Rose-Hulman Undergraduate Mathematics Journal

Volume 22
Issue 1

Article 6

Disjointness of Linear Fractional Actions on Serre Trees

Henry W. Talbott
Brown University, henry_talbott@brown.edu

Disjointness of Linear Fractional Actions on Serre Trees

Cover Page Footnote

The author would like to thank Prof. Rich Schwartz for mentoring him throughout this project, and Prof. David Fisher for being an invaluable resource.

ℝose-Hulman Undergraduate Mathematics Journal
Volume 22, Issue 1, 2021

Disjointness of Linear Fractional Actions on Serre Trees

By *Henry W. Talbott*

Abstract. Serre showed that, for a discrete valuation field, the group of linear fractional transformations acts on an infinite regular tree with vertex degree determined by the residue degree of the field. Since the p-adics and the polynomials over the finite field of order p act on isomorphic trees, we may ask whether pairs of actions from these two groups are ever conjugate as tree automorphisms. We analyze permutations induced on finite vertex sets, and show a permutation classification result for actions by these linear fractional transformation groups. We prove that actions by specific subgroups of these groups are conjugate only in specific special cases.

1 Introduction

For a commutative ring R with unit 1_R, one may consider the projective special linear group

$$\mathrm{PSL}(2,\mathrm{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathrm{R}, ad-bc = 1_{\mathrm{R}} \right\} \Big/ \{\pm \mathrm{I}\}$$

Groups of this form are ubiquitous in algebra, and have a rich theory. A foundational result on special linear groups over fields is due to Borel and Tits (1973; see also Margulis, 1989): if two fields F_1 and F_2 satisfy certain properties, $\mathrm{PSL}(2,\mathrm{F}_1) \cong \mathrm{PSL}(2,\mathrm{F}_2)$ if and only if $\mathrm{F}_1 \cong \mathrm{F}_2$.

We will be interested in matrix groups of discrete valuation fields, or of the rings of integers of these fields. Two accessible examples of such fields are $\mathbb{Q}_p$, the p-adic numbers, and $\mathbb{F}_p((x))$, the field of fractions of polynomials over the finite field $\mathbb{F}_p$. In both cases, p must be a prime integer. These fields, along with other objects mentioned in this introduction, will be rigorously defined in the next section.

$\mathbb{Q}_p$ and $\mathbb{F}_p((x))$ have many common properties: their respective valuation norms both have image set $\{0\} \cup \{p^n\}_{n\in\mathbb{Z}}$, and there exists a canonical norm-preserving bijection

Mathematics Subject Classification. 20E08
Keywords. Serre trees, euclidean buildings, linear fractional transformations, Lie groups, group actions, p-adic, dynamics

between these fields. However, these fields are not isomorphic (in fact, they do not even have the same characteristic), so $\mathrm{PSL}(2,\mathbb{Q}_p) \ncong \mathrm{PSL}(2,\mathbb{F}_p((x)))$. While these linear groups are globally distinct, one may ask if there is some sense in which the algebraic structures of these groups are locally similar. *Serre trees* provide a framework for comparing $\mathrm{PSL}(2,\mathbb{Q}_p)$ and $\mathrm{PSL}(2,\mathbb{F}_p((x)))$ locally.

Specifically, Serre observed (1977) that to every discrete valuation ring R, one can associate an infinite regular tree $\mathrm{T_R}$, and that this tree admits a faithful group action by $\mathrm{PSL}(2,\mathrm{R})$. Since $\mathrm{PSL}(2,\mathbb{Q}_p)$ and $\mathrm{PSL}(2,\mathbb{F}_p((x)))$ both act on T_p, the regular tree in which every vertex has $p+1$ neighbors, we can ask whether any two actions from these groups are conjugate with respect to the full automormorphism group of the tree, $\mathrm{Aut}(\mathrm{T}_p)$ (fig. 1). In other words, does there exist $f \in \mathrm{PSL}(2,\mathbb{Q}_p)$, $g \in \mathrm{PSL}(2,\mathbb{F}_p((x)))$, and $h \in \mathrm{Aut}(\mathrm{T}_p)$ such that (thinking of each element as an automorphism of T_p),

$$g = h \circ f \circ h^{-1}$$

If so, what can we say about f and g? Notice this condition is weaker than isomorphism of the two groups, or even isomorphism of subgroups, since we are allowed to conjugate by elements of $\mathrm{Aut}(\mathrm{T}_p)$ that do not arise by action of either $\mathrm{PSL}(2,\mathbb{Q}_p)$ or $\mathrm{PSL}(2,\mathbb{F}_p((x)))$. In fact, conjugacy gives a very high amount of flexibility in some cases: for example, any two tree automorphisms that fix one point of T_p and act on its neighbors via a cyclic permutation of length $p+1$ are conjugate, via choosing an appropriate h to 'line up' the cycles around the fixed points.

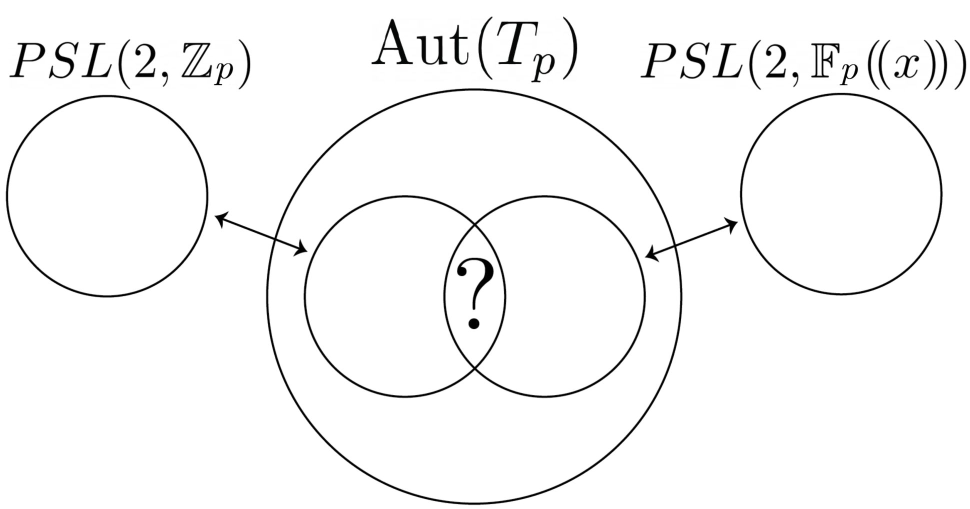

Figure 1: A diagram showing the inclusions of $\mathrm{PSL}(2,\mathbb{Z}_p)$ and $\mathrm{PSL}(2,\mathbb{F}_p[x])$ in $\mathrm{Aut}(\mathrm{T}_p)$. The arrows represent injective homomorphisms. We ask whether, up to conjugacy in $\mathrm{Aut}(\mathrm{T}_p)$, the images of the two projective matrix groups overlap.

For the projective special linear groups $\mathrm{PSL}(2,\mathbb{Z}_p)$ and $\mathrm{PSL}(2,\mathbb{F}_p[x])$ derived from the respective rings of integers of $\mathbb{Q}_p$ and $\mathbb{F}_p((x))$, we determine a condition for two actions to be conjugate. This condition turns out to be highly restrictive, even with the flexibility given by working with conjugacy in $\mathrm{Aut}(\mathrm{T}_p)$.

Theorem 1.1. Let $f \in \mathrm{PSL}(2,\mathbb{Z}_p)$, $g \in \mathrm{PSL}(2,\mathbb{F}_p[x])$, and $h \in \mathrm{Aut}(\mathrm{T}_p)$, where T_p is the Serre tree of $\mathbb{Z}_p$ and $\mathbb{F}_p[x]$. Also let $i_1 : \mathrm{PSL}(2,\mathbb{Z}_p) \to \mathrm{Aut}(\mathrm{T}_p)$ and $i_2 : \mathrm{PSL}(2,\mathbb{F}_p[x]) \to \mathrm{Aut}(\mathrm{T}_p)$ be natural inclusions, and assume

$$i_2(g) = h \circ i_1(f) \circ h^{-1}$$

Then $\mathrm{Ord}(f) = \mathrm{Ord}(g) < \infty$, and moreover $\mathrm{Ord}(f) = \mathrm{Ord}(g)$ is a divisor of $\frac{(p^2-1)p}{2}$.

The primary reason this condition is restrictive is that elements of $\mathrm{PSL}(2,\mathbb{Z}_p)$ or $\mathrm{PSL}(2,\mathbb{F}_p[x])$ with finite order are rare. In fact, it can be deduced from our primary technical lemmas that in the following exact sequences, the third nonzero term s are torsion-free (this fact was known to Serre and Tate (1968), although they do not provide a proof):

$$0 \to \mathrm{PSL}(2,\mathbb{F}_p) \to \mathrm{PSL}(2,\mathbb{Z}_p) \to \mathrm{PSL}(2,\mathbb{Z}_p)/\mathrm{PSL}(2,\mathbb{F}_p) \to 0$$

$$0 \to \mathrm{PSL}(2,\mathbb{F}_p) \to \mathrm{PSL}(2,\mathbb{F}_p[x]) \to \mathrm{PSL}(2,\mathbb{F}_p[x])/\mathrm{PSL}(2,\mathbb{F}_p) \to 0$$

By avoiding torsion, working with general matrices becomes significantly easier. However, the above language of exact sequences will generally be avoided in favor of explicit constructions.

We will also examine the space of invertible projective affine transformations over a field or ring:

$$\mathrm{Aff}(\mathrm{R}) = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a \in \mathrm{R}^*, b \in \mathrm{R} \right\}$$

In the case of $\mathrm{Aff}(\mathbb{Z}_p)$ and $\mathrm{Aff}(\mathbb{F}_p[x])$, we obtain a corollary for affine transformations:

Corollary 1.1. *Let $f \in Aff(\mathbb{Z}_p)$, $g \in Aff(\mathbb{F}_p[x])$, and $h \in Aut(\mathrm{T}_p)$ so that $g = h \circ f \circ h^{-1}$. Then $Ord(f) = Ord(g) < \infty$, and additionally $Ord(f) = Ord(g)$ is a divisor of $p(p-1)$.*

In section 2, we will rigorously define Serre trees and their associated group actions. In section 3, we will analyze the action of $\mathrm{PSL}(2,\mathbb{Z}_p)$ on T_p and derive crucial geometric information about this action. In section 4 we will determine similar information for $\mathrm{PSL}(2,\mathbb{F}_p[x])$ and prove theorem 1.1 as a consequence.

2 Key Definitions

2.1 Discrete Valuation Rings, $\mathbb{Z}_p$, and $\mathbb{F}_p[x]$

$\mathbb{Z}_p$ and $\mathbb{F}_p[x]$ are two natural examples of *discrete valuation rings*, or rings with unique maximal ideals. For our purposes, it is most useful to define $\mathbb{Z}_p$ as the ring of formal power series in p:

$$\mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i : a_i \in \{0,1,\ldots,p-1\} \text{ for all } i, \right\}$$

Addition and multiplication are done using the normal rules for manipulating power series, with the exception that coefficients are carried. When we restrict to elements of $\mathbb{Z}_p$ with finite power series expansions, we recover the monoid $\mathbb{Z}_{\geq 0}$ with the usual addition and multiplication rules.

$\mathbb{F}_p[x]$ is defined analogously to $\mathbb{Z}_p$, but with x in place of p, and with coefficients in $\mathbb{F}_p$:

$$\mathbb{F}_p[x] = \left\{ \sum_{i=0}^{\infty} a_i x^i : a_i \in \mathbb{F}_p \text{ for all } i \right\}$$

Addition and multiplication are carried out by using the normal rules for power series expansions, treating coefficients as elements of $\mathbb{F}_p$.

The fields of fractions of $\mathbb{Z}_p$ and $\mathbb{F}_p[x]$ are isomorphic to $\mathbb{Q}_p$ and $\mathbb{F}_p((x))$, respectively, where $\mathbb{Q}_p$ and $\mathbb{F}_p((x))$ are obtained by allowing finitely many negative coefficients:

$$\mathbb{Q}_p = \left\{ \sum_{i=k}^{\infty} a_i p^i : k \in \mathbb{Z}, a_i \in \{0,1,\ldots,p-1\} \text{ for all } i, a_k \neq 0 \right\} \cup \{0\}$$

$$\mathbb{F}_p((x)) = \left\{ \sum_{i=k}^{\infty} a_i x^i : k \in \mathbb{Z}, a_i \in \mathbb{F}_p \text{ for all } i, a_k \neq 0 \right\} \cup \{0\}$$

For $z \in \mathbb{Q}_p$ or $z \in \mathbb{F}_p((x))$ with the above notation, the canonical *valuation function* is defined as $\varphi(z) = k$, and the induced valuation norm is then given by $|z| = p^{-\varphi(z)} = p^{-k}$.

There exists a valuation-preserving (and thus norm-preserving) bijection from $\mathbb{Q}_p$ to $\mathbb{F}_p((x))$, given by

$$\psi : \mathbb{Q}_p \leftrightarrow \mathbb{F}_p((x)), \ \ \psi\left(\sum_{i=k}^{\infty} a_i p^i \right) = \sum_{i=k}^{\infty} a_i x^i$$

This observation will become critical once Serre trees are introduced.

2.2 Serre Trees

The Serre tree T_{R} of an arbitrary discrete valuation ring R can be defined in terms of the order of its residue field, or the field obtained by quotienting the ring by its unique maximal ideal. In this case, both $\mathrm{T}_{\mathbb{Z}_p}$ and $\mathrm{T}_{\mathbb{F}_p[x]}$ have residue field $\mathbb{F}_p$. As a consequence, $\mathrm{T}_{\mathbb{Z}_p}$ and $\mathrm{T}_{\mathbb{F}_p[x]}$ are both isomorphic to the infinite regular tree with $p+1$ vertices, which we will denote T_p (fig. 2).

