Torsion bounds for elliptic curves and Drinfeld modules

Florian Breuer (fbreuer@sun.ac.za)
Stellenbosch University, Stellenbosch, South Africa

October 17, 2008

Abstract

We derive asymptotically optimal upper bounds on the number of L-rational torsion points on a given elliptic curve or Drinfeld module defined over a finitely generated field K, as a function of the degree [L : K]. Our main tool is the adelic openness of the image of Galois representations attached to elliptic curves and Drinfeld modules, due to Serre and Pink-Rütsche, respectively. Our approach is to prove a general result for certain Galois modules, which applies simultaneously to elliptic curves and to Drinfeld modules.

2000 Mathematics Subject Classification: 11G05, 11G09
Keywords: Elliptic curves, Drinfeld modules, torsion points, Galois representations

1 Statement of main result

Let A be a Dedekind domain whose fraction field k is a global field, and let M be an A-module. For a non-zero ideal a ⊂ A we denote by

\[ M[a] := \{ x \in M \mid a \cdot x = 0, \forall a \in a \} \]

the a-torsion submodule of M, by \( M[a^\infty] := \bigcup_{n \geq 1} M[a^n] \) the a-power torsion submodule, and by \( M_{\text{tor}} = \bigcup_{a \subset A} M[a] \) the full torsion submodule.

Let K be a finitely generated field, and denote by \( K^{\text{sep}} \) the separable closure of K in an algebraic closure \( \bar{K} \). Let \( G_K = \text{Gal}(K^{\text{sep}}/K) \) act on M. For a submodule \( H \subset M \) and a finite extension \( L/K \) we denote by \( H(L) \) the subset of \( H \) fixed by \( \text{Gal}(K^{\text{sep}}/L) \). The cardinality of a finite set \( S \) is denoted \( |S| \).

The goal of this article is to prove the following.

Theorem 1.1 Suppose we are in one of the following two situations:

(a) \( A = \mathbb{Z}, \ K \) is a finitely generated field of characteristic 0 and M is an elliptic curve over K. Set \( \gamma = \text{rank}_\mathbb{Z}(\text{End}_K(M))/2 \).

(b) \( k \) is a global function field and \( A \) is the ring of elements of \( k \) regular outside a fixed place \( \infty \) of \( k \). \( M \) is a rank \( r \) Drinfeld \( A \)-module in generic characteristic over the finitely generated field \( K \), and set \( \gamma = \text{rank}_A(\text{End}_K(M))/r \).

Then we have

(I) Let \( p \subset A \) be a non-zero prime ideal. Then there exists a constant \( C \) depending on \( M, K \) and \( p \) such that, for any finite extension \( L/K \),

\[ |M[p^\infty](L)| \leq C[L : K]^\gamma. \]
There exists a constant $C$ depending on $M$ and $K$ such that, for any finite extension $L/K$,

$$|M_{\text{tor}}(L)| \leq C([L : K] \log \log[L : K])^{\gamma}. \quad (2)$$

Moreover, these bounds are asymptotically optimal in the sense that there exist towers of fields achieving these bounds for suitable values of $C$.

2 Galois modules

Continuing with the notation from the previous section, we call $M$ a $(G_K, A)$-module of rank $r$ if the action of $G_K$ commutes with the action of $A$, and $M[a] \cong (A/a)^r$ as $A$-modules for every non-zero ideal $a \subset A$.

Then for every non-zero ideal $a \subset A$ the action of $G_K$ induces a Galois representation

$$\rho_a : G_K \longrightarrow \text{Aut}(M[a]) \cong \text{GL}_r(A/a),$$

once we have chosen a basis for $M[a]$. We denote the index of the image by

$$I(a) := (\text{GL}_r(A/a) : \rho_a(G_K)).$$

Our main tool is

**Theorem 2.1** Let $M$ be a $(G_K, A)$-module of rank $r$.

(I) Let $p \subset A$ be a non-zero prime ideal. Suppose that there exists a constant $C_p$, depending on $M$, $K$ and $p$, such that $I(p^n) \leq C_p$ for all $n \in \mathbb{N}$. Then there exists a constant $C$ depending on $C_p, r$ and $K$ such that, for every finite extension $L/K$,

