Réf: Pierre Samuel, théorie algébrique des nombres

Développement: Théorème de d'Alembert-Gauss

Leçons: 125, 144, 141

Théorème: Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.

Preuve: On va montrer que tout $P \in \mathbb{C}[X]$ non constant admet une racine dans $\mathbb{C}$.

1) on se ramène à $P \in \mathbb{R}[X]$

2) récurrence sur n où $\deg P = 2^n q$ (avec q impair)

1) Soit $P \in \mathbb{C}[X]$. Si on pose $F = P\bar{P}$ ($\bar{P}$ a pour coefficients les conjugués des coefficients de P), alors $F \in \mathbb{R}[X]$ (cf rq fin, réc. sur $\deg P$)

Alors si $a \in \mathbb{C}$ est racine de F, si a n'est pas racine de P, a est racine de $\bar{P}$, i.e. $\bar{P}(a) = 0$ donc $\overline{P(\bar{a})} = 0$ donc $P(\bar{a}) = 0$ donc $\bar{a} \in \mathbb{C}$ est racine de P.

On a montré : F admet une racine dans $\mathbb{C} \Rightarrow P$ aussi

2) On suppose ici $P \in \mathbb{R}[X]$ et unitaire (le retour au cas non unitaire est immédiat)

Soit $n \in \mathbb{N}$ et H_n : " $\forall P \in \mathbb{R}[X]$ tel que $\deg P = 2^n q$ avec q impair, P admet une racine dans $\mathbb{C}$ ".

On montre H_n par récurrence sur n.

- si $n=0$ et $\deg P = 2^0 q$, $\deg P$ est impair et donc P admet une racine réelle d'après le TVI ($\lim_{x \to \pm\infty} P(x) = \pm\infty$)

- Soit $n \in \mathbb{N}^*$, supposons H_{n-1} vraie. Soit $P \in \mathbb{R}[X]$ tq $\deg P = 2^n q = d$ ($q \wedge 2 = 1$)

Soit K un corps de décomposition de P sur $\mathbb{C}$. Il existe donc $x_1, \dots, x_d \in K$ tels que $P = \prod_{i=1}^{d} (X - x_i)$ (dans $K[X]$)

Soit $c \in \mathbb{R}$ fixé. $\forall\, 1 \leq i \leq j \leq d$, on pose $y_{ij} = x_i + x_j + c x_i x_j$

$\# \{ y_{ij} \mid 1 \leq i \leq j \leq d \} = \frac{d(d+1)}{2}$ (d choix pour j, et pour chaque choix de j, j choix pour i, on a $\sum_{1}^{d} j = \frac{d(d+1)}{2}$)

$$= 2^{n-1} \underbrace{q(d+1)}_{\text{impair}}$$

Soit $Q = \prod_{1 \leq i \leq j \leq d} (X - y_{ij})$ $\quad \deg Q = 2^{n-1} q(d+1)$

Soit $\tilde{Q}(X, X_1, \dots, X_d) = \prod_{j \geq i} (X - X_i - X_j - c X_i X_j) \in \mathbb{R}[X][X_1, \dots, X_d]$

$\tilde{Q}$ est symétrique en les $(X_i)_{1 \leq i \leq d}$ donc d'après le théorème de Newton, $\exists\, R \in \mathbb{R}[X][X_1, \dots, X_d]$ tel que $\tilde{Q}(X, X_1, \dots, X_d) = R(X, \Sigma_1(X_1, \dots, X_d), \dots, \Sigma_d(X_1, \dots, X_d))$

où les Σ_i sont les polynômes symétriques élémentaires (cf rq)

On on rappelle les relations coefficients racines :

$$\prod_{i=1}^{d}(T-X_i) = T^n + \sum_{i=1}^{n} (-1)^i \Sigma_i(X_1,\dots,X_d)\, T^{n-i}$$

Donc $\forall i \in [\![1,d]\!]$ $\Sigma_i(x_1,\dots,x_d) \in \mathbb{R}$ (coeff du P à ± 1 près)

Donc $Q(X) = \tilde{Q}(X, x_1, \dots, x_d) \in \mathbb{R}[X]$ et $\deg Q = 2^{n-1}\underbrace{q(d-1)}_{\text{impair}}$.

