Carlitz Modules and the Function Field Analogue of Kronecker-Weber

Li-Chung Chen

May 6, 2002

1 Introduction

Hilbert's 9th problem asks for an explicit class field theory for all number fields. This has proved difficult, and the only known cases are for $\mathbb{Q}$ (cyclotomic theory) and for imaginary quadratic number fields (the theory of complex multiplication). However, the function field analogue has been solved, as independent work by L. Carlitz, D. Hayes, and V. Drinfeld has provided explicit construction of all abelian extensions of any global function field of positive characteristic.

This paper focuses on Carlitz's function field analogues to cyclotomic number fields. Using Carlitz modules, we will construct explicit abelian extensions of $\mathbb{F}(T)$, where $\mathbb{F}$ is a finite field, and we will state Hayes' result on the maximal abelian extensions of $\mathbb{F}(T)$. Then we will briefly discuss Drinfeld's generalization for general global function fields.

2 Drinfeld Modules Over $\mathbb{F}(T)$

Let $\mathbb{F}$ be a finite field with $q = p^s$ elements, and set $A = \mathbb{F}[T]$ and $k = \mathbb{F}(T)$. For a commutative k-algebra B (which we will later take to be the algebraic closure of k, $\bar{k}$), let $\tau : B \to B$ be given by $\tau(x) = x^q$. Because k has characeristic p, $(x+y)^p = x^p + y^p$ holds in B. Repeated application of this equality shows that τ is additive. In fact, a similar argument shows that any polynomial of the form $a_0 x + a_1 x^q + \ldots + a_r x^{q^r}$ acts additively on B. The set of these polynomials forms a ring (under composition) that is identified with the "twisted" polynomial ring $k\langle\tau\rangle$, in which we have $\tau a = a^q \tau$ for all $a \in k$. In other words, we will consider elements of $k\langle\tau\rangle$ to be polynomials that act on B, with $\tau \leftrightarrow x^q$ and $[1 \in k] \leftrightarrow x$.

Now we can define a Drinfeld module over $k = \mathbb{F}(T)$:

Definition 2.1 *A Drinfeld module for A defined over k is an $\mathbb{F}$-algebra homomorphism $\rho : A \to k\langle\tau\rangle$ such that*

1. *the constant term of ρ_a is a for all $a \in A$, and*
2. *$\rho_a \notin k$ for at least one $a \in A$.*

This is called a module because any commutative k-algebra B can be made into an A-module B_ρ by defining

$$a \cdot u = \rho_a(u) \text{ for all } a \in A, u \in B.$$

In this special case where $A = \mathbb{F}[T]$, giving ρ is the same as specifying ρ_T. The first condition implies that the constant term of ρ_T is T, and the converse clearly holds. Now if $\rho_T \in k$, then ρ would map into k. Hence the second condition is equivalent to $\rho_T \notin k$. Therefore, a Drinfeld module for A over k is given by specifying a nonconstant ρ_T with constant term T. We say that the *rank* of the Drinfeld module ρ is $\deg(\rho_T)$.

Consider the Drinfeld module given by $\rho_T = T + c_1\tau + c_2\tau^2 + \ldots + c_r\tau^r$, where $c_i \in k$ and $c_r \neq 0$. This induces an A-module structure $\bar{k}_\rho$ on $\bar{k}$ as described above. For nonzero $a \in A$, define the torsion submodule

$$\Lambda_\rho[a] = \left\{\lambda \in \bar{k} : \rho_a(\lambda) = 0\right\}.$$

It is clear by induction that ρ_{T^n} is a degree-rn polynomial in τ with constant term T^n. Hence for $a \in A$, ρ_a has degree $r\deg(a)$ in τ (and degree $q^{r\deg(a)}$ in x) with constant term a. But $\mathbb{F}\langle\tau\rangle$ corresponds to polynomials in x whose monomials have degrees that are powers of q. Thus the derivative of $\rho_a(x)$ is a and $\rho_a(x)$ is separable. Since $\Lambda_\rho[a]$ is just the set of roots of $\rho_a(x)$, it has size $q^{r\deg(a)}$. This information is sufficient to determine $\Lambda_\rho[a]$:

Theorem 2.2 *Let ρ be a Drinfeld module of rank r. Then for any nonzero $a \in A$, $\Lambda_\rho[a] \cong (A/aA)^r$ as A-modules (and hence as (A/aA)-modules because both sides are annihilated by a).*

Proof

First consider the case that $a = P^e$ is a prime power. Since $\Lambda_\rho[a]$ is finite, by the structure theorem of modules over a PID, we obtain an A-module isomorphism

$$\Lambda_\rho[P^e] \cong A/{Q_1}^{f_1}A \oplus A/{Q_2}^{f_2}A \oplus \ldots \oplus A/{Q_r}^{f_r}A$$

for some irreducible polynomials Q_i. But P^e annihilates $\Lambda_\rho[P^e]$, so it annihilates each $A/{Q_i}^{f_i}A$ and forces $Q_i/P \in \mathbb{F}^*$ (so we may assume $Q_i = P$) and $f_i \leq e$ for all i.

Now note that

$$\Lambda_\rho[P] = \{\lambda \in \Lambda_\rho[P^e] : \rho_P(\lambda) = 0\}$$

because any element annihilated by P is also annihilated by P^e. The left hand side has $q^{r\deg(P)}$ elements as determined earlier, and the right hand side has $|(A/PA)^t| = q^{t\deg(P)}$ elements. Hence $t = r$. This implies that $\Lambda_\rho[P^e]$ has $q^{f_1+\dots+f_r}$ elements. But we already know that $\Lambda_\rho[P^e]$ has $q^{r\deg(P^e)} = q^{re\deg(P)}$ elements and that each $f_i \le r$. Hence $f_i = r$ for all i and we are done with the prime power case.

For the general case, let the prime decomposition of a be $a = \alpha {P_1}^{e_1}{P_2}^{e_2}\dots{P_t}^{e_t}$ (where $\alpha \in \mathbb{F}^*$). We claim that $\Lambda_\rho[a] = \oplus_{i=1}^t \Lambda_\rho[{P_i}^{e_i}]$. Clearly $\Lambda_\rho[{P_i}^{e_i}] \subset \Lambda_\rho[a]$ for all i. Let $a_i = \frac{a}{\alpha {P_i}^{e_i}}$. Because the a_i's have greatest common divisor 1, there exist $b_i \in A$ such that $\sum_{i=1}^t b_i a_i = 1$. Then for any $m \in \Lambda_\rho[a]$, $m = \sum_{i=1}^t b_i(a_i m)$. But $a_i m \in \Lambda_\rho[{P_i}^{e_i}]$ because $P_i^{a_i}(a_i m) = \alpha^{-1}am = 0$. Thus $\Lambda_\rho[a] = \sum_{i=1}^t \Lambda_\rho[{P_i}^{e_i}]$. Now if we have $c_i \in \Lambda_\rho[{P_i}^{e_i}]$ such that $\sum_{i=1}^t c_i = 0$, then $0 = a_j \sum_{i=1}^t c_i = a_j c_j$ because ${P_i}^{e_i}$ divides a_j whenever $i \ne j$. But a_j is a unit in $A/{P_j}^{e_j}A$ and $\Lambda_\rho[{p_j}^{e_j}]$ is an $(A/{P_j}^{e_j}A)$-module. Thus $c_j = 0$ for all j and $\Lambda_\rho[a] = \oplus_{i=1}^t \Lambda_\rho[{P_i}^{e_i}]$.

Hence by the prime power case, we have

$$\Lambda_\rho[a] = \oplus_{i=1}^t \Lambda_\rho[{P_i}^{e_i}] \cong \oplus_{i=1}^t (A/{P_i}^{e_i}A)^r \cong (A/aA)^r$$

(using the Chinese remainder theorem).

