Weil pairing and the Drinfeld modular curve

van der Heiden, Gerrit

Chapter 4

Weil Pairing for Drinfeld Modules

4.1 Introduction

A paper based on this chapter is accepted for publication in *Monatshefte für Mathematik*. Let X be a projective, non-singular and absolutely irreducible curve over some finite field $\mathbb{F}_q$ of characteristic p. Put $k = \mathbb{F}_q(X)$ for the function field of X over $\mathbb{F}_q$. Let $\infty \in X$ be some chosen closed point, and let

$$A := \Gamma(X - \infty, \mathcal{O}_X)$$

be the ring of functions on X which are regular outside ∞. Let $K \supset \mathbb{F}_q$ be a field equipped with an A-algebra structure $\gamma : A \longrightarrow K$. We write $\mathbb{G}_{a,K}$ for the additive group over K. Let

$$\varphi : A \longrightarrow \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K})$$

be a Drinfeld module over K. This means that φ is a ring homomorphism such that

(1) there is an $a \in A$ with $\varphi_a \neq \gamma(a)$;

(2) let $\partial : \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K}) \longrightarrow K$ be the ring homomorphism which maps an endomorphism to its constant part, then $\partial \circ \varphi = \gamma$.

The prime ideal $\ker(\gamma)$ is called the *characteristic* of φ. We call an ideal $\mathfrak{a} \subset A$ *away from the characteristic* if $\mathfrak{a} \not\subset \ker(\gamma)$.

Let Ω_A denote the module of differentials of $A/\mathbb{F}_q$. For all ideals $\mathfrak{a} \subset A$

$$\Omega_{\mathfrak{a}} := \mathfrak{a}^{-1}\Omega_A/\Omega_A.$$

Let φ be a Drinfeld module of rank r over K. Let $\overline{K}$ denote the algebraic closure of K. In this chapter we construct for all proper ideals $\mathfrak{a} \subset A$ away from the characteristic an A-module homomorphism

$$w_{\mathfrak{a}} : \prod_{i=1}^{r} \ker(\varphi_{\mathfrak{a}})(\overline{K}) \longrightarrow \ker(\psi_{\mathfrak{a}})(\overline{K}) \otimes \Omega_{\mathfrak{a}}^{\otimes r-1}.$$

Here ψ is a rank 1 Drinfeld module associated to φ in a way we will explain. We will refer to $w_{\mathfrak{a}}$ as the *Weil pairing* (although, strictly speaking, $w_{\mathfrak{a}}$ is only a pairing if $r = 2$). The map $w_{\mathfrak{a}}$ induces an A-isomorphism

$$\wedge^r \ker(\varphi_{\mathfrak{a}})(\overline{K}) \xrightarrow{\sim} \ker(\psi_{\mathfrak{a}})(\overline{K}) \otimes \Omega_{\mathfrak{a}}^{\otimes r-1};$$

cf. Theorem 4.5.3.

The difficult part in constructing $w_{\mathfrak{a}}$ is the construction of the exterior product of a Drinfeld modules. It was Greg Anderson who first understood how to do this in his paper [1]. In this paper he develops *abelian t-modules* and *t-motives*, and he shows how Drinfeld modules can be considered as t-motives.
As Anderson introduced abelian t-modules and t-motives only in case $A = \mathbb{F}_q[t]$, we have to describe the natural generalizations of these notions to the case of general A. Note that the results of the Sections 4.2 and 4.3 can also be found in Potemine's paper [45], but without rigorous proofs. Also, we give a different, but equivalent definition of purity using Newton polygons. It turns out that the category of pure A-motives is closed under the operations of taking subquotients and tensor products. This enables us to construct the tensor product of Drinfeld modules. This construction coincides with the definitions that Hamahata gives in [26] for $A = \mathbb{F}_q[t]$.
The description of the $\mathfrak{a}$-torsion of an abelian A-module in terms of its corresponding A-motive in Section 4.4 enables us to construct $w_{\mathfrak{a}}$ as the mod $\mathfrak{a}$ reduction of Anderson's construction.
The construction of the Weil pairing commutes with taking inverse and direct limits, as is shown in Section 4.6. Finally, in Section 4.7 we give an explicit computation of the Weil pairing in case $A = \mathbb{F}_q[t]$.

Before defining the notions of A-motives and abelian A-modules, we recall the following proposition concerning $\mathrm{Hom}_{\mathbb{F}_q}(\mathbb{G}_{a,K}^n, \mathbb{G}_{a,K}^m)$, the group of all $\mathbb{F}_q$-linear group morphisms $\mathbb{G}_{a,K}^n \longrightarrow \mathbb{G}_{a,K}^m$ over K. Let

$$\mathcal{O}(\mathbb{G}_{a,K}^n) = K[X_1, \ldots, X_n], \quad \mathcal{O}(\mathbb{G}_{a,K}^m) = K[Y_1, \ldots, Y_m].$$

Proposition 4.1.1. *The group* $\mathrm{Hom}_{\mathbb{F}_q}(\mathbb{G}_{a,K}^n, \mathbb{G}_{a,K}^m)$ *consists of all finite sums* $\sum_{i\geq 0} A_i \tau^i$. *Here the morphism* $\tau \in \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K}^n)$ *is given on the underlying rings by*

$$\tau^{\#} : X_i \mapsto X_i^q, \quad i = 1, \ldots, n,$$

and the morphism $A_i \in \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{G}_{a,K}^n, \mathbb{G}_{a,K}^m)$ *is given by the* $m \times n$ *matrix* A_i^* *with coefficients in* K *such that*

$$A_i^{\#} : (Y_1, \ldots, Y_m) \mapsto A_i^*(X_1, \ldots, X_n).$$

Proof. A morphism $\lambda : \mathbb{G}_{a,K}^n \longrightarrow \mathbb{G}_{a,K}^m$ comes from a K-algebra homomorphism

$$\lambda^{\#} : K[Y_1, \ldots, Y_m] \longrightarrow K[X_1, \ldots, X_n]$$

which is compatible with the addition on both linear groups, i.e., the following diagram commutes:

$$\begin{array}{ccc} K[Y_1,\dots,Y_m] & \xrightarrow{\lambda^\#} & K[X_1,\dots,X_n] \\ {\scriptstyle m^\#_{\mathbb{G}^m_{a,K}}}\downarrow & & \downarrow{\scriptstyle m^\#_{\mathbb{G}^n_{a,K}}} \\ K[Y_1,\dots,Y_m]\otimes_K K[Y_1,\dots,Y_m] & \xrightarrow{\lambda^\#\otimes\lambda^\#} & K[X_1,\dots,X_n]\otimes_K K[X_1,\dots,X_n] \end{array}$$

with

$$m^\#_{\mathbb{G}^n_{a,K}} : X_i \mapsto X_i\otimes 1 + 1\otimes X_i, \quad m^\#_{\mathbb{G}^m_{a,K}} : Y_j \mapsto Y_j\otimes 1 + 1\otimes Y_j \quad \forall\ i,j.$$

This diagram commutes if and only if we have for every j

$$\lambda^\#(Y_j) = \sum_{l=0,i=1}^{<\infty,n} a_{i,j,l} X_i^{p^l}.$$

Let τ be the map given by

$$\tau : (X_1,\dots,X_n) \mapsto (X_1^p,\dots,X_n^p),$$

then we may write $\lambda^\# = \sum B_i\tau^i$ for some $m\times n$-matrices B_i with coefficients in K. Because in the proposition we are looking at $\mathbb{F}_q$-linear morphisms, we may replace the p's in the above consideration by q's. This proves the proposition. □

4.2 Abelian A-modules and A-motives

Let $K\{\tau\}$ be the skew polynomial ring whose multiplication is given by the rule $\tau k = k^q\tau$ for all $k\in K$. By Proposition 4.1.1 we see that $\mathrm{End}_{\mathbb{F}_q}(\mathbb{G}^n_{a,K})$ consists of all sums $\sum_i A_i\tau^i$ with $A_i^*\in M_{n\times n}(K)$ and such that $\tau^\#$ acts as the qth-power map on each X_i. In particular, we see that $\mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K})\cong K\{\tau\}$ and that $\mathrm{Hom}_{\mathbb{F}_q}(\mathbb{G}^n_{a,K},\mathbb{G}_{a,K})\cong K\{\tau\}^n$ as $K\{\tau\}$-modules.

Definition 4.2.1. An *Abelian A-module* over K is an $\mathbb{F}_q$-linear ring homomorphism $\varphi : A\longrightarrow \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}^n_{a,K})$ with the following properties. We denote $\varphi(a)=\sum_i A_i(a)\tau^i$.

(1) For all $a\in A$ the element $A_0(a)-\gamma(a)\cdot I$ is nilpotent.

(2) Put
$$M(\varphi) = \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{G}^n_{a,K},\mathbb{G}_{a,K})\cong K\{\tau\}^n;$$
$M(\varphi)$ is a left $K\{\tau\}\otimes_{\mathbb{F}_q} A$-module via
$$(\sum_i \lambda_i\tau^i\otimes a)\cdot f = \sum_i \lambda_i\tau^i\circ f\circ\varphi(a) \quad \text{with } f\in M(\varphi).$$
Then $M(\varphi)$ is a finitely generated, left $K\otimes_{\mathbb{F}_q} A$-module.

Remark 4.2.2. Note that we write τ for both $\tau\in\mathrm{End}_{\mathbb{F}_q}(\mathbb{G}^n_{a,K})$ and $\tau\in\mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K})$.

Definition 4.2.3. Let

$$\varphi : A \longrightarrow \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K}^n) \text{ and } \psi : A \longrightarrow \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K}^m)$$

be two abelian A-modules. A *morphism of abelian A-modules* from φ to ψ is a map $\lambda \in \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{G}_{a,K}^n, \mathbb{G}_{a,K}^m)$ such that $\lambda\varphi(a) = \psi(a)\lambda$ for all $a \in A$.

Definitions 4.2.1 and 4.2.3 together form the *category of Abelian A-modules over K*.

Let M be a left $K\{\tau\} \otimes_{\mathbb{F}_q} A$-module, then $\overline{M} = M \otimes \overline{K}$ is a left $\overline{K}\{\tau\} \otimes_{\mathbb{F}_q} A$-module.

Definition 4.2.4. An *A-motive M* is a left $K\{\tau\} \otimes_{\mathbb{F}_q} A$-module with the following properties:

(1) M is a finitely generated, projective $K \otimes_{\mathbb{F}_q} A$-module.

(2) M is a finitely generated $K\{\tau\}$-module.

(3) For all $a \in A$ there is an $n \in \mathbb{N}$ such that

$$(1 \otimes a - \gamma(a) \otimes 1)^n \overline{M} \subset \tau \overline{M}.$$

Definition 4.2.5. Let M and M' be two A-motives. A *morphism of A-motives* from M to M' is a $K\{\tau\} \otimes A$-linear map $\mu : M \longrightarrow M'$.

Definitions 4.2.4 and 4.2.5 together form the *category of A-motives*.

Remark 4.2.6. Note that

$$X_K = X \times_{\mathrm{Spec}(\mathbb{F}_q)} \mathrm{Spec}(K)$$

is a projective, absolutely irreducible, smooth curve over K. Because $\mathbb{F}_{q^{\deg(\infty)}}$ is a finite, separable extension of $\mathbb{F}_q$, it follows that

$$K \otimes_{\mathbb{F}_q} \mathbb{F}_{q^{\deg(\infty)}} \cong \oplus_{i=1}^{l} L_i$$

where the L_i are fields. The fields L_i are in 1-1 correspondence with the points $\infty_i \in X_K$ lying above ∞. Hence, $\infty \times \mathrm{Spec}(K) = \{\infty_1, \ldots, \infty_l\}$ as a set. The ring $K \otimes_{\mathbb{F}_q} A$ is the ring of functions on X_K which are regular outside $\infty \times X$. This is a Dedekind ring because X_K is a smooth curve over K. For the function fields we have

$$\mathbb{F}_q(X) \cong \mathrm{Quot}(A) \quad \text{and} \quad K(X_K) \cong \mathrm{Quot}(K \otimes_{\mathbb{F}_q} A).$$

Lemma 4.2.7. *Let M be a left $K\{\tau\} \otimes A$-module which is finitely generated over both $K\{\tau\}$ and $K \otimes A$. Then M is a projective $K \otimes A$-module if and only if M is free over $K\{\tau\}$.*

Proof. Let M_0 be the subgroup of M consisting of all $K \otimes A$-torsion points of M. Because $K \otimes A$ is Dedekind, we have the following equivalences: M is projective over $K \otimes A \iff$ M has no $K \otimes A$-torsion $\iff M_0 = 0$. Note that $\dim_K M_0 < \infty$ because $K \otimes A$ is Dedekind.
As $K\{\tau\}$ is a left Euclidean ring, M is isomorphic to

$$K\{\tau\}^m \oplus K\{\tau\}/K\{\tau\}f_1 \oplus \ldots \oplus K\{\tau\}/K\{\tau\}f_n$$

for some $m, n \in \mathbb{N}$ and $f_i \in K\{\tau\}$ with $\deg_\tau(f_i) > 0$. Consequently, M is free over $K\{\tau\}$ $\iff$ the $K\{\tau\}$-torsion subgroup M_1 of M is 0. Moreover, from this description it follows that $\dim_K M_1 < \infty$.
To prove the lemma, we show that $M_0 = M_1$. If $m \in M_0$, then there is an element $g = \sum_i k_i \otimes a_i \in K \otimes A$ with $g(m) = 0$. It is not difficult to see that $\tilde{g} = \sum_i k_i^q \otimes a_i$ annihilates τm. Therefore, $K\{\tau\}m \subset M_0$. As $\dim_K(M_0)$ is finite, there must be an element $f \in K\{\tau\}$ with $f \cdot m = 0$. Therefore, $M_0 \subset M_1$.
On the other hand, if $m \in M_1$, then there is an $f \in K\{\tau\}$ such that $f \cdot m = 0$. As the actions of $K\{\tau\}$ and A commute, we have for every $a \in A$ that $f \cdot (1 \otimes a) \cdot m = 0$. Consequently, $K \otimes A \cdot m \subset M_1$. Because $\dim_K(M_1) < \infty$, we see that $m \in M_0$ and thus $M_1 \subset M_0$. □

Remark 4.2.8. As G. Böckle pointed out to me, one can also reduce this to Anderson's proof of Lemma 1.4.5 by considering a morphism $\mathbb{F}_q[t] \hookrightarrow A$ and noting that M is finitely generated and free over $\mathbb{F}_q[t]$ if and only if it is finitely generated and projective over A.

