141 POLYNÔMES IRRÉDUCTIBLES À UNE INDÉTERMINÉE. CORPS DE RUPTURE. EXEMPLES ET APPLICATIONS.

Soit $\mathbb{K}$ un corps et A un anneau intègre, tous deux commutatifs.

I. Polynômes irréductibles [Per96, §II.3/III.3, p45–53/76] [Rom17, §12.8, p368]

I. A. Irréductibilité

Définition de l'irréductibilité de polynômes
Dans le cas d'un corps : simplification de l'irréductibilité, cas des polynômes de degré 1, exemples, lien entre réductibilité et existence de racines pour $\deg(P) \leq 3$
Lemme d'Euclide pour $A[X]$ principal/factoriel, exemple de $(X^2+1)^2$ réductible sur $\mathbb{R}[X]$ bien qu'il n'admette pas de racine
Décomposition en produit d'irréductibles
Il y a une infinité de polynômes irréductibles

I. B. Propriétés de $A[X]$ [Per96, §II.4, p50]

$A[X]$ principal correspond à A est un corps
A factoriel implique $A[X]$ factoriel
Notion de contenu, polynôme primitif, lemme de Gauss
Dans un corps : P irréductible si et seulement si (P) maximal

I. C. Critères d'irréductibilité [FGN07, §5.16, p188–190]

On suppose que A est un anneau factoriel
Lien entre les irréductibles de A et les irréductibles de $\mathrm{Frac}(A)$

Proposition 1. [Critère d'Eisenstein]
Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$. Soit $p \in A$ premier. Si $p \nmid a_n$, $\forall i < n, p \mid a_i$ et $p^2 \nmid a_0$, alors P est irréductible dans $\mathrm{Frac}(A)[X]$.

Exemple 2. Si $m \in \mathbb{Z}$ a un facteur premier sans carré alors $X^n - m$ est irréductible dans $\mathbb{Z}[X]$ pour tout $n \in \mathbb{N}$.

Proposition 3. *Soit I un idéal premier de A et $B = A/I$. Soit $P = \sum_{i=0}^{r} a_i X^i \in A[X]$ et $\overline{P}$ la réduction de P modulo I. Si $\overline{a_n}$ dans B, et si $\overline{P}$ est irréductible sur B ou $\mathrm{Frac}(B)$, alors P est irréductible sur K.*

Que l'on reformule dans le cas $A = \mathbb{Z}$, $I = (p)$, $B = \mathbb{F}_p$:

Proposition 4. *Soit $p \in \mathcal{P}$ et $P = \sum_{i=0}^{r} a_i X^i \in \mathbb{Z}[X]$. Soit $\overline{P}$ la réduction de P modulo p. Si $p \nmid a_n$ et si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.*

Exemple 5. $X^3 + 462X^2 + 2433X - 67691$ est irréductible dans $\mathbb{Z}[X]$, tout comme $X^p - X - 1$ pour tout $p \in \mathcal{P}$.

Cependant la réciproque est fausse, mais dans certains cas particuliers on peut s'en tirer en jonglant entre les corps utilisés

II. Extensions de corps et polynômes

II. A. Extensions de corps [Per96, §III.1, p65–66]

On ne considère que des corps commutatifs.

Définition 6. [Extension de corps, degré]
Soient $\mathbb{K}$ et $\mathbb{L}$ deux corps tels que $\mathbb{K} \subset \mathbb{L}$. On dit que $\mathbb{L}$ est une extension de corps de $\mathbb{K}$. $\mathbb{L}$ est alors un $\mathbb{K}$-e.v.. Lorsque $\dim(\mathbb{L})$ est fini, on note $[\mathbb{L} : \mathbb{K}] = \dim(\mathbb{L})$ et on l'appelle le degré de $\mathbb{L}$ sur $\mathbb{K}$. On dit alors que l'extension est finie.

Exemple 7. $\mathbb{R} \subset \mathbb{C}, \mathbb{Q} \subset \mathbb{Q}(i)$.

Degré d'une extension, exemples

Théorème 8. [Théorème de la base télescopique]
Soient $\mathbb{K}, \mathbb{L}, \mathbb{M}$ des corps, $(e_i)_{i\in I}$ une base de $\mathbb{L}$ sur $\mathbb{K}$, $(f_j)_{j\in J}$ une base de $\mathbb{M}$ sur $\mathbb{L}$. Alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$. En particulier, lorsque deux des degrés d'extensions sont finis, le troisième aussi et on a $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Définition 9. [Élément algébrique, transcendant]
Soit $\mathbb{L}$ une extension de $\mathbb{K}$, soit $\alpha \in \mathbb{L}$. Soit $\phi : \mathbb{K}[T] \longrightarrow \mathbb{L}$ le morphisme d'anneaux tel que $\phi_{|\mathbb{K}} = \mathrm{id}$ et $\phi(T) = \alpha$.
Si ϕ est injectif, on dit que α est transcendant sur $\mathbb{K}$. Sinon, $\alpha \in \mathbb{L}$ est algébrique sur $\mathbb{K}$ et $P \in \mathbb{K}[X]$ unitaire tel que $\ker(\phi) = (P)$. P est appelé polynôme minimal de α.

