RATIONAL FUNCTIONS WITH LINEAR RELATIONS

ARIANE M. MASUDA AND MICHAEL E. ZIEVE

Abstract. We find all polynomials f, g, h over a field K such that g and h are linear and $f(g(x)) = h(f(x))$. We also solve the same problem for rational functions f, g, h, in case the field K is algebraically closed.

1. Introduction

Around 1920, Fatou, Julia and Ritt made profound investigations of functional equations. In particular, they wrote at length on commuting rational functions: that is, $f, g \in \mathbb{C}(x)$ with $f(g(x)) = g(f(x))$. Fatou and Julia [7, 8] found all solutions when the Julia set of f or g is not the Riemann sphere. This includes the case of polynomials of degree at least 2, where up to conjugacy by a linear polynomial, either $f = x^n$ and $g = x^m$ are power polynomials, or $f = T_n$ and $g = T_m$ are Chebychev polynomials, or f and g have a common iterate. Using different methods which did not require the Julia set hypothesis, Ritt [12] determined precisely when two polynomials have a common iterate, and moreover [14] he found all commuting rational functions. Years later, Eremenko [6] proved Ritt's results using methods of modern iteration theory.

Julia showed that commuting rational functions have the same Julia set. Conversely, much subsequent work has shown that rational functions with the same Julia set are related to commuting rational functions (cf. [9] and the references therein). In particular, for polynomials this relationship involves composition with a rotational symmetry of the Julia set.

Several authors have considered analogous questions over fields K of positive characteristic, but there are few satisfactory results. There

Date: 12 May 2007.

2000 *Mathematics Subject Classification.* Primary 39B12; Secondary 12E05, 30D05.

Key words and phrases. Functional equation, commuting rational functions.

The authors thank Bob Beals, Alan Beardon, Alex Erëmenko and Patrick Ng for useful correspondence.

are new types of examples, for instance any two additive polynomials $\sum_i a_i x^{p^i}$ over the prime field $\mathbb{F}_p$ commute.

In fact, challenges arise already in finding the commuting polynomials $f, g \in K[x]$ in the special case $\deg(g) = 1$. Wells [15] and Mullen [10] solved this problem over finite fields K, so long as $\deg(f) < \#K$. Park [11] proved similar results. Eigenthaler and Nöbauer [5] solved the problem in various special cases, for instance if $\deg(f) = \operatorname{char}(K)$. In this paper we solve the problem in general, and more generally we find all $f, g, h \in K[x]$ with $\deg(g) = \deg(h) = 1$ such that $f \circ g = h \circ f$:

Theorem 1.1. *Let K be a field. The entries in the following list with $f \notin K$ comprise all values $\alpha, \beta, \gamma, \delta \in K$ and $f \in K[x] \setminus K$ such that $\alpha, \gamma \neq 0$ and $f(\alpha x + \beta) = \gamma f(x) + \delta$:*

(0) *$\alpha = \gamma = 1$, $\beta = \delta = 0$, and $f \in K[x]$;*

(1) *$\alpha = \gamma = 1$, $\beta \neq 0$, and $f = (\delta/\beta)x + r$ with*

$$\begin{cases} r \in K & \textit{if } \operatorname{char}(K) = 0 \\ r \in K[x^p - \beta^{p-1}x] & \textit{if } \operatorname{char}(K) = p > 0; \end{cases}$$

(2) *$\alpha \neq 1$, $\gamma = \alpha^e$, and $f = f_0 + f_1(x - \beta/(1-\alpha))$, where $e, s \in \mathbb{Z}_{\geq 0}$, $f_1 \in x^e K[x^s]$, $\alpha^s = 1$, and $f_0 \in K$ satisfies $\delta = (1 - \gamma) \cdot f_0$.*

In case $K = \mathbb{C}$, the polynomials in (2) are those for which the Julia set has a rotational symmetry [3]. Moreover, Ritt showed [13] that the decomposition of a complex polynomial into indecomposables is unique, except for nonuniqueness coming from composing a linear with its inverse, or using the commutativity of Chebychev polynomials, or using the identity $x^s \circ x^e\psi(x^s) = x^e\psi(x)^s \circ x^s$. Note that the polynomials $x^e\psi(x^s)$ from this identity occur in (2). Ritt's identity has a characteristic p analogue [4], namely $(x^p - x) \circ (x + \psi(x^p - x)) = (x + \psi^p - \psi) \circ (x^p - x)$, and it is interesting that the polynomials $x + \psi(x^p - x)$ occur in (1).

