

# ABSTRACT POLYNOMIALS IN NON-ABELIAN GROUPS

KNOX MILLSAPS

**Introduction.** The aim of this note is to give some generalizations for groups of the theories of abstract polynomials as developed by Fréchet, Gateaux, Martin, Mazur, Michal, Orlicz and more recently, Van der Lijn.<sup>1</sup> Although the theories are equivalent for functions with arguments and values in abelian groups,<sup>2</sup> this equivalence is not the case when the argument and value groups are non-abelian.<sup>3</sup>

In §1, a calculus of finite differences for functions with arguments and values in non-abelian groups which contain no elements of finite order is defined, and the fundamental definitions of polynomials and monomials are stated. In §2, the homogeneity in the increment of the  $n$ -difference of a polynomial of degree  $n$  is proved, and the theorem on unique pseudo-decomposition is proved after giving some preliminary theorems on the structure of differences of arbitrary functions and polynomials. In §3, a brief discussion of the extensions to non-abelian groups as value spaces is given.

I should like to thank Professor A. D. Michal for his helpful suggestions and constructive criticisms during the preparation of this note.

**1. Definitions.** For the purposes of polynomial theory the value groups are restricted to contain no elements of finite order.

To construct the calculus of finite differences for functions with arguments and values in non-abelian groups, we define

$$\omega\Delta[\alpha_1; \beta_1]f(x) \equiv \begin{cases} f(x\omega)f^{-1}(x) & \text{if } \alpha_1 = 1 \text{ and } \beta_1 = 1, \\ f(\omega x)f^{-1}(x) & \text{if } \alpha_1 = 1 \text{ and } \beta_1 = 2, \\ f^{-1}(x)f(x\omega) & \text{if } \alpha_1 = 2 \text{ and } \beta_1 = 1, \\ f^{-1}(x)f(\omega x) & \text{if } \alpha_1 = 2 \text{ and } \beta_1 = 2, \end{cases}$$

---

Presented to the Society, April 11, 1942; received by the editors April 21, 1942.

<sup>1</sup> References to these theories will be found in the bibliography. This list will be referred to by numbers in brackets.

<sup>2</sup> The equivalence of some of these definitions was proved by Martin in his California Institute of Technology thesis, 1932, and of the remaining definitions by Van der Lijn. A summary has been given by Van der Lijn [1, pp. 78-80].

<sup>3</sup> If the abstraction of additivity is multiplicative distributivity, then the generalizations of the definitions of Mazur and Orlicz [1, p. 63] and Van der Lijn, [1, pp. 60-61] are not equivalent; this is easily seen by considering  $f(x) \equiv x^k$ .

and inductively

$$\begin{aligned} \omega^n \Delta [\alpha_1, \dots, \alpha_n; \beta_1, \dots, \beta_n] f(x) \\ \equiv \omega \Delta [\alpha_n; \beta_n] \omega^{n-1} \Delta [\alpha_1, \dots, \alpha_{n-1}; \beta_1, \dots, \beta_{n-1}] f(x). \end{aligned}$$

DEFINITION OF A MONOMIAL. A  $[\alpha_1, \dots, \alpha_n; \beta_1, \dots, \beta_n]$  monomial<sup>4</sup> is a function  $f(x)$  which satisfies for all  $x$  and  $\omega$  the following functional equation

$$\omega^n \Delta [\alpha_1, \dots, \alpha_n; \beta_1, \dots, \beta_n] f(x) = f^{n^1}(\omega).$$

The obviously unique value of  $n$  is termed the degree of the monomial.

DEFINITION OF A POLYNOMIAL. A function  $f(x)$  which satisfies the following functional equation for all  $x$  and  $\omega$

$$\omega^{n+1} \Delta [\alpha_1, \dots, \alpha_{n+1}; \beta_1, \dots, \beta_{n+1}] f(x) = 1$$

will be called a  $[\alpha_1, \dots, \alpha_{n+1}; \beta_1, \dots, \beta_{n+1}]$  polynomial.<sup>5</sup>

The least value of  $n$  for which the above equation holds will be termed the degree of the polynomial.

The binomial coefficients are denoted in the usual manner;  $\Gamma_{k,n}^t$  is defined by

$$\Gamma_{k,n}^i \equiv \sum \frac{n!}{\alpha_1! \alpha_2! \dots \alpha_{k+1}!}$$

where  $\sum_{i=1}^{k+1} \alpha_i = n$ ,  $\sum_{q=2}^{k+1} (q-1) \alpha_q = i$ ,  $i \neq nk$ , and  $i \neq 0$ . An arbitrary element of the central subgroup will be denoted by  $\vartheta$ . To simplify notation, the dropping of unnecessary indices implies that the value of a product of factors is independent of the order of the particular factors controlled by the dropped indices.

