Jones, Rafe

An iterative construction of irreducible polynomials reducible modulo every prime. (English)

Zbl 1302.11086
J. Algebra 369, 114-128 (2012).

Summary: We give a method of constructing polynomials of arbitrarily large degree irreducible over a global field F but reducible modulo every prime of F. The method consists of finding quadratic $f \in F[x]$ whose iterates have the desired property, and it depends on new criteria ensuring all iterates of f are irreducible. In particular when F is a number field in which the ideal (2) is not a square, we construct infinitely many families of quadratic f such that every iterate f^n is irreducible over F, but f^n is reducible modulo all primes of F for $n \geq 2$. We also give an example for each $n \geq 2$ of a quadratic $f \in \mathbb{Z}[x]$ whose iterates are all irreducible over $\mathbb{Q}$, whose $(n-1)$st iterate is irreducible modulo some primes, and whose nth iterate is reducible modulo all primes. From the perspective of Galois theory, this suggests that a well-known rigidity phenomenon for linear Galois representations does not exist for Galois representations obtained by polynomial iteration. Finally, we study the number of primes $\mathfrak{p}$ for which a given quadratic f defined over a global field has f^n irreducible modulo $\mathfrak{p}$ for all $n \geq 1$.

MSC:

11R09	Polynomials (irreducibility, etc.)	Cited in **1** Review
37P15	Dynamical systems over global ground fields	Cited in **10** Documents

Keywords:

algebraic number theory; irreducibility of polynomials; polynomial iteration

Full Text: DOI arXiv

References:

[1] Ahmadi, Omran; Luca, Florian; Ostafe, Alina; Shparlinski, Igor, On stable quadratic polynomials, Glasg. math. J., 54, 2, 359-369, (2012) · Zbl 1241.11027

[2] Ali, Nidal, Stabilité des polynômes, Acta arith., 119, 1, 53-63, (2005) · Zbl 1088.11078

[3] Ayad, Mohamed; McQuillan, Donald L., Irreducibility of the iterates of a quadratic polynomial over a field, Acta arith., 93, 1, 87-97, (2000) · Zbl 0945.11020

[4] Ayad, Mohamed; McQuillan, Donald L.; Ayad, Mohamed; McQuillan, Donald L., Corrections to: "irreducibility of the iterates of a quadratic polynomial over a field", Acta arith., Acta arith., 99, 1, 97-97, (2001) · Zbl 0945.11020

[5] Boston, Nigel; Jones, Rafe, Settled polynomials over finite fields, Proc. amer. math. soc., 140, 6, 1849-1863, (2012) · Zbl 1243.11115

[6] Brandl, Rolf, Integer polynomials that are reducible modulo all primes, Amer. math. monthly, 93, 4, 286-288, (1986) · Zbl 0603.12002

[7] Danielson, Lynda; Fein, Burton, On the irreducibility of the iterates of $x^n - b$, Proc. amer. math. soc., 130, 6, 1589-1596, (2002), (electronic) · Zbl 1007.12001

[8] Fein, Burton; Schacher, Murray, Properties of iterates and composites of polynomials, J. lond. math. soc. (2), 54, 3, 489-497, (1996) · Zbl 0865.12003

[9] Flajolet, Philippe; Odlyzko, Andrew M., Random mapping statistics, (), 329-354 · Zbl 0747.05006

[10] Guralnick, Robert; Schacher, Murray M.; Sonn, Jack, Irreducible polynomials which are locally reducible everywhere, Proc. amer. math. soc., 133, 11, 3171-3177, (2005), (electronic) · Zbl 1134.11040

[11] Jones, Rafe, The density of prime divisors in the arithmetic dynamics of quadratic polynomials, J. lond. math. soc. (2), 78, 2, 523-544, (2008) · Zbl 1193.37144

[12] Jones, Rafe; Rouse, Jeremy, Galois theory of iterated endomorphisms, Proc. lond. math. soc. (3), 100, 3, 763-794, (2010), Appendix A by Jeffrey D. Achter · Zbl 1244.11057

[13] Neukirch, Jürgen, Algebraic number theory, Grundlehren math. wiss., vol. 322, (1999), Springer-Verlag Berlin, translated from the 1992 German original and with a note by Norbert Schappacher, with a foreword by G. Harder · Zbl 0956.11021

[14] Odoni, R.W.K., The Galois theory of iterates and composites of polynomials, Proc. lond. math. soc. (3), 51, 3, 385-414, (1985)

· Zbl 0622.12011

[15] Odoni, R.W.K., On the prime divisors of the sequence $w_{n + 1} = 1 + w_1 \cdots w_n$, J. lond. math. soc. (2), 32, 1, 1-11, (1985) · Zbl 0574.10020

[16] Odoni, R.W.K., Realising wreath products of cyclic groups as Galois groups, Mathematika, 35, 1, 101-113, (1988) · Zbl 0662.12010

[17] Ostafe, Alina; Shparlinski, Igor E., On the length of critical orbits of stable quadratic polynomials, Proc. amer. math. soc., 138, 8, 2653-2656, (2010) · Zbl 1268.11155

[18] Rosen, Michael, Number theory in function fields, Grad. texts in math., vol. 210, (2002), Springer-Verlag New York · Zbl 1043.11079

[19] Silverman, Joseph H., Variation of periods modulo \textit{p} in arithmetic dynamics, New York J. math., 14, 601-616, (2008) · Zbl 1153.11028

[20] Stoll, Michael, Galois groups over Q of some iterated polynomials, Arch. math. (basel), 59, 3, 239-244, (1992) · Zbl 0758.11045

[21] Vasiu, Adrian, Surjectivity criteria for \textit{p}-adic representations. I, Manuscripta math., 112, 3, 325-355, (2003) · Zbl 1117.11064