**Math 252: Modular Abelian Varieties, Fall 2003, Prof. William Stein**

# NÉRON MODELS AND THE SHAFAREVICH-TATE GROUP

Tseno V. Tselkov
tselkov@fas.harvard.edu

Abstract. This is a review paper, which establishes the existence of Néron models for elliptic curves and proves a theorem of Mazur relating the Shafarevich-Tate group of an abelian variety to the étale cohomology of its Néron model.

## 1. Introduction

The organization of this paper is the following.

In Section 2, we define the Shafarevich-Tate and the Selmer groups and give some motivation together with the most important facts about them.

Section 3 deals with the basic facts about reductions of elliptic curves.

In Section 4, we define arithmetic surfaces. Then we state a few results about them, which will be key in the sequel. We then move on to define Néron models of elliptic curves. We establish the uniqueness of the Néron model and prove that it behaves well under unramified base extensions.

Section 5 contains a complete proof of the existence of Néron models for elliptic curves. We first show that Néron models exist for elliptic curve with good reduction. Then we show that Néron models also exist in the case when we work over a strictly Henselian discrete valuation ring. Finally, we use faithfully flat descend and gluing to show that Néron models does exist in the general case, when we work over a Dedekind domain.

In Section 6, we give a proof of a theorem of Mazur relating the Shafarevich-Tate group of an abelian variety with the étale cohomology of its Néron model.

## 2. The Shafarevich-Tate and Selmer Groups

Let $E/K$ and $E'/K$ be elliptic curves defined over a number field $K$. Suppose we are given a non-zero isogeny $\phi : E \to E'$ defined over $K$. (The classic example is when $E' = E$ and $\phi = [m]$.) Then we have a natural exact sequence of Galois $G_{\bar{K}/K}$-modules,

$$0 \longrightarrow E[\phi] \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0,$$

where $E[\phi]$ denotes the kernel of $\phi$. Taking its Galois cohomology we obtain a long exact sequence

$$0 \longrightarrow E(K)[\phi] \longrightarrow E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta}$$

$$\xrightarrow{\delta} H^1(G_{\bar{K}/K}, E[\phi]) \longrightarrow H^1(G_{\bar{K}/K}, E) \longrightarrow H^1(G_{\bar{K}/K}, E') \longrightarrow 0$$

From it we directly obtain the fundamental short exact sequence

$$0 \longrightarrow E'(K)/\phi(E(K)) \xrightarrow{\delta} H^1(G_{\bar{K}/K}, E[\phi]) \longrightarrow H^1(G_{\bar{K}/K}, E)[\phi] \longrightarrow 0.$$

For each place $v$, let us fix an extension of $v$ to $\bar{K}$, which gives us an embedding $\bar{K} \subset \bar{K}_v$ and a decomposition group $G_v \subset G_{\bar{K}/K}$. Now $G_v$ clearly acts on $E(\bar{K}_v)$ and $E'(\bar{K}_v)$, so repeating the argument above gives us exact sequences

$$0 \longrightarrow E'(K_v)/\phi(E(K_v)) \xrightarrow{\delta} H^1(G_v, E[\phi]) \longrightarrow H^1(G_v, E)[\phi] \longrightarrow 0.$$

We have the natural inclusions $G_v \subset G_{\bar{K}/K}$ and $E(\bar{K}) \subset E(\bar{K}_v)$ and they give us restriction maps on cohomology as usual. Thus we obtain the following commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E'(K)/\phi(E(K)) & \xrightarrow{\delta} & H^1(G_{\bar{K}/K}, E[\phi]) & \longrightarrow & H^1(G_{\bar{K}/K}, E)[\phi] & \longrightarrow & 0. \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \prod_v E'(K_v)/\phi(E(K_v)) & \xrightarrow{\delta} & \prod_v H^1(G_v, E[\phi]) & \longrightarrow & \prod_v H^1(G_v, E)[\phi] & \longrightarrow & 0.
\end{array}$$

Now the following definitions come naturally

**Definition 1.** *Let $\phi : E/K \to E'/K$ be an isogeny as above. The Shafarevich-Tate group of $E/K$ is the subgroup of $H^1(G_v, E)$ defined by*

$$Ш(E/K) = \ker\left(H^1(G_{\bar{K}/K}, E) \to \prod_v H^1(G_v, E)\right).$$

*The $\phi$-Selmer group $E/K$ is the subgroup of $H^1(G_{\bar{K}/K}, E[\phi])$ defined by*

$$S^{(\phi)} = \ker\left(H^1(G_{\bar{K}/K}, E[\phi]) \to \prod_v H^1(G_v, E)\right).$$

**Remark 1.** *The groups $Ш(E/K)$ and $S^{(\phi)}(E/K)$ depend only on $E$ and $K$, and not on the extensions of $v$ to $\bar{K}$.*

The commutative diagram above and the definitions directly give us the following fact.

**Proposition 1.** *Let $\phi : E/K \to E'/K$ be an isogeny of elliptic curves defined over $K$. Then there is an exact sequence*

$$0 \to E'(K)/\phi(E(K)) \to S^{(\phi)}(E/K) \to Ш(E/K)[\phi] \to 0.$$

**Remark 2.** *It is well-known that $H^1(G_{\bar{K}/K})$ can be identified with the Weil-Châtelet group $WC(E/K)$ of equivalence classes of homogeneous spaces (or torsors) for $E/K$. Then we can view the Shafarevich-Tate group as the group of homogeneous spaces which have a $K_v$-rational point for every place $v$, i.e. $Ш(E/K)$ is the group of homogeneous spaces which are everywhere locally trivial modulo equivalence.*

The following theorem asserts the finiteness of the Selmer group, which is not hard to establish. For a complete proof we refer the reader to [6], Theorem 4.2.

**Theorem 1.** *Let $\phi : E/K \to E'/K$ be an isogeny of elliptic curves defined over $K$. Then the Selmer group $S^{(\phi)}(E/K)$ is finite.*

On the contrary, the finiteness of the Shafarevich-Tate group is among the open problems in mathematics. The famous conjecture due to Birch and Swinnerton-Dyer asserts that it is also finite.

**Conjecture 1.** *Let $E/K$ be an elliptic curve. The the Shafarevich-Tate group $Ш(E/K)$ is finite.*

## 3. Reduction of Elliptic Curves

Let $K$ be a local field, $R$ - its ring of integers, $\pi$ - an uniformizer for $R$, and $k$ - the residue field of $R$.

