Polynômes cyclotomiques

CloudSea

Cadre

On considère les polynômes cyclotomiques sur $\mathbb{C}$ $\phi_n = \prod_{\zeta \in \mathbb{U}_n^\times} (X - \zeta)$.
On montre que les ϕ_n sont dans $\mathbb{Z}[X]$ et qu'ils sont irréductibles sur $\mathbb{Q}$, donc sur $\mathbb{Z}$.

Recasages :
- [[102 Groupe des complexes de module 1]]
- [[141 Polynômes irréductibles]]
- [[144 Racines de polynômes]]

Backup :
- [[120 Anneau Z sur nZ]] a mettre dans le plan avant Dirichlet faible mais pas faire un DEV. Dirichlet Faible s'inscrit mieux dans la leçon
- [[125 Extensions de corps]] a mettre dans le plan mais plus parler des extensions cyclotomiques

Référence : Perrin p 83

Déroulé du développement

Montrer que $X^n - 1 = \prod_{d|n} \phi_d$

Pour tout diviseur d de n, $\mathbb{U}_d$ est le seul sous groupe de $\mathbb{U}_n$ d'ordre d. Donc les éléments d'ordre d sont exactement les générateurs de $\mathbb{U}_d$
Donc $\mathbb{U}_n = \bigsqcup_{d|n} \mathbb{U}_d^\times$, donc

$$X^n - 1 = \prod_{z \in \mathbb{U}_n} (X - z) = \prod_{d|n} \prod_{\zeta \in \mathbb{U}_d^\times} (X - \zeta) = \prod_{d|n} \phi_d$$

Montrons que $\phi_n \in \mathbb{Z}[X]$
$n = 1$

ok $\phi_1 = X - 1$

Et si $\forall k \leq n, \phi_k \in \mathbb{Z}[X]$, on a $X^n - 1 = \phi_n P$ où $P = \prod_{d|n, d<n} \phi_d \in \mathbb{Z}[X]$ par hypothèse de récurrence
Donc ϕ_n est le quotient de la division euclidienne de $X^n - 1$ par P dans $\mathbb{C}[X]$. Donc comme $X^n - 1$ et P sont dans $\mathbb{Z}[X]$, on a $\phi_n \in \mathbb{Z}[X]$

Ecrire $\phi_n = \prod_{i=1}^{r} P_i$ avec les P_i unitaires irréductibles sur $\mathbb{Z}$. Montrer que pour tout $\zeta \in \mathbb{U}_n^\times$, μ_ζ est un des P_i

Par théorème de Gauss, $\mathbb{Z}[X]$ est factoriel, donc on a $P_1, \cdots, P_r$ irréductibles tels que $\phi_n = \prod_{i=1}^{r} P_i$
ϕ_n est unitaire, donc quitte à multiplier par -1 on suppose les P_i unitaires

Soit $\zeta \in \mathbb{U}_n^\times$, et soit i tel que P_i annule ζ
P_i est non constant irréductible sur $\mathbb{Z}$, donc irréductible sur $\mathbb{Q}$, donc $P_i = \mu_\zeta$

Soit $\zeta \in \mathbb{U}_n^\times$ et p premier qui divise pas n, montrer que $\mu_\zeta = \mu_{\zeta^p}$

On se place sur $\mathbb{F}_p$
$\mu_{\zeta^p}(X^p)$ annule ζ, donc μ_ζ divise $\mu_{\zeta^p}(X^p)$, donc on a P tel que $\mu_{\zeta^p}(X^p) = \mu_\zeta P$
Dans $\mathbb{F}_p$, avec le Frobenius on obtient $\overline{\mu_{\zeta^p}}^p = \overline{\mu_\zeta}\,\overline{P}$
Donc soit $\overline{Q}$ un facteur irréductible de $\overline{\mu_\zeta}$, $\overline{Q}$ est aussi un facteur irréductible de $\overline{\mu_{\zeta^p}}$

