ACTA ARITHMETICA
108.2 (2003)

Cycles of polynomial mappings in several variables over rings of integers in finite extensions of the rationals

by

T. Pezda (Wrocław)

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 $\overline{x}_0, \overline{x}_1, \ldots, \overline{x}_{k-1}$ of different elements of R^N such that

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

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

The study of possible cycle lengths for polynomial mappings of one variable with coefficients from Z_K, the ring of integers in a finite extension K of the rationals, was started in [Na1], where it was shown that the lengths are bounded by $7^{7\cdot 2^n}$ with $[K:\mathbb{Q}] = n$. The proof used the result of [Ev] about the number of solutions of $x + y = a$ with $x, y \in Z_K$ invertible.

A much better bound, namely $(2^n - 1)2^{n+1}$, was obtained in [Pe1] via embeddings Z_K into its suitable localizations.

For the study of iterations of polynomials, rational mappings and power series over discrete valuations rings see [MoSi1], [MoSi2], [NeRo], [No], [Zi].

In [Pe2] an estimate for lengths of cycles for polynomials in N variables over some discrete valuation rings was obtained, and as a result it was inferred that the cycle length for a polynomial mapping in N variables with coefficients from Z_K, K as above, is bounded by $2^{n(1+3N+N^2)}$. As every finitely generated domain D of characteristic 0 is embeddable into a suitable p-adic ring the lengths of cycles in N variables with coefficients from D are bounded by a constant solely depending on D, N as pointed out in [HNa].

For a survey of topics related to polynomial cycles see [Na2], [Na3].

In this paper we will sharpen the results given in [Pe2]. This together with Theorem 3.2, which says that the cycle lengths for polynomial mappings in $N \geq 2$ variables are uniquely determined by the corresponding lengths in their localizations, will allow us to give some asymptotic formulae for cycles in $N \geq 2$ variables over Z_K.

2000 *Mathematics Subject Classification*: 11C08, 13B25.

Acknowledgements. The author is grateful to the referee, whose remarks led to simplifying the proofs and making the presentation clearer. They also suggested the generalization of the original version of Theorem 3.2.

2. Notations. 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 R/P is finite and has $N(P) = p^f$ elements (p is prime). Let π be a generator of the principal ideal P and let v be the norm of R, normalized so that $v(\pi) = 1/p$. We denote by w the corresponding exponent, defined by

$$w(x) = -\frac{\log v(x)}{\log p} \quad \text{for } x \neq 0 \quad \text{and} \quad w(0) = \infty.$$

We put $w(p) = e$. Hence e is the ramification index of R.

We extend v and w to R^N by putting

$$v(\overline{x}) = v((x^{(1)}, \ldots, x^{(N)})) = \max\{v(x^{(i)}),\, i = 1, \ldots, N\},$$
$$w(\overline{x}) = w((x^{(1)}, \ldots, x^{(N)})) = \min\{w(x^{(i)}),\, i = 1, \ldots, N\}.$$

The congruence symbol $\overline{x} \equiv \overline{y} \pmod{P^d}$ will be used for vectors $\overline{x}, \overline{y}$ in R^N to indicate that the corresponding components are congruent, or equivalently $w(\overline{x} - \overline{y}) \geq d$. The image of $\overline{x} \in R^N$ under the canonical mapping $R^N \to R^N/PR^N = (R/P)^N$ will be denoted by $\overline{x} + PR^N$.

A cycle $\overline{x}_0, \ldots, \overline{x}_{k-1}$ is called a $(*)$-*cycle* if $w(\overline{x}_i - \overline{x}_j) \geq 1$ for all i, j. We call a cycle $\overline{x}_0, \ldots$ *normalized* if $\overline{x}_0 = \overline{0}$, the zero element in R^N.

Let $B(R, N)$ be the maximal length, if it exists, of cycles of polynomial mappings in N variables over R. If the cycle lengths are unbounded we put $B(R, N) = \infty$.

Let $\mathcal{G}(R/P, M)$ denote the set of orders prime to p of cyclic subgroups of the linear group $GL_M(R/P)$ of invertible $M \times M$ matrices with coefficients from the field R/P.

Let $\mathcal{H}(R/P, M)$ denote the set of orders prime to p of elements $A \in GL_M(R/P)$ such that for some $\overline{y} \in (R/P)^M$ the vectors $\overline{y}, A\overline{y}, A^2\overline{y}, \ldots$ span the whole $(R/P)^M$.

Denote by $g(R/P, M)$ the biggest element in $\mathcal{G}(R/P, M)$. In the similar manner we define $h(R/P, M)$.

Let $\mathcal{CYCL}(R, N)$ be the set of all possible cycle lengths for polynomial mappings in N variables with coefficients from R.

In this paper a polynomial mapping refers, if not specified differently, to a polynomial mapping in several variables with coefficients from R.

If Φ is a polynomial mapping in N variables with coefficients from R then $\Phi'(\overline{0})$ denotes the Jacobian matrix of Φ at $\overline{0}$.

In [Pe2] it was shown that $B(R,N) \le p^{fN+e+fN+efN} g(R,N)^N$. As a corollary it was inferred that $B(Z_K,N) \le 2^{n(1+3N+N^2)}$, where Z_K is the ring of integers in K, a finite extension of $\mathbb{Q}$ of degree n.

3. Main results. Here $R, P, v, \ldots$ are as in the previous section. For real x let $\lceil x \rceil$ be the smallest integer $\ge x$. Define

$$Z(k) = \sum_{j=1}^{k} \lceil \log_p(2^{j-1}N + 1) \rceil.$$

THEOREM 3.1. *We have*:

(i) *The length of a* $(*)$*-cycle for a polynomial mapping in* N *variables is of the shape*

$$p^{\alpha} \prod_{i=1}^{r} h_i,$$

where

$$\alpha < \lceil \log_p(p^{Z(\lceil \log_2 e \rceil)} + N) \rceil + 1 + \log_p \frac{N(e+1)}{p-1},$$

and $h_i \in \mathcal{H}(R/P, l_i), l_1 + \ldots + l_r \le N$.

(ii) $B(R,N) < p^{fN}(p^{fN}-1)p^{\lceil \log_p(p^{Z(\lceil \log_2 e \rceil)}+N)\rceil + 1 + \log_p \frac{N(e+1)}{p-1}}$.

(iii) *For arbitrary* $1 \le r \le N$ *there is a* $(*)$*-cycle of length* $p^{fr}-1$ *in* R^N *and* $B(R,N) \ge p^{fN}(p^{fN}-1)$.

COROLLARY 3.1. *Let* K *be a finite extension of* $\mathbb{Q}$ *of degree* n. *Then*

$$B(Z_K,N) < \min_{\mathfrak{p}} p^{fN}(p^{fN}-1)p^{\lceil \log_p(p^{Z(\lceil \log_2 e \rceil)}+N)\rceil + 1 + \log_p \frac{N(e+1)}{p-1}} \ll 4^{nN}N^2,$$

where the minimum is taken over all non-zero prime ideals $\mathfrak{p}$ *of* Z_K, $\# Z_K/\mathfrak{p} = p^f$ *and* e *is the ramification index of* $\mathfrak{p}$.

THEOREM 3.2. *Let* R *be a Dedekind domain. Let* $\mathcal{P}(R)$ *denote the set of all non-zero prime ideals of* R. *If* $N \ge 2$ *then*

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

where $\widehat{R}_{\mathfrak{p}}$ *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* $\mathbb{Q}$.

REMARK 3.1. Theorem 3.2 does not hold for $N = 1$. In fact from [Pe1] it follows that $\bigcap_{p \text{ prime}} \mathcal{CYCL}(Z_p,1) = \{1,2,4\}$, whereas $\mathcal{CYCL}(Z,1) = \{1,2\}$.

THEOREM 3.3. *For natural* n *and* N *let*

$$B(n,N) = \max_{K\colon [K:\mathbb{Q}]=n} B(Z_K,N).$$

Then for $N \geq 2$:

(i) $$B(n,N) \geq (2^{nN}-1)(3^{n(N-\lceil N\log_3\frac{3}{2}\rceil)}-1)\left\lfloor\frac{2^{nN}}{3^{n(N-\lceil N\log_3\frac{3}{2}\rceil)}-1}\right\rfloor \gg 4^{nN};$$

(ii) $$\lim_{nN\to\infty,\,N\geq 2}\frac{\log_4 B(n,N)}{nN}=1,$$

in particular, *for $N \geq 2$*,

$$\lim_n \frac{\log_4 B(n,N)}{n} = N;$$

(iii) $4^N \ll B(Z,N) \ll 4^N N^2$.

THEOREM 3.4. *Let K be a fixed finite extension of $\mathbb{Q}$. For a prime number p denote by $c(p)$ the minimum of $\#Z_K/\mathfrak{P}$, where $\mathfrak{P}$ is a prime ideal of Z_K lying above pZ. Write $\{c(p) : p \text{ prime}\} = \{q_1 < q_2 < \ldots\}$. Let k be the largest with $q_k < q_1^2$. For positive real $y_1,\ldots,y_k$ set*

$$\Delta(y_1,\ldots,y_k)=\{(m,m_1,\ldots,m_k): 0\leq m,\ 0\leq m_i\leq y_i,\ i=1,\ldots,k;\\ m+m_1+\ldots+m_k\leq y_i+m_i,\ i=1,\ldots,k\},$$

$$M(y_1,\ldots,y_k)=\max_{(m,m_1,\ldots,m_k)\in\Delta(y_1,\ldots,y_k)}(m+m_1+\ldots+m_k).$$

Then:

(i) $$q_1<\exp(M(\ln q_1,\ldots,\ln q_k))\leq\liminf_N (B(Z_K,N))^{1/N} \leq \limsup_N (B(Z_K,N))^{1/N}\leq q_1^2.$$

(ii) *If $q_4 > q_1^2$ and $q_3q_2 > q_1^3$ then*

$$\lim_N (B(Z_K,N))^{1/N} = q_1^2$$

(*this holds for instance for $q_3 > q_1^2$*).

