ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 31, Number 3, Fall 2001

WITT SUBGROUPS AND CYCLIC DIEUDONNÉ MODULES KILLED BY p

ALAN KOCH

ABSTRACT. Let k be a perfect field of characteristic $p > 0$. We obtain a complete classification of cyclic Dieudonné modules killed by p, which in turn gives us a complete classification of Witt subgroups killed by p. Finally, we construct an explicit formula for the number of Witt subgroups of a given dimension over a finite field k and use this to disprove a conjecture of Lubin.

Let k be a perfect field of characteristic $p > 0$. Let G be an affine finite commutative k-group scheme. It is well known (e.g., [**11**]) that G splits into the direct sum of G' and G'', where G' is the maximal connected unipotent subgroup of G. While G'' can be classified using descent (over an algebraically closed field it decomposes into various roots of unity functors and constant group schemes of dimension p^r for various r), the classification of connected unipotent group schemes is more difficult.

To fully understand this subcategory of group schemes, we must introduce Dieudonné modules. Dieudonné modules are a class of modules (over a certain ring E) which correspond to these group schemes. It is for this reason that we are interested in studying Dieudonné modules. In this paper we will use Dieudonné modules to obtain a complete classification of Witt subgroups that are killed by p. A Witt subgroup refers to a finite subgroup scheme of any finite-length Witt vector group scheme. In the first section we describe the basic correspondence between group schemes and Dieudonné modules; we give additional properties for the Dieudonné modules that correspond to Witt subgroups killed by p, namely, the modules that are killed by p and are cyclic. In Sections 2 and 3 we classify all of the modules that correspond to Witt subgroups; we see that they can be parameterized by triples (l, m, η), where l and m are positive integers and η is an

1991 AMS *Mathematics Subject Classification.* 14L20.
Received by the editors on August 9, 1999, and in revised form on September 1, 2000.

element from a certain quotient group of $k^\times$. Finally, in the last section we explicitly describe these Witt subgroups, provide a formula for the total number of Witt subgroups killed by p when k is finite, and use these results to disprove a conjecture made by Lubin concerning the number of cyclic Dieudonné modules.

It is the hope that this paper will bring insight to Dieudonné module theory. Once the cyclic modules killed by p are classified, perhaps it can be extended to cyclic modules killed by p^h for some h, or even more general modules. In addition, the results provided here will be useful in classifying group schemes over rings of Witt vectors (which are unramified extensions of $\mathbf{Z}_p$) as in [**8**]; also the techniques used in Section 3 will be applied to classifying Hopf algebras which are generated as algebras by a single element [**9**]. While efforts have been made in [**1**] and [**2**] to discuss group schemes killed by p (not necessarily cyclic) over k (and $W(k)$), the results here are more explicit in both the Dieudonné module description and the group scheme description.

Throughout this paper we shall work over a fixed prime $p > 0$, and all group schemes are affine, commutative, connected and unipotent unless otherwise specified. By k we shall always mean a perfect field of characteristic p.

1. Group schemes and Dieudonné modules. In this section we discuss the basic properties of Dieudonné modules that will be needed for the rest of the paper. We also specialize these properties to the subclass of Dieudonné modules that correspond to Witt subgroups. Dieudonné modules are modules over a certain ring, whose description requires the ring of Witt vectors. We will start by recalling how this ring is defined. More details can be found in either [**3**] or [**7**].

Let k be a field of characteristic p. For any $n > 0$ define a polynomial $w_n(Z_0, Z_1, \ldots, Z_n)$ by

$$w_n(Z_0, Z_1, \ldots, Z_n) = p^n Z_n + p^{n-1} Z_{n-1}^p + \cdots + Z_0^{p^n}.$$

We use these to define additional polynomials $S_0, S_1, \ldots$; $P_0, P_1, \ldots$ via

$$w_n(S_0, \ldots, S_n) = w_n(X_0, \ldots, X_n) + w_n(Y_0, \ldots, Y_n)$$
$$w_n(P_0, \ldots, P_n) = w_n(X_0, \ldots, X_n) w_n(Y_0, \ldots, Y_n).$$

For example,

$$\begin{aligned} S_0(X_0, Y_0) &= X_0 + Y_0 \\ S_1((X_0, X_1), (Y_0, Y_1)) &= X_1 + Y_2 - \frac{(X_0 + Y_0)^p - X_0^p - Y_0^p}{p} \\ P_0(X_0, Y_0) &= X_0 Y_0 \\ P_1((X_0, X_1), (Y_0, Y_1)) &= X_0^p Y_1 + X_1 Y_0^p + p X_1 Y_1. \end{aligned}$$

The polynomials S_i and P_i have integer coefficients.

