The structure of $[N]$

Johan Commelin

March 19, 2012

Contents

Important. In this entire document N is a non-zero integer.

1 The structure of $[N]$

Let S be an arbitrary scheme, G/S an S-group scheme and $N \neq 0$ an integer. Then there exists an S-morphism "multiplication by N"

$$[N] \colon G \longrightarrow G$$

defined by $G(T) \xrightarrow{\cdot N} G(T)$ for all S-schemes T. (By the Yoneda lemma this gives a morphism $G \to G$.)

Assume G is commutative, then $[N]$ is a homomorphism. We denote with $G[N]$ the kernel of $[N]$. Note that $G[N]$ is again a group scheme over S (by the Yoneda lemma).

Let E/S be an elliptic curve.

Lemma 1. *Assume $S = Spec(\mathbb{C})$. The kernel $E[N]$ is a free $\mathbb{Z}/N\mathbb{Z}$-module of rank 2.*

Proof. From the theory of elliptic curves over the complex numbers, we know that E can be viewed (we actually view the analytic space E_h [Hart, B.1]) as a complex torus $\mathbb{C}/\Lambda$, where $\Lambda \subset \mathbb{C}$ is a lattice $\Lambda = \mathbb{Z} \oplus \omega\mathbb{Z}$ with $\Im(\omega) > 0$. Note that this is all in a non-canonical way.

In Theorem 10 we will show that $E[N]$ is etale over $\mathrm{Spec}(\mathbb{C})$. Nevertheless, from this point of view it is clear that $E[N] \cong \frac{1}{N}\Lambda/\Lambda$, which is indeed a free $\mathbb{Z}/N\mathbb{Z}$-module of rank 2. (It has basis $(1/N, \omega/N)$.) □

We would like to generalize this result over $\mathrm{Spec}(\mathbb{C})$ to arbitrary base schemes.

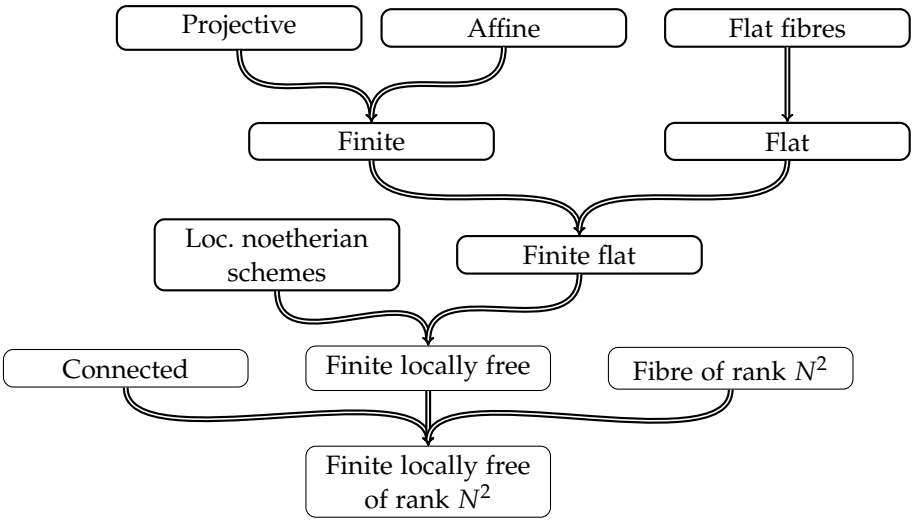


Figure 1: Diagram of sketching the idea behind the proof

Theorem 2. *Let S be an arbitrary scheme, E/S an elliptic curve and $N \neq 0$ an integer. Then the S-homomorphism "multiplication by N"*

$$[N] \colon E \longrightarrow E$$

is finite locally free of rank N^2.

The way we approach to the proof of this theorem is sketched in figure 1.

Lemma 3. *Let k be an algebraically closed field. Let $S = Spec(k)$, and X and Y two proper smooth S-curves. Assume X is irreducible. Let $f \colon X \to Y$ be an S-morphism. Then f is either finite flat or constant.*

Proof. See [Hart, II.6.8] and [G-W, 14.14].

A sketch: Since X and Y are proper, f is proper. Also $f(X)$ is closed in Y and proper over S. But also, since X is irreducible, $f(X)$ is irreducible. Therefore $f(X)$ is a point, or $f(X) = Y$.

