POLYNOMIAL EQUIVALENCE OF FINITE RINGS

GEORG GRASEGGER, GÁBOR HORVÁTH, AND KEITH A. KEARNES

Abstract. We prove that $\mathbb{Z}_{p^n}$ and $\mathbb{Z}_p[t]/(t^n)$ are polynomially equivalent if and only if $n \leq 2$ or $p^n = 8$. For the proof, employing Bernoulli numbers, we explicitly provide the polynomials which compute the carry-on part for the addition and multiplication in base p. As a corollary, we characterize finite rings of p^2 elements up to polynomial equivalence.

1. Introduction

One of the most basic objectives of algebra is to characterize different algebraic structures up to certain equivalences. Very often, characterization up to isomorphism is considered. In this paper, we investigate certain finite rings, and characterize them up to polynomial equivalence.

A polynomial function over an algebra is a function built up from projections, constant functions and basic operations using composition. Two algebras are *polynomially equivalent* if they are defined on the same domain and have the same polynomial functions [5]. It is easy to see that two algebras are polynomially equivalent if and only if the basic operations of one algebra can be expressed as polynomials of the other algebra, and vice versa.

The question to characterize algebras up to polynomial equivalence arises quite naturally. From a Computer Science perspective, polynomials capture the functions computable by the algebra, and polynomial equivalent algebras can compute exactly the same functions. In many cases though, different algebras are not defined on the same domain, but can still be polynomial equivalent if the elements are identified via some bijection φ. Therefore in the paper we use the following definition of polynomial equivalence.

2010 *Mathematics Subject Classification.* 13M10 (13B25, 11B68).

Key words and phrases. polynomial equivalence, finite rings, Bernoulli numbers, carry for base p addition, carry for base p multiplication.

Corresponding author: Gábor Horváth (ghorvath@science.unideb.hu).

The first author was partially supported by the strategic program "Innovatives OÖ 2010plus" by the Upper Austrian Government and by the Austrian Science Fund (FWF): W1214-N15, project DK11. The second author was partially supported by the Austrian Science Fund (FWF): P24077, by the Hungarian National Foundation grant no. K109185, and by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

Definition 1. Let $\mathcal{R}_1 = (R_1, +_1, \times_1)$ and $\mathcal{R}_2 = (R_2, +_2, \times_2)$ be two rings, and let $\varphi\colon R_1 \to R_2$ be a bijection. We say that the rings $\mathcal{R}_1$ and $\mathcal{R}_2$ are *polynomially equivalent via* φ if there exist polynomial functions f_1, g_1 over $\mathcal{R}_1$ and polynomial functions f_2, g_2 over $\mathcal{R}_2$ such that for arbitrary $x, y \in R_1$ we have

$$\begin{aligned}
\varphi(x +_1 y) &= f_2(\varphi(x), \varphi(y)),\\
\varphi(x \times_1 y) &= g_2(\varphi(x), \varphi(y)),\\
\varphi(f_1(x, y)) &= \varphi(x) +_2 \varphi(y),\\
\varphi(g_1(x, y)) &= \varphi(x) \times_2 \varphi(y).
\end{aligned}$$

In particular, $\mathcal{R}_1 \overset{\varphi}{\cong} (R_2, f_2, g_2)$ and $(R_1, f_1, g_1) \overset{\varphi}{\cong} \mathcal{R}_2$. One can extend this notion to arbitrary algebras in a natural way, but we skip the general definition as the scope of the paper is limited to rings. Note, however, that if the elements of the two rings are identified via the bijection φ, then our definition for polynomial equivalence coincides with the usual one.

One of the most interesting cases of nonisomorphic algebras that are polynomially equivalent comes from group theory. Any nonabelian simple group is polynomially complete by [9], thus its polynomial equivalence type is determined by its order. There are nonisomorphic nonabelian simple groups of the same order, e.g. both $PSL(4, 2)$ and $PSL(3, 4)$ have 20160 elements [11]. Similarly, any two simple unital rings of the same order are polynomially equivalent [8] but not necessarily isomorphic. In particular, the full matrix ring $M_m(q)$ is isomorphic to $M_n(r)$ if and only if $m = n$ and $q = r$, but they are polynomially equivalent if and only if $q^{m^2} = r^{n^2}$.

In our paper we consider the rings $\mathbb{Z}_{p^n}$ and $\mathbb{Z}_p[t]/(t^n)$ for positive integers n and primes p. These rings are isomorphic only for $n = 1$, but always have the same number of elements, same number of unary polynomial functions [4] and the same ideal structure. Their elements even have a natural correspondence: for $P = \{0, 1, \ldots, p-1\}$, every element of $\mathbb{Z}_{p^n}$ can be uniquely written in the form of $\sum_{i=0}^{n-1} a_i p^i$ ($a_i \in P$), and every element of $\mathbb{Z}_p[t]/(t^n)$ can be uniquely written in the form of $\sum_{i=0}^{n-1} a_i t^i$ ($a_i \in P$). We determine when these two rings are polynomially equivalent via some bijection.

Theorem 2. *Let p be a positive prime and n a positive integer. Let $P = \{0, 1, \ldots, p-1\}$. The two rings $\mathbb{Z}_{p^n}$ and $\mathbb{Z}_p[t]/(t^n)$ are*

1. *polynomially equivalent via $\varphi\colon \mathbb{Z}_{p^n} \to \mathbb{Z}_p[t]/(t^n)$, $\sum_{i=0}^{n-1} a_i p^i \mapsto \sum_{i=0}^{n-1} a_i t^i$ ($a_i \in P$) for $n \leq 2$ and for $p^n = 8$;*
2. *not polynomially equivalent via any bijection $\mathbb{Z}_{p^n} \to \mathbb{Z}_p[t]/(t^n)$ if $n \geq 3$, except for $p^n = 8$.*

The proof of Theorem 2 consists of two main parts. We prove item (1) in Section 3 and item (2) in Section 4. For proving item (1) we give the

polynomials for f_1, g_1, f_2, g_2. The main differences between the addition and multiplication of the two rings $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p[t]/(t^2)$ are essentially the carry-on parts of addition and multiplication in base p. It turns out that to make f_1, g_1, f_2, g_2 explicit, one has to determine the polynomials for these carry-on functions. Note that the existence of such polynomials follows from the fact that $\mathbb{Z}_p$ is polynomially complete, hence every function (and in particular, the carry-on functions) can be represented as polynomials (see e.g. [10]). Moreover, the polynomial equivalence of $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p[t]/(t^2)$ follows from the results of [1, 6], in particular the existence of f_1 and f_2 is proved in [1, Lemma 22]. We, in fact, provide the polynomials expressing the carry-on part of the addition and multiplication in base p, therefore making the polynomial equivalence of these rings explicit. We introduce these polynomials employing Bernoulli numbers in Sections 2.4 and 2.5, then prove the addition part of item (1) in Section 3.1 and the multiplication part of item (1) in Section 3.2.

