LOGIQUE ET ENSEMBLES

« non(P) » est vraie quand P est fausse.
« P et Q » est vraie quand P et Q sont vraies en même temps.
« P ou Q » est vraie quand P est vraie, ou bien Q, ou bien les deux.
« A ⇒ B » ≡ non(A) ou B ≡ non(B) ⇒ non(A)
« A ⇔ B » ≡ A ⇒ B et B ⇒ A ≡ (B et A) ou [non(A) et non(B)]

non(P et Q) = non(P) ou non(Q)
non(P ou Q)= non(P) et non(Q)
P et (Q ou R) = (P et Q) ou (P et R)
P ou (Q et R) = (P ou Q) et (P ou R)

$\forall x \in \mathrm{E}, R(x)$ ≡ $R(x)$ est vraie pour tout x de l'ensemble E.
$\exists x \in \mathrm{E}, R(x)$ ≡ on peut trouver au moins un x dans E vérifiant $R(x)$.

$$non\left(\forall x \in \mathrm{E}, R(x)\right) \equiv \exists x \in \mathrm{E}, non\left(R(x)\right)$$
$$non\left(\exists x \in \mathrm{E}, R(x)\right) \equiv \forall x \in \mathrm{E}, non\left(R(x)\right)$$

Attention : $\forall x, \exists y, R(x,y)$ et $\exists x, \forall y, R(x,y)$ ne sont pas équivalents !!!

- Raisonnement **direct** pour démontrer (P et (P ⇒ Q)) ⇒ Q
  « Soit P », « Supposons P », « Pour x=n on a » … « donc Q »
- Raisonnement **cas par cas** pour démontrer (P ou Q) ⇒ R
  « 1er cas : supposons P … 2e cas : supposons Q … donc R »
- Raisonnement **par contraposée** pour démontrer (P ⇒ Q)
  On doit démontrer (non(Q) ⇒ non(P)) ⇔ (P ⇒ Q).
- Raisonnement **par l'absurde** pour démontrer (P ⇒ Q)
  On suppose P et non(Q) puis on cherche une contradiction.
  C'est-à-dire non(P et non(Q)) ⇔ non(P) ou Q ⇔ (P ⇒ Q).
- Raisonnement **par récurrence** : soient a et n deux entiers naturels, P_n une proposition qui dépend de n. Alors on a :

$$\left(P_a \text{ et } \left(\forall n \geq a,\ P_n \Rightarrow P_{n+1}\right)\right) \Rightarrow \forall n \geq a,\ P_n$$

« $E \subset F$ » signifie $\forall x \in \mathrm{E}, x \in F$.
« $E = F$ » signifie $E \subset F$ et $F \subset E$.

Ensembles fondamentaux : $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

- Une relation binaire $\Re$ sur E est une partie de E^2.
  On note $x\Re y$ si $(x,y) \in \Gamma$. Une relation binaire $\Re$ sur E est une relation d'ordre si elle est :
  - o réflective $\forall x \in \mathrm{E}, x\Re x$
  - o antisymétrique $\forall x \forall y \in \mathrm{E}, \left(x\Re y \text{ et } y\Re x\right) \Rightarrow x = y$
  - o transitive $\forall x \forall y \forall z \in \mathrm{E}, \left(x\Re y \text{ et } y\Re z\right) \Rightarrow x\Re z$

  Une relation d'ordre est totale si $\forall x, y \in E,\ x\Re y$ ou $y\Re x$.
  On retrouve les notions de majorant, minorant, bornes supérieure et inférieure dans les relations d'ordre.

FONCTIONS ET APPLICATIONS

On appelle fonction de E dans F toute correspondance entre E et F telle que tout élément x de E soit en correspondance avec **au plus** un élément y de F. On appelle E l'ensemble de départ et F l'ensemble d'arrivée. On dit que y est l'image de x, x est un antécédent de y.

$f : E \to F$, $x \mapsto f(x)$ $\qquad G = \left\{(x,y) \in E \times F \mid y = f(x)\right\}$ définit le graphe de f.

$f : E \to F$ est une application si $D_f = \left\{x \in E \mid \exists y \in F,\ y = f(x)\right\} = E$.

