ELLIPTIC CURVES

October 12, 2025

Contents

1. Elliptic curves

1.1. General abelian varieties.

Definition 1.1.1 (Abelian variety over a field)**.** Let k be a field. An *abelian variety over k* is a complete, connected algebraic group variety defined over k, i.e.

- A is a smooth, proper, geometrically connected algebraic variety over k,

- A is endowed with a group structure defined by morphisms of varieties over k (multiplication $m : A \times_k A \to A$ and inverse $i : A \to A$),
- the group law satisfies the group axioms scheme-theoretically.

In particular, an abelian variety is a projective algebraic group variety (Definition A.0.5) over k.

Definition 1.1.2 (Abelian scheme)**.** Let S be a scheme (Definition A.0.8). An *abelian scheme over S* is a proper and smooth group scheme (Definition A.0.5)

$$\pi : A \to S$$

(♠ TODO: define geometric fiber, geometrically connected, abelia nvariety) with geometrically connected fibers. Each geometric fiber $A_{\overline{s}}$ (over a geometric point $\overline{s} \to S$) is then an abelian variety (Definition 1.1.1).

In particular, over a field, an abelian scheme is precisely an abelian variety.

Definition 1.1.3 (Elliptic curve over a scheme)**.** Let S be a scheme. An *elliptic curve over S* is a pair (E, π) where

- E is a scheme together with a morphism $\pi : E \to S$,
- (E, π) is an abelian scheme of relative dimension 1 over S, i.e. π is proper, smooth, of relative dimension 1, with geometrically connected fibers, and
- a chosen section $e : S \to E$, called the *zero section*, endowing (E, π) with the structure of a commutative group scheme over S.

Equivalently, an elliptic curve over S is a smooth proper curve of genus 1 over S together with a marked S-point that plays the role of the identity.

1.2. **Weierstrass equations.** (♠ TODO: polynomial rings)

1.2.1. *Algebraic facts entirely about Weierstrass equations.*

Definition 1.2.1 (General Weierstrass Equation over a Ring)**.** (♠ TODO: define homogenization of a polynomial) Let R be a (commutative unital) ring, and let $a_1, a_2, a_3, a_4, a_6 \in R$.

A *general Weierstrass equation over R* is either of the following equivalent descriptions:

- The affine equation in variables x, y over R

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

- The projective cubic equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

  in homogeneous coordinates X, Y, Z. Note that this defines a closed subscheme inside $\mathbf{P}^2_R = \operatorname{Proj} R[X, Y, Z]$.

A *short Weierstrass equation over R* is a Weierstrass equation for which $a_1 = a_3 = a_2 = 0$, having the form

$$y^2 = x^3 + a_4x + a_6,$$

or equivalently one which has projective homogenization

$$Y^2Z = X^3 + a_4XZ^2 + a_6Z^3.$$

Definition 1.2.2 (Admissible Change of Variables for a Weierstrass Equation)**.** Let R be a commutative ring with unity and let

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

be a general Weierstrass equation over R (Lemma 1.2.4) with coefficients $a_1, a_2, a_3, a_4, a_6 \in R$.

An *admissible change of variables* (or *isomorphism of Weierstrass equations*) over R is a change of variables of the form

$$x = u^2x' + r,$$
$$y = u^3y' + u^2sx' + t,$$

where $u \in R^\times$ (a unit of R) and $r, s, t \in R$. This transformation maps the given Weierstrass equation to another of the same form with possibly different coefficients, preserving its structure and properties.

Proposition 1.2.3 (Admissible Changes of Variables Preserving Short Weierstrass Form)**.** Let R be a commutative ring with unity. Suppose

$$y^2 = x^3 + Ax + B$$

is a short Weierstrass equation over R (Definition 1.2.1) with coefficients $A, B \in R$.

An admissible change of variables (Definition 1.2.2)

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t,$$

with $u \in R^\times$ and $r, s, t \in R$, transforms this equation into another short Weierstrass equation

$$y'^2 = x'^3 + A'x' + B',$$

if and only if the translation parameters satisfy $r = t = s = 0$. In this case, the coefficients transform as

$$A' = u^4A, \quad B' = u^6B.$$

Thus, the subgroup of admissible changes preserving the short Weierstrass form consists precisely of scaling transformations

$$x = u^2x', \quad y = u^3y'.$$

Lemma 1.2.4. Let R be a (commutative unital) ring. A general Weierstrass equation

$$\text{(A)} \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

is isomorphic (via an admissible change of variables (Definition 1.2.2)) to the following Weierstrass equations under the following conditions:

- If $2, 3 \in R^\times$, then to a short Weierstrass equation
$$y^2 = x^3 + Ax + B,$$
with $A, B \in R$.
- If $2 \in R^\times$, then to a simplified Weierstrass equation of the form
$$y^2 = x^3 + a_2x^2 + a_4x + a_6,$$
with $a_2, a_4, a_6 \in R$.
- If $3 \in R^\times$, then to a simplified Weierstrass equation of the form
$$y^2 + a_1xy + a_3y = x^3 + b_4x + b_6,$$
with $a_1, a_3, b_4, b_6 \in R$.

Notation 1.2.5 (Auxiliary Invariants for a General Weierstrass Equation)**.** Let R be a (commutative unital) ring. For the general Weierstrass equation (Lemma 1.2.4)
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$
with coefficients $a_1, a_2, a_3, a_4, a_6 \in R$, the following are standard notation:

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2, \\
b_4 &= 2a_4 + a_1a_3, \\
b_6 &= a_3^2 + 4a_6, \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6
\end{aligned}$$

For a short Weierstrass equation (Definition 1.2.1)
$$y^2 = x^3 + Ax + B,$$
with $A, B \in R$, these invariants simplify as follows:

$$\begin{aligned}
b_2 &= 0, \\
b_4 &= 2A, \\
b_6 &= 4B, \\
b_8 &= -A^2, \\
c_4 &= -24b_4 = -48A, \\
c_6 &= -216b_6 = -864B.
\end{aligned}$$