Let φ, ψ be two abelian A-modules of dimension n and m, respectively. Then a morphism $\lambda : \varphi \longrightarrow \psi$ is an element of $\mathrm{Hom}_{\mathbb{F}_q}(\mathbb{G}^n_{a,K}, \mathbb{G}^m_{a,K})$ such that $\lambda\varphi(a) = \psi(a)\lambda$ for all a. This gives rise to a map $f_\lambda : M(\psi) \longrightarrow M(\varphi)$ given by $m \mapsto \lambda(m) = m \circ \lambda$.

Theorem 4.2.9. *We define the functor*

$$\mathcal{F} : \{\textit{abelian } A\textit{-modules}\} \longrightarrow \{A\textit{-motives}\} \text{ givenby } \varphi \mapsto M(\varphi), \lambda \mapsto f_\lambda$$

where φ is an abelian A-module, $M(\varphi)$ is as in Definition 4.2.1, λ is a morphism between abelian A-modules, and f_λ is as described above. The functor $\mathcal{F}$ gives an anti-equivalence of the respective categories.

Proof. First we show that $M(\varphi)$ is in fact an A-motive. By property (1) of abelian A-modules, there is an $l \in \mathbb{N}$ such that $(\varphi(a) - \gamma(a))^l = \kappa\tau$. Here τ is the q-Frobenius in $\mathrm{End}_{\mathbb{F}_q}(\mathbb{G}^n_{a,K})$. For all $m \in \overline{M}(\varphi)$ we may write by Proposition 4.1.1

$$m = C_0 + (\sum_{i>0} C_i \tau^{i-1})\tau$$

for $C_i \in M_{1\times n}(\overline{K})$. Hence

$$(1 \otimes a - \gamma(a) \otimes 1)^l m = C_0(\varphi(a) - \gamma(a))^l - \mu\tau = (C_0\kappa - \mu)\tau$$

with

$$C_0\kappa - \mu \in \overline{M}(\varphi) = \overline{K} \otimes_K \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{G}^n_{a,K}, \mathbb{G}_{a,K}).$$

Note that $\tau(c_1,\dots,c_n) = (c_1^q,\dots,c_n^q)\tau$; hence, by the perfectness of $\overline{K}$ it follows that

$$(1\otimes a - \gamma(a)\otimes 1)^l m = (C_0\kappa - \mu)\tau = \tau\tilde{\mu}$$

where $\tilde{\mu}$ is some element in $\overline{M}(\varphi)$. This shows that property (3) of A-motives holds for $M(\varphi)$.
By property (2) of abelian A-modules, $M(\varphi)$ is a finitely generated $K\otimes A$-module. We already noted that $M(\varphi)$ is a free $K\{\tau\}$-module of rank n (cf. Definition 4.2.1); hence, by Lemma 4.2.7 $M(\varphi)$ is a projective $K\otimes A$-module. Thus, property (1) and property (2) of an A-motive hold for $M(\varphi)$. This proves that $\mathcal{F}$ maps abelian A-modules to A-motives.
To show that $\mathcal{F}$ is a contravariant functor, we describe its action on morphisms. Let

$$\varphi : A \longrightarrow \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K}^n) \text{ and } \psi : A \longrightarrow \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K}^m)$$

be two abelian A-modules. Suppose

$$\sum_i k_i\tau^i \otimes a \in K\{\tau\}\otimes A,$$

then

$$(\sum_i k_i\tau^i\otimes a)\cdot\lambda(m) = (\sum_i k_i\tau^i)\circ m\circ(\lambda\varphi(a))$$

$$= (\sum_i k_i\tau^i)\circ m\circ(\psi(a)\lambda) = \lambda((\sum_i k_i\tau^i\otimes a)m).$$

Hence λ is indeed $K\{\tau\}\otimes A$-linear.
This construction shows that the induced map

$$\mathcal{F} : \mathrm{Hom}(\varphi,\psi) \longrightarrow \mathrm{Hom}(M(\psi),M(\varphi))$$

commutes with composition. To see that this map on the Hom's is injective, we look at the action of $\lambda\in\mathrm{Hom}_{\mathbb{F}_q}(\mathbb{G}_{a,K}^n,\mathbb{G}_{a,K}^m)$ on the underlying rings:

$$\begin{array}{ccc} K[Y_1,\dots,Y_m] & \xrightarrow{\lambda} & K[X_1,\dots,X_n] \\ \downarrow{\scriptstyle m_\psi} & & \downarrow{\scriptstyle m_\psi\circ\lambda} \\ K[X] & \xrightarrow{=} & K[X] \end{array}$$

$\mathcal{F}(\lambda) = 0$ means that $m_\psi\circ\lambda = 0$ for all $m_\psi\in M(\psi)$. By Proposition 4.1.1 we may consider $\lambda = (a_{i,j})\in M_{m\times n}(K\{\tau\})$ via

$$\lambda : Y_i \mapsto \sum_{j=1}^m a_{i,j}(X_j).$$

In particular, if we take $m_\psi : Y_i\mapsto 0$, then the i'th row of $(a_{i,j})$ is zero. This implies that $\mathcal{F}$ is injective. To show that $\mathcal{F}$ on the Hom's is surjective, let $\lambda\in\mathrm{Hom}(M(\psi),M(\varphi))$. We may consider $M(\psi)$ and $M(\varphi)$ as $K\{\tau\}$-modules with bases $e_i : X\mapsto Y_i$ and $f_j : X\mapsto X_j$

on the underlying rings. Then $\lambda(e_i) = \sum_{j=1}^{n} b_{i,j} f_j$ for some $b_{i,j} \in K\{\tau\}$ and as before $(b_{i,j}) \in \mathrm{Mat}_{m\times n}(K\{\tau\})$ determines a map μ in $\mathrm{Hom}_{\mathbb{F}_q}(\mathbb{G}_{a,K}^n, \mathbb{G}_{a,K}^m)$ given by

$$\mu^* : (Y_1, \ldots, Y_m) \mapsto (b_{i,j})(X_1, \ldots, X_n).$$

Clearly, considered as map from $M(\psi)$ to $M(\varphi)$, we have $\mu(m) = \lambda(m)$ for all $m \in M(\psi)$. Because λ is A-linear, we have

$$\mu \circ \varphi_a = \lambda(1) \circ \varphi_a = \lambda(a \cdot 1) = \lambda(\psi_a) = \psi_a \circ \mu.$$

Hence, μ is a morphism from φ to ψ and $\mathcal{F}(\mu) = \lambda$. This proves the surjectivity.
As $\mathcal{F}$ on the Hom's is both injective and surjective, $\mathcal{F}$ is fully faithful.
To prove anti-equivalence, it remains to show that $\mathcal{F}$ is essentially surjective, i.e., that every A-motive is isomorphic to $M(\varphi)$ for some abelian A-module φ.
Let M be an n-dimensional A-motive, then M is free of rank n over $K\{\tau\}$ by Lemma 4.2.7. We choose a basis $\{e_1, \ldots, e_n\}$ of M over $K\{\tau\}$. For any $a \in A$ we write the action of a on M as follows:

$$a \cdot e_i = \sum_{j=1}^{n} (\sum_{k\geq 0} c_{i,j,k}(a)\tau^k) e_j \quad \text{with } c_{i,j,k}(a) \in K.$$

We define

$$\varphi : A \longrightarrow \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K}^n) \quad \text{by } \varphi(a) := \sum_{k\geq 0} C_k(a)\tau^k$$

where $C_k(a)$ is the matrix $(c_{i,j,k}(a))_{i,j} \in \mathrm{Mat}_{n\times n}(K)$. Because M has an A-module structure, φ is a ring homomorphism. Clearly, φ is $\mathbb{F}_q$-linear. By reversing the argument we gave above, we see that property (3) of an A-motive implies that φ has property (1) of an abelian A-module. Finally, to check that φ is an abelian A-module we need to check that $M(\varphi) = \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{G}_{a,K}^n, \mathbb{G}_{a,K})$ is a finitely generated $K \otimes A$-module. Let $\{f_1, \ldots, f_n\}$ be the basis of $M(\varphi)$ such that

$$f_i \circ \varphi(a) = \sum_{j=1}^{n} \sum_{k\geq 0} c_{i,j,k}(a)\tau^k.$$

(This means that $\{f_i\}$ is just the standard basis of $M(\varphi)$ up to the choice of τ.) Then the $K\{\tau\}$-linear map $\lambda : M \longrightarrow M(\varphi)$ given by $e_i \mapsto f_i$ is also A-linear, as one easily checks. Moreover, λ is an isomorphism between M and $M(\varphi)$. As M is finitely generated as $K \otimes A$-module, we may conclude that φ is an abelian A-module. Therefore, $\mathcal{F}$ is essentially surjective. □

Definition 4.2.10. We define the following notions:

(1) The *rank* of an A-motive M is the projective rank of M as $K \otimes A$-module. We denote the rank by $r(M)$.

(2) The *dimension* of an A-motive M is the rank of M as $K\{\tau\}$-module. We denote the dimension by $\rho(M)$.

(3) The *rank* (resp. *dimension*) of an abelian A-module φ, denoted by $r(\varphi)$ (resp. $\rho(\varphi)$) is the rank (resp. dimension) of its corresponding A-motive $M(\varphi)$.

Proposition 4.2.11. *The category of abelian A-modules of rank r and dimension 1 is anti-equivalent to the category of Drinfeld modules of rank r.*

Proof. It is clear that the category of abelian A-modules of dimension 1 is equivalent to the category of Drinfeld modules: both categories share property (1); property (2) follows from the fact that $\varphi_a \in K\{\tau\}$ for both φ an abelian A-module of dimension 1 and φ a Drinfeld module. So we only have to prove that the ranks are identical. This can be seen by noting that for a Drinfeld module φ the kernel $\ker(\varphi_a)(\overline{K})$ is a free A/a-module of rank r if a is away from the characteristic. The same thing is true for abelian A-modules, as we will show in Corollary 4.4.5. □

4.3 Pure A-motives

In the category of Drinfeld modules it is not at all obvious how to define tensor products and how to take subquotients. Also, the category of A-motives is not yet quite what we need. Instead, we look at a category $\mathcal{C}$ of which the category of A-motives is a subcategory.

Definition 4.3.1. The category $\mathcal{C}$ is defined as follows. The *objects* of $\mathcal{C}$ are $K\{\tau\} \otimes A$-modules such that the underlying $K \otimes A$-module is finitely generated and projective. The *morphisms* of $\mathcal{C}$ are homomorphisms of $K\{\tau\} \otimes A$-modules.

Remark 4.3.2. Note that the definition of $\mathcal{C}$ requires the specification of the field K. We write $\mathcal{C}_K$ if we want to stress the field K.

The category $\mathcal{C}$ is closed under taking subquotients and tensor products. Let us explain what we mean by this.

(1) *Subquotients.* Let

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

be an exact sequence of $K\{\tau\} \otimes A$-modules, and assume that M_3 has no $K \otimes A$-torsion. If M_2 is an object of $\mathcal{C}$, then M_1 and M_3 are also objects of $\mathcal{C}$. Namely, M_1 and M_3 are finitely generated, torsion free $K \otimes A$-modules. Therefore, they are projective $K \otimes A$-modules. The module M_3 is called a *subquotient* of M_2.

(2) *Tensor products.* Suppose that M_1 and M_2 are objects of $\mathcal{C}$. The *tensor product* $M_1 \otimes M_2$ of M_1 and M_2 is defined as follows:

$$M_1 \otimes M_2 := M_1 \otimes_{K \otimes A} M_2$$

which is equipped with the following τ-action:

$$\tau : m_1 \otimes m_2 \mapsto \tau m_1 \otimes \tau m_2.$$

Consequently, $M_1 \otimes M_2$ is a $K\{\tau\} \otimes A$-module which is finitely generated and projective as $K \otimes A$-module. Therefore, $M_1 \otimes M_2$ is an object of $\mathcal{C}$.

Furthermore, following Anderson, we introduce the notion of *purity* and we will show that the category of pure A-motives is a subcategory of $\mathcal{C}$ which is also closed under taking tensor products and subquotients. Moreover, we will show that the category of Drinfeld modules is a subcategory of the category of pure A-motives.
In a diagram the relation between the categories reads as follows:

$$\text{DRIN. MOD.} \overset{\mathcal{F}}{\hookrightarrow} \text{PURE } A\text{-MOT.} \hookrightarrow A\text{-MOT.} \hookrightarrow \mathcal{C}.$$

Using (1) and (2), we can associate to an object $M \in \mathcal{C}$ the exterior product $\wedge^r M$. This exterior product is a subquotient of $M^{\otimes r}$ and therefore an object of $\mathcal{C}$. Consequently, if M is a pure A-motive of rank r and dimension ρ, then $\wedge^r M$ is a pure A-motive of rank 1, and it turns out that $\wedge^r M$ has dimension ρ. We will establish the fact that any A-motive associated to any Drinfeld module is pure. This will enable us to construct the Weil pairing. Note that this section gives the theoretical background of some definitions in [26]. The main goal of this section is to prove the following theorem:

Theorem 4.3.3. *Let $\varphi : A \longrightarrow \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K})$ be a Drinfeld module of rank r over K, and let $M(\varphi)$ be its associated A-motive, then there exists a Drinfeld module ψ of rank 1 such that $M(\psi) \cong \wedge^r M(\varphi)$. The Drinfeld module ψ is unique up to isomorphy.*

We will give two equivalent definitions of purity. The first one uses Newton polygons and stresses the similarity with the classical notion of purity. The second definition uses lattices and is the natural extension of Anderson's definition in [1].

