Aequationes Math. 14 (1976), 1–32, University of Waterloo Birkhäuser Verlag, Basel

Expository papers

On multiplication and factorization of polynomials, II. Irreducibility discussion

A. M. Ostrowski

Contents

Introduction

In this part we apply the concepts and methods developped in the part I to the problem of irreducibility. In Chapter 10 we derive a pretty general result on absolute irreducibility and discuss in the following chapters in particular the problem of irreducibility in the case of 2, 3 and 4 term polynomials.

While the discussion in the case of 2 and 3 term polynomials could be carried completely out, we give for 4 term polynomials the complete discussion only if the baric polygon is a triangle.

Essential in these discussions are the two lemmas proved in §11 and §12.

§9. General observations on reducibility of polynomials

53. For the whole Part II of this paper we assume that K is of *characteristic* 0.

We will consider in what follows the problem of reducible polynomials $F := \sum_\nu c_\nu P_\nu$. F is called *reducible* if we can write

$$F = GH,$$

AMS (1970) subject classification: Primary 13-02, 13B25. Secondary 06A75.

Received January 21, 1975.

where G and H are proper polynomials. Then G and H are called *proper factors* of F. Although primarily one is interested in this connection in *integer polynomials*, it is more convenient to operate with *rational polynomials*. Indeed, dealing with rational polynomials we can use $m-r$-transformations as defined in Sec. 7, with integer $a_{\mu\nu}$ and $\det(a_{\mu\nu}) = \pm 1$, and in this way often considerably simplify the discussion.

On the other hand it is easy to see that the reducibility problem for rational polynomials is essentially equivalent to a reducibility problem for integer polynomials. In order to see this, we call *primitive* polynomial an integer polynomial, which is not divisible through any of the variables $x_1, \ldots, x_m$. Then it follows immediately that the product of two primitive polynomials is again primitive, while the product of a primitive polynomial with a PP, which is $\neq 1$, is never primitive. Then any rational polynomial F can be written as

$$F = PF^*,$$

where P is a product of powers and F^* is primitive. F^*, the *primitive kernel* of F, is obviously uniquely determined by F. If we now have $F = GH$ for proper polynomials F, G, H, it follows immediately $F^* = G^*H^*$, where the primitive polynomials G^* and H^* are also proper, and we see that the kernel of a reducible rational polynomial is reducible in the domain of integer polynomials.

54. In some cases it can be proved that a given rational polynomial F is irreducible not only in the domain of rational polynomials but even in the domain of all *algebraic polynomials*, that is, cannot be represented as a product GH where G, H are proper algebraic polynomials. On this level of investigation it is reasonable to consider also the irreducibility or reducibility of *algebraic polynomials* F.

If we have the decomposition of the algebraic polynomial F, $F = GH$, where G and H are proper algebraic polynomials, then denoting by D the common denominator of all exponents in F, G, H, we obtain the decomposition of $F(x_1^D, \ldots, x_m^D)$ in two proper rational factors. It is, however, more convenient to operate with algebraic polynomials as such.

In dealing with such problems we can use again the $m-r$-transformations of Sec. 7 with *rational* $a_{\mu\nu}$ and $\det(a_{\mu\nu}) \neq 0$.

55. Consider a sequence of algebraic PP of the type (1): $P_1, \ldots, P_k$.

If there exists an algebraic relation between these PP it can be always written in the form $P_1^{s_1} P_2^{s_2} \ldots P_k^{s_k} = 1$ *with integer* s_κ.

Indeed, an algebraic relation between these P_κ can be written in the form

$$\sum_\nu f_\nu P_1^{\sigma_1(\nu)} \ldots P_k^{\sigma_k(\nu)} = 0$$

with integer $\sigma_\kappa^{(\nu)}$ and not vanishing $f_\nu \in K$.

If this relation is identically satisfied after introducing the expressions of the P_κ in the variables x_μ, then there must exist at least two *different* expressions

$$P_1^{\sigma_1'}\dots P_k^{\sigma_k'}, \qquad P_1^{\sigma_1''}\dots P_k^{\sigma_k''}$$

which become identical when expressed in the x_μ, and therefore can cancel one another. But then we have the relation

$$P_1^{\sigma_1''-\sigma_1'}\dots P_k^{\sigma_k''-\sigma_k'}=1$$

where all $\sigma_\kappa''-\sigma_\kappa'$ are integers and not all of them vanish.

56. LEMMA 4. *The polynomial*

$$z_1^D+z_2^D+\dots+z_k^D \qquad (k\geqslant 3,\ D\geqslant 1) \tag{48}$$

is irreducible in the domain of integer polynomials if $k\geqslant 3$ *and* D *is a natural number.*

Proof. We can assume $D\geqslant 3$. Suppose we have

$$z_1^D+z_2^D+\dots+z_k^D=FG,$$

where the proper factors F and G must be homogeneous polynomials of the dimensions a, b, $a+b=D$, and none of the derivatives F'_{z_κ}, G'_{z_κ} vanishes identically.

Differentiating this with respect to z_k we obtain

$$Dz_k^{D-1}=F'_{z_k}G+G'_{z_k}F.$$

Write

$$F'_{z_k}=z_k^\alpha f, \qquad G'_{z_k}=z_k^\beta g,$$

where f and g are polynomials no longer divisible by z_k. Obviously

$$0\leqslant\alpha\leqslant a-1\leqslant D-2, \qquad 0\leqslant\beta\leqslant b-1\leqslant D-2.$$

57. Without loss of generality, we can assume $\alpha\leqslant\beta$, since otherwise we can interchange F and G. We obtain now

$$Dz_k^{D-1-\alpha}=fG+z_k^{\beta-\alpha}gF. \tag{49}$$

Since $D-1-\alpha>0$ and neither f nor G are divisible by z_k, it follows $\beta=\alpha$. Taking in (49) $z_k=0$ and denoting the corresponding values of f, g, F, G respectively by f_0, g_0, F_0, G_0, it follows

$$f_0G_0=-g_0F_0. \tag{50}$$

58. But now it is easy to see that F_0 and G_0 have no proper factors in common. Indeed, otherwise $F_0G_0=z_1^D+\cdots+z_{k-1}^D$ would be divisible by the square of a proper polynomial and the partial derivatives $Dz_1^{D-1},\ldots, Dz_{k-1}^{D-1}$ have no factor in common. It follows therefore from (50) that f_0 is divisible by F_0 and g_0 by G_0. Since the dimensions of f_0, g_0 are respectively smaller than those of F_0, G_0, this is impossible, and Lemma 4 is proved.

59. From Lemma 4 it follows immediately that

$$z_1^D+z_2^D+\cdots+z_k^D+1 \qquad (k\geqslant 2, D\geqslant 1) \tag{51}$$

is irreducible, since replacing generally z_k with z_k/z_{k+1} and multiplying by z_{k+1}^D we obtain (48) with $k+1$ instead of k. Further it follows by what has been said in Sec. 54, that the polynomials (48) and (51) are irreducible even in the domain of all algebraic polynomials

60. Let now n algebraic PP, $P_1,\ldots, P_n$, $n\geqslant 3$, in $x_1,\ldots, x_m$ be algebraically independent and consider the polynomial

$$\sum_{\nu=1}^{n} c_\nu P_\nu \qquad (c_1c_2\ldots c_n\neq 0). \tag{52}$$

It is easy to see that (52) is irreducible even in the domain of algebraic polynomials. Indeed, obviously $n\leqslant m$. By an $m-r$-transformation we can introduce m new variables y_ν, so that $y_\nu=P_\nu$ $(\nu=1,\ldots, n)$. (52) becomes $\sum_{\nu=1}^{n} c_\nu y_\nu$. Introducing here $c_\nu y_\nu=:z_\nu$ we obtain a polynomial (48) which is irreducible. This can be generalized:

61. THEOREM VII. *If $n+1$ algebraic PP: $P_0, P_1,\ldots, P_n, n\geqslant 2$, are such that $P_1/P_0,\ldots, P_n/P_0$ are algebraically independent, the algebraic polynomial*

$$\sum_{\nu=0}^{n} c_\nu P_\nu \qquad (c_0c_1\ldots c_n\neq 0,\ n\geqslant 2) \tag{53}$$

is irreducible in the domain of all algebraic polynomials.