- f est injective : tout élément de F a au plus un antécédent

$$\forall x, x' \in E,\ f(x) = f(x') \Rightarrow x = x'$$

- f est surjective : tout élément de F a au moins un antécédent

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

- f est bijective : elle est à la fois injective et surjective

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

La composée de deux injections|surjections|bijections est une injection|surjection|bijection.

$g \circ f$ est injective $\Rightarrow$ f est injective
$g \circ f$ est surjective $\Rightarrow$ g est surjective

Si $f : E \to F$ est bijective, on peut définir $f^{-1} : F \to E$ qui à y$\in F$ associe $f^{-1}(y) \in E$ son unique antécédent par f.

$f : E \to F$ et $g : \mathrm{F} \to G$ sont bijectives $\Rightarrow$ $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

f est injective $\Leftrightarrow$ $\forall y \in F,\ f^{-1}(\{y\})$ a un seul élément.
f est surjective $\Leftrightarrow$ $\mathrm{f}(E) = F$

COMPLEXES

$z \in \mathbb{C} \Leftrightarrow \exists! x, y \in \mathbb{R}^2,\ z = x + iy$ $\qquad \mathrm{Re}(z) = x \qquad \mathrm{Im}(z) = y$

- $z + z' = (x + x') + i(y + y')$ $\qquad$ si $z' \neq 0$ on a :

$$zz' = (xx' - yy') + i(xy' + x'y) \qquad \frac{z}{z'} = \frac{xx' + yy'}{x'^2 + y'^2} + i\frac{x'y - xy'}{x'^2 + y'^2}$$

- $\overline{z} = x - iy$ est le conjugué de z

$$\overline{z + z'} = \overline{z} + \overline{z'} \qquad \overline{zz'} = \overline{z}\ \overline{z'} \qquad 2\mathrm{Re}(z) = z + \overline{z}$$
$$z = \overline{z} \Leftrightarrow z \in \mathbb{R} \qquad z = -z' \Leftrightarrow z \in i\mathbb{R} \qquad 2i\,\mathrm{Im}(z) = z - \overline{z}$$

- Le module de z est positif et se note $|z| = \sqrt{x^2 + y^2}$

$$|z|^2 = z\,\overline{z} \qquad |z + z'| \leq |z| + |z'|$$
$$|z\,z'| = |z||z'| \qquad \big||z| - |z'|\big| \leq |z - z'|$$

$$|z + z'|^2 = |z|^2 + 2\mathrm{Re}(z'\,\overline{z})|z'|^2$$

- $e^{iq} = \cos q + i \sin q$ $\qquad e^{iq} = \dfrac{z}{|z|} \Leftrightarrow z = |z|\ e^{iq}$

$$\arg(z\,z') \equiv \arg z + \arg z' \ [2p] \qquad \arg(z/z') \equiv \arg z - \arg z' \ [2p]$$
$$\arg(-z) \equiv \arg z + p \ [2p] \qquad \arg(z^n) \equiv n \arg z \ [2p]$$
$$\mathrm{Re}(z) = |z| \cos q \qquad \mathrm{Im}(z) = |z| \sin q$$
$$2\cos q = e^{iq} + e^{-iq} \qquad 2i \sin q = e^{iq} - e^{-iq}$$

- G barycentre de $\{(A_i\ ;\ a_i)\}_{i=1\ldots n}$ $\qquad z_G = \dfrac{\sum_{i=1}^{n} a_i z_i}{\sum_{i=1}^{n} a_i}$

- $\left(\overrightarrow{AB}, \overrightarrow{AC}\right) = \arg\left(\dfrac{z_C - z_A}{z_B - z_A}\right) [2p]$

- $M(z) \to M'(z + a)$ est la translation de vecteur $\vec{v}(a)$.
$M(z) \to M'(ze^{iq})$ est la rotation de centre l'origine et d'angle q.
$|z - z_A| = r$ définit le cercle de centre $A(z_A)$ et de rayon r.