In the second case we obtain an inclusion of function fields $K(Y) \subset K(X)$. Both function fields are finitely generated field extenstions of transcendence degree 1 over k. Therefore $K(X)/K(Y)$ is a finite algebraic extension.

Now let $V = \mathrm{Spec}(B)$ be an affine open of Y, and let A be the integral closure of B in $K(X)$. Then it can be shown [Hart, I.3.9A] that A is a finite B-module, and that $f^{-1}V = \mathrm{Spec}(A)$. It follows that f is finite.

In [G-W, 14.14] it is shown that consequently f is flat. Let $x \in X$ and $y = f(x)$. Note that $\mathcal{O}_{Y,y}$ is a field if y is the generic point, or otherwise it is a DVR.

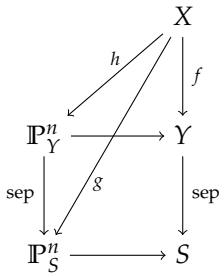
Then we have the diagram

$$\begin{array}{ccc} \mathcal{O}_{Y,y} & \longrightarrow & K(Y) \\ \downarrow & & \downarrow \\ \mathcal{O}_{X,x} & \longrightarrow & K(X) \end{array}$$

From this we deduce that $\mathcal{O}_{X,x}$ is a torsion-free module over the DVR (or field) $\mathcal{O}_{Y,y}$, hence flat. So all stalks are flat, therefore f is flat. □

Lemma 4. *Let S be a scheme and $f\colon X \to Y$ an S-morphism. If X/S is projective and Y/S is seperated, then f is projective.*

Proof. The structure morphism $X \to S$ factors as a closed immersion g via $\mathbb{P}^n_S \to S$ for some n. By the universal property of the fibred product, f and g induce a map $h\colon X \to \mathbb{P}^n_Y$. Since g is the composition of h with a seperated morphism, and g is a closed immersion, we see that h is a closed immersion. Hence f is projective.



□

Lemma 5. *Let $f\colon X \to Y$ be a morphism of noetherian schemes. If f is proper, and has finite fibres (i.e., f is quasi-finite), then f is finite.*

Proof. See [EGA IV(3), 8.11.1]. □

Lemma 6. *Let $f\colon X \to Y$ be a morphism of locally noetherian schemes that is projective and affine. Then f is finite.*

Proof. Let $(U_i)_i$ be an open affine cover of Y. Since f is affine, for all i we know that $f^{-1}(U_i)$ is affine. Since f is projective, $f_*\mathcal{O}_X$ is coherent. Thus $f_*\mathcal{O}_X(U_i) = \mathcal{O}_X(f^{-1}(U_i))$ is a finite $\mathcal{O}_Y(U_i)$-module. Hence f is finite. □

Proposition 7. *[Fibrewise criterion for flatness, locally noetherian] Let S be a scheme, $f\colon X \to Y$ a morphism of S-schemes. Assume*

1. *S, X and Y are locally noetherian;*
2. *X is flat over S;*
3. *For every $s \in S$ the morphism $f_s\colon X_s \to Y_s$ is flat.*

Then f is flat.

Proof. See [Stacks, 33.12.3, 039D]. □

Lemma 8. *Let $f\colon X \to Y$ be a morphism of noetherian schemes. Then f is finite locally free iff f is finite and flat.*

Proof. Clearly, locally free implies flat (since free modules are flat).

For the other implication see [Stacks, 24.43.2, 02KB].

In essence the proof boil down to commutative algebra. Let R be a ring, and M a finitely presented flat R-module.

Pick any prime $\mathfrak{p}$ and $x_1, \ldots, x_r \in M$ which map to a basis of $M \otimes_R \kappa(\mathfrak{p})$. By Nakayama's Lemma these elements generate M_g for some $g \in R, g \notin \mathfrak{p}$. The corresponding surjection $\phi\colon R_g^{\oplus r} \to M_g$ has the following two properties: (a) $\ker(\phi)$ is a finite R_g-module (see [Stacks, 7.4.2, 055Z]) and (b) $\ker(\phi) \otimes \kappa(\mathfrak{p}) = 0$ by flatness of M_g over R_g. Hence by Nakayama's lemma again there exists a $g' \in R_g$ such that $\ker(\phi)_{g'} = 0$. In other words, $M_{gg'}$ is free.

