Compléments sur les corps

I Caractéristique

Soit $\mathbb{K}$ un corps, on note $j\begin{pmatrix}\mathbb{Z} \longrightarrow \mathbb{K} \\ n \longmapsto n1_{\mathbb{K}}\end{pmatrix}$ c'est un morphisme

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

Th : i) $n=0$ Alors $\mathbb{K}$ contient un sous corps isomorphe à $\mathbb{Q}$
ii) $n \geqslant 1$ Alors n est un nbre premier et $\mathbb{K}$ contient un sous corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$

$\sqrt{}$ $\mathbb{K}$ C.C

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

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

donc $j(pq' - p'q) = 0$ ie $j(p)j(q') = j(p')j(q)$

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

Suite calcul direct.

si $n = qr$ $(q 1_{\mathbb{K}})(r 1_{\mathbb{K}}) = 0 \longrightarrow q 1_{\mathbb{K}} = 0$ ou $r 1_{\mathbb{K}} = 0$ Abs

ii) Si $\bar{k} = \bar{l}$ dans $\mathbb{Z}/p\mathbb{Z}$ alors $p / k-l$ ie

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

Le reste se fait alors par définition des lois

Not $\operatorname{Car}(\mathbb{K}) = 0$ ou $\operatorname{Car}(\mathbb{K}) = p$

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

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

II Corps finis

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

__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 $(e_1, \ldots, e_n)$ est une base de $\mathbb{F}_q$ sur $\mathbb{F}_p$ $\left(\begin{array}{l} \mathbb{F}_p^n \longrightarrow \mathbb{F}_q \\ (x_i) \longrightarrow \sum_1^n x_i e_i \end{array}\right)$
est un isomorphisme donc $|\mathbb{F}_q| = |\mathbb{F}_p|^n$

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

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

$x^{p^n} - x$ ③ $\mathbb{F}_q^*$ est cyclique $\Big\{$ Soit $a \in \mathbb{F}_q^*$ $\omega(a) = \text{ppcm}\{\omega(x) \mid x \in \mathbb{F}_q^*\}$
alors $\forall x \in \mathbb{F}_q^*$, $x^N = 1$ Or $X^N - 1$ possède
au plus n racines $\neq N = q-1$.

④ $\varphi \left(\begin{array}{l} x \longmapsto x^p \\ \mathbb{F}_q \longrightarrow \mathbb{F}_q \end{array}\right)$ est un automorphisme de $\mathbb{F}_q$

D/ $\varphi(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$ donc $\binom{p}{k}$ $1 = 0$

$1 \leq k \leq p-1$ $p \mid \binom{p}{k}$

$= x^p + y^p$

$\mathbb{F}_q$ est un CC : $\varphi(xy) = x^p y^p = \varphi(x)\varphi(y)$ ...

$\operatorname{Ker} \varphi = \{0\}$ $\mathbb{F}_q$ de cardinal fini donc φ est bijectif
$\hookrightarrow$ im $\mathbb{F}_q$ est un corps.

Ex $\mathbb{F}_2 = \left\{ \begin{pmatrix} a & bc \\ b & a \end{pmatrix} \middle| (a,b) \in \mathbb{Z}/p\mathbb{Z} \right\}$ où c n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$ $(p \geq 3)$

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

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

si $\det M = 0$ on a $b = 0 \Rightarrow a = 0$ Alors on a $M \neq 0$

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

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

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