4.3.1 Newton polygons

Assume that K is algebraically closed, and let

$$F := \text{the quotient field of } K \otimes A.$$

So F is the function field of the curve X_K. Let $\sigma : K \longrightarrow K$ be an $\mathbb{F}_q$-linear automorphism of K. Extend σ to an automorphism of $K \otimes A$ by letting it act trivially on A. Then σ extends naturally to an automorphism

$$\sigma : F \longrightarrow F.$$

Let $F\{\sigma\}$ be the corresponding skew polynomial ring. This means that its elements are finite sums $\sum_i f_i \sigma^i$ with $f_i \in F$. Multiplication in this ring is given by the rule $\sigma f = \sigma(f)\sigma$ for all $f \in F$; cf. [8, 0.8]. Similarly, $K\{\sigma\}$ is a skew polynomial ring.

Lemma 4.3.4. *The skew polynomial rings $F\{\sigma\}$ and $K\{\sigma\}$ are Euclidean domains.*

Proof. According to Theorem 1.2 in [8, p. 67], these skew polynomial rings are left-Euclidean. As σ is an automorphism of both F and K, the same argument shows that both skew polynomial rings are right-Euclidean. □

Let ν be a place of F corresponding to a closed point $x \in X_K$. We assume that σ respects the valuation at ν. This means that σ fixes x and that $v_\nu(\sigma(f)) = v_\nu(f)$ for all $f \in F$. The completion F_ν of F at ν is isomorphic to $K(\!(z)\!)$, and we have $\sigma(z) = z$.

Let $g = a_0 + a_1\sigma + \cdots + a_n\sigma^n \in F_\nu\{\sigma\}$ with $a_i \in F_\nu$.

Definition 4.3.5. The *Newton polygon* $N(g)$ *of* g *at* ν of F_ν is defined to be the convex hull of the set

$$\{(j, y_j) \in \mathbb{R} \times \mathbb{R} \mid j \in \{0, \dots, n\} \text{ and } y_j \geq v_\nu(a_j)\}.$$

The lower boundary of $N(g)$ has finitely many slopes. If we talk about the *slope of* $N(g)$, we mean the slope of the lower boundary of $N(g)$.
For any two skew polynomials $g_1, g_2 \in F_\nu\{\sigma\}$ we define the sum of $N(g_1)$ and $N(g_2)$ to be

$$N(g_1) + N(g_2) := \{(x_1, y_1) + (x_2, y_2) \mid (x_i, y_i) \in N(g_i) \text{ for } i = 1, 2\}.$$

Proposition 4.3.6. *Newton polygons have the following properties.*

i. Let $g_1, g_2 \in F_\nu\{\sigma\}$*, then*

$$N(g_1 g_2) = N(g_1) + N(g_2).$$

Moreover, the set of slopes of $N(g_1 g_2)$ *equals the union of the set of slopes of* $N(g_1)$ *and* $N(g_2)$*.*

ii. Let $g \in F_\nu\{\sigma\}$ *be monic. If* $N(g)$ *consists of two polygons* P_1 *and* P_2 *which have no slope in common, then* g *factors uniquely in* $F_\nu\{\sigma\}$ *as* $g = g_1 g_2$*. The skew polynomials* $g_i \in F_\nu\{\sigma\}$ *are monic, and* $N(g_i) = P_i$*.*

iii. Let $g_1, g_2 \in F_\nu\{\sigma\}$*, and let* $g = g_1 g_2$*. If* $N(g_1)$ *has no slope in common with* $N(g_2)$*, then the following* $F_\nu\{\sigma\}$*-modules are isomorphic:*

$$F_\nu\{\sigma\}/F_\nu\{\sigma\}g \cong F_\nu\{\sigma\}/F_\nu\{\sigma\}g_1 \oplus F_\nu\{\sigma\}/F_\nu\{\sigma\}g_2.$$

Proof. We can follow the proof of similar propositions in the case of differential modules and of polynomials over $\mathbb{C}(\!(z)\!)$; cf. [46] and [55].

i. Write $g_1 = \sum a_i \sigma^i$ and $g_2 = \sum b_j \sigma^j$, then $g_1 g_2 = \sum_k c_k \sigma^k$ with $c_k = \sum_{i+j=k} a_i \sigma^i(b_j)$. As σ respects the ν-valuation of elements in F, it is a straightforward matter to see that $N(g_1 g_2) \subset N(g_1) + N(g_2)$.
An *endpoint* of $N(g)$ is a point e on the lower boundary of $N(g)$ such that either $e = (0, *)$ or e connects two line segments of the lower boundary with distinct slopes. We denote the slope of the line segment which ends at e by s_e. For the endpoint $e = (0, *)$ we define $s_e = -\infty$.
Let u be an endpoint of $N(g_1)$. Consider the set V of all endpoints $\tilde{v}$ of $N(g_2)$ such that $s_{\tilde{v}} \leq s_u$. If V is not empty, then it makes sense to consider the endpoint $v \in V$ with $s_v \geq s_{\tilde{v}}$ for all $\tilde{v} \in V$ in this set. It is not difficult to see that $u + v$ is an endpoint of $N(g_1) + N(g_2)$.
Similarly, we can construct endpoints $u + v$ of $N(g_1) + N(g_2)$ by interchanging the roles of g_1 and g_2 in the above construction, i.e., u is the endpoint of $N(g_1)$ such that $s_u \leq s_v$ and s_u is maximal among all elements $s_{\tilde{u}}$ with $\tilde{u}$ an endpoint of $N(g_1)$ and $s_{\tilde{u}} \leq s_v$.
It is not difficult to see that all endpoints of $N(g_1) + N(g_2)$ arise in this way. Let $u + v$ be any endpoint of $N(g_1) + N(g_2)$. Write $u = (i_0, a_{i_0})$ and $v = (j_0, b_{j_0})$. Let $k = i_0 + j_0$. Using the properties of u and v described above, it is easy to show that for any pair

$(i,j) \neq (i_0,j_0)$ with $i+j=k$ one has $v_\nu(a_ib_j) > v_\nu(a_{i_0}b_{j_0})$. Hence, the ν-valuation $v_\nu(c_k) = v_\nu(a_{i_0}b_{j_0})$. Consequently, $N(g_1)+N(g_2) \subset N(g_1g_2)$.

ii. First we show the following *Claim* for a Newton polygon $N(g)$ which consists of at least two slopes. Let s be the smallest slope of $N(g)$, and let n be the length of the line segment with slope s. Then there exist monic skew polynomials $f_1, f_2 \in F_\nu\{\sigma\}$ with $g = f_1f_2$ and $\deg_\sigma(f_1) = n$. Moreover, $N(f_1)$ has only one slope, and this slope is equal to s. The slopes of the Newton polygon $N(f_2)$ are all $> s$.

a. We first prove the *Claim* for $s = 0$. Write $g = \sum_{i=k}^{\infty} z^i a_i$ with $a_i \in K\{\sigma\}$ and $a_k \neq 0$, then $\deg_\sigma(a_k) = n$. We construct a decomposition $g = f_1f_2$ as follows. Write

$$f_1 = \sum_{i\geq 0} z^i b_i \quad \text{and} \quad f_2 = z^k(\sum_{i\geq 0} z^i c_i)$$

with $b_i, c_i \in K\{\sigma\}$. Put $b_0 := a_k$ and $c_0 := 1$. The elements b_i and c_j are inductively determined as follows. Suppose that b_i, c_j are already determined for $0 \leq i,j < l$. To get $g = f_1f_2$, we see that we need the following equality for the coefficients of z^{l+k} that

$$b_0c_l + b_1c_{l-1} + \ldots + b_{l-1}c_1 + b_l = a_{l-k}.$$

As $K\{\sigma\}$ is Euclidean, it makes sense to take c_l equal to the quotient of the left-division of b_0 and $b_1c_{l-1} + \ldots + b_{l-1}c_1 - a_{k,l}$. Take b_l equal to the remainder of this division. This implies that $\deg_\sigma b_l < n$ for all $l \geq 1$. Therefore, the Newton polygon $N(f_1)$ has only one slope and this slope is equal to 0. Moreover, $N(f_2)$ has only slopes larger than 0.
After multiplying f_1 and f_2 with some constants in $K(\!(z)\!)^*$, we may assume that f_1 and f_2 are monic. This proves the *Claim* for $s = 0$.

b. Suppose now that the smallest slope is $s = \frac{s_1}{s_2}$ with $s_1 \in \mathbb{Z}$, $s_2 \in \mathbb{N}$ and $\gcd(s_1,s_2) = 1$. Write $g = \sum_{i\geq k,j} g_{i,j}z^i\sigma^j$ with $g_{i,j} \in K$. Consider the extension $K(\!(\xi)\!)/K(\!(z)\!)$ given by $\xi^{s_2} = z$. We extend the action of σ to $K(\!(\xi)\!)$ by putting $\sigma(\xi) = \xi$. Let

$$g'(\tilde{\sigma}) := g(\xi^{-s_1}\tilde{\sigma}),$$

then the smallest slope of $g' \in K(\!(\xi)\!)\{\tilde{\sigma}\}$ is 0 and

$$g' = \sum_{i\geq s_2k,j} g_{i,j}\xi^{-s_1j+s_2i}\tilde{\sigma}^j.$$

Applying *a*. to g' gives rise to a factorization $g = f_1f_2$ inside $K(\!(\xi)\!)\{\sigma\}$. From some bookkeeping it follows that f_1 and f_2 are indeed elements of $K(\!(z)\!)\{\sigma\}$. Let us work this out in detail. Denote by $\alpha'_m(\tilde{\sigma}) \in K\{\tilde{\sigma}\}$ the coefficient of ξ^m in g', i.e.,

$$\alpha'_m = \sum_{i,j:-s_1j+s_2i=m} g_{i,j}\tilde{\sigma}^j.$$

Let $\alpha_m(\sigma) := \alpha'_m(\xi^{s_1}\sigma)\xi^m$, then $\alpha_m(\sigma) \in K(\!(z)\!)\{\sigma\}$. We construct a factorization of g' as under *a*., i.e., $g' = f'_1 \cdot f'_2$ with $f'_1 = \sum_{i\geq 0} b'_i\xi^i$ and $f'_2 = \xi^{s_2k}\sum_{i\geq 0} c'_i\xi^i$ with $b'_i, c'_i \in K(\!(\xi)\!)\{\tilde{\sigma}\}$. Define $b'_0 := \alpha'_k$, which is the 'slope 0-part' of g', and define $c'_0 = 1$. Let $d'_l = \sum_{i=1}^{l-1} b'_i \cdot c'_{l-i}$, then the elements b'_l and c'_l in $K\{\tilde{\sigma}\}$ must satisfy the relation

$$b'_0 \cdot c'_l + b'_l = \alpha'_{l+k} - d'_l. \tag{4.1}$$

Let c_l' be the quotient of dividing the left-hand side by b_0' and let b_l' be the remainder of this division.
We translate this to a factorization of g. Define $b_l(\sigma) = b_l'(\xi^{s_1}\tilde{\sigma})\xi^l$. Similarly, we define c_l and d_l. Then $f_1 = \sum b_i$ and $f_2 = z^k \sum c_i$ gives a factorization of g. It remains to be shown that $b_i, c_i \in K(\!(z)\!)\{\sigma\}$.
First note that $b_0 \in K(\!(z)\!)\{\sigma\}$: it consists of all $g_{i,j}z^i\sigma^j$ with $j \leq n$ and such that (i,j) lies on the lower boundary of the Newton polygon $N(g)$. We proceed by induction: suppose that $b_i, c_i \in K(\!(z)\!)\{\sigma\}$ for $0 \leq i < l$, then (4.1) reads as

$$b_0 c_l + b_l = \alpha_{l+k} z^{-k} - d_l.$$

As b_0, d_l and α_{l+k} are all in $K(\!(z)\!)\{\sigma\}$, it follows that also the quotient c_l and the remainder b_l are elements of $K(\!(z)\!)\{\sigma\}$. This proves the *Claim*.
Instead of factoring $g = f_1 f_2$ where f_1 is the skew polynomial corresponding to the smallest slope, we can also uniquely factor $g = \tilde{f}_2\tilde{f}_1$ where $\tilde{f}_1$ corresponds to the smallest slope.
We can conclude the proof of *ii* as follows. If the minimal slope s of g is a slope of $N(P_1)$, then we factor $g = f_1 f_2$. If the minimal slope is a slope of $N(P_2)$, then we factor $g = \tilde{f}_2\tilde{f}_1$. Now we can do the same for the remaining term - either f_2 or $\tilde{f}_2$. Repeating in this way, gives us a unique factorization $g = g_1 g_2$ with the desired properties.
iii. We have $N(g) = N(g_1) + N(g_2) = N(g_2) + N(g_1)$. As $N(g_1)$ and $N(g_2)$ have no slope in common, there exist elements $\tilde{g}_i \in F_\nu\{\sigma\}$ with $N(\tilde{g}_i) = N(g_i)$ and

$$g_1 g_2 = g = \tilde{g}_2\tilde{g}_1. \tag{4.2}$$

As $N(g_1)$ and $N(\tilde{g}_2)$ have no slope in common, this relation is left-coprime. Similarly, this relation is right-coprime. This means that g is *decomposable*; cf. [8, p. 139]. According to the proof of Proposition 6.1 in [8, p. 140], we have the following isomorphism:

$$F_\nu\{\sigma\}/F_\nu\{\sigma\}g \cong F_\nu\{\sigma\}/F_\nu\{\sigma\}g_1 \oplus F_\nu\{\sigma\}/F_\nu\{\sigma\}\tilde{g}_2.$$