Proof. Put

$$\frac{c_\nu}{c_0} P_\nu/P_0=:Q_\nu \qquad (\nu=1,\ldots, n)\,; \tag{54}$$

then dividing the polynomial (53) by c_0P_0 we obtain

$$1+Q_1+\cdots+Q_n$$

with algebraically independent

$$Q_1, \ldots, Q_n; \tag{55}$$

but then we can again introduce n new variables $z_\nu := Q_\nu$ $(\nu = 1, \ldots, n)$ and obtain a polynomial of the type (51). Theorem VII is proved.

§ 10. A criterion for absolute irreducibility

62. Consider a general (commutative) field R of characteristic 0 and m variables $x_1, \ldots, x_m$ which are algebraically independent with respect to R. We say then of any polynomial $F(x_1, \ldots, x_m)$ with coefficients from R that it *lies in* R.

Assume now that F from R is a proper irreducible polynomial with respect to R. Then it can happen that there exists an algebraic extension of R, R^*, such that F has a proper factor $\varphi(x_1, \ldots, x_m)$ with coefficients from R^*. In this case we say that F becomes *reducible in* R^*, while if there does not exist any algebraic extension of R in which F becomes reducible, F is called *absolutely irreducible*. For instance $x_1^2 + x_2^2 + x_3^2$ is an absolutely irreducible polynomial, while $x_1^2 - 2x_2^2$ is irreducible in the field of rational numbers, but becomes reducible after adjunction of $\sqrt{2}$.

63. We develop in this chapter a criterion which allows in many cases to prove the absolute irreducibility and uses the concept of S terms of a polynomial explained in Sec. 52.

If the polynomial F is $= GH$, the factor polynomials G, H could be multiplied, G with an arbitrary coefficient $t \neq 0$ and H with $1/t$ and in this way the coefficients of G and H shifted into a field R^* which is possibly too large. However, it is immediately seen that if the coefficients of G are denoted by $\alpha_1, \alpha_2, \ldots$ and those of H by $\beta_1, \beta_2, \ldots$, all products $\alpha_\nu \beta_\mu$ lie in the 'smallest' field over R in which the decomposition $F = GH$ could be obtained using suitable cofactors. In particular already all coefficients of G and H lie in such a 'smallest' field if one of them is $= 1$. We can therefore *norm* the polynomial F taking the coefficient one of its S terms $= 1$ and requiring that both in G and H the corresponding S terms have the coefficients 1.[1]) We will say in this case that F, G, H are *normed.* Observe that if a polynomial, $f(x)$, in one variable x, is normed, all of its coefficients are rational functions of its zeros.

64. In principle the field R^* over R in which F becomes reducible, if such a field exists, need not to be finite or algebraic R. However, it is easy to see that it can

[1]) This was used, in the case that R is a number field, in the paper: A. M. Ostrowski, *Notiz über einen Satz der Galoisschen Theorie*, Math. Z. *12*, 317–322 (1922). This paper will be denoted in the sequel by [*N*].

be always replaced with a finite algebraic extension of R. Indeed, assume the decomposition

$$F(x_1,\dots,x_m)=G(x_1,\dots,x_m)\,H(x_1,\dots,x_m)$$

where G and H lie in R^* and all three polynomials are normed. Using the Kronecker's substitution $x_1=x$, $x_2=x^g$, $x_3=x^{g^2},\dots, x_n=x^{g^{n-1}}$ we obtain the equation

$$F(x, x^g,\dots, x^{g^{n-1}})=G(x, x^g,\dots, x^{g^{n-1}})\,H(x, x^g,\dots, x^{g^{n-1}})$$

where, if the integer g is chosen sufficiently large, no terms in G and in H are mixed up and the sequence of the coefficients remains the same. But then we have on both sides polynomials in one variable x and the roots of these polynomials are the roots of the left hand polynomial which lies in R. Therefore these roots are algebraic with respect to R and since G and H are normed their coefficients are also algebraic with respect to R.

65. THEOREM VIII. *Consider a commutative field R of characteristic* 0, *m variables $x_1,\dots,x_m$, algebraically independent with respect to R, and an integer polynomial $F(x_1,\dots,x_m)$ lying in R and irreducible with respect to R. Assume that F has a proper integer factor $\psi(x_1,\dots,x_m)$ which is absolutely irreducible and will be assumed as normed. Denote by K the field obtained from R by adjunction of all coefficients of ψ and let k be the highest order of an element of K with respect to R.*

Then each S term of F is, up to a factor from R, k-th power of the corresponding S term of ψ.

In particular, if the greatest common divisor of the exponents of all S terms of F is 1, *F is absolutely irreducible.*

66. *Proof.* Let n be the degree of ψ in $x_1,\dots,x_m$ (that is the maximal dimension of all PP occurring in ψ). Let n' be the smallest degree of an absolutely irreducible integer factor of F and let such a (normed) factor be φ_1, where, if $n'=n$, we take $\varphi_1:=\psi$. Let K' be the field obtained from R by adjunction of all coefficients of φ_1 and denote by k' the degree of K' with respect to R.

As the characteristic of R is 0, K' can be written as $R(\varrho_1)$ where ϱ_1 is a primitive element of K', of degree k' with respect to R.

67. Then each coefficient of φ_1 can be written as an integer polynomial in ϱ_1 and we can therefore write

$$\varphi_1=\Phi(\varrho_1, x_1,\dots,x_m)$$

where Φ is an integer polynomial of its $m+1$ variables with coefficients from R.

We consider then the k' conjugate polynomials with respect to R

$$\varphi_\kappa = \Phi(\varrho_\kappa, x_1, \ldots, x_m) \qquad (\kappa = 1, \ldots, k)$$

where $\varrho_2, \ldots, \varrho_k$ are the conjugates of ϱ_1. Each of the polynomials φ_κ is also a factor of F and therefore absolutely irreducible, since otherwise F would have a proper factor of degree $< n'$. Further, all φ_κ are distinct since otherwise the number of different conjugates of φ_1 would be $\leqslant k' - 1$ and φ_1 would lie in an extension of R of degree $< k'$. Since all φ_κ are normed they are essentially different[2]) and F must be divisible by their product

$$\prod_{\kappa=1}^{k'} \varphi_\kappa(x_1, \ldots, x_m).$$

This product lies, however, in R and is also normed, so that we must have, as F is irreducible in R,

$$F = c \prod_{\kappa=1}^{k'} \varphi_\kappa(x_1, \ldots, x_m), \qquad c \in R.$$

But ψ is a factor of F and must therefore be divisible through one of the φ_κ which is only possible, since ψ is absolutely irreducible, if $n' = n$ and therefore $\psi = \varphi_1$. We obtain

$$K' = K, \qquad k' = k.$$

68. Observe now that if $\psi = \varphi_1$ contains a term $c(\varrho_1) x_1^{\alpha_1} \ldots x_m^{\alpha_m}$ where $c(\varrho_1)$ is $\neq 0$ and a polynomial in ϱ_1 with coefficients from R, then each φ_κ contains the term $c(\varrho_\kappa) x_1^{\alpha_1} \ldots x_m^{\alpha_m}$ where $c(\varrho_\kappa)$ is the conjugate of $c(\varrho_1)$ and therefore $\neq 0$. We see that different φ_κ contain exactly the same PP and have therefore identical baric polyhedrons:

$$C_\psi = C_{\varphi_1} = \cdots = C_{\varphi_k}.$$

It follows that if to an S term P^* of F corresponds in ψ the S term $c(\varrho_1) x_1^{\alpha_1} \ldots x_m^{\alpha_m}$, the corresponding term in φ_κ is $c(\varrho_\kappa) x_1^{\alpha_1} \ldots x_m^{\alpha_m}$ and therefore

$$P^* = x_1^{k\alpha_1} \ldots x_m^{k\alpha_m} \prod_{\kappa=1}^{k} c(\varrho_\kappa).$$

Theorem VIII is proved.