Let $W(k) = \{(a_0, a_1, \dots) \mid a_i \in k\}$. We can make $W(k)$ into a ring by

$$\begin{aligned} (a_0, a_1, \dots) + (b_0, b_1, \dots) &= (S_0(a_0, b_0), S_1((a_0, a_1), b_0, b_1)), \dots) \\ (a_0, a_1, \dots) \cdot (b_0, b_1, \dots) &= (P_0(a_0, b_0), P_1((a_0, a_1), (b_0, b_1)), \dots). \end{aligned}$$

$W(k)$ is called the *ring of Witt vectors with coefficients in* k. $W(k)$ is a commutative ring with multiplicative identity $1_{W(k)} = (1, 0, 0, \dots)$. The characteristic of $W(k)$ is 0. Note that $p = 1_{W(k)} + 1_{W(k)} + \cdots + 1_{W(k)} = (0, 1, 0, 0, \dots)$. More generally, p^n is the vector with a 1 in the nth place and zeros elsewhere.

If we take $k = \mathbf{F}_p$, then $W(k) \cong \mathbf{Z}_p$, the ring of p-adic integers. If $k = \mathbf{F}_{p^r}$, then $W(k)$ is isomorphic to the unique unramified extension of $\mathbf{Z}_p$ of degree r.

We can use Witt vectors to define a unipotent group scheme, which we will call W. For any k-algebra A we define $W(A) = W(k) \otimes_k A$, which gives the Witt vectors with coefficients in A. Let $W_n = W_n(k) = W/p^n W$, the group scheme of Witt vectors of length n. Clearly W_n can be viewed as a unipotent group scheme in the same way.

The ring $W(k)$ is equipped with two k-group scheme homomorphisms F and V defined by

$$F(a_0, a_1, a_2, \dots) = (a_0^p, a_1^p, a_2^p, \dots)$$

and

$$V(a_0, a_1, a_2, \dots) = (0, a_0, a_1, a_2, \dots).$$

One of the properties of F and V is that $FV = VF = p = (0, 1, 0, 0, \dots)$. These maps induce maps on the W_ns which we shall also denote by F and V.

Let E be the ring of noncommutative polynomials $W(k)[F,V]$ with the relations $FV = VF = p$, $Fw = w^\sigma F$, $wV = Vw^\sigma$, with $w \in W(k)$ and w^σ defined by raising each component to the pth power. To any finite unipotent group scheme G we associate a left E-module $D^*(G) = \mathrm{Hom}_{k-gr}(G, C)$, the k-group scheme homomorphisms from G to C, where C is the E-module functor of Witt covectors as defined in [**5**].

The action of E on $D^*(G)$ is induced from the action on C:

$$e \cdot f(x) = f(e \cdot x)$$

where $e \in E$, $x \in G(A)$ for some k-algebra A, and $f : G \to C$.

The (exact) contravariant functor D^* induces an anti-equivalence between finite unipotent group schemes and finite length E-modules that are killed by a power of V. Moreover, if G is connected, then $D^*(G)$ is also killed by a power of F, so D^* induces an anti-equivalence between finite connected unipotent group schemes and E-modules killed by a power of both F and V. Here we will use the term *Dieudonné module* to refer to such a left E-module. (This notion of Dieudonné module is somewhat restrictive, for in [**4**], [**5**] a Dieudonné module can be used to describe formal groups or nonconnected, non-unipotent group schemes. However, this definition is all we will need for the results to follow.) The size of the group scheme and the Dieudonné module are related by

$$\dim_k G = p^{\mathrm{length}_W D^*(G)},$$

[**6**]. As an example, it can be shown that $D^*(W_n) = E/E(V^n)$, a fact we will use several times. Also, if we let $\boldsymbol{\alpha}_p$ be the unique k-group scheme of rank p (namely for any k-algebra A we have $\boldsymbol{\alpha}_p(A) = \{a \in A \mid a^p = 0\{$ with operation induced from the operation on A), then $\boldsymbol{\alpha}_p = \ker F : W_1 \to W_1$, so $D^*(\boldsymbol{\alpha}_p) = \mathrm{coker}\,(F : D^*(W_1) \to D^*(W_1)) = E/E(F,V)$.

Of interest to us will be the following special class of group schemes.

Definition 1.1. A *Witt subgroup* is a finite subgroup of W_n for some n.