(iii) *Let K be an extension of $\mathbb{Q}$ of degree 2 or 3 such that the ideal $2Z_K$ is not prime. Then*

$$\lim_N (B(Z_K,N))^{1/N} = 4.$$

4. Some properties of cycles. Let $\overline{x}_0,\ldots,\overline{x}_{k-1}$ be a cycle for a polynomial mapping Φ. We put $\overline{x}_m = \Phi(\overline{x}_{m-1})$ for $m = k, k+1, \ldots$

LEMMA 4.1. *Let $\overline{x}_0,\ldots,\overline{x}_{k-1}$ be a cycle for a polynomial mapping Φ.*

(i) *If $a \in R$ is invertible, $\overline{b} \in R^N$ and $\overline{y}_i = a\overline{x}_i + \overline{b}$ then $\overline{y}_0,\ldots,\overline{y}_{k-1}$ is a cycle for the polynomial mapping $a\Phi(a^{-1}(\overline{X}-\overline{b}))+\overline{b}$, which has coefficients from R.*

(ii) *If* $k = rs$ *then* $\overline{x}_0, \overline{x}_r, \overline{x}_{2r}, \ldots, \overline{x}_{(s-1)r}$ *is a cycle for* $\Phi^r = \underbrace{\Phi \circ \ldots \circ \Phi}_{r}$, *the rth iteration of* Φ.

(iii) *For* $r = 1, \ldots, k-1$ *and arbitrary* i, j *we have* $w(\overline{x}_{i+r} - \overline{x}_i) = w(\overline{x}_{j+r} - \overline{x}_j)$.

(iv) *If* $(r - i, k) = 1$ *then* $w(\overline{x}_r - \overline{x}_i) = w(\overline{x}_1 - \overline{x}_0)$.

(v) *There is a cycle* $\overline{y}_0, \ldots, \overline{y}_{k-1}$ *for some polynomial mapping* Ψ *such that all components of all* $\overline{y}_i$*'s are pairwise different.*

Proof. Points (i)–(iv) were proved in [Pe2]. For the proof of (v) consider an invertible matrix

$$A = \begin{pmatrix} 1 & b & b^2 & b^3 & \ldots & b^{N-1} \\ 0 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & \ldots & 1 \end{pmatrix}$$

for $b \in \mathbb{Z}$. Then there exists $b \in \mathbb{Z}$ such that $A\overline{x}_0, \ldots, A\overline{x}_{k-1}$ is a cycle for the polynomial mapping $A \circ \Phi \circ A^{-1}$ with coefficients from R such that the first components of this cycle are pairwise different.

Fix such a b. Take a fixed vector $\overline{v} \in R^N$ such that the first components of $A\overline{x}_0 + \overline{v}, \ldots, A\overline{x}_{k-1} + \overline{v}$ are non-zero. Then we consider an invertible matrix

$$B = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ c & 1 & 0 & \ldots & 0 \\ c^2 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ c^{N-1} & 0 & 0 & \ldots & 1 \end{pmatrix},$$

and for some $c \in \mathbb{Z}$ we get a cycle $B(A\overline{x}_0 + \overline{v}), \ldots, B(A\overline{x}_{k-1} + \overline{v})$ which fulfils our requirements. ∎

LEMMA 4.2. *Let* Φ *be a polynomial mapping in* N *variables with coefficients from* R. *Then* $\overline{x} \equiv \overline{y} \pmod{P^d}$ *implies* $\Phi(\overline{x}) \equiv \Phi(\overline{y}) \pmod{P^d}$.

Proof. Clear. ∎

PROPOSITION 4.1. *Let* R *be a discrete valuation ring with a valuation* v *and let* $\widehat{R}$ *be the completion of* R *with respect to* v. *Then* $\mathcal{CYCL}(R, N) = \mathcal{CYCL}(\widehat{R}, N)$ *for all* $N \ge 1$. *Moreover*, *the sets of lengths of* $(*)$*-cycles in* R^N *and* $\widehat{R}^N$ *also coincide.*

Proof. Clearly $\mathcal{CYCL}(R, N) \subset \mathcal{CYCL}(\widehat{R}, N)$. Let $\overline{x}_0, \ldots, \overline{x}_{k-1}$ be a cycle for a polynomial mapping $\Phi : \widehat{R}^N \to \widehat{R}^N$ with coefficients from $\widehat{R}$. We can assume, according to Lemma 4.1(v), that all components of $\overline{x}_i$'s are pairwise different. Put $\Phi = (\Phi^{(1)}, \ldots, \Phi^{(N)})$. Write

$$\Phi^{(i)}(X_1, \ldots, X_N) = c^{(i)}_{k-1} X_1^{k-1} + \ldots + c^{(i)}_0 + G_i(X_1, \ldots, X_N)$$

with $c_j^{(i)} \in \widehat{R}, G_i \in \widehat{R}[X_1, \ldots, X_N]$. Notice that for $i = 1, \ldots, N$ the numbers $c_0^{(i)}, \ldots, c_{k-1}^{(i)}$ satisfy the system of equations (with $\overline{x}_j = (\overline{x}_j^{(1)}, \ldots, \overline{x}_j^{(N)})$):

$$\begin{cases} c_0^{(i)} + c_1^{(i)} x_0^{(1)} + \ldots + c_{k-1}^{(i)} (x_0^{(1)})^{k-1} = x_1^{(i)} - G_i(x_0^{(1)}, \ldots, x_0^{(N)}), \\ c_0^{(i)} + c_1^{(i)} x_1^{(1)} + \ldots + c_{k-1}^{(i)} (x_1^{(1)})^{k-1} = x_2^{(i)} - G_i(x_1^{(1)}, \ldots, x_1^{(N)}), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ c_0^{(i)} + c_1^{(i)} x_{k-1}^{(1)} + \ldots + c_{k-1}^{(i)} (x_{k-1}^{(1)})^{k-1} = x_0^{(i)} - G_i(x_{k-1}^{(1)}, \ldots, x_{k-1}^{(N)}). \end{cases}$$

Now we replace $\overline{x}_0, \ldots, \overline{x}_{k-1}$ by $\overline{y}_0, \ldots, \overline{y}_{k-1}$ with coefficients from R, such that $\overline{y}_t$ is sufficiently close to $\overline{x}_t$. We proceed similarly with the coefficients of G_i, i.e. we take $H_i(X_1, \ldots, X_N)$ with the same monomials as in $G_i(X_1, \ldots, X_N)$ but with coefficients from R sufficiently close to the corresponding coefficients of G_i.

We thus get a tuple $\overline{y}_0, \ldots, \overline{y}_{k-1}$ with different elements, which is a cycle for $\widetilde{\Phi} = (\widetilde{\Phi^{(1)}}, \ldots, \widetilde{\Phi^{(N)}})$, where $\widetilde{\Phi^{(i)}}(X_1, \ldots, X_N) = \widetilde{c_0^{(i)}} + \ldots + \widetilde{c_{k-1}^{(i)}} X_1^{k-1} + H_i(X_1, \ldots, X_N)$ and the $\widetilde{c_j^{(i)}}$ are the solution of a similar system of equations, but with G_i replaced by H_i, and $\overline{x}_t$ by $\overline{y}_t$. Such a solution $(\widetilde{c_0^{(i)}}, \ldots, \widetilde{c_{k-1}^{(i)}})$ will lie in R.

The statement concerning $(*)$-cycles follows from the observation that approximating a $(*)$-cycle in $\widehat{R}^N$ sufficiently closely by elements from R^N we get a $(*)$-cycle in R^N. ∎

LEMMA 4.3. *Let $\overline{0} = \overline{x}_0, \overline{x}_1, \ldots, \overline{x}_{m-1}$ be a normalized $(*)$-cycle in R^N for Φ. Then $l \mid k$ implies $w(\overline{x}_l) \le w(\overline{x}_k)$ (also for $l, k \ge m$ with $\overline{x}_m, \overline{x}_{m+1}, \ldots$ defined at the beginning of this section).*

Proof. Put $k = ls$. We have

$$\begin{aligned} w(\overline{x}_k) &= w(\overline{x}_k - \overline{x}_0) = w(\overline{x}_{ls} - \overline{x}_0) \\ &= w((\overline{x}_{ls} - \overline{x}_{l(s-1)}) + (\overline{x}_{l(s-1)} - \overline{x}_{l(s-2)}) + \ldots + (\overline{x}_{2l} - \overline{x}_l) + (\overline{x}_l - \overline{x}_0)) \\ &\ge \min\{w(\overline{x}_{ls} - \overline{x}_{l(s-1)}), \ldots, w(\overline{x}_l - \overline{x}_0)\} = w(\overline{x}_l - \overline{x}_0) = w(\overline{x}_l). \end{aligned}$$

We have used Lemma 4.1(iii). ∎

LEMMA 4.4. *The length of a polynomial cycle in R^N can be written in the form ab, where a is the length of a certain $(*)$-cycle in R^N and $b \le p^{fN}$. Conversely, every number of that form is the length of a suitable cycle in R^N.*

Proof. The first part was proved in [Pe2]. To prove the existence part note that owing to Proposition 4.1 it suffices to consider the case of complete R (the number f is the same for both R and $\widehat{R}$).

