

# Cours de Mathématiques

Mathilde Andre

Vendredi 18 Juillet 2014

# Sommaire

<b>1</b>	<b>Rappels du lycée</b>	<b>2</b>
1.1	Multiple et division euclidienne . . . . .	2
1.2	Nombres premiers . . . . .	4
1.3	Congruence . . . . .	6
<b>2</b>	<b>Algèbre</b>	<b>7</b>
2.1	Quelques rappels sur $\mathbb{N}$ . . . . .	7
2.2	Construction de $\mathbb{Z}$ . . . . .	8
2.3	Les groupes . . . . .	9
2.3.1	Les sous groupes . . . . .	10
2.3.2	Morphisme de groupe . . . . .	10
2.3.3	Noyau . . . . .	10
2.3.4	Groupe quotient . . . . .	11

# Chapitre 1

## Rappels du lycée

### 1.1 Multiple et division euclidienne

#### Définition 1.1.

Soient  $a$  et  $b \in \mathbb{Z}$

$a$  est un multiple de  $b$  ssi  $\exists k \in \mathbb{Z}$  tel que :

$$a = kb$$

On dit aussi que :

- $a$  est divisible par  $b$
- $b$  est un diviseur  $a$
- $b$  divise  $a$

#### Définition 1.2.

Soient  $a \in \mathbb{Z}$  et  $b \in \mathbb{N}$ .

On appelle **division euclidienne de  $a$  par  $b$**  l'opération qui au couple  $(a,b)$  associe un couple  $(q,r)$  tel que :

$$a = b \times q + r \text{ avec } 0 \leq r < b$$

On appelle  $a$  le dividende,  $b$  le diviseur,  $q$  le quotient et  $r$  le reste.

**Définition 1.3.**

Soient  $a, b \in \mathbb{N}$

**pgcd :**

On appelle  $\text{pgcd}(a, b)$  le plus grand commun diviseur de  $a$  et de  $b$ .

**ppcm :**

On appelle  $\text{ppcm}(a, b)$  le plus petit commun multiple de  $a$  et de  $b$ .

**Proposition 1.1.**

Soient  $a, b \in \mathbb{N}$

$$\text{ppcm}(a, b) \times \text{pgcd}(a, b) = a \times b$$

*Démonstration :*

Soient  $m = \text{ppcm}(a, b)$  et  $\delta = \text{pgcd}(a, b)$

On a :  $a|\delta$  et  $b|\delta$  cad  $\exists k, k' \in \mathbb{Z}$  tel que  $a = k \times \delta$  et  $b = k' \times \delta$

On devrait alors avoir  $m \times \delta = k \times \delta \times k' \times \delta \Leftrightarrow m = k \times k' \times \delta$

Montrons donc que  $kk'\delta = \text{ppcm}(a, b)$

→  $kk'\delta$  est un multiple de  $a$  et  $b$  cad  $a|m$  et  $b|m$  ??

On a  $a = k \times \delta$  cad  $k' \times a = k' \times k \times \delta$  cad  $a|k'k\delta$

Idem pour  $b$

→  $kk'\delta$  est le **plus petit** multiple de  $a, b$  ??

□

**Proposition 1.2.**

Soient  $a, b \in \mathbb{N}$

$$\text{pgcd}(a, b) = \delta \Leftrightarrow a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$$

