

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

Michael Eisermann

Institut Fourier, Université Grenoble I
www-fourier.ujf-grenoble.fr/~eiserm

23 janvier 2009



Carl Friedrich Gauß (1777–1855)



Augustin Louis Cauchy (1789–1857)



Charles-François Sturm (1803–1855)

Séminaire de calcul formel et complexité, Université Rennes I

- 1 Le théorème fondamental de l'algèbre
- 2 Sturm 1829/1835 : racines réelles de polynômes réels
- 3 Sturm 1836 : racines complexes de polynômes complexes
- 4 Conclusions et perspectives

- 1** Le théorème fondamental de l'algèbre
 - Le théorème et son histoire
 - Racines réelles de polynômes réels
 - Racines complexes de polynômes complexes
- 2 Sturm 1829/1835 : racines réelles de polynômes réels
- 3 Sturm 1836 : racines complexes de polynômes complexes
- 4 Conclusions et perspectives

Théorème (version brève)

Tout polynôme complexe de degré n admet n racines complexes.

Le théorème fondamental de l'algèbre

Théorème (version brève)

Tout polynôme complexe de degré n admet n racines complexes.

Théorème (version longue)

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

Théorème (version brève)

Tout polynôme complexe de degré n admet n racines complexes.

Théorème (version longue)

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

Alors pour tout polynôme

$$F = Z^n + c_1 Z^{n-1} + \cdots + c_{n-1} Z + c_n$$

à coefficients $c_1, \dots, c_{n-1}, c_n \in \mathbb{C}$

Théorème (version brève)

Tout polynôme complexe de degré n admet n racines complexes.

Théorème (version longue)

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

Alors pour tout polynôme

$$F = Z^n + c_1 Z^{n-1} + \cdots + c_{n-1} Z + c_n$$

à coefficients $c_1, \dots, c_{n-1}, c_n \in \mathbb{C}$ il existe $z_1, z_2, \dots, z_n \in \mathbb{C}$ tels que

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

Théorème (version brève)

Tout polynôme complexe de degré n admet n racines complexes.

Théorème (version longue)

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

Alors pour tout polynôme

$$F = Z^n + c_1 Z^{n-1} + \cdots + c_{n-1} Z + c_n$$

à coefficients $c_1, \dots, c_{n-1}, c_n \in \mathbb{C}$ il existe $z_1, z_2, \dots, z_n \in \mathbb{C}$ tels que

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

Questions naturelles :

Théorème (version brève)

Tout polynôme complexe de degré n admet n racines complexes.

Théorème (version longue)

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

Alors pour tout polynôme

$$F = Z^n + c_1 Z^{n-1} + \cdots + c_{n-1} Z + c_n$$

à coefficients $c_1, \dots, c_{n-1}, c_n \in \mathbb{C}$ il existe $z_1, z_2, \dots, z_n \in \mathbb{C}$ tels que

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

Questions naturelles :

- Existe-t-il une démonstration élémentaire ? qui capte la géométrie ?

Théorème (version brève)

Tout polynôme complexe de degré n admet n racines complexes.

Théorème (version longue)

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

Alors pour tout polynôme

$$F = Z^n + c_1 Z^{n-1} + \cdots + c_{n-1} Z + c_n$$

à coefficients $c_1, \dots, c_{n-1}, c_n \in \mathbb{C}$ il existe $z_1, z_2, \dots, z_n \in \mathbb{C}$ tels que

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

Questions naturelles :

- Existe-t-il une démonstration élémentaire ? qui capte la géométrie ?
- Peut-on affaiblir l'hypothèse ? à quels corps ordonnés au lieu de \mathbb{R} ?

Théorème (version brève)

Tout polynôme complexe de degré n admet n racines complexes.

Théorème (version longue)

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

Alors pour tout polynôme

$$F = Z^n + c_1 Z^{n-1} + \cdots + c_{n-1} Z + c_n$$

à coefficients $c_1, \dots, c_{n-1}, c_n \in \mathbb{C}$ il existe $z_1, z_2, \dots, z_n \in \mathbb{C}$ tels que

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

Questions naturelles :

- Existe-t-il une démonstration élémentaire ? qui capte la géométrie ?
- Peut-on affaiblir l'hypothèse ? à quels corps ordonnés au lieu de \mathbb{R} ?
- Peut-on renforcer la conclusion ? la rendre effective ?

Stratégies de preuve

On connaît trois stratégies de preuve :

On connaît trois stratégies de preuve :

- 1 Analyse : compacité, fonctions analytiques, intégration, Stokes, ...
(d'Alembert 1746, Argand 1814, Cauchy 1820) ;

On connaît trois stratégies de preuve :

- 1 Analyse : compacité, fonctions analytiques, intégration, Stokes, ...
(d'Alembert 1746, Argand 1814, Cauchy 1820) ;
- 2 Algèbre : TVI pour polynômes, fonctions symétriques / théorie de Galois
(Euler 1749, Lagrange 1772, Laplace 1795, Gauß 1816) ;

On connaît trois stratégies de preuve :

- 1 Analyse : compacité, fonctions analytiques, intégration, Stokes, ...
(d'Alembert 1746, Argand 1814, Cauchy 1820) ;
- 2 Algèbre : TVI pour polynômes, fonctions symétriques / théorie de Galois
(Euler 1749, Lagrange 1772, Laplace 1795, Gauß 1816) ;
- 3 Topologie algébrique : notion d'indice [*winding number*]
(Gauß 1799/1816, Cauchy 1831, Sturm–Liouville 1836)

On connaît trois stratégies de preuve :

- 1 Analyse : compacité, fonctions analytiques, intégration, Stokes, ... (d'Alembert 1746, Argand 1814, Cauchy 1820) ;
- 2 Algèbre : TVI pour polynômes, fonctions symétriques / théorie de Galois (Euler 1749, Lagrange 1772, Laplace 1795, Gauß 1816) ;
- 3 Topologie algébrique : notion d'indice [*winding number*] (Gauß 1799/1816, Cauchy 1831, Sturm–Liouville 1836)

La preuve présentée ici est *réelle algébrique* et se situe entre 2 et 3.

On connaît trois stratégies de preuve :

- 1 Analyse : compacité, fonctions analytiques, intégration, Stokes, ... (d'Alembert 1746, Argand 1814, Cauchy 1820) ;
- 2 Algèbre : TVI pour polynômes, fonctions symétriques / théorie de Galois (Euler 1749, Lagrange 1772, Laplace 1795, Gauß 1816) ;
- 3 Topologie algébrique : notion d'indice [*winding number*] (Gauß 1799/1816, Cauchy 1831, Sturm–Liouville 1836)

La preuve présentée ici est *réelle algébrique* et se situe entre 2 et 3.

Cette preuve réelle algébrique, qu'est-ce qu'elle offre d'intéressant ?

On connaît trois stratégies de preuve :

- 1 Analyse : compacité, fonctions analytiques, intégration, Stokes, ... (d'Alembert 1746, Argand 1814, Cauchy 1820) ;
- 2 Algèbre : TVI pour polynômes, fonctions symétriques / théorie de Galois (Euler 1749, Lagrange 1772, Laplace 1795, Gauß 1816) ;
- 3 Topologie algébrique : notion d'indice [*winding number*] (Gauß 1799/1816, Cauchy 1831, Sturm–Liouville 1836)

La preuve présentée ici est *réelle algébrique* et se situe entre 2 et 3.

Cette preuve réelle algébrique, qu'est-ce qu'elle offre d'intéressant ?

- ✓ Elle est élémentaire : arithmétique + TVI des polynômes réels.

On connaît trois stratégies de preuve :

- 1 Analyse : compacité, fonctions analytiques, intégration, Stokes, ... (d'Alembert 1746, Argand 1814, Cauchy 1820) ;
- 2 Algèbre : TVI pour polynômes, fonctions symétriques / théorie de Galois (Euler 1749, Lagrange 1772, Laplace 1795, Gauß 1816) ;
- 3 Topologie algébrique : notion d'indice [*winding number*] (Gauß 1799/1816, Cauchy 1831, Sturm–Liouville 1836)

La preuve présentée ici est *réelle algébrique* et se situe entre 2 et 3.

Cette preuve réelle algébrique, qu'est-ce qu'elle offre d'intéressant ?

- ✓ Elle est élémentaire : arithmétique + TVI des polynômes réels.
- ✓ Tous les arguments sont valables sur un corps réel clos.

On connaît trois stratégies de preuve :

- 1 Analyse : compacité, fonctions analytiques, intégration, Stokes, ... (d'Alembert 1746, Argand 1814, Cauchy 1820) ;
- 2 Algèbre : TVI pour polynômes, fonctions symétriques / théorie de Galois (Euler 1749, Lagrange 1772, Laplace 1795, Gauß 1816) ;
- 3 Topologie algébrique : notion d'indice [*winding number*] (Gauß 1799/1816, Cauchy 1831, Sturm–Liouville 1836)

La preuve présentée ici est *réelle algébrique* et se situe entre 2 et 3.

Cette preuve réelle algébrique, qu'est-ce qu'elle offre d'intéressant ?

- ✓ Elle est élémentaire : arithmétique + TVI des polynômes réels.
- ✓ Tous les arguments sont valables sur un corps réel clos.
- ✓ La preuve est constructive : elle permet de localiser les racines.

On connaît trois stratégies de preuve :

- 1 Analyse : compacité, fonctions analytiques, intégration, Stokes, ... (d'Alembert 1746, Argand 1814, Cauchy 1820) ;
- 2 Algèbre : TVI pour polynômes, fonctions symétriques / théorie de Galois (Euler 1749, Lagrange 1772, Laplace 1795, Gauß 1816) ;
- 3 Topologie algébrique : notion d'indice [*winding number*] (Gauß 1799/1816, Cauchy 1831, Sturm–Liouville 1836)

La preuve présentée ici est *réelle algébrique* et se situe entre 2 et 3.

Cette preuve réelle algébrique, qu'est-ce qu'elle offre d'intéressant ?

- ✓ Elle est élémentaire : arithmétique + TVI des polynômes réels.
- ✓ Tous les arguments sont valables sur un corps réel clos.
- ✓ La preuve est constructive : elle permet de localiser les racines.
- ✓ L'algorithme est facile à implémenter et suffisamment efficace.

On connaît trois stratégies de preuve :

- 1 Analyse : compacité, fonctions analytiques, intégration, Stokes, ... (d'Alembert 1746, Argand 1814, Cauchy 1820) ;
- 2 Algèbre : TVI pour polynômes, fonctions symétriques / théorie de Galois (Euler 1749, Lagrange 1772, Laplace 1795, Gauß 1816) ;
- 3 Topologie algébrique : notion d'indice [*winding number*] (Gauß 1799/1816, Cauchy 1831, Sturm–Liouville 1836)

La preuve présentée ici est *réelle algébrique* et se situe entre 2 et 3.

Cette preuve réelle algébrique, qu'est-ce qu'elle offre d'intéressant ?

- ✓ Elle est élémentaire : arithmétique + TVI des polynômes réels.
- ✓ Tous les arguments sont valables sur un corps réel clos.
- ✓ La preuve est constructive : elle permet de localiser les racines.
- ✓ L'algorithme est facile à implémenter et suffisamment efficace.
- ✓ Démonstration formelle du théorème et de l'algorithme.

On connaît trois stratégies de preuve :

- 1 Analyse : compacité, fonctions analytiques, intégration, Stokes, ... (d'Alembert 1746, Argand 1814, Cauchy 1820) ;
- 2 Algèbre : TVI pour polynômes, fonctions symétriques / théorie de Galois (Euler 1749, Lagrange 1772, Laplace 1795, Gauß 1816) ;
- 3 Topologie algébrique : notion d'indice [*winding number*] (Gauß 1799/1816, Cauchy 1831, Sturm–Liouville 1836)

La preuve présentée ici est *réelle algébrique* et se situe entre 2 et 3.

Cette preuve réelle algébrique, qu'est-ce qu'elle offre d'intéressant ?

- ✓ Elle est élémentaire : arithmétique + TVI des polynômes réels.
- ✓ Tous les arguments sont valables sur un corps réel clos.
- ✓ La preuve est constructive : elle permet de localiser les racines.
- ✓ L'algorithme est facile à implémenter et suffisamment efficace.
- ✓ Démonstration formelle du théorème et de l'algorithme.

