



école
normale
supérieure

PRÉPARATION À L'AGRÉGATION

LEÇONS 120 121 123 125 141 144

Réductibilité des polynômes cyclotomiques sur les corps finis



MIANNAY MATTEO

<https://perso.eleves.ens-rennes.fr/people/matteo.miannay> (lien cliquable)

1 Ce que nous allons faire

Une étude assez complète des polynômes cyclotomiques sur les corps finis. Je pense que c'est un très bon développement. Attention, c'est fait main.

2 Introduction

On fixe $q = p^\alpha$ une puissance d'un nombre premier. on se place donc sur \mathbb{F}_q , on se donne n premier avec q et on note \mathbb{L} le corps de décomposition de $X^n - 1$ sur \mathbb{F}_q .

2.1 Racines de l'unité et racines primitives de l'unité

Déjà, $X^n - 1$ est à racines simples sur L . En effet, son polynôme dérivé est nX^{n-1} qui a pour seule racine 0 car on a choisi n et p premiers entre eux. Donc sur \mathbb{L} $X^n - 1$ a n racines, et on est donc dans la même situation que sur \mathbb{C} : on a bien n racines n -ièmes de l'unité. Ces racines, que l'on notera, au hasard, \mathbb{U}_n , forment un sous-groupe de L^* . Les sous-groupes finis du groupe multiplicatif d'un corps fini étant cycliques, \mathbb{U}_n admet $\varphi(n)$ générateurs, les racines primitives de l'unité, que l'on notera μ_n .

2.2 Polynôme cyclotomique sur \mathbb{F}_q et réduction modulo p

On sait que $X^n - 1 = \prod_{\zeta \in \mathbb{U}_n} (X - \zeta) = \prod_{d|n} \prod_{\zeta \in \mu_d} (X - \zeta)$

Ainsi, en notant $\Phi_{d, \mathbb{F}_q} = \prod_{\zeta \in \mu_d} (X - \zeta)$ le d -ème polynôme cyclotomique sur F_q , on a bien

$X^n - 1 = \prod_{d|n} \Phi_{d, \mathbb{F}_q}$. Bref, tout marche comme sur \mathbb{C} .

On notera, pour un polynôme $P \in \mathbb{Z}[X]$, \bar{P} sa réduction "modulo p ". (En réalité, c'est son image par l'unique morphisme d'anneau $\mathbb{Z}[X] \rightarrow \mathbb{F}_q[X]$)

On remarque que $\Phi_{1, \mathbb{F}_q} = X - 1$. Donc $\overline{X - 1} = \Phi_{1, \mathbb{F}_q}$.

Ainsi, de la formule $X^n - 1 = \prod_{d|n} \Phi_{d, \mathbb{F}_q}$, on déduit que $\Phi_{n, \mathbb{F}_q} = \frac{X^n - 1}{\prod_{d|n, d < n} \Phi_{d, \mathbb{F}_q}}$, on en déduit

par récurrence que $\Phi_{d, \mathbb{F}_q} = \bar{\Phi}_d$, où Φ_d désigne le d -ème polynôme cyclotomique sur F_q (on a utilisé le fait que $X^n - 1 = \prod_{d|n} \Phi_d$ dans $\mathbb{Z}[X]$).

Il est bien connu que dans $\mathbb{Z}[X]$ les polynômes cyclotomiques ont la bonne idée d'être irréductibles. Qu'en est-il sur $\mathbb{F}_q[X]$?

3 Réductibilité et irréductibilité des polynômes cyclotomiques sur $\mathbb{F}_q[X]$

On se donne ζ une racine n -ème primitive de l'unité dans \mathbb{F}_q . On s'intéresse au degré de l'extension $\mathbb{F}_q[\mu]$ sur \mathbb{F}_q qui est exactement le degré du polynôme minimal de ζ . Ceci nous donnera une bonne idée de si oui ou non notre polynôme cyclotomique est réductible : il le sera si et seulement si le degré de l'extension (que l'on notera s) est égal à $\varphi(n)$ (le degré du polynôme cyclotomique donc).

Nous allons montrer que s est en fait l'ordre de q dans $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$.

Pour cela, on s'intéresse à l'automorphisme de corps $F : \mathbb{F}_q[\zeta] \longrightarrow \mathbb{F}_q[\zeta], x \mapsto x^q$ (c'est une itérée du Frobenius).

F est d'ordre s dans $Aut(\mathbb{F}_q[\zeta])$. En effet, si $x \in \mathbb{F}_q$, $F^s(x) = x^{q^s} = x$, car q^s est le cardinal de \mathbb{F}_q . De plus, les inversibles de $\mathbb{F}_q[\mu]$ formant un groupe cyclique de cardinal $q^s - 1$, un élément est d'ordre $q^s - 1$. Pour cet élément, que l'on note x , on a effectivement, si $i < q^s - 1$, $F^i(x) \neq 1$, donc on ne peut avoir $i < q^s$ tel que $F^i(x) = x$, ce qui achève de montrer que le Frobenius est d'ordre s .

