

Table des matières

Chapitre 1 : Algèbre générale.....	2
1.1 - Logique - ensembles.....	2
1.2 - Tables de vérité.....	2
1.3 - Prédicat	3
1.4 - Ensembles.....	3
1.5 - Opérations sur les ensembles.....	4
1.6 - Ensembles usuels.....	5
1.7 - Cardinal ; ensemble fini.....	5
Chapitre 2 : Application et relation.....	7
2.1 - Application : définitions générales.....	7
2.2 - Applications particulières.....	7
2.4 - Quelques propriétés fondamentales.....	9
2.5 - Relations.....	9
2.6 - Relation d'équivalence.....	9
2.7 - Relation d'ordre.....	10
2.8 - Application monotone.....	10
Chapitre 3 : Nombres Complexes.....	11
3.1 - Définitions théoriques.....	11
3.2 - Représentation algébrique des complexes.....	11
3.2.1 - interprétation géométrique.....	12
3.3 - Représentation trigonométrique.....	13
3.4 - Racines n-ième des nombres complexes.....	13
3.4.1 - Racine n-ième de l'unité	13
3.4.2 - Racine carrée d'un complexe.....	13
3.4.3 - Racine carrée d'un nombre complexe.....	14
3.5 - Résolution des équations du 2ème degré dans	14
??? 3.4.3 - Racine carrée d'un complexe :.....	15
3.6 - Propriétés géométriques	15
Chapitre 4 : Polynômes.....	17
4.1 - Définitions.....	17
4.2 - Division Euclidienne.....	17
4.10 - Racines d'un polynôme.....	18
4.11 - Factorisation dans	18
4.12 - Multiplicité des racines.....	18
4.13 - Relation entre racines et coefficients.....	19
Chapitre 5 - Fonctions rationnelles dans $\mathbb{R}[x]$	21
Chapitre 6 : Dénombrement.....	23
6.1 Cardinal d'un ensemble.....	23
6.2 - Nombre d'applications de E ds F (finis).....	23
6.3 - Arrangements.....	23
6.4 Combinaison.....	24
6.5 - Distribution multinomiale.....	26
6.6 - Equation diophantienne.....	26

Chapitre 1 : Algèbre générale

1.1 - Logique - ensembles

A = « on a A »

A := tout eleve de l'EFREI a le bac

A est vrai => Associe a une variable logique A --> A est V ou F <=> Variable A vaut 1 ou 0

A <=> Soit $E = \{ e_i; i=1,2,\dots,149 \}$

BACH = { Bacheliers }

$\forall e_i \in E, e_i \in BACH$

Négation de A = $\bar{A} \Leftrightarrow i \in [1, \dots, 149] / e_i \notin BACH$

ou $\exists e_i \in E / e_i \notin BACH$

--> $\forall x \in E, P(x) = \exists x \in E / (\overline{P(x)})$

connecteur = Opération sur les assertions

= négation

ET = conjonction

OU = disjonction

==> = implication

<=> = équivalence

Soit $\underline{A}$: tout élève de l'EFREI est beau et intelligent.

Donc $\bar{A}$: un élève de l'EFREI est laid ou bete

1.2 - Tables de vérité

A	B	Faux	A^B	A\B	A	B\A	B										
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

A	B	$B \Rightarrow A$	$\bar{B}$	$A \vee \bar{B}$	$B \wedge \bar{B}$	$B \vee \bar{B}$	$A \wedge B$	$\overline{(A \wedge B)}$	$\bar{A}$	$\bar{A} \vee \bar{B}$	$A \vee B$	$\bar{A} \wedge \bar{B}$	$\overline{(A \vee B)}$	$A \Rightarrow B$	$\overline{(A \Rightarrow B)}$	$A \wedge \bar{B}$	$\bar{B} \Rightarrow A$
1	1	1	0	1	0	1	1	0	0	0	1	0	0	1	1	0	0
1	0	1	1	1	0	1	0	1	0	1	1	0	0	0	0	1	1
0	1	0	0	0	0	1	0	1	1	1	1	0	0	1	1	0	0
0	0	1	1	1	0	1	0	1	1	1	0	1	1	1	1	0	0
		_____						_____				_____		_____		_____	

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

$$B \vee \bar{B} = \text{VRAI}$$

$$B \wedge \bar{B} = \text{FAUX}$$

$$\overline{(A \wedge B)} = \bar{A} \vee \bar{B}$$

$$A \vee B = \bar{A} \wedge \bar{B}$$

$$\overline{(A \Rightarrow B)} = A \wedge \bar{B}$$

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

1.3 - Prédicat

Prédicat : énoncé contenant une variable

$$P(x) = x \in \mathbb{R}, x \geq 3$$

Si on sait trouver $E / \forall x \in E, P(x)$ et $\forall x \notin E, \overline{P(x)}$, on dit que le prédicat $P(x)$ est collectivisant et définit E

$\forall x \in E, A(x)$ a pour négation $\exists x \in E / \overline{A(x)}$

$$\overline{(\forall x \in E, A(x))} \Leftrightarrow \exists x \in E / \overline{A(x)}$$

$$\overline{(\exists x \in E / A(x))} \Leftrightarrow \forall x \in E, \overline{A(x)}$$

$$\overline{(\forall x \in E, P(x) \Rightarrow Q(x))} \Leftrightarrow \text{exist } x \in E / P \text{ et } \overline{Q}$$

$$A(x) : \exists ! x \in E / P(x)$$

1.4 - Ensembles

Cantor, à la fin du XIXe siècle a écrit la théorie des ensembles.

Soit E un ensemble

$$e \in E \text{ ou } e \notin E$$

$$\mathbb{N} = \{ 0, 1, 2, 3, \dots, n \} \quad \text{Entiers Naturels}$$

$$P = \{ \text{entiers naturels pairs} \} = \{ n \in \mathbb{N} / \exists p \in \mathbb{N} / n = 2p \}$$

Paradoxe de Russel :

$$E = \{ x / x \notin x \}$$

si $E \notin E, E \in E$ E n'existe pas donc l'ensemble

si $E \in E, E \notin E$ de tous les ensembles n'existe pas

Egalité $A = B$ ssi $\forall a \in A, a \in B$ et $b \in B, b \in A$

Inclusion $A \subset B$ ssi $\forall a \in A, a \in B$

$$(A \subset B \text{ et } B \subset A) \Rightarrow A = B$$

La relation inclusion est « anti-symétrique »

et $A \subset B$ et $B \subset C$ alors $A \subset C$

Inclusion est « transitive »

et $A \subset A$

Inclusion est « réflexive »

Si n a ses 3 propriétés, on dit que l'inclusion est ordre

si $A \subset B$ on dit que A est une partie de B

Ensemble Vide noté $\emptyset$

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

$\emptyset$ est une partie de E

Soit $P(A) = \{ \text{Parties de } A \}$

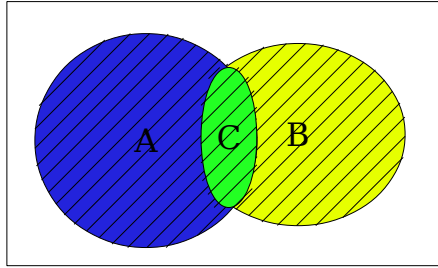
$$P(\emptyset) = \{ \emptyset \}$$

$$P(E) \neq \emptyset$$

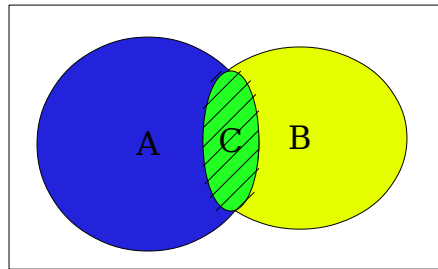
Si $E = \{x\}$, $\{x\}$ est un singleton
 $E = \{x, y\}$ $\{x, y\}$ est une paire
 $E = \{x_1, x_2, x_3 \dots x_n\}$ c'est un « n-uplet »

1.5 - Opérations sur les ensembles

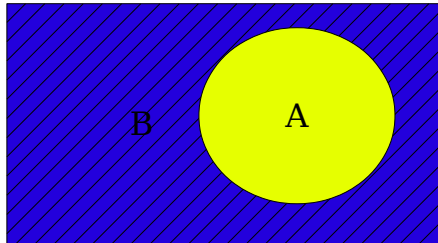
Soient A et B appartenant à $P(E)$



Reunion = $A \cup B = C = \{x \in E \mid x \in A \text{ ou } x \in B\}$
 $A \cup B = B \cup A$
 $A \cup A = A$

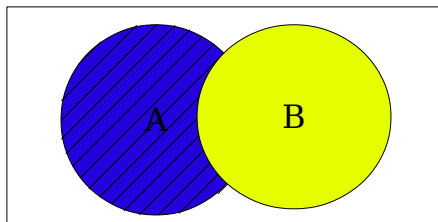


Intersection = $D = \{x \in E \mid x \in A \text{ et } x \in B\}$
 $A \cap B = B \cap A$
 $A \cap B = A \Leftrightarrow A \subset B$

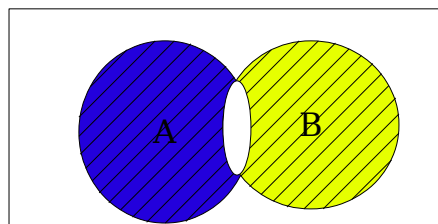


Complementation de A dans E = $\bar{A} = E \setminus A = B$

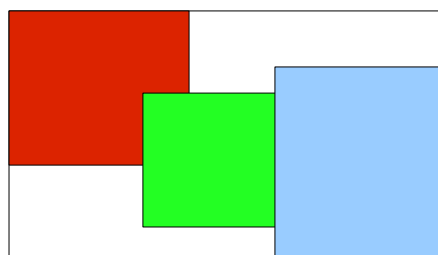
Toute propriété sur les ensembles A, B munie d'un connecteur est identique à la même propriété sur les assertions A et B avec les connecteurs logiques, en particulier les lois de De Morgan



Différence : $A \setminus B = A \cap \bar{B}$



Différence symétrique : $A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cap \bar{B}) \cup (B \cap \bar{A})$
 $A \Delta B = A \cdot \bar{B} + \bar{A} \cdot B$



Recouvrement : $X_i \in P(E), i \in 1, \dots, n$

La famille des X_i est un recouvrement de E ssi
 $X_1 \cap X_2 \dots \cap X_n = E = \bigcup X_i$

Un recouvrement est une partition ssi

1.6 - Ensembles usuels

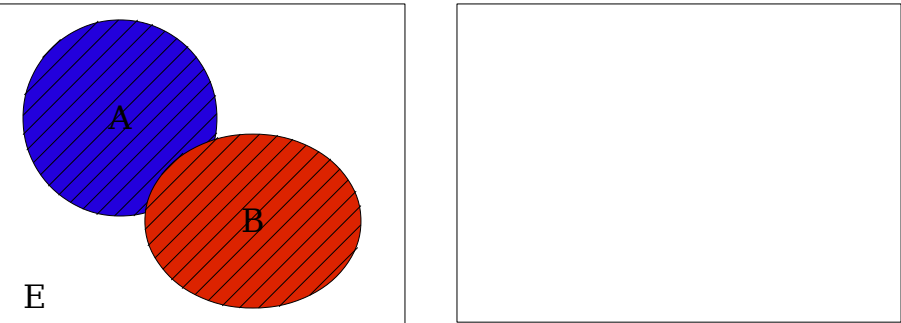
$\mathbb{N}=0,1,2,\dots,n\ldots$ = « Entiers Naturels »
 $\mathbb{N}^*_1=1,\dots,n\ldots$ = « Entiers positifs »
 $\mathbb{Z}=\dots,-n,\dots,-1,0,1,\dots,p\ldots$ = « Entiers Relatifs »
 $\mathbb{N}_n=0,1,\dots,n$
 $\mathbb{N}^*_n=1,\dots,n$
 $\mathbb{Q}$ = « nombres rationnels »
 $\mathbb{R}$ = « Reels »
 $\mathbb{C}$ = « Complexes »