- $e^{iq} + e^{iq'} = e^{i\frac{q+q'}{2}}\left(e^{i\frac{q-q'}{2}} + e^{i\frac{q'-q}{2}}\right) = e^{i\frac{q+q'}{2}}\ 2\cos\left(\frac{q-q'}{2}\right)$

$e^{iq} - e^{iq'} = e^{i\frac{q+q'}{2}}\left(e^{i\frac{q-q'}{2}} - e^{i\frac{q'-q}{2}}\right) = e^{i\frac{q+q'}{2}}\ 2i\ \sin\left(\frac{q-q'}{2}\right)$

- $x = |x|\, e^{iq} \neq 0 \qquad 0 \le k \le n-1$

$$z^n = x \Leftrightarrow z = \sqrt[n]{|x|}\, e^{i\frac{q}{n}+\frac{2kp}{n}}$$

- **Linéarisation** $\cos^n q\ \sin^m q \rightarrow \cos xq\ \sin yq$

On utilise les formules d'Euler puis on développe et regroupe les puissances exponentielles opposées. On réutilise enfin les formules d'Euler pour retrouver une somme de termes en $\cos xq$ et $\sin yq$.

$$\cos^n q = \left(\frac{e^{iq} + e^{-iq}}{2}\right)^n \qquad \sin^m q = \left(\frac{e^{iq} - e^{-iq}}{2i}\right)^m$$

- **Factorisation** $\cos xq\ \sin yq \rightarrow \cos^n q\ \sin^m q$

On se sert d'abord de la formule de Moivre puis on developpe l'expression obtenue selon la formule du binôme de Newton. Il ne reste plus qu'à identifier les parties réelles et imaginaires, qui correspondent exactement aux cosinus et sinus de n.

$$e^{inq} = \cos nq + i\sin nq = (\cos q + i\sin q)^n$$
$$\cos nq = \mathrm{Re}\left(e^{inq}\right) \qquad \sin nq = \mathrm{Im}\left(e^{inq}\right)$$

ARITHMETIQUE

- Division euclidienne : soit a,b $\in \mathbb{Z}$ avec b ≠0, il existe un unique couple (q,r) d'entiers relatifs tel que a = bq + r avec 0 ≤ r < |b|.

b | a ⇔ a = bq ⇔ r = 0 r ≠ 0 ⇔ bq < a < b(q+1)

a | b et b | a ⇔ a = ±b
a | b et b | c ⇒ a | c
a | b et a | c ⇒ a | b b + g c

- $c = \mathrm{pgcd}(a,b) = a \wedge b \Leftrightarrow c\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \Leftrightarrow \begin{cases} c \mid a \text{ et } c \mid b \\ d \mid a \text{ et } d \mid b \Rightarrow d \mid c \end{cases}$
- $c = \mathrm{ppcm}(a,b) = a \vee b \Leftrightarrow c\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z} \Leftrightarrow \begin{cases} a \mid c \text{ et } b \mid c \\ a \mid d \text{ et } b \mid d \Rightarrow c \mid d \end{cases}$
- a = bq + r avec 0 ≤ r < |b| ⇒ a ∧ b = b ∧ r

Algorithme d'Euclide : on fait des divisions euclidiennes successives et le pgcd de a et b et le dernier reste non nul. La suite (r_n) est strictement décroissante.

- a | b ⇒ a ∨ b = |b| ka ∨ kb = k (a ∨ b)

b | a ⇒ a ∧ b = |b| ka ∧ kb = k (a ∧ b)
a ∧ b = a+kb ∧ b (a ∧ b)(a ∨ b) = |ab|

a ∧ b = c ⇔ a/c ∧ b/c = 1

- **Bézout** a ∧ b = c ⇒ au + bv = c
  a ∧ b = 1 ⇔ au + bv = 1
- **Gauss** a | bc et a ∧ b = 1 ⇒ a | c
  a ∧ c = 1 et b ∧ c = d ⇒ ab ∧ c = d
  a ∧ c = 1 et b ∧ c = 1 ⇒ ab ∧ c = 1
  a | c et b | c et a ∧ b = 1 ⇒ ab | c

- Après avoir décomposer a et b en facteurs premiers :
  - Le pgcd est le produit des facteurs premiers communs, chacun étant affecté du plus petit des deux exposants.
  - Le ppcm est le produit des tous les facteurs premiers, chacun étant affecté du plus grand des deux exposants.

- p est premier $\Leftrightarrow$ $p \geq 2$ et ses seuls diviseurs sont 1 et lui même.

