Group schemes of order $p^2$

Kevin Buzzard

February 9, 2012

Last modified 01/08/2002.

Let $k$ be a sep closed field of char $p$. By Fontaine theory, the group schemes of order $p^2$ defined over $k$ which are killed by $p$ can be classified. We get products of the well-known group schemes of order $p$, namely $\mathbb{Z}/p\mathbb{Z}$, $\mu_p$ and $\alpha_p$, and then three more, all local-local, corresponding to Dieudonné modules that aren’t the direct sum of two smaller ones. Explicitly: let $M$ be a 2-dimensional $k$-vector space; then $F$ could be 0 and $V$ could be $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, or the other way around, or $F$ could be $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $V$ could be $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ too. And one can check that that’s the lot, up to isomorphism (note that a cunning change of basis brings $F = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $V = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, for any non-zero $\lambda$, to the last example above). One might ask what these last three “mystery” group schemes are. Well, one of them is $\alpha_{p^2}$.

Lemma 0.1. $\alpha_{p^2}$ is not self-dual.

Proof. One can check this by an explicit computation. Let $R$ denote the ring $k[X]/(X^p)$, with the obvious multiplication, and comultiplication given by $c(X) = X + Y$. Let $R^*$ denote the $k$-vector space dual to $R$. Let $e_i$, $0 \leq i < p^2$ denote the basis for $R^*$ dual to the basis $1, X, X^2, \ldots$ for $R$. The $k$-vector space $R^*$ inherits a multiplication from the comultiplication on $R$: if $e_i e_j$ denotes the product of $e_i$ and $e_j$ in $R^*$ then we see explicitly that $(e_i e_j)(X^k)$ will be the coefficient of $X^i Y^j$ in $(X + Y)^k$ and hence $e_i e_j = \binom{i+j}{i} e_{i+j}$ (strictly speaking one should perhaps remark that $\binom{i+j}{i} = 0$ in $k$ if $i + j > p^2$; this is a relief because $c$ wouldn’t be well-defined otherwise!). Associativity is a trivial combinatorial exercise; the unit element of $R^*$ is $e_0$, this being the co-unit in $R$, and the kicker is that if $i \geq 1$ then $(e_i)^p$ is $c e_{pi}$ with $c = (pi)!/i!p!$; interpreting this as the number of ways one can split $pi$ things into $p$ piles of size $i$ reveals that for $i \geq 1$ this number is a multiple of $p!$ and is hence 0 in $k$. So for any element $r = \lambda_0 e_0 + \lambda_1 e_1 + \ldots$ of $R$ we have $r^p = \lambda_0^p e_0 \in ke_0$. Hence $r = \lambda_0 e_0 + \lambda_1 e_1 + \ldots$ is nilpotent if $\lambda_0 = 0$ and is a unit otherwise. So $R^*$ is local and the maximal ideal is killed by raising to the power $p$. In particular $R$ and $R^*$ are not isomorphic even as rings, and hence $\alpha_{p^2}$ isn’t self-dual.

In particular, the argument on page DeRa-99 of Deligne-Rapoport isn’t right, but it can be fixed by working in the formal group—Toby pointed out to me the proof of Proposition 1.7 in Drinfeld’s paper on elliptic modules, which shows
that one can basically choose a coordinate on the formal group to make the D-R argument work. Similarly their justification of finiteness of $c$ is wrong, but can easily be modified: for example, looking at the Dieudonné module of $E[p]$ shows that there is only one subgroup of order $p$, which is all they need.

We have established that $\alpha_{p^2}$ is not self-dual. On the other hand it does contain a copy of $\alpha_p$ and the calculations above show that it’s connected with connected dual. So $F$ and $V$ are both nilpotent and $\alpha_{p^2}$ must correspond to one of our three mystery group-schemes but not the $F = V = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ one. It’s easy to see which: if $I$ is the maximal ideal of the global sections of $\alpha_{p^2}$ then $I/I^2$ is one-dimensional, so $M/FM$ is one-dimensional, so $F$ is non-zero. So $V = 0$ for $\alpha_{p^2}$. The dual of $\alpha_{p^2}$ has Dieudonné module the “mystery” module with $F = 0$ and $V$ non-zero.

One way of understanding the ring $R^*$ above is to think of $e_1$, $e_p$ as generators. One checks that if $0 \leq i, j \leq p - 1$ then $e_{i+pj}$ is just $e_i^j$ up to some non-zero constant; hence $R^*$ is isomorphic as a ring to $k[X,Y]/(X^p,Y^p)$. In particular $m/m^2$ is two-dimensional, as we expected.

Finally, Toby tells me that he can write down the Hopf algebra for the self-dual case—when $F$ and $V$ are nilpotent but non-zero. In this case Toby says that $R = k[X]/(X^{p^2})$ and $c$ is given by $c(X) = X + Y + ((X + Y)^{p^2} - X^{p^2} - Y^{p^2})/p''$ with the obvious abuse of notation. I checked explicitly for $p = 2$ that he was right: $c(X) = X + Y + X^2Y^2$ does give a Hopf algebra; the inverse of $X$ is $X$ again and this Hopf algebra is indeed self-dual.