$$|M[p^\infty](L)| \leq C[L : K]^{1/r}.$$

(II) Suppose that there exists a constant $C_0$, depending on $M$ and $K$, such that $I(a) \leq C_0$ for all non-zero $a \subset A$. Then there exists a constant $C$ depending on $C_0, r$ and $K$ such that, for every finite extension $L/K$,

$$|M_{\text{tor}}(L)| \leq C([L : K] \log \log[L : K])^{1/r}.$$

Moreover, these bounds are asymptotically optimal in the sense that there exist towers of fields achieving these bounds for suitable values of $C$.

2.1 Elementary Lemmas

We collect the following elementary results, which we will need in the proof of Theorem 2.1.

For a non-zero ideal $a \subset A$ we write $|a| := |A/a|$. We define the function

$$\theta(a) := \prod_{p | a} \left(1 - \frac{1}{|p|}\right)^{-1},$$

where the product ranges over all prime ideals $p | a$.
Lemma 2.2 There exist constants $C_1, C_2 > 0$, depending on $A$, such that $\theta(a) \leq C_1 \log \log |a|$ for all non-zero $a \subset A$. Moreover, if $a_n := \prod_{|p| \leq n} p$, then $\theta(a_n) \geq C_2 \log \log |a_n|$ for all $n \in \mathbb{N}$.

Proof. It is clear that $\theta(a)$ achieves its fastest growth (relative to $|a|$) for $a_n := \prod_{|p| \leq n} p$.

We start with the following version of Mertens’ Theorem [16, Theorems 2 and 3]:

$$\theta(a_n) = \prod_{|p| \leq n} \left(1 - \frac{1}{|p|}\right)^{-1} = C_1 \log n + O(1),$$

for an explicit constant $C_1 > 0$. On the other hand, we have,

$$\log |a_n| = \sum_{|p| \leq n} \log |p| = n + o(1).$$

When $k$ is a number field, this is [16, Theorem 2.2]. When $k$ is a function field over the finite field of $q$ elements, this follows readily from the well-known estimate

$$|\{p \text{ prime} \mid |p| = q^m\}| = \frac{q^n}{m} + O\left(\frac{q^{m/2}}{m}\right).$$

Lemma 2.3 Let $a \subset A$ be a non-zero ideal. Then

$$|GL_r(A/a)| = |a|^n \prod_{|p| \leq n} \left(1 - \frac{1}{|p|}\right) \left(1 - \frac{1}{|p|^2}\right) \cdots \left(1 - \frac{1}{|p|^r}\right).$$

Proof. Since $|GL_r(A/a)|$ is multiplicative in $a$, it suffices to prove the result for $a = p^n$, where $p \subset A$ is prime.

It is well-known that $|GL_r(A/p)| = (|p|^r - 1)(|p|^r - |p|) \cdots (|p|^r - |p|^{r-1})$, and the general result follows from the exact sequence

$$1 \rightarrow 1 + M_r(p/p^n) \rightarrow GL_r(A/p^n) \rightarrow GL_r(A/p) \rightarrow 1,$$

where $M_r$ denotes the additive group of $r \times r$ matrices.

Lemma 2.4 Let $K_i/K$ and $L_i/K_i$ be finite extensions inside $\bar{K}$, for $i = 1, 2, \ldots, r$. We denote by $\prod_{i=1}^r K_i$ the compositum of the fields $K_1, \ldots, K_r$ inside $\bar{K}$, and similarly for $\prod_{i=1}^r L_i$. Then

$$\frac{\prod_{i=1}^r [K_i : K]}{[\prod_{i=1}^r K_i : K]} \leq \frac{\prod_{i=1}^r [L_i : K]}{[\prod_{i=1}^r L_i : K]}.$$

