Dieudonné Modules and p-Divisible Groups

Brian Lawrence

September 26, 2014

The notion of ℓ-adic Tate modules, for primes ℓ away from the characteristic of the ground field, is incredibly useful. The analogous notion at the prime p is that of Dieudonné modules. At finite level, Dieudonné modules classify commutative finite group schemes of p-power order over a field of characteristic p. Dieudonné modules can be used to determine the local Brauer invariant of the endomorphism algebra of a simple abelian variety over a finite field at p-adic places of the center.

1 Commutative group schemes of p-power order

Let k be a perfect field of characteristic p. (We are mainly interested in k that is finite or algebraically closed.) We want to classify finite commutative group schemes of p-power order over k.

For motivation, suppose A is an abelian variety of dimension g over k. To make a p-adic analogue of the Tate module, we need to begin with the p-power torsion of A. The p^a-torsion of A, for a a positive integer, is a group scheme of order p^{2ag}. So we are naturally interested in a description of such group schemes.

Another motivation comes from the "connected-étale sequence": via perfectness of k and Galois descent from an algebraic closure, every finite commutative k-group scheme G is uniquely the direct product of connected (equivalently, infinitesimal) and étale parts:

$$G = G^{\mathrm{c}} \times G^{\mathrm{et}}.$$

The étale part is just a finite Galois module by another name. The connected part is considerably more complicated, but it is guaranteed to have p-power order. (See, for example, the Theorem of Section 14.4 of [Wat].)

Finite commutative group schemes of p-power order over k are classified in terms of Dieudonné modules, which we now define. See [Fon] for a detailed exposition and proof, or Section 1.4 of [CCO] for a concise summary. Note that in addition to the relative Frobenius homomorphism $F_{G/k} : G \to G^{(p)}$, Cartier duality provides a variant in the other direction: the (relative) *Verscheibung* homomorphism $V_{G/k} : G^{(p)} \to G$ is defined to be the Cartier dual of the relative

Frobenius of the Cartier dual of G. These satisfy the important relations

$$F_{G/k} \circ V_{G/k} = [p]_{G^{(p)}}, \quad V_{G/k} \circ F_{G/k} = [p]_G.$$

(There is a more robust definition of the relative Verscheibung homomorphism that works for all flat commutative group schemes over $\mathbf{F}_p$-schemes and recovers the notion defined via the crutch of Cartier duality in the finite flat finitely presented case as just described over fields; this is developed in SGA3 and is useful for comparing calculations with finite group schemes and calculations with abelian varieties and beyond.)

Given our perfect field k of characteristic p, let $W = W(k)$ denote the ring of Witt vectors of k (as defined in [Ser]). When k is finite, $W(k)$ is the ring of integers of the unique extension of $\mathbb{Q}_p$ whose residue field is k. Let σ denote the unique automorphism of $W(k)$ lifting the absolute Frobenius $x \mapsto x^p$ on k.

Definition 1.1. *The* Dieudonné ring D_k *over* k *is the associative* $W(k)$*-algebra (non-commutative when* $k \neq \mathbf{F}_p$*) generated by elements* F *and* V *subject to the relations*

$$FV = VF = p$$
$$Fc = \sigma(c)F$$
$$cV = V\sigma(c)$$

for all $c \in W(k)$.

We now state the relationship between Dieudonné modules and finite commutative group schemes of p-power order over k, as recorded in Theorem 1.4.3.2 of [CCO].

Theorem 1.2. *There is an additive anti-equivalence of categories between the category of finite commutative group schemes of* p*-power order over* k *and left* D_k*-modules of finite* W*-length. Writing* $M(G)$ *for the* D_k*-module associated to* G*, we have the following.*

1. *G has order p^r, where r is the W-length of $M(G)$.*
2. *The functor M is functorial in the base field: given a map $f : k \to k'$, we denote by $G_{k'}$ the group scheme over k' obtained by change of base; then we have naturally*
$$M(G_{k'}) \cong M(G) \otimes_{W(k)} W(k').$$
This applies in particular for $f : k \to k$ the absolute Frobenius.
3. *The relative Frobenius morphism $F_{G/k} : G \to G^{(p)}$ corresponds to the linearization*
$$M(G)^{(p)} = \sigma^*(M(G)) \to M(G)$$
of F and the Verschiebung morphism $V_{G/k} : G^{(p)} \to G$ corresponds to the linearization
$$M(G) \to \sigma^*(M(G)) = M(G)^{(p)}$$
of V.

