Michigan Math. J. 64 (2015), 109–142

Cycles of Polynomial Mappings in Several Variables over Discrete Valuation Rings and over Z

T. Pezda

Abstract. We find all possible cycle lengths of polynomial mappings in several variables over unramified discrete valuation domains. As a consequence, we determine the sets of all cycle lengths in R^N (where $N \geq 2$) for some Dedekind rings R. Finding these sets for $R = Z$ and any N is the main purpose of this paper.

1. Introduction

For a commutative ring R with unity and $\Phi = (\Phi_1, \ldots, \Phi_N)$, where $\Phi_i \in R[X_1, \ldots, X_N]$, we define a *cycle* for Φ as a k-tuple $\bar{x}_0, \bar{x}_1, \ldots, \bar{x}_{k-1}$ of different elements of R^N such that

$$\Phi(\bar{x}_0) = \bar{x}_1, \qquad \Phi(\bar{x}_1) = \bar{x}_2, \qquad \ldots, \qquad \Phi(\bar{x}_{k-1}) = \bar{x}_0.$$

The number k is called the *length* of this cycle.

Let $\mathcal{CYCL}(R, N)$ be the set of all possible cycle lengths for polynomial mappings in N variables with coefficients from R (we clearly assume that the elements of the considered cycles lie in R^N).

The main motivation to write this paper is finding $\mathcal{CYCL}(Z, N)$ for all natural N. As an exercise, one may treat the equality $\mathcal{CYCL}(Z, 1) = \{1, 2\}$. In [Pe2], the formula $\mathcal{CYCL}(Z, 2) = \{24, 18, 16, \text{and divisors}\}$ was established. In [Pe5], it was shown that the biggest element in $\mathcal{CYCL}(Z, N)$ equals $2 \cdot 4^N + o(4^N)$.

One of the main ingredients in obtaining these results is a local-to-global principle for polynomial cycles (see Section 2.4). This principle for $N \geq 2$ gives an expression of $\mathcal{CYCL}(R, N)$ in terms of $\mathcal{CYCL}(R_{\mathfrak{p}}, N)$, where $\mathfrak{p}$ runs over the family of all nonzero prime ideals of a Dedekind domain R.

Thus, in order to determine $\mathcal{CYCL}(Z, N)$, it is enough to determine $\mathcal{CYCL}(Z_p, N)$ for all prime p, where Z_p denotes the ring of p-adic numbers. In fact (see Theorem 2), it suffices to determine $\mathcal{CYCL}(Z_2, N)$ and $\mathcal{CYCL}(Z_3, N)$.

Using the notation of Theorem 1 and Section 2.1, we see that Z_p is a discrete valuation ring (DVR) of characteristic zero satisfying $e = 1$ (and therefore unramified). For the rings Z_p, the number f equals 1.

The main result of this paper is the following:

Received January 7, 2014. Revision received August 2, 2014.
This work is supported by the MNiSW grant N N201 366636.

THEOREM 1. *Let R be a discrete valuation ring of characteristic* 0, *and assume that P is the unique maximal ideal of R. We assume that the field R/P is finite and has p^f elements (p prime). Let w be the exponent of R. We assume that the ramification index $e = w(p)$ is equal to* 1; *in other words, R is unramified. Then $\mathcal{CYCL}(R, N)$ consists of all natural numbers of the form*

$$c \cdot k \cdot p^{\alpha},$$

where $1 \le c \le p^{fN}$, $k | [p^{fa_1} - 1, \dots, p^{fa_r} - 1]$ for some positive $a_1, \dots, a_r$: $a_1 + \cdots + a_r \le N$, and if (for $k > 1$) a is the smallest sum $a_1 + \cdots + a_r$ such that $k | [p^{fa_1} - 1, \dots, p^{fa_r} - 1]$ (and $a = 0$ for $k = 1$), then

(i) *for $p \ge 3$, we have $\alpha \le \max\{0, \log_p(\frac{2(N-a)}{p-1} p)\}$;*
(ii) *for $p = 2$, we have*

$$\alpha < 2 + \log_2(N - a) \text{ for } a \le N - 2,$$
$$\alpha \le 2 \text{ for } 1 \le a = N - 1,$$
$$\alpha \le 1 \text{ for all other possibilities, that is, } a = N \text{ or } N = 1.$$

Theorem 1 generalizes a result from [Pe1] and [Zie], where it was obtained that $\mathcal{CYCL}(Z_p, 1) = \{a \cdot b\colon\ 1 \le a \le p, b | p - 1\}$ for $p \ge 5$, $\mathcal{CYCL}(Z_3, 1) = \{1, 2, 3, 4, 6, 9\}$, and $\mathcal{CYCL}(Z_2, 1) = \{1, 2, 4\}$.

As a consequence of Theorem 1, we obtain the following:

THEOREM 2. *Let S be a Dedekind domain of characteristic* 0 *such that there are prime ideals $\mathfrak{p}$ of S with $S/\mathfrak{p}$ finite. Let $m = \min_{\mathfrak{p}\text{-prime}} \#(S/\mathfrak{p})$. Assume that for all prime ideals of S having norms smaller than m^2, the corresponding localizations $S_{\mathfrak{p}}$ are unramified. Then for $N \ge 2$, the set $\mathcal{CYCL}(S, N)$ is completely determined. Namely, for $N \ge 2$, we have*

$$\mathcal{CYCL}(S, N) = \bigcap_{\substack{\mathfrak{p}\text{-prime} \\ \#(S/\mathfrak{p}) < m^2}} \mathcal{CYCL}(S_{\mathfrak{p}}, N).$$

In particular, $\mathcal{CYCL}(Z, N)$ is completely determined and equals $\mathcal{CYCL}(Z_2, N) \cap \mathcal{CYCL}(Z_3, N)$ (for $N \ge 2$).

EXAMPLE 1. By Theorems 1 and 2 we have $\mathcal{CYCL}(Z, 3) = \mathcal{CYCL}(Z_2, 3) \cap \mathcal{CYCL}(Z_3, 3) = \{112, 98, 96, 84, 72, 70, 64, 60, 40, \text{and divisors}\} \cap \{702, 676, 650, 648, 624, 600, 598, 576, 572, 552, 546, 528, 520, 504, 494, 480, 468, 456, 442, 432, 416, 408, 390, 384, 364, 360, 336, 243, 225, 207, 198, 189, 171, 153, 135, \text{and their divisors}\} = \{112, 96, 84, 72, 64, 60, 40, \text{and their divisors}\}$.

Let Z_K be the ring of algebraic integers lying in a finite extension K of the rationals. It is known that if $(Z_K)_{\mathfrak{p}}$ are unramified DVR for all nonzero prime ideals $\mathfrak{p}$, then $K = Q$. So, from the formal point of view, the local-to-global principle and Theorem 1 determine $\mathcal{CYCL}(Z_K, N)$ for all $N \ge 2$ only for $K = Q$ (in this case, $Z_Q = Z$). However, owing to Theorem 2, the sets $\mathcal{CYCL}(Z_K, N)$ may be determined also for some $K \ne Q$ and some $N \ge 2$.

EXAMPLE 2. Let $L = Q(\sqrt{d})$ with square-free d satisfying $d \equiv 5 \pmod 8$, $d \equiv 1 \pmod 3$, $d \equiv 2 \pmod 5$, $d \equiv 2 \pmod 7$ (for example, $d = 37$).

Then $\mathfrak{p}_2 = 2Z_L$ is prime with norm 4, $3Z_L = \mathfrak{p}_3\mathfrak{p}_3'$ with different prime $\mathfrak{p}_3$ and $\mathfrak{p}_3'$, $\mathfrak{p}_5 = 5Z_L$ is prime with norm 25, $7Z_L = \mathfrak{p}_7\mathfrak{p}_7'$ with different prime $\mathfrak{p}_7$ and $\mathfrak{p}_7'$.

We then obtain that

$(Z_L)_{\mathfrak{p}_2}$ is a discrete valuation ring corresponding to $p = 2$, $f = 2$, $e = 1$;
$(Z_L)_{\mathfrak{p}_3} \cong (Z_L)_{\mathfrak{p}_3'}$ are discrete valuation rings corresponding to $p = 3$, $f = 1$, $e = 1$;
$(Z_L)_{\mathfrak{p}_5}$ is a discrete valuation ring corresponding to $p = 5$, $f = 2$, $e = 1$; and
$(Z_L)_{\mathfrak{p}_7} \cong (Z_L)_{\mathfrak{p}_7'}$ are discrete valuation rings corresponding to $p = 7$, $f = 1$, $e = 1$.

Note that $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_3'$, $\mathfrak{p}_7$, $\mathfrak{p}_7'$ are the only prime ideals of Z_L with norm smaller than $m^2 = 3^2 = 9$. Since $\widehat{(Z_L)_{\mathfrak{p}_3}} \cong Z_3$, $\widehat{(Z_L)_{\mathfrak{p}_7}} \cong Z_7$, by Theorem 2 we obtain, for $N \geq 2$,

$$\mathcal{CYCL}(Z_L, N) = \mathcal{CYCL}((Z_L)_{\mathfrak{p}_2}, N) \cap \mathcal{CYCL}(Z_3, N) \cap \mathcal{CYCL}(Z_7, N).$$

One may check that $\mathcal{CYCL}(Z_3, 3) \subset \mathcal{CYCL}(Z_7, 3)$, and we obtain $\mathcal{CYCL}(Z_{Q(\sqrt{37})}, 3) = \mathcal{CYCL}((Z_{Q(\sqrt{37})})_{\mathfrak{p}_2}, 3) \cap \mathcal{CYCL}(Z_3, 3) = \{702, 648, 624, 600, 576, 552, 546, 528, 520, 504, 480, 468, 456, 432, 416, 408, 390, 384, 364, 360, 336, 243, 225, 207, 198, 189, 171, 153, 135, \text{and their divisors}\}$.

From the proof of Theorem 2 (using the notation from Theorem 2) we have that, for $N \geq 2$,

$$\mathcal{CYCL}(S, N) = \bigcap_{\substack{\mathfrak{p}\text{-prime} \\ \#(S/\mathfrak{p}) < m^2}} \mathcal{CYCL}(S_{\mathfrak{p}}, N)$$

if $S_{\mathfrak{p}}$ is unramified for some $\mathfrak{p}$ such that $\#(S/\mathfrak{p}) = m$.

Theorem 1 determines $\mathcal{CYCL}(R, N)$ for unramified (i.e., satisfying $e = 1$) DVR of characteristic zero. It seems that finding a closed formula for all ramification indices e is difficult, if not impossible. It is worth emphasizing that a possible formula for $\mathcal{CYCL}(R, N)$ would not depend solely on p, e, f, N. For example, by Proposition 3.5 from [Pe4] it follows that $48 \notin \mathcal{CYCL}(R, 2)$ for R such that $p = 2$, $f = 1$, $e = 2$, $\pi^2 \equiv 2 \pmod{P^4}$, whereas $48 \in \mathcal{CYCL}(R, 2)$ for R such that $p = 2$, $f = 1$, $e = 2$, $\pi^2 + \pi^3 \equiv 2 \pmod{P^4}$. The element π is precisely defined in Section 2.1.

In [Pe4], we managed to gain enough knowledge of $\mathcal{CYCL}(R, 2)$ for some DVR R satisfying $ef \leq 2$ and $p \leq 7$ to determine $\mathcal{CYCL}(Z_K, 2)$ for $[K : Q] = 2$ (there are 14 such sets possible).

Estimates for cycle lengths in DVR R for polynomials, morphisms, and power series may be found in [Zie; Pe3; MorSil].

The local-to-global principle is not valid for $N = 1$. In this case, we have only the inclusion $\mathcal{CYCL}(R, 1) \subset \bigcap_{\mathfrak{p}} \mathcal{CYCL}(R_{\mathfrak{p}}, 1)$ for any integral domain R. This sometimes significantly reduces the number of possible elements of $\mathcal{CYCL}(R, 1)$,

and the remaining possibilities are treated by other methods, mainly by unit equations. Such an approach was used to find $\mathcal{CYCL}(Z_K, 1)$ for $[K: \ Q] = 3$ with negative discriminant in [Na2] and for K of signature $(0, 2)$ in [Pe6] (the sets $\mathcal{CYCL}(Z_K, 1)$ for quadratic K were determined in [Bo] and [Ba]), and in [Na1], where $\mathcal{CYCL}(Z[\frac{1}{p}], 1)$ and $\mathcal{CYCL}(Z[\frac{1}{2p}], 1)$ for prime p were found (the fact that $\mathcal{CYCL}(R, N)$ is finite for any finitely generated integral domain of characteristic zero was emphasized in [H-KNa]).

Recently (see [Pe7]), we managed to find a finitary procedure to find $\mathcal{CYCL}(Z_K, 1)$, working for any algebraic number field K.

For various aspects concerning polynomial cycles and precycles, we refer to [Ben; Can; FPS; NaPe; Erk; Mor].

1.1. A Sketch of the Proof

In Section 2.1, we may find the basic definitions and (in Lemma 2.1) some simple properties of polynomial mappings in DVR. In Proposition 2.1, we collect some useful results from earlier papers. Proposition 2.1(v) is of special importance since it connects the length of a cycle with the characteristic polynomial of some derivative.

In Section 2.2, we collect some identities concerning binomial coefficients.

Lemma 2.4 is very useful since it frequently allows us to restrict our attention to maps Φ whose derivative at $\bar{0}$ is of a very particular form.

For a local domain R (with a maximal ideal P), a cycle $\bar{x}_0, \bar{x}_1, \ldots$ in R^N is called a $(\star)$-cycle if $\bar{x}_i - \bar{x}_j \in P^N$ for all i, j. In the rest of the proof, we consider $(\star)$-cycles starting from $\bar{0}$, which, according to Proposition 2.1(i) and Lemma 2.1(i), does not restrict the problem we consider.

In view of Proposition 2.1(v)–(vi), the p-free parts of elements from $\mathcal{CYCL}\star(R, N)$ (defined in an obvious way) constitute the set of all divisors of the elements $[p^{fa_1} - 1, \ldots, p^{fa_r} - 1]$ with $a_1 + \cdots + a_r \le N$. So, the problem of finding $\mathcal{CYCL}(R, N)$ for DVR R is equivalent to the following one:

> Let k divide $[p^{fa_1} - 1, \ldots, p^{fa_r} - 1]$ for some $a_1 + \cdots + a_r \le N$.
>
> Find all α such that $k \cdot p^\alpha \in \mathcal{CYCL}\star(R, N)$.

In Section 3, we examine $(\star)$-cycles of length p^α for mappings Φ such that $A := (\Phi)'(\bar{0})$ satisfies $A(A - I)^M \equiv 0 \pmod{P}$ for some M. This assumption on A seems to be very restrictive, but according to the beginning of Section 5, it is not.

In the very important Propositions 3.1 and 3.2, we obtain the estimate $M \ge p^{\alpha-1}\frac{p-1}{2}$. In Proposition 3.1, we consider the case $w(\bar{x}_{p^{\alpha-1}}) \ge 2$ and, in Proposition 3.2, the case $w(\bar{x}_{p^{\alpha-1}}) = 1$. These two cases require quite different proofs. In addition, in these propositions we give conditions when $M = p^{\alpha-1}\frac{p-1}{2}$ may take place. Here, we notice the distinction between the cases $p = 2$ and $p > 2$.

In Section 4, in Proposition 4.1 (for $p \ge 3$) and Proposition 4.2 (for $p = 2$), we give key examples of $(\star)$-cycles of length p^α in R^N for $N \ge p^{\alpha-1}\frac{p-1}{2}$ (for $p \ge 3$) and $N > 2^{\alpha-2}$ (for $p = 2$). Since we search for $(\star)$-cycles of length p^α,

we should have $(\Phi^{p^\alpha})(\bar{0}) = \bar{0}$ and $(\Phi^{p^{\alpha-1}})(\bar{0}) \neq \bar{0}$ (and this is a necessary and sufficient condition).

In Propositions 4.1 and 4.2, the mapping Φ is defined with the use of N unspecified coefficients r_i, a_j (in Proposition 4.1), and r_i (in Proposition 4.2). Since we are not able to avoid using terms of degree ≥ 2, the calculation of suitable iterations is very tedious. Fortunately, for the proof of these propositions, it is sufficient to calculate everything (mod P^4). One of the required conditions, $(\Phi^{p^{\alpha-1}})(\bar{0}) \neq \bar{0}$, is satisfied independently of the choice of r_i, a_j (we point out a suitable coordinate of $(\Phi^{p^{\alpha-1}})(\bar{0})$, which certainly is not equal to 0).

In Lemmas 4.1 and 4.2, we, roughly speaking, calculate $(\Phi^{p^\alpha})(\bar{0})$ (mod P^4). After division by suitable powers of p, we see that the condition $(\Phi^{p^\alpha})(\bar{0}) = \bar{0}$ is equivalent to a system of N equations in N variables in R. The existence of a solution of this system follows from the N-dimensional generalization of Hensel's lemma (a proof of that generalization is very similar to the proof of the basic version of Hensel's lemma from the theory of p-adic numbers).

We finish Section 4 with the Proposition 4.3, which gives the existence part of Theorem 1. In the proof of Proposition 4.3, we introduce a simple construction, which for cycles of length k in R^m for Φ and of length l in R^n for Ψ gives a cycle of length $[k, l]$ for (Φ, Ψ) in $R^m \times R^n = R^{m+n}$. Owing to this construction and propositions from Section 4, we prove Proposition 4.3 with the exception of $(\star)$-cycles of lengths $4[2^{fa_1} - 1, \ldots, 2^{fa_r} - 1]$ for $1 \leq a \leq N - 1$, which require an additional construction.

