Representações de Galois p-ádicas

—

Seminário de Álgebra

Da insolubilidade da Quíntica ao Programa de Langlands

Enno Nagel
enno.nagel@math.uni-muenster.de

UFF — Rio de Janeiro, 6 de Junho 2017

1.1 Equações polinomiais

Definição

Um **polinômio** é uma expressão obtida pelas operações + e · sobre uma incógnita X e $\mathbb{Q}$.

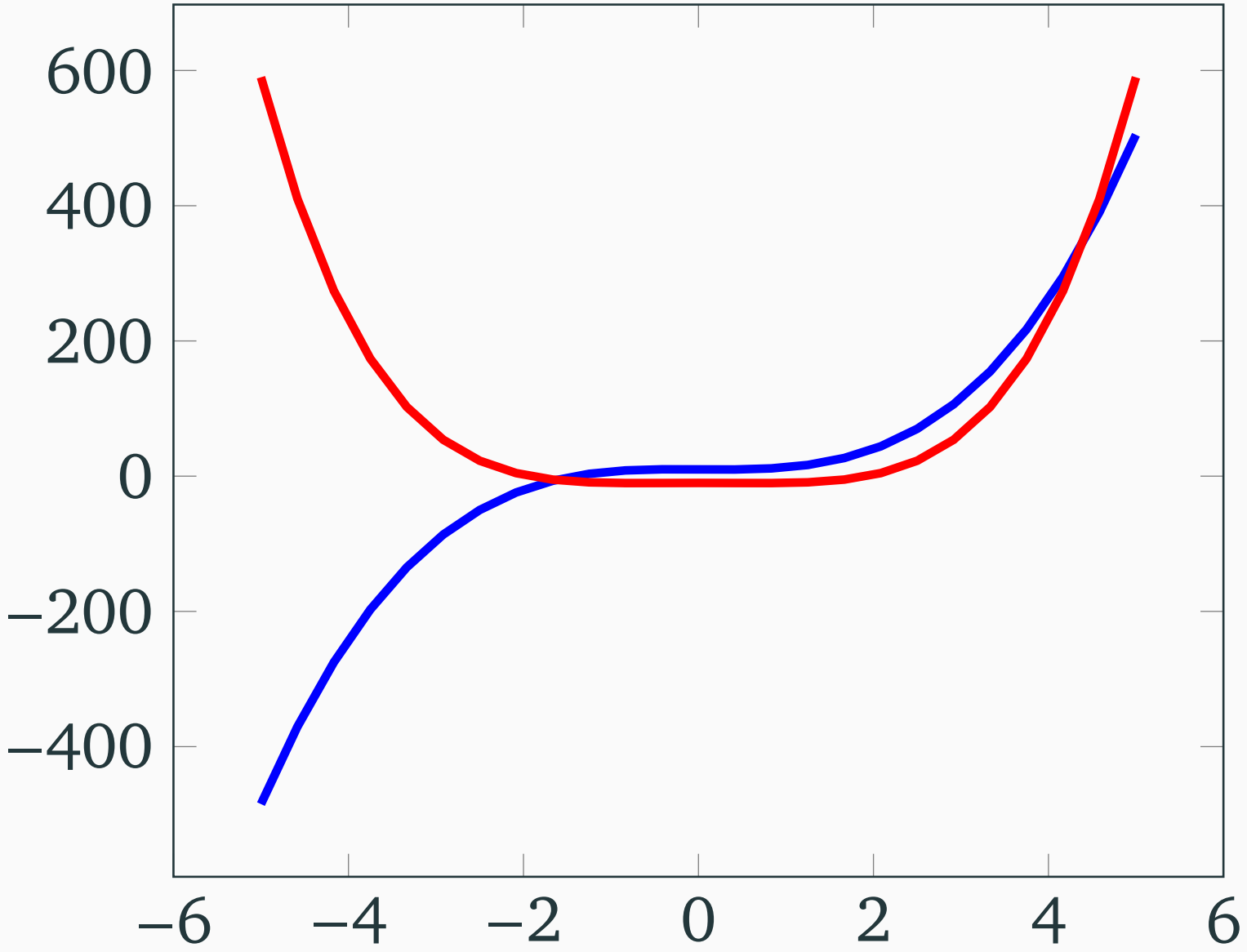
Ele pode ser escrito da forma

$$a_n \mathrm{X}^n + a_{n-1}\mathrm{X}^{n-1} + \cdots + a_0$$

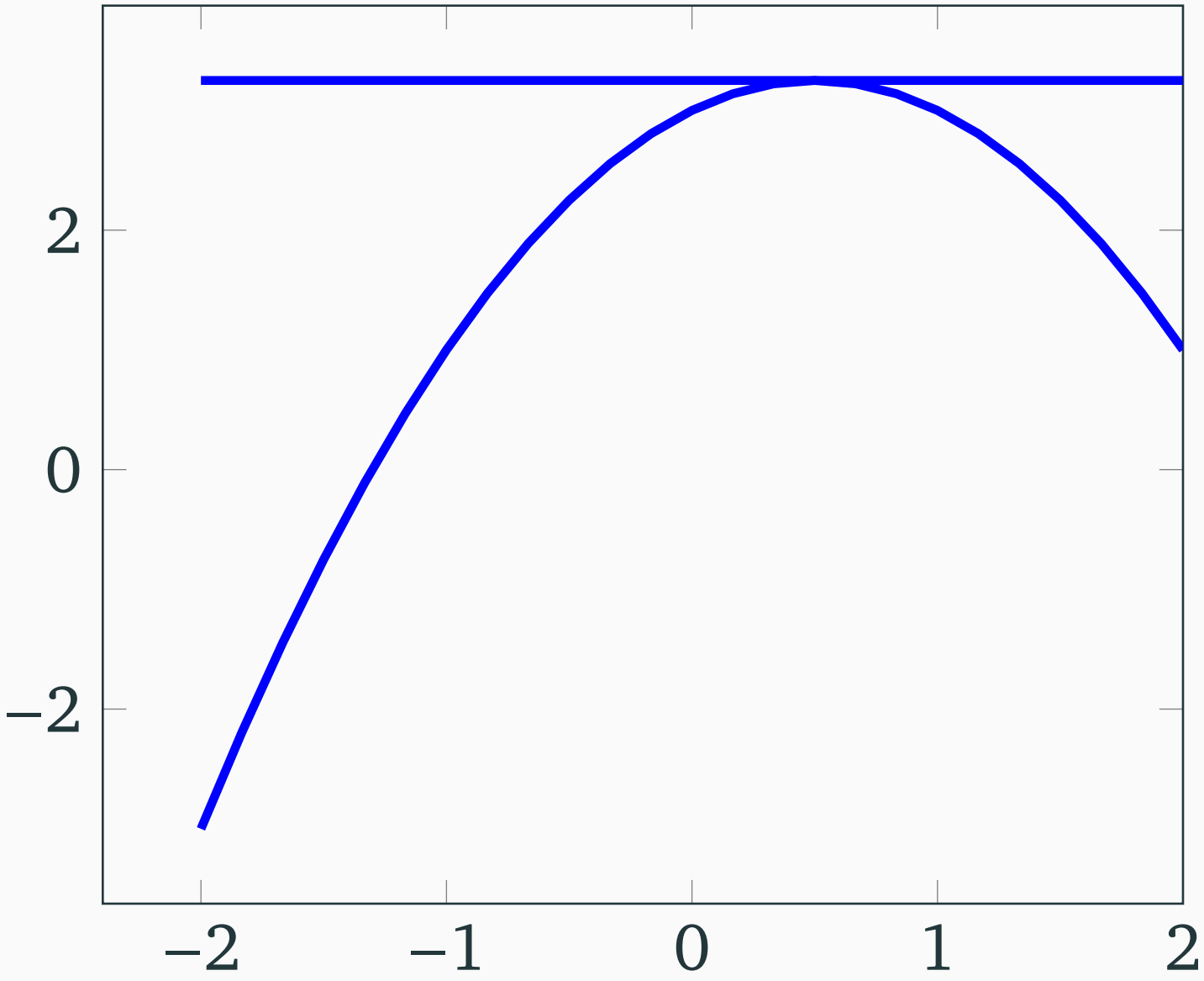
com $a_n, a_{n-1}, \ldots, a_0$ em $\mathbb{Q}$; fornece uma função $f : \mathbb{R} \longrightarrow \mathbb{R}$. Por exemplo, a função polinomial $f(x) = x^2 + x - 1$ tem a curva

Frequentemente, nos interessa o ponto

- em que duas tais curvas se intersectam, ou



- em que uma tal curva atinge seu máximo:



Achar as coordenadas destes pontos reduz-se a resolução de uma equação polinomial

$$f(\mathrm{X}) = \mathrm{X}^n + a_{n-1}\mathrm{X}^{n-1} + \cdots + a_0 = 0.$$

Isto é, queremos calcular as **raízes** de f, os números $r_1, \ldots, r_n$ tais que $f(r_1), \ldots, f(r_n) = 0$.

$\Longrightarrow$ Questão

Há uma fórmula para calcular as raízes de f?

1.2 Soluções em grau menor

Quanto maior o grau n do polinômio, tanto mais engenhosidade requerida para calcular a raiz:

- (Completamento do Quadrado) Se $n = 2$, isto é $x^2 + px + q = 0$, então

$$x^2 + px + q = (x + p/2)^2 - p^2/4 + q$$

e obtemos

$$x = -p/2 \pm \sqrt{p^2/4 - q}. \qquad (*)$$

- (Método de Cardan) Se $n = 3$, isto é $x^3 + ax^2 + bx + c = 0$, então
  1. Substitua x por $\tilde{x} = x + h$ com $h = -a/3$, para obtermos
  $$\tilde{x}^3 + p\tilde{x} + q = x^3 + ax^2 + bx + c.$$
  2. Substitua $\tilde{x}$ por $x' + x''$ tal que $x'x'' = -p/3$, para obter
  $$x'^3 + x''^3 + (x' + x'')(3x'x'' + p) + q = x'^3 + x''^3 + q.$$
  3. Ponha $\mathrm{X}' = x'^3$ e $\mathrm{X}'' = x''^3$, para obtermos
  $$\mathrm{X}' + \mathrm{X}'' = -q \qquad \text{e} \qquad \mathrm{X}'\mathrm{X}'' = -p^3/27.$$

  Como
  $$(\mathrm{X} + \alpha)(\mathrm{X} + \beta) = \mathrm{X}^2 + (\alpha + \beta)\mathrm{X} + \alpha\beta,$$
  $\Longrightarrow$ os valores X' e X'' são as soluções de
  $$\mathrm{X}^2 - q\mathrm{X} - p^3/27 = 0.$$

  A fórmula $(*)$ para $n = 2$ nos dá para $\tilde{x} = \sqrt[3]{\mathrm{X}'} + \sqrt[3]{\mathrm{X}''}$,
  $$\tilde{x} = \sqrt[3]{-q/2 + \sqrt{q^2/4 + p^3/27}} + \sqrt[3]{-q/2 - \sqrt{q^2/4 + p^3/27}}.$$

- Se $n = 4$, isto é $x^4 + \cdots = 0$, então o **Método de Ferrari** mostra como reduzir a uma equação polinomial de grau 3.

