Math. Proc. Camb. Phil. Soc. (2015), **159**, 275–302 © *Cambridge Philosophical Society* 2015
doi:10.1017/S0305004115000353
First published online 30 June 2015

Primitive submodules for Drinfeld modules

BY WENTANG KUO†

Department of Pure Mathematics, University of Waterloo,
Waterloo, Ontario N2L 3G1, Canada.
e-mail: wtkuo@uwaterloo.ca

AND DAVID TWEEDLE

Department of Mathematics and Statistics, University of The West Indies,
St. Augustine, Trinidad and Tobago, West Indies.
e-mail: david.tweedle@sta.uwi.edu

(*Received* 1 *April* 2014; *Revised* 1 *May* 2015)

Abstract

The ring $A = \mathbb{F}_r[T]$ and its fraction field k, where r is a power of a prime p, are considered as analogues of the integers and rational numbers respectively. Let K/k be a finite extension and let ϕ be a Drinfeld A-module over K of rank d and $\Gamma \subset K$ be a finitely generated free A-submodule of K, the A-module structure coming from the action of ϕ. We consider the problem of determining the number of primes $\wp$ of K for which the reduction of Γ modulo $\wp$ is equal to $\mathbb{F}_\wp$ (the residue field of the prime $\wp$). We can show that there is a natural density of primes $\wp$ for which Γ mod $\wp$ is equal to $\mathbb{F}_\wp$. In certain cases, this density can be seen to be positive.

1. *Introduction*

In [**17**], Lang and Trotter formulated an analogue of Artin's conjecture for elliptic curves. They proposed that for a given elliptic curve E defined over the rationals, and rational point $a \in E(\mathbb{Q})$, the set of primes p for which the reduction of a modulo p generates the group $E(\mathbb{F}_p)$ has a natural density.

For a finite set X, we use the notation $|X|$ to denote the number of elements of X.

Lang and Trotter examine the behaviour of Frob$_p$ (recall that this is the conjugacy class which corresponds to the Frobenius morphism acting on the residue field extension) in extensions $L_m = \mathbb{Q}(E[m], m^{-1}a)$, where m is a square-free positive integer, $m^{-1}a$ is a particular solution of $[m]y = a$ and $E[m]$ is the set of all m-torsion points in $E(\mathbb{C})$. They determine a conjugacy class $\mathcal{C}_m \subset \mathrm{Gal}\,(L_m/\mathbb{Q})$ such that if E has good reduction at p then m divides the index $[E(\mathbb{F}_p) : \langle\overline{a}\rangle]$ if and only if Frob$_p \in \mathcal{C}_m$. A heuristic argument using the Chebotarev density theorem suggests that the natural density of the set of primes p for which the reduction of a modulo p generates $E(\mathbb{F}_p)$ is given by the (absolutely convergent)

† Supported by an NSERC discovery grant.

sum

$$\sum_{m=1}^{\infty} \frac{\mu(m)\,|\mathcal{C}_m|}{[L_m : \mathbb{Q}]}.$$

Lang and Trotter also had the foresight to develop a similar condition for the problem of determining when a subgroup Γ of rational points of E reduced modulo p generates $E(\mathbb{F}_p)$. This problem seems to be more tractable. In particular, we have the following result of Gupta and Murty.

THEOREM 1 ([**10**, theorem 3]). *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication, and let $\Gamma \subset E(\mathbb{Q})$ be a free subgroup with* $\operatorname{rank}(\Gamma) \geqslant 18$. *Let $M_\Gamma(x)$ denote the number of primes less than or equal to x such that the reduction of Γ modulo p equals $E(\mathbb{F}_p)$. If we assume the generalized Riemann hypothesis for the fields $L_q = \mathbb{Q}(E[q], q^{-1}\Gamma)$, then there is a constant $C_E(\Gamma)$ such that*

$$M_\Gamma(x) = C_E(\Gamma)\frac{x}{\log x} + \mathbf{o}\left(\frac{x}{\log x}\right).$$

If E has complex multiplication, then the above result applies as long as $\operatorname{rank}(\Gamma) \geqslant 10$.

We now attempt to give a brief account of more recent results. In 2005, Chen and Yu in [**5**] extended the positive density results of [**10**] to include the possibility that the complex multiplication is given by a non-maximal order. In 2010, Akbary, Ghioca and V.K. Murty proved in [**2**] that the set of primes for which the index of the reduction of a free subgroup Γ is less than $1/\nu(p)$ has density one as long as $\nu(x) \to \infty$ and the rank of Γ is large enough. There have been some developments for the Lang–Trotter conjecture over function fields as well. In 2006, Hall and Voloch gave a partial result in [**12**] towards the Lang–Trotter conjecture for elliptic curves over function fields. Finally, in 2009, Akbary and Ghioca proved in [**1**] that the set of primes for which the reduction of Γ is less than $|\mathbb{F}_\wp|^\gamma$ has density zero, where Γ is an A-submodule of a Drinfeld module, and γ is chosen appropriately based on the rank of the Drinfeld module and the rank of Γ.

Our goal is to use this strategy to prove results for Drinfeld modules without any extra assumption. We obtain a very broad result where the influence of Gupta and Murty is clear, and yet it goes beyond what we would expect.

We must introduce some notation at this point to state our main theorem. We leave the definitions of all the terms until Section 2. The Drinfeld module $\phi : A \to K\{\tau\}$ is of generic characteristic and rank d, where $A = \mathbb{F}_r[T]$ and K is a finite extension of the field $k = \mathbb{F}_r(T)$. The ring of endomorphisms is denoted $\operatorname{End}(\phi)$ and can be used to define a Drinfeld module $\psi : \operatorname{End}(\phi) \to K'\{\tau\}$ of rank $\tilde{d}$. The integer r^* is determined by the constant field behaviour of certain fields M_s, where s is a square-free element of A. If all of the extensions M_s are geometric extensions of K, then we can take $r^* = 1$. The set Γ is an A-submodule of K freely generated by t elements which are also linearly independent over $\operatorname{End}(\phi)$. Finally, $N_\Gamma(x)$ is the number of finite primes $\wp$ of K of degree x such that Γ modulo $\wp$ is equal to $\phi(\mathbb{F}_\wp)$.

THEOREM 2. *Suppose that* $t = \operatorname{rank}(\Gamma) \geqslant 2d^2\tilde{d} + 2d^2 - 3d$. *Let $i \in \{0, 1, 2, \ldots, r^* - 1\}$, then there exists a constant $C_{\phi,\Gamma}(i)$ such that as $x \equiv i \pmod{r^*}$, we have*

$$N_\Gamma(x) = C_{\phi,\Gamma}(i)\frac{r^x}{x} + \mathbf{O}\left(\frac{r^x \log x}{x^2}\right).$$

If we put in $d = 1$, we see that Theorem 2 is a weaker, but slightly more general version of [**14**, theorem 4·2]. If we have $d = 2$, and assume that $\mathrm{End}(\phi) = A$, Theorem 2 requires that $\mathrm{rank}(\Gamma) \geqslant 18$ just as in Gupta and Murty's result [**10**, theorem 3]. If $d = 2$ but $\mathrm{End}(\phi) \neq A$ then Theorem 2 requires that $\mathrm{rank}(\Gamma) \geqslant 10$, again just as [**10**, theorem 3]. The restriction that Γ be an $\mathbb{F}_r[T]$-submodule of K is made to overcome technical difficulties. In the case that the endomorphism ring is non-trivial, we require that the generators of Γ be linearly independent over $\mathrm{End}(\phi)$ to allow us to exploit the additional structure that $\mathrm{End}(\phi)$ gives us. More specifically, as in [**13**], we can turn the action of $\mathrm{End}(\phi)$ into a Drinfeld module if we are careful. This new Drinfeld module extends the action of ϕ and gives us a more complete picture of the Kummer extensions. To be completely clear, we use this extra action of $\mathrm{End}(\phi)$ as a tool, our techniques are not enough to study the case when Γ is an $\mathrm{End}(\phi)$-submodule.

Let us consider some of the technical difficulties involved when Γ is an A-submodule of K but $A \neq \mathbb{F}_r[T]$. In order to calculate the Kummer theory we would need to use [**21**], which brings with it a lot of overhead calculations. On the other hand, we use [**1**, proposition 5·1] for some tail end estimates and it only applies in the case that $A = \mathbb{F}_r[T]$ and if we apply the proposition when Γ is an A-module for more general A, then the rank of Γ increases depending on our choice of subring $\mathbb{F}_r[T] \subseteq A$. Finally, our calculations of the discriminant of the Kummer extensions rely on [**8**] which again only applies for $\mathbb{F}_r[T]$. In order to generalise our theorem properly, these three obstacles must be overcome.

In order to prove Theorem 2, first we fix our notation once and for all in Section 2. We need to then calculate the discriminants of the Kummer extensions, which we use when applying the Chebotarev density theorem. We also need some algebraic facts for the calculation of the Galois groups of the Kummer extensions. These calculations are both done in Section 3 with the assistance of [**8**].

Our next step will be to revisit the paper [**17**] of Lang and Trotter. Given $s \in A$ square-free, we will study the extensions $M_s = K(\phi[s], \alpha_1, \ldots, \alpha_t)$, where $\phi_s(\alpha_i) = a_i$. In particular, we need to determine a conjugacy class $\mathcal{C}_s \subset \mathrm{Gal}(M_s/k)$ such that if ϕ has good reduction at a prime $\wp$ then s divides the index $[\phi(\mathbb{F}_\wp) : \Gamma_\wp]$ if and only if $\mathrm{Frob}_\wp \in \mathcal{C}_s$. In Section 4 we accomplish this.

In order to determine the degree of the extensions M_s/K, we must investigate the structure of $\mathrm{Gal}(M_s/K)$. We may hope that

$$\mathrm{Gal}(M_s/K) \cong \prod_{q|s} \mathrm{Gal}(M_q/K).$$

Although, this fact is unreasonable to expect in general, if s is coprime to some fixed $M \in A$, we are able to obtain the above decomposition, except that in the case that $\mathrm{End}(\phi) \neq A$, we may need to replace K by a separable extension K' of K such that every endomorphism of ϕ is defined over K' (such an extension is guaranteed by [**9**, theorem 4·7·8]). As in the elliptic curve case, we can see that

$$\mathrm{Gal}(M_q/K) \hookrightarrow \mathrm{GL}_d(A/q) \rtimes \phi[q]^t,$$

or in the case that $\mathrm{End}(\phi) = \mathcal{O}$, and $\psi : \mathcal{O} \to K'\{\tau\}$ is the Drinfeld module corresponding to $\mathrm{End}(\phi)$ having rank $\tilde{d}$,

$$\mathrm{Gal}(M_q K'/K') \hookrightarrow \mathrm{GL}_{\tilde{d}}(\mathcal{O}/q\mathcal{O}) \rtimes \phi[q]^t.$$

In Section 5, we prove that the above map is bijective as long as $\deg q$ is large enough. This requires going back to the papers [**4**] of Bašmakov and [**23**] and [**24**] of Ribet, and retooling their results for Drinfeld modules. It should be noted that Anly Li has done this in [**19**] for the case that ϕ is completely singular (i.e. ϕ has complex multiplication by a rank 1 Drinfeld module), and in his Master's thesis [**11**], Simon Häberli has proved a stronger result in line with Ribet's work in [**24**]. Finally, Richard Pink has extended these results in [**21**]. The result we need is somewhat simpler, in line with Ribet's earlier work [**23**], it is proved in Section 5.

Since our eventual goal is to apply an effective version of the Chebotarev density theorem, it remains to bound the degree $n(s)$ of M_s over K and the ratio $|\mathcal{C}_s|/n(s)$ where $\mathcal{C}_s$ is the conjugacy class corresponding to the Lang–Trotter condition. The bounding of the size of the conjugacy classes and the degree of the extensions are handled in Section 6.

We are then able to follow through the work of Gupta and Murty sufficiently well to complete estimates necessary to conclude Theorem 2. This is done in Section 7. We conclude with a breakdown of constants $C_{\phi,\Gamma}(i)$. We show that either at least one of the constants $C_{\phi,\Gamma}(i)$ is positive for some i, or $N_\Gamma(x) \ll 1$. This is done in section Section 8.

In adapting the work of Gupta and Murty to the case of Drinfeld modules, there are several main difficulties. Gupta and Murty's result is for elliptic curves defined over $\mathbb{Q}$ only, whereas our result is for Drinfeld modules defined over a more general class of function fields than just $k = \mathbb{F}_r(T)$ (the function field analogue to $\mathbb{Q}$). Also, in the elliptic curve case, there are two possibilities: either the elliptic curve has complex multiplication or it does not. These cases correspond to the case that $d = 2$, $\tilde{d} = 2$ and $h = 1$ and $d = 2$, $\tilde{d} = 1$ and $h = 2$. The cases that can occur for our result are more diverse, and we obtain a meaningful result for every possibility. Therefore, we had to be very careful to obtain a Lang–Trotter condition for these cases and, once this was done, the resulting conjugacy classes had to be calculated. Furthermore, we had to find the Galois groups of the extensions M_s/K. Another difficulty is that the question of natural density is complicated by two things: the existence of non-geometric field extensions and large conjugacy classes. It seems that a small increase of the complexity of the conjugacy classes can make it difficult to understand the resulting density. Therefore, it seems unreasonable at this point to obtain a strong and broad theorem which can tell you which Drinfeld modules will yield a positive density, and which choices will have obstructions.

A few words are in order about the case of Artin's conjecture for T-modules. Briefly, a T-module is a homomorphism

$$\Phi : A \longrightarrow \mathrm{End}\,(k^n)\{\tau\},$$

where $k = \mathbb{F}_r(T)$ and

$$\Phi_T = (T \cdot I + N)\tau^0 + \eta(\tau) \cdot \tau,$$

where N is a nilpotent matrix, and $\eta(\tau)$ is a non-zero polynomial with matrix coefficients.

The positive integer n is called the dimension of the T-module, and if $n = 1$ we recover a Drinfeld module as long as $\phi_T \neq T \cdot \tau$. To generalise this paper to the case of T-modules, we need to consider the images of Galois groups for division fields and Kummer extensions, the Kummer theory calculations, the discriminant calculations and other details. If we assume that all the calculations on division fields and Kummer extensions work, then our result can be extended to T-modules. However, it is not true.

