Chapitre 4 : Notes de cours

I Notions de logique

A) Mise en garde

L'objectif de ce paragraphe n'est pas une initiation à la logique mathématique formelle mais, plus modestement et plus fondamentalement, l'apprentissage de l'écriture et de la lecture d'un texte mathématique.

On trouvera un véritable exposé de la théorie des ensembles dans *Théorie axiomatique des ensembles*, J.L. Krivine.

L'auteur d'un texte mathématique utilise constamment deux langages : un langage de communication (ici, le Français) et le langage symbolique de la logique mathématique qui, outre tous les alphabets imaginables, contient des symboles.

La principale difficulté est que ces langages sont incompatibles entre eux et qu'il leur faut pourtant cohabiter et même s'éclairer l'un l'autre.

Le Français nous est nécessaire pour être compréhensibles : un texte écrit uniquement de manière symbolique est évidemment illisible. Mais il ne peut pas se substituer au langage symbolique qui est essentiel pour donner des définitions et des énoncés rigoureux. Par exemple, il va de soi que la définition de la continuité uniforme d'une fonction $f : \mathbb{R} \to \mathbb{R}$ ne peut se donner que sous la forme

$$\forall \varepsilon > 0, \exists \alpha > 0, \forall (x,y) \in \mathbb{R}^2, (|x-y| < \alpha \Rightarrow |f(x)-f(y)| < \varepsilon)$$

En outre, les énoncés écrits dans chacun de ces langages doivent être totalement disjoints. Un énoncé mélangeant les deux peut conduire à des erreurs grossières. En particulier, les symboles logiques $\Rightarrow, \Leftrightarrow, \forall, \exists$ ne doivent pas être utilisés comme des abréviations.

Les mots de la langue Française ne doivent pas non plus être considérés comme des objets mathématiques.

B) Assertions, axiomes

Une théorie formelle est constituée *d'assertions* portant sur des *objets*, dont la collection constitue *l'univers* de la théorie, reliés par des *relations*. Lorsque l'objet y est identique à x, on dira que x et y sont égaux et, en général, on écrit $x = y$ ou $y = x$.

Une assertion peut être *vraie* ou *fausse*. Toute théorie « raisonnable » est *non contradictoire*, c'est-à-dire qu'aucune assertion n'est à la fois vraie et fausse (principe du tiers exclus). On admet que c'est le cas de la théorie des ensembles qu'on utilise ici.

Certaines assertions sont supposées vraies à priori. On les appelle *axiomes* de la théorie.

Exemple :

Les mathématiques, que l'on peut identifier ici à la *théorie des ensembles* décrite sommairement plus loin, constituent une théorie formelle dont les objets sont des ensembles. Deux ensembles peuvent être reliés par *la relation d'appartenance*, notée $\in$.

$\mathbb{N}$, $\mathbb{R}$, $\sqrt{2}$, la fonction exponentielle sont des ensembles. On a $\sqrt{2} \in \mathbb{R}$.

C) Raisonnements

Le but du théoricien est de savoir si certaines assertions (celles qui l'intéressent) sont vraies ou fausses.

Pour obtenir de nouvelles assertions à partir d'assertions données A, B,…, on dispose des connecteurs logiques :

La *négation* (la négation de A est notée (non$A$) et se lit 'non A')

La *disjonction* (la disjonction de A et B est notée (A ou B) et se lit 'A ou B')

La *conjonction* (la conjonction de A et B est notée (A et B) et se lit 'A et B')

L'implication (l'implication de B par A est notée ($A \Rightarrow B$) et se lit 'A implique B')

L'équivalence (l'équivalence de A et B est notée ($A \Leftrightarrow B$) et se lit 'A équivaut à B' ou 'A si et seulement si B')

1) Règles de logique

Les assertions sont régies par les *règles de logiques*. On retiendra les définitions et les règles de raisonnement suivantes :

- Définitions :

- *Négation* : (non$A$) est vraie si et seulement si A est fausse.
- *Disjonction* : (A ou B) est vraie si et seulement si l'une au moins des assertions A ou B est vraie.
- *Conjonction* : (A et B est vraie si et seulement si les assertions A et B sont toutes deux vraies.
- *Implication* : l'assertion ($A \Rightarrow B$) n'est autre que ((non$A$) ou B). Ainsi, $A \Rightarrow B$ est vraie si et seulement si B est vraie ou A est fausse.

Remarque : la signification du symbole $\Rightarrow$ est très différente des expressions 'implique' ou 'si…, alors'

En particulier, $A \Rightarrow B$ est vraie dans le cas où A est fausse.

- *Equivalence* : l'assertion $A \Leftrightarrow B$ n'est autre que $((A \Rightarrow B) \text{ et } (B \Rightarrow A))$.

Donc $A \Leftrightarrow B$ est vraie si et seulement si on est dans l'un des deux cas :

A et B sont toutes les deux vraies.

Ou A et B sont toutes les deux fausses.

$A \Leftrightarrow B$ est fausse si et seulement si l'une est vraie et l'autre fausse.

- Règles de raisonnement :

- Comment prouver une assertion A ? plusieurs méthodes :

* Pour toute assertion A, ($A \Rightarrow A$) est vraie.

* Si les assertions B et $B \Rightarrow A$ sont vraies, alors A est vraie.

On peut rédiger cette démonstration de A de la manière suivante :

On sait que B et $B \Rightarrow A$ sont vraies, donc A est vraie.

* (Disjonction de cas). Si les trois assertions ($A_1 \Rightarrow A$), ($A_2 \Rightarrow A$) et (A_1 ou A_2) sont vraies, alors A est vraie.

On peut rédiger cette démonstration de A de la façon suivante :

Si A_1 est vraie, comme on sait que $A_1 \Rightarrow A$ est vraie, A l'est aussi.

Si A_1 est fausse, alors A_2 est vraie car (A_1 ou A_2) est vrai ; or, $A_2 \Rightarrow A$ est vraie donc A est encore vraie.

* (Raisonnement par l'absurde) Si A et B sont deux assertions telles que $(\text{non}A \Rightarrow B)$ et $(\text{non}A \Rightarrow \text{non}B)$ sont vraies, alors A est vraie.

Remarque :

Raisonner par l'absurde revient à ajouter l'axiome $(\text{non}A)$ à la théorie et à prouver que cette nouvelle théorie est contradictoire.

On peut rédiger cette démonstration de la manière suivante :

'Raisonnons par l'absurde en supposant A fausse. On a…' suivi des preuves de B et de non$B$.

- Comment prouver une implication ?

* (Directe) Pour prouver que $A \Rightarrow B$ est vraie, on suppose A vraie et on prouve B.

* (Syllogisme) Si les assertions $A \Rightarrow B$ et $B \Rightarrow C$ sont vraies, alors $A \Rightarrow C$ est aussi vraie.

* (Contraposée) Si A et B sont deux assertions, $\text{non}B \Rightarrow \text{non}A$ s'appelle contraposée de $A \Rightarrow B$. Ces deux assertions sont équivalentes. Pour prouver $A \Rightarrow B$, on peut donc supposer B fausse et montrer qu'alors A l'est aussi.

- Négations :

Théorème :

Soient A, B, C des assertions.

(1) non(non$A$) équivaut à A.

(2) non(A et B) équivaut à non$A$ ou non$B$.

(3) non(A ou B) équivaut à non$A$ et non$B$.

(4) $\text{non}(A \Rightarrow B)$ équivaut à A et non$B$.

2) Assertions indécidables

Dans certains cas, les axiomes d'une théorie T ne permettent pas de démontrer qu'une certaine assertion A est vraie ou fausse. A est alors dite *indécidable* dans T.

Si A est indécidable, A ou non$A$ est vraie, mais on ne sait pas laquelle des deux assertions l'est : la véracité de l'assertion A est 'indécidable' à l'intérieur de la théorie T.

De plus, si on ajoute aux axiomes de T l'assertion A (resp. non$A$), on obtient une nouvelle théorie T' (resp. T'') non contradictoire.

Exemples :

K. Gódel a montré que pour toute théorie des ensembles 'contenant l'ensemble $\mathbb{N}$', il existe une assertion indécidable. Un temps, certains ont émis l'idée que cela aurait pu être le cas du grand théorème de Fermat, qui a été récemment prouvé par A. Wiles :

$$\forall (n,x,y,z) \in \mathbb{N}^4, (n \geq 3 \text{ et } x^n + y^n = z^n) \Rightarrow xy = 0$$

P. Cohen a prouvé, en particulier, que dans la plus petite théorie des ensembles contenant l'arithmétique, l'assertion « il existe une partie E de $\mathbb{R}$ contenant $\mathbb{N}$ qui n'est en bijection ni avec $\mathbb{N}$ ni avec $\mathbb{R}$' » est indécidable.

C'est extrêmement troublant puisqu'on peut construire $\mathbb{R}$ de manière essentiellement unique à partir de $\mathbb{N}$!

D) Quantificateurs

1) Définitions

A partir d'une assertion $A(x)$ d'une théorie T, dépendant de l'objet x, on construit les deux assertions $\exists x : A(x)$ et $\forall x, A(x)$:

$\exists x : A(x)$ est vraie si et seulement si il existe un objet x tel que $A(x)$ soit vraie. Elle se lit : 'il existe x tel que $A(x)$'.

Pour prouver l'assertion $\exists x : A(x)$, il faut montrer l'existence d'un objet x vérifiant $A(x)$. Le plus souvent, on donnera un exemple, ou une méthode de construction, de l'objet x et on rédigera la démonstration sous la forme 'prenons $x = \ldots$' ou 'Prenons x tel que…' suivi de la vérification de $A(x)$.

Attention :

$\exists x : A(x)$ peut être vraie sans que l'on sache 'construire' un tel x, par exemple à l'aide d'un algorithme.

$\forall x, A(x)$ est vraie si et seulement si pour tout objet x, $A(x)$ est vraie. Elle se lit 'pour tout x, $A(x)$'.

Pour prouver l'assertion $\forall x, A(x)$, on prouvera toutes les assertions $A(x)$ pour tous les objets x et on rédigera la démonstration sous la forme 'Soit x. On a…' suivi de la vérification de $A(x)$.

