

Cours TalENS 2023-2024

Inazuma Eleven, Puzzles, Angles Droits, Glissières

Matthieu Boyer

27 Janvier 2024

Introduction Historique

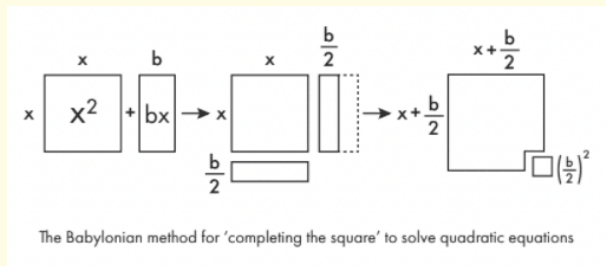


Figure – Source :

<https://bigthink.com/hard-science/quadratic-formula-history/>

Introduction Historique



MS 3048
Table for solving cubic equations, in the Sumerian sexagesimal system.
Babylonia, ca. 19th c. BC

Figure – Source : <https://www.schoyencollection.com/mathematics-collection/9-3-algebra/cubic-equations-table-ms-3048>

Introduction Historique

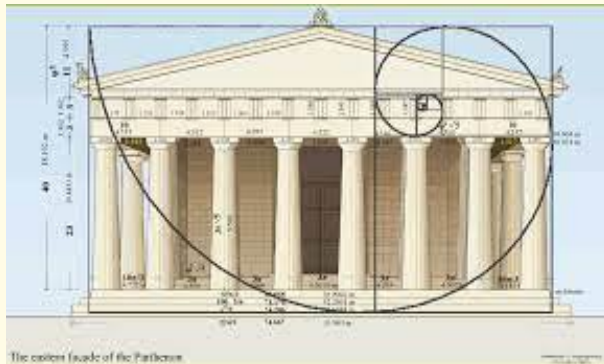


Figure – Source : <https://qph.cf2.quoracdn.net/main-qimg-a210b13c4f479bb2d8a5e4d0f1757688-lq>

Plan

Formalisme !

Polynômes sur un Corps

Equations Polynômiales et Applications

Algorithmes

Résolution des Equations

Le Corps

Définition 2.1: Corps

Un corps est un ensemble muni :

Le Corps

Définition 2.1: Corps

Un corps est un ensemble muni :

- D'une addition avec un neutre 0 notée

$$+ : (x, y) \mapsto x + y$$

Le Corps

Définition 2.1: Corps

Un corps est un ensemble muni :

- ▶ D'une addition avec un neutre 0 notée
 $+ : (x, y) \mapsto x + y$
- ▶ D'une multiplication avec un neutre 1 notée
 $\times : (x, y) \mapsto xy$ distributive sur l'addition

Le Corps

Définition 2.1: Corps

Un corps est un ensemble muni :

- ▶ D'une addition avec un neutre 0 notée
 $+ : (x, y) \mapsto x + y$
- ▶ D'une multiplication avec un neutre 1 notée
 $\times : (x, y) \mapsto xy$ distributive sur l'addition

Pour laquelle tout élément (sauf 0) est inversible pour la multiplication et la loi de produit nul est vérifiée.

Le Corps

Définition 2.1: Corps

Un corps est un ensemble muni :

- ▶ D'une addition avec un neutre 0 notée
 $+ : (x, y) \mapsto x + y$
- ▶ D'une multiplication avec un neutre 1 notée
 $\times : (x, y) \mapsto xy$ distributive sur l'addition

Pour laquelle tout élément (sauf 0) est inversible pour la multiplication et la loi de produit nul est vérifiée.

On notera \mathbb{K} un tel ensemble. \mathbb{R} , \mathbb{Q} , $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ sont des corps.

Polynômes à une Indéterminée

Définition 2.2: Polynôme sur \mathbb{K}

Un polynôme à coefficients dans \mathbb{K} est une suite finie d'éléments de \mathbb{K} .

