ACTA ARITHMETICA
LXX.3 (1995)

Factorisation in fractional powers

by

A. J. van der Poorten (Sydney, N.S.W.)

This note provides a uniform bound for the number of irreducible factors of $f(x_1^{q_1},\dots,x_n^{q_n})$, where f is an irreducible polynomial defined over a field of characteristic zero and not effectively just in one variable, and $q_1,\dots,q_n$ are arbitrary positive integers. The argument derives from that of Ritt [2], where it arises in studying factorisation in the ring of exponential polynomials.

Let $g(x_1,\dots,x_n)$ be a polynomial and let $q_1,\dots,q_n$ be positive integers. One says that a polynomial $f(x_1,\dots,x_n)$ is *primary in* x_1 if an identity $f(x_1,\dots,x_n) = g(x_1^{q_1},x_2,\dots,x_n)$ entails $q_1 = 1$, and that $f(x_1,\dots,x_n)$ is *primary* (thus, in each of its variables) if an identity $f(x_1,\dots,x_n) = g(x_1^{q_1},\dots,x_n^{q_n})$ entails $q_1 = \dots = q_n = 1$. We use the term *monomial* in $x_1,\dots,x_n$ for a rational function $x_1^{a_1}\dots x_n^{a_n}$ with integral, but not necessarily nonnegative, exponents.

Suppose that a polynomial f in several variables is the product of a monomial and of a polynomial in some monomial z in those variables. In that case, f is effectively just a polynomial in the one variable z; we will refer to it in that way.

Theorem. *Let $f(x_1,\dots,x_n)$ be an irreducible primary polynomial of multi-degree $d_1,\dots,d_n$ defined over a field $\mathbb{F}$ of characteristic zero, and suppose that f is not effectively just a polynomial in one variable. Then for each $i\in\{1,\dots,n\}$ there is a pair (i,j) with $i\neq j\in\{1,\dots,n\}$ so that, viewed as a polynomial in just x_i and x_j, the polynomial $f(x_1,\dots,x_n)\equiv f_{i,j}(x_i,x_j)$ is not effectively just a polynomial in one variable. Moreover, $f(x_1,\dots,x_n)$ has a factorisation into irreducibles in the ring generated over the ground field by all fractional powers of the variables $x_1,\dots,x_n$. The number of such irreducible factors does not exceed $\min d_id_j$, with the minimum taken over the pairs (i,j) described above.*

1991 *Mathematics Subject Classification*: Primary 11B37.

Work supported in part by grants from the Australian Research Council and a research agreement with Digital Equipment Corporation.

The core of the proof is the following proposition dealing with the seemingly easier case of an irreducible primary polynomial in just two variables defined over an algebraically closed field.

Proposition. *Let $f(x,y)$ be an irreducible primary polynomial of bidegree d_x, d_y defined over an algebraically closed field $\mathbb{K}$ of characteristic zero. Suppose $f(x,y)$ has at least three terms. Then $f(x,y)$ has at most $d_x d_y$ factors over $\mathbb{K}$ in fractional powers of x and y.*

Proof. Let p and q be an arbitrary pair of positive integers. We study factorisations in $\mathbb{K}[x,y]$ of the polynomial $f(x^p,y^q)$. Our plan is first to refine the selection of the integers p and q, replacing them by integers p' and q', divisors of p and q respectively, so that $f(x^{p'},y^{q'})$ has a primary irreducible factor. We then bound the number of primary irreducible factors of $f(x^{p'},y^{q'})$.

Accordingly, let $g(x,y^{q_1})$ denote an irreducible factor of $f(x,y^q)$ so that $g(x,y)$ is primary in y. Further, let ζ_q be a qth root of unity and consider the polynomial $g(x,\zeta_q^{q_1}y^{q_1})$ obtained by replacing y by $\zeta_q y$. Since the substitution leaves $f(x,y^q)$ invariant it is evident that $g(x,\zeta_q^{q_1}y^{q_1})$ divides $f(x,y^q)$.

