II. Algebraic Theory of Elliptic Curves

In this chapter we sketch the general theory of elliptic curves from an algebraic viewpoint. This material is fairly standard, although some of our proofs may differ from the ones appearing in standard textbooks (cf. [Si 1], [Mi], [Ca 1], [Hu]). The reader may prefer to stick to the usual old-fashioned algebraic geometry (see [Si 1], Ch. 1,2) and ignore any discussion of non-perfect fields.

1. Elliptic Curves - Generalities

1.1 What is an elliptic curve?

(1.1.1) Elliptic curves over C. Informally, an elliptic curve over $\mathbf{C}$ is a smooth projective curve E (over $\mathbf{C}$) such that the corresponding Riemann surface $E(\mathbf{C})$ is isomorphic to $\mathbf{C}/L$, for some lattice $L \in \mathbf{C}$. In other words, $E(\mathbf{C})$ can be parametrized by elliptic functions with respect to L.

(1.1.2) Examples: (1) The projectivization of the affine cubic curve $y^2 = f(x)$, where $f \in \mathbf{C}[x]$ is a polynomial of degree $\deg(f) = 3$ with three distinct roots (by I.4.4.2).
(2) The desingularized projectivization $V \cup \{O_+, O_-\}$ of the affine curve $V : y^2 = f(x)$, where $f \in \mathbf{C}[x]$ is a polynomial of degree $\deg(f) = 4$ with four distinct roots (I.3.7.8, I.4.2.5-7).
(3) A smooth intersection of two quadrics in $\mathbf{P}^3(\mathbf{C})$ (as in I.6.4.4-5).

(1.1.3) Definition. *An* **elliptic curve** *over a field K is a pair (E, O), where E is a smooth projective curve over K, geometrically irreducible (i.e. irreducible over $\overline{K}$), of genus $g = 1$, and $O \in E(K)$ is a K-rational point of E ("the origin").*

(1.1.4) (1) Recall that, if X is a smooth projective curve over K, irreducible over $\overline{K}$, then the *genus* of X is defined as the dimension of the space of regular differentials on E:

$$g(X) = \dim_K \Gamma(X, \Omega_{X/K}).$$

(2) For any field extension L/K, the curve $X_L = X \otimes_K L$ (defined by the same polynomial equations as X, but considered as a curve over L) is again a smooth projective curve over L, irreducible over $\overline{L}$, and

$$\Gamma(X_L, \Omega_{X_L/L}) = \Gamma(X, \Omega_{X/K}) \otimes_K L \implies g(X_L) = g(X).$$

(3) In particular, if (E, O) is an elliptic curve over K, then (E_L, O) is an elliptic curve over L, for any field extension L/K.
(4) If $K = \mathbf{C}$, then the set of complex points $X(\mathbf{C})$ has a natural structure of a compact Riemann surface and $\Gamma(X, \Omega_{X/\mathbf{C}}) = \Omega^1(X(\mathbf{C}))$, which implies that

$$g(X) = g_{an}(X(\mathbf{C})) = g(X(\mathbf{C})).$$

(1.1.5) Notation. Let X be as in 1.1.4.

(1) The field of rational functions on X will be denoted by $R(X)$.
(2) If $K = \overline{K}$ is algebraically closed, then the abelian group of divisors on X is defined as

$$\mathrm{Div}(X) = \{\sum n_P(P) \,|\, n_P \in \mathbf{Z}, P \in X(K), \text{ the sum is finite}\}.$$

The degree of a divisor $D = \sum n_P(P)$ is defined to be $\deg(D) = \sum n_P \in \mathbf{Z}$. The divisor D is *effective* (notation: $D \geq 0$) if $n_P \geq 0$ for all P.
(3) If K is a perfect field, then the absolute Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$ of K acts on $\mathrm{Div}(X_{\overline{K}})$ (through its action on $X(\overline{K})$). The abelian group of divisors on X is defined as the subgroup of G_K-invariant divisors on $X_{\overline{K}}$:

$$\mathrm{Div}(X) = \mathrm{Div}(X_{\overline{K}})^{G_K}.$$

We denote by $\deg_K$ the restriction of the degree map $\deg : \mathrm{Div}(X_{\overline{K}}) \longrightarrow \mathbf{Z}$ to $\mathrm{Div}(X)$; its kernel will be denoted by $\mathrm{Div}^0(X) = \mathrm{Ker}(\deg_K)$.

(4) If K is not perfect, then one must use a scheme-theoretical language:

$$\mathrm{Div}(X) = \{\sum n_x(x) \,|\, n_x \in \mathbf{Z}, x \in |X|, \text{ the sum is finite}\},$$

where $|X|$ denotes the set of closed points of X (if K is perfect, then closed points of X correspond to G_K-orbits in $X(\overline{K})$). The degree of a divisor is defined as

$$\deg_K(\sum n_x(x)) = \sum n_x \cdot [k(x) : K],$$

where $k(x)$ is the residue field of x.

(5) Each (non-zero) rational function $f \in R(X)^*$ has a divisor $\mathrm{div}(f) \in \mathrm{Div}(X)$, which has degree zero. One defines the abelian group $Cl(X)$ of divisor classes on X (resp. its subgroup $Cl^0(X)$ of divisor classes of degree zero) as in the analytic case (see I.3.9).

(6) For any field extension L/K, a divisor $D \in \mathrm{Div}(X)$ defines a divisor $D_L \in \mathrm{Div}(X_L)$. If $D = \mathrm{div}(g)$ is principal, so is $D_L = \mathrm{div}(g_L)$ (where $g_L = g$, but considered as an element of the field $R(X_L) \supset R(X)$).

(1.1.6) If K is perfect and X has a K-rational point, then the canonical maps

$$Cl(X) \longrightarrow Cl(X_{\overline{K}})^{G_K}, \qquad Cl^0(X) \longrightarrow Cl^0(X_{\overline{K}})^{G_K}$$

are isomorphisms (but we are not going to use this fact).

(1.1.7) The Riemann-Roch Theorem. Let X be as in 1.1.4. For each divisor $D \in \mathrm{Div}(X)$, put

$$L(D) = \{0\} \cup \{f \in R(X)^* \,|\, D + \mathrm{div}(f) \geq 0\}, \qquad \ell(D) = \dim_K L(D) \quad (< \infty).$$

(1) If $\deg_K(D) < 0$, then $L(D) = \{0\}$ and $\ell(D) = 0$ (as $\deg_K(\mathrm{div}(f)) = 0$).

(2) If $g \in R(X)^*$ and $D' = D + \mathrm{div}(g)$, then the map $f \mapsto fg$ defines an isomorphism of vector spaces $L(D') \xrightarrow{\sim} L(D)$; in particular, $\ell(D)$ depends only on the class of the divisor D in $Cl(X)$.

(3) The rational differentials on X form a vector space $\Omega_{R(X)/K}$ over $R(X)$ of dimension one. If $\omega, \omega' \in \Omega_{R(X)/K} - \{0\}$, then $\omega' = g\omega$ for some $g \in R(X)^*$; it follows that the class of the divisor $\mathrm{div}(\omega') = \mathrm{div}(\omega) + \mathrm{div}(g)$ is independent of any choices; it is the *canonical class* $\mathcal{K} \in Cl(X)$ of X.

(4) The map

$$L(\mathrm{div}(\omega)) \longrightarrow \Gamma(X, \Omega_{X/K}), \qquad f \mapsto f\omega$$

is an isomorphism; thus $\ell(\mathcal{K}) = g(X) = g$.

(5) The Riemann-Roch Theorem states that, for each $D \in \mathrm{Div}(X)$,

$$\ell(D) - \ell(\mathcal{K} - D) = 1 - g + \deg_K(D).$$

(6) Letting $D = \mathcal{K}$ (i.e. $D = \mathrm{div}(\omega)$ as in (3)), then we obtain

$$\deg_K(\mathcal{K}) = \deg_K(\mathrm{div}(\omega)) = 2g - 2.$$

(7) If $\deg_K(D) > 2g - 2$, then $\deg_K(\mathcal{K} - D) < 0$, which implies that $\ell(\mathcal{K} - D) = 0$ (by (1)), hence

$$\ell(D) = 1 - g + \deg_K(D).$$

1.2 The group law

(1.2.1) Proposition. *Let (E, O) be an elliptic curve over K. Then the map*

$$\begin{aligned} E(K) &\longrightarrow Cl^0(E) \\ P &\mapsto \text{ the class of } (P) - (O) \end{aligned}$$

is bijective (hence the same formula defines a bijection $E(L) \xrightarrow{\sim} Cl^0(E_L)$, for any field over $L \supset K$).

Proof. (cf. [Si 1], Prop. III.3.4, if K is perfect). *Injectivity:* assume that $P, Q \in E(K)$ and $(P) - (O) = (Q) - (O) + \mathrm{div}(f)$ for some $f \in R(E)^*$. If $P \neq Q$, then $\mathrm{div}(f) = (P) - (Q) \neq 0$. This implies that f defines a non-constant rational map (hence a morphism) $f : E \longrightarrow \mathbf{P}^1_K$ of degree $\deg(f) = 1$. It follows that f is an isomorphism $f : E \xrightarrow{\sim} \mathbf{P}^1_K$, which contradicts the fact that $g(E) = 1 \neq 0 = g(\mathbf{P}^1_K)$; thus $P = Q$.
Surjectivity: if $D \in \mathrm{Div}^0(E)$, then the Riemann-Roch Theorem implies that $\ell(D + (O)) = 1$; fixing $f \in L(D + (O)) - \{0\}$, then $D' := D + (O) + \mathrm{div}(f) \geq 0$ is an effective divisor of degree $\deg_K(D') = 1$, hence $D' = (P)$ for a K-rational point $P \in E(K)$. As $D = (P) - (O) - \mathrm{div}(f)$, the class of D coincides with that of $(P) - (O)$.

(1.2.2) Corollary. (i) *The addition "+" on $Cl^0(E)$ induces the structure of an abelian group $(E(K), \boxplus)$ on $E(K)$, with neutral element O, characterized by*

$$P \boxplus Q = R \iff (\exists f \in R(E)^*) \quad (P) + (Q) = (R) + (O) + \mathrm{div}(f).$$

(ii) *For any field extension L/K, the group law induced on $E(L)$ by the bijection $E(L) \xrightarrow{\sim} Cl^0(E_L)$ restricts to the group law $\boxplus$ on $E(K)$.*

(1.2.3) Smooth plane cubics. Let $E \subset \mathbf{P}^2_K$,

$$E : F(X, Y, Z) = 0 \qquad\qquad (F \in K[X, Y, Z] \text{ homogeneous of degree } 3)$$

be a smooth projective plane cubic curve and $O \in E(K)$. The pair (E, O) is an elliptic curve over K, since $g(E) = (3-1)(3-2)/2 = 1$ (irreducibity of E over $\overline{K}$ follows from Bézout's Theorem; cf. 3.7.5(i)). We claim that the abstract group law $\boxplus$ on (E, O) is given by the formula (I.10.1.1.1): if L is a field containing K and $P, Q \in E(L)$, let

$$\ell : aX + bY + cZ = 0, \qquad \ell' : a'X + b'Y + c'Z = 0 \qquad\qquad (a, \ldots, c' \in L)$$

be the equations of the lines $\overline{PQ}$ and $\overline{(P * Q)O}$, respectively. The rational function $f = \ell/\ell' \in R(E_L)^*$ has divisor

$$\mathrm{div}(f) = (P) + (Q) + (P * Q) - (P * Q) - (O) - ((P * Q) * O) = (P) + (Q) - (O) - ((P * Q) * O),$$

hence

$$(P * Q) * O = P \boxplus Q$$

as claimed (note that, in general, the inverse $-P$ with respect to the group law is *not* equal to $P * O$; cf. I.10.1.4).

This discussion applies, in particular, to the pair (C, O) from the next Proposition.

(1.2.4) Proposition (The generalized Weierstrass equation). *Let (E, O) be an elliptic curve over K. There exist rational functions $x, y \in R(E)^*$ such that the map*

$$\begin{aligned} \alpha : E &\longrightarrow \mathbf{P}^2_K \\ P &\mapsto (x(P) : y(P) : 1) \qquad\qquad (P \neq O) \\ O &\mapsto O = (0 : 1 : 0) \end{aligned}$$

induces an isomorphism between (E,O) and (C,O), where C is the (smooth) cubic projective curve

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{1.2.4.1}$$

for some $a_j \in K$ (we say that C is an elliptic curve in a **generalized Weierstrass form**. *(Conversely, if C in (1.2.4.1) is smooth, then (C,O) is an elliptic curve over K, by 1.2.3.)*

Proof. (cf. [Si 1], Prop. III.3.1). It follows from the Riemann-Roch Theorem that $\ell(n(O)) = n$ for each $n \geq 1$ ($\Longrightarrow L((O)) = K$). In particular, there exist rational functions $x \in L(2(O)) - K$ (an analogue of $\wp(z)$) and $y \in L(3(O)) - L(2(O))$ (an analogue of $\wp'(z)$). The triple $x, y, 1$ forms a basis of $L(3(O))$ and defines a non-constant rational map

$$(x : y : 1) : E - - - - \succ \mathbf{P}^2_K \ ,$$

which extends to a (unique) morphism $\alpha : E \longrightarrow \mathbf{P}^2_K$, since E is a regular curve and $\mathbf{P}^2_K$ is projective. As

$$x^2 \in L(4(O)) - L(3(O)), \qquad xy \in L(5(O)) - L(4(O)),$$

it follows that the rational functions $1, x, y, x^2, xy$ form a basis of $L(5(O))$. Going one step further, we have

$$x^3, y^2 \in L(6(O)) - L(5(O)), \qquad \dim_K(L(6(O))/L(5(O))) = 1,$$

which implies that there exists a linear relation

$$x^3 - ay^2 \in L(5(O)) \qquad\qquad (a \in K^*).$$

Replacing x (resp. y) by ax (resp. a^2y), we can assume that $a = 1$; thus there exists a linear relation

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0 \qquad\qquad (a_j \in K), \tag{1.2.4.2}$$

which is an algebraic version of the differential equation I.7.1.8 satisfied by the Weierstrass function $\wp(z)$. In particular, the morphism α factors as

$$E \xrightarrow{\beta} C \hookrightarrow \mathbf{P}^2_K,$$

where C is the projectivization of (1.2.4.2), i.e. the projective curve (1.2.4.1) (where $x = X/Z$ and $y = Y/Z$, as usual). It is easy to see that the polynomial $f(x,y)$ is irreducible in $\overline{K}[x,y]$; thus C is a reduced and geometrically irreducible curve.

The affine coordinates $x, y \in R(C)$ define rational functions on C, hence rational maps $x, y : C - - - \succ \mathbf{P}^1_K$. As before, the composite rational maps $x \circ \beta, y \circ \beta$ (again defined by $x, y \in R(E)$) extend to morphisms $x \circ \beta, y \circ \beta : E \longrightarrow \mathbf{P}^1_K$, of degrees 2 and 3, respectively; thus $\deg(\beta) = [R(E) : \beta^* R(C)] = 1$, as it divides both 2 and 3. This means that β is birational, i.e. induces an isomorphism $E \xrightarrow{\sim} \widetilde{C}$, where $\widetilde{C}$ is the normalization (canonical desingularization) of C. We claim that C is smooth over K (which implies that $\widetilde{C} = C$, concluding the proof): if not, then the discussion in 1.3.4-5 below shows that $\widetilde{C}_L \xrightarrow{\sim} \mathbf{P}^1_L$ over a suitable finite extension $L \supset K$, which contradicts the fact that $g(\widetilde{C}_L) = g(E_L) = 1 \neq 0 = g(\mathbf{P}^1_L)$.

(1.2.5) The affine curve $C \cap \{Z \neq 0\} = C - \{O\}$ is given by the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.2.5.1}$$

(where $x = X/Z, y = Y/Z$). If $char(K) \neq 2$ (resp. $char(K) \neq 3$), one can simplify (1.2.5.1) by completing the square (resp. the cube), i.e. by the substitution $y + (a_1x + a_3)/2 \mapsto y$ (resp. $x + a_2/3 \mapsto x$). As a result, we obtain the following simplified forms of (1.2.5.1).

(i) If $char(K) \neq 2, 3$, then

$$y^2 = x^3 + a_4x + a_6. \tag{1.2.5.2}$$

(ii) If $char(K) = 3$, then

$$y^2 = x^3 + a_2x^2 + a_4x + a_6. \tag{1.2.5.3}$$

(iii) If $char(K) = 2$, then

$$y^2 + a_1xy + a_3y = x^3 + a_4x + a_6. \tag{1.2.5.4}$$

(1.2.6) The variable (= general = tautological) points. Examples: (i) Let $(E, O) = (C, O)$ be an elliptic curve given by the generalized Weierstrass equation (1.2.4.1). We would like to consider a "general point" (x, y) on $E - \{O\}$, whose coordinates would satisfy the equation (1.2.5.1) (and its consequences), but no other polynomial equations with coefficients in K. Such a point can be constructed as follows: put

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

and let

$$A = K[x, y]/(y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6) = K[x, y]/(f(x, y))$$

be the ring of functions on the affine curve $E - \{O\} = \mathrm{Spec}(A)$; its field of fractions is equal to the field of rational functions on E: $R(E) = \mathrm{Frac}(A)$. Let $\overline{x}, \overline{y}$ be, respectively, the images of x, y in A; the "tautological point" (or "general point") of E is the point with affine coordinates

$$(\overline{x}, \overline{y}) \in (E - \{O\})(A) \subset (E - \{O\})(\mathrm{Frac}(A)) \subset E(\mathrm{Frac}(A)) = E(R(E)).$$

(ii) Sometimes we shall use several "independent" general points of E: for $j = 1, \dots, n$, put

$$A_j = K[x_j, y_j]/(f(x_j, y_j)), \qquad B = A_1 \otimes_K \cdots \otimes_K A_n = K[x_1, y_1, \dots, x_n, y_n]/(f(x_1, y_1), \dots, f(x_n, y_n))$$

and denote by $\overline{x}_j$ (resp. $\overline{y}_j$) the image of x_j (resp. of y_j) in B; then

$$\mathrm{Spec}(B) = (E - \{O\})^n = (E - \{O\}) \times_K \cdots \times_K (E - \{O\}) \subset \underbrace{E \times_K \cdots \times_K E}_{n \text{ factors}} = E^n, \qquad \mathrm{Frac}(B) = R(E^n)$$

and the "tautological point" of E^n

$$((\overline{x}_1, \overline{y}_1), \dots, (\overline{x}_n, \overline{x}_n)) \in (E - \{O\})^n(B) \subset (E - \{O\})^n(\mathrm{Frac}(B)) \subset E^n(\mathrm{Frac}(B)) = E^n(R(E^n))$$

can be viewed as an n-tuple of independent general points of E.
(iii) This construction makes sense for an arbitrary reduced irreducible scheme X: if $\mathrm{Spec}(A) \subset X$ is any (non-empty) open affine subset, then A is an integral domain and the ring of rational functions on X is a field, equal to $R(X) = \mathrm{Frac}(A)$. The canonical maps

$$\mathrm{Spec}(R(X)) = \mathrm{Spec}(\mathrm{Frac}(A)) \longrightarrow \mathrm{Spec}(A) \hookrightarrow X$$

then define the tautological point $P \in X(R(X))$.

(1.2.7) Theorem (E is a "commutative group scheme" over K). (i) *There exist (unique) morphisms $m : E \times_K E \longrightarrow E$ and $\iota : E \longrightarrow E$ such that, for each field $L \supset K$ and all $P, Q \in E(L)$,*

$$P \boxplus Q = m(P, Q), \qquad -P = [-1]P = \iota(P).$$

(ii) **"Associativity".** *The following diagram is commutative:*

$$\begin{array}{ccc} E \times_K E \times_K E & \xrightarrow{\mathrm{id} \times m} & E \times_K E \\ \downarrow{\scriptstyle m \times \mathrm{id}} & & \downarrow{\scriptstyle m} \\ E \times_K E & \xrightarrow{m} & E. \end{array}$$

(iii) **"Commutativity".** *Let $s : E \times_K E \longrightarrow E \times_K E$ be the morphism $s(P,Q) = (Q,P)$; then $m \circ s = m$.*
(iv) **"Inverse".** *The composite morphism*

$$E \xrightarrow{\Delta} E \times_K E \xrightarrow{\mathrm{id}\times\iota} E \times_K E \xrightarrow{m} E$$

(where $\Delta(P) = (P,P)$ is the diagonal map) is the constant map with value O.

Proof. (i) (cf. [Si 1], Thm. III.3.6, if K is perfect). *The inverse:* thanks to 1.2.4, we can assume that $(E,O) = (C,O)$, in which case O is an inflection point of E, hence $-P = O * P$ (cf. I.10.1.4). It follows that, if $P = (x_P, y_P) \in (E - \{O\})(L)$, then $-P$ lies on the vertical line $x - x_P = 0$, hence

$$-(x_P, y_P) = (x_P, -y_P - a_1 x_P - a_3). \tag{1.2.7.1}$$

The formula

$$\iota(x,y) = (x, -y - a_1 x - a_3)$$

defines a morphism $E - \{O\} \longrightarrow E - \{O\}$, hence a rational map

$$E - - \succ E\ ,$$

which automatically extends to a (unique) morphism $\iota : E \longrightarrow E$. As ι is non-constant, it is surjective, hence $\iota(O) = O$, proving that $-P = \iota(P)$ for all $P \in E(L)$ (and all fields $L \supset K$).

One can see directly (without using the formula (1.2.7.1)) that the inverse map is induced, on the points of a suitable (non-empty) open subset $U \subset E - \{O\}$, by a morphism $\iota_U : U \longrightarrow E - \{O\}$: let $P = (\overline{x}, \overline{y}) \in (E - \{O\})(R(E))$ be the tautological point of E constructed in 1.2.6(i); then the point $-P \in (E - \{O\})(R(E))$ (defined using the group law on $E_{R(E)}$) is a morphism $-P : \mathrm{Spec}(R(E)) \longrightarrow E - \{O\}$. The coordinates of $-P$ are rational functions on $E - \{O\}$; removing from $E - \{O\}$ the union of their poles (which turns out to be empty in this case, as $-P = (\overline{x}, -\overline{y} - a_1\overline{x} - a_3)$) we obtain the sought for morphism $\iota_U : U \longrightarrow E - \{O\}$. Note that, in this argument, it was not necessary to assume that $(E,O) = (C,O)$; one could have used the abstract definition of the tautological point from 1.2.6(iii).
The sum $\boxplus$: A similar argument applied to two independent points

$$((\overline{x}_1, \overline{y}_1), (\overline{x}_2, \overline{x}_2)) \in (E - \{O\})^2(R(E \times_K E))$$

shows that there exists a (non-empty) open subset $U \subset E \times_K E$ and a morphism $m_U : U \longrightarrow E$ such that, for all fields $L \supset K$ and all $P, Q \in U(L)$, we have $P \boxplus Q = m_U(P,Q)$. They are several ways to conclude the argument; for example, one can assume that $(E,O) = (C,O)$, in which case the sum $(x_1,y_1) \boxplus (x_2,y_2)$ can be computed explicitly, as in I.7.5.7. The resulting formulas show that the map $(P,Q) \mapsto P \boxplus Q$ is, indeed, defined by a morphism $m_U : U \longrightarrow E$, where $E \times_K E - U = \{(P,P)\} \cup \{(P,-P)\} \cup \{(P,O)\} \cup \{(O,P)\}$. One then shows, again by an explicit calculation, that $\boxplus$ is defined by a morphism on a suitable open set containing $E \times_K E - U$ (see [Si 1], 3.6.1). There is an alternative argument which uses translation maps (see [Si 1], 3.6); in our case one has to be careful, as the field K is not necessarily perfect; hovewer, the set of points $E(K^{sep})$ defined over the separable closure of K is dense in E (as E is smooth over K), which is sufficient for the argument.
(ii) Let $L = R(E \times_K E \times_K E) = R(E^3)$ be the field of rational functions on E^3. As in 1.2.6(ii), we have three independent general points $P_j = (\overline{x}_j, \overline{y}_j) \in E(L)$ $(j = 1,2,3)$ of E, defining the tautological point $(P_1,P_2,P_3) : \mathrm{Spec}(L) \longrightarrow E^3$. As the group operation $\boxplus$ is associative on $E(L)$, we have equalities

$$\begin{gathered} m \circ (m \times \mathrm{id}) \circ (P_1,P_2,P_3) = m \circ (P_1 \boxplus P_2, P_3) = (P_1 \boxplus P_2) \boxplus P_3 = P_1 \boxplus (P_2 \boxplus P_3) = \\ = m \circ (P_1, P_2 \boxplus P_3) = m \circ (\mathrm{id} \times m) \circ (P_1,P_2,P_3) \in E(L). \end{gathered}$$

Interpreting both sides as rational maps $E \times_K E \times_K E - - - - - \succ E$, it follows that the morphisms $m \circ (m \times \mathrm{id})$ and $m \circ (\mathrm{id} \times m)$ define the same rational map. As the target E is projective (hence separated), the two morphisms must be equal. A similar argument proves (iii) and (iv).

