Livres utiliser pour preparer le cours

Euclid, The thirteen books of the Elements, by Thomas L. Heath, en particulier livres VII. - IX.

R. Strichartz, The Way of Analysis
(Définition des réels par des suites de Cauchy)

L. Cohen, G. Ehrlich, The Structure of the Real Number System
($\mathbb{Z}$ et $\mathbb{Q}$ et $\mathbb{R}$)

E. Bloch, The Real Numbers and Real Analysis
(coupures de Dedekind)

Notes de Chiron (réels comme décimaux infinis)

J. M. Arnaudiès, H. Fraysse, Analyse

Nombres naturels

$\mathbb{N}$ $0, 1, 2, 3, \ldots, n, n+1, \ldots$

Soit $n \in \mathbb{N}$. Alors $s(n) := n+1$ s'appelle

héritier de n.
(successeur)

On observe que

A i) 0 est un nombre naturel,

A ii) chaque nombre naturel a un héritier,

A iii) 0 n'est pas un héritier d'un nombre naturel,

A iv) deux nombres naturels ayant le même héritier sont égaux,

A v) soit $X \subset \mathbb{N}$ un sous-ensemble de $\mathbb{N}$. Si $0 \in X$ et si pour chaque nombre naturel appartenant à X, son héritier appartient

à $\mathbb{X}$ alors $\mathbb{X} = \mathbb{N}$.

Ai) — Av) sont des axiomes d'arithmétique de nombres naturels

Av'

De ces axiomes ont déduit des operations $+$, $\cdot$ et la relation $<$.

Kronecker à dit "Dieu a créé nombres naturels, et tout autre est fait par un homme".

Mais on définit aussi des nombres naturels.

$0 := \emptyset$ l'ensemble vide

$1 := \{\emptyset\}$

$2 := \{\emptyset, \{\emptyset\}\} = \{0, 1\}$

$3 := \{0, 1, 2\}$

$\vdots$

$S(n) := \{n, \{n\}\}$ $n \cup \{n\}$

Alors on définit l'addition, la multiplication, la relation $<$. Par exemple

$$n < m \iff n \in m.$$

si $a > b$ $\overbrace{a=b}^{\text{ou}}$ $a - b = x$ t.q. $a = b + x$

Règles de raisonnement

modus ponens

- Si $P \Rightarrow Q$ est vraie et si P est vraie alors Q est vraie.

tautologie — toujours vraie

1. non (P et non P)
2. P ou non P
3. $(\text{non } Q \Rightarrow \text{non } P) \Rightarrow (P \Rightarrow Q)$
4. $((P \text{ et non } Q) \Rightarrow (R \text{ et non } R)) \Rightarrow (P \Rightarrow Q)$
- ...

$a \Rightarrow b$

1 = vrai
0 = faux

$1 \Rightarrow 0$ fausse

$0 \Rightarrow 0$
$0 \Rightarrow 1$
$1 \Rightarrow 1$
} vraie

Exemple.

On veut montrer que $P \Rightarrow Q$.

On montre que non$Q \Rightarrow$ non$P$ est vraie. $\bullet_3$ est vraie donc $\bullet$ implique que $P \Rightarrow Q$ est vraie.

Exemple. Reductio ad absurdum

$a > b \Rightarrow a+1 > b+1$

On veut montrer que $P \Rightarrow Q$.

$a > b$ $\quad$ $a+1 \leq b+1$ $\quad$ $a > b$ et $a \leq b$

On montre que (P et non $Q \Rightarrow$ fausse R et non R)

Donc (P et non $Q \Rightarrow$ R et non R fausse) vraie et $\bullet_4$ est vraie donc la règle modus ponen implique ($P \Rightarrow Q$) vraie.

Récurrence mathématique

On veut montrer la suite de propositions $A_0, A_1, A_2, \ldots$.

Par exemple

A_n : $0 + 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$

(Récurrence mathématique)

Théorème. Si la proposition A_0 est vraie et si pour chaque $n \in \mathbb{N}$, A_n vraie implique A_{n+1} vraie, alors toutes les propositions $A_0, A_1, A_2, \ldots$ sont vraie.

Preuve.

Soit $\mathbb{X} := \{ m \in \mathbb{N} \mid A_m \text{ vraie} \}$.

A_0 est vraie donc $0 \in \mathbb{X}$.

Soit $m \in \mathbb{X}$ un élément quelconque de $\mathbb{X}$. Donc A_m est vraie. On sait que A_m vraie implique A_{m+1} vraie. Cette implication est donc vraie. Donc par modus ponen, A_{m+1} est vraie. Donc $m+1 \in \mathbb{X}$.

On a : $0 \in \mathbb{X}$ et

si $m \in \mathbb{X}$ un élément quelconque alors $s(m) = m+1 \in \mathbb{X}$. Donc par l'axiome Av) $\mathbb{X} = \mathbb{N}$. Donc toutes les propositions $A_0, A_1, \ldots$ sont vraies. ∎

L'axiome

Av') Soit $X \subset \mathbb{N}$ un sous-ensemble non vide de $\mathbb{N}$. Alors X contient l'élément plus petit.

$$((X \subset \mathbb{N} \text{ et } X \neq \emptyset) \Rightarrow (\exists\, a \in X \text{ t.q. } \forall (x \in X \text{ et } x \neq a),\ a < x))$$

est équivalent à Av.

Théorème. Pour chaque $n \in \mathbb{N}$ on a

A_n: $0+1+2+\ldots+n = \frac{n(n+1)}{2}$.

Preuve.

On a $0 = \frac{0(0+1)}{2}$,

donc A_0 est vraie.

Soit $n \in \mathbb{N}$ quelconque. Si A_n vraie, alors $0+1+\ldots+n = \frac{n(n+1)}{2}$.

Alors $0+1+\ldots+n+(n+1) = \frac{n(n+1)}{2} + (n+1) =$

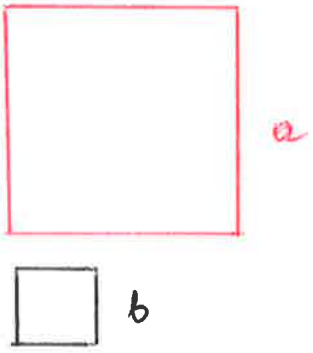
$= \frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)(n+2)}{2} = \frac{(n+1)((n+1)+1)}{2}$.

