Anaël Marit ENS Rennes

CYCLOTOMIE

- 102, 104, 121, 123, 127, 141, 120, 125 –

—

Ce développement est modulaire : il contient trop de choses pour être présenté tel quel. On peut prendre les parties les plus intéressantes pour la leçon en cours et admettre le reste, mais il s'apprend bien comme un seul bloc uni.

J'ai décomposé ce document en quatre parties, les trois dernières étant indépendantes :

1. *En premier lieu, on montre plusieurs résultats préliminaires, essentiels pour manipuler les polynômes cyclotomiques, mais qui peuvent être simplement énoncés dans le plan pour gagner du temps et faire des choses plus poussées en développement.*
2. *On prouve ensuite l'irréductibilité des polynômes cyclotomiques dans $\mathbb{Q}[X]$. Indispensable pour la 102 mais peut ne pas être mis en avant dans d'autres leçons, par exemple la 121, la 123 ou la 125.*
3. *On applique l'étude des polynômes cyclotomiques à la démonstration d'une version faible du théorème de progression arithmétique de Dirichlet. Un must have pour la 121 !*
4. *Dans la dernière partie, on étudie la réductibilité des polynômes cyclotomiques à coefficients dans les corps finis. Cette partie est certainement la plus délicate, mais elle est plus originale que le travail dans $\mathbb{Q}[X]$. Elle me semble parfaite pour la 123, la 141 et dans une moindre mesure, la 120.*

Soit K un corps et n un entier. Dans toute la suite, on fixe L un corps de décomposition du polynôme $X^n - 1$. On pose $\mu_n(K)$ le groupe des racines n-ièmes de l'unité dans L et $\mu_n^*(K)$ celui des racines n-ièmes primitives de l'unité, c'est-à-dire les éléments d'ordre n dans le groupe $\mu_n(K)$. On définit alors le n-ième polynôme cyclotomique à coefficients dans L :

$$\Phi_{n,K} := \prod_{\omega \in \mu_n^*(K)} (X - \omega) \in L[X] \tag{1}$$

Généralités sur les polynômes cyclotomiques ([2], section VI.1)

Cette section contient un certain nombre de résultats préliminaires indispensables à connaître pour la suite mais qui peuvent être admis ou pas selon le temps et la leçon présentée.

Lemme 1 (Une relation de récurrence). *On suppose que la caractéristique de K ne divise pas n. Alors :*

$$X^n - 1 = \prod_{d|n} \Phi_{d,K} \tag{2}$$

Démonstration. Le polynôme $X^n - 1$ est séparable car il ne partage aucune de ses racines dans L avec son polynôme dérivé $nX^{n-1} \neq 0$ [(i)]. Il est donc à racines simples dans L. Par le théorème

(i). Ce polynôme est non nul car n n'est pas divisé par la caractéristique de K.

de Lagrange :

$$\mu_n(K) = \bigsqcup_{d|n} \mu_n^*(K) \tag{3}$$

et donc :

$$\begin{aligned} X^n - 1 &= \prod_{\omega \in \mu_n(K)} (X - \omega) && (4)\\ &= \prod_{d|n} \prod_{\omega \in \mu_d^*(K)} (X - \omega) && (5)\\ &= \prod_{d|n} \Phi_{d,K} && (6) \end{aligned}$$

□

Lemme 2.

$$\Phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$$

Démonstration. On procède par récurrence forte sur n. Si $n = 1$, alors $\Phi_{n,\mathbb{Q}} = X - 1 \in \mathbb{Z}[X]$. Supposons donc $n \geqslant 2$ et que tous les polynômes cyclotomiques d'ordre inférieur strict à n sont à coefficients entiers. Alors, d'après le lemme 1, $X^n - 1 = \Phi_{n,\mathbb{Q}} P$ où $P \in \mathbb{Z}[X]$. On peut voir cette écriture comme celle d'une divison euclidienne dans $L[X]$. Mais alors, comme P est unitaire dans $\mathbb{Z}[X]$, on peut également faire la division euclidienne de $X^n - 1$ par P :

$$X^n - 1 = QP + R, \quad \deg(R) < \deg(P) \tag{7}$$

Comme il s'agit également d'une division euclidienne dans $L[X]$, on peut conclure par unicité : $R = 0,\ Q = \Phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$. □

Remarque : Par la même preuve, on prouve que $\Phi_{n,K} \in \mathbb{F}_p[X]$ si K est de caractéristique p première.

Lemme 3. *Si K est de caractéritique $p > 0$, et si n est premier avec p, alors :*

$$\Phi_{n,K} = \overline{\Phi_{n,\mathbb{Q}}} \tag{8}$$

c'est-à-dire que $\Phi_{n,K}$ est obtenu en projetant les coefficients (entiers) de $\Phi_{n,\mathbb{Q}}$ dans $\mathbb{F}_p$.