Polynômes à une Indéterminée

Définition 2.2: Polynôme sur \mathbb{K}

Un polynôme à coefficients dans \mathbb{K} est une suite finie d'éléments de \mathbb{K} .

On les note sous la forme :

$$\sum_{i=0}^d a_i X^i$$

Polynômes à une Indéterminée

Définition 2.2: Polynôme sur \mathbb{K}

Un polynôme à coefficients dans \mathbb{K} est une suite finie d'éléments de \mathbb{K} .

On appelle le symbole X l'indéterminée. Ce n'est pas un nombre.
On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans \mathbb{K} . On appelle d le degré de P .

Calcul sur les Polynômes

Proposition 2.1: Opérations

Si $P = \sum_{i=0}^{d_1} a_i X^i$ et $Q = \sum_{j=0}^{d_2} b_j X^j$ sont deux polynômes :

- ▶ $P + Q = \sum_{i=0}^{\max(d_1, d_2)} (a_i + b_i) X^i$ est un polynôme de degré $\leq \max(\deg P, \deg Q)$.

Calcul sur les Polynômes

Proposition 2.1: Opérations

Si $P = \sum_{i=0}^{d_1} a_i X^i$ et $Q = \sum_{j=0}^{d_2} b_j X^j$ sont deux polynômes :

- ▶ $P + Q = \sum_{i=0}^{\max(d_1, d_2)} (a_i + b_i) X^i$ est un polynôme de degré $\leq \max(\deg P, \deg Q)$.
- ▶ $X^k P = \sum_{i=0}^d a_i X^{i+k}$ est un polynôme.

Calcul sur les Polynômes

Proposition 2.1: Opérations

Si $P = \sum_{i=0}^{d_1} a_i X^i$ et $Q = \sum_{j=0}^{d_2} b_j X^j$ sont deux polynômes :

- ▶ $P + Q = \sum_{i=0}^{\max(d_1, d_2)} (a_i + b_i) X^i$ est un polynôme de degré $\leq \max(\deg P, \deg Q)$.
- ▶ $X^k P = \sum_{i=0}^d a_i X^{i+k}$ est un polynôme.
- ▶ En particulier, PQ est un polynôme de degré $\deg P + \deg Q$ et si $k \in \mathbb{N}$, P^k est un polynôme.

Calcul sur les Polynômes

Définition 2.3: Composition

Pour $\alpha \in \mathbb{K}$, on note $P(\alpha) \in \mathbb{K}$ le nombre : $\sum_{i=0}^{d_1} a_i \alpha^i$. On note de plus $P \circ Q$ le polynôme

$$P \circ Q = \sum_{i=0}^{d_1} a_i Q(X)^i$$

On a $\deg P \circ Q = \deg P \times \deg Q$.

La fonction $\tilde{P} : \alpha \mapsto P(\alpha)$ est continue.

Polynômes à Plusieurs Indéterminées

Définition 2.4: Polynômes à Plusieurs Indéterminées

Un polynôme à $k + 1$ indéterminées est un polynôme à coefficients dans $\mathbb{K}[X_1, \dots, X_k]$

Polynômes à Plusieurs Indéterminées

Définition 2.4: Polynômes à Plusieurs Indéterminées

Un polynôme à $k + 1$ indéterminées est un polynôme à coefficients dans $\mathbb{K}[X_1, \dots, X_k]$

Remarque 2.1: Intégrité

En réalité, $\mathbb{K}[X]$ n'est pas un corps, mais seulement un anneau intègre.

Polynômes à Plusieurs Indéterminées

Définition 2.4: Polynômes à Plusieurs Indéterminées

Un polynôme à $k + 1$ indéterminées est un polynôme à coefficients dans $\mathbb{K}[X_1, \dots, X_k]$

P se met sous la forme

$$P(X) = \sum_{i_1=0}^{d_1} \sum_{i_2=0}^{d_2} \dots \sum_{i_k=0}^{d_k} \alpha_{i_1, \dots, i_k} X_1^{i_1} X_2^{i_2} \dots X_k^{i_k}$$

Plan

Formalisme !

