

Nombres et structures

Mathématiques tout-en-un MPSE/PESI
par des champs et Voruzfeld

Prof: jacques.guolino@spei.fr
@mta.org

- I- Logique et ensembles
- II- Corps et complexes
- III- Polynômes
- IV- Structures
- V- Applications et relations
- VI- Dénombrabilité
- VII- Arithmétique

Chapitre I: Logique et ensembles

1.1) Assertion

- Une assertion est un énoncé de dépendant pas de valeurs de variables.

ex. $A: 2+2=4$ A est vrai / On a A

↓

Variable logique A est vraie V ou $A=1$
 A est fausse $\bar{V}$ ou $A=0$

B: Tous les élèves de l'EFREI ont la base.
 B est vraie.

Soit $E = \{ e_i ; \text{ où } e_i \text{ est un élève de l'EPHEI} ; i \in [1;10] \}$

$\text{Bach} = \{ \text{bacheliers} \}$

B. $\forall e_i \in E, e_i \in \text{Bach}$

Connecteurs : opérateurs sur les assertions

- négation : $A \rightarrow \text{non } A = \bar{A}$
ex: $\bar{B}$: $\exists e_i \in E : e_i \notin \text{Bach}$

→

généralisation : $\overline{\forall x \in A, P} = \exists x \in A, \bar{P}$

- conjonction : $E \text{ ET } A$

ex: $A \wedge B$ est vrai si A est vraie ET B est vrai

- disjonction : $O \vee U$

ex: $A \vee B$ est vrai si A ou B est vrai

- implication : $\Rightarrow$

ex: $A \Rightarrow B$ est vrai si $\begin{cases} A \text{ vrai alors } B \text{ est vrai} \\ A \text{ est faux} \end{cases}$

→

$$\overline{A \Rightarrow B} = A \cdot \bar{B}$$

- équivalence : $\Leftrightarrow$

ex: $A \Leftrightarrow B$ si $\begin{cases} A = V \Rightarrow B = V \\ A = F \Rightarrow B = F \end{cases}$

ex: C: tout élève de l'éfrei est beau et intelligent

$\bar{C}$: Il existe au moins un élève de l'éfrei qui soit pas beau ou pas intelligent

↳ C: $\forall e \in E, e \in \text{Beau} \text{ et } e \in \text{Intel}$
 $\bar{C}$: $\exists e \in E \mid \underbrace{e \notin \text{Beau}}_{e \in \text{laide}} \text{ ou } \underbrace{e \notin \text{Intel}}_{e \in \text{bête}}$

1.2) Table de vérité

→ Au des

A	B	A+B	$\bar{B}$	A.B	$\overline{A+B}$	A.B	$\overline{A+B}$	A.B	$\bar{A}$	$\bar{A}+\bar{B}$	A+B	$\bar{A}+\bar{B}$	$\bar{A}+\bar{B}$	$\bar{A}+\bar{B}$	$\bar{A}+\bar{B}$
1	1	1	0	0	0	1	1	0	0	0	1	0	0	1	1
1	0	0	1	1	0	1	0	1	0	1	1	0	0	0	0
0	1	1	0	0	0	1	0	1	1	1	1	0	0	1	1
0	0	1	1	0	0	1	0	1	1	1	0	1	1	1	1

$\uparrow \uparrow$ $\uparrow \uparrow$

$$\overline{A \Rightarrow B} = A \cdot \bar{B}$$

$$\bar{B} \cdot \bar{B} = 0 \quad \leftarrow \text{principe de Non Contradiction}$$

$$\bar{B} + \bar{B} = 1 \quad \leftarrow \text{principe du tiers exclus}$$

$$\rightarrow \begin{cases} \frac{A \cdot B}{A+B} = \frac{A+B}{A \cdot B} \quad \leftarrow \text{lois de De Morgan} \end{cases}$$

$$(A \Rightarrow B) \Leftrightarrow (\bar{B} \Rightarrow \bar{A}) \quad \leftarrow \text{Contraposée de } A \Rightarrow B$$

$$(A \Rightarrow B) \Leftrightarrow (\bar{A} + B)$$

A	B	F	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮
			$A \wedge B$	$A \vee B$	$A \setminus B$	$B \setminus A$	B	XOR	$A \vee B$	NOR	$A \supset B$	$\overline{B}$	$B \supset A$	$\overline{A}$	$A \supset B$	$NAND$	
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1

On montrerait de même :

$$\left. \begin{aligned} (A \wedge B) \wedge C &= A \wedge (B \wedge C) \\ (A \vee B) \vee C &= A \vee (B \vee C) \end{aligned} \right\} \text{associativité}$$

$$\left. \begin{aligned} A \wedge (B \vee C) &= (A \wedge B) \vee (A \wedge C) \\ A \vee (B \wedge C) &= (A \vee B) \wedge (A \vee C) \end{aligned} \right\} \text{distributivité}$$

$$\left. \begin{aligned} A + A &= A \\ A \cdot A &= A \end{aligned} \right\} \text{idempotence}$$

$$\overline{\overline{A}} = A$$

$$\left. \begin{aligned} A + 0 &= A \\ A \cdot 1 &= A \\ A + 0 &= 0 \\ A + 1 &= 1 \end{aligned} \right\} \text{éléments neutres}$$

$$A + AB = A \quad \left. \begin{aligned} & \text{absorption} \end{aligned} \right\}$$

$$\begin{aligned} A + \bar{A}B &= A + B \quad \left. \begin{aligned} & \text{simplification} \end{aligned} \right\} \text{car } A + \bar{A}B = A + AB + \bar{A}B \\ &= A + (A + \bar{A}) \cdot B \\ &= A + 1 \cdot B \\ &= A + B \end{aligned}$$

noc

tautologie : assertion toujours vraie

1.3) Prédicat

- Un prédicat est une énoncé contenant une variable qui est V ou F selon les valeurs de la variable

ex: $x \in \mathbb{R}, x > 3$ est vrai ou faux selon x .

ex 2: le réel x est un entier impair : $P(x)$
est "presque toujours" faux

- Soit un prédicat $P(x)$.
si $\exists x \in E$ tq $\forall x \in E, P(x)$ est vrai
on dit que $P(x)$ est une propriété collectivisante

quantificateurs :

- $\forall$: quel que soit
- $\exists$: il existe
- $\exists!$: il existe 1 et 1 seul.

$$\forall x \in E, A(x) = \exists x \in E | \bar{A}(x) \quad \leftarrow \text{tautologie}$$

$$\exists x \in E | \bar{A}(x) = \forall x \in E, \bar{A}(x)$$

$$\forall x \in E, P(x) \Rightarrow Q(x) = \exists x \in E | P(x) \wedge \bar{Q}(x)$$

1.4) Ensembles

- Un ensemble est formé d'éléments ayant une propriété collectivisante.

Soit E un ensemble : $e \in E$
 $e \notin E$

• égalité de 2 ensembles:

$$A=B \text{ si } \forall a \in A, a \in B \text{ et } \forall b \in B, b \in A$$

• inclusion

$$A \subset B \text{ si } \forall a \in A, a \in B$$

A est une partie de B.

$$\text{Partie de } E: P(E) = \{\text{parties de } E\} = \{A \mid A \subset E\}$$

→ l'inclusion est

- transitive: $A \subset B \text{ et } B \subset C \Rightarrow A \subset C$
- réflexive: $A \subset A$
- antisymétrique: $A \subset B \text{ et } B \subset A \Rightarrow A = B$

→ l'inclusion est une relation d'ordre

• ensemble vide: ensemble n'ayant aucun élément
il est noté $\emptyset$

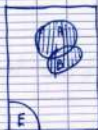
$$\forall E, \emptyset \subset E$$

$$\text{ex: } \{x \in \mathbb{N} : x+1=0\} = \emptyset$$

$$P(E) \neq \emptyset \text{ car } \emptyset \in P(E)$$

ex: supposons que x est le seul élément de E
dans $P(E)$ a 2 éléments: $\emptyset; E = \{x\}$
si $E = \{x\}$ dans E est un singleton.

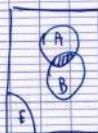
1.5) Opérations sur les ensembles



• réunion de A et B $= A \cup B$
 $= \{x \in E \text{ tq } x \in A \text{ ou } x \in B\}$
non exclusif

$\rightarrow A \cup A = A$

$\rightarrow A \cup B = A \Leftrightarrow B \subset A$



• intersection : $A \cap B = \{x \in E\}$
 $= \{x \in A \text{ et } x \in B\}$

$\rightarrow A \cap A = A$

$\rightarrow A \cap B = B \Leftrightarrow B \subset A$



• complémentarité

Sont A et B $\in P(E)$

A et B sont complémentaires dans E

ssi $(A \cup B = E \text{ et } A \cap B = \emptyset)$

on le note $B = \bigcup_E A = \bar{A} = E \setminus A$
si E évident

$\rightarrow \bigcup_E (\bigcap_E A) = A \quad \bar{\bar{A}} = A$

$\rightarrow$ toute propriété sur les variables logiques munies des opérations ou, et, $\Rightarrow$ est identique sur des ensembles munies de $\cup, \cap, \bar{}$.

ex. $A \cap B = B \cap A$ de m $\bar{A \cap B} = \bar{A} \cup \bar{B}$
 $\bar{A \cup B} = \bar{A} \cap \bar{B}$

$$\rightarrow A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$



• Produit (cartésien) d'ensemble
noté $A \cdot B$

$$A \cdot B = \{(a; b) \mid a \in A, b \in B\}$$

$$\rightarrow A \cdot B \neq B \cdot A$$

$$\rightarrow A^2 = A \cdot A$$



$$F \cap G = L$$

$$F \cap G = \emptyset$$

$$F = \overline{G}$$

1.6) Ensembles usuels

$$\mathbb{N} = \{0; 1; 2; \dots; m; \dots\} \quad \text{entiers naturels}$$

$$\mathbb{F}_2 = \{0; 1\} \quad \text{corps fermé à 2 éléments}$$

$$\mathbb{N}^* = \{1; 2; \dots; m; \infty\} \quad \text{entiers positifs}$$

$$\mathbb{Z} = \{-m; \dots; -1; 0; 1; \dots; m; \dots\} \quad \text{entiers relatifs}$$

$$\mathbb{N}_m = \{0; 1; \dots; m\} \quad \text{et} \quad \mathbb{N}_m^* = \{1; 2; \dots; m\}$$

$\mathbb{Q}$ = "rationnels" = $\{p/q \text{ où } p \in \mathbb{Z} \text{ et } q \in \mathbb{N}^*\}$

$\mathbb{R}$ = "réels" = ??

mq $\exists$ réels non rationnels

prenons z rationnel $z = \frac{p}{q}$

22 | 7

10 | 3,142857142857...

20 | 60

développement décimal périodique
de période 6.

