# A short presentation of the course *Algebraic number theory and Galois theory*

Sara Checcoli
(Institut Fourier, Grenoble)

M2R-Maths-Fonda 2017-2018
'Number theory and Geometry'
UGA

# Topics

- Part I: Galois theory;

# Topics

- Part I: Galois theory;
- Part II: Introduction to $p$-adic fields.

# Part I: Galois theory - Introduction

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial.

# Part I: Galois theory - Introduction

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial.

**Question:** Are there "simple" general formulae to express the roots of $f(x)$?

# Part I: Galois theory - Introduction

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial.

**Question:** Are there "simple" general formulae to express the roots of $f(x)$?

- $\deg f(x) = 2$: **Yes** (formula by Brahmagupta, 628 ca.)

# Part I: Galois theory - Introduction

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial.

**Question:** Are there "simple" general formulae to express the roots of $f(x)$?

- $\deg f(x) = 2$: **Yes** (formula by Brahmagupta, 628 ca.)
  $f(x) = ax^2 + bx + c$

# Part I: Galois theory - Introduction

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial.

**Question:** Are there "simple" general formulae to express the roots of $f(x)$?

- $\deg f(x) = 2$: **Yes** (formula by Brahmagupta, 628 ca.)
  $f(x) = ax^2 + bx + c \to x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

# Part I: Galois theory - Introduction

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial.

**Question:** Are there "simple" general formulae to express the roots of $f(x)$?

- $\deg f(x) = 2$: **Yes** (formula by Brahmagupta, 628 ca.)
  $f(x) = ax^2 + bx + c \rightarrow x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
- $\deg f(x) = 3$: **Yes** (formulae by Tartaglia, 1539)

# Part I: Galois theory - Introduction

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial.

**Question:** Are there "simple" general formulae to express the roots of $f(x)$?

- $\deg f(x) = 2$: **Yes** (formula by Brahmagupta, 628 ca.)
  $f(x) = ax^2 + bx + c \to x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
- $\deg f(x) = 3$: **Yes** (formulae by Tartaglia, 1539)
- $\deg f(x) = 4$: **Yes** (formulae by Ferrari and Cardano, 1540)

# Part I: Galois theory - Introduction

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial.

**Question:** Are there "simple" general formulae to express the roots of $f(x)$?

- $\deg f(x) = 2$: **Yes** (formula by Brahmagupta, 628 ca.)
  $f(x) = ax^2 + bx + c \to x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
- $\deg f(x) = 3$: **Yes** (formulae by Tartaglia, 1539)
- $\deg f(x) = 4$: **Yes** (formulae by Ferrari and Cardano, 1540)

All these formulas only uses $+, -, \times, \div, \sqrt[n]{}$

# Part I: Galois theory - Introduction

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial.

**Question:** Are there "simple" general formulae to express the roots of $f(x)$?

- $\deg f(x) = 2$: **Yes** (formula by Brahmagupta, 628 ca.)
  $f(x) = ax^2 + bx + c \rightarrow x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
- $\deg f(x) = 3$: **Yes** (formulae by Tartaglia, 1539)
- $\deg f(x) = 4$: **Yes** (formulae by Ferrari and Cardano, 1540)

All these formulas only uses $+, -, \times, \div, \sqrt[n]{}$

$\rightarrow$ if $\deg f(x) \leq 4$, $f(x) = 0$ can be *solved by radicals*.

# Part I: Galois theory - Introduction

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial.

**Question:** Are there "simple" general formulae to express the roots of $f(x)$?

- $\deg f(x) = 2$: **Yes** (formula by Brahmagupta, 628 ca.)
  $f(x) = ax^2 + bx + c \rightarrow x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
- $\deg f(x) = 3$: **Yes** (formulae by Tartaglia, 1539)
- $\deg f(x) = 4$: **Yes** (formulae by Ferrari and Cardano, 1540)

All these formulas only uses $+, -, \times, \div, \sqrt[n]{}$

$\rightarrow$ if $\deg f(x) \leq 4$, $f(x) = 0$ can be *solved by radicals*.

