

On Hilbert's Irreducibility Theorem

by A. SCHINZEL (Warszawa)

In this paper irreducibility means irreducibility over the rational field and all polynomials and rational functions considered are supposed to have rational coefficients. Hilbert's Irreducibility Theorem asserts that if polynomials $f_m(t_1, \dots, t_r, x_1, \dots, x_s)$ ($m = 1, 2, \dots, n$) are irreducible as polynomials in $r+s$ variables and a polynomial $z(t_1, t_2, \dots, t_r)$ is not identically 0, then there exist infinitely many integer systems $(t'_1, t'_2, \dots, t'_r)$ such that all the polynomials $f_m(t'_1, t'_2, \dots, t'_r, x_1, \dots, x_s)$ are irreducible as polynomials in x_1, \dots, x_s and $z(t'_1, t'_2, \dots, t'_r) \neq 0$ (cf. [3], Chapter VIII, § 2). The main aim of this paper is to prove the following refinement of this theorem.

THEOREM 1. *Let $f_m(t_1, \dots, t_r, x_1, \dots, x_s)$ ($1 \leq m \leq n$) be irreducible polynomials in $r+s$ variables and let $z(t_1, \dots, t_r)$ be any polynomial $\neq 0$. There exist r arithmetical progressions P_1, \dots, P_r such that if $t'_l \in P_l$ ($1 \leq l \leq r$), then all the polynomials $f_m(t'_1, \dots, t'_r, x_1, \dots, x_s)$ are irreducible as polynomials in x_1, \dots, x_s and $z(t'_1, \dots, t'_r) \neq 0$.*

The Theorem applies also to fractional values of t_l if we adopt the following definition.

DEFINITION. An arithmetical progression consists of all rational numbers $\equiv b \pmod{a}$, where a, b are fixed integers, $a \neq 0$ and the congruence for rationals is understood in the ordinary sense.

The proof of the fundamental lemma follows closely the proof of Theorem 1 in [1].

LEMMA 1. *Let $F(t_1, \dots, t_r, u)$ be a polynomial such that for no rational function $\varphi(t_1, \dots, t_r)$, $F(t_1, \dots, t_r, \varphi(t_1, \dots, t_r)) = 0$ identically. There exist r arithmetical progressions P_1, \dots, P_r such that if $t_l \in P_l$ ($1 \leq l \leq r$), then $F(t_1, \dots, t_r, u) \neq 0$ for all rational u .*

Proof. We may assume without loss of generality that F has integer coefficients. Using Gauss's Lemma we factorize F into a product of polynomials with integer coefficients:

$$(1) \quad F(t_1, \dots, t_r, u) = F_0(t_1, \dots, t_r)F_1(t_1, \dots, t_r, u) \dots F_k(t_1, \dots, t_r, u),$$

where $k \geq 0$ and each F_j ($1 \leq j \leq k$) is irreducible, of positive degree d_j in u . Let $a_j(t_1, \dots, t_r)$ be the coefficient at u^{d_j} in F_j ($1 \leq j \leq k$).

It follows from the assumption that $d_j > 1$ ($1 \leq j \leq k$). It follows from Hilbert's theorem that there exist integers t'_1, t'_2, \dots, t'_r such that all the polynomials $F_j(t'_1, \dots, t'_r, u)$ are irreducible and

$$F_0(t'_1, \dots, t'_r) \prod_{j=1}^k a_j(t'_1, \dots, t'_r) \neq 0.$$

Since each $F_j(t'_1, \dots, t'_r, u)$ is irreducible of degree > 1 , there exist for each $j \leq k$ infinitely many primes q such that the congruence

$$F_j(t'_1, \dots, t'_r, u) \equiv 0 \pmod{q}$$

is insoluble ([3], cf. also proof of Theorem 1 in [1]), and in particular there is a prime q_j with the above property, such that

$$(2) \quad F_0(t'_1, \dots, t'_r) a_j(t'_1, \dots, t'_r) \not\equiv 0 \pmod{q_j} \quad (1 \leq j \leq k).$$

Now, let P_l be the progression $q_1 q_2 \dots q_k v + t'_l$ and assume that $t_l \in P_l$ ($1 \leq l \leq r$), i.e.