Serre trees are part of a much larger family of geometric objects, the *Euclidean buildings*, and are a fundamental class of examples of 1-dimensional Euclidean buildings

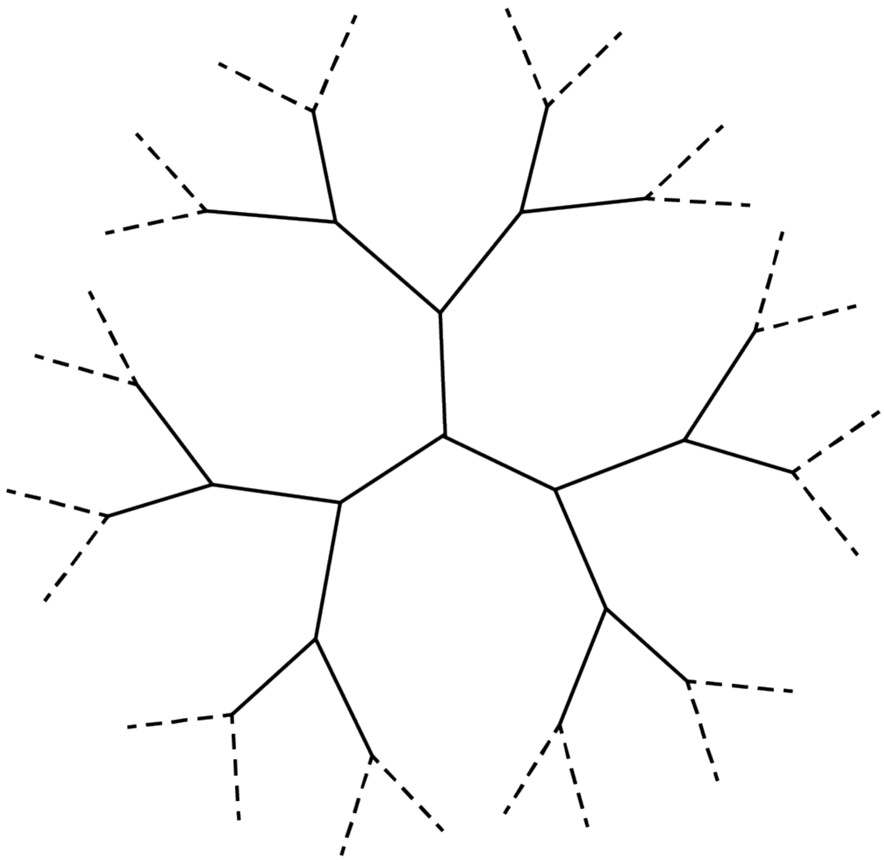

Figure 2: The local structure of the infinite regular tree T_2.

(Brown, 1989). Serre originally defined these trees as arising from scale-equivalence classes of rank-two modules over a given base ring (1977); it is not obvious from Serre's original definition that the objects presented are trees, nor that they have the regular structure described above. We will instead follow the more concrete geometric interpretation given by Armitage and Parker (2007).

2.3 p-adic Balls, the Ultrametric Inequality, and Serre Trees

For two elements x, y in a field with norm $|\cdot|$, define $d(x, y) = |x - y|$. The valuation norms on $\mathbb{Q}_p$ and $\mathbb{F}_p((x))$ both satisfy the ultrametric inequality, or for any x, y, z,

$$d(x, z) \leq \max(d(x, y), d(y, z))$$

This inequality is a strengthening of the standard triangle inequality. As a consequence, translations of balls are either disjoint or equal:

Lemma 2.1. *Let* $\mathrm{B}(x_1,r), \mathrm{B}(x_2,r)$ *be two closed balls in* $\mathbb{Q}_p$ *with equal radius. Then* $\mathrm{B}_1=\mathrm{B}_2$ *or* $\mathrm{B}_1\cap\mathrm{B}_2=\emptyset$.

Proof. When $r=0$, we have that two points are either equal or disjoint, which is certainly true in this field. Assume $r>0$. Since the norm is discrete except at 0, we can assume without loss of generality that $r=p^k$ for some $k\in\mathbb{Z}$. If $\mathrm{B}(x_1,r)\cap\mathrm{B}(x_2,r)\neq\emptyset$, then assume $y\in\mathrm{B}(x_1,r)\cap\mathrm{B}(x_2,r)$. For any $z\in\mathrm{B}(x_1,r)$, $d(z,x_1)\le r$. Additionally, $d(x_1,y)\le r$, and $d(y,x_2)\le r$. Applying the ultrametric inequality twice,

$$d(z,x_2)\le\max(d(z,x_1),d(x_1,y),d(y,x_2))\le r$$

So $z\in\mathrm{B}(x_2,r)$, and $\mathrm{B}(x_1,r)\subseteq\mathrm{B}(x_2,r)$. By symmetry, $\mathrm{B}(x_1,r)=\mathrm{B}(x_2,r)$. ∎

Corollary 2.2. *For any* $k\in\mathbb{Z}$*, the balls of radius* p^k *partition* $\mathbb{Q}_p$.

Corollary 2.3. *Let* $\mathrm{B}(x,r)\subset\mathbb{Q}_p$*. If* $y\in\mathrm{B}(x,r)$*, then* $\mathrm{B}(x,r)=\mathrm{B}(y,r)$.

Effectively, any point in a p-adic ball serves as its 'center'! Identical results hold in the case of $\mathbb{F}_p((x))$.

We will assume for the remainder of the paper that all balls are closed with nonzero radius. Now, let V be the set of all balls in $\mathbb{Q}_p$ with radius p^k for some $k\in\mathbb{Z}$; by the remark in the proof of the above lemma, this covers every ball in $\mathbb{Q}_p$ up to equality. V serves as the vertex set of T_p under our construction. Visually, we can think of balls of equal radius being stacked in horizontal 'layers' in order of radius, with each layer representing a partition of $\mathbb{Q}_p$ into balls. Arranging balls of greater radius 'higher' on the tree, the partition corresponding to each layer refines the partition above it (see fig. 3). We will notate each ball using coset notation, so that $\mathrm{B}(z,p^{-k})=z+p^k\mathbb{Z}_p$ represents the ball of radius p^{-k} 'centered' at z. With this notation, two balls $z+p^k\mathbb{Z}_p$ and $z'+p^k\mathbb{Z}_p$ are equal if and only if $z-z'\in p^k\mathbb{Z}_p$.

The edge set E of T_p is defined via *maximal containment*:

Definition 2.1. If B_1 and B_2 are two distinct balls in some field, B_1 is maximally contained in B_2 if $\mathrm{B}_1\subset\mathrm{B}_2$ and there exists no B_3 such that $\mathrm{B}_1\subsetneq\mathrm{B}_3\subsetneq\mathrm{B}_2$.

Example 2.1. If $\mathrm{B}=1+2^3\mathbb{Z}_2$, then B is maximally contained in $1+2^2\mathbb{Z}_2$, and B maximally contains $1+2^4\mathbb{Z}_2$ and $1+2^3+2^4\mathbb{Z}_2$.

E is then defined as the set of all unordered pairs of balls such that one is maximally contained in the other. Over the p-adics, if the radius of B_1 is p^k and the radius of B_2 is p^j, an alternate way of characterizing maximal containment is that $\mathrm{B}_1\subset\mathrm{B}_2$ and $k=j-1$, or $\mathrm{B}_2\subset\mathrm{B}_1$ and $k=j+1$.

Definition 2.2 (p-adic Serre tree)**.** Let V_p be the set of all balls in $\mathbb{Q}_p$, and let E_p be the set of unordered pairs $(\mathrm{B}_1,\mathrm{B}_2)$ such that $\mathrm{B}_1,\mathrm{B}_2\in\mathbb{Q}_p$ and either B_1 is maximally contained in B_2 or B_2 is maximally contained in B_1. Then $\mathrm{T}_p=\mathrm{G}(\mathrm{V}_p,\mathrm{E}_p)$, the graph constructed by interpreting V_p as a vertex set and E_p as an edge set, is the Serre tree of $\mathbb{Q}_p$.

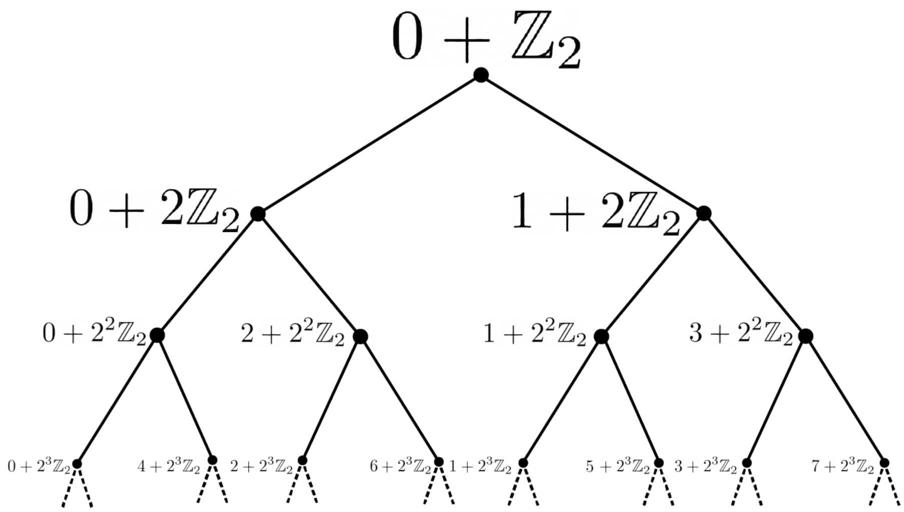

Figure 3: A rooted subtree of T_2, labeled with the 2-adic ball associated to each vertex. Each ball contains two maximal sub-balls.

It is not immediately obvious from the above definition that T_p is in fact a tree. We give a proof sketch: assume $B_0 = B(a_0, p^{k_0})$ is a vertex contained in a cycle C of T_p. Notice that any ball in T_p is adjacent to p balls of smaller radius and 1 ball of larger radius. Of the two vertices adjacent to B_0 in C, at least one is a ball with smaller radius, p^{k_0-1}; call this ball B_1. If B_2 is the other vertex adjacent to B_1 in C, it must have radius p^{k_0-2}, since the only ball adjacent to B_1 in C with greater or equal radius to B_1 is B_0. Continuing this argument, we form a chain of adjacent vertices $B_0, B_1, B_2, B_3, \ldots \subset C$ with strictly decreasing radius. So no $B_n \in C$ can be equal to B_0, a contradiction.

Having constructed $T_{\mathbb{Z}_p}$, we have all the structure in place to build $T_{\mathbb{F}_p[x]}$. We remarked earlier that there is a norm-preserving bijection between $\mathbb{Q}_p$ and $\mathbb{F}_p((x))$. As a function between $\mathbb{Q}_p$ and $\mathbb{F}_p((x))$, this bijection sends balls to balls, and preserves both radii and containment (and therefore maximal containment). Since $T_{\mathbb{Z}_p}$ was only defined in terms of balls on $\mathbb{Q}_p$ and their relations, our bijection shows that $T_{\mathbb{F}_p[x]}$ can be constructed in exactly the same manner as $T_{\mathbb{Z}_p}$, and moreover $T_{\mathbb{F}_p[x]} \cong T_{\mathbb{Z}_p}$ in the sense of graph isomorphism.

Definition 2.3 (Laurent Serre tree)**.** Let V_p be the set of all balls in $\mathbb{F}_p((x))$, and let E_p be the set of unordered pairs (B_1, B_2) such that $B_1, B_2 \in \mathbb{F}_p((x))$ and B_1 is maximally contained in B_2 or B_2 is maximally contained in B_1. Then $T_p = G(V_p, E_p)$, the graph constructed by interpreting V_p as a vertex set and E_p as an edge set, is the Serre tree of $\mathbb{F}_p((x))$.

2.4 Linear Fractional Transformations on T_p

We claimed that the Serre tree $\mathrm{T_R}$ admits a group action by PSL(2, K), where K is the field of fractions of R. How is this action defined? Rather than use the matrix notation presented in the introduction, we will represent PSL(2, K) as a group of *linear fractional transformations*:

$$\mathrm{PSL}(2,\mathrm{K}) = \left\{ f(z) = \frac{az+b}{cz+d} : a,b,c,d \in \mathrm{K}, ad-bc = 1 \right\}$$

With this notation, the group law on PSL(2, K) becomes function composition, and each element $f(z)$ is an invertible function $f : \mathbb{P}^1(\mathrm{K}) \to \mathbb{P}^1(\mathrm{K})$. As is standard, we think of $\mathbb{P}^1(\mathrm{K})$ as $\mathrm{K} \cup \{\infty\}$. The map

$$\psi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \frac{az+b}{cz+d}$$

is the canonical isomorphism between the matrix notation of PSL(2, K) and our new notation. We will use both notations, depending on context, and will sometimes use $\mathrm{M}(z)$ to notate a matrix $\mathrm{M} \in \mathrm{PSL}(2,\mathrm{K})$ acting on some vertex or point z.

One apparent issue is that representations of the form $f(z) = \frac{az+b}{cz+d}$ are not quite unique. After all, for any element s,

$$\frac{az+b}{cz+d} = \frac{s}{s} \cdot \frac{az+b}{cz+d} = \frac{asz+bs}{csz+ds}$$

However, a quick calculation shows that

$$\det\left(\begin{bmatrix} as & bs \\ cs & ds \end{bmatrix}\right) = s^2 \det\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)$$

So the only choice of s that leaves the determinant fixed is $s = \pm 1$. But these choices of s correspond to multiplying by $\pm$I, which we quotiented by to obtain PSL(2, K)! So the $\frac{az+b}{cz+d}$ notation is well-defined once we require that $ad - bc = 1$. This issue of multiple representations can thus mostly be ignored, although it will be useful in section 4.4.

Similarly,

$$\mathrm{Aff}(\mathrm{K}) = \{f(z) = az + b : a \in \mathrm{K}^*, b \in \mathrm{K}\}$$

where the multiple representations issue is resolved by requiring that any matrix $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ corresponding to an affine transformation satisfy $d = 1$.

