Barsotti-Tate groups and abelian varieties

Pol van Hoften
UCL, 17137331
pol.hoften.17@ucl.ac.uk

June 3, 2019

1 Introduction and motivation

Elliptic curves E over a field k are often studied by studying their torsion subgroups $E[n]$ for various n. In particular if l is a prime coprime to the characteristic of k then the l-adic Tate module

$$T_l E = \varprojlim E[l^n](\overline{k})$$

is a $\mathbb{Z}_l$-module of rank 2 with an interesting action of $G_k = \mathrm{Gal}(\overline{k}/k)$.

However, when $l = p$, then the torsion points $E[p^n]$ are usually not well captured by their points over $\overline{k}$. In fact, for supersingular elliptic curves

$$\varprojlim E[p^n](\overline{k}) = \{e\}.$$

This does not mean that the schemes $E[p^n]$ are not interesting though, they contain a lot of information about the elliptic curve E. Moreover, they are easier to study in families, especially when p is not invertible on the base. It turns out that it is best to study *all* the $E[p^n]$ at the same time, for all n. This rather quickly leads us to formulate the notion of a p-divisible group and study some examples.

2 A crash course in finite flat group schemes

2.1 Basics

Definition 1. *A group scheme G over a (locally Noetherian) scheme is called finite flat if its structure morphism is finite and flat. In particular it will have an order (which will be a locally constant function on S).*

Remark 1. In this talk, the base scheme S will usually be a complete Noetherian local ring like $\mathbb{Z}_p$. So it can be useful to think about the example of an elliptic curve over $\mathbb{Z}_p$.

Example 1. If S is any scheme and G is an abstract group, then there is a constant group scheme $\underline{G}_S$.

Example 2. If $S = \mathrm{Spec}\, Z$ and n is any number, then $\mu_n = \mathrm{Spec}\, \mathbb{Z}[x]/(x^n - 1)$ is the group scheme of n-th rooths of unity. It is also $\mathbb{G}_m[n]$ and can be base changed to $\mu_{n,S}$ for any scheme S.

Example 3. If $S = \mathbb{F}_p$ then we define $\alpha_{p^n} = \mathbb{G}_a[p^n]$, it is represented by $\operatorname{Spec} \mathbb{F}_p[x]/(x^n)$ and can be base changed to any $\mathbb{F}_p$-scheme S.

Example 4 (Key Example). If $\mathcal{A}/S$ is an elliptic curve over S, then $\mathcal{A}[n]$ is a finite flat group scheme for every n. By an elliptic curve over a scheme S we mean an abelian scheme of relative dimension 1, i.e., where an abelian scheme is a proper smooth group scheme.

Proposition 1 (Deligne). *If G/S is a commutative group scheme of order n, then $[n] : G \to G$ is the zero morphism.*

Corollary 1. *If G/S is a group scheme of order n and n is invertible in S, then G is an étale group scheme.*

If we now take $S = \mathbb{Z}_p$, then this means that all groups that are not étale must have order p^k for some k.

2.2 Cartier duality

There is a duality theory for commutative finite flat group schemes, due to Cartier, that we will make use of. It is denoted by $G \mapsto G^D$ and it is an exact functor.

Example 5. The group schemes $\underline{\mathbb{Z}/n/zz}$ and μ_n are dual.

Example 6. The group scheme α_p is self dual.

Example 7. If $\mathcal{E}/S$ is an abelian scheme then

$$(\mathcal{E}[n])^D = \mathcal{E}^t[n],$$

where $()^D$ denotes Cartier duality and $\mathcal{E}^t$ is the dual abelian scheme. In particular if $\mathcal{E}/S$ is an elliptic curve (or a principally polarized abelian scheme) then $\mathcal{E} = \mathcal{E}^t$ and so $\mathcal{E}[n]$ is self dual for all n.

