PERMUTABLE POLYNOMIALS AND RELATED TOPICS

H.Woracek **G.Eigenthaler**

1 Introduction

Let $\Bbbk$ be a field and $\Bbbk[x]$ the polynomial ring over $\Bbbk$ in one indeterminate. Consider the semigroup $\langle \Bbbk[x], \circ \rangle$ where $\circ$ denotes the composition of polynomials defined as $(f \circ g)(x) = f(g(x))$. The semigroup $\langle \Bbbk[x], \circ \rangle$ is not commutative, i.e. the equality $f \circ g = g \circ f$ does not hold in general. Thus the question arises which specific polynomials f and g permute, i.e. satisfy $f \circ g = g \circ f$, and, in a more structural setting, which subsemigroups of $\langle \Bbbk[x], \circ \rangle$ are commutative.

We consider mainly the case that $\Bbbk = \mathbb{C}$, the field of complex numbers, as in this case a result of J.Ritt (see [38]) answers the first mentioned question. This leads us to an answer to the second question in form of a complete list of commutative subsemigroups of $\langle \Bbbk[x], \circ \rangle$ for $\Bbbk = \mathbb{C}$ (see Theorem 2).

In §2 we recall some basic facts concerning the semigroup $\langle \Bbbk[x], \circ \rangle$. We introduce the notion of the gap-degree of a polynomial in §3. The gap-degree is an invariant under conjugation and provides a convenient tool for working with permutable polynomials. In §4 we give a classification of commutative subsemigroups of $\langle \mathbb{C}[x], \circ \rangle$ which contain no linear polynomials. Together with some well known results this leads us to a complete list of commutative subsemigroups of $\langle \mathbb{C}[x], \circ \rangle$ (see List IV in §5). Finally, in §6 we apply our results to some related questions, namely the classification of maximal commutative subsemigroups and the classification of generalized permutable chains.

We would like to point out that, as we refer to certain results of J.Ritt, in most parts of the paper $\Bbbk$ equals $\mathbb{C}$. Apart from this some methods developed in this note depend only on the fact that $\Bbbk$ is of characteristic zero and algebraically closed; in particular, this is the case for §3.

As a complete proof of the presented results employing only purely algebraic methods is still missing we have tried to collect literature concerning the subject of permutable polynomials and related topics, including various results in the case that char $\Bbbk \neq 0$ and some papers which give connections to other areas.

2 Some basic facts about the semigroup $\langle \Bbbk[x], \circ \rangle$

For $f \in \Bbbk[x]$ denote by $[f]$ the (exact) degree of f. It is well known that $[.] : \langle \Bbbk[x], \circ \rangle \to \langle \mathbb{N}_0, \cdot \rangle$ is a homomorphism (as $\Bbbk$ denotes a field, $\Bbbk$ contains no zero divisors). The polynomial x is neutral with respect to composition and, again due to the fact that $\Bbbk$ is a field, the units of $\langle \Bbbk[x], \circ \rangle$ are exactly the linear polynomials. Furthermore the inverse of the polynomial $L(x) = ax + b$ is easily seen to be $\frac{1}{a}x - \frac{b}{a}$; we will denote the inverse of L by $L^{(-1)}$. The n-th iterate of a polynomial f will be abbreviated as $f^{(n)}$, i.e.

$$f^{(n)} = \underbrace{f \circ \cdots \circ f}_{n \text{ times}}.$$

The operation of composition is right-distributive with respect to addition and multiplication of polynomials, i.e.

$$(f+g)\circ h = (f\circ h)+(g\circ h) \text{ and}$$
$$(f\cdot g)\circ h = (f\circ h)\cdot(g\circ h)$$

holds. From this and the fact that [.] is a homomorphism it follows easily that every nonconstant polynomial is right-regular. On the other hand not every nonconstant polynomial is left-regular.

Given any invertible polynomial $L(x)=ax+b$, we can define an (inner) automorphism Φ_L of $\langle \Bbbk[x],\circ\rangle$ as $\Phi_L(f)=L^{(-1)}\circ f\circ L$ for $f\in\Bbbk[x]$. Clearly the relations $\Phi_L\circ\Phi_M=\Phi_{M\circ L}$ and $(\Phi_L)^{-1}=\Phi_{L^{(-1)}}$ are satisfied. Thus the set of all inner automorphisms forms a group acting on $\Bbbk[x]$, antiisomorphic to the group of linear polynomials.

We call two polynomials f and g conjugates of each other, if they belong to the same domain of transitivity with respect to this group, i.e. if there exists a linear polynomial L, such that $\Phi_L(f)=g$ holds. At some stage it is convenient to consider a coarser equivalence relation: We call two polynomials f and g weakly conjugates of each other, if there exist linear polyninomials L_1 and L_2, such that $L_1\circ f\circ L_2=g$ holds.

A polynomial f permutes with a constant polynomial a if and only if a is a fixed point of f: $f(a)=a$. Thus any commutative subsemigroup of $\langle \Bbbk[x],\circ\rangle$ contains at most one constant. On the other hand, given any commutative subsemigroup $\mathcal{S}$ we can extend $\mathcal{S}$ to a - still commutative - semigroup $\mathcal{S}'=\mathcal{S}\cup\{a\}$ if and only if a is a common fixed point of all polynomials of $\mathcal{S}$. In view of this fact we can confine our attention to commutative semigroups which contain no constant polynomials. In the sequel the notion of commutative semigroup will always be understood in this manner.

A straightforward argument using Zorn's Lemma shows that every commutative subsemigroup of $\langle \Bbbk[x],\circ\rangle$ is contained in some maximal commutative subsemigroup.

If f permutes with g, then obviously f permutes also with every power $g^{(n)}$ of g. The converse statement is not true, as the following example shows: Let $f(x)=\zeta x$ where ζ is a primitive third root of unity and let $g(x)=x^2$. Then

$$(x^2)^{(2)}\circ\zeta x = x^4\circ\zeta x = \zeta x\circ x^4 = \zeta x\circ(x^2)^{(2)},$$

but

$$x^2\circ\zeta x = \zeta^2 x\circ x^2 \neq \zeta x\circ x^2.$$

But at least the following result, which will be used in the subsequent sections, holds.

Lemma 1 *Let f permute with $g^{(n_i)}$ for $n_i\in\mathbb{N}$, $i=1,\ldots,k$ and let $d=\gcd(n_1,\ldots,n_k)$. Then f permutes with $g^{(d)}$.*

Proof : For $[g]=0$ the statement is trivial, so let $[g]>0$ and suppose w.l.o.g. $d=\lambda_1 n_1+\ldots+\lambda_l n_l-\lambda_{l+1}n_{l+1}-\ldots-\lambda_k n_k$ with $\lambda_i\geq 0$. As f permutes with each $g^{(n_i)}$ we find

$$f\circ g^{(\lambda_1 n_1+\ldots+\lambda_l n_l)} = g^{(\lambda_1 n_1+\ldots+\lambda_l n_l)}\circ f$$

and

$$f\circ g^{(\lambda_{l+1} n_{l+1}+\ldots+\lambda_k n_k)} = g^{(\lambda_{l+1} n_{l+1}+\ldots+\lambda_k n_k)}\circ f.$$

Thus

$$f\circ g^{(d)}\circ g^{(\lambda_{l+1} n_{l+1}+\ldots+\lambda_k n_k)} = f\circ g^{(\lambda_1 n_1+\ldots+\lambda_l n_l)} = g^{(\lambda_1 n_1+\ldots+\lambda_l n_l)}\circ f =$$

$$= g^{(d)} \circ g^{(\lambda_{l+1}n_{l+1}+\ldots+\lambda_k n_k)} \circ f = g^{(d)} \circ f \circ g^{(\lambda_{l+1}n_{l+1}+\ldots+\lambda_k n_k)},$$

which implies $g^{(d)} \circ f = f \circ g^{(d)}$.

□

3 The gap-degree of a polynomial

In this section we study an invariant of a polynomial under conjugation. The results proved in the sequel provide some tools for the study of permutable polynomials and give an insight to the behaviour of linear polynomials when composed with another (arbitrary) polynomial.

Definition 1 *Let $f \in \Bbbk[x]$, $[f] \geq 1$. Consider the field extension $[\Bbbk(x) : \Bbbk]$ and the subring $\Bbbk[f]$. Denote by $\mathcal{G}(f)$ the group of all automorphisms of $[\Bbbk(x) : \Bbbk]$ which leave $\Bbbk[f]$ (as a whole) invariant. The number $\mathcal{L}(f) = |\mathcal{G}(f)|$ will be called the gap-degree of f.*

A well known theorem (see e.g. [43]) states that the automorphisms of $[\Bbbk(x) : \Bbbk]$ are exactly those endomorphisms which map x to some linear fractional element $L(x) = \frac{ax+b}{cx+d}$ of $\Bbbk(x)$. Denote by α_L the automorphism of $[\Bbbk(x) : \Bbbk]$ with $\alpha_L : x \mapsto L(x)$, i.e. $\alpha_L(f) = f \circ L$.

Lemma 2 *The group $\mathcal{G}(f)$ consists exactly of those automorphisms α_L, where L is a linear polynomial and satisfies an equation of the form*

$$L_1 \circ f = f \circ L \tag{1}$$

for some linear polynomial L_1.

Proof : The condition $\alpha_L(\Bbbk[f]) \subseteq \Bbbk[f]$ implies that $\alpha_L(f) = f \circ L \in \Bbbk[f]$. Thus $f \circ L$ is a polynomial (in the indeterminate x), which implies that L is a polynomial. Furthermore $f \circ L = L_1 \circ f$ where L_1 is a polynomial, which then must have degree 1.

Conversely suppose that (1) holds for some linear polynomial L_1. Then $\alpha_L(\Bbbk[f]) = \Bbbk[f]$, as for arbitrary $g \circ f \in \Bbbk[f]$ the formulas

$$\alpha_L(g \circ f) = g \circ (f \circ L) = (g \circ L_1) \circ f$$

and

$$\alpha_L(L_1^{-1} \circ f) = L_1^{-1} \circ f \circ L = L_1^{-1} \circ L_1 \circ f = f$$

hold.

□

We have $\alpha_{L \circ M} = \alpha_M \circ \alpha_L$, hence $L \mapsto \alpha_{L^{(-1)}}$ defines a group-isomorphism. In view of this fact and the above lemma we can consider $\mathcal{G}(f)$ in the following as a group of linear polynomials.

