vis des structures de magma sous-jacentes. Un ***sous-semi-groupe*** d'un semi-groupe, est un sous-magma de celui-ci, tout sous-magma d'un semi-groupe en est un. Un élément ***e*** d'un magma (E, τ) est dit ***neutre à droite*** si pour tout *x* de E on a $x\tau e = x$, ***e*** est dit ***neutre à gauche*** si pour tout *x* de E on a $e\tau x = x$, il est dit neutre s'il est neutre à droite et à gauche. Si un magma possède un neutre e celui-ci est unique : (si e et e' sont deux neutre alors : $e\tau e' = e = e'$).

Demi-groupe : Un magma est appelé ***demi-groupe*** si ce magma possède un neutre *e* ; un morphisme f de ***demi-groupes*** est un morphisme de la structure de magma sous-jacente et qui vérifie : l'image du neutre est le neutre. Donc $f(x\tau y) = f(x)\ \tau' f(y)$ et $f(e) = e'$. On définit le noyau de f comme étant $\boldsymbol{ker}(f) = \{x \in E \mid f(x) = e'\}$.

Monoïde : Un ***monoïde*** est un magma qui est à la fois semi-groupe et demi-groupe, en d'autres termes loi interne associative avec un neutre. Soit *a* un élément d'un ***demi-groupe*** (E, τ) de neutre *e*, un élément a' est dit symétrique à droite de *a* si $a\tau a' = e$, un élément *a*'' est dit symétrique à gauche de *a* si $a''\tau\, a = e$, un élément symétrique de *a* de gauche et de droite est appelé ***élément symétrique*** de *a*, et on le note ***sym***(a), on dit alors que *a* est symétrisable ; si *a* et *b* sont ***symétrisables***, il est simple de vérifier la formule : $\boldsymbol{sym}(a\tau b) = \boldsymbol{sym}(b)\ \tau\ \boldsymbol{sym}(a)$. On note par ***sym***(E) l'ensemble des éléments ***symétrisables*** de E

La structure de groupe : Un ***groupe*** est un monoïde (G, τ) dont tout élément est inversible. Si (E, τ) est monoïde (***sym***(E), τ'), τ' est la loi induite de τ sur ***sym***(E), est

un groupe. Un ***sous–groupe*** de (G, τ) est une partie H de G sur laquelle la loi induite du groupe forme un groupe, on note $H \leq G$. Soit H un sous-groupe de (G, τ), pour tout x de G on définit $xH = \{xh \in G \mid h \in H\}$ dite la ***classe à droite*** de x par H, et $Hx = \{hx \in G \mid h \in H\}$dite la ***classe à gauche*** de x par H. xH et Hx ne sont pas égales en général, H définit sur G deux relations $x \backsim y \iff y \in xH$, et $x \sim y \iff y \in Hx$ ce sont deux relations d'équivalence sur G, les ensembles quotients $G/\backsim$ et $G/\sim$ n'ont pas la structure de groupe ($xHyH$ n'es pas égale à xyH). Il y a des sous-groupes H où $xH = Hx$ pour tout x de G, de tels sous-groupes sont dits ***distingués*** ou ***caractéristiques***, On note $H \triangleleft G$. Pour de tels sous-groupes les deux relations d'équivalences sont identiques aboutissant à un même ensemble quotient $G/\backsim = G/\sim$ qui sera noté G/H. appelé groupe quotient dont la loi quotient est $\bar{x}\,\tau\,\bar{y} = \overline{x\tau y}$, soit (G, τ) un groupe et a un élément quelconque de G, l'application $\varphi_a : G \longrightarrow G$, $x \longmapsto axa^{-1}$ est un automorphisme appelé ***automorphisme intérieur*** par a. On note ***Aut***(G) l'ensemble des ***automorphismes,*** de (G, τ), et ***Int***(G) l'ensemble des ***automorphismes intérieur***s de (G, τ). (***Aut***(G), $\circ$) est un groupe, et (***Int***(G), $\circ$) est un sous-groupe de (***Aut***(G), $\circ$). On remarque que tout sous-groupe distingué de (G, τ) est invariant par tout automorphisme intérieur.

Les cardinaux : On définit sur la classe $\mathcal{Ens}$ la relation : pour tous A et B des ensembles, $A \backsim B \iff$ (il existe une application bijective de A sur B); il est facile à démontrer que $\backsim$ est réflexive et transitive, (la preuve qu'elle est symétrique est plus compliquée : ***Bernstein***); l'ensemble quotient $\mathcal{Ens}/\backsim$ est l'ensemble des classes des éléments A de $\mathcal{Ens}$, la classe de A dans cette relation d'équivalence est noté ***Card***(A), le ***cardinal*** de A, $\mathcal{Ens}/\backsim$ est noté $\mathcal{Card} = \{\text{card}(A) \mid A \in \mathcal{Ens}\}$. La classe de {} : ***Card***({}) est notée 0, la classe de {0} : ***Card***({0}) est noté 1, la classe de {0,1} : ***Card***({0 ;1}) est noté 2, par récurrence la classe de {0,1, 2,…., $n-1$}sera noté n, ($n-1$ la classe qui vient après $n-2$) on note par $\mathbb{N}$ l'ensemble des ***cardinaux*** (classes) des ensembles finis : {0, 1, 2,…., n,….} sera noté $\mathbb{N}$ et appelé l'ensemble des entiers naturels (à prouver que c'est bien un ensemble). On définit sur $\mathcal{Card}$ une addition : si α = ***Card***(A) et β = ***Card***(B), on définit $\alpha + \beta$ comme étant ***Card***$(A \times \{0\} \cup B \times \{1\})$ il n'est pas difficile de prouver que cette addition est une loi de composition interne sur $\mathcal{Card}$, qu'elle est associative commutative de neutre 0, ($\mathcal{Card}$, +) est donc un monoïde. On définit sur $\mathcal{Card}$ une multiplication : si α = ***Card***(A) et β = ***Card***(B), on définit $\alpha\beta$ comme étant ***Card***$(A \times B)$ il n'est pas difficile de prouver que cette multiplication est une loi de composition interne sur $\mathcal{Card}$, qu'elle est associative commutative de neutre 1, ($\mathcal{Card}$, $\bullet$) est donc un monoïde (on note xy ou $x.y$ au lieu de $x \bullet y$). Les restrictions de cette addition et cette multiplication à $\mathbb{N}$ font de $\mathbb{N}$ des monoïdes ($\mathbb{N}$, +) et ($\mathbb{N}$, $\bullet$) on remarque aussi que dans $\mathcal{Card}$, $\bullet$ est ***distributive*** par rapport à + : α, β et γ trois cardinaux : $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$. Dans les

monoïdes ($\mathbb{N}$, +) et ($\mathbb{N}$, •) tout élément est simplifiable, mais ce n'est pas le cas dans les monoïdes ($\mathcal{Card}$, +) et ($\mathcal{Card}$, •). Soit α = ***Card***(A) et β = ***Card***(B), on définit le cardinal : α^{β} comme étant ***Card***(B^A) (où B^A est l'ensemble des applications de A dans B) on trouve toutes les propriétés de l'***exponentiation*** : $\alpha^{\beta+\gamma} = \alpha^{\beta}\alpha^{\gamma}$, $(\alpha^{\beta})^{\gamma} = \alpha^{\beta\gamma}$, $(\alpha\beta)^{\gamma} = \alpha^{\gamma}\beta^{\gamma}$.

Les ordinaux : Deux ensemble ordonnés (E, $\leq$) et (F, $\preccurlyeq$) sont dit semblables s'il existe une bijection croissante de l'un sur l'autre : $x \leq y \implies f(x) \preccurlyeq f(y)$. On définit d'abord les ensembles ***bien ordonnés***, une relation d'ordre $\preccurlyeq$ sur un ensemble E est un ***bon ordre*** si toute partie A de E possède un ***plus petit élément***, (dit aussi un ***premier élément*** : c'est un élément de A qui est plus petit que tous les éléments de A). Ainsi l'ordre induit d'un bon ordre sur toute partie A de E est de nouveau un bon ordre. Un exemple ($\mathbb{N}$, $\leq$) est un ensemble bien ordonné (par l'ordre naturel) les ordres induits sur {0, 2, 4, 6,…..} et {1, 3, 4, 6,…..} sont aussi des ***bons ordres***, on suppose qu'un ensemble bien ordonné est écrit dans l'ordre croissant de ses termes, c'est-à-dire si un élément *a* est écrit à gauche de *b* ceci signifie que $a \leq b$, ainsi on peut définir une ***juxtaposition*** ($\vee$) de deux ensembles disjoints bien ordonnés, en écrivant le second à gauche du premier (ceci signifie que tout élément du premier est plus petit que tout élément du second) par exemple : {0, 2, 4, 6,…..}$\vee${1, 3, 4, 6,…..} = {0, 2, 4, 6,…..,1, 3, 4, 6,…..} C'est le même ensemble que $\mathbb{N}$ mais ce n'est pas le même ordre, (l'ordre naturel de $\mathbb{N}$). La réunion d'une famille bien ordonnée d'ensembles disjoints deux à deux biens ordonnés est bien ordonné, (à bien définir ce bon ordre), tous les ensembles finis ***totalement ordonnés*** sont ***bien ordonnés***, tous les ensembles ***finis*** totalement ordonnés ayant le même nombre d'éléments sont ***semblables*** entre eux. C'est le moment de définir le principe ***d'induction mathématique*** : Toute partie S de $\mathbb{N}$ qui contient 0 et que, si *n* appartient à S alors *n*+1 appartient aussi à S, alors S = $\mathbb{N}$. Et le principe ***d'induction transfinie*** : si ***e*** est le premier élément d'un ensemble ***bien ordonné*** E, S partie de E telle que e appartient à S et, si *n* appartient à S alors *n* +1 appartient aussi à S ; alors S = E. on comprend les mots ***prédécesseur immédiat*** et ***successeur immédiat*** par exemple ; dans l'ensemble bien ordonné {0, 2, 4, 6,…..,1, 3, 4, 6,…..} seulement 0 et 2 n'ont pas de prédécesseurs immédiats, mais on peut dire que dans un ensemble bien ordonné, seulement le dernier élément n'a pas de successeur. Un élément w d'un ensemble bien ordonné E est dit un ***point limite***, s'il n'a pas un prédécesseur immédiat, et s'il n'est pas le premier élément, (dans l'exemple précédent 1 est un point limite, mais pas 0), on définit le ***segment initial*** d'un élément *a* d'un ensemble E bien ordonné, (s(*a*) est l'ensemble des éléments de E qui précèdent ***strictement*** a). Une partie F d'un ensemble bien ordonné E, est semblable à E s'il existe une application *f* de E dans F tel que $a \leq f(a)$, deux ensembles bien ordonnés E et F sont semblables, alors il y a une seule application de ***similitude*** de E sur F. la similitude entre E et F est une relation d'équivalence, la classe d'un ensemble ordonné, se note ***ord(E)***, sur la classe des ensemble ordonnés, parmi les quels les ensembles bien ordonnés. La classe λ = ***ord***(E) d'un ensemble bien ordonné E est appelée ***nombre ordinal***. On note 0, 1, 2, 3, …. Les nombre ordinaux des ensembles finis, {}, {1}, {1, 2},{1, 2, 3},…… il sont appelés les ***ordinaux finis***,

tous les autre ordinaux sont appelés ***ordinaux transfinis***. ω = ***ord***($\mathbb{N}$) est un ordinal transfini, du fait que $\mathbb{N}$ est bien ordonné et infini. On définit de nouveau une relation d'ordre sur les ordinaux, $\lambda \precsim \mu$ ssi λ = ***ord***(E) et μ = ***ord***(F) E est semblable à un segment initial de B. (ou en particulier semblable à B) c'est bien une relation d'ordre, et cet ordre est total. ω = ***ord***({0, 2, 4, 6,…..}) = ***ord***({0, 1, 3, 4,…..}) $\prec$ ***ord***({0, 2, 4, 6,…..,1, 3, 4, 6,…..}).

Les groupes commutatifs : Soit (G, +) un groupe commutatif, dont le neutre est noté 0 et le symétrique de x est noté $-x$, un tel groupe est appelé ***abélien***. $\mathbb{Z}_n$ (ensemble des congruences modulo *n* dans $\mathbb{Z}$) est un groupe abélien pour tout entier naturel *n*, Soit H un sous-groupe de (G, +), il est abélien, on définit les classes des éléments x de G par H : xH = {$xh \in$ G | $h \in$ H}, on a bien xH = Hx, une relation R_H, par H sur G est ; x R_H y équivaut à $y - x \in$ H, c'est une relation d'équivalence sur G, dont l'ensemble quotient sera noté G/H. la classe de x par R_H est $\bar{x}$ = xH = Hx. On définit sur G/H une loi ***induite*** : $\bar{x} + \bar{y} = \overline{x+y}$, on remarque que (G/H, +) est un groupe abélien. L'application p : G $\longrightarrow$ G/H, $x \longmapsto \bar{x}$ est un morphisme de groupes surjectif appelé ***projection***, dont le noyau ***ker***(p) vaut H. Soit f : G $\longrightarrow$ G' un morphisme entre deux groupes commutatifs, f induit un ***isomorphisme*** $\bar{f}$: G/***ker***(f) $\longrightarrow$ ***Im***(f).

La structure d'anneau : Un anneau est un triplet ordonné (A, +, •) d'un ensemble A et de deux lois de compositions internes sur A : + une ***première*** loi, et • une ***deuxième*** loi; (A, +) est un groupe commutatif de neutre 0, (A, •) est un monoïde dont le neutre est 1, et • est ***distributif*** par rapport à + ; Si la ***deuxième*** loi • est commutative, l'anneau sera dit commutatif ; un anneau contient au moins 0 et 1, si 0 = 1 il est obligatoirement réduit à un singleton. 0a = 0 pour tout a de l'anneau. ($\mathbb{Z}$, +, •) est un anneau commutatif. B une partie de A, on dit que B est un sous-anneau de A si (B, +) est un sous –groupe de (A, +), (B, •) est un sous-monoïde de (A, •), un morphisme de l'anneau (A, +, •) dans l'anneau (B, +, •) est une application f : A $\longrightarrow$ B qui est morphisme du groupe (A, +) dans le groupe (B, +), et morphisme du monoïde (A, •) dans le monoïde (B, •). La caractéristique d'un anneau A est le plus petit entier strictement positif n tel que n1 = 1 + 1 + …. + 1 (n fois) = 0, si ce n n'existe pas on dit que a est de caractéristique 0. ($\mathbb{Z}_p$, +, •) est de caractéristique p, ($\mathbb{Q}$, +, •), ($\mathbb{R}$, +, •), ($\mathbb{C}$, +, •) sont de caractéristique 0.

La structure de corps : Un corps est un anneau (K, +, •) dont tout élément non nul est inversible, il est commutatif si la deuxième loi est commutative, ($\mathbb{Q}$, +, •), ($\mathbb{R}$, +, •), ($\mathbb{C}$, +, •)

Sont des corps commutatifs infinis, ($\mathbb{Z}_p$, +, •) où p est un nombre premier naturel est un corps commutatif fini.

La structure de A-mod (module sur un anneau A) : on appelle ***A-module-à-droite*** tout triplet ordonné (E, A, φ) où (E, +) est un groupe commutatif, (A, +, •) est un anneau et, φ est un élément de E^{AxE} (une application de A × E dans E appelée une loi externe : φ(*a,x*) se note *ax*) vérifiant : **MOD1** : $(a + b)x = ax + bx$, **MOD2** : a(x + y) = $ax + ay$, **MOD3d** : $a(bx) = (ba)x$ **MOD4** : $1x = x$. (E, A, φ) est un ***A-module-à-gauche*** si : **MOD1** : (a + b)x = ax + bx, **MOD2** : $a(x + y) = ax + ay$, **MOD3g** : $a(bx) = (ab)x$ **MOD4** : $1x = x$. ***A-module-à-droite*** et ***A-module-à-gauche*** seront synonymes si (A, +, •) est un anneau commutatif.

La structure de K-ev (espace vectoriel sur un corps K) : on appelle ***K-espace-vectoriel*** tout triplet ordonné (E, K, φ) où (E, +) est un groupe commutatif, (K, +, •) est un corps commutatif et, φ est un élément de E^{KxE} (une application de K × E dans E appelée une loi externe : φ(*a,x*) se note *ax*) vérifiant : **EV1** : $(a + b)x = ax + bx$, **EV2** : $a(x + y) = ax + ay$, **EV3** : $a(bx) = (ba)x$ **EV4** : $1x = x$.

