Corps

Koerper, field

”Le corps conditionne le raisonnement.”

Définition 4.1. *Un corps K est un anneau commutatif possedant au moins deux elements $0_K \neq 1_K$ et tel que tout element non-nul est inversible:*

$$K^\times = K - \{0_K\}.$$

Ex: $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

$\mathbb{Z}$ n'est pas un corps: 2 n'est pas inversible ds $\mathbb{Z}$

$\mathbb{Z}^\times = \{\pm 1\}$

Théorème 4.3. *Soit $q \geqslant 1$ un un entier, alors l'anneau des classes de congruences modulo q $(\mathbb{Z}/q\mathbb{Z}, +, .)$ est un corps ssi q est premier (q a exactement deux diviseurs distincts 1 et q)*

Notation 4.1. *Soit $p \geqslant 2$ un nombre premier, le corps fini a p elements $(\mathbb{Z}/p\mathbb{Z}, +, .)$ est note $\mathbb{F}_p$.*

Preuve : $q=1$ $\mathbb{Z}/\mathbb{Z} = \{\bar{0}(1)\}$ n'est pas un corps.

$$\left(\mathbb{Z}/q\mathbb{Z}\right)^{\times} = \{\bar{a}(q) \text{ t.q } (a,q)=1\}$$

Supposons q premier et $\bar{a}(q) \neq \bar{0}(q)$

$\iff$ $q \nmid a$

mais comme q est premier si $q \nmid a$ alors

$(a,q)=1 \Rightarrow a(q)$ inversible ds $\mathbb{Z}/q\mathbb{Z}$

(par Bezout).

Réciproque : si q est composé :

$$q = q_1 q_2 \quad \text{avec} \quad 1 < q_1, q_2 < q$$

alors $q_1(q) \neq 0(q)$ $\quad q_2(q) \neq 0(q)$

si $\mathbb{Z}/q\mathbb{Z}$ était un corps $q_1(q)$ et $q_2(q)$ seraient inversible mod q $\Rightarrow$ $q_1 q_2(q)$ est inversible

$q_1 q_2(q) = q(q) = 0(q)$. pas inversible.

PROPOSITION 4.3 (Petit Theoreme de Fermat). *Soit $p \geqslant 2$ un nombre premier et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps a p elements. Pour tout $x \in \mathbb{F}_p$ on a*

$$x^p = x. \qquad \forall x \in \mathbb{F}_p \quad x^p - x = 0_{\mathbb{F}_p}$$

PROPOSITION 4.4. *Soit p un nombre premier alors pour tout $x, y \in \mathbb{F}_p$ on a*

$$(x+y)^p = x^p + y^p.$$

Preuve (Petit Thm de Fermat)

$x = n(p) \quad n \in \mathbb{N}$

$n(p) = 1(p) + \ldots + 1(p)$ (n fois)

$x^p = (n(p))^p = (1(p) + \ldots + 1(p))^p = 1^p + \ldots + 1^p(p)$

$$= \underbrace{1 + \cdots + 1}_{n \text{ fois}}(p) = n(p) = x.$$

□

Preuve (Prop 4.4)

$$(x+y)^p = (x+y)x\ldots.x(x+y) \quad (p \text{ fois})$$

est une somme de produit de p termes formés de x et de y et comme $\mathbb{F}_p$ est commutatif

$$= \sum_{k=0}^{p} C_p^k x^k y^{p-k} \qquad C_p^k = \frac{p!}{k!\cdot(p-k)!}$$

$$= x^p + y^p + \sum_{k=1}^{p-1} C_p^k x^k y^{p-k}$$

si $1 \leq k \leq p-1$ C_p^k est divisible par p.

$$C_p^k = \frac{p!}{k!\,(p-k)!} = p \cdot \frac{(p-1)!}{k!\,(p-k)!}$$

si $\frac{(p-1)!}{k!\,(p-k)!}$ n'est pas un entier comme C_p^k

est un entier & p premier $\Rightarrow$

p divise $k!(p-k)!$ mais

$k!(p-k)!$ est un produit d'entiers

compris entre 1 et $p-1$

$= (k(k-1)\dots\times 1)\times((p-k)(p-k-1)\dots\ 2\cdot 1)$

et p ne peut diviser ce produit,

$$\Rightarrow \quad C_p^k \bmod p = 0(p)$$

$$\text{et } (x+y)^p = x^p + y^p + \underbrace{\sum_{k=1}^{p-1} C_p^k x^k y^{p-k}}_{=0(p)}$$

$$= x^p + y^p \,.$$

□

Anneaux vs. Corps

THÉORÈME 4.1. *Soit K un corps alors tout ideal $I \subset K$ est soit $I = \{0_K\}$ ou bien $I = K$.*
Reciproquement, soit A un anneau commutatif possedant au moins deux elements alors si ses ideaux sont $\{0_K\}$ ou bien K alors K est un corps.