Sous des hypothèses minimales nous obtenons des conclusions maximales.

Théorème (caractérisation des nombres réels)

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

Théorème (caractérisation des nombres réels)

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

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

Théorème (caractérisation des nombres réels)

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 (caractérisation des nombres réels)

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 (caractérisation des nombres réels)

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 :*

Théorème (caractérisation des nombres réels)

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 (caractérisation des nombres réels)

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 (caractérisation des nombres réels)

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 (caractérisation des nombres réels)

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} .

Ceci nécessite la logique de second ordre.

Théorème (caractérisation des nombres réels)

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} .

Ceci nécessite la logique de second ordre. Beaucoup moins suffira :

Théorème (caractérisation des nombres réels)

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} .

Ceci nécessite la logique de second ordre. Beaucoup moins suffira :

Définition (corps réel clos)

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

Théorème (caractérisation des nombres réels)

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} .

Ceci nécessite la logique de second ordre. Beaucoup moins suffira :

Définition (corps réel clos)

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

Exemples : les nombres réels \mathbb{R} , les réels algébriques $\mathbb{Q}^c \subset \mathbb{R}$, ...

Théorème (caractérisation des nombres réels)

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} .

Ceci nécessite la logique de second ordre. Beaucoup moins suffira :

Définition (corps réel clos)

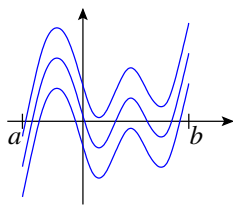
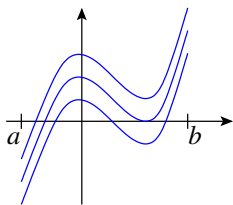
Un corps ordonné $(\mathbf{R}, +, \cdot, \leq)$ est dit *réel clos* si tout polynôme $P \in \mathbf{R}[X]$ satisfait à la propriété des valeurs intermédiaires sur \mathbf{R} .

Exemples : les nombres réels \mathbb{R} , les réels algébriques $\mathbb{Q}^c \subset \mathbb{R}$, ...

Tout corps ordonné admet une unique clôture réelle. Exemple : $\mathbb{R}(X)^c$.

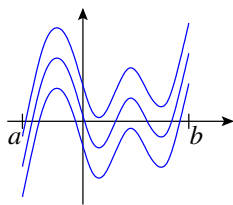
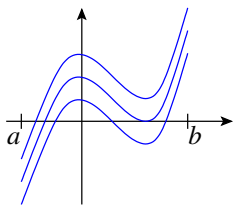
Racines réelles de polynômes réels

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



Racines réelles de polynômes réels

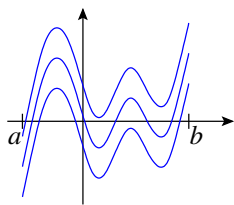
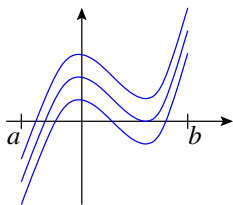
Comment déterminer/majorer le nombre de racines de $P \in \mathbf{R}[X]$ dans $[a, b]$?



Réponses partielles par Descartes (1596-1650), Fourier (1768-1830), ...

Racines réelles de polynômes réels

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



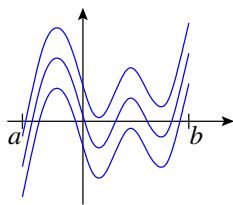
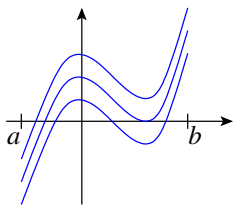
Réponses partielles par Descartes (1596-1650), Fourier (1768-1830), ...

Théorème de Sturm (1829/35)

Si \mathbf{R} est réel clos, alors $\#\{x \in [a, b] \mid P(x) = 0\} = V_a^b(S_0, S_1, \dots, S_n)$.

Racines réelles de polynômes réels

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



Réponses partielles par Descartes (1596-1650), Fourier (1768-1830), ...

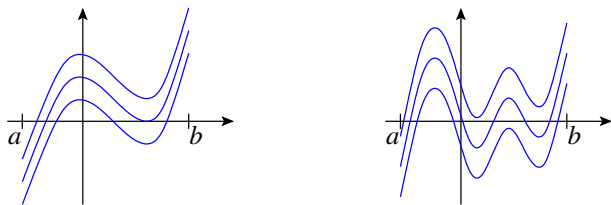
Théorème de Sturm (1829/35)

Si \mathbf{R} est réel clos, alors $\#\{x \in [a, b] \mid P(x) = 0\} = V_a^b(S_0, S_1, \dots, S_n)$.

Ici la suite S_0, S_1, \dots, S_n est obtenue de $S_0 = P$ et $S_1 = P'$ par division euclidienne itérée, $S_{k-1} = Q_k S_k - S_{k+1}$, jusqu'à ce que $S_{n+1} = 0$.

Racines réelles de polynômes réels

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



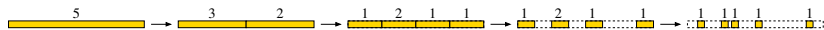
Réponses partielles par Descartes (1596-1650), Fourier (1768-1830), ...

Théorème de Sturm (1829/35)

Si \mathbf{R} est réel clos, alors $\#\{x \in [a, b] \mid P(x) = 0\} = V_a^b(S_0, S_1, \dots, S_n)$.

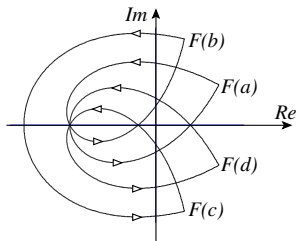
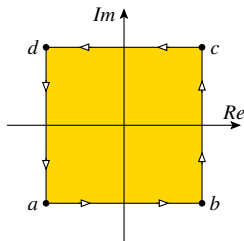
Ici la suite S_0, S_1, \dots, S_n est obtenue de $S_0 = P$ et $S_1 = P'$ par division euclidienne itérée, $S_{k-1} = Q_k S_k - S_{k+1}$, jusqu'à ce que $S_{n+1} = 0$.

Ce théorème permet de compter puis de localiser toutes les racines réelles :



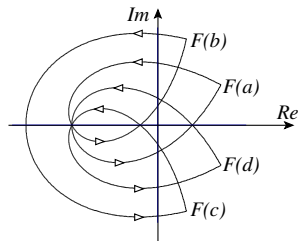
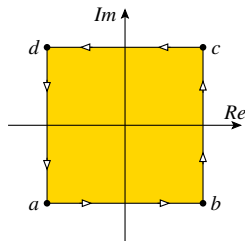
L'indice complexe : motivation géométrique

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



L'indice complexe : motivation géométrique

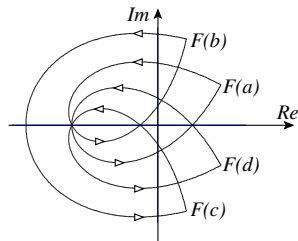
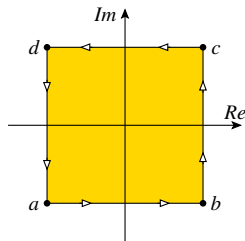
Exemple : $F = Z^5 - 5Z^4 - 2Z^3 - 2Z^2 - 3Z - 12$ et $\Gamma = [-1, +1] \times [-1, +1]$.



Idée géométrique (Gauß 1799) :

L'indice complexe : motivation géométrique

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

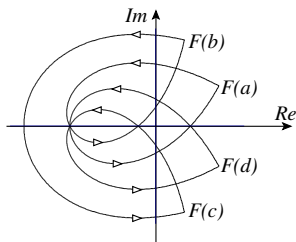
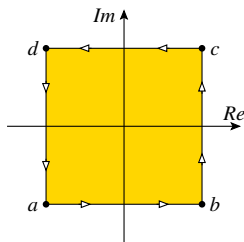


Idée géométrique (Gauß 1799) :

On définit $\text{ind}(F|_{\partial\Gamma})$ comme le nombre des tours de $F|_{\partial\Gamma}$ autour de 0.

L'indice complexe : motivation géométrique

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



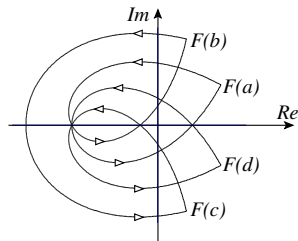
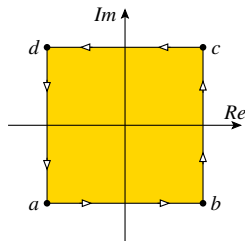
Idée géométrique (Gauß 1799) :

On définit $\text{ind}(F|_{\partial\Gamma})$ comme le nombre des tours de $F|_{\partial\Gamma}$ autour de 0.

- Si Γ est grand, alors $\text{ind}(F|_{\partial\Gamma}) = \text{ind}(Z^n|_{\partial\Gamma}) = n$.

L'indice complexe : motivation géométrique

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



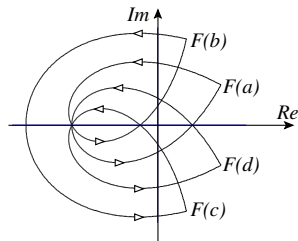
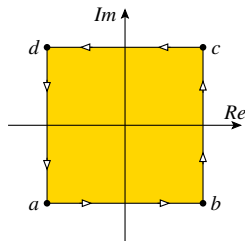
Idée géométrique (Gauß 1799) :

On définit $\text{ind}(F|_{\partial\Gamma})$ comme le nombre des tours de $F|_{\partial\Gamma}$ autour de 0.

- Si Γ est grand, alors $\text{ind}(F|_{\partial\Gamma}) = \text{ind}(Z^n|_{\partial\Gamma}) = n$.
- Si Γ est petit, alors $\text{ind}(F|_{\partial\Gamma}) = \text{ind}(\text{const}|_{\partial\Gamma}) = 0$.

L'indice complexe : motivation géométrique

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



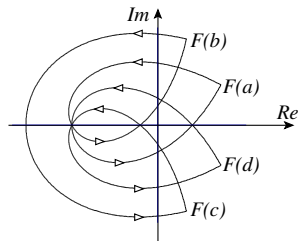
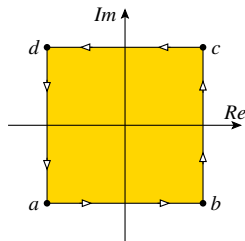
Idée géométrique (Gauß 1799) :

On définit $\text{ind}(F|_{\partial\Gamma})$ comme le nombre des tours de $F|_{\partial\Gamma}$ autour de 0.

- Si Γ est grand, alors $\text{ind}(F|_{\partial\Gamma}) = \text{ind}(Z^n|_{\partial\Gamma}) = n$.
- Si Γ est petit, alors $\text{ind}(F|_{\partial\Gamma}) = \text{ind}(\text{const}|_{\partial\Gamma}) = 0$.
- L'indice ne change que si $F|_{\partial\Gamma}$ passe par 0.

L'indice complexe : motivation géométrique

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



Idee géométrique (Gauß 1799) :

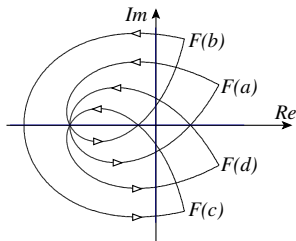
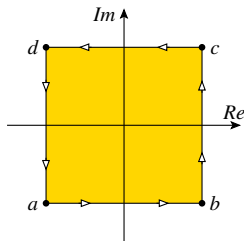
On définit $\text{ind}(F|_{\partial\Gamma})$ comme le nombre des tours de $F|_{\partial\Gamma}$ autour de 0.

- Si Γ est grand, alors $\text{ind}(F|_{\partial\Gamma}) = \text{ind}(Z^n|_{\partial\Gamma}) = n$.
- Si Γ est petit, alors $\text{ind}(F|_{\partial\Gamma}) = \text{ind}(\text{const}|_{\partial\Gamma}) = 0$.
- L'indice ne change que si $F|_{\partial\Gamma}$ passe par 0.