Donc A_{n+1} est vraie. Le théorème de récurrence math. implique donc $0+1+\ldots+n = \frac{n(n+1)}{2}$

pour chaque n naturel.

Définition 2 de livre V de Euclide.

b mesure a si a est un multiple de b.



Définition 1 de livre X.

Deux magnitudes sont commensurables s'ils sont mesurés par la même mesure (magnitudes).

a (12 cm)

b (10 cm)

c (2 cm)

d (1 cm)

c_1 (0.5 cm)

} mesures communes de a et b

Comment trouver une mesure commune ?

a

b

$a > b$

$a_1 = a - b$

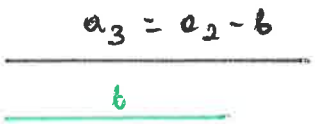
b

$a_1 > b$

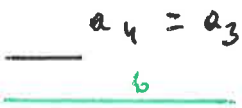
$a_2 = a_1 - b = (a - b) - b$

b

$a_2 > b$



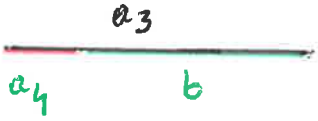
$a_3 > b$



$b > a_4$

On recommence

Ici a_4 mesure b,



donc a_4 mesure a_3

⋮ . . . a_2

donc a_4 mesure a_1

donc a_4 mesure a.

Montrons que a_4 est la plus grande mesure commune de a et b. (PGMes $C(a,b)$).

Le preuve par reductio ad absurdum.

Supposons que ce n'est pas vraie. Alors $g > a_4$ mesure a et b. Donc g mesure a_1, donc g mesure .. a_2, a_3, a_4. Comme g mesure a_4 alors $g \leqslant a_4$. Donc $g > a_4$ et $g \leq a_4$. Donc a_4 est le plus grand mesure commune.

Proposition 3 de livre X

Ayant donnés deux magnitudes commensurables trouver leur plus grande mesure commune.

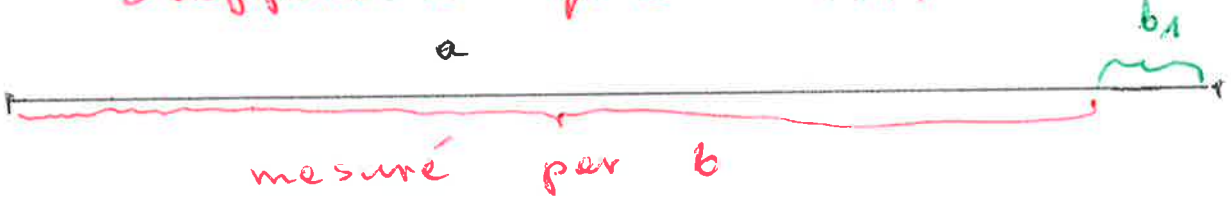
Euclide presente la procedure pour trouver une mesure commune et il montre qu'on obtient la PGMesure Commune (Donc il montre que la PGMesC existe).

Si $a = b$ alors la mesure commune.

$a > b$

Si a est mesuré par b alors b est une mesure commune et la PGMesC (a, b)

Supposons que non.



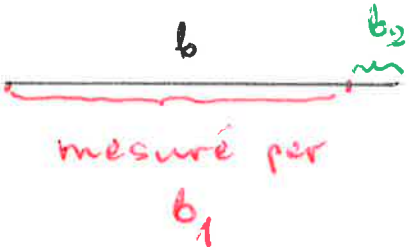
Postulat d'Archimède

$b_1 < b$

Si b_1 mesure b alors b_1 mesure a.

et on voit que b_1 est la PGMesC (a, b).

Supposons que non.



$b_2 < b_1$ et de plus

$b_2 < \frac{1}{2} b$. ‖

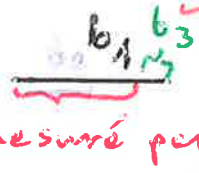
(Si $b_2 \geq \frac{1}{2} b$ alors $b_1 > b_2 \geq \frac{1}{2} b$.

mais $b_1 > \frac{1}{2} b \Rightarrow b_2 < \frac{1}{2} b$, car $b_1 + b_2 = b$)

donc absurde

Si b_1 est mesuré par b_2 alors ... b et a sont mesurés par b_2 et alors $b_2 = PGMC(a,b)$

Si non



$b_3 < b_2$ et de plus

$b_3 < \frac{1}{2} b_1$ ‖

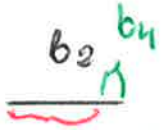
(Si $b_3 \geq \frac{1}{2} b_1$ alors

$b_2 > b_3 \geq \frac{1}{2} b_1$. On a alors $b_1 = b_2 + b_3$

donc $b_3 < \frac{1}{2} b_1$)

Si b_2 est mesuré par b_3 alors .... a et b sont mesurés par b_3 et b_3 et la $PGMC(a,b)$.

Si non



mesuré par b_3

$b_4 < b_3$ et de plus

$b_4 < \frac{1}{2} b_2$

(si $b_4 \geq \frac{1}{2} b_2$ alors $b_3 > \frac{1}{2} b_2$,

$b_2 = b_3 + b_4$ donc $b_4 < \frac{1}{2} b_2$)

et on continue

$b_2 < \frac{1}{2} b$

$b_4 < \frac{1}{2} b_2$

$b_6 < \frac{1}{2} b_4$

$b_{2n} < \frac{1}{2^n} b$

on

$b_3 < \frac{1}{2} b_1$

$b_5 < \frac{1}{2} b_3$

$b_{2n+1} < \frac{1}{2^n} b_1$

Mais on a supposé que a et b ont une mesure commune $c > 0$. Cette mesure commune c va alors mesuré chaque b_n. Mais c'est impossible car b_n devient plus petit que c. Donc le procedure s'arrête en certain moment et la dernière $b_i > 0$ est Une mesure commune de a et b et c'est le PGMasC (a, b) ∎

parle de AV1

$\mathbb{N}$

$a, b \in \mathbb{N}$ sont commensurables car 1 une mesure commune.