Suppose $\zeta_q^{q_1} \neq 1$. It is immediate that the polynomials $g(x,y^{q_1})$ and $g(x,\zeta_q^{q_1}y^{q_1})$ are distinct, and that they are coprime. For if not, there is a factor $A(x,y^q)$ of $g(x,y^{q_1})$, and that contradicts the irreducibility of $g(x,y^{q_1})$, or the primality of $g(x,y)$ in y.

It follows similarly that as we vary our choice of ζ_q we obtain $q/(q,q_1)$ distinct and coprime polynomials $g(x,\zeta_q^{q_1}y^{q_1})$. We claim that their product is $f(x,y^q)$, up to multiplication by a nonzero constant. Indeed, this product is invariant under each substitution $y \mapsto \zeta_q y$, ζ_q a qth root of unity, and so is a polynomial $G(x,y^q)$ which divides the polynomial $f(x,y^q)$. But then $G(x,y)$ divides $f(x,y)$. Thus the irreducibility of $f(x,y)$ entails our claim. Conversely, because $G(x,y^q)$ is invariant under each substitution $y \mapsto \zeta_{q_1} y$, ζ_{q_1} a q_1th root of unity, so is $f(x,y^q)$ up to multiplication by a constant. Thus, because $f(x,y)$ is primary, we learn that q_1 divides q.

We have observed that, up to multiplication by a nonzero constant, $f(x,y^q)$ is given by

$$\prod g(x,\zeta_{q/q_1}y^{q_1}),$$

with the product running over the distinct (q/q_1)th roots of unity ζ_{q/q_1}. Moreover, we see that $g(x,y)$ is primary (that is, also primary in x) since otherwise this product representation contradicts the primality of $f(x,y)$ in x.

By a similar argument, $g(x^p,y)$ is given, again up to multiplication by a nonzero constant, by

$$\prod h(\zeta_{p/p_1}x^{p_1},y),$$

with the polynomial $h(x,y)$ irreducible and primary.

By our construction, $h(x^{p_1}, y)$ is irreducible. Symmetry suggests that so is $h(x, y^{q_1})$. Indeed, if $b(x, y)$ is a proper factor of $h(x, y^{q_1})$ then $b(x^{p_1}, y)$ is a proper factor of $h(x^{p_1}, y^{q_1})$. Then $\prod h(\zeta_{p/p_1} x^{p_1}, y^{q_1}) = cg(x^p, y^{q_1})$, c some nonzero constant, has a proper factor $B(x^p, y) = \prod b(\zeta_{p/p_1} x^{p_1}, y)$. This entails that $B(x, y)$ is a proper factor of $g(x, y^{q_1})$, contradicting the irreducibility of $g(x, y^{q_1})$.

Accordingly, we shall study the factor $h(x^{p_1}, y^{q_1})$ in place of $f(x^p, y^q)$. The advantage gained is that both $h(x^{p_1}, y)$ and $h(x, y^{q_1})$ are irreducible.

It will be useful to notice that $g(x, y)$ has bi-degree $(q_1/q)d_x, d_y$ and therefore that $h(x, y)$ has bi-degree $(q_1/q)d_x, (p_1/p)d_y$.

Suppose now that $k(x^{p_2}, y^{q_2})$ is an irreducible factor of $h(x^{p_1}, y^{q_1})$, with $k(x, y)$ primary. Repeating the opening argument shows that q_2 divides q_1 and that, with the product running over the (q_1/q_2)th roots of unity ζ_{q_1/q_2},

$$K(x^{p_2}, y^{q_1}) = \prod k(x^{p_2}, \zeta_{q_1/q_2} y^{q_2})$$

divides $h(x^{p_1}, y^{q_1})$. So $K(x^{p_2}, y)$ is a factor of the irreducible polynomial $h(x^{p_1}, y)$; hence the two polynomials differ only by multiplication by a nonzero constant.