All the required notions and lemmas for the proof are summarized in Section 2. Finally, in Section 5 we apply Theorem 2 to characterize the rings containing p^2 elements up to polynomial equivalence and prove the following.

Corollary 3. *Let us use the notation of* [3] *for rings having p^2 elements, that is let $A = \mathbb{Z}_{p^2}$, $B = p\mathbb{Z}_{p^3}$, $C = p^2\mathbb{Z}_{p^4}$, $D = \mathbb{Z}_p \oplus \mathbb{Z}_p$, E and F be the two noncommutative p^2-element rings, $G = \mathbb{Z}_p[t]/(t^2)$, $H = \mathbb{Z}_p \oplus p\mathbb{Z}_{p^2}$, $I = t\mathbb{Z}_p[t]/(t^3)$, $J = p\mathbb{Z}_{p^2} \oplus p\mathbb{Z}_{p^2}$, and K be the p^2-element field, where $\oplus$ denotes the direct sum of rings. Then the rings A, E, F, G are polynomially equivalent to each other, B is polynomially equivalent to I for $p = 2$, and no other two rings having p^2 elements are polynomially equivalent.*

Finally, we note that some of our results follow from the known theory of polynomially rich algebras (see e.g. [6]). Polynomially rich algebras are defined for arbitrary algebras, not only for rings. Nevertheless, their theory goes beyond the scope of this paper, therefore we translate the known results for rings.

That is, a ring $\mathcal{R}$ is called polynomially rich if every map $f\colon \mathcal{R}^n \to \mathcal{R}$ preserving ideals and the type of every single factor $\mathcal{I}/\mathcal{J}$ for $\mathcal{I}, \mathcal{J} \lhd \mathcal{R}$ is a polynomial over $\mathcal{R}$. In particular, if two polynomially rich rings have the same ideal structure and have the same single factors $\mathcal{I}/\mathcal{J}$ for ideals $\mathcal{I}, \mathcal{J}$, then they are polynomially equivalent. Theorem 24 of [6] shows that a ring $\mathcal{R}$ having a unique minimal ideal $\mathcal{I}$ is polynomially rich if and only if conditions (SC1) and (GRp) hold for this ring. Now, (SC1) holds for $\mathcal{R}$ if and only if for every ideal $\mathcal{J} \gneqq \mathcal{I}$ the ideal $\mathcal{I}\mathcal{J}$ is nonzero (that is, it contains $\mathcal{I}$).

It is much harder to translate the condition (GFp) for rings, but from Lemma 4 of [1] it follows that if for such a ring $\mathcal{I}^2 = 0$ and there

exists a nonconstant, nonidentity unary, idempotent polynomial (i.e. a polynomial p for which $p \circ p = p$), then the ring is polynomially rich.

Now, the ideal structure of the rings A, E, F and G are the same: there exists a unique ideal squaring to 0, the factor by this ideal is isomorphic to the p-element field. It is clear that (SC1) holds for all four rings, and an easy calculation shows that $x \mapsto x^{p^2}$ is a nonconstant, nonidentity idempotent polynomial for all four rings, hence (GFp) holds, as well. Thus the polynomial functions of all four rings are the ones preserving their (same) ideal structures, and hence they are all polynomially equivalent. In Section 5 we provide an elementary proof of Corollary 3.

2. Preliminaries

2.1. **Notation.** Throughout the paper, p always denotes a positive prime, n a positive integer, and m a nonnegative integer. We use i and j for running indices, k for indexing Bernoulli numbers. We use $\equiv_p$ for indicating that the two sides are congruent modulo p. By P we denote the set $\{\, 0, 1, \ldots, p-1 \,\}$.

For rings $\mathcal{R}_1$ and $\mathcal{R}_2$, a function from $\mathcal{R}_i$ will be denoted by using the index $i \in \{\, 1, 2 \,\}$. We denote the addition of $\mathcal{R}_i$ by $+_i$, the subtraction of $\mathcal{R}_i$ by $-_i$, and the multiplication of $\mathcal{R}_i$ by $\times_i$ ($i \in \{\, 1, 2 \,\}$). For $p > 2$ we write $+_p$ and $\times_p$ for the modulo p addition and multiplication over P. Finally, we use the usual $+$ and $\cdot$ for the usual addition and multiplication over the integers, unless we explicitly indicate otherwise.

2.2. **Polynomially equivalent rings via a bijection.** Let $\mathcal{R}_1$ and $\mathcal{R}_2$ be two finite rings having the same number of elements. Let $\varphi\colon \mathcal{R}_1 \to \mathcal{R}_2$ be a bijection and assume $\mathcal{R}_1$ and $\mathcal{R}_2$ are polynomially equivalent via φ. Conjugating every polynomial function over $\mathcal{R}_2$ by adding $\varphi(0_1)$ to them, we can assume that $\varphi(0_1) = 0_2$.