$\Longrightarrow$ toda equação polinomial de grau $2, 3, 4$ tem soluções que se exprimem

- pelos seus coeficientes $a_0, a_1, \ldots$ e números racionais,
- sujeitos às operações $+, \cdot$ e $\sqrt[n]{\cdot}$ (para $n = 2, 3, 4$)

Questão

Há uma fórmula dando as raízes para $n = 5$?

1.3 Permutações de Raízes

Para raízes $r_1, \ldots, r_n$, o seu **Corpo de Números** é

$$\begin{aligned}&\mathbb{Q}(r_1, \ldots, r_n)\\ :=&\{ \text{ todos os números obtidos por } + \text{ e } \cdot \text{ sobre } \mathbb{Q} \text{ e } r_1, \ldots, r_n\}\end{aligned}$$

Por exemplo, para $f(\mathrm{X}) = \mathrm{X}^4 - 2$ com raízes $\{\pm\sqrt[4]{2}, \pm\sqrt{-1}\sqrt[4]{2}\}$, estes números têm a forma

$$\begin{aligned}\mathbb{Q}(\sqrt{-1}\sqrt[4]{2}) =&\mathbb{Q} \quad \oplus\mathbb{Q}\sqrt[4]{2} \quad \oplus\mathbb{Q}\sqrt[4]{2}^2 \quad \oplus\mathbb{Q}\sqrt[4]{2}^3\\ &\oplus\mathbb{Q}\sqrt{-1} \quad \oplus\mathbb{Q}\sqrt{-1}\sqrt[4]{2} \quad \oplus\mathbb{Q}\sqrt{-1}\sqrt[4]{2}^2 \quad \oplus\mathbb{Q}\sqrt{-1}\sqrt[4]{2}^3,\end{aligned}$$

um espaço vetorial de dimensão 8 sobre $\mathbb{Q}$.

Extensão Radical

Definição (Corpo Radical)

Um corpo de números $\mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ é **radical** se, para cada $i = 1, \ldots, m$, existe s_i tal que

$$\alpha_i^{s_i} \text{ em } \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1}).$$

Por exemplo

$$r = \sqrt[2]{\sqrt[3]{2} + 5 - \sqrt[2]{12}}.$$

é no corpo de números radical

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt[2]{12}, \sqrt[2]{\sqrt[3]{2} + 5 - \sqrt[2]{12}}).$$

Observação (Radical = Formulável)

As raízes de um polinômio

$$\text{são num corpo de números radical}$$
$$\Longleftrightarrow$$
$$\text{são dadas por uma fórmula.}$$

Notamos que,

- o corpo radical pode ser maior que o gerado pelas raízes;
- em particular os geradores podem diferir das raízes.

Questão

Como as raízes revelam a radicalidade?

Grupo de Galois

Recordemo-nos de que um **automorfismo** é uma aplicação

- injetora cujo domínio iguala a sua imagem (= **auto**), e
- que respeita as operações $+$ e $\cdot$ (= **homomorfismo**).

Definição (Grupo de Galois)

Sejam $r_1, \ldots, r_n$ as raízes de um polinômio irredutível em $\mathbb{Q}[X]$. O seu **Grupo de Galois** é

$$\begin{aligned} &\mathrm{Gal}(\mathbb{Q}(r_1, \ldots, r_n)/\mathbb{Q}) \\ :=&\{ \text{ todas as } \textbf{permutações} \text{ das raízes } r_1, \ldots, r_n \text{ que} \\ &\quad \textbf{se estendem a automorfismos sobre } \mathbb{Q}(r_1, \ldots, r_n) \ \} \end{aligned}$$

Por exemplo para $f(X) = X^4 - 2$ e as suas raízes

$$\{\pm\sqrt[4]{2}, \pm\sqrt{-1}\sqrt[4]{2}\},$$

toda permutação σ que respeita $+$ e $\cdot$ satisfaz

- $\sigma(-\cdot) = -\sigma(\cdot)$,
- $\sigma(\sqrt{-1}) = \pm\sqrt{-1}$,

$\Longrightarrow$ há 8 permutações no Grupo de Galois dadas

- por $\dagger$ em $\{\pm 1, \pm\sqrt{-1}\}$ dado por $\sqrt[4]{2} \mapsto \dagger\sqrt[4]{2}$, e
- por $*$ em $\{\pm 1\}$ dado por $\sqrt{-1}\sqrt[4]{2} \mapsto *\sqrt{-1}\sqrt[4]{2}$,

assim que as permutações são dadas pela tabela

$$\left|\begin{array}{c|c|c|c} \sqrt[4]{2} & -\sqrt[4]{2} & \sqrt{-1}\sqrt[4]{2} & -\sqrt{-1}\sqrt[4]{2} \\ \downarrow & \downarrow & \downarrow & \downarrow \\ \dagger\sqrt[4]{2} & -\dagger\sqrt[4]{2} & *\sqrt{-1}\dagger\sqrt[4]{2} & -*\sqrt{-1}\dagger\sqrt[4]{2} \end{array}\right|$$

O corpo radical básico $\mathbb{Q}(\sqrt[n]{\alpha})$

Examinamos o corpo radical $\mathbb{Q}(\sqrt[n]{\alpha})$ que é incluso no corpo

$$\mathbb{Q}(\sqrt[n]{\alpha}, \zeta_n) \quad \text{onde } \zeta_n \text{ é uma raiz de } 1 \text{ de ordem } n$$

gerado pelas raízes do polinômio $f(\mathrm{X}) = \mathrm{X}^n - \alpha$.