Produit d'ensemble

Soient 2 ensembles A et B
Soit $a\in A, b\in B$
(a,b) couple, element l'ensemble produit A.B
 $A.B\neq B.A$ en général.
on note $A^2 = A.A$ $A^n=A^{(n-1)}.A$ n supeq 2

1.7 - Cardinal ; ensemble fini

Si E a une nombre fini n d'elements, on dit que $n = \text{card } E$
--> $\text{card } (A.B) = \text{card } A . \text{card } B$
--> $\text{card } A^n=(\text{card } A)^n, \forall n\geq 1$
On dit que deux ensembles sont équipotents ssi ils ont même cardinaux (aussi pour les ensembles infinis)
 $P = \{ \text{ensemble des nombres pairs} \} = \{ k\in\mathbb{N} / \exists p\in\mathbb{N} / k=2p \}$
--> $\text{card } A\cap B\leq \inf(\text{card } A, \text{card } B)$
--> $\text{card } A\cup B=\text{card } A+\text{card } B-\text{card } A\cap B$ (Formule des 4 cardinaux)



Card L1 = 143
 $M = \{ \text{aiment les maths} \}$
 $\text{card } M = 88$
 $\text{card } I = 122$
 $\text{card } M\cap I = 69$
 $\text{card } M\cup I = 88+122-69=141$
 $\text{card } L1\setminus M\cup I = 2$

Card P(E) = 2

$n = \text{Card } E$	$P(E)$	$\text{Card } P(E)$
0	$\emptyset$	1
1 $E = \{ x_1 \}$ 2 $E = \{ x_1, x_2 \}$	$\emptyset$ $\emptyset$ ou x_2	2 4
$E = \{ x_1, \dots, x_n \}$	$\emptyset$ ou x_n	Hyp Card $P(E_n) = 2^n$
$E_{n+1} = x_1, \dots, x_n, x_{n+1}$	$\emptyset$ ou x_{n+1}	

$$\begin{aligned}\text{Card } P(E_{n+1}) &= 2 \text{ Card } P(E_n) \\ &= 2 \cdot 2^n \\ &= 2^{(n+1)}\end{aligned}$$

L'hypothèse est héréditaire.

Vraie pour $n=0$ donc toujours vraie $\forall n \in \mathbb{N}$

Théorème de Cantor

$$\text{Card } P(E) > \text{Card } E$$

Application :

$$\text{Card } \mathbb{N} = \aleph_0$$

$$2 \cdot \aleph_0 = \aleph_0$$

$$\aleph_0 + 1 = \aleph_0$$

$$\text{Card } P(\mathbb{N}) = 2^{(\text{card } \mathbb{N})}$$

$$\aleph_1 = \text{card } \mathbb{R}$$

$$\exists ? E \text{ dont } \aleph_0 < \text{Card } E < \aleph_1 \quad ==> \quad \text{Hypothèse indécidable}$$

On peut faire une infinité d'ensembles infinis

Chapitre 2 : Application et relation

2.1 - Application : définitions générales

Soient E, F, deux ensembles

on appelle application Phi de E dans F, notée : $\Phi : E \rightarrow F$

une « correspondance » telle que :

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

$$\{(e, f) \in E \times F \mid f = \Phi(e)\} = G \subset E \times F$$

G est le graphe de Phi

e est l'antécédent de f, image de e

E est l'ensemble de départ, F est l'ensemble d'arrivée

$\{\text{appli de E ds F}\} = \mathcal{F}(E, F)$

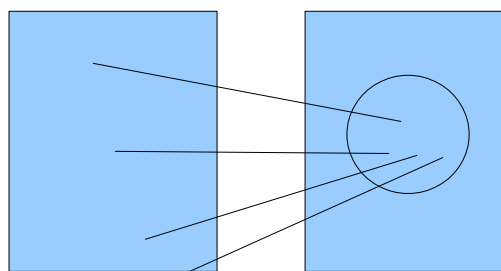
$$\Phi(E) = \{f \in F : \exists e \in E : f = \Phi(e)\}$$

Exemple : $f : \mathbb{N} \rightarrow \mathbb{Q}$ définie par $f(n) = 2n + \frac{1}{2}$
 $f \in \mathcal{F}(\mathbb{N}, \mathbb{Q})$

Egalité : Φ et Ψ $\Psi \in \mathcal{F}(E, F)$ $\Phi = \Psi \Leftrightarrow \forall e \in E, \Phi(e) = \Psi(e)$

Identité : $\forall e \in E \quad \mathcal{I}_{E(e)} = e$

2.2 - Applications particulières



Surjection

Φ est surjective $\Leftrightarrow \Phi(E) = F$

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

Théorème de Cantor :

il n'existe pas de surjection de E sur $\mathcal{P}(E)$

Injection

Φ est injective ssi $\forall (x_1, x_2) \in E^2, x_1 \neq x_2 \Rightarrow \Phi(x_1) \neq \Phi(x_2)$

équivalent à $\Phi(x_1) = \Phi(x_2) \Rightarrow x_1 = x_2, \forall x_1, x_2$

Exemple :

$$f \in \mathcal{F}(\mathbb{N}, \mathbb{Q}) : f(n) = 2n + \frac{1}{2}$$

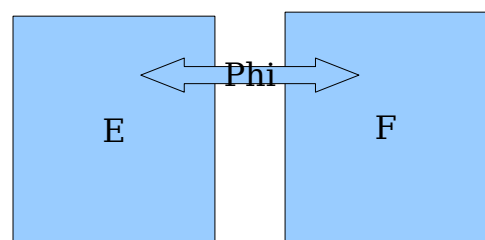
Injective car : $f(n_1) = f(n_2) \Rightarrow 2n_1 + \frac{1}{2} = 2n_2 + \frac{1}{2} \Rightarrow n_1 = n_2$

surjectif : NON. Par exemple, $\frac{1}{3} \in \mathbb{Q}$ mais $f(n) = 2n + \frac{1}{2} = \frac{1}{3}$

Si f est injective et surjective, f est bijective

Φ bijective $\forall f \in F, \exists! x \in E \text{ tq } f = \Phi(x)$

avec $\forall e \in E, \exists! y \in F \text{ tq } y = \Phi(e)$



Phi bijective $\Rightarrow \exists$ application $\Phi^{-1} \in F(F, E) tq \forall y \in F, \exists! x \in E, avec y = \Phi(x)$

On a donc : $x = \Phi^{-1}(y)$

Φ^{-1} est l'application réciproque de Phi et est bijective.

Soit $y = 2x + 3 = f(x)$

Injective : $f(x_1) = f(x_2) \Rightarrow 2x_1 + 3 = 2x_2 + 3$
 $\Rightarrow x_1 = x_2$ donc f injective.

Surjective car : $\forall y \in \mathbb{R}, \exists x \in \mathbb{R} tq x = \frac{(y-3)}{2}$

Lors $f(x) = y$

alors $f^{-1}: f^{-1}(x) = \frac{(x-3)}{2}$

Phi permutation dans $\mathbb{N}_4 \hat{=} \{1, 2, 3, 4\}$

$\Phi(1) = 2 \quad \Phi(2) = 1 \quad \Phi(3) = 4 \quad \Phi(4) = 3$

« « Matrice 1 » »

Phi est bijective

Restriction :

$\Phi \in F(E, F)$ sont E' intersec E

$\Psi \in F(E', F)$ est restriction de Φ a E' ssi

$\forall e \in E', \Psi(e) = \Phi(e)$

On peut noter $\Psi = \Phi|_{E'}$; pour E' et Φ donnés, Ψ est unique.

Proglongement

REPOMPER LE TEXTE !!!!!!!!!!!!!!!

2. composition d'application

« « Image 1 » »

$\forall x \in E, \exists! y \in F tq y = f(x)$

} $\forall x \in E, \exists! z \in G : z = g(f(x))$

$\forall y \in F, \exists! z \in G tq z = g(y)$

donc $\forall h \in F(E, G) tq z = h(x)$

on note $h = g \circ f$ est le produit de composition de f par g

--> La composée de 2 surjection est surjective

--> La composée de 2 injections est injective

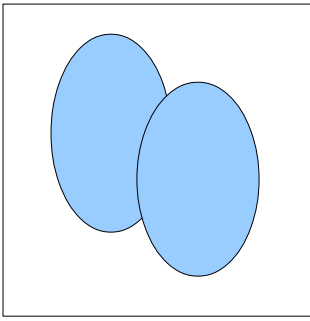
Involution

$f \in F(E, E)$ est involutive ssi $f \circ f = \text{id}_E$

--> Le $\Phi \in \mathbb{N}_4 \hat{=}$ permutation de $\mathbb{N}_4 \hat{=}$ precedent est involutif.

--> La sytmetrie dans $\mathbb{R}^2$ est involutive.

2.4 - Quelques propriétés fondamentales



« Image 2 » »

$$f : E \rightarrow F$$

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

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

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

$$f \text{ injective} \Leftrightarrow f(A \cap B) = f(A) \cap f(B)$$

2.5 - Relations

Soient 2 ensembles A, B

Soit $G \subset A \times B$

G définit une relation R entre $(a, b) \in A \times B$

$(a, b) \in G$, on dit a est relié à b : $a R b$

$(a, b) \notin G$, on dit a n'est pas relié à b

G est le graphe de la relation B

Exemple : $\leq$ dans $\mathbb{R}^2$ $x \leq y$ a pour graphe.

« image 3 » »

Une relation binaire sur E est une relation R sur $E \times E$

Ex : la relation « divise » notée $|$ dans $\mathbb{N}$
définie par : $a | b$ ssi $\exists \lambda \in \mathbb{N} \text{ tq } b = \lambda a$

Réflexivité : $\forall x \in E, x R x$

Symétrie : $x R y \Rightarrow y R x$

Transitivité : $x R y \text{ et } y R z \Rightarrow x R z$

Antisymétrie : $(x R y \text{ et } y R x) \Rightarrow x = y$

L'égalité dans $\mathbb{R}$ est réflexive, symétrique et transitive

L'inclusion dans $\mathcal{P}(E)$ est réflexive, antisymétrique et transitive

L'orthogonalité de 2 droites dans $\mathbb{R}^2$ est symétrique.

2.6 - Relation d'équivalence

R relation dans E est une équivalence ssi R est : Réflexive ET symétrique ET transitive

La similitude de triangles est une équivalence.

Souvent, on note l'équivalence par $\equiv$ ou « alternatif »

On peut préciser : $x \equiv y (R)$ (modulo R)

Classe d'équivalence.

Soit $(E, \equiv)$ Soit $x \in E$

$\overset{\circ}{x} = \{ y \in E \text{ tq } y \equiv x \}$ est la classe d'équivalence de x

alors :

$$\rightarrow x \equiv y \Rightarrow \overset{\circ}{x} = \overset{\circ}{y}$$

L'ensemble des classes d'équivalence dans $(E, \equiv)$ est une partition de E.

