p-adikus lineáris csoportok reprezentációi

Zábrádi Gergely
zger@cs.elte.hu

2013. febr. 26.

Motiváció

$f(x) \in \mathbb{Z}[x]$ irreducibilis. Hogy bomlik fel f modulo p? ($2 \nmid p$ prím)

Motiváció

$f(x) \in \mathbb{Z}[x]$ irreducibilis. Hogy bomlik fel f modulo p? ($2 \nmid p$ prím)
Legegyszerűbb példa:

$$x^2 - d \equiv x^2 \pmod{p} \iff p \mid d$$

$$x^2 - d \equiv (x-b)(x+b) \pmod{p} \quad (b \neq 0) \iff \left(\frac{d}{p}\right) = 1$$

$$x^2 - d \text{ irreducibilis } \pmod{p} \iff \left(\frac{d}{p}\right) = -1 \ .$$

Motiváció

$f(x) \in \mathbb{Z}[x]$ irreducibilis. Hogy bomlik fel f modulo p? ($2 \nmid p$ prím)
Legegyszerűbb példa:

$$x^2 - d \equiv x^2 \pmod{p} \iff p \mid d$$

$$x^2 - d \equiv (x-b)(x+b) \pmod{p} \quad (b \neq 0) \iff \left(\frac{d}{p}\right) = 1$$

$$x^2 - d \text{ irreducibilis } \pmod{p} \iff \left(\frac{d}{p}\right) = -1 \ .$$

Ha $d = 2^\epsilon q_1 \dots q_r$, akkor – a kvadratikus reciprocitást használva –

$$\left(\frac{d}{p}\right) = \left(\frac{2}{p}\right)^\epsilon \prod_{i=1}^{r} \left(\frac{q_i}{p}\right) = (-1)^{\epsilon(p^2-1)/8} \prod_{i=1}^{r} (-1)^{(p-1)(q_i-1)/4} \left(\frac{p}{q_i}\right) \ .$$

Így ($p \nmid 2d$ esetén) $x^2 - d$ felbonthatósága $\mathbb{F}_p$ fölött csak p mod $(4d)$-tól függ.

Fogalmazzuk át a problémát!

Kérdés: Általánosabb $f(x)$ esetén van-e hasonló feltétel p-re?

Fogalmazzuk át a problémát!

Kérdés: Általánosabb $f(x)$ esetén van-e hasonló feltétel p-re?
Válasz: Megoldatlan! Kvadratikus reciprocitás általánosítása?
$\rightsquigarrow$ Langlands-program.

Fogalmazzuk át a problémát!

Kérdés: Általánosabb $f(x)$ esetén van-e hasonló feltétel p-re?
Válasz: Megoldatlan! Kvadratikus reciprocitás általánosítása?
$\rightsquigarrow$ Langlands-program.
Vissza az $f(x) = x^2 - d$ példához:
Kulcsészrevétel: $\left(\frac{d}{p}\right)$, mint p függvénye egy

$$\left(\frac{d}{\cdot}\right) : (\mathbb{Z}/4d\mathbb{Z})^\times \to \{\pm 1\}$$

homomorfizmus (Dirichlet-karakter).

Fogalmazzuk át a problémát!

Kérdés: Általánosabb $f(x)$ esetén van-e hasonló feltétel p-re?
Válasz: Megoldatlan! Kvadratikus reciprocitás általánosítása?
$\rightsquigarrow$ Langlands-program.
Vissza az $f(x) = x^2 - d$ példához:
Kulcsészrevétel: $\left(\frac{d}{p}\right)$, mint p függvénye egy

$$\left(\frac{d}{\cdot}\right) : (\mathbb{Z}/4d\mathbb{Z})^\times \to \{\pm 1\}$$

homomorfizmus (Dirichlet-karakter).
Mihez rendeltük ezt hozzá?

Fogalmazzuk át a problémát!

Kérdés: Általánosabb $f(x)$ esetén van-e hasonló feltétel p-re?
Válasz: Megoldatlan! Kvadratikus reciprocitás általánosítása?
$\rightsquigarrow$ Langlands-program.
Vissza az $f(x) = x^2 - d$ példához:
Kulcsészrevétel: $\left(\frac{d}{p}\right)$, mint p függvénye egy

$$\left(\frac{d}{\cdot}\right) : (\mathbb{Z}/4d\mathbb{Z})^\times \to \{\pm 1\}$$

homomorfizmus (Dirichlet-karakter).
Mihez rendeltük ezt hozzá?

A Galois-csoport egy karakteréhez!

Fogalmazzuk át a problémát!

Kérdés: Általánosabb $f(x)$ esetén van-e hasonló feltétel p-re?
Válasz: Megoldatlan! Kvadratikus reciprocitás általánosítása?
$\rightsquigarrow$ Langlands-program.
Vissza az $f(x) = x^2 - d$ példához:
Kulcsészrevétel: $\left(\frac{d}{p}\right)$, mint p függvénye egy

$$\left(\frac{d}{\cdot}\right) : (\mathbb{Z}/4d\mathbb{Z})^\times \to \{\pm 1\}$$

homomorfizmus (Dirichlet-karakter).
Mihez rendeltük ezt hozzá?

A Galois-csoport egy karakteréhez!

Milyen Galois-csoport? Milyen karakter? Polinomról volt szó...

- F: az $f(x)$ felbontási teste $\mathbb{Q}$ felett. Pl. $F = \mathbb{Q}(\sqrt{d})$.
- $\mathrm{Gal}(F/\mathbb{Q})$ a Galois-csoport. Pl. $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \cong Z_2$.
  Egyetlen nemtriviális karakter: $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \to \{\pm 1\}$.

- F: az $f(x)$ felbontási teste $\mathbb{Q}$ felett. Pl. $F = \mathbb{Q}(\sqrt{d})$.
- $\mathrm{Gal}(F/\mathbb{Q})$ a Galois-csoport. Pl. $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \cong Z_2$.
  Egyetlen nemtriviális karakter: $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \to \{\pm 1\}$.

Hogyan látszik $\mathrm{Gal}(F/\mathbb{Q})$-n $f(x)$ felbonthatósága mod p?

- F: az $f(x)$ felbontási teste $\mathbb{Q}$ felett. Pl. $F = \mathbb{Q}(\sqrt{d})$.
- $\mathrm{Gal}(F/\mathbb{Q})$ a Galois-csoport. Pl. $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \cong Z_2$.
  Egyetlen nemtriviális karakter: $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \to \{\pm 1\}$.

Hogyan látszik $\mathrm{Gal}(F/\mathbb{Q})$-n $f(x)$ felbonthatósága mod p?

- $\mathcal{O}_F = \{\beta \in F : m_\beta(x) \in \mathbb{Z}[x]\}$ az F alg. egészeinek gyűrűje.
- $(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ prímideálokra való felbontás $\mathcal{O}_F$-ben.

- F: az $f(x)$ felbontási teste $\mathbb{Q}$ felett. Pl. $F = \mathbb{Q}(\sqrt{d})$.
- $\mathrm{Gal}(F/\mathbb{Q})$ a Galois-csoport. Pl. $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \cong Z_2$.
  Egyetlen nemtriviális karakter: $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \to \{\pm 1\}$.

Hogyan látszik $\mathrm{Gal}(F/\mathbb{Q})$-n $f(x)$ felbonthatósága mod p?

- $\mathcal{O}_F = \{\beta \in F : m_\beta(x) \in \mathbb{Z}[x]\}$ az F alg. egészeinek gyűrűje.
- $(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ prímideálokra való felbontás $\mathcal{O}_F$-ben.

