INSTITUT DE FRANCE
Académie des sciences

Comptes Rendus
Mathématique

Ruichao Jiang, Javad Tavakoli and Yiqiang Zhao

An upper bound and finiteness criteria for the Galois group of weighted walks with rational coefficients in the quarter plane

Volume 359, issue 5 (2021), p. 563-576

Published online: 13 July 2021

https://doi.org/10.5802/crmath.196

Les Comptes Rendus. Mathématique *sont membres du Centre Mersenne pour l'édition scientifique ouverte*
www.centre-mersenne.org
e-ISSN : 1778-3569

Comptes Rendus
Mathématique
2021, 359, nº 5, p. 563-576
https://doi.org/10.5802/crmath.196

Combinatorics, Probability theory / *Combinatoire, Probabilités*

An upper bound and finiteness criteria for the Galois group of weighted walks with rational coefficients in the quarter plane

Un majorant et des critères de finitude pour le groupe de Galois de marches pondérées avec des coefficients rationnels dans le quart de plan

Ruichao Jiang[a], **Javad Tavakoli**[*, a] **and Yiqiang Zhao**[b]

[a] The University of British Columbia Okanagan, Kelowna, BC V1V 1V7, Canada

[b] Carleton University, Ottawa, ON K1S 5B6, Canada

E-mail: javad.tavakoli@ubc.ca

Abstract. Using Mazur's theorem on torsions of elliptic curves, an upper bound 24 for the order of the finite Galois group $\mathscr{H}$ associated with weighted walks in the quarter plane $\mathbb{Z}_+^2$ is obtained. The explicit criterion for $\mathscr{H}$ to have order 4 or 6 is rederived by simple geometric arguments. Using division polynomials, a recursive criterion for $\mathscr{H}$ to have order $4m$ or $4m+2$ is also obtained. As a corollary, an explicit criterion for $\mathscr{H}$ to have order 8 is given through a method simpler than the existing one.

Résumé. En utilisant le théorème de Mazur sur les torsions de courbes elliptiques, on obtient un majorant 24 pour l'ordre du groupe fini de Galois $\mathscr{H}$ associé aux marches pondérées dans le quart de plan $\mathbb{Z}_+^2$. Le critère explicite pour que $\mathscr{H}$ soit d'ordre 4 ou 6 est obtenu par un simple argument géométrique. En utilisant des polynômes de division, un critère récursif pour $\mathscr{H}$ d'ordre $4m$ ou $4m+2$ est également obtenu. Comme corollaire, un critère explicite pour que $\mathscr{H}$ soit d'ordre 8 est donné et est beaucoup plus simple que la méthode existante.

Manuscript received 9th September 2020, revised 16th January 2021 and 6th February 2021, accepted 3rd March 2021.

* Corresponding author.

1. Introduction

Counting lattice walks is a classic problem in combinatorics. A combinatorial walk with nearest-neighbour step length can be seen as a weighted walk with weight 1 for the allowed directions and weight 0 for the forbidden directions. If a multiple step length requirement is allowed, a combinatorial walk can be seen as a weighted walk with integer weights. Without loss of generality, for a weighted walk, we may assume that the weights sum to 1 by normalization. If we allow the weights of a walk to take arbitrary non-negative real values that sum to 1, then we arrive at the realm of probabilistic walks in the quarter plane. So a weighted walk is the same thing as a probabilistic walk and a weighted walk with rational weights is the same thing as a combinatorial walk with different step lengths in different directions.

In the probabilistic scenario, an approach called the "kernel method" has been well developed and summarized in the book [6]. In the kernel method, Malyshev [14] defined a group $\mathscr{H}$, called the Galois group associated with any walk in $\mathbb{Z}_+^2$. The finiteness of $\mathscr{H}$ turns out to be important. In fact, the whole Chapter 4 of [6] is devoted to the study of the finiteness of $\mathscr{H}$. Here are some applications of $\mathscr{H}$:

(1) The finiteness of $\mathscr{H}$ helps to find an explicit formula of the generating function of the walk. See [9, 10] on the 2-demand queueing model and [13] on Gessel's walks.
(2) The generating function of the walk is holonomic, i.e. satisfying some linear differential equation if and only if $\mathscr{H}$ has finite order. Moreover the generating function is algebraic if and only if $\mathscr{H}$ has finite order and the orbit sum is zero. See [7] and [3, Theorem 42].

Bousquet-Mélou and Mishna [2] defined a similar group W and showed that for combinatorial walks with nearest-neighbour step length in the quarter plane, W can only have order 4, 6, or 8, if W has finite order. For a weighted walk, Kauers and Yatchak [12] found three walks with order 10, which is by far the largest known finite group order. The difference of W and $\mathscr{H}$ is that the former is defined on the whole $\mathbb{C}^2$ while $\mathscr{H}$ is defined on a compact Riemann surface Q determined by a biquadratic polynomial $Q(x, y)$. In fact, $\mathbb{C}^2$ can be foliated by a pencil of biquadratic curves, possibly with singular fibers. The theory of QRT (Quispel, Roberts, and Thompson) map in discrete dynamical system is concerned with this situation. In this paper, we focus on a single curve Q and consider $\mathscr{H}$.

In this paper, we only consider the generic case when the kernel of the walk determines genus 1 surface. We found 24 as an upper bound on the finite order of $\mathscr{H}$ when the weights of the walk are rationals. In particular, this result says that if the order of $\mathscr{H}$ is finite, then it cannot be arbitrarily large, in contrast to the genus 0 case, where $\mathscr{H}$ can have arbitrary finite orders [8]. The following list summarizes different objects considered in the paper and also serves as an outline of the proof:

(1) A biquadratic polynomial $Q(x, y)$ defines a connected real curve $Q \subset \mathbb{R}^2$. The composition of the horizontal and the vertical switches is called a QRT map δ on Q.
(2) By going to complex numbers, $Q(x, y)$ defines a Riemann surface, also called $Q \subset \mathbb{C}^2$. The Abel–Jacobi map $\mathscr{J}$ determines a lattice Λ generated by $\omega_1, \omega_2 \in \mathbb{C}$, unique up to the modular group $\mathrm{PSL}(2, \mathbb{Z})$ action, such that $Q \cong \mathbb{C}/\Lambda$.
(3) The Weierstrass function $\wp$ and its derivative $\wp'$ can be used to construct the uniformization map $\mathscr{W}$, an "inverse" of the Abel–Jacobi map $\mathscr{J}$. It is not an actual inverse because the image of $\mathscr{W}$ is not Q but an elliptic curve E in the Weierstrass normal form.
(4) Both $\mathscr{J}$ and $\mathscr{W}$ are defined analytically. However, their composition turns out to be a polynomial map. So if we start with a $Q(x, y)$ with rational coefficients, we obtain an elliptic curve E with rational coefficients.
(5) Moreover, the QRT map δ induces an addition by a rational point on E.
(6) So the Mazur theorem applies and the bound is obtained.