[2]) This means that $\varphi_\kappa / \varphi_\lambda$ cannot be independent of $x_1, \ldots, x_m$, if $\kappa \neq \lambda$.

It follows in particular that the degrees of all highest terms of F in any of the possible lexicographic orderings are divisible by k.[3])

§11. An analogue of Eisenstein-Schönemann theorem

69. We consider in the following the set of all integral polynomials in $x_1, \ldots, x_m$ with coefficients from a field K and denote this set by J.

We will consider a weight function $W(F)$ such that $W(x_\nu) > 0$ $(\nu = 1, \ldots, m)$, and the corresponding monobaric ordering.

Observe that the additivity property of $W(F)$ remains conserved for not necessarily isobaric polynomials. Indeed, consider two polynomials from J, decomposed into isobaric aggregates:

$$F = \varphi_0 + \varphi_1 + \cdots + \varphi_k,$$
$$G = \psi_0 + \psi_1 + \cdots + \psi_k.$$

As the *leading aggregate of a product is the product of the leading aggregates of factors*, the leading aggregate of FG is $\varphi_0\psi_0$ and it follows

$$W(FG) = W(\varphi_0\psi_0) = W(\varphi_0) + W(\psi_0) = W(F) + W(G).$$

We are now going to prove a lemma which is to a certain degree an analogon of the Eisenstein-Schönemann theorem in the theory of numbers.

70. LEMMA 5. *Assuming a variable z, independent of J, consider the polynomial*

$$Z := \varphi + \sum_{\pi=1}^{p} \psi_\pi z^{\pi k} + \chi z^n \quad (n > pk \geqslant 2; \chi \wedge \psi_\pi \wedge \varphi \in J, \chi\varphi \neq 0) \tag{56}$$

where φ and χ are non-vanishing polynomials from J. Assume that:

$$W(\varphi) > \operatorname{Max}(W(\chi), W(\psi_1), \ldots, W(\psi_p)), \tag{57}$$

that the polynomial φ has no multiple factors and that $(\varphi, \chi, \psi_1, \ldots, \psi_p) = 1$.

Assume that Z is a product of two polynomials depending on z:

$$Z = FG, \tag{58}$$
$$F = f_0 + f_1 z^{u_1} + \cdots + f_s z^{u_s}, \quad 0 < u_1 < \cdots < u_s, \ s \geqslant 1, \tag{59}$$
$$G = g_0 + g_1 z^{v_1} + \cdots + g_t z^{v_t}, \quad 0 < v_1 < \cdots < v_t, \ t \geqslant 1, \tag{60}$$

where all f_σ, g_τ belong to J and none of them vanishes.

[3]) This result was already given in [N] where it was also indicated that a considerable generalization was possible.

Then

$$(\varphi, \psi_1, \ldots, \psi_p) = 1, \tag{61}$$

all exponents u_σ, v_τ are divisible by k – and the same holds of course for n.

71. *Proof.* Consider the set, J_z, of all integer polynomials in z with coefficients from J. In order to define a weight function in J_z, whose restriction on J is our W, it is sufficient to put $W(z) := \varepsilon$, for a positive ε. ε is now chosen so small, that we have

$$W(\varphi) > W(\chi) + n\varepsilon, \qquad W(\varphi) > W(\psi_\pi) + n\varepsilon \quad (\pi = 1, \ldots, p). \tag{62}$$

This is certainly possible in virtue of (57).

Then it follows that in Z the weight of φ dominates the weights of other terms and we have therefore

$$W(Z) = W(\varphi), \qquad W(Z - \varphi) < W(\varphi). \tag{63}$$

72. From (58)–(60) it follows that

$$f_0 g_0 = \varphi, \qquad W(f_0) + W(g_0) = W(\varphi), \qquad (f_0, g_0) = 1, \tag{64}$$

since $\varphi = f_0 g_0$ has no multiple factors.

Denote by $\bar{\varphi}$ the leading aggregate of φ and by $\bar{f}_0$, $\bar{g}_0$ the leading aggregates of f_0 and g_0. Obviously $\bar{\varphi} = \bar{f}_0 \bar{g}_0$. But $\bar{\varphi}$ is in (56) also the leading aggregate of Z. It follows therefore from (58) that $\bar{f}_0$ and $\bar{g}_0$ are respectively the leading aggregates of F, G. Thence

$$W(F) = W(f_0) > W(F - f_0), \qquad W(G) = W(g_0) > W(G - g_0). \tag{65}$$

We see in particular that

$$W(f_\sigma) < W(f_0) \quad (\sigma = 1, \ldots, s), \qquad W(g_\tau) < W(g_0) \quad (\tau = 1, \ldots, t). \tag{66}$$

73. We first are going to prove (61).

Indeed, otherwise there would exist an irreducible proper polynomial ω from J as a common divisor of φ and the ψ_π. We would then have, leaving out all terms divisible by ω, modulo ω,

$$FG \equiv \chi z^n = f_s g_t z^n,$$
$$F \equiv F_1 := H_0 z^{U_0} + \cdots + H_{s_1} z^{U_{s_1}},$$
$$G \equiv G_1 := K_0 z^{V_0} + \cdots + K_{t_1} z^{V_{t_1}}.$$

If now one of the expressions F_1, G_1 consisted of more than one term, we would have

$$\chi z^n \equiv H_0 K_0 z^{U_0+V_0} + \cdots + H_{s_1} K_{t_1} z^{U_{s_1}+V_{t_1}} \quad (\operatorname{mod} \omega) \tag{67}$$

where $U_{s_1}+V_{t_1} > U_0+V_0$ and neither H_0K_0 nor $H_{s_1}K_{t_1}$ are divisible by ω. But then the last congruence is plainly impossible. It follows that, modulo ω, $F \equiv f_s z^{U_s}$, $G \equiv g_t z^{V_t}$, and therefore $f_0 \equiv g_0 \equiv 0$, so that $\varphi = f_0 g_0 = 0$ would have the factor ω^2. (67) is proved.

75. In the following part of the proof the notation $o(z^N)$ means an integer polynomial divisible by z^{N+1}.

Assume now that the assertion of Lemma 5 is false. We can then assume that not all u_σ are divisible by k. Let u_{σ_0} be the first u_σ in (59), not divisible by k, and put, dividing u_{σ_0} by k:

$$u_{\sigma_0} = lk+\alpha, \quad 0<\alpha<k, \, l \text{ integer, } \geqslant 0. \tag{68}$$

Then F can be rewritten, ordered in ascending powers of z, as

$$F = \sum_{\lambda=0}^{l} \gamma_\lambda z^{\lambda k} + \gamma z^{lk+\alpha} + o(z^{lk+\alpha}), \quad \gamma := f_{\sigma_0} \neq 0, \tag{69}$$

where not all γ_λ need be $\neq 0$.

If now G could be written as $G = \sum_{\lambda=0}^{l} \delta_\lambda z^{\lambda k} + o(z^{lk+\alpha})$, then we would have in the product $Z = FG$ the term

$$\gamma g_0 z^{lk+\alpha},$$

which cannot be cancelled and is different from χz^n, as $u_s < n$.