Let $b = 1 + r$ for a suitable $0 \le r < p^{fN}$ and fix $\overline{a}_0, \ldots, \overline{a}_r \in R^N$ such that $\overline{a}_i + PR^N \ne \overline{a}_j + PR^N$ for $i \ne j$, and moreover $\overline{a}_0 = \overline{0}$. Put

$\overline{a}_j = (\overline{a}_j^{(1)}, \ldots, \overline{a}_j^{(N)})$. Fix a $(*)$-cycle $\overline{y}_0 = \overline{0}, \ldots, \overline{y}_{a-1}$ for a mapping Φ. Put $M = ab = a(1+r)$.

We will show that $\overline{y}_0, \overline{y}_0+\overline{a}_1, \ldots, \overline{y}_0+\overline{a}_r, \overline{y}_1, \overline{y}_1+\overline{a}_1, \ldots, \overline{y}_1+\overline{a}_r, \ldots, \overline{y}_{a-1}, \ldots, \overline{y}_{a-1}+\overline{a}_r$ is a $(*)$-cycle in R^N. For this purpose take for $n \geq 1$ a polynomial mapping

$$\begin{aligned}\Psi_n(X) &= \Psi_n(X_1, \ldots, X_N) \\ &= \prod_{w=1}^{N} (1 - (X_w - \overline{a}_r^{(w)})^{p^{fn}(p^f-1)}) \Phi(X - \overline{a}_r) \\ &\quad + \sum_{j=0}^{r-1} \Big(\prod_{w=1}^{N} (1 - (X_w - \overline{a}_j^{(w)})^{p^{fn}(p^f-1)}) \Big) (X + \overline{a}_{j+1} - \overline{a}_j).\end{aligned}$$

For $j = 0, \ldots, r$ and $l \geq 0$ we have

$$\Psi_n^{l(1+r)+j}(\overline{y}_0) \equiv \overline{y}_l + \overline{a}_j \pmod{P^{n+1}}.$$

Let I_n be the ideal of $R[X_1, \ldots, X_N]$ generated by $\prod_{j=0}^{M-1}(X_w - (\Psi_n^j(\overline{y}_0))^{(w)})$, $w = 1, \ldots, N$. Let $L_n = (L_n^{(1)}, \ldots, L_n^{(N)})$ be such that

$$L_n^{(w)} = \sum_{0 \leq i_1, \ldots, i_N \leq M-1} b_{w,i_1,\ldots,i_N}^{(n)} X_1^{i_1} \ldots X_N^{i_N}$$

with $L_n^{(w)}$ congruent $\pmod{I_n}$ to the wth component $\Psi_n^{(w)}$ of Ψ_n. We easily see that $L_n^j(\overline{y}_0) = \Psi_n^j(\overline{y}_0)$ for $j = 0, \ldots, M$.

As R is compact, there is a sequence $n_1 < n_2 < \ldots$ such that for all $0 \leq i_1, \ldots, i_N \leq M-1$ and $w = 1, \ldots, N$ we have $\lim_{k\to\infty} b_{w,i_1,\ldots,i_N}^{(n_k)} = c_{w,i_1,\ldots,i_N}$ for some $c_{w,i_1,\ldots,i_N} \in R$. Put $L = (L^{(1)}, \ldots, L^{(N)})$, where

$$L^{(w)}(X_1, \ldots, X_N) = \sum_{0 \leq i_1, \ldots, i_N \leq M-1} c_{w,i_1,\ldots,i_N} X_1^{i_1} \ldots X_N^{i_N}.$$

Then for $j = 0, \ldots, r$ and $l \geq 0$ such that $l(1+r)+j \leq M$ we have

$$L^{l(1+r)+j}(\overline{y}_0) = \lim_{k\to\infty} L_{n_k}^{l(1+r)+j}(\overline{y}_0) = \lim_{k\to\infty} \Psi_{n_k}^{l(1+r)+j}(\overline{y}_0) = \overline{y}_l + \overline{a}_j,$$

which easily gives the statement of the lemma. ∎

LEMMA 4.5. *Let $\overline{0} = \overline{x}_0, \overline{x}_1, \ldots, \overline{x}_{m-1}$ be a $(*)$-cycle in R^N (this cycle is normalized according to the definition from Section 2). Let $\{w(\overline{x}_1), \ldots, w(\overline{x}_{m-1})\} = \{d_1 < \ldots < d_r\}$ and $m_i = \min\{j : w(\overline{x}_j) = d_i\}$. Then $1 = m_1 \mid m_2 \mid \ldots \mid m_r \mid m$.*

Proof. Let $i \geq 1$ and put $l = (m_i, m_{i+1})$. Lemma 4.3 implies that $w(\overline{x}_l) \leq w(\overline{x}_{m_i})$; on the other hand $tm_i + sm_{i+1} \equiv l \pmod{m}$ with suitable positive integers t, s. Thus, using Lemma 4.1(iii), we have

$$\begin{aligned} w(\overline{x}_l) &= w(\overline{x}_{tm_i+sm_{i+1}}) \\ &\geq \min(\{w(\overline{x}_{(j+1)m_i+sm_{i+1}} - \overline{x}_{jm_i+sm_{i+1}}) : 0 \leq j \leq t-1\} \\ &\quad \cup \{w(\overline{x}_{(k+1)m_{i+1}} - \overline{x}_{km_{i+1}}) : 0 \leq k \leq s-1\}) \geq w(\overline{x}_{m_i}), \end{aligned}$$

as $w(\overline{x}_{m_{i+1}}) > w(\overline{x}_{m_i})$. Thus we get $w(\overline{x}_l) = w(\overline{x}_{m_i})$, and $m_i \nmid m_{i+1}$ would imply $l < m_i$, a contradiction. A similar argument shows that each m_i divides m. ∎

LEMMA 4.6. *Let Φ be a polynomial mapping in several variables (with coefficients from R), $\Phi(\overline{0}) = \overline{x}, w(\overline{x}) = d, \Phi'(\overline{0}) = A$. Then*

$$\overline{x}_s = \Phi^s(\overline{0}) \equiv (A^{s-1} + A^{s-2} + \ldots + A + I)\overline{x} \pmod{P^{2d}} \quad \text{for all } s \geq 0.$$

Proof. By induction. Note that for $\overline{y}$ such that $w(\overline{y}) \geq d$ one has (from Taylor's expansion) $\Phi(\overline{y}) \equiv \Phi(\overline{0}) + \Phi'(\overline{0})\overline{y} \pmod{P^{2d}}$. ∎

LEMMA 4.7. *Let $\overline{0} = \overline{x}_0, \overline{x}_1, \ldots, \overline{x}_{m-1}$ be a $(*)$-cycle for Φ, m_i as in Lemma 4.5, and put $(\Phi^{m_i})'(\overline{0}) = A_i$. Then*

$$\frac{m_{i+1}}{m_i} = \min\{M : (A_i^{M-1} + \ldots + A_i + I)\pi^{-d_i}\overline{x}_{m_i} \equiv \overline{0} \pmod{P}\}.$$

A similar relation holds for m/m_r.

Proof. The previous lemma gives $\overline{x}_{Mm_i} \equiv (A_i^{M-1} + \ldots + A_i + I)\overline{x}_{m_i} \pmod{P^{2d_i}}$. Since $d_i > 0$, the number $\min\{M : (A_i^{M-1} + \ldots + A_i + I)\pi^{-d_i}\overline{x}_{m_i} \equiv \overline{0} \pmod{P}\}$ is therefore the minimal M such that $w(\overline{x}_{Mm_i}) > d_i$. By definition we have $m_{i+1} = \min\{j : w(\overline{x}_j) = d_{i+1}\} = \min\{j : w(\overline{x}_j) > d_i\}$. Owing to $m_i \mid m_{i+1}$ we get the result. A similar argument works for the case $i = r$. ∎

5. $(*)$-cycles of length not divisible by p

PROPOSITION 5.1. *Let m be the length of a $(*)$-cycle in R^N not divisible by p. Then we can write $m = h_1 \ldots h_r$, where $h_i \in \mathcal{H}(R/P, l_i), l_1 + \ldots + l_r \leq N$.*

Proof. Let $\overline{x}_0, \overline{x}_1, \ldots, \overline{x}_{m-1}$ be a $(*)$-cycle for a polynomial mapping Φ of R^N. By Lemma 4.1(i), we can assume that $\overline{x}_0 = \overline{0}$. Let d_i, m_i be as in Lemma 4.5, i.e.

$$\{w(\overline{x}_1), \ldots, w(\overline{x}_{m-1})\} = \{d_1 < \ldots < d_r\}, \quad m_i = \min\{j : w(\overline{x}_j) = d_i\}.$$

Lemma 4.3 shows that $\pi^{-d_i}\overline{x}_{km_i}, k = 1, 2, \ldots,$ are well defined elements of R^N. Define auxiliary linear spaces over the field R/P:

$$L_i = \mathrm{Lin}(\{\pi^{-d_i}\overline{x}_{km_i} + PR^N : k = 0, 1, 2, \ldots\}).$$

Here, Lin means the linear span over R/P. We consider L_i in a natural way as a linear subspace of $(R/P)^N$.

For $s = 1, \ldots, r$ define $A_s = (\Phi^{m_s})'(\overline{0})$, which is an $N \times N$ matrix with coefficients from R. It could be considered in a natural way as a linear transformation of $(R/P)^N$.

