

Un retour aux racines

Le théorème fondamental de l'algèbre rendu effectif :
une preuve algébrique réelle par des suites de Sturm

Michael Eisermann

Institut Fourier, Université Grenoble



Carl Friedrich Gauss (1777–1855)

Séminaire des Magistères
Jeudi 2 octobre 2008



Augustin Louis Cauchy (1789–1857)



Charles-François Sturm (1803–1855)

- 1 Les trois types de preuve du théorème fondamental
- 2 Racines réelles d'un polynôme réel
- 3 Racines complexes d'un polynôme complexe
- 4 Aspects algorithmiques

Théorème

Tout polynôme complexe de degré n admet n racines complexes.

Théorème

Tout polynôme complexe de degré n admet n racines complexes.

Plus précisément : Soit \mathbb{R} le corps des nombres réels,
et soit $\mathbb{C} = \mathbb{R}[i]$ où $i^2 = -1$ le corps des nombres complexes.

Théorème

Tout polynôme complexe de degré n admet n racines complexes.

Plus précisément : Soit \mathbb{R} le corps des nombres réels,
et soit $\mathbb{C} = \mathbb{R}[i]$ où $i^2 = -1$ le corps des nombres complexes.

Théorème

Pour tout polynôme

$$F = a_n Z^n + a_{n-1} Z^{n-1} + \cdots + a_1 Z + a_0$$

*à coefficients complexes $a_0, a_1, \dots, a_{n-1}, a_n \in \mathbb{C}$ vérifiant $a_n \neq 0$
il existe $z_1, z_2, \dots, z_n \in \mathbb{C}$ telles que*

$$F = a_n (Z - z_1)(Z - z_2) \cdots (Z - z_n).$$

Théorème

Tout polynôme complexe de degré n admet n racines complexes.

Plus précisément : Soit \mathbb{R} le corps des nombres réels,
et soit $\mathbb{C} = \mathbb{R}[i]$ où $i^2 = -1$ le corps des nombres complexes.

Théorème

Pour tout polynôme

$$F = a_n Z^n + a_{n-1} Z^{n-1} + \cdots + a_1 Z + a_0$$

*à coefficients complexes $a_0, a_1, \dots, a_{n-1}, a_n \in \mathbb{C}$ vérifiant $a_n \neq 0$
il existe $z_1, z_2, \dots, z_n \in \mathbb{C}$ telles que*

$$F = a_n (Z - z_1)(Z - z_2) \cdots (Z - z_n).$$

Questions :

Théorème

Tout polynôme complexe de degré n admet n racines complexes.

Plus précisément : Soit \mathbb{R} le corps des nombres réels, et soit $\mathbb{C} = \mathbb{R}[i]$ où $i^2 = -1$ le corps des nombres complexes.

Théorème

Pour tout polynôme

$$F = a_n Z^n + a_{n-1} Z^{n-1} + \cdots + a_1 Z + a_0$$

à coefficients complexes $a_0, a_1, \dots, a_{n-1}, a_n \in \mathbb{C}$ vérifiant $a_n \neq 0$ il existe $z_1, z_2, \dots, z_n \in \mathbb{C}$ telles que

$$F = a_n (Z - z_1)(Z - z_2) \cdots (Z - z_n).$$

Questions :

- L'énoncé serait faux sur \mathbb{Q} . Pourquoi est-il vrai sur \mathbb{R} ?

Théorème

Tout polynôme complexe de degré n admet n racines complexes.

Plus précisément : Soit \mathbb{R} le corps des nombres réels, et soit $\mathbb{C} = \mathbb{R}[i]$ où $i^2 = -1$ le corps des nombres complexes.

Théorème

Pour tout polynôme

$$F = a_n Z^n + a_{n-1} Z^{n-1} + \cdots + a_1 Z + a_0$$

à coefficients complexes $a_0, a_1, \dots, a_{n-1}, a_n \in \mathbb{C}$ vérifiant $a_n \neq 0$ il existe $z_1, z_2, \dots, z_n \in \mathbb{C}$ telles que

$$F = a_n (Z - z_1)(Z - z_2) \cdots (Z - z_n).$$

Questions :

- L'énoncé serait faux sur \mathbb{Q} . Pourquoi est-il vrai sur \mathbb{R} ?
- Quels outils sont utilisés dans les diverses démonstrations ?

Théorème

Tout polynôme complexe de degré n admet n racines complexes.

Plus précisément : Soit \mathbb{R} le corps des nombres réels, et soit $\mathbb{C} = \mathbb{R}[i]$ où $i^2 = -1$ le corps des nombres complexes.

Théorème

Pour tout polynôme

$$F = a_n Z^n + a_{n-1} Z^{n-1} + \cdots + a_1 Z + a_0$$

à coefficients complexes $a_0, a_1, \dots, a_{n-1}, a_n \in \mathbb{C}$ vérifiant $a_n \neq 0$ il existe $z_1, z_2, \dots, z_n \in \mathbb{C}$ telles que

$$F = a_n (Z - z_1)(Z - z_2) \cdots (Z - z_n).$$

Questions :

- L'énoncé serait faux sur \mathbb{Q} . Pourquoi est-il vrai sur \mathbb{R} ?
- Quels outils sont utilisés dans les diverses démonstrations ?
- Pour quels corps ordonnés l'énoncé est-il vrai ?

Théorème

Tout polynôme complexe de degré n admet n racines complexes.

Plus précisément : Soit \mathbb{R} le corps des nombres réels, et soit $\mathbb{C} = \mathbb{R}[i]$ où $i^2 = -1$ le corps des nombres complexes.

Théorème

Pour tout polynôme

$$F = a_n Z^n + a_{n-1} Z^{n-1} + \cdots + a_1 Z + a_0$$

à coefficients complexes $a_0, a_1, \dots, a_{n-1}, a_n \in \mathbb{C}$ vérifiant $a_n \neq 0$ il existe $z_1, z_2, \dots, z_n \in \mathbb{C}$ telles que

$$F = a_n (Z - z_1)(Z - z_2) \cdots (Z - z_n).$$

Questions :

- L'énoncé serait faux sur \mathbb{Q} . Pourquoi est-il vrai sur \mathbb{R} ?
- Quels outils sont utilisés dans les diverses démonstrations ?
- Pour quels corps ordonnés l'énoncé est-il vrai ?
- Peut-on améliorer l'énoncé ? le rendre effectif ?

Quelques protagonistes

Scipione del Ferro (1456-1526)

Niccolò Fontana Tartaglia (1500-1557)

Gerolamo Cardano (1501-1576)

Lodovico Ferrari (1522-1565)

Quelques protagonistes

Scipione del Ferro (1456-1526)

Niccolò Fontana Tartaglia (1500-1557)

Gerolamo Cardano (1501-1576)

Lodovico Ferrari (1522-1565)

Niels Henrik Abel (1802-1829)

Évariste Galois (1811-1832)

Quelques protagonistes

Scipione del Ferro (1456-1526)

Niccolò Fontana Tartaglia (1500-1557)

Gerolamo Cardano (1501-1576)

Lodovico Ferrari (1522-1565)

Niels Henrik Abel (1802-1829)

Évariste Galois (1811-1832)

Albert Girard (1595-1632)

René Descartes (1596-1650)

Gottfried Leibniz (1646-1716)

Quelques protagonistes

Scipione del Ferro (1456-1526)

Niccolò Fontana Tartaglia (1500-1557)

Gerolamo Cardano (1501-1576)

Lodovico Ferrari (1522-1565)

Niels Henrik Abel (1802-1829)

Évariste Galois (1811-1832)

Albert Girard (1595-1632)

René Descartes (1596-1650)

Gottfried Leibniz (1646-1716)

Leonhard Euler (1707-1783)

Jean le Rond d'Alembert (1717-1783)

Joseph-Louis Lagrange (1736-1813)

Pierre-Simon Laplace (1749-1827)

Quelques protagonistes

Scipione del Ferro (1456-1526)

Niccolò Fontana Tartaglia (1500-1557)

Gerolamo Cardano (1501-1576)

Lodovico Ferrari (1522-1565)

Niels Henrik Abel (1802-1829)

Évariste Galois (1811-1832)

Albert Girard (1595-1632)

René Descartes (1596-1650)

Gottfried Leibniz (1646-1716)

Leonhard Euler (1707-1783)

Jean le Rond d'Alembert (1717-1783)

Joseph-Louis Lagrange (1736-1813)

Pierre-Simon Laplace (1749-1827)

Carl Friedrich Gauss (1777-1855)

Quelques protagonistes

Scipione del Ferro (1456-1526)
Niccolò Fontana Tartaglia (1500-1557)
Gerolamo Cardano (1501-1576)
Lodovico Ferrari (1522-1565)

Niels Henrik Abel (1802-1829)
Évariste Galois (1811-1832)

Albert Girard (1595-1632)
René Descartes (1596-1650)
Gottfried Leibniz (1646-1716)

Leonhard Euler (1707-1783)
Jean le Rond d'Alembert (1717-1783)
Joseph-Louis Lagrange (1736-1813)
Pierre-Simon Laplace (1749-1827)

Carl Friedrich Gauss (1777-1855)

Augustin Louis Cauchy (1789–1857)
Charles-François Sturm (1803–1855)

Tourisme mathématique



Quelques protagonistes

Scipione del Ferro (1456-1526)
Niccolò Fontana Tartaglia (1500-1557)
Gerolamo Cardano (1501-1576)
Lodovico Ferrari (1522-1565)

Niels Henrik Abel (1802-1829)
Évariste Galois (1811-1832)

Albert Girard (1595-1632)
René Descartes (1596-1650)
Gottfried Leibniz (1646-1716)

Leonhard Euler (1707-1783)
Jean le Rond d'Alembert (1717-1783)
Joseph-Louis Lagrange (1736-1813)
Pierre-Simon Laplace (1749-1827)

Carl Friedrich Gauss (1777-1855)

Augustin Louis Cauchy (1789–1857)
Charles-François Sturm (1803–1855)

Tourisme mathématique



- 1** Les trois types de preuve du théorème fondamental
 - Analyse : la preuve de Cauchy–Argand
 - Algèbre : la preuve de Laplace–Gauss
 - Topologie algébrique : la notion de l'indice
- 2 Racines réelles d'un polynôme réel
- 3 Racines complexes d'un polynôme complexe
- 4 Aspects algorithmiques

Les trois types de preuve du théorème fondamental

On connaît essentiellement trois types de démonstration :

Les trois types de preuve du théorème fondamental

On connaît essentiellement trois types de démonstration :

- 1 analyse : compacité, exponentielle, intégration, Stokes, ...

Les trois types de preuve du théorème fondamental

On connaît essentiellement trois types de démonstration :

- 1 analyse : compacité, exponentielle, intégration, Stokes, ...
- 2 algèbre : théorie de Galois / fonctions symétriques, valeurs intermédiaires

Les trois types de preuve du théorème fondamental

On connaît essentiellement trois types de démonstration :

- 1 analyse : compacité, exponentielle, intégration, Stokes, ...
- 2 algèbre : théorie de Galois / fonctions symétriques, valeurs intermédiaires
- 3 topologie algébrique : degré d'un lacet $\gamma: \mathbb{S}^1 \rightarrow \mathbb{C} \setminus \{0\}$

Les trois types de preuve du théorème fondamental

On connaît essentiellement trois types de démonstration :

- 1 analyse : compacité, exponentielle, intégration, Stokes, ...
- 2 algèbre : théorie de Galois / fonctions symétriques, valeurs intermédiaires
- 3 topologie algébrique : degré d'un lacet $\gamma: \mathbb{S}^1 \rightarrow \mathbb{C} \setminus \{0\}$

La preuve que je présenterai ici est du dernier type mais *réelle algébrique*.

Les trois types de preuve du théorème fondamental

On connaît essentiellement trois types de démonstration :

- 1 analyse : compacité, exponentielle, intégration, Stokes, ...
- 2 algèbre : théorie de Galois / fonctions symétriques, valeurs intermédiaires
- 3 topologie algébrique : degré d'un lacet $\gamma: \mathbb{S}^1 \rightarrow \mathbb{C} \setminus \{0\}$

La preuve que je présenterai ici est du dernier type mais *réelle algébrique*. Elle n'est pas la plus courte mais elle offre de nombreux avantages :

Les trois types de preuve du théorème fondamental

On connaît essentiellement trois types de démonstration :

- 1 analyse : compacité, exponentielle, intégration, Stokes, ...
- 2 algèbre : théorie de Galois / fonctions symétriques, valeurs intermédiaires
- 3 topologie algébrique : degré d'un lacet $\gamma: \mathbb{S}^1 \rightarrow \mathbb{C} \setminus \{0\}$

La preuve que je présenterai ici est du dernier type mais *réelle algébrique*. Elle n'est pas la plus courte mais elle offre de nombreux avantages :

- La démonstration est élémentaire.
 - Arithmétique des polynômes réels à une variable,
 - Le théorème de valeurs intermédiaires.

Les trois types de preuve du théorème fondamental

On connaît essentiellement trois types de démonstration :

- 1 analyse : compacité, exponentielle, intégration, Stokes, ...
- 2 algèbre : théorie de Galois / fonctions symétriques, valeurs intermédiaires
- 3 topologie algébrique : degré d'un lacet $\gamma: \mathbb{S}^1 \rightarrow \mathbb{C} \setminus \{0\}$

La preuve que je présenterai ici est du dernier type mais *réelle algébrique*. Elle n'est pas la plus courte mais elle offre de nombreux avantages :

- La démonstration est élémentaire.
 - Arithmétique des polynômes réels à une variable,
 - Le théorème de valeurs intermédiaires.
- Ainsi tous les arguments sont valables sur un corps réel clos.

Les trois types de preuve du théorème fondamental

On connaît essentiellement trois types de démonstration :

- 1 analyse : compacité, exponentielle, intégration, Stokes, ...
- 2 algèbre : théorie de Galois / fonctions symétriques, valeurs intermédiaires
- 3 topologie algébrique : degré d'un lacet $\gamma: \mathbb{S}^1 \rightarrow \mathbb{C} \setminus \{0\}$

La preuve que je présenterai ici est du dernier type mais *réelle algébrique*. Elle n'est pas la plus courte mais elle offre de nombreux avantages :

- La démonstration est élémentaire.
 - Arithmétique des polynômes réels à une variable,
 - Le théorème de valeurs intermédiaires.
- Ainsi tous les arguments sont valables sur un corps réel clos.
- La preuve est constructive : elle permet de localiser les racines.