Pl. $\mathbb{Q}(\sqrt{d})$-ben:

- $(p) = \mathfrak{p}_1^2 \iff p \mid d \iff x^2 - d \equiv x^2 \pmod{p}$;
- $(p) = \mathfrak{p}_1\mathfrak{p}_2 \iff \left(\frac{d}{p}\right) = 1 \iff x^2 - d \equiv (x-b)(x-c) \pmod{p}$;
- $(p) = (p)$ prím $\iff \left(\frac{d}{p}\right) = -1 \iff x^2 - d$ irred. mod p.

Állítás (Ha $\mathcal{O}_F = \mathbb{Z}[\alpha]$ ($f(\alpha) = 0$), akkor)

$(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i} \iff f(x) \equiv \prod_{i=1}^{k} g_i(x)^{e_i} \pmod{p}$.

Állítás (Ha $\mathcal{O}_F = \mathbb{Z}[\alpha]$ ($f(\alpha) = 0$), akkor)

$(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i} \iff f(x) \equiv \prod_{i=1}^{k} g_i(x)^{e_i} \pmod{p}$.

- $\mathrm{Gal}(F/\mathbb{Q})$ tranzitívan hat $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$-en. Orbit-stabilizátor lemma $\Rightarrow r = |\mathrm{Gal}(F/\mathbb{Q}) : \mathrm{Gal}(F/\mathbb{Q})_{\mathfrak{p}_1}|$.

Állítás (Ha $\mathcal{O}_F = \mathbb{Z}[\alpha]$ ($f(\alpha) = 0$), akkor)

$(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i} \iff f(x) \equiv \prod_{i=1}^{k} g_i(x)^{e_i} \pmod{p}$.

- $\mathrm{Gal}(F/\mathbb{Q})$ tranzitívan hat $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$-en. Orbit-stabilizátor lemma $\Rightarrow r = |\mathrm{Gal}(F/\mathbb{Q}) : \mathrm{Gal}(F/\mathbb{Q})_{\mathfrak{p}_1}|$.
- $\mathrm{Gal}(F/\mathbb{Q})_{\mathfrak{p}_1}$ véges sok p-től eltekintve ciklikus. Kitüntetett generátor: Frob_p, melyre $\mathrm{Frob}_p(\beta) \equiv \beta^p \pmod{\mathfrak{p}_1}$. $\mathfrak{p}_1$ választása: konjugáltság.

Állítás (Ha $\mathcal{O}_F = \mathbb{Z}[\alpha]$ ($f(\alpha) = 0$), akkor)

$(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i} \iff f(x) \equiv \prod_{i=1}^{k} g_i(x)^{e_i} \pmod{p}$.

- $\mathrm{Gal}(F/\mathbb{Q})$ tranzitívan hat $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$-en. Orbit-stabilizátor lemma $\Rightarrow r = |\mathrm{Gal}(F/\mathbb{Q}) : \mathrm{Gal}(F/\mathbb{Q})_{\mathfrak{p}_1}|$.
- $\mathrm{Gal}(F/\mathbb{Q})_{\mathfrak{p}_1}$ véges sok p-től eltekintve ciklikus. Kitüntetett generátor: Frob_p, melyre $\mathrm{Frob}_p(\beta) \equiv \beta^p \pmod{\mathfrak{p}_1}$. $\mathfrak{p}_1$ választása: konjugáltság.

A konkrét példánkban: $\sqrt{d} \in \mathbb{F}_p \iff \mathrm{Frob}_p(\sqrt{d}) \equiv (\sqrt{d})^p \equiv \sqrt{d} \pmod{\mathfrak{p}_1} \iff \mathrm{Frob}_p(\sqrt{d}) = \sqrt{d} \iff \mathrm{Frob}_p$-t az 1-be viszi a $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \to \{\pm 1\}$ karakter. Itt p kivételes $\iff p \mid 4d$.

Állítás (Ha $\mathcal{O}_F = \mathbb{Z}[\alpha]$ ($f(\alpha) = 0$), akkor)

$(p) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i} \iff f(x) \equiv \prod_{i=1}^{k} g_i(x)^{e_i} \pmod{p}$.

- $\mathrm{Gal}(F/\mathbb{Q})$ tranzitívan hat $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$-en. Orbit-stabilizátor lemma $\Rightarrow r = |\mathrm{Gal}(F/\mathbb{Q}) : \mathrm{Gal}(F/\mathbb{Q})_{\mathfrak{p}_1}|$.
- $\mathrm{Gal}(F/\mathbb{Q})_{\mathfrak{p}_1}$ véges sok p-től eltekintve ciklikus. Kitüntetett generátor: Frob_p, melyre $\mathrm{Frob}_p(\beta) \equiv \beta^p \pmod{\mathfrak{p}_1}$. $\mathfrak{p}_1$ választása: konjugáltság.

A konkrét példánkban: $\sqrt{d} \in \mathbb{F}_p \iff \mathrm{Frob}_p(\sqrt{d}) \equiv (\sqrt{d})^p \equiv \sqrt{d} \pmod{\mathfrak{p}_1} \iff \mathrm{Frob}_p(\sqrt{d}) = \sqrt{d} \iff \mathrm{Frob}_p$-t az 1-be viszi a $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \to \{\pm 1\}$ karakter. Itt p kivételes $\iff p \mid 4d$. Tehát $x^2 - d$ mod p felbonthatóságának leírása a

$$\{\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \text{ karakterei}\} \to \{(\mathbb{Z}/4d\mathbb{Z})^\times \text{ karakterei}\}$$

megfeleltetésen múlik. N.B. $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\mu_{4d})$ (lásd később).

Problémák:

Problémák:

- $f(x)$-et változtatva mind F és így $\mathrm{Gal}(F/\mathbb{Q})$, mind $N = 4d$ és így $(\mathbb{Z}/N\mathbb{Z})^\times$ változik.

Problémák:

- $f(x)$-et változtatva mind F és így $\mathrm{Gal}(F/\mathbb{Q})$, mind $N = 4d$ és így $(\mathbb{Z}/N\mathbb{Z})^\times$ változik.
- $\mathrm{Gal}(F/\mathbb{Q})$ nem mindig kommutatív, ezért (1-dimenziós) karakterei nem írják le teljesen.

Problémák:

- $f(x)$-et változtatva mind F és így $\mathrm{Gal}(F/\mathbb{Q})$, mind $N = 4d$ és így $(\mathbb{Z}/N\mathbb{Z})^\times$ változik.
- $\mathrm{Gal}(F/\mathbb{Q})$ nem mindig kommutatív, ezért (1-dimenziós) karakterei nem írják le teljesen.

Lehetséges megoldások:

Problémák:

- $f(x)$-et változtatva mind F és így $\mathrm{Gal}(F/\mathbb{Q})$, mind $N = 4d$ és így $(\mathbb{Z}/N\mathbb{Z})^\times$ változik.
- $\mathrm{Gal}(F/\mathbb{Q})$ nem mindig kommutatív, ezért (1-dimenziós) karakterei nem írják le teljesen.

Lehetséges megoldások:

- Változó f és F helyett $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim_F \mathrm{Gal}(F/\mathbb{Q})$ abszolút Galois-csoport: egyetlen objektum. $\overline{\mathbb{Q}}$: az algebrai számok teste, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ pedig $\mathbb{Q}$ automorfizmuscsoportja.

Problémák:

- $f(x)$-et változtatva mind F és így $\mathrm{Gal}(F/\mathbb{Q})$, mind $N = 4d$ és így $(\mathbb{Z}/N\mathbb{Z})^\times$ változik.
- $\mathrm{Gal}(F/\mathbb{Q})$ nem mindig kommutatív, ezért (1-dimenziós) karakterei nem írják le teljesen.

