CHAPITRE 3

ENTIERS NATURELS ET ARITHMETIQUE

I ENSEMBLE DES ENTIERS NATURELS

Définition:

L'ensemble des entiers naturels est un ensemble totalement ordonné ($\leq$) , non vide, qui de plus vérifie les propriétés suivantes:

1.Toute partie non vide de N admet un plus petit élément.

2.Toute partie non vide et majorée admet un plus grand élément.

3.N n'admet pas de plus grand élément.

Les opérations dans N

*Nous connaissons deux lois de composition interne dans N, l'***addition*** et la ***multiplication**.

L'addition et la multiplication sont **commutatives, associatives.**

L'addition admet un **élément neutre 0.**

La multiplication admet un **élément neutre 1.**

La multiplication est **distributive par rapport à** *l'addition.*

II RECURRENCE

Propriété :

Soit A une partie de N contenant 0 telle que :

$\forall n \in N, n \in A \Rightarrow n+1 \in A$

Alors *A = N*

Dém: par l'absurde. Soit B=N \ A …

Cette propriété nous amène à présenter le raisonnement par récurrence.

Principe de récurrence:

Soit P(n) un prédicat défini sur N.

Si $P(n_0)$ est une proposition vraie, $n_0 \in N$.

Si $\forall n \geq n_0 \quad P(n) \Rightarrow P(n+1)$ *est vraie*

Alors *P(n) est vraie pour tout $n \geq n_0$*

Exemples:

1. Montrer :

Pour $x \in R$, $x \neq 1$; $n \in N$

$$1+x+x^2+....+x^n = \frac{1-x^{n+1}}{1-x}$$

2. Démontrer , $n \in N$

$$\sum_{k=1}^{k=n} kk! = (n+1)! - 1$$

Formule du binôme de Newton
Un peu de dénombrement (TD)

Aprés avoir défini C_n^p, nombre de parties de E à p éléments ou nombre de combinaison de n éléments pris p à p.

$$C_n^p = \frac{n!}{p!(n-p)!}$$

Montrer par récurrence sur N que $(1+x)^n = \sum_{p=0}^{p=n} C_n^p x^p$

Plus généralement :

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

On en déduit le card(P(E))

Card(P(E)) est le nombre de sous-ensembles de E.

Or C_n^p *est le nombre de sous-ensembles de E ayant p éléments, lorsque E admet n éléments.*

Donc $\sum_{p=0}^{n} C_n^p$ *est le cardinal de P(E) et pour x=1*

$$\sum_{p=0}^{n} C_n^p = 2^n$$

Définition:

Une propriété P(n) telle que :

P(n) $\Rightarrow$ *P(n+1) pour tout n* $\geq n_0$*, s 'appelle une* **propriété héréditaire à partir de n_0.**

III ARITHMETIQUE DES ENTIERS
III1. Division euclidienne dans N:

Théorème:

$\forall (a,b) \in N \times N^*, \exists$ un couple unique (q, r) d'entiers naturels t.q :

$a = bq + r, 0 \leq r \angle b$

Définition:

Effectuer la **division euclidienne** *de a par b, c'est déterminer les entiers q et r .*

Remarque:

- **a** *est le* **dividende, b** *est le* **diviseur**
- **q** *est le* **quotient, r** *est le* **reste.**

- *Lorsque r=0, b* **divise** *a et on le note :* **b | a**
- *(a, b)∈* $N \times N^*$ *, b | a⇔∃k∈N t.q a= k.b*

Exemples:

1. *Effectuer la division euclidienne de 184 par 7.*
   184 = 7×26 + 2
   q = 26 et r = 2.

2. *8 | 184, en effet : 184 = 8×23*
   q = 23 et r = 0

III2. PGCD de deux entiers naturels

Tout d'abord remarquons que **1 divise tout entier.**

Soient a et b deux entiers naturels non nuls.