LEMMA 5.1. *For $i < s$ and natural j we have $A_s \pi^{-d_i} \overline{x}_{jm_i} \equiv \pi^{-d_i} \overline{x}_{jm_i}$ $(\operatorname{mod} P)$. Equivalently $A_s|_{L_i} = \mathrm{id}_{L_i}$.*

Proof. We have $\overline{x}_{jm_i + m_s} = \Phi^{m_s}(\overline{x}_{jm_i}) = \overline{x}_{m_s} + A_s \overline{x}_{jm_i}$ plus terms of degree ≥ 2 in $\overline{x}_{jm_i}$. By Lemma 4.3 we have $w(\overline{x}_{jm_i}) \geq d_i$. So $\overline{x}_{jm_i+m_s} \equiv \overline{x}_{m_s} + A_s \overline{x}_{jm_i}$ $(\operatorname{mod} P^{2d_i})$. From Lemma 4.1 we get $\overline{x}_{jm_i+m_s} \equiv \overline{x}_{jm_i}$ $(\operatorname{mod} P^{d_s})$. Finally, since $d_s > d_i$, we get $A_s \overline{x}_{jm_i} \equiv \overline{x}_{jm_i}$ $(\operatorname{mod} P^{d_i+1})$ and by division by π^{d_i}, we get the statement. ∎

LEMMA 5.2. *We have $L_i \cap (L_1 + \ldots + L_{i-1}) = \{\overline{0}\}$ for $i \leq r$. In other words the sum $L_1 + \ldots + L_r$ is direct. Moreover $L_i \neq \{\overline{0}\}$ and $\dim L_i = \min\{s : \pi^{-d_i} \overline{x}_{(s+1)m_i} + PR^N \in \mathrm{Lin}(\pi^{-d_i} \overline{x}_{sm_i} + PR^N, \pi^{-d_i} \overline{x}_{(s-1)m_i} + PR^N, \ldots, \pi^{-d_i} \overline{x}_{m_i} + PR^N)\}$.*

Proof. Notice that Lemma 4.6 gives

$$\overline{0} = \overline{x}_m = \overline{x}_{(m/m_i)m_i} \equiv (A_i^{m/m_i - 1} + \ldots + A_i + I)\overline{x}_{m_i} \ (\operatorname{mod} P^{2d_i})$$

and

$$(A_i^{m/m_i - 1} + \ldots + A_i + I)(\pi^{-d_i} \overline{x}_{m_i} + PR^N) = \overline{0}.$$

As for $t \geq 0$ the operators $A_i^{m/m_i - 1} + \ldots + A_i + I$ and $A_i^{t-1} + \ldots + A_i + I$ commute we then have

$$(A_i^{m/m_i - 1} + \ldots + A_i + I)(A_i^{t-1} + \ldots + A_i + I)(\pi^{-d_i} \overline{x}_{m_i} + PR^N) = \overline{0}$$

and again using Lemma 4.6,

$$(A_i^{m/m_i - 1} + \ldots + A_i + I)(\pi^{-d_i} \overline{x}_{tm_i} + PR^N) = \overline{0}.$$

So finally $(A_i^{m/m_i - 1} + \ldots + A_i + I)|_{L_i} = 0$.

For $\overline{y} \in L_i \cap (L_1 + \ldots + L_{i-1})$ we thus have, owing to Lemma 5.1,

$$\overline{0} = (A_i^{m/m_i - 1} + \ldots + A_i + I)\overline{y} = \frac{m}{m_i}\, \overline{y}.$$

As m/m_i is not 0 in R/P we thus obtain $\overline{y} = \overline{0}$.

Let s be the minimal natural such that $\pi^{-d_i} \overline{x}_{(s+1)m_i} + PR^N \in \mathrm{Lin}(\pi^{-d_i} \overline{x}_{jm_i} + PR^N : 1 \leq j \leq s)$. To obtain the asserted formula for $\dim L_i$ it suffices to show for $t \geq s+1$ that

$$\pi^{-d_i} \overline{x}_{tm_i} + PR^N \in \mathrm{Lin}(\pi^{-d_i} \overline{x}_{(t-1)m_i} + PR^N, \ldots, \pi^{-d_i} \overline{x}_{m_i} + PR^N).$$

From the very definition of s this holds for $t = s+1$. Assume that it holds for some $t \geq s+1$. This gives

$$A_i \pi^{-d_i} \overline{x}_{tm_i} + PR^N \in \mathrm{Lin}(A_i \pi^{-d_i} \overline{x}_{(t-1)m_i} + PR^N, \ldots, A_i \pi^{-d_i} \overline{x}_{m_i} + PR^N).$$

As for $l \geq 0$ we have $\overline{x}_{(l+1)m_i} \equiv \overline{x}_{m_i} + A_i \overline{x}_{lm_i} \pmod{P^{2d_i}}$ we get

$$\pi^{-d_i}\overline{x}_{(l+1)m_i} + PR^N = \pi^{-d_i}\overline{x}_{m_i} + A_i \pi^{-d_i}\overline{x}_{lm_i} + PR^N \tag{1}$$

and

$$A_i \pi^{-d_i}\overline{x}_{lm_i} + PR^N \in \mathrm{Lin}(\pi^{-d_i}\overline{x}_{(l+1)m_i} + PR^N, \pi^{-d_i}\overline{x}_{m_i} + PR^N). \tag{2}$$

Hence we obtain

$$\begin{aligned}\pi^{-d_i}\overline{x}_{(t+1)m_i} + PR^N &= \pi^{-d_i}\overline{x}_{m_i} + A_i \pi^{-d_i}\overline{x}_{tm_i} + PR^N \\ &\in \mathrm{Lin}(\pi^{-d_i}\overline{x}_{m_i} + PR^N, A_i\pi^{-d_i}\overline{x}_{(t-1)m_i} + PR^N, \ldots, A_i\pi^{-d_i}\overline{x}_{m_i} + PR^N).\end{aligned}$$

From this and (2) we get the statement of the lemma. ∎

Lemma 5.3. *$A_i - I$ is invertible on L_i and*

$$\begin{aligned}\frac{m_{i+1}}{m_i} &= \min\{M : A_i^M = I \text{ on } L_i\} \\ &= \min\{M : A_i^{M-1} + \ldots + A_i + I = 0 \text{ on } L_i\}.\end{aligned}$$

A similar relation holds for m/m_r.

Proof. From the proof of Lemma 5.2 we have $A_i^{m/m_i-1} + \ldots + A_i + I = 0$ on L_i and $(A_i^{m/m_i-1} - I) + \ldots + (A_i - I) = -(m/m_i)I$ on L_i. As $m/m_i \notin P$ it follows that $A_i - I$ is invertible on L_i. So $A_i^{M-1} + \ldots + A_i + I|_{L_i} = 0$ if and only if $(A_i^M - I)|_{L_i} = 0$.

For $M \geq 1$ we have $A_i^{M-1} + \ldots + A_i + I|_{L_i} = 0$ if and only if

$$(A_i^{M-1} + \ldots + A_i + I)\pi^{-d_i}\overline{x}_{m_i} \in PR^N.$$

The statement now follows from Lemma 4.7. ∎

From (1) it follows that

$$L_i = \mathrm{Lin}(\pi^{-d_i}\overline{x}_{m_i} + PR^N, A_i\pi^{-d_i}\overline{x}_{m_i} + PR^N, A_i^2\pi^{-d_i}\overline{x}_{m_i} + PR^N, \ldots).$$

To finish the proof of Proposition 5.1 notice that

$$m = \frac{m_2}{m_1} \cdot \frac{m_3}{m_2} \cdot \ldots \cdot \frac{m}{m_r}$$

with, according to Lemma 5.3, $m_2/m_1 \in \mathcal{H}(R/P, l_1), \ldots, m/m_r \in \mathcal{H}(R/P, l_r)$, where $\dim L_i = l_i$ (clearly L_i is isomorphic to $(R/P)^{l_i}$). The statement of the proposition now follows from Lemma 5.2. ∎

6. $(*)$-cycles of length p^α

Proposition 6.1. *Let $\overline{0} = \overline{x}_0, \overline{x}_1, \ldots, \overline{x}_{p^\alpha - 1}$ be a $(*)$-cycle for a polynomial mapping Φ. Then*

$$\alpha < \lceil \log_p(p^{Z(\lceil \log_2 e \rceil)} + N) \rceil + 1 + \log_p \frac{N(e+1)}{p-1},$$

where $Z(k)$ is defined in Section 3.

Proof. Put $w(\overline{x}_{p^r}) = d_r, A_r = (\Phi^{p^r})'(\overline{0})$. In particular $d_r = \infty$ for $r \geq \alpha$.

LEMMA 6.1. *For any $k > l \geq 0$, we have*

$$\overline{x}_{p^k} \equiv \sum_{v=0}^{p^{k-l}-1} A_l^v \overline{x}_{p^l} \equiv \sum_{v=0}^{p^{k-l}-1} \binom{p^{k-l}}{v} (A_l - I)^{p^{k-l}-1-v} \overline{x}_{p^l} \pmod{P^{2d_l}},$$

$$d_k \geq \min\{2d_l, d_l + e, w((A_l - I)^{p^{k-l}-1} \overline{x}_{p^l})\},$$

$$w((A_l - I)^{p^{k-l}-1} \overline{x}_{p^l}) \geq \min\{d_k, 2d_l, d_l + e\}.$$

Proof. The congruences follow from Lemma 4.6 and from the identity $\sum_{v=0}^{n-1} X^v = \sum_{v=0}^{n-1} \binom{n}{v} (X-1)^{n-1-v}$. The inequalities follow from the second congruence upon observing that $w(p) = e$. ∎

LEMMA 6.2. *Let A be an $N \times N$ matrix with coefficients from R. Let $\overline{x} \in R^N$ with $w(\overline{x}) = d$ and r be a natural number. Assume that $A^M \overline{x} \equiv \overline{0} \pmod{P^{d+r}}$ for some natural M. Then $A^{Nr} \overline{x} \equiv \overline{0} \pmod{P^{d+r}}$.*

Proof. Induction on r. For $r = 0$ this clearly holds. Now assume that it holds for all $r \leq s$ and all possible A, $\overline{x}$, d. So for some M we have $A^M \overline{x} \equiv \overline{0} \pmod{P^{d+s+1}}$. Then A acts on $L = \mathrm{Lin}(\pi^{-d}\overline{x} + PR^N, A(\pi^{-d}\overline{x} + PR^N), A^2(\pi^{-d}\overline{x} + PR^N), \ldots)$, which is a subspace of $(R/P)^N$. We see that A is nilpotent on L, the dimension of L is $\leq N$, so we get $A^N|_L = 0$. This means $A^N(\pi^{-d}\overline{x} + PR^N) = \overline{0}$ or equivalently $A^N \overline{x} \equiv \overline{0} \pmod{P^{d+1}}$.