(1.2.8) Corollary. (i) *For each $n \in \mathbf{Z}$, multiplication by n (defined as in 0.5.0) on E is given by a morphism $[n] = [n]_E : E \longrightarrow E$.*
(ii) *For each $P \in E(K)$, there is a morphism $\tau_P : E \longrightarrow E$ (the "translation map") such that, for each field $L \supset K$ and each point $Q \in E(L)$, $\quad P \boxplus Q = \tau_P(Q)$.*

Proof. (i) $[0]$ is the constant map equal to O and $[1] = \mathrm{id}$. For $n > 1$, one defines inductively $[n] = m \circ ([n-1] \times \mathrm{id}) \circ \Delta$, where Δ is the diagonal map $\Delta : E \longrightarrow E \times_K E$, $\Delta(P) = (P, P)$. For $n < 0$, $[n] = \iota \circ [-n]$.
(ii) τ_P is defined as the composite morphism

$$E = \mathrm{Spec}(K) \times_K E \xrightarrow{P \times \mathrm{id}} E \times_K E \xrightarrow{m} E.$$

(1.2.9) Exercise. *Let (E, O) be as in 1.2.3.*
(i) *If O is an inflection point of E, show that there exists a linear change of homogeneous coordinates defined over K transforming (E, O) into (C, O) of the form (1.2.4.1).*
(ii) *If O is not an inflection point of E, choose new homogeneous coordinates $(X : Y : Z)$ in such a way that $O = (1 : 0 : 0)$, $\{Z = 0\}$ is the tangent line to E at O, $\{Z = 0\} \cap E = 2(O) + (P)$, where $P = (0 : 1 : 0)$ and $\{X = 0\}$ is the tangent line to E at P. Show that the (rational) change of variables $x' = x$, $y' = xy$ ($x = X/Z$, $y = Y/Z$, as usual) transforms E into a smooth projective cubic curve E' and P into an inflection point P' of E' (see [Cl], 2.4).*

1.3 Non-smooth Generalized Weierstrass Equations

(1.3.1) Assume that the projective plane curve

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

(where $a_j \in K$) is not smooth, i.e. that there exists at least one singular (= non-smooth) point $S \in C(\overline{K})$.

If there were another singular point $T \in C(\overline{K})$, then the intersection of the line $\overline{ST}$ with C would contradict Bézout's Theorem; thus S is unique.

In particular, S is fixed by any element of the automorphism group $\mathrm{Aut}(\overline{K}/K)$, which implies that $K(S)$ (the field of definition of S) is a purely inseparable extension of K.

(1.3.2) The point $S = (x_S, y_S)$ necessarily lies on the affine curve $C_{\mathrm{aff}} = C - \{O\}$, given by the equation

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0,$$

hence

$$\begin{aligned} \partial f/\partial x(S) &= a_1y_S - 3x_S^2 - 2a_2x_S - a_4 = 0, \\ \partial f/\partial y(S) &= 2y_S + a_1x_S + a_3 = 0, \end{aligned}$$

which implies that

$$\begin{aligned} -y_S^2 &= x_S^3 + a_2x_S^2 + a_4x_S + a_6, \\ 2(3x_S^2 + 2a_2x_S + a_4) + a_1(a_1x_S + a_3) &= 0. \end{aligned}$$

If $char(K) \neq 2, 3$, these equations show that

$$[K(S) : K] \leq [K(S) : K(x_S)] \cdot [K(x_S) : K] \leq 2 \cdot 2 = 4,$$

hence $S \in C(K)$ is defined over K.

On the other hand, if K is a non-perfect field of characteristic $p = 2$ (resp. $p = 3$) and $a \in K^*$, $a \notin K^{*p}$, then the curve

$$y^2 = x^3 + a$$

has a non-smooth point $S = (0, a^{1/2})$ (resp. $S = (-a^{1/3}, 0)$) defined over a purely inseparable extension $K(a^{1/p})/K$ of degree p.

(1.3.3) Assume, from now on, that $S \in C(K)$ is defined over K. Applying the change of variables $x \mapsto x - x_S, y \mapsto y - y_S$, we can assume that $S = (0, 0)$, which implies that $a_6 = a_3 = a_4 = 0$, hence C_{aff} is given by

$$y^2 + a_1xy - a_2x^2 = x^3. \tag{1.3.3.1}$$

The tangent cone to C at S is given by the vanishing of the quadratic form on the L.H.S. of (1.3.3.1). In other words, writing $y = \lambda x$, then the roots of

$$Q(\lambda) = \lambda^2 + a_1\lambda - a_2 = 0 \tag{1.3.3.2}$$

are the slopes of the tangents to the various branches of C passing through S.

The geometry of C strongly depends on the nature of the solutions of (1.3.3.2).

(1.3.4) The multiplicative case. Assume that the polynomial $Q(\lambda)$ has two distinct roots $\lambda_1, \lambda_2 \in \overline{K}$. Then $K(\lambda_1, \lambda_2)$ is either equal to K, or is a separable quadratic extension of K.

Let $L \supset K(\lambda_1, \lambda_2)$ be any extension of K over which Q splits. Then the base change of C_{aff} to L is given by

$$(C_L)_{\text{aff}} : (y - \lambda_1 x)(y - \lambda_2 x) = x^3$$

and the rational function

$$t = \frac{y - \lambda_1 x}{y - \lambda_2 x} = \frac{u}{v} \in R(C_L) \tag{1.3.4.1}$$

on C_L – viewed as a rational map to $\mathbf{P}^1_L$ – admits an inverse, which is a birational *morphism*

$$\mathbf{P}^1_L \longrightarrow C_L, \qquad (u : v) \mapsto \left(\frac{u - v}{\lambda_2 - \lambda_1} : \frac{\lambda_2 u - \lambda_1 v}{\lambda_2 - \lambda_1} : \left(\frac{u - v}{\lambda_2 - \lambda_1} \right)^3 \frac{1}{uv} \right), \qquad (1 : 0), (0 : 1) \mapsto S, \tag{1.3.4.2}$$

which identifies $\mathbf{P}^1_L$ with the normalization of C_L. This morphism has a very simple geometric description: $\mathbf{P}^1_L$ parametrizes the set of lines in $\mathbf{P}^2_L$ containing S (with the point $0 = (0 : 1) \in \mathbf{P}^1(L)$ (resp. $\infty = (1 : 0) \in \mathbf{P}^1(L)$) corresponding to the tangent line $y = \lambda_1 x$ (resp. $y = \lambda_2 x$) at S). Each such line ℓ intersects C at S with intersection multiplicity ≥ 2; the map (1.3.4.2) associates to ℓ its third intersection point with C.

(1.3.5) The additive case. Assume that $Q(\lambda)$ has a double root $\lambda \in \overline{K}$. Then $K(\lambda)$ is either equal to K, or is a purely inseparable quadratic extension of K (the latter case can occur only if K is a non-perfect field of characteristic $char(K) = 2$). It follows that $a_1 = 2b_1$ for some $b_1 \in K$; the change of variables $y \mapsto y - b_1 x$ reduces to the case

$$C_{\text{aff}} : y^2 - b_2x^2 = x^3, \qquad b_2 = \lambda^2 \in K, \qquad 2b_2 = 0.$$

Over any field $L \supset K(\lambda)$, we have

$$(C_L)_{\text{aff}} : (y - \lambda x)^2 = x^3$$

and the rational function

$$t = \frac{x}{y - \lambda x} = \frac{u}{v} \tag{1.3.5.1}$$

on C_L has an inverse, which is a morphism

$$\mathbf{P}^1_L \longrightarrow C_L, \qquad (u:v) \mapsto \left(\frac{u^2}{v^2} : \frac{u^3}{v^3} + \lambda\frac{u^2}{v^2} : 1\right), \qquad (1:0) \mapsto S \tag{1.3.5.2}$$

identifying $\mathbf{P}^1_L$ with the normalization of C_L. This morphism has the same geometric description as the map (1.3.4.2).

(1.3.6) The group law on the smooth part of C. If $L \supset K$ is an extension of K, it is tempting to use the same geometric construction as in 1.2.3 to define an abelian group law on $C(L)$ (with $O = (0:1:0)$ as a neutral element). This does not quite work if the line ℓ contains the singular point S, which means that we have to consider only the smooth part of $C(L)$

$$C^{\mathrm{sm}}(L) = C(L) - \{S\}$$

and lines $\ell \subset \mathbf{P}^2_L$ that do not contain S. If $Q_1, Q_2 \in C^{\mathrm{sm}}(L)$, then the line $\ell = \overline{Q_1Q_2}$ (defined to be the tangent to C at Q_1 if $Q_1 = Q_2$) does not contain S – by Bézout's Theorem – and the third intersection Q_3 of ℓ with C also lies in $C^{\mathrm{sm}}(L)$. We put

$$Q_3 := Q_1 * Q_2, \qquad Q_1 \boxplus Q_2 := O * (Q_1 * Q_2). \tag{1.3.6.1}$$

Does (1.3.6.1) define an abelian group structure on $C^{\mathrm{sm}}(L)$ (with neutral element $O = (0:1:0)$)? Let us analyze the situation in more detail.

(1.3.7) The split multiplicative case. Assume that we are in the multiplicative case 1.3.4 and that $L \supset K(\lambda_1, \lambda_2)$. In the homogeneous coordinates $(U_1 : U_2 : Z)$, where $U_j = Y - \lambda_j X$, the curve C_L is given by

$$C_L : (\lambda_2 - \lambda_1)^3 U_1 U_2 Z = (U_1 - U_2)^3, \qquad S = (0:0:1)$$

and the rational function (1.3.4.1) defines a bijection

$$t = \frac{U_1}{U_2} : C^{\mathrm{sm}}(L) \xrightarrow{\sim} \mathbf{P}^1(L) - \{0, \infty\} = L^*.$$

Assume that the line $\ell : Z = aU_1 + bU_2$ intersects C^{sm} at three points Q_1, Q_2, Q_3. Then

$$(t-1)^3 - (\lambda_2 - \lambda_1)^3 t(at+b) = (t - t(Q_1))(t - t(Q_2))(t - t(Q_3)),$$

which implies that

$$t(Q_1)t(Q_2)t(Q_3) = 1,$$

hence t defines an isomorphism of abelian groups

$$(C^{\mathrm{sm}}(L), \boxplus) \xrightarrow{\sim} (L^*, \times).$$

(1.3.8) The split additive case. Assume that we are in the additive case 1.3.5 and that $L \supset K(\lambda)$. In the homogeneous coordinates $(X : Y : Z)$, the curve C_L is given by

$$C_L : (Y - \lambda X)^2 Z = X^3, \qquad S = (0:0:1)$$

and the rational function (1.3.5.1) defines a bijection

$$t = \frac{X}{Y - \lambda X} : C^{\mathrm{sm}}(L) \xrightarrow{\sim} \mathbf{P}^1(L) - \{\infty\} = L.$$

Assume that the line $\ell : Z = aX + bY$ intersects C^{sm} at three points Q_1, Q_2, Q_3. Then

$$t^3 - (at+b) = (t - t(Q_1))(t - t(Q_2))(t - t(Q_3)),$$

which implies that

$$t(Q_1) + t(Q_2) + t(Q_3) = 0,$$

hence t defines an isomorphism of abelian groups

$$(C^{\mathrm{sm}}(L), \boxplus) \xrightarrow{\sim} (L, +).$$

(1.3.9) The non-split multiplicative case. Assume that we are in the multiplicative case 1.3.4 and that $K' := K(\lambda_1, \lambda_2)$ is not equal to K. Then K'/K is a Galois extension of degree 2; let σ be the non-trivial element of $\mathrm{Gal}(K'/K)$. Then $\lambda_2 = \sigma(\lambda_1)$ and the discussion in 1.3.7 implies that the rational function

$$t = \frac{y - \lambda_1 x}{y - \sigma(\lambda_1)x}$$

induces an isomorphism of abelian groups

$$t : C^{\mathrm{sm}}(K) \xrightarrow{\sim} \{w/\sigma(w) \,|\, w \in (K')^*\} = \mathrm{Ker}\left(N_{K'/K} : (K')^* \longrightarrow K^*\right) \tag{1.3.9.1}$$

(the last equality by Hilbert's Theorem 90, as in 0.4.2.0). The group on the R.H.S. of (1.3.9.1) is usually referred to as the "twisted multiplicative group". We have already encountered it in our discussion of the group of points on the circle $x^2 + y^2 = 1$ in 0.4.2.

(1.3.10) The non-split additive case. Assume that we are in the additive case 1.3.5 and that $K' := K(\lambda)$ is not equal to K. Then $char(K) = 2$ and K'/K is a purely inseparable extension of degree 2, with $\lambda^2 = b_2 \in K$.

For $Q = (x, y) \in C^{\mathrm{sm}}_{\mathrm{aff}}(K)$, write the value $t(Q)$ in the basis $1, -\lambda$ of K'/K:

$$t(Q) = \frac{x}{y - \lambda x} = \frac{y - \lambda x}{x^2} = \alpha - \lambda\beta, \qquad \alpha, \beta \in K.$$

Then

$$\alpha^2 - b_2\beta^2 = (\alpha - \lambda\beta)^2 = \frac{(y - \lambda x)^2}{x^4} = \frac{1}{x} = \beta,$$

and the discussion in 1.3.8 implies that t induces an isomorphism of abelian groups

$$t : C^{\mathrm{sm}}(K) \xrightarrow{\sim} \left(\{\alpha - \lambda\beta \,|\, \alpha, \beta \in K,\, \alpha^2 - b_2\beta^2 = \beta\}, +\right)$$

(the "twisted additive group").

(1.3.11) Exercise ([Be]). *Let $Q \subset \mathbf{P}^2_K$ be a smooth conic and $L \subset \mathbf{P}^2_K$ a line (both defined over K). Fix a point $O \in Q(K) - L(K)$.*
(i) *Show that the recipe (I.10.1.1.1) applied to the* **reducible** *cubic curve $Q \cup L \subset \mathbf{P}^2_K$ defines an abelian group law on $Q(K) - L(K)$.*
(ii) *Describe the structure of this group (it depends on the nature of the intersection $Q \cap L$).*
(iii) *What is the relation to the group law on the circle (0.1.1)?*

(1.3.12) Exercise. *Relate the discussion in 1.3.7-8 to (an algebraic version of) I.3.9.13(ii), using 1.3.4-5.*

2. Isogenies (definitions and examples)

2.1 Definitions and basic properties

(2.1.1) Definition. *Let (E,O) and (E',O') be elliptic curves over K. An* **isogeny** *$\lambda : E \longrightarrow E'$ is a non-constant morphism of curves over K satisfying $\lambda(O) = O'$ (hence λ induces an isogeny $\lambda_L = \lambda \times \mathrm{id} : E_L = E \otimes_K L \longrightarrow E'_L = E' \otimes_K L$, for any field $L \supset K$). The* **degree** *of the isogeny λ is the degree of the field extension $R(E)/\lambda^*(R(E'))$.*

(2.1.2) Proposition. *If $\lambda : E \longrightarrow E'$ is an isogeny, then the induced map on K-rational points $\lambda : E(K) \longrightarrow E'(K)$ is a homomorphism of abelian groups.*

Proof. (cf. [Si 1], Thm. III.4.8, if K is perfect). This follows from the commutative diagram

$$\begin{array}{ccc} E(K) & \xrightarrow{\lambda} & E'(K) \\ \downarrow\wr & & \downarrow\wr \\ Cl^0(E) & \xrightarrow{\lambda_*} & Cl^0(E'), \end{array}$$

where the map λ_* is defined on the level of divisors by $\lambda_*(\sum n_P(P)) = \sum n_P(\lambda(P))$ if K is perfect, and by $\lambda_*(\sum n_x(x)) = \sum n_x[k(x) : k(\lambda(x))](x)$ in general.

(2.1.3) Proposition (Isogenies are "homomorphisms of groups schemes"). *If $\lambda : E \longrightarrow E'$ is an isogeny, then:*
(i) *λ commutes with the group laws on E and E', i.e. the following diagram is commutative:*

$$\begin{array}{ccc} E \times_K E & \xrightarrow{\lambda\times\lambda} & E' \times_K E' \\ \downarrow m & & \downarrow m' \\ E & \xrightarrow{\lambda} & E'. \end{array}$$

(ii) $(\forall n \in \mathbf{Z}) \quad \lambda \circ [n]_E = [n]_{E'} \circ \lambda$.

Proof. The statement (i) is proved by the same argument as in 1.2.8(ii): let $L = R(E \times_K E)$ be the field of rational functions on $E \times_K E$ and $((\overline{x}_1, \overline{y}_1), (\overline{x}_2, \overline{y}_2)) \in (E \times_K E)(L)$ the tautological point of $E \times_K E$, defined in 1.2.6(ii). Applying 2.1.2 to $\lambda_L : E_L \longrightarrow E'_L$, we obtain

$$\lambda_L((\overline{x}_1, \overline{y}_1) \boxplus (\overline{x}_2, \overline{y}_2)) = \lambda_L(\overline{x}_1, \overline{y}_1) \boxplus \lambda_L(\overline{x}_2, \overline{y}_2) \in E'(L).$$

Interpreting both sides as rational maps $\beta : E \times_K E \dashrightarrow E'$, it follows that the morphisms $\lambda \circ m, m' \circ (\lambda \times \lambda) : E \times_K E \longrightarrow E'$ define the same rational map. As the target E' is projective (hence separated), the morphisms $\lambda \circ m$ and $m' \circ (\lambda \times \lambda)$ must be equal. The statement (ii) follows from (i) by induction on $|n|$.

(2.1.4) Notation. For elliptic curves E, E' over K and a field $L \supset K$, we denote

$$\begin{aligned} \mathrm{Hom}_L(E,E') &= \{0\} \cup \{\lambda : E_L \longrightarrow E'_L \mid \lambda \text{ is an isogeny}\} \\ \mathrm{Isom}_L(E,E') &= \{\lambda \in \mathrm{Hom}_L(E,E') \mid \lambda \text{ is an isomorphism}\} = \{\lambda \in \mathrm{Hom}_L(E,E') \mid \deg(\lambda) = 1\} \\ \mathrm{End}_L(E) &= \mathrm{Hom}_L(E,E), \qquad \mathrm{Aut}_L(E) = \mathrm{Isom}_L(E,E), \end{aligned}$$

where 0 is the constant morphism with value O'. If $\lambda : E \longrightarrow E'$ is an isogeny, we put

$$\mathrm{Ker}(\lambda)(L) = \{P \in E(L) \mid \lambda(P) = O'\}.$$

(2.1.5) Exercise. *Show that $\mathrm{End}_L(E)$ is a ring with respect to the operations $\lambda \boxplus \mu$ and $\lambda\mu = \lambda \circ \mu$, where*

$$\lambda \boxplus \mu : E \xrightarrow{\Delta} E \times_K E \xrightarrow{\lambda\times\mu} E \times_K E \xrightarrow{m} E$$

($\Delta(P) = (P, P)$ is the diagonal map). [Hint: The proof of one of the distributive laws requires 2.1.3.]

(2.1.6) Exercise. *If $\lambda \in \mathrm{Hom}_L(E, E')$, $\mu \in \mathrm{Hom}_L(E', E'')$ and $\mu \circ \lambda = 0$, then $\lambda = 0$ or $\mu = 0$. In particular, the ring $\mathrm{End}_L(E)$ does not have zero divisors.*

(2.1.7) Proposition. *Let $k = \mathbf{Q}$ (resp. $k = \mathbf{F}_p$) if $char(K) = 0$ (resp. if $char(K) = p > 0$). If E, E' are elliptic curves over K and $\lambda \in \mathrm{Hom}_K(E, E')$, then there exists a subfield $K_0 \subset K$ of finite type over k, elliptic curves E_0, E_0' over K_0 and an element $\lambda_0 \in \mathrm{Hom}_{K_0}(E_0, E_0')$ such that $\lambda = (\lambda_0)_K$ is the base change of λ_0.*

Proof. We take K_0 to be the field generated over k by the coefficients of the (finitely many) polynomials defining E, E' and λ.

(2.1.8) Assume that (E, O) and (E', O') are elliptic curves over $\mathbf{C}$ and $\lambda \in \mathrm{Hom}_{\mathbf{C}}(E, E') - \{0\}$ an isogeny. Fix isomorphisms $(E, O) \xrightarrow{\sim} (C, O)$, $(E', O') \xrightarrow{\sim} (C', O')$ (defined over $\mathbf{C}$) with elliptic curves in the form (1.2.4.1). The Abel-Jacobi maps from I.4.4.1 then define isomorphisms of Riemann surfaces $C(\mathbf{C}) \xrightarrow{\sim} \mathbf{C}/L$, $C'(\mathbf{C}) \xrightarrow{\sim} \mathbf{C}/L'$ (under which O, O' correspond to 0), for suitable lattices $L, L' \subset \mathbf{C}$. The holomorphic map $\lambda^{an} : E(\mathbf{C}) \longrightarrow E'(\mathbf{C})$ (given by λ) then gives rise, via the above isomorphisms, to a non-constant holomorphic map $\mu : \mathbf{C}/L \longrightarrow \mathbf{C}/L'$ satisfying $\mu(0) = 0$, i.e. an isogeny in the analytic sense (cf. I.7.6.3). Conversely, any such μ is algebraic, i.e. comes from a (unique) isogeny $\lambda : E \longrightarrow E'$ (this follows from I.7.6.6(ii)). In particular, we have, in the notation of I.7.6.7,

$$\mathrm{End}_{\mathbf{C}}(E) = \mathrm{End}(\mathbf{C}/L).$$

(2.1.9) Exercise. *Let E be an elliptic curve over a field K of characteristic $char(K) = 0$. Then there exists a subfield $K_0 \subset K$ of finite type over $\mathbf{Q}$, an elliptic curve E_0 over K_0 satisfying $(E_0)_K \xrightarrow{\sim} E$ and*

$$\mathrm{End}_K(E) = \mathrm{End}_{K_0}(E_0) = \mathrm{End}_{\mathbf{C}}(E_0) = \begin{cases} \mathbf{Z} \\ \\ \mathbf{Z} + \mathbf{Z}\alpha, \qquad \alpha^2 + a\alpha + b = 0,\ a, b \in \mathbf{Z},\ a^2 - 4b < 0. \end{cases}$$

(for some embedding $K_0 \hookrightarrow \mathbf{C}$).

2.2 Isomorphisms (= isogenies of degree one)

(2.2.1) Let E, E' be elliptic curves over K. We would like to determine the set $\mathrm{Isom}_L(E, E')$ of isomorphisms between E_L and E_L' over various extensions L of K. Thanks to 1.2.4 we can assume that both E and E' are given by a generalized Weierstrass equation, with the corresponding affine curves of the form

$$\begin{aligned} E - \{O\} &: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \\ E' - \{O'\} &: y'^2 + a_1'x'y' + a_3'y' = x'^3 + a_2'x'^2 + a_4'x' + a_6' \end{aligned} \tag{2.2.1.1}$$

(where $a_i, a_i' \in K$).

(2.2.2) Proposition. *Any element of $\mathrm{Isom}_K(E, E')$ is given by the formulas*

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + u^2sx' + t \end{aligned} \qquad (r, s, t \in K,\ u \in K^*). \tag{2.2.2.1}$$

Conversely, any change of variables (2.2.2.1) transforms E into an elliptic curve E' over K in a generalized Weierstrass form.