Démonstration. On procède encore une fois par récurrence en utilisant le lemme 1. Pour $n = 1$,

c'est clair. Supposons $n \geqslant 2$ et que pour tout $d|n,\ d < n$ le résultat est acquis [ii]. Alors :

$$\overline{X^n - 1} = \Phi_{n,K} \prod_{\substack{d|n \\ d\neq n}} \Phi_{d,K} \qquad \text{(lemme 1 dans } K\text{)} \tag{9}$$

$$= \Phi_{n,K} \prod_{\substack{d|n \\ d\neq n}} \overline{\Phi_{d,\mathbb{Q}}} \qquad \text{(hypothèse de récurrence)} \tag{10}$$

$$= \overline{\Phi_{n,\mathbb{Q}} \prod_{\substack{d|n \\ d\neq n}} \Phi_{d,\mathbb{Q}}} \qquad \text{(lemme 1 dans } \mathbb{Q}\text{)} \tag{11}$$

$$= \overline{\Phi_{n,\mathbb{Q}}} \prod_{\substack{d|n \\ d\neq n}} \overline{\Phi_{d,\mathbb{Q}}} \tag{12}$$

Il ne reste qu'à simplifier par $\prod_{\substack{d|n \\ d\neq n}} \overline{\Phi_{d,\mathbb{Q}}}$. □

Irréductibilité sur $\mathbb{Q}$ ([2], théorème VI.11)

Nous allons montrer dans cette partie le très classique :

Théorème 4 (Irréductibilité dans $\mathbb{Q}[X]$). *$\Phi_{n,\mathbb{Q}}$ est irréductible dans $\mathbb{Q}[X]$ et dans $\mathbb{Z}[X]$.*

Soit f un diviseur irréductible unitaire de $\Phi_{n,\mathbb{Q}}$ dans $\mathbb{Q}[X]$. On va montrer que $f = \Phi_{n,\mathbb{Q}}$ en montrant que ces deux polynômes ont les mêmes racines complexes.

On a $f|X^n - 1$. Notons $h \in \mathbb{Q}[X]$ tel que $fh = X^n - 1$.

Lemme 5.

$$f, h \in \mathbb{Z}[X]$$

Démonstration. Comme $X^n - 1$ et f sont unitaires, h l'est également. Soit $r \in \mathbb{N}^*$ tel que $rf \in \mathbb{Z}[X]$. Notons alors r' le pgcd des coefficients de rf. Comme f est unitaire, $r'|r$ et donc $\frac{r}{r'}f \in \mathbb{Z}[X]$ est de contenu 1 avec $\frac{r'}{r} \in \mathbb{Z}$. Notons cet entier $\tilde{r}$. On fait de même avec h : il existe $\tilde{q}$ un entier tel que $\tilde{q}h$ soit à coefficients entiers et de contenu 1. On a alors :

$$\tilde{r}\tilde{q}(X^n - 1) = (\tilde{r}f)(\tilde{q}h) \tag{13}$$

En appliquant le contenu (qui est multiplicatif) à cette égalité, on obtient :

$$1 = \tilde{r}\tilde{q} \tag{14}$$

D'où $\tilde{r} = \tilde{q} = 1$ et $f \in \mathbb{Z}[X], h \in \mathbb{Z}[X]$. □

(ii). Si n est premier avec p, c'est également le cas de tous ses diviseurs.

Ce résultat va nous permettre de projeter nos égalités dans $\mathbb{F}_p[X]$ par la suite.

Soit ω une racine complexe de f. Pour montrer $f = \Phi_{n,\mathbb{Q}}$, il suffit de montrer que si m est un entier premier avec n, alors ω^m est encore racine de f, car dans ce cas ces deux polynômes auront les mêmes racines. On peut encore réduire le problème en montrant que pour tout p un nombre premier ne divisant pas n, alors ω^p est racine de f. En le montrant pour toute racine ω, on aura bien que ω^m est encore racine de f si m est premier avec n. On a :

$$0 = (\omega^p)^n - 1 = f(\omega^p)h(\omega^p) \tag{15}$$

Par l'absurde, on suppose $f(\omega^p) \neq 0$. Alors $h(\omega^p) = 0$. Puisque f est irréductible et unitaire sur $\mathbb{Q}$, c'est le polynôme minimal de ω et donc on a :

$$f|h(X^p) \text{ i.e. } \exists g \in \mathbb{Q}[X] \ : \ h(X^p) = fg \tag{16}$$