If $f(z) \in \mathrm{PSL}(2,\mathbb{Q}_p)$ and $\mathrm{B} \subset \mathbb{Q}_p$ is a ball, then either $f(\mathrm{B})$ is a ball or $f(\mathrm{B})^c$ is a ball, where $f(\mathrm{B})$ is the pointwise image of B (Parker, 2007). Since no ball B contains the point $\infty \in \mathrm{P}^1(\mathbb{Z}_p)$, checking whether $\infty \in f(\mathrm{B})$ is a practical way to check whether $f(\mathrm{B})$ or $f(\mathrm{B})^c$ is a ball. Associating each ball B with B^c, $f(z)$ defines a bijection on the vertices of the p-adic Serre tree. Moreover, if B_1 and B_2 are two p-adic balls such that B_1 is

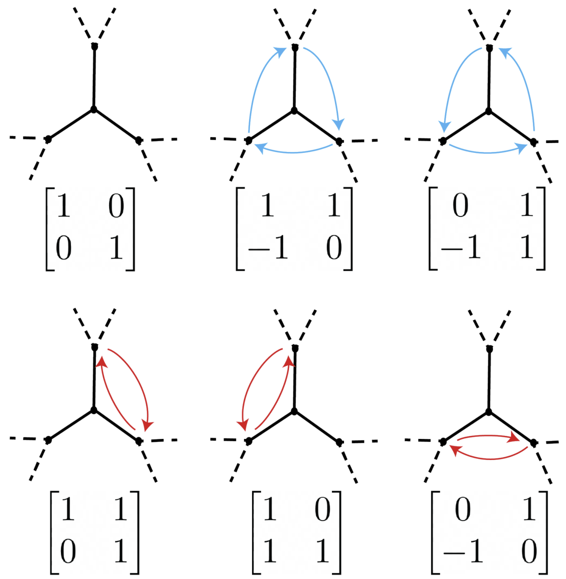

Figure 4: The action of six elements of $\mathrm{PSL}(2,\mathbb{Z}_2)$ on a portion of the tree T_2; specifically, the vertex $0+\mathbb{Z}_2$ and the three adjacent vertices $0+2^{-1}\mathbb{Z}_2$, $0+2\mathbb{Z}_2$, and $1+2\mathbb{Z}_2$. In each subfigure, $0+\mathbb{Z}_2$ is the central vertex, and is fixed by the action.

maximally contained in B_2, and neither balls is mapped to the complement of a ball, then either $f(\mathrm{B}_1)$ is maximally contained in $f(\mathrm{B}_2)$ or $f(\mathrm{B}_2)$ is maximally contained in $f(\mathrm{B}_1)$ (Parker, 2007). If either B_1 or B_2 is mapped to the complement of a ball, this statement holds after taking proper complements. Since $f(z)$ can be thought of as a bijective vertex map that preserves edge relations, $f(z)$ acts as an isomorphism on $\mathrm{T}_{\mathbb{Q}_p}$. Proofs of these assertions can be reduced to direct calculations. Moreover, this images-of-balls construction transfers essentially verbatim to the case of $\mathrm{PSL}(2,\mathbb{F}_p((x)))$ acting on T_p, and the proofs generalize to this case without issue.

Example 2.2. If $\mathrm{B}=1+2^3\mathbb{Z}_2$ and $f(z)=(1+2)z+(1+2^2)$, then

$$f(\mathrm{B})=f(1)+2^3\mathbb{Z}_2=(1+2)+(1+2^2)+2^3\mathbb{Z}_2=2^3+2^3\mathbb{Z}_2=0+2^3\mathbb{Z}_2$$

As a more complex example that is best left to a computer, if $f(z)=\frac{(1+2)z+2}{(1+2+2^2)z+(1+2^2)}$ and $\mathrm{B}=2^{-1}+2+2^3+2^5+2^6\mathbb{Z}_2$, then

$$f(\mathrm{B})=1+2+2^2+2^3+2^4+2^6+2^7+2^8\mathbb{Z}_2$$

Example 2.3. Figure 4 shows how six elements of $\mathrm{PSL}(2,\mathbb{Z}_2)$ locally act on T_2.

Parker (2007) also shows that the group action homomorphisms $\mathrm{PSL}(2,\mathbb{Q}_p)\to\mathrm{Aut}(\mathrm{T}_p)$ and $\mathrm{PSL}(2,\mathbb{F}_p((x)))\to\mathrm{Aut}(\mathrm{T}_p)$ are injective:

Lemma 2.4. *The actions of* $\mathrm{PSL}(2,\mathbb{Q}_p)$, $\mathrm{PSL}(2,\mathbb{F}_p((x)))$, *Aff*$(\mathbb{Q}_p)$, *and Aff*$(\mathbb{F}_p((x)))$ *on* T_p *are faithful.*

Due to the above lemma, we can think of these groups as embedded subgroups of $\mathrm{Aut}(\mathrm{T}_p)$. We will often abuse notation and use $f(z)$ or $\mathrm{M}(z)$ to refer to both the linear fractional transformation and its corresponding automorphism on T_p - this identification makes more sense once we consider *rays* of T_p.

2.5 Rays, Ends and the Boundary of T_p

Serre (1977) observed that the 'boundary' of T_p can be associated with the projective line over its base field, in our case either $\mathbb{Q}_p \cup \{\infty\}$ or $\mathbb{F}_p((x)) \cup \{\infty\}$. Intuitively, this statement makes sense: as one chooses a path down the tree, one chooses a nested sequence of balls of decreasing radius, which converge to a single point. On the other hand, all paths of balls of strictly increasing radii eventually converge, so we label this 'upwards' limit point ∞ (using the picture suggested by fig. 3). This idea can be made precise by defining *rays* (see fig. 5):

Definition 2.4. A ray r on T_R is an infinite path of vertices with one endpoint and no backtracking. Two rays r_1 and r_2 are equivalent if their intersection is again a ray, and an equivalence class of rays is called an end. A line l on T_R is an infinite path of vertices with no endpoints and no backtracking.

The set of ends of T_p is in bijection with both $\mathbb{Q}_p \cup \{\infty\}$ and $\mathbb{F}_p((x)) \cup \{\infty\}$, and this bijection agrees with the already-established bijection between $\mathbb{Q}_p$ and $\mathbb{F}_p((x))$. As suggested above, an intuitive way to see this is that an end represents all nested sequences of balls that 'zoom in' to the same point, and defining ends in this way is the standard way of extending the idea of 'boundary' to the infinite tree T_p. For any element h of $\mathrm{Aut}(\mathrm{T}_p)$, the fact that h is a tree automorphism implies it sends equivalent rays to equivalent rays, and hence is a well-defined map on ends.

Crucially, ends interact nicely with the actions of $\mathrm{PSL}(2,\mathbb{Q}_p)$ and $\mathrm{PSL}(2,\mathbb{F}_p((x)))$ (Parker, 2007). We'll state this fact for $\mathbb{Q}_p$, and the equivalent statement will also hold for $\mathbb{F}_p((x))$. Although we won't give a full proof, this lemma holds because we define the action of linear fractional transformations on vertices in terms of pointwise images of balls.

Lemma 2.5. *Let* $\mathrm{M} \in \mathrm{PSL}(2,\mathbb{Q}_p)$, *and let* E_z *be the end of* T_p *associated to some* $z \in \mathbb{P}^1(\mathbb{Q}_p)$. *If* $\mathrm{M}(z)$ *is the image of* z *under* $\mathrm{M} : \mathbb{P}^1(\mathbb{Q}_p) \to \mathbb{P}^1(\mathbb{Q}_p)$, *and* $\mathrm{M}(\mathrm{E}_z)$ *is the image of* E_z *(i.e. the equivalence class of images of rays in* E_z*) under the automorphism* $\mathrm{M} : \mathrm{T}_p \to \mathrm{T}_p$, *then*

$$\mathrm{M}(\mathrm{E}_z) = \mathrm{E}_{\mathrm{M}(z)}$$

Sometimes, it will be helpful to go back and forth between the automorphism M induces on T_p, and the map M induces on the 'boundary' of T_p; this second map is just the function $\mathrm{M} : \mathbb{P}^1(\mathbb{Q}_p) \to \mathbb{P}^1(\mathbb{Q}_p)$.

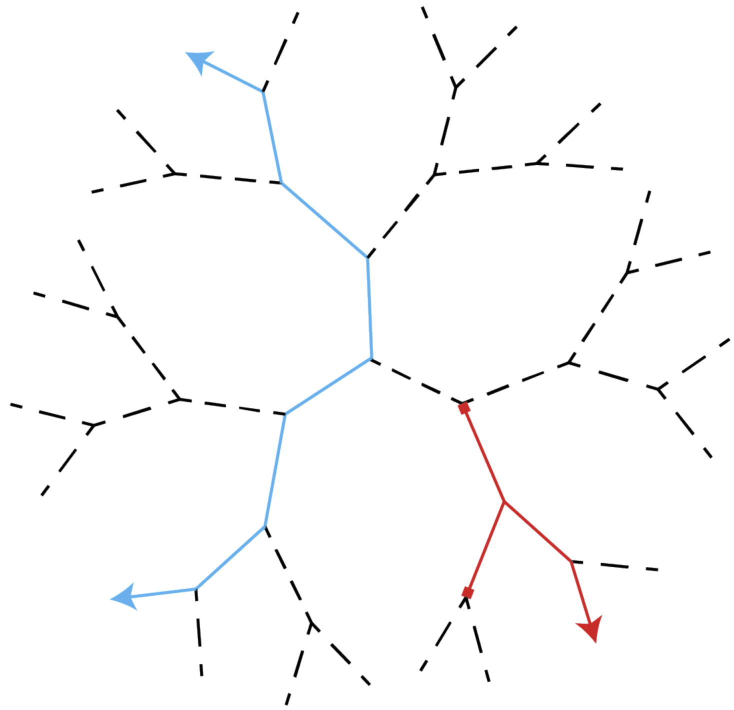

Figure 5: A line (blue) and two equivalent rays (red) on T_2.

2.6 Conjugation and Orbits

One of the most useful tools we'll use is conjugation, since it preserves the permutation structures we'll be interested in. For a set S, a group G acting on S, and $s \in S$, $g \in G$, define $\mathrm{Ord}_g(s)$ as the least positive integer m such that $g^m(s) = s$ if such an m exists, and ∞ otherwise. Then:

Lemma 2.6. *Let* S *be a set and let* G *be a group acting on* S*. For all* $s \in S$*, and* $g, h \in G$ *such that* $Ord_g(s)$ *is finite,*

$$Ord_g(s) = Ord_{hgh^{-1}}(h(s))$$

Proof. Assume that $g^m(s) = s$ for some $m \geq 1$. Then $(hgh^{-1})^m = hg^m h^{-1}$, and

$$h(g^m(h^{-1}(h(s)))) = h(g^m(s)) = h(s)$$

So $\mathrm{Ord}_{hgh^{-1}}(h(s)) \leq \mathrm{Ord}_g(s)$. On the other hand, if $(hgh^{-1})^m(h(s)) = h(s)$, then

$$h(g^m(h^{-1}(h(s)))) = h(s)$$

$$\to h(g^m(s)) = h(s) \to g^m(s) = s$$

So $\mathrm{Ord}_g(s) \le \mathrm{Ord}_{hgh^{-1}}(h(s))$. In conclusion,

$$\mathrm{Ord}_g(s) = \mathrm{Ord}_{hgh^{-1}}(h(s))$$

■

In particular, if S is finite of size n, then the symmetric group S_n naturally acts on S, and a bit more work shows that conjugation in S_n preserves the orbit structures induced by permutations.

3 Analyzing $\mathrm{PSL}(2, \mathbb{Z}_p)$

3.1 Preliminary Lemmas and Computational Tools

Let $\mathrm{M} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{PSL}(2, \mathbb{Z}_p)$. Our first goal will be to obtain a specific computational description of how M acts on vertices of T_p.

If $c = 0$, then a is a unit and $d = a^{-1}$; M corresponds to the function

$$f(z) = \frac{az+b}{a^{-1}} = a^2 z + ab$$

$f(z)$ fixes ∞, so must send balls to balls and complements of balls to complements of balls. Moreover, the action of a general affine map is straightforward to compute:

Lemma 3.1. *Let $a, b \in \mathbb{Z}_p$, $a \in \mathbb{Z}_p^*$, and let $r + p^k\mathbb{Z}_p$ be a p-adic ball. Then if $f(z) = az + b$,*

$$f(r + p^k\mathbb{Z}_p) = f(r) + p^k\mathbb{Z}_p$$

Proof. As stated above, $f(z)$ fixes ∞, so the image under f of $r + p^k\mathbb{Z}_p$ is a ball. Moreover, this image certainly contains $f(r)$.

The claim now follows from the fact that $f(z)$ is an isometry on $\mathbb{Q}_p$. For $r, s \in \mathbb{Q}_p$,

$$|f(r) - f(s)| = |(ar+b) - (as+b)| = |a(r-s)| = |a||r-s| = |r-s|$$

since a is a p-adic unit and so $|a| = 1$. ■

In particular, for $a, b \in \mathbb{Z}_p$, $ab \in \mathbb{Z}_p$, so $f(0 + \mathbb{Z}_p) = ab + \mathbb{Z}_p = 0 + \mathbb{Z}_p$.

If $c \neq 0$, we can apply a standard decomposition to M. Notice b is substituted out via the relation $b = \frac{ad-1}{c}$:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & ac^{-1} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} c & 0 \\ 0 & c^{-1} \end{bmatrix} \begin{bmatrix} 1 & dc^{-1} \\ 0 & 1 \end{bmatrix} = \mathrm{A}_2\mathrm{RDA}_1$$

Note that not all of these matrices necessarily lie in $\mathrm{PSL}(2, \mathbb{Z}_p)$. The first and last matrix are affine, so act as isomorphisms on $\mathbb{Q}_p$. $\begin{bmatrix} c & 0 \\ 0 & c^{-1} \end{bmatrix}$ corresponds to the map $f(z) = c^2 z$, and if $c = p^k u$ where $k \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^*$, and $r + p^j\mathbb{Z}_p$ is some ball, $f(r + 2^j\mathbb{Z}_p) = c^2 r + p^{j+2k}\mathbb{Z}_p$. In effect, $f(z) = c^2 z$ acts as a dilation map.

$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ corresponds to the map $r(z) = -\frac{1}{z}$, and has a somewhat complex action: assume $p^k u + p^j\mathbb{Z}_p$ is a ball such that $u \in \mathbb{Z}_p^*$ as above. If $p^k u + 2^j\mathbb{Z}_p$ does not contain 0, $r(p^k u + 2^j\mathbb{Z}_p) = r(p^k u) + 2^{j-2k}\mathbb{Z}_p$. On the other hand, any ball containing 0 can be written in the form $0 + p^j\mathbb{Z}_p$, and $r(0 + p^j\mathbb{Z}_p) = p^{-j}\mathbb{Z}_p$. Calculations verifying these assertions are performed by Parker (2007), and are of a similar spirit to lemma 3.1.

Applying the above rules in succession via the decomposition of M gives an explicit rule for the action of M. Lemma 3.2, originally stated by Parker (2007), provides an example of this type of computation, and is proven here in the interest of clarity:

Lemma 3.2. *Let* $\mathrm{M} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{PSL}(2, \mathbb{Z}_p)$. *Then* $\mathrm{M}(0 + \mathbb{Z}_p) = 0 + \mathbb{Z}_p$.

