Math. Z. (2015) 279:1007–1028
DOI 10.1007/s00209-014-1400-9

Mathematische Zeitschrift

Elliptic points of the Drinfeld modular groups

A. W. Mason · Andreas Schweizer

Received: 10 January 2014 / Accepted: 5 September 2014 / Published online: 30 October 2014

Abstract Let K be an algebraic function field with constant field $\mathbb{F}_q$. Fix a place ∞ of K of degree δ and let A be the ring of elements of K that are integral outside ∞. We give an explicit description of the elliptic points for the action of the Drinfeld modular group $G = GL_2(A)$ on the Drinfeld's upper half-plane Ω and on the Drinfeld modular curve $G\backslash\Omega$. It is known that under the *building map* elliptic points are mapped onto vertices of the *Bruhat–Tits tree* of G. We show how such vertices can be determined by a simple condition on their stabilizers. Finally for the special case $\delta = 1$ we obtain from this a surprising free product decomposition for $PGL_2(A)$.

Keywords Drinfeld modular group · Drinfeld modular curve · Elliptic point · Bruhat–Tits tree · Vertex stabilizer · Free product

Mathematics Subject Classification 11F06 · 11G09 · 20E06 · 20E08 · 20G30

List of symbols

$\mathbb{F}_q$	The finite field of order q
K	An algebraic function field of one variable with constant field $\mathbb{F}_q$
$g(K)$	The genus of K
$L_K(u)$	The L-polynomial of K
∞	A chosen place of K
δ	The degree of the place ∞
A	The ring of all elements of K that are integral outside ∞

A. W. Mason
Department of Mathematics, University of Glasgow, Glasgow G12 8QW, Scotland, UK
e-mail: awm@maths.gla.ac.uk

A. Schweizer (✉)
Department of Mathematics, Korea Advanced Institute of Science
and Technology (KAIST), Daejeon 305-701, South Korea
e-mail: schweizer@kaist.ac.kr

$\widetilde{K}$	The quadratic constant field extension $\mathbb{F}_{q^2}K$ of K
$\widetilde{A}$	$\mathbb{F}_{q^2}A$, the integral closure A in $\widetilde{K}$
ν	The additive, discrete valuation of K defined by ∞
π	A local parameter at ∞ in K
K_∞	$\cong \mathbb{F}_{q^\delta}((\pi))$, the completion of K with respect to ∞
$\mathcal{O}_\infty$	$\cong \mathbb{F}_{q^\delta}[[\pi]]$, the valuation ring of K_∞
C_∞	The completion of an algebraic closure of K_∞
Ω	$= C_\infty - K_\infty$, Drinfeld's upper half-plane
$\mathcal{T}$	The Bruhat–Tits tree of $GL_2(K_\infty)$
G	The group $GL_2(A)$
G_w	The stabilizer in G of $w \in \text{vert}(\mathcal{T}) \cup \text{edge}(\mathcal{T})$
G_ω	The stabilizer in G of $\omega \in \Omega$
Z	The centre of G
$\text{Cl}(R)$	The ideal class group of the Dedekind ring R
$\text{Cl}^0(F)$	The divisor class group of degree 0 of the function field F
$E(G)$	The elliptic elements of G on Ω
$\text{Ell}(G)$	The elliptic points of G on $G\backslash\Omega$

1 Introduction

Let K be an algebraic function field of one variable with constant field $\mathbb{F}_q$, the finite field of order q, and let ∞ be a fixed place of K of degree δ. Let K_∞ be the completion of K with respect to ∞ and let C_∞ be the ∞-completion of an algebraic closure of K_∞. The set $\Omega = C_\infty \backslash K_\infty$ is often referred to as *Drinfeld's upper half-plane*. We denote the ring of all those elements of K which are integral outside ∞ by A. (The simplest examples are $K = \mathbb{F}_q(t)$ and $A = \mathbb{F}_q[t]$.) The group $G = GL_2(A)$ plays a fundamental role [3] in the theory of *Drinfeld modular curves*. For this reason we will call G a *Drinfeld modular group*. Drinfeld [3] has extended the classical theory of modular curves to the function field setting. Here $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are replaced by K, K_∞, C_∞, respectively. The roles of the *classical upper half-plane*, $\mathbb{H}$, (in $\mathbb{C}$) and the *classical modular group*, $SL_2(\mathbb{Z})$, are assumed by Ω and G, respectively. The group G acts as a set of linear fractional transformations on Ω.

Let S be a subgroup of G. We say that elements $\omega_1,\ \omega_2 \in \Omega$ are *S-equivalent* if and only if $\omega_1 = s(\omega_2)$, for some $s \in S$. For each subgroup S of G and $\omega \in \Omega$, let S_ω denote the *stabilizer* of ω in S.

Definition The element $\omega \in \Omega$ is called an *elliptic* element of S if S_ω is non-trivial, i.e. it does *not* consist entirely of scalar matrices. It is clear that S acts on its set of elliptic elements, $E(S)$. We put $\text{Ell}(S) = S\backslash E(S)$ and refer to its elements as the *elliptic points* of S.

Elliptic points are very important for a number of reasons. One of the purposes of Drinfeld's theory is to provide an analytical description for the so-called *Drinfeld modular curve*, $G\backslash\Omega$ and hence $S\backslash\Omega$, for every finite index subgroup S. Of particular importance in this regard is, for example, the *genus* of such a curve whose evaluation usually depends on the *Hurwitz formula* [4, p. 87]. This relates the genera of $G\backslash\Omega$ and $S\backslash\Omega$ and contains terms coming from the ramification. But ramification in the covering $S\backslash\Omega \to G\backslash\Omega$ can only occur above elliptic points and cusps.

For $SL_2(\mathbb{Z})$, it is a classical result that every element of $\mathbb{H} = \{z \in \mathbb{C} : \text{Im}z > 0\}$ which is fixed by a non-scalar matrix is $SL_2(\mathbb{Z})$-equivalent to one of $i, \rho \in \mathbb{H}$, where $i^2 = -1$ and

$\rho^2+\rho+1=0$. Moreover every element of finite order in $SL_2(\mathbb{Z})$ lies in the stabilizer of one of these "elliptic" elements. It follows then that $SL_2(\mathbb{Z})$ has precisely two "elliptic points". As we shall see the situation for Drinfeld modular groups is much more complicated.

Our first principal result provides a precise description of an elliptic element.

Theorem A *Fix any $\varepsilon \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$. An element $\omega \in \Omega$ is an elliptic element of G if and only if*

$$\omega = \frac{\varepsilon + s}{t}$$

for some $s, t \in A$ $(t \neq 0)$, for which

$$(\varepsilon^q + s)(\varepsilon + s) = tt', \text{ with } t' \in A.$$

It follows that G has elliptic elements if and only if δ is odd. Every elliptic element $\omega \in \Omega$ lies in $\mathbb{F}_{q^2}K\backslash K$. We deduce from Theorem A that the stabilizer G_ω of every elliptic $\omega \in \Omega$ is isomorphic to $\mathbb{F}_{q^2}^*$. We are also able to deduce that $|\operatorname{Ell}(G)| = L_K(-1)$, where $L_K(u)$ is the *L-polynomial* of K [15, Section 5.1]. These deductions are already known [4, p. 50]. However our approach is more elementary than that of Gekeler. Moreover, we derive more precise information and interesting applications.

The Galois automorphism of $\mathbb{F}_{q^2}/\mathbb{F}_q$ extends to that of $\mathbb{F}_{q^2}K/K$ and gives rise to a *conjugate map*, $\omega \mapsto \overline{\omega}$, on $E(G)$. Many of our results depend on whether or not ω and $\overline{\omega}$ are G-conjugate. Of particular interest in this context is the subset of $\operatorname{Ell}(G)$ consisting of all those points corresponding to elliptic elements ω for which ω and $\overline{\omega}$ are G-equivalent. We are able to identify this subset with a certain group of involutions (see Theorem 3.8) and for this reason we denote it by $\operatorname{Ell}(G)_2$. It turns out, rather surprisingly perhaps, that $|\operatorname{Ell}(G)_2|$, as with $|\operatorname{Ell}(G)|$, does not depend on A, i.e. is independent of the particular choice of ∞. For $q \geq 8$ we can bound the size of $\operatorname{Ell}(G)_2$ from below, using arguments from algebraic number theory.

Associated with the group $GL_2(K_\infty)$ is its *Bruhat–Tits building* which in this case is a *tree*, $\mathcal{T}$. See [14, Chapter II, Section 1]. From this G inherits an action on $\mathcal{T}$. Most of our results involve the well-known *building map*

$$\lambda : \Omega \longrightarrow \mathcal{T}.$$

See [4, p. 41], [5, p. 37]. Our next principal result elaborates on the way elliptic elements are mapped into $\mathcal{T}$ under the building map. It is known that, if $\omega \in E(G)$, then $\lambda(\omega) = v$, for some $v \in \operatorname{vert}(\mathcal{T})$, and that $G_\omega \leq G_v$. As usual G_v denotes the stabilizer of the vertex v of $\mathcal{T}$ in G. It is known [14, Proposition 2, p. 76] that G_v is always *finite*. We prove the following.

Theorem B *Suppose that δ is odd.*

(a) Let $v \in \operatorname{vert}(\mathcal{T})$. Then

$$v = \lambda(\omega), \text{ for some } \omega \in E(G), \text{ if and only if } q^2-1 \text{ divides } |G_v|.$$

(b) Suppose that $\omega \in E(G)$ and $\lambda(\omega) = v$.

(i) If ω, $\overline{\omega}$ are G-equivalent, then

$$G_v \cong GL_2(\mathbb{F}_q).$$

(ii) Otherwise,

$$G_v = G_\omega \cong \mathbb{F}_{q^2}^*.$$

Let $\widetilde{v}$ denote the image in $\operatorname{vert}(G\backslash\mathcal{T})$ of a vertex v of $\mathcal{T}$. We put $\widetilde{K} = \mathbb{F}_{q^2}K$.

Theorem C *If δ is odd, there exist bijections between the following sets*

(i) vertices $\tilde{v}$ of $G\backslash\mathcal{T}$ such that $q^2 - 1$ divides $|G_v|$;
(ii) conjugacy classes (in G) of cyclic subgroups of G of order $q^2 - 1$;
(iii) the orbits of the $Gal(\widetilde{K}/K)$-action on $\mathrm{Ell}(G)$.

