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* 0 *ou* 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 ($\star$)

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 ($\star$)

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 - Factorisation en irréductibles de $X^n - 1$ ($\star$)

Montrer que la factorisation en irréductibles dans $\mathbb{Q}[X]$ de $X^n - 1$ est

$$X^n - 1 = \prod_{d|n} \phi_d(X).$$

Exercice 4 - Calculs de polynômes cyclotomiques ($\star$)

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 5 - Polynômes cyclotomiques et corps finis ($\star$)

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 6 - Première loi de réciprocité quadratique ($\star$)

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

Exercice 7 - Un polynôme irréductible sur $\mathbb{Q}[X]$ mais réductible sur $\mathbb{F}_p[X]$ pour tout p ($\star\star$)

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 $\mathbb{F}_q$).

Exercices avancés pouvant servir de développement

Exercice 8 - Préliminaires commun aux Théorèmes A et B ($\star\star$)

Les deux questions suivantes sont indépendantes mais servent toutes les deux aux deux exercices suivants.

1. Soit L un corps contenant une racine primitive n-ème de l'unité α. On pose $\mu_n'(L)$ l'ensemble de toutes les racines primitives n-ème dans L. Montrer que
$$\mu_n'(L) = \{\alpha^\ell / \operatorname{pgcd}(\ell, n) = 1\}$$
(i.e., $(\mathbb{Z}/n\mathbb{Z})^\times$ agit simplement transitivement sur $\mu_n'(L)$).
2. **Un critère d'irréductibilité :** Soit $F \in K[X]$ un polynôme unitaire et K/L une extension de K dans lequel F est scindé à racines simples, $F(X) = \prod(X - z_i)$. On suppose que pour tout i, j il existe un automorphisme de $\sigma : L \to L$ invariant sur K tel que $\sigma(z_i) = z_j$. Montrer que F est irréductible dans $K[X]$.
*(on pourra poser P un diviseur non trivial unitaire de F **dans** $K[X]$, remarquer que P est scindé dans L et montrer que toutes les racines de F sont des racines de P).*

Exercice 9 - Théorème (A) - Critère d'irréductibilité de ϕ_n sur les $\mathbb{F}_q$ ($\star\star\star$)

On souhaite montrer le théorème suivant :

Théorème (A)**.** *Soit n et $q = p^s$ premiers entre eux alors ϕ_n irréductible dans $\mathbb{F}_q[X]$ si et seulement si la classe de q dans $\mathbb{Z}/n\mathbb{Z}$ engendre $(\mathbb{Z}/n\mathbb{Z})^\times$.*

On pose $\mathbb{F}_q$ le corps à q élément, n premier à q et L une extension finie de $\mathbb{F}_q$ contenant $\mu_n'(L)$, l'ensemble des racines primitives n-ème de l'unité, i.e., les racines de ϕ_n. On pose aussi

$$\begin{array}{rccc} \sigma_q : & L & \longrightarrow & L \\ & x & \longmapsto & x^q \end{array}$$

et on rappelle que $\sigma_q(x) = x$ si, et seulement si, $x \in \mathbb{F}_q$. Soit $\alpha \in \mu_n'(L)$. On définit $\Lambda_\alpha = \{\alpha^{q^j}, j \in \mathbb{N}\}$.

1. Montrer que si la classe de q engendre $(\mathbb{Z}/n\mathbb{Z})^\times$ alors $\Lambda_\alpha = \mu_n'(L)$. En déduire que ϕ_n est irréductible.

On suppose désormais que ϕ_n est irréductible. On pose $P = \prod_{\lambda \in \Lambda_\alpha}(X - \lambda) \in L[X]$. On va montrer que si q n'engendre pas $(\mathbb{Z}/n\mathbb{Z})^\times$ alors P est un diviseur stricte de ϕ_n dans $\mathbb{F}_q[X]$.

2. Montrer que σ_q décrit une bijection de Λ_α dans lui même.
3. En déduire que $P \in \mathbb{F}_q[X]$.
4. Conclure.

Exercice 10 - Irréductibilité de ϕ_d pour $d|n$ ($\star\star\star\star$)

On souhaite montrer le théorème suivant :

Théorème (B)**.** *Soit n un entier et K un corps de caractéristique nulle ou p tel que $\operatorname{pgcd}(n, p) = 1$. On suppose que ϕ_n irréductible dans $K[X]$. Alors pour tout $d|n$, ϕ_d irréductible dans $K[X]$.*

1. Soit $d|n$. Montrer que le morphisme $\pi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ de réduction modulo d induit un morphisme surjectif
$$(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/d\mathbb{Z})^\times.$$
(on pourra montrer que c'est le cas pour $n = p^a$ et $d = p^b$ avec $b \leq a$ puis prouver le cas général à l'aide du théorème des restes).

On suppose maintenant ϕ_n irréductible et on pose $L = K[X]/\phi_n$ un corps de rupture de ϕ_n et ω la classe de X dans L. Soient $\alpha, \beta \in \mu_n'(L)$ on veut montrer qu'il existe $\sigma : L \to L$ qui fixe K tel que $\sigma(\alpha) = \beta$.

