On a Special Case of Hilbert’s Irreducibility Theorem

Marius Cavachi

Faculty of Mathematics, ‘Ovidius’ University of Constanța,
Bd. Mamaia 124, 8700 Constanța, Romania

Communicated by D. Zagier

Received March 31, 1998; revised June 29, 1999; accepted October 1, 1999

We prove that if \( K \) is a finite extension of \( \mathbb{Q} \), \( P \) is the set of prime numbers in \( \mathbb{Z} \) that remain prime in the ring \( R \) of integers of \( K \), \( f, g \in K[X] \) with \( \deg g > \deg f \) and \( f, g \) are relatively prime, then \( f + pg \) is reducible in \( K[X] \) for at most a finite number of primes \( p \in P \). We then extend this property to polynomials in more than one indeterminate. These results are related to Hilbert’s irreducibility theorem.

Throughout this paper, an algebraic number field \( K \) is such that the extension \( \mathbb{Q} \subseteq K \) is normal. We shall denote by \( R \) the ring of algebraic integers of \( K \). It is well-known that the set \( P \) of prime numbers in \( \mathbb{Z} \) that remain prime in \( R \) is infinite (see [2, p. 136]).

If \( f, g \in K[X] \) are relatively prime, by Hilbert’s irreducibility theorem, the irreducible polynomial \( f(X) + Yg(X) \in K[X, Y] \) remains irreducible in \( K[X] \) for infinitely many \( Y = n \in \mathbb{Z} \). We shall make this property more precise in our particular context.

**Theorem 1.** Let \( K \) be an algebraic number field such that the extension \( \mathbb{Q} \subseteq K \) is normal. Let \( R \) be the ring of algebraic integers of \( K \) and \( P \) the set of prime numbers in \( \mathbb{Z} \) that remain prime in \( R \). Let \( f, g \) be two polynomials in \( K[X] \) having no common root. If \( \deg g > \deg f \), then the polynomial \( f + pg \) is reducible in \( K[X] \) for at most a finite number of primes \( p \in P \).

**Proof.** Consider the set \( P' = \{ p \in P \mid f + pg \text{ is reducible} \} \) and assume \( P' \) is infinite. We may suppose \( f, g \in R[X] \). Let \( p \in P' \) and \( f + pg = u'_p \cdot v'_p \) in \( K[X] \) with \( \deg u'_p \geq 1 \) and \( \deg v'_p \geq 1 \). Further, we may take \( u'_p = (1/\alpha) u_p \) and \( v'_p = (1/\beta) v_p \), with \( \alpha, \beta \in \mathbb{Z} \) and \( u_p, v_p \in R[X] \). Then \( x f + pg = u_p \cdot v_p \). We choose \( a \in \mathbb{Z}_+ \) as the smallest positive integer for which \( a(f + pg) \) may be non-trivially decomposed over \( R \), i.e.:

\[
a(f + pg) = u_p \cdot v_p, \quad \text{with} \quad v_p, u_p \in R[X].
\]
We shall first prove that $p$ does not divide $a$. Let $\alpha$ be the degree of the extension $\mathbb{Q} \subseteq K$. We denote by $h^*$ the polynomial obtained from $h \in K[X]$ after applying to its coefficients the $\mathbb{Q}$-automorphism $\sigma \in G$. We have:

$$a^* \prod_{\sigma \in G} (f + pg)^v = \prod_{\sigma \in G} u_p^\sigma \cdot \prod_{\sigma \in G} v_p^\sigma. \tag{2}$$

If $p \mid a$, then $p \mid \prod_{\sigma \in G} u_p^\sigma \cdot \prod_{\sigma \in G} v_p^\sigma$ in $R[X]$. As $p$ is prime in $R$, there exists $\sigma_0 \in G$ so that $p \mid u_{\sigma_0}^p$ or $p \mid v_{\sigma_0}^p$. Suppose $p \mid u_{\sigma_0}^p$; by applying $\sigma_0^{-1}$ we obtain $p \mid u_p$, so that $u_p = p \cdot u_{\sigma_0}^p$, with $u_{\sigma_0}^p \in R[X]$. Then $(a/p)(f + pg) = u_p^p \cdot v_p$ and the minimality of $a$ is contradicted.

Let now $m$ (respectively $k$, $r$) be the degree of $g$ (respectively $u_p$, $v_p$) and $g_m$ (respectively $b_k$, $c_r$) the leading coefficient of $g$ (respectively $u_p$, $v_p$). From (1) we derive: $apg_m = b_kc_r$. Thus we may suppose $b_k = pd_k$ in $R$.

Then, by using the norm $N$ of $K$ over $\mathbb{Q}$ and the relation (1) we get:

$$a^*(p^N(g_m)X^{nm} + \cdots) = (p^N(d_k)X^{nk} + \cdots) \cdot (N(c_r)X^{nr} + \cdots) \tag{3}$$

in $\mathbb{Z}[X]$. Considering the contents of the above polynomials and simplifying with $a^*$, we obtain:

$$Q_p(X) := \prod_{\sigma \in G} (f + pg)^\sigma = R_p(X) \cdot T_p(X) \tag{4}$$

in $\mathbb{Z}[X]$, where the leading coefficient $t_p$ of $T_p$ divides the integer $N(g_m)$ (since $p \nmid a$).