**Question:** Is this always the case for higher degree polynomials?

# Part I: Galois theory - Introduction

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial.

**Question:** Are there "simple" general formulae to express the roots of $f(x)$?

- $\deg f(x) = 2$: **Yes** (formula by Brahmagupta, 628 ca.)
  $f(x) = ax^2 + bx + c \rightarrow x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
- $\deg f(x) = 3$: **Yes** (formulae by Tartaglia, 1539)
- $\deg f(x) = 4$: **Yes** (formulae by Ferrari and Cardano, 1540)

All these formulas only uses $+, -, \times, \div, \sqrt[n]{}$

$\rightarrow$ if $\deg f(x) \leq 4$, $f(x) = 0$ can be *solved by radicals*.

**Question:** Is this always the case for higher degree polynomials?
**No!**

# Part I: Galois theory - Introduction

**Theorem (Abel-Ruffini)** There is no general formula in radicals for the roots that works for all polynomials of a given degree $\geq 5$.

# Part I: Galois theory - Introduction

**Theorem (Abel-Ruffini)** There is no general formula in radicals for the roots that works for all polynomials of a given degree $\geq 5$.

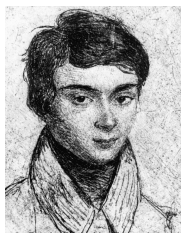
**Questions:** What's behind this phenomenon?

# Part I: Galois theory - Introduction

**Theorem (Abel-Ruffini)** There is no general formula in radicals for the roots that works for all polynomials of a given degree $\geq 5$.

**Questions:** What's behind this phenomenon?

***Evariste Galois***
(Bourg la Reine, 1811 - Paris, 1832)

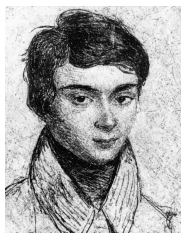


# Part I: Galois theory - Introduction

**Theorem (Abel-Ruffini)** There is no general formula in radicals for the roots that works for all polynomials of a given degree $\geq 5$.

**Questions:** What's behind this phenomenon?

***Evariste Galois***
(Bourg la Reine, 1811 - Paris, 1832)



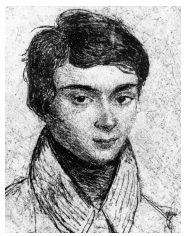
Studied the "symmetries" among the roots & 'invented' group theory

# Part I: Galois theory - Introduction

**Theorem (Abel-Ruffini)** There is no general formula in radicals for the roots that works for all polynomials of a given degree $\geq 5$.

**Questions:** What's behind this phenomenon?

***Evariste Galois***
(Bourg la Reine, 1811 - Paris, 1832)



Studied the "symmetries" among the roots & 'invented' group theory

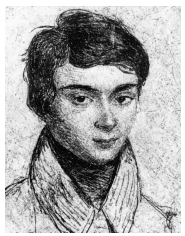
- {permutations of the roots of $f(x)$ fixing the algebraic relations with coefficients in $\mathbb{Q}$ among the roots} is a group, the Galois group of $f(x)$.

# Part I: Galois theory - Introduction

**Theorem (Abel-Ruffini)** There is no general formula in radicals for the roots that works for all polynomials of a given degree $\geq 5$.

**Questions:** What's behind this phenomenon?

***Evariste Galois***
(Bourg la Reine, 1811 - Paris, 1832)



Studied the "symmetries" among the roots & 'invented' group theory

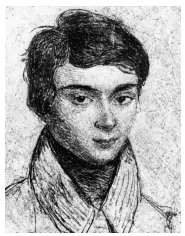
- {permutations of the roots of $f(x)$ fixing the algebraic relations with coefficients in $\mathbb{Q}$ among the roots} is a group, the Galois group of $f(x)$.
- $f(x) = 0$ is solvable by radicals $\Leftrightarrow$ the Galois group of $f(x)$ is solvable.

# Part I: Galois theory - Introduction

**Theorem (Abel-Ruffini)** There is no general formula in radicals for the roots that works for all polynomials of a given degree $\geq 5$.

