Seoul National University 2024 Fall

Research Internship

Periodic Orbits of Nontrivial Types

Younghun Jo

Department: Mathematical Sciences

September 24, 2024

Contents

1 Notations and Terminologies **1**

2 Properties of Periodic Orbits **1**

3 Orbit Extension **2**

4 Periodic Orbits of Linear Maps **3**

5 Orbits of Nontrivial Types **4**

5.1 Orbits of Type $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ 4

5.2 Orbits of Type $\widetilde{F}$ 4

References **4**

In this article, we prove the existence of periodic orbits of polynomial maps on $\mathbb{Z}^2$ of certain nontrivial types. Our method is based on the local–global principle originated from [2, Theorem 3.2], and the construction from [2, Lemma 4.4] for periodic orbits of polynomial maps.

1 Notations and Terminologies

Let R be a commutative ring with unity of characteristic zero, and N be a positive integer. For a collection of endomorphisms $S \subseteq \operatorname{End}(R^N)$, generating a monoid $\langle S \rangle$ under composition, we call a subset $\mathcal{O} \subseteq R^N$ an *S-orbita*[1] if $\langle S \rangle$ acts on $\mathcal{O}$ by permutations. For a point $x \in R^N$, the S-orbita

$$\mathcal{O}_S(x) = \{f(x) : f \in \langle S \rangle\}$$

generated by x is called the *S-orbit of x*. In particular, if $\mathcal{O}_S(x)$ is finite, we say that x is *S-periodic*.

Let κ and μ be cardinal numbers, and $\pi : \kappa \to \operatorname{Sym}(\mu)$ be a set map, where $\operatorname{Sym}(\mu)$ is the symmetric group over the set μ. Note that π naturally defines a left action of the free monoid κ^* with κ generators on μ. For a collection $S = \{f_k\}_{k\in\kappa} \subseteq \operatorname{End}(R^N)$ consisting of κ endomorphisms that are not necessarily distinct, we call an S-orbita $\mathcal{O}$ is *of type* π if the action of $\langle S \rangle$ on $\mathcal{O}$ is given by π, that is, for $\mathcal{O} = \{x_i\}_{i\in\mu}$, we have $f_k(x_i) = x_{\pi_k(i)}$ for all $i \in \mu$ and $k \in \kappa$. Since we are interested in periodic orbits, we will identify a positive integer with the corresponding cardinal number and often put a positive integer n in place of μ.

Denote by $\operatorname{Type}(R, N, \kappa)$ the collection of all possible types of periodic orbit given κ polynomial maps in N variables with coefficients in R. More precisely, an element of $\operatorname{Type}(R, N, \kappa)$ is a tuple $(n, \pi : \kappa \to \operatorname{Sym}(n))$ so that there exists a periodic orbit on R^N of type π. Similarly, denote by $\operatorname{Type}(R, N)$ the collection of all possible types of periodic orbit in N variables with coefficients in R, that is,

$$\operatorname{Type}(R, N) = \bigcup \operatorname{Type}(R, N, \kappa).$$

2 Properties of Periodic Orbits

Lemma 2.1. *Let R be a commutative ring with unity of characteristic zero, and N be a positive integer, and κ be a cardinal number. Let $\mathcal{O} = \{x_1, \ldots, x_n\}$ be a periodic orbit on R^N of type $\pi : \kappa \to \operatorname{Sym}(n)$.*

(a) Let $\sigma \in \operatorname{AGL}_N(R)$ be an invertible affine transformation, that is, $\sigma(x) = Ax + b$ for some $A \in \operatorname{GL}_N(R)$ and $b \in R^N$. Then, $\sigma(\mathcal{O})$ is also a periodic orbit of type π.

(b) There exists a periodic orbit of type π whose coordinates of the points are pairwise distinct.

Proof. (a) Suppose that $\mathcal{O}$ is π-periodic with respect to the collection $S \subseteq \operatorname{End}(R^N)$ of endomorphisms. Then, the set $\sigma(\mathcal{O})$ is π-periodic with respect to

$$S^\sigma = \{f^\sigma = \sigma \circ f \circ \sigma^{-1} : f \in S\}.$$

(b) We can achieve this by applying a suitable $\sigma \in \operatorname{AGL}_N(R)$ to $\mathcal{O}$. See [2, Lemma 4.1(v)]. ☐

Also, we can show the following local–global principle.