La structure de K-alg (algèbre sur un corps K) : On appelle ***K-algèbre*** tout K-ev (A, K, φ) où (A, +, •) est un anneau, (K, +, •) est un corps commutatif et, φ est un élément de A^{KxA} (une application de K × A dans E appelée une loi externe : φ(a,x) se note ax) vérifiant : **ALG1** : $a(x + y) = ax + ay$, **ALG2** : $a(xy) = (ax)y = x(ay)$. Cette algèbre est commutative si (A, +, •) est un anneau commutatif. Pour tous réels a, b avec $a < b$, $\mathbb{R}^{[a,b]}$ est une ℝ-alg. Soit a un élément du K-ev E, aK est l'ensemble $\{\alpha a \in E \mid \alpha \in K\}$ ***ensemble engendré*** par a, si $a = 0$, Ka est réduit à {0}, si a n'est pas nul, Ka est appelé ***droite vectorielle***, c'est l'ensemble des vecteurs colinéaires à a, et c'est un sous-K-ev de E. Soit $A = \{a_1, a_2, a_3, \ldots, a_{n-1}, a_n\}$ un sous ensemble fini de E, On note [A] ou $Ka_1 + Ka_2 + Ka_3 + \ldots + Ka_{n-1} + Ka_n$, (Ou indifféremment $a_1K + a_2K + a_3K + \ldots + a_{n-1}K + a_nK$ si le corps K est commutatif) l'ensemble $\{\alpha_1a_1 + \alpha_2a_2 + \alpha_3a_3 + \ldots + \alpha_{n-1}a_{n-1} + \alpha_na_n \mid \alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_{n-1}, \alpha_n \in K\}$ c'est l'ensemble engendré par A, on remarque que [A] est un sous-K-ev de E appelé le sous-K-ev des ***combinaisons linéaires*** des éléments de A. ON définit ***Vect***(A) comme étant l'intersection de tous les sous-K-ev F de E contenant A, on voit que ***Vect***(A) est l'***intersection*** de tous les sous-K-ev contenant A, et qu'il est lui-même un sous-K-ev de E, on l'appelle sous-K-ev ***engendré*** par A. On remarque aussi que [A] = ***Vect***(A), le sous-K-ev des combinaisons linéaires de A n'est autre que le sous-K-ev engendré par A, (ceci reste vrai si A est un ensemble infini, où une combinaison linéaire est une combinaison linéaire d'un nombre fini de A.) On dit que E est ***engendré*** par A si ***Vect***(A) = E. D'autre part un ensemble fini $A = \{a_1, a_2, a_3, \ldots, a_{n-1}, a_n\}$ de E est dit libre, si toute combinaison linéaire nulle de A, est constituée par des coefficients tous nuls, autrement dit il n'y a de combinaison linéaire nulle de A que $0a_1 + 0a_2 + 0a_3 + \ldots + 0a_{n-1} + 0a_n$ ceci reste vrai pour une partie A infini de E, à condition de prendre toutes les combinaisons linéaires de toutes les parties finie de A), si A est libre on dit aussi ***linéairement indépendants***. Un sous-ensemble B générateur et linéairement indépendant est appelé une ***Base***. On admet que tout K-ev a une base, et que toutes les bases ont même cardinal, dans le cas où B est une base fini de cardinal n, on dit que E est de ***dimension*** n. et ***dim***(E) = n. Si $\boldsymbol{e} = \{e_1, e_2, e_3, \ldots, e_{n-1}, e_n\}$ est une base de E, les sous-K-ev F_k = ***Vect***$(e_1, e_2, e_3, \ldots, e_{k-1}, e_k)$ sont des sous espaces emboîtés, chacun a

une dimension supérieure à son précédent d'une unité : $\{0\}= F_0 \leq F_1 \leq F_2 \leq F_3 \leq \ldots..\leq F_{n-1} \leq F_n = E$, on dit que c'est un ***drapeau*** de E.

Les applications linéaires entre espaces vectoriels : une application linéaire f d'un K-ev E dans un autre F, est un morphisme, $f : E \longrightarrow F$, $x \longmapsto f(x)$, c'est-à-dire : $f(\alpha x + y) = \alpha f(x) + f(y)$. On remarque que l'image par toute application linéaire d'un ***sous-K-ev*** de E est un ***sous-K-ev*** de F, c'est vrai aussi pour l'image réciproque d'un sous-K-ev de F, en particulier ***ker***(*f*) et ***Im***(*f*) sont des sous-K-ev. Si E est de ***dimension*** finie, ***ker***(*f*) et ***Im***(*f*) sont de dimension finie et on note la ***nullité*** de *f* : ***null***(f) = ***dim***(***ker***(f)) et ***rg***(*f*) = ***dim***(***rg***(*f*)) le ***rang*** de f, on remarque que : ***dim***(***ker***(*f*)) + ***dim***(***rg***(*f*)) = ***dim***(E), ***null***(*f*) + ***rg***(*f*) = ***dim***(E).

Les formes linéaires : Une forme linéaire f sur K-ev E, est un morphisme, $f : E \longrightarrow K$, $x \longmapsto f(x)$, on note E* l'ensemble de toutes les formes linéaires sur E, c'est un K-ev, si E est de dimension finie, et $\boldsymbol{e} = \{e_1, e_2, e_3,\ldots..,e_{n-1}, e_n\}$ une base de E, soit $x = \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 + \ldots..+ \alpha_{n-1} e_{n-1} + \alpha_n e_n$ un élément de E, l'application $e_i^* : E \longrightarrow F$, $x \longmapsto \alpha_i$, est une forme linéaire $e_i^*(e_i) = 1$ et $e_i^*(e_j) = 0$ pour j différent de i. $e^* = \{e_1^*, e_2^*,\ldots., e_n^*\}$ est une base de E* dite ***base duale*** de ***e***, donc ***dim***(E*) = ***dim***(E) = *n*.

Les matrices : On note $\mathbf{M}_K(n, p)$ l'ensemble des tableau rectangulaire à n lignes et p colonnes à éléments dans le corps K(ou plus généralement un anneau A à la place de K), on définit sur $\mathbf{M}_K$ l'ensemble de toutes les matrices à coefficients dans K, une additions et une multiplication qui ne sont pas partout définies, un produit par un élément du corps (on dit produit par un scalaire) qui est partout définie. $\mathbf{M}_K(n, p)$ est un K-ev. $\mathbf{M}_K(n, n)$ est noté $\mathbf{M}_K(n)$ est l'ensemble des matrices carrée de taille *n*, c'est un anneau non commutatif qui contient ($n > 1$) des diviseurs de zéro.

Exercices sur les groupes

1) Soit (E, T) un magma associatif (*T loi interne associative*)

i) Démontrer que si *a* et *u* sont deux éléments de E tels que $\gamma_a : E \longrightarrow E$, $x \longmapsto a\mathrm{T}x$ est une application surjective. Si *u* est un élément de E tel que $u\mathrm{T}a = a$ alors :

$$\forall x \in E \quad x = u\mathrm{T}x$$

ii) Si $a \in E$ et si $\gamma_a : E \longrightarrow E$, $x \longmapsto a\mathrm{T}x$ et $\delta_a : E \longrightarrow E$, $x \longmapsto x\mathrm{T}a$ sont surjectifs, alors (E,T) possède un neutre (*autrement dit (E,T) devient un* ***monoïde***)

iii) Si $a \in E$ et si $\gamma_a : E \longrightarrow E$, $x \longmapsto a\mathrm{T}x$ et $\delta_a : E \longrightarrow E$, $x \longmapsto x\mathrm{T}a$ sont surjectifs, alors $\forall x \in E$, x est symétrisable (autrement *dit (E, T) devient un groupe*)

iv) Supposons que (E, T) possède un neutre et que E est fini, montrer que tout élément régulier est symétrisable.

2) Soit (G, •, *e*) un groupe et $A \subset G$, on définit :
$A^{-1} = \{a^{-1} \in G \mid a \in A\}$

$\forall x, y \in G$: $xAy = \{xay \in G \mid a \in A, b \in B\}$
$A, B \subset G$: $AB = \{ab \in G \mid a \in A, b \in B\}$

i) On suppose que G est ordonné par $\leq$ et vérifiant :

$\forall$ a, b, c $\in G$: $a \leq b \Longrightarrow (ac \leq bc$ et $ca \leq cb)$

Soit $P = \{x \in G \mid x \geq e\}$ (on convient $x \geq y \iff y \leq x$)

a) Montrer que $P^{-1} = \{x \in G \mid x \leq e\}$

b) Montrer que : $P \bigcap P^{-1} = \{ e \}$, $PP \subset P$, et $\forall a \in G$: $aPa^{-1} \subset P$

c) Montrer que si $\leq$ est un ordre total alors $P \bigcup P^{-1} = G$.

ii) Réciproquement, on suppose que $\exists P \subset G$, $P \neq \{e\}$, vérifiant :
$P \bigcap P^{-1} = \{ e \}$, $PP \subset P$, et $\forall a \in G$: $aPa^{-1} \subset P$

On définit £ par : $a \leq b \iff ba^{-1} \in P$.

a) Montrer que $\leq$ est une relation d'ordre.

b) Montrer que $\forall a, b, c \in G$: $a \leq b \Longrightarrow (ac \leq bc$ et $ca \leq cb)$
Montrer que si $P \bigcup P^{-1} = G$, alors $\leq$ est une relation d'ordre ***totale***.

3) Soit (G, **.**, *e*) un groupe (non commutatif) et $H \lhd G$, on suppose qu'il existe $f : G \longrightarrow H$ un morphisme de groupe tel que : $\forall x \in H$, $f(x) = x$ (H est stable par f, même invariant point par point).
Montrer que G est ***isomorphe*** à $(G/H) \times H$.

4) ***a***) Montrer que tout sous-groupe d'un groupe monogène est monogène.
b) En déduire que tout sous-groupe d'un groupe cyclique est cyclique.
(***N.B***. *G monogène signifie qu'il est infini et engendré par un seul élément*)

5) Montrer que tout groupe fini d'ordre premier est cyclique, et il est engendré par chacun de ses éléments distincts du neutre.

6) Montrer que tout sous-groupe d'un groupe monogène est monogène.

7) Soit (G, **.**) un groupe d'ordre 4 dont on désigne par e l'élément neutre.
a) Montrer que G est cyclique ou tout élément de g est d'ordre 2.
b) En déduire que g est commutatif et que : $G = \mathbb{Z}/4\mathbb{Z}$ ou $G = ((\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}), +)$

8) Soit (G, +) un groupe abélien de neutre 0, $H_1 \leq G$ (H_1 sous-groupe de G) et $H_2 \leq G$ tel que :

$$G = H_1 + H_2 = \{ x_1 + x_2 \mid x_1 \in H_1 \text{ et } x_2 \in H_2\} \quad (\boldsymbol{s})$$

a) Montrer que les deux assertions suivantes sont équivalentes :
i) Tout x de G s'écrit d'une façon unique $x = x_1 + x_2$ tel que $x_1 \in H_1$ et $x_2 \in H_2$.
ii) $H_1 + H_2 = \{0\}$
Si (***s***) et (***i***) ou ***ii***)) sont vérifiées on écrit $G = H_1 \oplus H_2$.

b) On suppose que $G = H_1 \oplus H_2$. Montrer que :
i) G est isomorphe à $(H_1 \times H_2, +)$.
ii) $G/H_1 = H_2$ et $G/H_2 = H_1$.

9) soit (G, +) un groupe abélien de neutre 0.

a) Soit f un endomorphisme de (G,+) vérifiant : $f \circ f = f$. Montrer que G = Im(f) $\oplus$ Ker(f).

b) Réciproquement, soit H, N $\leq$ G tels que G = H $\oplus$ N. Montrer qu'il existe un endomorphisme f de G tel que $f \circ f = f$, Im(f) = H , Ker(f) = N.

c) Soit $G = (\mathbb{Z} \times \mathbb{Z}, +)$, $H = \mathbb{Z} \times \{0\}$, $H = \{0\} \times \mathbb{Z}$.

i) Montrer que G = H $\oplus$ N.

ii) Déterminer un endomorphisme f de G tel que : $f \circ f = f$, Im(f) = H , Ker(f) = N.

10) Soit (G, $\bullet$) un groupe de neutre e, et vérifiant $\forall x, y \in G : (xy)^2 = x^2y^2$.

On pose $G^{(2)} = \{x^2 \in G \mid x \in G\}$ et $G_{(2)} = \{x \in G \mid x^2 = e\}$

i) Montrer que $G^{(2)}$ et $G_{(2)}$ sont deux sous-groupes distingués de G.

ii) On considère l'application $\theta : G \longrightarrow G^{(2)}$, $x \longmapsto x^2$

a) Montrer que θ est un morphisme de groupes surjectif.

b) Déterminer Ker(θ).

c) montrer que $G_{(2)}$ est commutatif.

d) Déduire que $G^{(2)} \approx G/G_{(2)}$.

11) Soit (G, $\bullet$) un groupe de neutre e, $H_1 \leq G$ et $H_2 \leq G$ tel que $G = H_1 \bullet H_2$.

i) Montrer que les deux assertions suivantes sont équivalentes :

a) $\forall x \in G$: x s'écrit d'une façon unique $x = x_1x_2$ avec $x_1 \in H_1$ et $x_2 \in H_2$.
$\forall x_1 \in H_1$ et $\forall x_2 \in H_2$: on a $x_2x_1 = x_1x_2$.

b) $H_1 \lhd G$ et $H_2 \lhd G$ et $H_1 \cap H_2 = \{e\}$

ii) Montrer que l'une des deux assertions équivalentes de ***i***) implique $G \approx H_1 \times H_2$.

12) Soit (G, $\bullet$) un groupe de neutre e, et (G', $\bullet$) un groupe de neutre e', (*il n'y aura pas d'ambiguïté sur les lois de compositions*) soit $f : G \longrightarrow G'$ un morphisme de groupes.

i) Montrer que si $X \lhd G$, alors $f(X) \lhd G'$.

ii) Montrer que $Y' \lhd G'$, alors $f^{-1}(X') \lhd G$.

13) Soit (G, $\bullet$) un groupe de neutre e, et (G', $\bullet$) un groupe de neutre e', soit $f : G \longrightarrow G'$ un morphisme de groupes, N = Ker(f).

i) On suppose que $H' \lhd G'$.

a) Montrer que $H = f^{-1}(H') \lhd G$ et $N \lhd G$.

b) Si f est surjectif : H'= f(H) et $H/N \approx H'$.

ii) Soit $K \lhd G$ et K'= f(K).

a) Montrer que $f^{-1}(K') = K \iff N \subset K$

b) Si f est surjective et $K \lhd G$. Montrer que $K' = f(K) \lhd G'$

14) Soit $H \lhd G$ avec $|H| = p$, $|G| = n$, quel est l'ordre de G/H.

15) Soit (G, $\bullet$) un monoïde de neutre e, on appelle centre de G l'ensemble

$$Z = \{a \in G \mid \forall x \in G, ax = xa\}$$

i) Montrer que Z est un sous-monoïde de G. (monoïde pour la loi de composition induite : il suffit de montrer que la loi induite est interne)

ii) Montrer que si G est un groupe, alors Z est un sous-groupe distingué de g.

iii) Quel est le noyau de $\varphi : G \longrightarrow \mathcal{Int}(G)$, $a \longmapsto f_a$. ($f_a(x) = a^{-1}xa$)

iv) A quelle condition φ est un isomorphisme ?
v) Quel est le centre Z du monoïde $(E^E, \circ)$ des applications de E dans E.

16) Soit G, G' deux groupes multiplicatifs de neutres respectifs e et e, on définit dans $G \times G'$ la loi : $(a, a') \bullet (b, b') = (ab, a'b')$
i) Montrer que $G \times G'$ est un groupe pour cette loi, dit groupe produit.
ii) On considère les applications

$$f : G \longrightarrow G \times G',\ a \longmapsto (a, e'),\ \text{et}\ g : G' \longrightarrow G \times G',\ b \longmapsto (e, b),\ \text{et}$$

Démontrer que f et g sont des ***monomorphismes*** (*morphismes injectifs*) et leurs images Im(*f*) et Im(*g*) sont des sous-groupes distingués de $G \times G'$.
iii) Montrer que tout élément de *f*(G) commute avec tout élément de *g*(G'), et que tout élément z de $G \times G'$ se décompose en $z = z_1.z_2$ avec $z_1 \in f(G)$, $z_2 \in g(G')$, et que cette décomposition est unique.

17) Soit G, un groupe, et A une partie de G, on appelle centralisateur de A le sous-ensemble : $Z(A) = \{x \in G \mid \forall a \in A, ax = xa\}$
i) Démontrer que $Z \leq Z(A) \leq G$.
ii) Démontrer que $Z(\boldsymbol{gp}(A)) = Z(A)$ (où ***gp***(A) est le sous-groupe engendré par A)
iii) Démontrer que $H \lhd G \implies Z(H) \lhd G$.