Proof. The case of $c = 0$ is a consequence of lemma 3.1. Otherwise, M decomposes into $\mathrm{A}_2\mathrm{R}\mathrm{D}\mathrm{A}_1$ as above. First, assume c is a unit. Then

$$\mathrm{A}_1(0 + \mathbb{Z}_p) = dc^{-1} + \mathbb{Z}_p = 0 + \mathbb{Z}_p$$

since $dc^{-1} \in \mathbb{Z}_p$. Again, since c is a unit,

$$\mathrm{D}(0 + \mathbb{Z}_p) = 0 + \mathbb{Z}_p$$

$\mathrm{R}(0 + \mathbb{Z}_p) = 0 + \mathbb{Z}_p$, and lastly $\mathrm{A}_2(0 + \mathbb{Z}_p) = 0 + \mathbb{Z}_p$ for an analogous reason as A_1.

Now assume c is not a unit, so $c = p^k u$ where $k > 0$ and u is a unit. d is necessarily a unit, as otherwise $ad - bc = 1$ would be a nonunit. $\mathrm{A}_1(0 + \mathbb{Z}_p) = p^{-k}du^{-1} + \mathbb{Z}_p$. Then

$$\mathrm{D}(p^{-k}du^{-1} + \mathbb{Z}_p) = p^k du + p^{2k}\mathbb{Z}_p$$

Since $0 \notin p^k du + p^{2k}\mathbb{Z}_p$,

$$\mathrm{R}(p^k du + p^{2k}\mathbb{Z}_p) = -p^{-k}d^{-1}u^{-1} + p^{2k-2k}\mathbb{Z}_p = -p^{-k}d^{-1}u^{-1} + \mathbb{Z}_p$$

Lastly,

$$\mathrm{A}_2(-p^{-k}d^{-1}u^{-1} + \mathbb{Z}_p) = -p^{-k}d^{-1}u^{-1} + ac^{-1} + \mathbb{Z}_p$$

Moreover, if $\infty \in \mathrm{M}(0 + \mathbb{Z}_p)$, then there exists some $z \in \mathbb{Z}_p$ so that $bz + d = 0$. But since b is a nonunit, bz is a nonunit, and $bz + d$ is a unit. So $bz + d = 0$ is impossible, and ∞ is not in the image of M. In other words, $\mathrm{M}(0 + \mathbb{Z}_p)$ is a ball, rather than the complement of a ball.

This verifies that $\mathrm{M}(0 + \mathbb{Z}_p)$ is a ball of radius 1. Lastly, notice that $\mathrm{M}(0) = bd^{-1} \in \mathbb{Z}_p$, since d is a unit. Therefore $\mathrm{M}(0 + \mathbb{Z}_p)$ can be written as $bd^{-1} + \mathbb{Z}_p$, which is equal to $0 + \mathbb{Z}_p$. ■

Lemma 3.2 gives us a fixed point to work with. Since we know $0+\mathbb{Z}_p$ is fixed by $\mathrm{PSL}(2,\mathbb{Z}_p)$, and that functions in $\mathrm{PSL}(2,\mathbb{Z}_p)$ act as graph isomorphisms on T_p, functions in $\mathrm{PSL}(2,\mathbb{Z}_p)$ must permute the sets of vertices of distance k from $0+\mathbb{Z}_p$, for all $k \geq 0$. We will call these vertex sets *layers* (fig. 6).

Definition 3.1. Let T_p be the p-adic Serre tree. For $k \geq 0$, L_k, the kth layer from the vertex $0+\mathbb{Z}_p$, is the set of all vertices of T_p of distance exactly k from $0+\mathbb{Z}_p$.

L_1 consists of the vertices adjacent to $0+\mathbb{Z}_p$, and contains $p+1$ vertices. Moving outwards on T_p, $|\mathrm{L}_k| = (p+1)p^{k-1}$.

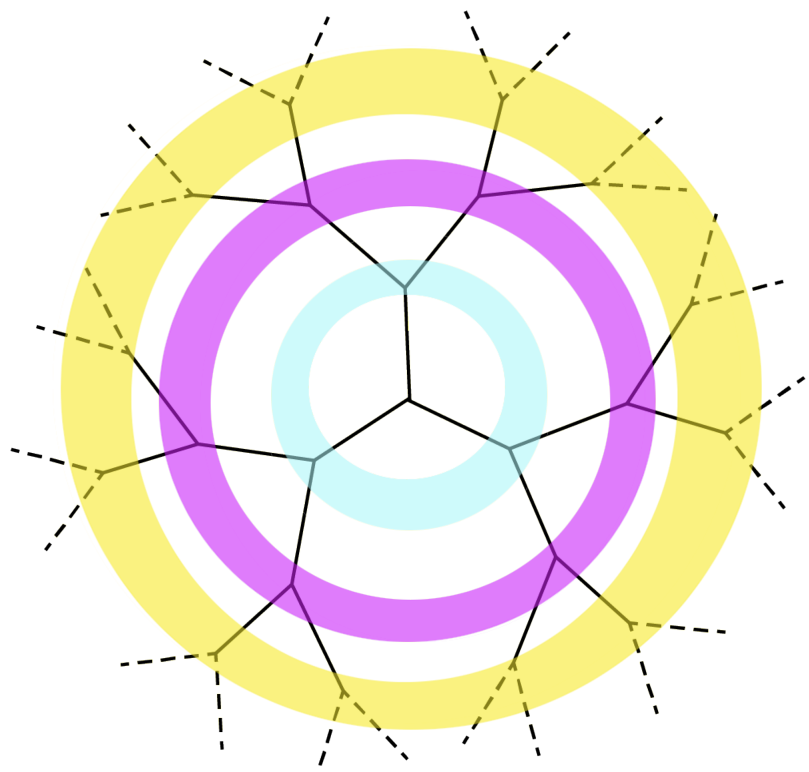

Figure 6: The layers L_1, L_2, and L_3 of T_2.

Since each L_k is finite, passing from the action of $\mathrm{PSL}(2,\mathbb{Z}_p)$ on T_p to its action on L_k reduces our problem to analyzing permutations of finite sets. We can restrict further to especially nice permutations by considering matrices of a certain form.

A standard fact about $\mathbb{Z}_p$ is that there is a surjective ring homomorphism φ_n projecting $\mathbb{Z}_p$ to $\mathbb{Z}/p^n\mathbb{Z}$ for any n, obtained by taking the quotient of $\mathbb{Z}_p$ by the ideal $p^n\mathbb{Z}_p$. In effect, we discard terms in our power series with coefficient p^n or greater. Any such projection map φ_n extends to a projection homomorphism

$$\psi_n : \mathrm{PSL}(2,\mathbb{Z}_p) \to \mathrm{PSL}(2,\mathbb{Z}/p^n\mathbb{Z})$$

by applying φ_n to each entry of a given matrix.

Definition 3.2. A matrix

$$\mathrm{M} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{PSL}(2,\mathbb{Z}_p)$$

is identity-like if

$$\psi_1(\mathrm{M}) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in \mathrm{PSL}(2,\mathbb{Z}/p\mathbb{Z})$$

An analogous definition (obtained by projecting to $\mathrm{PSL}(2,\mathbb{Z}/p\mathbb{Z})$) applies to matrices in $\mathrm{PSL}(2,\mathbb{Z}/p^n\mathbb{Z})$. Identity-like matrices are immediately useful:

Lemma 3.3. *Let* $\mathrm{M} \in \mathrm{PSL}(2,\mathbb{Z}_p)$ *be identity-like, or of the form*

$$\mathrm{M} = \begin{bmatrix} 1+pa & pb \\ pc & 1+pd \end{bmatrix}$$

for some $a,b,c,d \in \mathrm{PSL}(2,\mathbb{Z}_p)$. *Then* M *fixes* L_1.

Proof. We know that pc is not a unit, so we decompose M:

$$\mathrm{M} = \mathrm{A}_2\mathrm{RDA}_1$$

$$\begin{bmatrix} 1+pa & pb \\ pc & 1+pd \end{bmatrix} =$$

$$\begin{bmatrix} 1 & (1+pa)(pc)^{-1} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} pc & 0 \\ 0 & (pc)^{-1} \end{bmatrix} \begin{bmatrix} 1 & (1+pd)(pc)^{-1} \\ 0 & 1 \end{bmatrix}$$

The first step will be to check that $0 + p^{-1}\mathbb{Z}_p$ is fixed. $\mathrm{A}_1(0 + p^{-1}\mathbb{Z}_p) = p^{-1}c^{-1} + dc^{-1} + p^{-1}\mathbb{Z}_p$. Assume that c has the form $p^k u$, where u is a unit, so $pc = p^{k+1}u$. Then

$$\mathrm{D}(p^{-1}c^{-1} + dc^{-1} + p^{-1}\mathbb{Z}_p) = p^2c^2(p^{-1}c^{-1} + dc^{-1}) + p^{2k+1}\mathbb{Z}_p$$

$$= pc + p^2dc + p^{2k+1}\mathbb{Z}_p$$

0 is not contained in $pc + p^2dc + p^{2k+1}\mathbb{Z}_p$, since $|pc + p^2dc| = |pc| = p^{-(k+1)}$. Therefore,

$$\mathrm{R}(pc + p^2dc + p^{2k+1}\mathbb{Z}_p) =$$

$$-\frac{1}{pc+p^2dc} + p^{(2k+1)-2(k+1)}\mathbb{Z}_p = -\frac{1}{pc+p^2dc} + p^{-1}\mathbb{Z}_p$$

And lastly

$$\mathrm{A}_2\left(-\frac{1}{pc+p^2dc}+p^{-1}\mathbb{Z}_p\right)=(1+pa)(pc)^{-1}-\frac{1}{pc+p^2dc}+p^{-1}\mathbb{Z}_p$$

We could attempt to simplify the center of the above ball, but we will instead notice that the only ball of radius p^{-1} in L_1 is $0+p^{-1}\mathbb{Z}_p$. Since M permutes L_1, necessarily

$$(1+pa)(pc)^{-1}-\frac{1}{pc+p^2dc}+p^{-1}\mathbb{Z}_p=0+p^{-1}\mathbb{Z}_p$$

and

$$\mathrm{M}(0+p^{-1}\mathbb{Z}_p)=0+p^{-1}\mathbb{Z}_p$$

We will now turn our attention to balls in L_1 of the form $r+p\mathbb{Z}_p$, where r can be assumed to be in $\{0,1,\ldots,p-1\}$. M cannot invert balls of this type: that would imply there is some $z\in r+p\mathbb{Z}_p$ such that $\mathrm{M}(z)=\infty$, or $pcz+1+pd=0$. But we can see that $pcz+1+pd$ is a unit. Moreover, M must send each $r+p\mathbb{Z}_p$ to another ball in L_1, and $0+p^{-1}\mathbb{Z}_p$ is fixed. So in fact M must send $r+p\mathbb{Z}_p$ to some $r'+p\mathbb{Z}_p$ such that $\mathrm{M}(r)\in r'+p\mathbb{Z}_p$. To show $r+p\mathbb{Z}_p$ is fixed by M, it is therefore sufficient to show that $\mathrm{M}(r)-r\in p\mathbb{Z}_p$. This is not so bad:

$$\begin{aligned}\mathrm{M}(r)-r=\frac{r+par+pb}{pcr+1+pd}-r&=\frac{r+par+pb}{1+pcr+pd}-\frac{r+pcr^2+pdr}{1+pcr+bd}\\&=\frac{p(ar+b+cr^2+dr)}{1+pcr+bd}\end{aligned}$$

The denominator is a unit, while the numerator is divisible by p. Therefore $\mathrm{M}(r)-r\in p\mathbb{Z}_p$ as claimed. ■

3.2 Integral Branches and Orbits

Lemma 3.3 is an example of a broader phenomenon, whereby in some cases we can reduce the coefficients of M to their representatives modulo $p^k\mathbb{Z}_p$ when working on the layer L_k. To make this phenomenon more precise, we will need yet more definitions.

Definition 3.3. Let $v\in\mathrm{T}_p$. A branch of T_p at v is a connected component of T_p-v. If $v=0+\mathbb{Z}_p$, the integral branches are those containing a point of the form $a+p\mathbb{Z}_p$ where $a\in\{0,1,\ldots,p-1\}$. For a general v, the downwards branches are those not containing ∞ on their boundaries.

The term 'downwards branches' is meant to line up with the visualization in figure 3. Of course, the above definitions easily carry over when interpreting T_p as the Serre tree of $\mathbb{F}_p[x]$ rather than $\mathbb{Z}_p$.

The three branches of a given v in T_2 are shown in fig. 7, and lemma 3.3 implies that identity-like matrices fix the branches of $0+\mathbb{Z}_p$. We will now generalize lemma 3.3.

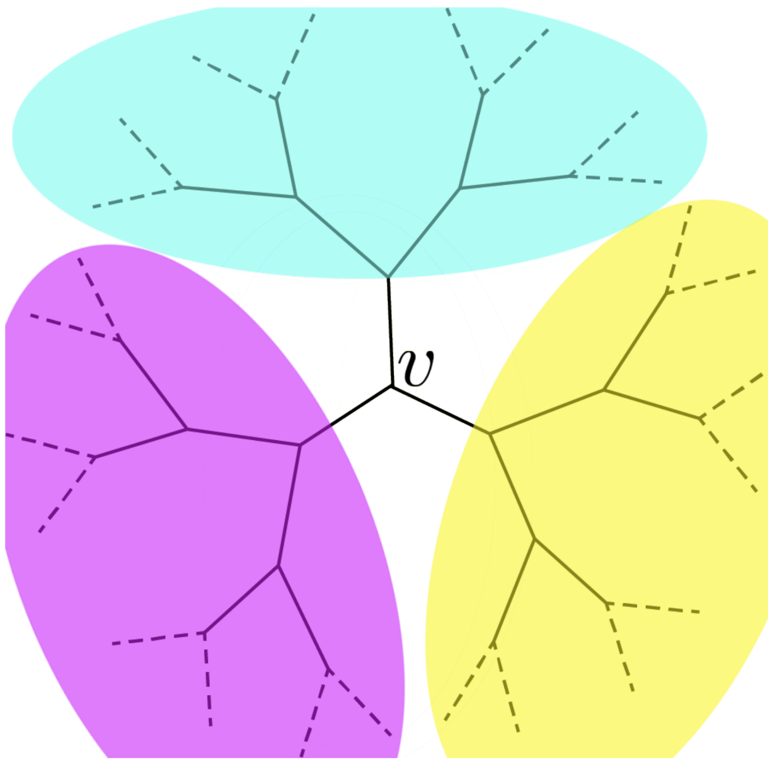

Figure 7: The three branches of a vertex v in T_2. A point in T_p will have $p+1$ branches.

