

Equacions Algebraiques

Xevi Guitart

Algunes cares

Algunes cares



Algunes cares



Evariste Galois (1811-1832)

Algunes cares



Evariste Galois (1811-1832)



Algunes cares



Evariste Galois (1811-1832)



Emmy Noether
(1882-1935)

Algunes cares



Evariste Galois (1811-1832)



Emmy Noether
(1882-1935)



Algunes cares



Evariste Galois (1811-1832)



Emmy Noether
(1882-1935)



Emil Artin (1898-1962)

Introducció

- En aquest curs veurem **Teoria de Galois**

- ▶ Connexió entre dos tipus d'objectes algebraics:

grups i cossos

Definició de cos

Un cos F és un anell commutatiu unitari on tot element $\neq 0_F$ té invers pel producte i $1_F \neq 0_F$.

Exemples

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ si p és primer.

- Motivació (històrica): problema de la resolubilitat d'equacions polinòmiques per radicals.

Introducció

- En aquest curs veurem **Teoria de Galois**
 - ▶ Connexió entre dos tipus d'objectes algebraics:

grups i **cossos**

Definició de cos

Un cos F és un anell commutatiu unitari on tot element $\neq 0_F$ té invers pel producte i $1_F \neq 0_F$.

Exemples

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ si p és primer.

- Motivació (històrica): problema de la resolubilitat d'equacions polinòmiques per radicals.

Introducció

- En aquest curs veurem **Teoria de Galois**
 - ▶ Connexió entre dos tipus d'objectes algebraics:

grups i **cossos**

Definició de cos

Un cos F és un anell commutatiu unitari on tot element $\neq 0_F$ té invers pel producte i $1_F \neq 0_F$.

Exemples

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ si p és primer.

- Motivació (històrica): problema de la resolubilitat d'equacions polinòmiques per radicals.

Introducció

- En aquest curs veurem **Teoria de Galois**
 - ▶ Connexió entre dos tipus d'objectes algebraics:

grups i **cossos**

Definició de cos

Un cos F és un anell commutatiu unitari on tot element $\neq 0_F$ té invers pel producte i $1_F \neq 0_F$.

Exemples

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ si p és primer.

- Motivació (històrica): problema de la resolubilitat d'equacions polinòmiques per radicals.

Introducció

- En aquest curs veurem **Teoria de Galois**
 - ▶ Connexió entre dos tipus d'objectes algebraics:

grups i **cossos**

Definició de cos

Un cos F és un anell commutatiu unitari on tot element $\neq 0_F$ té invers pel producte i $1_F \neq 0_F$.

Exemples

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ si p és primer.

- Motivació (històrica): problema de la resolubilitat d'equacions polinòmiques per radicals.

Resolubilitat per radicals

- Grau 2: $ax^2 + bx + c \rightsquigarrow$ arrels: $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
 - ▶ Fórmula per les arrels en termes de: coeficients i $+$, $-$, $\cdot$, $\div$ i $\sqrt{}$
 - ▶ Diem que l'equació quadràtica general és **resoluble per radicals**
- Graus 3 i 4: també hi ha fórmules (les veureu a problemes)
- Segles XVI-XIX: els matemàtics cercaven fórmules per graus ≥ 5
- No hi ha fórmula general per polinomis de grau ≥ 5 (Abel–Rufini)
- Això no resol del tot el problema:
 - ▶ Hi ha polinomis en què les arrels es poden expressar per radicals a partir dels coeficients, e.g., $x^5 - 7$
 - ▶ Hi ha polinomis en què això no sigui cert?
 - ▶ Potser no hi ha una fórmula que valgui per a tots els polinomis, sinó diferents fórmules
- Galois: caracteritza quan les arrels d'un polinomi es poden expressar per radicals, en termes de teoria de grups
 - ▶ De fet Galois inventa la noció i el terme grup
- Artin i Noether transformen la teoria de Galois, centrant-la en la teoria de cossos i emprant l'àlgebra lineal com a eina fonamental
 - ▶ Aquesta visió és essencialment la que s'estudia avui en dia

Resolubilitat per radicals

- Grau 2: $ax^2 + bx + c \rightsquigarrow$ arrels: $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
 - ▶ Fórmula per les arrels en termes de: coeficients i $+$, $-$, $\cdot$, $\div$ i $\sqrt[n]{\cdot}$
 - ▶ Diem que l'equació quadràtica general és **resoluble per radicals**
- Graus 3 i 4: també hi ha fórmules (les veureu a problemes)
- Segles XVI-XIX: els matemàtics cercaven fórmules per graus ≥ 5
- No hi ha fórmula general per polinomis de grau ≥ 5 (Abel–Rufini)
- Això no resol del tot el problema:
 - ▶ Hi ha polinomis en què les arrels es poden expressar per radicals a partir dels coeficients, e.g., $x^5 - 7$
 - ▶ Hi ha polinomis en què això no sigui cert?
 - ▶ Potser no hi ha una fórmula que valgui per a tots els polinomis, sinó diferents fórmules
- Galois: caracteritza quan les arrels d'un polinomi es poden expressar per radicals, en termes de teoria de grups
 - ▶ De fet Galois inventa la noció i el terme grup
- Artin i Noether transformen la teoria de Galois, centrant-la en la teoria de cossos i emprant l'àlgebra lineal com a eina fonamental
 - ▶ Aquesta visió és essencialment la que s'estudia avui en dia

