El problema de Galois inverso: variedades abelianas, conjetura de Goldbach y formas modulares

Samuele Anni

Seminario Latinoamericano de Teoría de Números

10 junio 2021

Université d'Aix-Marseille, Institut de Mathématiques

El problema de Galois inverso

El problema de Galois inverso

Sea G un grupo finito. ¿Existe una extensión de Galois $K/\mathbb{Q}$ tal que $\mathrm{Gal}(K/\mathbb{Q}) \cong G$?

El problema de Galois inverso

Sea G un grupo finito. ¿Existe una extensión de Galois $K/\mathbb{Q}$ tal que $\mathrm{Gal}(K/\mathbb{Q}) \cong G$?

El problema de Galois inverso efectivo

Sea G un grupo finito. Dar una expresión para un cuerpo de números $K/\mathbb{Q}$ tal que $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.

El problema de Galois inverso

Sea G un grupo finito. ¿Existe una extensión de Galois $K/\mathbb{Q}$ tal que $\mathrm{Gal}(K/\mathbb{Q}) \cong G$?

El problema de Galois inverso efectivo

Sea G un grupo finito. Dar una expresión para un cuerpo de números $K/\mathbb{Q}$ tal que $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.

El problema de Galois inverso y uniforme

Sea G_n una familia paramétrica de grupos finitos. Dar un único "objeto" asociado a una familia de cuerpos de números K_n tal que $\mathrm{Gal}(K_n/\mathbb{Q}) \cong G_n$ para todo n.

Teorema

Si $G_n \cong \mathbb{Z}/n\mathbb{Z}$ con $n \in \mathbb{Z}_{>1}$, entonces G_n es un grupo de Galois.

Demostración.

$p \equiv 1 \bmod (n)$ $\quad \mathbb{Q}(\zeta_p)/\mathbb{Q}$ $\quad G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$

$n \mid p-1$ $\quad \exists H \subset G$ de orden $\frac{p-1}{n}$ $\quad p-1$

$G \cong \mathbb{Z}/n\mathbb{Z} = \mathrm{Gal}(\mathbb{Q}(\zeta_p)^H/\mathbb{Q})$

H $\quad \mathbb{Q}(\zeta_p)$ $\quad$ de G

$\mathbb{Q}(\zeta_p)^H$

G $\quad \mathbb{Q}$

□

Teorema

Si $G_n \cong S_n$ con $n \in \mathbb{Z}_{>1}$, entonces G es un grupo de Galois.

Demostración.

K_n : cuerpo de descomposición de $x^n - x - 1$

Entonces, $\mathrm{Gal}(K_n/\mathbb{Q}) \cong S_n$ para todo n (realización uniforme). $\square$

$\{x^n - x - 1\}_n$

El problema de Galois inverso

Sea G un grupo finito. ¿Existe una extensión de Galois $K/\mathbb{Q}$ tal que $\mathrm{Gal}(K/\mathbb{Q}) \cong G$?

Objetivo de esta charla

Realizar **explícitamente** para todo* $g \in \mathbb{Z}_{\geq 1}$, el grupo $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, simultáneamente para todo los primos impares ℓ, usando la ℓ-torsión de la jacobiana de la misma curva hiperelíptica.

Sea $\overline{\mathbb{Q}}$ una clausura algebraica de $\mathbb{Q}$ y sea $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Sea A una variedad abeliana principalmente polarizada sobre $\mathbb{Q}$ de dimensión g.

Sea ℓ un primo y $A[\ell]$ el subgrupo de ℓ-torsion:

$$A[\ell] := \{P \in A(\overline{\mathbb{Q}}) \mid [\ell]P = 0\} \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}.$$

$G_{\mathbb{Q}} \to GL_{2g}(\mathbb{F}_\ell)$

$A[\ell]$ es un espacio vectorial sobre $\mathbb{F}_\ell$ de dimensión $2g$, así como también es un $G_{\mathbb{Q}}$-módulo.

