Hindes, Wade

Classifying Galois groups of small iterates via rational points. (English) Zbl 1441.11281

Int. J. Number Theory 14, No. 5, 1403-1426 (2018).

Let $\phi(x)$ be a monic quadratic polynomial over Z and put $\phi^0(x) = x$ and $\phi^n(x) = \phi(\phi^{n-1}(x))$ for $n \geq 1$. The paper deals with Galois group $G_n(\phi, b)$ of the polynomial $\phi^n(x) - b$, where $b \in Z$ is generic for ϕ, i.e. for all n the equation $\phi^n(x) = b$ has 2^n distinct solutions. Moreover let $T_{2,n}(\phi)$ be the graph whose set of vertices equals $\bigcup_{m=0}^{n}\{z : \phi^m(z) = b\}$, and two elements z_1, z_2 are joined by an edge if $z_2 = \phi(z_1)$. If $T_{2,n}$ is the binary rooted tree with n levels, then the graphs $T_{2,n}(\phi)$ and $T_{2,n}$ are isomorphic. Since $G_n(\phi, b)$ acts on $T_{2,n}(\phi)$, it is a subgroup of $\mathrm{Aut}(T_{2,n})$. Therefore the inverse limit $G(\phi, b) = \varprojlim G_n(\phi, b)$ is a subgroup of the group of automorphisms $\mathrm{Aut}(T_2)$ of the full binary rooted tree T_2.

It has been conjectured (see [*N. Boston* and *R. Jones*, Pure Appl. Math. Q. 5, No. 1, 213–225 (2009; Zbl 1167.11011)]) that if $\phi(x) = x^2 + c \in Z[x]$, all its iterates are irreducible and $c \neq -2$, then the index of $G(\phi, 0)$ in $\mathrm{Aut}(T_2)$ is finite, and this has been shown to be true for certain large families of polynomials (see [*M. Stoll*, Arch. Math. 59, No. 3, 239–244 (1992; Zbl 0758.11045)] and [*H.-C. Li*, Arch. Math. 114, No. 3, 265–269 (2020; Zbl 1435.37108)]). *C. Gratton* et al. [Bull. Lond. Math. Soc. 45, No. 6, 1194–1208 (2013; Zbl 1291.37121)] and the author [Acta Arith. 159, 149–197 (2013; Zbl.1296.14017)] showed that the conjecture follows from the ABC conjecture.

The author established earlier [Proc. Amer. Math.Soc. 144, 1931–1939 (2016; Zbl.1338.14026)] that if the Vojta conjecture holds [*P. Vojta*, Lect. Notes Math. 2009, 111–224 (2011; Zbl 1258.11076)], then there exist an integer $n = n(\phi)$ such that if $G_n(\phi, 0) = \mathrm{Aut}(T_n(\phi))$, then $G(\phi, 0) = \mathrm{Aut}(T_2)$. He showed also (J. Number Th. 148, 372–383 (2015); Zbl.1391.37090) that for a large class of quadratic polynomials over the field of rational functions over a field of zero characteristics the analogous assertion holds with $n = 17$ without any unproved assumptions.

In this paper the implications

$$G_3(\phi, 0) = \mathrm{Aut}(T_{2,3}) \longrightarrow G_5(\phi, 0) = \mathrm{Aut}(T_{2,5})$$

and, if $c \neq 3$ also

$$G_2(\phi, 0) = \mathrm{Aut}(T_{2,2}) \longrightarrow G_5(\phi, 0) = \mathrm{Aut}(T_{2,5})$$

are established (Theorem 1.3), and this implies that if $c \neq 3$ and neither $-c$ nor $-(c + 1)$ is a square, then one has $G_5(\phi, 0) = \mathrm{Aut}(T_{2,5})$. Theorem 1.6 gives similar implications in case $b = 1$. The proofs are based on the determination of all rational points on hyperelliptic curves

$$C_\varepsilon : \ y^2 = -x^{\varepsilon_0}\phi^1(x)^{\varepsilon_1} \cdots \phi^n(x)^{\varepsilon_n},$$

with $\varepsilon_i \in \{0, 1\}$, which is performed using the Chabauty-Coleman method (see e.g. [*W. McCallum* and *B. Poonen*, Panor. Synth. 36, 99–117 (2012; Zbl 1377.11077)]) and the Mordell-Weil sieve (see [*N. Bruin* and *M. Stoll*, LMS J. Comput. Math. 13, 272–306 (2010; Zbl 1278.11069)].