**Questions:** What's behind this phenomenon?

***Evariste Galois***
(Bourg la Reine, 1811 - Paris, 1832)



Studied the "symmetries" among the roots & 'invented' group theory

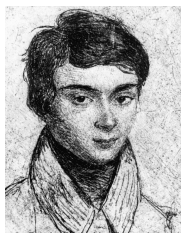
- {permutations of the roots of $f(x)$ fixing the algebraic relations with coefficients in $\mathbb{Q}$ among the roots} is a group, the Galois group of $f(x)$.
- $f(x) = 0$ is solvable by radicals $\Leftrightarrow$ the Galois group of $f(x)$ is solvable.
- The Galois group of a generic polynomial of degree $n$ is $S_n$, not solvable for $n \geq 5$

# Part I: Galois theory - Introduction

**Theorem (Abel-Ruffini)** There is no general formula in radicals for the roots that works for all polynomials of a given degree $\geq 5$.

**Questions:** What's behind this phenomenon?

***Evariste Galois***
(Bourg la Reine, 1811 - Paris, 1832)



Studied the "symmetries" among the roots & 'invented' group theory

- {permutations of the roots of $f(x)$ fixing the algebraic relations with coefficients in $\mathbb{Q}$ among the roots} is a group, the Galois group of $f(x)$.
- $f(x) = 0$ is solvable by radicals $\Leftrightarrow$ the Galois group of $f(x)$ is solvable.
- The Galois group of a generic polynomial of degree $n$ is $S_n$, not solvable for $n \geq 5 \rightarrow$ Abel-Ruffini.

# Part I: Galois theory - Course content

**Highlights:**

- Introduce Galois extensions (over general fields) and their Galois groups

# Part I: Galois theory - Course content

**Highlights:**

- Introduce Galois extensions (over general fields) and their Galois groups
- Prove the fundamental theorem of Galois theory (Galois correspondence)

# Part I: Galois theory - Course content

**Highlights:**

- Introduce Galois extensions (over general fields) and their Galois groups
- Prove the fundamental theorem of Galois theory (Galois correspondence)
- Prove the generalisation of Abel-Ruffini theorem about extensions solvable by radicals

# Part I: Galois theory - Course content

**Highlights:**

- Introduce Galois extensions (over general fields) and their Galois groups
- Prove the fundamental theorem of Galois theory (Galois correspondence)
- Prove the generalisation of Abel-Ruffini theorem about extensions solvable by radicals
- *Inverse Galois problem*: given a finite group $G$, is there an irreducible polynomial in $\mathbb{Q}[x]$ having $G$ as Galois group?

# Part I: Galois theory - Course content

**Highlights:**

- Introduce Galois extensions (over general fields) and their Galois groups
- Prove the fundamental theorem of Galois theory (Galois correspondence)
- Prove the generalisation of Abel-Ruffini theorem about extensions solvable by radicals
- *Inverse Galois problem*: given a finite group $G$, is there an irreducible polynomial in $\mathbb{Q}[x]$ having $G$ as Galois group? Open!

# Part I: Galois theory - Course content

**Highlights:**

- Introduce Galois extensions (over general fields) and their Galois groups
- Prove the fundamental theorem of Galois theory (Galois correspondence)
- Prove the generalisation of Abel-Ruffini theorem about extensions solvable by radicals
- *Inverse Galois problem*: given a finite group $G$, is there an irreducible polynomial in $\mathbb{Q}[x]$ having $G$ as Galois group? Open! $\rightarrow$ Some cases where the answer is yes.

# Part I: Galois theory - Course content

**Highlights:**

- Introduce Galois extensions (over general fields) and their Galois groups
- Prove the fundamental theorem of Galois theory (Galois correspondence)
- Prove the generalisation of Abel-Ruffini theorem about extensions solvable by radicals
- *Inverse Galois problem*: given a finite group $G$, is there an irreducible polynomial in $\mathbb{Q}[x]$ having $G$ as Galois group? Open! $\rightarrow$ Some cases where the answer is yes.
- (If time) Some elements of Galois theory for infinite extensions

# Part II: $p$-adic fields - Introduction

**Distances on $\mathbb{Q}$:**

# Part II: $p$-adic fields - Introduction

**Distances on $\mathbb{Q}$:** Fix a prime number $p$.

# Part II: $p$-adic fields - Introduction

**Distances on $\mathbb{Q}$:** Fix a prime number $p$.

- Usual distance: $x$ and $y$ in $\mathbb{Q}$ are close if $|x-y|$ is small.

