

open.michigan

Author(s): Andrew Snowden

License: Unless otherwise noted, this material is made available under the terms of the **Creative Commons Attribution 3.0 License**: <http://creativecommons.org/licenses/by/3.0/>


We have reviewed this material in accordance with U.S. Copyright Law **and have tried to maximize your ability to use, share, and adapt it.** The citation key on the following slide provides information about how you may share and adapt this material.

Copyright holders of content included in this material should contact open.michigan@umich.edu with any questions, corrections, or clarification regarding the use of content.

For more information about **how to cite** these materials visit <http://open.umich.edu/education/about/terms-of-use>.

Any **medical information** in this material is intended to inform and educate and is **not a tool for self-diagnosis** or a replacement for medical evaluation, advice, diagnosis or treatment by a healthcare professional. Please speak to your physician if you have questions about your medical condition.

Viewer discretion is advised: Some medical content is graphic and may not be suitable for all viewers.

 UNIVERSITY OF MICHIGAN



Attribution Key

for more information see: <http://open.umich.edu/wiki/AttributionPolicy>

Use + Share + Adapt

{ Content the copyright holder, author, or law permits you to use, share and adapt. }

-  **Public Domain – Government:** Works that are produced by the U.S. Government. (17 USC § 105)
-  **Public Domain – Expired:** Works that are no longer protected due to an expired copyright term.
-  **Public Domain – Self Dedicated:** Works that a copyright holder has dedicated to the public domain.
-  **Creative Commons – Zero Waiver**
-  **Creative Commons – Attribution License**
-  **Creative Commons – Attribution Share Alike License**
-  **Creative Commons – Attribution Noncommercial License**
-  **Creative Commons – Attribution Noncommercial Share Alike License**
-  **GNU – Free Documentation License**

Make Your Own Assessment

{ Content Open.Michigan believes can be used, shared, and adapted because it is ineligible for copyright. }

-  **Public Domain – Ineligible:** Works that are ineligible for copyright protection in the U.S. (17 USC § 102(b)) *laws in your jurisdiction may differ

{ Content Open.Michigan has used under a Fair Use determination. }

-  **Fair Use:** Use of works that is determined to be Fair consistent with the U.S. Copyright Act. (17 USC § 107) *laws in your jurisdiction may differ

Our determination **DOES NOT** mean that all uses of this 3rd-party content are Fair Uses and we **DO NOT** guarantee that your use of the content is Fair.

To use this content you should **do your own independent analysis** to determine whether or not your use will be Fair.

Lecture 6: Group schemes 2

This is the second lecture on group schemes, and is divided into three sections. In the first, I discuss Cartier duality and give the basic examples. In the second, I go deeper into the theory over finite fields, giving the classification of height 1 group schemes, and using it to classify the simple group schemes over an algebraically closed field. I also briefly discuss Dieudonné modules. In the third section, I apply the theory of group schemes to the study of abelian varieties. First, I relate abelian variety duality and Cartier duality. Then I characterize ordinary and supersingular elliptic curves using their p -torsion. Finally, I give a tight bound on the p -torsion of an abelian variety.

1 Cartier duality

Let $G = \text{Spec}(A)$ be a finite commutative group scheme over the field k . Let A^* be the k -linear dual of A . Since the Hopf algebra axioms are completely symmetric with respect to reversing arrows, A^* is still a Hopf algebra, and, of course, both commutative and cocommutative. We let $G^\vee = \text{Spec}(A^*)$, a finite commutative group scheme over k . We call G^\vee the Cartier dual of G . Obviously, G and G^\vee have the same order and the natural map $(G^\vee)^\vee \rightarrow G$ is an isomorphism.

We now describe the functor of points of G^\vee . Let R be a k -algebra. Giving a k -algebra homomorphism $A^* \rightarrow R$ is the same as giving an R -algebra homomorphism $A_R^* \rightarrow R$, where $(-)_R = - \otimes R$. Taking R -linear duals, this is the same as giving a morphism R -coalgebras $R \rightarrow A_R$ of R -coalgebras. This, in turn, is the same as giving an element x of A_R such that $\Delta(x) = x \otimes x$ and $\eta(x) = 1$, where Δ is the comultiplication and η is the counit on A_R . (The bijection takes a map $R \rightarrow A_R$ to the image of $1 \in R$. The condition on x is exactly the condition needed to make the map one of coalgebras.) We note that one of the Hopf algebra axioms is $m(\text{id} \otimes i)\Delta = \eta$, and so $xi(x) = 1$, i.e., x is a unit of A_R . But giving a unit of A_R is the same as giving a map $R[t, t^{-1}] \rightarrow A_R$, and the condition $\Delta(x) = x \otimes x$ exactly makes this map one of Hopf algebras! We have thus shown:

Proposition 1. *There is a natural bijection $G^\vee(R) = \text{Hom}(G_R, (\mathbf{G}_m)_R)$. Equivalently, $G^\vee = \underline{\text{Hom}}(G, \mathbf{G}_m)$ as sheaves on the big fppf site.*

In words: the R -points of G^\vee are the characters of G defined over R .