In Section 5, we consider $(\star)$-cycles of length kp^α for a mapping Φ. Denote $C := \Phi'(\bar{0})$ and write the characteristic polynomial of the matrix $B := C$ (mod P) as $(-1)^N X^{a_0}(X-1)^{b_0} F_1(X)^{b_1} \cdot \ldots \cdot F_r(X)^{b_r}$, where F_i are irreducible and monic, and the degree of F_i is a_i. Using Proposition 2.1(v), we get $k | [p^{fa_1} - 1, \ldots, p^{fa_r} - 1]$. We take a suitably chosen iteration Ψ of Φ and notice that Ψ has a $(\star)$-cycle of length p^α. A linear mapping $A := (\Psi)'(\bar{0})$ satisfies $A(A-I)^{\max\{b_0, b_1, \ldots, b_r\}} \equiv 0$ (mod P). For a given k dividing some $[p^{fa_1} - 1, \ldots, p^{fa_r} - 1]$, we therefore, using the results from Section 3, obtain in Lemma 5.1 an estimate for α in terms of p, M, where M is the smallest b such that $A(A-I)^b \equiv 0$ (mod P).

The purpose of Lemma 5.2 is to find all tuples $k, N, a, M, r, a_0, b_0, \ldots, r, b_r$, p, α such that the estimate from Lemma 5.1 is weaker than the estimate from Theorem 1. All such tuples are threatening the validity of Theorem 1. The "threatening" tuples from Lemma 5.2 are then discarded in Proposition 5.1.

2. Auxiliary Results

Let $\bar{0} = (0, 0, \ldots, 0)$, and let I denote the unit matrix. We sometimes use the symbol $\delta_{i \geq k}$, which equals 1 if $i \geq k$ and 0 otherwise. Let $\bar{e}_i$ be the ith vector from the canonical basis, that is, it has 1 at the ith coordinate and 0 otherwise. The ith coordinate of a vector $\bar{u}$ is denoted by $(\bar{u})_i$.

2.1. Cycles in Some Discrete Valuation Domains

Throughout, R is a discrete valuation domain of characteristic zero, and P is the unique maximal ideal of R. We assume that the quotient field $K = R/P$ is finite and has p^f elements (p-prime). Let π be a generator of the principal ideal P, and let v be the norm of R normalized so that $v(\pi) = \frac{1}{p}$. We denote by w the corresponding exponent defined by $w(x) = -\frac{\log v(x)}{\log p}$ for $x \neq 0$ and $w(0) = \infty$.

We put $e := w(p)$. Thus, e is the ramification index of R. We extend w to R^N by putting $w(x_1, \ldots, x_N) = \min\{w(x_1), \ldots, w(x_N)\}$.

The congruence symbol $\bar{x} \equiv \bar{y} \pmod{P^d}$ will be used for vectors $\bar{x}, \bar{y} \in R^N$ to indicate that their corresponding components are congruent (mod P^d) or, equivalently, $w(\bar{x} - \bar{y}) \geq d$. We use a similar convention for matrices.

A polynomial cycle $\bar{x}_0, \bar{x}_1, \ldots, \bar{x}_{k-1}$ is called a (polynomial) ($\star$)-cycle if $w(\bar{x}_i - \bar{x}_j) \geq 1$ for all i, j. Let $\mathcal{CYCL}\star(R, N)$ be the set of all possible lengths of ($\star$)-cycles for polynomial mappings in N variables with coefficients from R.

If Φ is a polynomial mapping in N variables with coefficients from R, then $\Phi'(\bar{x})$ denotes the Jacobian matrix of Φ at $\bar{x}$.

LEMMA 2.1. *Let $R, P, \ldots$ be as before. Then*

(i) *if in R^N there is a ($\star$)-cycle of length k, then in R^N there is a ($\star$)-cycle of the form $\bar{0} = \bar{x}_0, \bar{x}_1, \ldots, \bar{x}_{k-1}$;*

(ii) *let $\Phi : R^N \to R^N$ be a polynomial mapping with coefficients from R. Let $\Phi(\bar{0}) = \bar{x} \neq 0$ and $w(\bar{x}) = d > 0$. Put $\Phi'(\bar{0}) = A$. Then for every positive integer l, we have $\Phi^l(\bar{0}) \equiv (A^{l-1} + A^{l-2} + \cdots + A + I)\bar{x} \equiv ((A - I)^{l-1} + \binom{l}{1}(A - I)^{l-2} + \cdots + \binom{l}{l-2}(A - I) + lI)\bar{x} \pmod{P^{2d}}$;*

(iii) *let $\Phi : R^N \to R^N$ be a polynomial mapping with coefficients from R, $w(\Phi(\bar{0})) = d$. Then $(\Phi^r)'(\bar{0}) \equiv (\Phi'(\bar{0}))^r \pmod{P^d}$ holds for every positive integer r;*

(iv) *let A be a linear mapping of R^N with coefficients from R. Let ω be a nonnegative integer or ∞ (we put $P^\infty = (0)$). Let $W_1(X), W_2(X) \in Z[X]$; $\bar{u} \in R^N$. Assume that $W(X) \in (W_1(X), W_2(X))$ or (in case of $\omega = \infty$) that $W(X)$ is any gcd of $W_1(X), W_2(X)$ in $Q[X]$.*

If $W_1(A)\bar{u} \equiv W_2(A)\bar{u} \equiv \bar{0} \pmod{P^\omega}$, then $W(A)\bar{u} \equiv \bar{0} \pmod{P^\omega}$.

In particular, let b, c, d be nonnegative integers. Then $A(A - I)^b\bar{u} \equiv \bar{0} \pmod{P^d}$, $(A - I)^c\bar{u} \equiv \bar{0} \pmod{P^d}$ implies $(A - I)^{\min\{b,c\}}\bar{u} \equiv \bar{0} \pmod{P^d}$.

Proof. (i) This is a special case of Lemma 4.1(i) from [Pe3].

(ii) The congruence $\Phi^l(\bar{0}) \equiv (A^{l-1} + A^{l-2} + \cdots + A + I)\bar{x} \pmod{P^{2d}}$ is given in Lemma 4.6 from [Pe3]. The rest follows from the identity $\sum_{i=0}^{l-1} x^i = \sum_{i=0}^{l-1} \binom{l}{i}(x - 1)^{l-1-i}$.

(iii) Clearly, $\bar{z} \equiv \bar{y} \pmod{P^d}$ implies $\Phi'(\bar{z}) \equiv \Phi'(\bar{y}) \pmod{P^d}$ and $\Phi(\bar{z}) \equiv \Phi(\bar{y}) \pmod{P^d}$. Hence, $\Phi^{r-1}(\bar{0}) \equiv \Phi^{r-2}(\bar{0}) \equiv \cdots \equiv \Phi(\bar{0}) \equiv \bar{0} \pmod{P^d}$ and $(\Phi^r)'(\bar{0}) = \Phi'(\Phi^{r-1}(\bar{0})) \circ \cdots \circ \Phi'(\Phi(\bar{0})) \circ \Phi'(\bar{0}) \equiv (\Phi'(\bar{0}))^r \pmod{P^d}$.

(iv) Let ω be an integer. There are polynomials $F_1(X), F_2(X) \in Z[X]$ such that $W(X) = F_1(X)W_1(X) + F_2(X)W_2(X)$. Hence, $W(A)\bar{u} = F_1(A)W_1(A)\bar{u} + F_2(A)W_2(A)\bar{u} \equiv \bar{0} \pmod{P^\omega}$.

The proof for $\omega = \infty$ requires only minor changes. □

In the following proposition, we collect some useful facts about cycles in discrete valuation rings.

PROPOSITION 2.1. *Let $R, P, p, f, v, \ldots$ be as before. Then*

(i) *a number k lies in $\mathcal{CYCL}(R, N)$ if and only if $k = ab$, where $a \le p^{fN}$, and b is the length of a suitable $(\star)$-cycle in R^N. In particular, $\{1, 2, \ldots, p^{fN}\} \subset \mathcal{CYCL}(R, N)$;*

(ii) *if $\hat{R}$ is the completion of R with respect to the norm v, then*

$$\mathcal{CYCL}(R, N) = \mathcal{CYCL}(\hat{R}, N) \quad \text{and} \quad \mathcal{CYCL}^\star(R, N) = \mathcal{CYCL}^\star(\hat{R}, N)$$

(note that for $\hat{R}$, the numbers p, e, f are the same as for R);

(iii) *for every $1 \le r \le N$, we have $p^{fr} - 1 \in \mathcal{CYCL}^\star(R, N)$;*

(iv) *if, in addition, R is complete, then in R^N there is a $(\star)$-cycle $\bar{x}_0, \bar{x}_1, \ldots$ of length $p^{fN} - 1$, having all coordinates of all $\bar{x}_i$ in P, for a linear mapping A having different eigenvalues and whose eigenvalues are primitive roots of unity of order $p^{fN} - 1$;*

(v) *let $\bar{0} = \bar{x}_0, \bar{x}_1, \ldots, \bar{x}_{m-1}$ be a $(\star)$-cycle for a (polynomial) mapping Φ in N variables with coefficients from R. Put $\Phi'(\bar{0}) := A$. Write the characteristic polynomial $F(X) \in K[X]$ (recall that $K = R/P$) of the matrix $B = A \pmod{P}$ as $(-1)^N X^{a_0}(X-1)^{b_0} F_1(X)^{b_1} \cdot \ldots \cdot F_r(X)^{b_r}$, where $a_0, b_0 \ge 0$, $F_1, \ldots, F_r$ are pairwise different, monic, and irreducible polynomials $\ne X, X-1$ in $K[X]$, and $b_1, \ldots, b_r > 0$. Put $a_i := \deg F_i$ for $1 \le i \le r$. Hence, $a_1 + a_2 + \cdots + a_r \le a_0 + b_0 + a_1 b_1 + \cdots + a_r b_r = N$. Write $m = kp^\alpha$, where $\alpha \ge 0$ and p does not divide k. Hence, $k = 1$ for $r = 0$, and k divides $[p^{fa_1} - 1, \ldots, p^{fa_r} - 1]$ $(= lcm\ (p^{fa_1} - 1, \ldots, p^{fa_r} - 1))$ for $r > 0$;*

(vi) *let m be a positive integer not divisible by p. Then there is a $(\star)$-cycle of length m in R^N if and only if there are $r > 0$ and positive integers $a_1, \ldots, a_r$ with $a_1 + \cdots + a_r \le N$ such that m divides $[p^{fa_1} - 1, \ldots, p^{fa_r} - 1]$;*

(vii) *assume, in addition, that $e = 1$ and $p = 2$. Then the lengths of $(\star)$-cycles in R^N are bounded by $2(2^{fN} - 1)$.*

Proof. (i) The first part is Lemma 4.4 in [Pe3]. Since $\bar{0}$ is a $(\star)$-cycle for the zero mapping, we have $\{1, 2, \ldots, p^{fN}\} \subset \mathcal{CYCL}(R, N)$.

(ii) This is Proposition 4.1 in [Pe3].

(iii) This is Theorem 3.1(iii) in [Pe3].

(iv) It follows from the proof of Theorem 3.1(iii) in [Pe3]. Namely, the statement is clear for $p^{fN} - 1 = 1$. For $p^{fN} - 1 > 1$, we consider an element ξ that is a primitive root of unity of order $p^{fN} - 1$ and a root of an irreducible polynomial $F \in R[X]$ of degree N. Each root of F is also a primitive root of unity of order $p^{fN} - 1$.

Let $\Lambda : R[\xi] \to R[\xi]$ be the multiplication by ξ. One sees that the eigenvalues of Λ, treated as a linear mapping over R, are exactly the roots of F. To finish the proof, notice that $R[\xi]$ is, as an R-module, naturally isomorphic to R^N, and to Λ there corresponds a linear mapping of R^N with the same eigenvalues.

(v), (vi) This is Proposition 3.1 in [Pe5].

(vii) This is Proposition 3.2(ii) in [Pe5]. □

2.2. *Some Facts Concerning Binomial Coefficients*

LEMMA 2.2. *Let p be prime.*

(i) *For $n, k \geq 0$, the number $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is not divisible by p if and only if all the digits in the expansion of n in the base p are not smaller than the corresponding digits for k;*

(ii) *for $\alpha > 0$ and $0 < i < p^\alpha$, we have $p^2 \nmid \binom{p^\alpha}{i}$ if and only if $p^{\alpha-1} | i$;*

(iii) *for $a, b, c \geq 0$, we have $\sum_{i=0}^{c} \binom{i}{a}\binom{c-i}{b} = \binom{c+1}{a+b+1}$;*

(iv) *for $a, b, c, d \geq 0$, we have $\sum_{i=0}^{d} \binom{i}{a}\binom{d-i}{b}\binom{d-i}{c} = \sum_{l=0}^{c} \binom{b}{c-l}\binom{b+l}{l}\binom{d+1}{a+b+l+1}$;*

(v) *If $0 \leq c, d, b-m, a+m+l+1 < 2^{\alpha-1}$, then $\sum_{J=0}^{2^\alpha-1} \binom{J}{c}\binom{J}{d}\binom{J+1}{b-m}\binom{2^\alpha-1-J}{a+m+l+1}$ is even.*

Proof. (i) may be proved on its own or stated as a consequence of Lucas' theorem.

(ii) follows easily from the known formula for the maximal power of p dividing $n!$.

Formula in (iii) has a natural combinatorial interpretation.

(iv) From (iii) we obtain that

$$\begin{aligned}
\sum_{i=0}^{d} \binom{i}{a}\binom{d-i}{b}\binom{d-i}{c} &= \sum_{i=0}^{d} \binom{i}{a}\binom{d-i}{b} \sum_{l=0}^{c} \binom{d-i-b}{l}\binom{b}{c-l} \\
&= \sum_{l=0}^{c} \binom{b}{c-l} \sum_{i=0}^{d} \binom{i}{a}\binom{d-i}{b}\binom{d-i-b}{l} \\
&= \sum_{l=0}^{c} \binom{b}{c-l} \sum_{i=0}^{d} \binom{i}{a}\binom{d-i}{b+l}\binom{b+l}{l} \\
&= \sum_{l=0}^{c} \binom{b}{c-l}\binom{b+l}{l}\binom{d+1}{a+b+l+1}.
\end{aligned}$$

(v) It follows from the observation (resulting from (i)) that $\binom{J}{n} \equiv \binom{J+2^{\alpha-1}}{n} \pmod 2$ for any $0 \leq n < 2^{\alpha-1}$. Hence, for $0 \leq J < 2^{\alpha-1}$, the summand corresponding to J is congruent (mod 2) to the summand corresponding to $J + 2^{\alpha-1}$. □

LEMMA 2.3. *Let* $\Phi = (\Phi_1, \ldots, \Phi_N) : R^N \longrightarrow R^N$, *where* $\Phi_i = b_i + X_i + \sum_j g_{ij} X_j + p \sum_j c_{ij} X_j + \sum_{j \le k} r_{ijk} X_j X_k$. *Put* $H = (g_{ij} + pc_{ij})_{i,j=1}^N$ *and* $\Phi(\bar{0}) = \bar{x}$. *Then, for any* $W \ge 0$,

(i)

$$\Phi^W(\bar{0}) = \sum_{m \ge 0} \binom{W}{m+1} H^m \bar{x} + \sum_{1 \le i,j,k \le N} r_{ijk} \sum_{m,s,t \ge 0} \alpha_{mst} (H^s \bar{x})_j (H^t \bar{x})_k H^m \bar{e}_i + E,$$

where

$$\alpha_{mst} = \sum_{n=0}^{t+1} \binom{s+1}{t+1-n} \binom{s+1+n}{n} \binom{W}{m+s+n+2},$$

and each summand in each coordinate of E *has the homogenous degree with respect to* r_{ijk} *at least* 2.

(ii) *In each summand of each coordinate of* $\Phi^W(\bar{0})$ (*written in the simplest form*), *the homogenous degree with respect to* r_{ijk} *is fewer by* 1 *than the homogenous degree with respect to* b_i.

(iii) *Assume, in addition, that* $N = 2^{\alpha-2} + 1$; $\alpha \ge 4$; $G := (g_{ij})_{i,j} = J_N(0)$ (*for the precise definition of* $J_m(\lambda)$, *see Section 2.3*); $A := I + G$; $c_{ij} = 0$; $\bar{x} = 2\bar{e}_N$. *Assume, moreover, that* $W = 2^\alpha$.

Then E_T (*the* T*th coordinate of* E *from* (i)) *equals* $\mathcal{E}_T + F_T$, *where*

$$\begin{aligned}\mathcal{E}_T = {} & 8 \sum_{i_2,k_2,l_2} \sum_{i_1,k_1,l_1} r_{i_2k_2l_2} r_{i_1k_1l_1} \\ & \times \mathcal{M}(i_2 - T, N+1-l_2, N+1-k_1, N+1-l_1, i_1-k_2) \\ & + 8 \sum_{i_2,k_2,l_2} \sum_{i_1,k_1,l_1} r_{i_2k_2l_2} r_{i_1k_1l_1} \\ & \times \mathcal{M}(i_2 - T, N+1-k_2, N+1-k_1, N+1-l_1, i_1-l_2),\end{aligned}$$

each summand in F_T *has the homogenous degree with respect to* r_{ikl} *at least* 3 (*in particular, by* (ii)), $16 | F_T$), *and*

$$\mathcal{M}(a,b,c,d,z) = \sum_{m=0}^{b} \sum_{l=0}^{z} \binom{m}{z-l} \binom{m+l}{l} \times \sum_{J=0}^{2^\alpha - 1} \binom{J}{c} \binom{J}{d} \binom{J+1}{b-m} \binom{2^\alpha - 1 - J}{a+m+l+1} \tag{1}$$

for $a, b, c, d, z \ge 0$. *If any of* a, b, c, d, z *is negative, then, by definition,* $\mathcal{M}(a,b,c,d,z) = 0$.

(iv) *Assume, in addition, that* $\bar{x} = p\bar{e}_N$. *Then in each summand of each coordinate of* $\Phi^W(\bar{0})$ (*written in the simplest form*), *the homogenous degree with respect to* r_{ijk} *and* c_{ij} *is fewer by at least* 1 *than the exponent* ω *such that* p^ω *divides this summand.*

Proof. (i) By induction or using the ideas from the proof of Lemma 2.1(ii), we obtain that the part of $\Phi^W(\bar{0})$ not depending at all on r_{ijk} equals $\sum_{m\geq 0}\binom{W}{m+1}H^m\bar{x}$.

