The Galois image of twisted Carlitz modules

Ernst-Ulrich Gekeler

Saarbrücken 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 \( \text{def}(\Delta, N) \), 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 \( \Delta \), 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 \( \phi \) 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 \( \text{Gal}(F) = \text{Gal}(F^{\text{sep}}|F) \) in the Tate module \( T(\phi) \), a free \( \hat{A} \)-module of rank \( r \), where

\[
\hat{A} = \lim_{\leftarrow N \in A} A/N \rightarrow \prod_{P \text{ prime of } A} A_P
\]

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

\[
\pi(\phi) : \text{Gal}(F) \rightarrow \text{GL}(r, \hat{A}).
\]

As an immediate consequence of Drinfeld’s construction [1], \( \pi \) has open image (i.e., \( \text{im} \pi(\phi) \) has finite index in the compact group \( \text{GL}(r, \hat{A}) \)) if \( r = 1 \). This has been generalized to \( r \geq 2 \) by Pink and Rütsche [5], under the obviously necessary assumption that \( \phi \) has no complex multiplications, that is, if the endomorphism ring \( \text{End}(\phi) \) 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 \( \text{im} \pi(\phi) \) derived from them are rather weak.

In the present paper we give

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

in the case where \( r = 1 \) and \( F = K \), i.e., when \( \phi \) is a twist \( \phi = \rho^{(\Delta)} \) of the Carlitz module \( \rho \) 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 $\text{im} \, \pi(\rho(\Delta))$ in $\text{GL}(1,A) = A^*$, is always a divisor of $q - 1$.

0.3 Corollary. Let $K(\text{tor}(\rho(\Delta)))$ 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 $K(\text{tor}(\rho(\Delta)))$ 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 $A$;

$K_P$ is the completion of $A$ resp. $K$ at $P$;

$\mathbb{F}_p = A/P = \text{field extension of degree } \deg(P) \text{ of } \mathbb{F}_q$;

$M, N, \ldots$ elements of $A$, $\text{rad}(N) = \text{radical of } N = \text{maximal squarefree monic divisor of } N$;

$\mu_n = \text{group of } n\text{-th roots of unity in the algebraic closure of } \mathbb{F}_q$,

$\mu = \mu_{q-1} = \mathbb{F}_q^*$;

$|X|$ = cardinality of the finite set $X$;

$A/N = A/(N) = \text{residue class ring of } A \text{ modulo } (N)$, 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 $\rho$ over $K$ defined by the operator polynomial

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

Given any $0 \neq N \in A$, we let $\rho_N(X) \in K[X]$ be the $N$-th division polynomial of $\rho$ (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 $\text{Gal}(K(N)/K) \overset{\cong}{\rightarrow} (A/N)^*$; if $x \in N \rho$ and $\sigma_M \in \text{Gal}(K(N)/K)$ corresponds to the class of $M \in A$ coprime with $N$ then $\sigma_M(x) = \rho_M(x)$;
(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 $\mathbb{F}_q^\ast \rightarrow (A/N)^\ast$;

(v) if the place $P$ of $A$ is coprime with $N$ (hence $P$ is unramified in $K(N)$), then the residue class $P$ of $P$ in $(A/N)^\ast$ 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 $\phi$ be another rank-one Drinfeld $A$-module over $K$, given by

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

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

$$K^{(\Delta)}(N) = K(N \rho^{(\Delta)}) = \text{the “N-th division field of } \rho^{(\Delta)}\text{”}.$$

Similar to (1.2)(i), $K^{(\Delta)}(N)$ is abelian over $K$, but with Galois group a possibly proper subgroup of $(A/N)^\ast$. The main purpose of this work is to describe the defect

$$\text{def}(\Delta, N) := [(A/N)^\ast : \text{Gal}(K^{(\Delta)}(N)|K)]$$

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 $\delta$ provides an isomorphism $\delta : \rho^{(\Delta)} \xrightarrow{\cong} \rho$, or $\delta^{-1} : \rho \xrightarrow{\cong} \rho^{(\Delta)}$. In particular,

$$\delta^{-1} : N \rho \xrightarrow{\cong} \delta^{-1}$

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

$$\chi^{(\Delta)} : \text{Gal}(K) \rightarrow \mu = \mu_{q-1} = \mathbb{F}_q^\ast$$

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

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 \( \Delta \) if \( \Delta \) is free of \((q-1)^{th}\) powers) is defined.