For example, consider the simplest T-module, the nth tensor power of the Carlitz module, denoted $C^{\otimes n}$. This is a T-module defined by

$$C_T^{\otimes n} = (T \cdot I + N)\tau^0 + E\tau,$$

where

$$N = \begin{bmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 \\ 0 & \cdots & \cdots & 0 \end{bmatrix}, E = \begin{bmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ 1 & \cdots & \cdots & 0 \end{bmatrix}.$$

But it is known that the representation

$$\mathrm{Gal}\,(k^{\mathrm{sep}}/k) \longrightarrow (A/qA)^{\times},$$

$$\sigma \longrightarrow \{\lambda \to \sigma(\lambda), \lambda \in \Phi[q]\},$$

is the nth power of the analogous representation for the Carlitz module. So even in this simplest of cases, it is not true that the above representation is onto for *most* q, (see [**3**, proposition 1·11·1]). In the Carlitz module case, the representation is onto for every q, and indeed by Pink's result [**21**], the result generalises. But if this representation is not onto, we lose a key stepping stone in the Kummer theory. Therefore, before generalisation, we must make explicit calculations in the case of the nth power of the Carlitz module, so that we can see what should be true.

Another obstruction to a generalisation to T-modules is a technical one - the calculation of the different of the Kummer extensions. In calculating discriminants or differents, it is useful to describe the field extension as the splitting field of an appropriate polynomial, and then standard techniques allow us to calculate bounds for the different exponent. But the torsion points of a T-module are not so simply described as for Drinfeld modules. These fields are described by a multi-variable system of (non-linear) equations. We cannot just calculate the norm of an appropriate element as in the one-variable situation. In order to resolve this, we might need to develop a new method to deal with the multi-variable cases.

2. *Notation*

Let us define some notation to be used for the rest of the paper. Let $A = \mathbb{F}_r[T]$ and $k = \mathbb{F}_r(T)$. A *prime* q of A is a monic, irreducible polynomial of A. The *degree* of an element of A is the usual polynomial degree. Let K be a finite extension of k. A *place* $\wp$ of K is a local ring $\mathfrak{o}_\wp \subset K$ paired with a maximal ideal $\mathfrak{m}_\wp \subset \mathfrak{o}_\wp$, such that the fraction field of $\mathfrak{o}_\wp$ is K and $\mathfrak{m}_\wp$ is principal. There is a valuation associated to $\wp$, denoted by $v_\wp$. A place $\wp$ that lies over the infinite place of k, is called an infinite place, and all other places are called finite. A finite place of K is also called a prime of K. In this paper, all degrees will be relative to $\mathbb{F}_r$ so that the degree of a prime of K is $\deg \wp = [\mathfrak{o}_\wp/\mathfrak{m}_\wp : \mathbb{F}_r]$. A *divisor* D of K is a finite formal sum over the places of K,

$$D = \sum_\wp v_\wp(D) \cdot \wp,$$

where $v_\wp(D) \in \mathbb{Z}$ for each place $\wp$ of K and $v_\wp(D) = 0$ for all places $\wp$ except for finitely many. The degree of such a divisor is

$$\deg D = \sum_\wp v_\wp(D) \deg \wp.$$

A field extension K'/K is *geometric* if it is algebraic and $K' \cap \overline{\mathbb{F}}_r = \mathbb{F}_r$, where $\overline{\mathbb{F}}_r$ is the algebraic closure of $\mathbb{F}_r$ inside a fixed algebraic closure $\overline{K}$ of K.

Let ϕ be a Drinfeld A-module of rank d defined over a finite extension K of k and assume that ϕ is of generic characteristic. More concretely, we may define ϕ by saying that ϕ is an $\mathbb{F}_r$-algebra homomorphism from A to $K\{\tau\}$ defined by

$$\phi_T = a_{d,T} \cdot \tau^d + \cdots + a_{1,T} \cdot \tau + T \cdot \tau^0,$$

where $a_{d,T}, \ldots, a_{1,T} \in K$, and $a_{d,T} \neq 0$. Here, τ refers to the rth power Frobenius map, and $K\{\tau\}$ to the non-commutative ring generated by τ with the relation $\tau w = w^r \tau$ for $w \in K$.

An endomorphism of ϕ is a polynomial $\rho \in \overline{K}\{\tau\}$, where $\overline{K}$ is a fixed algebraic closure of K, such that

$$\phi_z \circ \rho = \rho \circ \phi_z,$$

for all $z \in A$. Denote the set of all endomorphisms by $\mathrm{End}\,(\phi)$. Then A can be viewed as a subset of $\mathrm{End}\,(\phi)$.

For $a \in A$, define the a-torsion of ϕ to be all the elements $\alpha \in \overline{K}$ satisfying $\phi_a(\alpha) = 0$. We denote the set of a-torsion to be $\phi[a]$. If $\mathfrak{a}$ is an ideal of A, we can similarly set

$$\phi[\mathfrak{a}] = \bigcap_{a \in \mathfrak{a}} \phi[a].$$

Finally, if ρ is an endomorphism of ϕ then

$$\phi[\rho] = \{\alpha \in \overline{K} \text{ such that } \rho(\alpha) = 0\}.$$

It is known that $\mathrm{End}\,(\phi) \otimes_A k$ is a field extension of k, with degree dividing the rank of ϕ. Let $L = \mathrm{End}\,(\phi) \otimes_A k$, let $h = [L : k]$ and $d = \tilde{d} \cdot h$. Let $\mathcal{O} = \mathrm{End}\,(\phi)$ and recall that $\mathcal{O}$ is an order in L, and let $\psi : \mathcal{O} \to K'\{\tau\}$ be the Drinfeld $\mathcal{O}$-module induced by the endomorphism ring (see [**13**]), where K' can be taken to be a finite separable extension of K by [**9**, theorem 4·7·8].

Let Γ be a finitely generated, free A-submodule of $\phi(K)$ (see [**22**] for the structure of $\phi(K)$), and assume that Γ generates a free $\mathcal{O}$-submodule of $\psi(K')$ of the same rank as Γ. That is $\Gamma = \mathcal{A} \cdot \{a_1, \ldots, a_t\}$ and if

$$\psi_{b_1}(a_1) + \cdots + \psi_{b_t}(a_t) = 0,$$

for some $b_1, \ldots, b_t \in \mathcal{O}$ then

$$b_1 = b_2 = \cdots = b_t = 0.$$

For all but finitely many primes $\wp$ of K, we may reduce Γ modulo $\wp$ to obtain a submodule $\Gamma_\wp$ of the Drinfeld module $\phi(\mathbb{F}_\wp)$, where $\mathbb{F}_\wp$ is the residue field of K modulo $\wp$.

Let

$$N_\Gamma(x) = \left|\{\wp \text{ a prime of } K \,|\, \deg \wp = x, \Gamma_\wp = \phi(\mathbb{F}_\wp)\}\right|.$$

For each prime $q \in A$, let $M_q = K(\phi[q], \alpha_1, \ldots, \alpha_t)$, where $\phi_q(\alpha_i) = a_i$ for each $i = 1, \ldots, t$. We will show later that the degree of the constant field extensions of M_q/K can be bounded independently of q, therefore let r^* be the least common multiple of all the degrees of the constant field extensions of M_q over $\mathbb{F}_r$.

3. *Preliminary algebra*

In this section, we introduce the exponential functions associated to a Drinfeld module and use them to find bounds for the discriminant of the Kummer extensions. We will also prove some results which are algebraic in nature.

Our end goal is to use estimates based on the Chebotarev density theorem. To do this, we must know the degree of the extensions M_s/K, the size of the conjugacy classes $\mathcal{C}_s$, the ratio between these values, and finally, we must know the degree of the discriminant divisor associated to M_s. First, we will calculate the different divisor of the Kummer extensions. We use a localised approach, starting from [**8**]. For a comprehensive review see [**6**, **8**, **26**].

To find out the (possibly wild) ramification over various places, we must complete at the places in question, then use Drinfeld's uniformisation results. For a place $\wp$ of K, let $K_\wp$ be the completion of K at $\wp$, and $C_\wp$ be the completion of the algebraic closure of $K_\wp$ at $\wp$. Let $G_\wp$ be the group $\mathrm{Gal}\,(K_\wp^{\mathrm{sep}}/K_\wp)$. Recall that $n(s) = [M_s : K]$ and let $d(s)$ be the degree of the different divisor $\mathrm{Diff}\,(M_s/K)$ (see [**7**, section 3·6]) for $s \in A$ square-free.

THEOREM 3 ([**9**, theorem 4·6·9]). *For the infinite place $\wp$ of K corresponding to the valuation at ∞, there exists an entire $C_\wp$-homomorphism $e_\wp^\phi : C_\wp \to C_\wp$ defined over $K_\wp$ such that*

$$e_\wp^\phi(ax) = \phi_a(e_\wp^\phi(x))$$

for all $a \in A$ and $x \in C_\wp$. The kernel of $e_\wp^\phi$, $\Lambda_\wp$ is an A-lattice which is $G_\wp$-invariant in $C_\wp$ of rank d.

THEOREM 4 ([**6**, proposition 7·2]). *Let $\wp$ be a finite place of K such that the reduction of ϕ mod $\wp$ is rank $\overline{d}$. Then there exists an entire homomorphism $e_\wp^\phi : C_\wp \to C_\wp$ and a Drinfeld module ρ of rank $\overline{d}$ which has good reduction at $\wp$ such that*

$$e_\wp^\phi(\rho_a(x)) = \phi_a(e_\wp^\phi(x)).$$

Let $\Lambda_\wp = \ker(e_\wp^\phi)(C_\wp)$, then $\Lambda_\wp$ is an A-lattice invariant under $G_\wp$ of rank $d - \overline{d}$.

Denote by $(s)_0$ the divisor of K corresponding to the finite part of the divisor (s).

PROPOSITION 1 ([**8**, proposition 6]). *Let s be a non-constant element of A. Then there exists a divisor Δ_ϕ of K such that*

$$\mathrm{Diff}\,(K(\phi[s]), K) \leqslant t \cdot (s)_0 + \Delta_\phi$$

as divisors of $K(\phi[s])$ (for divisors D_1, D_2 of a field L, we say $D_1 \leqslant D_2$ if $v_\wp(D_1) \leqslant v_\wp(D_2)$ for every place $\wp$ of L).

LEMMA 1. *Let P be a non-torsion point, $\wp$ any place of K. Let Y_0 be a particular solution to $e_\wp^\phi(X) = P$. Then there exists a constant N_0, depending on ϕ, P, such that if $\wp = \infty$*

$$v_\wp(\mathrm{Diff}\,(K_\wp(\Lambda_\wp, Y_0))/K_\wp(\Lambda_\wp)) \leqslant N_0$$

and if $\wp$ is a finite place of bad reduction, then

$$v_\wp(\mathrm{Diff}\,(K_\wp(\Lambda_\wp, Y_0, \phi[a])/K_\wp(\Lambda_\wp, \phi[a]))) \leqslant N_0.$$

Proof. In both cases, we examine the Newton polygon of the function $e_\wp^\phi(X) - P$. The function $e_\wp^\phi$ is entire, thus so is $e_\wp^\phi - P$. By considering the different of each of the finitely many extensions considered above, each of which is finite, we get an upper bound for the different as required. An exact bound depends upon P and the coefficients of $e_\wp^\phi$.

If $\wp = \infty$, then we will proceed similar to [**15**].

Definition 1. We will define a divisor of K, denoted $\Delta_{\alpha,\phi}$ in the following way, by defining $v_\wp(\Delta_{\Gamma,\phi})$ depending on $\wp$ and Γ, where Γ is freely generated over A by t elements.

(i) If $\wp$ is an infinite place, let $v_{\wp}(\Delta_{\Gamma,\phi}) = t \cdot N_0$.

(ii) If $\wp$ is a finite place of K for which ϕ has good reduction at $\wp$, set $v_{\wp}(\Delta_{\Gamma,\phi}) = 0$.

(iii) If $\wp$ is a finite place of K for which ϕ has potential good reduction at $\wp$, set $v_{\wp}(\Delta_{\Gamma,\phi}) = 1$.

(iv) If $\wp$ is a place of M_s where ϕ has bad reduction, then set $v_{\wp}(\Delta_{\Gamma,\phi}) = t \cdot N_0 + 1$.

Definition 2. Let Δ_Γ be the divisor for which $v_{\wp}(\Delta_\Gamma) = \sum \max(0, -v_{\wp}(\alpha_i))$ where the sum is over the roots α_i of $\phi_s(X) - P_i$.

THEOREM 5. *The different of M_s over K satisfies*

$$\mathrm{Diff}\,(M_s/K) \leqslant \Delta_\phi + \Delta_{\phi,\Gamma} + d \cdot (s)_0 + t \cdot (s)_0 + d(\deg s) \cdot \Delta_\Gamma.$$

Thus the degree of the above divisor, denoted by $d(s)$ satisfies

$$d(s)/n(s) \ll (t+d) \cdot \deg s.$$

Proof. Write $\mathrm{Diff}\,(M_s/K) = \mathrm{Diff}\,(M_s/K(\phi[s])) + \mathrm{Diff}\,(K(\phi[s])/K)$, by [**26**, chapter III, section 4, proposition 8]. By Proposition 1 [**8**, proposition 6], $\mathrm{Diff}\,(K(\phi[s])/K) \leqslant \Delta_\phi + d \cdot (s)_0$. Write $M_s = K(\phi[s], \alpha_1, \ldots, \alpha_t)$ where each α_i is a root of $\phi_s(X) - P_i$. Consider the derivative with respect to X of $\phi_s(X)$ given by $\partial(\phi_s) = s$, since ϕ_s has linear term equal to s and all other terms are annihilated by the derivative. If $\wp$ is a place of good reduction for ϕ, then $v_{\wp}(\mathrm{Diff}\,(M_s/K(\phi[s]))) \leqslant t \cdot v_{\wp}(\partial(\phi_s))$ which is a standard discriminant calculation. Clearly, this quantity is given by $t v_{\wp}(\partial(\phi(s)) = t v_{\wp}(s)$. If $\wp$ is an infinite place then by Proposition 1, $v_{\wp}(\mathrm{Diff}\,(M_s/K(\phi[s]))) \leqslant t \cdot N_0 = v_{\wp}(\Delta_{\Gamma,\phi})$. If ϕ has potential good reduction at $\wp$ then there is an extension which is tamely ramified extension at $\wp$ where ϕ has good reduction, so $v_{\wp}(\mathrm{Diff}\,(M_s/K(\phi[s]))) \leqslant 1$. If in addition, $v_{\wp}(\alpha) < 0$, where α is a root of $\phi_s(X) - a_i$, then the different is bounded by $(d(\deg s) - 2)(-v - \wp(\alpha)) + v(s)$. If $\wp$ is a place of bad reduction for ϕ, then over a tamely ramified extension ϕ is isomorphic to a Drinfeld module of stable reduction. By Proposition 1, $v_{\wp}(\mathrm{Diff}\,(M_s/K(\phi[s]))) \leqslant t \cdot v_{\wp}(\Delta_{\phi,\Gamma}) + 1$. The second part follows by taking degrees and noticing that the only part on the right hand side that depends on s is $(t+d)(s)_0$.

