Journal of Algebra 343 (2011) 138–142

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

A polynomial Zsigmondy theorem

Anthony Flatters, Thomas Ward *

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, UK

ARTICLE INFO

Article history:
Received 2 March 2010
Available online 3 August 2011
Communicated by Efim Zelmanov

MSC:
11A41
11B39

Keywords:
Zsigmondy theorem
Polynomial ring
Primitive divisor

ABSTRACT

We find an analogue of the primitive divisor results of Bang and Zsigmondy in polynomial rings.

1. Introduction

A prime divisor of a term A_n of a sequence $(A_n)_{n\geqslant 1}$ in a unique factorization domain is called primitive if it divides no earlier term. The classical Zsigmondy theorem [6], generalizing earlier work of Bang [1] in the case $b = 1$, shows that every term beyond the sixth in the sequence $(a^n - b^n)_{n\geqslant 1}$ has a primitive divisor (where $a > b > 0$ are coprime integers). Results of this form are important in group theory and in the theory of recurrence sequences (see the monograph [2, Sect. 6.3] for a discussion and references).

Our purpose here is to consider similar questions in polynomial rings. The arguments used follow well-established lines with some modifications needed to avoid terms in the sequence where the Frobenius automorphism precludes primitive divisors. We show that every term beyond the second admits a primitive divisor. Related results for Lucas sequences and elliptic divisibility sequences in function fields have recently been found by Ingram, Mahé, Silverman, Stange, Streng [3].

* Corresponding author.
E-mail address: t.ward@uea.ac.uk (T. Ward).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2011.07.010

2. Polynomial analogues

Let k be a field, and consider a sequence $(F_n)_{n\geqslant 1}$ of elements of $k[T]$. Since $k[T]$ is a unique factorization domain, each term of the sequence factorizes into a product of irreducible polynomials over k, so we may ask which terms have an irreducible factor which is not a factor of an earlier term. Irreducible factors with this property will be called *primitive prime divisors*. As usual, we write $\mathrm{ord}_\pi h$ (or $\mathrm{ord}_p n$) for the maximal power to which an irreducible π divides h in $k[T]$ (or to which a rational prime p divides n in $\mathbb{Z}$).

The specific sequence we are interested in has $F_n = f^n - g^n$, where f, g are non-zero, coprime polynomials in $k[T]$ which are not both units.

Lemma 2.1. *If $\pi \in k[T]$ is an irreducible dividing F_n for some $n \geqslant 1$, then for* $\mathrm{char}(k) = p > 0$,

$$\mathrm{ord}_\pi(F_{mn}) = p^{\mathrm{ord}_p(m)}\,\mathrm{ord}_\pi(F_n),$$

and for $\mathrm{char}(k) = 0$,

$$\mathrm{ord}_\pi(F_{mn}) = \mathrm{ord}_\pi(F_n),$$

for any $m \geqslant 1$.

Proof. We may write

$$f^n - g^n = \pi^{\mathrm{ord}_\pi(F_n)} Q$$

for some $Q \in k[T]$ with $\pi \nmid Q$. Write $a = \mathrm{ord}_\pi(F_n)$, so

$$f^{mn} = \left(g^n + \pi^a Q\right)^m = g^{mn} + \sum_{i=1}^{m} \binom{m}{i} \pi^{ai} Q^i g^{n(m-i)}.$$

Thus

$$F_{mn} = m\pi^a g^{n(m-1)} Q + \sum_{i=2}^{m} \binom{m}{i} \pi^{ai} Q^i g^{n(m-i)}.$$

We deduce that if $\mathrm{char}(k) = p > 0$, then for $p \nmid m$ (or for $\mathrm{char}(k) = 0$),

$$\mathrm{ord}_\pi(F_{mn}) = \mathrm{ord}_\pi(F_n).$$

Now suppose that $m = p^e k$ with $e > 0$ and $p \nmid k$. Then, for $\mathrm{char}(k) = p > 0$,

$$f^{nm} - g^{nm} = \left(f^{nk} - g^{nk}\right)^{p^e}.$$

Now $\mathrm{ord}_\pi(F_{nk}) = \mathrm{ord}_\pi(F_n)$ since $p \nmid k$, so $\mathrm{ord}_\pi(F_{mn}) = p^e\,\mathrm{ord}_\pi(F_n)$ as required. □

Recall that a sequence (F_n) is a divisibility sequence if $F_r \mid F_s$ whenever $r \mid s$, and is a strong divisibility sequence if $\gcd(F_r, F_s) = F_{\gcd(r,s)}$ for all $r, s \geqslant 1$.

Proposition 2.2. *The sequence $(F_n)_{n\geqslant 1}$ is a strong divisibility sequence.*

Before we prove this we require a few subsidiary results. Recall from [4, Prop. 2.13] the following basic properties of the resultant of two homogeneous polynomials.