We see that the term of the form γr_{ijk}, with a vector γ, depending only on b_{i_1}, $g_{i_1j_1}$, and $c_{i_1j_1}$, appears in $\Phi^W(\bar{0})$ with

$$\gamma=\sum_{0\leq J\leq W-1}(I+H)^{W-1-J}\left(\sum_{s\geq 0}\binom{J}{s+1}H^s\bar{x}\right)_j\left(\sum_{t\geq 0}\binom{J}{t+1}H^t\bar{x}\right)_k\bar{e}_i.$$

So, $\gamma=\sum_{m,s,t\geq 0}\alpha_{mst}(H^s\bar{x})_j(H^t\bar{x})_kH^m\bar{e}_i$, where $\alpha_{mst}=\sum_{J=0}^{W-1}\binom{W-1-J}{m}\times\binom{J}{s+1}\binom{J}{t+1}$.

Lemma 2.2(iv), applied for $a=m$, $b=s+1$, $c=t+1$, $d=W-1$, gives the required formula for α_{mst}.

(ii) and (iv) follow by an easy induction on W.

(iii) Put $A_J=I+A+A^2+\cdots+A^{J-1}$. Note that $A_J\bar{x}$ is the part of $\Phi^J(\bar{0})$ with no r_{ikl}. By a direct induction, the summands of $\Phi^W(\bar{0})$ of (homogenous) degree 2 with respect to r_{ikl} give $\mathcal{E}$ equal to

$$\begin{aligned}&\sum_{i_2,k_2,l_2}\sum_{i_1,k_1,l_1}r_{i_2k_2l_2}r_{i_1k_1l_1}\\&\quad\times\sum_{J+K+L=W-2}(A_J\bar{x})_{k_1}(A_J\bar{x})_{l_1}((A^K\bar{e}_{i_1})_{k_2}(A_{J+K+1}\bar{x})_{l_2}\\&\quad+(A^K\bar{e}_{i_1})_{l_2}(A_{J+K+1}\bar{x})_{k_2})A^L\bar{e}_{i_2}.\end{aligned}$$

One may alternatively justify this formula as follows. For fixed (i_2,k_2,l_2), (i_1,k_1,l_1), the terms in the inner sum corresponding to fixed $J,K,L\geq 0$ satisfying $J+K+L=W-2$ correspond to $r_{i_1k_1l_1}$ emerging at the Jth iteration of Φ (then such "marked" $r_{i_1k_1l_1}$ appears in i_1th row with the coefficient $(A_J\bar{x})_{k_1}(A_J\bar{x})_{l_1}$). Then this term is mapped K times by linear terms of Φ, and in $\Phi^{J+K+1}(\bar{0})$, it appears as $r_{i_1k_1l_1}A^K(A_J\bar{x})_{k_1}(A_J\bar{x})_{l_1}\bar{e}_{i_1}$.

Next, we act by Φ with the use of $r_{i_2k_2l_2}X_{k_2}X_{l_2}$. If we take $r_{i_1k_1l_1}$ from $(\Phi^{J+K+1}(\bar{0}))_{k_2}$, then from $(\Phi^{J+K+1}(\bar{0}))_{l_2}$ we must take the terms with no r_{ikl}, that is, $(A_{J+K+1}\bar{x})_{l_2}$. We can also take $r_{i_1k_1l_1}$ from $(\Phi^{J+K+1}(\bar{0}))_{l_2}$, and then from $(\Phi^{J+K+1}(\bar{0}))_{k_2}$ we must take terms with no r_{ikl}, that is, $(A_{J+K+1}\bar{x})_{k_2}$.

Hence, at the $(J+K+1)$th iteration, we have terms divisible by $r_{i_2k_2l_2}r_{i_1k_1l_1}$, and then we act by A (we cannot use any r_{ikl} in order to receive terms of degree 2) L times. Since we are computing $\Phi^W(\bar{0})$, we have $J+K+L=W-2$.

Since $A=I+G$, we have $A^J=\sum_{m\geq 0}\binom{J}{m}G^m$ and (cf. Lemma 2.1(ii)) $A_J=\sum_{m\geq 0}\binom{J}{m+1}G^m$. Taking this into account, we get

$$\begin{aligned}\mathcal{E}=8&\sum_{i_2,k_2,l_2}\sum_{i_1,k_1,l_1}r_{i_2k_2l_2}r_{i_1k_1l_1}\\&\times\sum_{r,s,t,\mu,v\geq 0}\sum_{J+K+L=W-2}\binom{L}{r}\binom{J+K+1}{s+1}\binom{J}{t+1}\binom{J}{v+1}\binom{K}{\mu}\mathcal{A},\end{aligned}$$

where

$$\mathcal{A} = (G^t \bar{e}_N)_{k_1} (G^v \bar{e}_N)_{l_1} ((G^s \bar{e}_N)_{k_2} (G^\mu \bar{e}_{i_1})_{l_2} + (G^s \bar{e}_N)_{l_2} (G^\mu \bar{e}_{i_1})_{k_2}) G^r \bar{e}_{i_2}.$$

Let $W = 2^\alpha$.

Since $(G^s \bar{e}_i)_j$ is nonzero only for $s = i - j \geq 0$, we get that the Tth coordinate of $\mathcal{E}$ equals

$$\begin{aligned}\mathcal{E}_T = 8 \sum_{i_2,k_2,l_2} \sum_{i_1,k_1,l_1} & r_{i_2 k_2 l_2} r_{i_1 k_1 l_1} \\ & \times (\mathcal{M}(i_2 - T, N + 1 - l_2, N + 1 - k_1, N + 1 - l_1, i_1 - k_2) \\ & + \mathcal{M}(i_2 - T, N + 1 - k_2, N + 1 - k_1, N + 1 - l_1, i_1 - l_2)),\end{aligned}$$

where

$$\mathcal{M}(a, b, c, d, z) = \sum_{J+K+L=2^\alpha-2} \binom{L}{a} \binom{J+K+1}{b} \binom{J}{c} \binom{J}{d} \binom{K}{z},$$

and if any argument from a, b, c, d, z is negative, then $\mathcal{M}(a, b, c, d, z) = 0$ by definition.

Since $\binom{J+K+1}{b} = \sum_{m=0}^{b} \binom{J+1}{b-m} \binom{K}{m}$, we get

$$\begin{aligned}\mathcal{M}(a, b, c, d, z) = & \sum_{m=0}^{b} \sum_{J=0}^{2^\alpha-2} \binom{J+1}{b-m} \binom{J}{c} \binom{J}{d} \\ & \times \sum_{K=0}^{2^\alpha-2-J} \binom{K}{m} \binom{K}{z} \binom{2^\alpha - 2 - J - K}{a}.\end{aligned}$$

Let $a, b, c, d, z \geq 0$. Lemma 2.2(iv) gives $\sum_{K=0}^{2^\alpha-2-J} \binom{K}{m} \binom{K}{z} \binom{2^\alpha-2-J-K}{a} = \sum_{l=0}^{z} \binom{m}{z-l} \binom{m+l}{l} \binom{2^\alpha-1-J}{a+m+l+1}$. Hence, (1) holds. □

2.3. Using Matrices in the Jordan Form

Recall that the Jordan form of a given square matrix $A \in M_{N \times N}(K)$ is built from $m \times m$ matrices of the form

$$J_m(\lambda) := \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & 0 & \vdots \\ \vdots & 0 & \ddots & \ddots & 0 \\ \vdots & \vdots & 0 & \lambda & 1 \\ \vdots & \vdots & \vdots & 0 & \lambda \end{pmatrix}$$

with an eigenvalue λ (lying in a fixed algebraic closure of K) on the main diagonal.

Let $\mathcal{J}_m(\lambda)$ be the class of all upperdiagonal $m \times m$ matrices with λ on the main diagonal.

LEMMA 2.4. *Let R be as in Section 2.1, and let $\bar{0} = \bar{x}_0, \dots, \bar{x}_{k-1}$ be a cycle in R^N for Φ. Put $\Phi'(\bar{0}) = A$. Assume that all the eigenvalues of $A \pmod P$ $\in M_{N\times N}(K)$ (lying in the algebraic closure of K) lie in K. Then there is an invertible matrix H with coefficients from R such that*

(i) $(H\Phi H^{-1})'(\bar{0}) \pmod P$ *is equal to the Jordan form of* $A \pmod P$;

(ii) $\bar{0} = \bar{y}_0, \bar{y}_1, \dots, \bar{y}_{k-1}$ *is a cycle for* $\Psi = H\Phi H^{-1}$, *where* $\bar{y}_i = H\bar{x}_i$. *Moreover,* $w(\bar{y}_i) = w(\bar{x}_i)$ (*in particular,* $\bar{0} = \bar{x}_0, \bar{x}_1, \dots, \bar{x}_{k-1}$ *is a* $(\star)$*-cycle if and only if* $\bar{0} = \bar{y}_0, \bar{y}_1, \dots, \bar{y}_{k-1}$ *is such*), *and for all* r, $(A-I)^r\bar{x}_1 \equiv \bar{0} \pmod{P^{w(\bar{x}_1)+1}}$ *iff* $(B-I)^r\bar{y}_1 \equiv \bar{0} \pmod{P^{w(\bar{y}_1)+1}}$, *where* $B = \Psi'(\bar{0})$.

Proof. From the theory of linear spaces it follows that there is a matrix H_1 with coefficients from K (here we use the assumption) such that $H_1 A \pmod P H_1^{-1}$ is the Jordan form of $A \pmod P$. Let H be an $N \times N$ matrix with coefficients from R: $H \pmod P = H_1$. H is invertible since R is local. Put $\bar{y}_i = H\bar{x}_i$. Then $\bar{0} = \bar{y}_0, \bar{y}_1, \dots, \bar{y}_{k-1}$ is a cycle for $\Psi = H \circ \Phi \circ H^{-1}$ (clearly, Ψ is a polynomial mapping with coefficients from R). Clearly, $w(\bar{y}_i) = w(\bar{x}_i)$ holds, and $(H\Phi H^{-1})'(\bar{0}) \pmod P = H_1 A \pmod P H_1^{-1}$. The rest follows from $(B-I)^r\bar{y}_1 \equiv (HAH^{-1}-I)^r H\bar{x}_1 \equiv H(A-I)^r\bar{x}_1 \pmod{P^{w(\bar{x}_1)+1}}$ and $w(H\bar{x}) = w(\bar{x})$ for any $\bar{x} \in R^N$. □

2.4. A Local-to-Global Principle

We shall use the following theorem (it is Theorem 3.2 from [Pe3]).

THEOREM. *Let R be a Dedekind domain, and let $\mathcal{P}(R)$ denote the family of all nonzero prime ideals of R. If $N \geq 2$, then*

$$\mathcal{CYCL}(R,N) = \bigcap_{\mathfrak{p}\in\mathcal{P}(R)} \mathcal{CYCL}(R_{\mathfrak{p}},N) = \bigcap_{\mathfrak{p}\in\mathcal{P}(R)} \mathcal{CYCL}(\hat{R}_{\mathfrak{p}},N),$$

where $\hat{R}_{\mathfrak{p}}$ is the completion of $R_{\mathfrak{p}}$ with respect to the obvious valuation. In particular, this holds for the rings of integers in finite extensions of Q.

3. Cycles of Length p^α

In this section, we assume that R is as in Section 2.1 and, in addition, $e = w(p) = 1$. We use the notation from Section 2.1. We denote $\prod_{i=0}^{r} C_i := C_r C_{r-1} \cdots C_0$.

PROPOSITION 3.1. *Let $\bar{0} = \bar{x}_0, \bar{x}_1, \dots, \bar{x}_{p^\alpha-1}$ be a $(\star)$-cycle in R^N of length $p^\alpha (\alpha \geq 1)$ for a (polynomial) mapping Φ such that $A = \Phi'(\bar{0})$ fulfills $A(A-I)^M \equiv 0 \pmod P$. Assume that $w(\bar{x}_{p^{\alpha-1}}) \geq 2$.*

Then $M \geq p^{\alpha-1}(p-1)/2$, and the equality may take place only if the conditions $p = 2, \alpha \geq 2$, and $w((A-I)^{2^{\alpha-2}-1}\bar{x}_1) = 1$ hold simultaneously.

Proof. Below $W_1, W_2, \dots$ are some polynomials with integer coefficients such that $W_i(0) = 0$ for all $i \geq 1$.

Let γ be the smallest such that $w(\bar{x}_{p^\gamma}) \geq 2$. Put $\delta = \alpha - 1 - \gamma$. So, we have $\delta \geq 0$. Put $(\Phi^{p^\gamma})'(\bar{0}) = B$ and $(\Phi^{p^{\alpha-1}})'(\bar{0}) = D$. Then, by Lemma 2.1(iii), we get $D \equiv B^{p^\delta} \pmod{P^2}$, $D \equiv A^{p^{\alpha-1}} \pmod{P}$, and $B \equiv A^{p^\gamma} \pmod{P}$. Hence, $B - I = (A - I)^{p^\gamma} + pC$ for some matrix C with coefficients from R.

Since $A^{p^\gamma} - I = (A - I)^{p^\gamma} + pW_1(A - I)$; $B - I \equiv (A - I)^{p^\gamma} \pmod{P}$; $D - I \equiv (A - I)^{p^{\alpha-1}} \pmod{P}$, we have, using $p \in P$,

$$
\begin{aligned}
&(D - I)^{p-1} + \binom{p}{p-1}(D - I)^{p-2} + \cdots + \binom{p}{2}(D - I) + pI \\
&\quad \equiv (B^{p^\delta} - I)^{p-1} + pI + pW_2(A - I) \\
&\quad \equiv (B - I)^{p^\delta(p-1)} + pI + pW_3(A - I) \\
&\quad \equiv ((A - I)^{p^\gamma} + pC)^{p^\delta(p-1)} + pI + pW_3(A - I) \\
&\quad \equiv (A - I)^{p^{\alpha-1}(p-1)} + p \sum_{J=0}^{p^\delta(p-1)-1} (A - I)^{p^\gamma J} C (A - I)^{p^\gamma(p^\delta(p-1)-1-J)} \\
&\qquad + pI + pW_3(A - I) \pmod{P^2}. \qquad (2)
\end{aligned}
$$

Put $d = w(\bar{x}_{p^{\alpha-1}})$. Hence, $d \geq 2$.

From Lemma 2.1(ii) it follows that $\bar{0} = (\Phi^{p^\alpha})(\bar{0}) = ((\Phi^{p^{\alpha-1}})^p)(\bar{0}) \equiv ((D - I)^{p-1} + \binom{p}{1}(D - I)^{p-2} + \cdots + pI)\bar{x}_{p^{\alpha-1}} \equiv (A - I)^{p^{\alpha-1}(p-1)}\bar{x}_{p^{\alpha-1}} \pmod{P^{d+1}}$.

Thus, $(A - I)^{p^{\alpha-1}(p-1)}\bar{x}_{p^{\alpha-1}} \equiv \bar{0} \pmod{P^{d+1}}$, and from $A(A - I)^M \bar{x}_{p^{\alpha-1}} \equiv \bar{0} \pmod{P^{d+1}}$, using Lemma 2.1(iv), we arrive at $(A - I)^{\min(M, p^{\alpha-1}(p-1))} \times \bar{x}_{p^{\alpha-1}} \equiv \bar{0} \pmod{P^{d+1}}$. In particular, $M > 0$.

Assume that $M \leq p^{\alpha-1}\frac{p-1}{2}$. Hence,

$$
(A - I)^{p^{\alpha-1}(p-1)/2}\bar{x}_{p^{\alpha-1}} \equiv \bar{0} \pmod{P^{d+1}}. \qquad (3)
$$

Since $M \geq 1$, the number $p^{\alpha-1}(p - 1)$ is even.

Assume, in addition, that $p^\delta(p - 1)$ *is even.*

If $J < p^\delta\frac{p-1}{2}$, then $J \leq p^\delta\frac{p-1}{2} - 1$, and $p^\gamma(p^\delta(p-1) - 1 - J) \geq p^\gamma p^\delta\frac{p-1}{2} = p^{\alpha-1}\frac{p-1}{2}$ follows. So, by (3), for such J, we obtain $p(A - I)^{p^\gamma J}C(A - I)^{p^\gamma(p^\delta(p-1)-1-J)}\bar{x}_{p^{\alpha-1}} \equiv \bar{0} \pmod{P^{d+2}}$.

Thus, by Lemma 2.1(ii) and (2) (for some matrix C_1 with coefficients from R) we get $\bar{0} = ((\Phi^{p^{\alpha-1}})^p)(\bar{0}) \equiv ((D - I)^{p-1} + \cdots + pI)\bar{x}_{p^{\alpha-1}} \equiv ((A - I)^{p^{\alpha-1}(p-1)} + p(A - I)^{p^{\alpha-1}(p-1)/2}C_1 + pI + pW_3(A - I))\bar{x}_{p^{\alpha-1}} \equiv \bar{0} \pmod{P^{d+2}}$. Putting $\bar{u} = ((A - I)^{p^{\alpha-1}(p-1)/2} + pC_1)\bar{x}_{p^{\alpha-1}}$, we then obtain

$$
p(I + W_3(A - I))\bar{x}_{p^{\alpha-1}} + (A - I)^{p^{\alpha-1}(p-1)/2}\bar{u} \equiv \bar{0} \pmod{P^{d+2}}. \qquad (4)
$$

From (3) it follows that $\bar{u} \equiv \bar{0} \pmod{P^{d+1}}$. Since $(A - I)^{p^{\alpha-1}(p-1)/2}$ and $W_3(A - I)$ commute, using (3), we infer by acting $(A - I)^{p^{\alpha-1}(p-1)/2}$ on both sides of (4) that $(A - I)^{p^{\alpha-1}(p-1)}\bar{u} \equiv \bar{0} \pmod{P^{d+2}}$.

The last congruence, $\bar{u} \equiv \bar{0} \pmod{P^{d+1}}$, and $A(A-I)^M \bar{u} \equiv \bar{0} \pmod{P^{d+2}}$ (using Lemma 2.1(iv)) give $(A-I)^{p^{\alpha-1}(p-1)/2}\bar{u} \equiv \bar{0} \pmod{P^{d+2}}$, and by (4) we obtain $(pI + pW_3(A-I))\bar{x}_{p^{\alpha-1}} \equiv \bar{0} \pmod{P^{d+2}}$ or, equivalently, $(I + (W_3(A-I))\bar{x}_{p^{\alpha-1}} \equiv \bar{0} \pmod{P^{d+1}}$. Since $1 + W_3(X) | 1 - (W_3(X))^{p^{\alpha-1}(p-1)}$ (as polynomials), we then obtain

$$(I - (W_3(A-I))^{p^{\alpha}(p-1)})\bar{x}_{p^{\alpha-1}} \equiv \bar{0} \pmod{P^{d+1}}. \tag{5}$$

But $W_3(0) = 0$, and in view of (3), we obtain $(W_3(A-I))^{p^{\alpha}(p-1)}\bar{x}_{p^{\alpha-1}} \equiv \bar{0} \pmod{P^{d+1}}$.

