Canad. Math. Bull. Vol. **43** (3), 2000 pp. 282–293

Characteristic p Galois Representations That Arise from Drinfeld Modules

Nigel Boston and David T. Ose

Abstract. We examine which representations of the absolute Galois group of a field of finite characteristic with image over a finite field of the same characteristic may be constructed by the Galois group's action on the division points of an appropriate Drinfeld module.

0 Introduction

There are well-known methods of producing representations of the absolute Galois group of a number field. These include the use of elliptic curves, modular forms, and most generally étale cohomology groups of varieties [FM]. There are many conjectures as to which Galois representations are produced this way. For instance, Serre's conjecture [S] states that every odd, irreducible representation of the form $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}_p})$ should be associated to a modular form of a particular kind. Here *odd* means that complex conjugation maps to a matrix of determinant -1.

In this paper, we consider representations of the absolute Galois group of a field of nonzero characteristic. Suppose that K has characteristic $p \neq 0$. We describe a method, due to Drinfeld [D], of obtaining representations of the form $\mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{GL}_r(\overline{\mathbf{F}_p})$ and address the problem of which representations arise this way. This construction resembles the way that Galois representations are given by the Galois action on the p-division points of elliptic curves (but does not only produce rank $r = 2$ representations). We obtain a fairly complete answer in the case $r = 1$ (which actually involves some nontrivial computations) and a partial answer for larger r. This has applications to finding generic equations for cyclic extensions of K of degree m, even when the m-th roots of unity are not all in K. The question of what representations of the form $\mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{GL}_r(R)$ (R a discrete valuation ring of equal characteristic with finite residue field) are produced by extending the method of Drinfeld, is addressed in the second author's University of Illinois Ph.D. thesis [O].

1 Drinfeld Representations

Let K be a field of characteristic p. Suppose that K contains $\mathbf{F}_q$. Define the *Ore ring* to be the set of polynomials in F over K, $K\{F\} = \{\sum a_i F^i : a_i \in K\}$, with the noncommutative

Received by the editors September 3, 1998.

The first author was partially supported by NSF grant DMS 96-22590, the Sloan Foundation, and the Rosenbaum Foundation. The authors thank God for leading them to results. They also thank Bucknell University for supporting their collaboration, the University of Illinois for enabling them to visit England, the Newton Institute for its hospitality, and Hendrik Lenstra for useful comments on this work.

AMS subject classification: 11G09, 11R32, 11R58.

multiplication $Fa = a^q F$. This ring is also known as the ring of $\mathbf{F}_q$-linear polynomials or alternatively $\mathrm{End}_{\mathbf{F}_q}(\mathbf{G}_a/K)$, where $\mathbf{G}_a/K$ is the additive group scheme over K with F interpreted as the Frobenius morphism that sends x to x^q hence $Fx = x^q$, $F^2x = x^{q^2}$, $\ldots$. For its basic properties, see Chapter 1 of [G]. Let $g(F) \in K\{F\}$ be of degree $r > 0$. Let $\phi \in A = \mathbf{F}_q[T]$ be irreducible and of degree $d > 0$. We make the assumption that $\phi(b) \neq 0$, where b is the constant term of g. The set $V = \Big\{x \in \overline{K} : \Big(\phi\big(g(F)\big)\Big)x = 0\Big\}$ is a vector space over $\mathbf{F}_{q^d}$ of dimension r, sometimes called the ϕ-division points, on which $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ acts (the assumption on $\phi(b)$ ensuring that $\Big(\phi\big(g(F)\big)\Big)x$ is separable so that V has the claimed cardinality). The following examples will come in handy later.

Example 1.1 Let $q = 2$, $g(F) = aF + b$, and $\phi = T^2 + T + 1$. Then

$$\Big(\phi\big(g(F)\big)\Big)x = a^3x^4 + a(b^2 + b + 1)x^2 + (b^2 + b + 1)x.$$

Example 1.2 Let $q = 3$, $g(F) = aF + b$, and $\phi = T^2 + 1$. Then

$$\Big(\phi\big(g(F)\big)\Big)x = a^4x^9 + a(b^3 + b)x^3 + (b^2 + 1)x.$$

Example 1.3 Let $q = 2$, $g(F) = aF + b$, and $\phi = T^3 + T + 1$. Then

$$\Big(\phi\big(g(F)\big)\Big)x = a^7x^8 + a^3(b^4 + b^2 + b)x^4 + a(b^4 + b^3 + b^2 + 1)x^2 + (b^3 + b + 1)x.$$

We therefore obtain a representation $\rho\colon G_K \to \mathrm{GL}_r(\mathbf{F}_{q^d})$. The question we wish to address is what representations arise this way. Such representations will be called *Drinfeld* (but note that Drinfeld modules may be more general). More precisely, $\rho\colon G_K \to \mathrm{GL}_r(\mathbf{F}_{q^d})$ is Drinfeld if there exist an irreducible polynomial $\phi \in A$ of degree d, an $\mathbf{F}_q$-algebra isomorphism $A/(\phi) \cong \mathbf{F}_{q^d}$, a rank r Drinfeld A-module defined by $T \mapsto g(F) = \sum_{i=0}^{r} b_iF^i$ with $b_r \neq 0$ and $\phi(b_0) \neq 0$, and an $A/(\phi)$-basis of $V_{g,\phi} = \{x \in K^{\mathrm{sep}} : \phi\big(g(F)\big)x = 0\}$, such that the resulting representation

$$G_K \to \mathrm{GL}(V_{g,\phi}) \cong \mathrm{GL}_r\big(A/(\phi)\big) \cong \mathrm{GL}_r(\mathbf{F}_{q^d})$$

is ρ.