18) Soit G un groupe, à tout couple (a,b) f'éléments de g on associe $[a,b] = aba^{-1}b^{-1}$ que l'on nomme ***commutateur*** de a et b :

$$[ab]ba = ab$$

On note C l'ensemble des commutateurs des éléments de G, et G'= ***gp***(C) dit groupe dérivé de G.

i) Montrer que $(\boldsymbol{gp}(C) \subset H \leq G) \implies H \lhd G$.

ii) Soit $f : G \longrightarrow G'$ un morphisme de groupes, montrer que f(G) est commutatif si et seulement si $\boldsymbol{gp}(C) \subset \ker(f)$.

iii) Soit $H \lhd G$, .montrer que : (G/H commutatif) $\iff$ $(\boldsymbol{gp}(C) \subset H)$

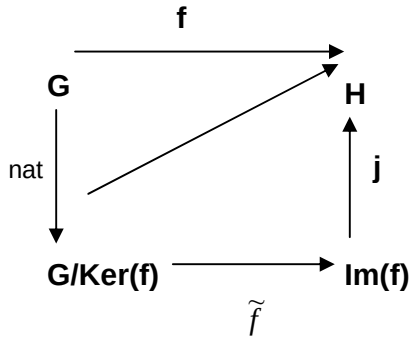
Groupes

Suites de composition

On note $\mathcal{G}$ la classe de tous les groupes, $\mathcal{AG}$ la sous-classe des groupes abéliens (commutatifs). $\mathbb{Z}$ L'anneau intègre des entiers rationnels, n étant un entier positif $\mathbf{C}_n = \mathbb{Z}/n = \{0, a, 2a, \ldots, (n-1)a\}$ le groupe cyclique d'ordre n. $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ le groupe ou l'anneau quotient des entiers modulo n.

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n.$$

Soit G, H$\in \mathcal{G}$. f : G $\longrightarrow$ H in morphisme de groupes, G/Ker(f) le groupe quotient de G par le noyau de f, Ker(f) $\lhd$ G (est un sous-groupe normal)

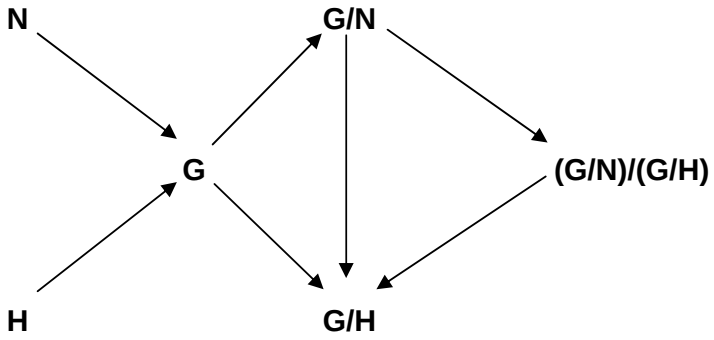


Soit H, K$\in \mathcal{G}$, H, K des sous-groupes de g, X = H$\cup$K, et L = gp(X) (le sous-groupe de G engendré par X)

$$HK \subset gp(X) \subset gp(H,K)$$
$$H \subset HK$$
$$K \subset HK$$
$$HK \leq G \Longrightarrow HK = KH$$

Remarque : si H, K$\leq$ G et K$\lhd$G alors

$$H \cap K \lhd H \implies H/(H \cap K) \cong HK/K$$



Troisième théorème d'isomorphisme : si H, N$\leq$ G et N$\lhd$G alors H$\cong$H/N.
Si de plus H$\lhd$G alors :

$$H \cap K \lhd H \implies (G/N)/(H/N) \cong G/H$$

Chaîne normale dans un groupe : Soit G un groupe et la suite emboîtée :

$$1 \leq G_r \leq G_{r-1} \leq \ldots\ldots\ldots \leq G_2 \leq G_1 \leq G_0 = G$$

On dit que c'est une série normale si chaque groupe est normal dans le suivant, dans ce cas $G_j \lhd G_{j-1}$. et G_{j-1}/G_j le groupe quotient appelé facteur.

Raffinement : Soit deux chaînes normales dans G :

$$1 \leq G_r \leq G_{r-1} \leq \ldots\ldots\ldots \leq G_2 \leq G_1 \leq G_0 = G \quad (1)$$
$$1 \leq H_s \leq H_{s-1} \leq \ldots\ldots\ldots \leq h_2 \leq H_1 \leq H_0 = G \quad (2)$$

On dit que (2) est un raffinement de (1) si elle est obtenue par insertion d'élément à (1).

si $G_{j-1}/G_j \cong H_{j-1}/H_j$ on dit que les deux séries sont équivalentes.

Zassenhaus : $H' \lhd H \leq G$ et $K' \lhd K \leq G$ alors

$$K'(H' \cap K) \lhd K'(H \cap K)$$
$$H'(K' \cap H) \lhd H'(H \cap K)$$
$$\frac{K'(H \cap K)}{K'(H' \cap K)} \cong \frac{H \cap K}{H' \cap K} \cong \frac{H'(H \cap K)}{H'(H \cap K')}$$

Shreier : deux chaînes normales dans un groupe G ont des raffinements isomorphes.

Série de composition : C'est une chaîne normale maximale de G.

Série de Jordan-Hölder : Si g possède une série de composition, alors toute chaîne normale a un raffinement isomorphe à une série de composition.

Groupes abéliens

$\mathcal{AG}$ est la classe des groupes abéliens (commutatifs).

Groupe abélien de type fini : Soit $A \in \mathcal{G}$, $B = \{a_1, a_2, \ldots\ldots, a_n\}$ est dit ensemble générateur fini de a si :

Pour tout x de A, il existe des entiers relatifs : $\lambda_1, \lambda_2, \ldots\ldots, \lambda_n \in \mathbb{Z}$ tel que :

$$x = \lambda_1 a_1 + \lambda_2 a_2 + \ldots\ldots + \lambda_n a_n.$$

Dans la notation multiplicative:

$$x = a_1^{\lambda_1} + a_2^{\lambda_2} + \ldots\ldots + a_n^{\lambda_n}.$$

Soit $A_1, A_2, \ldots, A_n$ les groupes cycliques engendrés respectivement par $a_1, a_2, \ldots\ldots, a_n$.

$$A = A_1 \oplus A_2 \oplus \ldots. \oplus A_n.$$

Comme xy = yx gans a, alors pour tout entier n on a :

$$(xy)^n = x^n y^n$$

n étant fixé dans $\mathbb{Z}$, l'application.

$\varphi_n : A \longrightarrow A$, $x \longmapsto nx$ est un endomorphisme du groupe A.

Sous-groupe de torsion : Soit $\mathcal{T}(A)$ l'ensemble :

$$\mathcal{T}(A) = \{ x \in A \mid \text{il existe un entier n, } nx = 0 \}$$

On vérifie que $\mathcal{T}(A)$ est un sous-groupe de A. $\mathcal{T}(A)$ est appelé ***sous-groupe de torsion*** de A.

NB. Si $\mathcal{T}(A) = \{0\}$ A est dit sans torsion.

Le groupe quotient $A/\mathcal{T}(A)$ est sans torsion.

Notons $\mathcal{GAST}$ l'ensemble de tous les **g**roupes **a**béliens **s**ans **t**orsion.

Génération d'un groupe abélien sans torsion :

$A \in \mathcal{GAST}$ un groupe abélien sans torsion.

Groupe abélien libre : Soit $L \in GA$ un groupe abélien. Et soit $\mathcal{B} = \{e_1, e_2, \ldots\ldots, e_n\}$
On dit que $\mathcal{B}$ est une ***base*** de L si : pour tout x de L.

Il existe un seul ensemble d'entiers $\lambda = (\lambda_1, \lambda_2, \ldots\ldots, \lambda_n) \in \mathbb{Z}^n$ tel que :

$$x = \lambda_1 a_1 + \lambda_2 a_2 + \ldots\ldots + \lambda_n a_n.$$

L peut avoir plusieurs bases mais toutes ces bases ont le même nombre d'éléments.
Si un groupe abélien possède une base il est dit ***libre***.
Le ***rang*** d'un groupe abélien libre est le cardinal d'une de ses bases.

Notons GAL l'ensemble de tous les **g**roupes **a**béliens **l**ibres.

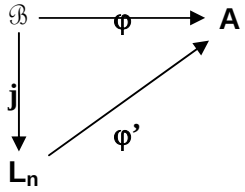
$A \in GAL$ un groupe abélien libre.

Application universelle : Soit $L_n \in GAL$ un groupe abélien libre de rang n, et $\mathcal{B} = \{e_1, e_2, \ldots\ldots, e_n\}$ une base de L_n.
$j : \mathcal{B} \longrightarrow L_n$. étant l'injection canonique.

Pour toute application $\varphi : \mathcal{B} \longrightarrow A$.

Il existe un seul homomorphisme $\varphi' : L_n \longrightarrow A$. tel que :

$$\varphi' \circ j = \varphi.$$



$$\varphi'\left(\sum_{i=1}^{n} \lambda_i e_i\right) = \sum_{i=1}^{n} \lambda_i \varphi(e_i)$$

Si φ est surjectif, $Im(\varphi) = Im(\varphi') = A$ et A devient de type fini.

On note $GATF$ la classe des groupes abéliens de type fini.

Théorème : soit A un groupe abélien de type fini $A \in GATF$:
A est Libre si et seulement si il est sans torsion :

$$A \in GAL \implies A \in GAST.$$

Autrement dit

$$A \in GATF \implies (A \in GAL \iff A \in GAST)$$

Démonstration
$GAL \subset GAST$: Soit x un élément quelconque de A, de base $\mathcal{B} = \{e_1, e_2, \ldots\ldots, e_n\}$ $x = \lambda_1 a_1 + \lambda_2 a_2 + \ldots\ldots + \lambda_n a_n$. si $mx = 0$ alors :

$$mx = m\lambda_1 a_1 + m\lambda_2 a_2 + \ldots\ldots + m\lambda_n a_n = 0$$

$x = (\lambda_1 + m\lambda_1)a_1 + (\lambda_2 + m\lambda_2)a_2 + \ldots\ldots + (\lambda_n + m\lambda_n)a_n$.
Comme x doit s'exprimer d'une façon unique en fonction de la base:

$$m\lambda_1 = 0,\ m\lambda_2 = 0\ ,\ \ldots\ldots\ldots,\ m\lambda_n = 0$$

Donc $m = 0$

On en conclut que x n'est pas de torsion, et par suite A est sans torsion.

$GAST \subset GAL$: soit x un élément sans torsion, de A (de type fini)
On suppose qu'il y a un ensemble générateur $\{e_1, e_2, \ldots\ldots, e_n\}$ et que

$$x = \lambda_1 a_1 + \lambda_2 a_2 + \ldots\ldots + \lambda_n a_n = 0$$

Si les coefficients ont un diviseur commun δ :

$$x = \delta\lambda'_1 a_1 + \delta\lambda'_2 a_2 + \ldots\ldots + \delta\lambda'_n a_n = 0$$

$$x = \delta(\lambda'_1 a_1 + \lambda'_2 a_2 + \ldots\ldots + \lambda'_n a_n) = 0$$

Mais si δ n'est pas nul, $x' = \lambda'_1 a_1 + \lambda'_2 a_2 + \ldots\ldots + \lambda'_n a_n$ serait de torsion s'il n'est pas nul, donc forcément :

$$\lambda'_1 a_1 + \lambda'_2 a_2 + \ldots\ldots + \lambda'_n a_n = 0 \quad (3)$$

On continu par récurrence su n :
Si n =1 :
$\lambda'_1 a_1 = 0$ comme pas d'éléments de torsion : $\lambda'_1 = 0$ (si non a_1 serait de torsion)
Si $\lambda'_1 = 1$ alors :

$$a_1 + \lambda'_2 a_2 + \ldots\ldots + \lambda'_n a_n = 0$$

$$a_1 = -(\lambda'_2 a_2 + \ldots\ldots + \lambda'_n a_n)$$

Le groupe sera engendré par n-1 éléments, on applique l'hypothèse de récurrence.

Supposons pour fixer les idées $|\lambda'_1| \geq |\lambda'_2| > 0$

Il existe α de $\mathbb{Z}$ tel que $|\lambda'_1 - \alpha\lambda'_2| < |\lambda'_2|$, on pose $a'_2 = a_2 + \alpha a_1$.
(3) devient :

$$(\lambda'_1 - \alpha\lambda'_2)a_1 + \lambda'_2 a'_2 + \ldots\ldots + \lambda'_n a_n = 0 \quad (4)$$

On renumérote et on recommence jusqu'à arriver à un des coefficients se réduit à +1 ou –1.

$$a_1 = -(\lambda'_2 a_2 + \ldots\ldots + \lambda'_n a_n) \text{ ou } a_1 = +(\lambda'_2 a_2 + \ldots\ldots + \lambda'_n a_n)$$

De nouveau le groupe est engendré par n –1 éléments et on applique l'hypothèse de récurrence.
Dans les cas qui restent $\lambda'_1 = 0$, donc $\lambda'_2 a_2 + \ldots\ldots + \lambda'_n a_n = 0$ et on continue par récurrence pour en déduire que tous le reste des coefficients sont nuls.
Ainsi :

Dans $GATF$: $GAL = GAST$

Conséquence : tout groupe abélien de type fini est la somme directe d'un groupe fini et d'un groupe libre.
En effet soit $A \in GATF$, posons $T(A) = T$ ceci donne $T(A/T) = 0$ (A/T sans torsion) alors d'après le théorème précédent A/T est libre, soit donc une base $\mathcal{B}' = \{\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_n\}$ une base de A/T, ($A \xrightarrow{nat} A/T$ l'application naturelle étant surjective) on considère les antécédents $\{e_1, e_2, \ldots\ldots, e_n\}$ dans A engendrent un sous-groupe L : $L = \langle e_1, e_2, \ldots\ldots, e_n \rangle$, L est libre et $L \leq A$ (car L isomorphe à A/T libre)
On a :

$$L \leq A \text{ et } T(A) \leq A$$

$$L \cap T(A) = 0$$

D'autre part pour tout x de a on a $x = a + \lambda_1 e_1 + \lambda_2 e_2 + \ldots\ldots + \lambda_n e_n$. Avec a hors de L. l'image de x par nat est $\mu_1 \bar{e}_1 + \mu_2 \bar{e}_2 + \ldots\ldots + \mu_n \bar{e}_n$, et nat(a) = 0.

A est dans le noyau T de nat donc a est un élément de torsion.
Donc

$$A \subset T+L$$
$$A \subset T(A)+L$$

Avec $T(A)+L \subset A$:

$$A = T(A)+L$$

Avec $L \bigcap T(A) = 0$

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

Conclusion : Tout groupe de type fini est la somme directe d'un groupe (de torsion) fini et d'un groupe libre.

Remarque : les groupes libres étant régulier, il suffit de travailler sur les groupe finis.

Conséquence : Tout groupe abélien libre est sans torsion :

Tout groupe de fini est la somme de groupes cycliques : on remarque que

$$\mathbf{C}_2 \oplus \not\cong_3 \mathbf{C}_6 \qquad \mathbf{C}_3 \oplus \mathbf{C}_3 \not\cong \mathbf{C}_6$$

Ceci suggère que si le nombre premier se répète, il y a de nouvelles lois qui entrent en jeu.

Groupe primaire, p-groupe : un groupe G est dit primaire si tout élément de g a un ordre puissance d'un nombre premier p:

Pour tout x de G il existe r entier positif tel que : $ord(x) = p^r$

Additivement $p^r x = 0$

p est le même, on dit que G est un ***p-groupe***.

Le sous p-groupe : Soi A un groupe abélien, on définit

$$A_p = \{x \in A \mid \text{ il existe r positif, } ord(x) = p^r\}$$

C'est un sous-groupe de G. il est par ailleurs un ***p-groupe***. C'est le sous ***p-groupe*** maximal contenu dans G. comme l'ordre d'un sous-groupe est un diviseur de l'ordre du groupe (théorème de Lagrange) p doit diviser |G|.

NB. Si p ne divise pas |G| alors G ne contient aucun ***p-groupe***.

Remarque : Tout groupe abélien fini ou de type fini ne peut contenir qu'un nombre fini de ***p-groupes*** (les ***p*** sont en nombre fini)

Théorème : Tout groupe fini s'exprime d'une façon unique. comme une somme directe finie de ***p-groupes***.

$$A = A_{p_1} \oplus \ldots\ldots\ldots \oplus A_{p_r}$$

Les composants sont des sous- ***p-groupes***. Maximaux.

Théorème : Tout p-groupe abélien fini est somme directe de groupe cycliques.

Théorème : tout groupe abélien de type fini est somme directe de groupes cycliques.

Groupe Symétrique

Groupe opérant sur un ensemble : Soit (G, **.**, e) un groupe et E un ensemble, on dit que G opère sur E s'il existe une application :

$$\omega : G\times E \longrightarrow E,\ (g, a) \longmapsto ga = \omega(g, a)$$
$$\omega \in (G\times E)^E$$

Vérifiant :

$$(g_1g_2)a = g_1(g_2a) \quad \text{et} \quad ea = a$$

Sous-groupe opérateur : si H est un sous-groupe de G, ω_H la restriction de ω à $G\times E$:

$$\omega_H : H\times E \longrightarrow E,\ (h, a) \longmapsto ha = \omega(h, a)$$

Est aussi une opération sur E par H.