It follows that p_2 divides p_1. Accordingly we make $p_2 = 1$ by replacing p by p/p_2 and thus p_1 by p_1/p_2 throughout. Of course, similarly, or by symmetry, we may choose to make $q_2 = 1$ by replacing q by q/q_2 and thus q_1 by q_1/q_2 throughout. After these replacements, our choice of p and q is now such that $f(x^p, y^q)$ has an irreducible factor $k(x, y)$, primary in both variables.

By arguments already reported above, it follows that because $k(x, y)$ is primary the p_1 polynomials $k(\zeta_{p_1} x, y)$, as ζ_{p_1} runs through the p_1th roots of unity, are distinct and coprime and their product $L(x^{p_1}, y)$ is a factor of $h(x^{p_1}, y^{q_1})$. Thus $L(x, y)$ is a factor of the irreducible polynomial $h(x, y^{q_1})$ and must coincide with it up to multiplication by a nonzero constant.

Suppose that $k(x, y)$ has bi-degree ∂_x, ∂_y. Then $\partial_x = (q_1/q)d_x$ because that is the degree of $h(x, y^{q_1})$ in x. By symmetry we must also have $\partial_y = (p_1/p)d_y$. Above we saw that $h(x^{p_1}, y)$ is given by the product $\prod k(x, \zeta_{q_1} y)$, up to multiplication by a nonzero constant. Hence $q_1 \partial_x = p_1 (q_1/q) d_x$. We can conclude that $p_1 = q_1$.

For notational convenience we sometimes write $p_1 = q_1 = t$ in the sequel. We also note that we have shown that $k(x, y)$ has bi-degree $(t/q)d_x, (t/p)d_y$.

Collecting our result thus far, we see that up to multiplication by a nonzero constant, the polynomial $f(x^p, y^q)$ is a product of pqt^{-1} polynomials each of the shape $k(\zeta_p x, \zeta_q y)$, with ζ_p a pth root of unity and ζ_q a qth root of unity. Our adjusting the choice of p and q by setting $p_2 = q_2 = 1$ is vindicated in that otherwise $f(x^p, y^q)$ does not have a factor that is primary in both its variables.

It is immediate that $f(x^p, y^q)$ has a factorisation in at most pqt^{-1} irreducible polynomials. We recall that $k(x,y)$ is one such factor and notice that it follows that all the factors are primary.

Now we invoke the assumption that $f(x,y)$ has at least three terms, whence, being irreducible, it is not effectively just a polynomial in one variable, that is, it is not the product of a polynomial in a monomial z in x and y and of a monomial w in x and y.

We claim that $k(x,y)$ has at least three terms $c_i x^{\alpha_i} y^{\beta_i}$, $i = 1,2,3$, so that the determinant

$$\begin{vmatrix} \alpha_1 & \beta_1 & 1 \\ \alpha_2 & \beta_2 & 1 \\ \alpha_3 & \beta_3 & 1 \end{vmatrix}$$

is nonzero. If not, then $k(x,y)$ is of the shape $wl(z)$ with l a polynomial over $\mathbb{K}$ and w and z monomials in x and y. Thus by the product representation above, $f(x^p, y^q)$ is a polynomial which may be written as a product of a power of w and of a polynomial in z, contradicting either its irreducibility over $\mathbb{K}$ or that it has at least three terms.

Hence the 2×2 determinant

$$\Delta = \begin{vmatrix} \alpha_1 - \alpha_3 & \beta_1 - \beta_3 \\ \alpha_2 - \alpha_3 & \beta_2 - \beta_3 \end{vmatrix}$$

does not vanish. However, the bi-degree of $k(x,y)$ is $(t/q)d_x, (t/p)d_y$. It follows that the absolute value of this determinant does not exceed $(t^2/(pq))d_x d_y$. Indeed, without loss of generality, $\alpha_1 \ge \alpha_2 \ge \alpha_3$. If $(\beta_1 - \beta_3)(\beta_2 - \beta_3) \ge 0$ we are done. If not, then

$$|\Delta| = (\alpha_1 - \alpha_3)|\beta_2 - \beta_3| + (\alpha_2 - \alpha_3)|\beta_1 - \beta_3| \le (q_1/q)d_x|\beta_2 - \beta_1|$$

and again we have our claim.