The organization of the rest of the paper is as follows: in Section 2 we introduce the model; Section 3 is an introduction of the theory of Riemann surfaces by vector field; Section 4 is an introduction of the theory of elliptic curves; in Section 5 we study the composition of the Abel–Jacobi map and the uniformization map; in Section 6 we prove our main results; Section 7 covers the criteria for $\mathscr{H}$ to have order $4m$ or $4m+2$. Section 8 is the conclusion.

2. Probabilistic model

In this section, we introduce the probability model of interest. We shall consider walks in $\mathbb{Z}_+^2$ with step length limited to 1 (nearest-neighbor) and the walk is considered to be homogeneous, that is, the transition probabilities $p_{i,j}$ $(-1 \le i, j \le 1)$ are independent of the current place.

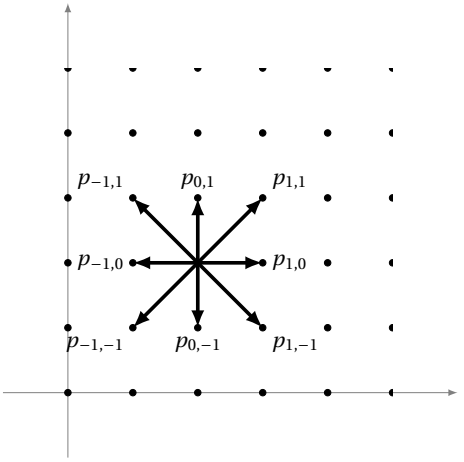

Figure 1. The model. $p_{0,0}$ is not shown.

To determine the stationary distribution $\{\pi_{ij}, i, j \in \mathbb{N}\}$ of the walk, following [6], the generating function method is applied. The generating function of the stationary distribution π_{ij} (excluding the probabilities of the boundary states) is

$$\pi(x,y) = \sum_{i,j\ge 1} \pi_{ij} x^{i-1} y^{j-1}, \tag{1}$$

where $x, y \in \mathbb{C}$ and $|x|, |y| < 1$.

$\pi(x,y)$ satisfies the following functional equation:

$$Q(x,y)\pi(x,y) = q(x,y)\pi(x) + \tilde{q}(x,y)\tilde{\pi}(y) + \pi_0(x,y), \tag{2}$$

where

$$Q(x,y) := xy\left(\sum_{i,j} p_{i,j} x^i y^j - 1\right). \tag{3}$$

Other terms reflect the boundary conditions on the random walk, which do not enter our study. Unlike $\pi(x,y)$, which is defined by a power series in the unit disc, $Q(x,y)$ is a polynomial and thus can be analytically continued to the whole complex plane $\mathbb{C}$.

$Q(x,y)$ is called the *kernel* of the random walk and is biquadratic, i.e. both quadratic in x and quadratic in y:

$$Q(x,y) := a(x)y^2 + b(x)y + c(x) := \tilde{a}(y)x^2 + \tilde{b}(y)x + \tilde{c}(y) \tag{4}$$

where

$$\begin{aligned} a(x) &= p_{1,1}x^2 + p_{0,1}x + p_{-1,1}, \\ b(x) &= p_{1,0}x^2 + (p_{0,0}-1)x + p_{-1,0}, \\ c(x) &= p_{1,-1}x^2 + p_{0,-1}x + p_{-1,-1}, \end{aligned}$$

and

$$\begin{aligned} \tilde{a}(y) &= p_{1,1}y^2 + p_{1,0}y + p_{1,-1}, \\ \tilde{b}(y) &= p_{0,1}y^2 + (p_{0,0}-1)y + p_{0,-1}, \\ \tilde{c}(y) &= p_{-1,1}y^2 + p_{-1,0}y + p_{-1,-1}. \end{aligned}$$

The following maps are defined on Q:

Definition 1 (Involutions and the QRT map). *The vertical switch ξ:*

$$\xi(x,y) := \left(x, -\frac{b(x)}{a(x)} - y\right). \tag{5}$$

The horizontal switch η:

$$\eta(x,y) := \left(-\frac{\tilde{b}(y)}{\tilde{a}(y)} - x, y\right). \tag{6}$$

The QRT map:

$$\delta := \xi \circ \eta. \tag{7}$$

Remark. As mentioned in the introduction, the QRT map is usually studied in a foliation of $\mathbb{C}^2$ by a pencil of biquadratic curves. We abuse the language and still call our δ here the QRT map, for a lack of better name and also the restriction of the original QRT map being an automorphism on each fiber.

ξ and η generate a group $\mathscr{H}$.

Definition 2 (Galois group). *The group*

$$\mathscr{H} := \langle \xi, \eta \rangle \tag{8}$$

is called the Galois group of the walk.

Remark. The reason why $\mathscr{H}$ is coined as Galois is essentially that Malyshev [14] adopted a field-theoretic definition of the Riemann surface Q, where a point on Q is defined as a discrete valuation on the function field $\mathbb{C}[x,y]/Q(x,y)$.

Remark. The QRT map $\delta = \eta \circ \xi$ generates a subgroup $\mathscr{H}_0 := \langle \delta \rangle \subseteq \mathscr{H}$. It's easy to see the index of $\mathscr{H}_0$ in $\mathscr{H}$ is two. Hence $\mathscr{H}_0$ is a normal subgroup of $\mathscr{H}$.

3. Results from Riemann surface theory

This section is a brief introduction to the theory of Riemann surfaces. There are various approaches for the theory of Riemann surfaces. Following [4], we adopt a dynamical system approach.

The kernel $Q(x,y) = 0$ determines a compact Riemann surface Q. In order to determine the topological structure of Q, we need to consider the partial discriminants of $Q(x,y)$.

Definition 3 (Partial discriminant). *The partial discriminants of*

$$Q(x,y) = a(x)y^2 + b(x)y + c(x) = \tilde{a}(y)x^2 + \tilde{b}(y)x + \tilde{c}(y)$$

are defined, respectively, as

$$\begin{aligned} \Delta_1(y) &:= \tilde{b}^2(y) - 4\tilde{a}(y)\tilde{c}(y), \\ \Delta_2(x) &:= b^2(x) - 4a(x)c(x). \end{aligned} \tag{9}$$

If the partial discriminant $\Delta_1(y)$ or equivalently $\Delta_2(x)$ has no multiple zeros, Q will double cover the Riemann sphere $\widehat{\mathbb{C}}$ with four distinct branching points [6]. By the Riemann–Hurwitz formula, the topological genus of Q is

$$g(Q) = 2(g(\widehat{\mathbb{C}}) - 1) + \frac{4}{2}(2-1) + 1 = 1. \tag{10}$$

We shall assume that Q has genus 1, which is generic.