Since our schemes are noetherian, finite implies finite presentation. □

Proof (Theorem 2). Note that finite locally free is a notion that is local on the target, and therefore, using the results of Jinbi's talk we may assume that S is of the form $\operatorname{Spec}(\mathbb{Z}[a_1, a_2, a_3, a_4, a_6, 1/\Delta])$ and that E is defined by a Weierstrass equation. In particular S is noetherian, and E is locally noetherian.

Jinbi has shown that E is projective over S, and since E is separated (since proper) over S, we see that by Lemma 4 that $[N]$ is also projective.

To see that $[N]$ is affine, let $s \in S$ be given, and consider the fibre over s. In this fibre (which is in the $\mathbb{P}^2_{\kappa(s)}$) there is a homogeneous polynomial P of sufficiently high degree such that none of the N-torsion points of the fibre lie in the zero-locus of P. (Note that if the fibre lies over an infinite field, then a line will be sufficient.) Therefore, the N-torsion lies in the complement of this zero-locus, which is affine. Since it is a closed condition for these N-torsion points to lie in the zero-locus of P, we conclude that there is an open neighbourhood of s where the condition is satisfied. It follows that $[N]$ is affine.

Now Lemma 6 shows that $[N]$ is finite.

We now want to show that $[N]$ has flat fibres. Therefore, let $s \in S$ be a point, and consider $[N]_s\colon E_s \to E_s$. Since $\kappa(s) \to \overline{\kappa(s)}$ is faithful flat, it suffices to show that $[N]_{\overline{s}}\colon E_{\overline{s}} \to E_{\overline{s}}$ is flat. Observe that we can view $[N]$ as the composition of multiplication with the prime factors p_i of N. By Lemma 3 the $[p_i]_{\overline{s}}$ and $[N]_{\overline{s}}$ are either constant or flat. If $[N]_{\overline{s}}$ is constant, then so is one of the $[p_i]_{\overline{s}}$. If $p_i \neq \operatorname{char}(\kappa(s))$ it the tangent map is non-constant (we will see this later) hence $[p_i]_{\overline{s}}$ is non-constant. If $p_i = \operatorname{char}(\kappa(s))$ then p_i is unequal to 2 or 3. Since there is (as Jinbi has shown) at least 2-torsion or 3-torsion we see that $[p_i]_{\overline{s}}$ is non-constant. Hence, by Lemma 3 we see that $[N]_{\overline{s}}$ is finite flat. Consequently, all fibres are flat. And since S and E are locally noetherian and E is flat (since smooth) over S we conclude with Proposition 7 that $[N]$ is flat.

So $[N]$ is finite flat, and therefore Lemma 8 shows that $[N]$ is finite locally free.

Observe that S is connected, and therefore the rank is constant. As shown in Lemma 1, the rank is N^2 at $\mathbb{C}$-valued points, hence $[N]$ is finite locally free of rank N^2. □

2 $[N]$ on commutative group schemes

Let $f\colon G \to S$ be a smooth commutative S-group scheme. We want to study the multiplication by $[N]$ in this more abstract setting. In particular, we will prove that $[N]$ is etale if and only if N is invertible in S (i.e., S is a $\mathbb{Z}[1/N]$-scheme). This can be done in multiple ways. We will take the more categorical point of view, using the functor of points and the notion of formally etale. At the end we will state one lemma that indicates what is needed for a more algebro-geometric proof.

2.1 Categorical approach

First of all we recall that a map is etale if it is formally etale and locally of finite presentation. Since G/S is smooth, it is also locally of finite presentation and therefore locally of finite type. Now a cancellation property [G-W, 10.35] states that $[N]$ is locally of finite presentation.

Therefore, we want to prove that $[N]$ is formally etale if and only if N is invertible in S.

We do not yet assume that N is invertible in S. This will only be done in one of the implications in Theorem 10. We will now prepare everything that is needed to show that $G[N]$ is etale over S. In Theorem 10 we will then assume that N is invertible, make the final claim, and show that $G[N]/S$ is etale, which in turn implies that $[N]$ is etale.