Example 2. Suppose $G = \mathbf{Z}/r\mathbf{Z}$. Then $A = \prod_{i \in \mathbf{Z}/r\mathbf{Z}} ke_i$, with multiplication $e_i e_j = \delta_{ij} e_i$ and comultiplication $\Delta(e_n) = \sum_{i+j=n} e_i e_j$. Let e_i^* be the dual basis of A^* . The element $\Delta(e_n^*)$ is the linear functional $A \otimes A \rightarrow A \rightarrow k$, where the first map is multiplication and the second is e_n^* . Given the formula for multiplication, we see that $\Delta(e_n^*)(e_i \otimes e_j)$ is 1 if $i = j = n$ and 0 otherwise. Thus $\Delta(e_n^*) = e_n^* \otimes e_n^*$. The product $e_i^* e_j^*$ is the linear functional $A \rightarrow A \otimes A \rightarrow k$, where the first map is comultiplication and the second is $e_i^* \otimes e_j^*$. We thus see that $(e_i^* e_j^*)(e_n)$ is 1 if $i + j = n$ and 0 otherwise. Thus $e_i^* e_j^* = e_{i+j}^*$. It follows that $e_i^* \mapsto t^i$ defines an isomorphism of Hopf algebras $A^* \rightarrow k[t]/(t^r - 1)$. Thus $(\mathbf{Z}/r\mathbf{Z})^\vee = \mu_r$. (This can be seen more conceptually using the description of the functor of points of G^\vee .) Of course, this gives $\mu_r^\vee = \mathbf{Z}/r\mathbf{Z}$ as well. \square

Example 3. Let's now consider the case $G = \alpha_p$, where k has characteristic p . So $A = k[t]/(t^p)$. Let $e_i = t^i$ for $0 \leq i < p$. We have $e_i e_j = e_{i+j}$ for $i + j < p$ and $e_i e_j = 0$ for $i + j \geq p$. We have

These are notes for Math 679, taught in the Fall 2013 semester at the University of Michigan by Andrew Snowden.

$\Delta(t) = t \otimes 1 + 1 \otimes t$. Since Δ is a ring homomorphism,

$$\Delta(e_n) = (t \otimes 1 + 1 \otimes t)^n = \sum_{i+j=n} \binom{n}{i} t^i \otimes t^j.$$

Now, let e_i^* be the dual basis of A^* . Then $\Delta(e_n^*)(e_i \otimes e_j)$ is equal to 1 if $i + j = n$ and 0 otherwise. Thus $\Delta(e_n^*) = \sum_{i+j=n} e_i^* \otimes e_j^*$. We have that $(e_i^* e_j^*)(e_n)$ is equal to $\binom{n}{i}$ if $n = i + j$ and 0 otherwise; thus $e_i^* e_j^* = \binom{i+j}{i} e_{i+j}^*$ if $i + j < n$, and 0 otherwise. It follows that $e_i^* \mapsto t^i/i!$ defines an isomorphism of Hopf algebras $A^* \rightarrow A$. Thus $\alpha_p^\vee = \alpha_p$. \square

We have already seen two fundamental types of finite commutative group schemes: the local (i.e., connected) ones, and the étale ones. Cartier duality allows us to further refine these types by considering the type of the dual as well. We thus have local–local, local–étale, étale–local, and étale–étale group schemes (the first refers to the type of G , the second to G^\vee). Examples (in characteristic p) of these are α_p , μ_p , $\mathbf{Z}/p\mathbf{Z}$, and $\mathbf{Z}/\ell\mathbf{Z}$ (for $\ell \neq p$). In characteristic 0, we only have étale–étale. Over a perfect field, every finite group scheme canonically decomposes into a product $G_{ll} \times G_{le} \times G_{el} \times G_{ee}$, where G_{ll} is local–local, etc.