Since Q has genus 1 and is orientable (a complex manifold is always orientable), it is topologically a torus.

After determining the topological structure, we need to classify the complex structure of Q. In fact, the complex structure of a torus can be classified by an associated lattice structure. Since Q has genus 1, there exists a non-vanishing vector field on Q due to the following proposition proved by Hopf [11]:

Proposition 4. *A compact, oriented manifold M possesses a nowhere vanishing vector field if and only if its Euler characteristic is zero.*

In fact, in our case, we have an explicitly nowhere vanishing vector field as follows:

Definition 5 (Hamiltonian vector field). *The Hamiltonian vector field v_H is defined as*

$$v_H := \frac{\partial Q}{\partial y}\frac{\partial}{\partial x} - \frac{\partial Q}{\partial x}\frac{\partial}{\partial y} = \big[2a(x)y + b(x)\big]\frac{\partial}{\partial x} - \big[2\tilde{a}(y)x + \tilde{b}(y)\big]\frac{\partial}{\partial y}. \tag{11}$$

In fact, Q has genus 1 if and only if the Hamiltonian vector field v_H is nowhere vanishing. This can be seen from the following lemma, which expresses the coefficients of v_H in terms of the partial discriminants.

Lemma 6.

$$\big[2a(x)y + b(x)\big]^2 = \Delta_2(x),$$
$$\big[2\tilde{a}(y)x + \tilde{b}(y)\big]^2 = \Delta_1(y).$$

Proof. For the first equation,

$$\begin{aligned} &[2a(x)y + b(x)]^2 = \Delta_2(x) \\ \Longleftrightarrow\ & b^2(x) + 4a(x)b(x)y + 4a^2(x)y^2 = b^2(x) - 4a(x)c(x) \\ \Longleftrightarrow\ & 4a(x)Q(x,y) = 0. \end{aligned}$$

The second equation can be proved similarly. □

The Hamiltonian vector field v_H determines a unique differential form as follows:

Definition 7 (Abelian differential). *The Abelian differential ω_H is determined by v_H via the relation $\langle \omega_H, v_H \rangle = 1$, where the pairing is the canonical pairing between vector fields and differential forms. Moreover, ω_H is explicitly given by*

$$\omega_H = \frac{\mathrm{d}x}{\sqrt{\Delta_2(x)}} = -\frac{\mathrm{d}y}{\sqrt{\Delta_1(y)}}. \tag{12}$$

Remark. The Abelian differential ω_H is well defined for the following reason: first of all, the dimension of the vector space of holomorphic differential forms on a Riemann surface is equal to the genus of the surface, hence two differential forms on Q differ at most by a scalar multiplication; second, the relation $\langle \omega_H, v_H \rangle = 1$ completely determines this scalar.

We need to consider the flow generated by this vector field. Since we are dealing with Riemann surfaces, we let the time variable of the flow take values in $\mathbb{C}$. In this case, the flow is sometimes called flow box.

Definition 8 (Integral curve). *A complex curve*

$$\gamma_{v,q} : \mathbb{C} \longrightarrow Q$$

is called the integral curve passing through q at time $t = 0$ of the vector field v if

$$\gamma'_{v,q}(t) = v(\gamma_{q,v}(t)) \quad \textit{and} \quad \gamma_{v,q}(0) = q.$$

Since Q is compact, the existence of the integral curve of a vector field is guaranteed by the Picard–Lindelöf theorem in ordinary differential equation theory.

Definition 9 (Flow). *The flow of the vector field v is the map*

$$\begin{aligned} \exp_v : \mathbb{C} \times Q &\longrightarrow Q \\ (t, q) &\longmapsto \gamma_{v,q}(t). \end{aligned}$$

The flow $\exp_{v_H}$ defines an action of the additive group $\mathbb{C}$ on Q.

Lemma 10. *The action of $\mathbb{C}$ defined by the flow $\exp_{v_H}$ is transitive on Q, i.e. $\forall\ q_1, q_2 \in Q$, $\exists\ t \in \mathbb{C}$ such that $\exp_{v_H}(t, q_1) = q_2$.*

Proof. Since v_H is nowhere vanishing, by the Picard–Lindelöf theorem, $\forall\ q_0 \in Q$, $q \in \mathrm{Orb}(q_0)$, there exists a ball $B_t(\delta t) \subseteq \mathbb{C}$ centered at t with radius δt such that $\exp_{v_H}(t, q) = q$ and $\exp_{v_H}(t, \cdot)$ maps $B_t(\delta t)$ homeomorphically into $\mathrm{Orb}(q_0)$. Hence, $\mathrm{Orb}(q_0)$ is open in Q. These open orbits form a partition of Q by open sets. Hence, $\mathrm{Orb}(q_0)$, being the complement of the union of all other open orbits, is also closed. Since Q is connected, there is only one orbit, i.e. $\mathrm{Orb}(q_0) = Q$. Hence, any two points q_1, q_2 can be mapped from one to the other by $q_1 \mapsto q_0 \mapsto q_2$, i.e. the action is transitive. □

Now we investigate the period of the flow. We have shown that for fixed $q \in Q$, the map $\exp_{v_H}(\cdot, q)$ is surjective and locally homeomorphic, hence $\exp_{v_H}(\cdot, q)$ is a covering map. Moreover, since $\mathbb{C}$ is simply connected, $\exp_{v_H}(\cdot, q)$ is a universal covering from $\mathbb{C}$ onto Q for all $q \in Q$. The universal covering of a torus is determined by a lattice Λ. Hence we have the following definition.

Definition 11 (Period group). *The period group $\Lambda \subseteq \mathbb{C}$ of the Hamiltonian vector field v_H is the additive subgroup of $\mathbb{C}$ consisting of elements $t \in \mathbb{C}$ such that $\exp_{v_H}(t, q) = q$ for all $q \in Q$. Let ω_H be the Abelian differential determined by v_H. Then Λ can be given explicitly by $\Lambda = \langle \omega_1, \omega_2 \rangle$, where*

$$\omega_1 = \int_{\gamma_1} \omega_H \qquad \textit{and} \qquad \omega_2 = \int_{\gamma_2} \omega_H,$$

where $[\gamma_1]$ and $[\gamma_2]$ form a basis of $H_1(Q, \mathbb{Z})$, the first homology group of Q with coefficients in $\mathbb{Z}$.

