Mathematica Bohemica

Cyril Gavala; Miroslav Ploščica; Ivana Varga

Congruence preserving operations on the ring $\mathbb{Z}_{p^3}$

Mathematica Bohemica, Vol. 148 (2023), No. 4, 519–535

Persistent URL: http://dml.cz/dmlcz/151972

CONGRUENCE PRESERVING OPERATIONS ON THE RING $\mathbb{Z}_{p^3}$

Cyril Gavala, Miroslav Ploščica, Ivana Varga, Košice

Received October 11, 2021. Published online October 11, 2022.
Communicated by Radomír Halaš

Abstract. We investigate the interval $I(p^3)$ in the lattice of clones on the ring $\mathbb{Z}_{p^3}$ between the clone of polynomial operations and the clone of congruence preserving operations. All clones in this interval are known and described by means of generators. In this paper, we characterize each of these clones by the property of preserving a small set of relations. These relations turn out to be in a close connection to commutators.

Keywords: congruence; clone; polynomial

MSC 2020: 08A40, 03B50

1. Introduction and preliminaries

A *clone* on a set A is a family of operations which contains all projections and is closed under composition. The family of all clones on A forms a lattice. This lattice is completely known for $|A| = 2$. If $|A| > 2$, then the lattice of all clones is uncountable and its full description seems intractable. Much of the research is devoted to describing various parts of this lattice. The clones connected with some algebraic structure on A seem to be especially interesting. There are several papers investigating clones containing some group operation on A. For instance, see Idziak [11], Aichinger and Mayr [1], and Mayr [12].

An n-ary operation f on an algebra A is called *compatible* or *congruence preserving* if $(x_1, y_1), \dots, (x_n, y_n) \in \theta$ implies $(f(x_1, \dots, x_n), f(y_1, \dots, y_n)) \in \theta$ for every congruence $\theta \in \operatorname{Con} A$. It is clear that all compatible operations form a clone, denoted by $\operatorname{Comp}(A)$. This clone includes the clone $\operatorname{P}(A)$ of all polynomial operations on A. So, $\operatorname{P}(A) \subseteq \operatorname{Comp}(A)$ and there is a natural problem of describing the interval between $\operatorname{P}(A)$ and $\operatorname{Comp}(A)$.

The research has been supported by Project vvgs-pf-2020-1426 and VEGA Grant No. 1/0152/22.

DOI: 10.21136/MB.2022.0155-21

One of the most popular algebras are the rings $\mathbb{Z}_n$ of integers modulo n. Clones connected with modular arithmetic were studied in papers [17], [19], [20], [3], [4], and others. Let $I(n)$ denote the interval in the lattice of clones between $\mathrm{P}(\mathbb{Z}_n)$ and $\mathrm{Comp}(\mathbb{Z}_n)$. The problem of describing $I(n)$ reduces to the case when $n = p^k$ is a prime power (see [15]). If n is a prime, then it is well known that $\mathrm{P}(\mathbb{Z}_n) = \mathrm{Comp}(\mathbb{Z}_n)$. The case $k = 2$ has been solved by Remizov in [16], who showed that $I(p^2)$ is a 2-element lattice. Alternative proofs of this result can be found in Bulatov [6], and also in [15]. Partial results for $k = 3$ have been established in [16], [9], [10], and [13]. A complete description of $I(p^3)$ has been achieved in [15], relying substantially on Bulatov's description of all clones on $\mathbb{Z}_{p^2}$ containing the addition and constants.

The main aim of the present paper is the study of invariant relations. We say that an *operation* $f\colon A^n \to A$ *preserves a relation* $E \subseteq A^k$ if for every $i = 1, \dots, n$, $(a_{i1}, \dots, a_{ik}) \in E$ implies

$$(f(a_{11}, \dots, a_{n1}), \dots, f(a_{1k}, \dots, a_{nk})) \in E.$$

The relation E is an *invariant relation* of a clone C if every $f \in C$ preserves it. Let $\mathrm{Inv}(C)$ denote the set of all invariant relations of the clone C. Conversely, let Σ be a set of relations on A. An operation f on A is called a *polymorphism* of Σ if f preserves every $E \in \Sigma$. Let $\mathrm{Pol}(\Sigma)$ denote the set of all polymorphisms of Σ. It is well known that $C = \mathrm{Pol}(\mathrm{Inv}(C))$ for every clone C on a finite set A.

So, every clone can be described by the set of its invariant relations. However, the set $\mathrm{Inv}(C)$ is, in general, infinite and complicated. To obtain a good description of C, one has to find a small subset $\Sigma \subseteq \mathrm{Inv}(C)$ such that $C = \mathrm{Pol}(\Sigma)$. In our paper, we achieve this aim for every $C \in I(p^3)$ for any prime p.

The description of clones in $I(p^3)$ in [15] is achieved by presenting generating sets of operations. So, the results of the present paper provide an alternative, or complementary, description. Such a description helps to understand the algebraic properties of these clones. It is convenient, for example, for membership testing.

Some of our results have appeared in the master thesis [8].

The elements of $\mathbb{Z}_n$ are denoted by $0, 1, \dots, n-1$. For $n = p^3$, where p is prime, we denote the two special subsets of $\mathbb{Z}_n$ as $M_1 = \{0, 1, \dots, p-1\}$ and $M_2 = \{0, 1, \dots, p^2 - 1\}$. Congruences on the ring $\mathbb{Z}_n$ are the usual congruences modulo d for every $d|n$. For vectors in $(\mathbb{Z}_n)^k$ we adopt the convention that $\mathbf{x} = (x_1, \dots, x_k)$, $\mathbf{l} = (l_1, \dots, l_k)$, etc. If f is an m-ary operation on $\mathbb{Z}_n$, then we use f to denote also the m-ary operation on $(\mathbb{Z}_n)^k$ defined pointwise, that is

$$f(\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(m)})_i = f(x_i^{(1)}, \dots, x_i^{(m)}),$$

where $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(m)} \in \mathbb{Z}_n^k$.

We use [7] as a reference for the commutator theory. If α and β are congruences of an algebra A, then $M(\alpha,\beta)_A$ is the subalgebra of A^4 generated by all 4-tuples of the form (a,a,a',a') with $(a,a')\in\alpha$ and (b,b',b,b') with $(b,b')\in\beta$. The elements of $M(\alpha,\beta)_A$ are usually considered as matrices

$$\begin{pmatrix} a & a \\ a' & a' \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} b & b' \\ b & b' \end{pmatrix},$$

but we find it convenient to write them as row vectors. The *commutator* $[\alpha,\beta]_A$ is defined as the smallest congruence γ of A with the property that $(x_1,x_2,x_3,x_4)\in M(\alpha,\beta)$ and $(x_1,x_2)\in\gamma$ implies $(x_3,x_4)\in\gamma$.