O Grupo de Galois G' de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Q}$ é descrito por

$$\begin{aligned} \mathrm{G}' &\hookrightarrow (\mathbb{Z}/n\mathbb{Z})^* \\ \sigma &\mapsto k \quad \text{determinado por } \sigma(\zeta) = \zeta^k, \text{ e} \end{aligned}$$

o Grupo de Galois G'' de $\mathbb{Q}(\sqrt[n]{\alpha}, \zeta_n)$ sobre $\mathbb{Q}(\zeta_n)$ por

$$\begin{aligned} \mathrm{G}'' &\hookrightarrow \mathbb{Z}/n\mathbb{Z} \\ \sigma &\mapsto k \quad \text{determinado por } \sigma(\alpha) = \zeta^k \alpha. \end{aligned}$$

Os monomorfismos $G' \hookrightarrow \mathbb{Z}/n\mathbb{Z}^*$ e $G'' \hookrightarrow \mathbb{Z}/n\mathbb{Z}$ unem-se a

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{\alpha}, \zeta_n)/\mathbb{Q}) \hookrightarrow \begin{pmatrix} \mathbb{Z}/n\mathbb{Z}^* & \mathbb{Z}/n\mathbb{Z} \\ & 1 \end{pmatrix}$$

Teorema (Galois)

Seja p um número primo e f em $\mathbb{Q}[X]$ de grau p.

Há uma fórmula para os zeros de f

$$\Longleftrightarrow$$

O Grupo de Galois dos zeros de f é incluso em $\begin{pmatrix} \mathbb{F}_p^* & \mathbb{F}_p \\ & 1 \end{pmatrix}$

Para $p = 5$ e $f(X) = X^5 - X + 1$, todas as permutações das raízes $r_1, \ldots, r_5$ respeitam $+$ e $\cdot$. Isto é, o Grupo de Galois é

$$\{ \text{todas as permutações de } \mathbb{F}_5 \},$$

o qual não é um subgrupo de $\begin{pmatrix} \mathbb{F}_5^* & \mathbb{F}_5 \\ & 1 \end{pmatrix}$. Logo, não há fórmula.

Normas sobre $\mathbb{Q}$

Uma **norma** sobre $\mathbb{Q}$ é uma aplicação $|\cdot| : \mathbb{Q} \longrightarrow [0, \infty[$ tal que

- $|x| = 0 \iff x = 0$,
- $|xy| = |x||y|$, e
- $|x + y| \leq |x| + |y|$.

Teorema (Ostrowsi)

Toda norma sobre $\mathbb{Q}$ é equivalente

- *ou à norma usual $|\cdot|$,*
- *ou a uma norma p-ádica $|\cdot|_p$ para um número primo p.*

De uma vez por todas, denote $p = 2, 3, \ldots$ um número primo.

2.1 Norma p-ádica

Definição (Norma p-ádica)

Para x em $\mathbb{Z}$, seja

$$|x|_p := p^{-n} \quad \text{se } x = p^n s \text{ com } p \text{ não dividindo } s$$

e estendido multiplicativamente a $\mathbb{Q}$.

A norma p-ádica $|\cdot|_p$ mede quantas vezes p divide um número inteiro. Contra-intuitivamente, quanto **mais** divide, tanto **menor**.

Nota (sobre a Contra-Intuição)

Uma norma sobre $\mathbb{Q}$ é p-ádica se e tão-somente se ela é **não-Arquimediana**, isto é, $|\underbrace{1 + \cdots + 1}_{n \text{ vezes}}| \leq 1$ para todo n.

Completamento

Em analogia a $\mathbb{R}$ = { todos os limites de $\mathbb{Q}$ quanto à norma $|\cdot|$ },

Definição (Números p-ádicos)

O corpo valorado dos **números p-ádicos** $\mathbb{Q}_p$ é o completamento de $\mathbb{Q}$ pela norma p-ádica $|\cdot|_p$.

Em analogia à expansão decimal de um número real

$$a_{-\mathrm{N}}10^{\mathrm{N}} + \cdots + a_0 + a_1 10^{-1} + a_2 10^{-2} + \cdots ,$$

Proposição (**Expansão p-ádica**)

Cada número p-ádico escreve-se de maneira única

$$\sum_{i \geq -\mathrm{N}} a_i p^i = a_{-\mathrm{N}} p^{-\mathrm{N}} + \cdots + a_0 + a_1 p^1 + a_2 p^2 + \cdots$$

para $a_{-\mathrm{N}}, \ldots, a_0, a_1, \ldots$ *em* $\{0, \ldots, p-1\}$.