Lemma 3.4. *Let* $\mathrm{M}_1, \mathrm{M}_2 \in \mathrm{PSL}(2,\mathbb{Z}_p)$ *be identity-like. Let* $r + p^k\mathbb{Z}_p$ *lie on an integral branch of* T_p*, and additionally assume that* $\psi_k(\mathrm{M}_1) = \psi_k(\mathrm{M}_2)$*. Then* $\mathrm{M}_1(r + p^k\mathbb{Z}_p) = \mathrm{M}_2(r + p^k\mathbb{Z}_p)$.

Proof. Since $r + p^k\mathbb{Z}_p$ is on an integral branch, $r \in \mathbb{Z}_p$. Additionally, since M_1 and M_2 are both identity-like, they will send $r + p^k\mathbb{Z}_p$ to balls on the same integral branch, and on the same layer L_k. Let

$$\mathrm{M}_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \ \mathrm{M}_2 = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$$

Neither matrix can send $r + p^k\mathbb{Z}_p$ to the complement of a ball: this would imply that for some $z \in r + p^k\mathbb{Z}_p$, $cz + d = 0$ or $c'z + d' = 0$, respectively. Since c and c' are nonunits and d and d' are units, this equation cannot be solved by any $z \in \mathbb{Z}_p$. Therefore, $\mathrm{M}_1(r + p^k\mathbb{Z}_p) = \mathrm{M}_1(r) + p^k\mathbb{Z}_p$, and $\mathrm{M}_2(r + p^k\mathbb{Z}_p) = \mathrm{M}_2(r) + p^k\mathbb{Z}_p$. So we merely need to show that $\mathrm{M}_1(r) - \mathrm{M}_2(r) \in p^k\mathbb{Z}_p$.

$$\mathrm{M}_1(r) - \mathrm{M}_2(r) = \frac{ar + b}{cr + d} - \frac{a'r + b'}{c'r + d'}$$
$$= \frac{(ar + b)(c'r + d') - (a'r + b')(cr + d)}{(cr + d)(c'r + d')}$$

Applying φ_k to the numerator of the above expression, we observe $\varphi_k(a) = \varphi_k(a')$, $\varphi_k(b) = \varphi_k(b')$, $\varphi_k(c) = \varphi_k(c')$, and $\varphi_k(d) = \varphi_k(d')$. So φ_k of the numerator is equal to 0 in $\mathbb{Z}/p^k\mathbb{Z}$, showing $\mathrm{M}_1(r) - \mathrm{M}_2(r) \in p^k\mathbb{Z}_p$. ■

We need two more lemmas, which will allow us to make simplifying assumptions when calculating the order of a point under an identity-like matrix M. The first lemma is a counting argument. It uses the fact that the identity-like matrices of $\mathrm{PSL}(2,\mathbb{Z}_p)$ form a subgroup J, which is easily seen by noticing $\mathrm{J} = \ker\psi_1$, where ψ_1 is the projection map from $\mathrm{PSL}(2,\mathbb{Z}_p)$ to $\mathrm{PSL}(2,\mathbb{Z}/p\mathbb{Z})$. Likewise, define J_n as the identity-like matrices in $\mathrm{PSL}(2,\mathbb{Z}/p^n\mathbb{Z})$, which is a subgroup by a similar projection onto $\mathrm{PSL}(2,\mathbb{Z}/p\mathbb{Z})$.

Lemma 3.5. *Let* $n \geq 1$ *and* $p > 2$*. Then*

$$|\mathrm{PSL}(2,\mathbb{Z}/p^n\mathbb{Z})| = \frac{(p^2 - 1)p^{3n-2}}{2}$$

and

$$|\mathrm{J}_n| = p^{3n-3}$$

If $p = 2$*, then*

$$|\mathrm{PSL}(2,\mathbb{Z}/2^n\mathbb{Z})| = 3 \cdot 2^{3n-2}$$

and

$$|\mathrm{J}_n| = 2^{3n-3}$$

Proof. All elements of $\mathrm{SL}(2,\mathbb{Z}/p^n\mathbb{Z})$ can be written in the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. If a and b are both nonunits, $ad-bc=1$ is impossible, so assume a is a unit. We may now choose any elements of $\mathbb{Z}/p^n\mathbb{Z}$ for b and c, which restricts d to $d=\frac{1+bc}{a}$ by $ad-bc=1$. Since there are p^{n-1} nonunits in $\mathbb{Z}/p^n\mathbb{Z}$, there are $(p-1)p^{n-1}$ units, so there are $((p-1)p^{n-1})(p^n)(p^n)=(p-1)p^{3n-1}$ matrices in $\mathbb{Z}/p^n\mathbb{Z}$ such that the top left entry is a unit.

If a is not a unit, b must be a unit. We may choose any element for d, and c is restricted to $c=\frac{ad-1}{b}$. Choosing one nonunit, one unit, and one arbitrary element gives $(p^{n-1})((p-1)p^{n-1})p^n=(p-1)p^{3n-2}$ possible matrices. Therefore,

$$|\mathrm{SL}(2,\mathbb{Z}/p^n\mathbb{Z})|=(p-1)p^{3n-1}+(p-1)p^{3n-2}=(p-1)(p+1)p^{3n-2}$$

To obtain the size of $\mathrm{PSL}(2,\mathbb{Z}/p^n\mathbb{Z})$, recall that

$$\mathrm{PSL}(2,\mathbb{Z}/p^n\mathbb{Z})=\mathrm{SL}(2,\mathbb{Z}/p^n\mathbb{Z})/\{\pm\mathrm{I}\}$$

and $\{\pm\mathrm{I}\}$ is a subgroup of size 2 when $p>2$ (i.e. $1\neq-1$). For $p=2$, $\mathrm{I}=-\mathrm{I}$, and $\mathrm{PSL}(2,\mathbb{Z}/p^n\mathbb{Z})=\mathrm{SL}(2,\mathbb{Z}/p^n\mathbb{Z})$.

As for J_n, we can notice that any identity-like matrix in $\mathrm{SL}(2,\mathbb{Z}/p^n\mathbb{Z})$ can be written in the form

$$\begin{bmatrix} 1+pa & pb \\ pc & 1+pd \end{bmatrix}$$

where a,b,c,d are elements of $\mathbb{Z}/p^{n-1}\mathbb{Z}$. The only restriction that must be satisfied is

$$(1+pa)(1+pd)-p^2bc=1 \iff pd=\frac{(1+p^2bc)-(1+pa)}{1+pa}$$

$$\iff d=\frac{pbc-a}{1+pa}$$

Therefore choosing a,b,c determines d uniquely. Sicne a, b, and c can be chosen arbitrarily from $\mathbb{Z}/p^{n-1}\mathbb{Z}$, we find

$$|\mathrm{J}_n|=(p^{n-1})^3=p^{3n-3}$$

For $p>2$, going from $\mathrm{SL}(2,\mathbb{Z}/p^n\mathbb{Z})$ to $\mathrm{PSL}(2,\mathbb{Z}/p^n\mathbb{Z})$ doesn't affect the size of J_n, since $-\mathrm{I}\notin\mathrm{J}_n$ by definition. For $p=2$, $-\mathrm{I}=\mathrm{I}$, so again nothing changes. ■

Corollary 3.6. *Let* $\mathrm{M}\in\mathrm{PSL}(2,\mathbb{Z}/p^n\mathbb{Z})$ *and* $p>2$. *Then* $\mathrm{M}^{\frac{(p^2-1)p}{2}}$ *is identity-like. If* $p=2$, *then* M^6 *is identity-like.*

Proof. Let $\psi_{n,1} : \mathrm{PSL}(2,\mathbb{Z}/p^n\mathbb{Z}) \to \mathrm{PSL}(2,\mathbb{Z}/p\mathbb{Z})$ be the projection map and $p > 2$. Since $\psi_{n,1}$ is a homomorphism and $|\mathrm{PSL}(2,\mathbb{Z}/p\mathbb{Z})| = \frac{(p^2-1)p}{2}$,

$$\psi_{n,1}\left(\mathrm{M}^{\frac{(p^2-1)p}{2}}\right) = \psi_{n,1}(\mathrm{M})^{\frac{(p^2-1)p}{2}} = \mathrm{I}$$

by Lagrange's theorem. But $\psi_{n,1}\left(\mathrm{M}^{\frac{(p^2-1)p}{2}}\right) = \mathrm{I}$ is equivalent to $\mathrm{M}^{\frac{(p^2-1)p}{2}}$ being identity-like. The situation when $p = 2$ is analogous. ■

This lemma has a fairly powerful consequence regarding orbits of points on T_p under M. But first, a definition:

Definition 3.4. Let $\mathrm{M} \in \mathrm{PSL}(2,\mathbb{Z}_p)$ and let v be a vertex of T_p. Let $\mathrm{Ord}_{\mathrm{M}}(v)$ be the order of v under the group action of M.

Since any $v \in \mathrm{T}_p$ lies in L_k for some k, and all L_k are finite $\mathrm{PSL}(2,\mathbb{Z}_p)$-invariant sets, $\mathrm{Ord}_{\mathrm{M}}(v)$ is always a finite positive integer. We can now state another lemma:

Lemma 3.7. *Let* M *be an identity-like matrix in* $\mathrm{PSL}(2,\mathbb{Z}_p)$ *and let v be a vertex of* T_p *lying on the intersection of* L_k *and an integral branch. Then the order of v under* M *is equal to p^m for some non-negative integer m.*

Proof. By lemma 3.4, it suffices to consider the image of M in $\mathrm{PSL}(2,\mathbb{Z}/p^k\mathbb{Z})$, which we will denote M_k. Since $\mathrm{M}_k \in \mathrm{J}_k$, Lagrange's theorem and lemma 3.5 tells us that $\mathrm{M}_k^{p^{3k-3}} = \mathrm{I}$, and hence $\mathrm{M}_k^{p^{3k-3}}(z) = z$. It follows that $\mathrm{Ord}_{\mathrm{M}}(z) | p^{3k-3}$, so $\mathrm{Ord}_{\mathrm{M}}(z) = p^m$ for some $m \geq 0$. ■

Lemma 3.2 shows that we can analyze the action of $\mathrm{M} \in \mathrm{PSL}(2,\mathbb{Z}_p)$ on T_p by analyzing the permutations it induces on the finite sets L_k. Lemma 3.3 shows that for certain matrices, we can restrict our attention to considering the subpermutation M induces on the intersection of each integral branch with L_k. Lemma 3.4 shows we can even reduce M by projecting it down to $\mathrm{PSL}(2,\mathbb{Z}/p^k\mathbb{Z})$. We have reduced studying the action of $\mathrm{PSL}(2,\mathbb{Z}_p)$ on T_p to studying the action of a finite matrix group on a finite set, which will prove to be a fairly tractable problem.

3.3 Finding Orbits of Exponentially Increasing Length

Our goal will be to show that for some $\mathrm{M} \in \mathrm{PSL}(2,\mathbb{Z}_p)$, a fixed $e \in \mathbb{Z}_p$, and a sequence of balls $(e + p^k\mathbb{Z}_p)$ where $k \to \infty$, $\mathrm{Ord}_{\mathrm{M}}(e + p^k\mathbb{Z}_p)$ increases exponentially with respect to k. For this paper, 'increasing exponentially' will mean that $\mathrm{Ord}_{\mathrm{M}}(e + p^k\mathbb{Z}_p)$ is bounded below by some function ar^{k-b}, where $a \in \mathbb{R}_{>0}$, $b \in \mathbb{R}$, and $r \in \mathbb{R}_{>1}$. Finding precise values of a, b, and r is unimportant to us, although in this case we can generally take $r = p$. The next lemma is the primary building block of our main theorem:

Lemma 3.8. *Let* $\mathrm{M} \in \mathrm{PSL}(2, \mathbb{Z}_p)$, $\mathrm{M} \neq \mathrm{I}$ *be an identity-like matrix, and*

$$\mathrm{M} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

For sufficiently large k *and for some* $e \in \mathbb{Z}_p$, $\mathit{Ord}_{\mathrm{M}}(e + p^k\mathbb{Z}_p)$ *increases exponentially with respect to* k.

Proof. We will make the assumption for now that $e = 0$, and will only be required to take other values of e in special cases of M. Projection to $\mathrm{PSL}(2, \mathbb{Z}/p\mathbb{Z})$ shows that all powers M^n are identity-like. Define

$$\mathrm{M}^n = \begin{bmatrix} a_n & b_n \\ c_n & d_n \end{bmatrix}$$

Assume for our matrix M that $a = 1 + p^{i_a}u_a$, $b = p^{i_b}u_b$, $c = p^{i_c}u_c$, and $d = 1 + p^{i_d}u_d$, where u_a, u_b, u_c, u_d are all units and i_a, i_b, i_c, i_d are all positive integers. We will go through the proof in this general case, and then explore relaxing these assumptions.

We want to find the order of $0 + p^k\mathbb{Z}_p$ under M, which is equivalent to finding the least n such that

$$\mathrm{M}^n(0 + p^k\mathbb{Z}_p) = \frac{b_n}{d_n} - 0 \in p^k\mathbb{Z}_p$$

Since d_n is a unit for all n, this condition is equivalent to

$$b_n \in p^k\mathbb{Z}_p \iff |b_n| \leq p^{-k}$$

As we saw from lemma 3.7, $0 + p^k\mathbb{Z}_p$ has orbit length of the form p^j. Therefore, to find the least n above, it's sufficient to check $n = p^l$ for various l. Our calculations will make use of the binomial theorem for matrices, which we can apply in this case since the identity matrix commutes with all matrices.

We will consider the effect of raising M to a single power of p.

$$\begin{aligned} \mathrm{M}^p &= \left(\begin{bmatrix} 1 + p^{i_a}u_a & p^{i_b}u_b \\ p^{i_c}u_c & 1 + p^{i_d}u_d \end{bmatrix} \right)^p \\ &= \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} p^{i_a}u_a & p^{i_b}u_b \\ p^{i_c}u_c & p^{i_d}u_d \end{bmatrix} \right)^p \\ &= \sum_{j=0}^{p} \binom{p}{j} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}^{p-j} \begin{bmatrix} p^{i_a}u_a & p^{i_b}u_b \\ p^{i_c}u_c & p^{i_d}u_d \end{bmatrix}^j \end{aligned}$$

We have $\binom{p}{1} = p$, and a well-known combinatorial result asserts that p divides $\binom{p}{j}$ for all $1 \leq j \leq p - 1$.