The next equation is a generalization of an identity due to Marchaud<sup>6</sup>

$$\omega^{k+1} \Delta [\beta_1, \dots, \beta_n] f(x) = \sum_{i=0}^{nk} \sum_j^n \omega \Delta [\beta_1, \dots, \beta_n] f [P_{ij}],$$

<sup>4</sup> The inner automorphisms of a group are interesting examples of a  $[1; 2]$  monomial; similarly, the canonical transformations of quantum mechanics.

<sup>5</sup> If the elements of a group are taken to be the  $n \times n$  matrices whose elements are in a commutative field and whose determinants do not vanish, and if the group operation is defined as row by column multiplication, then  $f[||x_j^i||] \equiv ||a_i^k x_m^k x_n^m b_j^n||$  is a  $[1, 1; 2, 1]$  polynomial.

<sup>6</sup> Marchaud [1, p. 368].

where  $j = 1, \dots, \Gamma_{k,n}^i$  and  $P_{ij}$  denotes a particular permutation of  $\omega, \omega, \dots, \omega$  ( $i$  times) and  $x$ .

**2. Fundamental theorems.** Let  $A(x)$  denote a function with arguments in a non-abelian group and values in an abelian group. The theorems of Van der Lijn for functions with arguments and values in abelian groups can be extended with a few immediate changes to hold for differences of the type  ${}^n\Delta A(x)$ . This section is devoted to abstractions for differences of the kind  ${}^n\Delta[\beta_1, \dots, \beta_n]A(x)$ , where  $\omega$  is an arbitrary element.

**THEOREM I.** *If  $A(x)$  is a  $[\beta_1, \dots, \beta_{n+1}]$  polynomial of degree  $n$ , and if  $k$  is an integer, then*

$$\omega^k \Delta[\beta_1, \dots, \beta_n]A(x) = k^n \omega^n \Delta[\beta_1, \dots, \beta_n]A(x).$$

**PROOF.** For  $k=0$  or  $1$ , the theorem is trivial. For  $k>1$ , we hypothetically have

$${}^n\Delta[\beta_1, \dots, \beta_n]A(x, \omega^i) - {}^n\Delta[\beta_1, \dots, \beta_n]A(x, \omega^{i-1}) = 0.$$

By a few manipulations and Marchaud's identity we get

$$\begin{aligned} \omega^k \Delta[\beta_1, \dots, \beta_n]A(x) &= \sum_{i=0}^{n(k-1)} \Gamma_{k-1,n}^i \omega^n \Delta[\beta_1, \dots, \beta_n]A(x) \\ &= k^n \omega^n \Delta[\beta_1, \dots, \beta_n]A(x). \end{aligned}$$

For  $k<0$ , we evidently have

$$\begin{aligned} \omega^k \Delta[\beta_1, \dots, \beta_n]A(x) &= (\omega^{-1})^{-k} \Delta[\beta_1, \dots, \beta_n]A(x) \\ &= (-k)^n \omega^{-n} \Delta[\beta_1, \dots, \beta_n]A(x) \\ &= (-)^n (-k)^n \omega^n \Delta[\beta_1, \dots, \beta_n]A(x) \\ &= k^n \omega^n \Delta[\beta_1, \dots, \beta_n]A(x). \end{aligned}$$

**THEOREM II.** *If  ${}^n\Delta[\beta_1, \dots, \beta_n]A(x) = g(\omega)$ , where  $g(\omega)$  is independent of  $x$ , then  $g(\omega)$  is a  $[\beta_1, \dots, \beta_n]$  monomial of degree  $n$  in  $\omega$ .*

**THEOREM III.** *If  $A(x)$  is a  $[\beta_1, \dots, \beta_{n+1}]$  polynomial of degree  $n$ , then  ${}^n\Delta[\beta_1, \dots, \beta_n]A(x)$  is independent of  $x$ .*

**PROOF.** If  $n+2$  elements of the argument group are denoted by  $x_i$ , where

$$x_{i+1} = \prod(x_i, \xi), \quad i = 0, \dots, n+1,$$

then by steps roughly analogous to the usual proof of similar theorems we can derive

$$\sum_{p=0}^n \sum_{i=0}^{n+1} C_{n+1,i} C_{n,p} (-)^i i^{n-p} k^p \omega \Delta [\beta_1, \dots, \beta_n] A(x_i) = 0.$$

In the last equation we see that  $\sum_{p=0}^n C_{n,p} k^p$  is a simple polynomial. From this observation we deduce<sup>7</sup>

$$\sum_{i=0}^{n+1} (-)^i C_{n+1,i} i^{n-p} \omega \Delta [\beta_1, \dots, \beta_n] A(x_i) = 0, \quad p = 0 \dots, n.$$

