Representações p-ádicas

—

Seminário de Pesquisa

Da insolubilidade da Quíntica ao Programa de Langlands p-ádico

Enno Nagel
enno.nagel@uni-muenster.de

31 de Maio 2019

1 Existência de Raízes

- Resolubilidade de Polinómios Inteiros
- Norma p-ádica
- Princípio Local-Global

2 Descrição de Raízes

3 Programa de Langlands

4 Estender Langlands

5 Aplicar Langlands

Definição

Um *polinômio* é uma expressão obtida pelas operações + e · sobre um número finito de incógnitas $\mathrm{X}_1, \ldots, \mathrm{X}_d$ e $\mathbb{Q}$.

Em uma variável 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

1.1 Resolubilidade de Polinómios Inteiros

Fixa P em $\mathbb{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_d]$ um polinómio com coeficientes inteiros de múltiplas incógnitas.

Questão (difícil sobre a Existência de Raízes Inteiras)

Existe x em $\mathbb{Z}^d$ com $\mathrm{P}(x) = 0$?

Exemplo

Seja $\mathrm{X}^n + \mathrm{Y}^n = \mathrm{Z}^n$.

- Se $n = 2$, então $(3, 4, 5)$ é uma solução inteira positiva.
- Se $n > 2$, então não existe solução cujas entradas são inteiros positivos (por [Wiles e Taylor-Wiles, 95]).

Questão (fácil sobre a existência de Raízes módulares)

$$\forall m \in \mathbb{N} \text{ existe } x \in \mathbb{Z}^d \text{ com } \mathrm{P}(x) \equiv 0 \bmod m$$

$$\overset{\text{Chinês}}{\iff} \forall p \text{ primo } \forall n \in \mathbb{N} \text{ existe } x \in \mathbb{Z}^d \text{ com } \mathrm{P}(x) \equiv 0 \bmod p^n$$

$$\iff \forall p \text{ primo existe } x \in \mathbb{Z}_p^d \text{ com } \mathrm{P}(x) = 0.$$

De uma vez por todas, denote $p = 2, 3, \ldots$ um número primo. Seja $x \in \mathbb{Z}^d$ tal que $\mathrm{P}(x) = 0$.

- Como p^n divide 0 para todo n, se $\mathrm{P}(x) = 0$, então $\mathrm{P}(x) \equiv 0 \bmod p^n$ para todo $n \in \mathbb{N}$, e
- como p^n divide p^{n+1}, se $\mathrm{P}(x) \equiv 0 \bmod p^{n+1}$, então $\mathrm{P}(x) \equiv 0 \bmod p^n$ para todo $n \in \mathbb{N}$.

$\implies$ Quanto maior o expoente n da congruência $\mathrm{P}(x) \equiv 0 \bmod p^n$, tanto mais próximo é x de uma solução!

1.2 Norma p-ádica

Quantifiquemos esta proximidade modular pela *norma p-ádica* $|\cdot|_p$: Uma *norma* sobre $\mathbb{Q}$ é uma aplicação $|\cdot| : \mathbb{Q} \longrightarrow [0, \infty[$ com

- $|x| = 0$ se, e tão-somente se $x = 0$,
- $|xy| = |x||y|$, e
- $|x + y| \leq |x| + |y|$.

Teorema (de Ostrowsi [1916)

] 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.*

Definição (Norma p-ádica)

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

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

que qual se estende 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.

Equivalentemente, $|\cdot|$ satisfaz a *desigualdade triangular forte*

$$|a + b| \leq \max\{|a|, |b|\}.$$

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* $\{0, \ldots, p-1\}$.

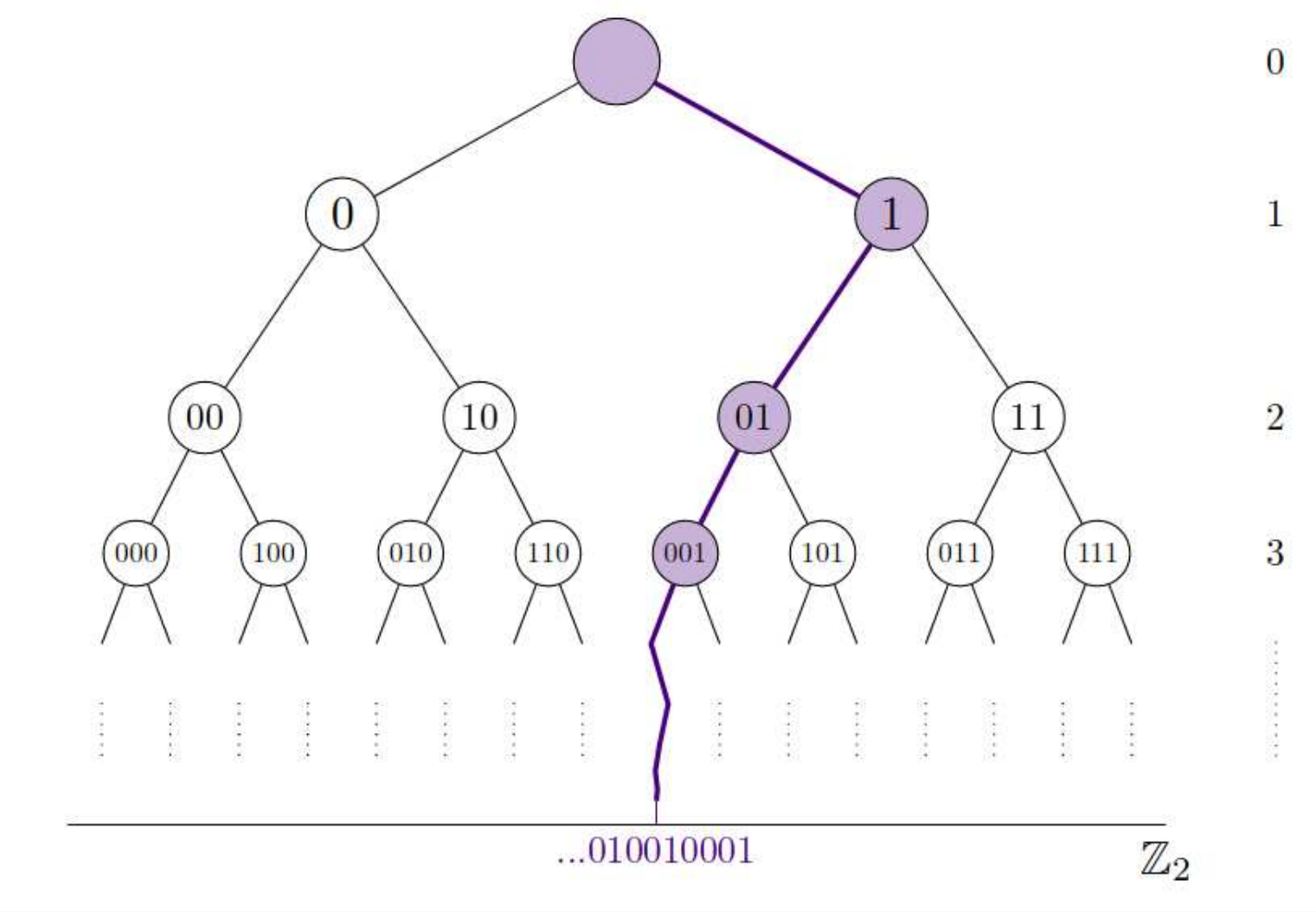


Figura: A bola unitária $\mathbb{Z}_2$ em $\mathbb{Q}_2$ como árvore binária: Cada número corresponde (pelos seus dígitos binários) a um ramo infinito e cada bola a um vértice da árvore. Observemos que duas bolas são, ou disjuntas, ou uma é contida na outra!