*Démonstration :*

Aide :  $a\mathbb{Z} + b\mathbb{Z} = \{ak + bk' | k, k' \in \mathbb{Z}\}$

- $\Rightarrow$  Si  $\text{pgcd}(a, b) = \delta$ , montrons que  $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$   
 Soit  $m \in a\mathbb{Z} + b\mathbb{Z}$  donc  $\exists a', b' \in \mathbb{Z}$  tel que  $m = a \times a' + b \times b'$   
 Or  $\delta|a$  et  $\delta|b$  donc  $\exists k, k' \in \mathbb{Z}$  tel que  $a = k \times \delta$  et  $b = k' \times \delta$   
 Donc  $m = k \times \delta \times a' + k' \times \delta \times b' \Leftrightarrow m = \delta \times (ka' + k'b')$  cad  $m \in \delta\mathbb{Z}$
- $\Leftarrow$  Si  $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$ , montrons que  $\text{pgcd}(a, b) = \delta$ 
  1. Montrons que  $\delta$  est un diviseur commun á a et b.  
 $a = a \times 1 + b \times 0 \in a\mathbb{Z} + b\mathbb{Z}$  donc  $a \in \delta\mathbb{Z}$  cad  $\delta|a$   
 Idem pour b.
  2. Montrons que  $\delta$  est bien le **plus grand** diviseur de a et b.  
 Soit  $\Delta$  un diviseur commun á a et b donc  $\exists a', b' \in \mathbb{Z}$ ,  $a = a'\Delta$  et  $b = b'\Delta$   
 Nous allons montrer que  $\Delta|\delta$  cad  $\Delta \leq \delta$   
 $\delta \in \delta\mathbb{Z}$  donc  $\delta \in a\mathbb{Z} + b\mathbb{Z}$  donc  $\exists k, k' \in \mathbb{Z}$  tel que
 
$$\begin{aligned}\delta &= ak + bk' \\ \Leftrightarrow \delta &= a'\Delta k + b'\Delta k' \\ \Leftrightarrow \delta &= \Delta \times (ka' + k'b')\end{aligned}$$

Donc  $\Delta|\delta$  cad  $\Delta \leq \delta$  cad  $\delta = \text{pgcd}(a, b)$

□

## 1.2 Nombres premiers

### Définition 1.4.

Soit  $n \in \mathbb{N}$ .

On dit que n est un nombre premier s'il admet exactement deux diviseurs : 1 et lui-même.

**Proposition 1.3.**

Soit  $n \in \mathbb{N}, n > 1$

1.  $n$  admet au moins un diviseur premier
2. si  $n$  n'est pas premier,  $n$  admet au moins un diviseur premier  $p$  tel que  $p \leq \sqrt{n}$

*Démonstration :*

- ❶ → Si  $n$  est premier, la propriété est vérifiée :  $n|n$   
 → Si  $n$  n'est pas premier, il admet dans  $\mathbb{N}$  d'autres diviseurs que 1 et  $n$ .  
 Soit  $p$  le plus petit diviseur de  $n$ .  
 $p$  est-il premier ?  
 Raisonnement par l'absurde :  
 Si  $p$  n'est pas premier, alors appelons  $p'$  son plus petit diviseur.  
 On a :  $p'|p \Rightarrow p'|n$  mais  $p' < p \Rightarrow$  **Contradiction !**
- ❷ On a montré que si  $n$  n'est pas premier il admet au moins un diviseur premier. Soit  $p$  ce diviseur.  
 Alors  $p|n$  donc  $\exists k \in \mathbb{Z}$  tel que  $n = k \times p$ . Donc  $k$  est aussi un diviseur de  $n$  et  $k \geq p$  d'où  $n = pk \geq p^2$  donc  $\sqrt{n} \geq p$ .

□

**Theoreme 1.1.**

Il existe une infinité de nombres premiers.

*Démonstration :*

Raisonnement par l'absurde :

Supposons que  $\mathcal{P}$  est finit. Donc on peut écrire  $\mathcal{P} = \{p_1, p_2, p_3, \dots, p_n\}$

Considérons  $k \in \mathbb{N}$  tel que  $k = p_1 \times p_2 \times \dots \times p_n + 1$

$k \geq 2$ , donc d'après la proposition précédente,  $k$  possède un diviseur premier notons le  $q$ .

Le nombre  $q$  est l'un des  $p_i$ .

Donc  $q|p_1 \times p_2 \times \dots \times p_n$  et  $q|k$ .

Donc  $q|k - p_1 \times p_2 \times \dots \times p_n$ .

Donc  $q|1$  cad  $q=1$  mais 1 n'est pas premier  $\Rightarrow$  Contradiction!!

□

## 1.3 Congruence

### Définition 1.5.

Soient  $n \in \mathbb{N}, n \geq 2$  et  $a, b \in \mathbb{Z}$  On dit que deux entiers  $a$  et  $b$  sont congru modulo  $n$  ssi ils ont même reste par la division euclidienne par  $n$ .