Observe that we can view $G[N]$ as the pullback of 0 along $[N]$. I.e., the following diagram is cartesian.

$$\begin{array}{ccc} G[N] & \longrightarrow & S \\ \downarrow & & \downarrow{\scriptstyle 0} \\ G & \xrightarrow{[N]} & G \end{array}$$

Let C be a ring and $I \subset C$ an ideal satisfying $I^2 = 0$. Consider the following diagram

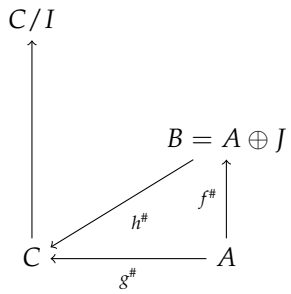
$$\begin{array}{ccc} \operatorname{Spec}(C/I) & \xrightarrow{\overline{g}} & G[N] \\ \downarrow & & \downarrow \\ & & G \\ & \overset{g_0}{\nearrow} & \downarrow \\ \operatorname{Spec}(C) & \xrightarrow{g} & S \end{array}$$

Here g and $\overline{g}$ are given, such that the rectangle commutes (as in the definition of formally etale). We can lift g along $G \to S$ since G/S is smooth. However, this is not unique.

Write $V = \{g_1 \in G(C) : \overline{g_1} = \overline{g} \in G(C/I)\}$ for the set of possible lifts. Essentialy g_0 is a fixed element in V. Observe that for all $g_1 \in V$ we have $g_1 - g_0 \in H = \ker(G(C) \to G(C/I))$. So we have $V = g_0 + H$. Observe that $\overline{N \cdot g_0} = N \cdot \overline{g_0} = 0$ and therefore $Ng_0 \in H$.

Now we may view open affine subsets of S and G. Indeed since 0 is an immersion, it is a closed immersion followed by an open immersion. Therefore there exist commutative rings A and B, such that $\mathrm{Spec}(A) \subset S$ and $\mathrm{Spec}(B) \subset G$ and also 0 is still a section of f. So now assume $S = \mathrm{Spec}(A)$ and $G \supset \mathrm{Spec}(B)$ without loss of generality.

Then, like Jinbi has shown, we can write $B = A \oplus J$, where $J = \ker(0^\#)$. Now, for all $h \in H$ we have the following diagram.



Since $\overline{h} = 0 \in G(C/I)$ and since G is a group scheme, we see that $\overline{h} = \overline{0 \circ g}$. As $J = \ker(0^\#)$ it follows that $\overline{h}^\#$ maps J to $0 \in C/I$. This shows that J is mapped into I by $h^\#$. Also, since $I^2 = 0$, J^2 maps to 0. Thus $h^\#$ induces a map $J/J^2 \to I$. Hence we have a map from H to $\mathrm{Hom}_A(J/J^2, I) = \mathrm{Der}_A(B, I)$. This map is explicitly given by

$$\begin{aligned} H &\to \mathrm{Der}_A(B, I) \\ h &\mapsto \Big(b \mapsto h^\#(b) - g^\#(b(0))\Big). \end{aligned}$$

We note that this map is a bijection, since the inverse is given by

$$\Big(b \mapsto d(b) + g^\#(b(0))\Big)^* \leftarrow\!\shortmid d.$$

Now we have a bijection between two sets, that both have a group structure: H gets its group structure from G, and $\mathrm{Der}_A(B, I)$ is an A-module. We want to show that our given bijection is a group homomorphism. Therefore we prove that our construction is functorial in G.

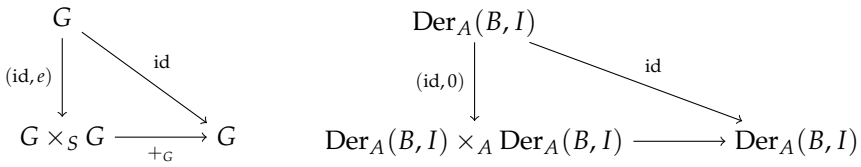
Lemma 9. *Let A, C and I be as in the text above. Let X_1 and X_2 be A-schemes. Let $\phi\colon X_1 \to X_2$ be an A-morphism. Let $p \in X_1(C)$ be a point. Then there exists a tangent map $T'_{f,p}\colon Der_A(B_1, I) \to Der_A(B_2, I)$. (Here we implicitly assume $X_i = Spec(B_i)$ for some rings B_i.)*

Proof. Similar to the way above we can assume $X_i = \operatorname{Spec}(B_i)$, and obtain A-modules $\operatorname{Der}_A(B_i, I)$. Indeed there exists a map

$$T'_{f,p} \colon \operatorname{Der}_A(B_1, I) \to \operatorname{Der}_A(B_2, I)$$
$$d \mapsto d \circ f^{\#}.$$