Notice that a Witt subgroup is not a subgroup of W. As an example, we have already seen $\boldsymbol{\alpha}_p$ is a subgroup of W_1 and is finite, hence it is

a Witt subgroup. For a more complicated example, let G be the group scheme given by

$$G(A) = \{a \in A \mid a^{p^2} = 0\}$$

with group operation given by

$$a +_G b = a + b - \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!}\, a^{pi} b^{p(p-i)}.$$

Then G is isomorphic to the Witt subgroup

$$G'(A) = \{(a^p, a) \mid a^{p^2} = 0\} \subset W_2(A).$$

In fact, $F(a^p, a) = (a^{p^2}, a^p) = (0, a^p) = V(a^p, a)$ and $p(a^p, a) = (0, a^{p^2}) = (0, 0)$, hence

$$D^*(G) = D^*(G') = E/E(F - V, F^2).$$

A Dieudonné module is *cyclic* if it is of the form E/I for some ideal $I \subset E$. The connection between cyclic Dieudonné modules and Witt subgroups is given by

Lemma 1.2. *G is a Witt subgroup if and only if $D^*(G)$ is a cyclic Dieudonné module.*

Proof. Since $G \subset W_n$ for some n, we must have $D^*(G)$ as a quotient of $D^*(W_n) = E/E(V^n)$, which is cyclic. Conversely, if $M = D^*(G)$ is a Dieudonné module, there is an n such that $V^n M = 0$. Now if $M = E/I$, then $V^n \in I$, and we get the projection $E/E(V^n) \twoheadrightarrow E/I$ which, when applying the inverse functor to D^*, gives us the injection $G \hookrightarrow W_n$. □

We now restrict our attention to Witt subgroups G that are killed by p. Let $M = D^*(G)$. If $pG = 0$, it is easy to show that $pM = 0$. Thus we may classify all Witt subgroups killed by p by classifying all cyclic Dieudonné modules killed by p.

If $pM = 0$, then $M = M/pM$ is a module over $E/pE = k[F, V]/(FV)$. Thus we need only consider actions on our modules by elements of

the form $a + \sum_{i=1}^{n} b_i F^i + \sum_{j=1}^{m} c_j V^j$, eliminating the need to consider multiples of p or polynomials with "cross terms" $F^i V^j$. In particular, an E-module homomorphism between cyclic Dieudonné modules killed by p is given by multiplication by an element in E/pE.

Finally, notice that if G is killed by p, then the length of $D^*(G)$ over $W(k)$ is exactly equal to the dimension over k, hence

$$\dim_k G = p^{\dim_k D^*(G)}.$$

2. Cyclic Dieudonné modules killed by p. Having established that Witt subgroups killed by p correspond to cyclic Dieudonne modules killed by p, it suffices to completely classify this class of cyclic Dieudonné modules.

Proposition 2.1. *Let M be a cyclic Dieudonné module killed by p. Then there exist positive integers l and m such that either*

$$M \cong E/E(F^l, V^m, p) \quad \textit{or} \quad M \cong E/E(F^l - \eta V^m, p)$$

where $\eta \in k^\times$.

Proof. Assume M is not isomorphic to $E/E(F^l, V^m, p)$ for any l, m. E is Noetherian [**3**], so M must be of the form E/I, where

$$I = (F^n, f_1(F) - g_1(V), f_2(F) - g_2(V), \ldots, f_s(F) - g_s(V), V^r, p)$$

for some n, r and polynomials $f_i(F) \in k[F]$, $g_i(V) \in k[V]$. Of course, we can assume each $f_i(F)$ has degree no more than $n-1$ and each $g_i(V)$ has degree no more than $r-1$. (Note that we can also assume that there are no "cross terms" in these relations as $FV = VF = p \in I$.) Assume $F^{n-1}M \neq 0$.

We shall first consider the case $s = 1$. Let $x \in M$ be the element corresponding to $1 \in E$ under the natural projection $E \to M$. Notice that neither $f(F) = f_1(F)$ nor $g(V) = g_1(V)$ can be zero. For instance, if $g(V) = 0$, then $f(F) \neq 0$, since $M \ncong E/E(F^l, V^m, p)$, but $f(F)x = 0 \in M$, so we can solve this equation for the smallest

power of F; which means that we could write a power of F strictly in terms of larger powers of F, violating the fact that $F^{n-1}M \neq 0$.

Let $f(F) = \sum_{i=l}^{n-1} c_i F^i$ and $g(V) = \sum_{i=m}^{r-1} d_i V^i$ for some l and m with $c_i, d_i \in k$, $c_l d_m \neq 0$.