2.2 Grupo de Galois p-ádico

Seja $\bar{\cdot}$ = fecho algébrico de $\cdot$. Enquanto o Grupo de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ é infinito,

$$\mathrm{Gal}(\bar{\mathbb{R}}/\mathbb{R}) = \mathrm{Gal}(/\mathbb{R}) = \{\bar{\cdot}, \mathrm{id}\}$$

é dado pela conjugação complexa $\bar{\cdot}$ e a identidade id só;
$\implies$ Completando $\mathbb{Q}$ a $\mathbb{R}$ simplifica o Grupo de Galois.

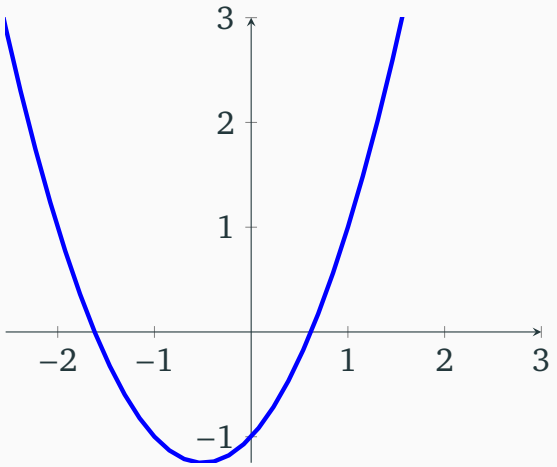
Semelhantemente,

$$\mathbb{Q} \subseteq \mathbb{Q}_p \text{ é denso }, \implies \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q});$$

Completando $\mathbb{Q}$ a $\mathbb{Q}_p$ simplifica o Grupo de Galois.

Quer dizer, mais fácil encontrar raízes de polinômios sobre $\mathbb{R}$ ou $\mathbb{Q}_p$ do que sobre $\mathbb{Q}$. Como teremos ferramentas analíticas:

- Por exemplo, para o polinômio $f(\mathrm{X}) = \mathrm{X}^2 + \mathrm{X} - 1$ com a curva



  ter uma solução, basta pelo Teorema de Valor Intermediário achar pontos x' e x'' tais que $f(x') < 0$ e $f(x'') > 0$.

- O **Método de Newton** funciona tão bem sobre $\mathbb{R}$ quanto sobre $\mathbb{Q}_p$ e ali porta o nome **Lema de Hensel**.

2.3 Princípio Local-Global

Definição (Equação Diofantina)

Uma **equação diofantina** é uma equação

$$\mathrm{P}(\mathrm{X}_1, \ldots, \mathrm{X}_d) = 0$$

para um polinômio P sobre $\mathbb{Z}$.

Em vez de procurarmos soluções em $\mathbb{Z} \times \cdots \times \mathbb{Z}$, procuramo-las primeiro módulo p, p^2, ... para todos os números primos p.

Proposição (Solução módulo $p, p^2, \ldots$ = Solução p-ádica)

As congruências $\mathrm{P}(x) \equiv 0$ *são resolúveis* $\mod p, p^2, \ldots$

$$\Longleftrightarrow$$

A equação $\mathrm{P}(x) = 0$ *é resolúvel em* $\mathbb{Z}_p$ *(= completam. de* $\mathbb{Z}$ *por* $|\cdot|_p$*)*

Redução de $\mathbb{Q}$ aos seus Completamentos

Um polinômio P é **quadrático** se ele se escreve da forma

$$\mathrm{P}(\mathrm{X}_1, \ldots, \mathrm{X}_n) = \sum_{i,j=1,\ldots,n} a_{i,j} \mathrm{X}_i \mathrm{X}_j$$

Teorema (Hasse-Minkowski)

*Seja $\mathrm{P}(x) = 0$ uma equação diofantina. Se P é **quadrática**, então*

$$\mathrm{P}(x) = 0 \text{ é (não-trivialmente) resolúvel sobre } \mathbb{Z}$$

$$\Longleftrightarrow$$

$$\mathrm{P}(x) = 0 \text{ é resolúvel sobre } \mathbb{R} \text{ e sobre todos os } \mathbb{Q}_p \text{ para } p \text{ primo}$$

Este princípio, a redução de uma questão aritmética sobre $\mathbb{Q}$ (ou $\mathbb{Z}$) a uma sobre $\mathbb{R}$ e $\mathbb{Q}_p$, chama-se o **princípio local-global**:

$$\text{local} = \mathbb{R} \text{ ou } \mathbb{Q}_p \quad \text{e} \quad \text{global} = \mathbb{Q}$$

Corolário (do Teorema de Chevalley-Warning)

Seja $\mathrm{P}(x) = 0$ *uma equação diofantina. Se* P *é quadrática e tem* $n \geq 5$ *variáveis, então*

$$\mathrm{P}(x) = 0 \textit{ é (não-trivialmente) resolúvel sobre } \mathbb{Z}$$
$$\Longleftrightarrow$$
$$\mathrm{P}(x) = 0 \textit{ é resolúvel sobre } \mathbb{R}$$

Demonstração.

