Université Claude Bernard LYON 1
Master MA Mathématiques générales
Algèbre et calcul formel

TD 4

Exercice 1.
Montrer que la décomposition en facteurs irréductibles de $X^{p^n} - X$ dans $\mathbb{F}_p[X]$ est donnée par :

$$X^{p^n} - X = \prod_{\substack{P \in \mathrm{Irr}_p(m) \\ m|n}} P$$

où $\mathrm{Irr}_p(m)$ désigne l'ensemble des polynômes unitaires , irréductibles de degré m dans $\mathbb{F}_p[X]$.

Exercice 2.
Soit K un corps fini ayant p^n élément ; montrer que le groupe $\mathrm{Gal}(K/\mathbb{F}_p)$ des automorphismes de K est engendré par $\mathcal{F}_{K/\mathbb{F}_p}$. En déduire que ce groupe est cyclique d'ordre n.

Exercice 3.

1. On considère les polynômes cyclotomiques Φ_n. Montrer que
   (a) $\Phi_{np}(X) = \Phi_n(X^p)/\Phi_n(X)$ pour p premier ne divisant pas n
   (b) $\Phi_{np^e}(X) = \Phi_{np}(X^{p^{e-1}})$ pour p premier ne divisant pas n
   (c) $\Phi_{p_1^{e_1}\cdots p_r^{e_r}}(X) = \Phi_{p_1\cdots p_r}(X^{p_1^{e_1-1}\cdots p_r^{e_r-1}})$
2. En déduire un algorithme permettant de calculer le polynôme Φ_n. Calculer Φ_{108}.

Exercice 4.
On considère des entiers $n \geq 2$ et p premier ne divisant pas n ; on désigne par m l'ordre de $\overline{p}$ dans $(\mathbb{Z}/\mathbb{Z}n)^\times$, par K un corps fini ayant p^m éléments, par $\mu_n(K)$ le sous-groupe de $K^\star$ formé des racines de $X^n - 1$ et par x un générateur du groupe $\mu_n(p)$.

1. Montrer que pour tout corps fini L, de caractéristique p, contenant l'ensemble des racines de $X^n - 1$ il existe un morphisme $f : K \longrightarrow L$ et que l'on a $f(\mu_n(K)) = \mu_n(L)$.
2. On considère la $\mathbb{Q}$-extension cyclotomique $C = \mathbb{Q}[\zeta]$ avec $\zeta = e^{\frac{2\pi i}{n}}$.
   (a) Montrer qu'il existe un unique automorphisme $\varphi_p : C \longrightarrow C$ de C tel que $\varphi_p(\zeta) = \zeta^p$.
   (b) En déduire un homomorphisme de groupes $\eta : \mathrm{Gal}(K/\mathbb{F}_p) \longrightarrow \mathrm{Gal}(C/\mathbb{Q})$ tel que $\eta(\mathcal{F}_{K/\mathbb{F}_p}) = \varphi_p$.
   (c) Montrer que η est injectif.
   (d) On rappelle que l'on a un isomorphisme de groupes :

   $$\theta : \mathrm{Gal}(C/\mathbb{Q}) \longrightarrow (\mathbb{Z}/\mathbb{Z}n)^\times$$

   caractérisé par la condition $\theta(\sigma) = \overline{k}$ avec $\sigma(\zeta) = \zeta^k$. Que vaut $\theta \circ \eta$?