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

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

\[
K_{P}(\delta) = K_{P}(\sqrt[4]{\Delta}) = K_{P}(\sqrt[q^{d}-1]{\Delta}) = K_{P}(\overline{\delta}),
\]

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

\[
\chi^{(\Delta)}(P) = F(\overline{\delta})/\overline{\delta} = \overline{\delta}_{q^{d}-1}^{(q^{d}-1)/(q-1)} = N_{\overline{F}_{P}}^{F}(\overline{\Delta}) = (\overline{\Delta}/\overline{P})_{q-1}
\]

by definition of the power residue symbol. \( \square \)

Note that \( (\overline{\Delta}/\overline{P})_{q-1} \) is related with \( (\overline{P}/\overline{\Delta})_{q-1} \) 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 \( \Delta \). Then the Frobenius element of \( P \) in \( \text{Gal}(K^{(\Delta)}(N)|K) \hookrightarrow (A/N)^{*} \) is \( (\overline{\Delta}/\overline{P})_{q-1}^{-1} \) 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 \( \Delta \) 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

\[
H := \text{Gal}(K(\delta)|K) \hookrightarrow \mu = \mathbb{F}_{q}^{*}
\]

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

\[
G := \text{Gal}(K(N)(\delta)|K)
\]

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

$$(\bar{M}, \eta) \text{ acts trivially on } K^{(\Delta)}(N)$$

$\iff \forall y \in N\rho^{(\Delta)} : (\bar{M}, \eta)(y) = y$

$\iff \forall x \in N\rho : (\bar{M}, \eta)(\frac{x}{\bar{\delta}}) = \left(\frac{x}{\bar{\delta}}\right)$

$\iff \forall x \in N\rho : \sigma_{\bar{M}}(x \cdot \eta \cdot \delta)^{-1} = x\delta^{-1}$

$\iff \forall x \in N\rho : \rho_{M}(x) = \eta \cdot x,$

since by (1.7) and (2.1), $\eta \in H$ acts on $\delta$ through multiplication by $\eta$. This means that $\bar{M}$ 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 $K(\Delta)(\delta)$ over $K^{(\Delta)}(N)$. Then $R = \{(\bar{M}, \eta) \in G \mid \bar{M} = \eta\}$, and $\text{Gal}(K^{(\Delta)}(N)|K)$ equals the image in $(A/N)^*$ of the homomorphism

$$G \rightarrow (A/N)^*$$

$$(\bar{M}, \eta) \mapsto \eta^{-1}\bar{M}.$$  \[\square\]

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

(2.4)

Thus we can read off:

**2.5 Corollary.** $\text{def}(\Delta, N) := [(A/N)^* : \text{Gal}(K^{(\Delta)}(N)|K)]$ is a divisor of $q - 1$.  \[\square\]
2.6 Corollary. def(\(\Delta, N\)) = 1 if \(K(N)\) and \(K(\delta)\) are linearly disjoint. This happens in particular if \(\Delta\) is a constant.

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

(2.7) We define the groups \(H_0 := \text{Gal}(K(\delta)|K(\delta) \cap K(N)) \subset H\) and \(S := \text{Gal}(K(\delta) \cap K(N)|K)\). 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 \(\psi : H \rightarrow S\) is the raising to the \(h_0\)-th power in \(H\). Let

\[ \varphi : \text{Gal}(K(N)|K) = (A/N)^* \rightarrow S \]

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 \(H \hookrightarrow \mu = F_q^* \hookrightarrow (A/N)^*\) we consider \(H\) as a subgroup of \((A/N)^*\). Then

\[ |R| = |\{(\overline{M}, \eta) \in G \mid \overline{M} = \eta\}| = |\{\eta \in H \mid \varphi(\eta) = \psi(\eta)\}| \]

\[ = |\ker(\psi \varphi^{-1}|_H)|. \]

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

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

which in any case is a divisor of \(|S| = h/h_0\).