Lemma 4. *Let $\mathcal{R}_1$ and $\mathcal{R}_2$ be finite rings, $\varphi\colon \mathcal{R}_1 \to \mathcal{R}_2$ a bijection. Assume $\mathcal{R}_1$ and $\mathcal{R}_2$ are polynomially equivalent via φ. Then there exists a bijection $\varphi'\colon \mathcal{R}_1 \to \mathcal{R}_2$ such that $\varphi'(0_1) = 0_2$, and $\mathcal{R}_1$ and $\mathcal{R}_2$ are polynomially equivalent via φ'. Moreover, if $\mathcal{I}_1 \lhd \mathcal{R}_1$, then $\varphi'(\mathcal{I}_1) \lhd \mathcal{R}_2$.*

Proof. Let h_2 be an arbitrary invertible unary polynomial over $\mathcal{R}_2$ such that $h_2(0_2) = \varphi(0_1)$. Such a polynomial exists, e.g. $h_2(x) = x +_2 \varphi(0_1)$ suffices. Denote the inverse polynomial of h_2 by h_2^{-1}. Let $h_1\colon \mathcal{R}_1 \to \mathcal{R}_1$ be the corresponding polynomial over $\mathcal{R}_1$, that is

$\varphi(h_1(x)) = h_2(\varphi(x))$. Let h_1^{-1} denote the inverse of h_1. Then for

$$\begin{aligned}
&\varphi' \colon \mathcal{R}_1 \to \mathcal{R}_2, && x \mapsto h_2^{-1}(\varphi(x)),\\
&f_1' \colon \mathcal{R}_1 \times \mathcal{R}_1 \to \mathcal{R}_1, && (x,y) \mapsto h_1\left(f_1\left(h_1^{-1}(x), h_1^{-1}(y)\right)\right),\\
&g_1' \colon \mathcal{R}_1 \times \mathcal{R}_1 \to \mathcal{R}_1, && (x,y) \mapsto h_1\left(g_1\left(h_1^{-1}(x), h_1^{-1}(y)\right)\right),\\
&f_2' \colon \mathcal{R}_2 \times \mathcal{R}_2 \to \mathcal{R}_2, && (x,y) \mapsto h_2^{-1}(f_2(h_2(x), h_2(y))),\\
&g_2' \colon \mathcal{R}_2 \times \mathcal{R}_2 \to \mathcal{R}_2, && (x,y) \mapsto h_2^{-1}(g_2(h_2(x), h_2(y))),
\end{aligned}$$

the rings $\mathcal{R}_1$ and $\mathcal{R}_2$ are polynomially equivalent via φ', where f_1', g_1' correspond to $+_2$ and $\times_2$, and f_2', g_2' correspond to $+_1$ and $\times_1$, moreover $\varphi'(0_1) = 0_2$.

If $\mathcal{I}_1 \lhd \mathcal{R}_1$ is an ideal, then the congruence defined by $\mathcal{I}_1$ is preserved by polynomials of $\mathcal{R}_1$, in particular by f_1' and g_1'. Therefore the φ'-image of this congruence is preserved by $+_2$ and $\times_2$, and thus is a congruence of $\mathcal{R}_2$. As every congruence of a ring is defined by an ideal and $\varphi'(\mathcal{I}_1) \ni \varphi'(0_1) = 0_2$, $\varphi'(\mathcal{I}_1)$ must be an ideal of $\mathcal{R}_2$. □

Note that a similar proof shows that for general algebras the φ-image of a coset of a congruence has to be a coset of a congruence.

2.3. **Bernoulli Numbers.** Bernoulli numbers are defined by the recurrence formula

$$\sum_{k=0}^{m} \binom{m+1}{k} B_k = 0$$

for $m \geq 1$, and $B_0 = 1$ [7, Chapter 15]. With this definition we have $B_1 = -1/2$, and $B_k = 0$ for every other odd k.

A basic property of Bernoulli numbers [7, Chapter 15, Theorem 1] is that for all $m \geq 0, y \geq 1$ integers, we have

$$\frac{1}{m+1} \sum_{k=0}^{m} (-1)^k \binom{m+1}{k} B_k y^{m+1-k} = \sum_{k=1}^{y} k^m. \tag{1}$$

For $2 \mid k$ Clausen [2] and Von Staudt [12] proved the following on the denominators of the Bernoulli numbers:

$$B_k + \sum_{\substack{q \text{ prime} \\ (q-1)|k}} \frac{1}{q} \in \mathbb{Z}. \tag{2}$$

In particular, $B_0 = 1$ is an integer, and if $p - 1 > k \geq 1$, then p does not divide the denominator of B_k (in its simplified form). Thus B_k for $p - 1 > k$ can be calculated modulo p. Furthermore we use a consequence of Voronoi's Congruence [7, Proposition 15.2.3], which relates the numerator and denominator of a Bernoulli number modulo an integer. Let $p \geq 3$ be a prime and x an integer not divisible by p.

For positive even $k < p-1$ one can compute B_k/k modulo p, and then

$$\frac{B_k}{k}(x^k - 1) \equiv_p x^{k-1} \sum_{j=1}^{p-1} j^{k-1} \left\lfloor \frac{jx}{p} \right\rfloor. \tag{3}$$

Finally, for an odd prime p and for $a \in \{\, 1, \ldots, p-1 \,\}$, after evaluating the sum of the corresponding geometric series, one has

$$\sum_{i=1}^{p-1} a^i \equiv_p \begin{cases} 0, & \text{if } a \neq 1, \\ -1, & \text{if } a = 1, \end{cases} \tag{4}$$

$$\sum_{\substack{k=2 \\ 2|k}}^{p-3} a^{k-1} \equiv_p \begin{cases} -\frac{1}{a}, & \text{if } a^2 \not\equiv_p 1, \\ -\frac{3}{2a}, & \text{if } a^2 \equiv_p 1, \end{cases} \tag{5}$$

where the second sum runs only on the even indices for a prime $p > 3$.

2.4. **Carry-on for addition modulo p.**

Lemma 5. *Let p be an odd prime, and let $P = \{\, 0, 1, \ldots, p-1 \,\}$. Let $a\colon P \times P \to P$ be the carry-on for the modulo p addition, that is*

$$a(x,y) = \begin{cases} 0, & \text{if } x + y < p, \\ 1, & \text{if } x + y \geq p. \end{cases}$$

Let $A(x,y)$ be defined by

$$A(x,y) = \sum_{i=1}^{p-1} \sum_{k=0}^{p-i-1} \frac{1}{p-i} (-1)^{k+i+1} B_k \binom{p-i}{k} x^i y^{p-i-k},$$

where every sum and multiplication is considered modulo p. Then $a(x,y) = A(x,y)$ for arbitrary $x, y \in P$.