Proof. Elementary.
2.2 Fields of definition

Let \( H \subset M[\mathfrak{a}] \) be a subset, define

\[
\text{Fix}_{\text{Aut}(M[\mathfrak{a}])(H)} := \{ \sigma \in \text{Aut}(M[\mathfrak{a}]) \mid \sigma(h) = h, \forall h \in H \},
\]

and denote by \( K(H) \) the field generated by \( H \) over \( K \), i.e. \( K(H) \) is the fixed field of \( \rho_{\mathfrak{a}}^{-1}(\text{Fix}_{\text{Aut}(M[\mathfrak{a}])(H)}) \). When \( H = \{ x \} \) we write \( K(H) = K(x) \). Then \( \rho_{\mathfrak{a}} \) induces an isomorphism:

**Lemma 2.5**

\[
\text{Gal} \left( K(H)/K \right) \cong \frac{\rho_{\mathfrak{a}}(G_K)}{\rho_{\mathfrak{a}}(G_K) \cap \text{Fix}_{\text{Aut}(M[\mathfrak{a}])(H)}}.
\]

\[\square\]

Let \( x \in M_{\text{tor}} \). Then we say that \( x \) has order \( \mathfrak{a} \), where \( \mathfrak{a} \subset A \) is a non-zero ideal, if \( x \in M[\mathfrak{a}] \) but \( x \notin M[\mathfrak{b}] \) for any ideal \( \mathfrak{b} \supseteq \mathfrak{a} \). We also denote by \( \zeta_A(s) = \prod_p (1 - |p|^{-s})^{-1} \) the zeta-function of \( A \).

**Proposition 2.6** Let \( x \in M_{\text{tor}} \) be a point of order \( \mathfrak{a} \). Then

\[
[K(x) : K] = \frac{1}{C} |\mathfrak{a}|^r \prod_{p | \mathfrak{a}} \left( 1 - \frac{1}{|p|^r} \right)
\]

where \( 1 \leq C \leq I(\mathfrak{a}) \).

**Proof.** Choose a basis for \( M[\mathfrak{a}] \) such that \( x \) is the first basis element. This choice determines the isomorphism \( \text{Aut}(M[\mathfrak{a}]) \cong \text{GL}_r(A/\mathfrak{a}) \). The stabilizer of \( x \) in \( \text{GL}_r(A/\mathfrak{a}) \) is of the form

\[
\text{Fix}_{\text{GL}_r(A/\mathfrak{a})}(x) = \begin{pmatrix} 1 & * & \cdots & * \\ 0 & \vdots & \ddots & \text{GL}_{r-1}(A/\mathfrak{a}) \\ 0 & \text{GL}_{r-1}(A/\mathfrak{a}) \end{pmatrix}
\]

where the starred entries of the first row are arbitrary elements of \( A/\mathfrak{a} \) and the bottom right \( (r-1) \times (r-1) \) block is \( \text{GL}_{r-1}(A/\mathfrak{a}) \). It follows from Lemma 2.5 that

\[
|\text{Fix}_{\text{GL}_r(A/\mathfrak{a})}(x)| = |\mathfrak{a}|^{r-1} |\text{GL}_{r-1}(A/\mathfrak{a})|
\]

\[
= |\mathfrak{a}|^{r(r-1)} \prod_{p | \mathfrak{a}} \left( 1 - \frac{1}{|p|} \right) \left( 1 - \frac{1}{|p|^r} \right) \cdots \left( 1 - \frac{1}{|p|^{r-1}} \right).
\]

From Lemma 2.5 follows that

\[
[K(x) : K] = \frac{1}{C} \frac{|\text{GL}_r(A/\mathfrak{a})|}{|\text{Fix}_{\text{GL}_r(A/\mathfrak{a})}(x)|}
\]

\[
= \frac{1}{C} |\mathfrak{a}|^r \prod_{p | \mathfrak{a}} \left( 1 - \frac{1}{|p|^r} \right),
\]

where \( 1 \leq C \leq I(\mathfrak{a}) \).

\[\square\]
Proposition 2.7 Suppose $r \geq 2$. Then there exists a constant $C > 0$ depending on $I(a)$ and $K$, such that the following holds. Let $x_1, \ldots, x_r \in M[a]$ be a basis for $M[a]$. Then
\[
\prod_{i=1}^{r} \left[ K(x_i) : K \right] \leq C \theta(a).
\]

Of course, $[K(x_1) : K] = [K(M[a]) : K]$ if $r = 1$.

