
Corps finis

On construit des corps finis comme des extensions finies d'un corps fini $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, où p est un premier, le sous-corps premier. (Le sous-corps \mathbb{Q} d'un corps de caractéristique 0 s'appelle également un sous-corps premier.)

Tout corps fini est une extension finie de son sous-corps premier, et il sont semblables aux extensions cyclotomiques $\mathbb{Q}(\zeta_n)$ de \mathbb{Q} . On développe et précise les analogies et les rapports avec des corps cyclotomiques dans la suite.

Polynômes cyclotomiques

Soit $\Phi_n(x)$ le *polynôme cyclotomique* défini récursivement par

$$x^n - 1 = \prod_{m|n} \Phi_m(x).$$

En particulier, $\Phi_1(x) = x - 1$ et pour p premier, $\Phi_p(x) = x^{p-1} + \dots + x + 1$.

Rappel. La *caractéristique* d'un anneau A (unitaire) est le générateur (non-négatif) du noyau de l'unique homomorphisme $\mathbb{Z} \rightarrow A$.

Propriétés des polynômes cyclotomiques en caractéristique 0

1. $\Phi_n(x) \in \mathbb{Z}[x]$
2. $\Phi_n(x)$ est irréductible dans $\mathbb{Q}[x]$.
3. $\deg(\Phi_n(x)) = \varphi(n)$ ($= |\mathbb{Z}/n\mathbb{Z}^*|$ par définition)
4. Dans $\mathbb{C}[x]$, on a

$$\Phi_n(x) = \prod_{k \in \mathbb{Z}/n\mathbb{Z}^*} (x - \zeta_n^k),$$

où $\zeta_n = e^{2\pi i/n}$.

5. $\mathbb{Q}[x]/(\Phi_n(x)) \cong \mathbb{Q}(\zeta_n)$ et $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}^*$

Les groupes cycliques $\mu_n = \{\zeta_n^k \mid k \in \mathbb{Z}/n\mathbb{Z}\}$ des racines n -ièmes de l'unité sont les seuls sous-groupes finis de \mathbb{C}^* , et les polynômes cyclotomiques sont les polynômes minimaux de ces éléments distingués. Par ailleurs, tous les éléments non nuls d'un corps fini ont un ordre fini (et le groupe \mathbb{F}_q^* est un groupe cyclique), donc les polynômes cyclotomiques jouent un rôle important dans la théorie des corps finis.

Propriétés des polynômes cyclotomiques en caractéristique p

1. Si $n = p^r - 1$, alors $\Phi_n(x)$ est un produit de polynômes irréductibles de degré r .
2. Si n et p sont premiers entre eux et r est l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^*$, alors $\Phi_n(x)$ est un produit de polynômes irréductibles de degré r .

3. Si n et p sont premiers entre eux, alors $\Phi_{p^i n}(x) = \Phi_n(x)^{\varphi(p^i)}$.

En utilisant le fait que tout corps fini de q éléments est le corps de décomposition de $x^q - x$, on démontre le théorème suivant, duquel on dérive les propriétés ci-dessus.

Théorème. *Pour chaque p premier et $r \geq 1$, il existe un et un seul corps, à isomorphisme près, avec p^r éléments.*

Preuve des propriétés des polynômes cyclotomiques.

1. Chaque racine de $\Phi_n(x)$ dans \mathbb{F}_{p^r} est un générateur du groupe $\mathbb{F}_{p^r}^*$, donc aussi de l'extension $\mathbb{F}_{p^r}/\mathbb{F}_p$. Par conséquent, elle satisfait une polynôme minimal de degré r .
2. Soit α une racine de $\Phi_n(x)$ dans \mathbb{F}_{p^r} ; alors l'ordre de α dans $\mathbb{F}_{p^r}^*$ est n . Les conditions suivantes sont équivalentes :
 - α est un élément de \mathbb{F}_{p^s} .
 - n divise $p^s - 1$.
 - l'ordre de p modulo n divise s .

Si un élément α n'est pas contenu dans \mathbb{F}_{p^s} pour un diviseur propre s de r , il engendre l'extension $\mathbb{F}_{p^r}/\mathbb{F}_p$, et son polynôme minimal (sur \mathbb{F}_p) est de degré r . Par conséquent, les diviseurs irréductibles de $\Phi_n(x)$ sont tous de degré r .

Remarque. Si $n = p^r - 1$, alors l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^*$ est r , donc ce résultat est une généralisation du résultat précédent.