Lehetséges megoldások:

- Változó f és F helyett $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim_F \mathrm{Gal}(F/\mathbb{Q})$ abszolút Galois-csoport: egyetlen objektum. $\overline{\mathbb{Q}}$: az algebrai számok teste, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ pedig $\mathbb{Q}$ automorfizmuscsoportja.
- Karakterek helyett – nem felt. 1-dimenziós – reprezentációk.

Problémák:

- $f(x)$-et változtatva mind F és így $\mathrm{Gal}(F/\mathbb{Q})$, mind $N = 4d$ és így $(\mathbb{Z}/N\mathbb{Z})^\times$ változik.
- $\mathrm{Gal}(F/\mathbb{Q})$ nem mindig kommutatív, ezért (1-dimenziós) karakterei nem írják le teljesen.

Lehetséges megoldások:

- Változó f és F helyett $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim_F \mathrm{Gal}(F/\mathbb{Q})$ abszolút Galois-csoport: egyetlen objektum. $\overline{\mathbb{Q}}$: az algebrai számok teste, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ pedig $\mathbb{Q}$ automorfizmuscsoportja.
- Karakterek helyett – nem felt. 1-dimenziós – reprezentációk.
- *Inverz limeszt* veszünk: $\hat{\mathbb{Z}}^\times := \varprojlim_N (\mathbb{Z}/N\mathbb{Z})^\times =$
  $= \{(a_N)_N \colon a_N \in (\mathbb{Z}/N\mathbb{Z})^\times, a_N \equiv a_M \pmod{M} \text{ ha } M \mid N\}$.
  Kínai maradéktétel $\Rightarrow \hat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times$, ahol $\mathbb{Z}_p = \varprojlim_r \mathbb{Z}/p^r\mathbb{Z}$ és megérkeztünk...

...a p-adikus számok(hoz)

...a p-adikus számok(hoz)

- A p-adikus abszolútérték $|\cdot|_p : \mathbb{Q} \to \mathbb{R}^{\geq 0}$, $|\frac{a}{b}p^n|_p := p^{-n}$, ha $p \nmid ab$, és $|0|_p := 0$.

...a p-adikus számok(hoz)

- A p-adikus abszolútérték $|\cdot|_p \colon \mathbb{Q} \to \mathbb{R}^{\geq 0}$, $|\frac{a}{b}p^n|_p := p^{-n}$, ha $p \nmid ab$, és $|0|_p := 0$.
- A p prím hatványai „kicsik”: $\lim_{n\to\infty} p^n = 0$.

...a p-adikus számok(hoz)

- A p-adikus abszolútérték $|\cdot|_p \colon \mathbb{Q} \to \mathbb{R}^{\geq 0}$, $|\frac{a}{b}p^n|_p := p^{-n}$, ha $p \nmid ab$, és $|0|_p := 0$.
- A p prím hatványai „kicsik”: $\lim_{n\to\infty} p^n = 0$.
- A p-adikus számok teste: $\mathbb{Q}_p := \widehat{(\mathbb{Q}, |\cdot|_p)}$ a $\mathbb{Q}$ telítése.

...a p-adikus számok(hoz)

- A p-adikus abszolútérték $|\cdot|_p \colon \mathbb{Q} \to \mathbb{R}^{\geq 0}$, $|\frac{a}{b}p^n|_p := p^{-n}$, ha $p \nmid ab$, és $|0|_p := 0$.
- A p prím hatványai „kicsik”: $\lim_{n\to\infty} p^n = 0$.
- A p-adikus számok teste: $\mathbb{Q}_p := \widehat{(\mathbb{Q}, |\cdot|_p)}$ a $\mathbb{Q}$ telítése.
- Konkrét megadásuk: $0 \neq x \in \mathbb{Q}_p$ p-adikus sorfejtése: $x = x_{-N}p^{-N} + \cdots + x_n p^n + \ldots$, ahol $x_n \in \{0, 1, \ldots, p-1\}$, $x_{-N} \neq 0 \Rightarrow |x|_p = p^N$.

...a p-adikus számok(hoz)

- A p-adikus abszolútérték $|\cdot|_p \colon \mathbb{Q} \to \mathbb{R}^{\geq 0}$, $|\frac{a}{b}p^n|_p := p^{-n}$, ha $p \nmid ab$, és $|0|_p := 0$.
- A p prím hatványai „kicsik”: $\lim_{n\to\infty} p^n = 0$.
- A p-adikus számok teste: $\mathbb{Q}_p := \widehat{(\mathbb{Q}, |\cdot|_p)}$ a $\mathbb{Q}$ telítése.
- Konkrét megadásuk: $0 \neq x \in \mathbb{Q}_p$ p-adikus sorfejtése: $x = x_{-N}p^{-N} + \cdots + x_n p^n + \ldots$, ahol $x_n \in \{0, 1, \ldots, p-1\}$, $x_{-N} \neq 0 \Rightarrow |x|_p = p^N$.
- Teljes (ultra)metrikus tér: $|x + y|_p \leq \max(|x|_p, |y|_p)$.

...a p-adikus számok(hoz)

- A p-adikus abszolútérték $|\cdot|_p\colon \mathbb{Q} \to \mathbb{R}^{\geq 0}$, $|\frac{a}{b}p^n|_p := p^{-n}$, ha $p \nmid ab$, és $|0|_p := 0$.
- A p prím hatványai „kicsik”: $\lim_{n\to\infty} p^n = 0$.
- A p-adikus számok teste: $\mathbb{Q}_p := \widehat{(\mathbb{Q}, |\cdot|_p)}$ a $\mathbb{Q}$ telítése.
- Konkrét megadásuk: $0 \neq x \in \mathbb{Q}_p$ p-adikus sorfejtése: $x = x_{-N}p^{-N} + \cdots + x_n p^n + \ldots$, ahol $x_n \in \{0, 1, \ldots, p-1\}$, $x_{-N} \neq 0 \Rightarrow |x|_p = p^N$.
- Teljes (ultra)metrikus tér: $|x + y|_p \leq \max(|x|_p, |y|_p)$.
- A zárt egységgömb $\mathbb{Z}_p := \{x \in \mathbb{Q}_p\colon |x|_p \leq 1\}$ egy részgyűrű, melyben a nyílt egységgömb $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p\colon |x|_p < 1\}$ az egyetlen maximális ideál. $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ a p elemű test, és $\mathbb{Z}_p \cong \varprojlim_r \mathbb{Z}/p^r\mathbb{Z}$.

...a p-adikus számok(hoz)

- A p-adikus abszolútérték $|\cdot|_p\colon \mathbb{Q} \to \mathbb{R}^{\geq 0}$, $|\frac{a}{b}p^n|_p := p^{-n}$, ha $p \nmid ab$, és $|0|_p := 0$.
- A p prím hatványai „kicsik”: $\lim_{n\to\infty} p^n = 0$.
- A p-adikus számok teste: $\mathbb{Q}_p := \widehat{(\mathbb{Q}, |\cdot|_p)}$ a $\mathbb{Q}$ telítése.
- Konkrét megadásuk: $0 \neq x \in \mathbb{Q}_p$ p-adikus sorfejtése: $x = x_{-N}p^{-N} + \cdots + x_n p^n + \ldots$, ahol $x_n \in \{0, 1, \ldots, p-1\}$, $x_{-N} \neq 0 \Rightarrow |x|_p = p^N$.
- Teljes (ultra)metrikus tér: $|x+y|_p \leq \max(|x|_p, |y|_p)$.
- A zárt egységgömb $\mathbb{Z}_p := \{x \in \mathbb{Q}_p\colon |x|_p \leq 1\}$ egy részgyűrű, melyben a nyílt egységgömb $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p\colon |x|_p < 1\}$ az egyetlen maximális ideál. $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ a p elemű test, és $\mathbb{Z}_p \cong \varprojlim_r \mathbb{Z}/p^r\mathbb{Z}$.
- $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p} \rightsquigarrow \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

Tétel (Kronecker-Weber) (1853, 1886, 1896 Hilbert)

$\mathbb{Q}$ maximális Abel-féle bővítése $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\mu_\infty) = \bigcup_N \mathbb{Q}(\mu_N)$, ahol $\mu_N = \{\varepsilon \in \mathbb{C} \colon \varepsilon^N = 1\}$.