Definition 1.2.6 (Discriminant of a General Weierstrass Equation)**.** Let R be a (commutative unital) ring. For the general Weierstrass equation (Definition 1.2.1)
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

with coefficients $a_1, a_2, a_3, a_4, a_6 \in R$, the following are standard notation: Let R and $a_1, a_2, a_3, a_4, a_6 \in R$ be as above. The *discriminant of the general Weierstrass equation*

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

is defined as the element $\Delta \in R$ given by

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

(Notation 1.2.5)

The discriminant for a short Weierstrass equation (Definition 1.2.1)

$$y^2 = x^3 + Ax + B,$$

with $A, B \in R$ is thus

$$\Delta = -16(4A^3 + 27B^2).$$

Definition 1.2.7 (*j-invariant* of a General Weierstrass Equation)**.** Let R be a (commutative unital) ring. For the general Weierstrass equation (Definition 1.2.1)

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

with coefficients $a_1, a_2, a_3, a_4, a_6 \in R$, the following are standard notation:

The *j-invariant* associated to the Weierstrass equation (assuming Δ is invertible in R (Definition A.0.1)) is the element $j \in R$ given by

$$j = \frac{c_4^3}{\Delta},$$

(Notation 1.2.5)

For a short Weierstrass equation (Definition 1.2.1)

$$y^2 = x^3 + Ax + B,$$

with $A, B \in R$ the j-invariant becomes

$$j = 1728\frac{4A^3}{4A^3 + 27B^2} = 1728\frac{4A^3}{-\frac{\Delta}{16}} = -1728\frac{4A^3}{\Delta/16}.$$

Theorem 1.2.8 (Effect of an Admissible Change of Variables on the Discriminant and j-invariant)**.** Let R be a commutative ring with unity. Consider a general Weierstrass equation over R (Lemma 1.2.4),

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

with coefficients $a_1, a_2, a_3, a_4, a_6 \in R$, and let $\Delta \in R$ and $j \in R$ be its discriminant (Definition 1.2.6) and j-invariant (Definition 1.2.7), respectively.

Suppose this equation is transformed by an admissible change of variables (Definition 1.2.2)

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t,$$

where $u \in R^\times$ (a unit), and $r, s, t \in R$ into the Weierstrass equation

$$(y')^2 + a_1'x'y' + a_3'y' = (x')^3 + a_2'(x')^2 + a_4'x' + a_6'.$$

Write b'_i and c'_j for the standard invariants (Notation 1.2.5) for this Weierstrass equation and write Δ' and j' for the discriminant and j-invariant of the transformed Weierstrass equation.

Then the invariants transform according to the following:

$$
\begin{array}{rl}
\hline
ua'_1 &= a_1 + 2s \\
u^2 a'_2 &= a_2 - sa_1 + 3r - s^2 \\
u^3 a'_3 &= a_3 + ra_1 + 2t \\
u^4 a'_4 &= a_4 - sa_3 + 2ra_2 - (t+rs)a_1 + 3r^2 - 2st \\
u^6 a'_6 &= a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1 \\
\hline
u^2 b'_2 &= b_2 + 12r \\
u^4 b'_4 &= b_4 + rb_2 + 6r^2 \\
u^6 b'_6 &= b_6 + 2rb_4 + r^2 b_2 + 4r^3 \\
u^8 b'_8 &= b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4 \\
\hline
u^4 c'_4 &= c_4 \\
u^6 c'_6 &= c_6 \\
u^{12}\Delta' &= \Delta \\
j' &= j \\
\hline
\end{array}
$$

In particular, the discriminant changes by a factor of the twelfth power of the inverse of the unit u, while the j-invariant remains invariant under all admissible changes of variables.

1.2.2. *Elliptic curves as plane curves given by Weierstrass equations.*

Definition 1.2.9 (Elliptic Curve over a Ring Given by a Projective Weierstrass Equation)**.** Let R be a commutative ring with unity.

Let
$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$
be a homogeneous Weierstrass equation (Definition 1.2.1) where $a_1, a_2, a_3, a_4, a_6 \in R$. Let
$$\mathcal{E} \subseteq \mathbf{P}^2_R = \operatorname{Proj} R[X, Y, Z]$$
be the R-scheme defined by the homogeneous Weierstrass equation.

Equip this scheme $\mathcal{E}$ with the structural morphism $\pi : \mathcal{E} \to \operatorname{Spec} R$ induced by the projection, and the distinguished R-rational *point at infinity* defined by the section
$$O : \operatorname{Spec} R \to \mathcal{E}$$
given by the projective point $(X : Y : Z) = (0 : 1 : 0)$.

Assuming that the discriminant Δ (Definition 1.2.7) (of the affinization of the Weierstrass equation) is invertible on $\operatorname{Spec} R$, i.e. is an element of $R^\times$ (Definition A.0.1), the pair $(\mathcal{E}, O)$ is an elliptic curve over R (Definition 1.2.7) and is called the *elliptic curve over R defined by the projective Weierstrass equation* with coefficients a_1, a_2, a_3, a_4, a_6.

The *j-invariant* $j = j_{\mathcal{E}}$ of $\mathcal{E}$ refers to the j-invariant (Definition 1.2.7) of the Weierstrass equation.

(♠ TODO: define an R-rational point on a scheme, projective space, projective points)

Theorem 1.2.10 (Existence of a Weierstrass Equation for an Elliptic Curve over a Scheme)**.** Let S be a scheme. Let $\mathcal{E} \to S$ be an elliptic curve over S (Definition 1.1.3).

(♠ TODO: make precise the notion of Zariski local) Then, Zariski locally on S, there exists a Weierstrass equation (Definition 1.2.1)

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

with coefficients $a_1, a_2, a_3, a_4, a_6 \in \Gamma(U, \mathcal{O}_S)$ for some open subscheme $U \subseteq S$, and an isomorphism of elliptic curves over U identifying $\mathcal{E}|_U$ with the elliptic curve defined by (the projective homogenization of) this Weierstrass equation (Definition 1.2.9).

In other words, every elliptic curve over a scheme admits a Weierstrass equation locally in the Zariski topology on the base.