□

Let $K_{\rho,a} = k(\Lambda_\rho[a])$. It was noted above that $\Lambda_\rho[a]$ is the set of roots of a separable polynomial. Hence $K_{\rho,a}/k$ is a Galois extension. Because $\rho_a(x) \in k[x]$, $\rho_a(\lambda) = 0$ iff $\rho_a(\sigma\lambda) = 0$ for all $\sigma \in \mathrm{Gal}(K_{\rho,a}/k)$. Thus ρ maps $\Lambda_\rho[a]$ into itself bijectively. But further, for any $b \in A$, $\lambda \in \Lambda_\rho[a]$, and $\sigma \in \mathrm{Gal}(K_{\rho,a}/k)$, we have $\sigma(\rho_b\lambda) = \rho_b(\sigma\lambda)$ because $\rho_b(x) \in k[x]$. Thus σ acts as an A-module automorphism on $\Lambda_\rho[a]$ and hence as an A/aA-module automorphism because a annihilates $\Lambda_\rho[a]$. Therefore, we get a homomorphism

$$\mathrm{Gal}(K_{\rho,a}/k) \to \mathrm{Aut}_{A/aA}(\Lambda_\rho[a]).$$

Now if $\sigma \in \mathrm{Gal}(K_{\rho,a}/k)$ maps to the identity, then it fixes every element in $\Lambda_\rho[a]$. But these elements generate $K_{\rho,a}$, so σ must be the identity. Therefore the above map is injective, and we have established this important fact:

Proposition 2.3 *If $K_{\rho,a} = k(\Lambda_\rho[a])$, then $K_{\rho,a}/k$ is Galois and there is an injection*

$$\mathrm{Gal}(K_{\rho,a}/k) \to GL_r(A/aA).$$

Corollary 2.4 *If ρ has rank 1, then $K_{\rho,a}/k$ is an abelian extension.*

Proof

This follow immediately because $GL_1(A/aA) = (A/aA)^*$ is abelian and $\mathrm{Gal}(K_{\rho,a}/k)$ is a subgroup of it.

□

Therefore, a Drinfeld module (on $\mathbb{F}[t]$ over $\mathbb{F}(t)$) given by $\rho_T = T + c\tau$ (where $c \in k^*$) produces many examples of abelian extensions of $\mathbb{F}(t)$. We will be interested in the special case where ρ is given by $\rho_T = T + \tau$. In this case we denote ρ as C and call it a *Carlitz module.*

3 Carlitz Modules and Their Induced Extensions

In this section, we will work solely with Carlitz modules and hence will abbreviate Λ for $\Lambda_C = \Lambda_\rho$, Λ_a for $\Lambda_C[a]$, and K_a for $K_{C,a}$. Corollary 2.4 shows that $\mathrm{Gal}(K_a/k)$ is a subgroup of $(A/aA)^*$ for $a \neq 0$. We will show that $\mathrm{Gal}(K_a/k) \cong (A/aA)^*$, and along the way we will establish some properties of Carlitz modules. We will see that K_a is analogous to cyclotomic extensions of $\mathbb{Q}$.

First some important remarks about the polynomial $C_a(x)$:

Lemma 3.1 *For nonzero $a \in A$ of degree d, $C_a(x)$ is of the form*

$$[a,0]x + [a,1]x^q + \ldots + [a,d]x^{q^d}$$

with $[a,0] = a$, $[a,d] \neq 0$, and each $[a,i] \in A$. If a is monic, then $[a,d] = 1$.

Proof

Reduce to the case $a = T^n$ and induct on n. The base case works because $C_T = T + \tau$ is monic in $A\langle\tau\rangle$. Note that this lemma fails for any other rank-1 Drinfeld module.

□

Recall that $\Lambda_a \cong A/aA$ as A-modules. Hence it has $\Phi(a) = |(A/aA)^*|$ generators. If λ_a is a generator, then every $\lambda \in \Lambda_a$ is of the form $\phi_b(\lambda_a)$ for some $b \in A$. But $\phi_b(x)$ is just a polynomial in $k[x]$, so $\lambda \in k(\lambda_a)$. Therefore, $K_a = k(\Lambda_a) = k(\lambda_a)$.