Claim 1. *$l \neq 0$ and $m \neq 0$.*

Of course, we can always assume $m \neq 0$. Suppose $l = 0$. Since $M \cong M/pM$, x generates M as an $E/pE \cong k[F,V]/(FV)$-module. Then

$$c_0 x = \sum_{i=m}^{r-1} d_i V^i x - \sum_{i=1}^{n-1} c_i F^i x.$$

But then

$$x = \sum_{i=m}^{r-1} d_i' V_x^i - \sum_{i=1}^{n-1} c_i' F_x^i, \quad \text{where } c_i' = \frac{c_i}{c_0},\ d_i' = \frac{d_i}{d_0}.$$

This gives

$$F^{n-1}x = \sum_{i=m}^{r-1} d_i'^{p^{n-1}} F^{n-1} V^i x - \sum_{i=1}^{n-1} c_i'^{p^{n-1}} F^{n-1+i} x.$$

If $n = 1$, we get $x = \sum_{i=m}^{r-1} d_i'^{p^{n-1}} V^i x$, which is impossible as repeated substitutions for x would express x as higher and higher powers of V, forcing x to be zero. Suppose $n > 1$. As $F^n x = 0 = px$, we get

$$F^{n-1}x = \sum_{i=m}^{r-1} d_i'^{p^{n-1}} F^{n-2} V^{i-1} px - 0 = 0,$$

contradicting the fact that $F^{n-1}M \neq 0$. Thus $l \neq 0$, and the claim is proved. □

Claim 2. *$F^{l+1}M = 0$ and $V^{m+1}M + 0$; hence, we may let $n = l+1$ and $r = m+1$.*

Suppose $n > l+1$ and $F^{n-1}M \neq 0$. Then

$$\begin{aligned} F^{n-l-1}f(F)x &= \sum_{i=l}^{n-1} F^{n-l-1}c_iF^ix \\ &= \sum_{i=l}^{n-1} c_i^{p^{n-l-1}}F^{n-l-1+i}x \\ &= c_l^{p^{n-l-1}}F^{n-1}x. \end{aligned}$$

But we also have

$$\begin{aligned} F^{n-l-1}f(F)x &= F^{n-l-1}g(V)x \\ &= \sum_{i=1}^{r-1} F^{n-l-1}d_iV^ix \\ &= \sum_{i=1}^{r-1} F^{n-l-2}d_i^pV^{i-1}px = 0. \end{aligned}$$

Thus $c_l^{p^{n-l-1}}F^{n-1}x = 0$. Since $c_l \neq 0$, $F^{n-1}x = 0$, contradicting our choice of n. Thus we may let $n = l+1$. A similar argument for $r = m+1$ establishes the claim.

Our Dieudonné module is now of the form

$$E/E(F^{l+1}, c_lF^l - d_mV^m, V^{m+1}, p).$$

Of course, $E(F^{l+1}, c_lF^l - d_mV^m, V^{m+1}, p) = E(F^{l+1}, F^l - (d_m/c_l)V^m, V^{m+1}, p)$. If we let $\eta = (d_m/c_l)$, notice that

$$F^{l+1} = F(F^l - \eta V^m) + \eta^pV^{m-1}(p)$$

and

$$V^{m+1} = \eta^{-p^{-1}}F^{l-1}(p) - \eta^{-p^{-1}}V(F^l - \eta V^m)$$

so, for $s = 1$, we get

$$M \cong E/E(F^l - \eta V^m, p).$$

Finally, if $s > 1$, then there is another relation, say $f'(F) = g'(V)$ where we have $f'(F) = \sum_{i=l'}^{l} a_iF^i$ and $g'(V) = \sum_{i=m'}^{m} b_iV^i$. Using the

above methods, it is clear that $l'+1 = l+1$ and $m'+1 = m+1$, hence $l' = l$ and $m' = m$. So $f'(F) = a_l F^l$ and $g'(V) = b_m V^m$. Thus

$$a_l F^l x = b_m V^m x \quad \text{and} \quad c_l F^l x = d_m V^m x.$$

where $a_l, b_m, c_l, d_m \in k^\times$. Since $F^l x \neq 0$ and $V^m x \neq 0$, we get

$$F^l x = \frac{b_m}{a_l} V^m x = \frac{d_m}{c_l} V^m x,$$

so the additional relation $f'(F) - g'(V)$ is extraneous, i.e., it is a multiple of $f(F) - g(V)$. Thus we can always take $s = 1$, hence all cyclic Dieudonné modules killed by p are of the form

$$E/E(F^l, V^m, p) \quad \text{or} \quad E/E(F^l - \eta V^m, p). \qquad \square$$

We shall adopt the following notation for our cyclic Dieudonné modules:

$$M_{l,m} = E/E(F^l, V^m, p)$$
$$M_{l,m,\eta} = E/E(F^l - \eta V^m, p)$$

where l, m are positive integers and $\eta \in k^\times$.

Remark. The modules of the form $M_{l,m}$ are all nonisomorphic; however, this is not true for modules of the form $M_{l,m,\eta}$. In the next section we shall give a classification where all of the modules are nonisomorphic.