Polynômes sur un Corps

Equations Polynômiales et Applications

Algorithmes

Résolution des Equations

Equation Polynômiale

Définition 2.5: Equation Polynômiale

Une équation polynômiale est une équation de la forme

$$P(x) = \sum_{i=0}^d a_i x^i = b$$

Equation Polynômiale

Définition 2.5: Equation Polynômiale

Une équation polynômiale est une équation de la forme

$$P(x) = \sum_{i=0}^d a_i x^i = b$$

On peut se restreindre au cas $b = 0$ en enlevant b à P .

Equation Polynômiale

Définition 2.5: Equation Polynômiale

Une équation polynômiale est une équation de la forme

$$P(x) = \sum_{i=0}^d a_i x^i = b$$

On peut se restreindre au cas $b = 0$ en enlevant b à P .

On appelle *racines* de l'équation les éléments de $\{\alpha \mid P(\alpha) = b\}$. On dit que $d = \deg P$ est le degré de l'équation.

Equation Polynômiale

Définition 2.5: Equation Polynômiale

Une équation polynômiale est une équation de la forme

$$P(x) = \sum_{i=0}^d a_i x^i = b$$

Pour k indéterminées, on remplace x par un k -uplets
 x_1, \dots, x_k

Solutions à une Équation Polynômiale

Proposition 2.1: Nombres de Solution

Une équation définie par P a au plus $\deg P$ solutions

Solutions à une Équation Polynômiale

Proposition 2.1: Nombres de Solution

Une équation définie par P a au plus $\deg P$ solutions

Théorème 2.1: D'Alembert Gauss

Une équation polynômiale définie par P a toujours exactement $\deg P$ solutions sur un corps algébriquement clos. \mathbb{C} est algébriquement clos.

Applications I

Définition 2.6: Droite

Une droite est un ensemble de la forme $D(a, b) = \{ax + b \mid x \in \mathbb{R}\}$

Applications I

Définition 2.6: Droite

Une droite est un ensemble de la forme $D(a, b) = \{ax + b \mid x \in \mathbb{R}\}$

En particulier, si on a deux droites $D(a, b), D(a', b')$, leur intersection est définie par l'ensemble

$$\{ax + b = a'x + b'\} = \{(a - a')x + (b - b') = 0\}$$

Applications II

Définition 2.7: Cercle

Un cercle est un ensemble de la forme $C((x_0, y_0), r) = \{(x - x_0)^2 + (y - y_0)^2 = r^2\}$

De la même manière que pour les droites, on peut vérifier que les points à l'intersection de deux cercles sont solutions d'une équation polynomiale.

Plan

Formalisme !

Algorithmes

Analyse des Algorithmes

Algorithmes sur les Polynômes

Résolution des Equations

Notion de Complexité

Définition 3.1: Complexité

On appelle complexité en temps d'un algorithme le nombre d'opérations nécessaires à l'effectuer.

La complexité est une notion de vitesse d'un algorithme.

Notion de Complexité

Définition 3.1: Complexité

On appelle complexité en temps d'un algorithme le nombre d'opérations nécessaires à l'effectuer.

La complexité est une notion de vitesse d'un algorithme.

Définition 3.2: Notation de Landau

On dit que $u_n = \mathcal{O}(v_n)$ si il existe c tel que $\frac{u_n}{v_n} \leq c$ pour tout n .

La notation grand \mathcal{O} est une notion de vitesse de croissance.

Quelques Exemples

Proposition 3.1: Croissances Comparées

► On a $\alpha^n = \mathcal{O}(\beta^n)$ si $0 \leq \alpha \leq \beta$

Quelques Exemples

Proposition 3.1: Croissances Comparées

- ▶ On a $\alpha^n = \mathcal{O}(\beta^n)$ si $0 \leq \alpha \leq \beta$
- ▶ On a $n^\alpha = \mathcal{O}(n^\beta)$ si $0 \leq \alpha \leq \beta$