Formalmente, para $a_0, a_1, \ldots$ em $\{0, \ldots, p-1\}$,

$$\mathbb{Z}_p := \left\{ (a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \ldots) \in \prod_{\mathbb{Z}} / p^n \mathbb{Z} \right\}.$$

Definição (Limite Inverso)

Seja $\rho_n \colon \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ a supressão do último termo

$$\rho_n \colon a_0 + a_1 p^1 + \cdots + a_{n-1} p^{n-1} + a_n p^n \mapsto a_0 + a_1 p^1 + \cdots + a_{n-1} p^{n-1},$$

e sejam as supressões sucessivas dos últimos termos

$$\cdots \to \mathbb{Z}/p^{n+1}\mathbb{Z} \xrightarrow{\rho_n} \mathbb{Z}/p^n\mathbb{Z} \to \cdots \to \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\rho_1} \mathbb{Z}/p\mathbb{Z} \to 0.$$

Temos $\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ onde o *limite inverso* $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ é definido por

$$\{(s_1, s_2, s_3, \ldots) \in \prod \mathbb{Z}/p^n\mathbb{Z} : \rho_1(s_2) = s_1, \rho_2(s_3) = s_2, \ldots\}.$$

Expansões p-ádicas Exemplares

- Em $\mathbb{Z}_p$,

$$-1 = (p-1, p^2-1, \ldots)$$

Expandindo $p^n - 1 = (p-1) + (p-1)p + \cdots + (p-1)p^{n-1}$,

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots.$$

Por exemplo, $-1 = 1 + 2 + 2^2 + \cdots$ em $\mathbb{Z}_2$.

- Para $p > 2$, vale $2 = (2, 2, \ldots)$ e

$$1/2 = ((p+1)/2, (p^2+1)/2, (p^3+1)/2, \ldots)$$

em $\mathbb{Z}_p$. Ao expandirmos na base p,

$$(p^n+1)/2 = [(p-1)/2]\cdot p^{n-1} + \cdots + [(p-1)/2]\cdot p + (p+1)/2,$$

obtemos

$$1/2 = (p+1)/2 + [(p-1)/2]\cdot p + [(p-1)/2]\cdot p^2 + \cdots.$$

Por exemplo, $1/2 = 2 + 3 + 3^2 + 3^3 \cdots$ em $\mathbb{Z}_3$.

1.3 Princípio Local-Global

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*

$$\mathrm{P}(x) = 0 \textit{ é (não-trivialmente) resolúvel sobre } \mathbb{Z}$$
$$\Longleftrightarrow$$
$$\mathrm{P}(x) = 0 \textit{ é resolúvel sobre } \mathbb{R} \textit{ e sobre todos os } \mathbb{Q}_p \textit{ para } p \textit{ primo}$$

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* ou *de Hasse*:

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

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*

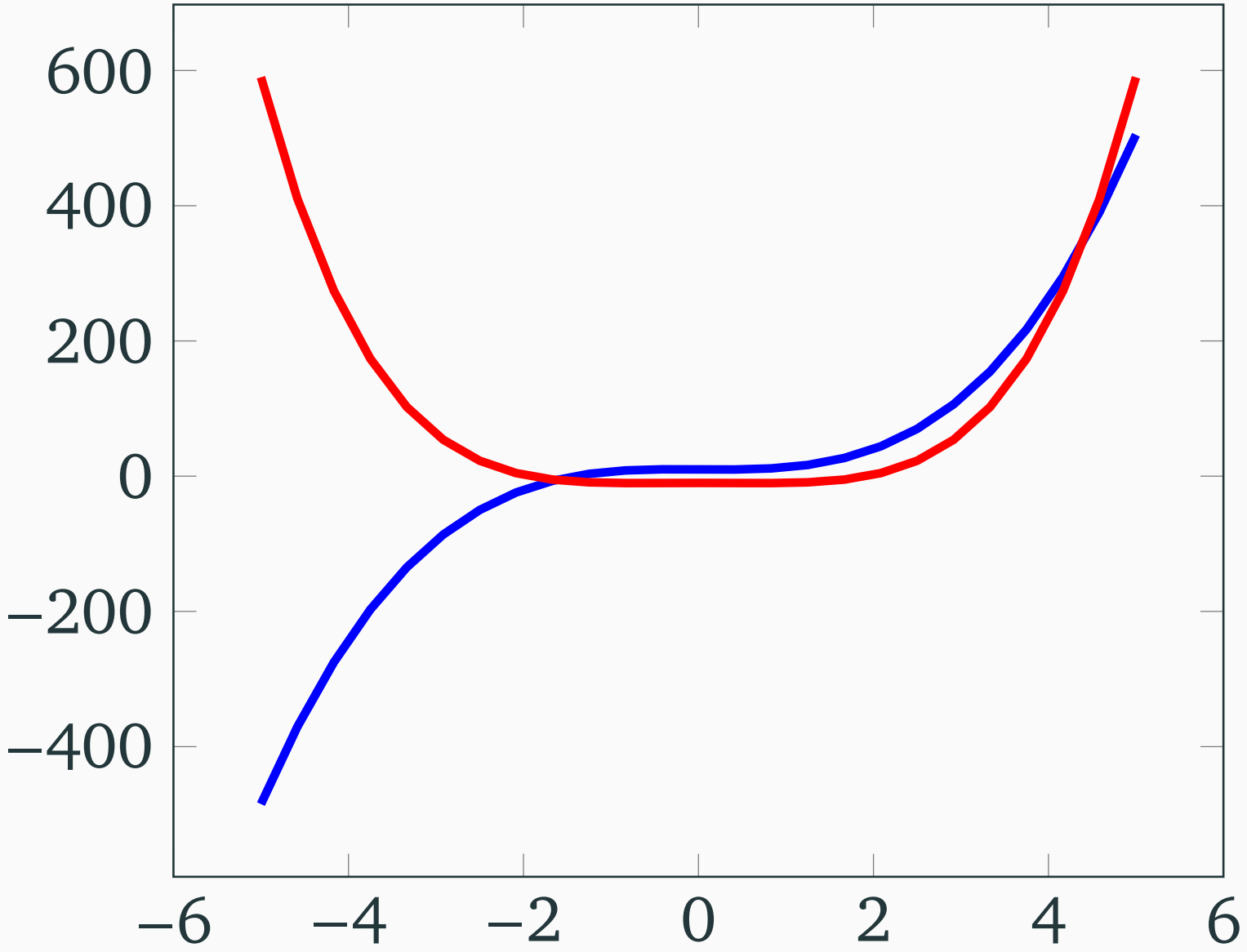
$$\mathrm{P}(x) = 0 \textit{ é (não-trivialmente) resolúvel sobre } \mathbb{Z}$$
$$\Longleftrightarrow$$
$$\mathrm{P}(x) = 0 \textit{ é resolúvel sobre } \mathbb{R}$$

Demonstração.

