ref : Demazure
p. 206

Developpement : Polynômes cyclotomiques :

leçons 141
121
144

Soit $n \in \mathbb{N}^*$, ζ une racine primitive $n^{\text{ième}}$ de l'unité. Le $n^{\text{ième}}$ polynôme cyclotomique est $\varphi_n(X) := \prod\limits_{\substack{k=1 \\ k \wedge n = 1}}^{n} (X - \zeta^k)$.

Théorème :

Les polynômes cyclotomiques sont à coefficients dans $\mathbb{Z}$.

Lemme :

On a $X^n - 1 = \prod\limits_{d \mid n} \varphi_d$

Preuve du lemme :

Dans $\mathbb{C}$, on a la décomposition $X^n - 1 = \prod\limits_{k=1}^{n} (X - \zeta^k)$.

On a la partition de $[\![1, n]\!]$ suivante : $[\![1,n]\!] = \bigsqcup\limits_{d \mid n} \{1 \leq k \leq n ;\ k \wedge n = d\}$

Ainsi $X^n - 1 = \prod\limits_{d \mid n} \prod\limits_{\substack{k=1 \\ k \wedge n = d}}^{n} (X - \zeta^k) = \prod\limits_{d \mid n} \prod\limits_{\substack{k=1 \\ k \wedge (\frac{n}{d}) = 1}}^{n/d} (X - \zeta^{kd})$

$= \prod\limits_{d \mid n} \prod\limits_{\substack{k=1 \\ k \wedge d = 1}}^{d} (X - \zeta^{nk/d}) = \prod\limits_{d \mid n} \varphi_d(X)$ ■

En effet, ζ racine primitive $n^{\text{ième}}$ de l'unité $\Rightarrow \zeta^{n/d}$ racine primitive $d^{\text{ième}}$

Lemme : Soit A anneau commutatif unitaire intègre et $\mathbb{K}$ un corps contenant A. Soit $F, G \in A[X]$ avec G unitaire (ou de coef dominant inversible) tq $\exists\, H \in \mathbb{K}[X]$ vérifiant $F = GH$. Alors $H \in A[X]$.

Preuve du lemme :

G unitaire donc on peut faire la division euclidienne de F par G dans $A[X]$. On a ainsi $F = GQ + R$, avec $Q, R \in A[X]$ et $\deg(R) < \deg(G)$. Cette division euclidienne est bien entendue également la division euclidienne dans $\mathbb{K}[X]$. Or $\mathbb{K}$ corps donc $\mathbb{K}[X]$ euclidien, et on a unicité de la division euclidienne dans $\mathbb{K}[X]$. Ainsi $R = 0$ et $Q = H$, donc $H \in A[X]$. ▪

Preuve théorème :

Nous allons faire une récurrence sur n.

* initialisation : $n = 1$

$\varphi_1(X) = X - 1 \in \mathbb{Z}[X]$

* hérédité : Supposons $\exists n \in \mathbb{N}$, $n \geq 2$ tq $\forall d < n$, $\varphi_d \in \mathbb{Z}[X]$.

Par le premier lemme, $X^n - 1 = \varphi_n(X) \cdot \prod_{\substack{d \mid n \\ d \neq n}} \varphi_d(X)$

et par hypothèse de récurrence, $\prod_{\substack{d \mid n \\ d \neq n}} \varphi_d(X) \in \mathbb{Z}[X]$, ainsi que $X^n - 1$. Par le second lemme, $\varphi_n(X) \in \mathbb{Z}[X]$. ▪

Théorème : $\forall n \in \mathbb{N}$, $\varphi_n(X)$ irréductible dans $\mathbb{Z}[X]$, et donc dans $\mathbb{Q}[X]$.

Preuve :

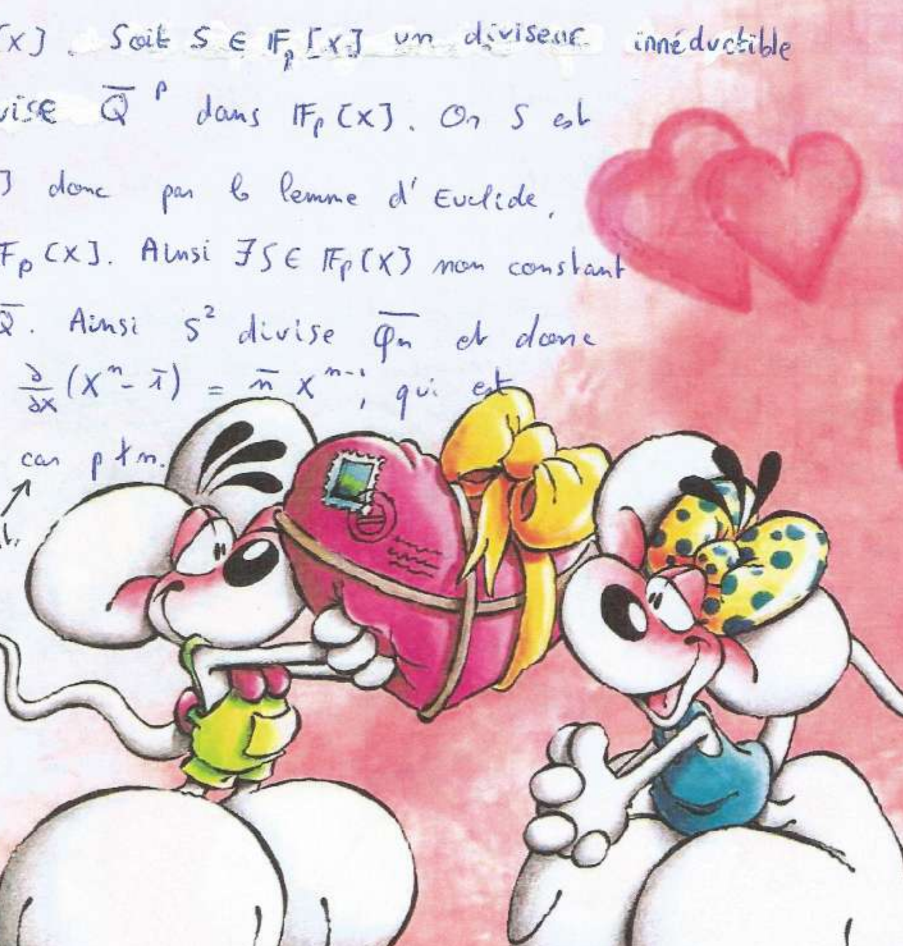
▶ Soit $P \in \mathbb{Z}[X]$ un facteur irréductible de φ_n non constant, et $Q \in \mathbb{Z}[X]$ tq $\varphi_n = PQ$. Soit ξ une racine de P dans $\mathbb{C}$. Nous allons mq pour tout nombre premier p ne divisant pas n, ξ^p racine de P.

Supposons que ce ne soit pas le cas. Alors ξ^p racine de Q, et donc ξ racine de $Q(X^p)$. P irréductible sur $\mathbb{Q}[X]$ et annule ξ donc c'est le polynôme minimal de ξ sur $\mathbb{Q}[X]$ et par conséquent $P \mid Q(X^p)$. Réduisons modulo p l'égalité $\varphi_n = PQ$:

$$\overline{\varphi_n} = \overline{P}.\overline{Q} \quad \text{dans } \mathbb{F}_p[X].$$

De plus, $\overline{Q(X^p)} = \overline{Q}^p$ (dans $\mathbb{F}_p[X]$). Comme P divise $Q(X^p)$, $\overline{P}$ divise $\overline{Q}^p$ dans $\mathbb{F}_p[X]$. Soit $S \in \mathbb{F}_p[X]$ un diviseur irréductible de $\overline{P}$. Alors S divise $\overline{Q}^p$ dans $\mathbb{F}_p[X]$. Or S est irréductible dans $\mathbb{F}_p[X]$ donc par le lemme d'Euclide, S divise $\overline{Q}$ dans $\mathbb{F}_p[X]$. Ainsi $\exists S \in \mathbb{F}_p[X]$ non constant tq S divise $\overline{P}$ et $\overline{Q}$. Ainsi S^2 divise $\overline{\varphi_n}$ et donc divise $X^n - \overline{1}$. Or, $\frac{\partial}{\partial X}(X^n - \overline{1}) = \overline{n} X^{n-1}$, qui est premier avec $X^n - \overline{1}$ car $p \nmid n$.

(on a regardé les coefficients dominants qui ne doivent pas être premiers entre eux. Or $p = 1$ dans $\mathbb{F}_p$ donc $1 \wedge m = 1$)



Par conséquent, $X^n - \bar{1}$ ne peut avoir de facteur carré non constant ce qui contredit l'hypothèse de départ. Ainsi, ξ^p racine de P.

- Maintenant, pour k premier avec n, en écrivant $k = p_1 \cdots p_k$ et en appliquant récursivement* le cas précédent, on montre que ξ^k est racine de P.

Ainsi, φ_n divise P et donc $\varphi_n = P$, i.e. φ_n irréductible dans $\mathbb{Z}[X]$. Le contenu de φ_n valant 1, φ_n irréductible dans $\mathbb{Q}[X]$.

Commentaires:

① Soit $R(X) \in \mathbb{F}_p[X]$, $R(X) = \sum_{i=1}^{n} a_i X^i$ avec $a_i^p = a_i$

$$R(X^p) = \sum_{i=1}^{n} a_i X^{ip} = \sum_{i=1}^{n} (a_i X^i)^p \underset{\substack{\uparrow \\ \text{endo de Frobenius}}}{=} \left(\sum_{i=1}^{n} a_i X_i\right)^p = R(X)^p$$

② Une (lointaine) application de l'irréductibilité de φ_n est le théorème de la progression arithmétique de Dirichlet.

③ Un polynôme minimal n'a de sens que dans un anneau principal (donc pas dans $\mathbb{Z}[X]$)

④ La division euclidienne est possible si on divise par un polynôme unitaire. Preuve: On procède par récurrence et on divise tout monôme X^n par $P = \alpha X^p + P_0$, ce qui nous ramène à un degré inférieur.

---

* • au rang $n=1$, c'est le cas précédent.
• Supposons vrai au rang $s-1$.
$k \wedge m = 1 \Rightarrow p_1 \cdots p_{s-1} \wedge m = 1$
$\underset{HR}{\Rightarrow} P(\xi^{p_1 \cdots p_{s-1}}) = 0$
Or $k \wedge m = 1 \Rightarrow p_s \wedge m = 1$ donc
$P((\xi^{p_1 \cdots p_{s-1}})^{p_s}) = P(\xi^k) = 0$

Thm $P \in \mathbb{Z}[X]$ et $\underbrace{\text{primitif}}_{\text{de } ct=1}$ et irréductible sur $\mathbb{Q}[X] \Rightarrow$ irréductible sur $\mathbb{Z}[X]$.

Contraposée : Soit P primitif.

si P réductible sur $\mathbb{Z}$, on peut écrire $P = QR$ où $Q, R \in \mathbb{Z}[X]$ et $d°Q$, $d°R \geq 1$

Alors P réductible dans $\mathbb{Q}[X]$ car $P = QR$ décomp non banale car $ct(P) = 1$.

Contrex si P non primitif :

$P = 2X$ irréd sur $\mathbb{Q}[X]$ mais $P = \underset{\substack{\uparrow \\ \text{non inversible dans } \mathbb{Z}.}}{2} \times X$

Th $P \in \mathbb{Z}[X]$ unitaire $\Rightarrow P$ primitif

OK

Th P irréductible sur $\mathbb{Z} \Rightarrow \begin{cases} P \text{ cste irréd. sur } \mathbb{Z} \\ \text{ou} \\ P \text{ primitif, } d°P \geq 1, \ P \text{ irréd. sur } \mathbb{Q}. \end{cases}$

Preuve :

Soit P irréductible sur $\mathbb{Z}$.

. si P constant, P non nul non inversible donc irréd.

. sinon : Alors $d° P \geq 1$. Par contraposée, si P n'est pas primitif, ($ct(P) = d > 1$), on a $P = d.\hat{P}$ avec $\hat{P}$ primitif.

or d et $\hat{P}$ non inversibles de $\mathbb{Z}$, donc P réductible dans $\mathbb{Z}$.

si P primitif et réductible sur $\mathbb{Q}$, on a $P = \overset{\in \mathbb{Q}[X]}{Q} R^{\in \mathbb{Q}[X]}$

Soit q et n tq qQ et $nR \in \mathbb{Z}[X]$. Alors $q.n.P = qQ\,nR$

et $ct(qnP) = qn$.

d'autre part $ct(qQ\,nR) = c(qQ)\,c(nR)$

Or $\dfrac{qQ}{c(qQ)} \in \mathbb{Z}[X]$ et $\dfrac{nR}{c(nR)} \in \mathbb{Z}[X]$ donc $P = \dfrac{qQ}{c(qQ)} \dfrac{nR}{c(nR)}$

donc P réductible dans $\mathbb{Z}[X]$.

Si $p \in \mathbb{P}$, toutes les racines $p^{\text{ièmes}}$ de l'unité sauf 1 sont des racines primitives de l'unité ($p^{\text{ièmes}}$), et $\Phi_p(X) = \frac{X^p - 1}{X-1} = \sum_{k=0}^{p-1} X^k$

<u>En effet :</u>

. Soit z racine primitive $p^{\text{ième}}$ de l'unité. L'ordre de z dans le groupe mult $\mathbb{C}^*$ divise donc p, donc $z = \left\{\begin{array}{l}1\\p\end{array}\right.$. Ainsi, $z = 1$ ou z racine primitive d'ordre p.

. $$\varphi_p(X) = \prod_{\substack{k=1 \\ k \wedge p = 1}}^{p} (X - \xi^k) = \frac{X^p - 1}{X-1} = \sum_{k=0}^{p-1} X^k$$

En effet, on retire 1 qui n'est pas racine primitive d'ordre p