Proposition 2.3. *Write*

$$A(X,Y)=a_0\prod_{j=1}^{n}(X-\alpha_j Y)$$

and

$$B(X,Y)=b_0\prod_{j=1}^{m}(X-\beta_j Y)$$

for some $\alpha_j,\beta_j\in\bar{k}$. *Then*

$$\operatorname{Res}(A,B)=a_0^n b_0^m\prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j).$$

Moreover, there exists homogeneous polynomials $F_1(X,Y)$, $G_1(X,Y)$ *of degree* $m-1$ *and homogeneous polynomials* $F_2(X,Y)$, $G_2(X,Y)$ *of degree* $n-1$ *in* $\mathbb{Z}[a_0,\dots,a_n,b_0,\dots,b_m][X,Y]$ *with the property that*

$$F_1A+G_1B=\operatorname{Res}(A,B)X^{m+n-1},$$
$$F_2A+G_2B=\operatorname{Res}(A,B)Y^{m+n-1}.$$

We now proceed with the proof of Proposition 2.2. For $c\in\mathbb{N}$ write

$$P_c(X,Y)=\frac{X^c-Y^c}{X-Y}=\sum_{i=0}^{c-1}X^{c-1-i}Y^i.$$

Lemma 2.4. *Let* m,n *be positive coprime integers. Then* $\operatorname{Res}(P_m,P_n)=\pm1$.

Proof. Notice that (by the definition of the resultant as a determinant)

$$\operatorname{Res}(A,B)\in\mathbb{Z}[a_0,\dots,a_n,b_0,\dots,b_m];$$

moreover the statement of the lemma is independent of the characteristic, so we may work in characteristic zero without loss of generality.

By Proposition 2.3 we have $\operatorname{Res}(P_m,P_n)=\prod_{i=1}^{n-1}\prod_{j=1}^{m-1}(\zeta_n^i-\zeta_m^j)$ where ζ_d denotes any choice of primitive dth root of unity. Thus each factor in the product takes the form $\zeta_{n'}-\zeta_{m'}$ for $m',n'>1$ divisors of m, n respectively. Now

$$\zeta_{m'}-\zeta_{n'}=\zeta_{m'}(1-\overline{\zeta_{m'}}\zeta_{n'}),$$

and, since m', n' are coprime, $1-\overline{\zeta_{m'}}\zeta_{n'}=1-\eta_{m'n'}$ for some primitive $m'n'$th root of unity $\eta_{m'n'}$. Since $m'n'$ has at least two distinct prime factors, it follows from [5, Prop. 2.8] that $1-\eta_{m'n'}$ is a unit in $\mathbb{Z}[\zeta_{m'n'}]$. Hence $\operatorname{Res}(P_m,P_n)$ is a product of units and is thus a unit. Since $\operatorname{Res}(P_m,P_n)\in\mathbb{Z}$, this means that $\operatorname{Res}(P_m,P_n)\in\{\pm1\}$. □

Corollary 2.5. *Let f, g be coprime elements of a unique factorization domain R. Then for positive coprime integers m, n, $P_m(f,g)$, $P_n(f,g)$ are coprime.*

Proof. From Proposition 2.3, we see that the ideal I of R generated by $P_m(f,g)$ and $P_n(f,g)$ contains f^{m+n-1} and g^{m+n-1}. Since f^{m+n-1}, g^{m+n-1} are coprime, it follows that $1 \in I$, and the result follows. $\square$

We now have all that is needed to prove strong divisibility.

Proof of Proposition 2.2. Let $d = \gcd(m,n)$. We note that

$$f^m - g^m = \left(f^d - g^d\right) P_{m/d}\left(f^d, g^d\right)$$

and

$$f^n - g^n = \left(f^d - g^d\right) P_{n/d}\left(f^d, g^d\right).$$

Now from Corollary 2.5 we see that $P_{m/d}(f^d, g^d)$ and $P_{n/d}(f^d, g^d)$ are coprime, and the result follows. $\square$

We will also make use of the following simple observation. Let K be a field, and let $\Phi_d \in K[x,y]$ denote the dth homogeneous cyclotomic polynomial. Then if $n > 2$ and f, g are not both units of $K[x]$, $\Phi_n(f,g)$ is not a unit of $K[x]$. To see this note that $\Phi_n(f,g)$ is a unit of $K[x]$ if and only if $f - \zeta g$ is a unit for all $\phi(n)$ primitive nth roots of unity ζ. This is clearly impossible if $\phi(n) \geqslant 2$ and at least one of the polynomials f, g is a non-unit.

The preparatory results Lemma 2.1, Proposition 2.2 and the observation above combine to give a polynomial form of Zsigmondy's theorem as follows.