La polarización induce un emparejamiento simpléctico, el **emparejamiento de Weil** mod ℓ en $A[\ell]$, que es un emparejamiento bilineal, alternado y no degenerado:

$$\langle\ ,\ \rangle\ :\ A[\ell] \times A[\ell] \to \mu_\ell$$

que es invariante de Galois: $\forall \sigma \in G_{\mathbb{Q}}\,,\ \forall v, w \in A[\ell]$

$$\langle \sigma v, \sigma w \rangle = \chi(\sigma)\langle v, w \rangle,$$

donde $\chi : G_{\mathbb{Q}} \to \mathbb{F}_\ell^\times$ es el carácter ciclotómico mod ℓ.

$(A[\ell], \langle\ ,\ \rangle)$ es un espacio vectorial simpléctico sobre $\mathbb{F}_\ell$ de dimensión $2g$ equipado con una acción de $G_{\mathbb{Q}}$. Esto da una representación

$$\overline{\rho}_{A,\ell} : G_{\mathbb{Q}} \to \mathrm{GSp}(A[\ell], \langle\ ,\ \rangle) \cong \mathrm{GSp}_{2g}(\mathbb{F}_\ell).$$

Ejemplo: $g = 1$

Consideramos $\ell = 3$ y la curva elíptica sobre $\mathbb{Q}$:

$$E: \quad y^2 = x^3 + 5x + 22 \qquad (53.a1)$$

El polinomio de 3-división ψ_3 : las raíces son las x-coordenadas de los puntos de 3-torsión. En este caso el polinomio es

$$\psi_3(x) = 3x^4 + 30x^2 + 264x - 25.$$

Es fácil demostrar que $\psi_3(x)$ es irreducible sobre $\mathbb{Q}$ y así gracias a un teorema de Reverter y Vila tenemos que

$$\overline{\rho}_{E,3} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_3)$$

es sobreyectiva.

Ejemplo: $g = 1$

$$\overline{\rho}_{E,3} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_3)$$

es sobreyectiva, entonces existe un cuerpo de números $K/\mathbb{Q}$, el núcleo de la representación, tal que $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_3)$.

K es el cuerpo de descomposición de

$$x^8 + 3x^7 + 7x^6 + \frac{29}{3}x^5 + \frac{26}{3}x^4 + 4x^3 + x^2 + \frac{5}{9}X - \frac{7}{27}.$$

Teorema (Serre)

Sea $A/\mathbb{Q}$ una variedad abeliana principalmente polarizada de dimensión g. Supongamos que $g = 2$, 6 o g es impar y, además, que $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$. Entonces existe una cota B_A tal que para todos los números primos $\ell > B_A$ la representación $\overline{\rho}_{A,\ell}$ es sobreyectiva.

Se sabe que la conclusión del teorema es falsa para g generales (contraejemplo de Mumford para $g = 4$).

Pregunta abierta

¿Es posible tener una **cota uniforme** B_g que depende solo de g?

$$B_A \sim \left((14g)^{64g^2} d\, h_A\right)^{2^{10} g^3}$$

Género 1

La representación de Galois asociada a la ℓ-torsion de la **curva elíptica**

$$y^2 + y = x^3 - x \qquad (37.a1)$$

es sobreyectiva para todo los primos ℓ. Esto da una realización $\mathrm{GL}_2(\mathbb{F}_\ell)$ como grupo de Galois para todo los primos ℓ.

Género 2 **(Dieulefait)**

Sea C la **curva hiperelíptica de género 2**:

$$y^2 = x^5 - x + 1 \qquad (45904.d.734464.1)$$

y sea J su jacobiana. Dieulefait demostró que $\overline{\rho}_{J,\ell}$ es sobreyectiva para todo los primos impares ℓ. Esto da una realización $\mathrm{GSp}_4(\mathbb{F}_\ell)$ como grupo de Galois para todo los primos impares ℓ.

Genus 3 (A., Lemos y Siksek)

Sea $C/\mathbb{Q}$ la siguiente curva hiperelíptica de género 3,

$$C \ : \ y^2 + (x^4 + x^3 + x + 1)y = x^6 + x^5.$$

y sea J su jacobiana. Entonces

$$\overline{\rho}_{J,\ell}(G_{\mathbb{Q}}) = \mathrm{GSp}_6(\mathbb{F}_\ell)$$

para todo los primos impares ℓ. Además, $\overline{\rho}_{J,2}(G_{\mathbb{Q}}) \cong S_5 \times C_2 \subseteq S_8$.