  Il existe une infinité de nombre premiers.
  Tout entier $n \geq 2$ a au moins un facteur premier p.
  Si n est premier il est évident que p = n, sinon $p \leq \sqrt{n}$.
  Tout nombre autre que 0 et 1 se décompose de manière unique en produits de nombres premiers.

  p est premier et p | ab $\Rightarrow$ p | a ou p | b

- $a \equiv b\ [n] \Leftrightarrow n \mid (a-b) \Leftrightarrow a = b + kn$
  $a \equiv r\ [n]$ et $0 \leq r < n \Leftrightarrow$ r est le reste de a/n
  $a \equiv b\ [n]$ et $b \equiv c\ [n] \Rightarrow a \equiv c\ [n]$
  $a \equiv b\ [n]$ et $a' \equiv b'\ [n] \Rightarrow a + a' \equiv b + b'\ [n]$
  $a \equiv b\ [n]$ et $a' \equiv b'\ [n] \Rightarrow aa' \equiv bb'\ [n]$
  $a \equiv b\ [n] \Rightarrow ac \equiv bc\ [n]$
  $a \equiv b\ [n]$ et $p \in \mathbb{N} \Rightarrow a^p \equiv b^p\ [n]$

- $a \wedge n = 1 \Leftrightarrow$ il existe un entier u tel que $au \equiv 1\ [n]$ $(a \in \mathbb{N}^+)$
  Pour trouver u, chercher une relation de Bézout entre a et n.

- Petit théorème de Fermat
  Si p est un nombre premier et x un entier alors $x^p \equiv x\ [p]$.
  Si en plus p ne divise pas x alors on a $x^{p-1} \equiv 1\ [n]$.

- Théorème chinois des restes

$$\begin{cases} x \equiv a\ [n] \\ x \equiv b\ [k] \end{cases} \Leftrightarrow x \equiv \frac{akv + bnu}{n \wedge k}\ [n \vee k] \qquad \text{avec } nu + kv = n \wedge k$$

- Méthode de résolution $9x \equiv 21\ [15] \Leftrightarrow 9x - 15y = 21$

  Cette équation admet des solutions dans $\mathbb{Z}$ si et seulement si $(9 \wedge -15) = (9 \wedge 15)$ divise 21. On utilise l'algorithme d'Euclide :

  15 = 9*1 + 6
  9 = 6*1 + 3
  6 = 3*2 + 0 $\Rightarrow$ $9 \wedge 15 = 3$

  On remarque que 21 = 3*7 puis on remonte l'algorithme :

  3 = 9 – 6
  3 = 9 – (15 – 9)
  3 = 9*2 + 15*(-1) $\Rightarrow$ (14 ; -7) est solution particulière (en multipliant par 7)

  9x - 15y = 21 = 9(14) - 15(-7) $\Rightarrow$ 9(x-14) = 15 (y-7)

  En divisant par le pgcd on trouve 3(x-14) = 5(y-7)
  Le théorème de Gauss nous donne 3 | (y-7) donc y = 3k + 7
  On remplace dans l'équation bleue et on trouve que
  9x – 14*9 = (15*3)k $\Rightarrow$ 9x = 45k + 14*9 $\Rightarrow$ x = 5k + 14.
  Réciproquement on vérifie que 9(5k + 14) – 15(3k+7) = 21
  $\Leftrightarrow$ 45k + 14*9 – 45k – 7*15 = 21 $\Leftrightarrow$ 2*3 – 1*5 = 1 $\Leftrightarrow$ VRAI

  On peut enfin conclure : S = { (5k + 14 ; 3k + 7) / $k \in \mathbb{Z}$ }

- $\{x_0 + kp / k \hat{I} \mathbb{Z}\}$ est la classe d'équivalence x_0 de modulo p, c'est-à-dire l'ensemble des entiers x_0 vérifiant $x_0 \equiv 0\ [p]$.

$$\mathbb{Z}/p\mathbb{Z} = \{x_0 + kp \ / \ x_0 \in \{0 \ldots p-1\},\ k \in \mathbb{Z}\}$$

  est l'ensemble des classes d'équivalence de modulo p

- $\mathbb{Z}/p\mathbb{Z}$ muni de l'addition et de la multiplication est un anneau.
  Les classes d'équivalence peuvent s'ajouter et se multiplier.
  Attention : en général, ab = 0 n'entraine pas a = 0 ou b = 0.
  Par exemple dans $\mathbb{Z}/10\mathbb{Z}$: 3+5=8 ; 3*5=15=5 ; 2*5=10=0.