We now have enough information to control the error term in the Chebotarev density theorem. We proceed to the algebraic considerations. The following two abstractions will be used in the determination of $\mathrm{Gal}\,(M_s/K)$. Essentially, our strategy is as in [**23**, pp. 72].

LEMMA 2. *Let R be a product of fields. Let V be a free rank k R-module. Let $\mathfrak{B} = V^n$. Let $G = \mathrm{End}\,(V)$ and for $g \in G$ let $g \cdot (v_1, \ldots, v_n) = (gv_1, \ldots, gv_n)$. Let B be a G-submodule of $\mathfrak{B}$. Let $\pi_i : B \to V$ be the restriction onto the i-th component. Assume that each π_i is onto and that the maps $\pi_1, \ldots, \pi_n$ are linearly independent over R. Then $B = \mathfrak{B}$.*

Proof. By induction on n, the base case being trivial. Let

$$B' = \{(x_1, \ldots, x_n) : (x_1, \ldots, x_n, 0) \in B\},$$

with projections $\pi'_1, \ldots, \pi'_n$.

We want to show that B' satisfies the hypotheses of the lemma, with $\mathfrak{B}' = V^n$. This will imply that $B' = \mathfrak{B}'$, and the fact that π_{n+1} is onto will complete the proof, since at this point we know that B contains all things of the form $(*, \ldots, *, 0)$ and $(0, \ldots, 0, *)$.

Claim. The map $\pi'_i : B' \to V$ is onto for $1 \leqslant i \leqslant n$.

Proof of claim. Without loss of generality take $i = 1$. Since we are allowed multiplication by elements of G, either $\alpha\pi_1'$ is zero for some non-zero element $\alpha \in R$ or π_1' is onto. So suppose that $\alpha\pi_1' = 0$. Then $(x_1, \dots, x_n, 0) \in C$ implies that $\alpha x_1 = 0$. Thus, we get an invertible matrix X such that $X\pi_{n+1} = \alpha\pi_1$. To see this, as π_{n+1} is onto, there are $x_1, \dots, x_k \in B$ such that $\pi_{n+1}(x_1), \dots, \pi_{n+1}(x_k)$ is a basis for V. Then for each $y \in B$ there are elements $c_1, \dots, c_k \in R$ such that $\pi_{n+1}(y) = \sum c_j\pi_{n+1}(x_j)$. This implies that $\alpha\pi_1(y) = \sum \alpha c_j \pi_1(x_j)$. But there is a matrix X such that $\pi_1(x_j) = X\pi_{n+1}(x_j)$ for each j. This implies that $\alpha\pi_1(y) = \alpha X(\sum c_j\pi_{n+1}(x_j)) = \alpha X\pi_{n+1}(y)$.

Now, we want to show that the G-action implies that X is a multiple of the identity, which would be a contradiction to the assumption that π_i's are independent over R. Let $Y \in \mathrm{End}(V)$ be arbitrary, then we see that $Y(\alpha X) = (\alpha X)Y$. To see this let $y \in B$ and notice

$$\begin{aligned}(\alpha X)Y\pi_{n+1}(y) &= \alpha X\pi_{n+1}(Yy) = \alpha\pi_1(Yy)\\ &= \alpha Y\pi_1(y) = \alpha YX\pi_{n+1}(y),\end{aligned}$$

and, since $\pi_{n+1}(y)$ is onto, we see that αX is in the center of $\mathrm{End}(V)$. Thus αX is a multiple of the identity. This contradicts the assumption that the projections are independent over R. Therefore π_1 is onto.

The other conditions of the lemma are already satisfied. Thus $B' = \mathfrak{B}'$. But this implies that $B = \mathfrak{B}$ as required.

PROPOSITION 2. *Suppose that the equation $a+b = 1$ has a solution for $a, b \in (\mathcal{O}/s\mathcal{O})^\times$. Then taking sums of $\mathrm{GL}_{\tilde{d}}(\mathcal{O}/s\mathcal{O})$ generates all $\tilde{d}$-by-$\tilde{d}$ matrices over $\mathcal{O}/s\mathcal{O}$. In particular, if s is coprime to the conductor $\mathfrak{c}$ and coprime to the discriminant of L/k (so that the ideal $s\mathcal{O}$ is square-free) and the constant field of L has more than 2 elements, or if the constant field of L has two elements and all divisors of s have degree at least 2, the conditions of the lemma are satisfied.*

Proof. We check to see that all matrices $m\delta_{i,j}$ with an m in the (i, j)th entry can be written as sums from $\mathrm{GL}_{\tilde{d}}(\mathcal{O}/s\mathcal{O})$. If $i \neq j$, then

$$m\delta_{i,j} = -\,\mathrm{id} + (\mathrm{id} + m\delta_{i,j})$$

is a sum of invertible matrices. Therefore, suppose that $i = j$. If we can write m as a sum of two elements of $(\mathcal{O}/s\mathcal{O})^\times$, we will be done. We proceed exactly as in [**15**]. For each $q|s$, let $a_q = 1$ if $m \equiv 0 \mod q$, and $a_q = am$ if $m \mod q$ is invertible. Similarly, for each $q|s$, let $b_q = -1$ if $m \equiv 0 \mod q$ and $b_q = bm$ if $m \mod q$ is invertible. Let $a^* \in A/s$ be the unique solution to $a^* \equiv a_q \mod q$ for all q, and b^* the solution to $b^* \equiv b_q \mod q$ for all q. Then certainly $m = a^* + b^*$ is a sum of invertible elements. Now write $m\delta_{i,i}$ as the sum of $\mathrm{diag}(1, \dots, 1, a^*, 1, \dots, 1) + \mathrm{diag}(-1, \dots, -1, b^*, -1, \dots, -1)$ which are both invertible matrices.

4. *Lang–Trotter revisited*

In this section, let q be a prime of A and $\wp$ be a prime of K for which ϕ has good reduction. We want to determine, for this fixed prime q, if the natural map

$$\Gamma \longrightarrow \phi(\mathbb{F}_\wp)/\phi_q(\phi(\mathbb{F}_\wp))$$

is a surjective map. If it is surjective for all primes q then clearly the reduction of $\Gamma \pmod{\wp}$ is all of $\phi(\mathbb{F}_\wp)$. If it fails to be surjective for at least one prime q, then clearly $\Gamma \pmod{\wp}$ is not equal to $\phi(\mathbb{F}_\wp)$.

This leads us to define

$$M_q = K(\phi[q], \alpha_1, \ldots, \alpha_t),$$

where α_i is a root of $\phi_q(X) = a_i$. We can see that these choices of the α_i's do not affect the extension M_q. These choices for α_i determine a linear map $\lambda : \Gamma \to \phi_q^{-1}\Gamma$ such that

$$\phi_q \circ \lambda = \mathrm{id}_\Gamma .$$

Let $G_q = \mathrm{Gal}(M_q/K)$. Then G_q is isomorphic to a subgroup of $\mathrm{GL}_d(\mathbb{F}_q) \rtimes \phi[q]^t$ by mapping $\sigma \in G_q$ to (γ, f) where $\gamma(x) = \sigma(x)$ for $x \in \phi[q]$. Now, consider the map f from Γ to $\phi[q]$ which is defined for $a \in \Gamma$ by

$$f(a) := \sigma\lambda(a) - \lambda(a).$$

Now, the map f can be viewed as an element of $\phi[q]^t$ by sending it to $(f(a_1), \ldots, f(a_t))$. Now, the action of σ on $u \in \phi_q^{-1}\Gamma$ is given by

$$\sigma(u) = \gamma(u - \lambda\phi_q(u)) + \lambda\phi_q(u) + f(\phi_q(u)).$$

We can now see that $\sigma(u) = u$ if and only if

$$(\gamma - 1)(u - \lambda\phi_q(u)) = -f(\phi_q(u)).$$

Suppose that $\wp$ is a prime that is unramified in the extension M_q. For example, suppose that the degree of $\wp$ is large enough (independently of the degree of q) and also that if $q_\wp$ is the prime of A lying below $\wp$ then $q \nmid q_\wp$. Let $\sigma_{\wp,q} \in G_q$ be an element of the conjugacy class of the Frobenius corresponding to $\wp$, and write $\sigma_{\wp,q} = (\gamma_{\wp,q}, f_{\wp,q})$. Following the work of Lang and Trotter [**17**, pp. 291], we will obtain a criterion for $(\phi(\mathbb{F}_\wp)/\Gamma_\wp)[q] \neq 0$ in terms of $\sigma_{\wp,q}$.

Notice that just as in the elliptic curve case, we have the equality

$$[\phi(\mathbb{F}_\wp) : \phi_q(\phi(\mathbb{F}_\wp))] = \left|\phi(\mathbb{F}_\wp) \cap (\phi \otimes \mathbb{F}_\wp)[q]\right| = \left|\mathrm{Ker}(\gamma_{\wp,q} - 1)\right| .$$

Consider the map $\Gamma \to \phi(\mathbb{F}_\wp)/\phi_q(\mathbb{F}_\wp)$ and denote by $\Gamma_{\wp,q}$ the kernel of this map. We wish to compare the quantity

$$\left|\Gamma/\Gamma_{\wp,q}\right|$$

with the quantity

$$\left|\mathrm{Ker}(\gamma_{\wp,q} - 1)\right| .$$

We want to express the inequality $|\Gamma/\Gamma_{\wp,q}| < |\mathrm{Ker}(\gamma_{\wp,q} - 1)|$ in terms of $\gamma_{\wp,q}$ and $f_{\wp,q}$, as this is the situation when q will divide the index of $\Gamma_\wp$ in $\phi(\mathbb{F}_\wp)$. As $\mathbb{F}_q$-vector spaces, we have

$$\Gamma/\Gamma_{\wp,q} \cong f_{\wp,q}(\Gamma)/(\mathrm{Im}(\gamma_{\wp,q} - 1) \cap f_{\wp,q}(\Gamma)).$$

By taking dimensions of both sides, this is equivalent to

$$\dim f_{\wp,q}(\Gamma) - \dim(f_{\wp,q}(\Gamma) \cap \mathrm{Im}(\gamma_{\wp,q} - 1)) < \dim \mathrm{Ker}(\gamma_{\wp,q} - 1).$$

Let $\mathcal{C}_q$ be the union of conjugacy classes of G_q defined by the condition that $(\gamma, f) \in \mathcal{C}_q$

whenever

$$\dim f(\Gamma) - \dim(f(\Gamma) \bigcap \mathrm{Im}\,(\gamma - 1)) < \dim \mathrm{Ker}\,(\gamma - 1).$$

Notice that this definition only assumes that G_q is a subgroup of $\mathrm{GL}_d(A/qA) \rtimes \phi[q]^t$. The following lemma gives a useful alternative condition for the above.

PROPOSITION 3. *Let $(\gamma, f) \in \mathrm{Gal}\,(M_q/K)$. Then $(\gamma, f) \in \mathcal{C}_q$ if and only if*

$$f(\Gamma) + \mathrm{Im}\,(\gamma - 1) \neq \phi[q].$$

Proof. The set $\mathcal{C}_q$ is defined by the condition

$$\dim f(\Gamma) - \dim(f(\Gamma) \bigcap \mathrm{Im}\,(\gamma - 1)) < \dim \mathrm{Ker}\,(\gamma - 1),$$

and we want to show that this is equivalent to the condition

$$f(\Gamma) + \mathrm{Im}\,(\gamma - 1) \neq \phi[q].$$

As

$$f(\Gamma)/(f(\Gamma) \bigcap \mathrm{Im}\,(\gamma - 1)) \cong (f(\Gamma) + \mathrm{Im}\,(\gamma - 1))/\,\mathrm{Im}\,(\gamma - 1),$$

we have

$$\dim(f(\Gamma)) - \dim(f(\Gamma) \bigcap \mathrm{Im}\,(\gamma - 1)) = \dim(f(\Gamma) + \mathrm{Im}\,(\gamma - 1)) - \dim(\mathrm{Im}\,(\gamma - 1)).$$

Now, by the rank-nullity theorem,

$$\dim(\mathrm{Im}\,(\gamma - 1)) + \dim(\mathrm{Ker}\,(\gamma - 1)) = \dim \phi[q] = d$$

and therefore the original condition is equivalent to

$$\dim(f(\Gamma) + \mathrm{Im}\,(\gamma - 1)) - \dim(\mathrm{Im}\,(\gamma - 1)) < \dim \mathrm{Ker}\,(\gamma - 1),$$

or

$$f(\Gamma) + \mathrm{Im}\,(\gamma - 1) \neq \phi[q].$$

We will be able to calculate the degrees of these extensions and the size of $\mathcal{C}_q$ based on knowledge of the endomorphism ring of ϕ.

Remark 1. In Section 6, we will calculate the size of $\mathcal{C}_q$ relative to the degree of M_q/K. To do this, it is convenient to identify $\mathrm{Gal}\,(M_q/K)$ with matrices over A/q with $d + t$ columns and d rows. By choosing a basis for $\phi[q]$ over A/q, we can identify $\gamma \in \mathrm{Gal}\,(K(\phi[q])/K)$ as an invertible d-by-d matrix with entries in A/q. As above, we can identify $\mathrm{Gal}\,(M_q/K(\phi[q]))$ with a subset of $\phi[q]^t$, and again by choice of basis, this leads to a d-by-t matrix with entries in A/q. By the above proposition, we count those pairs (γ, f) with $f(\Gamma) + \mathrm{Im}\,(\gamma - 1) \neq \phi[q]$. Therefore, consider the d-by-$d + t$ matrix with $\gamma - \mathrm{id}$ in the first d columns and d rows, and $f(a_1), \ldots, f(a_t)$ in the next t columns. Then $(\gamma, f) \in \mathcal{C}_q$ if and only if this matrix has rank at most $d - 1$. Later, we will count the number of such matrices.