(Def 5 de Livre VII)

Définition. Soient $a, b \in \mathbb{N}$. On dit que b divise a s'il existe $c \in \mathbb{N}$ (b est un diviseur de a) tel que

$$a = c \cdot b, \qquad b \neq 0$$

(a est mesuré par b)

(Notez que a et b ont alors la mesure commune b.)

Notation: b divise a on note $b \mid a$.

$b \nmid a \equiv b$ ne divise pas a

Voici certains faits evidents

- $b \mid a$ et $c \mid b \Rightarrow c \mid a$,
- $b \mid a$ et $c \neq 0 \Rightarrow bc \mid ac$,
- $c \mid a$ et $c \mid b \Rightarrow c \mid a+b$
- $c \mid a$ et $c \mid b$ et $a > b \Rightarrow c \mid a-b$
- $c \neq 0, ac = bc \Rightarrow a = b$.

(Déf. 11 de Livre VII)

Définition. Soit $p \in \mathbb{N}$, On dit que p est premier si $p > 1$ et si les seuls diviseurs de p sont 1 et p.

2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~, 11, ~~12~~, ...

Proposition. Chaque nombre naturel plus grand que 1 est un produit des nombres premiers, ou est un nombre premier (produit d'un nombre premier).

Preuve.

Preuve par récurrence :

A_n : n est un produit de nombres premiers ou un nombre premier $n \geq 1$

A_2 : 2 est un premier, donc A_2 vraie

A_3 : 3 est un premier donc A_3 vraie

Supposons $A_2, A_3, \ldots, A_n$ vraies ($n \geq 2$). $n \geq 3$

$n+1$ ⇒ Si $n+1$ est premier alors A_{n+1} vraie

? changer l'ordre

> Si : $n+1 = a \cdot b$ $a > 1$ et $b > 1$

alors $a < n+1$ et $b < n+1$ donc A_a et A_b sont vraies.

Donc $a = p_1 \cdots p_r$ et $b = q_1 \cdots q_s$ produits des premiers

donc $n+1 = a \cdot b = p_1 \cdots p_r \cdot q_1 \cdots q_s$ produit des premiers

donc A_{n+1} est vrais.

Mais A_2 n'implique pas A_3!

On doit vérifier aussi A_3.

(Prop. 31, 32 Livre VII de Euclide)

Corollaire. Soit $n \in \mathbb{N}$ et $n > 1$. Alors un nombre premier divise n.

Théorème (Prop. 20 livre IX de Euclide)

~~Le nombre de nombres premiers est plus grand que n'importe quel $n \in \mathbb{N}$.~~ Il y a une infinité des nombres premiers.

Preuve. Supposons qu'il y a seulement n nombres premiers $p_1, p_2, \ldots, p_n$.

Soit $m = p_1 \cdot p_2 \cdots p_n + 1$.

On a $m > 1$.

~~Si m est un nombre premier alors $m > p_1$, $m > p_2$ $m > p_n$ donc p_1, p_2, p_n, m $n+1$ nombres premiers.~~

Alors il existe un nombre premier q t.q. $q \mid m$. (par Corollaire)

Mais $p_1 \nmid m, \ldots p_n \nmid m$ donc $q \neq p_1$, $q \neq p_2, \ldots q \neq p_n$. Donc il y a $n+1$ ou plus nombres premiers.

Théorème (division euclidienne, Prop. 2 Livre VII de Euclide)

Soient $a, b \in \mathbb{N} \setminus \{0\}$. Alors il un unique couple $(q, r) \in \mathbb{N} \times \mathbb{N}$ tel que

$$a = q \cdot b + r \quad \text{et} \quad 0 \leq r < b.$$

De plus

~~d~~ $d \mid a$ et $d \mid b$ ~~alors~~ si et seule si $d \mid b$ et $d \mid r$

Définition (Déf. 12 de livre VII de Euclide)

Soient $a, b \in \mathbb{N}$. On dit que a et b sont premiers entre eux si

$$c \mid a \text{ et } c \mid b \implies c = 1.$$

Définition (Déf. 12 de livre VII)

Soient $a, b \in \mathbb{N}$. On dit que a et b sont premiers entre eux si

$$c \mid a \quad \text{et} \quad c \mid b \implies c = 1.$$

Deux nombres $a, b \in \mathbb{N}$ sont commensurables, par exemple 1 est une mesure commune.

Proposition (Division euclidienne)

Soient $a, b \in \mathbb{N}$ et $b \neq 0$. Alors il existe $q \in \mathbb{N}$ et $r \in \mathbb{N}$ tels que

$$* \qquad a = q \cdot b + r \quad \text{avec} \quad r < b.$$

De plus q et r tels que $*$ sont uniques.

Preuve.

Si $a < b$ alors $q = 0$ et $r = a$.

Si $a \geqslant b > 0$ alors il existe $\mathbb{Q} \in \mathbb{N}$ t. q. $\mathbb{Q} b > a$ (par exemple $\mathbb{Q} = a$).

Soit $\mathbb{X} = \{ Q \in \mathbb{N} \mid Qb > a \} \neq \emptyset$.

Soit q' le plus petit élément de $\mathbb{X}$. (Axiome AV'). Alors $q' > 0$. Soit $q := q' - 1$

Alors

* $$q \cdot b \leqslant a < (q+1) b .$$

Donc $a = q \cdot b + r$ où $r = a - qb$

et * implique $0 \leqslant r < b$. ■

unicité : $a = qb + r$; $a = q_1 b + r_1$; $q > q_1 \Rightarrow r_1 > r \Rightarrow (q - q_1) b = r_1 - r \Rightarrow$ $0 \leq r_1 - r < b$, $r_1 - r$ multiple de $b \Rightarrow r_1 = r$,

Théorème (Propositions 1 et 2 de livre VII)

Trouver le plus grand commun diviseur de deux nombres naturels.

(L'algorithme d'Euclide pour trouver PGCD (a, b)). L'algorithme montre que PGCD(a,b) existe et on le trouve.