Les trois types de preuve du théorème fondamental

On connaît essentiellement trois types de démonstration :

- 1 analyse : compacité, exponentielle, intégration, Stokes, ...
- 2 algèbre : théorie de Galois / fonctions symétriques, valeurs intermédiaires
- 3 topologie algébrique : degré d'un lacet $\gamma: \mathbb{S}^1 \rightarrow \mathbb{C} \setminus \{0\}$

La preuve que je présenterai ici est du dernier type mais *réelle algébrique*. Elle n'est pas la plus courte mais elle offre de nombreux avantages :

- La démonstration est élémentaire.
 - Arithmétique des polynômes réels à une variable,
 - Le théorème de valeurs intermédiaires.
- Ainsi tous les arguments sont valables sur un corps réel clos.
- La preuve est constructive : elle permet de localiser les racines.
- L'algorithme est relativement facile à implémenter sur ordinateur.

Les trois types de preuve du théorème fondamental

On connaît essentiellement trois types de démonstration :

- 1 analyse : compacité, exponentielle, intégration, Stokes, ...
- 2 algèbre : théorie de Galois / fonctions symétriques, valeurs intermédiaires
- 3 topologie algébrique : degré d'un lacet $\gamma: \mathbb{S}^1 \rightarrow \mathbb{C} \setminus \{0\}$

La preuve que je présenterai ici est du dernier type mais *réelle algébrique*. Elle n'est pas la plus courte mais elle offre de nombreux avantages :

- La démonstration est élémentaire.
 - Arithmétique des polynômes réels à une variable,
 - Le théorème de valeurs intermédiaires.
- Ainsi tous les arguments sont valables sur un corps réel clos.
- La preuve est constructive : elle permet de localiser les racines.
- L'algorithme est relativement facile à implémenter sur ordinateur.
- La démarche mène à une preuve formelle du théorème.

Les trois types de preuve du théorème fondamental

On connaît essentiellement trois types de démonstration :

- 1 analyse : compacité, exponentielle, intégration, Stokes, ...
- 2 algèbre : théorie de Galois / fonctions symétriques, valeurs intermédiaires
- 3 topologie algébrique : degré d'un lacet $\gamma: \mathbb{S}^1 \rightarrow \mathbb{C} \setminus \{0\}$

La preuve que je présenterai ici est du dernier type mais *réelle algébrique*. Elle n'est pas la plus courte mais elle offre de nombreux avantages :

- La démonstration est élémentaire.
 - Arithmétique des polynômes réels à une variable,
 - Le théorème de valeurs intermédiaires.
- Ainsi tous les arguments sont valables sur un corps réel clos.
- La preuve est constructive : elle permet de localiser les racines.
- L'algorithme est relativement facile à implémenter sur ordinateur.
- La démarche mène à une preuve formelle du théorème.
- Parallèlement elle fournit une preuve formelle de l'implémentation.

La preuve par la topologie algébrique : outils utilisés

On note $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ le cercle unité dans \mathbb{C} .

La preuve par la topologie algébrique : outils utilisés

On note $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ le cercle unité dans \mathbb{C} .

Un lacet dans $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ est une application continue $\gamma: S^1 \rightarrow \mathbb{C}^*$.

La preuve par la topologie algébrique : outils utilisés

On note $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ le cercle unité dans \mathbb{C} .

Un lacet dans $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ est une application continue $\gamma: S^1 \rightarrow \mathbb{C}^*$.

Outil utilisé : Il existe une fonction $\text{ind}: \{\text{lacets dans } \mathbb{C}^*\} \rightarrow \mathbb{Z}$ qui compte le nombre de tours autour de 0.

La preuve par la topologie algébrique : outils utilisés

On note $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ le cercle unité dans \mathbb{C} .

Un lacet dans $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ est une application continue $\gamma: S^1 \rightarrow \mathbb{C}^*$.

Outil utilisé : Il existe une fonction $\text{ind}: \{\text{lacets dans } \mathbb{C}^*\} \rightarrow \mathbb{Z}$ qui compte le nombre de tours autour de 0. Plus précisément :

La preuve par la topologie algébrique : outils utilisés

On note $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ le cercle unité dans \mathbb{C} .

Un lacet dans $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ est une application continue $\gamma: S^1 \rightarrow \mathbb{C}^*$.

Outil utilisé : Il existe une fonction $\text{ind}: \{\text{lacets dans } \mathbb{C}^*\} \rightarrow \mathbb{Z}$ qui compte le nombre de tours autour de 0. Plus précisément :

1 $\text{ind}(\text{id}) = 1$.

La preuve par la topologie algébrique : outils utilisés

On note $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ le cercle unité dans \mathbb{C} .

Un lacet dans $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ est une application continue $\gamma: S^1 \rightarrow \mathbb{C}^*$.

Outil utilisé : Il existe une fonction $\text{ind}: \{\text{lacets dans } \mathbb{C}^*\} \rightarrow \mathbb{Z}$ qui compte le nombre de tours autour de 0. Plus précisément :

1 $\text{ind}(\text{id}) = 1.$

2 $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2).$

La preuve par la topologie algébrique : outils utilisés

On note $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ le cercle unité dans \mathbb{C} .

Un lacet dans $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ est une application continue $\gamma: S^1 \rightarrow \mathbb{C}^*$.

Outil utilisé : Il existe une fonction $\text{ind}: \{\text{lacets dans } \mathbb{C}^*\} \rightarrow \mathbb{Z}$ qui compte le nombre de tours autour de 0. Plus précisément :

- 1 $\text{ind}(\text{id}) = 1$.
- 2 $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.
- 3 $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ sont homotopes dans \mathbb{C}^* .

La preuve par la topologie algébrique : outils utilisés

On note $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ le cercle unité dans \mathbb{C} .

Un lacet dans $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ est une application continue $\gamma: S^1 \rightarrow \mathbb{C}^*$.

Outil utilisé : Il existe une fonction $\text{ind}: \{\text{lacets dans } \mathbb{C}^*\} \rightarrow \mathbb{Z}$ qui compte le nombre de tours autour de 0. Plus précisément :

- 1 $\text{ind}(\text{id}) = 1$.
- 2 $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.
- 3 $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ sont homotopes dans \mathbb{C}^* .

La difficulté est de démontrer l'existence d'une telle application ind !
Il faut d'abord la construire puis établir toutes les propriétés requises.

La preuve par la topologie algébrique : outils utilisés

On note $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ le cercle unité dans \mathbb{C} .

Un lacet dans $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ est une application continue $\gamma: S^1 \rightarrow \mathbb{C}^*$.

Outil utilisé : Il existe une fonction $\text{ind}: \{\text{lacets dans } \mathbb{C}^*\} \rightarrow \mathbb{Z}$ qui compte le nombre de tours autour de 0. Plus précisément :

1 $\text{ind}(\text{id}) = 1.$

2 $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2).$

3 $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ sont homotopes dans \mathbb{C}^* .

La difficulté est de démontrer l'existence d'une telle application ind !
Il faut d'abord la construire puis établir toutes les propriétés requises.

Pour réaliser cette construction, tous les moyens sont bons :

La preuve par la topologie algébrique : outils utilisés

On note $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ le cercle unité dans \mathbb{C} .

Un lacet dans $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ est une application continue $\gamma: S^1 \rightarrow \mathbb{C}^*$.

Outil utilisé : Il existe une fonction $\text{ind}: \{\text{lacets dans } \mathbb{C}^*\} \rightarrow \mathbb{Z}$ qui compte le nombre de tours autour de 0. Plus précisément :

- 1 $\text{ind}(\text{id}) = 1$.
- 2 $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.
- 3 $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ sont homotopes dans \mathbb{C}^* .

La difficulté est de démontrer l'existence d'une telle application ind !
Il faut d'abord la construire puis établir toutes les propriétés requises.

Pour réaliser cette construction, tous les moyens sont bons :

- Théorie des revêtements, appliquée à $\exp: \mathbb{C} \rightarrow \mathbb{C}^*$.

La preuve par la topologie algébrique : outils utilisés

On note $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ le cercle unité dans \mathbb{C} .

Un lacet dans $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ est une application continue $\gamma: S^1 \rightarrow \mathbb{C}^*$.

Outil utilisé : Il existe une fonction $\text{ind}: \{\text{lacets dans } \mathbb{C}^*\} \rightarrow \mathbb{Z}$ qui compte le nombre de tours autour de 0. Plus précisément :

- 1 $\text{ind}(\text{id}) = 1$.
- 2 $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.
- 3 $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ sont homotopes dans \mathbb{C}^* .

La difficulté est de démontrer l'existence d'une telle application ind !
Il faut d'abord la construire puis établir toutes les propriétés requises.

Pour réaliser cette construction, tous les moyens sont bons :

- Théorie des revêtements, appliquée à $\exp: \mathbb{C} \rightarrow \mathbb{C}^*$.
- Groupe fondamental $\text{ind}: \pi_1(\mathbb{C}^*, 1) \xrightarrow{\sim} \mathbb{Z}$ via Seifert–van Kampen.

La preuve par la topologie algébrique : outils utilisés

On note $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ le cercle unité dans \mathbb{C} .

Un lacet dans $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ est une application continue $\gamma: S^1 \rightarrow \mathbb{C}^*$.

Outil utilisé : Il existe une fonction $\text{ind}: \{\text{lacets dans } \mathbb{C}^*\} \rightarrow \mathbb{Z}$ qui compte le nombre de tours autour de 0. Plus précisément :

- 1 $\text{ind}(\text{id}) = 1$.
- 2 $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.
- 3 $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ sont homotopes dans \mathbb{C}^* .

La difficulté est de démontrer l'existence d'une telle application ind !
Il faut d'abord la construire puis établir toutes les propriétés requises.

Pour réaliser cette construction, tous les moyens sont bons :

- Théorie des revêtements, appliquée à $\exp: \mathbb{C} \rightarrow \mathbb{C}^*$.
- Groupe fondamental $\text{ind}: \pi_1(\mathbb{C}^*, 1) \xrightarrow{\sim} \mathbb{Z}$ via Seifert–van Kampen.
- Homologie $\text{ind}: H_1(\mathbb{C}^*) \xrightarrow{\sim} \mathbb{Z}$ via les axiomes d'Eilenberg–Steenrod.

La preuve par la topologie algébrique : outils utilisés

On note $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ le cercle unité dans \mathbb{C} .

Un lacet dans $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ est une application continue $\gamma: S^1 \rightarrow \mathbb{C}^*$.

Outil utilisé : Il existe une fonction $\text{ind}: \{\text{lacets dans } \mathbb{C}^*\} \rightarrow \mathbb{Z}$ qui compte le nombre de tours autour de 0. Plus précisément :

- 1 $\text{ind}(\text{id}) = 1$.
- 2 $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.
- 3 $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ sont homotopes dans \mathbb{C}^* .

La difficulté est de démontrer l'existence d'une telle application ind !
Il faut d'abord la construire puis établir toutes les propriétés requises.

Pour réaliser cette construction, tous les moyens sont bons :

- Théorie des revêtements, appliquée à $\exp: \mathbb{C} \rightarrow \mathbb{C}^*$.
- Groupe fondamental $\text{ind}: \pi_1(\mathbb{C}^*, 1) \xrightarrow{\sim} \mathbb{Z}$ via Seifert–van Kampen.
- Homologie $\text{ind}: H_1(\mathbb{C}^*) \xrightarrow{\sim} \mathbb{Z}$ via les axiomes d'Eilenberg–Steenrod.
- Analyse complexe, indice analytique $\text{ind}(\gamma) = \frac{1}{2i\pi} \int_{\gamma} \frac{dz}{z}$.

La preuve par la topologie algébrique : outils utilisés

On note $\mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ le cercle unité dans \mathbb{C} .

Un lacet dans $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ est une application continue $\gamma: \mathbb{S}^1 \rightarrow \mathbb{C}^*$.

Outil utilisé : Il existe une fonction $\text{ind}: \{\text{lacets dans } \mathbb{C}^*\} \rightarrow \mathbb{Z}$ qui compte le nombre de tours autour de 0. Plus précisément :

- 1 $\text{ind}(\text{id}) = 1$.
- 2 $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.
- 3 $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ sont homotopes dans \mathbb{C}^* .

La difficulté est de démontrer l'existence d'une telle application ind !
Il faut d'abord la construire puis établir toutes les propriétés requises.

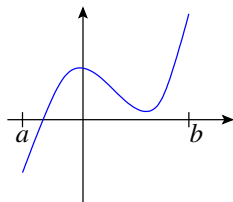
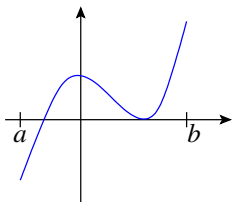
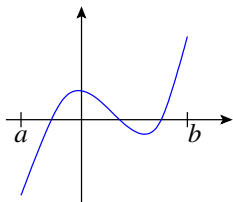
Pour réaliser cette construction, tous les moyens sont bons :

- Théorie des revêtements, appliquée à $\exp: \mathbb{C} \rightarrow \mathbb{C}^*$.
- Groupe fondamental $\text{ind}: \pi_1(\mathbb{C}^*, 1) \xrightarrow{\sim} \mathbb{Z}$ via Seifert–van Kampen.
- Homologie $\text{ind}: H_1(\mathbb{C}^*) \xrightarrow{\sim} \mathbb{Z}$ via les axiomes d'Eilenberg–Steenrod.
- Analyse complexe, indice analytique $\text{ind}(\gamma) = \frac{1}{2i\pi} \int_{\gamma} \frac{dz}{z}$.
- Algèbre réelle, indice de Cauchy via les suites de Sturm.

- 1 Les trois types de preuve du théorème fondamental
- 2 Racines réelles d'un polynôme réel**
 - Le théorème des valeurs intermédiaires
 - Comptage des zéros et des pôles
 - Le théorème de Sturm
- 3 Racines complexes d'un polynôme complexe
- 4 Aspects algorithmiques

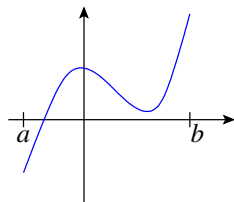
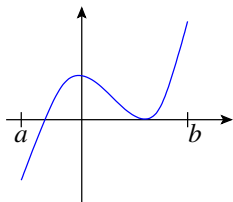
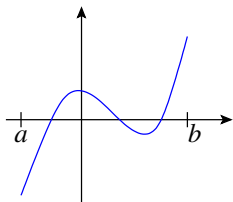
Objectif

Comment déterminer le nombre des racines de $P \in \mathbb{R}[X]$ dans $[a, b]$?



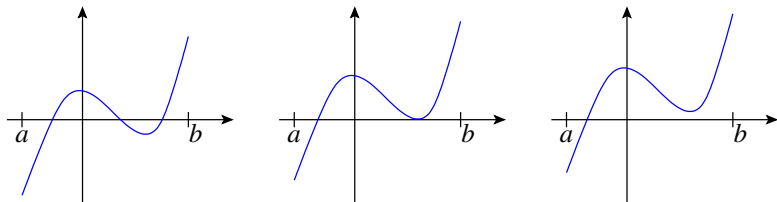
Objectif

Comment déterminer le nombre des racines de $P \in \mathbb{R}[X]$ dans $[a, b]$?