Proof. (cf. [Si 1], III.3.1(b)). Any $\lambda \in \mathrm{Isom}_K(E, E')$ induces isomorphisms of vector spaces

$$\lambda^* : L(n(O')) \xrightarrow{\sim} L(n(O)), \qquad f' \mapsto f \circ \lambda$$

(for all $n \in \mathbf{Z}$). This implies, by the definition of x, y, x', y' (see the proof of 1.2.4), that

$$x = \lambda^*(ax' + b), \qquad y = \lambda^*(cy' + dx' + e),$$

for some constants $a, b, c, d, e \in K$ with $a, c \neq 0$. As

$$y^2 - x^3 \in L(5(O)), \qquad y'^2 - x'^3 \in L(5(O')),$$

it follows that $c^2 = a^3$; putting $u = c/a \in K^*$, we obtain $a = u^2$ and $c = u^3$, as claimed. The converse statement is trivial (as the map (2.2.2.1) has an inverse of the same form).

(2.2.3) Special case: *$char(K) \neq 2, 3$.* If the characteristic of K is not equal to 2 or 3, then we can assume (by 1.2.5) that the curves E, E' are in the form

$$E - \{O\} : y^2 = x^3 + a_4x + a_6, \qquad E' - \{O'\} : y'^2 = x'^3 + a'_4x' + a'_6. \tag{2.2.3.1}$$

The only transformations (2.2.2.1) preserving the equations (2.2.3.1) are given by

$$x = u^2x', \qquad y = u^3y' \qquad\qquad (u \in K^*). \tag{2.2.3.2}$$

The substitution (2.2.3.2) transforms $E - \{O\}$ into

$$E' - \{O'\} : (u^3y')^2 = (u^2x')^3 + a_4(u^2x') + a_6 \iff y'^2 = x'^3 + u^{-4}a_4x' + u^{-6}a_6,$$

hence

$$a'_4 = u^{-4}a_4, \qquad a'_6 = u^{-6}a_6. \tag{2.2.3.3}$$

We have thus proved the following

(2.2.4) Proposition. *Let E, E' be elliptic curves of the form (2.2.3.1) over a field K of characteristic $char(K) \neq 2, 3$. Then, for any field $L \supset K$, the formulas (2.2.3.2) define a bijection*

$$\mathrm{Isom}_L(E, E') \xrightarrow{\sim} \{u \in L^* \mid u^{-4}a_4 = a'_4,\ u^{-6}a_6 = a'_6\}.$$

(2.2.5) Corollary. *Under the assumptions of 2.2.4,*

$$\mathrm{Aut}_L(E) = \begin{cases} \mu_2(L) = \{\pm 1\}, & a_4, a_6 \neq 0 \\ \mu_4(L), & a_6 = 0 \ (\Longrightarrow a_4 \neq 0) \\ \mu_6(L), & a_4 = 0 \ (\Longrightarrow a_6 \neq 0), \end{cases}$$

where $\mu_n(L) = \{u \in L^* \mid u^n = 1\}$.

(2.2.6) The discriminant and the j-invariant (*$char(K) \neq 2, 3$*). Let us write the equation of E in the form

$$E - \{O\} : y^2 = x^3 + Ax + B \qquad\qquad (A, B \in K).$$

By I.3.7.7,

$$E \text{ is smooth} \iff 0 \neq \mathrm{disc}(x^3 + Ax + B) = -4A^3 - 27B^2.$$

Mimicking the formulas from the analytic theory over $\mathbf{C}$ (I.7.1.10), we write

$$(2y)^2 = 4x^3 - g_2x - g_3 \qquad\qquad (g_2 = -4A,\ g_3 = -4B)$$

and put

$$\Delta = g_2^3 - 27g_3^2 = -16(4A^3 + 27B^2), \qquad j(E) = \frac{(12g_2)^3}{\Delta} = \frac{4(12A)^3}{4A^3 + 27B^2}.$$

Similarly, write E' in the form

$$E' - \{O'\} : y'^2 = x'^3 + A'x' + B' \qquad\qquad (A', B' \in K).$$

If there is an isomorphism $\lambda : E_L \xrightarrow{\sim} E'_L$ (over some field $L \supset K$), then there exists $u \in L^*$ satisfying

$$u^{-4}A = A', \qquad u^{-6}B = B' \tag{2.2.6.1}$$

(by 2.2.4), hence

$$j(E') = \frac{4(12A)^3 u^{-12}}{4A^3 u^{-12} + 27B^2 u^{-12}} = j(E).$$

Conversely, if $j(E) = j(E') \neq 0$, then $B^2/A^3 = B'^2/A'^3$, hence (2.2.6.1) holds for suitable $u \in \overline{K}^*$ (this is also true if $j(E) = j(E') = 0$, for trivial reasons). We have thus proved the following

(2.2.7) Proposition. *Let E, E' be elliptic curves over a field K of characteristic $char(K) \neq 2, 3$. Then the following conditions are equivalent:*
(i) $j(E) = j(E')$.
(ii) *There exists a field $L \supset K$ and an isomorphism $E_L \xrightarrow{\sim} E'_L$.*
(iii) *There exists a field $L \supset K$ of finite degree over K and an isomorphism $E_L \xrightarrow{\sim} E'_L$.*

(2.2.8) Examples: Let $A, B \in K$, $D \in K^*$.
(1) If $2(4A^3 + 27B^2) \neq 0 \in K$, then the elliptic curves

$$E : y^2 = x^3 + Ax + B, \qquad E' : Dy'^2 = x'^3 + Ax' + B$$

(written in the affine form) become isomorphic over $L = K(\sqrt{D})$. The curve E' is usually referred to as the **quadratic twist of E over $K(\sqrt{D})/K$**, as its isomorphism class over K depends only on the field $K(\sqrt{D})$.
(2) If $2A \neq 0 \in K$, then the elliptic curves

$$E : y^2 = x^3 + Ax, \qquad E' : y'^2 = x'^3 + DAx'$$

become isomorphic over $L = K(\sqrt[4]{D})$.
(3) If $6B \neq 0 \in K$, then the elliptic curves

$$E : y^2 = x^3 + B, \qquad E' : y'^2 = x'^3 + DB$$

become isomorphic over $L = K(\sqrt[6]{D})$.

(2.2.9) Exercise. *Let E, E' be as in 2.2.8(n); show that E is isomorphic to E' (over K) $\iff$ $D \in K^{*2n}$ $(n = 1, 2, 3)$.*

(2.2.10) Exercise. *Let E, E' be elliptic curves over a field K of characteristic $char(K) \neq 2, 3$. Assume that there exists an extension $L \supset K$ and an isomorphism $E_L \xrightarrow{\sim} E'_L$. Show that the pair (E, E') is isomorphic (over K) to one of the pairs in 2.2.8, for suitable $D \in K^*$.*

(2.2.11) Exercise. *Let K be a field of characteristic $char(K) \neq 2, 3$ and $j \in K$. Show that there exists an elliptic curve E over K with $j(E) = j$.*

(2.2.12) Exercise. *Let $L, L' \subset \mathbf{C}$ be lattices satisfying $j(L) = j(L')$. Show that there exists $\lambda \in \mathbf{C}^*$ such that $L' = \lambda L$.*

(2.2.13) Exercise. *Give an explicit list of isomorphism classes of elliptic curves over $\mathbf{F}_2$. Which among them become isomorphic over $\mathbf{F}_4$?*

2.3 Multiplication maps

(2.3.1) Proposition. *Let E be an elliptic curve over a field K. Then, for each $n \in \mathbf{Z} - \{0\}$, the multiplication by n is an isogeny $[n] : E \longrightarrow E$ (i.e. $[n]$ is not constant).*

Proof. We only sketch the argument; see ([Si 1], III.4.2(a)) for more details. We can assume that $n > 1$; as $[n](O) = O$, we have to show that $[n]$ is not the constant map with value O. If $char(K) \neq 2$, then an explicit calculation of $[2](x, y)$ shows that the set $E(\overline{K})[2] = \mathrm{Ker}([2])(\overline{K})$ is finite ($\Longrightarrow$ [2] in not constant $\Longrightarrow$ $[2^k]$ is not constant for all $k \geq 1$) and contains a point $P \neq O$; thus, if $2 \nmid m$, then $[m](P) = P \neq O$, hence $[m]$ is not constant. It follows that $[2^k \cdot m]$ is not constant, either. For $char(K) = 2$ one applies the same argument, with [2] replaced by [3].

(2.3.2) Corollary. *The map $n \mapsto [n]$ is an injective homomorphism $\mathbf{Z} \hookrightarrow \mathrm{End}_K(E)$.*

(2.3.3) We shall see later on that $\deg([n]) = n^2$, and that $[n]$ is 'unramified' $\iff$ $char(K) \nmid n$.

2.4 Isogenies of degree two ($char(K) \neq 2$)

(2.4.1) The analytic version. If $L \subset L' \subset \mathbf{C}$ are lattices in $\mathbf{C}$ such that $L'/L \xrightarrow{\sim} \mathbf{Z}/2\mathbf{Z}$, then the identity on $\mathbf{C}$ induces a holomorphic map

$$\lambda : \mathbf{C}/L \longrightarrow \mathbf{C}/L' \tag{2.4.1.1}$$

of degree $\deg(\lambda) = 2$. Conversely, it follows from I.7.6.1 that every holomorphic map $\lambda : \mathbf{C}/L \longrightarrow \mathbf{C}/L'$ of degree $\deg(\lambda) = 2$ between two tori is given by the above construction, possibly after replacing L by αL (for suitable $\alpha \in \mathbf{C}^*$).

The Theorem on Elementary Divisors implies that there is a basis ω_1, ω_2 of L such that $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$, $L' = \mathbf{Z}\frac{\omega_1}{2} + \mathbf{Z}\omega_2$. The kernel of λ is then equal to $\mathrm{Ker}(\lambda) = \{0, \omega_1/2 \ (\mathrm{mod}\, L)\}$, where $\omega_1/2 \ (\mathrm{mod}\, L)$ is a point of exact order 2 on $\mathbf{C}/L$.

(2.4.2) The algebraic version. Let E be an elliptic curve over a field K of characteristic $char(K) \neq 2$ and $P_0 \in E(K) - \{O\}$ a K-rational point satisfying $[2]P_0 = O$.

We can assume that E is given in the generalized Weierstrass form

$$E - \{O\} : y^2 = f(x) = x^3 + ax^2 + bx + c \qquad\qquad (a, b, c \in K),$$

where the polynomial $f \in K[x]$ has distinct roots $e_1, e_2, e_3 \in \overline{K}$. As $P_0 = (e_1, 0)$ (say) is K-rational, we can replace x by $x - e_1$, hence assume that E is in the form

$$E - \{O\} : y^2 = x(x^2 + ax + b), \qquad P_0 = (0, 0), \qquad a, b \in K, \qquad b(a^2 - 4b) \neq 0$$

(the last condition is equivalent to E being smooth).

We would like to construct an isogeny $\lambda : E \longrightarrow E'$ of degree two with "$\mathrm{Ker}(\lambda)$" equal to $\{O, P_0\}$. Morally, this means that (the pull-backs under λ) of rational functions on E' will correspond to those rational functions on E which are invariant under the translation $\tau_{P_0} : P \mapsto P \boxplus P_0$ (as in I.7.6.6).

(2.4.3) In the analytic case 2.4.1, the functions

$$f(z) = \wp(z; L) + \wp(z + \frac{\omega_1}{2}; L), \qquad f'(z) = \wp'(z; L) + \wp'(z + \frac{\omega_1}{2}; L)$$

are both L'-periodic, have poles of order 2 (resp. 3) at $z \in L'$ (and no other poles) and have Laurent expansions

$$f(z) = z^{-2} + c_0 + \cdots, \qquad f'(z) = -2z^{-3} + c_1 z + \cdots$$

at $z = 0$. This implies that

$$f(z) = \wp(z; L') + c_0, \qquad f'(z) = \wp'(z; L'), \tag{2.4.3.1}$$

hence the isogeny λ is given by the formula

$$\lambda(\wp(z;L),\wp'(z;L)) = (f(z)-c_0, f'(z)).$$

It remains to express the functions $f(z), f'(z)$ in terms of $(x,y) = (\wp(z;L),\wp'(z;L))$.

(2.4.4) We shall do this calculation in the algebraic setup: denote the coordinates of a point $P \in E - \{O\}$ by $(x(P), y(P))$ and put

$$X := x(P) + x(P \boxplus P_0) + c, \qquad Y := y(P) + y(P \boxplus P_0),$$

where $c \in K$ is a constant, to be determined later. As the line

$$y = \frac{y(P)}{x(P)}x$$

intersects E at the points

$$P_0 = (0,0), \qquad P = (x(P), y(P)), \qquad [-1](P \boxplus P_0) = (x(P \boxplus P_0), -y(P \boxplus P_0)),$$

it follows that

$$x(x^2+ax+b) - \left(\frac{y(P)}{x(P)}x\right)^2 = x(x-x(P))(x-x(P \boxplus P_0)),$$

hence

$$a + x(P) + x(P \boxplus P_0) = \left(\frac{y(P)}{x(P)}\right)^2, \qquad x(P)x(P \boxplus P_0) = b.$$

Taking $c = a$ and dropping P from the notation, we obtain

$$X = x + a + \frac{b}{x} = \left(\frac{y}{x}\right)^2, \qquad Y = \frac{y}{x}\left(x - \frac{b}{x}\right) \tag{2.4.4.1}$$

and

$$Y^2 = X\left(x^2 - 2b + \frac{b^2}{x^2}\right) = X\left(\left(x+\frac{b}{x}\right)^2 - 4b\right) = X((X-a)^2 - 4b).$$

To sum up, E' is given by the equation

$$E' - \{O'\} : Y^2 = X(X^2 - 2aX + (a^2-4b)) = X(X^2 + a'X + b') \tag{2.4.4.2}$$

and $\lambda : E \longrightarrow E'$ by (2.4.4.1). Note that E' is smooth, as

$$b'(a'^2 - 4b') = (a^2-4b)\cdot 16b \neq 0.$$

(2.4.5) Exercise. *Express $j = j(E)$ and $j' = j(E')$ in terms of the parameter $u = 4b/a^2 \in \mathbf{P}^1(K)$. For which values of u is $j = j'$?*

(2.4.6) Relation to Complex Multiplication. Assume that, in the analytic situation, there is an element $\lambda \in \mathcal{O} = \mathrm{End}(\mathbf{C}/L)$ satisfying $\lambda\overline{\lambda} = 2$. Multiplication by λ then induces an isogeny $[\lambda] : \mathbf{C}/L \longrightarrow \mathbf{C}/L$ of degree $\deg([\lambda]) = 2$, so in this case E' is isomorphic to E, hence $j = j'$.

The possible values of λ (up to the action of $\mathrm{Aut}(\mathbf{C}/L)$) are the following:

$$\begin{aligned} &\mathcal{O} = \mathbf{Z}[i], && \lambda = 1+i \\ &\mathcal{O} = \mathbf{Z}[i\sqrt{2}], && \lambda = i\sqrt{2} \\ &\mathcal{O} = \mathbf{Z}[\frac{1+i\sqrt{7}}{2}], && \lambda = \frac{1\pm i\sqrt{7}}{2}. \end{aligned} \tag{2.4.6.1}$$

(2.4.7) Exercise. *Compute $j(\mathcal{O})$ for $\mathcal{O}$ from (2.4.6.1).*

(2.4.8) Iterating this construction. If we apply the procedure from 2.4.4 to the curve E', we obtain an isogeny $\lambda' : E' \longrightarrow E''$, where E'' is given by

$$E'' - \{O''\} : v^2 = u(u^2 + 4au + 16b)$$

and

$$\lambda'(X,Y) = (u,v) = \left(\left(\frac{Y}{X} \right)^2, \frac{Y}{X} \left(X - \frac{a^2 - 4b}{X} \right) \right).$$

Note that the formulas

$$x = u/4, \qquad y = v/8$$

define an isomorphism $E'' \xrightarrow{\sim} E$; denote by $\widehat{\lambda} : E' \longrightarrow E$ its composition with λ'.

(2.4.9) Exercise. *Show that $\widehat{\lambda} \circ \lambda = [2]$, i.e. $\widehat{\lambda}$ is the "dual isogeny" to λ.*

(2.4.10) This implies that, in the analytic setup 2.4.1, $E'' = \mathbf{C}/L''$, where $L'' = \mathbf{Z}\frac{\omega_1}{2} + \mathbf{Z}\frac{\omega_2}{2} = \frac{1}{2}L$ and λ' is again induced by the identity on $\mathbf{C}$.

2.5 Complex Multiplication by $\mathbf{Z}[i]$

(2.5.1) The projective curves V and E from I.8.1-3, which were constructed from the affine curves

$$V_{\text{aff}} : y^2 = 1 - x^4, \qquad E_{\text{aff}} : v^2 = 4u^3 - 4u,$$

can be considered over an arbitrary field K. If $char(K) \neq 2$, which we shall assume throughout Sect. 2.5, both V and E are smooth over K. In fact, V and E are elliptic curves with distinguished points $O_V = (0,1)$, $O_E = (0:1:0)$ and the map $f : V \longrightarrow E$, $f(x,y) = (1/x^2, -2y/x^3)$ from I.8.3.2 is an isogeny of degree 2. The group law on both V and E is given by the same formulas as over $\mathbf{C}$ (see (I.8.4.2.2)).

(2.5.2) Action of $\mathbf{Z}[i]$. Assume that the polynomial $T^2 + 1$ is reducible over K; fix one of its roots $I \in K$, $I^2 = -1$.

(2.5.2.1) Definition. *Define morphisms $[i]_X : X \longrightarrow X$ ($X = V, E$) by the same formulas as in the analytic case (I.8.4.1.1)):*

$$[i]_V : V \longrightarrow V, \qquad (x,y) \mapsto (Ix, y); \qquad [i]_E : E \longrightarrow E, \qquad (u,v) \mapsto (-u, Iv).$$

(2.5.2.2) Exercise. *For $X = V, E$, the morphism $[i]_X$ is an automorphism $[i]_X \in \mathrm{Aut}_K(X)$ satisfying*

$$[i]_X \circ [i]_X = [-1]_X, \qquad (\forall n \in \mathbf{Z}) \;\; [i]_X \circ [n]_X = [n]_X \circ [i]_X, \qquad [i]_E \circ f = f \circ [i]_V.$$

(2.5.2.3) Definition. *For $X = V, E$ and $m + ni \in \mathbf{Z}[i]$ ($m, n \in \mathbf{Z}$), define a morphism $[m+ni]_X \in \mathrm{End}_K(X)$ by*

$$[m + ni]_X = [m]_X \boxplus ([n]_X \circ [i]_X) : X \longrightarrow X.$$

(2.5.2.4) Exercise. *For $X = V, E$ and $\alpha, \beta \in \mathbf{Z}[i]$,*

$$[\alpha]_X \boxplus [\beta]_X = [\alpha + \beta]_X, \qquad [\alpha]_X \circ [\beta]_X = [\alpha\beta]_X, \qquad [\alpha]_E \circ f = f \circ [\alpha]_V.$$

(2.5.2.5) Exercise. *The formulas from I.8.3.7(ii) define an isomorphism of curves $g : V \xrightarrow{\sim} E$ (over K) satisfying $f(O_V) = O_E$. [This shows that V is, indeed, an elliptic curve.]*

(2.5.3) Lemma. *Let $X = V, E$. For each $\alpha \in \mathbf{Z}[i] - \{0\}$, the morphism $[\alpha]_X : X \longrightarrow X$ is an isogeny (hence the map $\alpha \mapsto [\alpha]_X$ induces an injective ring homomorphism $\mathbf{Z}[i] \longrightarrow \mathrm{End}_K(X)$).*

Proof. As $\alpha \neq 0$, the composite morphism $[\alpha]_X \circ [\overline{\alpha}]_X = [\alpha\overline{\alpha}]_X$ is non-zero (by 2.3.1), hence $[\alpha]_X$ is non-zero as well.

(2.5.4) Exercise. *Show that, for each* $\alpha \in \mathbf{Z}[i] - \{0\}$, $\deg([\alpha]_X) = N\alpha = \alpha\overline{\alpha}$. *[Hint: if* $char(K) = p > 0$, *factorize* α *in* $\mathbf{Z}[i]$ *and use I.9.3.7,10.]*

(2.5.5) A supersingular example. If $p \equiv 3 \pmod 4$ is a prime number, then $K = \mathbf{Z}[i]/p\mathbf{Z}[i]$ is a field isomorphic to $\mathbf{F}_{p^2}$; let $I \in K$ be the image of i in K.

The endomorphism ring $\mathrm{End}_K(V)$ contains the following elements: $[i]_V$ satisfying $[i]_V^2 = -1$ (where we simplify the notation and write n instead of $[n]_V$, for $n \in \mathbf{Z}$) and also the *Frobenius morphism*

$$\phi_p : V \longrightarrow V, \qquad (x, y) \mapsto (x^p, y^p),$$

which will be investigated in more detail in 3.1 below. The congruence I.8.4.9 for $\alpha = -p$ and the formulas

$$\phi_p \circ [i]_V(x, y) = \phi_p(Ix, y) = (I^p x^p, y^p) = (-Ix^p, y^p) = [-i]_V(x^p, y^p) = [-i]_V \circ \phi_p(x, y)$$

imply that

$$\phi_p^2 = [-p]_V = -p, \qquad \phi_p \circ [i]_V = [-i]_V \circ \phi_p.$$

To sum up, we have constructed a (non-zero) homomorphism of rings

$$\begin{gathered} \mathbf{Z}[I, J]/ < I^2 = -1, J^2 = -p, IJ = -JI > \longrightarrow \mathrm{End}_K(V) \\ I \mapsto [i]_V, \qquad J \mapsto \phi_p. \end{gathered} \tag{2.5.5.1}$$

Tensoring (2.5.5.1) with $\mathbf{Q}$ we obtain a (non-zero) homomorphism of $\mathbf{Q}$-algebras

$$B := \mathbf{Q}[I, J]/ < I^2 = -1, J^2 = -p, IJ = -JI > \longrightarrow \mathrm{End}_K(V) \otimes_{\mathbf{Z}} \mathbf{Q}. \tag{2.5.5.2}$$

Knowledgeable readers will recognize in the L.H.S. of (2.5.5.2) the quaternion algebra

$$B = \left(\frac{-1, -p}{\mathbf{Q}}\right)_2 = \mathbf{Q} \cdot 1 + \mathbf{Q} \cdot I + \mathbf{Q} \cdot J + \mathbf{Q} \cdot IJ, \qquad I^2 = -1,\ J^2 = -p,\ IJ = -JI,$$

which is a central simple algebra over $\mathbf{Q}$ (i.e. B has no non-trivial bilateral ideals and its centre is equal to $\mathbf{Q}$). This implies that the homomorphism (2.5.5.2), being non-zero, must be injective. In fact, it is an *isomorphism*, but we are not going to prove this.

(2.5.6) In general, elliptic curves with non-commutative endomorphism rings are quite rare; they occur only over fields of characteristic $p > 0$, and for each p there are only finitely many of them (up to isomorphism over some extension of the base field). For such curves, $\mathrm{End}_K(-) \otimes \mathbf{Q}$ is isomorphic to the unique quaternion algebra over $\mathbf{Q}$ ramified exactly at p and ∞ (see [Hu], Ch. 13.6; [Si 1], V.3).

2.6 Complex Multiplication by $\mathbf{Z}[\rho]$

(2.6.1) Let $\rho = e^{2\pi i/3}$; then $\rho^2 + \rho + 1 = 0,\ \rho - \rho^2 = i\sqrt{3}$.