Maintenant, comme ζ est d'ordre n dans \mathbb{F}_q (c'est une racine primitive n -ème), $x^n = 1$, et d'après ce qui précède, $\zeta^{q^s-1} = 1$. Donc $q^s - 1 = 0[n]$, donc $q^s = 1[n]$.

Maintenant, il faut se convaincre que s est minimal. sinon, si il existe $j < s$ tel que $q^j = 1[n]$, alors $\zeta^{q^j} = F^j(\zeta) = \zeta$, et $\zeta \in Fix(F^j)$ qui est un sous-corps strict de $\mathbb{F}_q[\zeta]$, ce qui est absurde.

Donc s est le plus petit entier à vérifier $q^s = 1[n]$, c'est exactement dire que s est l'ordre de q dans $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$.

On a bien montré que s est l'ordre de q dans $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$. Ceci montre donc que le degré du polynôme minimal de ζ ne dépend que de q et de n , et est l'ordre de q dans $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$, que l'on notera r dans la suite.

4 Conclusion sur les polynômes cyclotomiques

On a donc montré que les polynômes cyclotomiques étaient produit de $\frac{\varphi(n)}{r}$ polynômes irréductibles. Dès lors, ils sont irréductibles si et seulement si $r = \varphi(n)$. Ceci veut donc dire que $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$ est cyclique (car il y a un élément d'ordre $\varphi(n)$), et engendré par la classe de q .

Or, on sait que $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$ est cyclique si et seulement si $n \in \{1, 2, 4, p^\alpha, 2p^\alpha\}$ où p est un premier plus grand que 3.

On a fait le boulot!

5 Envie de réduire ?

On suppose que $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$ est cyclique. Soit $a \in \mathbb{N}$ tel que la classe de a engendre $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$. On voudrait réduire notre polynôme cyclotomique sur un \mathbb{F}_p , p premier (ça se manipule mieux que \mathbb{F}_q !). Il faut donc qu'on trouve un p premier dont la classe modulo n engendre $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$. Et bien ça existe.... Et il y en a une infinité. C'est exactement ce que dit le théorème de la progression arithmétique de Dirichlet. Je trouve que c'est très sympa à dire à l'oral!

6 Contre exemple pour la réduction modulo p

On considère $\Phi_8 = X^4 + 1$. Ce polynôme est irréductible sur \mathbb{Z} car c'est un polynôme cyclotomique (ça se fait aussi à la main), et il ne l'est jamais sur F_p . Prouvons le avec notre théorème! Notre théorème s'applique seulement pour les p premiers avec 4. Il faut donc traiter $p = 2$ à part, mais sur F_q , où q est une puissance de 2, on a $X^4 + 1 = (X + 1)^4$. Rien de plus réductible.

Maintenant si p est premier, on regarde $(\frac{\mathbb{Z}}{8\mathbb{Z}})^* = \{1, 3, 5, 7\}$ dont tout les éléments sont d'ordre 1 ou 2. Donc $(\frac{\mathbb{Z}}{8\mathbb{Z}})^*$ n'est pas cyclique, et Φ_8 ne saurait être réductible sur un F_q , donc encore moins sur un F_p .

Ceci fournit un contre-exemple pour la réduction modulo p . Il est vrai que si $P \in \mathbb{Z}[X]$ unitaire est irréductible sur un \mathbb{F}_p il l'est sur \mathbb{Z} , mais la réciproque n'est pas vraie, comme on vient de le voir.

Une autre méthode possible est la suivante, je la trouve instructive, mais elle n'utilise pas le théorème : Si -1 est un carré dans \mathbb{F}_q , que $i^2 = -1$, alors $X^4 + 1 = (X^2 + i)(X^2 - i)$. Sinon, si -2 est un carré dans \mathbb{F}_q , $X^4 + 1 = X^4 + 2X^2 + 1 - 2X^2 = (X^2 + 1)^2 - (\sqrt{2}X)^2 = (X^2 + \sqrt{-2}X + 1)(X^2 - \sqrt{-2}X + 1)$ Sinon, si 2 est un carré, on fait la même chose, mais avec $X^2 - 1$.

Et si -1 et -2 ne sont pas des carrés dans \mathbb{F}_q , alors si on note $\pi : (\mathbb{F}_q)^* \mapsto \frac{(\mathbb{F}_q)^*}{(\mathbb{F}_q)^{*2}} \sim \mathbb{U}_2$, on a $\pi(-1) = \pi(-2) = -1$, donc $\pi(2) = \pi(-1) * \pi(-2) = 1$, et 2 est un carré dans \mathbb{F}_q .

7 Et les recasages ?

120 Anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$ (j'ai appris le développement exclusivement pour cette leçon), 121 nombres premiers, 123 corps finis, 125 extensions de corps, 141 polynômes irréductibles, 144 racines d'un polynôme

8 Oucéfé?

Dans le Escoffier Théorie de Galois, dans les exercices sur les corps finis. C'est corrigé, et c'est un superbe livre.