Quelques Exemples

Proposition 3.1: Croissances Comparées

- ▶ On a $\alpha^n = \mathcal{O}(\beta^n)$ si $0 \leq \alpha \leq \beta$
- ▶ On a $n^\alpha = \mathcal{O}(n^\beta)$ si $0 \leq \alpha \leq \beta$
- ▶ A l'inverse $n^\alpha = \mathcal{O}(n^\beta)$ avec $\alpha \leq \beta \leq 0$

Quelques Exemples

Proposition 3.1: Croissances Comparées

- ▶ On a $\alpha^n = \mathcal{O}(n^\beta)$ si $0 \leq \alpha \leq \beta$
- ▶ On a $n^\alpha = \mathcal{O}(n^\beta)$ si $0 \leq \alpha \leq \beta$
- ▶ A l'inverse $n^\alpha = \mathcal{O}(n^\beta)$ avec $\alpha \leq \beta \leq 0$
- ▶ On a $\log n \leq n^\alpha$ si $\alpha > 0$.

Propriétés

Proposition 3.2: Opérations

Si $u_n = \mathcal{O}(v_n)$

Propriétés

Proposition 3.2: Opérations

Si $u_n = \mathcal{O}(v_n)$

► Si $v_n = \mathcal{O}(w_n)$ on a $u_n = \mathcal{O}(w_n)$

Propriétés

Proposition 3.2: Opérations

Si $u_n = \mathcal{O}(v_n)$

- ▶ Si $v_n = \mathcal{O}(w_n)$ on a $u_n = \mathcal{O}(w_n)$
- ▶ $\lambda u_n = \mathcal{O}(v_n) = \mathcal{O}(\lambda v_n)$

Propriétés

Proposition 3.2: Opérations

Si $u_n = \mathcal{O}(v_n)$

- ▶ Si $v_n = \mathcal{O}(w_n)$ on a $u_n = \mathcal{O}(w_n)$
- ▶ $\lambda u_n = \mathcal{O}(v_n) = \mathcal{O}(\lambda v_n)$
- ▶ Si $w_n = \mathcal{O}(z_n)$ on a : $u_n + w_n = \mathcal{O}(v_n + z_n)$.

Propriétés

Proposition 3.2: Opérations

Si $u_n = \mathcal{O}(v_n)$

- ▶ Si $v_n = \mathcal{O}(w_n)$ on a $u_n = \mathcal{O}(w_n)$
- ▶ $\lambda u_n = \mathcal{O}(v_n) = \mathcal{O}(\lambda v_n)$
- ▶ Si $w_n = \mathcal{O}(z_n)$ on a : $u_n + w_n = \mathcal{O}(v_n + z_n)$.
- ▶ $u_n = \mathcal{O}(u_n)$.

Plan

Formalisme !

Algorithmes

Analyse des Algorithmes

Algorithmes sur les Polynômes

Résolution des Equations

Algorithmes Simples

Algorithme

Analyse

Input $P = (a_0, \dots, a_n),$

$Q = (b_i, \dots, b_n)$

Calculer les puissances de x jusqu'à n

Calculer $a_i x^i$

return Somme des résultats

On effectue n additions, on a une complexité en $\mathcal{O}(n)$.

Algorithmes Simples

Algorithme

Analyse

Input $P = (a_0, \dots, a_n)$

$Q = (b_i, \dots, b_n)$

Calculer les puissances de x jusqu'à n

Calculer $a_i x^i$

return Somme des résultats

On effectue n produits par puissance, donc a une complexité en $\mathcal{O}(n^2)$

Algorithmes Simples

Algorithme	Analyse
Input $P = (a_0, \dots, a_n)$ $Q = (b_i, \dots, b_n)$ Calculer les puissances de x jusqu'à n Calculer $a_i x^i$ return Somme des résultats	On effectue n produits par puissance, donc a une complexité en $\mathcal{O}(n^2)$

En réalité, il existe un algorithme plus efficace pour calculer un produit de polynômes, appelé Fast Fourier Transform, et celui-ci fonctionne en $\mathcal{O}(n \log n)$.