Definition 1.2.11. Let R be a Dedekind domain (Definition A.0.4) with field of fractions K. Given an elliptic curve E/K, a *Weierstrass model of E over R* is a closed subscheme $W \subseteq \mathbb{P}^2_R$ defined by a (projective) Weierstrass equation (Definition 1.2.1) such that W is flat over R, whose generic fiber $W_K = W \times_{\operatorname{Spec} R} \operatorname{Spec} K$ is isomorphic to E as a curve over K.

Definition 1.2.12. Let R be a Dedekind domain (Definition A.0.4) with field of fractions K and let E/K be an elliptic curve (Definition 1.1.3). A *minimal Weierstrass model of E over R* is a Weierstrass model (Definition 1.2.11) W of E over R such that for every nonzero prime ideal $\mathfrak{p} \subset R$, the $R_{\mathfrak{p}}$-model $W_{R_{\mathfrak{p}}} = W \times_{\operatorname{Spec} R} \operatorname{Spec} R_{\mathfrak{p}}$ is a Weierstrass model whose discriminant (Definition 1.2.6) $\Delta(W_{R_{\mathfrak{p}}})$ has minimal possible $v_{\mathfrak{p}}$-adic valuation among all Weierstrass models of E over $R_{\mathfrak{p}}$.

A (either non-homogeneous/affine or homogeneous/projective) Weierstrass equation (Definition 1.2.1) yielding a minimal Weierstrass model of E over R would be called a *minimal Weierstrass equation of E/R*.

(♠ TODO: define the ring of S-integers) In the case that R is the ring of integers of a local field, or more generally a DVR (Definition A.0.3), we might call a minimal Weierstrass model a *local minimal Weierstrass model* and the equation a *local minimal Weierstrass equation*. In the case that R has infinitely many prime ideals (e.g. R is the ring of integers or some ring of S-integers of a global field), or more generally more than one nonzero prime ideal, we might call a minimal Weierstrass model a *global minimal Weierstrass model* and the equation a *global minimal Weierstrass equation*.

Lemma 1.2.13 (cf. [Sil09, Remark VII.1.1, Exercise 7.1] for a discussion over local fields)**.** Let R be a DVR (Definition A.0.3) with field of fractions (Definition A.0.2) K. Let E/K be an elliptic curve (Definition 1.1.3). Writing a general Weierstrass equation in the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{B}$$

where the coefficients a_i are in K.

1. There exists a (local) minimal Weierstrass model $\mathcal{E}$ of E over R (Definition 1.2.12).
2. Writing the minimal Weierstrass equation in the form (B) where the coefficients a_i are in R, we must have $v(a_i) < i$ for at least one of the i.
3. Given a Weierstrass equation in the form (B) over R, if $v(\Delta) < 12$, $v(c_4) < 4$ or $v(c_6) < 6$ (Notation 1.2.5, Definition 1.2.6), then the equation is minimal over R.
4. If 2 and 3 are invertible in R and if the equation is minimal over R, then $v(\Delta) < 12$ or $v(c_4) < 4$. (♠ TODO: carefully verify this)

Proof. 1. This is obvious, say due to the well-ordering principle of the integers.
2. If $v(a_i) < i$ was false for all of the i, then the formula for the discriminant (Definition 1.2.6) shows that $v(\Delta) \geq 12$. Let π be a uniformizer of R (Definition A.0.3). The admissible change of variables (Definition 1.2.2)
$$x = \pi^2 x'$$
$$y = \pi^3 y'$$
yields a Weierstrass equation in the variables x' and y' whose discriminant Δ' satisfies
$$\Delta' = \pi^{-12}\Delta.$$
by Theorem 1.2.8 In fact, the resulting Weierstrass equation is still over R, and hence the original Weierstrass equation over R could not have been minimal.
3. This holds because a change of variables affects the valuation of Δ, c_4, and c_6 by a multiple of 12, 4, and 6 respectively.
4. (♠ TODO:)

□

For general local fields K, Tate's algorithm determines whether a given equation is minimal for the ring of integers (♠ TODO: cite)

(♠ TODO: talk about when global minimal weierstrass equations exist, say over global fields, cf. Silverman proposition VIII 8.2, Corollray 8.3)

1.3. **Isogenies of abelian varieties.**

Definition 1.3.1 (Isogeny of abelian schemes)**.** Let S be a scheme (Definition A.0.8), and let A and B be abelian schemes over S (Definition 1.1.2). An *isogeny of abelian schemes over S* or *S-isogeny of abelian schemes* is a morphism of group schemes (Definition A.0.6)
$$\varphi : A \to B$$
(♠ TODO: define finite, faithfully flat, and sujrective scheme morpshisms) over S which is finite, faithfully flat, and surjective.

Equivalently, φ is a morphism of abelian schemes whose geometric fibers are *iscgenies of abelian varieties*, i.e., surjective homomorphisms with finite kernel.

Equivalently, some might define an isogeny of abelian schemes over S to simply be an isogeny of the abelian varieties (Definition A.0.7) as algebraic groups over S (Definition A.0.5), depending on what they mean by an "isogeny of algebraic group schemes".

The kernel of φ is often denoted by $\ker \varphi$ or $A[\varphi]$.

Definition 1.3.2. Let A and B be abelian varieties over a field k. We say that A and B are *isogenous*, often written $A \sim B$, if there exists an k-isogeny (Definition 1.3.1) $A \to B$. The relation $\sim$ turns out to be an equivalence relation on the set of abelian varieties over a fixed field k.

2. Néron models of abelian varieties

(♠ TODO: define smooth, separated, finite type morphism of schemes)

Definition 2.0.1 (Néron mapping property)**.** Let R be a Dedekind domain (Definition A.0.4) with fraction field K (Definition A.0.2), and let A/K be an abelian variety. A smooth separated group scheme (Definition A.0.5) $\mathcal{A}/R$ of finite type extending A satisfies the *Néron mapping property* if for every smooth R-scheme S and every K-morphism $f_K : S_K \to A$, there exists a unique R-morphism $f : S \to \mathcal{A}$ extending f_K.

Definition 2.0.2 (Néron model of an abelian variety)**.** Let K be a field that is the fraction field of a Dedekind domain (Definition A.0.4) R, and let A/K be an abelian variety (Definition 1.1.1). A *Néron model of A over R* is a smooth separated group scheme $\mathcal{A}/R$ of finite type such that:

- The generic fiber of $\mathcal{A}$ is A.
- $\mathcal{A}$ satisfies the Néron mapping property.