Let $\mathcal{O}_a$ denote the integral closure of A in K_a. The integral closure of A in k is A because A is factorial and hence integrally closed. Thus k and A are analogous to $\mathbb{Q}$ and $\mathbb{Z}$, and $(K_a, \mathcal{O}_a)$ is analogous to a rational cyclotomic field and its ring of integers.

Lemma 3.2 *Suppose $\lambda_a \in \Lambda_a$ is a generator and $b \in A$ is relatively prime to a. Then $C_b(\lambda_a)/\lambda_a$ is a unit in $\mathcal{O}_a$.*

Proof

It is clear that if $a = \beta a'$ for a' monic and $\beta \in \mathbb{F}^*$, then $\Lambda_{a'} = \Lambda_a$ and the other corresponding items are equal. Thus we may assume that a is monic.

By Lemma 3.1, $C_a(\lambda_a) = 0$ implies $\lambda_a \in \mathcal{O}_a$. Further, $C_b(\lambda_a)/\lambda_a$ is a polynomial in λ_a with coefficients in A, so it is also in $\mathcal{O}_a$. Thus it suffices to check that $\lambda_a/C_b(\lambda_a)$ is in $\mathcal{O}_a$.

Because a and b are relatively prime, there exist $f, g \in A$ such that $fb = 1 + ga$. Then $C_f C_b = C_1 + C_g C_a$ and $C_f(C_b(\lambda_a)) = \lambda_a + C_g(C_a(\lambda_a)) = \lambda_a$. Hence

$$\lambda_a/C_b(\lambda_a) = C_f(C_b(\lambda_a))/C_b(\lambda_a).$$

Now $C_b(\lambda_a)$ is a root of $C_a(x)$ and is hence in $\mathcal{O}_a$. Thus similar to above, $C_f(C_b(\lambda_a))/C_b(\lambda_a)$ is a polynomial in $C_b(\lambda_a)$ with coefficients in A; thus $\lambda_a/C_b(\lambda_a) \in \mathcal{O}_a$.

□

With the lemma, we can do the prime power case:

Proposition 3.3 *Suppose $P \in A$ is monic irreducible and $e \geq 1$. Then K_{P^e} is totally ramified with ramification index $\Phi(P^e)$ at the prime PA, but is unramified at all other primes. Hence*

$$[K_{P^e} : k] = \Phi(P^e) \text{ and } \mathrm{Gal}(K_{P^e}/k) \cong (A/P^eA)^*.$$

Finally, the prime ideal above PA is $(\lambda) = \lambda\mathcal{O}_{P^e}$, where λ is any generator of Λ_{P^e}.

Proof

Let λ be a generator of Λ_{P^e}. It satisfies the monic polynomial $C_{P^e}(x) \in A[x]$ and is thus in $\mathcal{O}_{P^e}$. Because $A = \mathbb{F}[T]$ is a factorial integral domain, by Gauss' lemma the minimal polynomial $g(x)$ of λ is a monic polynomial in $A[x]$. Hence $C_{P^e}(x) = f(x)g(x)$ where $f(x) \in A[x]$.

By Lemma 3.1, the derivative of $C_{P^e}(x)$ is P^e. Thus $P^e = C'_{P^e}(\lambda) = f(\lambda)g'(\lambda) + f'(\lambda)g(\lambda) = f(\lambda)g'(\lambda)$. Because λ is a generator, we showed above that $K_{P^e} = k(\lambda)$. Hence $g'(\lambda)$ is contained in the different $\mathcal{D}$ of $\mathcal{O}_{P^e}/A$. Now because $f(x) \in A[x]$ and $\lambda \in \mathcal{O}_{P^e}$, we see that $f(\lambda) \in \mathcal{O}_{P^e}$. Hence for any prime ideal $I \subset \mathcal{O}_{P^e}$,

$$\begin{aligned} I \text{ ramifies over } k &\Longrightarrow I|\mathcal{D} \\ &\Longrightarrow P^e = f(\lambda)g'(\lambda) \in g'(\lambda)\mathcal{O}_{P^e} \subset \mathcal{D} \subset I \\ &\Longrightarrow P \subset I \cap A \\ &\Longrightarrow I \text{ is over } PA. \end{aligned}$$

Thus PA is the only possible prime ideal in A ramified in $\mathcal{O}_{P^e}$.