[1] This is not a standard terminology. *Orbita* was borrowed from the Latin root of the word *orbit*.

Theorem 2.2 (The local–global principle)**.** *Let R be a Dedekind domain. For all positive integer $N \geq 2$ and cardinal number κ, we have*

$$\mathrm{Type}(R,N,\kappa) = \bigcap_{\mathfrak{p}\in \operatorname{Spec} R\backslash\{0\}} \mathrm{Type}(R_{\mathfrak{p}},N,\kappa) = \bigcap_{\mathfrak{p}\in \operatorname{Spec} R\backslash\{0\}} \mathrm{Type}(\widehat{R}_{\mathfrak{p}},N,\kappa)$$

and

$$\mathrm{Type}(R,N) = \bigcap_{\mathfrak{p}\in \operatorname{Spec} R\backslash\{0\}} \mathrm{Type}(R_{\mathfrak{p}},N) = \bigcap_{\mathfrak{p}\in \operatorname{Spec} R\backslash\{0\}} \mathrm{Type}(\widehat{R}_{\mathfrak{p}},N).$$

Note that [2, Theorem 3.2] is the $M = 1$ case of this theorem.

3 Orbit Extension

Throughout this section, let R be a complete discrete valuation ring of characteristic zero and $\mathfrak{p}$ be the unique maximal ideal of R. We further assume that the residue field $R/\mathfrak{p}$ is finite with q elements. Note that R is compact. Let $\operatorname{ord}_{\mathfrak{p}} : R \to \mathbb{Z} \cup \{\infty\}$ be the surjective discrete valuation of R.

If we have a periodic orbit on R^N that is constant modulo $\mathfrak{p}$, then we can construct an extended orbit by inserting additional points. The following is a slight generalization of [2, Lemma 4.4].

Lemma 3.1 (Orbit extension)**.** *Let $\mathcal{O} = \{x_1, \ldots, x_n\}$ be a finite orbita on R^N of type $\pi : \kappa \to \mathrm{Sym}(n)$. Suppose that $\mathcal{O}$ is constant modulo $\mathfrak{p}$, that is, $x_{i_1} \equiv x_{i_2} \pmod{\mathfrak{p}}$ for all i_1, i_2. Let $y_1, \ldots, y_m$ be points in R^N that are pairwise distinct modulo $\mathfrak{p}$. Note that $1 \leq m \leq \#(\mathbb{R}/\mathfrak{p})$. Then, the set*

$$\widetilde{\mathcal{O}} = \{\widetilde{x}_{(i,j)} = x_i + y_j : 1 \leq i \leq n, 1 \leq j \leq m\}$$

is an orbita on R^N of type $\widetilde{\pi} : \kappa \to \mathrm{Sym}(nm)$, where

$$\widetilde{\pi}_k(i,j) = \begin{cases} (i, j+1) & \text{if } 1 \leq j \leq m-1, \\ (\pi_k(i), 1) & \text{if } j = m. \end{cases}$$

In particular, if $\mathcal{O}$ is a periodic orbit, then so is $\widetilde{\mathcal{O}}$.

Proof. For a point $x \in R^N$, we will denote the r-th coordinate of x by $x^{(r)}$. We may assume that $x_i \equiv 0 \pmod{\mathfrak{p}}$ for all i. Suppose that $\mathcal{O}$ is an S-orbita where $S = \{f_k\}_{k\in\kappa}$. Fix $k \in \kappa$. For each $l \in \mathbb{N}$, define a polynomial map

$$\begin{aligned} \widetilde{g}_{kl}(X) &= \widetilde{g}_{kl}(X_1, \ldots, X_N) \\ &= \sum_{j=1}^{m-1} \prod_{r=1}^{N} \big(1 - (X_r - y_j^{(r)})^{q^l(q-1)}\big) \cdot (X + y_{j+1} - y_j) \\ &\quad + \prod_{r=1}^{N} \big(1 - (X_r - y_m^{(r)})^{q^l(q-1)}\big) \cdot \big(f_k(X - y_m) + y_1\big). \end{aligned}$$