2.3 Connected- 'etale sequence

If G is a group scheme over a field, then so is the connected component of the identity, usually denoted by G^0. This is till true when the base S is a complete local ring (like $\mathbb{Z}_p$). The quotient G/G^0 exists by general results of Grothendieck and the quotient is the maximal étale quotient of G:

$$0 \to G^0 \to G \to G^{\text{ét}} \to 0.$$

In fact, if S is a perfect scheme (which is the only case we care about), then the sequence splits and we get a product decomposition

$$G = G^0 \times G^{\text{étale}}$$

2.4 The p-torsion of an elliptic curve

Let E be an elliptic curve over $\overline{\mathbb{F}_p}$, then we would like to compute what kind of group scheme $E[p]$ is (we already know that $E[l^n]$ is for $l \neq p$). We know that is is a group scheme of order p^2, killed by multiplication by p, and moreover that

$$\#E[p](\overline{\mathbb{F}_p}) \neq p^2,$$

so it cannot be étale.

Example 8. Suppose that E is an ordinary elliptic curve, which means that $\#E[p](\overline{\mathbb{F}_p}) = p$. This means that there is a subgroup

$$\underline{\mathbb{Z}/p\mathbb{Z}} \to E[p]$$

and by the connected-etale sequence (which splits, since we are over a perfect base), we have that

$$E[p] = \underline{\mathbb{Z}/p\mathbb{Z}} \times E[p]^0.$$

Using Cartier duality and the fact that $E[p]$ is self dual, we find that $E[p]^0 = \underline{\mathbb{Z}/p\mathbb{Z}} = \mu_p$.

Example 9. Doing a bit more work (in particular one needs to classify group schemes of order p, p^2), one can show that there is a nonsplit short exact sequence

$$0 \to \alpha_p \to E[p] \to \alpha_p \to 0$$

for supersingular E.

3 Barsotti-Tate groups

3.1 Basics

Recall from the introduction that we are interested in the p^n-torsion of abelian schemes, for all n. This motivates the following definition

Definition 2. *Let S be a scheme, then a Barsotti-Tate group or p-divisible group G of height h over S is an inductive system*

$$(G_n, i_n : G_n \to G_{n+1})$$

where G_n are finite flat group schemes and i_n are

A1 The order of G_n is p^{nh}

A2 There is an equality $G_{n+1}[p^n] = G[n]$ (equality of sub-groupschemes).

Example 10. Let $G_n = \underline{\mathbb{Z}/p^n\mathbb{Z}}$ and i_n be the natural inclusions. This forms a p-divisible group of height 1 usually denoted by $\underline{\mathbb{Q}_p/\mathbb{Z}_p}$.

Example 11. If $G_n = \mathbb{G}_m[p^n]$ with i_n being the natural inclusion, we get a p-divisible group of height 0.

Example 12. If $\mathcal{A}/S$ is an abelian scheme of relative dimension g, then $A[p^\infty]$ forms a p-divislbe group of height $2g$.

Remark 2. We have really given an inductive system of group schemes, and so it is natural to wonder about the colimit of this system. Unfortunately, this will not usually exist in the category of schemes (but it makes sense as an fppf-sheaf). We will discuss for étale and connected p-divisible groups separately.

3.2 Cartier duality and connected-étale sequence

Let G be a p-divisible group, then there are short exact sequences

$$0 \longrightarrow G_n \xrightarrow{i_n} G_{n+1} \xrightarrow{j_n} G_n \to 0$$

Here j_n fits in a diagram (which defines it uniquely)

$$\begin{tikzcd}
G_m \arrow[r, "i_n"] \arrow[dr, dotted, "j_n"] & G_{m+1} \arrow[d, "{[p]}"] \\
 & G_{m+1}.
\end{tikzcd}$$

Now applying Cartier duality to each G_n gives us a p-divisible group G^D where $(G^D)_n = G_n^D$ and the maps are j_n^D.