In particular, among the uncountably many points of $G\backslash\Omega$ lying over any given vertex $\tilde{v}$ of $G\backslash\mathcal{T}$ there are exactly

- *one elliptic point if $G_v \cong GL_2(\mathbb{F}_q)$;*
- *two ($Gal(\widetilde{K}/K)$-conjugate) elliptic points if $G_v \cong \mathbb{F}_{q^2}^*$;*
- *no elliptic points in all other cases.*

Finally we focus our attention on the important special case where $\delta = 1$. It can be shown that a vertex v of $\mathcal{T}$ gives rise to an *isolated* vertex of $G\backslash\mathcal{T}$ when (and *only* when) $\delta = 1$ and $v = \lambda(\omega)$ as in Theorem B. Isolated vertices are important for the following reason. If such a vertex and its incident edge arise from a vertex v and incident edge e of $\mathcal{T}$, then, from Bass–Serre theory [14, Theorem 13, p. 55],

$$G \cong H \underset{L}{*} K,$$

where $H = G_v$ and $L = G_e$, the stabilizer of e. Combining this with the previously discussed results, we can prove our final principal result.

Theorem D *Suppose that $\delta = 1$. Then there exists a subgroup P such that*

$$PGL_2(A) \cong \left(\mathop{*}_{i=1}^{r} \mathbb{Z}/(q+1)\mathbb{Z} \right) * P$$

where

$$r = \frac{1}{2}(|\,\mathrm{Ell}(G)| - |\,\mathrm{Ell}(G)_2|).$$

Moreover, if $q \geq 8$ is fixed, then r grows exponentially with the genus of K.

This decomposition has a number of interesting consequences.

We recall that A is an arithmetic Dedekind domain with $A^* = \mathbb{F}_q^*$. In addition $\nu(a) \leq 0$, for all $a \in A$. Moreover $\nu(a) = 0$ if and only if $a \in \mathbb{F}_q^*$. By definition Z consists of all the scalar matrices αI_2, where $\alpha \in \mathbb{F}_q^*$. As usual, the *degree* of a prime ideal of A or of a prime divisor of K is the degree of its residue field over the constant field. By linear extension one obtains the degree of any ideal or divisor.

It is well known that if δ is odd, the place ∞ of K has exactly one extension to $\widetilde{K}$, denoted by ∞'. In this case, $\widetilde{A}$ is the ring of all those elements of $\widetilde{K}$ which are integral outside ∞'. We note that, if $\varepsilon \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$, then $\widetilde{A} = A + \varepsilon A$. The action of $Gal(\widetilde{K}/K)$ on $\widetilde{K}$ is given by

$$\overline{a + \varepsilon b} = a + \varepsilon^q b,$$

where $a, b \in K$. Also, for any set J in $\widetilde{K}$, for example if J is an ideal of $\widetilde{A}$, we write $\overline{J}$ for the conjugate set $\{\overline{x} \ : \ x \in J\}$.

2 Elliptic elements on the Drinfeld upper halfplane Ω

Before our first principal result we record some elementary properties of non-trivial elements of elliptic point stabilizers.

Lemma 2.1 *Let $\omega \in \Omega$ be an elliptic element and let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be a non-scalar element of G_ω. Then the minimal polynomial of ω over K is*

$$m_\omega(x) = x^2 + \sigma x + \tau,$$

where $\sigma = (d-a)/c$ and $\tau = -b/c$.

Proof Follows from the fact that $M(\omega) = \omega$. Note that $bc \neq 0$, since $\omega \notin K$. □

Before proceeding the following observation is critical.

The matrix $M \in G$ fixes $\omega \in \Omega$ if and only if $\begin{bmatrix} \omega \\ 1 \end{bmatrix}$ is an eigenvector of M.

Lemma 2.2 *Let $\omega \in \Omega$ be an elliptic point and let $M \in G_\omega$ be non-scalar. Then $\omega \in \widetilde{K}$, and $\begin{bmatrix} \omega \\ 1 \end{bmatrix}$ is an eigenvector of M with eigenvalue $\varepsilon \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$.*

Proof Let

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

Then $bc \neq 0$ by Lemma 2.1. It follows that $K(\omega)$ is a quadratic extension of K. Now there exists ε such that

$$a\omega + b = \varepsilon\omega \text{ and } c\omega + d = \varepsilon.$$

Obviously $K(\omega) = K(\varepsilon)$. Moreover, ε is an eigenvalue of M and so

$$\varepsilon^2 + \eta\varepsilon + \rho = 0,$$

where $\eta = -(a+d)$ and $\rho = \det(M) = (ad - bc) \in \mathbb{F}_q^*$. Let B denote the integral closure of A in $K(\varepsilon)$. Since $M^{-1} \in G_\omega$ has eigenvalue ε^{-1}, we have $\varepsilon, \varepsilon^{-1} \in B^*$. Now $\varepsilon \notin K_\infty$ (since $\omega \notin K_\infty$), so the place ∞ has only one extension ∞' to $K(\varepsilon)$, and B consists of the elements that are integral outside ∞'. Since ε is invertible at all places outside ∞', by the product formula it must also be invertible at ∞' and hence a constant. So ε is algebraic over $\mathbb{F}_q$ and since it generates a quadratic extension of K we conclude that $\varepsilon \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. Thus

$$K(\omega) = K(\varepsilon) = \widetilde{K}.$$

□

Proposition 2.3 [4, p. 50] *Let ω be any elliptic element of any G. Then*

$$G_\omega \cong \mathbb{F}_{q^2}^*.$$

This isomorphism is given by mapping $M \in G_\omega$ to the eigenvalue of $\begin{bmatrix} \omega \\ 1 \end{bmatrix}$ and it also respects addition of matrices.

Proof By Lemma 2.2 $\begin{bmatrix} \omega \\ 1 \end{bmatrix}$ is an eigenvector for all $M \in G_\omega$ with corresponding eigenvalue $\varepsilon \in \mathbb{F}_{q^2}^*$ depending on M. Applying $\tau \in Gal(\widetilde{K}/K)$, we see that $\begin{bmatrix} \overline{\omega} \\ 1 \end{bmatrix}$ is an eigenvector with eigenvalue ε^q. Hence there exists a matrix $X \in GL_2(\widetilde{K})$, such that, for all $M \in G_\omega$,

$$XMX^{-1} = \mathrm{diag}(\varepsilon, \varepsilon^q).$$

There is therefore a monomorphism

$$G_\omega \hookrightarrow \mathbb{F}_{q^2}^*.$$

To show that this map is surjective, we observe that by definition G_ω contains a nonscalar N with eigenvalues $\mu, \mu^q \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ and that for all $\alpha, \beta \in \mathbb{F}_q$, with $(\alpha, \beta) \neq (0, 0)$,

$$Y = \alpha I_2 + \beta N \in G_\omega,$$

and

$$XYX^{-1} = \mathrm{diag}(\alpha + \beta\mu, \alpha + \beta\mu^q).$$

The result follows. □

For an alternative proof of Proposition 2.3 see [4, p. 50].

Corollary 2.4 [4, p. 50] *G has elliptic elements if and only if δ is odd.*

Proof If ω is an elliptic element then, by definition, $\omega \notin K_\infty$. By the proof of Lemma 2.2 there exists $\varepsilon \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ such that $\varepsilon \notin K_\infty$. In addition,

$$\mathbb{F}_{q^2} \subseteq K_\infty \iff \delta \quad \text{is even.}$$

On the other hand, if δ is odd, every $\varepsilon \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ is fixed by

$$M = \begin{bmatrix} \varepsilon^q + \varepsilon & -\varepsilon^{q+1} \\ 1 & 0 \end{bmatrix},$$

and hence elliptic. □

Actually, one can give a precise description of the elliptic elements of G.

Theorem 2.5 *Let δ be odd. Fix any $\varepsilon \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. Then ω is an elliptic element of G if and only if*

$$\omega = \frac{\varepsilon + s}{t}$$

for some $s, t \in A$ $(t \neq 0)$, for which

$$(\varepsilon^q + s)(\varepsilon + s) = tt', \text{ with } t' \in A.$$

Proof Suppose $\omega = \frac{\varepsilon + s}{t}$ as above. Let

$$M_0 = \begin{bmatrix} s' & -t' \\ t & -s \end{bmatrix},$$

where $s' = (\varepsilon + \varepsilon^q) + s$. Then it is easily verified that (non-scalar) $M_0 \in G_\omega$. Moreover M_0 has eigenvalues ε and ε^q and determinant $\varepsilon^{q+1} \in \mathbb{F}_q^*$.

Conversely, let $\omega \in \Omega$ be elliptic. By Proposition 2.3 we can choose $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in G_ω such that $\varepsilon(M) = \varepsilon$. Then from the proof of Lemma 2.2

$$\omega = (\varepsilon - d)/c.$$

Now $M(\omega) = \omega$ and so

$$c\omega^2 + (d - a)\omega - b = 0.$$

Let ω' be the other root of this quadratic equation. Then $\omega' = \frac{\varepsilon^q + s}{t}$ and

$$\omega\omega' = -b/c = (\varepsilon^q - d)(\varepsilon - d)/c^2.$$

Thus the condition is satisfied with $s = -d$ and $t = c$. □

If $\omega = \frac{\varepsilon+s}{t}$ is elliptic and $M \in G_\omega$, then from $M\omega = \omega$ one immediately obtains $M\overline{\omega} = \overline{\omega}$. So the conjugate $\overline{\omega} = \frac{\varepsilon^q+s}{t}$ is also elliptic with the same stabilizer, i.e.

$$G_{\overline{\omega}} = G_\omega.$$

A finer analysis of this in the next three sections will lead to some interesting group-theoretic consequences. Among many others we will need the following easy intermediate result.