Now let ζ denote a primitive tth root of unity. Then with $v = 0, 1, \ldots \ldots, t-1$ the product of the t polynomials $k(\zeta x, \zeta^v y)$ yields the polynomial $h(x^{p_1}, y^{q_1}) = h(x^t, y^t)$ up to multiplication by a nonzero constant. Because $k(x,y)$ is an irreducible factor of $h(x^{p_1}, y^{q_1})$, for $v = u$, say, we must have $k(\zeta x, \zeta^u y) = ck(x,y)$, with the constant c some power of ζ. This remark is

$$\begin{pmatrix} \alpha_1 - \alpha_3 & \beta_1 - \beta_3 \\ \alpha_2 - \alpha_3 & \beta_2 - \beta_3 \end{pmatrix} \begin{pmatrix} 1 \\ u \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{t}.$$

It follows that

$$\begin{vmatrix} \alpha_1 - \alpha_3 & \beta_1 - \beta_3 \\ \alpha_2 - \alpha_3 & \beta_2 - \beta_3 \end{vmatrix} \equiv 0 \pmod{t},$$

so, given our bound on the absolute value of the determinant, we have shown that

$$t \le \frac{t^2}{pq} d_x d_y \quad \text{which is} \quad pq \le t d_x d_y.$$

Because t is a common divisor of p and q, this yields a bound on p and q of the desired kind. Indeed, the bound for the number of irreducible factors of $f(x^p, y^q)$ is pqt^{-1}, and this is at most $d_x d_y$. Since that quantity is independent of our choice of p and q this proves the Proposition. ∎

Turning to the proof of the Theorem we first verify the opportunity to select suitable pairs of variables $x_i = x$ and $x_j = x_{j(i)} = y$, say. We write $f(x_1, \dots, x_n) = \sum f_\mu \mathbf{x}^\mu$ and observe that given the variable $x_i = x$ there are triples of exponent vectors μ_1, μ_2 and μ_3, say, so that the pair $\mu_1 - \mu_3$, $\mu_2 - \mu_3$ is linearly independent and its coordinates belonging to x are distinct. Because of that linear independence, there is some other variable $x_j = y$, say, so that disregarding all but the coordinates belonging to x and y, the two exponent vectors remain linearly independent. Thus, on viewing $f(x_1, \dots, x_n)$ as a polynomial $f(x, y)$ in just the two variables x and y we see that $f(x, y)$ retains the property that it is not the product of a monomial and of a polynomial in a monomial in its variables. Of course it must then have at least three terms.

Hence we may view $f(x_1, \dots, x_n)$ as a polynomial $f(x, y)$ in just two variables over the field $\mathbb{L}$ of rational functions over $\mathbb{F}$ in the remaining $n-2$ variables. Then $f(x, y)$ is primary since the original polynomial is primary, and it is irreducible over $\mathbb{L}$, for, in effect by Gauß's lemma, any factorisation of $f(x, y)$ over $\mathbb{L}$ entails a factorisation of the irreducible polynomial $f(x_1, \dots, x_n)$ over the base field $\mathbb{F}$.

As it is our ultimate object to find a bound, independent of $(q_1, \dots, q_n)$, on the number of irreducible factors of any polynomial $f(x_1^{q_1}, \dots, x_n^{q_n})$ there is no loss in our viewing $f(x, y)$ as defined over the algebraic closure $\mathbb{K}$ of the field $\mathbb{L}$ of rational functions over $\mathbb{F}$ in the $n-2$ variables other than x and y. For, plainly, our doing so can only increase the number of its possible factors.