Every clone $C\in I(p^3)$ can be also regarded as an algebra having C as the set of all term operations. The denotations $M(\alpha,\beta)_C$ and $[\alpha,\beta]_C$ refer to this algebra. Notice that all these algebras have the same congruences: trivial congruences 0 and 1, the congruence $\bmod p$ and the congruence $\bmod p^2$. If C is the clone of polynomials of the ring $\mathbb{Z}_{p^3}$, we simply write $M(\alpha,\beta)$ and $[\alpha,\beta]$.

Finally, let us mention an analogous question for the lattice $I(p^2)$. This lattice consists of two elements, namely $\mathrm{P}(\mathbb{Z}_{p^2})$ and $C=\mathrm{Comp}(\mathbb{Z}_{p^2})$. These two clones can be distinguished by the commutator $[\bmod p,\bmod p]$. It is well known that $[\bmod p,\bmod p]=0$ in the ring $\mathbb{Z}_{p^2}$, while $[\bmod p,\bmod p]_C=\bmod p$ (see [6]). Hence, the separating relation is $M(\bmod p,\bmod p)$. The explicit description of this relation is not difficult: (x_1,x_2,x_3,x_4) is in $M(\bmod p,\bmod p)$ if and only if the following conditions are satisfied:

(1) $x_1-x_2-x_3+x_4=0$;
(2) $x_i\equiv x_j \pmod p$ for every $i,j\in\{1,2,3,4\}$.

This fact leads to the characterization of the clone $\mathrm{P}(\mathbb{Z}_{p^2})$ by invariant relations.

Theorem 1.1. *Let f be an operation on $\mathbb{Z}_{p^2}$. The following are equivalent:*

(i) *f is a polynomial operation on the ring $\mathbb{Z}_{p^2}$;*
(ii) *f preserves the congruence modulo p and the relation $M(\bmod p,\bmod p)$.*

2. The lattice $I(p^3)$

The lattice of $I(p^3)$ of clones between $\mathrm{P}(\mathbb{Z}_{p^3})$ and $\mathrm{Comp}(\mathbb{Z}_{p^3})$ has been described in [15]. For a nonpolynomial operation f, by $C(f)$ we denote the clone generated by addition, multiplication, constants and the operation f. Similarly, $C(f,g)$ is the clone generated by addition, multiplication, constants, and operations f and g. We use the following operations.

The i-ary operation ξ_i on $\mathbb{Z}_{p^3}$ $(i \geqslant 2)$ is defined by

$$\xi_i(\mathbf{x}) = \begin{cases} p^2 k_1 k_2 \dots k_i & \text{if } \mathbf{x} = (k_1 p, \dots, k_i p) \text{ for some } k_1, \dots, k_i \in M_2, \\ 0 & \text{otherwise.} \end{cases}$$

The operation π is unary:

$$\pi(x) = \begin{cases} pk^p & \text{if } x = kp \text{ for some } k \in M_2, \\ 0 & \text{otherwise.} \end{cases}$$

The remaining operations ψ, ϱ, τ and φ are binary, they are defined as

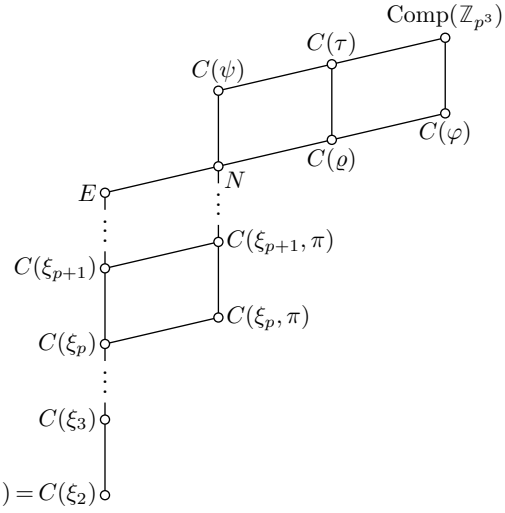
$$\psi(x,y) = \begin{cases} pk^p l^p & \text{if } x = kp,\ y = lp \text{ for some } k, l \in M_2, \\ 0 & \text{otherwise,} \end{cases}$$

$$\varrho(x,y) = \begin{cases} pk^p(l^p - l) & \text{if } x = kp,\ y = lp \text{ for some } k, l \in M_2, \\ 0 & \text{otherwise,} \end{cases}$$

$$\varphi(x,y) = \begin{cases} klp^2 & \text{if } x = kp^2,\ y = lp^2 \text{ for some } k, l \in M_1, \\ 0 & \text{otherwise,} \end{cases}$$

$$\tau(x,y) = \begin{cases} klp & \text{if } x = kp,\ y = lp \text{ for some } k, l \in M_2, \\ 0 & \text{otherwise.} \end{cases}$$

The lattice $I(p^3)$ is depicted below. The clone E is the union of all $C(\xi_i)$ and N is the union of all $C(\xi_i, \pi)$ for $i = 3, 4, \dots$



3. Clones and commutators

As shown in [15], there is a close relationship between clones from $I(p^3)$ and clones on $\mathbb{Z}_{p^2}$ containing the addition. In distinguishing these clones on $\mathbb{Z}_{p^2}$, an important role is played by commutators and relations connected with them (see [6] and [5]). The relations $M(\alpha,\beta)$ considered below have been used in the definition of the commutator and, explicitly or implicitly, in many papers about commutators. Especially, they are behind Bulatov's classification of clones on $\mathbb{Z}_{p^2}$. One can reasonably expect that a similar situation will occur in $I(p^3)$. In our paper we confirm this conjecture. In the sequel, α and β denote the congruences $\bmod p^2$ and $\bmod p$, respectively.

Let the 4-ary relation S be defined by the rule that $(x_1,x_2,x_3,x_4)\in S$ if and only if the following conditions are satisfied:

(S1) $x_1-x_2-x_3+x_4=0$;
(S2) $x_i\equiv x_j \pmod{p^2}$ for every $i,j\in\{1,2,3,4\}$.

Lemma 3.1. $S=M(\alpha,\alpha)$.

Proof. It is easy to see that S, as a subset of the ring $\mathbb{Z}^4_{p^3}$, is closed under addition. Now we show that it is also closed under multiplication. Consider 4-tuples (x_1,x_2,x_3,x_4), (y_1,y_2,y_3,y_4) from S. Since all elements are congruent modulo p^2 and $x_4=x_3+x_2-x_1$, we can express them as $x_2=x_1+a_1p^2$, $y_2=y_1+a_2p^2$, $x_3=x_1+b_1p^2$, $y_3=y_1+b_2p^2$, $x_4=x_1+a_1p^2+b_1p^2$, $y_4=y_1+a_2p^2+b_2p^2$, where $a_1,a_2,b_1,b_2\in M_1$. Then for the 4-tuple $(x_1y_1,x_2y_2,x_3y_3,x_4y_4)$ we have

$$\begin{aligned}x_1y_1-x_2y_2-x_3y_3+x_4y_4 &= x_1y_1-x_1y_1-a_1p^2y_1-a_2p^2x_1-x_1y_1-b_1p^2y_1\\ &\quad -b_2p^2x_1+x_1y_1+a_1p^2y_1+b_1p^2y_1+a_2p^2x_1+b_2p^2x_1\\ &= 0.\end{aligned}$$

So, the 4-tuple $(x_1y_1,x_2y_2,x_3y_3,x_4y_4)$ satisfies (S1). The verification of (S2) is straightforward, hence S is closed under multiplication and therefore it is a subalgebra of $\mathbb{Z}^4_{p^3}$.