Resolubilitat per radicals

- Grau 2: $ax^2 + bx + c \rightsquigarrow$ arrels: $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
 - ▶ Fórmula per les arrels en termes de: coeficients i $+$, $-$, $\cdot$, $\div$ i $\sqrt[n]{\cdot}$
 - ▶ Diem que l'equació quadràtica general és **resoluble per radicals**
- Graus 3 i 4: també hi ha fórmules (les veureu a problemes)
- Segles XVI-XIX: els matemàtics cercaven fórmules per graus ≥ 5
- No hi ha fórmula general per polinomis de grau ≥ 5 (Abel–Rufini)
- Això no resol del tot el problema:
 - ▶ Hi ha polinomis en què les arrels es poden expressar per radicals a partir dels coeficients, e.g., $x^5 - 7$
 - ▶ Hi ha polinomis en què això no sigui cert?
 - ▶ Potser no hi ha una fórmula que valgui per a tots els polinomis, sinó diferents fórmules
- Galois: caracteritza quan les arrels d'un polinomi es poden expressar per radicals, en termes de teoria de grups
 - ▶ De fet Galois inventa la noció i el terme grup
- Artin i Noether transformen la teoria de Galois, centrant-la en la teoria de cossos i emprant l'àlgebra lineal com a eina fonamental
 - ▶ Aquesta visió és essencialment la que s'estudia avui en dia

Resolubilitat per radicals

- Grau 2: $ax^2 + bx + c \rightsquigarrow$ arrels: $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
 - ▶ Fórmula per les arrels en termes de: coeficients i $+$, $-$, $\cdot$, $\div$ i $\sqrt[n]{}$
 - ▶ Diem que l'equació quadràtica general és **resoluble per radicals**
- Graus 3 i 4: també hi ha fórmules (les veureu a problemes)
- Segles XVI-XIX: els matemàtics cercaven fórmules per graus ≥ 5
- No hi ha fórmula general per polinomis de grau ≥ 5 (Abel–Rufini)
- Això no resol del tot el problema:
 - ▶ Hi ha polinomis en què les arrels es poden expressar per radicals a partir dels coeficients, e.g., $x^5 - 7$
 - ▶ Hi ha polinomis en què això no sigui cert?
 - ▶ Potser no hi ha una fórmula que valgui per a tots els polinomis, sinó diferents fórmules
- Galois: caracteritza quan les arrels d'un polinomi es poden expressar per radicals, en termes de teoria de grups
 - ▶ De fet Galois inventa la noció i el terme grup
- Artin i Noether transformen la teoria de Galois, centrant-la en la teoria de cossos i emprant l'àlgebra lineal com a eina fonamental
 - ▶ Aquesta visió és essencialment la que s'estudia avui en dia

Resolubilitat per radicals

- Grau 2: $ax^2 + bx + c \rightsquigarrow$ arrels: $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
 - ▶ Fórmula per les arrels en termes de: coeficients i $+$, $-$, $\cdot$, $\div$ i $\sqrt[n]{}$
 - ▶ Diem que l'equació quadràtica general és **resoluble per radicals**
- Graus 3 i 4: també hi ha fórmules (les veureu a problemes)
- Segles XVI-XIX: els matemàtics cercaven fórmules per graus ≥ 5
- No hi ha fórmula general per polinomis de grau ≥ 5 (Abel–Rufini)
- Això no resol del tot el problema:
 - ▶ Hi ha polinomis en què les arrels es poden expressar per radicals a partir dels coeficients, e.g., $x^5 - 7$
 - ▶ Hi ha polinomis en què això no sigui cert?
 - ▶ Potser no hi ha una fórmula que valgui per a tots els polinomis, sinó diferents fórmules
- Galois: caracteritza quan les arrels d'un polinomi es poden expressar per radicals, en termes de teoria de grups
 - ▶ De fet Galois inventa la noció i el terme grup
- Artin i Noether transformen la teoria de Galois, centrant-la en la teoria de cossos i emprant l'àlgebra lineal com a eina fonamental
 - ▶ Aquesta visió és essencialment la que s'estudia avui en dia

Resolubilitat per radicals

- Grau 2: $ax^2 + bx + c \rightsquigarrow$ arrels: $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
 - ▶ Fórmula per les arrels en termes de: coeficients i $+$, $-$, $\cdot$, $\div$ i $\sqrt[n]{}$
 - ▶ Diem que l'equació quadràtica general és **resoluble per radicals**
- Graus 3 i 4: també hi ha fórmules (les veureu a problemes)
- Segles XVI-XIX: els matemàtics cercaven fórmules per graus ≥ 5
- No hi ha fórmula general per polinomis de grau ≥ 5 (Abel–Rufini)
- Això no resol del tot el problema:
 - ▶ Hi ha polinomis en què les arrels es poden expressar per radicals a partir dels coeficients, e.g., $x^5 - 7$
 - ▶ Hi ha polinomis en què això no sigui cert?
 - ▶ Potser no hi ha una fórmula que valgui per a tots els polinomis, sinó diferents fórmules
- Galois: caracteritza quan les arrels d'un polinomi es poden expressar per radicals, en termes de teoria de grups
 - ▶ De fet Galois inventa la noció i el terme grup
- Artin i Noether transformen la teoria de Galois, centrant-la en la teoria de cossos i emprant l'àlgebra lineal com a eina fonamental
 - ▶ Aquesta visió és essencialment la que s'estudia avui en dia

