6. Entiers algébriques

VI.1) Soit $x = \frac{p}{q}$, $q \in \mathbb{N}^*$ $p \in \mathbb{Z}$ $p \wedge q = 1$

On suppose x racine de $P = \sum_{i=0}^{n} a_i X^i$ où $\forall i\ a_i \in \mathbb{Z}$ et $a_n = 1$.

alors $q^n \sum_{i=0}^{n} a_i \left(\frac{p}{q}\right)^i = 0$

$$q\left(\sum_{i=0}^{n-1} a_i p^i q^{n-1-i}\right) = -p^n$$

Donc $q \mid p^n$ or $q \wedge p = 1$ donc $q \wedge p^n = 1$

et par conséquent $q \mid 1$, puis $q = 1$.

En conclusion $x \in \mathbb{Z}$. q.e.d.

VI.2) On peut écrire $a = c(a)\,\alpha$ où $\alpha \in \mathbb{Z}[X]$ avec $c(\alpha) = 1$

De même on écrit $\beta = c(\beta)\,\beta$ avec $c(\beta) = 1$.

Donc $ab = c(a)\,c(\beta)\,\alpha\beta$.

$c(ab) = c(a)\,c(\beta)$ équivaut à $c(\alpha\beta) = 1$.

Soit p un nombre premier, soit $i_\alpha = \max\{i,\ p \nmid \alpha_i\}$

(un tel i_α existe car $\{i,\ p \nmid \alpha_i\} \neq \emptyset$ puisque $c(\alpha) = 1$)

Définissons de même $i_\beta = \max_i \{i,\ p \nmid \beta_i\}$.

Examinons le coefficient $\gamma_{i_\alpha + i_\beta}$ de $X^{i_\alpha + i_\beta}$ dans $\alpha\beta$

$$\gamma_{i_\alpha + i_\beta} = \sum_{p+q = i_\alpha + i_\beta} \alpha_p \beta_q = \underbrace{\sum_{p > i_\alpha} \alpha_p \beta_q}_{\text{divisible par } p} + \underbrace{\alpha_{i_\alpha}\,\beta_{i_\beta}}_{\substack{\text{premier} \\ \text{avec } p}} + \underbrace{\sum_{q > i_\beta} \alpha_p \beta_q}_{\text{divisible par } p}$$

Donc $p \nmid \gamma_{i_\alpha + i_\beta}$.

$\forall p \in \mathcal{P}\ \exists i\ p \nmid \gamma_i$ donc $c(\alpha\beta) = 1$.

q.e.d.

VI.3). Il existe au moins un polynôme P_x dans $\mathbb{Z}[X]$, unitaire et de degré minimal et tel que $P_x(x)=0$.

- Supposons que ce polynôme ne soit pas irréductible dans $\mathbb{Q}[X]$, alors on peut écrire

$$P_x = PQ, \quad P \in \mathbb{Q}[X],\ Q \in \mathbb{Q}[X]\ 1 \leq \deg P < \deg P_x$$

Ecrivons $\boxed{P = \frac{a}{b} P_1}$ où $P_1 \in \mathbb{Z}[X]$ et $c(P_1)=1$ $a \wedge b = 1$

$\boxed{Q = \frac{c}{d} Q_1}$ où $Q_1 \in \mathbb{Z}[X]$ et $c(Q_1)=1$ $c \wedge d = 1$

alors $$P_x = \frac{ac}{bd} P_1 Q_1 = \frac{a'}{b'} P_1 Q_1 \quad \text{avec } a' \wedge b' = 1,\ b' \in \mathbb{N}^*.$$

$$b' P_x = a' P_1 Q_1$$

$$c(b' P_x) = c(a' P_1 Q_1)$$

$$b' c(P_x) = a' c(P_1) c(Q_1)$$

$$b' = a' \quad \text{et donc } a' = b' \text{ puis}$$

$$\boxed{P_x = P_1 Q_1 \quad \text{où } P_1 \in \mathbb{Z}[X] \quad Q_1 \in \mathbb{Z}[X] \quad 1 \leq \deg P_1 < \deg P_x.}$$

(On a montré ici qu'un polynôme de $\mathbb{Z}[X]$, irréductible sur $\mathbb{Z}[X]$ est irréductible sur $\mathbb{Q}[X]$, par la contraposée)

Or a $\underline{P_x(x) = 0 = P_1(x) Q_1(x)}$, donc $P_1(x)=0$ ou $Q_1(x)=0$ ce qui contredit la minimalité du degré.

Par contraposée P_x est irréductible dans $\mathbb{Q}[X]$.

De plus en effectuant la division euclidienne par P_x on trouve.

$\underline{\forall q \in \mathbb{Q}[X] \quad q(x)=0 \iff P_x \mid q \text{ (dans } \mathbb{Q}[X]}$.

Un tel polynôme est donc unique.

Si $\tilde{P}_x$ vérifie la même propriété alors

$$P_x \mid \tilde{P}_x \text{ et } \tilde{P}_x \mid P_x$$

Or P_x et $\tilde{P}_x$ sont unitaires donc $\underline{P_x = \tilde{P}_x}$.

Si P_x possède une racine de multiplicité au moins double dans $\mathbb{C}$ alors $\underline{P\text{gcd}_{\mathbb{C}[X]}(P_x, P'_x) \neq 1}$.

Or le PGCD peut être calculé dans $\mathbb{Q}[X]$ sans sortir de $\mathbb{Q}[X]$ en utilisant la division euclidienne et l'algorithme d'Euclide.

Donc $\underline{P\text{gcd}_{\mathbb{Q}[X]}(P_x, P'_x) \neq 1}$, ce qui contredit l'irréductibilité de P_x.