The relation $M(\alpha,\alpha)$ is the subalgebra generated by all 4-tuples (a,a,a',a') and (a,a',a,a'), where $(a,a')\in\alpha$. These generators obviously satisfy (S1) and (S2), so $M(\alpha,\alpha)\subseteq S$. To show the reverse inclusion, let $\mathbf{x}=(x_1,x_2,x_3,x_4)\in S$. Hence, $x_2=x_1+ap^2$, $x_3=x_1+bp^2$, $x_4=x_1+ap^2+bp^2$ for some $a,b\in M_1$. It is easy to see that every $\mathbf{x}\in S$ can be expressed by generators of $M(\alpha,\alpha)$ as

$$\mathbf{x}=(x_1,x_1,x_1,x_1)+a(0,p^2,0,p^2)+b(0,0,p^2,p^2).$$

Hence, $\mathbf{x}\in M(\alpha,\alpha)$. □

Lemma 3.2. *The operation τ preserves S.*

P r o o f. Let $\mathbf{x}, \mathbf{y} \in S$. If $\mathbf{x}$ or $\mathbf{y}$ has entries not divisible by p, then $\tau(\mathbf{x}, \mathbf{y}) = (0,0,0,0) \in S$. Let $\mathbf{x} = (k_1p, k_2p, k_3p, k_4p)$, $\mathbf{y} = (l_1p, l_2p, l_3p, l_4p)$, where $k_i, l_i \in M_2$ and $z_i = \tau(k_ip, l_ip)$ for $i = 1,2,3,4$. We need to show that $\mathbf{z} = (z_1, z_2, z_3, z_4) \in S$. It follows from (S2) that $k_2p = k_1p + a_1p^2$, $k_3p = k_1p + b_1p^2$, $l_2p = l_1p + a_2p^2$, $l_3p = l_1p + b_2p^2$, where $a_1, b_1, a_2, b_2 \in M_1$. Since $\mathbf{x}$ and $\mathbf{y}$ satisfy (S1), then

$$k_4p = k_1p + a_1p^2 + b_1p^2, \quad l_4p = l_1p + a_2p^2 + b_2p^2.$$

The condition (S2) holds trivially for $\mathbf{z}$, we check (S1):

$$\begin{aligned} &pk_1l_1 - p(k_1 + a_1p)(l_1 + a_2p) - p(k_1 + b_1p)(l_1 + b_2p) \\ &\quad + p(k_1 + a_1p + b_1p)(l_1 + a_2p + b_2p) \\ &= -k_1a_2p^2 - l_1a_1p^2 - k_1b_2p^2 - l_1b_1p^2 + k_1a_2p^2 + k_1b_2p^2 + l_1a_1p^2 + l_1b_1p^2 = 0. \end{aligned}$$

□

Lemma 3.3. *The operation φ does not preserve S.*

P r o o f. Consider $(0,0,p^2,p^2), (0,p^2,0,p^2)$ from S. After applying φ, we get the 4-tuple $(\varphi(0,0), \varphi(0,p^2), \varphi(p^2,0), \varphi(p^2,p^2)) = (0,0,0,p^2) \notin S$. □

Lemma 3.2 means that $M(\alpha,\alpha)_{C(\tau)} = M(\alpha,\alpha)$. Consequently, $[\alpha,\alpha]_{C(\tau)} = 0$, the same as in the ring $\mathbb{Z}_{p^3}$. On the other hand, the proof of Lemma 3.3 shows that $M(\alpha,\alpha)_{C(\varphi)}$ contains the 4-tuple $(0,0,0,p^2)$, hence $[\alpha,\alpha]_{C(\varphi)} > 0$, which implies $[\alpha,\alpha]_{C(\varphi)} = \alpha$.

The next separating relation is the 4-ary relation T such that $(x_1,x_2,x_3,x_4) \in T$ if and only if the following conditions are satisfied:
(T1) $x_1 - x_2 - x_3 + x_4 = 0$;
(T2) $x_1 \equiv x_3 \pmod{p^2}$;
(T3) $x_i \equiv x_j \pmod{p}$ for every $i, j \in \{1,2,3,4\}$.

Lemma 3.4. $T = M(\alpha,\beta)$.

P r o o f. Clearly, T is closed under addition. To check the multiplication, consider 4-tuples $(x_1,x_2,x_3,x_4), (y_1,y_2,y_3,y_4) \in T$. By (T2), $x_3 - x_1 = ap^2$, $y_3 - y_1 = bp^2$ for some $a, b \in M_1$. By (T1), $x_4 - x_2 = x_3 - x_1 = ap^2$, $y_4 - y_2 = y_3 - y_1 = bp^2$.

To show that $(x_1y_1, x_2y_2, x_3y_3, x_4y_4) \in T$, we compute:

$$\begin{aligned} x_1y_1 - x_2y_2 - x_3y_3 + x_4y_4 &= x_1y_1 - x_2y_2 - (x_1 + ap^2)(y_1 + bp^2) \\ &\quad + (x_2 + ap^2)(y_2 + bp^2) \\ &= bp^2(x_2 - x_1) + ap^2(y_2 - y_1) = 0, \end{aligned}$$

as $x_2 - x_1$ and $y_2 - y_1$ are congruent with 0 modulo p by (T3). This shows that $(x_1y_1, x_2y_2, x_3y_3, x_4y_4)$ satisfies (T1). Further,

$$x_3y_3 - x_1y_1 = (x_3 - x_1)y_3 + x_1(y_3 - y_1) = ap^2y_3 + bp^2x_1 \equiv 0 \pmod{p^2},$$

so (T2) holds.

Next, $x_i \equiv x_j \pmod{p}$ and $y_i \equiv y_j \pmod{p}$ imply $x_iy_i \equiv x_jy_j \pmod{p}$, which shows (T3). Therefore, T is closed under multiplication, too.