We also prove an analogous result for rational functions:

Theorem 1.2. *Let K be a field of characteristic $p \geq 0$. The entries in the following list with $f \notin K$ comprise all $g, h \in K(x)$ and $f \in K(x) \setminus K$ such that $f \circ g = h \circ f$ and each of g and h has degree one and has a fixed point in $K \cup \{\infty\}$; here $u, v, \psi \in K(x)$ and* $\deg(u) = \deg(v) = 1$:

(1) *$f = u^{-1} \circ (\delta x + \psi(x^p - x)) \circ v^{-1}$, $g = v(v^{-1}(x) + 1)$, and $h = u^{-1}(u(x) + \delta)$, where $\delta \in K$, and if $p = 0$ then $\psi \in K$;*

(2) *$f = u^{-1} \circ x^e\psi(x^s) \circ v^{-1}$, $g = v(\alpha v^{-1}(x))$, $h = u^{-1}(\alpha^e u(x))$, where $e, s \in \mathbb{Z}$, $\alpha \in K^*$, and $\alpha^s = 1$.*

Our hypothesis on fixed points is always true if K is algebraically closed. To apply this result to arbitrary fields K, one might need u, v, ψ to have coefficients in an extension of K.

In case $K = \mathbb{C}$, these results were proved by af Hällström [1, 2]. His method has some features in common with ours, but is somewhat more complicated.

We give a quick inductive proof of Theorem 1.1 in the next section. Then in Sections 3 and 4 we use ideas from dynamics and Galois theory to prove Theorem 1.2, which yields another proof of Theorem 1.1. Finally, in Section 5 we deduce the results of Wells [15], Mullen [10] and Park [11] as consequences of Theorem 1.1.

2. Polynomial solutions

In this section we prove Theorem 1.1.

Pick $\alpha, \beta, \gamma, \delta \in K$ with $\alpha, \gamma \neq 0$, and let $f \in K[x]$ have degree $n > 0$. We will determine when $f(\alpha x + \beta) = \gamma f(x) + \delta$. We assume $\gamma = \alpha^n$, since otherwise $f(\alpha x + \beta)$ and $\gamma f(x) + \delta$ have distinct leading coefficients. First suppose $\alpha = 1$, so $\gamma = 1$. If $\beta = 0$ then our equation becomes $f(x) = f(x) + \delta$, so $\delta = 0$; conversely, if $\beta = \delta = 0$ then trivially every f is a solution. So assume $\beta \neq 0$, and put $r := f - (\delta/\beta)x$; then f satisfies $f(x + \beta) = f(x) + \delta$ if and only if r satisfies $r(x+\beta) = r(x)$. Let $p := \operatorname{char}(K)$ and $m := \deg(r)$. If $p \nmid m$ then there are no such r, since $r(x + \beta) - r(x)$ has degree $m - 1$. In particular, if $p = 0$ then $r \in K$, so assume $p > 0$. Plainly every $\hat{r} \in K[x^p - \beta^{p-1}x]$ satisfies $\hat{r}(x + \beta) = \hat{r}(x)$. For any $r \in K[x]$ with $r(x + \beta) = r(x)$, we know that $p \mid \deg(r)$, so there is some $\hat{r} \in K[x^p - \beta^{p-1}x]$ which has the same leading term as r; but then $\tilde{r} := r - \hat{r}$ satisfies $\tilde{r}(x) = \tilde{r}(x + \beta)$ and $\deg(\tilde{r}) < \deg(r)$, so it follows by induction on $\deg(r)$ that $r \in K[x^p - \beta^{p-1}x]$.