Conclusion : toutes les racines de P_x (dans $\mathbb{C}$) sont simples.

VI.4) $\boxed{P_x(x_i) = 0}$ et P_x est unitaire, dans $\mathbb{Z}[X]$ et irréductible, donc $\boxed{P_x = P_{x_i}}$ et par conséquent

$$R \in \mathbb{Q}[X] \text{ et } R(x_i) = 0 \Leftrightarrow P_{x_i} \mid R \Leftrightarrow P_x \mid R.$$

VI.5) $\boxed{P_x(X - y_1) \cdots P_x(X - y_m) = \sum_{i=0}^{m \deg(P_x)} c_i X^i = Q(X)}$

où $c_i = c_i(y_1, \ldots, y_m)$ est une fraction polynomiale des y_i, à coefficients dans $\mathbb{Z}$ (fraction des coefficients de P_x).

D'après le résultat de la question V.5)

$$c_i = P_i\left(S_1(y_1, \ldots, y_m), \ldots, S_m(y_1, \ldots, y_m)\right)$$ où P_i est dans $\mathbb{Z}[T_1, \ldots, T_m]$.

Or $S_k(y_1, \ldots, y_m) \in \mathbb{Z}$ puisque y est un entier algébrique. Donc $\boxed{Q \in \mathbb{Z}[X]}$.

Or $Q(x+y) = P_x(x) P_x(x+y-y_2) \cdots = 0$ donc

$\boxed{x+y \text{ est un entier algébrique}}$

VI.6) On emploie la même technique

Si $y=0$ alors $xy=0$ est un entier algébrique.

Si $y\neq 0$ alors $\forall i\ y_i\neq 0$ (Sinon $P_y = P_{y_i} = X$ et $y=0$)

On considère alors :

$$Q = (y_1 \quad y_m)^{\deg(P_x)} P_x\left(\frac{X}{y_1}\right) \quad P_x\left(\frac{X}{y_m}\right) \in \mathbb{Z}[X] \quad (*)$$

unitaire de degré $m\deg(P_x)$

et $Q(xy)=0$

Donc xy est ~~algébrique~~ un entier algébrique.

(*) le coefficient de X^i dans Q est

$$q_i = (y_1 \quad y_m)^{\deg(P_x)} \sum_{i_1+\ +i_m=i} a_{i_1} \quad a_{i_m} \frac{1}{y_1^{i_1}} \quad \frac{1}{y_m^{i_m}}$$

soit

$$\sum_{i_1+\ +i_m=i} a_{i_1} \quad a_{i_m} y_1^{d-i_1} \quad y_m^{d-i_m}$$

qui est bien un polynôme symétrique en les y_i, à coefficients entiers.

De plus $q_{md} = (y_1 \quad y_m)^{d} \frac{1}{y_1^{d}} \quad \frac{1}{y_m^{d}} = 1$

car $i_1+\ +i_m = md$ et $\forall k\ i_k \leq d$ implique $i_1 = \ = i_m = d$ (et $a_{i_1} = \ a_{i_m} = 1$).

VI.7 $\prod_{i=1}^{r} q(x_i) \in \mathbb{Z}$ (car $Q = \prod_{i=1}^{r} q(T_i)$ est symétrique à coefficients entiers donc $Q = Q_1(S_1, \ldots, S_r)$).

De plus $\left|\prod_{i=1}^{r} q(x_i)\right| = \prod_{i=1}^{r} |q(x_i)| \leq \|q\|_I^r < 1$

Donc $\prod_{i=1}^{r} q(x_i) = 0$ Donc $\exists i\ q(x_i)=0$, donc $p_x \mid q$ donc $q(x)=0$

Puis $F(I) \subset J(I)$ (↑ question VI.4).

VI 8) $P = X(X^2-1)(X^2-2)$

P est unitaire et dans $\mathbb{Z}[X]$ et impair.

$\forall x \in [0,1] \quad |P(x)| \leq 2\, x(1-x^2) = 2(x-x^3) \leq 2\,\frac{1}{\sqrt{3}}\left(-\frac{2}{3}\right)$

$\forall x \in [0,1] \quad |P(x)| \leq \frac{4}{3\sqrt{3}}$

$\forall x \in [1,2] \quad |P(x)| \leq 2 \times \sup_{t\in[1,2]} (t-1)(2-t) = 2 \times \frac{1}{4} = \frac{1}{2}$

et $P(2)=0$ et P est croissante sur $[2, \frac{3}{2}]$

$\forall x \in [2, \frac{3}{2}] \quad |P(x)| \leq \frac{3}{2} \times \frac{5}{4} \times \frac{1}{4} < 1$.

Donc $\boxed{\| P \|_{[-\frac{3}{2},\frac{3}{2}]} \leq \max\left(\frac{4}{3\sqrt{3}}, \frac{1}{2}, \frac{15}{32}\right) < 1}$

On a donc $F(I) \subset J(I) \subset Z(P) = \{0, \pm 1, \pm\sqrt{2}\}$.

Or il est clair que $0, \pm 1$ et $\pm\sqrt{2}$ sont des entiers algébriques (racines de X, $X-1$, X^2-2, $X+1$) dont les conjugués sont dans $[-\frac{3}{2}, \frac{3}{2}]$.

Donc $\{-\sqrt{2}, -1, 0, 1, \sqrt{2}\} \subset F(I) \subset J(I) \subset \{-\sqrt{2}, -1, 0, 1, \sqrt{2}\}$.

et Finalement, pour $I = [-\frac{3}{2}, \frac{3}{2}]$

$$\boxed{F(I) = J(I) = \{-\sqrt{2}, -1, 0, 1, \sqrt{2}\}}$$