If such a model exists, it is unique up to unique isomorphism.

3. Reduction

(♠ TODO: read the following definitions) (♠ TODO: define neron model of an abelian variety) (♠ TODO: what kind of field is K here?)

Notation 3.0.1 (Reduction of abelian varieties at a non-archimedean place)**.** Let A/K be an abelian variety and let v be a non-archimedean place of K. Denote by $\mathcal{A}/\mathcal{O}_v$ the Néron model of A over $\mathcal{O}_v$, which is a smooth, separated, finite type group scheme over $\mathcal{O}_v$ with generic fiber A.

The special fiber $\mathcal{A}_v := \mathcal{A} \otimes_{\mathcal{O}_v} k_v$ is called the reduction of A at v.

Definition 3.0.2 (Reduction type of an abelian variety over a non-archimedean place)**.** Let A/K be an abelian variety, v a non-archimedean place of K, and $\mathcal{A}/\mathcal{O}_v$ its Néron model. The reduction type of A at v is defined as follows:

- A has *good reduction at v* if $\mathcal{A}_v$ is an abelian variety (i.e., smooth, connected, complete, of dimension equal to $\dim A$).
- A has *bad reduction at v* if $\mathcal{A}_v$ is not an abelian variety.

– Within bad reduction, A has *multiplicative reduction at v* if the connected component $\mathcal{A}_v^0$ of $\mathcal{A}_v$ is an extension of an abelian variety by a torus of positive dimension.
– A has *additive reduction at v* if $\mathcal{A}_v^0$ has a non-trivial unipotent subgroup.

Definition 3.0.3 (Reduction type of an abelian variety over a global field)**.** Let A/K be an abelian variety over a global field K. The *reduction type of A at a place v of K* is the classification of the reduction of A over v as good, multiplicative, or additive, according to the preceding definition at all non-archimedean places. At archimedean places, reduction type is not defined.

4. Mordell-Weil theorem for abelian varieties over global fields

Theorem 4.0.1 (Mordell–Weil Theorem)**.** (♠ TODO: for function fields, I think I need to say that the curve is not isotypical) (♠ TODO: Try to find a mordell-weil statement over $\mathbb{Q}(T)$) Let K be a global field (Definition A.0.9), and let E be an abelian variety (Definition 1.1.1) defined over K. Then the group $E(K)$ of K-rational points on E is a finitely generated abelian group; that is, there exist integers $r \geq 0$ and a finite abelian group T such that

$$E(K) \cong \mathbb{Z}^r \times T.$$

Here, r is called the *Mordell–Weil rank of E over K* or the *algebraic rank of E over K*, and T is the torsion subgroup of $E(K)$.

5. Selmer group for an isogeny of abelian varieties over global fields

Definition 5.0.1 (Principal homogeneous space (torsor) for a group scheme over a base scheme)**.** Let S be a scheme, and let G be a group scheme over S. A *principal homogeneous space* (or *G-torsor*) over S is an S-scheme X equipped with an action

$$a : G \times_S X \to X$$

satisfying:

- The action a is simply transitive fpqc-locally on S, i.e. there exists an fpqc covering $\{U_i \to S\}$ such that for each i, the base-changed scheme $X_{U_i} \cong G_{U_i}$ as G_{U_i}-schemes.
- The morphism
$$G \times_S X \to X \times_S X, \quad (g, x) \mapsto (g \cdot x, x)$$
is an isomorphism of S-schemes, expressing the free and transitive nature of the action.

(♠ TODO: explain what is meant by local triviality) Such a torsor is étale locally trivial or locally trivial in the fpqc topology.

Definition 5.0.2 (Weil–Châtelet group of an abelian variety over a field)**.** Let k be a field, and let A be an abelian variety defined over k. Denote by $G_k = \mathrm{Gal}(\overline{k}/k)$ the absolute Galois group of k.

The *Weil–Châtelet group of A over k*, denoted $\mathrm{WC}(A/k)$, is defined as the collection equivalence classes of homogeneous spaces for A/k (Definition 5.0.1).

Theorem 5.0.3. Let k be a field, and let A be an abelian variety defined over k. Denote by $G_k = \mathrm{Gal}(\overline{k}/k)$ the absolute Galois group of k.

The Weil–Châtelet group $\mathrm{WC}(A/k)$ is in natural bijection with the Galois cohomology group $H^1(G_k, A(\overline{k}))$ where $A(\overline{k})$ denotes the group of $\overline{k}$-rational points of A with its natural continuous G_k-action. The bijection can be given by the map

$$\begin{aligned}\mathrm{WC}(A/k) &\to H^1(G_k, A(\overline{k}))\\ \{C/k\} &\mapsto \{\sigma \mapsto p_0^\sigma - p_0 \text{ for any point } p_0 \in C(\overline{k})\}.\end{aligned}$$

(♠ TODO: define Galois cohomology)

Definition 5.0.4 (Kummer map associated to an isogeny of an abelian variety)**.** Let k be a field, and let A and B be abelian varieties defined over k. Suppose $\varphi : A \to B$ is an isogeny defined over k (Definition 1.3.1). Denote by $G_k = \mathrm{Gal}(\overline{k}/k)$ the absolute Galois group of k.

The short exact sequence

$$0 \to \ker\varphi \to A(\overline{k}) \xrightarrow{\varphi} B(\overline{k}) \to 0.$$

yields the following long exact sequence in Galois cohomology:

$$\begin{aligned}0 \to \ker\varphi(k) \to& A(k) \xrightarrow{\varphi} B(k)\\ \xrightarrow{\delta_\varphi} H^1(G_k, \ker\varphi) \to& H^1(G_k, A(\overline{k})) \to H^1(G_k, B(\overline{k})) \to \cdots .\end{aligned}$$

The *Kummer map associated to the isogeny φ* is the Galois cohomological connecting homomorphism

$$\delta_\varphi : B(k) \to H^1(G_k, \ker\varphi),$$

above. In fact, there is a short exact sequence

$$0 \to B(k)/\varphi(A(k)) \xrightarrow{\delta'_\varphi} H^1(G_k, \ker\varphi) \to H^1(G_k, A)[\varphi] \to 0$$

where the map δ'_φ is induced by δ_φ. We may also let the *Kummer map associated to φ* refer to this map δ'_φ. We may also use the abuse of notation δ_φ to denote δ'_φ.