Réponses partielles par René Descartes (1596-1650),
François Budan (1761-1840), Joseph Fourier (1768-1830), ...

Comment déterminer le nombre des racines de $P \in \mathbb{R}[X]$ dans $[a, b]$?



Réponses partielles par René Descartes (1596-1650),
François Budan (1761-1840), Joseph Fourier (1768-1830), ...

La réponse complète fut donnée par Sturm en 1829/35 :

$$\#\{x \in [a, b] \mid P(x) = 0\} = V_a^b(S_0, S_1, \dots, S_n).$$

Théorème

Pour tout corps ordonné $(\mathbf{R}, +, \cdot, \leq)$ sont équivalents :

Théorème

Pour tout corps ordonné $(\mathbf{R}, +, \cdot, \leq)$ sont équivalents :

1 *(\mathbf{R}, \leq) satisfait à l'axiome de la borne supérieure.*

Théorème

Pour tout corps ordonné $(\mathbf{R}, +, \cdot, \leq)$ sont équivalents :

- 1** (\mathbf{R}, \leq) satisfait à l'axiome de la borne supérieure.
- 2** Tout intervalle $[a, b] \subset \mathbf{R}$ est compact.

Théorème

Pour tout corps ordonné $(\mathbf{R}, +, \cdot, \leq)$ sont équivalents :

- 1** *(\mathbf{R}, \leq) satisfait à l'axiome de la borne supérieure.*
- 2** *Tout intervalle $[a, b] \subset \mathbf{R}$ est compact.*
- 3** *Tout intervalle $[a, b] \subset \mathbf{R}$ est connexe.*

Théorème

Pour tout corps ordonné $(\mathbf{R}, +, \cdot, \leq)$ sont équivalents :

- 1 (\mathbf{R}, \leq) satisfait à l'axiome de la borne supérieure.
- 2 Tout intervalle $[a, b] \subset \mathbf{R}$ est compact.
- 3 Tout intervalle $[a, b] \subset \mathbf{R}$ est connexe.
- 4 Toute $f: \mathbf{R} \rightarrow \mathbf{R}$ continue a la propriété des valeurs intermédiaires :
 $a < b \wedge f(a) < 0 < f(b) \implies \exists x \in \mathbf{R} : a < x < b \wedge f(x) = 0.$

Théorème

Pour tout corps ordonné $(\mathbf{R}, +, \cdot, \leq)$ sont équivalents :

- 1** (\mathbf{R}, \leq) satisfait à l'axiome de la borne supérieure.
- 2** Tout intervalle $[a, b] \subset \mathbf{R}$ est compact.
- 3** Tout intervalle $[a, b] \subset \mathbf{R}$ est connexe.
- 4** Toute $f: \mathbf{R} \rightarrow \mathbf{R}$ continue a la propriété des valeurs intermédiaires :
 $a < b \wedge f(a) < 0 < f(b) \implies \exists x \in \mathbf{R} : a < x < b \wedge f(x) = 0.$

Deux tels corps sont isomorphes par un unique isomorphisme de corps.

Théorème

Pour tout corps ordonné $(\mathbf{R}, +, \cdot, \leq)$ sont équivalents :

- 1** *(\mathbf{R}, \leq) satisfait à l'axiome de la borne supérieure.*
- 2** *Tout intervalle $[a, b] \subset \mathbf{R}$ est compact.*
- 3** *Tout intervalle $[a, b] \subset \mathbf{R}$ est connexe.*
- 4** *Toute $f: \mathbf{R} \rightarrow \mathbf{R}$ continue a la propriété des valeurs intermédiaires :
 $a < b \wedge f(a) < 0 < f(b) \implies \exists x \in \mathbf{R} : a < x < b \wedge f(x) = 0.$*

Deux tels corps sont isomorphes par un unique isomorphisme de corps.

Un tel objet existe : on l'appelle le corps des nombres réels, noté \mathbb{R} .

Théorème

Pour tout corps ordonné $(\mathbf{R}, +, \cdot, \leq)$ sont équivalents :

- 1 (\mathbf{R}, \leq) satisfait à l'axiome de la borne supérieure.
- 2 Tout intervalle $[a, b] \subset \mathbf{R}$ est compact.
- 3 Tout intervalle $[a, b] \subset \mathbf{R}$ est connexe.
- 4 Toute $f: \mathbf{R} \rightarrow \mathbf{R}$ continue a la propriété des valeurs intermédiaires :
 $a < b \wedge f(a) < 0 < f(b) \implies \exists x \in \mathbf{R} : a < x < b \wedge f(x) = 0.$

Deux tels corps sont isomorphes par un unique isomorphisme de corps.

Un tel objet existe : on l'appelle le corps des nombres réels, noté \mathbb{R} .

Définition (corps réel clos)

Un corps ordonné $(\mathbf{R}, +, \cdot, \leq)$ est dit *réel clos* si tout polynôme $P \in \mathbf{R}[X]$ a la propriété de valeurs intermédiaires.

Théorème

Pour tout corps ordonné $(\mathbf{R}, +, \cdot, \leq)$ sont équivalents :

- 1 (\mathbf{R}, \leq) satisfait à l'axiome de la borne supérieure.
- 2 Tout intervalle $[a, b] \subset \mathbf{R}$ est compact.
- 3 Tout intervalle $[a, b] \subset \mathbf{R}$ est connexe.
- 4 Toute $f: \mathbf{R} \rightarrow \mathbf{R}$ continue a la propriété des valeurs intermédiaires :
 $a < b \wedge f(a) < 0 < f(b) \implies \exists x \in \mathbf{R} : a < x < b \wedge f(x) = 0.$

Deux tels corps sont isomorphes par un unique isomorphisme de corps.
Un tel objet existe : on l'appelle le corps des nombres réels, noté \mathbb{R} .

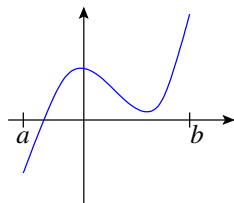
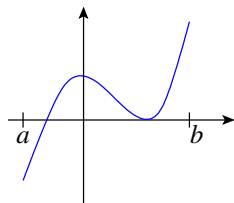
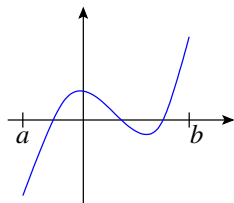
Définition (corps réel clos)

Un corps ordonné $(\mathbf{R}, +, \cdot, \leq)$ est dit *réel clos* si tout polynôme $P \in \mathbf{R}[X]$ a la propriété de valeurs intermédiaires.

Exemples : les réels \mathbb{R} , les réels algébriques $\mathbb{Q}^c \subset \mathbb{R}$, puis $\mathbb{R}(X)^c, \dots$
Tout corps ordonné admet une unique clôture réelle.

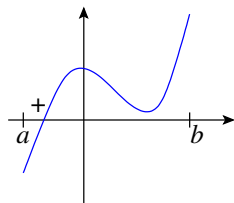
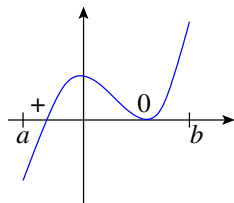
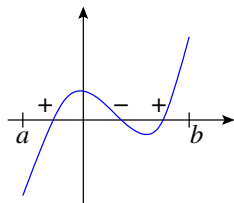
Zéros et pôles

On souhaite compter les zéros d'un polynôme $P \in \mathbf{R}[X]$ dans $[a, b]$:



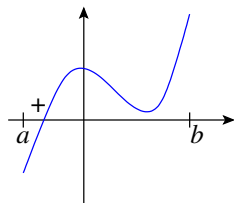
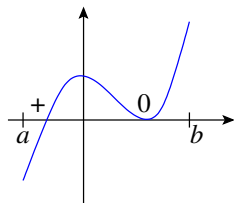
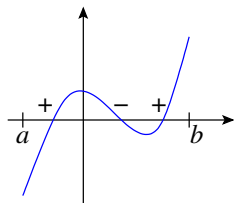
Zéros et pôles

On souhaite compter les zéros d'un polynôme $P \in \mathbf{R}[X]$ dans $[a, b]$:

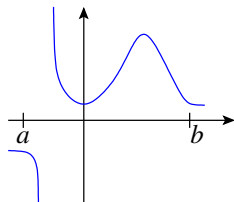
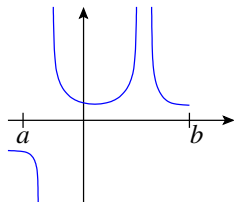
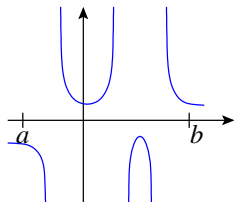


Zéros et pôles

On souhaite compter les zéros d'un polynôme $P \in \mathbf{R}[X]$ dans $[a, b]$:

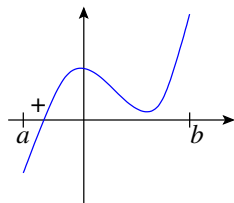
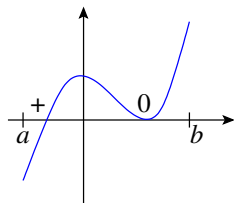
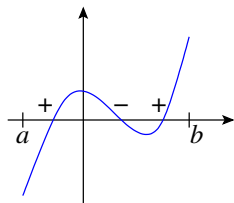


De manière équivalente on peut compter les pôles de $1/P$:

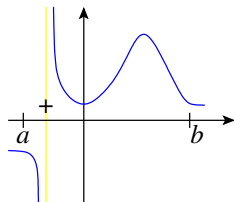
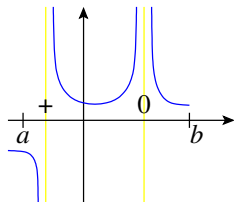
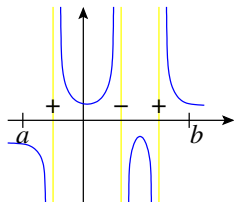


Zéros et pôles

On souhaite compter les zéros d'un polynôme $P \in \mathbf{R}[X]$ dans $[a, b]$:

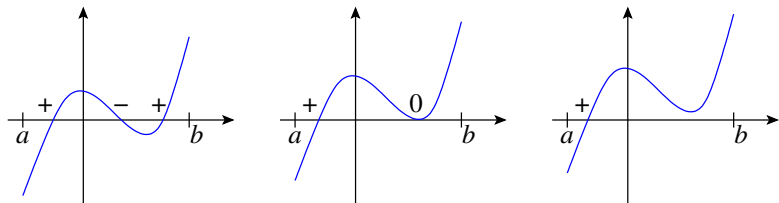


De manière équivalente on peut compter les pôles de $1/P$:

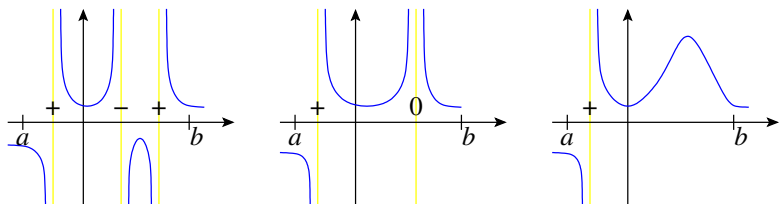


Zéros et pôles

On souhaite compter les zéros d'un polynôme $P \in \mathbf{R}[X]$ dans $[a, b]$:



De manière équivalente on peut compter les pôles de $1/P$:



Il sera avantageux de considérer plus généralement des fractions Q/P .

Indice de Cauchy en un point

Pour $R, S \in \mathbf{R}[X]^*$ on définit $f: \mathbf{R} \setminus \mathcal{L}(S) \rightarrow \mathbf{R}$ par $f(x) = R(x)/S(x)$.

Indice de Cauchy en un point

Pour $R, S \in \mathbf{R}[X]^*$ on définit $f: \mathbf{R} \setminus \mathcal{Z}(S) \rightarrow \mathbf{R}$ par $f(x) = R(x)/S(x)$.

Ici $\mathcal{Z}(S) = \{x \in \mathbf{R} \mid S(x) = 0\}$ est l'ensemble des racines de S .

Indice de Cauchy en un point

Pour $R, S \in \mathbf{R}[X]^*$ on définit $f: \mathbf{R} \setminus \mathcal{Z}(S) \rightarrow \mathbf{R}$ par $f(x) = R(x)/S(x)$.

Ici $\mathcal{Z}(S) = \{x \in \mathbf{R} \mid S(x) = 0\}$ est l'ensemble des racines de S .

On note $\lim_a^- f$ et $\lim_a^+ f$ les limites à gauche et à droite en $a \in \mathbf{R}$.

Indice de Cauchy en un point

Pour $R, S \in \mathbf{R}[X]^*$ on définit $f: \mathbf{R} \setminus \mathcal{Z}(S) \rightarrow \mathbf{R}$ par $f(x) = R(x)/S(x)$.

Ici $\mathcal{Z}(S) = \{x \in \mathbf{R} \mid S(x) = 0\}$ est l'ensemble des racines de S .

On note $\lim_a^- f$ et $\lim_a^+ f$ les limites à gauche et à droite en $a \in \mathbf{R}$.

$$\text{Ind}_a^\varepsilon(f) := \begin{cases} +1 & \text{si } \lim_a^\varepsilon f = +\infty, \\ -1 & \text{si } \lim_a^\varepsilon f = -\infty, \\ 0 & \text{dans tous les autres cas.} \end{cases}$$

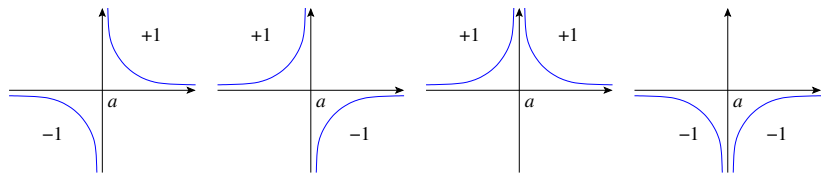
Indice de Cauchy en un point

Pour $R, S \in \mathbf{R}[X]^*$ on définit $f: \mathbf{R} \setminus \mathcal{Z}(S) \rightarrow \mathbf{R}$ par $f(x) = R(x)/S(x)$.

Ici $\mathcal{Z}(S) = \{x \in \mathbf{R} \mid S(x) = 0\}$ est l'ensemble des racines de S .

