Reprinted from JOURNAL OF NUMBER THEORY
All Rights Reserved by Academic Press, New York and London

Vol. 42, No. 2, October 1992
Printed in Belgium

On the Irreducibility of the Polynomials $P(t^m, Y)$

PIERRE DÈBES

Institut Henri Poincaré, 11, rue Pierre et Marie Curie,
75231 Paris Cedex 05, France

Communicated by M. Waldschmidt

Received April 15, 1991

We characterize the polynomials $P(X, Y)$ that are irreducible over a number field K and such that for some $t \in K$, the specialized polynomials $P(t^m, Y)$ are reducible in $K[Y]$ for infinitely many integers m. As a consequence, we show for example that if P is absolutely irreducible and if t is neither a strict power in K nor of the form $-4w^4$ or $-w^2$ with $w \in K$, then $P(t^m, Y)$ is irreducible in $K[Y]$ for infinitely many integers m (cf. Corollary 1.8). © 1992 Academic Press, Inc.

In this paper, we let $P = P(X, Y) \in \bar{\mathbf{Q}}(X)[Y]$ be a polynomial in Y, K be a number field, and t be an element of K. We assume that t is different from 0 and is not a root of unity, i.e., $t \in K^x \setminus \mu_\infty$. Our main results are of two types (labeled [1] and [2] below); they are complete characterisations of the couples (P, t) for which

[1] The equation $P(t^m, y) = 0$ has a solution $y \in K$ for infinitely many integers m.

[2] P is irreducible in $K(X)[Y]$ and the polynomial $P(t^m, Y)$ is reducible in $K[Y]$ for infinitely many integers m.

Problem [2] is the more interesting. Polynomials of the form $P(X, Y) = A(X, Y)^m - X$, with $A(X, Y) \in K(X)[Y]$, are good candidates; so are polynomials of the form $P(X, Y) = A(X, Y)^4 + 4X$. We will show that the solutions to problem [2] are the irreducible divisors of these polynomials. The main results (Theorems 1.1 and 1.2) and their consequences are precisely stated in Sect. 1. They should be regarded as irreducibility results for the specialized polynomials $P(t^m, Y)$ and thereby as new versions of Hilbert's irreducibility theorem (see in particular, Corollaries 1.7 and 1.8). Recall that Hilbert's irreducibility theorem [Hi, La2, Chap. 9] asserts that for any r polynomials $P_1(X, Y), \ldots, P_r(X, Y)$, irreducible in $K(X)[Y]$, there exist infinitely many $x \in K$ such that each of the polynomials $P_i(x, Y)$ is irreducible in $K[Y]$, $i = 1, \ldots, r$. Using Siegel's theorem on integral points

0022-314X/92 $5.00

on algebraic curves, one can show that, for all but finitely many $a \in K$, one can take x of the form $a + t^m$ (for $m \geqslant 1$) [Se, Chap. 9.7]. Here we improve on this result by specifying under what condition a can be taken to be 0. We also use Siegel's theorem but the reduction to it is different and requires some preliminary irreducibility results for the polynomials $P(X^m, Y)$ (Sect. 2). The proofs of Theorems 1.1 and 1.2 are given in Sect. 3.

Notation. If k is a field, $\mu_n(k)$ (or simply μ_n when there is no risk of confusion) denotes the set of all nth roots of unity in $\bar{k}$. The set μ_∞ is the union of all μ_n, for $n \in \mathbf{N}$. If T is an indeterminate, $k((T))$ denotes the field of formal power series in T with coefficients in k. If n is any integer, $T^{1/n}$ is a nth root of T in the algebraic closure $\overline{k(T)}$ of $k(T)$ and $\bar{k}(T^{1/\infty})$ denotes the union of all fields $\bar{k}(T^{1/n})$, for $n \in \mathbf{N}$. Unless otherwise specified, the word "polynomial" means "polynomial in the one variable Y." Polynomials are very often considered up to a nonzero constant, for example, in statements like "$P \in K(X)[Y]$." Also, we always assume that the specialized polynomials $P(x, Y)$ that we consider are defined, that is, x is not a pole of the coefficients in $\bar{k}(X)$ of the polynomial $P(X, Y)$.

The integer $e(P)$ that we now define is a controlling parameter for both our problems. Assume k has characteristic 0 and $P = P(X, Y) \in \bar{k}(X)[Y]$ ($\deg_Y P \geqslant 1$). The integer $e = e(P)$ is defined as the smallest integer such that the polynomial $P(X, Y)$ has a root in $\bar{k}((X^{1/e}))$ (existence of $e(P)$ follows from Puiseux's theorem).

Remarks. (a) Assume that P is irreducible in $\bar{k}(X)[Y]$ and consider the factorization of P in the u.f.d. $\bar{k}((X))[Y]$. The degrees of the irreducible polynomials in this factorization correspond to the multiplicities of the zeroes of the function x on a smooth model of the curve $P(x, y) = 0$. The integer $e(P)$ is the smallest of those integers.

(b) The integer $e(P)$ remains the same if $P(X, Y)$ is replaced by $P(aX, Y)$, for any $a \in \bar{k}$; the definition of $e(P)$ is geometric. This will be of frequent use throughout this paper.

(c) If P is irreducible in $\bar{k}(X)[Y]$, then P has a root in $\bar{k}(X^{1/\infty})$ iff it has a root in $\bar{k}(X^{1/e})$ iff all of its roots lie in $\bar{k}(X^{1/e})$ (where $e = e(P)$).

The central role played by the parameter $e = e(P)$ is revealed by the following lemma.

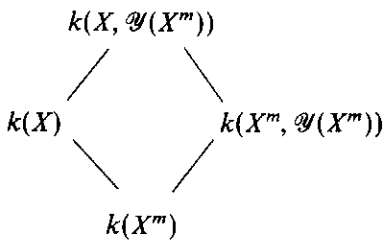
LEMMA 0.1. *Let $P = P(X, Y) \in k(X)[Y]$. The following statements are equivalent.*

(i) *$P(X^e, Y)$ is irreducible in $k(X)[Y]$.*

(ii) *$P(X^m, Y)$ is irreducible in $k(X)[Y]$ for all integers $m \geqslant 1$.*

Proof. Denote by P_e the polynomial $P_e(X, Y) = P(X^e, Y)$. Assume that P_e is irreducible in $k(X)[Y]$. Let $m \geq 1$ be an integer. We show below that the polynomial $P_e(X^m, Y) = P(X^{em}, Y)$ is irreducible in $k(X)[Y]$; this clearly implies that $P(X^m, Y)$ is irreducible in $k(X)[Y]$.

By definition, the polynomial P_e has a root in $\bar{k}((X))$. Denote this root by $\mathscr{Y}(X)$. Consider this diagram:



We have

$$[k(X^m, \mathscr{Y}(X^m)): k(X^m)] = [k(T, \mathscr{Y}(T)): k(T)] = \deg_Y P_e.$$

On the other hand, it follows from Eisenstein's criterion that the polynomial $T^m - X^m$ is irreducible in $\bar{k}((X^m))[T]$. In particular, we have

$$[k(X, \mathscr{Y}(X^m)): k(X^m, \mathscr{Y}(X^m))] = [k(X): k(X^m)] = m.$$

Consequently, one gets

$$[k(X, \mathscr{Y}(X^m)): k(X)] = \deg_Y P_e,$$

which means that $P_e(X^m, Y)$ is irreducible in $k(X)[Y]$.

1. Main Results and Consequences

1.1. *Statement of the Main Results*

Theorems 1.1 and 1.2 below relate respectively to problems labeled [1] and [2] in the introduction.

THEOREM 1.1. *Let $P = P(X, Y) \in \bar{\mathbf{Q}}(X)[Y]$, let K be a number field, and let $t \in K^x \setminus \mu_\infty$. Assume P is irreducible in $\bar{\mathbf{Q}}(X)[Y]$. The following statements are equivalent.*

(i) *The equation $P(t^m, y) = 0$ has a solution $y \in K$ for infinitely many integers m.*

(ii) *There exists an integer u such that the polynomial $P(t^u X^e, Y)$ has a root in $K(X)$.*

(iii) *The polynomial P is a degree e divisor in $K(X)[Y]$ of some polynomial of the form*

$$A(X, Y)^e - t^{-u}X \qquad \text{with} \quad A \in K(X)[Y] \text{ and } u \in \mathbf{N}$$

(where $e = e(P)$).

Notes. (a) We have assumed "P irreducible in $\bar{\mathbf{Q}}(X)[Y]$" so as to simplify the formulation of statement (iii). One may always restrict to this case when studying the equation $P(t^m, y) = 0$.

(b) The term "t^u" in statements (ii) and (iii) comes from the fact that if a polynomial $P(X, Y)$ satisfies condition (i), then so does any polynomial $P(t^u X, Y)$, with $u \in \mathbf{Z}$.

THEOREM 1.2. *Let K be a number field, let $P = P(X, Y) \in K(X)[Y]$, and let $t \in K^\times \setminus \mu_\infty$. Assume P is irreducible in $K(X)[Y]$. The following statements are equivalent.*

(i) *The polynomial $P(t^m, Y)$ is reducible in $K[Y]$ for infinitely many integers m.*

(ii) *There exists an integer u such that the polynomial $P(t^u X^e, Y)$ is reducible in $K(X)[Y]$ (where $e = e(P)$).*

(iii) *The polynomial P is a divisor in $K(X)[Y]$ of some polynomial of the form*

$$A(X, Y)^p - t^{-u}X$$

or

$$4A(X, Y)^4 + t^{-u}X,$$

where $A \in K(X)[Y]$, p is some prime number, and $u \in \mathbf{N}$.

The statements (ii) $\Rightarrow$ (i) (left to the reader) and (iii) $\Rightarrow$ (ii) (below) are the easy parts in both Theorems 1.1 and 1.2. The two converses are proved in Sects. 2 and 3.

Proof of (iii) $\Rightarrow$ (ii) *in Theorem* 1.2. We may assume that $u = 0$ in both conditions (ii) and (iii). What we actually prove is that condition (iii) implies that $P(X^p, Y)$ (or $P(X^4, Y)$) is reducible in $K(X)[Y]$; the conclusion (ii) then follows from Lemma 0.1. Of course, this is clear if the polynomial P is exactly of the given form. More generally, assume that P is a divisor of a polynomial of the given form. Let $\mathcal{Y}_P$ be a root in $\overline{K(X)}$ of the polynomial P.

1st case. P is a divisor of $A(X, Y)^p - X$. Then, the function field $K(X, \mathcal{Y}_P)$ contains a pth root $X^{1/p}$ of X. Thus we have

$$[K(X, \mathcal{Y}_P): K(X^{1/p})] = \deg_Y P/p < \deg_Y P.$$

Consequently, $P(X, Y)$ is reducible in $K(X^{1/p})[Y]$, or, equivalently, $P(X^p, Y)$ is reducible in $K(X)[Y]$.

Note. This last point is left to the reader. It will be of frequent use throughout the paper, just like this other similar one. For $P \in K(X)[Y]$ and $m \in \mathbf{N}$, the following statements are equivalent: (i) $P(X^m, Y)$ has a root in $K(X)$ and (ii) $P(X, Y)$ has a root in $K(X^{1/m})$, where $X^{1/m}$ is any mth root of X in $\overline{K(X)}$.

2nd case. P is a divisor of $4A(X, Y)^4 + X$. Then, the function field $K(i, X, \mathscr{Y}_P)$ contains a 4th root $X^{1/p}$ of X (note that $-4 = (1+i)^4$). Thus we have

$$[K(X^{1/4}, \mathscr{Y}_P): K(X^{1/4})] \leqslant [K(i, X, \mathscr{Y}_P): K(X^{1/4})] \leqslant 2 \deg_Y P/4 < \deg_Y P.$$

Consequently, $P(X, Y)$ is reducible in $K(X^{1/4})[Y]$, i.e., $P(X^4, Y)$ is reducible in $K(X)[Y]$.

The proof of (iii) $\Rightarrow$ (ii) in Theorem 1.1 can be worked out on similar principles.

Remark 1. In (iii) in both Theorems 1.1 and 1.2, the polynomial P may be only a strict divisor of some polynomial of the given form. In Sect. 2, we give an example of a polynomial P that has a root in $\bar{K}(X^{1/\infty})$ but is not of the form $A(X, Y)^\alpha - XB(X, Y)^\alpha$, for any $\alpha > 1$ and $A, B \in \bar{\mathbf{Q}}(X)[Y]$ (cf. Sect. 2.1).

1.2. *Consequences of Theorem* 1.1

The following conclusions about the equation $P(t^m, y) = 0$ should be drawn from Theorem 1.1.

COROLLARY 1.3. *Let $P = P(X, Y) \in \bar{\mathbf{Q}}(X)[Y]$, K be a number field, and $t \in K^\times \backslash \mu_\infty$. Assume that P is irreducible in $\bar{\mathbf{Q}}(X)[Y]$ and that the equation $P(t^m, y) = 0$ has a solution $y \in K$ for infinitely many integers m.*

Then, the following are true:

(a) *$P \in K(X)[Y]$ and $\deg_Y P = e(P)$.*

(b) *The equation $P(X, Y) = 0$ has a solution in $\bar{K}(X^{1/\infty})$.*

(c) *More precisely, there exists an integer u such that the roots $\mathscr{Y}_1, \ldots, \mathscr{Y}_e$ in $\overline{\mathbf{Q}(X)}$ of the polynomial P are the e $(= e(P))$ conjugates over $\bar{\mathbf{Q}}(X)$ of an element $\mathscr{Y}_1 \in K((t^{-u}X)^{1/e})$.*

(d) *Any field that contains K and the coefficients of $\mathscr{Y}_i$, regarded as a rational fraction in $X^{1/e}$, contains a eth root of t^u, $i = 1, \ldots, e$ (where u is any integer satisfying (c)).*

(e) *Let d be the smallest integer such that $t^d \in K^e$. Then, all but a finite number of those integers m for which $P(t^m, y) = 0$ has a solution $y \in K$ lie in a same coset modulo d (namely, the coset of u).*

Remark 2. Geometrically, the condition "$\deg_Y P = e(P)$" means that the function x has a unique zero on a smooth model of the algebraic curve $P(x, y) = 0$. It is also equivalent to the irreducibility of the polynomial P in $\bar{K}((X))[Y]$.

Remark 3. The integer d is defined in (e) as the smallest integer such that $t^d \in K^e$. Related to d are the integers

$$d' = [K(t^{1/e}): K] \qquad \text{and} \qquad d'' = [K(\mu_e, t^{1/e}): K(\mu_e)].$$

One can show that

$$d''/d/d'/e$$

and that these inequalities are strict in general. Thus, conclusion (e) of Corollary 1.3 is true with d deplaced by d'' (but not as good). It is false with d replaced by d' (take $P = Y^4 - X$ and $t = -9$ for which we have $e = 4$, $d = 2$, and $d' = 4$).

Remark 4. In (c), the integer u can be required to satisfy $0 \leqslant u < d$; then it is unique. More precisely, two integers u and v satisfying condition (c) are necessarily congruent modulo d. (Assume that the polynomial P has some root in $K((t^{-u}X)^{1/e})$ and some other one in $K((t^{-v}X)^{1/e})$. Set $P_1 = P(t^u X, Y)$. The polynomial $P_1(X, Y)$ has some root in $K(X^{1/e})$ and some other one in $K((t^{u-v}X)^{1/e})$. Conclusion (d) may be applied to the polynomial P_1: one gets that the field K contains an eth root of t^{u-v}. Consequently, $t^{u-v} \in K^e$ and $u \equiv v \ [\mathrm{mod}\ d]$.)

Proof of Corollary 1.3. We assume that condition (i) of Theorem 1.1 holds. Then (a) and (b) are part of (iii). Now, from (ii), there exists $u \in \mathbf{N}$ and $\mathscr{Z}(X) \in K(X)$ such that

$$(1) \quad P(t^u X^e, \mathscr{Z}(X)) = 0.$$

The rational fraction $\mathscr{Z}(X)$ can be written in a unique way:

$$\mathscr{Z}(X) = \sum_{i=0}^{e-1} x_i(X^e)\, X^i, \qquad \text{where} \quad x_i \in K(T),\ i = 0, \ldots, e-1.$$

Substituting an eth root $(t^{-u}X)^{1/e}$ of $(t^{-u}X)$ for X in (1) yields

$$P(X, \mathscr{Z}((t^{-u}X)^{1/e})) = 0.$$

Set $\mathscr{Y}_1 = \mathscr{Z}((t^{-u}X)^{1/e})$. The roots $\mathscr{Y}_1, ..., \mathscr{Y}_e$ in $\overline{\mathbf{Q}(X)}$ of the polynomial P are the e $(=e(P))$ conjugates over $\bar{\mathbf{Q}}(X)$ of $\mathscr{Y}_1$. For $i=1, ..., e$, $\mathscr{Y}_i$ is of the form

$$(2) \quad \mathscr{Y}_i = \sum_{i=0}^{e-1} x_i(t^{-u}X)\,\zeta^i(t^{-u}X)^{i/e}, \qquad \text{where} \quad \zeta \in \mu_e.$$

Let L be any field that contains the field K and the coefficients of $\mathscr{Y}_i$, regarded as a rational fraction in $X^{1/e}$. Then $\mathscr{Y}_i$ can be written in a unique way:

$$(3) \quad \mathscr{Y}_i = \sum_{i=0}^{e-1} y_i(X)\,X^{i/e}, \qquad \text{where} \quad y_i \in L(T),\ i=0, ..., e-1.$$

It follows from (2) and (3) that, for every index i such that $x_i \neq 0$, we have

$$\zeta^i(t^{-u})^{i/e} \in L.$$

But the indices i such that $x_i \neq 0$, together with the integer e, are relatively prime. Indeed, this follows from the minimality of the integer $e=e(P)$. Therefore, one obtains

$$\zeta(t^{-u})^{1/e} \in L.$$

This proves (d). It remains to prove (e). We may assume that $u=0$. Then it follows from Remark 4 that

(4) If $P(t^vX^e, Y)$ has a root in $K(X)$, then $v \equiv 0 \ [\mathrm{mod}\ d]$.

Now, let v be an integer such that $v \not\equiv 0 \ [\mathrm{mod}\ d]$. The polynomial $\hat{P} = P(t^vX^e, Y)$ has no root in $K(X)$. Applying Theorem 1.1 ((ii) $\Rightarrow$ (i)) to the polynomial $\hat{P}$ (note that $e(\hat{P})=1$) yields

(5) The equation $P(t^{v+me}, y)=0$ has a solution $y \in K$ for only finitely many integers m.

This concludes the proof of (e).

The following corollaries are consequences of conclusions (d) and (e) of Corollary 1.3.

COROLLARY 1.4. *Let $P=P(X, Y)$ be irreducible in $\bar{\mathbf{Q}}(X)[Y]$. Let K be a number field and t be an element of K that is not a strict power in K. Assume that the equation $P(t^m, y)=0$ has a solution $y \in K$ for all but finitely many integers m. Then* $\deg_Y P = 1$.

(Corollary 1.4 follows immediately from Corollary 1.3 (e).)

COROLLARY 1.5. *Let $P=P(X, Y)$ be irreducible in $\bar{\mathbf{Q}}(X)[Y]$ and K be a number field. Let t_1 and t_2 be two elements of K such that, for some choice of $t_2^{1/e}$, one has $K(t_2^{1/e}) \cap K(\mu_e, t_1^{1/e}) = K$. Let d_1 be the smallest integer such that $t_1^{d_1} \in K^e$. Assume that*

(*) *the equation* $P(t_1^m, y)=0$ *has a solution* $y \in K$ *for infinitely many integers* m *such that* $m \not\equiv 0 \pmod{d_1}$.

Then, the equation $P(t_2^m, y)=0$ *has a solution* $y \in K$ *for only finitely many integers* m.

For example, let $\mathscr{y} \in \mathbf{Q}(\sqrt{2X})\backslash\mathbf{Q}(X)$ and P be its irreducible polynomial over $\mathbf{Q}(X)$. The equation $P(2^m, y)=0$ has a solution $y \in \mathbf{Q}$ for infinitely many odd m. From Corollary 1.5, we may conclude that the same is true for the equation $P(t^m, y)=0$ iff $2t$ is a square in $\mathbf{Q}$.

Proof of Corollary 1.5. Assume that both $P(t_i^m, y)=0$, $i=1, 2$, have a solution $y \in K$ for infinitely many integers m. From Corollary 1.3, there exist two integers u_1 and u_2 such that the polynomial P has some root in $K((t_i^{-u_i}X)^{1/e}))$, $i=1, 2$. From Corollary 1.3 (d), we get

$$K(t_2^{u_2/e}) \supseteq K(\zeta' t_1^{u_1/e}) \qquad \text{for some} \quad \zeta' \in \mu_e.$$

It follows from the assumption on t_1 and t_2 that

$$K(\zeta' t_1^{u_1/e}) = K.$$

This shows that $t_1^{u_1} \in K^e$. Therefore $u_1 \equiv 0 \pmod{d_1}$ and the equation $P(t_1^m, y)=0$ has a solution $y \in K$ for infinitely many integers m such that $m \equiv 0 \pmod{d_1}$. But this, combined with Corollary 1.3 (e), contradicts assumption (*).

1.3. *Consequences of Theorem* 1.2

Theorem 1.2 contains the following irreducibility results.

COROLLARY 1.6. *Let* K *be a number field and* $P=P(X, Y) \in K(X)[Y]$.

(a) *Assume that the polynomial* $P(X^e, Y)$ *is irreducible in* $\bar{\mathbf{Q}}(X)[Y]$ (*i.e., absolutely irreducible*). *Then, for all* $t \in K^x \backslash \mu_\infty$, *the polynomial* $P(t^m, Y)$ *is irreducible for all but finitely many integers* m.

(b) *If* P *is irreducible in* $K(X)[Y]$ *and has a root in* $\bar{\mathbf{Q}}((X))$ (*i.e.,* $e=1$), *then, for all* $t \in K^x \backslash \mu_\infty$, *the polynomial* $P(t^m, Y)$ *is irreducible for all but finitely many integers* m.

Proof. (a) Only note that "$P(X^e, Y)$ irreducible in $\bar{\mathbf{Q}}(X)[Y]$" implies "$P(t^u X^e, Y)$ irreducible in $K(X)[Y]$ for all $t \in K$ and all $u \in \mathbf{Z}$." (b) corresponds exactly to the special case "$e=1$" of Theorem 1.2.

Note. Corollary 1.6.(a) is false if the polynomial $P(X^e, Y)$ is only

assumed to be irreducible in $K(X)[Y]$. (Consider for example the polynomial $P = Y^2 - 2X$.)

We now derive a new version of Hilbert's irreducibility theorem.

COROLLARY 1.7. *Let K be a number field, and $P_1, ..., P_n$ be n polynomials, irreducible in $K(X)[Y]$. Let $t \in K^x \setminus \mu_\infty$. Then there exists an integer s of K such that, for all but finitely many integers m, the polynomial $P_i(st^m, Y)$ is irreducible in $K[Y]$, $i = 1, ..., n$.*

The special case of Corollary 1.7 where $K = \mathbf{Q}$ and $t \in \mathbf{Z}$ was proved in [De2] in a completely effective way. The result here is more general but is not effective, due to ineffectiveness in Siegel's theorem. In [De2], one uses some of Sprindzuk's results [Sp, De1] instead. Corollary 1.7 shows in particular that Hilbert's irreducibility theorem is "compatible with the strong approximation theorem for algebraic numbers"; that is, there exist elements of K that satisfy simultaneously the conclusions of both theorems. This consequence of Corollary 1.7 was proved independently by Y. Morita [Mo]; we point out that in the case $K = \mathbf{Q}$, it was already contained in [De1, Sect. 3.3].

Proof of Corollary 1.7. In fact, we prove that, for sufficiently big m and with the extra assumption $\deg_Y P_i \geqslant 2$, $i = 1, ..., r$, the polynomial $P_i(st^m, Y)$ has no root in K for $i = 1, ..., n$. A standard argument (which is recalled in Sect. 3 (Proposition 3.1)) allows us to restrict to this weaker conclusion. One may also assume that the polynomials are irreducible in $\bar{\mathbf{Q}}(X)[Y]$: indeed, it is well known that if $P(X, Y)$ is irreducible in $K(X)[Y]$ but is not absolutely irreducible, the K-rational points (x, y) on the affine curve $P(x, y) = 0$ are singular points and so are in finite number. Now let f be the l.c.m. of the integers $e(P_1), ..., e(P_n)$ and τ be an fth root of t. The polynomials $P_1, ..., P_n$ are irreducible in $K(\tau)(X)[Y]$. From [De1, Sect. 3, Proposition 3], there exists an integer s of K such that the polynomials $P_1(sX^f, Y), ..., P_n(sX^f, Y)$ are irreducible in $K(\tau)(X)[Y]$: for example, one can take for s any sufficiently big prime number. Apply now Corollary 1.6 (b) to the data $(P_i(sX^f, Y), K(\tau), \tau)$, $i = 1, ..., n$. One gets that for all but finitely many integers m, the polynomial $P_i(s(\tau^m)^f, Y)$ is irreducible in $K(\tau)(X)[Y]$. In particular, for all but finitely many integers m, the equation $P_i(st^m, y) = 0$ has no solution $y \in K$, $i = 1, ... n$.

We end this section with a rather unexpected result. Its proof, which relies on some subsequent results, is given in Sect. 2.3.

COROLLARY 1.8. *Let K be a number field and $P = P(X, Y) \in K(X)[Y]$ be an absolutely irreducible polynomial. Let t be an element of K that is neither*

a strict power in K nor of the form $-4w^4$ with $w \in K$. Then the polynomial $P(t^m, Y)$ is irreducible in $K[Y]$ for infinitely many integers m (in fact, for all m in an arithmetic progression $(\alpha n + \beta)_{n \geq 0}$).

Remark 5. (a) Unlike Corollary 1.7, Corollary 1.8 does not extend to the case of several polynomials (think of $P_1 = Y^2 - X$, $P_2 = Y^2 - 2X$ and $t = 2$).

(b) The conclusion of Corollary 1.8 may be false for t of the form $-4w^4$ or $-w^2$ with $w \in K$. Take $P = Y^4 - X$ and $t = -4$. We have

$$P(t^{2m}, Y) = Y^4 - 2^{4m}$$
$$P(t^{2m+1}, Y) = Y^4 + 4.2^{4m}.$$

It follows from the reducibility in $\mathbf{Q}(X)[Y]$ of $Y^4 - X^4$ and $Y^4 + 4X^4$ that for all integers m, the polynomial $P(t^m, Y)$ is reducible in $\mathbf{Q}(X)[Y]$.

(c) Corollary 1.8 is false if the polynomial P is not assumed to be absolutely irreducible. For example, take for P the irreducible polynomial of $\sqrt{X} + \sqrt{2}$ over $\mathbf{Q}(X)$. The polynomials $P(X^2, Y)$ and $P(2X^2, Y)$ are reducible in $\mathbf{Q}(X)[Y]$: indeed, they have respectively $X + \sqrt{2}$ and $\sqrt{2}(1 + X)$ as a root, two elements of degree 2 over $\mathbf{Q}(X)$ whereas $\deg_Y P = 4$. Thus, for $t = 2$, the polynomial $P(t^m, Y)$ is reducible in $\mathbf{Q}(X)[Y]$, for all integers m.

2. The Polynomials $P(X^m, Y)$

2.1. *An iff Criterion for the Irreducibility of the Polynomial $P(X^m, Y)$*

For the rest of the paper, for P irreducible in $K(X)[Y]$, we denote by $\mathcal{Y}_P$, a root in $\overline{K(X)}$ of the polynomial P; note that $\mathcal{Y}_P$ is a primitive element over the field $K(X)$ of the function field

$$K(X)[Y]/P(K(X)[Y]).$$

In this section, the field K can be any field of characteristic 0.

Lemma 2.1. *Let $P = P(X, Y)$ be irreducible in $K(X)[Y]$ and $m \geq 2$ be an integer. The following statements are equivalent.*

(i) *The polynomial $P(X^m, Y)$ is reducible in $K(X)[Y]$.*

(ii) $X \in K(X, \mathscr{U}_p)^p$ *for some prime divisor* p *of* m, *or* $4/m$, *and* $X \in -4K(X, \mathscr{U}_p)^4$.

(iii) *The polynomial* P *is a divisor in* $K(X)[Y]$ *of some polynomial of the form*

$$A(X, Y)^p - X \qquad \text{for some prime divisor } p \text{ of } m$$

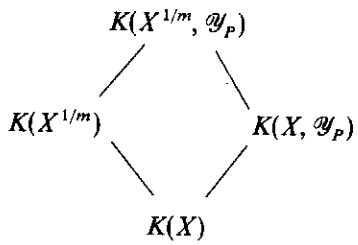
or (1)

$$4A(X, Y)^4 + X \qquad \text{and then } 4/m,$$

where $A \in K(X)[Y]$.

Note that (ii) $\Rightarrow$ (iii) in Theorem 1.2 is a consequence of Lemma 2.1.

Proof of Lemma 2.1. Consider the diagram



where $X^{1/m}$ denotes some mth root of X. The condition (i) is equivalent to

$$[K(X^{1/m}, \mathscr{U}_p): K(X^{1/m})] < [K(X, \mathscr{U}_p): K(X)]$$

or also to

$$[K(X^{1/m}, \mathscr{U}_p): K(X, \mathscr{U}_p)] < [K(X^{1/m})): K(X)].$$

This last condition is equivalent to the reducibility of the polynomial $T^m - X$ in $K(X, \mathscr{U}_p)[T]$. Thus, the equivalence between (i) and (ii) comes from Capelli's theorem [La1, Ch. VIII, Theorem 16]. Condition (iii) is a reformulation of condition (ii).

Assume $P(X^m, Y)$ is reducible in $K(X)[Y]$. Let p be any of the integers for which (1) holds (p is a prime number or $p = 4$). It follows from (ii) that $X \in \bar{K}(X, \mathscr{U}_p)^p$. The definitions of $e = e(P)$ and $\mathscr{U}_p$ then lead to

$$X \in \bar{K}((X^{1/e}))^p.$$

Therefore the integer p is necessarily a divisor of e (use the X-adic valuation). This shows that Lemma 2.1 contains Lemma 0.1 given in the

introduction. The following proposition summarizes the results of this section.

PROPOSITION 2.2. *Let $P=P(X, Y)$ be irreducible in $K(X)[Y]$. Then*

— Either $P(X^e, Y)$ is irreducible in $K(X)[Y]$ and then $P(X^m, Y)$ is irreducible in $K(X)[Y]$ for all integers m.

— Or, $P(X^e, Y)$ is reducible in $K(X)[Y]$ and then,

• There exists a divisor p of e such that p is a prime number or $p=4$ and $P(X^p, Y)$ is reducible in $K(X)[Y]$.

•• $P(X^m, Y)$ is reducible in $K(X)[Y]$ iff m is a multiple of some integer p that satisfies •. In particular, if $(e, m)=1$, then $P(X^m, Y)$ is irreducible in $K(X)[Y]$.

2.2. *An Example*

We indicated previously that in Lemma 2.1(iii), the polynomial P may be only a strict divisor of some polynomial of the given form. We will actually prove a little bit more. We give an example of a polynomial $P=P(X, Y)\in\mathbf{Q}(X)[Y]$, absolutely irreducible, which has a root in $\mathbf{Q}(X^{1/\infty})$ but is not of the form $A(X, Y)^d-XB(X, Y)^d$ with $d>1$ and A and B in $\bar{\mathbf{Q}}(X)[Y]$ (up to a constant in $\bar{\mathbf{Q}}(X)$).

EXAMPLE. Let P be the irreducible polynomial over $\bar{\mathbf{Q}}(X)$ of $\mathscr{Y}_P=X^{1/9}+X^{2/9}-X^{3/9}$. It is easily checked that $\mathbf{Q}(X, \mathscr{Y}_P)=\mathbf{Q}(X^{1/9})$, so $[\mathbf{Q}(X, \mathscr{Y}_P)\colon \mathbf{Q}(X)]=[\bar{\mathbf{Q}}(X, \mathscr{Y}_P)\colon \bar{\mathbf{Q}}(X)]=\deg_Y P=9$ and that $e=9$. Note then that if P is of the form $A(X, Y)^d-XB(X, Y)^d$ with $d>1$, then $P(X^d, Y)$ is reducible in $\bar{\mathbf{Q}}(X)[Y]$. Therefore, from Proposition 2.2, it suffices to prove that P is not of the given form for $d=3$. So assume that the polynomial P can be written

$$P(X, Y)=(a_3Y^3+a_2Y^2+a_1Y+a_0)^3-X(b_3Y^3+b_2Y^2+b_1Y+b_0)^3,$$

where $a_i, b_i\in\bar{\mathbf{Q}}(X)$. Then the polynomial $P(X^3, Y)$ splits as

$$\begin{aligned}P(X^3, Y)=&\left[Y^3+\frac{a_{23}-Xb_{23}}{a_{33}-Xb_{33}}Y^2+\frac{a_{13}-Xb_{13}}{a_{33}-Xb_{33}}Y+\frac{a_{03}-Xb_{03}}{a_{33}-Xb_{33}}\right]\\&\times\left[Y^3+\frac{a_{23}-jXb_{23}}{a_{33}-jXb_{33}}Y^2+\frac{a_{13}-jXb_{13}}{a_{33}-jXb_{33}}Y+\frac{a_{03}-jXb_{03}}{a_{33}-jXb_{33}}\right]\\&\times\left[Y^3+\frac{a_{23}-j^2Xb_{23}}{a_{33}-j^2Xb_{33}}Y^2+\frac{a_{13}-j^2Xb_{13}}{a_{33}-j^2Xb_{33}}Y+\frac{a_{03}-j^2Xb_{03}}{a_{33}-j^2Xb_{33}}\right],\end{aligned}$$

where

$$\begin{aligned}a_{i3}&=a_i(X^3)\\b_{i3}&=b_i(X^3)\end{aligned}\qquad\text{for}\quad i=0, 1, 2.$$

Now, the polynomial is also divisible in $\bar{\mathbf{Q}}(X)[Y]$ by the irreducible polynomial over $\bar{\mathbf{Q}}(X)$ of

$$\mathscr{Y}_p(X^3) = X^{1/3} + X^{2/3} - X.$$

Some calculations show that this polynomial is

$$(Y+2X)^3 - X(Y+X+1)^3$$
$$= (1-X)[Y^3 + 3XY^2 + 3X(X-1)\,Y + X(X^2-4X-1)].$$

Up to the constant $1-X$, this polynomial must be one of the three factors of $P(X^3, Y)$ above. With no loss of generality one may assume that it is the first one. Hence, one gets

$$\frac{a_{23} - Xb_{23}}{a_{33} - Xb_{33}} = 3X$$

$$\frac{a_{13} - Xb_{13}}{a_{33} - Xb_{33}} = 3X^2 - 3X$$

$$\frac{a_{03} - Xb_{03}}{a_{33} - Xb_{33}} = X(X^2 - 4X - 1).$$

The first two equations can be rewritten as

$$a_{23} - (b_{23} + 3a_{33})\,X + b_{33}X^2 = 0$$
$$(a_{13} + 3X^3 b_{33}) + (3a_{33} - b_{13})\,X - 3(a_{33} + b_{33})\,X^2 = 0.$$

Since $1, X, X^2$ are linearly independent over $\bar{\mathbf{Q}}(X^3)$, we must have $a_{33} = b_{33} = 0$, i.e., $a_3 = b_3 = 0$, whence a contradiction.

2.3. *Proof of Corollary* 1.8

We prove that under the assumptions of Corollary 1.8, the polynomial $P(t^m, Y)$ is irreducible in $K[Y]$ for all m in an arithmetic progression $(\alpha n + \beta)_{n \geq 0}$. From Corollary 1.6(b), it suffices to show that there exists an integer β such that the polynomial $P(t^\beta X^e, Y)$ is irreducible in $K(X)[Y]$; one may then take $\alpha = e = e(P)$.

Let L be the set consisting of all the divisors p of e such that p is a prime or $p = 4$. Let $p \in L$; from Lemma 2.1, if $P(t^u X^p, Y)$ is reducible in $K(X)[Y]$, then

$$\begin{aligned} &t^{-u}X \in (K(X, \mathscr{Y}_p))^p && \text{if } p \text{ is a prime} \\ &t^{-u}X \in -4(K(X, \mathscr{Y}_p))^4 && \text{if } p = 4. \end{aligned} \tag{2}$$

Now let two elements u and v be such that $P(t^uX^p, Y)$ and $P(t^vX^p, Y)$ are reducible in $K(X)[Y]$. Assume $p \neq 4$ (the case $p=4$ is similar). It follows from (2) that $t^{v-u} \in (K(X, \mathscr{Y}_P))^p$, or, equivalently, the field $K(X, \mathscr{Y}_P)$ contains a pth root $t^{(v-u)/p}$ of t^{v-u}. But $P(X, Y)$ is assumed to be absolutely irreducible; equivalently, the field $K(X, \mathscr{Y}_P)$ is a regular extension of K (i.e., $K(X, \mathscr{Y}_P) \cap \bar{K} = K$). Therefore we get $t^{(v-u)/p} \in K$. But, due to our assumptions and Capelli's theorem [La1, Ch. VII, Sect. 9, Theorem 16], we have $[K(t^{1/p}): K] = p$. So we have necessarily $u \equiv v \pmod p$.

We have shown that for all $p \in L$, there exists an integer u_p with the following property: if u is any integer such that $u \not\equiv u_p \pmod p$, then the polynomial $P(t^uX^p, Y)$ is irreducible in $K(X)[Y]$. Let β be an integer such that $\beta \not\equiv u_p \pmod p$ for all $p \in L$ (existence of β is an easy consequence of the Chinese remainder theorem). Then for all $p \in L$, the polynomial $P(t^\beta X^p, Y)$ is irreducible in $K(X)[Y]$. From Proposition 2.2 (applied to the polynomial $P(t^\beta X, Y)$), the polynomial $P(t^\beta X^e, Y)$ is necessarily irreducible in $K(X)[Y]$.

3. Proof of the Main Results

3.1. *The Diophantine Ingredient*

The following lemma is a consequence of Siegel's finiteness result on the integral points on algebraic curves. We give a rapid proof. The details can be found in [Se]. The field K is a number field. The set of all absolute values of K is denoted by M_K.

Lemma 3.1. *Let C be a quasi-affine curve defined over K and $\bar{C}$ be a complete smooth model of C. Let S be a finite subset of M_K that contains all the archimedean absolute values of K. Let x be a function on C defined over K. Assume that the subset $x^{-1}(0, \infty)$ of $\bar{C}$ contains at least 3 points. Then there are only finitely many $M \in C(K)$ (i.e., K-rational points M on C) such that $|x(M)|_v = 1$, for all $v \notin S$.*

Proof. Recall that if X is a quasi-affine variety defined over K, a subset of χ of $X(K)$ is said to be quasi-integral on X relatively to S if, for all f in the coordinate ring of X, there exists $a \in K$ such that $|af(M)|_v \leqslant 1$, for all $M \in \chi$ and all $v \notin S$. Let

$$P_S = \{x \in K \mid |x|_v = 1 \text{ for all } v \notin S\}.$$

The set P_S is quasi-integral on $\mathbf{P}_1 \backslash \{0, \infty\}$ relatively to S: indeed, the coordinate ring of the affine subset $\mathbf{P}_1 \backslash \{0, \infty\}$ is generated by x and $1/x$. Then consider the quasi-affine subset of C:

$$C_{\text{aff}} = \bar{C} \backslash x^{-1}(0, \infty).$$

The morphism $x: \bar{C} \to \mathbf{P}_1$ induced by x on $\bar{C}$ is a finite morphism. Thus, C_{aff} is an affine subset of C; furthermore, the set

$$\mathscr{C}_S = C_{\text{aff}}(K) \cap x^{-1}(P_S)$$

is quasi-integral on C_{aff} relatively to S [Se, Chap. 8.1]. Now $\bar{C}$ is a complete smooth model of C_{aff}; the set of points at infinity on C_{aff} is the set $\bar{C} \setminus C_{\text{aff}} = x^{-1}(0, \infty)$. From the assumption, it consists of at least 3 points. From Siegel's theorem, the set $\mathscr{C}_S$ is a finite set.

3.2. *Proof of Theorem* 1.1

We are given a polynomial $P = P(X, Y) \in \bar{\mathbf{Q}}(X)[Y]$, absolutely irreducible, a number field K, and $t \in K^x \setminus \mu_\infty$.

(i) $\Rightarrow$ (ii). We distinguish two cases.

1st case. $e = e(P) = 1$. Denote the affine curve $P(x, y) = 0$ by C and a smooth projective model of C by $\bar{C}$. Let L be a field that contains K and such that $P \in L(X)[Y]$. Let S be the subset of M_L of all absolute values of L such that v is archimedean or $|t|_v \neq 1$. The condition (i) implies that there are infinitely many L-rational points M on C such that $|x(M)|_v = 1$ for all $v \notin S$. From Lemma 3.1, the subset $x^{-1}(0, \infty)$ of $\bar{C}$ consists of at most 2 points. But, due to the assumption "$e = 1$," the function x has a simple zero on $\bar{C}$ (cf. Remark 1(a)). Conclude that the function x is of degree 1 on C. Equivalently, $\deg_Y P = 1$; i.e., P has a root $\mathscr{Y} \in L(X)$. It remains to show that P has a root in $K(X)$. This readily follows of "$\mathscr{Y}(t^m) \in K$ for infinitely many integers m."

2nd case. General case. Let f be the smallest integer such that the polynomial $P(X, Y)$ has all of its roots in $\bar{\mathbf{Q}}((X^{1/f}))$. Condition (i) implies that there exists an integer u such that the equation $P(t^u(t^m)^f, Y) = 0$ has a solution $y \in K$ for infinitely many integers m. Consider a factorization

$$P(t^u X^f, Y) = P_1(X, Y) \cdots P_r(X, Y)$$

of the polynomial $P(t^u X^f, Y)$ in the u.f.d. $\bar{\mathbf{Q}}(X)[Y]$. For some index i, the equation $P_i(t^m, y) = 0$ has a solution $y \in K$ for infinitely many integers m. Applying the preceding case to the polynomial P_i, for which $e(P_i) = 1$, yields the required conclusion.

Remark. The reduction to the first case can be regarded as some version of an idea of Neron [La2, Chap. 9, Sect. 1]. Given $P(X, Y) \in K(X)[Y]$, Neron introduces the curve $C_\varphi: P(\varphi(x), y) = 0$, a pull-back of the curve $P(x, y) = 0$, where the polynomial $\varphi(X) \in \mathbf{Z}[X]$ is chosen so that the genus of C_φ is >0. Then Siegel's theorem yields that for all but finitely many integers x of K, the polynomial $P(\varphi(x), Y)$ has no root in K. Here,

the idea is to consider the pull-back $P(x^f, y)=0$ of the curve $P(x, y)=0$. That way, we are reduced to a situation where the set $x^{-1}\{0, \infty\}$ consists of at least 3 points and so where Siegel's theorem can be applied as well. One can also, like in [Se, Chap. 9.7], change x into $x+a$; for some suitable a, one gets $|x^{-1}\{0, \infty\}| \geqslant 3$ as well. But this change is inadequate here for it moves out the origin of $\mathbf{P}_1$; one obtains results on polynomials $P(a+t^m, Y)$ (and not $P(t^m, Y)$).

(ii) $\Rightarrow$ (iii). We may assume $u=0$, i.e., that the polynomial $P(X^e, Y)$ has a root in $K(X)$. Equivalently, the polynomial $P(X, Y)$ has a root $\mathscr{Y}_P$ in $K(X^{1/e})$. This root can be written

$$\mathscr{Y}_P = \mathscr{Z}(X^{1/e}), \qquad \text{where} \quad \mathscr{Z}(T)=\sum_{i=0}^{e-1} \mathscr{Z}_i(X)\, T^i \in K(X)[T].$$

The conjugates of $\mathscr{Y}_P$ over $K(X)$ are the elements

$$\mathscr{Z}(\zeta X^{1/e}),$$

where ζ runs over the set μ_e of eth roots of 1. These conjugates are distinct. Indeed, if $\mathscr{Z}(\zeta X^{1/e})=\mathscr{Z}(\zeta' X^{1/e})$, then every index i such that $\mathscr{Z}_i(X)\neq 0$ must be a multiple of the order $\zeta^{-1}\zeta'$. Since, from the definition of e, these indices together with the integer e are relatively prime, we get that $\zeta=\zeta'$. Thus, we conclude that $[K(X, \mathscr{Y}_P): K(X)]=e$ and so that

$$K(X, \mathscr{Y}_P) = K(X^{1/e}).$$

This shows in particular that the polynomial P is a degree e polynomial with coefficients in $K(X)$. It can also be derived that for some polynomial $A \in K(X)[Y]$,

$$X^{1/e} = A(X, \mathscr{Y}_P).$$

The polynomial $A(X, Y)^e - X$ is then a multiple in $K(X)[Y]$ of the polynomial P.

(iii) $\Rightarrow$ (i) was proved in Sect. 1.1.

3.3. *Proof of Theorem* 1.2

We are given a number field K, $t \in K^\times \backslash \mu_\infty$, and a polynomial $P=P(X, Y)$ irreducible in $K(X)[Y]$. (iii) $\Rightarrow$ (i) and (ii) $\Rightarrow$ (iii) were respectively proved in Sects. 1.1 and 2.1 (cf. Lemma 2.1). It remains to prove (i) $\Rightarrow$ (ii).

Let f be the smallest integer such that the polynomial $P=P(X, Y)$ has all of its roots in $\bar{\mathbf{Q}}((X))$. The condition (i) implies that there exists an integer u such that the polynomial $P(t^u(t^m)^f, Y)$ is reducible in $K(X)[Y]$

for infinitely many integers m. Let $\bar{P} = P(t^u X^f, Y)$; the polynomial $\bar{P}$ has this property:

(1) The polynomial $\bar{P}(t^m, Y)$ is reducible in $K(X)[Y]$ for infinitely many integers m.

Next we are going to use this standard result (e.g., [La, Chap. 9, Sect. 1]).

PROPOSITION 3.1. *Let $\bar{P}$ be an irreducible polynomial in $K(X)[Y]$ and $\overline{K(X, \mathscr{Y}_P)}^n$ be its splitting field over $K(X)$. Then there exists a finite set $\chi = \chi(\bar{P})$ of elements $\mathscr{Y}$ in $\overline{K(X, \mathscr{Y}_P)}^n \backslash K(X)$ with the following property. For each $\mathscr{Y} \in \chi$, denote its irreducible polynomial over $K(X)$ by $M_{\mathscr{Y}}$. Then, for all but finitely many $x \in K$, we have this conclusion*:

(2) *If $\bar{P}(x, Y)$ is reducible in $K(X)[Y]$, then there exists $\mathscr{Y} \in \chi$ such that the polynomial $M_{\mathscr{Y}}(x, Y)$ has a root in K.*

Assume that our polynomial $\bar{P}$ is irreducible in $K(X)[Y]$. Then it follows from (1) and Proposition 3.1 that there exists $\mathscr{Y} \in \chi(\bar{P})$ such that

(3) The polynomial $M_{\mathscr{Y}}(t^m, Y)$ has a root in K for infinitely many integers m.

The polynomial $M_{\mathscr{Y}}$ is then necessarily absolutely irreducible (see proof of Corollary 1.7 for more details on the argument). Next observe that $\deg_Y M_{\mathscr{Y}} \geqslant 2$, whereas $e(M_{\mathscr{Y}}) = 1$ (by choice of f). Corollary 1.3(a) provides a contradiction. So we conclude that the polynomial $\bar{P} = P(t^u X^f, Y)$ is reducible in $K(X)[Y]$. From Lemma 0.1, the polynomial $P(t^u X^e, Y)$ is reducible in $K(X)[Y]$ as well.

REFERENCES

[De1] P. DÈBES, G-fonctions et théorème d'irréductibilité de Hilbert, *Acta Arith.* **47** (1986).

[De2] P. DÈBES, Parties hilbertiennes et progressions géométriques, *C.R. Acad. Sci. Paris Sér. I* **302** (1986).

[Hi] D. HILBERT, Uber die Irreduzibilität ganzer rationaler Funktionen mit ganzahligen Koeffizienten, *J. angew. Math.* **110** (1892), 104–129.

[La1] S. LANG, "Algebra," Addison-Wesley, New York, 1965.

[La2] S. LANG, "Fundamentals of Diophantine Geometry," Springer-Verlag, Berlin, 1983.

[Mo] Y. MORITA, A note on the Hilbert Irreducibility Theorem, *Proc. Japan Acad. Ser. A* **66** (1990).

[Se] J.-P. SERRE, "Lectures on the Mordell-Weil Theorem," translated by M. Brown from notes by M. Walschmidt, Vieweg, 1990.

[Sp] V. G. SPRINDZUK, Arithmetic specializations in polynomials, *J. Reine Angew. Math.* **340** (1983), 26–52.

Printed by Catherine Press, Ltd., Tempelhof 41, B-8000 Brugge, Belgium