On l'appelle ensemble quotient de E par $\equiv$ noté $E/\equiv$

2.7 - Relation d'ordre

R relation définie sur E est une relation d'ordre ssi :

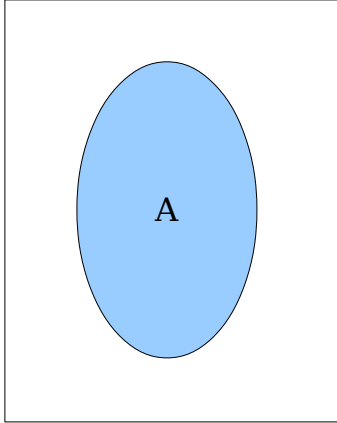
R est réflexive, antisymétrique et transitive.

E est ordonné par R

E est totalement ordonné par R si $\forall x, y \in E \quad xRy \text{ ou } yRx$

On peut noter les ordres par $\leq$

Dans $\mathbb{R}$, $\leq$ est un ordre.



(E, $\leq$) (R ordre)

M est un majorant de A ssi :

$$\forall a \in A, a \leq M$$

m est un minorant de A ssi :

$$\forall a \in A, m \leq a$$

A contient au plus un majorant (minorant).

S'il existe, on l'appelle « plus grand element » de A
de meme pour « plus petit »

Le plus petit des majorants (s'il existe) est la borne Supérieure de A

M est maximal dans A ssi

$$a \in A \text{ et } M \leq a \Rightarrow M = a$$

$$a \in A \text{ et } a \leq m \Rightarrow a = m$$

toute partie non vide de $\mathbb{N}$ admet un plus petit element

2.8 - Application monotone

(A, $\leq$) et (B, $\leq'$)

$$f \in F(A, B)$$

f est croissante ssi : $a_1 \leq a_2 \Rightarrow f(a_1) \leq' f(a_2)$

Chapitre 3 : Nombres Complexes

3.1 - Définitions théoriques

$(\mathbb{R}, +, .)$ est supposé connu

$\mathbb{C} = z$ ou $z = (a, b)$ avec $a, b \in \mathbb{R}$
avec 2 opérations $+$ et $.$

$(\mathbb{C}, +)$ est un groupe abélien

$+$ est une loi de composition interne (LCI)

avec $(x, y) + (x', y') = (x+x', y+y')$

$+$ est associative

$$(z_1 + z_2) + z_3 = z_1 + (z_2 + z_3)$$

$+$ admet un neutre $0 = (0, 0)$ avec $z + 0 = 0 + z = z$
car $(x, y) + (0, 0) = (x+0, y+0) = (x, y)$

$\forall z = (x, y) \in \mathbb{C}, \exists$ symétrique de z noté $-z$ tel que $z + (-z) = (-z) + z = 0$
avec $-z = (-x, -y)$

et $+$ est commutative ($\Leftrightarrow$ abélien) $z + z' = z' + z$

On définit une deuxième loi, multiplication dans $\mathbb{C}$ notée $.$ définie par

$$z_1 \cdot z_2 = (x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1)$$

- est une LCI

- est associative $z_1 \cdot (z_2 \cdot z_3) = (z_1 \cdot z_2) \cdot z_3$

- est distributive $z_1 \cdot (z_2 + z_3) = z_1 \cdot z_2 + z_1 \cdot z_3$ et $(z_1 + z_2) \cdot z_3 = z_1 \cdot z_3 + z_2 \cdot z_3$

- admet un neutre $(1, 0)$ noté 1

- admet un inverse noté z^{-1} pour tout $z \neq (0, 0) = 0$ avec $z \cdot z^{-1} = z^{-1} \cdot z = 1$ $z^{-1} = \frac{x}{x^2 + y^2} - \frac{y}{x^2 + y^2}i$

- est commutative

$(\mathbb{C}, +, .)$ est un corps commutatif

On a donc :

$$1 = (1, 0) \in \mathbb{C} \text{ a donc symétrique } -1 = (-1, 0)$$

Remarque $(0, 1) \cdot (0, 1) = (-1, 0) = -1$
on appelle $(0, 1)$ $i \in \mathbb{C}$ $i \cdot i = -1 = i^2$

On définit une 3ème équation toujours notée .

$$\forall \lambda \in \mathbb{R} \quad \forall z = (x, y) \in \mathbb{C} \rightarrow z' = \lambda \cdot z = (\lambda x, \lambda y)$$

alors

$$z = (x, y) = (x, 0) + (0, y) = x \cdot (1, 0) + y \cdot (0, 1) = x \cdot 1 + y \cdot i$$

z est noté $z + iy$ notation algébrique des complexes.

3.2 - Représentation algébrique des complexes.

$\mathbb{C} = \{z\}$ $z = (x, y)$ noté $z = x + iy$ avec $i^2 = -1$

et

$$z_1 + z_2 = (x_1 + iy_1) + (x_2 + iy_2) = x_1 + x_2 + i(y_1 + y_2)$$

$$z_1 \cdot z_2 = x_1 x_2 - y_1 y_2 + i(x_1 y_2 + x_2 y_1)$$

$z = x + iy$ sym $z = -z = -x - iy$

$$\text{si } z \neq 0 \text{ inverse de } z = z^{-1} = \frac{x}{x^2 + y^2} - \frac{iy}{x^2 + y^2}$$

partie réelle de $z = R(z) = x$

Partie imaginaire de $z = Ym(z) = y$

Si $\Re(z)=0$, z est « imaginaire pur »

Si $\Im(z)=0$, z est un réel

Conjugué de $z = \bar{z} = x - iy$

$\rightarrow z = \bar{z} \Leftrightarrow z \in \mathbb{R}$

$\rightarrow z + \bar{z} = 2\Re(z) \quad z - \bar{z} = 2\Im(z)$

$\rightarrow z + z' = \bar{z} + \bar{z}' \quad ; \quad z \cdot \bar{z}' = \bar{z} \cdot z' \quad \text{et} \quad \frac{z}{z'} = z \cdot \frac{1}{z'} = z \cdot (z')^{-1}$

3.2.1 - interprétation géométrique

« « schema 1 » »

$z = x + iy \rightarrow M \in O_x, O_y$ avec $M(x, y)$

on dit z est l'afixe de M

$\rho = ||\vec{OM}||$ est le module de z noté $|z|$

$z = x + iy \Rightarrow |z| = \sqrt{x^2 + y^2} = \rho$

$\theta = (Ox, \vec{OM})$ est l'argument de z noté $\arg z$, défini à 2π près

$\rightarrow |z| = \sqrt{x^2 + y^2} \Rightarrow |z|^2 = z \cdot \bar{z}$

$\rightarrow \Re(z) \leq |z| \quad |\Im(z)| \leq |z| \quad \text{et} \quad |z| \leq |\Re(z)| + |\Im(z)| \Rightarrow |z|^2 \leq (|x| + |y|)^2 = x^2 + y^2 + 2|x||y| \Rightarrow \text{VRAI}$

Inégalité triangulaire

$|z + z'| \leq |z| + |z'|$ car

$|z + z'|^2 = (z + z')(z + z') = (z + z')(\bar{z} + \bar{z}') = z\bar{z} + z'\bar{z}' + z\bar{z}' + \bar{z}z' = |z|^2 + |z'|^2 + z\bar{z}' + \bar{z}z'$

Posons $Z = z\bar{z}'$ et $t = Z + \bar{Z} \in \mathbb{R}$
 $t = Z\Re(Z) \leq 2|Z|$

$|Z| = |z\bar{z}'| = |z| \cdot |\bar{z}'| = |z| \cdot |z'|$

Donc, $|z + z'| \leq \sqrt{|z|^2 + |z'|^2 + 2|z||z'|} = (|z| + |z'|)^2$

$|z| = \text{module de } z = |-z| = |\bar{z}|$

$z \neq 0 \quad z^{-1} = \frac{\bar{z}}{|z|^2}$

$z = x + iy = \rho(\cos(\theta) + i\sin(\theta))$

On note $e^{i\theta} = \cos(\theta) + i\sin(\theta)$

$e^{i0} = 1 = e^{i2\pi} \quad e^{i\pi} = -1$

$z = \rho e^{i\theta}$ noté $[\rho, \theta] = z$ « représentation trigonométrique de z »

alors $\bar{z} = [\rho, -\theta] = \rho e^{-i\theta}$

$z^{-1} = \frac{\bar{z}}{|z|^2} = \rho \frac{(\cos(\theta) - i\sin(\theta))}{\rho^2} = \frac{1}{\rho} e^{-i\theta} = [\frac{1}{\rho}, -\theta]$

Produit

$z_1 = \rho_1 e^{i\theta_1} \quad z_2 = \rho_2 e^{i\theta_2}$

$z_1 z_2 = \rho_1 \rho_2 e^{i\theta_1} * e^{i\theta_2}$

$z_1 z_2 = \rho_1 \rho_2 e^{i(\theta_1 + \theta_2)}$

$\arg(z_1 z_2) = \arg(z_1) + \arg(z_2)$

3.3 - Représentation trigonométrique

$$[\rho_1, \theta_1] \cdot [\rho_2, \theta_2] = [\rho_1 \rho_2, \theta_1 + \theta_2]$$

en particulier

$$(e^{i\theta})^n = e^{in\theta}$$

$$(\cos(\theta) + i\sin(\theta))^n = \cos n\theta + i\sin n\theta$$

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

3.4 - Racines n-ieme des nombres complexes

Soit $\lambda \in \mathbb{C}$ fixé. On cherche $z \in \mathbb{C}$ tq $z^n = \lambda$

Résolution trigonometrique :

$$\lambda = r(\cos \alpha + i\sin \alpha) \quad \text{on cherche } z = \rho e^{i\theta} \quad p \text{ et } r \in \mathbb{R}^{+}$$

$$\rho^n e^{in\theta} = r e^{i\alpha}$$

$$\rho^n = r \quad \rho = r^{\frac{1}{n}}$$

$$n\theta = \alpha + 2k\pi \quad \theta = \alpha + \frac{2k\pi}{n}, \forall k \in \mathbb{Z}$$

$$z_k = r^{\frac{1}{n}} e^{i(\alpha + \frac{2k\pi}{n})} \quad k \in [0, 1, 2, \dots, n-1]$$

Il y a donc n racines distinctes, de même module.