Now suppose $\alpha \neq 1$. Let s be the multiplicative order of α, if this order is finite; otherwise put $s = 0$. Thus the integers m with $\alpha^m = 1$ are precisely the multiples of s. Let u be the leading coefficient of f, and put $\hat{f} := u \cdot (x - \beta/(1 - \alpha))^n$; then

$$\hat{f}(\alpha x + \beta) = u \cdot (\alpha x - \alpha\beta/(1 - \alpha))^n = u\alpha^n \cdot (x - \beta/(1 - \alpha))^n = \gamma \hat{f}(x).$$

Now put $\tilde{f} := f - \hat{f}$, and note that $\tilde{n} := \deg(\tilde{f}) < n$; moreover, f satisfies $f(\alpha x + \beta) = \gamma f(x) + \delta$ if and only if $\tilde{f}$ satisfies $\tilde{f}(\alpha x + \beta) = \gamma \tilde{f}(x) + \delta$. If $\tilde{n} > 0$, then the leading coefficients of $\tilde{f}(\alpha x + \beta)$ and $\gamma \tilde{f}(x) + \delta$ are identical if and only if $\alpha^{\tilde{n}} = \gamma = \alpha^n$, or equivalently $\tilde{n} \equiv n \pmod{s}$. By induction on $\deg(f)$, it follows that f satisfies $f(\alpha x + \beta) = \gamma f(x) + \delta$ if and only if $f = f_0 + f_1(x - \beta/(1 - \alpha))$ where $f_0 \in K$ satisfies $f_0 = \gamma f_0 + \delta$ and $f_1 \in xK[x]$ has only terms of degree congruent to $n \pmod{s}$. The result follows. □

3. Solutions involving scalings or translations

In this section we solve the equation $f \circ g = h \circ f$ in rational functions $f, g, h \in K(x)$ where $g, h \in xK^* \cup \{x+1\}$. Here K is a field of characteristic $p \geq 0$. Let $L = K(x^p - x)$ if $p > 0$, and put $L = K$ if $p = 0$.

Lemma 3.1. *For $f \in K(x)$, we have $f(x+1) = f(x)$ if and only if $f \in L$.*

Proof. Let σ be the K-automorphism of $K(x)$ which maps $x \mapsto x+1$. Then L is the subfield of $K(x)$ fixed by σ. Thus $f \in L$ if and only if $\sigma(f) = f$, or equivalently $f(x+1) = f(x)$. □

Corollary 3.2. *For $f \in K(x)$, we have $f(x+1) = f(x) + 1$ if and only if $f - x \in L$.*

Proof. Putting $r(x) := f(x) - x$, we have $f(x+1) = f(x) + 1$ if and only if $r(x+1) = r(x)$, so the result follows from Lemma 3.1. □

Corollary 3.3. *For any $\gamma \in K$ and $f \in K(x)$ with $f \neq 0$, we have $f(x+1) = \gamma f(x)$ if and only if $\gamma = 1$ and $f \in L$.*

Proof. The leading terms of both the numerator and denominator of $f(x)$ are identical to those of $f(x+1)$, so if $f(x+1) = \gamma f(x)$ then $\gamma = 1$; now the result follows from Lemma 3.1. □

Lemma 3.4. *For any $\alpha, \gamma \in K^*$ and any nonzero $f \in K[x]$, we have $f(\alpha x) = \gamma f(x)$ if and only if $f = x^e \psi(x^s)$ for some $\psi \in K[x]$ and $e, s \in \mathbb{Z}_{\geq 0}$ with $\alpha^e = \gamma$ and $\alpha^s = 1$.*

Proof. Equate coefficients of terms of the same degrees in $f(\alpha x)$ and $\gamma f(x)$. □

Corollary 3.5. *For any $\alpha, \gamma \in K^*$ and any nonzero $f \in K(x)$, we have $f(\alpha x) = \gamma f(x)$ if and only if $f = x^e \psi(x^s)$ for some $\psi \in K(x)$ and $e, s \in \mathbb{Z}$ with $\alpha^e = \gamma$ and $\alpha^s = 1$.*

Proof. The 'if' direction is clear, so suppose $f(\alpha x) = \gamma f(x)$. Write $f = f_1/f_2$ with coprime $f_1, f_2 \in K[x]$. Then the denominators of $f(\alpha x)$ and $\gamma f(x)$ are $f_2(\alpha x)$ and $f_2(x)$, so $f_2(\alpha x) = \eta f_2(x)$ for some $\eta \in K^*$. Thus $f_1(\alpha x) = \gamma \eta f_1(x)$. Now the result follows by applying Lemma 3.4 to both f_1 and f_2. □