Par conséquent, en degré $n \geq 1$, le polynôme F doit avoir une racine.

L'indice complexe : motivation géométrique

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



Idee géométrique (Gauß 1799) :

On définit $\text{ind}(F|_{\partial\Gamma})$ comme le nombre des tours de $F|_{\partial\Gamma}$ autour de 0.

- Si Γ est grand, alors $\text{ind}(F|_{\partial\Gamma}) = \text{ind}(Z^n|_{\partial\Gamma}) = n$.
- Si Γ est petit, alors $\text{ind}(F|_{\partial\Gamma}) = \text{ind}(\text{const}|_{\partial\Gamma}) = 0$.
- L'indice ne change que si $F|_{\partial\Gamma}$ passe par 0.

Par conséquent, en degré $n \geq 1$, le polynôme F doit avoir une racine.

Problème technique : Comment définir rigoureusement cet indice ?

L'indice complexe : propriétés algébriques

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

L'indice complexe : propriétés algébriques

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

Soit $\Omega = \{\text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^*, \gamma(0) = \gamma(1), \text{ polynomiaux par morceaux}\}$.

L'indice complexe : propriétés algébriques

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

Soit $\Omega = \{\text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^*, \gamma(0) = \gamma(1), \text{ polynomiaux par morceaux}\}$.

Théorème

Il existe une application $\text{ind}: \Omega \rightarrow \mathbb{Z}$ ayant les propriétés suivantes :

L'indice complexe : propriétés algébriques

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

Soit $\Omega = \{\text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^*, \gamma(0) = \gamma(1), \text{ polynomiaux par morceaux}\}$.

Théorème

Il existe une application $\text{ind}: \Omega \rightarrow \mathbb{Z}$ ayant les propriétés suivantes :

- 0** *Calculabilité : $\text{ind}(\gamma)$ se calcule par l'algorithme de Sturm sur \mathbf{R} .*

L'indice complexe : propriétés algébriques

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

Soit $\Omega = \{\text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^*, \gamma(0) = \gamma(1), \text{ polynomiaux par morceaux}\}$.

Théorème

Il existe une application $\text{ind}: \Omega \rightarrow \mathbb{Z}$ ayant les propriétés suivantes :

- 0** *Calculabilité : $\text{ind}(\gamma)$ se calcule par l'algorithme de Sturm sur \mathbf{R} .*
- 1** *Normalisation : Pour tout rectangle $\Gamma \subset \mathbf{C}$ on a*

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

L'indice complexe : propriétés algébriques

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

Soit $\Omega = \{\text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^*, \gamma(0) = \gamma(1), \text{ polynomiaux par morceaux}\}$.

Théorème

Il existe une application $\text{ind}: \Omega \rightarrow \mathbb{Z}$ ayant les propriétés suivantes :

0 *Calculabilité* : $\text{ind}(\gamma)$ se calcule par l'algorithme de Sturm sur \mathbf{R} .

1 *Normalisation* : 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 *Multiplicativité* : $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.

L'indice complexe : propriétés algébriques

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

Soit $\Omega = \{\text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^*, \gamma(0) = \gamma(1), \text{ polynomiaux par morceaux}\}$.

Théorème

Il existe une application $\text{ind}: \Omega \rightarrow \mathbb{Z}$ ayant les propriétés suivantes :

0 *Calculabilité : $\text{ind}(\gamma)$ se calcule par l'algorithme de Sturm sur \mathbf{R} .*

1 *Normalisation : 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 *Multiplicativité : $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.*

3 *Invariance par homotopie : $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ dans \mathbf{C}^* .*

L'indice complexe : propriétés algébriques

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

Soit $\Omega = \{\text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^*, \gamma(0) = \gamma(1), \text{ polynomiaux par morceaux}\}$.

Théorème

Il existe une application $\text{ind}: \Omega \rightarrow \mathbb{Z}$ ayant les propriétés suivantes :

0 *Calculabilité* : $\text{ind}(\gamma)$ se calcule par l'algorithme de Sturm sur \mathbf{R} .

1 *Normalisation* : 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 *Multiplicativité* : $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.

3 *Invariance par homotopie* : $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ dans \mathbf{C}^* .

La difficulté réside dans la *construction* !

L'indice complexe : propriétés algébriques

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

Soit $\Omega = \{\text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^*, \gamma(0) = \gamma(1), \text{ polynomiaux par morceaux}\}$.

Théorème

Il existe une application $\text{ind}: \Omega \rightarrow \mathbb{Z}$ ayant les propriétés suivantes :

0 *Calculabilité* : $\text{ind}(\gamma)$ se calcule par l'algorithme de Sturm sur \mathbf{R} .

1 *Normalisation* : 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 *Multiplicativité* : $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.

3 *Invariance par homotopie* : $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ dans \mathbf{C}^* .

La difficulté réside dans la *construction* ! Tous les moyens sont bons :

L'indice complexe : propriétés algébriques

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

Soit $\Omega = \{\text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^*, \gamma(0) = \gamma(1), \text{ polynomiaux par morceaux}\}$.

Théorème

Il existe une application $\text{ind}: \Omega \rightarrow \mathbb{Z}$ ayant les propriétés suivantes :

0 *Calculabilité* : $\text{ind}(\gamma)$ se calcule par l'algorithme de Sturm sur \mathbf{R} .

1 *Normalisation* : 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 *Multiplicativité* : $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.

3 *Invariance par homotopie* : $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ dans \mathbf{C}^* .

La difficulté réside dans la *construction* ! Tous les moyens sont bons :

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

L'indice complexe : propriétés algébriques

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

Soit $\Omega = \{\text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^*, \gamma(0) = \gamma(1), \text{ polynomiaux par morceaux}\}$.

Théorème

Il existe une application $\text{ind}: \Omega \rightarrow \mathbb{Z}$ ayant les propriétés suivantes :

0 *Calculabilité* : $\text{ind}(\gamma)$ se calcule par l'algorithme de Sturm sur \mathbf{R} .

1 *Normalisation* : 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 *Multiplicativité* : $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.

3 *Invariance par homotopie* : $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ dans \mathbf{C}^* .

La difficulté réside dans la *construction* ! Tous les moyens sont bons :

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

L'indice complexe : propriétés algébriques

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

Soit $\Omega = \{\text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^*, \gamma(0) = \gamma(1), \text{ polynomiaux par morceaux}\}$.

Théorème

Il existe une application $\text{ind}: \Omega \rightarrow \mathbb{Z}$ ayant les propriétés suivantes :

0 *Calculabilité* : $\text{ind}(\gamma)$ se calcule par l'algorithme de Sturm sur \mathbf{R} .

1 *Normalisation* : 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 *Multiplicativité* : $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.

3 *Invariance par homotopie* : $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ dans \mathbf{C}^* .

La difficulté réside dans la *construction* ! Tous les moyens sont bons :

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

L'indice complexe : propriétés algébriques

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

Soit $\Omega = \{\text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^*, \gamma(0) = \gamma(1), \text{ polynomiaux par morceaux}\}$.

Théorème

Il existe une application $\text{ind}: \Omega \rightarrow \mathbb{Z}$ ayant les propriétés suivantes :

0 *Calculabilité* : $\text{ind}(\gamma)$ se calcule par l'algorithme de Sturm sur \mathbf{R} .

1 *Normalisation* : 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 *Multiplicativité* : $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.

3 *Invariance par homotopie* : $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ dans \mathbf{C}^* .

La difficulté réside dans la *construction* ! Tous les moyens sont bons :

- Théorie des revêtements, appliquée à $\exp: \mathbb{C} \rightarrow \mathbb{C}^*$ avec groupe \mathbb{Z} .
- 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.
- Topologie différentielle, théorème de Sard et degré topologique.

L'indice complexe : propriétés algébriques

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

Soit $\Omega = \{\text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^*, \gamma(0) = \gamma(1), \text{ polynomiaux par morceaux}\}$.

Théorème

Il existe une application $\text{ind}: \Omega \rightarrow \mathbb{Z}$ ayant les propriétés suivantes :

0 *Calculabilité* : $\text{ind}(\gamma)$ se calcule par l'algorithme de Sturm sur \mathbf{R} .

1 *Normalisation* : 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 *Multiplicativité* : $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.

3 *Invariance par homotopie* : $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ dans \mathbf{C}^* .

La difficulté réside dans la *construction* ! Tous les moyens sont bons :

- Théorie des revêtements, appliquée à $\exp: \mathbb{C} \rightarrow \mathbb{C}^*$ avec groupe \mathbb{Z} .
- 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.
- Topologie différentielle, théorème de Sard et degré topologique.
- Analyse complexe, indice analytique $\text{ind}(\gamma) = \frac{1}{2i\pi} \int_{\gamma} \frac{dz}{z}$.

L'indice complexe : propriétés algébriques

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

Soit $\Omega = \{\text{lacets } \gamma: [0, 1] \rightarrow \mathbf{C}^*, \gamma(0) = \gamma(1), \text{ polynomiaux par morceaux}\}$.

Théorème

Il existe une application $\text{ind}: \Omega \rightarrow \mathbb{Z}$ ayant les propriétés suivantes :

0 *Calculabilité* : $\text{ind}(\gamma)$ se calcule par l'algorithme de Sturm sur \mathbf{R} .

1 *Normalisation* : 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 *Multiplicativité* : $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.

3 *Invariance par homotopie* : $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ dans \mathbf{C}^* .

La difficulté réside dans la *construction* ! Tous les moyens sont bons :

- Théorie des revêtements, appliquée à $\exp: \mathbb{C} \rightarrow \mathbb{C}^*$ avec groupe \mathbb{Z} .
- 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.
- Topologie différentielle, théorème de Sard et degré topologique.
- Analyse complexe, indice analytique $\text{ind}(\gamma) = \frac{1}{2i\pi} \int_{\gamma} \frac{dz}{z}$.
- Algèbre réelle, indice algébrique $\text{ind}: \Omega \rightarrow \mathbb{Z}$ via les suites de Sturm.

Racines complexes de polynômes complexes

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

Racines complexes de polynômes complexes

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

Nous savons construire l'indice, ayant les bonnes propriétés,

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

Racines complexes de polynômes complexes

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

Nous savons construire l'indice, ayant les bonnes propriétés,

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

Ceci donne une preuve effective du théorème fondamental de l'algèbre :

Racines complexes de polynômes complexes

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

Nous savons construire l'indice, ayant les bonnes propriétés,

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

Ceci donne une preuve effective du théorème fondamental de l'algèbre :

- $\text{ind}_{\partial\Gamma}(F)$ compte les racines de F dans Γ . (Sturm complexe)

Racines complexes de polynômes complexes

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

Nous savons construire l'indice, ayant les bonnes propriétés,

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

Ceci donne une preuve effective du théorème fondamental de l'algèbre :

- $\text{ind}_{\partial\Gamma}(F)$ compte les racines de F dans Γ . (Sturm complexe)
- $\text{ind}_{\partial\Gamma}(F) = \deg(F)$ pour Γ assez grand. (Borne de Cauchy)

Racines complexes de polynômes complexes

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

Nous savons construire l'indice, ayant les bonnes propriétés,

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

Ceci donne une preuve effective du théorème fondamental de l'algèbre :

- $\text{ind}_{\partial\Gamma}(F)$ compte les racines de F dans Γ . (Sturm complexe)
- $\text{ind}_{\partial\Gamma}(F) = \deg(F)$ pour Γ assez grand. (Borne de Cauchy)

Ainsi l'indice permet de localiser toutes les racines de F dans \mathbf{C} :

Racines complexes de polynômes complexes

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

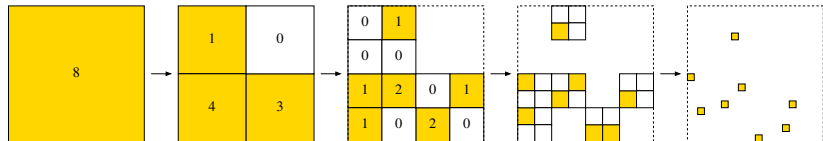
Nous savons construire l'indice, ayant les bonnes propriétés,

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

Ceci donne une preuve effective du théorème fondamental de l'algèbre :

