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

Corrigé de la fiche de 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 $\mathbb{F}_p[X]$.

Corrigé.
Soit $P \in \mathrm{Irr}_p(m)$ avec m qui divise n ; $K = \mathbb{F}_p[X]/\langle P \rangle$ est un corps fini dans lequel P possède une racine donc $P|X^{p^m} - X$; comme $m|n$ on a $X^{p^m} - X|X^{p^n} - X$ et finalement $P|X^{p^n} - X$. Réciproquement soit $P \in \mathrm{Irr}_p(m)$ avec $P|X^{p^n} - X$; le corps fini $K = \mathbb{F}_p[X]/\langle P \rangle = \mathbb{F}_p[x]$ est l'ensemble des racines de $X^{p^m} - X$. Puisque $P(x) = 0$, x est racine de $X^{p^n} - X$ ie. on a $\mathcal{F}^n_{K/\mathbb{F}_p}(x) = 0$ de sorte que $\mathcal{F}^n_{K/\mathbb{F}_p} = 0$ d'où $m|n$.

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.

Corrigé.
On a $K = \mathbb{F}_p[x]$; on note $P = p_{x,\mathbb{F}_p}$ le polynôme minimal de x. L'ensemble de racines de P dans K est $\{x, x^p, \cdots, x^{p^{n-1}}\}$. Soit σ un automorphisme de K ; remarquons que σ laisse $\mathbb{F}_p$ fixé. Comme $\sigma(P(x)) = P(\sigma(x)) = 0$ on a que $\sigma(x) = x^{p^i}$ et comme x est élément primitif on a $\sigma = \mathcal{F}^i_{K/\mathbb{F}_p}$.

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}.

Corrigé.
1a. Montrons que $\Phi_n(X^p) = \Phi_{np}(X)\Phi_n(X)$. Le polynôme $\Phi_n(X)$ a pour racines les $x \in \mathbb{C}^\star$ qui sont d'ordre n tandis que $\Phi_{np}(X)$ a pour racines les $x \in \mathbb{C}^\star$ qui sont d'ordre np. Ces racines sont distinctes entre elles et les deux polynômes sont premiers entre eux .
Si x est d'ordre n, x^p est d'ordre n (car si $x^{pk} = 1$ on a $n|p$ et comme n et p sont premiers entre eux on a $n|k$ tandis que si x est d'ordre np, x^p est encore d'ordre n (car si $x^{pk} = 1$ on a $np|pk$donc $n|k$). Ainsi toute racine de $\Phi_{np}(X)\Phi_n(X)$ est racine de $\Phi_n(X^p)$. enfin on a :

$$\deg(\Phi_{np}(X)\Phi_n(X)) = \varphi(np) + \varphi(n) = (p-1\varphi(n + \varphi(n) = p\varphi(n) = \deg(\Phi_n(X^p)$$

d'où l'égalité des deux polynômes.

1b.Comparons les racines des polynômes $\Phi_{np^e}(X)$ et $\Phi_{np}(X^{p^{e-1}})$. Les racines de $\Phi_{np^e}(X)$ sont les $x \in \mathbb{C}^\star$ qui sont d'ordre np^e. Mais si x est d'ordre np^e, alors $x^{p^{e-1}}$ est d'ordre np : en effet si $x^{k\,p^{e-1}} = 1$ on a $np^e | k\,p^{e-1}$ d'où $np|k$ et par suite $x^{p^{e-1}}$ est racine de $\Phi_{np}(X)$ et x est une racine de $\Phi_{np}(X^{p^{e-1}})$. Toutes les racines de ces polynômes sont simples et l'on a $\deg(\Phi_{np^e}(X)) = \varphi(np^e)$ tandis que $\deg(\Phi_{np}(X^{p^{e-1}})) = p^{e-1}\deg(\Phi_{np}(X) = p^{e-1}\varphi(np)$ mais, comme n et p sont premeirs entre eux on a :

$$\varphi(np^e) = \varphi(n)\varphi(p^e) = p^{e-1}(p-1)\varphi(n) = p^{e-1}\varphi(p)\varphi(n) = p^{e-1}\varphi(np)$$

d'où l'égalité des polynômes considérés.
1c. Le cas $r = 1$ est un cas particulier de 1b.
Posons $n = p_1^{e_1} \cdots p_r^{e_r}$, $N := \dfrac{n}{p_1 \cdots p_r}$ et supposons par récurrence sur r que l'on a :

