Universität des Saarlandes

Fachrichtung 6.1 – Mathematik

Preprint Nr. 368

The Galois image of twisted Carlitz modules

Ernst-Ulrich Gekeler

Saarbrücken 2015

Fachrichtung 6.1 – Mathematik
Universität des Saarlandes

Preprint No. 368
submitted: October 13, 2015

The Galois image of twisted Carlitz modules

Ernst-Ulrich Gekeler

Saarland University
Department of Mathematics
Campus E2 4
66123 Saarbrücken
Germany
gekeler@math.uni-sb.de

Edited by
FR 6.1 – Mathematik
Universität des Saarlandes
Postfach 15 11 50
66041 Saarbrücken
Germany

Fax: + 49 681 302 4443
e-Mail: preprint@math.uni-sb.de
WWW: http://www.math.uni-sb.de/

THE GALOIS IMAGE OF TWISTED CARLITZ MODULES

ERNST-ULRICH GEKELER

ABSTRACT. We determine the defect $\mathrm{def}(\Delta, N)$, i.e., the deviation from surjectivity of the attached Galois representation, and the degree $f(\Delta, N)$ of the constant field extension in the N-th torsion field of the twisted Carlitz module with discriminant Δ, where $\Delta, N \in A = \mathbb{F}_q[T]$.

MSC: primary 11G09, secondary 11R32, 11R60

Keywords: Drinfeld module, twisted Carlitz module,
Galois representation

0. Introduction

Let $A = \mathbb{F}_q[T]$ be the polynomial ring over a finite field $\mathbb{F}_q$ with field of fractions $K = \mathbb{F}_q(T)$. A Drinfeld A-module ϕ of rank $r \in \mathbb{N}$ over a finite field extension F of K provides a Galois representation $\pi = \pi(\phi)$ of the absolute Galois group $\mathrm{Gal}(F) = \mathrm{Gal}(F^{\mathrm{sep}}|F)$ in the Tate module $T(\phi)$, a free $\hat{A}$-module of rank r, where

$$\hat{A} = \varprojlim_{N \in A} A/N \xrightarrow{\cong} \prod_{P \text{ prime of } A} A_P \tag{0.1}$$

is the profinite completion of A. Choosing a basis of $T(\phi)$, we have

$$\pi(\phi) : \mathrm{Gal}(F) \longrightarrow \mathrm{GL}(r, \hat{A}).$$

As an immediate consequence of Drinfeld's construction [1], π has open image (i.e., $\mathrm{im}\,\pi(\phi)$ has finite index in the compact group $\mathrm{GL}(r, \hat{A})$) if $r = 1$. This has been generalized to $r \geq 2$ by Pink and Rütsche [5], under the obviously necessary assumption that ϕ has no complex multiplications, that is, if the endomorphism ring $\mathrm{End}(\phi)$ is reduced to A. This is similar to the Tate conjecture for abelian varieties proved by Faltings [2]. While the above results are effective, the bounds for the index of $\mathrm{im}\,\pi(\phi)$ derived from them are rather weak.

In the present paper we give

- an explicit description of $\mathrm{im}\,\pi(\phi)$,
- the degrees of the associated constant field extensions

in the case where $r = 1$ and $F = K$, i.e., when ϕ is a twist $\phi = \rho^{(\Delta)}$ of the Carlitz module ρ over K (see below for precise definitions). The main results are Theorem 3.13 and Theorem 4.11. Crudely simplified versions are as follows.

0.2 Corollary. *The defect of* $\rho^{(\Delta)}$ *over* K, *i.e., the index of* $\operatorname{im}\pi(\rho^{(\Delta)})$ *in* $\mathrm{GL}(1,\hat{A}) = \hat{A}^*$, *is always a divisor of* $q-1$.

0.3 Corollary. *Let* $K(\mathrm{tor}(\rho^{(\Delta)}))$ *be the field extension obtained from* K *by adjoining all the torsion points of* $\rho^{(\Delta)}$. *Then the degree of the algebraic closure of* $\mathbb{F}_q$ *in* $K(\mathrm{tor}(\rho^{(\Delta)}))$ *is a divisor of* $q-1$.

(Both the quantities occurring in (0.2) and (0.3) are specified in Theorem 3.13 and 4.11, respectively.)

Notation.

$A = \mathbb{F}_q[T]$ resp. $K = \mathbb{F}_q(T)$ denotes the ring of polynomials resp. the field of rational functions in the indeterminate T over the finite field $\mathbb{F}_q$ with q elements;
$P, Q, \ldots$ denote places of A, i.e., monic irreducible polynomials in A;
A_P resp. K_P is the completion of A resp. K at P;
$\mathbb{F}_P = A/P =$ field extension of degree $\deg(P)$ of $\mathbb{F}_q$;
$M, N, \ldots$ elements of A, $\mathrm{rad}(N) =$ radical of $N =$ maximal squarefree monic divisor of N;
$\mu_n =$ group of n-th roots of unity in the algebraic closure of $\mathbb{F}_q$, $\mu = \mu_{q-1} = \mathbb{F}_q^*$;
$|X| =$ cardinality of the finite set X;
$A/N = A/(N) =$ residue class ring of A modulo (N), with multiplicative group $(A/N)^*$.

1. The Carlitz module and its twists.

We assume the reader to be familiar with the basic theory of Drinfeld modules as presented e.g. in [3], [6] or [8].