Soit $m = 0,101001000100001$

développement non périodique

donc $\mathbb{R} \setminus \mathbb{Q} \neq \emptyset$

1.7) Cardinal et ensembles finis

E est un ensemble fini $\exists m \in \mathbb{N}$ tq $E = \{e_1, \dots, e_m\}$

m est le cardinal de E $m = \text{card } E$

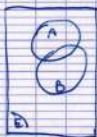
ex: $\text{card}(A \cup B) \leq \text{card } A + \text{card } B$

$\text{card}(A \cap B) \leq \min(\text{card } A, \text{card } B)$

$\text{card}(A \cdot B) = \text{card } A \cdot \text{card } B$

$\rightarrow \text{card}(A^m) = (\text{card } A)^m$

→



$$\text{card}(A \cup B) = \text{card } A + \text{card } B - \text{card}(A \cap B)$$



$$\begin{aligned} \text{card}(A \cup B \cup C) &= \text{card}(A \cup (B \cup C)) \\ &= \text{card } A + \text{card}(B \cup C) - \text{card}(A \cap (B \cup C)) \\ &= \text{card } A + \text{card } B + \text{card } C \\ &\quad - \text{card}((A \cap B) \cup \text{card}(A \cap C)) + \text{card } C \\ &= \text{card } A + \text{card } B + \text{card } C - \text{card}(B \cap C) \\ &\quad - \text{card}(A \cap C) + \text{card}((A \cap B) \cap (A \cap C)) \end{aligned}$$

→

$$\rightarrow \text{card } P(E) = 2^{\text{card } E}$$

car $\text{card } \emptyset = 0$ donc $\text{card } P(\emptyset) = 1$

si $\text{card } E_1 = 1$ $E_1 = \{e_1\}$ $P(E) = \{\emptyset, \{e_1\}\}$ $\text{card } P(E) = 2$

démonstration:

$$E_m = \{e_1, e_2, \dots, e_m\} \quad \text{card } P(E_m) = ?$$

n	E_m	$P(E_m)$	$\text{card}(P(E_m))$
0	$\emptyset$	$\emptyset$	1
1	$\{e_1\}$	$\emptyset, \{e_1\}$	2
2	$\{e_1, e_2\}$	$\emptyset, \{e_1\}, \{e_2\}, \{e_1, e_2\}$	4
3	$\{e_1, e_2, e_3\}$	$\emptyset$	8

Hyp H_m : $\text{card } P(E_m) = 2^m$

H_0 est vraie

Supposons H_m vraie

alors $\text{card } P(E_{m+1}) = 2 \times \text{card } P(E_m) = 2 \times 2^m = 2^{m+1}$

L'hypothèse est héréditaire, vraie pour $m=0$,
donc toujours vraie $\forall m \in \mathbb{N}$

1.8) Autres opérations

La différence symétrique



$$\begin{aligned} A \Delta B &= D = (A \setminus B) \cup (B \setminus A) \\ &= A \cdot \overline{B} \cup \overline{A} \cdot B \end{aligned}$$

Le Recouvrement et Partition



Soit la famille des X_i : $\{X_i; i \in I \subset \mathbb{N}\}$
cette famille est un recouvrement
de E si $\bigcup_{i \in I} X_i = X_1 \cup X_2 \cup \dots \cup X_m$
 $= E$

Un recouvrement est une partition si tous les
éléments sont disjoints:

$\{X_i\}_{i \in I}$ est une partition de E si $\begin{cases} \bigcup_{i \in I} X_i = E \\ X_i \cap X_j = \emptyset \quad \forall (i, j) \in I^2, i \neq j \end{cases}$

Chapitre II : Nombres complexes

2.1) Définitions

→ $\{\mathbb{R}, +, \cdot\}$ est le corps des réels

→ $\mathbb{C}$ est l'ensemble des nombres complexes
égal à $\{(a; b) \in \mathbb{R}^2\}$ avec

- une loi d'addition notée $+$ telle que

$$\forall z_1, \forall z_2 \in \mathbb{C} \quad z_1 + z_2 = (a_1 + a_2; b_1 + b_2)$$

vérifiant :

- L.C.I. , loi de composition interne

- associative: $(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$

- $\exists$ élément neutre $0 = (0; 0)$

$$\forall z \quad z + 0 = 0 + z = z$$

- $\forall z \in \mathbb{C}, \exists$ symétrique de z noté $-z$

$$\forall z \quad z + (-z) = -z + z = 0$$

$$\text{donc } -(a; b) = (-a; -b)$$

- commutativité: $z_1 + z_2 = z_2 + z_1$

→ Alors $\{\mathbb{C}, +\}$ est un groupe abélien

- une loi de multiplication notée $\times$ ou $\cdot$

$$z \cdot z' = (a; b)(a'; b') = (aa' - bb'; ab' + a'b)$$

$\forall z$:

- L.C.I.

- associative: $z_1 \times (z_2 \times z_3) = (z_1 \times z_2) \times z_3$

- $\exists$ neutre noté $1 = (1; 0)$

$$\text{car } (a; b)(1; 0) = (a \cdot 1 - b \cdot 0; a \cdot 0 + b \cdot 1) \\ = (a; b)$$

• $\forall z \neq 0$, z a un inverse noté $z^{-1} = \frac{1}{z}$
 car $z \cdot \frac{1}{z}$ tq $z \cdot z^{-1} = 1$

$$\text{car } z = (a; b) \quad z^{-1} = \left(\frac{a}{a^2+b^2} ; \frac{b}{a^2+b^2} \right)$$

$$z \cdot z^{-1} = \left(\frac{a \cdot a}{a^2+b^2} - \frac{b \cdot b}{a^2+b^2} ; \frac{-ab}{a^2+b^2} + \frac{ab}{a^2+b^2} \right) = 1$$

car $a^2+b^2 \neq 0 \Rightarrow a=b=0 \Rightarrow z=0$

$\rightarrow$ On dit que $(\mathbb{C}, +, \cdot)$ est un corps

De plus $z_1 \cdot z_2 = z_2 \cdot z_1$

↳ ce corps est commutatif

Soit -1 le symétrique de 1
 $-1 = (-1; 0)$

Soit $(0; 1) = i$

donc $i^2 = (0; 1) \cdot (0; 1) = (-1; 0) = -1$

donc $\boxed{i^2 = -1}$

- Soit le produit externe $\star$ tq

$$\forall \lambda \in \mathbb{R} ; \forall z = (a; b) \in \mathbb{C}$$

$$\lambda \star (a; b) = (\lambda \cdot a ; \lambda \cdot b)$$

donc $z(0; b) = (a; 0) + (0; b)$

soit $z = a \star 1 + b \star i$

On note $a \star 1$ par a
 et $b \star i$ par $i \cdot b$

donc z s'écrit $z = a + i b$

donc $\mathbb{C} = \{z = a + i b \text{ tq } a \in \mathbb{R}, b \in \mathbb{R}; i^2 = -1\}$

2.2) Représentation algébrique des nombres complexes

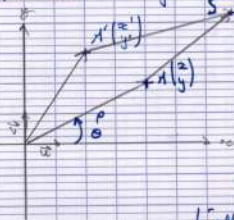
- $a + ib$ est la représentation algébrique de $z \in \mathbb{C}$

avec $z_1 + z_2 = (a_1 + ib_1) + i(b_2 + ib_2)$
 $0 + z = z + 0 = z$
 $-z = -a + ib$
 et associativité

- partie réelle de $z = \operatorname{Re}(z) = a$
- partie imaginaire de $z = \operatorname{Im}(z) = b$
- conjugué de $z = \bar{z} = a - ib$

$\rightarrow z + \bar{z} = 2\operatorname{Re}(z)$
 $\rightarrow z - \bar{z} = 2i\operatorname{Im}(z)$
 $\rightarrow z = \bar{z} \Leftrightarrow z \in \mathbb{R}$
 $\rightarrow a + ib = \bar{a} + i\bar{b} \Leftrightarrow \begin{cases} a = \bar{a} \\ b = \bar{b} \end{cases}$
 $\rightarrow z = 0 \Leftrightarrow a = b = 0$
 $\rightarrow \overline{z + z'} = \bar{z} + \bar{z'}$
 $\rightarrow \overline{z \cdot z'} = \bar{z} \cdot \bar{z'}$
 $\rightarrow \overline{\bar{z}} = z$ ("la combinaison est involutive")

2.3) Représentation trigonométrique



Le plan $(Ox; Oy)$ est le plan complexe où $M(\vec{x})$ apparait affixe $z = x + iy$

Soit stq $\vec{OS} = \vec{OA} + \vec{OB}$
 $\vec{OS} = \vec{OA}$

L'affixe de S est $z = x + iy$

$$\rho = \text{module de } z' = \sqrt{x^2 + y^2} = OM = |z|$$

$$\theta = \text{argument de } z' = \text{angle}(\vec{Ox}; \vec{OM}) \text{ à } 2\pi \text{ près}$$

$$\rightarrow |\bar{z}| = |z| = |-z|$$

$$\rightarrow z^{-1} = \frac{1}{z}$$

$$\rightarrow |z|^2 = z\bar{z}$$

$$\rightarrow z^2 + y^2 \leq z^2 + y^2 + 2|z||y| = (|z| + |y|)^2$$

$$|z|^2 = (|z| + |y|)^2$$

$$|z| = |z| + |y|$$

$$\rightarrow |z| = 0 \Leftrightarrow z = 0$$

$$\begin{aligned} \rightarrow |z \cdot z'| &= \sqrt{zz' \cdot \bar{z}\bar{z}'} = \sqrt{z\bar{z} \cdot z'\bar{z}'} = \sqrt{|z|^2 \cdot |z'|^2} \\ &= |z| \cdot |z'| \end{aligned}$$

$$\rightarrow \text{inégalité triangulaire } |z \cdot z'| \leq |z| + |z'|$$

$$\rightarrow z = x + iy = \rho \left(\frac{x}{\rho} + i \frac{y}{\rho} \right) \quad \cos \theta = \frac{\operatorname{Re}(z)}{|z|} \quad \sin \theta = \frac{\operatorname{Im}(z)}{|z|}$$

$$\cos^2 \theta + \sin^2 \theta = 1$$

$$\text{Puisque } e^{i\theta} = \cos \theta + i \sin \theta \text{ donc } e^{i\pi} = -1$$

$$\text{On a } z = \rho e^{i\theta} = \text{"représentation trigonométrique"} = [\rho; \theta]$$

$$\rightarrow \bar{z} = [\rho; -\theta] \quad -z = [\rho; \theta + \pi]$$

2.4) Exponentielle complexe

$$e^{i\theta} = \cos \theta + i \sin \theta \quad e^{i\alpha} + e^{i\beta} = e^{i(\alpha+\beta)}$$

$$e^{i2\theta} = (e^{i\theta})^2 \quad \text{donc} \quad e^{in\theta} = (e^{i\theta})^n$$

→ $\cos n\theta + i \sin n\theta = (\cos \theta + i \sin \theta)^n$ Formule de Moivre