Tétel (Kronecker-Weber) (1853, 1886, 1896 Hilbert)

$\mathbb{Q}$ maximális Abel-féle bővítése $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\mu_\infty) = \bigcup_N \mathbb{Q}(\mu_N)$, ahol $\mu_N = \{\varepsilon \in \mathbb{C} : \varepsilon^N = 1\}$.

$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) = \varprojlim_N \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \cong \varprojlim_N (\mathbb{Z}/N\mathbb{Z})^\times = \hat{\mathbb{Z}}^\times$ – izomorf csoportok karakterei megegyeznek.

Tétel (Kronecker-Weber) (1853, 1886, 1896 Hilbert)

$\mathbb{Q}$ maximális Abel-féle bővítése $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\mu_\infty) = \bigcup_N \mathbb{Q}(\mu_N)$, ahol $\mu_N = \{\varepsilon \in \mathbb{C} : \varepsilon^N = 1\}$.

$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) = \varprojlim_N \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \cong \varprojlim_N (\mathbb{Z}/N\mathbb{Z})^\times = \hat{\mathbb{Z}}^\times$ – izomorf csoportok karakterei megegyeznek.
$\hat{\mathbb{Z}}^\times = \mathrm{GL}_1(\hat{\mathbb{Z}})$ kommutatív $\Rightarrow \nexists$ többdim. irred. reprezentációk.
Langlands ($\sim$1967):

$$\{\text{„}n-\text{dim Galois-reprezentációk''}\} \longleftrightarrow \{\text{„}\mathrm{GL}_n \text{ repr.-k.''}\}?$$

Tétel (Kronecker-Weber) (1853, 1886, 1896 Hilbert)

$\mathbb{Q}$ maximális Abel-féle bővítése $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\mu_\infty) = \bigcup_N \mathbb{Q}(\mu_N)$, ahol $\mu_N = \{\varepsilon \in \mathbb{C} : \varepsilon^N = 1\}$.

$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) = \varprojlim_N \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \cong \varprojlim_N (\mathbb{Z}/N\mathbb{Z})^\times = \hat{\mathbb{Z}}^\times$ – izomorf csoportok karakterei megegyeznek.
$\hat{\mathbb{Z}}^\times = \mathrm{GL}_1(\hat{\mathbb{Z}})$ kommutatív $\Rightarrow \nexists$ többdim. irred. reprezentációk.
Langlands ($\sim$1967):

$$\{\text{„}n-\text{dim Galois-reprezentációk''}\} \longleftrightarrow \{\text{„}\mathrm{GL}_n \text{ repr.-k.''}\}?$$

Megjegyzés: $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. Rögzítve a p-t („lokálisan p-nél'') elég $\mathrm{GL}_n(\mathbb{Z}_p)$-t vizsgálni.

Tétel (Kronecker-Weber) (1853, 1886, 1896 Hilbert)

$\mathbb{Q}$ maximális Abel-féle bővítése $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\mu_\infty) = \bigcup_N \mathbb{Q}(\mu_N)$, ahol $\mu_N = \{\varepsilon \in \mathbb{C} : \varepsilon^N = 1\}$.

$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) = \varprojlim_N \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \cong \varprojlim_N (\mathbb{Z}/N\mathbb{Z})^\times = \hat{\mathbb{Z}}^\times$ – izomorf csoportok karakterei megegyeznek.
$\hat{\mathbb{Z}}^\times = \mathrm{GL}_1(\hat{\mathbb{Z}})$ kommutatív $\Rightarrow \nexists$ többdim. irred. reprezentációk.
Langlands (∼1967):

$$\{\text{„}n-\text{dim Galois-reprezentációk''}\} \longleftrightarrow \{\text{„}\mathrm{GL}_n \text{ repr.-k.''}\}?$$

Megjegyzés: $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. Rögzítve a p-t („lokálisan p-nél'') elég $\mathrm{GL}_n(\mathbb{Z}_p)$-t vizsgálni.
$\rightsquigarrow$ Galois-oldalon: $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ helyett $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ reprezentációi.
Megengedjük $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ olyan reprezentációit is, amiknek a képe nem véges $\Rightarrow$ $\mathrm{GL}_n(\mathbb{Z}_p)$ (kompakt) helyett $\mathrm{GL}_n(\mathbb{Q}_p)$ (nem kompakt).

Az általános lineáris csoport

$\mathrm{GL}_n(\mathbb{Q}_p) := \{A \in \mathbb{Q}_p^{n\times n} : \det A \neq 0\}$ csoport.

Definíció

$G := \mathrm{GL}_n(\mathbb{Q}_p)$ reprezentációja: (V, π) rendezett pár, V: vektortér (valamilyen K test felett); $\pi : \mathrm{GL}_n(\mathbb{Q}_p) \to \mathrm{GL}(V)$ csoporthomomorfizmus.

Az általános lineáris csoport

$\mathrm{GL}_n(\mathbb{Q}_p) := \{A \in \mathbb{Q}_p^{n\times n} : \det A \neq 0\}$ csoport.

Definíció

$G := \mathrm{GL}_n(\mathbb{Q}_p)$ reprezentációja: (V, π) rendezett pár, V: vektortér (valamilyen K test felett); $\pi : \mathrm{GL}_n(\mathbb{Q}_p) \to \mathrm{GL}(V)$ csoporthomomorfizmus.

G egy topologikus csoport $\Rightarrow$ folytonos reprezentációk: V egy topologikus vektortér, és

$$G \times V \to V; \qquad (g, v) \mapsto \pi(g)v \in V$$

folytonos.

Az általános lineáris csoport

$\mathrm{GL}_n(\mathbb{Q}_p) := \{A \in \mathbb{Q}_p^{n\times n} : \det A \neq 0\}$ csoport.

Definíció

$G := \mathrm{GL}_n(\mathbb{Q}_p)$ reprezentációja: (V, π) rendezett pár, V: vektortér (valamilyen K test felett); $\pi : \mathrm{GL}_n(\mathbb{Q}_p) \to \mathrm{GL}(V)$ csoporthomomorfizmus.

G egy topologikus csoport $\Rightarrow$ folytonos reprezentációk: V egy topologikus vektortér, és

$$G \times V \to V; \qquad (g, v) \mapsto \pi(g)v \in V$$

folytonos.

Példa (tautologikus reprezentáció)

$V = \mathbb{Q}_p^n$, $\pi : \mathrm{GL}_n(\mathbb{Q}_p) \to \mathrm{GL}_n(\mathbb{Q}_p)$ az identitás.

Milyen reprezentációk vannak?

Milyen reprezentációk vannak?

- Algebrai reprezentációk (kapcsolat: Lie-algebra reprezentációk)

Milyen reprezentációk vannak?

- Algebrai reprezentációk (kapcsolat: Lie-algebra reprezentációk)

Példa: Algebrai reprezentációk

$V = \{\mathbb{Q}_p$ fölötti homogén k-adfokú n-változós polinomok$\}$,
$\mathrm{GL}_n(\mathbb{Q}_p)$ hat az $(x_1, \ldots, x_n)$ változókon, mint oszlopvektorokon.

Milyen reprezentációk vannak?