Remark. Under a modular group $\mathrm{PSL}(2, \mathbb{Z})$ action, we may choose $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$, where $\tau = \pm\frac{\omega_2}{\omega_1}$. The $\pm$ sign here makes $\mathrm{Im}(\tau) > 0$.

After passing to the quotient group, the covering map $\exp_{v_H}(\cdot, q)$ for an arbitrary q becomes an isomorphism between complex manifolds.

$$\exp_{v_H}(\cdot, q) : \mathbb{C}/\Lambda \to Q.$$

Here we abuse the notation for the covering map and its quotient.

As an isomorphism, the inverse map of $\exp_{v_H}(\cdot, q)$ exists. Moreover, it has an integral representation given by the Abel–Jacobi map.

Proposition 12 (Abel–Jacobi map). *Let $q \in Q$ be a fixed arbitrary point. Then the Abel–Jacobi map with base point q is defined by*

$$\begin{aligned} \mathscr{J} : Q &\longrightarrow \mathbb{C}/\Lambda \\ q' &\longmapsto \int_q^{q'} \omega \pmod{\Lambda}. \end{aligned} \tag{13}$$

$\mathscr{J}$ is well defined and does not depend on the path from q to q'. Moreover, $\mathscr{J}$ is the inverse of $\exp_{v_H}(\cdot, q)$ if we choose the same $q \in Q$ for both functions.

Now we need the transformation property of the QRT map under the Abel–Jacobi map.

Proposition 13. *The QRT map δ induces an addition on $\mathbb{C}/\Lambda$ via the Abel–Jacobi map, i.e. the following diagram is commutative:*

$$\begin{array}{ccc} Q & \xrightarrow{\delta} & Q \\ \downarrow{\scriptstyle \mathscr{J}} & & \downarrow{\scriptstyle \mathscr{J}} \\ \mathbb{C}/\Lambda & \xrightarrow{\delta^*} & \mathbb{C}/\Lambda \end{array}$$

The map δ^* is given by

$$\begin{aligned} \delta^* : \mathbb{C}/\Lambda &\longrightarrow \mathbb{C}/\Lambda \\ z &\longmapsto z + \omega_3 \pmod{\Lambda}, \end{aligned}$$

where $\omega_3 := \int_\gamma \omega_H \pmod{\Lambda}$ for any curve $\gamma : [0,1] \to Q$ such that $\gamma(1) = \delta(\gamma(0))$.

4. Results from elliptic curve theory

The theory of Riemann surface is intimately related to the theory of complex algebraic curves. In particular, a complex torus corresponds to an elliptic curve over $\mathbb{C}$. However, one advantage of the algebraic theory is that it not only works over $\mathbb{C}$ but also works over other fields, for example $\mathbb{Q}$. Eventually we will use results on elliptic curves over $\mathbb{Q}$. We will write $E(K)$ to emphasize that the polynomial defining the elliptic curve E has coefficients over K and there exists a point on E with coordinates in K.

Our goal is to transform a biquadratic curve Q to an elliptic curve $E(\mathbb{C})$ in the Weierstrass normal form as defined below. We have already transformed Q to $\mathbb{C}/\Lambda$ via the Abel–Jacobi map $\mathscr{J}$. Now we show how to transform $\mathbb{C}/\Lambda$ to $E(\mathbb{C})$. For this, we need the Weierstrass uniformization map.

Definition 14 (Weierstrass normal form). *An elliptic curve $E(\mathbb{C})$ is said to be in the Weierstrass normal form if $E(\mathbb{C})$ is defined by the polynomial*

$$y^2 = 4x^3 - g_2 x - g_3.$$

Remark. The nomenclature g_2 and g_3 here is related to the modular invariants defined later.

An elliptic curve carries an intrinsic abelian group structure $+ : E \times E \to E$, which can be defined without any embedding into some ambient space. Hence, in principle, there exists a group structure on the biquadratic curve Q. However, we do not know any explicit description of this group. In particular, we do not know the relationship between the Galois group $\mathscr{H}$ and the group structure on Q. On the other hand, in the Weierstrass normal form, the group structure is well known and has a geometrical description, known as the chord-tangent construction.

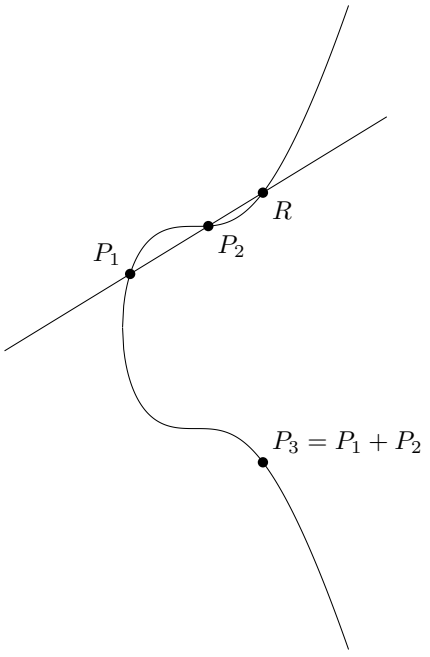

Figure 2. The group law on an elliptic curve E in Weierstrass normal form. Only the real part of E is shown.

Definition 15 (Chord-tangent construction). *The group law*

$$+ : E \times E \to E$$

on an elliptic curve E in Weierstrass normal form is given by

(1) *For any two points $P_1, P_2 \in E$, if $P_1 \neq P_2$, join P_1 and P_2; if $P_1 = P_2$, draw the tangent line of E at $P_1 = P_2$. Denote the third intersection of the line P_1P_2 or the tangent line with E by R;*
(2) *Reflect the point R with respect to the x-axis and the result is $P_1 + P_2$.*

Remark. For a proof that + is well defined, i.e., it is indeed a group law on E, see [19]. The only difficulty is to show the associativity of +, which uses the result: if two cubic curves intersect in nine points and a third cubic curve passes through eight of the intersections, then it also passes through the ninth intersection. Since the whole construction is algebraic, this group law works for any base field.

To define the Weierstrass uniformization, we need the Weierstrass elliptic function $\wp$.

Definition 16 (Weierstrass elliptic function). *For a lattice Λ, the Weierstrass function $\wp : \mathbb{C} - \Lambda \to \mathbb{C}$ is defined by*

$$\wp(z) := \frac{1}{z^2} + \sum_{\substack{\omega \neq 0 \\ \omega \in \Lambda}} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right] \tag{14}$$

with derivative being

$$\wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}. \tag{15}$$

Remark. Both series for $\wp$ and $\wp'$ converge locally uniformly in $\mathbb{C} - \Lambda$, hence they define holomorphic functions on $\mathbb{C} - \Lambda$. Moreover, by the definition, $\wp$ and $\wp'$ are doubly periodic functions with period lattice Λ.