4. *For $K_0 = W[1/p]$, the Cartier dual of G has associated Dieudonné module naturally isomorphic to the $K_0/W(k)$-dual of $M(G)$ equipped with F and V operators that are semi-linear dual to the V and F operators on $M(G)$ respectively.*

5. *The quotient $M(G)/FM(G)$ is naturally isomorphic to the dual of the tangent space to G at the identity.*

2 Elementary Discussion and Examples

To illustrate the correspondence between commutative group schemes of p-power order and their Dieudonné modules, we compute the correspondence explicitly for some groups of small order.

A Dieudonné module, i.e. a left D_k-module, is a W-module equipped with actions of F and V satisfying the relations in Definition 1.1: the F- and V-actions are W-semilinear, they commute with each other, and their composition (in either order) is multiplication by p. We are interested in Dieudonné modules of finite W_k-length.

For k a finite field we know that $W = W(k)$ is the ring of integers of some unramified extension of $\mathbb{Q}_p$; in general, W is a complete discrete valuation ring with residue field k and uniformizer p. (See e.g. Theorem 3 in Section 2.5 of [Ser].) By the classification of modules over a PID, every Dieudonné module with finite W-length has as its underlying W-module a finite direct sum of modules $W/(p^{n_i})$.

For the examples below we assume k is algebraically closed.

2.1 Group Schemes of Order p

We first classify the commutative finite group schemes of order p over k. These are to be in bijection with left D_k-modules whose underlying W-module is of length 1. The only W-module M of length 1 is a line over $W/(p) = k$. Thus, to specify our D_k-module it suffices to give actions of F and V on a basis element e of a k-line such that their product acts as multiplication by p.

Suppose

$$Fe = \alpha e$$

$$Ve = \beta e$$

for some α and β in k. By semilinearity, we have

$$FVe = \alpha\sigma(\beta)e;$$

the requirement that $FV = p$ implies that at least one of α and β must be zero. Conversely, if at least one of α and β is zero, then the condition $FV = VF = p$ is satisfied. So to specify the Dieudonné module with basis we need only give values $\alpha, \beta \in k$, at least one equal to zero.

Under change of basis $e' = \lambda e$ with $\lambda \in k^\times$, by semilinearity α and β become

$$\alpha' = \frac{\sigma(\lambda)}{\lambda}\alpha = \lambda^{p-1}\alpha$$

$$\beta' = \frac{\lambda}{\sigma(\lambda)}\beta = \lambda^{-(p-1)}\beta.$$

Since k is algebraically closed, we may thereby arrange by a change of basis that if one of α and β is nonzero then it is in fact equal to 1. Thus we obtain three possibilities for the pair (α, β): the pair may be $(0,0)$, $(0,1)$, or $(1,0)$. It is clear that these represent three distinct isomorphism classes of D_k-module. To what groups do they correspond?

The relative Frobenius kills a connected order-p group scheme, while its action on an étale group scheme has trivial kernel. Thus, the unique étale group scheme of order p (consisting of p reduced points with the group structure of $\mathbb{Z}/(p)$ corresponds to $(\alpha, \beta) = (1, 0)$.

There are two well-known connected group schemes of order p, namely μ_p and α_p. The first, μ_p, is the kernel of the p-th power map acting on the multiplicative group $\mathbb{G}_m$; specifically, the scheme is $\operatorname{Spec} k[x]/(x^p - 1)$, and the group law is multiplication. The second, α_p, is that subgroup of the additive group $\mathbb{G}_a$ cut out by the equation $x^p = 0$. The relative Frobenius kills both these groups; we need to distinguish them by the action of the Verschiebung. We will use Cartier duality.