Par HR, $\exists z_c \in \mathbb{C}$ tq $Q(z_c) = 0$

Les racines de Q étant les y_{ij}, l'un d'entre eux est z_c, il est noté

$y_{i(c),j(c)}$.

$|\mathbb{R}| = +\infty$ et $|\{(i,j) \in [\![1,d]\!] \mid i \le j\}| < +\infty$ donc d'après le principe des tiroirs et des chaussettes (cf rq) il existe deux réels $c \neq c'$ tels que $\begin{cases} i(c) = i(c') =: r \\ j(c) = j(c') =: s \end{cases}$

$$\begin{cases} x_r + x_s + c\, x_r x_s = z_c \in \mathbb{C} \\ x_r + x_s + c'\, x_r x_s = z_{c'} \in \mathbb{C} \end{cases}$$

Par combinaisons linéaires, $x_r + x_s \in \mathbb{C}$

$\left(L_1 \leftarrow L_1 - \frac{c}{c'} L_2\right)$ si $c \neq 0$ donne $\underbrace{\left(1 - \frac{c}{c'}\right)}_{\in \mathbb{C}} (x_r + x_s) \in \mathbb{C}$ (si $c' = 0$, clair) et car $c \neq 0$ ($c \neq c'$)

$x_r x_s \in \mathbb{C}$ | $x_r x_s = \underbrace{\frac{1}{c}}_{\in \mathbb{C}} \left(z_c - \underbrace{(x_r + x_s)}_{\in \mathbb{C}}\right)$ si $c \neq 0$ (si $c = 0$, $c' \neq 0$, pris de même))

x_s et x_r sont racines de $X^2 - (x_r + x_s)X + x_r x_s \in \mathbb{C}[X]$

Or tout polynôme de degré 2 dans $\mathbb{C}$ a ses racines dans $\mathbb{C}$ (cf

Comme $K \supset \mathbb{C}$, $x_1, x_0 \in \mathbb{C}$ (c'est ici que sert le fait que K soit corps de décomposition de P sur $\mathbb{C}$) :

P a donc une racine dans $\mathbb{C}$, ce qui prouve l'hérédité, puis le théorème.

Remarques :

- Si $P \in \mathbb{C}[X]$, $P\bar{P} \in \mathbb{R}[X]$: soit $n = \deg P$
  $P = \sum_{i=0}^{n} a_i X^i$
  - $a\bar{a} \in \mathbb{R}_+$
  - $P\bar{P} = (a_n X^n + Q)(\bar{a}_n X^n + \bar{Q})$ $\quad Q = \sum_{i=0}^{n-1} a_i X^i$
    $= \underbrace{a_n \bar{a}_n}_{\in \mathbb{R}} X^{2n} + \underbrace{(a_n \bar{Q} + \bar{a}_n Q)}_{= \overline{\bar{a}_n Q + a_n \bar{Q}}} X^n + \underbrace{Q\bar{Q}}_{\in \mathbb{R}[X] \text{ (HR)}}$
    $\bar{a}_n Q + a_n \bar{Q} \in \mathbb{R}[X]$.

- Dans $A[X_1, \dots, X_n]$ (A anneau commutatif (intègre ?))

$$\sum_k = \sum_{1 \le i_1 < \dots < i_k \le n} X^{i_1} \dots X^{i_k}$$

$$\sum_1 = X_1 + X_2 + \dots + X_n$$

$$\sum_2 = \sum_{1 \le i < j \le n} X_i X_j$$

$$\sum_n = X_1 X_2 \dots X_n$$

(convention : $\sum_0 = 1$)

- principe des tiroirs : si E et F sont deux ensembles finis tq $|E| > |F|$, alors il n'existe pas d'injection de E dans F.

- justification du message en 141 : $\mathbb{C}$ est un corps de rupture important,
- le corps de décomp se trouve avec des corps de ruptures, on trouve $\mathbb{C}$ décomp en Π facts irréd.