Demonstra-se que todo polinômio quadrático de $n \geq 5$ variáveis tem um zero sobre todo $\mathbb{Q}_p$ para p primo pelo Teorema de Chevalley-Warning sobre a existência de raizes de um polinómio cujo grau é maior do que a característica p do corpo. □

1 Grupo de Galois

2 Números p-ádicos

3 Programa de Langlands

- Teoria do Corpo de Classes p-ádico
- Programa de Langlands p-ádico
- Cálculo da Redução $\mod p$

Teorema (Galois)

Seja p primo, f em $\mathbb{Q}[X]$ irred. de grau p e G o Grupo de Galois.

$$\textit{Há uma fórmula para os zeros de } f$$
$$\Longleftrightarrow$$
$$\textit{Há um monomorfismo entre grupos } G \hookrightarrow \begin{pmatrix} \mathbb{F}_p^* & \mathbb{F}_p \\ & 1 \end{pmatrix}$$

Uma **representação** é um homomorfismo

$$G \to \begin{pmatrix} * & \cdots & * \\ \vdots & \ddots & \vdots \\ * & \cdots & * \end{pmatrix}$$

entre um grupo G e um grupo de matrizes sobre um corpo ou, equivalentemente, uma ação

$$G \curvearrowright V$$

de G sobre um espaço vetorial V (de dimensão finita ou infinita).

3.1 Teoria do Corpo de Classes p-ádico

A **Teoria do Corpo de Classes** classifica as representações de dimensão 1 de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Todas elas fatoram através do seu quociente abeliano máximo. Vamos descrevê-lo:

Teorema (Kronecker-Weber)

*A extensão **abeliana máxima** de $\mathbb{Q}_p$ (= a maior extensão em $\overline{\mathbb{Q}}_p$ cujo Grupo de Galois é abeliano) é $\mathbb{Q}_p(\mu)$ com*

$$\mu = \bigcup_{n\in\mathbb{N}} \mu_n \quad e \quad \mu_n = \{ \textit{todos os } \zeta \textit{ em } \overline{\mathbb{Q}}_p \textit{ tal que } \zeta^n = 1\}$$

as raízes da unidade. Equivalentemente, com $\cdot^{\mathrm{ab}}$ o maior quociente abeliano,

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)^{\mathrm{ab}} = \mathrm{Gal}(\mathbb{Q}_p(\mu)/\mathbb{Q}_p)$$

Com

$$\mu_{p^\infty} = \bigcup_{n\in\mathbb{N}} \mu_{p^n} \quad \text{e} \quad \mu_{\nmid p} = \bigcup_{n\in\mathbb{N}} \mu_{p^n-1},$$

vale

$$\mathbb{Q}_p(\mu) = \mathbb{Q}_p(\mu_{p^\infty}) \otimes \mathbb{Q}_p(\mu_{\nmid p}).$$

Tem-se

$$\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p) \xrightarrow{\sim} \mathbb{Z}/p^n\mathbb{Z}^*$$
$$\sigma \mapsto k \quad \text{com } \sigma(\zeta) = \zeta^k \text{ para } \zeta \text{ gerador de } \mu_{p^n}$$

e

$$\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n-1})/\mathbb{Q}_p) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$$
$$\sigma \mapsto k \quad \text{com } \sigma = \phi^k \text{ para } \phi = \cdot^p \text{ Frobenius}$$

$$\Longrightarrow$$

$$\mathrm{Gal}(\mathbb{Q}_p(\mu)/\mathbb{Q}_p) \xrightarrow{\sim} \mathbb{Z}_p^* \times \widehat{\mathbb{Z}} = \widehat{\mathbb{Q}}_p^*$$

Definimos o **Grupo de Weil** $\mathrm{Weil}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ pela imagem inversa

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)^{\mathsf{ab}} & \xrightarrow{\sim} & \mathbb{Z}_p^* \times \widehat{\mathbb{Z}} = \widehat{\mathbb{Q}}_p^* \\ \bigcup & & \bigcup \\ \mathrm{Weil}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)^{\mathsf{ab}} & \xrightarrow{\sim} & \mathbb{Z}_p^* \times \mathbb{Z} = \mathbb{Q}_p^* \end{array}$$

Corolário (Langlands para $\dim \mathrm{V} = 1$)

Dado um corpo topológico e V *um espaço vetorial de dimensão* 1*, há um espaço vetorial* B *tal que "naturalmente"*

$$\left\{ \begin{array}{c} \textit{representações contínuas} \\ \mathrm{Weil}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \curvearrowright \mathrm{V} \end{array} \right\} \overset{\sim}{\longleftrightarrow} \left\{ \begin{array}{c} \textit{representações contínuas} \\ \mathrm{GL}_1(\mathbb{Q}_p) \curvearrowright \mathrm{B} \end{array} \right\}$$

3.2 Programa de Langlands p-ádico

Para $\dim \mathrm{V} > 1$, a formulação da correspondência depende da topologia do corpo $\mathbf{K}$ sobre o qual V é definido:

Correspondências de Langlands Locais

- Se $\mathbf{K} =$ ou $\mathbf{K} = \overline{\mathbb{Q}}_l$ para $l \neq p$ (= o caso **clássico**),
  $\Longrightarrow$ (pela incompatibilidade das topologias entre $\mathbf{K}$ e $\mathbb{Q}_p$)
  a correspondência reduz-se a topologia discreta à direita;
- Se $\mathbf{K}$ é uma extensão completa de $\mathbb{Q}_p$ (= o caso **p-ádico**),
  $\Longrightarrow$ a direita não permite esta redução e é mais ampla.