Generos superiores

¿Qué pasa con $g \geq 4$?

Resultado principal

Teorema (A., Dokchitser)

Sea g un entero positivo tal que se satisfaga la hipótesis $(2\mathrm{G}+\epsilon)$.

Entonces existe un entero explícito $N \in \mathbb{Z}$ y un polinomio mónico explícito $f_0 \in \mathbb{Z}[x]$ de grado $2g+2$ tal que si

1. $f(x) \equiv f_0$ mód N, *y*
2. $C\colon y^2 = f(x)$ *es semiestable en todos los números primos* $p \nmid N$

entonces por cada número primo ℓ:

$$\mathrm{Gal}(\mathbb{Q}(\mathrm{Jac}(C)[\ell])/\mathbb{Q}) \cong \begin{cases} \mathrm{GSp}_{2g}(\mathbb{F}_\ell) \text{ si } \ell \neq 2 \\ S_{2g+2} \text{ si } \ell = 2. \end{cases}$$

En el resto de la charla explicaré el papel de la hipótesis$(2\mathrm{G}+\epsilon)$ y daré algunas ideas de la prueba del teorema.

Parejas de Goldbach

Sea $g \in \mathbb{Z}_{\geq 0}$.

Hipótesis $(2\mathrm{G}+\epsilon)$

Existen primos q_1, q_2, q_3, q_4, q_5 tales que:

$2g+2 = q_1+q_2 = q_4+q_5, \qquad 2g+2 > q_3 > q_5 > q_2 \geq q_1 > q_4.$

La hipótesis $(2\mathrm{G}+\epsilon)$ ha sido verificada para g hasta 10^7: las únicas excepciones son $0, 1, 2, 3, 4, 5, 7$ y 13.

~~$(2G+\varepsilon)$~~ $g=13$ $2g+2 = 28 = 17+11 = 23+5$

$(2G+\varepsilon)$ ✓ $g=6$ $2g+2 = 14 = 11+3 = 7+7 < 13$

Comentarios

- Si $(2\mathrm{G}+\epsilon)$ no se cumple, aún es posible obtener la misma conclusión excepto para una lista finita de números primos ℓ:

Género g	números primos excluidos
2	$3, 5$
3	$3, 5, 7$
4	$5, 7$
5	$5, 7, 11$
7	$5, 11, 13$
13	$11, 17, 23$

- Es posible probar que por cada g que satisfaga $(2\mathrm{G}+\epsilon)$ existe una **densidad positiva** de $f(x) \in \mathbb{Z}[x]$ como en el teorema anterior.

$2g+2$

Notación: sea $C : y^2 = f(x)$ una curva hiperelíptica sobre $\mathbb{Q}$ con $f(x) \in \mathbb{Z}[x]$ un polinomio monico y libre de cuadrados de grado $2g+2$ y sea $J = \mathrm{Jac}(C)$.

Ejemplo: $g = 6$

$$
\begin{aligned}
f_0(x) = x^{14} &+ 1122976550518058592759939074\, x^{13} + 1024732349070635834864352\, x^{12} \\
&+ 1120184609916242124087443456\, x^{11} + 186398290364786000921886720\, x^{10} \\
&+ 1685990245699349559300014080\, x^{9} + 387529952672653585935499264\, x^{8} \\
&+ 1422826957983635547417870336\, x^{7} + 585983998625429997308035072\, x^{6} \\
&+ 607434202225985243206107136\, x^{5} + 1820210247550502007557029888\, x^{4} \\
&+ 533014336994715937945092096\, x^{3} + 595803405154942945879752704\, x^{2} \\
&+ 1276845913825955586899050496\, x + 13236723818180308138226688000.
\end{aligned}
$$

$$
N = p_t^2 \cdot p_t'^2 \cdot p_{lin} \cdot p_{irr} \cdot p_2^2 \cdot p_2'^2 \cdot p_3^3 \cdot p_3'^3 \cdot 2^{2g+2} \cdot \prod_{3 \le p \le g} p^2 =
$$

$$
= 7^2 \cdot 11^2 \cdot 23 \cdot 29 \cdot 19^2 \cdot 41^2 \cdot 37^3 \cdot 17^3 \cdot 2^{14} \cdot 3^2 \cdot 5^2 = 2201590757511816436065484800
$$