76. Therefore we can write, ordering G in ascending powers of z:

$$G = \sum_{\varrho=0}^{r} \delta_\varrho z^{\varrho k} + \delta z^{rk+\beta} + \cdots, \quad \delta = g_{\tau_0} \neq 0, \tag{70}$$

$$v_{\tau_0} = rk+\beta, \quad 0<\beta<k, \, r \text{ integer, } \geqslant 0, \, rk+\beta \leqslant lk+\alpha. \tag{71}$$

But if we had here $rk+\beta < lk+\alpha$, we could interchange F and G. We have therefore only to consider the case

$$lk+\alpha = rk+\beta, \quad l=r, \, \alpha=\beta.$$

Then FG would contain the term

$$(f_0\delta + g_0\gamma)\, z^{lk+\alpha},$$

the exponent of which is $\not\equiv 0 (\operatorname{mod} k)$ and $<n$. We must have therefore

$$f_0\delta + g_0\gamma = 0, \quad f_0 g_{\tau_0} = -g_0 f_{\sigma_0}. \tag{72}$$

Since however, by (67), f_0 and g_0 have no non-trivial common divisors in J, we see that

$$\frac{g_{\tau_0}}{g_0}, \frac{f_{\sigma_0}}{f_0}$$

must be polynomials from J. But then it would follow

$$W(f_0) \leqslant W(f_{\sigma_0}), \quad W(g_0) \leqslant W(g_{\tau_0})$$

in contradiction to (66). Lemma 5 is proved.

§ 12. An application of Puiseux developments

77. LEMMA 6. *Assume natural n and m and put*

$$r := n\left[\frac{m+1}{2}\right] - 1, \text{[4]} \tag{73}$$

$$Z^* := x^m + y^{nm} + f(x, y), \tag{74}$$

where $f(x, y)$ is an integer polynomial with numerical coefficients, with $f(0, 0) \neq 0$ and such that for every PP, $x^\lambda y^\kappa$, actually occurring in f, we have

$$\lambda n + \kappa \leqslant r. \tag{75}$$

Then Z^* is absolutely irreducible in the domain of integer polynomials.

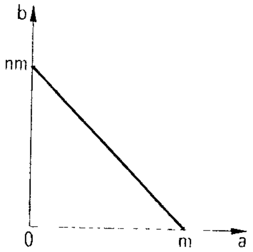
78. *Proof.* By (73) we obtain

$$r \leqslant \frac{n(m+1)}{2} - 1 = nm\left(\frac{1}{2} + \frac{1}{2m} - \frac{1}{nm}\right) \leqslant nm\left(1 - \frac{1}{nm}\right) < nm,$$

and therefore, by (75), the degree of f in x is $<m$. But then Z^* cannot have a proper factor independent of x, since x^m in Z^* has the coefficient 1. Therefore Z^* is certainly irreducible for $m = 1$, and we can from now on assume $m \geqslant 2$.

[4] The symbol $[a]$ denotes generally the greatest rational integer $\leqslant a$.

Under our assumption the baric diagram of Z^* is:



Assume now that Z^* is reducible,

$$Z^*=FG, \tag{76}$$

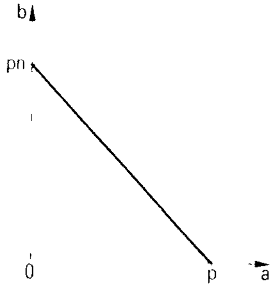
where F and G are integer polynomials of *positive degrees* with respect to x. We can assume that p, the degree of F in x, is $\leqslant m/2$. Observe that in any case

$$\left[\frac{m}{2}\right]+\left[\frac{m+1}{2}\right]=m,$$

as is immediately verified for odd and even m.

Since the baric triangle of Z^* is the sum of the baric polygons of F and G, these two polygons must be triangles, similar to the baric triangle of Z^*, as follows from Sec. 46.

But then the baric triangle of F is:



so that the degree of F with respect to y is pn.

79. If we now write F out as sum of monomials,

$$F=\sum_{\lambda,\kappa} a_{\lambda\kappa}x^{\lambda}y^{\kappa},$$

we must have

$$\frac{\lambda}{p}+\frac{\kappa}{pn}\leqslant 1, \qquad \kappa\leqslant n(p-\lambda). \tag{77}$$

Ordering F in powers of x,

$$F=\sum_{\lambda=0}^{p} x^{\lambda} f_{p-\lambda}(y), \tag{78}$$

it follows that the degree of $f_{p-\lambda}(y)$ is $\leqslant n(p-\lambda)$.

The function $x(y)$, defined by $Z^*=0$, has m Puiseux developments in decreasing powers of y in the neighbourhood of $y=\infty$. Since the Newton diagram of Z^* is the hypotenuse of its baric triangle, the first terms of these Puiseux developments are obtained from

$$x^m+y^{nm}=0,\ x=\varepsilon y^n,\ \varepsilon^m=-1.$$

But then we have, with $y\to\infty$, $|x|\sim|y|^n$, and for $\lambda=0, 1, \ldots, p$:

$$f_{p-\lambda}(y)=0(y^{n(p-\lambda)}) \qquad (y\to\infty), \tag{79}$$

and further in virtue of (75)

$$f(x,y)=0(y^r) \qquad (y\to\infty). \tag{80}$$

80. We obtain now from $Z^*=0$, in virtue of (80),

$$x^m=-y^{nm}\left(1+\frac{f(x,y)}{y^{nm}}\right)=-y^{nm}\left(1+0\left(\frac{1}{y^{nm-r}}\right)\right),$$

$$x=\varepsilon y^n\left(1+0\left(\frac{1}{y^{nm-r}}\right)\right), \qquad \varepsilon^m=-1. \tag{81}$$

From (81) it follows further

$$x^{\lambda}=\varepsilon^{\lambda}y^{\lambda n}\left(1+0\left(\frac{1}{y^{nm-r}}\right)\right)=\varepsilon^{\lambda}y^{\lambda n}+0\left(\frac{1}{y^{nm-r-\lambda n}}\right) \qquad (1\leqslant\lambda\leqslant p),$$

and multiplying by $f_{p-\lambda}(y)$, in virtue of (79),

$$x^{\lambda}f_{p-\lambda}(y)=(\varepsilon y^n)^{\lambda} f_{p-\lambda}(y)+0\left(\frac{1}{y^{nm-np-r}}\right) \qquad (0\leqslant\lambda\leqslant p),$$

where the relation corresponding to $\lambda=0$ is trivial.

Observe now that

$$n(m-p)-r \geqslant n\left(m-\left[\frac{m}{2}\right]-\left[\frac{m+1}{2}\right]\right)+1=1 .$$

Therefore it follows

$$x^{\lambda} f_{p-\lambda}(y)=(\varepsilon y^{n})^{\lambda} f_{p-\lambda}(y)+0\left(\frac{1}{y}\right) \quad (\lambda=0, 1, \ldots, p). \tag{82}$$

81. Formula (82) holds for every of the m branches of $x(y)$, assigning to ε the corresponding one of its m values. Therefore p of these branches satisfy the equation

$$F(x(y), y)=0, \tag{83}$$

and we take now in (82) one of the values of ε for which (83) is satisfied.

But then we obtain, summing (82) for $\lambda=0, 1, \ldots, p$,

$$F(x(y), y)=\sum_{\lambda=0}^{p}(\varepsilon y^{n})^{\lambda} f_{p-\lambda}(y)+0\left(\frac{1}{y}\right).$$

Here the first right-hand sum is a polynomial in y, while the 0 term goes to 0 with $y \rightarrow \infty$, and it follows

$$\sum_{\lambda=0}^{p}(\varepsilon y^{n})^{\lambda} f_{p-\lambda}(y) \equiv F(\varepsilon y^{n}, y)=0 .$$

But this is a polynomial identity, and it would follow for $y=0$, in virtue of (76): $Z^{*}(0, 0)=0$, contrary to the hypothesis. Lemma 6 is proved.