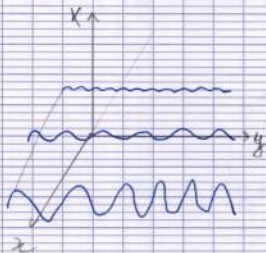
→ $\cos \theta = \frac{e^{i\theta} + e^{-i\theta}}{2}$ Formules d'Euler

$$\sin \theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}$$

généralisation: $Z = X + iY = e^{\theta} = e^{x+iy} = e^x (\cos y + i \sin y)$

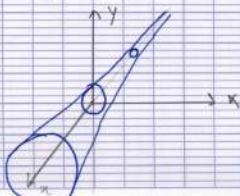
$X + iY = e^x (\cos y + i \sin y)$ graphique à 3D dans $\mathbb{R}^4$

Projections sur (OX, OX, OY) :



$$X = e^x \cos y$$

Projections sur (OX, OY, OZ) :



$$X = e^x \cos y$$

$$Y = e^x \sin y$$

$$X^2 + Y^2 = e^{2x}$$

Fonctions hyperboliques

$$\cos x = \frac{e^{ix} + e^{-ix}}{2}$$

$$\sin x = \frac{e^{ix} - e^{-ix}}{2}$$

$$\cosh x = \frac{e^x + e^{-x}}{2}$$

$$\sinh x = \frac{e^x - e^{-x}}{2}$$

$$\tan x = \frac{\sin x}{\cos x}$$

$$\tanh x = \frac{\sinh x}{\cosh x}$$

→

$$\text{On a : } \begin{aligned} \cos^2 x + \sin^2 x &= 1 \\ \cosh^2 x - \sinh^2 x &= 1 \end{aligned}$$

Généralisation:

$$\cos y = \frac{e^{iy} + e^{-iy}}{2}$$

$$\sin y = \frac{e^{iy} - e^{-iy}}{2}$$

$$\cosh y = \frac{e^y + e^{-y}}{2}$$

$$\sinh y = \frac{e^y - e^{-y}}{2}$$

$$\begin{aligned} \rightarrow \sin iy &= i \cosh y \\ \cos iy &= \cosh y \\ \sinh iy &= i \sin y \\ \cosh iy &= \cos y \end{aligned}$$

2.5) Racines $m^{\text{ièmes}}$ de nombres complexes

Pb: chercher z tq $z^m = \lambda$ où $\lambda \in \mathbb{C}$ est fixé non nul

$$\text{Posons } \lambda = r(\cos \alpha + i \sin \alpha) \\ z = \rho(\cos \theta + i \sin \theta)$$

$$\text{d'où } \rho = \sqrt[m]{r} = r^{\frac{1}{m}} \text{ et } \theta = \frac{\alpha}{m} + \frac{2k\pi}{m} \quad \forall k \in \{0, 1, \dots, m-1\}$$

L'équation a donc m racines distinctes.

Cas particulier:

$$\rightarrow \lambda = 1 : \text{racines } m^{\text{ièmes}} \text{ de l'unité} \\ z^m = 1 \quad \text{donc } z = e^{i(\frac{2k\pi}{m})} \quad k \in \{0, m-1\}$$

$$m=1 \quad z=1 \quad \text{une racine } z_1=1$$

$$m=2 \quad z^2=1 \quad z_1=-1 \quad z_2=1$$

$$m=3 \quad z^3=1 \quad z_1=1 \quad z_2=e^{\frac{2i\pi}{3}}=j \quad z_3=e^{\frac{4i\pi}{3}}=j^2 \\ j^3=1 \quad \bar{j}=j^2 \quad 1+j+j^2=\dots=0$$

$$m=4 \quad z^4=1 \quad z_k = e^{\frac{2ik\pi}{4}}$$

$$4 \text{ racines: } z_1=1 \quad z_2=i \quad z_3=-1 \quad z_4=-i$$

$$z_1+z_2+z_3+z_4=0$$

Racine carrée d'un complexe:

$$\text{Soit } \lambda = a+ib \text{ donné, on cherche } z = x+iy \text{ tq} \\ z^2 = \lambda \quad x^2 + 2ixy - y^2 = a+ib$$

$$\Leftrightarrow \begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases} \quad \text{avec } b \neq 0 \text{ donc } xy \neq 0$$

d'où $y = \frac{b}{2x}$ et $x^2 - \frac{b^2}{4x^2} = a$

soit $4x^4 - b^2 = 4ax^2$
 $4x^4 - 4ax^2 - b^2 = 0$ équation biquadratique à coefficients réels

Posons $X = 2x^2$: $X^2 - 2aX - b^2 = 0$

$\Delta = 4a^2 + 4b^2 > 0$

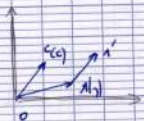
donc 2 racines X_1 positive et X_2 positive
 on ne garde que X_1 positive

d'où 2 solutions $x_1 = \sqrt{\frac{X_1}{2}}$ $x_2 = -\sqrt{\frac{X_1}{2}}$

d'où $y_1 = \frac{b}{2x_1}$ et $y_2 = \frac{b}{2x_2}$

2.6) Propriétés géométriques

* translation de vecteur $\vec{c} \rightarrow T_{\vec{c}}$



$$A \xrightarrow{T_{\vec{c}}} A' \\ \vec{AA'} = \vec{c}$$

$$z' = z + c$$

* Rotation $R(0; \alpha)$



$$z = \rho e^{i\theta}$$

$$A \xrightarrow{R(0; \alpha)} A'(z')$$

$$z' = \rho e^{i(\theta + \alpha)} \\ z' = z e^{i\alpha}$$

La rotation d'angle α correspond à la multiplication par $e^{i\alpha}$.

* Similitude de centre O , de rapport k et d'angle α



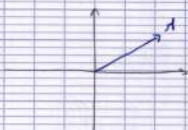
$$\vec{OA'} = k \vec{OA}$$

$$z_1 = k z'$$

$$z_1 = k z e^{i\alpha} = \lambda z$$

$$\lambda = k e^{i\alpha}$$

* Symétrie



$$A \xrightarrow{\text{Sym/O}} A_1$$

$$A \xrightarrow{\text{Sym/O}} A_2$$

$$A \xrightarrow{\text{Sym/O}} A_2$$

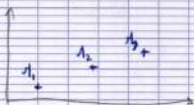
$$z_1 = \bar{z}$$

$$z_2 = -\bar{z}$$

$$z_2 = -\bar{z}$$

* Alignements

3 pts $A_1(z_1)$ $A_2(z_2)$ $A_3(z_3)$ tous distincts



alignés $\Leftrightarrow \vec{A_1A_2}$ et $\vec{A_1A_3}$ colinéaires

$$\Leftrightarrow (\vec{A_1A_2}; \vec{A_1A_3}) = 0 \text{ } [\pi]$$

$$\Leftrightarrow \arg(z_2 - z_1) = \arg(z_3 - z_1) = 0 \text{ } [\pi]$$

$$\Leftrightarrow \arg\left(\frac{z_2 - z_1}{z_3 - z_1}\right) = 0 \text{ } [\pi]$$

$$\Leftrightarrow \frac{z_2 - z_1}{z_3 - z_1} \in \mathbb{R} \Leftrightarrow A_1, A_2, A_3 \text{ alignés}$$

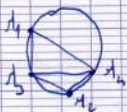
* Concyclicité



$$(\vec{A_1A_3}, \vec{A_1A_4}) = (\vec{A_2A_3}, \vec{A_2A_4})$$

$$\arg \frac{z_4 - z_1}{z_3 - z_1} = \arg \frac{z_4 - z_2}{z_3 - z_2}$$

$$\arg \left(\frac{\frac{z_4 - z_1}{z_3 - z_1}}{\frac{z_4 - z_2}{z_3 - z_2}} \right) = 0 \text{ } [\pi]$$

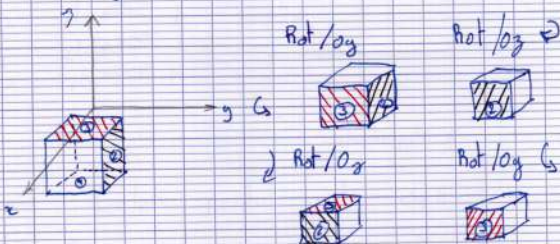


$$(\vec{A_1 A_3}, \vec{A_2 A_4}) = (\vec{A_1 A_3}, \vec{A_1 A_4}) + \pi$$

$$\arg\left(\frac{z_1 - z_3}{z_3 - z_2}\right) = \arg\left(\frac{z_3 - z_1}{z_2 - z_1}\right) + \pi$$

$$\left(\frac{z_4 - z_1}{z_3 - z_1}, \frac{z_4 - z_2}{z_3 - z_2} \right) \in \mathbb{R} \Leftrightarrow 4 \text{ points sont cocycliques}$$

2.7) Hypercomplexes



$$R/I_y \cdot R/I_x \neq R/I_y \cdot R/I_z$$

$$H = \{\text{quaternions } q\}$$

$$q = a1 + bi + cj + dk$$

•	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

H est un corps non commutatif

Chapitre III : Polynômes

3.0) Préambule : corps $F_2 = \text{corps fini à 2 éléments}$

3.1) Définition

Soit K un corps $K = \mathbb{R}$, ou $\mathbb{C}$, ou F_2

↳ addition $+$ est ou exclusif

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$\{F_2, +, \cdot\}$ est un corps abélien.

- On appelle $K[X]$ l'ensemble des polynômes $P(x)$ sur le corps K , où P est une suite presque partout nulle de coefficients appartenant à K .

$$P = (p_0; p_1; p_2; \dots; p_m; 0; \dots)$$

- polynôme nul $[0] = (0; 0; \dots; 0)$
- degré de $P = d^0 P = m$ tq $p_i = 0 \forall i > m$
- valuation de $P = v(P) = k$
tq $p_i = 0 \forall i < k$
- $d^0 [0] = -\infty$

3.2) Structure de $K[X]$

3.2.1) Addition

$$\left. \begin{array}{l} P = (p_0, p_1, \dots, p_m, 0, \dots) \\ Q = (q_0, q_1, \dots, q_m, 0, \dots) \end{array} \right\} S = P+Q = (p_0+q_0, p_1+q_1, \dots)$$
$$d^0(P+Q) \leq \sup(d^0 P, d^0 Q)$$

- $+$ est une loi :
- LCI
 - associative
 - $\exists$ neutre $[0]$
 - $\forall P = (p_0; \dots; p_n; 0 -) \exists -P = (-p_0; \dots; -p_n; 0 -)$
 $\text{t.q. } P + (-P) = 0$
 - commutative

donc $(K[X], +)$ est un groupe abélien

3.2.2) Multiplication

$$P \cdot Q = (r_0; r_1; \dots; r_i; r_2; 0 -)$$

$$r_0 = p_0 \cdot q_0$$

$$r_1 = p_0 q_1 + p_1 q_0$$

$$r_i = \sum_{k=0}^{h_i} p_k q_{i-k}$$

$$d^0(P \cdot Q) = d^0 P \cdot d^0 Q$$

cette multiplication est :

- LCI
- $\exists$ neutre $[1] = (1; 0 -)$ $d^0[1] = 0$
- $[1] \cdot P = P \quad \forall P \in K[X]$

il n'existe pas d'inverse

- multiplication est distributive : $P \cdot (Q + R) = P \cdot Q + P \cdot R$
- commutative

$(K[X], +, \cdot)$ est un anneau.