By (4.2) the elements g_2 and $\tilde{g}_2$ are similar and consequently,

$$F_\nu\{\sigma\}/F_\nu\{\sigma\}\tilde{g}_2 \cong F_\nu\{\sigma\}/F_\nu\{\sigma\}g_2,$$

cf. [8, p. 123] and Proposition 3.4 in [8, p. 126]. □

Let V be a cyclic $F\{\sigma\}$-module with $\dim_F V < \infty$, and let $x \in V$ be a cyclic element. Then there exists a unique monic polynomial $g \in F\{\sigma\}$ with $\deg_\sigma g = \dim_F V$ and $g \cdot x = 0$. We define

$$\text{The Newton polygon } N(V) \text{ of } V \text{ at } \nu \text{ is } N(V) := N(g).$$

Proposition 4.3.7. *Let V be a cyclic $F\{\sigma\}$-module such that $\dim_F V < \infty$, then the Newton polygon $N(V)$ of V does not depend on the chosen cyclic element $x \in V$.*

Proof. Note that the Newton polygon of $V \otimes_F F_\nu$ is the same as the Newton polygon of V, hence we may assume that V is an $F_\nu\{\sigma\}$-module. We write $W(g)$ for the module $F_\nu\{\sigma\}/F_\nu\{\sigma\}g$. For an element $e \in V$ we write g_e for the unique monic skew polynomial

of minimal degree with $g(e) = 0$.
Suppose that $x, y \in V$ are two cyclic elements of V. Then $W(g_x) \cong W(g_y)$. The proposition follows if we can prove that $N(g_x) = N(g_y)$.
1. Suppose that both $N(g_x)$ and $N(g_y)$ have only one slope. Then $N(g_x)$ and $N(g_y)$ have the same slope, as can be seen as follows. Let $n = \deg(g_x) = \deg(g_y)$. Let B_x be the matrix of the action of σ on the basis $\{x, \sigma x, \ldots, \sigma^{n-1}x\}$, and let B_y be the matrix of the action of σ on the basis $\{y, \sigma y, \ldots, \sigma^{n-1}y\}$. An easy computation shows that $v_\nu(\det(B_y)) = v_\nu(\det(B_x))$. As $\det(B_y)$ and $\det(B_x)$ are the constant terms of g_y and g_x respectively, the slopes of $N(g_x)$ and $N(g_y)$ are equal.
2. Note that $N(g_y)$ necessarily has only one slope if $N(g_x)$ has only one slope. Namely, if $N(g_y)$ has k distinct slopes s_i, then we may write $W(g_y) \cong \oplus W_i$ with each W_i has slope s_i. Via the isomorphism $W(g_x) \cong W(g_y)$ we see that the module W_i is isomorphic to a direct summand of $W(g_x)$. Consequently, by 1. W_i has the same slope as $N(g_x)$.
3. Suppose that $W(g_x)$ has k distinct slopes $s_1, \ldots, s_k$. Then there exists a decomposition $W(g_x) \cong \oplus W_i$ with each W_i has slope s_i. Under the isomorphism $W(g_x) \cong W(g_y)$ this gives rise to a decomposition $\oplus W_i'$ of $W(g_y)$ with W_i' has slope s_i. □

Finally, we define the Newton polygon for any torsion $F\{\sigma\}$-module V with $\dim_F V < \infty$. By Theorem 2.3 in [8, p. 292] there is a minimal decomposition of V into cyclic modules V_i. This decomposition is unique up to isomorphy. We define

$$N(V) := \sum_i N(V_i).$$

By the uniqueness up to isomorphism of the decomposition, it follows with the previous proposition that the Newton polygon $N(V)$ is well-defined.

The following lemma is useful in the sequel.

Lemma 4.3.8. *Let V be a torsion $F\{\sigma\}$-module with $\dim_F V < \infty$.*

i. If V has no σ-torsion, then V is cyclic.

ii. If all slopes of the Newton polygon $N(V)$ of V are $\neq 0$, then V has no σ-torsion.

Proof. i. An element $g \in F\{\sigma\}$ is called *invariant* if $gF\{\sigma\} = F\{\sigma\}g$. As σ is an automorphism of F of infinite order, it is not difficult to see that the only invariant elements in $F\{\sigma\}$ are of the form $f\sigma^n$ with $f \in F$.
Using this, *i.* follows immediately from Theorem 2.1 in [8, p. 292]. This theorem implies that V can be written as $V = \oplus_{i=1}^n F\{\sigma\}/F\{\sigma\}g_i$ where g_i is a *total divisor* of g_{i+1} for $i = 1, \ldots, n-1$. This latter means that there is an invariant element $h \in F\{\sigma\}$ with $g_i \mid h \mid g_{i+1}$.
V has no σ-torsion if and only if $\sigma \not| \ g_i$ for all i. By the previous it follows that $V = F\{\sigma\}/F\{\sigma\}g_1$. This also proves *ii.* □

Definition 4.3.9. Let V be a torsion $F\{\sigma\}$-module with $\dim_F V < \infty$, then V is called *pure at ν* if the Newton polygon of V at ν has only one slope. If V is pure, this slope is called the *weight $w_\nu(V)$ of V at ν*.

4.3.2 Purity with Newton polygons

The previous discussion of Newton polygons will be applied to objects $M \in \mathcal{C}$. Let r denote the projective $K \otimes A$-rank of M. Let

$$M_F = M \otimes_{K \otimes A} F.$$

This is an r-dimensional F-vector space.
As K is algebraically closed, there lie $d_\infty = \deg(\infty)$ points $\infty_1, \ldots, \infty_{d_\infty} \in X_K$ above the point $\infty \in X$. The action of τ on $K \otimes A$ is an automorphism which acts trivially on A. This action of τ naturally extends to an action of τ on F. For ν we take the places corresponding to ∞_i.

Lemma 4.3.10. *The map $\sigma = \tau^{d_\infty}$ respects the v_{∞_i} valuation for $i = 1, \ldots, d_\infty$.*

Proof. Note that τ acts trivially on X. Therefore, τ permutes the points $\infty_i \in X_K$. Consider $X \times \mathrm{Spec}(\mathbb{F}_{q^{d_\infty}})$. There lie d_∞ points above ∞ on this curve, and σ acts trivially on this curve. So σ acts trivially on the points $\infty_i \in X_K$. □

This lemma implies that the previous considerations on Newton polygons can be applied to the skew polynomial ring $F\{\sigma\}$ and to the places corresponding to ∞_i. For V we take M_F, which is a torsion $F\{\sigma\}$-module with $\dim_F M_F = r < \infty$.

Definition 4.3.11. An object $M \in \mathcal{C}$ is called *pure* if

(1) M_F is pure at ∞_i and $w_{\infty_i}(M_F) > 0$ for all i;

(2) $w_{\infty_1}(M_F) = \ldots = w_{\infty_{d_\infty}}(M_F)$.

The *weight* $w(M)$ *of* M is defined to be

$$w(M) := w_{\infty_i}(M_F).$$

Remark 4.3.12. The condition $w_{\infty_i}(M_F) > 0$ in the definition of purity is not very natural. We put it there for notational convenience. In the sequel we need this condition for our application to pure A-motives. E.g., in Proposition 4.3.16 we need that $w(M) \neq 0$. Consequently, in Proposition 4.3.22 we need $w(M) > 0$.

Note that by Lemma 4.3.8 a pure module M is cyclic.

4.3.3 Purity with lattices

We still assume that K is algebraically closed. Let R denote the ring of functions $f \in F$ which are regular in $\infty_1, \ldots, \infty_{d_\infty}$. This ring R is semi-local and Dedekind, so R is a PID. This implies that any finitely generated, torsion free R-module is free. In particular, any finitely generated R-submodule of M_F is free because it is torsion free.
An R-submodule $\Lambda \subset M_F$ is called an *R-lattice in M_F* if Λ contains a basis of M_F over F. Therefore, any R-lattice in M_F is a free R-module of rank r.
In R we pick an element t such that t has a pole of order 1 at each ∞_i. This means that $t^{-1} \in R$ and that $v_{\infty_i}(t^{-1}) = 1$ for all i.

Proposition 4.3.13. *Let V be a torsion $F\{\sigma\}$-module with $\dim_F V < \infty$, then V is pure of weight $w(V) \in \mathbb{Q}_{>0}$ if and only if there exists an R-lattice $\Lambda = \oplus_{i=1}^{n} Re_i \subset V$ with $n = \dim_F V$ and there exist integers $u, v > 0$ such that $t^{-u}\sigma^v \Lambda = \Lambda$ and $\frac{u}{v} = w(V)$.*

Proof. Proof of '$\Rightarrow$'. Let x be a cyclic element of $V \cong F\{\sigma\}/F\{\sigma\}g$. Let $v = \deg_\sigma(g) = \dim_F V$, and let $u = w(V) \cdot v$. Then the matrix of $t^{-u}\sigma^v$ on the basis $\{x, \sigma x, \ldots, \sigma^{v-1}x\}$ lies in $\mathrm{Gl}_v(R)$. So take

$$\Lambda = \oplus_{i=0}^{v-1} R \cdot \sigma^i x.$$

Proof of '$\Leftarrow$'. The matrix of $t^{-u}\sigma^v$ on $\{e_1, \ldots, e_n\}$ lies in $\mathrm{Gl}_n(R)$. Clearly, there is a generator x of V such that $x = \sum_{i=1}^{n} a_i e_i$ with $a_i \in R$ for all i, and there is an i with $a_i \in R^*$, say $a_1 \in R^*$. If we replace e_1 by x, then the matrix of $t^{-u}\sigma^v$ on $\{x, e_2, \ldots, e_n\}$ is still in $\mathrm{Gl}_n(R)$. So we may assume that e_1 generates V.
Write $t^{-u}\sigma^v e_1 = \sum_{i=1}^{n} a_i e_i$ with $a_i \in R$. If e_1 and $t^{-u}\sigma^v e_1$ are independent over F, we may assume that $a_2 \in R^*$, hence the basis transformation P which replaces e_2 by $t^{-u}\sigma^v e_1$ lies in $\mathrm{Gl}_n(R)$. So the matrix of $t^{-u}\sigma^v$ on this new basis lies in $\mathrm{Gl}_n(R)$. Arguing in this way, we end up with an F-basis β which contains the elements $e_1, t^{-u}\sigma^v e_1, \ldots, t^{-u(k-1)}\sigma^{v(k-1)}e_1$ such that

$$t^{-uk}\sigma^{vk}e_1 = \sum_{i=0}^{k-1} a_i \cdot t^{-ui}\sigma^{vi}e_1.$$

Because the matrix of $t^{-u}\sigma^v$ on β lies in $\mathrm{Gl}_n(R)$, it follows that the monic polynomial $\sum_{i=0}^{k} a_i \sigma^{vi}$ with $a_k = 1$ has slope 0. Therefore, the monic polynomial

$$h = \sum_{i=0}^{k} a_i t^{-u(i-k)}\sigma^{vi}$$

has one slope $\frac{u}{v}$. Note that $he_1 = 0$. If g is the minimal monic polynomial with $ge_1 = 0$, then $g \mid h$. Hence by Proposition 4.3.6 it follows that $N(g)$ has only one slope and that this slope equals $\frac{u}{v} = w(V)$. □

Remark 4.3.14. 1. Let M be a pure object in $\mathcal{C}$ of rank r, and let m be a cyclic element of M_F, then this proposition implies that the eigenvalues $\lambda_j \in \overline{F}$ of the matrix of σ on the basis $\{m, \sigma m, \ldots, \sigma^{r-1}m\}$ all have the same valuation at each ∞_i. Namely, $v_{\infty_i}(\lambda_j) = w(V)$ for all i and j.
2. We can even give an equivalent definition for purity in terms of the valuations of the eigenvalues. Let F^{s} be the separable closure of F. Then there is an element $\pi \in F^{\mathrm{s}}$ with $v_{\infty_i}(\pi^v t) = 0$ for all i. Let

$$R^{\mathrm{s}} = \{f \in F^{\mathrm{s}} \mid v_{\infty_i}(f) \geq 0\}.$$

Then V is pure of $w(V)$ iff there is a basis $\{e_1, \ldots, e_n\}$ of V over F^{s} such that the eigenvalues of the matrix of σ on this basis all have the same valuation $v_{\infty_i}(\lambda_j) = \frac{u}{v} = w(V)$ for all i and j. We take here $u, v \in \mathbb{N}$, and we see that the matrix of $\pi^u\sigma$ on this basis lies in $\mathrm{Gl}_r(R^{\mathrm{s}})$.
3. Although it might seem more natural to consider M_F as $F\{\tau\}$-module, for the definition of purity in terms of Newton polygons we need M_F as $F\{\sigma\}$-module. The above proposition states a criterion for purity in terms of M_F considered as $F\{\tau\}$-module because purity in terms of lattices reads as $t^u\tau^{d_\infty v}\Lambda = \Lambda$.

Following Anderson, we show that a pure object $M \in \mathcal{C}$ is a finitely generated $K\{\tau\}$-module.