82. It is now easy to show that the absolute irreducibility of Z^{*} in Lemma 6 holds under the hypothesis of this lemma also in the *domain of algebraic polynomials*, if, in the case of odd $m>1$, we replace r with $r^{*}:=nm/2-1$.

Indeed, assume that in the decomposition (76) of Z^{*} both F and G are algebraic polynomials; then we can write for a suitable *even* w:

$$Z^{*}=F(x^{1/w}, y^{1/w})\, G(x^{1/w}, y^{1/w}),$$

$F(u, v)$, $G(u, v)$ can be assumed to be integer polynomials. Replacing here $x^{1/w}$ by ξ and $y^{1/w}$ by n we obtain

$$\xi^{wm}+\eta^{wnm}+f(\xi^{w}, \eta^{w})=F(\xi, \eta)\, G(\xi, \eta). \tag{84}$$

But if we replace m in Lemma 6 by wm, the corresponding r becomes

$$\varrho := \frac{wnm}{2} - 1 .$$

If $nm = 1$, $n = m = 1$, $r = 0$, f is a constant so that the conditions of Lemma 6 are satisfied. If $nm > 1$ we have for every PP, $x^\lambda y^\kappa$, in f, in virtue of our new assumption,

$$\lambda n + \kappa \leqslant r^* := \frac{nm}{2} - 1 .$$

But then the corresponding PP in $f(\xi^w, \eta^w)$ is $\xi^{w\lambda}\eta^{w\kappa}$, and we have then

$$w\lambda n + w\kappa \leqslant wr^* .$$

It is now sufficient to prove $wr^* \leqslant \varrho$. And this follows from

$$wr^* = \frac{wnm}{2} - w < \frac{wnm}{2} - 1 .$$

We see that the decomposition (84) is impossible.

83. We will finally show that the assertion of Lemma 6 remains valid in the domain of all algebraic polynomials, if Z^* is an *algebraic polynomial* of the form

$$Z^* := x^\alpha + y^{n\alpha} + \varphi(x^{1/w}, y^{1/w}), \tag{85}$$

where α is a positive rational number, n and w are natural numbers and φ is an integer polynomial in $x^{1/w}$ and $y^{1/w}$, satisfying the condition that for every PP, $x^\lambda y^\kappa$, actually occurring in φ, we have

$$\lambda n + \kappa \leqslant r^* := \frac{n\alpha}{2} - 1 . \tag{86}$$

84. As to the integer w it can be chosen in such a way that $w\alpha$ becomes an even integer and that the decomposition of Z^* becomes

$$Z^* = F(x^{1/w}, y^{1/w})\, G(x^{1/w}, y^{1/w}), \tag{87}$$

where F and G are rational polynomials in $x^{1/w}$ and $y^{1/w}$.

Replacing in (87) $x^{1/w}$ with ξ and $y^{1/w}$ with η we obtain the relation

$$\xi^{w\alpha}+\eta^{nw\alpha}+\varphi(\xi,\eta)=F(\xi,\eta)\,G(\xi,\eta). \tag{88}$$

But then for every PP in $\varphi(x^{1/w}, y^{1/w})$, $x^\lambda y^\kappa$, we have (86) and therefore for every PP in $\varphi(\xi,\eta)$, $\xi^{w\lambda}\eta^{w\kappa}$,

$$w\lambda n+w\kappa\leqslant wr^*=\frac{nw\alpha}{2}-w<\frac{nw\alpha}{2}-1=\varrho,$$

so that the decomposition (88) is impossible in virtue of Lemma 6.

§13. Irreducibility of polynomials with 2 or 3 terms

85. We consider first rational polynomials with *two distint terms*

$$ax_1^{u_1}\ldots x_m^{u_m}+bx_1^{v_1}\ldots x_m^{v_m},\ ab\neq 0, \tag{89}$$

and are going to prove

THEOREM IX. *The polynomial* (89) *is absolutely irreducible if and only if all differences* $u_\mu-v_\mu$ *have the greatest common divisor* 1:

$$(u_1-v_1,\ldots,u_m-v_m)=1. \tag{90}$$

86. *Proof.* Dividing by the first term of (89), we can replace (89) with

$$Z:=1+cx_1^{\alpha_1}\ldots x_m^{\alpha_m}, \tag{91}$$

while the condition (90) is now replaced by

$$(\alpha_1,\ldots,\alpha_m)=1. \tag{92}$$

It is immediately clear that if (92) does not hold, (91) is reducible – replacing the field K by a convenient finite algebraic extension of K.

Indeed, if there exists an integer $d>1$ such that

$$\alpha_\mu=d\beta_\mu\qquad(\mu=1,\ldots,m)$$

with integers β_μ, we can put $P:=x_1^{\beta_1}\ldots x_m^{\beta_m}$ and Z becomes

$$Z=1+cP^d, \qquad d>1\,;$$

but this is obviously reducible adjoining to K the element $c^{1/d}$ and the d-th roots of -1.

87. Assume now (92). It is well known that then it is possible to find $m(m-1)$ rational integers $\alpha_{\mu\nu}$ ($\mu=2,\ldots,m$; $\nu=1,\ldots,m$) so that the determinant

$$\begin{vmatrix} \alpha_1,\ldots,\alpha_m \\ \alpha_{21},\ldots,\alpha_{2m} \\ \vdots \\ \alpha_{m1},\ldots,\alpha_{mm} \end{vmatrix}$$

is 1. Putting now $y_1:=x_1^{\alpha_1}\ldots x_m^{\alpha_m}$,

$$y_\mu:=x_1^{\alpha_{\mu 1}}\ldots\, x_m^{\alpha_{\mu m}} \qquad (\mu=2\ldots m)$$

we have an $m-r$-transformation and Z becomes

$$1+cy_1,$$

which is obviously absolutely irreducible. Theorem IX is proved.

88. We consider now a polynomial with *three (distinct) terms*

$$aP_1+bP_2+cP_3, \qquad abc\neq 0. \tag{93}$$

We are going to prove

THEOREM X. *The polynomial* (93) *is absolutely irreducible, even in the domain of* ***algebraic*** *polynomials, if P_2/P_1, P_3/P_1 are independent.*

If P_2/P_1, P_3/P_1 are not independent, then, if P_1, P_2, P_3 are algebraic PP, (93) *is reducible in the domain of algebraic polynomials. If P_1, P_2, P_3 are rational PP and P_2/P_1, P_3/P_1 are not independent, the polynomial* (93) *is reducible in the domain of rational polynomials.*

89. *Proof.* The first part of the above theorem follows immediately from Theorem VII in Sec. 61 for $n=2$.

We now are going to prove the remaining part of the theorem. We divide (93) through aP_1 and assume therefore our polynomial in the form

$$1+aP_1+bP_2, \qquad ab\neq 0, \tag{94}$$

where P_1, P_2 are not independent. Putting

$$P_1 := x_1^{\alpha_1}\ldots x_m^{\alpha_m},\ P_2 := x_1^{\beta_1}\ldots x_m^{\beta_m},$$

we have for two convenient integers u, v: $v\alpha_\mu = u\beta_\mu$,

$$\gamma_\mu := \frac{\alpha_\mu}{u} = \frac{\beta_\mu}{v} \qquad (\mu=1,\ldots,m;\ u>0,\ v\lesseqgtr 0). \tag{95}$$

90. Assume first that P_1, P_2 are algebraic *PP*, not all rational, so that not all of the α_μ, β_μ are integers. Put $Q := x_1^{\gamma_1}\ldots x_m^{\gamma_m}$.