On note alors :

$$a \equiv b \pmod{n} \text{ ou } a \equiv b \pmod{n}$$

### Theoreme 1.2.

Soient  $n \in \mathbb{N}, n \geq 2$  et  $a, b \in \mathbb{Z}$

$$a \equiv b \pmod{n} \Leftrightarrow (a - b) \equiv 0 \pmod{n}$$

*Démonstration.*  $\Rightarrow$

□

# Chapitre 2

## Algèbre

Cours 1

### 2.1 Quelques rappels sur $\mathbb{N}$

#### Proposition 2.1.

Tout ensemble  $A$  non vide  $\subset \mathbb{N}$  a un plus petit élément

#### Définition 2.1.

**Majorant** : On dit que  $M$  est un majorant de  $A \subset \mathbb{N}$  ssi  $\forall n \in A, n \leq M$

On dit aussi que  $A$  est majoré



**Définition 2.2.**

**Relation d'équivalence** : Soit  $\mathcal{R}$  une relation binaire sur  $A \subset \mathbb{N}$ .  
 $\mathcal{R}$  est une relation d'équivalence ssi elle est :

1. reflexive :  $\forall x \in A, x\mathcal{R}x$
2. symetrique :  $\forall (a,b) \in A^2, \text{ si } a\mathcal{R}b \Rightarrow b\mathcal{R}a$
3. transitive :  $\forall (a,b,c) \in A^3, \text{ si } a\mathcal{R}b \text{ et } b\mathcal{R}c \Rightarrow a\mathcal{R}c$

**Classe d'équivalence** : La classe d'équivalence de  $x$  pour  $\mathcal{R}$  est tous les  $y$  tel que  $x\mathcal{R}y$ , on la note  $\bar{x}$

## 2.2 Construction de $\mathbb{Z}$

### Comment construire $\mathbb{Z}$ ?

Soit  $\mathcal{R}$  une relation d'équivalence sur  $\mathbb{N} \times \mathbb{N}$  définit ainsi :  
 $\forall (a,b) \in A^2 \text{ et } (a',b') \in A^2, (a,b)\mathcal{R}(a',b') \text{ ssi } a + b' = a' + b$

### Quelles sont les classes d'équivalences de $(0, 0)$ et $(0, a)$ ?

1.  $\overline{(0,0)} = \{(x,y) \in \mathbb{N} \times \mathbb{N}, (x,y)\mathcal{R}(0,0)\} = \{(x,y) \in \mathbb{N} \times \mathbb{N}, x = y\} = \{(x,x), x \in \mathbb{N}\}$
2.  $\overline{(0,a)} = \{(x,y) \in \mathbb{N} \times \mathbb{N}, x + a = y\} = \{(x, x + a), x \in \mathbb{N}\}$

On a :  $\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)}$

On a donc :  $\overline{(0,a)} + \overline{(a,0)} = \overline{(a,a)} = \overline{(0,0)}$

Et on note :  $\overline{(a,0)} = -a$

### La démonstration par récurrence :

On va montrer que  $P(n)$  vraie pour tout  $n \in \mathbb{N} \Leftrightarrow$

1.  $P(0)$  vrai
2. Supposons  $P(n)$  vrai alors  $P(n+1)$  vrai

Supposons  $\mathcal{P}(0)$  vrai et

Si  $\mathcal{P}(n)$  vrai  $\Rightarrow \mathcal{P}(n+1)$  vrai

On va faire une démonstration par l'absurde :

Il existe un  $m \in \mathbb{N}, \mathcal{P}(m)$  faux

Soit  $A = \{n \in \mathbb{N}, \mathcal{P}(n) \text{ faux}\}$

$A \subset \mathbb{N} \Rightarrow A$  admet un plus petit element, appelons le  $i$ .

Donc  $i \neq 0$  et  $\mathcal{P}(i-1)$  est vrai.