2 A Useful Lemma

Let $g(F) = aF + b$ and so $r = 1$. Then ρ maps to $\mathbf{F}_{q^d}^*$, and hence factors through $\mathrm{Gal}(L/K)$, where L/K is a cyclic extension of degree dividing $q^d - 1$ ($L = K(V)$ in the notation of the introduction—we will denote it by $L_{a,b,\phi}$ in later work). Let ζ be a root of ϕ, $K' = K(\zeta)$, and $L' = L(\zeta)$.

$$\begin{array}{ccc} L = K(x) & \longrightarrow & L' = L(\zeta) \\ \uparrow & & \uparrow \\ K & \longrightarrow & K' = K(\zeta) \end{array}$$

https://doi.org/10.4153/CMB-2000-035-5 Published online by Cambridge University Press

The extension L'/K' is a Kummer extension since $K' = K(\zeta)$ contains $\mathbf{F}_q(\zeta) = \mathbf{F}_{q^d}$. Thus, $L' = K'(v)$ where $v^{q^d-1} \in K'$, say $v^{q^d-1} = c$.

What we need to know is the following. What is c in terms of a, b, ζ?

Lemma 2.1 *With the set-up as above,*

$$c = \frac{(\zeta - b)(\zeta - b^q)\cdots(\zeta - b^{q^{d-1}})}{a^{1+q+\cdots+q^{d-1}}}.$$

Proof Let $\phi(T) = (T - \zeta)\psi(T)$, so $\psi(T)$ is a polynomial over $\mathbf{F}_q(\zeta) = \mathbf{F}_{q^d}$ of degree $d - 1$. Let $x \neq 0$ satisfy $\big(\phi(aF + b)\big)x = 0$, so that $L = K(x)$ (since L/K is cyclic) and $L' = K'(x)$.

We claim that if $v = \big(\psi(aF + b)\big)x$, then $L' = K'(v)$, and most importantly

$$v^{q^d-1} = (\zeta - b)(\zeta - b^q)\cdots(\zeta - b^{q^{d-1}})/a^{1+q+\cdots+q^{d-1}}.$$

This follows from the following identity in $K'\{F\}$ (here $[q]_k = (q^k - 1)/(q - 1)$ and $c_i = \zeta - b^{q^i}$):

$$(a^{[q]_d}F^d - c_0c_1c_2\cdots c_{d-1})\psi(aF + b) = h(F)\phi(aF + b),$$

where

$$h(F) = a^{[q]_{d-1}}F^{d-1} + a^{[q]_{d-2}}c_{d-1}F^{d-2} + a^{[q]_{d-3}}c_{d-1}c_{d-2}F^{d-3} + \cdots + a^{[q]_0}c_{d-1}c_{d-2}\cdots c_1.$$

This is verified by checking that the coefficients of F^n of each side of the identity agree for all n. This calculation is omitted. (In fact, the identity was discovered by extensive computer algebra calculations with *Mathematica* of small degree cases.) We apply both sides of the identity to x. This yields $a^{[q]_d}v^{q^d} - c_0c_1c_2\cdots c_{d-1}v = 0$. Hence $v^{q^d} = \big((c_0c_1c_2\cdots c_{d-1})/a^{[q]_d}\big)v$, and we are done, if we can show that $L' = K'(v)$ (note that this will also show that $v \neq 0$). We shall see that this follows from the next lemma.

Lemma 2.2 *The (right) greatest common divisor of $\phi(aF + b)$ and $\psi(aF + b)$ is* 1, *i.e., they are (right) relatively prime.*

Proof As described in Example 1.10.3 of [G], the greatest common divisor is calculated as follows. Let W_ϕ and W_ψ denote the set of zeros in K^{sep} of $\big(\phi(aF + b)\big)x = 0$ and $\big(\psi(aF + b)\big)x = 0$ respectively. If $W = W_\phi \cap W_\psi$, then the greatest common divisor is the additive polynomial $\prod_{\alpha\in W}(x - \alpha)$. We therefore need to show that $W = \{0\}$. This is accomplished by using the easily verified identity

$$\phi(aF + b) = -\zeta\psi(aF + b) + \psi(aF + b)(aF + b).$$

Suppose that $u \in W$, $u \neq 0$. By the last identity, $\big(\psi(aF + b)\big)(aF + b)u = 0$. Since the coefficients of ϕ are in $\mathbf{F}_q$, $\big(\phi(aF+b)\big)(aF+b)u = (aF+b)\big(\phi(aF+b)\big)u = 0$, so $aF+b$ is an endomorphism of W, *i.e.*, W is an $\mathbf{F}_q[aF+b]$-submodule of W_ϕ. Since W_ϕ is 1-dimensional over $\mathbf{F}_q[aF+b]/\big(\phi(aF+b)\big) \cong \mathbf{F}_{q^d}$, $W = W_\phi$, which contradicts the fact that $\#W_\psi < \#W_\phi$.

This incidentally shows that the identity in the proof of Lemma 2.1 above in fact gives the least common multiple of $\phi(aF+b)$ and $\psi(aF+b)$ since its degree is

$$\deg\big(\phi(aF+b)\big)+\deg\big(\psi(aF+b)\big)-\deg\Big(\gcd\big(\phi(aF+b),\psi(aF+b)\big)\Big)$$
$$=d+(d-1)-0=2d-1,$$

(see section 1.10 of [G], where consequences of the existence of a right division algorithm in Ore rings are discussed).