Resolubilitat per radicals

- Grau 2: $ax^2 + bx + c \rightsquigarrow$ arrels: $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
 - ▶ Fórmula per les arrels en termes de: coeficients i $+$, $-$, $\cdot$, $\div$ i $\sqrt[n]{}$
 - ▶ Diem que l'equació quadràtica general és **resoluble per radicals**
- Graus 3 i 4: també hi ha fórmules (les veureu a problemes)
- Segles XVI-XIX: els matemàtics cercaven fórmules per graus ≥ 5
- No hi ha fórmula general per polinomis de grau ≥ 5 (Abel–Rufini)
- Això no resol del tot el problema:
 - ▶ Hi ha polinomis en què les arrels es poden expressar per radicals a partir dels coeficients, e.g., $x^5 - 7$
 - ▶ Hi ha polinomis en què això no sigui cert?
 - ▶ Potser no hi ha una fórmula que valgui per a tots els polinomis, sinó diferents fórmules
- Galois: caracteritza quan les arrels d'un polinomi es poden expressar per radicals, en termes de teoria de grups
 - ▶ De fet Galois inventa la noció i el terme grup
- Artin i Noether transformen la teoria de Galois, centrant-la en la teoria de cossos i emprant l'àlgebra lineal com a eina fonamental
 - ▶ Aquesta visió és essencialment la que s'estudia avui en dia

Resolubilitat per radicals

- Grau 2: $ax^2 + bx + c \rightsquigarrow$ arrels: $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
 - ▶ Fórmula per les arrels en termes de: coeficients i $+$, $-$, $\cdot$, $\div$ i $\sqrt[n]{}$
 - ▶ Diem que l'equació quadràtica general és **resoluble per radicals**
- Graus 3 i 4: també hi ha fórmules (les veureu a problemes)
- Segles XVI-XIX: els matemàtics cercaven fórmules per graus ≥ 5
- No hi ha fórmula general per polinomis de grau ≥ 5 (Abel–Rufini)
- Això no resol del tot el problema:
 - ▶ Hi ha polinomis en què les arrels es poden expressar per radicals a partir dels coeficients, e.g., $x^5 - 7$
 - ▶ Hi ha polinomis en què això no sigui cert?
 - ▶ Potser no hi ha una fórmula que valgui per a tots els polinomis, sinó diferents fórmules
- Galois: caracteritza quan les arrels d'un polinomi es poden expressar per radicals, en termes de teoria de grups
 - ▶ De fet Galois inventa la noció i el terme grup
- Artin i Noether transformen la teoria de Galois, centrant-la en la teoria de cossos i emprant l'àlgebra lineal com a eina fonamental
 - ▶ Aquesta visió és essencialment la que s'estudia avui en dia

Resolubilitat per radicals

- Grau 2: $ax^2 + bx + c \rightsquigarrow$ arrels: $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
 - ▶ Fórmula per les arrels en termes de: coeficients i $+$, $-$, $\cdot$, $\div$ i $\sqrt[n]{\cdot}$
 - ▶ Diem que l'equació quadràtica general és **resoluble per radicals**
- Graus 3 i 4: també hi ha fórmules (les veureu a problemes)
- Segles XVI-XIX: els matemàtics cercaven fórmules per graus ≥ 5
- No hi ha fórmula general per polinomis de grau ≥ 5 (Abel–Rufini)
- Això no resol del tot el problema:
 - ▶ Hi ha polinomis en què les arrels es poden expressar per radicals a partir dels coeficients, e.g., $x^5 - 7$
 - ▶ Hi ha polinomis en què això no sigui cert?
 - ▶ Potser no hi ha una fórmula que valgui per a tots els polinomis, sinó diferents fórmules
- Galois: caracteritza quan les arrels d'un polinomi es poden expressar per radicals, en termes de teoria de grups
 - ▶ De fet Galois inventa la noció i el terme grup
- Artin i Noether transformen la teoria de Galois, centrant-la en la teoria de cossos i emprant l'àlgebra lineal com a eina fonamental
 - ▶ Aquesta visió és essencialment la que s'estudia avui en dia

Resolubilitat per radicals

- Grau 2: $ax^2 + bx + c \rightsquigarrow$ arrels: $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
 - ▶ Fórmula per les arrels en termes de: coeficients i $+$, $-$, $\cdot$, $\div$ i $\sqrt[n]{\cdot}$
 - ▶ Diem que l'equació quadràtica general és **resoluble per radicals**
- Graus 3 i 4: també hi ha fórmules (les veureu a problemes)
- Segles XVI-XIX: els matemàtics cercaven fórmules per graus ≥ 5
- No hi ha fórmula general per polinomis de grau ≥ 5 (Abel–Rufini)
- Això no resol del tot el problema:
 - ▶ Hi ha polinomis en què les arrels es poden expressar per radicals a partir dels coeficients, e.g., $x^5 - 7$
 - ▶ Hi ha polinomis en què això no sigui cert?
 - ▶ Potser no hi ha una fórmula que valgui per a tots els polinomis, sinó diferents fórmules
- Galois: caracteritza quan les arrels d'un polinomi es poden expressar per radicals, en termes de teoria de grups
 - ▶ De fet Galois inventa la noció i el terme grup
- Artin i Noether transformen la teoria de Galois, centrant-la en la teoria de cossos i emprant l'àlgebra lineal com a eina fonamental
 - ▶ Aquesta visió és essencialment la que s'estudia avui en dia