Hence, from (5), we get $\bar{x}_{p^{\alpha-1}} \equiv \bar{0} \pmod{P^{d+1}}$, a contradiction.

So, we obtained that if $M \le p^{\alpha-1}\frac{p-1}{2}$, then $p^{\delta}(p-1)$ is odd, and it follows that $\delta = 0$ and $p = 2$. Since $M \le p^{\alpha-1}\frac{p-1}{2}$, we get $\alpha \ge 2$.

In view of $\delta = 0$, we obtain, using Lemma 2.1(ii) and Lemma 2.2(i), that $\bar{0} \not\equiv \bar{x}_{2^{\alpha-2}} \equiv ((A-I)^{2^{\alpha-2}-1} + \binom{2^{\alpha-2}}{1}(A-I)^{2^{\alpha-2}} + \cdots + 2^{\alpha-2}I)\bar{x}_1 \equiv (A-I)^{2^{\alpha-2}-1}\bar{x}_1 \pmod{P^2}$.

By Lemma 2.1(ii), $\bar{0} = (\Phi^{2^{\alpha}})(\bar{0}) \equiv (A-I)^{2^{\alpha}-1}\bar{x}_1 \pmod{P^2}$. Now, for $M < p^{\alpha-1}\frac{p-1}{2} = 2^{\alpha-2}$, the last congruence, by Lemma 2.1(iv), would give $(A-I)^{2^{\alpha-2}-1}\bar{x}_1 \equiv \bar{0} \pmod{P^2}$, a contradiction. □

REMARK 3.1. In the proof of Proposition 3.1, we obtained $M > 0$ not using $w(\bar{x}_{p^{\alpha-1}}) \ge 2$, but only $w(\bar{x}_{p^{\alpha-1}}) > 0$.

PROPOSITION 3.2. *Let $\bar{0} = \bar{x}_0, \bar{x}_1, \ldots, \bar{x}_{p^{\alpha}-1}$ be a $(\star)$-cycle in R^N of length p^{α} $(\alpha \ge 1)$ for a (polynomial) mapping Φ such that $A = \Phi'(\bar{0})$ fulfills $A(A-I)^M \equiv 0 \pmod{P}$. Assume that $w(\bar{x}_{p^{\alpha-1}}) = 1$. Then $M \ge p^{\alpha-1}\frac{p-1}{2}$, and the equality may take place only for $p \ge 3$ and $(A-I)^{p^{\alpha-1}(p-1)/2-1}\bar{x}_1 \not\equiv \bar{0} \pmod{P^2}$.*

Proof. Let us first consider $p = 2$. Since $\bar{x}_{2^{\alpha-1}} \equiv (A-I)^{2^{\alpha-1}-1}\bar{x}_1 \pmod{P^2}$, the inequality $M \le p^{\alpha-1}\frac{p-1}{2} = 2^{\alpha-2}$ would, by Lemma 2.1(iv), give $(A-I)^{2^{\alpha-2}}\bar{x}_1 \equiv \bar{0} \pmod{P^2}$ (note that, since $M > 0$ by Remark 3.1, we have $\alpha \ge 2$). This, in view of $2^{\alpha-2} \le 2^{\alpha-1} - 1$, gives $w(\bar{x}_{2^{\alpha-1}}) \ge 2$, a contradiction.

So, let $p \ge 3$.

Let $I_1, \ldots, I_s$ be the sizes of the basic blocks corresponding to the eigenvalue 1 with the help of which the Jordan form of the matrix $A \pmod{P}$ is built.

Let I_{s+1} be the multiplicity of the possible eigenvalue 0 of $A \pmod{P}$. Note that, by Remark 3.1, we have $s > 0$; I_{s+1} may be 0. Notice that $I_1, \ldots, I_s \le M$ (which follows from the considering the Jordan form of $A \pmod{P}$).

Using Lemma 2.4 and renaming the variables in the pattern $X_1 \to X_{(1,1)}$, $X_2 \to X_{(1,2)}, \ldots, X_{I_1} \to X_{(1,I_1)}, X_{I_1+1} \to X_{(2,1)}$, and so on, we may thus assume that $A = G + pC$, where C is a matrix with coefficients from R, and the $((i,j),(k,l))$th entry of G equals 0 except for $(i,j) = (k,l)$ (with $i \le s$) or $(i = k \le s, l = j+1)$, where it equals 1.

Since $\bar{0} \equiv (A-I)^{p^{\alpha}-1}\bar{x}_1 \pmod{P^2}$, we may define n_0 as the smallest n satisfying $(A-I)^n \bar{x}_1 \equiv \bar{0} \pmod{P^2}$. Moreover, $(\bar{x}_1)_{(s+1,l)} \equiv 0 \pmod{P^2}$ for any $l \le I_{s+1}$.

In view of $A(A-I)^M \bar{x}_1 \equiv \bar{0} \pmod{P^2}$ and $(A-I)^{p^{\alpha}-1}\bar{x}_1 \equiv \bar{0} \pmod{P^2}$, using Lemma 2.1(iv), we obtain $(A-I)^M \bar{x}_1 \equiv \bar{0} \pmod{P^2}$, and $M \ge n_0$ follows.

Since $\bar{x}_{p^{\alpha-1}} \equiv (A-I)^{p^{\alpha-1}-1}\bar{x}_1 \pmod{P^2}$ and $w(\bar{x}_{p^{\alpha-1}}) = 1$, we get $M \ge n_0 \ge p^{\alpha-1}$.

From the definition of n_0 it follows that n_0 is the biggest n such that $(\bar{x}_1)_{(i,n)} \not\equiv 0 \pmod{P^2}$ for some $i \le s$. After some possible reordering of variables, we may assume that this holds for $i = 1$, that is, $(\bar{x}_1)_{(1,n_0)} \not\equiv 0 \pmod{P^2}$.

In order to prove the assertion of the proposition, it suffices to disprove $M = p^{\alpha-1}\frac{p-1}{2} > n_0$.

Assume the contrary, that is, $M = p^{\alpha-1}\frac{p-1}{2} > n_0$.

Let $\Gamma := (\Phi^{p^{\alpha}}(\bar{0}))_{(1,n_0-p^{\alpha-1}+1)}$. We are going to get that $\Gamma \not\equiv 0 \pmod{P^3}$, contradicting $\Phi^{p^{\alpha}}(\bar{0}) = \bar{0}$.

LEMMA 3.1. *Under the same notation and assumptions,*

(i) *only constant and linear terms of* Φ *may influence* $\Gamma \pmod{P^3}$,
(ii) $\Gamma \not\equiv 0 \pmod{P^3}$.

Proof. Put $H := G - I$.

(i) Clearly, it suffices to deal with summands of Φ of degree 2. Let γ be the coefficient of $X_{(i,j)}X_{(k,l)}$ in $\Phi_{(m,n)}$, the (m,n)th coordinate of Φ. By Lemma 2.3(i), γ influences (linearly) $\Gamma \pmod{P^3}$ with the coefficient

$$c := \sum_{m_1,s_1,t_1 \ge 0} \alpha_{m_1 s_1 t_1} (H^{s_1}\bar{x}_1)_{(i,j)} (H^{t_1}\bar{x}_1)_{(k,l)} (H^{m_1}\bar{e}_{(m,n)})_{(1,n_0-p^{\alpha-1}+1)}.$$

Taking into account the very special form of $H \pmod{P}$, we get $(H^{m_1}\bar{e}_{(m,n)})_{(1,n_0-p^{\alpha-1}+1)} \in P$ for $m > 1$ or $m_1 \ge I_1 - (n_0 - p^{\alpha-1})$ and $(H^{s_1}\bar{x}_1)_{(i,j)} \in P^2$ for $s_1 \ge n_0$ (and a similar relation for t_1).

So, we restrict our interest to summands of c corresponding to $m_1 \le I_1 - (n_0 - p^{\alpha-1}) - 1 \le M - (n_0 - p^{\alpha-1}) - 1$; $s_1, t_1 \le n_0 - 1$.

But for such indices (for $n_1 \le t_1 + 1$), we have $m_1 + s_1 + n_1 + 2 \le M - (n_0 - p^{\alpha-1}) - 1 + n_0 - 1 + n_0 + 2 \le p^{\alpha-1}\frac{p-1}{2} + n_0 + p^{\alpha-1} < p^{\alpha}$ and (in view of $n_0 < p^{\alpha-1}\frac{p-1}{2}$ and Lemma 2.2(i)) $p \mid \binom{p^{\alpha}}{m_1+s_1+n_1+2}$. Hence, $p \mid \alpha_{m_1 s_1 t_1} = \sum_{n_1=0}^{t_1+1} \binom{s_1+1}{t_1+1-n_1}\binom{s_1+1+n_1}{n_1}\binom{p^{\alpha}}{m_1+s_1+n_1+2}$. Finally, $p^3 \mid c$.

(ii) By (i) and Lemma 2.3(i) we have

$$\Gamma \equiv \sum_{m \ge 0} \binom{p^{\alpha}}{m+1} ((H+pC)^m \bar{x}_1)_{(1,n_0-p^{\alpha-1}+1)} \pmod{P^3}.$$

Since $p\big|\binom{p^\alpha}{m+1}$ for $0 \le m < p^\alpha - 1$, we then obtain

$$\begin{aligned}\Gamma &\equiv \sum_{m=0}^{p^\alpha-1} \binom{p^\alpha}{m+1}(H^m \bar{x}_1)_{(1,n_0-p^{\alpha-1}+1)} \\ &\quad + \sum_{J=0}^{p^\alpha-2} (H^{p^\alpha-2-J} pCH^J \bar{x}_1)_{(1,n_0-p^{\alpha-1}+1)} \\ &:= S_1 + S_2 \pmod{P^3}.\end{aligned}$$

In S_2, if $J \ge M$ or $p^\alpha - 2 - J \ge M - (n_0 - p^{\alpha-1})$, then

$$(H^{p^\alpha-2-J} pCH^J \bar{x}_1)_{(1,n_0-p^{\alpha-1}+1)} \equiv 0 \pmod{P^3}.$$

However, $J \le M - 1$ and $p^\alpha - 2 - J \le M - (n_0 - p^{\alpha-1}) - 1$ would give $p^\alpha \le 2M - n_0 + p^{\alpha-1} < p^\alpha$, a contradiction. So, $S_2 \equiv 0 \pmod{P^3}$.

From the definition of n_0 and Lemma 2.2(i) we get

$$S_1 \equiv \binom{p^\alpha}{p^{\alpha-1}}(H^{p^{\alpha-1}-1}\bar{x}_1)_{(1,n_0-p^{\alpha-1}+1)} \equiv p(\bar{x}_1)_{(1,n_0)} \not\equiv 0 \pmod{P^3}.$$

Thus, $\Gamma \not\equiv 0 \pmod{P^3}$. □

The proof of the proposition is now completed. □

4. Examples of ($\star$)-Cycles of Length p^α

Here, R is as in Section 3.

PROPOSITION 4.1. *Let $p \ge 3$ and $\alpha \ge 1$. Then for $N \ge p^{\alpha-1}\frac{p-1}{2}$, there is a ($\star$)-cycle of length p^α in R^N.*

Proof. Clearly, it suffices to take $N = p^{\alpha-1}\frac{p-1}{2}$. Moreover (see Proposition 2.1(ii)), we assume that R is complete. Let $\Phi = (\Phi_1, \dots, \Phi_N) : R^N \to R^N$ be defined as follows:

$\Phi_i(X_1, \dots, X_N) = X_i + X_{i+1} + pc_i X_{2+p^{\alpha-1}(p-3)/2}$ for $i \not\equiv 1 \pmod{p^{\alpha-1}}$, $i < N$;
$\Phi_i(X_1, \dots, X_N) = X_i + X_{i+1}$ for $i \equiv 1 \pmod{p^{\alpha-1}}$, $i < N$;
$\Phi_N(X_1, \dots, X_N) = p + X_N + \sum_{t=0}^{(p-3)/2} r_t X_1 X_{1+tp^{\alpha-1}}$ for $\alpha = 1$ (i.e., $N \equiv 1 \pmod{p^{\alpha-1}}$);
$\Phi_N(X_1, \dots, X_N) = p + X_N + \sum_{t=0}^{(p-3)/2} r_t X_1 X_{1+tp^{\alpha-1}} + pc_N X_{2+p^{\alpha-1}(p-3)/2}$ for $\alpha > 1$.

Notice that $1 + \frac{p-3}{2}p^{\alpha-1} \le p^{\alpha-1}\frac{p-1}{2}$. Moreover, $2 + p^{\alpha-1}\frac{p-3}{2} \le p^{\alpha-1}\frac{p-1}{2}$ fails only for $\alpha = 1$, but then $i \equiv 1 \pmod{p^{\alpha-1}}$ for all $i < N$. Thus, Φ is well defined.

We are going to show that for a suitable choice of c_i, r_t, the tuple $\bar{0}, \Phi(\bar{0}), \dots, \Phi^{p^{\alpha-1}}(\bar{0})$ is a ($\star$)-cycle of length p^α for Φ.

LEMMA 4.1. *The Tth coordinate of $(\Phi^{p^\alpha})(\bar{0})$ is of the following form*:

(i)

$$\begin{aligned}
&\binom{p^\alpha}{p^{\alpha-1}((p-1)/2-g)}p + p^2\binom{p^{\alpha-1}((p+1)/2+g)}{p^{\alpha-1}(1+g)}r_{(p-3)/2-g}\\
&\quad + p^2 U_{p,\alpha,g}\left(r_m\colon\ 0\le m < \frac{p-3}{2}-g\right)\\
&\quad + p^3 V_{p,\alpha,g}(r_0,\dots,r_{(p-3)/2},c_i\colon\ i\not\equiv 1 \pmod{p^{\alpha-1}})\\
&\text{for } T = 1+gp^{\alpha-1} \text{ with some } g\colon 0\le g\le \frac{p-3}{2};
\end{aligned}$$

(ii)

$$\begin{aligned}
&\binom{p^\alpha}{p^{\alpha-1}(p-1)/2-T+1}p + p^2\binom{p^\alpha}{p^{\alpha-1}}c_T\\
&\quad + p^3 c_T r_0\left(\binom{p^{\alpha-1}(p-1)}{p^{\alpha-1}(p-1)/2} + 2\binom{T-1+p^{\alpha-1}(p+1)/2}{p^{\alpha-1}(p-1)/2}\right)\\
&\quad + p^3\tilde{U}_{p,\alpha,T}(r_0,\dots,r_{(p-3)/2},c_i\ (i\not\equiv 1 \pmod{p^{\alpha-1}}, i>T))\\
&\quad + p^4\tilde{V}_{p,\alpha,T}(r_0,\dots,r_{(p-3)/2},c_i\colon\ i\not\equiv 1 \pmod{p^{\alpha-1}})\\
&\text{for } T\not\equiv 1 \pmod{p^{\alpha-1}},
\end{aligned}$$

where the polynomials $U_{p,\alpha,g}$, $V_{p,\alpha,g}$, $\tilde{U}_{p,\alpha,T}$, $\tilde{V}_{p,\alpha,T}$ have integer coefficients, and $U_{p,\alpha,(p-3)/2}=0$.

Proof. Write $\Phi'(\bar{0}) = I + G + pC$, where $G = J_{p^{\alpha-1}(p-1)/2}(0)$. For $i\not\equiv 1 \pmod{p^{\alpha-1}}$, let C_i be an $N\times N$ matrix with only one nonzero entry, namely its $(i, 2+p^{\alpha-1}\frac{p-3}{2})$th entry equals c_i.

We write $\Phi^{p^\alpha}(\bar{0})$ in the simplest form, that is, without any redundant terms. Let us take a particular summand Γ of $(\Phi^{p^\alpha}(\bar{0}))_T$. Let a be the homogenous degree of Γ with respect to r_h, and let b be the corresponding degree with respect to c_i. Lemma 2.1(iv) shows that Γ is divisible by p^{a+b+1}.

From the point of view of the validity of the lemma, only some values of (a,b) (as listed in cases 1–5) are of interest.

Case 1: $a=1$, $b=0$. Let Γ be divisible by r_h.

According to Lemma 2.3(i), such a term equals

$$\Gamma = r_h \sum_{m,s,t\ge 0} \alpha_{mst}(G^s(p\bar{e}_N))_1(G^t(p\bar{e}_N))_{1+hp^{\alpha-1}}(G^m\bar{e}_N)_T$$

with

$$\alpha_{mst} = \sum_{n=0}^{t+1}\binom{s+1}{t+1-n}\binom{s+1+n}{n}\binom{p^\alpha}{m+s+n+2}.$$

Since $(G^s\bar{e}_N)_1\neq 0$ only for $s = N-1 = p^{\alpha-1}\frac{p-1}{2}-1$ (and then equals 1), we may assume that $s = p^{\alpha-1}\frac{p-1}{2}-1$. In a similar manner, we may assume that

$t = p^{\alpha-1}(\frac{p-1}{2} - h) - 1$; $m = p^{\alpha-1}\frac{p-1}{2} - T$. Hence,

$$\begin{aligned}\Gamma &= p^2 r_h \alpha_{N-T,N-1,p^{\alpha-1}((p-1)/2-h)-1} \\ &= p^2 r_h \sum_{n=0}^{p^{\alpha-1}((p-1)/2-h)} \binom{N}{p^{\alpha-1}((p-1)/2-h)-n} \\ &\quad \times \binom{N+n}{n}\binom{p^\alpha}{2N-T+n+1}.\end{aligned}$$

Then write $\Gamma := p^2 r_h \gamma$.

Using Lemma 2.2(i), we obtain that if $T \not\equiv 1 \pmod{p^{\alpha-1}}$, then $p|\gamma$, in full accordance with the assertion.