By the lemma, we can find polynomials $j(F), k(F) \in K'\{F\}$ such that

$$j(F)\psi(aF+b)+k(F)\phi(aF+b)=1.$$

Applying this to x gives $j(F)v = x$, so $x \in K'(v)$ and since $v = \big(\psi(aF+b)\big)x$, $v \in K'(x)$ and so $L' = K'(v)$.

This can also be proven in a more conceptual way by using Hayes' theory [H].

3 The Cases $d = 1$ and $d = 2$

Lemma 2.1 allows us to show that every representation $G_K \to \mathrm{GL}_1(\mathbf{F}_{q^d})$ is Drinfeld if $d = 1$ or 2, except for one special case for $d = 2$, namely when $K = \mathbf{F}_q$ and the image of the representation is in $\mathrm{GL}_1(\mathbf{F}_q)$. The idea is to let L be the fixed field of the representation's kernel and to show that $L = L_{a,b,\phi}$ for some $a, b \in K$ and irreducible $\phi \in \mathbf{F}_q[T]$ of degree d. Note that this is enough to show that the associated representation is Drinfeld since the Drinfeld property depends only on the field L, whereas the representation can be changed by picking a different basis for the corresponding V.

Theorem 3.1 *If $d = 1$ or 2, then every representation $G_K \to \mathrm{GL}_1(\mathbf{F}_{q^d})$ is Drinfeld, unless $d = 2$, $K = \mathbf{F}_q$, and the image of the representation is in $\mathrm{GL}_1(\mathbf{F}_q)$.*

Proof There are two cases.

(I) $d = 1$. Given representation $G_K \to \mathrm{GL}_1(\mathbf{F}_q)$, we let L be the fixed field of its kernel. Then L/K is a Kummer extension and so is of the form $L = K(v)$, where $v^{q-1} = c \in K$.

Taking $a = 1$, $b = -c$, and $\phi(T) = T$ (so that $\zeta = 0$), we get by the Drinfeld construction a representation that, by the last lemma, yields $L_{a,b,\phi} = L$ (since $(\zeta - b)/a = c$).

(II) $d = 2$. There are now three cases, namely according as $\zeta \in K$, $\zeta \notin L$, or $\zeta \in L - K$.

Case (i): $\zeta \in K$. Then $\mathbf{F}_q(\zeta) = \mathbf{F}_{q^2} \le K$ and so L/K is a Kummer extension, say $L = K(v)$ with $v^{q^2-1} = c \in K$. We wish to find $a, b \in K$ such that

$$\frac{(\zeta-b)(\zeta-b^q)}{a^{q+1}} = c.$$

Note that

$$\frac{(\zeta-b)(\zeta-b^q)}{a^{q+1}} = \frac{\zeta-b}{\zeta^q-b}\left(\frac{\zeta^q-b}{a}\right)^{q+1},$$

https://doi.org/10.4153/CMB-2000-035-5 Published online by Cambridge University Press

so if we set $b = (c\zeta^q - \zeta)/(c-1)$ and $a = \zeta^q - b$, then this all simplifies to c. We just have to make sure that $c \neq 1$, but c is only defined up to a (q^2-1)-th power, so we have the necessary flexibility, unless $K = \mathbf{F}_{q^2} = L$. In that case, we need to pick $b \in K$ such that $(\zeta - b)(\zeta - b^q)$ is a $(q+1)$-th power in K^*, *i.e.*, is a nonzero element of $\mathbf{F}_q$. This is accomplished in exactly the same way as described in case (ii) below.

Case (ii): $\zeta \notin L$. The idea is to show that the process, considered in the lemma of Section 1, for obtaining L' as the compositum of $K' = K(\zeta)$ and L can be suitably reversed.

Since L and $K(\zeta)$ are disjoint, the extension L'/K is Galois with Galois group $\langle\sigma\rangle \times \langle\tau\rangle$ where σ has order 2 and τ has order m dividing q^2-1. The fixed fields of σ and τ are L and $K' = K(\zeta)$ respectively.

The extension L'/K' is Kummer and so $L' = K'(v)$ for some v such that $v^{q^2-1} = c \in K'$. We claim that there exist $a, b \in K$ such that $\big((\zeta - b)(\zeta - b^q)\big)/a^{q+1} = c$. The argument goes as follows.

Let $w = \sigma(v)$. Then $w^{q^2-1} = \sigma(c)$. Suppose, without loss of generality, that $\tau(v) = \eta v$, where η is an m-th root of unity in K'. The fact that σ and τ commute, implies that $\tau(w) = \eta^q w$. Let $y = wv^{-q}$. We check that $\tau(y) = y$ and so $y \in K'$. We calculate that $\sigma(y)y^q c = 1$.

At this point, we have a division into two cases depending on whether $y \in K$ or not.