Definition 17 (Modular invariants). *The modular invariants for a lattice Λ are defined by*

$$g_2(\Lambda) := 60 \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \omega^{-4} \quad \textit{and} \quad g_3(\Lambda) := 140 \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \omega^{-6}. \tag{16}$$

Remark. The modular invariants g_2 and g_3 are related to Eisenstein series. The Eisenstein series of weight $2k$, for $k \geq 2$, are defined as

$$G_{2k}(\Lambda) = \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \omega^{-2k}.$$

Then, obviously $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_4(\Lambda)$. Later in Lemma 22, we will see a relationship between g_2 and g_3 with Eisenstein invariants.

Now define a function $F(z) := \wp'(z)^2 - 4\wp(z)^3 + g_2(\Lambda)\wp(z) + g_3(\Lambda)$. Then, by the definition, $F(z)$ has period lattice Λ. From the series expansions of $\wp, \wp', g_2$, and g_3, $F(z)$ is holomorphic and $F(0) = 0$. By the maximum principle, $F \equiv 0$. Hence, Weierstrass functions and their derivatives establish an isomorphism between Riemann surfaces of genus 1 and elliptic curves over $\mathbb{C}$. In fact, this isomorphism is not only a complex analytical isomorphism but also a group isomorphism. For a proof, see [18, p. 173].

Proposition 18 (Weierstrass Uniformization Map). *The map*

$$\begin{aligned} \mathscr{W} : \mathbb{C}/\Lambda &\longrightarrow E(\mathbb{C}) \\ z &\longmapsto (\wp(z), \wp'(z)) \end{aligned}$$

is an isomorphism of complex manifolds and also a group isomorphism.

Remark. That the Weierstrass uniformization map is a group isomorphism explains various addition formulas of elliptic functions. It can be seen as an "inverse" of the Abel–Jacobi map. $\mathscr{J}$ transforms Q to $\mathbb{C}/\Lambda$ and $\mathscr{W}$ transforms $\mathbb{C}/\Lambda$ to $E(\mathbb{C})$, which is isomorphic to Q. The composition $\mathscr{W} \circ \mathscr{J}$ has the effect of a change of coordinates.

For elliptic curves over $\mathbb{Q}$, the following theorems hold.

Theorem 19 (Mordell). *The rational points on an elliptic curve form a finitely generated abelian group.*

The proof of the Mordell theorem can be found in [18].

Theorem 20 (Mazur). *For any $E(\mathbb{Q})$, the torsion subgroup T has only the following forms:*

(1) $\mathbb{Z}/N\mathbb{Z}$, *where* $1 \leq N \leq 10$ *or* $N = 12$,
(2) $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$, *where* $1 \leq N \leq 4$.

Remark. The proof of the Mazur theorem is rather complicated, and by now there is no simpler proof than the original papers [15, 16]. The rough idea is to study the modular curves $Y_1(N)$ and their compactification $X_1(N)$, which are moduli spaces of the elliptic curves with a torsion point of order N. Mazur showed that for $N > 13$, $Y_1(N)$ is empty. The result for $N = 13$ was obtained in 1973 by Mazur and Tate [17]. The result for $N = 11$ was obtained in 1940 by Billing and Mahler [1].

5. Composition of $\mathscr{J}$ and $\mathscr{W}$

In Section 6, we will apply the Mordell theorem and the Mazur theorem to obtain our main result. First, we need to show that the elliptic curve $E = \mathscr{W} \circ \mathscr{J}(Q)$ has rational coefficients and $\Omega_3 = \mathscr{W}(\omega_3)$ is a rational point.

We consider the action of the QRT map on three objects: the biquadratic curve Q, the complex torus $\mathbb{C}/\Lambda$, and the elliptic curve $E(\mathbb{C})$.

Notice that the modular invariants $g_2(\Lambda)$ and $g_3(\Lambda)$ depend analytically on Λ. However, Proposition 22 computes $g_2(\Lambda)$ and $g_3(\Lambda)$ algebraically in terms of the coefficients of Q. Before stating this proposition, we need to introduce the following invariants of a general quartic polynomial.

Definition 21 (Eisenstein invariants). *Let $f(x) = ax^4 + 4bx^3 + 6cx^2 + 4dx + e$ be a quartic polynomial. The Eisenstein invariants of f are*

$$\begin{aligned} D(f) &:= ae + 3c^2 - 4bd, \\ E(f) &:= ad^2 + b^2e - ace - 2bcd + c^3. \end{aligned} \tag{17}$$

The following proposition relates the Eisenstein invariants of the partial discriminants of the biquadratic curve Q with the modular invariants of the Weierstrass normal curve $E(\mathbb{C})$. The proof can be found in [4, Corollary 2.4.7].

Proposition 22. *Let*

$$\mathscr{W} \circ \mathscr{J} : Q \longrightarrow \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})$$

be the composition of the Abel–Jacobi map and the Weierstrass uniformization map. Then, the $E(\mathbb{C})$ is given by:

$$\begin{aligned} y^2 &= 4x^3 - Dx + E \\ D &:= D(\Delta_1) = D(\Delta_2), \\ E &:= E(\Delta_1) = E(\Delta_2), \end{aligned} \tag{18}$$

where D and E are Eisenstein invariants of the partial discriminants Δ_1 and Δ_2 of Q respectively.

Remark. Although both the Abel–Jacobi map $\mathscr{J}$ and the uniformization map $\mathscr{W}$ are analytic, their composition is completely given by polynomial functions.

Denote $\mathscr{W}(\omega_3)$ by Ω_3. Since $\mathscr{W}$ is a group isomorphism, and by Proposition 13, the QRT map δ induces an addition operation δ^* on $\mathbb{C}/\Lambda$, we know that δ also induces an addition operator $\delta^{**} : P \mapsto P + \Omega_3$ for $P \in E(\mathbb{C})$.

Proposition 24 calculates the coordinates of Ω_3 in terms of the Frobenius invariants. The proof can be found in [4, Proposition 2.5.6]. Since the coordinates of Ω_3 are important, we sketch the proof here. First, we study the pullback of the Weierstrass function $\wp$ on $\mathbb{C}/\Lambda$ by the Abel–Jacobi map.