# Part II: $p$-adic fields - Introduction

**Distances on $\mathbb{Q}$:** Fix a prime number $p$.

- Usual distance: $x$ and $y$ in $\mathbb{Q}$ are close if $|x-y|$ is small.

- $p$-adic distance: $x$ and $y$ in $\mathbb{Q}$ are close if $x-y$ is *highly* divisible by $p$

# Part II: $p$-adic fields - Introduction

**Distances on $\mathbb{Q}$:** Fix a prime number $p$.

- Usual distance: $x$ and $y$ in $\mathbb{Q}$ are close if $|x-y|$ is small.

- $p$-adic distance: $x$ and $y$ in $\mathbb{Q}$ are close if $x-y$ is *highly* divisible by $p$ (i.e. $x-y=p^v(a/b)$ where $(p,ab)=1$ and $v$ is *big*).

# Part II: $p$-adic fields - Introduction

**Distances on $\mathbb{Q}$:** Fix a prime number $p$.

- Usual distance: $x$ and $y$ in $\mathbb{Q}$ are close if $|x-y|$ is small. Completion of $\mathbb{Q}$ with respect to $|\cdot|$
- $p$-adic distance: $x$ and $y$ in $\mathbb{Q}$ are close if $x-y$ is *highly* divisible by $p$ (i.e. $x-y=p^v(a/b)$ where $(p,ab)=1$ and $v$ is *big*).

# Part II: $p$-adic fields - Introduction

**Distances on $\mathbb{Q}$:** Fix a prime number $p$.

- Usual distance: $x$ and $y$ in $\mathbb{Q}$ are close if $|x-y|$ is small. Completion of $\mathbb{Q}$ with respect to $|\cdot| \rightsquigarrow \mathbb{R}$
- $p$-adic distance: $x$ and $y$ in $\mathbb{Q}$ are close if $x-y$ is *highly* divisible by $p$ (i.e. $x-y = p^v(a/b)$ where $(p, ab) = 1$ and $v$ is *big*).

# Part II: $p$-adic fields - Introduction

**Distances on $\mathbb{Q}$**: Fix a prime number $p$.

- Usual distance: $x$ and $y$ in $\mathbb{Q}$ are close if $|x-y|$ is small.
  Completion of $\mathbb{Q}$ with respect to $|\cdot| \rightsquigarrow \mathbb{R}$
- $p$-adic distance: $x$ and $y$ in $\mathbb{Q}$ are close if $x-y$ is *highly* divisible by $p$ (i.e. $x-y=p^v(a/b)$ where $(p,ab)=1$ and $v$ is *big*).
  Completion of $\mathbb{Q}$ with respect to $|\cdot|_p$

# Part II: $p$-adic fields - Introduction

**Distances on $\mathbb{Q}$**: Fix a prime number $p$.

- Usual distance: $x$ and $y$ in $\mathbb{Q}$ are close if $|x-y|$ is small.
  Completion of $\mathbb{Q}$ with respect to $|\cdot| \rightsquigarrow \mathbb{R}$
- $p$-adic distance: $x$ and $y$ in $\mathbb{Q}$ are close if $x-y$ is *highly* divisible by $p$ (i.e. $x-y=p^v(a/b)$ where $(p,ab)=1$ and $v$ is *big*).
  Completion of $\mathbb{Q}$ with respect to $|\cdot|_p \rightsquigarrow \mathbb{Q}_p$ the field of *$p$-adic numbers*