Put $w(A^N \overline{x}) = d + m$. So $m \geq 1$.

If $m \geq s + 1$ then $A^N \overline{x} \equiv \overline{0} \pmod{P^{d+s+1}}$ and clearly $A^{N(s+1)} \overline{x} \equiv \overline{0} \pmod{P^{d+s+1}}$.

If $m \leq s$ then we use the inductive assumption for $A^N \overline{x}$ instead of $\overline{x}$ and $s + 1 - m$ instead of r. Hence $A^{N(s+1-m)} A^N \overline{x} \equiv \overline{0} \pmod{P^{d+m+s+1-m}}$ and, as $N(s+1) \geq N(s+1-m) + N$, we get $A^{N(s+1)} \overline{x} \equiv \overline{0} \pmod{P^{d+s+1}}$. ∎

LEMMA 6.3. *We have $d_{Z(k)} \geq 2^k$ for $k \leq \lceil \log_2 e \rceil$.*

Proof. Recall that $\lceil x \rceil$ and $Z(k)$ were defined in Section 3. For $k = 0$ we have $Z(0) = 0; d_0 = w(\overline{x}_1) \geq 1$ (as we consider $(*)$-cycles). Assume that for some $k \leq \log_2 e$ we have $d_{Z(k)} \geq 2^k$ and consider $d_{Z(k+1)}$ with $k + 1 \leq \lceil \log_2 e \rceil$. For $r > Z(k)$, Lemma 6.1 yields

$$d_r \geq \min\{2d_{Z(k)}, d_{Z(k)} + e, w((A_{Z(k)} - I)^{p^{r-Z(k)}-1} \overline{x}_{p^{Z(k)}})\}. \tag{3}$$

For $\beta > \max\{Z(k), \alpha\}$, Lemma 6.1 implies

$$w((A_{Z(k)} - I)^{p^{\beta-Z(k)}-1} \overline{x}_{p^{Z(k)}}) \geq d_{Z(k)} + 2^k,$$

whence by Lemma 6.2,

$$w((A_{Z(k)} - I)^{2^k N} \overline{x}_{p^{Z(k)}}) \geq d_{Z(k)} + 2^k.$$

Since $p^{Z(k+1)-Z(k)} - 1 \geq 2^k N$ we have

$$w((A_{Z(k)} - I)^{p^{Z(k+1)-Z(k)}-1}\overline{x}_{p^{Z(k)}}) \geq d_{Z(k)} + 2^k.$$

Now taking $r = Z(k+1)$ in (3) we arrive at

$$d_{Z(k+1)} \geq \min\{2d_{Z(k)}, d_{Z(k)} + e, d_{Z(k)} + 2^k\} \geq 2^{k+1}. \blacksquare$$

LEMMA 6.4. *$A_k \equiv A_l^{p^{k-l}} \pmod{P^{d_l}}$ for $0 \leq l \leq k$, which means that all entries of A_k are congruent $\pmod{P^{d_l}}$ to the corresponding entries of $A_l^{p^{k-l}}$.*

Proof. We have

$$A_k = (\Phi^{p^k})'(\overline{0}) = \prod_{j=0}^{p^{k-l}-1} (\Phi^{p^l})'(\overline{x}_{jp^l}) \equiv ((\Phi^{p^l})'(\overline{0}))^{p^{k-l}} \equiv A_l^{p^{k-l}} \pmod{P^{d_l}},$$

as from Lemma 4.3, $\overline{x}_{jp^l} \equiv \overline{0} \pmod{P^{d_l}}$ and therefore $(\Phi^{p^l})'(\overline{x}_{jp^l}) \equiv (\Phi^{p^l})'(\overline{0})$ $\pmod{P^{d_l}}$. $\blacksquare$

LEMMA 6.5. *Let m be such that $d_m \geq e$. Then $d_{\lceil \log_p(p^m+N)\rceil} \geq e+1$.*

Proof. For $m \geq \alpha$ this is obvious. So let $m < \alpha$. Lemma 6.1 gives

$$\begin{aligned} w((A_m - I)^{p^{\alpha-m}-1}\overline{x}_{p^m}) &\geq \min\{d_\alpha, 2d_m, d_m + e\} = \min\{\infty, 2d_m, d_m + e\} \\ &\geq d_m + 1. \end{aligned}$$

By Lemma 6.4 we have $A_m \equiv A_0^{p^m} \pmod{P}$. Hence

$$\begin{aligned} \overline{0} &\equiv (A_m - I)^{p^{\alpha-m}-1}\overline{x}_{p^m} \equiv (A_0^{p^m} - I)^{p^{\alpha-m}-1}\overline{x}_{p^m} \\ &\equiv (A_0 - I)^{(p^{\alpha-m}-1)p^m}\overline{x}_{p^m} \pmod{P^{d_m+1}}. \end{aligned}$$

Now we use Lemma 6.2 to obtain $(A_0 - I)^N\overline{x}_{p^m} \equiv \overline{0} \pmod{P^{d_m+1}}$. Note that $\beta = \lceil \log_p(p^m + N)\rceil$ is bigger than m and $(p^{\beta-m} - 1)p^m \geq N$. Hence

$$(A_m - I)^{p^{\beta-m}-1}\overline{x}_{p^m} \equiv (A_0 - I)^{(p^{\beta-m}-1)p^m}\overline{x}_{p^m} \equiv \overline{0} \pmod{P^{d_m+1}}.$$

Having this we apply Lemma 6.1 to obtain $d_\beta \geq \min\{2d_m, d_m+e, d_m+1\} \geq e+1$. $\blacksquare$

LEMMA 6.6. *Let $m \geq \log_p N$ be such that $d_m \geq e+1$. Then*

$$\alpha < m + 1 + \log_p \frac{N(e+1)}{p-1}.$$

Proof. We may assume that $\alpha > m$. Applying Lemma 6.1 (with $k = \alpha$, $l = \alpha - 1$), we obtain

$$\overline{0} = \overline{x}_{p^\alpha} \equiv \sum_{v=0}^{p-1} \binom{p}{v} (A_{\alpha-1} - I)^{p-v-1}\overline{x}_{p^{\alpha-1}} \pmod{P^{2d_{\alpha-1}}}; \tag{4}$$

in particular

$$\overline{0} \equiv (A_{\alpha-1} - I)^{p-1}\overline{x}_{p^{\alpha-1}} \pmod{P^{d_{\alpha-1}+1}}.$$

Since $(A_{\alpha-1}-I)^{p-1} \equiv (A_0^{p^{\alpha-1}}-I)^{p-1} \equiv (A_0-I)^{p^{\alpha-1}(p-1)} \pmod{P}$, we obtain

$$\overline{0} \equiv (A_0 - I)^{p^{\alpha-1}(p-1)}\overline{x}_{p^{\alpha-1}} \pmod{P^{d_{\alpha-1}+1}}$$

and therefore, by Lemma 6.2, $(A_0 - I)^N\overline{x}_{p^{\alpha-1}} \equiv \overline{0} \pmod{P^{d_{\alpha-1}+1}}$. Since $p^{\alpha-1} \geq p^m \geq N$, we get

$$(5) \qquad (A_{\alpha-1} - I)\overline{x}_{p^{\alpha-1}} \equiv (A_0 - I)^{p^{\alpha-1}}\overline{x}_{p^{\alpha-1}} \equiv (A_0 - I)^{p^m}\overline{x}_{p^{\alpha-1}} \equiv (A_m - I)\overline{x}_{p^{\alpha-1}} \equiv \overline{0} \pmod{P^{d_{\alpha-1}+1}}.$$

Applying $A_{\alpha-1} - I$ to (4) yields

$$(A_{\alpha-1} - I)^p\overline{x}_{p^{\alpha-1}} \equiv -\sum_{v=1}^{p-1}\binom{p}{v}(A_{\alpha-1} - I)^{p-v}\overline{x}_{p^{\alpha-1}} \equiv \overline{0} \pmod{P^{d_{\alpha-1}+e+1}}.$$

Since $d_m \geq e+1$, Lemma 6.4 implies $A_m^{p^{\alpha-m-1}} \equiv A_{\alpha-1} \pmod{P^{e+1}}$, and therefore using (5) we get

$$\begin{aligned}\overline{0} &\equiv (A_m^{p^{\alpha-1-m}} - I)^p\overline{x}_{p^{\alpha-1}} \\ &\equiv \Bigg(\sum_{v=0}^{p^{\alpha-1-m}-1}\binom{p^{\alpha-1-m}}{v}(A_m - I)^{p^{\alpha-1-m}-v}\Bigg)^p\overline{x}_{p^{\alpha-1}} \\ &\equiv (A_m - I)^{p^{\alpha-m}}\overline{x}_{p^{\alpha-1}} \pmod{P^{d_{\alpha-1}+e+1}}.\end{aligned}$$