Before we proceed to determine the group $\mathcal{G}(f)$ for a given polynomial f, we introduce another notion.

Definition 2 *Let $f \in \Bbbk[x]$, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ with $n = [f] \geq 2$. Denote by $l(f)$ the smallest number $k \geq 1$, such that $a_{n-k} \neq 0$. In the case $f(x) = a_n x^n$ let $l(f) = n$. If $l(f) > 1$, i.e. $a_{n-1} = 0$, we say that f has gap-form. We call the number $l(f)$ the gap of f.*

From now on let us assume that char $\Bbbk = 0$.

Lemma 3 *Let $f \in \Bbbk[x]$, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ with $[f] \geq 2$, let $L(x) = ax + b$ and consider the polynomial $g = f \circ L$. Then $l(g) > 1$ if and only if*

$$b = -\frac{a_{n-1}}{na_n}. \tag{2}$$

Proof : We compute the highest coefficients of g:

$$g(x) = f \circ L(x) = a_n(ax+b)^n + a_{n-1}(ax+b)^{n-1} + \ldots =$$

$$= a_n a^n x^n + (a_n n a^{n-1} b + a_{n-1}a^{n-1})x^{n-1} + \ldots.$$

Thus g has gap-form if and only if

$$a_n n a^{n-1} b + a_{n-1}a^{n-1} = 0,$$

which is equivalent to (2), as $a \neq 0$.

□

Corollary 1 *Let $f \in \Bbbk[x]$, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ with $[f] \geq 2$. Then there is a conjugate g of f which has gap-form.*

Proof : As multiplication from the left with linear polynomials does not change $l(f)$, we can take

$$g = (x + \frac{a_{n-1}}{na_n}) \circ f \circ (x - \frac{a_{n-1}}{na_n}).$$

□

From now on assume that $\Bbbk$ is not only of characteristic zero, but also algebraically closed.

The following proposition gives a method to compute $\mathcal{L}(f)$ from the coefficients of f.

Proposition 1 *Let $f \in \Bbbk[x]$, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, $n = [f] \geq 2$ and suppose that f has gap-form.*

(i) In case that $1 < l(f) < n$ denote by $n = k_1 > k_2 > \ldots > k_l > 0$ those indices $k_i \in \{1, \ldots, n\}$ for which $a_{k_i} \neq 0$. Then the formula

$$\mathcal{L}(f) = \gcd(k_1 - k_2, k_2 - k_3, \ldots, k_{l-1} - k_l)$$

holds. Furthermore the gap-degree $\mathcal{L}(f)$ is the maximum number r, such that $f(x) - a_0$ admits a representation of the form

$$f(x) - a_0 = x^k p(x^r), \text{ for } k \geq 1 \text{ and } p \in \Bbbk[x],\ p(0) \neq 0, \tag{3}$$

and we have $\mathcal{G}(f) = \{\zeta x | \zeta^{\mathcal{L}(f)} = 1\} \cong \mathbb{Z}_{\mathcal{L}(f)}$.

(ii) In case that $l(f) = n$, i.e. that $f(x) = a_n x^n + a_0$, we have $\mathcal{L}(f) = |\Bbbk|$ and $\mathcal{G}(f) = \{ax | a \in \Bbbk, a \neq 0\}$.

Case (ii) occurs if and only if f is weakly conjugated to the power x^n.

Proof : Consider the case $1 < l(f) < n$. Denote by c the maximum of all numbers r such that a representation (3) is possible, and let $d = \gcd(k_1 - k_2, k_2 - k_3, \ldots, k_{l-1} - k_l)$. In first place we show $c = d$.

Let r be any number such that (3) holds for some $k \in \mathbb{N}$ and $p \in \Bbbk[x]$. Then

$$\{k_1, \ldots, k_l\} \subseteq \{k, k + r, k + 2r, \ldots, k + [p]r\}$$

holds, which implies $r|(k_i - k_{i+1})$ for each $i = 1, \ldots, l - 1$ and therefore $r|d$.

To show the converse relation we establish a representation (3) for $r = d$:

$$f(x) - a_0 = x^{k_l}(a_{k_1}x^{k_1-k_l} + a_{k_2}x^{k_2-k_l} + \ldots + a_{k_l}).$$

As $d|(k_i - k_{i+1})$ for each i, d also divides $k_i - k_l$. Thus $f(x) - a_0 = x^k p(x^d)$ with $k = k_l$ and

$$p(x) = a_{k_1}x^{\frac{k_1-k_l}{d}} + a_{k_2}x^{\frac{k_2-k_l}{d}} + \ldots + a_{k_l}.$$

We proceed to determine $\mathcal{G}(f)$. Let ζ be a d-th root of unity, then

$$f \circ \zeta x = (f - a_0) \circ \zeta x + a_0 = x^k p(x^d) \circ \zeta x + a_0 = \zeta^k x \circ x^k p(x^d) + a_0 =$$
$$= \zeta^k x \circ (f - a_0) + a_0 = \zeta^k x \circ f + (1 - \zeta^k)a_0 = L_1 \circ f,$$

where $L_1(x) = \zeta^k x + (1-\zeta^k)a_0$. Thus $\zeta x \in \mathcal{G}(f)$ by Lemma 2. Let conversely $L(x) = ax + b$ be an element of $\mathcal{G}(f)$. Then there exists, again by Lemma 2, a linear polynomial $L'(x) = a'x + b'$, such that $L' \circ f = f \circ L$. Thus $l(f \circ L) = l(L' \circ f) = l(f) > 1$, which implies $b = 0$ by Lemma 3. Let $p(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_0$, then

$$f \circ L = (x^k p(x^d) + a_0) \circ (ax) = a^k x^k p(a^d x^d) + a_0 =$$
$$a^k(b_m a^{dm} x^{dm+k} + b_{m-1}a^{d(m-1)}x^{d(m-1)+k} + \ldots + b_0 x^k) + a_0$$

and

$$L' \circ f = a'(b_m x^{dm+k} + b_{m-1}x^{d(m-1)+k} + \ldots + b_0 x^k) + b'.$$

Comparing coefficients we find

$$a' = a^{dm+k} \text{ and } b' = a_0.$$

Let b_i $(i \neq m)$ be any nonzero coefficient of p and compare the coefficients of x^{di+k}:

$$b_i a^{di+k} = a^{dm+k} b_i,$$

that is $a^{d(m-i)} = 1$. The numbers $k_1, \ldots, k_l$ are exactly those numbers $di + k$ with $b_i \neq 0$ and $k_1 = dm + k$. Thus $d = \gcd(k_1 - k_2, k_1 - k_3, \ldots, k_1 - k_l) = \gcd(\{d(m - i)|b_i \neq 0\})$ and therefore $a^d = 1$. We found $\mathcal{G}(f) = \{\zeta x|\zeta^d = 1\}$ and thus $\mathcal{L}(f) = |\mathcal{G}(f)| = d$.

Consider now the case $l(f) = n$. Similar to the first case we find for each $L(x) = ax + b \in \mathcal{G}(f)$ that $l(f \circ L) = l(L' \circ f) = l(f) > 1$, hence $b = 0$. On the other hand

$$f \circ ax = (a_n x^n + a_0) \circ ax = (a^n x + (1 - a^n)a_0) \circ f$$

holds, and therefore $ax \in \mathcal{G}(f)$ for arbitrary $a \in \Bbbk, a \neq 0$. Thus $\mathcal{G}(f) = \{ax|a \in \Bbbk, a \neq 0\}$.

If $f(x) = a_n x^n + a_0$, we find $f = (a_n x + a_0) \circ x^n$. Thus f is weakly conjugated to x^n. Conversely, let f be weakly conjugated to x^n, i.e. $f = (a'x + b') \circ x^n \circ (ax + b)$. As f has gap-form Lemma 3 implies $b = 0$ and we find $f(x) = a'a^n x^n + b'$.

□

Proposition 2 *The gap-degree is constant on weak conjugacy classes. Let* $f \in \Bbbk[x]$, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, $n = [f] \geq 2$ *and let* $f' = \Phi_L(f)$ *with* $L(x) = x - \frac{a_{n-1}}{na_n}$. *Then* $\mathcal{L}(f) = \mathcal{L}(f')$ *and the latter can be computed via Proposition 1.*

(i) In case that $1 < l(f') < n$ *the group* $\mathcal{G}(f)$ *is given by*

$$\mathcal{G}(f) = \{\zeta x + (\zeta - 1)\frac{a_{n-1}}{na_n} | \zeta^{\mathcal{L}(f)} = 1\} \cong \mathbb{Z}_{\mathcal{L}(f)}.$$

(ii) In case that $l(f') = n$ *we have*

$$\mathcal{G}(f) = \{ax + (a-1)\frac{a_{n-1}}{na_n} | a \in \Bbbk, a \neq 0\}.$$

Again case (ii) occurs if and only if f *is weakly conjugated to the power* x^n.

Proof : Since $\Bbbk[f] = \Bbbk[L \circ f]$ for any linear polynomial L, we have $\mathcal{G}(f) = \mathcal{G}(L \circ f)$. Suppose $g = L_1 \circ f \circ L_2$, then $\mathcal{G}(g) = \mathcal{G}(L_2^{(-1)} \circ L_1^{(-1)} \circ g) = \mathcal{G}(L_2^{(-1)} \circ f \circ L_2)$. In the following we establish an isomorphism between $\mathcal{G}(f)$ and $\mathcal{G}(L_2^{(-1)} \circ f \circ L_2)$. This will prove the first assertion.

Let L be a linear polynomial and consider the conjugation Φ_L. If $H \in \mathcal{G}(f)$ we have

$$H_1 \circ f = f \circ H \text{ for some } H_1,$$

and therefore also

$$\Phi_L(H_1) \circ \Phi_L(f) = \Phi_L(f) \circ \Phi_L(H).$$

Thus $\Phi_L(H) \in \mathcal{G}(\Phi_L(f))$, i.e.

$$\Phi_L(\mathcal{G}(f)) \subseteq \mathcal{G}(\Phi_L(f)).$$

Since a similar argument shows

$$\Phi_{L^{(-1)}}(\mathcal{G}(\Phi_L(f))) \subseteq \mathcal{G}(f),$$

we have $\mathcal{G}(\Phi_L(f)) \subseteq \Phi_L(\mathcal{G}(f))$, thus the conjugation Φ_L yields an isomorphism between $\mathcal{G}(f)$ and $\mathcal{G}(\Phi_L(f))$.