The *Carlitz module* is the Drinfeld A-module ρ over K defined by the operator polynomial

$$\rho_T(X) = TX + X^q \in K[X]. \tag{1.1}$$

Given any $0 \neq N \in A$, we let $\rho_N(X) \in K[X]$ be the N-th division polynomial of ρ (which has degree $q^{\deg(N)}$ in X) with kernel ${}_N\rho$, a free A/N-module of rank one. For non-constant N, we let $K(N) = K({}_N\rho)$ be the splitting field of $\rho_N(X)$. The field extension $K(N)|K$ is strongly analogous with a cyclotomic extension of $\mathbb{Q}$, viz:

(1.2) (i) $K(N)|K$ is abelian with Galois group $\mathrm{Gal}(K(N)|K) \xrightarrow{\cong} (A/N)^*$; if $x \in {}_N\rho$ and $\sigma_{\overline{M}} \in \mathrm{Gal}(K(N)|K)$ corresponds to the class of $M \in A$ coprime with N then $\sigma_{\overline{M}}(x) = \rho_M(x)$;

(ii) if $N = P^k$ is a power of the prime P then P is completely ramified in $K(N)$ and any finite prime Q different from P is unramified in $K(N)$;
(iii) if $N = P_1^{k_1} \cdots P_s^{k_s}$ is the prime factorization of N, $N_i = P_i^{k_i}$, then the $K(N_i)$ are linearly disjoint over K;
(iv) the infinite place of K is tamely ramified in $K(N)$ with decomposition group = ramification group $\mathbb{F}_q^* \hookrightarrow (A/N)^*$;
(v) if the place P of A is coprime with N (hence P is unramified in $K(N)$), then the residue class $\overline{P}$ of P in $(A/N)^*$ is the Frobenius element of $K(N)|K$ at P;
(vi) $\mathbb{F}_q$ is algebraically closed in $K(N)$.
All of this has been shown in [4], see also [3] and [8].

Now let ϕ be another rank-one Drinfeld A-module over K, given by

$$\phi_T(X) = TX + \Delta X^q = \rho_T^{(\Delta)}(X) \in K[X],\ 0 \neq \Delta \in K, \tag{1.3}$$

which we regard as the twist $\rho^{(\Delta)}$ of ρ by Δ. Let $\delta \in K^{\mathrm{sep}}$ be a fixed $(q-1)$-th root of Δ. The Drinfeld modules ρ and $\rho^{(\Delta)}$ become isomorphic over the field $K(\delta)$. As for the Carlitz module ρ, we define

$$_N\rho^{(\Delta)} = \text{kernel of } \rho_N^{(\Delta)}, \tag{1.4}$$

$K^{(\Delta)}(N) = K({}_N\rho^{(\Delta)})$ = the "N-th division field of $\rho^{(\Delta)}$". Similar to (1.2)(i), $K^{(\Delta)}(N)$ is abelian over K, but with Galois group a possibly proper subgroup of $(A/N)^*$. The main purpose of this work is to describe the *defect*

$$\mathrm{def}(\Delta, N) := [(A/N)^* : \mathrm{Gal}(K^{(\Delta)}(N)|K)] \tag{1.5}$$

and to find out how the other statements of (1.2) must be modified for $\rho^{(\Delta)}$. As

$$\rho_T(\delta X) = \delta\rho_T^{(\Delta)}(X)$$

(and similarly $\rho_N(\delta X) = \delta\rho_N^{(\Delta)}(X)$ for arbitrary $N \in A$), multiplication with δ provides an isomorphism $\delta :\ \rho^{(\Delta)} \xrightarrow{\cong} \rho$, or $\delta^{-1} :\ \rho \xrightarrow{\cong} \rho^{(\Delta)}$. In particular,

$$\begin{array}{cccc} \delta^{-1} : & {}_N\rho & \xrightarrow{\cong} & {}_N\rho^{(\Delta)} \\ & x & \longmapsto & \delta^{-1}x \end{array} \tag{1.6}$$

as A-modules. Let $\mathrm{Gal}(K)$ be the absolute Galois group of K and $\pi :\ \mathrm{Gal}(K) \longrightarrow \hat{A}^*$, $\pi^{(\Delta)} :\ \mathrm{Gal}(K) \longrightarrow \hat{A}^*$ be the Galois representations attached to ρ and $\rho^{(\Delta)}$, respectively. That is, for each N, π composed with the natural projective $\hat{A}^* \longrightarrow (A/N)^*$ is the map from $\mathrm{Gal}(K)$ to $(A/N)^*$ described in (1.2)(i), and similarly for $\pi^{(\Delta)}$. Let further

$$\chi^{(\Delta)} :\ \mathrm{Gal}(K) \longrightarrow \mu = \mu_{q-1} = \mathbb{F}_q^* \tag{1.7}$$

be the character $\sigma \longmapsto \sigma(\delta)/\delta$, which is independent of the choice of the $(q-1)$-th root δ.

1.8 Lemma. *With the above notation,* $\pi^{(\Delta)} = \chi^{(\Delta)^{-1}} \otimes \pi$.

Proof. This follows from combining (1.6) and (1.7). $\square$

Using class field theory, we regard $\chi^{(\Delta)}$ as a character of the idèle class group of K, or of a generalized ideal class group. In particular, its value $\chi^{(\Delta)}(P)$ on a prime P unramified in $K(\delta)$ (i.e., P coprime with Δ if Δ is free of $(q-1)$-th powers) is defined.

1.9 Lemma. *Let P be a prime of A coprime with Δ. Then* $\chi^{(\Delta)}|(P) = (\frac{\Delta}{P})_{q-1}$, *where* $(\frac{}{P})_{q-1}$ *is the* $(q-1)$*-th power residue symbol at* P, *cf.* [6] *p.* 24.

Proof. Let K_P be the completion of K at P and $F = F_P$ the Frobenius element at P, acting as $x \longmapsto x^{q^d}$ ($d := \deg(P)$) on the residue class field $\mathbb{F}_P = A/P$. We have

$$K_P(\delta) = K_P(\sqrt[q-1]{\Delta}) = K_P(\sqrt[q-1]{\overline{\Delta}}) = K_P(\overline{\delta}),$$

where $\overline{\Delta}$ is the reduction $(\operatorname{mod} P)$ and $\overline{\delta}^{q-1} = \overline{\Delta}$. Therefore

$$\chi^{(\Delta)}(P) = F(\overline{\delta})/\overline{\delta} = \overline{\delta}^{(q^d-1)} = \overline{\Delta}^{(q^d-1)/(q-1)} = N^{\mathbb{F}_P}_{\mathbb{F}_q}(\overline{\Delta}) = (\frac{\Delta}{P})_{q-1}$$

by definition of the power residue symbol. $\square$

Note that $(\frac{\Delta}{P})_{q-1}$ is related with $(\frac{P}{\Delta})_{q-1}$ through the $(q-1)$-th reciprocity law ([6], Theorem 3.5).

