Chapitre I: Rappels et définitions

I-0- Historique :

L'arithmétique, vient du mot grec "arithmos" et qui signifie "nombre", est une branche de mathématiques qui correspond à la science des nombres. Elle a été étudié par de nombreuses anciennes civilisations comme les civilisations babylonienne, égyptienne, indienne et grecque. plus tard, les arabes ont excellé dans cette dernière surtout avec l'apparition d'autres sciences mathématiques notamment l'algèbre.

Au départ l'arithmétique s'est limitée à l'étude des entiers naturels. Les phythagoriciens (av. J-C) attribuent une valeur mystique à certains nombres et les classent selon leurs propriétés arithmétiques ou géométriques. Dans cet axe, ils introduisent les notions des nombres parfaits, amicaux, triangulaires, carrés, pentagonaux, hexagonaux, ... etc.

Définition 0-1 (Nombres parfaits):
Un entier naturel est parfait s'il est égal à la somme de ses diviseurs propres..

Exemple 0-1:

① $6 = 1+2+3$ parfait

② $28 = 1+2+4+7+14$ parfait

③ $8 \neq 1+2+4$ n'est pas parfait.

Définition 0_2 (Nombres amicaux)

Deux entiers sont amicaux si chacun est la somme des diviseurs propres de l'autre.

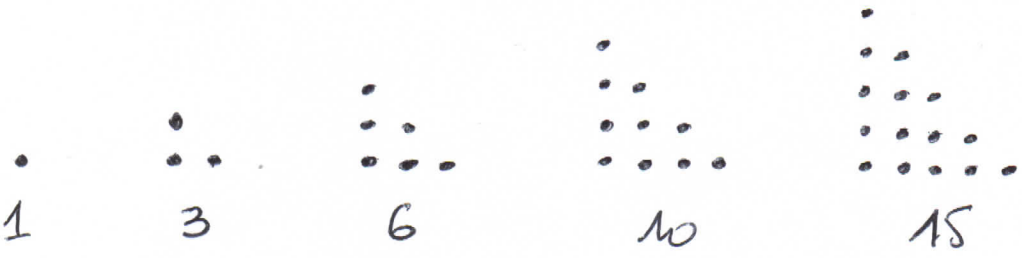
Exemple 0_2 :

Le premier couple des nombres distincts amicaux est (220, 284).

- Somme des diviseurs de 220 : $1+2+4+5+10+11+20+22+44+55+110 = 284$
- Somme des diviseurs de 284 : $1+2+4+71+142 = 220$.

Définition 0_3 (Nombres triangulaires) :

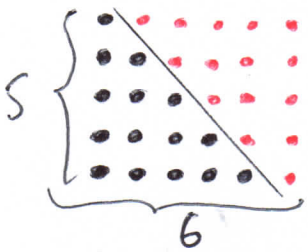
Un nombre triangulaire est un entier naturel non nul égal au nombre des pastilles dans un triangle construit à la manière des figures suivantes :



Le triangle trivial (le point).

Ces représentations permettent de déduire que le n_ième nombre triangulaire $T_n = 1 + 2 + \cdots + n$, $\forall n \geq 1$ vaut $\frac{n(n+1)}{2}$ comme suit :

par exemple pour $n = 5$, on a :

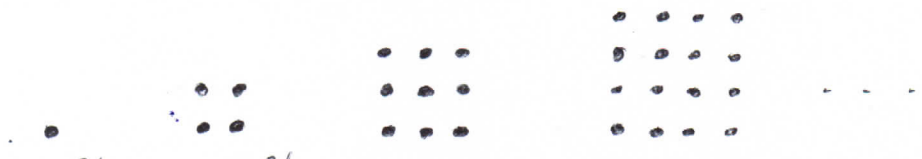


rectangle (6.5)

$$T_5 = 1+2+3+4+5 = \frac{5\times 6}{2} = 15.$$

$$\forall n \geq 1 : T_n = 1+2+\cdots+n = \frac{n(n+1)}{2}$$ (peut se démontrer par récurrence).

Définition 0-4 (Nombres carrés):
Un nombre carré est celui que l'on peut représenter par un carré.
La suite des nombres carrés est: 1, 4, 9, 16, 25, 36, ...



$1 = 1^2$ $4 = 2^2$ $9 = 3^2$ $16 = 4^2$

* La somme de deux nombres triangulaires successifs est un carré.

Exemple:

$15 + 10 = 25$

* La somme des n premiers nombres impaires est un carré.

Exemple:

$1+3+5+7+9 = 25 = 5^2$.

I.1. Groupes

Etant donné un ensemble E, une loi de composition interne, ou opération "$*$" sur E est une application de $E \times E$ dans E, que l'on note

$$(x,y) \longmapsto x * y$$

Définition: Une opération $*$ sur E est dite

1. associative si $\forall (x,y,z) \in E \times E \times E$, $(x*y)*z = x*(y*z)$
2. posséder un élément neutre s'il existe un élément $e \in E$ vérifiant $\forall x \in E$, $e*x = x*e = x$.
3. Commutative, si $\forall (x,y) \in E \times E$, $x*y = y*x$.