In case that $1 < l(f') < n$ Proposition 1 yields $\mathcal{G}(f') = \{\zeta x | \zeta^{\mathcal{L}(f')} = 1\}$ and therefore

$$\mathcal{G}(f) = \Phi_{L^{(-1)}}(\mathcal{G}(f')) = \{\zeta x + (\zeta - 1)\frac{a_{n-1}}{na_n} | \zeta^{\mathcal{L}(f)} = 1\}.$$

In the case $l(f') = n$ the result follows by a similar argument.

□

For future reference we state a result of H.Engstrøm (see [16]), and give some formulas involving gap and gap-degree.

Proposition 3 (H.Engstrøm 1941) *Let* $f, g \in \Bbbk[x]$. *If* $\Bbbk[f] \cap \Bbbk[g] \neq \Bbbk$ *then there exists a polynomial* h *of degree* $[h] = \gcd([f], [g])$, *such that*

$$f = f_1 \circ h \text{ and } g = g_1 \circ h$$

holds for appropriate f_1 *and* g_1.

Let us remark that Proposition 3 also follows from a result in [28] (ch.6, Theorem 5.84) by using the well known fact that $\Bbbk[f] = \Bbbk(f) \cap \Bbbk[x]$ for any $f \in \Bbbk[x]$.

Lemma 4 *Let $f, g \in \Bbbk[x]$, $n = [f], m = [g] \geq 2$, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, $g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_0$ and suppose $f(x) \neq a_n x^n$ and $g(x) \neq b_m x^m$. Then the gap of the polynomial $f \circ g$ is given by the following formulas:*

(i) If $l(g) \neq [g]l(f)$ then $l(f \circ g) = l(g)$,

(ii) if $l(g) = [g]l(f)$ then $l(f \circ g) \geq l(g)$.

In the last case equality holds if and only if

$$a_n n b_m^{l(f)-1} b_{m-l(g)} + a_{n-l(f)} \neq 0. \tag{4}$$

The gap of the polynomial $f \cdot g$ is given by the formulas:

(iii) If $l(f) \neq l(g)$ then $l(f \cdot g) = \min(l(f), l(g))$,

(iv) If $l(f) = l(g)$ then $l(f \cdot g) \geq l(f) = l(g)$.

In the last case equality holds if and only if

$$a_n b_{m-l(g)} + a_{n-l(f)} b_m \neq 0. \tag{5}$$

Furthermore we have:

(v) $l(a_n x^n \circ g) = l(g)$,

(vi) $l(f \circ b_m x^m) = m l(f)$,

(vii) $l(a_n x^n \cdot g) = l(g)$,

(viii) $l(g^{(r)}) = l(g)$ for $r \in \mathbb{N}$.

Proof : Let $k = l(f)$ and $l = l(g)$, then $f(x) = a_n x^n + a_{n-k}x^{n-k} + \ldots + a_0$ and $g(x) = b_m x^m + b_{m-l}x^{m-l} + \ldots + b_0$ where $a_{n-k}, b_{m-l} \neq 0$.

We compute the highest coefficients of $f \circ g$:

$$\begin{aligned} f \circ g(x) &= a_n(b_m x^m + b_{m-l}x^{m-l} + \ldots + b_0)^n + \\ &+ a_{n-k}(b_m x^m + b_{m-l}x^{m-l} + \ldots + b_0)^{n-k} + \ldots = \\ &= a_n b_m^n x^{nm} + a_n n b_m^{n-1} b_{m-l} x^{nm-l} + a_{n-k} b_m^{n-k} x^{nm-mk} + \ldots . \end{aligned} \tag{6}$$

From (6) the assertions (i), (ii) and (4) follow.

We compute the highest coefficients of $f \cdot g$:

$$\begin{aligned} f \cdot g(x) &= (a_n x^n + a_{n-k}x^{n-k} + \ldots + a_0) \cdot (b_m x^m + b_{m-l}x^{m-l} + \ldots + b_0) = \\ &= a_n b_m x^{n+m} + a_{n-k} b_m x^{n+m-k} + a_n b_{m-l} x^{n+m-l} + \ldots . \end{aligned} \tag{7}$$

From (7) we obtain (iii), (iv) and (5).

To prove (v) we compute

$$a_n x^n \circ g = a_n(b_m x^m + b_{m-l}x^{m-l} + \ldots + b_0)^n =$$

$$= a_n(b_m^n x^{nm} + n b_m^{n-1} b_{m-l} x^{nm-l} + \ldots).$$

The relations (vi) and (vii) are obvious. To establish (viii) we use induction on r. For $r = 1$ (viii) is clearly true. Let $r \geq 2$ and suppose that $l(g^{(r-1)}) = l(g)$. As $[g] \geq 2$

$$l(g) < [g]l(g) = [g]l(g^{(r-1)})$$

holds. Thus (i) applies to $g^{(r)} = g^{(r-1)} \circ g$ and we obtain $l(g^{(r)}) = l(g)$.

□

Lemma 5 *Let $f, g \in \Bbbk[x]$ be as in Lemma 4 and assume furthermore that $f \circ g = g \circ f$, then $l(f) = l(g)$.*

Proof : By (i) and (ii) of Lemma 4 we obtain

$$l(f \circ g) = l(g \circ f) \geq l(f).$$

In case $l(g) \neq [g]l(f)$ we have $l(f \circ g) = l(g)$ and therefore $l(g) \geq l(f)$. If $l(g) = [g]l(f)$ we also have $l(g) \geq l(f)$. By symmetry $l(f) \geq l(g)$ and thus $l(f) = l(g)$.

□

Before we can state the next result we have to introduce another notation. Denote by $\mathcal{G}^*(f)$ the group of all linear polynomials L_1, such that a relation of the form

$$L_1 \circ f = f \circ L$$

for some linear polynomial L holds.

Lemma 6 *Let $f \in \Bbbk[x]$, $[f] \geq 2$. Then*

$$\mathcal{G}(f) \supseteq \mathcal{G}(f^{(2)}) \supseteq \mathcal{G}(f^{(3)}) \supseteq \ldots. \tag{8}$$

We have $\mathcal{G}(f) = \mathcal{G}(f^{(2)})$ if and only if $\mathcal{G}^*(f) \subseteq \mathcal{G}(f)$. In this case equality holds throughout the chain (8).

The condition $\mathcal{G}^*(f) \subseteq \mathcal{G}(f)$ is satisfied for instance if $1 < l(f) < [f]$ and $f(0) = 0$.

Proof : Let $L \in \mathcal{G}(f^{(n)})$ and let $m < n$. Then

$$f^{(n-m)} \circ (f^{(m)} \circ L) = (L_1 \circ f^{(n-m)}) \circ f^{(m)},$$

and Proposition 3 implies that there exists a polynomial h of degree $[h] = [f^{(m)}]$, such that

$$f^{(m)} \circ L = L_2 \circ h \text{ and } f^{(m)} = L_3 \circ h$$

holds. Thus $f^{(m)} \circ L = (L_2 \circ L_3^{(-1)}) \circ f^{(m)}$, i.e. $L \in \mathcal{G}(f^{(m)})$.

Suppose $\mathcal{G}(f) = \mathcal{G}(f^{(2)})$ and let $L_1 \in \mathcal{G}^*(f)$. Then $L_1 \circ f = f \circ L$ for some $L \in \mathcal{G}(f) = \mathcal{G}(f^{(2)})$. Let $L_2 \circ f^{(2)} = f^{(2)} \circ L$, then

$$L_2 \circ f^{(2)} = f \circ f \circ L = f \circ L_1 \circ f.$$

Thus $L_2 \circ f = f \circ L_1$, which shows $L_1 \in \mathcal{G}(f)$. Conversly suppose that $\mathcal{G}^*(f) \subseteq \mathcal{G}(f)$ and let $L \in \mathcal{G}(f)$. Then

$$f^{(2)} \circ L = f \circ L_1 \circ f = L_2 \circ f^{(2)}$$

holds since $L_1 \in \mathcal{G}^*(f) \subseteq \mathcal{G}(f)$, and therefore $L \in \mathcal{G}(f^{(2)})$. Repeating the above argument $(m-1)$ times we obtain

$$f^{(m)} \circ L = L_m \circ f^{(m)}$$

which shows $L \in \mathcal{G}(f^{(m)})$.

Let f satisfy $1 < l(f) < [f]$ and $f(0) = 0$. Then we have a representation

$$f(x) = x^k p(x^r) \text{ with } k \geq 1 \text{ and } r = \mathcal{L}(f),$$

and

$$\mathcal{G}(f) = \{\zeta x | \zeta^r = 1\}.$$

As $f \circ \zeta x = \zeta^k x \circ f$ we find

$$\mathcal{G}^*(f) = \{\zeta^k x | \zeta^r = 1\} \subseteq \mathcal{G}(f).$$

□

Another sufficient condition in order that $\mathcal{G}^*(f) \subseteq \mathcal{G}(f)$ holds is given in the next lemma.

Lemma 7 *Let $f \in \Bbbk[x]$, $[f] \geq 2$. Suppose that $1 < l(f)$ and that for some $n \in \mathbb{N}$ and a linear polynomial ϵx the relation*

$$f^{(n)} \circ \epsilon x = \delta x \circ f^{(n)}, \text{ where } \delta \neq 1 \tag{9}$$

holds, then $f(0) = 0$. If furthermore $l(f) < [f]$, then $\mathcal{G}^*(f) \subseteq \mathcal{G}(f)$ and in particular $\mathcal{L}(f^{(k)}) = \mathcal{L}(f)$ for $k \in \mathbb{N}$.