1.10 Corollary. *Let P be a prime of A coprime with N and Δ. Then the Frobenius element of P in* $\operatorname{Gal}(K^{(\Delta)}(N)|K) \hookrightarrow (A/N)^*$ *is* $(\frac{\Delta}{P})^{-1}_{q-1}$ *times the residue class* $\overline{P}$ *of P modulo N.*

Proof. (1.2)(v) + (1.8) + (1.9). $\square$

2. The torsion fields.

We fix the data Δ and N. All the groups H, H_0, R, S that appear below depend on these choices.

As follows from (1.6), the field $K^{(\Delta)}(N)$ is contained in the compositum $K(N)(\delta)$ of $K(N)$ and the Kummer extension $K(\delta)$ of K. Now

$$H := \operatorname{Gal}(K(\delta)|K) \hookrightarrow \mu = \mathbb{F}_q^* \tag{2.1}$$

is the image of $\chi^{(\Delta)}$, and equals μ if and only if Δ is not a d-th power for any divisor $d > 1$ of $q-1$. By Galois theory,

$$G := \operatorname{Gal}(K(N)(\delta)|K) \tag{2.2}$$

is a well-defined subgroup of $\operatorname{Gal}(K(N)|K) \times \operatorname{Gal}(K(\delta)|K) = (A/N)^* \times H$. For an element $(\overline{M}, \eta)$ of G (where $\overline{M}$ is the residue class of M

modulo N) we have:

$$
\begin{aligned}
&(\overline{M},\eta) \text{ acts trivially on } K^{(\Delta)}(N)\\
&\Leftrightarrow \forall\, y \in {}_N\rho^{(\Delta)} :\ (\overline{M},\eta)(y) = y\\
&\Leftrightarrow \forall\, x \in {}_N\rho :\ (\overline{M},\eta)(\tfrac{x}{\delta}) = (\tfrac{x}{\delta})\\
&\Leftrightarrow \forall\, x \in {}_N\rho :\ \sigma_{\overline{M}}(x)(\eta\cdot\delta)^{-1} = x\delta^{-1}\\
&\Leftrightarrow \forall\, x \in {}_N\rho :\ \rho_M(x) = \eta\cdot x,
\end{aligned}
$$

since by (1.7) and (2.1), $\eta \in H$ acts on δ through multiplication by η. This means that $\overline{M}$ as an element of $(A/N)^*$ agrees with $\eta \in H \hookrightarrow \mathbb{F}_q^* \hookrightarrow (A/N)^*$. We thus get the following result.

2.3 Proposition. *Let $R \subset G$ be the Galois group of $K(N)(\delta)$ over $K^{(\Delta)}(N)$. Then $R = \{(\overline{M},\eta) \in G \mid \overline{M} = \eta\}$, and $\mathrm{Gal}(K^{(\Delta)}(N)|K)$ equals the image in $(A/N)^*$ of the homomorphism*

$$
\begin{array}{ccc}
G & \longrightarrow & (A/N)^* \\
(\overline{M},\eta) & \longmapsto & \eta^{-1}\overline{M}
\end{array}\ . \qquad \square
$$

We don't know yet the group G, but it consists of certain elements of shape $(\overline{M},\eta)$ and fits into the diagram with exact row and column

(2.4)

$$
\begin{tikzcd}
 & & 1 \arrow[d] & & & \\
 & & \{(1,\eta)\in G\} \arrow[d] & & & \\
1 \arrow[r] & \{(\overline{M},\eta)\in G|\overline{M}=\eta\} = R \arrow[r] & G \arrow[rr] \arrow[ddd] & & \mathrm{Gal}\big(K^{(\Delta)}(N)|K\big) \arrow[r] & 1 \\
 & & & (\overline{M},\eta) \arrow[r, mapsto] \arrow[d, mapsto] & \eta^{-1}\overline{M} & \\
 & & & \overline{M} & & \\
 & & (A/N)^* \arrow[r, equal] \arrow[d] & \mathrm{Gal}(K(N)|K) & & \\
 & & 1 & & &
\end{tikzcd}
$$

Thus we can read off:

2.5 Corollary. $\mathrm{def}(\Delta,N) := [(A/N)^* : \mathrm{Gal}(K^{(\Delta)}(N)|K)]$ *is a divisor of $q-1$.* $\square$

2.6 Corollary. $\mathrm{def}(\Delta, N) = 1$ *if* $K(N)$ *and* $K(\delta)$ *are linearly disjoint. This happens in particular if* Δ *is a constant.*

Proof. If $K(N)$ and $K(\delta)$ are linearly disjoint then $G = \mathrm{Gal}(K(N)|K) \times \mathrm{Gal}(K(\delta)|K)$, so by (2.4) the groups $\mathrm{Gal}(K(N)|K)$ and $\mathrm{Gal}(K^{(\Delta)}(N)|K)$ have the same order. The second assertion comes from (1.2)(vi). $\square$