- $\text{ind}_{\partial\Gamma}(F)$ compte les racines de F dans Γ . (Sturm complexe)
- $\text{ind}_{\partial\Gamma}(F) = \deg(F)$ pour Γ assez grand. (Borne de Cauchy)

Ainsi l'indice permet de localiser toutes les racines de F dans \mathbf{C} :



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

Indice réel algébrique

- Sturm 1829/35 : Mémoire sur la résolution des équations numériques

Indice réel algébrique

- Sturm 1829/35 : Mémoire sur la résolution des équations numériques
- Cauchy 1831/37 : Calcul des résidus et calcul des indices

Indice réel algébrique

- Sturm 1829/35 : Mémoire sur la résolution des équations numériques
- Cauchy 1831/37 : Calcul des résidus et calcul des indices
- Sturm–Liouville 1836 : Démonstration d'un théorème de M. Cauchy

Indice réel algébrique

- Sturm 1829/35 : Mémoire sur la résolution des équations numériques
- Cauchy 1831/37 : Calcul des résidus et calcul des indices
- Sturm–Liouville 1836 : Démonstration d'un théorème de M. Cauchy

Réception dans des manuels

- Serret 1877 : Cours d'algèbre supérieure (Sturm réel et complexe)

Indice réel algébrique

- Sturm 1829/35 : Mémoire sur la résolution des équations numériques
- Cauchy 1831/37 : Calcul des résidus et calcul des indices
- Sturm–Liouville 1836 : Démonstration d'un théorème de M. Cauchy

Réception dans des manuels

- Serret 1877 : Cours d'algèbre supérieure (Sturm réel et complexe)
- Weber 1898 : Lehrbuch der Algebra (Sturm réel, à peine complexe)

Indice réel algébrique

- Sturm 1829/35 : Mémoire sur la résolution des équations numériques
- Cauchy 1831/37 : Calcul des résidus et calcul des indices
- Sturm–Liouville 1836 : Démonstration d'un théorème de M. Cauchy

Réception dans des manuels

- Serret 1877 : Cours d'algèbre supérieure (Sturm réel et complexe)
- Weber 1898 : Lehrbuch der Algebra (Sturm réel, à peine complexe)
- Runge 1898 : Encyklopädie (Sturm réel et complexe)

Indice réel algébrique

- Sturm 1829/35 : Mémoire sur la résolution des équations numériques
- Cauchy 1831/37 : Calcul des résidus et calcul des indices
- Sturm–Liouville 1836 : Démonstration d'un théorème de M. Cauchy

Réception dans des manuels

- Serret 1877 : Cours d'algèbre supérieure (Sturm réel et complexe)
- Weber 1898 : Lehrbuch der Algebra (Sturm réel, à peine complexe)
- Runge 1898 : Encyklopädie (Sturm réel et complexe)

Degré topologique

- Kronecker 1869 : Systeme von Functionen mehrer Variabeln

Indice réel algébrique

- Sturm 1829/35 : Mémoire sur la résolution des équations numériques
- Cauchy 1831/37 : Calcul des résidus et calcul des indices
- Sturm–Liouville 1836 : Démonstration d'un théorème de M. Cauchy

Réception dans des manuels

- Serret 1877 : Cours d'algèbre supérieure (Sturm réel et complexe)
- Weber 1898 : Lehrbuch der Algebra (Sturm réel, à peine complexe)
- Runge 1898 : Encyklopädie (Sturm réel et complexe)

Degré topologique

- Kronecker 1869 : Systeme von Functionen mehrer Variabeln
- Brouwer 1912 : Abbildungen von Mannigfaltigkeiten

Indice réel algébrique

- Sturm 1829/35 : Mémoire sur la résolution des équations numériques
- Cauchy 1831/37 : Calcul des résidus et calcul des indices
- Sturm–Liouville 1836 : Démonstration d'un théorème de M. Cauchy

Réception dans des manuels

- Serret 1877 : Cours d'algèbre supérieure (Sturm réel et complexe)
- Weber 1898 : Lehrbuch der Algebra (Sturm réel, à peine complexe)
- Runge 1898 : Encyklopädie (Sturm réel et complexe)

Degré topologique

- Kronecker 1869 : Systeme von Functionen mehrer Variabeln
- Brouwer 1912 : Abbildungen von Mannigfaltigkeiten
- Weyl 1924 : Fundamentalsatz der Algebra

Indice réel algébrique

- Sturm 1829/35 : Mémoire sur la résolution des équations numériques
- Cauchy 1831/37 : Calcul des résidus et calcul des indices
- Sturm–Liouville 1836 : Démonstration d'un théorème de M. Cauchy

Réception dans des manuels

- Serret 1877 : Cours d'algèbre supérieure (Sturm réel et complexe)
- Weber 1898 : Lehrbuch der Algebra (Sturm réel, à peine complexe)
- Runge 1898 : Encyklopädie (Sturm réel et complexe)

Degré topologique

- Kronecker 1869 : Systeme von Functionen mehrer Variabeln
- Brouwer 1912 : Abbildungen von Mannigfaltigkeiten
- Weyl 1924 : Fundamentalsatz der Algebra

Algorithmes et implémentations

- Lehmer 1969 : Search procedures for polynomial equation solving

Indice réel algébrique

- Sturm 1829/35 : Mémoire sur la résolution des équations numériques
- Cauchy 1831/37 : Calcul des résidus et calcul des indices
- Sturm–Liouville 1836 : Démonstration d'un théorème de M. Cauchy

Réception dans des manuels

- Serret 1877 : Cours d'algèbre supérieure (Sturm réel et complexe)
- Weber 1898 : Lehrbuch der Algebra (Sturm réel, à peine complexe)
- Runge 1898 : Encyklopädie (Sturm réel et complexe)

Degré topologique

- Kronecker 1869 : Systeme von Functionen mehrer Variabeln
- Brouwer 1912 : Abbildungen von Mannigfaltigkeiten
- Weyl 1924 : Fundamentalsatz der Algebra

Algorithmes et implémentations

- Lehmer 1969 : Search procedures for polynomial equation solving
- Wilf 1978 : Bisection algorithm for computing zeros of polynomials

Indice réel algébrique

- Sturm 1829/35 : Mémoire sur la résolution des équations numériques
- Cauchy 1831/37 : Calcul des résidus et calcul des indices
- Sturm–Liouville 1836 : Démonstration d'un théorème de M. Cauchy

Réception dans des manuels

- Serret 1877 : Cours d'algèbre supérieure (Sturm réel et complexe)
- Weber 1898 : Lehrbuch der Algebra (Sturm réel, à peine complexe)
- Runge 1898 : Encyklopädie (Sturm réel et complexe)

Degré topologique

- Kronecker 1869 : Systeme von Functionen mehrer Variabeln
- Brouwer 1912 : Abbildungen von Mannigfaltigkeiten
- Weyl 1924 : Fundamentalsatz der Algebra

Algorithmes et implémentations

- Lehmer 1969 : Search procedures for polynomial equation solving
- Wilf 1978 : Bisection algorithm for computing zeros of polynomials
- Schönhage 1982 : The fundamental theorem of algebra in terms of computational complexity

- 1 Le théorème fondamental de l'algèbre
- 2 **Sturm 1829/1835 : racines réelles de polynômes réels**
 - L'indice de Cauchy pour les polynômes réels
 - La formule d'inversion de Cauchy
 - Suites de Sturm
- 3 Sturm 1836 : racines complexes de polynômes complexes
- 4 Conclusions et perspectives

Changements de signe : conventions de comptage

On considère un corps ordonné $(\mathbf{R}, +, \cdot, \leq)$.

Changements de signe : conventions de comptage

On considère un corps ordonné $(\mathbf{R}, +, \cdot, \leq)$.

Nous comptons le nombre $V(s_0, s_1)$ des changements de signes :

Changements de signe : conventions de comptage

On considère un corps ordonné $(\mathbf{R}, +, \cdot, \leq)$.

Nous comptons le nombre $V(s_0, s_1)$ des changements de signes :

$$V(+, -) = V(-, +) = 1,$$

Changements de signe : conventions de comptage

On considère un corps ordonné $(\mathbf{R}, +, \cdot, \leq)$.

Nous comptons le nombre $V(s_0, s_1)$ des changements de signes :

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

Changements de signe : conventions de comptage

On considère un corps ordonné $(\mathbf{R}, +, \cdot, \leq)$.

Nous comptons le nombre $V(s_0, s_1)$ des changements de signes :

$$V(+, -) = V(-, +) = 1,$$

$$V(+, +) = V(-, -) = V(0, 0) = 0,$$

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

Changements de signe : conventions de comptage

On considère un corps ordonné $(\mathbf{R}, +, \cdot, \leq)$.

Nous comptons le nombre $V(s_0, s_1)$ des changements de signes :

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

Définition

Pour une suite (s_0, \dots, s_n) d'éléments dans \mathbf{R} nous posons

$$V(s_0, \dots, s_n) := \sum_{k=1}^n V(s_{k-1}, s_k) = \sum_{k=1}^n \frac{1}{2} |\text{sign}(s_{k-1}) - \text{sign}(s_k)|.$$

Changements de signe : conventions de comptage

On considère un corps ordonné $(\mathbf{R}, +, \cdot, \leq)$.

Nous comptons le nombre $V(s_0, s_1)$ des changements de signes :

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

Définition

Pour une suite (s_0, \dots, s_n) d'éléments dans \mathbf{R} nous posons

$$V(s_0, \dots, s_n) := \sum_{k=1}^n V(s_{k-1}, s_k) = \sum_{k=1}^n \frac{1}{2} |\text{sign}(s_{k-1}) - \text{sign}(s_k)|.$$

Pour une suite (S_0, \dots, S_n) de polynômes dans $\mathbf{R}[X]$ nous posons

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

Changements de signe : conventions de comptage

On considère un corps ordonné $(\mathbf{R}, +, \cdot, \leq)$.

Nous comptons le nombre $V(s_0, s_1)$ des changements de signes :

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

Définition

Pour une suite (s_0, \dots, s_n) d'éléments dans \mathbf{R} nous posons

$$V(s_0, \dots, s_n) := \sum_{k=1}^n V(s_{k-1}, s_k) = \sum_{k=1}^n \frac{1}{2} |\text{sign}(s_{k-1}) - \text{sign}(s_k)|.$$

Pour une suite (S_0, \dots, S_n) de polynômes dans $\mathbf{R}[X]$ nous posons

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

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

Changements de signe : conventions de comptage

On considère un corps ordonné $(\mathbf{R}, +, \cdot, \leq)$.

Nous comptons le nombre $V(s_0, s_1)$ des changements de signes :

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

Définition


Pour une suite (s_0, \dots, s_n) d'éléments dans \mathbf{R} nous posons

$$V(s_0, \dots, s_n) := \sum_{k=1}^n V(s_{k-1}, s_k) = \sum_{k=1}^n \frac{1}{2} |\text{sign}(s_{k-1}) - \text{sign}(s_k)|.$$

Pour une suite (S_0, \dots, S_n) de polynômes dans $\mathbf{R}[X]$ nous posons

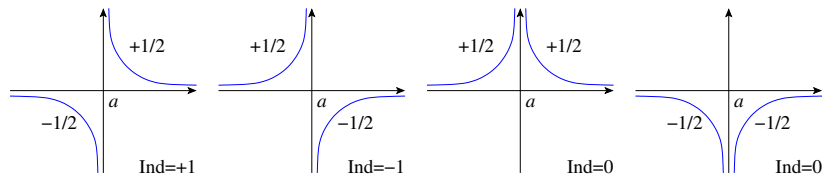
$$V_a(S_0, \dots, S_n) := V(S_0(a), \dots, S_n(a)).$$

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

 Définition traditionnelle (Descartes, Fourier) : on forme d'abord la suite réduite \hat{s} en supprimant les éléments nuls de s , puis on définit $\hat{V}(s) := V(\hat{s})$.