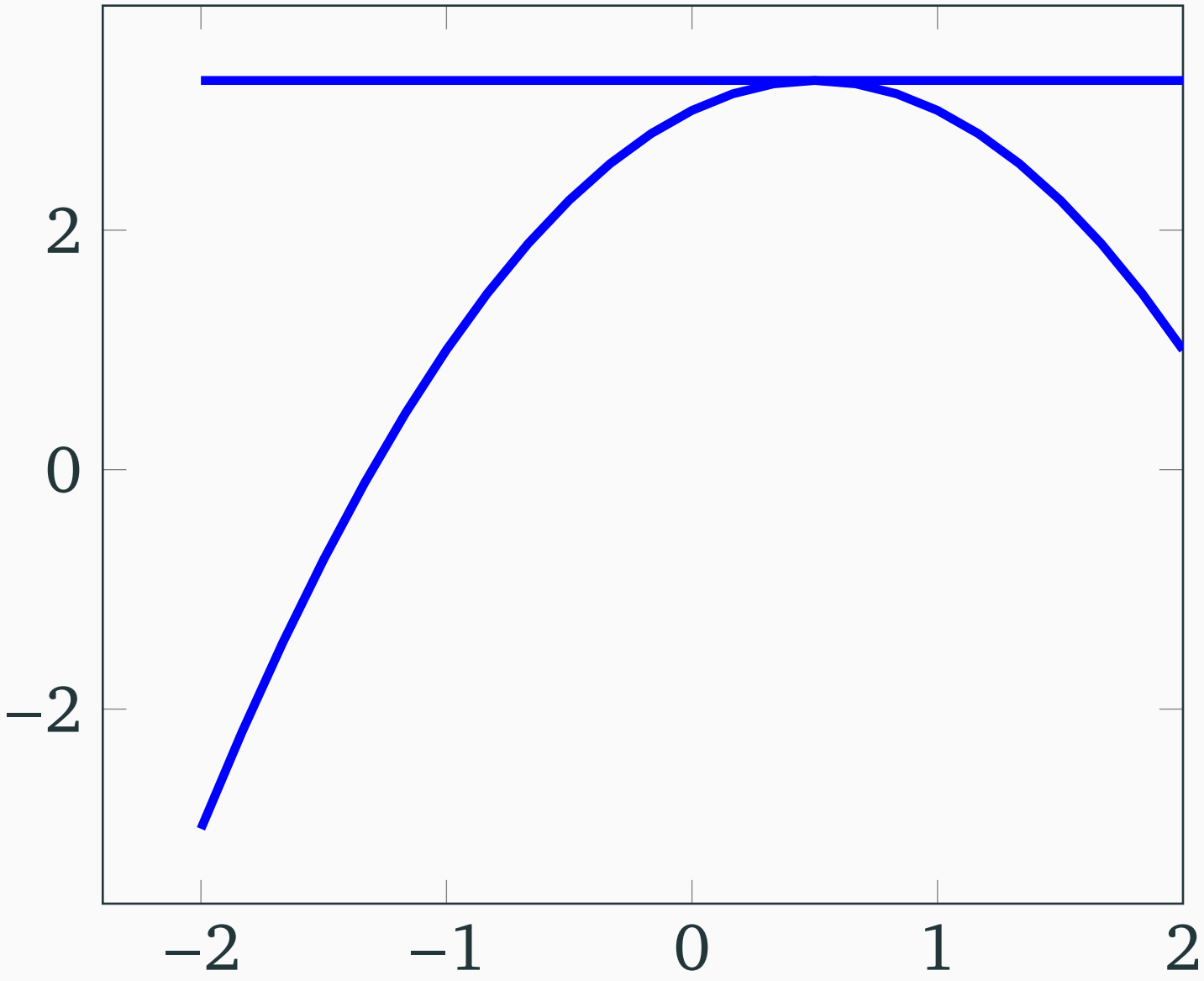
Demonstra-se que todo polinômio quadrático de $n \geq 5$ variáveis tem um zero sobre todo $\mathbb{Q}_p$ para p primo pelo Teorema de Chevalley-Warning sobre a existência de raízes de um polinómio cujo grau é maior que a característica p do corpo. □

Frequentemente, nos interessa o ponto

- em que duas tais curvas polinomiais se intersectam, ou



- em que uma tal curva atinge seu máximo:



Achar as coordenadas destes pontos reduz-se à 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

Existe uma fórmula para calcular as raízes de f?

2.2 Soluções em grau menor

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

- (Completamento do Quadrado ou a Fórmula de Bhaskara [= Matemático e Astronomo Indiano do Século XII]) 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

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

2.3 Permutações de Raízes

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

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

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

são num corpo de números radical

$$\Longleftrightarrow$$

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 à sua imagem (= *auto*), e
- que respeita as operações + e · (= *homomorfismo*).

Definição (Grupo de Galois)

Sejam $r_1, \ldots, r_n$ as raízes de um polinômio *irredutível* (= sem fator racional de grau menor) em $\mathbb{Q}[X]$. O seu *Grupo de Galois* é

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

Por exemplo, para $f(\mathrm{X}) = \mathrm{X}^4 - 2$ 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 $\mathbb{Q}(\sqrt[n]{\alpha})$

Examinemos 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, 1821)

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

Existe uma fórmula para os zeros de f

$$\Longleftrightarrow$$

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

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 existe fórmula.

2.4 Grupo de Galois p-ádico

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

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

é dado pela conjugação complexa $\overline{\cdot}$ e a identidade id só;

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

Semelhantemente, para a restrição de $\overline{\mathbb{Q}}_p$ a $\overline{\mathbb{Q}}$, como

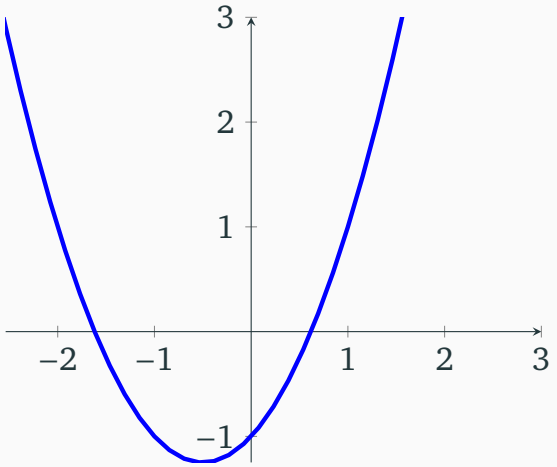
$$\mathbb{Q} \subseteq \mathbb{Q}_p \text{ é denso }, \implies \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q});$$

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

Porém, $\#\,\mathrm{Gal}(\overline{\mathbb{R}}/\mathbb{R}) = 2$, mas $\#\,\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) = \infty$.

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 encontrar 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*.

Teorema (Galois)

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

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

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 Representações de Galois p-ádicas

Construamos uma representação de Galois p-ádica de dimensão 1 pelas p^∞-ésimas raízes da unidade (isto é, raiz de unidade para uma potência de p):

Definição

Denote $\mu_n = \{\zeta \in \overline{\mathbb{Q}}_p : \zeta^n = 1\}$ o grupo abeliano das raízes da unidade, e põe

$$\mathrm{T}_p := \varprojlim_{\cdot p} \mu_{p^n} \xrightarrow{\sim} \mathbb{Z}_p,$$

com a ação de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ sobre T_p bem-definida por

$$\begin{aligned} \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) &\twoheadrightarrow \mathbb{Z}_p^* \\ \sigma &\mapsto k \text{ com } \sigma(\zeta) = \zeta^k. \end{aligned}$$

Construamos uma ação de Galois p-ádica de dimensão 2 pelos pontos p-ádicos de p^{∞}-ésima torção de uma curva elíptica:

Figura: Curvas elípticas no plano real para vários parâmetros de b e a.