(2.7) We define the groups $H_0 := \mathrm{Gal}(K(\delta)|K(\delta) \cap K(N)) \subset H$ and $S := \mathrm{Gal}(K(\delta) \cap K(N)|K)$. If $h := |H|$ and $h_0 := |H_0|$, then $H = \mu_h$, $H_0 = \mu_{h_0}$, $S = \mu_{h/h_0}$, and the restriction map $\psi : H \longrightarrow S$ is the raising to the h_0-th power in H. Let

$$\varphi : \mathrm{Gal}(K(N)|K) = (A/N)^* \longrightarrow S$$

be the other restriction map, induced from $K(\delta) \cap K(N) \hookrightarrow K(N)$. Then

$$G = \{(\overline{M}, \eta) \in (A/N)^* \times H \mid \varphi(\overline{M}) = \psi(\eta)\},$$

and has order $|G| = h_0|(A/N)^*|$. Via $H \hookrightarrow \mu = \mathbb{F}_q^* \hookrightarrow (A/N)^*$ we consider H as a subgroup of $(A/N)^*$. Then

$$\begin{aligned} |R| &= |\{(\overline{M}, \eta) \in G \mid \overline{M} = \eta\} = |\{\eta \in H \mid \varphi(\eta) = \psi(\eta)\}| \\ &= |\ker(\psi\varphi^{-1}|_H)|. \end{aligned}$$

As $H_0 \subset \ker(\psi\varphi^{-1}|_H)$, h_0 divides $|R|$, which in turn divides h. Comparison with (2.4) finally yields

$$\mathrm{def}(\delta, N) = [(A/N)^* : \mathrm{Gal}(K^{(\Delta)}(N)|K)] = \frac{|R|}{h_0}, \tag{2.8}$$

which in any case is a divisor of $|S| = h/h_0$.

(2.9) As the kernel of $(A/N)^* \longrightarrow (A/\mathrm{rad}(N))^*$ is a p-group ($p := \mathrm{char}(\mathbb{F}_q)$) and $(A/\mathrm{rad}(N))^*$ is p-free, the field $K(\delta) \cap K(N)$ is already contained in $K(\mathrm{rad}(N))$, and the map φ of (2.7) factors over $(A/\mathrm{rad}(N))^*$. This shows that the canonical map

$$(A/N)^*/\mathrm{Gal}(K^{(\Delta)}(N)|K) \longrightarrow (A/\mathrm{rad}(N))^*/\mathrm{Gal}(K^{(\Delta)}(\mathrm{rad}(N))|K)$$

is in fact an isomorphism. Thus:

2.10 Proposition. *The defects* $\mathrm{def}(\Delta, N)$ *and* $\mathrm{def}(\Delta, \mathrm{rad}(N))$ *agree.* $\square$

3. The defect of $\rho^{(\Delta)}$.

As the isomorphism type of $\rho^{(\Delta)}$ depends only on the class of $\Delta \in K^*$ in $K^*/(K^*)^{q-1}$, we assume from now on that Δ is integral, i.e., $\Delta \in A \setminus \{0\}$, and not divisible by $(q-1)$-th powers. Let $c \in \mathbb{F}_q^*$ be a fixed primitive $(q-1)$-th root of unity. Then we may write

$$\Delta = c^{k_0} P_1^{k_1} \cdots P_s^{k_s} \tag{3.1}$$

with different monic primes P_i of A of degrees $d_i = \deg\ P_i$, and $0 \leq k_i < q-1$ for $0 \leq i \leq s$, with $0 < k_i$ if $i > 0$. We arrange them in such a way that $P_1, \ldots, P_r$ divide N $(r \leq s)$ and $P_{r+1}, \ldots, P_s$ are coprime with N. Note that $s = 0$, i.e., Δ constant, is allowed.

We next must identify the Kummer extensions $K(\delta) = K(\sqrt[q-1]{\Delta})$ in the framework of Carlitz torsion fields. Let for the moment P be a fixed monic prime in A, of degree d, and $\tilde{P} = (-1)^d P$.

3.2 Lemma. *The unique subfield in $K(P)$ of degree $q-1$ over K is the Kummer extension $K(\sqrt[q-1]{\tilde{P}})$.*

Proof. Dinesh Thakur in [7] constructed d Gauß sums g_j $(1 \leq j \leq d)$ such that $(\prod_{1 \leq j \leq d} g_j)^{q-1} = (-1)^d P = \tilde{P}$. The different g_j lie in the d-th constant field extension $K(P)\mathbb{F}_P$ of $K(P)$ by $\mathbb{F}_P = A/P \cong \mathbb{F}_{q^d}$, while their product

$$\mathbf{G}_P := \prod_{1 \leq j \leq d} g_j \tag{3.2.1}$$

lies in $K(P)$. For ramification reasons, $[K(\mathbf{G}_P) : K] = q-1$, which shows the assertion. $\square$

For later use, we recall the transformation formula, where $N_{\mathbb{F}_q}^{\mathbb{F}_P} : \mathbb{F}_P \longrightarrow \mathbb{F}_q$ denotes the norm map:

$$\sigma_{\overline{M}}(\mathbf{G}_P) = N_{\mathbb{F}_q}^{\mathbb{F}_P}(\overline{M}) \cdot \mathbf{G}_P \tag{3.3}$$

for $\overline{M} \in \mathbb{F}_P^* = (A/P)^* = \mathrm{Gal}(K(P)|K)$, which follows from [7], Theorem I (or may be checked directly).

In view of the above, we define for $\mathbf{k} = (k_1, \ldots, k_s) \in \mathbb{N}^s$

$$\mathbf{G}_{\mathbf{k}} := \prod_{1 \leq i \leq s} \mathbf{G}_{P_i}^{k_i}. \tag{3.4}$$

As immediate consequences of (3.2) and (3.3), the following hold:

(3.5)(i) $\mathbf{G}_{\mathbf{k}} \in K(\mathrm{rad}(\Delta))$ (if Δ is as in (3.1));
(ii) $\mathbf{G}_{\mathbf{k}}^{q-1} = (-1)^d \prod_{1 \leq i \leq s} P_i^{k_i}$, where $d := \sum_{1 \leq i \leq d} k_i d_i$ is the degree $\deg(\Delta)$ of Δ;
(iii) $\sigma_{\overline{M}}(\mathbf{G}_{\mathbf{k}}) = \lambda_{\mathbf{k}}(\overline{M}) \cdot \mathbf{G}_{\mathbf{k}}$, where $\sigma_{\overline{M}} \in \mathrm{Gal}(K(\Delta)|K) = (A/\Delta)^*$ is the class of $M \in A$, Δ non-constant and coprime with M. Here $\lambda_{\mathbf{k}}$ is the μ-valued character

$$\begin{array}{rccc} \lambda_{\mathbf{k}} : & (A/\Delta)^* & \longrightarrow & \mu \\ & \overline{M} & \longmapsto & \prod_{1 \leq i \leq s} \nu_i^{k_i}(\overline{M}) \end{array} \tag{3.6}$$

with the canonical maps

$$\begin{array}{rcccl} \nu_i: (A/\Delta)^* & \longrightarrow & (A/P_i)^* & \longrightarrow & \mathbb{F}_q^* = \mu\,. \\ & & x & \longmapsto & N_{\mathbb{F}_q}^{\mathbb{F}_{P_i}}(x) \end{array}$$

Note that $\lambda_{\mathbf{k}}$ factors over $(A/\mathrm{rad}(\Delta))^*$.

Thus we can realize the field $K(\delta) = K(\sqrt[q-1]{\Delta})$ as a Kummer subextension of $K(\Delta)$ or even of $K(\mathrm{rad}(\Delta))$, provided that $c^{k_0} = (-1)^d$. It remains to generalize this to arbitrary scalars c^{k_0}. Let γ be a $(q-1)$-th root of c (so it is a primitive $(q-1)^2$-th root of unity). Then $\delta^* := \gamma^{k_0}\mathbf{G}_{\mathbf{k}}$ satisfies $(\delta^*)^{q-1} = (-1)^d\Delta$. Therefore we put

$$(3.7) \qquad k_0^* = \begin{cases} k_0, \text{ if } q \text{ or } d = \deg\Delta \text{ is even,} \\ \text{the unique } k \equiv k_0 + (q-1)/2 \pmod{q-1} \text{ with} \\ 0 \le k < q-1, \text{ otherwise.} \end{cases}$$

Then $\delta := \gamma^{k_0^*}\mathbf{G}_{\mathbf{k}}$ is a $(q-1)$-th root of Δ.

3.8 Lemma. *(i) The degree $h = [K(\delta) : K]$ equals*

$$(q-1)/\gcd(q-1, k_0, k_1, \ldots, k_s) = (q-1)/\gcd(q-1, k_0^*, k_1, \ldots, k_s).$$

(ii) The degree $h_0 = [(K(\delta) \cap K(N) : K]$ is given by

$$h_0 = (q-1)/\gcd(q-1, k_0^*, k_{r+1}, \ldots, k_s).$$

Proof. (i) The first formula is obvious from (3.1) and Lemma 3.2. The second one (i.e., that k_0 may be replaced by k_0^*) can be seen as follows: Suppose that $k_0^* \equiv k_0 + (q-1)/2 \pmod{q-1}$. Then at least one of $k_1, k_2, \ldots, k_s$ is odd and $q-1$ is even. Let $g := \gcd(k_1, \ldots, k_s)$, which is odd, so 2 is invertible modulo g. Hence the ideal $(q-1)$ generated by $q-1$ in $\mathbb{Z}/(g)$ equals the ideal generated by $(q-1)/2$, which gives $\gcd((q-1), k_0, k_1, \ldots, k_s) = \gcd(q-1, k_0, g) = \gcd((q-1)/2, k_0, g) = \gcd((q-1/2, k_0^*, g) = \gcd(q-1, k_0^*, k_1, \ldots, k_s)$.
(ii) The field $K(\delta) \cap K(N)$ is the Kummer extension of K generated by δ^{h_0}. Some power δ^n lies in $K(N)$ if and only if the following conditions are satisfied:

$$(3.8.1) \qquad \begin{array}{rcl} k_i \cdot n & \equiv & 0 \pmod{q-1},\ r < i \le s, \\ k_0^* \cdot n & \equiv & 0 \pmod{q-1}. \end{array}$$

Therefore,

$$\begin{array}{rcl} h_0 & = & \min\{n \in \mathbb{N} \mid (3.8.1) \text{ holds for } n\} \\ & = & (q-1)/\gcd(q-1, k_0^*, k_{r+1}, \ldots, k_s). \end{array}$$

□

With the notation of (2.7) we have the canonical restriction homomorphisms

$$\begin{aligned} \varphi: &\quad \mathrm{Gal}(K(N)|K) = (A/N)^* \longrightarrow S = \mathrm{Gal}(K(\delta)\cap K(N)|K) = \mu_{h/h_0} \\ \psi: &\quad H = \mathrm{Gal}(K(\delta)|K) = \mu_h \longrightarrow S. \end{aligned}$$

As φ describes the action of $(A/N)^*$ on δ^{h_0}, if is given by

$$\varphi = \lambda_{\mathbf{k}}^{h_0}, \tag{3.9}$$

where $\lambda_{\mathbf{k}}$ is defined in (3.6); raising to the h_0-th power, the components $\nu_i^{k_i}$ with $r < i \leq s$ are annihilated, as is the contribution of the scalar $\gamma^{k_0^* h_0}$, which lies in $\mathbb{F}_q^*$. In more detail, φ is the map

$$\begin{array}{rcl} (A/N)^* \longrightarrow (A/P_1\cdots P_r)^* & \longrightarrow & S = \mu_{h/h_0} \\ x & \longmapsto & \lambda_{\mathbf{k}}^{h_0}(x) = [\prod_{1\leq i\leq r} \nu_i^{k_i}(x)]^{h_0}. \end{array}$$