2) Cas de plusieurs quantificateurs

Lorsqu'on dispose d'une assertion $A(x, y, ...)$ dépendant de plusieurs objets, on pourra 'superposer' des quantificateurs. Par exemple $\exists x : (\forall y, (\exists z : A(x, y, z)))$ est une assertion.

Dans le cas d'une assertion comportant plusieurs quantificateurs, on prendra garde à l'ordre de ceux-ci et à leur parenthésage.

Remarque :

Pour prouver l'assertion $\exists x : (\forall y, A(x, y))$, il faut prouver l'existence d'un x vérifiant $A(x, y)$ pour tout y. L'objet x ne doit donc pas dépendre de y.

Pour prouver $\forall y, (\exists x : A(x, y))$, il faut prouver que, pour tout y, il existe x tel que $A(x, y)$. x peut, dans ce cas, dépendre de y.

Théorème :

Soit $A(x, y)$ une assertion dépendant des objets x et y. Les assertions suivantes sont vraies :

$$(\exists x : (\exists y : A(x, y))) \Leftrightarrow (\exists y : (\exists x : A(x, y)))$$

$$(\forall x, (\forall y, A(x, y))) \Leftrightarrow (\forall y, (\forall x, A(x, y)))$$

$$(\exists x : (\forall y, A(x, y))) \Rightarrow (\forall y, (\exists x : A(x, y)))$$

Remarque :

On écrira souvent $\exists x, y : A(x, y)$ ou $\forall x, y, A(x, y)$ au lieu de $\exists x : (\exists y : A(x, y))$ ou $\forall x, (\forall y, A(x, y))$.

L'implication $(\forall y, (\exists x : A(x, y))) \Rightarrow (\exists x : (\forall y, A(x, y)))$ est, en général, fausse. Beaucoup de problèmes de mathématiques reviennent à prouver cette implication pour des assertions $A(x, y)$ particulières.

3) Notations

On utilisera les abréviations suivantes :

$\exists x : (x \in y \text{ et } A(x))$ s'écrira plutôt $\exists x \in y : A(x)$

$\forall x, (x \in y \Rightarrow A(x))$ s'écrira plutôt $\forall x \in y, A(x)$

On utilise aussi l'assertion suivante :

$\exists! x : A(x)$ se lit : 'il existe un unique x tel que $A(x)$' et qui équivaut à la conjonction des deux assertions : $\exists x : A(x)$ et $\forall x, y, (A(x) \text{ et } A(y)) \Rightarrow x = y$

4) Négation d'une assertion quantifiée

On retiendra que $\text{non}(\exists x : A(x))$ équivaut à $\forall x, \text{non}(A(x))$.

Et $\text{non}(\forall x, A(x))$ équivaut à $\exists x : \text{non}(A(x))$.

Remarque : lorsqu'il y a plusieurs quantificateurs, la négation s'écrit de manière automatique…

II Notions de théorie des ensembles

A) Axiomes de la théorie des ensembles

Intuitivement, l'univers U de la théorie des ensembles est une 'collection' d'objets appelés ensembles.

Attention : l'univers U n'est pas lui-même un ensemble, ce sont les objets de U qu'on appelle ensemble. On retiendra que tous les objets qu'on définit en mathématique (nombres, points, vecteurs, fonctions, espaces de fonctions…) sont des ensembles.

U est muni de la relation d'appartenance, notée $\in$, qui vérifie un certain nombre d'axiomes. La relation $x \in y$ se lit indifféremment 'x appartient à y' ou 'y contient x'…Lorsque l'assertion $x \in y$ est fausse, on écrira $x \notin y$ et on lira 'x n'appartient pas à y'…

Pour alléger le langage, on définit aussi la relation d'inclusion :

Soient deux ensembles a et b. On dit que a est inclus dans b ou que a est une partie de b…, et on note $a \subset b$, lorsque l'assertion $\forall x, (x \in a \Rightarrow x \in b)$ est vraie. C'est-à-dire que a est inclus dans b si et seulement si tout élément de a est élément de b.

Il existe plusieurs théories des ensembles, ayant des systèmes d'axiomes différents. La plus couramment utilisée est celle de Zermelo–Fraenkel ; elle permet la construction des ensembles usuels et c'est dans son cadre que nous nous placerons (et que se font aussi quasiment toutes les mathématiques actuelles).

Nous n'en expliciterons pas complètement les axiomes ; citons simplement les premiers :

- Axiome d'extensionnalité (1) :

Deux ensembles ayant exactement les mêmes éléments sont identiques (ou égaux)

- Axiome du singleton :

Si x est un ensemble, il existe un ensemble (unique d'après (1)) ; noté $\{x\}$, et appelé singleton x, ayant exactement pour éléments x. On a $\forall y, (y \in \{x\} \Leftrightarrow y = x)$.

(Cet axiome n'est pas à proprement parler un axiome de la théorie, il se déduit des autres)

- Axiome de la réunion :

Si x et y sont deux ensembles, il existe un ensemble (unique d'après (1)), noté $x \cup y$, tel que $\forall z, (z \in x \cup y \Leftrightarrow (z \in x \text{ ou } z \in y))$

- Axiome de l'ensemble des parties :

Pour tout ensemble a, il existe un ensemble (unique d'après (1)), noté $P(a)$, dont les éléments sont les parties de a, c'est-à-dire tel que $\forall x, (x \in P(a) \Leftrightarrow x \subset a)$

- Ensemble défini par une assertion :

Il y a d'autres axiomes qui permettent, dans certains cas, de définir un ensemble par une propriété caractéristique de ses éléments. Nous n'énoncerons pas ces axiomes, mais nous nous contenterons de signaler la terminologie :

Il existe des assertions $A(x)$ (parfois dites collectivisantes), dépendant de l'ensemble x, telles qu'il existe un ensemble a (unique d'après (1)) vérifiant $\forall x, (x \in a \Leftrightarrow A(x))$

Dans ce cas, l'ensemble a est noté $\{x | A(x)\}$; on dit aussi que a est défini en compréhension par $A(x)$.

Les axiomes évoqués ci-dessus précisent quelles sont les assertions 'collectivisantes' et les règles de construction de ces assertions. Nous admettrons sans justification que les assertions que nous utiliserons sont 'collectivisantes'. Attention, ce n'est pas une propriété générale :

Par exemple, la relation $x \notin x$ ne définit pas un ensemble. En effet, si on avait $a = \{x | x \notin x\}$, alors l'assertion $a \in a$ serait à la fois vraie et fausse.

B) Construction d'ensembles

1) Paires, ensembles définis en extension

Si x, y sont deux ensembles, la réunion $\{x\} \cup \{y\}$ est appelée paire x, y et notée $\{x, y\}$. On a $\forall z, z \in \{x, y\} \Leftrightarrow z = x \text{ ou } z = y$

En particulier, si $x = y$, on a $\{x, y\} = \{x\}$

Plus généralement, si $x_1, \ldots x_p$ sont des ensembles, il existe un unique ensemble, noté $\{x_1, \ldots x_p\}$, dont les éléments sont exactement $x_1, \ldots x_p$.

2) Intersections

Si x et y sont deux ensembles, on admet que l'assertion $A(z)$ définie par $(z \in x \text{ et } z \in y)$ est collectivisante. L'ensemble qu'elle définit est appelé intersection de x et y, noté $x \cap y$.

3) Complémentaires, différences, ensemble vide

Si x, y sont deux ensembles, on admet que l'assertion $A(z)$ définie par $(z \in y \text{ et } z \notin x)$ est collectivisante. L'ensemble qu'elle définit est appelé différence de y et x, noté $y \setminus x$

Dans de cas où $x \subset y$, $y \setminus x$ est appelé complémentaire de x dans y et est noté $C_y x$.

Théorème :

Il existe un unique ensemble a tel que $\forall x, x \notin a$. On note cet ensemble $\varnothing$.

Démonstration :

Si on prend x un ensemble quelconque, $C_x x$ convient. L'unicité résulte de l'axiome 1.

4) Couples, *p*-uplets, produits cartésiens

On appelle couple a, b et on note (a,b), la paire $\{a,\{a,b\}\}$. On appelle triplet a, b, c le couple $(a,(b,c))$ et par récurrence (une fois les entiers connus !), on définit le $(p+1)$-uplet $(a_1,...a_{p+1})$ comme étant le couple, dont le second élément est un p-uplet, $(a_1,(a_2,...a_{p+1}))$.

Théorème :

On a égalité entre les p-uplets $(a_1,a_2,...a_p)$ et $(b_1,b_2,...b_p)$ si et seulement si $b_1 = a_1, \ldots\ b_p = a_p$.

On admet que si E, F sont des ensembles, l'assertion $A(z)$ définie par $\exists x \in E : \exists y \in F : z = (x,y)$ est collectivisante. L'ensemble qu'elle définit est appelé produit cartésien de E et F, noté $E \times F$.

Plus généralement, si E_1, … E_p sont des ensembles, il existe un unique ensemble, appelé produit cartésien des E_i $(i = 1..p)$ et noté $E_1 \times ... \times E_p$ dont les éléments sont exactement les p-uplets $(x_1,...x_p)$ avec $\forall i = 1..p, x_i \in E_i$.

5) Propriétés

Théorème :

Pour a, b, c ensembles, on a les relations :

$a \cup b = b \cup a$, $a \cup \varnothing = a$, $(a \cup b) \cup c = a \cup (b \cup c)$.

$a \cap b = b \cap a$, $a \cap \varnothing = \varnothing$, $(a \cap b) \cap c = a \cap (b \cap c)$.

$a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$, $a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$

Si de plus $a \subset c$ et $b \subset c$, on a :

$C_c(a \cup b) = (C_c a) \cap (C_c b)$, $C_c(a \cap b) = (C_c a) \cup (C_c b)$

Si les E_i $(i = 1..p)$ sont des ensembles non vides, $E_1 \times ... \times E_p$ est non vide.

C) Correspondances, relations binaires, fonctions et applications

1) Définitions

Soient E et F deux ensembles. On appelle correspondance de E vers F tout triplet $\gamma = (G,E,F)$ où G est une partie de $E \times F$. G, E, F s'appellent respectivement *graphe*, *source*, *but* de γ.