Proof : The relation (9) shows that $\epsilon x \in \mathcal{G}(f^{(n)})$. Thus, by Lemma 6 we also have $\epsilon x \in \mathcal{G}(f^{(n-1)})$, i.e.

$$f^{(n-1)} \circ \epsilon x = L \circ f^{(n-1)}$$

holds for some linear polynomial L. We compute

$$f \circ L \circ f^{(n-1)} = f \circ f^{(n-1)} \circ \epsilon x = f^{(n)} \circ \epsilon x = \delta x \circ f^{(n)},$$

and therefore

$$f \circ L = \delta x \circ f. \tag{10}$$

As $l(f) > 1$ the right hand side of (10) has gap-form and, according to Lemma 3, the polynomial L must be a multiplication $L(x) = \gamma x$. Due to this fact we may compute

$$f(0) = (f \circ \gamma x)(0) = (\delta x \circ f)(0) = \delta f(0).$$

As $\delta \neq 1$ we find $f(0) = 0$ which implies together with Lemma 6 the assertion.

□

In the following definition we consider another group of linear polynomials. This concept has been studied in [13].

Definition 3 *Let $f \in \Bbbk[x]$, $[f] \geq 2$. Denote by $\mathcal{G}^p(f)$ the group of all linear polynomials L which permute with f:*

$$L \circ f = f \circ L.$$

Furthermore let $\mathcal{L}^p(f) = |\mathcal{G}^p(f)|$.

Some results on $\mathcal{G}^p(f)$ will be recalled in §5.

For future reference let us state the following rather obvious facts.

Lemma 8 *Let $f \in \Bbbk[x]$, $[f] \geq 2$. Then $\mathcal{G}^p(f) \subseteq \mathcal{G}^p(f^{(n)})$ holds for each $n \in \mathbb{N}$. In case $\mathcal{L}(f)$ is finite we also have $\mathcal{L}^p(f^{(n)})|\mathcal{L}(f)$.*

Proof : The first assertion is obvious. To prove the remaining part of the lemma, note that

$$\mathcal{G}^p(f^{(n)}) \subseteq \mathcal{G}(f^{(n)}) \subseteq \mathcal{G}(f).$$

□

æ

4 Commutative semigroups which do not contain a linear polynomial

In this section we give a complete list of all commutative subsemigroups of $\langle \mathbb{C}[x], \circ \rangle$ which contain no linear polynomials (except possibly the trivial one, namely x).

To start with let us recall two well known results. Here $\Bbbk$ again is a field of characteristic zero.

Proposition 4 *Let $\Bbbk$ be algebraically closed and let $\mathcal{S}$ be a commutative subsemigroup of $\langle \Bbbk[x], \circ \rangle$. If $\mathcal{S}$ contains an element which is conjugated to a power ax^n ($a \in \Bbbk$, $a \neq 0$, $n \geq 2$), then*

$$\Phi_L(\mathcal{S}) \subseteq P_r = \{\zeta x^k | k \equiv 1 \ mod r, \zeta^r = 1\}$$

for some r and an appropriate conjugation Φ_L.

Proposition 5 *Let $\mathcal{S}$ be a commutative subsemigroup of $\langle \Bbbk[x], \circ \rangle$. If $\mathcal{S}$ contains an element which is conjugated to a Chebyshev polynomial t_n or $-t_n$, respectively ($n \geq 2$), then either (i) or (ii) holds for some conjugation Φ_L:*

(i) $\Phi_L(\mathcal{S}) \subseteq D_1 = \{t_n | n \in \mathbb{N}\}$,

(ii) $\Phi_L(\mathcal{S}) \subseteq D_2 = \{\pm t_k | k \ odd\}$.

A proof of these results can be found e.g. in [14]. Another interesting proof of Proposition 5 is given in [3]. All these proofs employ only purely algebraic methods.

We proceed treating the remaining case of a commutative subsemigroup $\mathcal{S}$ of $\langle \mathbb{C}[x], \circ \rangle$ with no element conjugated to a power ax^n or a Chebyshev polynomial $\pm t_n$. To do so we use two results of J.Ritt (see [36] and [38]) which have been proved using topological and analytic methods.

Proposition 6 (J.Ritt 1923) *Let $f, g \in \mathbb{C}[x]$, $[f], [g] \geq 2$ be permutable and suppose that neither f nor g is conjugated to a power or a Chebyshev polynomial. Then there exists a conjugation Φ_L and a polynomial $h(x) = xp(x^r)$, such that*

$$\Phi_L(f) = \epsilon_1 h^{(m)} \text{ and } \Phi_L(g) = \epsilon_2 h^{(n)}.$$

Here $\epsilon_1^r = \epsilon_2^r = 1$ if r is chosen maximal. If furthermore $r > 1$, we have $r = \mathcal{L}^p(h)$.

Proposition 7 (J.Ritt 1920) *Let $f, g \in \mathbb{C}[x]$, $[f], [g] \geq 2$ and let ϵ and δ be roots of unity with*

$$f \circ \epsilon x = \epsilon^l x \circ f \text{ and } g \circ \delta x = \delta^{l'} x \circ g$$

for some $l, l' \in \mathbb{N}$. If $\epsilon f^{(m)} = \delta g^{(n)}$ for some numbers $m, n \in \mathbb{N}$, then there exists a conjugation Φ_L and a polynomial $h(x) = x^k p(x^r)$ ($k \geq 0$, $p(0) \neq 0$), such that

$$\Phi_L(f) = \epsilon_1 h^{(s)} \text{ and } \Phi_L(g) = \epsilon_2 h^{(t)}.$$

Here $\epsilon_1^r = \epsilon_2^r = 1$ if r is chosen maximal. If furthermore $k \geq 1$ and $r > 1$, we have $r = \mathcal{L}(h)$.

Proposition 7 actually is proved in [36] only in the case $\epsilon = \delta = 1$, but it is easy to see that the proof given there also works in the more general situation.

Before we proceed to generalize Proposition 6 we have to state a corollary of Proposition 6 and a lemma.

Corollary 2 *The formulation "there exists a conjugation Φ_L and a polynomial $h(x)$" in Proposition 6 and Proposition 7 can be strengthened to "for each conjugation Φ_L which conjugates f (and thus g) to gap-form there exists a polynomial $h(x)$".*

Proof : If we have $\epsilon_1 = \epsilon_2 = 1$ we can apply any conjugation Φ_M to the representations given in Proposition 6 and Proposition 7, respectively and obtain a representation of the same type. If $\epsilon_1 \neq 1$ or $\epsilon_2 \neq 1$ the polynomial h has gap-form. Any conjugation Φ_M which conjugates f (and thus g) to gap-form therefore differs only by a conjugation $\Phi_{\gamma x}$ from Φ_L. Applying $\Phi_{\gamma x}$ to the representations of Proposition 6 and Proposition 7, respectively does not change the type of representation given.

□

Lemma 9 *Let $f_1, f_2, \ldots$ be a (possibly finite) sequence of permutable polynomials which admit the representation*

$$f_i(x) = \epsilon_i [x^k p(x^r)]^{(k_i)}$$

where $\epsilon_i^r = 1$, i.e. $f_i \circ \epsilon_i x = \epsilon_i^{l_i} x \circ f_i$ for convenient numbers l_i. Then (i) or (ii) holds:

(i) $f_i = h^{(k_i)}$ for some polynomial h.

(ii) For some i we have $\epsilon_i^k \neq 1$. In this case we have in particular $k \geq 1$ and $r > 1$.

Proof : Assume that (ii) does not hold, i.e. $\epsilon_i^k = 1$ for all i. Then

$$x^k p(x^r) \circ \epsilon_i x = x^k p(x^r)$$

and thus also

$$x^k p(x^r) \circ \epsilon_i^{-1} x = x^k p(x^r).$$

This implies

$$f_i(x) = [\epsilon_i x \circ x^k p(x^r) \circ \epsilon_i^{-1} x]^{(k_i)} \text{ for } i = 1, 2, \ldots.$$

As the polynomials f_i permute we have that all numbers ϵ_i are equal and therefore obtain a representation of the desired form.

□

The following two lemmata generalize Proposition 6.

Lemma 10 *Let $n \in \mathbb{N}$, let $f_1, \ldots, f_n \in \mathbb{C}[x]$, $[f_i] \geq 2$ be pairwise permutable polynomials with gap-form and suppose that no polynomial f_i is conjugated to a power or a Chebyshev polynomial. Then (i) or (ii) holds:*

(i) There exist a polynomial g and numbers $m_1, \ldots, m_n \in \mathbb{N}$, such that

$$f_i = g^{(m_i)} \text{ for } i = 1, \ldots, n. \tag{11}$$

(ii) There exist a polynomial $g(x) = x^k g_1(x^r)$ where $k \geq 1$, $g_1(0) \neq 0$ and $r = \mathcal{L}(g) > 1$, numbers $m_1, \ldots, m_n \in \mathbb{N}$ and r-th roots of unity $\epsilon_1, \ldots, \epsilon_n$, such that

$$f_i = \epsilon_i g^{(m_i)} \text{ for } i = 1, \ldots, n. \tag{12}$$

Here

$$\epsilon_i^{k^{m_j}-1} = \epsilon_j^{k^{m_i}-1} \text{ for } i, j = 1, \ldots, n \tag{13}$$

and for at least one $i \in \{1, \ldots, n\}$ we have $\epsilon_i^k \neq 1$.

Proof : First of all we clarify condition (13). To do so assume $f_i = \epsilon_i g^{(m_i)}$ with g as above and compute $f_i \circ f_j$ and $f_j \circ f_i$:

$$f_i \circ f_j = \epsilon_i x \circ g^{(m_i)} \circ \epsilon_j x \circ g^{(m_j)} = \epsilon_i \epsilon_j^{k^{m_i}} x \circ g^{(m_i+m_j)},$$

$$f_j \circ f_i = \epsilon_j x \circ g^{(m_j)} \circ \epsilon_i x \circ g^{(m_i)} = \epsilon_j \epsilon_i^{k^{m_j}} x \circ g^{(m_i+m_j)}.$$

Thus f_i and f_j permute if and only if (13) holds.

To prove the lemma use induction on n. Consider first the case that $n = 2$. Then Proposition 6 implies together with Lemma 9 the assertion of the lemma.

We proceed to treat the case $n > 2$. The inductive hypothesis implies that (i) or (ii) holds for the polynomials $f_1, \ldots, f_{n-1}$.