Para todo polinomio $f(x) \in \mathbb{Z}[x]$ tal que

1. $f(x) \equiv f_0 \mod N$, y
2. $C: y^2 = f(x)$ es semiestable en todos los números primos $p \nmid N$ (e.g. $f = f_0$).

$$
\mathrm{Gal}(\mathbb{Q}(J[\ell])/\mathbb{Q}) \cong \begin{cases} \mathrm{GSp}_{12}(\mathbb{F}_\ell) & \text{si } \ell \neq 2 \\ S_{14} & \text{si } \ell = 2. \end{cases}
$$

Subgrupos de $\mathsf{GSp}_{2g}(\mathbb{F}_\ell)$

Transvección

Definición

Sea $(V, \langle\ ,\ \rangle)$ *un espacio vectorial simpléctico de dimensión finita sobre* $\mathbb{F}_\ell$. *Una* **transvección** *es un elemento* $T \in \mathrm{GSp}(V, \langle\ ,\ \rangle)$ *que fija un hiperplano* $H \subset V$.

Por lo tanto, una transvección es un elemento unipotente $\sigma \in \mathrm{GSp}(V, \langle\ ,\ \rangle)$ tal que $\sigma - I$ tiene rango 1.

¿Cuándo $\overline{\rho}_{J,\ell}(G_{\mathbb{Q}})$ contiene una transvección?

Sea $C/\mathbb{Q}$ una curva hiperelíptica del género g:

$$C : y^2 = f(x)$$

donde $f \in \mathbb{Z}[x]$ es un polinomio mónico y libre de cuadrados.

Sea $p \neq \ell$ un primo impar tal que p no divida el discriminante de f y y supongamos que f módulo p tiene una raíz en $\overline{\mathbb{F}}_p$ de multiplicidad precisamente 2, con todas las demás raíces simples.

Entonces el modelo de Néron de la jacobiana J en p tiene una dimensión tórica 1, es decir, $\overline{\rho}_{J,\ell}(G_{\mathbb{Q}})$ contiene una transvección (Grothendieck, Hall).

Clasificación de subgrupos de $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ con una transvección

Teorema (Arias-de-Reyna, Dieulefait y Wiese; Hall)

Sea $\ell \geq 5$ un primo y sea V un espacio vectorial simpléctico sobre $\mathbb{F}_\ell$ de dimensión $2g$. Sea G un subgrupo de $\mathrm{GSp}(V)$ tal que:

1. *G contiene una transvección;*
2. *V es un G-módulo irreducible sobre $\mathbb{F}_\ell$;*
3. *V es un módulo G primitivo.*

Entonces G contiene $\mathrm{Sp}(V)$. Lo mismo es válido para $\ell = 3$, siempre que $V \otimes \overline{\mathbb{F}}_3$ sea un módulo G irreducible y primitivo.

Variedades abelianas semiestables

El caso semiestable

Teorema (A., Lemos y Siksek)

Sea A una variedad abeliana semiestable principalmente polarizada de dimensión $g \geq 1$ sobre $\mathbb{Q}$ y sea $\ell \geq \max(5, g+2)$ primo.

Supongamos que la imagen de $\overline{\rho}_{A,\ell} : G_{\mathbb{Q}} \to \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ contiene una transvección.

Entonces $\overline{\rho}_{A,\ell}$ es reducible o sobreyectiva.

Idea de la prueba

Denote $\overline{\rho} = \overline{\rho}_{A,\ell}$. Sea $G = \overline{\rho}(G_{\mathbb{Q}}) \subseteq \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$.

Dado que G contiene una transvección, es suficiente mostrar que el caso imprimitivo no ocurre.

Supongamos lo contrario. Escribamos $V = \oplus_{i=1}^{h} V_i$ donde V_i son subespacios simplécticos no singulares de dimensión $2m < 2d$.