Suppose we are given an elliptic curve $E/K$ with Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

**Definition 2.** *Let $E/K$ be an elliptic curve. A Weierstrass equation as above is called a minimal Weierstrass equation for $E$ if $v(\Delta)$ is minimal subject to $a_1, a_2, a_3, a_4, a_6 \in R$.*

It is quite easy to show that every elliptic curve has a minimal Weierstrass equation.

**Proposition 2.** *Every elliptic curve has a minimal Weierstrass equation.*

*Proof.* We can certainly find a Weierstrass equation with all $a_i \in R$. Among those there is a minimal $v(\Delta)$ since $v$ is discrete. □

Now let us consider the natural reduction map $R \to R/\pi R$ denoted by $t \mapsto \tilde{t}$. Having chosen a minimal Weierstrass equation for $E/K$, we can reduce its coefficients modulo $\pi$ to obtain a curve over $k$, namely

$$\tilde{E} : y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6}.$$

**Definition 3.** *The curve $\tilde{E}/k$ is called the reduction of $E$ modulo $\pi$.*

**Remark 3.** *It is not hard to show that the minimality condition on the equation for $E$ implies that the equation for $\tilde{E}$ is unique up to the standard change of coordinates.*

Now let $P \in E(K)$. We can find homogeneous coordinates $P = [x_0, y_0, z_0]$ with $x_0, y_0, z_0 \in R$ and at least one of them in $R^\times$. Then the reduced point $\tilde{P} = [\tilde{x_0}, \tilde{y_0}, \tilde{z_0}]$ clearly is in $\tilde{E}(\mathrm{k})$. Thus we obtain a reduction map

$$E(K) \to \tilde{E}(k), \quad P \mapsto \tilde{P}.$$

The reduced curve $\tilde{E}/k$ may or may not be singular. In fact it might be one of three types and we classify $E$ according to these possibilities.

**Definition 4.** *Let $E/K$ be an elliptic curve and let $\tilde{E}$ be the reduced curve for a minimal Weierstrass equation.*
*(a) $E$ has good (or stable) reduction over $K$ if $\tilde{E}$ is non-singular.*
*(b) $E$ has multiplicative (or semi-stable) reduction over $K$ if $\tilde{E}$ has a node.*
*(c) $E$ has additive (or unstable) reduction over $K$ if $\tilde{E}$ has a cusp.*
*In cases (b) and (c) $E$ is said to have bad reduction.*

**Remark 4.** *It is a standard fact how the reduction type can be read off from a minimal Weierstrass equation. For a precise explanation the reader can consult [6], Proposition 5.1.*

## 4. Arithmetic Surfaces and Properties of Néron Models

To even define Néron models for elliptic curves we shall need some preliminaries on arithmetic surfaces. To simplify the discussion we shall make the following convention: All Dedekind domains and all discrete valuation rings have perfect residue fields. Let $R$ be a Dedekind domain. Intuitively, an arithmetic surface is an $R$-scheme $\mathcal{C} \to \mathrm{Spec}(R)$ whose fibers are curves.

**Definition 5.** *Let $R$ be a Dedekind domain with fraction field $K$. An arithmetic surface (over $R$) is an integral, normal, excellent scheme $\mathcal{C}$, which is flat and of finite type over $R$, and whose generic fiber is a non-singular connected projective curve $C/K$ and whose special fibers are unions of curves over the appropriate residue fields.*

**Remark 5.** *The special fibers may be reducible or singular or even non-reduced.*

In the sequel, we shall use the following key results about arithmetic surfaces, the proofs of which can be found in [5], Chapter 4, Section 4.

**Proposition 3.** *Let $R$ be a Dedekind domain with fraction field $K$, let $\mathcal{C}/R$ be an arithmetic surface, and let $C/K$ be the generic fiber of $\mathcal{C}$.*
*(a) If $\mathcal{C}$ is proper over $R$, then $C(K) = \mathcal{C}(R)$.*
*(b) Suppose that the scheme $C$ is regular, and let $\mathcal{C}^0 \subset \mathcal{C}$ be the largest subscheme of $\mathcal{C}$ such that the map $\mathcal{C}^0 \to Spec R$ is a smooth morphism. Then $\mathcal{C}(R) = \mathcal{C}^0(R)$.*

**Theorem 2.** *Let $R$ be a Dedekind domain with fraction field $K$, and let $C/K$ be a non-singular projective curve of genus $g$.*
*(a) (Resolution of Singularities for Arithmetic Surfaces) There exists a regular arithmetic surface $\mathcal{C}/R$, proper over $R$, whose generic fiber is isomorphic*

*to $C/K$. We call $\mathcal{C}/R$ a proper regular model for $C/K$.*
*(b) (Minimal Models Theorem) Assume that $g \geq 1$. Then there exists a proper regular model $\mathcal{C}^{\min}/R$ for $C/K$ with the following minimality property: Let $\mathcal{C}/R$ be any other proper regular model for $C/K$. Fix an isomorphism from the generic fiber of $\mathcal{C}$ to the generic fiber of $\mathcal{C}^{\min}$. Then the induced birational map $\mathcal{C} \to \mathcal{C}^{\min}$ is an $R$-isomorphism. We call $\mathcal{C}^{\min}$ the minimal regular model for $C/K$. It is unique up to unique $R$-isomorphism.*

We can now move on to defining Néron models and giving their basic properties. Suppose we have a discrete valuation ring $R$ with fraction field $K$. Intuitively, the Néron model of an elliptic curve $E/K$ is an arithmetic surface $\mathcal{E}/R$ whose generic fiber is the given elliptic curve.

**Definition 6.** *Let $R$ be a Dedekind domain with fraction field $K$, and let $E/K$ be an elliptic curve. A Néron model for $E/K$ is a smooth group scheme $\mathcal{E}/R$ whose generic fiber is $E/K$ and which satisfies the following universal property (Néron Mapping Property):*
*Let $\mathcal{X}/R$ be a smooth $R$-scheme with generic fiber $X/K$, and let $\phi_K : X_{/K} \to E_{/K}$ be a rational map defined over $K$. Then there exists a unique $R$-morphism $\phi_R : \mathcal{X}_{/R} \to \mathcal{E}_{/R}$ extending $\phi_K$.*

**Remark 6.** *The most natural and important instance of the Néron mapping property is the case $\mathcal{X} = Spec(R)$ and $X = Spec(K)$. Then the set of $K$-maps $X_{/K} \to E_{/K}$ is the group of $K$-rational points $E(K)$, and the set of $R$-morphisms $\mathcal{X}_{/R} \to \mathcal{E}_{/R}$ is the group of sections $\mathcal{E}(R)$. In this situation the Néron mapping property asserts that the natural inclusion $\mathcal{E}(R) \hookrightarrow E(K)$ is a bijection.*

We shall now present some of the more important properties of Néron models and we start with uniqueness.

