1 Recasages

- **122 :** Anneaux principaux. Exemples et applications
- **142 :** PGCD et PPCM, algorithmes de calculs. Applications.

2 Développement

Théorème :

Soit A un anneau factoriel et $K = \text{Frac}(A)$. $P(X) = a_n x^n + \cdots + a_0 \in A[X]$.
Soit $p \in A$ un élément irréductible. On suppose :

- $p \nmid a_n$
- $p^2 \nmid a_0$
- $p \mid a_i, \forall i \in \{0, \ldots, n-1\}$

Alors P est irréductible sur $K[X]$.

Preuve :

Etape 1 : On montre que le produit deux polynômes primitifs de $A[X]$ est primitif.

Soit P, Q primitifs et $C = PQ$, on suppose par l'absurde que C n'est pas primitif, c'est-à-dire qu'il existe p premier qui divise tous les coefficients c_k de C.

On a donc $\overline{C} = 0$ dans $A/(p)[X]$ et donc :

$$\overline{PQ} = 0 \implies \overline{P} = 0 \quad \text{ou} \quad \overline{Q} = 0 \quad \text{par intégrité de } A/(p)$$

On a donc que p divise tous les coefficients de P ou de Q ce qui est absurde car $c(P) = c(Q) = 1$.

Etape 2 : On montre que pour $P, Q \in A[X],\ c(PQ) = c(P)c(Q)$.

On a :

$$PQ = c(P)c(Q)\frac{P}{c(P)}\frac{Q}{c(Q)}$$

Les polynômes $\dfrac{P}{c(P)}$ et $\dfrac{Q}{c(Q)}$ sont primitifs donc leur produit aussi d'après l'étape 1.

On a donc :

$$c(PQ) = c\left(c(P)c(Q)\frac{P}{c(P)}\frac{Q}{c(Q)}\right) = c(P)c(Q)\,\underbrace{c\left(\frac{P}{c(P)}\frac{Q}{c(Q)}\right)}_{=1} = c(P)c(Q)$$

Etape 3 : On raisonne par l'absurde en supposant que P est réductible sur $K[X]$.

On montre tout d'abord que P est alors réductible sur $A[X]$.
On écrit $P = c(P)P'$ avec P' primitif et $P' = Q'R' \in K[X]$.
On note q (resp. r) le produit des dénominateurs des coefficients de Q' (resp. de R').
On note donc $Q = qQ'$ et $R = rR'$ deux polynômes de $A[X]$.
D'où :

$$qrP' = qQ'rR' = QR \implies qr = c(Q)c(R)$$

On a donc :

$$P = c(P)\frac{Q}{c(Q)}\frac{R}{c(R)} = \underbrace{\left(c(P)\frac{Q}{c(Q)}\right)}_{\in A[X]} \cdot \underbrace{\left(\frac{R}{c(R)}\right)}_{\in A[X]}$$

On a donc bien que P est réductible sur $A[X]$.

Quitte à considérer des polynômes primitifs (c'est-à-dire à multiplication par le contenu près), on suppose qu'on peut écrire $P = QR$ avec $Q, R \in A[X]$.
On écrit alors :

$$\begin{cases} Q &= b_q X^q + \cdots + b_0 \\ R &= c_r X^r + \cdots + c_0 \end{cases} \qquad \text{où} \quad 1 \leq r, q \leq n-1$$

A est factoriel et p irréductible donc l'idéal (p) est premier et donc l'anneau quotient $A/(p)$ est intègre.
On projète l'égalité $P = QR$ dans $A/(p)[X]$ on a alors :

$$\overline{a_n} X^n = \overline{Q} \cdot \overline{R}$$

Cette égalité est toujours vraie dans $\text{Frac}(A/(p))[X] = L[X]$.

L est un corps donc $L[X]$ est principal et en considérant le morphisme

$$\phi : \begin{cases} L[X] & \to & L \\ P & \mapsto & P(0) \end{cases}$$

On a que $L[X]/(X) \simeq L$ donc (X) est maximal et donc X est irréductible et donc par uunicité de la décomposition en polynômes irréductibles on a que :

$$X \mid \overline{Q} \ \text{ et } \ X \mid \overline{R} \ \text{ d'où } \ \overline{b_0} = \overline{c_0} = 0$$

C'est-à-dire qu'on a $p \mid b_0$ et $p \mid c_0$ et donc $p^2 \mid a_0$. Ce qui est absurde par hypothèse du critère, d'où l'irréductibilité de P.

Application:

$\phi_p(X) = X^{p-1} + \cdots + X + 1$ est irréductible dans $\mathbb{Z}[X]$.

Preuve :

On a :

$$\begin{aligned}\phi_p(X+1) &= \sum_{k=0}^{p-1}(X+1)^k \\ &= \frac{(X+1)^p - 1}{X} \\ &= \frac{1}{X}\left(\sum_{k=0}^{p}\left(p//k\right)X^k - 1\right) \\ &= \frac{1}{X}(X^p + pX^{p-1} + \cdots + pX) \\ &= X^{p-1} + pX^{p-2} + \cdots + p\end{aligned}$$

Par critère d'Eisenstein on a :

- $p^2 \nmid \underbrace{a_0}_{=p}$
- $p \nmid \underbrace{a_{p-1}}_{=1}$
- $\forall k \in \{1, \ldots, p-1\},\ p \mid k!\binom{p}{k} \implies p \mid \binom{p}{k}$ car $p \wedge k! = 1$ On a donc $p|a_i$ pour tout $i \in \{0, \ldots, p-2\}$

On a donc que ϕ_p est irréductible sur $\mathbb{Q}[X]$ et $c(\phi_p) = 1$ donc irréductible sur $\mathbb{Z}[X]$.

3 Compléments

- Savoir démontrer :

$$p \text{ irréductible} \implies (p) \text{ premier} \implies A/(p) \text{ intègre}$$

  - Supposons p irréductible sur A et que $p \mid qr$ avec $q \in A^\times$ ou $r \in A^\times$.
    On a donc $p \mid q$ ou $p \mid r$ par lemme de Gauss donc p est un élément premier et donc (p) est un idéal premier.
  - Supposons (p) premier.
    Soient $\overline{q}, \overline{r} \in A/(p)$ tels que $\overline{q} \cdot \overline{r} = 0$.
    On a donc $qr \in (p)$ et donc $q \in (p)$ ou $r \in (p)$ car (p) est premier.
    C'est-à-dire qu'on a $\overline{q} = 0$ ou $\overline{r} = 0$, d'où $A/(p)$ est intègre.

- Savoir démontrer que si L est un corps, $L[X]$ est un anneau principal.

$$L \text{ est un corps} \implies L[X] \text{ est euclidien} \implies L[X] \text{ est principal}$$

- Savoir démontrer que $L[X]/(X) \simeq L$.
  On a $\ker\phi = (X)$ et donc $L[X]/\ker\phi \simeq \mathrm{Im}\phi$ d'où le résultat. On montre "à la main" la bijection entre $L[X]/\ker\phi$ et $\mathrm{Im}\phi$.

- Savoir démontrer :

$$(a) \text{ maximal} \implies a \text{ irréductible}$$

  Soit $a = bc$, montrons que b ou c est inversible.
  On a que (a) est maximal, donc premier et donc a est un élément premier. On a donc que $a \mid b$ ou $a \mid c$ et donc $c \in A^\times$ ou $b \in A^\times$ et donc a est irréductible.

4 Références

- Cours d'algèbre, *Perrin*
- Oraux X-ENS Algèbre 1, *F-G-N*