2. Montrer que le morphisme
$$\begin{array}{rccc} \gamma : & \mu_n'(L) & \longmapsto & \mu_d'(L) \\ & \alpha & \longmapsto & \alpha^{n/d} \end{array}$$
est surjectif.

3. Justifier le fait qu'il existe $r, \ell \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que $\alpha = \omega^r$ et $\beta = \omega^{r\ell}$.
4. Soit ℓ premier à n, on pose
$$\begin{aligned} K[X] &\longmapsto L \\ F(X) &\longmapsto F(\omega^\ell). \end{aligned}$$
Montrer que ce morphisme d'anneau induit un morphisme de corps $\sigma_\ell : L \to L$ qui laisse K invariant.
5. Montrer que $\sigma_\ell(\alpha^{n/d}) = \beta^{n/d}$. En déduire que ϕ_d est irréductible dans $K[X]$.
6. Montrer que σ_ℓ est un automorphisme *(on se rappelle qu'un automorphisme de corps est toujours injectif et qu'une extension L de L de degré m est en particulier un L-espace vectoriel de dimension m).*
7. Conclure.

Application de ces résultats

Exercice 11 - Réductibilité des polynômes cyclotomiques sur $\mathbb{F}_q$ ($\star\star$)

1. Montrer que $(\mathbb{Z}/8\mathbb{Z})^\times$ n'est pas cyclique. Retrouver le résultat comme quoi ϕ_8 est réductible sur $\mathbb{F}_p[X]$ pour tout premier p.
2. Montrer que ϕ_n est réductible sur $\mathbb{F}_q[X]$ pour tout q si et seulement si $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique *(on pourra appliquer le théorème de la progression arithmétique pour le sens non trivial).*
3. Quelles sont les polynômes cyclotomiques réductibles sur tous les corps finis ? *(on pourra utiliser l'exercice 9 de la feuille précédente sur les groupes cycliques).*

Exercice 12 - Un petit résultat de divisibilité ($\star\star$)

1. Soit $P \in K[X]$ un polynôme de degré m. Montrer que P est irréductible sur K si et seulement si P n'a pas de racine dans L pour tout extension de K de degré $d < m$.
2. Soit d le plus petit entier tel qu'il existe une extension L de K de degré d dans laquelle P a une racine. Est-ce que d divise m ? Est-ce le cas si P est un polynôme cyclotomique ?
3. Soit $p \neq 2$. Montrer que pour tout $r \geq 3$ on a $2^r | p^{2^{r-2}} - 1$ on pourra appliquer la question précédente à ϕ_{2^r} et $K = \mathbb{F}_p$.

Remarques sur les théorèmes A et B

Je me suis servi de la page suivante pour faire ces exercices

https ://agreg-maths.univ-rennes1.fr/documentation/docs/Cyclotomiques.pdf

Apparemment, on peut aussi trouver le théorème A dans Demazure, Algèbre, coro 8.15 p206.

Les théorèmes A et B peuvent chacun faire un développement pour l'agrégation. J'ai moi-même proposé ces deux théorèmes en développement lors de mon oral d'algèbre pour la leçon "Leçon 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications."

Je me suis permis d'adapter les notes de Daniel Ferrand à ma façon. J'ai quelque peu modifié certaines parties, notamment la question 1 de l'exercice 10 est traitée différemment dans le document original (ça ne fait pas intervenir le théorème des restes). Il me semble aussi que l'hypothèse σ automorphisme peut être supprimée du critère d'irréductibilité de l'exercice 8 et donc on pourrait supprimer la question 6 de l'exercice 10 (un morphisme de corps est toujours injectif mais il ne me semble pas que l'hypothèse de surjectivité serve quelque part). Je ne suis cependant pas sur à 100% donc j'ai préféré laissé tel quel. Si vous trouvez des erreurs ou des simplifications ou que vous avez des commentaires à faire je vous prie de m'en faire part.

Attention au fait que ces développements sont assez difficiles, sentez vous à l'aise pour les faire. Il me semble que ces résultats sont assez méconnus en général et qu'il faut donc être doublement vigilant.e si vous les présentez (une coquille peut s'être glissée quelque part sans que personne ne l'ai vu jusqu'à maintenant). Notez bien que l'ensemble des automorphismes de L qui fixent K est couramment noté $\mathrm{Gal}(L/K)$ et est un objet central en théorie de Galois. Il est donc fort probable qu'un.e des membres du jury vous attaque dessus. Cette théorie est hors programme de l'agrégation et vous pouvez donc tout à fait légitimement indiquer au jury que vous n'êtes pas à l'aise avec cette théorie et il ne vous embêtera pas plus dessus (en principe). En effet, même si la terminologie fait penser à la théorie de Galois, **tout ce qui est utilisé ici est démontré et figure au programme de l'agrégation**.

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 :) !