(2.9) As the kernel of \((A/N)^* \rightarrow (A/\text{rad}(N))^*\) is a \(p\)-group \((p := \text{char}(F_q))\) and \((A/\text{rad}(N))^*\) is \(p\)-free, the field \(K(\delta) \cap K(N)\) is already contained in \(K(\text{rad}(N))\), and the map \(\varphi\) of (2.7) factors over \((A/\text{rad}(N))^*\). This shows that the canonical map

\[ (A/N)^*/\text{Gal}(K^{(\Delta)}(N)|K) \rightarrow (A/\text{rad}(N))^*/\text{Gal}(K^{(\Delta)}(\text{rad}(N))|K) \]

is in fact an isomorphism. Thus:

2.10 Proposition. The defects \(\text{def}(\Delta, N)\) and \(\text{def}(\Delta, \text{rad}(N))\) agree. □

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 \(\Delta\) is integral, i.e., \(\Delta \in A \setminus \{0\}\), and not divisible by \((q - 1)\)-th powers. Let \(c \in F_q^*\) be a fixed primitive \((q - 1)\)-th root of unity. Then we may write

\[ \Delta = c^{k_0} P_1^{k_1} \ldots P_s^{k_s} \]
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., $\Delta$ 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

\[
G_P := \prod_{1 \leq j \leq d} g_j
\]

lies in $K(P)$. For ramification reasons, \([K(G_P) : K] = q - 1\), which shows the assertion.

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

\[
\sigma_{\mathbb{F}_q}(G_P) = N_{\mathbb{F}_q}^{\mathbb{F}_p}(\mathbb{M}) \cdot G_P
\]

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

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

\[
G_k := \prod_{1 \leq i \leq s} G_{P_i}^{k_i}.
\]

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

(3.5)(i) $G_k \in K(\text{rad}(\Delta))$ (if $\Delta$ is as in (3.1));

(ii) $G_k^{q-1} = (-1)^d \prod_{1 \leq i \leq s} P_i^{k_i}$, where $d := \sum_{1 \leq i \leq d} k_i d_i$ is the degree $\deg(\Delta)$ of $\Delta$;

(iii) $\sigma_{\mathbb{F}_q}(G_k) = \lambda_k(\mathbb{M}) \cdot G_k$, where $\sigma_{\mathbb{F}_q} \in \text{Gal}(K(\Delta)|K) = (A/\Delta)^*$ is the class of $M \in A$, $\Delta$ non-constant and coprime with $M$. Here $\lambda_k$ is the $\mu$-valued character

\[
\lambda_k : (A/\Delta)^* \rightarrow \mu
\]

\[
\mathbb{M} \rightarrow \prod_{1 \leq i \leq s} \nu_i^{k_i}(\mathbb{M})
\]
with the canonical maps
\[ \nu_i : (A/\Delta)^* \rightarrow (A/P_i)^* \rightarrow \mathbb{F}_q^* = \mu. \]
\[ x \mapsto N_{\mathbb{F}_q}(x) \]
Note that \( \lambda_k \) factors over \((A/\mathrm{rad}(\Delta))^*\).

Thus we can realize the field \( K(\delta) = K(\sqrt[q]{\Delta}) \) as a Kummer sub-extension 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 \( \gamma \) be a \((q-1)\)-th root of \( c \) (so it is a primitive \((q-1)^2\)-th root of unity). Then \( \delta^* := \gamma^{k_0} G_k \) satisfies \( (\delta^*)^{q-1} = (-1)^d \Delta \). Therefore we put
\[
(3.7) \quad k_0^* = \begin{cases} 
  k_0, & \text{if } q \text{ or } d = \deg \Delta \text{ is even,} \\
  \text{the unique } k \equiv k_0 + (q-1)/2 \pmod{q-1} \text{ with } 0 \leq k < q-1, & \text{otherwise.}
\end{cases}
\]

Then \( \delta := \gamma^{k_0^*} G_k \) is a \((q-1)\)-th root of \( \Delta \).

