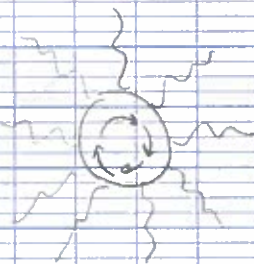


Compléments sur les corps



I Caractéristique:

Soit K un corps, on note $j: \begin{pmatrix} \mathbb{Z} & \rightarrow & K \\ n & \rightarrow & n1_K \end{pmatrix}$ c'est un morphisme

$$\text{Ker } j = n\mathbb{Z}$$

Th: (i) $n=0$ Alors K contient un sous corps isomorphe à \mathbb{Q}

(ii) $n \neq 0$ Alors n est un nombre premier et K contient un sous corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$

✓ K C.C

D/ (i) On pose pour $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ $\tilde{j}\left(\frac{p}{q}\right) = \frac{j(p)}{j(q)}$

\tilde{j} est correctement définie: car $\frac{p}{q} = \frac{p'}{q'}$ il vient $pq' - p'q = 0$

$$\text{donc } j(pq' - p'q) = 0 \text{ et } j(p)j(q') = j(p')j(q)$$

$$\frac{j(p)}{j(q)} = \frac{j(p')}{j(q')} \text{ dans } K$$

Suite calcul direct.

(ii) Si $k = l$ dans $\mathbb{Z}/p\mathbb{Z}$ alors $p/k = l$ ce

$$k-l = mp \Rightarrow j(k-l) = j(m)j(p) = 0$$

Le reste se fait alors par définition des lois

Not: $\text{Car}(K) = \mathbb{Q}$ ou $\text{Car}(K) = p$

On suppose $\mathbb{Q} \subset K$ ou $\mathbb{Z}/p\mathbb{Z} \subset K$

Ex $\mathbb{Z}/p\mathbb{Z} (x)$ est caractéristique p et infini

II Corps finis

Soit F_q un corps fini contenant $F_p = \mathbb{Z}/p\mathbb{Z}$ ($q = |F_q|$)

Prop: ① $\exists m \in \mathbb{N}^+ \quad q = p^m$

② F_q est un F_p -espace vectoriel de dim finie puisque'il est fini
Si (e_1, \dots, e_m) est une base de F_q sur F_p $\left(\begin{array}{c} F_p^m \rightarrow F_q \\ (x_i) \rightarrow \sum_{i=1}^m x_i e_i \end{array} \right)$
est un isomorphisme donc $|F_q| = p^m$

③ $\forall x \in F_q, x^q = x$

④ F_q^* est un groupe \times si $x \in F_q^*, x^{q-1} = 1, x^q = x$

$x \mapsto x^p$ ⑤ F_q^* est cyclique } Soit $a \in F_q^*$ $\omega(a) = \text{ppcm} \{ \omega(x) \mid x \in F_q^* \}$
alors $\forall x \in F_q^*, x^N = 1$ ou $x^N = 1$ possible
au plus n racines $\neq N = q-1$.

⑥ $\varphi \left(\begin{array}{c} x \mapsto x^p \\ F_q \rightarrow F_q \end{array} \right)$ est un automorphisme de F_q

$$\text{⑦ } \varphi(x+y) = (x+y)^p = \sum_{k=0}^p \binom{p}{k} x^k y^{p-k} \quad \text{donc } \binom{p}{k} \equiv 0 \pmod{p} \quad 1 \leq k \leq p-1$$
$$= x^p + y^p$$

$$F_q \text{ est lin } (\varphi(xy) = x^p y^p = \varphi(x)\varphi(y)) \dots$$

$\text{Ker } \varphi = \{0\}$ F_q domaine fini donc φ est bijectif
 $L = \text{im } \varphi$ est un corps.

Ex $\mathbb{F}_2 \left\{ \begin{pmatrix} a & bc \\ b & a \end{pmatrix} \mid (a, b) \in \mathbb{Z}/p\mathbb{Z} \right\}$ où c mat. inversible
dans $\mathbb{Z}/p\mathbb{Z}$ (p7,3)

$$aI + b \begin{pmatrix} 0 & c \\ 1 & 0 \end{pmatrix} = aI + bA, \quad \chi_A = X^2 - c \text{ irréductible}$$

$$\text{Soit } M \in \mathbb{F}_2 \setminus \{0\} \quad \det M = a^2 = b^2 c$$

$$\text{si } \det M = 0 \text{ on a } b = 0 \Rightarrow a = 0 \text{ Absur } M \neq 0$$

$$b \neq 0 \Rightarrow a^2 = b^2 c \Rightarrow \left(\frac{a}{b}\right)^2 = c \text{ A l'inverse}$$

$$\begin{pmatrix} a & bc \\ b & a \end{pmatrix} \begin{pmatrix} a' & b'c \\ b' & a' \end{pmatrix} = \begin{pmatrix} a a' + b b' c & c(ab' + ba') \\ c(ab + a'b) & b b' c + a a' \end{pmatrix}$$

$$\begin{pmatrix} a & bc \\ b & a \end{pmatrix}^{-1} = \frac{1}{a^2 - b^2 c} \begin{pmatrix} a & -bc \\ -b & a \end{pmatrix} \in \mathbb{F}_2$$