→ Cet anneau est intègre

car: $P_r = P_m \cdot Q_m = [0] \Rightarrow P = [0] \text{ ou } Q = [0]$

$r_p = P_m \cdot q_m$ n'est nul que si $p_m = 0$ ou $q_m = 0$
si K est intègre.

3.2.3) Multiplication de P par un scalaire λ

• Soit $\lambda \in K$, $P = (p_0, \dots, p_m; 0-)$

$\lambda \cdot P = (\lambda p_0, \dots, \lambda p_m; 0-)$

Avec cette multiplication $\{K[X], +, *\}$ est un K -espace vectoriel.

3.2.4) Notation polynomiale

$[1] = (1; 0, \dots; 0-) = x^0$

$(0, 1; 0, \dots; 0-) = x^1$

$(0, 0, 1; 0, \dots; 0-) = x^2$

$(0, 0, \dots, 0, 1; 0-) = x^m$ où $0 \leq m < \infty$

$P(x) = (p_0, p_1, p_2, \dots; p_m; 0-)$

$= p_0 x^0 + p_1 x^1 + \dots + p_m x^m$

il existe la fonction polynome $p(z) = p_0 + p_1 z + \dots + p_m z^m$

exemples : $P_1 = X^3 + X^2 + 1$
 $P_2 = X^3 + X + 1$

Addition: dans $B[X]$

$$P_1 + P_2 = 2X^3 + X^2 + X + 2$$

$$P_1 \cdot P_2 = (X^3 + X^2 + 1)(X^3 + X + 1) \\ = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$

dans $F_2[X]$

$$P_1 + P_2 = X^2 + X$$

$$P_1 \cdot P_2 = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$

3.3) Division euclidienne

(Soient A et B deux polynomes : $\exists ! (Q, R) \text{ tq}$
 $A = B \cdot Q + R$ avec $d^0 R < d^0 B$

A = dividende

B = diviseur

Q = quotient

R = reste

• Si $R = 0$ on dit que B divise A , noté $B|A$

méthode: $A = X^4 + 1$ $B = X^2 + X + 1$

$$\begin{array}{r|l} X^4 & +1 \\ - (X^2 + X + 1)X^2 & \\ \hline -X^3 - X^2 - X & +1 \\ - (-X^3 - X^2 - X) & \\ \hline X + 1 & \end{array} \quad \begin{array}{l} X^2 - X + 1 \\ X^2 - X \\ \hline \end{array}$$

$\hookrightarrow Q = X^2 - X$
 $R = X + 1$

d'où $(X^4 + 1) = (X^2 + X + 1)(X^2 - X) + (X + 1)$

* dans $F_2[X]$:

$$\begin{array}{r|l}
 X^4 & +1 \\
 + X^4 + X^3 + X^2 & \\
 \hline
 & X^3 + X^2 + 1 \\
 + X^3 + X^2 + X & \\
 \hline
 & X + 1
 \end{array}
 \quad
 \begin{array}{l}
 X^2 + X + 1 \\
 X^2 + X \\
 \hline
 \end{array}$$

3.4) Division selon les puissances croissantes

$$\begin{aligned}
 \text{Soit } A &= a_0 + a_1 X + \dots + a_m X^m \\
 B &= b_0 + b_1 X + \dots + b_p X^p
 \end{aligned}$$

$\exists!$ (Q, R) quotient et reste de A divisé par B à l'ordre m tq

$$A = BQ + X^{m+1} \cdot R$$

ex: $A = 1 + X$ à diviser par $B = 1 + X^2$ à l'ordre 2, selon les puissances croissantes.

$$\begin{array}{r|l}
 1 + X & 1 + X^2 \\
 - 1 & + X^2 \\
 \hline
 & X - X^2 \\
 & - X & + X^3 \\
 \hline
 & - X^2 - X^3 \\
 & - - X^2 - X^4 \\
 \hline
 & - X^3 + X^4
 \end{array}$$

$$1+X = (1+X^2)(1+X-X^2) + X^3(-1+X)$$

3.5) PGCD

3.5.1) Définition

On appelle PGCD de 2 polynômes A et B , un polynôme D de degré maximal diviseur de A et de B .

On note $D = A, B$

Si D est PGCD(A, B) alors λD l'est aussi $\forall \lambda \in K^*$

"Le PGCD est défini à une constante multiplicative près."

- A et B sont premiers entre eux si $\text{PGCD}(A, B) = 1$
On note $A, B = 1$

3.5.2) Idéal dans $K[X]$

- On appelle $\mathcal{I}$ idéal dans $K[X]$ toute partie de $K[X]$ tq:

$$\forall A \text{ et } B \in \mathcal{I}, A + B \in \mathcal{I}$$

$$\forall A \in \mathcal{I}, \forall P \in K[X] A \cdot P \in \mathcal{I}$$

Amq: $\rightarrow \{0\}$ est un idéal de $K[X]$

$\rightarrow K[X]$ est un idéal de $K[X]$

$\rightarrow$ Soient A et $B \in \mathcal{I}, \forall U$ et $V \in K[X]$
 $A \cdot U + B \cdot V \in \mathcal{I}$

$\hookrightarrow$ Tout idéal de $K[X]$ comprend:

- soit uniquement $\{0\}$

- soit uniquement tous les multiples d'un même polynôme D non nul.

3.5.3) idéal engendré par 2 polynômes A et B

Soient A et $B \in K[X]$

$\rightarrow \{AU + BV, \forall U \text{ et } V \in K[X]\}$ est un idéal de $K[X]$
Il est donc formé des multiples d'un même polynôme D .

Or $A = A[1] + B[0]$ donc $A \in \mathcal{I}$ donc $D|A$
 $B = A[0] + B[1]$ donc $B \in \mathcal{I}$ donc $D|B$ $\left. \vphantom{\begin{matrix} A \in \mathcal{I} \\ B \in \mathcal{I} \end{matrix}} \right\} D | A \wedge B$

De plus $D \in \mathcal{I}$, $\exists (U_0, V_0)$ tq $D = AU_0 + BV_0$
 $A \wedge B$ divise A et divise B
donc $D = A \wedge B$

$\rightarrow$ Théorème de Bézout (1^{ère} forme)

$D = A \wedge B \rightarrow \exists (U, V) \in K[X]$ tq $AU + BV = D$

cas particulier: $D = 1$

alors $\exists (U, V)$ tq $AU + BV = 1$

alors $A \wedge B | A$ et $A \wedge B | B$ donc $A \wedge B | (AU + BV) = 1$

donc $A \wedge B = 1$

$\rightarrow$ Théorème de Bézout (2^{ème} forme)

$1 = A \wedge B \iff \exists (U, V) \in K[X]$ tq $AU + BV = 1$

3.6) Théorèmes sur la divisibilité

$\rightarrow A \wedge B = 1$ et $A \wedge C = 1 \Rightarrow A \wedge BC = 1$

car $\exists (U, V)$ tq $AU + BV = 1$ et $\exists (U', V')$ tq $AU' + CV' = 1$

donc $(AU + BV)(AU' + CV') = 1$

$A(AU' + CV') + B(UV') = 1$

$A \wedge BC = 1$

→ $A, B = 1$ $A|C$ et $B|C$ alors $AB|C$

car $C = PA - BQ$ $P, Q \in K[X]$

soit $\exists (U, V) \text{ tq } AU + BV = 1$

d'où $ACU + BCV = C$

soit $ABQU + BPAV = C$

$AB(QU + PV) = C$

donc $AB|C$

rac

→ Théorème de Gauss : $A, B = 1$ et $A|BC \Rightarrow A|C$

car $\exists (U, V) \text{ tq } AU + BV = 1 \quad (U, V) \in K[X]$

$BC = AQ$ où $Q \in K[X]$

d'où $ACU + BCV = C$

$ACU + AQV = C$

$A(CU + QV) = C$

$A|C$

rac

↳ Rmq : $D = A, B \Leftrightarrow$ les racines de D sont les racines communes de A et de B

It, $A, B = 1 \Rightarrow A$ et B n'ont pas de racines communes

3.7) PPCM

- Le PPCM de 2 polynômes A et B est un polynôme de degré minimal multiple de A et de B . Il est défini à une constante multiplicative près. On le note $A \vee B$

→ $(A, B) \cdot (A \vee B) = A \cdot B$

3.8) Dérivée de polynôme

$$P = p_0 + p_1 X + p_2 X^2 + \dots + p_m X^m \quad p_i \in K$$

$$\text{dérivée de } P = P' = p_1 + 2p_2 X + \dots + m p_m X^{m-1} \quad (m > 0)$$

$$\text{si } m = 0 \text{ alors } P' = 0$$

$$\text{si } m = -\infty \text{ alors } P' = 0$$

$$\rightarrow (P+Q)' = P' + Q'$$

$$\rightarrow kP = kP' \quad (k \in K)$$

$$\rightarrow (P \cdot Q)' = P'Q + P \cdot Q'$$

$$\hookrightarrow (P \cdot P)' = (P^2)' = 2PP'$$

$$\hookrightarrow (P^m)' = m P^{m-1} P'$$

$\rightarrow$ Théorème de Leibnitz

$$(PQ)^{(h)} = \sum_{j=0}^{h-1} C_h^j P^{(j)} Q^{(h-j)}$$

$$\hookrightarrow \begin{aligned} P &= p_0 + p_1 X + p_2 X^2 + \dots + p_m X^m \\ P^{(n)} &= p_m \frac{n!}{m!} \end{aligned}$$

$\rightarrow$ $\begin{cases} \text{fonction polynôme } f: \mathbb{R} \rightarrow \mathbb{R} & f(x) = p_0 + p_1 x + \dots + p_n x^n \\ \text{formule de Mac-Laurin:} \end{cases}$

$$f(x) = f(0) + \frac{x}{1!} f'(0) + \dots + \frac{x^n}{n!} f^{(n)}(0) \quad \text{pour } f \text{ polynôme de degré } n$$

$\rightarrow$ formule de Taylor-Young:

$$\textcircled{1} P(x+h) = P(h) + \frac{x}{1!} P'(h) + \dots + \frac{x^n}{n!} P^{(n)}(h)$$

$$\textcircled{2} P(x) = P(x_0) + \frac{x-x_0}{1!} P'(x_0) + \dots + \frac{(x-x_0)^n}{n!} P^{(n)}(x_0)$$

cas simple: $P(x) = x^m$

$$P'(x) = m x^{m-1}$$

$$P^{(n)}(x) = m!$$

$$P^{(n)}(x) = m(m-1) \dots (m-k+1) x^{m-k}$$

$$\hookrightarrow P(x+h) = (x+h)^m = h^m + \frac{x}{1!} m \cdot h^{m-1} + \dots + \frac{x^k}{k!} m(m-1) \dots (m-k+1) h^{m-k} + \dots + \frac{x^m}{m!} m!$$

$$(x+h)^m = \sum_{h=0}^{h=m} C_m^k x^k h^{m-k} \quad \text{avec } C_m^k = \frac{m!}{k!(m-k)!}$$

donc $(a+b)^m = \sum_{k=0}^{k=m} C_m^k a^k b^{m-k}$ (binôme de Newton)