Lemma 4.3.15. *Let t be as in Proposition 4.3.13, then there is an $N \in \mathbb{N}$ such that*

$$K \otimes A + t^N R = F.$$

Proof. This is essentially Riemann-Roch, which states that for a divisor D

$$l(D) - l(\omega - D) = \deg(D) + 1 - g$$

where ω is a canonical divisor. Write $D = \sum_{i=1}^{d_\infty} [\infty_i]$. We may choose N such that $l(\omega - kD) = 0$ for all $k \geq N$. We claim that the natural map $K \otimes A \longrightarrow F/t^N R$ is surjective. To prove this, we consider the following filtration of F:

$$t^N R \subset t^{N+1} R \subset \dots.$$

For $i = 1, \dots, d_\infty$ let $\pi_i \in R$ be generators of the maximal ideals of R. We may choose the π_i such that $t^{-1} = \prod_i \pi_i$. Clearly, the K-vectorspace $t^{N+i+1}R/t^{N+i}R$ is generated by the functions $\pi_j^{-(N+i+1)}$ for $j = 1, \dots, d_\infty$. So this K-vectorspace has dimension d_∞. On the other hand,

$$l((N+i+1)D) = l((N+i)D) + d_\infty.$$

So we may choose generators of $t^{N+i+1}R/t^{N+i}R$ inside $K \otimes A$. This proves the surjectivity of the map. □

Proposition 4.3.16. *Let K be algebraically closed and let M be an object of $\mathcal{C}$. If M is pure, then M is finitely generated as $K\{\tau\}$-module.*

Proof. We let $m \in M_F$ be a generator of M_F as $F\{\tau\}$-module such that

$$m, \tau m, \dots, \tau^{r-1} m \in M.$$

We let

$$\Lambda = \oplus_{i=0}^{r-1} R \cdot \tau^i m.$$

Furthermore, we write $\pi_i \in R$ for $i = 1, \dots, d_\infty$ for the generators of the maximal ideals of R. We may assume that $t^{-1} = \prod_i \pi_i$.
Claim 1. There is an integer N such that

$$M + t^N \Lambda = M_F.$$

Because we chose generators of Λ over R inside M, we may apply Lemma 4.3.15 componentwise. So there is an N' with

$$M_F = \oplus_i F\tau^i m = \oplus_i (K \otimes A\tau^i m + t^{N'} R\tau^i m) \subset M + t^{N'}\Lambda \subset M_F.$$

This proves *Claim 1.*
Claim 2. We let the integers $u, v > 0$ be such that $w(M) = d_\infty \frac{u}{v}$. Let M_j be the following filtration of M:

$$(ii) \qquad M_j := M \cap t^{(j+N)u}\Lambda, \quad j \geq 1,$$

then

$$(iii) \qquad M_{j+1} = M_j + t^u M_j = M_j + \tau^v M_j.$$

To prove this, we will prove

$$(iv) \quad M_{j+1}/M_j \cong t^{(j+1+N)u}\Lambda/t^{(j+N)u}\Lambda \cong \tau^{(j+1+N)v}\Lambda/\tau^{(j+N)v}\Lambda.$$

(iv) is a consequence of *Claim 1*, as one may see by straightforward computation. Note that the second isomorphism follows from the definition of purity, which states that $t^u\Lambda = \tau^v\Lambda$. Using *Claim 1* and a straightforward computation, it follows that (iv) implies (iii). This proves *Claim 2*.
Claim 3. M is a finitely generated $K\{\tau\}$-module.
To prove *Claim 3*, we will prove $\dim_K M_1 < \infty$. By *Claim 2* we have $M = K\{\tau\} \cdot M_1$. This proves *Claim 3*.
We write

$$M' = \oplus_{i=1}^r K \otimes A \cdot \tau^i m \subset M,$$

and we let $M_1' = M' \cap M_1$. Because M is projective of rank r, M'/M is a finitely generated torsion $K \otimes A$-module and thus $\dim_K M'/M < \infty$. So it suffices to prove that $\dim_K M_1' < \infty$. Now

$$M_1' \subset M' \cap t^{(N+1)u}\Lambda = \oplus_{i=1}^r (K \otimes A \cap t^{(N+1)u}R) \cdot \tau^i m.$$

For all $x \in K \otimes A$ one has $v_{\pi_i}(x) \leq 0$, hence $K \otimes A \cap t^{-1}R = 0$. Therefore, the obvious map

$$K \otimes A \cap t^{(N+1)u+n}R \longrightarrow t^{(N+1)u+n}R/t^{-1}R$$

is injective. This latter object is a finite dimensional K-vector space. Hence $\dim_K M' < \infty$. □

Corollary 4.3.17. *Let K be algebraically closed and let M be a pure object of $\mathcal{C}$, then the weight of M is*

$$w(M) = w(M_F) = \frac{\dim_{K\{\tau\}} M}{\dim_{K\otimes A} M} = \frac{\rho}{r}.$$

Proof. First assume that K is algebraically closed. We use the notation as in *Claim 2* of the proof of the previous proposition. On the one hand, it follows that

$$\dim_K M_{j+1}/M_j = \dim_K t^{(j+1+N)u}\Lambda/t^{(j+N)u}\Lambda = d_\infty ru$$

because the K-vectorspace $t^{j+1}R/t^jR$ has dimension d_∞. On the other hand, we have $M_{j+1} = M_j + \tau^v M_j$, hence

$$\dim_K M_{j+1}/M_j = \rho v$$

where $\rho = \dim_{K\{\tau\}} M$. So $\frac{u}{v} = d_\infty \frac{\rho}{r}$. □

Remark 4.3.18. An alternative proof for Proposition 4.3.16 and Corollary 4.3.17 would be the following. Consider an element $a \in A$ such that the A is a finite $\mathbb{F}_q[a]$-algebra. Then a pure A-motive M gives rise to a pure $\mathbb{F}_q[a]$-motive M. By [1] it follows that M is a finitely generated $K\{\tau\}$-module. The formula for the weight follows then also from Anderson's computation.

Finally, we define purity for general K, so we drop the assumption that K is algebraically closed.

Definition 4.3.19. Let M be an object of $\mathcal{C}$, then M is called *pure*, if $M \otimes_K \overline{K}$ is pure. The *weight* $w(M)$ of M is defined to be the weight of $M \otimes \overline{K}$.

First we will show that Proposition 4.3.16 and Corollary 4.3.17 still hold in this context.

Lemma 4.3.20. *Let M be an object of $\mathcal{C}$ with projective $K \otimes A$-rank r. Then $M \otimes_K \overline{K}$ is an object of $\mathcal{C}_{\overline{K}}$ with projective $\overline{K} \otimes A$-rank r. Moreover, under this condition M is a finitely generated $K\{\tau\}$-module of dimension ρ if and only if $\overline{M}$ is a finitely generated $\overline{K}\{\tau\}$-module of dimension ρ.*

Proof. Clearly, $\overline{M}$ is a finitely generated projective $\overline{K} \otimes A$-module of rank r. If M is finitely generated over $K\{\tau\}$ of dimension ρ, then it is free of dimension ρ; cf. Lemma 4.2.7. Hence also $\overline{M} = \overline{K} \otimes_K M$ is free of dimension ρ over $\overline{K}\{\tau\}$.
On the other hand, let $\overline{M}$ be finitely generated over $\overline{K}\{\tau\}$ of dimension ρ, then it is free. Suppose that M is not finitely generated over $\overline{K}\{\tau\}$, then there exists a strictly increasing sequence $(M_i)_{i\geq 0}$ of $K\{\tau\}$-submodules of M. Because $\overline{K}$ over K is flat, this would give a strictly increasing sequence $(\overline{K} \otimes M_i)$ of $\overline{K}\{\tau\}$-modules, contradicting the fact that $\overline{M}$ is finitely generated. □

This lemma implies the following proposition.

Proposition 4.3.21. *Let M be an object of $\mathcal{C}$. If M is pure, then M is finitely generated as $K\{\tau\}$-module. Moreover, in that case*

$$w(M) = \frac{\rho}{r},$$

where $r = \dim_{K\otimes A} M$ and $\rho = \dim_{K\{\tau\}} M$.

We can now consider the subcategory of $\mathcal{C}$ consisting of all pure objects of $\mathcal{C}$. In the following proposition we show that this subcategory is closed under the constructions of linear algebra which we defined in the introduction of this section. Moreover, we show that the same holds for the subcategory of pure A-motives in $\mathcal{C}$.

Proposition 4.3.22. *Let M, M' and M'' be non-zero objects of $\mathcal{C}$.*

i. Let M be pure and let

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

be an exact sequence, then M' and M'' are also pure and

$$w(M') = w(M'') = w(M).$$

If we suppose that M is a pure A-motive, then also M' and M'' are pure A-motives.

ii. Let M and M' be pure, then the $K\{\tau\}\otimes A$-module $M\otimes_{K\otimes A} M'$ is a pure object of $\mathcal{C}$ and

$$w(M\otimes M') = w(M) + w(M').$$

If we suppose that M and M' are pure A-motives, then also $M\otimes M'$ is a pure A-motive.

Proof. We write $\overline{N} = N\otimes_K \overline{K}$ for any $K\{\tau\}\otimes A$-module N.
i. The exact sequence of the proposition gives rise to the following exact sequence of $F\{\sigma\}$-modules:

$$0 \longrightarrow \overline{M}'_F \longrightarrow \overline{M}_F \longrightarrow \overline{M}''_F \longrightarrow 0.$$

Let Λ be an R-lattice in M_F with $t^u\Lambda = \sigma^v\Lambda$. Define $\Lambda'\subset M'_F$ to be the module whose image is $\Lambda\cap M'_F$, and define Λ'' to be the image of Λ inside M''_F. Then Λ' and Λ'' are R-lattices. Using the $F\{\sigma\}$-linearity of the maps in the exact sequence, it follows immediately that

$$t^u\Lambda' = \sigma^v\Lambda' \quad\text{and}\quad t^u\Lambda'' = \sigma^v\Lambda''.$$

Consequently, M' and M'' are both pure of weight $w(M)$.
For the 'A-motive'-part we only need to check property (3) of Definition 4.2.4 for M' and M''. For M' it follows because $\tau M\cap M' = \tau M'$. For M'' it follows, because τM is mapped onto $\tau M''$.
ii. By Definition 4.3.13 there exist integers $u, v, u', v' > 0$ and R-lattices $\Lambda\subset \overline{M}_F$, $\Lambda'\subset \overline{M}'_F$ with $t^u\Lambda = \sigma^v\Lambda$ and $t^{u'}\Lambda = \sigma^{v'}\Lambda$. So

$$\sigma^{vv'}(\Lambda\otimes\Lambda') = \sigma^{vv'}\Lambda\otimes\sigma^{v'v}\Lambda' = t^{uv'}\Lambda\otimes t^{u'v}\Lambda' = t^{uv'+u'v}(\Lambda\otimes\Lambda').$$

Clearly, $\Lambda\otimes\Lambda'\subset \overline{M}_F\otimes\overline{M}'_F$ is an R-lattice. So $\overline{M}\otimes\overline{M}'$ is pure of weight $w(M)+w(M')$. Note that

$$\overline{M}\otimes\overline{M}' \cong \overline{(M\otimes M')},$$

hence $M\otimes M'$ is pure of weight $w(M)+w(M')$.
For the 'A-motive'-part we only need to check property (3) of Definition 4.2.4. Note that $\tau M\otimes\tau M' = \tau(M\otimes M')$. From this property (3) easily follows. □

Corollary 4.3.23. *If φ is a pure abelian A-motive of rank r and dimension n, then there exists a pure abelian A-motive ψ of rank 1, and dimension n with $M(\psi)\cong \wedge^r_{K\otimes A} M(\varphi)$. The A-motive ψ is unique up to isomorphism.*

Proof. Let $M(\varphi)$ be the pure A-motive associated to φ, then the module $\wedge^r_{K\otimes A}M(\varphi)$ is also a pure A-motive. By Proposition 4.3.22 it has weight

$$w(\wedge^r_{K\otimes A}M(\varphi)) = rw(M(\varphi)) = n.$$

Clearly, $\wedge^r_{K\otimes A}M(\varphi)$ has rank 1; hence, it has dimension n. By Theorem 4.2.9 there exists a pure abelian A-module ψ of rank 1 and dimension n with $M(\psi)\cong\wedge^r_{K\otimes A}M(\varphi)$. □

By Proposition 4.2.11 a Drinfeld module of rank r is an abelian A-module of dimension 1 and rank r. The following proposition states that every Drinfeld module is pure.

Proposition 4.3.24. *Every abelian A-module φ of rank r and dimension 1 is pure of weight $\frac{1}{r}$.*

Proof. Let $M = M(\varphi) = K\{\tau\} \cdot m$ be the A-motive associated to φ. We may assume that $K = \overline{K}$: if this is not the case, we replace M by $M \otimes \overline{K}$.
Let $a \in A$ and $n = r \deg(a)$, and write

$$\varphi_a = \sum_{i=0}^{n} k_i \tau^i \quad \text{with } k_i \in K, k_n \in K^*.$$

Let $e_i = \tau^i m$ for $i = 0, \ldots, n-1$, and let

$$\Lambda = Re_0 \oplus \cdots \oplus Re_{n-1}.$$

Then Λ is an R-lattice: the elements $e_0, e_1, \ldots, e_{r-1}$ generate M_F over F.

1. $\Lambda \subset \tau\Lambda$; this follows from property (3) of Definition 4.2.4, which states that for all $b \in A$ there is an $n \in \mathbb{N}$ such that

   $$(1 \otimes b - \gamma(b) \otimes 1)^n M \subset \tau M.$$

   Because $\frac{1}{(1 \otimes b - \gamma(b) \otimes 1)^n} \in R$, it follows that the generators $\tau^i m$ of Λ are elements of $\tau\Lambda$.