On note $\lim_a^- f$ et $\lim_a^+ f$ les limites à gauche et à droite en $a \in \mathbf{R}$.

$$\text{Ind}_a^\varepsilon(f) := \begin{cases} +1 & \text{si } \lim_a^\varepsilon f = +\infty, \\ -1 & \text{si } \lim_a^\varepsilon f = -\infty, \\ 0 & \text{dans tous les autres cas.} \end{cases}$$



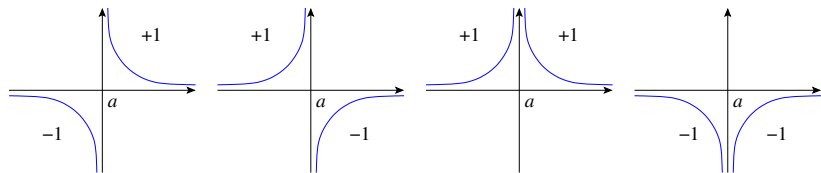
Indice de Cauchy en un point

Pour $R, S \in \mathbf{R}[X]^*$ on définit $f: \mathbf{R} \setminus \mathcal{Z}(S) \rightarrow \mathbf{R}$ par $f(x) = R(x)/S(x)$.

Ici $\mathcal{Z}(S) = \{x \in \mathbf{R} \mid S(x) = 0\}$ est l'ensemble des racines de S .

On note $\lim_a^- f$ et $\lim_a^+ f$ les limites à gauche et à droite en $a \in \mathbf{R}$.

$$\text{Ind}_a^\varepsilon(f) := \begin{cases} +1 & \text{si } \lim_a^\varepsilon f = +\infty, \\ -1 & \text{si } \lim_a^\varepsilon f = -\infty, \\ 0 & \text{dans tous les autres cas.} \end{cases}$$



On définit l'indice de Cauchy de f en a par

$$\text{Ind}_a(f) := \frac{1}{2} [\text{Ind}_a^+(f) - \text{Ind}_a^-(f)].$$

Définition

Pour $a < b$ dans \mathbb{R} on définit l'indice de Cauchy de f sur $[a, b]$ par

$$\text{Ind}_a^b(f) := \frac{1}{2} \text{Ind}_a^+(f) + \sum_{x \in]a, b[} \text{Ind}_x(f) - \frac{1}{2} \text{Ind}_b^-(f).$$

Définition

Pour $a < b$ dans \mathbb{R} on définit l'indice de Cauchy de f sur $[a, b]$ par

$$\text{Ind}_a^b(f) := \frac{1}{2} \text{Ind}_a^+(f) + \sum_{x \in]a, b[} \text{Ind}_x(f) - \frac{1}{2} \text{Ind}_b^-(f).$$

Pour $b < a$ on pose $\text{Ind}_a^b(f) := -\text{Ind}_b^a(f)$, et on pose $\text{Ind}_a^a(f) := 0$.

Définition

Pour $a < b$ dans \mathbb{R} on définit l'indice de Cauchy de f sur $[a, b]$ par

$$\text{Ind}_a^b(f) := \frac{1}{2} \text{Ind}_a^+(f) + \sum_{x \in]a, b[} \text{Ind}_x(f) - \frac{1}{2} \text{Ind}_b^-(f).$$

Pour $b < a$ on pose $\text{Ind}_a^b(f) := -\text{Ind}_b^a(f)$, et on pose $\text{Ind}_a^a(f) := 0$.

La somme est bien définie : seul un nombre fini de points contribuent.

Définition

Pour $a < b$ dans \mathbb{R} on définit l'indice de Cauchy de f sur $[a, b]$ par

$$\text{Ind}_a^b(f) := \frac{1}{2} \text{Ind}_a^+(f) + \sum_{x \in]a, b[} \text{Ind}_x(f) - \frac{1}{2} \text{Ind}_b^-(f).$$

Pour $b < a$ on pose $\text{Ind}_a^b(f) := -\text{Ind}_b^a(f)$, et on pose $\text{Ind}_a^a(f) := 0$.

La somme est bien définie : seul un nombre fini de points contribuent.

L'indice jouit des propriétés suivantes (similaire à l'intégrale) :

Définition

Pour $a < b$ dans \mathbf{R} on définit l'indice de Cauchy de f sur $[a, b]$ par

$$\text{Ind}_a^b(f) := \frac{1}{2} \text{Ind}_a^+(f) + \sum_{x \in]a, b[} \text{Ind}_x(f) - \frac{1}{2} \text{Ind}_b^-(f).$$

Pour $b < a$ on pose $\text{Ind}_a^b(f) := -\text{Ind}_b^a(f)$, et on pose $\text{Ind}_a^a(f) := 0$.

La somme est bien définie : seul un nombre fini de points contribuent.

L'indice jouit des propriétés suivantes (similaire à l'intégrale) :

découpage: $\text{Ind}_a^b(f) + \text{Ind}_b^c(f) = \text{Ind}_a^c(f)$ pour tout $a, b, c \in \mathbf{R}$.

Définition

Pour $a < b$ dans \mathbf{R} on définit l'indice de Cauchy de f sur $[a, b]$ par

$$\text{Ind}_a^b(f) := \frac{1}{2} \text{Ind}_a^+(f) + \sum_{x \in]a, b[} \text{Ind}_x(f) - \frac{1}{2} \text{Ind}_b^-(f).$$

Pour $b < a$ on pose $\text{Ind}_a^b(f) := -\text{Ind}_b^a(f)$, et on pose $\text{Ind}_a^a(f) := 0$.

La somme est bien définie : seul un nombre fini de points contribuent.

L'indice jouit des propriétés suivantes (similaire à l'intégrale) :

découpage: $\text{Ind}_a^b(f) + \text{Ind}_b^c(f) = \text{Ind}_a^c(f)$ pour tout $a, b, c \in \mathbf{R}$.

invariance: $\text{Ind}_a^b(f \circ \tau) = \text{Ind}_{\tau(a)}^{\tau(b)}(f)$ pour tout fonction $\tau(x) = ux + v$.

Définition

Pour $a < b$ dans \mathbf{R} on définit l'indice de Cauchy de f sur $[a, b]$ par

$$\text{Ind}_a^b(f) := \frac{1}{2} \text{Ind}_a^+(f) + \sum_{x \in]a, b[} \text{Ind}_x(f) - \frac{1}{2} \text{Ind}_b^-(f).$$

Pour $b < a$ on pose $\text{Ind}_a^b(f) := -\text{Ind}_b^a(f)$, et on pose $\text{Ind}_a^a(f) := 0$.

La somme est bien définie : seul un nombre fini de points contribuent.

L'indice jouit des propriétés suivantes (similaire à l'intégrale) :

découpage: $\text{Ind}_a^b(f) + \text{Ind}_b^c(f) = \text{Ind}_a^c(f)$ pour tout $a, b, c \in \mathbf{R}$.

invariance: $\text{Ind}_a^b(f \circ \tau) = \text{Ind}_{\tau(a)}^{\tau(b)}(f)$ pour toute fonction $\tau(x) = ux + v$.

somme: $\text{Ind}_a^b(f + g) = \text{Ind}_a^b(f) + \text{Ind}_a^b(g)$ s'il n'y a pas de pôle commun.

Définition

Pour $a < b$ dans \mathbf{R} on définit l'indice de Cauchy de f sur $[a, b]$ par

$$\text{Ind}_a^b(f) := \frac{1}{2} \text{Ind}_a^+(f) + \sum_{x \in]a, b[} \text{Ind}_x(f) - \frac{1}{2} \text{Ind}_b^-(f).$$

Pour $b < a$ on pose $\text{Ind}_a^b(f) := -\text{Ind}_b^a(f)$, et on pose $\text{Ind}_a^a(f) := 0$.

La somme est bien définie : seul un nombre fini de points contribuent.

L'indice jouit des propriétés suivantes (similaire à l'intégrale) :

découpage: $\text{Ind}_a^b(f) + \text{Ind}_b^c(f) = \text{Ind}_a^c(f)$ pour tout $a, b, c \in \mathbf{R}$.

invariance: $\text{Ind}_a^b(f \circ \tau) = \text{Ind}_{\tau(a)}^{\tau(b)}(f)$ pour toute fonction $\tau(x) = ux + v$.

somme: $\text{Ind}_a^b(f + g) = \text{Ind}_a^b(f) + \text{Ind}_a^b(g)$ s'il n'y a pas de pôle commun.

produit: $\text{Ind}_a^b(gf) = \sigma \text{Ind}_a^b(f)$ si $g|_{[a, b]}$ est de signe constant $\sigma \in \{\pm 1\}$.

Définition

Pour $a < b$ dans \mathbf{R} on définit l'indice de Cauchy de f sur $[a, b]$ par

$$\text{Ind}_a^b(f) := \frac{1}{2} \text{Ind}_a^+(f) + \sum_{x \in]a, b[} \text{Ind}_x(f) - \frac{1}{2} \text{Ind}_b^-(f).$$

Pour $b < a$ on pose $\text{Ind}_a^b(f) := -\text{Ind}_b^a(f)$, et on pose $\text{Ind}_a^a(f) := 0$.

La somme est bien définie : seul un nombre fini de points contribuent.

L'indice jouit des propriétés suivantes (similaire à l'intégrale) :

découpage: $\text{Ind}_a^b(f) + \text{Ind}_b^c(f) = \text{Ind}_a^c(f)$ pour tout $a, b, c \in \mathbf{R}$.

invariance: $\text{Ind}_a^b(f \circ \tau) = \text{Ind}_{\tau(a)}^{\tau(b)}(f)$ pour tout fonction $\tau(x) = ux + v$.

somme: $\text{Ind}_a^b(f + g) = \text{Ind}_a^b(f) + \text{Ind}_a^b(g)$ s'il n'y pas de pôle commun.

produit: $\text{Ind}_a^b(gf) = \sigma \text{Ind}_a^b(f)$ si $g|_{[a, b]}$ est de signe constant $\sigma \in \{\pm 1\}$.

réduction: $\text{Ind}_a^b(QR/QS) = \text{Ind}_a^b(R/S)$ pour tout $Q, R, S \in \mathbf{R}[X]^*$.

Définition

Pour $a < b$ dans \mathbf{R} on définit l'indice de Cauchy de f sur $[a, b]$ par

$$\text{Ind}_a^b(f) := \frac{1}{2} \text{Ind}_a^+(f) + \sum_{x \in]a, b[} \text{Ind}_x(f) - \frac{1}{2} \text{Ind}_b^-(f).$$

Pour $b < a$ on pose $\text{Ind}_a^b(f) := -\text{Ind}_b^a(f)$, et on pose $\text{Ind}_a^a(f) := 0$.

La somme est bien définie : seul un nombre fini de points contribuent.

L'indice jouit des propriétés suivantes (similaire à l'intégrale) :

découpage: $\text{Ind}_a^b(f) + \text{Ind}_b^c(f) = \text{Ind}_a^c(f)$ pour tout $a, b, c \in \mathbf{R}$.

invariance: $\text{Ind}_a^b(f \circ \tau) = \text{Ind}_{\tau(a)}^{\tau(b)}(f)$ pour toute fonction $\tau(x) = ux + v$.

somme: $\text{Ind}_a^b(f + g) = \text{Ind}_a^b(f) + \text{Ind}_a^b(g)$ s'il n'y a pas de pôle commun.

produit: $\text{Ind}_a^b(gf) = \sigma \text{Ind}_a^b(f)$ si $g|_{[a,b]}$ est de signe constant $\sigma \in \{\pm 1\}$.

réduction: $\text{Ind}_a^b(QR/QS) = \text{Ind}_a^b(R/S)$ pour tout $Q, R, S \in \mathbf{R}[X]^*$.

On peut donc définir $\text{Ind}_a^b(\frac{R}{S}) := \text{Ind}_a^b(f)$ pour $\frac{R}{S} \in \mathbf{R}(X)^*$.

Proposition (dérivée logarithmique)

$$\text{Nous avons } \text{Ind}_a(f'/f) = \begin{cases} +1 & \text{si } a \text{ est un zéro de } f, \\ -1 & \text{si } a \text{ est un pôle de } f, \\ 0 & \text{sinon.} \end{cases}$$

Proposition (dérivée logarithmique)

$$\text{Nous avons } \text{Ind}_a(f'/f) = \begin{cases} +1 & \text{si } a \text{ est un zéro de } f, \\ -1 & \text{si } a \text{ est un pôle de } f, \\ 0 & \text{sinon.} \end{cases}$$

Démonstration.

On a $f = (X - a)^m g$ où $m \in \mathbb{Z}$ et $g \in \mathbf{R}(X)^*$ tel que $g(a) \in \mathbf{R}^*$.

Proposition (dérivée logarithmique)

$$\text{Nous avons } \text{Ind}_a(f'/f) = \begin{cases} +1 & \text{si } a \text{ est un zéro de } f, \\ -1 & \text{si } a \text{ est un pôle de } f, \\ 0 & \text{sinon.} \end{cases}$$

Démonstration.

On a $f = (X - a)^m g$ où $m \in \mathbb{Z}$ et $g \in \mathbf{R}(X)^*$ tel que $g(a) \in \mathbf{R}^*$.

D'après Leibniz on a $f' = m(X - a)^{m-1}g + (X - a)^m g'$ donc

$$\frac{f'}{f} = \frac{m}{X - a} + \frac{g'}{g}.$$

Proposition (dérivée logarithmique)

$$\text{Nous avons } \text{Ind}_a(f'/f) = \begin{cases} +1 & \text{si } a \text{ est un zéro de } f, \\ -1 & \text{si } a \text{ est un pôle de } f, \\ 0 & \text{sinon.} \end{cases}$$

Démonstration.

On a $f = (X - a)^m g$ où $m \in \mathbb{Z}$ et $g \in \mathbf{R}(X)^*$ tel que $g(a) \in \mathbf{R}^*$.

D'après Leibniz on a $f' = m(X - a)^{m-1}g + (X - a)^m g'$ donc

$$\frac{f'}{f} = \frac{m}{X - a} + \frac{g'}{g}.$$

Ici g'/g n'a pas de pôle en a . On conclut que $\text{Ind}_a(f'/f) = \text{sign}(m)$. □

Proposition (dérivée logarithmique)

$$\text{Nous avons } \text{Ind}_a(f'/f) = \begin{cases} +1 & \text{si } a \text{ est un zéro de } f, \\ -1 & \text{si } a \text{ est un pôle de } f, \\ 0 & \text{sinon.} \end{cases}$$

Démonstration.

On a $f = (X - a)^m g$ où $m \in \mathbb{Z}$ et $g \in \mathbf{R}(X)^*$ tel que $g(a) \in \mathbf{R}^*$.

D'après Leibniz on a $f' = m(X - a)^{m-1}g + (X - a)^m g'$ donc

$$\frac{f'}{f} = \frac{m}{X - a} + \frac{g'}{g}.$$

Ici g'/g n'a pas de pôle en a . On conclut que $\text{Ind}_a(f'/f) = \text{sign}(m)$. □

Corollaire

Pour tout polynôme $P \in \mathbf{R}[X]^*$ et pour tout $a < b$ dans \mathbf{R}
l'indice $\text{Ind}_a^b(P'/P)$ compte le nombre des racines de P dans $[a, b]$.
D'éventuelles racines sur le bord $\{a, b\}$ comptent pour un demi.