**Proposition 4.** *Let $R$ be a Dedekind domain with fraction field $K$, and let $E/K$ be an elliptic curve. Suppose that $\mathcal{E}_1/R$ and $\mathcal{E}_2/R$ are Néron models for $E/K$. Then there exists a unique $R$-isomorphism $\psi : \mathcal{E}_1/R \to \mathcal{E}_2/R$ whose restriction to the generic fiber is the identity map on $E/K$. In other words, the Néron model of $E/K$ is unique up to unique isomorphism.*

*Proof.* The identity map $E/K \to E/K$ is a rational map from the generic fiber of $\mathcal{E}_1$ to the generic fiber of $\mathcal{E}_2$, and $\mathcal{E}_1$ is smooth over $R$, so the Néron mapping property for $\mathcal{E}_2$ asserts that the identity map extends uniquely to an $R$-morphism $\varphi : \mathcal{E}_1/R \to \mathcal{E}_2/R$. Similarly, exchanging the places of $\mathcal{E}_1$ and $\mathcal{E}_2$ we obtain a unique $R$-morphism $\phi : \mathcal{E}_2/R \to \mathcal{E}_1/R$ which is the identity on the generic fiber. But then both $\phi \circ \varphi : \mathcal{E}_1 \to \mathcal{E}_1$ and the identity map $\mathcal{E}_1 \to \mathcal{E}_1$ are $R$-morphisms that are the same (identity) map on the generic fiber, so the uniqueness part of the Néron mapping property asserts that $\phi \circ \varphi$ equals the identity map. Thus, $\phi$ and $\varphi$ are isomorphisms. □

Néron models also behave well under unramified base extension.

**Proposition 5.** *Let $R$ be a Dedekind domain with fraction field $K$, and let $E/K$ be an elliptic curve. Let $K'/K$ be a finite unramified extension, and let $R'$ be the integral closure of $R$ in $K'$. Let $\mathcal{E}/R$ be a Néron model for $E/K$. Then $\mathcal{E} \times_R R'$ is a Néron model for $E/K'$.*

*Proof.* Let $\mathcal{X}'/R'$ be a smooth $R'$-scheme with generic fiber $X'/K'$ and let $\phi_{K'} : X'_{K'} \to E_{/K'}$ be a rational map. Let us consider the composition

$$\mathcal{X}' \to \mathrm{Spec}R' \to \mathrm{Spec}R.$$

It makes $\mathcal{X}'$ into an $R$-scheme. Moreover, the assumptions on $K'$ imply that the map $\mathrm{Spec}R' \to \mathrm{Spec}R$ is a smooth morphism and hence the composition is a smooth morphism, so $\mathcal{X}'$ is a smooth $R$-scheme.

Now the Néron mapping property for $\mathcal{E}/R$ tells us that there is an $R$-morphism $\phi_R : \mathcal{X}' \to \mathcal{E}$, whose restriction to the generic fiber is the composition

$$X' \xrightarrow{\phi_{K'}} E \times_K K' \xrightarrow{p_1} E.$$

To establish the existence part of the Néron mapping property note that the two $R$-morphisms $\phi_R : \mathcal{X}' \to \mathcal{E}$ and $\mathcal{X}' \to \mathrm{Spec}R'$ determine an $R$-morphism (and thus an $R'$-morphism) to the fiber product $\phi_{R'} : \mathcal{X}' \to \mathcal{E} \times_R R'$, which is unique, so $\mathcal{E} \times_R R'$ is a Méron model for $E/K'$. □

## 5. Existence of Néron Models

The goal of this section is to prove the existence of a Néron model for elliptic curves.

**Theorem 3.** *Let $R$ be a Dedekind domain with fraction field $K$, let $E/K$ be an elliptic curve, let $\mathcal{C}/R$ be a minimal proper regular model for $E/K$ as in Theorem 2, and let $\mathcal{E}/R$ be the largest subscheme of $\mathcal{C}/R$ which is smooth over $R$. Then $\mathcal{E}/R$ is a Néron model for $E/K$.*

The proof involves numerous steps. We start with the following local statement that over a discrete valuation ring asserts the existence of a group scheme with generic fiber a given elliptic curve.

**Proposition 6.** *Let $R$ be a discrete valuation ring with fraction field $K$, let $E/K$ be an elliptic curve, and choose a Weierstrass equation for $E/K$ with coefficients in $R$,*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

*This Weierstrass equation defines a scheme $\mathcal{W} \subset \mathbb{P}^2_R$. Let $\mathcal{W}^0 \subset \mathcal{W}$ be the largest subscheme of $W$ which is smooth over $R$.*
*(a) Both $\mathcal{W}/R$ and $\mathcal{W}^0/R$ have generic fiber $E/K$.*
*(b) The natural map $\mathcal{W}(R) \to E(K)$ is a bijection. If $\mathcal{W}$ is regular, then the natural map $\mathcal{W}^0(R) \to \mathcal{W}(R)$ is also bijection, so in this case there is natural identification $\mathcal{W}^0(R) = E(K)$.*
*(c) The addition and negation maps on $E$ extend to $R$-morphisms $\mathcal{W}^0 \times_R \mathcal{W}^0 \to \mathcal{W}^0$ and $\mathcal{W}^0 \to \mathcal{W}^0$, which make $\mathcal{W}^0$ into a group scheme over $R$.*

**Remark 7.** *If $E/K$ has good reduction and if we take a minimal Weierstrass equation for $E/K$, then $\mathcal{W}$ itself is smooth over $R$. Thus in this case the above theorem asserts that $\mathcal{W} = \mathcal{W}^0$ is a group scheme over $R$.*

**Remark 8.** *If $E/K$ has bad reduction, then there is exactly one singular point on the reduction $\tilde{E}$ (mod $\wp$). In other words, the special fiber $\tilde{\mathcal{W}}$ of $\mathcal{W}$ contains exactly one singular point, say $\gamma \in \tilde{\mathcal{W}} \subset \mathcal{W}$. Then $\mathcal{W}^0 = \mathcal{W} - \{\gamma\}$. In particular, $\mathcal{W}^0$ and $\mathcal{W}$ have the same generic fiber.*

*Proof.* (a) $\mathcal{W}$ is the closed subscheme of $\mathbb{P}^2_R = \mathrm{Proj} R[X,Y,Z]$ defined by the single homogeneous equation

$$\mathcal{W} : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Its generic fiber is the variety in $\mathbb{P}^2_K$ defined by the same equation. Thus, the generic fiber of $\mathcal{W}$ is exactly $E/K$. $\mathcal{W}^0$ has the same generic fiber, so this completes part (a).

