(cf théorème 8 du chapitre 3)

$\mathbb{R} \longrightarrow \mathbb{C}$

$\mathbb{R} \times \mathbb{C} \longrightarrow \mathbb{C}$
$(x, z) \longmapsto x \cdot z = xz$

$\mathrm{Hom}_{\mathbb{R}\text{-algèbres}}(\mathbb{C}, \mathbb{C}) = \{\mathrm{Id}_{\mathbb{C}}, z \mapsto \bar{z}\}$

$\cap$

$\mathrm{Hom}_{\text{anneaux}}(\mathbb{C}, \mathbb{C})$

φ c'est-à-dire 1) $\varphi \in \mathrm{Hom}_{\text{anneaux}}(\mathbb{C}, \mathbb{C})$

2) $\forall x \in \mathbb{R}, \forall z \in \mathbb{C}, \varphi(xz) = x\varphi(z)$

$z = 1$ $\quad \forall x \in \mathbb{R}, \varphi(x) = x$

$\varphi \in \mathrm{Hom}_{\mathbb{R}\text{-algèbres}}(\mathbb{C}, \mathbb{C})$
$z \in \mathbb{C}$ $\quad \varphi(z)$?

$z = a + i.b \quad a, b \in \mathbb{R}$

$\varphi(z) = \varphi(a) + \varphi(i)\,\varphi(b) = a + \varphi(i)\,b$

Il suffit de déterminer $\varphi(i)$

$i^2 + 1 = 0$ $\quad P = X^2 + 1 \in \mathbb{R}[X]$
$P(i) = 0$

donc $\varphi(i)^2 + \varphi(1) = 0$

donc $\varphi(i)^2 + 1 = 0$ donc $\varphi(i)$ est aussi une racine de P

donc $\varphi(i) = i$ ou $\varphi(i) = -i$

$\mathbb{C} \underset{\mathbb{R}\text{-algèbres}}{\simeq} \mathbb{R}[X]/\langle X^2+1\rangle = \mathbb{R}[X]/\langle P\rangle$

$P = X^2 + 1 \in \mathbb{R}[X]$

$\varphi : \mathbb{R}[X] \longrightarrow \mathbb{C}$ $\quad \varphi$ surjectif
$Q \longmapsto Q(i)$ $\quad \ker(\varphi) = \langle P\rangle$

(théorème 8 du chapitre 3)

$\mathrm{Hom}_{\mathbb{K}\text{-algèbres}}(\mathbb{K}[X]/\langle P\rangle, A) \underset{\text{bijection}}{\simeq} \{\text{racines de } P \text{ dans } A\}$

$\mathbb{K}[X] \longrightarrow A \longleftarrow\!| \ \alpha \in A$ tq $P(\alpha) = 0$
$Q \longmapsto Q(\alpha)$
(se factorise par $\langle P\rangle$)

$\mathbb{K} = \mathbb{R}$ $\quad A = \mathbb{C}$
$P = X^2 + 1$

$\mathrm{Hom}_{\mathbb{R}\text{-algèbres}}(\mathbb{R}[X]/\langle X^2+1\rangle, \mathbb{C}) \simeq \{i, -i\}$

$\mathbb{R}[X] \longrightarrow \mathbb{C} \longleftarrow\!| \ i$
$Q \longmapsto Q(i)$

$\mathbb{R}[X] \longrightarrow \mathbb{C} \longleftarrow\!| \ -i$
$Q \longmapsto Q(-i)$

$\varphi : \mathbb{R}[X] \longrightarrow \mathbb{C}$ $\quad \ker(\varphi) = (X^2+1)$
$Q \longmapsto Q(i)$

On note x l'image de X dans $\dfrac{\mathbb{R}[X]}{(X^2+1)}$

(théorème 6 du chapitre 3)

dans $\dfrac{\mathbb{R}[X]}{\langle X^2+1\rangle}$ est un $\mathbb{R}$-espace vectoriel de base $\{1, x\}$

induit $\tilde{\varphi} : \mathbb{R}[X]/\langle X^2+1\rangle \longrightarrow \mathbb{C}$

π ; $\{a + xb\}_{(a,b) \in \mathbb{R}^2}$; $\pi(a + Xb)$

$\tilde{\varphi}(a + xb) = \varphi(a + Xb) = a + ib$

$Q \longmapsto Q(i)$

$\mathbb{R}[X]/\langle X^2+1\rangle \simeq \mathbb{C}$
$a + bx \longmapsto a + ib$
$a, b \in \mathbb{R}$

(Théorème 5 du chapitre 3)

3.

$$C_{\mathbb{K}} : \begin{array}{ccc} \mathbb{K}^\times & \longrightarrow & \mathbb{K}^\times \\ x & \longmapsto & x^2 \end{array}$$