$a, b \in \mathbb{N}$ $\quad a > b > 0$

$*_0$ $\quad a = q \cdot b + r \qquad b > r$

$*_1$ $\quad b = q_1 r + r_1 \qquad r > r_1$

$*_2$ $\quad r = q_2 r_1 + r_2 \qquad r_1 > r_2$

$*_3$ $\quad r_1 = q_3 r_2 + r_3 \qquad r_2 > r_3$

$*_4$ $\quad r_2 = q_4 r_3 + r_4$

On a

$$a > b > r > r_1 > r_2 > r_3 \overset{0}{\overset{+}{}}$$

tous sont nombres naturels donc on obtient $r_n = 0$ pour certain $n < a$

Supposons que $r_4 = 0$ donc

$$r_2 = q_4 r_3 .$$

Alors $r_3 \mid r_2 \Rightarrow r_3 \mid r_1 \Rightarrow r_3 \mid r \Rightarrow$

$\Rightarrow r_3 \mid b \Rightarrow r_3 \mid a$.

Donc r_3 est un diviseur commun de a et b.

Montrons que r_3 est PGDC(a,b).

Si non, alors il existe $(\exists)$ $d > r_3$ et $d \mid a$ et $d \mid b$. Alors $d \mid r$

$\Rightarrow d \mid r_1 \Rightarrow d \mid r_2 \Rightarrow d \mid r_3$

donc $d \leqslant r_3$. Donc $d > r_3$ et $d \leqslant r_3$.

(on veut montrer $P \begin{cases} x_1 \\ \vdots \\ x_2 \end{cases} \Rightarrow r_3 = \text{PGCD}(a,b)$.

On a montré (P et non $(r_3 = \text{PGCD}(a,b))$) $\Rightarrow$ R et non R

Donc par Reductio ad Absurdum

P c'est-à dire notre procedure $\Rightarrow r_3 = \text{PGCD}(a,b)$.

trop long dé...

Dans $*_3$ $\quad r_1 = q_3 r_2 + r_3$

on remplace r_2 par $r - q_2 r_1$ de $*_2$, donc

$$r_1 = q_3 r - q_3 q_2 r_1 + r_3$$

$$\overbrace{(1 + q_2 q_3)}^{\mathbb{Q}} r_1 = q_3 r + r_3$$

On remplace r_1 par $b - q_1 r$ de $*_1$

$$\overbrace{(1 + q_2 q_3)}^{\mathbb{Q}} (b - q_1 r) = q_3 r + r_3$$

$$\mathbb{Q} b = \overbrace{(\mathbb{Q} q_1 + q_3)}^{\mathbb{Q}_1} r + r_3$$

On remplace r par $a - qb$ de $*_0$

$$\mathbb{Q} b = \mathbb{Q}_1 a - \mathbb{Q}_1 q b + r_3$$

donc $\quad \underbrace{(\mathbb{Q} + \mathbb{Q}_1 q)}_{A} b - \underbrace{\mathbb{Q}_1}_{B} a = \underbrace{r_3}_{\text{PGCD}(a,b)}$

<u>Corollaire</u> Soient $a, b \in \mathbb{N}$ et, $a > b > 0$.

Alors il existe $A, B \in \mathbb{N}$ t. q.

$$A a - B b = \text{PGCD}(a, b)$$

ou

$$B \cdot b - A \cdot a = \text{PGCD}(a, b) \quad . \blacksquare$$

Si $a > 0$, $\text{PGCD}(a, 0) = a$ et

$$1 \cdot a - 0 \cdot 0 = a$$

$\text{PGCD}(0, 0) := 0$

Proposition (Prop. 30 de Livre VII)

Soient $a, b \in \mathbb{N}$. Soit p un nombre premier. Si $p \mid a \cdot b$ alors $p \mid a$ ou $p \mid b$.

Preuve.

Preuve de Euclide.

$p \mid a \cdot b$. Supposons que $p \nmid a$. Alors p et a sont premiers entre eux. On a $ab = m \cdot p$. Donc les rapports $p : a = b : m$.

Dans ce rapport p et a sont premiers entre eux. Donc parmi toutes paires qui ont le même rapport ils sont les plus petits. Mais alors b est multiple de p et m de a (Prop. 21, Prop 20 de livre VII)

Preuve

$p \mid a \cdot b$. Supposons que $p \nmid a$. Alors p et a sont premiers entre eux, donc $PGCD(p, a) = 1$. Donc il existe $x, y \in \mathbb{N}$ t.q. $xp - ya = 1$ (ou $ya - xp = 1$).

$xp = ya + 1 \Rightarrow xpb = yab + b$

$= m \cdot p$

$\Rightarrow \quad xpb - ymp = b \quad \Rightarrow \quad p(xb - ym) = b$

$\Rightarrow \quad p \mid b.$

Corollaire. Soit p un nombre premier et soient $a_1, \ldots, a_n \in \mathbb{N}$. Si $p \mid a_1 a_2 \ldots a_n$ alors $\exists 1 \leq j \leq , \; p \mid a_j$.

Théorème fondamental de l'arithmetique de nombres naturels.

Décomposition d'un nombre naturel (>1) en produit des nombres premiers est unique.

Soit $n \in \mathbb{N}$ et $n > 1$. Alors il existe de nombre premiers $p_1 < p_2 < \ldots < p_r$ et les nombres naturels $\alpha_1 > 0$, $\alpha_2 > 0, \ldots \alpha_r > 0$ tels que

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_r^{\alpha_r}.$$

De plus r, la liste des p_i et des α_i correspondants à n est unique

Preuve.

On a déjà vu que chaque $n > 1$ est un produit des nombres premiers.

Preuve de l'unicité de la décomposition...

Lemme. Soient $a, b, c \in \mathbb{N}$ et $c \neq 0$.
si $ac = bc$ alors $a = b$.

Supposons que

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad \text{et} \quad n = q_1^{\beta_1} \cdots q_s^{\beta_s}$$

avec $p_1 < p_2 < p_r$, $\alpha_i > 0$ et $q_1 < q_2 < q_s$, $\beta_j > 0$

$p_i \mid n$ donc $p_i \mid q_1^{\beta_1} \cdots q_s^{\beta_s} \Rightarrow$

$p_i \mid q_j^{\beta_j}$ pour certain $j \Rightarrow p_i \mid q_j$

$\Rightarrow p_i = q_j$.