3.4.1 - Racine n-ieme de l'unité $n\sqrt{1}$

$$N = 1 \quad 1\sqrt{1} = z_1 = 1$$

$$n = 2 \quad z^2 = 1 \quad z_1 = 1 \quad z_2 = -1 \\ z_1 + z_2 = 0$$

$$n = 3 \quad z^3 = 1 \quad z = 1 \cdot e^{\frac{i2k\pi}{3}} \quad k \in (0, 1, 2) \\ z_1 = 1 \quad z_2 = e^{\frac{i2\pi}{3}} \quad z_3 = e^{\frac{i4\pi}{3}} \\ z_2 = \frac{-1}{2} + \frac{i\sqrt{3}}{2} = j \quad z_3 = \frac{-1}{2} - i\frac{\sqrt{3}}{2} = j^2 = \bar{j} \quad 1 + j + j^2 = 0$$

$$n = 4 \quad z^4 = 1 \quad z_4 = e^{\frac{i2k\pi}{4}} \quad k \in (0, 1, 2, 3) \\ z_1 = 1 \quad z_2 = i \quad z_3 = -1 \quad z_4 = -i \quad z_1 + z_2 + z_3 + z_4 = 0$$

3.4.2 - Racine carrée d'un complexe

Soit $\lambda = x + iy$ connu, $y \neq 0$

On cherche $z = a + ib$ tq $z^2 = \lambda = (a + ib)^2 = a^2 - b^2 + 2iab$

d'ou :

$$a^2 - b^2 = x \quad \text{Posons } b = \frac{y}{2a} \quad (\text{a et b sont non nuls car } y \neq 0)$$

$$2ab = y$$

$$\text{d'où : } a^2 - \frac{y^2}{4a^2} = x \quad 4a^4 - y^2 = 4a^2 x$$

$$\text{Soit : } 4a^4 - 4xa^2 - y^2 = 0 \quad (\text{équation bicarrée à coeff. constant négatif. Si on n'a pas ça, on s'est planté})$$

$$\text{Posons } A = a^2 : \quad 4A^2 - 4xA - y^2 = 0$$

$$A = \frac{4x + \sqrt{16x^2 + 16y^2}}{8} = \frac{x + \sqrt{x^2 + y^2}}{2} = a^2$$

$$a_1 = +\sqrt{\frac{x + \sqrt{x^2 + y^2}}{2}} \quad a_2 = -\sqrt{\frac{x + \sqrt{x^2 + y^2}}{2}}$$

$$b_1 = \frac{y}{2a_1} \quad b_2 = \frac{y}{2a_2}$$

$$\text{D'où : } z_1 = \dots \quad z_2 = \dots \quad z_2 = -z_1$$

3.4.3 - Racine carrée d'un nombre complexe

$$\sqrt{-5 - 12i} = a + ib$$

$$\text{d'où : } a^2 - b^2 = -5 \quad b = \frac{-6}{a} \quad \text{d'où : } a^4 + 5a^2 - 36 = 0$$

$$ab = -6 \quad \text{et } a^2 - \frac{36}{a^2} = -5 \quad a^2 = \frac{-5 + \sqrt{25 + 144}}{2} = \frac{-5 + 13}{2} = 4$$

$$a_1 = 2 \quad b_1 = \frac{-6}{2} = -3 \quad z_1 = 2 - 3i$$

$$a_2 = -2 \quad b_2 = \frac{-6}{-2} = +3 \quad z_2 = -2 + 3i$$

3.5 - Résolution des équations du 2eme degré dans $\mathbb{C}$

$$aZ^2 + bZ + c = 0 \quad a \neq 0 \quad a, b \text{ et } c \in \mathbb{C}$$

$$\text{d'où } Z^2 = -\frac{b}{a}Z - \frac{c}{a} = 0$$

$$\left(Z + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} - \frac{c}{a} = 0$$

$$\left(Z + \frac{b}{2a}\right)^2 = \frac{b^2}{4a^2} + \frac{c}{a} = \frac{b^2 - 4ac}{4a^2}$$

$$Z + \frac{b}{2a} = \pm \sqrt{\frac{b^2 - 4ac}{4a^2}}$$

$$Z = -\frac{b}{2a} \pm \sqrt{\frac{b^2 - 4ac}{4a^2}}$$

$$Z = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \quad 2 \text{ solutions : } Z_1 \text{ et } Z_2 \quad Z_1 + Z_2 = -\frac{b}{a} \quad Z_1 Z_2 = \frac{c}{a}$$

??? 3.4.3 - Racine carrée d'un complexe :

Si 2 nombres complexes ont pour somme S et pour produit P, ils sont racines de $Z^2 - SZ + P = 0$

Ex : $z^2 - (4+3i)z + 13(1+i) = 0$

$$\Delta = (4+3i)^2 - 52(1+i) = 16 - 9 + 24i - 52 - 52i = -45 - 28i$$

$$\sqrt{\Delta} = a + ib$$

$$a^2 - b^2 = -45 \quad b = \frac{-14}{a} \text{ et } a^2 - \frac{196}{a^2} = -45 \Rightarrow a^2 + 45a^2 - 196 = 0$$

$$ab = -14$$

$$S = 2025 + 800 - 16 = 2809 = 53^2 \quad (\text{ouf... o_O})$$

$$a^2 = \frac{-45 + 53}{2} = 4 \quad a_1 = 2 \quad b_1 = -7$$

$$a_2 = -2 \quad b_2 = 7$$

$$\sqrt{\Delta} = \pm(2 - 7i)$$

$$z = \frac{4 + 3i \pm (2 - 7i)}{2}$$

$$z_1 = 3 - 2i \quad z_2 = 1 + 5i$$

$$\text{verif : } z_1 + z_2 = 4 + 3i \text{ niceeeee! Rofl :-/}$$

Equation du 3eme degré puis 4eme degré puis 5eme degré.

3.6 - Propriétés géométriques

« « SCHEMA 15 » »

$$z' = x' + iy' \quad z' = z + c$$

$$x' = x + c_x$$

$$y' = y + c_y$$

Rotation $Rot_{0,\theta}$

« « SCHEMA 16 » »

$$M' = Rot_{0,\theta}(M) \quad \text{La rotation } 0,\theta \text{ correspond a une multiplication par } e^{i\theta}$$

$$z' = z \cdot e^{i\theta}$$

Alignement de 3 points $M_1 M_2 M_3$

« « SCHEMA 16 » »

$M_1 M_2 M_3$ alignés

$$\Leftrightarrow \arg(z_2 - z_1) = \arg(z_3 - z_1) [\pi]$$

$$\Leftrightarrow \arg(z_2 - z_1) = 0 [\pi]$$

$$\Leftrightarrow \arg \frac{z_2 - z_1}{z_3 - z_1} = 0 [\pi]$$

$$M_1 M_2 M_3 \text{ alignés} \Leftrightarrow \frac{z_2 - z_1}{z_3 - z_1} \in \mathbb{R}$$

Cocyclité de 4 points

« « SCHEMA 17 » »

$$\text{angle}(M_1 \vec{M}_2, M_1 \vec{M}_4) = \text{angle}(M_2 \vec{M}_3, M_3 \vec{M}_4)$$

$$\arg(z_4 - z_1) - \arg(z_3 - z_1) = \arg(z_4 - z_2) - \arg(z_3 - z_2) [\pi]$$

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

$$arg(\frac{\frac{z_4-z_1}{z_3-z_1}}{\frac{z_3-z_1}{z_4-z_2}})=0[\pi] \qquad \Rightarrow \qquad \frac{\frac{z_4-z_1}{z_3-z_1}}{\frac{z_3-z_1}{z_4-z_2}} \in \mathbb{R} \quad M_1M_2M_3M_4 \text{ cocycliques}$$

Chapitre 4 : Polynomes

4.1 - Définitions

K est un corps ($\mathbb{R}$ ou $\mathbb{C}$)

l'ensemble des polynomes P est noté $K[X]$

P est une suite presque partout nulle de $coeff \in K$

$P = (p_0, p_1, p_2, \dots, p_n, 0, \dots)$ ou $P_n \neq 0$

on pose le degré de P = n

$[0] = [0, 0, \dots, 0, \dots]$

Addition $P = (p_0, p_1, p_2, \dots, p_n, 0, 0, 0, \dots)$ $Q = (q_0, q_1, q_2, \dots, q_n, 0, 0, 0, \dots)$
 $S = P + Q = ((p_0 + q_0, p_1 + q_1, \dots, p_l + q_l, 0, 0, 0, \dots))$ $l = \sup(n, m)$

$$d^0 P = n \quad d^0 Q = m$$

$$d^0 S \leq \max(n, m) < 3$$

($K[x]$, +) est un groupe abélien. Neutre est [0] et $\text{sym}[(p_0, \dots, p_n, 0, 0, \dots)] = (-p_0, \dots, -p_n, 0, 0, \dots)$

Multipli. $P = (p_0, p_1, p_2, \dots, p_n, 0, 0, 0, \dots)$ $Q = (q_0, q_1, q_2, \dots, q_n, 0, 0, 0, \dots)$

$R = P \cdot Q = \ll \text{produit de P par Q} \gg$

$$R = (r_0, \dots, r_j, \dots, r_l) \quad \text{avec} \quad \begin{aligned} r_0 &= p_0 q_0 \\ r_1 &= p_0 q_1 + p_1 q_0 \\ r_2 &= p_0 q_2 + p_1 q_1 + p_2 q_0 \\ &\dots\dots\dots \\ r_l &= p_n q_m \end{aligned}$$

$$d^0(PQ) = d^{0P} + d^{0Q} < 3$$

Le produit est :
interne
associatif
distributif par rapport a l'addition
existe neutre 1 = (1, 0, 0, 0, ...)
commutatif

($K[x]$, +, .) est un anneau commutatif

Multiplication par un scalaire ($\lambda \in K$)

$$P = (p_0, p_1, \dots, p_n) \quad X^2 = (0, 0, 1, 0, 0, 0, \dots) \\ \lambda P = (\lambda p_0, \lambda p_1, \dots, \lambda p_n) \quad \lambda \in K \quad X^n = (\dots n \text{ zéros} \dots, 1, 0, \dots)$$

alors :

$$\begin{aligned} P &= (p_0, p_1, \dots, p_n) \\ 1 &= (1, 0, \dots) \\ X &= (0, 1, 0, 0, \dots) \\ P &= p_0(1, 0, \dots) + p_1(0, 1, 0, \dots) + \dots + p_n(0, 0, \dots, 1, 0) \\ P &= p_0 \cdot 1 + p_1 \cdot X + p_2 \cdot X^2 + \dots + p_n X^n \end{aligned}$$

Notation polynomiale $\Leftrightarrow f(x) = p_0 + p_1 x + \dots + p_n x^2$ (fonction polynomiale)

4.2 - Division Euclidienne

Soient A et B deux polynomes avec $B \neq 0$

Il existe un seul couple Q et R tq :

$$A = BQ + R \quad \text{avec} \quad d^0 R < d^0 B$$

on appelle respectivement Q et R le quotient et le reste de la division Euclidienne de A par B

$$\text{ex : } A = x^4 + 1 \quad B = x^2 + x + 1$$

« « SCHEMA 18 » »

$$x^4 + 1 = (x^2 + x + 1)(x^2 - x) + x + 1$$

$$A = B * Q + R$$

$$A = x^5 - 7x^3 + x - 6$$

$$B = x^3 + x^2 - x - 1$$

« SCHEMA 19 » »

4.10 - Racines d'un polynome

Factorisation dans $\mathbb{C}$

$$P(z) = A(z - z_1)^{\alpha_1} \dots (z - z_k)^{\alpha_k}$$

z_i racine de multiplicité α_i

4.11 - Factorisation dans $\mathbb{R}$

Si z_1 est une racine complexe, alors $\bar{z}_i$ est aussi une racine de $P(z)$ car :

$$P(z) = a_n z^n + \dots + a_1 z + a_0 \quad \text{avec } a_i \in \mathbb{R}$$

alors : $P(\bar{z}) = \overline{P(z)}$

$$(z - z_i)(z - \bar{z}_i) = z^2 - (z_i + \bar{z}_i)z + z_i \bar{z}_i$$

Dans $\mathbb{R}$ $\mathbb{R}$ $\mathbb{R}$

$$P(z) = A(z - r_1)^{\alpha_1} \dots (z - r_j)^{\alpha_j} (z^2 + p_1 z + q_1)^{\beta_1} \dots (z^2 + p_l z + q_l)^{\beta_l}$$

$A = \text{Cste } \mathbb{R}$ pour les j racines réelles de $P(z)$ \underline{\hspace{2cm}} /
pour les l couples de racines cplx

