Feuille de TD n° 5

Exercice 1 Le nombre de polynômes irréductibles sur un corps fini

a) Soit k un corps de cardinal q. Montrer qu'un corps de décomposition du polynôme $X^{q^n} - X$ sur k est un corps de cardinal q^n.

b) Soit $\mathbb{F}_q$ un corps de cardinal q. Soit $P \in \mathbb{F}_q[X]$ irréductible de degré d. Montrer que
$$P \,|\, X^{q^n} - X \Leftrightarrow d \,|\, n \ .$$

c) On note $I_d(q)$ l'ensemble des polynômes irréductibles *unitaires* de degré d sur $\mathbb{F}_q$.
Déduire de la question précédente que :
$$X^{q^n} - X = \prod_{d|n} \prod_{P \in I_d(q)} P \ .$$

d) En déduire la formule :
$$|I_n(q)| = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$$
où $\mu(a) = (-1)^l$ si a est produit de l nombre premiers distincts et 0 sinon.

e) En déduire que
$$Z(t) := \frac{1}{1-t} \prod_P \frac{1}{1 - t^{\deg P}} = \frac{1}{(1-t)(1-qt)}$$
où P décrit les polynômes irréductibles unitaires dans $\mathbb{F}_q[X]$.
Indication. Calculer $\frac{Z'}{Z}$.

Exercice 2 Fractions rationnelles invariantes sur $\mathbb{F}_q$

Soit $\mathbb{F}_q$ un corps de cardinal q. On note G le groupe des automorphismes du corps $\mathbb{F}_q(X)$ définis par les changements de variables
$$X \mapsto \frac{aX + b}{cX + d}$$
où $a, b, c, d \in \mathbb{F}_q$ et $ad - bc \neq 0$.

a) Déterminer l'ordre du groupe G.

b) Montrer que $\mathbb{F}_q(X)^G = \mathbb{F}_q(Y)$ où
$$Y = \frac{(X^{q^2} - X)^{q+1}}{(X^q - X)^{q^2+1}} \ .$$

Exercice 3 Démonstration de la loi de réciprocité quadratique au moyen du résultant

a) Vérifier que pour tout $k \geq 1$, il existe un unique polynôme $T_k \in \mathbb{Z}[X]$ unitaire de degré k tel que

$$X^k + \frac{1}{X^k} = T_k\left(X + \frac{1}{X}\right) \ .$$

Indication. On pourra utiliser la formule de récurrence

$$T_{k+1}(y) + T_{k-1}(y) = yT_k(y) \ .$$

Soit p un nombre premier impair.
On note $F_p \in \mathbb{Z}[X]$ unitaire de degré $\frac{p-1}{2}$ tel que :

$$X^{\frac{p-1}{2}} F_p\left(X + \frac{1}{X}\right) = 1 + ... + X^{p-1} \ .$$

b) Montrer que $F_p(0) = \pm 1$.

c) Montrer que si $p \neq q$ sont premiers impairs, alors F_p, F_q sont premiers entre eux sur $\mathbb{F}_l$ pour chaque nombre premier l.

d) En déduire $\text{Rés}(F_p, F_q) = \pm 1$.
Indication. Par l'absurde. S'il existait l, nombre premier divisant $\text{Rés}(F_p, F_q)$*, alors les polynômes F_p et F_q auraient une racine commune dans une extension du corps $\mathbb{F}_l$ ...*

e) Que vaut $F_p(X)$ dans $\mathbb{F}_p[X]$?

f) En déduire que $\text{Rés}(F_p, F_q) = \left(\frac{q}{p}\right) \bmod p$.
Indication. On rappelle que $\left(\frac{q}{p}\right) = q^{\frac{p-1}{2}} \bmod p$!

g) En déduire la loi de réciprocité quadratique :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \ .$$