Evaluation Naïve

Algorithme

Input $P = (a_0, \dots, a_n), x$

Calculer les puissances de x jusqu'à n

Calculer $a_i x^i$

return Somme des résultats

Analyse

De manière naïve, on calcule x^i en temps $\mathcal{O}(i)$. On a alors une complexité en $\mathcal{O}(n^2)$.

Evaluation Naïve

Algorithme

Analyse

Input $P = (a_0, \dots, a_n), x$

Calculer les puissances de x jusqu'à n

Calculer $a_i x^i$

return Somme des résultats

Sans rentrer dans les détails, on peut calculer x^i en temps $\log(i)$. On fait donc un nombre d'opérations en $\mathcal{O}(n \log n)$.

Algorithme de Horner

Proposition 3.3: Evaluation Rapide de Horner

$$P(X) = \sum_{k=0}^n a_k X^k = (((a_n \times X + a_{n-1}) \\ \times X + a_{n-2}) \\ \dots + a_1) \times X + a_0$$

Algorithme de Horner

Proposition 3.3: Evaluation Rapide de Horner

$$P(X) = \sum_{k=0}^n a_k X^k = (((a_n \times X + a_{n-1}) \\ \times X + a_{n-2}) \\ \dots + a_1) \times X + a_0$$

De ceci, on déduit un algorithme d'évaluation des polynômes en n multiplications et n additions !

Plan

Formalisme !

Algorithmes

Résolution des Equations

Formellement

Méthodes de Résolution Graphique

Degrés 1 et 2

Théorème 4.1: Solution des Equations Affines

L'unique solution de $ax + b = c$ avec $a \neq 0$ est $x = \frac{c-b}{a}$

Degrés 1 et 2

Théorème 4.1: Solution des Equations Affines

L'unique solution de $ax + b = c$ avec $a \neq 0$ est $x = \frac{c-b}{a}$

Théorème 4.2: Solution des Equations Quadratiques

Les deux solutions de $ax^2 + bx + c = d$ avec $a \neq 0$ sont :

$$x_+ = \frac{-b + \sqrt{b^2 - 4a(c-d)}}{2a} \text{ et } x_- = \frac{-b - \sqrt{b^2 - 4a(c-d)}}{2a}$$

Celles-ci ne sont réelles que si $\sqrt{b^2 - 4a(c-d)} \geq 0$ et sont égales s'il y a égalité. Sinon, elles sont complexes conjuguées.

Degrés 3, 4 et plus

Théorème 4.3: Solutions des Cubiques et Quartiques

Il existe des formules pour les solutions des équations de la forme $ax^3 + bx^2 + cx + d = e$ et $ax^4 + bx^3 + cx^2 + dx + e = f$ où $a \neq 0$. Ces racines ne sont pas toujours réelles, mais une équation de degré trois a toujours une racine réelle.

Degrés 3, 4 et plus

Théorème 4.3: Solutions des Cubiques et Quartiques

Il existe des formules pour les solutions des équations de la forme $ax^3 + bx^2 + cx + d = e$ et $ax^4 + bx^3 + cx^2 + dx + e = f$ où $a \neq 0$. Ces racines ne sont pas toujours réelles, mais une équation de degré trois a toujours une racine réelle.

Théorème 4.4: Klein Vierergruppe

Il ne peut pas exister de formule pour les solutions des équations polynômiales de degré ≥ 5 .

Plan

Formalisme !

Algorithmes

Résolution des Equations

Formellement

Méthodes de Résolution Graphique

Théorème des Valeurs Intermédiaires

Théorème 4.5: des Valeurs Intermédiaires

- Formulation Réelle : Si f est continue sur un intervalle, son image est un intervalle.

Théorème des Valeurs Intermédiaires

Théorème 4.5: des Valeurs Intermédiaires

- ▶ Formulation Réelle : Si f est continue sur un intervalle, son image est un intervalle.
- ▶ Formulation Générale : Si f est continue sur le connexe par arcs X , son image est connexe par arcs.