2 Group schemes over finite fields

2.1 Frobenius and Verschiebung

Let $G = \text{Spec}(A)$. We have already seen the Frobenius map $F_p: G \rightarrow G^{(p)}$, though we have not carefully defined it. Let σ be the p th power map (on any ring of characteristic p), the so-called absolute Frobenius. Then $\sigma(\alpha x) = \sigma(\alpha)\sigma(x)$ for $\alpha \in k$ and $x \in A$, and so $\sigma: A \rightarrow A$ is not a homomorphism of k -algebras. Let $A^{(p)} = k \otimes_{k, \sigma} A$, i.e., $\alpha \otimes x = 1 \otimes \alpha^p x$ in $A^{(p)}$. Then the map $A^{(p)} \rightarrow A$ given by $\alpha \otimes x \mapsto \alpha x^p$ is a well-defined map of k -algebras; this is F_p . We define F_q , for $q = p^r$, by using σ^r in place of σ .

Proposition 4. *G is étale if and only if F_p is an isomorphism, and connected if and only if $F_q = 0$ for some $q = p^r$.*

Proof. Suppose $G = \text{Spec}(A)$ is connected. Then clearly $F_q = 0$ on A for some A , since the maximal ideal of A is nilpotent. If F_p is an isomorphism on G then F_p is an isomorphism on G° as well, and so $G^\circ = 0$, i.e., G is étale. Now, F_q induces an isomorphism $G(\bar{k}) \rightarrow G^{(q)}(\bar{k})$. Thus if $F_q = 0$ for some q then $G(\bar{k}) = 0$, i.e., $G^{\text{ét}} = 0$, and so G is connected.

The dual of the Frobenius map on G^\vee is a map $V_p: G^{(p)} \rightarrow G$, called the Verschiebung map. It is a homomorphism, and one can show $F_p V_p = V_p F_p = [p]$. Obviously, V_p is an isomorphism if and only if G^\vee is étale and $V_q = 0$ for some q if and only if $G^\vee = 0$. \square

2.2 Classification in height 1

Let $G = \text{Spec}(A)$ be a finite commutative connected group scheme over k , which we assume to have characteristic p . Write $L(G)$ for the Lie algebra of G , which is naturally the dual of the k -vector space I/I^2 , where I is the maximal ideal of A .

We say that a derivation $D: A \rightarrow A$ is invariant if $\Delta D = (D \otimes 1)\Delta$, where Δ is comultiplication. Given $v \in L(G)$, thought of as an element of $(I/I^2)^*$, let D_v be the composition

$$A \rightarrow A \otimes A \rightarrow A \otimes I/I^2 \rightarrow A$$

where the first map is Δ , the second is $\text{id} \otimes \pi$, where π is projection onto I/I^2 (as discussed previously), and the final map is $\text{id} \otimes v$. Then one easily verifies that $v \mapsto D_v$ is an isomorphism of $L(G)$ with the space of invariant derivations.

Let D be a derivation of A . Let D^n be the n -fold iterate of D on A . Since $D^n(xy)$ is computed using the binomial theorem, it follows that D^p satisfies the Leibniz rule, and is therefore a derivation. It's easy to verify that if D is invariant then so is D^p , and so $D \mapsto D^p$ induces a map $L(G) \rightarrow L(G)$ which we denote by F . Note that $F(av) = a^p F(v)$ for $a \in k$.

We define an F -module over k to be a k -vector space L equipped with an additive map F satisfying $F(av) = a^p F(v)$ for $a \in k$ and $v \in V$. Thus $L(G)$ is an example of an F -module.

Example 5. Suppose $G = \alpha_p = \text{Spec}(k[t]/(t^p))$. One easily verifies that $D = \frac{d}{dt}$ is an invariant differential and spans $L(G)$. We have $D^p = 0$ since $D^p(t) = 0$ and t generates. Thus $L(G) = k$, with $F = 0$. \square

Example 6. Suppose $G = \mu_p = \text{Spec}(k[t]/(t^p - 1))$. One easily verifies that $D = t \frac{d}{dt}$ is an invariant differential and spans $L(G)$. We have $D^p = D$ since $D^p(t) = t = D(t)$. Thus $L(G) = k$, with F being the p th power map. \square

It is clear that G is not determined from $L(G)$, for two reasons: (1) in the étale case, $L(G) = 0$; and (2) a non-isomorphism of groups can induce an isomorphism on tangent spaces, e.g., the map $\mu_{p^2} \rightarrow \mu_p$. We say that G has height 1 if it is connected and killed by Frobenius. This hypothesis eliminates the two obvious obstructions just mentioned. In fact:

Theorem 7. *The functor $G \mapsto L(G)$ is an equivalence between the category finite commutative height 1 group schemes over k and the category of finite dimensional F -modules.*

Proof. Let L be a finite dimensional F -module. Let A be the quotient of $\text{Sym}(L)$ by the ideal generated by $x^p - F(x)$ for $x \in L$. Then A is obviously a finite dimensional k -algebra. One verifies that $x \mapsto x \otimes 1 + 1 \otimes x$ for $x \in L$ descends to a comultiplication on A , and that A is naturally a Hopf algebra. The inverse functor takes L to $\text{Spec}(A^*)$, the Cartier dual of $\text{Spec}(A)$. For details, see Mumfords "Abelian varieties" ([MR0282985](#)), section 14. \square

2.3 Consequences of classification

Theorem 8. *Suppose k is algebraically closed. Then $L(\alpha_p)$ and $L(\mu_p)$ are the only simple objects in the category of finite dimensional F -modules (up to isomorphism).*

Proof. Let L be an F -module. If there exists $x \in L$ non-zero such that $F(x) = 0$ then kx is a non-trivial submodule of L isomorphic to $L(\alpha_p)$. Now suppose $F(x) \neq 0$ for all $x \neq 0$; we must show L contains $L(\mu_p)$.

Let e_1, \dots, e_n be a basis of L . Identify an element $x = \sum a_i e_i$ of L with the vector $v = (a_i)$. Write $F(e_i) = \sum_j C_{ij} e_j$ with $C_{ij} \in k$, and let C be the matrix (C_{ij}) . Then if x corresponds to the vector $v = (a_i)$, we see that $F(x)$ corresponds to the vector Cv^p , where $v^p = (a_i^p)$. From this we see that C is invertible: indeed, if $Cv = 0$ then $F(x) = 0$, where x corresponds to the vector $v^{1/p}$ (which exists since k is closed).

We thus see that F -fixed vectors of L correspond to solutions to the equation $v^p = C^{-1}v$. Let $R = k[x_i]/(x_i^p - \sum_j C_{ij}^{-1} x_j)$. Then F -fixed vectors exactly coincide with k -points of $\text{Spec}(R)$. Note that $\Omega_{R/k}^1 = 0$ and R has dimension p^n over k . It follows that $\text{Spec}(R)$ is finite étale over k , and thus has exactly p^n k -points, since k is closed. We have therefore shown that $\dim_{\mathbf{F}_p}(L^{F=1}) = \dim_k(L)$. It is easy to see that the natural map $L^{F=1} \otimes_{\mathbf{F}_p} k \rightarrow L$ is injective (apply F to a hypothetical minimal linear dependence), which implies that $L \cong L(\mu_p)^{\oplus n}$. \square

Theorem 9. *Suppose k is algebraically closed. Then the simple finite commutative group schemes over k are $\mathbf{Z}/\ell\mathbf{Z}$ ($\ell \neq p$ prime), $\mathbf{Z}/p\mathbf{Z}$, μ_p , and α_p .*

Proof. A simple group scheme is either connected or étale. The simple étale group schemes are obviously $\mathbf{Z}/\ell\mathbf{Z}$ and $\mathbf{Z}/p\mathbf{Z}$. A simple connected group scheme is killed by Frobenius, and therefore of height 1, and therefore μ_p or α_p . \square

Corollary 10. *Let G be a finite commutative group scheme of order n . Then $[n] = 0$ on G . In particular, for any $x \in G(R)$ we have $nx = 0$.*

Proof. This can be verified over \bar{k} . If it is true for the outer groups in a short exact sequence, then it's true for the middle group. It therefore suffices to verify the case of simple group schemes, which follows easily from the classification. \square

Remark 11. An F -isomodule is an F -module with F injective. Then the category of F -isomodules is equivalent to the category of groups G such that $G_{\bar{k}}$ is isomorphic to μ_p^n for some n . But, by Cartier duality, this category is equivalent to the category of groups G such that $G_{\bar{k}}$ is isomorphic to $(\mathbf{Z}/p\mathbf{Z})^n$, which is the same to say that G is étale and killed by p . But we know that this category is equivalent to the category of \mathbf{F}_p -representations of G_k . We find that we have an equivalence of categories

$$\{F\text{-isomodules}\} \cong \{\mathbf{F}_p\text{-representations of } G_k\}.$$