What is the restriction of φ to $\mathbb{F}_q^* \hookrightarrow (A/N)^*$? First, the map

$$\nu_i:\ (A/N)^* \longrightarrow (A/P_i)^* \xrightarrow{N^{\mathbb{F}_{P_i}}_{\mathbb{F}_q}} \mathbb{F}_q^*$$

acts on $x \in \mathbb{F}_q^*$ as $\nu_i(x) = x^{1+q+\cdots+q^{d_i-1}} = x^{d_i}$. Therefore,

$$\varphi(x) = x^{d'h_0} = x^{dh_0},$$

with $d' = \sum_{1\leq i\leq r} k_i d_i$, since $d'h_0 \equiv (\sum_{1\leq i\leq s} k_i d_i)h_0 = dh_0$ modulo $q-1$, by (3.8.1). As $\psi(x) = x^{h_0}$ for $x \in H$, we find (see (2.7)):

$$\begin{aligned} |R| &= |\ker(\psi\varphi^{-1}|_H)| = |\{x \in \mu_h | x^{h_0 - dh_0} = 1\}| \\ &= \gcd((d-1)h_0, h) = \gcd((d'-1)h_0, h) \end{aligned} \tag{3.10}$$

Plugging into (2.8) and simplifying gives

(3.11)

$$\begin{aligned} &\mathrm{def}(\Delta, N) = |R|/h_0 = \gcd(d'-1, h/h_0) \\ &= \gcd\left(d'-1, \tfrac{\gcd(q-1,k_0^*,k_{r+1},\ldots,k_s)}{\gcd(q-1,k_0^*,k_1,\ldots,k_s)}\right) = \gcd(d'-1, q-1, k_0^*, k_1, \ldots, k_s) \\ &= \gcd(d-1, q-1, k_0^*, k_{r+1}, \ldots, k_s), \end{aligned}$$

where the equality next to the last follows from Lemma 3.12 with $b := \gcd(q-1, k_0^*, k_{r+1}, \ldots, k_s)$, $L := \{k_1, \ldots, k_r\}$. We need the following elementary result.

3.12 Lemma. *Let $b \in \mathbb{N}$ and $L \subset \mathbb{N}$ be a finite subset, $0 < d = \sum_{\ell\in L} d_\ell \cdot \ell$ with non-negative integers d_ℓ. Then*

$$\gcd(d-1, b) = \gcd(d-1, b/\gcd(b, L)).$$

Proof. Obviously the right hand side divides the left hand side. Write $g = \gcd(b, L)$, $b = g \cdot b^*$, $d = g \cdot d^*$. The stated equality is

$$\gcd(gd^* - 1, gb^*) = \gcd(gd^* - 1, b^*).$$

Each divisor t of the LHS must be coprime with g, which shows that it divides the RHS. □

We collect what has been shown.

3.13 Theorem. *Let $\phi = \rho^{(\Delta)}$ be the twisted Carlitz module, where $\Delta = c^{k_0} P_1^{k_1} \cdots P_s^{k_s}$ with a primitive $(q-1)$-th root of unity c and $s \geq 0$ different monic primes P_i of degrees d_i, $0 \leq k_0 < q-1$, $0 < k_i < q-1$ for $1 \leq i \leq s$ and $d = \sum_{1 \leq i \leq s} k_i d_i = \deg \Delta$.*
Let further N be a non-constant element of A and suppose that P_i divides N for $1 \leq i \leq r$ and P_i is coprime with N for $r < i \leq s$. The image of $\mathrm{Gal}(K)$ in $\mathrm{Aut}_A({}_N\rho^{(\Delta)}) = (A/N)^*$ (that is, $\mathrm{Gal}(K^{(\Delta)}(N)|K)$) has index (see (3.7) for k_0^*)

$$\mathrm{def}(\Delta, N) = \gcd(d-1, q-1, k_0^*, k_{r+1}, \ldots, k_s).$$

□

Suppose that M divides N. From the commutative diagram of natural maps

$$\begin{array}{ccc} \mathrm{Gal}(K^{(\Delta)}(N)|K) & \hookrightarrow & (A/N)^* \\ \downarrow & & \downarrow \\ \mathrm{Gal}(K^{(\Delta)}(M)|K) & \hookrightarrow & (A/M)^* \end{array}$$

we see that the quotient by $\mathrm{Gal}(K^{(\Delta)}(N)|K)$ of $(A/N)^*$ is stable as soon as $\mathrm{rad}(N)$ is divisible by $\mathrm{rad}(\Delta)$. This implies (notations and assumptions as in (3.13)):

3.14 Corollary. *The image of $\mathrm{Gal}(K)$ under the representation $\pi^{(\Delta)} : \mathrm{Gal}(K) \longrightarrow (\hat{A})^*$ provided by the twisted Carlitz module $\rho^{(\Delta)}$ is the inverse image in $(\hat{A})^*$ of a subgroup of $(A/\mathrm{rad}(\Delta))^*$ of index*

$$\mathrm{def}(\rho^{(\Delta)}) = \mathrm{def}(\Delta) = \gcd(d-1, q-1, k_0^*).$$

□

Obviously, this is a sharpening of Corollary 0.2 in the Introduction.

As $\mathrm{Gal}(K^{(\Delta)}(N)|K)$ is now known by (2.3) to (2.8) and Theorem 3.13, it is straightforward (though laborious if N and Δ have common divisors) to determine the ramification of $K^{(\Delta)}(N)$ over K. We restrict to stating, without details, the result in the most simple case.

3.15 Example. Suppose that N and Δ are coprime. From considering the ramification we find that $K(N)$ and $K(\delta)$ are linearly disjoint over K, so by Corollary 2.6, $\mathrm{def}(\Delta, N) = 1$, i.e.,

$$\mathrm{Gal}(K^{(\Delta)}(N)|K) \xrightarrow{\cong} (A/N)^*.$$

Furthermore, in this case, the infinite prime of K is tamely ramified in $K^{(\Delta)}(N)$ with ramification group $\mathbb{F}_q^* \hookrightarrow (A/N)^*$. Each prime divisor Q of N is ramified in $K^{(\Delta)}(N)$, with ramification group equal to the canonical subgroup $(A/Q^k)^* \hookrightarrow (A/N)^*$ given by the Chinese Remainder Theorem, if Q^k is the exact Q-divisor of N. Each prime divisor P of Δ is ramified in $K^{(\Delta)}(N)$, with ramification group isomorphic with its ramification group in $K(\delta)|K$, and contained in $\mathbb{F}_q^* \hookrightarrow (A/N)^* \xrightarrow{\cong} \mathrm{Gal}(K^{(\Delta)}(N)|K)$.