En particular, existe un homomorfismo $\phi : G \to S_h$ con imagen transitiva tal que $\sigma(V_i) = V_{\phi(\sigma)(i)}$.
Sea $\pi = \phi \circ \overline{\rho}$:

$$G_{\mathbb{Q}} \xrightarrow[\overline{\rho}]{} G \xrightarrow[\phi]{} S_h \qquad (\pi : G_{\mathbb{Q}} \to S_h)$$

Idea de la prueba

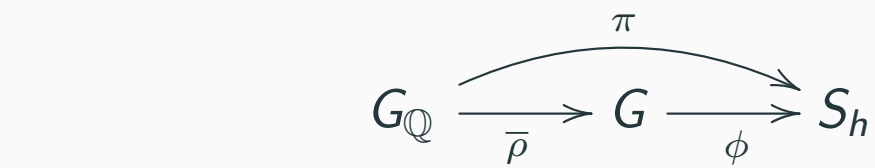
$$G_{\mathbb{Q}} \xrightarrow[\overline{\rho}]{} G \xrightarrow[\phi]{} S_h \qquad \text{con } G_{\mathbb{Q}} \xrightarrow{\pi} S_h$$

Sea $H = \ker(\pi)$. Entonces $H = G_K$ para algún cuerpo de números $K/\mathbb{Q}$. Además, $\overline{\rho}|_{G_K}$ es reducible ya que V_i son estable bajo la acción de G_K.

En la demostración mostramos que para $\ell \geq \text{máx}(5, g+2)$ la extensión $K/\mathbb{Q}$ no está ramificada en todos los números primos, y así K tiene discriminante ± 1

$\Rightarrow K = \mathbb{Q} \quad \Rightarrow \quad \pi$ is trivial $\Rightarrow$ contradicción

Idea de la prueba



Sea $p \neq \ell$ un primo. Como A es semiestable, I_p actúa unipotentemente en V, entonces $\overline{\rho}(\sigma)$ tiene orden una potencia de ℓ para $\sigma \in I_p$.

El orden de $\overline{\rho}(\sigma)$ es divisible por el orden de $\pi(\sigma)$ que divide $h!$

Como $h = 2g/2m \leq g < \ell \Rightarrow \pi(\sigma) = 1 \Rightarrow K/\mathbb{Q}$ no está ramificado en p.

La prueba de $p = \ell$ es más complicada. La cota se obtiene considerando la imagen del subgrupo de inercia y aplicando un resultado de Raynaud.

Género 3

Dejemos ahora que $A/\mathbb{Q}$ sea una **variedad abeliana principalmente polarizada de dimensión 3**.

Hipótesis

(a) A es semiestable;

(b) $\ell \geq 5$;

(c) $\overline{\rho}_{A,\ell}(G_{\mathbb{Q}})$ contiene una transvección.

Entonces $\overline{\rho}_{A,\ell}$ es reducible o sobreyectiva.

"Algoritmo" (A., Lemos y Siksek)

Método práctico que debería, en la mayoría de los casos, producir un pequeño entero B (que depende de A) tal que para $\ell \nmid B$, la representación $\overline{\rho}_{A,\ell}$ es irreducible y, por tanto, sobreyectiva.

Un paso: analizar los factores de Jordan–Hölder de *dimensión* 2.

Lema

Supongamos que el $G_{\mathbb{Q}}$-módulo $A[\ell]$ no tiene ningún factor de Jordan–Hölder de dimensión 1, pero tiene un subespacio irreducible U de dimensión 2 o 4. Entonces $A[\ell]$ tiene un factor de Jordan–Hölder de dimensión 2 con determinante χ.

Sea N el conductor de A. Sea W un factor de Jordan–Hölder de $A[\ell]$ de dimensión 2 con determinante χ.

La representación

$$\tau : G_{\mathbb{Q}} \to \mathrm{GL}(W) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$$

es impar (ya que el determinante es χ), irreducible (ya que W es un factor de Jordan–Hölder de $A[\ell]$ de dimensión 2).