Variation des signes

On compte les changements de signes entre $s_0, s_1 \in \mathbf{R}$ par

$$V(s_0, s_1) := \frac{1}{2} |\text{sign}(s_0) - \text{sign}(s_1)|.$$

Variation des signes

On compte les changements de signes entre $s_0, s_1 \in \mathbf{R}$ par

$$V(s_0, s_1) := \frac{1}{2} |\text{sign}(s_0) - \text{sign}(s_1)|.$$

Ceci résume les 9 cas suivants :

$$\begin{aligned} V(+, -) = V(-, +) &= 1, & V(+, +) = V(-, -) = V(0, 0) &= 0, \\ V(+, 0) = V(0, +) &= \frac{1}{2}, & V(-, 0) = V(0, -) &= \frac{1}{2}. \end{aligned}$$

On compte les changements de signes entre $s_0, s_1 \in \mathbf{R}$ par

$$V(s_0, s_1) := \frac{1}{2} |\text{sign}(s_0) - \text{sign}(s_1)|.$$

Ceci résume les 9 cas suivants :

$$\begin{aligned} V(+, -) = V(-, +) &= 1, & V(+, +) = V(-, -) = V(0, 0) &= 0, \\ V(+, 0) = V(0, +) &= \frac{1}{2}, & V(-, 0) = V(0, -) &= \frac{1}{2}. \end{aligned}$$

Définition

La variation des signes d'une suite $s = (s_0, \dots, s_n)$ dans \mathbf{R} est définie par

$$V(s) := \sum_{k=1}^n \frac{1}{2} |\text{sign}(s_{k-1}) - \text{sign}(s_k)|.$$

On compte les changements de signes entre $s_0, s_1 \in \mathbf{R}$ par

$$V(s_0, s_1) := \frac{1}{2} |\text{sign}(s_0) - \text{sign}(s_1)|.$$

Ceci résume les 9 cas suivants :

$$\begin{aligned} V(+, -) = V(-, +) &= 1, & V(+, +) = V(-, -) = V(0, 0) &= 0, \\ V(+, 0) = V(0, +) &= \frac{1}{2}, & V(-, 0) = V(0, -) &= \frac{1}{2}. \end{aligned}$$

Définition

La variation des signes d'une suite $s = (s_0, \dots, s_n)$ dans \mathbf{R} est définie par

$$V(s) := \sum_{k=1}^n \frac{1}{2} |\text{sign}(s_{k-1}) - \text{sign}(s_k)|.$$

La variation des signes d'une suite (S_0, \dots, S_n) dans $\mathbf{R}[X]$ en $a \in \mathbf{R}$ est

$$V_a(S_0, \dots, S_n) := V(S_0(a), \dots, S_n(a)).$$

Variation des signes

On compte les changements de signes entre $s_0, s_1 \in \mathbf{R}$ par

$$V(s_0, s_1) := \frac{1}{2} |\text{sign}(s_0) - \text{sign}(s_1)|.$$

Ceci résume les 9 cas suivants :

$$\begin{aligned} V(+, -) = V(-, +) &= 1, & V(+, +) = V(-, -) = V(0, 0) &= 0, \\ V(+, 0) = V(0, +) &= \frac{1}{2}, & V(-, 0) = V(0, -) &= \frac{1}{2}. \end{aligned}$$

Définition

La variation des signes d'une suite $s = (s_0, \dots, s_n)$ dans \mathbf{R} est définie par

$$V(s) := \sum_{k=1}^n \frac{1}{2} |\text{sign}(s_{k-1}) - \text{sign}(s_k)|.$$

La variation des signes d'une suite (S_0, \dots, S_n) dans $\mathbf{R}[X]$ en $a \in \mathbf{R}$ est

$$V_a(S_0, \dots, S_n) := V(S_0(a), \dots, S_n(a)).$$

Pour la différence en $a, b \in \mathbf{R}$ nous posons $V_a^b := V_a - V_b$.

On compte les changements de signes entre $s_0, s_1 \in \mathbf{R}$ par

$$V(s_0, s_1) := \frac{1}{2} |\text{sign}(s_0) - \text{sign}(s_1)|.$$

Ceci résume les 9 cas suivants :

$$\begin{aligned} V(+, -) = V(-, +) &= 1, & V(+, +) = V(-, -) = V(0, 0) &= 0, \\ V(+, 0) = V(0, +) &= \frac{1}{2}, & V(-, 0) = V(0, -) &= \frac{1}{2}. \end{aligned}$$

Définition

La variation des signes d'une suite $s = (s_0, \dots, s_n)$ dans \mathbf{R} est définie par

$$V(s) := \sum_{k=1}^n \frac{1}{2} |\text{sign}(s_{k-1}) - \text{sign}(s_k)|.$$

La variation des signes d'une suite (S_0, \dots, S_n) dans $\mathbf{R}[X]$ en $a \in \mathbf{R}$ est

$$V_a(S_0, \dots, S_n) := V(S_0(a), \dots, S_n(a)).$$

Pour la différence en $a, b \in \mathbf{R}$ nous posons $V_a^b := V_a - V_b$.

Le théorème des valeurs intermédiaires prend la forme $\text{Ind}_a^b(\frac{1}{P}) = V_a^b(P)$.

Proposition (Cauchy 1837)

Si $P, Q \in \mathbf{R}[X]$ n'ont pas de racine commune en a ni en b , alors

$$\text{Ind}_a^b\left(\frac{Q}{P}\right) + \text{Ind}_a^b\left(\frac{P}{Q}\right) = V_a^b(P, Q).$$

Proposition (Cauchy 1837)

Si $P, Q \in \mathbf{R}[X]$ n'ont pas de racine commune en a ni en b , alors

$$\text{Ind}_a^b\left(\frac{Q}{P}\right) + \text{Ind}_a^b\left(\frac{P}{Q}\right) = V_a^b(P, Q).$$

Démonstration. On peut supposer que $P \neq 0$ et $Q \neq 0$ et $\text{pgcd}(P, Q) = 1$.

Proposition (Cauchy 1837)

Si $P, Q \in \mathbf{R}[X]$ n'ont pas de racine commune en a ni en b , alors

$$\text{Ind}_a^b\left(\frac{Q}{P}\right) + \text{Ind}_a^b\left(\frac{P}{Q}\right) = V_a^b(P, Q).$$

Démonstration. On peut supposer que $P \neq 0$ et $Q \neq 0$ et $\text{pgcd}(P, Q) = 1$.

Si $[a, b]$ ne contient aucun pôle, alors le coté gauche est nul ;
le coté droite est nul par le théorème des valeurs intermédiaires.

Proposition (Cauchy 1837)

Si $P, Q \in \mathbf{R}[X]$ n'ont pas de racine commune en a ni en b , alors

$$\text{Ind}_a^b\left(\frac{Q}{P}\right) + \text{Ind}_a^b\left(\frac{P}{Q}\right) = V_a^b(P, Q).$$

Démonstration. On peut supposer que $P \neq 0$ et $Q \neq 0$ et $\text{pgcd}(P, Q) = 1$.

Si $[a, b]$ ne contient aucun pôle, alors le coté gauche est nul ;
le coté droite est nul par le théorème des valeurs intermédiaires.

La formule est additive par rapport au découpage de l'intervalle $[a, b]$.
On peut donc supposer que a est l'unique pôle, puis $P(a) = 0$ et $Q(a) \neq 0$.

Proposition (Cauchy 1837)

Si $P, Q \in \mathbf{R}[X]$ n'ont pas de racine commune en a ni en b , alors

$$\text{Ind}_a^b\left(\frac{Q}{P}\right) + \text{Ind}_a^b\left(\frac{P}{Q}\right) = V_a^b(P, Q).$$

Démonstration. On peut supposer que $P \neq 0$ et $Q \neq 0$ et $\text{pgcd}(P, Q) = 1$.

Si $[a, b]$ ne contient aucun pôle, alors le coté gauche est nul ;
le coté droite est nul par le théorème des valeurs intermédiaires.

La formule est additive par rapport au découpage de l'intervalle $[a, b]$.
On peut donc supposer que a est l'unique pôle, puis $P(a) = 0$ et $Q(a) \neq 0$.
Ainsi Q est de signe constant sur $[a, b]$, et P est de signe constant sur $]a, b]$.

Proposition (Cauchy 1837)

Si $P, Q \in \mathbf{R}[X]$ n'ont pas de racine commune en a ni en b , alors

$$\operatorname{Ind}_a^b\left(\frac{Q}{P}\right) + \operatorname{Ind}_a^b\left(\frac{P}{Q}\right) = V_a^b(P, Q).$$

Démonstration. On peut supposer que $P \neq 0$ et $Q \neq 0$ et $\operatorname{pgcd}(P, Q) = 1$.

Si $[a, b]$ ne contient aucun pôle, alors le coté gauche est nul ;
le coté droite est nul par le théorème des valeurs intermédiaires.

La formule est additive par rapport au découpage de l'intervalle $[a, b]$.
On peut donc supposer que a est l'unique pôle, puis $P(a) = 0$ et $Q(a) \neq 0$.

Ainsi Q est de signe constant sur $[a, b]$, et P est de signe constant sur $]a, b]$.

À gauche on trouve $\operatorname{Ind}_a^b\left(\frac{P}{Q}\right) = 0$ et $\operatorname{Ind}_a^b\left(\frac{Q}{P}\right) = \frac{1}{2} \operatorname{Ind}_a^+\left(\frac{Q}{P}\right)$.

Proposition (Cauchy 1837)

Si $P, Q \in \mathbf{R}[X]$ n'ont pas de racine commune en a ni en b , alors

$$\operatorname{Ind}_a^b\left(\frac{Q}{P}\right) + \operatorname{Ind}_a^b\left(\frac{P}{Q}\right) = V_a^b(P, Q).$$

Démonstration. On peut supposer que $P \neq 0$ et $Q \neq 0$ et $\operatorname{pgcd}(P, Q) = 1$.

Si $[a, b]$ ne contient aucun pôle, alors le coté gauche est nul ;
le coté droite est nul par le théorème des valeurs intermédiaires.

La formule est additive par rapport au découpage de l'intervalle $[a, b]$.
On peut donc supposer que a est l'unique pôle, puis $P(a) = 0$ et $Q(a) \neq 0$.

Ainsi Q est de signe constant sur $[a, b]$, et P est de signe constant sur $]a, b]$.

À gauche on trouve $\operatorname{Ind}_a^b\left(\frac{P}{Q}\right) = 0$ et $\operatorname{Ind}_a^b\left(\frac{Q}{P}\right) = \frac{1}{2} \operatorname{Ind}_a^+\left(\frac{Q}{P}\right)$.

À droite on trouve $V_a(P, Q) = \frac{1}{2}$.

Proposition (Cauchy 1837)

Si $P, Q \in \mathbf{R}[X]$ n'ont pas de racine commune en a ni en b , alors

$$\operatorname{Ind}_a^b\left(\frac{Q}{P}\right) + \operatorname{Ind}_a^b\left(\frac{P}{Q}\right) = V_a^b(P, Q).$$

Démonstration. On peut supposer que $P \neq 0$ et $Q \neq 0$ et $\operatorname{pgcd}(P, Q) = 1$.

Si $[a, b]$ ne contient aucun pôle, alors le coté gauche est nul ;
le coté droite est nul par le théorème des valeurs intermédiaires.

La formule est additive par rapport au découpage de l'intervalle $[a, b]$.
On peut donc supposer que a est l'unique pôle, puis $P(a) = 0$ et $Q(a) \neq 0$.

Ainsi Q est de signe constant sur $[a, b]$, et P est de signe constant sur $]a, b]$.

À gauche on trouve $\operatorname{Ind}_a^b\left(\frac{P}{Q}\right) = 0$ et $\operatorname{Ind}_a^b\left(\frac{Q}{P}\right) = \frac{1}{2} \operatorname{Ind}_a^+\left(\frac{Q}{P}\right)$.

À droite on trouve $V_a(P, Q) = \frac{1}{2}$. Pour V_b on distingue deux cas :

- Si $V_b(P, Q) = 0$, alors $PQ > 0$ sur $]a, b]$, donc $\lim_a^+\left(\frac{Q}{P}\right) = +\infty$.

Proposition (Cauchy 1837)

Si $P, Q \in \mathbf{R}[X]$ n'ont pas de racine commune en a ni en b , alors

$$\text{Ind}_a^b\left(\frac{Q}{P}\right) + \text{Ind}_a^b\left(\frac{P}{Q}\right) = V_a^b(P, Q).$$

Démonstration. On peut supposer que $P \neq 0$ et $Q \neq 0$ et $\text{pgcd}(P, Q) = 1$.

Si $[a, b]$ ne contient aucun pôle, alors le coté gauche est nul ;
le coté droite est nul par le théorème des valeurs intermédiaires.

La formule est additive par rapport au découpage de l'intervalle $[a, b]$.
On peut donc supposer que a est l'unique pôle, puis $P(a) = 0$ et $Q(a) \neq 0$.

Ainsi Q est de signe constant sur $[a, b]$, et P est de signe constant sur $]a, b]$.

À gauche on trouve $\text{Ind}_a^b\left(\frac{P}{Q}\right) = 0$ et $\text{Ind}_a^b\left(\frac{Q}{P}\right) = \frac{1}{2} \text{Ind}_a^+\left(\frac{Q}{P}\right)$.

À droite on trouve $V_a(P, Q) = \frac{1}{2}$. Pour V_b on distingue deux cas :

- Si $V_b(P, Q) = 0$, alors $PQ > 0$ sur $]a, b]$, donc $\lim_a^+\left(\frac{Q}{P}\right) = +\infty$.
- Si $V_b(P, Q) = 1$, alors $PQ < 0$ sur $]a, b]$, donc $\lim_a^+\left(\frac{Q}{P}\right) = -\infty$.

Proposition (Cauchy 1837)

Si $P, Q \in \mathbf{R}[X]$ n'ont pas de racine commune en a ni en b , alors

$$\text{Ind}_a^b\left(\frac{Q}{P}\right) + \text{Ind}_a^b\left(\frac{P}{Q}\right) = V_a^b(P, Q).$$

Démonstration. On peut supposer que $P \neq 0$ et $Q \neq 0$ et $\text{pgcd}(P, Q) = 1$.

Si $[a, b]$ ne contient aucun pôle, alors le coté gauche est nul ;
le coté droite est nul par le théorème des valeurs intermédiaires.

La formule est additive par rapport au découpage de l'intervalle $[a, b]$.
On peut donc supposer que a est l'unique pôle, puis $P(a) = 0$ et $Q(a) \neq 0$.