Proof. From Lemma 2.5 we obtain
\[
[K(M[a]) : K] = \frac{1}{I(a)} |GL_r(A/a)|.
\]

Now Lemma 2.3 and Proposition 2.6 give
\[
\prod_{i=1}^{r} [K(x_i) : K] \leq I(a) \prod_{p\mid a} \left( 1 - \frac{1}{|p|^r} \right)^{-1} \left( 1 - \frac{1}{|p|} \right)^{-1} \left( 1 - \frac{1}{|p|^{r-1}} \right)^{-1} \left( 1 - \frac{1}{|p|} \right)^{-1} \left( 1 - \frac{1}{|p|^{r-1}} \right)^{-1} \cdots 
\]
\[
\leq I(a) \zeta_A(2) \zeta_A(3) \cdots \zeta_A(r-1) \cdot \prod_{p\mid a} \left( 1 - \frac{1}{|p|} \right)^{-1}.
\]

The intuition is that the fields generated by linearly independent torsion points have minimal intersection. Explicitly,

Corollary 2.8 There exists a constant $C > 0$ depending on $I(a)$ and $K$, such that the following holds. Let $x_1, x_2 \in M[a]$ be points of order $a$ for which $\langle x_1 \rangle \cap \langle x_2 \rangle = \{0\}$. Then
\[
[K(x_1) \cap K(x_2) : K] \leq C \theta(a).
\]

2.3 Proof of Theorem 2.1

Proof of Theorem 2.1 Let $H = M_{\text{tor}}(L)$, which is finite since we assume that the indices $I(a)$ are bounded. Let $a \subset A$ be the minimal ideal for which $H \subset M[a]$. One can choose a basis $x_1, \ldots, x_r$ of $M[a] \cong (A/a)^r$ such that $H = \langle y_1, \ldots, y_r \rangle$, with $y_i \in \langle x_i \rangle$, and $y_i$ is of order $a_i$, for each $i = 1, \ldots, r$. Then $K(H)$ is the compositum of the $K(y_i)$’s in $L$.

From Lemma 2.4, Proposition 2.7 and Lemma 2.2 we obtain
\[
\prod_{i=1}^{r} [K(y_i) : K] \leq \prod_{i=1}^{r} [K(x_i) : K] \leq C_1 \theta(a) \leq C_2 \log \log |a|,
\]
for some constant $C_2$ independent of $H$. From Proposition 2.6 now follows that
\[
[K(H) : K] \geq \frac{\prod_{i=1}^{r} [K(y_i) : K]}{C_2 \log \log |a|} \quad \text{(or } [K(y_1) : K] \text{ if } r = 1) \]
\[
\geq \frac{1}{I(a)^r \zeta_A(r)^r C_2 \log \log |a|} \quad \text{(or } \frac{1}{I(a)} \frac{|a_1|}{C_2 \log \log |a|} \text{ if } r = 1) \]
\[
\geq C_2 \frac{|H|^r}{\log \log |H|}.
\]
where $C_2$ is independent of $H$, by the assumption on $I(a)$.

It follows that $|H| \leq C_3([K(H) : K] \log \log [K(H) : K])^{1/r}$, which proves part (II).

If $H = M[p^\infty](L)$, then in the above argument we find that $a = p^n$ for some $n$, and $	heta(p^n) = (1 - |p|^{-1})^{-1}$ only depends on $p$, so the log log-term falls away. Part (I) follows.

Lastly, we show that the bounds are sharp. In case (II), let $a_n := \prod_{|p| \leq n} p$ for $n \in \mathbb{N}$, as in Lemma 2.2. Now set $L_n := K(M[a_n])$. By Lemmas 2.5 and 2.3,

$$[L_n : K] = \frac{1}{I(a_n)}|GL_r(A/a_n)| = \frac{1}{I(a_n)}|a_n|^{r^2} \prod_{p|a_n} \left(1 - \frac{1}{|p|}\right) \left(1 - \frac{1}{|p|^r}\right) \cdots \left(1 - \frac{1}{|p|^r}\right).$$