(b) Since $\mathcal{W}$ is a closed subscheme of $\mathbb{P}^2_R$ then it is certainly proper over $R$. This allows us to apply Proposition 3 to conclude that $E(K) = \mathcal{W}(R)$, which is the first part of (b). If in addition $\mathcal{W}$ is regular, then again by Proposition 3 we get that $\mathcal{W}(R) = \mathcal{W}^0(R)$, which implies $E(K) = \mathcal{W}^0(R)$.

(c) The proof of this part is quite explicit and rather long computation, so we refer the reader to [5], Theorem 5.3.(c) for all details. □

The next ingredient in the proof is the following generalization of a theorem of Weil. Weil's theorem asserts that a rational map from a smooth variety to a complete group variety is automatically a morphism, and Artin has extended it to a scheme-theoretic setting.

**Proposition 7.** *Let $R$ be a Dedekind domain, let $G/R$ be a group scheme over $R$, let $\mathcal{X}/R$ be a smooth $R$-scheme, and let $\phi : \mathcal{X} \to G$ be a rational map over $R$. Write $\mathrm{Dom}(\phi)$ for the domain of $\phi$, and suppose that $\mathrm{Dom}(\phi)$ is dense in every fiber of $\mathcal{X}/R$.*
*(a) The complement $\mathcal{X} - \mathrm{Dom}(\phi)$ is a subscheme of $\mathcal{X}$ of pure codimension one.*
*(b) If $G$ is proper over $R$, then $\mathrm{Dom}(\phi) = \mathcal{X}$. In other words, $\phi$ is a morphism.*

*Proof.* Following [5] we shall phrase our exposition in terms of points, but to be completely rigorous, our "points" should be $T$-valued points for arbitrary $R$-schemes $T$.

Let us consider the rational map

$$F : \mathcal{X} \times_R \mathcal{X} \to G, \quad F(x,y) = \phi(x)\phi(y)^{-1}.$$

We claim that there is a natural identification

$$\mathrm{Dom}(\phi) \longleftrightarrow \Delta \cap \mathrm{Dom}(F), \quad x \longleftrightarrow (x,x),$$

where $\Delta$ is the diagonal in $\mathcal{X} \times_R \mathcal{X}$. Indeed, if $x \in \mathrm{Dom}(\phi)$ then $F(x,x) = \phi(x)\phi(x)^{-1}$ is defined, so $(x,x) \in \mathrm{Dom}(F)$. Conversely, if $(x,x) \in \mathrm{Dom}(F)$

we need to show that $x \in \mathrm{Dom}(\phi)$. Firstly, since $\mathrm{Dom}(F)$ is open, there is a non-empty open set $U \subset \mathcal{X}$ such that $x \times_R U \subset \mathrm{Dom}(F)$. Secondly, since $\mathrm{Dom}(\phi)$ is open, there is a point $y \in U \cap \mathrm{Dom}(\phi)$, which means that $\phi(x) = F(x,y)\phi(y)$, so $x \in \mathrm{Dom}(\phi)$ and the claim is proved.

Let $K(\mathcal{X} \times \mathcal{X})$ be the function field of the scheme $\mathcal{X} \times_R \mathcal{X}$, and let $\mathcal{O}_{G,0}$ be the local ring of $G$ along with the identity section, i.e. $\mathcal{O}_{G,0}$ is the ring of rational functions on $G$ which are well-defined at some point of the image of the map $\sigma_0 : \mathrm{Spec}R \to G$, where $\sigma_0$ is the identity element of the group scheme $G$.

Then we clearly get a ring homomorphism

$$F^* : \mathcal{O}_{G,0} \to K(\mathcal{X} \times \mathcal{X}), \quad f \mapsto f \circ F.$$

Our next goal is to show that

$$x \in \mathrm{Dom}(\phi) \Leftrightarrow (x,x) \in \mathrm{Dom}(F^* f) \text{ for all } f \in \mathcal{O}_{G,0}.$$

Indeed, let $f \in \mathcal{O}_{G,0}$ and suppose $x \in \mathrm{Dom}(\phi)$. Then $(x,x) \in \mathrm{Dom}(F)$ by the claim proven above, and since $F(x,x) = \phi(x)\phi(x)^{-1}$ is the identity element of $G$, then $F^*(f)$ is defined at $(x,x)$. Conversely, if $F^*(f) = f \circ F$ is defined at $(x,x)$ for all functions $f \in \mathcal{O}_{G,0}$, then $F$ must be defined at $(x,x)$. Thus we get that

$$x \in \mathrm{Dom}(\phi) \Leftrightarrow (x,x) \in \mathrm{Dom}(F^* f) \text{ for all } f \in \mathcal{O}_{G,0} \Leftrightarrow F^*(\mathcal{O}_{G,0}) \subset \mathcal{O}_{\mathcal{X}\times\mathcal{X},(x,x)},$$

where $\mathcal{O}_{\mathcal{X}\times\mathcal{X},(x,x)} \subset K(\mathcal{X} \times \mathcal{X})$ is the local ring of $\mathcal{X} \times_R \mathcal{X}$ at $(x,x)$.

The scheme $\mathcal{X} \times_R \mathcal{X}$ is smooth over $R$, so in particular it is normal. This implies that a function $f \in K(\mathcal{X} \times \mathcal{X})$ will be defined at $(x,x)$ unless its polar divisor $\mathrm{div}_\infty(f)$ goes through $(x,x)$. In other words,

$$\mathcal{O}_{\mathcal{X}\times\mathcal{X},(x,x)} = \{g \in K(\mathcal{X} \times \mathcal{X})^* : (x,x) \notin \mathrm{div}_\infty(g)\} \cup \{0\}.$$

This together with the result above describing the domain of $\phi$ gives us

$$\begin{aligned} \mathcal{X} - \mathrm{Dom}(\phi) &= \{x \in \mathcal{X} : F^*(\mathcal{O}_{G,0}) \not\subset \mathcal{O}_{\mathcal{X}\times\mathcal{X},(x,x)}\} \\ &= \{x \in \mathcal{X} : (x,x) \in \mathrm{div}_\infty(F^* f) \text{ for some } f \in \mathcal{O}_{G,0}\} \\ &\cong \Delta \cap \bigcup_{f \in \mathcal{O}_{G,0}} \mathrm{div}_\infty(F^* f) \\ &= \bigcup_{f \in \mathcal{O}_{G,0}} (\Delta \cap \mathrm{div}_\infty(F^* f)). \end{aligned}$$

The diagonal $\Delta$ is a complete intersection in $\mathcal{X} \times_R \mathcal{X}$, and each divisor $\mathrm{div}_\infty(F^* f)$ has pure codimension one in $\mathcal{X} \times_R \mathcal{X}$, so each of the intersections $\Delta \cap \mathrm{div}_\infty(F^* f)$ has pure codimension one in $\Delta$. It follows that the union over $f \in \mathcal{O}_{G,0}$ also has pure codimension one since we know a priori that it is a proper closed subset of $\Delta$. Thus, the proof of (a) is completed.

(b) We shall use the following lemma asserting that a rational map from a smooth scheme to a proper scheme is defined off of a subset of codimension at least two. Then this lemma together with part (a) directly give us (b).

**Lemma 1.** *Let $R$ be a Dedekind domain, let $\mathcal{X}/R$ be a smooth $R$-scheme, let $\mathcal{Y}/R$ be a proper $R$-scheme, and let $\phi : \mathcal{X} \to \mathcal{Y}$ be a dominant rational map defined over $R$. Then every component of $\mathcal{X} - Dom(\phi)$ has codimension at least two in $\mathcal{X}$.*

*Proof.* Let $\mathcal{Z} \subset \mathcal{X}$ be an irreducible subscheme of codimension one in $\mathcal{X}$. We need to show that $\phi$ is defined at the generic point of $\mathcal{Z}$, i.e. $\phi$ is defined on a non-empty open subset of $\mathcal{Z}$. Let us consider the local ring $\mathcal{O}_{\mathcal{X},\mathcal{Z}}$ of $\mathcal{X}$ at $\mathcal{Z}$. It is a discrete valuation ring since it is local ring of dimension one, which is regular since $\mathcal{X}/R$ is smooth.

Now, the dominant map induces a morphism $\mathrm{Spec}K(\mathcal{X}) \to \mathrm{Spec}K(\mathcal{Y})$ from the generic point of $\mathcal{X}$ to the generic point of $\mathcal{Y}$. Thus we obtain the following commutative diagram

$$\begin{array}{ccc} \mathcal{X} & \xrightarrow{\phi} & \mathcal{Y} \\ \uparrow & & \uparrow \\ \mathrm{Spec}\mathcal{O}_{\mathcal{X},\mathcal{Z}} & & \\ \uparrow & & \uparrow \\ \mathrm{Spec}K(\mathcal{X}) & \longrightarrow & \mathrm{Spec}K(\mathcal{Y}), \end{array}$$

The discrete valuation ring $\mathcal{O}_{\mathcal{X},\mathcal{Z}}$ has fraction field $K(\mathcal{X})$ and since $\mathcal{Y}$ is proper over $R$, by the valuative criterion of properness ([2], Theorem 4.7.) we get that the rational map

$$\mathrm{Spec}\mathcal{O}_{\mathcal{X},\mathcal{Z}} \to \mathcal{X} \to \mathcal{Y}$$

extends to a morphism $\mathrm{Spec}\mathcal{O}_{\mathcal{X},\mathcal{Z}} \to \mathcal{Y}$. This means that $\phi$ is defined at the generic point of $\mathcal{Z}$, which is what we needed to complete the proof of the lemma and the theorem. □

□

Combining the results of the last two Propositions 6 and 7 we can establish the existence of Néron models for elliptic curves with good reduction.

**Corollary 1.** *Let $R$ be a Dedekind domain with fraction field $K$, let $E/K$ be an elliptic curve given by a Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

*having coefficients in $R$, and let $\mathcal{W} \subset \mathbb{P}^2_R$ be the closed subscheme of $\mathbb{P}^2_R$ defined by this Weierstrass equation. Suppose that $\mathcal{W}$ is smooth over $R$ or, equivalently, that the Weierstrass equation has good reduction at every prime of $R$. Then $\mathcal{W}/R$ is a Néron model for $E/K$.*

*Proof.* By Proposition 6 the addition law on $E/K$ extends to make $\mathcal{W}$ into a group scheme over the localization (which is a discrete valuation ring) of $R$ at each of its prime ideals. Moreover, since these group laws are given by the same equations, they together make $\mathcal{W}$ into a group scheme over $R$.

We only need to also verify that $\mathcal{W}$ has the Néron mapping property. Let $\mathcal{X}/K$ be a smooth $R$-scheme with generic fiber $X/K$, take any rational map $\phi_K : X_{/K} \to E_{/K}$ defined over $K$, and let $\phi : \mathcal{X} \to \mathcal{W}$ be the associated rational map over $R$. Now $\mathcal{W}$ is a closed subscheme of $\mathbb{P}^2_R$ and thus is proper over $R$, so by Proposition 7 the map $\phi$ extends to a morphism, which establishes the Néron mapping property. So, $\mathcal{W}/R$ is indeed a Néron model for $E/K$. □

Unfortunately, we cannot hope to have good reduction at every prime. The strategy to go around that is the folowing. Firstly, prove Theorem 3 for strictly Henselian discrete valuation rings. Secondly, descend from the strict Henselization of a discrete valuation ring down to the ring itself and thirdly, glue the Néron models over discrete valuation rings to get a Néron model over a Dedekind domain.

For completeness let us say the basics of Henselian rings.