Given a p-divible group G over $\mathbb{Z}_p$ (or R), we can start by forming the étale-connected sequence of each separate G_n. Then we get a diagram

$$\begin{tikzcd}
G_n^0 \arrow[r] \arrow[d, dotted] & G_n \arrow[r] \arrow[d] & G_n^{\text{ét}} \arrow[d, dotted] \\
G_{n+1}^0 \arrow[r] & G_n \arrow[r] & G_{n+1}^{\text{ét}}
\end{tikzcd}$$

and we would like to show the dotted arrows exists. Since connected components map to connected components it is clear that the leftmost dotted arrow exists. Moreover, $G_n^{\text{ét}}$ is the maximal étale quotient and so the rightmost dotted arrows also exist.

Lemma 1. *The systems $\{G_n^0\}$ and $G_n^{ét}$ form p-divisible groups denoted by G^0 and $G^{ét}$, respectively.*

Proof. Omitted. It comes down to showing that the functor $G \mapsto G^0$ and $G \mapsto G^{\text{ét}}$ are exact functors. See [Lip] for details. □

3.3 Étale p-divisible groups

If G is an étale p-divisible group over $\mathbb{Z}_p$, then each G_n is just an étale finite flat group scheme. Equivalently, we can consider each G_n as an abstract finite abelian group with an action of $\pi_1^{\text{ét}}$. The axioms of p-divisible groups actually imply that $G_n \cong (\mathbb{Z}/p^n\mathbb{Z})^h$ as abstract group (a p^n torsion group of order p^n is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$).

Therefore we can quite easily 'take the colimit' of étale p-divisible groups. Every étale p-divisible group 'is' just

$$(\mathbb{Q}_p/\mathbb{Z}_p)^h$$

with a continuous action of $\pi_1^{\text{ét}}$. If we dualize this we find

$$\hom(\mathbb{Q}_p/\mathbb{Z}_p, G) = \mathbb{Z}_p^h$$

with a Galois action, this is usually thought of as the Tate module of G and only depends on $G^{\text{ét}}$.

3.4 Relation to formal groups

Now let G be a connected p-divisible group over $\mathbb{Z}_p$ (or R). This means that all of the G_n are non-reduced schemes over $\mathbb{Z}_p$ with the same underlying topological space. In any case, in this situation we could hope that the colimit $\varinjlim G_n$ is a *formal scheme.* In other words, if A_n are $\mathbb{Z}_p$-algebras such that $\operatorname{Spec} A_n = G_n$ we expect that

$$\varprojlim_{i_n^\sharp} A_n$$

is a nice topological ring $\mathcal{A}$ and then

$$\varinjlim_{i_n} G_n \cong \operatorname{Spf} \mathcal{A}.$$

In fact, the group law on the G_n should induce a group law on the formal scheme $\operatorname{Spf} \mathcal{A}$!

Definition 3. *A commutative formal Lie group (of dimension n) over $\mathbb{Z}_p$ is a commutative group object Γ in the category of formal schemes over $\mathbb{Z}_p$ such that $\Gamma = \operatorname{Spf} \mathbb{Z}_p[\![X_1, \cdots, X_n]\!]$. Equivalently, it is a continuous map*

$$\mathbb{Z}_p[\![X_1, \cdots, X_n]\!] \to \mathbb{Z}_p[\![Y_1, \cdots, Y_n, Z_1, \cdots, Z_n]\!]$$

given by a tuple of power series $f(Y, Z) = (f_1(Y, Z), \cdots, f_n(Y, Z))$, such that:

1. *$f(T, 0) = T = f(0, T)$ (composition is unital).*
2. *$f(T, f(Y, Z)) = f(f(T, Y), Z)$ (composition is associative).*
3. *$f(Y, Z) = F(Z, Y)$ (composition is commutative).*

The existence of an inverse follows from these axioms, as well as the fact that

$$f(Y, Z) = Y + Z + \text{ higher order terms.}$$

Example 13. Formal additive group and formal multiplicative group:

$$f(Y, Z) = Y + Z$$
$$f(Y, Z) = Y + Z + YZ.$$

Example 14. If A is an Abelian variety over $\mathbb{Z}_p$ of dimension g then we can complete it at the origin to get a formal Lie group of dimension g.