Según la conjetura de modularidad de Serre (Teorema de Khare, Wintenberger, Dieulefait y Kisin), τ es **modular**:

$$\tau \cong \overline{\rho}_{f,\ell}$$

τ es equivalente a la representación mod ℓ asociada a una forma modular nueva f del nivel $M \mid N$ y peso 2.

La modularidad nos da un criterio para descartar los factores de Jordan–Hölder de dimensión 2 **pero** necesitamos calcular los espacios de formas modulares $S_2^{\mathrm{new}}(M)$ para todos los $M \mid \mathrm{cond}(A)$.

Este enfoque para el género 3 no generaliza: al aumentar g, el conductor aumenta (es al menos 10.323^g) y el cálculo de las formas nuevas de tales niveles no es posible actualmente.

Por otro lado, analizar los factores de Jordan–Hölder de dimensión más altas es aún más "desafiante".

Nuevo enfoque

Eliminar la hipótesis de la semiestabilidad e introducir primos de mala reducción de modo que la inercia local tenga un comportamiento específico.

Irreducibilidad y Goldbach

Definición

Sea $t \in \mathbb{Z}_{>0}$. *Decimos que* $f(x) = \sum_{i=0}^{m} a_i x^i \in \mathbb{Z}_p[x]$ *es un* t-**polinomio de Eisenstein** *de grado* $m \in \mathbb{Z}_{>0}$ *si es monico y* $\mathrm{ord}_p(a_i) \geq t$ *para todo* $i \neq m$, *mientras que* $\mathrm{ord}_p(a_0) = t$.

Definición

Sean $q_1, \ldots, q_k$ *números primos y sea* $t \in \mathbb{Z}_{>0}$.

Sea $f(x) \in \mathbb{Z}_p[x]$ *un polinomio monico libre de cuadrados. Entonces* $f(x)$ *es de* **tipo** $t - \{q_1, \ldots, q_k\}$ *si*

$$f(x) = h(x) \prod_{i=1}^{k} g_i(x - \alpha_i)$$

sobre $\mathbb{Z}_p[x]$, *con* $\alpha_i \in \mathbb{Z}_p$, $\overline{\alpha}_i \neq \overline{\alpha}_j$ *(reducción) para todos los* $i \neq j$, *donde* $g_i(x) \in \mathbb{Z}_p[x]$ *es un polinomio* t*-Eisenstein de grado* q_i *y* $\overline{h}(x)$ *es separable y tal que* $\overline{h}(\alpha_i) \neq 0$ *para todos los* i.

Definición

Sea $f(x) \in \mathbb{Z}_p[x]$ un polinomio monico libre de cuadrados. Decimos que f es de **tipo** *$t - \{q_1, \ldots, q_k\}$ en un primo p si $f(x) \in \mathbb{Z}_p[x]$ es de tipo $t - \{q_1, \ldots, q_k\}$.*

La noción de tipo se puede expresar en términos de condiciones de congruencia.

De vuelta al ejemplo

$$
\begin{aligned}
f_0(x) = x^{14} + {} & 1122976550518058592759939074 \; x^{13} + 1024732349070635834864435 2\; x^{12} + \\
+ {} & 1120184609916242124087443456 \; x^{11} + 1863982903647860009218867 20\; x^{10} + \\
+ {} & 1685990245699349559300014080 \; x^{9} + 3875299526726535859354992 64\; x^{8} + \\
+ {} & 1422826957983635547417870336 \; x^{7} + 5859839986254299973080350 72\; x^{6} + \\
+ {} & 607434202225985243206107136 \; x^{5} + 1820210247550502007557029888\; x^{4} + \\
+ {} & 533014336994715937945092096 \; x^{3} + 5958034051549429458797527 04\; x^{2} + \\
+ {} & 1276845913825955586899050496 \; x + 13236723818180308138226688 00.
\end{aligned}
$$

$$N = p_t^2 \cdot p_t'^2 \cdot p_{lin} \cdot p_{irr} \cdot p_2^2 \cdot p_2'^2 \cdot p_3^3 \cdot p_3'^3 \cdot 2^{2g+2} \cdot \prod_{3 \leq p \leq g} p^2 =$$

$$= 7^2 \cdot 11^2 \cdot 23 \cdot 29 \cdot 19^2 \cdot 41^2 \cdot 37^3 \cdot 17^3 \cdot 2^{14} \cdot 3^2 \cdot 5^2 = 2201590757511816436065484800$$