PROPOSITION 4. *Let $\wp$ be a prime of K where ϕ has good reduction. Let $q_\wp \in A$ be the prime lying below $\wp$. The reduction $\Gamma_\wp$ of Γ modulo $\wp$ equals $\phi(\mathbb{F}_\wp)$ if and only if for each prime $q \neq q_\wp$, the Frobenius of G_q at $\wp$, $\sigma_{\wp,q} = (\gamma_{\wp,q}, f_{\wp,q})$, does not lie in the conjugacy class $\mathcal{C}_q$ and further that $|A/q_\wp| = |\mathbb{F}_\wp|$ but $\phi_{q_\wp}(\Gamma) \neq 0$.*

Remark 2. Remember that to define the Frobenius at $\wp$ we need for $\wp$ to be unramified in the field M_q. To guarantee this we can assume that $q \nmid q_\wp$. But in excluding this prime we must be able to guarantee that $\Gamma \rightarrow \phi(\mathbb{F}_\wp)/\phi_{q_\wp}(\mathbb{F}_\wp)$ is onto. Fortunately, we will see later that the number of primes which this proposition does not apply to are negligible.

5. *Galois groups and cohomology*

Recall that $\mathrm{End}\,(\phi) = \mathcal{O}$ and Γ generates a free $\mathcal{O}$-submodule of K' of rank t (recall that K' is the field over which all endomorphisms of ϕ are defined and it is a finite separable extension of K). Let s be a square-free monic polynomial in A, and let $M_s = \prod_{q|s} M_q$, $G_s = \mathrm{Gal}\,(M_s/K)$, $\mathcal{C}_s$ be the conjugacy class in G_s determined by all $\mathcal{C}_q$ for $q|s$.

Since $\phi_s = \psi_s$ for all $s \in A$, $K'M_s = K'(\phi[s], \phi_s^{-1}(\Gamma))$ and as $\psi[s] = \phi[s]$, we have that

$$K'M_s = K'(\psi[s], \psi_s^{-1}(\Gamma)).$$

Following [**23**] and [**24**] we establish that $\mathrm{Gal}\,(K'M_s/K'(\psi[s])) \cong \psi[s]^t$ for s such that $(s, M) = 1$ for some fixed $M \in A$. The work of Pink and Rutsche [**20**, theorem 0·2] implies that $\mathrm{Gal}\,(K'(\psi[q])/K') \cong \mathrm{GL}_{\tilde{d}}(\mathcal{O}/q\mathcal{O})$ for all but finitely many primes q of A. Let $\mathcal{O}_L$ be the integral closure of A in L. We will therefore take M_0 to include all primes of A that are ramified in L, and that divide the conductor $\mathfrak{c}$ of $\mathcal{O} \subset \mathcal{O}_L$, and such that $\mathrm{Gal}\,(K'(\phi[q])/K')$ is not equal to $\mathrm{GL}_{\tilde{d}}(\mathcal{O}/q\mathcal{O})$. By assuming that q is coprime to the conductor of $\mathcal{O}$ we avoid the problems associated to $\mathcal{O}$ being a possibly non-maximal order in L, and by assuming it is coprime to the discriminant of L/k, q will be unramified, and so $q\mathcal{O}_L$ is a square-free ideal in $\mathcal{O}_L$.

Let s be a monic square-free polynomial in A. Let K^{sep} be the separable closure of K in a fixed algebraic closure $\overline{K}$ of K. Let $G = \mathrm{Gal}\,(K^{\mathrm{sep}}/K')$, $H = \mathrm{Gal}\,(K^{\mathrm{sep}}/K'(\psi[s]))$.

Consider the set $\psi_s^{-1}(K) = \{x \in K^{\mathrm{sep}} : \psi_s(x) \in K'\}$. Fix an additive section $\lambda : K' \rightarrow \psi_s^{-1}(K')$. This may be done by Poonen's theorem, [**22**].

For $\sigma \in H$, let $\xi(\sigma) : K' \rightarrow \psi[s]$ be defined by

$$\xi(\sigma)(\cdot) = \sigma \circ \lambda(\cdot) - \lambda(\cdot),$$

Since σ fixes $\psi[s]$, this map is independent of the choice of λ. Therefore:

$$\xi : H \times K' \longrightarrow \phi[s].$$

We will show that this map ξ induces a map from H to $\mathrm{Hom}_{\mathcal{O}}(\mathcal{O}\Gamma, \psi[s]) \cong \psi[s]^t$, where $\mathcal{O}\Gamma$ is the free submodule of K' generated by Γ under the action of ψ. Our goal then is to show that this map is onto if we are allowed to choose an $M \in A$ such that $(s, M) = 1$. Our first step is to show that ξ is a homomorphism in both coordinates. Our next step will be to investigate what happens when we multiply ξ by various elements $g \in G$. This is very important, because if we assume that $\mathrm{Gal}\,(K'(\phi[s])/K') \cong \mathrm{GL}_{\tilde{d}}(\mathcal{O}/s\mathcal{O})$ then we can induce an action of $\tilde{d}$-by-$\tilde{d}$ matrices over $\mathcal{O}/s\mathcal{O}$ on the image of H in $\mathrm{Hom}_{\mathcal{O}}(\mathcal{O}\Gamma, \psi[s])$. We then use Poonen's theorem [**22**] and cohomological techniques (adapted from [**23**] and [**24**]) to prove that there is an injective map

$$\mathcal{O}\Gamma/(\psi_s(K') \bigcap \mathcal{O}\Gamma) \longrightarrow H^1(H, \psi[s]).$$

We conclude the section with a technical lemma which concludes that

$$\mathrm{Gal}\,(K'M_s/K'(\psi[s])) \cong \psi[s]^t.$$

PROPOSITION 5. *The map ξ does not depend on the choice of λ. Consider elements σ_1, σ_2 of H, elements a, b of K' and $m \in \mathcal{O}$. Then*

$$\xi(\sigma_1, a + b) = \xi(\sigma_1, a) + \xi(\sigma_1, b), \tag{5·1(a)}$$

$$\xi(\sigma_1\sigma_2, a) = \xi(\sigma_1, a) + \xi(\sigma_2, a), \tag{5·1(b)}$$

$$\xi(\sigma_1, \psi_m(a)) = \psi_m(\xi(\sigma_1, a)). \tag{5·1(c)}$$

Proof. Notice that λ, λ' are two sections, then $\lambda(a) - \lambda'(a) \in \psi[s]$. This difference is fixed by σ, so $\xi(\sigma, a) = \sigma \circ \lambda(a) - \lambda(a)$ is independent of the choice of λ. Equation 5·1(a) follows since λ is additive. For Equation 5·1(b), let us examine

$$\begin{aligned}\xi(\sigma_1\sigma_2, a) &= \sigma_1\sigma_2(\lambda(a)) - \lambda(a)\\ &= \sigma_1(\sigma_2(\lambda(a)) - \sigma_2(\lambda(a)) + \sigma_2(\lambda(a)) - \lambda(a)\\ &= \sigma_1(\lambda^{\sigma_2}(a)) - \lambda^{\sigma_2}(a) + \sigma_2(\lambda(a)) - \lambda(a)\\ &= \xi(\sigma_1, a) + \xi(\sigma_2, a),\end{aligned}$$

which follows since $\lambda^{\sigma_2} := \sigma_2 \circ \lambda$ is another choice of section for ξ, and ξ does not depend on the choice of section. Equation 5·1(c) follows since ψ_s has coefficients in K' and by Equation 5·1(a).

We note that ξ can be viewed as a map in three ways: $\xi : H \times K' \to \psi[s]$, $\xi : H \to \mathrm{Hom}_{\mathcal{O}}(K', \psi[s])$, and $\xi : K' \to \mathrm{Hom}(H, \psi[s])$.

If we are given $f \in \mathrm{Hom}_{\mathcal{O}}(K', \psi[q])$, it is natural to consider for $g \in G$, the map $g \cdot f \in \mathrm{Hom}_{\mathcal{O}}(K', \psi[q])$. We may also conjugate by $g \in G$ and then apply ξ. We consider the map $\xi(g \cdot g^{-1}) : H \to \mathrm{Hom}_{\mathcal{O}}(K', \psi[s])$. In fact, these two maps are equal.

PROPOSITION 6. *Let $g \in G$, the Galois group of K^{sep}/K'. For $h \in H$ we know that $ghg^{-1} \in H$. Let $a \in K'$. We have the equality*

$$g\xi(h, a) = \xi(ghg^{-1}, a).$$

If g is such that g acts identically to the map ψ_q on $\psi[s]$, for some q coprime to s then we also have

$$g\xi(h, a) = \xi(h, \phi_q(a)).$$

Proof. As before, $\lambda^{g^{-1}} = g^{-1}\lambda$ is another section satisfying $\psi_s(\lambda^{g^{-1}}) = \mathrm{id}_{K'}$. Therefore,

$$\xi(h, a) = hg^{-1}\lambda(a) - g^{-1}\lambda(a)$$

and so,

$$g\xi(h, a) = ghg^{-1}\lambda(a) - \lambda(a) = \xi(ghg^{-1}, a).$$

Now, assume that g when restricted to a map $\psi[s] \to \psi[s]$ acts as ψ_q for some q coprime to s. Then certainly,

$$g\xi(h, a) = \phi_q(\xi(h, a)) = \xi(h, \phi_q(a)),$$

by the previous proposition.

From now on, assume that $\mathrm{Gal}(K'(\psi[s])/K') \cong \mathrm{GL}_{\tilde{d}}(\mathcal{O}/s\mathcal{O})$ (that is $(s, M_0) = 1$). We claim that the action of $\mathrm{GL}_{\tilde{d}}(\mathcal{O}/s\mathcal{O})$ can be extended to $M_{\tilde{d}}(\mathcal{O}/s\mathcal{O})$, the space of $\tilde{d}$-by-$\tilde{d}$ matrices over $\mathcal{O}/s\mathcal{O}$.

PROPOSITION 7. *Let $g_1, \ldots, g_n, h_1, \ldots, h_m \in G$, and* $\mathrm{res} : G \to \mathrm{GL}_{\tilde{d}}(\mathcal{O}/s\mathcal{O})$ *be the restriction of g to an invertible map* $\psi[s] \to \psi[s]$. *Suppose that*

$$\sum_{i=1}^{n} \mathrm{res}\,(g_i) = \sum_{j=1}^{m} \mathrm{res}\,(h_j).$$

Then

$$\sum_{i=1}^{n} g_i \xi = \sum_{j=1}^{m} h_j \xi,$$

as maps from $H \times K' \to \psi[s]$.

Proof. Since $\xi(h, a) \in \psi[s]$, and both sums restrict to the same map on $\psi[s]$, the result follows.

Now, if we can write $X \in M_{\tilde{d}}(\mathcal{O}/s\mathcal{O})$ as a sum $X = \mathrm{res}\,(g_1) + \cdots + \mathrm{res}\,(g_n)$ for $g_i \in G$ for all such matrices X, then we can define $X\xi(h, a) = \sum \xi(g_i h g_i^{-1}, a) = \xi(g_1 h g_1^{-1} \cdots g_n h g_n^{-1}, a)$. That is, we can say that the image of $\xi(\cdot, a)$ is an $M_{\tilde{d}}(\mathcal{O}/s\mathcal{O})$-module.

The remaining condition to check is to make sure that when we take sums of various matrices in $\mathrm{GL}_{\tilde{d}}(\mathcal{O}/s\mathcal{O})$ we get all $\tilde{d}$-by-$\tilde{d}$ matrices over $\mathcal{O}/s\mathcal{O}$. This is Proposition 2.

LEMMA 3. *There exists $M_1 \in A$ such that the cohomology group*

$$H^1(\mathrm{Gal}\,(K'(\psi[s])/K'), \psi[s]) = 0,$$

for all $s \in A$ such that s is coprime to M_1.

Proof. By [**20**, theorem 0·1], $\mathrm{Gal}\,(K'(\psi[s])/K') \cong \mathrm{GL}_{\tilde{d}}(\mathcal{O}/s\mathcal{O})$ if $(s, M_0) = 1$. Let M_1 be such that if $M_0 | M_1$ and the conditions of Proposition 2 are satisfied for s where $(s, M_1) = 1$. Therefore, we can write $1 = a + b$ where $a, b \in (\mathcal{O}/s\mathcal{O})^\times$. Let $\gamma \in \mathrm{GL}_{\tilde{d}}(\mathcal{O}/s\mathcal{O})$ be equal to $a\,\mathrm{id}_{\phi[s]}$. Then γ is in the center of $\mathrm{GL}_{\tilde{d}}(\mathcal{O}/s\mathcal{O})$ and is such that the map $\gamma - 1$ is an automorphism of $(\mathcal{O}/s\mathcal{O})^{\tilde{d}}$. Hence, by Sah's Lemma [**16**, chapter 6, lemma 10·2], $H^1(\mathrm{Gal}\,(K'(\psi[s])/K'), \psi[s])$ is zero for all s with $(s, M_1) = 1$.