Lemma 23. *Let $\mathscr{J} : Q \to \mathbb{C}/\Lambda$ be the Abel–Jacobi map. Then the pullback of the Weierstrass function $\wp$ on $\mathbb{C}/\Lambda$ is a rational function $\mathscr{P}(x, y)$ on Q. Moreover, assume that $(0,0) \in Q(x, y)$, i.e., $p_{-1,-1} = 0$, then $\mathscr{P}(x, y)$ has the following expression:*

$$\begin{aligned} \mathscr{P}(x, y) := &-(p_{1,-1}x + p_{0,01})(p_{-1,1}y + p_{-1,0})/xy \\ &+ \big((p_{0,0} - 1)^2 - 4p_{0,1}p_{0,-1} - 4p_{1,0}p_{-1,0} + 8p_{1,-1}p_{-1,1}\big)/12. \end{aligned} \tag{19}$$

Proof. Assume that $p_{0,1} \neq 0$ and $p_{-1,0} \neq 0$, i.e., Q is not tangent to the x-axis and y-axis at $(0,0)$. Then the function $1/xy$ has a pole of order two at $(0,0) \in Q$. From $Q(x,0) = (p_{1,-1}x + p_{0,-1})x$ and $Q(0,y) = (p_{-1,1}y + p_{-1,0})y$, it follows that $1/xy$ has a pole of order one at $(-p_{0,-1}/p_{1,-1}, 0)$ and $(0, -p_{-1,0}/p_{-1,1})$, respectively. It follows that the function $b(x,y) := -(p_{1,-1}x + p_{0,01})(p_{-1,1}y + p_{-1,0})/xy$ has only one pole of order two on the biquadratic curve Q. Let $\gamma(t) = (x(t), y(t))$ be the integral curve of the Hamiltonian vector field v_H. We need to evaluate the Taylor expansions of $x(t)$ and $y(t)$. The Hamiltonian equations say

$$\frac{\mathrm{d}x}{\mathrm{d}t} = \frac{\partial Q}{\partial y}, \quad \frac{\mathrm{d}y}{\mathrm{d}t} = -\frac{\partial Q}{\partial x}.$$

Hence, for any meromorphic function $f(x,y)$, we have

$$\frac{\mathrm{d}f(x(t),y(t))}{\mathrm{d}t} = \frac{\partial f}{\partial x}\frac{\mathrm{d}x}{\mathrm{d}t} + \frac{\partial f}{\partial y}\frac{\mathrm{d}y}{\mathrm{d}t} = \frac{\partial Q}{\partial y}\frac{\partial f}{\partial x} - \frac{\partial Q}{\partial x}\frac{\partial f}{\partial y} = v_H f.$$

Consequently, $\frac{\mathrm{d}^n f}{\mathrm{d}t^n} = v_H^n f$, which means applying v_H on f n times. In particular, choosing f to be the projections on the first and second variables gives the derivatives of $x(t)$ and $y(t)$, respectively, to any order. It follows that

$$b(x(t),y(t)) = \frac{1}{t^2} - \big((p_{0,0}-1)^2 - 4p_{0,1}p_{0,-1} - 4p_{1,0}p_{-1,0} + 8p_{1,-1}p_{-1,1}\big)/12 + \mathcal{O}(|t|).$$

Define $\mathscr{P}(x,y) := b(x,y) + ((p_{0,0}-1)^2 - 4p_{0,1}p_{0,-1} - 4p_{1,0}p_{-1,0} + 8p_{1,-1}p_{-1,1})/12$. Then $t \mapsto \mathscr{P}(x(t),y(t))$ is a meromorphic function of $t \in \mathbb{C}$ with a pole of order two at Λ and no other poles. Moreover, by the periodicity of the Hamiltonian flow, $\mathscr{P}(x(t),y(t))$ is doubly periodic. By the maximum principle, $\mathscr{P}(x(t),y(t)) \equiv \wp(t)$. Since $\mathscr{P}(x,y)$ depends continuously on the coefficients $p_{i,j}$, Equation (5) also holds true in the case $p_{0,1}=0$ or $p_{-1,0}=0$. □

Remark. Lemma 23 establishes a canonical isomorphism between the function field $K(Q)$ and $K(\mathbb{C}/\Lambda)$. Since a translation of Q to the origin $(0,0)$ does not affect $K(Q)$, our assumption $(0,0) \in Q(x,y)$ does not lose any generality. The formula of $\mathscr{P}'(x,y)$ is complicated but can be computed as $v_H\mathscr{P}(x,y)$. We refer the reader to [4, Lemma 2.4.13].

Proposition 24 (Frobenius Invariants). *The addition δ^{**} on $E(\mathbb{C})$ induced by the QRT map δ sends the point at infinity O to $\Omega_3 = (X,Y)$, where*

$$\begin{aligned} X &= (p_{0,0}^2 - 4p_{0,-1}p_{0,1} - 4p_{-1,0}p_{1,0} + 8p_{-1,1}p_{1,-1} + 8p_{-1,-1}p_{1,1})/12 \\ Y &= -\det\mathbb{P}, \end{aligned} \tag{20}$$

where

$$\mathbb{P} = \begin{pmatrix} p_{1,1} & p_{1,0} & p_{1,-1} \\ p_{0,1} & p_{0,0}-1 & p_{0,-1} \\ p_{-1,1} & p_{-1,0} & p_{-1,-1} \end{pmatrix}.$$

Proof. If $0 \notin Q$, but instead we have $(r,0) \in Q$, which is always possible since we work with complex numbers. A translation $x \mapsto r+x$, where r is a root of $p_{1,-1}r^2 + p_{0,-1}r + p_{-1,-1} = 0$, may be applied first and we can assume that $(0,0) \in Q$. We take $(0,0)$ as the initial value of the Hamiltonian flow. The QRT map δ on Q sends $(0,0)$ to (x_0,y_0), where

$$x_0 = -\frac{p_{0,-1}}{p_{1,-1}} \quad \text{and} \quad y_0 = -\frac{p_{1,0}x_0^2 + (p_{0,0}-1)x_0 + p_{-1,0}}{p_{1,1}x_0^2 + p_{0,1}x_0 + p_{-1,1}}.$$

Then $X = \mathscr{P}(x_0,y_0)$ and $Y = \mathscr{P}'(x_0,y_0) = v_H\mathscr{P}(x_0,y_0)$, where $\mathscr{P}(x,y)$ is the pullback of the Weierstrass function by the Abel–Jacobi map. □

Remark. The quantities X and Y are called Frobenius invariants by Duistermaat [4]. It would be interesting if a probabilistic interpretation of (X,Y) could be found. The calculation of X and Y is tedious and in [4], a formula manipulation program is used.