2. Because $\frac{1}{a} \in R$, we have $\Lambda \subset a\Lambda$.

With these two properties it follows that $a\Lambda = \tau^n \Lambda$ by simply looking at the generators of $a\Lambda$ and $\tau^n\Lambda$. First note that

$$\tau^n e_i = \tau^{n+i} m = \tau^i \left(\frac{1}{k_n} \varphi_a - \sum_{j=0}^{n-1} \frac{k_i}{k_n} \tau^j \right) m$$

$$= \frac{1}{k_n^{q^i}} a e_i - \sum_{j=0}^{n-1} \left(\frac{k_j}{k_n} \right)^{q^i} \tau^{i+j} m,$$

so if we let i run from 0 up to $n-1$, we see that the generators $\tau^n e_i$ of $\tau^n\Lambda$ are elements of $a\Lambda$.
On the other hand, note that

$$a e_i = \tau^i \varphi_a m = \sum_{j=0}^{n} k_j \tau^{i+j} m.$$

So if we let i run from 0 up to $n-1$, we see that the generators ae_i of $a\Lambda$ lie in $\tau^n\Lambda$.
Now $\frac{t^{\deg(a)}}{a^{d_\infty}} \in R^*$, hence $t^{\deg(a)}\Lambda = \tau^{d_\infty n}\Lambda = \sigma^n\Lambda$. So M is pure of weight $\frac{1}{r}$. □

Remark 4.3.25. If we assume $d_\infty = 1$, then the proof of this proposition follows immediately from the description of purity in terms of the Newton polygon: let $s_1, \ldots, s_k$ be generators of the $\mathbb{F}_q$-algebra A, then

$$M(\varphi) \cong (K\{\tau\} \otimes A)/(\varphi_{s_1} \otimes 1 - 1 \otimes s_1, \ldots, \varphi_{s_k} \otimes 1 - 1 \otimes s_k).$$

The Newton polygon of $\varphi_{s_i} \otimes 1 - 1 \otimes s_i$ has slope $\frac{1}{r}$ at ∞ for all i. So M is pure of weight $\frac{1}{r}$.

This enables us to prove Theorem 4.3.3:

Proof. Proposition 4.3.24 proves that $M(\varphi)$ is pure; hence, by Corollary 4.3.23 the exterior product $\wedge^r_{K \otimes A} M(\varphi)$ is in fact a Drinfeld module of rank 1. □

4.4 The $\mathfrak{a}$-torsion of an abelian A-module

Let φ be an abelian A-module of dimension n and let $\mathfrak{a} \subset A$ be a proper ideal away from the characteristic. In this section we give a description of

$$\ker(\varphi_{\mathfrak{a}})(\overline{K}) := \bigcap_{a \in \mathfrak{a}} \ker(\varphi_a)(\overline{K})$$

in terms of the corresponding A-motive $M = M(\varphi)$. As before we denote $\overline{M} = M \otimes_K \overline{K}$. An ideal $\mathfrak{a} \subset A$ commutes with the elements in $K\{\tau\} \otimes A$. So it makes sense to consider $\overline{M}/\mathfrak{a}\overline{M}$. We equip $\mathrm{Hom}_{\mathbb{F}_q}(A, \mathbb{F}_q)$ with an A-module structure by $a \cdot h(b) = h(ab)$ for all $a, b \in A$. Similarly, we equip $\mathrm{Hom}_{\mathbb{F}_q}(A, \overline{K})$ with an $\overline{K}\{\tau\} \otimes A$-module structure by

$$(f \otimes a)h(b) = fh(ab) \quad \text{for all } f \in \overline{K}\{\tau\} \text{ and } a, b \in A.$$

We let Ω_A be the differential module of A over $\mathbb{F}_q$, which is a projective module of rank 1. Let $P \in X$ be a point, then we denote by $\mathrm{Res}_P(\omega)$ the residue at P of the differential ω. We denote

$$\Omega_{\mathfrak{a}} = \mathfrak{a}^{-1}\Omega_A/\Omega_A.$$

Finally, for a $\overline{K}\{\tau\} \otimes A$-module N we write N^τ for the τ-invariant part of N.

Proposition 4.4.1. *There is a canonical isomorphism of $A/\mathfrak{a}$-modules*

$$\Omega_{\mathfrak{a}} \cong \mathrm{Hom}_{\mathbb{F}_q}(A/\mathfrak{a}, \mathbb{F}_q) \quad \text{by } \omega \mapsto g_\omega : a \mapsto \mathrm{Tr}_{\mathbb{F}_q} \circ \mathrm{Res}_\infty(a\omega).$$

Here Res_∞ is the residue map and $\mathrm{Tr}_{\mathbb{F}_q}$ is the trace map.

Proof. Consider the residue map

$$\mathrm{Res}_\infty : A \times \mathfrak{a}^{-1}\Omega_A \longrightarrow \mathbb{F}_{q^{d_\infty}}$$

given by $(a, \omega) \mapsto \mathrm{Res}_\infty(a\omega)$. It is easy to verify that this map induces a non-degenerate pairing

$$\mathrm{Res}_\infty : A/\mathfrak{a} \times \Omega_{\mathfrak{a}} \longrightarrow \mathbb{F}_{q^{d_\infty}}.$$

The composition with the trace map gives a perfect pairing. □

Theorem 4.4.2. (S. Lang)
For $g \in \mathrm{Gl}_n(\overline{K})$ we put $\tau(g)$ for τ applied to each entry of g. The map

$$\mathrm{Gl}_n(\overline{K}) \longrightarrow \mathrm{Gl}_n(\overline{K}), \text{givenby } g \mapsto g^{-1}\tau(g)$$

is surjective.

Proof. This is shown in [36]. □

Lemma 4.4.3. *The $\overline{K}\{\tau\} \otimes A$-module map*

$$(\overline{M}/\mathfrak{a}\overline{M})^\tau \otimes_{\mathbb{F}_q} \overline{K} \longrightarrow \overline{M}/\mathfrak{a}\overline{M}$$

is an isomorphism.

Proof. The map $(\overline{M}/\mathfrak{a}\overline{M})^\tau \otimes_{\mathbb{F}_q} \overline{K} \longrightarrow \overline{M}/\mathfrak{a}\overline{M}$ is clearly injective, so we only need to prove that

$$\dim_{\mathbb{F}_q}(\overline{M}/\mathfrak{a}\overline{M})^\tau = \dim_{\overline{K}} \overline{M}/\mathfrak{a}\overline{M}.$$

Let $n = \dim_{\overline{K}} \overline{M}/\mathfrak{a}\overline{M}$. If we choose a basis β for this vectorspace, we may write down the matrix B_τ of τ on β.
Let φ be the abelian A-module corresponding to M, and write $\varphi_a = \sum_i A_i(a)\tau^i$. By assumption $\mathfrak{a}$ is away from the characteristic. This means that $\gamma(a) \neq 0$ and thus $A_0(a) \neq 0$ for all non-zero $a \in \mathfrak{a}$. From this it is not difficult to see that τ defines an $\mathbb{F}_q$-linear automorphism of $\overline{M}/\mathfrak{a}\overline{M}$. Therefore, the matrix B_τ lies in $\mathrm{Gl}_n(\overline{K})$.
Consider the map χ which associates to a basis transformation g the matrix of τ on the basis $g(\beta)$:

$$\chi : \mathrm{Gl}_n(\overline{K}) \longrightarrow \mathrm{Gl}_n(\overline{K}), \quad \text{by} \quad g \mapsto \tau(g) \cdot B_\tau \cdot g^{-1}.$$

By $\tau(g)$ we denote the matrix that we get from applying τ to each entry of g. By Lang's Theorem 4.4.2 the unit element is in the image of χ. This implies that there is a basis of $\overline{M}/\mathfrak{a}\overline{M}$ such that τ is given on this basis by the identity matrix. Because τ fixes each basis element, we have that this basis also forms a basis for the $\mathbb{F}_q$-vectorspace $(\overline{M}/\mathfrak{a}\overline{M})^\tau$. □

Proposition 4.4.4. *Let L be a field extension of K and let $\mathbb{G}_{a,K}^n$ be equipped with an abelian A-module φ. Let $M_L = M(\varphi) \otimes_K L$, then there is a canonical A-module isomorphism:*

$$\mathbb{G}_a^n(L) \xrightarrow{\sim} \mathrm{Hom}_{L\{\tau\}\otimes A}\left(M_L, \mathrm{Hom}_{\mathbb{F}_q}(A, \mathbb{G}_a(L))\right)$$

$$\text{by} \quad x \mapsto h_x : (m, a) \mapsto (m \circ \varphi_a)(x).$$

This isomorphism induces a canonical A-isomorphism

$$\ker(\varphi_\mathfrak{a})(L) \longrightarrow \mathrm{Hom}_{L\{\tau\}\otimes A}\left(M_L, \Omega_\mathfrak{a} \otimes_{\mathbb{F}_q} \mathbb{G}_a(L)\right).$$

If $L = \overline{K}$, then this latter object is canonically A-isomorphic to

$$\mathrm{Hom}_{A/\mathfrak{a}}\left((\overline{M}/\mathfrak{a}\overline{M})^\tau, \Omega_\mathfrak{a}\right).$$

Proof. Note that $M_L \cong L\{\tau\}^n$. To see that the described map is surjective, note that it is also an L-linear map. Choose an L-basis $x_1, \ldots, x_n$ of $\mathbb{G}_{a,K}^n(L)$, and let $e_1, \ldots, e_n$ be the corresponding basis of M_L over $L\{\tau\}$, i.e., $e_i(x_j) = \delta_{i,j} \in L \cong \mathbb{G}_{a,K}(L)$.
For any homomorphism h from the left-hand side we have $h(m, a) = h(m \circ \varphi_a, 1)$. Write $m \circ \varphi_a = \sum_i \lambda_i e_i$ with $\lambda_i \in L\{\tau\}$, then

$$h(m, a) = \sum_i \lambda_i h(e_i, 1).$$

In particular, it follows that $h = \sum_i \lambda_i h(e_i, 1) h_{x_i}$. Consequently, the map is surjective. As both sides have the same dimension as L-vectorspace, the first isomorphism follows.
For the second isomorphism note that the first isomorphism induces an isomorphism

$$\ker(\varphi_\mathfrak{a})(L) \xrightarrow{\sim} \mathrm{Hom}_{L\{\tau\}\otimes A}\left(M_L, \mathrm{Hom}_{\mathbb{F}_q}(A/\mathfrak{a}, \mathbb{G}_a(L))\right).$$

The second isomorphism follows because $\Omega_{\mathfrak{a}}$ is canonically isomorphic to $\mathrm{Hom}_{\mathbb{F}_q}(A/\mathfrak{a}, \mathbb{F}_q)$; cf. Lemma 4.4.1.
For the third isomorphism we note that

$$\mathrm{Hom}_{\overline{K}\{\tau\}\otimes A}\left(\overline{M}, \Omega_{\mathfrak{a}} \otimes \mathbb{G}_a(\overline{K})\right) = \mathrm{Hom}_{\overline{K}\{\tau\}\otimes A}\left(\overline{M}/\mathfrak{a}\overline{M}, \Omega_{\mathfrak{a}} \otimes \mathbb{G}_a(\overline{K})\right).$$

Any $A/\mathfrak{a}$-linear map

$$h : (\overline{M}/\mathfrak{a}\overline{M})^{\tau} \longrightarrow \Omega_{\mathfrak{a}}$$

gives rise to a $\overline{K} \otimes A$-linear map

$$\tilde{h} : \overline{M}/\mathfrak{a}\overline{M} \longrightarrow \Omega_{\mathfrak{a}} \otimes \overline{K}$$

by tensoring both sides with $\overline{K}$. This map $\tilde{h}$ is also $\overline{K}\{\tau\} \otimes A$-linear because τ commutes with elements from A. So there is a canonical $A/\mathfrak{a}$-linear map

$$\mathrm{Hom}_{A/\mathfrak{a}}\left((\overline{M}/\mathfrak{a}\overline{M})^{\tau}, \Omega_{\mathfrak{a}}\right) \longrightarrow \mathrm{Hom}_{\overline{K}\{\tau\}\otimes A}\left(\overline{M}, \Omega_{\mathfrak{a}} \otimes \overline{K}\right)$$

which is injective. To see that it is surjective, we use Lemma 4.4.3. By this lemma there is an $\mathbb{F}_q$-basis of $(\overline{M}/\mathfrak{a}\overline{M})^{\tau}$ which induces a $\overline{K}$ basis of $\overline{M}/\mathfrak{a}\overline{M}$. Consequently, any $\overline{K}\{\tau\} \otimes A$-linear map

$$h : \overline{M} \longrightarrow \Omega_{\mathfrak{a}} \otimes \mathbb{G}_a(\overline{K}))$$

comes from an $A/\mathfrak{a}$-linear map

$$h : (\overline{M}/\mathfrak{a}\overline{M})^{\tau} \longrightarrow \Omega_{\mathfrak{a}}.$$

This finishes the proof. □

Corollary 4.4.5. *The kernel* $\ker(\varphi_{\mathfrak{a}})(\overline{K})$ *is a free* $A/\mathfrak{a}$*-module of rank* r*.*

Proof. The A-motive $\overline{M}$ has projective $\overline{K} \otimes A$-rank r. Because $A/\mathfrak{a}$ is a PID, this implies that $\overline{M}/\mathfrak{a}\overline{M}$ is a free $\overline{K} \otimes A/\mathfrak{a}$-module of rank r. Therefore, the τ-invariant submodule $(\overline{M}/\mathfrak{a}\overline{M})^{\tau}$ is a free $A/\mathfrak{a}$-module of rank r. As $\Omega_{\mathfrak{a}}$ is a free $A/\mathfrak{a}$-module of rank 1, we see that

$$\mathrm{Hom}_{A/\mathfrak{a}}((\overline{M}/\mathfrak{a}\overline{M})^{\tau}, \Omega_{\mathfrak{a}}) \cong (A/\mathfrak{a})^{r}.$$

□

Remark 4.4.6. Corollary 4.4.5 completes the proof of Proposition 4.2.11.

4.5 Construction of the Weil pairing.

In the previous two sections we discussed the natural generalization of Anderson's constructions in [1]. In Section 4.3 we showed that there exists a pure abelian A-module ψ of rank 1 and dimension n such that $M(\psi) \cong \wedge^r_{K\otimes A} M(\varphi)$; cf. Corollary 4.3.23. In the previous section we described $\ker(\varphi_{\mathfrak{a}})(\overline{K})$. These two results are the main ingredients for the construction of the Weil pairing.

