Journal of Number Theory 139 (2014) 1–28

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

# Classification of polynomial mappings between commutative groups

Uwe Schauz

*Department of Mathematical Science, Xi'an Jiaotong-Liverpool University, Suzhou 215123, China*

ARTICLE INFO

*Article history:*
Received 7 April 2013
Received in revised form 23 December 2013
Accepted 29 December 2013
Available online 7 February 2014
Communicated by David Goss

*MSC:*
05E99
13F20
41A05

*Keywords:*
Integer-valued polynomials
Commutative groups
Polynomial functions
Polynomial mappings
Interpolation

ABSTRACT

Some polynomials $P$ with rational coefficients give rise to well defined maps between cyclic groups, $\mathbb{Z}_q \longrightarrow \mathbb{Z}_r$, $x + q\mathbb{Z} \longmapsto P(x) + r\mathbb{Z}$. More generally, there are polynomials in several variables with tuples of rational numbers as coefficients that induce maps between commutative groups. We characterize the polynomials with this property, and classify all maps between two given finite commutative groups that arise in this way. We also provide interpolation formulas and a Taylor-type theorem for the calculation of polynomials that describe given maps.



## 1. Introduction

The polynomial

$$P := -\tfrac{1}{8}X^4 + \tfrac{3}{4}X^3 - \tfrac{7}{8}X^2 - \tfrac{3}{4}X + 1 \tag{1}$$

*E-mail address:* uwe.schauz@xjtlu.edu.cn.

http://dx.doi.org/10.1016/j.jnt.2013.12.010

induces a map $\mathbb{Z}_3 \longrightarrow \mathbb{Z}_9$ in a canonical way. At first, it gives rise to a map $\mathbb{Z} \longrightarrow \mathbb{Q}$ which actually is integer valued, as one can show. Second, this map $\mathbb{Z} \longrightarrow \mathbb{Z}$ induces the map $\mathbb{Z} \longrightarrow \mathbb{Z}_9$, $x \longmapsto P(x) + 9\mathbb{Z}$. Finally, it turns out that our new map is even 3-periodic,

$$P(x+3) \equiv P(x) \pmod 9. \tag{2}$$

So, we obtain a well defined map

$$P : \mathbb{Z}_3 \longrightarrow \mathbb{Z}_9, \qquad x = \hat{x} + 3\mathbb{Z} \longmapsto P(x) := P(\hat{x}) + 9\mathbb{Z}. \tag{3}$$

Moreover, the map $P$ is a kind of *Lagrange Polynomial*. For $x \in \mathbb{Z}_3 := \mathbb{Z}/3\mathbb{Z}$,

$$P(x) = \binom{0}{x}_{3,9} := \begin{cases} 1 + 9\mathbb{Z} & \text{if } x = 0, \\ 0 + 9\mathbb{Z} & \text{if } x \neq 0. \end{cases} \tag{4}$$

As any function is a linear combination of Lagrange Functions, we see that any map $\mathbb{Z}_3 \longrightarrow \mathbb{Z}_9$ can be represented by a polynomial in $\mathbb{Q}[X]$ of degree at most 4. Of course, not every polynomial over $\mathbb{Q}$ gives rise to a well defined map $\mathbb{Z}_3 \longrightarrow \mathbb{Z}_9$, but we have enough polynomials to obtain all maps. This is not true for maps $\mathbb{Z}_q \longrightarrow \mathbb{Z}_r$ in general: it holds only if $q$ and $r$ are powers of a common prime $p$. In contrast, if $q$ is coprime to $r$ then only constant maps can be described by a rational polynomial. These two extremal results are the antagonistic forces that determine the general case. To reduce the question of representability of maps between $\mathbb{Z}_q$ and $\mathbb{Z}_r$, with general $q$ and $r$, to these two cases, we split the domain $\mathbb{Z}_q$ and the codomain $\mathbb{Z}_r$ into cyclic $p$-groups, and decompose polynomial maps $\mathbb{Z}_q \longrightarrow \mathbb{Z}_r$ into maps between the cyclic $p$-factors. More precisely, we write the domain $\mathbb{Z}_q$ as direct product of $n$ cyclic $p$-groups, and introduce one variable $X_j$ for each of them. Similarly, the codomain $\mathbb{Z}_r$ is split into $t$ cyclic $p$-groups, and the coefficients of our polynomials are split into rational $t$-tuples accordingly. These decompositions can be done without changing the property of polynomial representability (Theorem 3.16), but they bring us closer to our two extremal cases. Decompositions also allow the treatment of maps between arbitrary finite commutative groups $A$ and $B$. Our main result, Theorem 3.15, says that, if $A_1, A_2, \ldots, A_t$ and $B_1, B_2, \ldots, B_t$ are the (possibly trivial or noncyclic) primary components of $A$ and $B$ (corresponding to the different prime divisors $p_1, p_2, \ldots, p_t$ of $|A||B|$), then the polynomial representable maps in $B^A$ are exactly the maps

$$(f_1, \ldots, f_t) \in B_1^{A_1} \times \cdots \times B_t^{A_t}, \qquad (a_1, \ldots, a_t) \mapsto \big(f_1(a_1), \ldots, f_t(a_t)\big). \tag{5}$$

Partial results in this direction, but sometimes over more general rings and sometimes in the language of iterated differences, were obtained in several other papers, e.g. in [2–5, 7–14,17], and in the books [1,15]. Our paper differs from most of these investigations in that we do not restrict ourselves to the case where domain and codomain coincide. We also do not just count or determine the isomorphy type of modules of certain maps.