So, let $T \equiv 1 \pmod{p^{\alpha-1}}$ and put $T = 1 + gp^{\alpha-1}$ (for some $0 \le g \le \frac{p-3}{2}$). This gives

$$\begin{aligned}\gamma \equiv \delta_{h\le(p-3)/2-g} &\binom{p^{\alpha-1}(p-1)/2}{p^{\alpha-1}((p-3)/2-h-g)} \\ &\times \binom{p^{\alpha-1}((p+1)/2+g)}{p^{\alpha-1}(1+g)} \pmod p,\end{aligned}$$

again in full accordance with the assertion of the lemma.

Case 2: $a = 1, b = 1$ (only for $T \not\equiv 1 \pmod{p^{\alpha-1}}$). Let Γ be divisible by $r_g c_i$. It suffices to deal with $i \le T$.

Lemma 2.3(i) gives

$$\Gamma = p^3 r_g(\gamma_1 + \gamma_2 + \gamma_3),$$

where

$\gamma_1 := \sum_{m,s,t\ge 0} \alpha_{mst}(\sum_{J=0}^{s-1} G^{s-1-J} C_i G^J \bar{e}_N)_1 (G^t \bar{e}_N)_{1+gp^{\alpha-1}} (G^m \bar{e}_N)_T$;

$\gamma_2 := \sum_{m,s,t\ge 0} \alpha_{mst}(G^s \bar{e}_N)_1 (\sum_{J=0}^{t-1} G^{t-1-J} C_i G^J \bar{e}_N)_{1+gp^{\alpha-1}} (G^m \bar{e}_N)_T$; and, finally,

$\gamma_3 := \sum_{m,s,t\ge 0} \alpha_{mst}(G^s \bar{e}_N)_1 (G^t \bar{e}_N)_{1+gp^{\alpha-1}} (\sum_{J=0}^{m-1} G^{m-1-J} C_i G^J \bar{e}_N)_T$.

We are going to look for nonzero terms in γ_1, γ_2, γ_3. Put $\alpha_{mst} = \sum_{n=0}^{t+1} \binom{s+1}{t+1-n}\binom{s+1+n}{n}\binom{p^\alpha}{m+s+n+2} := \sum_{n=0}^{t+1} \beta_n$.

In γ_1 we must have (otherwise, the corresponding summand is 0) $J = p^{\alpha-1} - 2$; $m = N - T$; $t = p^{\alpha-1}(\frac{p-1}{2} - g) - 1$; $s - 1 - J = i - 1$; $s = i - 2 + p^{\alpha-1}$.

We see that the only possibility that $p \nmid \beta_n$ is when $m + s + n + 2 = p^\alpha$, which leads to $N - T + i - 2 + p^{\alpha-1} + p^{\alpha-1}(\frac{p-1}{2} - g) + 2 \ge p^\alpha$ and $i - T - p^{\alpha-1} g \ge 0$. Since $i \le T$, we see that $p \nmid \beta_n$ only for $i = T$, $g = 0$, and $n = t + 1 = p^{\alpha-1}(\frac{p-1}{2} - g) = p^{\alpha-1}\frac{p-1}{2}$.

Hence, if $i < T$ or ($i = T$, $g > 0$), then $p|\gamma_1$; if $i = T$, $g = 0$, then $\gamma_1 \equiv \binom{T-1+p^{\alpha-1}(p+1)/2}{p^{\alpha-1}(p-1)/2} c_T \pmod p$.

For γ_2, γ_3, we proceed in a similar manner and obtain: if $i < T$ or ($i = T$, $g > 0$), then $p|\gamma_2, \gamma_3$; if ($i = T$, $g = 0$), then $\gamma_1 \equiv \gamma_2 \pmod p$ and $\gamma_3 \equiv \binom{2N}{N} c_T \pmod p$.

This agrees with the assertion of the lemma.

Case 3: $a=0$, $b=2$ (only for $T \not\equiv 1 \pmod{p^{\alpha-1}}$). Lemma 2.3(i) shows that the sum γ of all Γ with $a=0$, $b=2$ in $(\Phi^{p^\alpha}(\bar{0}))_T$ equals $\gamma = p^3 \sum_{m\geq 0} \binom{p^\alpha}{m+1} \times \sum_{i,j\not\equiv 1 \pmod{p^{\alpha-1}}} \sum_{J+K+L=m-2} (G^J C_i G^K C_j G^L \bar{e}_N)_T$.

Hence,

$$\gamma \equiv p^3 \sum_{i,j\not\equiv 1 \pmod{p^{\alpha-1}}} \sum_{J+K+L=p^\alpha-3} (G^J C_i G^K C_j G^L \bar{e}_N)_T \pmod{p^4}.$$

In the last inner sum, it suffices to take $L = p^{\alpha-1}-2$; $K = j-2-p^{\alpha-1}\frac{p-3}{2}$; $J = i-T$ (otherwise, the corresponding summand is 0). But, for such values of J, K, L, we have $J+K+L = i+j-T-4-p^{\alpha-1}\frac{p-5}{2}$. Since $J+K+L = p^\alpha-3$, we then obtain $i+j-T = p^{\alpha-1}\frac{3p-5}{2}+1$, and $\min\{i,j\} > T$ follows.

Thus, only (i,j) such that $\min\{i,j\} > T$ may influence $\gamma \pmod{p^4}$, which agrees with the assertion of the lemma.

Case 4: $a=0$, $b=1$. Let Γ be divisible by c_i. Lemma 2.3(i) gives

$$\Gamma = p^2 \sum_{m\geq 0} \binom{p^\alpha}{m+1} \sum_{J+K=m-1} (G^J C_i G^K \bar{e}_N)_T.$$

The summand $(G^J C_i G^K \bar{e}_N)_T$ is nonzero only for $K = p^{\alpha-1}-2$; $J = i-T$, and then $m = i-T+p^{\alpha-1}-1$.

Hence, $\Gamma = p^2\binom{p^\alpha}{i-T+p^{\alpha-1}} c_i$ for $i \geq T$, and $\Gamma = 0$ for $i < T$. Since $i-T+p^{\alpha-1} < p^\alpha$, we have $p \mid \binom{p^\alpha}{i-T+p^{\alpha-1}}$, again in full agreement with the assertion of the lemma.

Case 5: $a=0$, $b=0$. Lemma 2.3(i) shows that

$$\Gamma = p \sum_{m\geq 0} \binom{p^\alpha}{m+1} (G^m \bar{e}_N)_T = p\binom{p^\alpha}{p^{\alpha-1}(p-1)/2+1-T}.$$

The lemma is proved. □

Lemma 2.3(i) gives $(\Phi^{p^{\alpha-1}}(\bar{0}))_{N-p^{\alpha-1}+1} \equiv p \pmod{p^2}$, and $\Phi^{p^{\alpha-1}}(\bar{0}) \neq \bar{0}$ follows.

Let $(\Phi^{p^\alpha}(\bar{0}))_{1+gp^{\alpha-1}} = p^2 L_g$ for $0 \leq g \leq \frac{p-3}{2}$, and $(\Phi^{p^\alpha}(\bar{0}))_T = p^3 M_T$ for $T \not\equiv 1 \pmod{p^{\alpha-1}}$. Observe that M_T, L_g are polynomials with coefficients from R.

We order the polynomials M_T, L_g as follows. First, we put M_T according to rising indices, and then we put L_g according to rising indices. Each M_T precedes each L_g.

Let $\Psi : R^N \to R^N$ be a map whose coordinates are of the form M_T or L_g, respecting the just mentioned order. For example, if $p^\alpha = 25$, then $\Psi = (M_2, M_3, M_4, M_5, M_7, M_8, M_9, M_{10}, L_0, L_1)$. We treat Ψ as the polynomial mapping in $\{c_i\}, \{r_g\}$.

We order these variables as follows. This order is similar to the way we ordered the polynomials M_T, L_g. The only change is that we order $\{r_g\}$ according to decreasing indices. For example, if $p^\alpha = 25$, then $c_2, c_3, c_4, c_5, c_7, c_8, c_9, c_{10}, r_1, r_0$ is the proper order of variables.

We observe that there is a unique solution $\bar{z}_0 = \bar{z} \pmod P$ of $\Psi(\bar{z}) \equiv \bar{0} \pmod P$. Namely, using $L_{(p-3)/2} = 0$, we first determine the last coordinate of $\bar{z}_0$, that is, $r_0 \pmod P$. Then we determine $r_1 \pmod P$ (using $L_{(p-5)/2} = 0$), $\ldots$, $r_{(p-3)/2} \pmod P$, and $c_T \pmod P$ starting from the biggest T (using $M_T = 0$).

We observe that $\Psi'(\bar{z}_0) \pmod P$ is upperdiagonal (recall the order of variables introduced before) with nonzero terms on the main diagonal. The key observation is that for any $1 \le T \le N + p^{\alpha-1}\frac{p-1}{2}$, we have $\frac{1}{p}\binom{p^\alpha}{p^{\alpha-1}} + r_0\binom{p^{\alpha-1}(p-1)}{p^{\alpha-1}(p-1)/2} + 2r_0\binom{T-1+p^{\alpha-1}(p+1)/2}{p^{\alpha-1}(p-1)/2} \equiv 2r_0\binom{T-1+p^{\alpha-1}(p+1)/2}{p^{\alpha-1}(p-1)/2} \not\equiv 0 \pmod p$ for r_0 satisfying $L_{(p-3)/2} = 0$.

Hence, $\Psi'(\bar{z}_0)$ is invertible. Using the N-dimensional Hensel's lemma, we obtain that there is a unique solution of $\Psi(\bar{z}) = \bar{0}$. The coordinates of this solution, that is, c_T and r_g determine entirely Φ such that the tuple $\bar{0}, \Phi(\bar{0}), \ldots$ is a $(\star)$-cycle of length p^α for Φ. The proof of the proposition is now completed. □

PROPOSITION 4.2. *Let $p = 2$ and $\alpha \ge 1$. Then for $N > p^{\alpha-1}\frac{p-1}{2} = 2^{\alpha-2}$, there is a $(\star)$-cycle of length $p^\alpha = 2^\alpha$ in R^N.*

Proof. The mapping $X \mapsto -X + 2$ has the $(\star)$-cycle $0, 2$ of length $2 = 2^1$ in R^1. The mapping $(X, Y) \mapsto (-Y, X)$ has the $(\star)$-cycle $(2, 0)$, $(0, 2)$, $(-2, 0)$, $(0, -2)$ of length $4 = 2^2$ in R^2.

For $\alpha \ge 3$, we take R complete (see Proposition 2.1(ii)). Clearly, it suffices to take $N = 2^{\alpha-2} + 1$.

First, we consider $\alpha \ge 4$. So, we have to show that in $R^{2^{\alpha-2}+1}$ there is a $(\star)$-cycle of length 2^α. Let $\Phi = (\Phi_1, \ldots, \Phi_N) : R^N \to R^N$ be defined as follows: $\Phi_{2k-1}(X_1, \ldots, X_N) = X_{2k-1} + X_{2k} + r_{2k-1}X_1X_2 + r_{2k}X_1X_3$, $\Phi_{2k}(X_1, \ldots, X_N) = X_{2k} + X_{2k+1}$ for $1 \le k \le 2^{\alpha-3}$; and $\Phi_N(X_1, \ldots, X_N) = 2 + X_N + r_NX_1X_2 + r_{N+1}X_1X_3$.

We are going to show that for a suitable choice of $r_1, \ldots, r_{N+1}$ a tuple $\bar{0}, \Phi(\bar{0}), \ldots, \Phi^{2^\alpha-1}(\bar{0})$ is a $(\star)$-cycle for Φ (of length 2^α). We need the following:

LEMMA 4.2. *Let $\Phi, p, R, \alpha, N = 2^{\alpha-2} + 1, \ldots$ be as before. Put $\mathcal{I}_N = 16Z[r_1, \ldots, r_{N+1}]$, and for $T < N = 2^{\alpha-2} + 1$, we put $\mathcal{I}_T = 8Z[r_{T+1}, r_{T+2}, \ldots, r_{N+1}] + 16Z[r_1, \ldots, r_{N+1}]$. Then*

(i) $(\Phi^{2^{\alpha-1}}(\bar{0}))_N \equiv 4r_{N+1} \pmod{8Z[r_1, \ldots, r_{N+1}]}$;

(ii) $(\Phi^{2^\alpha}(\bar{0}))_T \pmod{\mathcal{I}_T}$ *equals*

$8r_Tr_{N+1}$ *for $T < N$, T odd;*
$8r_Nr_{N+1} + 8r_{N+1}$ *for $T = N$;*
$8r_Tr_N$ *for T even.*

Proof. We sometimes switch to the notation from Lemma 2.3. For example, $r_{5,1,3} = r_6$; $r_{2,3,4} = 0$.

(i) Since (in Φ) r_{ijk} may be nonzero only for $(j = 1; k \in \{2, 3\})$, for nonzero r_{ijk}, we obtain $j = 1$ and $k = 2 + \Delta$ with $\Delta \in \{0, 1\}$. Lemma 2.3(i) gives

$$(\Phi^{2^{\alpha-1}}(\bar{0}))_N \equiv 2^\alpha + 4r_{N,1,2}\alpha_{0,N-1,N-2} + 4r_{N,1,3}\alpha_{0,N-1,N-3} \pmod{8Z[r_1, \ldots, r_{N+1}]}.$$

Since $\alpha \geq 4$, we obtain that $8|2^\alpha$ and $\alpha_{0,N-1,N-2}$ is even, whereas $\alpha_{0,N-1,N-3}$ is odd. Moreover, $r_{N,1,3} = r_{N+1}$, and we are done.

(ii)1. The part of $(\Phi^{2^\alpha}(\bar{0}))_T$ consisting of all terms divisible by at most one r_i, by Lemma 2.3(i), equals

$$2\binom{2^\alpha}{N-T+1} + 4\sum_{i\geq 0}\sum_{\Delta=0}^{1} r_{i,1,2+\Delta}\delta_{i\geq T}\alpha_{i-T,2^{\alpha-2},2^{\alpha-2}-1-\Delta}. \tag{6}$$

Since $N - T + 1 < 2^{\alpha-1}$, we have $8|\binom{2^\alpha}{N-T+1}$. For $T = N$, we even have $16|2\binom{2^\alpha}{N-T+1}$. Hence, the first term of (6) has no influence on the validity of the assertion.

For $i \geq T$, we have

$$\alpha_{i-T,2^{\alpha-2},2^{\alpha-2}-1-\Delta} = \sum_{n=0}^{2^{\alpha-2}-\Delta} \binom{2^{\alpha-2}+1}{2^{\alpha-2}-\Delta-n}\binom{2^{\alpha-2}+1+n}{n}\binom{2^\alpha}{i-T+2^{\alpha-2}+n+2}. \tag{7}$$

Since $i - T + 2^{\alpha-2} + n + 2 \leq 3 \cdot 2^{\alpha-2} + 2 < 2^\alpha$, we have $2|\binom{2^\alpha}{i-T+2^{\alpha-2}+n+2}$, and $2|\alpha_{i-T,2^{\alpha-2},2^{\alpha-2}-1-\Delta}$ follows. Hence, in the second term of (6), only summands corresponding to $i = T$ may influence the validity of the assertion of this lemma.

Let therefore $i = T$. The only summand of (7) possibly not divisible by 4 corresponds to $n = 2^{\alpha-2} - 2$. Hence, $\alpha_{0,2^{\alpha-2},2^{\alpha-2}-1-\Delta} \equiv 2\binom{2^{\alpha-2}+1}{2-\Delta} \pmod 4$, and $\alpha_{0,2^{\alpha-2},2^{\alpha-2}-1-\Delta}$ is not divisible by 4 only for $\Delta = 1$. Hence, the second term (equal to $8r_{N+1}$) in (6) influences the validity of the assertion only for $i = T = N$.

(ii)2. Now we consider terms divisible by two r_i (note that, by Lemma 2.3(ii), we may neglect considering terms divisible by three r_i). Hence, we consider $\mathcal{E}_T$ from Lemma 2.3(iii).

We have $k_1 = k_2 = 1$ and $l_1 = 2 + \Delta$; $l_2 = 2 + \delta$ for some $\Delta, \delta \in \{0, 1\}$.

Lemma 2.3(iii) shows that

$$\begin{aligned}\mathcal{E}_T = {} & 8\sum_{i_1,i_2 \text{ odd}}\sum_{\Delta,\delta=0}^{1} r_{i_2,1,2+\delta}r_{i_1,1,2+\Delta} \\ & \times \mathcal{M}(i_2 - T, 2^{\alpha-2} - \delta, 2^{\alpha-2} + 1, 2^{\alpha-2} - \Delta, i_1 - 1) \\ & + 8\sum_{i_1,i_2 \text{ odd}}\sum_{\Delta,\delta=0}^{1} r_{i_2,1,2+\delta}r_{i_1,1,2+\Delta} \\ & \times \mathcal{M}(i_2 - T, 2^{\alpha-2} + 1, 2^{\alpha-2} + 1, 2^{\alpha-2} - \Delta, i_1 - 2 - \delta).\end{aligned} \tag{8}$$

We are interested in terms of this sum not belonging to $\mathcal{I}_T$.

First, let us deal with even T. Note that for odd $i > T$, the variables $r_{i,1,2}$, $r_{i,1,3}$ correspond to r_i, r_{i+1}, and $i, i+1 > T$. Since we look in (8) for terms not belonging to $\mathcal{I}_T$, we may assume that $\min\{i_1, i_2\} \le T-1$. If $i_2 < T$, then, by definition, the corresponding summand vanishes.

