1 Recasages

- **102 :** Groupe des nombres complexes de module 1. Racines de l'unité. Applications.
- **120 :** Anneaux $\mathbb{Z}/n\mathbb{Z}$.
- **121 :** Nombres premiers. Applications.
- **123 :** Corps finis. Applications.
- **141 :** Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

2 Développement

Théorème :

Soit $n \in \mathbb{N}^*$, ϕ_n le n° polynôme cyclotomique est à coefficients unitaires et irréductible sur $\mathbb{Z}$.

Preuve :

Etape 1: On montre que pour tout $n \in \mathbb{N}^*$, $\phi_n \in \mathbb{Z}[X]$ est unitaire.

Par récurrence on définit la propriété :

$$\mathcal{P}_n : \phi_n \in \mathbb{Z}[X] \text{ est unitaire}$$

- Si $n = 1$, on a $\phi_1(X) = X - 1 \in \mathbb{Z}[X]$ est unitaire.
- Supposons $\mathcal{P}_d$ vraie pour tout $d < n$. On a :

$$X^n - 1 = \phi_n(X) \underbrace{\prod_{\substack{d<n \\ d|n}} \phi_d(X)}_{g(X)}$$

On a $g(X) \in \mathbb{Z}(X)$ unitaire par hypothèse de récurrence.
Donc ϕ_n est unitaire.
De plus, on effectue la division euclidienne de $X^n - 1$ par g (car g est unitaire), d'où:

$$X^n - 1 = g(X)P(X) + R(X) \quad \text{avec} \quad P, R \in \mathbb{Z}[X] \quad \text{et} \quad \deg(R) < \deg(g)$$

D'où $g(X)(\phi_n(X) - P(X)) = R(X)$, donc pour des raisons de degré on a nécessairement $\phi_n = P \in \mathbb{Z}[X]$.

Etape 2: On montre que pour tout $n \in \mathbb{N}^*$, ϕ_n est irréductible sur $\mathbb{Z}[X]$.

- Soit ω une racine primitive n° de l'unité de $f(X)$ son polynôme minimal sur $\mathbb{Q}$.
On a $f(X)|X^n - 1$ donc il existe $h(X) \in \mathbb{Q}[X]$ tel que :

$$X^n - 1 = f(X)h(X) \quad \text{avec} \quad f, h \in \mathbb{Z}[X]$$

- Soit p premier, ω^p est aussi racine primitive n° de l'unité (car $p \wedge n = 1 \implies \omega = \omega^{\lambda p + \mu n} = (\omega^p)^\lambda$).
Notons g son polynôme minimal sur $\mathbb{Q}[X]$. On montre de même que $g \in \mathbb{Z}[X]$.

(En effet, $\mathbb{Z}[X]$ est factoriel donc $\phi_n(X) = f_1^{\alpha_1}(X)...f_r^{\alpha_r}(X)$, f_i unitaire irrédutible sur $\mathbb{Z}[X]$. On note $f = f_i$ qui annule ω, de même pour g.)

- On montre que $f = g$.
On a $g(\omega^p) = 0$ donc ω est racine de $g(X^p)$ d'où $f(X)|g(X^p)$.
Il existe donc $l(X) \in \mathbb{Z}[X]$ tel que $g(X^p) = f(X)l(X)$.
On projète cette égalité dans $\mathbb{F}_p$ on a alors :

$$g(X) = a_r X^r + ... + a_0 \implies \overline{g(X)}^p = (\overline{a_r} X^r + ... + \overline{a_0})^p = \overline{a_r}^p X^{pr} + ... + \overline{a_0}^p = \overline{g(X^p)}$$

On a alors $\overline{g(X)}^p = \overline{f(X)} \cdot \overline{l(X)}$.