It follows that

$$|M_{\text{tor}}(L_n)| \geq |M(a_n)| = |a_n|^r \geq C_2([L_n : K] \log \log [L_n : K])^{1/r}.$$

Case (I) is similar: We let $a_n := p^n$ and $L_n := K(M[p^n])$. This time $\theta(p^n)$ is constant and we find

$$|M[p^\infty](L_n)| \geq |M[p^n]| = |p^n|^r \geq C_2[L_n : K]^{1/r}.$$

$\square$

3 Proof of the main result

3.1 Drinfeld modules

Suppose that $k$ is a global function field, and fix a place $\infty$ of $k$. Let $A$ be the ring of elements of $k$ regular away from $\infty$, and let $\varphi$ be a Drinfeld $A$-module of rank $r$ in generic characteristic defined over the finitely generated field $K$. We denote by $\text{End}_L(\varphi)$ the ring of endomorphisms of $\varphi$ defined over a field $L/K$. See [3] Chapter 4] for basic facts about Drinfeld modules.

Proof of Theorem 1.1(b).

We first reduce to the case where $\text{End}_K(\varphi) = A$. Replacing $K$ by a finite extension if necessary, we may assume that $\text{End}_K(\varphi) = \text{End}_K(\varphi)$. Let $R = \text{End}_K(\varphi)$, then since $\varphi$ has generic characteristic, $R$ is an order in a purely imaginary extension $k'/k$, i.e. $k'$ has only one place above $\infty$. Furthermore, $[k' : k]$ divides $r$. Denote by $A'$ the integral closure of $A$ in $k'$.

By [3] Prop 4.7.19] there exists a Drinfeld $A$-module $\psi$ and an isogeny $P : \varphi \to \psi$, defined over $K$, such that $\text{End}_K(\psi) = A'$. Now $P$ induces a morphism $\varphi_{\text{tor}}(L) \to \psi_{\text{tor}}(L)$, and the dual isogeny $\tilde{P}$ likewise induces a morphism $\psi_{\text{tor}}(L) \to \varphi_{\text{tor}}(L)$, of degree independent of $L$. Hence

$$c_1|\psi_{\text{tor}}(L)| \leq |\varphi_{\text{tor}}(L)| \leq c_2|\psi_{\text{tor}}(L)|$$

for constants $c_1, c_2 > 0$ independent of $L$.

Now $\psi$ may be extended to a Drinfeld $A'$-module of rank $r' = r/[A' : A]$, which we denote by $\psi'$. We claim that $\psi_{\text{tor}}(L) = \psi'_{\text{tor}}(L)$. Let $c \in A'$, then $\psi'_c \in \text{End}_K(\psi)$, and $\psi'_c \circ \psi'_d = \psi'_{cd}$ for some $d \in A$, where $\psi'_c$ denotes the dual of $\psi'_c$ as an isogeny. Hence $\ker(\psi'_c) \subset \ker(\psi'_d)$ and so $\psi'_{\text{tor}}(L) \subset \psi_{\text{tor}}(L)$. The other inclusion is obvious.

Thus it suffices to prove Theorem 1.1(b) with $(\varphi, A, r, \gamma)$ replaced by $(\psi', A', r', 1/r')$. The result now follows from Theorem 2.1 together with the following important result of Pink and Rütsche [13]:

6
Theorem 3.1 (Pink-Rütsche) Let $\varphi$ be a rank $r$ Drinfeld $A$-module in generic characteristic, defined over the finitely generated field $K$. Suppose that $\text{End}_K(\varphi) = \text{End}_K(\varphi) = A$. Then there exists a constant $C_0$ depending on $\varphi$ and on $K$, such that such that the index $I(\mathfrak{a})$ of the image of the Galois representation on $\varphi[\mathfrak{a}] \cong (A/\mathfrak{a})^r$ is bounded by $C_0$ for all $\mathfrak{a} \subset A$.

\[ \square \]

3.2 Elliptic curves

Let $K$ be a finitely generated field of characteristic zero, and $E/K$ an elliptic curve. For a field $L/K$ we denote by $\text{End}_L(E)$ the ring of endomorphisms of $E$ defined over $L$.