$$(3) \quad t_l \equiv t'_l \pmod{q_1 \dots q_k} \quad (1 \leq l \leq r).$$

It follows that

$$F_0(t_1, \dots, t_r) a_j(t_1, \dots, t_r) \equiv F_0(t'_1, \dots, t'_r) a_j(t'_1, \dots, t'_r) \pmod{q_1 q_2 \dots q_k}$$

and by (2)

$$(4) \quad F_0(t_1, \dots, t_r) \neq 0,$$

$$(5) \quad a_j(t_1, \dots, t_r) \not\equiv 0 \pmod{q_j} \quad (1 \leq j \leq k).$$

Suppose now that for some rational u_0 , $F(t_1, \dots, t_r, u_0) = 0$. It follows from (1) and (4) that $k > 0$ and for some $j_0 \leq k$

$$(6) \quad F_{j_0}(t_1, \dots, t_r, u_0) = 0.$$

By (3) the denominators of t_1, \dots, t_r are not divisible by q_{j_0} . In view of (5) the same is true for the denominator of u_0 and (3) and (6) imply

$$F_{j_0}(t'_1, \dots, t'_r, u_0) \equiv 0 \pmod{q_{j_0}},$$

which is impossible by the choice of q_{j_0} .

This contradiction completes the proof.

Proof of Theorem 1. It follows from Kronecker's criterion for the reducibility of polynomials in several variables (cf. [3], Chapter VIII, § 3) that for every irreducible polynomial $f(t_1, \dots, t_r, x_1, \dots, x_s)$ there exists a finite number of irreducible polynomials $g_j(t_1, \dots, t_r, y)$ and a polynomial

$\Phi(t_1, \dots, t_r) \neq 0$ such that if for some t'_1, \dots, t'_r all the polynomials $g_j(t'_1, \dots, t'_r, y)$ are irreducible and $\Phi(t'_1, \dots, t'_r) \neq 0$, then $f(t'_1, \dots, t'_r, x_1, \dots, x_s)$ is irreducible. In view of this fact it is sufficient to prove our Theorem for $s = 1$. We shall do that by induction with respect to n .

For $n = 1$ let

$$f_1(t_1, \dots, t_r, x) = f = \sum_{\nu=0}^j a_\nu(t_1, \dots, t_r) x^{j-\nu}.$$

By Lemma 1 of [5], for each positive integer $i \leq j$ there exists a polynomial $\Omega_{i,j}(u; v_1, \dots, v_j)$ with integer coefficients (the coefficient at the highest power of u being equal to 1) having the following property.

If $A(x), B(x)$ are arbitrary polynomials,

$$A(x) = \sum_{\nu=0}^j a_\nu x^{j-\nu}, \quad B(x) = \sum_{\nu=0}^h b_\nu x^{h-\nu}, \quad a_0 b_0 \neq 0, \quad h \geq i$$

and $B(x)$ divides $A(x)$, then

$$(7) \quad \Omega_{i,j} \left(\frac{b_i}{b_0}; \frac{a_1}{a_0}, \dots, \frac{a_j}{a_0} \right) = 0.$$

For $i \leq j$ let

$$(8) \quad \Omega_{i,j}(u; a_1(t_1, \dots, t_r), a_0(t_1, \dots, t_r) a_2(t_1, \dots, t_r), \dots, a_0(t_1, \dots, t_r)^{j-1} a_j(t_1, \dots, t_r)) \\ = F_i(t_1, \dots, t_r; u) \prod_{\mu=1}^{m_i} (u - \psi_{i,\mu}(t_1, \dots, t_r)),$$

where $m_i \geq 0$, F_i and $\psi_{i,\mu}$ ($1 \leq \mu \leq m_i$) are polynomials and for no polynomial $\varphi(t_1, \dots, t_r)$

$$F_i(t_1, \dots, t_r, \varphi(t_1, \dots, t_r)) = 0 \text{ identically.}$$

Since $F_i(t_1, \dots, t_r, u)$ has the coefficient at the highest power of u equal to 1, it follows that for no rational function $\varphi(t_1, \dots, t_r)$, $F_i(t_1, \dots, t_r, \varphi(t_1, \dots, t_r)) = 0$ identically, and thus for no rational function $\varphi(t_1, \dots, t_r)$,

$$(9) \quad \prod_{i=1}^j F_i(t_1, \dots, t_r, \varphi(t_1, \dots, t_r)) = 0 \text{ identically.}$$