$\mathcal{C}_{\mathbb{K}}^* = \{$ ensemble des carrés non nuls de $\mathbb{K}\}$

$\ker(C_{\mathbb{K}}) = \{1_{\mathbb{K}}, -1_{\mathbb{K}}\}$ $\qquad = C_{\mathbb{K}}(\mathbb{K}^\times)$

On en déduit $\mathbb{K}^\times / \ker(C_{\mathbb{K}}) \xrightarrow[\text{iso de groupes}]{\sim} C_{\mathbb{K}}(\mathbb{K}^\times) = \mathcal{C}_{\mathbb{K}}^*$

↳ en particulier une bijection

$\mathbb{K}$ fini $\quad \operatorname{card}\left(\mathbb{K}^\times / \ker(C_{\mathbb{K}})\right) = \operatorname{card}(\mathbb{K}^\times) / \operatorname{card}(\ker(C_{\mathbb{K}}))$

$\operatorname{card}(\mathbb{K}) = q$

$\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$ donc $\operatorname{card}(\mathcal{C}_{\mathbb{K}}^*) = (q-1)/2$ (car $1_{\mathbb{K}} \neq -1_{\mathbb{K}}$)

$\mathcal{C}_{\mathbb{K}} = \mathcal{C}_{\mathbb{K}}^* \cup \{0\}$ $\quad \operatorname{card}(\mathcal{C}_{\mathbb{K}}) = \frac{q-1}{2} + 1 = \frac{q+1}{2}$

$R_{\mathbb{K}}$:

$$\mathcal{C}_{\mathbb{K}}^* \overset{?}{=} \{x \in \mathbb{K}^\times,\ x^{\frac{q-1}{2}} = 1_{\mathbb{K}}\} = \{\text{racines dans } \mathbb{K} \text{ du polynôme } X^{\frac{q-1}{2}} - 1_{\mathbb{K}}\}$$

$\subset$ Lagrange dans $\mathbb{K}^\times$ $\quad \operatorname{card}(\mathbb{K}^\times) = q-1$

$x \in \mathcal{C}_{\mathbb{K}}^*$ $\quad x = y^2$ avec $y \in \mathbb{K}^\times$

$x^{\frac{q-1}{2}} = (y^2)^{\frac{q-1}{2}} = y^{q-1} = 1_{\mathbb{K}}$

↓ Lagrange

$$\operatorname{card}(R_{\mathbb{K}}) \leq \deg\left(X^{\frac{q-1}{2}} - 1_{\mathbb{K}}\right) = \frac{q-1}{2}$$

$\mathcal{C}_{\mathbb{K}}^* \subset R_{\mathbb{K}}$ donc $\operatorname{card}(R_{\mathbb{K}}) \geqslant \operatorname{card}(\mathcal{C}_{\mathbb{K}}^*)$

$\operatorname{card}(\mathcal{C}_{\mathbb{K}}^*) = \frac{q-1}{2}$ $\quad \operatorname{card}(R_{\mathbb{K}}) \leq \frac{q-1}{2}$ $\quad = \frac{q-1}{2}$

donc $\operatorname{card}(R_{\mathbb{K}}) = \frac{q-1}{2}$ $\quad$ donc $\mathcal{C}_{\mathbb{K}}^* = R_{\mathbb{K}}$

Pourquoi un corps fini de cardinal impair est de caractéristique différente de 2 ?

CORPS FINIS

Théorème 3 (chapitre 4)

$\mathbb{K}$ corps fini
$\mathrm{car}(\mathbb{K}) = c \in \mathbb{N}$

$$\varphi_{\mathbb{K}} : \mathbb{Z} \longrightarrow \mathbb{K}, \quad n \longmapsto n \cdot 1_{\mathbb{K}} \qquad \ker(\varphi_{\mathbb{K}}) = c\mathbb{Z}$$

induit un morphisme injectif $\tilde{\varphi}_{\mathbb{K}} : \mathbb{Z}/c\mathbb{Z} \hookrightarrow \mathbb{K}$
(injectivité)

(slogan : $\varphi : A \to B$ induit un morphisme injectif $A/\ker(\varphi) \hookrightarrow B$
"φ identifie $A/\ker(\varphi)$ à un sous-anneau de B"
(strict en général))

$\mathbb{Z}/c\mathbb{Z}$ est un sous-anneau de $\mathbb{K}$, or $\mathbb{K}$ est intègre
Donc $\mathbb{Z}/c\mathbb{Z}$ est intègre donc $c = 0$ ou c est un nombre premier

Or si $c = 0$ $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$ s'identifie à un sous-anneau de $\mathbb{K}$
or $\mathbb{Z}$ est infini donc $\mathbb{K}$ est infini

Donc si $\mathbb{K}$ est fini, c est un nombre premier.