𝔖(E) opère canoniquement sur E : soit E^E l'ensemble des applications de E dans E, $(E^E, \circ)$ est un monoïde dont le neutre est Id_E, si on note par ***𝔖(E)*** l'ensembles des éléments inversibles (*bijectifs*) de ce monoïde, $(\mathfrak{S}(E), \circ)$ est un groupe. On m'appelle groupe symétrique de E.
L'application

$$\omega : \mathfrak{S}(E)\times E \longrightarrow E,\ (\sigma, a) \longmapsto \sigma(a) = \omega(\sigma, a)$$

Est bien une opération sur E par ***𝔖(E)***.

Opération triviale : soit l'opération

$$\omega : G\times E \longrightarrow E,\ (g, a) \longmapsto a = \omega(g, a)$$

C'est bien une opération, dite triviale.

Opération induite par un morphisme : soit : $\eta : G \longrightarrow \mathfrak{S}(E)$, un morphisme de groupes, celui-ci induit une opération sur e par G de la façon suivante :

$$\omega_\eta : G\times E \longrightarrow E,\ (g,a) \longmapsto ga = \eta(g)(a) = \omega_\eta(g, a)$$

On vérifie que c'est bien une opération :
$(g_1g_2)a = \eta(g_1g_2)(a) = \eta(g_1)\eta(g_2)(a) = \eta(g_1)(g_2a) = g_1(g_2a)$
Et

$$ea = \eta(e)(a) = Id_E(a) = a.$$

Orbite d'un élément de E : Soit *a* un élément de E sur lequel on opère par le groupe G, on appelle orbite de *a* l'ensemble :

$$\boldsymbol{Orb}(a) = \{ga \in E \mid g \in G\}$$
Noté aussi : G*a*
$$\boldsymbol{Orb}(a) = Ga$$

Cas particulier d'une opération triviale :

$$\boldsymbol{Orb}(a) = Ga = \{a\}$$

C'est un singleton.
Relation d'équivalence $\mathcal{R}$ sur E par une opération :

$$a\ \mathcal{R}\ b \Leftrightarrow \boldsymbol{Orb}(a) = \boldsymbol{Orb}(b)$$

Donc les orbites font une *partition* de E.

Opération transitive : si E forme une seule orbite, on dit que l'opération correspondante est transitive :

$$\boldsymbol{Orb}(a) = Ga = E$$

Donc pour tout a et b de E il existe g de G tel que : ga = b

Opération simplement transitive :
Si

Pour tout a et b de E il existe un seul g de G tel que : ga = b

L'application :

$$f_x : G \longrightarrow E,\ x \longmapsto gx$$

est une bijection qui peut identifier E au groupe G.
E forme une seule orbite, pour tout a de G : $\boldsymbol{Orb}(a) = Ga = E$

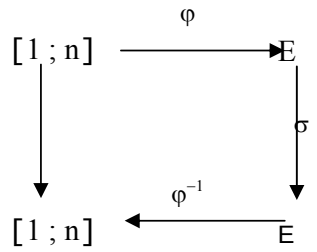
Exemple : Les espaces affines sur un corps.

Cas de E fini

E ensemble de cardinal n : Soit E est fini de cardinal n, il est équipotent à {1, 2, 3, ….., n} = [1 ; n]
Si

$$\varphi : E \longrightarrow [1 ; n]$$

Est une bijection de E sur [1 ; n].



L'application

$$\mathfrak{S}(E) \longrightarrow \mathfrak{S}([1 ; n]),\ \sigma \longmapsto \varphi^{-1}\sigma\varphi.$$

Est un isomorphisme de groupe, qui permet d'identifier le groupe symétrique d'un ensemble de cardinal n, à $\mathfrak{S}_n = \mathfrak{S}([1 ; n])$,
En conclusion on peut faire les propriétés de $\mathfrak{S}(E)$ en travaillant seulement sur $\mathfrak{S}_n$.

cycle : $\sigma \in \mathfrak{S}_n$ est un ***cycle*** si son orbite n'est pas réduite à un singleton

k-cycle : soit $\sigma \in \mathfrak{S}_n$ le sous-groupe de $\mathfrak{S}_n$ engendré par σ se note $<\sigma>$ est cyclique, et s'il est de cardinal k, on a $= \{\sigma, \sigma^1, \sigma^2, \ldots\ldots, \sigma^k = Id$, on l'appelle *k-cycle*.

Comme $<\sigma>$ est un sous-groupe de $\mathfrak{S}_n$, $<\sigma>$ opère sur $[1 ; n]$,

$[1 ; n]$ est une seule orbite pour $<\sigma> \iff <\sigma>$ n'est pas réduite à un ***singleton***
Support d'une permutation :

$$\boldsymbol{supp}(\sigma) = \{ i \in [1 ; n] \mid \sigma(i) \neq i \}$$

Longueur d'une permutation : soit σ une permutation $\in \mathfrak{S}_n$, on appelle longueur de σ :

$$\boldsymbol{Long}(\sigma) = \boldsymbol{max}\text{Card}(\boldsymbol{orb}(x))$$

Tout $\sigma \in \mathfrak{S}_n$, est produit fini unique de cycles (produit commutatif)
Tout $\sigma \in \mathfrak{S}_n$, est produit fini (non unique) de transpositions (produit non commutatif) la parité du nombre des facteurs est la même.

Transposition : une transposition est un 2-cycle.

Signature d'une permutation : soit $\sigma \in \mathfrak{S}_n$ une permutation on appelle signature de σ le nombre :

$$\boldsymbol{sig}(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Les facteurs sont après arrangement des numérateurs +1 ou –1 donc

$$\boldsymbol{sig}(\sigma) \in \{+1, -1\}$$

On vérifie que

$$\boldsymbol{sig}(\sigma\tau) = \boldsymbol{sig}(\sigma)\boldsymbol{sig}(\tau)$$

L'application

$$\boldsymbol{sig} : \mathfrak{S}_n \longrightarrow \{+1, -1\}$$

est un morphisme de groupe.

Si σ est un cycle de longueur k : $\boldsymbol{sig}(\sigma) = (-1)^{k-1}$
Si σ est une transposition, c'est un 2-cycle : $\boldsymbol{sig}(\sigma) = (-1)^{2-1} = -1$.

Groupe alterné de E : $\mathfrak{A}_n = \ker(\boldsymbol{sig}) = \boldsymbol{sig}^{-1}(+1)$ est un sous-groupe distingué de $\mathfrak{S}_n$ dit ***groupe alterné*** de $[1 ; n]$.
Soit τ une transposition, l'application $\mathfrak{S}_n \longrightarrow \mathfrak{S}_n$; $\sigma \longmapsto \tau\sigma$ est un bijection (mais pas un isomorphisme) elle applique $\mathfrak{A}_n$ sur $\mathfrak{S}_n \setminus \mathfrak{A}_n$ on en conclut

$$\text{Card}(\mathfrak{A}_n) = \text{card}(\mathfrak{S}_n \setminus \mathfrak{A}_n)$$

$$\text{Mais } \text{Card}(\mathfrak{A}_n) + \text{card}(\mathfrak{S}_n \setminus \mathfrak{A}_n) = \text{card}(\mathfrak{S}_n) = n !$$

Donc

$$\text{Card}(\mathfrak{A}_n) = \frac{n!}{2} \text{ et } \text{card}(\mathfrak{S}_n \setminus \mathfrak{A}_n) = \frac{n!}{2}$$

Inversion : On appelle inversion de $\sigma \in \mathfrak{S}_n$ tout couple (i,j) de $[1 ; n]^2$ tel que

$$(\sigma(i) - \sigma(j)) \times (i - j) < 0$$

Ensemble des inversions de σ :

$$\boldsymbol{Inv}(\sigma) = \{(i,j) \in [1\,;\,n]^2 \mid (\sigma(i) - \sigma(j)) \times (i-j) < 0\}$$

On vérifie que

$$\boldsymbol{sig}(\sigma) = (-1)^{\mathrm{card}(\boldsymbol{Inv}(\sigma))}$$

si m est le nombre des orbites de $<\sigma>$: $\boldsymbol{sig}(\sigma) = (-1)^{n-m}$

Sous Groupes de Sylow
Représentation des groupes

Soit (G,.,1) un groupe multiplicatif et K un corps, on rappelle que $\mathcal{M}_n(K)$ est l'anneau des matrices carrées d'ordre n à éléments dans k, $\mathcal{GL}_n(K)$ le groupe multiplicatif des matrices inversibles de $\mathcal{M}_n(K)$.

Définition : soit $\rho : G \longrightarrow \mathcal{GL}_n(K)$ un morphisme de groupe :

$$\rho(x_1x_2) = \rho(x_1)\rho(x_2)$$

x_1x_2 produit dans G, $\rho(x_1)\rho(x_2)$ produit dans $\mathcal{GL}_n(K)$

Si on prend x_1 l'unité 1 de G, on aura :

$\rho(1.x_2) = \rho(1)\rho(x_2)$, comme ρ est un morphisme $\rho(1)$ est I_n la matrice unité de $\mathcal{GL}_n(K)$ donc :

$$\rho(x_2) = \rho(1)\rho(x_2)$$

$$\rho(1) = I_n$$

Exemple : Représentation du groupe cyclique d'ordre 3 dans $\mathcal{GL}_2(K)$:

$C_3 = \{a, a^2, a^3 = 1\}$ engendré par ***a*** : il faut trouver une matrice inversible $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ prise comme $\rho(a)$ vérifiant :

$$I_2 = \rho(1) = \rho(a^3) = [\rho(a)]^3 = A^3$$

$$A^3 = I_2.$$

$$A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},\ A^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix},\ A^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$\mathrm{Im}(\rho)$ est le sous-groupe cyclique de $\mathcal{GL}_2(K)$ engendré par $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$

C_3 est isomorphe à $\mathrm{Im}(\rho) = \{ \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \}$

On dit que C_3 est représenté dans $\mathcal{GL}_2(K)$

Ici ρ est injectif on dit qu'il est ***fidèle***.

NB. Dans le cas où $\boldsymbol{Im}(\rho) = I_n$. On dit que ρ est ***trivial***.

Représentations équivalentes : soit

$\rho : G \longrightarrow \mathcal{GL}_d(K)$ et $\sigma : G \longrightarrow \mathcal{GL}_{d'}(K)$ deux représentations de G, on dit qu'elles sont équivalentes si :

$$d = d'$$

et pour tout x de G : $\sigma(x) = P^{-1}\rho(x)P$

Où P est une matrice inversible de $\mathcal{GL}_d(K)$

C'est bien une relation d'équivalence sur l'ensemble des représentations de G. (les classes d'équivalences se graduent par degrés).

Exemple : si ω est la racine cubique de l'unité $\omega^3 = 1$:

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -\omega & -\omega^2 \end{pmatrix}=\begin{pmatrix} \omega & \omega^2 \\ 1+\omega & 1+\omega^2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ -\omega & -\omega^2 \end{pmatrix}\begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}=\begin{pmatrix} \omega & \omega^2 \\ -\omega^2 & -\omega \end{pmatrix}=\begin{pmatrix} \omega & \omega^2 \\ 1+\omega & 1+\omega^2 \end{pmatrix}$$

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -\omega & -\omega^2 \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ -\omega & -\omega^2 \end{pmatrix}\begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}=\begin{pmatrix} \omega & \omega^2 \\ 1+\omega & 1+\omega^2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ -\omega & -\omega^2 \end{pmatrix}^{-1}\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -\omega & -\omega^2 \end{pmatrix}=\begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$$

Donc ρ est équivalent à σ :

$$\sigma : G \longrightarrow \mathcal{GL}_n(K),\ \sigma(a) = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}$$

Ainsi :

$$\sigma(a^2) = \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix},\ \sigma(a^3) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\ (\ \omega^3 = \omega^6 = 1\ )$$

G-***module*** : Soit G un groupe multiplicatif, E un K-ev de dimension d :
Pour tout x de G on a

$$E \longrightarrow E,\ v \longmapsto \rho(x)(v) = f(v) = x(v)$$

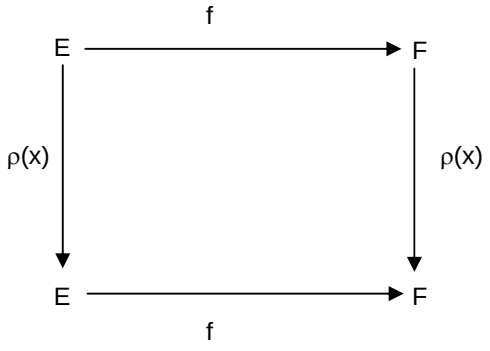
f étant un élément de $End_K(E)$ de matrice $\rho(x) = M_f$.
On dit que E est un ***G-module***.
Soit E, F deux G-modules :

$E \longrightarrow E,\ v \longmapsto \rho(x)(v) = x(v)$

$F \longrightarrow F,\ v \longmapsto \rho(x)(v) = x(v)$

G : E ⟶ F est un isomorphisme de G-modules si :

$$g(\rho(x)(v)) = \rho(x)g(v)$$



Exercices sur les anneaux et les corps

1) Soit (A, +, .) un anneau, et f un endomorphisme de A, on pose $A_0 = \{x \in A |\ f(x) = x\}$ montrer que A_0 est un sous-anneau de A.
Soit E un ensemble on note A^E l'ensemble de toutes les applications de A dans E, et l'on définit sur A^E les lois f + g et f.g par :

$$E \xrightarrow{f+g} A,\ x \longmapsto f(x) + g(x) \quad \text{et} \quad E \xrightarrow{f.g} A,\ x \longmapsto f(x).g(x)$$

Montrer que $(A^E, +, .)$ est un anneau.
Trouver une condition pour que $(A^E, +, .)$ Soit commutatif.
On suppose que chacun des ensemble E et A possède au moins deux éléments, trouver un diviseur de zéro dans $(A^E, +, .)$.

2) Soit A, A' deux anneaux unitaires, $f : A \longrightarrow A'$ un morphisme d'anneaux unitaires. On note N = Ker(f) ; soit I' un idéal bilatère de A', et soit $\mathfrak{I} = f^{-1}(\mathfrak{I}')$.

i) Montrer que $\mathfrak{I}$ est un idéal bilatère de A contenant N.

ii) On note $p : A \longrightarrow A/\mathfrak{I}$ et $p' : A \longrightarrow A'/\mathfrak{I}'$ et les surjections canoniques,

a) Montrer qu'il existe une application unique $\bar{f} : A/\mathfrak{I} \longrightarrow A'/\mathfrak{I}'$ telle que :

$$\bar{f} \circ p = p \circ f$$

b) Montrer que $\bar{f}$ est un morphisme d'anneaux unitaires.

c) montrer que f est injective.

d) Montrer que si f est surjective, alors $\bar{f}$ est un isomorphisme d'anneaux.

3) Soit A, A' deux anneaux unitaires, $f : A \longrightarrow A'$ un morphisme d'anneaux. On note N = Ker(f) ;

i) Soit B' un sous-anneau de a', montrer que $B = f^{-1}(B')$ est un sous-anneau de a contenant N.

ii) Si *f* est surjective, montrer que B' = *f*(B) et que les anneaux B/N et B' sont isomorphes.

4) Soit A un anneau unitaire et T un ensemble quelconque et $\{\mathfrak{I}_t\}_{t \in T}$ une famille d'idéaux à gauche dans a. on suppose que pour tout couple (t, r) d'éléments de t, il existe s dans T tel que $\mathfrak{I}_t \subset \mathfrak{I}_s$ et $\mathfrak{I}_r \subset \mathfrak{I}_s$.
Montrer que $\mathfrak{I} = \bigcup_{t \in T} \mathfrak{I}_t$ est un idéal à gauche.

5) Soit A un anneau unitaire $\mathfrak{I}$ un idéal à gauche de A, $\mathcal{K}$ un idéal à droite de A, on désigne $\mathfrak{I} * \mathcal{K}$ l'ensemble des x de A ayant la propriété suivante :
Il existe n un entier naturel non nul et des familles finies $x_1, x_2, \ldots, x_n$ de $\mathfrak{I}$ et $y_1, y_2, \ldots, y_n$ de $\mathcal{K}$ tel que : $x = x_1y_1 + x_2y_2 + \ldots + x_ny_n$.

i) Montrer que I*K est un idéal bilatère.

ii) Soit $\mathcal{B}$ l'ensemble des idéaux bilatères de A. montrer que $(\mathcal{B}, *)$ est un monoïde.

iii) On suppose que A est commutatif, montrer que $\mathfrak{I} + \mathfrak{K} = A \Rightarrow \mathfrak{I} * \mathfrak{K} = \mathfrak{I} \cap \mathfrak{K}$.