Case 1: Assume (i) holds for $f_1, \ldots, f_{n-1}$, i.e. we have a representation

$$f_i = g^{(m_i)} \text{ for } i = 1, \ldots, n-1.$$

Let $\gcd(m_1,\ldots,m_{n-1})=d$. As f_n permutes with each polynomial f_i, Lemma 1 implies that f_n permutes with $g^{(d)}$. Note that by Lemma 4 $l(g^{(d)})=l(g)=l(f_1)>1$. Thus Proposition 6 implies together with Corollary 2 that

$$g^{(d)}(x)=\epsilon_1[xp(x^u)]^{(k_1)} \text{ and}$$

$$f_n(x)=\epsilon_2[xp(x^u)]^{(k_2)} \text{ with } \epsilon_1^u=\epsilon_2^u=1.$$

Proposition 7 shows that

$$g(x)=\delta_1[x^lq(x^s)]^{(l_1)} \text{ and} \tag{14}$$
$$xp(x^u)=\delta_2[x^lq(x^s)]^{(l_2)} \text{ with } \delta_1^s=\delta_2^s=1.$$

From this we find

$$g^{(d)}(x)=\epsilon_1\delta_2^{n_1}[x^lq(x^s)]^{(l_2k_1)} \text{ and}$$
$$f_n(x)=\epsilon_2\delta_2^{n_2}[x^lq(x^s)]^{(l_2k_2)}$$

for some $n_1,n_2\in\mathbb{N}$. In order to apply Lemma 9 we have to show that $\epsilon_i^s=1$, as then

$$f_i(x)=\gamma_i[x^lq(x^s)]^{(l_2k_1\frac{m_i}{d})} \text{ for } i=1,\ldots,n-1$$

with some s-th roots of unity γ_i.

If $\epsilon_1=\epsilon_2=1$ we are done. So suppose that $\epsilon_1\neq 1$ or $\epsilon_2\neq 1$. We have

$$[x^lq(x^s)]^{(l_2)}\circ\epsilon_ix=\epsilon_ix\circ[x^lq(x^s)]^{(l_2)} \text{ for } i=1,2.$$

As all occurring polynomials have gap-form Lemma 7 is applicable and we find $l\geq 1$ and $s=\mathcal{L}(x^lq(x^s))$. Furthermore

$$u|\mathcal{L}([x^lq(x^s)]^{(l_2)})=\mathcal{L}(x^lq(x^s))=s,$$

thus $\epsilon_i^s=1$, and Lemma 9 yields a representation of type (i) or (ii).

Case 2: Assume (ii) holds for $f_1,\ldots,f_{n-1}$, i.e. we have a representation

$$f_i=\epsilon_ig^{(m_i)} \text{ for } i=1,\ldots,n-1.$$

Here $g(x)=x^kg_1(x^r)$ with $r=\mathcal{L}(g)>1$ and (w.l.o.g.) $\epsilon_1^k\neq 1$. As f_1 permutes with f_n Proposition 6 together with Corollary 2 implies that

$$f_n(x)=\delta_1[xq(x^s)]^{(s_1)} \text{ and}$$

$$f_1(x)=\delta_2[xq(x^s)]^{(s_2)}=\epsilon_1[x^kg_1(x^r)]^{(m_1)}$$

with $\delta_1^s=\delta_2^s=1$. As $[xq(x^s)]>l(xq(x^s))=l(f_1)>1$ we have by Lemma 6

$$s|\mathcal{L}(xq(x^s))=\mathcal{L}(f_1),$$

and similarly

$$\mathcal{L}(f_1)=\mathcal{L}(x^kg_1(x^r))=r.$$

Applying Proposition 7 we find

$$x^kg_1(x^r)=\gamma_1[x^lq_1(x^t)]^{(t_1)} \text{ and} \tag{15}$$

$$xq(x^s) = \gamma_2[x^l q_1(x^t)]^{(t_2)}$$

with $\gamma_1^t = \gamma_2^t = 1$. As

$$[x^l q_1(x^t)]^{(t_1)} \circ \epsilon_1 x = \epsilon_1^k x \circ [x^l q_1(x^t)]^{(t_1)}$$

and $l(x^l q_1(x^t)) = l(x^k g_1(x^r)) > 1$ Lemma 7 implies $l \geq 1$. Thus

$$r = \mathcal{L}(x^k g_1(x^r)) = \mathcal{L}(x^l q_1(x^t)) = t$$

(if t is chosen maximal). From this we obtain

$$f_i(x) = \epsilon_i[x^k g_1(x^r)]^{(m_i)} = \epsilon_i[\gamma_1[x^l q_1(x^t)]^{(t_1)}]^{(m_i)} =$$

$$= \epsilon_i \gamma_1^{l_i}[x^l q_1(x^t)]^{(t_1 m_i)}$$

for some numbers l_i, and

$$f_n(x) = \delta_1[\gamma_2[x^l q_1(x^t)]^{(t_2)}]^{(s_1)} =$$

$$= \delta_1 \gamma_2^{l_n}[x^l q_1(x^t)]^{(s_1 t_2)}$$

for some number l_n. As $r = t$ and $s|r$ we can apply Lemma 9 to obtain a representation either of type (i) or of type (ii).

□

Remark 1 *The splitting of the assertion of Lemma 10 into types (i) and (ii) is justified by the following observation: If type (ii) occurs the polynomials f_i have gap-form and satisfy $f_i(0) = 0$. On the other hand, in case of type (i), arbitrary polynomials with gap-form may occur.*

From (14) and (15) we obtain the following fact.

Remark 2 *In each inductive step the degree of the representing polynomial g does not increase.*

The next lemma shows that the assertion of Lemma 10 remains true in the case that $n \to \infty$.

Lemma 11 *Let $f_1, f_2, \ldots \in \mathbb{C}[x]$, $[f_i] \geq 2$ be a sequence of pairwise permutable polynomials with gap-form, and suppose that no polynomial f_i is conjugated to a power or a Chebyshev polynomial. Then a representation of type (i) or type (ii) of Lemma 10 holds.*

Proof : We apply Lemma 10 to $\{f_1, f_2\}$ and obtain a polynomial g_2 and a representation of the form (11) or (12) employing g_2. Proceeding from this representation we apply the inductive step of the proof of Lemma 10 to $\{f_1, f_2, f_3\}$ and obtain a polynomial g_3 and a representation of the form (11) or (12) employing g_3. Carrying on in this way we get a sequence of polynomials g_n, such that for each n a representation of the form (11) or (12) employing g_n holds for f_i, i up to n. By Remark 2 we have $[g_2] \geq [g_3] \geq \ldots$.

Let g_2 be a polynomial of minimal possible degree, such that f_1 and f_2 admit a representation of the form (11) or (12) involving g_2. Starting the above procedure with this polynomial we get a sequence $g_2, g_3, \ldots$ with $[g_n] \geq [g_2]$, as each g_n yields in particular a representation of f_1 and f_2, by Lemma 9. Thus

$$[g_2] = [g_3] = [g_4] = \ldots \ .$$

We have representations

$$f_i = \epsilon_{i,k} g_k^{(m_i)} \text{ for } i = 1, \ldots, k \text{ and } k \geq 2$$

(independently of whether type (i) or (ii) of Lemma 10 occurs). In particular we have for each $k \geq 3$

$$f_1 = \epsilon_{1,2} g_2^{(m_1)} = \epsilon_{1,k} g_k^{(m_1)}$$

and thus due to Proposition 7

$$g_2(x) = \delta_1 [x^l p(x^r)]^{(s)} \text{ and } g_k(x) = \delta_2 [x^l p(x^r)]^{(s)}$$

with $\delta_1^r = \delta_2^r = 1$. Here obviously $\delta_i x \in \mathcal{G}(f_1)$ for $i = 1, 2$. Thus the numbers δ_i are $\mathcal{L}(f_1)$-th roots of unity, i.e. g_2 and g_k differ only by a $\mathcal{L}(f_1)$-th root of unity. Therefore one specific polynomial $g = \zeta g_2$ (where $\zeta^{\mathcal{L}(f_1)} = 1$) must occur infinitely often among the polynomials g_k and we find

$$f_i = \epsilon_i g^{(m_i)} \text{ for each } i \in \mathbb{N}.$$

Applying Lemma 9 yields the assertion.

□

Lemma 10 and Lemma 11 put us in position to give a complete list of commutative subsemigroups of $\langle \mathbb{C}[x], \circ \rangle$ containing no linear polynomials.

Theorem 1 *Let $\mathcal{S}$ be a commutative subsemigroup of $\langle \mathbb{C}[x], \circ \rangle$ which does not contain any linear polynomial (except possibly x itself). Then $\mathcal{S}$ is conjugated to a subsemigroup of one of the following commutative semigroups:*

List I

(i) $\mathcal{P}_r = \{\zeta x^k | k \equiv 1 \ mod r, \zeta^r = 1\}$,

(ii) $\mathcal{D}_1 = \{t_n | n \in \mathbb{N}\}$,

(iii) $\mathcal{D}_2 = \{\pm t_k | k \ odd\}$,

(iv) $\mathcal{R}_1 = \langle \epsilon_i g^{(m_i)} | i = 1, \ldots, n \rangle$, *where* $n \in \mathbb{N}$, *or* $\mathcal{R}_1 = \langle \epsilon_i g^{(m_i)} | i = 1, 2, \ldots \rangle$, *with* $g(x) = x^k p(x^r)$, $k \geq 0$, $\epsilon_i^r = 1$ *and*

$$\epsilon_i^{k^{m_j}-1} = \epsilon_j^{k^{m_i}-1} \text{ for all } i \text{ and } j.$$

Proof : Let $\mathcal{S}$ be a commutative semigroup which contains no linear polynomials. The cases (i)-(iii) are settled by Proposition 4 and Proposition 5. Thus assume that no element of $\mathcal{S}$ is conjugated to a power or a Chebyshev polynomial. Let $f \in \mathcal{S}$, $[f] = n(> 1)$. A result of E.Jacobsthal (see [19]) states that for any given degree $k(> 1)$ there are at most $n - 1$ polynomials of degree k permuting with f. Thus $\mathcal{S}$ is countable and has in particular an at most countable set of generators $f_1, f_2, \ldots$. By Lemma 5 there is a conjugation Φ_L such that all polynomials $\Phi_L(f_i)$ have gap-form. Applying Lemma 10 or Lemma 11, respectively proves the assertion of the theorem.

□

5 A list of commutative subsemigroups of $\langle \mathbb{C}[x], \circ \rangle$

Together with some well known results Theorem 1 will lead us to a complete list of arbitrary commutative subsemigroups of $\langle \mathbb{C}[x], \circ \rangle$.