Donc $\{p_1, p_2, \ldots p_r\} \subset \{q_1\ q_2 \ldots q_s\}$

Par la même raisonement

$\supset$

Donc $\{p_1, p_2, \ldots p_r\} = \{q_1\ q_2 \cdots q_s\}$, $s = r$.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \text{ et } n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}.$$

si $\alpha_j > \beta_j$ alors $p_1^{\alpha_1} \cdots p_j^{\alpha_j - \beta_j} \cdots p_r^{\alpha_r} = p_1^{\beta_1} \cdots p_{j-1}^{\beta_{j-1}} p_{j+1}^{\beta_{j+1}} \cdots p_r^{\beta_r}$

$\mathcal{L}$ $\mathcal{D}$

Donc $p_j \mid \ell \Rightarrow p_j \mid D \Rightarrow$

$p_j \mid p_k^{\beta_k}$ avec $k \neq j \Rightarrow p_j \mid p_k$ p_j, p_k premiers distincts

$\Rightarrow p_j = p_k$ et $p_j \neq p_k$.

Donc $\alpha_j = \beta_j$.

Donc ..

■

$\mathbb{Z}$ nombres entiers

$\ldots -3, -2, -1, 0, 1, 2, 3, \ldots$

L'ensemble $\mathbb{Z}$ est muni d'une addition $+$ et une multiplication $\times$ (notée aussi $\cdot$) et de deux éléments 0 et 1 tels que

$+_1$ $\quad a + b = b + a$, (commutativité)

$+_2$ $\quad a + (b + c) = (a + b) + c$ (associativité)

$+_3$ $\quad a + 0 = a$ (0 est l'élément neutre pour $+$)

$+_4$ $\quad \forall a \in \mathbb{Z}$ $\exists$ unique $x \in \mathbb{Z}$ t.q. $a + x = 0$

(on note $x = -a$)

$*_1$ $\quad a \times b = b \times a$

$*_2$ $\quad a \times (b \times c) = (a \times b) \times c$

$*_3$ $\quad 1 \times a = a$ (1 est neutre pour $\times$)

$\times_4$ $\quad a \times (b + c) = a \times b + a \times c$ (distributivité de $\times$ par rapport à l'addition)

$(\times_5)$ $\quad a \times b = 0 \Rightarrow a = 0$ ou $b = 0$. 1er fait

De plus $0 \times a = 0$ $\mathbb{Z}_1$, $(-1) \times a = -a$, $(-a) \times b = -(a \times b)$, $(-1) \times (-1) = 1$

Définition. Soit A un ensemble non-vide muni de deux opérations $+$ et $\times$ et de deux éléments 0_A et 1_A qui satisfont $+_1 - +_4$ et $\times_1 - \times_4$. On dit alors que A est un anneau commutatif. Si A satisfait aussi $(\times_5)$ alors on dit que A n'a pas de diviseurs de zéro.

Exemple

$$\mathbb{Z}[\sqrt{-5}] = \{ a + b\sqrt{-5} \mid a, b \in \mathbb{Z} \}$$

$$(a + b\sqrt{-5}) + (c + d\sqrt{-5}) := (a+c) + (b+d)\sqrt{-5}$$

$$(a + b\sqrt{-5}) \times (c + d\sqrt{-5}) :=$$

$$(ac - 5bd) + (ad + bc)\sqrt{-5}$$

$$\sqrt{-5} \times \sqrt{-5} = -5$$

Exemple

$$\mathbb{Z}[i] \qquad i^2 = -1$$

De plus $\mathbb{Z}$ est muni de rélation d'ordre $<$.

Soient $a, b \in \mathbb{Z}$. On dit que $b < a$ si $a - b = a + (-b) \in \mathbb{N} \setminus \{0\}$.

On dit $b \leq a$ si $b < a$ ou $b = a$.

La rélation $\leq$ sur $\mathbb{Z}$ satisfait :

$<_0$ $\forall a \in \mathbb{Z}$, $a \leq a$

$<_1$ $\forall a, b \in \mathbb{Z}$, $a \leq b$ ou $b \leq a$

$<_2$ $\forall a, b \in \mathbb{Z}$, $a \leq b$ et $b \leq a \Rightarrow a = b$ (antisymétrique)

$<_3$ $\forall a, b, c \in \mathbb{Z}$, $a \leq b$ et $b \leq c \Rightarrow a \leq c$ (transitive)

La rélation $\leq$ est compatible avec $+$ et $\times$

$<_4$ $a \leq b \Rightarrow a + c \leq b + c$

$<_5$ $a \leq b$ et $c \geqslant 0 \Rightarrow a \times c \leqslant b \times c$

$<_6$ $a < 0$ et $b < 0 \Rightarrow a \times b > 0$

Preuve de $<_6$:

$0 + (-a) \in \mathbb{N} \setminus \{0\}$, $0 + (-b) = -b \in \mathbb{N} \setminus \{0\}$,

$\mathbb{N} \setminus \{0\}$

$(-a) \times (-b) = ((-1) \times a) \times ((-1) \times b) =$

$= (-1) \times (a \times ((-1) \times b)) = (-1) \times ((a \times (-1)) \times b) =$

$= (-1) \times ((-1) \times a) \times b) = ((-1) \times ((-1) \times a)) \times b =$

$= (((-1) \times (-1)) \times a) \times b \overset{\mathbb{Z}_3}{=} (1 \times a) \times b = a \times b \in \mathbb{N} \setminus \{0\}$ $a, b > 0$

Définition. Soit $X \subset \mathbb{Z}$ un sous-ensemble non vide de $\mathbb{Z}$. On dit que X est majoré (resp. minoré) s'il existe $a \in \mathbb{Z}$, tel que $\forall x \in X$, $x \leq a$ (resp. $x \geq a$).

Définition. Soit $X \subset \mathbb{Z}$ un sous-ensemble non vide de $\mathbb{Z}$. On dit que $a \in X$ est un élément plus grand (resp. plus petit) de X si $\forall x \in X$, $x \leq a$ (resp $a \leq x$).

Théorème. Soit $X \subset \mathbb{Z}$ un sous-ensemble non vide. Si X est majoré (resp. minoré) alors X possède un élément plus grand (resp. plus petit).

Preuve. $X \subset \mathbb{Z}$, $X \neq \emptyset$ et X est majoré. Donc $\exists\, a \in \mathbb{Z}$, $\forall x \in X$ $x \leq a$.