6) Soit A un anneau commutatif et a, b, c des éléments de A.
Calculer la somme $(a + b + c)^3 + (a - b - c)^3 + (-a + b - c)^3 + (-a - b + c)^3$.

5) dans un anneau quelconque (A, +, .) on définit une nouvelle loi $x*y = xy - yx$
i) Montrer que $*$ est anticommutative
ii) Démontrer l'identité de Jacobi $x*(y*z) + y*(z*x) + z*(x*y) = 0$

6) Soit A un anneau unitaire d'unité 1 et soit x de A tel que $y = 1 - x$ soit nilpotent, c'est-à-dire il existe n un entier non nul tel que $y^n = 0$.
Montrer que x est inversible et que si x' est son inverse alors $1 - x'$ est nilpotent.

7) Soit A un anneau contenant un sous-anneau A' isomorphe à Q et soit x un élément de A, nilpotent d'indice p +1 (p +1 est le plus petit entier tel que $x^{p+1} = 0$)
On pose $e^x = 1 + x + \frac{x^2}{2!} + \ldots\ldots + \frac{x^{p-1}}{(p-1)!} + \frac{x^p}{p!}$
Soit y un élément nilpotent d'indice q + 1 de A, avec $q \leq p$. montrer que :
Si x et y sont permutables on a : $e^{x+y} = e^x . e^y$

8) Soit E un ensemble quelconque et $A = \mathcal{P}(E)$ l'ensemble de toutes les parties de E, on définit sur A les loi de composition internes $\cap$ et Δ.
Montrer que $(A, \cap, \Delta)$ est un anneau commutatif et unifère, on l'appelle anneau de ***Boole***.

9) Soit (A, +, .) un anneau intègre et unifère, on dit que A est un ***anneau factoriel*** s'il vérifie les propriétés suivantes :
(***AF1***) Tout élément non nul de A est décomposable en un produit fini d'éléments irréductibles.

Elément irréductible : Un élément a de A est dit irréductible si et seulement si a est divisible par les éléments de $(a\mathfrak{U}) \cup \mathfrak{U}$ où $\mathfrak{U}$ est l'ensemble des éléments inversibles de A.
(***AF2***) Cette décomposition est ***unique*** à un facteur inversible près.
(Anglais : ***U***nique ***F***actorisation ***D***omain)
Montrer que si ***p*** est un élément irréductible de A, et divise ab alors ***p*** divise l'un des facteurs a ou b.

10) Soit (K, +, .) un corps et a un élément de K, donner une expression simple du produit :

$$p = (1 + a)(1 + a^2)(1 + a^4)(1 + a^8)\ldots\ldots\ldots\ldots (1 + a^{2n})$$

Soit A un anneau, $\mathfrak{p}$ un idéal de A, on dit que $\mathfrak{p}$ est un idéal premier si :

$$(\forall\, a, b \in A)\ ((ab \in \mathfrak{p}) \Rightarrow (a \in \mathfrak{p} \text{ ou } b \in \mathfrak{p}))$$

Montrer que si p est bilatère alors :

$$(A/\mathfrak{p} \text{ est intègre}) \Rightarrow (\mathfrak{p} \text{ est premier})$$

11) Soit A un anneau unifère, et $\mathfrak{M}$ un idéal bilatère de A, on dit que $\mathfrak{M}$ est un idéal ***maximal*** de A si :
($\mathfrak{M}1$) $\mathfrak{M} \neq A$
($\mathfrak{M}2$) Pour tout idéal $\mathfrak{p}$ de A : $(\mathfrak{M} \subset \mathfrak{p} \subset A) \Rightarrow (\mathfrak{p} = \mathfrak{M} \text{ ou } \mathfrak{p} = A)$

i) Caractériser les idéaux maximaux de $\mathbb{Z}$.

ii) Montrer que si $A/\mathfrak{M}$ est un corps alors $\mathfrak{M}$ est un idéal maximal.

Anneaux

1) Anneaux : (R, +, .) un triplet d'un ensemble non vide A, et deux lois de composition internes, + et . , on dit qu'il est un anneau si :

(A1) (R, +, .) Est un groupe abélien ou commutatif.

(A2) (R, .) Est un monoïde.

(A3) + est une loi distributive par rapport à. ;

On note 0_A le zéro neutre de la loi + ;

On note 1_A le un neutre de la loi .;

2) Remarque : si $0_A = 1_A$ alors $A = \{0_A\}$ (pas difficile)

3) Homomorphisme d'anneaux : soit R, S deux anneaux, $f : R \longrightarrow S$ une application, on dit que f est un homomorphisme d'anneaux (ou simplement morphisme d'anneaux) si : $f(x_1+x_2) = f(x_1) + f(x_2)$ $f(x_1.x_2) = f(x_1).f(x_2)$ $f(1_R) = 1_S$.

4) ***Exemple*** : $\zeta : R \longrightarrow S$, $x \longmapsto 0_S$ vérifie les deux premières mais pas $\zeta(1_R) = 1_S$. Donc ce n'est pas un morphisme.

5) Idéal d'un anneau : Soit R un anneau, $\mathfrak{a}$ un sous-ensemble de R,

(Ig) on dit que $\mathfrak{a}$ est un idéal à droite de R si

$(\mathfrak{a}, +)$ est un sous-groupe de (R,+)

$R\mathfrak{a} \subset \mathfrak{a}$.

(Id) on dit que $\mathfrak{a}$ est un idéal à gauche de R si

$(\mathfrak{a}, +)$ est un sous-groupe de (R,+)

$\mathfrak{a}R \subset \mathfrak{a}$.

(Ib) on dit que $\mathfrak{a}$ est un idéal (idéal bilatère) de R si

$(\mathfrak{a}, +)$ est un sous-groupe de (R, +)

$\mathfrak{a}R \subset \mathfrak{a}$. et $R\mathfrak{a} \subset \mathfrak{a}$.

Notation : $\mathfrak{a} \lhd R$

6) Exemples d'idéaux :

1) m strictement positif de $\mathbb{Z}$: $m\mathbb{Z}$ est un idéal de $\mathbb{Z}$.

2) $\mathbb{Z}/(m)$ est un anneaux, (des classes résiduelles modulo m)

3) Soit R, S deux anneaux, $f : R \longrightarrow S$ un morphisme d'anneaux :

Ker(f) le noyau de f : $Ker(f) = \{x \in R \mid f(x) = 0_S\}$ est un idéal de R, et c'est aussi un sous-anneau.

Im(f) l'image de f : $Im(f) = \{ f(x) \in S \mid x \in R\}$ est un sous-anneau de S.

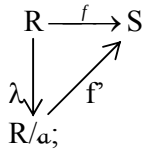
7) Quotient d'un anneau par un idéal : Soit $\mathfrak{a} \lhd R$, l'ensemble quotient $R/\mathfrak{a} = \{x + \mathfrak{a} \mid x \in R\}$, Et la surjection canonique : $\lambda : R \longrightarrow R/\mathfrak{a}$; $x \longmapsto x + \mathfrak{a} = \bar{x}$, c'est un morphisme d'anneaux.

8) Théorème : $f : R \longrightarrow S$ un morphisme d'anneaux :

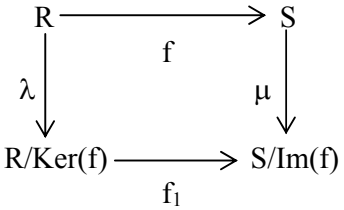
$$\mathrm{Ker}(f) \lhd R, \quad \mathrm{Im}(f) \lhd R$$

9) Théorème de factorisation des anneaux : $f : R \longrightarrow S$ un morphisme d'anneaux :

$$\lambda : R \longrightarrow R/\mathfrak{a};\ x \longmapsto x + \mathfrak{a} = \bar{x}, \quad f' : R/\mathfrak{a} \longrightarrow S;\ x + \mathfrak{a} \longmapsto f(x).$$



10) Premier théorème d'isomorphisme :



f_1 est un isomorphisme d'anneaux.

11) Deuxième théorème d'isomorphisme : $S \leq R$ et $\mathfrak{a} \lhd R$, alors :

$$(1)\ S \cap \mathfrak{a} \lhd R, \quad (2)\ S/(S \cap \mathfrak{a}) \cong (S + \mathfrak{a})/\mathfrak{a},$$

12) Troisième théorème d'isomorphisme: $\mathfrak{a} \lhd R, \quad \mathfrak{a} \subset \mathfrak{b} \subset R,$
On a :

$$\mathfrak{b}/\mathfrak{a} \lhd R/\mathfrak{b} \quad \text{et} \quad (R/\mathfrak{b})/(\mathfrak{b}/\mathfrak{a}) \cong R/\mathfrak{a}.$$

13) Idéal maximal : soit $\mathfrak{m} \lhd R$, alors :

$$(\mathfrak{m} \text{ Est maximal}) \iff \{\forall\ \mathfrak{a} \lhd R : \mathfrak{m} \subset \mathfrak{a} \implies (\mathfrak{m} = R \text{ ou } \mathfrak{m} = \mathfrak{a})\ \}$$

14) Anneau simple : On dit qu'un anneau R est simple si les seuls sous anneaux de R sont {0} et R lui-même.

$$\forall\ \mathfrak{a} \lhd R : \mathfrak{a} = R \text{ ou } \mathfrak{a} = \{0\}$$

15) Remarque : Tout anneau commutatif simple est un corps.

16) Remarque : par le *troisième théorème d'isomorphisme* :

$\mathfrak{m} \lhd R$, est maximal $\iff$ $R/\mathfrak{a}$ est un anneau simple.

Si R est commutatif :

$$\mathfrak{m} \lhd R, \text{ est maximal } \iff R/\mathfrak{a} \text{ est un corps.}$$

Cas non commutatif : il y a des anneaux simples qui ne sont pas des corps.

17) ***Construction d'idéaux*** : Soit X une partie d'un anneau R, on définit l'idéal ***engendré*** par X, l'intersection de tous les idéaux de R contenant X. on le note (X).
On démontre :

$$(X) = \{a_1x_1b_1 + a_2x_2b_2 + \ldots..+a_ix_ib_i + \ldots..+a_nx_nb_n \mid a_i,b_i \in R, x_i \in X \}$$

N.B. L'intersection de toute famille d'idéaux de R est un idéal de R.

18) Modules sur les anneaux : Soit (M, +) un groupe abélien, (R,+, .) un anneau intègre, on suppose que R opère sur G par l'application :

$$R \times M \longrightarrow M, \ (r, x) \longmapsto rx$$

$$r(x_1+ x_2) = rx_1 + rx_2$$
$$(r_1+ r_2)x = r_1x + r_2x$$
$$r_1(r_2x) = (r_1r_2)x$$
$$1.x = x$$

M est dit R-module.
Les R-modules sont des outils pour étudier les anneaux.

19) Sous-module : $N \subset M$ est dit un sous-module de r si S est un R-module pour

$$R \times N \longrightarrow N, \ (r, x) \longmapsto rx$$

Qui est la restreinte réduite de

$$R \times M \longrightarrow M, \ (r, x) \longmapsto rx$$

On note $N \prec M$, N doit être un sous-groupe du groupe abélien M on écrit indifféremment $N \lhd M$ ou $N \leq M$.)

20) Théorème : $N \prec M$ si et seulement si toute combinaison linéaire de deux éléments de N par des éléments de R, se trouve dans N.

Exemple : Si $N \leq M$. N est un sous- $\mathbb{Z}$ -module de M.

Exemple : Tout groupe (G, +) est un $\mathbb{Z}$-module.

21) ***Morphisme de modules*** : soit $M \longrightarrow N$ une application entre deux modules, on dit que c'est un morphisme de modules si :

$$f(r_1x_1+ r_2x_2) = r_1f(x_1) + r_2f(x_2)$$

On note ***Hom***(M, N) l'ensemble de tous les morphismes de M dans N.

22) ***Noyau et Image d'un morphisme*** : on note ***ker(f)*** le sous-ensemble $f^{-1}(0_N)$ des éléments de M dont l'image par f est 0_N, et on note ***Im(f)*** l'ensemble des images par f de tous les élément de m, on le note aussi ***f(M)***.

CoKer et CoImage :

$$\text{CoKer}(f) = N/\text{Im}(f)\ , \quad \text{CoImage}(f) = M/\text{Ker}(f)$$

Remarque : l'image de tout sous-module par un morphisme en est un.

$$M_1 \prec M \implies f(M_1) \prec f(M) \prec N$$

L'image réciproque de tout sous-module par un morphisme en est un.

$$N_1 \prec N \Rightarrow f^{-1}(0_N) \prec f^{-1}(N_1) \prec f^{-1}(N) \prec M$$

23) Suites exactes : soit $\ldots \xrightarrow{f_{i-2}} M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+2}} \ldots\ldots\ldots$
On dit que cette suite de morphisme de modules est exacte si l'image de chacun coïncide avec le noyau du suivant. Si suivant figure dans la suite.

24) Extension de modules : Soit $0 \longrightarrow M' \xrightarrow{\lambda} M \xrightarrow{\mu} M'' \longrightarrow 0$. une suite exacte de morphismes de modules, on dit alors que cette suite est une extension de M' par M''.

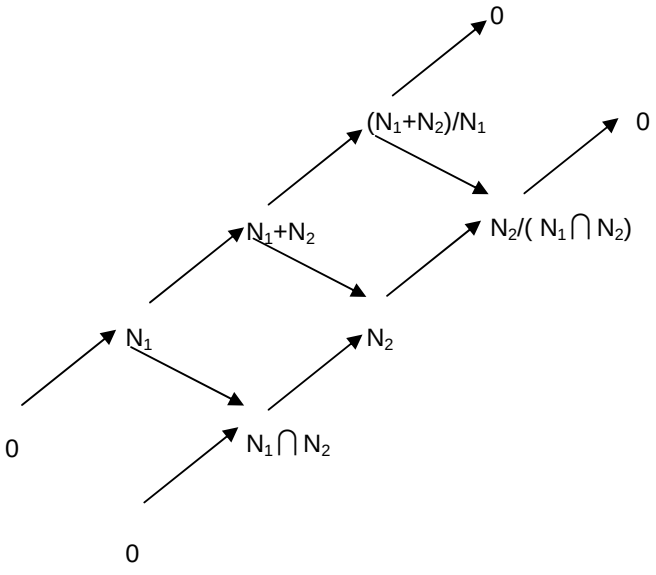
25) Suite exacte scindée : Soit $0 \longrightarrow M' \xrightarrow{\lambda} M \xrightarrow{\mu} M'' \longrightarrow 0$. Une suite exacte de morphismes de modules, on dit que cette suite est scindée si M est une somme directe de deux modules un isomorphe à M', l'autre isomorphe à M/M''.

$$M = M_1 \oplus M2, \text{ avec } M_1 \cong M' \text{ et } M_2 \cong M/M''$$

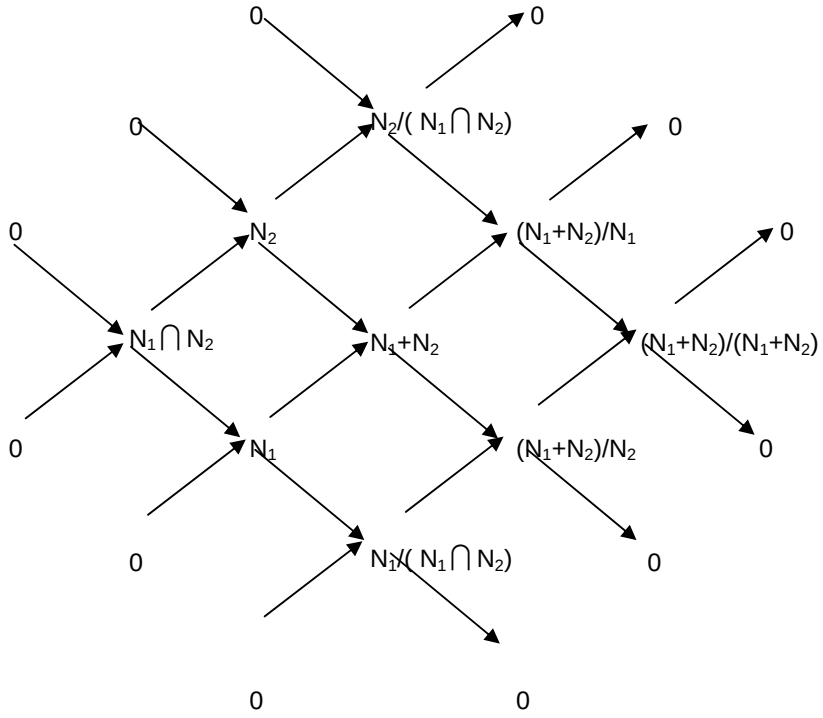
26) ***Réseau de morphismes*** : c'est un réseau où chaque nœud est un module et chaque lien est un morphisme de modules, on dit ***diagramme*** à la place d réseau.