Also assume for the moment that $p \geq 3$, so that p divides each of the entries of M^{p-2}, and can be factored out from this matrix. Then we can factor $p\mathrm{M}^2$ out of all terms of the above binomial expression except the first two:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + p \begin{bmatrix} p^{i_a} u_a & p^{i_b} u_b \\ p^{i_c} u_c & p^{i_d} u_d \end{bmatrix} + p \begin{bmatrix} p^{i_a} u_a & p^{i_b} u_b \\ p^{i_c} u_c & p^{i_d} u_d \end{bmatrix}^2 \left(\ldots \right)$$

The $(\ldots)$ term represents the rest of the binomial expression after factoring, and can safely be ignored. Expanding $(\mathrm{M}-\mathrm{I})^2$, we have

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + p \begin{bmatrix} p^{i_a} u_a & p^{i_b} u_b \\ p^{i_c} u_c & p^{i_d} u_d \end{bmatrix}$$

$$+ p \begin{bmatrix} p^{2i_a} u_a^2 + p^{i_b+i_c} u_b u_c & p^{i_b} u_b (p^{i_a} u_a + p^{i_d} u_d) \\ p^{i_c} u_c (p^{i_a} u_a + p^{i_d} u_d) & p^{2i_d} u_d^2 + p^{i_b+i_c} u_b u_c \end{bmatrix} \left(\ldots \right)$$

Pulling out the upper-right entries from the above sum, we find

$$b_p = 0 + p(p^{i_b} u_b) + p(p^{i_b u_b} u_b (p^{i_a} u_a + p^{i_d} u_d))(\ldots)$$

$$= p^{i_b+1} u_b (1 + (p^{i_a} u_a + p^{i_d} u_d)(\ldots))$$

As above, $(\ldots)$ represents terms from the rest of the binomial expansion. We now compare $|b|$ to $|b_p|$:

$$|b| = |p^{i_b} u_b| = p^{-i_b}, \quad |b_p| = |p^{i_b+1} u_b (1 + (p^{i_a} u_a + p^{i_d} u_d)(\ldots))| = p^{-(i_b+1)}$$

This equation holds because $1 + (p^{i_a} u_a + p^{i_b} u_b)(\ldots)$ is a unit.

We have essentially shown that $|b_p| = \frac{1}{p}|b|$. Now, we can take M^p as our new M and rerun the above argument on $(\mathrm{M}^p)^p = \mathrm{M}^{p^2}$, which will show that $|b_{p^2}| = \frac{1}{p}|b_p|$. Proceeding inductively,

$$|b_{p^m}| = \frac{1}{p^m}|b|$$

For sufficiently large k such that $p^{-k} < |b|$, the least m such that $\mathrm{M}^{p^m}(0 + p^k\mathbb{Z}_p) = 0 + p^k\mathbb{Z}_p$ will be the least m such that

$$\frac{|b|}{p^m} < p^{-k}$$

Such an m will be equal to $k - \mathrm{C}$ for some constant C depending on $|b|$ but not on k. Therefore, for sufficiently large k we find that $\mathrm{Ord}_{\mathrm{M}}(0 + p^k\mathbb{Z}_p) = p^m = p^{k-\mathrm{C}}$ increases exponentially in k.

We now wish to relax the assumption we made that $p^{i_a}u_a$, $p^{i_b}u_b$, $p^{i_c}u_c$, and $p^{i_d}u_d$ are all nonzero. From the expression

$$b_p = p^{i_b+1}u_b(1+(p^{i_a}u_a+p^{i_d}u_d)(...))$$

we can see that $p^{i_a}u_a = 0$, $p^{i_c}u_c = 0$, or $p^{i_d}u_d = 0$ do not affect our result that $|b_p| = \frac{1}{p}|b|$. On the other hand, $b = 0$ appears to create a problem, as this implies M fixes all $0+p^k\mathbb{Z}_p$. We can resolve this issue by conjugating M. Let $e \in \mathbb{Z}_p$. Then

$$\begin{bmatrix} 1 & e \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} \left(\begin{bmatrix} 1 & e \\ 0 & 1 \end{bmatrix} \right)^{-1} =$$

$$\begin{bmatrix} 1 & e \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} \begin{bmatrix} 1 & -e \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & e \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & -ea \\ c & d-ec \end{bmatrix} = \begin{bmatrix} a+ec & -ea+ed-e^2c \\ c & d-ec \end{bmatrix}$$

The upper right term of this matrix is $e(d-a-ec)$. If $c \neq 0$, we can certainly find some e such that $e(d-a-ec) \neq 0$, and identity-likeness is preserved by conjugation. Showing this new matrix has orbits of exponentially increasing length for $0+p^k\mathbb{Z}_p$ is equivalent to showing M has orbits of exponentially increasing length for vertices of the form $e+p^k\mathbb{Z}_p$.

On the other hand, if $b = 0$ and $c = 0$, M is a diagonal matrix, and $a_m = a^m$, $b_m = b^m$. In this case, we will let $e = 1$. Since $\mathrm{M}(1) = \frac{a}{d}$, and more generally $\mathrm{M}^m(1) = \frac{a^m}{d^m} = \left(\frac{a}{d}\right)^m$, let $\frac{a}{d} = f = 1+p^{i_f}u_f$. We can assume $u_f \neq 0$ since $\frac{a}{d} = \pm 1$ together with $ad-bc = ad = 1$ implies M is the identity matrix in $\mathrm{PSL}(2,\mathbb{Z}_p)$.

$$\mathrm{M}(1+p^k\mathbb{Z}_p) = 1+p^k\mathbb{Z}_p \iff \frac{a}{d} - 1 \in p^k\mathbb{Z}_p$$

$$\mathrm{M}^m(1+p^k\mathbb{Z}_p) = 1+p^k\mathbb{Z}_p \iff \left(\frac{a}{d}\right)^m - 1 \in p^k\mathbb{Z}_p$$

Define $f_m = \left(\frac{a}{d}\right)^m = (1+p^{i_f}u_f)^m$. We can analyze raising f to the p:

$$f_p = f^p = (1+p^{i_f}u_f)^p = \sum_{j=0}^{p} \binom{p}{j} (p^{i_f}u_f)^j$$

Assuming $p \geq 3$ (and using $i_f \geq 1$), we can factor out p^{2i_f+1} from $\binom{p}{j}(p^{i_f}u_f)^j$ for $j \geq 2$, and have

$$1+p^{i_f+1}u_a+p^{2i_f+1}u_f^2(...)$$

Therefore

$$|f_p - 1| = \frac{1}{p}|f-1|$$

An analogous inductive argument as in the previous cases shows that for sufficiently large k, $\mathrm{Ord}_{\mathrm{M}}(1+p^k\mathbb{Z}_p)$ increases exponentially in k.

We are left with the special case of $p=2$. Luckily, a direct calculation will suffice. Let $\mathrm{M}^n = \begin{bmatrix} a_n & b_n \\ c_n & d_n \end{bmatrix}$ as usual, and $a = 1+2^{i_a}u_a$, $b = 2^{i_b}u_b$, $c = 2^{i_c}u_c$, and $d = 1+2^{i_d}u_d$. We want to find the least n such that

$$\mathrm{M}^n(0+2^k\mathbb{Z}_2) = 0+2^k\mathbb{Z}_2 \iff |b_n| \le 2^{-k}$$

$0+2^k\mathbb{Z}_2$ has orbit length 2^j for some j. Consider squaring M:

$$\mathrm{M}^2 = \left(\begin{bmatrix} 1+2^{i_a}u_a & 2^{i_b}u_b \\ 2^{i_c}u_c & 1+2^{i_d}u_d \end{bmatrix}\right)^2$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + 2\begin{bmatrix} 2^{i_a}u_a & 2^{i_b}u_b \\ 2^{i_c}u_c & 2^{i_d}u_d \end{bmatrix} + \begin{bmatrix} 2^{i_a}u_a & 2^{i_b}u_b \\ 2^{i_c}u_c & 2^{i_d}u_d \end{bmatrix}^2$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 2^{i_a+1}u_a & 2^{i_b+1}u_b \\ 2^{i_c+1}u_c & 2^{i_d+1}u_d \end{bmatrix} +$$

$$\begin{bmatrix} 2^{2i_a}u_a^2 + 2^{i_b i_c}u_b u_c & 2^{i_b}u_b(2^{i_a}u_a + 2^{i_d}u_d) \\ 2^{i_c}u_c(2^{i_a}u_a + 2^{i_d}u_d) & 2^{2i_d}u_d^2 + 2^{i_b+i_c}u_b u_c \end{bmatrix}$$

So

$$b_2 = 0 + 2^{i_b+1}u_b + 2^{i_b}u_b(2^{i_a}u_a + 2^{i_d}u_d) = 2^{i_b}u_b(2+2^{i_a}u_a + 2^{i_d}u_d)$$

Since $2+2^{i_a}u_a+2^{i_d}u_d$ isn't a unit, $|b_2| < |b|$. If both $i_a, i_d \ge 2$, then in fact $|2+2^{i_a}u_a + 2^{i_d}u_d| = \frac{1}{2}$, so $|b_2| = \frac{1}{2}|b|$. However, $2+2^{i_a}u_a+2^{i_d}u_d$ might not have norm exactly $\frac{1}{2}$ - this scenario could occur if either $i_a = 1$ or $i_d = 1$. In a worst-case scenario, we could have $2+2^{i_a}u_a+2^{i_d}u_d = 0$, in which case M^2 fixes $0+2^k\mathbb{Z}_2$.

If $|2+2^{i_a}u_a+2^{i_d}u_d| < \frac{1}{2}$ but $2+2^{i_a}u_a+2^{i_d}u_d \neq 0$, then $|b_2| = \frac{1}{2^l}|b|$ for some fixed l. However, this scenario required $i_a = 1$ or $i_d = 1$, or in other notation, $|a-1| = \frac{1}{2}$ or $|d-1| = \frac{1}{2}$. Using the above calculation, we can observe that

$$a_2 = 1 + 2^{i_a+1}u_a + 2^{2i_a}u_a^2 + 2^{i_b+i_c}u_b u_c$$

Each of $2^{i_a+1}u_a$, $2^{2i_a}u_a^2$, and $2^{i_b+i_c}u_b u_c$ have norm at least $\frac{1}{4}$, so $|a_2 - 1| < \frac{1}{2}$. Analogously, $|d_2 - 1| < \frac{1}{2}$. Since this property avoids the issue we encountered above, we can rerun our calculation and precisely determine $|b_4| = \frac{1}{2}|b_2|$. Continuing inductively,

$$|b_{2^m}| = \frac{1}{2^{m-1}}|b_2| = \frac{1}{2^{m+l-1}}|b_2|$$

For sufficiently large k, this shows $\mathrm{Ord}_{\mathrm{M}}(0+2^k\mathbb{Z})$ increases exponentially in k.

If $(2+2^{i_a}u_a+2^{i_d}u_d)=0$, then $a+d=0$, or $a=-d$. Plugging into the determinant equation $ad-bc=1$, $-a^2=1+bc$. Reduce this equation mod 4: b and c are both divisible by 2 by the identity-likeness assumption, so bc vanishes, and we are left with $a^2\equiv-1 \mod 4$. This equation has no solutions, so we arrive at a contradiction.

If $b=0$, then we conjugate as in the $p>2$ case and repeat that argument. If $b=c=0$, then as before set $e=1$, $f=\frac{a}{d}=1+2^{i_f}u_f$, and $f_m=\left(\frac{a}{d}\right)^m=(1+2^{i_f}u_f)^m$. Then

$$\mathrm{M}^m(1+2^k\mathbb{Z}_p)=1+2^k\mathbb{Z}_2 \iff |f_m-1|\le 2^{-k}$$

We know this point has order 2^n for some n, so we'll analyze the effect of squaring f:

$$f_2=(1+2^{i_f}u_f)^2=1+2^{i_f+1}u_f+2^{2i_f}u_f^2$$

Certainly $|f_2-1|<|f-1|$, but $|f_2-1|=\frac{1}{2}|f-1|$ fails if $i_f=1$, or $|f-1|=\frac{1}{2}$. However, as long as $2^{i_f+1}u_f+2^{2i_f}u_f^2\ne0$, we will instead obtain some l so that $|f_2-1|=\frac{1}{2^l}|f-1|$. But now $|f_2-1|<\frac{1}{2}$, so we can induct on the above calculation and obtain

$$|f_{2^m}-1|=\frac{1}{2^{m-1}}|f_2|=\frac{1}{2^{m+l-1}}|f_2|$$

The proof now follows as in $p>2$. If in fact $2^{i_f+1}u_f+2^{2i_f}u_f^2=0$, then $f^2=1$ and $f=\pm1$, contradicting our assumptions.

Since the $p=2$ case is taken care of, we are done. ■

This addresses the question of finding orbits of exponentially increasing length on some branch. Since we'd like orbits of exponentially increasing length on more than one integral branch, we need to work out some subtleties related to how we proved lemma 3.8.

3.4 Conjugation and Generalizing to Multiple Branches

Lemma 3.9. *Let* $\mathrm{M}\in\mathrm{PSL}(2,\mathbb{Z}_p)$, $\mathrm{M}\ne\mathrm{I}$ *be an identity-like matrix, and*

$$\mathrm{M}=\begin{bmatrix} a & b\\ c & d\end{bmatrix}$$

For at least two integer branches $\mathrm{B}_1,\mathrm{B}_2$ *of* T_p *and for sufficiently large* k*, there exist points* $p_1,p_2,\dots\subset\mathrm{B}_i$ *such that* $p_i\in\mathrm{K}_{i+k}$ *and* $\mathrm{Ord}_{\mathrm{M}}(p_i)$ *increases exponentially in* i*.*

Proof. This proof will break down into checking several cases. First, assume $b\ne0$. Since $b\ne0$, we apply the proof from lemma 3.8, and see directly that points of the form $0+p^k\mathbb{Z}_p$ has exponentially increasing orbits under M with respect to k.

Now, let $M' = \begin{bmatrix} 1 & -e \\ 0 & 1 \end{bmatrix}$ for some unit $e \in \mathbb{Z}_p$. Then

$$M'M(M')^{-1} = \begin{bmatrix} 1 & -e \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & e \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & -e \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b+ae \\ c & d+ec \end{bmatrix}$$

$$= \begin{bmatrix} a-ec & b+ae-de-e^2c \\ c & d+ec \end{bmatrix}$$

Notice that the term $b+ae-de-e^2c$ is a quadratic polynomial with respect to e. Moreover, since $b \neq 0$, this polynomial is nonzero, and so only has finitely many solutions $e \in \mathbb{Z}_p$. Since each branch not containing $0+p\mathbb{Z}_p$ contains infinitely many possible choices for e, choose any e on such a branch such that $-ce^2+e(a-d)+b \neq 0$. For this choice of e, $0+p^k\mathbb{Z}_p$ has exponentially increasing orbits under $M'M(M')^{-1}$, so $e+p^k\mathbb{Z}_p$ for all $k \geq 1$ has exponentially increasing orbits under M.