Before examining isomorphism questions, we need a quick result on the dimensions of our modules.

Lemma 2.2. *Let l and m be positive integers, $\eta \in k^\times$. Let $M_{l,m} = E/E(F^l, V^m, p)$ and $M_{l,m,\eta} = E/E(F^l - \eta V^m, p)$. Then*

(i) $\dim_k M_{l,m,\eta} = l + m$

(ii) $\dim_k M_{l,m} = l + m - 1$.

Proof. It is easy to see that

$$\{x, Fx, F^2x, \ldots, F^l x, Vx, V^2x, \ldots, V^{m-1}x\}$$

is a k-basis for $M_{l,m,\eta}$ where $x = 1_{M_{l,m,\eta}}$; and that

$$\{y, Fy, F^2y, \dots, F^{l-1}y, Vy, V^2y, \dots, V^{m-1}y\}$$

is a k-basis for $M_{l,m}$ where $y = 1_{M_{l,m}}$. □

3. The complete classification of nonisomorphic modules. We now address the question: when are two Dieudonné modules as given in (2.1) isomorphic? Any homomorphism of cyclic modules $\phi : M \to M'$ is uniquely determined by $\phi(1_M)$. If $\phi(1_M) = h$, then $\phi(e \cdot 1_M) = e \cdot \phi(1_M) = e \cdot h \in M'$. Of course, this h must "preserve the module relations," i.e., if $e \cdot 1_M = 0$, then $\phi(e \cdot 1_M) = e \cdot h$ must be zero in M'. We will say that ϕ is given by h in this case.

In the case where M' is killed by p, we can take $h = h(F, V) \in k[F, V]/(FV)$ and think of it as a polynomial with no cross terms. In order for ϕ to be an isomorphism, the constant term of this polynomial must be nonzero.

We start with some easy results.

Lemma 3.1. *Let $M_{l,m} = E/E(F^l, V^m, p)$, $M_{l',m'} = E/E(F^{l'}, V^{m'}, p)$, $M_{l,m,\eta} = E/E(F^l - \eta V^m, p)$ and $M_{l',m',\eta'} = E/E(F^{l'} - \eta' V^{m'}, p)$ where l, l', m and m' are positive integers and $\eta, \eta' \in k^\times$. Then*

(i) *$M_{l,m} \cong M_{l',m'}$ if and only if $l = l'$ and $m = m'$.*

(ii) *If $M_{l,m,\eta} \cong M_{l',m',\eta'}$, then $l = l'$ and $m = m'$.*

(iii) *$M_{l,m,\eta} \ncong M_{l',m'}$ for any choice of l, l', m, m', η.*

Proof. (i) The powers of F and V that kill M are invariant under isomorphism, so $F^l M_{l,m} = 0$, $F^{l-1} M_{l,m} \neq 0$ implies that $F^l M_{l',m'} = 0$, $F^{l-1} M_{l',m'} \neq 0$; hence, $l' = l$. A similar argument shows $m = m'$.

(ii) Similar to (i), only here we use $F^{l+1} M_{l,m,\eta} = 0$, $F^l M_{l,m} \neq 0$.

(iii) Suppose $M_{l,m,\eta} \cong M_{l',m'}$. By (2.2), we must have $l + m = l' + m' - 1$, so without loss of generality we may assume $l < l'$.

For an isomorphism $\phi : M_{l,m,\eta} \to M_{l',m'}$ given by $h \in k[F, V]/(FV)$ we get

$$0 = \phi(0) = \phi((F^l - \eta V^m)x) = (F^l - \eta V^m)hy$$

where $x = 1_{M_{l,m,\eta}}$ and $y = 1_{M_{l',m'}}$. Write $h = a + Fh_1 + Vh_2$, $a \in k^\times$, $h_1 \in k[F]$, $h_2 \in k[V]$. Then

$$\begin{aligned}(F^l - \eta V^m)hy &= ap^l F^l y - a^{p^{-m}} \eta V^m y + (F^l - \eta V^m)(Fh_1 + Vh_2)y \\ &= a^{p^l} F^l y - a^{p^{-m}} \eta V^m y + h' F^{l+1} y + h'' V^{m+1} y\end{aligned}$$

for the appropriate choice of h' and h''. Since the powers of F and V are linearly independent in $M_{l',m'}$, we must have $F^l y = 0$, which contradicts our assumption that $l < l'$. □

Thus, all of the $M_{l,m}$'s are different and are different from all of the $M_{l,m,\eta}$'s. In fact, the only possible isomorphisms are between M_{l,m,η_1} and M_{l,m,η_2}. The primary goal of this section is to determine exactly how many isomorphism classes of modules we have for a given l and m. For the remainder of this section, we shall fix l and m and write M_η for $M_{l,m,\eta}$.