Then obviously

$$P_1 = Q^u,\ P_2 = Q^v,\ Z = 1+aQ^u+bQ^v. \tag{96}$$

Since here the exponents u, v are distinct and $\neq 0$, Z has at least two proper factors, linear in Q, over an algebraic extension of K.

If P_1, P_2 are rational *PP*, that is if all α_μ, β_μ are integers, we can choose in (95):

$$u=(\alpha_1,\ldots,\alpha_n), \qquad v=\pm(\beta_1,\ldots,\beta_m).$$

But then the γ_μ are integers, Q_μ is a rational *PP* and the factors of Z in (96), linear in Q, are rational polynomials. Theorem X is proved.

§14. Polynomials with 4 terms. General discussion

91. If we consider now the general algebraic polynomial with *four* distinct *PP*,

$$Z := aP_1+bP_2+\gamma P_3+dP_4, \qquad ab\gamma d\neq 0, \tag{97}$$

we have to distinguish three cases according as among the quotients

$$P_1/P_4,\ P_2/P_4,\ P_3/P_4, \tag{98}$$

there are 3, 2 or 1 independents.

If all quotients (98) are independent, it follows from Theorem VII that Z is *always absolutely irreducible* in the domain of algebraic polynomials.

92. On the other hand, if there is among (98) only one independent, it is easy to

show that Z is *always reducible* in the domain of algebraic polynomials, and even, if all quotients (98) are rational PP, in the domain of rational polynomials. Indeed, dividing by aP_1 and changing the notations we can write in this case

$$Z := 1 + aP_1 + bP_2 + \gamma P_3, \qquad ab\gamma \neq 0,$$
$$P_1 = x_1^{\alpha_1} \dots x_m^{\alpha_m}, \qquad P_2 = x_1^{\beta_1} \dots x_m^{\beta_m}, \qquad P_3 = x_1^{\gamma_1} \dots x_m^{\gamma_m},$$

where for convenient integers u, v, w we have

$$\frac{\alpha_\mu}{u} = \frac{\beta_\mu}{v} = \frac{\gamma_\mu}{w} \qquad (\mu = 1, \dots, m). \tag{99}$$

93. Then, denoting for each μ by δ_μ the common value of the quotients (99) and putting $Q := x_1^{\delta_1} \dots x_m^{\delta_m}$, we obtain $P_1 = Q^u$, $P_2 = Q^v$, $P_3 = Q^w$,

$$Z = 1 + aQ^u + bQ^v + \gamma Q^w.$$

But here u, v, w are distinct integers, none of which vanishes, so that, writing $Z = 0$, we obtain an algebraic equation of a degree $\geqslant 3$, and Z has at least three factors, linear in Q.

If in particular P_1, P_2, P_3 are rational PP, that is if all α_μ, β_μ, γ_μ are integers, we can choose

$$u = (\alpha_1, \dots, \alpha_m), \qquad v = \pm(\beta_1, \dots, \beta_m), \qquad w = \pm(\gamma_1, \dots, \gamma_m),$$

so that Q becomes a rational PP and Z is reducible in the domain of rational polynomials.

94. We consider from now on the case, where among the quotients (98) there are *exactly two independent* ones.

This condition can be expressed in a simpler way, introducing the representative points of the P_ν in the corresponding m-dimensional space, E. If

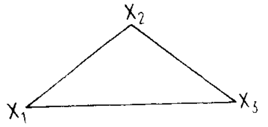
$$P_1 = x_1^{\alpha_1} \dots x_m^{\alpha_m}, \qquad P_2 = x_1^{\beta_1} \dots x_m^{\beta_m},$$
$$P_3 = x_1^{\gamma_1} \dots x_m^{\gamma_m}, \qquad P_4 = x_1^{\delta_1} \dots x_m^{\delta_m},$$

the corresponding representative points in E are

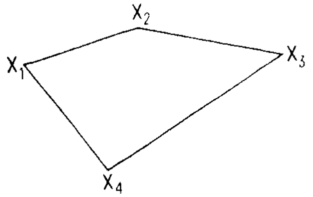
$$X_1 = (\alpha_1, \dots, \alpha_m), \qquad X_2 = (\beta_1, \dots, \beta_m),$$
$$X_3 = (\gamma_1, \dots, \gamma_m), \qquad X_4 = (\delta_1, \dots, \delta_m),$$

and our condition signifies that $X_1, \ldots, X_4$ lie in a plane, without being collinear.

The corresponding baric diagram is then either a triangle:



or a quadrangle:



In the first case we choose the notation so that X_1, X_2, X_3 are the three summits of the triangle, while, if the point X_4 lies on one of the sides, then the opposite summit is X_1.

95. In both cases the points X_1, X_2, X_3 are not collinear.

Dividing Z by aP_1 we bring the point X_1 into the origin, while the corresponding term in Z becomes 1. Then we can assume that P_1, P_2 are independent, and we can then by an $m-r$-transformation of Sec. 7 introduce as new variables:

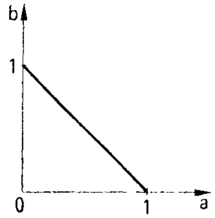
$$y_1 := P_2, y_2 := P_3.$$

Then we have

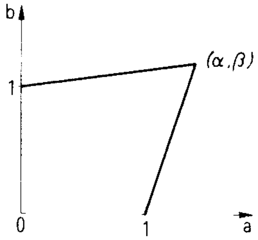
$$P_4 = y_1^\alpha y_2^\beta,$$

with rational α, β.

96. But now it is easy to see that both α and β are *positive*. Indeed, if the baric polygon of Z is a triangle, this triangle becomes now, in the $a-b$-plane:



while the point (α, β) lies either inside of this triangle or inside the hypotenuse. In the case of the quadrangle, since the inside of a convex quadrangle goes by an affine transformation always into the inside of the corresponding quadrangle, the situation is as in the diagram:



We see that in this case, too, α and β are *positive*.

Further we can take the coefficients of y_1 and y_2 into the variables, so that the only coefficient not necessarily $=1$ is that of P_4.

Let now n be the common denominator of α and β, $\alpha = p/n$, $\beta = q/n$. Then putting

$$y_1 := x^n, \qquad y_2 := y^n,$$

we obtain finally Z in the form

$$Z = 1 + x^n + y^n + cx^p y^q \quad (c \neq 0, p \wedge q > 0, \text{ integers}). \tag{100}$$

97. If the baric polygon of Z in (100) is a triangle, we must have

$$p + q \leqslant n, p < n, q < n.$$

If Z is not irreducible, it follows from the Lemma 5 that n/p and n/q are both integers, $\geqslant 2$, and that the factors of Z are polynomials in x^p and y^q. Introducing x^p and y^q as new variables and changing correspondingly the notations, we have to consider the reducible polynomials of the shape

$$Z = 1 + x^m + y^n + cxy, \qquad m \wedge n \geqslant 2,\ c \neq 0. \tag{101}$$

§ 15. Four term polynomials with a baric triangle

98. From here on we assume that c is a real or complex number. Without loss of generality we can assume in (101) $m \geqslant n$. Assume that (101) is not irreducible; then we have

$$x^m + y^n + cxy + 1 = F(x, y)\, G(x, y), \tag{102}$$

$$x^m + y^{nm} + cxy^m + 1 = F(x, y^m)\, G(x, y^m). \tag{103}$$

We assume first that $n \geqslant 4$, $m \geqslant 5$. Then we have for r in Lemma 6

$$r = n\left[\frac{m+1}{2}\right] - 1,$$

and (103) is impossible, if the condition corresponding to (75) is satisfied, that is, for $f = cxy^m$, $\lambda = 1$, $\kappa = m$:

$$n + m \leqslant n\left[\frac{m+1}{2}\right] - 1. \tag{104}$$

If we first assume m even, $m = 2k$, $k \geqslant 3$, the condition (104) becomes

$$n + 2k \leqslant nk - 1, \qquad n(k-1) \geqslant 2k + 1,$$

and since $n \geqslant 4$ it is sufficient to prove that

$$4(k-1) \geqslant 2k + 1, \qquad 2k \geqslant 5,$$

and this is satisfied since $k \geqslant 3$.

