Polynomial Zsigmondy theorems

Anthony Flatters, Thomas Ward

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

Abstract

We find analogues of the primitive divisor results of Zsigmondy, Bang, Bilu–Hanrot–Voutier, and Carmichael in polynomial rings, following the methods of Carmichael.

Keywords: Zsigmondy theorem, Polynomial ring, Primitive divisor

2010 MSC: 11A41, 11B39

A prime divisor of a term $a_n$ of a sequence $(a_n)_{n \geq 1}$ is called primitive if it divides no earlier term. The classical Zsigmondy theorem [4], generalizing earlier work of Bang [1] (in the case $b = 1$), shows that every term beyond the sixth in the sequence $(a^n - b^n)_{n \geq 1}$ 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 [3, Sect. 6.3] for a discussion and references).

Our purpose here is to consider similar questions in polynomial rings. The method of Carmichael [2] is used to find analogous results, with some modifications needed to avoid terms in the sequence where the Frobenius automorphism precludes primitive divisors. In even characteristic the results take a slightly different form, and an analogue of Bang’s theorem is found here.

1. Polynomial analogues

Let $k$ be a field (of odd characteristic, unless stated otherwise), and consider a sequence $(f_n)_{n \geq 1}$ 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 $\text{ord}_\pi f$ (or $\text{ord}_p n$) for the maximal power to which an irreducible $\pi$ divides $f$ 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 $k[T]$.
Lemma 1.1. If $\pi \in k[T]$ is an irreducible dividing $f_n$ for some $n \geq 1$, then for $\text{char}(k) = p > 0$,

$$\text{ord}_\pi(f_{mn}) = p^\text{ord}_p(m) \text{ord}_\pi(f_n),$$

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

$$\text{ord}_\pi(f_{mn}) = \text{ord}_\pi(f_n).$$

Proof. We may write

$$f_n - g_n = \pi^{\text{ord}_\pi(f_n)}Q$$

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

$$f_{mn} = (g^n + \pi^aQ)^m = g^{mn} + \sum_{i=1}^m \binom{m}{i} \pi^aQ^i g^{n(m-i)}.$$

Thus

$$f_{mn} = m g^{n(m-1)} + \sum_{i=2}^m \binom{m}{i} \pi^aQ^i g^{n(m-i)}. \quad (1)$$

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

$$\text{ord}_\pi(f_{mn}) = \text{ord}_\pi(f_n).$$

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

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

Now $\text{ord}_\pi(f_{nk}) = \text{ord}_\pi(f_n)$ since $p \nmid k$, so $\text{ord}_\pi(f_{mn}) = p^e \text{ord}_\pi(f_n)$ as required.

Recall that a sequence $(f_n)$ is a divisibility sequence if $f_r | f_s$ whenever $r | s$, and is a strong divisibility sequence if $\gcd(f_r, f_s) = f_{\gcd(r,s)}$ for all $r, s \geq 1$.

Lemma 1.2. The sequence $(f_n)_{n \geq 1}$ is a strong divisibility sequence.

Proof. Fix $m, n \in \mathbb{N}$, and let $\ell = \gcd(m, n)$. It is clear that the sequence $(f_n)$ is a divisibility sequence, so $f_r | \gcd(f_m, f_n)$. By Bézout’s lemma there exist $c, d \in \mathbb{N}$ with $\ell = cn - dm$, and

$$f_{cn}(f^{dm} + g^{dm}) - f_{dn}(f^{cn} + g^{cn}) = 2 f^{dm} g^{dm} f_\ell. \quad (2)$$

Any common divisor of $f_m$ and $f_n$ must divide $f_{cn}$ and $f_{dm}$. Since $k$ has odd characteristic, 2 is a unit in $k[T]$ and so (2) shows that any common divisor of $f_n$ and $f_m$ divides $f^{dm} g^{dm} f_\ell$. Since both $f$ and $g$ are coprime to $f_k$ for any $k$, any divisor of $f_m$ and $f_n$ divides $f_\ell$, completing the proof.
We will use the following simple observation several times. Let \( K \) be a field, and let \( \Phi_d \in K[x, y] \) denote the \( d \)th homogeneous cyclotomic polynomial. If \( f, g \in K[T] \) have \( \deg(f) \neq \deg(g) \), then it is clear that \( \Phi_n(f, g) \) is not a unit for any \( n \in \mathbb{N} \). If \( \deg(f) = \deg(g) = d \), and \( \zeta \) is a primitive \( n \)th root of unity over \( K \), then
\[
\Phi_n(f, g) = \prod_{i \in \mathbb{Z}} \Phi_i(f - \zeta^i g).
\]
For \( \Phi_n(f, g) \) to be a unit requires that \( f - \zeta^i g \) is a unit for each \( i \). Write
\[
f = \sum_{j=1}^d a_j T^j, \quad g = \sum_{j=1}^d b_j T^j.
\]
For \( f - \zeta^i g \) to be a unit requires that \( a_d = \zeta^i b_d \). Now for \( n > 2 \), the Euler function \( \phi(n) \geq 2 \), and so we can pick \( 0 < i_1 < i_2 < n \) with \( \gcd(i_1, n) = \gcd(i_2, n) = 1 \). If \( a_d = \zeta^{i_1} b_d \) and \( a_d = \zeta^{i_2} b_d \), then as \( a_d, b_d \neq 0 \) by assumption, we must have \( \zeta^{i_2 - i_1} = 1 \), contradicting the fact that \( \zeta \) is a primitive \( n \)th root of unity. We deduce that, for coprime polynomials \( f, g \in k[T] \),
\[
\Phi_n(f, g) \text{ is not a unit if } n > 2.
\]