Now, let $(s, M_1) = 1$ and consider the short exact sequence of G modules

$$0 \hookrightarrow \phi[s] \hookrightarrow K^{\mathrm{sep}} \xrightarrow{\psi_s} K^{\mathrm{sep}} \longrightarrow 0.$$

Taking cohomology gives the exact sequence

$$0 \longrightarrow 0 \longrightarrow K' \xrightarrow{\psi_s} K' \longrightarrow H^1(G, \psi[s])$$

as the elements of $\psi[s]$ are not in K' (as $\mathrm{Gal}\,(K'(\psi[s])/K') \cong \mathrm{GL}_{\tilde{d}}(\mathcal{O}/s\mathcal{O})$) and K' is the fixed field of G. This induces the injective map

$$K'/\psi_s(K') \overset{\delta}{\hookrightarrow} H^1(G, \psi[s]).$$

We also have a restriction map

$$H^1(G, \psi[s]) \hookrightarrow H^1(H, \psi[s]),$$

which is injective if $(s, M_1) = 1$. To see this, let us briefly write down the relevant exact sequence for general G, H and G-module A.

$$0 \longrightarrow H^1(G/H, A^H) \longrightarrow H^1(G, A) \longrightarrow H^1(H, A)^{G/H} \longrightarrow H^2(G/H, A^H) \longrightarrow H^2(G, A).$$

But the first cohomology group is 0 ($H^1(\mathrm{GL}_{\tilde{d}}(\mathcal{O}/s\mathcal{O}), (\mathcal{O}/s\mathcal{O})^{\tilde{d}}) = 0$ by Lemma 3), and the third is a subset of $H^1(H, \psi[s])$. Again, this leads to an injection.

Further, the map that ξ induces from $K'/\psi_s(K')$ to $H^1(H, \psi[s])$ is given by the composition of these two maps, and so is injective for s such that $(s, M_1) = 1$.

Let $B = \mathrm{Im}\,(\sigma \to (\xi(\sigma, a_1), \ldots, \xi(\sigma, a_t)), \mathfrak{B} = \psi[s]^t$. Then B is an $\mathrm{End}\,(\psi[s])$-invariant submodule of $\mathfrak{B}$, as the G-action generated by it is isomorphic to the full matrix group $M_{\tilde{d}}(\mathcal{O}/s\mathcal{O})$. Now, consider the map $\mathcal{O}\Gamma/\psi_s(\mathcal{O}\Gamma) \to \mathcal{O}\Gamma/(\mathcal{O}\Gamma \cap \psi_s(K')) \to K'/\psi_s(K')$. We need to find $M \in A$ such that the first map is an injection for s coprime to M. Let

$$\Gamma' = \{x \in K' | \psi_m(x) \in \mathcal{O}\Gamma \text{ for some } m \in \mathcal{O}\}.$$

By Poonen's theorem, there exists an infinite sequence $Q_1, Q_2, \ldots$ which generates the module K'/ψ_{tor} freely. By our assumption that $\mathrm{Gal}\,(K'(\psi[s])/K') \cong \mathrm{GL}_{\tilde{d}}(\mathcal{O}/s\mathcal{O})$, we know that the s-primary part of $\psi_{\mathrm{tor}} \subset K'$ is trivial. Let n be such that $\mathcal{O}\Gamma \subset \mathcal{O} \cdot \{Q_1, \ldots, Q_n\}$. But then

$$\Gamma' \subset \mathcal{O} \cdot \{Q_1, \ldots Q_n\} \oplus \psi_{\mathrm{tor}}.$$

There exists $M \in A$ such that $\psi_M(\Gamma') \subset \Gamma$ and $M_1 | M$. Taking s coprime to M implies that each projection $\xi_i(\cdot)$ is independent over $\mathcal{O}/s\mathcal{O}$.

Finally, each projection is onto $\psi[s]$ is the image is a G-submodule of $\psi[s]$ and so it is either zero or onto. The assumption that $(s, M) = 1$ implies that it must be onto.

THEOREM 6. *If $s \in A$ is coprime to M and square-free then the group* $\mathrm{Gal}\,(K'M_s/K')$ *is isomorphic to* $\psi[s]^t \rtimes \mathrm{GL}_{\tilde{d}}(\mathcal{O}/s\mathcal{O})$.

Proof. Let us first recall that $\mathrm{Gal}\,(K'M_s/K')$ is isomorphic to a subgroup of $\psi[s]^t \rtimes \mathrm{GL}_{\tilde{d}}(\mathcal{O}/s\mathcal{O})$. For it to be isomorphic to the entire group, we only need to check if $\mathrm{Gal}\,(K'(\phi[s])/K') \cong \mathrm{GL}_{\tilde{d}}(\mathcal{O}/s\mathcal{O})$ and $\mathrm{Gal}\,(K'M_s/K'(\psi[s])) \cong \psi[s]^t$. The first follows since s is coprime to M. The image of $\mathrm{Gal}\,(K'M_s/K'(\psi[s]))$ is a G-invariant submodule of $\psi[s]^t$ such that the projection onto each copy of $\psi[s]$ is onto and all the projections are linearly independent over the product of fields $\psi[s] \cong \prod_{q|s}(\mathcal{O}/q)$. By Lemma 2, this implies that $\mathrm{Gal}\,(K'M_s/K'(\psi[s])) \cong \psi[s]^t$.

PROPOSITION 8. *If ϕ has rank 1 and r is a prime number, then assume that all primes of degree 1 divide M. Then the extensions $K'M_s$ for s square-free are geometric extensions of $K'(\phi[s])$ if $(s, M) = 1$.*

Proof. If $K'M_s/K'(\phi[s])$ is not geometric, then there is an intermediate field k_1 such that $k_1 = K'(\phi[s]) \otimes \mathbb{F}_{r^\ell}$ for some $\ell \neq 1$. The group $\mathrm{Gal}\,(k_1/K'(\phi[s]))$ is a cyclic group as it is generated by the Frobenius map acting on the constant field of k_1. But as k_1 is also a subfield of M_s, we must have that group $\mathrm{Gal}\,(k_1/K'(\phi[s]))$ is a subgroup of $\phi[s]$. As an additive group, the exponent of $\phi[s]$ is the field characteristic of $\mathbb{F}_r$, so ℓ is a prime number. But $\mathrm{Gal}\,(k_1/K'(\phi[s])$ is a G-submodule of $\mathrm{Gal}\,(K'M_s/K'(\phi[s]))$ since k_1 is Galois. In particular, our previous arguments imply that $\mathrm{Gal}\,(k_1/K'(\psi[s]))$ must be isomorphic to an $\mathrm{End}\,(V)$-submodule of V^t, with $V = (\mathcal{O}/s\mathcal{O})^{\tilde{d}}$. In fact, the only way that V has a submodule of prime order is if the rank of ϕ is 1, r is a prime and there is a prime of degree 1 dividing s.

6. *Degrees of extensions*

Now, let K' be a finite Galois extension of K such that $\psi : \mathcal{O} \to K'\{\tau\}$ is the rank $\tilde{d}$ Drinfeld module corresponding to the ring of endomorphisms $\operatorname{End}(\phi) = \mathcal{O}$, $L = \mathcal{O} \otimes k$, $h = [L : k]$ and $d = h\tilde{d}$. For square-free $s \in A$, define $n(s) = [M_s : K]$.

PROPOSITION 9. *For all primes q such that $(q, M) = 1$, we have*

$$[K'M_q : K'] = |\phi[q]|^t \cdot |\operatorname{GL}_{\tilde{d}}(\mathcal{O}/q\mathcal{O})|.$$

For all square-free $s \in A$,

$$r^{\deg s(dt+\tilde{d}d-h)}\varphi(s)^h \ll n(s) \ll r^{\deg s(dt+\tilde{d}d)},$$

where $\varphi(s) = |(A/s)^\times|$ and the implied constants do not depend on s.

Proof. Notice that

$$[K'M_s : K'] \leqslant n(s) \leqslant [K'M_s : K'][K' : K].$$

Hence, we may prove the inequality for $[K'M_s : K']$. Now, let $M \in A$ be as in Theorem 6. Write $s = s_1s_2$ where $(s_2, M) = 1$ and $s_1|M$. As there are only finitely many possibilities for s_1, proving the inequality with s replaced by s_2 will be enough to prove the proposition. Let q be a prime dividing s_2. Then

$$\begin{aligned}[K'M_q : K']/r^{\deg q(dt+\tilde{d}d)} &= \prod_{i=0}^{\tilde{d}-1}(1 - r^{\deg q(i-\tilde{d})})^h \\ &= \prod_{i=1}^{\tilde{d}}(1 - r^{-i\deg q})^h.\end{aligned}$$

Clearly, $[K'M_q : K'] \leqslant r^{\deg q(dt+\tilde{d}d)}$. As the fields $K'M_q$ are linearly disjoint over K' for $(q, M) = 1$, we have

$$\begin{aligned}[K'M_{s_2} : K'] &= \prod_{q|s_2}[K'M_q : K'] \\ &= \prod_{q|s_2} r^{\deg q(d\tilde{d}+dt)} \prod_{i=1}^{\tilde{d}}(1 - r^{-i\deg q})^h \\ &\gg r^{\deg s(d\tilde{d}+dt)} \prod_{q|s_2}(1 - r^{-\deg q})^h,\end{aligned}$$

where the last line of inequality follows since the products

$$\prod_{q \text{ prime}} (1 - r^{-i\deg q})$$

all converge absolutely if $i \geqslant 2$. The proposition follows.

We need to calculate the size of the conjugacy class $\mathcal{C}_q$. To do this we will use the following lemma. Let F be a finite extension of E of degree c. Let $d = \tilde{d} \cdot c$ and t a non-negative integer. Consider $\operatorname{GL}_{\tilde{d}}(F)$ as a subgroup of $\operatorname{GL}_d(E)$ by the Weil restriction. Define

$$\mathfrak{M}' = \{W \in M_{d,d+t}(E) |\text{ the first } d \text{ col. of } W \text{ are in } M_{\tilde{d}}(F), \text{ and } \operatorname{rank}(W) \leqslant d-1\}$$

and

$$\mathfrak{M} = \{W \in \mathfrak{M}' \mid \text{the first } d \text{ col. of } W \text{ are in } \mathrm{GL}_{\tilde{d}}(F) - \mathrm{id}\}.$$

LEMMA 4. *$\mathfrak{M}$ and $\mathfrak{M}'$, as varieties over E, have dimension $d\tilde{d} + td - t - 1$, and $\mathfrak{M}'$ is irreducible.*

Proof. For $W \in \mathfrak{M}'$, we can view it as two parts, the matrix formed by the first d columns is a linear transformation from $F^{\tilde{d}}$ to $F^{\tilde{d}}$, and the rest of matrix is a linear transformation from E^t to E^d.

Let $G(1, d)$ be the Grassmannian variety of $(1, d)$ type over E. We define

$$\Psi \subset M_{d,d+t} \times G(1, d),$$

by

$$\Psi = \{(M, \Lambda) \mid W \in \mathfrak{M}', \ \Lambda \subset \mathrm{Ker}\,(W^T)\}.$$

If we fix a one-dimensional subspace Λ, which is determined by a non-zero vector v in E^d. We can identify E^d with $F^{\tilde{d}}$ and then v can be identified as a vector v' in $F^{\tilde{d}}$. The fiber of $\pi_2 : \Psi \rightarrow G(1, d)$ over Λ is just the space of $\{(A_1, A_2) \mid A_1 \in \mathrm{Hom}\,(F^{\tilde{d}}/\langle v' \rangle, F^{\tilde{d}}),\ A_2 \in \mathrm{Hom}\,(E^d/{<}v{>}, E^t)\}$. The space $\mathrm{Hom}\,(F^{\tilde{d}}/\langle v' \rangle, F^{\tilde{d}})$ is a variety of dimension $(\tilde{d}-1)\tilde{d}$ over F; as a variety over E, $\mathrm{Hom}\,(F^{\tilde{d}}/\langle v' \rangle, F^{\tilde{d}})$ is of dimension $c \cdot ((\tilde{d} - 1)\tilde{d})$ by the general fact of the Weil restriction. Thus, the dimension of the fiber over Λ is

$$c \cdot ((\tilde{d} - 1)\tilde{d}) + t(d - 1) = d(\tilde{d} - 1) + dt - t = d\tilde{d} + td - d - t.$$

We conclude that the variety Ψ is irreducible of dimension

$$\dim(G(1, d)) + d\tilde{d} + td - d - t = (d - 1) + d\tilde{d} + td - d - t = d\tilde{d} + td - t - 1.$$

Since the map $\pi_1 : \Psi \rightarrow M_{d,d+t}$ is generically one to one onto $\mathfrak{M}'$, we deduce that the same is true for $\mathfrak{M}'$. Certainly, $\mathfrak{M} \subset \mathfrak{M}'$. To show that $\mathfrak{M}$ has the same dimension as $\mathfrak{M}'$, we will show that the complement of $\mathfrak{M}$ in $\mathfrak{M}'$ is contained in a variety with strictly smaller dimension. The complement of $\mathfrak{M}$ in $\mathfrak{M}'$ is

$$\left\{W = \begin{pmatrix} D & E \end{pmatrix} \mid \det(D + I) = 0, \mathrm{rank}\,(W) \leqslant d - 1\right\}.$$

This set has codimension 1 in $\mathfrak{M}'$, finishing the proof of the Lemma.

By Lang–Weil's theorem [**18**, theorem 1], we get the following result immediately.

THEOREM 7. *Let $\mathbb{F}_l$ be a finite field and F be a finite field extension of degree c. Let $\mathfrak{M}(\mathbb{F}_l, c, d)$ be the set of $d + t$-by-d matrices as in the above argument (so that $E = \mathbb{F}_l$). Then*

$$|\mathfrak{M}(\mathbb{F}_l, c, d)| = l^{d\tilde{d}+td-t-1} + \mathbf{O}(l^{(d\tilde{d}+td-t-1)-1/2}).$$

PROPOSITION 10. *For all primes q, such that $(q, M) = 1$,*

$$|\mathcal{C}_q| \ll r^{\deg q[(d-1)t+\tilde{d}d-1]}.$$

Proof. By the construction of M, if $(q, M) = 1$ then q is unramified in the extension $L = \mathcal{O} \otimes k$. Now, L/k is Galois (check that if $\sigma \in \mathrm{Gal}\,(K^{\mathrm{sep}}/K)$ and $P \in \mathrm{End}\,(\phi)$ then σP (apply σ to the coefficients of P) is also an endomorphism of ϕ). Therefore, we may factor $q\mathcal{O}$ into prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_g$ of $\mathcal{O}$. Given that $(q, M) = 1$, we know that $\mathrm{Gal}\,(K'M_s/K') \cong \mathrm{GL}_{\tilde{d}}(\mathcal{O}/q\mathcal{O}) \rtimes \psi[q]^t$. Therefore, given $\sigma \in \mathrm{Gal}\,(K'M_s/K')$ let $\sigma_1, \ldots, \sigma_g$ be the restrictions of σ to $\mathrm{Gal}\,(K'M_{\mathfrak{q}_1}/K'), \ldots, \mathrm{Gal}\,(K'M_{\mathfrak{q}_g}/K')$. By consulting Proposition 3 and the remark immediately following it, $\sigma \in \mathcal{C}_q$ if and only if for some $1 \leqslant i \leqslant g$, $\sigma_i \in \mathcal{C}_i$ which is the conjugacy class defined above with $\tilde{d}$ remaining the same but $c = [\mathcal{O}/\mathfrak{q}_i : A/q]$ and so $[L : k] = g \cdot c$, and $d' = \tilde{d} \cdot c$. So $\mathcal{C}_q$ is the union of the lifts of all the $\mathcal{C}_i$ for $i = 1, \ldots, n$. Therefore, the result follows by the previous theorem.