Lemma 2.6 *If δ is odd, mapping $\{\omega, \overline{\omega}\}$ to $G_\omega = G_{\overline{\omega}}$ is a natural bijection between the unordered pairs $\{\omega, \overline{\omega}\}$ of conjugate elliptic points and cyclic subgroups of G of order $q^2 - 1$.*

Proof The inverse map is given by mapping the cyclic subgroup to its two fixed points $\{\omega, \overline{\omega}\}$. These are indeed elliptic. If not, they would lie in K_∞, and consequently the eigenvalue of the eigenvector $\begin{bmatrix} \omega \\ 1 \end{bmatrix}$ would be in $K_\infty \cap \mathbb{F}_{q^2}^* = \mathbb{F}_q^*$, in contradiction to the order of the subgroup. □

Lemma 2.6 also shows that if δ is odd, then the intersection of any two cyclic subgroups of G of order $q^2 - 1$ is exactly Z.

We conclude this section with a further restriction on the factor t in Theorem 2.5 which we make use of later on.

Lemma 2.7 *Let $\omega = \frac{\varepsilon+s}{t} \in \Omega$ be an elliptic element as in Theorem 2.5. Then*

(a) $\deg(\mathfrak{p})$ *is even for every prime ideal* $\mathfrak{p}$ *of* A *that divides* tA.
(b) $\nu(t)$ *is even.*

Proof (a) Let $\mathfrak{p}$ be a prime ideal of A of odd degree. Then $\mathfrak{p}$ is inert in $\widetilde{A}$. Let $\widetilde{\mathfrak{p}}$ be the prime ideal in $\widetilde{A}$ above $\mathfrak{p}$. If $\mathfrak{p}$ divides (t) in A, then $\widetilde{\mathfrak{p}}$ divides $(\varepsilon + s)(\varepsilon^q + s)$ in $\widetilde{A}$. Since $\widetilde{\mathfrak{p}}$ is a prime ideal, it must divide one of the two factors. Applying the Frobenius automorphism of $\widetilde{K}/K$, it also divides the other factor. Hence $\widetilde{\mathfrak{p}}$ divides $(\varepsilon - \varepsilon^q) = \widetilde{A}$, a contradiction.
(b) By (a) and the product formula $\delta\nu(t)$ is even, and δ is odd by Corollary 2.4. □

3 Elliptic points on the Drinfeld modular curve $G\backslash\Omega$

In view of Corollary 2.4 we assume throughout this section that δ is odd.

Central to the definition of $G\backslash\Omega$ is the following equivalence relation.

Definition Let $\omega_1, \omega_2 \in \Omega$. We say that ω_1, ω_2 are *G-equivalent*, written $\omega_1 \equiv \omega_2$, if and only if there exists $g \in G$ such that

$$\omega_1 = g(\omega_2).$$

If $\omega_1 = g(\omega_2)$ then

$$gG_{\omega_2}g^{-1} = G_{\omega_1}.$$

It follows that G-equivalent points of Ω have isomorphic stabilizers in G. As we shall see the converse does not hold.

It is clear that G acts on its elliptic points, $E(G)$. We denote the set of equivalence classes by $\mathrm{Ell}(G)$. The elements of this set are referred to as the *elliptic points* of G.

In particular if δ is odd, then from Theorem 2.5 every $\varepsilon \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ is an elliptic point of G. Moreover, if ε and ε' are any two elements of $\mathbb{F}_{q^2}\backslash\mathbb{F}_q$, then $\varepsilon' = \alpha\varepsilon + \beta$ for some $\alpha \in \mathbb{F}_q^*,\ \beta \in \mathbb{F}_q$ and hence

$$\varepsilon \equiv \varepsilon'.$$

In particular, $\varepsilon \equiv \overline{\varepsilon}$. However, this does not always hold for general elliptic points. For an arbitrary elliptic point ω we will investigate later the precise conditions under which ω and $\overline{\omega}$ are G-equivalent. (They are not always equivalent despite the fact that $G_\omega = G_{\overline{\omega}}$.)

Lemma 3.1 *Let*

$$\omega = \frac{\varepsilon + s}{t}$$

be an elliptic element, where ε, s, t are as defined in Theorem 2.5. *Then*

(a) $J_\omega := tA + (\varepsilon + s)A \trianglelefteq \widetilde{A}.$
(b) The ideal J_ω does not depend on the choice of $\varepsilon \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$.

Proof (a) It suffices to prove that $\varepsilon J_\omega \subseteq J_\omega$. Now

$$\varepsilon t = t(\varepsilon + s) - st \in J_\omega.$$

On the other hand,

$$\varepsilon(\varepsilon + s) = (\varepsilon + \varepsilon^q)(\varepsilon + s) - (\varepsilon^q + s)(\varepsilon + s) + s(\varepsilon + s) \in J_\omega,$$

by the properties of ε, s, t.

(b) Choosing a different $\varepsilon' \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$, there exist $\alpha \in \mathbb{F}_q^*$ and $\beta \in \mathbb{F}_q$ with $\varepsilon' = \alpha\varepsilon + \beta$. So $\omega = \frac{\varepsilon' - \beta + \alpha s}{\alpha t}$, which gives the same ideal. □

Let A_0 denote A or $\widetilde{A}$. If I, I' are ideals in A_0, we write

$$I \sim_{A_0} I' \Longleftrightarrow aI = bI',$$

for some non-zero $a, b \in A_0$.

Our next result is crucial since it enables us to identify $\mathrm{Ell}(G)$ with a subgroup of $\mathrm{Cl}(\widetilde{A})$.

Lemma 3.2 *Let ω and ω' be elliptic elements of G. Then*

$$\omega \equiv \omega' \iff J_\omega \sim_{\widetilde{A}} J_{\omega'}.$$

Proof Let $\omega = \frac{\varepsilon+s}{t}$ and $\omega' = \frac{\varepsilon+s'}{t'}$. Then

$$tA + (\varepsilon + s)A \sim_{\widetilde{A}} t'A + (\varepsilon + s')A$$

if and only if there exist $a, b, c, d \in A$ with $ad - bc \in \mathbb{F}_q^*$ and a non-zero $\rho \in \widetilde{K}$ such that

$$\rho t' = (at + b(\varepsilon + s)) \ \text{ and } \ \rho(\varepsilon + s') = (ct + d(\varepsilon + s)).$$

□

Mapping an elliptic element ω to the ideal class $[J_\omega] \in \mathrm{Cl}(\widetilde{A})$ induces by Lemma 3.2 an injective map from $\mathrm{Ell}(G)$ into $\mathrm{Cl}(\widetilde{A})$. In order to describe its image, we need the norm map N from ideals of $\widetilde{A}$ to ideals of A, and also from divisors of $\widetilde{K}$ to divisors of K.

If $\widetilde{P}$ is a prime ideal of $\widetilde{A}$, then $N(\widetilde{P}) = P^{f(\widetilde{P}/P)}$ where $P = \widetilde{P} \cap A$ is the underlying prime ideal of A and $f(\widetilde{P}/P)$ is the inertia degree. This definition is then canonically extended to products. (See [17, Ch. V, §11, p. 306].) Analogously for divisors (cf. [12, p. 82]).

In our simple situation we can equivalently say: If $J \trianglelefteq \widetilde{A}$, then $N(J)$ is the A-ideal $J\overline{J} \cap A$.

Actually, $N(J)$ is also the A-ideal generated by all norms of elements in J [17, Ch. V, §11, Lemma 3, p. 307], but this is not completely obvious. And in practice it is more awkward to handle than the other properties.

The norm map N induces group homomorphisms

$$\overline{N} : \mathrm{Cl}(\widetilde{A}) \longrightarrow \mathrm{Cl}(A)$$

and

$$\overline{N} : \mathrm{Cl}^0(\widetilde{K}) \longrightarrow \mathrm{Cl}^0(K).$$

Since δ is odd, both norm maps are surjective. As ∞ is inert in $\widetilde{K}$ by [12, Proposition 8.13], we can apply [11, Proposition 2.2] which tells us that $\overline{N}$ is surjective onto $\mathrm{Cl}(A)$. The surjectivity onto $\mathrm{Cl}^0(K)$ is known from the theory of Jacobian varieties. Alternatively, by [11, Lemma 1.2] we have

$$|\mathrm{Cl}(\widetilde{A})| = \delta|\mathrm{Cl}^0(\widetilde{K})| \text{ and } |\mathrm{Cl}(A)| = \delta|\mathrm{Cl}^0(K)|.$$

So one surjectivity implies the other one.

Our next goal is to show that the kernel of $\overline{N}$ is the image of $\mathrm{Ell}(G)$. The following description of an element of $\mathrm{Cl}(\widetilde{A})$ is essential for our purposes.

Lemma 3.3 *Let $J \trianglelefteq \widetilde{A}$. Then, for any fixed $\varepsilon \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$, there exist $a \in A$ and an ideal $I \trianglelefteq A$ such that*

$$J \sim_{\widetilde{A}} J' = I + (\varepsilon + a)A.$$

Moreover $J' \cap A = I$ and $N(J') = I$.

Proof Now $\widetilde{A} = A + \varepsilon A$ and so, by [2, Chapter VII, Section 4.10, Proposition 24], there exists $a, b \in A$ and an A-module I', A-isomorphic to an A-ideal such that

$$J = I' + (a + \varepsilon b)A.$$

Since A is Dedekind there are two possibilities.

(a) $I' = xA$, *for some nonzero* $x \in \widetilde{A}$:
Then

$$J \sim_{\widetilde{A}} \overline{x}J.$$

By multiplying by another term in A (to "clear denominators") we may assume that $x \in A$.

(b) $I' = Ax + Ay$, *with* $ey = fx \neq 0$, *where* $x, y \in \widetilde{A}$ *and* $e, f \in A$:

Replacing J with $fy^{-1}J$ and then "clearing denominators" as above we may assume that $x, y \in A$.

From now on we replace I' with I, where $I \trianglelefteq A$. Let $i \in I$. Then $i\varepsilon \in J$ and so $i = bb'$, where $b' \in A$. On the other hand $\varepsilon(a + \varepsilon b) \in J$, and since $\varepsilon^2 = \alpha\varepsilon + \beta$ with $\alpha, \beta \in \mathbb{F}_q$, this implies $a = bb''$, where $b'' \in A$. We now replace J with $J' = b^{-1}J$, which has the desired form.