Say $y \in K$. Then $\sigma(y) = y$. Hence, $c = (1/y)^{q+1}$ is the $(q+1)$-th power of an element of K and so, to write c in the form $(\zeta - b)(\zeta - b^q)/a^{q+1}$ (up to (q^2-1)-th powers of elements of K'), we must equivalently be able to pick $b \in K$ such that $(\zeta - b)(\zeta - b^q)$ is a $(q+1)$-th power in K times a (q^2-1)-th power in K'. This can be done so long as $K \neq \mathbf{F}_q$. For instance, in the case of odd characteristic, suppose $\phi = T^2 - \lambda$. Pick any $u \in K - \mathbf{F}_q$. Set $b = (u^{q+1} - \lambda)/(u^q - u)$. Then

$$\frac{(\zeta - b)(\zeta - b^q)}{a^{q+1}} = \left(\frac{(\zeta - u)(\zeta - u^q)}{(u^q - u)a}\right)^{q+1} = \left(\frac{u-b}{a}\right)^{q+1} \big(\zeta(u+\zeta)\big)^{q^2-1},$$

which is of the desired form. In the case of even characteristic, suppose $\phi = T^2 + T + \lambda \in \mathbf{F}_q[T]$ is irreducible. Pick $u \in K - \mathbf{F}_q$ and set $b = (u^{q+1} + u + \lambda)/(u^q - u)$. The rest proceeds as the odd characteristic case.

If $K = \mathbf{F}_q$, then since c is a $(q+1)$-th power of an element $1/y$ of K, we can pick v so that $v^{q-1} = 1/y \in K$. Then $L = K(v)$ has degree dividing $q-1$ over K. Suppose now $(\zeta - b)(\zeta - b^q) = k^{q+1} r^{q^2-1}$ for some $b, k \in K$, $r \in K'$. Since $K' = \mathbf{F}_{q^2}$, $r^{q^2-1} = 1$. Moreover, $k^{q+1} = k^2$ and $b^q = b$ since they are in K. The equation reduces to $(\zeta - b)^2 = k^2$, so $\zeta - b = \pm k$, which is impossible because $\zeta \notin K$.

Say $y \notin K$. Since $1/\sigma(y) \in K' - K$ and $K' = K(\zeta)$ has degree 2 over K, we can write $1/\sigma(y) = s\zeta - r$ with $r, s \in K$, $s \neq 0$. Then $(s\zeta - r)(s^q\zeta - r^q) = 1/\big(\sigma(y)y^q\big) = c$. Let $b = r/s$ and $a = 1/s$. We have shown that $\big((\zeta - b)(\zeta - b^q)\big)/a^{q+1} = c$.

It follows that L' is the compositum of $L_{a,b,\phi}$ and K'. The fixed field of σ equals L and $L_{a,b,\phi}$ and so the two fields must coincide.

Case (iii): $\zeta \in L - K$. In this case we have a tower of fields $K \subset K' \subset L = L'$ with, say, $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ so that $\mathrm{Gal}\big(L/K(\zeta)\big) = \langle\sigma^2\rangle$. Since $L/K(\zeta)$ is Kummer, there is v such that $\sigma^2(v) = \eta v$ with η an m-th root of unity, where $m = [L : K(\zeta)]$. Note that since $[L : K] = 2m$ divides $q^2 - 1$, η is a square in $\mathbf{F}_{q^2}^*$. We can write $\eta = \mu^{2q}$ then with $\mu \in \mathbf{F}_{q^2}^*$.

https://doi.org/10.4153/CMB-2000-035-5 Published online by Cambridge University Press

Setting $y = v^q\sigma(v)^{-1}\mu$, we check that $\sigma(y)y^q = v^{q^2-1} = c$, say. So long as $y \notin K$, we can pick $a, b \in K$ such that $(\zeta - b)/a = \sigma(y)$ and we are done. The case of $y \in K$ is handled exactly as in (ii) above.

Lemma 3.2 *Let ζ be a root of irreducible quadratic polynomial $\phi \in \mathbf{F}_q[T]$. If $\mathbf{F}_q \subset K$ is a proper subfield, then there exists $b \in K$ such that $(\zeta - b)(\zeta - b^q)$ is a $(q+1)$-th power in K times a (q^2-1)-th power in $K(\zeta)$.*

Proof We do two cases, namely where q is even and ϕ has the form $T^2 + T + \lambda$ and where q is odd and ϕ has the form $T^2 - \lambda$. Other cases are handled similarly (see the comments at the end of this section). In both cases we pick any $u \in K - \mathbf{F}_q$.

For q even, set $b = (u^{q+1} + u + \lambda)/(u^q + u)$. We compute

$$\text{(E)} \quad (\zeta - b)(\zeta - b^q) = \frac{\bigl(\zeta(u^q + u) + (u^{q+1} + u + \lambda)\bigr)\bigl(\zeta(u^{q^2} + u^q) + (u^{q(q+1)} + u^q + \lambda)\bigr)}{(u^q + u)^{q+1}}.$$

The numerator of (E) is checked to be $\bigl((\zeta - u)(\zeta - u^q)\bigr)^{q+1}$.

For q odd, set $b = (u^{q+1} - \lambda)/(u^q - u)$. As for even characteristic, we compute

$$\text{(O)} \qquad (\zeta - b)(\zeta - b^q) = \frac{\bigl(\zeta(u^q - u) - (u^{q+1} - \lambda)\bigr)\bigl(\zeta(u^{q^2} - u^q) - (u^{q(q+1)} - \lambda)\bigr)}{(u^q - u)^{q+1}}.$$

As before, the numerator of (O) may be rewritten as $\bigl((\zeta - u)(\zeta - u^q)\bigr)^{q+1}$.