Let $\mathfrak{a} \subset A$ be a proper ideal away from the characteristic. Let φ be a pure abelian A-module of rank r and dimension n. Let ψ be a pure abelian A-module of rank 1 and dimension n with $M(\psi) \cong \wedge^r_{K\otimes A} M(\varphi)$. Let

$$N := (\overline{M}(\varphi)/\mathfrak{a}\overline{M}(\varphi))^{\tau},$$

then N is a free $A/\mathfrak{a}$-module of rank r.

Lemma 4.5.1. *Let*

$$\mathrm{Det} : \prod_{i=1}^{r} \mathrm{Hom}_{A/\mathfrak{a}}(N, \Omega_{\mathfrak{a}}) \longrightarrow \mathrm{Hom}_{A/\mathfrak{a}}(\wedge^r N, \Omega_{\mathfrak{a}}^{\otimes r})$$

be the map defined by $\mathrm{Det} : (h_1, \ldots, h_r) \mapsto h_1 \wedge \ldots \wedge h_r$ *with*

$$h_1 \wedge \cdots \wedge h_r : n_1 \wedge \cdots \wedge n_r \mapsto \sum_{\sigma \in S_r} \mathrm{sgn}(\sigma) \cdot h_1(n_{\sigma(1)}) \otimes \cdots \otimes h_r(n_{\sigma(r)}).$$

This map gives rise to an A-linear isomorphism

$$\wedge^r \mathrm{Hom}_{A/\mathfrak{a}}(N, \Omega_{\mathfrak{a}}) \xrightarrow{\sim} \mathrm{Hom}_{A/\mathfrak{a}}(\wedge^r N, \Omega_{\mathfrak{a}}^{\otimes r}).$$

Proof. Consider the map $N^{\otimes r} \longrightarrow \Omega_{\mathfrak{a}}^{\otimes r}$ given by

$$n_1 \otimes \ldots \otimes n_r \mapsto \sum_{\sigma \in S_r} \mathrm{sgn}(\sigma) \cdot h_1(n_{\sigma(1)}) \otimes \cdots \otimes h_r(n_{\sigma(r)}).$$

This map is alternating and A-multilinear, so it factors over $\wedge^r N$. This shows that Det exists.
To see that Det gives rise to an isomorphism as claimed in the lemma, note that the left-hand side and the right-hand side of the isomorphism are isomorphic to $A/\mathfrak{a}$. Therefore, it is enough to see that Det is surjective. Let $n_1, \ldots, n_r$ be a basis of N and let e be a basis of $\Omega_{\mathfrak{a}}$. We let $h_1, \ldots, h_r$ be the basis dual to $n_1, \ldots, n_r$, i.e., $h_i(n_j) = \delta_{i,j} \cdot e$. An easy computation shows that

$$h_1 \wedge \ldots \wedge h_r : n_1 \wedge \ldots \wedge n_r \mapsto e \otimes \ldots \otimes e.$$

As $\Omega_{\mathfrak{a}}^{\otimes r} = A/\mathfrak{a} \cdot e \otimes \ldots \otimes e$, it follows that $h_1 \wedge \ldots \wedge h_r$ generates $\mathrm{Hom}_{A/\mathfrak{a}}(\wedge^r N, \Omega_{\mathfrak{a}}^{\otimes r})$. □

Lemma 4.5.2. *There is a canonical isomorphism*

$$\wedge^r N \cong_A (\wedge^r \overline{M}(\varphi)/\mathfrak{a} \wedge^r \overline{M}(\varphi))^{\tau}.$$

Proof. First note that

$$(\otimes^r_{\overline{K} \otimes A} \overline{M}(\varphi)) \otimes_A A/\mathfrak{a} \cong \otimes^r_{\overline{K} \otimes A} (\overline{M}(\varphi))/\mathfrak{a}\overline{M}(\varphi))$$

as $\overline{K} \otimes A$-modules. Consequently, we have a canonical $\overline{K}\{\tau\} \otimes A/\mathfrak{a}$-isomorphism

$$\wedge^r \overline{M}(\varphi)/\mathfrak{a} \wedge^r \overline{M}(\varphi) \xrightarrow{\sim} \wedge^r (\overline{M}(\varphi)/\mathfrak{a}\overline{M}(\varphi)).$$

The right-hand side of this isomorphism is isomorphic to $\wedge^r_{\overline{K} \otimes A}(N \otimes_{\mathbb{F}_q} \overline{K}) \cong (\wedge^r_A N) \otimes \overline{K}$; cf. Lemma 4.4.3. Taking τ-invariants proves the lemma. □

Theorem 4.5.3. *Let φ be an abelian A-module of rank r and dimension n and let ψ be an abelian A-module of rank 1 and dimension 1 such that $\wedge^r M(\varphi) \cong M(\psi)$. Let $\mathfrak{a} \subset A$ be a proper ideal of A away from the characteristic, then there exists a* Weil pairing

$$w_{\mathfrak{a}} : \prod_{i=1}^{r} \ker(\varphi_{\mathfrak{a}})(\overline{K}) \longrightarrow \ker(\psi_{\mathfrak{a}})(\overline{K}) \otimes \Omega_{\mathfrak{a}}^{\otimes r-1}$$

which is unique up to a unique isomorphism of ψ and which induces an A-isomorphism

$$\wedge^r \ker(\varphi_{\mathfrak{a}})(\overline{K}) \xrightarrow{\sim} \ker(\psi_{\mathfrak{a}})(\overline{K}) \otimes \Omega_{\mathfrak{a}}^{\otimes r-1}.$$

Proof. The proof follows simply by gathering all the properties on $\ker(\varphi_{\mathfrak{a}})(\overline{K})$ and the map Det that we have discussed so far. Recall that we have a canonical isomorphism $\ker(\varphi_{\mathfrak{a}}) \cong \mathrm{Hom}_{A/\mathfrak{a}}(N, \Omega_{\mathfrak{a}})$; cf. Proposition 4.4.4. Using Lemma 4.5.1 we get a canonical map

$$\mathrm{Det} : \ker(\varphi_{\mathfrak{a}}) \longrightarrow \mathrm{Hom}_{A/\mathfrak{a}}(\wedge^r N, \Omega_{\mathfrak{a}}^{\otimes r})$$

which is surjective, alternating and multilinear. As $\Omega_{\mathfrak{a}}$ is a free $A/\mathfrak{a}$-module, we have

$$\mathrm{Hom}_{A/\mathfrak{a}}(\wedge^r N, \Omega_{\mathfrak{a}}^{\otimes r}) \cong \mathrm{Hom}_{A/\mathfrak{a}}(\wedge^r N, \Omega_{\mathfrak{a}}) \otimes \Omega_{\mathfrak{a}}^{\otimes r-1}.$$

As $\wedge^r M(\varphi) \cong M(\psi)$, we can replace $\wedge^r N$ in the right-hand side of this isomorphism by $(\overline{M}(\psi)/\mathfrak{a}\overline{M}(\psi))^{\tau}$; cf. Lemma 4.5.2. Applying Proposition 4.4.4 gives that

$$\mathrm{Hom}_{A/\mathfrak{a}}(\wedge^r N, \Omega_{\mathfrak{a}}^{\otimes r}) \cong \ker(\psi_{\mathfrak{a}})(\overline{K}) \otimes \Omega_{\mathfrak{a}}^{\otimes r-1}$$

because $M(\psi) \cong \wedge^r M(\varphi)$. This defines $w_{\mathfrak{a}}$. This construction of $w_{\mathfrak{a}}$ is unique up to an isomorphy of ψ. □

4.5.1 Properties of the Weil pairing

We will use the notations from Theorem 4.5.3. Let $\mathfrak{a}, \mathfrak{b} \subset A$ be two proper ideals away from the characteristic of φ. This implies that the polynomial $\varphi_a(Z)$ is separable for all $a \in \mathfrak{a}$ and $a \in \mathfrak{b}$. Therefore, the Weil pairing is already defined over K^{s}, the separable closure of K. Let $G_K = \mathrm{Gal}(K^{\mathrm{s}}/K)$.

Proposition 4.5.4. *With the notations as above, the Weil pairing has the following properties:*

i. Galois equivariance. *Let* $x_1, \ldots, x_r \in \ker(\varphi_{\mathfrak{a}})(K^{\mathrm{s}})$ *and* $\sigma \in G_K$, *then*

$$w_{\mathfrak{a}}(x_1^{\sigma}, \ldots, x_r^{\sigma}) = w_{\mathfrak{a}}(x_1, \ldots, x_r)^{\sigma}.$$

ii. Compatibility. *Let*

$$x \in \ker(\varphi_{\mathfrak{ab}})(K^{\mathrm{s}}), \quad y_1, \ldots, y_{r-1} \in \ker(\varphi_{\mathfrak{a}})(K^{\mathrm{s}}),$$

then for all $b \in \mathfrak{b}$ *we have*

$$b \cdot w_{\mathfrak{ab}}(x, y_1, \ldots, y_{r-1}) = w_{\mathfrak{a}}(\varphi_b(x), y_1, \ldots, y_{r-1}).$$

iii. Duality. *Let* φ *and* φ' *be two Drinfeld modules over* K *of rank* r *and of general characteristic such that*

$$\wedge^r M(\varphi) \cong \wedge^r M(\varphi').$$

Let ψ *be a Drinfeld module of rank* 1 *with*

$$\wedge^r M(\varphi) \cong \wedge^r M(\varphi') \cong M(\psi).$$

Let $u : \varphi \longrightarrow \varphi'$ *be an isogeny, then* u *induces a map*

$$\det(u) : \psi \longrightarrow \psi$$

and $\det(u) = \psi_a$ *for some* $a \in A$. *There exists an isogeny* $u^* : \varphi' \longrightarrow \varphi$ *such that*

$$u^*u = \varphi_{\det(u)} \text{ and } \det(u^*) = \det(u).$$

The isogeny u^* *is called the* adjoint *of* u, *and it has the following property: let* $x_1, \ldots, x_r \in \ker(\varphi_{\mathfrak{a}})$, *then*

$$w_{\mathfrak{a}}(u^*ux_1, x_2, \ldots, x_r) = w_{\mathfrak{a}}(ux_1, ux_2, \ldots, ux_r).$$

Proof. *i*. Note that G_K acts trivially on $\Omega_{\mathfrak{a}}$. Consider the commutative diagram

$$\begin{array}{ccc} \ker(\varphi_{\mathfrak{a}})(K^{\mathrm{s}}) & \xrightarrow[\cong]{} & (A/\mathfrak{a})^r \\ {\scriptstyle w_{\mathfrak{a}}}\downarrow & & \downarrow{\scriptstyle \det} \\ \ker(\psi_{\mathfrak{a}})(K^{\mathrm{s}}) & \xrightarrow[\cong]{} & (A/\mathfrak{a}) \end{array}$$

The action of σ on a division point can be seen as the action of a matrix in $\mathrm{Gl}_r(A/\mathfrak{a})$ via this diagram. Let $\rho : G_K \longrightarrow \mathrm{Gl}_r(A/\mathfrak{a})$ be the corresponding representation. Using the diagram, we see that the action of σ on $w_{\mathfrak{a}}(x_1, \ldots, x_r)$ is given on the right-hand side of the diagram as the action of $\det(\rho(\sigma))$. And thus the Weil pairing commutes with the action of G_K.
ii. Note that x corresponds to a $K^{\mathrm{s}}\{\tau\} \otimes A$-linear map

$$h_x : M(\varphi) \otimes_K K^{\mathrm{s}} \longrightarrow \Omega_{\mathfrak{ab}} \otimes K^{\mathrm{s}},$$

and $bh_x = h_{\varphi_b(x)}$. Because $\varphi_b(x) \in \ker(\varphi_{\mathfrak{a}})(K^{\mathrm{s}})$, it follows that the image of the map $h_{\varphi_b(x)}$ lies in $\Omega_{\mathfrak{a}} \otimes K^{\mathrm{s}}$.
iii. The isogeny u defines an isogeny $\det(u) : \psi \longrightarrow \psi$ because both $\wedge^r M(\varphi)$ and $\wedge^r M(\varphi')$ are isomorphic to $M(\psi)$. As K has general characteristic, $\mathrm{End}_K(\psi) = A$. It follows that $\det(u) = \psi_c$ for some $c \in A$. As the Weil pairing w_c maps $\prod_{i=1}^r \ker(\varphi_c)(\overline{K})$ surjectively to $\ker(\psi_c)$, it follows that $\ker(u) \subset \ker(\varphi_c)(\overline{K})$. Therefore, there exists a dual isogeny $u^* : \varphi' \longrightarrow \varphi'$ with $uu^* = \varphi_c$. For the latter part of *iii* note that:

$$w_{\mathfrak{a}}(ux_1, ux_2, \ldots, ux_r) = \psi_c w_{\mathfrak{a}}(x_1, x_2, \ldots, x_r) = w_{\mathfrak{a}}(u^*ux_1, x_2, \ldots, x_r).$$

□

4.6 Extension to inverse and direct limits

Let $\mathfrak{p} \subset A$ be a prime ideal away from the characteristic of some Drinfeld module φ of rank r over some A-field K. By the compatibility property 4.5.4.*ii* the Weil pairing can be extended to the Drinfeld-Tate module and to the $\mathfrak{p}$-divisible group of φ.
Let $b \in A$ such that $b = \mathfrak{p}^k$ for some $k \in \mathbb{N}$.