4. The constant field extension.

We keep the assumptions of the last section: Δ and N are fixed and subject to (3.1).

(4.1) Let $\mathbb{F}(\Delta, N)$ be the algebraic closure of $\mathbb{F}_q$ in $K^{(\Delta)}(N)$, of degree $f(\Delta, N)$. In this section we determine $f(\Delta, N)$ and also $f(\Delta)$, the degree of the algebraic closure of $\mathbb{F}_q$ in $K(\mathrm{tor}(\rho^{(\Delta)})) = \varinjlim_{N} K^{(\Delta)}(N)$.

(4.2) We next put $\mathbb{F}' = \mathbb{F}_q(\gamma) = \mathbb{F}_{q^{q-1}}$, the extension of degree $q-1$ of $\mathbb{F}_q$, $K' = K \cdot \mathbb{F}' = \mathbb{F}'(T)$, $K'(N) = K(N)\mathbb{F}'$, etc. We identify $\mathrm{Gal}(\mathbb{F}'|\mathbb{F}) \xrightarrow{\cong} \mu$, $\sigma \longmapsto \sigma(\gamma)/\gamma$, through the choice of the primitive $(q-1)$-the root $c \in \mathbb{F}_q^*$ and $\gamma^{q-1} = c$. Then

$$\mathrm{Gal}(K'(N)|K) \xrightarrow{\cong} (A/N)^* \times \mu.$$

As results from definitions, $K^{(\Delta)}(N)$ is contained in $K'(N)(\delta)$. Consider the diagram of subfields

(4.3)
$$\begin{tikzcd}
 & K'(N)(\delta) \arrow[dl, dash] \arrow[d, dash, "R'"] \arrow[dr, dash] & \\
K'(N) \arrow[dd, dash, "(A/N)^*"'] \arrow[dr, dash] \arrow[dddr, dash, "(A/N)^*\times\mu"] & K^{(\Delta)}(N) & K(\delta) \arrow[dl, dash, "H'_0"'] \arrow[dddl, dash, "H"] \\
 & K'(N) \cap K(\delta) \arrow[dd, dash, "S'"] & \\
K' \arrow[dr, dash, "\mu"'] & & \\
 & K &
\end{tikzcd}$$

where each line indicates an inclusion and the group nearby is the Galois group.

We find that

$$G' := \mathrm{Gal}(K'(N)(\delta)|K)$$

is a subgroup of $\mathrm{Gal}(K'(N)|K) \times \mathrm{Gal}(K(\delta)|K) = (A/N)^* \times \mu \times H$ which projects onto the two factors $(A/N)^* \times \mu$ and H. Let μ' be the image of

$$R' := \mathrm{Gal}(K'(N)(\delta) \mid K^{(\Delta)}(N))$$

under the canonical projection to μ. By Galois theory, μ' is the group of K' over $\mathbb{F}(\Delta, N)(T)$. That is

$$f(\Delta, N) = (q-1)/|\mu'|. \tag{4.4}$$

Our strategy is thus to determine R' and its projection to μ, which shows some similarity with our proceeding in Section 3.

First, we obtain $h_0' := |H_0'| = [K(\delta) : K'(N) \cap K(\delta)]$ by a slight modification of the argument of Lemma 3.8: As δ^n lies in $K'(N)$ if and only if

$$k_i n \equiv \pmod{q-1},\ r < i \leq s \tag{3.8.1$'$}$$

holds, we find

$$h_0' = (q-1)/\gcd(q-1, k_{r+1}, \ldots, k_s). \tag{4.5}$$

Therefore, the canonical map $\psi' :\ H = \mathrm{Gal}(K(\delta)/K) = \mu$ to $S' = \mathrm{Gal}(K'(N) \cap K(\delta)|K) = \mu_{h/h_0'}$ is $x \longmapsto x^{h_0'}$. Second, we describe the natural map

$$\varphi' :\ \mathrm{Gal}(K'(N)|K) \longrightarrow S'.$$

As $\delta = \gamma^{k_0^*} G_{\mathbf{k}}$ (see (3.7)),

$$\delta^{h_0'} \equiv \gamma^{k_0^* h_0'} \prod_{1 \leq i \leq r} G_{P_i}^{k_i h_0'} \text{ modulo } K^*.$$

Hence $(\overline{M}, \omega) \in \mathrm{Gal}(K'(N)|K) = (A/N)^* \times \mu$ acts on $\delta^{h_0'}$ through

$$\begin{aligned} \sigma_{\overline{M},\omega}(\delta^{h_0'}) &= \omega^{k_0^* h_0'} \lambda_{\mathbf{k}}^{h_0'}(\overline{M}) \cdot \delta^{h_0'} \\ &= \omega^{k_0^* h_0'} [\prod_{1 \leq i \leq r} \nu_i^{k_i}(\overline{M})]^{h_0'} \cdot \delta^{h_0'}. \end{aligned}$$

(Compare to (3.9); again the $\nu_i^{k_i}$ with $r < i \leq s$ don't contribute.) Therefore

$$\varphi'(\overline{M}, \omega) = \omega^{k_0^* h_0'} \lambda_{\mathbf{k}}^{h_0'}(\overline{M}) \in S' = \mu_{h/h_0'} \tag{4.6}$$

and

$$G' = \{(\overline{M}, \omega, \eta) \in (A/N)^* \times \mu \times H \mid \varphi'(\overline{M}, \omega) = \psi'(\eta)\}. \tag{4.7}$$

We are now able to describe R' similar to (2.3).

4.8 Proposition. *(i)* $R' = \{(\overline{M}, \omega, \eta) \in G' \mid \overline{M} = \eta\}$*;*
(ii) $R' \cong \{(\eta, \omega) \in H \times \mu \mid \eta^{h_0'(d-1)} = \omega^{-k_0^* h_0'}\}$.