3.9) Schéma de Horner

$$P(x) = P_0 + P_1 x + \dots + P_m x^m \quad \text{à calculer pour } x=a$$

$$P(x) = (((P_m x + P_{m-1})x + P_{m-2})x + \dots + P_1)x + P_0$$

ex: $p(x) = 2 + 7x + 5x^2 + 4x^3$

• pour $x=3$

calcul classique :

$$7 \times 3 = 21$$

$$x^2 = 3 \times 3 = 9$$

$$5 \times 9 = 45$$

$$x^3 = 3 \times 3 \times 3 = 9$$

$$4 \times 27 = 108$$

$$p(3) = 2 + 21 + 45 + 108 = 176$$

↳ 6 multiplications

↳ 3 additions

méthode de Horner :

$$p = (((4x+5)x+7)x+2$$

$$4 \times 3 = 12$$

$$12 + 5 = 17$$

$$17 \times 3 = 51$$

$$51 + 7 = 58$$

$$58 \times 3 = 174$$

$$174 + 2 = 176$$

↳ 3 multiplications

↳ 3 additions

3.6) Racines de polynômes

$K = \mathbb{R}$ ou $\mathbb{C}$

$P \in K[X] \leftrightarrow$ fonction polynôme $p(x)$

• on appelle racine de $p(x)$ les valeurs $x_1, x_2, \dots, x_k$ tq $p(x_i) = 0$

→ le reste de la division (euclidienne) de $p(x)$ par $x-a$ est $p(a)$

→ a est racine de $p(x)$ si $(x-a) \mid p(x)$

→ $x^m - a^m$ est divisible par $(x-a)$

→ un polynôme de degré $m > 0$ admet au plus m racines

→ le polynôme nul admet une infinité de racines et c'est le seul

→ P_m et Q_m polynômes de degré m ayant les m valeurs en plus de m points sont égaux

→ Théorème de D'Alembert

donne $\mathbb{C}[X]$ tout polynôme de degré $m \geq 1$ admet au moins une racine $\in \mathbb{C}$

↳ $P(x)$ de degré n : $P(x) = \alpha(x-z_1)(x-z_2)\dots(x-z_n)$
($\alpha \in \mathbb{C}$)

$P(x)$ a strictement n racines dans $\mathbb{C}$

$\Rightarrow$ On dit que x_0 est racine multiple d'ordre m de $P(x)$ ssi $P(x) = (x-x_0)^m Q(x)$ où $Q(x_0) \neq 0$

$\rightarrow$ dans $\mathbb{C}$, soit $P(x)$ de degré n ayant comme racines γ_1 de multiplicité α_1 , γ_2 de multiplicité $\alpha_2, \dots, \gamma_h$ de " α_h .

$$\text{alors } P(x) = \lambda (x-\gamma_1)^{\alpha_1} (x-\gamma_2)^{\alpha_2} \dots (x-\gamma_h)^{\alpha_h} \quad \lambda \in \mathbb{C}$$

la Factorisation irréductible dans $\mathbb{C}$ et
 $\alpha_1 + \alpha_2 + \dots + \alpha_h = n = \deg P$

Dans $\mathbb{R}[X]$ $p_m(x) = a_m x^m + \dots + a_1 x + a_0 \quad a_i \in \mathbb{R}$
 $p_m(x)$ a donc m racines réelles ou complexes, simples ou multiples.

si x_1 est racine $p_m(x_1) = 0$
 alors $\overline{p_m(x_1)} = \overline{p_m(x_1)} = 0$

donc x_1 racine complexe (non réelle) $\Rightarrow \overline{x_1}$ est aussi racine

conclusion: si m est impair, $p_m(x)$ a au moins une racine réelle.

Soit h la multiplicité de x_0 racine de $p(x)$.

$$p(x) = (x-x_0)^h q(x) \quad q(x_0) \neq 0$$

$$p'(x) = h(x-x_0)^{h-1} q(x) + (x-x_0)^h q'(x)$$

$$= (x-x_0)^{h-1} [h q(x) + (x-x_0) q'(x)]$$

$$q_1(x) \quad q_1(x_0) = h q(x_0) \neq 0$$

donc x_0 est racine d'ordre $h-1$ de $q_1(x)$

$\rightarrow x_0$ est racine multiple d'ordre h de $p(x)$

$$\Leftrightarrow p(x_0) = p'(x_0) = \dots = p^{(h-1)}(x_0) = 0 \neq p^{(h)}(x_0)$$

3.11) Factorisation dans $\mathbb{R}$

$$(i) P(X) = a (x - z_1)^{\alpha_1} \dots (x - z_n)^{\alpha_n} \quad z_i \in \mathbb{C}, \quad a \in \mathbb{C}$$

$$\alpha_1 + \alpha_2 + \dots + \alpha_n = n = d^{\circ} P$$

Supposons $P(X) \in \mathbb{R}[X]$ si z_i complexe est racine
 $\bar{z}_i$ est aussi racine

$$(x - z_i)^{\alpha_i} (x - \bar{z}_i)^{\alpha_i} \text{ apparaît dans (1)}$$

$$(x^2 - (z_i + \bar{z}_i)x + z_i \bar{z}_i)^{\alpha_i} \quad " \quad " \quad "$$

Soit $(x^2 + p_i x + q_i)^{\alpha_i}$ apparaît dans (1)

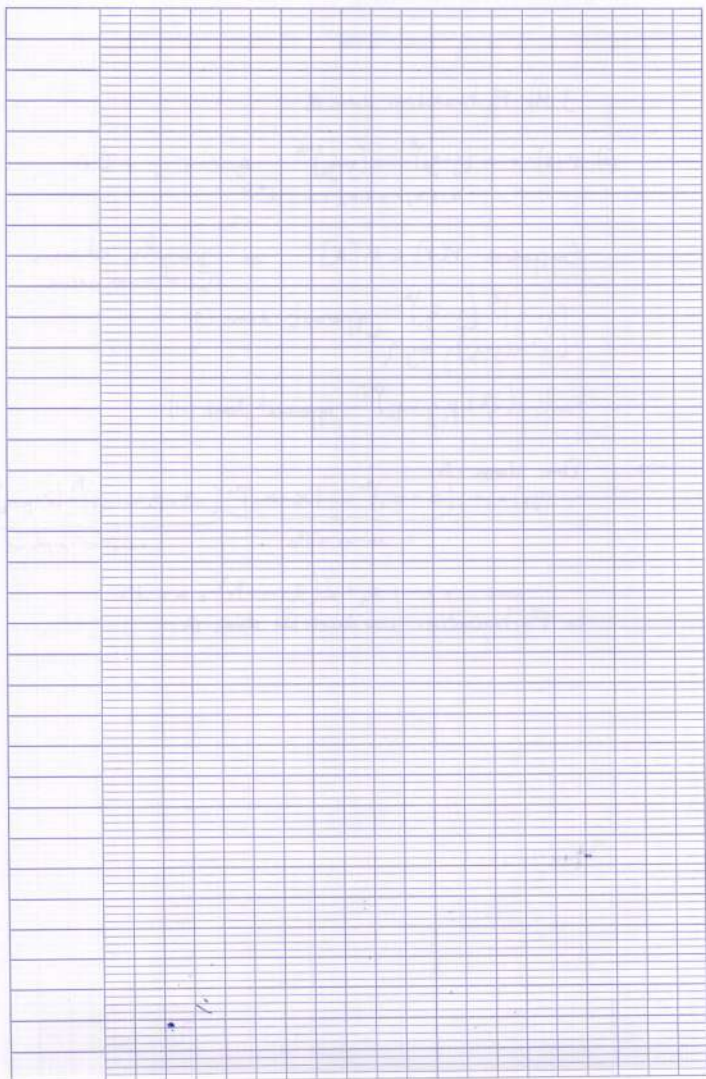
→

Donc dans $\mathbb{R}$:

$$P(X) = a \underbrace{(x - x_1)^{\alpha_1} \dots (x - x_n)^{\alpha_n}}_{n \text{ racines réelles}} \underbrace{(x^2 + p_1 x + q_1)^{\beta_1} \dots (x^2 + p_r x + q_r)^{\beta_r}}_{\text{racines complexes}}$$

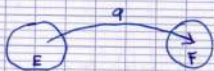
$$\text{avec } \alpha_1 + \dots + \alpha_n + 2(\beta_1 + \dots + \beta_r) = n = d^{\circ} P$$

↳ Factorisation irréductible dans $\mathbb{R}$



Chapitre 4: Applications et Relations

4.1) Applications : définitions générales



- q est une application de E dans F si elle associe à tout élément $e \in E$ un et un seul $f \in F$.

• E est l'ensemble de départ.

• F est l'ensemble d'arrivée.

• f est l'image de e .

• e est un antécédent de f .

• $e \xrightarrow{q} f$ ou $f = q(e)$

• $q: E \rightarrow F$

• $q \in \mathcal{F}(E, F)$

• $q(E) = \{f \in F : \exists e \in E : f = q(e)\}$

• Identité dans $E = \text{id}_E : \forall e \in E \text{ id}_E(e) = e$

• Surjection : $q \in \mathcal{F}(E, F)$ est surjective

ssi $q(E) = F \Leftrightarrow \forall f \in F, \exists e \in E, f = q(e)$

• Théorème de Cantor : il n'existe pas de surjection de E dans $\mathcal{P}(E)$

• injective : $q \in \mathcal{F}(E, F)$ est injective ssi

$e_1 \neq e_2 \Rightarrow q(e_1) \neq q(e_2)$

ce qui équivaut à $q(e_1) = q(e_2) \Rightarrow e_1 = e_2$

L'application ^{induction} n'est pas injective

• bijection : q est bijective ssi q est injective et surjective

$\Leftrightarrow \forall f \in F, \exists! e \in E : f = q(e)$

dans $\exists q^{-1} \in \mathcal{F}(F, E)$ tq $e = q^{-1}(f)$

q^{-1} est l'application réciproque de q , et q^{-1} est aussi bijective.