Preuve : (Rappel) Un idéal I d'un anneau A commutatif est un s-gpe de $(A,+)$ tq $\forall a \in A \; \forall x \in I$ $a.x \in I$.

Si K = Corps et $I \subset K$ un idéal

Si $I \neq \{0_K\}$ soit $x \in I - \{0\}$ alors

x est inversible car $x \neq 0$ et $K = \mathbb{C}$ ps

et $\forall a \in K$ on $(a.x^{-1}).x \in I$

$\| $

$a.x^{-1}.x = a \in I$

$I = K$

Réciproque : si les seuls idéaux de l'anneau K sont $\{0_K\}$ et K $\Rightarrow$ K = Corps : exercice.

□

THÉORÈME 4.2. *Soit K un corps, B un anneau et $\varphi \in \mathrm{Hom}_{Ann}(K, B)$ un morphisme d'anneaux. Alors si φ n'est pas nul ($\varphi \neq \underline{0}_B$) φ est injectif:*

$$\varphi : K \hookrightarrow B.$$

En particulier K s'identifie alors a son image $\varphi(K)$ qui est un sous-corps de B.

Preuve: si $\varphi \neq 0_B \Rightarrow \ker \varphi \neq K$

comme K = corps et $\ker \varphi$ et un ideal de K

$\ker \varphi = \{0_K\} \Rightarrow \varphi$ est injective.

□

Caractéristique d'un corps

$K = \mathrm{Caps}$.

$\mathrm{Car}(K) = q_K \in \mathbb{N}$ tq si on considère le morphisme canonique

$\mathrm{Can}_K : n \in \mathbb{Z} \longrightarrow n_K = \underbrace{1_K + \dots + 1_K}_{n \text{ fois}} \in K$

$\ker(\mathrm{Can}_K) = q_K \mathbb{Z}$

- $q_K = 0$. $\mathrm{Can}_K : \mathbb{Z} \hookrightarrow K$ est injectif

$\Rightarrow$ K contient un anneau isomorphe à $\mathbb{Z}$ $\mathrm{Can}_K(\mathbb{Z})$.

$\Rightarrow$ K est infini.

En fait K contient une copie de $\mathbb{Q}$

Soit $\iota_K := \mathrm{Can}_K : \mathbb{Z} \to K$

si $b \neq 0$ $\quad i_K(b) \neq 0_K$ donc est inversible

On définit alors un morphisme de $\mathbb{Q}$ vers K en posant

$$i_K\left(\frac{a}{b}\right) = i_K(a) \cdot i_K(b)^{-1}$$

On vérifie que $\iota_K : \mathbb{Q} \to K$ est un morphisme de Corps qui prolonge $\mathrm{Can}_K : \mathbb{Z} \to K$.

Comme $\mathbb{Q}$ = Corps et ι_K est non-nul $\iota_K : \mathbb{Q} \hookrightarrow K$ est injectif.

si $q_K \geq 1$.

$q_K > 1$ si $q_K = 1$ $\ker(\mathrm{Can}_K) = \mathbb{Z}$

$\mathrm{Can}_K = \underline{0}_K$ pas possible

$\mathrm{Can}_K(1) = 1_K \neq 0_K$

en fait q_K est premier.

Si $q_K = q_1 q_2$ avec $1 < q_1, q_2 < q_K$

on aurait que $\mathrm{Can}_K(q_K) = O_K$ car q_K est dans le noyau.

et $\mathrm{Can}_K(q_K) = \mathrm{Can}_K(q_1 q_2) = \mathrm{Can}_K(q_1)\mathrm{Can}_K(q_2)$

$= O_K$

$\Rightarrow$ ou bien $\mathrm{Can}_K(q_1) = O_K$ ou bien $\mathrm{Can}_K(q_2) = O_K$

Sinon ils seraient tous deux inversibles et leur produit le serait. (K=corps)

$\Rightarrow$ q_K est premier. $q_K = p$

$Car(K) = p$.