Définition: On dit qu'un élément $x \in E$ possède un symétrique (ou inverse ou opposé) s'il existe $y \in E$ vérifiant

$$x*y = y*x = e.$$

Définition (groupe)
Un groupe est la donnée d'un ensemble G muni d'une opération possédant les propriétés suivantes:

1. Elle est associative
2. Elle possède un élément neutre.
3. Tout élément de G admet un inverse.

Si de plus l'opération est commutative, on dit que le groupe est commutatif ou abélien.

Un groupe G est fini si l'ensemble G est fini, et le nombre

d'éléments de G est appelé "ordre de G".

Exemples: $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes commutatifs

$(\mathbb{N},+)$ et $(\mathbb{Z},+)$ n'est pas un groupe.

Remarque Un groupe dont l'opération est représentée par la multiplication (addition) sera appelé groupe multiplicatif (additif) et son élément neutre sera désigné par 1 (par 0).

Définition (morphisme de groupe)

Soit $(G_1,*)$, $(G_2,*)$ deux groupes, une application f de G_1 dans G_2 est un morphisme de groupes si :

$$\forall (x,y) \in G_1 \times G_2,\ f(x*y) = f(x)\cdot f(y).$$

Si de plus, l'application f est une bijection, on dit que f est isomorphisme de groupes.

Définition : (sous-groupe)

Soit G un groupe multiplicatif. Une partie H de G est un sous-groupe de G si les conditions suivantes sont réalisées,

1. $\forall (x,y) \in H \times H,\ xy \in H$.
2. $1 \in H$
3. $\forall x \in H,\ x^{-1} \in H$.

Définition: Si G est un groupe multiplicatif, on définit les puissances de x par

$$\forall k \in \mathbb{Z}, \quad x^k = \begin{cases} 1 & k = 0 \\ \underbrace{x.x \dots x}_{k \text{ fois}} & k > 0 \\ \underbrace{x^{-1}.x^{-1} \dots x^{-1}}_{-k \text{ fois}} & k < 0 \end{cases}$$

On pose alors $\langle x \rangle = \{ x^k, k \in \mathbb{Z} \} \subseteq G$.

- Si G est additif, on définit les multiples de x par

$$\forall k \in \mathbb{Z}, \quad kx = \begin{cases} 0 & k = 0 \\ \underbrace{x+x+\dots+x}_{k \text{ fois}} & k > 0 \\ \underbrace{(-x)+(-x)+\dots+(-x)}_{-k \text{ fois}} & k < 0 \end{cases}$$

on pose $\langle x \rangle = \{ kx \mid k \in \mathbb{Z} \} \subseteq G$.

l'ensemble $\langle x \rangle$ est un sous-groupe de G et de plus il est le plus petit sous-groupe de G contenant x, on l'appele le sous-groupe engendré par x.

Définition: - S'il existe $x \in G$, tel que $G = \langle x \rangle$, alors G est dit monogène
- Un groupe monogène fini est appelé groupe cyclique.

Exemple: $G = \mathbb{Z}$ et $n \in \mathbb{Z}$, alors $\langle n \rangle = \{ kn. \mid k \in \mathbb{Z} \}$
le groupe $\langle n \rangle$ de $\mathbb{Z}$ est désigné par $n\mathbb{Z}$.

Définition: (Ordre d'un élément)
Si G est un groupe fini et $x \in G$, on appelle ordre de x l'ordre du sous-groupe $\langle x \rangle$ de G engendré par x.

Théorème (*) Soit G un groupe fini, et soit $x \in G$, m l'ordre de x. Alors

1. m divise l'ordre de G.

2. m est le plus petit entier positif tel que $x^m = 1$.

3. Les éléments $1, x, x^2, \dots, x^{m-1}$ sont tous distincts dans G.

Théorème (Lagrange)
Dans un groupe fini, l'ordre d'un sous-groupe divise l'ordre du groupe.

I.2. Groupes quotients

Rappelons qu'une relation binaire $\mathcal{R}$ définie sur un ensemble E est une relation d'équivalence si elle possède les propriétés suivantes :

- Réflexivité, $\forall x \in E$, $x \mathcal{R} x$
- Symétrie, $\forall (x,y) \in E \times E$, $x \mathcal{R} y \Leftrightarrow y \mathcal{R} x$.
- Transitivité, $\forall (x,y,z) \in E \times E \times E$, $\left.\begin{array}{l} x \mathcal{R} y \\ y \mathcal{R} z \end{array}\right\} \Rightarrow x \mathcal{R} z$

Soit G un groupe noté additivement, et soit H un sous groupe de G.

1. La relation binaire définie sur G par

$$x \mathcal{R} y \text{ ssi } y - x \in H$$

est une relation d'équivalence sur G

Si $x \mathcal{R} y$ on dit que x et y sont équivalents modulo H.

