CHAPITRE 2

Nombres entiers, initiation à l’arithmétique- Nombres rationnels

Nombres entiers, initiation à l'arithmétique, nombres rationnels.

- L’ensemble **N** des **entiers positifs**
- L’anneau **Z** des **entiers relatifs**
- Nombres **rationnels**

L’ensemble N des entiers positifs

Les axiomes de N (G. Peano)

- 1. N contient au moins un élément (noté « 0 »)
- 2. Tout élément n de N admet un *successeur* S(n)
- 3. Deux éléments ayant mêmes successeurs sont égaux
- 4. « 0 » n'est successeur d'aucun élément
- 5. Le seul sous-ensemble de N contenant à la fois 0 et les successeurs de tous ses éléments est N tout entier *(principe de récurrence)*

G. PEANO
(1858-1932)

Deux opérations sur N

- somme = a
- répéter b fois
- somme = S (somme)

a + b

- produit = 0
- répéter a fois
- produit = produit + b

a x b

Un ordre total sur N

a « est plus petit que b »

Il existe un élément x de N tel que $b = a + x$

Cet ordre est compatible avec addition et multiplication

$$a \leq b$$

Trois propriétés « clef » de N (équivalentes aux axiomes de Peano)

- 1. Toute partie A non vide possède un plus petit élément (borne inférieure)
- 2. Toute partie A non vide et majorée admet un plus grand élément (borne supérieure)
- 3. L'ensemble N tout entier n'a pas de majorant

(1) → Cet ordre est total
(on peut toujours comparer deux éléments)

Les deux principes de récurrence

Données : une assertion R {n} où figure le caractère « n » et un nombre entier n_0 fixé

PRINCIPE 1 L'assertion :

$$\left(R\{n_0\} \text{ et } [\forall n \geq n_0,\ R\{n\} \Rightarrow R\{n+1\}] \right)$$

$$\Downarrow$$

$$\left(\text{pour tout n plus grand que } n_0,\ R\{n\}\right)$$

est une évidence dans l'axiomatique de Peano

PRINCIPE 2 L'assertion :

$$R\{n_0\} \text{ et } [\forall n \geqq n_0, R\{k\},\ k=n_0,\ldots,n] \Rightarrow R\{n+1\}]]$$

$$\Downarrow$$

$$\left(\text{pour tout n plus grand que } n_0,\ R\{n\}\right)$$

est une évidence dans l'axiomatique de Peano

Les nombres premiers : illustration de deux modèles de raisonnement

- Tout nombre entier supérieur ou égal à 2 admet un diviseur premier (preuve par récurrence)

- Il y a une infinité de nombres premiers (preuve par l'absurde)

Le théorème d'Euclide

Soient a et b deux entiers positifs avec b non nul.
Il existe un UNIQUE couple d'entiers (q,r) tels que :

$$a = b\,q + r$$

et

r est entre 0 (inclus) et b-1 (inclus)

Définition : le nombre r est dit RESTE dans la division EUCLIDIENNE de a par b.

Le nombre q est dit QUOTIENT dans la division EUCLIDIENNE de a par b.

Quelques applications du théorème d'Euclide

- La recherche du PGCD
- Le développement en base b

Deux « programmes » basés sur l'algorithme d'Euclide

fonction PGCD = PGCD (a,b)


MATLAB 7.1.lnk

fonction X= newbase (a,b)


MATLAB 7.1.lnk

fonction PGCD=PGCD (a,b)

L'algorithme d'Euclide

Al-Khwarizmi
(780 – Bagdad 850)

```
x=a ;
y=b ;
tant  que y>0
    [q,r] = div(x,y);
    si r==0
        PGCD = y;
        y = 0 ;
    sinon
        [q1,r1] = div(y,r);
        x = r;
        PGCD = x ;
        y=r1 ;
    fin
fin
```

$a = b\,q_0 + r_0$ $\quad PGCD(a,b) = PGCD(b,r_0)$

$b = r_0\,q_1 + r_1$ $\quad PGCD(b,r_0) = PGCD(r_0,r_1)$

$r_0 = r_1\,q_2 + r_2$ $\quad PGCD(r_0,r_1) = PGCD(r_1,r_2)$

....