Supposons que X n'admet pas un élément plus grand.

$X \neq \emptyset \Rightarrow \exists\, x_0 \in X$.

$\mathbb{X}$ n'admet pas un élément plus grand

donc $\exists\ x_1 \in \mathbb{X}\ ,\ x_0 < x_1$.

x_1 n'est pas un élément plus grand de $\mathbb{X}$

donc $\exists\ x_2 \in \mathbb{X}\ ,\ x_1 < x_2$.

$\vdots$

$\exists\ x_n \in \mathbb{X}\ ,\ x_{n-1} < x_n$

$\vdots$

Mais x_m avec $m = a+1-x_0$ satisfait

$x_m > a$ et $x_m \in \mathbb{X}$, donc

$x_m \leqslant a$. Mais c'est absurde

Donc $\mathbb{X}$ possède un élément plus grand, cet élément est unique.

Comment on définit $\mathbb{Z}$?

Relations d'équivalence

Définition. Une relation dans un ensemble $\mathcal{X}$ est un sous ensemble $\mathcal{R}$ de $\mathcal{X} \times \mathcal{X}$.

On écrit $x \mathcal{R} x_1$ si $(x, x_1) \in \mathcal{R}$.

Définition. Soit $\mathcal{X}$ un ensemble. Une relation $\mathcal{R}$ dans $\mathcal{X}$ est une relation d'équivalence si :

1) $\forall x \in \mathcal{X}$, $x \mathcal{R} x$ (réflexivité)

2) $\forall x \in \mathcal{X}, \forall y \in \mathcal{X}$, $x \mathcal{R} y \Rightarrow y \mathcal{R} x$ (symétrie)

3) $\forall x \in \mathcal{X}, \forall y \in \mathcal{X}, \forall z \in \mathcal{X}$, $x \mathcal{R} y$ et $y \mathcal{R} z \Rightarrow x \mathcal{R} z$ (transitivité)

Exemples.

1) $<$ relation dans $\mathbb{N}$

2) $=$ relations dans $\mathbb{N}$, sous-ensemble de $\mathbb{N} \times \mathbb{N}$ correspondant est $\Delta \subset \mathbb{N} \times \mathbb{N}$, c'est une relation d'équivalence.

Déf. Soit $\mathcal{R}$ une relation d'équivalence dans $\mathbb{X}$. Soit $y \in \mathbb{X}$. L'ensemble

$$\overline{y}^{\mathcal{R}} := \{ x \in \mathbb{X} \mid y \mathcal{R} x \}$$

s'appelle classe d'équivalence de y suivant la relation $\mathcal{R}$.

Exemple. Soit $\mathcal{P}$ une relation dans $\mathbb{N}$ définie par :

$x \mathcal{P} y$ ssi x et y sont paires ou x et y sont impaires.

On voit que $\mathcal{P}$ est une relation d'équivalence dans $\mathbb{N}$. On a

$$\overline{0}^{\mathcal{P}} = \{ 0, 2, 4, \ldots, 2n \ldots \},$$

$$\overline{1}^{\mathcal{P}} = \{ 1, 3, 5, \ldots, 2n+1, \ldots \}.$$

De plus $\overline{0}^{\mathcal{P}} \cup \overline{1}^{\mathcal{P}} = \mathbb{N}$.

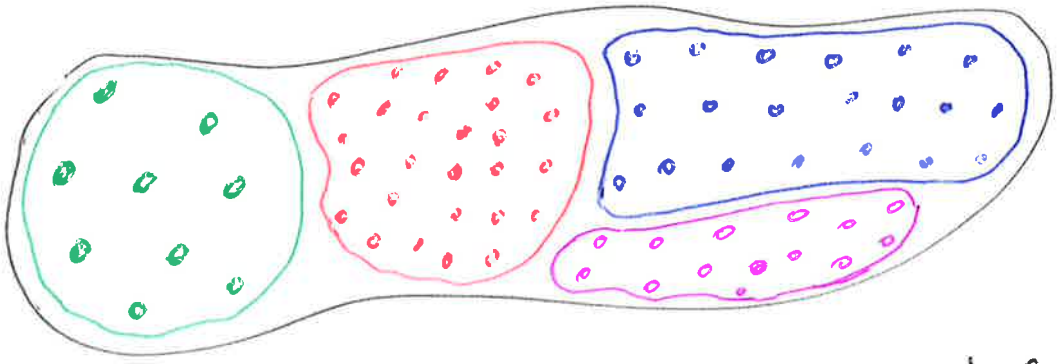
Théorème. Soit $\mathcal{R}$ une relation d'équivalence dans un ensemble $\mathbb{X}$. Alors :

i) $\forall x \in \mathbb{X}$, $x \in \bar{x}^{\mathcal{R}}$;

ii) $\forall x \in \mathbb{X}, \forall y \in \mathbb{X}$, $x \mathcal{R} y \Longleftrightarrow \bar{x}^{\mathcal{R}} = \bar{y}^{\mathcal{R}} \equiv \bar{x}^{\mathcal{R}} \cap \bar{y}^{\mathcal{R}} \neq \emptyset$;

iii) $\mathbb{X}$ = l'union disjointe de classes d'équivalence.

De plus $\bar{x}^{\mathcal{R}} \neq \bar{y}^{\mathcal{R}} \Rightarrow \bar{x}^{\mathcal{R}} \cap \bar{y}^{\mathcal{R}} = \emptyset$.



L'ensemble de classes d'équivalence suivant $\mathcal{R}$ s'appelle l'ensemble quotient de $\mathbb{X}$ par la relation $\mathcal{R}$ et on note

$$\mathbb{X}/\mathcal{R} .$$

L'application $p : \mathbb{X} \longrightarrow \mathbb{X}/\mathcal{R}$, $x \longmapsto \bar{x}^{\mathcal{R}}$ s'appelle l'application canonique de $\mathbb{X}$ dans $\mathbb{X}/\mathcal{R}$.

Si $\alpha \in \mathbb{X}/\mathcal{R}$, on appelle représentant de α, tout élément de $\mathbb{X}$ appartenant à α.