Definition 5.0.5 (Selmer group for an isogeny of abelian varieties over a global field)**.** (♠ TODO: It should be possible to define this for more general group schemes) Let K be a global field (Definition A.0.9), and let A and B be abelian varieties (Definition 1.1.1) defined over K. Suppose $\varphi : A \to B$ is an isogeny defined over K (Definition 1.3.1).

Denote by $G_K = \mathrm{Gal}(\overline{K}/K)$ the absolute Galois group of K, and by $\mathrm{Sel}^\varphi(A/K)$ (or $\mathrm{Sel}^{(\varphi)}(A/K)$) the *Selmer group of φ over K*, defined as the subgroup of the Galois cohomology group $H^1(K, \ker\varphi)$ given by

$$\mathrm{Sel}^\varphi(A/K) := \ker\left(H^1(K, \ker\varphi) \to \prod_v H^1(K_v, A(\overline{K}))[\varphi]\right),$$

(♠ TODO: define the kummer map associated to φ) where the product runs over all places (Definition A.0.10) v of K, and $H^1(K_v, A)[\varphi]$ denotes the image of the local Kummer map associated to φ.

We describe the map

$$H^1(K, \ker\varphi) \to \prod_v H^1(K_v, A(\overline{K}))[\varphi] \tag{C}$$

(♠ TODO: define a decomposition group) used to define the kernel above: for each place v of K, fix an extension v to $\overline{K}$, which yields an embedding $\overline{K} \subset \overline{K}_v$ and a decomposition group $G_v \subset G_K$. Note that G_v acts on $A(\overline{K}_v)$ and $B(\overline{K}_v)$, and the base change φ_v of φ to K_v induces a Kummer short exact sequence (Definition 5.0.4)

$$0 \to B(K_v)/\varphi(A(K_v)) \xrightarrow{\delta_{\varphi_v}} H^1(G_v, A[\varphi]) \to H^1(G_v, A(\overline{K}_v))[\varphi] \to 0.$$

The natural inclusions $G_v \subset G_K$ and $E(K) \subset E(K_v)$ give restriction maps on cohomology, and we have a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & B'(K)/\varphi(A(K)) & \xrightarrow{\delta_\varphi} & H^1(G_K, A[\varphi]) & \longrightarrow & H^1(G_K, A(\overline{K}))[\phi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \prod_v B'(K_v)/\varphi(A(K_v)) & \xrightarrow{\delta_{\varphi_v}} & \prod_v H^1(G_v, A[\varphi]) & \longrightarrow & \prod_v H^1(G_v, A(\overline{K}_v))[\phi] & \longrightarrow & 0
\end{array}$$

The map (C) is the one given in the above commutative diagram.

The Selmer group is a finite, computable abelian group.

Remark 5.0.6. (♠ TODO: discuss variants of selmer groups) There are many variants of selmer groups.

(♠ TODO: define the shafarevich group) (♠ TODO: read the following statements)

Proposition 5.0.7 (Equivalent characterizations of the Selmer group)**.** *With notation as above, the Selmer group $\mathrm{Sel}^\varphi(A/K)$ admits the following equivalent descriptions:*

- *It is the subgroup of $H^1(G_K, \ker\varphi)$ consisting of classes that are locally in the image of the local Kummer maps $\delta_{\varphi_v} : B(K_v)/\varphi(A(K_v)) \to H^1(G_v, A[\varphi])$ for every place v of K.*
- *It consists of Galois cohomology classes of $\ker\varphi$ that come from global torsors under A which become trivial locally everywhere.*
- *It can be viewed as the preimage of the local images under the restriction maps:*

$$\mathrm{Sel}^\varphi(A/K) = \left\{\xi \in H^1(G_K, \ker\varphi) \;\middle|\; \mathrm{res}_v(\xi) \in \mathrm{Im}(\delta_{\varphi_v})\ \forall v\right\}.$$

Corollary 5.0.8 (Functors of Selmer groups under isogenies)**.** *Let $\varphi : A \to B$ and $\psi : B \to C$ be isogenies of abelian varieties over a global field K. There is a natural map of Selmer groups*

$$\mathrm{Sel}^\varphi(A/K) \to \mathrm{Sel}^{\psi\circ\varphi}(A/K)$$

induced by composition of isogenies, compatible with the connecting Kummer maps and functorial in the category of isogenies and abelian varieties.

6. Heights of elliptic curves

6.1. Heights of points in projective varieties over number fields.

Definition 6.1.1 (Absolute value and height on projective space)**.** (♠ TODO: define the product formula) Let K be a global field equipped with a set of normalized absolute values M_K satisfying the product formula. For each $v \in M_K$, let $|\cdot|_v$ denote the corresponding absolute value on K.

Consider a point

$$P = (x_0 : x_1 : \cdots : x_n) \in \mathbb{P}^n(K).$$

The *height* $H(P)$ of P is defined as

$$H(P) = \prod_{v \in M_K} \max\{|x_0|_v, |x_1|_v, \ldots, |x_n|_v\}.$$

The *logarithmic height* (or *log height*) of P is defined as

$$h(P) = \log H(P) = \sum_{v \in M_K} \log \max\{|x_0|_v, |x_1|_v, \ldots, |x_n|_v\}.$$

6.2. Heights of elliptic curves over number fields.

Definition 6.2.1 (naive height of an elliptic curve over a number field, cf. [Sil89])**.** (♠ TODO: can this definition be aplicable for a global function field) Let K be a number field. For $a, b \in K$ with $4a^3 + 27b^2 \neq 0$, let $E(a, b)$ be the elliptic curve given by (affine) Weierstrass equation (Definition 1.2.1)

$$E(a, b) : y^2 = x^3 + ax + b$$

1. Define the *(naive muitiplicative) height of an elliptic curve* E/K to be

$$H(E) = \inf_{\substack{a,b \in K \\ E \cong_K E(a,b)}} H([a^3, b^2, 1])$$

   where H is the height function (Definition 6.1.1) of points in $\mathbb{P}^2(K)$.
2. Define the *(naive logarithmic) height of an elliptic curve* E/K to be

$$h(E) = \inf_{\substack{a,b \in K \\ E \cong_K E(a,b)}} h([a^3, b^2, 1])$$

   where h is the logarithmic height function (Definition 6.1.1) of points in $\mathbb{P}^2(K)$.