PROPOSITION 11. *Let $s \in A$ be square-free, then*

$$\frac{|\mathcal{C}_s|}{n(s)} \ll r^{\deg s(-t-1+h)}/\varphi(s)^h,$$

as $\deg s \to \infty$.

Proof. Combine Proposition 10 and Proposition 9.

7. *Analysis*

The aim of this section is to estimate the function $N_\Gamma(x)$ that counts the primes $\wp$ of K of degree x of good reduction for ϕ such that the reduction of Γ modulo $\wp$ generates $\phi(\mathbb{F}_\wp)$.

Let $S = \{q \in A | q \text{ is a prime of } A\}$, S^* be the monic polynomials which are square-free products of the elements of S, $S_y = \{q \in S | \deg q \leqslant y\}$ and S_y^* be defined similarly to S^*. A place $\wp$ of K is of **first-degree** if the residue degree $f_\wp = [\mathfrak{o}_\wp/\mathfrak{m}_\wp : A/q_\wp] = \deg \wp / \deg q_\wp = 1$ where $q_\wp$ is the prime of A lying below $\wp$. Let $\mathcal{P}_K^1$ denote all the primes of K which are of first-degree. Let

$$N(x, y) = \left|\left\{\wp \in \mathcal{P}_K^1 | \deg \wp = x, \sigma_{\wp,q} \notin \mathcal{C}_q \text{ for all } q \in S_y\right\}\right|.$$

As is usual, $N(x, y)$ will be used to estimate $N_\Gamma(x)$ up to an error term $M_x(y, x)$. Define

$$M_x(y_1, y_2) = \left|\left\{\wp \in \mathcal{P}_K^1 | \deg \wp = x, \sigma_{\wp,q} \in \mathcal{C}_q \text{ for some } q \in S, y_1 < \deg q \leqslant y_2\right\}\right|.$$

PROPOSITION 12.

$$N_\Gamma(x) = N(x, y) + \mathbf{O}\left(M_x(y, x) + r^{x/2}\right),$$

as $x \to \infty$.

Proof. Let $\wp$ be a prime which is counted by $N_\Gamma(x)$. Then, by Proposition 4, $\sigma_{\wp,q} \notin \mathcal{C}_q$ for any prime q, and hence $\wp$ is counted by $N(x, y)$ or the degree $f_\wp = [\mathbb{F}_\wp : A/q_\wp] \geqslant 2$. The number of primes satisfying the second condition is bounded by $r^{x/2}$. Thus $N_\Gamma(x) \leqslant N(x, y) + r^{x/2}$. Now, we show that $N(x, y) \leqslant N_\Gamma(x) + \mathbf{O}\,(M_x(y, x))$. This follows because if $\wp$ is a prime counted by $N(x, y)$ but not by $N_\Gamma(x)$ then by Proposition 4, $\sigma_{\wp,q} \in \mathcal{C}_q$ for some prime q with $\deg q > y$ or $\phi_{q_\wp}(\phi(\mathbb{F}_\wp)) \neq \phi(\mathbb{F}_\wp)$. But if $\sigma_{\wp,q} \in \mathcal{C}_q$ then $\phi(\mathbb{F}_\wp)$ contains non-trivial q-torsion and so $\deg q \leqslant \deg \wp = x$. As $\wp$ is counted by $N(x, y)$ it is of first-degree over k. If $\phi(\mathbb{F}_\wp)$ has non-trivial $q_\wp$-torsion, then $\phi(\mathbb{F}_\wp) \cong A/q_\wp$. But these primes are counted by $N_\Gamma(x)$ as long as Γ does not reduce to zero modulo $\wp$. The number of such primes is bounded by a constant. The proposition follows from these estimates.

Our aim is therefore to estimate $N(x, y)$ and $M_x(y, x)$ for appropriately chosen y. But the principle of inclusion and exclusion implies that

$$N(x, y) = \sum_{s \in S_y^*} \mu(s)\pi(x, s),$$

where $\pi(x, s)$ denotes the number of primes of K of first-degree and of degree x for which the Artin symbol lies in $\mathcal{C}_s$. We can use the Chebotarev density theorem to estimate $\pi(x, s)$ and therefore $N(x, y)$.

In the statement of the following theorem, $\mathbb{F}_L$ and $\mathbb{F}_{L'}$ are the constant fields of L and L'. The integer $\hat{d}$ depends on the field L. The integer r_L is the degree of the extension $[\mathbb{F}_{L'} : \mathbb{F}_L]$. Also, the size of the finite field $\mathbb{F}_L$ will be a prime power ℓ. The prime counting function $\pi_{\mathcal{C}}(x)$ will denote the number of primes $\wp$ of L of degree x such that the Artin symbol of $\wp$ lies in $\mathcal{C}$. The genera of L and L' are g_L and $g_{L'}$.

THEOREM 8 ([**7**, chapter 6, section 4]). *Let L'/L be a finite Galois extension with Galois group G. Let $\mathcal{C} \subset G$ be a conjugacy class whose restriction to $\mathbb{F}_{L'}$ is the ith power of the Frobenius automorphism of $\mathbb{F}_L$. Then, for $x \in \mathbb{N}$, if $x \not\equiv i \pmod{r_L}$, we have*

$$\pi_{\mathcal{C}}(x) = 0.$$

If $x \equiv i \pmod{r_L}$,

$$\left|\pi_{\mathcal{C}}(x) - r_L \frac{|\mathcal{C}|}{|G|} \frac{\ell^x}{x}\right| \leqslant \frac{2|\mathcal{C}|}{x|G|}((|G| + g_{L'} r_L)(\ell^x)^{1/2} + |G|(2g_L + 1)(\ell^x)^{1/4} + g_{L'} r_L + |G|\hat{d}).$$

Although the effective version is not explicitly listed as a theorem, one can trace through [**7**, chapter 6, section 4] to find all the constants.

PROPOSITION 13. *Let $s \in A$ be square-free and denote by $\mathbb{F}(s)$ the constant field of M_s, with $r(s) = [\mathbb{F}(s) : \mathbb{F}_r]$. Let i be an integer in the range $0 \leqslant i \leqslant r(s) - 1$. Let $G_{i,s}$ be the subset of* Gal (M_s/K) *whose restriction to $\mathbb{F}(s)$ is the ith power of the Frobenius of $\mathbb{F}(s)$ over $\mathbb{F}_r$ and $x \equiv i \pmod{r(s)}$. Then*

$$\left|\pi(x, s) - r(s) \frac{|\mathcal{C}_s \cap G_{i,s}|}{n(s)} \frac{r^x}{x}\right| = \mathbf{O}\left(\frac{r^{x/2 + \deg s[(d-1)t + \tilde{d}d - 1]}}{x} \deg s\right).$$

Proof. For each $i = 0, 1, 2, \ldots, r(s) - 1$, let $G_{i,s}$ be the subset of Gal (M_s/K) which restricts to the ith power of the Frobenius morphism of the constant field of M_s over $\mathbb{F}_r$. As the constant field of K is not necessarily $\mathbb{F}_r$, some of these sets may be empty.

Let $g(s)$ be the genus of M_s. By the Riemann–Hurwitz formula [**25**, theorem 7·16] and Theorem 5, we get that

$$g(s) \leqslant \frac{n(s)}{r_s}(2g_k - 2) + (t + d) \deg s.$$

Now, applying Theorem 8 and accounting for all the constants, we get that

$$\left|\pi'(x, s) - r(s) \frac{|\mathcal{C}_s \cap G_{i,s}|}{n(s)} \frac{r^x}{x}\right| \leqslant \frac{|\mathcal{C}_s|}{n(s)x} n(s)(t + d) \deg s \cdot r^{x/2},$$

where $\pi'(x, s)$ counts the number of primes of K of degree x whose Artin symbol lies in $\mathcal{C}_s$. The difference,

$$|\pi'(x, s) - \pi(x, s)|$$

counts those primes $\wp$ of K of degree x whose Artin symbol lies in $\mathcal{C}_s$ and which satisfy

$$\deg \wp \geqslant 2 \deg q_\wp,$$

where $q_\wp$ is the prime of A which lies below $\wp$. There are at most $r^{x/2}$ primes q of A satisfying $\deg q \leqslant x/2$ and there are at most $[K : k]$ primes $\wp$ of K lying over a particular prime q of A. Hence,

$$|\pi'(x, s) - \pi(x, s)| \ll r^{x/2}.$$

By Proposition 10, $|\mathcal{C}_s| \ll r^{\deg s[(d-1)t+\tilde{d}d-1]}$, so

$$\left|\pi(x, s) - r(s)\frac{|\mathcal{C}_s \cap G_{i,s}|}{n(s)}\frac{r^x}{x}\right| \ll \frac{1}{x}r^{\deg s[(d-1)t+\tilde{d}d-1]}(t+d)\deg s \cdot r^{x/2}.$$

The following proposition says that the main contribution to $N_\Gamma(x)$ is about $\delta_y r^x/x$ where δ_y is a constant that depends on y. We must show that δ_y is absolutely convergent, and also that it converges *fast enough*. Everything after this is about controlling the remainder term. Our strategy is as usual for these types of problems, that is, we split up the remaining interval into parts, and use different estimates on each part.

PROPOSITION 14. *Let $y = \log_r x + \mathbf{o}(1)$. Let $x \in \mathbb{N}$, and remember that $G_{x,s}$ is the set of all elements of* Gal (M_s/K) *which are the xth power of the Frobenius of the constant field of M_s over $\mathbb{F}_r$. Then*

$$\left|N(x, y) - \sum_{s\in S_y^*}\mu(s)r(s)\frac{|\mathcal{C}_s \cap G_{x,s}|}{n(s)}\frac{r^x}{x}\right| = \mathbf{O}\left(r^{(3/4)x}\right).$$

Remark 3. Notice that $G_{x,s}$ only depends on the congruence class of $x \pmod{r}(s)$.

Proof. By the prime number theorem, [**25**, theorem 5·12],

$$|S_y| \ll \frac{r^y}{y},$$

as $y \to \infty$.

Summing over all $s \in S_y^*$, we get

$$\begin{aligned}\left|N(x, y) - \sum_{s\in S_y^*}\mu(s)r(s)\frac{|\mathcal{C}_s \cap G_{x,s}|}{n(s)}\frac{r^x}{x}\right| &= \mathbf{O}\left(\frac{r^{x/2}}{x}\sum_{s\in S_y^*}\deg(s)r^{\deg s[(d-1)t+\tilde{d}d-1]}\right)\\ &= \mathbf{O}\left(\frac{r^{x/2}}{x}x\prod_{q \text{ prime}, \deg q\leqslant y}\left(1+r^{\deg q[(d-1)t+\tilde{d}d-1]}\right)\right),\end{aligned}$$

because for $s \in S_y^*$, we have that $\deg s \ll y(r^y/y) \ll x$, since $y = \mathbf{O}(\log x)$.

To complete the proof, we want to make sure y can be chosen such that $y - \log_r(x) = \mathbf{o}(1)$ and

$$\prod_{q \text{ prime}, \deg q\leqslant y}\left(1+r^{\deg q[(d-1)t+\tilde{d}d-1]}\right) = \mathbf{O}\left(r^{x/4}\right).$$

We can bound the product

$$\prod_{q \text{ prime}, \deg q\leqslant y}\left(1+r^{\deg q[(d-1)t+\tilde{d}d-1]}\right) \leqslant 2^{\mathbf{O}(r^y/y)}\prod_{q \text{ prime}, \deg q\leqslant y}r^{\deg q[(d-1)t+\tilde{d}d-1]}.$$

Now,

$$\sum_{q \text{ prime},\, \deg q \leqslant y} \deg q \ll y \frac{r^y}{y} = r^y.$$

So the product can be bounded by

$$r^{\mathbf{O}(r^y)},$$

which can be made $\mathbf{O}(r^{x/4})$ if $y - \log_r x = \mathbf{o}(1)$.

So, now we know that $N(x, y)$ is the main term, let us make sure that δ_y converges nicely.

In the following theorem, the integer r^* is defined to be the maximum possible value of $r(s)$ (the degree of the constant field of M_s over $\mathbb{F}_r$) as s runs over all square-free elements of A. This definition makes sense if we recall Proposition 8, that implies that the degree of the constant field of M_s is bounded. We have previously defined r^* as the least common multiple of the degrees of the constant field extensions of M_q/K where q runs over all primes of A. Our two definitions will agree since

$$M_s = \prod_{q|s} M_q$$

and so, if $\mathbb{F}(s)$ is the constant field of M_s, we have

$$\mathbb{F}(s) = \prod_{q|s} \mathbb{F}(q),$$

which implies that $r(s)$ is the least common multiple of the degrees $r(q)$ as q runs over all prime divisors of s, from which the two definitions can be seen to agree.

PROPOSITION 15. *Let* $i \in \{0, 1, 2, \ldots, r^* - 1\}$. *Then*

$$C_{\phi,\Gamma}(i) = \sum_{s \in S^*} \mu(s) r(s) \frac{|\mathcal{C}_s \cap G_{i,s}|}{n(s)}$$

converges absolutely.

Proof. By Proposition 11, we must show that

$$\sum_s r^{\deg s(-t-1+h)} / \varphi(s)^h$$

converges, where the sum is taken over square-free $s \in A$. Consider

$$\prod_{q \text{ prime}} (1 + r^{\deg q(-t-1+h)} / (r^{\deg q} - 1)^h).$$

This product converges to a non-zero real number if and only if the sum

$$\sum_{q \text{ prime}} r^{\deg q(-t-1+h)} / (r^{\deg q} - 1)^h$$

converges. But this sum is bounded by

$$\sum_{q \text{ prime}} 2^h r^{\deg q(-t-1)},$$

which is convergent.