On the other hand, in order to apply the Proposition we must also show that we do not need $f(x, y)$ to be irreducible over $\mathbb{K}$. To see we may do that, suppose that

$$f(x, y) = f_1(x, y) \dots f_m(x, y),$$

with irreducible factors of respective bi-degrees $d_x^{(1)}, d_y^{(1)}, \dots, d_x^{(m)}, d_y^{(m)}$. Because $f(x, y)$ is irreducible over $\mathbb{L}$, these factors over the algebraic closure $\mathbb{K}$ of $\mathbb{L}$ must retain the property of not decomposing as the product of a monomial in x and y and a polynomial in a monomial in x and y. For, plainly, the f_i are conjugate over some algebraic extension of $\mathbb{L}$, and if one were effectively just a polynomial in one variable then f would itself be effectively just a polynomial in one variable, contradicting the choice of x, y from $\{x_1, \dots, x_n\}$. Hence, applied to each irreducible factor $f_i(x, y)$ over $\mathbb{K}$, the Proposition shows that $f(x,y)$ itself has at most

$$d_x^{(1)}d_y^{(1)}+\cdots+d_x^{(m)}d_y^{(m)}\le(d_x^{(1)}+\cdots+d_x^{(m)})(d_y^{(1)}+\cdots+d_y^{(m)})=d_xd_y$$

factors in fractional powers of x and y.

We now note that on returning to the original data we may renumber the variables so that, say, $x=x_1$ and $y=x_2$. Then we will have shown that, over $\mathbb{K}$ and hence a fortiori over $\mathbb{F}$, $f(x,y)=f(x,y,x_3,\ldots,x_n)$ of bi-degree d_x,d_y, has at most d_xd_y factors in fractional powers of x and y and in $x_3,\ldots,x_n$. This result is, of course, independent of the degrees $d_3,\ldots,d_n$ of the remaining variables. It follows that we have this same bound for the number of factors of $f(x,y,x_3^{q_3},\ldots,x_n^{q_n})$, with arbitrary positive integers $q_3,\ldots,q_n$ and once again in fractional powers of x and y and in $x_3,\ldots,x_n$, completing the proof of the Theorem. ■

Remarks. First a few caveats. One would like to state the Theorem for an arbitrary polynomial f, but it remains essential that f not have any factor that is "essentially just a polynomial in a single variable"; hence our insisting that f be irreducible. Equally, the restriction to characteristic zero seems unfortunate. In the alternative situation one should note that the present argument falters whenever distinct factors are claimed, and fails if the characteristic divides t at the assertion that one obtains *distinct* divisors of $h(x^t,y^t)$. However, the fact that $f(x^l,y^l)=(f(x,y))^l$ for polynomials f over the finite field $\mathbb{F}_l$ of l elements is, essentially, the only difficulty. In those terms it is easy to see from the present argument, let alone the careful details of [3], that only the restriction that the characteristic not divide t is required to obtain for arbitrary characteristic a result similar to that of the Theorem.

As said, our argument derives from that of Ritt [2]. A little more is needed to obtain the results cited and demonstrated by Schinzel [3], see pages 101–113, and attributed primarily to Gourin [1]. However, one can see from our argument, in passing, the extra feature that $f(x_1^{q_1},\ldots,x_n^{q_n})$ has a factorisation in distinct irreducibles and that each factor contains every one of the variables.

I am grateful to Graham Everest whose questions about factorisation in the ring of exponential polynomials led to my constructing the present argument, and to the extensive advice of an anonymous referee which led to my refining and correcting it.

References

[1] E. Gourin, *On irreducible polynomials in several variables which become reducible when the variables are replaced by powers of themselves*, Trans. Amer. Math. Soc. 32 (1930), 485–501.

[2] J. F. Ritt, *A factorisation theory for functions* $\sum_{i=1}^{n} a_i e^{\alpha_i z}$, ibid. 29 (1927), 584–596.

[3] A. Schinzel, *Selected Topics on Polynomials*, University of Michigan Press, Ann Arbor, 1982.

CENTRE FOR NUMBER THEORY RESEARCH
MACQUARIE UNIVERSITY
SYDNEY, NEW SOUTH WALES 2109, AUSTRALIA
E-mail: ALF@MPCE.MQ.EDU.AU

Received on 1.8.1994 (2653)