D'après la remarque qui précède, il y a par suite 3 cas possibles, à savoir $2t+\varepsilon = 1$, $2t+\varepsilon = 16$ et $2t+\varepsilon \geqslant 34$, qui donnent respectivement $t = 0$, $\varepsilon = 1$ et $a = 1$, ou bien $t = 1$, $\varepsilon = -1$ et $a = F_3 - 1 = 2^8$, ou bien $t = 8$, $\varepsilon = 0$ et $a = 8F_3$, ou bien $t \geqslant 17$, $\varepsilon \geqslant 0$ et $a \geqslant F_2 F_3$, ou enfin $t \geqslant 18$ et $a \geqslant 18F_3 - 1$. Donc, (2) entraîne pour $a \geqslant 1$ que

(3) $\quad a = 1$, ou bien $a = 2^8$, ou bien $a = 8F_3$, ou bien $a \geqslant F_2F_3$.

Ceci établi, examinons les $a > 1$ naturels assujettis à (1). On a $a = F_4 t + \varepsilon$ (où $t \geqslant 1$ et $\varepsilon = 0$ ou $\varepsilon = \pm 1$) et vu que $F_4 \equiv 2 \pmod{F_1F_2F_3}$, on conclut que $F_1F_2F_3 \mid (2t+\varepsilon)[(2t+\varepsilon)^2 - 1]$.

D'après (3), on a ici $2t+\varepsilon = 1$, ou bien $2t+\varepsilon = 2^8$, ou bien $2t+\varepsilon = 8F_3$, ou enfin $2t+\varepsilon \geqslant F_2F_3$, ce qui donne 5 cas possibles suivants:

1. $t = 1$, $\varepsilon = -1$, $a = F_4 - 1 = a_1$;
2. $t = 2^7$, $\varepsilon = 0$, $a = 2^7 F_4 = a_2$;
3. $t = 4F_3$, $\varepsilon = 0$, $a = 4F_3F_4 = a_3$;
4. $t = \frac{1}{2}(F_2F_3 - 1)$, $\varepsilon = 1$, $a = \frac{1}{2}F_4(F_2F_3 - 1) + 1 = a_4$;
5. $t \geqslant \frac{1}{2}(F_2F_3 + 1)$, $a \geqslant \frac{1}{2}F_4(F_2F_3 + 1) - 1 = a_5$.

Or $a_1^2 + 1 = F_5$, $13 \mid a_2^2 + 1$, $37 \mid a_3^2 + 1$, $2 \mid a_4^2 + 1$ et $a_5 = 8(2^4+1) \times (2^8+1)(2^{12}+1)$, ce qui achève la démonstration.

Démonstration du théorème 2. Soient a et m des nombres naturels quelconques dont $a > 1$. Il existe par hypothèse un nombre premier de Fermat F_i tel que $F_i \nmid a(a^{2^m} - 1)$. On a $F_i \mid a^{F_i - 1} - 1$ en vertu du théorème d'Euler et comme

$$a^{F_i-1} - 1 = (a^{2^m} - 1)\prod_{j=m}^{2^i-1}(a^{2^j} + 1),$$

on a $F_i \mid a^{2^j} + 1$ pour un $j \geqslant m$.

Si $a^{2^j} + 1 = F_i$, il vient $a = 2^{2^{i-j}}$, ce qui est incompatible avec l'hypothèse. On a donc $a^{2^j} + 1 \neq F_i$ et le nombre $a^{2^j} + 1$ (où $j \geqslant m$) est composé.

Reçu par la Rédaction le 29. 1. 1962

COLLOQUIUM MATHEMATICUM

VOL. X 1963 FASC. 1

REMARK ON RATIONAL TRANSFORMATIONS

BY

W. NARKIEWICZ (WROCŁAW)

In [1] and [2] it was proved that if a field K is finitely generated over the rationals, and X is an infinite subset of K, then every polynomial mapping X onto itself must be linear. It seems to be true that every rational function mapping an infinite subset X of such a field onto itself must be a homography. The purpose of this note is to prove this in the case of the field R of rational numbers.

Let R_∞ be the set obtained by adjoining an ideal element ∞ to R. For every rational function $F(t)$ we put $F(\infty) = \lim_{|t|\to\infty}|F(t)|$ and if z is a pole of $F(t)$, then we put $F(z) = \infty$. We shall prove the following

THEOREM. *If X is an infinite subset of R_∞, and $F(t)$ a rational function, such that $X \subset F(X)$, then $F(t) = (at+b)/(ct+d)$ with suitable rational a, b, c, d.*

A. Schinzel posed the following problem (see [3]):

Let $f(x, y)$ be a polynomial with rational coefficients, and X an infinite set of rational numbers with the property that for every x in X there exists such an y in X that $f(x, y) = 0$. Prove that $f(x, y)$ must have a factor which is linear in y or symmetrical in x, y.

As a corollary of our theorem we obtain a positive solution of that problem in the case of $f(x, y) = P(y) - Q(y)x$.