On peut construire "le" corps fini à p^r éléments, comme $\mathbb{F}_{p^r} = \mathbb{F}_p[\zeta_n]$ où le polynôme minimal de ζ_n est un diviseur $f_n(x)$ de degré r du polynôme cyclotomique $\Phi_n(x)$, pour $n = p^r - 1$. En général, il y a plusieurs choix de diviseur irréductible de $\Phi_n(x)$, et si $m|n$, ($m \neq n$) est tel que l'ordre de p est (toujours) r modulo m (dans le quotient de groupes $\mathbb{Z}/n\mathbb{Z}^* \rightarrow \mathbb{Z}/m\mathbb{Z}^*$), on a $\mathbb{F}_p[\zeta_m] \cong \mathbb{F}_p[\zeta_n]$.

Éléments primitifs de $\mathbb{F}_{p^r}/\mathbb{F}_p$ et $\mathbb{F}_{p^r}^*$. Dans une extension L/K , on dit que $\alpha \in L$ est un élément *primitif* (relatif à K) si $L = K[\alpha]$. Pour toute extension finie de corps, il existe un élément primitif. Pour un corps fini $K = \mathbb{F}_{p^r}$ un élément α du groupe $\mathbb{F}_{p^r}^*$ est *primitif* si et seulement si l'ordre de α est $p^r - 1$. Dans le premier cas, la définition de primitif concerne la propriété d'être un générateur de L comme K -algèbre et dans le deuxième elle concerne la propriété d'être un générateur du groupe K^* . Un polynôme de degré r dans $\mathbb{F}_p[x]$ est dit primitif si et seulement s'il est le polynôme minimal d'un élément primitif de $\mathbb{F}_{p^r}^*$.

Exercices

1. Combien d'anneaux (commutatifs) d'ordre 4 est-il y a ? (Indication : Considérer les éventuels homomorphismes surjectifs $\mathbb{Z} \rightarrow R$ ou $\mathbb{F}_2[x] \rightarrow R$.)
2. Montre que r divise $\varphi(p^r - 1)$. Plus généralement, pour tout entier $a > 1$ et $r \geq 1$, démontrer que r divise $\varphi(a^r - 1)$. (Indication : utiliser le théorème de Lagrange.)
3. Trouver les premiers p et les entiers $r \geq 1$ tel qu'il existe un seul polynôme primitif de degré r dans $\mathbb{F}_p[x]$.
4. Montrer qu'il existe un polynôme irréductible de degré r dans $\mathbb{F}_p[x]$ pour tout premier p et entier r .
5. Montrer qu'il existe un polynôme primitif de degré r dans $\mathbb{F}_p[x]$ pour tout premier p et entier r .
6. Démontrer l'unicité du corps de q éléments en le décrivant comme corps de décomposition de $x^q - x$.
7. Montrer que $x^p - x - a$ est irréductible dans $\mathbb{F}_p[x]$ pour tout a dans \mathbb{F}_p^* .
8. Déterminer la factorisation de $\Phi_7(x)$ dans $\mathbb{F}_2[x]$.
9. Décrire les éléments primitifs de $\mathbb{F}_{2^3}/\mathbb{F}_2$ et de $\mathbb{F}_{2^3}^*$ en termes de racines des polynômes cyclotomiques.
10. Déterminer la factorisation de $\Phi_{15}(x)$ dans $\mathbb{F}_2[x]$.
11. Décrire les éléments primitifs de $\mathbb{F}_{2^4}/\mathbb{F}_2$ et de $\mathbb{F}_{2^4}^*$ en termes des racines des polynômes cyclotomiques.
12. Trouver des isomorphismes :

$$\mathbb{F}_2[\zeta_{15}] = \mathbb{F}_2[x]/(x^4 + x + 1) \longrightarrow \mathbb{F}_2[\zeta_5] = \mathbb{F}_2[x]/(x^4 + x^3 + x^2 + x + 1),$$

et

$$\mathbb{F}_2[\zeta_{15}] = \mathbb{F}_2[x]/(x^4 + x + 1) \longrightarrow \mathbb{F}_2[\zeta_{15}] = \mathbb{F}_2[x]/(x^4 + x^3 + 1).$$

13. Montrer que $\phi(\alpha) = \alpha^p$ est un homomorphisme d'anneaux $A \rightarrow A$ pour tout anneau A de caractéristique p premier. Il s'appelle l'endomorphisme de Frobenius (ou l'automorphisme de Frobenius lorsqu'il est un isomorphisme).
14. Montrer que tout homomorphisme d'un corps K est injectif, et conclure que l'endomorphisme de Frobenius est un automorphisme dans le cas d'un corps fini.
15. Soit $\phi : \mathbb{F}_q \rightarrow \mathbb{F}_q$ l'automorphisme de Frobenius, où $q = p^r$. Déterminer les éléments fixés par ϕ et par ϕ^r .
16. Démontrer que $\text{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle \phi \rangle$, un groupe cyclique d'ordre r .