On note $c = p$
$\mathbb{Z}/p\mathbb{Z}$ est un corps (p premier)

$\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{K}$ structure de $\mathbb{Z}/p\mathbb{Z}$-algèbres
munit $\mathbb{K}$ d'une structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel

$\mathbb{K}$ est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension finie

(c'est-à-dire : $\mathbb{K}$ admet une famille génératrice finie)
en tant que $\mathbb{Z}/p\mathbb{Z}$ espace vectoriel

$\mathbb{K}$ (qui est fini) est une famille génératrice de $\mathbb{K}$!

(Théorie des espaces vectoriels de dimension finie) Soit n la dimension de $\mathbb{K}$ en tant que $\mathbb{Z}/p\mathbb{Z}$ espace vectoriel. Il existe un isomorphisme de $\mathbb{Z}/p\mathbb{Z}$-espaces vectoriels

$$\mathbb{K} \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^n$$

iso de $\mathbb{Z}/p\mathbb{Z}$-algèbres ? $n \geq 2$

iso de $\mathbb{Z}/p\mathbb{Z}$-ev
donc une bijection

donc $\mathrm{card}(\mathbb{K}) = \mathrm{card}((\mathbb{Z}/p\mathbb{Z})^n) = [\mathrm{card}(\mathbb{Z}/p\mathbb{Z})]^n = p^n$

p premier, $n \in \mathbb{N}$, $n \geq 1$ — exhiber un corps fini de cardinal p^n ?

$n = 1$: $\mathbb{Z}/p\mathbb{Z}$

n quelconque : P élément irréductible de $\mathbb{Z}/p\mathbb{Z}[X]$ de degré n (existe-t-il un tel P ?)

$$\mathbb{L} = \mathbb{Z}/p\mathbb{Z}[X]/\langle P \rangle$$

$\mathbb{Z}/p\mathbb{Z}$ est un corps, $P \in \mathbb{Z}/p\mathbb{Z}[X]$ irréductible $\Rightarrow$ $P\,\mathbb{Z}/p\mathbb{Z}[X]$ est un idéal maximal de $\mathbb{Z}/p\mathbb{Z}[X]$

donc $\mathbb{L}$ est un corps

(Théorème 6 du chapitre 3) $\mathbb{L}$ est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension $\deg(P) = n$

$$\pi : \mathbb{Z}/p\mathbb{Z}[X] \longrightarrow \mathbb{L} = \mathbb{Z}/p\mathbb{Z}[X]/\langle P \rangle$$

(morphisme quotient)

(de base $1, \alpha, \alpha^2, \dots, \alpha^{\deg(P)-1}$)

$$X \longmapsto \alpha := \pi(X)$$

donc $\mathrm{card}(\mathbb{L}) = p^n$ (cf. raisonnement ci-dessus)

$p = 2$ $n = 2$ ($\mathbb{Z}/4\mathbb{Z}$ n'est pas un corps de cardinal 4)

$$P = \alpha X^2 + \beta X + \gamma \qquad \alpha \neq 0,\ \alpha, \beta, \gamma \in \mathbb{Z}/2\mathbb{Z} \qquad \alpha = \overline{1}_2,\ \beta, \gamma \in \{\overline{0}_2, \overline{1}_2\}$$

$\mathbb{Z}/2\mathbb{Z}$ est un corps, $\deg(P) = 2$: un tel P est irréductible $\Leftrightarrow$ P n'a pas de racine dans $\mathbb{Z}/2\mathbb{Z}$

$\Leftrightarrow \begin{cases} P(\overline{0}_2) \neq \overline{0}_2 \\ P(\overline{1}_2) \neq \overline{0}_2 \end{cases}$

$P = X^2 + X + \overline{1}_2$ est le seul polynôme irréductible de degré 2 de $\mathbb{Z}/2\mathbb{Z}[X]$

$P(\overline{0}_2) = \overline{0}_2^2 + \overline{0}_2 + \overline{1}_2 = \overline{1}_2 \neq \overline{0}_2$

$P(\overline{1}_2) = \overline{1}_2^2 + \overline{1}_2 + \overline{1}_2 = \overline{3}_2 = \overline{1}_2 \neq \overline{0}_2$

Donc $\mathbb{L} := \mathbb{Z}/2\mathbb{Z}[X]/\langle X^2 + X + \overline{1}_2 \rangle$ est un corps de cardinal 4.

Théorème : Le groupe des inversibles d'un corps fini est cyclique.

A anneau $\quad A^\times$ groupe

$n \in \mathbb{Z} \quad (\mathbb{Z}/n\mathbb{Z})^\times$

p premier $\quad (\mathbb{Z}/p\mathbb{Z})^\times$ cyclique $\quad$ générateur ?