- Algebrai reprezentációk (kapcsolat: Lie-algebra reprezentációk)

Példa: Algebrai reprezentációk

$V = \{\mathbb{Q}_p$ fölötti homogén k-adfokú n-változós polinomok$\}$,
$\mathrm{GL}_n(\mathbb{Q}_p)$ hat az $(x_1, \ldots, x_n)$ változókon, mint oszlopvektorokon.

Itt $K = \mathbb{Q}_p$ és π egy racionális törtfüggvénye a koordinátáknak $\mathrm{GL}_n(\mathbb{Q}_p)$-n. Spec. eset: tautologikus reprezentáció.

Milyen reprezentációk vannak?

- Algebrai reprezentációk (kapcsolat: Lie-algebra reprezentációk)

Példa: Algebrai reprezentációk

$V = \{\mathbb{Q}_p$ fölötti homogén k-adfokú n-változós polinomok$\}$,
$\mathrm{GL}_n(\mathbb{Q}_p)$ hat az $(x_1, \ldots, x_n)$ változókon, mint oszlopvektorokon.

Itt $K = \mathbb{Q}_p$ és π egy racionális törtfüggvénye a koordinátáknak $\mathrm{GL}_n(\mathbb{Q}_p)$-n. Spec. eset: tautologikus reprezentáció.

- Sima reprezentációk – (klasszikus) Langlands-program

Milyen reprezentációk vannak?

- Algebrai reprezentációk (kapcsolat: Lie-algebra reprezentációk)

Példa: Algebrai reprezentációk

$V = \{\mathbb{Q}_p$ fölötti homogén k-adfokú n-változós polinomok$\}$,
$\mathrm{GL}_n(\mathbb{Q}_p)$ hat az $(x_1, \ldots, x_n)$ változókon, mint oszlopvektorokon.

Itt $K = \mathbb{Q}_p$ és π egy racionális törtfüggvénye a koordinátáknak $\mathrm{GL}_n(\mathbb{Q}_p)$-n. Spec. eset: tautologikus reprezentáció.

- Sima reprezentációk – (klasszikus) Langlands-program

V általában végtelen dimenziós, viszont a K test topológiája mégsem játszik szerepet:

Milyen reprezentációk vannak?

- Algebrai reprezentációk (kapcsolat: Lie-algebra reprezentációk)

Példa: Algebrai reprezentációk

$V = \{\mathbb{Q}_p$ fölötti homogén k-adfokú n-változós polinomok$\}$,
$\mathrm{GL}_n(\mathbb{Q}_p)$ hat az $(x_1, \ldots, x_n)$ változókon, mint oszlopvektorokon.

Itt $K = \mathbb{Q}_p$ és π egy racionális törtfüggvénye a koordinátáknak $\mathrm{GL}_n(\mathbb{Q}_p)$-n. Spec. eset: tautologikus reprezentáció.

- Sima reprezentációk – (klasszikus) Langlands-program

V általában végtelen dimenziós, viszont a K test topológiája mégsem játszik szerepet:

Definíció

A (V, π) egy sima reprezentációja $\mathrm{GL}_n(\mathbb{Q}_p)$-nek, ha folytonos úgy, hogy V-t a diszkrét topológiával látjuk el.

Sima reprezentációk

Mit jelent ez pontosan?

Sima reprezentációk

Mit jelent ez pontosan?

- Diszkrét topológia: minden egyelemű $\{v\} \subset V$ nyílt.

Sima reprezentációk

Mit jelent ez pontosan?

- Diszkrét topológia: minden egyelemű $\{v\} \subset V$ nyílt.
- Folytonosság: nyílt őse nyílt, azaz ha $\pi(g)w = v$, akkor $\exists$ $g \in U \subseteq \mathrm{GL}_n(\mathbb{Q})$ nyílt környezet, melyre $\pi(h)w = v$ minden $h \in U$-ra.

Sima reprezentációk

Mit jelent ez pontosan?

- Diszkrét topológia: minden egyelemű $\{v\} \subset V$ nyílt.
- Folytonosság: nyílt őse nyílt, azaz ha $\pi(g)w = v$, akkor $\exists$ $g \in U \subseteq \mathrm{GL}_n(\mathbb{Q})$ nyílt környezet, melyre $\pi(h)w = v$ minden $h \in U$-ra.

Hogy néz ki g egy U környezete?

Sima reprezentációk

Mit jelent ez pontosan?

- Diszkrét topológia: minden egyelemű $\{v\} \subset V$ nyílt.
- Folytonosság: nyílt őse nyílt, azaz ha $\pi(g)w = v$, akkor $\exists$ $g \in U \subseteq \mathrm{GL}_n(\mathbb{Q})$ nyílt környezet, melyre $\pi(h)w = v$ minden $h \in U$-ra.

Hogy néz ki g egy U környezete?
Például $U = \{h \in \mathrm{GL}_n(\mathbb{Q}_p) \colon g^{-1}h \equiv I \pmod{p^k}\}$, ahol I az egységmátrix. Ez egy nyílt részcsoport egy mellékosztálya és $\pi(h)w = v = \pi(g)w \iff \pi(g^{-1}h)w = w$.

Sima reprezentációk

Mit jelent ez pontosan?

- Diszkrét topológia: minden egyelemű $\{v\} \subset V$ nyílt.
- Folytonosság: nyílt őse nyílt, azaz ha $\pi(g)w = v$, akkor $\exists$ $g \in U \subseteq \mathrm{GL}_n(\mathbb{Q})$ nyílt környezet, melyre $\pi(h)w = v$ minden $h \in U$-ra.

Hogy néz ki g egy U környezete?
Például $U = \{h \in \mathrm{GL}_n(\mathbb{Q}_p) \colon g^{-1}h \equiv I \pmod{p^k}\}$, ahol I az egységmátrix. Ez egy nyílt részcsoport egy mellékosztálya és $\pi(h)w = v = \pi(g)w \iff \pi(g^{-1}h)w = w$.

Tétel

Tehát egy (V, π) reprezentáció pontosan akkor sima, ha minden $v \in V$ vektor stabilizátora G-ben egy nyílt részcsoport.

Példa sima reprezentációra

K test a diszkrét topológiával, $H \leq G$ zárt részcsoport (pl. a felsőháromszög-mátrixok részcsoportja), és $V = C_c(G/H, K)$ (lokálisan konstans kompakt tartójú függvények).
$(\pi(g)f)(g_0H) := f(g^{-1}g_0H)$ ha $f \in V$ és $g, g_0 \in G$.

Példa sima reprezentációra

K test a diszkrét topológiával, $H \leq G$ zárt részcsoport (pl. a felsőháromszög-mátrixok részcsoportja), és $V = C_c(G/H, K)$ (lokálisan konstans kompakt tartójú függvények).
$(\pi(g)f)(g_0H) := f(g^{-1}g_0H)$ ha $f \in V$ és $g, g_0 \in G$.

A fenti példa nem más, mint H triviális reprezentációjának az indukált reprezentációja: $\mathrm{ind}_H^G(1_H)$.

Példa sima reprezentációra

K test a diszkrét topológiával, $H \leq G$ zárt részcsoport (pl. a felsőháromszög-mátrixok részcsoportja), és $V = C_c(G/H, K)$ (lokálisan konstans kompakt tartójú függvények).
$(\pi(g)f)(g_0H) := f(g^{-1}g_0H)$ ha $f \in V$ és $g, g_0 \in G$.

A fenti példa nem más, mint H triviális reprezentációjának az indukált reprezentációja: $\mathrm{ind}_H^G(1_H)$.