(2.6.2) Exercise. *Let* K *be a field of characteristic* $char(K) \neq 3$ *and* $D \in K^*$.
(i) *Show that* $E : X^3 + Y^3 = DZ^3$ *is an elliptic curve over* K *(with origin* $O = (1 : -1 : 0)$*).*
(ii) *Find a change of variables transforming* (E, O) *into a curve in a generalized Weierstrass form.*
(iii) *If* $char(K) \neq 2$, *show that, for suitable* $A \in K^*$, E *is isomorphic over* K *to the elliptic curve*

$$E_A : y^2 = x^3 + A.$$

(iv) *Assume that* $\zeta \in \overline{K}$ *is a primitive cubic root of unity, i.e.* $\zeta^3 = 1 \neq \zeta$. *Define* $[\rho] : E_{K(\zeta)} \longrightarrow E_{K(\zeta)}$ *by* $[\rho](X : Y : Z) \mapsto (X : Y : \zeta Z)$ *and show that the map* $m + n\rho \mapsto [m] + ([n] \circ [\rho])$ *defines an injective ring homomorphism*

$$\mathbf{Z}[\rho] \longrightarrow \mathrm{End}_{K(\zeta)}(E).$$

(v) *Compute explicitly the action of* $[-1]$ *and* $[\rho - \rho^2]$ *on* E *and find all points* $P \in E(\overline{K})$ *satisfying* $[\rho - \rho^2]P = O$ *(resp.* $[3]P = O$*).*

(vi) *If $char(K) \neq 2$, show that the isomorphism from (iii) transforms $[\rho - \rho^2] \in \mathrm{End}_{K(\zeta)}(E)$ into an isogeny $\lambda : E_A \longrightarrow E_{-27A}$ of degree 3 defined over K. Determine* $\mathrm{Ker}(\lambda)(\overline{K})$.

(2.6.3) Exercise. *Consider the elliptic curve $E : X^3 + Y^3 = Z^3$ (with $O = (1 : -1 : 0)$) over a field K of characteristic $char(K) = 2$.*
(i) *Show that* $\phi_2^2 = \phi_4 = [-2] \in \mathrm{End}_K(E)$.
(ii) *If $K \supset \mathbf{F}_4$, show that there is an injective homomorphism*

$$R := \mathbf{Z}[\rho][\phi]/ < \phi^2 = -2,\ \phi\rho = \rho^{-1}\phi > \longrightarrow \mathrm{End}_K(E).$$

(iii) *Show that the map*

$$\rho \mapsto \frac{-1 + i + j + k}{2}, \qquad \phi \mapsto i - j$$

induces an injective homomorphism $R \hookrightarrow \mathbf{H}$ into the algebra of Hamilton quaternions; determine its image.
(iv) *Determine* $\mathrm{Aut}_K(E)$ *(for $K \supset \mathbf{F}_4$).*

3. Isogenies (main properties)

3.1 The dual isogeny

(3.1.1) Example: Let $L \subset L' \subset \mathbf{C}$ be lattices satisfying $L'/L \xrightarrow{\sim} \mathbf{Z}/2\mathbf{Z}$ and let

$$\lambda : \mathbf{C}/L \longrightarrow \mathbf{C}/L', \qquad z \ (\mathrm{mod}\, L) \mapsto z \ (\mathrm{mod}\, L')$$

be the (analytic) isogeny of degree 2 studied in 2.4. According to the general recipe from I.7.6.5, the formula

$$\widehat{\lambda} : \mathbf{C}/L' \longrightarrow \mathbf{C}/L, \qquad z \ (\mathrm{mod}\, L') \mapsto 2z \ (\mathrm{mod}\, L)$$

defines an (analytic) isogeny of degree 2 satisfying

$$\widehat{\lambda} \circ \lambda = [2], \qquad \lambda \circ \widehat{\lambda} = [2].$$

Choosing a basis $\omega_1, \omega_2 \in L$ such that $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$, $L' = \mathbf{Z}\frac{\omega_1}{2} + \mathbf{Z}\omega_2$, we have

$$\lambda^{-1}\,(z \ (\mathrm{mod}\, L')) = \{z \ (\mathrm{mod}\, L),\ (z + \omega_1/2) \ (\mathrm{mod}\, L)\},$$
$$2z \ (\mathrm{mod}\, L) = z + (z + \omega_1/2) \ (\mathrm{mod}\, L) - \omega_1/2 \ (\mathrm{mod}\, L).$$

The latter formula can be rewritten as

$$\widehat{\lambda}(Q) = \boxplus_{P \in \lambda^{-1}(Q)} P \boxminus \boxplus_{P \in \lambda^{-1}(O)} P; \tag{3.1.1.1}$$

in other words, $\widehat{\lambda}(Q)$ corresponds to the class of the divisor $\lambda^*((Q) - (O))$ under the isomorphism $\boxplus : Cl^0(\mathbf{C}/L) \xrightarrow{\sim} \mathbf{C}/L$ from I.5.3.6.

(3.1.2) Proposition. *Let $\lambda : E' \longrightarrow E$ be an isogeny between elliptic curves over K of degree* $\deg(\lambda) = n$. *Then there is a unique isogeny $\widehat{\lambda} : E \longrightarrow E'$ (the* **dual isogeny** *to λ) satisfying $\lambda \circ \widehat{\lambda} = [n]_E$.*

Proof. Uniqueness: If $\mu, \nu : E \longrightarrow E'$ are isogenies satisfying $\lambda \circ \mu = \lambda \circ \nu$, then $\lambda \circ (\mu \boxminus \nu) = 0$, hence $\mu \boxminus \nu = 0$ (by 2.1.6), i.e. $\mu = \nu$.
Existence: We shall try to construct $\widehat{\lambda}$ by generalizing the formula (3.1.1.1). It is natural to expect that, for each field $L \supset K$, $\widehat{\lambda}$ should act on the L-rational points by the following composite map:

$$E(L) \xrightarrow{\sim} Cl^0(E_L) \xrightarrow{\lambda_L^*} Cl^0(E'_L) \xleftarrow{\sim} E'(L), \tag{3.1.2.1}$$

where the isomorphisms are those from 1.2.1; we apply this observation to the field $L = R(E)$ and the "general point" $Q \in E(L)$ defined in 1.2.6. Denote by $Q'(\lambda) \in E'(L)$ the image of Q under the map (3.1.2.1); then $Q'(\lambda)$ defines a rational map $E - - \succ E'$, which extends to a (unique) morphism $\widetilde{\lambda} : E \longrightarrow E'$.

In the scheme theoretical language, the points Q and $Q'(\lambda)$ correspond to morphisms

$$Q : \mathrm{Spec}(L) \longrightarrow E, \qquad Q'(\lambda) = \widetilde{\lambda} \circ Q : \mathrm{Spec}(L) \xrightarrow{Q} E \xrightarrow{\widetilde{\lambda}} E'.$$

As the composite map

$$(\lambda_L)_* \circ (\lambda_L)^* : \mathrm{Div}(E_L) \longrightarrow \mathrm{Div}(E'_L) \longrightarrow \mathrm{Div}(E_L)$$

is given by multiplication by n, it follows that $\lambda_L(Q'(\lambda)) = [n]_E(Q)$, hence

$$\lambda \circ Q'(\lambda) : \mathrm{Spec}(L) \xrightarrow{Q} E \xrightarrow{\widetilde{\lambda}} E' \xrightarrow{\lambda} E$$

is equal to

$$[n]_E \circ Q : \mathrm{Spec}(L) \xrightarrow{Q} E \xrightarrow{[n]_E} E.$$

In other words, the morphisms $\lambda \circ \widetilde{\lambda}, [n]_E : E \longrightarrow E$ define the same rational map $E - - \succ E$, which implies that they are equal:

$$\lambda \circ \widetilde{\lambda} = [n]_E.$$

In particular, $\widetilde{\lambda} : E \longrightarrow E'$ is a non-constant morphism. Instead of proving directly that $\widetilde{\lambda}(O) = O'$ (i.e. that $\widetilde{\lambda}$ is an isogeny), we use the following trick: the point $P := \widetilde{\lambda}(O) \in E'(K)$ satisfies $\lambda(P) = [n](O) = O$; putting

$$\widehat{\lambda} = \tau_{-P} \circ \widetilde{\lambda} : E \xrightarrow{\widetilde{\lambda}} E' \xrightarrow{\tau_{-P}} E'$$

(where τ_{-P} denotes the translation map by $-P = \boxminus P$), then $\widehat{\lambda} : E \longrightarrow E'$ will be an isogeny (as $\widehat{\lambda}(O) = O'$) satisfying

$$\lambda \circ \widehat{\lambda} = \lambda \circ \tau_{-P} \circ \widetilde{\lambda} = \lambda \circ \widetilde{\lambda} = [n]_E$$

(as $\lambda(P) = 0$), as required.

(3.1.3) (i) It is convenient to define $\widehat{0} = 0$ and $\deg(0) = 0$; then $\widehat{\lambda}$ makes sense for all elements of $\mathrm{Hom}_L(E', E)$.

(ii) If $L \supset K$ is any field, then $\widehat{\lambda_L} = (\widehat{\lambda})_L$ (as $([n]_E)_L = [n]_{E_L}$).

(iii) In the situation of 2.5.2, $\widehat{[\alpha]}_X = [\overline{\alpha}]_X$ $(X = V, E)$, thanks to 2.5.4.

(iv) In the situation of 2.5.5, $\widehat{\phi}_p = -\phi_p$; combined with (iii), this implies that the map $\lambda \mapsto \widehat{\lambda}$ on $\mathrm{End}_K(E)$ induces the standard involution $I \mapsto -I$, $J \mapsto -J$, $IJ \mapsto -IJ$ on the quaternion algebra B.

(3.1.4) Theorem. *Let $\lambda : E' \longrightarrow E$ be an isogeny of degree $\deg(\lambda) = n$. Then*

(i) $\widehat{\lambda} \circ \lambda = [n]_{E'}, \quad \lambda \circ \widehat{\lambda} = [n]_E$.

(ii) *If $\mu : E'' \longrightarrow E'$ is an isogeny, then* $\widehat{\lambda \circ \mu} = \widehat{\mu} \circ \widehat{\lambda}$.

(iii) *If $\mu : E' \longrightarrow E$ is an isogeny, then* $\widehat{\lambda \boxplus \mu} = \widehat{\lambda} \boxplus \widehat{\mu}$.

(iv) *For all $m \in \mathbf{Z}$,* $\widehat{[m]} = [m], \quad \deg[m] = m^2$.

(v) $\deg(\widehat{\lambda}) = \deg(\lambda)$.

(vi) $\widehat{\widehat{\lambda}} = \lambda$.

Proof. (cf. [Si 1], III.6.2). (i) We know that $\lambda \circ \widehat{\lambda} = [n]_E$, hence

$$(\widehat{\lambda} \circ \lambda) \circ \widehat{\lambda} = \widehat{\lambda} \circ (\lambda \circ \widehat{\lambda}) = \widehat{\lambda} \circ [n]_E = [n]_{E'} \circ \widehat{\lambda} \implies \widehat{\lambda} \circ \lambda = [n]_{E'}.$$

(using 2.1.3 and 2.1.6).
(ii) If $r = \deg(\mu)$, then

$$\lambda \circ \mu \circ \widehat{\mu} \circ \widehat{\lambda} = \lambda \circ [r]_{E'} \circ \widehat{\lambda} = [r]_E \circ \lambda \circ \widehat{\lambda} = [r]_E \circ [n]_E = [rn]_E = [\deg(\lambda \circ \mu)] = \lambda \circ \mu \circ \widehat{\lambda \circ \mu},$$

which implies the result (again using 2.1.3 and 2.1.6).
(iii) This is a non-trivial statement, which will be proved in 3.1.6-9 below.
(iv) The equality $\widehat{[m]} = [m]$ follows from (iii) (and the case $m = -1$) by induction on $|m|$. It implies that

$$[\deg([m])] = [m] \circ \widehat{[m]} = [m^2] \implies \deg([m]) = m^2$$

(using 2.3.2).
(v) This follows from the fact that

$$\deg(\lambda)\deg(\widehat{\lambda}) = \deg(\lambda \circ \widehat{\lambda}) = \deg([n]) = n^2 = \deg(\lambda)^2.$$

(vi) Combining (i) and (v), we obtain

$$[n]_E \circ \widehat{\widehat{\lambda}} = \lambda \circ \widehat{\lambda} \circ \widehat{\widehat{\lambda}} = \lambda \circ [n]_{E'} = \lambda \circ \widehat{\lambda} \circ \lambda = [n]_E \circ \lambda \implies \widehat{\widehat{\lambda}} = \lambda.$$

(3.1.5) Corollary. *The function*

$$\deg : \mathrm{Hom}_L(E', E) \longrightarrow \mathbf{Z}$$

is quadratic, i.e. the function

$$(\lambda, \mu) \mapsto \deg(\lambda \boxplus \mu) - \deg(\lambda) - \deg(\mu)$$

is a bilinear form on $\mathrm{Hom}_L(E', E)$.

(3.1.6) Proof of 3.1.4(iii) (beginning). A truly "functorial" proof would deduce the statement from the "Theorem of the square". Instead, we shall try to explain the "usual" proof (cf. [Si 1], III.6.2; [Ca 3], App. C; note that, if $char(K) > 0$, then the proof involves elliptic curves over non-perfect fields; this fact was glossed over in [Si 1]).

The idea of the proof is to consider the graphs Γ_ν of the isogenies $\nu = \lambda, \mu, \lambda \boxplus \mu$ as divisors on the surface $E' \times_K E$, and to study their restrictions to the elliptic curves $L' \times_K E = E_{L'}$ and $E' \times_K L = E'_L$ over the fields $L = R(E)$ and $L' = R(E')$, respectively. More precisely, consider the divisor

$$D = (\Gamma_{\lambda \boxplus \mu}) - (\Gamma_\lambda) - (\Gamma_\mu) + (\Gamma_0) \in \mathrm{Div}(E' \times_K E). \tag{3.1.6.1}$$

Restricting D to $E_{L'}$, i.e. viewing the "horizontal" coordinate in the direction of E' as constant, we deduce that D is "almost" principal. Using this information and restricting D to E'_L, i.e. viewing the "vertical" coordinate as constant, we obtain

$$Q'(\lambda \boxplus \mu) = Q'(\lambda) \boxplus Q'(\mu) \boxplus P_1 \tag{3.1.6.2}$$

for some $P_1 \in E'(K)$, which implies that

$$\widetilde{\lambda \boxplus \mu} = \tau_{P_1} \circ (\widetilde{\lambda} \boxplus \widetilde{\mu}) \implies \widehat{\lambda \boxplus \mu} = \widehat{\lambda} \boxplus \widehat{\mu},$$

as required. Let us first explain the terminology in a simplified setting.

(3.1.7) A toy model. Let $C_1 = \mathbf{A}^1_K = \mathrm{Spec}(K[x_1])$ and $C_2 = \mathbf{A}^1_K = \mathrm{Spec}(K[x_2])$ be two affine lines over K; denote by $L_j = R(C_j) = K(x_j)$ $(j = 1, 2)$ their fields of rational functions. The product $X = C_1 \times_K C_2 = \mathbf{A}^2_K = \mathrm{Spec}(K[x_1, x_2])$ is an affine plane; we view x_1 (resp. x_2) as the horizontal (resp. the vertical) coordinate on X.

(3.1.7.1) Divisors on the surface $X = C_1 \times_K C_2$. A **divisor** on X is a formal finite linear combination $\sum_C n_C(C)$ of reduced irreducible curves $C \subset X$, with integral coefficients $n_C \in \mathbf{Z}$; they form an abelian group $\mathrm{Div}(X)$ with respect to addition. Each curve C is given by an equation

$$C : f_C(x_1, x_2) = 0,$$

where $f_C \in K[x_1, x_2]$ is a non-constant irreducible polynomial. This polynomial is unique only up to multiplication by a constant in K^*; however, we fix f_C, for each curve C as above.

If the polynomial $f_C(x_1, x_2)$ depends only on x_1 (resp. only on x_2), then the curve $C : f_C(x_1) = 0$ (resp. $C : f_C(x_2) = 0$) is vertical (resp. horizontal). Such curves generate the groups of vertical (resp. horizontal) divisors on X:

$$\mathrm{Div}(X)_{\mathrm{vert}} = \sum_{\text{vertical } C} n_C(C), \qquad \mathrm{Div}(X)_{\mathrm{hor}} = \sum_{\text{horizontal } C} n_C(C)$$

The (two-dimensional) ring $K[x_1, x_2]$ is factorial, which means that each non-zero rational function $g \in R(X)^* = K(x_1, x_2)^*$ factorizes uniquelly as

$$g = a \prod_C f_C^{\mathrm{ord}_C(g)}, \qquad (a \in K^*,\ \mathrm{ord}_C(g) \in \mathbf{Z}); \tag{3.1.7.1.1}$$

the **divisor of** g is defined as

$$\mathrm{div}(g) = \sum_C \mathrm{ord}_C(g)(C) \in \mathrm{Div}(X).$$

As $\mathrm{div}(f_C) = (C)$, the **divisor class group of** X

$$Cl(X) = \mathrm{Div}(X)/\{\mathrm{div}(g) \,|\, g \in R(X)^*\} \tag{3.1.7.1.2}$$

vanishes: $Cl(X) = 0$.

(3.1.7.2) Variables versus constants. It is often useful to view one of the coordinates, say x_2, as being "constant", and consider only x_1 as a "true" variable. What does this mean?

For example, in the factorization (3.1.7.1.1), we disregard all horizontal curves $C : f_C(x_2) = 0$. Algebraically, this amounts to considering the factorization of g in the localized (one-dimensional) ring

$$(K[x_2] - \{0\})^{-1} K[x_1, x_2] = K(x_2)[x_1] = L_2[x_1],$$

which is the ring of functions on a curve (= the affine line) over the field $L_2 = K(x_2)$. Geometrically, the localization

$$j_1^a : K[x_1, x_2] \hookrightarrow K(x_2)[x_1] = L_2[x_1]$$

defines an injective morphism

$$j_1 : \mathbf{A}^1_{L_2} = (C_1)_{L_2} = C_1 \times_K \mathrm{Spec}(L_2) = \mathrm{Spec}(L_2[x_1]) \longrightarrow \mathrm{Spec}(K[x_1, x_2]) = C_1 \times_K C_2,$$

whose image is obtained from $C_1 \times_K C_2$ by removing all horizontal curves $C : f_C(x_2) = 0$ (and the generic point).

The slogan "view x_2 as a constant" means that one restricts a given geometric object from $C_1 \times_K C_2$ to $(C_1)_{L_2}$, via the morphism j_1. For example, for the divisor group we obtain the map "forget all horizontal curves"

$$\begin{aligned} j_1^* : \mathrm{Div}(C_1 \times_K C_2) &\longrightarrow \mathrm{Div}((C_1)_{L_2}) \\ \sum_C n_C(C) &\mapsto \sum_{C \text{ not horizontal}} n_C(C_{L_2}), \end{aligned}$$

where $C_{L_2} = C \times_K L_2 : (j_1^a(f_C))(x_1, x_2) = 0$ is considered as a closed point on $\mathbf{A}^1_{L_2}$ (of course, $j_1^a(f_C)$ is the same polynomial as f_C, but this time considered as an element of $K(x_2)[x_1] = L_2[x_1]$: x_1 is variable, but x_2 is not). Note that

$$\mathrm{Ker}(j_1^*) = \mathrm{Div}(X)_{\mathrm{hor}}.$$

Similarly, viewing x_1 as being "constant" amounts to localizing

$$j_2^a : K[x_1, x_2] \hookrightarrow K(x_1)[x_2] = L_1[x_2]$$

and restricting via the morphism

$$j_2 : \mathbf{A}^1_{L_1} = (C_2)_{L_1} = \mathrm{Spec}(L_1) \times_K C_2 = \mathrm{Spec}(L_1[x_2]) \longrightarrow \mathrm{Spec}(K[x_1, x_2]) = C_1 \times_K C_2,$$

giving rise to the map "forget all vertical curves"

$$\begin{aligned} j_2^* : \mathrm{Div}(C_1 \times_K C_2) &\longrightarrow \mathrm{Div}((C_2)_{L_1}) \\ \sum_C n_C(C) &\mapsto \sum_{C \text{ not vertical}} n_C(C_{L_1}), \end{aligned}$$

where $C_{L_1} = L_1 \times_K C$, satisfying $\mathrm{Ker}(j_2^*) = \mathrm{Div}(X)_{\mathrm{vert}}$.

It is important to note that

$$\mathrm{div}(j_1^a(g)) = j_1^*(\mathrm{div}(g)), \qquad \mathrm{div}(j_2^a(g)) = j_2^*(\mathrm{div}(g)), \qquad (\forall g \in R(X)^*),$$

where we have also denoted by j_1^a, j_2^a the canonical maps (in fact, the identity maps)

$$\begin{aligned} j_1^a : R(C_1 \times_K C_2) = \mathrm{Frac}(K[x_1, x_2]) &\longrightarrow \mathrm{Frac}(K(x_2)[x_1]) = R((C_1)_{L_2}) \\ j_2^a : R(C_1 \times_K C_2) = \mathrm{Frac}(K[x_1, x_2]) &\longrightarrow \mathrm{Frac}(K(x_1)[x_2]) = R((C_2)_{L_1}). \end{aligned}$$

(3.1.7.3) Example: Let $\Gamma_\alpha \subset C_1 \times_K C_2$ be the graph of the morphism $\alpha : C_1 \longrightarrow C_2$ given by "$\alpha(x_1) = x_1^2$", i.e. corresponding to the morphism of K-algebras

$$\alpha^a : K[x_2] \longrightarrow K[x_1], \qquad \alpha^a(x_2) = x_1^2.$$

In other words, Γ_α is the reduced irreducible curve

$$\Gamma_\alpha : x_1^2 - x_2 = 0$$

on $C_1 \times_K C_2 = \mathbf{A}^2_K$, i.e.

$$(\Gamma_\alpha) = \mathrm{div}(x_1^2 - x_2).$$

If we consider x_1 as being constant, then

$$\begin{aligned} j_2^*((\Gamma_\alpha)) = (\Gamma_\alpha)_{L_1} = (\text{the point with the coordinate } x_2 \text{ equal to } x_1^2 \text{ on } (C_2)_{L_1} = \mathbf{A}^1_{L_1}) = \\ = (\alpha_{L_1})_*(\text{the tautological point with the coordinate } x_1 \text{ equal to } x_1 \text{ on } (C_1)_{L_1} = \mathbf{A}^1_{L_1}) \end{aligned}$$

(in the last line, x_1 appears twice: first as a variable, then as a constant).
If we consider x_2 as being constant, then

$$\begin{aligned} j_1^*((\Gamma_\alpha)) = (\Gamma_\alpha)_{L_2} = (\text{the prime ideal } (x_1^2 - x_2) \text{ in } L_2[x_1]) = \\ = \text{"(the point with the coordinate } x_1 \text{ equal to } \sqrt{x_2})+ \\ +(\text{the point with the coordinate } x_1 \text{ equal to } -\sqrt{x_2}) \text{ on } (C_1)_{L_2} = \mathbf{A}^1_{L_2}\text{"} = \\ = (\alpha_{L_2})^*(\text{the tautological point with the coordinate } x_2 \text{ equal to } x_2 \text{ on } (C_2)_{L_2} = \mathbf{A}^1_{L_2}) \end{aligned}$$

(again, in the last line, x_2 appears first as a variable, then as a constant).

(3.1.8) Divisors. Intuitively, one would like to define a divisor on an arbitrary variety (or a scheme) as a linear combination of "subvarieties" of codimension one. There are two versions of this notion: "Weil divisors" and "Cartier divisors"; however, the two coincide on "nice" varieties, such as the surface $E' \times_K E$.

More precisely, let X be a (separated, noetherian, irreducible) regular scheme (X is regular, for example, if it is smooth over a field). If $X = \mathrm{Spec}(A)$ is affine, then a divisor on X is a finite linear combination

$$\sum_{\mathfrak{p}} n_{\mathfrak{p}}(\mathfrak{p}) \qquad\qquad (n_{\mathfrak{p}} \in \mathbf{Z}),$$

where each $\mathfrak{p} \subset A$ is a prime ideal of codimension one (i.e. such that $\dim(A_{\mathfrak{p}}) = 1$); in the example 3.1.7, $A = K[x_1, x_2]$ and $\mathfrak{p} = (f_C)$. In general, a divisor is a finite sum

$$\sum_{x} n_x(x) \qquad\qquad (n_x \in \mathbf{Z}),$$

where each $x \in X$ is a point of codimension one (i.e. such that $\dim(\mathcal{O}_{X,x}) = 1$). The closure of $\{x\}$ in X is a reduced and irreducible subscheme of X of codimension one.