If on the other hand m is odd, $m = 2k + 1$, $k \geqslant 2$, (104) becomes

$$n + 2k + 2 \leqslant n(k+1), \qquad kn \geqslant 2k + 2,$$

and this relation is satisfied since $n \geqslant 4$, $k \geqslant 2$.

99. We have now to consider the cases:

(A) $m \geqslant 5$, $2 \leqslant n \leqslant 3$,

(B) $m = 4$, $2 \leqslant n \leqslant 4$,

(C) $m = 3$, $2 \leqslant n \leqslant 3$,

(D) $m = 2$, $n = 2$.

In the case (A), Z must have a factor linear in y, so that there exists a polynomial $\varphi(x)$ for which, replacing y with $\varphi(x)$ in Z,

$$\varphi^n + x^m + cx\varphi + 1 = 0, \qquad \varphi^n = -x^m - cx\varphi - 1 \qquad (m \geqslant 5,\ 2 \leqslant n \leqslant 3). \tag{105}$$

It follows then that the highest term of φ is εx^p, where $\varepsilon^n = -1$, $p = m/n$. If we denote the next term in φ with αx^q, the first two terms of φ^n are

$$\varphi^n = \varepsilon^n x^{np} + n\varepsilon^{n-1}\alpha x^{(n-1)p+q}.$$

Since $cx\varphi$ begins with $-c\varepsilon x^{p+1}$, we obtain

$$(n-1)p+q=p+1, \qquad (n-2)p+q=1.$$

But this is only possible if $n=2$, $q=1$, $m=2p$.

100. We write now φ as

$$\varphi=\varepsilon x^p+\alpha x+\beta;$$

substituting it in (105), we obtain

$$\varphi^2=-x^{2p}-cx\varphi-1,$$

while, on the other hand

$$\varphi^2=\varepsilon^2x^{2p}+2\varepsilon\alpha x^{p+1}+2\beta\varepsilon x^p+\alpha^2x^2+2\alpha\beta x+\beta^2. \tag{106}$$

But since $m=2p>5$, it follows $p\geqslant 3$, so that all exponents on the right side of (106) are *distinct*. The expression on the right of (105) is

$$-x^{2p}-c\varepsilon x^{p+1}-c\alpha x^2-c\beta x-1. \tag{107}$$

Then, since $\beta^2=-1$, $\beta\neq 0$, φ^2 contains the term $2\beta\varepsilon x^p$, while (107) does not contain such a term. We see that Z in the case (A) is irreducible.

101. We consider now the case (B) and assume first that Z has no linear factors in y. Then we must have $m=n=4$, Z becomes

$$Z:=x^4+y^4+cxy+1 \tag{108}$$

and its decomposition into a product of two quadratic factors can be written as

$$Z=(h+h_1+c_1)(k+k_1+c_2), \tag{109}$$

where h, k are homogeneous quadratic and h_1, k_1 are homogeneous linear polynomials in x, y, whiley c_1, c_2 are constants.

Then it follows at once

$$c_1c_2=1, \qquad c_2=\frac{1}{c_1}.$$

Further we have

$$hk = x^4 + y^4.$$

Since x^4+y^4 has no multiple factors, h and k have no factors in common. On the other hand the cubic terms on the right in (109) are, since Z does not have any cubic terms,

$$k_1 h + h_1 k \equiv 0, \tag{110}$$

and here k_1 must be divisible by k and h_1 by h. We see that $h_1 = k_1 = 0$. The decomposition (109) becomes

$$Z = (h + c_1)\left(k + \frac{1}{c_1}\right). \tag{111}$$

102. Now, since in any decomposition (111) a fixed linear factor of x^4+y^4 is combined with one of the 3 other factors, we obtain essentially 3 possible decompositions of x^4+y^4:

(a) $h = x^2 + iy^2, \qquad k = x^2 - iy^2,$

(b) $h = x^2 + \sqrt{2}xy + y^2, \qquad k = x^2 - \sqrt{2}xy + y^2,$

(c) $h = x^2 + i\sqrt{2}xy - y^2, \qquad k = x^2 - i\sqrt{2}xy - y^2,$

as is immediately verified by multiplication.

We have now to choose c, c_1 and h, k in such a way that (111) holds, and this amounts to

$$\frac{1}{c_1} h + c_1 k = cxy. \tag{112}$$

Comparing here on both sides the coefficients of x^2, we obtain in all three cases the condition $(1/c_1) + c_1 = 0$, $c_1^2 = -1$, $c_1 = \pm i$. Comparing on both sides of (112) the coefficients of y^2, we obtain in the case (a) $c_1 - (1/c_1) = 0$, so that the case (a) is impossible. On the other hand we obtain in the cases (b) and (c) again $c_1 + (1/c_1) = 0$.

Compare finally in (112) the coefficients at xy. In the case (b) we obtain

$$c = -2\sqrt{2}\,c_1 \tag{113}$$

and in the case (c)

$$c = -2\sqrt{2}\,ic_1. \tag{114}$$

Introducing these values into (111) we have, taking $c_1 = i$, the decompositions

$$x^4 + y^4 - 2\sqrt{2}\,ixy + 1 = (x^2 + \sqrt{2}\,xy + y^2 + i)(x^2 - \sqrt{2}\,xy + y^2 - i),$$
$$x^4 + y^4 + 2\sqrt{2}\,xy + 1 = (x^2 + i\sqrt{2}\,xy - y^2 + i)(x^2 - i\sqrt{2}\,xy - y^2 - i),$$
$$x^4 + y^4 - 2\sqrt{2}xy - 1 = (x^2 + i\sqrt{2}xy - y^2 - i)(x^2 - i\sqrt{2}xy - y^2 + i).$$

Replacing here i with with $-i$, the second and third formulas are not changed, while the first formula goes into the complexe conjugate one. All together we obtain four values for c in (108):

$$c=\pm 2\sqrt{2},\ \pm 2\sqrt{2}\,i.$$

103. We have now to consider the possibility that, in the case (B), Z has a *linear factor* (as well as in the cases (C), (D)).

This linear factor, since it must contain both x and y, can be written as $x-uy-v$. We obtain then from (101), putting there $uy+v$ instead of x,

$$(uy+v)^m \equiv -y^n - cuy^2 - cvy - 1, \qquad 2\leqslant m\leqslant 4,\ n\leqslant m. \tag{115}$$

From this formula follows $m\leqslant n$, and since we assumed $n\leqslant m$ we see that we must have $n=m$ and have now 3 cases to consider:

$$m=n=4; \qquad m=n=3; \qquad m=n=2.$$

Since then $v^m=-1$, $v\neq 0$, the expression on the left, developped in y, has $m+1$ *distinct* terms. We see that $m\leqslant 3$ and therefore there are no linear factors in the case (B).