Lorsque $(x,y)\in G$, on dit que *y correspond* à *x*.

On appelle *domaine de définition* de la correspondance γ la partie $D=\{x\in E|\exists y\in F:(x,y)\in G\}\subset E$ et on appelle *image* de γ la partie $I=\{y\in F|\exists x\in E:(x,y)\in G\}\subset F$

Une correspondance de *E* vers *E* s'appelle une relation binaire sur *E*.

Une correspondance $\gamma=(G,E,F)$ de E vers F telle que à tout $x\in E$ correspond au plus un élément $y\in F$ est appelée une *fonction* de *E* vers *F*. Cette propriété s'écrit :

$\forall(x,y,y')\in E\times F\times F,((x,y)\in G \text{ et } (x,y')\in G)\Rightarrow y=y'$

On appelle *application* de *E* dans *F* toute fonction γ de *E* vers *F* dont le domaine de définition est $D=E$.

En particulier, une fonction de *E* vers *F* de domaine de définition $D\subset E$ est une application de *D* vers *F*.

Les correspondances de E vers F constituent un ensemble, qu'on peut identifier à $P(E\times F)$. On admet que celles de ces correspondances qui sont des applications constituent aussi un ensemble, *l'ensemble des applications de E vers F*, noté $\mathfrak{F}(E,F)$ ou F^E.

2) Notations fonctionnelles

Si $\gamma=(G,E,F)$ est une fonction de E vers F de domaine de définition $D\subset E$, alors pour tout $x\in D$, il existe un unique $y\in F$ tel que $(x,y)\in G$. y s'appelle *image* de *x* par γ, on le note $\gamma(x)$.

On notera aussi γ sous la forme $\gamma:x\in D\subset E\mapsto\gamma(x)\in F$

Soit $\gamma:D\subset E\to F$ une fonction de *E* vers *F*. Pour tout élément *x* de *D*, $y=\gamma(x)$ s'appelle image de *x* par γ, *x* est alors *un antécédent* de *y* par γ.

Exemples :

On appelle *diagonale* du produit cartésien $E\times E$ l'ensemble $\Delta=\{(x,y)\in E\times E|x=y\}$. La correspondance (Δ,E,E) est une application de *E* vers *E* appelée *identité* de *E* et notée Id_E.

Soient E, F deux ensembles, et $G=\{(x,y,z)\in(E\times F)\times E|z=x\}$. La correspondance $(G,E\times F,E)$ est une application appelée *projection* de $E\times F$ sur *E*. On définit de manière analogue la projection de $E\times F$ sur *F*.

3) Cas de l'ensemble vide

Soient $E=\varnothing$ et *F* un ensemble. On a $E\times F=\varnothing$ donc il existe une unique correspondance de *E* vers *F* ; son graphe est $G=\varnothing$. En fait, cette correspondance est en fait une application, appelée *application vide*.

De même pour tout ensemble *E*, il existe une unique correspondance de *E* vers $\varnothing$; son graphe est $\varnothing$. Mais cette correspondance n'est une application que si *E* est aussi $\varnothing$: il n'existe pas d'application d'un ensemble non vide vers $\varnothing$.

4) Composition, restrictions, corestrictions, réciproques de correspondances

Soient A, B, C trois ensembles. Si $\alpha=(G,A,B)$ et $\beta=(H,B,C)$ sont des correspondances, alors on peut définir

$K=\{(x,z)\in A\times C \mid \exists y\in B:((x,y)\in G \text{ et } (y,z)\in H)\}$

Et $\gamma=(K,A,C)$ est une correspondance, appelée *composée* de α et β, notée $\gamma=\beta\circ\alpha$.

Soient A, B, C trois ensembles avec $C\subset A$ et $\gamma=(G,A,B)$ une correspondance. Alors $(G\cap(C\times B),C,B)$ est une correspondance, appelée *restriction* de γ à C et notée $\gamma_{/C}$.

Si de plus γ est une fonction (resp. une application), sa restriction à C est encore une fonction (resp. une application).

Soient A, B, C trois ensembles avec $C\subset B$ et $\gamma=(G,A,B)$ une correspondance. Alors $(G\cap(A\times C),A,C)$ est une correspondance, appelée *corestriction* de γ à C.

Attention :

Si de plus γ est une fonction, sa corestriction à C est encore une fonction, mais son domaine de définition n'est pas, en général, celui de γ. La corestriction d'une application $f:E\to F$ à $C\subset F$ est une application si et seulement si l'image de E par f est incluse dans C.

Soient A, B deux ensembles et $\gamma=(G,A,B)$ une correspondance.

On note $G^{<-1>}=\{(y,x)\in B\times A \mid (x,y)\in G\}$

La correspondance $(G^{<-1>},B,A)$ s'appelle la *réciproque* de γ.

Remarque :

Une composée, une restriction de fonctions (resp. applications) est une fonction (resp. application)

Mais la réciproque d'une fonction ou d'une application n'est pas toujours une fonction ou une application.

5) Injections, surjections, bijections

- Définitions :

Une application $f:E\to F$ telle que tout $y\in F$ admet au moins (resp. au plus) un antécédent est appelée *surjection* (resp. *injection*). Une application qui est à la fois une surjection et une injection est appelée *bijection*. Au lieu de surjection (resp. injection, resp. bijection), on dit aussi application *surjective* (resp. injective, resp. bijective). Ces définitions s'écrivent sous les formes logiques suivantes :

f est surjective si et seulement si $\forall y\in F,(\exists x\in E:f(x)=y)$

f est injective si et seulement si $\forall(x,x')\in E^2,(f(x)=f(x')\Rightarrow x=x')$

f est bijective si et seulement si $\forall y\in F,(\exists! x\in E:f(x)=y)$

Exemples :

L'identité de l'ensemble E est bijective.

Si A est une partie de E, on appelle *injection canonique* de A dans E l'application $j_A = (\mathrm{Id}_E)_{/A} : A \to E$. C'est, bien sûr, une injection.

Si $F \neq \varnothing$, la projection $(x,y) \in E \times F \mapsto x \in E$ est surjective.

- Propriétés

Théorème :

(1) Une composée de bijections (resp. injections, resp. surjections) est une bijection (resp. injection, resp. surjection).

(2) La correspondance réciproque d'une bijection $f : E \to F$ est une bijection, notée $f^{-1} : F \to E$.

(3) Une application $f : E \to F$ est une bijection si et seulement si il existe une application $g : F \to E$ telle que $f \circ g = \mathrm{Id}_E$ et $g \circ f = \mathrm{Id}_F$

(4) Soient $f : E \to F$ et $g : F \to G$. Si $g \circ f$ est injective, alors f est injective. Si $g \circ f$ est surjective, alors g est surjective.

6) Image directe ou image réciproque d'une partie par une application

Soient E, F deux ensembles et $f : E \to F$ une application.

Pour toute partie B de F, on appelle *image réciproque* de B par f l'ensemble $f^{-1}(B) = \{x \in E \mid f(x) \in B\} \subset E$. De même pour tout $A \subset E$, on appelle *image directe* de A par f l'ensemble $f(A) = \{y \in F \mid \exists x \in A : f(x) = y\} \subset F$.

Remarques :

(1) Soit l'application $f : E \to F$. On peut définir deux applications $f_{\mathrm{dir}} : A \in P(E) \to f(A) \in P(F)$ et $f_{\mathrm{récip}} : B \in P(F) \to f^{-1}(B) \in P(E)$. Il ne faut pas confondre f_{dir} et f et encore moins $f_{\mathrm{récip}}$ et la réciproque de f, f^{-1}, qui n'est définie que si f est bijective.

(2) On peut aussi définir l'image directe de $A \subset E$ par f comme étant $f(A) = \{f(a) \mid a \in A\}$ où on considère la famille $(f(a))_{a \in A}$.

D) Familles, produits cartésiens

1) Familles, sous-familles

Soient I, E deux ensembles. On appelle *famille* d'éléments de E indexée par I toute application $f : I \to E$. Dans ce cas, on oublie la notation fonctionnelle et on écrit la famille sous la forme $(f(i))_{i \in I}$ ou même $(x_i)_{i \in I}$.

On retiendra que pour toute famille indexée par I et pour tout $i \in I$, il existe un unique élément d'indice i.

Si $J \subset I$, on appelle *sous-famille* indexée par J de $(x_i)_{i \in I}$ la restriction à J de l'application $i \in I \mapsto x_i$.

Cas particulier :

Une famille indexée par $I = \mathbb{N}$ est appelée *suite*.

2) Réunion, intersection et produit d'une famille d'ensembles

Soit $(E_i)_{i\in I}$ une famille d'ensembles. On admet que les assertions $U(x)$ et $I(x)$ définies respectivement par $\exists i : x\in E_i$ et $\forall i, x\in E_i$ sont collectivisantes. L'unique ensemble F, noté $\bigcup_{i\in I} E_i$, tel que $\forall x,(x\in F \Leftrightarrow (\exists i\in I : x\in E_i))$ est appelé *réunion* des E_i et l'unique ensemble G, noté $\bigcap_{i\in I} E_i$, tel que $\forall x,(x\in G \Leftrightarrow (\forall i\in I, x\in E_i))$ est appelé *intersection* des E_i.

Soit $(E_i)_{i\in I}$ une famille d'ensembles et $E=\bigcup_{i\in I} E_i$. On admet que les familles $(x_i)_{i\in I}$ d'éléments de E telles que $\forall i\in I, x_i\in E_i$ constituent un ensemble, appelé *produit cartésien* des E_i et noté $\prod_{i\in I} E_i$.

Remarque :

Ces définitions généralisent celles vues en B)4). Les propriétés vues alors se généralisent aussi.

E) Exemples de relation binaire

1) Notation

Soient E un ensemble et R une relation binaire sur E de graphe $G\subset E^2$.

Pour $(x,y)\in E^2$, on définit l'assertion xRy par $xRy \Leftrightarrow (x,y)\in G$.

2) Propriétés éventuelles d'une relation binaire

Soit R une relation binaire sur E de graphe $G\subset E\times E$.