This equivalence can be described explicitly using the "kernel object" k^s , which has a compatible Galois action and F -module structure. Precisely, an F -isomodule M is taken to $(M \otimes k^s)^{F=1}$ while a Galois representation V is taken to $(V \otimes k^s)^{G_k}$. Fontaine generalized this to a description of the category of $\mathbf{Z}_p[G_k]$ -modules. \square

2.4 Dieudonné theory

It would of course be desirable to remove the height 1 restriction in the above classification of group schemes. This is exactly what Dieudonné theory does, assuming k is perfect. Let $W = W(k)$ be the Witt vectors of k . If $k = \mathbf{F}_q$, which is the most common case, W is the ring of integers in the unramified extension of \mathbf{Q}_p with residue field k . The absolute Frobenius on k induces an automorphism φ of W . A Dieudonné module is a W -module D equipped with two additive maps $F, V: D \rightarrow D$ satisfying $F(ax) = \varphi(a)x$, $V(ax) = \varphi^{-1}(a)x$, and $FV = VF = p$. The main theorem is then:

Theorem 12. *Suppose k is perfect. The category of finite commutative group schemes over k of p -power order is equivalent to the category of Dieudonné modules of finite length over W .*

Write $D(G)$ for the Dieudonné module associated to G . The functor D has several nice properties in addition to being an equivalence:

- D is an exact functor.
- The group G is killed by p^n if and only if $D(G)$ is.
- The order of G is equal to p^r , where r is the length of $D(G)$ as a W -module.
- G is connected if and only if F is nilpotent on $D(G)$, and étale if and only if F is an isomorphism on $D(G)$.

- $D(G^\vee)$ is naturally the dual of $D(G)$, where the dual of a Dieudonné module M is the W -module $\mathrm{Hom}_W(M, K/W)$ with F and V defined by $(Ff)(x) = \varphi(f(Vx))$ and $(Vf)(x) = \varphi^{-1}(f(Fx))$. Here K is the field of fractions of W .
- If G has height 1 then $D(G)^\vee = L(G)$ (and $V = 0$).

3 Applications to abelian varieties

3.1 Duality of abelian varieties revisited

We previously showed that if $f: X \rightarrow Y$ is an isogeny of complex tori then $\ker(f)$ and $\ker(f^\vee)$ are naturally Pontryagin dual groups. We now generalize this to arbitrary fields:

Proposition 13. *Let $f: A \rightarrow B$ be an isogeny of abelian varieties. Then $\ker(f^\vee)$ is naturally Cartier dual to $\ker(f)^\vee$.*

Proof. Put $G = \ker(f)$. Applying $\underline{\mathrm{Hom}}(-, \mathbf{G}_m)$ to the short exact sequence of fppf sheaves

$$0 \rightarrow G \rightarrow A \rightarrow B \rightarrow 0,$$

we obtain a long exact sequence

$$0 \rightarrow \underline{\mathrm{Hom}}(B, \mathbf{G}_m) \rightarrow \underline{\mathrm{Hom}}(A, \mathbf{G}_m) \rightarrow \underline{\mathrm{Hom}}(G, \mathbf{G}_m) \rightarrow \underline{\mathrm{Ext}}^1(B, \mathbf{G}_m) \rightarrow \underline{\mathrm{Ext}}^1(A, \mathbf{G}_m).$$

There are no maps from an abelian variety to \mathbf{G}_m (since abelian varieties are proper and \mathbf{G}_m is affine), so the first two groups vanish. We've seen that $\underline{\mathrm{Hom}}(-, \mathbf{G}_m)$ is Cartier duality for finite commutative group schemes and $\underline{\mathrm{Ext}}^1(-, \mathbf{G}_m)$ is duality for abelian varieties. Thus $G^\vee = \ker(f^\vee)$. A more elementary proof is given in section 15 of Mumfords "Abelian varieties" ([MR0282985](#)). \square

Corollary 14. *Let A be an abelian variety. Then $A[n]$ and $A^\vee[n]$ are Cartier dual. In particular, there is a canonical pairing $A[n] \times A^\vee[n] \rightarrow \mu_n$, the Weil pairing.*

3.2 The p -torsion of an elliptic curve

Let E be an elliptic curve over k , which we assume to be algebraically closed of characteristic p . Then $G = E[p]$ is a finite commutative group scheme over k of order p^2 . We know a lot about such group schemes, so it's reasonable to think we could describe G fairly precisely.