Note that all arguments of $\mathcal{M}$ in (8) are smaller than $2^{\alpha-1}$, and (still under $\min\{i_1, i_2\} < T$) $(i_2 - T) + (2^{\alpha-2} - \delta) + (i_1 - 1) + 1$, $(i_2 - T) + (2^{\alpha-2} + 1) + (i_1 - 2 - \delta) + 1 \le 2^{\alpha-1}$, with equality only for $i_2 = 2^{\alpha-2} + 1$, $i_1 = T - 1$, $\delta = 0$. In view of the formula for $\mathcal{M}$ in Lemma 2.3(iii) and Lemma 2.2(v), we then get that, for even T,

$$\mathcal{E}_T \equiv 8 \sum_{\Delta=0}^{1} r_{N,1,2} r_{T-1,1,2+\Delta} (\Gamma_1 + \Gamma_2) \pmod{\mathcal{I}_T},$$

with $\Gamma_1 := \mathcal{M}(N - T, 2^{\alpha-2}, 2^{\alpha-2} + 1, 2^{\alpha-2} - \Delta, T - 2)$ and $\Gamma_2 := \mathcal{M}(N - T, 2^{\alpha-2} + 1, 2^{\alpha-2} + 1, 2^{\alpha-2} - \Delta, T - 3)$.

Lemma 2.3(iii) and Lemma 2.2(i), (iv), (v) show that

$$\begin{aligned}\Gamma_1 &\equiv \binom{2^{\alpha-2} + T - 2}{T-2} \sum_{J=0}^{2^\alpha - 1} \binom{J}{2^{\alpha-2}+1} \binom{J}{2^{\alpha-2} - \Delta} \binom{2^\alpha - 1 - J}{2^{\alpha-1}} \\ &\equiv \binom{2^{\alpha-2}+1}{2-\Delta} \pmod 2,\end{aligned}$$

and Γ_1 is odd only for $\Delta = 1$.

Since $2 \mid \binom{2^{\alpha-2}+1+(T-3)}{T-3}$, the same lemmas as above show that $2 \mid \Gamma_2$. Altogether, we get $\mathcal{E}_T \equiv 8 r_{N,1,2} r_{T-1,1,3} = 8 r_N r_T \pmod{\mathcal{I}_T}$ for even T.

Secondly, let T be odd. Like in the case of even T, it suffices to deal with $\min\{i_1, i_2\} \le T$. Moreover, if $\min\{i_1, i_2\} < T$ (and therefore $\min\{i_1, i_2\} \le T - 2$) or $\max\{i_1, i_2\} \le N - 1$, then $(i_2 - T) + 2^{\alpha-2} - \delta + i_1 - 1 + 1$, $(i_2 - T) + 2^{\alpha-2} + 1 + (i_1 - 2 - \delta) + 1 < 2^{\alpha-1}$, and, by Lemma 2.2(v) and Lemma 2.3(iii), the corresponding terms in (8) do lie in $\mathcal{I}_T$. Hence, it suffices to deal with (i_1, i_2) satisfying $\{i_1, i_2\} = \{T, 2^{\alpha-2} + 1\}$. Since $r_{T,1,3}$ corresponds to r_{T+1}, by (8) we obtain that, for odd $T < N$,

$$\mathcal{E}_T \equiv 8 \sum_{\delta=0}^{1} r_{N,1,2+\delta} r_T (\Gamma_1 + \Gamma_2) + 8 \sum_{\Delta=0}^{1} r_T r_{N,1,2+\Delta} (\Gamma_3 + \Gamma_4) \pmod{\mathcal{I}_T},$$

where $\Gamma_1 := \mathcal{M}(N - T, 2^{\alpha-2} - \delta, 2^{\alpha-2} + 1, 2^{\alpha-2}, T - 1)$; $\Gamma_2 := \mathcal{M}(N - T, 2^{\alpha-2} + 1, 2^{\alpha-2} + 1, 2^{\alpha-2}, T - 2 - \delta)$; $\Gamma_3 := \mathcal{M}(0, 2^{\alpha-2}, 2^{\alpha-2} + 1, 2^{\alpha-2} - \Delta, 2^{\alpha-2})$; $\Gamma_4 := \mathcal{M}(0, 2^{\alpha-2} + 1, 2^{\alpha-2} + 1, 2^{\alpha-2} - \Delta, 2^{\alpha-2} - 1)$. In a similar manner, we get

$$\mathcal{E}_N \equiv 8 \sum_{\Delta,\delta=0}^{1} r_{N,1,2+\delta} r_{N,1,2+\Delta} (\Gamma_5 + \Gamma_6) \pmod{\mathcal{I}_T},$$

where $\Gamma_5 := \mathcal{M}(0, 2^{\alpha-2}-\delta, 2^{\alpha-2}+1, 2^{\alpha-2}-\Delta, 2^{\alpha-2})$ and $\Gamma_6 := \mathcal{M}(0, 2^{\alpha-2}+1, 2^{\alpha-2}+1, 2^{\alpha-2}-\Delta, 2^{\alpha-2}-1-\delta)$.

CLAIM 4.1. *Under the same notation and assumptions, Γ_i is odd only for*:

(i) $i=4$; $\Delta=1$;
(ii) $i=5$; $\delta=\Delta=1$;
(iii) $i=6$; $\Delta=1$; $\delta\in\{0,1\}$.

Proof. The scheme of the proof of all items is similar. For $i=1,\dots,6$, put $\Gamma_i = \mathcal{M}(a,b,c,d,z)$. Lemma 2.3(iii) gives (for $i\neq 2$ or $T\neq 1$) that

$$\Gamma_i = \sum_{m=0}^{b}\sum_{l=0}^{z}\binom{m}{z-l}\binom{m+l}{l}\sum_{J=0}^{2^\alpha-1}\binom{J}{c}\binom{J}{d}\binom{J+1}{b-m}\binom{2^\alpha-1-J}{a+m+l+1}. \quad (9)$$

Put $m=b-\phi_1$; $l=z-\phi_2$. Note that

$a+m+l+1 = 2^{\alpha-1}+(1-\delta-\phi_1-\phi_2) \le 2^{\alpha-1}+1$ for $i=1,2,5,6$;
$a+m+l+1 = 2^{\alpha-1}+(1-\phi_1-\phi_2) \le 2^{\alpha-1}+1$ for $i=3,4$.

Clearly, $c, d, \phi_1 < 2^{\alpha-1}$, and if $a+m+l+1 < 2^{\alpha-1}$, then, by Lemma 2.2(v), the inner sum in (9) is even.

Note that $c=2^{\alpha-2}+1$ is odd. Lemma 2.2(i) gives that, for any J, the numbers $\binom{J}{c}\binom{J+1}{1}$ and $\binom{J}{c}\binom{2^\alpha-1-J}{2^{\alpha-1}+1}$ are even.

Hence, the inner sum in (9) may be odd only for $\phi_1=0$; $a+m+l+1=2^{\alpha-1}$. The last condition gives $\phi_2=1-\delta$ for $i=1,2,5,6$; $\phi_2=1$ for $i=3,4$. From this point on we assume that ϕ_2 assumes these values. We therefore obtain $\Gamma_i \equiv \delta_{\phi_2\le z}\binom{b}{\phi_2}\binom{b+z-\phi_2}{z-\phi_2}\sum_{J=0}^{2^\alpha-1}\binom{J}{c}\binom{J}{d}\binom{2^\alpha-1-J}{2^{\alpha-1}}$ (mod 2) and, using Lemma 2.2(iv),

$$\Gamma_i \equiv \delta_{\phi_2\le z}\binom{b}{\phi_2}\binom{b+z-\phi_2}{z-\phi_2} \times \sum_{L=0}^{d}\binom{c}{d-L}\binom{c+L}{L}\binom{2^\alpha}{2^{\alpha-1}+c+L+1} \pmod 2.$$

Since $c=2^{\alpha-2}+1$; $2^{\alpha-2}-2\le d$, using Lemma 2.2(i), we then get

$$\Gamma_i \equiv \delta_{\phi_2\le z}\binom{b}{\phi_2}\binom{b+z-\phi_2}{z-\phi_2}\binom{2^{\alpha-2}+1}{d-2^{\alpha-2}+2}\binom{2^{\alpha-1}-1}{2^{\alpha-2}-2} \pmod 2. \quad (10)$$

We have $d\in\{2^{\alpha-2}, 2^{\alpha-2}-1\}$, and the last but one binomial coefficient in (10), that is, $\binom{2^{\alpha-2}+1}{d-2^{\alpha-2}+2}$, is odd only for $d=2^{\alpha-2}-1$.

Hence, Γ_1, Γ_2 are even, and the remaining Γ_i may be odd only for $\Delta=1$.

Let us assume that $\Delta=1$ and $i\in\{3,4,5,6\}$. Therefore, $d=2^{\alpha-2}-1$ and $\phi_2\le z$.

In Γ_3, the coefficient $\binom{b}{\phi_2}$ is even, and so is Γ_3.

As to Γ_4, for $\Delta=1$, we have $\Gamma_4 \equiv \binom{2^{\alpha-2}+1}{1}\binom{2^{\alpha-2}+1+2^{\alpha-2}-1-1}{2^{\alpha-2}-2} \equiv 1 \pmod 2$. Hence, Γ_4 is odd only for $\Delta=1$.

For Γ_5, for $\Delta = 1$, we have $\Gamma_5 \equiv \binom{2^{\alpha-2}-\delta}{1-\delta}\binom{2^{\alpha-1}-1}{2^{\alpha-2}-1+\delta} \equiv \binom{2^{\alpha-2}-\delta}{1-\delta} \pmod 2$. Hence, Γ_5 is odd only for $\delta = \Delta = 1$.

As to Γ_6, for $\Delta = 1$, we obtain $\Gamma_6 \equiv \binom{2^{\alpha-2}+1}{1-\delta}\binom{2^{\alpha-1}-1}{2^{\alpha-2}-2} \equiv 1 \pmod 2$. Hence, Γ_6 is odd only for $\Delta = 1$ and any $\delta \in \{0, 1\}$. □

The assertion of the lemma follows from Claim 4.1 (do not forget about $8r_{N+1}$ for $T = N$ from (ii)1). □

Put $r_{N+1} = 1$.

Since the Nth coordinate of $\Phi^{2^{\alpha-1}}(\bar{0})$ is congruent to $4 \pmod{8Z[r_1, \ldots, r_N]}$, we obtain $\Phi^{2^{\alpha-1}}(\bar{0}) \neq \bar{0}$.

To reach our goal, that is, $\Phi^{2^\alpha}(\bar{0}) = \bar{0}$, we proceed in a similar way as in the proof of Proposition 4.1. Notice only that we first determine the coset of $r_N \pmod P$ (namely $r_N \equiv 1 \pmod P$) and then the cosets $\pmod P$ of $r_{N-1}, r_{N-2}, \ldots, r_1$.

Let $r'_1, \ldots, r'_N$ be a solution of a suitable system of congruences $\pmod{16R}$. In particular, $r'_N \equiv 1 \pmod P$. After dividing the resulting equations by 8, we compose a mapping from R^N to R^N whose Jacobian matrix $\pmod P$ taken at $(r'_1, \ldots, r'_N)$ is upperdiagonal with 1 on the main diagonal. We finish like in the proof of Proposition 4.1.

We are left with $\alpha = 3$.

Take $\Phi(x, y, z) = (x + y + x^2, y + z + bx^2 + axy, 2 + z + cx^2)$. We see that $\Phi^4(\bar{0}) = (12, *, *) \neq \bar{0}$. By a direct calculation, $\Phi^8(\bar{0}) = (8a + 8c + 8ac + 8 + 16U_1(a, b, c), 8 + 8b + 8a + 8ac + 16U_2(a, b, c), 8c + 16U_3(a, b, c))$ for some polynomials U_1, U_2, U_3 with integer coefficients.

Put $\Psi(a, b, c) = (a + c + ac + 1 + 2U_1(a, b, c), 1 + b + a + ac + 2U_2(a, b, c), c + 2U_3(a, b, c))$.

We see that $\Psi(1, 0, 0) \equiv \bar{0} \pmod P$. Moreover,

$$\Psi'(1, 0, 0) \equiv \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \pmod P, \quad \text{and} \quad \Psi'(1, 0, 0) \text{ is invertible.}$$

The existence of $a, b, c \in R$: $\Psi(a, b, c) = \bar{0}$ follows from Hensel's lemma. □

Using Propositions 2.1, 4.1, and 4.2 and the preceding lemmas, we get the following:

PROPOSITION 4.3. *Let R be as in this section. Let k be such that $k|[p^{fa_1} - 1, \ldots, p^{fa_r} - 1]$ for some $a_1, \ldots, a_r$ fulfilling $a_1 + \cdots + a_r \leq N$. For $k > 1$, let a be the minimum of $a_1 + \cdots + a_r$: $k|[p^{fa_1} - 1, \ldots, p^{fa_r} - 1]$ (and $a = 0$ if $k = 1$). Then in R^N there are $(\star)$-cycles of length kp^α for all α satisfying*

(i) $\alpha \leq \max\{0, \log_p(\frac{2(N-a)}{p-1}p)\}$ *for* $p \geq 3$;

(ii) *and for* $p = 2$:

$$\alpha < 2 + \log_2(N - a) \text{ for } a \leq N - 2,$$

$\alpha \le 2$ *for* $1 \le a = N - 1$,
$\alpha \le 1$ *for* $a = N$ *or* $N = 1$.

Proof. (i) By Proposition 2.1(vi), in R^a there is a $(\star)$-cycle $\bar{0}, \Phi(\bar{0}), \dots, \Phi^{k-1}(\bar{0})$ of length k for some polynomial mapping $\Phi : R^a \to R^a$ with coefficients from R. By Proposition 4.1, for $N - a \ge p^{\alpha-1}\frac{p-1}{2}$ in R^{N-a}, there is a $(\star)$-cycle $\bar{0}, \Psi(\bar{0}), \dots, \Psi^{p^\alpha-1}(\bar{0})$ of length p^α for a suitable $\Psi : R^{N-a} \to R^{N-a}$. Then we see that the mapping $(\Phi, \Psi) : R^a \times R^{N-a} \to R^a \times R^{N-a} = R^N$ given by $(\Phi, \Psi)(\bar{x}, \bar{y}) = (\Phi(\bar{x}), \Psi(\bar{y}))$ has a $(\star)$-cycle $\bar{0}, (\Phi, \Psi)(\bar{0}), \dots$ of length $[k, p^\alpha] = kp^\alpha$ (if $a = 0$ or $a = N$ in this reasoning, then we skip considering Φ or Ψ, respectively).

(ii) We proceed in a similar manner to (i). Using Proposition 4.2, we have that for $N - a > 2^{\alpha-2}$ in R^{N-a}, there is a $(\star)$-cycle of length 2^α. This settles the case $a \le N - 2$.

In the remaining possibility $a \ge N - 1$, *we take* R *complete* (see Proposition 2.1(ii)).

Let $k|m := [2^{fa_1} - 1, \dots, 2^{fa_r} - 1]$ with $a = a_1 + \cdots + a_r \ne 0$. Let (see Proposition 2.1(iv)) $\bar{x}_{i,0}, \bar{x}_{i,1}, \dots, \bar{x}_{i,2^{fa_i}-2}$ be a $(\star)$-cycle for a linear mapping $\Phi_i : R^{a_i} \to R^{a_i}$ having different eigenvalues and whose eigenvalues are primitive roots of unity of order $2^{fa_i} - 1$. Put $A = (\Phi_1, \dots, \Phi_r) : R^{a_1} \times \cdots \times R^{a_r} \to R^{a_1} \times \cdots \times R^{a_r} = R^a$ and $\bar{x}_0 = (\bar{x}_{1,0}, \dots, \bar{x}_{r,0})$. Then $\bar{x}_0, A(\bar{x}_0), \dots$ is a $(\star)$-cycle of length $m \ne 1$ for the linear mapping $A : R^a \to R^a$. In particular, $\bar{x}_0 \ne \bar{0}$. We may also assume that all the coordinates of $\bar{x}_0$ lie in P.

Let $s > 0$ be the smallest satisfying $(-A)^s\bar{x}_0 = \bar{x}_0$. Since $(-A)^{2m}\bar{x}_0 = A^{2m}\bar{x}_0 = \bar{x}_0$, we see that $s|2m$. If s is odd, then $s|m$ and $\bar{x}_0 = (-A)^m\bar{x}_0 = -A^m\bar{x}_0 = -\bar{x}_0$, contradicting $\bar{x}_0 \ne \bar{0}$. Hence, $s = 2t$ for some $t|m$. Then $\bar{x}_0 = (-A)^{2t}\bar{x}_0 = A^{2t}\bar{x}_0$, and $m|t$ follows. We have obtained that

$(*)$ $\bar{x}_0, (-A)\bar{x}_0, \dots$ is a $(\star)$-cycle in R^a of length $2m$ for $-A$.

For the remaining subcase $1 \le a = N - 1$, we take $\bar{x}_0$, A already fixed and put $\Phi(x, \bar{y}) = (-x + 2, \bar{x}_0 + (1 - x)A\bar{y})$ for $x \in R$ and $\bar{y} \in R^{N-1}$.

To get the assertion of the proposition, it suffices to prove the following:

LEMMA 4.3. $(0, \bar{0}), \Phi((0, \bar{0})), \dots$ *is a* $(\star)$*-cycle of length* $4m$ *for* Φ.

Proof. Let $\Psi_0 = \Phi^2$. Thus, $\Psi_0(0, \bar{y}) = (0, (I - A)\bar{x}_0 - A^2\bar{y})$. Put $\Psi(\bar{y}) = (I - A)\bar{x}_0 - A^2\bar{y}$. Since $\Phi^{2l+1}((0, \bar{0})) = (2, \star)$, in order to prove the assertion, it suffices to get

(i) $\Psi^{2m}(\bar{0}) = \bar{0}$;

(ii) $\Psi^{2m/q}(\bar{0}) \ne \bar{0}$ for any prime $q|2m$.

By Proposition 2.1 or Lemma 2.3 we have $\Phi^{2m}(\bar{0}) = (I - A^2 + (-A^2)^2 + \cdots + (-A^2)^{2m-1})(I - A)\bar{x}_0$.

Since $X^{2m} - 1|(1 - X^2 + (-X^2)^2 + \cdots + (-X^2)^{2m-1})(1 - X)$ (note that m is odd) and $(A^{2m} - I)\bar{x}_0 = ((-A)^{2m} - I)\bar{x}_0 = \bar{0}$, we get (i).

Let $q|2m$ be prime. Put $W_0(X) = X^{2m} - 1$, $W_q(X) = (1 - X^2 + (-X^2)^2 + \cdots + (-X^2)^{\frac{2m}{q}-1})(1 - X)$.