Factorisation irréductible dans $\mathbb{R}$

Ex : Factoriser $P(x) = x^4 - x$

$$P(x) = x(x^3 - 1) \quad \text{Factorisation de } P \text{ dans } \mathbb{C} : P = x(x-1)(x-j)(x-\bar{j})$$

$$\mathbb{R} : P = x(x-1)(x^2 + x + 1)$$

4.12 - Multiplicité des racines

z_i est racine multiple d'ordre α_i de $P(z)$

ssi $P(z) = (z - z_i)^{\alpha_i} Q(z)$ avec $Q(z_i) \neq 0$

alors si $\alpha_i > 1$

$$P'(z) = \alpha_i (z - z_i)^{\alpha_i - 1} Q(z) + (z - z_i)^{\alpha_i} Q'(z)$$

$$P'(z) = (z - z_i)^{\alpha_i - 1} (\alpha_i Q(z) + (z - z_i) Q'(z))$$

$$\underline{\hspace{2cm}} Q_1(z) \underline{\hspace{2cm}}$$

z_i est racine multiple d'ordre $\alpha_i - 1$ de $P'(z)$

Conclusion :

$$z_i \text{ racine multiple d'ordre } k \text{ de } P(z) \Leftrightarrow P(z) = (z - z_i)^k Q(z) \quad Q(z_i) \neq 0$$

$$\Rightarrow P(z_i) = 0 = P'(z_i) = P''(z_i) = \dots = P^{(k-1)}(z_i) \neq P^{(k)}(z_i) \quad \text{et réciproquement}$$

Formule de Taylor appliquée en z_i :

$$P(z) = P(z_i) + \frac{z-z_i}{1!} P'(z_i) + \dots + \frac{(z-z_i)^{k-1}}{(k-1)!} P^{(k-1)}(z_i) + \frac{(z-z_i)^k}{k!} P^{(k)}(z_i) + \dots + \frac{(z-z_i)^n}{n!} P^{(n)}(z_i)$$

$$\frac{(z-z_i)^k}{k!} P^{(k)}(z_i) + \dots + \frac{(z-z_i)^n}{n!} P^{(n)}(z_i) = 0$$

$$P(z) = (z-z_i)^k \left[\frac{P^{(k)}(z_i)}{k!} + \dots + \frac{(z-z_i)^{n-k}}{n!} P^{(n)}(z_i) \right] \quad [] = Q(z) \quad Q(z_i) \neq 0$$

Exemple 1 :

Montrer que $P(x) = 1 + \frac{x}{1} + \frac{x^2}{2!} + \dots + \frac{x^n}{n!}$ n'a pas de racines multiples.

Supposons a racine au moins double de P(x)

alors $P(a) = 0$ et $P'(a) = 0$

$$\text{or} \quad P'(x) = 1 + \frac{2x}{2!} + \frac{3x^2}{3!} + \dots + \frac{nx^{n-1}}{n!}$$

$$\text{soit} \quad P'(x) = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \dots + \frac{x^{n-1}}{(n-1)!}$$

$$\text{alors} \quad P(a) = 0 \quad \text{et} \quad P'(a) = 0 \quad P(a) - P'(a) = \frac{a^n}{n!} = 0$$

donc $a > 0$ or $P(0) \neq 0$

donc 0 n'est pas racine, donc pas de racine multiple.

$$P(x) = x^5 - x^3 - 4x^2 - 3x - 2$$

a factoriser.

$$P(1) = 1 - 1 - 4 - 3 - 2 \neq 0$$

$$P(-1) = -1 + 1 - 4 + 3 - 2 = -3 \quad \text{bof...}$$

$$P(2) = 32 - 8 - 16 - 6 - 2 = 0 \quad \text{ouf !}$$

Mise en facteurs par division euclidienne

« « SCHEMA 30 » »

$$P(x) = (x-2)(x^4 + 2x^3 + 3x^2 + 2x + 1)$$

$$\frac{(x-2)}{Q(x)} \quad \text{Pas de racine « évidente » réelle}$$

$$Q(1) \neq 0 \quad Q(-1) \neq 0$$

$$Q(i) = 1 - 2i - 3 + 2i + 1 = -1$$

$$Q(5) = 5 + 2 + 3j^2 + 2j + 1 = 3j^2 + 3j + 3$$

$$= 3(j^2 + j + 1)$$

$$= 0$$

$$\text{Or} \quad (x-j)(x-\bar{j}) = x^2 - \bar{j}x - jx + 1$$

$$x^2 - x(\bar{j}+j) + 1$$

$$x^2 - x(-1) + 1$$

$$x^2 + x + 1$$

« « SCHEMA 31 » »

$$P(x) = (x-2)(x^2 + x + 1)^2 = (x-2)(x-j)^2(x-\bar{j})^2$$

$$\frac{(x-2)}{\mathbb{R}} \quad \frac{(x-j)^2(x-\bar{j})^2}{\mathbb{C}}$$

4.13 - Relation entre racines et coefficients

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$$P(x) = a_n (x-r_1)(x-r_2) \dots (x-r_n) \quad (\text{les } n \text{ racines sont réelles ou complexes, simples ou multiples})$$

$$P(x) = a_n(x^4 - (r_1 + r_2 + \dots + r_n)x^{n-1} + (r_1r_2 + \dots + r_{n-1}r_n)x^{n-2} + \dots + (-1)^n r_1 \dots r_n)$$

$$\text{d'où : } S_1 = r_1 + r_2 + \dots + r_n = \frac{-a_{n-1}}{a_n}$$

$$S_2 = \sum_{1 \leq i < j \leq n} r_i r_j = \frac{+a_{n-2}}{a_n}$$

$$S_n = P = r_1 r_2 \dots r_n = (-1)^n \frac{a_0}{a_n}$$

cas particulier : $n=2$ $ax^2 + bx + c = 0$

$$S = r_1 + r_2 = \frac{-b}{a} \quad r_1 r_2 = \frac{c}{a} = P$$

Deux nombres dont la somme est S et le produit P sont racines de $X^2 - SX + P = 0$

Application : recherche des racines « évidentes »

$$a_n x^n + \dots + a_1 x + a_0 = 0$$

quelles sont les racines rationnelles $\frac{p}{q}$ avec $p \wedge q = 1$

$$a_n \frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \dots + a_1 \frac{p}{q} + a_0 = 0$$

$$a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n = 0$$

$$a_n p^n = q(-a_{n-1} p^{n-1} - \dots - a_1 q^{n-1})$$

$$q \mid a_n p^n \quad \text{or } q \wedge p = 1 \quad \text{donc } q \wedge p^n = 1$$

donc (th de Gauss) : $q \mid a_n$

Th de Gauss : $A \mid BC$ et $A \wedge B = 1$
 $\Rightarrow A \mid C$

de meme : $a_0 q^n = p(-a_n p^{n-1} - \dots - a_1 q^{n-1})$ or $p \wedge q^n = 1 \Rightarrow p \mid a_0$

racines a essayer : ± 1 ; ± 7 ; $\pm 1/3$; $\pm 7/3$

Chapitre 5 - Fonctions rationnelles dans $\mathbb{R}[x]$

Soit $F(x) = \frac{P(x)}{Q(x)}$ ou P et Q sont 2 polynomes

1ere étape $d^\circ P \geq d^\circ Q$ on divise P par Q.
On trouve le quotient E(x) et le reste R(x).

$$P = EQ + R \quad d^\circ R < d^\circ Q$$

$$F = \frac{EQ + R}{Q}$$

$$F = E + \frac{R}{Q} \quad E \text{ est la partie entiere de la fraction rationnelle } d^\circ R < d^\circ Q$$

2eme étape On étudie $\frac{R}{Q}$ (donc PGCD de R et de Q)

$$\text{Soit } D = R \wedge Q \quad \begin{matrix} R = G.N \\ Q = G.D \end{matrix}$$

$$\frac{R}{Q} = \frac{N}{D} \text{ ou } N \wedge D = 1$$

3eme étape Simplification de $\frac{N}{D}$ ou $d^\circ N < d^\circ D$
et $N \wedge D = 1$

On détermine les racines de D appelées les pôles de la fraction rationnelle.
et on a ainsi la factorisation irréductible de D ds $\mathbb{R}[X]$

$$D = \alpha \underbrace{(x-a)^m \dots (x-a)^m}_{\text{Racines usuelles}} \underbrace{(x^2+px+q)^k \dots (x^2+px+q)^k}_{\text{Racines complexes}}$$

$$\text{Alors, } \frac{N}{D} = \underbrace{\frac{A_1}{x-a} + \frac{A_2}{(x-a)^2} + \dots + \frac{A_m}{(x-a)^m}}_{\substack{\text{elements de la 1ere espece} \\ \text{pour le pôle a}}} + \dots + \underbrace{\frac{B_1 x + C_1}{x^2+px+q} + \frac{B_2 x + C_2}{(x^2+px+q)^2} + \dots + \frac{B_k x + C_k}{(x^2+px+q)^k}}_{\substack{\text{idem} \\ \text{pour autres} \\ \text{pôles réels.}}} + \dots + \underbrace{\dots}_{\substack{\text{éléments de la 2eme espece} \\ \text{autres} \\ \text{éléments de la} \\ \text{2eme espece}}}$$

Exemple : $F(x) = \frac{x^5 - x^4 - 19x^3 + 49x^2 - 29x + 5}{x^4 - x^3 - 19x^2 + 49x - 30}$

1ere étape : calcul de la partie entière

$x^5 - x^4 - 19x^3 + 49x^2 - 29x + 5$	$x^4 - x^3 - 19x^2 + 49x - 30$
$x^5 - x^4 - 19x^3 + 49x^2 - 30x$	x
$x + 5$	

$$F(x) = x + \frac{x+5}{x^4 - x^3 - 19x^2 + 49x - 30}$$

x = partie entière E(x)

$$\text{reste} = \frac{R}{Q}$$

$$\begin{matrix} x^4 - x^3 - 19x^2 + 49x - 30 \\ -(x^4 + 5x^3) \end{matrix}$$

Etape 1 : recherche de la partie entière

Etape 2 : recherche du PGCD de $\frac{R}{Q}$

$x^4 - x^3 - 19x^2 + 49x - 30$	$x + 5$
$x^4 + 5x^3$ $-6x^3 - 19x^2 + 49x - 30$ $-6x^3 - 30x^2$ $11x^2 + 49x - 30$ $11x^2 + 55x$ $-6x - 30$ $-6x - 30$	$x^3 - 6x^2 + 11x - 6$

Etape 3 : recherche des pôles ; factorisation du dénominateur.