Resolubilitat per radicals

- Grau 2: $ax^2 + bx + c \rightsquigarrow$ arrels: $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
 - ▶ Fórmula per les arrels en termes de: coeficients i $+$, $-$, $\cdot$, $\div$ i $\sqrt[n]{}$
 - ▶ Diem que l'equació quadràtica general és **resoluble per radicals**
- Graus 3 i 4: també hi ha fórmules (les veureu a problemes)
- Segles XVI-XIX: els matemàtics cercaven fórmules per graus ≥ 5
- No hi ha fórmula general per polinomis de grau ≥ 5 (Abel–Rufini)
- Això no resol del tot el problema:
 - ▶ Hi ha polinomis en què les arrels es poden expressar per radicals a partir dels coeficients, e.g., $x^5 - 7$
 - ▶ Hi ha polinomis en què això no sigui cert?
 - ▶ Potser no hi ha una fórmula que valgui per a tots els polinomis, sinó diferents fórmules
- Galois: caracteritza quan les arrels d'un polinomi es poden expressar per radicals, en termes de teoria de grups
 - ▶ De fet Galois inventa la noció i el terme grup
- Artin i Noether transformen la teoria de Galois, centrant-la en la teoria de cossos i emprant l'àlgebra lineal com a eina fonamental
 - ▶ Aquesta visió és essencialment la que s'estudia avui en dia

Resolubilitat per radicals

- Grau 2: $ax^2 + bx + c \rightsquigarrow$ arrels: $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
 - ▶ Fórmula per les arrels en termes de: coeficients i $+$, $-$, $\cdot$, $\div$ i $\sqrt[n]{}$
 - ▶ Diem que l'equació quadràtica general és **resoluble per radicals**
- Graus 3 i 4: també hi ha fórmules (les veureu a problemes)
- Segles XVI-XIX: els matemàtics cercaven fórmules per graus ≥ 5
- No hi ha fórmula general per polinomis de grau ≥ 5 (Abel–Rufini)
- Això no resol del tot el problema:
 - ▶ Hi ha polinomis en què les arrels es poden expressar per radicals a partir dels coeficients, e.g., $x^5 - 7$
 - ▶ Hi ha polinomis en què això no sigui cert?
 - ▶ Potser no hi ha una fórmula que valgui per a tots els polinomis, sinó diferents fórmules
- Galois: caracteritza quan les arrels d'un polinomi es poden expressar per radicals, en termes de teoria de grups
 - ▶ De fet Galois inventa la noció i el terme grup
- Artin i Noether transformen la teoria de Galois, centrant-la en la teoria de cossos i emprant l'àlgebra lineal com a eina fonamental
 - ▶ Aquesta visió és essencialment la que s'estudia avui en dia

Resolubilitat per radicals

- Grau 2: $ax^2 + bx + c \rightsquigarrow$ arrels: $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
 - ▶ Fórmula per les arrels en termes de: coeficients i $+$, $-$, $\cdot$, $\div$ i $\sqrt[n]{}$
 - ▶ Diem que l'equació quadràtica general és **resoluble per radicals**
- Graus 3 i 4: també hi ha fórmules (les veureu a problemes)
- Segles XVI-XIX: els matemàtics cercaven fórmules per graus ≥ 5
- No hi ha fórmula general per polinomis de grau ≥ 5 (Abel–Rufini)
- Això no resol del tot el problema:
 - ▶ Hi ha polinomis en què les arrels es poden expressar per radicals a partir dels coeficients, e.g., $x^5 - 7$
 - ▶ Hi ha polinomis en què això no sigui cert?
 - ▶ Potser no hi ha una fórmula que valgui per a tots els polinomis, sinó diferents fórmules
- Galois: caracteritza quan les arrels d'un polinomi es poden expressar per radicals, en termes de teoria de grups
 - ▶ De fet Galois inventa la noció i el terme grup
- Artin i Noether transformen la teoria de Galois, centrant-la en la teoria de cossos i emprant l'àlgebra lineal com a eina fonamental
 - ▶ Aquesta visió és essencialment la que s'estudia avui en dia

Teoria de Galois

Idea (moderna)

Donat un polinomi $f \in \mathbb{Q}[x]$ li associem un cos K_f

$K_f =$ cos més petit que conté les arrels de f

- Exemple: $f = x^2 + 1 \rightsquigarrow K_f = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$
- Problemes sobre $f \longleftrightarrow$ problemes sobre K_f

Teoria de Galois

$K_f \rightsquigarrow$ grup finit $\text{Gal}(K_f/\mathbb{Q})$, de manera que

- Problemes sobre $K_f \longleftrightarrow$ problemes sobre $\text{Gal}(K_f/\mathbb{Q})$