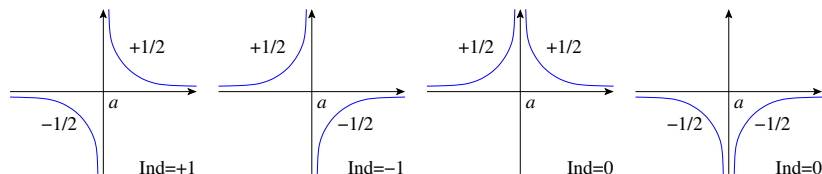
L'indice de Cauchy : comptage de pôles

On compte les pôles d'une fraction rationnelle $f \in \mathbf{R}(X)^*$ comme suit :



L'indice de Cauchy : comptage de pôles

On compte les pôles d'une fraction rationnelle $f \in \mathbf{R}(X)^*$ comme suit :



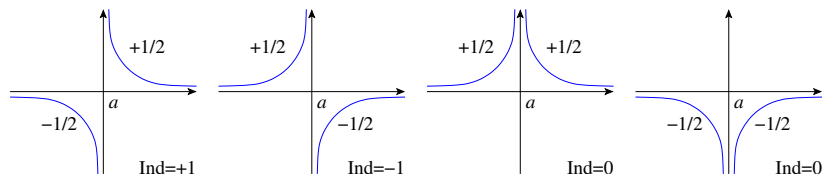
Définition (indice de Cauchy)

Pour $f \in \mathbf{R}(X)^*$ et $a \in \mathbf{R}$ on pose

$$\text{Ind}_a(f) := \text{Ind}_a^+(f) - \text{Ind}_a^-(f) \quad \text{où} \quad \text{Ind}_a^\varepsilon(f) := \begin{cases} +\frac{1}{2} & \text{si } \lim_a^\varepsilon f = +\infty, \\ -\frac{1}{2} & \text{si } \lim_a^\varepsilon f = -\infty, \\ 0 & \text{sinon.} \end{cases}$$

L'indice de Cauchy : comptage de pôles

On compte les pôles d'une fraction rationnelle $f \in \mathbf{R}(X)^*$ comme suit :



Définition (indice de Cauchy)

Pour $f \in \mathbf{R}(X)^*$ et $a \in \mathbf{R}$ on pose

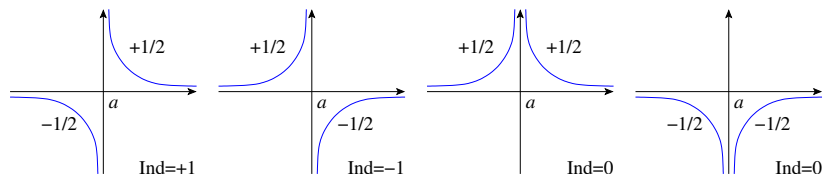
$$\text{Ind}_a(f) := \text{Ind}_a^+(f) - \text{Ind}_a^-(f) \quad \text{où} \quad \text{Ind}_a^\varepsilon(f) := \begin{cases} +\frac{1}{2} & \text{si } \lim_a^\varepsilon f = +\infty, \\ -\frac{1}{2} & \text{si } \lim_a^\varepsilon f = -\infty, \\ 0 & \text{sinon.} \end{cases}$$

Pour un intervalle $[a, b] \subset \mathbf{R}$ on pose

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

L'indice de Cauchy : comptage de pôles

On compte les pôles d'une fraction rationnelle $f \in \mathbf{R}(X)^*$ comme suit :



Définition (indice de Cauchy)

Pour $f \in \mathbf{R}(X)^*$ et $a \in \mathbf{R}$ on pose

$$\text{Ind}_a(f) := \text{Ind}_a^+(f) - \text{Ind}_a^-(f) \quad \text{où} \quad \text{Ind}_a^\varepsilon(f) := \begin{cases} +\frac{1}{2} & \text{si } \lim_a^\varepsilon f = +\infty, \\ -\frac{1}{2} & \text{si } \lim_a^\varepsilon f = -\infty, \\ 0 & \text{sinon.} \end{cases}$$

Pour un intervalle $[a, b] \subset \mathbf{R}$ on pose

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

Propriétés : $\text{Ind}_a^b(f) + \text{Ind}_b^c(f) = \text{Ind}_a^c(f)$ et $\text{Ind}_a^b(f \circ \tau) = \text{Ind}_\tau^{\tau(b)}(f)$.

Formule d'inversion (Cauchy 1837)

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

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

Formule d'inversion (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 $\text{pgcd}(P, Q) = 1$.

Formule d'inversion (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 $\text{pgcd}(P, Q) = 1$.

❶ Supposons d'abord que $[a, b]$ ne contient pas de racine de P ni de Q .

Formule d'inversion (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 $\operatorname{pgcd}(P, Q) = 1$.

❶ Supposons d'abord que $[a, b]$ ne contient pas de racine de P ni de Q .

- En absence de pôles, les indices $\operatorname{Ind}_a^b\left(\frac{Q}{P}\right)$ et $\operatorname{Ind}_a^b\left(\frac{P}{Q}\right)$ sont nuls.

Formule d'inversion (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 $\operatorname{pgcd}(P, Q) = 1$.

❶ Supposons d'abord que $[a, b]$ ne contient pas de racine de P ni de Q .

- En absence de pôles, les indices $\operatorname{Ind}_a^b\left(\frac{Q}{P}\right)$ et $\operatorname{Ind}_a^b\left(\frac{P}{Q}\right)$ sont nuls.
- Le TVI assure que P et Q ne changent pas de signe, donc $V_a^b(P, Q) = 0$.

Formule d'inversion (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 $\operatorname{pgcd}(P, Q) = 1$.

❶ Supposons d'abord que $[a, b]$ ne contient pas de racine de P ni de Q .

- En absence de pôles, les indices $\operatorname{Ind}_a^b\left(\frac{Q}{P}\right)$ et $\operatorname{Ind}_a^b\left(\frac{P}{Q}\right)$ sont nuls.
- Le TVI assure que P et Q ne changent pas de signe, donc $V_a^b(P, Q) = 0$.

❷ La formule est additive par rapport à bisection de l'intervalle.

Formule d'inversion (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 $\operatorname{pgcd}(P, Q) = 1$.

❶ Supposons d'abord que $[a, b]$ ne contient pas de racine de P ni de Q .

- En absence de pôles, les indices $\operatorname{Ind}_a^b\left(\frac{Q}{P}\right)$ et $\operatorname{Ind}_a^b\left(\frac{P}{Q}\right)$ sont nuls.
- Le TVI assure que P et Q ne changent pas de signe, donc $V_a^b(P, Q) = 0$.

❷ La formule est additive par rapport à bisection de l'intervalle.

Il ne reste qu'à regarder le cas d'un seul pôle : $P(a) = 0$ et $Q(a) \neq 0$.

Formule d'inversion (Cauchy 1837)

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

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

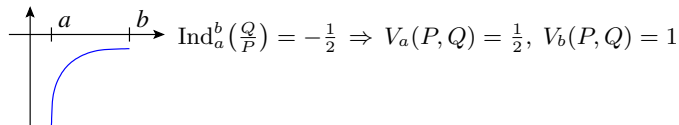
Démonstration. On peut supposer que $P \neq 0$ et $Q \neq 0$ et $\text{pgcd}(P, Q) = 1$.

❶ Supposons d'abord que $[a, b]$ ne contient pas de racine de P ni de Q .

- En absence de pôles, les indices $\text{Ind}_a^b\left(\frac{Q}{P}\right)$ et $\text{Ind}_a^b\left(\frac{P}{Q}\right)$ sont nuls.
- Le TVI assure que P et Q ne changent pas de signe, donc $V_a^b(P, Q) = 0$.

❷ La formule est additive par rapport à bisection de l'intervalle.

Il ne reste qu'à regarder le cas d'un seul pôle : $P(a) = 0$ et $Q(a) \neq 0$.



Formule d'inversion (Cauchy 1837)

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

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

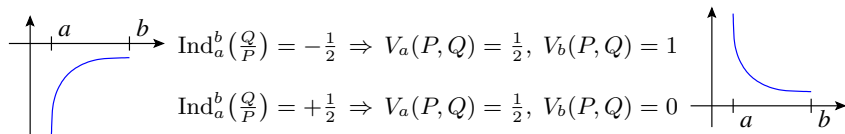
Démonstration. On peut supposer que $P \neq 0$ et $Q \neq 0$ et $\text{pgcd}(P, Q) = 1$.

❶ Supposons d'abord que $[a, b]$ ne contient pas de racine de P ni de Q .

- En absence de pôles, les indices $\text{Ind}_a^b\left(\frac{Q}{P}\right)$ et $\text{Ind}_a^b\left(\frac{P}{Q}\right)$ sont nuls.
- Le TVI assure que P et Q ne changent pas de signe, donc $V_a^b(P, Q) = 0$.

❷ La formule est additive par rapport à bisection de l'intervalle.

Il ne reste qu'à regarder le cas d'un seul pôle : $P(a) = 0$ et $Q(a) \neq 0$.



Définition (suite de Sturm)

Une suite (S_0, \dots, S_n) dans $\mathbf{R}[X]$ est *de Sturm* sur $[a, b] \subset \mathbf{R}$ si elle vérifie :

Définition (suite de Sturm)

Une suite (S_0, \dots, S_n) dans $\mathbf{R}[X]$ est *de Sturm* sur $[a, b] \subset \mathbf{R}$ si elle vérifie :
Si $S_k(x) = 0$ pour $0 < k < n$ et $x \in [a, b]$, alors $S_{k-1}(x)S_{k+1}(x) < 0$.

Définition (suite de Sturm)

Une suite (S_0, \dots, S_n) dans $\mathbf{R}[X]$ est *de Sturm* sur $[a, b] \subset \mathbf{R}$ si elle vérifie :
Si $S_k(x) = 0$ pour $0 < k < n$ et $x \in [a, b]$, alors $S_{k-1}(x)S_{k+1}(x) < 0$.

Corollaire (de la formule d'inversion)

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

Définition (suite de Sturm)

Une suite (S_0, \dots, S_n) dans $\mathbf{R}[X]$ est *de Sturm* sur $[a, b] \subset \mathbf{R}$ si elle vérifie :
Si $S_k(x) = 0$ pour $0 < k < n$ et $x \in [a, b]$, alors $S_{k-1}(x)S_{k+1}(x) < 0$.

Corollaire (de la formule d'inversion)

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

Démonstration. La formule d'inversion est télescopique : pour $n = 2$ on a

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

Définition (suite de Sturm)

Une suite (S_0, \dots, S_n) dans $\mathbf{R}[X]$ est *de Sturm* sur $[a, b] \subset \mathbf{R}$ si elle vérifie :
Si $S_k(x) = 0$ pour $0 < k < n$ et $x \in [a, b]$, alors $S_{k-1}(x)S_{k+1}(x) < 0$.

Corollaire (de la formule d'inversion)

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

Démonstration. La formule d'inversion est télescopique : pour $n = 2$ on a

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

Proposition (fraction continue selon l'algorithme d'Euclide)

Pour $\frac{R}{S}$ où $\text{pgcd}(R, S) = 1$ l'algorithme d'Euclide produit une suite de Sturm $S_0 = S, S_1 = R, \dots, S_n = 1, S_{n+1} = 0$ telle que $S_{k-1} = Q_k S_k - S_{k+1}$. \square

Définition (suite de Sturm)

Une suite (S_0, \dots, S_n) dans $\mathbf{R}[X]$ est *de Sturm* sur $[a, b] \subset \mathbf{R}$ si elle vérifie :
Si $S_k(x) = 0$ pour $0 < k < n$ et $x \in [a, b]$, alors $S_{k-1}(x)S_{k+1}(x) < 0$.