Prop: en fait $\mathrm{Car}_K(\mathbb{Z})$ est un corps isomorphe au $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

Preuve: notons que $\forall n \in \mathbb{Z}\ \forall k \in \mathbb{Z}$

$$\mathrm{Car}_K(n+pk) = \mathrm{Car}_K(n) + \mathrm{Car}_K(p.k)$$
$$= \mathrm{Car}_K(n) \quad (p.k \in \ker \mathrm{Car}_K)$$

$\Longrightarrow Can_K(n)$ ne dépend que de $n(p) \in \mathbb{Z}/p\mathbb{Z}$

On peut définir un morphisme

$$i_K : \mathbb{Z}/p\mathbb{Z} \to K$$
$$n(p) \to Can_K(n)$$

i_K est un morphisme d'anneaux $\neq 0_K$ car

$$i_K(1(p)) = \mathrm{Car}_K(1) = 1_K \neq 0_K$$

i_K est injectif $\left(\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p = \text{Corps} \right)$ □

$\Longrightarrow$ Si $\mathrm{Car}(K) = p \geq 2$ alors

K contient un copie de $\mathbb{F}_p$.

(K ne contient pas de copie de $\mathbb{F}_{p'}$ si $p' \neq p$)

Définition 4.7. *Le corps $\mathbb{Q} \subset K$ (si $\mathrm{car}(K) = 0$) ou bien $\mathbb{F}_p \subset K$ (si $\mathrm{car}(K) = p > 0$) s'appelle le sous-corps premier de K.*

le + petit sous corps de K.

Le Frobenius

PROPOSITION 4.4. *Soit K un corps de caracteristique $p > 0$ alors l'application*

$$\bullet^p : \begin{array}{ccc} K & \mapsto & K \\ x & \mapsto & x^p \end{array}$$

est un morphisme d'anneaux non-nul (donc necessairement injectif).

Preuve: $\mathrm{Car}(K) = p$ $\forall x, y \in K$

$$(x.y)^p = (x.y) \times (x.y) \times \ldots . (x.y) \quad p \text{ fois}$$

$$= (x. \quad .x) \times (y. \ldots . y) \quad p \text{ fois}$$

$$= x^p . y^p$$

K commutatif

$$(x+y)^p = x^p + y^p \; ?$$

$$= x^p + y^p + \sum_{k=1}^{p-1} C_p^k x^k y^{p-k}$$

et C_p^k est divisible par p si $1 \leq k \leq p-1$

$$\Rightarrow C_p^k \cdot 1_K = 0_K \Rightarrow C_p^k x^k y^{p-k} = 0_K$$

$\mathrm{Frob}_p : x \in K \longrightarrow x^p \in K$

Frob_p = Frobenius de K

$\mathrm{Frob}_p(1_K) = 1_K \neq 0$ Frob_p est injectif.

Rmq : soit $x \in K$ alors

$\mathrm{Frob}_p(x) = x$ ie $x^p = x$ ssi

$x \in \mathbb{F}_p \subset K$


©Bandai Namco

Corps de fractions

Cas de $\mathbb{Z}$: $\mathbb{Z}$ n'est pas un corps

car les elts $\neq 0, \pm 1$ ne sont pas inversible

$\rightarrow$ on invente les fractions rationelles

$$\left\{ \frac{a}{b},\ a \in \mathbb{Z}\ \ b \in \mathbb{Z} - \{0\} \right\} = \mathbb{Q}$$

une fraction $\frac{a}{b}$ admet une infinité de

représentation $\frac{a}{b} = \frac{ak}{b.k}$ pour tout $k \in \mathbb{Z} - \{0\}$

LEMME 4.1. *Soit $\{0\} \neq A \subset K$ un sous anneau non-nul d'un corps K alors A est commutatif et*

$$\forall a, b \in A,\ a.b = 0 \Longleftrightarrow a = 0 \text{ ou } b = 0. \tag{4.2.1}$$

Exemple: $q = q_1 \times q_2$ $1 < q_1, q_2 < q$

$q_1 q_2 (q) = 0 (q) = q_1(q) \times q_2(q)$

mais $q_1(q)$ et $q_2(q)$ ne sont pas nuls mod q.

