ON A CERTAIN GROUP STRUCTURE FOR POLYNOMIALS

T. T. MOH¹

ABSTRACT. A problem of C. C. Yang concerning level sets in complex analysis is generalized and algebraized to a problem about a group structure of polynomials. The group structure is established and several partial solutions of Yang's problem follow at once.

1. Introduction. In [1] C. C. Yang has raised the following interesting problem about level sets in complex analysis.

PROBLEM 1. *Let $p(z)$ and $q(z)$ be two polynomials of the same degree over the complex numbers $\mathbb{C}$ such that*

$$p(z)(p(z) - 1) = 0 \Leftrightarrow q(z)(q(z) - 1) = 0.$$

Prove (or disprove) that either $p \equiv q$ or $p + q \equiv 1$.

Let us complete the square. We have

$$p(z)(p(z) - 1) = \left(p(z) - \frac{1}{2}\right)^2 - \frac{1}{4}.$$

In fact the above problem is to determine if the zero set of a function $F = f^2 - \frac{1}{4}$ completely determines the function f up to $\pm$ sign. We may assume that the function F is monic and replace $\frac{1}{4}$ by any nonzero constant. Hence we have the following problem which is equivalent to Problem 1.

PROBLEM 1*. *Let $F(z) = f^2 - \alpha^2$, $G(z) = g^2 - \beta^2$ be two nonconstant monic polynomials of the same degree with α, β nonzero constants. Furthermore*

$$F(z) = 0 \Leftrightarrow G(z) = 0.$$

Prove (or disprove) that $F(z) \equiv G(z)$.

We may raise the following "global" problem.

PROBLEM 2. *Given a set S . Determine all polynomials $F(z) = f^2 - \alpha^2$ with f monic, α a nonzero constant and $F(z)$ does not vanish outside S .*

An even more general problem follows.

PROBLEM 3. *Given a set S . Determine the algebraic structure of the set of polynomials $F(z) = f^2 - \alpha^2$ with f monic, α a polynomial $(f, \alpha) = 1$, $\deg f - \deg \alpha > a$ constant and $F(z)$ does not vanish outside S .*

We give the following definition.

Received by the editors August 6, 1978 and, in revised form, May 1, 1980.

1980 *Mathematics Subject Classification.* Primary 12D05, 12D10

Key words and phrases. Level set, generator, rank, abelian group, Hurwitz formula.

¹This work was partially supported by the National Science Foundation under grant no. 0029-50-1395, at Purdue University.

DEFINITION. Let k be a field of characteristic $\neq 2$. Let $F = f^2 - \alpha^2$ with $f, \alpha \in k[x]$ and $(f, \alpha) = 1$. Let F_α denote the pair (F, α) . Let $n \geq 1$ and $P_n = \{F_\alpha: F \text{ and } f \text{ monic, } \deg f - \deg \alpha \geq n\}$.

REMARK. In the above definition $F_\alpha \neq F_{-\alpha}$ if $\alpha \neq 0$.

DEFINITION. Let S be a set. Let $P_n(S) = \{F_\alpha \in P_n: F \text{ has no zeros outside } S\}$.

DEFINITION. Let $F_\alpha = f^2 - \alpha^2, G_\beta = g^2 - \beta^2$. Let

$$h = (fg + \alpha\beta, \beta f + \alpha g)$$

be monic, then we shall define $*$ as follows

$$F_\alpha * G_\beta = \left[\frac{1}{h} (fg + \alpha\beta) \right]^2 - \left[\frac{1}{h} (\beta f + \alpha g) \right]^2.$$

Our main theorem is the following.

THEOREM. The group $(P_n, *)$ is the torsion free abelian group. Given any set S , $P_n(S)$ is a subgroup of P_n . Furthermore $P_n(S) = \{e\}$ if $\text{card}(S) < n$ and $P_n(S)$ is of rank $< \text{card}(S) - n$ if $n < \text{card}(S) < \infty$ where $\text{card}(S)$ denotes the cardinal number of the set S .