Théorème des Valeurs Intermédiaires

Théorème 4.5: des Valeurs Intermédiaires

- Formulation Réelle : Si f est continue sur un intervalle, son image est un intervalle.
- Formulation Générale : Si f est continue sur le connexe par arcs X , son image est connexe par arcs.

En pratique cela signifie que si :

$$f(a) = c, f(b) = d \text{ alors } \forall y \in [c, d], \exists x, f(x) = y$$

Méthode de Newton-Raphson

Théorème 4.6: Caractérisation de Carathéodory

Une fonction est dérivable en x_0 si et seulement si il existe un nombre noté $f'(x_0)$ tel que, au voisinage de x_0 :

$$f(x) = f(x_0) + f'(x_0)(x - x_0)$$

Méthode de Newton-Raphson

Théorème 4.6: Caractérisation de Carathéodory

Une fonction est dérivable en x_0 si et seulement si il existe un nombre noté $f'(x_0)$ tel que, au voisinage de x_0 :

$$f(x) = f(x_0) + f'(x)(x - x_0)$$

En particulier, les polynômes sont dérivables, donc si on cherche une racine x_0 , on peut, en suivant la pente, trouver une racine.

Méthode de Newton-Raphson

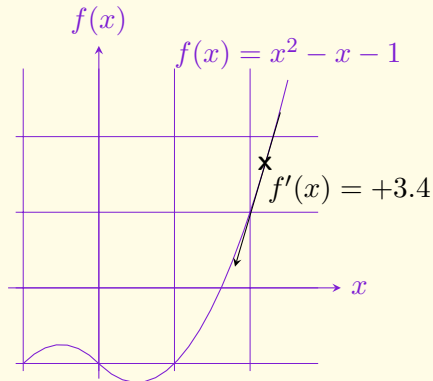
Théorème 4.6: Caractérisation de Carathéodory

Une fonction est dérivable en x_0 si et seulement si il existe un nombre noté $f'(x_0)$ tel que, au voisinage de x_0 :

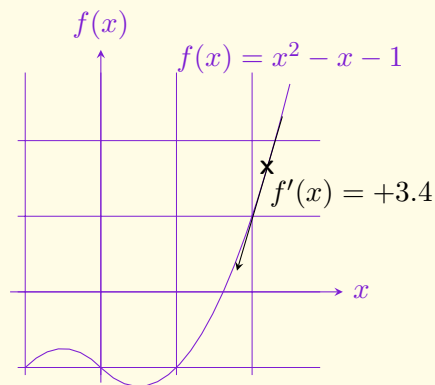
$$f(x) = f(x_0) + f'(x)(x - x_0)$$

En particulier, les polynômes sont dérivables, donc si on cherche une racine x_0 , on peut, en suivant la pente, trouver une racine. Si $f(x) > 0$ et on va selon x croissant si $f'(x) < 0$ sinon x décroissant et à l'inverse sinon.

Méthode de Newton-Raphson Graphique



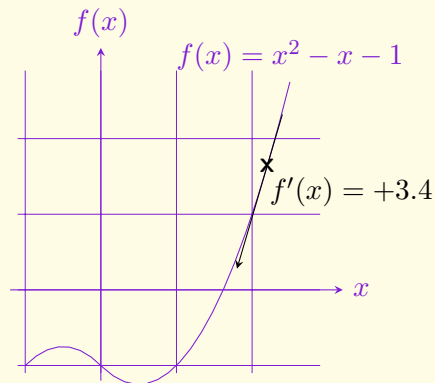
Méthode de Newton-Raphson Graphique



On vérifie bien qu'on va trouver une racine en

$$\varphi = \frac{1 + \sqrt{5}}{2}$$

Méthode de Newton-Raphson Graphique



On vérifie bien qu'on va trouver une racine en

$$\varphi = \frac{1 + \sqrt{5}}{2}$$

Il y en a une autre en

$$\bar{\varphi} = \frac{1 - \sqrt{5}}{2}$$

Toutefois, cette méthode graphique nécessite de savoir tracer une fonction polynômiale.

Orthogone de Lill