**Proof of Theorem 1.1(a).**

Suppose that $E$ does not have complex multiplication. Then $E$ is a rank 2 $(G_K, \mathbb{Z})$-module, and the result follows from Theorem 2.1 with $A = \mathbb{Z}$ and $r = 2$ once we have established

**Theorem 3.2 (Serre)** Suppose $E/K$ is an elliptic curve without complex multiplication, defined over a finitely generated field $K$ of characteristic zero. Then there exists a constant $C_0$, depending on $E$ and on $K$, such that the index $I(n)$ of the image of the Galois representation on $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ is bounded by $C_0$ for all $n \in \mathbb{Z}$.

**Proof.** Let $j$ denote the $j$-invariant of $E$ and let $K_1 = \mathbb{Q}(j)$. Then by [20, §III, Prop 1.4] there exists an elliptic curve $E'/K_1$ with $j(E') = j$ which becomes isomorphic to $E$ over a finite extension of $K$. It suffices to prove Theorem 3.2 with $E$ replaced by $E'$.

The result holds for $K_1$, in the sense that the cokernel of $\rho_n : \text{Gal}(K_1^{\text{sep}}/K_1) \to \text{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is bounded independently of $n$. Indeed, if $K_1$ is a number field then this is Serre’s celebrated Open Image Theorem [18], whereas if $j$ is transcendental then the result follows by an older result of Weber [8, p68].

Now let $K_1 \subset K_2 \subset K$ such that $K_2/K_1$ is purely transcendental and $K/K_2$ is finite. The result also holds for $K_2$ since $\text{Gal}(K_2^{\text{sep}}/K_2) \cong \text{Gal}(K_1^{\text{sep}}/K_1)$. As $\text{Gal}(K^{\text{sep}}/K)$ is a subgroup of index $[K : K_2]$ in $\text{Gal}(K_2^{\text{sep}}/K_2)$, it follows that the result also holds for $K$.

Next, suppose that $E$ has complex multiplications by an order in the quadratic imaginary field $k/\mathbb{Q}$. After replacing $K$ by a finite extension and $E$ by a $K$-isogenous elliptic curve if necessary, we may assume that $\text{End}_K(E) = \text{End}_K(E) = A$ is the maximal order in $k$. Now $E$ is a rank 1 $(G_K, A)$-module, and for any finite extension $L/K$ the torsion points in $E(L)$ with respect to the $A$-module structure coincide with the usual torsion points. Again, the result follows from Theorem 2.1 with $r = 1$ together with the following consequence of CM theory.

**Theorem 3.3 (CM)** Suppose $E/K$ is an elliptic curve defined over a finitely generated field $K$ of characteristic zero. Suppose that $\text{End}_K(E) = \text{End}_K(E) = A$ is the maximal order in a quadratic imaginary field $k$. Then there exists a constant $C_0$, depending on $E$ and on $K$, such that the index $I(\mathfrak{a})$ of the image of the Galois representation on $E[\mathfrak{a}] \cong A/\mathfrak{a}$ is bounded by $C_0$ for all $\mathfrak{a} \subset A$.

**Proof.** As before, let $j$ denote the $j$-invariant of $E$, and set $K_1 = \mathbb{Q}(j)$. Since $E$ has complex multiplication, $K_1$ is a number field and the result holds for $K_1$ by [18, §4.5]. The result now extends to $K$ as in the proof of Theorem 3.2.

\[ \square \]
4 Discussion

When $M$ is an elliptic curve with complex multiplication, then the lower bound in Theorem 1.1 improves the bound $|M_{\text{tor}}(L)| \geq C[L : K] \sqrt{\log \log [L : K]}$ (for suitable fields $L$) often encountered in the literature (e.g. [1, 2]).

4.1 Other applications of Galois modules

Applying Theorem 2.1 to the rank 1 $(G_{\mathbb{Q}}, \mathbb{Z})$-module $M = G_{\mathbb{Q}}$, we get the well known result that the number of roots of unity in a number field $L/\mathbb{Q}$ is bounded by $C[L : \mathbb{Q}] \log \log [L : \mathbb{Q}]$, for an absolute constant $C > 0$.