Définition 4.2. *Un anneau A non-nul, commutatif, tel que $\forall a, b \in A$ on ait*

$$a.b = 0 \Longleftrightarrow a = 0 \text{ ou } b = 0$$

est dit integre. (domain)

Preuve du lemme : Soit $A \subset K$ $A \neq \{0_K\}$

et soient $a, b \in A$ tq $a.b = 0_K$

si a, et b sont tous deux $\neq 0_K$

alors a et b sont inversible et $a.b$ est inversible

$\Rightarrow a.b \in K - \{0\} \quad a.b \neq 0_K$

THÉORÈME 4.2. *Soit A un anneau integre (en particulier commutatif) , alors il existe un corps K et un morphisme d'anneau injectif*

$$\iota : A \hookrightarrow K$$

(de sorte qu'on peut considerer A comme un sous-anneau de K en identifiant A a son image $\iota(A) \subset K$) et tel que K a la propriete de minimalite suivante: pour tout corps K' et tout morphisme injectif

$$\iota' : A \hookrightarrow K',$$

il existe un morphisme (necessairement injectif)

$$\iota'_K : K \hookrightarrow K'$$

prolongeant le morphisme ι' (ainsi A et K peuvent etre vus comme des sous-anneaux de K').

K s'appelle le corps des fraction de A $K = \mathrm{Frac}(A)$.

Ex: $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.

Construction A commutatif integre.

On considere le produit

$$A \times (A - \{0\}) = \{ (a,b) \quad a \in A \quad b \in A \quad b \neq 0_A \}$$

$$(a,b) \rightsquigarrow \frac{a}{b} \overset{?}{=} \frac{ac}{bc} \quad \text{pour tout } c \in A - \{0\}$$

On definit sur $A \times A - \{0\}$ une relation d'équivalence

On dit que

$(a,b) \sim (a',b')$ ssi $ab' = a'b$

Fait: $\sim$ est d'equivalence

- Reflexif: $(a,b) \sim (a,b) \iff ab = ab$
- Symetrique $(a,b) \sim (a',b') \Rightarrow (a',b') \sim (a,b)$

$ab' = a'b \quad a'b = ab'$

- transitive: $(a,b)\sim(a',b')$ $(a',b')\sim(a'',b'')$

$\Rightarrow (a,b)\sim(a'',b'')$

On a $ab'=a'b$ et $a'b''=a''b'$

on a $a'b''b=a''b'b \Rightarrow a'bb''=a''bb'$

$\Rightarrow ab'b''=a''bb'$

$\Rightarrow ab''b'=a''bb'$

$\Rightarrow (ab''-a''b)b'=0$

On sait que $b' \neq 0$ par intégrité de A

$\Rightarrow a b'' - a'' b = 0 \Rightarrow a b'' = a'' b$

Etant donné $(a,b) \in A \times A - \{0\}$ on note

$\frac{a}{b}$ la classe d'équivalence de (a,b)

$= \{ (a',b') \in A \times A - \{0\} \text{ tq } (a',b') \sim (a,b) \}$

A = anneau intègre

$$A \times A - \{0\} = \{ (a,b) \quad a \in A \quad b \in A - \{0\} \}$$

$$(a,b) \sim (a',b') \iff ab' = a'b \quad \left(\frac{a}{b} = \frac{a'}{b'} \right)$$

$$\frac{a}{b} := \{ (a',b') \quad (a',b') \sim (a,b) \} \subset A \times A^*$$

$$A^* = A - \{0\}$$

$$\mathrm{Frac}(A) = \left\{ \frac{a}{b} \;\; a \in A \;\; b \in A - \{0\} \right\} \subset \mathcal{P}(A \times A - \{0\})$$

On définit une addition et une multiplication sur $\mathrm{Frac}(A)$ en posant

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$$

⚠ $bd \neq 0$ car $b, d \neq 0$

$$\frac{a}{b} \times \frac{c}{d} := \frac{ac}{bd}$$

Il faut vérifie que la + et le x ne dépendent pas du choix des représentant (a,b) et (c,d) des classe $\frac{a}{b}$, $\frac{c}{d}$