Proof. (i) The argument is the same as in the proof of Proposition 2.3.
$(\overline{M}, \omega, \eta) \in G$ acts trivially on $K^{(\Delta)}(N)$
$\Leftrightarrow \forall x \in {}_N\rho:\ (\overline{M}, \omega, \eta)(x/\delta) = x/\delta$
$\Leftrightarrow \forall x \in {}_N\rho:\ \sigma_{\overline{M},\omega}(x)/(\eta\delta) = x/\delta$
$\Leftrightarrow \forall x \in {}_N\rho:\ \rho_M(y) = \eta x$
$\Leftrightarrow \overline{M} = \eta$ as elements of $(A/N)^*$.
(ii) This results from (i), (4.7), and the descriptions of ψ' and φ' given in (4.5) and (4.6), taking into account that for $\overline{M} = \eta \in \mathbb{F}_q^* \hookrightarrow (A/N)^*$,

$$\lambda_{\mathbf{k}}^{h_0'}(\eta) = \eta^{d'h_0'} = \eta^{dh_0'}$$

since $d'h_0' = (\sum_{1 \le i \le r} k_i d_i) h_0' \equiv (\sum_{1 \le i \le s} k_i d_i) h_0'$ modulo $q-1$. □

The following elementary lemma is left as an exercise.

4.9 Lemma: *Let m, n be natural numbers, a, b integers, μ_m resp. μ_n the corresponding groups of roots of unity.*
(i) $|\{(\eta, \omega) \in \mu_m \times \mu_n \mid \eta^a = \omega^b\}| = \gcd(mn, an, bm)$.
(ii) The projection of the group in (i) to the second factor μ_n has order $\gcd(mn, an, bn)/\gcd(a, m)$.

We apply this to the description of R' given in (4.8), with $m = h$, $n = q-1$, $a = h_0'(d-1)$, $b = h_0' k_0^*$, and find upon simplification: The group μ' of (4.3) and (4.4) has order

$$(4.10) \qquad |\mu'| = \gcd(\frac{h}{h_0'}(q-1), (d-1)(q-1), hk_0^*)/\gcd(\frac{h}{h_0'}, d-1).$$

Note that the only ingredient of this formula that depends on N is $h_0' = (q-1)/\gcd(q-1, k_{r+1}, \ldots, k_s)$, which takes the value 1 if $\mathrm{rad}(N)$ is a multiple of $\mathrm{rad}(\Delta)$. We thus get the wanted description of $f(\Delta, N)$ and $f(\Delta)$, which covers Corollary 0.3 from the Introduction.

4.11 Theorem. *(i) The degree $f(\Delta, N)$ of the constant field extension in $K^{(\Delta)}(N)$ is given by*

$$f(\Delta, N) = (q-1)/|\mu'|$$

with $|\mu'|$ as in (4.10).
(ii) If $\mathrm{rad}(N)$ *is a multiple of* $\mathrm{rad}(\Delta)$ *then* $f(\Delta, N) =: f(\Delta) = (q-1)/|\mu'|$ *with*

$$|\mu'| = \gcd(h(q-1), (d-1)(q-1), hk_0^*)/\gcd(h, d-1).$$

(iii) Suppose that $h = q-1$. Then

$$f(\Delta, N) = \gcd((q-1)/h_0', d-1)/\gcd((q-1)/h_0', d-1, k_0^*)$$

and

$$f(\Delta) = \gcd(q-1, d-1)/\gcd(q-1, d-1, k_0^*).$$

□

We conclude with simple examples for the evaluation of the quantities that occur in Theorem 4.11.

4.12 Examples. (i) Let $\Delta = c^{k_0}$ be constant. Then $h = (q-1)/\gcd(q-1, k_0^*)$, $h_0' = 1$ and $|\mu'| = q-1$. Therefore $f(\Delta, N) = 1$ for each N.
(ii) Let $\Delta = c^{k_0}P$ with some prime P and N be coprime with P. Then $h = h_0' = |\mu'| = q-1$ and therefore $f(\Delta, N) = 1$.
(iii) Let $\Delta = c^{k_0}P$ be as in (ii) with $\deg P = d$ and N be divisible by P. Then $h = q-1$, $h_0' = 1$, $|\mu'| = (q-1)\gcd(q-1, d-1, k_0^*)/\gcd(q-1, d-1)$, and $f(\Delta, N) = \gcd(q-1, d-1)/\gcd(q-1, d-1, k_0^*)$. Through suitable choices of d and k_0, each divisor of $q-1$ may be realized as $f(\Delta, N)$ for such Δ and N.

References

[1] Drinfeld, V. G.: Elliptic modules. (Russian) Mat. Sb. (N.S.) 94(136) (1974), 594-627, 656.

[2] Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. (German) [Finiteness theorems for abelian varieties over number fields] Invent. Math. 73 (1983), no. 3, 349-366.

[3] Goss, D.: Basic structures of function field arithmetic. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 35. Springer-Verlag, Berlin, 1996.

[4] Hayes, D. R.: Explicit class field theory for rational function fields. Trans. Amer. Math. Soc. 189 (1974), 77-91.

[5] Pink, R.; Rütsche, E.: Adelic openness for Drinfeld modules in generic characteristic. J. Number Theory 129 (2009), no. 4, 882-907.

[6] Rosen, M.: Number theory in function fields. Graduate Texts in Mathematics, 210. Springer-Verlag, New York, 2002.

[7] Thakur, D.S.: Gauss sums for $\mathbb{F}_q[T]$. Invent. Math. 94 (1988), no. 1, 105-112.

[8] Thakur, D.S.: Function field arithmetic. World Scientific Publishig Co., Inc., River Edge, NJ, 2004.

Ernst-Ulrich Gekeler
Fachrichtung 6.1 Mathematik
Universität des Saarlandes
Campus E2 4
66123 Saarbrücken
Germany

gekeler@math.uni-sb.de