↳ $q^{-1}[q(e)] = e$ et $q^{-1} \circ q = \text{id}_E$

• $q(E)$ = "image de E par q "

• $q(E) \subset F$

• $q_1 = q_2 \Leftrightarrow \forall e \in E, q_1(e) = q_2(e)$

ex: $f: \mathbb{R} \rightarrow \mathbb{R}$ tq $f(x) = \sin x$ $\begin{cases} \text{n'est pas surjective} \\ \text{n'est pas injective} \end{cases}$

$f: \mathbb{R} \rightarrow [-1; 1] : f(x) = \sin x$ $\begin{cases} \text{est surjective} \\ \text{n'est pas injective} \end{cases}$

$f: [-\frac{\pi}{2}; \frac{\pi}{2}] \rightarrow [-1; 1] : f(x) = \sin x$ est bijective
sa fonction réciproque est $\arcsin$

• On appelle permutation de E toute bijection de E dans E

ex: $\varphi: \mathbb{N}_4^* \rightarrow \mathbb{N}_4^*$ tq $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

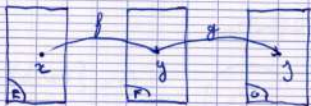
alors $\varphi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \varphi$ (cas particulier)

• restriction: Soit $\varphi \in \mathcal{G}(E, F)$ $E \neq \emptyset$
Soit $E' \subset E$, $E' \neq \emptyset$

• On appelle restriction g de φ à E' l'application E' dans F
tq $g(e) = \varphi(e) \forall e \in E'$
On peut noter $g = \varphi|_{E'}$

• Soit g une application de E' dans F avec $E' \subset E$
on dit que φ est un prolongement de g dans E
si $g = \varphi|_{E'}$

4.2) Composition d'application



$$f \in \mathcal{F}(E, F) \quad g \in \mathcal{F}(F, G)$$

$$\forall x \in E, \exists! y \in G \text{ tq } y = g(f(x)) = g \circ f(x) = h(x)$$

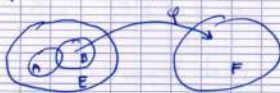
$h = g \circ f \in \mathcal{F}(E, G)$ est la composée de f par g
 → la composée de 2 injections est une injection
 ————— injections ————— injection
 ————— bijections ————— bijection

$$\cdot \mathcal{F}(E) = \mathcal{F}(E, E)$$

• $\varphi \in \mathcal{F}(E)$ est involutivessi $\varphi \circ \varphi = \text{Id}_E$
 ex: dans l'espace $\mathbb{R}^3$ la symétrie σ_c est involutive

4.3) Propriétés élémentaires

$$\varphi \in \mathcal{F}(E, F)$$



$$\rightarrow A \subset B \Rightarrow \varphi(A) \subset \varphi(B)$$

$$\rightarrow \varphi(A \cup B) = \varphi(A) \cup \varphi(B)$$

$$\rightarrow \varphi(A \cap B) \subset \varphi(A) \cap \varphi(B)$$

→ Si φ est injective alors $\varphi(A \cap B) = \varphi(A) \cap \varphi(B)$
 car $\varphi(A \cap B) \subset \varphi(A) \cap \varphi(B)$

et soit $y \in \varphi(A) \cap \varphi(B)$

alors $y \in \varphi(A) \Rightarrow \exists x \in A \text{ tq } y = \varphi(x)$

$y \in \varphi(B) \Rightarrow \exists x' \in B \text{ tq } y = \varphi(x')$

or φ est injective donc $x = x' \in A \cap B$

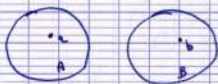
donc $y \in \varphi(A \cap B)$

donc $\varphi(A) \cap \varphi(B) \subset \varphi(A \cap B)$

rac

4.4) Relations

4.4.1) Définition



$$G = \{(a, b) \in A, B\}$$

tg (a, b) vérifie une propriété caractéristique)

On dit alors que $a R b$ si $(a, b) \in G$

R est une relation définie sur A, B . G est le graphe de R

ex: $A = B = \mathbb{R}$ $x R y$ si $y \geq x$

le graphe de cette relation est le demi-plan situé au dessus de la bissectrice $y = x$

Si $A = B = E$ on dit que la relation R est une relation binaire sur E .

ex: 1 est une relation dans $\mathbb{N}$

2 est relié à 4 214

3 n'est pas relié à 5 315

• réflexivité: R défini sur E est réflexive si $\forall x \in E, x R x$

• transitivité: R est transitive si $\forall (x, y, z) \in E^3$ $x R y$ et $y R z \Rightarrow x R z$

• symétrie: R est symétrique si $\forall (x, y) \in E^2$ $x R y \Leftrightarrow y R x$

• antisymétrie: R est antisymétrique dans E si $\forall (x, y) \in E^2$ $(x R y \text{ et } y R x) \Rightarrow x = y$

4.4.2) Relation d'équivalence

- R dans E est une relation d'équivalence (ou une équivalence) ssi R est réflexive, symétrique et transitive. On note souvent R par $\equiv$
ex: similitude de triangles: $x \equiv y$
ou $x \sim y$

- Soit $\sim$ une équivalence dans E .
on appelle donc classe d'équivalence de x , notée $\bar{x}$, l'ensemble des $a \in E$ tq $a \sim x$.

ex: Dans $\mathbb{N}$ $x \sim y$ ssi $2 \mid (x-y)$

↳ réflexive car $2 \mid (x-x)$ $x \sim x$

↳ symétrique car $x \sim y \Rightarrow 2 \mid (x-y) \Rightarrow 2 \mid (y-x)$

donc $2 \mid (y-x)$ donc $y \sim x$

↳ transitive car :

$x \sim y$ et $y \sim z \Rightarrow 2 \mid (x-y)$ $2 \mid (y-z)$

donc $x-y = 2k$, $k \in \mathbb{Z}$

$y-z = 2k'$, $k' \in \mathbb{Z}$

$x-z = 2(k+k')$, $k+k' \in \mathbb{Z}$

donc $2 \mid (x-z) \Rightarrow x \sim z$

$\bar{0} = \mathbb{P} = \{\text{pairs}\}$

$\bar{1} = \mathbb{I} = \{\text{impairs}\}$

$\mathbb{N} = \bar{0} \cup \bar{1}$

et $\bar{0} \cap \bar{1} = \emptyset$

} $\bar{0}$ et $\bar{1}$ forment une partition de $\mathbb{N}$.

- Soit $(E, \sim)$, l'ensemble des classes d'équivalence forment une partition de E .

4.4.3) Relation d'ordre

- Soit R une relation dans E et une relation d'ordre (ou un ordre) ssi R est réflexive, transitive et antisymétrique. On note en général $\succsim$
 - $\hookrightarrow$ dans R est un ordre
 - $\hookrightarrow R$ n'est pas un ordre
- E est alors ordonné par $\succsim$;
- E est totalement ordonné par $\succsim$ ssi $\forall (x, y) \in E^2$ $x \succsim y$ ou $y \succsim x$.
- $(E, \leq)$ $A \subseteq E$
 - majorant $\lambda \in E$ est un majorant de A ssi $\forall a \in A, a \leq \lambda$.
 - mineurant $m \in E$ est un mineurant de A ssi $\forall a \in A, m \leq a$.
 - A est borné ssi A est majoré et minoré.
 - A contient au plus un majorant, et au plus un mineurant
- le plus petit élément (s'il existe) des majorants est la borne supérieure de A
- le plus grand élément (s'il existe) des mineurants est la borne inférieure de A .
- M est maximal dans A ssi $M \in A$ et $x \in A$ avec $M \leq x \Rightarrow x = M$
- m est minimal ————— $m \in A$ et $y \in A$ avec $y \leq m \Rightarrow y = m$

ex: $E = \mathbb{R}$ $A =]-1; +1[$

$\hookrightarrow -2$ est mineurant de A

$\hookrightarrow -3$ ————— de A

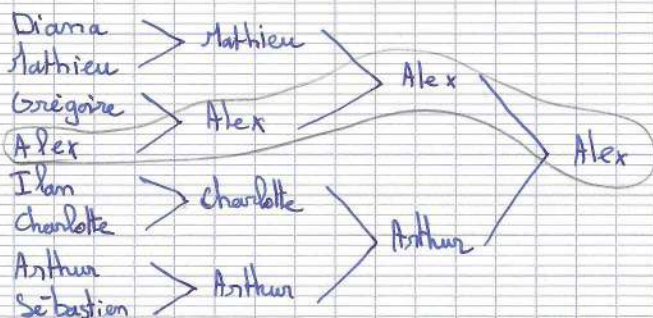
$\hookrightarrow -1$ est mineurant de A

} -1 est le plus grand des mineurants, c'est la borne inférieure de A .

ex: Tournoi de tennis

$a \gg b$ si

$b = a$
ou
 a battu b
ou
 a battu c et c battu b



minimaux: Diana, Grégoire, Ilan, Sébastien

+ petit: $\emptyset$

maximal: Alex

+ grand: Alex

↳ Dopage: matchs d'Alex annulés:

minimaux: idem

+ petit: $\emptyset$

maximal: Mathieu, Grégoire, Arthur

+ grand: $\emptyset$

4.4.4) Application croissante

• E et F deux ensembles ordonnés par $\leq_E$ et $\leq'_F$

↳ $f: E \rightarrow F$ est croissante si $x \leq_E y \Rightarrow f(x) \leq'_F f(y)$

↳ ———— décroissante — $x \leq_E y \Rightarrow f(y) \leq'_F f(x)$

Chapitre V: Dénombrément

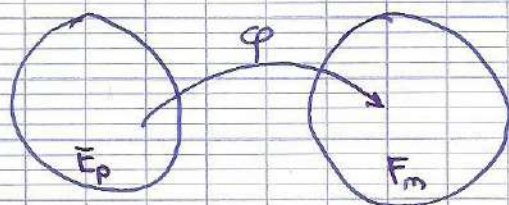
5.1) Cardinal d'un ensemble

- On dit que A et B ont même puissance, ou qu'ils sont équipotents, ssi il existe une bijection de A dans B
→ l'équipotence est une relation d'équivalence.
- On écrit $\text{card } A = \text{card } B$
- On dit que $\text{card } A \leq \text{card } B$ ssi $\exists$ injection de A dans B .
→ $E \subset F \Rightarrow \text{card } E \leq \text{card } F$
- Le cardinal de $\{1, 2, \dots, n\} = n$
- E est fini ssi $\exists m \in \mathbb{N}^*$ tq $\text{card } E = m$
→ $\text{card}(E \cdot F) = \text{card } E \cdot \text{card } F$
- E est dénombrable ssi $\text{card } E = \text{card } \mathbb{N} = \aleph_0$ (aleph)
→ $\aleph_0 + 1 = \aleph_0$
→ $\aleph_0 \cdot \aleph_0 = \aleph_0$
- On a vu que $\text{card } P(E) = 2^{\text{card } E}$
→ Théorème de Cantor: $\text{card } E < \text{card } P(E)$
 $\text{card } \mathbb{N} < \text{card } P(\mathbb{N})$
 $\aleph_0 < \aleph_1$
hyp: $\text{card } \mathbb{R} = \aleph_1$
Mq $\mathbb{R}$ n'est pas dénombrable
On considère tous les réels $\in]0, 1[$
Supposons $\exists$ bijection entre $\mathbb{R}$ et $\mathbb{N}$ ↗

$0, a_{11} a_{12} a_{13} \dots$
 $0, a_{21} a_{22} a_{23} \dots$
 $\vdots$
 $0, a_{n1} a_{n2} a_{n3} \dots$
 $\vdots$

Or $0, (a_{m+1}), (a_{m+2}), \dots, (a_{m+1} + 1) \notin$ cette liste
 donc $\text{card } \mathbb{R} > \text{card } \mathbb{N}$
 $X_0 < X_1 < X_2 < X_3$
 $\text{card}(\mathbb{N}) \uparrow \text{card } \mathbb{R} \quad \text{card}(P(\mathbb{R})) \quad \text{card}(P(P(\mathbb{R})))$
 rien

5.2) Nombre d'applications de E dans F



$$\varphi \in \mathcal{F}(E_p, F_m)$$

$$E_p = \{e_1; \dots; e_p\}$$

$$F_m = \{f_1; \dots; f_m\}$$

$$\rightarrow \text{card } \mathcal{F}(E_p; F_m) = (\text{card } F_m)^{\text{card } E_p} = m^p$$

5.3) Nombre d'injections de E_p dans F_m

Une injection est définie par la liste $\varphi(e_1) \dots \varphi(e_p)$ ordonnée et sans répétition de p éléments pris parmi les m éléments de F_m . C'est un arrangement de p parmi m .