Ainsi Q est de signe constant sur $[a, b]$, et P est de signe constant sur $]a, b]$.

À gauche on trouve $\text{Ind}_a^b\left(\frac{P}{Q}\right) = 0$ et $\text{Ind}_a^b\left(\frac{Q}{P}\right) = \frac{1}{2} \text{Ind}_a^+\left(\frac{Q}{P}\right)$.

À droite on trouve $V_a(P, Q) = \frac{1}{2}$. Pour V_b on distingue deux cas :

- Si $V_b(P, Q) = 0$, alors $PQ > 0$ sur $]a, b]$, donc $\lim_a^+\left(\frac{Q}{P}\right) = +\infty$.
- Si $V_b(P, Q) = 1$, alors $PQ < 0$ sur $]a, b]$, donc $\lim_a^+\left(\frac{Q}{P}\right) = -\infty$.

Dans les deux cas on trouve $\frac{1}{2} \text{Ind}_a^+\left(\frac{Q}{P}\right) = V_a^b(P, Q)$.



Définition

Une suite (S_0, \dots, S_n) dans $\mathbf{R}[X]$ est dite *de Sturm* par rapport à un intervalle $[a, b] \subset \mathbf{R}$ si elle satisfait à la condition suivante :

Définition

Une suite (S_0, \dots, S_n) dans $\mathbf{R}[X]$ est dite *de Sturm* par rapport à un intervalle $[a, b] \subset \mathbf{R}$ si elle satisfait à la condition suivante :

Si $S_k(x) = 0$ où $0 < k < n$ et $x \in [a, b]$, alors $S_{k-1}(x)S_{k+1}(x) < 0$.

Définition

Une suite (S_0, \dots, S_n) dans $\mathbf{R}[X]$ est dite *de Sturm* par rapport à un intervalle $[a, b] \subset \mathbf{R}$ si elle satisfait à la condition suivante :

Si $S_k(x) = 0$ où $0 < k < n$ et $x \in [a, b]$, alors $S_{k-1}(x)S_{k+1}(x) < 0$.

Corollaire (de la formule d'inversion)

Si $(S_0, S_1, \dots, S_{n-1}, S_n)$ est une suite de Sturm dans $\mathbf{R}[X]$, alors

$$\text{Ind}_a^b \left(\frac{S_1}{S_0} \right) + \text{Ind}_a^b \left(\frac{S_{n-1}}{S_n} \right) = V_a^b(S_0, S_1, \dots, S_{n-1}, S_n).$$

Définition

Une suite (S_0, \dots, S_n) dans $\mathbf{R}[X]$ est dite *de Sturm* par rapport à un intervalle $[a, b] \subset \mathbf{R}$ si elle satisfait à la condition suivante :

Si $S_k(x) = 0$ où $0 < k < n$ et $x \in [a, b]$, alors $S_{k-1}(x)S_{k+1}(x) < 0$.

Corollaire (de la formule d'inversion)

Si $(S_0, S_1, \dots, S_{n-1}, S_n)$ est une suite de Sturm dans $\mathbf{R}[X]$, alors

$$\text{Ind}_a^b\left(\frac{S_1}{S_0}\right) + \text{Ind}_a^b\left(\frac{S_{n-1}}{S_n}\right) = V_a^b(S_0, S_1, \dots, S_{n-1}, S_n).$$

Démonstration. Pour $n = 2$ la formule d'inversion nous donne

$$\text{Ind}_a^b\left(\frac{S_1}{S_0}\right) + \text{Ind}_a^b\left(\frac{S_0}{S_1}\right) + \text{Ind}_a^b\left(\frac{S_2}{S_1}\right) + \text{Ind}_a^b\left(\frac{S_1}{S_2}\right) = V_a^b(S_0, S_1, S_2).$$

Les contributions au milieu s'annulent. On conclut par récurrence sur n . \square

Suites de Sturm par l'algorithme d'Euclide

Pour $P_0, P_1 \in \mathbf{R}[X]^*$ on itère la division euclidienne : $P_{k+1} = Q_k P_k - P_{k-1}$.

Suites de Sturm par l'algorithme d'Euclide

Pour $P_0, P_1 \in \mathbf{R}[X]^*$ on itère la division euclidienne : $P_{k+1} = Q_k P_k - P_{k-1}$.
Ce processus s'arrête avec $P_{n+1} = 0$ et $P_n \sim \gcd(P_0, P_1)$.

Suites de Sturm par l'algorithme d'Euclide

Pour $P_0, P_1 \in \mathbf{R}[X]^*$ on itère la division euclidienne : $P_{k+1} = Q_k P_k - P_{k-1}$.
Ce processus s'arrête avec $P_{n+1} = 0$ et $P_n \sim \gcd(P_0, P_1)$.

Définition & proposition

La suite de Sturm euclidienne (S_0, S_1, \dots, S_n) associée à (P_0, P_1) est définie par $S_k := P_k/P_n$. Il s'agit effectivement d'une suite de Sturm.

Suites de Sturm par l'algorithme d'Euclide

Pour $P_0, P_1 \in \mathbf{R}[X]^*$ on itère la division euclidienne : $P_{k+1} = Q_k P_k - P_{k-1}$.
Ce processus s'arrête avec $P_{n+1} = 0$ et $P_n \sim \gcd(P_0, P_1)$.

Définition & proposition

La suite de Sturm euclidienne (S_0, S_1, \dots, S_n) associée à (P_0, P_1) est définie par $S_k := P_k/P_n$. Il s'agit effectivement d'une suite de Sturm.

Démonstration. Pour $0 < k < n$ nous avons

$$S_{k+1} = Q_k S_k - S_{k-1}.$$

Si $S_k(x) = 0$, alors $S_{k+1}(x) = -S_{k-1}(x)$.

Suites de Sturm par l'algorithme d'Euclide

Pour $P_0, P_1 \in \mathbf{R}[X]^*$ on itère la division euclidienne : $P_{k+1} = Q_k P_k - P_{k-1}$.
Ce processus s'arrête avec $P_{n+1} = 0$ et $P_n \sim \gcd(P_0, P_1)$.

Définition & proposition

La suite de Sturm euclidienne (S_0, S_1, \dots, S_n) associée à (P_0, P_1) est définie par $S_k := P_k/P_n$. Il s'agit effectivement d'une suite de Sturm.

Démonstration. Pour $0 < k < n$ nous avons

$$S_{k+1} = Q_k S_k - S_{k-1}.$$

Si $S_k(x) = 0$, alors $S_{k+1}(x) = -S_{k-1}(x)$.

Si l'on avait $S_{k-1}(x) = S_{k+1}(x) = 0$, alors on aurait $S_j(x) = 0$ pour tout j .

Suites de Sturm par l'algorithme d'Euclide

Pour $P_0, P_1 \in \mathbf{R}[X]^*$ on itère la division euclidienne : $P_{k+1} = Q_k P_k - P_{k-1}$.
Ce processus s'arrête avec $P_{n+1} = 0$ et $P_n \sim \gcd(P_0, P_1)$.

Définition & proposition

La suite de Sturm euclidienne (S_0, S_1, \dots, S_n) associée à (P_0, P_1) est définie par $S_k := P_k/P_n$. Il s'agit effectivement d'une suite de Sturm.

Démonstration. Pour $0 < k < n$ nous avons

$$S_{k+1} = Q_k S_k - S_{k-1}.$$

Si $S_k(x) = 0$, alors $S_{k+1}(x) = -S_{k-1}(x)$.

Si l'on avait $S_{k-1}(x) = S_{k+1}(x) = 0$, alors on aurait $S_j(x) = 0$ pour tout j .

Or, $S_n = 1$ par construction, donc cette dégénérescence est impossible. \square

Suites de Sturm par l'algorithme d'Euclide

Pour $P_0, P_1 \in \mathbf{R}[X]^*$ on itère la division euclidienne : $P_{k+1} = Q_k P_k - P_{k-1}$.
Ce processus s'arrête avec $P_{n+1} = 0$ et $P_n \sim \gcd(P_0, P_1)$.

Définition & proposition

La suite de Sturm euclidienne (S_0, S_1, \dots, S_n) associée à (P_0, P_1) est définie par $S_k := P_k/P_n$. Il s'agit effectivement d'une suite de Sturm.

Démonstration. Pour $0 < k < n$ nous avons

$$S_{k+1} = Q_k S_k - S_{k-1}.$$

Si $S_k(x) = 0$, alors $S_{k+1}(x) = -S_{k-1}(x)$.

Si l'on avait $S_{k-1}(x) = S_{k+1}(x) = 0$, alors on aurait $S_j(x) = 0$ pour tout j .

Or, $S_n = 1$ par construction, donc cette dégénérescence est impossible. \square

Définition

Pour $\frac{P_1}{P_0} \in \mathbf{R}(X)$ et $a, b \in \mathbf{R}$ on définit l'indice de Sturm par

$$V_a^b \left(\frac{P_1}{P_0} \right) := V_a^b(S_0, S_1, \dots, S_n).$$

Théorème (Sturm 1829/35, Cauchy 1831/37)

Pour tout $R, S \in \mathbf{R}[X]$ nous avons l'égalité

$$\text{Ind}_a^b\left(\frac{R}{S}\right) = V_a^b\left(\frac{R}{S}\right).$$

Théorème (Sturm 1829/35, Cauchy 1831/37)

Pour tout $R, S \in \mathbf{R}[X]$ nous avons l'égalité

$$\text{Ind}_a^b\left(\frac{R}{S}\right) = V_a^b\left(\frac{R}{S}\right).$$

Démonstration.

Théorème (Sturm 1829/35, Cauchy 1831/37)

Pour tout $R, S \in \mathbf{R}[X]$ nous avons l'égalité

$$\text{Ind}_a^b\left(\frac{R}{S}\right) = V_a^b\left(\frac{R}{S}\right).$$

Démonstration. Soit (S_0, S_1, \dots, S_n) la suite de Sturm euclidienne pour $\frac{R}{S}$:

$$\text{Ind}_a^b\left(\frac{R}{S}\right) = \text{Ind}_a^b\left(\frac{S_1}{S_0}\right) + \text{Ind}_a^b\left(\frac{S_{n-1}}{S_n}\right) = V_a^b(S_0, S_1, \dots, S_n) = V_a^b\left(\frac{R}{S}\right).$$

Théorème (Sturm 1829/35, Cauchy 1831/37)

Pour tout $R, S \in \mathbf{R}[X]$ nous avons l'égalité

$$\text{Ind}_a^b\left(\frac{R}{S}\right) = V_a^b\left(\frac{R}{S}\right).$$

Démonstration. Soit (S_0, S_1, \dots, S_n) la suite de Sturm euclidienne pour $\frac{R}{S}$:

$$\text{Ind}_a^b\left(\frac{R}{S}\right) = \text{Ind}_a^b\left(\frac{S_1}{S_0}\right) + \text{Ind}_a^b\left(\frac{S_{n-1}}{S_n}\right) = V_a^b(S_0, S_1, \dots, S_n) = V_a^b\left(\frac{R}{S}\right).$$

Corollaire (Sturm 1829/35)

Pour tout polynôme $P \in \mathbf{R}[X]^*$ nous avons

$$\#\{x \in [a, b] \mid P(x) = 0\} = \text{Ind}_a^b\left(\frac{P'}{P}\right) = V_a^b\left(\frac{P'}{P}\right).$$

D'éventuelles racines sur le bord comptent pour un demi.

- 1 Les trois types de preuve du théorème fondamental
- 2 Racines réelles d'un polynôme réel
- 3 Racines complexes d'un polynôme complexe**
 - L'indice de Cauchy
 - La formule du produit
 - Comptage des racines
 - Invariance par homotopie
- 4 Aspects algorithmiques

Soit \mathbf{R} un corps réel clos et soit $\mathbf{C} = \mathbf{R}[i]$ où $i^2 = -1$.

Soit \mathbf{R} un corps réel clos et soit $\mathbf{C} = \mathbf{R}[i]$ où $i^2 = -1$.

Nous allons construire une fonction

$$\text{ind}: \left\{ \begin{array}{l} \text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^* \\ \text{polynomiaux par morceaux} \end{array} \right\} \rightarrow \mathbb{Z}$$

qui compte le nombre de tours autour de 0.

Soit \mathbf{R} un corps réel clos et soit $\mathbf{C} = \mathbf{R}[i]$ où $i^2 = -1$.

Nous allons construire une fonction

$$\text{ind}: \left\{ \begin{array}{l} \text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^* \\ \text{polynomiaux par morceaux} \end{array} \right\} \rightarrow \mathbb{Z}$$

qui compte le nombre de tours autour de 0.

Plus précisément :

Soit \mathbf{R} un corps réel clos et soit $\mathbf{C} = \mathbf{R}[i]$ où $i^2 = -1$.

Nous allons construire une fonction

$$\text{ind}: \left\{ \begin{array}{l} \text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^* \\ \text{polynomiaux par morceaux} \end{array} \right\} \rightarrow \mathbb{Z}$$

qui compte le nombre de tours autour de 0.

Plus précisément :

1 Pour tout rectangle $\Gamma \subset \mathbf{C}$ on a $\text{ind}(\partial\Gamma) = \begin{cases} 1 & \text{si } 0 \in \text{Int } \Gamma, \\ 0 & \text{si } 0 \in \mathbf{C} \setminus \Gamma. \end{cases}$

Soit \mathbf{R} un corps réel clos et soit $\mathbf{C} = \mathbf{R}[i]$ où $i^2 = -1$.

Nous allons construire une fonction

$$\text{ind}: \left\{ \begin{array}{l} \text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^* \\ \text{polynomiaux par morceaux} \end{array} \right\} \rightarrow \mathbb{Z}$$

qui compte le nombre de tours autour de 0.

Plus précisément :

- 1 Pour tout rectangle $\Gamma \subset \mathbf{C}$ on a $\text{ind}(\partial\Gamma) = \begin{cases} 1 & \text{si } 0 \in \text{Int } \Gamma, \\ 0 & \text{si } 0 \in \mathbf{C} \setminus \Gamma. \end{cases}$
- 2 $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.

Soit \mathbf{R} un corps réel clos et soit $\mathbf{C} = \mathbf{R}[i]$ où $i^2 = -1$.

Nous allons construire une fonction

$$\text{ind}: \left\{ \begin{array}{l} \text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^* \\ \text{polynomiaux par morceaux} \end{array} \right\} \rightarrow \mathbb{Z}$$

qui compte le nombre de tours autour de 0.

Plus précisément :

- 1 Pour tout rectangle $\Gamma \subset \mathbf{C}$ on a $\text{ind}(\partial\Gamma) = \begin{cases} 1 & \text{si } 0 \in \text{Int } \Gamma, \\ 0 & \text{si } 0 \in \mathbf{C} \setminus \Gamma. \end{cases}$
- 2 $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.
- 3 $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ sont homotopes dans \mathbf{C}^* .

