Lemme de Gauss et critère d'Eisenstein :

Références : [Gou S8] [Rom 382]

Énoncé : Soit $P \in \mathbb{Z}[X]$, $P(X) = \sum_{n=0}^{d} a_n X^n$. Si il existe p un nombre premier tel que :

i) $p \nmid a_n$, ii) $p \mid a_k$ $\forall k \in [\![0; n-1]\!]$, iii) $p^2 \nmid a_0$

Alors P est irréductible dans $\mathbb{Q}[X]$

Étapes : par contraposée : on suppose i) et ii) et on mq (P réductible dans $\mathbb{Q}[X] \Rightarrow p^2 \mid a_0$)

Étape 1 : se ramener à travailler dans $\mathbb{Z}[X]$

Lemme 1 : Lemme de Gauss : $c(PQ) = c(P)c(Q)$

Lemme 2 : Si P est irréductible dans $\mathbb{Z}[X]$ alors il est irréductible dans $\mathbb{Q}[X]$

Étape 2 : Si P est réductible dans $\mathbb{Q}[X]$ alors il est réductible dans $\mathbb{Z}[X]$ et on mq $p^2 \mid a_0$

Application : Pour p premier, $\Phi_p(X) = X^{p-1} + \dots + 1$ est irréductible. Astuce considérer $(X-1)\Phi(X) = X^p - 1$ pour obtenir $X\Phi(X+1) = (X+1)^p - 1$ puis $\Phi(X+1) = \sum_{k=0}^{p-1} \binom{p}{k} X^k$

Autres astuces : • Étudier les possibles racines rationnelles

Ex [Esc 262] Mq $5X^3 - 4X^2 + 6$ est irréd dans $\mathbb{Q}[X]$

• Si P est irréd dans $\mathbb{Z}/p\mathbb{Z}[X]$ il est irréd dans $\mathbb{Z}[X]$

Critère d'Eisenstein - démonstration :

Soit $P \in \mathbb{Z}[X]$ un polynôme non constant tel que $P = \sum_{k=0}^{n} a_k X^k$. Si il existe p premier tel que :

i) $p \nmid a_n$

ii) $p \mid a_k$ pour tout $k \in [\![0; n-1]\!]$

iii) $p^2 \nmid a_0$

Alors P est irréductible dans $\mathbb{Q}[X]$.

Démo : Supposons $P = \sum_{k=0}^{n} a_k X^k$ est un polynôme non constant tel que $p \nmid a_n$ et $p \mid a_k \ \forall k \in [\![0; n-1]\!]$

Mq (P réductible dans $\mathbb{Q}[X] \Rightarrow p^2 \mid a_0$).

Étape 1 : se ramener à étudier $P = QR$ avec $Q, R \in \mathbb{Z}[X]$

Lemme 1 : Lemme de Gauss. $c(PQ) = c(P)c(Q)$.

Preuve : mq si PQ n'est pas primitif alors P ou Q n'est pas primitif

Si $c(PQ) \neq 1$ alors $\exists p \in \mathbb{N}$ premier tel que $p \mid c(PQ)$

Donc $\overline{PQ} = \overline{0}$ or $\overline{PQ} = \overline{P} \cdot \overline{Q}$

Or comme $\mathbb{F}_p$ est un corps, c'est en particulier un anneau intègre donc $\mathbb{F}_p[X]$ est intègre donc $\overline{P} = \overline{0}$ ou $\overline{Q} = \overline{0}$. Donc $p \mid c(P)$ ou $q \mid c(Q)$. Donc $c(P) > 1$ ou $c(Q) > 1$

Donc P ou Q n'est pas primitif.

Par contraposée on a alors P, Q primitifs $\Rightarrow PQ$ primitif.

Prenons alors $P, Q \in \mathbb{Z}[X]$,

$\frac{1}{c(P)} P$ et $\frac{1}{c(Q)} Q$ sont des polynômes primitifs

Donc $\frac{1}{c(P)c(Q)} PQ = R$ est primitif.

Donc $PQ = c(P)c(Q)R$. Donc $c(P)c(Q)$ est le plus grand diviseur commun des coefficients de PQ.