There are examples to indicate that the above theorem is the best possible. Some cases of Problem 1* can be answered at once by using the above theorem.

We wish to express our thanks to D. Drasin and A. Weitsman for showing us the problem of Yang and to W. Heinzer for helping us prove Lemma 5.

2. Proof of the Theorem. First we study the group structure of $(P_n, *)$.

LEMMA 1. $(P_n, *)$ is associative.

PROOF. Let

$$F_\alpha: F = f^2 - \alpha^2,$$

$$G_\beta: G = g^2 - \beta^2,$$

$$H_\gamma: H = h^2 - \gamma^2.$$

Then

$$\begin{aligned} F \cdot G \cdot H &= (fgh + \beta\gamma f + \alpha\gamma g + \alpha\beta h)^2 - (\alpha gh + \beta fh + \gamma fg + \alpha\beta\gamma)^2 \\ &= p^2 - \delta^2. \end{aligned}$$

Let $(p, \delta) = q$ be monic. Then $F * (G * H): U = u^2 - \epsilon^2$ and $(F * G) * H: U = u^2 - \epsilon^2$, where $u = p/q, \epsilon = \delta/q$.

LEMMA 2. $F_\alpha * F_{-\alpha} = e: 1 = 1^2 - 0^2$.

PROOF. Trivial.

LEMMA 3. $F_\alpha * G_\beta = G_\beta * F_\alpha$.

PROOF. Trivial.

LEMMA 4. Let $F_\alpha: F = f^2 - \alpha^2$ and $\alpha_m = \sum_{i \text{ odd}} C_i m f^{m-i} \alpha^i$. Then

$$\underbrace{F_\alpha * F_\alpha * \dots * F_\alpha}_m = (F^m)_{\alpha_m}.$$

PROOF. The above statement is true for $m = 1$. Let us assume it is true for m . Then we have

$$\begin{aligned} F^m &= \left(\sum_{j \text{ even}} C_j^m f^{m-j} \alpha^j \right)^2 - \left(\sum_{i \text{ odd}} C_i^m f^{m-i} \alpha^i \right)^2 \\ &\quad \times \left(\sum_{j \text{ even}} C_j^m f^{m-j} \alpha^j \right)^f - \left(\sum_{i \text{ odd}} C_i^m f^{m-i} \alpha^i \right) \alpha \\ &= \sum_{j \text{ even}} C_j^{m+1} f^{m+1-j} \alpha^j \left(\sum_{j \text{ even}} C_j^m f^{m-j} \alpha^j \right) \alpha + \left(\sum_{i \text{ odd}} C_i^m f^{m-i} \alpha^i \right) f \\ &= \sum_{i \text{ odd}} C_i^{m+1} f^{m+1-i} \alpha^i. \end{aligned}$$

Moreover we have

$$\sum_{j \text{ even}} C_j^{m+1} f^{m+1-j} \alpha^j \pm \sum_{i \text{ odd}} C_i^{m+1} f^{m+1-i} \alpha^i = (f \pm \alpha)^{m+1}.$$

Hence $(\sum_{j \text{ even}} C_j^{m+1} f^{m+1-j} \alpha^j, \sum_{i \text{ odd}} C_i^{m+1} f^{m+1-i} \alpha^i) = ((f + \alpha)^{m+1}, (f - \alpha)^{m+1}) = 1$.

Thus $(F^m)_{\alpha_m} * F_{\alpha} = (F^{m+1})_{\alpha_{m+1}}$.

Combining Lemmas 1, 2, 3, and 4 we conclude that $(P_n, *)$ is a torsion free abelian group. Clearly $P_n(S)$ is a subgroup of P_n .

LEMMA 5. If $\text{card}(S) < n$ then $P_n(S) = \{e\}$.