Definition 4.6.1. The *Drinfeld-Tate module of* φ *at* $\mathfrak{p}$ is defined to be

$$T_{\mathfrak{p}}(\varphi) := \varprojlim \ker(\varphi_{b^n})(K^{\mathrm{s}}).$$

The $\mathfrak{p}$-*divisible group* $\varphi_{\mathfrak{p}^\infty}$ is by definition

$$\varphi_{\mathfrak{p}^\infty} := \varinjlim \ker(\varphi_{\mathfrak{p}^n}).$$

Remark 4.6.2. The definition of $T_{\mathfrak{p}}$ does not depend on the choice of b. Note that $\ker(\varphi_{b^n})(K^{\mathrm{s}}) \cong (A/b^nA)^r$. We can fix this isomorphism for every n such that it commutes with the transition maps and then

$$T_{\mathfrak{p}} \cong \hat{A}_{\mathfrak{p}}^r \quad \text{with } \hat{A}_{\mathfrak{p}} = \varprojlim A/\mathfrak{p}^n.$$

We write

$$\hat{\Omega}_{\mathfrak{p}} := \varprojlim \Omega_{b^n} \quad \text{and} \quad \Omega_{\mathfrak{p}^\infty} = \varinjlim \Omega_{\mathfrak{p}^n}.$$

Theorem 4.6.3. *Let φ be a Drinfeld module of rank r and let ψ be a Drinfeld module of rank 1 with $M(\psi) \cong \wedge^r M(\varphi)$. Let $\mathfrak{p} \subset A$ be a prime ideal away from the characteristic. The Weil pairing induces a $\mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{s}}/K_{\mathfrak{p}})$-equivariant $\hat{A}_{\mathfrak{p}}$-isomorphism*

$$w_{\mathrm{DT}} : \wedge^r_{\hat{A}_{\mathfrak{p}}} T_{\mathfrak{p}}(\varphi) \longrightarrow T_{\mathfrak{p}}(\psi) \otimes_{\hat{A}_{\mathfrak{p}}} \hat{\Omega}_{\mathfrak{p}}^{\otimes r-1}.$$

Similarly, the Weil pairing induces a $\mathrm{Gal}(K^{\mathrm{s}}/K)$-equivariant A-isomorphism

$$w_\infty : \wedge^r \varphi_{\mathfrak{p}^\infty} \longrightarrow \psi_{\mathfrak{p}^\infty} \otimes \Omega_{\mathfrak{p}^\infty}^{\otimes r-1}.$$

Proof. Let $b \in A$ such that $b = \mathfrak{p}^l$ for some $l \in \mathbb{N}$. For every $n \in \mathbb{N}$ we have a surjective, alternating and A-linear map

$$w_b : \prod_{i=1}^r \ker(\varphi_{b^n})(K^{\mathrm{s}}) \longrightarrow \ker(\psi_{b^n})(K^{\mathrm{s}}) \otimes \Omega_{b^l}^{\otimes r-1}.$$

By the property *ii.* in Proposition 4.5.4 these maps give rise to an $A_{\mathfrak{p}}$-multilinear, alternating map

$$w : \prod_{i=1}^r T_{\mathfrak{p}}(\varphi) \longrightarrow \varprojlim (\ker(\psi_{b^n})(K^{\mathrm{s}}) \otimes \Omega_{b^n}^{\otimes r-1}).$$

As the transition map $\varphi_b : \ker(\varphi_{b^{n+1}})(K^{\mathrm{s}}) \longrightarrow \ker(\varphi_{b^n})(K^{\mathrm{s}})$ is surjective for every n, it is easy to check that the kernels $\ker(w_{b^n})$ form a surjective system. Therefore, w is surjective and thus induces an $\hat{A}_{\mathfrak{p}}$-isomorphism

$$\prod_{i=1}^r \ker(\varphi_{b^n})(K^{\mathrm{s}}) \xrightarrow{\sim} \ker(\psi_{b^n})(K^{\mathrm{s}}) \otimes \Omega_{b^l}^{\otimes r-1};$$

cf. Proposition 10.2 in [2].
Note that $\hat{\Omega}_{\mathfrak{p}}$ is a flat $\hat{A}_{\mathfrak{p}}$-module. By the definition of $T_{\mathfrak{p}}(\psi)$ this gives the following exact sequence of $A_{\mathfrak{p}}$-modules for all $k \in \mathbb{N}$:

$$0 \longrightarrow b^k T_{\mathfrak{p}}(\psi) \otimes \hat{\Omega}_{\mathfrak{p}}^{\otimes r-1} \longrightarrow T_{\mathfrak{p}}(\psi) \otimes \hat{\Omega}_{\mathfrak{p}}^{\otimes r-1} \longrightarrow \ker(\psi_{b^k}) \otimes \hat{\Omega}_{\mathfrak{p}}^{\otimes r-1} \longrightarrow 0.$$

For the latter module in this sequence we have

$$\ker(\psi_{b^k}) \otimes \hat{\Omega}_{\mathfrak{p}}^{\otimes r-1} \cong \ker(\psi_{b^k}) \otimes_A \Omega_{b^k}^{\otimes r-1}.$$

This proves that

$$\varprojlim (\ker(\psi_{b^n}) \otimes \Omega_{b^n}^{\otimes r-1}) \cong T_{\mathfrak{p}}(\psi) \otimes \hat{\Omega}_b^{\otimes r-1} \cong T_{\mathfrak{p}}(\psi) \otimes \hat{\Omega}_{\mathfrak{p}}^{\otimes r-1}.$$

This gives us the isomorphism w_{DT} of the theorem.
To see the isomorphism w_∞, note that the direct limit is exact. So we get an isomorphism

$$\wedge^r \varphi_{\mathfrak{p}^\infty} \xrightarrow{\sim} \varinjlim(\ker(\psi_{b^n})(K^{\mathrm{s}}) \otimes \Omega_{b^n}).$$

Note that

$$\ker(\psi_{b^n})(K^{\mathrm{s}}) \otimes \Omega_{b^n} \cong \ker(\psi_{b^n})(K^{\mathrm{s}}) \otimes_A \Omega_{\mathfrak{p}^\infty}.$$

As the direct limit commutes with tensor products, the isomorphism $w_{\mathfrak{p}^\infty}$ follows. □

4.7 The case $A = \mathbb{F}_q[t]$

Let $A = \mathbb{F}_q[t]$ and let φ be a Drinfeld module over some A-field K. Let $f \in A$ be a non-constant element away from the characteristic. In this section we will compute explicit formulas for the Weil pairing w_f if φ has rank 2. Note that $K\{\tau\}[t] \cong K\{\tau\} \otimes A$.

Proposition 4.7.1. *Let φ be a Drinfeld module over K of rank r given by $\varphi_t = \sum_{i=0}^r a_i \tau^i$. Recall that $a_0 = \gamma(t)$ and $a_r \in K^*$. Let ψ be a Drinfeld module over K of rank 1 given by $\psi_t = \gamma(t) + (-1)^{r-1} a_r \tau$. Then the A-motive $M(\psi)$ associated to ψ is isomorphic as $K\{\tau\}[t]$-module to the exterior product $\wedge^r_{K[t]} M(\varphi)$.*

Proof. $M(\varphi)$ is generated as $K[t]$-module by τ^i for $i = 0, \ldots, r-1$, hence $\wedge^r M(\varphi)$ is generated by $e_0 = \wedge_{i=0}^{r-1} \tau^i$. We see

$$\tau(e_0) = \tau \wedge \ldots \wedge \tau^{r-1} \wedge \frac{1}{a_r}(t - \sum_{0 \le i < r} a_i \tau^i) = (-1)^{r-1} \frac{1}{a_r}(t - \gamma(t)) e_0.$$

Furthermore, we know that $\wedge^r M(\varphi)$ is associated to a Drinfeld module $\psi : A \longrightarrow K\{\tau\}$ of rank 1 given by $\psi_t = \gamma(t) + c\tau$ for some $c \in K^*$. Hence we have, according to the multiplication-by-t induced by ψ, that $\tau(e_0) = \frac{1}{c}(t - \gamma(t)) e_0$. Consequently, $c = (-1)^{r-1} a_r$. This proves the proposition. □

Remark 4.7.2. Note that in [26] it is not very obvious where the definition $\psi_t = \gamma(t) + (-1)^{r-1} a_r \tau$ comes from.

The ψ from Proposition 4.7.1 will be the *standard choice* for the rank 1 Drinfeld module associated to φ.

4.7.1 An explicit example for $r = 2$

From now on assume that φ has rank 2. We will write $f = \sum_{i=0}^n c_i t^i$ and assume that $c_n = 1$. Proposition 4.5.4 gives a pairing

$$w_f : \ker(\varphi_f)(\overline{K}) \times \ker(\varphi_f)(\overline{K}) \longrightarrow \ker(\psi_f)(\overline{K}) \otimes \Omega_f.$$

Recall that $\Omega_f = \frac{1}{f}\mathbb{F}_q[t]dt / \mathbb{F}_q[t]dt$. Let $\omega_0, \ldots, \omega_{n-1}$ be a basis of the $\mathbb{F}_q$-vector space Ω_f such that $\mathrm{Res}_\infty(t^j \omega_i) = \delta_{i,j}$. Consequently, if $a = \sum_{i=0}^{n-1} a_i t^i \in \mathbb{F}_q[t]/(f)$, then $\mathrm{Res}_\infty(\omega_i a) = a_i$.

We take 1 and τ as the generators of $M(\varphi)$ over $K[t]$ and $1 \wedge \tau$ as the generator of $\wedge^2 M(\varphi)$. The isomorphism $\wedge^2 M(\varphi) \cong M(\psi)$ is given by $1 \wedge \tau \mapsto 1$. By the construction in Section 4.5 we have for $x, y \in \ker(\varphi_f)(\overline{K})$ that the map $h_x \wedge h_y$ is determined by

$$h_x(1) \otimes h_y(\tau) - h_x(\tau) \otimes h_y(1).$$

The map $h_x : \overline{M}(\varphi) \longrightarrow \mathrm{Hom}_{\mathbb{F}_q}(A, \overline{K})$ is given by

$$h_x(1) : a \mapsto \varphi_a(x);$$

cf. Proposition 4.4.4. By the isomorphism of Proposition 4.4.1

$$h_x(1) = \sum_{i=0}^{n-1} \varphi_{t^i}(x) \otimes \omega_i \in \overline{K} \otimes \Omega_f.$$

This implies that

$$h_x(\tau) = \sum_{i=0}^{n-1} \varphi_{t^i}(x)^q \otimes \omega_i.$$

We have the same for h_y. This gives us

$$h_x \wedge h_y : 1 \wedge \tau \mapsto \sum_{i,j=0}^{n-1} (\varphi_{t^i}(x)\varphi_{t^j}(y)^q - \varphi_{t^i}(x)^q \varphi_{t^j}(y)) \otimes \omega_i \otimes \omega_j.$$

It follows that $h_x \wedge h_y = \sum_{j=0}^{n-1} h_j \otimes \omega_j$. Here

$$h_j : \overline{M}(\psi) \longrightarrow \overline{K} \otimes \Omega_f$$

is given by

$$h_j : 1 \mapsto \sum_{i=0}^{n-1} (\varphi_{t^i}(x)\varphi_{t^j}(y)^q - \varphi_{t^i}(x)^q \varphi_{t^j}(y)) \otimes \omega_i.$$

And thus h_j corresponds to the element $w_j \in \ker(\psi_f)$ with

$$\psi_{t^i}(w_j) = \varphi_{t^i}(x)\varphi_{t^j}(y)^q - \varphi_{t^i}(x)^q \varphi_{t^j}(y).$$

In particular,

$$w_j = \psi_1(w_j) = x\varphi_{t^j}(y)^q - x^q \varphi_{t^j}(y).$$

These considerations imply the following proposition:

Proposition 4.7.3. *Let $A = \mathbb{F}_q[t]$, and let φ be a Drinfeld module over K of rank 2 given by $\varphi_t = \gamma(t) + a_1\tau + a_2\tau^2$. Let ψ be the rank 1 Drinfeld module given by $\psi_t = \gamma(t) - a_2\tau$. Then the Weil pairing*

$$w_f : \ker(\varphi_f)(\overline{K}) \times \ker(\varphi_f)(\overline{K}) \longrightarrow \ker(\psi_f)(\overline{K}) \otimes \Omega_f$$

is given by the formula

$$w_f : (x, y) \mapsto \sum_{j=0}^{n-1} w_j(x, y) \otimes \omega_j$$

in which

$$w_j(x, y) = x\varphi_{t^j}(y)^q - x^q \varphi_{t^j}(y).$$

For the basis elements ω_i of Ω_f we have

$$\omega_i = \left(\sum_{j=0}^{n-i-1} c_{i+j+1} t^j \right) \cdot \omega_{n-1}.$$

Namely, we have $t\omega_i = \omega_{i-1} - c_i\omega_{n-1}$ for $i = 1, \ldots, n-1$ and $t\omega_0 = -c_0\omega_{n-1}$. The above formula follows by induction.

Proposition 4.7.4. *Choose ω_{n-1} as basis element of the A/fA-module Ω_f. Let*

$$\ker(\psi_f)(\overline{K}) \otimes \Omega_f \xrightarrow{\sim} \ker(\psi_f)(\overline{K}), \quad a \otimes \omega_{n-1} \mapsto a,$$

and let

$$w_j(x, y) = x\varphi_{t^j}(y)^q - x^q\varphi_{t^j}(y),$$

then the Weil pairing w_f of Proposition 4.7.3 induces a pairing

$$w : \ker(\varphi_f)(\overline{K}) \times \ker(\varphi_f)(\overline{K}) \longrightarrow \ker(\psi_f)(\overline{K}),$$

given by

$$w : (x, y) \mapsto \sum_{i=0}^{n-1} \Big(\sum_{j=0}^{n-i-1} c_{i+j+1} t^j \Big) \cdot w_j.$$

Proof. Just note that $\omega_i = (\sum_{j=0}^{n-i-1} c_{i+j+1} t^j) \cdot \omega_{n-1}$ according to the above computation. The result follows from Proposition 4.7.3. □

Example 4.7.5. Let $f = t^2 + c_1 t + c_0$, then

$$w(x, y) = (t + c_1)w_0 + w_1$$

$$= \psi_t(xy^q - x^q y) + c_1(xy^q - x^q y) + x\varphi_t(y)^q - x^q\varphi_t(y)$$
$$= \varphi_t(x)y^q - \varphi_t(x)^q y + c_1(xy^q - x^q y) + x\varphi_t(y)^q - x^q\varphi_t(y).$$