

Lemme d'Eisenstein: Perrin p 76 122-125-141-120.

Soit A un anneau factoriel, K le corps des fractions de A ,
 $f(X) = a_n X^n + \dots + a_0$ avec $a_i \in A$. Soit $p \in A$ irréductible. On suppose:

1) $p \nmid a_n$

2) $\forall i = 0, \dots, n-1; p \mid a_i$

3) $p^2 \nmid a_0$

Alors f est irréductible dans $K[X]$

Démonstration: Si f n'est pas irréductible dans $K[X]$, on a: $f(X) = Q(X)R(X)$
où $Q, R \in A[X]$ et $\deg(Q), \deg(R) < \deg(f)$

Poseons alors $\begin{cases} Q(X) = b_q X^q + \dots + b_0 \\ R(X) = c_r X^r + \dots + c_0 \end{cases}$ avec $b_i, c_i \in A, 0 \leq q, r < n$

Comme A est factoriel et p irréductible alors l'idéal (p) est premier
donc $B = A/(p)$ est intègre.

Projetons l'égalité $f = QR$ dans $B[X]$:

$$\overline{f}(X) = \overline{a_n} X^n = (\overline{b_q} X^q + \dots + \overline{b_0})(\overline{c_r} X^r + \dots + \overline{c_0})$$

Comme $\overline{a_n} \neq 0$, alors $\overline{b_q}, \overline{c_r} \neq 0$.

Soit L le corps des fractions de B . Alors cette égalité est encore
vraie dans $L[X]$. Comme $L[X]$ est principal et X irréductible;
par unicité de la décomposition en facteurs irréductibles dans $L[X]$,
on a: $X \mid \overline{b_q}, \overline{c_r}$ donc $\overline{b_0} = \overline{c_0} = 0$ dans B .

Dans ce cas: $p^2 \mid a_0 = b_0 c_0$ contrairement à l'hypothèse.

Finalement: f est irréductible dans $K[X]$.

Application: Irréductibilité de Φ_p dans $\mathbb{Q}[X]$

Soient p est premier et $\Phi_p = X^{p-1} + \dots + X + 1$ le p -ième polynôme
cyclotomique.

1) Montrons que $U = (X+1)^{p-1} + \dots + (X+1) + 1$ est irréductible dans $\mathbb{Q}[X]$

$$U = \Phi_p(X+1) = \sum_{i=0}^{p-1} (X+1)^i = \frac{1 - (X+1)^p}{1 - (X+1)} = \frac{(X+1)^p - 1}{X}$$

$$= \frac{1}{X} \left[\sum_{k=0}^p \binom{p}{k} X^k - 1 \right] = \frac{1}{X} \left[\binom{p}{0} X^0 + \dots + \binom{p}{p} X^p - 1 \right]$$

$$= \underbrace{1}_{a_{p-1}} X^{p-1} + \underbrace{\binom{p}{p-1}}_{a_{p-2}} X^{p-2} + \dots + \underbrace{\binom{p}{1}}_{a_0 = p} X \in \mathbb{Z}[X]$$

On veut appliquer le critère d'Eisenstein:

1) $p \nmid 1$ 3) $p^2 \nmid p$

Montrons que $p \mid a_{p-2}, \dots, a_0$ i.e. $p \mid \binom{p}{p-1}, \dots, \binom{p}{2}, \binom{p}{1}$

Soit $k \in \{2, \dots, p-1\}$

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \quad \text{donc} \quad k! \cdot \binom{p}{k} = p(p-1) \times \dots \times (p-k+1)$$

donc $p \mid k! \cdot \binom{p}{k}$ or p est premier avec $k!$ car $k < p$

donc par le théorème de Gauss: $p \mid \binom{p}{k}$.

Finalement: U est irréductible dans $\mathbb{Q}[X]$

2) Supposons par l'absurde que $\Phi_p = BC$ où $B, C \in \mathbb{Q}[X]$ avec $\deg(B), \deg(C) < \deg(\Phi_p)$

Alors $U = \Phi_p(X+1) = B(X+1)C(X+1)$ avec $\deg(B(X+1)) = \deg(B) < \deg(U)$

et $\deg(C(X+1)) < \deg(U)$

Alors U n'est pas irréductible. Contradiction.

Application 2: Il existe des polynômes de tout degré qui sont irréductibles dans $\mathbb{Q}[X]$.

Soit $f = X^n - 2$, $n \geq 1$ et $p = 2$

Alors $p^2 \nmid (-2)$; $p \mid (-2)$; $p \nmid 1$.

$\parallel$ $\parallel$ $\parallel$
 a_0 a_0 a_n
 $\uparrow$

④ R P = QR, Q, R ∈ K[X]; ∃ Q̃, R̃ ∈ A[X] / A = Q̃R̃

Savoir a = produit du dénominateur de Q

$$b = \text{-----} R$$

Alors aQ; bR ∈ A[X]

donc dans A[X], abP = (aQ)(bR)

En passant au contenu: ab c(P) = c(aQ) c(bR) (1)

$$\text{donc } ab = \frac{1}{c(P)} c(aQ) c(bR)$$

donc P = $\frac{1}{ab} (aQ)(bR) = c(P) \frac{(aQ)}{c(aQ)} \frac{(bR)}{c(bR)}$ qui est un produit de polynômes dans A[X].

⑤ Lemme p. 51 si P, Q sont primitifs et c(P) = c(Q) = 1

si c(PQ) ≠ 1, ∃ p ∈ A m / p | c(PQ) car A est factoriel

Comme c(P) = c(Q) = 1, ∃ i₀, j₀ ∈ ℕ / i₀ < i₀, p | a_{i₀} et p ∤ a_{i₀}

∃ j₀, p | b_{j₀} et p ∤ b_{j₀}

$$\text{Par lepp: } p | c_{i_0+j_0} = \sum_{i+j=i_0+j_0} a_i b_j = a_{i_0} b_{j_0} + \text{reste}$$

Donc alors p | a_{i_0} b_{j_0} (car)

Si d = c(P), e = c(Q); P' = $\frac{P}{d}$; Q' = $\frac{Q}{e}$ alors c(P') = c(Q') = 1

et PQ = de P'Q' avec c(P'Q') = 1. donc c(PQ) = de = $\underbrace{c(P') c(Q')}_{c(P) c(Q)}$.