Corollaire (de la formule d'inversion)

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

Démonstration. La formule d'inversion est télescopique : pour $n = 2$ on a

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

Proposition (fraction continue selon l'algorithme d'Euclide)

Pour $\frac{R}{S}$ où $\text{pgcd}(R, S) = 1$ l'algorithme d'Euclide produit une suite de Sturm $S_0 = S, S_1 = R, \dots, S_n = 1, S_{n+1} = 0$ telle que $S_{k-1} = Q_k S_k - S_{k+1}$. \square

Corollaire : le théorème de Sturm

Pour tout polynôme $P \in \mathbf{R}[X]$ sur un corps \mathbf{R} réel clos on a

$$\#\{x \in [a, b] \mid P(x) = 0\} = \text{Ind}_a^b\left(\frac{P'}{P}\right) = V_a^b(S_0, S_1, \dots, S_n).$$

- 1 Le théorème fondamental de l'algèbre
- 2 Sturm 1829/1835 : racines réelles de polynômes réels
- 3 Sturm 1836 : racines complexes de polynômes complexes
 - L'indice de Cauchy pour les polynômes complexes
 - La formule du produit
 - Invariance par homotopie
- 4 Conclusions et perspectives

L'indice complexe : rappel des propriétés algébriques

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

L'indice complexe : rappel des propriétés algébriques

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

Nous voulons construire l'indice algébrique

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

L'indice complexe : rappel des propriétés algébriques

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

Nous voulons construire l'indice algébrique

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

On exige les propriétés suivantes :

L'indice complexe : rappel des propriétés algébriques

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

Nous voulons construire l'indice algébrique

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

On exige les propriétés suivantes :

1 Normalisation : Pour tout rectangle $\Gamma \subset \mathbf{C}$ on a

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

L'indice complexe : rappel des propriétés algébriques

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

Nous voulons construire l'indice algébrique

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

On exige les propriétés suivantes :

1 Normalisation : 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 Multiplicativité : $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.

L'indice complexe : rappel des propriétés algébriques

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

Nous voulons construire l'indice algébrique

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

On exige les propriétés suivantes :

1 Normalisation : 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 Multiplicativité : $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.

3 Invariance par homotopie : $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ dans \mathbf{C}^* .

L'indice complexe : rappel des propriétés algébriques

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

Nous voulons construire l'indice algébrique

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

On exige les propriétés suivantes :

1 Normalisation : 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 Multiplicativité : $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.

3 Invariance par homotopie : $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ dans \mathbf{C}^* .

Bénéfice algorithmique : calcul par les suites de Sturm.

L'indice complexe : rappel des propriétés algébriques

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

Nous voulons construire l'indice algébrique

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

On exige les propriétés suivantes :

1 Normalisation : 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 Multiplicativité : $\text{ind}(\gamma_1 \cdot \gamma_2) = \text{ind}(\gamma_1) + \text{ind}(\gamma_2)$.

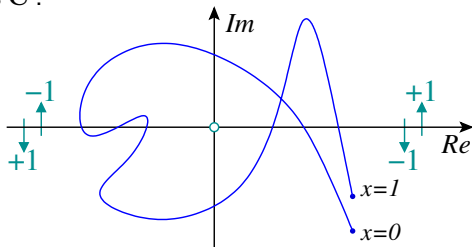
3 Invariance par homotopie : $\text{ind}(\gamma_0) = \text{ind}(\gamma_1)$ si $\gamma_0 \sim \gamma_1$ dans \mathbf{C}^* .

Bénéfice algorithmique : calcul par les suites de Sturm.

Calcul formel au lieu du numérique : tous les calculs sont exacts.

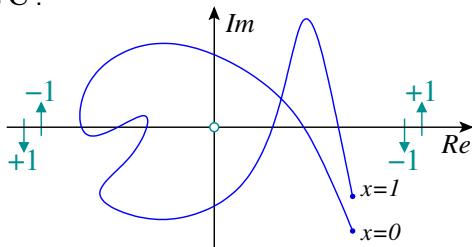
L'indice complexe : motivation géométrique et définition algébrique

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



L'indice complexe : motivation géométrique et définition algébrique

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

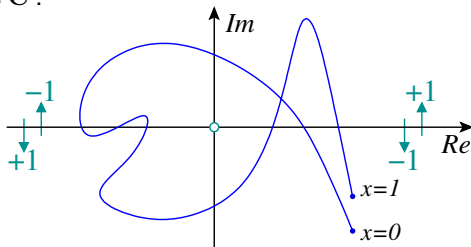


Observation

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

L'indice complexe : motivation géométrique et définition algébrique

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



Observation

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

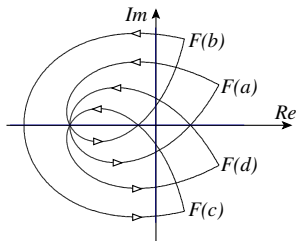
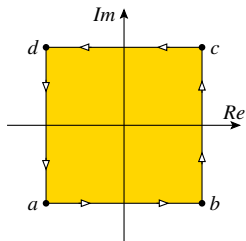
Plus généralement : pour $a, b \in \mathbf{C}$ on considère $\gamma(x) = F(a + (b - a)x)$.

Définition

Pour $F \in \mathbf{C}[Z]$ et $a, b \in \mathbf{C}$ on pose $\text{ind}_{[a,b]}^{\mathbf{C}}(F) = \text{ind}_{[0,1]}^{\mathbf{C}} F(a + (b - a)X)$.

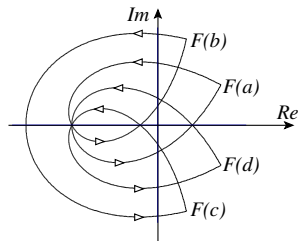
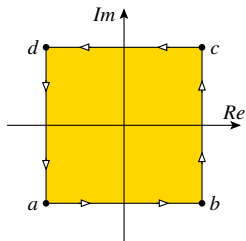
L'indice par rapport à un rectangle

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



L'indice par rapport à un rectangle

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



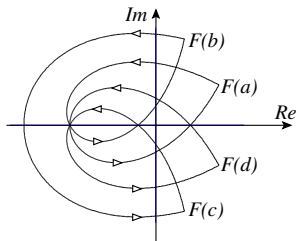
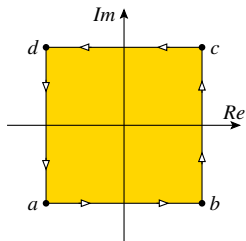
Définition

Pour tout polynôme $F \in \mathbf{C}[Z]$ et tout rectangle $\Gamma \subset \mathbf{C}$ on pose

$$\text{ind}_{\partial\Gamma}^{\mathbf{C}}(F) := \text{ind}_{[a,b]}^{\mathbf{C}}(F) + \text{ind}_{[b,c]}^{\mathbf{C}}(F) + \text{ind}_{[c,d]}^{\mathbf{C}}(F) + \text{ind}_{[d,a]}^{\mathbf{C}}(F).$$

L'indice par rapport à un rectangle

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



Définition

Pour tout polynôme $F \in \mathbf{C}[Z]$ et tout rectangle $\Gamma \subset \mathbf{C}$ on pose

$$\text{ind}_{\partial\Gamma}^{\mathbf{C}}(F) := \text{ind}_{[a,b]}^{\mathbf{C}}(F) + \text{ind}_{[b,c]}^{\mathbf{C}}(F) + \text{ind}_{[c,d]}^{\mathbf{C}}(F) + \text{ind}_{[d,a]}^{\mathbf{C}}(F).$$

Proposition (normalisation)

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

La formule du produit

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

La formule du produit

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

Lemme (formule du produit)

Pour toute paire de fractions rationnelles $\frac{P}{Q}, \frac{R}{S} \in \mathbf{R}(X)^*$ nous avons

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

La formule du produit

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

Lemme (formule du produit)

Pour toute paire de fractions rationnelles $\frac{P}{Q}, \frac{R}{S} \in \mathbf{R}(X)^*$ nous avons

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

Cas particulier : pour $P = S$ et $Q = R$ on retrouve la formule d'inversion.

La formule du produit

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

Lemme (formule du produit)

Pour toute paire de fractions rationnelles $\frac{P}{Q}, \frac{R}{S} \in \mathbf{R}(X)^*$ nous avons

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

Cas particulier : pour $P = S$ et $Q = R$ on retrouve la formule d'inversion.

Le cas général se démontre exactement comme le cas particulier.

La formule du produit

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

Lemme (formule du produit)

Pour toute paire de fractions rationnelles $\frac{P}{Q}, \frac{R}{S} \in \mathbf{R}(X)^*$ nous avons

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

Cas particulier : pour $P = S$ et $Q = R$ on retrouve la formule d'inversion.
Le cas général se démontre exactement comme le cas particulier.

Théorème (multiplicativité)

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

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

La formule du produit

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

Lemme (formule du produit)

Pour toute paire de fractions rationnelles $\frac{P}{Q}, \frac{R}{S} \in \mathbf{R}(X)^*$ nous avons

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

Cas particulier : pour $P = S$ et $Q = R$ on retrouve la formule d'inversion.
Le cas général se démontre exactement comme le cas particulier.

Théorème (multiplicativité)

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

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

Corollaire (comptage de racines complexes, cas scindé)

Soit $F \in \mathbf{C}[Z]$ scindé, $F = c(Z - z_1) \cdots (Z - z_n)$ sur \mathbf{C} , sans racines sur les sommets de Γ .

La formule du produit

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

Lemme (formule du produit)

Pour toute paire de fractions rationnelles $\frac{P}{Q}, \frac{R}{S} \in \mathbf{R}(X)^*$ nous avons

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

Cas particulier : pour $P = S$ et $Q = R$ on retrouve la formule d'inversion.
Le cas général se démontre exactement comme le cas particulier.

Théorème (multiplicativité)

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

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

Corollaire (comptage de racines complexes, cas scindé)

Soit $F \in \mathbf{C}[Z]$ scindé, $F = c(Z - z_1) \cdots (Z - z_n)$ sur \mathbf{C} , sans racines sur les sommets de Γ . Alors l'indice $\text{ind}_{\partial\Gamma}^{\mathbf{C}}(F)$ compte les racines dans Γ .

La formule du produit

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

Lemme (formule du produit)

Pour toute paire de fractions rationnelles $\frac{P}{Q}, \frac{R}{S} \in \mathbf{R}(X)^*$ nous avons

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

Cas particulier : pour $P = S$ et $Q = R$ on retrouve la formule d'inversion.
Le cas général se démontre exactement comme le cas particulier.

Théorème (multiplicativité)

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

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

Corollaire (comptage de racines complexes, cas scindé)

Soit $F \in \mathbf{C}[Z]$ scindé, $F = c(Z - z_1) \cdots (Z - z_n)$ sur \mathbf{C} , sans racines sur les sommets de Γ . Alors l'indice $\text{ind}_{\partial\Gamma}^{\mathbf{C}}(F)$ compte les racines dans Γ .



Nous devons encore montrer que sur \mathbf{C} tout polynôme est scindé sur \mathbf{C} .

Comptage de racines complexes

Nous devons montrer : si $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) > 0$, alors $F(z) = 0$ pour un $z \in \Gamma$.

Comptage de racines complexes

Nous devons montrer : si $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) > 0$, alors $F(z) = 0$ pour un $z \in \Gamma$.

Par contraposé : si $F(z) \neq 0$ pour tout $z \in \Gamma$, alors $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$.

Comptage de racines complexes

Nous devons montrer : si $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) > 0$, alors $F(z) = 0$ pour un $z \in \Gamma$.

Par contraposé : si $F(z) \neq 0$ pour tout $z \in \Gamma$, alors $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$.

Nous plongeons $\mathbb{C}[Z] \subset \mathbb{C}[X, Y]$ via $Z = X + iY$.

Comptage de racines complexes

Nous devons montrer : si $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) > 0$, alors $F(z) = 0$ pour un $z \in \Gamma$.

Par contraposé : si $F(z) \neq 0$ pour tout $z \in \Gamma$, alors $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$.

Nous plongeons $\mathbb{C}[Z] \subset \mathbb{C}[X, Y]$ via $Z = X + iY$.

Lemme (version locale)

Si $F \in \mathbb{C}[X, Y]$ ne s'annule pas en $(x, y) \in \mathbb{R}^2$, alors il existe $\delta > 0$ tel que $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$ pour tout $\Gamma \subset [x - \delta, x + \delta] \times [y - \delta, y + \delta]$.

Comptage de racines complexes

Nous devons montrer : si $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) > 0$, alors $F(z) = 0$ pour un $z \in \Gamma$.

Par contraposé : si $F(z) \neq 0$ pour tout $z \in \Gamma$, alors $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$.

Nous plongeons $\mathbb{C}[Z] \subset \mathbb{C}[X, Y]$ via $Z = X + iY$.

Lemme (version locale)

Si $F \in \mathbb{C}[X, Y]$ ne s'annule pas en $(x, y) \in \mathbb{R}^2$, alors il existe $\delta > 0$ tel que $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$ pour tout $\Gamma \subset [x - \delta, x + \delta] \times [y - \delta, y + \delta]$.

