

ON IRREDUCIBLE POLYNOMIALS OVER \mathbf{Q} WHICH ARE REDUCIBLE OVER \mathbf{F}_p FOR ALL p

MOHAMED AYAD

ABSTRACT. Examples of polynomials having the property of being irreducible over \mathbf{Q} but reducible over \mathbf{F}_p for all primes p are constructed. If some conditions of linear disjointness are satisfied by two number fields, then any integer generating the compositum of these fields satisfies this property. We study the question of whether the above property is preserved for a given polynomial under translations. It is shown, in particular, that the polynomial $x^n - nax^{n-1} - b$ satisfies the above property, for any even integer $n \geq 4$, any integer $a \neq 0$ and all but finitely b of the form $b = (-1)^{n/2}c^2 - a^n(n-1)^{n-1}$, where c is a positive integer.

1. Introduction. Let $f(x)$ be a monic polynomial with integral coefficients. In order to prove that this polynomial is irreducible over \mathbf{Q} , one may try to find a prime p such that $f(x)$ is irreducible modulo p . But some authors, the first one being Hilbert, have shown that such a prime may as well not exist. Lee [13] has shown that if a is a square-free rational integer neither equal to 1 nor to -1 , then the polynomial

$$f(x) = x^4 + 2(1 - a)x^2 + (1 + a)^2$$

is irreducible over \mathbf{Q} but reducible modulo p for every prime p .

Definition 1. A given monic polynomial with integral coefficients has the property (P) if it is irreducible over \mathbf{Q} but reducible over \mathbf{F}_p for every prime p .

Golomb [8, Theorem 2] proved that the cyclotomic polynomial $\phi_n(x)$ satisfies (P) if and only if $n \neq 1, 2, p^k, 2p^k$ where p is an odd prime and k is a positive integer. Indeed, Lee's and Golomb's examples are

Keywords and phrases. Irreducible polynomial, inert prime, Hilbert's irreducibility theorem, linearly disjoint extensions, linear relations connecting roots of polynomials.

Received by the editors on March 17, 2008, and in revised form on April 2, 2008.

DOI:10.1216/RMJ-2010-40-5-1377 Copyright ©2010 Rocky Mountain Mathematics Consortium