LEMMA 1. *Suppose that X is a set and T a transformation mapping a subset X_0 of X onto X. Suppose moreover that there exists a function $s(x)$ defined on X with values in the set of natural numbers subject to conditions:*

(i) *For every constant c the equation $s(x) = c$ has only a finite number of solutions.*

(ii) *There exists a constant C such that from $s(x) \geqslant C$ follows $s(Tx) > s(x)$.*

Then the set X is finite.

Proof of the lemma. If $X = X_0$, then the finiteness of X follows from lemma 1 in [1] if we put there $f(x) = s(x)$, $g(x) = 1$ for all x and

$B(M) = 2$ for every M. Suppose now that $X\setminus X_0$ is non-void. Let us associate with every x in $X\setminus X_0$ an infinite sequence $y_1^{(x)}, y_2^{(x)}, \ldots$, and adjoin these sequences to the set X to obtain a set Y. Let us define for every x in $X\setminus X_0$ and $m = 1, 2, \ldots$: $s(y_m^{(x)}) = s(x)+m$; $Tx = y_1^{(x)}$, $Ty_m^{(x)} = y_{m+1}^{(x)}$.

Conditions (i) and (ii) are obviously satisfied by the set Y and the extended transformation T and function $s(x)$; moreover $T(Y) = Y$. Hence, as in the case $X = X_0$, we can apply lemma 1 of [1] to obtain the finiteness of Y, which is clearly a contradiction.

For any polynomial $W(t)$ let us write $W(p, q) = q^r W(p/q)$, where r is the degree of $W(t)$.

LEMMA 2. *If $P(t)$, $Q(t)$, are relatively prime polynomials with integral coefficients, then the greatest common divisor:*

$$\mu(p, q) = \big(P(p, q), Q(p, q)\big)$$

is, for all relatively prime integers p, q, bounded by a constant depending on P and Q only, but not on p, q.

This lemma is well-known, but I was not able to find a source to quote, and so I give a proof for the convenience of the reader.

Proof. There exist an integer A and polynomials $G(t)$, $H(t)$ with integral coefficients such that $P(t)G(t)+Q(t)H(t) = A$. Let m, n, r, s be the degrees of P, Q, G, H, respectively. Then, with $k = \max(m+r, n+s)$, $j = k-m-r$, $j' = k-n-s$, we have

$$Aq^k = q^j P(p, q)G(p, q)+q^{j'}Q(p, q)H(p, q);$$

thus $\mu(p, q)$ divides Aq^k. Let $\nu(p, q) = \big(\mu(p, q), q\big)$. It follows immediately that $\nu(p, q)$ divides the coefficient of t^m in $P(t)$ and so is bounded by a constant independent of p, q.

Let us put $\mu(p, q) = d_1(p, q)\cdot\nu(p, q)$, $q = d_2(p, q)\nu(p, q)$. Then $d_1(p, q)$ divides $A\cdot\nu(p, q)^{k-1}$, whence it is also bounded by a constant independent of p, q. Consequently the same may be said about $\mu(p, q)$.

Proof of the theorem. Let X be an infinite subset of R_∞ and $F(t) = P(t)/Q(t)$ a rational function such that $X \subset F(X)$. ($P(t)$ and $Q(t)$ are relatively prime polynomials with integral coefficients, of degree m, n respectively).

Let us define: $T(x) = F(x)$, $s(\infty) = 1$ and $s(p/q) = |p|+q$ if $(p, q) = 1$ and $q > 0$; then put in lemma 1 the set X for X_0 and $F(X)$ for X. Condition (i) is thus obviously satisfied. Now it is sufficient to prove that if $F(t)$ is not a homography then condition (ii) is also satisfied, for in this case lemma 1 would lead to contradiction with the assumption that X is infinite.

Let $w_1(p, q) = \big(q^{|n-m|}, P(p, q)\big)$, $w_2(p, q) = \big(q^{|n-m|}, Q(p, q)\big)$. It can be easily seen that w_1 and w_2 are bounded by a constant independent of p, q.

Let $F(p/q) = A/B \neq 0$ ($(p, q) = 1, (A, B) = 1$). If $n \geqslant m$, then $A \geqslant q^{n-m}P(p, q)/\mu(p, q)w_2(p, q)$ and $B \geqslant Q(p, q)/\mu(p, q)w_2(p, q)$. Thus in this case

$$s\big(F(p/q)\big) \geqslant \{q^{n-m}|P(p, q)|+|Q(p, q)|\}/\mu(p, q)w_2(p, q).$$

Similarly if $n < m$, then

$$s\big(F(p/q)\big) \geqslant \{|P(p, q)|+|Q(p, q)|q^{m-n}\}/\mu(p, q)w_1(p, q).$$

Lemma 2 leads us to

$$s\big(F(p/q)\big) \geqslant \begin{cases} \dfrac{1}{M_1}\,[|P(p, q)|+|Q(p, q)|\,q^{m-n}] & \text{if} \quad m > n, \\ \dfrac{1}{M_1}\,[|P(p, q)|\,q^{n-m}+|Q(p, q)|] & \text{if} \quad m \leqslant n \end{cases} \tag{1}$$

with some constant $M_1 > 0$.