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 \( g \) equals the ideal generated by \((q-1)/2\), which gives \( \gcd((q-1), k_0, k_1, \ldots, k_s) = \gcd(q-1, k_0, g) = \gcd((q-1)/2, k_0, g) = \gcd((q-1)/2, k_0^*, g) \). (ii) The field \( K(\delta) \cap K(N) \) is the Kummer extension of \( K \) generated by \( \delta^{h_0} \). Some power \( \delta^n \) lies in \( K(N) \) if and only if the following conditions are satisfied:
\[
(3.8.1) \quad k_i \cdot n \equiv 0 \pmod{q-1}, \quad r < i \leq s,
\]
\[ k_0^* \cdot n \equiv 0 \pmod{q-1}. \]
Therefore,
\[ h_0 = \min \{ n \in \mathbb{N} | (3.8.1) \text{ holds for } n \} = (q-1)/\gcd(q-1, k_0^*, k_{r+1}, \ldots, k_s). \]
With the notation of (2.7) we have the canonical restriction homomorphisms
\[ \varphi : \text{Gal}(K(N)|K) = (A/N)^* \longrightarrow S = \text{Gal}(K(\delta) \cap K(N)|K) = \mu_{h/h_0} \]
\[ \psi : H = \text{Gal}(K(\delta)|K) = \mu_h \longrightarrow S. \]
As \( \varphi \) describes the action of \((A/N)^*\) on \(\delta h_0\), if is given by
(3.9) \[ \varphi = \lambda_{h_0}^h, \]
where \(\lambda_k\) is defined in (3.6); raising to the \(h_0\)-th power, the components \(\nu_i^k\) with \(r < i \leq s\) are annihilated, as is the contribution of the scalar \(\gamma_{k_0}^h\), which lies in \(\mathbb{F}_q^*\). In more detail, \(\varphi\) is the map
\[ (A/N)^* \longrightarrow (A/P_1 \cdots P_r)^* \longrightarrow S = \mu_{h/h_0} \]
\[ x \mapsto \lambda_{h_0}^h(x) = [\prod_{1 \leq i \leq r} \nu_i^k(x)]^{h_0}. \]
What is the restriction of \(\varphi\) to \(\mathbb{F}_q^* \hookrightarrow (A/N)^*\)? First, the map
\[ \nu_i : (A/N)^* \longrightarrow (A/P_i)^* \xrightarrow{N_{P_i}^P \mathbb{F}_q^*} \mathbb{F}_q^* \]
acts on \(x \in \mathbb{F}_q^*\) as \(\nu_i(x) = x^{1+q+\cdots+q^{i-1}} = x^{d_i} \). Therefore,
\[ \varphi(x) = x^{d_0} = x^{dh_0}, \]
with \(d' = \sum_{1 \leq i \leq r} k_id_i\), since \(d'h_0 \equiv (\sum_{1 \leq i \leq s} k_id_i)h_0 = dh_0\) modulo \(q - 1\), by (3.8.1). As \(\psi(x) = x^{h_0}\) for \(x \in H\), we find (see (2.7)):
(3.10) \[ |R| = |\ker(\psi\varphi^{-1}|_H)| = |\{x \in \mu_h | x^{h_0} = 1\}| \]
\[ = \gcd((d' - 1)h_0, h) = \gcd((d' - 1)h_0, h) \]
Plugging into (2.8) and simplifying gives
(3.11) \[ \text{def}(\Delta, N) = |R|/h_0 = \gcd(d' - 1, h/h_0) \]
\[ = \gcd(d' - 1, \frac{\gcd(q-1,k_0^*k_{r+1}\ldots,k_s)}{\gcd(q-1,k_0^*k_{r+1}\ldots,k_s)}) \] \[ = \gcd(d' - 1, q - 1, k_0^*, k_1, \ldots, k_s) \]
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 \(d_{\ell}\). Then
\[ \gcd(d - 1, b) = \gcd(d - 1, b/\gcd(b, L)). \]
Proof. Obviously the right hand side divides the left hand side. Write
\( g = \gcd(b, L), \quad b = g \cdot b^*, \quad d = g \cdot d^* \). 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. \( \square \)

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 \( d_i \), \( 0 \leq k_0 < q - 1, \quad 0 < k_i < q - 1 \)
for \( 1 \leq i \leq s \) and \( d = \sum_{1 \leq i \leq s} k_id_i = \deg \Delta \).