# Part II: $p$-adic fields - Introduction

**Distances on $\mathbb{Q}$:** Fix a prime number $p$.

- Usual distance: $x$ and $y$ in $\mathbb{Q}$ are close if $|x-y|$ is small.
  Completion of $\mathbb{Q}$ with respect to $|\cdot| \rightsquigarrow \mathbb{R}$
- $p$-adic distance: $x$ and $y$ in $\mathbb{Q}$ are close if $x-y$ is *highly* divisible by $p$ (i.e. $x-y=p^v(a/b)$ where $(p,ab)=1$ and $v$ is *big*).
  Completion of $\mathbb{Q}$ with respect to $|\cdot|_p \rightsquigarrow \mathbb{Q}_p$ the field of *$p$-adic numbers*

**Origins:**

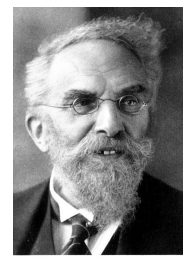
# Part II: $p$-adic fields - Introduction

**Distances on $\mathbb{Q}$:** Fix a prime number $p$.

- Usual distance: $x$ and $y$ in $\mathbb{Q}$ are close if $|x-y|$ is small.
  Completion of $\mathbb{Q}$ with respect to $|\cdot| \rightsquigarrow \mathbb{R}$
- $p$-adic distance: $x$ and $y$ in $\mathbb{Q}$ are close if $x-y$ is *highly* divisible by $p$ (i.e. $x-y = p^v(a/b)$ where $(p, ab) = 1$ and $v$ is *big*).
  Completion of $\mathbb{Q}$ with respect to $|\cdot|_p \rightsquigarrow \mathbb{Q}_p$ the field of *$p$-adic numbers*

**Origins:**

- Hensel (1897): bring the methods of power series into number theory



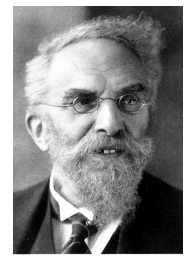
# Part II: $p$-adic fields - Introduction

**Distances on $\mathbb{Q}$:** Fix a prime number $p$.

- Usual distance: $x$ and $y$ in $\mathbb{Q}$ are close if $|x-y|$ is small.
  Completion of $\mathbb{Q}$ with respect to $|\cdot| \rightsquigarrow \mathbb{R}$
- $p$-adic distance: $x$ and $y$ in $\mathbb{Q}$ are close if $x-y$ is *highly* divisible by $p$ (i.e. $x-y = p^v(a/b)$ where $(p, ab) = 1$ and $v$ is *big*).
  Completion of $\mathbb{Q}$ with respect to $|\cdot|_p \rightsquigarrow \mathbb{Q}_p$ the field of *$p$-adic numbers*

**Origins:**

- Hensel (1897): bring the methods of power series into number theory




(mimic the Taylor series expansion of rational functions in $\mathbb{C}(x)$ for rational numbers)

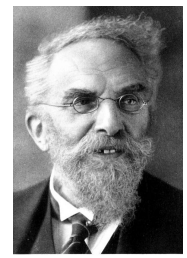
# Part II: $p$-adic fields - Introduction

**Distances on $\mathbb{Q}$:** Fix a prime number $p$.

- Usual distance: $x$ and $y$ in $\mathbb{Q}$ are close if $|x-y|$ is small.
  Completion of $\mathbb{Q}$ with respect to $|\cdot| \rightsquigarrow \mathbb{R}$
- $p$-adic distance: $x$ and $y$ in $\mathbb{Q}$ are close if $x-y$ is *highly* divisible by $p$ (i.e. $x-y=p^v(a/b)$ where $(p,ab)=1$ and $v$ is *big*).
  Completion of $\mathbb{Q}$ with respect to $|\cdot|_p \rightsquigarrow \mathbb{Q}_p$ the field of *$p$-adic numbers*

**Origins:**

- Hensel (1897): bring the methods of power series into number theory




  (mimic the Taylor series expansion of rational functions in $\mathbb{C}(x)$ for rational numbers)
- $\mathbb{Q}_p = \{\sum_{n\geq n_0} a_n p^n \mid 0 \leq a_i \leq p-1, n_0 \in \mathbb{Z}\}$