Proof. First, we prove that A is well defined. Now, B_k appears in the formula only for $k < p-1$, and thus can be calculated modulo p. The fraction $1/(p-i)$ can be calculated modulo p, as well. Hence, A is a well defined polynomial over $\mathbb{Z}_p$.

If $y = 0$, then $A(x,y) = 0 = a(x,y)$. Otherwise, $y \in \{\, 1, \ldots, p-1 \,\}$, and

$$A(x,y) \equiv_p \sum_{i=1}^{p-1} x^i \frac{1}{p-i} \sum_{k=0}^{p-i-1} (-1)^{k+i+1} B_k \binom{p-i}{k} y^{p-i-k}$$

(we apply (1) with $m = p-i-1$)

$$= \sum_{i=1}^{p-1} (-1)^{i+1} x^i \sum_{k=1}^{y} k^{p-i-1}$$

(for $k \in \{1, \dots, p-1\}$ we have $k^{p-1} \equiv_p 1$)

$$\equiv_p \sum_{k=1}^{y} \sum_{i=1}^{p-1} (-1)^{i+1} x^i k^{-i} \equiv_p -\sum_{k=1}^{y} \sum_{i=1}^{p-1} \left(-\frac{x}{k}\right)^i.$$

By (4), we have

$$\sum_{i=1}^{p-1} \left(-\frac{x}{k}\right)^i \equiv_p \begin{cases} -1, & \text{if } k \equiv_p -x, \\ 0, & \text{if } k \not\equiv_p -x. \end{cases}$$

Now, there exists at most one $k \in \{1, \dots, y\}$ such that $k \equiv_p -x$, and such a k exists if and only if $y \geq p - x$, that is if $x + y \geq p$. Thus,

$$-\sum_{k=1}^{y} \sum_{i=1}^{p-1} \left(-\frac{x}{k}\right)^i \equiv_p \begin{cases} -\sum_{k=1}^{y} 0 = 0, & \text{if } x + y < p, \\ 1, & \text{if } x + y \geq p. \end{cases}$$

Therefore, $A(x, y) = a(x, y)$ for arbitrary $x, y \in P$. □

2.5. **Carry-on for multiplication modulo p.**

Lemma 6. *Let p be an odd prime, and let $P = \{0, 1, \dots, p-1\}$. Let $m \colon P \times P \to P$ be the carry-on for the modulo p multiplication, that is*

$$m(x, y) = \left\lfloor \frac{xy}{p} \right\rfloor.$$

Let $M(x, y)$ be defined by

$$M(x, y) = \sum_{k=1}^{p-2} \frac{B_k}{k} \left(x - x^{p-k}\right) \left(y - y^{p-k}\right),$$

where every sum and multiplication is considered modulo p. Then $m(x, y) = M(x, y)$ for arbitrary $x, y \in P$.

Proof. First, we prove that M is well defined. Now, B_k appears in the formula only for $k < p - 1$, and thus can be calculated modulo p. The fraction $1/k$ can be calculated modulo p, as well. Hence, M is a well defined polynomial over $\mathbb{Z}_p$.

For $x = 0$, or $y \in \{0, 1\}$ the equation $M(x, y) = m(x, y)$ is clear. Otherwise, $x^{p-1} = 1$, $y^{p-1} = 1$, and the term for the index $k = 1$ in $M(x, y)$ is $B_1/1 \cdot (x - x^{p-1}) \cdot (y - y^{p-1}) = -(x-1)(y-1)/2$. For $y = p - 1 \equiv_p -1$ and for even k we have $y - y^{p-k} \equiv_p 0$. Since $B_k = 0$ for odd $k \geq 3$, we have then $M(x, p-1) \equiv_p -(x-1) \cdot (-2)/2 = x - 1 = \lfloor x(p-1)/p \rfloor = m(x, p-1)$. This finishes the proof in case $y \in \{0, 1, p-1\}$, and hence the case $p = 3$. Assume $x \neq 0$, $y \notin \{0, 1, p-1\}$, $p > 3$. Now,

$$\sum_{k=1}^{p-2} \frac{B_k}{k} \left(x - x^{p-k}\right) \left(y - y^{p-k}\right)$$

(we cut the sum for $k=1$ and use that if $2 \nmid k \geq 3$, then $B_k = 0$)

$$\equiv_p -\frac{(x-1)(y-1)}{2} + \sum_{\substack{k=2 \\ 2|k}}^{p-3} \frac{B_k}{k} \left(x - x^{p-k}\right) \left(y - y^{p-k}\right)$$

(we have $x \equiv_p x^p$)

$$\equiv_p -\frac{(x-1)(y-1)}{2} + \sum_{\substack{k=2 \\ 2|k}}^{p-3} \frac{B_k}{k} \left(x^p - x^{p-k}\right) \left(y - y^{p-k}\right)$$

$$\equiv_p -\frac{(x-1)(y-1)}{2} + \sum_{\substack{k=2 \\ 2|k}}^{p-3} x^{p-k}(y - y^{p-k}) \cdot \frac{B_k}{k}(x^k - 1)$$

(we apply (3) for $2 \mid k$)

$$\equiv_p -\frac{(x-1)(y-1)}{2} + \sum_{\substack{k=2 \\ 2|k}}^{p-3} x^{p-k}(y - y^{p-k}) \cdot x^{k-1} \sum_{j=1}^{p-1} j^{k-1} \left\lfloor \frac{jx}{p} \right\rfloor$$

(we have $x^{p-k} \cdot x^{k-1} = x^{p-1} \equiv_p 1$, $y^{p-k} = y^{p-1} \cdot y^{1-k} \equiv_p y^{1-k}$)

$$\equiv_p -\frac{(x-1)(y-1)}{2} + \sum_{\substack{k=2 \\ 2|k}}^{p-3} (y - y^{1-k}) \sum_{j=1}^{p-1} j^{k-1} \left\lfloor \frac{jx}{p} \right\rfloor$$

$$= -\frac{(x-1)(y-1)}{2} + \sum_{j=1}^{p-1} \left\lfloor \frac{jx}{p} \right\rfloor \sum_{\substack{k=2 \\ 2|k}}^{p-3} (y - y^{1-k}) j^{k-1}. \tag{6}$$

