Torsion Subgroups of Abelian Varieties

Raoul Wols

April 19, 2016

In this talk I will explain what abelian varieties are and introduce torsion subgroups on abelian varieties. k is always a field, and $\mathbf{Var}_k$ always denotes the category of varieties over k. That is to say, geometrically integral separated schemes of finite type with a morphism to k. Recall that the product of two $A, B \in \mathbf{Var}_k$ is just the fibre product over k: $A \times_k B$.

Definition 1. Let $\mathbf{C}$ be a category with finite products and a terminal object $1 \in \mathbf{C}$. An object $G \in \mathbf{C}$ is called a *group object* if G comes equipped with three morphism; namely a "unit" map

$$e : 1 \to G,$$

a "multiplication" map

$$m : G \times G \to G$$

and an "inverse" map

$$i : G \to G$$

such that

$$\begin{tikzcd} G \times G \times G \arrow[r, "\mathrm{id}_G \times m"] \arrow[d, "m \times \mathrm{id}_G"] & G \times G \arrow[d, "m"] \\ G \times G \arrow[r, "m"] & G \end{tikzcd}$$

commutes, which tells us that m is associative, and such that

$$\begin{tikzcd} G \arrow[r, "(e, \mathrm{id}_G)"] \arrow[d, "(\mathrm{id}_G, e)"'] \arrow[dr, "\mathrm{id}_G"] & G \times G \arrow[d, "m"] \\ G \times G \arrow[r, "m"] & G \end{tikzcd}$$

commutes, which tells us that e is indeed the neutral "element", and such that

$$\begin{tikzcd} G \arrow[r, "(\mathrm{id}_G, i) \circ \Delta"] \arrow[d, "(i, \mathrm{id}_G) \circ \Delta"'] \arrow[dr, "e'"'] & G \times G \arrow[d, "m"] \\ G \times G \arrow[r, "m"'] & G \end{tikzcd}$$

commutes, which tells us that i is indeed the map that sends "elements" to inverses. Here we use $\Delta : G \to G \times G$ to denote the diagonal map coming from the universal property of the product $G \times G$. The map e' is the composition $G \to 1 \xrightarrow{e} G$.

Now specialize to $\mathbf{C} = \mathbf{Var}_k$. The terminal object is then $1 = (\mathrm{Spec}(k) \xrightarrow{\mathrm{id}} \mathrm{Spec}(k))$, and giving a unit map $e : 1 \to G$ for some scheme G over k is equivalent to giving an element $e \in G(k)$.

Remark 2. Since we view schemes as representable sheaves of sets, definition 1 is equivalent to saying that for a group object G there exists a factorization

$$\begin{tikzcd} & \mathbf{Grp} \arrow[dr, "\text{forget}"] & \\ \mathbf{Sch}/k \arrow[ur, dotted] \arrow[rr, "G"] & & \mathbf{Sets} \end{tikzcd}$$

When one hears the term abelian variety, one might take a guess at a straightforward definition: it is a group object in $\mathbf{Var}_k$ which is abelian. It turns out that this is not the correct definition.

Definition 3. An abelian variety is a group object $A \in \mathbf{Var}_k$ which is proper as a variety.

Notice that we don't even require A to be abelian. This will follow automatically.

Definition 4. Let A, B be abelian varieties and let $f : A \to B$ be a morphism. Then f is called a *homomorphism* if the diagram

$$\begin{tikzcd} A \times A \arrow[r, "f \times f"] \arrow[d, "m_A"'] & B \times B \arrow[d, "m_B"] \\ A \arrow[r, "f"'] & B \end{tikzcd}$$

commutes.

Definition 5. Let A be an abelian variety and $a \in A(k)$ a point. We define the *(right) translation by* a, denoted τ_a, as the morphism $\tau_a := m_A \circ (\mathrm{id}_A, a')$.

So, translation τ_a is given by

$$A \xrightarrow{(\mathrm{id}_A, a')} A \times A \xrightarrow{m_A} A.$$

The following lemma plays a central role for abelian varieties. It paves the way for much of the results. The lemma can also be found in [2, Theorem 1.1] and [3, Lemma 1.12].

Lemma 6 (Rigidity)**.** *Let $X, Y, Z \in \mathbf{Var}_k$ and assume that X is complete. Suppose a morphism $f : X \times Y \to Z$ is given with the property that there exists a $y \in Y(k)$ and a $z \in Z(k)$ such that $f \circ (\mathrm{id}_X, y) = z$. Then f factors through the projection $\mathrm{pr}_Y : X \times Y \to Y$. That is, there exists a morphism $g : Y \to Z$ such that $f = g \circ \mathrm{pr}_Y$.*