(♠ TODO: read tjhe following)

Definition 6.2.2 (Height of an elliptic curve over a number field or function field)**.** (♠ TODO: define non-logarithmic height) Let K be a global field, i.e., either a number field or a function field. Fix a set of normalized absolute values M_K on K satisfying the product formula.

Let E/K be an elliptic curve given by a Weierstrass equation with coefficients in K. The *(logarithmic) height of E* is defined by

$$h(E) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \log \max \left\{ |4a_4|_v^3, |27a_6|_v^2 \right\},$$

where a_4, a_6 are the coefficients of the minimal Weierstrass equation of E, $|\cdot|_v$ are the normalized absolute values on K, and n_v are the local degrees.

This height measures the arithmetic complexity of the elliptic curve and generalizes the classical height notion on points to the curve itself.

6.3. Heights functions of elliptic curves over number fields. (♠ TODO: read tjhe following)

Definition 6.3.1 (Weil height function on elliptic curves)**.** Let K be a global field with a set of absolute values M_K normalized so that the product formula holds. Let E/K be an elliptic curve defined by a Weierstrass equation with coefficients in K.

The *(logarithmic) height* of a point $P = (x : y : z) \in E(\overline{K})$ (projective coordinates) is defined by

$$h(P) = \frac{1}{[L:K]} \sum_{v \in M_L} \log \max\{|x|_v, |y|_v, |z|_v\},$$

where L is a finite extension of K over which P is defined, and the sum is taken over all places v of L, with $|\cdot|_v$ suitably normalized absolute values.

The *height of the elliptic curve* E itself is defined by

$$h(E) = h(j(E)),$$

where $j(E)$ is the j-invariant of E.

Definition 6.3.2 (Naive height and canonical height)**.** Given an elliptic curve E/K and a point $P \in E(\overline{K})$, the *naive height* $h(P)$ is as above. The *canonical height* $\hat{h}(P)$ is a quadratic form on $E(\overline{K})$ defined by the Néron-Tate construction, satisfying

$$\hat{h}(nP) = n^2 \hat{h}(P), \quad \text{and} \quad |\hat{h}(P) - h(P)| < C$$

for some constant C depending on E and K.

7. Serre's open image theorem

Serre's celebrated open image theorem was originally proved for elliptic curves over number fields without complex multiplication. (♠ TODO: complex multiplication)

Theorem 7.0.1 (Serre's open image theorem, [Ser72, Théorème 2])**.** Let E/K be an elliptic curve (Definition 1.1.3) over a number field such that E does not have complex multiplication over $\overline{K}$. (♠ TODO: complex multiplication, algebraically closed field extension, algebraic closure). For all but finitely many prime numbers ℓ, the Galois representation

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_\ell E)$$

on the ℓ-adic Tate module $T_\ell E$ of E is surjective. (♠ TODO: ℓ-adic tate module)

Serre later proved a generalization for abelian varieties:

Theorem 7.0.2 ([Ser00, Corollaire au Théorème 3])**.** Let A/K be an abelian variety (Definition 1.1.1) of dimension n over a number field (Definition A.0.9) such that $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$. (♠ TODO: complete)

1. For all but finitely many primes ℓ, the "mod-ℓ" Galois representation

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(A[\ell](\overline{K})) \cong \mathrm{GSp}_{2n}(\mathbb{F}_\ell)$$

   is surjective, where $\mathrm{Aut}(A[\ell](\overline{K}))$ is the group of automorphisms on the $\mathbb{F}_\ell$-vector space $A[\ell](\overline{K})$ preserving the Weil pairing (♠ TODO: Weil pairing)
2. For all but finitely many primes ℓ, the "ℓ-adic" Galois representation

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_\ell A) \cong \mathrm{GSp}_{2n}(\mathbb{Z}_\ell)$$

   is surjective, where $\mathrm{Aut}(T_\ell A)$ is the group of automorphisms on the $\mathbb{Z}_\ell$-module $T_\ell A$ preserving the Weil pairing (♠ TODO: Weil pairing, Tate module)
3. The image of the "adélic" Galois representation

$$\mathrm{Gal}(\overline{K}/K) \to \prod_\ell{}' \mathrm{Aut}(V_\ell A) \cong \prod_\ell{}' \mathrm{GSp}_{2n}(\mathbb{Q}_\ell)$$

   is open (with respect to the adélic topology), where $\prod_\ell' \mathrm{Aut}(V_\ell A)$ is the restricted product (Definition A.0.11) of the groups $\mathrm{Aut}(V_\ell A)$ of automorphisms on the $\mathbb{Q}_\ell$-vectors spaces $V_\ell A = V_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ preserving the Weil pairing.

Appendix A. Miscellaneous definitions

Definition A.0.1. Let $(R, +, \cdot)$ be a not-necessarily commutative ring. A *unit* or *invertible element of R* is an element $u \in R$ such that there exist an element $v \in R$ such that

$$uv = 1 = vu.$$

Such an element v is called the *multiplicative inverse of u* and is often denoted by u^{-1}. If it exists, then it is unique.

The set of units of R forms a group, often denoted by $R^\times$ or R^*, under the multiplication operation $\cdot$. It is called the *group of units* or *unit group* of R.

Definition A.0.2. Let R be an integral domain, and consider the set $R\times(R\setminus\{0\})$ as above. Define a relation $\sim$ on $R\times(R\setminus\{0\})$ by declaring that

$$(a,b)\sim(c,d) \quad \text{if and only if} \quad ad=bc,$$

for $a,c\in R$ and $b,d\in R\setminus\{0\}$. This relation is an equivalence relation. Its equivalence classes are denoted by $\frac{a}{b}$.