The relation $M(\alpha, \beta)$ is the subalgebra generated by all the 4-tuples of the form (a, a, a', a') with $(a, a') \in \alpha$ and (b, b', b, b') with $(b, b') \in \beta$. These generators obviously satisfy (T1), (T2) and (T3), so $M(\alpha, \beta) \subseteq T$. Now, let $(x_1, x_2, x_3, x_4) \in T$. Conditions (T2) and (T3) imply that $x_2 = x_1 + ap$, $x_3 = x_1 + bp^2$ for some $a \in M_2$, $b \in M_1$ and from (T1) we have $x_4 = x_1 + ap + bp^2$. Then

$$\mathbf{x} = (x_1, x_1 + ap, x_1 + bp^2, x_1 + ap + bp^2) = (x_1, x_1, x_1, x_1) + a(0, p, 0, p) + b(0, 0, p^2, p^2).$$

Hence, $T \subseteq M(\alpha, \beta)$. □

Lemma 3.5. *The operation ψ preserves T.*

P r o o f. Let $\mathbf{x} = (x_1, x_2, x_3, x_4)$ and $\mathbf{y} = (y_1, y_2, y_3, y_4)$ belong to T. Let $z_i = \psi(x_i, y_i)$. We need to show that $(z_1, z_2, z_3, z_4) \in T$. We discuss various cases. If x_1 or y_1 is not a multiple of p, then clearly $(z_1, z_2, z_3, z_4) = (0, 0, 0, 0) \in T$. Suppose that $x_1 = kp$, $y_1 = lp$, $k, l \in M_2$. Then $x_3 = kp + ap^2$, $y_3 = lp + bp^2$ for some $a, b \in M_1$. We obtain $z_1 = pk^pl^p$ and $z_3 = p(k + ap)^p(l + bp)^p = pk^pl^p = z_1$.

Since $x_4 - x_2 = x_3 - x_1$ and $y_4 - y_2 = y_3 - y_1$, we have $x_2 \equiv x_4 \pmod{p^2}$ and $y_2 \equiv y_4 \pmod{p^2}$. The same argument as above shows $z_2 = z_4$. The equalities $z_1 = z_3$ and $z_2 = z_4$ clearly imply (T1) and (T2). The fulfillment of (T3) is trivial, hence the proof is complete. □

Lemma 3.6. *The operation ϱ does not preserve the relation T.*

P r o o f. It is easy to check that $(0, p, 0, p), (0, 0, p^2, p^2) \in T$. After applying ϱ, the 4-tuple $(\varrho(0, 0), \varrho(p, 0), \varrho(0, p^2), \varrho(p, p^2)) = (0, 0, 0, -p^2)$ does not belong to T. □

Lemma 3.5 means that $M(\alpha, \beta)_{C(\psi)} = M(\alpha, \beta)$. Consequently, $[\alpha, \beta]_{C(\psi)} = 0$, the same as in the ring $\mathbb{Z}_{p^3}$. On the other hand, the proof of Lemma 3.6 shows that $M(\alpha, \beta)_{C(\varrho)}$ contains the 4-tuple $(0, 0, 0, -p^2)$, hence $[\alpha, \beta]_{C(\varrho)} > 0$, which implies $[\alpha, \beta]_{C(\varrho)} = \alpha$.

Further, we introduce U as the 4-ary relation such that $(x_1, x_2, x_3, x_4) \in U$ if and only if the following conditions are satisfied:

(U1) $x_1 - x_2 - x_3 + x_4 \equiv 0 \pmod{p^2}$;

(U2) $x_i \equiv x_j \pmod{p}$ for every $i, j \in \{1, 2, 3, 4\}$.

(Compare this with the relation $M(\operatorname{mod} p, \operatorname{mod} p)$ in the introduction.)

Lemma 3.7. $U = M(\beta, \beta)$.

P r o o f. It is clear that U is closed under addition. Now we prove that multiplication preserves U. Take $(x_1, x_2, x_3, x_4), (y_1, y_2, y_3, y_4) \in U$ and we show that $(x_1y_1, x_2y_2, x_3y_3, x_4y_4) \in U$. Since all elements are congruent modulo p and $x_4 \equiv x_2 + x_3 - x_1 \pmod{p^2}$, we can express them as $x_2 = x_1 + a_1p$, $y_2 = y_1 + a_2p$, $x_3 = x_1 + b_1p$, $y_3 = y_1 + b_2p$, $x_4 = x_1 + a_1p + b_1p + c_1p^2$, $y_4 = y_1 + a_2p + b_2p + c_2p^2$, where $a_1, a_2, b_1, b_2 \in M_2$, $c_1, c_2 \in M_1$. Then for the 4-tuple $(x_1y_1, x_2y_2, x_3y_3, x_4y_4)$ we have

$$\begin{aligned} x_1y_1 - x_2y_2 - x_3y_3 + x_4y_4 &\equiv x_1y_1 - x_1y_1 - a_1py_1 - a_2px_1 - x_1y_1 - b_1py_1 \\ &\quad - b_2px_1 + x_1y_1 + a_1py_1 + b_1py_1 + a_2px_1 + b_2px_1 \\ &\equiv 0 \pmod{p^2}. \end{aligned}$$

So, the 4-tuple $(x_1y_1, x_2y_2, x_3y_3, x_4y_4)$ satisfies (U1). The verification of (U2) is straightforward, since multiplication is preserved by congruences of $\mathbb{Z}_{p^3}$. Hence U is closed under multiplication and therefore it is a subalgebra of $\mathbb{Z}_{p^3}^4$.

The relation $M(\beta, \beta)$ is the subalgebra generated by all 4-tuples (a, a, a', a') and (a, a', a, a'), where $(a, a') \in \beta$. These generators clearly satisfy (U1) and (U2), so $M(\beta, \beta) \subseteq U$. To show the reverse inclusion, let $\mathbf{x} = (x_1, x_2, x_3, x_4) \in U$. Hence, $x_2 = x_1 + ap$, $x_3 = x_1 + bp$ for some $a, b \in M_2$ and $x_4 = x_1 + ap + bp + cp^2$, where $c \in M_1$. It is easy to see that every $\mathbf{x} \in U$ can be expressed by elements of $M(\beta, \beta)$ in a form

$$\mathbf{x} = (x_1, x_1, x_1, x_1) + a(0, p, 0, p) + b(0, 0, p, p) + c(0, 0, 0, p^2).$$

Recall, that since $M(\beta, \beta)$ is a subalgebra containing $(0, p, 0, p)$ and $(0, 0, p, p)$, it also contains the product $(0, p \cdot 0, 0 \cdot p, p \cdot p)$, so $\mathbf{x} \in M(\beta, \beta)$. □

Lemma 3.8. *The operation φ preserves U.*

P r o o f. Suppose $\mathbf{x}, \mathbf{y} \in U$ and let $z_i = \varphi(x_i, y_i)$ for $i = 1, 2, 3, 4$. Since every z_i is congruent with 0 modulo p^2, the fulfillment of (U1) and (U2) is trivial. □

Lemma 3.9. *The operation ψ does not preserve the relation U.*

P r o o f. It is easy to see that $(0, 0, p, p), (0, p, 0, p)$ are from U. After applying ψ, we get a 4-tuple $(\psi(0, 0), \psi(0, p), \psi(p, 0), \psi(p, p)) = (0, 0, 0, p)$, which does not belong to the relation U. □

Lemma 3.8 implies that $M(\beta,\beta)_{C(\varphi)} = M(\beta,\beta)$. The commutator $[\beta,\beta]_{C(\varphi)}$ equals the congruence α. On the other hand, the subalgebra $M(\beta,\beta)_{C(\psi)}$ contains the 4-tuple $(0,0,0,p)$ (see Lemma 3.9), hence the commutator $[\beta,\beta]_{C(\psi)}$ equals β.