$c(PQ) = c(P)c(Q)$. ∎

Lemme 2: Si $P \in \mathbb{Z}[X]$ est irréductible dans $\mathbb{Z}[X]$, alors P est irréductible dans $\mathbb{Q}[X]$

Preuve: Supposons $P \in \mathbb{Z}[X]$ irréductible dans $\mathbb{Z}[X]$. Soient $Q, R \in \mathbb{Q}[X]$ tq $P = QR$.

$\exists n, m \in \mathbb{N}$ tq $nQ(X) = Q_1(X) \in \mathbb{Z}[X]$ et $mR(X) = R_1(X) \in \mathbb{Z}[X]$

Donc $nm P(X) = Q_1(X) R_1(X)$

Or $nmc(P) = c(Q_1)c(R_1)$ par le lemme de Gauss.

Donc comme $P = QR = \frac{1}{n \cdot m} Q_1(X) R_1(X)$

on a $P = \frac{c(Q_1)c(R_1)}{n \cdot m} Q_2(X) R_2(X)$ avec $Q_2, R_2 \in \mathbb{Z}[X]$

Ainsi, $P = \underbrace{c(P) Q_2(X)}_{\in \mathbb{Z}[X]} \underbrace{R_2(X)}_{\in \mathbb{Z}[X]}$

Or P est irréductible dans $\mathbb{Z}[X]$ donc $\deg(Q_2)=0$ ou $\deg(R_2)=0$

Donc $\deg(R)=0$ ou $\deg(Q)=0$ et P est irréductible dans $\mathbb{Q}[X]$

Étape 2 : Supposons P réductible dans $\mathbb{Q}[X]$. Alors par le lemme précédent il est réductible dans $\mathbb{Z}[X]$.

Donc $\exists Q, R \in \mathbb{Z}[X]$ tels que $P = QR$.

Comme p divise tous les coefficients de P sauf a_n,

On projette dans $\mathbb{F}_p$: $\overline{P}(X) = \overline{a_n} X^n$

Et si on note $Q = \sum_{k=0}^{d_1} b_k X^k$, $R = \sum_{k=0}^{d_2} c_k X^k$ avec $d_1+d_2=n$

On a $\overline{P}(X) = \overline{a_n} X^n = (\overline{b_{d_1}} X^{d_1} + \dots + \overline{b_0})(\overline{c_{d_2}} X^{d_2} + \dots + \overline{c_0})$

Comme $\overline{a_n} \neq \overline{0}$ on a aussi $\overline{b_{d_1}} \neq \overline{0}$ et $\overline{c_{d_2}} \neq \overline{0}$ par intégrité de $\mathbb{F}_p$. Donc $\overline{Q}$ est de degré d_1 et $\overline{R}$ de degré d_2. Comme $\mathbb{F}_p[X]$ est principal on a unicité de la DPFI, et comme X est irréductible, et X^n divise P alors X divise $\overline{Q}(X)$ et $\overline{R}(X)$ donc $\overline{b_0} = \overline{c_0} = \overline{0}$

Donc $p \mid b_0$ et $p \mid c_0$.

Or le coefficient constant de P est $b_0 c_0$. Donc $p^2 \mid a_0$. □

Application : Les polynômes cyclotomiques sont

irréductibles. [Gou 91] [Rom 384]

$U_n = \{e^{2ik\pi/n} ; k \in \mathbb{Z}\}$, Soit $k \in \mathbb{Z}$, $e^{2ik\pi/n}$ engendre U_n ssi k est premier avec n

(gᵏ engendre $\langle g \rangle$ ssi k est premier avec n (Bézout)).

On note $\Pi_n = \{e^{2ik\pi/n} ; k \in [\![1; n-1]\!], k \wedge n = 1\}$.