$f_0 \equiv (x^7 - 19) \cdot ((x-1)^7 - 19) \text{ mód } 19^3$	tipo 1 $- \{7, 7\}$	en 19
$f_0 \equiv (x^{11} - 41) \cdot ((x-1)^3 - 41) \text{ mód } 41^3$	tipo 1 $- \{3, 11\}$	en 41
$f_0 \equiv (x^{13} - 37^2) \cdot (x+1) \text{ mód } 37^3$	tipo 2 $- \{13\}$	en 37
$f_0 \equiv (x^{11} - 17^2) \cdot (x^3 + x + 14) \text{ mód } 17^3$	tipo 2 $- \{11\}$	en 17

Teorema

Supongamos que $f \in \mathbb{Z}_p[x]$ *tiene el tipo* $t - \{q_1, \ldots, q_k\}$ *con* $q_i \neq 2, p$ *para todo* i.

Entonces, por cada $\ell \neq p$, *el grupo de inercia* $I_{\mathbb{Q}_p}$ *actúa dócilmente en* $H^1_{ét}(C/\overline{\mathbb{Q}}_p, \mathbb{Q}_\ell)$ *y en* $J[\ell]$ *mediante un cociente de orden* $2\prod_i q_i$.

Además, los valores propios no triviales (con multiplicidad) de cualquier generador τ *de inercia dócil son*

$$-\zeta_{q_1}, -\zeta_{q_1}^2, \ldots, -\zeta_{q_1}^{q_1-1}, \ldots, -\zeta_{q_k}, -\zeta_{q_k}^2, \ldots, -\zeta_{q_k}^{q_k-1} \quad \textit{si } t \textit{ es impar}$$

o

$$\zeta_{q_1}, \zeta_{q_1}^2, \ldots, \zeta_{q_1}^{q_1-1}, \ldots, \zeta_{q_k}, \zeta_{q_k}^2, \ldots, \zeta_{q_k}^{q_k-1} \quad \textit{si } t \textit{ es par.}$$

El ingrediente principal de la prueba es la teoría de los "clusters" (Dokchitser T., Dokchitser V., Maistret y Morgan).

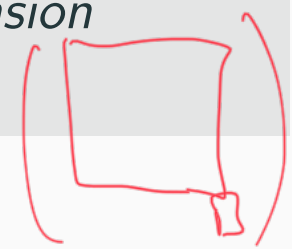
Lema

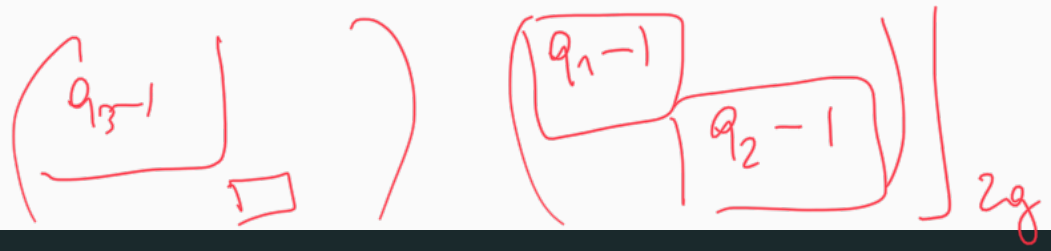
Sea p un primo impar. Supongamos que $f \in \mathbb{Z}_p[x]$ tiene el tipo $t - \{q_1, \ldots, q_k\}$ donde $q_1, \ldots, q_k$ son primos impares, coprimos con pt. Supongamos además que p es una raíz primitiva módulo cada uno de los q_i.

Entonces, para cada primo $\ell \neq p, q_1, \ldots, q_k$ tenemos

$$(J[\ell] \otimes_{\mathbb{F}_\ell} \overline{\mathbb{F}}_\ell)_{ss} = \bigoplus_i W_{q_i} \oplus \mathbf{1} \oplus \cdots \oplus \mathbf{1}$$

donde W_{q_i} es une $G_{\mathbb{Q}}$-subpresentación irreducibles de dimensión $(q_i - 1)$.