Définition 1:

d est un **diviseur commun** *de a et b* **si** *d est à la fois un diviseur de a et de b.*

Soit E l'ensemble des diviseurs communs de a et b.

- $E \neq \emptyset$, *en effet* $1 \in E$.
- *De plus, a et b majorent tout élément de E*

Définition2:

D'après les propriétés de N, E est non vide et majoré donc admet **un plus grand élément** *appelé le* **pgcd(a, b).**

pgcd(a, b) | a et pgcd(a, b) | b et pgcd(a, b) est le plus grand entier qui vérifie cette propriété.

III3. Théorème de Bezout

Définition:

Les deux entiers naturels a et b sont **premiers entre eux** *si* **pgcd(a, b) = 1**, *nous pouvons alors énoncer*

Théorème de Bezout :

Les deux propositions sont équivalentes:

a et b sont premiers entre eux

$\exists (u, v) \in Z^2$ **t.q** $a.u+b.v = 1$

Démonstration d'une implication:

$\exists (u, v) \in Z^2$ *t.q* $a.u+b.v = 1 \Rightarrow$ *a et b sont premiers entre eux*

Soit d un diviseur commun à a et b, alors d divise

a.u et b.v et aussi a.u + b.v, or a.u +b.v =1

D'où d divise 1, donc d = 1

a et b sont premiers entre eux

III4. Recherche pratique du pgcd

Faisons d'abord deux remarques préliminaires:

- $a = b.q$ ***(b|a)*** $\Rightarrow$ ***pgcd(a, b) = b***
- $a = b.q+r \Rightarrow$ ***pgcd(a, b) = pgcd(b, r)***

(à démontrer)

D'où une recherche algorithmique du pgcd appelé

Algorithme d'Euclide

Algorithme d'Euclide

Le but est donc de rechercher le pgcd(a, b), a et b entiers naturels différents de 0.

écrivons les divisions euclidiennes successives:

$a = bq_1+r_1 \quad 0<= r_1< b$

$b = r_1q_2+r_2 \quad 0<= r_2< r_1$

$r_1 = r_2q_3+r_3 \quad 0<= r_3< r_2$

……………………..

$r_{n-1} = r_nq_{n+1}+r_{n+1} \quad 0<= r_{n+1}< r_n$

Les restes successifs forment une suite d'entiers positifs strictement décroissante,donc on parvient nécessairement à un reste nul, soit r_{n+1}.
Il suffit alors de remonter:
$pgcd(a, b) = pgcd(b, r_1) \ldots = pgcd(r_{n-1}, r_n) = r_n$

Remarque:
Dans cette présentation le nombre d'étapes est de n+1.
il est nécessairement majoré par b, donc fini!

Ecriture de l'algorithme:

fonction *pgcd (a, b :entiers) : entier*
var *q, r :entiers*
début
- $r \leftarrow b$
- *tant que* $r \neq 0$
- *début*
- $q = E(a/b)$
- $r = a - b.q$
- $a \leftarrow b$
- $b \leftarrow r$
- *fin de tant que*

Retourner *(a)*
fin

Remarque:

- *Les entiers a et b sont des entiers non nuls, d'après la définition du pgcd.*
- *Si a et b sont tels que a<b, la première boucle de l'algorithme nous ramène à échanger a et b et dans ce cas là, on retrouve la recherche du pgcd(a, b) avec* $a \geq b$.