Tétel (Harris és Taylor 2001, Henniart 2000)

Ha $\ell \neq p$, akkor létezik egy kölcsönösen egyértelmű természetes megfeleltetés:

$$\left\{\begin{array}{c}\text{„}\mathrm{GL}_n(\mathbb{Q}_p)\text{ irreducibilis}\\ \text{sima reprezentációi''}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\text{„}\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)\ n\text{-dim.}\\ \text{reprezentációi }\overline{\mathbb{Q}_\ell}\text{ felett''}\end{array}\right\}.$$

Idézőjelek oka az előző tételben:

- $\mathrm{GL}_n(\mathbb{Q}_p)$ oldalán algebrailag zárt, 0-karakterisztikájú testek (pl. $\overline{\mathbb{Q}_\ell}$ vagy $\mathbb{C}$) feletti reprezentációk kellenek

Idézőjelek oka az előző tételben:

- $\mathrm{GL}_n(\mathbb{Q}_p)$ oldalán algebrailag zárt, 0-karakterisztikájú testek (pl. $\overline{\mathbb{Q}_\ell}$ vagy $\mathbb{C}$) feletti reprezentációk kellenek
- Kell egy végességi feltétel a sima reprezentációkra: (V, π) *megengedhető*, ha minden $H \leq G$ kompakt nyílt részcsoportra $\dim_K V^H < \infty$.

Idézőjelek oka az előző tételben:

- $\mathrm{GL}_n(\mathbb{Q}_p)$ oldalán algebrailag zárt, 0-karakterisztikájú testek (pl. $\overline{\mathbb{Q}_\ell}$ vagy $\mathbb{C}$) feletti reprezentációk kellenek
- Kell egy végességi feltétel a sima reprezentációkra: (V, π) *megengedhető*, ha minden $H \leq G$ kompakt nyílt részcsoportra $\dim_K V^H < \infty$.
- Nem az egész $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, hanem egy sűrű részcsoport

$$W_{\mathbb{Q}_p} = \{g \in \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \mid \exists n \in \mathbb{Z} \forall x \in \overline{\mathbb{Z}_p}\colon g(x) \equiv x^{p^n} \pmod{\mathfrak{p}}\}$$

reprezentációit kell tekinteni.

Idézőjelek oka az előző tételben:

- $\mathrm{GL}_n(\mathbb{Q}_p)$ oldalán algebrailag zárt, 0-karakterisztikájú testek (pl. $\overline{\mathbb{Q}_\ell}$ vagy $\mathbb{C}$) feletti reprezentációk kellenek
- Kell egy végességi feltétel a sima reprezentációkra: (V, π) *megengedhető*, ha minden $H \leq G$ kompakt nyílt részcsoportra $\dim_K V^H < \infty$.
- Nem az egész $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, hanem egy sűrű részcsoport

$$W_{\mathbb{Q}_p} = \{g \in \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \mid \exists n \in \mathbb{Z} \forall x \in \overline{\mathbb{Z}_p}\colon g(x) \equiv x^{p^n} \pmod{\mathfrak{p}}\}$$

reprezentációit kell tekinteni.

Mit jelent az, hogy „természetes megfeleltetés”?

Idézőjelek oka az előző tételben:

- $\mathrm{GL}_n(\mathbb{Q}_p)$ oldalán algebrailag zárt, 0-karakterisztikájú testek (pl. $\overline{\mathbb{Q}_\ell}$ vagy $\mathbb{C}$) feletti reprezentációk kellenek
- Kell egy végességi feltétel a sima reprezentációkra: (V, π) *megengedhető*, ha minden $H \leq G$ kompakt nyílt részcsoportra $\dim_K V^H < \infty$.
- Nem az egész $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, hanem egy sűrű részcsoport

$$W_{\mathbb{Q}_p} = \{g \in \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \mid \exists n \in \mathbb{Z} \forall x \in \overline{\mathbb{Z}_p}\colon g(x) \equiv x^{p^n} \pmod{\mathfrak{p}}\}$$

reprezentációit kell tekinteni.

Mit jelent az, hogy „természetes megfeleltetés”?

- L-függvények (és ε-faktorok) megegyeznek a két oldalon.
- A megfeleltetés megjelenik bizonyos geometriai objektumok (Shimura-varietások) kohomológiájában.

Idézőjelek oka az előző tételben:

- $\mathrm{GL}_n(\mathbb{Q}_p)$ oldalán algebrailag zárt, 0-karakterisztikájú testek (pl. $\overline{\mathbb{Q}_\ell}$ vagy $\mathbb{C}$) feletti reprezentációk kellenek
- Kell egy végességi feltétel a sima reprezentációkra: (V, π) *megengedhető*, ha minden $H \leq G$ kompakt nyílt részcsoportra $\dim_K V^H < \infty$.
- Nem az egész $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, hanem egy sűrű részcsoport

$$W_{\mathbb{Q}_p} = \{g \in \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \mid \exists n \in \mathbb{Z} \forall x \in \overline{\mathbb{Z}_p}\colon g(x) \equiv x^{p^n} \pmod{\mathfrak{p}}\}$$

reprezentációit kell tekinteni.

Mit jelent az, hogy „természetes megfeleltetés”?

- L-függvények (és ε-faktorok) megegyeznek a két oldalon.
- A megfeleltetés megjelenik bizonyos geometriai objektumok (Shimura-varietások) kohomológiájában.

A tétel igaz $\mathbb{Q}_p$ helyett $F/\mathbb{Q}_p$ véges bővítésre is. Ez az ún. *lokális Langlands-megfeleltetés*.

Kérdés: Mit lehet mondani az eredeti problémáról, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ reprezentációiról?

Kérdés: Mit lehet mondani az eredeti problémáról, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ reprezentációiról? Nem sokat...

Kérdés: Mit lehet mondani az eredeti problémáról, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ reprezentációiról? Nem sokat...

Tétel (Wiles; Taylor és Wiles 1995; Breuil, Conrad, Diamond és Taylor 2001),

Minden $\mathbb{Q}$ feletti elliptikus görbe moduláris. ($\Rightarrow$ Fermat-sejtés.)

Kérdés: Mit lehet mondani az eredeti problémáról, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ reprezentációiról? Nem sokat...

Tétel (Wiles; Taylor és Wiles 1995; Breuil, Conrad, Diamond és Taylor 2001),

Minden $\mathbb{Q}$ feletti elliptikus görbe moduláris. ($\Rightarrow$ Fermat-sejtés.)

E elliptikus görbéhez ℓ-adikus Galois-reprezentáció ($\ell \neq p$ prím): $V_\ell(E) := \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \varprojlim E[\ell^n]$. $\dim_{\mathbb{Q}_\ell} V_\ell(E) = 2$. Invariánsok: $a_p(E) := \mathrm{Tr}(\mathrm{Frob}_p \mid V_\ell(E)) \in \mathbb{Z} \subset \mathbb{Z}_\ell$.
Modularitás (L-üggvények egyezése): $\exists f = \sum_{n=0}^{\infty} a_n(f) q^n$ moduláris forma, melyre $a_p(f) = a_p(E)$ ($\forall p$-re).

Kérdés: Mit lehet mondani az eredeti problémáról, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ reprezentációiról? Nem sokat...

Tétel (Wiles; Taylor és Wiles 1995; Breuil, Conrad, Diamond és Taylor 2001),

Minden $\mathbb{Q}$ feletti elliptikus görbe moduláris. ($\Rightarrow$ Fermat-sejtés.)

E elliptikus görbéhez ℓ-adikus Galois-reprezentáció ($\ell \neq p$ prím): $V_\ell(E) := \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \varprojlim E[\ell^n]$. $\dim_{\mathbb{Q}_\ell} V_\ell(E) = 2$. Invariánsok: $a_p(E) := \mathrm{Tr}(\mathrm{Frob}_p \mid V_\ell(E)) \in \mathbb{Z} \subset \mathbb{Z}_\ell$.
Modularitás (L-üggvények egyezése): $\exists f = \sum_{n=0}^{\infty} a_n(f) q^n$ moduláris forma, melyre $a_p(f) = a_p(E)$ ($\forall p$-re).
Stratégia:

- Modulo ℓ megfeleltetés: olyan f moduláris forma kell, amire $a_p(f) \equiv a_p(E) \pmod{\ell}$.