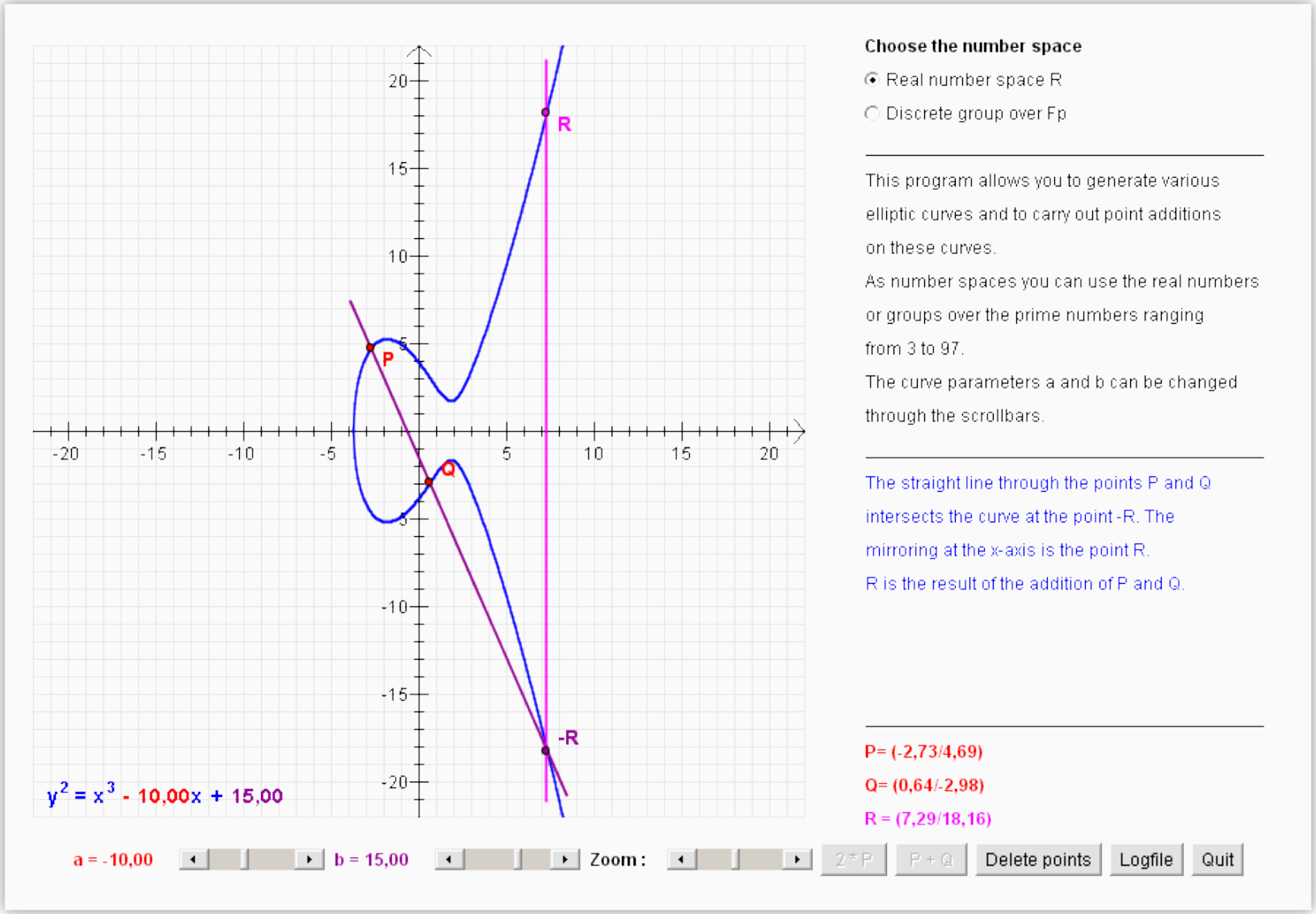


Figura: A adição de dois pontos numa curva elíptica no plano real ilustrado pelo `CrypTool`.

Os pontos de p-torção de uma curva elíptica

Os pontos de uma curva *elíptica* E, dados pela equação de Weierstrass

$$\mathrm{Y}^2 = \mathrm{X}^3 + a\mathrm{X} + b$$

para a e b em $\mathbb{Q}$ com $4a^3 + 27b^2 \neq 0$, formam um grupo abeliano pela regra geométrica

$$\mathrm{P} + \mathrm{Q} + \mathrm{R} = 0, \text{ se estão na mesma reta, e } -(x, y) \coloneqq (x, -y)$$

o que corresponde a uma regra algébrica.

Definição

Seja $\mathrm{E}[n] = \{\mathrm{P} \in \mathrm{E}(\overline{\mathbb{Q}}_p) : n\mathrm{P} = 0\}$ o grupo ab. dos pontos de torção e

$$\mathrm{T}_p(\mathrm{E}) \coloneqq \varprojlim_{\cdot p} \mathrm{E}[p^n]$$

Como $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ opera sobre $\overline{\mathbb{Q}}_p$, opera sobre os pares $\mathrm{T}_p(\mathrm{E}) \xrightarrow{\sim} \mathbb{Z}_p \oplus \mathbb{Z}_p$ e a sua ação é usualmente indecomponível.

3.2 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* $\mathbb{Q}_p(\mu)$ *onde*

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

denote o conjunto de todas as raízes da unidade.
Equivalentemente, se $\cdot^{\mathrm{ab}}$ *denote 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

$$\mu_{p^\infty} = \bigcup_{n\in\mathbb{N}} \mu_{p^n} \quad \text{e} \quad \mu_{\not| p} = \bigcup_{n\in\mathbb{N}} \mu_{p^n-1},$$

vale

$$\mathbb{Q}_p(\mu) = \mathbb{Q}_p(\mu_{p^\infty}) \otimes \mathbb{Q}_p(\mu_{\not| p}).$$

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

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

$\Longrightarrow$ Se se tome o limite projetivo, então obtém-se

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

O *Grupo de Weil* $\mathrm{Weil}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ é definida pela imagem inversa

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)^{\mathsf{ab}} & \xrightarrow{\sim} & \mathbb{Z}_p^* \times \widehat{\mathbb{Z}} = \widehat{\mathbb{Q}}_p^* \\ \bigcup & & \bigcup \\ \mathrm{Weil}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)^{\mathsf{ab}} & \xrightarrow{\sim} & \mathbb{Z}_p^* \times \mathbb{Z} = \mathbb{Q}_p^* = \mathrm{GL}_1(\mathbb{Q}_p) \end{array}$$

Corolário (Teoria do Corpo das Classes [Kronecker, Artin et al, 1930] = 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"*

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

3.3 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 $\mathbf{K} = \mathbb{C}$ 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 à 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 Clássica

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

Existe uma bijeção "natural" entre

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

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.

Correspondência p-ádica

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

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

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

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 (da série de composição) 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:

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

Os ϕ-*módulos filtrados* são dados por um espaço vetorial V sobre $\mathbb{Q}_p$ de dimensão finita com

- um automorfismo $\phi \curvearrowright \mathrm{V}$, e
- uma filtração sobre V indexada pelos inteiros.

Em $\dim \mathrm{V} = 2$ parametrizam-se por :

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

3.4 Langlands para Representações Cristalinas

- $\mathscr{C}^r(\mathbb{Z}_p, \mathbf{K}) = \{$as funções r-vezes deriváveis $f : \mathbb{Z}_p \to \mathbf{K}\}$ e
- $\mathscr{C}^r(\mathbb{Z}_p, \mathbf{K})^* = \{$os funcionais $\int : \mathscr{C}^r(\mathbb{Z}_p, \mathbf{K}) \to \mathbf{K}\}$ o dual.

Fato (Passos para a Correspondência em dimensão 2)

1. $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \curvearrowright \mathrm{V} = \mathbf{K} \oplus \mathbf{K}$ *cristalina*
   $\updownarrow$ *Correspondência de Fontaine*
   $\mathrm{M} := \left(\begin{smallmatrix} \mathbb{Z}_p^* & p^{\mathbb{Z}} \\ & 1 \end{smallmatrix}\right) \curvearrowright \mathscr{V} \hookrightarrow \mathbf{K}[[\mathrm{X}]] \oplus \mathbf{K}[[\mathrm{X}]]$
2. $\mathrm{M} \curvearrowright \mathscr{V} \hookrightarrow \mathbf{K}[[\mathrm{X}]] \oplus \mathbf{K}[[\mathrm{X}]]$
   $\updownarrow$ *avaliação do dual em uma base ortogonal*
   $\mathrm{M} \curvearrowright \mathrm{E}^* \hookrightarrow \mathscr{C}^r(\mathbb{Z}_p, \mathbf{K})^* \oplus \mathscr{C}^s(\mathbb{Z}_p, \mathbf{K})^*$
2'. $\mathrm{M} \curvearrowright \mathrm{E}^* \rightsquigarrow \mathrm{GL}_2(\mathbb{Q}_p) \curvearrowright \mathrm{E}^*$
3. $\mathrm{GL}_2(\mathbb{Q}_p) \curvearrowright \mathrm{E}^* \hookrightarrow \mathscr{C}^r(\mathbb{Z}_p, \mathbf{K})^* \oplus \mathscr{C}^s(\mathbb{Z}_p, \mathbf{K})^*$
   $\updownarrow$ *Duplo-dual*
   $\mathrm{GL}_2(\mathbb{Q}_p) \curvearrowright \mathrm{E} \twoheadleftarrow \mathscr{C}^r(\mathbb{Z}_p, \mathbf{K}) \oplus \mathscr{C}^s(\mathbb{Z}_p, \mathbf{K})$ *Banach*

1 Correspondência de Fontaine

Denotem

- $1, \zeta_p, \zeta_{p^2}, \ldots :=$ raízes da unidade cuja ordem é uma potência de p, e
- $\mathbb{Q}_p^{\text{cyc}:=\mathbb{Q}_p(1,\zeta_p,\zeta_{p^2},\ldots)}$ o corpo ciclotómico.