- Si p est premier alors $\mathbb{Z}/p\mathbb{Z}$ est intègre et c'est même un corps.
  ab=0 ⇒ a=0 ou b=0 et chaque élément non nul est inversible.

- En pratique, on se servira souvent d'un tableau de congruence.

POLYNOMES

$\mathbf{K}[X]$ est l'ensemble des polynômes à coefficients dans **K**.

- $P \in \mathbf{K}[X]$ s'écrit de manière unique $a_nX^n + \dots + a_1X + a_0$ avec $a_n \neq 0$.
  $a_n \in \mathbf{K}$ est le coefficient dominant, si $a_n = 1$ on dit que P est unitaire.
  $n \in \mathbb{N}$ est le degré de P. Par convention le degré du polynôme nul est $-\infty$. On dit que P est constant ou de degré 0 lorsque $P \in \mathbf{K}$.

  deg PQ = deg P + deg Q
  deg P+Q ≤ max(deg P, deg Q) (égalité si deg P ≠ deg Q)

- A | B ⇔ B = AQ ⇒ deg A ≤ deg B A | B et B | C ⇒ A | C
  A | B et B | A ⇒ ∃ $l \in \mathbf{K}$, B = l A A | B et A | C ⇒ A | (B + C)

  Pour tout $n \in \mathbb{N}$, on a X – 1 | X^n – 1 $X^4 - 1 = (X-1)(X^3+X^2+X+1)$

- A = BQ + R avec deg R < deg B R=0 ⇒ B | A

- A∧B est le polynôme unitaire de plus haut degré divisant A et B.

Si P est unitaire, PA∧PB = P(A∧B) C | A et C | B ⇒ C | A∧B
A et B premiers entre eux ⇔ A∧B = 1 A∧B = P ⇒ (A/P)∧(B/P) = 1

(l A)∧B = A∧B P∧0 = 1/a P (a coefficient dominant de P)
A∧B = B∧R = 1/a R_N (R_N le dernier reste non nul de l'algorithme)
(d'Euclide et a coefficient dominant de R_N)

- **Bézout** A∧B = P ⇒ AU + BV = P
  A∧B = 1 ⇒ AU + BV = 1 et si A et B sont non constants,
  deg U < deg B et deg V < deg A

- **Gauss** A | BC et A∧B = 1 ⇒ A | C

- a est racine de P ⇔ P(a)=0 ⇔ (X-a) | P ⇔ P(a) est le reste de la division euclidienne de P par (X-a), on a P(X) = (X-a) Q(X) + P(a).

- Soit P un polynôme unitaire de degré 2. Soient a et b ses deux racines complexes, on a P = (X – a)(X – b) = X^2 – (a + b)X + (ab)

- Un polynôme de degré n a au plus n racines dans **K**. Le plus grand entier positif r tel que $(X-a)^r$ divise P s'appelle l'ordre de multiplicité de a (on parlera alors de racine simple ou mutliple).

  a est racine multiple ⇔ $(X - a)^2$ | P ⇔ P(a) = P'(a) = 0

- Théorème d'Alembert-Gauss : tout polynôme non constant de $\mathbb{C}[X]$ a au moins une racine dans $\mathbb{C}$.

- Les racines communes à P et Q dans $\mathbb{C}$ sont les racines complexes de P∧Q. Corrolaire 1 : un polynôme P de degré ≥ 2 a une racine multiple dans $\mathbb{C}$ si et seulement si P∧P' n'est pas constant. Corrolaire 2 : les racines multiples d'un polynôme P de degré ≥ 2 dans $\mathbb{C}$ sont les racines complexes de P∧P'.

- Un polynôme irréductible est un polynôme <u>non constant</u> dont les seuls diviseurs sont les polynômes de la forme a ou aP avec $a \in \mathbf{K}$.

Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 ainsi que les polynômes de degré 2 dont le discriminant est négatif.

- Si P est irréductible alors on a P | AB ⇒ P | A ou P | B et
  $\forall Q \in \mathbf{K}[X]$, P | Q ou P∧Q = 1

- Tout polynôme non constant et unitaire se décompose de manière unique en produit de polynômes irréductibles et unitaires.

  $P = a_nX^n + \dots + a_0 = a_n.P_1.P_2 \dots P_r$ avec $r \in \mathbb{N}$