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 Gal(\(K\)) in Aut_{\(A/(N\rho(\Delta))\)}(\(A/N\)) \(\text{(that is, Gal(K(\Delta)(N)|K))}\)
has index \( (3.7) \) for \( k^* \)
\[
def(\Delta, N) = \gcd(d - 1, q - 1, k^*_0, k^*_r+1, \ldots, k^*_s).
\]

Suppose that \( M \) divides \( N \). From the commutative diagram of natural maps
\[
\begin{array}{ccc}
\text{Gal(K(\Delta)(N)|K)} & \hookrightarrow & (A/N)^* \\
\downarrow & & \downarrow \\
\text{Gal(K(\Delta)(M)|K)} & \hookrightarrow & (A/M)^*
\end{array}
\]
we see that the quotient by Gal(K(\(\Delta)(N)|K) of \( (A/N)^* \) is stable as soon as \( \text{rad}(N) \) is divisible by \( \text{rad}(\Delta) \). This implies (notations and assumptions as in (3.13)):

3.14 Corollary. The image of Gal(\(K\)) under the representation \( \pi(\Delta) : \text{Gal(K)} \to (\hat{A})^* \) provided by the twisted Carlitz module \( \rho(\Delta) \) is the inverse image in \( (\hat{A})^* \) of a subgroup of \( (A/\text{rad}(\Delta))^* \) of index
\[
def(\rho(\Delta)) = \def(\Delta) = \gcd(d - 1, q - 1, k^*_0).
\]

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

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

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

Furthermore, in this case, the infinite prime of $K$ is tamely ramified in $K(\Delta)(N)|K$, 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 $\Delta$ is ramified in $K(\Delta)(N)|K$, with ramification group isomorphic with its ramification group in $K(\delta)|K$, and contained in $\mathbb{F}_q^* \hookrightarrow (A/N)^* \xrightarrow{\cong} \text{Gal}(K(\Delta)(N)|K)$.

4. The constant field extension.

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

(4.1) Let $F(\Delta, N)$ be the algebraic closure of $F_q$ 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 $F_q$ in $K(\text{tor}(\rho(\Delta))) = \lim_{N \rightarrow \infty} K(\Delta)(N)$.

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

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

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

(4.3) 

\[ \begin{array}{ccc}
K' & \xrightarrow{R'} & K'(N)(\delta) \\
\downarrow & & \downarrow \\
K' & & K'(N)(\delta) \\
\downarrow & \downarrow & \downarrow \\
K'(N) & \xrightarrow{H_{\delta}} & K(\delta) \\
\downarrow & & \downarrow \\
(A/N)^* & & (A/N)^* \times \mu \\
\downarrow & & \downarrow \\
K' & \xrightarrow{H} & K'(N) \cap K(\delta) \\
\downarrow & \downarrow & \downarrow \\
K' & \xrightarrow{S'} & K'(N) \cap K(\delta) \\
\downarrow & \downarrow & \downarrow \\
K & \xrightarrow{\mu} & K'(N) \cap K(\delta) \\
\downarrow & \downarrow & \downarrow \\
K & \xrightarrow{\mu} & K'(N) \cap K(\delta) \\
\end{array} \]
where each line indicates an inclusion and the group nearby is the Galois group.

We find that
\[ G' := \text{Gal}(K'(N)(\delta)|K) \]
is a subgroup of \( \text{Gal}(K'(N)|K) \times \text{Gal}(K(\delta)|K) = (A/N)^* \times \mu \times H \) which projects onto the two factors \((A/N)^* \times \mu\) and \(H\). Let \( \mu' \) be the image of
\[ R' := \text{Gal}(K'(N)(\delta) | K'(\Delta)(N)) \]
under the canonical projection to \( \mu \). By Galois theory, \( \mu' \) is the group of \( K' \) over \( \mathbb{F}(\Delta, N)(T) \). That is
\[ f(\Delta, N) = (q - 1)/|\mu'|. \]

Our strategy is thus to determine \( R' \) and its projection to \( \mu \), 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 \( \delta \) lies in \( K'(N) \cap K(\delta) \), we find
\[ k_i n \equiv (\text{mod } q - 1), \quad r < i \leq s \]
holds, we find
\[ h'_0 = (q - 1)/\gcd(q - 1, k_{r+1}, \ldots, k_s). \]