Operem os Grupos de Galois

$$\overline{\mathbb{Q}}_p \overset{\mathrm{H}\curvearrowright}{\text{---}} \mathbb{Q}_p^{\text{cyc}} \overset{\Gamma\curvearrowright}{\text{---}} \mathbb{Q}_p$$

onde

$\Gamma := \mathrm{Gal}(\mathbb{Q}_p^{\text{cyc}/\mathbb{Q}_p)} \xrightarrow{\sim} \mathbb{Z}_p^*$

$\sigma \mapsto x$ dado por $\sigma(\zeta) = \zeta^x$ para todo $\zeta_1 = 1, \zeta_p, \ldots$

Fato (Corpo de Normas, [Fon90])

Os Grupos de Galois absolutos de $\mathbb{F}_p((t))$ *e* $\mathbb{Q}_p^{\text{cyc}}$ *são isomórficos.*

Seja $\varphi :=$ o *Frobenius* o automorfismo de $\mathbb{F}_p((t))$ dado por $\cdot^p$.

Fato (Mondromia [Kat70])

Seja $\mathbf{E}$ *um corpo de característica* p*. Existe uma equivalência entre categorias*

$$\left\{ \begin{array}{l} \textit{ações contínuas} \\ \textit{de } \mathrm{Gal}(\overline{\mathbf{E}}/\mathbf{E}) \textit{ em} \\ \textit{espaços vetoriais /} \\ \mathbb{F}_p \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{l} \textit{ações semi-lineares injetoras} \\ \textit{de } \varphi \textit{ em espaços vetoriais /} \ \mathbf{E} \end{array} \right\}$$

Demonstração.

Plausível porque o Frobenius gera o Grupo de Galois como grupo

Corolário

Seja $\mathscr{E} := \{\sum_{n\in\mathbb{Z}} a_n \mathrm{X}^n : \{|a_1|, |a_2|, \ldots\}$ *limitado e* $a_{-n} \overset{n\to\infty}{\to} 0\}$ *o anel completo em* $\mathbb{Q}_p[[\mathrm{X}^{\pm 1}]]$. *Existe uma equivalência entre categorias*

$$\left\{\begin{array}{l}\text{ações contínuas}\\ \text{de } \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{cyc})} \text{ em}\\ \text{espaços vetoriais / } \mathbb{Q}_p\end{array}\right\} \xrightarrow{\sim} \left\{\begin{array}{l}\text{ações semi-lineares injetoras}\\ \text{de } \varphi \text{ em espaços vetoriais / } \mathscr{E}\end{array}\right\}$$

Demonstração.

- Pelo Corpo de Normas (Fontaine) $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{cyc})} \cong \mathrm{Gal}(\overline{\mathbb{F}_p((t))}/\mathbb{F}_p((t)))$, e
- Pelo Fato precedente (Katz), e
- pelo levantamento dos coeficientes do espaço vetorial de $\mathbb{F}_p$ a $\mathbb{Q}_p$ pelo funtor de Witt e inversão de p. □

Teorema (Fontaine)

Seja $\mathscr{E} := \{\sum_{n\in\mathbb{Z}} a_n \mathrm{X}^n : \{|a_1|, |a_2|, \ldots\}$ *limitado e* $a_{-n} \overset{n\to\infty}{\to} 0\}$ *o anel completo em* $\mathbb{Q}_p[[\mathrm{X}^{\pm 1}]]$ *com*

- $\varphi \curvearrowright \mathscr{E}$ *por* $t^\varphi := (1+t)^p - 1$, *e*
- $\Gamma \curvearrowright \mathscr{E}$ *por* $t^\gamma := (1+t)^\gamma - 1 = \sum \binom{\gamma}{n} t^n$ *onde* $\Gamma \cong \mathbb{Z}_p^*$

Existe uma equivalência entre categorias

$$\left\{\begin{array}{l}\text{ações contínuas}\\ \text{de } \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \text{ em}\\ \text{espaços vetoriais / } \mathbb{Q}_p\end{array}\right\} \xrightarrow{\sim} \left\{\begin{array}{l}\text{ações semi-lineares injetoras}\\ \text{de } \varphi \text{ e } \Gamma \text{ comutativos}\\ \text{em espaços vetoriais / } \mathscr{E}\end{array}\right\}$$

Demonstração.

Pelo Teorema precedente para $\mathrm{H} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{cyc})}$ usando

$$\overline{\mathbb{Q}}_p \overset{\mathrm{H}\curvearrowright}{\longleftarrow} \mathbb{Q}_p^{\mathrm{cyc}} \overset{\Gamma\curvearrowright}{\longleftarrow} \mathbb{Q}_p.$$

2 Isomorfismo de Iwasawa

Seja $\mathbf{K}$ uma ext. finita de $\mathbb{Q}_p$ com anel de inteiros $\mathbf{o_K}$. Denote

- $\mathscr{C}^0(\mathbb{Z}_p, \mathbf{K}) := \{$ as funções contínuas $f : \mathbb{Z}_p \to \mathbf{K}\}$, e
- $\mathscr{D}^0(\mathbb{Z}_p, \mathbf{K}) := \{$ os funcionais $\int : \mathscr{C}^0(\mathbb{Z}_p, \mathbf{K}) \to \mathbf{K}\}$.

Teorema (de Iwasawa)

Vale $\mathscr{D}^0(\mathbb{Z}_p, \mathbf{K}) \xrightarrow{\sim} \mathbf{K} \otimes_{\mathbf{o_K}} \mathbf{o_K}[[\mathrm{X}]]$ *como* $\mathbf{K}$*-álgebras topológicas.*

Demonstração.

- Pela densidade das funções localmente constantes, isto é, $\mathbf{o_K}[\mathbb{Z}/p\mathbb{Z}] \cup \mathbf{o_K}[\mathbb{Z}/p^2\mathbb{Z}] \cup \ldots$ em $\mathscr{C}^0(\mathbb{Z}_p, \mathbf{o_K})$

$$\mathscr{D}^0(\mathbb{Z}_p, \mathbf{o_K}) \xrightarrow{\sim} \varprojlim \mathbf{o_K}[\mathbb{Z}/p^n\mathbb{Z}] =: \mathbf{o_K}[[\mathbb{Z}_p]], \quad \text{e}$$

- pelo *Isomorfismo de Iwasawa* que envia o gerador $\mathbf{1}$ de $\mathbb{Z}_p$ a $1 + \mathrm{X}$

$$\mathbf{o_K}[[\mathbb{Z}_p]] \xrightarrow{\sim} \mathbf{o_K}[[\mathrm{X}]].$$

3 Dualidade de Schikhof

Corolário (Teorema de Mahler)

Seja $\binom{\cdot}{n} : \mathbb{Z}_p \to \mathbf{K}$ *com* $\binom{x}{n} := x(x-1)\cdots(x-n+1)/n!$.
Temos

$$\{ \text{ as sequências em } \mathbf{K} \text{ que convergem a zero } \} \xrightarrow{\sim} \mathscr{C}^0(\mathbb{Z}_p, \mathbf{K})$$
$$(a_n) \mapsto \sum a_n \binom{\cdot}{n}$$

Demonstração.