27) ***Diagramme commutatif*** : Soit ($\mathcal{D}$) un diagramme, on dit que ce diagramme est commutatif si le composé des morphismes allant d'un point à un autre par tous les chemin possibles donnent le même morphisme.

28) Second théorème d'isomorphisme par diagramme commutatif:

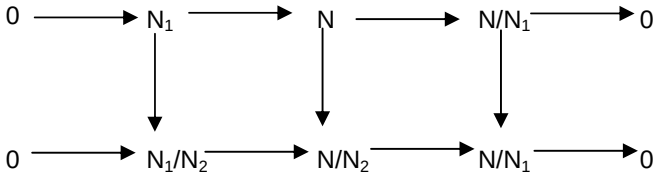


29) Second théorème d'isomorphisme par diagramme commutatif:

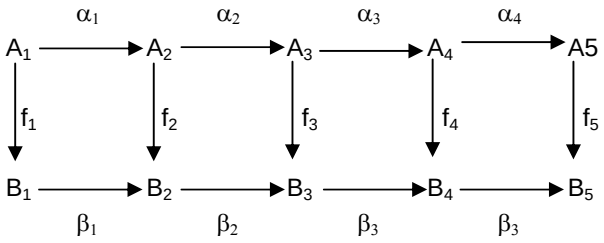


30) Troisième théorème d'isomorphisme par diagramme commutatif :

$N_1 \leq N_2 \leq N$



31) Lemme des cinq :



$(f_1, f_2, f_4, f_5$ isomorphismes) $\Longrightarrow$ f_3 isomorphisme.

(f_1 morphisme surjectif , f_2, f_4 morphismes injectifs) $\Longrightarrow$ f_3 morphisme injectif.
(f_5 morphisme injectif , f_2, f_4 morphismes surjectifs) $\Longrightarrow$ f_3 morphisme surjectif.

32) Exercice : Soit n = rs, et la suite de morphismes :

$$0 \longrightarrow r\mathbb{Z}/n \longrightarrow \mathbb{Z}/n \longrightarrow s\mathbb{Z}/n \longrightarrow 0$$
$$\bar{x} \longmapsto \bar{x} \longmapsto s\,\bar{x}$$

Cette suite est exacte si et seulement si :

$$PGCD(r, s) = 1$$

Anneau principal

33) Anneau Intègre : Soit A un anneau, de zéro 0 et un 1.

34) Diviseur de zéro : Soit *a* un élément non nul de A, on dit que *A* est un diviseur de zéro si :

$$\exists b \text{ non nul dans A, tel que } ab = 0$$

Si D est l'ensemble des diviseurs non nuls de zéro de A :
Et si I l'ensemble des non diviseurs de zéro :

$$A = I \cup D \cup \{0\}$$
$$I \cap D = \varnothing \quad I \cap \{0\} = \varnothing \quad \{0\} \cap D = \varnothing$$

On note $A^* = A\backslash\{0\} = I \cup D$

35) Définition : On dit que l'anneau A est intègre s'il ne contient pas des diviseur de zéro non nuls

$$D = \varnothing$$

36) Anneau Euclidien : Soit A un anneau intègre on définit une application :

$$\deg : A^* \longrightarrow \mathbb{N}$$

Vérifiant :

(E1) $\forall\ a, b \in A^* :\ \deg(ab) < \deg(a)$
(E2) $\forall\ a, b \in A^* :\ \exists q, r \in A$ tq $a = bq + r$, avec $\deg(r) < \deg(b)$ ou $r = 0$

37) Idéal principal : Soit A un anneau intègre, et $\mathfrak{a}$ un idéal de A ($\mathfrak{a} \lhd A$) : on dit que $\mathfrak{a}$ est un idéal principal de A si :

$\exists a$ dans A, tel que $\mathfrak{a}$ est engendré par a : $\mathfrak{a} = aA = (a)$

7) Définition d'un ***Anneau principal*** :
On dit que A est ***principal*** s'il est intègre et si tout idéal de A est principal.

Exemples : $\mathbb{Z}$ est un anneau principal.
Si K est un corps, K[X] est un anneau principal.

38) Théorème : tout anneau euclidien est principal.
Soit A un anneau euclidien, et $\mathfrak{a} \lhd A$:
Il est évident que $\forall\, a \in \mathfrak{a} : aA \subset \mathfrak{a}$.

Réciproquement :

Soit $S = \{\deg(x) \mid x \in \mathfrak{a}\} \subset \mathbb{N}$.
MinS existe soit $m =$ ***Min***S, il existe un $a \in \mathfrak{a} : m = \deg(a)$
Pour tout $b \in \mathfrak{a} : \exists q, r \in A$ tq $b = aq + r$, avec $\deg(r) < \deg(a)$ ou $r = 0$
Comme a est de plus petit degré : $\deg(r) < \deg(a)$ est impossible, il ne reste que $r = 0$, donc : $b = aq \in aA = (a)$, conclusion $\mathfrak{a} \subset aA$
Finalement : $\mathfrak{a} = aA$ et $\mathfrak{a}$ est principal.

39) PGCD : Soient a et b deux éléments de l'anneau principal A :
(a) et (b) sont des idéaux principaux, donc $(a) \bigcap (b)$ est un idéal, donc c'est un idéal principal :

$$(a) \bigcap (b) = (d)$$

$a = da'$ et $b = db'$ d est un diviseur commun de a et b.
Tout diviseur commun de a et b doit diviser d, donc d est le plus grand commun diviseur de a et b, on note : $d = a \wedge b$

40) Anneau Bezoutien : Un anneau intègre a est dit ***bezoutien*** si :
Tout idéal de A engendré par deux éléments est principal :
$\forall\ a, b \in A : aA + bA = (a, b)$ est principal :

$$\exists d \in A : (a, b) = (d)$$

41) Théorème : soit B un anneau ***bezoutien***, on a :

$\forall\ a, b \in A$: si $d = a \wedge b : \exists s, r \in A$ tq : $ra + sb = d$.

42) Théorème : soit B un anneau intègre, on a :

1) Si B un anneau ***bezoutien***, alors : $\forall\ a, b \in B$: le PGCD de a, b $a \wedge b$ existe.
2) Si B est intègre, et $\forall\ a, b \in B$: le PGCD de a, b, existe ; alors B est ***bezoutien***,
3) Si B est de type fini, alors B est principal.
4) Si $a_1, a_2, \ldots, a_n \in A$ et d leur PGCD : $d = (a_1, a_2, \ldots, a_n)$ alors :
5) Tout ensemble fini d'élément de B possède un PGCD et un PPCM.

43) Radical : Soit R un anneau commutatif, $\mathfrak{a}, \mathfrak{b}$ des idéaux de R on définit les opérations suivantes sur les idéaux :

$$\mathfrak{a} + \mathfrak{a} = \{a + b \in R \mid a \in \mathfrak{a} \text{ et } b \in \mathfrak{a}\}$$
$$\mathfrak{a}\,\mathfrak{a} = \{\sum a_i b_i \in R \mid a_i \in \mathfrak{a} \text{ et } b_i \in \mathfrak{a}\}$$
$$\mathfrak{a} : \mathfrak{a} = \{x \in R \mid x\,\mathfrak{a} \subset \mathfrak{a}\}$$

Si S est une partie de R:

$$\mathfrak{a} : S = \bigcap \{\mathfrak{a} : (x) \mid x \in S\}$$

(x) étant l'idéal de R engendré par x.

Exercices : Montrer

$$\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$$
$$(\mathfrak{a} : \mathfrak{b})\,\mathfrak{b} \subset \mathfrak{a} \subset \mathfrak{a} : \mathfrak{b}$$
$$(\bigcap \mathfrak{a}_i) : \mathfrak{b} = \bigcap (\mathfrak{a}_i : \mathfrak{b})$$
$$\mathfrak{a} : (\bigcap \mathfrak{b}_i) = \bigcap (\mathfrak{a} : \mathfrak{b}_i)$$
$$(\mathfrak{a} : \mathfrak{b}) : \mathfrak{c} = \mathfrak{a} : (\mathfrak{b}\,\mathfrak{c})$$

$\mathfrak{a} = (a_1, \ldots\ldots, a_r)$ et $\mathfrak{b} = (b_1, \ldots\ldots, b_s)$ alors

$$\mathfrak{a} + \mathfrak{b} = (a_1, \ldots\ldots, a_r, b_1, \ldots\ldots, b_s)$$

$$\mathfrak{a}\,\mathfrak{b} = (a_1 b_1, \ldots\ldots, a_1 b_s, \ldots\ldots, a_r b_1, \ldots\ldots, a_r b_s)$$

$(\mathfrak{a} \cap \mathfrak{b}).(\mathfrak{a} + \mathfrak{b}) = \mathfrak{a}\mathfrak{b}$

(n diviseur de m) $\Rightarrow$ (m):(n) = (m/n)

(n premier avec m) $\Rightarrow$ (m):(n) = (0)

(6):(35) = (0)

44) Théorème : Soit $\mathfrak{a}, \mathfrak{b}$ deux idéaux de type fini de R tel que $\mathfrak{a} + \mathfrak{b}$ est un idéal principal, alors : $\mathfrak{a} \cap \mathfrak{b}$ est de type fini.

Idéaux premiers et factorisation : Soit R un anneau ***factoriel*** (tout *élément a une factorisation unique*)

Atome : un élément ***a*** de R est dit atome si :

(a1) ***a*** est non inversible

(a2) ***a*** n'est pas produit de deux non inversibles.

Premier : un élément p de R est dit premier si :

(p1) ***p*** n'est ni nul ni inversible

(p2) pour tous a, b de R : si ***p*** divise ab alors ***p*** divise a ou b.

Remarque : dans un anneau factoriel, toute atome est un premier.
Si x est non nul et non inversible, x est produit d'atomes.

Anneau atomique : soit a un anneau intègre, on dit que A est atomique si :

(A) tout élément non nul et non inversible est produit d'atomes.

Remarque :

A anneau factoriel $\Leftrightarrow$
(A intègre, et tout non nul non inversible est produit de premiers)

N.B. Les anneaux algébriques ne sont pas en général des anneaux factoriels.

Un ***atome*** correspond à un ***idéal maximal***

Un ***premier*** correspond à un ***idéal premier***

Idéal premier : soit $\mathfrak{p}$ un idéal de R, on dit que $\mathfrak{p}$ est un idéal premier si :

(ip1) $\mathfrak{p} \neq R$

(ip2) $\forall x, y \in R$ si $xy \in \mathfrak{p}$ alors ($x \in \mathfrak{p}$ et $y \in \mathfrak{p}$)

N.B. R n'est pas un idéal premier de R.

p premier $\Leftrightarrow$ ***(p)*** l'idéal engendré par p est premier.

45) Théorème : soit $\mathfrak{p}$ un idéal de R :

$\mathfrak{p}$ premier $\Leftrightarrow$ $R/\mathfrak{p}$ est un anneau intègre.

NB. Dans un anneau commutatif R : $\mathfrak{p}$ maximal $\Leftrightarrow$ $\mathfrak{p}$ premier.
Si R n'est pas nul il possède nécessairement au moins un idéal maximal, et celui-ci est premier.

46) Partie multiplicative : Soit s une partie de l'anneau R, on dit que S est une partie multiplicative si :
(PM1) $1 \in S$
(PM2) $x, y \in S \Rightarrow xy \in S$.

Remarque : Soit S une partie multiplicative ne contenant pas 0, alors :
Il existe un idéal $\mathfrak{m}$ de R qui est maximal pour la propriété $\mathfrak{m} \cap S = \varnothing$

47) Le NilRadical : Soit R un anneau commutatif on dit qu'un élément a de R est ***nilpotent*** si :
Il existe un entier n tel que $a^n = 0$

On note ***NilRad***(R) l'ensemble des éléments ***nilpotents*** de R :

$$\textbf{\textit{NilRad}}(R) = \{a \in R \mid \text{Il existe un entier n tel que } a^n = 0\}$$

48) Radical d'un idéal : soit $\mathfrak{a}$ un idéal de R on appelle radical de a et on note $\sqrt{\mathfrak{a}}$ ***l'ensemble*** :

$$\sqrt{\mathfrak{a}} = \{x \in R \mid \text{Il existe un entier n tel que } x^n \in \mathfrak{a}\}$$

Exercices : montrer que $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$ et $\sqrt{\mathfrak{a}^n} = \sqrt{\mathfrak{a}}$

$$\sqrt{\mathfrak{ab}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$$

NB. Dans un anneau ***Artinien*** tout idéal premier est maximal :

Si $(\mathfrak{p}_i)$ est une chaîne d'idéaux alors : $\bigcap \mathfrak{p}_i$ et $\bigcup \mathfrak{p}_i$ sont premiers.

La Localisation (anneaux locaux)

49) Théorème : Soit R un anneau commutatif non nécessairement intègre. S une partie multiplicative, on définit sur $R \times S$ une relation binaire $\approx$:

$$(r, s) \approx (r', s') \iff [\text{il existe un t dans s tel que } t(rs' - r's) = 0]$$

Montrer en exercice que $\approx$ est une relation d'équivalence.
L'ensemble quotient $R \times S / \approx$ sera noté R_S et il est muni naturellement d'une structure d'anneau, la classe d'équivalence de (r, s) sera notée $\frac{r}{s}$ comme pour les fractions rationnelles. Les opérations induites seront :

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'} \qquad \frac{r}{s}\frac{r'}{s'} = \frac{rr'}{ss'}$$

NB. Si S ne contient pas de diviseurs de 0 (si R est intègre, 0 ne doit pas être dans s), l'application naturelle

$$\lambda : R \longrightarrow R_S \quad x \longmapsto \frac{x}{1} \text{ est injective.}$$

Ceci permet d'identifier R avec l'image $\lambda(R)$ on écrira indifféremment x ou $\frac{x}{1}$, exactement comme on fait dans $\mathbb{Q}$ $n = \frac{n}{1}$.

Application inversant X : soit $f : R \longrightarrow R'$ une application, on dit qu'elle inverse X, si tout élément de f(X) est inversible dans R'.

50) Théorème : Soit R un anneau commutatif, et S une partie multiplicative de R, on suppose que R_S est l'anneau local par S, et que l'application naturelle $\lambda : R \longrightarrow R_S$ définie par $x \longmapsto \frac{x}{1}$, inverse S, alors (λ, R_S) est une solution ***d'application universelle*** :

Pour toute morphisme d'anneaux $f : R \longrightarrow R'$ inversant S, il existe un seul morphisme (celui-ci est donc un isomorphisme) $f' : R_S \longrightarrow R'$ tel que :

$$f' \circ \lambda = f$$

Donc : R_S est déterminé à un isomorphisme unique près.

51) Cas de S = R\\$\mathfrak{p}$: Soit $\mathfrak{p}$ un idéal premier de R, on vérifie (en exercice) que S = R\\$\mathfrak{p}$: est une partie multiplicative l'anneau R_S est noté aussi R_p, dit anneau local de l'idéal premier $\mathfrak{p}$ ou, anneau local de R en $\mathfrak{p}$.

si l'application naturelle est $\lambda : R \longrightarrow R_p$

$\lambda(\mathfrak{p})$ est un idéal maximal de R_p

Produit tensoriel

Module libre : Soit K un anneau commutatif et X un ensemble, on définit l'anneau $K_x = K \times \{x\}$ isomorphe à K par l'application naturelle

$$k \longmapsto (k, x)$$

Les opérations sur :

$$k' + h' = (k, x) + (h, x) = (k+h, x)$$
$$k(h, x) = (kh, x)$$

On dit que K_x est une copie de K.

Soit X un ensemble on appelle K-module libre sur X le K-module libre :

$K^{(X)} = \bigoplus_{x \in X} K_x$ somme directe de X copies de K.

Un élément de $K^{(X)}$ est de la forme $(e_x)_{x \in X}$ suite d'éléments de K indexés par l'ensemble X.

Une base de ce module libre est $\{(\delta_{ab})_{b \in X}\}_{a \in X}$

On peut écrire $K^{(X)} = \{\sum \alpha_i x_i \mid \alpha_i \in K, x_i \in X$, les α_i non nuls sont finis$\}$

On rappelle que K^X est l'ensemble des applications de X dans K.

La somme $\sum \alpha_i x_i + \sum \beta_i x_i = \sum (\alpha_i + \beta_i) x_i$

Produit par un scalaire $k . \sum \alpha_i x_i = \sum (k\alpha_i) x_i$

Famille linéairement indépendante : $\{x_i\}$ est une famille linéairement indépendante si

$$\sum \alpha_i x_i = 0 \quad \Rightarrow \quad \text{tous les } \alpha_i = 0$$

Famille linéairement dépendante : $\{x_i\}$ est une famille linéairement dépendante si elle n'est pas linéairement indépendante.