Kérdés: Mit lehet mondani az eredeti problémáról, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ reprezentációiról? Nem sokat...

Tétel (Wiles; Taylor és Wiles 1995; Breuil, Conrad, Diamond és Taylor 2001),

Minden $\mathbb{Q}$ feletti elliptikus görbe moduláris. ($\Rightarrow$ Fermat-sejtés.)

E elliptikus görbéhez ℓ-adikus Galois-reprezentáció ($\ell \neq p$ prím): $V_\ell(E) := \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \varprojlim E[\ell^n]$. $\dim_{\mathbb{Q}_\ell} V_\ell(E) = 2$. Invariánsok: $a_p(E) := \mathrm{Tr}(\mathrm{Frob}_p \mid V_\ell(E)) \in \mathbb{Z} \subset \mathbb{Z}_\ell$.
Modularitás (L-üggvények egyezése): $\exists f = \sum_{n=0}^{\infty} a_n(f) q^n$ moduláris forma, melyre $a_p(f) = a_p(E)$ ($\forall p$-re).
Stratégia:

- Modulo ℓ megfeleltetés: olyan f moduláris forma kell, amire $a_p(f) \equiv a_p(E) \pmod{\ell}$.
- Próbáljuk meg a Galois -reprezentációt és a moduláris formát is egyszerre „felemelni” 0-karakterisztikába.

Tétel (Serre-sejtés 1967, Khare és Wintenberger 2008)

A $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ minden irreducibilis $\dim_{\mathbb{F}_{\ell^r}} V = 2$ páratlan (komplex konjugálás determinánsa -1) reprezentációjához $\exists\, f$ moduláris forma, melyre $a_p(f) \equiv \mathrm{Tr}(\mathrm{Frob}_p \mid V) \pmod{\ell}$.

Tétel (Serre-sejtés 1967, Khare és Wintenberger 2008)

A $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ minden irreducibilis $\dim_{\mathbb{F}_{\ell^r}} V = 2$ páratlan (komplex konjugálás determinánsa -1) reprezentációjához $\exists\, f$ moduláris forma, melyre $a_p(f) \equiv \mathrm{Tr}(\mathrm{Frob}_p \mid V) \pmod{\ell}$.

Megjegyzés: A megfordítás Deligne (1971) tétele.

Tétel (Serre-sejtés 1967, Khare és Wintenberger 2008)

A $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ minden irreducibilis $\dim_{\mathbb{F}_{\ell^r}} V = 2$ páratlan (komplex konjugálás determinánsa -1) reprezentációjához $\exists\, f$ moduláris forma, melyre $a_p(f) \equiv \mathrm{Tr}(\mathrm{Frob}_p \mid V) \pmod{\ell}$.

Megjegyzés: A megfordítás Deligne (1971) tétele.
„Felemelés” 0-karakterisztikába: mely objektumoknak van az adott modulo ℓ redukciójuk (mindkét oldalon)? Majd ezt a két halmazt megfeleltetni egymásnak.

Tétel (Serre-sejtés 1967, Khare és Wintenberger 2008)

A $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ minden irreducibilis $\dim_{\mathbb{F}_{\ell^r}} V = 2$ páratlan (komplex konjugálás determinánsa -1) reprezentációjához $\exists\, f$ moduláris forma, melyre $a_p(f) \equiv \mathrm{Tr}(\mathrm{Frob}_p \mid V) \pmod{\ell}$.

Megjegyzés: A megfordítás Deligne (1971) tétele.
„Felemelés” 0-karakterisztikába: mely objektumoknak van az adott modulo ℓ redukciójuk (mindkét oldalon)? Majd ezt a két halmazt megfeleltetni egymásnak.
Különböző lokális feltételek: Szükség van az $\ell = p$ esetre is!

Tétel (Serre-sejtés 1967, Khare és Wintenberger 2008)

A $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ minden irreducibilis $\dim_{\mathbb{F}_{\ell^r}} V = 2$ páratlan (komplex konjugálás determinánsa -1) reprezentációjához $\exists\, f$ moduláris forma, melyre $a_p(f) \equiv \mathrm{Tr}(\mathrm{Frob}_p \mid V) \pmod{\ell}$.

Megjegyzés: A megfordítás Deligne (1971) tétele.
„Felemelés" 0-karakterisztikába: mely objektumoknak van az adott modulo ℓ redukciójuk (mindkét oldalon)? Majd ezt a két halmazt megfeleltetni egymásnak.
Különböző lokális feltételek: Szükség van az $\ell = p$ esetre is!
Modulo p és a p-adikus Langlands-program (Breuil 2000-es évek):

$$\left\{ \begin{array}{c} \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \text{ } n-\text{dim-s } \mathbb{F}_{p^r} \\ (\text{ill. } K/\mathbb{Q}_p \text{ véges}) \text{ reprezentációi} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \mathrm{GL}_n(\mathbb{Q}_p) \text{ } \mathbb{F}_{p^r} \text{ (ill. } K) \\ \text{feletti reprezentációi} \end{array} \right\}?$$

Topológiai feltételek $\mathrm{GL}_n(\mathbb{Q}_p)$ modulo p ill. p-adikus repr.-ira:

Topológiai feltételek $\mathrm{GL}_n(\mathbb{Q}_p)$ modulo p ill. p-adikus repr.-ira:

- mod p: sima reprezentációk

$K/\mathbb{Q}_p$ véges felett: sima reprezentációk $\rightsquigarrow \mathbb{C}$ feletti sima reprezentációk... Két különböző megközelítés:

Topológiai feltételek $\mathrm{GL}_n(\mathbb{Q}_p)$ modulo p ill. p-adikus repr.-ira:

- mod p: sima reprezentációk

$K/\mathbb{Q}_p$ véges felett: sima reprezentációk $\rightsquigarrow$ $\mathbb{C}$ feletti sima reprezentációk... Két különböző megközelítés:

- Folytonos reprezentációk p-adikus Banach-tereken.

Topológiai feltételek $\mathrm{GL}_n(\mathbb{Q}_p)$ modulo p ill. p-adikus repr.-ira:

- mod p: sima reprezentációk

$K/\mathbb{Q}_p$ véges felett: sima reprezentációk $\rightsquigarrow \mathbb{C}$ feletti sima reprezentációk... Két különböző megközelítés:

- Folytonos reprezentációk p-adikus Banach-tereken.
- Lokálisan analitikus reprezentációk lokálisan konvex vektortereken.

Topológiai feltételek $\mathrm{GL}_n(\mathbb{Q}_p)$ modulo p ill. p-adikus repr.-ira:

- mod p: sima reprezentációk

$K/\mathbb{Q}_p$ véges felett: sima reprezentációk $\rightsquigarrow \mathbb{C}$ feletti sima reprezentációk... Két különböző megközelítés:

- Folytonos reprezentációk p-adikus Banach-tereken.
- Lokálisan analitikus reprezentációk lokálisan konvex vektortereken.

Definíció

$\mathrm{GL}_n(\mathbb{Q}_p)$ egy K feletti Banach-tér reprezentációja: (V, π) pár; V egy K feletti vektortér, $\|\cdot\|: V \to \mathbb{R}^{\geq 0}$ norma, amire nézve teljes, és $\pi: \mathrm{GL}_n(\mathbb{Q}_p) \to \mathrm{GL}(V)$ folytonos.