By (5), we have

$$\sum_{\substack{k=2 \\ 2|k}}^{p-3} y j^{k-1} = y \sum_{\substack{k=2 \\ 2|k}}^{p-3} j^{k-1} \equiv_p \begin{cases} -y/j, & \text{if } j \not\equiv_p \pm 1, \\ -3y/(2j), & \text{if } j \equiv_p \pm 1, \end{cases}$$

$$-\sum_{\substack{k=2 \\ 2|k}}^{p-3} y^{1-k} j^{k-1} = -\sum_{\substack{k=2 \\ 2|k}}^{p-3} \left(\frac{j}{y}\right)^{k-1} \equiv_p \begin{cases} y/j, & \text{if } j \not\equiv_p \pm y, \\ 3y/(2j), & \text{if } j \equiv_p \pm y, \end{cases}$$

and since $y \in \{2, \ldots, p-2\}$, we obtain

$$\sum_{\substack{k=2 \\ 2|k}}^{p-3} \left(y - y^{1-k}\right) j^{k-1} \equiv_p \begin{cases} -y/(2j), & \text{if } \pm 1 \equiv_p j \not\equiv_p \pm y, \\ +y/(2j), & \text{if } \pm 1 \not\equiv_p j \equiv_p \pm y, \\ 0, & \text{if } \pm 1 \not\equiv_p j \not\equiv_p \pm y. \end{cases}$$

Now, we cut the sum in (6) into five parts: two parts for $\pm 1 \equiv_p j \not\equiv_p \pm y$, two parts for $\pm 1 \not\equiv_p j \equiv_p \pm y$, and one part for $j \notin \{\pm 1, \pm y\}$:

$$\begin{aligned}
&-\frac{(x-1)(y-1)}{2}+\sum_{j=1}^{p-1}\left\lfloor\frac{jx}{p}\right\rfloor\sum_{\substack{k=2\\2|k}}^{p-3}(y-y^{1-k})j^{k-1}\\
&\equiv_p -\frac{(x-1)(y-1)}{2}+\underbrace{\left\lfloor\frac{x}{p}\right\rfloor\cdot\frac{-y}{2}}_{j=1}+\underbrace{\left\lfloor\frac{(p-1)x}{p}\right\rfloor\cdot\frac{y}{2}}_{j=p-1}\\
&+\underbrace{\left\lfloor\frac{yx}{p}\right\rfloor\cdot\frac{1}{2}}_{j=y}+\underbrace{\left\lfloor\frac{(p-y)x}{p}\right\rfloor\cdot\frac{-1}{2}}_{j=p-y}+\sum_{\substack{j=2\\j\neq\pm y}}^{p-3}\left\lfloor\frac{jx}{p}\right\rfloor\cdot 0
\end{aligned}$$

(we have $\lfloor x/p\rfloor = 0$, $\lfloor (p-1)x/p\rfloor = \lfloor x - x/p\rfloor = x-1$, and similarly $-\lfloor (p-y)x/p\rfloor = -\lfloor x - yx/p\rfloor = -(x-1)+\lfloor yx/p\rfloor$)

$$\begin{aligned}
&\equiv_p -\frac{(x-1)(y-1)}{2}+0+\frac{(x-1)y}{2}\\
&+\left\lfloor\frac{yx}{p}\right\rfloor\cdot\frac{1}{2}-\frac{x-1}{2}+\left\lfloor\frac{yx}{p}\right\rfloor\cdot\frac{1}{2}+0=\left\lfloor\frac{yx}{p}\right\rfloor.
\end{aligned}$$

Therefore, $M(x,y) = m(x,y)$ for arbitrary $x, y \in P$. □

3. Proof of item (1) of Theorem 2

For $n = 1$, the two rings are isomorphic, hence polynomially equivalent. For $p^n = 4$, by computing the operation tables, it is easy to check that the following polynomials satisfy the requirements:

$$\begin{aligned}
f_1(x,y) &= x+y+2xy,\\
g_1(x,y) &= xy,\\
f_2(x,y) &= x+y+txy,\\
g_2(x,y) &= xy.
\end{aligned}$$

Here, we denoted the additions and the multiplications for both rings in the usual way, because we believe that it does not cause confusion and the formulas are more understandable this way. Furthermore, the following polynomials satisfy the requirements for $p^n = 8$:

$$\begin{aligned}
f_1(x,y) &= x+y+2xy+xy(1+x)(1+y)+2xy\left(1+x^2\right)\left(1+y^2\right),\\
g_1(x,y) &= xy+x^2y^2(3+x)(3+y),\\
f_2(x,y) &= x+y+txy+xy(1+x)(1+y)+txy(x+y)^2,\\
g_2(x,y) &= xy+x^2y^2(1+x)(1+y).
\end{aligned}$$

The fact that these polynomials indeed satisfy the requirements can be checked by hand or by a computer program rather easily. In the

following, we provide some guidelines how it could be performed manually. Let $\mathcal{R}_1 = \mathbb{Z}_8$, $\mathcal{R}_2 = \mathbb{Z}_2[t]/t^3$. Let $P = \{0, 1\}$. We identify the elements of $\mathcal{R}_1$ and $\mathcal{R}_2$ with the elements of $P \times P \times P$ via the bijections $x_0 + 2x_1 + 4x_2 \mapsto (x_0, x_1, x_2)$ and $x_0 + tx_1 + t^2x_2 \mapsto (x_0, x_1, x_2)$ for $x_0, x_1, x_2 \in P$. Thus, we consider both $\mathcal{R}_1$ and $\mathcal{R}_2$ on the domain $P \times P \times P$, i.e. $\mathcal{R}_1 = (P \times P \times P, +_1, \times_1)$, $\mathcal{R}_2 = (P \times P \times P, +_2, \times_2)$. Note, that for this proof $+$ and $\cdot$ denote the modulo 2 operations.