Let $W(X) \in \mathbf{Z}[X]$ be any gcd of $W_0(X)$ and $W_q(X)$ (in $Q[X]$).

Suppose that $\Psi^{2m/q}(\bar{0}) = \bar{0}$, that is, $W_q(A)\bar{x}_0 = \bar{0}$. Since $W_0(A)\bar{x}_0 = \bar{x}_0$, we obtain by Lemma 2.1(iv) that $W(A)\bar{x}_0 = \bar{0}$.

If $q = 2$, then $W(X) = 1 - X$. But then $(I - A)\bar{x}_0 = \bar{0}$, $(-A)^2\bar{x}_0 = \bar{x}_0$, contradicting $(*)$.

If $q > 2$, then $W(X) = X^{2m/q} - 1$, and we get $((-A)^{2m/q} - I)\bar{x}_0 = \bar{0}$, contradicting $(*)$. □

The proof of the proposition is now completed. □

Notice that Proposition 4.3, together with Proposition 2.1(i), proves the "existence" part of Theorem 1.

5. ($\star$)-Cycles of Length kp^α. Estimates of α. The Finish of the Proof of Theorem 1

Let R be as in Sections 3 or 4. Proposition 2.1(ii) gives $\mathcal{CYCL}_\star(R, N) = \mathcal{CYCL}_\star(\hat{R}, N)$, and thus we may assume that R is complete.

Let $kp^\alpha \in \mathcal{CYCL}_\star(R, N)$ (with $p \nmid k$). By Lemma 2.1(i), in R^N there is a $(\star)$-cycle of the form $\bar{0} = \bar{x}_0, \bar{x}_1, \ldots, \bar{x}_{kp^\alpha - 1}$ for some mapping Φ. Put $\Phi'(\bar{0}) = C$ and $B := C \pmod P$. We treat B as the matrix with entries from $K = R/P$.

Write the characteristic polynomial $F(X)$ of the matrix B as $(-1)^N X^{a_0}(X - 1)^{b_0} F_1(X)^{b_1} \cdot \ldots \cdot F_r(X)^{b_r}$, where $a_0, b_0 \geq 0$, $F_1, \ldots, F_r$ are pairwise different monic polynomials $\neq X, X - 1$ that are irreducible over K, and $b_1, \ldots, b_r > 0$. Put $a_i := \deg F_i$ for $1 \leq i \leq r$. By Proposition 2.1(v), $k = 1$ if $r = 0$, and k divides $[p^{fa_1} - 1, \ldots, p^{fa_r} - 1]$ if $r > 0$. Put $J := [p^{fa_1} - 1, \ldots, p^{fa_r} - 1](p + 1)^N$, $\Psi = \Phi^J$, and $\Psi'(\bar{0}) = A$. Considering the Jordan form of the matrix B, we see, using $F_i(X) | X^{p^{fa_i}-1} - 1$, that $(I + B + \cdots + B^{J-1})^{\max\{b_1,\ldots,b_r\}}(B - I)^{b_0} B^{a_0} = 0$ (the size of the biggest basic block not corresponding to the eigenvalue 0 in the Jordan form is not bigger than $\max\{b_0, \ldots, b_r\}$) and $(B^J - I)^{\max\{b_0,b_1,\ldots,b_r\}} \times B^{a_0} = 0$.

Hence,

$$(I + C + \cdots + C^{J-1})^{\max\{b_1,\ldots,b_r\}}(C - I)^{b_0} C^{a_0} \equiv 0 \pmod P \tag{11}$$

and

$$(A - I)^{\max\{b_0,b_1,\ldots,b_r\}} A \equiv 0 \pmod P. \tag{12}$$

From the simple properties of periodic points we get that $\bar{0}, \Psi(\bar{0}), \Psi^2(\bar{0}), \ldots, \Psi^{p^\alpha - 1}(\bar{0})$ is a $(\star)$-cycle of length p^α for Ψ (the crucial fact here is $p \nmid J = [p^{fa_1} - 1, \ldots, p^{fa_r} - 1](p + 1)^N$).

Let a be defined as in Theorem 1. In particular, $a \leq a_1 + \cdots + a_r \leq N$.

Let M be the smallest b such that $(A - I)^b A \equiv (C^J - I)^b C^J \equiv 0 \pmod P$. In particular, $M \leq \max\{b_0, \ldots, b_r\}$. We have the following:

LEMMA 5.1. *Let R be as before. Then we have*

(i) $p^{\alpha - 1}\frac{p-1}{2} \leq M \leq \max\{b_0, b_1, \ldots, b_r\}$.

(ii) *Suppose that* $p^{\alpha-1}\frac{p-1}{2} = M$. *Then*

$$(I + C + \cdots + C^{J-1})^{p^{\alpha-1}(p-1)/2}(C - I)^{p^{\alpha-1}(p-1)/2-1}C^{a_0} \not\equiv 0 \pmod{P}, \quad (13)$$

and, in particular, $\max\{b_1, \ldots, b_r\} > p^{\alpha-1}\frac{p-1}{2}$ *or* $b_0 \geq p^{\alpha-1}\frac{p-1}{2}$.

Proof. (i) follows from Propositions 3.1 and 3.2.

(ii) Put $W_1(X) = (1 + X + \cdots + X^{J-1})^{p^{\alpha-1}(p-1)/2}(X - 1)^{p^{\alpha-1}(p-1)/2-1} = (X^J - 1)^{p^{\alpha-1}(p-1)/2-1}(1 + X + \cdots + X^{J-1})$; $W_2(X) = W_1(X)X^{a_0}$; $W_3(X) = (1 + X + \cdots + X^{J-1})^{p^\alpha}(X - 1)^{p^\alpha-1}$.

If $p^{\alpha-1}\frac{p-1}{2} = M$, then by Propositions 3.1 and 3.2 we get $w((A - I)^{p^{\alpha-1}(p-1)/2-1}\Psi(\bar{0})) = 1$. Since $\Psi(\bar{0}) \equiv (I + C + \cdots + C^{J-1})\bar{x}_1 \pmod{P^2}$ and $A \equiv C^J \pmod{P}$, we obtain $W_1(C)\bar{x}_1 \not\equiv \bar{0} \pmod{P^2}$.

Suppose that (13) does not hold. Then $W_2(C)\bar{x}_1 \equiv \bar{0} \pmod{P^2}$. Lemma 2.1(ii) and Lemma 2.2(i) give $\bar{0} \equiv (A - I)^{p^{\alpha-1}}\Psi(\bar{0}) \equiv W_3(C)\bar{x}_1 \pmod{P^2}$. Since $W_1(X) \in (W_2(X), W_3(X))$, Lemma 2.1(iv) then gives $W_1(C)\bar{x}_1 \equiv \bar{0} \pmod{P^2}$, a contradiction.

The final assertion of (ii) follows from comparison of (11) with (13). □

Now we characterize tuples $k, N, a, M, r, a_0, b_0, \ldots, a_r, b_r, p, \alpha$ (with the same notation) satisfying the following condition:

(C) α obeys the estimates from Lemma 5.1 and disobeys the estimate from Proposition 4.3.

Note that for $p = 2$, it suffices to deal with $\alpha \geq 2$.

LEMMA 5.2 (with the same notation). (C) *may take place only if one of the following possibilities holds*:

(i) $p = 2$; $a_0 = b_0 = 0$; $r = 1$; $a = a_1 = 1$; $N = 2^d + 1$ (*for some* $d \geq 1$); $M = b_1 = N$; $\alpha = d + 2$.

(ii) $p = 2$; $a_0 = 0$; $M = b_0 = N - a = 2^d$ (*for some* $d \geq 1$ *or, only for* $a = 0$, $d = 0$); $r \geq 0$; $b_1 = \cdots = b_r = 1$ *and* $\alpha = d + 2$.

Proof. Assume that (C) holds. We may assume that $b_1 \geq b_2 \geq \cdots \geq b_r$.

1. Suppose that $b_1 > p^{\alpha-1}\frac{p-1}{2}$.

In this case, $p^{\alpha-1}\frac{p-1}{2} \leq b_1 - 1 \leq a_1(b_1 - 1) \leq N - a_0 - b_0 - a_1 - a_2b_2 - \cdots - a_rb_r \leq N - a$.

We then see that $p^{\alpha-1}\frac{p-1}{2} \leq N - a$, and the equality implies that $b_1 = p^{\alpha-1}\frac{p-1}{2} + 1$, $a_1 = 1$, $a_0 = 0$, $b_0 = 0$, and $r = 1$ (for if $r \geq 2$, then in view of $a_1 = 1$, we have $[p^{fa_1} - 1, \ldots, p^{fa_r} - 1] = [p^{fa_2} - 1, \ldots, p^{fa_r} - 1]$ and $a \leq a_2 + \cdots + a_r$ follows). Moreover, using Lemma 5.1, we get $M \geq p^{\alpha-1}\frac{p-1}{2}$, but the equality here is impossible due to (13).

Looking at Proposition 4.3, we see that if $b_1 > p^{\alpha-1}\frac{p-1}{2}$, then (C) may hold only for $p = 2$, $N = 2^d + 1$, $d = \alpha - 2 \geq 1$, $a_0 = 0$, $b_0 = 0$, $r = a_1 = 1$, $b_1 = M = N$, and this gives (i) of the lemma.

2. Suppose that $b_0 > p^{\alpha-1}\frac{p-1}{2}$.

In this case, $p^{\alpha-1}\frac{p-1}{2} \le b_0 - 1 < N - (a_1 + \cdots + a_r) \le N - a$, and (C) is not satisfied.

3. Suppose that $\max\{b_0, b_1, \ldots, b_r\} \le p^{\alpha-1}\frac{p-1}{2}$.

Lemma 5.1 then gives $b_0 = p^{\alpha-1}\frac{p-1}{2}$ and $p^{\alpha-1}\frac{p-1}{2} \le b_0 \le N - a_0 - (a_1 + \cdots + a_r) \le N - a$. Hence, $p^{\alpha-1}\frac{p-1}{2} \le N - a$, and the equality here implies that $a_0 = 0$, $b_1 = \cdots = b_r = 1$.

Looking at Proposition 4.3, we see, using Lemma 5.1, that if $\max\{b_0, b_1, \ldots, b_r\} = p^{\alpha-1}\frac{p-1}{2}$, then (C) may hold only for $p = 2$, $N = 2^d + a$, $d = \alpha - 2$ (and $d \ge 1$ or, only for $a = 0$, $d \ge 0$), $a_0 = 0$, $b_0 = 2^d$, $r \ge 0$, $b_1 = \cdots = b_r = 1$, $M = 2^d$, and this gives (ii) of the lemma. □

In order to prove Theorem 1, we shall show that condition (C) on α cannot be satisfied. We use the notation from the very beginning of this section.

Lemma 5.2 gives us two cases to be considered.

First case: (i) of Lemma 5.2.

In this case, $F_1(X) = X - \lambda$ for some $\lambda \in K$, $\lambda \ne 0, 1$. By Lemma 2.4 we may assume that $\Phi'(\bar{0}) = C \equiv J_N(\lambda) \pmod{P}$.

Since $\bar{x}_J \equiv (I + C + \cdots + C^{J-1})\bar{x}_1 \pmod{P^2}$, we see that the last coordinate of $\bar{x}_J$ lies in P^2.

Let β_1 be the coefficient of the term X_1X_2 in the Nth coordinate of Φ. An easy induction gives that the coefficient β_n of the term X_1X_2 in the Nth coordinate of Φ^n is congruent to $\lambda^{n-1}(1 + \lambda + \lambda^2 + \cdots + \lambda^{n-1})\beta_1 \pmod{P}$. In particular, $\beta_J \in P$. Take $\Psi = \Phi^J$.

Hence, $\bar{0}, \bar{x}_J, \ldots$ would be a $(\star)$-cycle for Ψ of length 2^α, satisfying the just mentioned conditions for $\bar{x}_J$ and Ψ. However, the existence of such a cycle is denied by Proposition 5.1(2) below.

Second case: (ii) of Lemma 5.2.

Let $R' = R[\xi]$, where ξ is the primitive Jth root of unity, and P' is the maximal ideal of R' and $K' = R'/P'$. Since $p \nmid J$, we obtain that R' is an unramified discrete valuation domain.

We treat our original $(\star)$-cycle as a cycle in R'^N. Then the characteristic polynomial of $\Phi'(\bar{0}) \pmod{P'}$ (treated as a polynomial with coefficients from K') equals $(-1)^N(X-1)^{2^{\alpha-2}}\prod_{i=1}^{a}(X - \lambda_i)$, where λ_i are distinct elements of K' satisfying $\lambda_i^J = 1$. Moreover, the Jordan form of $\Phi'(\bar{0}) \pmod{P'}$ equals $C_1 := \left(\begin{smallmatrix} J_{2^{\alpha-2}}(1) & 0 \\ 0 & \Lambda \end{smallmatrix}\right)$, where Λ is an $a \times a$ diagonal matrix with λ_i on the diagonal.

Using Lemma 2.4, we obtain then that in R'^N there is a $(\star)$-cycle $\bar{0}, \bar{y}_1, \ldots$ for some mapping Φ_0 satisfying $\Phi_0'(\bar{0}) \equiv C_1 \pmod{P'}$. We easily see that the jth coordinate of $\bar{y}_J \pmod{P'^2}$ may be nonzero only for $j \le 2^{\alpha-2}$. Hence, $\bar{0}, \bar{y}_J, \bar{y}_{2J}, \ldots$ would be a $(\star)$-cycle for Φ_0^J of length 2^α, satisfying the just mentioned conditions for $\bar{y}_J$ and Φ_0^J. However, the existence of such a cycle is further denied by Proposition 5.1(1).

Thus, in order to prove Theorem 1, it suffices to prove the following:

PROPOSITION 5.1. *Let R be as in this section (in particular, $e = w(p) = 1$). In addition, we assume that $p = 2$ and $\alpha \geq 2$.*

Let $\Psi : R^N \to R^N$ be a polynomial mapping with coefficients from R satisfying (for $A := \Psi'(\bar{0})$) one of the following conditions:

(1) (*for some $L \geq 0$, but for $\alpha = 2$, we require $L = 0$*) $A \equiv \left(\begin{smallmatrix} \mathcal{J} & 0 \\ 0 & I \end{smallmatrix}\right) \pmod{P}$, *where I is the $L \times L$ identity matrix, 0s refer to zero matrices of obvious sizes, and $\mathcal{J} \in \mathcal{J}_{2^{\alpha-2}}(1)$ has coefficients from R;*.

(2) (*only for $\alpha \geq 3$*) $A \equiv \mathcal{J} \pmod{P}$ *for some $\mathcal{J} \in \mathcal{J}_{2^{\alpha-2}+1}(1)$, and the coefficient of the term X_1X_2 in the $(N = 2^{\alpha-2} + 1)$th coordinate of Ψ lies in P.*

Then there are no $(\star)$-cycles for Ψ of the form $\bar{0} = \bar{x}_0, \bar{x}_1, \ldots, \bar{x}_{2^{\alpha}-1}$ such that the jth coordinate of $\bar{x}_1 \pmod{P^2}$ may be nonzero only for $j \leq 2^{\alpha-2}$.

Proof. Assume the contrary. Let $\bar{0} = \bar{x}_0, \bar{x}_1, \ldots, \bar{x}_{2^{\alpha}-1}$ be a $(\star)$-cycle in R^N for Ψ such that the jth coordinate of $\bar{x}_1 \pmod{P^2}$ may be nonzero only for $j \leq 2^{\alpha-2}$. Write Ψ in the form $\Psi = \Psi_1 + \Psi_2 + \Psi_3$, where Ψ_1 consists of all terms of degree 0 or 1 in Ψ, and Ψ_2 consists of all terms of degree 2 in Ψ.

From Lemma 2.1(ii) and Lemma 2.2(i) it follows that $\bar{x}_{2^{\alpha-1}} \equiv (A - I)^{2^{\alpha-1}-1}\bar{x}_1 \pmod{P^2}$. Using $2^{\alpha-1} - 1 \geq 2^{\alpha-2} + 1$ (for $\alpha \geq 3$), we then get $\bar{x}_{2^{\alpha-1}} \equiv \bar{0} \pmod{P^2}$. Put $d := w(\bar{x}_{2^{\alpha-1}}) \geq 2$.

For $1 \leq j < 2^{\alpha-2}$, the binomial coefficient $\binom{2^{\alpha-2}}{j}$ is even. Thus, we may write $A^{2^{\alpha-2}} \pmod{P}$ in the form $A^{2^{\alpha-2}} \pmod{P} = I + T$, where $T = 0$ (for case (1)) and (in case (2)) T has possibly only one nonzero term (which lies in the first row and in the last column).

In view of $w(p) = 1$, we have $\Psi'(\bar{x}_i) = A + \Psi_2'(\bar{x}_i) + \Psi_3'(\bar{x}_i) \equiv A + \Psi_2'(\bar{x}_i) \pmod{P^2}$. Since we are dealing with $(\star)$-cycles, we have $\Psi_2'(\bar{x}_i) \equiv \bar{0} \pmod{P}$.