One may also bound the orders of $\text{Gal}(K^{\text{sep}}/L)$-stable submodules (equivalently, degrees of $L$-rational isogenies) of elliptic curves or Drinfeld modules.

**Proposition 4.1** Let $M$ be a $(G_K, A)$-module of rank $r \geq 2$. Let $L/K$ be a finite extension and $H \subset M$ a $\text{Gal}(K^{\text{sep}}/L)$-stable cyclic submodule of order $a \subset A$, i.e. $H \cong A/a$. Then

$$|H| = |a| \leq C[L : K]^{1/(r-1)},$$

where the constant $C$ depends on $M, K, r$ and the index $I(a)$, but not on $L$.

**Proof.** One shows, as in Proposition 2.6, that the stabilizer of $H$ in $\text{Aut}(M[a])$ has order

$$|\text{Stab}_{\text{Aut}(M[a])}(H)| = |(A/a)\times| \cdot |a|^{r-1} \cdot |\text{GL}_{r-1}(A/a)|$$

$$= |a|^{r^2-r+1} \prod_{p | a} \left( 1 - \frac{1}{|p|} \right) \left( 1 - \frac{1}{|p|^2} \right) \cdots \left( 1 - \frac{1}{|p|^{r-1}} \right)$$

and hence

$$[K(H) : K] \leq \frac{1}{I(a)} \frac{|\text{GL}_r(A/a)|}{|\text{Stab}_{\text{Aut}(M[a])}(H)|}$$

$$\geq \frac{\zeta_A(r)}{I(a)} |a|^{r-1}.$$  

The result follows. \qed

**Corollary 4.2** Suppose $M$ is an elliptic curve without complex multiplication defined over a finitely generated field $K$ of characteristic zero, or that $M$ is a Drinfeld $A$-module of rank $r \geq 2$ in generic characteristic with $\text{End}_{\mathbb{F}}(M) = A$, defined over the finitely generated field $K$. Then there exists a constant $C > 0$, depending on $M, K$ and $r$ such that, for any finite extension $L/K$, the degree of any $L$-rational cyclic isogeny $M \to M'$ is bounded by $C[L : K]^{1/(r-1)}$, (where $r = 2$ if $M$ is an elliptic curve). \qed
4.2 Uniform bounds

One may ask if the constants in Theorem 1.1 may be chosen independently of $M$ (this would follow from a uniform bound on $I(a)$).

When $M$ is a Drinfeld module of rank 1 this was shown by Poonen [14, Theorem 8]. For Drinfeld modules of higher rank the existence of an upper bound on $|M_{\text{tor}}(L)|$ depending only on $r$, $A$ and $[L : K]$ is conjectured by Poonen [loc. cit.], though there are various partial results, typically with the upper bound depending on primes of bad reduction, see for example [2 14 17].

When $E$ is an elliptic curve over a number field $K$, uniform upper bounds on $|E_{\text{tor}}(L)|$ do exist, as shown by Mazur, Kamienny and Merel [7 11 12], but these bounds are not yet known to be polynomial in the degree $[L : K]$ in general. When $E$ has everywhere good reduction, then we have the explicit bound $|E_{\text{tor}}(L)| \leq 1977408[L : \mathbb{Q}] \log[L : \mathbb{Q}]$, due to Hindry and Silverman, [9].

If $E$ is an elliptic curve with complex multiplication defined over a number field, one may translate Poonen’s proof of [14, Theorem 8] from rank 1 Drinfeld modules to the rank 1 $(G_K, \text{End}(E))$-module $E$, and one obtains

$$|E_{\text{tor}}(L)| \leq C[L : \mathbb{Q}] \log \log[L : \mathbb{Q}],$$

where the constant $C$ depends only on the endomorphism ring $\text{End}(E)$. On the other hand, it follows from [15 19] that the exponent of the group $E_{\text{tor}}(L)$ is bounded by $C[L : \mathbb{Q}] \log \log[L : \mathbb{Q}]$ for an absolute constant $C$.

4.3 Abelian varieties

Suppose $M$ is an abelian variety of dimension $g$ defined over a number field $K$. Masser has shown that $|M_{\text{tor}}(L)| \leq C([L : K] \log[L : K])^g$, see [9 10]. The exponent $g$ is not optimal in general.