104. Assume now $m=n=3$. Developping (115) and comparing the coefficients on both sides we obtain

$$(-u)^3=1,\ 3u^2v=-cu,\ 3uv^2=-cv,\ (-v)^3=1.$$

The 2nd and 3rd of these relations give $c=-3uv$. Since $-u$ and $-v$ are 3rd roots of 1, we can write then

$$c=-3\varepsilon,\ \varepsilon^3=1. \tag{116}$$

If we denote now $-u$ by ε_1, it follows $-v=\varepsilon/\varepsilon_1$, and if these relations are satisfied we have a linear factor

$$x+\varepsilon_1 y+\varepsilon\varepsilon_1^2,$$

where the 3 values of c are -3, -3ε, $-3\varepsilon^2$, denoting here by $\varepsilon\neq 1$ a primitive 3rd root of 1. Taking here for ε_1 its 3 possible values we obtain in each case 3 distinct linear factors of Z, and Z is their product. The simplest of the 3 formulas is the following formula, classical in the theory of the division of circle:

$$\begin{aligned} x^3+y^3+1-3xy &= (x+y+1)(x^2+y^2+1-x-y-xy) \\ &= (x+y+1)(x+\varepsilon_1 y+\varepsilon_1^2)(x+\varepsilon_1^2 y+\varepsilon_1). \end{aligned} \tag{117}$$

The other formulas are obtained from (117) replacing there y with εy.

105. Finally, in the case $m=2$ we obtain from (117) for $m=2$, comparing the coefficients on the right and on the left, $c=\pm 2$, and the corresponding Z are indeed products:

$$x^2+y^2\pm 2xy+1=(x\pm y+i)(x\pm y-i), \tag{118}$$

where both signs are the same.

106. To summarize our results we have for $m=n=4$ for c:

$$c=\pm 2\sqrt{2}, \qquad c=\pm 2\sqrt{2}\,i; \tag{119}$$

for $m=n=3$:

$$c=-3\varepsilon, \qquad \varepsilon^3=1; \tag{120}$$

for $m=n=2$:

$$c=\pm 2. \tag{121}$$

Returning to the general form of the polynomial Z, as given in Sec. 92,

$$Z:=1+aP_1+bP_2+\gamma P_3, \tag{122}$$

we have completed now the discussion of the case that in (122) P_1 and P_2 are independent and

$$P_3=P_1^pP_2^q, \qquad p+q\leqslant 1, p\wedge q>0, \tag{123}$$

where the inequalities on p and q signify that the baric polyhedron of Z is a triangle.

Rewritting now our conditions in terms of P_1, P_2, P_3, we see that Z can be only reducible if

$$p=q=\frac{1}{m} \quad (m=2\vee 3\vee 4). \tag{124}$$

For the coefficients a, b, γ, we obtain the condition

$$\gamma=c\sqrt[m]{ab},$$

where the values of c corresponding to the 3 values of m are given by (119), (120), (121). If all these conditions are satisfied, Z is indeed reducible in the domain of algebraic polynomials.

If we consider the irreducibility in the domain of rational polynomials we must add the condition that $P_1^{1/m}$ and $P_2^{1/m}$ are rational.

§ 16. Observations on four term polynomials with a baric plane quadrangle

107. We consider now a general four term polynomial with a *plane baric quadrangle*. In this case we must restrict ourselves to some few reductions of the problem. Assuming one of the terms $\equiv 1$, it can be written as

$$1 + P_1 + P_2 + P_3,$$

where P_1 and P_2 correspond to the two summits of the baric quadrangle adjacent to the summit at the origin.

Then, if we introduce

$$P_1 =: \xi, \qquad P_2 =: \eta$$

as new variables, our polynomial can be written as

$$1 + \xi + \eta + c\xi^\alpha\eta^\beta, \qquad \alpha + \beta > 1,$$

where $c \neq 0$ and α, β are rational positive numbers. Denoting a common denominator of α and β by n and putting further

$$\xi = x^n, \qquad \eta = y^n,$$

we obtain finally

$$Z := 1 + x^n + y^n + cx^py^q, \qquad c \neq 0, p + q > n, \tag{125}$$

where p and q are positive integers.

We have now to consider the cases, where Z is reducible in the domain of algebraic polynomials. However, choosing n conveniently, Z would become reducible in the domain of rational and even integer polynomials, so that we can restrict ourselves to the consideration of the reducibility of (125) in the domain of integer polynomials.

108. We consider first the case where either p or $q = n$. Without loss of generality assume $p = n$,

$$Z = x^n(1 + cy^q) + (1 + y^n).$$

Putting now

$$R := -\frac{1 + y^n}{1 + cy^q}, \tag{126}$$

all n roots of the equation with respect to x, $Z=0$, have the form $\varepsilon R^{1/n}$ for a fixed choice of $R^{1/n}$ and an arbitrary n-th root of unity, ε. Suppose now that the polynomial $F(x, y)$ is a divisor of Z of degree $m<n$ with respect to x. We assume F in the form $x^m+\cdots$ with coefficients which are rational in y. Then all roots of the equation in $x:F=0$ have also the form $\varepsilon R^{1/n}$, and it follows that $R^{m/n}$ is a rational function in y. Put now

$$(m, n)=:g, \qquad n/g=:s>1. \tag{127}$$

Then, choosing the integers a and b with $an-bm=g$, it follows that

$$R^{a-bm/n}\equiv R^{1/s}$$

is a rational function in y, and we can write

$$R^{1/s}=\frac{f(y)}{g(y)}, \quad (f, g)=1,$$

where f and g are relatively prime polynomials in y. Raising this into the power s it follows now

$$(1+y^n)g^s=-(1+cy^q)f^s. \tag{128}$$

But here, since $s>1$, the multiple factors of f^s cannot occur in the left-side expression, as $(f, g)=1$ and $1+y^n$ has no multiple factors.

109. We see that Z cannot have a factor of degree $m<n$ in x for $p=n$. And as to the factors of degree n, they are only and always possible if $1+cy^q$ and $1+y^n$ have common factors.

Writing c in the form $e^{-\xi\pi i}$ with a convenient complex ξ the condition for ξ becomes, denoting by κ and λ convenient integers,

$$\exp\frac{(\xi+2\kappa+1)\pi i}{q}=\exp\frac{(2\lambda+1)\pi i}{n}$$

or

$$\frac{\xi+2\kappa+1}{q}\equiv\frac{2\lambda+1}{n} \pmod 2,$$

$$\xi=\frac{2\lambda+1}{n}q-2\kappa-1+2rq,$$

for a convenient integer r, and therefore finally

$$c := \exp(1-(2\lambda+1)\,q/n)\,\pi i, \tag{129}$$

for an arbitrary integer λ.

We can therefore from now on assume $p \lessgtr n$, $q \lessgtr n$.

110. We are now going to show that Z, given by (125), is always irreducible if $p<n$, $q<n$.

Indeed, assume that Z is reducible. If we then apply the Lemma 5 of Sec. 11, replacing there z with x and k with p, we obtain in the notations of the lemma

$$\chi = 1, \qquad \psi_1 = cy^q, \qquad \varphi = 1 + y^n.$$

Therefore, if we use the degree in y as weight, all conditions of the Lemma 5 are satisfied, and we see that n is divisible by p. By symmetry n is also divisible by q. But then we have certainly

$$p \leqslant \frac{n}{2}, \qquad q \leqslant \frac{n}{2}$$

and $p+q>n$ is impossible.

Since we can still interchange x with y we see that we could from now on assume without loss of generality

$$p > n, \qquad q \lessgtr n. \tag{130}$$

111. We finally observe that if $q<n$ the form (125) can be somewhat simplified.

In this case we can apply the Lemma 5 of Sec. 11 replacing there z with x and n with p. Then we obtain

$$\chi = cy^q, \qquad \psi = 1, \qquad \varphi = 1 + y^n.$$

Here the conditions of the Lemma 5 are satisfied if we take the degree in y as weight. It follows that in this case p in (125) is divisible by n and we can therefore, changing the notations, reduce Z to the form

$$Z = 1 + x + y^n + cx^p y^q, \qquad 1 < q < n, \; p > 1. \tag{131}$$

List of technical terms and notations

$:=$ reads: is a notation for
$=:$ reads: will be denoted by
$\wedge$ reads: as well as
$\vee$ reads: or

CH-6926 Certenago/Montagnola, Ti.,
Schweiz (Switzerland)