Définition de $\mathbb{Z}$

Soit $\mathcal{R}$ une relation dans l'ensemble $\mathbb{N} \times \mathbb{N}$ définie par

$(a,b)\,\mathcal{R}\,(c,d)$ si et seulement si $a+d = b+c$.

$\mathcal{R}$ est une relation d'équivalence car

i) $(a,b)\,\mathcal{R}\,(a,b)$ car $a+b = a+b$

ii) $(a,b)\,\mathcal{R}\,(c,d) \iff a+d = b+c \iff$

$c+b = d+a \iff (c,d)\,\mathcal{R}\,(a,b)$

iii) $(a,b)\,\mathcal{R}\,(c,d)$ et $(c,d)\,\mathcal{R}\,(e,f) \implies$

$a+d = b+c$ et $c+f = d+e \implies$

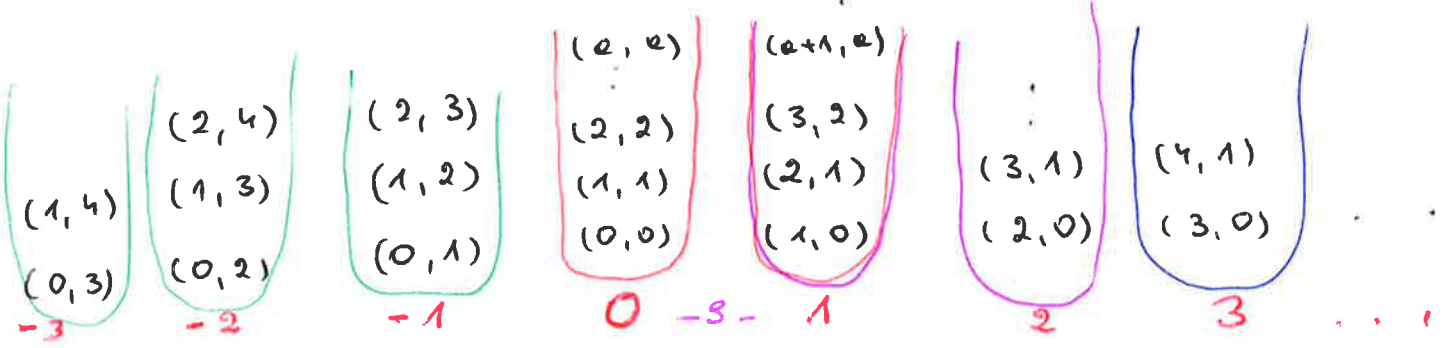
$(a+d)+(c+f) = (b+c)+(d+e) \implies$

$(a+f)+(c+d) = (b+e)+(c+d) \implies a+f = b+e$

$\implies (a,b)\,\mathcal{R}\,(e,f)$.

Définition.

$$\mathbb{Z} := \mathbb{N} \times \mathbb{N} / \mathcal{R}$$



Soient $\alpha, \beta \in \mathbb{Z}$. Soient $(a,b) \in \alpha$ ($a-b$) et $(c,d) \in \beta$. ($c-d$) On définit

$$\alpha + \beta := \overline{(a+c, b+d)}^{\mathcal{R}} \qquad (a+c)-(b+d)$$

$$\alpha \times \beta := \overline{(ac+bd, ad+bc)}^{\mathcal{R}}$$

$\alpha < \beta$ si $a+d < c+b$ dans $\mathbb{N}$.

Mais si $(a_1, b_1) \in \alpha$ et $(c_1, d_1) \in \beta$ est-ce que

$$\overline{(a_1+c_1, b_1+d_1)}^{\mathcal{R}} = \overline{(a+c, b+d)}^{\mathcal{R}} ?$$

Si $(a,b) \in \alpha$ et $(a_1, b_1) \in \alpha$ alors $(a,b) \mathcal{R} (a_1, b_1)$. Donc

$$\left.\begin{aligned} a + b_1 &= a_1 + b. \\ \text{De même} \quad c + d_1 &= c_1 + d. \end{aligned}\right\} \Longrightarrow \text{(implique)}$$

$$(a+c) + (b_1+d_1) = (a_1+c_1) + (b+d)$$

$\Rightarrow$

$$(a+c, b+d) \mathcal{R} (a_1+c_1, b_1+d_1)$$

$$\Rightarrow \quad \overline{(a+c,\, b+d)}^{\mathcal{R}} = \overline{(a_1+c_1,\, b_1+d_1)}^{\mathcal{R}}.$$

On doit vérifier le même pour $\times$ et $<$.

De plus on vérifier les postulats $*_1 - *_4$ et $*_1 - *_5$ de la page $\mathbb{Z}_1$ et la compatibilité de $<$ avec les operations $+$ et $\times$ de la page $\mathbb{Z}_3$.

Vérifions $+_3$.

$$0 := \overline{(0,0)}^{\mathcal{R}} = \overline{(n,n)}^{\mathcal{R}}$$

$$\alpha + 0 = \overline{(a,b)}^{\mathcal{R}} + \overline{(0,0)}^{\mathcal{R}} =$$

$$= \overline{(a+0,\, 0+b)}^{\mathcal{R}} = \overline{(a,b)}^{\mathcal{R}} = \alpha.$$

D'où viens la définition de la multiplication $\times$ dans $\mathbb{Z}$?

$$\overline{(a,b)}^{\mathcal{R}} \times \overline{(c,d)}^{\mathcal{R}}$$

$$(a-b)(c-d) = ac + bd - ad - bc$$

Donc $\overline{(ac+bd,\, ad+bc)}^{\mathcal{R}}$.

Notons que l'ensemble des classes

$$\left\{ \overline{(a+n,a)}^{\mathcal{R}} \mid n \in \mathbb{N} \right\}$$

nous identifions avec l'ensemble de nombres naturels $\mathbb{N}$.