Ou vmq : si $\frac{a'}{b'} = \frac{a}{b}$ et $\frac{c'}{d'} = \frac{c}{d} \Rightarrow \frac{a'd'+b'c'}{b'd'} = \frac{ad+bc}{bd}$

ie. si $(a',b') \sim (a,b)$ et $(c',d') \sim (c,d)$ alors $(a'd'+b'c', b'd') \sim (ad+bc, bd)$

$a'b = b'a$ $c'd = d'c$ et on v mq

$(a'd' + b'c')bd \overset{?}{=} (ad+bc)b'd'$

$a'd'bd + b'c'bd \overset{?}{=} adb'd' + bcb'd'$

$ab'd'd + b'cbd' = adb'd' + bcb'd'$ (par commutativité)

Pareil avec la multiplication.

On obtient une structure d'anneau pour $\mathrm{Frac}(A)$ d'élt nul $0_{\mathrm{Frac}(A)} = \frac{0_A}{1_A}$

et d'élt unité $1_{\mathrm{Frac}(A)} = \frac{1_A}{1_A}$.

si $\frac{a}{b} \neq 0_{\mathrm{Frac}(A)} \iff a \neq 0_A$

et $\frac{a}{b}$ est inversible d'inverse $\frac{b}{a}$

$$\frac{a}{b} \times \frac{b}{a} = \frac{ab}{ab} = \frac{1_A}{1_A}$$

On obtient un Cap $Frac(A)$

On a également un morphisme injectif

$$i : A \hookrightarrow Frac(A)$$

$$a \longrightarrow \frac{a}{1_A}$$

Minimalité de $Frac(A)$:

$i' : A \hookrightarrow K'$ alors il existe un morphisme

$i'_{Frac(A)} : Frac(A) \hookrightarrow K'$ tq

$i'_{Frac(A)}$ prolonge i'

$$i'_{Frac}\left(\frac{a}{1_A}\right) = i'(a).$$

Si A se plonge ds un corps K' alors $Frac(A)$ se plonge ds K' de manière compatible

$A = \mathbb{Z}$

$\mathbb{Z} \hookrightarrow \mathbb{Q} = Frac(\mathbb{Z})$

$a \longrightarrow \frac{a}{1} = a$

On aurait pu prendre $\mathbb{R}$ à la place de $\mathbb{Q}$

$\mathbb{Q}$ est le + petit corps contenant les inverses des elts $\neq 0$ de $\mathbb{Z}$.

Construction de $\mathbb{C}$

Leibniz

"... eine feine und wunderbare Zuflucht des menschlichen Geistes, beinahe ein Zwitterwesen zwischen Sein und Nichtsein."

"Even better than the real thing."

Bono

Motivation (Renaissance)

Resoudre des equations polynomiales

$$aX^2 + bX + c = 0$$

$$aX^3 + bX^2 + cX + d = 0$$

$\Delta = b^2 - 4ac < 0$

$\rightsquigarrow$ Nombres imaginaire tq

i vérifiant $i^2 = -1$.

$\mathbb{C} = \{ x + iy \quad x, y \in \mathbb{R} \}$ muni de loi d'addition et de $\times$ naturelle

Construction à l'aide de Matrices 2×2

Rappels : K corps

$$M_2(K) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \; a, b, c, d \in K \}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} := \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} := \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$

$$\begin{array}{rccc} & M_2(K) & \mapsto & K \\ \det : & M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \mapsto & \det(M) = ad - bc \end{array}$$

$\det MN = \det M . \det N$

$\det M \in K^* \iff M \in M_2(K)^*$

$$M^{-1} = \frac{1}{\det M} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} \frac{d}{\det M} & \frac{-b}{\det M} \\ \frac{-c}{\det M} & \frac{a}{\det M} \end{pmatrix}$$

Multiplication externe

$$K \times M_2(K) \longrightarrow M_2(K)$$

$$\left(\lambda, \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \longrightarrow \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda c \end{pmatrix}$$