$r_{N-2} = q_N\,r_{N-1} + r_N$ $\quad PGCD(r_{N-2},r_{N-1}) = PGCD(r_{N-1},r_N)$

$r_{N-1} = q_{N+1}\,r_N + 0$ $\quad PGCD(r_{N-1},r_N) = r_N$

fonction X=newbase (a,b)
Comment écrire a «en base b » ?

- X=[ ] ;
- x=a ;
- tant que x > 0
- [q,r]= div (x,b);
- x=q;
- X=[r , X] ;
- fin

$$a = b\,q + d_0$$
$$= b\,(b\,q_1 + d_1) + d_0$$
$$= b\,(b\,(b\,q_2 + d_2) + d_1) + d_0$$
$$= d_0 + d_1\,b + \ldots + d_{N-1}\,b^{N-1}$$

$$a : [\, d_{N-1}\ d_{N-2}\ \ldots\ d_2\ d_1\ d_0\,]$$

L'anneau Z des entiers relatifs

- Construction de l'anneau ordonné (Z,+,x)
- Un exemple de calcul algébrique : l'identité de Bézout

François Viète
1540 – 1603

Etienne Bézout
1730 – 1783

La construction de Z à partir de l'ensemble N x N des couples d'entiers positifs ou nuls :

PERTE

GAIN

$$[(a,b)] = \{ (p,q) \; ; \; a + q = b + p \}$$

Si b > a, la classe [(a,b)] est notée

b-a

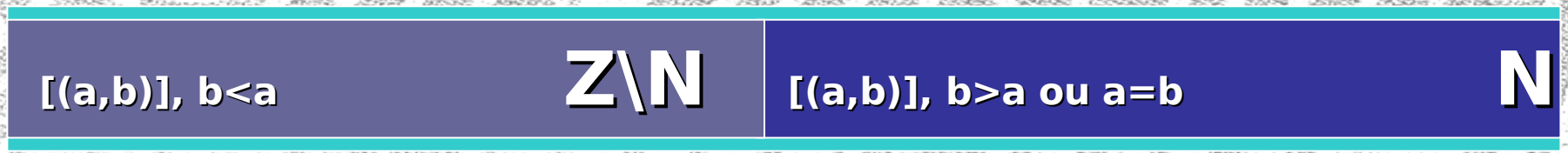
Si a > b, la classe [(a,b)] est notée

- (a-b)

Si a = b, la classe [(a,a)] est notée

0

N sous-ensemble de Z



Deux opérations ...

$$[(a_1 , b_1)] + [(a_2 , b_2)] := [(a_1 + a_2 , b_1 + b_2)]$$

$$[(a_1 , b_1)] \times [(a_2 , b_2)] := [(a_1 b_2 + a_2 b_1 , a_1 a_2 + b_1 b_2)]$$

… et un ordre total prolongeant l'ordre sur N en incorporant les deux règles additionnelles suivantes :

- **Si a et b sont des éléments de N, -a est inférieur ou égal à b**
- **Si a et b sont des éléments de N, -a est inférieur ou égal à –b si et seulement si b est inférieur ou égal à a.**

L'ordre est compatible aux deux opérations

Propriétés des opérations

(Z,+) groupe abélien

+

- **Commutativité**
  $x+y=y+x$
- **Associativité**
  $x+(y+z)= (x+y)+z$
- **Elément neutre 0**
  $x+0 = 0+x = x$
- **Tout élément x admet un « opposé » -x**
  $x+(-x) = (-x)+x = 0$

(Z,+,x) anneau commutatif unitaire

x

- **Commutativité**
  $x \times y=y \times x$
- **Associativité**
  $x \times (y \times z)= (x \times y) \times z$
- **Elément unité 1=[(0,1)]**
  $x \times 1 = 1 \times x = x$

Distributivité mult/addition

$x \times (y+z) = (x \times y) + (x \times z)$

Propriétés de Z liées à l'ordre

Toute partie non vide et minorée admet en son sein un plus petit élément (borne inférieure)

Toute partie non vide et majorée admet en son sein un plus grand élément (borne supérieure)

Un exemple de calcul algébrique dans Z: l'identité de Bézout

1730 - 1783

La division dans Z

Soient A et B deux entiers **relatifs** :

On dit que **B divise A** s'il existe un entier relatif q tel que **A=Bq**.