First of all let us consider semigroups of linear polynomials. In [14] we find the following result, which holds for an arbitrary field $\Bbbk$.

Proposition 8 *Let $\mathcal{S}$ be a commutative semigroup consisting entirely of linear polynomials. Then $\mathcal{S}$ is conjugated to a subsemigroup of one of the two following commutative semigroups.*

List II

(i) $\mathcal{T} = \{x + a | a \in \Bbbk\}$,

(ii) $\mathcal{S}_0 = \{ax | a \in \Bbbk, a \neq 0\}$.

The next result determines the set $\mathcal{G}^p(f)$, i.e. all linear polynomials permuting with a given nonlinear polynomial.

Proposition 9 *Let $\Bbbk$ be a field of characteristic zero, $f \in \Bbbk[x]$, $[f] \geq 2$ and let Φ_L be a conjugation, such that $f_1 = \Phi_L(f)$ has gap-form. Then $\mathcal{G}^p(f) = \Phi_{L^{(-1)}}(\mathcal{G}^p(f_1))$ and*

List III

(i) $\mathcal{G}^p(f_1) = \{x\}$ *if* $f_1(0) \neq 0$,

(ii) $\mathcal{G}^p(f_1) = \{\zeta x | \zeta^r = 1\}$ *if* $f_1(0) = 0$ *and*

$$r = \max\{u \in \mathbb{N} | f_1(x) = xg(x^u) \text{ for some } g \in \Bbbk[x]\}.$$

A proof of this result can be found in [13]. Proposition 9 yields the well known example of the commutative semigroup $\mathcal{R} = \langle \zeta x, g \rangle$, where $g(x) = xp(x^r)$ and ζ is a primitive r-th root of unity. This is a special case of the commutative semigroup $\mathcal{R}_1$ occurring in Theorem 1 (if we add the linear polynomials ζx): $\mathcal{R}_1 = \langle \epsilon_i g^{(m_i)} | i = 1, \ldots, n \rangle$, where $n \in \mathbb{N}$, or $\mathcal{R}_1 = \langle \epsilon_i g^{(m_i)} | i = 1, 2, \ldots \rangle$ with $g(x) = x^k p(x^r)$, $k \geq 0$, $\epsilon_i^r = 1$ and

$$\epsilon_i^{k^{m_j}-1} = \epsilon_j^{k^{m_i}-1} \text{ for all } i \text{ and } j. \tag{16}$$

The following proposition shows that this seemingly more general type of commutative semigroups actually does not yield "new" semigroups.

Proposition 10 *Consider the commutative semigroup $\mathcal{R}_1 = \langle \epsilon_i g^{(m_i)} | i = 1, \ldots, n \rangle$ ($\mathcal{R}_1 = \langle \epsilon_i g^{(m_i)} | i = 1, 2, \ldots \rangle$, respectively) and assume (w.l.o.g.) that $\gcd(m_1, \ldots, m_n) = 1$ ($\gcd(m_1, m_2, m_3, \ldots) = 1$, respectively). Then there exists an r-th root of unity γ, such that*

$$\mathcal{R}_1 \subseteq \mathcal{R} = \langle \xi x, \gamma g \rangle$$

where ξ is a primitive $\mathcal{L}^p(g)$-th root of unity, i.e. $\mathcal{R}$ is commutative. Furthermore $\mathcal{L}^p(g)$ computes as $\mathcal{L}^p(g) = \gcd(k-1, r)$.

Before we can give a proof of Proposition 10, we have to state another lemma.

Lemma 12 *Let $n \in \mathbb{N}$, $k, r \in \mathbb{N}$, $k, r \geq 2$ and let $m_1, \ldots, m_n \in \mathbb{N}$, $\gcd(m_1, \ldots, m_n) = 1$. Then the set of solutions of the system of congruences*

$$x_i(k^{m_j} - 1) \equiv x_j(k^{m_i} - 1) \ mod r \ for \ i, j = 1, \ldots, n \tag{17}$$

equals the set of all integral linear combinations of the vectors

$$\begin{pmatrix} 1 + k + \ldots + k^{m_1 - 1} \\ 1 + k + \ldots + k^{m_2 - 1} \\ \vdots \\ 1 + k + \ldots + k^{m_n - 1} \end{pmatrix}, \quad \begin{pmatrix} \frac{r}{\gcd(k-1,r)} \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ \ldots \ , \quad \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \frac{r}{\gcd(k-1,r)} \end{pmatrix}. \tag{18}$$

Proof : Obviously every linear combination of vectors (18) gives a solution of the system (17). To show the converse let us first compute the number of modulo r incongruent linear combinations of the vectors (18). Note that

$$\gcd(k^{m_1} - 1, \ldots, k^{m_n} - 1) = k - 1,$$

i.e. there exist numbers $\mu_1, \ldots, \mu_n$, such that

$$k - 1 = \mu_1(k^{m_1} - 1) + \ldots + \mu_n(k^{m_n} - 1).$$

Dividing by $k - 1$ we obtain

$$1 = \mu_1(1 + k + \ldots + k^{m_1 - 1}) + \ldots + \mu_n(1 + k + \ldots + k^{m_n - 1})$$

which yields

$$\gcd(1 + k + \ldots + k^{m_1 - 1}, \ldots, 1 + k + \ldots + k^{m_n - 1}) = 1. \tag{19}$$

Consider a linear combination

$$\lambda_0 \begin{pmatrix} 1 + k + \ldots + k^{m_1 - 1} \\ 1 + k + \ldots + k^{m_2 - 1} \\ \vdots \\ 1 + k + \ldots + k^{m_n - 1} \end{pmatrix} + \lambda_1 \begin{pmatrix} \frac{r}{\gcd(k-1,r)} \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \ldots + \lambda_n \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \frac{r}{\gcd(k-1,r)} \end{pmatrix} \tag{20}$$

and suppose that

$$\lambda_0 \begin{pmatrix} 1 + k + \ldots + k^{m_1 - 1} \\ 1 + k + \ldots + k^{m_2 - 1} \\ \vdots \\ 1 + k + \ldots + k^{m_n - 1} \end{pmatrix} + \begin{pmatrix} \lambda_1 \frac{r}{\gcd(k-1,r)} \\ \vdots \\ \lambda_n \frac{r}{\gcd(k-1,r)} \end{pmatrix} \equiv 0 \bmod r.$$

Then

$$\lambda_0 \begin{pmatrix} 1 + k + \ldots + k^{m_1 - 1} \\ 1 + k + \ldots + k^{m_2 - 1} \\ \vdots \\ 1 + k + \ldots + k^{m_n - 1} \end{pmatrix} \equiv 0 \bmod \frac{r}{\gcd(k-1, r)}$$

and thus (19) implies that

$$\lambda_0 \equiv 0 \bmod \frac{r}{\gcd(k-1,r)}.$$

We found that linear combinations of type (20) with different coefficients λ_0 in $\{1,\ldots,\frac{r}{\gcd(k-1,r)}\}$ yield incongruent solutions (modulo r). For fixed $\lambda_0 \in \{1,\ldots,\frac{r}{\gcd(k-1,r)}\}$ we obviously get $\gcd(k-1,r)^n$ incongruent solutions (modulo r). In fact we found $\frac{r}{\gcd(k-1,r)} \cdot \gcd(k-1,r)^n = \gcd(k-1,r)^{n-1} \cdot r$ incongruent solutions of (17), namely linear combinations of type (20) with $\lambda_0 \in \{1,\ldots,\frac{r}{\gcd(k-1,r)}\}$ and $\lambda_1,\ldots,\lambda_n \in \{1,\ldots,\gcd(k-1,r)\}$.

We use a method which can be found e.g. in [2] (Chapter 4 of Section 2) to compute the number of incongruent solutions of (17).

To do so consider the matrix A of coefficients of the system (17). To illustrate the form of this matrix consider for example the case $n = 4$. Then we have

$$A = \begin{pmatrix} c_2 & -c_1 & 0 & 0 \\ c_3 & 0 & -c_1 & 0 \\ c_4 & 0 & 0 & -c_1 \\ 0 & c_3 & -c_2 & 0 \\ 0 & c_4 & 0 & -c_2 \\ 0 & 0 & c_4 & -c_3 \end{pmatrix}, \text{ with } c_i = k^{m_i} - 1.$$

The rank of the matrix A equals $n-1$. We compute the greatest common divisors d_h of the $h \times h$ subdeterminants of A for $h = 1,\ldots,n-1$. Obviously $(k-1)^h$ divides d_h. On the other hand we can find for each $i = 1,\ldots,n$ an $h \times h$ minor of A with determinant $\pm(k^{m_i}-1)^h$. As $\gcd((k^{m_1}-1)^h,\ldots,(k^{m_n}-1)^h) = (k-1)^h$ we have

$$d_h = (k-1)^h \text{ for } h = 1,\ldots,n-1,$$

where $d_0 = 1$ by convention. Thus the so called elementary divisors of A are given as

$$e_h = \frac{d_h}{d_{h-1}} = k-1 \text{ for } h = 1,\ldots,n-1.$$

Then the number $|A,r|$ of incongruent solutions of (17) is given by the formula

$$|A,r| = \gcd(e_1,r) \cdot \ldots \cdot \gcd(e_{n-1},r) \cdot r = \gcd(k-1,r)^{n-1} \cdot r.$$

Thus each solution of the system (17) is a linear combination of the type (20) which proves the lemma.

□

Proof : [of Proposition 10] If $r = 1$, then no nontrivial roots of unity appear, i.e. $\epsilon_i = 1$. Thus $\mathcal{R}_1 \subseteq \langle g \rangle$.

Suppose therefore $r > 1$ and consider first of all the cases that $k = 0$ or 1. If $k = 0$ we have $g(x) = p(x^r)$ and thus

$$g(x) \circ \epsilon x = g(x) \text{ whenever } \epsilon^r = 1.$$

As $\epsilon_i g^{(m_i)}$ permutes with $\epsilon_j g^{(m_j)}$ we find

$$\epsilon_i g^{(m_i+m_j)} = \epsilon_i g^{(m_i)} \circ \epsilon_j g^{(m_j)} = \epsilon_j g^{(m_j)} \circ \epsilon_i g^{(m_i)} = \epsilon_j g^{(m_j+m_i)},$$

which implies $\epsilon_i = \epsilon_j$. Put $\delta = \epsilon_1$ $(= \epsilon_2 = \epsilon_3 = \ldots)$, then

$$(\delta g)^{(m_i)} = \delta g^{(m_i)}$$

and therefore $\mathcal{R}_1 \subseteq \langle \delta g \rangle$.

In case that $k = 1$ we have

$$g(x) \circ \epsilon x = \epsilon x \circ g(x) \text{ whenever } \epsilon^r = 1.$$

Thus $\mathcal{R}_1 \subseteq \langle \zeta x, g \rangle$ where ζ denotes a primitive r-th root of unity.

In the following we may assume that $k \geq 2$ and $r \geq 2$, which makes the preceding lemma applicable.

Assume for the moment that $\mathcal{R}_1 = \langle \epsilon_i g^{(m_i)} | i = 1, \ldots, n \rangle$ with $n \in \mathbb{N}$. Let ζ be a primitive r-th root of unity and let $\epsilon_i = \zeta^{x_i}$. As the relations (16) hold, we find

$$x_i(k^{m_j} - 1) \equiv x_j(k^{m_i} - 1) \bmod r \text{ for } i, j = 1, \ldots, n.$$

According to Lemma 12 we have

$$x_i \equiv \lambda(1 + k + \ldots + k^{m_i - 1}) + \lambda_i r' \bmod r \text{ for } i = 1, \ldots, n,$$

where $r' = \frac{r}{\gcd(k-1, r)}$.

Let $\gamma = \zeta^{\lambda}$, then

$$(\gamma g)^{(m_i)} = \gamma^{1+k+\ldots+k^{m_i-1}} g^{(m_i)} = \zeta^{\lambda(1+k+\ldots+k^{m_i-1})} g^{(m_i)} = \zeta^{-\lambda_i r'} \cdot \zeta^{x_i} g^{(m_i)}.$$

As $(\zeta^{-\lambda_i r'})^{\gcd(k-1,r)} = 1$ we have

$$\epsilon_i g^{(m_i)} = \delta_i (\gamma g)^{(m_i)} \text{ for } i = 1, \ldots, n,$$

where δ_i are $\gcd(k-1, r)$-th roots of unity. Thus

$$\epsilon_i g^{(m_i)} \in \mathcal{R} = \langle \xi x, \gamma g \rangle,$$

where ξ is a primitive $\gcd(k-1, r)$-th root of unity.

Consider now the case that $\mathcal{R}_1 = \langle \epsilon_i g^{(m_i)} | i = 1, 2, \ldots \rangle$. The numbers

$$f_h = \gcd(k^{m_1} - 1, \ldots, k^{m_h} - 1) \text{ for } h = 1, 2, \ldots$$

satisfy $f_{h+1} | f_h$ for each h. Thus they must remain constant for sufficiently large h, and for such h we have

$$f_h = k - 1 = \gcd(k^{m_1} - 1, k^{m_2} - 1, \ldots)$$

and $\gcd(m_1, \ldots, m_h) = 1$. For each such h we find

$$\epsilon_i g^{(m_i)} \in \langle \xi x, \gamma_h g \rangle \text{ for } i = 1, \ldots, h,$$

where ξ is a primitive $\gcd(k-1, r)$-th root of unity and γ_h is an r-th root of unity. So at least one of the γ_h must occur infinitely often as h increases. Thus we find eventually for each i

$$\epsilon_i g^{(m_i)} \in \langle \xi x, \gamma g \rangle$$

where γ is a fixed r-th root of unity, which proves the assertion of the proposition.

□

Putting together Proposition 8, Proposition 9, Proposition 10 and Theorem 1 we obtain a complete list of commutative semigroups:

Theorem 2 *Let $\mathcal{S}$ be a commutative subsemigroup of $\langle \mathbb{C}[x], \circ \rangle$. Then $\mathcal{S}$ is conjugated to a subsemigroup of one of the following commutative semigroups:*

List IV

(i) (linear polynomials): $\mathcal{T}$, $\mathcal{S}_0$.

(ii) (nonlinear polynomials except the trivial linear polynomial x):

$$\mathcal{P}_1 = \{x^n | n \in \mathbb{N}\},$$

$$\mathcal{D}_1 = \{t_n | n \in \mathbb{N}\},$$

$$\mathcal{Q} = \{g^{(n)} | n \in \mathbb{N}_0\} \text{ with } g \in \mathbb{C}[x], [g] \geq 2,$$

where g has gap-form and is not conjugated to a power or a Chebyshev polynomial.

(iii) (nonlinear polynomials and nontrivial linear polynomials):
$\mathcal{P}_r = \{\zeta x^k | k \equiv 1 \ mod r, \zeta^r = 1\} = \langle \xi x, x^k | k \equiv 1 \ mod r \rangle$ $(r \geq 2)$ where ξ is a primitive r-th root of unity,

$$\mathcal{D}_2 = \{\pm t_k | k \text{ odd}\} = \langle -x, t_k | k \text{ odd} \rangle,$$

$$\mathcal{R} = \langle \zeta x, g \rangle, \text{ where } [g] \geq 2$$

and g is not conjugated to a power or a Chebyshev polynomial, $g(x) = xp(x^r)$, $r = \mathcal{L}^p(g) > 1$ and ζ is a primitive r-th root of unity.

Proof : Let $\mathcal{S}$ be a commutative semigroup. If $\mathcal{S}$ consists entirely of linear polynomials, consider Proposition 8.

If there are nonlinear polynomials in $\mathcal{S}$, consider the subsemigroup $\mathcal{S}'$ of $\mathcal{S}$ which contains all nonlinear polynomials of $\mathcal{S}$. Then, according to Theorem 1, a certain conjugate $\Phi_L(\mathcal{S}')$ of $\mathcal{S}'$ is contained in a semigroup occurring in List I.

Suppose first $\Phi_L(\mathcal{S}') \subseteq \mathcal{P}_r$ and choose r maximal. Then $\Phi_L(\mathcal{S}) \subseteq \mathcal{P}_r$, as no other linear polynomials than ζx $(\zeta^r = 1)$ permute with $\Phi_L(\mathcal{S}')$.

Suppose that $\Phi_L(\mathcal{S}') \subseteq \mathcal{D}_1$ or $\Phi_L(\mathcal{S}') \subseteq \mathcal{D}_2$. As $\mathcal{G}^p(t_n) = \{x\}$ or $\{\pm x\}$ if n is even or odd respectively, we again have $\Phi_L(\mathcal{S}) \subseteq \mathcal{D}_1$ or $\Phi_L(\mathcal{S}) \subseteq \mathcal{D}_2$.

Finally consider the case $\Phi_L(\mathcal{S}') = \mathcal{R}_1 = \langle \epsilon_i g^{(m_i)} | i = 1, \ldots, n \rangle$ or $\langle \epsilon_i g^{(m_i)} | i = 1, 2, \ldots \rangle$ (from the proof of Theorem 1 we see that in this case actually the equality sign holds). According to Proposition 10 we have $\Phi_L(\mathcal{S}') \subseteq \langle \zeta x, g^{(d)} \rangle$ where $d = \gcd(m_1, \ldots, m_n)$ ($\gcd(m_1, m_2, \ldots)$, respectively) and ζ is a primitive $\mathcal{L}^p(g^{(d)})$-th root of unity. Thus $\Phi_L(\mathcal{S}) \subseteq \mathcal{Q}$ or $\Phi_L(\mathcal{S}) \subseteq \mathcal{R}$ holds.

□

6 Maximal commutative semigroups and permutable chains

In this section we give some applications of Theorem 2.

First it is easy to determine all maximal commutative subsemigroups of $\langle \mathbb{C}[x], \circ \rangle$. Note that a maximal commutative semigroup must be conjugated to one of the semigroups listed in List IV. Thus it suffices to give conditions whether a semigroup occurring in List IV is maximal or not. It turns out that, roughly speaking, this is the case whenever the contrary is not obvious.

Theorem 3 *The commutative semigroups $\mathcal{T}, \mathcal{S}_0, \mathcal{P}_r$ ($r = 1, 2, 3, \ldots$), $\mathcal{D}_1$ and $\mathcal{D}_2$ are maximal (among all commutative semigroups).*

The semigroup $\mathcal{Q} = \{g^{(n)} | n \in \mathbb{N}\}$ is maximal if and only if $\mathcal{L}^p(g) = 1$ and g cannot be written in the form $g = f^{(k)}$ for some $f \in \mathbb{C}[x]$ and $k > 1$.

The semigroup $\mathcal{R} = \langle \zeta x, g \rangle$ is maximal if and only if g cannot be written in the form $g = \xi f^{(k)}$ where $\mathcal{L}^p(f) = \mathcal{L}^p(g)$, $k > 1$ and $\xi^{\mathcal{L}^p(g)} = 1$.

Proof : The assertions involving $\mathcal{T}, \mathcal{S}_0, \mathcal{P}_r, \mathcal{D}_1$ and $\mathcal{D}_2$ are proved in [14].

Consider the case of $\mathcal{Q}$: If $\mathcal{L}^p(g) \neq 1$ then $\mathcal{Q} \subsetneq \langle \zeta x, g \rangle$ where ζ is a primitive $\mathcal{L}^p(g)$-th root of unity. Suppose on the other hand that $\mathcal{Q} \subsetneq \mathcal{S}$ and $\mathcal{L}^p(g) = 1$, then $\mathcal{S}$ cannot contain linear polynomials. A conjugate of $\mathcal{S}$ appears in List IV. So the only possibility is that $\mathcal{S}$ is itself of type $\mathcal{Q}$. Thus $\{g^{(n)} | n \in \mathbb{N}\} \subsetneq \{f^{(n)} | n \in \mathbb{N}\}$ which shows that $g = f^{(k)}$ for some $k > 1$.