Multiplication par les scalaires

On a les propriétés suivantes

- Neutralité $1_K \cdot M = M$
- associativité $(\lambda . \mu) . M = \lambda . (\mu . M)$
- distributivité $(\lambda + \mu) M = \lambda M + \mu M$

$$\lambda (M+N) = \lambda M + \lambda N$$

$$K \longrightarrow M_2(K)$$

$$i: \quad \lambda \longmapsto \lambda I_2 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$$

i est un morphisme d'anneaux $\neq 0_{M_2(K)}$

donc injective: On peut realiser K comme un sscorps de l'anneau $M_2(K)$

THÉORÈME 5.1. *Soit K un corps et $M_2(K)$ l'algebre des matrices 2×2 a coefficients dans K. Soit $d \in K - K^2$ un element de K qui n'est pas un carre: $\forall x \in K,\ x^2 - d \neq 0$ et*

$$I_d := \begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix}.$$

(ex : $K = \mathbb{R}$, $d = -1$)

Alors la matrice I_d verifie

$$I_d^2 = d.\mathrm{Id}_2 = \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix}$$

Soit

$$K[I_d] := K.\mathrm{Id}_2 + K.I_d = \left\{ Z = x.\mathrm{Id}_2 + y.I_d = \begin{pmatrix} x & dy \\ y & x \end{pmatrix},\ x, y \in K \right\} \subset M_2(K)$$

l'ensemble des combinason lineaires des matrices Id_2 et I_d. Alors $K[I_d]$ a les proprietes suivantes:

1. *L'ecriture d'un element Z sous la forme $Z = x.\mathrm{Id}_2 + y.I_d$ est unique.*
2. *$K[I_d]$ muni du produit de matrices est un sous-anneau commutatif de $M_2(K)$ contenant l'anneau des matrices scalaires $K.\mathrm{Id}_2$ et c'est meme un corps : toute matrice non-nulle de $K[I_d]$ est inversible dans $K[I_d]$.*
3. *Plus precisemment soit*

$$Z = x\mathrm{Id}_2 + y.I_d = \begin{pmatrix} x & dy \\ y & x \end{pmatrix}$$

alors

$$\det(Z) = x^2 - dy^2$$

et si $\det(Z) \neq 0$ (alors Z est inversible) on a

$$Z^{-1} = \frac{1}{x^2 - dy^2}(x.\mathrm{Id}_2 - yI_d) = \begin{pmatrix} \frac{x}{x^2-dy^2} & d\frac{-y}{x^2-dy^2} \\ \frac{-y}{x^2-dy^2} & \frac{x}{x^2-dy^2} \end{pmatrix} \in K[I_d].$$

Ex: $K = \mathbb{R}$ $\quad d = -1$

$$I_{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$\mathbb{R}[I_{-1}] = \left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \quad x, y \in \mathbb{R} \right\}$$

est un corps qui contient $\mathbb{R}.I_{d_2} \simeq \mathbb{R}$

et tel que $I_{-1}^2 = -I_d$

si on pose $I_{-1} =: i$ on identifie

$\mathbb{R}$ avec $\mathbb{R}.I_d$. On peut écrire

tout elt $z = x I_d + y.i = x + iy$

de $\mathbb{R}[I_{-1}]$ et on obtient le Corps $\mathbb{C}$.

"Preuve:" $d \in K$ tq d n'est pas un $\square$ ds K

$$Z = x\,Id_2 + y\,I_d$$

$$= \begin{pmatrix} x & yd \\ y & x \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

ssi $x=0$ et $y=0$

le morphisme de gpe additif

$(x,y) \in K^2 \longrightarrow xId_2 + yI_d = \begin{pmatrix} x & yd \\ y & x \end{pmatrix}$

est injectif : Tout $Z \in K[I_d]$ s'écrit de manière unique $Z = xId_2 + yI_d$.

Si $Z, Z' \in K[I_d]$,

$$Z + Z' = \begin{pmatrix} x+x' & d(y+y') \\ y+y' & x+y \end{pmatrix} \in K[I_d]$$

$z.z' \in K[I_d]$?

$$z.z' = \begin{pmatrix} xx'+dyy' & (xy'+yx')d \\ xy'+yx' & xx'+dyy' \end{pmatrix}$$

$$= (xx'+dyy')I_{d_2} + (xy'+yx')I_d$$

$$\in K[I_d]$$

$$z \cdot z' = (x I_{d_2} + y I_d)(x' I_{d_2} + y' I_d)$$

$$= x x' I_{d_2}^2 + x y' I_{d_2} I_d + y x' I_d I_{d_2} + y y' I_d^2$$

$$= x x' I_{d_2} + x y' I_d + y x' I_d + y y' d I_{d_2} = (x x' + d y y') I_{d_2} + (x y' + y x') I_d$$

$K[I_2]$ est un ss anneau de $M_2(K)$

il est commutatif : K est commutatif

et des formules pour ZZ' et $Z'Z$.