The Cartier dual of μ_p is $\mathbf{Z}/(p)$, which is étale, so its Verscheibung is nonzero. Thus, μ_p corresponds to the pair $(0,1)$. On the other hand, one can show that α_p is its own Cartier dual, which is again infinitesimal, so α_p corresponds to $(0,0)$. (Alternatively, via the theory of the Verscheibung homomorphism that makes sense beyon the finite case, one can show that the Verscheibung homomorphism for $\mathbf{G}_a$ vanishes, ultimately because its Frobenius is finite flat, so this gives the conclusion for the subgroup scheme α_p by functoriality.)

2.2 A Group Scheme of Order p^2

We move on to order p^2 killed by p. It is an elementary exercise in semi-linear algebra to show that there are three possibilities for the Dieudonné module of an infinitesimal group scheme with infinitesimal dual (i.e., the module is a k-vector space of dimension 2 on which V and F are each nilpotent). We focus here on deducing the one corresponding to p-torsion $G = E[p]$ of a supersingular elliptic curve E over k. (In particular, we get the non-obvious conclusion that its isomorphism class is independent of the elliptic curve.)

Since G has order p^2, its Dieudonné module $M(G)$ has length 2. Since G is killed by p, by functoriality $M(G)$ is also killed by p. Thus the underlying W-module of $M(G)$ is $(W/(p))^2$. Again, all we need to do now is to determine the actions of F and V on $(W/(p))^2$.

The relative Frobenius on a smooth connected commutative group scheme of dimension 1 is a finite flat morphism of degree p, so its kernel has order

p. Thus F acts on $M(G)$ in such a way that its kernel has W-length 1, and similarly for V since n-torsion in an elliptic curve is self-dual (by Cartier-Nishi duality, via the connection between duality for abelian varieties and for finite commutative group schemes, as discussed in [Mu]). Since G is infinitesimal (as E is supersingular), the action of F on $M(G)$ is nilpotent, so (by some easy semilinear algebra) we can find a k-basis e_1, e_2 of $M(G)$ such that

$$Fe_1 = e_2$$

and

$$Fe_2 = 0.$$

By the relation $VF = p$ we have

$$Ve_2 = VFe_1 = 0,$$

and from $FV = p$ we know that

$$Ve_1 = \alpha e_2$$

for some $\alpha \in k$. Since the kernel of V has W-length 1, the action of V on $M(G)$ is nonzero, so $\alpha \neq 0$. Thus, by scaling the basis element e_1 as above and using that k is *algebraically closed*, we may assume that $\alpha = 1$, and we have determined the Dieudonné module of our group scheme.

3 Dieudonné modules associated to abelian varieties

Let A be an abelian variety of dimension g over a perfect field k of characteristic p. By analogy with the Tate module away from p, we will use Dieudonné theory to define a p-adic module that captures the p-power torsion of A. The *Dieudonné module* of A is defined to be

$$T_pA = \varprojlim M(A[p^n]).$$

This inverse limit is naturally a module over the noncommutative Dieudonné ring D. Additionally we define

$$V_pA = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_pA.$$

As in the ℓ-adic case ($\ell \neq p$) we find by a computation at finite level that T_p is, as a W-module, free of rank $2g$. The Tate theorem holds for T_pA as well: the natural map

$$\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{Hom}_k(A, B) \to \mathrm{Hom}_{D_k}(T_pB, T_pA)$$

is an isomorphism. The proof of injectivity is essentially the same as in the Tate module case: the argument for $\ell \neq p$ carries through with the simplification that

$\mathrm{Hom}(A,B)$ is already known to be finitely generated (by the work with $\ell \neq p$). The proof of surjectivity is more involved: as in the ℓ-adic case, we need to compute the rank of

$$\mathrm{Hom}_D(T_pB, T_pA)$$

and compare it with the rank of the image. For the ℓ-adic Tate module with $\ell \neq p$ this is well-known from the theory of abelian varieties (see [Mu]), and for the Dieudonné module the computation is carried out in Appendix A.1.2 of [CCO].

