#A12 INTEGERS 17 (2017)

REDUCIBILITY OF POLYNOMIALS OVER ALGEBRAIC NUMBER FIELDS

P. Singthongla
Department of Mathematics, Khon Kaen University, Khon Kaen, Thailand
thepativat@gmail.com

N. R. Kanasri[1]
Department of Mathematics, Khon Kaen University, Khon Kaen, Thailand
naraka@kku.ac.th

V. Laohakosol[2]
Department of Mathematics, Kasetsart University, Bangkok, Thailand
fscivil@ku.ac.th

Received: 2/9/16, Revised: 8/11/16, Accepted: 3/24/17, Published: 4/24/17

Abstract

Let R be the ring of algebraic integers of an algebraic number field K such that the extension $\mathbb{Q} \subseteq K$ is normal. Let $P' = \{\nu \in \mathbb{Z} \mid \nu = p_1 p_2 \cdots p_s \text{ with } s \in \mathbb{N} \text{ and } p_1, p_2, \ldots, p_s \in P\}$, where P is the set of prime numbers in $\mathbb{Z}$ that remain prime in R. We prove that if f and g are two polynomials in $K[x]$ having no common root, then there exist at most finitely many $\nu \in P'$ such that $a(f + \nu g) = u_\nu v_\nu$ for some $a \in \mathbb{Z}, u_\nu, v_\nu \in R[x]$ with $\deg u_\nu \geq 1, \deg v_\nu \geq 1$ and ν divides the leading coefficient of u_ν or ν divides the leading coefficient of v_ν. Moreover, we extend this result to polynomials in more than one indeterminates.

1. Introduction

Throughout this paper, let K be an algebraic number field which is a normal extension of degree n over $\mathbb{Q}$ and let R denote the ring of algebraic integers of K. Then there exist exactly n distinct automorphisms $\sigma \in G := Gal(K/\mathbb{Q})$, the Galois group of K over $\mathbb{Q}$. For $\sigma \in G$, let $\hat{\sigma} : K[x] \to K[x]$ be defined by

$$\hat{\sigma}\left(a_0 + a_1 x + \cdots + a_m x^m\right) = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_m)x^m$$

[1]The author is supported by the Research and Academic Affairs Promotion Fund, Faculty of Science, Khon Kaen University, Fiscal year 2016 (RAAPF), Thailand.
[2]The author is supported by the Center for Advanced Studies in Industrial Technology and the Faculty of Science, Kasetsart University.

for all $a_0, a_1, \ldots, a_m \in K$ and $m \in \mathbb{N} \cup \{0\}$. Then $\hat{\sigma}$ is a ring isomorphism and $\hat{\sigma}(f) \in R[x]$ for all $f \in R[x]$.

Let P be the set of prime numbers in $\mathbb{Z}$ that remain prime in R. It is well-known that P is infinite if K is a cyclic extension of $\mathbb{Q}$ (see [5, p.136]). If $f, g \in K[x]$ are relatively prime, by Hilbert's irreducibility theorem, the irreducible polynomials $f + yg \in K[x, y]$ remain irreducible in $K[x]$ for infinitely many $y = n \in \mathbb{Z}$ (see [4]). In 2000, M. Cavachi, [2], made this property more precise by proving that if $f, g \in K[x]$ are relatively prime, then $f + pg$ are reducible in $K[x]$ for at most a finite number of primes $p \in P$ and then extended this result to polynomials in more than one indeterminates.

In the present work, let

$$P' = \{\nu \in \mathbb{Z} \mid \nu = p_1 p_2 \cdots p_s \text{ with } s \in \mathbb{N} \text{ and } p_1, p_2, \ldots, p_s \in P\}.$$

We extend the result of M. Cavachi by proving that if f and g are two polynomials in $K[x]$ having no common root, then there exist at most finitely many $\nu \in P'$ such that $a(f + \nu g) = u_\nu v_\nu$ for some $a \in \mathbb{Z}, u_\nu, v_\nu \in R[x]$ with $\deg u_\nu \geq 1, \deg v_\nu \geq 1$, and either ν divides the leading coefficient of u_ν or ν divides the leading coefficient of v_ν. Moreover, we extend this result to polynomials in more than one indeterminates.

2. Main Results

To prove the main results, we start with the following two lemmas.

Lemma 1. *If $f \in R[x]$, then*

$$\prod_{\sigma \in G} \hat{\sigma}(f) \in \mathbb{Z}[x].$$

Proof. Let $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$, $f(x) = f_0 + f_1 x + \cdots + f_m x^m \in R[x]$ with $f_m \neq 0$ and

$$g = \prod_{\sigma \in G} \hat{\sigma}(f).$$

Since $f \in R[x]$, we have $\hat{\sigma}(f) \in R[x]$ for all $\sigma \in G$. Thus $g \in R[x]$ is a polynomial of degree mn, say $g(x) = g_0 + g_1 x + \cdots + g_{mn} x^{mn}$. Now for each $\tau \in G$, we have

$$\begin{aligned}
\hat{\tau}(g) &= \prod_{\sigma \in G} \hat{\tau}\left(\hat{\sigma}(f)\right) \\
&= \hat{\tau}\left(\sigma_1(f_0) + \sigma_1(f_1)x + \cdots + \sigma_1(f_m)x^m\right) \cdots \hat{\tau}\left(\sigma_n(f_0) + \sigma_n(f_1)x + \cdots + \sigma_n(f_m)x^m\right) \\
&= \left(\tau \circ \sigma_1(f_0) + \cdots + \tau \circ \sigma_1(f_m)x^m\right) \cdots \left(\tau \circ \sigma_n(f_0) + \cdots + \tau \circ \sigma_n(f_m)x^m\right) \\
&= \prod_{\sigma \in G} \hat{\sigma}(f) \\
&= g,
\end{aligned}$$

since G is a group. Consequently, for each $i = 0, 1, \ldots, mn$, we have $\tau(g_i) = g_i$ for all $\tau \in G$, and so all the K-conjugates of g_i are equal. It follows that $g_i \in \mathbb{Q}$ for all $i = 0, 1, \ldots, mn$ (see [1, p.121]). But $g_i \in R$, so $g_i \in \mathbb{Z}$ for all $i = 0, 1, \ldots, mn$. Therefore, $g \in \mathbb{Z}[x]$ as desired. □

Lemma 2. *Let $p \in P$ and $f, g \in R[x]$. If $p \mid fg$, then $p \mid f$ or $p \mid g$.*

Proof. Assume that $p \mid fg$ but $p \nmid f$ and $p \nmid g$. Let

$$f(x) = u_0 + u_1 x + \cdots + u_k x^k \text{ and } g(x) = v_0 + v_1 x + \cdots + v_r x^r$$

with $u_0, u_1, \ldots, u_k, v_0, v_1, \ldots, v_r \in R$. Then all the coefficients of fg are divisible by p while there exist coefficients of f and g which are not divisible by p. Let u_j be the first coefficient of f which p does not divide. Similarly, let v_i be the first coefficient of g which p does not divide. In fg, the coefficient of x^{j+i} is

$$c_{j+i} = u_j v_i + (u_{j+1} v_{i-1} + \cdots + u_{j+i} v_0) + (u_{j-1} v_{i+1} + \cdots + u_0 v_{j+i}).$$

Now, by our choice of u_j, we have $p \mid u_{j-1}, p \mid u_{j-2}, \ldots, p \mid u_0$, so that $p \mid (u_{j-1} v_{i+1} + \cdots + u_0 v_{j+i})$. Similarly, by our choice of v_i, we have $p \mid v_{i-1}, p \mid v_{i-2}, \ldots, p \mid v_0$, so that $p \mid (u_{j+1} v_{i-1} + \cdots + u_{j+i} v_0)$. Since $p \mid c_{j+i}$, we have that $p \mid u_j v_i$. As p is a prime in R, either $p \mid u_j$ or $p \mid v_i$, which is a contradiction. □

It is well-known that every algebraic number is of the form r/s, where r is an algebraic integer and s is a nonzero ordinary integer. Thus, for $f, g \in K[x]$ and $\nu \in \mathbb{Z}$, if

$$f + \nu g = u' v'$$

in $K[x]$ with $\deg u' \geq 1$ and $\deg v' \geq 1$, then we may take $u = \alpha u'$ and $v = \beta v'$ for some $\alpha, \beta \in \mathbb{Z}$ and $u, v \in R[x]$ with $\deg u \geq 1$ and $\deg v \geq 1$. Thus

$$\alpha\beta(f + \nu g) = uv.$$

This implies that $f + \nu g$ is reducible in $K[x]$ if and only if $a(f + \nu g)$ is reducible in $R[x]$ for some integer a.

The following theorem is our main result.

Theorem 1. *If f and g are polynomials in $K[x]$ having no common root and $\deg g > \deg f$, then there exist at most finitely many $\nu \in P'$ such that $a(f + \nu g) = u_\nu v_\nu$ for some $a \in \mathbb{Z}, u_\nu, v_\nu \in R[x]$ with $\deg u_\nu \geq 1, \deg v_\nu \geq 1$, and either ν divides the leading coefficient of u_ν or ν divides the leading coefficient of v_ν.*

Proof. Let Ω be the set of integers $\nu \in P'$ such that $a(f + \nu g) = u_\nu v_\nu$ for some $a \in \mathbb{Z}, u_\nu, v_\nu \in R[x]$ with $\deg u_\nu \geq 1, \deg v_\nu \geq 1$, and either ν divides the leading coefficient of u_ν or ν divides the leading coefficient of v_ν. Suppose that Ω is infinite and we may assume that $f, g \in R[x]$.

Let $\nu \in \Omega$. Then we can choose $a \in \mathbb{Z}$ as the smallest positive integer such that

$$a\,(f+\nu g) = u_\nu v_\nu \tag{1}$$

for some $u_\nu,\ v_\nu \in R[x]$ satisfying the above conditions. We first prove that g.c.d$(a,\nu) = 1$. Let $p \in \mathbb{Z}$ be any prime divisor of ν. Then p is a prime in R. If $p \mid a$, then $p \mid u_\nu v_\nu$. By Lemma 2, either $p \mid u_\nu$ or $p \mid v_\nu$. We may assume that $p \mid u_\nu$, so $u_\nu = pu'_\nu$ with $u'_\nu \in R[x]$. Then $(a/p)\,(f+\nu g) = u'_\nu v_\nu$, which contradicts the minimality of a.

As n is the degree of the extension $\mathbb{Q} \subseteq K$, there exist exactly n distinct automorphisms $\sigma \in G$ and

$$a^n \prod_{\sigma\in G} \hat{\sigma}(f+\nu g) = \prod_{\sigma\in G} \hat{\sigma}\,(u_\nu) \prod_{\sigma\in G} \hat{\sigma}\,(v_\nu)\,. \tag{2}$$

Let m (respectively k, r) be the degree of g (respectively u_ν, v_ν) and g_m (respectively b_k, c_r) the leading coefficient of g (respectively u_ν, v_ν). Using (1), we get $a\nu g_m = b_k c_r$. By the properties of ν in Ω, we may assume $b_k = \nu d_k$ for some $d_k \in R$. Using Lemma 1, the norm N of K over $\mathbb{Q}$ and the relation (2), we have

$$a^n(\nu^n N(g_m)x^{nm} + \cdots) = (\nu^n N(d_k)x^{nk} + \cdots)(N(c_r)x^{nr} + \cdots) \tag{3}$$

in $\mathbb{Z}[x]$. Using g.c.d$(a,\nu) = 1$ and the fact that the content of $a^n(\nu^n N(g_m)x^{nm}+\cdots)$ is the product of the contents of $\nu^n N(d_k)x^{nk} + \cdots$ and $N(c_r)x^{nr} + \cdots$, we obtain

$$Q_\nu := \prod_{\sigma\in G} \hat{\sigma}(f+\nu g) = R_\nu T_\nu, \tag{4}$$

where $R_\nu, T_\nu \in \mathbb{Z}[x]$ possessing the properties that the leading coefficient t_ν of T_ν divides $N(g_m)$ and $\deg T_\nu < mn$.

Since $\deg g > \deg f$, we get $\lim_{z\to\infty} \dfrac{\hat{\sigma}(f(z))}{\hat{\sigma}(g(z))} = 0$ for all $\sigma \in G$. It follows that for each $\sigma \in G$, there exists $M > 0$ such that

$$\left|\frac{\hat{\sigma}(f(z))}{\hat{\sigma}(g(z))}\right| < 1$$

provided that $|z| > M$. If z_0 is a root of T_ν, then it is also a root of Q_ν. Consequently,

$$\hat{\sigma}(f(z_0)) + \nu\hat{\sigma}(g(z_0)) = \hat{\sigma}(f(z_0)+\nu g(z_0)) = 0$$

for some $\sigma \in G$. Thus, $\left|\dfrac{\hat{\sigma}(f(z_0))}{\hat{\sigma}(g(z_0))}\right| = \nu \geq 1$ and so $|z_0| \leq M$. This proves that the set of all roots of T_ν is bounded by M. Now, we have that $T_\nu \in \mathbb{Z}[x]$, $\deg T_\nu < mn$ and t_ν can only take only a finite number of values. By Vieta's relations for T_ν, we deduce that all the coefficients of T_ν are bounded by the same constant, not depending upon

ν. It follows that the set $\{T_\nu \mid \nu \in \Omega\}$ is finite because $T_\nu \in \mathbb{Z}[x]$. As Ω is infinite, there exist distinct $\nu_1, \nu_2, \ldots, \nu_{n+1} \in \Omega$ such that $T_{\nu_1} = T_{\nu_2} = \ldots = T_{\nu_{n+1}}$. Let z_1 be a root of T_{ν_1}. Then z_1 is also a root of $Q_{\nu_1}, Q_{\nu_2}, \ldots, Q_{\nu_{n+1}}$, which implies that there exist $\sigma \in G$ and $i \neq j$ such that z_1 is a root of both polynomials $\hat{\sigma}(f+\nu_i g) = \hat{\sigma}(f) + \nu_i \hat{\sigma}(g)$ and $\hat{\sigma}(f+\nu_j g) = \hat{\sigma}(f) + \nu_j \hat{\sigma}(g)$. Let K' be the splitting field of Q_{ν_i} over K. Since $Q_{\nu_i} \in \mathbb{Z}[x]$, we get that $\hat{\sigma}\left(Q_{\nu_i}\right) = Q_{\nu_i}$. Thus K' is also a splitting field of $\hat{\sigma}\left(Q_{\nu_i}\right)$ over K. It follows that there exists an automorphism $\bar{\sigma} : K' \to K'$ which extends $\sigma : K \to K$. By applying $\bar{\sigma}^{-1}$, we get that

$$f(\bar{\sigma}^{-1}(z_1)) + \nu_i g(\bar{\sigma}^{-1}(z_1)) = 0, \; f(\bar{\sigma}^{-1}(z_1)) + \nu_j g(\bar{\sigma}^{-1}(z_1)) = 0$$

and so $(\nu_i - \nu_j) g(\bar{\sigma}^{-1}(z_1)) = 0$. Since $\nu_i \neq \nu_j$, we obtain $g(\bar{\sigma}^{-1}(z_1)) = 0$ and so $f(\bar{\sigma}^{-1}(z_1)) = 0$. This shows that $\bar{\sigma}^{-1}(z_1)$ is a common root of f and g, which contradicts the hypothesis and the theorem is proved. $\square$

Remark. The above proof works for any normal extension K of $\mathbb{Q}$, but it is non-void only if P is infinite. This happens if K is cyclic.

The following examples give all of the integers ν in Theorem 1 for given polynomials f and g in $\mathbb{Z}[x]$. In this case, we may consider only $a = 1$.

Example 1. Let $f(x) = 2311x^2 + 184x + 2, g(x) = x^3$ be polynomials in $\mathbb{Z}[x]$ and $\nu \in \mathbb{N}$. Then

$$f(x) + \nu g(x) = \nu x^3 + 2311x^2 + 184x + 2.$$

`Case 1` $f(x) + \nu g(x) = (\nu x + a)(x^2 + bx + c)$ for some $a, b, c \in \mathbb{Z}$. Then we have

$$\nu b + a = 2311, \;\; \nu c + ab = 184 \text{ and } ac = 2.$$

If $a, c < 0$, then $\nu b = 2311 - a > 0$ and so $b > 0$. Since $\nu c = 184 - ab > 0$, we have $c > 0$, a contradiction. Thus $a, c > 0$. If $a = 2, c = 1$, then $\nu b = 2309$ and $\nu + 2b = 184$. It follows that $2b^2 - 184b + 2309 = 0$ and so $b = 46 \pm (1/2)\sqrt{3846} \notin \mathbb{Z}$, which is impossible. Thus $a = 1, c = 2$ and we get $\nu b = 2310$ and $2\nu + b = 184$. It follows that $b^2 - 184b + 4620 = 0$ and so $b = 30$ or 154. If $b = 30$, then $\nu = 77$, and if $b = 154$, then $\nu = 15$. In both cases, we have that

$$f(x) + 77g(x) = (77x + 1)(x^2 + 30x + 2)$$

and

$$f(x) + 15g(x) = (15x + 1)(x^2 + 154x + 2).$$

`Case 2` $f(x) + \nu g(x) = (x + a)(\nu x^2 + bx + c)$ for some $a, b, c \in \mathbb{Z}$. Then we have

$$\nu a + b = 2311, \;\; c + ab = 184 \text{ and } ac = 2.$$

By the same proof as in Case 1, we deduce that $a, c > 0$. If $a = 2, c = 1$, then $b = 183/2 \notin \mathbb{Z}$, which is impossible. Thus $a = 1, c = 2$ and so $b = 182$. It follows that $\nu = 2129$, which is a prime number. In this case, we get that

$$f(x) + 2129g(x) = (x + 1)(2129x^2 + 182x + 2).$$

From both cases, we deduce that $\Omega = \{15, 77, 2129\}$.

Example 2. Let $f(x) = 2312x^2 + 184x + 2, g(x) = 2x^3$ be polynomials in $\mathbb{Z}[x]$ and $\nu \in \mathbb{N}$. Then $f(x) + \nu g(x) = 2\nu x^3 + 2312x^2 + 184x + 2$.

`Case 1` $f(x) + \nu g(x) = (\nu rx + a)(sx^2 + bx + c)$ for some $a, b, c, r, s \in \mathbb{Z}$. Then we have

$$\nu rb + as = 2312, \nu rc + ab = 184, ac = 2 \text{ and } rs = 2.$$

If $a = -1, c = -2, r = -1, s = -2$, then $-\nu b = 2310$ and $2\nu - b = 184$. It follows that

$$b^2 + 184b + 2 \cdot 2310 = 0$$

and so $b = -30$ or -154. If $b = -30$, then $\nu = 77$. If $b = -154$, then $\nu = 15$. Thus,

$$f(x) + 77g(x) = (77x + 1)(2x^2 + 30x + 2),$$

and

$$f(x) + 15g(x) = (15x + 1)(2x^2 + 154x + 2).$$

If $a = -2, c = -1, r = -2, s = -1$, then $-2\nu b = 2310$ and $2\nu - 2b = 184$. It follows that

$$2b^2 + 184b + 2310 = 0$$

and so $b = -15$ or -77. If $b = -77$, then $\nu = 15$ and if $b = -15$, then $\nu = 77$. Thus,

$$f(x) + 15g(x) = (30x + 2)(x^2 + 77x + 1)$$

and

$$f(x) + 77g(x) = (154x + 2)(x^2 + 15x + 1).$$

If $a = -1, c = -2, r = -2, s = -1$, then $-2\nu b = 2311$ and $4\nu - b = 184$. It follows that

$$b^2 + 184b + 2 \cdot 2311 = 0$$

and so $b = -92 \pm \sqrt{3842} \notin \mathbb{Z}$, which is impossible. The remaining cases follow similarly.

`Case 2` $f(x) + \nu g(x) = (rx + a)(\nu sx^2 + bx + c)$ for some $a, b, c, r, s \in \mathbb{Z}$. Then we have

$$\nu sa + rb = 2312, rc + ab = 184, ac = 2 \text{ and } rs = 2.$$

If $a = -1, c = -2, r = -1, s = -2$, then $b = -182$ and so $2\nu = 2130$. Thus,

$$f(x) + 1065g(x) = (x + 1)(2130x^2 + 182x + 2).$$

If $a = -1, c = -2, r = -2, s = -1$, then $b = -180$ and so $\nu = 1952$. Thus,

$$f(x) + 1952g(x) = (2x + 1)(1952x^2 + 180x + 2).$$

If $a = -2, c = -1, r = -2, s = -1$, then $-2b = 182$ and so $\nu = 1065$. Thus,

$$f(x) + 1065g(x) = (2x + 2)(1065x^2 + 91x + 1).$$

If $a = -1, c = -2, r = 1, s = 2$, then $b = -186$ and so $-2\nu = 2498$, which is impossible. The remaining cases follow similarly. From all cases, we deduce that $\Omega = \{15, 77, 1065, 1952\}$.

Corollary 1. *Let f and g be two polynomials in $K[x]$ having no common root. If $\deg g \leq \deg f$ and $f(0) = 0$, then there exist at most finitely many $\nu \in P'$ such that $a(f + \nu g) = u_\nu v_\nu$ for some $a \in \mathbb{Z}, u_\nu, v_\nu \in R[x]$ with $\deg u_\nu \geq 1, \deg v_\nu \geq 1$ and either $\nu \mid u_\nu(0)$ or $\nu \mid v_\nu(0)$.*

Proof. Let

$$f(x) = f_1x + f_2x^2 + \cdots + f_kx^k \quad \text{and} \quad g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_mx^m,$$

with $m \leq k$ and $f_k, g_m, g_0 \neq 0$. Taking $x = 1/y$ and multiplying by y^k, we obtain

$$F(y) := y^k f\left(\frac{1}{y}\right) = f_1y^{k-1} + f_2y^{k-2} + \cdots + f_k \in K[y],$$
$$G(y) := y^k g\left(\frac{1}{y}\right) = g_0y^k + g_1y^{k-1} + g_2y^{k-2} + \cdots + g_my^{k-m} \in K[y].$$

Then $\deg G(y) = k > k-1 \geq \deg F(y)$. As f and g have no common root, so F and G have no common root. Thus, by Theorem 1, there exist at most finitely many $\nu \in P'$ such that

$$a(F(y) + \nu G(y)) = U_\nu(y)V_\nu(y) \tag{5}$$

for some $a \in \mathbb{Z}, U_\nu(y), V_\nu(y) \in R[y]$ with $r := \deg U_\nu \geq 1, s := \deg V_\nu \geq 1, k = r + s$ and either ν divides the leading coefficient of $U_\nu(y)$ or ν divides the leading coefficient of $V_\nu(y)$. Taking $y = 1/x$ in (5) and multiplying by x^k, we obtain

$$a\left(x^kF\left(\frac{1}{x}\right) + \nu x^kG\left(\frac{1}{x}\right)\right) = x^rU_\nu\left(\frac{1}{x}\right)x^sV_\nu\left(\frac{1}{x}\right).$$

Thus, for such integers ν, we get

$$a\,(f + \nu g) = u_\nu v_\nu$$

for some $u_\nu, v_\nu \in R[x]$ with $\deg u_\nu \geq 1, \deg v_\nu \geq 1$ and either $\nu \mid u_\nu(0)$ or $\nu \mid v_\nu(0)$ as desired. $\square$

The following are examples of Corollary 1.