As X is assumed to be regular, each local ring $\dim(A_{\mathfrak{p}})$ (resp. $\mathcal{O}_{X,x}$) in codimension one is a discrete valuation ring, defining a discrete valuation $\mathrm{ord}_{\mathfrak{p}}$ (resp. ord_x) on the field $R(X)$. The divisor of a rational function $g \in R(X)^*$ is then defined as

$$\mathrm{div}(g) = \sum_{\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(g)(\mathfrak{p}), \qquad \text{resp.} \quad \sum_{x} \mathrm{ord}_x(g)(x).$$

(3.1.9) Proof of 3.1.4(iii) (end). We can play the same game as in 3.1.7 with the surface $X = E' \times_K E$; the divisors on X are linear combinations of reduced irreducible curves on X. Let

$$Q : \mathrm{Spec}(L) = \mathrm{Spec}(R(E)) \longrightarrow E, \qquad Q' : \mathrm{Spec}(L') = \mathrm{Spec}(R(E')) \longrightarrow E'$$

be the tautological points of the two elliptic curves and

$$j = Q' \times \mathrm{id} : L' \times_K E = E_{L'} \longrightarrow E' \times_K E, \qquad j' = \mathrm{id} \times Q : E' \times_K L = E'_L \longrightarrow E' \times_K E$$

the corresponding inclusions. For any element $\lambda \in \mathrm{Hom}_K(E', E)$ and any field $F \supset K$, let $\lambda_F \in \mathrm{Hom}_F(E', E)$ be the same morphism, but considered as being defined over F. The graph of λ, defined as the fibre product

$$\begin{array}{ccc} \Gamma_\lambda & \longrightarrow & E' \times_K E \\ \downarrow & & \downarrow{\scriptstyle \lambda \times \mathrm{id}} \\ E & \xrightarrow{\Delta} & E \times_K E, \end{array}$$

is a reduced irreducible curve on $E' \times_K E$. As in 3.1.7.3, the restrictions of the divisor (Γ_λ) via the maps

$$j^* : \mathrm{Div}(E' \times_K E) \longrightarrow \mathrm{Div}(E_{L'}), \qquad j'^* : \mathrm{Div}(E' \times_K E) \longrightarrow \mathrm{Div}(E'_L)$$

are equal to

$$j^*\left((\Gamma_\lambda)\right) = (\lambda_{L'}(Q')) \tag{3.1.9.1}$$

$$j'^*\left((\Gamma_\lambda)\right) = \lambda_L^*\left((Q)\right). \tag{3.1.9.2}$$

For $\lambda = 0$, the curve $\Gamma_0 = E' \times \{O\}$ is horizontal, thus

$$j^*\left((\Gamma_0)\right) = (O)_{L'}, \qquad j'^*\left((\Gamma_0)\right) = 0. \tag{3.1.9.3}$$

Considering the horizontal coordinate in the direction of E' as constant, i.e. applying (3.1.9.1) to the divisor (3.1.6.1), we see that

$$j^*(D) = ((\lambda \boxplus \mu)_{L'}(Q')) - (\lambda_{L'}(Q')) - (\mu_{L'}(Q')) + (O)_{L'} \in \mathrm{Div}(E_{L'})$$

is a principal divisor on the elliptic curve $E_{L'}$, thanks to 1.2.1. This implies that D itself differs from a principal divisor by a vertical divisor, i.e.

$$D = \mathrm{div}(f) + d \times E \in \mathrm{Div}(E' \times_K E), \tag{3.1.9.4}$$

for some rational function $f \in R(E' \times_K E)^*$ and a divisor $d \in \mathrm{Div}(E')$. Considering now the vertical coordinate in the direction of E as constant, i.e. applying (3.1.9.2), we obtain the equality

$$(\lambda \boxplus \mu)_L^* ((Q)) - \lambda_L^* ((Q)) - \mu_L^* ((Q)) = \mathrm{div}(j'^a f) + d_L \in \mathrm{Div}(E'_L),$$

where $j'^a f = f$, but considered as an element of $R(E'_L) = R(E' \times_K E)$. It follows that the class of the divisor

$$(\lambda \boxplus \mu)_L^* ((Q) - (O)_L) - \lambda_L^* ((Q) - (O)_L) - \mu_L^* ((Q) - (O)_L)$$

in $Cl^0(E'_L)$ is equal to the class of d'_L, where

$$d' = d - (\lambda \boxplus \mu)^* ((O)) + \lambda^* ((O)) + \mu^* ((O)) \in \mathrm{Div}^0(E').$$

The last statement is nothing but the equality (3.1.6.2), with the point $P_1 \in E'(K)$ corresponding to the class of d' under the isomorphism 1.2.1. As observed in 3.1.6, this concludes the proof of 3.1.4(iii).

3.2 The Frobenius morphism

Let K be a field of characteristic $char(K) = p > 0$; the map $\sigma(a) = a^p$ is then a field homomorphism $\sigma : K \longrightarrow K$. Fix a power $q = p^r$ $(r \geq 1)$ of p; then $\sigma^r(a) = a^q$.

(3.2.1) For a polynomial $f(x) = \sum_\alpha c_\alpha x^\alpha \in K[x]$, put $f^{(q)}(x) = \sum_\alpha c_\alpha^q x^\alpha \in K[x]$. As $f(x)^q = f^{(q)}(x^q)$, it follows that

$$\text{if } a \in \overline{K} \text{ is a root of } f(x) \Longrightarrow a^q \text{ is a root of } f^{(q)}(x). \tag{3.2.1.1}$$

Similar properties hold for polynomials in several variables.

(3.2.2) A naive "definition". If X is an affine "variety" (more precisely, an affine scheme of finite type) over K given by the polynomial equations

$$f_1(x) = \cdots = f_N(x) = 0 \qquad\qquad (f_j \in K[x] = K[x_1, \ldots, x_M]),$$

we denote by $X^{(q)}$ the affine "variety" over K given by the equations

$$f_1^{(q)}(x) = \cdots = f_N^{(q)}(x) = 0.$$

In other words, if the ring of regular functions on X is equal to

$$A = K[x_1, \ldots, x_M]/(f_1, \ldots, f_N), \tag{3.2.2.1}$$

the corresponding ring of functions on $X^{(q)}$ will be given by

$$A^{(q)} = K[x_1, \ldots, x_M]/(f_1^{(q)}, \ldots, f_N^{(q)}). \tag{3.2.2.2}$$

In the scheme theoretical language, $X = \mathrm{Spec}(A), X^{(q)} = \mathrm{Spec}(A^{(q)})$. The morphism of K-algebras

$$\psi_q : A^{(q)} \longrightarrow A, \qquad \sum_\alpha c_\alpha x^\alpha \mapsto \sum_\alpha c_\alpha x^{q\alpha} \tag{3.2.2.3}$$

then defines a morphism $\phi_q : X \longrightarrow X^{(q)}$ (over K). On coordinates, if $a = (a_1, \ldots, a_m) \in X(\overline{K})$, then $\phi_q(a) = (a_1^q, \ldots, a_m^q) \in X^{(q)}(\overline{K})$, as in (3.2.1.1).

By working with homogeneous polynomials one can use the same formulas to define $X^{(q)}$ and ϕ_q for projective "varieties" over K.

(3.2.3) An invariant definition. Unfortunately, it is not immediately clear that the K-algebra (3.2.2.2) and the morphism (3.2.2.3) depend only on A, not on its particular presentation (3.2.2.1).

(3.2.3.1) Definition. *For any K-algebra A (commutative), put $A^{(q)} = A \otimes_{K,\sigma^r} K$. This is a K-algebra via the map $c \mapsto 1 \otimes c$ ($c \in K$).*

(3.2.3.2) This means that each element of $A^{(q)}$ is a finite sum of expressions $a \otimes c$ ($a \in A$, $c \in K$) satisfying $ac \otimes c' = a \otimes c^q c'$ ($a \in A$, $c, c' \in K$).

(3.2.3.3) Exercise. *Let A be as in (3.2.2.1). The formula*

$$\sum_\alpha c_\alpha x^\alpha \otimes c \mapsto \sum_\alpha c_\alpha^q c\, x^\alpha \qquad\qquad (f(x) \otimes c \mapsto c f^{(q)}(x))$$

defines an isomorphism of K-algebras

$$K[x_1, \ldots, x_M] \otimes_{K,\sigma^r} K \xrightarrow{\sim} K[x_1, \ldots, x_M],$$

which induces an isomorphism of K-algebras

$$A \otimes_{K,\sigma^r} K \xrightarrow{\sim} K[x_1, \ldots, x_M]/(f_1^{(q)}, \ldots, f_N^{(q)}).$$

Under this isomorphism, the map (3.2.2.3) corresponds to

$$\psi_q : \sum_\alpha c_\alpha x^\alpha \otimes c \mapsto \sum_\alpha c_\alpha^q c\, x^{q\alpha}.$$

(3.2.3.4) In other words, 3.2.3.1 is the correct functorial definition of $A^{(q)}$. In the scheme-theoretical language, this means that $X^{(q)}$ can be defined for an *arbitrary* K-scheme X as the fibre product

$$\begin{array}{ccc} X^{(q)} & \longrightarrow & X \\ \downarrow & & \downarrow \\ \mathrm{Spec}(K) & \xrightarrow{(\sigma^r)^*} & \mathrm{Spec}(K) \end{array}$$

(3.2.3.5) Example. If $A = K[x]$ (i.e. X is the affine line over K), then $A^{(q)} = K[x]$ and the morphism of K-algebras $\psi_q : A^{(q)} = K[x] \longrightarrow A = K[x]$ corresponding to ϕ_q is given by $\psi_q(x) = x^q$ (and $\psi_q(c) = c$).

In this example, the corresponding extension of the fields of rational functions $K(x) = \mathrm{Frac}(A) \supset \psi_q(\mathrm{Frac}(A^{(q)})) = K(x^q)$ is purely inseparable, of degree q.

If the field K is perfect, then $K(x^q) = K^q(x^q) = K(x)^q$. Moreover, if $\mathfrak{p} = (f(x)) \subset A = K[x]$ is a maximal ideal (where $f \in K[x]$ is a non-constant irreducible polynomial), then $f(x) = g^{(q)}(x)$ for some irreducible polynomial $g \in K[x]$, and the maximal ideal $\mathfrak{q} = (g) \subset A^{(q)} = K[x]$ satisfies $\psi_q(\mathfrak{q})A = (g^{(q)}(x^q)) = (f(x))^q = \mathfrak{p}^q$; in other words, the morphism ϕ_q is totally ramified at the point $\mathfrak{p}$.

(3.2.3.6) ϕ_q is usually called the *relative Frobenius morphism*, where "relative" refers to the fact that ψ_q is the identity on constants $c \in K$, but raises each variable x_j to its q-th power.

(3.2.3.7) If $K \subseteq \mathbf{F}_q$, then $\sigma^r = \mathrm{id}$ on K, hence $X^{(q)} = X$ for every K-scheme X.

(3.2.4) Proposition. *Let K be a perfect field of characteristic $p > 0$, $q = p^r$ $(r \geq 1)$ and X a smooth projective curve over K (ireducible over $\overline{K}$). Then:*
(i) *$X^{(q)}$ is also a smooth projective curve over K (ireducible over $\overline{K}$).*
(ii) *The extension of the fields of rational functions $R(X)/\phi_q^* R(X^{(q)})$ corresponding to the morphism $\phi_q : X \longrightarrow X^{(q)}$ is purely inseparable, of degree q (thus $\deg(\phi_q) = q$).*
(iii) *$\phi_q^* R(X^{(q)}) = R(X)^q$.*
(iv) *The morphism of curves $\phi_q : X \longrightarrow X^{(q)}$ is totally ramified at each (closed) point.*

Proof. (cf. [Si 1], II.2.11). The statement (i) follows from the fact that the horizontal arrows in the diagram 3.2.3.4 are isomorphisms, since the field K is perfect. For the affine line over K, we have verified the statements (ii)-(iv) by hand in 3.2.3.5. The general case easily follows, but we include the details for the reader's convenience.
(ii), (iii) As $\pi : X \longrightarrow \mathrm{Spec}(K)$ is smooth of relative dimension one, there exists an open affine subset $\mathrm{Spec}(A) \subset X$ which is étale (i.e. smooth of relative dimension zero) over the affine line $\mathbf{A}^1_K = \mathrm{Spec}(K[t])$. This implies that the corresponding extension of the fields of rational functions $R(X)/K(t) = \mathrm{Frac}(A)/K(t)$ is separable (and finite). In the diagram of fields

$$\begin{array}{ccc} K(t) & \subset & R(X) \\ | & & | \\ K(t)^q = K(t^q) & \subset & R(X)^q \end{array}$$

the horizontal extensions are separable, while the vertical extensions are purely inseparable; thus

$$[R(X) : R(X)^q] = [K(t) : K(t^q)] = q.$$

For each open affine subset $\mathrm{Spec}(A) \subset X$, where $A = K[x_1, \ldots, x_m]/I = K[x_1, \ldots, x_m]/(f_1, \ldots, f_n)$, the image of the map $\psi_q : A^{(q)} \longrightarrow A$ is equal to

$$K[x_1^q, \ldots, x_m^q]/(f_1^{(q)}(x^q), \ldots, f_n^{(q)}(x^q)) = K[x_1^q, \ldots, x_m^q]/(f_1(x)^q, \ldots, f_n(x)^q) = A^q$$

(using the fact that $K = K^q$, as K is perfect by assumption). This implies that $\phi_q^* R(X^{(q)}) = R(X)^q$.
(iv) For each A as in the proof of (iii), A is a Dedekind ring; let $\mathfrak{p} = (g_1 + I, \ldots, g_r + I) \in \mathrm{Max}(A)$ $(g_j \in K[x_1, \ldots, x_m])$ be any maximal ideal of A. Then $\mathfrak{p}^{(q)} = (g_1^{(q)} + I^{(q)}, \ldots, g_r^{(q)} + I^{(q)})$ is an ideal of $A^{(q)}$, satisfying

$$A^{(q)}/\mathfrak{p}^{(q)} = (A/\mathfrak{p}) \otimes_{K,\sigma} K \xrightarrow{\sim} A/\mathfrak{p} = k(\mathfrak{p})$$

(as $\sigma : K \longrightarrow K$ is an isomorphism, the field K being perfect). It follows that $\mathfrak{p}^{(q)}$ is a maximal ideal of $A^{(q)}$ and

$$\psi_q(\mathfrak{p}^{(q)}) = (g_1^{(q)}(x^q) + I^{(q)}, \ldots, g_r^{(q)}(x^q) + I^{(q)}) = \mathfrak{p}^q,$$

which means that $\mathfrak{p}^{(q)} = \psi_q^{-1}(\mathfrak{p})$ is totally ramified in $\psi_q(A^{(q)}) \subset A$, with ramification index equal to q.

(3.2.5) Corollary. *If K is as in 3.2.4 and E is an elliptic curve over K, then, for each $r \geq 1$, $E^{(q)}$ is an elliptic curve over K and $\phi_q : E \longrightarrow E^{(q)}$ is an isogeny (where we take $\phi_q(O)$ to be the distinguished K-rational point of $E^{(q)}$).*

(3.2.6) Proposition. *Let K be a perfect field of characteristic $p > 0$, $\lambda : E \longrightarrow E'$ an isogeny of elliptic curves over K. Then λ factors uniquelly as*

$$E \xrightarrow{\phi_q} E^{(q)} \xrightarrow{\mu} E',$$

where $q = p^r$ for some $r \geq 0$, μ is an isogeny and the extension $R(E^{(q)})/\mu^* R(E')$ is separable.

Proof. (cf. [Si 1], II.2.12). Let $F/\lambda^*(R(E'))$ be the maximal separable subextension of $R(E)/\lambda^*(R(E'))$. Then $R(E)/F$ is a purely inseparable extension of degree $q = p^r$ $(r \geq 0)$, hence $R(E)^q \subset F$. As

$$[R(E):F] = q = [R(E):\phi_q^* R(E^{(q)})] = [R(E):R(E)^q]$$

by 3.2.4(ii)-(iii), we have $F = R(E)^q = \phi_q^* R(E^{(q)})$. The tower of fields

$$R(E) \supset \phi_q^* R(E^{(q)}) \supset \lambda^*(R(E'))$$

then corresponds to a tower of (non-constant) morphisms

$$E \xrightarrow{\phi_q} E^{(q)} \xrightarrow{\mu} E'.$$

Define $O_{E^{(q)}} = \phi_q(O_E)$; then ϕ_q, μ are isogenies and the extension $R(E^{(q)})/\mu^*(R(E'))$ is separable, being isomorphic to $F/\lambda^*(R(E'))$.

(3.2.7) Corollary (of the proof). *If, in the situation of 3.2.6, the extension of fields $R(E)/\lambda^*(R(E'))$ is purely inseparable, then the isogeny $\lambda : E \longrightarrow E'$ is isomorphic to the isogeny $\phi_q : E \longrightarrow E^{(q)}$.*

3.3 The invariant differential

We refer to ([Al-Kl]; [Ei], Ch. 16; [Mat], Ch. 9) for basic properties of Kähler differentials.

(3.3.1) If E is an elliptic curve over K, then the space of regular differentials $\Gamma(E, \Omega_{E/K})$ on E is one-dimensional (as E has genus $g(E) = 1$).

(3.3.2) Proposition. (i) *If $\omega \in \Gamma(E, \Omega_{E/K}) - \{0\}$ is a non-zero regular differential, then* $\mathrm{div}(\omega) = 0$, *i.e. ω has no zeros (nor poles).*
(ii) *If E is given by a generalized Weierstrass equation*

$$E - \{O\} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_i \in K),$$

then

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y} \tag{3.3.2.1}$$

is a regular differential on E, hence $\Gamma(E, \Omega_{E/K}) = K \cdot \omega$ and ω has no zeros (nor poles).

Proof. (i) $D = \mathrm{div}(\omega) \geq 0$ is an effective divisor of degree $\deg_K(D) = 2g - 2 = 0$, hence $D = 0$.
(ii) (cf. [Si 1], III.1.5). We know that

$$\Gamma(E_{\overline{K}}, \Omega_{E_{\overline{K}}/\overline{K}}) = \Gamma(E, \Omega_{E/K}) \otimes_K \overline{K}.$$

Consequently, to show that ω is regular (i.e. $\omega \in \Gamma(E, \Omega_{E/K})$), we can replace E by $E_{\overline{K}}$ and ω by $\overline{\omega} = \omega \otimes 1 \in \Omega_{R(E)/K} \otimes_K \overline{K} \subset \Omega_{R(E_{\overline{K}})/\overline{K}}$. The same calculation as in the proof of I.4.2.2 then shows that $\mathrm{ord}_P(\overline{\omega}) = 0$ for all $P \in (E - \{O\})(\overline{K})$. As $\deg(\mathrm{div}(\overline{\omega})) = 2g - 2 = 0$, it follows that $\mathrm{ord}_O(\overline{\omega}) = 0$; thus $\mathrm{div}(\overline{\omega}) = 0$. In particular, $\overline{\omega}$ is regular, hence so is ω.

(3.3.3) Exercise. *How does the direct calculation of* $\mathrm{ord}_O(\overline{\omega})$ *from I.4.2.2 have to be modified in the algebraic context? [Hint: what is the analogue of I.3.3.8?]*

(3.3.4) The existence of a regular differential without zeros on E should come as a no surprise. E is an algebraic group, which implies that its cotangent bundle is trivial: choose a basis of the cotangent space at the origin and use translation maps to transport this basis all over E. For a fixed trivialization of the cotangent bundle, a constant section of the trivial bundle then corresponds to a regular differential ω without zeros.

As E is a curve, its cotangent bundle has rank one (it is a line bundle). Moreover, the only global sections of the trivial line bundle are the constants, since E is projective; thus ω is unique up to a constant multiple.

Last but not least, the construction of the trivialization of the cotangent bundle using the (commutative) group law implies that the differential ω is invariant in the following sense.

(3.3.5) Invariant differentials. We are going to show that ω from (3.3.2.1) is an *invariant differential*, i.e. that

$$\omega(Q_1 \boxplus Q_2) = \omega(Q_1) + \omega(Q_2), \tag{3.3.5.1}$$

if we consider the coordinates of $Q_j = (x_j, y_j)$ $(j = 1, 2)$ as variables. This property makes ω into an important tool for "linearizing" the group law on E (replacing the analytic uniformization $\mathbf{C}/L \xrightarrow{\sim} E(\mathbf{C})$ available in the complex case).

What are the basic examples of invariant differentials?

$$\text{The additive group : } \ dz \ \text{ satisfies } \ d(z_1 + z_2) = dz_1 + dz_2.$$
$$\text{The multiplicative group : } \ dz/z \ \text{ satisfies } \ d(z_1 z_2)/z_1 z_2 = dz_1/z_1 + dz_2/z_2.$$

In general, if $G \longrightarrow S$ is a "commutative group scheme" over a base scheme S (such as E over K), then a regular differential $\omega \in \Gamma(G, \Omega_{G/S})$ is *(translation) invariant* if

$$m^*(\omega) = p_1^*(\omega) + p_2^*(\omega), \tag{3.3.5.2}$$

where the morphisms

$$m : G \times_S G \longrightarrow G, \qquad p_1 : G \times_S G \longrightarrow G, \qquad p_2 : G \times_S G \longrightarrow G \tag{3.3.5.3}$$

denote the group law on G and the projections on the first (resp. the second) factor, respectively. Note that (3.3.5.2) is merely a fancy reformulation of (3.3.5.1).

(3.3.6) Proposition. *If E is an elliptic curve over K, then every regular differential $\omega \in \Gamma(E, \Omega_{E/K})$ on E is translation invariant, i.e. satisfies*

$$m^*(\omega) = p_1^*(\omega) + p_2^*(\omega)$$

in the notation of 3.3.5.3.

Proof. See ([Si 1], p. 82), for an 'elementary' proof. The following argument formalizes the last remark made in 3.3.4.

We can assume that $\omega \neq 0$. By 3.3.2(i), ω has no zeros on E, which means that multiplication by ω induces an isomorphism of invertible sheaves on E

$$\mathcal{O}_E \xrightarrow{\sim} \Omega_{E/K}$$

(i.e. a trivialization of the cotangent bundle of E). For the same reason, the map

$$\mathcal{O}_{E \times_K E}^{\oplus 2} \xrightarrow{\sim} \Omega_{E \times_K E/K}, \qquad (f_1, f_2) \mapsto f_1 \cdot (p_1^*\omega) + f_2 \cdot (p_2^*\omega)$$

is an isomorphism of sheaves on $E \times_K E$. Explicitly, if (Q_1, Q_2) is a variable point in some open subset U of $E \times_K E$, then the above map is given by

$$(f_1(Q_1, Q_2), f_2(Q_1, Q_2)) \mapsto f_1(Q_1, Q_2) \cdot \omega(Q_1) + f_2(Q_1, Q_2) \cdot \omega(Q_2),$$

where f_1, f_2 are regular functions on U. Taking global sections, we obtain an isomorphism of K-vector spaces

$$K^{\oplus 2} \xrightarrow{\sim} \Gamma(E \times_K E, \Omega_{E \times_K E/K}), \qquad (c_1, c_2) \mapsto c_1 \cdot (p_1^*\omega) + c_2 \cdot (p_2^*\omega).$$

As $m^*(\omega) \in \Gamma(E \times_K E, \Omega_{E \times_K E/K})$, it is of the form

$$m^*(\omega) = c_1 \cdot (p_1^*\omega) + c_2 \cdot (p_2^*\omega)$$

for some constants $c_1, c_2 \in K$. These constants can be determined by restricting to the curves $E \times_K \{O\} = \mathrm{Im}(i_1)$ and $\{O\} \times_K E = \mathrm{Im}(i_2)$, where $i_j : E \longrightarrow E \times_K E$ $(j = 1, 2)$ are the morphisms

$$i_1(P) = (P, O), \qquad i_2(P) = (O, P).$$

Then

$$m \circ i_j = p_j \circ i_j = \mathrm{id}, \quad p_j \circ i_k = 0 \quad (j \neq k) \quad \Longrightarrow \quad \omega = i_j^* m^*(\omega) = c_j \cdot \omega \quad \Longrightarrow \quad c_1 = c_2 = 1.$$

(3.3.7) Corollary. *If $\lambda, \mu : E' \longrightarrow E$ are two isogenies between elliptic curves over K, then*

$$(\lambda \boxplus \mu)^*(\omega) = \lambda^*(\omega) + \mu^*(\omega)$$

holds for every regular differential $\omega \in \Gamma(E, \Omega_{E/K})$.