Suppose $\phi : M_{\eta_1} \to M_{\eta_2}$ is an isomorphism. Let $x = 1_{M_{\eta_1}}$ and $y = 1_{M_{\eta_2}}$. Write

$$\phi(x) = ay + eFy + e'Vy, \quad a \in k^\times.$$

Then

$$\phi(F^l x) = a^{p^l} F^l y = a^{p^l} \eta_2 V^m y \quad \text{and} \quad \phi(\eta_1(V^m x) = a^{p^{-m}} \eta_1 V^m y$$

so we must have $a^{p^l} \eta_2 = a^{p^{-m}} \eta_1$, i.e., $(\eta_1/\eta_2) = a^{(p^l - p^{-m})}$. Thus we obtain

Lemma 3.2. *$M_{\eta_1} \cong M_{\eta_2}$ if and only if there exists an $a \in k^\times$ such that*

$$\left(\frac{\eta_1}{\eta_2}\right)^{p_m} = a^{p^{l+m}-1}. \qquad \square$$

Alternatively, let $\tau : k \to k$ be the $\mathbf{F}_p$-monomorphism defined by $\tau(x) = x^{p^{l+m}}$. Let G be the subgroup of $k^\times$ given by $\{\tau(x)/x\} \mid x \in k^\times\}$. Then we may restate the above lemma as follows: $M_{\eta_1} \cong M_{\eta_2}$ if and only if $(\eta_1/\eta_2)^{p^m} \in G$.

It k is algebraically closed, $f(x) = x^{p^{l+m}-1} - (\eta_1/\eta_2)^{p^m} = 0$ always has a solution, so we get

Corollary 3.3. *If k is algebraically closed, then $M_{\eta_1} \cong M_{\eta_2}$ for all $\eta_1, \eta_2 \in k$. In particular, all cyclic Dieudonné modules killed by a power of p are isomorphic to $E/(E(F^l, V^m, p)$ or $E/E(F^l - V^r, p)$.*

Let $k_0 \subset k$ be the subfield of elements fixed by τ. Notice that in the case $k \subset \mathbf{F}_{p^{l+m}}$ we have $k_0 = k$ so $\tau(x) = x$, hence G is trivial. Thus, $M_{\eta_1} \cong M_{\eta_2}$ if and only if $(\eta_1/\eta_2)^{p^m} = 1$, i.e., $\eta_1 = \eta_2$. Thus in this case no two M_n's are isomorphic.

The following two lemmas provide very useful properties of G:

Lemma 3.4. $G \cap k^{p^m} = G^{p^m}$.

Proof. It is clear that $G^{p^m} \subset G \cap k^{p^m}$. Let $g \in G \cap k^{p^m}$. Then $g = (\tau(x)/x)$ for some $s \in k^\times$ and there is an $a \in k^\times$ so that $a^{p^m} = g$. We shall show $a \in G$. If we raise both sides of $(\tau(x)/x) = a^{p^m}$ to the p^lth power, we obtain

$$\frac{\tau(x^{p^l})}{x^{p^l}} = a^{p^{l+m}} = \tau(a),$$

hence $\tau(a) \in G$. But $(\tau(1/a))/(1/a) \in G$ as well, hence

$$\tau(a) \cdot \frac{\tau(1/a)}{1/a} = a$$

is an element of G. □

Lemma 3.5. *Let G, k and k_0 be as above. Then $G \cong k^\times/k_0^\times$.*

Proof. The map $\phi : k^\times \to G$ given by $\phi(x) = \tau(x)/x$ is clearly a group homomorphism with kernel $k_0^\times$. □

Of course, the map $(\ )^{p^m}$ is injective, hence if $(\eta_1/\eta_2)^{p^m} = g = (\eta_1/\eta_3)^{p^m}$, then $\eta_2 = \eta_3$. Thus, for a given M_η, there is an injective

map from $\{\eta' \in k^\times \mid M_\eta \cong M_{\eta'}\}$ to G. In fact, since the corresponding elements of G must be p^mth powers, the image of the injective map lies in $G \cap k^{p^m} = G^{p^m}$. So for all $g \in G^{p^m}$ there is a unique $\gamma \in G$ so that $\gamma^{p^m} = g$. Given any such γ we have

$$\left(\frac{\eta}{\eta/\gamma}\right)^{p^m} = g,$$

hence $M_\eta \cong M_{\eta/\gamma}$. Thus we obtain

Theorem 3.6. *The isomorphism classes of cyclic Dieudonné modules of the form $E/E(F^l - \eta V^m, p)$ for a fixed l and m are in one-to-one correspondence with the quotient group $Q = k^\times/G^{p^m}$.*

We shall briefly revisit the case where k is algebraically closed. Here $G = k^\times$ and $G^{p^m} = G$, hence $Q = \{1\}$. In other words, there is exactly one isomorphism class, as was stated above.