Example 3. Let $f(x) = -66x^4 - (2+2i)x^2$ and $g(x) = 3x^4 + 3(-1+i)x^2 - 4$ be polynomials in $\mathbb{Q}(i)[x]$. Then f and g have no common root and

$$\begin{aligned} f(x) + 21g(x) &= -3x^4 + (-65+61i)\,x^2 - 84 \\ &= -\left(x^2 + 21(1-i)\right)\left(3x^2 + 2(1+i)\right), \end{aligned}$$

with $a = 1, \nu = 3 \cdot 7$ and $3, 7$ are primes in $\mathbb{Z}[i]$.

Example 4. Let $f(x) = \frac{47}{3}x^6 + 2\sqrt{-3}x^5 + \left(\frac{8}{3} + 4\sqrt{-3}\right)x^4 + \left(-26 + \frac{5}{3}\sqrt{-3}\right)x^3 + \frac{10}{3}x^2$ and $g(x) = -\frac{1}{3}x^6 + \left(\frac{1-\sqrt{-3}}{3}\right)x^3 - \frac{4}{3}x^2 - 4x - \frac{5}{3}$ be polynomials in $\mathbb{Q}(\sqrt{-3})[x]$. Then f and g have no common root and

$$\begin{aligned} 3\left(f(x) + 2\cdot 5^2 g(x)\right) &= -3x^6 + 6\sqrt{-3}x^5 + \left(8 + 12\sqrt{-3}\right)x^4 + \left(24 - 45\sqrt{-3}\right)x^3 \\ &\quad - 190x^2 - 600x - 250 \\ &= (\sqrt{-3}x^3 + 2x^2 - 2\cdot 5^2)(\sqrt{-3}x^3 + 4x^2 + 12x + 5), \end{aligned}$$

with $a = 3, \nu = 2\cdot 5^2$ and $2, 5$ are primes in $\mathbb{Z} + \mathbb{Z}\left(\frac{-1+\sqrt{-3}}{2}\right)$, the Eisenstein domain.

We now extend the main result to more than one indeterminates.

Theorem 2. *Let $f, g \in K[x_1, x_2, \ldots, x_m], m > 1,$ be two relatively prime polynomials. If $\deg_{x_1} g > \deg_{x_1} f$, then there exist at most finitely many $\nu \in P'$ such that $a(f + \nu g) = u_\nu v_\nu$ for some $a \in \mathbb{Z}, u_\nu, v_\nu \in R[x_1, x_2, \ldots, x_m], \deg_{x_1} u_\nu \geq 1, \deg_{x_1} v_\nu \geq 1$ and either ν divides the leading coefficient of $u_\nu \in R[x_2, \ldots, x_m][x_1]$ or ν divides the leading coefficient of $v_\nu \in R[x_2, \ldots, x_m][x_1]$.*

Proof. Let $f, g \in K[x_1, x_2, \ldots, x_m], m > 1,$ be two relatively prime polynomials. Then

$$f = f_r x_1^r + \cdots + f_1 x_1 + f_0 \quad \text{and} \quad g = g_s x_1^s + \cdots + g_1 x_1 + g_0,$$

where $f_i := f_i(x_2, \ldots, x_m), g_j := g_j(x_2, \ldots, x_m) \in K[x_2, \ldots, x_m]$ for all $i = 0, 1 \ldots, r$, $j = 0, 1 \ldots, s$ and $f_r, g_s \neq 0$. Thus $f, g \in K[x_2, \ldots, x_m][x_1]$ have no common root. It follows that the resultant $Res(f, g)$ of f and g is given by

$$Res(f, g) = f_r^s g_s^r \prod_{1\leq i\leq r, 1\leq j\leq s} (\alpha_i - \beta_j) \neq 0,$$

where $\alpha_1, \ldots, \alpha_r$ are the roots of f and $\beta_1, \ldots, \beta_s$ are the roots of g in an algebraic closure of $K(x_2, \ldots, x_m)$ and $Res(f, g) \in K[x_2, \ldots, x_m]$ (see [3, p.119]). Then there exist $a_2, \ldots, a_m \in K$ so that $Res(f, g)(a_2, \ldots, a_m) \neq 0$. Let $F = f(x_1, a_2, \ldots, a_m)$

and $G = g(x_1, a_2, \ldots, a_m)$. Then $F, G \in K[x_1]$ and so $\alpha F, \beta G \in R[x_1]$ for some $\alpha, \beta \in \mathbb{Z}$. Thus