Proof. Without loss of generality $k = \overline{k}$. Pick any point $x^* \in X(k)$ and define $g : Y \to Z$ by $g = f \circ (x^*, \mathrm{id}_Y)$. I claim that this is the g that we seek. Since $X \times Y$ is a variety, it is reduced (i.e. all stalks of the structure sheaf have no nilpotents). So it suffices to prove that $f = g \circ \mathrm{pr}_Y$ on k-rational points. Let $U \subset Z$ be an affine open around z and let $V = \mathrm{pr}_Y f^{-1}Z \setminus U$. Then $f^{-1}Z \setminus U$ is closed, and since X is complete, pr_Y is a closed map. Hence V is closed. If we take any point $w \notin V$, then $f(X \times \{w\}) \subset U$. Now since X is complete and U is affine, f must be constant on $X \times \{w\}$. So if we restrict f to the non-empty open set $X \times (Y \setminus V)$, then $f = g \circ \mathrm{pr}_Y$. But $X \times Y$ is irreducible, so $X \times (Y \setminus V)$ is dense. So $f = g \circ \mathrm{pr}_Y$ everywhere. □

Corollary 7. *Let $f : X \to Y$ be a morphism of abelian varieties. Then $f = \tau_{fe_X} \circ h$ for some homomorphism $h : X \to Y$.*

Proof. [3, Proposition 1.14] or [2, Corollary 1.2]. Here's a proof sketch: f sends e_X to fe_X, so after composing with the translation $\tau_{i_X fe_X}$ we may assume that f sends e_X to e_Y. Let φ be the difference of the two maps

$$\begin{tikzcd} X \times X \arrow[r, "m_X"] \arrow[d, "f \times f"'] & X \arrow[d, "f"] \\ Y \times Y \arrow[r, "m_Y"'] & Y \end{tikzcd},$$

and apply the rigidity lemma to φ. □

Corollary 8. *Every abelian variety is abelian.*

Proof. [2, Corollary 1.2] or [3, Corollary 1.14]. Both proofs use the fact that the inverse map of a group object G is a homomorphism if and only if G is abelian. □

Hence from here on out we write the group law additive.

Definition 9. Let A be an abelian variety, $n \in \mathbb{Z}_{>0}$. Then the regular map $n_A : A \to A$ is defined on points as $P \mapsto n \cdot P = P + \ldots P$. If $n = 0$, we set $n_A := 0$. If $n < 0$, then $n = -n'$ for some $n' > 0$. We then set $n_A := i_A \circ n'_A$. On points, this is just $P \mapsto -(P + \ldots + P)$.

Definition 10. Let $f : A \to B$ be a homomorphism between abelian varieties. We say f is an isogeny if f is surjective and $\ker f$ has dimension 0. Here, $\ker f$ is defined to be the fibre of f over 0 in the sense of algebraic spaces.

Definition 11. Let A be an abelian variety and L an invertible sheaf on A. We say L is *symmetric* if $(-1)_A^* L \cong L$.

Theorem 12. *Let $n \in \mathbb{Z}$. For every invertible sheaf L on an abelian variety A we have*

$$n_A^* L \cong L^{n(n+1)/2} \otimes (-1)_A^* L^{n(n-1)/2}.$$

In particular, if L is symmetric, then $n_A^* L \cong L^{n^2}$.

Proof. [2, Corollary 5.4] or [3, Corollary 2.12]. Both references make use of the "Theorem of the Cube", which is, for instance, [3, Theorem 2.7]. This theorem tells you that given a line bundle L on A, a complicated combination of tensors of this line bundle is trivial on the "cube" $A \times A \times A$. $\square$

We defined abelian varieties to be complete group objects. This implies that they are projective.

Theorem 13. *Every abelian variety is projective.*

Proof. [2, Theorem 6.4]. A very rough proof sketch is to construct a divisor D on A, and then proving that $3 \cdot D$ provides an embedding of A into $\mathbb{P}^n$, for some n. $\square$

The theorem that follows is crucial. It can be found in [2, Theorem 7.2].

Theorem 14. *Let A be an abelian variety of dimension g and $n > 0$. Then n_A is an isogeny of degree n^{2g}. Moreover, if $\mathrm{char}(k) = 0$ then n_A is always étale, and if $\mathrm{char}(k) > 0$, then $\mathrm{char}(k) \nmid n \iff n_A$ is étale.*

Proof. There exists a very ample invertible sheaf L on A [2, 6.4, 6.6]. Now $(-1)_A : A \to A$ is an isomorphism, so $(-1)_A^* L$ is again very ample. Hence $L \otimes (-1)_A^* L$ is also ample. Now we calculate

$$\begin{aligned}(-1)_A^* \left(L \otimes (-1)_A^* L\right) &\cong (-1)_A^* L \otimes (-1)_A^* (-1)_A^* L \\ &\cong (-1)_A^* L \otimes L \\ &\cong L \otimes (-1)_A^* L.\end{aligned}$$

Indeed, $(-1)_A(-1)_A = 1_A$. So the sheaf $L \otimes (-1)_A^* L$ is also symmetric. Denote this sheaf by L again. Then $n_A^* L \cong L^{n^2}$ by theorem 12, again ample. Let $K = \ker n_A$. Then $(n_A^* L)|_K$ is a trivial bundle which is still ample. But if V is any irreducible variety, then $\mathcal{O}_V$ being ample implies that V is a point. It follows that K must consist of a finite number of points, i.e. K is 0-dimensional. So n_A is an isogeny.

Now we determine its degree. Choose an ample symmetric divisor D on A. Then $\deg n_A \cdot (D)^g = (n_A^* D)^g$, by [1, 12.10]. But $n_A^* D$ is linearly equivalent to $n^2 \cdot D$ and so $(n_A^* D)^g = n^{2g} \cdot (D)^g$. We conclude that $\deg n_A = n^{2g}$.

To show that n_A is étale we look at the tangent spaces at the unit element 0 (written additively) of A. This is sufficient, since we can always use translations τ_a. Let $d : A \to \Omega^1_{A/k}$ be the derivation. Denote by T_0A the tangent space of A at 0. If $f, g : A \to B$ are any two homomorphisms of abelian varieties, then

$$d(f +_B g)_0 = (df)_0 +_{T_0B} (dg)_0,$$

in other words $f \mapsto (df)_0$ is a homomorphism. This is not a completely trivial fact; so it's an exercise to check that. In the meantime we conclude that $d(n_A)_0 = n$ (multiplication by the scalar n in T_0A). It's now clear that this is invertible when $\operatorname{char}(k) = 0$ or, when $\operatorname{char}(k) > 0$, if and only if n is not zero in k. $\square$

Definition 15. Let k be *separably closed* and let $\operatorname{char}(k) \nmid n$, $n > 0$. Let A be an abelian variety. We define the *n-torsion subgroup* A_n to be the pullback of n_A along the unique homomorphism $0 \to A$, as in

$$\begin{tikzcd} A_n \arrow[r] \arrow[d] & 0 \arrow[d] \\ A \arrow[r, "n_A"] & A \end{tikzcd}$$

As a representable sheaf, A_n is fully described by the group $A_n(k)$ (see [3, 10.1, 4.48, 3.26]).

By theorem 14, $A_n(k)$ has order n^{2g}. This holds for any $m \mid n$, so by the structure theorem for finite abelian groups,

$$A_n(k) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}.$$

Definition 16. Let k be separably closed. Fix a prime $\ell \neq \operatorname{char}(k)$. We define the *Tate module* of A (with respect to ℓ) as

$$T_\ell A := \varprojlim A_{\ell^n}(k).$$

This is an inverse limit. What this means is that the elements of $T_\ell A$ are infinite sequences $(a_1, a_2, \ldots)$ such that $a_n \in A(k)$ and $\ell_A \cdot a_n = a_{n-1}$, $\ell_A \cdot a_1 = 0$. We have that

$$\begin{aligned} T_\ell A &= \varprojlim A_{\ell^n}(k) \\ &\cong \varprojlim (\mathbb{Z}/\ell^n\mathbb{Z})^{2g} \\ &\cong \left(\varprojlim \mathbb{Z}/\ell^n\mathbb{Z}\right)^{2g} \\ &= \mathbb{Z}_l^{2g}. \end{aligned}$$

Exercise 1. Show that the usual properties of homomorphisms in **Grp** carry over to group objects. That is, show that $f(e_A) = e_B$ and show that $i_B \circ f = f \circ i_A$ if $f : A \to B$ is a homomorphism between group objects A, B in some category **C**. State and prove the first isomorphism theorem.

Exercise 2. Show that the affine line together with addition is a group object with a commutative group law, but is not an abelian variety.

Exercise 3. Show that in fact $a_n \in A_n(k)$ for all $n > 0$ instead of just $a_n \in A(k)$.

Exercise 4. Show that the map $f \mapsto (df)_0$ from the proof of theorem 14 is a homomorphism.

Exercise 5. Let $f : A \to B$ be a morphism between abelian varieties and choose a prime $\ell \nmid \mathrm{char}(k)$. Construct a homomorphism $T_\ell f : T_\ell A \to T_\ell B$ of $\mathbb{Z}_\ell$-modules and show that your construction is functorial.

Exercise 6. Let E be the elliptic curve over $\mathbb{F}_{17}$ given by

$$E : y^2 = x^3 + 13x + 14.$$

Over $\overline{\mathbb{F}}_{17}$ we know that $T_3 E \cong \mathbb{Z}_3^2$. Determine all the torsion points over $\mathbb{F}_{17}$.

References

[1] James S. Milne. Algebraic geometry (v5.00). `www.jmilne.org/math/`, 2005.

[2] James S. Milne. Abelian varieties (v2.00). `www.jmilne.org/math/`, 2008.

[3] Ben Moonen and Gerard van der Geer. Abelian varieties (preliminary version). `www.math.ru.nl/~bmoonen/BookAV`, 2016.