4. Clones and n-ary commutators

The clones between $P(\mathbb{Z}_{p^3})$ and N cannot be distinguished by the commutator considered in the previous section. However, they can be distinguished by n-ary commutators introduced by Bulatov in [5]. The basic properties of higher commutators for congruence permutable varieties have been further developed by Aichinger and Mudrinski in [2].

For an integer $n \geqslant 3$ let P_n be the power set of $\{1,\dots,n\}$. We use P_n for indexing 2^n-ary relations.

Let $\alpha_1,\dots,\alpha_n$ be congruences of an algebra A. Let $M(\alpha_1,\dots,\alpha_n)_A$ be the subalgebra of A^{2^n} generated by all 2^n-tuples $(\mathbf{u}(i,a,a')_J\colon\ J \in P_n)$, where $i \in \{1,\dots,n\}$, $(a,a') \in \alpha_i$ and

$$\mathbf{u}(i,a,a')_J = \begin{cases} a & \text{if } i \in J, \\ a' & \text{if } i \notin J. \end{cases}$$

The n-ary commutator $[\alpha_1,\dots,\alpha_n]_A$ is defined as the smallest congruence on A satisfying for every $\mathbf{x} = (x_J\colon\ J \in P_n) \in M(\alpha_1,\dots,\alpha_n)_A$ the implication

$$(x_J, x_{J\cup\{n\}}) \in \gamma \text{ for every } J \subsetneq \{1,\dots,n-1\} \Rightarrow (x_{\{1,\dots,n-1\}}, x_{\{1,\dots,n\}}) \in \gamma.$$

The relation $M(\alpha_1,\dots,\alpha_n)_A$ has also been investigated by Shaw (see [18]) and Opršal (see [14]), and the idea is implicitly used also in Bulatov [6].

For our purpose we consider the 2^n-ary relation R_n on $\mathbb{Z}_{p^3}$, such that $\mathbf{x} = (x_J\colon J \in P_n) \in R_n$ if and only if the following conditions are satisfied:

(R1) $x_J \equiv x_\emptyset \pmod p$ for every $J \in P_n$;

(R2) $\sum\limits_{K\subseteq J} (-1)^{|K|} x_K \equiv 0 \pmod{p^2}$ for every $J \in P_n$, $|J| \geqslant 2$;

(R3) $\sum\limits_{K\in P_n} (-1)^{|K|} x_K = 0$.

In the sequel we write x_0 and x_j instead of $x_\emptyset$ and $x_{\{j\}}$, respectively. We will see that the relation R_n coincides with $M(\beta,\beta,\dots,\beta)_{C(\xi_{n-1})}$ (n occurences of β). (In distinction from the previous section, the relations $M(\beta,\dots,\beta)$ computed in the ring $\mathbb{Z}_{p^3}$ cannot do the job.)

Lemma 4.1. *Every* $\mathbf{x} = (x_J\colon\ J \in P_n)$ *satisfying* (R2) *satisfies also*

(R4) $x_J - x_0 \equiv \sum\limits_{i\in J} (x_i - x_0) \pmod{p^2}$ *for every* $J \in P_n$.

P r o o f. We proceed by induction on $|J|$. The cases $|J| = 0$ and $|J| = 1$ are trivial. Let $|J| \geqslant 2$ and assume that (R4) holds for all proper subsets of J. We start from the equality

$$\sum_{K \subseteq J} (-1)^{|K|} \Big(x_0 + \sum_{i \in K} (x_i - x_0) \Big) = \sum_{K \subseteq J} (-1)^{|K|} x_0 + \sum_{i \in J} \sum_{i \in K \subseteq J} (-1)^{|K|} (x_i - x_0) = 0,$$

which is due to the fact that exactly one half of subsets of J have an even number of elements. (The same is true when we count subsets containing a fixed $i \in J$.) Using the induction hypothesis we obtain

$$(-1)^{|J|} \Big(x_0 + \sum_{i \in J} (x_i - x_0) \Big) + \sum_{K \subsetneq J} (-1)^{|K|} x_K \equiv 0 \pmod{p^2}.$$

The condition (R2) now implies

$$(-1)^{|J|} \Big(x_0 + \sum_{i \in J} (x_i - x_0) \Big) - (-1)^{|J|} x_J \equiv 0 \pmod{p^2},$$

hence $x_J \equiv x_0 + \sum_{i \in J} (x_i - x_0) \pmod{p^2}$. □

Let $q_{n,m}$ be the polynomial with integer coefficients and variables $t_i^{(k)}$, $i \in \{0, 1, \dots n\}$, $k \in \{1, \dots m\}$, defined as

$$q_{n,m} = \sum_{J \in P_n} (-1)^{|J|} \prod_{k=1}^{m} \Big(t_0^{(k)} + \sum_{i \in J} t_i^{(k)} \Big).$$

Lemma 4.2. *For every $n > m \geqslant 1$, $q_{n,m}$ is a zero polynomial.*

P r o o f. By distributivity, $q_{n,m}$ is the sum of all expressions of the form

$$(-1)^{|J|} t_{j_1}^{(1)} \dots t_{j_m}^{(m)},$$

where $j_1, \dots, j_m \in J \cup \{0\}$. For every m-tuple $(j_1, \dots, j_m)$, there are 2^l sets $J \in P_n$ satisfying $j_1, \dots, j_m \in J \cup \{0\}$, where $l = n - |\{j_1, \dots, j_m\} \setminus \{0\}| \geqslant 1$. Exactly half of these sets have an even number of elements, so the coefficient at $t_{j_1}^{(1)} \dots t_{j_m}^{(m)}$ in $q_{n,m}$ is 0. □

Lemma 4.3. *For every $n \geqslant 3$, the $(n-1)$-ary operation ξ_{n-1} preserves the relation R_n.*