We detail the proof for f_2 being the same function as $+_1$. The other three cases can be handled in a similar fashion. Now,

$$\begin{aligned}&(x_0, x_1, x_2) +_1 (y_0, y_1, y_2)\\ &\qquad = (x_0 + y_0, x_1 + y_1 + a(x_0, y_0), x_2 + y_2 + b(x_1, y_1, a(x_0, y_0))),\end{aligned}$$

where $x_i, y_i \in P$, a and b denote the binary and ternary carry-on functions:

$$a(x, y) = \begin{cases} 0, & \text{if } x + y < 2,\\ 1, & \text{if } x + y \geq 2,\end{cases}$$

$$b(x, y, z) = \begin{cases} 0, & \text{if } x + y + z < 2,\\ 1, & \text{if } x + y + z \geq 2.\end{cases}$$

Now, it is not hard to see that $a(x, y) = xy$ and $b(x, y, z) = xy+(x+y)z$, yielding

$$\begin{aligned}&(x_0, x_1, x_2) +_1 (y_0, y_1, y_2)\\ &\qquad = (x_0 + y_0, x_1 + y_1 + x_0y_0, x_2 + y_2 + x_1y_1 + (x_1 + y_1)x_0y_0).\end{aligned}$$

An easy computation shows that for $x = (x_0, x_1, x_2)$, $y = (y_0, y_1, y_2)$

$$\begin{aligned}&f_2(x, y)\\ &= x_0 + y_0 + t\,(x_1 + y_1 + x_0y_0) + t^2\,(x_2 + y_2 + x_1y_1 + (x_1 + y_1)x_0y_0)\,,\end{aligned}$$

which corresponds to the same tuple from $P \times P \times P$ as $(x_0, x_1, x_2) +_1 (y_0, y_1, y_2)$.

In the remaining of Section 3, p denotes an odd prime. Let $\mathcal{R}_1 = \mathbb{Z}_{p^2}$, $\mathcal{R}_2 = \mathbb{Z}_p[t]/(t^2)$. Let $P = \{0, 1, \ldots, p - 1\}$. We identify the elements of $\mathcal{R}_1$ and $\mathcal{R}_2$ with the elements of $P \times P$ via the bijections $x_0 + px_1 \mapsto (x_0, x_1)$ and $x_0 + tx_1 \mapsto (x_0, x_1)$ $(x_0, x_1 \in P)$. Thus, we consider both $\mathcal{R}_1$ and $\mathcal{R}_2$ on the domain $P \times P$, i.e. $\mathcal{R}_1 = (P \times P, +_1, \times_1)$, $\mathcal{R}_2 = (P \times P, +_2, \times_2)$.

3.1. **Addition.** Now, we have $(x_0, x_1) +_1 (y_0, y_1) = (x_0 +_p y_0, x_1 +_p y_1 +_p a(x_0, y_0))$, where

$$a(x_0, y_0) = \begin{cases} 0, & \text{if } x_0 + y_0 < p,\\ 1, & \text{if } x_0 + y_0 \geq p,\end{cases}$$

is the carry-on part of the addition in base p. Addition in $\mathcal{R}_2$ is the modulo p addition in both coordinates: $(x_0, x_1) +_2 (y_0, y_1) = (x_0 +_p y_0, x_1 +_p y_1)$. Thus, to express the operation $+_1$ in $\mathcal{R}_2$, one needs to find a polynomial over $\mathcal{R}_2$ (expressed by $+_2$ and $\times_2$) representing $a(x_0, y_0)$. Let $f_2(x, y) = x +_2 y +_2 t \times_2 A(x, y)$ over $\mathcal{R}_2$, where

$$A(x,y) = \sum_{i=1}^{p-1} \sum_{k=0}^{p-i-1} \frac{1}{p-i}(-1)^{k+i+1} B_k \binom{p-i}{k} x^i y^{p-i-k},$$

and every sum uses $+_2$, and every multiplication uses $\times_2$. Now, B_k appears in the formula only for $k < p-1$, and thus can be calculated modulo p. The fraction $1/(p-i)$ can be calculated modulo p, as well. Hence, f_2 is a polynomial over $\mathcal{R}_2$. Moreover, $t \times_2 t = 0$ yields

$$t \times_2 A(x_0 +_2 t \times_2 x_1, y_0 +_2 t \times_2 y_1) = t \times_2 A(x_0, y_0),$$

and thus

$$f_2(x_0 +_2 t \times_2 x_1, y_0 +_2 t \times_2 y_1) = x_0 +_2 y_0 +_2 t \times_2 (x_1 +_2 y_1 +_2 A(x_0, y_0))$$

over $\mathcal{R}_2$, that is,

$$f_2((x_0, x_1), (y_0, y_1)) = (x_0 +_p y_0, x_1 +_p y_1 +_p A(x_0, y_0)).$$

By Lemma 5, we have $A(x_0, y_0) = a(x_0, y_0)$, which proves that $+_1$ is a polynomial over $\mathcal{R}_2$. Hence, the polynomial f_2 corresponds to the addition of $\mathcal{R}_1$. Similarly, the polynomial $f_1(x, y) = x +_1 y -_1 p \times_1 A(x, y)$ over $\mathcal{R}_1$ expresses the addition of $\mathcal{R}_2$.

3.2. **Multiplication.** We continue with the multiplication in a similar fashion. Now, $(x_0, x_1) \times_1 (y_0, y_1) = (x_0 \times_p y_0, x_0 \times_p y_1 +_p x_1 \times_p y_0 +_p m(x_0, y_0))$, where

$$m(x_0, y_0) = \left\lfloor \frac{x_0 y_0}{p} \right\rfloor$$

is the carry-on part of the multiplication in base p. Multiplication in $\mathcal{R}_2$ is similar, except there is no carry-on part: $(x_0, x_1) \times_2 (y_0, y_1) = (x_0 \times_p y_0, x_0 \times_p y_1 +_p x_1 \times_p y_0)$. Thus, to express the operation $\times_1$ in $\mathcal{R}_2$, one needs to find a polynomial over $\mathcal{R}_2$ (expressed by $+_2$ and $\times_2$) representing $m(x_0, y_0)$. Let $g_2(x, y) = x \times_2 y +_2 t \times_2 M(x, y)$ over $\mathcal{R}_2$, where

$$M(x,y) = \sum_{k=1}^{p-2} \frac{B_k}{k} \left(x - x^{p-k}\right)\left(y - y^{p-k}\right),$$