$$Res(\alpha F, \beta G) = \alpha^s \beta^r f_r^s(a_2, \ldots, a_m) g_s^r(a_2, \ldots, a_m) \prod_{1 \le i \le r, 1 \le j \le s} \left(\alpha_i' - \beta_j'\right),$$

where $\alpha_1', \ldots, \alpha_r'$ are the roots of F and $\beta_1', \ldots, \beta_s'$ are the roots of G in an algebraic closure of K. It is clear that

$$Res(\alpha F, \beta G) = Res(\alpha f, \beta g)(a_2, \ldots, a_m) = \alpha^s \beta^r Res(f, g)(a_2, \ldots, a_m) \neq 0,$$

which implies that F, G have no common root and the leading coefficient of F and G are $f_r(a_2, \ldots, a_m) \neq 0$ and $g_s(a_2, \ldots, a_m) \neq 0$, respectively. Then $\deg F = \deg_{x_1} f < \deg_{x_1} g = \deg G$. If there are infinitely many $\nu \in P'$ such that

$$a(f + \nu g) = u_\nu v_\nu$$

for some $a \in \mathbb{Z}, u_\nu, v_\nu \in R[x_1, x_2, \ldots, x_m]$ with $\deg_{x_1} u_\nu \ge 1, \deg_{x_1} v_\nu \ge 1$ and either ν divides the leading coefficient of $u_\nu \in R[x_2, \ldots, x_m][x_1]$ or ν divides the leading coefficient of $v_\nu \in R[x_2, \ldots, x_m][x_1]$, then for such ν, we obtain

$$b(F + \nu G) = U_\nu V_\nu$$

for some $b \in \mathbb{Z}, U_\nu, V_\nu \in R[x_1]$ with $\deg U_\nu \ge 1, \deg V_\nu \ge 1$ and either ν divides the leading coefficient of U_ν or ν divides the leading coefficient of V_ν. This contradicts Theorem 1. □

3. Further Results

The condition that either ν divides the leading coefficient of u_ν or ν divides the leading coefficient of v_ν, is essential in Theorem 1. To see this, it is enough to consider $f(x) = 1$ and $g(x) = x^3$ in $\mathbb{Q}[x]$. Then

$$f(x) + k^3 g(x) = 1 + k^3 x^3 = (1 + kx)\left(1 - kx + k^2 x^2\right)$$

for all positive integers k.

In this section, we give some further results concerning the reducibility of $f + \nu g$ that does not satisfy the above condition, where f, g are polynomials in $\mathbb{Z}[x]$ with $\deg g = 2$ or 3.

Proposition 1. *Let $f, g \in \mathbb{Z}[x]$ be such that g is monic, $\deg f < \deg g = 2$ and $f(x) + pqg(x) = pqx^2 + Ax + B$ with $p, q, A, B \in \mathbb{Z}$ and $pq \neq 0$. Then $f(x) + pqg(x) = (px + a)(qx + b)$ in $\mathbb{Z}[x]$ if and only if*

$$a = \frac{A \pm \sqrt{A^2 - 4pqB}}{2q} \quad \text{and} \quad b = \frac{A \mp \sqrt{A^2 - 4pqB}}{2p} \tag{6}$$

are integers.

Proof. It is easy to show that if the integers a and b are as in (6), then $f(x) + pqg(x) = (px + a)(qx + b)$.

Conversely, assume that $f(x)+pqg(x) = (px+a)(qx+b)$ for some $a, b \in \mathbb{Z}$. Then

$$f(x) + pqg(x) = pqx^2 + (qa + pb)x + ab.$$

Thus $A = qa + pb$ and $B = ab$. It follows that $qa^2 - Aa + pB = 0$ and so (6) holds as desired. □

Example 5. Let $f(x) = x - 2$ and $g(x) = x^2$ be polynomials in $\mathbb{Z}[x]$ and $p = 3, q = 5$. Since $f(x) + 3 \cdot 5g(x) = 15x^2 + x - 2$, we have $A = 1, B = -2$ and so $a = \frac{1 \pm \sqrt{1+8\cdot 15}}{10}$, $b = \frac{1 \mp \sqrt{1+8\cdot 15}}{6}$. As a and b are integers, we obtain $a = -1, b = 2$. By Proposition 1, we deduce that

$$f(x) + 3 \cdot 5g(x) = (3x - 1)(5x + 2).$$

Proposition 2. *Let $f, g \in \mathbb{Z}[x]$ be such that g is monic, $\deg f < \deg g = 3$ and $f(x) + pqg(x) = pqx^3 + Ax^2 + Bx + C$ with $p, q, A, B, C \in \mathbb{Z}$ and $pq \neq 0$. Then $f(x) + pqg(x) = (px + a)(qx^2 + bx + c)$ in $\mathbb{Z}[x]$ if and only if*