P r o o f. Let $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(n-1)} \in R_n$, $\mathbf{x}^{(k)} = (x_J^{(k)} \colon J \in P_n)$. We need to show that $(y_J \colon J \in P_n) \in R_n$, where $y_J = \xi_{n-1}(x_J^{(1)}, \dots, x_J^{(n-1)})$. The conditions (R1) and (R2) are trivial, since ξ_{n-1} has values congruent with 0 modulo p^2. The equality (R3) is clear when any of $\mathbf{x}^{(k)}$ has entries not divisible by p, because then all y_J are zero. Suppose now that $x_i^{(k)} = pm_i^{(k)}$ for every k and every i. By (R4) we have

$$x_J^{(k)} = pm_0^{(k)} + \sum_{i \in J}(pm_i^{(k)} - pm_0^{(k)}) + p^2 n_J^{(k)}$$

for some $n_J^{(k)} \in M_1$. By the definition of ξ_{n-1},

$$\begin{aligned} y_J = \xi_{n-1}(x_J^{(1)}, \dots, x_J^{(n-1)}) &= p^2 \prod_{k=1}^{n-1} \Big(m_0^{(k)} + pn_J^{(k)} + \sum_{i \in J}(m_i^{(k)} - m_0^{(k)}) \Big) \\ &= p^2 \prod_{k=1}^{n-1} \Big(m_0^{(k)} + \sum_{i \in J}(m_i^{(k)} - m_0^{(k)}) \Big), \end{aligned}$$

hence

$$\sum_{K \in P_n} (-1)^{|K|} y_K = p^2 \sum_{K \in P_n} (-1)^{|K|} \prod_{k=1}^{n-1} \Big(m_0^{(k)} + \sum_{i \in J}(m_i^{(k)} - m_0^{(k)}) \Big).$$

Substituting $m = n-1$, $t_0^{(k)} = m_0^{(k)}$, $t_i^{(k)} = m_i^{(k)} - m_0^{(k)}$ in the polynomial $q_{n,m}$ we obtain

$$\sum_{K \in P_n} (-1)^{|K|} y_K = 0.$$

□

Lemma 4.4. *For every $n \geqslant 3$, the addition, multiplication, and constants preserve the relation R_n.*

P r o o f. The verification for the addition and constants is straightforward. Since $\xi_2(x_1, x_2)$ is equal to $\xi_{n-1}(x_1, x_2, p, \dots, p)$, Lemma 4.3 implies that ξ_2 preserves R_n.

Now, we check the multiplication. Let $\mathbf{x}, \mathbf{y} \in R_n$, let $z_J = x_J \cdot y_J$ for every $J \in P_n$. We show that $\mathbf{z} = (z_J \colon J \in P_n) \in R_n$. If both x_0 and y_0 are divisible by p, then by (R1) the same is true for any x_J and y_J, so $z_J = \xi_2(x_J, y_J)$, and $\mathbf{z} \in R_n$ follows from the fact that ξ_2 preserves R_n. In general, consider $\mathbf{u}$ and $\mathbf{v}$ defined by $u_J = x_J - x_0$, $v_J = y_J - y_0$. Clearly, $\mathbf{u}, \mathbf{v} \in R_n$ and $z_J = x_J \cdot y_J = u_J \cdot v_J + x_0 y_J + y_0 x_J - x_0 y_0$. Hence, $\mathbf{z}$ is the sum of four tuples that belong to R_n, so $\mathbf{z} \in R_n$. □

Lemma 4.5. *If $n > p$, then π preserves R_n.*

P r o o f. Let $\mathbf{x} = (x_J\colon J \in P_n) \in R_n$ and $y_J = \pi(x_J)$. We show that $\mathbf{y} = (y_J\colon J \in P_n)$ belongs to the relation R_n. The condition (R1) holds trivially. If the entries of $\mathbf{x}$ are not multiples of p, then $y_J = 0$ and all conditions are satisfied. Suppose that all $x_J = m_J p$, $m_J \in M_2$ for every J. By the definition of π we have $y_J = pm_J^p$. Since $m_J^p \equiv m_J \pmod p$, we obtain $y_J \equiv x_J \pmod{p^2}$. Hence, the validity of (R2) for $\mathbf{x}$ implies its validity for $\mathbf{y}$.

Simplifying the notation we have $x_i = m_i p$ for $i \in \{0, 1, \dots, n\}$. By Lemma 4.1,

$$x_J = m_0 p + \sum_{i\in J}(m_i p - m_0 p) + n_J p^2$$

for some $n_J \in M_1$. Then

$$y_J = p\biggl(m_0 + \sum_{i\in J}(m_i - m_0) + n_J p\biggr)^p = p\biggl(m_0 + \sum_{i\in J}(m_i - m_0)\biggr)^p.$$

Hence,

$$\sum_{J\in P_n}(-1)^{|J|}y_J = p\sum_{J\in P_n}(-1)^{|J|}\biggl(m_0 + \sum_{i\in J}(m_i - m_0)\biggr)^p.$$

Using Lemma 4.2 with $m = p$, substituting $t_0^{(k)} = m_0$ and $t_i^{(k)} = m_i - m_0$ (for $i > 0$ and every k), we obtain $\sum\limits_{J\in P_n}(-1)^{|J|}y_J = 0$. □

Recall that the 2^n-ary relation $M(\beta, \dots, \beta)_{C(\xi_{n-1})}$ is the subalgebra of $(C(\xi_{n-1}))^{2^n}$ generated by all tuples $\mathbf{u}(i, a, a')$, where $(a, a') \in \beta$ and $i \in \{1, \dots, n\}$, defined by

$$u(i, a, a')_J = \begin{cases} a & \text{if } i \in J, \\ a' & \text{if } i \notin J. \end{cases}$$

Since β is the congruence modulo p, it is easy to see that this subalgebra is in fact generated by all $\mathbf{g}^{(i)} = \mathbf{u}(i, p, 0)$ and the constant 2^n-tuple $\mathbf{1}$.

Lemma 4.6. *$R_n = M(\beta, \dots, \beta)_{C(\xi_{n-1})}$ for every $n \geqslant 3$.*

P r o o f. We have already proved that R_n is a subalgebra of $(C(\xi_{n-1}))^{2^n}$. Clearly, $\mathbf{1} \in R_n$. Let us check that $\mathbf{g}^{(i)} = (g_J^{(i)}\colon J \in P_n) \in R_n$ for every i. The validity of (R1) is trivial. Let $J \in P_n$, $|J| \geqslant 2$. If $i \in J$ then

$$\sum_{K\subseteq J}(-1)^{|K|}g_K^{(i)} = \sum_{i\in K\subseteq J}(-1)^{|K|}p = 0,$$

as exactly half of the subsets of J containing i have an even cardinality. If $i \notin J$, then the above sum equals 0 trivially. This shows both (R2) and (R3). Thus, R_n contains all the generators of $M(\beta, \dots, \beta)_{C(\xi_{n-1})}$.