Let $d = \deg(P)$. Because $\Lambda_{P^e} \cong A/P^eA$, we see that λ is a generator of Λ_{P^e} iff $C_{P^e}(\lambda) = 0$ and $C_{P^{e-1}}(\lambda) \neq 0$. Thus the $\Phi(P^e)$ generators are all the roots of

$$\begin{aligned} \frac{C_{P^e}(x)}{C_{P^{e-1}}(x)} &= \frac{C_P(C_{P^{e-1}}(x))}{C_{P^{e-1}}(x)} \\ &= P + [P,1]C_{P^{e-1}}(x)^{q-1} + \ldots + [P,d]C_{P^{e-1}}(x)^{q^d-1} \end{aligned}$$

(using Lemma 3.1). Note that this polynomial has degree $q^{\deg(P^{e-1})}(q^d-1) = q^{d(e-1)}(q^d-1) = \Phi(P^e)$. This polynomial and Lemma 3.2 imply that

$$P = \pm \prod_{\text{generator } \lambda} \lambda = \lambda^{\Phi(P^e)} \times \text{ unit}.$$

Hence $P\mathcal{O}_{P^e} = (\lambda)^{\Phi(P^e)}$.

Thus if $I \subset \mathcal{O}_{P^e}$ is a prime above PA, then $I \mid \lambda$ and $e(I/PA)$ is a multiple of $\Phi(P^e)$. In particular, $[K_{p^e} : k] \geq e(I/PA) \geq \Phi(P^e)$. However, since $K_{p^e} = k(\lambda)$ and λ is a root of the degree-$\Phi(P^e)$ polynomial above, we must have $[K_{p^e} : k] \leq \Phi(P^e)$. Therefore, we must have equalities and $[K_{p^e} : k] = e(I/PA) = \Phi(P^e)$. Since K_{p^e}/k is Galois, we have $efr = [K_{p^e} : k]$ and hence $f = r = 1$, i.e. PA is totally ramified and there is only one prime above PA. If (λ) factors, then there would either be more than one prime above PA or a larger ramification index. Hence (λ) is prime and is the only prime above PA.

Lastly, we already know that $\mathrm{Gal}(K_{P^e}/K)$ is a subgroup of the group $(A/P^eA)^*$ of order $\Phi(P^e)$. Because $\mathrm{Gal}(K_{P^e}/K)$ has order $\Phi(P^e)$, it must be the entire group.

$\square$

The general case now follows fairly directly:

Theorem 3.4 *Suppose $a = \alpha P_1{}^{e_1} P_2{}^{e_2} \ldots P_t{}^{e_t}$ is the prime decomposition of a, where each P_i is monic. Then K_a is the compositum of the fields $K_{P_i{}^{e_i}}$. The only ideals in A that ramify in $\mathcal{O}_a$ are the P_iA's. Furthermore, $[K_a : k] = \Phi(a)$, from which it follows that*

$$\mathrm{Gal}(K_a/k) \cong (A/aA)^*.$$

Proof

Set $a_i = \frac{m}{\alpha {P_i}^{e_i}}$. Let λ_a be a generator of $\Lambda_a \cong A/aA$. Then $\lambda_{{P_i}^{e_i}} = C_{a_i}(\lambda_a)$ is a generator of $\Lambda_{{P_i}^{e_i}} \cong a_i(A/aA)$. Thus $K_{{P_i}^{e_i}} = k(\lambda_{{P_i}^{e_i}}) = k(C_{a_i}(\lambda_a)) \subset k(\lambda_a) = K_a$, and we have $\prod_{i=1}^{t} K_{{P_i}^{e_i}} \subset K_a$.