6. Main result

Results in previous sections can be summarized in the following commutative diagram:

$$\begin{array}{ccc} Q & \xrightarrow{\delta} & Q \\ \downarrow{\scriptstyle \mathscr{J}} & & \downarrow{\scriptstyle \mathscr{J}} \\ \mathbb{C}/\Lambda & \xrightarrow{\delta^*} & \mathbb{C}/\Lambda \\ \downarrow{\scriptstyle \mathscr{W}} & & \downarrow{\scriptstyle \mathscr{W}} \\ E(\mathbb{C}) & \xrightarrow{\delta^{**}} & E(\mathbb{C}) \end{array}$$

Gathering around all information, we state the main result of this paper.

Theorem 25. *A finite Galois group $\mathscr{H}$ of the weighted walk with rational coefficients can have order at most 24.*

Proof. Since the kernel $Q(x,y)$ has rational coefficients, by Proposition 22, the associated elliptic curve E in the Weierstrass normal form $y^2 = 4x^3 - g_2x - g_3$ also has rational coefficients, i.e. $g_2, g_3 \in \mathbb{Q}$. By Proposition 24, $\Omega_3 = \mathscr{W}(\omega_3) \in E(\mathbb{Q})$. Then, the group $\langle\Omega_3\rangle$ generated by Ω_3 is a subgroup of $E(\mathbb{Q})$. By Proposition 13 and Proposition 18, $\mathscr{H}_0$ is isomorphic to $\langle\Omega_3\rangle$. Hence, $\mathscr{H}_0$ is a subgroup of $E(\mathbb{Q})$. By the Mordell theorem, $E(\mathbb{Q})$ is finitely generated. By the fundamental theorem of finitely generated abelian group, $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$, where $r \in \mathbb{N}$ and T is the torsion subgroup. Since $\mathscr{H}$ is assumed to be finite, $\mathscr{H}_0$ is a subgroup of the torsion subgroup T. By the Mazur theorem, $|T| \le 12$, therefore $|\mathscr{H}_0| \le 12$. Since $|\mathscr{H}/\mathscr{H}_0| = 2$, $|\mathscr{H}| \le 24$. □

We rederive two known criteria for the weighted walks having order 4 and 6 using geometric arguments. The original proofs appear in [6, Chapter 4].

Theorem 26 (Criterion for $\mathscr{H}$ of order 4). *$\mathscr{H}$ has order 4 if and only if* $\det\mathbb{P} = 0$.

Proof. $\mathscr{H}$ has order 4 if and only if Ω_3 is a torsion point of order 2 in $E(\mathbb{C})$. The result is obtained by the fact that a point in a Weierstrass normal curve has order 2 if and only if its Y coordinate is 0. □

Theorem 27 (Criterion for $\mathscr{H}$ of order 6). *$\mathscr{H}$ has order 6 if and only if*

$$\begin{vmatrix} -12X & 0 & D \\ 0 & 1 & Y \\ D & Y & DX+3E \end{vmatrix} = 0, \tag{21}$$

where $\Omega_3 = (X,Y)$ is given by Proposition 24 and $D := D(\Delta_1) = D(\Delta_2)$ and $E := E(\Delta_1) = E(\Delta_2)$ are Eisenstein invariants given by Proposition 22.

Proof. $\mathscr{H}$ has order 6 $\Leftrightarrow$ $\Omega_3 = (X,Y)$ is a torsion point of order 3 in $E(\mathbb{C})$ $\Leftrightarrow$ Ω_3 is a flex point $\Leftrightarrow$ $\det\big(\mathrm{Hess}(f)\big)$ vanishes on $(X,Y,1)$, where $f(x,y,z)$ is the homogeneous polynomial

$$f(x,y,z) = y^2z - 4x^3 + g_2xz^2 + g_3z^3.$$

The result is obtained by direct calculation. □

Remark. The following result for $\mathscr{H}$ to have order 6 is given by Proposition 4.1.8 in [6]: $\mathscr{H}$ has order 6 if and only if

$$\begin{vmatrix} \Delta_{11} & \Delta_{21} & \Delta_{12} & \Delta_{22} \\ \Delta_{12} & \Delta_{22} & \Delta_{13} & \Delta_{23} \\ \Delta_{21} & \Delta_{31} & \Delta_{22} & \Delta_{32} \\ \Delta_{22} & \Delta_{32} & \Delta_{23} & \Delta_{33} \end{vmatrix} = 0,$$

where Δ_{ij}'s are cofactors of the matrix $\mathbb{P}$.

7. Criterion for orders $4m$ and $4m+2$

In this section, we give criteria for $\mathscr{H}$ to have orders $4m$ or $4m+2$ using division polynomials. The criteria given in [6] are abstract, requiring linear dependence of certain functions in some function field. Our result is completely given by division polynomials.

Definition 28 (Division Polynomials). *Let $y^2 = 4x^3 - g_2x - g_3$ be an elliptic curve. The division polynomials are given by*

$$\begin{aligned}
\Psi_1 &= 1,\\
\Psi_2 &= y,\\
\Psi_3 &= 48x^4 - 24g_2x^2 - 48g_3x - g_2^2,\\
\Psi_4 &= y\big(64x^6 - 80g_2x^4 - 320g_3x^3 - 20g_2^2x^2 - 16g_2g_3x + g_2^3 - 32g_3^2\big),\\
\Psi_{2m+1} &= \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3, \qquad m \geq 2,\\
\Psi_{2m} &= \frac{1}{y}\Psi_m\big(\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2\big), \qquad m \geq 3.
\end{aligned}$$

The division polynomials are so called because they satisfy the following proposition.

Proposition 29. *Following the notation in Definition 28. $m|n \Rightarrow \Psi_m|\Psi_n$ in $\mathbb{Z}[x,y]$. And any point (x,y) is a torsion point of order dividing n if and only if $\Psi_n(x,y) = 0$.*

Proposition 29 provides explicit criteria for $\mathscr{H}$ to have orders $4m$ or $4m+2$.

Corollary 30 (Criterion for $\mathscr{H}$ of order $4m$). *$\mathscr{H}$ has order $4m$ if and only if $\Psi_n(X,Y) \neq 0$ for all $n|2m, n \neq 2m$ and $\Psi_{2m}(X,Y) = 0$.*

Corollary 31 (Criterion for $\mathscr{H}$ of order $4m+2$). *$\mathscr{H}$ has order $4m+2$ if and only if $\Psi_n(X,Y) \neq 0$ for all $n|(2m+1), n \neq 2m+1$ and $\Psi_{2m+1}(X,Y) = 0$.*

In particular, for $\mathscr{H}$ to have order 8, we have the following result:

Corollary 32 (Criterion for $\mathscr{H}$ of order 8). *$\mathscr{H}$ has order 8 if and only if $Y \neq 0$ and*

$$64X^6 - 80DX^4 - 320EX^3 - 20D^2X^2 - 16DEX + D^3 - 32E^2 = 0,$$

where D, E are Eisenstein invariants and X, Y are Frobenius invariants.