It remains to prove that $R_n \subseteq M(\beta,\dots,\beta)_{C(\xi_{n-1})}$. Let $\mathbf{x} \in R_n$. By (R1) we have $x_i - x_0 = pm_i$ for some $m_i \in M_2$. By (R2) we have

$$(-1)^{|J|}x_J + \sum_{K\subsetneq J}(-1)^{|K|}x_K \equiv 0 \pmod{p^2}$$

for every J with $2 \leqslant |J| < n$. After multiplying with $(-1)^{|J|}$ we obtain

$$x_J = m_J p^2 - \sum_{K\subsetneq J}(-1)^{|J\setminus K|}x_K$$

for some $m_J \in M_1$. We claim that

$$\mathbf{x} = x_0\cdot\mathbf{1} + \sum_{i=1}^{n} m_i\mathbf{g}^{(i)} + \sum_{k=2}^{n-1}\sum_{|K|=k} m_K\xi_k(\mathbf{g}^{(i)}\colon\ i\in K),$$

which implies $\mathbf{x} \in M(\beta,\dots,\beta)_{C(\xi_{n-1})}$, as all ξ_k with $k \leqslant n-1$ belong to $C(\xi_{n-1})$. For every $J \in P_n$ we have

$$g_J^{(i)} = \begin{cases} p & \text{if } i \in J,\\ 0 & \text{if } i \notin J \end{cases}$$

and (if $|K| = k \geqslant 2$)

$$\xi_k(\mathbf{g}_J^{(i)}\colon\ i\in K) = \begin{cases} p^2 & \text{if } K \subseteq J,\\ 0 & \text{if } K \nsubseteq J. \end{cases}$$

To prove our equality we have to show that

$$x_J = x_0 + \sum_{i\in J} m_i p + \sum_{K\subseteq J,|K|\geqslant 2} m_K p^2$$

for every $J \in P_n$. We proceed by induction on $|J|$. The cases $|J| = 0$ and $|J| = 1$ are trivial, let $|J| \geqslant 2$. By the induction hypothesis,

$$x_J = m_J p^2 - \sum_{K\subsetneq J}(-1)^{|J\setminus K|}\Bigg(x_0 + \sum_{i\in K} m_i p + \sum_{X\subseteq K,|X|\geqslant 2} m_X p^2\Bigg).$$

It is easy to see that, for every $X \subsetneq J$ (including $X = \emptyset$ and $X = \{i\}$),

$$\sum_{K\subsetneq J, X\subseteq K}(-1)^{|J\setminus K|} = -1.$$

Hence,

$$\begin{aligned}
\sum_{K\subsetneq J}(-1)^{|J\setminus K|}x_0 &= -x_0,\\
\sum_{K\subsetneq J}(-1)^{|J\setminus K|}\sum_{i\in K}m_ip &= \sum_{i\in J}\sum_{K\subsetneq J,i\in K}(-1)^{|J\setminus K|}m_ip = -\sum_{i\in J}m_ip,\\
\sum_{K\subsetneq J}(-1)^{|J\setminus K|}\sum_{X\subseteq K,|X|\geqslant 2}m_Xp^2 &= \sum_{X\subseteq J,|X|\geqslant 2}\sum_{K\subsetneq J,X\subseteq K}(-1)^{|J\setminus K|}m_Xp^2\\
&= -\sum_{X\subseteq J,|X|\geqslant 2}m_Xp^2,
\end{aligned}$$

which implies the desired equality. □

Lemma 4.7. *The n-ary operation ξ_n does not preserve the relation R_n.*

P r o o f. Clearly,

$$\xi_n(\mathbf{g}_J^{(1)},\dots,\mathbf{g}_J^{(n)}) = \begin{cases} p^2 & \text{if } J=\{1,\dots,n\},\\ 0 & \text{otherwise.}\end{cases}$$

This 2^n-tuple violates (R3). □

The shape of the relation R_n shows that the n-ary commutator $[\beta,\dots,\beta]_{C(\xi_{n-1})}$ is equal to 0. On the other hand, the 2^n-tuple from the proof of Lemma 4.7 shows that $[\beta,\dots,\beta]_{C(\xi_n)} > 0$.

It is also interesting that the n-ary commutator $[\beta,\dots,\beta]_{C(\xi_m)}$ equals 0 for every $2\leqslant m<n$ despite the fact that the sets $M(\beta,\dots,\beta)_{C(\xi_m)}$ are distinct.

Finally, we need a relation distinguishing clones $C(\xi_n)$ and $C(\xi_n,\pi)$, $p\leqslant n$. These clones cannot be distinguished by commutators. However, we can use another concept from the commutator theory: the similarity of algebras (see [7], Chapter 10).

The rings $\mathbb{Z}_{p^3}$ and $\mathbb{Z}_{p^2}$ are similar. This can be proved using [7], Theorem 10.8 with algebra $C=\beta$ which we now regard as a subring of $\mathbb{Z}_{p^3}\times\mathbb{Z}_{p^3}$. The ring C has ideals

$$\begin{gathered}
I_\varepsilon=\{(x,y)\in C\colon\ y=0\},\quad I_\eta=\{(x,y)\in C\colon\ x\equiv 0\ (\mathrm{mod}\ p^2)\},\\
I_\gamma=\{(p^2k,pk)\colon\ k\in M_2\},\quad I_\delta=\{(0,p^2l)\colon\ l\in M_1\}.
\end{gathered}$$

It is straightforward to check that these sets are indeed ideals of the ring C. They determine congruences on C, which satisfy the conditions of Theorem 10.8 in [7] and hence show the similarity of rings $\mathbb{Z}_{p^3}$ and $\mathbb{Z}_{p^2}$. (We skip the details.) Let

$$Q=\{(x_1,x_2,x_3,x_4)\in\mathbb{Z}_{p^3}^4\colon\ (x_1,x_2),(x_3,x_4)\in C;(x_1,x_2)-(x_3,x_4)\in I_\gamma\}.$$

So, Q can be identified with the congruence on the ring C determined by the ideal I_γ.

Lemma 4.8. *The 4-tuple $(x_1, x_2, x_3, x_4) \in Q$ if and only if the following conditions are satisfied:*

(Q1) $x_1 - px_2 - x_3 + px_4 = 0$;
(Q2) $x_i \equiv x_j \pmod{p}$ *for every* $i, j \in \{1, \dots, 4\}$.

P r o o f. Suppose that $\mathbf{x} = (x_1, x_2, x_3, x_4)$ satisfies (Q1)–(Q2). Then $x_2 - x_4 = pk$ for some $k \in M_2$. From (Q1) we obtain that $x_1 - x_3 = px_2 - px_4 = p^2k$, so $(x_1, x_2) - (x_3, x_4) = (p^2k, pk)$. The condition (Q2) ensures that $(x_1, x_2), (x_3, x_4) \in C$, hence $\mathbf{x} \in Q$.

Conversely, let $(x_1, x_2), (x_3, x_4) \in C$ be such that $x_1 - x_3 = p^2k$, $x_2 - x_4 = pk$ for some $k \in M_2$. Then clearly (Q2) holds, and it is easy to check that $x_1 - px_2 - x_3 + px_4 = 0$, so (Q1) is satisfied too. □

Since Q is a congruence, it is preserved by the addition and multiplication. Obviously, all constant 4-tuples are in Q.