Therefore, the canonical map \( \psi' : H = \text{Gal}(K(\delta)/K) = \mu \) to \( S' = \text{Gal}(K'(N) \cap K(\delta)|K) = \mu_{h/h'_0} \) is \( x \mapsto x_{h'_0} \). Second, we describe the natural map
\[ \varphi' : \text{Gal}(K'(N)|K) \longrightarrow S'. \]

As \( \delta = \gamma^{k_\delta}G_k \) (see (3.7)),
\[ \delta^{h_0} \equiv \gamma^{k_\delta h_0} \prod_{1 \leq i \leq r} G_{P_i}^{k_i h_0} \text{ modulo } K^*. \]

Hence \( (\overline{M}, \omega) \in \text{Gal}(K'(N)|K) = (A/N)^* \times \mu \) acts on \( \delta^{h_0} \) through
\[ \sigma_{\overline{M}, \omega}(\delta^{h_0}) = \omega^{k_\delta h_0} G_{\overline{M}}^{h_0} \cdot \delta^{h_0} \]
\[ = \omega^{k_\delta h_0} \prod_{1 \leq i \leq r} \nu_i^{k_i(\overline{M})} \cdot \delta^{h_0}. \]

(Compare to (3.9); again the \( \nu_i^{k_i} \) with \( r < i \leq s \) don’t contribute.) Therefore
\[ \varphi'(\overline{M}, \omega) = \omega^{k_\delta h_0} G_{\overline{M}}^{h_0} \in S' = \mu_{h/h'_0} \]
and
\[ G' = \{ (\overline{M}, \omega, \eta) \in (A/N)^* \times \mu \times H \mid \varphi'(\overline{M}, \omega) = \psi'(\eta) \}. \]

We are now able to describe \( R' \) similar to (2.3).
(iii) Suppose that $h_1$.

(ii) If $\text{rad}(\Delta') = \text{rad}(\Delta)$, which covers Corollary 0.3 from the Introduction.

Proof. (i) The argument is the same as in the proof of Proposition 2.3. Let $\rho$ act trivially on $\rho(N) = \eta \delta$, where $\delta$ is the smallest positive integer such that $\delta^d \equiv 1 \pmod{q}$. Then

\[\rho \circ \sigma = \rho \circ (\rho(N)) = \rho(\Delta') \rho = \rho(\Delta) = \eta \delta \]

in $K(\Delta)(N)$.

\[\forall x \in N \rho : (\overline{M}, \omega, \eta)(x/\delta) = x/\delta\]

\[\forall x \in N \rho : (\overline{M}, \omega, \eta)(\bar{x})/\delta = \bar{x} = x/\delta\]

\[\forall x \in N \rho : \rho_M(y) = \eta x\]

\[\overline{M} = \eta \text{ as elements of } (A/N)^{\ast}.

The following elementary lemma is left as an exercise.

4.9 Lemma: Let $m, n$ be natural numbers, $a, b$ integers, $\mu_m$ resp. $\mu_n$ 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 $\mu_n$ has order

\[\gcd(mn, an, bm)/ \gcd(a, m)\]

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 $\mu'$ of (4.3) and (4.4) has order

\[|\mu'| = \gcd(h/h_0', (q - 1), (d - 1)(q - 1), h_0'k_0^+)/ \gcd(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 $\text{rad}(N)$ is a multiple of $\text{rad}(\Delta)$. 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 $\text{rad}(N)$ is a multiple of $\text{rad}(\Delta)$ then $f(\Delta, N) = (q - 1)/|\mu'|$ with

\[|\mu'| = \gcd(h(q - 1), (d - 1)(q - 1), h_0'k_0^+)/ \gcd(h, d - 1).

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

\[f(\Delta, N) = \gcd((q - 1)/h_0', d - 1)/ \gcd((q - 1)/h_0', d - 1, k_0^+)\]
\( f(\Delta) = \gcd(q - 1, d - 1)/\gcd(q - 1, d - 1, k_0^*) \).

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

\section*{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 \( \Delta \) and \( N \).

\section*{REFERENCES}