On the other hand, as $\lim_{z \to \infty} f^*(z)/g^*(z) = 0$ for all $\sigma \in G$, there exists $M > 0$ such that for each $\sigma \in G$ we have $|f^*(z)/g^*(z)| < 1$ if $|z| > M$. The roots of $T_p$ are among those of $Q_p$, hence their modules are bounded by $M$, a constant independent on $p$. Now, observing that $t_p$ can only take a finite number of values and that $\deg T_p < m$, from Viêt’s relations for $T_p$ we deduce that all the coefficients of $T_p$ are bounded (in module) by the same constant $M_0$, not depending upon $p$. Finally, $T_p \in \mathbb{Z}[X]$, thus the set $\{T_p \mid p \in \mathbb{P}\}$ is finite. As $\mathbb{P}$ is infinite, there exist $p_1, p_2, \ldots, p_{n+1} \in \mathbb{P}$, mutually distinct, such that $T_{p_1} = T_{p_2} = \cdots = T_{p_{n+1}}$. If we choose a root of $T_{p_1}$, then $z$ is also a root of $Q_{p_1}, Q_{p_2}, \ldots, Q_{p_{n+1}}$. Hence there exists $\sigma \in G$ and $i \neq j$ such that $z$ is a root of both $(f + p_i g)^\sigma$ and $(f + p_j g)^\sigma$. This means that, extending $\sigma$ to an automorphism $\bar{\sigma}$ of a normal extension $\mathbb{Q} \subseteq K'$, with $K(z) \subseteq K'$, $\bar{\sigma}^{-1}(z)$ is a common root of $f$ and $g$, contradicting the hypothesis. The proof is now complete. \[\square\]

Remark 1. The above proof works for any extension $K$ of $\mathbb{Q}$, but it is non-void only if $P$ is infinite. This happens if $Gal(K, \mathbb{Q})$ contains an element of order $\deg K$ (by Cebotarev density), in particular when $\mathbb{Q} \subseteq K$ is cyclic.
Corollary. If \( f, g \in K[X] \) are relatively prime, \( \deg g \leq \deg f \) and \( f(0) = 0 \), then \( f + pg \) is reducible for at most a finite number of \( p \in P \).

**Proof.** One only has to change the variable \( x \) into \( 1/x \). 

We now extend the previous result to more than one indeterminate.

**Theorem 2.** Let \( K \) be an algebraic number field as in the statement of Theorem 1 and let \( f, g \in K[X_1, X_2, ..., X_m] \), \( m > 1 \), be two relatively prime polynomials. If \( \deg_{X_1} g > \deg_{X_1} f \), then \( f + pg \) is reducible for at most a finite number of \( p \in P \).

**Proof.** As the leading coefficient of \( g \) (as a polynomial in \( X_1 \)) viewed in \( K[X_2, ..., X_m] \) has a finite number of divisors in this ring, we easily deduce the existence of a finite set \( A \subseteq Z \) such that \( f + ng \) has no divisors of positive degree in \( K[X_2, ..., X_m] \) for \( n \in Z \setminus A \). From the fact that \( f, g \in K[X_2, ..., X_m][X_1] \) have no common factors we deduce that the result \( \text{Res}(f, g) \) is non-null. Hence there exist \( a_2, ..., a_m \in K \) so that \( \text{Res}(f, g)(a_2, ..., a_m) \neq 0 \). From known properties of the resultant we conclude that \( f(X_1, a_2, ..., a_m) \) and \( g(X_1, a_2, ..., a_m) \) are relatively prime in \( K[X_1] \). In addition, changing the variables \( X_1, ..., X_m \) into \( a_2, ..., a_m \) the leading coefficient of \( g \) remains non-null. If \( f + pg \) is irreducible for infinitely many primes in \( P \), then \( f(X_1, a_2, ..., a_m) + pg(X_1, a_2, ..., a_m) \) is irreducible for infinitely many primes in \( P - A \), which contradicts Theorem 1.

**Example.** The polynomial \( f \in \mathbb{Q}[X], f(X) = X^{n+2} + X^n + pX + p, n \geq 2 \), is reducible for at most a finite number of primes \( p \in Z \). The same polynomial, viewed in \( \mathbb{Q}[i][X] \) is reducible for at most a finite number of prime integers of the form \( 4k + 3 \) (just apply the Corollary).

**Remark 2.** The condition \( f(0) = 0 \) is essential in the Corollary. To see this it is enough to consider \( f(X) = X^2 + 1 \) and \( g(X) = -1 \) in \( \mathbb{Q}[X] \). Then \( f(X) + pg(X) = X^2 - (p - 1) \) is reducible whenever \( p - 1 \) is a perfect square, and there are probably infinitely many such numbers.

**ACKNOWLEDGMENT**

The author is thankful to the referee for his pertinent observations and for signaling him the papers [1] and [3], related to the theme of this note. He is also thankful to Alexandru Gica for very useful comments.
REFERENCES