Lemma 4.9. *The operations ξ_n for every $n \in \mathbb{N}$, $n \geqslant 2$, preserve the relation Q.*

P r o o f. Consider 4-tuples $(x_1^{(j)}, x_2^{(j)}, x_3^{(j)}, x_4^{(j)}) \in Q$, where $j \in \{1, \dots, n\}$. Let us put $y_i = \xi_n(x_i^{(1)}, \dots, x_i^{(n)})$, $i \in \{1, 2, 3, 4\}$. We need to show that $(y_1, y_2, y_3, y_4) \in Q$. Since ξ_n can only take values that are congruent with 0 modulo p^2, the condition (Q2) is trivial and (Q1) reduces to the condition $y_1 = y_3$. The only nontrivial case is when $x_1^{(j)} = k_j p$, $k_j \in M_2$ for every j. Then $x_3^{(j)} = k_j p + c_j p^2$ for some $c_j \in M_1$ and hence

$$y_3 = p^2 \prod_{j=1}^{4} (k_j + c_j p) = p^2 \prod_{j=1}^{4} k_j = y_1.$$

□

Lemma 4.10. *The operation π does not preserve Q.*

P r o o f. It is easy to check that $(0, 0, p^2, p) \in Q$ and $(\pi(0), \pi(0), \pi(p^2), \pi(p)) = (0, 0, 0, p)$ does not belong to Q. □

The preservation of Q by the operations ξ_n implies that the algebras $C(\xi_n)$ and $C(\xi_n)/\alpha$ are similar. (Use the same argument as in the case of $\mathbb{Z}_{p^3}$ and $\mathbb{Z}_{p^2}$.)

To sum up the results, for each clone $C \in I(p^3)$ we define the set Σ_C of invariant relations according to the following table.

C	Σ_C
$C(\xi_i), i < p$	congruences, R_{i+1}
$C(\xi_i), i \geqslant p$	congruences, R_{i+1}, Q
E	congruences, Q
$C(\xi_i, \pi), i \geqslant p$	congruences, R_{i+1}
N	congruences, T, U
$C(\psi)$	congruences, T
$C(\varrho)$	congruences, S, U
$C(\tau)$	congruences, S
$C(\varphi)$	congruences, U

Theorem 4.1. *Let C be a clone and f be an operation on $\mathbb{Z}_{p^3}$. The following are equivalent:*

(i) *$f \in C$;*
(ii) *f preserves all relations from Σ_C.*

So, $C = \mathrm{Pol}(\Sigma_C)$.

P r o o f. (i) $\Rightarrow$ (ii) In the above lemmas we have proved that the generators of C preserve all relations from Σ_C. So, every $f \in C$ preserves them, too.

(ii) $\Rightarrow$ (i) Every operation from $C(f)$ preserves all relations from Σ_C. As proved in the above lemmas, every clone $D \in I(p^3)$ with $D \nsubseteq C$ contains an operation which does not preserve a relation from Σ_C. Therefore $C(f) \subseteq C$ and hence $f \in C$. □

In particular, since $\mathrm{P}(\mathbb{Z}_{p^3})$ is the clone of polynomial operations, we have the following result.

Corollary 4.1. *The following are equivalent:*

(i) *f is a polynomial operation on the ring $\mathbb{Z}_{p^3}$;*
(ii) *f preserves congruences, the relation R_3 (and the relation Q, if $p = 2$).*

References

[1] *E. Aichinger, P. Mayr*: Polynomial clones on groups of order *pq*. Acta Math. Hung. *114* (2007), 267–285. zbl MR doi
[2] *E. Aichinger, N. Mudrinski*: Some applications of higher commutators in Mal'cev algebras. Algebra Univers. *63* (2010), 367–403. zbl MR doi
[3] *A. A. Bulatov*: Polynomial reducts of modules I. Rough classification. Mult.-Valued Log. *3* (1998), 135–154. zbl
[4] *A. A. Bulatov*: Polynomial reducts of modules II. Algebras of primitive and nilpotent functions. Mult.-Valued Log. *3* (1998), 173–193. zbl
[5] *A. A. Bulatov*: On the number of finite Mal'tsev algebras. Contributions to General Algebra 13. Johannes Heyn, Klagenfurt, 2001, pp. 41–54. zbl MR

[6] *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. *8* (2002), 193–221. zbl MR doi
[7] *R. Freese, R. McKenzie*: Commutator Theory for Congruence Modular Varieties. London Mathematical Society Lecture Note Series 125. Cambridge University Press, Cambridge, 1987. zbl MR
[8] *C. Gavala*: Compatible Operations on Rings of Integers Modulo n: Master Thesis. Šafárik University Košice, Košice, 2016. (In Slovak.)
[9] *G. P. Gavrilov*: On the superstructure of the class of polynomials in multivalued logics. Discrete Math. Appl. *6* (1996), 405–412; translation from Diskretn. Mat. *8* (1996), 90–97. zbl MR doi
[10] *G. P. Gavrilov*: On the closed classes of multivalued logic containing the polynomial class. Discrete Math. Appl. *7* (1997), 231–242; translation from Diskretn. Mat. *9* (1997), 12–23. zbl MR doi
[11] *P. M. Idziak*: Clones containing Mal'tsev operations. Int. J. Algebra Comput. *9* (1999), 213–226. zbl MR doi
[12] *P. Mayr*: Polynomial clones on squarefree groups. Int. J. Algebra Comput. *18* (2008), 759–777. zbl MR doi
[13] *D. G. Meshchaninov*: Superstructures of the class of polynomials in P_k. Math. Notes *44* (1988), 850–854; translation from Mat. Zametki *44* (1988), 673–681. zbl MR doi
[14] *J. Opršal*: A relational description of higher commutators in Mal'cev varieties. Algebra Univers. *76* (2016), 367–383. zbl MR doi
[15] *M. Ploščica, I. Varga*: Clones of compatible operations on rings $\mathbb{Z}_{p^k}$. J. Mult.-Val. Log. Soft Comput. *36* (2021), 391–404. zbl
[16] *A. B. Remizov*: Superstructure of the closed class of polynomials modulo k. Discrete Math. Appl. *1* (1991), 9–22; translation from Diskretn. Mat. *1* (1989), 3–15. zbl MR doi
[17] *A. Salomaa*: On infinitely generated sets of operations in finite algebras. Ann. Univ. Turku., Ser. A I *74* (1964), 13 pages. zbl MR
[18] *J. Shaw*: Commutator relations and the clones of finite groups. Algebra Univers. *72* (2014), 29–52. zbl MR doi
[19] *Á. Szendrei*: Idempotent reducts of abelian groups. Acta Sci. Math. *38* (1976), 171–182. zbl MR
[20] *Á. Szendrei*: Clones of linear operations on finite sets. Finite Algebra and Multiple-Valued Logic. Colloquia Mathematica Societatis János Bolyai 28. North-Holland, Amsterdam, 1981, pp. 693–738. zbl MR

Authors' address: *Cyril Gavala*, *Miroslav Ploščica*, *Ivana Varga* (corresponding author), Šafárik University, Faculty of Science, Institute of Mathematics, Jesenná 5, 04154 Košice, Slovakia e-mail: `cyril.gavala@student.upjs.sk`, `miroslav.ploscica@upjs.sk`, `ivana.varga@student.upjs.sk`.