Teorema (Galois)

$f \in \mathbb{Q}[x]$ resoluble per radicals $\iff \text{Gal}(K_f/\mathbb{Q})$ resoluble

- $f = x^5 - x - 1$ té $\text{Gal}(K_f/\mathbb{Q}) \simeq S_5$, per tant no és resoluble
- Més en general: $f \in F[x]$ amb F un cos qualsevol
 - ▶ $F \subset K_f$ que conté les arrels de f
 - ▶ K_f es diu que és una extensió de $F \rightsquigarrow$ paper central en la teoria

Teoria de Galois

Idea (moderna)

Donat un polinomi $f \in \mathbb{Q}[x]$ li associem un cos K_f

$K_f =$ cos més petit que conté les arrels de f

- Exemple: $f = x^2 + 1 \rightsquigarrow K_f = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$
- Problemes sobre $f \longleftrightarrow$ problemes sobre K_f

Teoria de Galois

$K_f \rightsquigarrow$ grup finit $\text{Gal}(K_f/\mathbb{Q})$, de manera que

- Problemes sobre $K_f \longleftrightarrow$ problemes sobre $\text{Gal}(K_f/\mathbb{Q})$

Teorema (Galois)

$f \in \mathbb{Q}[x]$ resoluble per radicals $\iff \text{Gal}(K_f/\mathbb{Q})$ resoluble

- $f = x^5 - x - 1$ té $\text{Gal}(K_f/\mathbb{Q}) \simeq S_5$, per tant no és resoluble
- Més en general: $f \in F[x]$ amb F un cos qualsevol
 - ▶ $F \subset K_f$ que conté les arrels de f
 - ▶ K_f es diu que és una extensió de $F \rightsquigarrow$ paper central en la teoria

Teoria de Galois

Idea (moderna)

Donat un polinomi $f \in \mathbb{Q}[x]$ li associem un cos K_f

$K_f =$ cos més petit que conté les arrels de f

- Exemple: $f = x^2 + 1 \rightsquigarrow K_f = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$
- Problemes sobre $f \longleftrightarrow$ problemes sobre K_f

Teoria de Galois

$K_f \rightsquigarrow$ grup finit $\text{Gal}(K_f/\mathbb{Q})$, de manera que

- Problemes sobre $K_f \longleftrightarrow$ problemes sobre $\text{Gal}(K_f/\mathbb{Q})$

Teorema (Galois)

$f \in \mathbb{Q}[x]$ resoluble per radicals $\iff \text{Gal}(K_f/\mathbb{Q})$ resoluble

- $f = x^5 - x - 1$ té $\text{Gal}(K_f/\mathbb{Q}) \simeq S_5$, per tant no és resoluble
- Més en general: $f \in F[x]$ amb F un cos qualsevol
 - ▶ $F \subset K_f$ que conté les arrels de f
 - ▶ K_f es diu que és una extensió de $F \rightsquigarrow$ paper central en la teoria

Teoria de Galois

Idea (moderna)

Donat un polinomi $f \in \mathbb{Q}[x]$ li associem un cos K_f

$K_f =$ cos més petit que conté les arrels de f

- Exemple: $f = x^2 + 1 \rightsquigarrow K_f = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$
- Problemes sobre $f \longleftrightarrow$ problemes sobre K_f

Teoria de Galois

$K_f \rightsquigarrow$ grup finit $\text{Gal}(K_f/\mathbb{Q})$, de manera que

- Problemes sobre $K_f \longleftrightarrow$ problemes sobre $\text{Gal}(K_f/\mathbb{Q})$

Teorema (Galois)

$f \in \mathbb{Q}[x]$ resoluble per radicals $\iff \text{Gal}(K_f/\mathbb{Q})$ resoluble

- $f = x^5 - x - 1$ té $\text{Gal}(K_f/\mathbb{Q}) \simeq S_5$, per tant no és resoluble
- Més en general: $f \in F[x]$ amb F un cos qualsevol
 - ▶ $F \subset K_f$ que conté les arrels de f
 - ▶ K_f es diu que és una extensió de $F \rightsquigarrow$ paper central en la teoria

Teoria de Galois

Idea (moderna)

Donat un polinomi $f \in \mathbb{Q}[x]$ li associem un cos K_f

$K_f =$ cos més petit que conté les arrels de f

- Exemple: $f = x^2 + 1 \rightsquigarrow K_f = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$
- Problemes sobre $f \longleftrightarrow$ problemes sobre K_f

Teoria de Galois

$K_f \rightsquigarrow$ grup finit $\text{Gal}(K_f/\mathbb{Q})$, de manera que

- Problemes sobre $K_f \longleftrightarrow$ problemes sobre $\text{Gal}(K_f/\mathbb{Q})$

Teorema (Galois)

$f \in \mathbb{Q}[x]$ resoluble per radicals $\iff \text{Gal}(K_f/\mathbb{Q})$ resoluble

- $f = x^5 - x - 1$ té $\text{Gal}(K_f/\mathbb{Q}) \simeq S_5$, per tant no és resoluble
- Més en general: $f \in F[x]$ amb F un cos qualsevol
 - ▶ $F \subset K_f$ que conté les arrels de f
 - ▶ K_f es diu que és una extensió de $F \rightsquigarrow$ paper central en la teoria