These preparatory results give a polynomial form of Zsigmondy’s theorem as follows.

**Theorem 1.3.** Suppose \( \text{char}(k) = p > 0 \), and let \( P \) be the sequence obtained from \( (f_n)_{n \geq 1} \) by deleting the terms \( f_n \) with \( p | n \). Then each term of \( P \) beyond the second has a primitive prime divisor. If \( \text{char}(k) = 0 \), then the sequence \( (f_n)_{n \geq 1} \) has the property that all terms beyond the second have a primitive prime divisor.

**Proof.** Notice that
\[
f_n = \prod_{d | n} \Phi_d(f, g),
\]
and so
\[
\Phi_n(f, g) = \prod_{d | n} \Phi_d^{\mu(n/d)}
\]
by Möbius inversion. Thus
\[
\text{ord}_\pi(\Phi_n(f, g)) = \sum_{d | n} \mu(\frac{n}{d}) \text{ord}_\pi(f_d)
\]
for any prime \( \pi \in k[T] \). Suppose now that \( \pi \) is a prime divisor of \( f_n \) which is not primitive, so that \( \pi | f_m \) for some \( m < n \) chosen to be minimal with that property. Then \( m | n \) by Lemma 1.2 and
\[
\text{ord}_\pi(f_{mk}) = \text{ord}_\pi(f_m)
\]
for any \( k \) with \( p \nmid k \), by Lemma 1.1. In addition, we claim it follows that \( \text{ord}_\pi(f_c) = 0 \) unless \( m \mid c \). Suppose this were not the case, then \( \text{ord}_\pi(f_c) > 0 \) for some \( c \) with \( m \nmid c \), and Lemma 1.2 yields \( \pi \mid f_{\gcd(m,c)} \). However, since \( m \nmid c \), \( \gcd(m,c) \prec m \), so this contradicts the minimality of \( m \). Thus (5) gives

\[
\text{ord}_\pi(\Phi_n(f,g)) = \sum_{d \mid m} \mu\left(\frac{n}{dm}\right) \text{ord}_\pi(f_{dm}) = \sum_{d \mid m} \mu\left(\frac{n}{dm}\right) \text{ord}_\pi(f_m) = \text{ord}_\pi(f_m) \sum_{d \mid m} \mu\left(\frac{n}{dm}\right) = 0
\]
as \( m < n \). We deduce that any non-primitive prime divisor of \( f_n \) does not divide \( \Phi_n(f,g) \). By (3) above, \( \Phi_n(f,g) \) 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 record two simple observations that arise from this argument.

1. In fact (4) 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 exactly \( \Phi_n(f,g) \). This gives a lower bound for the size of the primitive part \( f_n^* \) of \( f_n \) under the assumption that \( \deg(f) \neq \deg(g) \):

\[
\deg(f_n^*) = \phi(n) \max\{\deg(f), \deg(g)\} > n^{1-\delta} \max\{\deg(f), \deg(g)\}
\]
for \( \delta > 0 \) and large enough \( n \).

2. It is also clear that we need to remove all the terms from the sequence with index divisible by \( p \). If \( n = pc \) for some \( c \geq 1 \), then \( f_n = f_{pc} = (f_c)^p \); so any term with index divisible by \( p \) fails to have a primitive prime divisor.

Theorem 1.3 is a form of Zsigmondy theorem for polynomial rings, but it is not clear how to prove strong divisibility when \( \text{char}(k) = 2 \). Computations suggest that the result is still true in this case. When \( g = 1 \) and \( \text{char}(k) = 2 \), the sequence \( (f_n)_{n \geq 1} \) satisfies the strong divisibility property, giving the analogue of Bang’s Theorem in all characteristics.