Suppose now that $p^{\alpha-m-1}(p-1) \geq (e+1)N$. Then Lemma 6.2 implies

$$\overline{0} \equiv (A_m - I)^{p^{\alpha-m-1}(p-1)}\overline{x}_{p^{\alpha-1}} \pmod{P^{d_{\alpha-1}+e+1}}$$

and therefore, by Lemma 6.4 and (5),

$$\begin{aligned}(A_{\alpha-1} - I)^{p-1}\overline{x}_{p^{\alpha-1}} &\equiv (A_m^{p^{\alpha-1-m}} - I)^{p-1}\overline{x}_{p^{\alpha-1}} \\ &= \Bigg(\sum_{v=0}^{p^{\alpha-1-m}-1}\binom{p^{\alpha-1-m}}{v}(A_m - I)^{p^{\alpha-1-m}-v}\Bigg)^{p-1}\overline{x}_{p^{\alpha-1}} \\ &\equiv (A_m - I)^{p^{\alpha-1-m}(p-1)}\overline{x}_{p^{\alpha-1}} \equiv \overline{0} \pmod{P^{d_{\alpha-1}+e+1}}.\end{aligned}$$

By (4) and (5) we then obtain

$$\begin{aligned}\overline{0} &\equiv (A_{\alpha-1} - I)^{p-1}\overline{x}_{p^{\alpha-1}} \equiv -\sum_{v=1}^{p-1}\binom{p}{v}(A_{\alpha-1} - I)^{p-v-1}\overline{x}_{p^{\alpha-1}} \\ &\equiv -p\overline{x}_{p^{\alpha-1}} \pmod{P^{d_{\alpha-1}+e+1}},\end{aligned}$$

contradicting $w(p\overline{x}_{p^{\alpha-1}}) = d_{\alpha-1}+e$. Hence $(e+1)N > p^{\alpha-m-1}(p-1)$, which is equivalent to the assertion. ∎

To finish the proof of the proposition notice that Lemma 6.3 leads to $d_{Z(\lceil\log_2 e\rceil)} \geq e$ and, by Lemma 6.5, $d_{\lceil\log_p(p^{Z(\lceil\log_2 e\rceil)}+N)\rceil} \geq e+1$. As of course $\lceil\log_p(p^{Z(\lceil\log_2 e\rceil)} + N)\rceil \geq \log_p N$, Lemma 6.6 finally yields the statement. ∎

7. Proof of Theorem 3.1

7.1. *Proof of Theorem 3.1(i).* Theorem 3.1(i) follows directly from Propositions 5.1 and 6.1 because if we have a $(*)$-cycle of length mp^α then there is a $(*)$-cycle of length m and there is a $(*)$-cycle of length p^α (this follows directly from Lemma 4.1(ii)).

7.2. *Proof of Theorem 3.1(ii).* Note that the numbers $h_i \in \mathcal{H}(R/P, l_i)$ satisfy $h_i \le p^{fl_i} - 1$ and $\prod_{i=1}^r h_i \le (p^{fl_1} - 1) \ldots (p^{fl_r} - 1) < p^{f(l_1+\ldots+l_r)} \le p^{fN}$. The rest follows from Theorem 3.1(i) and Lemma 4.4.

7.3. *Proof of Theorem 3.1(iii).* Note that in the passage from R to $\widehat{R}$ the number f is preserved. Having a $(*)$-cycle of a given length in R^r by extending by zeros we obtain a $(*)$-cycle of the same length in R^N. So in view of Lemma 4.4 and Proposition 4.1 it suffices to find a $(*)$-cycle of length $p^{fN} - 1$ in R^N for a complete R. As the statement of this point is clear for $p^{fN} - 1 = 1$, we assume that $p^{fN} - 1 > 1$.

Let a field S be a finite extension of R/P of degree N. Let ξ_0 be a generator of the multiplicative group $S \setminus \{0\}$. Then the minimal monic polynomial $f \in (R/P)[X]$ of ξ_0 over R/P is of degree N. Write $X^{p^{fN}-1} - 1 = f(X)g(X)$ with relatively prime polynomials f, g. From the Hensel lemma there are $F, G \in R[X]$ such that $X^{p^{fN}-1} - 1 = F(X)G(X)$ where $F \pmod{P} = f$, $G \pmod{P} = g, \deg F = N, F$ monic. Clearly F is irreducible.

Let ξ be such that $F(\xi) = 0$. We have a bijection $j : R^N \to R[\xi]$ given by

$$j(x_1, \ldots, x_N) = x_1 + x_2\xi + \ldots + x_N\xi^{N-1}.$$

Let $\Lambda : R[\xi] \to R[\xi]$ be multiplication by ξ. It is easy to check that $j^{-1}\Lambda j : R^N \to R^N$ is a polynomial mapping (even linear).

Let r be the smallest natural such that $\xi^r = 1$. So $F(X) \mid X^r - 1$ and $f(X) \mid X^r - 1$. Hence $\xi_0^r = 1$ and this gives $p^{fN} - 1 \le r$. So $1, \xi, \ldots, \xi^{p^{fN}-2}$ are pairwise different elements of $R[\xi]$. The tuple $j^{-1}(p), j^{-1}(\xi p), \ldots, j^{-1}(\xi^{p^{fN}-2}p)$ is a cycle of length $p^{fN} - 1$ for $j^{-1}\Lambda j$. It is a $(*)$-cycle as $j^{-1}(\xi p) - j^{-1}(p) = (0, p, 0, \ldots, 0) - (p, 0, 0, \ldots, 0)$ for $N \ge 2$ and $(\xi - 1)p$ for $N = 1$. Notice that for $N = 1$ the number ξ lies in R.

8. Proof of Corollary 3.1. The first estimate in the corollary follows from Theorem 3.1(ii), as we can embed Z_K into $(Z_K)_\mathfrak{p}$. We have $2Z_K = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_t^{e_t}$. Set $f_1 = [Z_K/\mathfrak{P}_1 : \mathbb{Z}/2\mathbb{Z}]$. We consider Z_K as a subring of $(Z_K)_{\mathfrak{P}_1}$, which satisfies the assumptions of Theorem 3.1 with $p = 2, e = e_1, f = f_1, ef \le n$. So Theorem 3.1(ii) gives

$$B(Z_K, N) \le 2^{fN}(2^{fN} - 1)2^{\lceil \log_2(2^{Z(\lceil \log_2 e \rceil)} + N) \rceil + 1 + \log_2(N(e+1))}.$$

Taking into account the definition of $Z(k)$ we easily arrive at the statement of the corollary, considering separately the cases $f = n$, $e = 1$ and $f \le n/2, e \le n$.

9. Proof of Theorem 3.2. The equality $\mathcal{CYCL}(R_{\mathfrak{p}}, N) = \mathcal{CYCL}(\widehat{R}_{\mathfrak{p}}, N)$ follows from Proposition 4.1, as $R_{\mathfrak{p}}$ is a discrete valuation ring. Clearly, $\mathcal{CYCL}(R, N) \subset \mathcal{CYCL}(R_{\mathfrak{p}}, N)$ for all $\mathfrak{p} \in \mathcal{P}(R)$.

Suppose now that $k \in \mathcal{CYCL}(R_{\mathfrak{p}}, N)$ for all $\mathfrak{p} \in \mathcal{P}(R)$, and let $\mathcal{B} \subset \mathcal{P}(R)$ be a finite non-empty set such that $\#(R/\mathfrak{p}) \ge k$ for all $\mathfrak{p} \in \mathcal{P}(R) \setminus \mathcal{B}$ and for some positive $\alpha(\mathfrak{p})$ the ideal $\prod_{\mathfrak{p}\in\mathcal{B}} \mathfrak{p}^{\alpha(\mathfrak{p})}$ is principal. For each $\mathfrak{p} \in \mathcal{B}$, let $\overline{x}_{\mathfrak{p},0}, \ldots, \overline{x}_{\mathfrak{p},k-1}$ be a cycle of some polynomial mapping $\Phi_{\mathfrak{p}} : R_{\mathfrak{p}}^N \to R_{\mathfrak{p}}^N$. We set $\Phi_{\mathfrak{p}} = (\Phi_{\mathfrak{p}}^{(1)}, \ldots, \Phi_{\mathfrak{p}}^{(N)})$, where $\Phi_{\mathfrak{p}}^{(r)} \in R_{\mathfrak{p}}[X_1, \ldots, X_N]$ and $\overline{x}_{\mathfrak{p},i} = (x_{\mathfrak{p},i}^{(1)}, \ldots, x_{\mathfrak{p},i}^{(N)})$ with $x_{\mathfrak{p},i}^{(r)} \in R_{\mathfrak{p}}$. According to Lemma 4.1(v), we may assume that $x_{\mathfrak{p},i}^{(r)} \ne x_{\mathfrak{p},v}^{(s)}$ whenever $(i, r) \ne (v, s)$.

For $\mathfrak{p} \in \mathcal{P}(R)$, let $w_{\mathfrak{p}} : R_{\mathfrak{p}} \to \mathbb{Z} \cup \{\infty\}$ be the (surjective) exponent of $R_{\mathfrak{p}}$, i.e. $w_{\mathfrak{p}}(R_{\mathfrak{p}}) = \{\infty, 0, 1, 2, \ldots\}$. Let $M \in R$ be such that

$$w_{\mathfrak{p}}(M) > w_{\mathfrak{p}}\Big(\prod_{(i,r)\ne(v,s)} (x_{\mathfrak{p},i}^{(r)} - x_{\mathfrak{p},v}^{(s)})\Big) \quad \text{for all } \mathfrak{p} \in \mathcal{B}$$

and $w_{\mathfrak{p}}(M) = 0$ for all $\mathfrak{p} \in \mathcal{P}(R) \setminus \mathcal{B}$ (the existence of such an M clearly follows from the properties of $\mathcal{B}$). Our construction depends on a suitable approximation of the elements $x_{\mathfrak{p},i}^{(r)}$ by elements from R which is supplied by the following lemma.