Teoria de Galois

Idea (moderna)

Donat un polinomi $f \in \mathbb{Q}[x]$ li associem un cos K_f

$K_f =$ cos més petit que conté les arrels de f

- Exemple: $f = x^2 + 1 \rightsquigarrow K_f = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$
- Problemes sobre $f \longleftrightarrow$ problemes sobre K_f

Teoria de Galois

$K_f \rightsquigarrow$ grup finit $\text{Gal}(K_f/\mathbb{Q})$, de manera que

- Problemes sobre $K_f \longleftrightarrow$ problemes sobre $\text{Gal}(K_f/\mathbb{Q})$

Teorema (Galois)

$f \in \mathbb{Q}[x]$ resoluble per radicals $\iff \text{Gal}(K_f/\mathbb{Q})$ resoluble

- $f = x^5 - x - 1$ té $\text{Gal}(K_f/\mathbb{Q}) \simeq S_5$, per tant no és resoluble
- Més en general: $f \in F[x]$ amb F un cos qualsevol
 - ▶ $F \subset K_f$ que conté les arrels de f
 - ▶ K_f es diu que és una extensió de $F \rightsquigarrow$ paper central en la teoria

Teoria de Galois

Idea (moderna)

Donat un polinomi $f \in \mathbb{Q}[x]$ li associem un cos K_f

$K_f =$ cos més petit que conté les arrels de f

- Exemple: $f = x^2 + 1 \rightsquigarrow K_f = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$
- Problemes sobre $f \longleftrightarrow$ problemes sobre K_f

Teoria de Galois

$K_f \rightsquigarrow$ grup finit $\text{Gal}(K_f/\mathbb{Q})$, de manera que

- Problemes sobre $K_f \longleftrightarrow$ problemes sobre $\text{Gal}(K_f/\mathbb{Q})$

Teorema (Galois)

$f \in \mathbb{Q}[x]$ resoluble per radicals $\iff \text{Gal}(K_f/\mathbb{Q})$ resoluble

- $f = x^5 - x - 1$ té $\text{Gal}(K_f/\mathbb{Q}) \simeq S_5$, per tant no és resoluble
- Més en general: $f \in F[x]$ amb F un cos qualsevol

• $F \subset K_f$ que conté les arrels de f

• K_f es diu que és una extensió de $F \rightsquigarrow$ paper central en la teoria

Teoria de Galois

Idea (moderna)

Donat un polinomi $f \in \mathbb{Q}[x]$ li associem un cos K_f

$K_f =$ cos més petit que conté les arrels de f

- Exemple: $f = x^2 + 1 \rightsquigarrow K_f = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$
- Problemes sobre $f \longleftrightarrow$ problemes sobre K_f

Teoria de Galois

$K_f \rightsquigarrow$ grup finit $\text{Gal}(K_f/\mathbb{Q})$, de manera que

- Problemes sobre $K_f \longleftrightarrow$ problemes sobre $\text{Gal}(K_f/\mathbb{Q})$

Teorema (Galois)

$f \in \mathbb{Q}[x]$ resoluble per radicals $\iff \text{Gal}(K_f/\mathbb{Q})$ resoluble

- $f = x^5 - x - 1$ té $\text{Gal}(K_f/\mathbb{Q}) \simeq S_5$, per tant no és resoluble
- Més en general: $f \in F[x]$ amb F un cos qualsevol
 - ▶ $F \subset K_f$ que conté les arrels de f
 - ▶ K_f es diu que és una **extensió** de $F \rightsquigarrow$ paper central en la teoria

Teoria de Galois

Idea (moderna)

Donat un polinomi $f \in \mathbb{Q}[x]$ li associem un cos K_f

$K_f =$ cos més petit que conté les arrels de f

- Exemple: $f = x^2 + 1 \rightsquigarrow K_f = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$
- Problemes sobre $f \longleftrightarrow$ problemes sobre K_f

Teoria de Galois

$K_f \rightsquigarrow$ grup finit $\text{Gal}(K_f/\mathbb{Q})$, de manera que

- Problemes sobre $K_f \longleftrightarrow$ problemes sobre $\text{Gal}(K_f/\mathbb{Q})$

Teorema (Galois)

$f \in \mathbb{Q}[x]$ resoluble per radicals $\iff \text{Gal}(K_f/\mathbb{Q})$ resoluble

- $f = x^5 - x - 1$ té $\text{Gal}(K_f/\mathbb{Q}) \simeq S_5$, per tant no és resoluble
- Més en general: $f \in F[x]$ amb F un cos qualsevol
 - ▶ $F \subset K_f$ que conté les arrels de f
 - ▶ K_f es diu que és una extensió de $F \rightsquigarrow$ paper central en la teoria

Teoria de Galois

Idea (moderna)

Donat un polinomi $f \in \mathbb{Q}[x]$ li associem un cos K_f

$K_f =$ cos més petit que conté les arrels de f

- Exemple: $f = x^2 + 1 \rightsquigarrow K_f = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$
- Problemes sobre $f \longleftrightarrow$ problemes sobre K_f