N.B. il faut faire attention que si une famille est linéairement dépendante un élément de la famille ne s'exprime pas forcément comme combinaison linéaire des autres.

Remarque : $K^{[1;n]} \cong K^n$ (isomorphisme)

Produit tensoriel : Soit K un anneau commutatif, U, V, W des K-modules.
On construit le module libre sur k par l'ensemble $U \times V$:

$$A = K^{(U \times V)}$$

$U \times V$ est identifié à une partie de $K^{(U \times V)}$

On définit les ensembles :

$X_1 = \{ (u + u', v) - (u, v) - (u', v) \mid u, u' \in U, \ v \in V \}$
$X_2 = \{ (u, v + v') - (u, v) - (u, v') \mid u \in U, \ v, v' \in V \}$
$X_3 = \{ (\alpha u , v) = \alpha(u, v) \mid u \in U, \ v \in V , \alpha \in K \}$
$X_4 = \{ (u , \alpha v) = \alpha(u, v) \mid u \in U, \ v \in V , \alpha \in K \}$

Par réunion on définit :

$$U \lozenge V = X_1 \bigcup X_4 \bigcup X_4 \bigcup X_4.$$

Soit B le sous K-module libre de A engendré par $U \lozenge V$, il est aussi le K-module libre défini sur $U \lozenge V$:

$$B = K^{(U \lozenge V)}$$

$U \lozenge V$ fait partie de par l'injection canonique $j : U \lozenge V \longrightarrow K^{(U \lozenge V)}$

Comme $B = K^{(U \lozenge V)}$ est un sous module de $A = K^{(U \times V)}$ ceci donne le module quotient A/B
La surjection canonique

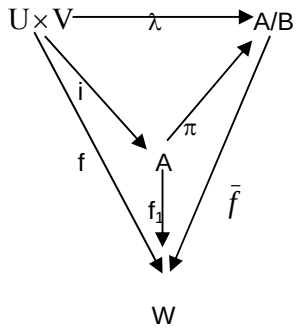
$$\pi : K^{(U \times V)} \longrightarrow A/B$$

Soit $f : U \times V \longrightarrow W$ une application bilinéaire

$$f(u + u', v) = f(u, v) + f(u', v)$$
$$f(u, v + v') = f(u,v) + f(u, v')$$
$$f(\alpha u , v) = \alpha f(u, v)$$
$$f(u , \alpha v) = \alpha f(u, v)$$

A étant un K-module libre il est solution d'un problème d'application universelle
f en tant qu'une application, peut être prolongée en un morphisme unique

$$f_1 : A \longrightarrow W$$



$$\ker(f_1) \supset B$$

Donc pour tout x élément de B $f_1(x) = 0$
En particulier :
$(u + u', v) - (u, v) - (u', v) \in B$ alors
$f_1((u + u', v) - (u, v) - (u', v)) = f_1(u + u', v) - f_1(u, v) - f_1(u', v) = 0$
Donc

$$f_1(u + u', v) = f_1(u, v) + f_1(u', v)$$

$(u, v + v') - (u, v) - (u, v') \in B$ alors
$f_1((u, v + v') - (u, v) - (u, v')) = f_1(u, v + v') - f_1(u, v) - f_1(u, v') = 0$
Donc

$$f_1(u, v + v') = f_1(u, v) + f_1(u, v')$$

$(\alpha u, v) - \alpha(u, v) \in B$ alors
$f_1((\alpha u , v) - \alpha(u, v)) = f_1(\alpha u , v) - f_1(\alpha(u, v)) = f_1(\alpha u , v) - \alpha f_1(u, v) = 0$
Donc :

$$f_1(\alpha u , v) = \alpha f_1(u, v)$$

$(u, \alpha v) - \alpha(u, v) \in B$ alors
$f_1((u , \alpha v) - \alpha(u, v)) = f_1(u , \alpha v) - f_1(\alpha(u, v)) = f_1(u , \alpha v) - \alpha f_1((u, v)) = 0$
Donc

$$f_1(u , \alpha v) = \alpha f_1((u, v))$$

Le morphisme f_1 peut être décomposé à travers le quotient A/B :

$$f_1 = \bar{f} \circ \pi$$

Avec $\bar{f} : A/B \longrightarrow W$

Mais pour le quotient A/B le diagramme est aussi commutatif : $\pi \circ i = \lambda$

$$\bar{f} \circ (\pi \circ i) = f$$
$$(\bar{f} \circ \pi) \circ i = f$$
$$f_1 \circ i = f$$

On en déduit :

$$\bar{f} \circ \lambda = \bar{f} \circ (\pi \circ i) =$$
$$(\bar{f} \circ \pi) \circ i =$$
$$f_1 \circ i = f$$

D'où :

$$\bar{f} \circ \lambda = f$$

Par suite :

A/B = $K^{(U \times V)} / K^{(U \diamondsuit V)}$ on le note par $U \otimes V$:

$$U \otimes V = A/B.$$

λ (u, v) notée $u \otimes v$

Donc

$$\bar{f} \circ \lambda (u, v) = f(u, v)$$
$$\bar{f} (u \otimes v) = f(u, v)$$

Pour λ on a les mêmes égalités :

$$\lambda(u + u', v) = \lambda(u, v) + \lambda(u', v)$$
$$\lambda(u, v + v') = \lambda(u, v) + \lambda(u, v')$$
$$\lambda(\alpha u, v) = \alpha\lambda(u, v)$$
$$\lambda(u, \alpha v) = \alpha\lambda(u, v)$$

Qui s'écrivent en produit tensoriel :

$$(u + u') \otimes v = u \otimes v + u' \otimes v$$
$$u \otimes (v + v') = u \otimes v + u \otimes v'$$
$$(\alpha u) \otimes v) = \alpha(u \otimes v)$$
$$u \otimes (\alpha v) = \alpha\lambda(u \otimes v)$$

$u \mapsto u \otimes v$, $v \mapsto u \otimes v$ sont des morphismes canoniques de k-modules

On a

$$\mathrm{Hom}(U, \mathrm{Hom}(V,W)) \cong \mathrm{Hom}(U \otimes V, W)$$
$$U \otimes (V \otimes W) \cong (U \otimes V) \otimes W$$

Notés $U \otimes V \otimes W$

$$V \otimes U \cong U \otimes V$$
$$U \otimes (V \otimes W) \cong (U \otimes V) \otimes (U \otimes W)$$

Exercices sur les anneaux et les corps

1) Soit (A, +, .) un anneau, et f un endomorphisme de A, on pose $A_0 = \{x \in A \mid f(x) = x\}$ montrer que A_0 est un sous-anneau de A.

Soit E un ensemble on note A^E l'ensemble de toutes les applications de A dans E, et l'on définit sur A^E les lois f + g et f.g par :

$$E \xrightarrow{f+g} A,\ x \mapsto f(x) + g(x) \quad \text{et} \quad E \xrightarrow{f.g} A,\ x \longmapsto f(x).g(x)$$

Montrer que (A^E, +, .) est un anneau.

Trouver une condition pour que (A^E, +, .) soit commutatif.

On suppose que chacun des ensemble E et A possède au moins deux éléments, trouver un diviseur de zéro dans $(A^E, +, \bullet)$.

2) Soit A, A' deux anneaux unitaires, $f : A \longrightarrow A'$ un morphisme d'anneaux unitaires. On note N = ***Ker***(f) ; soit I' un idéal bilatère de A', et soit $\mathfrak{I} = f^{-1}(\mathfrak{I}')$.

i) Montrer que $\mathfrak{I}$ est un idéal bilatère de A contenant N.

ii) On note $\boldsymbol{p} : A \longrightarrow A/\mathfrak{I}$ et $\boldsymbol{p'} : A \longrightarrow A'/\mathfrak{I}'$ et les surjections canoniques,

a) Montrer qu'il existe une application unique $\bar{f} : A/\mathfrak{I} \longrightarrow A'/\mathfrak{I}'$ telle que :

$$\bar{f} \circ \boldsymbol{p} = \boldsymbol{p} \circ f$$

b) Montrer que $\bar{f}$ est un morphisme d'anneaux unitaires.

c) montrer que f est injective.

d) Montrer que si f est surjective, alors $\bar{f}$ est un isomorphisme d'anneaux.

3) Soit A, A' deux anneaux unitaires, $f : A \longrightarrow A'$ un morphisme d'anneaux. On note N = ***Ker***(f) ;

i) Soit B' un sous-anneau de a', montrer que $B = f^{-1}(B')$ est un sous-anneau de a contenant N.

ii) Si *f* est surjective, montrer que B' = *f*(B) et que les anneaux B/N et B' sont isomorphes.

4) Soit A un anneau unitaire et T un ensemble quelconque et $\{\mathfrak{I}_t\}_{t\in T}$ une famille d'idéaux à gauche dans a. on suppose que pour tout couple (t, r) d'éléments de t, il existe s dans T tel que $\mathfrak{I}_t \subset \mathfrak{I}_s$ et $\mathfrak{I}_r \subset \mathfrak{I}_s$.

Montrer que $\mathfrak{I} = \bigcup_{t\in T} \mathfrak{I}_t$ est un idéal à gauche.

5) Soit A un anneau unitaire $\mathfrak{I}$ un idéal à gauche de A, $\mathfrak{K}$ un idéal à droite de A, on désigne $\mathfrak{I} * \mathfrak{K}$ l'ensemble des x de A ayant la propriété suivante :

Il existe n un entier naturel non nul et des familles finies $x_1, x_2, \ldots, x_n$ de $\mathfrak{I}$ et $y_1, y_2, \ldots, y_n$ de $\mathfrak{K}$ tel que : $x = x_1y_1 + x_2y_2 + \ldots + x_ny_n$.

i) Montrer que I*K est un idéal bilatère.

ii) Soit $\mathcal{B}$ l'ensemble des idéaux bilatères de A. montrer que $(\mathcal{B}, *)$ est un monoïde.

iii) On suppose que A est commutatif, montrer que $\mathfrak{I} + \mathfrak{K} = A \Rightarrow \mathfrak{I} * \mathfrak{K} = \mathfrak{I} \cap \mathfrak{K}$.

6) Soit A un anneau commutatif et a, b, c des éléments de A.

Calculer la somme $(a + b + c)^3 + (a - b - c)^3 + (-a + b - c)^3 + (-a - b + c)^3$.

5) dans un anneau quelconque $(A, +, \bullet)$ on définit une nouvelle loi $x * y = xy - yx$

i) Montrer que $*$ est anticommutative

ii) Démontrer l'identité de Jacobi $x*(y*z) + y*(z*x) + z*(x*y) = 0$

6) Soit A un anneau unitaire d'unité 1 et soit x de A tel que y = 1 – x soit nilpotent, c'est-à-dire il existe n un entier non nul tel que $y^n = 0$.

Montrer que x est inversible et que si x' est son inverse alors 1 – x' est nilpotent.

7) Soit A un anneau contenant un sous-anneau A' isomorphe à Q et soit x un élément de A, nilpotent d'indice p +1 (p +1 est le plus petit entier tel que $x^{p+1} = 0$)

On pose $e^x = 1 + x + \frac{x^2}{2!} + \ldots\ldots + \frac{x^{p-1}}{(p-1)!} + \frac{x^p}{p!}$

Soit y un élément nilpotent d'indice q + 1 de A, avec q ≤ p. montrer que :

Si x et y sont permutables on a : $e^{x+y} = e^x \bullet e^y$

8) Soit E un ensemble quelconque et A = $\mathcal{P}$(E) l'ensemble de toutes les parties de E, on définit sur A les loi de composition internes $\cap$ et Δ.

Montrer que $(A, \cap, \Delta)$ est un anneau commutatif et unifère, on l'appelle anneau de ***Boole***.

9) Soit (A, +, •) un anneau intègre et unifère, on dit que A est un ***anneau factoriel*** s'il vérifie les propriétés suivantes :

(***AF1***) Tout élément non nul de A, est décomposable, en un produit fini d'éléments irréductibles.

Elément irréductible : Un élément a de A est dit irréductible si et seulement si a est divisible par les éléments de $(a\mathfrak{U}) \cup \mathfrak{U}$ où $\mathfrak{U}$ est l'ensemble des éléments inversibles de A.

(***AF2***) Cette décomposition est ***unique*** à un facteur inversible près.

(Anglais : ***U***nique ***F***actorisation ***D***omain)

Montrer que si ***p*** est un élément irréductible de A, et divise ab alors ***p*** divise l'un des facteurs a ou b.

10) Soit (K, +, •) un corps et a un élément de K, donner une expression simple du produit :

$$\boldsymbol{p} = (1 + a)(1 + a^2)(1 + a^4)(1 + a^8)\ldots\ldots\ldots\ldots (1 + a^{2n})$$

Soit A un anneau, $\mathfrak{p}$ un idéal de A, on dit que $\mathfrak{p}$ est un idéal premier si :

$$(\forall\, a, b \in A)\ ((ab \in \mathfrak{p}) \Rightarrow (a \in \mathfrak{p} \text{ ou } b \in \mathfrak{p}))$$

Montrer que si p est bilatère alors :

$$(A/\mathfrak{p} \text{ est intègre}) \Rightarrow (\mathfrak{p} \text{ est premier})$$

11) Soit A un anneau unifère, et $\mathfrak{M}$ un idéal bilatère de A, on dit que $\mathfrak{M}$ est un idéal ***maximal*** de A si :

($\mathfrak{M}1$) $\mathfrak{M} \neq A$

($\mathfrak{M}2$) Pour tout idéal $\mathfrak{p}$ de A : $(\mathfrak{M} \subset \mathfrak{p} \subset A) \Rightarrow (\mathfrak{p} = \mathfrak{M}$ ou $\mathfrak{p} = A)$

i) Caractériser les idéaux maximaux de $\mathbb{Z}$.

ii) Montrer que si $A/\mathfrak{M}$ est un corps alors $\mathfrak{M}$ est un idéal maximal.

Anneau Euclidien

Etude des nombres entiers pouvant s'écrire comme somme de deux carrés

A) Caractérisation des nombres premiers p pour lesquels –1 est résidu quadratique : Dans cette, on cherche les nombres premiers impairs p pour lesquels –1 est résidu quadratique modulo p, c'est à dire pour les quels –1 est un carré dans le corps $\mathbb{Z}/p\mathbb{Z}$.

A-1) On considère l'application définie sur $\mathbb{Z}/p\mathbb{Z}$ privé de 0 par $f(x) = x^{-1}$.

Montrer que f est réalise une involution de $\mathbb{Z}/p\mathbb{Z}$ privé de 0, dans lui-même. En déduire qu'elle est bijective et déterminer ses points fixes.

En regroupant quand cela est possible dans le produit $(p-1)!$, chaque facteur x et son image par f, établir l'égalité suivante dans le corps $\mathbb{Z}/p\mathbb{Z}$ (théorème de ***Wilson***)

$$(p-1)! = -1$$

A-2) On considère l'application définie sur $\mathbb{Z}/p\mathbb{Z}$ privé de 0, par $g(x) = -x^{-1}$.

Montrer que g réalise une involution de $\mathbb{Z}/p\mathbb{Z}$ privé de 0, dans lui-même, en déduire qu'elle est bijective et déterminer le nombre de ses points fixes en distinguant deux cas, selon que –1 est ou non résidu quadratique modulo p.

En regroupant (quand cela est possible) dans le produit $(p-1)!$ Chaque facteur x et son image par g, établir l'égalité suivante dans le corps $\mathbb{Z}/p\mathbb{Z}$

$$(p-1)! = (-1)^{\frac{p-3}{2}} \quad \text{si } -1 \text{ est résidu quadratique modulo } p$$

$$(p-1)! = (-1)^{\frac{p-1}{2}} \quad \text{si } -1 \text{ n'est pas résidu quadratique modulo } p$$

A-3) Déduire de ces résultats que :

A-3-1) Si p est congru à 3 (ou –1) modulo 4, alors –1 n'est pas résidu quadratique modulo p.

A-3-2) Si p est congru à 1 modulo 4, alors –1 est résidu quadratique modulo p.

Donner à titre d'exemple les racines carrées de –1 dans $\mathbb{Z}/17\mathbb{Z}$ et $\mathbb{Z}/29\mathbb{Z}$.

B) Caractérisation des nombres premiers p sommes de deux carrés : On rappelle que $\mathbb{Z}[\boldsymbol{i}]$ est le sous anneau de $\mathbb{C}$ défini par $\mathbb{Z}[\boldsymbol{i}] = \{a + \boldsymbol{i}b \mid (a, b) \in \mathbb{Z}\}$

B-1) Etablir qu'un élément $a + \boldsymbol{i}b$ de $\mathbb{Z}[\boldsymbol{i}]$ est inversible ***ssi*** (si et seulement si) $a^2 + b^2 = 1$, et en déduire les éléments inversibles dans $\mathbb{Z}[\boldsymbol{i}]$.