$\mathbb{Q}$

Définition. On appelle corps un ensemble K muni de deux lois de composition : une addition

$$+ : K \times K \longrightarrow K$$

et une multiplication

$$\times \text{ (notée aussi } \cdot \text{ ou)} : K \times K \longrightarrow K$$

et muni de deux éléments, 0 et 1 distingués tels que

$+_1$ $\quad a + b = b + a$,

$+_2$ $\quad a + (b + c) = (a + b) + c$,

$+_3$ $\quad a + 0 = a$,

$+_4$ $\quad \forall a \in K \ \exists x \in K, \ a + x = 0$ (on montre que tel x est unique et on note $x = -a$)

(Un ensemble qui satisfait $+_1, +_2, +_3, +_4$ s'appelle un groupe commutatif)

x_1 $\quad a \times b = b \times a$

x_2 $\quad a \times (b \times c) = (a \times b) \times c$

x_3 $\quad a \times 1 = a$

x_4 $\forall\, a \in K \setminus \{0\}\ \exists\, y \in K \setminus \{0\}$ (noté a^{-1} ou $\frac{1}{a}$) t. q. $a \cdot y = 1$,

c'est-à-dire $K \setminus \{0\}$ muni de $\times$ (lois) et de 1 est un groupe commutatif,

(d) $\quad a \times (b + c) = a \times b + a \times c$

Donc $\mathbb{Q}$ – l'ensemble de nombres rationnels – est un corps.

Définition. Soit K un corps. Si K est muni d'une relation $<$ telle que

i) $\forall\, (a, b) \in K^2$, exactement une de propositions

$$a < b,$$

$$a = b,$$

$$b < a$$

est vraie.

ii) la relation $<$ est transitive

iii) $a < b \Rightarrow a + c < b + c$

et

$a < b$ et $0 < c \Rightarrow ac < bc$.

alors on dit que K est un

corps ordonné.

$\mathbb{Q}$ est un corps ordonné.

NON $\exists x \in \mathbb{Z}$, $0 < x < 1$ $\mathbb{Z}$

$$\frac{a}{b} < \frac{c}{d} \Rightarrow \frac{a}{b} < \frac{1}{2}\left(\frac{a}{b} + \frac{c}{d}\right) < \frac{c}{d}$$

entre deux nombres rationnels on trouve toujours un troisième, une infinité des nombres rationnels.

Si $q \in \mathbb{Q}$ alors $\forall n \in \mathbb{N}$

pour TD, après 2 déc.

$\exists x \in \mathbb{Q}$, $q < x$ et $0 < x - q < \frac{1}{n}$

Définition. Soit K un corps ordonné.
On dit que K est **Archimédien**
si $\forall a \in K, \forall b \in K, 0 < a$ et $0 < b$
$\Rightarrow \exists n \in \mathbb{N}, b < \underbrace{a + a + \quad + a}_{n \text{ fois}}$.

Théorème. $\mathbb{Q}$ est un corps ordonné Archimédien

Preuve.

Soient $a, b \in \mathbb{Q}$, $a > 0$ et $b > 0$.

$a = \frac{p}{q}$ et $b = \frac{r}{s}$ $p, q, r, s \in \mathbb{N} - \{0\}$.

Soit $n := q \cdot r$. $n \in \mathbb{N}$ et

$$\underbrace{a + \quad + a}_{n \text{ fois}} + a = n \cdot a = q \cdot r \cdot \frac{p}{q} = r \cdot p > r > \frac{r}{s}.$$

Définition. Soit K un corps ordonné.
La fonction

$$| \ | : K \longrightarrow K$$

définie par

$$|x| := \begin{cases} \\ \end{cases} := \max\{x, -x\}$$

s'appelle valeur absolut de x.

Proposition. Soit K un corps ordonné. Alors

$$|x+y| \leq |x|+|y|,$$

$$|x| = 0 \quad \text{ssi} \quad x = 0,$$

$$x \leq |x| \quad \text{et} \quad -x \leq |x|,$$

$$||x|-|y|| \leq |\,|x|-|y|\,| \leq |x+y|$$

$$|x \cdot y| \leq |x| \cdot |y|$$

Preuve :

$$x \leq |x| \quad \text{et} \quad y \leq |y|$$

$$x+y \leq |x|+y \leq |x|+|y| \quad \Rightarrow \quad x+y \leq |x|+|y|$$

(iii) (iii) (ii) transitivité

De même

$$\underbrace{(-x)+(-y)}_{-(x+y)} \leq |x|+|y|$$

Donc

$$x+y \leq |x|+|y| \quad \Rightarrow |x+y| \leq |x|+|y|.$$

et

$$-(x+y) \leq |x|+|y|$$

Notation: Si K un corps, on note

$$K^\times := K \setminus \{0\}$$

Construction de $\mathbb{Q}$

Soit $\mathcal{R}$ relation dans $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ définie par

$$(a, b)\ \mathcal{R}\ (c, d) \quad \text{ssi} \quad ad = bc \quad \text{dans } \mathbb{Z}.$$

On montre que $\mathcal{R}$ est une relation d'équivalence. On définie

$$\mathbb{Q} := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \,/\, \mathcal{R}$$

$$\overline{(a, b)}^{\mathcal{R}} \longleftrightarrow \frac{a}{b}$$

$$\overline{(a, b)}^{\mathcal{R}} \times \overline{(c, d)}^{\mathcal{R}} := \overline{(ac, bd)}^{\mathcal{R}}$$

$$\overline{(a, b)}^{\mathcal{R}} + \overline{(c, d)}^{\mathcal{R}} := \overline{(ad + bc, bd)}^{\mathcal{R}}$$

$$\overline{(a, b)}^{\mathcal{R}} > \overline{(0, 1)}^{\mathcal{R}} \quad \text{si} \quad a \cdot b > 0 \quad \text{dans } \mathbb{Z}.$$

$\alpha, \beta \in \mathbb{Q}$, $\alpha > \beta$ si $\alpha - \beta > 0$ dans $\mathbb{Q}$.

$\overline{(n,1)}^{\mathcal{R}}$ on identifie avec $n \in \mathbb{Z}$.

Théorème. L'ensemble $\mathbb{Q} := \mathbb{Z} \times (\mathbb{Z} - \{0\}) / \mathcal{R}$

muni des lois $+$ et $\times$ et des

$0 := \overline{(0,1)}^{\mathcal{R}}$, $1 := \overline{(1,1)}^{\mathcal{R}}$ et de la

relation $>$ est un corps ordonné

Archimédien.

C'est le $\mathbb{Q}$ que on

connait. $\overline{(a,b)}^{\mathcal{R}} \dashrightarrow \frac{a}{b}$