Polynômes cyclotomiques

1 Rappels

Le polynôme cyclotomique d'ordre n est le polynôme défini sur $\mathbb{C}$ par

$$\phi_n(X) = \prod_{1\leq i\leq n/\ \mathrm{pgcd}(n,i)=1} X - \xi^i$$

où $\xi = e^{\frac{2i\pi}{n}}$ est une racine primitive n-ème de l'unité. On a $\deg \phi_n = \varphi(n)$ avec φ l'indicatrice d'Euler.

Exemple. *Les premiers polynômes cyclotomiques sont* $\phi_1 = X-1, \phi_2 = X+1, \phi_3 = (X-j)(X-j^2) = X^2+X+1, \phi_4 = (X-i)(X+i) = X^2+1$ *Plus généralement, pour tout p premier* $\phi_p = X^{p-1}+\cdots+X+1$.

On voit que les premiers polynômes cyclotomiques sont à coefficients entiers, c'est en fait vrai pour tous les polynômes cyclotomiques bien qu'ils soient, à priori, définis sur $\mathbb{C}$.

Le fait qu'ils soient à coefficients dans $\mathbb{Z}$ permet de les "considérer" sur n'importe quel corps K, on note toujours ϕ_n son image dans $K[X]$. La faculté qu'a ϕ_n à reconnaître les racines primitives n-ème de l'unité persiste quand sur n'importe quel corps. On résume dans le théorème suivant les propriétés importantes des polynômes cyclotomiques.

Théorème. *Soit* ϕ_n *le n-ème polynôme cyclotomique. Alors*

1. $\phi_n \in \mathbb{Z}[X]$
2. ϕ_n *est irréductible sur* $\mathbb{Q}$.
3. *Pour tout corps* K *de caractéristique* p *tel que* $\mathrm{pgcd}(p,n) = 1$, *alors les racines de* ϕ_n *dans* K *sont exactement les racines primitives n-ème de l'unité dans* K.

Cette dernière propriété est particulièrement intéressante pour $K = \mathbb{F}_q$ un corps fini. En effet, $\mathbb{F}_q^\times$ est cyclique de cardinal $q-1$ donc pour tout diviseur n de $q-1$, $\mathbb{F}_q^\times$ admet un élément α d'ordre n, i.e., $\alpha^n = 1$ mais $\alpha^k \neq 1$ pour $k \leq n$. Ceci revient à dire que α est une racine primitive n-ème de l'unité donc une racine de $\phi_n \in \mathbb{F}_q[X]$.

2 Exercices

Exercice 1 - image canonique de ϕ_n sur n'importe quel anneau

1. Soit A un anneau commutatif unitaire. Rappeler pourquoi il existe un unique morphisme d'anneau $\mathrm{char}\colon \mathbb{Z} \to A$.
2. Montrer qu'il existe un unique morphisme d'anneau $\mathrm{ev}_X\colon \mathbb{Z}[X] \to A[X]$ tel que $\mathrm{ev}_X(X) = X$ et $\mathrm{ev}_X(a) = \mathrm{char}(a)$ pour tout $a \in \mathbb{Z}$ *(pensez à utiliser les propriétés universelles).*
3. Donner une explication rigoureuse de la phrase ci-dessous en terme de ce qui vient d'être fait.

> Le fait qu'ils soient à coefficients dans $\mathbb{Z}$ permet de les "considérer" sur n'importe quel corps K, on note toujours ϕ_n son image dans $K[X]$.

Exercice 2 - Un anneau unique pour les contenir toutes

Soit $\phi_n \in K[X]$, montrer qu'une extension de rupture L de ϕ_n est aussi un corps de décomposition de ϕ_n. Que cela signifie-t-il en termes des racines primitives n-ème de l'unité dans L ?

Exercice 3 - Calculs de polynômes cyclotomiques

1. Montrer que $\phi_{2n}(X) = \phi_n(-X)$ pour n impair et $\phi_{2n}(X) = \phi_n(X^2)$ pour n pair.
2. Montrer que si $n = p^\alpha$ alors $\phi_n(X) = \phi_p(X^{\frac{n}{p}})$.
3. Déterminer ϕ_{12} et ϕ_8.

Exercice 4 - Polynômes cyclotomiques et corps finis

1. Le polynôme ϕ_6 est-il irréductible dans $\mathbb{F}_{61}[X]$? Dans $\mathbb{F}_{53}[X]$?
2. Le polynôme ϕ_9 est-il irréductible dans $\mathbb{F}_{19}[X]$? Dans $\mathbb{F}_{31}[X]$?
3. Donner une racine évidente de ϕ_3 dans $\mathbb{F}_{31}$. En déduire un générateur de $\mathbb{F}_{31}^\times$.
4. Donner une racine évidente de $\phi_4 = X^2+1$ dans $\mathbb{F}_{37}$. Montrer que $\phi_9(4) = 0 \in \mathbb{F}_{37}$. Donner un générateur de $\mathbb{F}_{37}^\times$.

Exercice 5 - Première loi de réciprocité quadratique

Montrer que -1 est un carré modulo p si, et seulement si, $p \equiv 1 \mod 4$.

Exercice 6 - Un polynôme irréductible sur $\mathbb{Q}[X]$ mais réductible sur $\mathbb{F}_p[X]$ pour tout p

On considère le polynôme $\phi_8 = X^4 + 1$.

1. Factoriser ϕ_8 dans $\mathbb{R}$. Est-il irréductible dans $\mathbb{Q}(\sqrt{2})$?
2. On souhaite montrer que $X^4 + 1$ est *réductible* sur $\mathbb{F}_p$ pour tout premier p.
   (a) Commencez par donner une factorisation de $\phi_8(X)$ sur $\mathbb{F}_2$.
   (b) Montrez que pour tout $p \neq 2$, $\mathbb{F}_{p^2}^\times$ contient un élément d'ordre 8.
   (c) Conclure que $\phi_8(X)$ n'est pas irréductible sur $\mathbb{F}_p$.
3. Décomposez $\phi_8(X)$ en produit de facteurs irréductibles dans $\mathbb{F}_7[X]$.

(on verra plus tard qu'il existe un critère d'irréductibilité des polynômes cyclotomiques ϕ_n sur $\mathbb{F}_q$).

Étant donnée la longueur de la feuille nous n'auront pas le temps de tout corriger pendant sur le créneau de 2h du TD. Si vous souhaitez des indications ou que vous avez des remarques ou corrections à apporter vous pouvez me contacter à fabien.narbonne@posteo.net ou venir me voir au bureau 634 du bâtiment 23.

Bonne préparation :) !