Topológiai feltételek $\mathrm{GL}_n(\mathbb{Q}_p)$ modulo p ill. p-adikus repr.-ira:

- mod p: sima reprezentációk

$K/\mathbb{Q}_p$ véges felett: sima reprezentációk $\rightsquigarrow$ $\mathbb{C}$ feletti sima reprezentációk... Két különböző megközelítés:

- Folytonos reprezentációk p-adikus Banach-tereken.
- Lokálisan analitikus reprezentációk lokálisan konvex vektortereken.

Definíció

$\mathrm{GL}_n(\mathbb{Q}_p)$ egy K feletti Banach-tér reprezentációja: (V, π) pár; V egy K feletti vektortér, $\|\cdot\|: V \to \mathbb{R}^{\geq 0}$ norma, amire nézve teljes, és $\pi: \mathrm{GL}_n(\mathbb{Q}_p) \to \mathrm{GL}(V)$ folytonos.

Példa Banach-tér reprezentációra

$B \leq \mathrm{GL}_n(\mathbb{Q}_p)$: felsőháromszög-mátrixok részcsoportja.
$V = \{f: G/B \to \mathbb{Q}_p \text{ folytonos}\}$ a sup-normával (G/B kompakt).

Tétel (Colmez 2008, Breuil, Berger, Paškunas, Emerton, Kisin)

Létezik egy természetes megfeleltetés

$$\left\{\begin{array}{c}\text{„}\mathrm{GL}_2(\mathbb{Q}_p)\text{ irreducibilis }p\text{-adikus}\\ \text{Banach-tér reprezentációi''}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\text{„}\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)\text{ 2-dim.}\\ \text{reprezentációi }\overline{\mathbb{Q}_p}\text{ felett''}\end{array}\right\}.$$

Tétel (Colmez 2008, Breuil, Berger, Paškunas, Emerton, Kisin)

Létezik egy természetes megfeleltetés

$$\left\{\begin{array}{c}\text{„}\mathrm{GL}_2(\mathbb{Q}_p)\text{ irreducibilis }p\text{-adikus}\\ \text{Banach-tér reprezentációi''}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\text{„}\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)\text{ 2-dim.}\\ \text{reprezentációi }\overline{\mathbb{Q}_p}\text{ felett''}\end{array}\right\}.$$

Igaz p-adikus helyett modulo p együtthatókra is. Általánosítás $\mathrm{GL}_n(\mathbb{Q}_p)$-re: teljesen megoldatlan, ha $n > 2$. Sőt, $F/\mathbb{Q}_p$ véges bővítés esetén $\mathrm{GL}_2(F)$-re is! Eszközök:

Tétel (Colmez 2008, Breuil, Berger, Paškunas, Emerton, Kisin)

Létezik egy természetes megfeleltetés

$$\left\{\begin{array}{c}\text{„}\mathrm{GL}_2(\mathbb{Q}_p)\text{ irreducibilis }p\text{-adikus}\\ \text{Banach-tér reprezentációi''}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\text{„}\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)\text{ 2-dim.}\\ \text{reprezentációi }\overline{\mathbb{Q}_p}\text{ felett''}\end{array}\right\}.$$

Igaz p-adikus helyett modulo p együtthatókra is. Általánosítás $\mathrm{GL}_n(\mathbb{Q}_p)$-re: teljesen megoldatlan, ha $n > 2$. Sőt, $F/\mathbb{Q}_p$ véges bővítés esetén $\mathrm{GL}_2(F)$-re is! Eszközök:

- Mod p: V megengedhető $\iff$ $|V^{\mathrm{GL}_n(\mathbb{Z}_p)}| < \infty$. Áttérve a duálisra $\iff$ $|V^*_{\mathrm{GL}_n(\mathbb{Z}_p)}| < \infty$. V diszkrét $\Rightarrow$ V^* kompakt. Nakayama lemma $\Rightarrow$ V^* végesen generált modulus $\mathbb{F}_p[[\mathrm{GL}_n(\mathbb{Z}_p)]] = \varprojlim_k \mathbb{F}_p[\mathrm{GL}_n(\mathbb{Z}/p^n\mathbb{Z})]$ felett.

Tétel (Colmez 2008, Breuil, Berger, Paškunas, Emerton, Kisin)

Létezik egy természetes megfeleltetés

$$\left\{\begin{array}{c}\text{„}\mathrm{GL}_2(\mathbb{Q}_p)\text{ irreducibilis }p\text{-adikus}\\ \text{Banach-tér reprezentációi''}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\text{„}\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)\text{ 2-dim.}\\ \text{reprezentációi }\overline{\mathbb{Q}_p}\text{ felett''}\end{array}\right\}.$$

Igaz p-adikus helyett modulo p együtthatókra is. Általánosítás $\mathrm{GL}_n(\mathbb{Q}_p)$-re: teljesen megoldatlan, ha $n > 2$. Sőt, $F/\mathbb{Q}_p$ véges bővítés esetén $\mathrm{GL}_2(F)$-re is! Eszközök:

- Mod p: V megengedhető $\iff |V^{\mathrm{GL}_n(\mathbb{Z}_p)}| < \infty$. Áttérve a duálisra $\iff |V^*_{\mathrm{GL}_n(\mathbb{Z}_p)}| < \infty$. V diszkrét $\Rightarrow V^*$ kompakt. Nakayama lemma $\Rightarrow V^*$ végesen generált modulus $\mathbb{F}_p[[\mathrm{GL}_n(\mathbb{Z}_p)]] = \varprojlim_k \mathbb{F}_p[\mathrm{GL}_n(\mathbb{Z}/p^n\mathbb{Z})]$ felett.
- *Megengedhető* Banach-tér reprezentáció: $V^* = \mathrm{Hom}^{ct}_K(V, K)$ végesen generált modulus $K \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[\mathrm{GL}_n(\mathbb{Z}_p)]]$ felett.

Tétel (Colmez 2008, Breuil, Berger, Paškunas, Emerton, Kisin)

Létezik egy természetes megfeleltetés

$$\left\{\begin{array}{c}\text{„}\mathrm{GL}_2(\mathbb{Q}_p)\text{ irreducibilis }p\text{-adikus}\\ \text{Banach-tér reprezentációi''}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\text{„}\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)\text{ 2-dim.}\\ \text{reprezentációi }\overline{\mathbb{Q}_p}\text{ felett''}\end{array}\right\}.$$

Igaz p-adikus helyett modulo p együtthatókra is. Általánosítás $\mathrm{GL}_n(\mathbb{Q}_p)$-re: teljesen megoldatlan, ha $n > 2$. Sőt, $F/\mathbb{Q}_p$ véges bővítés esetén $\mathrm{GL}_2(F)$-re is! Eszközök:

- Mod p: V megengedhető $\iff |V^{\mathrm{GL}_n(\mathbb{Z}_p)}| < \infty$. Áttérve a duálisra $\iff |V^*_{\mathrm{GL}_n(\mathbb{Z}_p)}| < \infty$. V diszkrét $\Rightarrow V^*$ kompakt. Nakayama lemma $\Rightarrow V^*$ végesen generált modulus $\mathbb{F}_p[[\mathrm{GL}_n(\mathbb{Z}_p)]] = \varprojlim_k \mathbb{F}_p[\mathrm{GL}_n(\mathbb{Z}/p^n\mathbb{Z})]$ felett.
- *Megengedhető* Banach-tér reprezentáció: $V^* = \mathrm{Hom}^{ct}_K(V, K)$ végesen generált modulus $K \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[\mathrm{GL}_n(\mathbb{Z}_p)]]$ felett.
- Lok. anal. reprezentációk duálisa: $D(G, K)$ disztribúcióalgebra felett modulus.

Köszönöm szépen a figyelmet!