The set of equivalence classes

$$\left\{\, \tfrac{a}{b} \,\middle|\, a\in R,\, b\in R\setminus\{0\} \,\right\}$$

under the relation $\sim$ defined above is called the *field of fractions of R*, and is denoted by $\mathrm{Frac}(R)$.

The operations on $\mathrm{Frac}(R)$ are defined by

$$\begin{aligned} \tfrac{a}{b}+\tfrac{c}{d} &= \tfrac{ad+bc}{bd}, \\ \tfrac{a}{b}\cdot\tfrac{c}{d} &= \tfrac{ac}{bd}, \end{aligned}$$

for $a,c\in R$ and $b,d\in R\setminus\{0\}$. With these operations, $\mathrm{Frac}(R)$ is a field.

Definition A.0.3 (Discrete valuation ring)**.** (♠ TODO: define principal ideal) A local integral domain $(R,\mathfrak{m})$ with maximal ideal $\mathfrak{m}$ is called a *discrete valuation ring (DVR)* if $\mathfrak{m}$ is principal and nonzero, and every nonzero ideal of R is of the form $\mathfrak{m}^n$ for some integer $n\geq 0$.

A *uniformizer of R* refers to any generator of $\mathfrak{m}$.

The *(normalized) discrete valuation* $v: R^\times \to \mathbb{Z}_{\geq 1}$ is given by

$$v(x) = \text{minimal } n \text{ such that } x\in\mathfrak{m}^n.$$

Alternatively, v may be extended to a map $v: R\to\mathbb{Z}_{\geq 1}\cup\{\infty\}$ by letting $v(0)=\infty$.

In fact, v extends to a discrete valuation on the fraction field of R (Definition A.0.2) by defining

$$v\left(\frac{a}{b}\right) = v(a)-v(b)$$

for $a\in R$ and $b\in R^\times$. This is a well defined map

$$v: K\to\mathbb{Z}\cup\{\infty\}.$$

Definition A.0.4 (Dedekind domain)**.** An integral domain R is called a *Dedekind domain* if it satisfies the following equivalent conditions: (♠ TODO: define field of fractions)

- R is Noetherian, integrally closed in its field of fractions, and every nonzero prime ideal of R is maximal.
- Equivalently: for every nonzero prime ideal $\mathfrak{p}$ of R, the localization $R_\mathfrak{p}$ is a discrete valuation ring (Definition A.0.3).

Definition A.0.5. Let S be a scheme. An algebraic group scheme over S (or an S-group scheme) is a group object G in the category of schemes over S; that is, G is an S-scheme equipped with S-morphisms: $m: G\times_S G\to G$ (*multiplication*), $i: G\to G$ (*inverse*), and

$e : S \to G$ (*identity*), satisfying the group axioms expressed by the commutativity of the following diagrams:

1. **Associativity**
$$\begin{tikzcd} G \times_S G \times_S G \arrow[r, "m\times\mathrm{id}"] \arrow[d, "\mathrm{id}\times m"'] & G \times_S G \arrow[d, "m"] \\ G \times_S G \arrow[r, "m"] & G \end{tikzcd}$$
2. **Identity**
$$\begin{tikzcd} G \times_S S \arrow[r, "\mathrm{id}\times e"] \arrow[dr, "\simeq"'] & G \times_S G \arrow[d, "m"] \\ & G \end{tikzcd} \qquad \begin{tikzcd} S \times_S G \arrow[r, "e\times\mathrm{id}"] \arrow[dr, "\simeq"'] & G \times_S G \arrow[d, "m"] \\ & G \end{tikzcd}$$
3. **Inverse**
$$\begin{tikzcd} G \arrow[r, "(\mathrm{id},i)"] \arrow[d, "\mathrm{id}"'] & G \times_S G \arrow[d, "m"] \\ G \arrow[r, "e\circ\pi"] & G \end{tikzcd}$$
where $\pi : G \to S$ is the structure morphism and $e \circ \pi$ sends g to the identity section.

(♠ TODO: defien relative affineness) If G is affine over S, we call it an *affine group scheme over S*.

If the base scheme S is the spectrum of a field k, then we call G a *k-algebraic group* or an *algebraic group (scheme) over k*. If G is additionally a k-variety, then we call G a *k-group variety*.

Definition A.0.6. Let S be a scheme, and let G and H be S-algebraic groups. A morphism of S-schemes $f : G \to H$ is a *homomorphism of algebraic groups* if f is a group homomorphism, i.e.,

- $f(m_G(x, y)) = m_H(f(x), f(y))$ for all $x, y \in G$,
- $f(i_G(x)) = i_H(f(x))$ for all $x \in G$, and
- $f(e_G) = e_H$.

It is called an *isomorphism of algebraic groups (over S)* if it is additionally an isomorphism of S-schemes. If there exists an isomorphism $f : G \to H$ of algebraic groups over S, then G and H are said to be *isomorphic S-algebraic groups*.

Definition A.0.7. (♠ TODO: TODO: define kernel,image of a group homomorphism of algebraic groups,) Let S be a scheme and let $f : G \to H$ be a homomorphism of S-algebraic groups.

There are related, but conflicting definitions for what it means for f to be an *isogeny of S-algebraic groups*:

1. We commonly say that f is an isogeny of algebraic groups if it is surjective and its kernel $\ker f$ is a finite flat group scheme over S.
2. Inequivalently, we might alternatively say that f is an isogeny of algebraic groups if $\ker f$ is a finite flat group scheme over S and its image has finite index in H.

Unless otherwise specified, the first definition will generally be used.

Definition A.0.8 (Scheme)**.** A *scheme* is a locally ringed space $(X, \mathcal{O}_X)$ that admits an open cover $\{U_i\}_{i\in I}$ such that each $(U_i, \mathcal{O}_X|_{U_i})$ is isomorphic (as a locally ringed space) to an affine scheme $(\mathrm{Spec}(A_i), \mathcal{O}_{\mathrm{Spec}(A_i)})$ for some commutative ring A_i. In other words, a scheme is a locally ringed space locally isomorphic to affine schemes.

Definition A.0.9. A *global field* is a field K that is either:

- a finite extension of the field of rational numbers $\mathbb{Q}$ (i.e., a number field), or
- a finite extension of the field of rational functions $\mathbb{F}_q(t)$ in one variable over a finite field $\mathbb{F}_q$ (i.e., a global function field).