Soit \mathbf{R} un corps réel clos et soit $\mathbf{C} = \mathbf{R}[i]$ où $i^2 = -1$.

Nous allons construire une fonction

$$\text{ind}: \left\{ \begin{array}{l} \text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^* \\ \text{polynomiaux par morceaux} \end{array} \right\} \rightarrow \mathbb{Z}$$

qui compte le nombre de tours autour de 0.

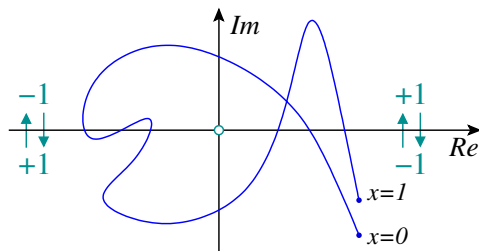
Plus précisément :

- 1 Pour tout rectangle $\Gamma \subset \mathbf{C}$ on a $\text{ind}(\partial\Gamma) = \begin{cases} 1 & \text{si } 0 \in \text{Int } \Gamma, \\ 0 & \text{si } 0 \in \mathbf{C} \setminus \Gamma. \end{cases}$
- 2 $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.
- 3 $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ sont homotopes dans \mathbf{C}^* .

Bénéfice algorithmique : l'indice se calcule par les suites de Sturm !

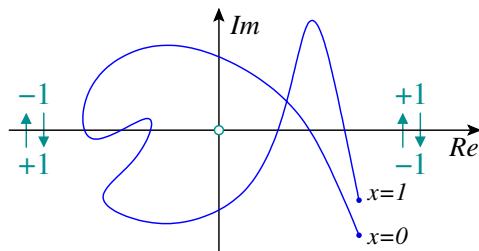
L'indice d'un chemin dans le plan complexe

Pour $F \in \mathbf{C}[X]$ la fonction $\gamma: [0, 1] \rightarrow \mathbf{C}, x \mapsto F(x)$ décrit un chemin dans \mathbf{C} .



L'indice d'un chemin dans le plan complexe

Pour $F \in \mathbf{C}[X]$ la fonction $\gamma: [0, 1] \rightarrow \mathbf{C}$, $x \mapsto F(x)$ décrit un chemin dans \mathbf{C} .

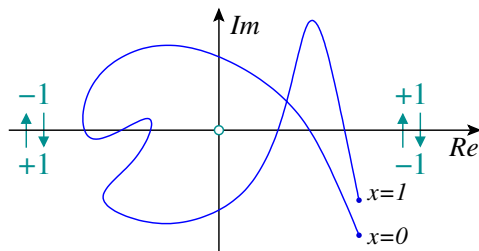


Observation

L'indice $\text{ind}_0^1(F) := \frac{1}{2} \text{Ind}_0^1\left(\frac{\text{re } F}{\text{im } F}\right)$ compte les tours autour de 0.

L'indice d'un chemin dans le plan complexe

Pour $F \in \mathbf{C}[X]$ la fonction $\gamma: [0, 1] \rightarrow \mathbf{C}$, $x \mapsto F(x)$ décrit un chemin dans \mathbf{C} .



Observation

L'indice $\text{ind}_0^1(F) := \frac{1}{2} \text{Ind}_0^1\left(\frac{\text{re } F}{\text{im } F}\right)$ compte les tours autour de 0.

Définition

Pour $F \in \mathbf{C}[Z]$ et $a, b \in \mathbf{C}$ on pose $\text{ind}_a^b(F) = \text{ind}_0^1 F((b-a)X + a)$.

L'indice par rapport à un rectangle

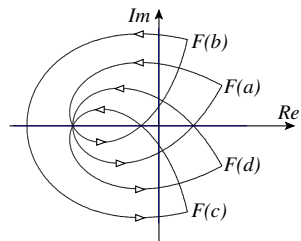
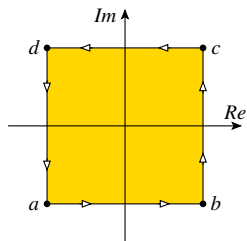


Illustration : $F = Z^5 - 5Z^4 - 2Z^3 - 2Z^2 - 3Z - 12$ sur $\Gamma = [-1, +1] \times [-1, +1]$.

L'indice par rapport à un rectangle

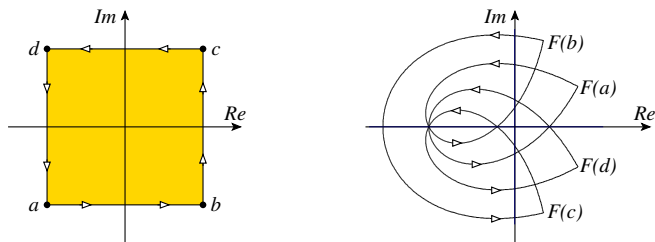


Illustration : $F = Z^5 - 5Z^4 - 2Z^3 - 2Z^2 - 3Z - 12$ sur $\Gamma = [-1, +1] \times [-1, +1]$.

Définition

Étant donné un polynôme $F \in \mathbf{C}[Z]$ et un rectangle $\Gamma \subset \mathbf{C}$, on pose

$$\text{ind}_{\partial\Gamma}(F) := \text{ind}_a^b(F) + \text{ind}_b^c(F) + \text{ind}_c^d(F) + \text{ind}_d^a(F).$$

L'indice par rapport à un rectangle

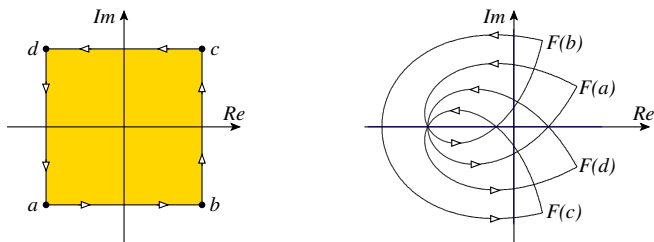


Illustration : $F = Z^5 - 5Z^4 - 2Z^3 - 2Z^2 - 3Z - 12$ sur $\Gamma = [-1, +1] \times [-1, +1]$.

Définition

Étant donné un polynôme $F \in \mathbf{C}[Z]$ et un rectangle $\Gamma \subset \mathbf{C}$, on pose

$$\text{ind}_{\partial\Gamma}(F) := \text{ind}_a^b(F) + \text{ind}_b^c(F) + \text{ind}_c^d(F) + \text{ind}_d^a(F).$$

Exemple

$$\text{ind}_{\partial\Gamma}(Z - z_0) = \begin{cases} 1 & \text{si } z_0 \text{ est dans l'intérieur de } \Gamma, \\ \frac{1}{2} & \text{si } z_0 \text{ est sur une arête de } \Gamma, \\ \frac{1}{4} & \text{si } z_0 \text{ est un sommet de } \Gamma, \\ 0 & \text{si } z_0 \text{ est à l'extérieur de } \Gamma. \end{cases}$$

La formule du produit

Pour $F = P + iQ$ et $G = R + iS$ on trouve $FG = (PR - QS) + i(PS + QR)$.

La formule du produit

Pour $F = P + iQ$ et $G = R + iS$ on trouve $FG = (PR - QS) + i(PS + QR)$.

Lemme

Si aucune des paires (P, Q) et (R, S) n'a de zéro commun en a ni en b , alors

$$\text{Ind}_a^b \left(\frac{PR - QS}{PS + QR} \right) = \text{Ind}_a^b \left(\frac{P}{Q} \right) + \text{Ind}_a^b \left(\frac{R}{S} \right) - V_a^b(1, QS(PS + QR)).$$

La formule du produit

Pour $F = P + iQ$ et $G = R + iS$ on trouve $FG = (PR - QS) + i(PS + QR)$.

Lemme

Si aucune des paires (P, Q) et (R, S) n'a de zéro commun en a ni en b , alors

$$\text{Ind}_a^b\left(\frac{PR - QS}{PS + QR}\right) = \text{Ind}_a^b\left(\frac{P}{Q}\right) + \text{Ind}_a^b\left(\frac{R}{S}\right) - V_a^b(1, QS(PS + QR)).$$

Théorème

Si $F, G \in \mathbf{C}[Z]$ ne s'annulent pas sur les sommets de $\Gamma \subset \mathbf{R}^2$, alors

$$\text{ind}_{\partial\Gamma}(F \cdot G) = \text{ind}_{\partial\Gamma}(F) + \text{ind}_{\partial\Gamma}(G).$$

La formule du produit

Pour $F = P + iQ$ et $G = R + iS$ on trouve $FG = (PR - QS) + i(PS + QR)$.

Lemme

Si aucune des paires (P, Q) et (R, S) n'a de zéro commun en a ni en b , alors

$$\text{Ind}_a^b\left(\frac{PR - QS}{PS + QR}\right) = \text{Ind}_a^b\left(\frac{P}{Q}\right) + \text{Ind}_a^b\left(\frac{R}{S}\right) - V_a^b(1, QS(PS + QR)).$$

Théorème

Si $F, G \in \mathbf{C}[Z]$ ne s'annulent pas sur les sommets de $\Gamma \subset \mathbf{R}^2$, alors

$$\text{ind}_{\partial\Gamma}(F \cdot G) = \text{ind}_{\partial\Gamma}(F) + \text{ind}_{\partial\Gamma}(G).$$

Corollaire

Supposons que $F \in \mathbf{C}[Z]$ soit scindé, $F = c(Z - z_1) \cdots (Z - z_n)$, et qu'aucune des racines z_1, \dots, z_n ne tombe sur un sommet de Γ . Alors $\text{ind}_{\partial\Gamma}(F)$ compte le nombre des racines dans Γ .

La formule du produit

Pour $F = P + iQ$ et $G = R + iS$ on trouve $FG = (PR - QS) + i(PS + QR)$.

Lemme

Si aucune des paires (P, Q) et (R, S) n'a de zéro commun en a ni en b , alors

$$\text{Ind}_a^b\left(\frac{PR - QS}{PS + QR}\right) = \text{Ind}_a^b\left(\frac{P}{Q}\right) + \text{Ind}_a^b\left(\frac{R}{S}\right) - V_a^b(1, QS(PS + QR)).$$

Théorème

Si $F, G \in \mathbf{C}[Z]$ ne s'annulent pas sur les sommets de $\Gamma \subset \mathbf{R}^2$, alors

$$\text{ind}_{\partial\Gamma}(F \cdot G) = \text{ind}_{\partial\Gamma}(F) + \text{ind}_{\partial\Gamma}(G).$$

Corollaire

Supposons que $F \in \mathbf{C}[Z]$ soit scindé, $F = c(Z - z_1) \cdots (Z - z_n)$, et qu'aucune des racines z_1, \dots, z_n ne tombe sur un sommet de Γ . Alors $\text{ind}_{\partial\Gamma}(F)$ compte le nombre des racines dans Γ .

Il faut encore s'affranchir de l'hypothèse que F soit scindé !

Lemme (version locale)

Si $F \in \mathbf{C}[X, Y]$ vérifie $F(x, y) \neq 0$ dans un point $(x, y) \in \mathbf{R}^2$, alors il existe $\delta > 0$ tel que $\text{ind}_{\partial\Gamma}(F) = 0$ pour tout $\Gamma \subset [x - \delta, x + \delta] \times [y - \delta, y + \delta]$.

Lemme (version locale)

Si $F \in \mathbf{C}[X, Y]$ vérifie $F(x, y) \neq 0$ dans un point $(x, y) \in \mathbf{R}^2$, alors il existe $\delta > 0$ tel que $\text{ind}_{\partial\Gamma}(F) = 0$ pour tout $\Gamma \subset [x - \delta, x + \delta] \times [y - \delta, y + \delta]$.

Théorème (version globale)

Soit $\Gamma = [x_0, x_1] \times [y_0, y_1]$ un rectangle dans \mathbf{C} . Si $F \in \mathbf{C}[X, Y]$ vérifie $F(x, y) \neq 0$ pour tout $(x, y) \in \Gamma$, alors $\text{ind}_{\partial\Gamma}(F) = 0$.

Lemme (version locale)

Si $F \in \mathbf{C}[X, Y]$ vérifie $F(x, y) \neq 0$ dans un point $(x, y) \in \mathbf{R}^2$, alors il existe $\delta > 0$ tel que $\text{ind}_{\partial\Gamma}(F) = 0$ pour tout $\Gamma \subset [x - \delta, x + \delta] \times [y - \delta, y + \delta]$.

Théorème (version globale)

Soit $\Gamma = [x_0, x_1] \times [y_0, y_1]$ un rectangle dans \mathbf{C} . Si $F \in \mathbf{C}[X, Y]$ vérifie $F(x, y) \neq 0$ pour tout $(x, y) \in \Gamma$, alors $\text{ind}_{\partial\Gamma}(F) = 0$.

Corollaire (comptage des racines)

Supposons que $F \in \mathbf{C}[Z]^$ ne s'annule pas dans les sommets de $\Gamma \subset \mathbf{C}$. Alors $\text{ind}_{\partial\Gamma}(F)$ compte les racines de F dans Γ .*

Démonstration. On factorise $F = (Z - z_1) \cdots (Z - z_m)G$

tel que le facteur restant $G \in \mathbf{C}[Z]^*$ n'ait pas de racines dans \mathbf{C} .

L'affirmation découle de la formule du produit et du théorème ci-dessus. \square

Définition (rayon de Cauchy)

Soit $F = a_n Z^n + a_{n-1} Z^{n-1} + \dots + a_1 Z + a_0$ dans $\mathbf{C}[Z]$ où $a_n \neq 0$.

On pose $M := \max\{0, |a_0|, \dots, |a_{n-1}|\}$ et on définit $\rho_F := 1 + M/|a_n|$.

Définition (rayon de Cauchy)

Soit $F = a_n Z^n + a_{n-1} Z^{n-1} + \dots + a_1 Z + a_0$ dans $\mathbf{C}[Z]$ où $a_n \neq 0$.

On pose $M := \max\{0, |a_0|, \dots, |a_{n-1}|\}$ et on définit $\rho_F := 1 + M/|a_n|$.

Théorème

Si $z \in \mathbf{C}$ vérifie $|z| \geq \rho_F$, alors $|F(z)| \geq |a_n| > 0$.

Définition (rayon de Cauchy)

Soit $F = a_n Z^n + a_{n-1} Z^{n-1} + \dots + a_1 Z + a_0$ dans $\mathbf{C}[Z]$ où $a_n \neq 0$.

On pose $M := \max\{0, |a_0|, \dots, |a_{n-1}|\}$ et on définit $\rho_F := 1 + M/|a_n|$.