Conversely, because the a_i's have greatest common divisor 1, there exist polynomials $b_i \in A$ such that $\sum_{i=1}^{t} b_i a_i = 1$. Thus

$$\lambda_a = \sum_{i=1}^{t} C_{b_i}(C_{a_i}(\lambda_a)) = \sum_{i=1}^{t} C_{b_i}(\lambda_{{P_i}^{e_i}}) \in \prod_{i=1}^{t} K_{{P_i}^{e_i}}.$$

Since λ_a generates K_a, we have $\prod_{i=1}^{t} K_{{P_i}^{e_i}} = K_a$.

Next, if $PA \subset A$ is a prime different from each P_iA, then by Proposition 3.3 it is unramified in every $K_{{P_i}^{e_i}}$. Hence it is also unramified in the compositum K_a. Conversely, each P_iA is ramified in K_a because it is already ramified in $K_{{P_i}^{e_i}}$.

Now we prove that $[K_a : k] = \Phi(a)$ by inducting on t. The base case $t = 1$ is exactly Proposition 3.3. If the result holds for $t-1$, then $[K_{a_t} : k] = \Phi(a_t)$. But by the above and by Proposition 3.3, P_tA is unramified in K_{a_t} and totally ramified in $K_{{P_t}^{e_t}}$. Hence K_{a_t} and $K_{{P_t}^{e_t}}$ are linearly disjoint over K, and

$$[K_a : k] = [K_{a_t} : k][K_{{P_t}^{e_t}} : k] = \Phi(a_t)\Phi({P_t}^{e_t}) = \Phi(a).$$

Induction is complete. So once again, because $\mathrm{Gal}(K_a/k)$ is a subgroup of $(A/aA)^*$ of the correct size, it must be the entire group.

□

4 The Maximal Abelian Extension of $\mathbb{F}(t)$

From the preceding discussion, the compositum $k(\Lambda)$ of all the fields K_a (for nonzero monic $a \in A$) is an abelian extension of k. Further, it is clear that $k(\Lambda) = \varinjlim_{a\neq 0} K_a$ and that $\mathrm{Gal}(k(\Lambda)/k) \cong \varprojlim_{a\neq 0}(A/aA)^*$, which is analogous to $\mathrm{Gal}(\mathbb{Q}(\lambda_\infty)/\mathbb{Q}) \cong \varprojlim_{m}(\mathbb{Z}/m\mathbb{Z})^* = \widehat{\mathbb{Z}}^*$ for number fields.

To construct more abelian extensions, we substitute $1/T$ for T everywhere above and obtain new but isomorphic abelian extensions. In particular, $K_{T^{n+1}}$ becomes what we call $k(\Lambda_{T^{-(n+1)}})$, whose Galois group over k is still of order $\Phi(T^{n+1}) = q^n(q-1)$. Since $(q^n, q-1) = 1$, the Galois group decomposes uniquely into the product of groups of order q^n and $q-1$. Let L_n be the fixed field of the order-$(q-1)$ subgroup. Then L_n/k is still an abelian extension. Let $L_\infty = \prod_{n=1}^{\infty} L_n$.

However, we have not yet obtained all the abelian extensions of k. It can be shown that the constant fields (i.e. the intersection with the algebraic closure $\bar{\mathbb{F}}$) of $k(\Lambda)$ and L_∞ are both $\mathbb{F}$. In other words, $k(\Lambda)$ and L_∞ are what are called *geometric* extensions of k. By extending the constant field, we obtain another abelian extension:

Proposition 4.1 $\mathrm{Gal}(\bar{\mathbb{F}}(T)/\mathbb{F}(T)) \cong \widehat{\mathbb{Z}}$.

Proof

We claim that $\mathrm{Gal}(\bar{\mathbb{F}}(T)/\mathbb{F}(T)) \cong \mathrm{Gal}(\bar{\mathbb{F}}/\mathbb{F})$. Any element $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}/\mathbb{F})$ extends to an element in $\mathrm{Gal}(\bar{\mathbb{F}}(T)/\mathbb{F}(T))$ by setting $\sigma(T) = T$. Conversely, if $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}(T)/\mathbb{F}(T))$ and $x \in \bar{\mathbb{F}}$, then x is algebraic over $\mathbb{F}$ (which is fixed by σ), so $\sigma(x)$ is also algebraic over $\mathbb{F}$ and $\sigma(x) \in \bar{\mathbb{F}}$. Thus σ sends $\bar{\mathbb{F}}$ to itself, and σ is the extension of an element of $\mathrm{Gal}(\bar{\mathbb{F}}/\mathbb{F})$.