Recherche du pgcd de 1764 et 3465

	$1 = q_1$	$1 = q_2$	$27 = q_3$
$3465 = a$	$1764 = b$	$1701 = r_1$	$63 = r_2$
$1701 = r_1$	$63 = r_2$	$0 = r_3$	

Pgcd(3465, 1764) = 63

III5. PPCM de deux entiers naturels

Soient a et b deux entiers naturels non nuls.
Définition 1:
$m \in N^*$ est un multiple de a $\Leftrightarrow \exists k \in N / m = k.a$
Définition 2:
$m \in N^*$ est un multiple commun à a et b
$\Leftrightarrow$ m est un multiple de a et un multiple de b
$\Leftrightarrow \exists k_1 \in N \wedge \exists k_2 \in N / m = k_1.a \wedge m = k_2.b$

Définition 3:
Considérons $M_{a\,b}$ le sous-ensemble de N^* des multiples communs à a et b. Cet ensemble est non vide puisque le produit a.b est un multiple commun donc appartient à M_{ab}.
Donc M_{ab} est une partie de N^*, non vide .
Elle admet un plus petit élément
le plus petit commun multiple de a et b
Notation: **ppcm(a, b)**

III6. Nombres entiers naturels premiers

Remarque:

- *Un entier naturel n non nul a au plus n diviseurs.*
- *Tout entier naturel est un diviseur de 0.*
- *1 admet un seul diviseur, lui-même.*

Définition:

Un entier naturel est premier lorsqu'il admet **exactement deux diviseurs.**

Remarques et exemples:

- *Tout entier strictement supérieur à 1 est donc premier lorsqu'il n'admet comme diviseurs que lui-même et 1.*
- *7 est premier puisqu'il n'admet que 2 diviseurs, lui-même et 1.*
- *12 n'est pas premier, voici l'ensemble de ses diviseurs : {1, 2, 3, 4, 6, 12}*

THEOREME FONDAMENTAL DE L'ARITHMETIQUE

Soit n un entier naturel différent de 0 et de 1.

Alors soit n est premier, soit n se décompose en un produit fini de nombres premiers.

En d'autres termes:

$n \in N, n \neq 0$ *et* $n \neq 1$

alors n est premier ou $\exists p_1, p_2, \ldots p_k$ *des entiers naturels premiers tq* $n = \prod_{i=1}^{i=k} p_i^{\alpha_i}$

avec $k \in N^*$ *et* $\alpha_i \in N^*$

III7. Ensemble des entiers relatifs

L'ensemble des entiers relatifs notés Z est muni de deux opérations + et $\times$ qui sont

- *Associatives*
- *Commutatives*
- *Z admet un élément neutre pour chacune (0 et 1)*
- *Tout entier relatif z admet un opposé -z*

III7.1. Division euclidienne dans Z

$\forall (a, b) \in Z \times Z^*$, $\exists$ *un couple unique* $(q, r) \in Z^2$ *t.q*

$a = b.q + r, \quad 0 \leq r < |b|$

q est le quotient, r est le reste .

Si r = 0, b divise a et on note **b|a.**

Remarque:

Les notions définis dans l 'ensemble des entiers naturels, peuvent être étendues à l 'ensemble des entiers relatifs, notamment:

- *nombres premiers entre eux*
- *théorème de Bezout*
- *pgcd*
- *ppcm*
- *nombres premiers (4 diviseurs au lieu de 2)*

III7.2. Congruences dans Z

La notion de congruence sera abordé plus largement dans le chapitre des relations. En voici simplement une définition.

Définition 1:

Soient z et z ' deux entiers relatifs, soit n∈N

z et z ' sont congrus modulo n *ou*

z est congru à z ' modulo n ⇔

z-z ' est divisible par n

113

Autre définition et remarque:

Définition 2 et notation :

$$\forall (z, z') \in Z^2, z \equiv z' (n) \Leftrightarrow \exists k \in Z \text{ t.q } z - z' = k.n$$

Remarque:

Lorsque 0 <z '< n, l'écriture z = z ' + k.n montre que

z ' est le reste de la division euclidienne de z par l 'entier naturel n.