Lemma 3.6. *For $\alpha \in K^*$ and $f \in K(x)$, we have $f(\alpha x) \neq f(x) + 1$.*

Proof. Suppose to the contrary that $f(\alpha x) = f(x) + 1$. Plainly $x = 0$ must be a pole of f. Write $f = f_1/f_2$ with coprime $f_1, f_2 \in K[x]$ (so $f_1(0) \neq 0$ and $f_2(0) = 0$, whence $\deg(f_2) > 0$). Then the denominators of $f(\alpha x)$ and $f(x)+1$ are $f_2(\alpha x)$ and $f_2(x)$, so we have $f_2(\alpha x) = \eta f_2(x)$ for some $\eta \in K^*$. Then

$$\frac{f_1(\alpha x)}{f_2(\alpha x)} = \frac{f_1(x)}{f_2(x)} + 1$$

implies that

$$\frac{f_1(\alpha x)}{\eta} = f_1(x) + f_2(x).$$

Since $f_1(0) \neq 0$ and $f_2(0) = 0$, substituting $x = 0$ gives $\eta = 1$. Thus $f_2(\alpha x) = f_2(x)$; since f_2 is nonconstant, it follows that $s := \#\langle\alpha\rangle < \infty$ and $f_2 \in K[x^s]$. But then $f_1(\alpha x) - f_1(x) = f_2(x) \in K[x^s]$, which is impossible since $f_1(\alpha x) - f_1(x)$ has no terms of degree divisible by s. $\square$

4. Solutions with arbitrary linears

In this section we solve the equation $f \circ g = h \circ f$ in rational functions $f, g, h \in K(x)$ with $\deg(g) = \deg(h) = 1$. Here K is a field of characteristic $p \geq 0$. We will reduce to the cases considered in the previous section, by means of the following observation: if $u, v \in K(x)$ satisfy $\deg(u) = \deg(v) = 1$, then $f \circ g = h \circ f$ if and only if $F \circ G = H \circ F$, where $F := u \circ f \circ v$, $G := v^{-1} \circ g \circ v$, and $H := u \circ h \circ u^{-1}$.

First consider the case of polynomials $f, g, h \in K[x]$. Then $g = \alpha x + \beta$ for some $\alpha, \beta \in K$ with $\alpha \neq 0$. If $\alpha \neq 1$ then $v := x + \beta/(1-\alpha)$ satisfies $v^{-1} \circ g \circ v = \alpha x$. If $\alpha = 1$ and $\beta \neq 0$ then $v := \beta x$ satisfies $v^{-1} \circ g \circ v = x+1$. Thus, in any case there is a degree-one $v \in K[x]$ such that $G := v^{-1} \circ g \circ v$ is either αx or $x+1$. Likewise, writing $h = \gamma x + \delta$, there is a degree-one $u \in K[x]$ such that $H := u \circ h \circ u^{-1}$ is either γx or $x + 1$. Now the above observation, in combination with the results of the previous section, implies the following version of Theorem 1.1:

Theorem 4.1. *The polynomials $f, g, h \in K[x]$ such that $f \circ g = h \circ f$ and $\deg(g) = \deg(h) = 1 \leq \deg(f)$ are as follows; here $u, v, \psi \in K[x]$ and $\deg(u) = \deg(v) = 1$:*

(1) *$f = u^{-1} \circ (x + \psi(x^p - x)) \circ v^{-1}$, $g = v(v^{-1}(x) + 1)$, and $h = u^{-1}(u(x) + 1)$, where if $p = 0$ then $\psi \in K$;*

(2) *$p > 0$, $f = \psi(x^p - x) \circ v^{-1}$, $g = v(v^{-1}(x)+1)$, and $h = x$, where $\deg(\psi) > 0$;*

(3) *$f = u^{-1} \circ x^e \psi(x^s) \circ v^{-1}$, $g = v(\alpha v^{-1}(x))$, $h = u^{-1}(\alpha^e u(x))$, where $e, s \in \mathbb{Z}_{\geq 0}$, $\alpha \in K^*$, $\alpha^s = 1$, and $\deg(x^e \psi(x^s)) > 0$.*

Note that we can combine the first two possibilities into the single possibility $f = u^{-1} \circ (\delta x + \psi(x^p - x)) \circ v^{-1}$, $g = v(v^{-1}(x) + 1)$, and $h = u^{-1}(u(x) + \delta)$ with $\delta \in K$.