**Lemma 1.4.** Let \( \text{char}(k) = 2 \) and let \( f \in k[T] \) be a non-zero non-unit. Then the sequence \((h_n = f^n - 1)_{n \geq 1}\) is a strong divisibility sequence.

**Proof.** As before, let \( \ell = \gcd(m,n) \) so \( h_{\ell} \mid \gcd(h_m,h_n) \) by the divisibility property. As before, there exist \( c,d \in \mathbb{N} \) with \( \ell = cn - dm \). A common divisor of \( h_n \) and \( h_m \) must divide \( h_{cn} \) and \( h_{dm} \), and

\[
h_{cn} - h_{dm} = f^{dm}h_{\ell},
\]
so any common divisor of \( h_n \) and \( h_m \) must divide \( f^{dm}h_{\ell} \). Since \( f \) and \( h_{\ell} \) are coprime for any \( k \), any divisor of \( h_m \) and \( h_n \) must divide \( h_{\ell} \). \( \square \)
Corollary 1.5. Assume that \( \text{char}(k) = p \geq 2 \) and \( h_n \in k[T] \) is as in Lemma 1.4. Then the sequence obtained from \( (h_n)_{n \geq 1} \) by deleting terms with index divisible by \( p \) has the property that all terms beyond the first have a primitive prime divisor.

2. Polynomial Lucas sequences

In this section we provide an analogue of the result of Bilu, Hanrot and Voutier on primitive prime divisors in Lucas sequences. Let \( k \) be a field, and fix \( \alpha \in \bar{k} \) such that \( [k(\alpha) : k] = 2 \). Let \( \sigma \) be the non-identity \( k \)-automorphism of \( k(\alpha) \), and define the polynomial sequence \( (L_n)_{n \geq 1} \) by

\[
L_n = \frac{P^n - (P_\sigma)^n}{P - P_\sigma},
\]

where for \( P = \sum_{i=0}^{d} a_i T^i \) we write \( P_\sigma = \sum_{i=0}^{d} \sigma(a_i) T^i \). Then \( L_n \in k[T] \) and we can again ask which terms of the sequence see new irreducible factors.

We follow the path of Carmichael [2] in deducing some elementary arithmetic properties of the sequence. In order to do this, there is a degenerate possibility that must be avoided, so from now on we assume that \( P + P_\sigma \) and \( PP_\sigma \) are coprime in \( k[T] \). Without this property, the sequence is not a strong divisibility sequence. For example, if \( k = \mathbb{Q}, \alpha = \sqrt{2} \), and \( P = T^2 + (1 + \sqrt{2})T + \sqrt{2} \), then \( \gcd(L_2, L_3) = T + 1 \neq 1 = L_1 \).

Lemma 2.1. The polynomials \( PP_\sigma \) and \( L_n \) are coprime in \( k[T] \) for \( n \geq 1 \).

Proof. The binomial expansion shows that

\[
(P + P_\sigma)^n = P^{n-1} + (P_\sigma)^{n-1} + PP_\sigma Q_1
\]

for some \( Q_1 \in k[T] \). Moreover,

\[
L_n = P^{n-1} + (P_\sigma)^{n-1} + PP_\sigma Q_2
\]

for some \( Q_2 \in k[T] \). If \( Q_3 \in k[T] \) is irreducible and divides both \( PP_\sigma \) and \( L_n \) then, by \( \Box \), we have \( Q_3|P^{n-1} + (P_\sigma)^{n-1} \). Then, by \( \Box \), \( Q_3|P + P_\sigma \), contradicting the standing assumption that \( P + P_\sigma \) and \( PP_\sigma \) are coprime. Thus the greatest common divisor of \( PP_\sigma \) and \( L_n \) must be a unit.

As mentioned above, we deduce the strong divisibility property for our sequence.

Lemma 2.2. Assume that \( \text{char}(k) \neq 2 \). Then the sequence \( (L_n)_{n \geq 1} \) is a strong divisibility sequence.

Proof. It is clear that \( (L_n)_{n \geq 1} \) is a divisibility sequence. As before, let \( \ell = \gcd(m, n) \) and choose \( c, d \in \mathbb{N} \) with \( cn - dm = \ell \). For brevity write \( \tilde{L}_n = P^n + P_\sigma^n \), and notice that

\[
L_{cn} \tilde{L}_{dm} - L_{dm} \tilde{L}_{cn} = 2(PP_\sigma)^{dm} L_\ell.
\]

Hence a common divisor of \( L_n \) and \( L_m \) divides \( (PP_\sigma)^{dm} L_\ell \), and hence must divide \( L_\ell \) by Lemma 2.1. \( \Box \)
The next result shows that in characteristic \( p \) we can still expect to find that, in general, terms with index divisible by \( p \) once again fail to produce primitive divisors.