B-2) Montrer que $\mathbb{Z}[\boldsymbol{i}]$ est euclidien, donc principal ; à cet effet, on montrera que tout couple $(a + \boldsymbol{i}b, c + \boldsymbol{i}d)$ de $(\mathbb{Z}[\boldsymbol{i}])^2$ avec $c + \boldsymbol{i}d \neq 0$, il existe au moins un couple $(p + \boldsymbol{i}q, r + \boldsymbol{i}s)$ de $(\mathbb{Z}[\boldsymbol{i}])^2$ tel que : $a + \boldsymbol{i}b = (c + \boldsymbol{i}d) \times (p + \boldsymbol{i}q) + r + \boldsymbol{i}s$ avec $r^2 + s^2 < c^2 + d^2$

B-3) On désigne par p un nombre premier impair congru à 1 modulo 4.

B-3-1) Déduire des résultats de la question A) l'existence de nombres entiers x tels que p divise $x^2 + 1$.

B-3-2) Monter que p ne divise ni $x - \boldsymbol{i}$ ni $x + \boldsymbol{i}$ dans l'anneau $\mathbb{Z}[\boldsymbol{i}]$.

B-3-3) En déduire qu'il existe deux éléments non inversibles $a + \boldsymbol{i}b$ et $c + \boldsymbol{i}d$ de l'anneau $\mathbb{Z}[\boldsymbol{i}]$ tel que $p = (a + \boldsymbol{i}b) \times (c + \boldsymbol{i}d)$, puis établir que $a^2 + b^2 = c^2 + d^2 = p$.

B-4) Montrer réciproquement qu'un nombre premier p somme de deux carrés d'entiers est soit égal à 2, soit congru à 1 modulo 4 s'il est impair.

C) Caractérisation, des nombres entiers naturels, sommes de deux carrés : Dans cette question, on désigne par n un nombre entier naturel non nul.

C-1) On considère quatre nombres entiers a, b, c, d. Montrer qu'il existe deux nombres entiers naturels x, y tels que $(a^2 + b^2) \times (c^2 + d^2) = x^2 + y^2$

C-2) En déduire que si les exposants des nombres premiers congrus à 3 modulo 4, figurant dans la décomposition de n en facteurs premiers sont pairs, alors n est somme de deux carrés d'entiers.

C-3) Réciproquement, on suppose qu'il existe deux nombres entiers x et y tels que $n = x^2 + y^2$, ou $n = d^2(a^2 + b^2)$ en notant d le ***pgcd*** de x et y. On considère un nombre entier p congru à 3 modulo 4 figurant dans la décomposition de n en facteurs premiers, et l'on note r $(r > 0)$ et s $(s \geq 0)$ ses exposants dans la décomposition en facteurs premiers de n et d.

C-3-1) Montrer que p ne divise pas à la fois a et b, que $r - 2s$ est positif, et que p^{r-2} divise $a^2 + b^2$

C-3-2) En déduire, si r est impair, l'existence d'un élément X de tel que $X^2 = -1$.

C-3-3) En déduire que *r* est nécessairement pair, puis conclure à quelle ***CNS*** (condition nécessaire et suffisante) un nombre entier naturel non nul *n* est somme de deux carrés d'entiers.

Algèbre MPSI 2004

1) ***Racines d'un polynôme complexe*** : Soit m un entier naturel, et A = $\{z_1, z_2,\ldots, z_m\}$, *m* nombres complexes, on définit l'***enveloppe convexe*** de A comme étant :

Convexe(A) =$\{\alpha_1 z_1 +\alpha_2 z_2 + \ldots+\alpha_m z_m |\ (\alpha_1, \alpha_2, \ldots, \alpha_m)\in[0;1]^m, \alpha_1 +\alpha_2 + \ldots+\alpha_m =1\}$

Soit P un élément de $\mathbb{C}[X]$, et $\{z_1, z_2,\ldots, z_n\}$ *n* entier naturel, ses racines distinctes ou non. Le but de l'exercice est de montrer que les racines du polynôme ***dérivé*** P' sont situées dans ***Convexe***($\{z_1, z_2, \ldots, z_n\}$), l'enveloppe convexe des racines de P.
Soit u un nombre complexe tel que P'(*u*) = 0.

1°) Prouver le résultat dans le cas où *u* est également racine de P.

2°) On suppose que *u* est racine de P' mais pas de P. En utilisant la décomposition en ***éléments simples*** de $\frac{P'}{P}$, montrer que : $\sum_{p=1}^{n} \frac{1}{\overline{u} - \overline{z_p}} = 0$.

En déduire que $u = \sum_{p=1}^{n} \alpha_p z_p$ avec :

$$\alpha_p = \frac{1}{|u - z_p|^2}\left(\sum_{k=1}^{n} \frac{1}{|u - z_k|^2}\right)^{-1}$$, puis conclure.

2) ***Centre du groupe symétrique*** :

A. Soit (G, *) un groupe. On considère le sous-ensemble ***Z***(G) = $\{g \in G \mid \forall h \in G, g*h = h*g\}$, (c'est l'ensemble des éléments de G qui commutent avec (***tous***) les éléments de G)

1°) Que peut-on dire de ***Z***(G) lorsque G est un groupe commutatif ?

2°) Montrer que ***Z***(G) est un ***sous-groue*** commutatif de G (même lorsque G n'est pas commutatif).

B. Soit $n\in\mathbb{N}^*$, on note S_n l'ensemble des permutations de $[\![1;n]\!]$ (i.e. les ***bijections*** de $[\![1;n]\!]$ dans lui-même). Pour $(i, j) \in [\![1;n]\!]^2$, l'application $\tau_{i,j}$ de $[\![1;n]\!]$ dans $[\![1;n]\!]$ définie par :

$\tau_{i,j}(i) = j$, $\tau_{i,j}(j) = i$, et $\forall k\in [\![1;n]\!]$, $\tau_{i,j}(k)= k$. ($\tau_{i,j}$ est la ***transposition*** échangeant *i* et *j*)

1°) Rappeler le ***cardinal*** de S_n. Donner tous les éléments de S_1, S_2, S_3. Déterminer le nombre des transpositions de $[\![1\,;n]\!]$.

2°) Montrer que $(S_n, \circ)$ est un groupe. Pour $n \geq 3$, comparer $\tau_{1,2}\circ\tau_{1,3}$ et $\tau_{1,3}\circ\tau_{1,2}$. La loi $\circ$ est-elle commutative sur S_n ?

3°) Soit i, j et k trois éléments distincts de $[\![1\,;n]\!]$ ($n \geq 3$). Soit f tel que $f(i) = j$. Montrer que $f \circ \tau_{i,k} \circ f^{-1} = \tau_{j,f(k)}$ puis que $f \circ \tau_{i,k} \neq \tau_{i,k} \circ f$.

4°) En déduire que, pour $n \geq 3$, $\boldsymbol{Z}(S_n) = \{ \boldsymbol{Id}_{[[i\,;n]]} \}$.

3) ***K[X] anneau principal*** : Soit **I** un sous-ensemble de K[X], où K un corps commutatif tel que :

(*i*) (**I**, +) est un sous-groupe de (K[X], +)

(*ii*) $\forall A \in \mathbf{I}, \forall P \in K[X], AP \in \mathbf{I}$.

1°)

a) Montrer que **I** est un sous-espace vectoriel de K[X], et que **I** est table par produit.

b) Si **I** est une sous-algèbre de K[X], montrer que **I** = K[X].

2°) Dans cette question, on veut montrer que qu'il existe $A_0 \in K[X]$, tel que :

$$\mathbf{I} = A_0K[X] = \{A_0P \mid P \in K[X]\}$$

a) Répondre à la question dans le cas $\mathbf{I} = \{0\}$.

b) On suppose désormais que $\mathbf{I} \neq \{0\}$. Soit $N = \{\boldsymbol{deg}(P) \mid P \in \mathbf{I}, P \neq 0\}$. Montrer que admet un plus petit élément p. Soit $A_0 \in \mathbf{I}$ tel que $\boldsymbol{deg}(A_0) = p$, et soit $U = \{A_0P \mid P \in K[X]\}$.

Montrer que $U = \mathbf{I}$ (procéder par ***double inclusion*** ; pour $\supset$ utiliser la ***division euclidienne*** par A_0)

3°) Montrer que : $\forall P \in K[X], \exists!(A, B) \in \mathbf{I} \times K_{p-1}[X]$, $P = A+B$ (*p* a la même définition qu'au ***2)***). On dit que **I** et $K_{p-1}[X]$, sont des sous-espaces ***supplémentaires*** de dans K[X].

Algèbre MPSI 2004 (Solution)

1) ***Racines d'un polynôme complexe*** : Soit m un entier naturel, et A = $\{z_1, z_2, \ldots, z_m\}$, *m* nombres complexes, on définit l'***enveloppe convexe*** de A comme étant :

Convexe(A) = $\{\alpha_1 z_1 + \alpha_2 z_2 + \ldots + \alpha_m z_m \mid (\alpha_1, \alpha_2, \ldots, \alpha_m) \in [0;1]^m,\ \alpha_1 + \alpha_2 + \ldots + \alpha_m = 1\}$

Soit P un élément de $\mathbb{C}[X]$, et $\{z_1, z_2, \ldots, z_n\}$ *n* entier naturel, ses racines distinctes ou non. Le but de l'exercice est de montrer que les racines du polynôme ***dérivé*** P' sont situées dans ***Convexe***($\{z_1, z_2, \ldots, z_n\}$), l'enveloppe convexe des racines de P.
Soit u un nombre complexe tel que P'(*u*) = 0.
1°) Prouver le résultat dans le cas où *u* est également racine de P.
2°) On suppose que *u* est racine de P' mais pas de P. En utilisant la décomposition en ***éléments simples*** de $\frac{P'}{P}$, montrer que : $\sum_{p=1}^{n} \frac{1}{\overline{u} - \overline{z_p}} = 0$.

En déduire que $u = \sum_{p=1}^{n} \alpha_p z_p$ avec :

$$\alpha_p = \frac{1}{|u - z_p|^2} \left(\sum_{k=1}^{n} \frac{1}{|u - z_k|^2} \right)^{-1}$$, puis conclure.

1°) Prouver le résultat dans le cas où *u* est également racine de P.

2°) On suppose que *u* est racine de P' mais pas de P. En utilisant la décomposition en ***éléments simples*** de $\frac{P'}{P}$, montrer que : $\sum_{p=1}^{n} \frac{1}{\overline{u} - \overline{z_p}} = 0$.

En déduire que $u = \sum_{p=1}^{n} \alpha_p z_p$ avec :

$$\alpha_p = \frac{1}{|u - z_p|^2} \left(\sum_{k=1}^{n} \frac{1}{|u - z_k|^2} \right)^{-1}$$, puis conclure.

2) ***Centre du groupe symétrique*** :

A. Soit (G, *) un groupe. On considère le sous-ensemble ***Z***(G) = $\{g \in G \mid \forall h \in G,\ g*h = h*g\}$, (c'est l'ensemble des éléments de G qui commutent avec (***tous***) les éléments de G)
1°) Que peut-on dire de ***Z***(G) lorsque G est un groupe commutatif ?
2°) Montrer que ***Z***(G) est un ***sous-groue*** commutatif de G (même lorsque G n'est pas commutatif).

1°) Que peut-on dire de ***Z***(G) lorsque G est un groupe commutatif ?

2°) Montrer que ***Z***(G) est un ***sous-groue*** commutatif de G (même lorsque G n'est pas commutatif).

B. Soit $n \in \mathbb{N}^*$, on note S_n l'ensemble des permutations de $[\![1;n]\!]$ (i.e. les ***bijections*** de $[\![1;n]\!]$ dans lui-même). Pour $(i, j) \in [\![1;n]\!]^2$, l'application $\tau_{i,j}$ de $[\![1;n]\!]$ dans $[\![1;n]\!]$ définie par :

$\tau_{i,j}(i) = j$, $\tau_{i,j}(j) = i$, et $\forall k \in [\![1;n]\!]$, $\tau_{i,j}(k) = k$. ($\tau_{i,j}$ est la ***transposition*** échangeant i et j)

1°) Rappeler le ***cardinal*** de S_n. Donner tous les éléments de S_1, S_2, S_3. Déterminer le nombre des transpositions de $[\![1;n]\!]$.

2°) Montrer que $(S_n, \circ)$ est un groupe. Pour $n \geq 3$, comparer $\tau_{1,2} \circ \tau_{1,3}$ et $\tau_{1,3} \circ \tau_{1,2}$. La loi $\circ$ est-elle commutative sur S_n ?

3°) Soit i, j et k trois éléments distincts de $[\![1;n]\!]$ ($n \geq 3$). Soit f tel que $f(i) = j$.

Montrer que $f \circ \tau_{i,k} \circ f^{-1} = \tau_{j,f(k)}$ puis que $f \circ \tau_{i,k} \neq \tau_{i,k} \circ f$.

4°) En déduire que, pour $n \geq 3$, $\boldsymbol{Z}(S_n) = \{ \boldsymbol{Id}_{[[i;n]]} \}$.

1°) Rappeler le ***cardinal*** de S_n. Donner tous les éléments de S_1, S_2, S_3. Déterminer le nombre des transpositions de $[\![1;n]\!]$.

2°) Montrer que $(S_n, \circ)$ est un groupe. Pour $n \geq 3$, comparer $\tau_{1,2} \circ \tau_{1,3}$ et $\tau_{1,3} \circ \tau_{1,2}$. La loi $\circ$ est-elle commutative sur S_n ?

3°) Soit i, j et k trois éléments distincts de $[\![1;n]\!]$ ($n \geq 3$). Soit f tel que $f(i) = j$.

Montrer que $f \circ \tau_{i,k} \circ f^{-1} = \tau_{j,f(k)}$ puis que $f \circ \tau_{i,k} \neq \tau_{i,k} \circ f$.

4°) En déduire que, pour $n \geq 3$, $\boldsymbol{Z}(S_n) = \{ \boldsymbol{Id}_{[[i;n]]} \}$.

3) ***K[X] anneau principal*** : Soit **I** un sous-ensemble de K[X], où K un corps commutatif tel que :

(*i*) (**I**, +) est un sous-groupe de (K[X], +)

(*ii*) $\forall A \in \mathbf{I}, \forall P \in K[X], AP \in \mathbf{I}$.

1°)

a) Montrer que **I** est un sous-espace vectoriel de K[X], et que **I** est table par produit.

b) Si **I** est une sous-algèbre de K[X], montrer que **I** = K[X].

2°) Dans cette question, on veut montrer que qu'il existe $A_0 \in K[X]$, tel que :

$$\mathbf{I} = A_0K[X] = \{ A_0P \mid P \in K[X] \}$$

a) Répondre à la question dans le cas **I** = {0}.

b) On suppose désormais que $\mathbf{I} \neq \{0\}$. Soit $\mathbb{N} = \{\deg(P) \mid P \in \mathbf{I}, P \neq 0\}$. Montrer que admet un plus petit élément *p*. Soit $A_0 \in \mathbf{I}$ tel que $\deg(A_0) = p$, et soit $\mathbb{U} = \{A_0P \mid P \in K[X]\}$.

Montrer que $\mathbb{U} = \mathbf{I}$ (procéder par ***double inclusion*** ; pour $\supset$ utiliser la ***division euclidienne*** par A_0)

3°) Montrer que : $\forall P \in K[X], \exists!(A, B) \in \mathbf{I} \times K_{p-1}[X], P = A+B$ (*p* a la même définition qu'au ***2)***). On dit que **I** et $K_{p-1}[X]$, sont des sous-espaces ***supplémentaires*** de dans K[X].

1°) a) Montrer que **I** est un sous-espace vectoriel de K[X], et que **I** est table par produit.

1°) b) Si **I** est une sous-algèbre de K[X], montrer que **I** = K[X].

2°) Dans cette question, on veut montrer que qu'il existe $A_0 \in K[X]$, tel que :

$$\mathbf{I} = A_0K[X] = \{ A_0P \mid P \in K[X] \}$$

2°) a) Répondre à la question dans le cas **I** = {0}.

2°) b) On suppose désormais que $\mathbf{I} \neq \{0\}$. Soit $\mathbb{N} = \{\deg(P) \mid P \in \mathbf{I}, P \neq 0\}$. Montrer que admet un plus petit élément *p*. Soit $A_0 \in \mathbf{I}$ tel que $\deg(A_0) = p$, et soit $\mathbb{U} = \{A_0P \mid P \in K[X]\}$.

Montrer que $\mathbb{U} = \mathbf{I}$ (procéder par ***double inclusion*** ; pour $\supset$ utiliser la ***division euclidienne*** par A_0)

3°) Montrer que : $\forall P \in K[X], \exists!(A, B) \in \mathbf{I} \times K_{p-1}[X], P = A+B$ (*p* a la même définition qu'au ***2)***). On dit que **I** et $K_{p-1}[X]$, sont des sous-espaces ***supplémentaires*** de dans K[X].