$$\Phi_n(X) = \Phi_{p_1 \cdots p_r}(X^N)$$

Posons $p = p_{r+1}$, $e = e_{r+1}$; par 3.b on a :

$$\Phi_{np^e}(X) = \Phi_{np}(X^{p^{e-1}})$$

par 3a on a :

$$\Phi_{np^e}(X) = \Phi_n(X^{p^e})/\Phi_n(X^{p^{e-1}})$$

l'hypothèse de récurrence montre que :

$$\Phi_{np^e}(X) = \Phi_{p_1 \cdots p_r}(X^{Np^e})/\Phi_{p_1 \cdots p_r}(X^{Np^{e-1}})$$

et on appliquant de nouveau 1a. on a

$$\Phi_{np^e}(X) = \Phi_{p_1 \cdots p_r p_{r+1}}(X^{Np^{e-1}})$$

On en déduit l'algorithme suivant :

Algorithme 1 (calcul polynôme cyclotomique)

1. *entrée* un entier $n \geq 2$
2. déterminer la liste $L := [p_1, \cdots, p_r]$ des diviseurs premiers de n
3. $F := \dfrac{X^{p_1} - 1}{X - 1}$
4. *boucle :* pour $i \in [2, \cdots, r]$ *:*
   (a) $F := \dfrac{F(X^{p_i})}{F(X)}$
5. $N := \dfrac{n}{p_1 \cdots p_r}$
6. *sortie* $F(X^N)$

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, de caractéristique p, L 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 $\theta \circ \eta$?

Corrigé.
1. Soit $p^{m'}$ le cardinal de L ; on a $n | p^{m'} - 1$ et par définition de m on a $m|m'$ d'où l'existence d'un morphisme $f : K \longrightarrow L$; si $x \in \mu_n(K)$ on a $x^n = 1$ d'où $f(x)^n = 1$ *ie.* $f(x) \in \mu_n(L)$ d'où $f(\mu_n(K)) \subset \mu_n(L)$. Comme f est injectif, les deux membres ont le même nombre d'éléments et l'on a l'égalité.
2.a On a $p_{\zeta,\mathbb{Q}} = \Phi_n$ d'où un isomorphisme $F_1 : \mathbb{Q}[X]/\langle\Phi_n\rangle \longrightarrow C$ caractérisé par $F_1(\overline{X}) = \zeta$. Comme ζ^p est un générateur de $\mu_n(\mathbb{C})$ donc un élément primitif de C, on a de même un isomorphisme $F_p : \mathbb{Q}[X]/\langle\Phi_n\rangle \longrightarrow C$ caractérisé par $F_p(\overline{X}) = \zeta^p$ et il suffit de poser $\varphi_p = F_p\, F_1^{-1}$.
2.b $\mathrm{Gal}(K/\mathbb{F}_p)$ est un groupe cyclique d'ordre m engendré par $\mathcal{F}_{K/\mathbb{F}_p}$. Mais on a $\varphi_p^m(\zeta) = \zeta^{p^m} = \zeta$ puisque $p^m \equiv 1 \bmod n$ d'où $\varphi_p^m = \mathrm{id}_C$. Il en résulte l'existence de $\eta : \mathrm{Gal}(K/\mathbb{F}_p) \longrightarrow \mathrm{Gal}(C/\mathbb{Q})$ tel que $\eta(\mathcal{F}_{K/\mathbb{F}_p}) = \varphi_p$.
2.c De plus si $\varphi_p^{m'} = \mathrm{id}_C$ on a $\varphi_p^{m'}(\zeta) = \zeta^{p^{m'}} = \zeta$ d'où $\zeta^{p^{m'}-1} = 1$ et $n|p^{m'} - 1$. On a donc $m|m'$ *ie.* φ_p est d'ordre m et par suite η est injectif.
2.d Remarquons que θ est bien défini, que c'est un homomorphisme injectif de groupes donc un isomorphisme puisque les deux membres ont le même nombre d'éléments[1]. On a alors $\theta \circ \eta(\mathcal{F}_{K/\mathbb{F}_p}) = \overline{p}$ de sorte que $\theta \circ \eta$ est un isomorphisme de $\mathrm{Gal}(K/\mathbb{F}_p)$ sur le sous-groupe $\langle\overline{p}\rangle$ de $(\mathbb{Z}/\mathbb{Z}n)^\times$ engendré par $\overline{p}$.

1. car la $\mathbb{Q}$-extension C est galoisienne donc $\mathrm{Card}(\mathrm{Gal}(C/\mathbb{Q})) = [C : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n)$