Let $\phi(X)$ be the polynomial corresponding to the multiplication by p map, then Γ is called p-divisible if the induced map $\mathcal{A} \to \mathcal{A}$ makes $\mathcal{A}$ into a finite free module over itself. In particular this means that the kernel of $[p]$ is a finite flat group scheme over $\mathbb{Z}_p$. Moreover, it must be connected since it is the spectrum of a local ring and so it has order p^h. Iterating this construction we find that $\Gamma[p^\infty]$ is a connected p-divisible group of height h.

We would like to associate to every connected p-divisible group G a p-divisible formal Lie group Γ (so that we can define the dimension of G, for example). The construction we sketched above (taking the colimit of the G_n) works, but it is not at all clear that the resulting formal scheme is 'formally smooth'.

Proposition 2 (Proposition 1 [Tat67])**.** *Let R be a complete Noetherian local ring whose residue field is of characteristic $p > 0$. Then $\Gamma \to \Gamma[p^\infty]$ is an equivalence between the category of p-divisible commutative formal Lie groups over R and the category of connected p-divisible groups over R.*

Proof. It suffices to prove that the functor is fully faithful and essentially surjective. Given a p-divisible group G the construction outlined above gives us a group object in the category of formal schemes, it is however not immediate that the underlying formal scheme is isomorphic to Spf $R[\![X_1, \cdots, X_n]\!]$. We refer to loc. cit. for the proof, we will however include a proof of fully faithfulness.

We want to show that given a divisible commutative formal Lie group Γ we have that $\Gamma = \varinjlim \Gamma[p^n]$. For this, it suffices to show that the ideals J_v cutting out the subschemes $G[p^n]$ form an alternative basis of the topology.

Let $\mathfrak{m}$ denote the maximal ideal of R, then the local ring $\mathcal{A} = \mathbb{Z}_p[\![X_1, \cdots, X_n]\!]$ has maximal ideal $\mathfrak{m}\mathcal{A} + I$ where $I = (X_1, \cdots, X_n)$. The ideal cutting out the kernel of $[p]$ is generated by $\mathfrak{m}\mathcal{A}+$ this needs to be fixed.

In the end everything comes down to the fact that $\phi(X) = pX+$ higher order terms. □

Remark 3. The construction above might seem like magic, but in fact it is very natural. Both p-divisible groups and formal Lie groups define fppf sheaves and the correspondence is actually an isomorphism of these sheaves.

Theorem 1. *Let G be a p-divisible group of height h, then*

$$h = \dim G + \dim G^D.$$

4 Good reduction of Abelian varieties

Now let A be an abelian variety over $\mathbb{Q}_p$ and consider its l-divisible groups $A[l^\infty]$ for all primes l. If A has good reduction, i.e., there is an abelian scheme $\mathcal{A}/\mathbb{Z}_p$ with generic fiber A, then these l-divisible groups extend to l-divisible groups over $\mathbb{Z}_p$.

For $l \neq p$, these will be étale p-divisible groups, i.e., groups with a Galois action. The fact that they extend just means that the Galois action is unramified. In fact, this is a sufficient criterion (Neron-Ogg-Shafarevich) for good reduction.

If $l = p$, then $A[p^\infty]$ is also an étale p-divisible group (since $\mathbb{Q}_p$ has characteristic 0), but it will not correspond to an unramified Galois module. In fact, it is always highly ramified, as we have

$$\Lambda^2 T_p A \cong \mathbb{Q}_p(-1)$$

the dual of the p-adic cyclotomic character, which is definitely 'very' ramified. Still, there is the following remarkable theorem of Grothendieck:

Theorem 2 (Grothendieck)**.** *Let A is above, then it has good reduction if and only if $A[l^\infty]$ extends to a l-divisible group over $\mathbb{Z}_p$ (including the case $l = p$).*

References

[Tat67] J. T. Tate. "p-divisible groups". In: *Proc. Conf. Local Fields (Driebergen, 1966)*. Springer, Berlin, 1967, pp. 158–183.

[Lip] Michael Lipnowski. *p-divisible groups.* URL: `https://services.math.duke.edu/~malipnow/expository/pdiv.pdf`.