Donc si $\mu_\zeta \neq \mu_{\zeta^p}$, alors $\mu_\zeta \mu_{\zeta^p}$ divise ϕ_n donc divise $X^n - 1$, donc $\overline{\mu_\zeta}\ \overline{\mu_{\zeta^p}}$ divise $X^n - 1$ dans $\mathbb{F}_p[X]$, donc $\overline{Q}^2$ divise $X^n - 1$
Or $(X^n - 1)' = \overline{n} X^{n-1}$ non nul car p divise pas n et admet 0 comme seule racine. Donc $X^n - 1$ est simplement scindé sur son CDD donc n'admet pas de facteur carré, absurde

En déduire que ϕ_n est le polynôme minimal de tous les ζ et conclure

Soit $\zeta = e^{\frac{2i\pi}{n}}$ et soit $\zeta^k \in \mathbb{U}_n^\times$. k est premier à n donc k s'écrit $k = \prod_{i=1}^{r} p_i$ où les p_i sont des nombres premiers qui ne divisent pas n. Donc par récurrence immédiate, $\mu_{\zeta^k} = \mu_\zeta$. Donc tous les $\zeta \in \mathbb{U}_n^\times$ ont le même polynôme minimal

Soit μ ce polynôme, on a donc $\mu | \phi_n$ et $\phi_n | \mu$ donc $\phi_n = \mu$. Donc ϕ_n est le polynôme mini-

mal de tous les $\zeta \in \mathbb{U}_n^\times$, donc il est irréductible sur $\mathbb{Q}$, donc sur $\mathbb{Z}$ car unitaire

Détail de certains points

Montrer que $\mathbb{U}_d$ est le seul sous groupe d'ordre d de $\mathbb{U}_n$

Notons $\omega = \exp\left(\frac{2i\pi}{n}\right)$
Déjà $\mathbb{U}_d$ est bien un sous groupe d'ordre d et il est engendré par $\omega^{\frac{n}{d}}$

Soit G un sous groupe d'ordre d de $\mathbb{U}_n$
G est cyclique donc on a $k \in [|1, n|]$ tel que $G = \langle \omega^k \rangle$
Soit p le pgcd de k et n, on va montrer que $G = \langle \omega^p \rangle$

p divise k, donc $G \subseteq \langle \omega^p \rangle$
Et Bézout donne $p = ku + nv$, donc $\omega^p = (\omega^k)^u(\omega^n)^v = (\omega^k)^u \in G$, donc $\langle \omega^p \rangle \subseteq G$
Et comme p divise n, ω^p est d'ordre $\frac{n}{p}$, donc $d = \frac{n}{p}$ donc $p = \frac{n}{d}$ donc $G = \mathbb{U}_d$

Faire le lien irréductible sur $\mathbb{Z}$ et sur $\mathbb{Q}$

Si P est irréductible sur $\mathbb{Z}$ et non constant, alors P est irréductible sur $\mathbb{Q}$

Soit $P \in \mathbb{Z}[X]$ irréductible (sur $\mathbb{Z}$) non constant
Soient $Q, R \in \mathbb{Q}[X]$ tels que $P = QR$. Soient $q, r \geq 1$ tels que qQ et rR sont dans $\mathbb{Z}[X]$

P est irréductible donc de contenu 1 donc

$$qr = qr\ c(P) = c(qrP) = c(qrQR) = c(qQ)\ c(rR)$$

Donc $P = \frac{1}{qr} qQrR = \frac{qQ}{c(qQ)} \frac{rR}{c(rR)}$ égalité dans $\mathbb{Z}[X]$
Donc comme P est irréductible, on a par exemple $\frac{qQ}{c(qQ)} = \pm 1$ donc P est irréductible sur $\mathbb{Q}$