Hence, using $A^{2^{\alpha-2}} \equiv I + T \pmod{P}$, we get

$$
\begin{aligned}
I + (\Psi^{2^{\alpha-1}})'(\bar{0}) &= I + \prod_{i=0}^{2^{\alpha-1}-1} \Psi'(\bar{x}_i) \\
&\equiv I + \prod_{i=0}^{2^{\alpha-1}-1} (A + \Psi_2'(\bar{x}_i)) \\
&\equiv I + A^{2^{\alpha-1}} + \sum_{i=0}^{2^{\alpha-1}-1} A^{2^{\alpha-1}-1-i}\Psi_2'(\bar{x}_i)A^i \\
&\equiv 2I + 2T + (A^{2^{\alpha-2}} - I)^2 + \sum_{i=0}^{2^{\alpha-2}-1} (A^{2^{\alpha-2}}A^{2^{\alpha-2}-1-i}\Psi_2'(\bar{x}_i)A^i \\
&\quad + A^{2^{\alpha-2}-1-i}\Psi_2'(\bar{x}_{i+2^{\alpha-2}})A^iA^{2^{\alpha-2}}) \\
&\equiv 2I + 2T + (A^{2^{\alpha-2}} - I)^2
\end{aligned}
$$

$$
\begin{aligned}
&+\sum_{i=0}^{2^{\alpha-2}-1}((I+T)A^{2^{\alpha-2}-1-i}\Psi_2'(\bar{x}_i)A^i\\
&+A^{2^{\alpha-2}-1-i}\Psi_2'(\bar{x}_{i+2^{\alpha-2}})A^i(I+T))\\
&\equiv 2I+2T+(A^{2^{\alpha-2}}-I)^2+T\Bigg(\sum_{i=0}^{2^{\alpha-2}-1}A^{2^{\alpha-2}-1-i}\Psi_2'(\bar{x}_i)A^i\Bigg)\\
&+\Bigg(\sum_{i=0}^{2^{\alpha-2}-1}A^{2^{\alpha-2}-1-i}\Psi_2'(\bar{x}_{i+2^{\alpha-2}})A^i\Bigg)T\\
&+\sum_{i=0}^{2^{\alpha-2}-1}(A^{2^{\alpha-2}-1-i}\Psi_2'(\bar{x}_i+\bar{x}_{i+2^{\alpha-2}})A^i)\pmod{P^2}.
\end{aligned}
$$

We are going to show that $I+(\Psi^{2^{\alpha-1}})'(\bar{0})\equiv 2G \pmod{P^2}$ for some $G\in\mathcal{J}_N(1)$, and this follows from the following lemma.

LEMMA 5.3 (under the assumptions and notation from the proposition).

(i) *The jth coordinates of vectors* $\bar{v}_1:=\sum_{i=0}^{2^{\alpha-2}-1}\bar{x}_i \pmod{P^2}$ *and* $\bar{v}_2:=\sum_{i=0}^{2^{\alpha-2}-1}\bar{x}_{i+2^{\alpha-2}} \pmod{P^2}$ *may be nonzero only for* $j\le 2$.

(ii) *For any* $0\le i\le 2^{\alpha-2}-1$, *we have* $\bar{x}_i+\bar{x}_{i+2^{\alpha-2}}\equiv 2c\bar{e}_1 \pmod{P^2}$ *for some* (*independent of* i) $c\in R$.

The following matrices have only zero terms on and below the main diagonal:

(iii) $2T \pmod{P^2}$,

(iv) $(A^{2^{\alpha-2}}-I)^2 \pmod{P^2}$,

(v) $T(\sum_{i=0}^{2^{\alpha-2}-1}(A^{2^{\alpha-2}-1-i}\Psi_2'(\bar{x}_i)A^i) \pmod{P^2}$,

(vi) $(\sum_{i=0}^{2^{\alpha-2}-1}A^{2^{\alpha-2}-1-i}\Psi_2'(\bar{x}_{i+2^{\alpha-2}})A^i)T \pmod{P^2}$,

(vii) $\sum_{i=0}^{2^{\alpha-2}-1}(A^{2^{\alpha-2}-1-i}\Psi_2'(\bar{x}_i+\bar{x}_{i+2^{\alpha-2}})A^i) \pmod{P^2}$.

Proof. (i) For $\alpha=2$, the assertion is clear.

Hence, let $\alpha\ge 3$. Lemma 2.1(ii) gives that $\bar{v}_1\equiv\sum_{i=1}^{2^{\alpha-2}-1}(I+A+\cdots+A^{i-1})\bar{x}_1\equiv(A-I)^{2^{\alpha-2}-2}\bar{x}_1 \pmod{P^2}$, and the assertion concerning $\bar{v}_1$ holds.

In order to prove the assertion concerning $\bar{v}_2$, it suffices to show that $\bar{v}_3:=\sum_{i=0}^{2^{\alpha-1}-1}\bar{x}_i\equiv\bar{0} \pmod{P^2}$. We have $\bar{v}_3\equiv(A-I)^{2^{\alpha-1}-2}\bar{x}_1 \pmod{P^2}$. Since $2^{\alpha-2}\le 2^{\alpha-1}-2$, we are done.

(ii) Owing to the assumed properties of $\bar{x}_1 \pmod{P^2}$ and $A \pmod{P}$, by Lemma 2.1(ii) we get $\bar{x}_{i+2^{\alpha-2}}\equiv(I+\cdots+A^{i-1})\bar{x}_1+A^i(I+\cdots+A^{2^{\alpha-2}-1})\bar{x}_1\equiv\bar{x}_i+A^i(A-I)^{2^{\alpha-2}-1}\bar{x}_1\equiv\bar{x}_i+2c\bar{e}_1 \pmod{P^2}$ for some (independent on i) $c\in R$.

(iii) It is obvious.

(iv) If A is as in (1) of Proposition 5.1, then the assertion is clear. So, let A be as in (2). In particular, $\alpha\ge 3$ and $N=2^{\alpha-2}+1$. Write A in the form $A=$

$I + M + 2W$ for M having nonzero terms only above the main diagonal (and, clearly, W has terms from R). Using Lemma 2.2, we get

$$\begin{aligned} A^{2^{\alpha-2}} &= (I + M + 2W)^{2^{\alpha-2}} \\ &\equiv (I + M)^{2^{\alpha-2}} + \sum_{i=0}^{2^{\alpha-2}-1} (I + M)^i 2W (I + M)^{2^{\alpha-2}-i-1} \\ &\equiv (I + M)^{2^{\alpha-2}} + 2 \sum_{i=0}^{2^{\alpha-2}-1} \left(\sum_{r,s\geq 0} \binom{i}{r} M^r W \binom{2^{\alpha-2} - i - 1}{s} M^s \right) \\ &\equiv (I + M)^{2^{\alpha-2}} + 2 \sum_{r,s\geq 0} \binom{2^{\alpha-2}}{r+s+1} M^r W M^s \pmod{P^2}. \end{aligned}$$

Since $2^{\alpha-2} \in P$ and M is upperdiagonal and nilpotent, we obtain that the coefficient in the Nth row and in the first column of $A^{2^{\alpha-2}}$ lies in P^2.

Put $A^{2^{\alpha-2}} - I = T + 2W_1$. Hence, the $(N, 1)$th entry of W_1 lies in P, and this easily gives the assertion.

(v) Again, it suffices to consider A as in (2). It suffices to show that γ equal to the $(N, 1)$th entry of the matrix $\sum_{i=0}^{2^{\alpha-2}-1} (A^{2^{\alpha-2}-1-i} \Psi_2'(\bar{x}_i) A^i)$ lies in P^2.

Since $A \pmod P \in \mathcal{J}_{2^{\alpha-2}+1}(1)$, we easily see that γ is congruent (mod P^2) to the $(N, 1)$th entry of $\sum_{i=0}^{2^{\alpha-2}-1} \Psi_2'(\bar{x}_i) = \Psi_2'(\bar{v}_1)$. The assertion now follows from the assumption concerning the coefficient of $X_1 X_2$ in the last coordinate of Ψ.

(vi) Very similar to (v).

(vii) Write $A \pmod P = I + M$, with M upperdiagonal and nilpotent.

Lemma 5.3(ii) gives $\Psi_2'(\bar{x}_i + \bar{x}_{i+2^{\alpha-2}}) \equiv \Psi_2'(2c\bar{e}_1) \equiv 2c\Psi_2'(\bar{e}_1) := 2B \pmod{P^2}$.

Thus, we get

$$\begin{aligned} &\sum_{i=0}^{2^{\alpha-2}-1} A^{2^{\alpha-2}-1-i} \Psi_2'(\bar{x}_i + \bar{x}_{i+2^{\alpha-2}}) A^i \\ &\quad\equiv 2 \sum_{i=0}^{2^{\alpha-2}-1} A^{2^{\alpha-2}-1-i} B A^i \equiv 2 \sum_{i=0}^{2^{\alpha-2}-1} (I + M)^{2^{\alpha-2}-1-i} B (I + M)^i \\ &\quad\equiv 2 \sum_{i=0}^{2^{\alpha-2}-1} \left(\sum_{r,s\geq 0} \binom{2^{\alpha-2} - i - 1}{r} M^r B \binom{i}{s} M^s \right) \\ &\quad\equiv 2 \sum_{r,s\geq 0} \binom{2^{\alpha-2}}{r+s+1} M^r B M^s \pmod{P^2}. \end{aligned}$$

Put $C_{r,s} := \binom{2^{\alpha-2}}{r+s+1} M^r B M^s$. To get the assertion of this point, it suffices to show for any i that $C_{r,s}\bar{e}_i$ is congruent (mod P) to some linear combination of

vectors $\bar{e}_1, \bar{e}_2, \dots, \bar{e}_{i-1}$. Since $\binom{2^{\alpha-2}}{r+s+1}$ is odd only for $r+s+1 = 2^{\alpha-2}$, we may assume that $r+s = 2^{\alpha-2}-1$.

First case. A is as in (1) of Proposition 5.1.

For $\alpha = 2$ and $L = 0$, the assertion is clear. We thus assume that $\alpha \geq 3$.

First, let $i > 2^{\alpha-2}$. If $s > 0$, then $M\bar{e}_i \equiv \bar{0} \pmod P$, and therefore also $C_{r,s}\bar{e}_i \equiv \bar{0} \pmod P$. If $s = 0$ and $r = 2^{\alpha-2}-1$, then $C_{r,s}\bar{e}_i$ is congruent (mod P) to a scalar multiplicity of $\bar{e}_1$, and we are done.

Secondly, let $i \leq 2^{\alpha-2}$. If $i \leq s+1$, then $M^s\bar{e}_i \pmod P$ is a scalar multiplicity of $\bar{e}_1$. Since the first column of $B = c\Psi_2'(\bar{e}_1)$ is congruent to $\bar{0}$ (mod P), we obtain $BM^s\bar{e}_1 \equiv \bar{0} \pmod P$, and we are done.

Let $s+1 < i \leq 2^{\alpha-2}$. Then $r > 0$ and $C_{r,s}\bar{e}_i \pmod P \in \mathrm{Lin}\{\bar{e}_1, \dots, \bar{e}_{2^{\alpha-2}-r}\} = \mathrm{Lin}\{\bar{e}_1, \dots, \bar{e}_{s+1}\} \subseteq \mathrm{Lin}\{\bar{e}_1, \dots, \bar{e}_{i-1}\}$, and we are done.

Second case. A is as in (2) of Proposition 5.1. Then the assumptions in (2) give that all entries in the first column and the $(N,2)$th entry of $B = \Psi_2'(\bar{0})$ lie in P.

If $i \leq s+1$, then $M^s\bar{e}_i \equiv \bar{0} \pmod P$ is a scalar multiplicity of $\bar{e}_1$. Hence, $BM^s\bar{e}_1 \equiv \bar{0} \pmod P$.

Let $i \geq s+3$. Then $C_{r,s}\bar{e}_i \in \mathrm{Lin}\{\bar{e}_1, \dots, \bar{e}_{2^{\alpha-2}+1-r}\}$. Since $2^{\alpha-2}+1-r = s+2 \leq i-1$, we are done.

Finally, let $i = s+2$. Then $M^s\bar{e}_i \in \mathrm{Lin}\{\bar{e}_1, \bar{e}_2\}$, $BM^s\bar{e}_i \in \mathrm{Lin}\{\bar{e}_1, \dots, \bar{e}_{2^{\alpha-2}}\}$, and $C_{r,s}\bar{e}_i \in \mathrm{Lin}\{\bar{e}_1, \dots, \bar{e}_{2^{\alpha-2}-r}\}$. Since $2^{\alpha-2}-r = s+1 = i-1$, we are done. □

So $I + (\Psi^{2^{\alpha-1}})'(\bar{0}) \equiv 2G \pmod{P^2}$ for some $G \in \mathcal{J}_N(1)$. In particular, G is invertible, and

$$w((I + (\Psi^{2^{\alpha-1}})'(\bar{0}))\bar{x}_{2^{\alpha-1}}) = 1 + w(\bar{x}_{2^{\alpha-1}}) = 1 + d. \tag{14}$$

But, by Lemma 2.1(ii) and $d \geq 2$ (and consequently $2d \geq 2+d$), it follows that $\bar{0} = \Psi^{2^\alpha}(\bar{0}) \equiv (I + (\Psi^{2^{\alpha-1}})'(\bar{0}))\bar{x}_{2^{\alpha-1}} \pmod{P^{d+2}}$ and $w((I + (\Psi^{2^{\alpha-1}})'(\bar{0}))\bar{x}_{2^{\alpha-1}}) \geq 2+d$, contradicting (14). □

Theorem 1 is now proved.

6. Proof of Theorem 2

By the theorem from Section 2.4 we have for $N \geq 2$ that $\mathcal{CYCL}(S,N) = \bigcap_{\mathfrak{p}\text{-prime}} \mathcal{CYCL}(S_{\mathfrak{p}}, N)$.

Let $\mathfrak{p}_0$ be prime such that $\#(S/\mathfrak{p}_0) = p^f = m$ (p prime).

It suffices to show that $\mathcal{CYCL}(S_{\mathfrak{p}_0}, N) \subset \mathcal{CYCL}(S_{\mathfrak{p}}, N)$ for $\mathfrak{p}$ prime with $\#(S/\mathfrak{p}) \geq m^2$.

Let first $p \geq 3$. By Proposition 2.1(i) it suffices to show that $\mathcal{CYCL}(S_{\mathfrak{p}_0}, N) \subset \{1, 2, \dots, p^{2fN}\}$.

By Theorem 1, any element of $\mathcal{CYCL}(S_{\mathfrak{p}_0}, N)$ is not bigger than (we use the notation from Theorem 1) $p^{fN}p^{fa}p^{\lfloor \max(0, \log_p(2(N-a)p/(p-1)))\rfloor}$. It suffices to have $\lfloor \max(0, \log_p(\frac{2(N-a)p}{p-1}))\rfloor \leq f(N-a)$, which clearly holds.

So let $p = 2$. Let $c \cdot k \cdot 2^\alpha$ (with odd k) be the length of a cycle in $S^N_{\mathfrak{p}_0}$, where $c \le p^{fN} = 2^{fN}$ and $k \cdot 2^\alpha$ is the length of a $(\star)$-cycle in R^N.

If $\alpha = 0$, then $c \cdot k \cdot 2^\alpha \le 2^{2fN}$, and we are done.

So let $\alpha > 0$. But in this case, by Proposition 2.1(vii), $k \cdot 2^\alpha < 2 \cdot 2^{fN}$. Since 2 is the length of a $(\star)$-cycle in $S^N_{\mathfrak{p}}$ for any prime $\mathfrak{p}$, from $c \cdot k \cdot 2^{\alpha-1} < 2^{2fN}$, by Proposition 2.1(i), we obtain $c \cdot k \cdot 2^\alpha \in \mathcal{CYCL}(S_{\mathfrak{p}}, N)$ for prime $\mathfrak{p}$ fulfilling $\#(S/\mathfrak{p}) \ge m^2 = 2^{2f}$.

References

[Ba] G. Baron, *Polynomiteration in algebraischen Zahlkörpern,* preprint, 1991.

[Ben] R. Benedetto, *Components and periodic points in non-Archimedean dynamics,* Proc. Lond. Math. Soc. (3) 84 (2002), no. 1, 231–256.

[Bo] J. Boduch, Cykle wielomianowe w pierścieniach algebraicznych liczb całkowitych (Polynomial cycles in rings of algebraic integers), MA thesis, The University of Wrocław, Wrocław, 1990.

[Can] J. K. Canci, *Cycles for rational maps of good reduction outside a prescribed set,* Monatsh. Math. 149 (2006), no. 4, 265–287.

[Erk] T. Erkama, *Periodic orbits of quadratic polynomials,* Bull. Lond. Math. Soc. 38 (2006), no. 5, 804–814.

[FPS] E. Flynn, B. Poonen, and E. Schaefer, *Cycles of quadratic polynomials and rational points on a genus-2 curve,* Duke Math. J. 90 (1997), no. 3, 435–463.

[H-KNa] F. Halter-Koch and W. Narkiewicz, *Polynomial cycles in finitely generated domains,* Monatsh. Math. 119 (1995), 275–279.

[Mor] P. Morton, *Arithmetic properties of periodic points of quadratic maps. II,* Acta Arith. 87 (1998), no. 2, 89–102.

[MorSil] P. Morton and J. Silverman, *Periodic points, multiplicities, and dynamical units,* J. Reine Angew. Math. 461 (1995), 81–122.

[Na1] W. Narkiewicz, *Polynomial cycles in certain rings of rationals,* J. Théor. Nombres Bordeaux 14 (2002), 529–552.

[Na2] ———, *Polynomial cycles in cubic fields of negative discriminant,* Funct. Approx. Comment. Math. 35 (2006), no. 1, 261–269.

[NaPe] W. Narkiewicz and T. Pezda, *Finite polynomial orbits in finitely generated domains,* Monatsh. Math. 124 (1997), 309–316.

[Pe1] T. Pezda, *Polynomial cycles in certain local domains,* Acta Arith. 66 (1994), 11–22.

[Pe2] ———, *On cycles and orbits of polynomial mappings* $Z^2 \mapsto Z^2$, Acta Math. Inform. Univ. Ostraviensis 10 (2002), 95–102.

[Pe3] ———, *Cycles of polynomial mappings in several variables over rings of integers in finite extensions of the rationals,* Acta Arith. 108 (2003), no. 2, 127–146.

[Pe4] ———, *Cycles of polynomial mappings in two variables over rings of integers in quadratic fields,* Cent. Eur. J. Math. 2 (2004), no. 2, 294–331.

[Pe5] ———, *Cycles of polynomial mappings in several variables over rings of integers in finite extensions of the rationals, II,* Monatsh. Math. 145 (2005), 321–331.

[Pe6] ———, *Polynomial cycles in rings of integers in fields of signature* $(0, 2)$, Funct. Approx. Comment. Math. 49 (2013), no. 2, 391–409.

[Pe7] ———, *An algorithm determining cycles of polynomial mappings in integral domains,* Publ. Math. Debrecen 84 (2014), no. 3–4, 399–414.

[Zie] M. Zieve, *Cycles of polynomial mappings,* Ph.D. thesis, UC Berkeley, 1996.

Department of Mathematics
University of Wrocław
pl. Grunwaldzki 2/4
50-384 Wrocław
Poland

pezda@math.uni.wroc.pl