# Part II: $p$-adic fields - Introduction

**$p$-adic fields:** Finite extensions of $\mathbb{Q}_p$.

# Part II: $p$-adic fields - Introduction

**$p$-adic fields:** Finite extensions of $\mathbb{Q}_p$.

- $K/\mathbb{Q}$ number field

# Part II: $p$-adic fields - Introduction

**$p$-adic fields:** Finite extensions of $\mathbb{Q}_p$.

- $K/\mathbb{Q}$ number field
- $\mathfrak{p}$ prime ideal of $K$ above $p$

# Part II: $p$-adic fields - Introduction

**$p$-adic fields:** Finite extensions of $\mathbb{Q}_p$.

- $K/\mathbb{Q}$ number field
- $\mathfrak{p}$ prime ideal of $K$ above $p$
- $|\cdot|_{\mathfrak{p}}$-adic absolute value

# Part II: $p$-adic fields - Introduction

**$p$-adic fields:** Finite extensions of $\mathbb{Q}_p$.

- $K/\mathbb{Q}$ number field
- $\mathfrak{p}$ prime ideal of $K$ above $p$
- $|\cdot|_{\mathfrak{p}}$-adic absolute value

Completion of $(K, |\cdot|_{\mathfrak{p}})$

# Part II: $p$-adic fields - Introduction

**$p$-adic fields:** Finite extensions of $\mathbb{Q}_p$.

- $K/\mathbb{Q}$ number field
- $\mathfrak{p}$ prime ideal of $K$ above $p$
- $|\cdot|_{\mathfrak{p}}$-adic absolute value

Completion of $(K, |\cdot|_{\mathfrak{p}}) \rightsquigarrow K_{\mathfrak{p}}/\mathbb{Q}_p$ a $p$-adic field.

# Part II: $p$-adic fields - Introduction

**$p$-adic fields:** Finite extensions of $\mathbb{Q}_p$.

- $K/\mathbb{Q}$ number field
- $\mathfrak{p}$ prime ideal of $K$ above $p$
- $|\cdot|_{\mathfrak{p}}$-adic absolute value

Completion of $(K, |\cdot|_{\mathfrak{p}}) \rightsquigarrow K_{\mathfrak{p}}/\mathbb{Q}_p$ a $p$-adic field.

**What are $p$-adic fields good for?**

# Part II: $p$-adic fields - Introduction

**$p$-adic fields:** Finite extensions of $\mathbb{Q}_p$.

- $K/\mathbb{Q}$ number field
- $\mathfrak{p}$ prime ideal of $K$ above $p$
- $|\cdot|_{\mathfrak{p}}$-adic absolute value

Completion of $(K, |\cdot|_{\mathfrak{p}}) \rightsquigarrow K_{\mathfrak{p}}/\mathbb{Q}_p$ a $p$-adic field.

**What are $p$-adic fields good for?** Just few examples

# Part II: $p$-adic fields - Introduction

**$p$-adic fields:** Finite extensions of $\mathbb{Q}_p$.

- $K/\mathbb{Q}$ number field
- $\mathfrak{p}$ prime ideal of $K$ above $p$
- $|\cdot|_{\mathfrak{p}}$-adic absolute value

Completion of $(K, |\cdot|_{\mathfrak{p}}) \rightsquigarrow K_{\mathfrak{p}}/\mathbb{Q}_p$ a $p$-adic field.

**What are $p$-adic fields good for?** Just few examples

- **Hasse local-global principle:** Let $Q(x_1, \ldots, x_n)$ be a quadratic form with coefficients in $\mathbb{Q}$.

# Part II: $p$-adic fields - Introduction

**$p$-adic fields:** Finite extensions of $\mathbb{Q}_p$.

- $K/\mathbb{Q}$ number field
- $\mathfrak{p}$ prime ideal of $K$ above $p$
- $|\cdot|_{\mathfrak{p}}$-adic absolute value

Completion of $(K, |\cdot|_{\mathfrak{p}}) \rightsquigarrow K_{\mathfrak{p}}/\mathbb{Q}_p$ a $p$-adic field.