Démonstration. Continuité (δ explicite, sur tout corps ordonné). □

Comptage de racines complexes

Nous devons montrer : si $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) > 0$, alors $F(z) = 0$ pour un $z \in \Gamma$.

Par contraposé : si $F(z) \neq 0$ pour tout $z \in \Gamma$, alors $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$.

Nous plongeons $\mathbb{C}[Z] \subset \mathbb{C}[X, Y]$ via $Z = X + iY$.

Lemme (version locale)

Si $F \in \mathbb{C}[X, Y]$ ne s'annule pas en $(x, y) \in \mathbb{R}^2$, alors il existe $\delta > 0$ tel que $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$ pour tout $\Gamma \subset [x - \delta, x + \delta] \times [y - \delta, y + \delta]$.

Démonstration. Continuité (δ explicite, sur tout corps ordonné). □

Théorème (version globale)

Si $F \in \mathbb{C}[X, Y]$ ne s'annule pas sur $\Gamma \subset \mathbb{R}^2$, alors $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$.

Comptage de racines complexes

Nous devons montrer : si $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) > 0$, alors $F(z) = 0$ pour un $z \in \Gamma$.

Par contraposé : si $F(z) \neq 0$ pour tout $z \in \Gamma$, alors $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$.

Nous plongeons $\mathbb{C}[Z] \subset \mathbb{C}[X, Y]$ via $Z = X + iY$.

Lemme (version locale)

Si $F \in \mathbb{C}[X, Y]$ ne s'annule pas en $(x, y) \in \mathbb{R}^2$, alors il existe $\delta > 0$ tel que $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$ pour tout $\Gamma \subset [x - \delta, x + \delta] \times [y - \delta, y + \delta]$.

Démonstration. Continuité (δ explicite, sur tout corps ordonné). □

Théorème (version globale)

Si $F \in \mathbb{C}[X, Y]$ ne s'annule pas sur $\Gamma \subset \mathbb{R}^2$, alors $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$.

Démonstration. Sur les nombres réels \mathbb{R} : compacité.

Comptage de racines complexes

Nous devons montrer : si $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) > 0$, alors $F(z) = 0$ pour un $z \in \Gamma$.

Par contraposé : si $F(z) \neq 0$ pour tout $z \in \Gamma$, alors $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$.

Nous plongeons $\mathbb{C}[Z] \subset \mathbb{C}[X, Y]$ via $Z = X + iY$.

Lemme (version locale)

Si $F \in \mathbb{C}[X, Y]$ ne s'annule pas en $(x, y) \in \mathbb{R}^2$, alors il existe $\delta > 0$ tel que $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$ pour tout $\Gamma \subset [x - \delta, x + \delta] \times [y - \delta, y + \delta]$.

Démonstration. Continuité (δ explicite, sur tout corps ordonné). □

Théorème (version globale)

Si $F \in \mathbb{C}[X, Y]$ ne s'annule pas sur $\Gamma \subset \mathbb{R}^2$, alors $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$.

Démonstration. Sur les nombres réels \mathbb{R} : compacité.

Sur un corps \mathbb{R} réel clos quelconque : suites de Sturm. □

Comptage de racines complexes

Nous devons montrer : si $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) > 0$, alors $F(z) = 0$ pour un $z \in \Gamma$.

Par contraposé : si $F(z) \neq 0$ pour tout $z \in \Gamma$, alors $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$.

Nous plongeons $\mathbb{C}[Z] \subset \mathbb{C}[X, Y]$ via $Z = X + iY$.

Lemme (version locale)

Si $F \in \mathbb{C}[X, Y]$ ne s'annule pas en $(x, y) \in \mathbb{R}^2$, alors il existe $\delta > 0$ tel que $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$ pour tout $\Gamma \subset [x - \delta, x + \delta] \times [y - \delta, y + \delta]$.

Démonstration. Continuité (δ explicite, sur tout corps ordonné). □

Théorème (version globale)

Si $F \in \mathbb{C}[X, Y]$ ne s'annule pas sur $\Gamma \subset \mathbb{R}^2$, alors $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$.

Démonstration. Sur les nombres réels \mathbb{R} : compacité.

Sur un corps \mathbb{R} réel clos quelconque : suites de Sturm. □

Corollaire (comptage de racines complexes, cas général)

Pour tout $F \in \mathbb{C}[Z]$ l'indice $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F)$ compte les racines de F dans Γ .

Comptage de racines complexes

Nous devons montrer : si $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) > 0$, alors $F(z) = 0$ pour un $z \in \Gamma$.

Par contraposé : si $F(z) \neq 0$ pour tout $z \in \Gamma$, alors $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$.

Nous plongeons $\mathbb{C}[Z] \subset \mathbb{C}[X, Y]$ via $Z = X + iY$.

Lemme (version locale)

Si $F \in \mathbb{C}[X, Y]$ ne s'annule pas en $(x, y) \in \mathbb{R}^2$, alors il existe $\delta > 0$ tel que $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$ pour tout $\Gamma \subset [x - \delta, x + \delta] \times [y - \delta, y + \delta]$.

Démonstration. Continuité (δ explicite, sur tout corps ordonné). □

Théorème (version globale)

Si $F \in \mathbb{C}[X, Y]$ ne s'annule pas sur $\Gamma \subset \mathbb{R}^2$, alors $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$.

Démonstration. Sur les nombres réels \mathbb{R} : compacité.

Sur un corps \mathbb{R} réel clos quelconque : suites de Sturm. □

Corollaire (comptage de racines complexes, cas général)

Pour tout $F \in \mathbb{C}[Z]$ l'indice $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F)$ compte les racines de F dans Γ .

Démonstration. On suppose que F n'a s'annule pas sur les sommets de Γ .

Comptage de racines complexes

Nous devons montrer : si $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) > 0$, alors $F(z) = 0$ pour un $z \in \Gamma$.

Par contraposé : si $F(z) \neq 0$ pour tout $z \in \Gamma$, alors $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$.

Nous plongeons $\mathbb{C}[Z] \subset \mathbb{C}[X, Y]$ via $Z = X + iY$.

Lemme (version locale)

Si $F \in \mathbb{C}[X, Y]$ ne s'annule pas en $(x, y) \in \mathbb{R}^2$, alors il existe $\delta > 0$ tel que $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$ pour tout $\Gamma \subset [x - \delta, x + \delta] \times [y - \delta, y + \delta]$.

Démonstration. Continuité (δ explicite, sur tout corps ordonné). □

Théorème (version globale)

Si $F \in \mathbb{C}[X, Y]$ ne s'annule pas sur $\Gamma \subset \mathbb{R}^2$, alors $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$.

Démonstration. Sur les nombres réels \mathbb{R} : compacité.

Sur un corps \mathbb{R} réel clos quelconque : suites de Sturm. □

Corollaire (comptage de racines complexes, cas général)

Pour tout $F \in \mathbb{C}[Z]$ l'indice $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F)$ compte les racines de F dans Γ .

Démonstration. On suppose que F n'a s'annule pas sur les sommets de Γ .

Soit $F = (Z - z_1) \cdots (Z - z_m)G$ tel que G n'ait pas de racines dans \mathbb{C} .

Comptage de racines complexes

Nous devons montrer : si $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) > 0$, alors $F(z) = 0$ pour un $z \in \Gamma$.

Par contraposé : si $F(z) \neq 0$ pour tout $z \in \Gamma$, alors $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$.

Nous plongeons $\mathbb{C}[Z] \subset \mathbb{C}[X, Y]$ via $Z = X + iY$.

Lemme (version locale)

Si $F \in \mathbb{C}[X, Y]$ ne s'annule pas en $(x, y) \in \mathbb{R}^2$, alors il existe $\delta > 0$ tel que $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$ pour tout $\Gamma \subset [x - \delta, x + \delta] \times [y - \delta, y + \delta]$.

Démonstration. Continuité (δ explicite, sur tout corps ordonné). □

Théorème (version globale)

Si $F \in \mathbb{C}[X, Y]$ ne s'annule pas sur $\Gamma \subset \mathbb{R}^2$, alors $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F) = 0$.

Démonstration. Sur les nombres réels \mathbb{R} : compacité.

Sur un corps \mathbb{R} réel clos quelconque : suites de Sturm. □

Corollaire (comptage de racines complexes, cas général)

Pour tout $F \in \mathbb{C}[Z]$ l'indice $\text{ind}_{\partial\Gamma}^{\mathbb{C}}(F)$ compte les racines de F dans Γ .

Démonstration. On suppose que F n'a s'annule pas sur les sommets de Γ .

Soit $F = (Z - z_1) \cdots (Z - z_m)G$ tel que G n'ait pas de racines dans \mathbb{C} .

On applique la multiplicativité de l'indice à F et le théorème ci-dessus à G .

Définition (borne de Cauchy)

Soit $F = Z^n + c_{n-1}Z^{n-1} + \cdots + c_1Z + c_0$ dans $\mathbf{C}[Z]$.

Définition (borne de Cauchy)

Soit $F = Z^n + c_{n-1}Z^{n-1} + \dots + c_1Z + c_0$ dans $\mathbf{C}[Z]$.

On pose $M := \max\{|c_0|, \dots, |c_{n-1}|\}$ et $\rho_F := 1 + M$.

Définition (borne de Cauchy)

Soit $F = Z^n + c_{n-1}Z^{n-1} + \dots + c_1Z + c_0$ dans $\mathbf{C}[Z]$.

On pose $M := \max\{|c_0|, \dots, |c_{n-1}|\}$ et $\rho_F := 1 + M$.

Théorème (localisation grossière des racines)

Pour tout $z \in \mathbf{C}$ tel que $|z| \geq \rho_F$ on a $|F(z)| \geq 1$.

Définition (borne de Cauchy)

Soit $F = Z^n + c_{n-1}Z^{n-1} + \dots + c_1Z + c_0$ dans $\mathbf{C}[Z]$.

On pose $M := \max\{|c_0|, \dots, |c_{n-1}|\}$ et $\rho_F := 1 + M$.

Théorème (localisation grossière des racines)

Pour tout $z \in \mathbf{C}$ tel que $|z| \geq \rho_F$ on a $|F(z)| \geq 1$.

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

Théorème (invariance par homotopie)

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 racine sur $\partial\Gamma$.

Théorème (invariance par homotopie)

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 racine sur $\partial\Gamma$. Alors $\text{ind}_{\partial\Gamma}^{\mathbf{C}}(F_0) = \text{ind}_{\partial\Gamma}^{\mathbf{C}}(F_1)$.

Théorème (invariance par homotopie)

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 racine sur $\partial\Gamma$. Alors $\text{ind}_{\partial\Gamma}^{\mathbf{C}}(F_0) = \text{ind}_{\partial\Gamma}^{\mathbf{C}}(F_1)$.

Démonstration. L'absence de racines sur $[0, 1] \times [a, b]$ garantit que

$$\begin{aligned} \text{ind}_{[a,b]}^{\mathbf{C}}(F | T = 0) - \text{ind}_{[a,b]}^{\mathbf{C}}(F | T = 1) \\ = \text{ind}_{[0,1]}^{\mathbf{C}}(F | Z = a) - \text{ind}_{[0,1]}^{\mathbf{C}}(F | Z = b). \end{aligned}$$

Théorème (invariance par homotopie)

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 racine sur $\partial\Gamma$. Alors $\text{ind}_{\partial\Gamma}^{\mathbf{C}}(F_0) = \text{ind}_{\partial\Gamma}^{\mathbf{C}}(F_1)$.

Démonstration. L'absence de racines sur $[0, 1] \times [a, b]$ garantit que

$$\begin{aligned} \text{ind}_{[a,b]}^{\mathbf{C}}(F | T = 0) - \text{ind}_{[a,b]}^{\mathbf{C}}(F | T = 1) \\ = \text{ind}_{[0,1]}^{\mathbf{C}}(F | Z = a) - \text{ind}_{[0,1]}^{\mathbf{C}}(F | Z = b). \end{aligned}$$

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

Théorème (invariance par homotopie)

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 racine sur $\partial\Gamma$. Alors $\text{ind}_{\partial\Gamma}^{\mathbf{C}}(F_0) = \text{ind}_{\partial\Gamma}^{\mathbf{C}}(F_1)$.