Next we consider rational functions. Any degree-one $g \in K(x)$ has a fixed point ρ, though this fixed point might lie in a quadratic extension of K. If $\rho = \infty$ then $g \in K[x]$; if $\rho \neq \infty$ then for $v = \rho + 1/x$ we see that $v^{-1} \circ g \circ v$ fixes ∞, and hence lies in $K[x]$. We can then proceed as above, resulting in a proof of Theorem 1.2.

5. Derivation of prior results

In this section we explain how Theorem 1.1 relates to the results of Wells [15], Mullen [10], and Park [11], all of which were formulated in a quite different manner.

It follows from Theorem 1.1 that, if K is a field of characteristic $p > 0$, and if we prescribe elements $\beta, \delta \in K$ with $\beta \neq 0$, then the polynomials $f \in K[x]$ such that $f(x + \beta) = f(x) + \delta$ are precisely the elements of $(\delta/\beta)x + K[x^p - \beta^{p-1}x]$. In particular, writing $f = \sum_{i=0}^{n} f_i x^i$, we see that the coefficients $f_0, f_p, f_{2p}, \ldots$ can be arbitrary elements of K, and these coefficients uniquely determine all the other f_i's. This generalizes the results of Wells and Park.

Wells [15] restricted to the case that $K = \mathbb{F}_q$ is finite, $\deg(f) < q$, and $\delta = \beta$. Wells used a different method. Namely, by considering terms of degree x^{i-1} in the functional equation $f(x + \beta) = f(x) + \beta$, one can solve for if_i in terms of the coefficients f_j with $j > i$; thus, by successively computing $f_n, f_{n-1}, \ldots, f_1$, we see that the coefficients f_i with $p \nmid i$ are uniquely determined by the coefficients f_{pj}. Hence there are at most $q^{q/p}$ possibilities for f; but this equals the number of mappings $\mathbb{F}_q \to \mathbb{F}_q$ which commute with the map $x \mapsto x + \beta$. Since every mapping $\mathbb{F}_q \to \mathbb{F}_q$ is induced by a unique polynomial of degree less than q, it follows that the f_{pj} can be arbitrary elements of $\mathbb{F}_q$. On the other hand, as noted above, this fact follows at once from our expression $x + K[x^p - \beta^{p-1}x]$ for all such f's.

Park [11] considered the case that K is finite, $\deg(f) < p^2$, and $\beta, \delta \in K^*$. He wrote out the conditions on the f_j's coming from equating terms of like degrees in the functional equation $f(x+\beta) = f(x)+\delta$, and proved his result via several pages of calculations involving binomial coefficients. In these calculations, the hypothesis $\deg(f) < p^2$ yielded crucial simplifications.

Next suppose $\alpha \in K^*$ is a primitive s^{th} root of unity, and suppose $\gamma = \alpha^e$ with $0 < e < s$. Fix $\beta, \delta \in K$. By Theorem 1.1, the polynomials $f \in K[x]$ such that $f(\alpha x + \beta) = \gamma f(x) + \delta$ are precisely the elements of

$$\frac{\delta}{1-\gamma} + \left(x - \frac{\beta}{1-\alpha}\right)^e K\left[\left(x - \frac{\beta}{1-\alpha}\right)^s\right].$$

In particular, writing $f = \sum_{i=0}^{n} f_i x^i$, the coefficients f_{e+sj} can be arbitrary elements of K, and these coefficients uniquely determine all the other f_i's. This generalizes the main result proved by Mullen.