114

Remarque:

On étudiera les congruences dans le chapitre IV, notamment pour n=2 et n=3

115

EXERCICE

(travail personnel à rendre suivant les indications données en cours)

Déterminer le pgcd des couples d'entiers suivants :

- *a=406 et b=696*
- *a=1540 et b=693*
- *a=462 et b=264*
- *En effectuant l'algorithme d'Euclide présenté sous forme de tableau*

116

CHAPITRE 4

LES RELATIONS

117

I PRODUIT CARTESIEN

I1. Produit cartésien de deux ensembles:

Soient E et F deux ensembles donnés, le produit cartésien de E et de F (ou produit de E par F) est l'ensemble des couples (x, y) où x est élément de E et y élément de F.

$$E \times F = \{(x, y) \text{ tels que } x \in E \text{ et } y \in F\}$$

118

Remarques:

- x et y sont les composantes du couple
- $(x, y)=(x', y') \Leftrightarrow x=x'$ et $y=y'$
- Lorsque $E = F$ le produit s'appelle carré cartésien de E , noté $E \times E$ ou E^2

119

I2. Généralisation:

Le concept de produit cartésien peut être généralisé à un nombre fini d'ensembles.

Soient $E_1, E_2, \ldots E_n$, $E_1 \times E_2 \times \ldots \times E_n$ sera l'ensemble suivant:

$E_1 \times E_2 \times \ldots \times E_n = \{(x_1, x_2, \ldots, x_n)$ tels que $x_1 \in E_1, x_2 \in E_2, \ldots, x_n \in E_n\}$

Soit E, E^n sera l'ensemble suivant:

$E^n = \{(x_1, x_2, \ldots, x_n)$ tels que $x_1 \in E, x_2 \in E, \ldots, x_n \in E\}$

$(x_1, x_2, \ldots, x_n)$ est appelé un n-uplet

120

Le produit cartésien n'est pas commutatif.

$A \times B \neq B \times A$

Le produit cartésien n'est pas associatif.

$(A \times B) \times C \neq A \times (B \times C)$

121

Exemples:

- $A=\{x, y, z\}$; $B=\{1,2\}$
- $A=\{x, y, z\}$; $B=\{1,2\}$; $C=\{\alpha\}$

122

Exercices

A et B deux ensembles donnés

Montrer que :

$$A \times B = \phi \Leftrightarrow A = \phi \vee B = \phi$$

Que peut-on conclure au sujet d'ensembles A et B si:

$$(A \times B) \cap (B \times A) \neq \phi$$

123

II RELATIONS

II1. Relation et prédicat:

Définition 1:

Soient E et F deux ensembles et $E \times F$ leur produit cartésien.
Une relation sur $E \times F$ est un prédicat défini sur $E \times F$.

$\forall x \in E, \forall y \in F$

x est en relation avec y par $R \Leftrightarrow xRy$

$\Leftrightarrow R(x, y)$

124

Quelques relations connues

dans R

$<; >; \leq; \geq; =; \neq;$

Dans Z

$\equiv; \mid;$

Dans P(E)

$\subset$

II2. Relation et graphe:

Définition 2:

Le graphe de la relation R est le sous-ensemble correspondant G de E×F.

La relation R est définie à l'aide de son graphe G

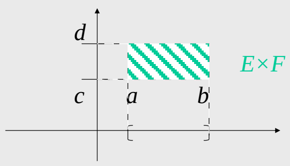
$$G = \{(x, y) \in E \times F \text{ t.q } x \mathrel{R} y\}$$

Exemple 1

Soit E et F deux parties de R.

E=[a, b]; F=[c, d]

Voici une **représentation cartésienne** *de E×F*



Soit G_R=E×F, comment définir cette relation à l'aide d'un prédicat?

Exemple 2

A={1, 2, 3, 4, 5, 6}

B={2, 6, 8, 9}

G_R={(1,2),(1,6),(1,8),(1,9),(2,2),(2,6),(2,8),(3,6),(3,9),(4,8),(6,6)}

Comment définir cette relation à l'aide d'un prédicat?

Exemple 3

Soit E un ensemble donné.