Theorem 2.6. *Suppose* $\mathrm{char}(k) = p > 0$, *and let F' be the sequence obtained from $(F_n)_{n\geqslant 1}$ by deleting the terms F_n with $p \mid n$. Then each term of F' beyond the second has a primitive prime divisor. If* $\mathrm{char}(k) = 0$, *then the full sequence $(F_n)_{n\geqslant 1}$ has the property that all terms beyond the second have a primitive prime divisor.*

Proof. Notice that

$$F_n = \prod_{d|n} \Phi_d(f,g), \tag{1}$$

and so

$$\Phi_n(f,g) = \prod_{d|n} F_d^{\mu(n/d)}$$

by Möbius inversion. Thus

$$\mathrm{ord}_\pi\left(\Phi_n(f,g)\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \mathrm{ord}_\pi(F_d) \tag{2}$$

for any prime $\pi \in k[T]$. Suppose now that π is a prime divisor of F_n which is not primitive, so that $\pi \mid F_m$ for some $m < n$ chosen to be minimal with that property. Then $m \mid n$ by Proposition 2.2 and

$$\mathrm{ord}_\pi(F_{mk}) = \mathrm{ord}_\pi(F_m)$$

for any k with $p \nmid k$, by Lemma 2.1. In addition, we claim that it follows that $\operatorname{ord}_\pi(F_c) = 0$ unless m divides c. Suppose that this were not the case. Then $\operatorname{ord}_\pi(F_c) > 0$ for some c with $m \nmid c$, and Proposition 2.2 yields $\pi \mid F_{\gcd(m,c)}$. However, since $m \nmid c$, $\gcd(m, c) < m$, so this contradicts the minimality of m. Thus (2) gives

$$\begin{aligned}
\operatorname{ord}_\pi\bigl(\Phi_n(f,g)\bigr) &= \sum_{d \mid \frac{n}{m}} \mu\left(\frac{n}{dm}\right) \operatorname{ord}_\pi(F_{dm}) \\
&= \sum_{d \mid \frac{n}{m}} \mu\left(\frac{n}{dm}\right) \operatorname{ord}_\pi(F_m) \\
&= \operatorname{ord}_\pi(F_m) \sum_{d \mid \frac{n}{m}} \mu\left(\frac{n}{dm}\right) = 0
\end{aligned}$$

as $m < n$. We deduce that any non-primitive prime divisor of F_n does not divide $\Phi_n(f, g)$. As remarked earlier, $\Phi_n(f, g)$ is non-constant for $n > 2$, and so $\Phi_n(f, g)$ has a prime divisor in $k[T]$. Therefore, as any prime divisor of $\Phi_n(f, g)$ is primitive, every term in P beyond the second has a primitive prime divisor. The proof for the characteristic zero case follows in exactly the same way. □

We end by recording three simple observations that arise from this argument.

1. If $\operatorname{char}(k) \neq 2$ and $f + g$ is non-constant, then the second term of (F_n) has a primitive prime divisor.
2. Eq. (1) shows a little more: any primitive prime divisor of F_n must divide $\Phi_n(f, g)$, and so the *primitive part* (that is, the product of all the primitive prime divisors to their respective powers) of F_n is $\Phi_n(f, g)$. This gives a lower bound for the size of the primitive part F_n^* of F_n under the assumption that $\deg(f) \neq \deg(g)$:
$$\deg\bigl(F_n^*\bigr) = \phi(n) \max\bigl\{\deg(f), \deg(g)\bigr\} > n^{1-\delta} \max\bigl\{\deg(f), \deg(g)\bigr\}$$
for any $\delta > 0$ and large enough n.
3. Since $F_{pc} = (F_c)^p$ for $c \geqslant 1$, any term with index divisible by p fails to have a primitive prime divisor, so the terms with index divisible by p must be removed.

Acknowledgment

The authors thank Min Sha for helpful suggestions, and in particular for removing an assumption on the characteristic in Proposition 2.2.

References

[1] A.S. Bang, Taltheoretiske undersølgelser, Tidskrifft Math. 5 (1886) 70–80, 130–137.
[2] G. Everest, A. van der Poorten, I. Shparlinski, T. Ward, Recurrence Sequences, Math. Surveys Monogr., vol. 104, American Mathematical Society, Providence, RI, 2003.
[3] P. Ingram, V. Mahé, J.H. Silverman, K. Stange, M. Streng, Algebraic divisibility sequences over function fields, arXiv:1105.5633, 2011.
[4] J.H. Silverman, The Arithmetic of Dynamical Systems, Grad. Texts in Math., vol. 241, Springer, New York, 2007.
[5] L.C. Washington, Introduction to Cyclotomic Fields, Grad. Texts in Math., vol. 83, Springer-Verlag, New York, 1982.
[6] K. Zsigmondy, Zur Theorie der Potenzreste, Monatsh. Math. 3 (1892) 265–284.