Chap 16 : Caractéristique

I. Généralités

A anneau unitaire

L'application $j\begin{cases}\mathbb{Z}\to A\\ n\mapsto n\times 1\end{cases}$ est un morphisme d'anneau. Son noyau est de la forme $q\mathbb{Z}, q\in\mathbb{N}$.

$\operatorname{car} A = q$ est appelé la caractéristique de A : $\forall x\in A, qx=0$

Si $q=0, j$ est un isomorphisme de $\mathbb{Z}$ sur un sous-anneau de A

Si $q\geq 1, j$ se factorise en un isomorphisme de $\mathbb{Z}/q\mathbb{Z}$ sur un sous-anneau de A

$\mathbb{K}$ corps

Si $\operatorname{car}\mathbb{K}=0, j$ s'étend en un isomorphisme de $\mathbb{Q}$ sur un sous-corps de $\mathbb{K}$

Si $\operatorname{car}\mathbb{K}\geq 2$, c'est un nombre premier p : $\mathbb{K}$ contient un sous-corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$

$\tilde{j}\left(\frac{m}{n}\right) j(m)\,j(n)^{-1}$ $\tilde{j}\Rightarrow$ mph inj de corps $\qquad p=ab\Rightarrow 0=j(p)=j(a)\,j(b)\Rightarrow j(a)=0$ ou $j(b)=0\Rightarrow p\mid a$ ou $p\mid b$

La 2^e proposition est vraie pour anneau intègre

Un corps premier est le plus petit sous-corps de $\mathbb{K}$: c'est le corps engendré par $1_{\mathbb{K}}$

Si $\operatorname{car}\mathbb{K}=0$, le corps premier "est" $\mathbb{Q}$ $\qquad$ Si $\operatorname{car}\mathbb{K}=p$ premier, le corps premier "est" $\mathbb{Z}/p\mathbb{Z}$

Un corps de caractéristique p peut être infini : $\mathbb{Z}/p\mathbb{Z}(X)$

II. Corps de caractéristique p ≥ 2

Tous les corps considérés sont commutatifs. $\mathbb{K}$ corps de caractéristique p

//HP// Morphisme de Frobenius : $\varphi\begin{cases}\mathbb{K}\to\mathbb{K}\\ x\mapsto x^p\end{cases}$ est un morphisme de corps injectif.

Si $\mathbb{K}$ est fini, c'est un automorphisme. $\qquad (x+y)^p=x^p+y^p$ $(\operatorname{car} p\mid C_p^k)$

$\mathbb{K}$ fini de car. p, $\mathbb{Z}/p\mathbb{Z}\subset\mathbb{K}\Rightarrow\mathbb{Z}/p\mathbb{Z}=\varphi^{-1}(\{0\})$ $\qquad$ (Fermat + n racines d'un polynôme)

$\mathbb{K}$ fini de car. p $\Rightarrow$ $\exists f\in\mathbb{N}^*$ tel que $\operatorname{car}\mathbb{K}=p^f$

Polynômes $\to$ Pas de formule de Taylor d'ordre $\geq p$.

$\to$ Pb avec la multiplicité des racines : $X^p-1=(X-1)^p$, $(X^p-1)'=0$

$\mathbb{K}$ corps fini commutatif $\qquad k\in\mathbb{Z}, S=\sum_{x\in\mathbb{K}^*}x^k=?$ $\qquad$ Si $\exists a\in\mathbb{K}^*, a^k\neq 1, S=0$ $\qquad$ Sinon, dans $\mathbb{Z}/p\mathbb{Z}$, $S=-1$

$\mathbb{K}^*$ est cyclique $(c$ tq $m=\omega(c)=\operatorname{ppcm}\{\omega(x)/x\in\mathbb{K}^*\}, x^{|\mathbb{K}|}=1\Rightarrow m\,||\,\mathbb{K}^*|, X^m-1$ a moins de m racines$)$

Utile : si $\mathbb{K}$ est fini, $a\in\mathbb{K}^*\Rightarrow x\mapsto ax$ bijection