R est dite *réflexive* si elle vérifie $\forall x\in E, xRx$ (c'est-à-dire si la diagonale de $E\times E$ est incluse dans G)

R est dite *symétrique* si elle vérifie $\forall (x,y)\in E^2, (xRy \Leftrightarrow yRx)$

R est dite *antisymétrique* si elle vérifie $\forall (x,y)\in E^2, (xRy \text{ et } yRx) \Rightarrow x=y$

R est dite *transitive* si elle vérifie $\forall (x,y,z)\in E^3, (xRy \text{ et } yRz) \Rightarrow xRz$.

3) Relations d'équivalence, ensembles quotients et partitions

- Définitions :

Une relation binaire R dans l'ensemble E est une *relation d'équivalence* si elle est réflexive, symétrique et transitive.

Soit R une relation d'équivalence sur l'ensemble E. Pour tout $x\in E$, on appelle *classe d'équivalence de x modulo R* la partie $C(x)=\{y\in E | xRy\}\subset E$.

On définit une application par $C : x\in E \mapsto C(x)\in P(E)$.

L'image $C(E)\subset P(E)$ de cette application est appelée *ensemble quotient de E par R* et est notée E/R.

La corestriction $C : x \in E \mapsto C(x) \in E/R$ de C à E/R s'appelle *projection canonique* ; comme elle est surjective, on dira souvent *surjection canonique*.

- Partition associée à une relation d'équivalence :

Propriétés :

Soit R une relation d'équivalence sur E. Pour tout $(x, y) \in E^2$, on a $x \in C(x)$ et soit $C(x) = C(y)$, soit $C(x) \cap C(y) = \varnothing$.

On appelle *partition* de E toute partie P de $P(E)$ telle que :

(1) P ne contient pas $\varnothing$ ($\forall A \in P, A \neq \varnothing$)

(2) P recouvre E ($E = \bigcup_{A \in P} A$)

(3) Deux éléments distincts de P sont disjoints
($\forall A, B \in P, (A \neq B \Rightarrow A \cap B = \varnothing)$)

Théorème :

Si R est une relation d'équivalence sur E, l'ensemble quotient E/R est une partition de E.

Réciproquement, si P est une partition de E, la relation R définie sur E par
$\forall (x, y) \in E^2, (xRy \Leftrightarrow \exists A \in P : (x \in A \text{ et } y \in A))$
Est une relation d'équivalence et on a $P = E/R$.

- Surjection canonique et partition par fibres :

Proposition :

(1) Soit X une partition de l'ensemble E. La relation définie par
$\forall (a, x) \in E \times X, aRx \Leftrightarrow a \in x$
est une surjection $E \to X$.

(2) Inversement, si $f : E \to F$ est une surjection, les fibres $f^{-1}\{y\}$ (pour $y \in F$) constituent une partition de E.

Remarque :

On peut généraliser le point (2) à une application quelconque en considérant la partie X de $P(E)$ constituée des fibres non vides.

- Cas d'un ensemble fini : dénombrement :

Théorème :

Soit E un ensemble fini.

(1) Pour toute partition P de E, on a $\text{card}(E) = \sum_{X \in P} \text{card}(X)$

(2) Soit $f : E \to F$ une application. Alors les fibres de f sont finies et on a $\text{card}(E) = \sum_{y \in F} \text{card}(f^{-1}\{y\})$

(3) Soit R une relation d'équivalence sur E. Alors le cardinal de E est égal à la somme des cardinaux des classes d'équivalence.

- Passage au quotient :

Soient R une relation d'équivalence sur l'ensemble E et $p : E \to E/R$ la projection canonique. Pour toute application $f : E \to F$ on cherche, si elle existe, une application $g : E/R \to F$ telle que $f = g \circ p$. Lorsque g existe, on dit que f passe au quotient ou se factorise par g.

Théorème :

Avec les notations ci-dessus : il y a au plus une fonction g solution. De plus, g existe si et seulement si $\forall (x, y) \in E^2, (xRy \Rightarrow f(x) = f(y))$

4) Relations d'ordre

- Définitions :

On appelle *relation d'ordre* dans l'ensemble E toute relation réflexive, antisymétrique et transitive.

Un couple (E, R) où E est un ensemble et R une relation d'ordre sur E est appelé *ensemble ordonné*.

Une relation d'ordre est en général notée $\leq$ (ou $\preceq \ldots$). Dans ce cas la relation $y \leq x$ est notée $x \geq y$ et la relation ($x \leq y$ et $x \neq y$) est notée $x < y$.

Une relation d'ordre $\leq$ sur E est dite *d'ordre total* si elle vérifie $\forall (x, y) \in E^2, (x \leq y \text{ ou } y \leq x)$. Elle est d'ordre partiel dans le cas contraire. Autrement dit, si deux éléments quelconques de E sont toujours 'comparables' pour $\leq$, la relation $\leq$ est dite d'ordre total.

Exemples :

$\leq$ est une relation d'ordre total dans $\mathbb{N}$ ou $\mathbb{R}$.

La relation de divisibilité notée | est une relation d'ordre partiel dans $\mathbb{N}$, ce n'est pas une relation d'ordre dans $\mathbb{Z}$ (par exemple, on a $-1 | 1$ et $1 | -1$ et $1 \neq -1$)

La relation d'inclusion est d'ordre partiel dans $P(E)$.

Si $(E, \leq)$ est un ensemble ordonné et si $A \subset E$, la restriction de $\leq$ à $A \times A$ est une relation d'ordre sur A.

- Majorants, plus grand élément, éléments maximaux :

(Et aussi minorants, plus petit élément, éléments minimaux)

Soit $(E, \leq)$ un ensemble ordonné et $A \subset E$. On appelle majorant (resp. minorant) de A tout élément $x \in E$ tel que $\forall a \in A, a \leq x$ (resp. $x \leq a$).

Une partie admettant au moins un majorant (resp. minorant) est dite majorée (resp. minorée)

Un élément de A qui majore (resp. minore) A est un plus grand élément (resp. plus petit élément) de A. Une partie a au plus un plus grand (resp. petit) élément.

Un élément M de E est dit maximal (resp. minimal) si il n'admet aucun majorant (resp. minorant) distinct de lui-même.

Exemples :

(1) Dans un ensemble ordonné non vide, la partie $\varnothing$ est minorée et majorée par tout élément.

(2) L'ensemble des majorants de $[0,1[$ dans $\mathbb{R}$ est $[1,+\infty[$; $[0,1[$ est majoré mais n'a pas de plus grand élément.

(3) Dans l'ensemble ordonné $(\mathbb{N}, |)$, $A=\{2,6,70,30\}$ est majorée par tout multiple de 210, elle n'a pas de plus grand élément mais admet un plus petit élément : 2. Si on munit A de la restriction de |, 2 est minimal dans $(A, |)$ et 70, 30 sont maximaux.

(4) Dans $(P(E),\subset)$, $\varnothing$ est minimal et E maximal.

- Bornes inférieures ou supérieures :

Soit $(E,\leq)$ un ensemble ordonné et $A\subset E$. On appelle borne supérieure de A un élément $M\in E$, s'il existe, tel que :

(1) M majore A ($\forall a\in A, a\leq M$)

(2) Tout majorant de A est supérieur à M :

$\forall x\in E,((\forall a\in A, a\leq x)\Rightarrow M\leq x)$

On définit de manière analogue une éventuelle borne inférieure.

Si l'ordre est total, on peut remplacer (2) par

(2b) : Tout élément strictement inférieur à M ne majore pas A :

$\forall x\in E,(x<M\Rightarrow(\exists a\in A, x<a))$

Remarques :

(1) Si la partie A admet un plus grand élément a, alors a est la borne supérieure de A.

(2) Dans tous les cas, une partie admet au plus une borne supérieure.

(3) Pour que A admette une borne supérieure (resp. inférieure), il faut que A soit majorée (resp. minorée) mais cette condition ne suffit pas.

(4) Dans $(\mathbb{R},\leq)$, toute partie non vide et majorée admet une borne supérieure. C'est vrai aussi dans $(\mathbb{N},\leq)$ puisqu'une partie non vide majorée de $\mathbb{N}$ a un plus grand élément.

- Bon ordre, ordre inductif :

Une relation d'ordre $\leq$ sur l'ensemble E est un *bon ordre* si toute partie non vide A de E admet un plus petit élément.

Remarque : une relation de bon ordre est un ordre total.

Exemple :

L'ordre naturel de $\mathbb{N}$ est un bon ordre. De tous les exemples usuels, c'est le seul.

Une relation d'ordre $\leq$ sur E est un ordre *inductif* si toute partie de E totalement ordonnée par $\leq$ admet une borne supérieure.

- L'axiome du choix.

Les mathématiques actuelles reposent toutes sur la théorie des ensembles de Zermelo–Frankael complétée par l'axiome du choix :

'Pour tout ensemble non vide I et toute famille d'ensembles non vides $(E_i)_{i\in I}$, le produit $\prod_{i\in I} E_i$ est non vide'.

Dans la théorie de Zermelo–Frankael, on peut prouver cette propriété quand I est fini, mais le cas général est indécidable.

L'intérêt de cet axiome du choix est de permettre de faire 'simultanément' une infinité de choix indépendants.

Il est, le plus souvent, utilisé à travers ses conséquences sur les ensembles ordonnés qui résultent du lemme de Zorn :

Dans la théorie des ensembles de Zermelo–Frankael, les assertions suivantes sont équivalentes :

(1) Pour tout ensemble X, il existe une application 'de choix' $C : P(X) \setminus \{\varnothing\} \to X$ telle que $\forall A \subset X, (A \neq \varnothing \Rightarrow C(A) \in A)$

(2) Pour tout ensemble non vide I et toute famille d'ensemble non vide $(E_i)_{i \in I}$, $\prod_{i \in I} E_i$ est non vide.

(3) Tout ensemble X peut être muni d'un bon ordre.

(4) Tout ensemble muni d'un ordre inductif admet un élément maximal.

Exemples :

L'utilisation d'une fonction de choix sur E permet de prouver qu'une application $f : E \to F$ est surjective si et seulement si il existe $g : F \to E$ telle que $f \circ g = \mathrm{Id}_F$

5) Une vague idée sur les catégories

On appellera ici *catégorie* une collection d'*objets* reliés entre eux par des *flèches* ou *morphismes*.

