Stoll, Michael

Galois group over $\mathbb{Q}$ of some iterated polynomials. (English) Zbl 0758.11045

Arch. Math. 59, No. 3, 239-244 (1992).

Let a be an integer such that $-a$ is not a square in $\mathbb{Q}$, $f := X^2 + a \in \mathbb{Z}[X]$, and denote the iterates of f by $f_0 := X$ and $f_{n+1} := f(f_n) = f_n^2 + a$ for all $n \geq 0$. Let $c_1 := -a$ and $c_{n+1} := f(c_n) = c_n^2 + a$ for $n \geq 1$. There is an integer sequence $(b_n)_{n\geq 1}$ with the b_n coprime in pairs such that for all $n \geq 1$, $c_n = \prod_{d|n} b_d$. Let K_n be the splitting field of f_n over $\mathbb{Q}$ and denote by $\Omega_n := \mathrm{Gal}(K_n/\mathbb{Q}) = \mathrm{Gal}(f_n/\mathbb{Q})$ its Galois group over the rational numbers. Let $[C_2]^n$ denote the n-fold wreath product of the 2-element group. Then it is known that Ω_n always injects into $[C_2]^n$. The following equivalence is shown in the paper: $\Omega_n \cong [C_2]$ if and only if $c_1, c_2, \dots, c_n$ are 2-independent in $\mathbb{Q}$.

Here, "2-independent" means that no nonempty product of some of the c_n is a square. This gives the following sufficient condition for $\Omega_n \cong [C_2]^n$ to hold: $|b_m|$ is not a square for $2 \leq m \leq n$.

This condition is then verified for all n in the following cases: ($a > 0$ and $a \equiv 1$ or $2 \bmod 4$) or ($a < 0$ and $a \equiv 0 \bmod 4$ and $-a$ not a square). So, for these a, one always has $\mathrm{Gal}(f_n/\mathbb{Q}) \cong [C_2]^n$ for all n.

Reviewer: M.Stoll (München)

MSC:

11R32	Galois theory
11R09	Polynomials (irreducibility, etc.)
11B37	Recurrences

Keywords:

iterated polynomials; recursion; Galois group; wreath product of the 2- element group

Full Text: DOI

References:

[1] J. E. Cremona, On the Galois groups of the iterates ofx 2+1. Mathematika36, 259-261 (1989). · Zbl 0699.12018 · doi:10.1112/S0025579300013127

[2] R. W. K. Odoni, Realising wreath products of cyclic groups as Galois groups. Mathematika35, 101-113 (1988). · Zbl 0662.12010 · doi:10.1112/S002557930000632X