Proof. By definition,

$$\lambda \boxplus \mu = m \circ g, \qquad \lambda = p_1 \circ g, \qquad \mu = p_2 \circ g,$$

where

$$g : E' \xrightarrow{\Delta} E' \times_K E' \xrightarrow{\lambda \times \mu} E \times_K E$$

(and $\Delta(P) = (P, P)$). Applying g^* to 3.3.6 yields the result:

$$(\lambda \boxplus \mu)^*(\omega) = g^* m^*(\omega) = g^* p_1^*(\omega) + g^* p_2^*(\omega) = \lambda^*(\omega) + \mu^*(\omega).$$

(3.3.8) Corollary. *If E is an elliptic curve over K and $\omega \in \Gamma(E, \Omega_{E/K})$ a regular differential on E, then*

$$[n]^*(\omega) = n\omega \qquad\qquad (n \in \mathbf{Z}).$$

Proof. Induction on $|n|$.

3.4 Separable (= unramified = étale) isogenies

(3.4.1) Let $\lambda : E' \longrightarrow E$ be an isogeny between elliptic curves over K. Choose non-zero regular differentials ω_E (resp. $\omega_{E'}$) on E (resp. E'). The exact sequence of Kähler differentials associated to the triple

$$K \hookrightarrow R(E) \xrightarrow{\lambda^*} R(E')$$

reads as follows (note that $\Omega_{R(E)/K}$ is denoted by Ω_E in [Si 1]):

$$\begin{array}{ccccccc} \Omega_{R(E)/K} \otimes_{R(E),\lambda^*} R(E') & \xrightarrow{\lambda^*} & \Omega_{R(E')/K} & \longrightarrow & \Omega_{R(E')/\lambda^* R(E)} & \longrightarrow & 0 \\ \| & & \| & & \| & & \\ R(E') \cdot \omega_E & \xrightarrow{\lambda^*} & R(E') \cdot \omega_{E'} & \longrightarrow & \Omega_{R(E')/\lambda^* R(E)} & \longrightarrow & 0 \end{array} \tag{3.4.1.1}$$

(3.4.2) Definition. *An isogeny $\lambda : E' \longrightarrow E$ is* **separable** *if the extension $R(E')/\lambda^* R(E)$ of the fields of rational functions is separable.*

(3.4.3) Lemma. *An isogeny $\lambda : E' \longrightarrow E$ is separable $\iff$ $\lambda^*(\omega_E) \neq 0$ (where ω_E is any non-zero regular differential on E).*

Proof. This follows from the exactness of the bottom row of (3.4.1.1) and the fact that a finite field extension L'/L is separable if and only if $\Omega_{L'/L} = 0$.

(3.4.4) Example: If $char(K) = p > 0$ and $\phi_q : E \longrightarrow E^{(q)}$ $(q = p^r,\ r \geq 1)$ is the relative Frobenius morphism, then $\phi_q^*(\omega_{E^{(q)}}) = 0$, as $d(x^q) = q x^{q-1}\, dx = 0$.

(3.4.5) Proposition. *Let $\lambda : E' \longrightarrow E$ be a separable isogeny.*
(i) *For each field $L \supset K$, the isogeny $\lambda_L : E'_L \longrightarrow E_L$ is also separable.*
(ii) *λ is unramified at each (closed) point $x' \in E'$ ($\Longleftrightarrow$ the extension of the residue fields $k(x')/k(x)$, where $x = \lambda(x')$, is separable).*
(iii) *For each $P \in E(\overline{K})$, the set*

$$\lambda^{-1}(P)(\overline{K}) := \{Q \in E'(\overline{K}) \,|\, \lambda(Q) = P\}$$

has $\deg(\lambda)$ elements.
(iv) *If P is defined over a separable extension of K, so are all elements of $\lambda^{-1}(P)(\overline{K})$.*
(v) *$\mathrm{Ker}(\lambda)(\overline{K}) = \lambda^{-1}(O)(\overline{K})$ is a finite subgroup of $E'(K^{sep})$ of order $\deg(\lambda)$, stable by the action of the Galois group $G_K = \mathrm{Gal}(K^{sep}/K)$ (where K^{sep} denotes the maximal separable extension of K contained in $\overline{K}$).*

Proof. (cf. [Si 1], III.4.10(c), if K is perfect). (i) For any non-zero regular differential ω_E on E, we have $\lambda_L^*(\omega_E \otimes 1) = \lambda^*(\omega_E) \otimes 1 \neq 0$.
(ii) This is a local question, so we can consider λ over a (non-empty) open subset $\mathrm{Spec}(A) = U \subset E$, where A is a Dedekind ring, of finite type as a K-algebra, with fraction field $\mathrm{Frac}(A) = R(E)$. Then $\lambda^{-1}(U) = U' = \mathrm{Spec}(A')$, where A' is the integral closure of A in $\mathrm{Frac}(R(E'))$ (with respect to the embedding of fields $\lambda^* : R(E) \longrightarrow R(E')$); the point x' corresponds to a maximal ideal $\mathfrak{p}' \subset A'$ and $x = \lambda(x')$ to the maximal ideal $\mathfrak{p} = (\lambda^*)^{-1}(\mathfrak{p}') \subset A$. The corresponding residue fields (= the fields of definitions of the points x, x') are equal to $k(x) = k(\mathfrak{p}) = A/\mathfrak{p}$, $k(x') = k(\mathfrak{p}') = A'/\mathfrak{p}'$.

Recall that λ is *unramified* at x' if the extension of the discrete valuation rings $A_{\mathfrak{p}} \subset A'_{\mathfrak{p}'}$ is unramified, i.e. if $k(\mathfrak{p}')/k(\mathfrak{p})$ is a separable extension and the ramification index $e(\mathfrak{p}'|\mathfrak{p}) = 1$ is trivial. This is, in turn, equivalent to the vanishing of the module of differentials

$$\Omega_{A'_{\mathfrak{p}'}/A_{\mathfrak{p}}} = \big(\Omega_{A'/A}\big)_{\mathfrak{p}'} = 0. \tag{3.4.5.1}$$

The A'-module $M = \Omega_{A'/A}$ is finitely generated and torsion, since

$$M \otimes_A \mathrm{Frac}(A) = \Omega_{\mathrm{Frac}(A')/\mathrm{Frac}(A)} = 0$$

vanishes (as the field extension $\mathrm{Frac}(A')/\mathrm{Frac}(A)$ is separable, by assumption). This implies that (3.4.5.1) holds for all $\mathfrak{p}' \notin \Sigma$, for some *finite* bad set Σ of maximal ideals of A'.

In the special case when the field $K = \overline{K}$ is algebraically closed, maximal ideals of A (resp. A') correspond to points in U (resp. U') with coordinates in $\overline{K}$. If $P' \in \Sigma \subset U'(\overline{K})$ is a bad point at which λ is not unramified, then there is another point $Q' \in U'(\overline{K})$ such that $P' \boxplus Q' \in U'(\overline{K}) - \Sigma$. Applying the traslation by Q', we see that the morphism

$$\lambda \circ \tau_{Q'} = \tau_Q \circ \lambda$$

(where $Q = \lambda(Q')$) is unramified at P', hence so must be λ (as τ_Q is an isomorphism). It follows that $\Sigma = \emptyset$, hence λ is unramified everywhere.

If the field K is arbitrary, the previous argument applies, thanks to (i), to the isogeny $\lambda_{\overline{K}} : E'_{\overline{K}} \longrightarrow E_{\overline{K}}$; thus $\lambda_{\overline{K}}$ is unramified everywhere, hence

$$\Omega_{A'/A} \otimes_K \overline{K} = \Omega_{A' \otimes_K \overline{K}/A \otimes_K \overline{K}} = 0,$$

which proves that $\Omega_{A'/A} = 0$, i.e. λ is unramified everywhere.
(iii) We can replace λ by $\lambda_{\overline{K}} : E'_{\overline{K}} \longrightarrow E_{\overline{K}}$ and assume that $K = \overline{K}$. In the notation of the proof of (ii), P becomes a maximal ideal of A and the set $S := \lambda^{-1}(P)(\overline{K})$ is the set of maximal ideals $Q \subset A'$ above P, i.e. such that $Q \cap A = P$. An algebraic version of I.3.2.3.5 states that

$$\sum_{Q \in S} e(Q|P) \cdot [k(Q) : k(P)] = [\mathrm{Frac}(A') : \mathrm{Frac}(A)] = \deg(\lambda).$$

However, the residue fields are equal to $k(Q) = A'/Q = \overline{K} = A/P = k(P)$ and each ramification index is equal to one, thanks to (ii); the formula then simply states that the number of elements of the set S is equal to $\deg(\lambda)$.
The statement (iv) and much of (v) follow from (ii) and (iii). It remains to be proved that, if $Q \in E'(K^{sep})$ satisfies $\lambda(Q) = O$, then $\lambda(\sigma(Q)) = O$ for all $\sigma \in G_K$. This follows from the fact that

$$O = \sigma(O) = \sigma(\lambda(Q)) = \lambda(\sigma(Q)),$$

as λ is defined over K.

(3.4.6) A toy model: Let $\mathbf{G}_m = \mathbf{A}^1_K - \{0\} = \mathrm{Spec}(K[x, 1/x])$ be the multiplicative group over a field K. This is an commutative algebraic group (or a group scheme, if you wish) over K, with the group law given by multiplication, i.e. by the morphism

$$\mathbf{G}_m \times_K \mathbf{G}_m = \mathrm{Spec}(K[x, 1/x] \otimes_K K[y, 1/y]) \xrightarrow{\sim} \mathrm{Spec}(K[x, 1/x, y, 1/y]) \xrightarrow{m} \mathrm{Spec}(K[t, 1/t])$$

corresponding to the K-algebra map

$$K[t, 1/t] \longrightarrow K[x, 1/x, y, 1/y], \qquad t \mapsto xy.$$

For each integer $n \geq 1$, the morphism $[n] : \mathbf{G}_m \longrightarrow \mathbf{G}_m$ corresponds to the map $x \mapsto x^n$. The invariant differential

$$\omega = \frac{dx}{x} \in \Gamma(\mathbf{G}_m, \Omega_{\mathbf{G}_m/K})$$

then satisfies

$$[n]^*(\omega) = \frac{d(x^n)}{x^n} = n\,\frac{dx}{x} = n\omega;$$

thus

$$[n]^*(\omega) \neq 0 \iff char(K) \nmid n, \tag{3.4.6.1}$$

which is equivalent to the separability of the extension of the fields of rational functions

$$R(\mathbf{G}_m)/[n]^*R(\mathbf{G}_m) = K(x)/K(x^n).$$

If (3.4.6.1) holds, then, for each point $P \in \mathbf{G}_m(\overline{K}) = \overline{K}^*$, the set of the n-th roots of P

$$[n]^{-1}(P)(\overline{K}) = \{Q \in \mathbf{G}_m(\overline{K}) = \overline{K}^* \mid Q^n = [n](Q) = P\}$$

consists of n elements, each of them generating a separable extension of K. In particular, if $P = 1$ is the neutral element of $\mathbf{G}_m$, then $[n]^{-1}(P)(\overline{K}) = \mu_n(\overline{K})$ is the set of the n-th roots of unity in $\overline{K}$.

3.5 Points of finite order

Points of finite order on a given elliptic curve are analogues of the roots of unity in the elementary context. Their coordinates are interesting numbers in their own right (as we have seen in I.8.5); here we simply count the number of points of a given order.

(3.5.1) Throughout Sect. 3.5, E will denote an elliptic curve over a field K and ω a non-zero regular differential on E.

(3.5.2) Proposition. *If $n \geq 1$ and $(char(K), n) = 1$, then $[n] : E \longrightarrow E$ is a separable isogeny,*

$$\#E(\overline{K})_n = \deg[n] = n^2$$

and the group of n-torsion points on E is isomorphic to

$$E(\overline{K})_n \xrightarrow{\sim} (\mathbf{Z}/n\mathbf{Z})^2.$$

Proof. According to 3.3.8, $[n]^*(\omega) = n\omega$, which is non-zero, as $(char(K), n) = 1$; thus $[n]$ is a separable isogeny, by 3.4.3. Applying 3.4.5(iii) and 3.1.4(iv), we deduce that $\#E(\overline{K})_n = n^2$. In order to show that $E(\overline{K})_n \xrightarrow{\sim} (\mathbf{Z}/n\mathbf{Z})^2$, it is sufficient to consider the case $n = p^r$, where p is a prime number, $p \neq char(K)$. For $r = 1$, $E(\overline{K})_p$ is killed by p and has order $\deg[p] = p^2$, hence $E(\overline{K})_p \xrightarrow{\sim} (\mathbf{Z}/p\mathbf{Z})^2$. For $r > 1$ one proceeds by induction, using the result for $r - 1$ and the structure theory of finite abelian groups.

(3.5.3) Corollary. *If $char(K) = p > 0$, then there is an integer $a = a(E) \in \{0, 1\}$ (depending only on $E_{\overline{K}}$) such that*

$$(\forall r \geq 1) \quad E(\overline{K})_{p^r} \xrightarrow{\sim} (\mathbf{Z}/p^r\mathbf{Z})^a.$$

Proof. As $[p]^*\omega = p\omega = 0$, 3.4.3 together with 3.2.6 imply that $[p]$ factors as

$$[p] : E \xrightarrow{\phi_q} E^{(q)} \xrightarrow{\mu} E,$$

where $q = p^b$ $(b \geq 1)$ and μ is a separable isogeny. As $\deg[p] = p^2$ and $\deg \phi_q = q$, it follows that $b \in \{1, 2\}$ and $\deg(\mu) = p^{2-b}$. Applying 3.4.5 to μ gives $E(\overline{K})_p \xrightarrow{\sim} (\mathbf{Z}/p\mathbf{Z})^a$ with $a = 2 - b$. For $r > 1$ use the same inductive argument as in the proof of 3.5.2.

(3.5.4) (1) If $a(E) = 1$ (resp. $a(E) = 0$), we say that E is **ordinary** (resp. **supersingular**). The proof of 3.5.3 shows that

$$E \text{ is ordinary} \iff [p]_E \text{ is not purely inseparable} \iff \widehat{\phi}_p \text{ is a separable isogeny.}$$

(2) Assume that $K = \overline{K}$ is an algebraically closed field of characteristic $char(K) = p > 2$ and $X = V$ or $X = E$ one of the two elliptic curves with complex multiplication by $\mathbf{Z}[i]$ (as in 2.5.2, we fix a square root I of -1 contained in K).

(2a) If $p \equiv 3 \pmod 4$, then $\widehat{\phi}_p = -\phi_p$ is not separable, hence the elliptic curve X is supersingular.

(2b) If $p \equiv 1 \pmod 4$, then p factors in $\mathbf{Z}[i]$ as $p = \alpha\overline{\alpha}$, where $\alpha = u + iv \equiv 1 \pmod{(2 + 2i)}$, $u^2 + v^2 = p$ $(u, v \in \mathbf{Z})$. We identify $\mathbf{Z}[i]/\alpha\mathbf{Z}[i]$ with the prime subfield $\mathbf{F}_p \subset K$ via the map $i \mapsto I$. The corresponding factorization $[p]_X = [\alpha]_X \circ [\overline{\alpha}]_X$ in $\mathrm{End}_K(X)$ then shows that

$$[\alpha]_X^*(\omega_X) = (u + vI)\omega_X = 0, \qquad [\overline{\alpha}]_X^*(\omega_X) = (u - vI)\omega_X = 2u\omega_X \neq 0.$$

It follows that the isogeny $[p]_X$ is not purely inseparable, hence the elliptic curve X is ordinary. Incidentally, this argument also shows that $\phi_p = u \circ [\alpha]_X$, for some automorphism $u \in \mathrm{Aut}_K(X)$, which proves Eisenstein's congruence I.9.4.6 for α up to the unknown factor u.

(3) It is true in general that supersingular elliptic curves in characteristic $p > 0$ are precisely those for which $\mathrm{End}_{\overline{K}}(E) \otimes \mathbf{Q}$ is a quaternion algebra (cf. the references in 2.5.6).

(3.5.5) Proposition. *If E is an elliptic curve over a field $K \subseteq \mathbf{F}_q$ $(q = p^r)$, then*

$$1 - \phi_q = [1] \boxminus \phi_q : E \longrightarrow E$$

is a separable isogeny.

Proof. We know from 3.2.4(ii) that the isogeny $\phi_q : E \longrightarrow E$ is not separable; thus $\phi_q^*(\omega) = 0$ (cf. 3.4.4). Applying 3.3.7, we obtain

$$(1 - \phi_q)^*(\omega) = [1]^*(\omega) - \phi_q^*(\omega) = \omega \neq 0,$$

which proves the result.

(3.5.6) Exercise. *Let E be an elliptic curve over K, $L \supset K$ any field and $A \subset E(L)$ a finite subgroup. Then A is isomorphic to the direct sum of at most two (finite) cyclic groups.*

III. Arithmetic of Elliptic Curves

In this chapter we shall study elliptic curves over fields K that are of interest to number theorists: finite fields, p-adic fields and number fields. In each case, the main question is to describe the set of K-rational points on a given elliptic curve. Our treatment will be rather minimalistic; the reader should consult [Hu], [Si 1] or [Ca 1] for more details.

1. Elliptic curves over finite fields

1.1 Elementary remarks

(1.1.1) Let p be a prime, $q = p^r$ and E an elliptic curve over $\mathbf{F}_q$. We are interested in counting the number of points $\#E(\mathbf{F}_{q^n})$ on E that are rational over the various finite extensions of $\mathbf{F}_q$.

In the special case when $q = p$ and E is given by the generalized Weierstrass equation (II.1.2.4.1), then $\#E(\mathbf{F}_p) - 1$ is equal to the number of solutions $(x, y) \in \mathbf{F}_p \times \mathbf{F}_p$ of the congruence

$$y^2 + a_1xy + a_3y \equiv x^3 + a_2x^2 + a_4x + a_6 \pmod{p}. \tag{1.1.1.1}$$

(1.1.2) Exercise. *For fixed $a, b, c \in \mathbf{Z}$, denote by $N_p(D)$ the number of solutions $(x, y) \in \mathbf{F}_p \times \mathbf{F}_p$ of the congruence*

$$Dy^2 \equiv x^3 + ax^2 + bx + c \pmod{p},$$

where p is a prime and $D \in \mathbf{Z}$. Show that, if $p \nmid 2DD'$,

$$N_p(D') = \begin{cases} N_p(D), & \text{if } \left(\frac{D}{p}\right) = \left(\frac{D'}{p}\right) \\ 2p - N_p(D), & \text{if } \left(\frac{D}{p}\right) = -\left(\frac{D'}{p}\right) \end{cases}$$

[Hint: Fix x.]

(1.1.3) If E has complex multiplication by $\mathbf{Z}[i]$ or $\mathbf{Z}[\rho]$, then (1.1.1.1) can be transformed into a diagonal congruence

$$Y^m \equiv aX^n + b \pmod{p} \tag{1.1.3.1}$$

with $(m, n) = (2, 4), (2, 3)$. In general, the number of solutions of (1.1.3.1) can be expressed in terms of Jacobi sums, or is given by an elementary expression (see [Ir-Ro] for more details).

(1.1.4) Exercise. *Reprove 0.5.3(iv), using the method from 1.1.2 (with a quadratic polynomial on the R.H.S.).*

1.2 Examples

(1.2.1) Let E an elliptic curve over $\mathbf{F}_q$. Denote by $\phi_q : E \longrightarrow E^{(q)} = E$ the corresponding Frobenius morphism. If E is in the generalized Weierstrass form, then $\phi_q(x, y) = (x^q, y^q)$. We shall identify $\mathbf{Z}$ with its image in $\mathrm{End}_K(E)$ (for any field $K \supset \mathbf{F}_q$); this means that we shall write n instead of $[n]$ (for $n \in \mathbf{Z}$). We denote by $\mathbf{Z}[\phi_q]$ (resp. $\mathbf{Q}[\phi_q]$) the subring (resp. the $\mathbf{Q}$-subalgebra) of $\mathrm{End}_{\mathbf{F}_q}(E)$ (resp. of $\mathrm{End}_{\mathbf{F}_q}(E) \otimes \mathbf{Q}$) generated by ϕ_q.

(1.2.2) Lemma. (i) $(\forall n \geq 1) \quad \#E(\mathbf{F}_{q^n}) = \deg(1 - \phi_q^n)$.
(ii) *If $\lambda : E' \longrightarrow E$ is an isogeny (over $\mathbf{F}_q$), then* $(\forall n \geq 1) \quad \#E'(\mathbf{F}_{q^n}) = \#E(\mathbf{F}_{q^n})$.

Proof. (i) By II.3.5.5, $1 - \phi_q^n = 1 - \phi_{q^n} : E \longrightarrow E$ is a separable isogeny, hence it follows from II.3.4.5(iii) that

$$\deg(1 - \phi_q^n) = \#\mathrm{Ker}(1 - \phi_q^n)(\overline{\mathbf{F}}_q) = \#\{P \in E(\overline{\mathbf{F}}_q) \mid \phi_q^n(P) = P\} = \#E(\mathbf{F}_{q^n}).$$

As regards (ii), the Snake Lemma applied to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E'(\overline{\mathbf{F}}_q) & \stackrel{\lambda}{\longrightarrow} & E(\overline{\mathbf{F}}_q) & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow 1-\phi_q^n & & \downarrow 1-\phi_q^n & & \\ 0 & \longrightarrow & A & \longrightarrow & E'(\overline{\mathbf{F}}_q) & \stackrel{\lambda}{\longrightarrow} & E(\overline{\mathbf{F}}_q) & \longrightarrow & 0 \\ & & & & \downarrow & & \downarrow & & \\ & & & & 0 & & 0 & & \end{array}$$

(where $A = \mathrm{Ker}(\lambda)(\overline{\mathbf{F}}_q)$ and f is induced by $1-\phi_q^n$) yields an exact sequence

$$0 \longrightarrow \mathrm{Ker}(f) \longrightarrow E'(\mathbf{F}_{q^n}) \stackrel{\lambda}{\longrightarrow} E(\mathbf{F}_{q^n}) \longrightarrow \mathrm{Coker}(f) \longrightarrow 0,$$

which implies the statement of (ii), as $\#\mathrm{Ker}(f) = \#\mathrm{Coker}(f)$ by the finiteness of A.

(1.2.3) Examples: (0) The discussion in 0.5.0-3 can be regarded as an elementary variant of 1.2.2, with 0.5.1 saying that $\phi_p = [p^*]$ on C.

(1) Consider the curves V, E from II.2.5 over $\mathbf{F}_p$, where $p \neq 2$ is a prime. By 1.2.2(ii), $\#V(\mathbf{F}_{p^n}) = \#E(\mathbf{F}_{p^n})$ $(n \geq 1)$. Note that the affine curve V_{aff} is of the diagonal form 1.1.3.

(1a) If $p \equiv 3 \pmod 4$, denote by $C : y^2 = 1 - x^2$ the affine circle and by $\widetilde{C} \subset \mathbf{P}^2$ its projectivization. Then

$$V(\mathbf{F}_p) = V_{\mathrm{aff}}(\mathbf{F}_p) = C(\mathbf{F}_p) = \widetilde{C}(\mathbf{F}_p) \stackrel{\sim}{\longrightarrow} \mathbf{P}^1(\mathbf{F}_p).$$

Indeed, the second (resp. the first and the third) equality follow from the fact that $\mathbf{F}_p^{*4} = \mathbf{F}_p^{*2}$ (resp. $-1 \notin \mathbf{F}_p^{*2}$), and the last one is the isomorphism "circle = line" from 0.3.1.1. As a result,

$$\#V(\mathbf{F}_p) = \#E(\mathbf{F}_p) = \#\mathbf{P}^1(\mathbf{F}_p) = p + 1.$$

This elementary method breaks down over $\mathbf{F}_{p^2}$. However, the congruence I.8.4.9 for $\alpha = -p$ yields the equality $\phi_{p^2} = [-p] \in \mathrm{End}_{\mathbf{F}_p}(V)$, hence

$$\#V(\mathbf{F}_{p^2}) = \#E(\mathbf{F}_{p^2}) = \deg[p+1] = (p+1)^2.$$

(1b) If $p \equiv 1 \pmod 4$, then $p = \alpha\overline{\alpha}$, where $\alpha = a + ib \in \mathbf{Z}[i]$, $\alpha \equiv 1 \pmod{(2+2i)}$. Let $I \in \mathbf{F}_p$ be the image of $i \in \mathbf{Z}[i]$ under the projection $\mathbf{Z}[i] \longrightarrow \mathbf{Z}[i]/\alpha\mathbf{Z}[i] = \mathbf{F}_p$. The congruence I.8.4.9 for α then yields $\phi_p = [\alpha] \in \mathrm{End}_{\mathbf{F}_p}(V)$, hence

$$\#V(\mathbf{F}_p) = \#E(\mathbf{F}_p) = \deg[1-\alpha] = (1-\alpha)(1-\overline{\alpha}) = p + 1 - \alpha - \overline{\alpha} = p + 1 - 2a.$$

This result is usually deduced from a calculation of Jacobi sums ([Ir-Ro], Ch. 8,10,11).