C'est l'ensemble des racines primitives de l'unité, et il est de cardinal $\varphi(n)$ (nombre de nombre premiers avec n entre 1 $n-1$)

Soit $n \in \mathbb{N}^*$, on définit le polynôme cyclotomique

$$\Phi_n(X) = \prod_{\omega \in \Pi_n} (X - \omega)$$

- Si p est premier, $\Pi_p = \{e^{ik2\pi/n}, k \in [\![1; p-1]\!]\}$

Et $X^p - 1 = \prod_{k=0}^{p-1} (X - e^{2ik\pi/n}) = (X-1) \prod_{\omega \in \Pi_p} (X - \omega) = (X-1)\Phi_p(X)$

Donc $\Phi_p(X) = \dfrac{X^p - 1}{(X-1)} = \sum_{k=0}^{p-1} X^k = X^{p-1} + \dots + X + 1$

- Si $n \in \mathbb{N}^*$ quelconque, $\Phi_n(X) = \prod_{d \mid n} \Phi_d(X)$

union disjointe

En effet, mq $\bigsqcup_{d \mid n} \Pi_d = U_n$

Soit $\omega \in \Pi_d$ avec d diviseur de n.

Alors $\omega^d = 1$ et $\omega^n = \omega^{d \times \frac{n}{d}} = 1^{\frac{n}{d}} = 1$, $\omega \in U_n$

Donc $\bigcup_{d|n} \Pi_d \subset \mathbb{U}_n$.

Soit $\omega \in \mathbb{U}_n$. $\exists k \in [\![0; n-1]\!]$ $\omega = e^{2i\pi k/n}$

Mq $\exists d \in \mathbb{N}^*$, $\omega^d = 1$

$\omega^d = e^{2i\pi kd/n}$

$\omega^d = 1$ si $\frac{kd}{n}$ est entier

Si on note $\delta = pgcd(k; n)$ et $k = \delta k'$, $n = \delta n'$

$\omega^d = 1$ si $\frac{k'd}{n'}$ est entier. Comme $n' \nmid k'$ car ils sont premiers entre eux, alors la condition devient $n' | d$. Le plus petit entier satisfaisant cette condition est $d = n'$. On a alors $\omega^d = 1$ pour $d = \frac{n}{k \wedge n}$

Donc $\omega \in \Pi_d \subset \bigcup_{d|n} \Pi_d$

Donc $\mathbb{U}_n = \bigcup_{d|n} \Pi_d$. Cette union est bien disjointe car un élément de Π_d est d'ordre d et un élément de $\Pi_{d'}$ est d'ordre d'.

Donc $\{\Pi_d \mid d|n\}$ forme une partition de $\mathbb{U}_n$.

Si $n = 1$, $\Pi_1 = \mathbb{U}_1 = \{1\}$ et $X - 1 = \Phi_1(X)$

Si $n \geq 2$, $X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega) = \prod_{d|n} \left(\prod_{\omega \in \Pi_d} (X - \omega) \right) = \prod_{d|n} \Phi_d(X)$

1) a) Soient $P, Q \in \mathbb{Z}[X]$ et p un nombre premier.
On suppose que p divise tous les coefficients du produit PQ.
Mq p divise tous les coef de P ou tous les coef de Q.

$$\sum_{k=0}^{n} a_k X^k = P(X) \qquad \sum_{k=0}^{m} b_k X^k = Q(X)$$

$$P(X)Q(X) = \sum_{k=0}^{n} a_k \left(\sum_{j=0}^{m} b_j X^j \right) X^k$$

$$= \sum_{i=0}^{n} \left(\sum_{j=0}^{m} a_i b_j X^{i+j} \right)$$

Les quelques lemmes de Rombaldi :

Lemme 12.8 : Soit p un nombre premier

1. $A_1, \dots, A_k$ des polynômes de $\mathbb{Z}[X]$ et $A = \sum_{j=1}^{k} A_j$,
on a alors $\mathbb{F}_p[X]$; $\overline{A}^p = \sum_{j=1}^{k} \overline{A_j}^p$

$$A_1 = \sum_{k=0}^{d_1} a_{1,k} X^k$$

$$\overline{A_1}^p = \sum_{k=0}^{d_1} \overline{a_{1,k}}^p X^k$$

↳ considérons $A_1 + A_2 = \sum_{k=0}^{d_1} a_{1,k} X^k + \sum_{k=0}^{d_2} a_{2,k} X^k$

$$\overline{A_1}^p + \overline{A_2}^p = \sum_{k=0}^{\min(d_1;d_2)} \left(\overline{a_{1,k}}^p + \overline{a_{2,k}}^p \right) X^k + \sum_{k=\min(d_1;d_2)+1}^{\max(d_1;d_2)} \overline{a_{i,k}}^p X^k$$