On appelle identité de E et on note $\boldsymbol{I_E}$ ***ou*** $\boldsymbol{1_E}$ *la relation binaire définie sur E par:*

$$\forall (x, y) \in E^2, x \, 1_E \, y \Leftrightarrow x = y$$

Comment définir cette relation à l'aide de son graphe, noté Δ_E ?

On en conclut le résultat suivant

Soit R une relation définie sur $E \times F$,

E et F deux ensembles donnés.

Soit G_R son graphe;

$$\forall (x, y) \in E \times F, x \mathrel{R} y \Leftrightarrow (x, y) \in G_R$$

Remarque et définition:

- *E et F sont deux ensembles donnés.*

L'ensemble des relations définies sur $E \times F$ est l'ensemble des parties de $E \times F$, soit $P(E \times F)$

- *Soit E un ensemble.*

*Une **relation binaire définie sur E** est une relation définie sur $E \times E$*

131

III PROPRIETES DES RELATIONS

*R est une relation définie sur $E \times E$ ou **relation binaire définie sur E***

1. ***R est réflexive*** $\forall x \in E,\ x R x$

2. ***R est antiréflexive*** $\forall x \in E, x \overline{R} x$

132

3. R est symétrique

$\forall (x, y) \in E^2, xRy \Rightarrow yRx$

remarque:

$\Leftrightarrow \forall (x, y) \in E^2, xRy \Leftrightarrow yRx$

4. R est antisymétrique

$\forall (x, y) \in E^2, [xRy \wedge yRx\ ] \Rightarrow x = y$

133

5. R est transitive

$\forall (x, y, z) \in E^3, [xRy \wedge yRz\ ] \Rightarrow xRz$

6. R est circulaire

$\forall (x, y, z) \in E^3, [xRy \wedge yRz\ ] \Rightarrow zRx$

134

EXERCICES

(travail personnel à rendre suivant les indications données en cours)

1. *La relation divise sur Z est réflexive.*
2. *La relation $<$ sur R est antiréflexive.*
3. *Soit la relation binaire S définie sur Z par:*

   $\forall (x,y) \in Z^2, xSy \Leftrightarrow x + y$ *est impair*

   Montrer que S est antiréflexive

135

CHAPITRE V

RELATIONS D' EQUIVALENCE
RELATIONS D'ORDRE
APPLICATIONS

136

I RELATIONS D' EQUIVALENCE

I.1 Définition et exemples:

Définition 1:

Une relation R définie sur E est une relation d'équivalence sur E **si** *R est à la fois* **réflexive, symétrique** *et* **transitive.**

I.2 Classes d'équivalence modulo R, Ensemble quotient:

Définition 2:

R est une relation d'équivalence définie sur E, et x∈E. On appelle **classe d'équivalence de x** *(modulo R) et on note $\overline{x}$ l'ensemble suivant:*

$$\overline{x} = \{y \in E \text{ tq } x \, R \, y\}$$

EXEMPLES:

1. Sur n'importe quel ensemble E, la relation d'égalité , 1_E est une relation d'équivalence et $\overline{x} = \{x\}$

2. Soit n ∈ N, la congruence* **modulo n** *est une relation d'équivalence : Cas particulier la congruence modulo 2.*

3. Etude de la relation définie sur R par :

$$\forall (x, y) \in R^2, x \, R \, y \Leftrightarrow x^2 = y^2$$

Théorème 1:

Soit R une relation d'équivalence définie sur E. On a:

$$\forall (x, y) \in E^2, \bullet \; \overline{x} = \overline{y} \Leftrightarrow xRy$$

$$\bullet \; \overline{x} \neq \overline{y} \Rightarrow \overline{x} \cap \overline{y} = \phi$$

Preuve:

1. x R y et soit t ∈ $\overline{x} \Rightarrow t \in \overline{y}$ et réciproquement.

2. par contraposition.