Démonstration. L'absence de racines sur $[0, 1] \times [a, b]$ garantit que

$$\begin{aligned} \text{ind}_{[a,b]}^{\mathbf{C}}(F | T = 0) - \text{ind}_{[a,b]}^{\mathbf{C}}(F | T = 1) \\ = \text{ind}_{[0,1]}^{\mathbf{C}}(F | Z = a) - \text{ind}_{[0,1]}^{\mathbf{C}}(F | Z = b). \end{aligned}$$

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

Corollaire

Pour $F \in \mathbf{C}[Z]^*$ et $\Gamma \supset B(\rho_F)$ on a $\text{ind}_{\partial\Gamma}^{\mathbf{C}}(F) = \text{deg } F$.

Théorème (invariance par homotopie)

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 racine sur $\partial\Gamma$. Alors $\text{ind}_{\partial\Gamma}^{\mathbf{C}}(F_0) = \text{ind}_{\partial\Gamma}^{\mathbf{C}}(F_1)$.

Démonstration. L'absence de racines sur $[0, 1] \times [a, b]$ garantit que

$$\begin{aligned} \text{ind}_{[a,b]}^{\mathbf{C}}(F | T = 0) - \text{ind}_{[a,b]}^{\mathbf{C}}(F | T = 1) \\ = \text{ind}_{[0,1]}^{\mathbf{C}}(F | Z = a) - \text{ind}_{[0,1]}^{\mathbf{C}}(F | Z = b). \end{aligned}$$

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

Corollaire

Pour $F \in \mathbf{C}[Z]^*$ et $\Gamma \supset B(\rho_F)$ on a $\text{ind}_{\partial\Gamma}^{\mathbf{C}}(F) = \text{deg } F$.

Démonstration. Soit $F = Z^n + c_{n-1}Z^{n-1} + \dots + c_0$.

Théorème (invariance par homotopie)

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 racine sur $\partial\Gamma$. Alors $\text{ind}_{\partial\Gamma}^{\mathbf{C}}(F_0) = \text{ind}_{\partial\Gamma}^{\mathbf{C}}(F_1)$.

Démonstration. L'absence de racines sur $[0, 1] \times [a, b]$ garantit que

$$\begin{aligned} \text{ind}_{[a,b]}^{\mathbf{C}}(F | T = 0) - \text{ind}_{[a,b]}^{\mathbf{C}}(F | T = 1) \\ = \text{ind}_{[0,1]}^{\mathbf{C}}(F | Z = a) - \text{ind}_{[0,1]}^{\mathbf{C}}(F | Z = b). \end{aligned}$$

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

Corollaire

Pour $F \in \mathbf{C}[Z]^*$ et $\Gamma \supset B(\rho_F)$ on a $\text{ind}_{\partial\Gamma}^{\mathbf{C}}(F) = \text{deg } F$.

Démonstration. Soit $F = Z^n + c_{n-1}Z^{n-1} + \dots + c_0$.

Alors $F_t = Z^n + t(c_{n-1}Z^{n-1} + \dots + c_0)$ déforme $F_1 = F$ en $F_0 = Z^n$.

Théorème (invariance par homotopie)

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 racine sur $\partial\Gamma$. Alors $\text{ind}_{\partial\Gamma}^{\mathbf{C}}(F_0) = \text{ind}_{\partial\Gamma}^{\mathbf{C}}(F_1)$.

Démonstration. L'absence de racines sur $[0, 1] \times [a, b]$ garantit que

$$\begin{aligned} \text{ind}_{[a,b]}^{\mathbf{C}}(F | T = 0) - \text{ind}_{[a,b]}^{\mathbf{C}}(F | T = 1) \\ = \text{ind}_{[0,1]}^{\mathbf{C}}(F | Z = a) - \text{ind}_{[0,1]}^{\mathbf{C}}(F | Z = b). \end{aligned}$$

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

Corollaire

Pour $F \in \mathbf{C}[Z]^*$ et $\Gamma \supset B(\rho_F)$ on a $\text{ind}_{\partial\Gamma}^{\mathbf{C}}(F) = \text{deg } F$.

Démonstration. Soit $F = Z^n + c_{n-1}Z^{n-1} + \dots + c_0$.

Alors $F_t = Z^n + t(c_{n-1}Z^{n-1} + \dots + c_0)$ déforme $F_1 = F$ en $F_0 = Z^n$.

La borne de Cauchy $\rho_t = 1 + tM$ diminue de $\rho_1 = \rho_F$ à $\rho_0 = 1$.

Théorème (invariance par homotopie)

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 racine sur $\partial\Gamma$. Alors $\text{ind}_{\partial\Gamma}^{\mathbf{C}}(F_0) = \text{ind}_{\partial\Gamma}^{\mathbf{C}}(F_1)$.

Démonstration. L'absence de racines sur $[0, 1] \times [a, b]$ garantit que

$$\begin{aligned} \text{ind}_{[a,b]}^{\mathbf{C}}(F | T = 0) - \text{ind}_{[a,b]}^{\mathbf{C}}(F | T = 1) \\ = \text{ind}_{[0,1]}^{\mathbf{C}}(F | Z = a) - \text{ind}_{[0,1]}^{\mathbf{C}}(F | Z = b). \end{aligned}$$

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

Corollaire

Pour $F \in \mathbf{C}[Z]^*$ et $\Gamma \supset B(\rho_F)$ on a $\text{ind}_{\partial\Gamma}^{\mathbf{C}}(F) = \deg F$.

Démonstration. Soit $F = Z^n + c_{n-1}Z^{n-1} + \dots + c_0$.

Alors $F_t = Z^n + t(c_{n-1}Z^{n-1} + \dots + c_0)$ déforme $F_1 = F$ en $F_0 = Z^n$.

La borne de Cauchy $\rho_t = 1 + tM$ diminue de $\rho_1 = \rho_F$ à $\rho_0 = 1$.

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

Théorème (invariance par homotopie)

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 racine sur $\partial\Gamma$. Alors $\text{ind}_{\partial\Gamma}^{\mathbf{C}}(F_0) = \text{ind}_{\partial\Gamma}^{\mathbf{C}}(F_1)$.

Démonstration. L'absence de racines sur $[0, 1] \times [a, b]$ garantit que

$$\begin{aligned} \text{ind}_{[a,b]}^{\mathbf{C}}(F | T = 0) - \text{ind}_{[a,b]}^{\mathbf{C}}(F | T = 1) \\ = \text{ind}_{[0,1]}^{\mathbf{C}}(F | Z = a) - \text{ind}_{[0,1]}^{\mathbf{C}}(F | Z = b). \end{aligned}$$

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

Corollaire

Pour $F \in \mathbf{C}[Z]^*$ et $\Gamma \supset B(\rho_F)$ on a $\text{ind}_{\partial\Gamma}^{\mathbf{C}}(F) = \text{deg } F$.

Démonstration. Soit $F = Z^n + c_{n-1}Z^{n-1} + \dots + c_0$.

Alors $F_t = Z^n + t(c_{n-1}Z^{n-1} + \dots + c_0)$ déforme $F_1 = F$ en $F_0 = Z^n$.

La borne de Cauchy $\rho_t = 1 + tM$ diminue de $\rho_1 = \rho_F$ à $\rho_0 = 1$.

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

Ceci prouve le théorème fondamental : Γ contient n racines de F .

- 1 Le théorème fondamental de l'algèbre
- 2 Sturm 1829/1835 : racines réelles de polynômes réels
- 3 Sturm 1836 : racines complexes de polynômes complexes
- 4 Conclusions et perspectives**

Conclusions et perspectives

Sur tout corps réel clos nous savons construire l'indice algébrique

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

Conclusions et perspectives

Sur tout corps réel clos nous savons construire l'indice algébrique

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

⇒ Preuve élémentaire et effective du théorème fondamental de l'algèbre.

Conclusions et perspectives

Sur tout corps réel clos nous savons construire l'indice algébrique

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

⇒ Preuve élémentaire et effective du théorème fondamental de l'algèbre.

Contrôle sur les degrés algébriques

A-t-on l'équivalence « \mathbf{R} réel n -clos $\iff \mathbf{R}[i]$ algébriquement n -clos » ?

Conclusions et perspectives

Sur tout corps réel clos nous savons construire l'indice algébrique

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

\Rightarrow Preuve élémentaire et effective du théorème fondamental de l'algèbre.

Contrôle sur les degrés algébriques

A-t-on l'équivalence « \mathbf{R} réel n -clos $\iff \mathbf{R}[i]$ algébriquement n -clos » ?

L'implication « \Rightarrow » est valable en petit degré. La réciproque « \Leftarrow » est claire.

Conclusions et perspectives

Sur tout corps réel clos nous savons construire l'indice algébrique

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

\Rightarrow Preuve élémentaire et effective du théorème fondamental de l'algèbre.

Contrôle sur les degrés algébriques

A-t-on l'équivalence « \mathbf{R} réel n -clos $\iff \mathbf{R}[i]$ algébriquement n -clos » ?

L'implication « \Rightarrow » est valable en petit degré. La réciproque « \Leftarrow » est claire.

Optimisation algorithmique : complexité asymptotique

Localisation des racines à b bits d'un polynôme de degré n :

algébrique : $\tilde{O}(n^4 b^2)$ vs numérique : $\tilde{O}(n^2(n+b))$, Schönhage 1982.

Conclusions et perspectives

Sur tout corps réel clos nous savons construire l'indice algébrique

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

⇒ Preuve élémentaire et effective du théorème fondamental de l'algèbre.

Contrôle sur les degrés algébriques

A-t-on l'équivalence « \mathbf{R} réel n -clos $\iff \mathbf{R}[i]$ algébriquement n -clos » ?

L'implication « \implies » est valable en petit degré. La réciproque « \impliedby » est claire.

Optimisation algorithmique : complexité asymptotique

Localisation des racines à b bits d'un polynôme de degré n :
algébrique : $\tilde{O}(n^4 b^2)$ vs numérique : $\tilde{O}(n^2(n+b))$, Schönhage 1982.

Comment rendre la version algébrique plus efficace ?

Conclusions et perspectives

Sur tout corps réel clos nous savons construire l'indice algébrique

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

⇒ Preuve élémentaire et effective du théorème fondamental de l'algèbre.

Contrôle sur les degrés algébriques

A-t-on l'équivalence « \mathbf{R} réel n -clos $\iff \mathbf{R}[i]$ algébriquement n -clos » ?

L'implication « \Rightarrow » est valable en petit degré. La réciproque « \Leftarrow » est claire.

Optimisation algorithmique : complexité asymptotique

Localisation des racines à b bits d'un polynôme de degré n :
algébrique : $\tilde{O}(n^4 b^2)$ vs numérique : $\tilde{O}(n^2(n+b))$, Schönhage 1982.

Comment rendre la version algébrique plus efficace ?

Indice algébrique en dimension supérieure

Théorème du point fixe de Brouwer sur des corps réels clos.

Conclusions et perspectives

Sur tout corps réel clos nous savons construire l'indice algébrique

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

⇒ Preuve élémentaire et effective du théorème fondamental de l'algèbre.

Contrôle sur les degrés algébriques

A-t-on l'équivalence « \mathbf{R} réel n -clos $\iff \mathbf{R}[i]$ algébriquement n -clos » ?

L'implication « \implies » est valable en petit degré. La réciproque « \impliedby » est claire.

Optimisation algorithmique : complexité asymptotique

Localisation des racines à b bits d'un polynôme de degré n :
algébrique : $\tilde{O}(n^4 b^2)$ vs numérique : $\tilde{O}(n^2(n+b))$, Schönhage 1982.

Comment rendre la version algébrique plus efficace ?

Indice algébrique en dimension supérieure

Théorème du point fixe de Brouwer sur des corps réels clos.

Contrôle sur les degrés algébriques ?



Je vous remercie de votre attention !

Michael.Eisermann@ujf-grenoble.fr
www-fourier.ujf-grenoble.fr/~eiserm

*The Fundamental Theorem of Algebra made effective :
an elementary real-algebraic proof via Sturm chains*

Vos remarques et suggestions seront les bienvenues !