Moreover, $J' \cap A = I$ is obvious. Finally,

$$J'\overline{J'} = I^2 + I(\varepsilon - a) + I(\varepsilon^q - a) + (\varepsilon - a)(\varepsilon^q - a)A \subseteq I^2 + I\widetilde{A} + (J' \cap A) \subseteq I\widetilde{A}.$$

Conversely, $J'\overline{J'}$ contains $I(\varepsilon - a) - I(\varepsilon^q - a)$, and hence $I(\varepsilon - \varepsilon^q) = I\widetilde{A}$. So together $J'\overline{J'} = I\widetilde{A}$ and thus $N(J') = I$. □

Theorem 3.4 *Mapping an elliptic element* ω *to the ideal class* $[J_\omega]$ *in* $\mathrm{Cl}(\widetilde{A})$ *induces a bijection between* $\mathrm{Ell}(G)$ *and the kernel of the surjective norm map* $\overline{N} : \mathrm{Cl}(\widetilde{A}) \longrightarrow \mathrm{Cl}(A)$.

Proof If $\omega = \frac{\varepsilon+s}{t}$ is elliptic, then the ideal $J_\omega = tA + (\varepsilon + s)A$ from Lemma 3.1 has norm tA by Lemma 3.3. So $[J_\omega]$ lies in the kernel of $\overline{N}$.

Conversely, we represent each element $[J]$ of $\mathrm{Cl}(\widetilde{A})$ by an ideal J of the form given by Lemma 3.3. Then $[J] \in \mathrm{Ker}\ \overline{N}$ if and only if $N(J) = I$ is principal, i.e. if and only if

$$J = Ac + A(a + \varepsilon),$$

for some non-zero $a, c \in A$.

Note that, if J is of this form, then $(a + \varepsilon)(a + \varepsilon^q) = cc'$, for some $c' \in A$, since $J \cap A = I$. Suppose that $Ac + Aa \neq A$. Then there exists a prime $\widetilde{A}$-ideal, $\mathfrak{p}$, containing a, c. Thus $(a + \varepsilon)(a + \varepsilon^q) \in \mathfrak{p}$ and so $\varepsilon \in \mathfrak{p}$, which implies that $\mathfrak{p} = \widetilde{A}$. Hence $Ac + Aa = A$ and so J is determined by the elliptic point $\omega = (a + \varepsilon)/c$. (See Theorem 2.5.) □

So far, $|\,\mathrm{Ell}(G)|$ seems to depend on the ring A, of which there are infinitely many non-isomorphic ones in the same function field K. But one can go one step further.

Lemma 3.5 *The canonical map from* $\mathrm{Cl}^0(\widetilde{K})$ *to* $\mathrm{Cl}(\widetilde{A})$ *restricts to an isomorphism of abelian groups between the kernel of* $\overline{N} : \mathrm{Cl}^0(\widetilde{K}) \longrightarrow \mathrm{Cl}^0(K)$ *and the kernel of* $\overline{N} : \mathrm{Cl}(\widetilde{A}) \longrightarrow \mathrm{Cl}(A)$.

Proof Mapping the divisor $\prod P^{e_P}$ of $\widetilde{K}$ to the fractional ideal $\prod_{P \neq \infty} P^{e_P}$ of $\widetilde{A}$ induces an isomorphism from $\mathrm{Cl}^0(\widetilde{K})$ to a subgroup of index δ in $\mathrm{Cl}(\widetilde{A})$, namely to the classes consisting of ideals whose degrees are divisible by δ. (Compare [12, Proposition 14.1].) But the degree of every principal ideal of A obviously is divisible by δ. So if the ideal class $[J]$ is in the kernel of $\overline{N}$, then δ divides $\deg(N(J)) = 2\deg(J)$ and hence $\deg(J)$ since δ is odd. Now one easily verifies that the map induces the desired isomorphism. □

Corollary 3.6 [4, p. 50] *With the above notation,*

$$|\,\mathrm{Ell}(G)| = L_K(-1).$$

Proof Combining Theorem 3.4 and Lemma 3.5 with [15, Theorem V.1.15 (c), (f)], we have

$$|\,\mathrm{Ell}(G)| = \frac{|\mathrm{Cl}^0(\widetilde{K})|}{|\mathrm{Cl}^0(K)|} = \frac{L_{\widetilde{K}}(1)}{L_K(1)} = L_K(-1).$$

□

Corollary 3.6 (as well as Proposition 2.3 and Corollary 2.4) is already known [4, p. 50]. However our approach is more elementary than that of Gekeler. In particular it avoids any mention of the fact that $G\backslash\Omega$ is a component of the moduli scheme for Drinfeld A-modules of rank 2. In addition, at this stage we don't yet need the *building map* $\lambda : \Omega \longrightarrow \mathcal{T}$, where $\mathcal{T}$ is the *Bruhat–Tits tree* associated with G. (See [14, Chapter II, Section 1.1], [4, p. 41].)

The remaining results in this section will elaborate on the structure of $\mathrm{Ell}(G)$.

Lemma 3.7 *(a) For $q \geq 4$ there exists only one non-rational function field K with $|\,\mathrm{Ell}(G)| = 1$, namely*

$$K = \mathbb{F}_4(x, y) \ \text{with} \ y^2 + y = x^3.$$

(b) More generally, for any positive integer n there are only finitely many nonrational function fields K with $q \geq 3$ and $|\,\mathrm{Ell}(G)| = n$.

Proof Using Corollary 3.6 and the Riemann Hypothesis for function fields [15, Theorem 5.2.1], [15, Theorem 5.1.15(e)] we have

$$n = |\,\mathrm{Ell}(G)| = L_K(-1) \geq (\sqrt{q} - 1)^{2g}.$$

For given n this bounds q, and for $q > 4$ it also bounds g.

In particular, $n = 1$ is only possible for $q \leq 4$; and if $n = 1$ for $q = 4$, then necessarily $L_K(u) = (1 + 2u)^{2g}$.

A function field K over $\mathbb{F}_q$ with $L_K(u) = (1 + \sqrt{q}u)^{2g}$ is called *maximal*. Equivalently, a maximal function field is a function field with $q + 1 + 2g\sqrt{q}$ places of degree 1.

By Ihara's Theorem [15, Proposition 5.3.3] the genus of a maximal function field is bounded by $g \leq \frac{q-\sqrt{q}}{2}$. For $q = 4$ this leaves only the possibility $g = 1$. But it is well known that $y^2 + y = x^3$ is the only elliptic function field over $\mathbb{F}_4$ with L-polynomial $(1 + 2u)^2$. Alternatively one could invoke [13, Theorem] here. This finishes the proof of (a).

For (b) we still have to take care of the cases $q = 3$ and 4. We exploit the following lower bound for the class number from [15, Exercise 5.8, p. 213]

$$L_K(1) \geq \frac{q-1}{2} \cdot \frac{q^{2g} + 1 - 2gq^g}{g(q^{g+1} - 1)} \geq \frac{q-1}{2} \cdot \frac{q^{2g} - 2gq^g}{gq^{g+1}} = \frac{q-1}{2}\left(\frac{q^{g-1}}{g} - \frac{2}{q}\right).$$

Applied to the field $\widetilde{K}$ this yields

$$L_{\widetilde{K}}(1) \geq \frac{c \cdot q^{2g}}{g}$$

where c is a nonzero constant depending on q. Combined with the upper bound

$$L_K(1) \leq (\sqrt{q} + 1)^{2g}$$

from the Riemann Hypothesis [15, Theorem 5.2.1], [15, Theorem 5.1.15(e)] this shows

$$|\,\mathrm{Ell}(G)| = \frac{L_{\widetilde{K}}(1)}{L_K(1)} \geq \frac{c \cdot q^{2g}}{g(\sqrt{q} + 1)^{2g}}.$$

So $|\,\mathrm{Ell}(G)|$ goes to infinity with g provided $q \geq 3$. □

We apply Lemma 3.2 to the cases for which $L_K(-1) = 1$. (One such is the genus zero case $K = \mathbb{F}_q(T)$.) Let $\varepsilon \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. Then, if ω is any elliptic point, there exists $g \in G$ such that $g(\omega) = \varepsilon$. In particular, then $\omega \equiv \overline{\omega}$ for all elliptic points.

We will determine now when this happens in general. By Lemma 3.3 we have

$$J_\omega J_{\overline{\omega}} = J_\omega \overline{J_\omega} = N(J_\omega)\widetilde{A} = t\widetilde{A}.$$

It follows that in $\mathrm{Cl}(\widetilde{A})$

$$[J_{\overline{\omega}}] = [J_\omega]^{-1}.$$

Hence

$$\omega \equiv \overline{\omega} \Longleftrightarrow [J_\omega]^2 = 1$$

in $\mathrm{Cl}(\widetilde{A})$, or equivalently, in $\mathrm{Cl}^0(\widetilde{K})$.

Definition Let $\mathrm{Ell}(G)_2$ be the subset of $\mathrm{Ell}(G)$ consisting of those orbits of elliptic elements for which $\overline{\omega} \equiv \omega$.

We have just proved the following result.

Theorem 3.8 *The bijection between* $\mathrm{Ell}(G)$ *and the kernel of the norm map* $\overline{N}$ *described in Theorem 3.4 restricts to a bijection between* $\mathrm{Ell}(G)_2$ *and the* 2*-torsion subgroup of the kernel of* $\overline{N}$ *in* $\mathrm{Cl}(\widetilde{A})$*, or by Lemma 3.5 equivalently, the* 2*-torsion subgroup of the kernel of* $\overline{N}$ *in* $\mathrm{Cl}^0(\widetilde{K})$.

In particular, $|\mathrm{Ell}(G)|$ *and* $|\mathrm{Ell}(G)_2|$ *only depend on* K*, not on the choice of the place* ∞ *(apart from the general condition that* δ *has to be odd).*

Hence if $\mathrm{Ell}(G) = \mathrm{Ell}(G)_2$ (for example, when $L_K(-1) = 1$) it follows that $\omega \equiv \overline{\omega}$ for all $\omega \in E(G)$. On the other hand we can prove the following.