Essai des diviseurs de -6

$x = 1$ est racine

Etape 4 : Ecrire la forme réduite générale

$$\frac{A}{B} = \frac{a}{x-1} + \frac{b}{x-2} + \frac{c}{x-3} = \frac{1}{(x-1)(x-2)(x-3)}$$

Etape 5 : calcul en coefficients

Bourrin :

$$a(x-2)(x-3) + b(x-1)(x-3) + c(x-1)(x-2) = 1$$

$$a(x^2 - 5x + 6) + b(x^2 - 4x + 3) + c(x^2 - 3x + 2) = 1$$

$$(a+b+c)x^2 + (-5a-4b-3c)x + 6a+3b+2c = 1$$

$$\begin{array}{lll} a+b+c=0 & a=-b-c & \\ 5a+4b+3c=0 & -5b-5c+4b+3c=0 & -b-2c=0 \\ 6a+3b+2c=1 & -6b-6c+3b+2c=1 & -3b-4c=1 \end{array}$$

d'ou $b = -2c$ et $6c - 4c = 1 = 2c$ d'ou $c = \frac{1}{2}$

et $b = -2 \cdot \frac{1}{2} = -1$ et $a = +1 - \frac{1}{2} = \frac{1}{2}$

$$\frac{A}{B} = x + \frac{1}{2(x-1)} - \frac{1}{(x-2)} + \frac{1}{2(x-3)}$$

+ malin : $\frac{1}{(x-1)(x-2)(x-3)} = \frac{a}{x-1} + \frac{b}{x-2} + \frac{c}{x-3}$ je multiplie par $x-2$ puis $x=2$

$$\frac{1}{(2-1)(2-3)} = -1 = b \quad \text{et de même} \quad \frac{1}{2}(1) = c$$

Chapitre 6 : Dénombrement

6.1 Cardinal d'un ensemble

On dit que 2 ensembles A et B ont « meme puissance » ou qu'ils sont équipotents ssi il existe une bijection entre A et B

On écrit alors $\text{card}(A) = \text{card}(B)$ ou $|A| = |B|$

→ L'équipotence est une relation d'équivalence

- on dit que $\text{card}(A) \leq \text{card}(B)$ ssi il existe une injection de A dans B

- On pose $\text{card} \{1, 2, 3, \dots, n\} = n$

- On dit que E est fini ssi $\exists n \in \mathbb{N} \text{ tq } \text{card}(E) = n$

→ Si E et F sont finis, $\text{card}(E * F) = \text{card } E \cdot \text{card } F$

- E est dénombrable ssi $\text{card } E = \text{card } \mathbb{N}$

- On pose $\text{card } \mathbb{N} = \aleph_0$ (aleph zéro)

Si E et F sont dénombrables, $E * F$ est dénombrable

$$\aleph_0 \cdot \aleph_0 = \aleph_0$$

Ex : Il existe une bijection entre $\mathbb{N}$ et $\mathbb{N}^2$

→ $\mathbb{Q} = \mathbb{Z} \cdot \mathbb{N}^*$ est dénombrable

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

Théorème de Cantor : $\text{card } P(E) > \text{card } E$

$$\text{card } P(\mathbb{N}) = \aleph_1 > \aleph_0$$

Hypothèse du continu : $\text{card } \mathbb{R} = \aleph_1$ et on ne saura jamais s'il existe un ensemble de cardinale entier $\aleph_0$ et $\aleph_1$

6.2 - Nombre d'applications de E ds F (finis)

$$E_p = e_1, e_2, \dots, e_p \quad F_n = f_1, f_2, \dots, f_n$$

{Application de E dans F} = $G(E, F)$

Hyp : $\text{card } G(E_p, F_n) = n^p$

$$\rightarrow \text{card } G(E, F) = \text{card } F^{\text{card } E}$$

car : par récurrence sur p :

Initialisation p=1

chaque appli. est définie par l'image de e_1

donc n choix possibles. L'hypothese est vraie pour p = 1

Supposons l'hypothese vraie au rang p

$$\text{card } G(E_{p+1}, F_n) = \text{card } G(E_p, F_n) \cdot \text{nb choix pour image de } e_{p+1}$$

$$\text{card } G(E_{p+1}, F_n) = n^p \cdot n = n^{p+1}$$

l'hypothèse est héréditaire, donc tjrs vrai.

rac.

6.3 - Arrangements

Soit ϕ injection de E_p dans F_n , ce qui impose $0 < p \leq n$

Les $\phi(e_i)$ sont tous distincts et forment une liste ordonnée de p éléments pris parmi les n elements de F_n , n appelée arrangement.

Soit A_n^p le nb des arrangements de p elements parmi n

A_n^p = nb d'injection de E_p dans F_n

Si $p=1$, $E_1 \rightarrow$ injection $\rightarrow F_n$ $A_n^1 = n$

Supposons connu A_n^{p-1} = nb injection E_{p-1} dans F_n

$$A_n^p = A_n^{p-1} (n-(p-1))$$

$$A_n^p = (n-p+1) A_n^{p-1}$$

$$A_n^{p-1} = (n-p+2) A_n^{p-2}$$

Soit : ...

$$A_n^2 = (n-1) A_n^1$$

$$A_n^1 = n$$

d'où $A_n^p = n(n-1)(n-2)\dots(n-p+1)$ = card{ injection de E_p dans F_n }

$\underbrace{\hspace{10em}}$
p termes décroissants à partir de n = Nb de listes ordonnées sans répétition de p object parmi n

cas particulier : $p = n$ alors l'injection de E dans F est aussi surjective.
dc bijective

Nb de bijections de E_n dans F_n est $A_n^n = n(n-1)\dots(2)(1)$

Posons $n! = 1*2*\dots*(n-1)n$ avec $0! = 1$ par convention

alors $A_n^p = \frac{n!}{(n-p)!} \quad \forall p \leq n$ cas particulier : $E_n = F_n$

les bijections de E_n dans E_n s'appellent des permutations

Nb permutations de $E_n = n!$

6.4 Combinaison

Soit $F = \{f_1, f_2, \dots, f_n\}$ on appelle combinaison une liste sans ordre, sans répétition de p elements
parmi les f_i
($p \leq n$)

Le nb de ces combinaisons est noté $C_n^p = \binom{n}{p}$

$$A_n^p = p! C_n^p \quad \text{soit} \quad C_n^p = \frac{n!}{p!(n-p)!} \quad 0 \leq p \leq n$$

$$C_n^p = \frac{n(n-1)\dots(n-p-1)}{p!} \quad \text{avec } n(n-1)\dots(n-p-1) = p \text{ termes}$$

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

$$\rightarrow C_n^p = C_{n-1}^p + C_{n-1}^{p-1} \quad 0 < p \leq n$$

$$\text{car : } C_{n-1}^p + C_{n-1}^{p-1} =$$

$$\frac{(n-1)!}{p!(n-1-p)!} + \frac{(n-1)!}{(p-1)!(n-p)!} = \frac{(n-1)!}{(p-1)!(n-p-1)!} \left[\frac{1}{p} + \frac{1}{n-p} \right] = \frac{(n-1)!(n-p+p)}{p!(n-p)!} = C_n^p$$

$$C_n^0 = \frac{n!}{0!(n-0)!} = 1$$

$$\text{de même : } C_n^n = 1$$

$$C_n^1 = C_n^{n-1} = n$$

Triangle de Pascal donnant C_n^p

n \ p	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

Binome de newton

$$(a+b)^n = \sum_{p=0}^{p=n} C_n^p a^p b^{n-p} \quad \forall n \in \mathbb{N}^*$$

démo par récurrence sur n

$$n=1 \quad (a+b)^1 = C_1^0 a^0 b^1 + C_1^1 a^1 b^0 = b+a \quad \text{ouf}$$

Remarque : Les coefficients du binome de Newton, sont dans la ligne n=0 du triangle de Pascal

$$\begin{aligned} \text{d'ou} \quad (a+b)^2 &= a^2 + 2ab + b^2 \\ (a+b)^3 &= a^3 + 3a^2b + 3ab^2 + b^3 \\ &\text{si le produit est commutatif} \end{aligned}$$

Remarques :

- $(1+1)^2 = \sum_{p=0}^{p=n} C_n^p = 2^n$

- Soit E de card n

E comprend C_n^0 parties a 0 elements

et C_n^1 parties a 1 elements

....

C_n^p parties a p elements

C_n^n parties a n elements

$$\text{d'ou} \quad \text{card } P(E) = C_n^0 + C_n^1 + \dots + C_n^n = 2^n$$

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

Applications :

- Nb grilles au logo : 6 nbs { 1 a 49 }

$$C_{49}^6 = \frac{49*48*47*46*45*44}{6*5*4*3*2} = 13983816$$

- Euromillion : 5 nbs { 1 a 50}, 2 étoiles {1,9}

$$\text{Nb grilles : } C_{50}^5 * C_9^2 = 76 \text{ millions}$$

- 3 dés a 6 faces, sans ordre :
commencant par 1 :

111 122 133 144 155 166
112 123 134 145 156

113 124 135 146
 114 125 136
 115 126
 116

$$6 + 5 + 3 + 2 + 1 = 21$$

....
 Total : 56

6.5 - Distribution multinomiale

n objets tous différents a mettre dans 2 cases avec n_1 dans la case 1, n_2 dans la case 2 (sans ordre)

Nb répartition :
$$C_n^{n_1} = \frac{n!}{n_1!(n-n_1)!} = \frac{n!}{(n_1)!(n_2)!}$$

k cases, n objets n_1 dans la case 1 ... n_k dans la case k

Nb répartition $D_k = C_n^{n_1} C_{n-n_1}^{n_2} \dots C_{n-n_1 \dots n_{k-2}}^{n_{k-1}} \cdot 1$

$$D_k = \frac{n!}{(n_1)!(n-n_1)!} \cdot \frac{(n-n_1)!}{(n_2)!(n-n_1-n_2)!} \dots \frac{(n-n_1 \dots n_{k-2})!}{(n_{k-1})!(n-n_1 \dots n_{k-1})!}$$

$$D_k = \frac{n!}{n_1! n_2! \dots (n_{k-1})! (n_k)!} \quad \text{distribution multinomiale}$$

consequence : $\prod_{i=1}^{i=k} (n_i)! \mid n!$ ex : 12! est divisible 3!4!5!

6.6 - Equation diophantienne

Diophante : étudiait les équations en nombres entiers

Nb de solutions : $u_1 + u_2 + \dots + u_p = n \quad u_i \in \mathbb{N}$

4 mégots à repartir entre 3 clodos

C_1	4	3	3	2	2	2	1	1	1	1	0	0	0	0	0
C_2	0	1	0	2	1	0	3	2	1	0	4	3	2	1	0
C_3	0	0	1	0	1	2	0	1	2	3	0	1	2	3	4

15 répartitions possibles.

Maths : $C_1 + C_2 + C_3 = 4 \quad C_i \in \mathbb{N}$

on est dans le « cas de Diophante »

Nb solutions de (1)

Il y a donc (n+p-1) traits (petits ou grands)

Définir une répartition, c'est choisir (p-1) de ces traits qui deviennent des séparateurs.

Le nb de choix est de C_{n+p-1}^{p-1}

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

cette equation a C_{n+p-1}^{p-1} solutions

$$\text{Ex : } C_1 + C_2 + C_3 = 4 \quad C_i \in \mathbb{N}$$

$$\text{a donc } C_{4+3-1}^{3-1} = C_6^2 = \frac{6*5}{2} = 15 \text{ solutions}$$

Extension : Nb solutions : $u_1 + u_2 + \dots + u_p \leq n \quad u_i \in \mathbb{N}, i=1..p$

Soit $u_p + 1$ tq $u_1 + u_2 + \dots + u_p + u_{p+1} = n \quad u_i \in \mathbb{N}, i=1, \dots, p+1$

Le nombre de solutions de (2) est : $C_{n+p+1-1}^{p+1-1} = C_{n+p}^p$

6.7 - Systeme de numération

6.7.1 - Nombres entiers

Soit $p \in \mathbb{N}$ dans la base b la représentation de p est :

$$p = (C_{n-1} C_{n-2} \dots C_2 C_1 C_0)_b = C_0 + C_1 \cdot b + C_2 \cdot b^2 + \dots + C_{n-1} \cdot b^{n-1}$$

$$0 \leq C_i \leq b-1$$

En hexa : 0 1 2 3 4 5 6 7 8 9 A B C D E F

6.7.2 - Nombres rationnels

$$\forall r \in \mathbb{Q}, r = \frac{a}{b} \quad a \in \mathbb{Z}, b \in \mathbb{N}^*$$

$$r = C_{n-1} C_{n-2} \dots C_1 C_0, d_1 d_2 \dots d_p \dots \text{développement décimal k r}$$

en base 10 : $r = C_{n-1} 10^{n-1} + \dots + C_1 \cdot 10 + C_0 + d_1 \cdot 10^{-1} + d_2 \cdot 10^{-2} + \dots + d_p 10^{-p} + \dots$

or, les restes « apres la virgule » de la division de a par b appartiennent a $[0, \dots, b-1]$

La suite des d_i est périodique, de période $\leq b$

Tout rationnel a un developpement décimal périodique, a partir d'un certain rang.