PROOF. We may assume k algebraically closed. Then $[k(x): k(\alpha/f)] = m + n = \deg f > \deg \alpha = m$. It follows from the Hurwitz formula that [2]

$$-2 = -2(n + m) + \sum (e(p) - 1)$$

where p runs through all places of $k(x)$ and $e(p)$ is the ramification index of p .

We have $e(p) = n$ if $p = (x = \infty)$ and $\sum (e(p) - 1) = 2(n + m) - d$ for p centered at $\alpha/f = \pm 1$ with d the total number of distinct roots for $f \pm \alpha$. Hence we have $d > n + 1$.

LEMMA 6. Let $F_{\alpha}: F = f^2 - \alpha^2$ and $G_{\beta}: G = g^2 - \beta^2 \in P_n(S)$. Let $b \in S$ and let F and G have zeros of multiplicities m and l , respectively, at b . Suppose $m \leq l$. Then $F_{\alpha} * G_{\beta}$ and $F_{-\alpha} * G_{\beta}$ have zeros of multiplicities $m + l$ and $l - m$ at b in some order.

PROOF. We assume without loss of generality that $(x - b)$ is a factor of $g - \beta$. Then

$$\beta^2 F - \alpha^2 G = (\beta f + \alpha g)(\beta f - \alpha g).$$

Suppose $x - b$ is a factor of $f - \alpha$. Then $x - b$ is a factor of $\beta f - \alpha g$ with multiplicity $\geq \min(m, l)$ with equality if $m \neq l$. Hence

$$(x - b)^{2m} | (F \cdot G, (\beta f - \alpha g)^2) \quad \text{and} \quad (x - b)^{2m+1} | (F \cdot G, (\beta f - \alpha g)^2).$$

Let $F_{-\alpha} * G_{\beta} = H_{\lambda} = h^2 - \lambda^2$. Then H has a zero of multiplicity $m - l$ at b . Since $x - b$ is a factor of $\beta f - \alpha g$, it cannot be a factor of $f + g$. Otherwise $x - b$ would

be a factor of $2\beta f$ and $2\alpha g$. If it is a factor of F (i.e. $m > 0$) then it cannot be a factor of either f or α . Hence it must be a factor of g and β , a contradiction. We conclude that

$$(x - b)|(F \cdot G, (\beta f + \alpha g)).$$

Let $F_\alpha * G_\beta = U_\epsilon$; $U = u^2 - \epsilon^2$. Then U has multiplicity $m + l$ at b .

Suppose $x - b$ is a factor $f + \alpha$. Then replace α by $-\alpha$ in the above argument. Q.E.D.

LEMMA 7. Suppose F_α : $F = f^2 - \alpha^2 \in P_n(S)$ where F has a zero of minimal positive multiplicity m at $b \in S$. Let G_β : $G = g^2 - \beta^2 \in P_n(S)$ with multiplicity l at $b \in S$. Then $l = m \cdot p$ for some integer p . Furthermore either $(F^p)_{\alpha_p} * G$ or $(F^p)_{(-\alpha)_p} * G$ does not vanish at b .

PROOF. Follows from Lemma 6 by Euclidean algorithm.

PROOF OF THE LAST PART OF THEOREM 1. If there is no element in $P_n(S)$ with positive multiplicity at $b \in S$ then $P_n(S) = P_n(S \setminus \{b\})$. The proof is completed by induction on the cardinality of S . Otherwise choose F_α : $F = f^2 - \alpha^2$ with smallest possible positive multiplicity. Then $P_n(S)$ is generated by F_α and $P_n(S \setminus \{b\})$.

3. Discussion.

PROPOSITION 1. Let $F_\alpha \in P_n$. If $F = G^l$ as ordinary power with G monic, then $G_\beta \in P_n$ for some β .