Teoria de Galois

$K_f \rightsquigarrow$ grup finit $\text{Gal}(K_f/\mathbb{Q})$, de manera que

- Problemes sobre $K_f \longleftrightarrow$ problemes sobre $\text{Gal}(K_f/\mathbb{Q})$

Teorema (Galois)

$f \in \mathbb{Q}[x]$ resoluble per radicals $\iff \text{Gal}(K_f/\mathbb{Q})$ resoluble

- $f = x^5 - x - 1$ té $\text{Gal}(K_f/\mathbb{Q}) \simeq S_5$, per tant no és resoluble
- Més en general: $f \in F[x]$ amb F un cos qualsevol
 - ▶ $F \subset K_f$ que conté les arrels de f
 - ▶ K_f es diu que és una **extensió** de $F \rightsquigarrow$ paper central en la teoria

Aplicacions de la teoria de Galois

- A problemes clàssics de construccions amb regla i compàs:
 - ▶ La quadratura del cercle
 - ▶ La trisecció de l'angle
 - ▶ Doblar el cub
 - ▶ Caracteritzar quins polígons regulars es poden construir amb regla i compàs. Per exemple el pentàgon sí, però l'heptàgon no. El de 17 costats també (Gauss)
- Paper central en la matemàtica actual en camps com
 - ▶ Teoria de nombres
 - ▶ Geometria algebraica aritmètica
 - ▶ Teoria de codis correctors d'errors
 - ▶ Criptografia

Aplicacions de la teoria de Galois

- A problemes clàssics de construccions amb regla i compàs:
 - ▶ La quadratura del cercle
 - ▶ La trisecció de l'angle
 - ▶ Doblar el cub
 - ▶ Caracteritzar quins polígons regulars es poden construir amb regla i compàs. Per exemple el pentàgon sí, però l'heptàgon no. El de 17 costats també (Gauss)
- Paper central en la matemàtica actual en camps com
 - ▶ Teoria de nombres
 - ▶ Geometria algebraica aritmètica
 - ▶ Teoria de codis correctors d'errors
 - ▶ Criptografia

Aplicacions de la teoria de Galois

- A problemes clàssics de construccions amb regla i compàs:
 - ▶ La quadratura del cercle
 - ▶ La trisecció de l'angle
 - ▶ Doblar el cub
 - ▶ Caracteritzar quins polígons regulars es poden construir amb regla i compàs. Per exemple el pentàgon sí, però l'heptàgon no. El de 17 costats també (Gauss)
- Paper central en la matemàtica actual en camps com
 - ▶ Teoria de nombres
 - ▶ Geometria algebraica aritmètica
 - ▶ Teoria de codis correctors d'errors
 - ▶ Criptografia

Aplicacions de la teoria de Galois

- A problemes clàssics de construccions amb regla i compàs:
 - ▶ La quadratura del cercle
 - ▶ La trisecció de l'angle
 - ▶ Doblar el cub
 - ▶ Caracteritzar quins polígons regulars es poden construir amb regla i compàs. Per exemple el pentàgon sí, però l'heptàgon no. El de 17 costats també (Gauss)
- Paper central en la matemàtica actual en camps com
 - ▶ Teoria de nombres
 - ▶ Geometria algebraica aritmètica
 - ▶ Teoria de codis correctors d'errors
 - ▶ Criptografia

Aplicacions de la teoria de Galois

- A problemes clàssics de construccions amb regla i compàs:
 - ▶ La quadratura del cercle
 - ▶ La trisecció de l'angle
 - ▶ Doblar el cub
 - ▶ Caracteritzar quins polígons regulars es poden construir amb regla i compàs. Per exemple el pentàgon sí, però l'heptàgon no. El de 17 costats també (Gauss)
- Paper central en la matemàtica actual en camps com
 - ▶ Teoria de nombres
 - ▶ Geometria algebraica aritmètica
 - ▶ Teoria de codis correctors d'errors
 - ▶ Criptografia

Aplicacions de la teoria de Galois

- A problemes clàssics de construccions amb regla i compàs:
 - ▶ La quadratura del cercle
 - ▶ La trisecció de l'angle
 - ▶ Doblar el cub
 - ▶ Caracteritzar quins polígons regulars es poden construir amb regla i compàs. Per exemple el pentàgon sí, però l'heptàgon no. El de 17 costats també (Gauss)
- Paper central en la matemàtica actual en camps com
 - ▶ Teoria de nombres
 - ▶ Geometria algebraica aritmètica
 - ▶ Teoria de codis correctors d'errors
 - ▶ Criptografia

Aplicacions de la teoria de Galois

- A problemes clàssics de construccions amb regla i compàs:
 - ▶ La quadratura del cercle
 - ▶ La trisecció de l'angle
 - ▶ Doblar el cub
 - ▶ Caracteritzar quins polígons regulars es poden construir amb regla i compàs. Per exemple el pentàgon sí, però l'heptàgon no. El de 17 costats també (Gauss)
- Paper central en la matemàtica actual en camps com
 - ▶ Teoria de nombres
 - ▶ Geometria algebraica aritmètica
 - ▶ Teoria de codis correctors d'errors
 - ▶ Criptografia

Galois: el personatge



Evariste Galois (1811-1832)