Theorem 3.9 *(a) For* $q \geq 8$ *there are only two function fields* K *of genus* $g > 0$ *for which* $\mathrm{Ell}(G) = \mathrm{Ell}(G)_2$*, namely*

$$K = \mathbb{F}_9(x, y) \ \ \textit{with} \ \ y^3 + y = x^4 \ \ (\textit{genus } 3)$$

and

$$K = \mathbb{F}_9(x, y) \ \ \textit{with} \ \ y^2 = x^3 - x \ \ (\textit{genus } 1).$$

(b) For fixed $q \geq 8$ *we have* $\lim\limits_{g\to\infty} \frac{|\mathrm{Ell}(G)_2|}{|\mathrm{Ell}(G)|} = 0.$

Proof (a) By Corollary 3.6 and the Riemann Hypothesis for function fields [15, Theorem 5.2.1], [15, Theorem 5.1.15(e)]

$$|\mathrm{Ell}(G)| = L_K(-1) \geq (\sqrt{q} - 1)^{2g}.$$

On the other hand, the 2-torsion rank of an abelian variety of dimension g is bounded by $2g$, and even by g if the characteristic is 2. Applying this to $\mathrm{Cl}^0(\widetilde{K})$ (compare [12, Chapter 11]) we get

$$|\mathrm{Ell}(G)_2| \leq 2^{2g},$$

and even $|\mathrm{Ell}(G)_2| \leq 2^g$ if the characteristic is 2. This proves both claims if $q > 9$ and also if $q = 8$.

For the remaining case $q = 9$ we note that by the same argument $|\mathrm{Ell}(G)| = |\mathrm{Ell}(G)_2|$ is only possible if $L_K(u) = (1 + 3u)^{2g}$, that is, if K is a maximal function field. Then Ihara's Theorem [15, Proposition 5.3.3] implies $g \leq 3$. Moreover, $g = 2$ is not possible, because then K would be hyperelliptic, i.e. a double covering of a rational function field $\mathbb{F}_9(T)$, and hence could have at most $2(9+1) < 22$ places of degree 1.

By [13, Theorem] there is a unique maximal function field of genus 3 over $\mathbb{F}_9$, namely $\mathbb{F}_9(x, y)$ with $y^3 + y = x^4$. Furthermore, by [13, Lemma 1] this function field has $\mathrm{Cl}^0(K) \cong \bigoplus_{i=1}^{6} \mathbb{Z}/4\mathbb{Z}$. Since $L_{\widetilde{K}}(t) = (1-9t)^6$, by the same argument we have $\mathrm{Cl}^0(\widetilde{K}) \cong \bigoplus_{i=1}^{6} \mathbb{Z}/8\mathbb{Z}$, and hence the kernel of the norm map is indeed isomorphic to $\bigoplus_{i=1}^{6} \mathbb{Z}/2\mathbb{Z}$.

For $g = 1$ we use the well-known fact that $y^2 = x^3 - x$ is the only elliptic function field over $\mathbb{F}_9$ with L-polynomial $(1 + 3u)^2$ or some explicit calculations with Weierstrass equations.

Finally, to prove claim (b) for $q = 9$ we bound $|\,\mathrm{Ell}(G)|$ from below by exactly the same procedure as in the proof of Lemma 3.7. Then $\frac{|\,\mathrm{Ell}(G)_2|}{|\,\mathrm{Ell}(G)|} \leq \frac{g \cdot 8^{2g}}{c \cdot 9^{2g}}$, which goes to 0. □

When $q > 9$ and $g > 0$ therefore G has an elliptic point ω_0 which is *not* equivalent to $\overline{\omega_0}$. As we shall see in the next two sections, points like these have a special significance for the Bruhat–Tits tree and the structure of G.

Remark 3.10 It is not clear whether for $q \leq 7$ there are only finitely many function fields K with $\mathrm{Ell}(G) = \mathrm{Ell}(G)_2$. And even if one could prove finiteness, the actual determination of all such fields would be a tedious task.

Let us consider the special case where K is a quadratic extension of a rational function field $\mathbb{F}_q(T)$, that is, K is hyperelliptic or possibly elliptic. In this case the degree 4 Galois extension $\widetilde{K}/\mathbb{F}_q(T)$ has 3 intermediate extensions, namely K, $\mathbb{F}_{q^2}(T)$, and the unramified quadratic twist of K, which we denote by K'.

Now the kernel of the norm map from $\mathrm{Cl}^0(\widetilde{K})$ to $\mathrm{Cl}^0(K)$ is isomorphic to $\mathrm{Cl}^0(K')$. So the determination of all hyperelliptic K with $\mathrm{Ell}(G) = \mathrm{Ell}(G)_2$ is equivalent to the determination of all hyperelliptic function fields with divisor class group of exponent 2.

For the more special case where in addition a degree 1 place of $\mathbb{F}_q(T)$ is ramified in K' this is the goal of the paper [1]. But even then case-by-case arguments and a computer search were needed.

More importantly, on the way from [1, Theorem 21] to [1, Theorem 37] several cases, including among others for $h = 8$ the cases $q = 5$, $g = 2$ and $q = 3$, $g = 3, 4$ as well as $q = 2$, $4 \leq g \leq 8$ seem to have got lost, and consequently the main result of that paper is incomplete. Without claim for completeness we point out some missing elliptic function fields K' with $\mathrm{Cl}^0(K') \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, to wit

$$\begin{aligned} K' &= \mathbb{F}_3(x, y) \text{ with } y^2 = x^3 - x, \\ K' &= \mathbb{F}_5(x, y) \text{ with } y^2 = x^3 + x, \\ K' &= \mathbb{F}_7(x, y) \text{ with } y^2 = x^3 - 1, \\ K' &= \mathbb{F}_9(x, y) \text{ with } y^2 = x^3 - \sqrt{-1}x. \end{aligned}$$

The last example is the unramified quadratic twist of the exceptional K in Theorem 3.9(a).

4 The images of elliptic points on the Bruhat–Tits tree $\mathcal{T}$

Associated with the group $GL_2(K_\infty)$ is its *Bruhat–Tits building* which in this case is a $(q^\delta + 1)$-regular *tree*, $\mathcal{T}$. The most convenient description for our purposes is the one in [14, Chapter II, Section 1]. See also [5, Section 1.3]. The vertices of $\mathcal{T}$ are the homothety classes of $\mathcal{O}_\infty$-lattices of rank 2 in $K_\infty \oplus K_\infty$. Two such vertices are joined by an edge if they contain lattices L_1 and L_2 such that L_2 is a maximal $\mathcal{O}_\infty$-sublattice of L_1. This definition is of course symmetric, because then πL_1 is a maximal sublattice of L_2.

Via its natural embedding into $GL_2(K_\infty)$, the group G acts on $\mathcal{T}$ *without inversion* [14, Corollary, p. 75]. Classical Bass–Serre theory [14, Theorem 13, p. 55] shows how the structure of G can be derived from that of the quotient graph $G\backslash\mathcal{T}$. The structure of this quotient is described in [14, Theorem 9, p. 106]. (Serre's approach uses the theory of vector bundles. For a more elementary approach see [7, Theorem 4.7].) In the sequel we will write v and e for vertices respectively edges of $\mathcal{T}$ and $\widetilde{v}$ and $\widetilde{e}$ for their images in $G\backslash\mathcal{T}$.

A central object in the study of Drinfeld's half-plane is the *building map*

$$\lambda : \Omega \longrightarrow \mathcal{T}.$$

See [4, p. 41], [5, Section 1.5]. We only mention the facts that we need and refer to the literature for a thorough description.

If $|\cdot|$ denotes the multiplicative valuation on C_∞, then every $\omega \in \Omega$ defines a norm $v_\omega(u, v) := |u\omega + v|$ on the vector space $K_\infty \oplus K_\infty$. By a theorem of Goldman and Iwahori there are two types of such norms. If the unit ball of v_ω is an $\mathcal{O}_\infty$-lattice L in $K_\infty \oplus K_\infty$, then $\lambda(\omega)$ is the vertex of $\mathcal{T}$ given by the homothety class of L. In all other cases v_ω is a "convex combination" of two norms that are of the former type and belong to two neighbouring vertices. Correspondingly λ then maps ω to a point on the edge joining these two vertices.

Another important feature is that λ respects the actions of $GL_2(K_\infty)$ on Ω and $\mathcal{T}$, that is

$$\lambda(g(\omega)) = g(\lambda(\omega)).$$

In particular, λ induces a map from the quotient space $G\backslash\Omega$ to the quotient graph $G\backslash\mathcal{T}$. Important information about $G\backslash\Omega$ is encoded in the (in a certain sense) simpler object $G\backslash\mathcal{T}$ (see for example [5]). Here we explore this theme with respect to elliptic points.

Lemma 4.1 *If $\omega \in \Omega$ is an elliptic element, then $\lambda(\omega)$ is a vertex of $\mathcal{T}$ and G_ω is a subgroup of $G_{\lambda(\omega)}$. Moreover, $\lambda(\omega) = \lambda(\overline{\omega})$.*

Proof If δ is odd, for every $\varepsilon \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ the associated norm $v_\varepsilon((u, v)) = |u\varepsilon + v|$ on $K_\infty \oplus K_\infty$ obviously is the maximum norm $\max\{|u|, |v|\}$, whose unit ball is the standard lattice $\mathcal{O}_\infty \oplus \mathcal{O}_\infty$. So all $\varepsilon \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ map to the standard vertex in $\mathcal{T}$.

Now if ω is any elliptic point, by Theorem 2.5 we have $\omega = \frac{\varepsilon+s}{t}$ and $\overline{\omega} = \frac{\varepsilon^q+s}{t}$ for suitable $s, t \in A$. So under λ both, ω and $\overline{\omega}$ map to the same vertex of $\mathcal{T}$, namely the image of the standard vertex under the action of $\begin{pmatrix} 1 & s \\ 0 & t \end{pmatrix} \in GL_2(K_\infty)$.

The fact $G_\omega \leq G_{\lambda(\omega)}$ is clear. (See also [5, (1.5.3), p. 37].) □

We recall [14, Proposition 2, p. 76] that the elements of finite order in G are precisely those in

$$\bigcup_{v \in \mathrm{vert}(\mathcal{T})} G_v.$$

We note that

$$Z \leq G_e \cap G_\omega,$$

for all $e \in \mathrm{edge}(\mathcal{T})$ and $\omega \in E(G)$. Hence $q - 1$ divides all $|G_v|$.