Reviewer: Władysław Narkiewicz (Wrocław)

MSC:

11R32	Galois theory
11G30	Curves of arbitrary genus or genus $\neq 1$ over global fields
14G05	Rational points
37P15	Dynamical systems over global ground fields

Keywords:

Galois groups; arithmetical dynamics; rational points on curves; quadratic polynomials; preimage tree;

arboreal representations

Software:

Magma; SageMath

Full Text: DOI arXiv

References:

[1] Balakrishnan, J.; Bradshaw, R.; Kedlaya, K., Explicit Coleman integration for hyperelliptic curves, Int. Algorithmic Number Theory Symp., 16-31, (2010), Springer, Berlin · Zbl 1261.14011

[2] Bosma, W.; Cannon, J.; Playoust, C., The magma algebra system. I. the user language, J. Symbolic Comput., 24, 235-265, (1997) · Zbl 0898.68039

[3] Bruin, N.; Stoll, M., The Mordell-Weil sieve: proving non-existence of rational points on curves, LMS J. Comput. Math., 13, 272-306, (2010) · Zbl 1278.11069

[4] de la Harpe, P., Topics in Geometric Group Theory, (2000), University of Chicago Press, Chicago, IL · Zbl 0965.20025

[5] Hamblen, S.; Jones, R.; Madhu, K., The density of primes in orbits of $z^d + c$, Int. Math. Res. Not., 7, 1924-1958, (2015) · Zbl 1395.11128

[6] Hindes, W., The arithmetic of curves defined by iteration, Acta Arith., 169, 1-27, (2015) · Zbl 1330.14032

[7] Hindes, W., Galois uniformity in quadratic dynamics over $k(t)$, J. Number Theory, 148, 372-383, (2015) · Zbl 1391.37090

[8] Hindes, W., The vojta conjecture implies Galois rigidity in dynamical families, Proc. Amer. Math Soc., 144, 1931-1939, (2016) · Zbl 1338.14026

[9] Jones, R., The density of prime divisors in the arithmetic dynamics of quadratic polynomials, J. London Math. Soc. (2), 78, 2, 523-544, (2008) · Zbl 1193.37144

[10] Jones, R., Galois representations from pre-image trees: an arboreal survey, Publ. Math. UFS Sci. Tech. Besançon, 2013, 107-136, (2013) · Zbl 1307.11069

[11] Katz, N., Galois properties of torsion points on abelian varieties, Invent. Math., 62, 3, 481-502, (1980) · Zbl 0471.14023

[12] McCallum, W.; Poonen, B., Explicit Methods in Number Theory: Rational Points and Diophantine Equations, 36, The method of Chabauty and Coleman, 99-117, (2012), Société Mathématiques de France · Zbl 1377.11077

[13] Mumford, D., Tata Lectures on Theta II, (1984), Birkhäuser, Boston

[14] SageMath, the Sage Mathematics Software System (Version 7.2), The Sage Developers (2016), http://www.sagemath.org; see specifically the implementations for "Hyperelliptic curves over p-adic fields".

[15] Serre, J.-P., Abelian ℓ-Adic Representations and Elliptic Curves, (1968), W. A. Benjamin, New York

[16] Silverman, J., The Arithmetic of Elliptic Curves, 106, (2009), Springer Science \& Business Media · Zbl 1194.11005

[17] Stoll, M., Galois groups over $\Bbb Q$ of some iterated polynomials, Arch. Math. (Basel), 59, 3, 239-244, (1992) · Zbl 0758.11045

[18] Stoll, M., Rational points on curves, J. Théor. Nombres Bordeaux, 23, 1, 257-277, (2011) · Zbl 1270.11030

[19] Vasiu, A., Surjectivity criteria for p-adic representations, part I, Manuscripta Math., 112, 3, 325-355, (2003) · Zbl 1117.11064

[20] Vojta, P., Arithmetic Geometry, Diophantine approximation and Nevanlinna theory, 111-224, (2010), Springer, Berlin · Zbl 1258.11076