PROOF. Let $F = f^2 - \alpha^2 = (f - \alpha)(f + \alpha) = G^l$. Since $(f - \alpha, f + \alpha) = 1$, then we have

$$f - \alpha = h_1^l, \quad f + \alpha = h_2^l,$$

with $(h_1, h_2) = 1$ and h_1, h_2 are monic. We have

$$2\alpha = \Pi(h_2 - w^l h_1)$$

where w is a primitive l th root of unity. Let

$$\deg h_1 = \deg h_2 = c, \quad \deg(h_2 - h_1) = e.$$

Then we have

$$\begin{aligned} \deg(h_1 + h_2) &= c, & \deg \alpha &= (l - 1)c + e, \\ \deg f &= lc, & n &= lc - [(l - 1)c + e] = c - e, \end{aligned}$$

and

$$G = h_1 h_2 = \left[\frac{1}{2}(h_1 + h_2) \right]^2 - \left[\frac{1}{2}(h_1 - h_2) \right]^2.$$

Choose $\beta = \frac{1}{2}(h_1 - h_2)$.

For Yang's problem the following Propositions 2 and 3 establish partial solutions.

PROPOSITION 2. If $\text{card } S = n + 1$, then $P_n(S)$ is a cyclic group of one generator. Hence the answer to Problem 1 in this case is affirmative.

PROOF. It follows trivially from our theorem.

PROPOSITION 3. If $\text{card } S = 2n - 1$, then there is at most one polynomial F with $\deg F = 2n$, F vanishes and only vanishes at every point of S and $F_\alpha \in P_n(S)$ for some α .

PROOF. Let $G: G = g^2 - \beta^2$ be another one. Then $F_\alpha * G_\beta \neq \{e\} = F_{-\alpha} * G_\beta$, since $(\beta f + \alpha g, \beta f - \alpha g, FG) = 1$ and we have

$$\begin{aligned} FG &= (fg + \alpha\beta)^2 - (\beta f + \alpha g)^2 \\ &= (fg - \alpha\beta)^2 - (\beta f - \alpha g)^2, \\ \beta^2 F - \alpha^2 G &= (\beta f + \alpha g)(\beta f - \alpha g). \end{aligned}$$

Suppose $S = \{b_1, \dots, b_{2n-1}\}$ with $(x - b_1)F = (x - b_2)G$. Then at least one of the two factors $\beta f + \alpha g$ and $\beta f - \alpha g$ must have at least $n - 1$ of the remaining points as roots. Thus either $F_\alpha * G_\beta$ or $F_{-\alpha} * G_\beta$ will have at most n distinct roots which contradicts Lemma 5.

We shall complete our article by listing several examples.

EXAMPLE 1. The rank of $P_1(S) = \text{card}(S) - 1$. Let $S = \{b_1, \dots, b_n\}$. Then $F_{\alpha_i} = (x - b_1)(x - b_i) = [x - \frac{1}{2}(b_1 + b_i)]^2 - [\frac{1}{2}(b_1 - b_i)]^2$ for $i = 2, \dots, n$ clearly generate $P_1(S)$.

EXAMPLE 2. Let

$$S = \{-\frac{1}{2}, 0, 1, \frac{3}{2}\}, \quad F_\alpha: x^2(x - \frac{3}{2})(x - 1)^2(x + \frac{1}{2}) = (x^3 - \frac{3}{2}x^2 + \frac{1}{4})^2 - (\frac{1}{4})^2$$

and

$$G_\beta: x(x - \frac{3}{2})(x - 1)(x + \frac{1}{2}) = (x^3 - x - \frac{3}{8})^2 - (\frac{3}{8})^2.$$

Then F_α and G_β generate $P_2(S)$ with rank $P_2(S) = 2$.

REFERENCES

1. *Complex analysis*, Proceedings of the SUNY Brockport Conference, Dekker, New York and Basel, 1978, p. 169.
2. W. Fulton, *Algebraic curves*, Benjamin, New York, 1969.

DEPARTMENT OF MATHEMATICS, PURDUE UNIVERSITY, WEST LAFAYETTE, INDIANA 47907