Par exemple, on considèrera les catégories des :

Ensembles : les objets sont les ensembles et les morphismes les applications.

Groupes : les objets sont les groupes et les morphismes les morphismes de groupes.

$\mathbb{K}$-espaces vectoriels ($\mathbb{K}$ corps fixé) : les objets sont les $\mathbb{K}$-espaces vectoriels et les morphismes les applications linéaires.

$\mathbb{K}$-espaces vectoriels normés ($\mathbb{K}$ corps fixé) : les objets sont les $\mathbb{K}$-espaces vectoriels normés et les morphismes les applications linéaires continues.

Dans chaque catégorie, nous définirons des notions pertinentes (par exemples, dans toutes les catégories citées, on dispose de la notion de produit cartésien, on peut aussi considérer l'objet de tous les morphismes d'un objet E vers un objet F…) mais, bien sûr, les notions pertinentes dans une catégorie ne le sont plus forcément dans une autre ! par exemple, dans la catégorie des ensembles une notion importante est celle d'un complémentaire d'une partie. Comme un $\mathbb{K}$-espace vectoriel est en particulier un ensemble, on pourra parler de complémentaire d'un sous-$\mathbb{K}$-espace vectoriel ; la notion de complémentaire garde un sens dans la catégorie des $\mathbb{K}$-espaces vectoriels mais n'a aucune pertinence : *on ne peut démontrer aucun résultat d'algèbre linéaire en utilisant la notion de complémentaire !* La notion pertinente dans la catégorie des $\mathbb{K}$-espaces vectoriels qui 'remplace' celle de complémentaire est la notion de sous-espace supplémentaire ; il n'y a malheureusement pas unicité des sous-espaces supplémentaires d'un sous-espace donné.

Par ailleurs, dans chaque catégorie, nous énoncerons des théorèmes dont les hypothèses préciseront en particulier la catégorie dans laquelle ils sont valides.

III Les structures algébriques fondamentales

A) Lois de composition internes et externes

1) Définitions

Soient E, F deux ensembles. On appelle *loi de composition interne* dans E toute application $T : E \times E \to E$. On appelle *loi de composition externe dans E à opérateurs dans F* toute application $T : F \times E \to E$.

Notation :

Si $T : F \times E \to E$ est une loi de composition (éventuellement interne si $E = F$), l'image de $(a,b) \in F \times E$ par la loi T sera notée aTb.

2) Propriétés éventuelles d'une loi de composition interne

Soit T une loi de composition interne sur E.

T est dite *associative* si elle vérifie $\forall (x,y,z) \in E^3, (xTy)Tz = xT(yTz)$

T est dite *commutative* si elle vérifie $\forall (x,y) \in E^2, xTy = yTx$

Un élément de E est dit *élément neutre à droite* (resp. *à gauche*) pour T si il vérifie la propriété $\forall x \in E, xTe = x$ (resp. $\forall x \in E, eTx = x$) Un élément neutre à gauche et à droite et appelé *élément neutre*.

Notation :

Lorsqu'une loi est commutative, on la note généralement + ; si elle admet un élément neutre, celui-ci est alors noté 0. Si la loi n'est pas notée +, qu'elle soit commutative ou pas, un élément neutre éventuel est souvent noté 1.

Un élément a de E est dit *régulier à droite* (resp. *à gauche*) pour T si il vérifie la propriété $\forall (x,y) \in E^2, aTx = aTy \Rightarrow x = y$

(resp. $\forall (x,y) \in E^2, xTa = yTa \Rightarrow x = y$)

Un élément régulier à droite et à gauche est appelé *élément régulier*.

Remarque :

Au lieu de régulier on dit parfois *simplifiable*.

Propriété : une loi de composition interne a au plus un élément neutre.

On suppose que la loi de composition T sur E admet un élément neutre e.

Un élément a de E est dit *symétrique à droite* (resp. *à gauche*) de l'élément b si il vérifie la propriété $bTa = e$ (resp. $aTb = e$), il est dit *symétrique* de b s'il est symétrique à droite et à gauche de b.

Un élément a de E est dit *symétrisable* si il admet un symétrique.

Propriétés :

(1) Si a et b sont symétrisables de symétriques a' et b', alors aTb l'est aussi et son symétrique est $b'Ta'$.

(2) Si T est associative et si a a un symétrique à gauche et un symétrique à droite, ils sont égaux. En particulier, a a au plus un symétrique.

Notation : Lorsque la loi de composition est associative, le symétrique d'un élément symétrisable a, s'il existe, est appelé *inverse* de a et noté a^{-1} sauf si la loi est notée + auquel cas le symétrique est appelé *opposé* et noté $-a$.

3) Cas de deux lois : distributivité

Soient T et * deux lois de composition internes sur E. * est dite *distributive à droite* (resp. *à gauche*) par rapport à T si elle vérifie :

$\forall (x,y,z) \in E^3, (xTy) * z = (x * z) T (y * z)$

(resp. $\forall (x,y,z) \in E^3, z * (xTy) = (z * x) T (z * y)$)

Elle est dite *distributive* si elle est distributive à droite et à gauche.

B) Structures fondamentales

1) Groupes

Définition :

On appelle *groupe* un couple (G,T) où T est une loi de composition interne dans G vérifiant les axiomes :

(1) T est associative.
(2) G admet un élément neutre e pour T.
(3) Tout élément de G admet un symétrique pour e.

Si de plus T est commutative, le groupe est dit *commutatif* ou *abélien*.

Propriétés :

(1) G admet un et un seul neutre.
(2) Tout élément $g \in G$ a un unique symétrique.
(3) Pour $(a,b) \in G^2$, l'équation $aTx = b$ (resp. $xTa = b$) a une unique solution, à savoir $x = (a^{-1}) Tb$ (resp. $x = bT(a^{-1})$ $x = bT(a^{-1})$).

2) Anneaux et corps

Définition :

On appelle *anneau non nécessairement commutatif* (ou 'anneau non commutatif' pour simplifier) un triplet $(A,+,T)$ où + et T sont des lois de compositions internes dans A vérifiant les axiomes :

(1) $(A,+)$ est un groupe abélien (d'élément neutre noté 0)
(2) T est associative et admet un élément neutre distinct de 0
(3) T est distributive par rapport à +.

Si de plus T est commutative, l'anneau est dit *commutatif*.

Plus généralement, deux éléments a et b d'un anneau A sont dits *commutables* si ils vérifient $aTb = bTa$.

Remarque :

L'élément neutre de la seconde loi T d'un anneau est unique, et noté en général 1, 1_A …

Un élément de A admettant un symétrique pour T est inversible.

Proposition :

Soit $(A,+,T)$ un *anneau non nécessairement commutatif*.

(1) L'ensemble, noté A^*, des éléments inversibles de l'anneau $(A,+,T)$ est un groupe pour la loi T.

(2) (Equation linéaire dans un anneau) Soient $a,b,c \in A$ avec a inversible. L'équation $aTx+b=c$ (resp. $xTa+b=c$) a une unique solution $x=(a^{-1})T(c-b)$ (resp. $x=(c-b)T(a^{-1})$)

On appelle *corps* un anneau commutatif $(\mathbb{K},+,T)$ donc tout élément non nul a un symétrique pour *T*, c'est-à-dire un anneau commutatif tel que $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

Attention :

Un corps est *toujours* commutatif. Un anneau non nécessairement commutatif dont tout élément non nul est symétrisable pour *T* est appelé *anneau à divisions* (et pas un corps non commutatif)

3) Espaces vectoriels et algèbres

Soit $\mathbb{K}$ un corps (commutatif).

On appelle $\mathbb{K}$-espace vectoriel tout triplet $(E,+,\cdot)$ où :

$(E,+)$ est un groupe abélien.

$(\lambda,V) \in \mathbb{K}\times E \mapsto \lambda.V \in E$ est une loi de composition externe sur E à opérateurs dans $\mathbb{K}$ telle que pour tout $(x,y,U,V) \in \mathbb{K}^2 \times E^2$:

(1) $1.V = V$ (2) $(x+y).V = x.V + y.V$

(3) $x.(U+V) = x.U + x.V$ (4) $(x\times y).V = x.(y.V)$

Les éléments d'un espace vectoriel *E* sont en général appelés *vecteurs*, bien qu'ils puissent être des nombres, des fonctions… En particulier, l'élément neutre du groupe $(E,+)$ est souvent noté $\vec{0}$.

On appelle $\mathbb{K}$-algèbre tout quadruplet $(A,+,*,.)$ où :

$(A,+,.)$ est un $\mathbb{K}$-espace vectoriel.

* est une loi de composition interne sur *A* associative et bilinéaire, c'est-à-dire telle que pour tout $(x,y,U,V,W) \in \mathbb{K}^2 \times A^3$:

$(x.U+y.V)*W = x.U*W + y.V*W$ et $U*(x.V+y.W) = x.U*V + y.U*W$

Si * admet un élément neutre, on le note en général 1… et on dit que l'algèbre est unitaire ; si * est commutative, l'algèbre est dite commutative.

Remarques :

(1) Les axiomes d'espace vectoriel gardent un sens si on remplace le corps $\mathbb{K}$ par un anneau commutatif. Toutefois, comme les propriétés fondamentales des espaces vectoriels ne se généralisent pas, dans ce cadre on ne parle pas d'espace vectoriel sur un anneau mais de *module sur un anneau commutatif*. Paradoxalement, on parlera d'algèbre sur un anneau commutatif (les axiomes sont les mêmes que pour un corps).

(2) Si $(A,+,*,.)$ est une algèbre unitaire, alors $(A,+,*)$ est un anneau (non nécessairement commutatif).

Attention :

Le programme ne contient aucune définition précise de la notion d'algèbre ; celle donnée ci-dessus est la plus classique mais il y a de nombreuses variantes.

Exemple :

Soit $(\mathbb{L},+,\times)$ un corps et $\mathbb{K}$ un sous–corps de $\mathbb{L}$. Si on note . la restriction du produit $\times:\mathbb{L}\times\mathbb{L}\to\mathbb{L}$ à $\mathbb{K}\times\mathbb{L}\to\mathbb{L}$, alors $(\mathbb{L},+,\times,.)$ est une $\mathbb{K}$-algèbre commutative unitaire intègre.