**What are $p$-adic fields good for?** Just few examples

- **Hasse local-global principle:** Let $Q(x_1, \ldots, x_n)$ be a quadratic form with coefficients in $\mathbb{Q}$. Then $Q(x_1, \ldots, x_n) = 0$ has a non trivial solution in $\mathbb{Q} \Leftrightarrow$ it has a solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all $p$.

# Part II: $p$-adic fields - Introduction

**$p$-adic fields:** Finite extensions of $\mathbb{Q}_p$.

- $K/\mathbb{Q}$ number field
- $\mathfrak{p}$ prime ideal of $K$ above $p$
- $|\cdot|_{\mathfrak{p}}$-adic absolute value

Completion of $(K, |\cdot|_{\mathfrak{p}}) \rightsquigarrow K_{\mathfrak{p}}/\mathbb{Q}_p$ a $p$-adic field.

**What are $p$-adic fields good for?** Just few examples

- **Hasse local-global principle:** Let $Q(x_1, \ldots, x_n)$ be a quadratic form with coefficients in $\mathbb{Q}$. Then $Q(x_1, \ldots, x_n) = 0$ has a non trivial solution in $\mathbb{Q} \Leftrightarrow$ it has a solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all $p$.
  $\rightarrow$ applications to diophantine equations

# Part II: $p$-adic fields - Introduction

**$p$-adic fields:** Finite extensions of $\mathbb{Q}_p$.

- $K/\mathbb{Q}$ number field
- $\mathfrak{p}$ prime ideal of $K$ above $p$
- $|\cdot|_{\mathfrak{p}}$-adic absolute value

Completion of $(K, |\cdot|_{\mathfrak{p}}) \rightsquigarrow K_{\mathfrak{p}}/\mathbb{Q}_p$ a $p$-adic field.

**What are $p$-adic fields good for?** Just few examples

- **Hasse local-global principle:** Let $Q(x_1, \ldots, x_n)$ be a quadratic form with coefficients in $\mathbb{Q}$. Then $Q(x_1, \ldots, x_n) = 0$ has a non trivial solution in $\mathbb{Q} \Leftrightarrow$ it has a solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all $p$.
  $\rightarrow$ applications to diophantine equations
- **Monsky's theorem:** It is not possible to dissect a square into an odd number of triangles of equal area

# Part II: $p$-adic fields - Introduction

**$p$-adic fields:** Finite extensions of $\mathbb{Q}_p$.

- $K/\mathbb{Q}$ number field
- $\mathfrak{p}$ prime ideal of $K$ above $p$
- $|\cdot|_{\mathfrak{p}}$-adic absolute value

Completion of $(K, |\cdot|_{\mathfrak{p}}) \rightsquigarrow K_{\mathfrak{p}}/\mathbb{Q}_p$ a $p$-adic field.

**What are $p$-adic fields good for?** Just few examples

- **Hasse local-global principle:** Let $Q(x_1, \ldots, x_n)$ be a quadratic form with coefficients in $\mathbb{Q}$. Then $Q(x_1, \ldots, x_n) = 0$ has a non trivial solution in $\mathbb{Q} \Leftrightarrow$ it has a solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all $p$.
  $\rightarrow$ applications to diophantine equations
- **Monsky's theorem:** It is not possible to dissect a square into an odd number of triangles of equal area (the proof uses $\mathbb{Q}_2$)

# Part II: $p$-adic fields - Introduction

**$p$-adic fields:** Finite extensions of $\mathbb{Q}_p$.

- $K/\mathbb{Q}$ number field
- $\mathfrak{p}$ prime ideal of $K$ above $p$
- $|\cdot|_{\mathfrak{p}}$-adic absolute value

Completion of $(K, |\cdot|_{\mathfrak{p}}) \rightsquigarrow K_{\mathfrak{p}}/\mathbb{Q}_p$ a $p$-adic field.