Remarquons que cette égalité pouvant être vue comme une division euclidienne dans $\mathbb{Q}[X]$, on obtient immédiatement que $g \in \mathbb{Z}[X]$ en effectuant la même division euclidienne dans $\mathbb{Z}[X]$. On peut donc projeter l'égalité dans $\mathbb{F}_p[X]$:

$$\bar{f}\bar{g} = \overline{h(X^p)} = \overline{h(X)}^p \text{ (iii)} \tag{17}$$

Soit alors $\theta \in \mathbb{F}_p[X]$ un diviseur irréductible de $\bar{f}$. Alors :

$$\theta|\bar{h}^p \implies \theta|\bar{h} \tag{18}$$

Or on a :

$$\overline{X^n - 1} = \bar{f}\bar{h} \tag{19}$$

Donc :

$$\theta^2|\overline{X^n - 1} \tag{20}$$

ce qui est absurde car n étant premier avec p, $X^n - 1$ est séparable dans $\mathbb{F}_p[X]$ et ses facteurs irréductibles sont donc simples. En remontant le file des arguments, on a bien montré que $\Phi_{n,\mathbb{Q}} = f$ et donc que les polynômes cyclotomiques sont tous irréductibles sur $\mathbb{Q}$!

Pour l'irréductibilité dans $\mathbb{Z}[X]$, il suffit d'utiliser le fait que ces polynômes sont unitaires, donc de contenu 1.

Corollaire 6. *$L/\mathbb{Q}$ est une extension de degré $\varphi(n)$, où φ désigne l'indicatrice d'Euler.*

Théorème de Dirichlet faible ([2], proposition VII.13)

Les polynôems cyclotomiques vont nous permettre de démontrer une version faible du théorème de progression arithmétique de Dirichlet.

Théorème 7 (Dirichlet faible). *La suite $(\lambda n + 1)_{\lambda \in \mathbb{N}}$ contient une infinité de nombres premiers. En d'autres termes, il existe une infinité de nombres premiers congrus à 1 modulo n.*

(iii). On utilise le fait que le morphisme de Frobenius s'étend en un morphisme d'anneaux sur $\mathbb{F}_p[X]$ laissant stable les éléments de $\mathbb{F}_p$.

L'énoncé est impliqué par le suivant : pour tout entier $N > n$, il existe une nombre premier $p \geqslant N$ congru à 1 modulo n. La cyclotomie va fournir un candidat astucieux en exploitant le lemme suivant :

Lemme 8. *Soit $a \in \mathbb{N}$. Si p est un nombre premier divisant $\Phi_{n,\mathbb{Q}}(a)$ mais pas $\Phi_{d,\mathbb{Q}}(a)$, où d parcours l'ensemble des diviseurs stricts de n, alors $p \equiv 1[n]$.*

Démonstration. Comme $p|\Phi_{n,\mathbb{Q}}(a)$, on a que $p|a^n - 1$. En réduisant modulo p, on obtient $a^n \equiv 1[p]$. Notons $o(a)$ l'ordre de a dans le groupe multiplicatif $\mathbb{F}_p^\times$. On vient de montrer que $o(a)|n$. Si $o(a) < n$, alors $\bar{a}^{o(a)} - 1 = 0$ dans $\mathbb{F}_p$ et donc :

$$p|a^{o(a)} - 1 = \prod_{d|o(a)} \Phi_{d,\mathbb{Q}}(a) \tag{21}$$

Il suit que p divise l'un des $\Phi_{d,\mathbb{Q}}(a), d|o(a)|n$, ce qui est exclu par hypothèse. Donc $o(a) = n$. Par théorème de Lagrange sur le groupe multiplicatif $\mathbb{F}_p^\times$ (d'ordre $p-1$), on a que $n|p-1$, c'est-à-dire $p \equiv 1[n]$. □

On propose alors p un diviseur premier de $\Phi_{n,\mathbb{Q}}(N!)$. On écrit $\Phi_{n,\mathbb{Q}}(N!) = pd$. Remarquons que $\Phi_{n,\mathbb{Q}}(0)$ est un entier, produit de racines de l'unité : c'est donc ± 1. Ceci mène à une relation de Bézout :

$$pd = \Phi_{n,\mathbb{Q}}(N!) = N!P(N!) + \Phi_{n,\mathbb{Q}}(0) \tag{22}$$

où P est un polynôme à coefficients entiers. Ainsi, p est premier avec $N!$ et en particulier, $p > N > n$ (et notamment p est premier à n).

Si d est un diviseur strict de n tel que $p|\Phi_{d,\mathbb{Q}}(N!)$, alors en réduisant modulo p l'égalité :

$$(N!)^n - 1 = \prod_{d|n} \Phi_{d,\mathbb{Q}}(N!) \tag{23}$$

il vient que $\overline{N!}$ est une racine double de $\overline{X^n - 1}$, ce qui est absurde car n et premier avec p et donc $\overline{X^n - 1}$ est séparable. En appliquant le lemme, on a que $p \equiv 1[n]$, et on montre le théorème !