We can now turn to the case where $b=0$. If $c \neq 0$, we can conjugate:

$$\begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} d-c & -c \\ a+(c-d) & a+c \end{bmatrix}$$

Since $-c \neq 0$ and conjugation preserves orders of elements within each integral branch (although the branches and the points themselves could be shuffled), this reduces to the previous case.

If both $b=0$ and $c=0$, then we know from the proof of lemma 3.8 that $1+p^k\mathbb{Z}_p$ has exponentially increasing orbits under M. We'll consider the sequence of points $2+p^k\mathbb{Z}_p$ for increasing $k \geq 1$. Since $M(z) = \frac{a}{d}z$,

$$M^n(2+p^k\mathbb{Z}_p) = 2+p^k\mathbb{Z}_p \iff 2\left(\frac{a}{z}\right)^n - 2 \in p^k\mathbb{Z}_p$$

If $p \neq 2$, this condition is equivalent to $\left(\frac{a}{z}\right)^n - 1 \in p^k\mathbb{Z}_p$ since 2 is a unit. So the fact that the sequence $1+p^k\mathbb{Z}_p$ for $k \geq 1$ has exponentially increasing orbits implies that $2+p^k\mathbb{Z}_p$ has the same property. If $p=2$, then

$$2\left(\left(\frac{a}{z}\right)^n - 1\right) \in 2^k\mathbb{Z}_2 \iff \left(\frac{a}{z}\right)^n - 1 \in 2^{k-1}\mathbb{Z}_2$$

The above expression, recalling the proof of lemma 3.8 in the case of $p=2$, implies that $\mathrm{Ord}_M(2+2^k\mathbb{Z}_2) = \frac{1}{2}\mathrm{Ord}_M(1+2^k\mathbb{Z}_2)$ for sufficiently large k. Since we know the orbits of

$1 + p^k\mathbb{Z}_p$ are exponentially increasing in k, the same property holds for $2 + p^k\mathbb{Z}_p$. Lastly, observe that $2 + p^k\mathbb{Z}_p$ lies on a different branch than $1 + p^k\mathbb{Z}_p$ - this last point is worthy of some elaboration, since different behavior occurs for $p = 2$ and $p > 2$. When $p > 2$, $1 + p\mathbb{Z}_p$ and $2 + p\mathbb{Z}_p$ are both adjacent to $0 + \mathbb{Z}_p$, and lie on the branches containing $1 + p^k\mathbb{Z}_p$ and $2 + p^k\mathbb{Z}_p$, respectively. When $p = 2$, points of the form $2 + 2^k\mathbb{Z}_2$ lie on the branch with $0 + 2\mathbb{Z}_2$ as the vertex adjacent to $0 + \mathbb{Z}_2$: this is the only integer branch aside from the branch containing $1 + 2\mathbb{Z}_2$. ■

We now have all the ingredients we need in the p-adic case, and can turn our attention to the case of $\mathbb{F}_p((x))$.

4 Analyzing $\mathrm{PSL}(2, \mathbb{F}_p[x])$

4.1 Geometric Preliminaries

Assume $\mathrm{N} \in \mathrm{PSL}(2, \mathbb{F}_p[x])$ is conjugate to an element of $\mathrm{PSL}(2, \mathbb{Z}_p)$ as tree automorphisms. In other words, there exists some $\mathrm{M} \in \mathrm{PSL}(2, \mathbb{Z}_p)$ and some $\varphi \in \mathrm{Aut}(\mathrm{T}_p)$ so that

$$\mathrm{N} = \varphi \circ \mathrm{M} \circ \varphi^{-1}$$

We will also assume that M is identity-like, since our analysis of actions on $\mathrm{PSL}(2, \mathbb{Z}_p)$ focused on matrices of this type. We can use the conjugacy equation above to determine a substantial amount of basic information about N.

First, note that M fixes $0 + \mathbb{Z}_p$. If we let $\varphi(0 + \mathbb{Z}_p) = v_0 = r + x^{k_0}\mathbb{F}_p[x]$, then

$$\mathrm{N}(v_0) = \varphi(\mathrm{M}(\varphi^{-1}(v_0))) = \varphi(\mathrm{M}(0 + \mathbb{Z}_p)) = \varphi(0 + \mathbb{Z}_p) = v_0$$

So N fixes v_0. Since φ is a tree automorphism, it induces a bijection between vertices adjacent to $0 + \mathbb{Z}_p$ and vertices adjacent to v_0. Since M fixes all vertices adjacent to $0 + \mathbb{Z}_p$, a calculation similar to above will show that N fixes all vertices adjacent to v_0.

More generally, let L'_k be the set of vertices of distance k from v_0. φ necessarily induces a bijection $\mathrm{L}_k \leftrightarrow \mathrm{L}'_k$ for every k, and by properties of conjugation (lemma 2.4) the existence of an element of order O under M in L_k implies the existence of an element of order O under N in L'_k, and vice-versa.

We should look at the $p + 1$ v_0-branches of T_p in relation to N. As in definition 3.3, we'll use the term 'downward branch' to refer to the p branches of v_0 not containing ∞ at their boundary. Since it is a tree automorphism, φ necessarily sends branches of $0 + \mathbb{Z}_p$ to branches of v_0.

Lemma 4.1. *Let* N *and* M *be as above. Then an integral branch of* $0 + \mathbb{Z}_p$ *containing points of exponentially increasing order is mapped to a downward branch of* v_0.

Proof. We know from lemma 3.8 that there are at least two integral branches of $0 + \mathbb{Z}_p$ containing points of exponentially increasing order. At most one of these branches can be mapped to the single non-downwards branch of v_0, so the other must be mapped to a downwards branch. ■

Our plan is now to show directly that no downwards branch of v_0 can contain points of exponentially increasing order. First, note that since N fixes the non-downwards branch containing ∞ at its boundary, N cannot send any ball on a downwards branch to the inverse of a ball. Moreover, since all balls on the intersection of some L'_k with a downward branch have the same radius, N fixes the radii of balls on downward branches. Combining these two facts, we obtain that for any $q + x^k\mathbb{F}_p[x]$ on a downwards branch, $\mathrm{N}(q + x^k\mathbb{F}_p[x]) = \mathrm{N}(q) + x^k\mathbb{F}_p[x]$.

Conceptually, the next lemma is comparable to lemma 3.4:

Lemma 4.2. *Assume* N *satisfies the conditions in the last paragraph, so* $\mathrm{N}(q + x^k\mathbb{F}_p[x]) = \mathrm{N}(q) + x^k\mathbb{F}_p[x]$ *for all vertices on downwards branches of* v_0*. Fix* $k \geq 0$ *and assume that* $q = x^{l_q}u_q$ *for some unit* u_q *and* $l_q \in \mathbb{Z}$*, so that* $q + x^k\mathbb{F}_p[x]$ *lies on a downwards branch of* v_0*. Assume that for some* m*,* N^m *is of the form*

$$\mathrm{N}^m = \begin{bmatrix} 1 + x^{l_a}u_a & x^{l_b}u_b \\ x^{l_c}u_c & 1 + x^{l_d}u_d \end{bmatrix}$$

for some units u_a, u_b, u_c, u_d *and integers* $l_a, l_b, l_c, l_d \geq \max(k+1, k+1-3l_q)$*. Then* N^m *fixes* $q + x^k\mathbb{F}_p[x]$*.*

Begin with

$$\mathrm{N}^m(q) - q = \frac{(1 + x^{l_a}u_a)q + x^{l_b}u_b}{x^{l_c}u_c q + (1 + x^{l_d}u_d)} - q$$

$$= \frac{(1 + x^{l_a}u_a)q + x^{l_b}u_b - x^{l_c}u_c q^2 - (1 + x^{l_d}u_d)q}{x^{l_c}u_c q + (1 + x^{l_d}u_d)}$$

We want to show this expression is in $x^k\mathbb{F}_p[x]$. $l_d \geq 1$, and $l_c \geq k+1-3l_q$ implies $l_c \geq 1-3l_q$ and thus $l_c + l_q \geq 1$. Therefore, the norm of $x^{l_c}u_c q + (1 + x^{l_d}u_d)$ will be 1, since the norm of $x^{l_d}u_d$ is p^{-l_d} and the norm of $x^{l_c}u_c q$ is $p^{-(l_c+l_q)}$. Therefore showing that

$$(1 + x^{l_a}u_a)q + x^{l_b}u_b - x^{l_c}u_c q^2 - (1 + x^{l_d}u_d)q \in x^k\mathbb{F}_p[x]$$

implies

$$\frac{(1 + x^{l_a}u_a)q + x^{l_b}u_b - x^{l_c}u_c q^2 - (1 + x^{l_d}u_d)q}{x^{l_c}u_c q + (1 + x^{l_d}u_d)} \in x^k\mathbb{F}_p[x]$$

as desired. But

$$(1 + x^{l_a}u_a)q + x^{l_b}u_b - x^{l_c}u_c q^2 - (1 + x^{l_d}u_d)q$$

$$x^{l_a}u_a q + x^{l_b}u_b - x^{l_c}u_c q^2 - x^{l_d}u_d q$$

$$= x^{l_a+l_q}u_a u_q + x^{l_b}u_b - x^{l_c+2l_q}u_c u_q^2 - x^{l_d+l_q}u_d u_q$$

If $l_q \geq 0$, then by $l_a+l_q, l_b, l_c+2l_q, l_d+l_q \geq k+1$, the above expression must be in $x^k\mathbb{F}_p[x]$. If $l_q < 0$, then $l_a, l_b, l_c, l_d \geq k+1-3l_q$, and so $l_a+l_q, l_b, l_c+2l_q, l_d+l_q \geq k+1$. Therefore, the above expression must be in $x^k\mathbb{F}_p[x]$. Either way, we obtain

$$\mathrm{N}^m(q) - q \in x^k\mathbb{F}_p[x]$$

$$\iff \mathrm{N}^m(q + x^k\mathbb{F}_p[x]) = q + x^k\mathbb{F}_p[x]$$

■

So by calculating powers of N, we can find an upper bound for $\mathrm{Ord}_\mathrm{N}(q + x^k\mathbb{F}_p[x])$.

4.2 Showing Orbit Lengths are Linear in k

Lemma 4.3. *Let* $\mathrm{N} \in \mathrm{PSL}(2, \mathbb{F}_p[x])$ *be an identity-like matrix such that* $\mathrm{N} \neq \mathrm{I}$, *and assume*

$$\mathrm{N} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Also fix $q \in \mathbb{F}_p((x))$ *and* $v_0 \in \mathrm{T}_p$, *and assume* N *fixes both* v_0 *and its branches. Lastly, assume* $q + x^k\mathbb{F}_p[x]$ *lies on a downward branch of* v_0 *for all sufficiently large* k. *Then* $\mathit{Ord}_\mathrm{N}(q + x^k\mathbb{F}_p[x])$ *is bounded above by a linear function in* k.

Fix some sufficiently large $k \geq 0$, so that $q + x^k\mathbb{F}_p[x] = x^{l_q}u_q + x^k\mathbb{F}_p[x]$ lies on a downwards branch of v_0. Let

$$\mathrm{N}^m = \begin{bmatrix} a_m & b_m \\ c_m & d_m \end{bmatrix}$$

By lemma 4.2, our goal is to find sufficiently large m so that all elements of $\mathrm{N}^m - \mathrm{I}$ have norm less than or equal to $p^{-\max(k+1, k+1-3l_q)}$. Assume $a = 1 + x^{l_a}u_a$, $b = x^{l_b}u_b$, $c = x^{l_c}u_c$, and $d = x^{l_d}u_d$, such that u_a, u_b, u_c, u_d are all units and $l_a, l_b, l_c, l_d \geq 1$. Consider raising N to the pth power:

$$\mathrm{N}^p = \begin{bmatrix} 1 + x^{l_a}u_a & x^{l_b}u_b \\ x^{l_c}u_c & 1 + x_{l_d}u_d \end{bmatrix}^p = \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} x^{l_a}u_a & x^{l_b}u_b \\ x^{l_c}u_c & x^{l_d}u_d \end{bmatrix} \right)^p$$

$$= \sum_{j=0}^{p} \binom{p}{j} \begin{bmatrix} x^{l_a}u_a & x^{l_b}u_b \\ x^{l_c}u_c & x^{l_d}u_d \end{bmatrix}$$

We now use the fact that p divides $\binom{p}{j}$ for all $1 \leq j \leq p-1$. Moreover, since our base ring $\mathbb{F}_p[x]$ has characteristic p, all terms in the above binomial expansion will vanish except the first and last. We're left with

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} x^{l_a}u_a & x^{l_b}u_b \\ x^{l_c}u_c & x^{l_d}u_d \end{bmatrix}^p$$

Now, let $l_m = \min(l_a, l_b, l_c, l_d) \geq 1$ be the minimal valuation of the entries, so that

$$\begin{bmatrix} x^{l_a} u_a & x^{l_b} u_b \\ x^{l_c} u_c & x^{l_d} u_d \end{bmatrix} = x^{l_m} \begin{bmatrix} x^{l_a - l_m} u_a & x^{l_b - l_m} u_b \\ x^{l_c - l_m} u_c & x^{l_d - l_m} u_d \end{bmatrix}$$

The above matrix is still an element of $\mathrm{PSL}(2, \mathbb{F}_p[x])$, so all of its entries will remain in $\mathbb{F}_p[x]$ under matrix exponentiation. Now

$$\begin{bmatrix} x^{l_a} u_a & x^{l_b} u_b \\ x^{l_c} u_c & x^{l_d} u_d \end{bmatrix}^p = (x^{l_m})^p \begin{bmatrix} x^{l_a - l_m} u_a & x^{l_b - l_m} u_b \\ x^{l_c - l_m} u_c & x^{l_d - l_m} u_d \end{bmatrix}^p$$

and we see that after multiplying $(x^{l_m})^p = x^{pl_m}$ back into the above matrix, the minimal valuation of the entries will be at least pl_m.

Define the *maximal norm* of an identity-like matrix N to be the maximum of the norms of the entries of N − I. For N above, its maximal norm is p^{-l_m} by definition of l_m, the minimal valuation. We have shown that N^p has maximal norm at most p^{-pl_m}.