LEMMA 9.1. *There exist elements* $x_i^{(r)}$ *of* R *such that* $w_{\mathfrak{p}}(x_{\mathfrak{p},i}^{(r)} - x_i^{(r)}) \ge k w_{\mathfrak{p}}(M)$ *for all* (i, r) *and* $\mathfrak{p} \in \mathcal{B}$ *and*

$$\min\Big\{w_{\mathfrak{p}}(x_i^{(1)} - x_v^{(1)}), w_{\mathfrak{p}}\Big(\prod_{r\ne s}(x_r^{(2)} - x_s^{(2)})\Big)\Big\} = 0$$

for $0 \le v < i \le k-1$ *and all* $\mathfrak{p} \in \mathcal{P}(R) \setminus \mathcal{B}$.

Proof. Let $z_i^{(r)} \in R$ be such that $w_{\mathfrak{p}}(x_{\mathfrak{p},i}^{(r)} - z_i^{(r)}) \ge k w_{\mathfrak{p}}(M)$ for all (i, r) and $\mathfrak{p} \in \mathcal{B}$. We shall construct elements $a_0, a_1, \ldots, a_{k-1} \in R$ such that

$$(6)\quad \min\Big\{w_{\mathfrak{p}}((z_i^{(1)} + M^k a_i) - (z_v^{(1)} + M^k a_v)), w_{\mathfrak{p}}\Big(\prod_{r\ne s}(z_r^{(2)} - z_s^{(2)})\Big)\Big\} = 0$$

for all $i \ne v$ and $\mathfrak{p} \in \mathcal{P}(R) \setminus \mathcal{B}$. Once this is done, we set $x_i^{(1)} = z_i^{(1)} + M^k a_i$ and $x_i^{(r)} = z_i^{(r)}$ for $r \ge 2$, and the lemma follows.

We set $a_0 = 0$ and suppose that for some $1 \le l \le k-1$ we have already constructed $a_0, a_1, \ldots, a_{l-1}$ such that (6) holds for $0 \le v < i \le l-1$ and all $\mathfrak{p} \in \mathcal{P}(R) \setminus \mathcal{B}$. Since the elements $z_i^{(r)}$ are pairwise distinct by construction, the set $\mathcal{B}'$ of all $\mathfrak{p} \in \mathcal{P}(R) \setminus \mathcal{B}$ satisfying

$$w_{\mathfrak{p}}\Big(\prod_{r \neq s}(z_r^{(2)} - z_s^{(2)})\Big) > 0$$

is finite. Hence it suffices to determine a_l such that, for all $\mathfrak{p} \in \mathcal{B}'$,

$$w_{\mathfrak{p}}(z_l^{(1)} - z_v^{(1)} + M^k(a_l - a_v)) = 0 \quad \text{for } 0 \le v < l.$$

For each $\mathfrak{p} \in \mathcal{B}'$, we have $M^k \notin \mathfrak{p}$ and $\#(R/\mathfrak{p}) \ge k > l$, and therefore there exists $a_{l,\mathfrak{p}} \in R_{\mathfrak{p}}$ such that $w_{\mathfrak{p}}(z_l^{(1)} - z_v^{(1)} + M^k(a_{l,\mathfrak{p}} - a_v)) = 0$ for $0 \le v < l$. Choosing $a_l \in R$ such that $a_l \equiv a_{l,\mathfrak{p}} \pmod{\mathfrak{p}R_{\mathfrak{p}}}$ for all $\mathfrak{p} \in \mathcal{B}'$ yields the assertion. ∎

Let now $x_i^{(r)} \in R$ be as in Lemma 9.1, set $\overline{x}_i = (x_i^{(1)}, \ldots, x_i^{(N)}) \in R^N$ and construct a polynomial mapping $\Phi = (\Phi^{(1)}, \ldots, \Phi^{(N)}) : R^N \to R^N$ such that $\overline{x}_0, \ldots, \overline{x}_{k-1}$ is a cycle of Φ. Let $\overline{\Phi}^{(r)} \in R[X_1, \ldots, X_N]$ be any polynomials satisfying $\overline{\Phi}^{(r)} \equiv \Phi_{\mathfrak{p}}^{(r)} \pmod{M^k R_{\mathfrak{p}}[X_1, \ldots, X_N]}$ for $\mathfrak{p} \in \mathcal{B}$. Put

$$\Phi^{(r)}(X_1, \ldots, X_N) = M^k b_0^{(r)} + \sum_{j=1}^{k-1} M^{k-j}\Big[b_j^{(r)} \prod_{v=0}^{j-1}(X_1 - x_v^{(1)}) + B_j^{(r)} \prod_{v=0}^{j-1}(X_2 - x_v^{(2)})\Big] + \overline{\Phi}^{(r)}(X_1, \ldots, X_N)$$

with suitable coefficients $b_j^{(r)}, B_j^{(r)} \in R$. We must determine these coefficients in such a way that

$$(7) \quad x_{i+1}^{(r)} = \Phi^{(r)}(x_i^{(1)}, \ldots, x_i^{(N)}) = M^k b_0^{(r)} + \sum_{j=1}^{i} M^{k-j}\Big[b_j^{(r)} \prod_{v=0}^{j-1}(x_i^{(1)} - x_v^{(1)}) + B_j^{(r)} \prod_{v=0}^{j-1}(x_i^{(2)} - x_v^{(2)})\Big] + \Phi^{(r)}(x_i^{(1)}, \ldots, x_i^{(N)})$$

for all $0 \le i \le k-1$ and $1 \le r \le N$ (where $x_k^{(r)} = x_0^{(r)}$). For $i = 0$, (7) reduces to $x_1^{(r)} = M^k b_0^{(r)} + \overline{\Phi}^{(r)}(x_0^{(1)}, \ldots, x_0^{(N)})$, which has a solution $b_0^{(r)} \in R$ since by construction $w_{\mathfrak{p}}(x_1^{(r)} - \overline{\Phi}^{(r)}(x_0^{(1)}, \ldots, x_0^{(N)})) \ge w_{\mathfrak{p}}(M^k)$ for all $\mathfrak{p} \in \mathcal{P}(R)$.

Suppose now that, for some $l \le k-1$, the coefficients $b_j^{(r)}, B_j^{(r)} \in R$ have been determined for $j \le l-1$ such that (7) holds for $i \le l-1$. We must find $b_l^{(r)}, B_l^{(r)}$ such that

$$A_1 b_l^{(r)} + A_2 B_l^{(r)} = A,$$

where for $s \in \{1,2\}$,

$$A_s = M^{k-l} \prod_{v=0}^{l-1} (x_l^{(s)} - x_v^{(s)}),$$

$$A = x_{l+1}^{(r)} - \sum_{j=0}^{l-1} M^{k-j} \Big[b_j^{(r)} \prod_{v=0}^{j-1} (x_l^{(1)} - x_v^{(1)}) + B_j^{(r)} \prod_{v=0}^{j-1} (x_l^{(2)} - x_v^{(2)}) \Big] - \overline{\Phi}^{(r)}(x_l^{(1)}, \ldots, x_l^{(N)}).$$

Hence it is sufficient to prove that, for all $\mathfrak{p} \in \mathcal{P}(R)$,

$$w_{\mathfrak{p}}(A) \ge w_{\mathfrak{p}}(A_1 R + A_2 R) = \min\{w_{\mathfrak{p}}(A_1), w_{\mathfrak{p}}(A_2)\}.$$

If $\mathfrak{p} \notin \mathcal{B}$, then $\min\{w_{\mathfrak{p}}(A_1), w_{\mathfrak{p}}(A_2)\} = 0$ by Lemma 9.1 and we are done. If $\mathfrak{p} \in \mathcal{B}$, then $w_{\mathfrak{p}}(A) \ge (k-l+1) w_{\mathfrak{p}}(M)$ by construction, and we shall prove that, for $s \in \{1,2\}$, $w_{\mathfrak{p}}(A_s) < (k-l+1) w_{\mathfrak{p}}(M)$. Indeed, for $0 \le v \le l-1$ and $\mathfrak{p} \in \mathcal{B}$, we have $x_l^{(s)} - x_v^{(s)} \equiv x_{\mathfrak{p},l}^{(s)} - x_{\mathfrak{p},v}^{(s)} \pmod{\mathfrak{p}^{k w_{\mathfrak{p}}(M)} R_{\mathfrak{p}}}$ and therefore, for $\mathfrak{p} \in \mathcal{B}$, we have

$$A_s \equiv M^{k-l} \prod_{v=0}^{l-1} (x_{\mathfrak{p},l}^{(s)} - x_{\mathfrak{p},v}^{(s)}) \pmod{\mathfrak{p}^{(2k-l) w_{\mathfrak{p}}(M)} R_{\mathfrak{p}}}.$$

By the definition of M, we have $w_{\mathfrak{p}}(\prod_{v=0}^{l-1} (x_{\mathfrak{p},l}^{(s)} - x_{\mathfrak{p},v}^{(s)})) < w_{\mathfrak{p}}(M)$, and since $k-l+1 \le 2k-l$, the assertion follows.

10. Proof of Theorem 3.3. Let m be the middle term appearing in Theorem 3.3(i). Note that $m < 4^{nN}$. Let K be a fixed field of degree n over $\mathbb{Q}$ such that pZ_K are prime ideals for all natural primes $p < 4^n$. Such a field exists owing to a much more general theorem due to Hasse. Lemma 4.4 guarantees that (for $\# Z_K/\mathfrak{p} = p^f$)

$$\{1, 2, \ldots, p^{fN}\} \subset \mathcal{CYCL}((Z_K)_{\mathfrak{p}}, N).$$

Owing to Theorem 3.2, to prove Theorem 3.3(i) it suffices to show that for every non-zero prime ideal $\mathfrak{p}$ of Z_K we have $m \in \mathcal{CYCL}((Z_K)_{\mathfrak{p}}, N)$.