Le nombre d'injections est le nombre d'arrangement A_m^p .

$$p = 1$$

$$A_m^1 = m$$

$$A_m^2 = (m-1)A_m^1$$

$$A_m^3 = (m-2)A_m^2$$

...

$$A_m^p = (m-(p-1))A_m^{p-1}$$

$$A_m^p = m(m-1) \dots (m-p+1)$$

p termes

cas particulier: $p = m$

le nombre de bijections de E_m dans F_m est A_m^m

avec $A_m^m = m(m-1) \dots (2)(1) = m!$

donc $A_m^p = \frac{m(m-1) \dots (2)(1)}{(m-p) \dots (2)(1)}$

→

$$A_m^p = \frac{m!}{(m-p)!}$$

avec par convention $0! = 1$

sous-cas particulier: $E_m = F_m$

↳ c'est une permutation, il y a $m!$ permutations

5.4) Combinaison

On appelle combinaison de p éléments parmi n une liste non ordonnée de p éléments sans répétition pris parmi n .

A chacune correspond une partie de E_m ayant un cardinal p .

Il y a C_m^p combinaisons différentes $\binom{p}{m}$ avec $p \leq m$

→

$$A_m^p = p! \cdot C_m^p$$

$$\text{avec } C_m^p = \frac{m!}{p!(m-p)!} = \frac{m(m-1) \dots (m-p+1)}{p(p-1) \dots \times 2 \times 1}$$

Propriétés:

$$\begin{cases} C_m^{m-p} = C_m^p \\ C_m^0 = 1 = C_m^m \\ C_m^1 = m = C_m^{m-1} \\ C_m^p = C_{m-1}^p + C_{m-1}^{p-1} \end{cases}$$

$$\begin{aligned} \text{car } C_{m-1}^p + C_{m-1}^{p-1} &= \frac{(m-1)!}{p!(m-p-1)!} + \frac{(m-1)!}{(p-1)!(m-p)!} \\ &= \frac{(m-1)!}{(p-1)!(m-p)!} \left[\frac{1}{p} + \frac{1}{m-p} \right] \\ &= \frac{(m-1)! \cdot (m-p)}{p!(m-p)!} = \frac{m!}{p!(m-p)!} = C_m^p \end{aligned}$$

rac

Triangle de Pascal:

$\begin{smallmatrix} p \\ m \end{smallmatrix}$	0	1	2	3	4	5
0	1					
1	1	1				
2	1	2	1			
3	1	3	3	1		
4	1	4	6	4	1	
5	1	5	10	10	5	1

Newton:

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

→ Remq 1: $a=b=1, 2^n = \sum_{p=0}^n C_m^p$

Remq 2: $a=x, b=1, (1+x)^n = \sum_{p=0}^n C_m^p x^p$

Remq 3: Le nb de parties de E_m ayant 0 éléments est C_m^0

1 ————— C_m^1

2 ————— C_m^2

m ————— C_m^m

$$\text{card } \mathcal{P}(E_m) = C_m^0 + C_m^1 + \dots + C_m^m = 2^n = 2$$

5.5) Equation diophantienne

ex: 4 mégots à donner à 3ados. Combien de répartitions?

Julien	4	3	3	2	2	2	1	1	1	1	0	0	0	0	0
Michel	0	1	0	2	1	0	3	2	1	0	4	3	2	1	0
Kevin	0	0	1	0	1	2	0	1	2	3	0	1	2	3	4

Les 15 répartitions

$$C_1 + C_2 + C_3 = 4 \quad C_i \geq 0$$

Equation de Diophante:

→

$$u_1 + u_2 + \dots + u_p = m \quad u_i \in \mathbb{N}$$

$$\begin{array}{ccccccc|cccc|cc} u_1 & u_2 & & & & & & & & & u_{p-1} & u_p \\ | & | & | & | & | & | & | & | & | & | & | & | \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array} \quad \begin{cases} m & \text{petits traits} \\ p-1 & \text{grands traits} \end{cases}$$

↳ il y a donc $m+p-1$ traits en tout

↳ il y a donc $\binom{m+p-1}{p-1}$ solutions

5.6) Systèmes de numération

5.6.1) Entiers

$$p \in \mathbb{N} = b_{m-1}b_{m-2} \dots b_1b_0$$

← dans la base b

où $0 \leq b_i \leq b$

si on rajoute un zéro à droite de p , cela multiplie par la base.

changement de base: $p = b_0 + b_1b' + b_2b'^2 + \dots + b_{m-1}b'^{m-1}$

ex: 6772_{10} en base 7

$$\begin{array}{r|l} 6772 & 7 \\ \hline 47 & 967 \\ 52 & 26 \\ 3 & 37 \\ & 1 \end{array} \quad \begin{array}{r|l} 967 & 7 \\ \hline 26 & 138 \\ 37 & 68 \\ 1 & 5 \end{array} \quad \begin{array}{r|l} 138 & 7 \\ \hline 68 & 19 \\ 5 & 5 \end{array} \quad \begin{array}{r|l} 19 & 7 \\ \hline 5 & 2 \\ 2 & 2 \end{array} \rightarrow 25513_7$$

5.6.2) Rationnels

$$r = a/b \quad a \in \mathbb{Z} \quad b \in \mathbb{N}^*$$

$$\frac{a}{b} = b_{m-1}10^{m-1} + \dots + b_110^1 + b_0 + c_110^{-1} + c_210^{-2} \dots$$

$$= \overbrace{b_{m-1} \dots b_1 b_0}_{10} , \underbrace{c_1 c_2 \dots}_{10}$$

d' développement toujours périodique

Réciproquement: Tout développement décimal périodique représente un rationnel

$$q = 0,2727272727 \dots$$

$$q = 27 \cdot 10^{-2} + 27 \cdot 10^{-4} + 27 \cdot 10^{-6} + \dots$$

$$= 27 \cdot 10^{-2} (1 + 10^{-2} + 10^{-4} + \dots) = 27 \cdot 10^{-2} \cdot \frac{1}{1-10^{-2}} = \frac{27 \cdot 10^{-2}}{99 \cdot 10^{-2}} = \frac{27}{99} = \frac{3}{11}$$

On $x = 0,10100100010000 \dots$ n'est pas rationnel ; $x \in \mathbb{R}$
↑
 irrationnel

• x est algébrique ssi il est racine d'un polynôme à coefficient rationnel.

Si x n'est pas algébrique, il est transcendant : π, e

Application: calcul de x^n quand n est grand

ex: $y = x^{10007}$

$$\underbrace{x \cdot x \cdot x \cdot \dots \cdot x}_{10006 \text{ multiplications}}$$

10006 multiplications

on converti n en binaire : $10007^{10} = 1001110010111$

$$= 2^{13} + 2^{10} + 2^9 + 2^8 + \dots$$

$$x^{10007} = x^{(2^{13})} \cdot x^{(2^{10})} \cdot x^{(2^9)} \cdot x^{(2^8)} \cdot x^{(2^7)} \cdot x^{(2^6)} \cdot x^{(2^5)} \cdot x^{(2^4)} \cdot x^{(2^3)} \cdot x^{(2^2)} \cdot x^{(2^1)} \cdot x^{(2^0)}$$

↳ 7 multiplications

Or $x^{(2^1)} = x^2 = x \cdot x$

$$x^{(2^2)} = x^4 = (x^2)^2$$

...

} 13 multiplications

20 multiplications

Chapitre VI : Arithmétique

6.1) Introduction

Etude de $(\mathbb{Z}, +, \cdot)$ qui est un anneau commutatif unitaire et intègre.

$$\begin{array}{ccc} \downarrow & & \downarrow \\ \exists ! \text{ tq } a \cdot 1 = a & & a \cdot b = 0 \Rightarrow a = 0 \text{ ou } b = 0 \end{array}$$

6.2) Divisibilité

a et $m \in \mathbb{Z}$ on dit que m divise a

ssi $\exists k \in \mathbb{Z}$ tq $a = m \cdot k$

On note $m \mid a$

- Dans $\mathbb{N}$, $\mid$ est une relation d'ordre
- $m \mid a \Leftrightarrow m \mid -a \Leftrightarrow -m \mid a \Leftrightarrow -m \mid -a$
- 0 ne divise que 0
- 1 et -1 divisent a , $\forall a \in \mathbb{Z}$
- $\forall a \in \mathbb{Z} \setminus \{-1, 1\}$ a a au moins 4 diviseurs

6.3) Division euclidienne

$$\forall (a, b) \in \mathbb{N}^2 \quad \exists ! (q, r) \in \mathbb{N}^2 \text{ tq } a = bq + r \text{ avec } 0 \leq r < b$$

6.4) Congruence modulo m

6.4.1) Définition

$m \in \mathbb{N}^*$, $(a, b) \in \mathbb{Z}^2$ a est congru à b modulo m ssi $m \mid (b - a)$

$$\Leftrightarrow \exists \lambda \in \mathbb{Z} \text{ tq } a = b + \lambda m$$

On note $a \equiv b \pmod{m}$

→ La congruence modulo m est une relation d'équivalence.
Elle définit dans $\mathbb{Z}$ des classes d'équivalence

$$\mathbb{Z}/m\mathbb{Z} = \{ \overset{\circ}{0}; \overset{\circ}{1}; \overset{\circ}{2}; \dots; \overset{\circ}{m-1} \} \quad (\text{comprend } m \text{ classes})$$

↳ en particulier $\mathbb{Z}/2\mathbb{Z} = \{ \overset{\circ}{0}; \overset{\circ}{1} \} = \text{corps } \mathbb{F}_2$

Applications:

↳ contrôle des n° INSEE

ex: $\begin{array}{ccccccccc} 1 & 9 & 2 & 0 & 8 & 7 & 5 & 1 & 1 & 3 & 7 & 3 & 0 & 9 & 5 \end{array}$ $97-2 = 95$
code

$[97] = 2$

↓ sexe
↓ année
↓ mois
↓ Paris
↓ naissance dans 6 mois

↳ clé d'une carte bancaire

ex: $\begin{array}{ccccccccc} 4 & 9 & 7 & 3 & 0 & 1 & 9 & 6 & 0 & 5 & 2 & 4 & 5 & 4 & 7 & 2 \end{array}$ ← algorithme de Luhn

↓ type (Visa, Mastercard)
↓ établissement

→ La congruence est compatible avec l'addition

$$\text{car } a \equiv b [m] \Leftrightarrow \exists k_1 \in \mathbb{Z} \text{ tq } a = b + k_1 m$$

$$c \equiv d [m] \Leftrightarrow \exists k_2 \in \mathbb{Z} \text{ tq } c = d + k_2 m$$

$$\text{d'où } a + c = b + d + \underbrace{(k_1 + k_2)}_{\in \mathbb{Z}} m$$

donc $a + c \equiv b + d [m]$
rac

Application: calcul du reste de division par 7 de 59^{45}

$$59 \equiv 3 [7]$$

$$59 \equiv 3^{45} [7]$$

$$3^0 \equiv 1 [7]$$

$$3^1 \equiv 3 [7]$$

$$3^2 \equiv 2 [7]$$

$$3^3 \equiv 6 [7]$$

$$3^4 \equiv 4 [7]$$

$$3^5 \equiv 5 [7]$$

$$3^6 \equiv 1 [7]$$

La suite des 3^k est périodique de période 6 dès 3^0

$$\text{on } 45 \equiv 3 [6]$$

$$\text{donc } 3^{45} \equiv 3^3 [7] \equiv 6 [7]$$

↳ le reste est 6

$$[\text{lemme: } a \equiv b [m] \Rightarrow a^k \equiv b^k [m]]$$

Application: critère de divisibilité
divisibilité par 9

$$p = \overline{b_{m-1} \dots b_1 b_0}_{10} = b_0 + 10b_1 + 10^2b_2 + \dots + 10^{m-1}b_{m-1}$$

$$\text{donc } p = b_0 + b_1 + \dots + b_{m-1} [9] \text{ car } 10^k \equiv 1[9]$$

un nombre est divisible par 9 si la somme de ses chiffres l'est

6.5) Nombres premiers

↳ GIMPS : Great Internet Measure Prime Search

$$M_n = 2^p - 1$$

$$13 \text{ nov } 1996: M_{35} = 2^{13394709} - 1$$

$$12 \text{ avril } 2009: M_{47} = 2^{42643801} - 1$$

VI. 5) Nombre premier

p est 1^{er} dans $\mathbb{N}$ ssi p n'est divisible que par 1 et p .

cible d'Euclide

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

→ Le nombre de 1^{er} est ∞ car $\forall n \in \mathbb{N}$, soit $p = n! + 1$

ou p n'est pas divisible par $2, 3, 4, 5, \dots, n$

ou bien p est premier

ou si ce n'est pas il est divisible par un premier $\in [n, p]$

fonction d'Euler

$$f(n) = n^2 + n + 41$$

$f(n)$ est 1^{er} $\forall n \in [0, 39]$

$$f(n) = 2 + (2(n-1)! [n])$$

$$f(2) = 2$$

$$f(3) = 3$$

$$f(4) = 2 \quad \text{n'est pas premier}$$

$$f(5) = 5$$

$$f(6) = 2$$

$$f(7) = 7$$

6. 6) Factorisation première

Soit $a \in \mathbb{N}$ $a \geq 2$

Soit p_1 1^{er} + petit diviseur (> 1); p_1 est 1^{er}

$$a = p_1 \cdot a_1$$

Si $a_1 \geq 2$ $a_1 = p_2 \cdot a_2$ p_2 1^{er}, + petit diviseur de a_1

$a = p_1 p_2 \dots p_h$ où les p_i sont 1^{er} et croissant

$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_h^{\alpha_h}$ où p_i est 1^{er} et $p_i < p_j$ si $i < j$

756	2
378	2
189	3
63	3
21	3
7	7
1	

$$a = 2^3 \cdot 3^3 \cdot 7^1$$

$$d | a \text{ si } d = 2^x \cdot 3^y \cdot 7^z$$

$$\text{nb diviseurs} = (2+1)(3+1)(1+1) = 3 \times 4 \times 2 = 24$$

diviseurs

6.7) PGCD, PPCM

Soit a et $b \in \mathbb{N}$

$$a = \prod_{j=1}^{h} q_j^{\alpha_j}$$

où q_j est un facteur 1^{er} de a ou de b

$$b = \prod_{j=1}^{h} q_j^{\beta_j}$$

$$\text{PGCD}(a, b) = a \cap b = \prod_{j=1}^h q_j^{\inf(\alpha_j, \beta_j)}$$

$$\text{PPCM}(a, b) = a \cup b = \prod_{j=1}^h q_j^{\sup(\alpha_j, \beta_j)}$$

$$(a \cup b)(a \cap b) = \prod_{j=1}^h q_j^{\inf(\alpha_j, \beta_j) + \sup(\alpha_j, \beta_j)}$$

$$a \cdot b = (a \cap b) \cdot (a \cup b)$$

a et b sont premiers entre eux si $a \cap b = 1$

6.8) Théorème sur la divisibilité

6.8.1) Théorème de Bézout

1^{re} forme $\rightarrow a, b \neq 0 \Rightarrow \exists (u, v) \in \mathbb{Z}^2$ tq $au + bv = d$

2^e forme $\rightarrow a \wedge b = 1 \Leftrightarrow \exists (u, v) \in \mathbb{Z}^2$ tq $au + bv = 1$

6.8.2) Théorème de Gauss

$a \mid bc$ et $a \wedge b = 1 \Rightarrow a \mid c$

6.8.3) autres théorèmes

$\rightarrow a \wedge b = 1$ et $a \wedge c = 1 \Rightarrow a \wedge bc = 1$

$\rightarrow a \wedge b = 1 \Rightarrow a^m \wedge b^n = 1, \forall (m, n) \in \mathbb{N}^2$

$\rightarrow a \wedge b = 1 \Rightarrow a \wedge (a+b) = 1$ et $(a+b) \wedge ab = 1$

6.8.4) Algorithme d'Euclide

On cherche $a \wedge b$ avec $a \geq b > 1$

$$a = bq + r \quad 0 \leq r < (b-1)$$

$$a \wedge b = b \wedge r$$

$$3809 \wedge 18459 = d$$

	4	1	5	2
18459	5809	3223	299	(293) — PGCD
3223	589	293	0	

$$3223 = a - 4b$$

$$589 = b - 1(a - 4b) = -a + 5b$$

$$293 = a - 4b - 5(-a + 5b) = 6a - 29b$$

$$\underbrace{6a}_{\downarrow} - \underbrace{29b}_{\downarrow} = a \wedge b$$

Autre exemple

4680	2
2340	2
1170	2
585	3
195	3
65	3
13	13
1	

$$4680 \wedge 89$$

89	2
42	2
21	3
7	7
1	

$$89 = 2^2 \cdot 3^2 \cdot 7^2$$

$$4680 = 2^3 \cdot 3^2 \cdot 5 \cdot 13$$

$$4680 \wedge 89 = 2^2 \cdot 3^2 = 12$$

6.9 Equation diophantienne

On cherche les solutions de $Ax + By = C$ (1)
dans $\mathbb{Z}$ avec $A, B \neq 0$; $\text{pgcd}(A, B) \in \mathbb{N}^*$

Étapes : calcul de $A \wedge B = 1$

Si d ne divise pas C , (1) n'a pas de solution
si $d \mid C$, on divise (1) par d

(2) $ax + by = c$, où $a \wedge b = 1$

On cherche u et $v \in \mathbb{Z}$: $au + bv = 1$ par l'algo d'Euclide

d'où $a(x + cu) + b(-u + cv) = 0$

d'où $ax + by = c$ (3)

$a(x - cu) = b(-u + cv)$ (4)

donc b divise $a(x - cu)$ or $b \wedge a = 1$ d'après Gauss
! b divise $x - cu$

donc $\exists d \in \mathbb{Z}$ tq $x - cu = db$

en remplaçant dans (4) $a \cdot db = b(-u + cv)$

$\cdot db = db$

Les solutions de (1) sont :

$$\begin{cases} x = cu + \lambda b \\ y = cv - \lambda a \end{cases} \quad \forall \lambda \in \mathbb{Z}$$

Ex Résoudre ds $\mathbb{Z}$: $8x - 6y = 10$ (1)

Posons $y = -y$: (1)' $8x + 6y = 10$

On $2 \wedge 6 = 2$

On $2 \nmid 10$ donc on continue

(2) $4x + 3y = 5$ où $4 \wedge 3 = 1$

$$\begin{array}{cc} 1 & 3 \\ 4 & 3 \end{array} \xrightarrow{(1)} \text{PGCD donc } 1 = 4 - 1(3)$$

$$\begin{array}{cc} 1 & 0 \\ 4 & 3 \end{array} \quad 4(1) - 3(-1) = 1$$

On multiplie par le 2^e mb de (2)

$$\begin{cases} 4(5) + 3(-5) = 5 \\ 4x + 3y = 5 \end{cases}$$

d'où $4(x-5) + 3(4-5) = 0$ (3)

$\exists 4(x-5) \text{ ou } 3 \nmid 4 = 1$ de d'après Gauss $3 \mid (x-5)$

$\exists \lambda \in \mathbb{Z} \mid x-5 = 3\lambda$

En reportant dans (2)

$4 \cdot 3\lambda = 3(-y-5)$

d'où $-y-5 = 4\lambda$

$x = 5 + 3\lambda$

$y = -5 - 4\lambda$

$x = 5 + 3\lambda$

$y = -5 - 4\lambda$

$\forall \lambda \in \mathbb{Z}$

6.10 Recherche de nbr premier

→ "Petit" Théorème de Fermat

p premier $\Rightarrow p \mid (n^p - n) \quad \forall n \in \mathbb{N}$

Cas particulier $n=2$

p premier $\Rightarrow p \mid (2^p - 2)$ soit $p \mid 2(2^{p-1} - 1)$

p premier $\geq 2 \Rightarrow p \mid (2^{p-1} - 1)$ test de primalité

Nbr de Mersenne : $M = 2^a - 1$

6.11 Application au cryptage



→ chiffrement par décalage

$a b \dots z \quad L = l + K[25]$
 $0 1 \dots 25$

$K=3$ codage de Cesar

Cryptage par substitution

(a b c ... z)

(0 1 2 ... 25)

permutation des $(0, \dots, 25)$

il y a $25!$ clefs possible

⇒ AES ou 4ES

⇒ RSA