Lema

Sean q_1, q_2 y q_3 primos tales que $q_1 < q_2 < q_3 < 2g+2$ y $q_1 + q_2 = 2g + 2$.

Supongamos que $f \in \mathbb{Z}[x]$ tiene el tipo $1 - \{q_1, q_2\}$ en un primo impar p_2 y el tipo $2 - \{q_3\}$ en un primo impar p_3, donde p_2 es una raíz primitiva módulo q_1 y q_2; y p_3 es una raíz primitiva módulo q_3.

Entonces, para cada primo $\ell \neq q_1, q_2, q_3, p_2, p_3$, el $G_{\mathbb{Q}}$-módulo $J[\ell]$ es absolutamente irreducible.

Teorema

Sea g un entero positivo que satisfaga $(2\mathrm{G}+\epsilon)$:

$$2g+2 = q_1+q_2 = q_4+q_5 \qquad 2g+2 > q_3 > q_5 > q_2 \geq q_1 > q_4.$$

Supongamos que $f \in \mathbb{Z}[x]$ tiene el tipo $1-\{q_1,q_2\}$ en un primo impar p_2, y el tipo $1-\{q_4,q_5\}$ en un primo impar p_2', el tipo $2-\{q_3\}$ en un primo impar p_3 y el tipo $2-\{q_5\}$ en un primo impar p_3', donde:

- *p_2 es una raíz primitiva módulo q_1 y q_2;*
- *p_2' es una raíz primitiva módulo q_4 y q_5;*
- *p_3 es una raíz primitiva módulo q_3;*
- *p_3' es una raíz primitiva módulo q_5.*

Entonces, para cada ℓ primo, el $G_{\mathbb{Q}}$-módulo $J[\ell]$ es absolutamente irreducible.

Demostración.

La aplicación del Lema anterior con q_1, q_2, q_3, demuestra la afirmación para todos los $\ell \neq p_2, p_3, q_1, q_2, q_3$. Aplicando el lema nuevamente con q_4, q_5, q_3 y con q_1, q_2, q_5 probamos el resultado para todo ℓ. $\square$

Generalización

Generalización : cuerpos de números

El problema de Galois inverso sobre cuerpos de números

Sea G un grupo finito et $K/\mathbb{Q}$ un cuerpo de números. ¿Existe una extensión de Galois L/K tal que $\mathrm{Gal}(L/K) \cong G$?

Hay una obstrucción proveniente del emparejamiento de Weil, p. ej.

$$E : y^2 + (\frac{\sqrt{101}+1}{2})y = x^3 + x^2 - 2x - 7 \quad \text{sobre } \mathbb{Q}(\sqrt{101})$$

$$\overline{\rho}_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{101}))) \cong \mathrm{GL}_2(\mathbb{F}_\ell) \quad \forall \text{ primo } \ell \neq 101$$

$$\rho_{E,101}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{101}))) \subseteq D \cdot \mathrm{SL}_2(\mathbb{F}_{101})$$

donde D es el conjunto de cuadrados invertibles en $\mathbb{F}_{101}$.

Generalización : otros grupos lineales

Pregunta

¿Cómo podemos resolver explícitamente el problema de Galois inverso para grupos como $\mathrm{GL}_2(\mathbb{F}_{\ell^2})$ or $\mathrm{PGL}_2(\mathbb{F}_{\ell^2})$?

Teorema (Wiese)

Supongamos la conjetura de Maeda para las formas modulares clásicas. Entonces, para todo entero impar d, el conjunto de primos ℓ para el que existe $K/\mathbb{Q}$ un cuerpo de números tal que $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{PGL}_2(\mathbb{F}_{\ell^d})$ tiene densidad 1.

El problema de Galois inverso: variedades abelianas, conjetura de Goldbach y formas modulares

Samuele Anni

Seminario Latinoamericano de Teoría de Números

10 junio 2021

¡Gracias!