Recall that the endomorphism algebra $\mathrm{End}^0(A)$ is a finite-dimensional semisisimple $\mathbf{Q}$-algebra (due to Poincaré reducibility, valid over any field). We now assume A is *simple* over k, so its center is a *field*. By Tate's work on the isogeny theorem for abelian varieties over finite fields (see the appendices in [Mu]), one knows that this center is generatred by tge q-Frobenius endomorphism π of A (with $q = \#k$), so it can be written as

$$Z = \mathbb{Q}[\pi]/h(\pi) \subseteq \mathrm{End}^0(A)$$

where h is the minimal polynomial of π acting on A. We wish to determine the invariants of this algebra at places over p.

First, we recall the structure of central simple algebras over local fields (treat in most references on local class field theory). Let K be a local field of characteristic p, and suppose C is a central simple algebra of finite dimension over K. The theory of valuations, well known over local fields, applies to central simple algebras as well, and in particular the valuation on K extends to a valuation on C. One knows that the extension C/K has well-defined inertial and ramification indices e and f, whose product is $\dim_K C$, and that f is the maximal degree of an unramified commutative subfield L of C over K; one also knows by the double centralizer theorem that any maximal commutative subfield of C is of degree a over K, with $a^2 = \dim_K C$. It follows that $e \leq a$, and one can show easily that the ramification degree must also satisfy $f \leq a$. But since $ef = a^2$ we must in fact have $e = f = a$.

The Galois group of L/K is cyclic of order $f = a$, generated by an automorphism σ which restricts to the Frobenius automorphism $x \mapsto x^p$ on the residue field. By Skolem-Noether, the automorphism σ of $L \subseteq C$ is induced by an inner automorphism of C, say conjugation by $c \in C$. Now let v be the valuation on C, normalized so that $v(L) = \mathbb{Z}$, and hence $v(C) = \frac{1}{a}\mathbb{Z}$. By local class field theory, the isomorphism class of C is exactly determined by the class

$$v(c) \in (\frac{1}{a}\mathbb{Z})/\mathbb{Z}.$$

This is the *Brauer invariant* of the central simple K-algebra C.

Now return to the problem of finding the invariants at p-adic places for the central simple Z-algebra algebra $\mathrm{End}^0 A$ with A simple over a finite field k. By contravariance of the Dieudonné functor, the algebra $\mathbf{Q}_p \otimes_{\mathbf{Q}} \mathrm{End}^0(A)$ over $Z_p = \prod_{v|p} Z_v$ is the *opposite* algebra of

$$\mathrm{Hom}_{D[1/p]}(V_pA, V_pA).$$

This is an algebra over the associative polynomial ring $D_k[1/p] = K_0[F]$ where F acts on $K_0 = W[1/p]$ by

$$Fc = \sigma(c)F.$$

Now if we set

$$a = [K_0 : \mathbb{Q}_p] = [k : \mathbb{F}_p],$$

then the conjugation action of F^a on K_0 is trivial, so F^a is in the center of $D[1/p]$. In fact, one sees by an explicit calculation that every element of $D[1/p]$ has a unique expression of the form

$$\sum a_i F^i$$

with $a_i \in K_0$. Using this normal form one sees that the center of $D[1/p]$ is exactly $\mathbb{Q}_p[F^a]$, a commutative polynomial ring in one variable.

In fact we can reduce the whole situation to finite $\mathbb{Q}_p$-algebras. The relative Frobenius π acting on the abelian variety A satisfies $h(\pi) = 0$, and this relative Frobenius corresponds via the Dieudonné module functor to F^a. Hence, the action of F^a on the Dieudonné module V_pA satisfies

$$h(F^a) = 0.$$

Thus V_pA is in fact a module over the associative ring

$$C = K_0[F]/h(F^a),$$

whose center is

$$\mathbb{Q}_p[F^a]/h(F^a) = Z_p := \prod_{v|p} Z_v.$$

Thus, we seek to determine

$$\mathrm{End}_C(V_pA)$$

(or rather, to determines is central simple factors over the p-adic fields Z_v).