Let now $m \geqslant n$. Then $s\big(F(p/q)\big) \geqslant q^m\{|P(p/q)|+|Q(p/q)|\}/M_1$.

Suppose that for an infinite sequence p_k/q_k we have $s\big(F(p_k/q_k)\big) \leqslant s(p_k/q_k)$.

We must prove that under this assumption $F(t)$ is a homography. We shall distinguish two cases: (a) for infinitely many k: $|p_k| \leqslant Wq_k$ with some constant W, and (b) the sequence $|p_k/q_k|$ tends to infinity.

In the case (a) we can freely assume that $|p_k| \leqslant Wq_k$ holds for every k, and then $s(p_k/q_k) \leqslant (1+W)q_k$. Consequently

$$q_k^{m-1}\big(|P(p_k/q_k)|+|Q(p_k/q_k)|\big) \leqslant (1+W)M_1. \tag{2}$$

As the polynomials $P(t)$ and $Q(t)$ have no common zeros, there exists a positive constant M_2 such that $|P(t)|+|Q(t)| \geqslant M_2$ holds for every t, and so from (2) we infer $q_k^{m-1} \leqslant (1+W)M_1/M_2$, which is possible for $m = 0, 1$ only (since q_k tends to infinity) and a fortiori for $n = 0, 1$, but this means that $F(t)$ is a homography.

In the case (b) we obtain

$$\frac{q_k^m}{|p_k|}\big(|P(p_k/q_k)|+|Q(p_k/q_k)|\big) \leqslant M_1(1+|q_k/p_k|). \tag{3}$$

At least one of the polynomials $P(t)$, $Q(t)$ is not constant, and as $n \leqslant m$, it is $P(t)$ which is not constant. Consequently for sufficiently great $|p_k/q_k|$ we have $|P(p_k/q_k)| \geqslant M_3 |p_k/q_k|^m$ with a suitable positive M_3. It follows that the left side of (3) is at least

$$M_3 \cdot \frac{q_k^m}{|p_k|} \cdot \frac{|p_k|^m}{q_k^m} = M_3 |p_k|^{m-1},$$

but the right side of (3) is bounded, and so we infer that $m = 0, 1$ and a fortiori $n = 0, 1$, which means that $F(t)$ is a homography. In the case $n > m$ the proof is almost the same, as can be easily seen from the symmetry of (1). We proved thus that if $x \neq \infty$, $F(x) \neq 0$, ∞ and $s(x)$ is sufficiently great, then $s(F(x)) > s(x)$. But in all remaining cases $s(x)$ is bounded by a constant. Consequently if $F(t)$ is not a homography the condition (ii) of lemma 1 is verified, which completes the proof of the theorem.

REFERENCES

[1] W. Narkiewicz, *On polynomial transformations*, Acta Arithmetica 7 (1962), p. 241-249.

[2] — *On polynomial transformations II*, Acta Arithmetica 8 (1962), p. 11-19.

[3] A. Schinzel, *P 417*, this volume, p. 187.

Reçu par la Rédaction le 19. 5. 1962

COLLOQUIUM MATHEMATICUM

VOL. X 1963 FASC. 1

ON THE DERIVATIVE OF CLOSE-TO-CONVEX FUNCTIONS

BY

J. KRZYŻ (LUBLIN)

Let D be a simply connected domain of hyperbolic type, i. e. a domain conformally equivalent to an open circle. Then the following definitions of close-to-convexity of D may be considered.

(B): D is said to be *close-to-convex*, or *accessible from outside along rays* [1], if the complement of D can be represented as a union of closed rays which do not cross each other.

(K): D is said to be *close-to-convex*, if for the function $f(z)$ mapping D conformally onto the unit circle $K = \{z: |z| < 1\}$ a univalent and convex function $\Phi(z)$, $z \epsilon K$, can be chosen so that $\Re\{f'(z)/\Phi'(z)\} > 0$ for any $z \epsilon K$ (see [2]).

As pointed out by Lewandowski [3], both definitions of close-to-convexity are equivalent.

For a domain D bounded by a Jordan curve Γ with a continuously changing tangent another equivalent definition of close-to-convexity was given in [2].

(K_1): D is said to be *close-to-convex*, if the maximal angle of a clockwise rotation of the outward normal along any subarc of Γ described in the positive (counter-clockwise) direction does not surpass π. Therefore we can also consider close-to-convex curves.

In particular, the class (L) of univalent functions $f(z) = z + a_2 z^2 + \ldots$ mapping K onto close-to-convex domains, i. e. the class of close-to-convex functions (introduced independently by Biernacki [1] and Kaplan [2]), may be considered. The class (L) contains functions such as convex, starlike, convex in one direction [5], starlike with respect to symmetric points [6], functions with the derivative of positive real part etc.

In [1], which does not seem to be universally known, Biernacki determined the region of variability of the functionals $\{z/f(z)\}$, $\{zf'(z)/f(z)\}$, for a fixed $z \epsilon K$ and f ranging over (L). In this article we solve an analogous problem for $\log f'(z)$ (Theorem 1), and hence we deduce the precise estimates of $\arg f'(z)$ for $f \epsilon (L)$ (Theorem 2). In spite of the fact that the