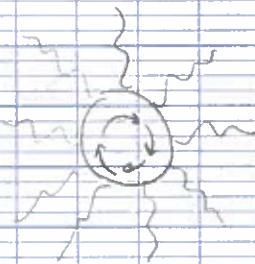


Compléments sur les corps



I Caractéristique:

Soit $P \in \mathbb{N}$ un corps, on note $\varphi : (\mathbb{Z} \rightarrow P)$ c'est un morphisme

$$\text{Ker } \varphi = m\mathbb{Z}$$

- Tb :
- i) $m=0$ Alors P contient un sous corps isomorphe à \mathbb{Q}
 - ii) $m > 1$ Alors m est un nombre premier et P contient un sous corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$

\sqrt{P} C.C

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

$\tilde{\varphi}$ est correctement définie: si $p/q = p'/q'$, il vient $pq - p'q' = 0$

$$\text{donc } \tilde{\varphi}(pq - p'q') = 0 \text{ i.e. } \tilde{\varphi}(p)\tilde{\varphi}(q) = \tilde{\varphi}(p')\tilde{\varphi}(q')$$

$$\frac{\tilde{\varphi}(p)}{\tilde{\varphi}(q)} = \frac{\varphi(p)}{\varphi(q)} \text{ dans } P$$

Si le calcul direct.

i) $\frac{m}{m} = 1 \in \mathbb{Z}$: $(1, 1)_P = 0 \rightarrow 1^2_P = 0 \text{ ou } 1^2_{\mathbb{Z}} = 0$ faux

ii) Si $k = l$ dans $\mathbb{Z}/p\mathbb{Z}$ alors $p/k = p/l$ i.e.

$$k-l = mp \Rightarrow \tilde{\varphi}(k-l) = \tilde{\varphi}(m)\tilde{\varphi}(p) = 0$$

Le résultat suit alors par définition des corps

Not: $\text{Car}(P) = \text{car}(\mathbb{F}_p) = p$

On suppose $(\mathbb{Q}) \subset P$ ou $\mathbb{Z}/p\mathbb{Z} \subset P$

$\exists \mathbb{Z}/p\mathbb{Z} (\times)$ est caractéristique p est infini

II Corps finis

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

Prop: ① $\exists n \in \mathbb{N}^*$ $q = p^n$

D/ \mathbb{F}_q est un \mathbb{F}_p -espace vectoriel de dim finie puisqu'il est fini

Si (e_1, \dots, e_m) est une base de \mathbb{F}_q sur \mathbb{F}_p ($\mathbb{F}_p^m \xrightarrow{(x_i) \rightarrow \sum x_i e_i} \mathbb{F}_q^m$)

est un isomorphisme donc $|F_q| = p^{m^*}$

② $\forall x \in \mathbb{F}_q^*, x^{q-1} = 0$

D/ \mathbb{F}_q^* est un groupe X si $x \in \mathbb{F}_q^*, x^{q-1} = 1, x^q = x$

③ \mathbb{F}_q^* est cyclique } Soit $a \in \mathbb{F}_q^*$ $\omega(a) = \min \{ \omega(x) \mid x \in \mathbb{F}_q^* \}$
 alors $\forall x \in \mathbb{F}_q^*, x^{\omega(a)} = 1$ on $x^N = 1$ possible au plus n racines $\neq N = q-1$.

④ $\Phi \left(\begin{matrix} x \mapsto x^p \\ \mathbb{F}_q \rightarrow \mathbb{F}_q \end{matrix} \right)$ est un automorphisme de \mathbb{F}_q

D/ $\Phi(x+y) = (x+y)^p = \sum_{k=0}^p \underbrace{\binom{p}{k}}_{\leq k \leq p+1 \text{ et } \binom{p}{k} \mid p!} x^k y^{p-k}$ donc $\binom{p}{k} \equiv 0$

$$= x^p + y^p$$

\mathbb{F}_q est un CC : $d(x,y) = x^p y^p = \Phi(x) \Phi(y) \dots$

$\{n \in \mathbb{N} : \Phi^n = \text{id}\}$ \mathbb{F}_q décomposé fini donc Φ est bijectif
 Lm \mathbb{F}_q 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 n'a pas de diviseur commun avec a
 demo $\mathbb{Z}/p\mathbb{Z}$ ($p \geq 3$)

$$aI + b \begin{pmatrix} 0 & c \\ 1 & 0 \end{pmatrix} = aI + bA, X_A = X^2 - c \text{ n'invertible}$$

Sait $M \in \mathbb{F}_2 \setminus \{0\}$ $\det M = a^2 - b^2c$

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

$$b \neq 0 \Rightarrow a^2 = b^2c \Rightarrow \left(\frac{a}{b}\right)^2 = c \text{ Ainsi}$$

$$\left(\begin{pmatrix} a & bc \\ b & a \end{pmatrix} \left(\begin{pmatrix} a' & b'c \\ b' & a' \end{pmatrix} = \begin{pmatrix} aa' + bb'c & c(ab' + ba') \\ c(ab - ab') & bb'c - aa' \end{pmatrix} \right) \right)$$

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