The results also simplify in the case where k is a finite field, say $k = \mathbf{F}_{p^r}$. In this case G is finite (as it is a subgroup of $k^\times$), hence $G^{p^m} = G$. Also, $k_0 = k \cap \mathbf{F}_{p^{l+m}} = \mathbf{F}_{p^d}$, where $d = \gcd(r, l+m)$. Here $Q = k^\times/G$. By (3.7) the order of G is $|k^\times|/|k_0^\times|$, so we obtain

Theorem 3.7. *Let $k = \mathbf{F}_{p^r}$. The number of isomoprhism classes of cyclic Dieudonné modules of the form $E/E(F^l - \eta V^m, p)$ for a fixed l and m is $p^d - 1$, where $d = \gcd(r, l+m)$.*

The group $k^\times$ is cyclic, and we shall denote a generator by α. Clearly G is also cyclic and is generated by $(\tau(\alpha)/\alpha) = \alpha^{p^{\gcd(r,l+m)}-1}$. Our classification can be a bit more explicit:

Corollary 3.8. *Let $k = \mathbf{F}_{p^r}$, $k_0 = k \cap \mathbf{F}_{p^{l+m}}$. Let α generate the cyclic group $k^\times$. Any cyclic Dieudonné module killed by p can be expressed uniquely as either*

$$M_{l,m} = E/E(F^l, V^m, p) \quad \text{or} \quad M_{l,m,\alpha^i} = E/E(F^l - \alpha^i V^m, p),$$

where l, m and i are positive integers, $0 \le i \le p^d - 2$ and $d = \gcd(r, l+m)$.

Proof. G is the unique subgroup of $\mathbf{F}_{p^r}^{\times} = \langle\alpha\rangle$ of order $(p^r-1)/(p^d-1)$, hence the powers of α in G are multiples of p^d-1. Therefore,

$$\alpha^0 = 1, \alpha, \alpha^2, \dots, \alpha^{p^{d-2}}$$

are distinct elements modulo G. □

In spite of the fact that every element of Q has finite order (indeed, for all $q \in Q$ we have $q^{p^m(p^{l+m})} = 1$), Q itself need not be finite. For example, take $\bar{k}$ to be an algebraically closed field, and consider the field $\bar{k}(t)$. We claim that, for $a \neq b \in \bar{k}^{\times}$, $1+at$ and $1+bt$ are not equivalent modulo G^{p^m}. Since $G^{p^m} \subset ((\bar{k}(t))^{p^m})^{\times} = ((\bar{k}(t^{p^m})))^{\times}$, it suffices to show that $1 + at \neq (1 + bt)f(t^{p^m})$ for all $f(t^{p^m})$. By an elementary degree argument, f must be constant, and clearly $1+at = (1+bt)c$ has no solution if $a \neq b$. Thus we have found an infinite number of distinct elements in Q, hence Q is infinite.

4. Witt subgroups killed by p over finite fields. Now that we understand the Dieudonné modules corresponding to Witt subgroups, it is not difficult to explicitly write down the group schemes.

Take any $M_{l,m} = E/E(F^l, V^m, p)$. We shall denote the corresponding group scheme by $G_{l,m}$. Let A be any k-algebra. Since $E/E(V^m) \to M$ is surjective, $G_{l,m}$ can be viewed as a subgroup of W_m. As $pM = 0$, we must have $pG_{l,m} = 0$, that is, for $(a_0, a_1, \dots, a_{m-1}) \in G_{l,m}(A)$, we must have

$$p(a_0, a_1, \dots, a_{m-1}) = (0, a_0^p, a_1^p, \dots, a_{m-2}^p) = (0, 0, \dots, 0).$$

In addition, since $F^l M = 0$, we must have

$$F^l(a_0, a_1, \dots, a_{m-1}) = (a_0^{p^l}, a_1^{p^l}, \dots, a_{m-1}^{p^l}) = (0, 0, \dots, 0).$$

For $M_{l,m,\eta} = E/E(F^l - \eta V^m, p)$, the surjection is from $E/E(V^{m+1} \to M$, so the corresponding group scheme $G_{l,m,\eta}$ is a subgroup of W_{m+1}. Here $pM = 0$ gives that $a_i^p = 0$ for $0 \leq i \leq m-1$, $(a_0, a_1, \dots, a_m) \in G_{l,m,\eta}(A)$. The relation $(F^l - \eta V^m)M = 0$ translates to the condition $a_m^{p^l} = \eta a_0$. Thus