**Lemma 2.3.** Let \( \text{char}(k) = p > 2 \). Then for \( n \) divisible by \( p \) (with the possible exception of \( n = p \)), \( L_n \) fails to have a primitive prime divisor.

*Proof.* Write \( L'_n = P^n - P^m \), and assume that \( n = cp \) for some \( c \geq 1 \). Then

\[
L'_{cp} = (L'_c)^p + \sum_{i=1}^{(p-1)/2} (-1)^{i-1} \binom{p}{i} (PP_s)^{ce} L'_{(p-2i)c}.
\]

However \( p | \binom{p}{i} \) for \( 1 \leq i \leq \frac{p-1}{2} \), so \( L'_{cp} = (L'_c)^p \), and therefore \( L_{cp} = (L'_1)^{p-1} L'_c \).

Thus, once again, terms whose index is divisible by the characteristic must be removed in order to find primitive divisors.

One more lemma is needed before making the key divisibility observation for the sequences \( (L_n)_{n \geq 1} \).

**Lemma 2.4.** Assume that \( \text{char}(k) \neq 2 \). Then \( L_m \) and \( L_m' \) are coprime in \( k[T] \).

*Proof.* Clearly

\[
\hat{L}_m^2 - (L'_m)^2 = 4(PP_s)^m,
\]

so

\[
\hat{L}_m^2 - (L'_m)^2 L'_m = 4(PP_s)^m.
\]

By assumption, 4 is a unit in \( k[T] \), so any prime \( \pi \in k[T] \) dividing \( L_m \) and \( L_m' \) also divides \( PP_s \), completing the proof by Lemma 2.1.

**Lemma 2.5.** Let \( L_n \) be as defined above. If \( \pi \in k[T] \) is a prime dividing \( L_n \), then for \( \text{char}(k) = p > 0 \) and \( m, n \) coprime to \( p \),

\[
\text{ord}_\pi(L_{mn}) = \text{ord}_\pi(L_n),
\]

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

\[
\text{ord}_\pi(L_{mn}) = \text{ord}_\pi(L_n).
\]

*Proof.* For \( m \) odd, this proceeds as in the proof of Lemma 2.3. The result is clearly true for \( m = 1 \). So now suppose that

\[
\text{ord}_\pi(L_{bn}) = \text{ord}_\pi(L_n)
\]

for each odd integer \( b < m \). Then we note that

\[
L_{mn} = (P - P_s)^{m-1}L_n + \sum_{i=1}^{(m-1)/2} (-1)^i \binom{m}{i} (PP_s)^{in} L_{(m-2i)n}.
\]
Not all terms inside the summation are zero, since \( m \) is coprime to \( p \), so by the inductive assumption we conclude the statement of the lemma by the ultrametric property of the valuation \( \text{ord}_\pi \). For \( m \) even, note that it is sufficient to prove this for \( m = 2 \). However, since
\[
L_{2m} = \frac{P^{2m} - P_{\sigma}^{2m}}{P - P_{\sigma}} = \frac{P^m - P_{\sigma}^m}{P - P_{\sigma}} \cdot (P^m + P_{\sigma}^m),
\]
we see that
\[
L_{2m} = \tilde{L}_m L_m.
\]
By Lemma 2.4, \( \tilde{L}_m, L_m \) are coprime in \( k[T] \), and so
\[
\text{ord}_\pi(L_{2m}) = \text{ord}_\pi(L_m).
\]

As before, we are now ready for our Zsigmondy theorem.

**Theorem 2.6.** Suppose \( \text{char}(k) = p > 2 \), and let \( Q \) be the sequence obtained from \((L_n)_{n \geq 1}\) by deleting the terms with \( p \mid n \). Then each term of \( Q \) beyond the second has a primitive prime divisor. If \( \text{char}(k) = 0 \), then the sequence \((L_n)_{n \geq 1}\) has the property that all terms beyond the second have a primitive prime divisor.

**Proof.** We begin by noting the fact that
\[
L_n = \prod_{\substack{d \mid n, \\
d > 1}} \Phi_d(P, P_{\sigma}),
\]
where \( \Phi_d \) is the \( d \)th homogeneous cyclotomic polynomial. By Möbius inversion,
\[
\Phi_n(P, P_{\sigma}) = \prod_{\substack{d \mid n, \\
d > 1}} L_d^{\mu(n/d)} = \prod_{d \mid n} L_d^{\mu(n/d)}.
\]
The rest of the proof proceeds along the same lines as the proof of Theorem 1.3 combining Lemmas 2.2 and 2.5 with [3].