In both characteristics, the expression is $(u - b)^{q+1}$ times a $(q^2 - 1)$-th power of an element of $K(\zeta)$, as seen in

$$\left(\frac{(\zeta - u)(\zeta - u^q)}{u^q - u}\right)^{q+1} = \begin{cases} (u - b)^{q+1}\bigl(\zeta(u + \zeta)\bigr)^{q^2-1}, & \text{when } \operatorname{char}(K) > 2 \\ (u - b)^{q+1}(u + \zeta + 1)^{q^2-1}, & \text{when } \operatorname{char}(K) = 2. \end{cases}$$

Corollary 3.3 *Every cyclic extension of $K \neq \mathbf{F}_q$ of degree dividing $q^2 - 1$ is the splitting field of an equation of the form*

$$a^{q+1}x^{q^2-1} + a(b^q + b + 1)x^{q-1} + (b^2 + b + \lambda) \quad \bigl(\operatorname{char}(K) = 2\bigr)$$
$$a^{q+1}x^{q^2-1} + a(b^q + b)x^{q-1} + (b^2 - \lambda) \quad \bigl(\operatorname{char}(K) > 2\bigr),$$

where $\lambda \in \mathbf{F}_q$ is chosen so that $T^2 + T + \lambda$, respectively $T^2 - \lambda$, is irreducible over $\mathbf{F}_q$.

Proof In the case of characteristic two, pick $\lambda \in \mathbf{F}_q$ such that $\phi(T) = T^2 + T + \lambda$ is irreducible over $\mathbf{F}_q$. Then $\phi(aF + b) = a^{q+1}F^2 + a(b^q + b + 1)F + (b^2 + b + \lambda)$. Applying this to x and dividing by x yields the desired equation. The odd characteristic case proceeds similarly with $\phi(T) = T^2 - \lambda$ (λ chosen to make ϕ irreducible over $\mathbf{F}_q$).

Note The corollary still holds if $K = \mathbf{F}_q$ and the degree does not divide $q - 1$. If the degree does divide $q - 1$, then the extension is Kummer and so a splitting field for *e.g.* $ax^{q-1} + b$.

https://doi.org/10.4153/CMB-2000-035-5 Published online by Cambridge University Press

Example 3.1 **(See Example 1.1)** Let K be a field of characteristic 2 and L/K cyclic of degree 3. Then L is a splitting field over K of a polynomial of the form $y^3 + cy + c$ with $c = 1+b+b^2 (b \in K)$. Note that this also comes from Serre's characteristic-free generic equation $x^3 - bx^2 + (b-3)x - 1$ [S2] on setting $x = y + b$ in characteristic 2.

Example 3.2 **(See Example 1.2)** Let $\rho\colon G_K \to \mathrm{GL}_1(\mathbf{F}_9)$ be surjective, K of characteristic 3. This defines a C_8-extension L/K. We therefore have a tower of quadratic extensions $K \subset N \subset M \subset L$. All C_4-extensions (in odd characteristic) are determined by a triple (α, β, γ) of elements of K, where $\epsilon = \frac{\alpha^2}{\beta^2+\gamma^2}$, $N = K(\sqrt{\epsilon})$, and $M = K(\sqrt{\alpha + \beta\sqrt{\epsilon}})$. We calculate that our Drinfeld representation yields the C_4-extension with invariants $\bigl(-(b^2+1), b, 1\bigr)$.

It is easy to see when triples (α, β, γ) and (δ, η, θ) yield the same C_4-extension, namely if and only if

(1) $(\eta^2 + \theta^2)/(\beta^2 + \gamma^2)$ is a square in K,
(2) δ/α is the sum of two squares in K, and
(3) $\eta/\beta = m^2 - n^2\epsilon$ where $m, n \in K$.

In light of our result, we wonder whether all triples are equivalent to a Drinfeld triple $\bigl(-(b^2+1), b, 1\bigr)$. Using condition (2), we see that

$$\alpha = -\frac{b^2+1}{m^2+n^2},$$

in which form not every element α can be written. This is, however, exactly the criterion for M/K to be extended to a C_8-extension (as seen by computations in $\mathrm{Br}_2(K)$). Indeed, our results are equivalent to establishing the criterion for a C_4-extension of any field of characteristic 3 to extend to a C_8-extension.

Partway through the main result of this section, we made the choice $b = (u^{q+1} - \lambda)/(u^q - u)$ for odd characteristic, and $b = (u^{q+1} + u + \lambda)/(u^q - u)$ for even characteristic. We now explain this choice in the case of odd characteristic. A similar approach works in even characteristic.

Setting $y = ax^{q-1}$ in the second equation of the corollary leads to

$$y^{q+1} + (b^q + b)y + (b^2 - \lambda) = 0. \tag{$*$}$$

The field $K(y)$ is an important intermediate field between $L_{a,b,\phi}$ and K, as evidenced in the next section. The choice of b that we are discussing, is one that will ensure that the equation $(*)$ splits completely. The idea is to set $y = u - b$ which yields

$$(u^{q+1} - \lambda) - b(u^q - u) = 0. \tag{$\dagger$}$$

Hence the choice of b. The fact that the equation splits completely can be forcefully seen by the next lemma.

Lemma 3.4 *Let $\mu = 1/\lambda$ and H_μ be the image in $\mathrm{PGL}_2(\mathbf{F}_q)$ of the nonsplit Cartan subgroup*

$$\left\{\begin{pmatrix} \alpha & \beta \\ \mu\beta & \alpha \end{pmatrix} : (\alpha, \beta) \neq (0,0)\right\},$$

https://doi.org/10.4153/CMB-2000-035-5 Published online by Cambridge University Press

a cyclic group of order $q + 1$. Then

$$(u^{q+1} - \lambda) - b(u^q - u) = \prod_{\sigma \in H_\mu} \big(u - \sigma(U)\big),$$

where U is one root of $(\dagger)$ and σ acts by fractional linear transformation.