Definition A.0.10 (Place of a global field)**.** Let F be a global field. A *place of F* is an equivalence class of absolute values on F.

If any (equivalently all) representatives of a place v of F is an archimedean absolute value (resp. non-archimedean absolute value), then we say that v is an *archimedean place* (resp. *non-archimedean place*). A representative of a place v is often denoted by $|\cdot|_v$.

Definition A.0.11. Let $\{X_i\}_{i\in I}$ be a family of topological spaces indexed by a set I. For each $i \in I$, let $K_i \subseteq X_i$ be a topological subspace.

The *restricted product topology* on the restricted product

$$\prod_{i\in I}{}' X_i := \left\{ (x_i)_{i\in I} \in \prod_{i\in I} X_i \;\middle|\; x_i \in K_i \text{ for all but finitely many } i \in I \right\},$$

with respect to the subsets $\{K_i\}_{i\in I}$, is the coarsest topology such that:

- The natural inclusion maps $X_j \to \prod'_{i\in I} X_i$, defined by $x_j \mapsto (y_i)$ where $y_j = x_j$ and $y_i = k_i$ (a fixed element in K_i) for all $i \neq j$, are continuous for all $j \in I$.
- The subspace topology on the product $\prod_{i\in F} X_i$ for any finite subset $F \subseteq I$ (where coordinates outside F are fixed in K_i) coincides with the product topology on finitely many factors.

Equivalently, the restricted product topology is generated by the base consisting of sets of the form

$$\prod_{i\in F} U_i \times \prod_{i\notin F} K_i,$$

where $F \subseteq I$ is finite, U_i are open sets in X_i, and outside F the coordinates lie in K_i.

Definition A.0.12. Let K be a global field. Write M_K for the set of all places (Definition A.0.10) of K and write M_K^∞ for the set of archimedean places of K. Let $S \subseteq M_K$ be some subset of places of K (typically, S is a finite set). For each $v \in M_K$, write $\mathcal{O}_v$ for the ring of integers in the completion K_v

- The *adèle ring of K*, denoted $\mathbb{A}_K$, is the restricted direct product of the K_v (over all places v of K), with respect to the $\mathcal{O}_v$ at non-archimedean v:

$$\mathbb{A}_K = \left\{ (x_v)_v \in \prod_{v \in M_K} K_v \;\middle|\; x_v \in \mathcal{O}_v \text{ for all but finitely many non-archimedean } v \right\}.$$

- The *idèle group of K*, commonly denoted $\mathbb{A}_K^\times$ or $\mathbb{I}_K$, is the group of invertible elements of $\mathbb{A}_K$:

$$\mathbb{I}_K = \mathbb{A}_K^\times = \left\{ (x_v)_v \in \prod_{v \in M_K} K_v^\times \;\middle|\; x_v \in \mathcal{O}_v^\times \text{ for all but finitely many non-archimedean } v \right\},$$

  where $\mathcal{O}_v^\times$ denotes the group of units of $\mathcal{O}_v$ for non-archimedean v.
- The *adèle ring outside S of K*, commonly denoted $\mathbb{A}_K^S$ or $\mathbb{A}_{K,S}$, is the restricted product of the completions K_v over all places $v \in M_K \setminus S$, with respect to the rings of integers $\mathcal{O}_v$ at non-archimedean places:

$$\mathbb{A}_{K,S} = \mathbb{A}_K^S = \left\{ (x_v)_v \in \prod_{v \in M_K \setminus S} K_v \;\middle|\; x_v \in \mathcal{O}_v \text{ for all but finitely many non-archimedean } v \right\}.$$

- The *idèle group outside S of K*, commonly denoted $(\mathbb{A}_K^\times)^S$, $(\mathbb{A}_{K,S}^\times)$, $\mathbb{I}_K^S$, or $\mathbb{I}_{K,S}$ is the group of invertible elements of $\mathbb{A}_K^S$:

$$(\mathbb{A}_K^\times)^S = \left\{ (x_v)_v \in \prod_{v \in M_K \setminus S} K_v^\times \;\middle|\; x_v \in \mathcal{O}_v^\times \text{ for all but finitely many non-archimedean } v \right\}.$$

- The *ring of finite adèles of K*, commonly denoted $\mathbb{A}_{K,\mathrm{fin}}$, $\mathbb{A}_K^{\mathrm{fin}}$, $\mathbb{A}_{K,\mathrm{f}}$, $\mathbb{A}_K^{\mathrm{f}}$, is the adèle ring outside $S = M_K^\infty$, the set of archimedean places of K:

$$\mathbb{A}_{K,\mathrm{fin}} := \mathbb{A}_K^{M_K^\infty} = \left\{ (x_v)_v \in \prod_{v \notin M_K^\infty} K_v \;\middle|\; x_v \in \mathcal{O}_v \text{ for all but finitely many non-archimedean } v \right\}.$$

- The *finite idèle group of K*, commonly denoted $\mathbb{A}_{K,\mathrm{fin}}^\times$, $\mathbb{I}_{K,\mathrm{fin}}$, $\mathbb{I}_K^{\mathrm{fin}}$, $\mathbb{I}_{K,\mathrm{f}}$, $\mathbb{I}_K^{\mathrm{f}}$ etc. is the group of units of the ring of finite adèles:

$$\mathbb{A}_{K,\mathrm{fin}}^\times := (\mathbb{A}_K^\times)^{M_K^\infty} = \left\{ (x_v)_v \in \prod_{v \notin M_K^\infty} K_v^\times \;\middle|\; x_v \in \mathcal{O}_v^\times \text{ for all but finitely many non-archimedean } v \right\}.$$

All of these are equipped with the restricted product topology induced by the topologies of the local fields K_v and the subspace topologies thereof.

References

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. math*, 15:259–331, 1972.

[Ser00] Jean-Pierre Serre. Lettre à marie-france vignéras du 10/2/1986. *Oeuvres–Collected Papers*, 4:38–55, 2000.

[Sil89] Joseph H. Silverman. Elliptic curves of bounded degree and height. *Proceedings of the American Mathematical Society*, 105(3):540–545, 1989.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 2 edition, 2009.