C) Sous–structures

1) Parties stables pour une loi de composition interne

Définition :

Soit T une loi de composition sur l'ensemble E. Une partie A est dite *stable* pour T si elle vérifie $\forall(x,y)\in A^2, xTy\in A$

Remarque :

La partie vide est stable pour toute loi de composition interne, donc si on veut éviter les mauvaises surprises, pour montrer par exemple qu'une partie d'un groupe est un sous–groupe, on commencera par vérifier qu'il est non vide ((1) ci-dessous)

2) Sous-groupes, sous-groupes distingués

Définition :

On appelle *sous-groupe* du groupe (G,T) toute partie $H\subset G$ vérifiant les axiomes :

(1) H contient l'élément neutre de G.

(2) H est stable par T.

(3) Pour tout $x\in H$, l'inverse x^{-1} de x pour T est élément de H.

Le sous-groupe H est dit *distingué* si il vérifie de plus :

$\forall h\in H,\forall g\in G, gThTg^{-1}\in H$

Remarques :

(1) On peut remplacer les axiomes (2) et (3) par l'unique axiome $\forall(a,b)\in H^2, aTb^{-1}\in H$

(2) Si (G,T) est un groupe commutatif, tout sous-groupe est distingué. Mais ce résultat est faux dans le cas général.

Proposition :

Une intersection quelconque de sous-groupes du groupe (G,T) est un sous-groupe de (G,T).

3) Sous–anneaux et idéaux, sous–corps

Définition :

On appelle *sous–anneau* de l'anneau $(A,+,T)$ tout sous-groupe du groupe $(A,+)$ contenant 1 et stable par T.

On appelle *idéal* de l'anneau commutatif $(A,+,T)$ tout sous-groupe B du groupe $(A,+)$ tel que $\forall (a,b)\in A\times B, aTb = bTa \in B$. Pour tout $a\in A$, la partie $A = \{aTx | x\in A\}$ est un idéal, appelé idéal principal de A engendré par a.

Remarques :

(1) Dans un anneau non commutatif, la notion d'idéal se scinde en trois notions : idéal à droite, idéal à gauche, idéal bilatère. Par exemple, un idéal à gauche de $(A,+,T)$ est un sous-groupe B de A tel que $\forall (a,b)\in A\times B, aTb\in B$.

Dans la suite, on ne parlera d'idéal que dans le cas d'anneaux commutatifs.

(2) Il existe des anneaux ayant des idéaux non principaux : par exemple, $2\mathbb{Z}[X]+X\mathbb{Z}[X]$ est un idéal non principal de $\mathbb{Z}[X]$.

Définition :

On appelle sous–corps du corps $(\mathbb{K},+,T)$ tout sous–anneau L de $\mathbb{K}$ tel que :

$\forall x\in L\setminus\{0\}, x^{-1}\in L$

Propriété :

L'anneau commutatif est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et A.

4) Sous-espaces vectoriels, sous–algèbres

Définitions :

On appelle sous-$\mathbb{K}$-espace vectoriel du $\mathbb{K}$-espac vectoriel E toute partie non vide H de E stable par combinaison linéaire, c'est-à-dire telle que :

(1) $\vec{0}\in H$ (2) $\forall (x,y)\in E^2, \forall (U,V)\in H^2, x.U+y.V\in H$

On appelle sous–algèbre d'une $\mathbb{K}$-algèbre A tout sous-$\mathbb{K}$-espace vectoriel B stable par produit.

Attention :

Le programme ne contient aucune définition précise de la notion de sous-algèbre. Celle donnée ci-dessus est la plus classique mais il y a de nombreuses variantes, en particulier lorsque A est unitaire, où on impose parfois à une sous–algèbre de contenir l'élément unité de sorte qu'une sous–algèbre d'une algèbre unitaire soit aussi un sous–anneau.

D) Morphismes

1) Définitions

Soient (G,T) et (G',T') deux groupes. On appelle *morphisme de groupes* toute application $f: G\to G'$ telle que $\forall (x,y)\in G^2, f(xTy) = f(x)T'f(y)$

Soient $(A,+,T)$ et $(A',+,T')$ deux anneaux. On appelle *morphisme d'anneaux* toute application $f: A\to A'$ telle que $f(1_A) = 1_{A'}$,

$\forall (x,y)\in A^2, f(x+y) = f(x)+f(y)$ et $f(xTy) = f(x)T'f(y)$

Un *morphisme de corps* est un morphisme d'anneaux entre deux corps.

On appelle *isomorphisme* tout morphisme bijectif, *endomorphisme* tout morphisme d'une structure dans elle-même et *automorphisme* tout endomorphisme bijectif.

2) Automorphismes intérieurs d'un groupe

Définition :

Soit (G,T) un groupe. Pour $g \in G$, l'application $A_g : x \in G \mapsto gTxTg^{-1}$ est un automorphisme de (G,T), appelé *automorphisme intérieur* associé à *g*.

Propriétés :

(1) $g \in G \mapsto A_g$ est un morphisme de (G,T) dans le groupe $(\sigma_g, \circ)$ des bijections de l'ensemble *G*. Autrement dit, $\forall g,h \in G, (A_g)^{-1} = A_{g^{-1}}$, $A_g \circ A_h = A_{gTh}$

(2) Un sous-groupe de (G,T) est distingué si et seulement si il est stable par tout automorphisme intérieur de (G,T).

3) Noyau, image d'un morphisme

Si *f* est un morphisme, l'image de *f* est l'ensemble image de *f*.

Si *f* est un morphisme de groupes $f : (G,T) \to (G',T')$, le noyau de *f* est $\ker f = f^{-1}\{e'\}$, image réciproque de l'élément neutre *e'* de (G',T').

Le noyau d'un morphisme d'anneaux est celui du morphisme de groupes abéliens sous-jacent. Si $f : (A,+,T) \to (A',+,T')$ est un morphisme d'anneaux, on a $\ker f = f^{-1}\{0\}$

Propriétés :

L'image directe ou réciproque d'un sous-groupe (resp. d'un sous–anneau) par un morphisme de groupes (resp. d'anneaux) est un sous-groupe (resp. un sous–anneau)

L'image réciproque d'un sous-groupe distingué (resp. d'un idéal) par un morphisme de groupes (resp. d'anneaux commutatifs) est un sous-groupe distingué (resp. un idéal)

En particulier, l'image d'un morphisme de groupes (resp. d'anneaux) est un sous-groupe (resp. un sous–anneau) alors que le noyau d'un morphisme de groupes (resp. d'anneaux commutatifs) est un sous-groupe distingué (resp. un idéal)

Remarques :

(1) Tout morphisme de corps est injectif.

(2) L'image directe d'un sous-groupe distingué (resp. idéal) d'un groupe (resp. anneau) n'est pas en général un sous-groupe distingué (resp. un idéal)

4) Eléments remarquables d'un anneau

Pour l'étude de l'anneau $(A,+,T)$ et d'un élément $a \in A$, on a parfois intérêt à considérer les applications de translation d_a, g_a suivantes :

$d_a : x \in (A,+) \mapsto xTa \in (A,+)$, $g_a : x \in (A,+) \mapsto aTx \in (A,+)$.

Définition :

Les éléments de l'anneau $(A,+,\times)$ (non nécessairement commutatif) inversibles pour $\times$ sont dits tout simplement *inversibles* ; ils forment un ensemble A^* contenant l'élément neutre 1 de $\times$ et stable par $\times$.

Proposition :

Pour tout anneau (même non commutatif), $(A^*,\times)$ est un groupe.

Propriétés :

Soit $(A,+,T)$ un anneau et $a \in A$.

(1) Les applications de translation d_a et g_a sont des endomorphismes du groupe additif $(A,+)$.

(2) On a les équivalences :

- a a un inverse à gauche $\Leftrightarrow d_a$ est surjective.
- a a un inverse à droite $\Leftrightarrow g_a$ est surjective.

Définition :

Un élément $a \in A$ tel que d_a (resp. g_a) est injectif est dit *simplifiable* (ou régulier) *à droite* (resp. *à gauche*). Il est dit simplifiable (ou régulier) s'il est simplifiable à droite et à gauche. Par exemple tout élément inversible est simplifiable (mais $2 \in \mathbb{Z}$ est simplifiable non inversible). Un élément $a \in A$ non simplifiable à droite (resp. à gauche) est un diviseur de 0 à droite (resp. à gauche), c'est-à-dire qu'il existe $b \in A \setminus \{0\}$ tel que $bTa = 0$ (resp. $aTb = 0$)

Un anneau dont tout élément est simplifiable (ou, ce qui revient au même, n'ayant aucun diviseur de 0) est dit *intègre*.

E) Constructions

Les procédés suivants permettent de construire des groupes, des anneaux, des corps mais ils permettent aussi de déterminer rapidement la structure d'un ensemble muni de lois de composition internes données.

1) Structures induites

Soit E un ensemble muni d'une loi T et $A \subset E$ une partie stable par T. La restriction $T_{/A\times A} : A \times A \to E$ est ainsi à valeurs dans A, et sa corestriction $T' : A \times A \to A$ est une loi de composition interne dans A. On l'appelle *loi induite de T* sur A.

Propriétés :

Si T est associative ou commutative, T' l'est aussi. Si $e \in A$ est élément neutre de T dans E, e est aussi élément neutre de T'. Si T admet $e \in A$ comme neutre, un élément $a \in A$ est symétrisable pour T' si et seulement si il l'est pour T *et* son symétrique a' pour T est dans A.

Notation :

Une loi induite est notée avec le même symbole que la loi de départ.

Théorème :

Un sous-groupe (resp. sous–anneau, resp. sous–corps) d'un groupe (resp. anneau, resp. corps) est un groupe (resp. un anneau, resp. un corps) pour les lois induites.

2) Produits

Soit I un ensemble d'indices et, pour tout $i \in I$, un ensemble E_i muni d'une loi de composition interne T_i. La loi de composition T définie sur le produit cartésien $E = \prod_{i \in I} E_i$ par $\forall (X,Y) = ((x_i)_{i \in I}, (y_i)_{i \in I}) \in E^2, XTY = (x_i T_i y_i)_{i \in I}$ est appelée *loi produit*.