Correspondência de Langlands Clássica ($\dim \mathrm{V} = n > 1$)

Há uma bijeção “natural” entre

$$\left\{ \begin{array}{c} \text{rep's contínuas semi-simples} \\ \mathrm{WD}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \curvearrowright \mathrm{V} \\ \text{de dimensão } n \text{ sobre} \end{array} \right\} \overset{\sim}{\leftrightarrow} \left\{ \begin{array}{c} \text{rep's lisas irredutíveis} \\ \mathrm{GL}_n(\mathbb{Q}_p) \curvearrowright \mathrm{B} \\ \text{(em geral dim. } \infty\text{) sob.} \end{array} \right\}$$

onde

- o grupo $\mathrm{WD}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) = \mathrm{Weil}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \rtimes \mathrm{N}^{\mathbb{Z}}$ é o produto semi-direto com um operador nilpotente N sobre V, e
- uma representação é **lisa** se o grupo de isotropia de cada vetor é aberto.

Funtor de Langlands p-ádico ($\dim \mathrm{V} = n > 1$)

Seja $\mathbf{K}$ um corpo p-ádico. Há um funtor entre

$$\left\{ \begin{array}{c} \text{rep's cont's unitárias (a. de c.f.)} \\ \mathrm{GL}_n(\mathbb{Q}_p) \curvearrowright \mathrm{B} \text{ sobre um} \\ \text{espaço de Banach sobre } \mathbf{K} \end{array} \right\} \to \left\{ \begin{array}{c} \text{rep's cont's} \\ \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \curvearrowright \mathrm{V} \\ \text{de dim. } n \text{ sobre } \mathbf{K} \end{array} \right\}$$

onde

- uma representação sobre um espaço normado é **unitária** se a norma é invariante sob a ação do grupo,
- **a.** abrevia admissível (= o espaço dos vetores fixados sob um subgrupo aberto é de dimensão finita) e **c.f.** abrevia comprimento finito,

Para $n = 2$, demonstrou-se que este funtor realiza correspondências em subclasses de representações entre $\mathrm{GL}_2(\mathbb{Q}_p)$ e $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Exibamos uma tal subclasse:

$$\left\{ \begin{array}{c} \text{rep's contínuas} \\ \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \curvearrowright \mathrm{V} \end{array} \right\} \supset \left\{ \begin{array}{c} \textbf{rep's cristalinas} \\ \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \curvearrowright \mathrm{V} \end{array} \right\} = \left\{ \begin{array}{c} \boldsymbol{\phi}\textbf{-módulos} \\ \textbf{filtrados} \end{array} \right\}$$

Os ϕ-módulos filtrados em $\dim \mathrm{V} = 2$ parametrizam-se por :

- um **talude** $\mu > 0$ em $\mathbb{Q}$, e
- um **peso** $k \geq 2$ em $\mathbb{Z}$.

Observação (pela Compacidade de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$)

Rep. $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \curvearrowright \mathrm{V}$ sobre um espaço vetorial sobre $\mathbb{Q}_p$
$\rightsquigarrow$ Rep. $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \curvearrowright \overline{\mathrm{V}}$ sobre um espaço vetorial sobre $\overline{\mathbb{F}}_p$

Rep's $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \curvearrowright \overline{\mathrm{V}}$ em $\dim \overline{\mathrm{V}} = 2$ parametrizam-se por:

- um par a, b em $\mathbb{Z}$, e
- um par λ, η em $\overline{\mathbb{F}}_p^*$.

3.3 Cálculo da Redução $\mathrm{mod}\ p$

Questão (Computação da Redução $\mathrm{mod}\ p$)

Dada uma ação cristalina de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ *sobre* $\overline{\mathbb{Q}}_p$ *por*

- *um talude* $\mu > 0$ *em* $\mathbb{Q}$*, e um peso* $k \geq 2$ *em* $\mathbb{Z}$*,*

calcule

- *os pares* a, b *em* $\mathbb{Z}$ *e* λ, μ *em* $\overline{\mathbb{F}}_p^*$*,*

que parametrizam a ação $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ *sobre* $\overline{\mathbb{F}}_p$*.*

O caso

- de talude μ em $]0, 1[$ foi tratado em [BG09],
- de talude $\mu = 1$ foi tratado em [BGR16],
- de talude μ em $]1, 2[$ foi tratado em [BG15],
- de talude μ em $]2, 3[$ está sendo tratado por Aftab Pande (UFRJ) e os seus colaboradores (UFAL).

Estratégia

A redução de $\mathbb{Q}_p$ a $\overline{\mathbb{F}}_p$ aplica-se

- tanto às ações de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$,
- quanto às de $\mathrm{GL}_2(\mathbb{Q}_p)$.

Estas reduções $\mathrm{V} \mapsto \overline{\mathrm{V}}$ e $\mathrm{B} \mapsto \overline{\mathrm{B}}$ respeitam a Correspondência de Langlands p-ádica. Quer dizer, o seguinte diagrama comuta:

$$\begin{array}{ccc}
\left\{\begin{array}{c}\text{representações contínuas}\\ \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \curvearrowright \mathrm{V}\\ \text{sobre esp. vet. de dim. 2 / } \mathbb{Q}_p\end{array}\right\} & \to & \left\{\begin{array}{c}\text{rep's contínuas unitárias}\\ \mathrm{GL}_2(\mathbb{Q}_p) \curvearrowright \mathrm{B}\\ \text{sobre esp. de Banach / } \mathbb{Q}_p\end{array}\right\} \\
\downarrow & & \downarrow \\
\left\{\begin{array}{c}\text{representações contínuas}\\ \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \curvearrowright \overline{\mathrm{V}}\\ \text{sobre esp. vet. de dim. 2 / } \overline{\mathbb{F}}_p\end{array}\right\} & \hookrightarrow & \left\{\begin{array}{c}\text{representações lisas}\\ \mathrm{GL}_2(\mathbb{Q}_p) \curvearrowright \overline{\mathrm{B}}\\ \text{sobre (vastos) esp. vet. / } \overline{\mathbb{F}}_p\end{array}\right\}
\end{array}$$