To make sure that our main term is correct, we must ensure that the constant δ_y tends to a convergent series fast enough. We take care of this now.

PROPOSITION 16.

$$\left|\sum_{s\in S^*}\mu(s)\frac{|\mathcal{C}_s\cap G_{x,s}|}{n(s)}r^x/x-\sum_{s\in S_y^*}\mu(s)\frac{|\mathcal{C}_s\cap G_{x,s}|}{n(s)}r^x/x\right|=\mathbf{O}(r^x/x^2).$$

Proof. As usual,

$$\begin{aligned}\sum_{s\in S^*\setminus S_y^*}\frac{|\mathcal{C}_s|}{n(s)}&\ll\sum_{s\in S^*\setminus S_y^*}r^{\deg s(-t-1+h)}/\varphi(s)^h\\&\ll\sum_{\deg q\geqslant y}r^{\deg q(-t-1)}\sum_{s\in S^*}r^{\deg s(-t-1+h)}/\varphi(s)^h\\&\ll\sum_{i=y}^{\infty}r^{-i(t+1)}r^i\\&\ll r^{-yt}\ll x^{-t},\end{aligned}$$

which is sufficient as long as $t\geqslant 1$.

To summarise what we have done up to this point, we have proved that

$$N_\Gamma(x)=C_{\phi,\Gamma}(i)\frac{r^x}{x}+\mathbf{O}\left(M_x(y,x)+\frac{r^x}{x^2}\right).$$

To complete the proof we must show that $M_x(y,x)$ is $\mathbf{O}(r^x\log x/x^2)$. We will split up the interval $(y,x]$ into three parts. The tail end of the interval will be dealt with by the following bound from [**1**]. This is very tail end of the interval. We restate it as follows:

PROPOSITION 17 ([**1**, proposition 5·1]). *Let $\ell\geqslant 1$ be an integer, and let*

$$T_\ell:=\{\wp\text{ of good reduction for }\Gamma\text{ such that }[\Gamma_\wp:\mathbb{F}_r]\leqslant\ell\},$$

where Γ has good reduction at $\wp$ if all the generators of Γ are integral at $\wp$ and ϕ has good reduction at $\wp$. Then

$$|T_\ell|=\mathbf{O}\left(r^{\ell(1+d/t)}\right).$$

We will split the interval $(y,x]$ into $(y,\alpha x]$, $(\alpha x,\alpha x+\beta\log x]$, and $(\alpha x+\beta\log x,x]$ for a suitable choice of α,β. The first two intervals are handled by Chebotarev density theorem and the third is handled by the use of the proposition from [**1**]. Let us concentrate on the first interval which will determine the choice of α.

PROPOSITION 18. *Let $\alpha=(2(d+\tilde{d}d-1))^{-1}-2\log_r(x)/x$, then as $x\to\infty$*

$$M(y,\alpha x)=\mathbf{O}\left(\frac{r^x}{x^2}\right).$$

Proof. If we consider the restriction of $\sigma_{\wp,q}\in\mathcal{C}_q$ to $\mathrm{Gal}(K(\phi[q],q^{-1}a_1)/K)$ there are at most $\mathbf{O}(r^{(d+\tilde{d}d-2)\deg q})$ possibilities for $\sigma_{\wp,q}$. The size of the Galois group is $r^{(d+\tilde{d}d)\deg q}+\mathbf{O}(r^{(d+\tilde{d}d-1)\deg q})$, so that using the Chebotarev density theorem again we obtain

$$M(y,\alpha x)\leqslant\sum_{q\in S_{\alpha x}\setminus S_y}\left[\frac{r^{x-2\deg q}}{x}+\mathbf{O}(r^{(\tilde{d}d+d-2)\deg q}\cdot r^{x/2}x)\right].$$

The sum of the error terms is $\mathbf{O}(r^{x[(d+\tilde{d}d-2)\alpha+\alpha+1/2]}) = \mathbf{O}(r^x/x^2)$. Now, the number of q with $\deg q = i$ is $\mathbf{O}((r^i/i))$, thus the first summand is bounded by a constant times

$$\sum_{i\geqslant y} \frac{r^{x-i}}{xi} \ll r^{-y}\frac{r^x}{x^2} = \mathbf{O}\left(\frac{r^x}{x^2}\right).$$

Let $z = \alpha x + \beta \log x$, where $\beta > 0$ is a constant which will be chosen later. We now see that the middle interval can be handled. After this, we will just need to control the tail term by a judicious choice of β.

PROPOSITION 19. *The estimate for the interval* $(\alpha x, z)$ *is*

$$M(\alpha x, z) = \mathbf{O}(r^x \log x/x^2),$$

as $x \to \infty$.

Proof. For this part, replacing A by its endomorphism ring only changes our estimate by at most a constant, therefore we may assume that the endomorphism ring is no larger than A. Suppose that $\wp$ is a prime counted by $M(\alpha x, z)$. Then there is a prime q with $\alpha x \leqslant \deg q < z$ such that $\phi(\mathbb{F}_\wp)$ has non-trivial q-torsion. This amounts to the condition that the Frobenius of $\wp$ has eigenvalue one in the Galois group $G_{q,1} = \mathrm{Gal}\,(K(\phi[q])/K)$. Let $\mathcal{C}_{q,1}$ be the conjugacy class of elements of $G_{q,1}$ which have eigenvalue 1. Then $|\mathcal{C}_{q,1}|$ is bounded by a constant independent of q times $r^{\deg q(\tilde{d}d-1)}$ and the order of $G_{q,1}$ is asymptotically $r^{\deg q(d\tilde{d})}$. Therefore, by an application of the Chebotarev density theorem, we have that

$$M(\alpha x, z) \ll \sum_{\alpha x \leqslant \deg q < z} \left(\frac{r^{x-\deg q}}{x} + r^{\deg q(d\tilde{d}-1)+x/2}\right).$$

Now by the prime number theorem for A, the first summand can be bounded by

$$\sum_{\alpha x\leqslant i<z} \frac{r^{x-i}}{x}\frac{r^i}{i} = \frac{r^x}{x}\sum_{\alpha x\leqslant i<z} 1/i \ll \frac{r^x}{x}(\log(z/\alpha x)) \ll \frac{r^x \log x}{x^2}.$$

As we have already chosen α, we check that the error term is bounded by a constant times

$$\sum_{\alpha x\leqslant i<z} r^{id\tilde{d}+x/2} \ll \beta \log x r^{zd\tilde{d}+x/2}.$$

If $d = 1$, then this sum can be controlled as in [**14**, theorem 4·3]. If $d \geqslant 2$, then

$$\begin{aligned} zd\tilde{d} + x/2 &= (2(d+\tilde{d}d-1))^{-1}xd\tilde{d} - 2\log_r(x)d\tilde{d} + d\tilde{d}\beta\log x + x/2 \\ &\leqslant \frac{x}{2}\left(\frac{d\tilde{d}}{d\tilde{d}+d-1}+1\right) + d\tilde{d}\beta\log x \\ &= x(1-\epsilon) + d\tilde{d}\beta\log x \end{aligned}$$

where $\epsilon = (d - 1/2(d\tilde{d}+d-1)) > 0$ if $d > 1$. Hence, the error is bounded by a constant times

$$r^{x(1-\epsilon)}x^{d\tilde{d}\beta} \ll r^{x(1-\epsilon')} \text{ as } x \longrightarrow \infty, \epsilon' > 0.$$

The estimate follows.

The following theorem is purely a calculation, based on our choice of α which was forced earlier and Proposition 17.

PROPOSITION 20. *Suppose that* $t \geqslant (2d^2\tilde{d} + 2d^2 - 3d)$*, then we may choose* $\beta > 0$ *such that for* $z = \alpha x + \beta \log x$*,*

$$M(z, x) = \mathbf{O}(r^x/x^2),$$

as $x \to \infty$*.*

Proof. The number of $\wp$'s such that $\sigma_{\wp,q} \in \mathcal{C}_q$ with $\deg q > z$, and $\deg \wp = x$, is bounded by $\mathbf{O}(r^{(x-z)(1+d/t)})$ by Proposition 17.

Notice that

$$x - z = (1 - (2d\tilde{d} + 2d - 2)^{-1})x - (\beta - 2/\log r)\log x.$$

This error is bounded by $\mathbf{O}(r^{(1-\alpha)x(1+d/t)} \cdot x^{-\log r\beta(1+d/t)})$. Thus if $t \geqslant 2d^2\tilde{d} + 2d^2 - 3d$ and β is large enough, this error becomes $\mathbf{O}(r^x/x^2)$.

Combining Propositions 18, 20 and 19, to bound the error, and Propositions 12, 14 and 16, we get:

THEOREM 9. *Let the rank of* Γ *be* t *and suppose that* $t \geqslant 2d^2\tilde{d} + 2d^2 - 3d$*. Then there exists a non-negative real constants* $C_{\phi,\Gamma}(i)$*, where* $i \in \{0, 1, \ldots, r^* - 1\}$ *such that as* $x \equiv i \pmod{r^*}$*,*

$$N_\Gamma(x) = C_{\phi,\Gamma}(i)\frac{r^x}{x} + \mathbf{O}\left(\frac{r^x \log x}{x^2}\right).$$

8. *Positivity of constants*

Let us first describe a general situation, then we may try to fit the constants of Theorem 2 into this situation. Let us suppose that $\mathcal{L}$ is an indexing set for a collection of pairs $\{(\mathcal{C}_\ell, K_\ell)\}_{\ell\in\mathcal{L}}$ where K_ℓ are Galois extensions of K and $\mathcal{C}_\ell$ is a subset of $\operatorname{Gal}(K_\ell/K)$ closed under conjugation. For a finite subset $\varnothing \neq U \subset \mathcal{L}$ define

$$K_U = \prod_{\ell\in U} K_\ell, \;\; \mathcal{C}_U = \{\sigma \in \operatorname{Gal}(K_U/K) : \sigma|_{K_\ell} \in \mathcal{C}_\ell \text{ for all } \ell \in U\}, \;\; \mu(U) = (-1)^{|U|}$$

and set $\mathbb{F}(U)$ to be the constant field of K_U with $r(U) = [\mathbb{F}(U) : \mathbb{F}_r]$ to be the degree of the constant field of K_U over $\mathbb{F}_r$. If $U = \varnothing$ set $K_\varnothing = K$ and define the other symbols similarly. For each congruence class $[0], [1], \ldots, [r(U) - 1]$ modulo $r(U)$ let $G_{i,U}$ be the subset of $\operatorname{Gal}(K_U/K)$ which restricts to the ith power of the Frobenius on $\mathbb{F}(U)/\mathbb{F}_r$. Notice that if $U = \varnothing$ then $G_{i,\varnothing} = \varnothing$ whenever i is not a multiple of the degree of the constant field of K over $\mathbb{F}_r$. In this case, automatically the entire constant is equal to zero. We are interested in computing the following constant related to the collection. Let

$$\delta(\{(\mathcal{C}_\ell, K_\ell)\}_{\ell\in\mathcal{L}})(i) = \sum_{\substack{U\subset\mathcal{L}\\|U|<\infty}} \mu(U)r(U)|\mathcal{C}_U \cap G_{i,U}|[K_U : K]^{-1},$$

if it converges absolutely.

THEOREM 10. *Let* $\{(\mathcal{C}_\ell, K_\ell)\}_{\ell\in\mathcal{L}}$ *be a family of mutually disjoint Galois extensions of* K*, such that the following conditions hold*:

(i) *the numbers* $r(U)$ *obtain a maximum value of* r^**;*

(ii) *for every* $\ell \in \mathcal{L}$*,* $\mathcal{C}_\ell \neq \operatorname{Gal}(K_\ell/K)$*;*

(iii) *the series* $\sum_{\substack{U\subset\mathcal{L}\\|U|<\infty}} |\mathcal{C}_U|[K_U : K]^{-1}$ *converges.*

Then

$$\delta(\{(\mathcal{C}_\ell, K_\ell)\}_{\ell\in\mathcal{L}})(i) = r(\varnothing)\left|G_{i,\varnothing}\right|\prod_{\ell\in\mathcal{L}}\left(1-\frac{r(\ell)|\mathcal{C}_\ell\cap G_{i,\ell}|}{r(\varnothing)[K_\ell : K]}\right),$$

and this constant is positive for at least one congruence class modulo r^*.

Proof. We need to show that if $U_1, U_2 \subset \mathcal{L}$ and $U_1 \cap U_2 = \varnothing$ then

$$\begin{aligned}[K_{U_1\cup U_2} : K] &= [K_{U_1} : K][K_{U_2} : K]\\ r(U_1\cup U_2)r(\varnothing) &= r(U_1)r(U_2)\\ |\mathcal{C}_{U_1\cup U_2}\cap G_{i,U_1\cup U_2}| &= |\mathcal{C}_{U_1}\cap G_{i,U_1}||\mathcal{C}_{U_2}\cap G_{i,U_2}|.\end{aligned}$$

The first line follows because the extensions are mutually disjoint and Galois (so they are linearly disjoint). The second equation follows from this as well. The third line follows since $\mathrm{Gal}(K_{U_1\cup U_2}/K) \cong \mathrm{Gal}(K_{U_1}/K)\times\mathrm{Gal}(K_{U_2}/K)$ and by definition of $\mathcal{C}_{U_1\cup U_2}$.

Now, we must show that at least one of the constants above is positive for some $i \in \{0, 1, \ldots, r^*-1\}$. As the numbers $r(U)$ obtain a maximum, we must have that $r(\ell) = r(\varnothing)$ for all $\ell \in \mathcal{L}$ except for finitely many. For these ℓ, we have $G_{i,\ell} = \mathrm{Gal}(K_\ell/K)$ as long as $r(\varnothing)|i$, and since $\mathcal{C}_\ell \neq \mathrm{Gal}(K_\ell/K)$ the product corresponding to these ℓ will be positive. We just have to make sure that each the term in the product corresponding to ℓ with $r(\ell) \neq r(\varnothing)$ is positive for some multiple of $r(\varnothing)$.