Now, let i_0 be the least value of $i \leq j$ such that $m_i = 0$, if such values exist; otherwise let $i_0 = j$. For each positive integer $h < i_0$ and each system μ_1, \dots, μ_h , where $1 < \mu_i \leq m_i$ ($1 \leq i \leq h$) put

$$(10) \quad g_{\mu_1, \dots, \mu_h}(t_1, \dots, t_r, x) \\ = (a_0(t_1, \dots, t_r) x)^h + \sum_{i=1}^h \psi_{i,\mu_i}(t_1, \dots, t_r) (a_0(t_1, \dots, t_r) x)^{h-i}.$$

Since f is irreducible and $h < j$, the polynomials f and g_{μ_1, \dots, μ_h} are relatively prime; thus there exist polynomials $Q_{\mu_1, \dots, \mu_h}(t_1, \dots, t_r, x)$, $S_{\mu_1, \dots, \mu_h}(t_1, \dots, t_r, x)$ and $R_{\mu_1, \dots, \mu_h}(t_1, \dots, t_r)$ such that

$$(11) \quad Q_{\mu_1, \dots, \mu_h} f + S_{\mu_1, \dots, \mu_h} g_{\mu_1, \dots, \mu_h} = R_{\mu_1, \dots, \mu_h} \neq 0.$$

Now by Lemma 1 and (9) there exist r progressions P_1, \dots, P_r such that if $t_l \in P_l$ ($1 \leq l \leq r$), then

$$(12) \quad \alpha_0(t_1, \dots, t_r) z(t_1, \dots, t_r) \prod_{\substack{\mu_1, \dots, \mu_h \\ h < i_0}} R_{\mu_1, \dots, \mu_h}(t_1, \dots, t_r) \prod_{i=1}^j F_i(t_1, \dots, t_r, u) \neq 0$$

for all rational u .

We are going to prove that these progressions P_1, \dots, P_r have the properties required in the Theorem. Suppose, therefore, that for some t'_1, \dots, t'_r where $t'_l \in P_l$ ($1 \leq l \leq r$), $f(t'_1, \dots, t'_r, x)$ is reducible and divisible by a monic polynomial

$$(13) \quad g(x) = x^h + \sum_{\nu=1}^h \beta_\nu x^{h-\nu}, \quad \text{where } 1 \leq h < j.$$

By (12), $\alpha_0(t'_1, \dots, t'_r) \neq 0$. Put $\alpha_\nu = \alpha_\nu(t'_1, \dots, t'_r)$ ($0 \leq \nu \leq j$),

$$A(x) = \alpha_0^{j-1} f\left(t'_1, \dots, t'_r, \frac{x}{\alpha_0}\right) = x^j + \sum_{\nu=1}^j \alpha_0^{\nu-1} \alpha_\nu x^{j-\nu},$$

$$B(x) = \alpha_0^h g\left(\frac{x}{\alpha_0}\right) = x^h + \sum_{\nu=1}^h \alpha_0^\nu \beta_\nu x^{h-\nu}.$$

Clearly $B(x)$ divides $A(x)$, and by (7) for each $i \leq h$

$$\Omega_{i,j}(\alpha_0^i \beta_i; \alpha_1, \alpha_0 \alpha_2, \dots, \alpha_0^{j-1} \alpha_j) = 0.$$

By (8) and (12) it follows that $i_0 > 1$, $h < i_0$ and that for some system μ'_1, \dots, μ'_h

$$\alpha_0^i \beta_i = \psi_{i, \mu'_i}(t'_1, \dots, t'_r) \quad (1 \leq i \leq h, 1 \leq \mu'_i \leq m_i).$$