Facteurs irréductibles dans $\mathbb{F}_q[X]$ ([1], exercice 14.7)

Dans cette section, on va étudier la réductibilité des polynômes cyclotomiques à coefficients dans un corps fini.

Soit q une puissance d'un nombre premier p. Soit n un entier premier avec p. On pose $s := [L : K]$.

Théorème 9. *Tous les facteurs irréductibles de $\Phi_{n,\mathbb{F}_q}$ sont d'ordre s. De plus, s est l'ordre de q dans le groupe mutliplicatif $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$.*

Démonstration. Comme toutes les racines de $\Phi_{n,K}$ engendrent l'extension $L/\mathbb{F}_q$, leurs polynômes minimaux sont tous de degré s.

Pour montrer que q est d'ordre s dans $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$, on s'intéresse à

$$\begin{aligned} \mathrm{Frob}_q : L &\to L \\ x &\mapsto x^q \end{aligned}$$

On va montrer que Frob_q est d'ordre s dans $\mathrm{Aut}_{\mathbb{F}_q}(L)$, le groupe des automorphismes de l'extension $L/\mathbb{F}_q$. Considérons α un générateur du groupe multiplicatif $L^\times$, d'ordre q^s-1. Considérons alors $k \in \mathbb{N}$. On a :

$$\begin{aligned} \mathrm{Frob}_q^{\circ k}(\alpha) = \alpha &\iff \alpha^{q^k} = \alpha && (24)\\ &\iff o(\alpha) | q^k - 1 && (25)\\ &\iff q^s - 1 | q^k - 1 && (26)\\ & && (27) \end{aligned}$$

D'où nécessairement, s est inférieur ou égal à l'ordre de Frob_q. Comme d'un autre côté, $\mathrm{Frob}_q^{\circ s}$ est l'identité sur $\mathbb{F}_q$ par théorème de Lagrange, on obtient bien que Frob_q est d'ordre s. Pour terminer, prenons $\omega \in \mu_n^*(\mathbb{F}_q)$. Alors, pour $k \in \mathbb{N}$:

$$\begin{aligned} \mathrm{Frob}_q^{\circ k}(\omega) = \omega &\iff \mathrm{Frob}_q^{\circ k} = Id_L \qquad \text{car } L = \mathbb{F}_q(\omega) && (28)\\ &\iff s | k && (29) \end{aligned}$$

Mais d'autre part :

$$\begin{aligned} \mathrm{Frob}_q(\omega)^{\circ k} = \omega &\iff \omega^{q^s-1} = 1 && (30)\\ &\iff q^k - 1 \equiv 0[n] \text{ car } \omega \in \mu_n^*(\mathbb{F}_q) && (31)\\ &\iff o(q) | k && (32) \end{aligned}$$

Ces deux suites d'équivalences prouvent bien que l'ordre de q dans $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ est s. □

On a quelques conséquences intéressantes de cette étude :

Corollaire 10. *Si n est tel que $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ n'est pas cyclique, alors $\Phi_{n,\mathbb{Q}}$ est réductible sur tous les corps finis de cardinal premier avec n.*

Démonstration. Si q est une puissance d'un nombre premier ne divisant pas n, alors les facteurs irréductibles de $\overline{\Phi_{n,\mathbb{Q}}} = \Phi_{n,\mathbb{F}_q}$ sont tous de degré l'ordre de q dans $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$. Donc si $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ n'est pas cyclique, q ne peut pas être d'ordre $\varphi(n)$ et les facteurs irréductibles de $\Phi_{n,\mathbb{F}_q}$ sont stricts. □

Corollaire 11. *$\Phi_{8,\mathbb{Q}}$ est un polynôme irréductible dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$ mais réductible sur tous les corps finis.*

Démonstration. On a $\Phi_{8,\mathbb{Q}} = X^4 + 1$. Soit $\mathbb{F}_q$ un corps fini de caractéristique p première.
Si $p = 2$, alors $\Phi_{8,\mathbb{F}_q} = (X+1)^4$ est réductible.

Sinon, p est premier avec 8. Dans ce cas, il suffit de remarquer que :

$$\left(\mathbb{Z}/8\mathbb{Z}\right)^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \tag{33}$$

En particulier, ce groupe n'est pas cyclique, et donc $\Phi_{8,\mathbb{F}_Q}$ est réductible.

□

Références

[1] Jean-Pierre Escofier. *Théorie de Galois*. Dunod, 1997.

[2] Ivan Gozard. *Théorie de Galois*. Ellipses, 1997.