and every sum uses $+_2$, and every multiplication uses $\times_2$. Now, B_k appears in the formula only for $k < p-1$, and thus can be calculated modulo p. The fraction $1/k$ can be calculated modulo p, as well. Hence, g_2 is a polynomial over $\mathcal{R}_2$. Moreover, $t \times_2 t = 0$ yields

$$t \times_2 M(x_0 +_2 t \times_2 x_1, y_0 +_2 t \times_2 y_1) = t \times_2 M(x_0, y_0),$$

and thus

$$g_2(x_0 +_2 t \times_2 x_1, y_0 +_2 t \times_2 y_1) = \\ x_0 \times_2 y_0 +_2 t \times_2 (x_0 \times_2 y_1 +_2 x_1 \times_2 y_0 +_2 M(x_0, y_0))$$

over $\mathcal{R}_2$, that is,

$$g_2((x_0, x_1), (y_0, y_1)) = (x_0 \times_p y_0, x_0 \times_p y_1 +_p x_1 \times_p y_0 +_p M(x_0, y_0)).$$

By Lemma 6, we have $M(x_0, y_0) = m(x_0, y_0)$, which proves that $\times_1$ is a polynomial over $\mathcal{R}_2$. Hence, the polynomial g_2 corresponds to the multiplication of $\mathcal{R}_1$. Similarly, the polynomial $g_1(x, y) = x +_1 y -_1 p \times_1 M(x, y)$ over $\mathcal{R}_1$ expresses the multiplication of $\mathcal{R}_2$.

4. Proof of item (2) of Theorem 2

Let $\mathcal{R}_1 = \mathbb{Z}_{p^n}$, $\mathcal{R}_2 = \mathbb{Z}_p[t]/(t^n)$, and assume that they are polynomially equivalent via $\varphi\colon \mathcal{R}_1 \to \mathcal{R}_2$. By Lemma 4 we may assume $\varphi(0_1) = 0_2$. Let f_2 over $\mathcal{R}_2$ correspond to the addition in $\mathcal{R}_1$. Let $\mathcal{I}_1$ be the unique ideal in $\mathcal{R}_1$ containing p^2-many elements, i.e. $\mathcal{I}_1 = (p^{n-2})$, and let $\mathcal{I}_2$ be the unique ideal in $\mathcal{R}_2$ containing p^2-many elements, i.e. $\mathcal{I}_2 = (t^{n-2})$. Then by Lemma 4 we have $\varphi(\mathcal{I}_1) = \mathcal{I}_2$. In this section 0 denotes the zero element of $\mathcal{R}_2$, $+$ and $\cdot$ denote the addition and multiplication of $\mathcal{R}_2$. Assume $n \geq 3$, then $\mathcal{I}_2^3 = (0)$.

Consider $f_2(x, y)$ over $\mathcal{R}_2$, restricted to $\mathcal{I}_2$. This function corresponds to the addition over $\mathcal{R}_1$ restricted to $\mathcal{I}_1$. Since $\mathcal{I}_2^3 = (0)$, for every $x, y \in \mathcal{I}_2$ the function f_2 attains the same value at $(x, y) \in \mathcal{I}_2 \times \mathcal{I}_2$ as $a + bx + cy + dxy + ex^2 + fy^2$ for some $a, b, c, d, e, f \in \mathcal{R}_2$. Now, $f_2(0, 0) = 0$ implies $a = 0$, $f_2(x, 0) = x$ implies $bx + ex^2 = x$, $f_2(0, y) = y$ implies $cy + fy^2 = y$, hence $f_2'(x, y) = x + y + dxy$ attains the same values on $\mathcal{I}_2$ as f_2. By induction on m, it is easy to prove that for every positive integer m we have $f_2'(f_2'(\dots f_2'(f_2'(x, x), x), \dots, x), x) = mx + d\binom{m}{2}x^2$, if we compose the polynomial f_2' with itself $m - 1$-many times. Consider the case $m = p$. For $p > 2$, by $p \mid \binom{p}{2}$ we obtain that $f_2'(f_2'(\dots f_2'(f_2'(x, x), x), \dots, x), x)$ is the constant 0 function over $\mathcal{I}_2$, while $x +_1 x +_1 \dots +_1 x = p \times_1 x$ is not a constant function over $\mathcal{I}_1$. This contradiction proves that if $p > 2$, $n \geq 3$, then $\mathcal{R}_1$ and $\mathcal{R}_2$ are not polynomially equivalent.

If $n \geq 4$, then already $\mathcal{I}_2^2 = (0)$. Thus, $f_2'(x, y) = x + y$, and therefore $\varphi\colon \mathcal{R}_1 \to \mathcal{R}_2$ is an isomorphism between the additive groups of $\mathbb{Z}_{p^2}$ and $(\mathbb{Z}_p)^2$. This contradiction proves that if $n \geq 4$, then $\mathcal{R}_1$ and $\mathcal{R}_2$ are not polynomially equivalent.

5. Proof of Corollary 3

Let us use the notation of [3], that is $A = \mathbb{Z}_{p^2}$, $B = p\mathbb{Z}_{p^3}$, $C = p^2\mathbb{Z}_{p^4}$, $D = \mathbb{Z}_p \oplus \mathbb{Z}_p$, E and F are the two noncommutative p^2-element rings, $G = \mathbb{Z}_p[t]/(t^2)$, $H = \mathbb{Z}_p \oplus p\mathbb{Z}_{p^2}$, $I = t\mathbb{Z}_p[t]/(t^3)$, $J = p\mathbb{Z}_{p^2} \oplus p\mathbb{Z}_{p^2}$, and K

is the p^2-element field, where $\oplus$ denotes the direct sum of rings. Note that $p\mathbb{Z}_{p^2}$ and $p^2\mathbb{Z}_{p^4}$ are zero rings.