Como

- a flecha acima é conhecida, e
- a flecha abaixo é injetora,

$\Longrightarrow$

Cálculo da ação de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ sobre $\overline{\mathrm{V}}$, dado a ação sobre V

$\|$

Cálculo da ação de $\mathrm{GL}_2(\mathbb{Q}_p)$ sobre $\overline{\mathrm{B}}$, dado a ação sobre B

Cálculo da Representação $\overline{\mathrm{B}}$ sobre $\overline{\mathbb{F}}_{\mathrm{P}}$

Seja o talude μ em $]2, 3[$ e fixamos o peso $k > 2$ em $\mathbb{Z}$. Seja

$$\mathrm{V} := \bigoplus_{i+j=k} \overline{\mathbb{F}}_p \mathrm{X}^i \mathrm{Y}^j$$

o espaço vetorial dos polinômios homogéneos em duas variáveis de grau k; sobre o qual $\mathrm{GL}_2(\mathbb{F}_p)$ age por

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \mathrm{X} \mapsto a\mathrm{X} + c\mathrm{Y} \quad \text{e} \quad \mathrm{Y} \mapsto b\mathrm{X} + d\mathrm{Y}$$

Seja $\mathrm{G} = \mathrm{GL}_2(\mathbb{Q}_p)$. Sejam $\mathrm{K} = \mathrm{GL}_2(\mathbb{Z}_p)$ o subgrupo (afora conjugação) compacto máximo e $\mathrm{Z} = \mathbb{Q}_p^*$ o centro de G.
A ação de G sobre V estende-se trivialmente a uma ação de KZ.

Definição

A representação **induzida** da representação V de KZ a G é

$$\mathrm{ind}_{\mathrm{KZ}}^{\mathrm{G}} \mathrm{V} := \mathrm{V} \otimes_{\overline{\mathbb{F}}_p[\mathrm{KZ}]} \overline{\mathbb{F}}_p[\mathrm{G}].$$

Descrição Explicita da Representação Induzida

A G-representação induzida descreve-se explicitamente como

$$\mathrm{ind}_{\mathrm{KZ}}^{\mathrm{G}} \mathrm{V} = \{f : \mathrm{G} \to \mathrm{V} : f(kz \cdot g) = kz \cdot f(g) \text{ para } kz \in \mathrm{KZ}\}$$

e G age pela translação à direita $f^g := f(\cdot g)$.

Definimos sub-representações de V por

$$\mathrm{V}^{***} := \{ \text{ os polinômios em } \mathrm{V} \text{ divisíveis por } \Theta^3 \},$$

onde $\Theta = \mathrm{X}^p\mathrm{Y} - \mathrm{X}\mathrm{Y}^p$, e

$$\mathrm{V}_{***} := \{ \text{ os polinômios em } \mathrm{V} \text{ gerados por } \mathrm{X}^2\mathrm{Y}^{k-2} \ \}.$$

e ponha

$$\mathrm{Q} := \mathrm{V}/(\mathrm{V}^{***} + \mathrm{V}_{***}).$$

Temos um epimorfismo entre $\overline{\mathbb{F}}_p[\mathrm{G}]$-módulos

$$\mathrm{ind}_{\mathrm{KZ}}^{\mathrm{G}} \mathrm{Q} \twoheadrightarrow \overline{\mathrm{B}}.$$

$\Longrightarrow$ Calcule

1. todos os fatores da Série de Decomposição de Q, e
2. os da Série de Decomposição de Q que sobrevivem em $\overline{\mathrm{B}}$.

Estes cálculos dependem de condições combinatórias dadas

- pela classe de congruência de r módulo $p-1 = \#\mathbb{F}_p^*$, e
- pela classe de congruência de r módulo $p = \#\mathbb{F}_p$

Por [BG09, Lema 3.4]:

- Se Q tiver só um fator J, então Q já descreve $\overline{\mathrm{B}}$ inteiramente.
- Se Q tiver mais de um fator, então mostre que em $\overline{\mathrm{B}}$ resta um único fator J e conclua a descrição de $\overline{\mathrm{B}}$.

Os últimos cálculos usam a descrição explicita do epimorfismo que é dado pela imagem de um **Operador de Hecke** (cf. [BG09]).

1. Grupo de Galois
2. Números p-ádicos
3. Programa de Langlands

As notas estão disponíveis em

`konfekt.bitbucket.io/talks/galois`.

- K. Buzzard and T. Gee, **Explicit reduction modulo p of certain two-dimensional crystalline representations**, Int. Math. Res. Not. IMRN (2009), no. 12, 2303–2317. MR 2511912. DOI 10.1093/imrn/rnp017.
- S. Bhattacharya and E. Ghate, **Reductions of Galois representations for slopes in** $(1, 2)$, Doc. Math. **20** (2015), 943–987. MR 3404215.
- S. Bhattacharya, E. Ghate, and S. Rozensztajn, **Reductions of Galois representations of slopes** 1, preprint (2016).