(2) The same method also applies to "biquadratic twists" of the curves V, E (in the sense of II.2.2.8(2)). More precisely, fix an integer $D \in \mathbf{Z} - \{0\}$, a prime number $p \nmid 2D$ and consider the affine curves

$$(V_D)_{\mathrm{aff}} : y_D^2 = 1 - Dx_D^4, \qquad (E_D)_{\mathrm{aff}} : v_D^2 = 4u_D^3 - 4Du_D$$

and the corresponding smooth projective curves V_D, E_D (all defined over $\mathbf{F}_p$). As before, V_D and E_D are elliptic curves over $\mathbf{F}_p$ and the map $f_D(x,y) = (1/x_D^2, -2y_D/x_D^3)$ defines an isogeny $f_D : V_D \longrightarrow E_D$ of degree 2.

Fix a fourth root $D^{1/4} \in \overline{\mathbf{F}}_p$ of D modulo p. Then the formulas

$$x = x_D D^{1/4}, \qquad y = y_D, \qquad u = u_D (D^{1/4})^{-2}, \qquad v = v_D (D^{1/4})^{-3}$$

define isomorphisms $\overline{X} \stackrel{\sim}{\longrightarrow} \overline{X}_D$ (where $X = V, E$ and $\overline{X} = X_{\overline{\mathbf{F}}_p}$ denotes the base change of X to $\overline{\mathbf{F}}_p$) which make the following diagram commutative:

$$\begin{array}{ccc} \overline{V} & \xrightarrow{\sim} & \overline{V}_D \\ \big\downarrow{\scriptstyle f} & & \big\downarrow{\scriptstyle f_D} \\ \overline{E} & \xrightarrow{\sim} & \overline{E}_D \end{array}$$

(2a) If $p \equiv 3 \pmod 4$, then the same argument as in (1a) shows that

$$\#V_D(\mathbf{F}_p) = \#E_D(\mathbf{F}_p) = \#\mathbf{P}^1(\mathbf{F}_p) = p+1.$$

(2b) If $p \equiv 1 \pmod 4$, we again write $p = \alpha\overline{\alpha}$ and $\mathbf{F}_p = \mathbf{Z}[i]/\alpha\mathbf{Z}[i]$, as in (1b).

Let $(x,y) \in V_{\mathrm{aff}}(\overline{\mathbf{F}}_p)$; when is the corresponding point $(x_D, y_D) = (x(D^{1/4})^{-1}, y) \in (V_D)_{\mathrm{aff}}(\overline{\mathbf{F}}_p)$ defined over $\mathbf{F}_p$? We have

$$(x_D, y_D) \in V_D(\mathbf{F}_p) \iff (x_D, y_D) = (x_D^p, y_D^p) \iff (D^{\frac{p-1}{4}}x, y) = (x^p, y^p);$$

recalling that the biquadratic residue symbol

$$\left(\frac{D}{\alpha}\right)_4 \in \{\pm 1, \pm i\}$$

is defined by the generalized Euler's criterion

$$\left(\frac{D}{\alpha}\right)_4 \equiv D^{\frac{p-1}{4}} \pmod \alpha,$$

it follows that

$$(x_D, y_D) \in V_D(\mathbf{F}_p) \iff \left(\phi_p - \left[\left(\frac{D}{\alpha}\right)_4\right]\right)(x,y) = 0$$

(the same argument also applies to the points of $V - V_{\mathrm{aff}}$). The formulas

$$\phi_p = [\alpha], \qquad \left(\frac{D}{\alpha}\right)_4^{-1} = \left(\frac{D}{\overline{\alpha}}\right)_4,$$

together with 1.2.2 then imply

$$\#V_D(\mathbf{F}_p) = \#E_D(\mathbf{F}_p) = \deg\left(\left[\left(\frac{D}{\alpha}\right)_4^{-1}\right]\phi_p - 1\right) = \deg\left(\left[\left(\frac{D}{\overline{\alpha}}\right)_4\right]\alpha - 1\right) = p + 1 - \left(\frac{D}{\overline{\alpha}}\right)_4\alpha - \left(\frac{D}{\alpha}\right)_4\overline{\alpha}.$$

1.3 Theorem of Hasse

(1.3.1) Proposition. *Let E be an elliptic curve over $\mathbf{F}_q$ ($q = p^r$); put $\phi = \phi_q \in \mathrm{End}_{\mathbf{F}_q}(E)$. Then*
(i) *$\phi + \widehat{\phi} = a$, where $a \in \mathbf{Z}$, $|a| \le 2\sqrt{q}$.*
(ii) *$\phi^2 - a\phi + q = \widehat{\phi}^2 - a\widehat{\phi} + q = 0$ holds in $\mathrm{End}_{\mathbf{F}_q}(E)$.*
(iii) *If $|a| = 2\sqrt{q}$, then $r \in 2\mathbf{Z}$, $\phi = \widehat{\phi} = a/2 = \pm p^{r/2} = \pm\sqrt{q}$, $\mathbf{Z}[\phi] = \mathbf{Z}$.*
(iv) *If $|a| < 2\sqrt{q}$, then $\mathbf{Q}[\phi] \xrightarrow{\sim} \mathbf{Q}(\sqrt{a^2 - 4q})$ is an imaginary quadratic field.*
(v) *The two roots $\alpha, \beta \in \mathbf{C}$ of the polynomial $T^2 - aT + q = (T-\alpha)(T-\beta)$ are complex conjugate (i.e. $\beta = \overline{\alpha}$) and satisfy $|\alpha| = |\beta| = \sqrt{q}$.*

Proof. For every pair of integers $u, v \in \mathbf{Z}$, we obtain from II.3.1.4(iii) and II.3.2.4(ii) that

$$\deg(u + v\phi) = (u + v\phi)(u + v\widehat{\phi}) = u^2 + uv(\phi + \widehat{\phi}) + v^2 \deg\phi = u^2 + uv(\phi + \widehat{\phi}) + qv^2 \in \mathrm{End}_{\mathbf{F}_q}(E).$$

As $\deg(u+v\phi)$ is an integer, it follows that $\phi+\widehat{\phi}=a\in\mathbf{Z}$ ($\Longrightarrow \widehat{\phi}=a-\phi\in\mathbf{Z}[\phi]$), proving (i) and (ii), as

$$\phi^2-a\phi+q=\phi^2-(\phi+\widehat{\phi})\phi+\phi\widehat{\phi}=0$$

(and similarly for $\widehat{\phi}$). Moreover, the integer $\deg(u+v\phi)$ is always non-negative, which implies that

$$Q(u,v)=u^2+auv+qv^2=\deg(u+v\phi)\geq 0$$

is a positive semi-definite quadratic form on $\mathbf{Z}\times\mathbf{Z}$. It follows that the discriminant $\mathrm{disc}(Q)=a^2-4q\leq 0$, hence $|a|\leq 2\sqrt{q}$. If $|a|=2\sqrt{q}$, then r is even, $a/2=\pm p^{r/2}=\pm\sqrt{q}\in\mathbf{Z}$ and

$$(a/2-\phi)(a/2-\widehat{\phi})=Q(a/2,-1)=0,$$

proving (iii). If $|a|<2\sqrt{q}$, then the polynomial T^2-aT+q has two complex conjugate (non-real) roots

$$\alpha,\overline{\alpha}=\tfrac{a\pm\sqrt{a^2-4q}}{2}\in\mathbf{C}.$$

This implies that the $\mathbf{Q}$-algebra $R=\mathbf{Q}[T]/(T^2-aT+q)$ is a field, isomorphic to $\mathbf{Q}(\sqrt{a^2-4q})$; the two isomorphisms are given by

$$R\xrightarrow{\sim}\mathbf{Q}(\sqrt{a^2-4q}),\qquad T\mapsto\alpha\quad(\text{resp. }\ T\mapsto\overline{\alpha}).$$

By (ii), $\phi\notin\mathbf{Q}\subset\mathrm{End}_{\mathbf{F}_q}(E)\otimes\mathbf{Q}$, hence the map $T\mapsto\phi$ yields an isomorphism $R\xrightarrow{\sim}\mathbf{Q}[\phi]$. The statement (v) follows from the previous discussion.

(1.3.2) Theorem (Hasse). *In the notation of 1.3.1, let $\alpha,\beta\in\mathbf{C}$ be the roots of $T^2-aT+q=(T-\alpha)(T-\beta)$. Then*

$$\begin{gathered}\beta=\overline{\alpha},\qquad \alpha\overline{\alpha}=q,\qquad \alpha+\overline{\alpha}=a,\qquad |\alpha|=|\overline{\alpha}|=\sqrt{q}\\ (\forall n\geq 1)\qquad \#E(\mathbf{F}_{q^n})=(1-\alpha^n)(1-\overline{\alpha}^n)=q^n+1-\alpha^n-\overline{\alpha}^n\\ |\#E(\mathbf{F}_{q^n})-q^n-1|\leq 2q^{n/2}.\end{gathered}$$

Proof. In the notation of the proof of 1.3.1, in the case $|a|<2\sqrt{q}$ we have the isomorphisms

$$\mathbf{Q}[\phi]\xleftarrow{\sim}\mathbf{Q}[T]/(T^2-aT+q)\xrightarrow{\sim}\mathbf{Q}(\sqrt{a^2-4q}),$$

under which T corresponds to ϕ on the L.H.S. (resp. to α on the R.H.S.). This implies that $\widehat{\phi}=a-\phi$ on the L.H.S. corresponds to $a-\alpha=\overline{\alpha}$ on the R.H.S, hence

$$\#E(\mathbf{F}_{q^n})=\deg(1-\phi^n)=(1-\phi^n)(1-\widehat{\phi}^n)=(1-\alpha^n)(1-\overline{\alpha}^n)\in\mathbf{Z}\subset\mathrm{End}_{\mathbf{F}_q}(E),\tag{1.3.2.1}$$

by 1.2.2 and 3.1.4(iii). If $|a|=2\sqrt{q}$, then $\phi=\widehat{\phi}=\alpha=\overline{\alpha}=a/2=\pm\sqrt{q}\in\mathbf{Z}\subset\mathrm{End}_{\mathbf{F}_q}(E)$, hence (1.3.2.1) holds in this case, too. Everything else follows from 1.3.1.

(1.3.3) Zeta function of E. Let E be an elliptic curve over $\mathbf{F}_q$. Consider the generating function

$$Z(E,t)=\exp\left(\sum_{n=1}^{\infty}\#E(\mathbf{F}_{q^n})\frac{t^n}{n}\right)\in\mathbf{Q}[[t]].\tag{1.3.3.1}$$

The equality of formal power series

$$\sum_{n=1}^{\infty}\frac{c^nt^n}{n}=-\log(1-ct)\qquad\qquad(c\in\mathbf{C})$$

together with Hasse's Theorem 1.3.2 imply that

$$Z(E,t) = \frac{(1-\alpha t)(1-\overline{\alpha}t)}{(1-t)(1-qt)} \tag{1.3.3.2}$$

is a *rational function*. The **zeta function** of E, defined by

$$\zeta(E,s) = Z(E,q^{-s}),$$

is then equal to

$$\zeta(E,s) = \frac{(1-\alpha q^{-s})(1-\overline{\alpha}q^{-s})}{(1-q^{-s})(1-q^{1-s})}, \tag{1.3.3.3}$$

which is a meromorphic function in $\mathbf{C}$ satisfying

$$\zeta(E,s) = \zeta(E,1-s).$$

The fact that

$$|\alpha| = |\overline{\alpha}| = \sqrt{q}$$

is equivalent to the **Riemann hypothesis for** $\zeta(E,s)$:

$$\zeta(E,s) = 0 \Longrightarrow \mathrm{Re}(s) = \frac{1}{2}.$$

(1.3.4) Example: In the situation of 1.2.3(2a), the formula $\#V_D(\mathbf{F}_p) = p+1$ together with 1.3.2 imply that $\widehat{\phi}_p = -\phi_p$, hence $\phi_p^2 = -\widehat{\phi}_p\phi_p = -p$ in $\mathrm{End}_{\mathbf{F}_p}(V_D)$. For $D=1$, we obtain Eisenstein's congruence I.8.4.9 (I.9.4.6) for $\alpha = -p$.

1.4 Vista: Zeta functions in geometry

(1.4.1) The Riemann zeta function can be written either as an infinite series, or as an infinite product:

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p} \left(1-p^{-s}\right)^{-1}, \tag{1.4.1.1}$$

where the product is taken over all prime numbers. Noting that the set of primes corresponds to the set of maximal ideals $\mathrm{Max}(\mathbf{Z}) = \{(p)\}$ of the ring $\mathbf{Z}$, the following generalization of (1.4.1.1) is fairly natural.

(1.4.2) Let

$$A = \mathbf{Z}[T_1,\ldots,T_M]/(f_1,\ldots,f_N) \tag{1.4.2.1}$$

be a finitely generated ring (over $\mathbf{Z}$). By Hilbert's Nullstellensatz, an ideal $I \subset A$ is maximal $\iff$ A/I is a finite field. We denote, for each maximal ideal $\mathfrak{m} \in \mathrm{Max}(A)$, by

$$N(\mathfrak{m}) = \#A/\mathfrak{m} = \#k(\mathfrak{m})$$

the number of elements of the residue field of $\mathfrak{m}$ (roughly speaking, $N(\mathfrak{m})$ measures the "size" of $\mathfrak{m}$). The **zeta function of** A is then defined as

$$\zeta(A,s) = \prod_{\mathfrak{m}\in\mathrm{Max}(A)} \left(1-N(\mathfrak{m})^{-s}\right)^{-1}. \tag{1.4.2.2}$$

One can show that the product (1.4.2.2) is absolutely convergent in the half-plane $\mathrm{Re}(s) > \dim(A)$.

(1.4.3) Examples: (1) $\zeta(\mathbf{Z},s) = \zeta(s)$. More generally, for each integer $N \geq 1$,

$$\zeta(\mathbf{Z}[1/N],s)=\prod_{p\nmid N}\left(1-p^{-s}\right)^{-1}=\sum_{\substack{n=1\\(n,N)=1}}^{\infty}n^{-s}.$$

(2) As $\mathbf{Z}[i]$ is a principal ideal domain, the description of its irreducible elements in 0.4.3.0 implies that

$$\zeta(\mathbf{Z}[i],s)=\left(1-2^{-s}\right)^{-1}\prod_{p\equiv 1(4)}\left(1-p^{-s}\right)^{-2}\prod_{p\equiv 3(4)}\left(1-p^{-2s}\right)^{-1}=\zeta(s)\prod_{p\neq 2}\left(1-(-1)^{\frac{p-1}{2}}p^{-s}\right)^{-1}=$$
$$=\zeta(s)\sum_{\substack{n=1\\2\nmid n}}^{\infty}(-1)^{\frac{n-1}{2}}n^{-s}.$$

(3) More generally, if $\mathcal{O}_K$ is the ring of integers in a number field K, then $\zeta(\mathcal{O}_K,s)$ coincides with the "Dedekind zeta-function of K".

(1.4.4) Putting together all maximal ideals with the same residue characteristic $char(A/\mathfrak{m})=p$, we obtain

$$\zeta(A,s)=\prod_{p}\zeta(A/pA,s),\tag{1.4.4.1}$$

where

$$A/pA=\mathbf{F}_p[T_1,\dots,T_M]/(\overline{f}_1,\dots,\overline{f}_N),\qquad\qquad(\overline{f}_j=f_j\ (\mathrm{mod}\,p)).\tag{1.4.4.2}$$

Let us compute the factor $\zeta(A/pA,s)$ in the simplest non-trivial case $A=\mathbf{Z}[T]$. Maximal ideals of $A/pA=\mathbf{F}_p[T]$ are of the form $\mathfrak{m}=(f)$, where $f\in\mathbf{F}_p[T]$ is a monic irreducible polynomial of degree $d=\deg(f)\geq 1$; then $N(\mathfrak{m})=p^d$. Denote by a_d the number of such polynomials with $\deg(f)=d$ fixed; factorizing the polynomial $T^{p^N}-T$ into irreducible factors yields

$$(\forall N\geq 1)\qquad\sum_{d|N}da_d=p^N.$$

Writing

$$\zeta(\mathbf{F}_p[T],s)=\prod_{d=1}^{\infty}(1-p^{-ds})^{-a_d}=Z(p^{-s}),$$

where

$$Z(t)=Z(\mathbf{F}_p[T],t)=\prod_{d=1}^{\infty}(1-t^d)^{-a_d},$$

we obtain

$$\log Z(t)=\sum_{d=1}^{\infty}a_d\sum_{n=1}^{\infty}\frac{t^{nd}}{n}=\sum_{N=1}^{\infty}\frac{t^N}{N}\sum_{d|N}da_d=\sum_{N=1}^{\infty}\frac{p^Nt^N}{N}=-\log(1-pt),$$

hence

$$Z(\mathbf{F}_p[T],t)=\frac{1}{1-pt},\qquad\zeta(\mathbf{F}_p[T],s)=\frac{1}{1-p^{1-s}}.$$

(1.4.5) This calculation can be generalized to arbitrary A as follows. The ring A from (1.4.2.1) is the ring of functions on the affine "variety over $\mathbf{Z}$"

$$X:f_1=\dots=f_N=0,\qquad X\subset\mathbf{A}_{\mathbf{Z}}^M\tag{1.4.5.1}$$

and A/pA is the ring of functions on the affine "variety" over $\mathbf{F}_p$

$$X_p = X \otimes_{\mathbf{Z}} \mathbf{F}_p : \overline{f}_1 = \cdots = \overline{f}_N = 0, \qquad X_p \subset \mathbf{A}^M_{\mathbf{F}_p}. \tag{1.4.5.2}$$

The points on X_p with coordinates in $\overline{\mathbf{F}}_p$ correspond bijectively to homomorphisms of $\mathbf{F}_p$-algebras $A/pA \longrightarrow \overline{\mathbf{F}}_p$, by the correspondence

$$\mathrm{Hom}_{\mathbf{F}_p - Alg}(A/pA, \overline{\mathbf{F}}_p) \xrightarrow{\sim} X_p(\overline{\mathbf{F}}_p), \qquad \alpha \mapsto a = (a_1, \ldots, a_M) = (\alpha(T_1), \ldots, \alpha(T_M)) \in \overline{\mathbf{F}}_p^M.$$

The kernel of $\alpha : A/pA \longrightarrow \mathbf{F}_p$ is a maximal ideal $\mathfrak{m} \in A/pA$, whose degree $d = \deg(\mathfrak{m})$ (defined by $N(\mathfrak{m}) = p^d$) is equal to the degree of the smallest extension $\mathbf{F}_p(a)/\mathbf{F}_p$ over which the coordinates of a are defined. Two points $a, b \in X_p(\overline{F}_p)$ define the same $\mathfrak{m}$ if and only if they are conjugate by an element of $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$. Conversely, if $\mathfrak{m} \in A/pA$, then there are exactly $d = \deg(\mathfrak{m})$ embeddings $k(\mathfrak{m}) = (A/pA)/\mathfrak{m} \hookrightarrow \overline{\mathbf{F}}_p$; composing them with the canonical projection $(A/pA) \longrightarrow k(\mathfrak{m})$ we obtain d conjugate points in $X_p(\overline{\mathbf{F}}_p)$. It follows that

$$(\forall N \geq 1) \qquad \sum_{d|N} d \sum_{\deg(\mathfrak{m})=d} 1 = \#X_p(\mathbf{F}_{p^N}). \tag{1.4.5.3}$$

In the case $A/pA = \mathbf{F}_p[T]$ this boils down to the correspondence between irreducible monic polynomials of degree d in $\mathbf{F}_p[T]$ and the sets of their roots, which form d-tuples of conjugate points. The identity (1.4.5.3) then becomes (1.4.4.2).

As in 1.4.4, put

$$\zeta(A/pA, s) = Z(A/pA, p^{-s}).$$

The same calculation as in 1.4.4 then yields

$$\log Z(A/pA, t) = \sum_{d=1}^{\infty} \sum_{n=1}^{\infty} \frac{t^{dn}}{n} \sum_{\deg(\mathfrak{m})=d} 1 = \sum_{N=1}^{\infty} \frac{t^N}{N} \sum_{d|N} d \sum_{\deg(\mathfrak{m})=d} 1 = \sum_{N=1}^{\infty} \#X_p(\mathbf{F}_{p^N}) \frac{t^N}{N},$$

hence

$$Z(A/pA, t) = \exp\left(\sum_{N=1}^{\infty} \#X_p(\mathbf{F}_{p^N}) \frac{t^N}{N} \right), \qquad \zeta(A/pA, s) = \exp\left(\sum_{N=1}^{\infty} \#X_p(\mathbf{F}_{p^N}) \frac{p^{-sN}}{N} \right). \tag{1.4.5.4}$$

This explains the origin of the definition (1.3.3.1).

(1.4.6) One can translate the previous definitions into a purely geometric language, which will make sense also for non-affine "varieties", in fact for arbitrary schemes of finite type over $\mathrm{Spec}(\mathbf{Z})$. What does this mean? If X is such a scheme, then it is a finite union of affine "varieties" of the type considered in 1.4.4 (i.e. $X = \mathrm{Spec}(A_1) \cup \cdots \cup \mathrm{Spec}(A_r)$, where each ring A_i is as in (1.4.2.1)). A "closed point" $x \in |X|$ then corresponds to a maximal ideal $\mathfrak{m} \in A_i$ in one of the A_i's; one defines $N(x) = N(\mathfrak{m})$ and

$$\zeta(X, s) = \prod_{x \in |X|} (1 - N(x)^{-s})^{-1}.$$

If $X = \mathrm{Spec}(A)$ is affine, then $\zeta(\mathrm{Spec}(A), s) = \zeta(A, s)$. The discussion from 1.4.4-5 makes sense in this more general context: (1.4.4.1) is replaced by

$$\zeta(X, s) = \prod_p \zeta(X_p, s), \tag{1.4.6.1}$$

where $X_p = X \otimes_{\mathbf{Z}} \mathbf{F}_p$ is the fibre of X over $(p) \in \mathrm{Spec}(\mathbf{Z})$, and (1.4.5.4) reads as

$$\zeta(X_p, s) = \exp\left(\sum_{N=1}^{\infty} \#X_p(\mathbf{F}_{p^N})\frac{p^{-sN}}{N}\right). \tag{1.4.6.2}$$

(1.4.7) Examples: (1) **Affine space**. Let $A = \mathbf{Z}[T_1, \ldots, T_d]$, $X = \mathrm{Spec}(A) = \mathbf{A}^d_{\mathbf{Z}}$. Then $X_p = \mathbf{A}^d_{\mathbf{F}_p}$, hence $\#X_p(\mathbf{F}_{p^N}) = p^{dN}$,

$$Z(\mathbf{A}^d_{\mathbf{F}_p}, t) = \exp\left(\sum_{N=1}^{\infty} p^{dN}\frac{t^N}{N}\right) = \frac{1}{1-p^d t}, \qquad \zeta(\mathbf{A}^d_{\mathbf{F}_p}, s) = \frac{1}{1-p^{d-s}}, \qquad \zeta(\mathbf{A}^d_{\mathbf{Z}}, s) = \zeta(s-d).$$

(2) **Projective space**. Let $X = \mathbf{P}^d_{\mathbf{Z}}$ be the d-dimensional projective space over $\mathbf{Z}$; then $X_p = \mathbf{P}^d_{\mathbf{F}_p}$. For every field F there is a decomposition of $\mathbf{P}^d(F)$ into a disjoint union

$$\mathbf{P}^d(F) = \mathbf{A}^d(F) \cup \mathbf{P}^{d-1}(F) = \mathbf{A}^d(F) \cup \mathbf{A}^{d-1}(F) \cup \cdots \cup \mathbf{A}^0(F). \tag{1.4.7.2.1}$$

Taking $F = \mathbf{F}_{p^N}$, we obtain $\#\mathbf{P}^d_{\mathbf{F}_p}(\mathbf{F}_{p^N}) = p^{dN} + p^{(d-1)N} + \cdots + 1$, hence

$$Z(\mathbf{P}^d_{\mathbf{F}_p}, t) = \frac{1}{(1-p^d t)(1-p^{d-1}t)\cdots(1-t)}, \qquad \zeta(\mathbf{P}^d_{\mathbf{F}_p}, s) = \frac{1}{(1-p^{d-s})(1-p^{d-1-s})\cdots(1-p^{-s})},$$
$$\zeta(\mathbf{P}^d_{\mathbf{Z}}, s) = \zeta(s-d)\zeta(s-d+1)\cdots\zeta(s).$$

(3) **Elliptic curve with CM by $\mathbf{Z}[i]$**. Let $V \subset \mathbf{P}^2_{\mathbf{Z}}$ be the projective curve from II.2.5, considered as a projective scheme over $\mathbf{Z}$. Combining the results of 1.2.3 with (1.3.3.2-3), we obtain

$$\zeta(V \otimes_{\mathbf{Z}} \mathbf{Z}[\tfrac{1}{2}], s) = \zeta(\mathbf{Z}[i][\tfrac{1}{2}], s)\zeta(\mathbf{Z}[i][\tfrac{1}{2}], s-1)L(V, s)^{-1},$$

where

$$L(V, s) = \prod_{\pi}(1 - \pi|\pi|^{-2s})^{-1} = \sum_{\alpha \equiv 1 \pmod{2+2i}} \frac{\alpha}{|\alpha|^{2s}},$$

and the product is taken over all irreducible elements $\pi \in \mathbf{Z}[i]$ satisfying $\pi \equiv 1 \pmod{2+2i}$.