PGCD (A,B) := PGCD (|A|,|B|)
(si A,B non tous les deux nuls)

Le théorème de Bézout
1. Clause d'existence

Soient a et b deux entiers relatifs non tous les deux nuls et d leur PGCD

Il existe au moins un couple d'entiers (u_0, v_0) dans Z^2 tel que :

$$a\,u_0 + b\,v_0 = d \qquad (*)$$

Une démarche algorithmique récursive

fonction [PGCD,u,v] = bezout (a,b)

```
x = a ;
y = abs(b) ;
[q,r] = div (x,y) ;
si r == 0
    PGCD = y ;
    u=0 ;
    v=1 ;
sinon
    [d , u1 ,v1] = bezout (y,r) ;
    PGCD = d ;
    u = v1 ;
    v = signe (b) * (u1- q*v1) ;
fin
```

$a = b\, q_0 + r_0$

$b = r_0\, q_1 + r_1$

$r_0 = r_1\, q_2 + r_2$

....

$r_{N-3} = q_{N-1}\, r_{N-2} + r_{N-1}$

$r_{N-2} = q_N\, r_{N-1} + d$

$r_{N-1} = q_{N+1}\, d + 0$ $\quad$ PGCD $(r_{N-1}, r_N) = d$

$d = r_{N-2} - q_N\, r_{N-1} = r_{N-2} - q_N\,(r_{N-3} - q_{N-1}\, r_{N-2}) = \ldots = u\, a + v\, b$

Le théorème de Bézout
2. Clause d'unicité

On suppose a et b non nuls, de PGCD égal à d, avec a = d a', b = d b' et PGCD(a',b')=1

Les solutions (u,v) dans Z^2 de l'équation

$$a\,u + b\,v = d \qquad (*)$$

sont exactement les couples de la forme

$$(u_0 + b'\,k,\ v_0 - a'\,k)$$

où k désigne un entier arbitraire et (u_0,v_0) une solution particulière de (*)

Le lemme de Gauss

Soient a et b deux entiers relatifs non nuls

On suppose PGCD (a,b) =1

Alors, si c est un nombre entier relatif tel que b divise ac, nécessairement b divise c.

Carl F. Gauss (1777-1855)

Le théorème d'Euclide (élargi à Z)

Soient a un entier relatif et b un entier positif non nul.
Il existe un UNIQUE couple d'entiers (q,r) tels que :

$$a = b\,q + r$$

et

r est entre 0 (inclus) et b-1 (inclus)

Définition : le nombre r est dit RESTE dans la division EUCLIDIENNE de a par b.

Le nombre q est dit QUOTIENT dans la division EUCLIDIENNE de a par b.

Nombres rationnels

Fractions et développements décimaux périodiques : deux approches des rationnels

Fractions : la construction de Q à partir de l'ensemble Z x N*

le point de vue « abstrait »

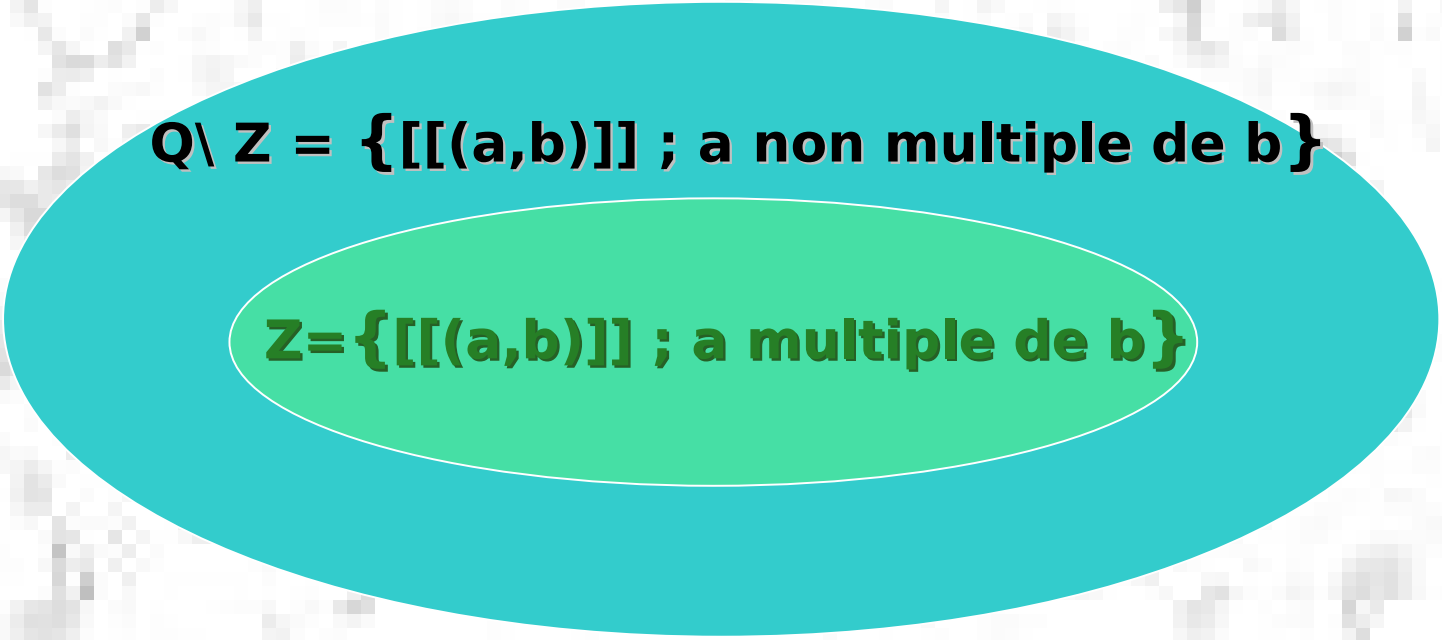
$$[[(a,b)]] = \{ (p,q) \text{ dans } Z \times N^* ; a\,q = p\,b \}$$