- El 1830 sotmet a l'acadèmia de ciències de Paris el seu article sobre la resolubilitat
- És rebutjat per Cauchy el 1831, que deia que hi faltaven detalls
- Galois estava molt involucrat en la vida política, participant en manifestacions republicanes
- És acusat de sedició, empresonat i expulsat de l'Ecole Normale
- El 1832 va morir en un duel
- Els motius del duel no estan clars del tot...
- Diuen que la nit abans del duel acabà de pulir el seu article
- El seu article és redescobert i publicat per Liouville el 1846

Galois: el personatge



Evariste Galois (1811-1832)

- El 1830 sotmet a l'acadèmia de ciències de Paris el seu article sobre la resolubilitat
- És rebutjat per Cauchy el 1831, que deia que hi faltaven detalls
- Galois estava molt involucrat en la vida política, participant en manifestacions republicanes
- És acusat de sedició, empresonat i expulsat de l'Ecole Normale
- El 1832 va morir en un duel
- Els motius del duel no estan clars del tot...
- Diuen que la nit abans del duel acabà de pulir el seu article
- El seu article és redescobert i publicat per Liouville el 1846

Galois: el personatge



Evariste Galois (1811-1832)

- El 1830 sotmet a l'acadèmia de ciències de Paris el seu article sobre la resolubilitat
- És rebutjat per Cauchy el 1831, que deia que hi faltaven detalls
- Galois estava molt involucrat en la vida política, participant en manifestacions republicanes
- És acusat de sedició, empresonat i expulsat de l'Ecole Normale
- El 1832 va morir en un duel
- Els motius del duel no estan clars del tot...
- Diuen que la nit abans del duel acabà de pulir el seu article
- El seu article és redescobert i publicat per Liouville el 1846

Galois: el personatge



Evariste Galois (1811-1832)

- El 1830 sotmet a l'acadèmia de ciències de Paris el seu article sobre la resolubilitat
- És rebutjat per Cauchy el 1831, que deia que hi faltaven detalls
- Galois estava molt involucrat en la vida política, participant en manifestacions republicanes
- És acusat de sedició, empresonat i expulsat de l'Ecole Normale
- El 1832 va morir en un duel
- Els motius del duel no estan clars del tot...
- Diuen que la nit abans del duel acabà de pulir el seu article
- El seu article és redescobert i publicat per Liouville el 1846

Galois: el personatge



Evariste Galois (1811-1832)

- El 1830 sotmet a l'acadèmia de ciències de Paris el seu article sobre la resolubilitat
- És rebutjat per Cauchy el 1831, que deia que hi faltaven detalls
- Galois estava molt involucrat en la vida política, participant en manifestacions republicanes
- És acusat de sedició, empresonat i expulsat de l'Ecole Normale
- El 1832 va morir en un duel
- Els motius del duel no estan clars del tot...
- Diuen que la nit abans del duel acabà de pulir el seu article
- El seu article és redescobert i publicat per Liouville el 1846

Galois: el personatge



Evariste Galois (1811-1832)

- El 1830 sotmet a l'acadèmia de ciències de Paris el seu article sobre la resolubilitat
- És rebutjat per Cauchy el 1831, que deia que hi faltaven detalls
- Galois estava molt involucrat en la vida política, participant en manifestacions republicanes
- És acusat de sedició, empresonat i expulsat de l'Ecole Normale
- El 1832 va morir en un duel
- Els motius del duel no estan clars del tot...
- Diuen que la nit abans del duel acabà de pulir el seu article
- El seu article és redescobert i publicat per Liouville el 1846

Galois: el personatge



Evariste Galois (1811-1832)

- El 1830 sotmet a l'acadèmia de ciències de Paris el seu article sobre la resolubilitat
- És rebutjat per Cauchy el 1831, que deia que hi faltaven detalls
- Galois estava molt involucrat en la vida política, participant en manifestacions republicanes
- És acusat de sedició, empresonat i expulsat de l'Ecole Normale
- El 1832 va morir en un duel
- Els motius del duel no estan clars del tot...
- Diuen que la nit abans del duel acabà de pulir el seu article
- El seu article és redescobert i publicat per Liouville el 1846

Galois: el personatge



Evariste Galois (1811-1832)

- El 1830 sotmet a l'acadèmia de ciències de Paris el seu article sobre la resolubilitat
- És rebutjat per Cauchy el 1831, que deia que hi faltaven detalls
- Galois estava molt involucrat en la vida política, participant en manifestacions republicanes
- És acusat de sedició, empresonat i expulsat de l'Ecole Normale
- El 1832 va morir en un duel
- Els motius del duel no estan clars del tot...
- Diuen que la nit abans del duel acabà de pulir el seu article
- El seu article és redescobert i publicat per Liouville el 1846

Galois: el personatge



Evariste Galois (1811-1832)

- El 1830 sotmet a l'acadèmia de ciències de Paris el seu article sobre la resolubilitat
- És rebutjat per Cauchy el 1831, que deia que hi faltaven detalls
- Galois estava molt involucrat en la vida política, participant en manifestacions republicanes
- És acusat de sedició, empresonat i expulsat de l'Ecole Normale
- El 1832 va morir en un duel
- Els motius del duel no estan clars del tot...
- Diuen que la nit abans del duel acabà de pulir el seu article
- El seu article és redescobert i publicat per Liouville el 1846