D'après notre supposition on a alors  $\mathcal{P}(i)$  vrai : CONTRADICTION

## 2.3 Les groupes

### Définition 2.3.

On dit que  $(G, *)$  est un groupe avec  $G$  un ensemble et  $*$  une loi sur  $G$  ssi :

1.  $*$  est associative cad  $\forall x, y, z \in G \ (x * y) * z = x * (y * z)$
2.  $G$  admet un élément neutre :  $\exists e \in G, \forall x \in G, x * e = e * x = x$
3. Tout élément de  $G$  admet un symétrique :  
 $\forall x \in G, \exists x^{-1}, x * x^{-1} = x^{-1} * x = e$

On dit qu'un groupe est abélien ou commutatif si  $*$  est commutative.

### Exemple 2.1.

Exemple de groupe non abélien : Les permutations

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Calculer  $a \circ b$  puis  $b \circ a$

$$b \circ c = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$c \circ b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Donc l'ensemble des permutations muni de la loi de composition n'est pas un groupe abélien.

### 2.3.1 Les sous groupes

#### Définition 2.4.

On dit que  $(H, *) \subset G$  un ensemble et  $*$  est un sous-groupe de  $G$  ssi :

1.  $H \neq \emptyset$
2.  $H$  admet le même élément neutre que  $G$
3.  $H$  est stable :  $\forall x, y \in G, x * y \in H$

#### Exemple 2.2.

**Quels sont les sous-groupes de  $\mathbb{Z}$  ?**

Les sous groupes de  $\mathbb{Z}$  sont les  $k\mathbb{Z}$

$$k\mathbb{Z} = \{\forall x \in \mathbb{Z}, kx\}$$

**Demo :** Soit  $H$  un sous groupe de  $\mathbb{Z}$  ne contenant pas 0

$H \cap \mathbb{N}^* \in \mathbb{N}$  est non vide donc il admet un plus élément, notons le  $k$

Soit  $h \in H \cap \mathbb{N}^*$  alors division euclidienne de  $h$  par  $k$  :  $\exists(q, r) \in \mathbb{Z} \times \mathbb{H}$  tel que  $h = k^*q + r$  ac  $0 \leq r < k$  mais  $k$  est le plus petit élément de  $H$  donc  $r=0$ .

### 2.3.2 Morphisme de groupe

#### Définition 2.5.

Soient  $(G_1, *_1)$  et  $(G_2, *_2)$  deux groupes, et  $\phi : G_1 \longrightarrow G_2$ ,

$\phi$  est un morphisme de groupe ssi :  $\phi(x_1 *_1 x_2) = \phi(x_1) *_2 \phi(x_2)$  avec  $x_1, x_2 \in G_1$

### 2.3.3 Noyau

#### Définition 2.6.

Soient  $(G_1, *_1)$  et  $(G_2, *_2)$  deux groupes, et  $\phi : G_1 \longrightarrow G_2$ ,

On note  $Ker(\phi) = \{y \in G_1, \phi(y) = e_2\}$

**Proposition 2.2.**

$$\text{Ker}(\phi) = \{\emptyset\} \Leftrightarrow \phi \text{ est injective}$$

*Démonstration :*

- Si  $\phi$  injective alors si  $x, y \in G_1$  et  $\phi(x) = \phi(y) \Rightarrow x = y$

$$\begin{aligned} & \phi(x) = \phi(y) \\ \Leftrightarrow & \phi(x) * \phi(y)^{-1} = e_2 \\ \Leftrightarrow & \phi(x) * \phi(y^{-1}) = e_2 \\ \Leftrightarrow & \phi(x * y^{-1}) = e_2 \end{aligned}$$

Or  $x = y$   
 $x * y^{-1} = e_1$   
 Donc  $\phi(e_1) = e_2$  et  $\text{Ker}(\phi) = \{\emptyset\}$

- Si  $\text{Ker}(\phi) = \{\emptyset\}$  :  
 Soient  $x, y \in G_1$  tel que  $\phi(x) = \phi(y)$ .

$$\begin{aligned} \text{Alors } & \phi(x) * \phi(y)^{-1} = e_2 \\ \Leftrightarrow & \phi(x) * \phi(y^{-1}) = e_2 \\ \Leftrightarrow & \phi(x * y^{-1}) = e_2 \\ \Leftrightarrow & x * y^{-1} = e_2 \\ \Leftrightarrow & x = y \end{aligned}$$

Donc  $\phi$  est injective.

□

### 2.3.4 Groupe quotient

kzkzk