**Definition 7.** *A discrete valuation ring $R$ is called Henselian if it satisfies Hensel's lemma, i.e. $R$ is Henselian if for any monic polynomial $f(x) \in R[x]$ and any element $a \in R$ satisfying*

$$f(a) \equiv 0 (mod\ \wp), \quad f'(a) \neq 0 (mod\ \wp),$$

*there exists a unique element $\alpha \in R$ satisfying*

$$\alpha \equiv a (mod\ \wp), \quad f(\alpha) = 0.$$

*The ring $R$ is called strictly Henselian if it is Henselian and if its residue field $k = R/\wp$ is algebraically closed (recall that we work only with perfect residue fields).*

It is a well-known fact that every discrete valuation ring $R$ can be embedded in a minimal Henselian and minimal strictly Henselian ring in the following sense

**Proposition 8.** *Let $R$ be a discrete valuation ring.*
*(a) A local homomorphism $R \to R^h$ with $R^h$ Henselian is called a Henselization of $R$ if any other local homomorphism $R \to R'$ with $R'$ Henselian factors uniquely into $R \to R^h \to R'$. The Henselization exists.*
*(b) A local homomorphism $R \to R^{sh}$ with $R^{sh}$ strictly Henselian with residue field $k^{sh}$ is called a strict Henselization of $R$ if any other local homomorphism from $R$ into a strictly Henselian ring $R'$ with residue field $k'$ extends to $R^{sh}$, and, moreover, the extension is uniquely determined once the map $k^{sh} \to k'$ on residue fields has been specified. The strict Henselization exists.*

**Remark 9.** *Proposition 6.5. in [5] gives an explicit description of $R^h$ and $R^{sh}$, which we will not need for our purposes.*

We are now going to prove that the scheme $\mathcal{E}$ from Theorem 3 is a Néron model for $E$ provided that we work over a strictly Henselian discrete valuation ring and the group law of $E/K$ extends to make $\mathcal{E}$ into a group scheme over $R$.

**Proposition 9.** *Let $R$ be a strictly Henselian discrete valuation ring with fraction field $K$, let $E/K$ be an elliptic curve, let $\mathcal{C}/R$ be a minimal proper regular model for $E/K$, and let $\mathcal{E}/R$ be the largest subscheme of $\mathcal{C}/R$ which is smooth over $R$. If the group law on $E/K$ extends to make $\mathcal{E}$ into a group scheme over $R$, then $\mathcal{E}/R$ is a Néron model for $E/K$.*

*Proof.* We need to verify the Néron mapping property, so let $\mathcal{X}/R$ be a smooth $R$-scheme with generic fiber $X/K$, and let $\phi_K : X \to E$ be a rational map. We need to show that $\phi_K$ extends to a morphism $\mathcal{X} \to \mathcal{E}$.

We can apply Proposition 7 with $R = K$, since $E$ is clearly a proper group scheme over $K$ and $X$ is smooth over $K$, to get directly that $\phi_K$ is a morphism $X \to E$. So, the rational map $\phi : \mathcal{X} \to \mathcal{E}$ induced by $\phi_K$ is a morphism on the generic fiber.

To prove that $\phi$ is a morphism, let us assume the contrary and get a contradiction. As we assumed in the statement of the theorem $\mathcal{E}$ is a group scheme, so we can apply Proposition 7 to get that the set of points where the rational map $\phi$ is not defined is a set of pure codimension one in $\mathcal{X}$. Hence these is an irreducible closed subscheme $\mathcal{Z} \subset \mathcal{X}$ such that $\phi$ is not defined on the generic point $\eta_{\mathcal{Z}}$ of $\mathcal{Z}$. From algebraic geometry, since $\mathcal{X}$ is regular and $\mathcal{Z}$ is of codimension one, the local ring $\mathcal{O}_{\mathcal{X},\mathcal{Z}}$ is a discrete valuation ring and $\eta_{\mathcal{Z}} = \mathrm{Spec}\mathcal{O}_{\mathcal{X},\mathcal{Z}}$. Thus, we obtain the following diagram

$$\begin{array}{ccccc}
\mathcal{X} & \xrightarrow{\phi} & \mathcal{E} & \xrightarrow{\subset} & \mathcal{C} \\
\uparrow & & \uparrow & & \uparrow \\
\eta_{\mathcal{Z}} = \mathrm{Spec}\mathcal{O}_{\mathcal{X},\mathcal{Z}} & & & & \\
\uparrow & & \uparrow & & \uparrow \\
\mathrm{Spec}K(\mathcal{X}) & \xrightarrow{\phi_K} & \mathrm{Spec}K(\mathcal{E}) & \xrightarrow{=} & \mathrm{Spec}K(\mathcal{C}).
\end{array}$$

Now the scheme $\mathcal{C}$ is proper over $R$ and $\mathcal{O}_{\mathcal{X},\mathcal{Z}}$ is a discrete valuation ring, so by the valuative criterion of properness ([2], Theorem 4.7.) we have that $\phi$ extends to a morphism $\phi : \eta_{\mathcal{Z}} \to \mathcal{C}$. In other words, if we are mapping to the larger scheme $\mathcal{C}$, then $\phi$ is defined generically on $\mathcal{Z}$.

However, we area assuming that $\phi : \mathcal{X} \to \mathcal{E}$ does not extend generically to $\mathcal{Z}$, or equivalently that $\phi(\eta_{\mathcal{Z}}) \in \mathcal{C}$ is not contained in $\mathcal{E}$. In particular, if $k$ is the residue field of $R$ and $x_0 \in \mathcal{Z}(k)$ is such that $\phi : \mathcal{X} \to \mathcal{C}$ is defined at $x_0$, then $\phi(x_0) \notin \mathcal{E}$.

Since $R$ is strictly Henselian, by [5], Proposition 6.4., the set of $R$-valued points $\mathcal{X}(R)$ maps to a dense set of points in the special fiber of $\mathcal{X}$. In particular, we can find a point $x \in \mathcal{X}(R)$ which intersects $\mathcal{Z}$ at a point,

call it $x_0 \in \mathcal{Z}(k)$, at which the map $\phi : \mathcal{X} \to \mathcal{C}$ is defined. Composing $x$ with $\phi$ we obtain a rational map $\mathrm{Spec}R \to \mathcal{C}$, which by the valuative criterion of properness extends to a morphism $\mathrm{Spec}R \to \mathcal{C}$. On the other hand $\phi \circ x \in \mathcal{C}(R)$ and by our construction we have $\phi \circ x \notin \mathcal{E}(R)$. However, by Proposition 3 we have that $\mathcal{C}(R) = \mathcal{E}(R)$, so we have a contradiction. Thus $\phi$ extends to a morphism $\mathcal{X} \to \mathcal{E}$, and so $\mathcal{E}$ has the Néron mapping property. □

The next result completes the proof that $\mathcal{E}/R$ is a Néron model for $E/K$ at least over strictly Henselian discrete valuation ring. For a complete proof we refer to [5], Proposition 6.10.

**Proposition 10.** *Let $R$ be a strictly Henselian discrete valuation ring with fraction field $K$, let $E/K$ be an elliptic curve, let $\mathcal{C}/R$ be a minimal proper regular model for $E/K$, and let $\mathcal{E}/R$ be the largest subscheme of $\mathcal{C}/R$ which is smooth over $R$. Then the group law on $E/K$ extends to make $\mathcal{E}$ into a group scheme over $R$.*

We are now ready to prove the existence of Néron models for elliptic curves over Dedekind domains, i.e. to prove Theorem 3.

*Proof of Theorem 3.* If $R$ is strictly Henselian $\mathcal{E}/R$ is a Néron model for $E/K$ by Proposition 9 and Proposition 10.

Otherwise, let us suppose first that $R$ is a discrete valuation ring, and let $R^{sh}$ be the strict Henselization of $R$. Then we claim that $\mathcal{C}^{sh} = \mathcal{C} \times_R R^{sh}$ is a minimal proper regular model for $E/R^{sh}$. Indeed, $\mathcal{C}^{sh}$ is proper over $R^{sh}$ since proper morphism are stable under base extension. Next, $\mathcal{C}^{sh}$ is regular since $\mathcal{C}$ is regular and $R^{sh}$ is flat and unramified over $R$. Finally, the minimality of $\mathcal{C}^{sh}$ is a consequence of the construction of the minimal proper regular model in terms of a regular model with all exceptional curves blown down.

Now let $\mathcal{E}^{sh} = \mathcal{E} \times_R R^{sh}$. Then $\mathcal{E}^{sh}$ is the largest open subscheme of $\mathcal{C}^{sh}$ which is smooth over $R^{sh}$. Thus, $\mathcal{E}^{sh}/R^{sh}$ is a Néron model for $E/K^{sh}$ by the previous case. We shall use this to prove that $\mathcal{E}/R$ is a Néron model for $E/K$.

We need to verify that $\mathcal{E}/R$ has the Néron mapping property. Let $\mathcal{X}/R$ be a smooth $R$-scheme with generic fiber $X/K$ and let $\phi_K : X_{/K} \to E_{/K}$ be a rational map defined over $K$. We need to show that $\phi_K$ extends to a unique $R$-morphism $\mathcal{X} \to \mathcal{E}$. Let us consider the extension of $\mathcal{X}$ and $\phi_K$ to $R^{sh}$, let $\mathcal{X}^{sh} = \mathcal{X} \times_R R^{sh}$ and $\phi_K^{sh} : X^{sh}_{/K^{sh}} \to E_{/K^{sh}}$. Then the scheme $\mathcal{X}^{sh}$ is smooth over $R^{sh}$ since smoothness is closed under base change, so by the Néron mapping property for $\mathcal{E}^{sh}$ we have that $\phi_K^{sh}$ extends to a unique morphism $\phi_R^{sh} : \mathcal{X}^{sh}_{/R^{sh}} \to \mathcal{E}^{sh}_{/R^{sh}}$. Thus we obtain the following commutative

diagram

$$\begin{array}{ccc} \mathcal{X}^{sh} & \xrightarrow{\phi_R^{sh}} & \mathcal{E}^{sh} \\ \downarrow & & \downarrow \\ \mathcal{X} & \xrightarrow{\phi_K} & \mathcal{E}, \end{array}$$

where the top row is obtained from the bottom row using the base extension $\mathrm{Spec}R^{sh} \to \mathrm{Spec}R$. The strict Henselization $R^{sh}$ is faithfully flat over $R$ (see [1], 2.4, corollary 9), so we are exactly in a situation to apply faithfully flat descent (see [1], Chapter 6) to conclude that the rational map on the bottom row is, in fact, a morphism. Therefore $\mathcal{E}/R$ has the Néron mapping property, so $\mathcal{E}/R$ is a Néron model for $E/K$ in the case when $R$ is a discrete valuation ring.

Let us now consider the general case when $R$ is a Dedekind domain. By our previous considerations for each prime $\wp \in \mathrm{Spec}R$, the localization $\mathcal{E} \times_R R_\wp$ is a Néron model for $E$ over $K_\wp$. By Corollary 1 if we fix a Weierstrass equation $\mathcal{W}/R$ for $E/K$ and if we let $S \subset \mathrm{Spec}R$ be the set of primes for which $\mathcal{W}$ has bad reduction, then the part of $\mathcal{W}$ lying over $R_S$ $\mathcal{W} \times_R R_S$ is a Néron model for $E$ over $R_S$. This gives a Néron model over a dense open subset of $\mathrm{Spec}R$ and gluing it to the localized models over the finitely many bad fibers we get a Néron model over all of $\mathrm{Spec}R$. Thus the proof of Theorem 3 is complete.

□

## 6. Mazur's Theorem

Let $H^r(X, \ )$ denote the cohomology with compact support taken over the $fp\ qf$ site. The goal of this section is to relate the Shafarevich-Tate group with the groups $H^1(X, \mathcal{A})$ and $H^1(X, \mathcal{A}^0)$, which we shall define shortly. We shall work with arbitrary abelian variety since the argument that follows works in this generality, something which is certainly not the case in the preceding sections.

Let $A$ be an abelian variety over a number field $K$. Let $K_v$ be the completion of $K$ with respect to the valuation $v$. We can consider the standard maps that serve to define the Shafarevich-Tate group

$$w_v : H^1(\mathrm{Spec}K, A_{/K}) \to H^1(\mathrm{Spec}K_v, A_{/K_v}).$$

We can now form the following two subgroups of $H^1(\mathrm{Spec}K, A_{/K})$

$$\Sigma = \cap \ker(w_v) \quad \text{nonarchimedean } v,$$

$$Ш = \cap \ker(w_v) \quad \text{all } v.$$

As we can see from the definitions Ш is the Shafarevich-Tate group and $\Sigma$ is slightly bigger as we exclude the archimedean valuations. More specifically,

from the definitions above we see that there is an exact sequence

$$0 \to Ш \to \Sigma \to \bigoplus_v H^1(\bar{K}_v/K_v, A(\bar{K}_v)),$$

where the sum on the right is taken over all real archimedean valuations $v$.

When the topological group $A(\bar{K}_v)$ is connected $H^1(\bar{K}_v/K_v, A(\bar{K}_v)) = 0$, so if $A(\bar{K}_v)$ is connected for all real valuations $v$ of $K$, then $Ш = \Sigma$. In any case the exact sequence above implies that the quotient of $\Sigma$ by $Ш$ is a group of exponent 2, the order of which depends on the structure of $A_{K_v}$ for all real valuations $v$ of $K$, but certainly bounded. We are going to give a cohomological description of $\Sigma$.