The key to our approach is the independence of fields generated by linearly independent torsion points (Proposition 2.7), which holds because

$$r \cdot \text{codim} \text{Fix}_G(x) = \dim G,$$

when $G = \text{GL}_r$.

For abelian varieties, the image of Galois is contained in the Mumford-Tate group, which is an algebraic subgroup of $\text{GSp}_{2g}$. This suggests developing a theory of “symplectic” Galois modules. However, as $\dim \text{GSp}_{2g} = 2g^2 + g + 1$ does not factorize, an identity of the form (4) is not possible. This means that one must explicitly estimate the order of $\text{Fix}_G(A/a)(H)$ for submodules $H \subset M_{\text{tor}}$, which requires more effort. This is done by Hindry and Ratazzi [11 15], allowing them to obtain the optimal exponent $\gamma$ for which $|M_{\text{tor}}(L)| \leq C_{\varepsilon}[L : K]^\gamma + \varepsilon$ holds in various cases (here the constant $C_{\varepsilon}$ depends on $\varepsilon > 0$).

Acknowledgements. The seed for this article was sown in discussions with Marc Hindry and Amilcar Pacheco at the XX Escola de Álgebra in Rio de Janeiro.
References

[1] P. L. Clark and X. Xarles, Local bounds for torsion points on abelian varieties. *Canad. J. Math.* 60 (2008), no. 3, 532–555.

[2] D. Ghioca, The Lehmer inequality and the Mordell-Weil theorem for Drinfeld modules. *J. Number Theory* 122 (2007), no. 1, 37–68.

[3] D. Goss, *Basic Structures in Function Field Arithmetic*, Springer-Verlag, 1998.

[4] M. Hindry and N. Ratazzi, Torsion dans un produit de courbes elliptiques. arXiv:0804.3031v1 [math.NT], (2008).

[5] M. Hindry and N. Ratazzi, Points de torsion sur les variétés abéliennes de type GSp$_{2g}$. Manuscript, 2008.

[6] M. Hindry and J. H. Silverman, Sur le nombre de points de torsion rationnels sur une courbe elliptique, *C. R. Acad. Sci. Paris, Série I*, 329 (1999) 97–100.

[7] S. Kamienny, Torsion points on elliptic curves and $q$-coefficients of modular forms, *Invent Math.* 109 (1992) 221–229.

[8] S. Lang, *Elliptic functions, 2nd Edition*, GTM 112, Springer Verlag, 1987.

[9] D. Masser, Counting points of small height on elliptic curves, *Bull. Soc. Math. France* 117 (1989), 247–265.

[10] D. Masser, Letter to Daniel Bertrand of 10 November 1986.

[11] B. Mazur, Modular curves and the Eisenstein ideal, *Pub. Math. IHES* 47 (1978), 33–186.

[12] L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.* 124 (1996), no. 1-3, 437–449.

[13] R. Pink and E. Rütsche, Adelic openness for Drinfeld modules in generic characteristic. Preprint, 2008.

[14] B. Poonen, Torsion in rank 1 Drinfeld modules and the uniform boundedness conjecture. *Math. Ann.* 308, 571–586 (1997).

[15] D. Prasad and C. S. Yogananda, Bounding the torsion in CM elliptic curves. *C. R. Math. Acad. Sci. Soc. R. Can.* 23 (2001), no. 1, 1–5.

[16] M. Rosen, A generalization of Mertens’ Theorem. *J. Ramanujan Math. Soc.* 14 (1999), no. 1, 1–19.

[17] A. Schweizer, Torsion of Drinfeld modules and gonality. *Forum Math.* 16 (2004), 925–941.

[18] J.-P. Serre, Propriétés galoisiennes des points d’ordre fini des courbes elliptiques, *Invent. Math.* 15 (1972), 259-331.

[19] A. Silverberg, Torsion points on abelian varieties of CM-type. *Compositio Math.* 68 (1988), no. 3, 241–249.

[20] J. H. Silverman, *The arithmetic of elliptic curves*, GTM 106, Springer-Verlag, 1986.