Proof. If $Y = 0$, $\mathscr{H}$ will have order 4 by Theorem 26. Hence, in order that $\mathscr{H}$ has order 8, Y must be nonzero. Then, dividing by Y on the both sides of the equation $\Psi_4(X,Y) = 0$, we have

$$\mathscr{H} \text{ has order } 8 \iff 64X^6 - 80DX^4 - 320EX^3 - 20D^2X^2 - 16DEX + D^3 - 32E^2 = 0. \qquad \square$$

Remark. The following explicit result for $\mathscr{H}$ to have order 8 is given in [5]: $\mathscr{H}$ has order 8 if and only if

$$\begin{vmatrix} A & B & C \\ D & E & F \\ G & H & I \end{vmatrix} = 0,$$

where $A = 2\Delta_{22}\Delta_{32} - (\Delta_{21}\Delta_{33} + \Delta_{31}\Delta_{23})$, $B = 2(\Delta_{22}^2 - \Delta_{12}\Delta_{31} + \Delta_{21}\Delta_{23}) + \Delta_{11}\Delta_{33} + \Delta_{31}\Delta_{13}$, $C = 2\Delta_{12}\Delta 22 - (\Delta_{11}\Delta_{23} + \Delta_{21})$, $D = \Delta_{32}^2 - \Delta_{31}\Delta_{33}$, $E = -2\Delta_{32}\Delta 22 + \Delta_{31}\Delta_{23} + \Delta_{21}\Delta_{33}$, $F = \Delta_{22}^2 - \Delta_{21}\Delta_{23}$, $G = \Delta_{22}^2 - \Delta_{21}\Delta_{23}$, $H = -2\Delta_{22}\Delta 12 + \Delta_{11}\Delta_{23} + \Delta_{13}\Delta_{21}$, and $I = \Delta_{12}^2 - \Delta_{11}\Delta_{13}$, and Δ_{ij}'s are cofactors of the matrix $\mathbb{P}$.

The result of Corollary 32 is equivalent to the Equation (4.1.38) in the proof of Lemma 4.1.10 with $m = 2$ in [6]. However, there are no explicit formulas for Y, g_2 and g_3 in their equation.

8. Conclusion

We found that the finite group $\mathscr{H}$ can have order at most 24 for rational weighted walks. Geometric proofs of the criterion for $\mathscr{H}$ to have order 4 and 6 are given. In particular for the case of order 6, the result is simpler than Proposition 4.1.8 of [6]. Using division polynomial, a recursive criterion for $\mathscr{H}$ to have order $4m$ or $4m+2$ is also obtained and an explicit criterion for $\mathscr{H}$ to have order 8 is given almost with no computations.

By far, the largest order that has been known is 10 [12]. Since 24 is a theoretical upper bound, further work on finding possible realizations of higher orders is needed.

Acknowledgement

We thank an anonymous reviewer for providing insightful suggestions.

References

[1] G. Billing, K. Mahler, "On exceptional points on cubic curves", *J. Lond. Math. Soc.* **s1-15** (1940), no. 1, p. 32-43.
[2] M. Bousquet-Mélou, M. Mishna, "Walks with small steps in the quarter plane", in *Algorithmic probability and combinatorics*, Contemporary Mathematics, vol. 520, American Mathematical Society, 2010, p. 1-40.
[3] T. Dreyfus, K. Raschel, "Differential transcendence & algebraicity criteria for the series counting weighted quadrant walks", *Publ. Math. Besançon, Algèbre Théorie Nombres* **1** (2019), p. 41-80.
[4] J. J. Duistermaat, *Discrete integrable systems. QRT maps and elliptic surfaces*, Springer Monographs in Mathematics, Springer, 2010.
[5] G. Fayolle, R. Iasnogorodski, "Random walks in the quarter-plane: Advances in explicit criterions for the finiteness of the associated group in the genus 1 case", *Markov Process. Relat. Fields* **21** (2015), no. 4, p. 1005-1032.
[6] G. Fayolle, R. Iasnogorodski, V. Malyshev, *Random walks in the quarter plane*, 2nd ed., Probability Theory and Stochastic Modelling, vol. 40, Springer, 2017.
[7] G. Fayolle, K. Raschel, "On the holonomy or algebraicity of generating functions counting lattice walks in the quarter-plane", *Markov Process. Relat. Fields* **16** (2010), no. 3, p. 485-496.
[8] ———, "Random walks in the quarter-plane with zero drift: an explicit criterion for the finiteness of the associated group", *Markov Process. Relat. Fields* **17** (2011), no. 4, p. 619-636.
[9] L. Flatto, "Two parallel queues created by arrivals with two demands. II", *SIAM J. Appl. Math.* **45** (1985), no. 5, p. 861-878.
[10] L. Flatto, S. Hahn, "Two parallel queues created by arrivals with two demands. I", *SIAM J. Appl. Math.* **44** (1984), no. 5, p. 1041-1053.
[11] H. Hopf, "Vektorfelder in n-dimensionalen Mannifaltigkeiten", *Math. Ann.* **96** (1927), no. 1, p. 225-249.
[12] M. Kauers, R. Yatchak, "Walks in the quarter plane with multiple steps", in *Proceedings of FPSAC*, Discrete Mathematics & Theoretical Computer Science, The Association DMTCS, 2015, p. 25-36.
[13] I. Kurkova, K. Raschel, "Explicit expression for the generating function counting Gessel's walks", *Adv. Appl. Math.* **47** (2011), no. 3, p. 414-433.
[14] V. Malyshev, "Positive random walks and Galois theory", *Usp. Mat. Nauk* **1** (1971), p. 227-228.
[15] B. Mazur, "Modular curves and the Eisenstein ideal", *Publ. Math., Inst. Hautes Étud. Sci.* **47** (1977), p. 33-186.
[16] ———, "Rational isogenies of prime degree", *Invent. Math.* **44** (1978), p. 129.
[17] B. Mazur, J. T. Tate, "Points of order 13 on elliptic curves", *Invent. Math.* **22** (1973), no. 1, p. 41-49.
[18] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, 2009.
[19] J. H. Silverman, J. T. Tate, *Rational points on elliptic curves*, 2nd ed., Undergraduate Texts in Mathematics, Springer, 2015.