$$\begin{aligned}
a &= \sqrt[3]{\alpha} + \sqrt[3]{\beta} + \frac{A}{3q}, \\
b &= \frac{2A}{3p} - \frac{\sqrt[3]{\alpha}q}{p} - \frac{\sqrt[3]{\beta}q}{p}, \\
c &= \frac{B}{p} - \frac{1}{p}\left(\sqrt[3]{\alpha} + \sqrt[3]{\beta} + \frac{A}{3q}\right)\left(\frac{2A}{3p} - \frac{\sqrt[3]{\alpha}q}{p} - \frac{\sqrt[3]{\beta}q}{p}\right),
\end{aligned} \tag{7}$$

are integers, where

$$\alpha = -\frac{Q}{2} + \sqrt{\frac{Q^2}{4} + \frac{P^3}{27}}, \ \beta = -\frac{Q}{2} - \sqrt{\frac{Q^2}{4} + \frac{P^3}{27}}, \tag{8}$$

with

$$P = \frac{pB}{q} - \frac{A^2}{3q^2}, \ Q = \frac{pBA}{3q^2} - \frac{2A^3}{27q^3} - \frac{p^2C}{q}. \tag{9}$$

Proof. It is easy to show that if the integers a, b and c are as in (7), then $f(x) + pqg(x) = (px + a)(qx^2 + bx + c)$.

Conversely, assume that $f(x)+pqg(x) = (px+a)(qx^2+bx+c)$ for some $a, b, c \in \mathbb{Z}$. Then

$$f(x) + pqg(x) = pqx^3 + (qa + pb)x^2 + (ab + pc)x + ac.$$

Thus $A = qa + pb, B = ab + pc, C = ac$, and so

$$a = \frac{A - pb}{q} \ \text{ and } \ ab = B - pc. \tag{10}$$

It follows that
$$a^3 - \frac{A}{q}a^2 + \frac{pB}{q}a - \frac{p^2C}{q} = 0. \tag{11}$$
Substituting a by $y + A/3q$, we get the equation
$$y^3 + \left(\frac{pB}{q} - \frac{A^2}{3q^2}\right)y + \left(\frac{pBA}{3q^2} - \frac{2A^3}{27q^3} - \frac{p^2C}{q}\right) = 0,$$
which has $y = \sqrt[3]{\alpha} + \sqrt[3]{\beta}$ as a solution, where α, β and P, Q are defined as in (8) and (9), respectively. Thus, $a = \sqrt[3]{\alpha} + \sqrt[3]{\beta} + \frac{A}{3q}$ is a solution of (11). Taking the integer a in (10), we obtain b and c as in (7) as desired. □

Example 6. Let $f(x) = 16x^2 - 25x + 1, g(x) = x^3 + x$ be polynomials in $\mathbb{Z}[x]$ and p, q be prime numbers. Then $f(x) + pqg(x) = pqx^3 + 16x^2 + (pq - 25)x + 1$. If
$$f(x) + pqg(x) = (px + a)(qx^2 + bx + c)$$
for some $a, b, c \in \mathbb{Z}$, then
$$ac = 1, pb + aq = 16 \text{ and } pc + ab = pq - 25.$$
If $a = c = -1$, then
$$pb - q = 16 \;\text{ and }\; 25 - b = p(q + 1). \tag{12}$$
It follows that $0 < b \leq 24$ and more precisely, only $b = 7$ satisfies the two equations in (12). Thus, $18 = p(q + 1)$, which implies that $p = 3, q = 5$. Hence
$$f(x) + 15g(x) = (3x - 1)(5x^2 + 7x - 1) = 15x^3 + 16x^2 - 10x + 1.$$
If $a = c = 1$, then
$$pb + q = 16 \;\text{ and }\; 25 + b = p(q - 1). \tag{13}$$
It follows that $b(p^2 + 1) = 5(3p - 5) > 0$ and so $b > 0$. Thus, $0 < q < 16$ and more precisely, only $q = 3$ satisfies two equations in (13). Then $pb = 13$, which implies that $p = 13, b = 1$. Thus,
$$f(x) + 39g(x) = (13x + 1)(3x^2 + x + 1) = 39x^3 + 16x^2 + 14x + 1.$$

References

[1] S. Alaca and K. S. Williams, *Introductory Algebraic Number Theory*, Cambridge University Press, Cambridge, 2004.

[2] M. Cavachi, On a special case of Hilbert's irreducibility theorem, *J. Number Theory* **82** (2000), 96-99.

[3] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, New York, 2000.

[4] M. Fried, On Hilbert's irreducibility theorem, *J. Number Theory* **6** (1974), 211-231.

[5] G. J. Janusz, *Algebraic Number Fields*, Academic Press, New York, 1973.