Case 1: $\mathfrak{p}$ *lies above some* pZ_K *with* $p > 4^n$. We then have $p^{fN} \ge p^N > 4^{nN} > m$, so $m \in \mathcal{CYCL}((Z_K)_{\mathfrak{p}}, N)$.

Case 2: $\mathfrak{p} = pZ_K$ *with some* p *such that* $5 \le p \le 4^n$. In this case $p^{fN} = p^{nN} \ge 5^{nN} > m$ and again we are done.

Case 3: $\mathfrak{p} = 3Z_K$. Note that $N - \lceil N \log_3 \frac{3}{2} \rceil \ge 1$ (as $N \ge 2$). Now Theorem 3.1(iii) shows that there is a $(*)$-cycle of length $3^{n(N - \lceil N \log_3 \frac{3}{2} \rceil)} - 1$ in $(Z_K)_{\mathfrak{p}}^N$.

Note that for $N \geq 2, (n, N) \neq (1, 3)$ one has

$$(2^{nN} - 1)\left\lfloor \frac{2^{nN}}{3^{n(N-\lceil N \log_3 \frac{3}{2} \rceil)} - 1} \right\rfloor \leq 3^{nN},$$

so Lemma 4.4 guarantees that for such (n, N) we get $m \in \mathcal{CYCL}((Z_K)_\mathfrak{p}, N)$.

For $(n, N) = (1, 3)$ we have $m = 56 = 14 \cdot 4$, so by Lemma 4.4 we should find a $(*)$-cycle of length 4 in Z_3^3. A tuple $(3, 0, 0)$, $(0, 3, 0)$, $(-3, 0, 0)$, $(0, -3, 0)$ is such a cycle for the mapping $(X, Y, Z) \mapsto (-Y, X, Z)$.

CASE 4: $\mathfrak{p} = 2Z_K$. This case clearly follows from Lemma 4.4 and Theorem 3.1(iii).

The last estimate follows from the consideration of two cases, namely $3^{n(N-\lceil N \log_3 \frac{3}{2} \rceil)} - 1 \leq \frac{1}{2} 2^{nN}$ and $2^{nN} \geq 3^{n(N-\lceil N \log_3 \frac{3}{2} \rceil)} - 1 > \frac{1}{2} 2^{nN}$.

Theorem 3.3(ii) follows from Theorem 3.3(i) and Corollary 3.1; so does Theorem 3.3(iii), as $\mathbb{Q}$ is the only field of degree 1 over $\mathbb{Q}$.

11. Proof of Theorem 3.4

11.1. *Proof of Theorem 3.4(i).* Let $[K : \mathbb{Q}] = n$ and put

$$q_1 = p_1^{f_1}, \ \ldots, \ q_k = p_k^{f_k} \quad (p_i \text{ prime}). \tag{8}$$

Notice that for $y_1 < \ldots < y_k$ we have

$$y_1 < M(y_1, \ldots, y_k) \leq 2y_1$$

(the left inequality follows from $(y_1, \varepsilon, 0, 0, \ldots, 0) \in \Delta(y_1, \ldots, y_k)$ for small ε). Hence $q_1 < \exp(M(\ln q_1, \ldots, \ln q_k))$. The right inequality in Theorem 3.4(i) follows directly from Corollary 3.1.

So we turn to the inequality

$$\exp(M(\ln q_1, \ldots, \ln q_k)) \leq \liminf_N (B(Z_K, N))^{1/N}.$$

Let $(m, m_1, \ldots, m_k)$ be a fixed element in $\Delta(\ln q_1, \ldots, \ln q_k)$ such that

$$m + m_1 + \ldots + m_k = M(\ln q_1, \ldots, \ln q_k).$$

Fix $\varepsilon > 0$. Let N be sufficiently large. Fix $r, r_1, \ldots, r_k$ such that

$$r \in [\exp((1-\varepsilon)mN), \exp(mN)], \quad r_i \in [\exp((1-\varepsilon)m_iN), \exp(m_iN)],$$

and additionally assume that for $m_i > 0$ the number r_i is of the shape $p_i^{n!T_i} - 1$, where T_i is natural. Note that as $m, m_1, \ldots, m_k, p_1, \ldots, p_k, n, \varepsilon$ are fixed such a choice of $r, r_1, \ldots, r_k$ is possible for sufficiently large N. Put $s = rr_1 \ldots r_k$. Notice that

$$s \leq \exp(N(m + m_1 + \ldots + m_k)) \leq \exp(N \cdot 2 \ln q_1) = q_1^{2N}. \tag{9}$$

LEMMA 11.1. $s \in \mathcal{CYCL}(Z_K, N)$.

Proof. According to Theorem 3.2 it suffices to show $s \in \mathcal{CYCL}((Z_K)_\mathfrak{p}, N)$ for all non-zero prime ideals $\mathfrak{p}$ of Z_K.

Case 1: $\#Z_K/\mathfrak{p} > q_1^2$. In this case Lemma 4.4 and (9) give the statement.

Case 2: $\#Z_K/\mathfrak{p} \le q_1^2$. From (8) we infer that $\mathfrak{p}$ lies above $p_j Z$ for some $j \le k$. Write $\#Z_K/\mathfrak{p} = p_j^{F_j}$. By the very definition of $q_1, \ldots, q_k$ and (8) we have

$$n \ge F_j \ge f_j. \tag{10}$$

To get the statement it suffices, by Lemma 4.4, to prove that

$$\frac{s}{r_j} = r r_1 \ldots r_{j-1} r_{j+1} \ldots r_k \le (p_j^{F_j})^N \tag{11}$$

and that r_j is the length of a $(*)$-cycle in $(Z_K)_{\mathfrak{p}}^N$.

Now (11) follows from

$$\begin{aligned}\frac{s}{r_j} &\le \exp(mN)\exp(m_1 N)\ldots\exp(m_{j-1}N)\exp(m_{j+1}N)\ldots\exp(m_k N)\\ &= \exp((m + m_1 + \ldots + m_{j-1} + m_{j+1} + \ldots + m_k)N) \le \exp(N \ln q_j)\\ &= q_j^N = (p_j^{f_j})^N \le (p_j^{F_j})^N.\end{aligned}$$

If $m_j = 0$ then $r_j = 1$ and clearly there is a $(*)$-cycle of length r_j in $(Z_K)_{\mathfrak{p}}^N$. So let $m_j > 0$. By Theorem 3.1(iii) it suffices to prove $U_j = n!T_j/F_j \le N$, which follows from

$$\begin{aligned}U_j = \frac{n!T_j}{F_j} &\le \frac{\ln(\exp(m_j N) + 1)}{F_j \ln p_j} \le \frac{\ln(\exp(N \ln q_j) + 1)}{f_j \ln p_j}\\ &= \frac{\ln(\exp(N \ln q_j) + 1)}{\ln q_j} \le N + \frac{1}{2} \quad \text{for large } N.\end{aligned}$$

Now, as U_j is natural by (10), the lemma follows. ■

To finish the proof note that for large N we have

$$\begin{aligned}B(Z_K, N) \ge s &\ge \exp((1-\varepsilon)(m + m_1 + \ldots + m_k)N)\\ &= \exp((1-\varepsilon)M(\ln q_1, \ldots, \ln q_k)N).\end{aligned}$$

11.2. *Proof of Theorem 3.4(ii).* It suffices to note that by the simplex method for $y_1 < y_2 < y_3$ we have

$$M(y_1, y_2, y_3) = \min\left\{2y_1, \frac{y_1 + y_2 + y_3}{2}\right\} \quad \text{and} \quad M(y_1, y_2) = M(y_1) = 2y_1.$$

11.3. *Proof of Theorem 3.4(iii).* Here we have $q_1 = 2$ and $q_3 \ge 5 \ge 2^2$. So the statement follows from (ii).

References

[Ev] J. H. Evertse, *On equations in S-units and the Thue–Mahler equation*, Invent. Math. 75 (1984), 561–584.

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

[MoSi1] P. Morton and J. Silverman, *Periodic points, multiplicities and dynamical units*, J. Reine Angew. Math. 461 (1995), 81–122.

[MoSi2] —, —, *Rational periodic points of rational functions*, Internat. Math. Res. Notices 1994, no. 2, 97–110.

[Na1] W. Narkiewicz, *Polynomial cycles in algebraic number fields*, Colloq. Math. 58 (1989), 149–153.

[Na2] —, *Polynomial Mappings*, Lecture Notes in Math. 1600, Springer, Berlin, 1995.

[Na3] —, *Arithmetics of dynamical systems, a survey*, Tatra Mt. Math. Publ. 11 (1997), 69–76.

[NeRo] M. Nevins and T. D. Rogers, *Quadratic maps as dynamical systems on the p-adic numbers*, preprint, 2000.

[No] D. G. Northcott, *Periodic points on an algebraic variety*, Ann. of Math. 51 (1950), 167–177.

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

[Pe2] —, *Cycles of polynomial mappings in several variables*, Manuscripta Math. 83 (1994), 279–289.

[Zi] M. Zieve, Ph.D. thesis, 1997.

Mathematical Institute
University of Wrocław
Pl. Grunwaldzki 2/4
50-384 Wrocław, Poland
E-mail: pezda@math.uni.wroc.pl

Received on 15.11.2001
and in revised form on 10.5.2002 (4152)