Segue da Dualidade de Schikhof,

- pois $\mathscr{D}^0(\mathbb{Z}_p, \mathbf{K}) \xrightarrow{\sim} \{$ as sequências limitadas em $\mathbf{K} \}$ pelo Teorema de Iwasawa, e
- o espaço normado $\{$ as sequências limitadas em $\mathbf{K} \}$ é dual ao $\{$ as sequências em $\mathbf{K}$ que convergem a zero $\}$. □

2' Isom. de Iwasawa para Funções Deriváveis

Seja $r \geq 0$. Denotem

- $\mathscr{C}^r(\mathbb{Z}_p, \mathbf{K}) :=$
  $\{$ as funções r-vezes deriváveis $f : \mathbb{Z}_p \longrightarrow \mathbf{K}\}$,
- $\mathscr{C}^r(\mathbb{Z}_p, \mathbf{K})^* := \{$ os funcionais $\int : \mathscr{C}^r(\mathbb{Z}_p, \mathbf{K}) \longrightarrow \mathbf{K}\}$ o dual,

e

$c^r(\mathbb{N}, \mathbf{K})^* := \{$ os $\sum a_n \mathrm{X}^n$ em $\mathbf{K}[[\mathrm{X}]]$ com $\{|a_n|/n^r\}$ limitado $\}$.

Corolário

A aplicação $\mathscr{C}^r(\mathbb{Z}_p, \mathbf{K})^* \xrightarrow{\sim} c^r(\mathbb{N}, \mathbf{K})^*$ *dada por*

$$\int \mapsto \sum_n a_n \mathrm{X}^n \quad \text{com } a_n = \int \binom{\cdot}{n}$$

é um isomorfismo entre espaços vetoriais normados.

3’ Dual. de Schikhof para Funções Deriváveis

Seja $r \geq 0$. Denotem

$$\mathscr{C}^r(\mathbb{Z}_p, \mathbf{K}) := \{ \text{ as funções } r\text{-vezes deriváveis } f : \mathbb{Z}_p \to \mathbf{K}\}$$

e

$$c^r(\mathbb{N}, \mathbf{K}) := \{ \text{ as sequências } (a_n) \text{ em } \mathbf{K} \text{ com } |a_n| n^r \to 0 \ \}.$$

Corolário

A aplicação $c^r(\mathbb{N}, \mathbf{K}) \xrightarrow{\sim} \mathscr{C}^r(\mathbb{Z}_p, \mathbf{K})$ *dada por*

$$(a_n) \mapsto \sum_n a_n \binom{\cdot}{n}.$$

é um isomorfismo entre espaços vetoriais normados.

Recado: Funtor de Langlands

Funtor de Langlands p-ádico

Sejam $\mathbb{F}$ e $\mathbf{K}$ extensões finitas de $\mathbb{Q}_p$. Existe um funtor entre

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

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 (da série de composição) finito,

Estado da Arte

Fato

A Correspondência de Langlands p-ádica é (completamente) formulada e demonstrada para: ▶ $n = 2$, e ▶ $\mathbb{F} = \mathbb{Q}_p$.

Demonstração (retraçada em [Col14]).

Vide também [Nag17] para uma detalhada reformulação da correspondência para representações cristalinas. □

Para $n > 2$ ou $\mathbb{F} \supset \mathbb{Q}_p$ a correspondência até hoje nem foi formulada sequer demonstrada!

$\Longrightarrow$ duas vias para generalizar esta correspondência:

1. Dimensões $n > 2$, e
2. Corpos $\mathbb{F} \supset \mathbb{Q}_p$.

4.1 Dimensão maior: Diferenciabilidade p-ádica

Para construir os espaços de Banach para $n > 2$ precisamos de uma noção de diferenciabilidade fracionaria (isto é, para um grau real $r \geq 0$) de várias variáveis que estende a sobre $\mathbb{Z}_p$.
Vejamos primeiro a situação clássica sobre $\mathbb{R}$. Seja $\mathrm{X} \subseteq \mathbb{R}$ um intervalo aberto e $f : \mathrm{X} \longrightarrow \mathbb{R}$.

Definição (da Diferenciabilidade na Reta)

Uma função f é $\mathscr{C}^1$ no ponto $x_0 \in \mathrm{X}$ se

$$f'(x_0) = \lim_{x \to x_0} \frac{f(x) - f(x_0)}{x - x_0}$$

exista. Declaramos que f é $\mathscr{C}^1$ se f é $\mathscr{C}^1$ em todos os pontos $x_0 \in \mathrm{X}$ e é contínua.

Se f é $\mathscr{C}^1$, denote $f' : X \to \mathbb{R}$ a derivada de f.

Proposição 4.1 (Completude do Espaço das Funções Diferençáveis)

Seja X compacto. O espaço $\mathscr{C}^1(X, \mathbb{R})$ com a norma

$$\|f\|_{\mathscr{C}^1} = \max\{\|f\|_{\sup}, \|f'\|_{\sup}\}$$

é completo.

Demonstração.

A prova usual usa o Teorema Fundamental do Cálculo. □

Se $\mathbb{R}$ é substituído por um corpo p-ádico tal como $\mathbb{Q}_p$, então esta proposição é incorreta!

$\Longrightarrow$ Definição alternativa da diferenciabilidade:

Proposição 4.2 (Demonstração alternativa à Proposição 4.1)

A função $f \in \mathscr{C}^1(\mathrm{X}, \mathbb{R})$ se e tão-somente se a função

$$f^{]1[}(x, y) = \frac{f(x) - f(y)}{x - y},$$

definida para todos $x, y \in \mathrm{X}$ desiguais, estende-se a uma função $f^{[1]} : \mathrm{X} \times \mathrm{X} \longrightarrow \mathbb{R}$ contínua.

Demonstração.

Se $(x, y) \longrightarrow (a, a) \in \mathrm{X} \times \mathrm{X}$, então

$$f^{]1[}(x, y) = f'(\xi) \longrightarrow f'(a) = f^{[1]}(a, a) \quad \text{com } \xi \in [x, y]$$

onde a primeira igualdade provém do TVM e a segunda da continuidade de f'. Logo $f^{[1]}$ é contínua em todos os pontos, pois $f^{]1[}(\{(x, y) \in \mathrm{X} \times \mathrm{X} : x \neq y)$ é denso em $f^{[1]}(\mathrm{X} \times \mathrm{X})$. □

Esta caracterização da diferenciabilidade evidencia a completude do espaço normado das funções diferençáveis:

Corolário

Seja X *compacto. O espaço* $\mathscr{C}^1(\mathrm{X}, \mathbb{R})$ *é completo.*

Demonstração.

Como visto acima pelo Teorema do valor médio, a norma $\|f\| = \max\{\|f\|_{\sup}, \|f^{[1]}\|_{\sup}\}$ é igual a norma

$$\|f\|_{\mathscr{C}^1} = \max\{\|f\|_{\sup}, \|f'\|_{\sup}\}.$$

Então, quanto à primeira norma, esta proposição é evidente. □

1 Definição da diferenciabilidade de grau 1

Como não existe análogo ao Teorema do Valor Intermediário e as suas consequências, como o Teorema do Valor Médio que é usado para demonstrar Proposição 4.2, propõe-se a definição seguinte para garantir um análogo à Proposição 4.1, a completude do espaço normado das funções diferençáveis:

Definição (para compensar o Teorema do Valor Médio)

Sejam $\mathrm{X} \subseteq \mathbf{K}$ aberto e $f : \mathrm{X} \to \mathbf{K}$. Então f é $\mathscr{C}^1$ no ponto $a \in \mathrm{X}$ se o limite

$$\lim_{(x,y)\to(a,a)} f^{]1[}(x,y) \quad \text{com } f^{]1[} = \frac{f(x)-f(y)}{x-y} \quad \text{para } x \neq y$$

existe. Então f é $\mathscr{C}^1$ se f é $\mathscr{C}^1$ em todos os pontos $a \in \mathrm{X}$ ou igualmente se $f^{]1[}$ estende a uma função $f^{[1]}$ contínua.

Questão

Como definir uma função duas *vezes diferençável?*

Observemos que ora $f^{[1]}$ é uma função em *duas* variáveis; tal que para definir uma função de uma única variável como *duplamente* diferençável, precisamos (ao contrário da reta) de tratar a diferenciação de funções de múltiplas variáveis!