Propriétés :

Supposons que les E_i sont tous non vides.

(1) La loi produit est associative (resp. commutative) si et seulement si chaque T_i l'est.

(2) Un élément $(a_i)_{i \in I}$ est neutre, régulier, symétrisable pour T (éventuellement à droite ou à gauche seulement) si et seulement si chaque a_i l'est pour T_i.

Théorème :

Un produit de groupes (resp. d'anneaux) est un groupe (resp. anneau) pour la loi produit (resp. les lois produits)

Attention :

Un produit cartésien d'au moins deux corps n'est pas un corps car, par exemple, $(0,1)$ est non nul non inversible dans $K_1 \times K_2$

3) Quotients

- Relations d'équivalence, partitions, quotients

Soit R une relation d'équivalence sur un ensemble E. Pour $x \in E$, on note $Cl_R(x)$ l'ensemble $Cl_R(x) = \{y \in E | xRy\}$. C'est la classe d'équivalence de x pour R.

Propriété :

L'ensemble des classes d'équivalence de la relation R est une partition de E.

Cette partition est notée E/R et est appelée ensemble quotient de E par R et l'application $x \in E \mapsto Cl_R(x) \in E/R$, qui est clairement surjective, est appelée *surjection canonique*.

- Compatibilité :

Soit T une loi de composition sur l'ensemble E et R une relation d'équivalence sur E. R est dite compatible avec T si elle vérifie :

$\forall (x,y,x',y') \in E^4, (xRx' \text{ et } yRy') \Rightarrow (xTy)R(x'Ty')$

- Exemples fondamentaux (pour les groupes)

Soit (G,T) un groupe et H un sous-groupe. On définit deux relations sur G R_H et ${}_H R$ par :

$\forall (x,y)\in G^2, xR_H y \Leftrightarrow y^{-1}Tx\in H$

Et $\forall (x,y)\in G^2, x\,{}_H R y \Leftrightarrow xTy^{-1}\in H$

Propriétés :

(1) R_H (resp. ${}_H R$) est une relation d'équivalence sur G. Ses classes sont les $aTH=\{aTh \mid h\in H\}$ (resp. HTa) pour $a\in G$

(2) Pour tout sous-groupe H, les propriétés suivantes sont équivalentes :

(i) H est distingué (ii) R_H est compatible avec T.

(iii) ${}_H R$ est compatible avec T. (iv) $R_H = {}_H R$

- Exemples fondamentaux (pour les anneaux commutatifs)

De même, si $(A,+,\times)$ est un anneau commutatif et B un sous–anneau, comme B est un sous-groupe distingué de $(A,+)$, la relation $R_B = {}_B R$ définie par $\forall (x,y)\in B^2, xR_B y \Leftrightarrow x-y\in B$ est compatible avec +

Propriété :

R_B est compatible avec $\times$ si et seulement si B est un idéal de $(A,+,\times)$.

- Structure quotient :

Propriétés :

Si E est muni d'une loi de composition interne T et d'une relation d'équivalence R compatible avec T, il existe une unique loi de composition interne θ sur le quotient E/R telle que la projection canonique $\pi : x\in E \mapsto \bar{x}\in E/R$ soit un morphisme.

Si en plus T est associative (resp. commutative), θ l'est aussi ; si $a\in E$ est neutre (resp. symétrisable de symétrique a') dans E pour T, alors $\bar{a}=\pi(a)$ est neutre (resp. symétrisable de symétrique $\bar{a}'=\pi(a')$) dans E/R pour θ.

Théorème :

Soit (G,T) un groupe (resp. $(A,+,T)$ un anneau) et R une loi de composition interne compatible avec T (resp. avec T et +). Le quotient G/R (resp. A/R) muni de la loi quotient de T par R (resp. des loi quotients de T et + par R) est un groupe (resp. un anneau) et la surjection canonique $\pi : G\to G/R$ (resp. $\pi : A\to A/R$) est un morphisme de groupes (resp. d'anneaux)

Dans le cas où R est égale à R_H pour un certain sous-groupe distingué (ou un idéal) H, le noyau de π est alors égal à H.

Notation :

Si H est un sous-groupe distingué (resp. un idéal) du groupe (G,T) (resp. de l'anneau $(A,+,T)$), le groupe (resp. l'anneau) quotient G/R_H (resp. A/R_H) est noté plutôt G/H (resp. A/H).

- Passage au quotient (propriété universelle du quotient)

Théorème :

(1) Pour les groupes :

Soit $f:(G,T)\to(G',T')$ un morphisme de groupes, H un sous-groupe distingué de G et $\pi:G\to G/H$ la surjection canonique. Il existe un morphisme de groupes $\varphi:(G/H,T)\to(G',T')$ tel que $f=\varphi\circ\pi$ si et seulement si $H\subset\ker f$.

(2) Pour les anneaux commutatifs :

Soit $f:(A,+,T)\to(A',+,T')$ un morphisme d'anneaux, H un idéal de A et $\pi:A\to A/H$ la surjection canonique. Il existe un morphisme d'anneaux $\varphi:(A/H,+,T)\to(A',+,T')$ tel que $f=\varphi\circ\pi$ si et seulement si $H\subset\ker f$.

IV Les entiers naturels et relatifs ; principe de récurrence

A) Entiers naturels et principe de récurrence

1) Les axiomes de Peano

Nous admettons l'existence d'un triplet $(\mathbb{N},0,\sigma)$ tel que :

(1) $0\in\mathbb{N}$

(2) $\sigma:\mathbb{N}\to\mathbb{N}$ est une injection d'image $\mathbb{N}^*=\mathbb{N}\setminus\{0\}$

(3) (Principe de récurrence) Une partie non vide de $\mathbb{N}$ contenant 0 et stable par σ est égale à $\mathbb{N}$.

Remarque :

Les axiomes (1) et (2) signifient que $\mathbb{N}$ est infini. (3) indique que tout ensemble infini contient une partie en bijection avec $\mathbb{N}$.

En fait, on peut construire $(\mathbb{N},0,\sigma)$ à l'aide des axiomes de Zermelo–Fraenkel de la théorie des ensembles.

Notation :

On pose $1=\sigma(0)\neq 0$, $2=\sigma(1)\notin\{0,1\}$…

2) Le semi–groupe commutatif ordonné $(\mathbb{N},+,\leq)$ des entiers naturels

Nous proposons les grandes lignes d'une construction axiomatique de $\mathbb{N}$.

- Addition dans $\mathbb{N}$:

Définition :

Un couple (E,T) tel que la loi T est associative, admet un élément neutre et tel que tout élément de E est régulier (ou simplifiable) est appelé (parfois) un *semi–groupe*.

Nous admettons l'existence d'une loi de composition interne notée + telle que $\mathbb{N}$ est un semi–groupe commutatif.

On a alors $\forall(x,y)\in\mathbb{N}^2,\sigma(x)+y=\sigma(x+y)$. En particulier, $\sigma(y)=y+1$. 0 est le seul élément symétrisable, son symétrique est $-0=0$.

Remarque :

Une telle loi est unique. On peut la construire grâce au principe de récurrence en posant $\forall n\in\mathbb{N},0+n=n$ et $\forall(p,n)\in\mathbb{N}^2,\sigma(p)+n=\sigma(n+n)$.

- Relation d'ordre dans $\mathbb{N}$:

Théorème :

La relation définie sur $\mathbb{N}$ par :

$\forall (x,y) \in \mathbb{N}^2, x \leq y \Leftrightarrow (\exists z \in \mathbb{N} : y = x + z)$

est une relation d'ordre total, compatible avec la loi + et telle que toute partie non vide a un plus petit élément et toute partie non vide majorée a un plus grand élément. En particulier, pour tout $x \in \mathbb{N}$,

$]x,+\infty[= \{x > n\}$ $]x,+\infty[= \{n \in \mathbb{N} | x < n\}$ est non vide de plus petit élément $x+1 = \sigma(x)$.

Ainsi, la relation $\leq$ est un bon ordre sur $\mathbb{N}$.

3) Utilisation pratique du principe de récurrence

Théorème :

Soit $A(p)$ une assertion dépendant de la variable $p \in \mathbb{N}$. L'assertion $\forall p \in \mathbb{N}, A(p)$ équivaut à $(A(0)$ et $(\forall p \in \mathbb{N}, (A(p) \Rightarrow A(p+1)))$. Une propriété $A(p)$ dépendant de $p \in \mathbb{N}$ telle que $\forall p \in \mathbb{N}, (A(p) \Rightarrow A(p+1))$ est dite *héréditaire*.

- En pratique :

Pour prouver une assertion par récurrence, il suffit de :

(1) Vérifier $A(0)$

(2) Prouver que $A(p)$ est héréditaire.

(3) Conclure en invoquant le principe de récurrence.

Le second point se rédige de la manière suivante ;

'supposons que $A(p)$ est vraie pour un entier p' suivi de la vérification de $A(p+1)$ où on utilise l'hypothèse $A(p)$.

- Récurrences fortes :

Pour prouver $A(p+1)$, on a parfois besoin d'informations sur p, $p-1 \ldots$ Dans ce cas, il suffit de remplacer $A(p)$ par l'assertion $B(p) : \forall k \leq p, A(k)$.

On obtient le théorème :

Soit $A(p)$ une assertion dépendant de la variable $p \in \mathbb{N}$. L'assertion $\forall p \in \mathbb{N}, A(p)$ équivaut à $A(0)$ et $\forall p \in \mathbb{N}, (\forall k \leq p, A(p)) \Rightarrow A(p+1)$

Ainsi, pour prouver que l'assertion $A(p)$ est vraie pour tout p, il suffit de :

(1) Vérifier $A(0)$

(2) Prouver que, pour tout $p \in \mathbb{N}$, si les assertions $A(k), k = 1..p$ sont vraies, alors $A(p+1)$ est vraie.

(3) Conclure en invoquant le principe de récurrence forte.

4) Suites et itérations

- Définition :

On appelle *suite* de l'ensemble E toute application $U : \mathbb{N} \to E$.

Notation : on notera, en général, U_n au lieu de $U(n)$ l'image de l'entier n par la suite U.