Let $\omega \in E(G)$. Then we know that $G_\omega \leq G_{\lambda(\omega)}$ and consequently $q^2 - 1$ divides $|G_{\lambda(\omega)}|$, by Proposition 2.3. One of the main aims of this section is to establish the converse of this result. However, for that we need a few lemmata.

Lemma 4.2 *Let $M \in G_v$. Then the eigenvalues of M lie in $\mathbb{F}_{q^2}$.*

Proof The characteristic polynomial of M is

$$t^2 - \tau t + \eta,$$

where $\tau = \mathrm{tr}(M)$ and $\eta = \det(M) \in \mathbb{F}_q^*$. Now M has finite order and so τ lies in the algebraic closure of $\mathbb{F}_q$ in A which is $\mathbb{F}_q$. □

Lemma 4.3 *Let $w \in \mathrm{vert}(\mathcal{T}) \cup \mathrm{edge}(\mathcal{T})$. Suppose that M_1, M_2 are matrices in G_w. If*

$$\det(\alpha_1 M_1 + \alpha_2 M_2) \in \mathbb{F}_q^*,$$

where $\alpha_1, \alpha_2 \in \mathbb{F}_q$, then

$$\alpha_1 M_1 + \alpha_2 M_2 \in G_w.$$

Proof If M_i fixes a vertex, that is, a lattice class Λ, then because of $M_i \in GL_2(A)$ by [14, II.1.3 Lemma 1, p. 76] it fixes any underlying lattice L. Thus $\alpha_1 M_1 + \alpha_2 M_2$ is an endomorphism of L. But since its determinant is invertible in $\mathcal{O}_\infty$, it actually is an automorphism of L. So it fixes the same lattice class. □

As is clear from the proof of Proposition 2.3, Lemma 4.3 also holds for G_ω, where $\omega \in E(G)$. Our next result shows that, when $v = \lambda(\omega)$, the structure of G_v can be determined completely.

Proposition 4.4 *Let $\omega \in \Omega$ be an elliptic element, and let let $v = \lambda(\omega)$ be its image under the building map. There are two possibilities.*

(i) If $\omega \not\equiv \overline{\omega}$, then

$$G_v = G_\omega \cong \mathbb{F}_{q^2}^*,$$

in which case $|G_v| = q^2 - 1$.

(ii) If $\omega \equiv \overline{\omega}$, then

$$G_v \cong GL_2(\mathbb{F}_q),$$

in which case $|G_v| = q(q-1)^2(q+1)$.

Proof By Proposition 2.3 and Lemma 4.1, $G_\omega \cong \mathbb{F}_{q^2}^*$ and $G_\omega \leq G_v$. By [10, Corollary 2.12] there are only two possibilities, namely $G_v = G_\omega \cong \mathbb{F}_{q^2}^*$ or $G_v \cong GL_2(\mathbb{F}_q)$.

If $M\omega = \overline{\omega}$, then M lies in G_v (by Lemma 4.1) but not in G_ω; so $G_v \cong GL_2(\mathbb{F}_q)$. To see the converse fix a generator M_1 of G_ω. Then there is another generator M_2 of G_ω that has the same characteristic polynomial. Hence M_1 and M_2 are conjugate in $G_v \cong GL_2(\mathbb{F}_q)$, say by the matrix M_3. Since M_3 respects the fixed points of G_ω, we have $M_3\omega = \overline{\omega}$. □

Our next lemma highlights the importance of the $q^2 - 1$ as a feature of our results.

Lemma 4.5 *For a vertex stabilizer G_v the following three statements are equivalent:*

(i) $q^2 - 1$ divides $|G_v|$.
(ii) G_v contains a matrix whose eigenvalues are not in $\mathbb{F}_q$.
(iii) G_v contains a cyclic subgroup of order $q^2 - 1$.

Proof (i) $\Rightarrow$ (ii): If $q+1$ is divisible by an odd prime r, then r divides neither q nor $q-1$. Let $M \in G_v$ be an element of order r. From the order we see that the eigenvalues of M cannot be in $\mathbb{F}_q$. If $q+1$ is not divisible by any odd prime, then it is divisible by 4. If G_v contains an element of order 4, we can argue as before. If not, we fix a 2-Sylow subgroup of P of G_v, which then is necessarily of exponent 2 and hence abelian. So all matrices in P can be simultaneously diagonalized. Since the eigenvalues can only be 1 and -1, there are only 4 such diagonal matrices. But the order of P is divisible by 8, a contradiction.

(ii) $\Rightarrow$ (iii): If the eigenvalues of M are not in $\mathbb{F}_q$, then by Lemma 4.2 they are in $\mathbb{F}_{q^2}\backslash\mathbb{F}_q$. Let

$$I(M) = \left\{\alpha I_2 + \beta M : \alpha, \beta \in \mathbb{F}_q^*,\ (\alpha, \beta) \neq (0,0)\right\}.$$

By Lemma 4.3 then $I(M) \leq G_v$. Part (iii) follows since $I(M) \cong \mathbb{F}_{q^2}^*$.

(iii) $\Rightarrow$ (i) is trivial. □

For some q (for example $q=4$) every subgroup of G of order q^2-1 is cyclic. On the other hand for the case $q=3$ the embedding of A_4 in $PGL_2(\mathbb{F}_3)$ gives rise to a subgroup S of G containing Z of order 8 for which S/Z is not cyclic.

In Lemma 4.5 the condition (i) can be replaced by

(i)′ $|G_v|$ *is divisible by* $q+1$ $(q \neq 3)$ *and* 8 $(q=3)$.

Here the restriction when $q=3$ is necessary. It is well-known [14, p. 86] that, when $A = \mathbb{F}_3[t]$, there is a vertex v' for which

(1) $|G_{v'}| = 12$,
(2) every matrix in $G_{v'}$ has eigenvalues in $\mathbb{F}_3^*$.

We note that the proof of Lemma 4.5 shows that when, $q \neq 3$, the following implication holds.

$$q+1 \textit{ divides } |G_v| \Rightarrow q^2-1 \textit{ divides } |G_v|.$$

As stated above the main aim in this section is to prove that the converse of Proposition 4.4 holds. We will prove that, if q^2-1 divides $|G_v|$, then $v = \lambda(\omega)$ for some elliptic point $\omega \in E(G)$. We require one more lemma.

Lemma 4.6 *Let δ be odd and let $M \in G$ be a matrix of finite order whose eigenvalues are not in $\mathbb{F}_q$. Then*

(i) M does not fix any edges of $\mathcal{T}$.
(ii) M fixes exactly one vertex of $\mathcal{T}$.

Proof (i) Suppose that M fixes an edge. Then there exists a matrix $P \in GL_2(K_\infty)$ that maps this edge to the standard edge whose stabilizer is $Z_\infty \cdot \mathcal{J}$ where Z_∞ is the centre of $GL_2(K_\infty)$ and $\mathcal{J}$ is the Iwahori group

$$\mathcal{J} = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathcal{O}_\infty) \ :\ c \in \pi\mathcal{O}_\infty\right\}.$$

From the determinant we see that P conjugates M into $\mathcal{J}$. Let $\widetilde{M} \in \mathcal{J}$ be this conjugate of M. Then the characteristic polynomial $X^2 - \tau X + \eta$ of $\widetilde{M}$ is irreducible over $\mathbb{F}_q$, and hence over $\mathbb{F}_{q^\delta}$ if δ is odd.

On the other hand, reducing $\widetilde{M}$ modulo the maximal ideal of $\mathcal{O}_\infty$ we obtain a matrix with the same characteristic polynomial. But the reduced matrix has the form $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ with entries in $\mathbb{F}_{q^\delta}$. So its characteristic polynomial splits over $\mathbb{F}_{q^\delta}$, a contradiction.

(ii) By [14, Proposition 2, p. 79] M fixes at least one vertex. If M fixes two different vertices of $\mathcal{T}$, then it fixes the whole geodesic on $\mathcal{T}$ between these two vertices and hence at least one edge in contradiction to (i). □

By the way, Lemma 4.6(ii) provides an alternative proof of the claim in Lemma 4.1 that $\lambda(\omega) = \lambda(\overline{\omega})$.

We now come to the principal results of this section.

Theorem 4.7 *Let δ be odd and let $v \in \mathrm{vert}(\mathcal{T})$. Then*

$$v = \lambda(\omega),\ \textit{for some } \omega \in E(G),\quad \textit{if and only if } q^2 - 1 \textit{ divides } |G_v|.$$

Proof If $v = \lambda(\omega)$ for some $\omega \in E(G)$, then $q^2 - 1$ divides $|G_v|$ by Proposition 4.4.

Conversely, assume that q^2-1 divides $|G_v|$. Then G_v contains a cyclic subgroup C of order q^2-1 by Lemma 4.5. By Lemma 2.6 this subgroup C fixes an elliptic point $\omega \in E(G)$. Again by Proposition 4.4 we know that $q^2 - 1$ divides $|G_{v'}|$ for $v' = \lambda(\omega)$. Since C is contained in G_v and $G_{v'}$, Lemma 4.6 implies $v' = v$. □

Theorem 4.8 *If δ is odd, there exist natural bijections between the following sets*

(i) vertices $\widetilde{v}$ of $G\backslash\mathcal{T}$ such that $q^2 - 1$ divides $|G_v|$;
(ii) conjugacy classes (in G) of cyclic subgroups of G of order $q^2 - 1$;
(iii) the orbits of the $Gal(\widetilde{K}/K)$-action on $\mathrm{Ell}(G)$.

Proof We first establish the bijection between (i) and (ii). Let v be a vertex of $\mathcal{T}$ with image $\widetilde{v}$ in $G\backslash\mathcal{T}$. If $G_v \cong \mathbb{F}_{q^2}^*$, this is such a cyclic subgroup of order $q^2 - 1$, and the stabilizers of the other lifts of $\widetilde{v}$ to $\mathrm{vert}(\mathcal{T})$ are exactly the conjugates of G_v. A similar argument applies if $G_v \cong GL_2(\mathbb{F}_q)$. Of course, then G_v has several cyclic subgroups of order $q^2 - 1$, but they are all conjugate (already in G_v).

Conversely, let C be a cyclic subgroup of G of order q^2-1. By Lemma 4.6 it fixes exactly one vertex of $\mathcal{T}$. So its conjugacy class fixes exactly one vertex of $G\backslash\mathcal{T}$.