We know two things right off the bat. First, G is not étale. And second, since E is self-dual (as an abelian variety), G is self-dual (in the sense of Cartier duality).

First suppose that E is ordinary. Then $G(k) \neq 0$, and so G^{et} is non-zero. Thus $G = G^\circ \times G^{\mathrm{et}}$, and both factors have order p . By the classification of étale groups, $G^{\mathrm{et}} = \mathbf{Z}/p\mathbf{Z}$. Since G is self-dual, G° is necessarily the dual of G^{et} , so $G^\circ = \mu_p$. We thus find $G = \mu_p \times \mathbf{Z}/p\mathbf{Z}$.

Now suppose that E is supersingular. Then $G(k) = 0$, and so $G^{\mathrm{et}} = 0$. It follows that G is local, and thus local–local since it is self-dual. Since the only simple local–local group is α_p , we must have an extension of the form

$$0 \rightarrow \alpha_p \rightarrow G \rightarrow \alpha_p \rightarrow 0.$$

This extension cannot be split, for then $G = \alpha_p \oplus \alpha_p$, which has a two-dimensional tangent space, but the tangent space of G agrees with that of E , and has dimension 1. We also cannot have $G = \alpha_{p^2}$, since this group is not self-dual (it has $V = 0$ but $F \neq 0$); of course, we cannot have

$G = \alpha_{p^2}^\vee$ either. In fact, up to isomorphism, there are only four self-extensions of α_p (as can easily be seen using Dieudonné theory), and G is the one we haven't named! One can describe G as the sum of α_{p^2} and its dual in $\text{Ext}^1(\alpha_p, \alpha_p)$, and one can also explicitly describe the Dieudonné module $D(G)$.

3.3 The p -torsion of an abelian variety

Let A be an abelian variety over k , assumed to be of characteristic p . Write $A[p] = G_1 \oplus G_2 \oplus G_3$ where G_1 is étale, G_2 is local-étale, and G_3 is local-local. Write $\#G_1 = p^r$, $\#G_2 = p^s$, and $\#G_3 = p^t$.

Proposition 15. *The numbers r , s , and t are isogeny invariant.*

Proof. Decompose $A[p^n]$ as $G_{1,n} \oplus G_{2,n} \oplus G_{3,n}$ as above. Note that $A[p^n]$ is a successive extension of $A[p]$'s; it follows that $G_{i,n}$ is a successive extension of G_i 's. In particular, $\#G_{1,n} = p^{nr}$, $\#G_{2,n} = p^{ns}$, and $\#G_{3,n} = p^{nt}$.

Now suppose that $A \rightarrow A'$ is an isogeny of degree d . Then, in the obvious notation, the kernel of $G_{1,n} \rightarrow G'_{1,n}$ has order at most d . Clearly, for $n \gg 0$, this is only possible if $r \leq r'$. Since “isogenous” is an equivalence relation, there exists an isogeny $A' \rightarrow A$, and so $r' \leq r$ as well. Thus $r = r'$. The equality of the other invariants is similar. \square

Proposition 16. *We have $r = s$ and $t = 2g - 2r$, where $g = \dim(A)$.*

Proof. By duality, we have $r(A) = s(A^\vee)$. But A and A^\vee are isogenous (via a polarization), and so $r = s$. The formula for t follows, since $A[p]$ has order p^{2g} . \square

Corollary 17. *We have $A[p](\bar{k}) = (\mathbf{Z}/p\mathbf{Z})^r$ with $r \leq g$.*

Proof. Since $r = s$, we have $2r = r + s \leq 2g$, and so $r \leq g$. \square

3.4 The Dieudonné module as a p -adic Tate module

Let A be an abelian variety of dimension g over k , a perfect field of characteristic p . Then $T_p(A)$, the p -adic Tate module of A , has rank at most g , and could even be 0; it is therefore very much unlike the ℓ -adic Tate modules of A . Define the Dieudonné module of A , denoted $D(A)$, to be the inverse limit of those of the $A[p^n]$. Then $D(A)$ is a free W -module of rank $2g$ equipped with a semi-linear map F , and thus looks more like the ℓ -adic Tate module. (Note: V is not needed since $VF = p$.)

Now suppose $k = \mathbf{F}_q$ with $q = p^r$. Let $F' = F^r$. Then F' is a W -linear automorphism of $D(A)$. This looks even more like the ℓ -adic Tate module! In fact, the analogy is very good: the eigenvalues of F' are the same as the eigenvalues of Frobenius on the ℓ -adic Tate module.