So, write out these exceptional ℓ as $\ell_1, \ell_2, \ldots, \ell_n$. We must find at least one i such that $|G_{i,\varnothing}| = 1$ and $\mathcal{C}_\ell$ does not contain all the Galois automorphisms which restrict down to ith powers of the Frobenius when restricted to the constant field of K_ℓ. Since $\mathcal{C}_\ell \neq \mathrm{Gal}(K_\ell/K)$ there exists $i_1, i_2, \ldots, i_k$ such that $r(\varnothing)|r(\{\ell_j\})$ and if $x \equiv i_j \mod r(\{\ell_j\})$ then $r(\{\ell_j\})|\mathcal{C}_{\{\ell_j\}}\cap G_{x,\{\ell_j\}}| < r(\varnothing)[K_{\{\ell_j\}} : K]$.

So let $x = x_0 r(\varnothing)$ and consider the simultaneous congruences

$$\begin{aligned}x_0 &\equiv \frac{i_1}{r(\varnothing)} \mod \frac{r(\{\ell_1\})}{r(\varnothing)}\\ x_0 &\equiv \frac{i_2}{r(\varnothing)} \mod \frac{r(\{\ell_2\})}{r(\varnothing)}\\ &\vdots\\ x_0 &\equiv \frac{i_n}{r(\varnothing)} \mod \frac{r(\{\ell_n\})}{r(\varnothing)}.\end{aligned}$$

By the Chinese remainder theorem, this gives a congruence class modulo r^* for which the density is positive.

THEOREM 11. *Let $\mathfrak{C} = \{(\mathcal{C}_\ell, K_\ell)\}_{\ell\in\mathcal{L}}$ be a collection of pairs of finite Galois extensions K_ℓ/K and subsets $\mathcal{C}_\ell$ of* $\mathrm{Gal}(K_\ell/K)$ *which are closed under conjugacy. Suppose that*:

(i) *the numbers $r(U)$ obtain a maximum value of r^*;*

(ii) *there exists a finite subset $\hat{U}$ of $\mathcal{L}$ such that the collection $\{(\mathcal{C}_\ell, K_\ell)\}_{\ell\in\mathcal{L}\setminus\hat{U}}$ satisfies the conditions of Theorem* 10.

Then there exists a finite subset $\mathfrak{L}$ of $\mathcal{L}$ such that

$$\delta(\mathfrak{C})(i) = \delta(\{(\mathcal{C}_\ell, K_\ell)\}_{\ell\in\mathfrak{L}})(i)\delta(\{(\mathcal{C}_\ell, K_\ell)\}_{\ell\in\mathcal{L}\setminus\mathfrak{L}})(i),$$

and if $\delta(\mathfrak{C})(i) = 0$ then there are only a finite number of primes $\wp$ with $\deg\wp \equiv i \mod r^*$ such that $\sigma_{\wp,\ell} \notin \mathcal{C}_\ell$ for all $\ell \in \mathfrak{L}$.

Proof. Let us construct the set $\mathfrak{L}$ by first setting $\hat{U} \subset \mathfrak{L}$. We will add in the fields that are not linearly disjoint with everything in $\hat{U}$ to $\mathfrak{L}$ and then see that we get a finite set. Set

$$\mathfrak{L} = \{\ell \in \mathcal{L} : K_\ell \bigcap K_{\hat{U}} \neq K\}.$$

Why is $\mathfrak{L}$ finite? This is because there are a finite number of possibilities for $K_\ell \bigcap K_{\hat{U}}$ and we must have for every pair of $\ell_1 \neq \ell_2 \in \mathcal{L} \setminus \hat{U}$

$$(K_{\{\ell_1\}} \bigcap K_{\hat{U}}) \bigcap (K_{\{\ell_2\}} \bigcap K_{\hat{U}}) = K.$$

Now, consider the set of primes

$$\{\wp \text{ prime, unramified in } K_{\mathfrak{L}} : \sigma_{\wp, K_\ell} \notin \mathcal{C}_\ell \text{ for any } \ell \in \mathfrak{L}\},$$

and by the Chebotarev density theorem, this set has about $\delta(\{(\mathcal{C}_\ell, K_\ell)\}_{\ell \in \mathfrak{L}})(i) r^x / x$ as $x \equiv i \pmod{r^*}$ elements of degree x and as $x \to \infty$. Now, recall that the lift of a set that is closed under conjugation is still closed under conjugation, and the union of sets that are closed under conjugation is still closed under conjugation. Therefore, there exists a conjugacy class $\mathcal{C}'_{\mathfrak{L}}$ such that $\sigma \in \mathcal{C}'_{\mathfrak{L}}$ if and only if $\sigma|_{K_\ell} \notin \mathcal{C}_\ell$ for all $\ell \in \mathfrak{L}$. Therefore, the above set of primes is equal to

$$\{\wp \text{ prime, unramified in } K_{\mathfrak{L}} : \sigma_{\wp, K_{\mathfrak{L}}} \in \mathcal{C}'_{\mathfrak{L}}\}.$$

Now, if the above set has density zero then by the Chebotarev density theorem there are no unramified primes in $K_{\mathfrak{L}}$ for which $\sigma_{\wp, K_\ell} \notin \mathcal{C}_\ell$ for all $\ell \in \mathfrak{L}$. This ends the proof.

THEOREM 12. *If the fields M_ℓ are mutually disjoint and $\mathcal{C}_\ell \neq \mathrm{Gal}\,(M_\ell/K)$ for all ℓ then $C_{\phi,\Gamma}(i) > 0$ for at least one i.*

Proof. This theorem follows from Theorem 10.

In particular, we have the following result, obtained by assuming that our Drinfeld module is similar to a Serre curve.

COROLLARY 1. *If the Drinfeld module ϕ satisfies $\mathrm{Gal}\,(K(\phi[\ell])/K) \cong \mathrm{GL}_d(A/\ell)$ for all ℓ then $C_{\phi,\Gamma}(i) > 0$ for at least one i.*

THEOREM 13. *Suppose that by excluding finitely many primes ℓ the fields M_ℓ become mutually linearly disjoint over K. Then for each $i \in \{0, 1, \ldots, r^* - 1\}$ either $N_\Gamma(x) = \mathbf{O}(1)$ as $x \equiv i \mod r^*$ or $C_{\phi,\Gamma}(i) > 0$. In particular, this holds when $\mathrm{End}\,(\phi) = \mathrm{End}_K(\phi)$ (that is, when all the endomorphisms are defined over K).*

If $\mathrm{End}\,(\phi) = \mathrm{End}_{K'}(\phi) \neq \mathrm{End}_K(\phi)$ then the fields $K'M_\ell$ are mutually linearly disjoint over K' after excluding finitely many primes. Hence, the number of primes of K which split completely in K' and contribute to $N_\Gamma(x)$ are $\mathbf{O}(1)$ or have positive density.

Proof. If $\mathrm{End}\,(\phi) = \mathrm{End}_K(\phi)$, then we want to check the conditions of Theorem 11 where the collections are the extensions M_ℓ and $\mathcal{C}_\ell \subseteq \mathrm{Gal}\,(M_\ell/K)$. If $\mathrm{End}\,(\phi) \neq \mathrm{End}_K(\phi)$ then we want to check the same conditions, but with M_ℓ replaced with $K'M_\ell$ and K replaced with K'. So we need to find a finite set $\hat{U}$ outside of which everything is mutually disjoint (and also that $\mathcal{C}_\ell \neq \mathrm{Gal}\,(M_\ell/K)$, or $\mathcal{C}_\ell \neq \mathrm{Gal}\,(K'M_\ell/K')$), this is Theorem 6 That the numbers $r(U)$ are bounded follows from Proposition 8. Proposition 15 implies that the constant converges absolutely.

Let us now suppose that $\mathrm{End}\,(\phi) = \mathrm{End}_K(\phi)$. Now, if $\mathcal{C}_\ell \neq \mathrm{Gal}\,(K_\ell/K)$ for all ℓ, then we can apply Theorem 11 to get a finite set $\mathfrak{L}$ such that $C_{\phi,\Gamma}(i)$ is a product of

$\delta(\{(\mathcal{C}_\ell, M_\ell)\}_{\ell\in\mathfrak{L}})(i)$ and $\delta(\{(\mathcal{C}_\ell, M_\ell)\}_{\ell\in\mathcal{L}\setminus\mathfrak{L}})(i)$, where the second δ is positive and the first δ is a finite sum. The trick is now to notice that the first δ is zero if and only if there is some arithmetic obstruction to Γ being primitive. We can see this by constructing a monster conjugacy class of $\mathrm{Gal}\,(M_{\mathfrak{L}}/K)$ to represent the density. Therefore if the main constant is not positive, this monster conjugacy class is equal to $\mathrm{Gal}\,(M_{\mathfrak{L}}/K)$ and so there are $\mathbf{O}(1)$ primes which contribute to $N_\Gamma(x)$.

If now $\mathrm{End}\,(\phi) \neq \mathrm{End}_K(\phi)$, we restrict ourselves to primes of K which split completely in K'. We are now reduced to counting those primes $\wp$ of K' of first-degree over K, for which $\sigma_\wp \notin \mathcal{C}'_\ell \subseteq \mathrm{Gal}\,(K'M_\ell/K')$ for all primes ℓ of A. Again, there is a proportion of primes for which this happens, and the proportion factors as $\delta(\{\mathcal{C}'_\ell, K'M_\ell\}_{\ell\in\mathfrak{L}})(i)$ and $\delta(\{(\mathcal{C}'_\ell, K'M_\ell)\}_{\ell\in\mathcal{L}\setminus\mathfrak{L}})(i)$ just as above. Now, if the first constant is zero it may be possible that the number of primes for which Γ is primitive is infinite, but there will be only a finite number which also split completely in K'. If the first constant is positive, then we get a positive proportion of primes of K which split completely in K' and for which Γ is primitive.

Acknowledgments. The research and writing of this work was partially completed as part of the Ph.D. thesis of the second author. The authors also wish to thank the referee for many useful insights and improvements to this paper.

REFERENCES

[1] A. Akbary and D. Ghioca. Periods of orbits modulo primes. *J. Number Theory.* **129** (2009), no. 11, 2831–2842.

[2] A. Akbary, D. Ghioca and V. Kumar Murty. Reductions of points on elliptic curves. *Math. Ann.* **347** (2010), no. 2, 365–394.

[3] G. W. Anderson and D. S. Thakur. Tensor powers of the Carlitz module and zeta values. *Ann. of Math.* (2) **132** (1990), no. 1, 159–191.

[4] M. I. Bašmakov. Cohomology of Abelian varieties over a number field. *Upsehi Mat. Nauk.* **27** (1972), no. 6(168), 25–66.

[5] Y.-M. J. Chen and J. Yu. On primitive points of elliptic curves with complex multiplication. *J. Number Theory.* **114** (2005), no. 1, 66–87.

[6] V. G. Drinfel'd. Elliptic modules. *Mat. Sb. (N.S.)* **94(136)** (1974), 594–627, 656.

[7] M. D. Fried and M. Jarden. *Field arithmetic (3rd edition).* Ergeb. Math. Grenzeb. 3. Folge. A Series of Modern Surveys in Mathematics vol. 11 (Springer-Verlag, Berlin, 2008, Revised by Jarden).

[8] F. Gardeyn. Une borne pour l'action de l'inertie sauvage sur la torsion d'un module de Drinfeld. *Arch. Math. (Basel)* **79** (2002), no. 4, 241–251.

[9] D. Goss. *Basic structures of function field arithmetic.* Ergeb. Math. Grenzeb. (3) vol. 35 (Springer-Verlag, Berlin, 1996).

[10] R. Gupta and M. Ram Murty. Primitive points on elliptic curves. *Compositio Math.* **58** (1986), no. 1, 13–44.

[11] S. Häberli. Kummer theory of Drinfeld modules. Master's thesis. Eidgenössiche Technische Hochschule Zürich (2011).

[12] C. Hall and J. F. Voloch. Towards Lang–Trotter for elliptic curves over function fields. *Pure Appl. Math. Q.* **2** (2006), no. 1, 163–178.

[13] D. Hayes. Explicit class field theory in global function fields. *In Studies in Algebra and Number Theory.* Adv. in Math. Suppl. Stud. vol. 6 (Academic Press, New York, 1979), pp. 173–217.

[14] C.-N. Hsu. On Artin's conjecture for the Carlitz module. *Compositio Math.* **106** (1997), no. 3, 247–266.

[15] C.-N. Hsu and J. Yu. On Artin's conjecture for rank one Drinfeld modules. *J. Number Theory.* **88** (2001), no. 1, 157–174.

[16] S. Lang. *Algebra (3rd edition).* Grad. Texts Math. vol. 211 (Springer-Verlag, New York, 2002).

[17] S. Lang and H. Trotter. Primitive points on elliptic curves. *Bull. Amer. Math. Soc.* **83** (1997), no. 2, 289–292.

[18] S. Lang and A. Weil. Number of points of varieties in finite fields. *Amer. J. Math.* **76** (1954), 819–827.

[**19**] A. LI. A note on Kummer theory of division points over singular Drinfeld modules. *Bull. Austral. Math. Soc.* **64** (2001), no. 1, 15–20.

[**20**] R. PINK and E. RÜTSCHE. Image of the group ring of the Galois representation associated to Drinfeld modules. *J. Number Theory* **129** (2009), no. 4, 866–881.

[**21**] R. PINK. Kummer theory for Drinfeld modules. arXiv preprint arXiv:1202.4732 (2012).

[**22**] B. POONEN. Local height functions and the Mordell–Weil theorem for Drinfel'd modules. *Compositio Math.* **97** (1995), no. 3, 349–368.

[**23**] K. A. RIBET. Dividing rational points on Abelian varieties of CM-type. *Compositio Math.* **33** (1976), no. 1, 69–74.

[**24**] K. A. RIBET. Kummer theory on extensions of abelian varieties by tori. *Duke Math. J.* **46** (1979), no. 4, 745–761.

[**25**] M. ROSEN. *Number theory in function fields.* Grad. Texts Math. vol. 210 (Springer–Verlag, New York, 2002).

[**26**] J.-P. SERRE. *Local fields.* Graduate Texts in Math. vol. 6 (Springer–Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg).