A REMARK ON PERMUTABLE POLYNOMIALS

Günther Eigenthaler, Harald Woracek

Abstract

In this short note, we show that two theorems of J.Ritt, which are concerned with the composition of polynomials over the field of complex numbers, hold more generally for any algebraically closed field of characteristic zero. Both theorems are heavily used in the theory of permutable polynomials.

Let $\mathbb{K}$ be a field and let $\mathbb{K}[x]$ be the polynomial ring over $\mathbb{K}$ in one indeterminate x. The composition $\circ$ of polynomials is the binary operation defined by

$$(f \circ g)(x) = f(g(x)), \ \ f, g \in \mathbb{K}[x].$$

The set $\mathbb{K}[x]$ together with the operation $\circ$ forms a noncommutative monoid with identity x. The polynomials f, g are called permutable, if they satisfy $f \circ g = g \circ f$.

In [EW] there is given a complete list of commutative subsemigroups of $\langle \mathbb{K}[x], \circ \rangle$ for $\mathbb{K} = \mathbb{C}$, the field of complex numbers. In this note we show that these results hold in fact for arbitrary algebraically closed fields $\mathbb{K}$ of characteristic 0.

The proof given in [EW] uses two results of J.Ritt ([R1], [R2], compare also Proposition 4.3 and Proposition 4.4 of [EW]), which are concerned with polynomials having complex coefficients. Apart from this, all other methods used in [EW] depend only on the fact that the coefficient field is algebraically closed and of characteristic 0. Hence, in order to reach our goal, it suffices to generalize the mentioned results of J.Ritt.

Before we can state these results we have to introduce some notation and recall some basic facts concerning the composition semigroup of polynomials.

The units of $\langle \mathbb{K}[x], \circ \rangle$ are exactly the linear polynomials. If $L(x) = ax + b$, $a \neq 0$, its (composition) inverse is given by

$$L^{(-1)}(x) = \frac{1}{a}x - \frac{b}{a}.$$

For any linear polynomial L the mapping

$$\Phi_L(f) = L^{(-1)} \circ f \circ L,\ f \in \mathbb{K}[x],$$

defines an automorphism of $\mathbb{K}[x]$, which is called an inner automorphism. Clearly the set of all inner automorphisms forms a group acting on $\mathbb{K}[x]$. Two polynomials $f, g \in \mathbb{K}[x]$ are said to be conjugated if they belong to the same domain of transitivity with respect to this group, i.e. if there is a unit L, such that $\Phi_L(f) = g$.

In the following $\mathbb{N}$ ($\mathbb{N}_0$) denotes the set of all positive (nonnegative) integers. For $f \in \mathbb{K}[x]$ we denote by $[f]$ the degree of f (in this context $[0] = 0$). Moreover, let $f^{(n)}$ be the n-th power of f with respect to composition: $f^{(n)} = f \circ \cdots \circ f$. Note that $[f \circ g] = [f] \cdot [g]$.

For any field $\mathbb{K}$ with characteristic $\neq 2$, the Chebyshev polynomial t_n defined by the relation

$$\cos(n\alpha) = t_n(\cos\alpha)$$

is a polynomial of degree n with coefficients in the prime field of $\mathbb{K}$ (compare [LN], IV). Now we are able to state the generalizations of Ritt's results:

Theorem 1. *Let $\mathbb{K}$ be an algebraically closed field,* $\operatorname{char}\mathbb{K} = 0$, *and let $f, g \in \mathbb{K}[x]$, $[f], [g] \geq 2$, be given. Assume that f and g are permutable, then there exists a unit $L \in \mathbb{K}[x]$, such that one of the following three cases occurs ($n = [f], m = [g]$):*

(i) $\Phi_L(f) = ax^n,\ \Phi_L(g) = bx^m,\ a, b \in \mathbb{K} \setminus \{0\}$,

(ii) $\Phi_L(f) = \pm t_n,\ \Phi_L(g) = \pm t_m$,

(iii) $\Phi_L(f) = \varepsilon_1 h^{(s)}$, $\Phi_L(g) = \varepsilon_2 h^{(t)}$, *where $h \in \mathbb{K}[x]$ is of the form $h(x) = xp(x^r)$, $p \in \mathbb{K}[x]$, $r \in \mathbb{N}$, $\varepsilon_1^r = \varepsilon_2^r = 1$, and $s = \frac{n}{[h]}$, $t = \frac{m}{[h]}$.*

Theorem 2. *Let $\mathbb{K}$ be an algebraically closed field,* $\operatorname{char}\mathbb{K} = 0$, *let $f, g \in \mathbb{K}[x]$, $[f], [g] \geq 2$, and let roots of unity $\varepsilon, \delta \in \mathbb{K}$ be given. Assume that for some numbers $l, l' \in \mathbb{N}$ and $u, v \in \mathbb{N}$ the relations*

$$f \circ \varepsilon x = \varepsilon^l x \circ f,\ g \circ \delta x = \delta^{l'} x \circ g \text{ and } \varepsilon f^{(u)} = \delta g^{(v)}$$

hold. Then there exist a unit $L \in \mathbb{K}[x]$, a polynomial $h(x) = x^k p(x^r)$, $p \in \mathbb{K}[x], k \in \mathbb{N}_0, r \in \mathbb{N}, p(0) \neq 0$, and $\varepsilon_1, \varepsilon_2 \in \mathbb{K}$, $\varepsilon_1^r = \varepsilon_2^r = 1$, such that ($s = \frac{[f]}{[h]}, t = \frac{[g]}{[h]}$)

$$\Phi_L(f) = \varepsilon_1 h^{(s)},\ \Phi_L(g) = \varepsilon_2 h^{(t)}.$$

As mentioned before, for the complex number field $\mathbb{K} = \mathbb{C}$ these results have been proved by J.Ritt, for Theorem 1 see [R2], for Theorem 2 see [R1].

The proofs of Theorem 1 and Theorem 2 depend on the following two well known facts from field theory:

Lemma 3. *Every countable field of characteristic* 0 *can be embedded into* $\mathbb{C}$.

Lemma 4. *Let a system of algebraic equations in finitely many variables over some field* $\mathbb{L}$ *be given, and suppose that the system has a solution in some extension field of* $\mathbb{L}$*, then there exists a solution in the algebraic closure of* $\mathbb{L}$.

Lemma 3 is obvious and Lemma 4 is a consequence of Hilbert's Nullstellensatz (see e.g. [K]).

Proof (of Theorem 1): Let $f(x) = a_n x^n + \ldots + a_1 x + a_0$, $f(x) = b_m x^m + \ldots + b_1 x + b_0$, and let $\mathbb{L}$ be the algebraic closure of $\mathbb{Q}(a_0, \ldots, a_n, b_0, \ldots, b_m)$, where $\mathbb{Q}$ is the prime field of $\mathbb{K}$. Then by Lemma 3, there exists an embedding $\varphi : \mathbb{L} \to \mathbb{C}$, which can be extended to an embedding $\psi : \mathbb{L}[x] \to \mathbb{C}[x]$ with $\psi(x) = x$. Since ψ is a composition homomorphism (see [LN], III.1), the polynomials $\psi(f), \psi(g) \in \mathbb{C}[x]$ are permutable.

Since Theorem 1 holds for $\mathbb{K} = \mathbb{C}$, there exists a unit $L \in \mathbb{C}[x]$, such that one of the cases *(i)*-*(iii)* occurs with $\psi(f), \psi(g)$ instead of f, g.

As it is easy to see by comparing coefficients, *(i)* is equivalent to a system of algebraic equations for a, b and the coefficients of L, *(ii)* to a system for the coefficients of L only, and *(iii)* to a system for $\varepsilon_1, \varepsilon_2$ and the coefficients of L and p (with fixed r, s, t).

In any case a solution in $\mathbb{C}$ exists, hence by Lemma 4 there is a solution in $\varphi(\mathbb{L})$. An application of ψ^{-1} completes the proof of Theorem 1.

□

Proof (of Theorem 2): The proof runs along the same lines as that of Theorem 1: the condition $p(0) \neq 0$ does not cause any troubles, the other conditions (with fixed k, r, s, t) are again equivalent to a system of algebraic equations.

□

Corollary 5. *All results in [EW] on commutative composition semigroups of polynomials hold for any algebraically closed field of characteristic* 0.

Acknowledgements: The authors are indebted to the referee for a valuable suggestion concerning Hilbert's Nullstellensatz.
As M.Goldstern pointed out, Theorem 1 and Theorem 2 can also be obtained by using Tarski's Theorem on algebraically closed fields (see e.g. [V]).

References

[EW] G.Eigenthaler, H.Woracek: *Permutable polynomials and related topics,*
Contributions to General Algebra 9 (1995), 163-182, Hölder-Pichler-Tempsky und B.G.Teubner, Wien-Stuttgart.

[K] E.Kunz: *Einführung in die kommutative Algebra und algebraische Geometrie,* Vieweg, Braunschweig, 1980.

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

[R1] J.F.Ritt: *On the iteration of rational functions,*
Trans.AMS 21 (1920), 348-356.

[R2] J.F.Ritt: *Permutable rational functions,*
Trans.AMS 25 (1923), 399-448.

[V] R.L.Vaught: *Alfred Tarski's work in model theory,*
J.Symbolic logic 51 (1987), 869-882.

Günther Eigenthaler
Institut für Algebra und
Diskrete Mathematik
Technische Universität Wien
Wiedner Hauptstraße 8-10/118.1
A-1040 Wien
AUSTRIA
email: g.eigenthaler@tuwien.ac.at

Harald Woracek
Institut für Analysis, Technische
Mathematik und
Versicherungsmathematik
Technische Universität Wien
Wiedner Hauptstraße 8-10/114.1
A-1040 Wien
AUSTRIA
email: hworacek@pop.tuwien.ac.at

AMS Classification numbers: 12E10, 20M14, 20M20