La classe [[(a,b)]] est notée a/b

Numérateur

Dénominateur

Z sous-ensemble de Q



Deux opérations ...

$$[[(a_1,b_1)]] + [[(a_2,b_2)]] := [[(a_1 b_2 + a_2 b_1 , b_1 b_2)]]$$

$$[[(a_1,b_1)]] \times [[(a_2,b_2)]] := [[(a_1 a_2 , b_1 b_2)]]$$

Propriétés des opérations

(Q ,+) groupe abélien

+

- **Commutativité**
  x+y=y+x
- **Associativité**
  x+(y+z)= (x+y) +z
- **Elément neutre 0 :**
  x+0 = 0 + x = x
- **Tout élément x admet un « opposé » -x**
  x+ (-x) = (-x) + x = 0

(Q,+, x) corps commutatif

x

- **Commutativité**
  x x y=y x x
- **Associativité**
  x x (y x z)= (x x y) x z
- **Elément unité 1 = [[(1,1)]]:**
  x x 1 = 1 x x = x
- **Tout élément non nul admet un inverse pour la multiplication :**
  [[(a,b)]] x [[(b,a)]] = 1

Distributivité mult/addition

x x (y+z) = (x x y) + (x x z)

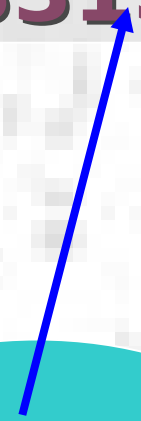
Fractions : développements décimaux

le point de vue « concret » (hérité de l'enseignement primaire)

Rationalité → **décimal** **périodique**

développement

23456 0	33567
3315 8 0	0,69



L'un des 33567 restes possibles !

Développement décimal périodique → rationalité

$x = 12,431\overline{572}$

$1000\,x - 12431 = 0,\overline{572}$

$1000\,(1000\,x - 12431) = 572,\overline{572}$

$1000\,(1000\,x - 12431) - 572 = 1000\,x - 12431$

$x = (999 \times 12431 + 572)/999000$

Fractions : écriture décimale et décimaux

$$x = m + 0, d_1\, d_2\, d_3\, d_4 \ldots \quad d_p \ldots..$$

Partie entière

décimales

$$m + 0, d_1\, d_2\, d_3\, d_4 \ldots \quad d_N\, \overline{0}$$

=

nombres décimaux

$$m + 0, d_1\, d_2\, d_3\, d_4 \ldots \quad (d_N - 1)\quad \overline{9}$$

Un « manque » à Q : un ensemble majoré n'a pas nécessairement de plus petit majorant dans Q !

Exemple : l'ensemble des nombres rationnels positifs dont le carré est inférieur ou égal à 2 !

Il faut en connaître une (ou plusieurs) preuves !!

Fin du chapitre 2