It is left as an exercise to prove that this is actually functorial. □

By the universal property of the fibred product we have $(X_1 \times_S X_2)(C) = X_1(C) \times_{S(C)} X_2(C)$, which shows that the tangent functor commutes with products. Now consider the diagrams

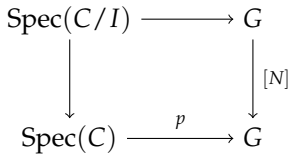


It follows that $T'_{+_G,g}(X, 0) = X$ and a similar argument shows that $(0, Y)$ is mapped to Y. Since the tangent map is an A-module homomorphism, we conclude that $T'_{+_G,g}$ is the usual addition on $\operatorname{Der}_A(B, I)$.

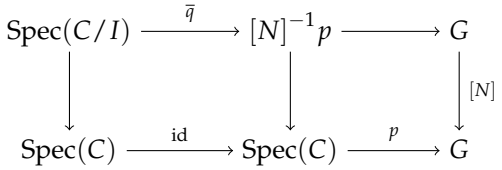
Theorem 10. *Let S be an arbitrary scheme, G/S a smooth commutative S-group scheme and $N \in \mathbb{Z}_{\geq 1}$ an integer. If N is invertible in S, then $[N]$ is etale over S.*

Proof. We want to show that there exists a unique $g_1 \in V$ such that $N \cdot g_1 = 0$ since this would mean that $g_1 \in G[N](C)$ is a unique lift of g. Equivalently, we want to show that there is a unique $h \in H$ such that $N(g_0 + h) = 0$. Recall that $-N \cdot g_0 \in H$. Since $H = \operatorname{Der}_A(B, I)$ is an A-module and N is invertible in A, we conclude that such an h exists and is unique. This shows that $G[N]$ is etale over S.

To show that $[N]$ is etale, again consider a diagram as in the definition of formally etale.



Now we insert the base change of $[N]$ along p and obtain



Now the right square is defined to be cartesian. It is clear that if we can lift in the left square, we can extend the lift to the rectangle by composition. Showing that we can indeed lift in the left square can essentially be done by an argument similar to the one for $G[N]$. ($[N]^{-1}p \to \operatorname{Spec}(C)$ is a $G[N]_C$-torsor.)

This shows that $[N]$ is formally etale. We had already shown that $[N]$ was locally of finite presentation. Hence $[N]$ is etale. □

Lemma 11. *Let S be an arbitrary scheme, G/S a commutative S-group scheme smooth of positive relative dimension over S and $N \in \mathbb{Z}_{\geq 1}$ an integer. If $[N]$ is etale over S, then N is invertible in S.*

Proof. Assume that N is not invertible in S. Then there exists an $s \in S$ such that the characteristic of $\kappa(s)$ divides N. Therefore in the fibre over s we see that $[N]$ is the zero-map, while the dimension is not 0. Hence $[N]$ is not etale. □

2.2 Sketch of an algebro-geometric approach

As promised, we would also give a hint of what would go into a more algebro-geometric proof of proving Theorem 10. The crucial ingredient is the following lemma.

Lemma 12. *Let $f\colon X \to Y$ be a morphism of schemes. Then f is smooth of relative dimension d if and only if*

- *f is locally of finite presentation;*
- *f is flat;*
- *the geometric fibres are smooth of dimension d.*

Proof. See [Stacks, 24.32.14, 01V9]. And also the paragraph above it. □

Since the first two conditions are clearly satisfied by $[N]$ (see the proof of Theorem 2) it suffices to show that the geometric fibers of $[N]$ are smooth of dimension 0. (To prove the statement for general commutative group schemes would obviously require proving the first two conditions as well.)

References

[G-W] U. GÖRTZ and T. WEDHORN. *Algebraic Geometry I*, 1st ed. Frankfurt, 2010. ISBN 9783834806765.

[EGA IV(3)] A. GROTHENDIECK. *Éléments de géométrie algébrique* (rédigés avec la collaboration de Jean Dieudonné) : IV. *Étude locale des schémas et des morphismes de schémas*, Troisième partie. Publications Mathiématiques de l'IHÉS, 28, 1966.

[Hart] R. HARTSHORNE. *Algebraic Geometry*, volume 52 of *Grad. Texts in Math.* Springer, 2006. ISBN 9780387902449.

[Stacks] J. DE JONG et al. *Stacks Project*. http://math.columbia.edu/algebraic_geometry/stacks-git, 2012.