Now $\mathbb{F}$ is a finite field of size q. Hence $\bar{\mathbb{F}} \cong \varinjlim_d \mathbb{F}_{q^d}$ and $\mathrm{Gal}(\bar{\mathbb{F}}(T)/\mathbb{F}(T)) \cong \mathrm{Gal}(\bar{\mathbb{F}}/\mathbb{F}) \cong \varprojlim_d \mathbb{Z}/d\mathbb{Z} = \widehat{\mathbb{Z}}$.

$\square$

Now we can state the function-field analogue of the Kronecker-Weber theorem:

Theorem 4.2 *(Hayes) $k(\Lambda)$, L_∞, and $\bar{\mathbb{F}}(T)$ are linearly disjoint over k and generate the maximal abelian extension of k.*

The proof uses class field theory and can be seen in [2] or [3].

5 Drinfeld Modules

Finally, we examine Drinfeld modules, the generalization of Carlitz modules over function fields other than $\mathbb{F}(t)$, and suggest how they relate to abelian extensions. We begin with some preliminary setup and definitions.

Definition 5.1 *A function field k over $\mathbb{F}$ is an extension of $\mathbb{F}$ of transcendence degree* 1.

Definition 5.2 *A prime of a function field $k/\mathbb{F}$ is a discrete valuation ring R with maximal ideal P such that $\mathbb{F} \subset R \subset k$ and R has quotient field k. This prime is referred to as P, and the associated valuation is denoted* $\mathrm{ord}_P(\cdot)$.

Now let $\mathbb{F} = \mathbb{F}_q$ and let $k/\mathbb{F}$ be a function field with constant field $\mathbb{F}$. Let ∞ be a fixed prime of k and let A be the ring of elements of k whose only poles are at ∞ (i.e. have nonnegative valuations at all other primes). Let L be a field containing $\mathbb{F}$. As before, regard τ as the map raising an element to the qth power, and let $L\langle\tau\rangle$ be the twisted polynomial ring with relation $\tau a = a^q \tau$ for $a \in L$. Fix an $\mathbb{F}$-algebra homomorphism $\delta : A \to L$. Then

Definition 5.3 *A Drinfeld A-module over L is an $\mathbb{F}$-algebra homomorphism $\rho : A \to L\langle\tau\rangle$ such that for all $a \in A$, the constant coefficient of ρ_a is $\delta(a)$. Also, we require that the image of ρ not be contained in L. The set of all such ρ is denoted* $\mathrm{Drin}_A(L)$.

Similar to before, if Ω is an L-algebra, then a Drinfeld module makes Ω into an A-module Ω_ρ by setting $a \cdot u = \rho_a(u)$ for $a \in A$, $u \in \Omega$. This construction applies to M, a fixed algebraically closed field extension of L. Thus we can define the torsion submodule $M_\rho[a] = \{u \in M_\rho : \rho_a(u) = 0\}$ as before.

Note that the above definition is consistent with our prior definition of Drinfeld modules over $\mathbb{F}(T)$. There $k = \mathbb{F}(T)$, ∞ is the prime at infinity, $A = \mathbb{F}[T]$, $L = k$, and δ is the inclusion. There is something to check here, namely that $\mathbb{F}[T]$ is the set of elements whose only poles are at ∞. Now by ∞ we mean the valuation where for polynomials $f, g \in \mathbb{F}[T]$, $\mathrm{ord}_\infty(f/g)$ is the highest exponent in g minus the highest exponent in f. It can be shown that the other primes of k correspond to nonzero prime ideals $P \subset \mathbb{F}[T]$, with valuation $\mathrm{ord}_P(z)$ being the exponent of P in the prime factorization of z. Hence $\mathbb{F}[T]$ is indeed the set of elements regular at all the non-∞ primes.