Proof The proof follows automatically by checking that $\sigma(U)$ satisfies $(\dagger)$.

4 Genus Constraints

In this section, we consider properties of $L_{a,b,\phi}/K$. Without loss of generality, we can replace K by its subfield $\mathbf{F}_q(a, b)$. The important facts are as follows.

Theorem 4.1 *Let $L = K(x)$ where x satisfies $\big(\phi(aF+b)\big)x = 0$ and $y = ax^{q-1}$. The extension $L/K(y)$ is Kummer and the equation satisfied by y has coefficients involving b but not a.*

Proof Letting $M = K(y)$, $L = M(x)$ is obtained by adjoining a $(q-1)$-th root of y/a. Since $\mathbf{F}_q \leq K$, this extension is Kummer.

To show that $\big(\phi(aF + b)\big)x$ is x times a polynomial in y, coefficients not involving a, it is sufficient to show this for $\big((aF + b)^n\big)x$. This can be proved by induction on n, using easily verified equation $(aF)^{m+1}x = a^{1+q+\cdots+q^m} x^{q^{m+1}} = y^{1+q+\cdots+q^m} \cdot x$ for every positive integer m.

It is therefore sufficient for our purposes to study the case of $K = \mathbf{F}_q(b)$ and $\phi = T + b$. (This case of the Drinfeld construction was first considered by Carlitz and, in greater detail, by Hayes [H].)

The idea is to calculate the genus of the intermediate field N of the extension L/K which has degree $\frac{q^d-1}{k(q-1)}$ over $\mathbf{F}_q(b)$ where k is a divisor of $\frac{q^d-1}{q-1}$ and of $[L : K]$. This intermediate field exists and is unique because the Galois group of L/K is cyclic of order dividing $\frac{q^d-1}{q-1}$.

Lemma 4.2 *The genus of N is*

$$g_N = \frac{1}{2}(d-2)\Big((q^d - 1)/\big(k(q-1)\big) - 1\Big).$$

Proof By Riemann-Hurwitz,

$$2g_N - 2 = -2\left(\frac{q^d - 1}{k(q-1)}\right) + \deg(\mathcal{D}),$$

where $\mathcal{D} = \mathcal{B}^s$, $\mathcal{B}$ is the totally ramified prime of N over (ϕ), and $s = e - 1 = \frac{q^d-1}{k(q-1)} - 1$. Then $\deg(\mathcal{B}) = d$ implies that

$$2g_N - 2 = -2\left(\frac{q^d - 1}{k(q-1)}\right) + d\left(\frac{q^d - 1}{k(q-1)} - 1\right),$$

whence the result.

Corollary 4.3 *The genus $g_N = 0$ if and only $d = 2$ or $k = \frac{q^d-1}{q-1}$.*

https://doi.org/10.4153/CMB-2000-035-5 Published online by Cambridge University Press

Example 4.1 This can now be used to produce an example of a representation that is not Drinfeld. We thank Lenstra for pointing this out. Let $K = \mathbf{F}_2(t)$ and $\rho\colon G_K \to \mathrm{GL}_1(\mathbf{F}_8)$ be the trivial representation. If ρ were Drinfeld, say associated to $\phi = T^3 + T + 1$, then, using Example 1.3, there would be $a, b \in K$ such that

$$a^7x^8 + a^3(b^4 + b^2 + b)x^4 + a(b^4 + b^3 + b^2 + 1)x^2 + (b^3 + b + 1)x = 0$$

would split completely. Setting $y = ax$, we would get a degree 7 equation in y over K, with coefficients involving only b. Then there would exist a point (Y, b) over K on the curve. It is easy to verify that it could not be a constant point. A non-constant point would give a genus 3 field $\mathbf{F}_2(Y, b)$ embedded in the genus 0 field $\mathbf{F}_2(t)$, contradicting Lüroth's theorem. The other choices for ϕ are handled likewise.

Theorem 4.4 *If $\rho\colon G_K \to \mathrm{GL}_1(\mathbf{F}_{q^d})$ is Drinfeld, then*

(1) $d = 1$ or $d = 2$ or
(2) $\pi \circ \rho$ surjects onto $\mathrm{GL}_1(\mathbf{F}_{q^d})/\,\mathrm{GL}_1(\mathbf{F}_q)$, where π is the quotient map

$$\mathrm{GL}_1(\mathbf{F}_{q^d}) \to \mathrm{GL}_1(\mathbf{F}_{q^d})/\,\mathrm{GL}_1(\mathbf{F}_q).$$

Proof Take k to be $\#\big(\pi \circ \rho(G_K)\big)$. Then b is such that N specializes to K and so by Lüroth, $g_N = 0$, leading to the desired result.

There are two important consequences to this, first that Drinfeld representations tend to have large images (results like this were already established by Goss [G, section 7.7]) and second that representations that are not Drinfeld certainly exist (by picking $d > 2$ and taking a representation which does not surject onto $\mathrm{GL}_1(\mathbf{F}_{q^d})/\,\mathrm{GL}_1(\mathbf{F}_q)$). In the next section, we show that there are many representations that are not Drinfeld but that are surjective.