Note that

$$\widetilde{g}_{kl}(\widetilde{x}_{(i,j)}) \equiv \widetilde{x}_{\widetilde{\pi}_k(i,j)} \pmod{\mathfrak{p}^{l+1}}$$

since for all $a \in R$, we have

$$1 - a^{q^l(q-1)} \equiv \begin{cases} 1 \pmod{\mathfrak{p}^{l+1}} & \text{if } a \in \mathfrak{p}, \\ 0 \pmod{\mathfrak{p}^{l+1}} & \text{otherwise.} \end{cases}$$

Consider the ideal

$$\mathfrak{I}_{kl} = \left\langle \prod_{i=1}^{n} \prod_{j=1}^{m} \big(X_r - \widetilde{g}_{kl}(\widetilde{x}_{(i,j)})\big) : 1 \le r \le N \right\rangle \le R[X_1, \dots, X_N],$$

and let $\widetilde{f}_{kl} \in \mathrm{End}(R^N)$ be a polynomial map congruent to $\widetilde{g}_{kl}$ modulo $\mathfrak{I}_{kl}$ such that each component $\widetilde{f}_{kl}^{(r)}$ is of multidegree $\le (mn-1, \dots, mn-1)$. Then by construction, we see that

$$\widetilde{f}_{kl}(\widetilde{x}_{(i,j)}) = \widetilde{g}_{kl}(\widetilde{x}_{(i,j)}) \equiv \widetilde{x}_{\widetilde{\pi}_k(i,j)} \pmod{\mathfrak{p}^{l+1}}$$

for all i, j. As R is compact and the sequence $(\widetilde{f}_{kl})_{l\in\mathbb{N}}$ is of bounded degree, there exists a subsequence of $(\widetilde{f}_{kl})_{l\in\mathbb{N}}$ converging to $\widetilde{f}_k \in \mathrm{End}(R^N)$. Put $\widetilde{S} = \{\widetilde{f}_k\}_{k\in\kappa}$, then $\widetilde{O}$ is an $\widetilde{S}$-orbita of type $\widetilde{\pi}$ as desired. □

4 Periodic Orbits of Linear Maps

From now on, we focus on the periodic orbits of polynomial maps on $\mathbb{Z}^2$. We restrict our view to the (affine) linear maps in this section. Suppose that $\mathcal{O} = \{x_1, \dots, x_n\} \subseteq \mathbb{Z}^2$ is an S-periodic orbit of type $\pi : \kappa \to \mathrm{Sym}(n)$, where each element of S is (affine) linear.

Theorem 4.1 ([5]). *The finite subgroups of* $\mathrm{GL}_2(\mathbb{Z})$ *is isomorphic to one of the following:*

- *cyclic group* $\mathbb{Z}/n\mathbb{Z}$, $n = 1, 2, 3, 4, 6$;
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;
- *symmetric group* S_3;
- *dihedral group* D_4, D_6,

and the above list is exhaustive.

Note that $\mathrm{AGL}_2(\mathbb{Z}) \hookrightarrow \mathrm{GL}_3(\mathbb{Z})$ by

$$(x \mapsto Ax + b) \longmapsto \begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix}.$$

Theorem 4.2 ([4]). *The finite subgroups of* $\mathrm{GL}_3(\mathbb{Z})$ *is isomorphic to one in the previous theorem or one of the following:*

- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$;
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$;
- *alternating group* A_4;
- $D_4 \times \mathbb{Z}/2\mathbb{Z}$;
- $D_6 \times \mathbb{Z}/2\mathbb{Z}$;
- $A_4 \times \mathbb{Z}/2\mathbb{Z}$,

and the above list is exhaustive.

I believe that none of the groups above is contained in $\mathrm{AGL}_2(\mathbb{Z})$, but I am not sure.

5 Orbits of Nontrivial Types

In this section, we prove the existence of certain types of periodic orbits on $\mathbb{Z}^2$ that are generated by two polynomial maps. Recall that in the single map case, the only types of orbits that appear are the cyclic orbits of order $1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24$.