Now, A and G are polynomially equivalent by Theorem 2. The proof detailed in Section 4 shows that B and I are not polynomially equivalent for $p \neq 2$. For $p = 2$, $\mathbb{Z}_8$ and $\mathbb{Z}_2[t]/(t^3)$ are polynomially equivalent by Theorem 2. Moreover, as described in the beginning of Section 3, the polynomials f_1, g_1 over $\mathbb{Z}_8$ exist over the unique four-element ideal B, and the polynomials f_2, g_2 over $\mathbb{Z}_2[t]/(t^3)$ exist over the unique four-element ideal I. Thus B and I are polynomially equivalent for $p = 2$. The rings E and F are opposite rings of each other, thus they are polynomially equivalent ($x +_1 y = x +_2 y$, $x \times_1 y = y \times_2 x$). Finally, we show that G and F are polynomially equivalent.

Let $P = \{\, 0, 1, \ldots, p-1 \,\}$ and consider. The ring F can be represented by

$$\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in P \right\},$$

with the usual matrix addition and multiplication. Let $\varphi\colon G \to F$ be defined by

$$a + bt \mapsto \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}.$$

Here, we denote the additions and the multiplications for both rings in the usual way, because we believe that it does not cause confusion and the formulas are more understandable this way. Now, φ is an isomorphism between the additive groups of G and F, hence it is enough to provide polynomials for the multiplications. Let e be the nonzero diagonal idempotent matrix in F. We claim that the polynomials

$$\begin{aligned} g_1(x, y) &= x^p y, \\ g_2(x, y) &= (p-1)xye + xy + yx \end{aligned}$$

give the multiplication for F and G, respectively. Indeed, if $x = a + bt$ and $y = c + dt$ (for arbitrary $a, b, c, d \in P$), then

$$\begin{aligned} \varphi\left(g_1(x, y)\right) &= \varphi\left((a+bt)^p\,(c+dt)\right) = \varphi\left(a^p\,(c+dt)\right) = \varphi\left(ac + adt\right) \\ &= \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \varphi(x)\,\varphi(y), \\ g_2\left(\varphi(x), \varphi(y)\right) &= (p-1)\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \\ &\quad + \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = (p-1)\begin{pmatrix} ac & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix} \\ &\quad + \begin{pmatrix} ac & bc \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac & ad+bc \\ 0 & 0 \end{pmatrix} = \varphi\left(ac + (ad+bc)t\right) \\ &= \varphi(xy). \end{aligned}$$

Polynomially equivalent rings must have the same ideal structure by Lemma 4, and the factors by the corresponding ideals must be polynomially equivalent. Thus, K is not polynomially equivalent to the others, as that is the only simple ring of p^2 elements. The only ring having $p+1$ nontrivial ideals is J, hence it is not polynomially equivalent to any of the other rings. There are two rings having two nontrivial ideals (D and H), and in D both ideals are isomorphic to the p-element field, while in H one of the ideals is isomorphic to the p-element zero-ring. Since the factors by the corresponding ideals isomorphic to the p-element field are not polynomially equivalent, neither are D and H.

A ring R which is not a zero-ring cannot be polynomially equivalent to C, because the multiplication of R cannot be expressed as a polynomial over C. Namely, every polynomial over C is of the form $g(x, y) = ax + by + c$. Now, if g corresponds to the multiplication, assuming 0 in R corresponds to 0 in C, then $g(0, 0) = 0$ yields $c = 0$, $g(x, 0) = 0$ yields $ax = 0$, $g(0, y) = 0$ yields $by = 0$, hence g is the 0 function.

Finally, the ring A is not polynomially equivalent to either B or I, because the factors by the unique nontrivial ideal are not polynomially equivalent.

6. Acknowledgements

We are grateful to Erhard Aichinger for drawing our attention to this problem. We thank Peter Mayr for discussions on this topic. We are indebted to the anonymous referee for their insightful suggestions.

References

[1] A. A. Bulatov, 'Polynomial clones containing the Mal'tsev operation of the groups $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$', *Mult.-Valued Log.* (2) **8** (2002), 193–221 Multiple-valued logic in Eastern Europe.

[2] T. Clausen, 'Theorem', *Astron. Nachr.* **17** (1840), 351–352.

[3] B. Fine, 'Classification of finite rings of order p^2', *Math. Mag.* (4) **66** (1993), 248–252.

[4] S. Frisch, 'Polynomial functions on finite commutative rings', in: *Advances in commutative ring theory. Proceedings of the 3rd international conference, Fez, Morocco* (ed. D. E. Dobbs et al.), volume 205 of *Lecture Notes in Pure and Applied Mathematics* (Marcel Dekker, New York, 1999) pp. 323–336.

[5] D. Hobby and R. McKenzie, *The structure of finite algebras*, volume 76 of *Contemporary Mathematics* (American Mathematical Society, Providence, 1988).

[6] P. M. Idziak and K. Słomczyńska, 'Polynomially rich algebras', *J. Pure Appl. Algebra* (1) **156** (2001), 33–68.

[7] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory* (Springer-Verlag, New York, 1982).

[8] M. Istinger and H. K. Kaiser, 'A characterization of polynomially complete algebras', *J. Algebra* (1) **56** (1979), 103–110.

[9] W. D. Maurer and J. L. Rhodes, 'A property of finite simple non-abelian groups', *Proc. Amer. Math. Soci.* **16** (1965), 552–554.

[10] L. Rédei and T. Szele, 'Algebraischzahlentheoretische Betrachtungen über Ringe. I', *Acta Math.* **79** (1947), 291–320.
[11] I. M. Schottenfels, 'Two non-isomorphic simple groups of the same order 20,160', *Ann. of Math. (2)* (1-4) **1** (1899–1900), 147–152.
[12] Ch. von Staudt, 'Beweis eines Lehrsatzes, die Bernoullischen Zahlen betreffend', *J. Reine Angew. Math.* **21** (1840), 372–374.

E-mail address: Georg.Grasegger@risc.jku.at

Doctoral Program Computational Mathematics, Research Institute for Symbolic Computation, Johannes Kepler University Linz, Altenberger Strasse 69, 4040 Linz, Austria

E-mail address: ghorvath@science.unideb.hu

Institute of Mathematics, University of Debrecen, Pf. 12, Debrecen, 4010, Hungary

Institute for Algebra, Johannes Kepler University Linz, Altenberger Strasse 69, 4040 Linz, Austria

E-mail address: Keith.Kearnes@Colorado.EDU

Department of Mathematics, University of Colorado, Boulder CO 80309-0395