Théorème

Si $z \in \mathbf{C}$ vérifie $|z| \geq \rho_F$, alors $|F(z)| \geq |a_n| > 0$.

Ainsi toutes les racines de F dans \mathbf{C} sont dans $B(\rho_F) = \{z \in \mathbf{C} \mid |z| < \rho_F\}$.

Théorème

Soit $F \in \mathbf{C}[T, Z]$. Supposons que pour tout $t \in [0, 1]$ le polynôme $F_t \in \mathbf{C}[Z]$ n'a pas de racines sur $\partial\Gamma$. Alors $\text{ind}_{\partial\Gamma}(F_0) = \text{ind}_{\partial\Gamma}(F_1)$.

Théorème

Soit $F \in \mathbf{C}[T, Z]$. Supposons que pour tout $t \in [0, 1]$ le polynôme $F_t \in \mathbf{C}[Z]$ n'a pas de racines sur $\partial\Gamma$. Alors $\text{ind}_{\partial\Gamma}(F_0) = \text{ind}_{\partial\Gamma}(F_1)$.

Démonstration. L'absence des zéros sur $[0, 1] \times [a, b]$ nous assure que

$$\text{ind}_a^b(F | T = 0) - \text{ind}_a^b(F | T = 1) = \text{ind}_0^1(F | Z = a) - \text{ind}_0^1(F | Z = b).$$

Théorème

Soit $F \in \mathbf{C}[T, Z]$. Supposons que pour tout $t \in [0, 1]$ le polynôme $F_t \in \mathbf{C}[Z]$ n'a pas de racines sur $\partial\Gamma$. Alors $\text{ind}_{\partial\Gamma}(F_0) = \text{ind}_{\partial\Gamma}(F_1)$.

Démonstration. L'absence des zéros sur $[0, 1] \times [a, b]$ nous assure que

$$\text{ind}_a^b(F | T = 0) - \text{ind}_a^b(F | T = 1) = \text{ind}_0^1(F | Z = a) - \text{ind}_0^1(F | Z = b).$$

La somme sur les quatre cotés de Γ donne $\text{ind}_{\partial\Gamma}(F_0) - \text{ind}_{\partial\Gamma}(F_1) = 0$. \square

Théorème

Soit $F \in \mathbf{C}[T, Z]$. Supposons que pour tout $t \in [0, 1]$ le polynôme $F_t \in \mathbf{C}[Z]$ n'a pas de racines sur $\partial\Gamma$. Alors $\text{ind}_{\partial\Gamma}(F_0) = \text{ind}_{\partial\Gamma}(F_1)$.

Démonstration. L'absence des zéros sur $[0, 1] \times [a, b]$ nous assure que

$$\text{ind}_a^b(F | T = 0) - \text{ind}_a^b(F | T = 1) = \text{ind}_0^1(F | Z = a) - \text{ind}_0^1(F | Z = b).$$

La somme sur les quatre cotés de Γ donne $\text{ind}_{\partial\Gamma}(F_0) - \text{ind}_{\partial\Gamma}(F_1) = 0$. \square

Corollaire

Pour tout polynôme $F \in \mathbf{C}[Z]^*$ et tout rectangle $\Gamma \subset \mathbf{C}$ contenant $B(\rho_F)$ nous avons $\text{ind}_{\partial\Gamma}(F) = \text{deg } F$.

Théorème

Soit $F \in \mathbf{C}[T, Z]$. Supposons que pour tout $t \in [0, 1]$ le polynôme $F_t \in \mathbf{C}[Z]$ n'a pas de racines sur $\partial\Gamma$. Alors $\text{ind}_{\partial\Gamma}(F_0) = \text{ind}_{\partial\Gamma}(F_1)$.

Démonstration. L'absence des zéros sur $[0, 1] \times [a, b]$ nous assure que

$$\text{ind}_a^b(F | T = 0) - \text{ind}_a^b(F | T = 1) = \text{ind}_0^1(F | Z = a) - \text{ind}_0^1(F | Z = b).$$

La somme sur les quatre cotés de Γ donne $\text{ind}_{\partial\Gamma}(F_0) - \text{ind}_{\partial\Gamma}(F_1) = 0$. \square

Corollaire

Pour tout polynôme $F \in \mathbf{C}[Z]^*$ et tout rectangle $\Gamma \subset \mathbf{C}$ contenant $B(\rho_F)$ nous avons $\text{ind}_{\partial\Gamma}(F) = \text{deg } F$.

Démonstration. Soit $F = a_n Z^n + a_{n-1} Z^{n-1} + \dots + a_0$ où $a_n \neq 0$.
On déforme $F_1 = F$ en $F_0 = a_n Z^n$ par $F_t = a_n Z^n + t(a_{n-1} Z^{n-1} + \dots + a_0)$.

Théorème

Soit $F \in \mathbf{C}[T, Z]$. Supposons que pour tout $t \in [0, 1]$ le polynôme $F_t \in \mathbf{C}[Z]$ n'a pas de racines sur $\partial\Gamma$. Alors $\text{ind}_{\partial\Gamma}(F_0) = \text{ind}_{\partial\Gamma}(F_1)$.

Démonstration. L'absence des zéros sur $[0, 1] \times [a, b]$ nous assure que

$$\text{ind}_a^b(F | T = 0) - \text{ind}_a^b(F | T = 1) = \text{ind}_0^1(F | Z = a) - \text{ind}_0^1(F | Z = b).$$

La somme sur les quatre cotés de Γ donne $\text{ind}_{\partial\Gamma}(F_0) - \text{ind}_{\partial\Gamma}(F_1) = 0$. \square

Corollaire

Pour tout polynôme $F \in \mathbf{C}[Z]^*$ et tout rectangle $\Gamma \subset \mathbf{C}$ contenant $B(\rho_F)$ nous avons $\text{ind}_{\partial\Gamma}(F) = \text{deg } F$.

Démonstration. Soit $F = a_n Z^n + a_{n-1} Z^{n-1} + \dots + a_0$ où $a_n \neq 0$. On déforme $F_1 = F$ en $F_0 = a_n Z^n$ par $F_t = a_n Z^n + t(a_{n-1} Z^{n-1} + \dots + a_0)$. Le rayon de Cauchy $r_t = 1 + tM/|a_n|$ décroît de $r_1 = \rho_F$ à $r_0 = 1$.

Théorème

Soit $F \in \mathbf{C}[T, Z]$. Supposons que pour tout $t \in [0, 1]$ le polynôme $F_t \in \mathbf{C}[Z]$ n'a pas de racines sur $\partial\Gamma$. Alors $\text{ind}_{\partial\Gamma}(F_0) = \text{ind}_{\partial\Gamma}(F_1)$.

Démonstration. L'absence des zéros sur $[0, 1] \times [a, b]$ nous assure que

$$\text{ind}_a^b(F | T = 0) - \text{ind}_a^b(F | T = 1) = \text{ind}_0^1(F | Z = a) - \text{ind}_0^1(F | Z = b).$$

La somme sur les quatre cotés de Γ donne $\text{ind}_{\partial\Gamma}(F_0) - \text{ind}_{\partial\Gamma}(F_1) = 0$. \square

Corollaire

Pour tout polynôme $F \in \mathbf{C}[Z]^*$ et tout rectangle $\Gamma \subset \mathbf{C}$ contenant $B(\rho_F)$ nous avons $\text{ind}_{\partial\Gamma}(F) = \text{deg } F$.

Démonstration. Soit $F = a_n Z^n + a_{n-1} Z^{n-1} + \dots + a_0$ où $a_n \neq 0$.

On déforme $F_1 = F$ en $F_0 = a_n Z^n$ par $F_t = a_n Z^n + t(a_{n-1} Z^{n-1} + \dots + a_0)$.

Le rayon de Cauchy $r_t = 1 + tM/|a_n|$ décroît de $r_1 = \rho_F$ à $r_0 = 1$.

Ainsi F_t n'a pas de racines sur $\partial\Gamma$, donc $\text{ind}_{\partial\Gamma}(F_1) = \text{ind}_{\partial\Gamma}(F_0) = n$. \square

Théorème

Soit $F \in \mathbf{C}[T, Z]$. Supposons que pour tout $t \in [0, 1]$ le polynôme $F_t \in \mathbf{C}[Z]$ n'a pas de racines sur $\partial\Gamma$. Alors $\text{ind}_{\partial\Gamma}(F_0) = \text{ind}_{\partial\Gamma}(F_1)$.

Démonstration. L'absence des zéros sur $[0, 1] \times [a, b]$ nous assure que

$$\text{ind}_a^b(F | T = 0) - \text{ind}_a^b(F | T = 1) = \text{ind}_0^1(F | Z = a) - \text{ind}_0^1(F | Z = b).$$

La somme sur les quatre cotés de Γ donne $\text{ind}_{\partial\Gamma}(F_0) - \text{ind}_{\partial\Gamma}(F_1) = 0$. \square

Corollaire

Pour tout polynôme $F \in \mathbf{C}[Z]^*$ et tout rectangle $\Gamma \subset \mathbf{C}$ contenant $B(\rho_F)$ nous avons $\text{ind}_{\partial\Gamma}(F) = \text{deg } F$.

Démonstration. Soit $F = a_n Z^n + a_{n-1} Z^{n-1} + \dots + a_0$ où $a_n \neq 0$.

On déforme $F_1 = F$ en $F_0 = a_n Z^n$ par $F_t = a_n Z^n + t(a_{n-1} Z^{n-1} + \dots + a_0)$.

Le rayon de Cauchy $r_t = 1 + tM/|a_n|$ décroît de $r_1 = \rho_F$ à $r_0 = 1$.

Ainsi F_t n'a pas de racines sur $\partial\Gamma$, donc $\text{ind}_{\partial\Gamma}(F_1) = \text{ind}_{\partial\Gamma}(F_0) = n$. \square

Ceci achève notre démonstration du théorème fondamental de l'algèbre :

Le rectangle $\Gamma \subset \mathbf{C}$ contient n racines de F .

- 1 Les trois types de preuve du théorème fondamental
- 2 Racines réelles d'un polynôme réel
- 3 Racines complexes d'un polynôme complexe
- 4 Aspects algorithmiques**
 - Localisation des racines complexes
 - Cross-over vers la méthode de Newton
 - Complexité algorithmique

Localisation des racines complexes

Soit \mathbf{R} un corps réel clos et soit $\mathbf{C} = \mathbf{R}[i]$ où $i^2 = -1$.

Localisation des racines complexes

Soit \mathbf{R} un corps réel clos et soit $\mathbf{C} = \mathbf{R}[i]$ où $i^2 = -1$.

On peut construire l'indice algébrique, ayant les bonnes propriétés,

$$\text{ind}: \left\{ \begin{array}{l} \text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^* \\ \text{polynomiaux par morceaux} \end{array} \right\} \rightarrow \mathbb{Z}.$$

Localisation des racines complexes

Soit \mathbf{R} un corps réel clos et soit $\mathbf{C} = \mathbf{R}[i]$ où $i^2 = -1$.

On peut construire l'indice algébrique, ayant les bonnes propriétés,

$$\text{ind}: \left\{ \begin{array}{l} \text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^* \\ \text{polynomiaux par morceaux} \end{array} \right\} \rightarrow \mathbb{Z}.$$

La construction est réelle algébrique.

\implies arithmétique des polynômes au lieu de l'analyse

\implies calcul formel au lieu de calcul numérique

Localisation des racines complexes

Soit \mathbf{R} un corps réel clos et soit $\mathbf{C} = \mathbf{R}[i]$ où $i^2 = -1$.

On peut construire l'indice algébrique, ayant les bonnes propriétés,

$$\text{ind}: \left\{ \begin{array}{l} \text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^* \\ \text{polynomiaux par morceaux} \end{array} \right\} \rightarrow \mathbb{Z}.$$

La construction est réelle algébrique.

\implies arithmétique des polynômes au lieu de l'analyse

\implies calcul formel au lieu de calcul numérique

Cet outil permet de prouver le théorème fondamental de l'algèbre :

Le corps \mathbf{C} est algébriquement clos.

Localisation des racines complexes

Soit \mathbf{R} un corps réel clos et soit $\mathbf{C} = \mathbf{R}[i]$ où $i^2 = -1$.

On peut construire l'indice algébrique, ayant les bonnes propriétés,

$$\text{ind}: \left\{ \begin{array}{l} \text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^* \\ \text{polynomiaux par morceaux} \end{array} \right\} \rightarrow \mathbb{Z}.$$

La construction est réelle algébrique.

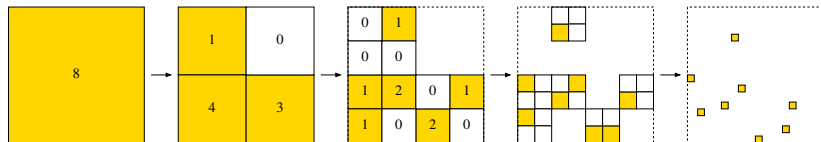
\implies arithmétique des polynômes au lieu de l'analyse

\implies calcul formel au lieu de calcul numérique

Cet outil permet de prouver le théorème fondamental de l'algèbre :

Le corps \mathbf{C} est algébriquement clos.

Mieux, l'indice permet de localiser les racines de tout polynôme $F \in \mathbb{C}[Z]$:



Localisation des racines complexes

Soit \mathbf{R} un corps réel clos et soit $\mathbf{C} = \mathbf{R}[i]$ où $i^2 = -1$.

On peut construire l'indice algébrique, ayant les bonnes propriétés,

$$\text{ind}: \left\{ \begin{array}{l} \text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^* \\ \text{polynomiaux par morceaux} \end{array} \right\} \rightarrow \mathbb{Z}.$$

La construction est réelle algébrique.

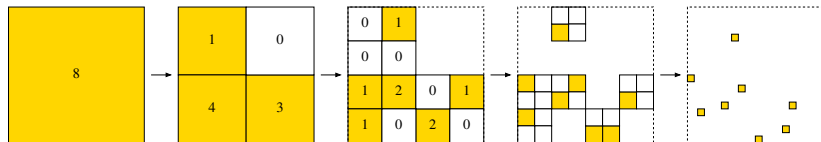
\implies arithmétique des polynômes au lieu de l'analyse

\implies calcul formel au lieu de calcul numérique

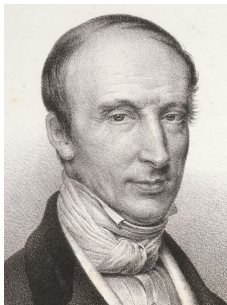
Cet outil permet de prouver le théorème fondamental de l'algèbre :

Le corps \mathbf{C} est algébriquement clos.

Mieux, l'indice permet de localiser les racines de tout polynôme $F \in \mathbb{C}[Z]$:



Dès qu'on a bien séparé les racines, on passe à la méthode de Newton.



Je vous remercie de votre attention !