The bijection between (ii) and (iii) follows by applying the action of G to the bijection in Lemma 2.6. □

Remark 4.9 Theorem 4.8 (in combination with Proposition 4.4) implies in particular that over every vertex $\widetilde{v}$ of $G\backslash\mathcal{T}$ with $G_v \cong GL_2(\mathbb{F}_q)$ there lies exactly one elliptic point of $G\backslash\Omega$; and over every vertex $\widetilde{v}$ of $G\backslash\mathcal{T}$ with $G_v \cong \mathbb{F}_{q^2}^*$ lie two ($Gal(\widetilde{K}/K)$-conjugate) elliptic points of $G\backslash\Omega$.

But when considering the building map $\lambda : \Omega \to \mathcal{T}$, over every vertex v of $\mathcal{T}$ with $G_v \cong GL_2(\mathbb{F}_q)$ there lie $q(q-1)$ elliptic points on Ω, in $q(q-1)/2$ pairs of $Gal(\widetilde{K}/K)$-conjugate elliptic points, corresponding to the $q(q-1)/2$ different cyclic subgroups of order q^2-1 in $GL_2(\mathbb{F}_q)$. (Compare Lemmas 2.6 and 4.6.) Over every vertex v of $\mathcal{T}$ with $G_v \cong \mathbb{F}_{q^2}^*$ we again have one pair of $Gal(\widetilde{K}/K)$-conjugate elliptic points on Ω.

One should not forget however that there also are uncountably many non-elliptic points lying over each of these vertices, as for every vertex v of $\mathcal{T}$ there are uncountably many points of Ω mapping to v under the building map.

A much more general statement than Proposition 4.4, namely the complete classification of all possible types of vertex stabilizers for any constant field (not just for $\mathbb{F}_q$) and for any δ is given in [10].

5 Isolated vertices and amalgams

A vertex $\widetilde{v}$ of the quotient graph $G\backslash\mathcal{T}$ is called *isolated* if there is only one edge of $G\backslash\mathcal{T}$ attached to it. Obviously this is equivalent to G_v acting transitively on the $q^\delta + 1$ edges of $\mathcal{T}$ attached to v.

Theorem 5.1 *Let $v \in \mathrm{vert}(\mathcal{T})$. Then $\widetilde{v}$ is an isolated vertex of $G\backslash\mathcal{T}$ if and only if the following two conditions both hold:*

(i) $\delta = 1$,
(ii) G_v *satisfies any of the three equivalent conditions of Lemma 4.5.*

Proof Assume first that $\delta = 1$ and G_v contains a cyclic group of order $q^2 - 1$. Then by Lemma 4.6 none of the elements outside Z can fix an edge. So G_v acts transitively on the $q + 1$ edges adjacent to v, and $\widetilde{v}$ is isolated.

Now assume conversely that $\widetilde{v}$ is isolated. Then G_v acts transitively on the $q^\delta + 1$ edges emanating from v. So $|G_v|$ is divisible by $(q-1)(q^\delta + 1)$.

If $q^\delta + 1$ is divisible by an odd prime r, then r divides neither q nor $q - 1$. Let $M \in G_v$ be an element of order r. From the order we see that the eigenvalues of M cannot be in $\mathbb{F}_q$. But by Lemma 4.2 they are in $\mathbb{F}_{q^2}$, so r divides $q + 1$. Together with r dividing $q^\delta + 1$ this implies that δ is odd. If δ were bigger than 1, then G_v would act transitively on at least $q^3 + 1$ edges. But $|G_v/Z| \leq q^3 - q$ by Proposition 4.4.

If $q^\delta + 1$ is not divisible by any odd prime, then it is divisible by 4, and hence q is congruent to 3 modulo 4 and δ is odd. As above we obtain $\delta = 1$. Moreover, $q + 1$ divides $|G_v|$ because it divides $q^\delta + 1$. □

Combining Theorem 5.1 with Theorem 4.8 we obtain the following

Corollary 5.2 *Let $\delta = 1$. Then the building map induces a bijection between the $Gal(\widetilde{K}/K)$-orbits on elliptic points of $G\backslash\Omega$ and the isolated vertices of $G\backslash\mathcal{T}$ with the properties described in Proposition 4.4.*

The number of isolated vertices with stabilizer isomorphic to $GL_2(\mathbb{F}_q)$ (resp. to $\mathbb{F}_{q^2}^*$) is $|\,\mathrm{Ell}(G)_2|$ (resp. $r = \frac{1}{2}(|\,\mathrm{Ell}(G)| - |\,\mathrm{Ell}(G)_2|)$). In particular, these numbers only depend on K, not on the choice of the degree one place ∞.

We also record a graph-theoretic property of isolated vertices.

Proposition 5.3 *(a) Let δ be odd and let $v_1, v_2 \in \mathrm{vert}(\mathcal{T})$, where $|G_{v_i}|$ is divisible by $q^2 - 1$, $(i = 1, 2)$. Then the (geodesic) distance between v_1 and v_2 (in $\mathcal{T}$) and consequently the distance between $\widetilde{v_1}$ and $\widetilde{v_2}$ (in $G\backslash\mathcal{T}$) is even.*
(b) The distance between any two isolated vertices of $G\backslash\mathcal{T}$ is even.

Proof (a) By Theorem 4.7 there exist $\omega_i \in E(G)$ with $v_i = \lambda(\omega_i)$, $(i = 1, 2)$. Fix $\varepsilon \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. By Theorem 2.5 we can write $\omega_i = \frac{\varepsilon + s_i}{t_i}$ with $s_i, t_i \in A$. Thus $\omega_2 = M(\omega_1)$ with

$$M = \begin{bmatrix} 1 & s_2 \\ 0 & t_2 \end{bmatrix} \begin{bmatrix} t_1 & -s_1 \\ 0 & 1 \end{bmatrix} \in GL_2(K_\infty).$$

Consequently $v_2 = M(v_1)$ by [GR, (1.5.3)]. Let $d(v_1, v_2)$ be the distance between v_1 and v_2. Then by [14, Corollary, p. 75] and Lemma 2.7(b)

$$d(v_1, v_2) \equiv \nu(\det(M)) \equiv \nu(t_1) + \nu(t_2) \equiv 0 \pmod 2.$$

Part (b) follows from part (a) and Theorem 5.1. □

The principal group-theoretic consequence of Theorem 5.1 is the following.

Theorem 5.4 *Suppose that* $\delta = 1$ *and that* $\widetilde{v}$ *is an isolated vertex of* $G\backslash\mathcal{T}$. *There are two possibilities.*

(i) If $G_v \cong GL_2(\mathbb{F}_q)$, *then there exists a subgroup* H *of* G *such that*

$$G \cong GL_2(\mathbb{F}_q) \underset{B_2(\mathbb{F}_q)}{*} H,$$

where $B_2(\mathbb{F}_q)$ *is the usual Borel subgroup of* $GL_2(\mathbb{F}_q)$ *(of order* $q(q-1)^2$*).*

(ii) If $G_v \cong \mathbb{F}_{q^2}^*$, *then there exists a subgroup* H *of* G *for which*

$$G \cong \mathbb{F}_{q^2}^* \underset{Z}{*} H.$$

Hence

$$PGL_2(A) \cong (\mathbb{Z}/(q+1)\mathbb{Z}) * H',$$

where $H' = H/Z$.

In both cases H *can be chosen such that it contains all upper triangular matrices from* G.

Proof Bass–Serre theory [14, Theorem 13, p. 55] presents G as the *fundamental group of a graph of groups* [14, p. 42] given by a *lift*

$$j : \mathcal{T}_0 \longrightarrow \mathcal{T},$$

where $\mathcal{T}_0$ is a maximal subtree of $G\backslash\mathcal{T}$. We can choose $j(\mathcal{T}_0)$ such that it contains all vertices Λ_n with

$$L_n := \mathcal{O}_\infty \oplus \pi^n \mathcal{O}_\infty$$

for sufficiently big n. These map to one of the infinite half-lines of $G\backslash\mathcal{T}$.

Now let v be the vertex of $j(\mathcal{T}_0)$ that maps to $\widetilde{v}$ and let e be the edge of $j(\mathcal{T}_0)$ incident with v. As $\widetilde{v}$ is isolated in $G\backslash\mathcal{T}$, we have $|G_v : G_e| = q+1$. By Bass–Serre theory [14, p. 42] we have

$$G \cong G_v \underset{G_e}{*} H,$$

where H is the fundamental group of the graph of groups obtained from $G\backslash\mathcal{T}$ by removing the isolated vertex $\widetilde{v}$ and the edge incident with it. In particular, H contains all stabilizers of all vertices of $j(\mathcal{T}_0)$ that are different from v. So by our construction H contains

$$G_{\Lambda_n} = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in GL_2(A) \;:\; v(b) \geq -n \right\}$$

for all sufficiently big n, and hence H contains all upper triangular matrices. □

When $\delta = 1$ a decomposition of type (i) always occurs because the standard vertex has stabilizer $GL_2(\mathbb{F}_q)$. More interesting decompositions occur when there are isolated vertices of type (ii).

Theorem 5.5 *Suppose that* $\delta = 1$. *Then there exists a subgroup* P *of* $PGL_2(A)$ *for which the following free product decomposition holds*

$$PGL_2(A) \cong \left(\mathop{*}_{i=1}^{r} \mathbb{Z}/(q+1)\mathbb{Z} \right) * P,$$

where

$$2r = |\,\mathrm{Ell}(G)| - |\,\mathrm{Ell}(G)_2|.$$

Actually, P can be chosen in such a way that it contains all upper triangular matrices from $PGL_2(A)$.