- Suites définies par récurrence :

Théorème :

Soient E un ensemble, $a \in E$ et $f : E \to E$ une application. Il existe une unique suite U telle que $U_0 = a$ et $\forall n \in \mathbb{N}, U_{n+1} = f(U_n)$.

- Itérations d'une loi de composition associative :

Théorème :

Soient T une loi de composition interne associative dans l'ensemble E et a un élément de E. Les relations $u_1 = v_1 = a$ et $\forall n \geq 1, u_{n+1} = aTu_n$ et $v_{n+1} = v_n Ta$ définissent deux suites $(u_n)_{n \in \mathbb{N}^*}$ et $(v_n)_{n \in \mathbb{N}^*}$.

Si de plus T est associative, les deux suites sont égales et leurs éléments commutent deux à deux.

Notations :

Lorsque la loi est notée +, l'élément $u_n = v_n$ est noté $n.a$ ou na. Dans les autres cas, on notera le plus souvent $u_n = a^n$. Si de plus T admet un élément neutre e (resp. 0 si $T = +$), on pose, pour tout $a \in E$, $a^0 = e$ (resp. $0.a = 0$)

5) Application 1 : multiplication dans $\mathbb{N}$.

Théorème :

Il existe une unique loi de composition interne $\times$ dans $\mathbb{N}$ telle que $\forall (n,a) \in \mathbb{N}^2, n \times a = n.a$.

$\times$ est associative, commutative, admet 1 pour unité. 1 est le seul élément symétrisable, son symétrique est $1^{-1} = 1$. La loi $\times$ est distributive par rapport à +.

6) Application 2 : identités remarquables dans un anneau

Théorème :

Soit $(A,+,T)$ un anneau, non nécessairement commutatif et $a,b \in A$ deux éléments qui commutent (c'est-à-dire tels que $aTb = bTa$). On a, pour tout $n \in \mathbb{N}$:

$$a^n - b^n = (a-b)T(\sum_{k=0}^{n} a^k T b^{n-1-k}) = (a^{n-1} + a^{n-2}Tb + ... + a^{n-1})(a-b)$$

Et $(a+b)^n = \sum_{k=0}^{n} C_n^k a^k T b^{n-k}$

Remarque :

Dans le corps des complexes, on a la relation bien meilleure :

$$a^n - b^n = \prod_{k=0}^{n-1} (a - e^{\frac{2ik\pi}{n}} b)$$

B) L'anneau ordonné des entiers relatifs $(\mathbb{Z},+,\times,\leq)$.

1) Le groupe abélien $(\mathbb{Z},+)$.

Théorème :

Il existe un groupe abélien $(\mathbb{Z},+)$ et une injection $i:\mathbb{N}\to\mathbb{Z}$ tels que :

$\forall(n,m)\in\mathbb{N}^2, i(n+m)=i(n)+i(m)$

L'injection i permet d'identifier $n\in\mathbb{N}$ et $i(n)\in\mathbb{Z}$. $\mathbb{Z}$ est la réunion disjointe des parties :

$\mathbb{N}^*=i(\mathbb{N}^*)$, $\{0\}$ et $-\mathbb{N}^*=-i(\mathbb{N}^*)=\{x\in\mathbb{Z}\,|\,\exists n\in\mathbb{N}^*: x=-i(n)\}$

Définition :

On appelle valeur absolue de $x\in\mathbb{Z}$ l'élément $|x|\in\mathbb{N}\subset\mathbb{Z}$ défini par $|x|=\begin{cases}x \text{ si } x\in\mathbb{N}\\ -x \text{ sinon}\end{cases}$ et signe de $x\in\mathbb{Z}\setminus\{0\}$ l'élément $s(x)\in\{-1,1\}$ défini par $s(x)=\begin{cases}1 \text{ si } x\in\mathbb{N}\\ -1 \text{ sinon}\end{cases}$

Propriété :

Pour tout $x\in\mathbb{Z}$, $x=s(x)|x|$

2) Multiplication dans $\mathbb{Z}$.

On prolonge la multiplication de $\mathbb{N}$ à $\mathbb{Z}$ en posant, pour $(x,y)\in\mathbb{Z}^2$, $x\times y=s(x)s(y)|x||y|$ où $(-1)a$ désigne l'opposé de $a\in\mathbb{Z}$.

Théorème :

Le triplet $(\mathbb{Z},+,\times)$ est un anneau commutatif, intègre, d'élément neutre (pour $\times$) 1. Les seuls éléments inversibles pour $\times$ sont 1 et -1.

3) Ordre dans $\mathbb{Z}$.

Théorème :

La relation binaire définie dans $\mathbb{Z}$ par $x\leq y\Leftrightarrow y-x\in\mathbb{N}$ est une relation d'ordre total qui prolonge l'ordre naturel de $\mathbb{N}$ et qui est compatible avec les opérations de $\mathbb{Z}$, c'est-à-dire qui vérifie :

$\forall(a,b)\in\mathbb{Z}^2,(a\geq 0,b\geq 0)\Rightarrow(a+b\geq 0,a\times b\geq 0)$

4) Puissances d'un élément d'un groupe

Définition :

On étend aux exposants négatifs les puissances (ou itérés) d'un élément g d'un groupe (G,T), ou d'un élément inversible d'un anneau, par :

$g^0=e_G$ neutre de (G,T)

Et $\forall n \in \mathbb{N}, g^{n+1} = g^n T g$, $\forall n \in \mathbb{Z} \setminus \mathbb{N}, g^n = (g^{-n})^{-1}$

Où on rappelle que x^{-1} désigne le symétrique (ou inverse) de *x* pour *T*.

Dans le cas particulier où la loi *T* est notée + (elle est alors commutative), on utilisera la notation :

$0.g = 0_G$ neutre de $(G,+)$

Et $\forall n \in \mathbb{N}, (n+1).g = (n.g) + g$, $\forall n \in \mathbb{Z} \setminus \mathbb{N}, (n.g) = -((-n)g)$

Proposition :

Soit (G,T) (resp. $(G,+)$) un groupe et $g \in G$.

L'application $\sigma_g : n \in (\mathbb{Z},+) \mapsto g^n \in (G,T)$ (resp. $n \in (\mathbb{Z},+) \mapsto n.g \in (G,+)$) est un morphisme de groupes.

C) Arithmétique dans l'anneau $(\mathbb{Z},+,\times)$.

1) Eléments premiers, premiers entre eux

Définitions :

Un élément *a* non nul, non inversible de $\mathbb{Z}$ est dit *premier* si, dès que *a* divise un produit *bc*, il divise l'un des facteurs *b* ou *c*.

Soit $(a_i)_{i \in I}$ une famille d'éléments de $\mathbb{Z}$. Les $(a_i)_{i \in I}$ sont dits *premiers entre eux dans leur ensemble* si les seuls éléments de $\mathbb{Z}$ qui divisent tous les a_i sont les éléments inversibles.

2) Division euclidienne dans $\mathbb{Z}$.

Théorème :

Pour tout $(a,b) \in \mathbb{Z}^2$ avec $b \neq 0$, il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leq r < b$.

3) Sous-groupes et idéaux de $\mathbb{Z}$.

Pour $n \in \mathbb{N}$, on pose $n\mathbb{Z} = \{xn | n \in \mathbb{N}\}$. En particulier, $0\mathbb{Z} = \{0\}$ et $1\mathbb{Z} = \mathbb{Z}$.

Théorème :

Soit *H* une partie de $\mathbb{Z}$. Les propriétés suivantes sont équivalentes :

(1) *H* est un sous-groupe de $(\mathbb{Z},+)$.

(2) *H* est un idéal de $(\mathbb{Z},+,\times)$

(3) *H* est un idéal principal de $(\mathbb{Z},+,\times)$, c'est-à-dire qu'il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

4) Théorème de Gauss et de Bézout

Théorème :

(Gauss) : Soit $(a,b,c)\in\mathbb{Z}^3$. Si a divise bc et si a est premier avec b alors a divise c.

(Bézout pour une famille) : Les éléments de $\mathbb{Z}$ $(a_i)_{i=1..n}$ sont premiers entre eux dans leur ensemble si et seulement si il existe des $(u_i)_{i=1..n}$ tels que $\sum_{i=1}^{n} u_i a_i = 1$

5) Factorisation dans $\mathbb{Z}$.

Théorème :

Tout élément $n\in\mathbb{Z}\setminus\{0\}$ s'écrit, de manière unique à permutation près des p_i, sou la forme $n=\varepsilon p_1^{r_1}\ldots p_s^{r_s}$ où $\varepsilon=\pm 1$, les p_i sont premiers et positifs, et les r_i sont des entiers naturels non nuls.

6) PGCD et PPCM dans $\mathbb{Z}$.

- PGCD :

Théorème :

Soient $(a_i)_{i=1..n}$ des éléments de $\mathbb{Z}$. Il existe un unique entier naturel $D\in\mathbb{N}$ tel que pour tout $x\in\mathbb{Z}$, x divise tous les a_i si et seulement si il divise D.

Propriétés et définition :

D s'appelle le PGCD (plus grand commun diviseur) des a_i. Il est caractérisé par le fait qu'il divise tous les a_i et qu'il existe des entiers $(u_i)_{i=1..n}$ tels que $D=\sum_{i=1}^{n} u_i a_i$. En fait, D est le générateur positif de l'idéal $a_1\mathbb{Z}+\ldots+a_n\mathbb{Z}$.

- PPCM :

Théorème :

Soit $(a_i)_{i=1..n}$ des éléments de $\mathbb{Z}$. L'ensemble des entiers multiples de tous les a_i est l'intersection des idéaux $a_i\mathbb{Z}$, c'est aussi un idéal. Ainsi, il existe un unique entier $M\in\mathbb{N}$ tel que pour tout $x\in\mathbb{Z}$, tous les a_i divisent x si et seulement si M divise x.

Propriété et définition :

M s'appelle le PPCM (plus petit commun multiple) des a_i. Il est caractérisé par le fait qu'il est multiple de tous les a_i et qu'il est le plus petit entier naturel ayant cette propriété.

- Cas de deux entiers :

Le PGCD D et le PPCM M des deux entiers a et b vérifient :

$MD=|ab|$.