$K[I_d]$ at un corps : si $Z \neq 0_{M_2(K)}$

Z est inversible et $Z^{-1} \in K[I_d]$?

$Z = \begin{pmatrix} x & yd \\ y & x \end{pmatrix}$ $\det Z = x^2 - dy^2 \neq 0$?

si $x^2 - dy^2 = 0$

$x^2 = dy^2$.

- si $y=0 \Rightarrow x=0 \Rightarrow Z = Q_{N_2(K)}$

- si $y \neq 0$ y est inversible

$$d = \frac{x^2}{y^2} = \left(\frac{x}{y}\right)^2 = \square$$ qui est exclu

si $(x,y) \neq (0,0)$ donc $Z \neq 0$ et Z inversible

$$Z^{-1} = \frac{1}{x^2 - dy^2} \begin{pmatrix} x & -yd \\ -y & x \end{pmatrix}$$

$$= \frac{x}{x^2 - dy^2} Id_2 - \frac{y}{x^2 - dy^2} I_d \in K[I_d]$$

$K[I_d]$ est notre corps.

La construction se generalise de la

manière suivante: etant donne

$P(X) = a_d X^d + \dots + a_1 X + a_0$ un polynome

a coef ds K qui est irreductible

si $d > 1$ alors $P(x) = 0$ n'a pas de sol

ds K : $\nexists\ \alpha \in K$ tq $P(\alpha) = 0$

($d \neq \square$ et $X^2 - d$ irred)

On peut construct un corps $K[\alpha]$
de matrice $d \times d$ contenant K
et une matrice $\alpha \in M_d(K)$ tq

$$P(\alpha) = O_{M_d(K)}.$$

Rmq : $\mathbb{C}$ a été construit pour résoudre les équations polynomiales de d° 2, 3, 4

Gauss a demontre que

$\forall P(X) \in \mathbb{R}[X]$ de $d^\circ > 0$, il existe $\alpha \in \mathbb{C}$

tq $P(\alpha) = 0$

$\mathbb{C}$ est algebriquement clos.

Modules sur un Anneau

Espace Vectoriel sur un Corps

DÉFINITION 6.1. *Soit $(A,+,.)$ un anneau commutatif, un A-module est un groupe commutatif $(M,+)$ muni d'une loi de multiplication externe*

$$\bullet * \bullet : \begin{array}{ccc} A \times M & \mapsto & M \\ (a,m) & \mapsto & a*m \end{array}$$

(appellee multiplication par les scalaires) ayant les proprietes suivantes:

(1) Associativite: $\forall a, a' \in A,\ m \in M,$

$$(a.a') * m = a * (a' * m).$$

(2) Distributivite: $\forall a, a' \in A,\ m, m' \in M,$

$$(a + a') * m = a * m + a' * m,\ a * (m + m') = a * m + a * m'.$$

(3) Neutralite de 1_A*:* $\forall m \in M,$

$$1_A * m = m.$$

Si $A = K$ est un corps alors M s'appelle egalement un K-espace vectoriel (K-EV) et les elements de M sont les vecteurs de M.

Rmq : $-m = -1_A * m$

$\forall n \in \mathbb{Z}$ $n.m = n_A * m$ $n_A = Can_A(n)$

$m+m-\cdots+m$ (n fois)

Exemples : A est un A-module

- $\{0_A\}$ est un A-module
- $I \subset A$ idéal $\Rightarrow I$ = A-module
- $A^d = \{(a_1, \dots, a_d) \quad a_i \in A\}$

est un A-module

$$\vec{a} = (a_1, \dots, a_d)$$

$$a * \vec{a} = (aa_1, \dots, aa_d)$$

A^d = A-module libre de rang d

dimension

- $M_2(A)$ est un A-module pour la x par les scalaires