Consider the case of $\mathcal{R}$ and assume $\mathcal{R} \subsetneq \mathcal{S}$. Then a conjugate $\Phi_L(\mathcal{S})$ must occur in List IV. The only possibility is that $\Phi_L(\mathcal{S})$ is of type $\mathcal{R}$: $\Phi_L(\mathcal{S}) = \langle \xi x, f \rangle$. As g and f both have gap-form the linear polynomial L must be a multiplication. Thus $\mathcal{S} = \langle \xi x, f_1 \rangle$ with $f_1 = \Phi_L(f)$. Furthermore $g = \xi^k x \circ f_1^{(k)}$ and therefore $\mathcal{L}^p(f_1) | \mathcal{L}^p(g)$. On the other hand $\zeta^l x \in \mathcal{R} \subsetneq \mathcal{S}$ for any $\zeta^l x \in \mathcal{G}^p(g)$ and therefore $\mathcal{L}^p(g) | \mathcal{L}^p(f_1)$. Thus $\mathcal{L}^p(g) = \mathcal{L}^p(f_1)$ and as $\mathcal{R} \neq \mathcal{S}$ we must have $k > 1$.

□

As another application we solve a problem of W.Nöbauer. To do so we have to recall some notation.

Let $\mathcal{S}$ be a commutative semigroup. Then the (multiplicative) semigroup $M(\mathcal{S}) = \{[f] | f \in \mathcal{S}\}$ of $\mathbb{N}$ is called the degree of $\mathcal{S}$. Given any subsemigroup M of $\mathbb{N}$ we obviously have the following commutative semigroups $\mathcal{S}$ with $M(\mathcal{S}) = M$:

List V

(i) $\mathcal{S} = \{x^n | n \in M\}$,

(ii) $\mathcal{S} = \{\zeta x^n | n \in M, \zeta^r = 1\}$ if M consists entirely of numbers $\equiv 1 \bmod r$,

(iii) $\mathcal{S} = \{t_n | n \in M\}$,

(iv) $\mathcal{S} = \{\pm t_n | n \in M\}$ if M consists entirely of odd numbers.

For which semigroups M are the above listed $\mathcal{S}$ the only commutative semigroups (apart of conjugates) with $M(\mathcal{S}) = M$?

Theorem 4 *Let M be a (multiplicative) subsemigroup of $\mathbb{N}$. Every commutative semigroup $\mathcal{S}$ with $M(\mathcal{S}) = M$ (apart of conjugates) occurs in List V above if and only if M does not consist entirely of powers of one specific number.*

Proof : Suppose that $M = \{k^n | n \in M_1\}$ for some $k \in \mathbb{N}$ and $M_1 \subseteq \mathbb{N}$. Let g be a polynomial of degree k which is neither conjugated to a power nor to a Chebyshev polynomial. Consider the commutative semigroup $\mathcal{S} = \{g^{(n)} | n \in M_1\}$, then $M(\mathcal{S}) = M$ and no conjugate of $\mathcal{S}$ can occur in List V.

On the other hand suppose $M(\mathcal{S}) = M$ and no conjugate of $\mathcal{S}$ occurs among the semigroups listed above. In the case $M = \{1\}$ we are done. If $M \neq \{1\}$ the only possibility for a conjugate of $\mathcal{S}$ is to be a subsemigroup of either $\mathcal{Q}$ or $\mathcal{R}$ (of List IV). In both cases $M(\mathcal{S}) \subseteq \{k^n | n \in \mathbb{N}\}$ with $k = [g]$.

□

References

[1] C.Alonso & J.Gutierrez & T.Recio: *A rational function decomposition algorithm by near-separated polynomials,*
to appear (in J. of Symb.Comp.).

[2] P.Bachmann: *Zahlentheorie IV. Die Arithmetik der quadratischen Formen,*
Teubner, Leipzig, 1898.

[3] E.A.Bertram: *Polynomials which commute with a Tschebyscheff-Polynomial,*
Amer.Math.Monthly 78 (1971), 650-651.

[4] F.Binder: *Polynomial Decomposition,*
Master Thesis, Univ. Linz, 1994.

[5] F.Binder: *Characterizations of polynomial bidecompositions: A simplified proof,*
to appear in this volume.

[6] H.D.Block & H.P.Thielman: *Commutative polynomials,*
Quart.J.Math. Oxford 2 (2) (1951), 241-243.

[7] L.Böttcher: *Beiträge zur Theorie der Iterationsrechnung (russian),*
Doctoral Dissertation, appeared in Bull.Kasan Math.Soc. 14 (1905), 176.

[8] W.Boyce: *On polynomials which commute with a given polynomial,*
Proc.AMS 33 (2) (1972), 229-234.

[9] F.J.Clauwens & B.J.Clauwens: *Commuting polynomials and λ-ring structures on $\mathbb{Z}[x]$,*
J. of Pure and Appl.Alg. 95 (1994), 261-269.

[10] C.Corrales-Rodrigáñez: *A note on Ritt's theorem on decomposition of polynomials,*
J.of Pure and Appl.Alg. 68 (1990), 293-296.

[11] H.Davenport & D.J.Lewis & A.Schinzel: *Equations of the form $f(x) = g(y)$,*
Quart.J.Math. Oxford 12 (2) (1961), 304-312.

[12] F.Dorey & G.Whaples: *Prime and composite polynomials,*
J. of Algebra 28 (1974), 88-101.

[13] G.Eigenthaler & W.Nöbauer: *Über die mit einem Polynom vertauschbaren linearen Polynome,*
Sb.d.Österr.Akad.d.Wiss., math.-nat.Klasse, Abt.II 199 (1990), 143-153.

[14] G.Eigenthaler & W.Nöbauer & J.Wiesenbauer: *Über Halbgruppen vertauschbarer Polynome,*
Sb.d.Österr.Akad.d.Wiss., math.-nat.Klasse, Abt.II 196 (1987), 227-247.

[15] G.Eigenthaler & R.Winkler: *Commutative composition semigroups of polynomials,*
Contr. to Gen.Alg. 6 (1988), 89-101; Hölder-Pichler-Tempsky und B.G.Teubner, Wien-Stuttgart.

[16] H.T.Engstrøm: *Polynomial substitutions,*
Amer.J.Math. 63 (1941), 249-255.

[17] A.Evyatar & D.B.Scott: *On polynomials in a polynomial,*
Bull.London Math.Soc. 4 (1972), 176-178.

[18] M.P.Fatou: *Sur les équations functionnelles,*
Compt.Rend. Paris 47 (1921), 161-271.

[19] E.Jacobsthal: *Über vertauschbare Polynome,*
Math.Z. 63 (1955), 243-276.

[20] M.Fried: *Arithmetical properties of function fields II. The generalized Schur problem,*
Acta Arithmetica 25 (1974), 225-258.

[21] M.Fried: *On a conjecture of Schur,*
Mich.Math.J. 17 (1970), 41-55.

[22] M.Fried: *On a theorem of Ritt and related Diophantine problems,*
J.f.reine u.angew.Math. 264 (1973), 40-55.

[23] M.Fried & R.E.MacRae: *On curves with separated variables,*
Math.Ann. 180 (1969), 220-226.

[24] M.Fried & R.E.MacRae: *On the invariance of chains of fields,*
Illinois J.Math. 13 (1969), 165-171.

[25] G.Julia: *Permutabilité des fractions rationnelles,*
Ann. de L'Ecole Normale Supérieure 39 (1922), 131-215.

[26] H.Kautschitsch: *Kommutative Teilhalbgruppen der Kompositionshalbgruppe von Polynomen und formalen Potenzreihen,*
Monatsh.f.Math. 74 (1970), 421-436.

[27] H.Kautschitsch: *Über vertauschbare Polynome mit vorgegebenen Gradzahlen,*
Arch.Math. 27 (1976), 611-619.

[28] H.Lausch & W.Nöbauer: *Algebra of polynomials,*
North-Holland, Amsterdam, 1973.

[29] H.Levi: *Composite polynomials with coefficients in an arbitrary field of characteristic zero,* Amer.J.Math. 64 (1942), 389-400.

[30] R.Lidl & W.B.Müller: *On commutative semigroups of polynomials with respect to composition,* Monatsh.f.Math. 102 (1986), 139-153.

[31] W.Nöbauer: *Einige ungelöste Probleme bei Polynomringen,* Coll.Math.Soc.János Bolyai; 6. Rings, Modules & Radicals (Keszthely, Hungary), 1971.

[32] W.Nöbauer: *Some remarks on permutable chains of polynomials,* Contr. to Gen.Alg. 5 (1987), 247-256; Hölder-Pichler-Tempsky und B.G.Teubner, Wien-Stuttgart.

[33] W.Nöbauer: *Über die Operation des Einsetzens in Polynomringen,* Math.Ann. 134 (1958), 248-259.

[34] W.Nöbauer: *Vertauschbare Polynome: An den Grenzen der Koeffizientenvergleichsmethode,* Sb.d.Österr.Akad.d.Wiss., math.-nat.Klasse, Abt.II 196 (1987), 403-417.

[35] O.Ore: *On a special class of polynomials (+ Errata),* Trans.AMS 35 (1933), 559-584; 36 (1934), 275.

[36] J.F.Ritt: *On the iteration of rational functions,* Trans.AMS 21 (1920), 348-356.

[37] J.F.Ritt: *Periodic functions with a multiplication theorem,* Trans.AMS 23 (1922), 16-25.

[38] J.F.Ritt: *Permutable rational functions,* Trans.AMS 25 (1923), 399-448.

[39] J.F.Ritt: *Prime and composite polynomials,* Trans.AMS 23 (1922), 51-66.

[40] T.J.Rivlin: *The Chebyshev polynomials,* J.Wiley, New York, 1974.

[41] A.Schinzel: *Selected topics on polynomials,* University of Michigan Press, Ann Arbor, 1982.

[42] P.Tortrat: *Sur la composition des polynomes,* Coll.Math. 55 (1988), 329-353.

[43] B.L. van der Waerden: *Algebra I,II,* Springer Verlag, Berlin-Heidelberg-New York, 1971.

[44] R.Winkler: *On maximal abelian groups of maps,* J.Austral.Math.Soc. (Ser.A) 55 (1993), 1-7.

[45] U.Zannier: *Ritt's second theorem in arbitrary characteristic,* J.f. reine u.angew.Math. 445 (1993), 175-203.

Harald Woracek
Institut für Technische Mathematik
Technische Universität Wien
Wiedner Hauptstraße 8-10/114
A-1040 Wien, Austria

Günther Eigenthaler
Institut für Algebra
Technische Universität Wien
Wiedner Hauptstraße 8-10/118
A-1040 Wien, Austria