In the case over $\mathbb{F}(T)$, giving a Drinfeld module is the same as setting ρ_T to be a nonconstant polynomial with constant T. The existence of Drinfeld modules in general is less clear, but it can be shown using analytic methods. The construction is similar to the construction of elliptic curves over the complex numbers $\mathbb{C}$ by means of two-dimensional $\mathbb{Z}$-lattices and the associated Weierstrass $\mathcal{P}$-functions.

Now in general δ need not be injective. Let $Q = \ker(\delta)$. Then Q is a prime ideal of A because A/Q is contained in the integral domain L. We say that Q is the *A-characteristic of L*. Then the following theorem defines the rank of a Drinfeld module:

Theorem 5.4 *Let $\rho \in \mathrm{Drin}_A(L)$, let Q be the A-characteristic of L, and let M be an algebraically closed field containing L. If $P \neq Q$ is a nonzero prime ideal of A and $e \geq 1$, then there exist a positive integer r independent of P and e such that*

$$M_\rho[P^e] \cong (A/P^e)^r.$$

If $Q \neq (0)$ and $e \geq 1$, then there exist an integer h, independent of e, such that

$$M_\rho[Q^e] \cong (A/Q^e)^{r-h}.$$

We say that r and h are the rank and height of ρ, respectively.

Corollary 5.5 *This definition of rank coincides with the previous definition over* $\mathbb{F}(T)$.

Proof

Use Theorem 2.2.

□

Proposition 5.6 *Let $r = \mathrm{rank}(\rho)$. Then for each $a \in A \setminus Q$, there is an injection*

$$\mathrm{Gal}(L(M_\rho[a])/L) \to GL_r(A/aA).$$

Proof

This is analogous to the proof in the case of $\mathbb{F}(T)$. Because $a \notin \ker(\delta)$, the constant term of ρ_a is nonzero. Hence for some polynomial $f(x) = c_0x + c_1x^q + \ldots + c_tx^{q^t} \in L[x]$ where $c_0 \neq 0$, we have $\rho_a(u) = f(u)$ for all $u \in M$. Because M is algebraically closed, $M_\rho[a]$ is just the set of roots of f, and $L(M_\rho[a])$ is f's splitting field. Now since $\mathbb{F} \subset L$, the characteristic of L divides q and $f'(x) = c_0 \in L^*$. Thus f is separable and $L(M_\rho[a])/L$ is Galois.

By arguments similar to before, each $\rho \in \mathrm{Gal}(L(M_\rho[a])/L)$ acts on $M_\rho[a] \cong (A/aA)^r$ as an A-module (hence (A/aA)-module) isomorphism. This defines a homomorphism $\mathrm{Gal}(L(M_\rho[a])/L) \to GL_r(A/aA)$ that is injective because $M_\rho[a]$ generates $L(M_\rho[a])$.

□

Corollary 5.7 *If ρ is a rank-1 Drinfeld A-module over L and $a \in A$ is not in the A-characteristic of L, then $L(M_\rho[a])/L$ is an abelian extension.*

Thus we see that adjoining torsion points of a Drinfeld module creates abelian extensions. This is the start of an explicit construction of the maximal abelian extension of a function field. For more details, see [1] and [4].

References

[1] V.G. Drinfeld. Elliptic Modules (Russian), *Math. Sbornik* **94** (1974), 597-627. English translation: *Math. USSR, Sbornik* **23** (1977), 159-170.

[2] D.R. Hayes. A brief introduction to Drinfeld modules, in The Arithmetic of Function Fields (eds. D. Goss et al), Walter de Gruyter & Co., New York-Berlin, 1992.

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

[4] D.R. Hayes. Explicit class field theory in global function fields, Studies in Algebra and Number Theory, *Adv. Math. Supplementary Studies* **6** (1979), 173-217.

[5] M. Rosen. Number Theory in Function Fields. Springer-Verlag, New York, 2002.