5 Surjective Representations That Are Not Drinfeld

Take $q = 2$, $d = 3$. We assume that K does not contain $\mathbf{F}_8$ and set $K' = K\mathbf{F}_8$. Then $\mathrm{Gal}(K'/K) = \langle\sigma\rangle$ has order 3. We will always fix a choice of σ and of $\eta \in \mathbf{F}_8$ such that $\eta^3 = \eta + 1$ and $\sigma(\eta) = \eta^2$. We provide a method (that in fact generalizes to any $d > 2$ and to other q) of obtaining numerous representations that are not Drinfeld, so long as K satisfies a certain hypothesis (P) below.

Definition Let $S = \{\sigma(x)x^{-2} : x \in (K')^*\}$, a subgroup of the multiplicative group of K'. Say that K satisfies hypothesis (P) if there is a coset of S in $(K')^*$ which contains no element of the form $r + s\zeta$ for some $r, s \in K$ and some $\zeta \in \mathbf{F}_8$.

Theorem 5.1 *Suppose that K satisfies hypothesis (P). Then there exists a* surjective *representation (in fact many such) $G_K \to \mathrm{GL}_1(\mathbf{F}_{q^d})$, that is not Drinfeld.*

Proof Let $f(x) = x\sigma^{-1}(x^2)\sigma^{-2}(x^4)$, a homomorphism of the multiplicative group of K' to itself. Note that f satisfies two useful identities, (i) $\sigma\big(f(x)\big) = f(x)^2\sigma(x)^{-7}$ and (ii) $x^7 = f(x)^{-1}\sigma^{-1}\big(f(x)\big)^2$.

https://doi.org/10.4153/CMB-2000-035-5 Published online by Cambridge University Press

Pick $y \in K'$ such that the coset of y contains no element of the form $r + s\zeta (r, s \in K)$. Let $c = f(y)$ and $L' = K(v)$ with $v^7 = c$. Then L'/K is Galois with Galois group $C_3 \times C_7$. (Note that $v \notin K$, since otherwise $f(v) = v^7 = f(y)$ and, by the injectivity of f proven below, $y = v \in K$, a contradiction.)

We claim that c is not of the form $\big((\zeta - b)(\zeta - b^2)(\zeta - b^4)\big)/a^7$ times a 7-th power of an element of K' for any $a, b \in K$, and so the subfield L of degree 7 over K is not obtained by the Drinfeld construction and we are done.

We first show that f is injective. Suppose that $x \in K'$ satisfies $f(x) = 1$. By identity (ii), we get that $x^7 = 1$ and so $x = \zeta^i$ for some i. Since $f(\zeta^i) = \zeta^{3i}$, it follows that $x = \zeta^i = 1$.

If the subfield L of degree 7 over K is obtained by the Drinfeld construction, then c is of the form $k^7\big((\zeta - b)(\zeta - b^2)(\zeta - b^4)\big)/a^7$ for some $a, b \in K$, $k \in K'$. We check that $x = k^{-1}\sigma^{-1}(k^2)$ is a solution of $f(x) = k^7$ and so, by the injectivity of f, is the unique such solution. Then, $f\big(k^{-1}\sigma^{-1}(k^2)(\zeta - b)/a\big) = c = f(y)$, and so by the injectivity of f, $(\zeta - b)/a = yk\sigma^{-1}(k^{-2})$, which contradicts our choice of y.

It remains to make some comments on what fields K satisfy hypothesis (P) and what fields do not. It is immediately clear that every finite field of characteristic 2 fails hypothesis (P)—indeed, as noted at the start of Section 3, the property of being Drinfeld depends only on the field cut out and a finite K possesses a unique degree 7 extension.

Lemma 5.2 *Suppose $k \in K$. Denote the following projective curves by $Q(1, k)$, $Q(2, k)$, and $Q(3, k)$.*

$Q(1, k)$: $ku^4 + ku^3v + u^2v^2 + ku^2v^2 + uv^3 + kuv^3 + kv^4 + u^3w + ku^3w + ku^2vw + kv^3w + v^2w^2 + kv^2w^2 + uw^3 + vw^3 + kvw^3 + kw^4 = 0.$

$Q(2, k)$: $u^4 + u^3v + ku^3v + u^2v^2 + ku^2v^2 + uv^3 + v^4 + u^3w + u^2vw + kuv^2w + v^3w + kv^3w + ku^2w^2 + kuvw^2 + v^2w^2 + kv^2w^2 + kuw^3 + vw^3 + w^4 = 0.$

$Q(3, k)$: $u^4 + ku^4 + u^3v + kuv^3 + v^4 + kv^4 + ku^3w + u^2vw + ku^2vw + kuv^2w + v^3w + ku^2w^2 + kuvw^2 + uw^3 + kuw^3 + kvw^3 + w^4 + kw^4 = 0.$

If there are no points, coordinates in K, on $Q(1, k) \cup Q(2, k) \cup Q(3, k)$, then K satisfies hypothesis (P).

Proof Suppose that K does not satisfy (P). Then $\eta + k\eta^2$ is in the same coset of S as some $r + s\zeta (r, s \in K, \zeta \in \mathbf{F}_8 - \mathbf{F}_2)$. So there is some $x = u + v\eta + w\eta^2$ ($u, v, w \in K$ not all 0) such that $\eta + k\eta^2 = \sigma(x)x^{-2}(r + s\zeta)$.