Reciproque : tout developpement décimal périodique représente un rationnel.

Ex : $k = 0,272727272 \dots$

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

$$k = 27 \cdot 10^{-2} (1 + 10^{-2} + 10^{-4} + \dots)$$

$$k = 27 \cdot 10^{-2} \frac{\lim_{n \rightarrow +\infty} 1 - (10^{-2})^n}{1 - 10^{-2}} = \frac{27 \times 10^{-2}}{99 \cdot 10^{-2}} = \frac{3}{11} \in \mathbb{Q}$$

Or il existe des développements décimaux non périodiques.

Ex : 0,0101001000100001... $\notin \mathbb{Q}$

il existe donc des nombres « irrationnels »

avec 2 catégories : $\rightarrow$ nbs algébriques : solution d'une eq. polynomiale a coeff. $\in \mathbb{Q}$

$\rightarrow$ nbs transcendants : e, π

Chapitre 7 - Arithmetique

7.1 - Introduction

C'est l'étude des nombres $\in \mathbb{Z}$ soit $\mathbb{N}$

C'est à dire $(\mathbb{Z}, +, \cdot)$ est un groupe abélien :
+ LCI
Associatif
existe neutre
 $\forall n \in \mathbb{Z}, \text{ exist } \text{sym}(n) = -n$
commutative

Multiplication . LCI, associative, distributive / +, commutative,
unitaire $\exists 1 \in \mathbb{Z} \text{ tq } 1 * n = n * 1 = n$
integre $a.b=0 \Rightarrow a=0 \text{ ou } b=0$

7.2 Divisibilité

Soit a et $m \in \mathbb{Z}$; on dit que m divise a ou que a est divisible par m , ou que m est diviseur de a , ssi

$$\exists k \in \mathbb{Z} \text{ tq } a = mk$$

On note $m|a$

Rappel : $|$ est une relation d'ordre dans $\mathbb{N}$

$$\rightarrow m|a \Leftrightarrow m|-a \Leftrightarrow -m|a \Leftrightarrow -m|-a$$

$\rightarrow 0$ ne divise que 0

$\rightarrow 1$ et -1 , a et $-a$ diviseurs de a

$$\rightarrow m|a \Rightarrow |m| \leq |a|$$

7.3 - Division euclidienne

$$\forall (a, b) \in \mathbb{N}^2, \exists!(q, r) \text{ tq } a = bq + r \quad \text{avec } 0 \leq r < b - 1$$

a = « dividende »

b = « diviseur »

q = « quotient »

r = « reste »

7.4 - Congruence

7.4.1 - Definition

Soit m entier positif

a est congru à $b \% m$ ssi : $m | (a-b)$

on note $a \equiv b [m]$

$$19 \equiv 34 [5]$$

La congruence est une relation d'équivalence

car :

- reflexive car $\forall a \in \mathbb{Z} \quad a \equiv a [m] \quad \text{car } m | (a-a) = 0$

- transitive $a \equiv b [m] \Leftrightarrow m | (a-b) \Leftrightarrow \exists \lambda_1 \in \mathbb{Z} \text{ tq } a-b = \lambda_1 m$

$$b \equiv c [m] \Leftrightarrow \exists \lambda_2 \in \mathbb{Z} \text{ tq } b-c = \lambda_2 m$$

$$\text{d'où : } a-b+b-c = a-c = (\lambda_1 + \lambda_2)m \quad \text{dc } m | (a-c)$$

$$\text{donc : } a \equiv c [m]$$

- symetrie $a \equiv b [m] \Rightarrow m | (a-b) \Rightarrow m | (b-a) \Rightarrow b \equiv a [m]$

rac.

Appli : Verif code securité sociale.

Christophe : 1 85 04 92 012 024 64

checksum : $n + K \equiv 0 [97]$

K s'obtient par : $r = \text{reste de la division euclidienne de } n \text{ par } 97$
 $k = 97 - r$

La congruence modulo m est une relation d'equivalence :

$$a \equiv b [m] \Leftrightarrow m \mid (b-a) \Leftrightarrow a \text{ et } b \text{ ont le m\^eme reste dans leurs divisions euclidiennes par } m$$

$\mathbb{Z}$ a des clauses d'équivalence pour $\equiv[m]$

L'ensemble quotient est noté $\mathbb{Z}/m\mathbb{Z}$

$$\rightarrow \mathbb{Z}/m\mathbb{Z} = \overset{\circ}{0}, \overset{\circ}{1}, \overset{\circ}{2}, \dots, \overset{\circ}{m-1}$$

car $\forall x \in \mathbb{Z} \quad x = qm + r \quad \text{avec } 0 \leq r \leq m-1$

donc : $x \equiv r[m]$ donc $x \in \overset{\circ}{r}$

et $a \in \mathbb{Z}/m\mathbb{Z}$

et $b \in \mathbb{Z}/m\mathbb{Z}$

$$a \equiv b[m] \Leftrightarrow m \mid (a-b) \Leftrightarrow a-b=qm$$

$$a=qm+b \quad \text{d'ou } q=0$$

$$\text{card } \mathbb{Z}/m\mathbb{Z} = m$$

$\rightarrow (\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ est un anneau unitaire, commutatif (pas toujours intègre).

+ est tel que : $\overset{\circ}{a} + \overset{\circ}{b} = \overline{\overset{\circ}{a + b}}$

neutre : $\overset{\circ}{0}$

$$sym \overset{\circ}{a} = \overline{m - a}$$

$$\cdot \overset{\circ}{a}.\overset{\circ}{b}=\overset{\circ}{ab}\exists \overset{\circ}{1}tq\overset{\circ}{1}.\overset{\circ}{a}=\overset{\circ}{a}$$

mais par exemple, pour $m = 6$: $\overset{\circ}{2}.\overset{\circ}{3}=\overset{\circ}{6}=\overset{\circ}{0} \quad \mathbb{Z}/6\mathbb{Z}$ n'est pas intègre.

Ex 1 :

m = 2	$\mathbb{Z}/2\mathbb{Z} = \overset{\circ}{0}, \overset{\circ}{1}$	0 = pairs 1 = impairs
-------	---	--------------------------

table d'opérations ou tables de Pythagore

$$\mathbb{Z}/3\mathbb{Z}=0,1,2$$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Application 1 : Vérif du n° de CB

4833 2484 5503 3472 clef d'algorithme de Luhn

8863 4474 1503 645

$$\frac{\quad}{\text{somme} = 8 [10] = \mathbf{2}}$$

Application 2 : Résolution d'équations algébriques.

$$f(x) = x^4 - x^2 \quad f(x) = 0 \quad \text{à résoudre dans } \mathbb{Z}/6\mathbb{Z}$$

$$f(0) = 0^4 - 0^2 = 0$$

$$f(1) = 1^4 - 1^2 = 0$$

$$f(2) = 2^4 - 2^2 = 12 = 0$$

$$f(3) = 3^4 - 3^2 = 81 - 9 = 72 = 0$$

$$f(4) = 4^4 - 4^2 = 256 - 16 = 240 = 0$$

$$f(5) = 625 - 25 = 600 = 0$$

Application 3 : critères de divisibilité

Théorèmes sur compatibilité

$$\left. \begin{array}{l} a \equiv b[m] \\ c \equiv d[m] \end{array} \right\} \begin{array}{l} a+c \equiv b+d[m] \\ ac \equiv bd[m] \end{array}$$

$$\text{d'où : } a \equiv b[m] \Rightarrow a^n \equiv b^n[m] \quad \forall n \in \mathbb{N}$$

en base 10 :

$$p = \overline{b_n - 1 b_n - 2 \dots b_1 b_0}^{10} \Leftrightarrow p = b_0 + 10b_1 + \dots + 10^{n-1}b_{n-1}$$

divisibilité par 2 :

$$10 \equiv 0[2] \quad p \equiv b_0[2]$$

p est divisible par 2 si son dernier chiffre l'est.

Divisibilité par 3

$$10 \equiv 1[3] \quad \text{donc } p \equiv b_0 + b_1 + \dots + b_{n-1}[3]$$

p est divisible par 3 si la somme de ses chiffres l'est.

divisibilité par 4

$$100 \equiv 0[4] \quad p \equiv b_0 + 10b_1[4] = \overline{b_1 b_0}^{10}[4]$$

p est divisible par 4 si le nombre formé de ses 2 derniers chiffres l'est.

ou $p \equiv b_0 + 2b_1[4] \quad 4194 : 2 * 9 + 4 = 22 \text{ n'est pas divisible par 4}$

divisibilité par 5

$$p \equiv b_0[5]$$

$$5 | p \Leftrightarrow 5 | b_0 \Leftrightarrow b_0 = 0 \text{ ou } b_0 = 5$$

divisibilité par 9

$$10 \equiv 1[9] \quad p \equiv b_0 + b_1 + \dots + b_{n-1}[9]$$

p est divisible par 9 si et seulement si la somme de ses chiffres l'est.

Application 4 : recherche des restes

Ex : reste de la division par 7 de 59^{45}

$$59 \equiv 3[7]$$

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

$$3^0 = 1[7] \quad 3^4 = 4[7]$$

$$3^1 = 3[7] \quad 3^5 = 5[7]$$

$$3^2 = 2[7] \quad 3^6 = 1[7]$$

$$3^3 = 6[7]$$

7.5 Nombres premiers

n est premier si $n \in \mathbb{N}^*$ et n est divisible seulement par 1 et par n

1 est-il premier ? bof :-/

Crible d'Eratosthene

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
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Le nombre de nombres premiers est infini.

Car : $\forall n \in \mathbb{N}, \exists$ un nb 1er plus grand que n

Soit $p = n! + 1$ $p > n$ car $n! + 1 = n(n-1)! + 1$ $n \geq 2$
 $\geq n + 1 > n$
et pour $n = 1$, $1! + 1 > 1$

rac

p n'est pas divisible par 2, ni par 3, ni par n.

Donc, ou bien p est 1er, alors la propriété est vraie

ou bien il n'est pas premier, donc il est divisible par un nombre premier $> n$

Comment trouver un nombre premier ?

Euler : $f(n) = n^2 + n + 41$ $\forall n \in [0, 40], f(n)$ est premier.

jusqu'à $n = 10$ millions. $\frac{1}{3}$ des $f(n)$ sont premiers.

On peut générer tous les nombres premiers par :

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

$f(2) = 2 + (2 \cdot 2 \cdot [3]) = 3$

$f(3) = 2 + (2 \cdot 6 \cdot [4]) = 2$

Record des nombres premiers.

1989	$391581 \cdot 2^{216193} - 1$	65087 chiffres
1998	$2^{673973} - 1$	200 000 chiffres
29 mai 2004	$2^{24036583} - 1$	7 235 733 chiffres
18 février 2005	$M42 = 2^{25964951} - 1$	7 816 230 chiffres
24 dec 2005	$M43 = 2^{30402457} - 1$	9 152 052 chiffres
4 sept 2006	$M44 = 2^{32582657} - 1$	9 808 358 chiffres

Nombres de Mersenne : $2^n - 1$ ou n est premier

7.6 Factorisation première

Soit $a \geq 2$; a admet au moins 1 diviseur plus grand que 1

Soit p_1 son plus petit diviseur $p_1 \geq 2$ $a = p_1 a_1$ p_1 est premier

Si $a_1 \geq 2$ alors $\exists p_2 tq a_1 = p_2 a_2$ p_2 est premier

Donc, $a = p_1 p_2 \dots p_n$ où $2 \leq p_1 \leq p_2 \leq \dots \leq p_n$

Factorisation premiere de a :

$$a = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_k^{\alpha_k} \quad q_1 < q_2 < \dots < q_k, \quad \alpha_i \geq 1, \quad q_i \text{ est premier}$$

La factorisation 1ere est unique.

$$\begin{array}{r|l} \text{Ex :} & \\ 756 & 2 \\ 378 & 2 \\ 189 & 3 \\ 63 & 3 \\ 21 & 3 \\ 7 & 3 \\ 1 & \end{array}$$

$$756 = 2^2 \cdot 3^3 \cdot 7$$

$$\text{Soit } a = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_k^{\alpha_k}$$

Soit d un diviseur de a $d \mid a$

$$d = q_1^{\beta_1} q_2^{\beta_2} \dots q_k^{\beta_k} \quad 0 \leq \beta_i \leq \alpha_i$$

β_i a donc $(\alpha_i + 1)$ valeurs possibles

β_k a donc $(\alpha_k + 1)$ valeurs possibles

$$\text{Nb diviseurs de } a = \prod_{i=1}^k (\alpha_i + 1)$$

Donc, 756 a $(2+1)(3+1)(1+1) = 3 \cdot 4 \cdot 2 = 24$ diviseurs, allant de 1 a 756

7.7 PGCD et PPCM

Soit a et b, deux entiers naturels.

Soit q_j les k premiers facteurs premiers dans a ou dans b

$$a = \prod_{j=1}^k q_j^{\alpha_j} \quad \alpha_j \geq 0 \quad b = \prod_{j=1}^k q_j^{\beta_j} \quad \beta_j \geq 0$$

$$\text{PGCD}(a, b) = a \wedge b = \prod_{j=1}^k q_j^{\inf(\alpha_j, \beta_j)} \quad \text{PPCM} = a \vee b = \prod_{j=1}^k q_j^{\sup(\alpha_j, \beta_j)}$$

$$a \wedge b \cdot a \vee b = \prod_{j=1}^k q_j^{\inf(\alpha_j, \beta_j) + \sup(\alpha_j, \beta_j)} = \prod_{j=1}^n q_j^{\alpha_j + \beta_j} = a \cdot b$$

$$(a \wedge b) \cdot (a \vee b) = a \cdot b$$

a et b sont premiers entre eux $\Leftrightarrow$ ils n'ont aucun facteur 1er commun.

on note : $a \wedge b = 1$

$$\begin{array}{r|l} 4680 & 2 \\ 2340 & 2 \\ 1170 & 2 \\ 585 & 3 \\ 195 & 3 \\ 65 & 5 \\ 13 & 13 \\ 1 & \end{array} \quad \begin{array}{r|l} 84 & 2 \\ 42 & 2 \\ 21 & 3 \\ 7 & 7 \\ 1 & \end{array}$$

$$4680 = 2^3 \cdot 3^2 \cdot 5^1 \cdot 13^1$$

$$84 = 2^2 \cdot 3^1 \cdot 7^1$$

$$4680 \wedge 84 = 2^2 \cdot 3^1 = 12$$

$$4680 \vee 84 = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^1 \cdot 13^1 = 32760$$

$$12 \cdot 32760 = 393120$$

$$4680 \cdot 84 = 393120$$

7.8 - REPOMPER TOUT CA !!!!!

7.8.2 - Théorème de Gauss

Hyp : $a \mid bc$ et $a \wedge b = 1$

$\forall \lambda \in \mathbb{Z} tq bc = a\lambda ; \exists (u, v) \in \mathbb{Z}^2 tq a \cup \dots$

Conséquence 1 :

$$a \wedge b = 1 \text{ et } a \wedge c = 1 \Rightarrow a \wedge bc = 1$$

$$\text{car : } \exists (u, v) \in \mathbb{Z}^2 tq au + bv = 1$$

$$\exists (u', v') \in \mathbb{Z}^2 tq au' + cv' = 1$$

$$(au + bv)(au' + cv') = 1$$

$$a(auu' + ucv' + bv u') + bc v v' = 1$$

$$\text{donc : } a \wedge bc = 1$$

rac

Conséquence 2 :

$$a \wedge b = 1 \text{ et } a \wedge b = 1 \Rightarrow a \wedge b^2 = 1$$

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

7.8.3 - Algorithme d'Euclide

$a \geq b > 0$ calcul de $d = a \wedge b$ puis de (u, v) tq $d = au + bv$

On divise a par b.

$$a = bq + r \quad 0 \leq r < b$$

$$\text{Si } r = 0 \quad a = bq \quad \text{alors } b \mid a \text{ et } b \mid b \text{ donc } a \wedge b = b$$

$$\text{Si } r \neq 0 \quad r = a - bq \quad a \wedge b \mid a \text{ et } a \wedge b \mid b \text{ donc } a \wedge b \mid r$$

$$\text{donc : } a \wedge b \mid b \wedge r$$

$$\text{et } b \wedge r \mid \text{ et } b \wedge r \mid r \text{ donc } b \wedge r \mid a \text{ donc } b \wedge r \mid a \wedge b$$

$$a \wedge b = b \wedge r \text{ le PGCD est le dernier diviseur (qui donne un reste non nul)}$$

	55	1	2	2
4680	84	60	24	12
480	24	12	0	
60				

$$60 = 4680 - 55(84) = a - 55b$$

$$24 = 84 - 1(60)$$

$$24 = b - (a - 55b)$$

$$24 = -a + 56b$$

$$12 = 60 - 2(24)$$

$$= a - 55b - 2(-a + 56b)$$

$$12 = 3a - 167b$$

$$\backslash u \wedge v _ /$$

$$a = 18459 \quad b = 3809$$

$$d = a \wedge b \text{ et } u \text{ et } v \text{ tq } au + bv = d$$

	4	1	5	2
18459	3809	3223	586	293
3223	586	293	0	

$$\begin{aligned}
 3223 &= a - bq \\
 &= 18459 - 4(3809) \\
 &= a - 4b
 \end{aligned}$$

$$\begin{aligned}
 586 &= 3809 - 1(3223) \\
 &= b - (a - 4b) \\
 &= -a + 5b
 \end{aligned}$$

$$\begin{aligned}
 293 &= 3223 - 5(586) \\
 &= a - 4b - 5(-a + 5b)
 \end{aligned}$$

$$293 = 6a - 29b \quad \text{Vérifié !}$$

7.9 - Equation de Diophante

On veut résoudre dans $\mathbb{Z}$: $Ax + By = c$ (1)

A, B, C sont des entiers

Etape 0 On change éventuellement les signes de x et y pour que A et B $\in \mathbb{N}^*$

Etape 1 Soit $d = A \wedge B$

1er cas : d ne divise pas C (1) est impossible

2e cas : on divise (1) par d

on obtient : $ax + by = c$ (2) ou $a \wedge b = 1$

Etape 2 Calcul de u et v $\in \mathbb{Z}$ tq $au + bv = 1$

d'où : $acu + bcv = c$ (3)

Etape 3 (4) = (2) - (3)

$$a(x - cu) + b(y - cv) = 0$$

$$a(x - cu) = b(-y + cv)$$

donc : $b \mid a(x - cu)$ or $b \wedge a = 1$ dc (Gauss) $b \mid (x - cu)$

$$\text{soit : } \exists \lambda \in \mathbb{Z} \text{ tq } x - cu = \lambda b \Rightarrow x = cu + \lambda b$$

$$\text{et } a\lambda b = b(-y + cv) \Rightarrow y = cv - \lambda a$$

Ex1 : Résoudre dans $\mathbb{Z}$ $8x - 6y = 10$

posons $Y = -y$ $8x + 6Y = 10$

$$8 \wedge 6 = 2 \quad 8 = 2^3 \quad 6 = 2 \cdot 3$$

Est-ce que 2 divise 10 ? Oui, il faut continuer

avec : $4x + 3Y = 5$ ou $4 \wedge 3 = 1$

$$1 = 1 \cdot 4 - 1 \cdot 3 \quad \text{d'où} \quad 4 \cdot 5 + 3(-5) = 5$$

On soustrait: $4(x - 5) + 3(Y + 5) = 0$

$$4(x - 5) = 3(-Y - 5)$$

$3 \wedge 4 = 1$ donc : $3 \mid (x - 5)$ d'après Gauss. donc : $x - 5 = 3\lambda$

$$\text{et } 4 \cdot 3\lambda = 3(-Y - 5) \quad -Y - 5 = 4\lambda$$

$$\text{et final : } x = 5 + 3\lambda \quad x = 5 + 3\lambda$$

$$Y = -5 - 4\lambda \quad y = 5 + 4\lambda$$

$$\text{vérif : } 8x - 6y = 40 + 24\lambda - 30 - 24\lambda = 10$$

Ex 2 : organisation du WEI avec 1 000 Etudiants
avec x cars de 53 places et y cars de 21 places.
resoudre dans $\mathbb{N}$: $53x + 21y = 1000$ (1)

Etape 0 OK
Etape 1 $53 \wedge 21 = 1$
 $1 \mid 1000$ oui ! Le pb est mathématiquement possible.
on divise (1) par 1 d'ou : $53x + 21y = 1000$
Etape 2 Calcul de u et v tq $53u + 21v = 1$

	2	1	1	10
53	21	11	10	1
11	10	1	0	

$$\begin{aligned} 11 &= 53 - 2 * 21 \\ 10 &= 21 - 1 * 11 \\ &= 21 - (53 - 2 * 21) \\ &= 3 * 21 - 53 \\ 1 &= 11 - 10 = (53 - 2 * 21) - (3 * 21 - 53) \\ &= 2 * 53 - 5 * 21 \end{aligned}$$

Donc :

$$\begin{aligned} 53x + 21y &= 1000 \\ 53 \cdot (2) + 21 \cdot (-5) &= 1 \\ 53 \cdot (2000) + 21 \cdot (-5000) &= 1000 \\ \text{d'ou : } 53(x - 2000) + 21(y + 5000) &= 0 \\ 53(x - 2000) &= 21(-y - 5000) \\ \text{or : } 21 \wedge 53 &= 1 \end{aligned}$$

$$\begin{aligned} \text{donc, d'apres Gauss :} \\ x - 2000 &= 21\lambda \\ 53\lambda &= -y - 5000 \\ x &= 2000 + 21\lambda \\ y &= -5000 - 53\lambda \end{aligned}$$

7.10 Application au cryptage

Voir DES, AES.

Idée du cryptage RSA (Rivest, Shaur, et Adleman)

Génération de la clef privée :

soient p et q 2 nombres premiers tres grands.

$$n = p * q \quad \Phi(n) = (p-1)(q-1)$$

$$\forall x \in \mathbb{Z}/n\mathbb{Z} \quad x^{\Phi(n)} \equiv 1[n]$$

Bob génère p et q

$$n = p \cdot q \quad \Phi(n) = (p-1)(q-1)$$

Il choisit $b < \Phi(n)$ et 1er avec $\Phi(n)$

$$b^{\Phi(n)} \equiv 1[n]$$

$$\text{Bob calcule } a \equiv b^{-1}[\Phi(n)] \quad ab \equiv 1[\Phi(n)]$$

la clef privée de Bob est a. Sa clef publique est $K = (n, b)$

Si Alice veut envoyer x :

$$X = x^b[n]$$

Bob $d_a(X)=X^a[n]=(x^b)^a[n]=x^{ab}[n]=x^{1[\Phi(n)]}[n]=x^{1+\lambda\Phi(n)}=x.(x^{\Phi(n)})^\lambda[n]=x$