2. Pour chaque $x \in G$, si $\bar{x}$ désigne la classe d'équivalence de x, alors

$$\bar{x} = \{x + h \;/\; h \in H\}.$$

On désigne par G/H l'ensemble quotient de G par la relation d'équivalence associée à H et les éléments de G/H sont les classes d'équivalences modulo H.

Remarque En notation multiplicative, la relation ci-dessus s'écrit $x \mathcal{R} y \iff y x^{-1} \in H$.

On suppose maintenant que G est abelien, soient $\alpha, \beta \in G/H$ c'est à dire deux classes d'équivalence modulo H.

On choisit un représentant $x \in G$ de α et $y \in G$ de β, c'est à dire on a $\bar{x} = \alpha$, $\bar{y} = \beta$. La somme de α et β est définie par $\alpha + \beta = \overline{x+y}$

On a $+$ est une loi interne dans G/H et G/H muni de cette loi est un groupe abélien, appelé groupe quotient du groupe G par le sous groupe H.

Exemple : (Le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$)

Soit $n \in \mathbb{N}$, $G = \mathbb{Z}$ et $H = n\mathbb{Z}$. La relation définie sur $\mathbb{Z}$ par : $x \mathcal{R} y \iff x - y \in n\mathbb{Z}$ est une relation d'équivalence, donc x et y sont équivalents modulo $n\mathbb{Z}$ si et seulement si n divise $x-y$, et on a pour chaque $x \in \mathbb{Z}$:

$$\bar{x} = \{x + nk \,,\, k \in \mathbb{Z}\}$$

De plus, on a pour tout $x, y \in \mathbb{Z}$: $\bar{x} + \bar{y} = \overline{x+y}$ est une loi interne dans $\mathbb{Z}/n\mathbb{Z}$, et $(\mathbb{Z}/n\mathbb{Z}, +)$ a la structure du groupe appelé groupe additif des entiers relatifs modulo n.

I.3. Anneaux et corps :

Définition : Un anneau est la donnée d'un ensemble A muni de deux opérations, une addition et une multiplication, vérifiant :

1. $(A, +)$ est un groupe commutatif, d'élément neutre noté 0.
2. La multiplication est associative et possède un éléinent neutre noté 1, appelé élément unité.
3. La multiplication est distributive par rapport à l'addition, c'est à dire

$$\forall (x,y,z) \in A\times A\times A, \quad \begin{cases} x(y+z) = xy + xz \\ (y+z)x = yx + zx. \end{cases}$$

- Si la multiplication est commutative, on dit que l'anneau A est commutatif.
- L'anneau A est dit integre si $\forall (x,y) \in A\times A$

$$\begin{matrix} x \neq 0 \\ y \neq 0 \end{matrix} \Rightarrow xy \neq 0$$

A^* désigne l'ensemble des éléments inversibles (pour la multiplication), et on a A^* est un groupe multiplicatif.

Exemple : (L'anneau $\mathbb{Z}$)

$(\mathbb{Z}, +, \cdot)$ est un anneau commutatif integre dont la multiplication est définit à partir de l'addition.

Les seuls éléments inversibles de $\mathbb{Z}$ sont 1 et -1, ce qui fait

$\mathbb{Z}^*$ est le groupe multiplicatif $\{1, -1\}$ à deux éléments.

Définition (L'anneau quotient $\mathbb{Z}/n\mathbb{Z}$)

Etant données deux classes $\alpha = \bar{a}$, $\beta = \bar{b} \in \mathbb{Z}/n\mathbb{Z}$.

La classe produit $\alpha \cdot \beta \in \mathbb{Z}/n\mathbb{Z}$ est définit comme suit :

$$\alpha \cdot \beta = \overline{a \cdot b}$$

La multiplication ci-dessus fait du groupe quotient $\mathbb{Z}/n\mathbb{Z}$ un anneau commutatif d'élément neutre $\bar{0}$ et d'unité $\bar{1}$.

L'anneau $\mathbb{Z}/n\mathbb{Z}$ est appelé anneau quotient de l'anneau $\mathbb{Z}$ par $n\mathbb{Z}$.

Définition Soit A et B deux anneaux. Une application f de A dans B est un morphisme d'anneaux si pour tout $(x, y) \in A \times A$,

$$f(x+y) = f(x) + f(y) \quad \text{et} \quad f(x \cdot y) = f(x) \cdot f(y).$$

Si de plus, f est bijective on dit que f est un isomorphisme d'anneaux et A et B sont isomorphes.

Proposition : (Formule du binôme de Newton)

Soit A un anneau commutatif. Soit $a, b \in A$ et soit $n \geq 1$ un entier, on a

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

Preuve : Utiliser la démonstration par récurrence.

Rappelons aussi qu'un corps $\mathbb{K}$ est un anneau dans lequel tout élément non nul admet un inverse pour la multiplication ce qui est équivalent à l'égalité $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ et on a tout corps est un anneau intègre.

Remarque : L'anneau $\mathbb{Z}$ n'est pas un corps car ses seuls éléments inversibles sont 1 et -1.