Suppose first that $\zeta = \eta$. Writing this in terms of u, v, w and clearing denominators, we get, by comparing coefficients of 1, η, η^2, three linear equations in r, s. We use two of these to solve for r, s and plug in the third to get that some expression in u, v, w is 0. The numerator of that expression is $Q(1, k)$.

Likewise, $\zeta = 1 + \eta$ yields $Q(1, k)$, $\zeta = \eta^2$ or $= 1 + \eta^2$ yields $Q(2, k)$, and $\zeta = \eta + \eta^2$ or $= 1 + \eta + \eta^2$ yields $Q(3, k)$. Since this exhausts the possibilities for ζ, this provides the desired contradiction.

This lemma is very useful in establishing that certain fields satisfy (P). With a little more work, we can establish a converse. As in the above proof, we might ask whether $a + b\eta + c\eta^2$

https://doi.org/10.4153/CMB-2000-035-5 Published online by Cambridge University Press

is in the same coset as some $r + s\zeta(a, b, c, r, s \in K)$. Proceeding as above yields $X(a, b, c)$, a union of three homogeneous quartics, with $X(0, 1, k)$ being $Q(1, k) \cup Q(2, k) \cup Q(3, k)$.

Lemma 5.3 *If $X(a, b, c)$ has no points over K for some choice of $a, b, c \in K$, then K satisfies hypothesis (P). If K satisfies hypothesis (P), then there is some choice of $a, b, c \in K$ for which $X(a, b, c)$ has no points over K.*

Proof Exactly as for the previous lemma.

Theorem 5.4 *The field $\mathbf{F}_2(t)$ satisfies hypothesis (P).*

Proof Setting $K = \mathbf{F}_2(t)$ and $k = t$ in Lemma 5.2, one checks that $Q(1, k) \cup Q(2, k) \cup Q(3, k)$ has no points over K.

This then yields, by Theorem 5.1, examples of surjective representations that are not Drinfeld.

6 Higher Degree Representations

Cases where $r > 1$ are poorly understood, except in one instance, namely when the given representation is into $\mathrm{GL}_r(\mathbf{F}_q)$. In that case, we can say the following.

Theorem 6.1 *Let K be infinite and $\rho\colon G_K \to \mathrm{GL}_r(\mathbf{F}_q)$ be a representation. Then ρ is Drinfeld. This is not necessarily true if K is finite.*

Proof Suppose that K is infinite. Let L be the fixed field of the kernel of ρ. Let H denote $\mathrm{Gal}(L/K)$, which is isomorphic to the image of ρ. Let V be the $\mathbf{F}_q[H]$-module corresponding to the embedding of H in $\mathrm{GL}_r(\mathbf{F}_q)$. By the normal basis theorem, V embeds $\mathbf{F}_q[H]$-linearly in the additive group L^+ of L (since L^+ contains free $\mathbf{F}_q[H]$-modules of arbitrarily high finite rank and by duality for group rings these are also cofree of arbitrary finite rank). Let $g(x) = \prod_{\alpha \in V}(x - \alpha)$. Since V is an $\mathbf{F}_q$-vector space, the polynomial g is indeed additive and so lies in $K\{F\}$. Define the Drinfeld module by having T map to $g \in K\{F\}$. Consequently the T-division points are the roots of g, *i.e.*, V, with the given action. Finally, the extension of K generated by the elements of V, $K(V)$, is indeed L, since ρ factors through $\mathrm{Gal}\big(K(V)/K\big)$.

Suppose that K is finite. If ρ is Drinfeld, then ϕ has degree $d = 1$, say $\phi = aT + b$. Then $\phi\big(g(F)\big) = ag(F) + b = h(F)$, say, so V is the set of zeros in K^{sep} of $h(F)x = 0$ and is an $\mathbf{F}_q$-subspace of L^+, where L is the fixed field of the kernel of ρ. The action of $H = \mathrm{Gal}(L/K)$ on L^+ restricts to V to produce ρ, but for large r, V will not embed in L^+, which is a free $\mathbf{F}_q[H]$-module of rank $[K : \mathbf{F}_q]$.

References

[FM] J.-M. Fontaine and B. Mazur, *Geometric Galois Representations.* In: Elliptic curves and modular forms (eds. J. H. Coates and S. T. Yau), Proceedings of a conference held in Hong Kong, December 18–21, 1993. International Press, Cambridge, MA, and Hong Kong.

[D] V. G. Drinfeld, *Elliptic Modules.* Math. USSR Sbornik **23**(1974), 561–592.

https://doi.org/10.4153/CMB-2000-035-5 Published online by Cambridge University Press

[G] D. Goss, *Basic structures of function field arithmetic.* Ergeb. Math. Grenzgeb. **35**, Springer, 1996.

[H] D. Hayes, *Explicit class field theory for rational function fields.* Trans. Amer. Math. Soc. **189**(1974), 77–91.

[O] D. Ose, *Toward a deformation theory for Galois representations of function fields.* J. Number Theory **70**(1998), 37–61.

[S] J.-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Duke Math. J. **54**(1987), 179–230.

[S2] ______, *Topics in Galois theory.* Bartlett and Jones, 1992.

Department of Mathematics
University of Illinois
Urbana, Illinois 61801
USA
email: boston@math.uiuc.edu

Department of Mathematics
Bucknell University
Lewisburg, Pennsylvania 17837
USA
email: ose-d@member.ams.org

https://doi.org/10.4153/CMB-2000-035-5 Published online by Cambridge University Press