La réciproque est fausse, $2X$ est irréductible sur $\mathbb{Q}$ mais 2 est pas inversible dans $\mathbb{Z}$ donc c'est réductible sur $\mathbb{Z}$

Si $P \in \mathbb{Z}[X]$ est irréductible sur $\mathbb{Q}$ et de contenu 1 (en particulier si P est unitaire), alors il est irréductible sur $\mathbb{Z}$

Soient $Q, R \in \mathbb{Z}[X]$ tels que $P = QR$
Comme P est irréductible sur $\mathbb{Q}$, on a par exemple Q constant
Or $c(P) = c(Q)c(R)$ donc $c(Q)$ divise 1, donc $c(Q) = \pm 1$ donc $Q = \pm 1$
Donc P est bien irréductible sur $\mathbb{Z}$

Montrer que le contenu est multiplicatif

On commence par le cas où P et Q sont primitifs (i.e. de contenu 1)
On note $P = \sum_{i=0}^{n} a_i X^i$ et $Q = \sum_{j=0}^{m} b_j X^j$
Soit p premier. Soit a_i le premier coeff de P non multiple de p et b_j la même pour Q
Le coeff $i+j$ de PQ est $\sum_{k=0}^{i+j} a_k b_{i+j-k}$
p divise tous les a_k pour $k < i$ et tous les b_{i+j-k} pour $i + j - k < j$ i.e. $i < k$ donc modulo p la somme vaut $a_i b_{i+j-j} = a_i b_j$ qui n'est donc pas multiple de p
Donc on a bien $c(PQ) = 1$

Maintenant soient P et Q quelconques

$$\begin{aligned} c(PQ) &= c\left(c(P)\frac{P}{c(P)}\ c(Q)\frac{Q}{c(Q)}\right) \\ &= c(P)\ c(Q)\ c\left(\frac{P}{c(P)}\ \frac{Q}{c(Q)}\right) \\ &= c(P)\ c(Q)\ c\left(\frac{P}{c(P)}\right)\ c\left(\frac{Q}{c(Q)}\right) \\ &= c(P)\ c(Q) \end{aligned}$$

La même preuve fonctionne sur un anneau quelconque qui admet un pgcd
Et ça permet de montrer de manière non triviale que A factoriel $\Rightarrow A[X]$ factoriel

Montrer que dans $\mathbb{F}_p$, on a bien $P(X^p) = P^p$

Notons $P = \sum_{k=0}^{n} a_k X^k$
Le morphisme de Frobenius donne

$$P^p = \left(\sum_{k=0}^{n} a_k X^k\right)^p = \sum_{k=0}^{n} a_k^p (X^p)^k$$

Et comme on est dans $\mathbb{F}_p$, pour tout a on a $a^p = a$, donc

$$P^p = \sum_{k=0}^{n} a_k^p (X^p)^k = \sum_{k=0}^{n} a_k (X^p)^k = P(X^p)$$

Version révisions

On se propose de montrer que les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}$

1. Montrer que $X^n - 1 = \prod_{d|n} \phi_d$ et en déduire que les ϕ_n sont à coefficients dans $\mathbb{Z}$

2. Décomposer ϕ_n en irréductibles dans $\mathbb{Z}[X]$ et montrer que tout μ_ζ est l'un de ces facteurs

3. Soit ζ une racine primitive et p qui divise pas n

3.1 En se plaçant sur $\mathbb{F}_p$, montrer que si $\overline{Q}$ est un facteur irréductible de $\overline{\mu_\zeta}$, alors c'est aussi un facteur irréductible de $\overline{\mu_{\zeta^p}}$

3.2 En déduire que si $\mu_\zeta \neq \mu_{\zeta^p}$ alors $X^n - 1$ admet un facteur carré sur $\mathbb{F}_p$ et que donc $\mu_\zeta = \mu_{\zeta^p}$

4. En déduire que ϕ_n est le polynôme minimal de tous les ζ et que donc il est irréductible sur $\mathbb{Q}$