Definição (da Diferenciablidade sobre os Espaços Vetoriais)

Sejam V e $\mathbf{E}$ espaços vetoriais, $\mathrm{X} \subseteq \mathrm{V}$ aberto e $f : \mathrm{X} \longrightarrow \mathbf{E}$. Então f é $\mathscr{C}^1$ no ponto $a \in \mathrm{X}$ se existe uma aplicação linear contínua A tal que para todos $\varepsilon > 0$ existe $\mathrm{U} \ni a$ aberto em X tal que

$$f(x+h) - f(x) = \mathrm{A} \cdot h + \mathrm{R}(x+h, x)$$

com o resto $\|\mathrm{R}(x+h, x)\| \leq \varepsilon \|h\|$ para todos $x + h, x \in \mathrm{U}$.

2 Diferenciabilidade iterada

Esta definição não rende diretamente uma definição de diferenciabilidade geral, mas indica como proceder em geral:

Definição (da Diferenciabilidade Parcial Simultânea)

Sejam $\mathrm{V}, \mathbf{E}, \mathrm{X} \subseteq \mathrm{V}$ e $f : \mathrm{X} \to \mathbf{E}$ como acima e tenha V coordenadas, isto é, $\mathrm{V} = \mathbf{K}^d$ com $e_1, \ldots, e_d$ a base natural. Então f é $\mathscr{C}^1$ se para todos $x + h, x \in \mathrm{X}$ com $h \in \mathbf{K}^{*d}$ a função $f^{]1[}(x + h, x)$ definida por

$$(x + h, x) \mapsto \mathrm{A} \in \mathrm{Hom}_{\mathbf{K}}(\mathrm{V}, \mathbf{E})$$

com $\mathrm{A} \cdot h_k e_k$ definida pelo seu valor

$$f(x+h_1e_1+\cdots+h_{k-1}e_{k-1}+h_ke_k) - f(x+h_1e_1+\cdots+h_{k-1}e_{k-1})$$

estende-se a uma função contínua $f^{[1]} : \mathrm{X} \times \mathrm{X} \to \mathrm{Hom}_{\mathbf{K}}(\mathrm{V}, \mathbf{E})$.

Observemos

- que $\mathrm{X} \times \mathrm{X} \subseteq \mathrm{V} \times \mathrm{V}$ é novamente um espaço vetorial com coordenados naturais, e
- que $\operatorname{im} f \subseteq \operatorname{Hom}_{\mathbf{K}}(\mathrm{V}, \mathbf{E})$ é novamente um espaço vetorial de dimensão finita!

$\Longrightarrow$ Podemos iterar a condição da diferenciabilidade pela sua aplicação à "derivada" $f^{[1]}$:

Definição (da Diferenciabilidade Iterada)

A função $f : \mathrm{X} \to \mathbf{E}$ é $\mathscr{C}^2$ se

- f é $\mathscr{C}^1$, e
- $f^{[1]} : \mathrm{X} \times \mathrm{X} \to \operatorname{Hom}_{\mathbf{K}}(\mathrm{V}, \mathbf{E})$ é $\mathscr{C}^1$.

Em geral, f é $\mathscr{C}^n$ se f é $\mathscr{C}^{n-1}$ e $f^{[n-1]}$ é $\mathscr{C}^1$.

3 Diferenciabilidade de grau real

Lembremo-nos de que o objetivo era dar uma definição de funções r-vezes diferençáveis para $r \geq 0$ em $\mathbb{R}$. Escrevamos $r = \nu + \rho$ com $\nu \in \mathbb{N}$ e $\rho \in [0, 1[$.

Definição (da Continuidade de Hölder reforçada)

Sejam $V, \mathbf{E}, X \subseteq V$ e $f : X \to \mathbf{E}$ como acima. Então f é $\mathscr{C}^\rho$ no ponto $a \in X$ se para todos $\varepsilon > 0$, existe um $U \subseteq X$ aberto tal que

$$\|f(x) - f(x)\| \leq \varepsilon \|x - y\|^\rho \quad \text{para todos } x, y \in U.$$

Em seguida f é $\mathscr{C}^\rho$ se f é $\mathscr{C}^\rho$ em todos os pontos $a \in X$.

Definição (da Diferenciabilidade Fracionária, [Nag16])

Uma função $f : X \to \mathbf{E}$ é $\mathscr{C}^r$ se f é $\mathscr{C}^\nu$ e $f^{[\nu]}$ é $\mathscr{C}^\rho$.

Descrições Mais Simples da Condição de Diferenciabilidade p-ádica ([Nag16])

1. Seja $\mathrm{X} \subseteq \mathbf{K}$ aberto. Uma função $f : \mathrm{X} \longrightarrow \mathbf{K}$ é $\mathscr{C}^r$ se, e tão-somente se, o resto de polinômio de Taylor

   $$\mathrm{R}_\nu f(x+h, x) = f(x+h) - [f(x) + f'(x)h \cdots - f^{(\nu)}(x)/\nu! h^\nu]$$

   satisfaz como função de duas variáveis $x + h, x$ uma condição de convergência de grau $o(|h|^r)$.
2. Seja $\mathrm{X} = \mathbb{Z}_p^d$. O espaço de Banach $\mathscr{C}^0(\mathrm{X}, \mathbf{K})$ (de funções contínuas) tem a *base ortogonal de Mahler* dos *polinómios binomiais* $\binom{\cdot}{n}$. Uma função $f : \mathrm{X} \longrightarrow \mathrm{K}$ é $\mathscr{C}^r$ se, e tão-somente se, os seus coeficientes de Mahler $(a_n)_{n \in \mathbb{N}^d}$ satisfazem $|a_n| n^r \longrightarrow 0$ para $|n| = n_1 + \cdots + n_d \longrightarrow \infty$.
3. Como consequência de ambos os pontos, para conjuntos abertos $\mathrm{U} \subseteq \mathbb{Q}_p^d$, uma função $f : \mathrm{U} \longrightarrow \mathbf{K}$ é r-vezes diferençável se, e tão-somente se, os restos dos seus polinómios de Taylor parciais convergem como acima.

4.2 Corpos Maiores: Polinómios de Fourier

Seja $r \geq 0$. Denotem

- $\mathscr{C}^r(\mathbb{Z}_p, \mathbf{K}) :=$
  $\{$ as funções r-vezes deriváveis $f : \mathbb{Z}_p \to \mathbf{K}\}$,
- $\mathscr{C}^r(\mathbb{Z}_p, \mathbf{K})^* := \{$ os funcionais $\int : \mathscr{C}^r(\mathbb{Z}_p, \mathbf{K}) \to \mathbf{K}\}$,

e

$c^r(\mathbb{N}, \mathbf{K})^* := \{$ os $\sum a_n \mathrm{X}^n$ em $\mathbf{K}[[\mathrm{X}]]$ com $\{|a_n|/n^r\}$ limitado $\}$.

Teorema ([BB10], [Col10], [Nag16])

A aplicação $\mathscr{C}^r(\mathbb{Z}_p, \mathbf{K})^* \xrightarrow{\sim} c^r(\mathbb{N}, \mathbf{K})^*$ dada por

$$\int \mapsto \sum_n a_n \mathrm{X}^n \quad \text{com } a_n = \int \binom{\cdot}{n}.$$

é um isomorfismo entre espaços vetoriais normados.

Seja $\mathbb{F}$ uma ext. finita de $\mathbb{Q}_p$ com anel de inteiros $\mathbf{o}_{\mathbb{F}}$.

Questão

Qual é o análogo do polinómio $\binom{\cdot}{n}$ sobre $\mathbb{Z}_p$ para $\mathbf{o}_{\mathbb{F}}$?