Moreover r is maximal in the following sense. Suppose that C is a cyclic subgroup of $PGL_2(A)$ of order $q+1$ for which

$$PGL_2(A) = C * Q.$$

Then there exists $v \in \mathrm{vert}(\mathcal{T})$ such that

(i) $G_v \cong \mathbb{F}_{q^2}$,
(ii) $\psi(G_v) = C$, *where* $\psi : G \to PGL_2(A)$ *is the natural map.*

Proof Let

$$\widetilde{V} = \{\widetilde{v} \in \mathrm{vert}(G\backslash\mathcal{T}) : \ G_v \cong \mathbb{F}^*_{q^2}\}.$$

Let $\widetilde{v_1},\ \widetilde{v_2} \in \widetilde{V}$. Then, by Theorem 4.7, $G_{v_i} = G_{\omega_i}$, for some $\omega_i \in E(G)$, where $\omega_i \not\equiv \overline{\omega_i}$, $(i = 1, 2)$. If $\widetilde{v_1} = \widetilde{v_2}$, then $v_2 = g(v_1)$, for some $g \in G$, so that $G_{\omega_2} = gG_{\omega_1}g^{-1} = G_{g(\omega_1)}$. It follows that $\{\omega_2,\ \overline{\omega_2}\} = \{g(\omega_1),\ g(\overline{\omega_1})\}$.

On the other hand if $\omega_j (\not\equiv \overline{\omega_j}) \in E(G)$ and $S_j = \{\omega_j\ \overline{\omega_j}\}$, where $j = 3, 4$, then for all $g \in G$ either $S_3 = g(S_4)$ or $S_3 \cap g(S_4) = \emptyset$. By Corollary 5.2 we have $|\widetilde{V}| = r$, where r is defined as above.

The free product decomposition is a consequence of an iteration of the process described in the proof of Theorem 5.4(ii).

For the last part of the theorem C, under ψ, lifts to a cyclic subgroup C' of G of order q^2-1. Now by [14, Proposition 2, p. 76] $C' \le G_v$, for some $v \in \mathrm{vert}(\mathcal{T})$. Then by Theorem 4.7 there are two possibilities for G_v, described in Proposition 4.4. Either $G_v = C'$ in which case we are finished, or $G_v \cong PGL_2(\mathbb{F}_q)$. In the latter case the canonical map from $PGL_2(A)$ onto C restricts to an epimorphism

$$PGL_2(\mathbb{F}_q) \twoheadrightarrow C.$$

This gives the desired contradiction. □

Theorem 5.6 *(a) For $q \ge 8$ and $g > 0$ there exist exactly two rings A (up to isomorphism) such that all isolated vertices of $GL_2(A)\backslash\mathcal{T}$ have stabilizers isomorphic to $GL_2(\mathbb{F}_q)$, namely $A = \mathbb{F}_9[x, y]$ with $y^3 + y = x^4$ (genus 3) or with $y^2 = x^3 - x$ (genus 1).*

(b) For fixed $q \ge 8$ the number r of free factors in Theorem 5.5 grows exponentially with g. More precisely, for $q \ge 8$ and all cases of positive genus except the two discussed in part (a) we have

$$r \ge \frac{1}{4}(\sqrt{q} - 1)^{2g} > \frac{3^g}{4}.$$

Proof (a) From Theorem 3.9(a) we know already that there are only two fields K with these properties. For any choice of the place ∞ of degree 1 we get a ring A with this property. It remains to show that different choices of ∞ give isomorphic rings.

For the genus 3 case we use that by [15, Exercise 6.10] the automorphism group of a Hermitian function field (that is, a function field $\mathbb{F}_{q^2}(x, y)$ with $y^q + y = x^{q+1}$) acts transitively on its places of degree 1. So different choices of ∞ will lead to isomorphic rings A.

The elliptic case can be seen by some easy calculations with Weierstrass equations.
(b) If $\mathrm{Ell}(G)_2$ is strictly smaller than $\mathrm{Ell}(G)$, then, because of the group structure, it has index at least 2. Hence, if there are elements of order bigger than 2 in $\mathrm{Ell}(G)$, their number is at least $\frac{1}{2}L_K(-1) \geq \frac{1}{2}(\sqrt{q}-1)^{2g}$. So in that case the number of isolated vertices with cyclic stabilizer is at least $\frac{1}{4}(\sqrt{q}-1)^{2g}$, which for $q \geq 8$ is bigger than $\frac{1}{4}3^g$. □

Remark 5.7 (a) It is, of course, well possible that the group $PGL_2(A)$ also splits off other free factors than those stipulated by Theorem 5.5. Let for example $A = \mathbb{F}_9[x, y]$ with $y^2 = x^3 - x$. Then $r = 0$, but from Takahashi's results [16] one obtains that in this case $PGL_2(A)$ is a free product of 10 infinite groups.

(b) By the same arguments as in the proof of Theorem 5.6(b), for $q \in \{5, 7\}$ we still have $r > \frac{1}{4}(\frac{3}{2})^g$ *provided* r is not zero. (Compare Remark 3.10.)

(c) Theorem 5.5 has a number of interesting consequences. For example suppose that $r \geq 2$ and that $q \equiv -1 \pmod 6$. Then there exists an epimorphism

$$\theta : PGL_2(A) \twoheadrightarrow PSL_2(\mathbb{Z}),$$

since

$$PSL_2(\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z}) * (\mathbb{Z}/3\mathbb{Z}).$$

Example 5.8 Let

$$A = \mathbb{F}_2[x, y] \quad \text{with} \quad y^2 + y = x^3 + x + 1.$$

This elliptic curve has exactly one rational point, namely the one at infinity. So $L_K(u) = 1 - 2u + 2u^2$, and thus $L_K(-1) = 5$ and $r = 2$. More precisely,

$$PGL_2(A) \cong GL_2(A) \cong \mathbb{Z}/3\mathbb{Z} * \mathbb{Z}/3\mathbb{Z} * \Delta(\infty),$$

where $\Delta(\infty) = B_2(A) *_{B_2(\mathbb{F}_2)} GL_2(\mathbb{F}_2)$ (cf. Takahashi [16], [8, Theorem 5.3] or (the proof of) [9, Lemma 5.2 (c)]). Since the normal hull of $B_2(A)$ in $GL_2(A)$ contains all elements from $\Delta(\infty)$, we see that a finite group can be generated by two elements of order 3 if and only if it is the quotient of this $GL_2(A)$ by a normal non-congruence subgroup of level A. For results on which classical finite simple groups can be generated by two elements of order 3 see [6, Corollary 1.8].

Example 5.9 Let

$$A = \mathbb{F}_7[x, y] \quad \text{with} \quad y^2 = x^3 + 4.$$

Then $L_K(u) = 1 - 5u + 7u^2$. Thus $L_K(-1) = 13$ and $r = 6$. So there exists a surjective homomorphism from $GL_2(A)$ to any finite (or infinite) group that is generated by at most 6 elements of orders dividing 8. More precisely, by Takahashi's description of the quotient graph (cf. [16]) we have

$$PGL_2(A) \cong \left(\mathop{*}_{i=1}^{6} \mathbb{Z}/8\mathbb{Z} \right) * \Delta(0) * \Delta(\infty),$$

where $\Delta(0)$, $\Delta(\infty)$ are infinite subgroups and, again, $\Delta(\infty)$ contains all upper triangular matrices (modulo Z).

In particular, there exists a normal non-congruence subgroup N of level A such that G/N is isomorphic to the permutation group of Rubik's cube (which is generated by 6 elements of order 4). Recall that the order of that permutation group is roughly 43×10^{18}.

Acknowledgments This paper is part of a project supported by grant 99-2115-M-001-011-MY2 from the National Science Council (NSC) of Taiwan. The biggest part was written while the second author was working at the Institute of Mathematics at Academia Sinica in Taipei. He wants to thank Julie Tzu-Yueh Wang, Wen-Ching Winnie Li, Jing Yu, Liang-Chung Hsia and Chieh-Yu Chang for help in general as well as for help with the application for that grant. During the final stage the second author was supported by ASARC in South Korea. Several ideas in the paper were developed during research visits of the second author at Glasgow University. The hospitality of their Mathematics Department is gratefully acknowledged. Finally, the second author thanks Ernst-Ulrich Gekeler for helpful discussions during a research visit to Saarbrücken.

References

1. Bautista-Ancona, V., Diaz-Vargas, J.: Quadratic function fields with exponent two ideal class group. J. Number Theory **116**, 21–41 (2006)
2. Bourbaki, N.: Commutative Algebra. Addison-Wesley, London (1972)
3. Drinfeld, V.G.: Elliptic modules. Math. USSR-Sbornik **23**, 561–592 (1976)
4. Gekeler, E.-U.: Drinfeld Modular Curves. Springer LNM 1231, Berlin (1986)
5. Gekeler, E.-U., Reversat, M.: Jacobians of Drinfeld modular curves. J. Reine Angew. Math. **476**, 27–93 (1996)
6. Liebeck, M., Shalev, A.: Classical groups, probabilistic methods, and the (2, 3)-generation problem. Ann. Math. **144**, 77–125 (1996)
7. Mason, A.W.: Serre's generalization of Nagao's theorem: an elementary approach. Trans. Am. Math. Soc. **353**, 749–767 (2003)
8. Mason, A.W., Schweizer, A.: The minimum index of a non-congruence subgroup of SL_2 over an arithmetic domain. II: The rank zero cases. J. Lond. Math. Soc. **71**, 53–68 (2005)
9. Mason, A.W., Schweizer, A.: Non-standard automorphisms and non-congruence subgroups of SL_2 over Dedekind domains contained in function fields. J. Pure Appl. Algebra **205**, 189–209 (2006)
10. Mason, A.W., Schweizer, A.: The stabilizers in a Drinfeld modular group of the vertices of its Bruhat–Tits tree: an elementary approach. Int. J. Algebra Comput. **23**(7), 1653–1683 (2013)
11. Rosen, M.: The Hilbert class field in function fields. Exp. Math. **5**, 365–378 (1987)
12. Rosen, M.: Number Theory in Function Fields. Springer GTM 210, Berlin (2002)
13. Rück, H.-G., Stichtenoth, H.: A characterization of Hermitian function fields over finite fields. J. Reine Angew. Math. **457**, 185–188 (1994)
14. Serre, J.-P.: Trees. Springer, Berlin (1980)
15. Stichtenoth, H.: Algebraic Function Fields and Codes, 2nd edn. Springer GTM 254, Berlin (2009)
16. Takahashi, S.: The fundamental domain of the tree of $GL(2)$ over the function field of an elliptic curve. Duke Math. J. **72**, 85–97 (1993)
17. Zariski, O., Samuel, P.: Commutative Algebra, vol. 1. Springer GTM 21, Berlin (1975)