**What are $p$-adic fields good for?** Just few examples

- **Hasse local-global principle:** Let $Q(x_1, \ldots, x_n)$ be a quadratic form with coefficients in $\mathbb{Q}$. Then $Q(x_1, \ldots, x_n) = 0$ has a non trivial solution in $\mathbb{Q} \Leftrightarrow$ it has a solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all $p$.
  $\rightarrow$ applications to diophantine equations
- **Monsky's theorem:** It is not possible to dissect a square into an odd number of triangles of equal area (the proof uses $\mathbb{Q}_2$)
- Galois representations

# Part II: $p$-adic fields - Introduction

**$p$-adic fields:** Finite extensions of $\mathbb{Q}_p$.

- $K/\mathbb{Q}$ number field
- $\mathfrak{p}$ prime ideal of $K$ above $p$
- $|\cdot|_{\mathfrak{p}}$-adic absolute value

Completion of $(K, |\cdot|_{\mathfrak{p}}) \rightsquigarrow K_{\mathfrak{p}}/\mathbb{Q}_p$ a $p$-adic field.

**What are $p$-adic fields good for?** Just few examples

- **Hasse local-global principle:** Let $Q(x_1, \ldots, x_n)$ be a quadratic form with coefficients in $\mathbb{Q}$. Then $Q(x_1, \ldots, x_n) = 0$ has a non trivial solution in $\mathbb{Q} \Leftrightarrow$ it has a solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all $p$.
  $\rightarrow$ applications to diophantine equations
- **Monsky's theorem:** It is not possible to dissect a square into an odd number of triangles of equal area (the proof uses $\mathbb{Q}_2$)
- Galois representations
- Berkovich spaces

# Part II: $p$-adic fields - Introduction

**$p$-adic fields:** Finite extensions of $\mathbb{Q}_p$.

- $K/\mathbb{Q}$ number field
- $\mathfrak{p}$ prime ideal of $K$ above $p$
- $|\cdot|_{\mathfrak{p}}$-adic absolute value

Completion of $(K, |\cdot|_{\mathfrak{p}}) \rightsquigarrow K_{\mathfrak{p}}/\mathbb{Q}_p$ a $p$-adic field.

**What are $p$-adic fields good for?** Just few examples

- **Hasse local-global principle:** Let $Q(x_1, \ldots, x_n)$ be a quadratic form with coefficients in $\mathbb{Q}$. Then $Q(x_1, \ldots, x_n) = 0$ has a non trivial solution in $\mathbb{Q} \Leftrightarrow$ it has a solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all $p$.
  $\rightarrow$ applications to diophantine equations
- **Monsky's theorem:** It is not possible to dissect a square into an odd number of triangles of equal area (the proof uses $\mathbb{Q}_2$)
- Galois representations
- Berkovich spaces
- ...

# Part II: $p$-adic fields - Content of the course

**Highlights:**

- Recall of basic results on number fields (ring of integers, splitting of primes in extensions,...) [depending on the audience]

# Part II: $p$-adic fields - Content of the course

**Highlights:**

- Recall of basic results on number fields (ring of integers, splitting of primes in extensions,...) [depending on the audience]
- Definition of $p$-adic fields and their properties

# Part II: $p$-adic fields - Content of the course

**Highlights:**

- Recall of basic results on number fields (ring of integers, splitting of primes in extensions,...) [depending on the audience]
- Definition of $p$-adic fields and their properties (in particular classification of unramified, tamely ramified and wildly ramified extensions)

# Part II: $p$-adic fields - Content of the course

**Highlights:**

- Recall of basic results on number fields (ring of integers, splitting of primes in extensions,...) [depending on the audience]
- Definition of $p$-adic fields and their properties (in particular classification of unramified, tamely ramified and wildly ramified extensions)
- Galois extensions of $p$-adic fields:

# Part II: $p$-adic fields - Content of the course

**Highlights:**

- Recall of basic results on number fields (ring of integers, splitting of primes in extensions,...) [depending on the audience]
- Definition of $p$-adic fields and their properties (in particular classification of unramified, tamely ramified and wildly ramified extensions)
- Galois extensions of $p$-adic fields: study the structure of their Galois group