- $\mathscr{C}^{\mathrm{la}(\mathbf{o}_{\mathbb{F}},\mathbf{K})} := \{$ as funções localm. analíticas $f : \mathbf{o}_{\mathbb{F}} \to \mathbf{K}\}$,
- $\mathscr{D}^{\mathrm{la}(\mathbf{o}_{\mathbb{F}},\mathbf{K})} := \{$ os funcionais $\int : \mathscr{C}^{\mathrm{la}(\mathbf{o}_{\mathbb{F}},\mathbf{K}) \to \mathbf{K}}\}$,

e, para B a bola unitária no completamento do fecho alg. de $\mathbb{Q}_p$,

$$\mathcal{O}(\mathrm{B}) := \{ \text{ os } \sum a_n \mathrm{X}^n \text{ em } \mathbf{K}[[\mathrm{X}]] \text{ que convergem em } \mathrm{B} \}.$$

Fato (Análogo ao Isomorfismo de Iwasawa, [ST01])

Existem polinómios $\mathrm{P}_0, \mathrm{P}_1, \ldots$ tais que $\mathscr{D}^{\mathrm{la}(\mathbb{Z}_p,\mathbf{K})} \xrightarrow{\sim} \mathcal{O}(\mathrm{B})$ def. por

$$\int \mapsto \sum_n a_n \mathrm{X}^n \quad \text{com } a_n = \int \mathrm{P}_n$$

é um isomorfismo entre álgebras de Fréchet.

Seja $s \geq 0$ e denote $\mathbf{K} = \mathbb{C}_p$ o completamento do fecho algébrico de $\mathbb{Q}_p$. Denotem

- $\mathscr{C}^s(\mathbf{o}_\mathbb{F}, \mathbf{K}) := \{$ as funções s-vezes deriváveis $f : \mathbf{o}_\mathbb{F} \to \mathbf{K}\}$,
- $\mathscr{C}^s(\mathbf{o}_\mathbb{F}, \mathbf{K})^* := \{$ os funcionais $\int : \mathscr{C}^s(\mathbf{o}_\mathbb{F}, \mathbf{K}) \to \mathbf{K}\}$,

e

$c^s(\mathbb{N}, \mathbf{K})^* := \{$ os $\sum a_n \mathrm{X}^n$ em $\mathbf{K}[[\mathrm{X}]]$ com $\{|a_n|/n^s\}$ limitado $\}$.

Teorema 4.1 (Extensão de $\mathbb{Z}_p$ para $\mathbf{o}_\mathbb{F}$ por [Nag18])

Seja $d := [\mathrm{F} : \mathbb{Q}_p]$. Se $r \geq d$, então, para os polinómios P_0, P_1, ... definidos em [STo1], a $\mathscr{D}^r(\mathbb{Z}_p, \mathbf{K}) \xrightarrow{\sim} c^{r/d}(\mathbb{N}, \mathbf{K})$ definida por

$$\int \mapsto \sum_n a_n \mathrm{X}^n \quad \text{com } a_n = \int \mathrm{P}_n$$

é um isomorfismo entre espaços normados.

3’ Dual. de Schikhof para Funções Deriváveis

Seja $s \geq 0$. Denotem

$$\mathscr{C}^s(\mathbf{o}_{\mathbb{F}}, \mathbf{K}) := \{ \text{ as funções } s\text{-vezes deriváveis } f : \mathbf{o}_{\mathbb{F}} \to \mathbf{K}\}$$

e

$$c^s(\mathbb{N}, \mathbf{K}) := \{ \text{ as sequências } (a_n) \text{ em } \mathbf{K} \text{ com } |a_n| n^s \to 0 \ \}.$$

Corolário ([Nag18])

Seja $r \geq 0$ e $d := [\mathrm{F} : \mathbb{Q}_p]$. A aplicação $c^{r/d}(\mathbb{N}, \mathbf{K}) \xrightarrow{\sim} \mathscr{C}^r(\mathbf{o}_{\mathbb{F}}, \mathbf{K})$ dada por

$$(a_n) \mapsto \sum_n a_n \binom{\cdot}{n}.$$

é um isomorfismo entre espaços vetoriais normados.

1 Existência de Raízes

2 Descrição de Raízes

3 Programa de Langlands

4 Estender Langlands

5 Aplicar Langlands

- Estratégia
- Cálculo da Redução $\mod p$

5.1 Estratégia

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

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

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

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 (da série de composição) finito,

Para $n = 2$, este funtor realiza a correspondências para representações entre $\mathrm{GL}_2(\mathbb{Q}_p)$ e $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ *cristalinas*:

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

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 $\overline{\mathbb{F}}_p^*$.

Questão (Computação da Redução $\mod p$)

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) em [NP19].

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:

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

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

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

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 Composição de Q, e
2. os da Série de Composição 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]).

Teorema ([NP19])

Seja $r := k-2$ *e* a *em* $\{3,\dots,p+1\}$ *tal que* $r \equiv a \bmod p-1$. *Se* $p \geq 5$, $r \geq 2p+2$ *e* $v(a_p)$ *em* $]2,3[$ *(e, se* $v(a_p) = 5/2$, *então* $v(a_p^2 - p^5) = 5$*), então*

$$\overline{\mathrm{V}}_{k,a_p} \cong \begin{cases} \mathrm{ind}(\omega_2^{a+1}), & \text{para } a = 3 \text{ e } r \not\equiv 2 \bmod p \\ \mathrm{ind}(\omega_2^{a+p}), & \text{para } a = 3 \text{ e } r \equiv 2 \bmod p^2 \\ \mathrm{ind}(\omega_2^{a+2p-1}), & \text{para } a = 4 \text{ e } r \not\equiv 4,3 \bmod p \\ \mathrm{ind}(\omega_2^{a+p}), & \text{para } a = 4 \text{ e } r \equiv 3 \bmod p \\ \mathrm{ind}(\omega_2^{a+1}), & \text{para } a = 4 \text{ e } r \equiv 4 \bmod p \\ \mathrm{ind}(\omega_2^{a+2p-1}), & \text{para } a = 5 \text{ e } r \equiv 2,3 \bmod p \\ \dots & \\ \upsilon(\sqrt{-1})\omega \oplus \upsilon(-\sqrt{-1})\omega, & \text{para } a = p \text{ e } r \equiv p \bmod p^3 \\ \dots & \end{cases}$$

1. Existência de Raízes
2. Descrição de Raízes
3. Programa de Langlands
4. Estender Langlands
5. Aplicar Langlands

As notas estão disponíveis em

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


L. Berger and C. Breuil, *Sur quelques représentations potentiellement cristallines de* $\mathbf{GL}_2(\mathbf{Q}_p)$, Astérisque **330** (2010), 155–211.


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).


P. Colmez, *Fonctions d'une variable* p*-adique*, Astérisque (2010), no. 330, 13–59. MR 2642404.


_____, *Le programme de Langlands p-adique*, European Congress of Mathematics Kraków, 2–7 July 2012, 2014, pp. 259–284.


J.-M. Fontaine, *Représentations p-adiques des corps locaux. I*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 249–309. MR 1106901.


N. M. Katz, *Nilpotent connections and the monodromy theorem: Applications of a result of Turrittin*, Inst. Hautes Études Sci. Publ. Math. (1970), no. 39, 175–232. MR 0291177. Confer `http://www.numdam.org/item?id=PMIHES_1970__39__175_0`.

 E. Nagel, *p-adic Taylor polynomials*, Indag. Math. (N.S.) **27** (2016), no. 3, 643–669. MR 3505986. DOI 10.1016/j.indag.2015.12.003. Confer http://www.sciencedirect.com/science/article/pii/S0019357715001275.

 _____, *From Crystalline to Unitary Representations*, Around Langlands correspondences, Contemp. Math., vol. 691, Amer. Math. Soc., Providence, RI, 2017, pp. 283–335. MR 3666058. DOI 10.1090/conm/691/13901. Confer https://konfekt.bitbucket.io/publications/fGModCrFct.pdf.

 _____, *p-adic Fourier bases of differentiable functions*, Documenta Mathematica **27** (2018), no. 23, 939 – 967. DOI 10.25537/dm.2018v23.939-967. Confer https://www.elibm.org/article/10011869.


E. Nagel and A. Pande, *Reductions of modular Galois Representations of Slope 2 to 3*, preprint (2019). arXiv 1801.08820. Confer `https://konfekt.bitbucket.io/publications/modGaloisSlope2To3.pdf`.


P. Schneider and J. Teitelbaum, *p-adic Fourier theory*, Doc. Math. **6** (2001), 447–481 (electronic). MR 1871671.