Mullen [10] restricted to the case that $K = \mathbb{F}_q$ is finite, $\deg(f) < q$, $\gamma = \alpha$ and $\delta = \beta$. He used the same method as Wells: equating coefficients of x^i in $f(\alpha x + \beta) = \alpha f(x) + \beta$ enables one to express $(\alpha^i - \alpha)f_i$ in terms of $f_{i+1}, f_{i+2}, \dots, f_n$. Since $\alpha^i \neq \alpha$ if $i \not\equiv 1 \pmod{s}$, it follows that all the f_i's are uniquely determined by the coefficients f_{1+sj}. Hence there are at most $q^{(q-1)/s}$ possibilities for f; but this equals the number of mappings $\mathbb{F}_q \to \mathbb{F}_q$ which commute with $x \mapsto \alpha x + \beta$, so the coefficients f_{1+sj} can be arbitrary elements of $\mathbb{F}_q$.

Remark. As stated, [10, Thm. 1] asserts that two polynomials are equal if they have the same coefficients. The proof in [10] shows that the result would remain true (and become nontrivial) if we require $p \nmid s$ when $b = 1$, and $\#\langle b \rangle \nmid (s-1)$ if $b \neq 1$. Our comments above refer to this corrected version of Mullen's result. Also, the papers [15, 10] comment on polynomials over $\mathbb{F}_q$ of degree $\geq q$ which commute with linear polynomials, but in those papers commutation is only studied modulo $x^q - x$; in other words, they consider $f(\alpha x + \beta) = \alpha f(x) + \beta$ as an equality of functions on $\mathbb{F}_q$, rather than an equality of polynomials.

To summarize, it seems that the complications Wells, Mullen and Park encountered were caused by their desire to phrase the results in terms of the coefficients of f as an element of $K[x]$; the key to our simpler presentation is that we directly represent f in terms of an additive subgroup of $K[x]$.

References

1. G. af Hällström, *Über halbvertauschbare Polynome*, Acta Acad. Abo. **21** (1957), no. 2, 20 pp.
2. ______, *Über Halbvertauschbarkeit zwischen linearen und allgemeineren rationalen Funktionen*, Math. Japon. **4** (1957), 107–112.
3. I. N. Baker and A. Erëmenko, *A problem on Julia sets*, Ann. Acad. Sci. Fenn. **12** (1987), 229–236.
4. R. M. Beals and M. E. Zieve, *Decompositions of polynomials*, preprint, 2007.
5. G. Eigenthaler and W. Nöbauer, *Über die mit einem Polynom vertauschbaren linearen Polynome*, Österreich. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. II **199** (1990), 143–153.
6. A. È. Erëmenko, *Some functional equations connected with the iteration of rational functions*, Algebra i Analiz **1** (1989), 102–116; English transl., Leningrad Math. J. **1** (1990), 905–919.)
7. P. Fatou, *Sur l'iteration analytique et les substitutions permutables*, J. Math. Pures Appl. (9) **2** (1923), 343–384.

8. G. Julia, *Mémoire sur la permutabilité des fractions rationnelles*, Ann. Acad. École Norm. Sup. **39** (1922), 131–215.
9. G. M. Levin and F. Przytycki, *When do two rational functions have the same Julia set?*, Proc. Amer. Math. Soc. **125** (1997), 2179–2190.
10. G. L. Mullen, *Polynomials over finite fields which commute with linear permutations*, Proc. Amer. Math. Soc. **84** (1982), 315–317.
11. H. G. Park, *Polynomials satisfying $f(x+a) = f(x) + c$ over finite fields*, Bull. Korean Math. Soc. **29** (1992), 277–283.
12. J. F. Ritt, *On the iteration of rational functions*, Trans. Amer. Math. Soc. **21** (1920), 348–356.
13. ———, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), 51–66.
14. ———, *Permutable rational functions*, Trans. Amer. Math. Soc. **25** (1923), 399–448.
15. C. Wells, *Polynomials over finite fields which commute with translations*, Proc. Amer. Math. Soc. **46** (1974), 347–350.

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, ON K1S 5B6, Canada.

Current address: Department of Mathematics and Statistics, University of Ottawa, Ottawa, ON K1N 6N5, Canada.

E-mail address: amasuda@uottawa.ca

Center for Communications Research, 805 Bunn Drive, Princeton, NJ 08540-1966, USA.

E-mail address: zieve@math.rutgers.edu

URL: http://www.math.rutgers.edu/∼zieve/