Exemple 10. $\sqrt{2}, i$ sont algébriques sur $\mathbb{Q}$. e et π sont transcendants sur $\mathbb{Q}$.

Théorème 11. [Caractérisation d'un algébrique]
Soit $\mathbb{L}$ une extension de $\mathbb{K}$. Pour $\alpha \in \mathbb{L}$, on a :

$$\alpha \text{ est algébrique sur } \mathbb{K} \iff \mathbb{K}[\alpha] = \mathbb{K}(\alpha) \iff \dim(\mathbb{K}[\alpha]) < +\infty$$

Liens entre irréductibilité et degré des extensions [Per96, §III.3, p77–79]

II. B. Corps de rupture et de décomposition [Per96, §III.1.c, p70]

Corps de rupture d'un polynôme irréductible, existence et unicité à isomorphisme près.
Exemple de $\mathbb{C}$, de $\mathbb{Q}[\sqrt{2}]$
Degré du corps de rupture
Corps de décomposition, existence et unicité à isomorphisme près
Exemple de $\mathbb{Q}(i, \sqrt{2})$
Théorème de l'élément primitif

II. C. Cloture algébrique [Per96, §III.1.c, p70]

Extension algébrique, corps algébriquement clos, formulations équivalentes
Théorème de D'ALEMBERT-GAUSS [Rom17, p378]
Application : toute matrice de $\mathcal{M}_n(\mathbb{C})$ est trigonalisable
Polynôme ne s'annulant pas sur un corps fini $\to$ tout corps fini n'est pas algébriquement clos
Clôture algébrique, tout corps admet une clôture algébrique unique à isomorphisme près

III. Polynômes cyclotomiques [Per96, §3.4, p80] [Rom17, §12.11.5, p383]

Soit $n \in \mathbb{N}^*$.

DÉFINITION 12. [POLYNÔMES CYCLOTOMIQUES]
On définit le n-ième polynôme cyclotomique $\Phi_n \in \mathbb{C}_n[X]$ par $\Phi_n(X) = \prod_{\zeta \in \mathbb{U}_n^\times} (X - \zeta)$.

PROPOSITION 13.
(i) Φ_n *est unitaire de degré* $\varphi(n) = \mathrm{card}(\{k \in [1, n] \mid k \wedge n = 1\})$.
(ii) $X^n - 1 = \prod_{d|n} \Phi_d$. *En particulier, si* n *est premier :* $\Phi_n = X^n - 1$.

COROLLAIRE 14.
- *On en déduit la fameuse formule* $\phi(n) = \sum_{d \mid n} \phi(d)$.
- *Pour* $n \geq 2$, $\sum_{\omega \in \mathbb{U}_n} \omega = 0$.

PROPOSITION 15. $\Phi_n \in \mathbb{Z}[X]$.

THÉORÈME 16. Φ_n *est irréductible sur* $\mathbb{Z}$ *et donc sur* $\mathbb{Q}$.

COROLLAIRE 17. *On a* $[\mathbb{Q}[e^{2i\pi/n}] : \mathbb{Q}] = \varphi(n)$.

APPLICATION 18. Théorème de DIRICHLET faible

COMMENTAIRES

Autres références : [BMP05, Gou09].

QUESTIONS

Q $X^4 + 1$ est-il irréductible ?
R Oui, il n'a pas de racine et on peut appliquer le critère d'EISENSTEIN à $(X + 1)^4 + 1$ avec $p = 2$.
Q $X^4 + 1$ est-il irréductible sur $\mathbb{F}_p$?
R Sur $\mathbb{F}_{p^2}$ cyclique, $X^8 - 1 = (X^4 + 1)(X^4 - 1)$ et $8 \mid (p^2 - 1) = (p - 1)(p + 1)$.
Q Peut-on construire une famille de polynômes $(X^n + a)_n$ irréductibles sur $\mathbb{Q}$ pour tout n ?

BIBLIOGRAPHIE

[BMP05] V. BECK, J. MALICK et G. PEYRÉ : *Objectif Agrégation*. H&K, 2ème édition, 2005.

[FGN07] S. FRANCINOU, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Algèbre 1*. Cassini, 2007.

[Gou09] X. GOURDON : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.