- Soit $\psi(X)$ un diviseur irréductible unitaire de $\overline{f(X)}$ sur $\mathbb{F}_p$.
Par lemme d'Euclide on a que $\psi(X)$ dvise $\overline{g(X)}$.
De plus, f et g divisent $X^n - 1$ donc fg divise $X^n - 1$ d'où $\overline{fg}$ divise $\overline{X^n - 1}$ d'où ψ^2 aussi.

Il existe donc $\theta(X) \in \mathbb{F}_p[X]$ tel que $X^n - 1 = \psi(X)^2\theta(X)$.
On dérive et on obtient :

$$nX^{n-1} = 2\psi(X)\psi'(X)\theta(X) + \psi(X)^2\theta'(X)$$

D'où $\psi(X)|nX^{n-1}$ d'où $\psi(X) = X$ mais X ne divise pas $X^n - 1$ donc impossible.

Contradiction obtenue par l'hypothèse que $f(X) \neq g(X)$ d'où $f = g$.
Donc on a que ω^p est racine de f.

- On a donc que f a pour racines ω^p pour tout p premier et non diviseur de n. On montre que toutes les racines primitives n° de l'unité sont racines de $f(X)$.

Soit u une telle racine alors $u = \omega^h$, $h \in \mathbb{N}$. u est racine primitive donc il existe $h' \in \mathbb{N}$ tel que $\omega = u^{h'}$ d'où :

$$\omega = \omega^{hh'} \implies \omega^{hh'-1} = 1$$

Or $\omega^n = 1$ d'où $n|hh'-1$ et donc $h \wedge n = 1$.

Soit $h = p_1...p_r$ la décomposition en facteurs premiers, p_i ne divisant pas n car $h \wedge n = 1$.
On montre par récurrence sur r que $u = \omega^h$ est racine de $f(X)$.

- Si $r = 1$, on a $u = \omega^{p_1}$ qui est recine d'après ce qui précède.
- Supposon la propriété vraie au rang $r-1$, on a alors $\omega^{p_1 \cdots p_{r-1}}$ qui est racine de $f(X)$.
  Elle est racine primitive n° de l'unité car $p_1...p_{r-1} \wedge n = 1$ d'où en posant $w' = \omega^{p_1 \cdots p_{r-1}}$ on a alors $u = \omega^{p_1 \cdots p_r} = \omega'^{p_r}$ est racine de $f(X)$ d'après ce qui précède.

- Toutes les racines primitives n° de l'unité sont donc racines de $f(X)$.
  On a donc que $\phi_n | f$ mais f est irréductible et unitaire (en tant que polynôme minimal) donc $\phi_n = f$.
  ϕ_n est donc le polynôme minimal sur $\mathbb{Q}$ de toutes les racines primitives n° de l'unité.
  Donc ϕ_n est irréductible sur $\mathbb{Q}[X]$ et donc sur $\mathbb{Z}[X]$ car son contenu est 1 car unitaire.

3 Compléments

Propriété :

Si $n \geq 1$, $X^n - 1 = \prod_{d|n} \phi_d(X)$.

Preuve :

Il suffit d'établir que $X^n - 1$ et $\prod_{d|n} \phi_d(X)$ ont les mêmes racines dans $\mathbb{C}$ avec les mêmes multiplicités.

- Si ω est racine d'ordre d de $X^n - 1$ alors $d|n$ et ω est racine d° primitive donc une racine de ϕ_d.
- Si ω est racine de ϕ_d où $d|n$, c'est-à-dire qu'il existe $\lambda \in \mathbb{Z}$ tel que $w^n = \left(w^d\right)^\lambda = 1$ et ω est racine de $X^n - 1$.
- Les racines de $X^n - 1$ sont simples, il en est de même des racines de $\prod_{d|n} \phi_d(X)$ car $\phi_d(X)$ à des racines simples et les racines de ϕ_d (d'ordre d) sont distinctes des racines de $\phi_{d'}$ (d'ordre d') pour $d' \neq d$.

4 Références

- Cours d'algèbre, *Perrin*
- Théorie des corps, *Carrega*