Théorème 2:

R est une relation d'équivalence définie sur E, alors:

1. $\forall x \in E, x \in \overline{x}$ d'où $\overline{x} \neq \phi$

2. *Une classe d'équivalence est un élément de P(E).*

Remarques:

1. Deux classes d'équivalence sont :

Soit ***disjointes*** $\overline{x} \cap \overline{y} = \varnothing$

Soit ***confondues*** $\overline{x} = \overline{y}$

2. D'après le théorème précédent, $\overline{x} \neq \varnothing$

Définition 3:

L'ensemble des classes d'équivalence modulo R est appelé **ensemble quotient de E par R**

et est noté E/R

$$E/R = \{c \in P(E) \; tq \; \exists x \in E \; tq \; \bar{x} = c\}$$

Remarque: $E/R \subset P(E) \Leftrightarrow E/R \in P(P(E))$

143

EXEMPLES :

- *Déterminer l'ensemble quotient suivant:*

$$E/I_E$$

$$E/I_E = \{\{x\}, x \in E\}$$

- *Considérons à nouveau la congruence modulo 2.*

Alors $Z/R_2 = Z/2Z = \{\bar{0}, \bar{1}\}$

144

EXERCICES

(travail personnel à rendre suivant les indications données en cours)

$\forall (x,y) \in R^2, xTy \Leftrightarrow \cos(x) = \cos(y)$

Montrer que

a)T est une relation d'équivalence

b)Quels sont ces classes d'équivalence?

145

II RELATIONS D'ORDRE SUR E

II1. Définition, exemples:

Définition:

Soit R une relation binaire définie sur E.

On dit que R est une relation d'ordre sur E ***si*** *R est* ***réflexive, antisymétrique, transitive.***

146

Notation:

Une relation d'ordre sera notée par un ***signe spécifique*** *soit par:* « $\prec$ »

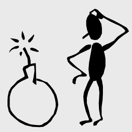
On pourra lire: « $x \prec y$ »

« x est dominé par y »

147

Exemple

Sur N, Z, Q, R les relations classiques, $\leq, \geq$ *sont des relations d 'ordre .*



Les relations $<$ *et* $>$ *ne sont pas des relations d 'ordre car elles ne sont pas réflexives.*

148

EXERCICE

(travail personnel à rendre suivant les indications données en cours)

Soit E un ensemble donné et soit P(E) . La relation définie sur P(E) par:

$$\forall (A,B) \in (P(E))^2, A\ R\ B \Leftrightarrow A \subset B$$

Montrer que l'inclusion est une relation d 'ordre sur E.

149

EXERCICE

(travail personnel à rendre suivant les indications données en cours)

Considérons la relation « divise » sur N

$$\forall (a,b) \in N^2, a \mid b \Leftrightarrow (\exists k \in N \text{ tq } b = ka)$$

Cette relation $/$ *est une relation d 'ordre sur N.*

150

II2. Ordre total, ordre partiel

Définition:

Une relation d 'ordre, $\prec$ *sur un ensemble E est appelée* **ordre total** *si pour tous éléments x et y de E, x et y sont comparables.*

$$\forall (x,y) \in E^2, x \prec y \vee y \prec x$$

Les relations précédemment évoquées ≤ ou ≥ sont des ordres totaux.

151

Définition:

Une relation, d 'ordre $\prec$ *sur un ensemble E qui n 'est pas une relation d 'ordre total est une relation* **d 'ordre partiel .**

En prenant la négation de la proposition précédente:

$$\exists (x,y) \in E^2 \text{ tq } \overline{x \prec y} \wedge \overline{y \prec x}$$

x et y sont alors 2 éléments non comparables.

152

Exemple

1. *Considérons la structure ordonnée (P(E),* $\subset$*) où E est un ensemble* **non vide et possède au moins 2 éléments.** *Alors*

$$\exists (\{e_1\},\{e_2\}) \in P(E)^2 \text{ tq}$$
$$\{e_1\} \not\subset \{e_2\} \wedge \{e_2\} \not\subset \{e_1\}$$

153