Theorem 4.1. *All Witt subgroups killed by p are of the form*

$$G_{l,m}(A) = \{(a_0, a_1, \dots, a_{m-1}) \in W_m(A) \mid a_0^p = a_1^p = \cdots = a_{m-2}^p = a_{m-1}^{p^l} = 0\},$$

or

$$G_{l,m,\eta}(A) = \{(a_0, a_1, \dots, a_m) \in W_{m+1}(A) \mid a_0^p = a_1^p = \cdots = a_{m-1}^p = 0, a_m^{p^l} = \eta a_0\}$$

for some $\eta \in Q = k^\times / G^{p^m}$.

Remark. If we allow $\eta = 0$, then we would get $G_{l,m,0} = G_{l,m+1}$. We shall not adopt this notation since the dimension of $G_{l,m,0}$ is not equal to the dimension of all of the other $G_{l,m,\eta}$s.

We shall conclude with some remarks concerning the number of Witt subgroups of a given dimension.

Proposition 4.2. *Let $k = \mathbf{F}_{p^r}$. The number of Witt subgroups of dimension p^n is $p^d(n-1)+1$ where $d = \gcd(n, r)$.*

Proof. By (2.2), we know that $\dim_k G_{l,m,\eta} = p^{l+m}$ and $\dim_k G_{l,m} = p^{l+m-1}$. It is clear that there are $n-1$ different choices of positive integers l and m so that $l + m = n$. Since each choice leads to $p^d - 1$ different η's (where $d = \gcd(r, l+m) = \gcd(n, r)$), we find that there are $(n-1)(p^d-1)$ distinct Witt subgroups of the form $G_{l,m,\eta}$. In addition, since there are n different choices of positive integers l and m so that $l + m - 1 = n$, and each gives rise to exactly one $G_{l,m}$, this adds another n Witt subgroup of dimension n. Thus the total number of Witt subgroups is $(n-1)(p^d-1) + n = p^d(n-1) + 1$. □

Remark. Of course, we can do a similar calculation if k is algebraically closed. In this case we replace $p^d - 1$ by 1 and get the total number to be $2n - 1$.

Finally, it is a conjecture of Lubin [**10**] that, given any positive integer n, the number of cyclic Dieudonné modules (not necessarily killed by

p) of length n is $n(n+1)/2$. Clearly, this cannot be the case for finite fields. The number of cyclic modules killed by p is $p^d(n-1)+1$, which depends on p. The appearance of the gcd in the formula also gives large fluctuations among fields of similar size, for example there are 13 Witt subgroups of dimension p^5 over $\mathbf{F}_{3^4}$ and $\mathbf{F}_{3^6}$, but over $\mathbf{F}_{3^5}$ there are 973. It seems likely that any such formula must take into consideration the size of the field in a fairly nontrivial way.

REFERENCES

1. V.A. Abrashkin, *Finite group schemes of period p over a discrete valuation ring*, Russian Math. Surveys **43** (1988), 199–240.

2. ———, *Honda systems of group schemes of period p*, Math. USSR-Izv. **30** (1988), 419–453.

3. M. Demazure and P. Gabriel, *Groupes Algebriques, Tome I*, North Holland Publ. Co., Amsterdam, 1970.

4. J.M. Fontaine, *Sur la construction du module de Dieudonné d'un groupe formel*, C.R. Acad. Sci. Paris Sér. I Math. **280** (1975), 1273–1276.

5. ———, *Groupes finis commutatifs sur les vecteurs de Witt*, C.R. Acad. Sci. Paris Sér. I Math. **280** (1975), 1423–1425.

6. A. Grothendieck, *Groupes de Barsotti-Tate et Cristaux de Dieudonné*, Les Presses de L'Université de Montréal, Canada, 1974.

7. N. Jacobson, *Lectures in abstract algebra III—Theory of fields and Galois theory*, Springer-Verlag, New York, 1964.

8. A. Koch, *Lifting Witt subgroups to characteristic zero*, New York J. Math. **4** (1998), 127–136.

9. ———, *Monogenic bialgebras over finite fields and rings of Witt vectors*, J. Pure Appl. Algebra **163** (2001), 193–207.

10. J. Lubin, Notes on a series of lectures on Dieudonné modules given at the State University of New York at Albany, 1989.

11. W. Waterhouse, *Introduction to affine group schemes*, Springer-Verlag, New York, 1979.

Department of Mathematics, Agnes Scott College, Decatur, GA 30030-3797
E-mail address: akoch@agnesscott.edu