This gives by (13) and (10)

$$(14) \quad \begin{aligned} \alpha_0^h g(x) &= (\alpha_0 x)^h + \sum_{i=1}^h \psi_{i, \mu'_i}(t'_1, \dots, t'_r) (\alpha_0 x)^{h-i} \\ &= g_{\mu'_1, \dots, \mu'_h}(t'_1, \dots, t'_r, x). \end{aligned}$$

Since $h < j$, we have by (11) and (12)

$$Q_{\mu'_1, \dots, \mu'_h}(t'_1, \dots, t'_r, x) f(t'_1, \dots, t'_r, x) + S_{\mu'_1, \dots, \mu'_h}(t'_1, \dots, t'_r, x) g_{\mu'_1, \dots, \mu'_h}(t'_1, \dots, t'_r, x) = R_{\mu'_1, \dots, \mu'_h}(t'_1, \dots, t'_r) \neq 0.$$

It follows hence by (14) that $g(x)$ divides

$$R_{\mu'_1, \dots, \mu'_h}(t'_1, \dots, t'_r) \neq 0,$$

which is impossible.

The contradiction obtained completes the proof for $n = 1$. Assume now that the Theorem holds for $n - 1$ polynomials ($n > 1$) and that we are given n irreducible polynomials $f_m(t_1, \dots, t_r, x)$ ($1 \leq m \leq n$) and a polynomial $z(t_1, \dots, t_r)$ not identically 0. By the inductive assumption there exist r progressions, say $a_l u + b_l$ ($1 \leq l \leq r$), such that if $t'_l \equiv b_l \pmod{a_l}$ ($1 \leq l \leq r$) then $f_m(t'_1, \dots, t'_r, x)$ for $m < n$ are irreducible and $z(t'_1, \dots, t'_r) \neq 0$.

Now, $f_n(a_1 u_1 + b_1, \dots, a_r u_r + b_r, x)$ is an irreducible polynomial in u_1, \dots, u_r, x and therefore by the already proved case of our Theorem there exist r progressions, say $c_l v + d_l$ ($1 \leq l \leq r$), such that if $u'_l \equiv d_l \pmod{c_l}$ then $f_n(a_1 u'_1 + b_1, \dots, a_r u'_r + b_r, x)$ is irreducible. Denote by P_l the progression $a_l c_l v + (a_l d_l + b_l)$ ($1 \leq l \leq r$). If $t'_l \in P_l$, then the polynomials $f_m(t'_1, \dots, t'_r, x)$ ($1 \leq m \leq n$) are irreducible and $z(t'_1, \dots, t'_r) \neq 0$, which completes the inductive proof.

Since rational numbers belonging to a progression according to our definition form a dense set, we get

COROLLARY. *Let $f_m(t_1, \dots, t_r, x_1, \dots, x_s)$ ($1 \leq m \leq n$) be irreducible polynomials in $r + s$ variables. The set of all rational points (t'_1, \dots, t'_r) for which the polynomials $f_m(t'_1, \dots, t'_r, x_1, \dots, x_s)$ ($1 \leq m \leq n$) are irreducible contains a Cartesian product of r dense linear sets.*

As the second application of Lemma 1 we prove the following generalization of Theorem 1 in [1].

THEOREM 2. *Let $F(t_1, \dots, t_r, u)$ be a polynomial such that for no polynomial $\psi(t_1, \dots, t_r)$,*

$$F(t_1, \dots, t_r, \psi(t_1, \dots, t_r)) = 0$$

identically. There exist r arithmetical progressions P_1, \dots, P_r such that if $t_l \in P_l$ ($1 \leq l \leq r$), then

$$F(t_1, \dots, t_r, u) \neq 0 \quad \text{for all integers } u.$$

LEMMA 2. *Let $\varphi_m(t_1, \dots, t_r)$ ($1 \leq m \leq n$) be rational but not integer functions. There exist r arithmetical progressions P_1, \dots, P_r such that if $t_l \in P_l$, then neither of the numbers $\varphi_m(t_1, \dots, t_r)$ is an integer.*

Proof by induction with respect to n . For $n = 1$, let

$$\varphi_1(t_1, \dots, t_r) = \frac{g(t_1, \dots, t_r)}{h(t_1, \dots, t_r)},$$

where g, h are coprime polynomials with integer coefficients and h is not a constant. Without loss of generality we may assume that h is of positive degree in t_1 . Denote by $a_0(t_2, \dots, t_r)$ the coefficient at the highest power of t_1 in h .