5.1 Orbits of Type $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

For each $n = 1, 2, 3, 4, 6$, there exists a linear map $A \in \mathrm{GL}_2(\mathbb{Z})$ of order n. Let p be a prime number, and consider A as a linear map over $\mathbb{Z}_p$. Then, we can pick a point $x \in p\mathbb{Z}_p^2$ so that $\mathcal{O} = \mathcal{O}_{\{A\}}(x) = \{x_1, \ldots, x_n\}$ is a cyclic orbit of size n. Also note that $\mathcal{O}$ is an $\{\mathrm{id}_{\mathbb{Z}^2}\}$-orbita.

Pick $1 \leq m \leq p^2$ points $y_1, \ldots, y_m \in \mathbb{Z}_p^2$ that are pairwise distinct modulo p, and let

$$\widetilde{\mathcal{O}} = \{\widetilde{x}_{(i,j)} = x_i + y_j : 1 \leq i \leq n, 1 \leq j \leq m\}.$$

Apply the orbit extension lemma with $S = \{A\}$ and $\{\mathrm{id}_{\mathbb{Z}^2}\}$ to obtain two maps f and g that makes $\widetilde{\mathcal{O}}$ an orbita, respectively. Consider the set $\{f^m, g\}$. Then, f^m and g sends $\widetilde{x}_{(i,j)}$ to $\widetilde{x}_{(i+1,j)}$ and $\widetilde{x}_{(i,j+1)}$, respectively, when we view the indices in appropriate moduli. Thus, $\widetilde{\mathcal{O}}$ is a $\{f^n, g\}$-periodic orbit of type

$$\pi : \{f^n, g\} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} = \langle a, b \mid a^n = b^m = aba^{-1}b^{-1} \rangle \leq \mathrm{Sym}(nm).$$

This construction can be done for all p when we pick $1 \leq m \leq 2^2 = 4$. Thus, by the local–global principle, there exists a periodic orbit of two maps of type $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ for all $n = 1, 2, 3, 4, 6$ and $m = 1, 2, 3, 4$.

5.2 Orbits of Type $\widetilde{F}$

Let $A, B \in \mathrm{GL}_2(\mathbb{Z})$ be linear maps such that $F = \langle A, B \rangle$ is a finite subgroup of $\mathrm{GL}_2(\mathbb{Z})$ of size n. Let p be a prime number, and consider A and B as linear maps over $\mathbb{Z}_p$. Put $S = \{A, B\}$, then we can pick a point $x \in p\mathbb{Z}_p^2$ so that $\mathcal{O} = \mathcal{O}_{\{A\}}(x) = \{x_1, \ldots, x_n\}$ is a periodic orbit of type $\pi : S \to F \leq \mathrm{Sym}(n)$. Applying the orbit extension lemma with S gives a collection of two maps $\widetilde{S}$ and a set of nm points $\widetilde{\mathcal{O}}$ so that $\widetilde{\mathcal{O}}$ is an $\widetilde{S}$-periodic orbit of size nm and of type $\widetilde{\pi}$.

This construction can be done for all p when we pick $1 \leq m \leq 2^2 = 4$. Thus, by the local–global principle, there exists a periodic orbit of two maps of type $\widetilde{\pi}$ for all finite $F \leq \mathrm{GL}_2(\mathbb{Z})$ and $m = 1, 2, 3, 4$. In particular, note that by taking $F = D_6$ and $m = 4$, we obtain a periodic orbit of size 48, which exceeds 24, the maximum orbit size that can be obtained by a single map.

References

[1] Hartshorne, R. (1977). Algebraic geometry. Springer.

[2] Pezda, T. (2003). Cycles of polynomial mappings in several variables over rings of integers in finite extensions of the rationals. *Acta Arithmetica*, **108**, 127–146.

[3] Silverman, J. H. (2007). The arithmetic of dynamical systems. Springer.

[4] Tahara, K. (1971). On the finite subgroups of $\mathrm{GL}(3, \mathbb{Z})$. *Nagoya Mathematical Journal*, **41**, 169–209.

[5] Voskresenskii, V. E. (1965). On two-dimensional algebraic tori II. *Mathematics of the USSR-Izvestiya*, **29**, 239–244.