I.L Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$ (102) (120) (121) (125) (127) (141)

Lemme 28:

1. Pour tout $n \in \mathbb{N}^*$, on a $X^n - 1 = \prod_{d|n} \phi_d$;
2. Le polynôme ϕ_n est unitaire et à coefficients dans $\mathbb{Z}$ pour tout n ;
3. Si $P = QR$ avec $P \in \mathbb{Z}[X]$ et $Q, R \in \mathbb{Q}[X]$ unitaires, alors $Q, R \in \mathbb{Z}[X]$.

Démonstration.

1. $X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta) = \prod_{d|n} \prod_{\zeta \in \mu_n^\times} (X - \zeta) = \prod_{d|n} \phi_d$
2. On procède par récurrence :
   si $n = 1$ alors $\phi_1 = X - 1$;
   si on suppose le résultat vrai jusqu'au rang $n - 1$ alors, par le premier point :
   $$X^n - 1 = \phi_n \prod_{d|n\ ,\ d<n} \phi_d$$
   Il s'agit de la division euclidienne de $X^n - 1$ par $\prod_{d|n\ ,\ d<n} \phi_d$ qui est bien dans $\mathbb{Z}[X]$ unitaire par HR. Donc le quotient est dans $Z[X]$. Et c'est aussi la division euclidienne dans $Q[X]$, mais celle-ci est unique. D'où le deuxième point (le caractère unitaire se voit sur les coefficients dominants).
3. On note q le générateur positif de l'idéal $\{n \in \mathbb{Z} \quad / \quad nQ \in \mathbb{Z}[X]\}$. Alors $qQ \in \mathbb{Z}[X]$ et est primitif par définition de q et car Q est unitaire. En effet si $p|qQ$, alors en particulier en regardant le coefficient dominant $p|q$. Donc $\frac{q}{p}Q \in \mathbb{Z}[X]$ et par minimalité de q, on a donc $p = 1$.
   On obtient de même $r \in \mathbb{Z}$ tel que $rR \in \mathbb{Z}[X]$ primitif.
   Alors $qrP = qQrR$ et en passant au contenu il vient que qr c$(P) = 1$ donc q et r sont dans $\mathbb{Z}$ inversibles. Ils valent donc tous deux ± 1.

■

Théorème 29:

Pour tout $n \in \mathbb{N}^*$, ϕ_n est irréductible sur $\mathbb{Q}$.

Démonstration. Soit $\zeta \in \mu_n^\times$. On va montrer que $\phi_n = \mu_\zeta$

1. Soit $\zeta' \in \mu_n^\times$. Alors il existe $m \in [\![1, \dots, n-1]\!]$ premier avec n tel que $\zeta' = \zeta^m$, il s'écrit
   $$m = p_1^{\alpha_1} \dots p_k^{\alpha_k}.$$
   Quitte à raisonner par récurrence sur le nombre de diviseurs premiers de m, OPS $m = p$ est premier.
2. Montrons que $\mu_\zeta = \mu_{\zeta^p}$. On note $f = \mu_\zeta$ et $g = \mu_{\zeta^p}$. Alors on a immédiatement que $f|g(X^p)$. Donc il existe $h \in \mathbb{Q}[X]$ tel que $fh = g(X^p)$.
   On a de plus que f et g sont à coefficients entiers. En effet, l'anneau $\mathbb{Z}[X]$ est factoriel, donc $\phi_n = f_1\beta_1 \dots f_r\beta_r$ en produit d'irréductibles.
   Alors l'un des f_{i_0} annule ζ et est unitaire et irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$. Par minimalité du polynôme minimal, on a donc $f = f_{i_0}$. Il en est de même pour g.

   Par le lemme on obtient donc que $h \in \mathbb{Z}[X]$. On a donc $fh = g(x^p)$ dans $\mathbb{Z}[X]$. On peut donc réduire cette équation modulo p.
   Supposons que $f \neq g$. Alors f et g sont deux irréductibles distincts divisant ϕ_n, et donc $fg \mid \phi_n$.

Soit φ un diviseur irréductible de $\overline{f}$. Alors $\varphi \mid \overline{fh} = \overline{g(X^p)} = \overline{g(X)}^p$. Donc par le lemme d'Euclide, $\varphi \mid \overline{g}$. On a alors :

$$\varphi^2 \mid \overline{f}\,\overline{g} \mid \overline{\phi_n} \mid \overline{X^n - 1}$$

Or le polynôme dérivé de $\overline{X^n - 1}$ est $\overline{nX^{n-1}}$ qui est non nul car p et n sont premiers entre eux. Mais alors 0 est la seule racine de $\overline{nX^{n-1}}$ sans être racine de $\overline{X^n - 1}$. Il n'a donc pas de racine multiple, c'est absurde et donc $f = g$.

3. On a donc $\mu_\zeta = f = g = \mu_{\zeta^m}$ pour tout $1 \leqslant m \leqslant n-1$ premier avec n. Donc μ_ζ admet $\varphi(n) = \deg(\phi_n)$ racines. De plus $\phi_n(\zeta) = 0$ donc ϕ_n est annulateur pour ζ et $\mu_\zeta \mid \phi_n$. Les deux polynômes sont donc associés. Comme de plus ils sont tous deux unitaires, ils sont égaux. Donc ϕ_n est un polynôme minimal et donc il est irréductible.

■

Une application des polynômes cyclotomiques concerne le théorème de progression arithmétique de Dirichlet que je présente maintenant.

Application 30: Progression arithmétique faible de Dirichlet

Pour tout $m \in \mathbb{N}_{\geqslant 2}$, il existe une infinité de nombres premiers $p \equiv 1 \pmod m$.

Dans toute la suite, $\mathcal{P}$ désigne l'ensemble des nombres premiers (positifs) et, pour $m \geqslant 1$, Φ_m désigne le m-ième polynôme cyclotomique.

Démonstration. **Étape 1.** *Soit $p \in \mathcal{P}$. Supposons que $p \mid \Phi_m(a)$ pour un certain entier $a \in \mathbb{Z}$, et que $p \nmid \Phi_d(a)$ pour tout $d \mid m$ avec $d \neq m$. Alors $p \equiv 1 \pmod m$.*

Comme $\Phi_m \mid X^m - 1$, on a $p \mid a^m - 1$, i.e. $\bar{a}^{\,m} = 1$ dans $\mathbb{F}_p$; en particulier $\bar{a} \in \mathbb{F}_p^\times$.

Donc l'ordre de $\bar{a}$ dans $\mathbb{F}_p^\times$ divise m.

Cet ordre vaut en fait exactement m : sinon, il existerait $d \mid m$, $d \neq m$, tel que $\bar{a}^{\,d} = 1$ dans $\mathbb{F}_p$, i.e.

$$p \mid a^d - 1 = \left(X^d - 1\right)\big|_{X=a} = \prod_{k \mid d} \Phi_k(a).$$

Donc $p \mid \Phi_k(a)$ pour un certain $k \mid d$. Or $k \mid d \mid m$ et $k \leqslant d < m$, donc $k \neq m$: ceci contredit l'hypothèse ($p \nmid \Phi_k(a)$ pour $k \mid m$, $k \neq m$). Contradiction.

L'ordre de $\bar{a}$ vaut donc exactement m. Par le théorème de Lagrange, cet ordre divise $|\mathbb{F}_p^\times| = p - 1$.

Donc $m \mid p - 1$, i.e. $p \equiv 1 \pmod m$.

Étape 2. *Pour tout entier $N \geqslant 2$, il existe $p \in \mathcal{P}$ tel que $p \equiv 1 \pmod N$.*

On note $Q := \prod_{\substack{d \mid N \\ d \neq N}} \Phi_d$. Alors $X^N - 1 = \Phi_N \cdot Q$.

Φ_N et Q sont premiers entre eux dans $\mathbb{Q}[X]$: ils sont scindés sur $\mathbb{C}$ et sans racine commune, par unicité de l'ordre des racines de l'unité (les racines de Φ_N sont les racines primitives N-ièmes de l'unité, celles de Q sont des racines d-ièmes primitives pour $d \mid N$, $d \neq N$). Et le pgcd est invariant par extension de corps, donc Φ_N et Q sont aussi premiers entre eux dans $\mathbb{Q}[X]$.

Par Bézout, il existe $U, V \in \mathbb{Q}[X]$ tels que $U\Phi_N + VQ = 1$.

Soit $a \in \mathbb{Z}$ tel que aU et aV soient dans $\mathbb{Z}[X]$ (un tel a est par exemple un multiple du ppcm des dénominateurs des coefficients de U et V).

Comme Φ_N est non constant, le nombre d'entiers $\beta \in \mathbb{Z}$ tels que $\Phi_N(\beta) \in \{-1, 0, 1\}$ est fini. Or le nombre de a possibles (au sens ci-dessus) est infini, car il suffit de prendre des multiples du ppcm des dénominateurs des coefficients de U et V.

$\Longrightarrow$ On peut donc choisir un tel a avec $\Phi_N(a) \notin \{-1, 0, 1\}$.

Il existe alors $p \in \mathcal{P}$ tel que $p \mid \Phi_N(a)$, d'où $p \mid a^N - 1$, donc $\bar{a}^{\,N} = 1$ dans $\mathbb{F}_p$, donc $\bar{a} \in \mathbb{F}_p^\times$ (en particulier $a \wedge p = 1$).

En évaluant $U\Phi_N + VQ = 1$ en $X = a$ puis en multipliant par a, et en posant $\tilde{U}(a) := aU(a) \in \mathbb{Z}$, $\tilde{V}(a) := aV(a) \in \mathbb{Z}$:

$$\tilde{U}(a)\,\Phi_N(a) + \tilde{V}(a)\,Q(a) = a.$$

Modulo p, comme $p \mid \Phi_N(a)$, il reste $\overline{\tilde{V}(a)} \cdot \overline{Q(a)} = \bar{a}$ dans $\mathbb{F}_p$. Comme $\bar{a}$ est inversible, on en déduit $\overline{Q(a)} \neq 0$, i.e. $p \nmid Q(a)$.

Par le lemme d'Euclide, $p \nmid \Phi_d(a)$ pour tout $d \mid N$, $d \neq N$.

Donc, par l'étape 1 (appliquée avec $m = N$), $p \equiv 1 \pmod{N}$.

Étape 3. *Conclusion.*

D'après l'étape 2, pour tout entier $N \geqslant 2$, il existe $p \in \mathcal{P}$ tel que $p \equiv 1 \pmod{N}$.

Soit $m \geqslant 2$ un entier. Supposons par l'absurde qu'il n'existe qu'un nombre fini de nombres premiers congrus à $1 \pmod{m}$; notons-les $p_1, \ldots, p_r$.

On pose $N := m\,p_1 \cdots p_r$. D'après ce qui précède, il existe $p \in \mathcal{P}$ (que l'on peut prendre > 0) tel que $p \equiv 1 \pmod{N}$.

Comme $p \in \mathcal{P}$, $p \neq 1$, donc $p \geqslant 1 + N = 1 + m\,p_1 \cdots p_r$, d'où $p > p_i$ pour tout $i \in \{1, \ldots, r\}$.

Donc $p \notin \{p_1, \ldots, p_r\}$. Or $m \mid N$ et $p \equiv 1 \pmod{N}$ entraîne $p \equiv 1 \pmod{m}$, donc p devrait figurer parmi $p_1, \ldots, p_r$: contradiction.

Il existe donc une infinité de nombres premiers $p \equiv 1 \pmod{m}$. ■