Since a morphism of C-modules is a fortiori a morphism of Z_p-modules, the endomorphism algebra of A is a subalgebra of the matrix algebra

$$\mathrm{End}_{Z_p}(V_pA);$$

in fact, it is exactly that subalgebra consisting of matrices (i.e. homomorphisms) which commute with the action of C. Thus, it is the centralizer of C in the matrix algebra.

Recall again the double centralizer theorem for finite-dimensional associated algebras over a commutative field, which states that if, in a simple algebra A, the subalgebra A_1 is the centralizer of the subalgebra A_2, then also A_2 is the centralizer of A_1. If in fact the algebra A a matrix algebra, then one might expect this duality to extend to some relationship between the invariants of A_1 and A_2. In fact, one can show that the invariants of A_1 are exactly the negatives of the invariants of A_2. The proof is not difficult. See Remark A.1.2.4 of [CCO]

for the local case; the same argument applies verbatim for the semilocal case, which we apply here.

Thus, it is sufficient to find the invariants of C at every place of Z_p. Note that Z_p is in general a product of local fields, indexed by the irreducible factors of h in $\mathbb{Q}_p$. Write

$$h = \prod_v h_v$$

as the product of polynomials irreducible over $\mathbb{Q}_p$. (There can be no repeated factors due to separability considerations.) So we have corresponding decompositions

$$Z_p = \prod_v Z_v$$

and

$$C = \prod_v C_v.$$

Each C_v is central simple over Z_v, hence isomorphic to a matrix algebra over a central division ring over Z_v. Recall that

$$C_v = K_0[F]/h_v(F^a)$$

and

$$Z_v = \mathbb{Q}_p[F^a]/h_v(F^a).$$

To find the invariant of C_v over Z_v, we need to find the central division ring over which C_v is a matrix algebra; then find its maximal unramified commutative subfield, and finally an element of $C_v^\times$ whose conjugation induces the Frobenius on that subfield. For the full details of the calculation below, see Theorem A.1.2.3 of [CCO].

Let f denote the degree of the maximal unramified extension of $\mathbb{Q}_p$ inside Z_v. Let Z_0 be the maximal unramified extension of $\mathbb{Q}_p$ that embeds into both Z_v and K_0. Defining $g = \gcd(f, a)$, we have

$$[Z_0 : \mathbb{Q}_p] = g.$$

Choose embeddings of Z_0 into K_0 and Z_v, and let $K_0 Z_v$ denote the tensor product

$$K_0 \otimes_{Z_0} Z_v.$$

This tensor product is easily seen to be a field itself, the compositum of K_0 and Z_v taken in some algebraic closure; the extension $K_0 Z_v / Z_v$ in unramified with degree a/g. Let Δ be the noncommutative algebra over $K_0 Z_v$ given by

$$\Delta = K_0 Z_v[F'],$$

up to the relations

$$F'^{a/g} = \pi \in Z$$

and

$$F'x' = \sigma'(x')F',$$

where σ' is the Z_0-automorphism of K_0Z_v induced by the identity on Z_v and σ^g on K_0. It is shown in [CCO] that C_v is a matrix algebra over Δ. It then follows by an elementary calculation that the invariant of C_v over Z_v is

$$\frac{1}{a/g}v(\pi^{f/g}) = \frac{v(\pi)}{v(q)}[Z_v : \mathbb{Q}_p].$$

References

[CCO] C-L. Chai, B. Conrad, and F. Oort, *Complex Multiplication and Lifting Problems*, American Mathematical Society, 2014.

[Fon] J.-M. Fontaine, *Groupes p-divisibles sur les corpes locaux*, Société Mathématique de France, in Astérisque, 47-48, 1977.

[Mu] D. Mumford, *Abelian Varieties*, Hindustan Book Agency, New Delhi, 2012.

[Ser] J.-P. Serre, *Corps Locaux*, Hermann, Paris, 1968.

[Wat] W. C. Waterhouse, *Introduction to Affine Group Schemes*, Springer, 1979.