Delimitando el grupo de automorfismos de una curva

Josep González

Abstract

Para una curva X de género $g > 1$ definida sobre un cuerpo K, es conocido que el grupo $\mathrm{Aut}_K(X)$ es finito. Si la característica de K es cero, entonces tenemos la cota de Hurwitz $|\mathrm{Aut}_K(X)| \leq 84(g-1)$. Cuando la característica de K es positiva, Stichtenoth provó que $|\mathrm{Aut}_K(X)| < 16g^4$ (cf. [Sti73]), excepto para las curva Hermíticas, para las cuales el orden de su grupo de automorfismos es conocido y mayor que esta cota. En particular, tenemos una cota para el orden de un automorfismo de la curva X. No obstante, no disponemos de un procedimiento general para descartar órdenes posibles de automorfismos.

Nuestro interés se centra en el caso en que K es un cuerpo de números. En esta situación, la reducción de la curva X en un primo de K de buena reducción es una curva $\widetilde{X}$ definida sobre un cuerpo finito $\mathbb{F}_q$. Aunque la inclusión

$$\mathrm{Aut}_K(X) \subset \mathrm{Aut}_{\mathbb{F}_q}(\widetilde{X})$$

puede ser estricta, cualquier información que permita descartar órdenes de los elementos del grupo $\mathrm{Aut}_{\mathbb{F}_q}(\widetilde{X})$ será útil para nuestro objetivo. Además, si es necesario, podemos cambiar el primo de buena reducción para X.

Par una curva X de género > 1 definida sobre un cuerpo finito $\mathbb{F}_q$, fijamos un entero $s > 1$ que sea potencia de un primo racional. Presentamos un criterio que, bajo ciertas condiciones sobre la sucesión $\{|X(\mathbb{F}_{q^n})|\}_{n\geq 1}$ dependiendo de s, asegura la no existencia de elementos del grupo $\mathrm{Aut}_{\mathbb{F}_q}(X)$ de orden s. Aunque este criterio no es una caracterización para la no existencia de tales automorfismos, es una potente herramienta que puede ser aplicada en muchas situaciones.

Para poder aplicar el criterio, sólo precisamos conocer el polinomio característico $Q(x)$ del endomorfismo Frob_q actuando en el módulo de Tate de la jacobiana de X. Para ser más precisos, sólo necesitamos disponer de $Q(x) \pmod{s}$. Comentaremos su aplicabilidad computacional y su efectividad.

Finalmente, mostraremos su aplicación a curvas modulares (no hiperelípticas) de género alto. La razón de elegir curva modulares es doble. Por un lado, el estudio de grupos de automorfismos de ciertas curvas modulares ha sido el origen que me ha conducido al establecimiento de este criterio. Por otro lado, la congruencia de Eichler-Shimura permite determinar el polinomio característico del endomorfismo Frob_ℓ de una varietat abeliana que es un coiente definido sobre $\mathbb{Q}$ de la jacobiana de la curva modular $X_0(N)$, cuando $\ell \nmid N$. En efecto, el polinomio caracterísitico se obtiene a partir de los ℓ-coeficientes de Fourier de ciertas formas modulares nuevas normalizads y éstos son proporcionados por programas como Magma o Sage.

Más concretamente, el criterio ha sido utilizado para provar la trivialidad del grupo

(i) $\mathrm{Aut}(X_0(p^2)/w_{p^2})$ para $p = 17, 19, 23, 29, 31$, donde w_{p^2} denota la involución de Fricke,

(ii) $\mathrm{Aut}(X_0(p)/w_p)$ para $p = 163, 193, 197, 211, 223, 227, 229, 269, 331, 347, 359, 383, 389, 431, 461, 563, 571, 607$.

Presentaremos una aplicación para las curvas modulares *non-split* Cartan de nivel primo p: $X_{ns}(p)$. Estas curvas son cocientes de las curvas modulares $X(p)$, que están definidas sobre $\mathbb{Q}$ y tienen una involución w definida sobre $\mathbb{Q}$, llamada involución modular. Su género es mayor que 1 para $p \geq 11$.

En un artículo conjunto con V. Dose, J. Fernández y R. Schoof (cf. [DFGS14]), probamos que

$$\mathrm{Aut}(X_{ns}(11)) = \mathrm{Aut}_{\mathbb{Q}}(X_{ns}(11)) \simeq (\mathbb{Z}/2\mathbb{Z})^2\,,$$

y se conjetura que $\mathrm{Aut}(X_{ns}(p)) = \{1, w\}$ para $p > 11$. Existen resultados parciales de V. Dose para $p \geq 37$ (cf. [Dos]).

Las curvas $X_{ns}(p)$ tienen géneros $8, 15, 20, 35, 54$ y 63 para $p = 13, 17, 19, 23, 29$ y 31 respectivamente. Las curvas

$$X_{ns}^{+}(p) := X_{ns}(p)/w$$

tienen géneros $3, 6, 8, 13, 24, 28$ para $p = 13, 17, 19, 23, 29$ y 31 respectivamente.

Utilizando argumentos modulares y el criterio presentado, probaremos que

Proposición 1. *Sea p un primo tal que $13 \leq p \leq 31$. Entonces,*

(i) El grupo $\mathrm{Aut}(X_{ns}^{+}(p))$ es trivial.

(ii) La involución modular w es el único automorfismo no trivial de $X_{ns}(p)$.

References

[DFGS14] V. Dose, J. Fernández, J. González, and R. Schoof. The automorphism group of the non-split Cartan modular curve of level 11. *Journal of Algebra*, 417:95–102, 2014.

[Dos] V. Dose. On the automorphisms of the non-split cartan modular curves of prime level.

[Sti73] Henning Stichtenoth. Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe. *Arch. Math. (Basel)*, 24:527–544, 1973.