Let $\mathcal{O}_K$ be the ring of integers of $K$, let $X = \mathrm{Spec}\mathcal{O}_K$, and let $\mathcal{A}/\mathcal{O}_K$ be the Néron model of $A_{/K}$.

For each closed point $x \in X$, the fiber $\mathcal{A}_x$ is a smooth commutative group scheme over $k(x)$. Let us denote by $\mathcal{A}_x^0 \subset \mathcal{A}_x$ its connected component and by $\mathcal{Z}_x \subset \mathcal{A}_x$ its complement. Then $\mathcal{Z}_x$ is non-empty for only finitely many points $x$ and thus $\mathcal{Z} = \cup \mathcal{Z}_x$ is a closed subscheme of $\mathcal{A}$. Let us denote by $\mathcal{A}^0 \subset \mathcal{A}$ its open complement. Then $\mathcal{A}^0$ is an open subgroup scheme of $\mathcal{A}$. Let $F$ be the quotient of $\mathcal{A}$ by $\mathcal{A}^0$ regarded as shaves for the $fp\ qf$ topology. We get

$$0 \to \mathcal{A}^0 \to \mathcal{A} \to F \to 0.$$

Since $\mathcal{A}$ and $\mathcal{A}^0$ are smooth group schemes the cohomology of the above sequence remains the same if computed for the $fp\ qf$, smooth, or étale topologies. By its definition, $F$ is a skyscraper sheaf - it is zero outside the finite set of $x \in X$ such that $\mathcal{A}_x$ is disconnected.

Now since $X$ is normal, from the Néron mapping property it follows that there is an inclusion

$$i : H^1(X, A) \hookrightarrow H^1(\mathrm{Spec}K, A_{/K}).$$

Here is the main result about $\Sigma$ that we are going to prove.

**Theorem 4.** *The inclusion $i$ sends the image of $H^1(X, \mathcal{A}^0) \to H^1(X, \mathcal{A})$ isomorphically to $\Sigma$.*

*Proof.* Let $I$ denote the image of $H^1(X, \mathcal{A}^0)$ in $H^1(X, \mathcal{A})$. Our goal is to show that $I = \Sigma$ and to do that we shall show both inclusions. Let us first show that $I \subset \Sigma$. Fix a nonarchimedean valuation $v$ and let us consider the following commutative diagram

$$\begin{array}{ccccc} H^1(X_v, F) & \xleftarrow{\cong} & H^1(X_v, \mathcal{A}) & \longrightarrow & H^1(K_v, A) \\ \uparrow & & \uparrow & & \uparrow \\ H^1(X, F) & \longleftarrow & H^1(X, \mathcal{A}) & \longrightarrow & H^1(K, A). \end{array}$$

The left-hand square comes from the long exact sequence on cohomology associated to the sequence $0 \to \mathcal{A}^0 \to \mathcal{A} \to F \to 0$. The right-hand square

comes from the inclusion map $i$ and its analogous when we consider the completion with respect to $v$.

Now, given the definition of $\Sigma$, to show that $I \subset \Sigma$ we need to show that $I$ goes to zero under the composition $H^1(X, \mathcal{A}) \to H^1(K, A) \to H^1(K_v, A)$. But from Lang's Theorem ([3]) it follows that $H^1(X_v, F) \leftarrow H^1(X_v, \mathcal{A})$ is an isomorphism. Also, $I$ goes to zero in $H^1(X, F)$ because of the long exact sequence on cohomology asspciated to $0 \to \mathcal{A}^0 \to \mathcal{A} \to F \to 0$. Thus, $I$ goes to zero in $H^1(X_v, \mathcal{A})$, and consequently in $H^1(K_v, A)$, which completes the proof of $I \subset \Sigma$.

Let us now also show that $\Sigma \subset I$. Take an element $y \in \Sigma$. According to Mazur there is a finite set of primes $S \subset X$ containing all primes of bad reduction for $\mathcal{A}$ such that $y \in H^1(X - S, \mathcal{A})$. Then Mazur asserts that we have the following diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(X, \mathcal{A}) & \longrightarrow & H^1(X - S, \mathcal{A}) & \longrightarrow & \bigoplus_{p \in S} H^2_{\cdot}(X_p, \mathcal{A}) \\ \downarrow & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle \cong} \\ 0 & \longrightarrow & \bigoplus_{p \in S} H^1(\hat{X}_p, \mathcal{A}) & \longrightarrow & \bigoplus_{p \in S} H^1(K_p, A) & \longrightarrow & \bigoplus_{p \in S} H^2_{\cdot}(\hat{X}_p, \mathcal{A}) \end{array}$$

The horizontal lines come from relative cohomology exact sequences and the zeros on the left and the right-hand vertical isomorphism follow from properties of relative cohomology. Moreover, Lang's Theorem ([3]) and the fact that $F$ has trivial support on $X - S$ give an isomorphism $H^1(X, F) \to \bigoplus_{p \in S} H^1(\hat{X}_p, \mathcal{A})$.

We need to show that $y \in I$. But $b(y) = 0$ since $y \in \Sigma$, so using the right-hand vertical isomorphism we see that $y$ goes to zero in $\bigoplus_{p \in S} H^2_{\cdot}(X_p, \mathcal{A})$. Consequently, it comes from an element $z \in H^1(X, \mathcal{A})$. Then $a(z)$ must be zero by the exactness of the second row, so $z$ goes to zero in $H^1(X, F)$ using the isomorphism we discussed at the end of the previous paragraph. But this is exactly the condition for $y \in I$, so $\Sigma \subset I$ and the proof of the theorem is completed. □

**References:**

[1] Bosch, S., Lutkebohmert, W., Raynaud, M., *Néron Models*, Springer, Berlin, 1990.

[2] Harthshorne, R., *Algebraic Geometry*, Springer-Verlag, New York, 1977.

[3] Lang, S., *Algebraic groups over finite fields*, Amer. J. Math 78, no. 3, 530 - 561, 1959.

[4] Mazur, B., *Rational Points of Abelian Varieties with Values in Towers of Number Fields* , Inventiones math. 18, 183 - 266, 1972.

[5] Silverman, J., *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, New York, 1994.

[6] Silverman, J., *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.