Feuille de TD n° 5

Correction de l'exercice 1 de la feuille 5

a) Soit k un corps de cardinal q. Alors k est de cractéristique un nombre premier p. C'est-à-dire que l'image de

$$\mathbb{Z} \to k,\ 1 \mapsto 1$$

est isomorphe à $\mathbb{F}_p$. Comme k est fini, k est un $\mathbb{F}_p-$espace vectoriel de dimension finie d. Alors comme groupes :

$$(k, +) \simeq \mathbb{F}_p^d$$

donc $q = |k| = p^d$.
Soit $P(X) = X^{q^n} - X$. Dans k, on a $\underbrace{1 + 1 + ... + 1}_{p} = 0$ donc dans k, $m.1 = 0$ pour tout multiple m de p. En particulier $q^n.1 = 0$ et $P'(X) = -1$. En particulier, les racines de O sont simples (car $P \wedge P' = 1$. Notons K un corps de décomposition de $P(X)$. Dans K, le polynôme P a q^n racines. distinctes.
Or, $f_p : K \to K$, $x \mapsto x^p$ est un morphisme de corps (en caractéristique p). On vérifie que $f_p^s = f_{p^s} : x \mapsto x^{p^s}$ pour tout entier s. Donc $x \mapsto x^{q^n}$ est un endomorphisme du corps K.
Puisque k est de cardinal q, pour tout $x \in k$, on a $x = 0$ ou $x \in k^\times \Rightarrow x^{q-1} = 1$ car $k^\times$ est un groupe d'ordre $q - 1$. Donc

$$^\forall x \in k,\ x^q = x\ .$$

En particulier, $^\forall x \in K$, $x^{q^n} = x^{q^{n-1}} = ... = x^q = x$.
Donc l'ensemble des racines de P

$$\{x \in K\ :\ x^{q^n} = x\}$$

est un sous-corps de K qui contient k. Puisque K est engendré par les racines, on a $K =$ l'ensemble des racines de P.
Donc K est de cardinal q^n.

b) Notons $\mathbb{F}q^n$ un corps de cardinal q^n (corps de décomposition de $X^{q^n} - X$ sur $\mathbb{F}_q$). Soit $P(X)$ irréductible unitaire sur $\mathbb{F}_q$ de degré d. Si $P | X^{q^n} - X$, alors si α est une racine de P, c'est aussi une racine de $X^{q^n} - X$.
D'où les inclusions :

$$\mathbb{F}_q \leq \mathbb{F}_q[\alpha] \leq \mathbb{F}_{q^n}$$

Comme P est irréductible, $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = \deg P = d$. Par multiplicativité des degrés, $d|[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ †.

Réciproquement si $d|n$, alors comme P est irréductible, le corps

$$\mathbb{F}_q[X]/(P)$$

est de cardinal q^d. En particulier, $X^{q^d} \bmod P = X$ dans le corps $\mathbb{F}_q[X]/(P)$ *c-à-d* : $P|X^{q^d} - X$.

Or :

$$d|n \Rightarrow q^d - 1|q^n - 1 \text{ dans } \mathbb{Z}$$

$$\Rightarrow X^{q^d-1} - 1|X^{q^n-1} - 1 \text{ dans } \mathbb{Z}[X] \text{ et donc aussi dans } \mathbb{F}_q[X]$$

$$\Rightarrow X^{q^d} - X|X^{q^n} - X$$

Donc on a aussi $P|X^{q^n} - X$.

c) Comme $X^{q^n} - X \wedge (X^{q^n} - X)' = 1$, dans la décomposition de $X^{q^n} - X$ en facteurs irréductibles sur $\mathbb{F}_q$, chaque facteur irréductible unitaires n'apparaît qu'une seule fois.

Chaque facteur irréductible est de degré d avec $d|n$ et réciproquement si P est irréductible de degré $d|n$, alors P est un facteur de $X^{q^n} - X$, d'où :

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in I_d(q)} P \ .$$

d) En comparant les degrés, on trouve :

$$q^n = \sum_{d|n} \sum_{P \in I_d(q)} d$$

$$= \sum_{d|n} d|I_d(q)| \ .$$

Il suffit maiontenant d'utiliser la formule d'inversion de Möbius.

Redémontrons-la dans ce cas particulier.

Soit $f(d) = d|I_d(q)|$. Posons $F(n) = \sum_{d|n} f(d)$ $(= q^n)$.

On a :

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) F(d) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{e|d} f(e)$$

†. En effet, si on note l la dimension de $\mathbb{F}_{q^n}$ comme $\mathbb{F}_q-$espace vectoriel, on a $(\mathbb{F}_{q^n}, +) \simeq \mathbb{F}_q^l \Rightarrow q^n = q^l \Rightarrow n = l$

$$= \sum_{e|n} f(e) \sum_{e|d|n} \mu\left(\frac{n}{d}\right)$$

$$= \sum_{e|n} f(e) \sum_{d'|\frac{n}{e}} \mu\left(\frac{\frac{n}{e}}{d'}\right) \quad (*)$$

or, pour tout entier $m \geq 1$,

$$\sum_{k|m} \mu\left(\frac{m}{k}\right) = \begin{cases} 1 & \text{si } m = 1 \\ 0 & \text{si } m > 1. \end{cases}$$

En effet si $m = p_1^{a_1}...p_t^{a_t}$ pour certains nombres premiers deux à deux distincts [†] et $t \in \mathbb{N}$, alors :

$$\sum_{k|m} \mu\left(\frac{m}{k}\right) = \sum_{k=0}^{t} \sum_{1 \leq i_1 < ... < i_k \leq t} \mu(p_{i_1}...p_{i_k})$$

$$= \sum_{k=0}^{t} \sum_{1 \leq i_1 < ... < i_k \leq t} (-1)^k$$

$$= \sum_{k=0}^{t} \binom{t}{k} (-1)^k$$

$$= 0 \text{ si } t > 0, \ 1 \text{ si } t = 0 \ c\text{-}\grave{a}\text{-}d \ m = 1. \quad .$$

Donc dans la somme $(*)$, il ne reste que le terme où $\frac{n}{e} = 1$ c-$\grave{a}$-d $e = n$. D'où :

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$$

c-$\grave{a}$-d dans le cas qui nous intéresse :

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d = n|I_n(q)| \ .$$

Exemples.
— $I_2(2) = \frac{1}{2}(2^2 - 2) = 1$;
— $I_3(2) = \frac{1}{3}(2^3 - 2) = 2$;
— $I_4(2) = \frac{1}{4}(2^4 - 2^2) = 3$;
— $I_2(3) = \frac{1}{2}(3^2 - 3) = 3$;
— $I_3(4) = \frac{1}{3}(3^3 - 3) = 8$ ...

†. et > 0

Remarque. Pour tout q, puissance d'un nombre premier, et tout $n \geq 1$, $|I_n(q)| > 0$. En effet,[‡] le groupe $\mathbb{F}_{q^n}^\times$ est cyclique engendré par un élément α. *A fortiori* $\mathbb{F}_{q^n}^\times = \langle\alpha\rangle \Rightarrow \mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$. Mais alors le polynôme minimal de α sur $\mathbb{F}_q$ est unitaire, irréductible de degré n.

‡. Admettons qu'il existe un corps de cardinal q, il existe alors un corps de cardinal q^n pour tout n : il suffit de prendre un corps de décomposition de $X^{q^n} - X$ sur $\mathbb{F}_q$ ...