N^p is still identity-like, so we can induct on the above calculation and conclude that the maximal norm of N^{p^i} is less than or equal to $p^{-p^i l_m}$. After substituting in equivalent definitions, lemma 4.2 directly states that if the maximal norm of N^{p^i} is less than $p^{-\max(k+1, k+1-3l_q)}$, then N^{p^i} fixes $q + x^k \mathbb{F}_p[x]$. But the maximal norm of N^{p^i} is bounded above by $p^{-p^i l_m}$, and

$$p^{-p^i l_m} \leq p^{-\max(k+1, k+1-3l_q)} \iff p^i l_m \geq \max(k+1, k+1-3l_q)$$

Now, $\max(k+1, k+1-3l_q)$ increases linearly in k, and l_m is fixed. Therefore, the least power p^i such that $p^i l_m \geq \max(k+1, k+1-3l_q)$ also increases linearly in k for sufficiently large k, and is in fact bounded above by $p\max(k+1, k+1-3l_q)$. But this power p^i is exactly what we need to raise N to in order to guarantee it fixes $q + x^k \mathbb{F}_p[x]$! Notice here that we want to determine the rate of growth of p^i, rather than i, since p^i is the power by which we're exponentiating N.

There are other cases to consider where $a = 1$, $b = 0$, $c = 0$, or $d = 1$, but these cases amount to little more than a difference in notation. In particular, the more extensive casework from lemma 3.8 is not necessary here. ■

Corollary 4.4. *Let* N*,* q*, and* v_0 *be as in lemma 4.2. Let* $v_0 = q_0 + x^{k_0}\mathbb{F}_p[x]$*. Then for sufficiently large* k*,* $\mathrm{Ord}_{\mathrm{N}}(q + x^k \mathbb{F}_p[x])$ *is bounded above by a linear function of* $k - k_0$*.*

Proof. This follows directly from the assertion that $\mathrm{Ord}_{\mathrm{N}}(q + x^k \mathbb{F}_p[x])$ is bounded above by a linear function of k, since k is itself a linear function of $k - k_0$. ■

The following lemma refines the above result by showing that a specific choice of q is not important in determining the bound.

Lemma 4.5. *Let* N *and* v_0 *be as above, and choose some* L'_k *for sufficiently large* k*. Then for every* $q + x^{k_0+k}\mathbb{F}_p[x]$ *on the intersection of the downwards branches of* v_0 *with* L'_k*,* $Ord_{\mathrm{N}}(q + x^{k_0+k}\mathbb{F}_p[x])$ *is bounded above by a linear function that depends on* k *but not on* q*.*

Proof. In the proof of lemma 4.3, we bounded $\mathrm{Ord}_{\mathrm{N}}(q + x^{k_0+k}\mathbb{F}_p[x])$ by $p\max((k_0 + k) + 1, (k_0 + k) + 1 - 3l_q)$, where q is written as $x^{l_q}u_q + x^{k_0+k}\mathbb{F}_p[x]$. However, if $v_0 = x^{r_0}u_0 + x^{k_0}\mathbb{F}_p[x]$ for some unit u_0 and integer r_0, then since $q + x^{k_0+k}\mathbb{F}_p[x]$ lies on a downwards branch of v_0, we can assume that $l_q \geq \min(r_0, k_0)$. This is because

$$q \in q + x^{k_0+k}\mathbb{F}_p[x] \subseteq x^{r_0}u_0 + x^{k_0}$$

and so

$$|x^{l_q}u_q - x^{r_0}u_0| \leq p^{-k_0}$$

If $l_q < r_0$, then $|x^{l_q}u_q - x^{r_0}u_0| = p^{-l_q}$ and $l_q \geq k_0$, showing $l_q \geq \min(r_0, k_0)$. Now, let $m = \min(r_0, k_0)$. $p\max((k_0+k)+1, (k_0+k)+1-3l_q) < p\max((k_0+k)+1, (k_0+k)+1-3m)$, so we can use $p\max((k_0+k)+1, (k_0+k)+1-3m)$ as our bound. Since m does not depend on q and this bound is still linear in k, we are done. ■

We need one more lemma and corollary before the main proof.

Lemma 4.6. *Let* $n \geq 1$ *and* $p > 2$*. Then*

$$|\mathrm{PSL}(2, \mathbb{F}_p[x]/x^n\mathbb{F}_p[x])| = \frac{(p^2-1)p^{3n-2}}{2}$$

If $p = 2$*, then*

$$|\mathrm{PSL}(2, \mathbb{F}_p[x]/x^n\mathbb{F}_p[x])| = (p^2-1)p^{3n-2}$$

Proof. This proof is analogous to lemma 3.5, since the numbers of units and nonunits are the same in $\mathbb{Z}/p^n\mathbb{Z}$ and $\mathbb{F}_p[x]/x^n\mathbb{F}_p[x]$.

Corollary 4.7. *Let* $\mathrm{N} \in \mathrm{PSL}(2, \mathbb{F}_p[x])$ *and* $p > 2$*. Then* $\mathrm{N}^{\frac{(p^2-1)p}{2}}$ *is identity-like. If* $p = 2$*, then* N^6 *is identity-like.*

Proof. The proof is analogous to corollary 3.1.

4.3 The Main Theorem: Incompatible Asymptotics

We are now ready for our main proof! We've already done almost all the work, and now just need to fit the pieces together. Up until this point, we've primarily been using matrix notation for linear fractional transformations, where functional iteration is captured by matrix multiplication. Since theorem 4.1 is stated in terms of function notation to match its initial presentation, we should mention that we are using dynamical iteration notation, where f^n represents the nth iterate of the function f.

Theorem 4.1. Let $f \in \mathrm{PSL}(2, \mathbb{Z}_p)$, $g \in \mathrm{PSL}(2, \mathbb{F}_p[x])$, and $h \in \mathrm{Aut}(\mathrm{T}_p)$, such that $g = h \circ f \circ h^{-1}$. Then $\mathrm{Ord}(f) = \mathrm{Ord}(g) < \infty$, and moreover $\mathrm{Ord}(f) = \mathrm{Ord}(g)$ is a divisor of $\frac{(p^2-1)p}{2}$ if $p > 2$, and $\mathrm{Ord}(f) = \mathrm{Ord}(g)$ is a divisor of 6 if $p = 2$. If f and g are identity-like, then in fact $\mathrm{Ord}(f) = \mathrm{Ord}(g) = 1$.

Proof. Assume $\mathrm{Ord}(f)$ and $\mathrm{Ord}(g)$ are not divisors of $\frac{(p^2-1)p}{2}$. We know that

$$g = h \circ f \circ h^{-1}$$

Assuming $p > 2$, raise both terms to the $\frac{(p^2-1)p}{2}$:

$$g^{\frac{(p^2-1)p}{2}} = (h \circ f \circ h^{-1})^{\frac{(p^2-1)p}{2}}$$

$$g^{\frac{(p^2-1)p}{2}} = h \circ f^{\frac{(p^2-1)p}{2}} \circ h^{-1}$$

By lemmas 3.5 and 4.5, both $g^{\frac{(p^2-1)p}{2}}$ and $f^{\frac{(p^2-1)p}{2}}$ are identity-like. Moreover, by assumption on the orders, $g^{\frac{(p^2-1)p}{2}} \neq \mathrm{I}$ and $f^{\frac{(p^2-1)p}{2}} \neq \mathrm{I}$. Let $f' = f^{\frac{(p^2-1)p}{2}}$ and $g' = g^{\frac{(p^2-1)p}{2}}$. If $p = 2$, let $f' = f^6$ and $g' = g^6$ to guarantee identity-likeness.

Proceeding from this assumption, let $h(0) = v_0$ (here we think of h as a function from the p-adic Serre tree to the Laurent Serre tree), where $v_0 = q_0 + x^{k_0}\mathbb{F}_p[x]$. Define L_k as the kth layer from 0 in the p-adic Serre tree, and L'_k as the kth layer from v_0 in the Laurent Serre tree. By lemma 3.8, we can find two integral branches B_1 and B_2 of 0 such that for a sufficiently large k, each $\mathrm{B}_i \cap \mathrm{L}_k$ contains a vertex $v_{k,i}$ such that $\mathrm{Ord}_{f'}(v_{k,i})$ increases exponentially with respect to k. By lemma 4.1, one of these branches, say B_1, is mapped to a downwards branch of v_0. Rename $\mathrm{B}_1 = \mathrm{B}$ and $v_{k,i} = v_k$. Since conjugation preserves orders of elements, we can consider the sequence $h(v_k) \in \mathrm{L}'_k$ and determine $\mathrm{Ord}_{g'}(h(v_k)) = \mathrm{Ord}_{f'}(v_k)$. By lemma 4.5, $\mathrm{Ord}_{g'}(h(v_k))$ is bounded above by an expression that is linear in k for sufficiently large k. So the sequence $\mathrm{Ord}_{g'}(h(v_k))$ is both exponentially increasing with respect to k, and bounded above by some expression that is linear with respect to k, as long as k is sufficiently large. Let $e(k)$ be the exponential lower bound and $l(k)$ be the linear upper bound. By

$$e(k) \leq \mathrm{Ord}_{g'}(h(v_k)) \leq l(k)$$

we have

$$e(k) \leq l(k)$$

for all sufficiently large k. Since any increasing exponential function (i.e. one where the base of exponentiation is strictly greater than 1) will overtake any linear function for sufficiently large k, we obtain a contradiction.

If f and g are already both identity-like, let $f' = f$ and $g' = g$ and continue as above.
■

4.4 A Corollary for Affine Maps

Theorem 4.1 has a corollary for affine maps. First, a familiar definition:

Definition 4.1. Let $f(z) = az + b = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \in \mathrm{Aff}(\mathbb{Z}_p)$, and let $\pi_1 : \mathrm{Aff}(\mathbb{Z}_p) \to \mathrm{Aff}(\mathbb{Z}/p\mathbb{Z})$ be the standard projection map. Then f is identity-like if $\pi_1(f) = \mathrm{I}$.

Notice that $\mathrm{PSL}(2, \mathbb{Z}_p)$ and $\mathrm{Aff}(\mathbb{Z}_p)$ have nonempty intersection, and the above definition is equivalent to the definition of identity-like elements of $\mathrm{PSL}(2, \mathbb{Z}_p)$ on the intersection. An analogous definition holds in the case of $\mathrm{Aff}(\mathbb{F}_p[x])$.

As in the special linear case, we can force f to be identity-like by taking a sufficiently high power:

Lemma 4.8. *Let $f(z) = az + b \in Aff(\mathbb{Z}_p)$. Then $f^{p(p-1)}$ is identity-like.*

Choosing an element of $\mathrm{Aff}(\mathbb{F}_p)$ requires selecting a unit a from $\mathbb{F}_p^*$ and an arbitrary element b from $\mathbb{F}_p$. $\mathbb{F}_p$ has p elements, $p-1$ of which are units, so necessarily $|\mathrm{Aff}(\mathbb{F}_p)| = p(p-1)$. The lemma now follows from Lagrange's theorem and the definition of an identity-like affine map. ■

Now, the main result.

Corollary 4.9. *Let $f \in Aff(\mathbb{Z}_p)$, $g \in Aff(\mathbb{F}_p[x])$, and $h \in Aut(\mathrm{T}_p)$ so that $g = h \circ f \circ h^{-1}$. Then $Ord(f) = Ord(g) < \infty$, and additionally $Ord(f) = Ord(g)$ is a divisor of $p(p-1)$.*

Proof Let f, g, and h be as above. Since $g = h \circ f \circ h^{-1}$, $g^2 = h \circ f^2 \circ h^{-1}$. Now, let f have matrix representation M, where

$$\mathrm{M} = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$$

and a is a unit. f is not generally an element of $\mathrm{PSL}(2, \mathbb{Z}_p)$, but f^2 has matrix representation

$$\mathrm{M}^2 = \begin{bmatrix} a^2 & b(a+1) \\ 0 & 1 \end{bmatrix}$$

This matrix still isn't an element of $\mathrm{PSL}(2, \mathbb{Z}_p)$, but notice that $f^2(z) = a^2 z + b(a+1)$ can also be written as $f^2(z) = \frac{az + a^{-1}b(a+1)}{a^{-1}}$, giving an equivalent matrix representation M' for f^2:

$$\mathrm{M}' = \begin{bmatrix} a & a^{-1}b(a+1) \\ 0 & a^{-1} \end{bmatrix}$$

and now $\mathrm{M}' \in \mathrm{PSL}(2, \mathbb{Z}_p)$. An analogous argument works to show $g^2 \in \mathrm{PSL}(2, \mathbb{F}_p[x])$. Of course, if f^2 and g^2 are in $\mathrm{PSL}(2, \mathbb{Z}_p)$ and $\mathrm{PSL}(2, \mathbb{F}_p[x])$, respectively, then their iterates are as well.

Since either p or $p-1$ is even, $2|p(p-1)$, and $f^{p(p-1)}$ and $g^{p(p-1)}$ are both identity-like and in $\mathrm{PSL}(2, \mathbb{Z}_p)$ and $\mathrm{PSL}(2, \mathbb{F}_p[x])$, respectively. So theorem 4.1 tells us that $f^{p(p-1)}$ and $g^{p(p-1)}$ are identity maps.

References

[1] Borel, A., Tits, J. (1973). *Homomorphismes Abstraits de Groups Algébriques Simples*. Annals of Mathematics, vol. 97, no. 3, pp. 499-571.

[2] Margulis, G. A. (1989). *Discrete Subgroups of Semisimple Lie Groups*. Berlin: Springer-Verlag.

[3] Serre, J.-P. (1977). *Trees*. Trans. Stilwell, J. Berlin: Springer-Verlag.

[4] Serre, J.-P., Tate, J. (1968). *Good Reduction of Abelian Varieties*. Annals of Mathematics, vol. 88, no. 3, pp. 492-517.

[5] Brown, K. S. (1989). *Buildings*. Berlin: Springer-Verlag.

[6] Armitage, J.V., Parker, J.R. (2007). *Jørgensen's Inequality for Non-Archimedean Metric Spaces*, pp. 97-111. In: Kapranov, M., Manin, Y.I., Moree, P., Kolyada, S., Potyagailo, L. (eds). Geometry and Dynamics of Groups and Spaces. Progress in Mathematics, vol. 265. Birkhauser: Basel and Boston.

[7] Parker, J. R. (2007). *p-adic Möbius Transformations*. In *Hyperbolic Spaces*. Published notes, https://maths.dur.ac.uk/~dma0jrp/img/HSjyvaskyla.pdf.

Henry W. Talbott
Brown University
htalbott@umich.edu