Since $(g, h) = 1$, there exist polynomials $Q(t_1, \dots, t_r)$, $S(t_1, \dots, t_r)$ and $R(t_2, \dots, t_r)$ such that

$$(15) \quad Qg + Sh = R \neq 0.$$

Choose integers t'_2, \dots, t'_r so that $a_0(t'_2, \dots, t'_r)R(t'_2, \dots, t'_r) \neq 0$. Since $h(t_1, t'_2, \dots, t'_r)$ depends upon t_1 , there exists an integer t'_1 such that

$$c = |h(t'_1, \dots, t'_r)| > |R(t'_2, \dots, t'_r)|.$$

Denote by P_l the progression $cv + t'_l$ ($1 \leq l \leq r$). If $t_l \in P_l$ ($1 \leq l \leq r$), we have

$$h(t_1, \dots, t_r) \equiv h(t'_1, \dots, t'_r) \equiv 0 \pmod{c},$$

$$R(t_2, \dots, t_r) \equiv R(t'_2, \dots, t'_r) \not\equiv 0 \pmod{c}$$

and in view of (15)

$$g(t_1, \dots, t_r) \not\equiv 0 \pmod{c},$$

which proves that $g(t_1, \dots, t_r)/h(t_1, \dots, t_r)$ is not an integer.

Assume now that the Lemma is true for $n-1$ rational functions and that we are given n rational but not integer functions $\varphi_m(t_1, \dots, t_r)$ ($1 \leq m \leq n$). By the inductive assumption there exist r progressions, say $a_l u + b_l$ ($1 \leq l \leq r$), such that if $t_l \equiv b_l \pmod{a_l}$, then none of the numbers $\varphi_m(t_1, \dots, t_r)$ ($1 \leq m \leq n-1$) is an integer. Now $\varphi_n(a_1 u_1 + b_1, \dots, a_r u_r + b_r)$ is a rational but not an integer function of u_1, \dots, u_r , and therefore, by the already proved case of our Lemma, there exist r progressions, say $c_l v + d_l$ ($1 \leq l \leq r$), such that if $u_l \equiv d_l \pmod{c_l}$ then the number $\varphi_n(a_1 u_1 + b_1, \dots, a_r u_r + b_r)$ is not an integer. Denote by P_l the progression $a_l c_l v + (a_l d_l + b_l)$ ($1 \leq l \leq r$). If $t_l \in P_l$ ($1 \leq l \leq r$), then none of the numbers $\varphi_m(t_1, \dots, t_r)$ ($1 \leq m \leq n$) is an integer, which completes the inductive proof.

Proof of Theorem 2. By the assumption, polynomial F can be written in the form

$$F(t_1, \dots, t_r, u) = F_0(t_1, \dots, t_r, u) \prod_{m=1}^n (u - \varphi_m(t_1, \dots, t_r)),$$

where F_0 is a polynomial such that for no rational function φ , $F_0(t_1, \dots, t_r, \varphi(t_1, \dots, t_r)) = 0$ identically, $n \geq 0$ and φ_m ($1 \leq m \leq n$) are rational but not integer functions.

By Lemma 1 there exist r progressions, say $a_l u + b_l$ ($1 \leq l \leq r$), such that if $t_l \equiv b_l \pmod{a_l}$, then

$$F_0(t_1, \dots, t_r, u) \neq 0 \quad \text{for all rational } u.$$

By Lemma 2 there exist r progressions, say $c_l v + d_l$ ($1 \leq l \leq r$), such that if $u_l \equiv d_l \pmod{c_l}$, then none of the numbers $\varphi_m(a_1 u_1 + b_1, \dots, a_r u_r + b_r)$ ($1 \leq m \leq n$) is an integer. It follows that the progressions $a_l c_l v + (a_l d_l + b_l)$ ($1 \leq l \leq r$) have the properties required in the theorem.

The following modifications of Lemma 1 and Theorem 2 could seem plausible (cf. [6]).

M1. Let $F(t_1, \dots, t_r, u, v)$ be a polynomial such that for no pair of rational functions $\varphi(t_1, \dots, t_r)$, $\psi(t_1, \dots, t_r)$

$$(16) \quad F(t_1, \dots, t_r, \varphi(t_1, \dots, t_r), \psi(t_1, \dots, t_r)) = 0 \text{ identically.}$$

There exist r arithmetical progressions P_1, \dots, P_r (respectively an infinite set S of integer points) such that if $t_l \in P_l$ ($1 \leq l \leq r$) (respectively $(t_1, \dots, t_r) \in S$), then

$$F(t_1, \dots, t_r, u, v) \neq 0 \quad \text{for all rational } u, v.$$

M2. Let $F(t_1, \dots, t_r, u, v)$ be a polynomial such that for no pair of polynomials $\varphi(t_1, \dots, t_r)$, $\psi(t_1, \dots, t_r)$, (16) holds. There exist r arithmetical progressions P_1, \dots, P_r (respectively an infinite set S of integer points) such that if $t_l \in P_l$ ($1 \leq l \leq r$) (respectively $(t_1, \dots, t_r) \in S$), then

$$F(t_1, \dots, t_r, u, v) \neq 0 \quad \text{for all integers } u, v.$$

Now, the strong form of M1 and both forms of M2 are false, as shown by the examples $F_1(t, u, v) = t + u^2 + v^3$ and $F_2(t, u, v) = (2t - 1)u - (v^2 + 1)(v^2 + 2)(v^2 - 2)$, respectively. Indeed, as to the former, it is well known that the equation $3s^6 + u^2 + v^3 = 0$ is insoluble in rational u, v for every rational $s \neq 0$, which would not be possible if for some rational functions $\varphi(t)$, $\psi(t)$ we had an identity $F_1(t, \varphi(t), \psi(t)) = 0$.

On the other hand, if $av + b$ is an arbitrary progression P , then according to a well-known theorem (cf. [4]) there exist integers u_0, v_0 such that $-u_0^2 - v_0^3 \in P$ and thus for $t_0 = -u_0^2 - v_0^3$, $t_0 \in P$ and $F_1(t_0, u_0, v_0) = 0$.

As to the second counterexample, if for some polynomials $\varphi(t)$, $\psi(t)$ we had an identity $F_2(t, \varphi(t), \psi(t)) = 0$, then

$$\left(\psi\left(\frac{1}{2}\right)^2 + 1\right) \left(\psi\left(\frac{1}{2}\right)^2 + 2\right) \left(\psi\left(\frac{1}{2}\right)^2 - 2\right) = 0,$$

which is impossible. On the other hand, if t is any integer, we easily see by factorizing $2t-1$ into prime factors that the congruence

$$(v^2+1)(v^2+2)(v^2-2) \equiv 0 \pmod{2t-1}$$

is soluble and so is the equation $F_2(t, u, v) = 0$.

As to the weak form of M1, I am unable to disprove it and to prove it seems to me very difficult even for $r = 1$.

References

- [1] H. Davenport, D. J. Lewis and A. Schinzel, *Polynomials of certain special types*, Acta Arith. 9 (1964), pp. 107-116.
- [2] H. Hasse, *Zwei Bemerkungen zu der Arbeit „Zur Arithmetik der Polynome“ von U. Wegner in den Mathematischen Annalen Bd. 105, S. 628-631*, Math. Ann. 106 (1932), pp. 455-456.
- [3] S. Lang, *Diophantine Geometry*, New York 1962.
- [4] L. J. Mordell, *Note on cubic equations in three variables with an infinity of integer solutions*, Ann. Mat. Pura Appl. (4) 29 (1949), pp. 301-305.
- [5] A. Schinzel, *Reducibility of polynomials in several variables*, Bull. Acad. Polon. Sci., Ser. Sci. Math. Astr. Phys. 11 (1963), pp. 633-638.
- [6] — *Some unsolved problems on polynomials*, Matematička Biblioteka, Beograd, 25 (1963), pp. 63-70.

Reçu par la Rédaction le 31. 12. 1963