If we consider one difference as given and the remaining  $n + 1$  differences as unknown, then the unique solutions are

$$\omega \Delta [\beta_1, \dots, \beta_n] A(x_i) = \omega \Delta [\beta_1, \dots, \beta_n] A(x_0), \quad i = 1, \dots, n + 1,$$

for the determinant of the system of equations is given by

$$(-)^{\delta(n)} \prod_{i=1}^{n+1} C_{n+1,i} V \neq 0$$

where  $V$  is a Vandermonde determinant and  $\delta(n) = 1$ , if  $n \equiv 1, 2 \pmod 4$ ;  $\delta(n) = 2$ , if  $n \equiv 0, 3 \pmod 4$ .

**THEOREM IV.** *If  $A(x)$  is a  $[\beta_1, \dots, \beta_{n+1}]$  polynomial of degree  $n$ , and if  $\rho_n = \prod_{i=0}^n (n-i)!$ , then we have the unique pseudo-decomposition*

$$\rho_n A(x) = \sum_{i=0}^n M_i(x),$$

where  $M_i(x)$  are  $[\beta_1, \dots, \beta_i]$  monomials of degree  $i$ .

**3. Further discussion.** With the generalized definition of a polynomial an extension of Theorem I for functions with arguments and values in non-abelian groups can be made. The trivial converse of Theorem III can be proved in an obvious manner. The non-abelian analogue of Theorem IV does not hold, for counterexamples can be exhibited.<sup>8</sup>

In conclusion, it is remarked that the difficulty with the non-abelian valued case is an inability to solve explicitly a system of group equations.

<sup>7</sup> It can be shown that if a simple polynomial  $\sum_{i=0}^n a_i x^i$  of degree  $n$  vanishes for  $n + 1$  distinct values of  $x$ , then the coefficients vanish.

<sup>8</sup> With the group defined in (5), a trivial, but sufficient, example is  $\|x_j^i\| = \|x_j^i\| \|\delta_j^i\| = \|\delta_j^i\| \|x_j^i\|$ .

## BIBLIOGRAPHY

M. FRÉCHET

1. *Une définition fonctionnelle des polynômes*, Nouvelles Annales de Mathématiques (4) vol. 9 (1909) pp. 145–162.
2. *Les polynômes abstraits*, Journal de Mathématiques vol. 8 (1929) pp. 71–92.

R. GATEAUX

1. *Sur diverses questions du calcul fonctionnel*, Bull. Soc. Math. France vol. 50 (1922) pp. 1–37.

A. MARCHAUD

1. *Sur les dérivées et sur les différences des fonctions de variables réelles*, Journal de Mathématiques vol. 6 (1927) pp. 337–425.

S. MAZUR AND W. ORLICZ

1. *Grundlegende Eigenschaften der polynomische Operationen*, Studia Mathematica vol. 5 (1934) pp. 58–68, 179–189.

A. D. MICHAL AND R. S. MARTIN

1. *Some expansions in vector space*, Journal de Mathématiques vol. 13 (1934) pp. 69–91.

G. VAN DER LIJN

1. *Les polynômes abstraits*, Bull. Sci. Math. vol. 64 (1940) pp. 55–80, 102–112, 163–196.

CALIFORNIA INSTITUTE OF TECHNOLOGY

## ON THE QUADRIC OF LIE

SU-CHENG CHANG

The most important quadric attached to an ordinary point of a non-ruled and nondegenerate surface is, perhaps, the quadric of Lie. The characteristic curve of the quadric of Lie varying along an asymptotic curve of the surface decomposes into an asymptotic tangent and two edges of the quadrilateral of Demoulin.<sup>1</sup> In this note we propose to determine whether the characteristic curve of the quadric of Lie may decompose into two conics when the quadric of Lie varies along certain curves of the surface. The answer is positive.

Let  $(u, v)$  be the asymptotic net of a surface  $(M)$  and  $(M, M_1, M_2, M_3)$  its normal tetrahedron of Cartan,  $MM_1, MM_2$  being the two asymptotic tangents and  $MM_3, M_1M_2$  being the directrices of Wilczynski. Except for a projective transformation the surface  $(M)$  is determined by the system

---

Received by the editors June 8, 1942.

<sup>1</sup> A. Demoulin, *Sur la théorie des lignes asymptotiques*, C. R. Acad. Sci. Paris vol. 147 (1908) pp. 413–415, *Sur la quadrique de Lie*, *ibid.* pp. 493–496, *Sur quelques propriétés des surfaces courbes*, *ibid.* pp. 565–568.