(1.4.8) Remarkable properties of zeta functions. In the examples 1.4.7(2-3), the zeta function of the projective space (resp. of an elliptic curve with complex multiplication) naturally decomposes as a product. Is this a general phenomenon? If yes, does this decomposition have a geometric explanation?

For the projective space, the answer is fairly straightforward: the decomposition (1.4.7.2.1) makes sense for any field, in particular for $F = \mathbf{C}$. In this case the closure of $\mathbf{A}^j(\mathbf{C}) = \mathbf{C}^j$ $(j = 0, \ldots, d)$ in $\mathbf{P}^d(\mathbf{C})$ represents a generator of the homology group $H_{2j}(\mathbf{P}^d(\mathbf{C}), \mathbf{Z}) \xrightarrow{\sim} \mathbf{Z}$, and all other homology groups of $\mathbf{P}^d(\mathbf{C})$ vanish.

One can interpret in the similar vein the decomposition of $\zeta(V, s)$: the factor $\zeta(\mathbf{Z}[i], s)$ (resp. $\zeta(\mathbf{Z}[i], s-1)$) corresponds to the homology group $H_0(V(\mathbf{C}), \mathbf{Z})$ (resp. $H_2(V(\mathbf{C}), \mathbf{Z})$), while the "interesting" factor $L(V, s)$ is related to $H_1(V(\mathbf{C}), \mathbf{Z})$.

What happens in general? Assume that $X \longrightarrow \mathrm{Spec}(\mathbf{Z})$ is projective, flat, $X \otimes_{\mathbf{Z}} \mathbf{Q}$ is smooth over $\mathbf{Q}$, and p is a prime number such that $X_p = X \otimes_{\mathbf{Z}} \mathbf{F}_p$ is smooth over $\mathbf{F}_p$ and irreducible; let $\mathbf{F}_q$ be the algebraic closure of $\mathbf{F}_p$ in the function field of X_p and $d = \dim(X_p)$ the dimension of X_p. Then:

(1) The zeta function $\zeta(X_p, s)$ is a rational function of q^{-s}; more precisely,

$$\zeta(X_p, s) = \frac{P_1(q^{-s})\cdots P_{2d-1}(q^{-s})}{P_0(q^{-s})\cdots P_{2d}(q^{-s})}, \qquad P_i(t) \in \mathbf{Z}[t],\ P_i(0) = 1.$$

(2) There exists a functional equation relating $P_i(q^{-s})$ and $P_{2d-i}(q^{s-d})$.
(3) $\deg(P_i) = \dim_{\mathbf{Q}} H_i(X(\mathbf{C}), \mathbf{Q})$.

(4) For each $i = 0, \dots, 2d$,

$$P_i(t) = \prod_{j=1}^{\deg(P_i)} (1 - \alpha_{i,j} t), \qquad |\alpha_{i,j}| = q^{i/2}.$$

These are the famous "Weil Conjectures" formulated by A. Weil in 1949 (and proved in this generality by: (1) Dwork; (2) and (3) Grothendieck; (4) Deligne).

The most remarkable aspect of this story is the fact that there should be some natural geometric objects $h_i(X)$ ("motives", in Grothendieck's terminology) associated to X, which should be responsible for the topological homology groups $H_i(X(\mathbf{C}), \mathbf{Z})$ (which depend only on the set of complex points of X), and at the same time also for the individual factors $P_i(q^{-s})$ appearing in the decomposition of the zeta function $\zeta(X_p, s)$ (which is defined solely in terms of the geometry of X_p over $\mathbf{F}_p$).

So what is a motive? Well, it is any %&!?*+ which has a zeta function ...

2. Elliptic curves over local fields

Throughout this section, R will denote a discrete valuation ring, $K = \mathrm{Frac}(R)$ is fraction field, $\pi \in R$ a uniformizing element and $k = R/\pi R$ the residue field of R. Typical examples include $R = k[[\pi]]$ and $R = \mathbf{Z}_p$, $\pi = p$.

2.1 Minimal Weierstrass models

Given an elliptic curve E over K, we would like to find a "nice" model $\mathcal{E}$ of E over R (and study its reduction $\widetilde{E} = \mathcal{E} \pmod{\pi}$ over k). Geometrically, $\mathcal{E} \longrightarrow \mathrm{Spec}(R)$ is a fibration over a one-dimensional base; its generic fibre E is an elliptic curve over K, while its special fibre $\widetilde{E} = \mathcal{E} \otimes_R k$ can have singularities.

(2.1.1) Definition. *Let E be an elliptic curve over K. A* **generalized Weierstrass model of E over R** *is a generalized Weierstrass equation*

$$\mathcal{E} : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2.1.1.1}$$

of an elliptic curve isomorphic to E, in which all coefficients $a_i \in R$ lie in R. (In a fancy language, (2.1.1.1) is a projective R-scheme $\mathcal{E} \subset \mathbf{P}^2_R$ such that $\mathcal{E} \otimes_R K$ is isomorphic to E.)

(2.1.2) Discriminant. Considering the coefficients a_i of (the affine form of) the generalized Weierstrass equation

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0 \tag{2.1.2.1}$$

as variables, the intersection of the ideal $(f, \partial f/\partial x, \partial f/\partial y)$ in $\mathbf{Z}[x, y, a_1, \dots, a_6]$ with $\mathbf{Z}[a_1, \dots, a_6]$ is a principal ideal, generated by a polynomial $\Delta(a_1, \dots, a_6) \in \mathbf{Z}[a_1, \dots, a_6]$ (unique up to a sign). We refer to ([Si 1], III.1) for the general formulas; if $a_1 = a_2 = a_3 = 0$, then we have the usual formula

$$\Delta = -16(4a_4^3 + 27a_6^2),$$

which is also equal to

$$\Delta = 8(9(3a_6 - 2a_4x)(2f - y\,\partial f/\partial y) + 2(4a_4^2 - 9a_6x + 6a_4x^2)\,\partial f/\partial x).$$

In general, replacing x, y by new variables x', y' as in (I.2.2.2.1)

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + u^2sx' + t \end{aligned} \qquad (r, s, t \in K,\ u \in K^*) \tag{2.1.2.2}$$

has the effect of multiplying Δ by u^{-12}. One can also define the j-invariant $j(a_1, \ldots, a_6)$ for an arbitrary generalized Weierstrass equation; it coincides with the function

$$j = \frac{4(12a_4)^3}{4a_4^3 + 27a_6^2}$$

defined in II.2.2.6 if $a_1 = a_2 = a_3 = 0$ and is invariant under the transformations (2.1.2.2).

If $a_i \in K$, then the curve (2.1.2.1) is smooth over K if and only if $\Delta \neq 0 \in K$.

(2.1.3) Definition. *We say that $\mathcal{E}$ in (2.1.1.1) is a* **minimal Weierstrass model** *of E over R if the valuation $\mathrm{ord}_\pi(\Delta(\mathcal{E})) \geq 0$ is minimal (among all generalized Weierstrass models of E over R).*

(2.1.4) Example. Assume that $char(k) \neq 2, 3$. Then (the affine form of) the Weierstrass model $\mathcal{E}$

$$y^2 = x^3 + \pi^6$$

is *not* minimal, as the change of variables

$$x = \pi^2 x', \qquad y = \pi^3 y'$$

transforms $\mathcal{E}$ into a model $\mathcal{E}'$ given by

$$y'^2 = x'^3 + 1.$$

In this example, $\mathrm{ord}_\pi(\Delta(\mathcal{E})) = 12$, $\mathrm{ord}_\pi(\Delta(\mathcal{E}')) = 0$.

(2.1.5) Proposition. (i) *E has a minimal Weierstrass model over R, which is unique up to transformations (2.1.2.2) with $u \in R^*$, $r, s, t \in R$.*
(ii) *If $\mathrm{ord}_\pi(\Delta(\mathcal{E})) < 12$, then $\mathcal{E}$ is a minimal Weierstrass model.*
(iii) *If $\mathcal{E}$ is a minimal Weierstrass model of E, then the R-submodule $R \cdot \omega_\mathcal{E} \subset \Gamma(E, \Omega_{E/K})$ (where $\omega_\mathcal{E} = dx/(2y + a_1x + a_3)$) does not depend on $\mathcal{E}$.*
(iv) *If $\mathcal{E}$ is any Weierstrass model of E over R, then any change of variables (2.1.2.2) that transforms $\mathcal{E}$ to a minimal Weierstrass model has $u, r, s, t \in R$.*

Proof. See [Si 1], VII.1.3.

2.2 Reduction of Minimal Weierstrass models

(2.2.1) Lemma-Definition. *Let E be an elliptic curve over K; fix a minimal Weierstrass model $\mathcal{E}$ of E over R. The* **reduction** *$\widetilde{E} := \mathcal{E} \otimes_R k$ of $\mathcal{E}$, i.e. (the projectivization of) the curve*

$$y^2 + \overline{a}_1 xy + \overline{a}_3 y = x^3 + \overline{a}_2 x^2 + \overline{a}_4 x + \overline{a}_6 \qquad (\overline{a}_i = a_i \pmod{\pi} \in k)$$

is a cubic projective curve over k, whose isomorphism class depends only on E. Its discriminant is equal to $\Delta(\widetilde{E}) = \Delta(\mathcal{E}) \pmod{\pi}$.

(2.2.2) Definition. *E has* **good reduction** *if $\mathrm{ord}_\pi(\Delta(\mathcal{E})) = 0$ ($\iff \Delta(\widetilde{E}) \neq 0 \in k \iff \widetilde{E}$ is an elliptic curve over k). E has* **bad reduction** *if $\pi | \Delta(\mathcal{E})$ ($\iff \widetilde{E}$ is not smooth over k).*

(2.2.3) Example. Assume that $char(k) \neq 2, 3$. Then

$$y^2 = x^3 + \pi$$

is (the affine form of) a minimal Weierstrass model $\mathcal{E}$ of E, by 2.1.5(ii); thus E has bad reduction. Passing to the ramified extension $K' = K(\pi')$, where $\pi'^6 = \pi$, the base change $E' = E \otimes_K K'$ of E has a Weierstrass model $\mathcal{E}'$ over R' (= the ring of integers in K') of the form

$$y'^2 = x'^3 + 1 \qquad (x' = x/\pi'^2,\ y' = y/\pi'^3),$$

hence E' has good reduction.

(2.2.4) The reduction map. Every point $P \in E(K)$ can be represented by a point $(a : b : c) \in \mathcal{E}(R)$ with homogeneous coordinates $a, b, c \in R$; these coordinates are determined up to a common factor in R^* and at least one of them lies in R^*. Taking their reductions modulo π, we obtain a point $(\overline{a} : \overline{b} : \overline{c}) \in \widetilde{E}(k)$, which depends only on P; it will be denoted by $\mathrm{red}(P)$. This defines a map

$$\mathrm{red} : E(K) \xleftarrow{\sim} \mathcal{E}(R) \xrightarrow{(\mathrm{mod}\,\pi)} \widetilde{E}(k) \tag{2.2.4.1}$$

which does not depend on the choice of $\mathcal{E}$ (by 2.1.5(i)).

(2.2.5) Let us assume, from now on, that if $\widetilde{E}$ is not smooth over k, then its (unique) non-smooth point S is defined over k. This assumption is automatically satisfied if $char(k) \neq 2, 3$ or if k is perfect (by II.1.3.1-2).

(2.2.6) Proposition-Definition. *Put*

$$\widetilde{E}^{\mathrm{sm}} = \begin{cases} \widetilde{E}, & \text{if } E \text{ has good reduction} \\ \widetilde{E} - \{S\}, & \text{if } E \text{ has bad reduction,} \end{cases}$$
$$E_0(K) = \mathrm{red}^{-1}(\widetilde{E}^{\mathrm{sm}}(k)).$$

Then the reduction map

$$\mathrm{red} : E_0(K) \longrightarrow \widetilde{E}^{\mathrm{sm}}(k)$$

is a homomorphism of abelian groups (with the group operation on the target defined as in II.1.3.6).

Proof. This follows from the fact that the usual geometric definition of the group law (in terms of intersections with lines in $\mathbf{P}^2$) defines an abelian group structure on $\mathcal{E}^{\mathrm{sm}}(R)$ (where $\mathcal{E}^{\mathrm{sm}} = \mathcal{E} - \{S\}$). [In fact, this defines on $\mathcal{E}^{\mathrm{sm}}$ a structure of a commutative group scheme over R, for which the natural maps $\mathcal{E}^{\mathrm{sm}} \otimes_R K \xrightarrow{\sim} E$ and $\mathcal{E}^{\mathrm{sm}} \otimes_R k \xrightarrow{\sim} \widetilde{E}^{\mathrm{sm}}$ are isomorphisms of group schemes.]

(2.2.7) Lifting of points - Example: The reduction map (2.2.4.1) need not be surjective, even if R is complete. For example, if $R = \mathbf{Z}_p$, $\pi = p$, $k = \mathbf{F}_p$, let

$$\mathcal{E} : y^2 = x^3 + p, \qquad \widetilde{E} : y^2 = x^3, \qquad P = (0, 0) \in \widetilde{E}(\mathbf{F}_p).$$

Then there is no $Q \in \mathcal{E}(\mathbf{Z}_p)$ with $\mathrm{red}(Q) = P$. Note that the point P in this example is the non-smooth point $P = S$ of $\widetilde{E}$.

(2.2.8) Proposition. *If R is complete, then the homomorphism*

$$\mathrm{red} : E_0(K) \longrightarrow \widetilde{E}^{\mathrm{sm}}(k)$$

is surjective.

Proof. This follows from Hensel's Lemma (cf. [Si 1], VII.2.1).

(2.2.9) The group structure on $E^{\mathrm{sm}}(k')$ (for any field extension k'/k) was analyzed in II.1.3.7-10. We say that E has **split multiplicative reduction**, resp. **non-split multiplicative reduction**, resp. **additive reduction**, if $\widetilde{E}$ is as in I.1.3.7, resp. I.1.3.9, resp. I.1.3.5.

(2.2.10) Theorem (Kodaira, Néron). *The group $E(K)/E_0(K)$ is finite. More precisely, if E has split multiplicative reduction, then $E(K)/E_0(K)$ is cyclic of order $\mathrm{ord}_\pi(\Delta(\mathcal{E})) = -\mathrm{ord}_\pi(j(E))$; in all other cases it is an abelian group of order ≤ 4.*

"Proof". The finiteness is easy to establish if the residue field k is finite. In general one has to use the theory of Néron models. See [Si 1], VII.6.2; [Si 2], IV.9.2.

(2.2.11) Denote the kernel of the reduction map from 2.2.8 by $E_1(K)$. Then

$$E_1(K) = \{O\} \cup \{(x, y) \in E(K) \,|\, \mathrm{ord}_\pi(x), \mathrm{ord}_\pi(y) < 0\}$$

and there is exact sequence (assuming that R is complete)

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \xrightarrow{\text{red}} \widetilde{E}^{\text{sm}}(k) \longrightarrow 0.$$

In Sect. 2.4 we shall investigate the torsion subgroup of $E_0(K)$ using a sequence of subgroups

$$E_0(K) \supset E_1(K) \supset E_2(K) \supset E_3(K) \cdots$$

analogous to the subgroups

$$R^* \supset 1 + \pi R \supset 1 + \pi^2 R \supset 1 + \pi^3 R \cdots$$

of the multiplicative group of R.

2.3 A digression on formal groups

(2.3.1) Given an elliptic curve E in its generalized Weierstrass form

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \tag{2.3.1.1}$$

we would like to study its local geometry around the point at infinity O. As in I.4.2.2, we have $\text{ord}_O(x) = -2$, $\text{ord}_O(y) = -3$; thus $z = -x/y$ is a local parameter at O. One can develop x and y into formal power series in z as follows: rewriting (2.3.1.1) in the new variables

$$z = -\frac{x}{y}, \qquad w = -\frac{1}{y},$$

we obtain

$$w = w(z) = z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3.$$

Writing $w = z^3 + \cdots$ and substituting into (2.3.1.2), we obtain recursively

$$w = z^3 + a_1 z^4 + \cdots = z^3 + a_1 z^4 + (a_1^2 + a_2)z^5 + \cdots = z^3(1 + A_1 z + A_2 z^2 + \cdots) \in \mathbf{Z}[a_1, \ldots, a_6][[z]]$$

where $A_i \in \mathbf{Z}[a_1, \ldots, a_6]$ are some universal polynomials (i.e. we view the coefficients a_i as variables). This yields formal expansions

$$\begin{aligned} x(z) &= \frac{z}{w(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z + \cdots \\ y(z) &= \frac{-1}{w(z)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + \cdots \\ \omega(z) &= \frac{dx}{2y + a_1 x + a_3} = (1 + a_1 z + (a_1^2 + a_2)z^2 + \cdots)\, dz \end{aligned} \tag{2.3.1.2}$$

with coefficients in $\mathbf{Z}[a_1, \ldots, a_6]$ (see [Si 1], IV.1 for more details).

(2.3.2) Similarly, the group law on E can also be written in the variables (z, w). For example, the inverse $P \mapsto -P = [-1]P$ is given in the (x, y)-coordinates by $[-1](x, y) = (x, -y - a_1 x - a_3)$. Passing to the (z, w)-coordinates, we obtain

$$[-1](z) = \frac{x(z)}{y(z) + a_1 x(z) + a_3} = -z + a_1 + \cdots \in \mathbf{Z}[a_1, \ldots, a_6][[z]]. \tag{2.3.2.1}$$

As regards the group law itself, note that a linear relation between $1, x, y$ is equivalent to a linear relation between $1, z, w$; thus we can use the standard geometric description of $\boxplus$ (I.10.1.1.1) also in the (z, w)-plane.

If z_1, z_2 are independent variables, put $P_i = (z_i, w(z_i))$ $(i = 1, 2)$ and consider the line $\ell = \overline{P_1 P_2} : w = az + b$ through the points P_1, P_2. Expanding both coefficients

$$a = a(z_1, z_2) = \frac{w(z_2) - w(z_1)}{z_2 - z_1}, \qquad b = b(z_1, z_2) = w(z_1) - a(z_1, z_2)z_1,$$

we obtain power series in z_1, z_2 with coefficients in $\mathbf{Z}[a_1, \ldots, a_6]$. Substituting $w = az + b$ to (2.3.1.2), we obtain a cubic equation for z with roots z_1, z_2, z_3. Comparing the coefficients at z^2 (as in I.7.5.7) yields a power series expansion for the third root z_3, hence also for

$$F(z_1, z_2) = [-1](z_3) = z_1 + z_2 - a_1 z_1 z_2 + \cdots \in \mathbf{Z}[a_1, \ldots, a_6][[z_1, z_2]], \tag{2.3.2.2}$$

which is the formal group law $\boxplus$ in terms of the z-coordinate.

The series F has the following properties:

$$F(z_1, z_2) = F(z_2, z_1), \qquad F(z_1, F(z_2, z_3)) = F(F(z_1, z_2), z_3), \qquad F(z, [-1]z) = 0,$$

which correspond to the commutativity, associativity and the inverse for $\boxplus$ on E (again, see [Si 1], IV.1 for more details).

(2.3.3) Definition. *A formal group $\mathscr{F}$ (commutative, of dimension one) over a commutative ring A is a power series $F(T_1, T_2) \in A[[T_1, T_2]]$ ("the formal group law of $\mathscr{F}$") with the following properties:*
(i) $F(T_1, T_2) = T_1 + T_2 + \cdots$.
(ii) $F(T_1, F(T_2, T_3)) = F(F(T_1, T_2), T_3)$.
(iii) $F(T_1, T_2) = F(T_2, T_1)$ *(this follows from (i)–(ii) for "good" rings A).*

(2.3.4) Exercise. *Given $F(T_1, T_2)$ satisfying (i)–(iii), show that $F(0, T) = F(T, 0) = T$ and that there is a unique power series $[-1](T) \in A[[T]]$ satisfying $F(T, [-1](T)) = 0$.*

(2.3.5) Examples: (1) **Formal additive group $\mathscr{F} = \widehat{\mathbf{G}}_a$:** $F(T_1, T_2) = T_1 + T_2$.
(2) **Formal multiplicative group $\mathscr{F} = \widehat{\mathbf{G}}_m$:** $F(T_1, T_2) = (1 + T_1)(1 + T_2) - 1 = T_1 + T_2 + T_1 T_2$.
(3) The construction from 2.3.2 gives a formal group $\widehat{\mathcal{E}}$ over $\mathbf{Z}[a_1, \ldots, a_6]$.

(2.3.6) Definition. *Let $\mathscr{F}$ be a formal group, with the formal group law $F(T_1, T_2)$. For an integer $n > 1$, put*

$$[n]_{\mathscr{F}}(T) = F(F(\cdots(F(\underbrace{T, T), T)\cdots, T}_{n-\text{times}}) \in A[[T]], \qquad [-n]_{\mathscr{F}}(T) = [n]_{\mathscr{F}}([-1](T)), \qquad [1]_{\mathscr{F}}(T) = T.$$

(2.3.7) Examples: (1) For $\mathscr{F} = \widehat{\mathbf{G}}_a$, $[n]_{\mathscr{F}}(T) = nT$. (2) For $\mathscr{F} = \widehat{\mathbf{G}}_m$, $[n]_{\mathscr{F}}(T) = (1 + T)^n - 1$.

(2.3.8) Definition. *Let A be a complete local ring with maximal ideal $\mathfrak{m}$ and $\mathscr{F}$ a formal group over A. For each $i \geq 1$, denote by $\mathscr{F}(\mathfrak{m}^i)$ the set $\mathfrak{m}^i$ with the abelian group law $x \boxplus_F y = F(x, y)$ (note that $F(x, y)$ is convergent to an element of $\mathfrak{m}^i$, if $x, y \in \mathfrak{m}^i$).*

(2.3.9) Examples: (1) $\widehat{\mathbf{G}}_a(\mathfrak{m}^i) = (\mathfrak{m}^i, +)$. (2) $\widehat{\mathbf{G}}_m(\mathfrak{m}^i) \xrightarrow{\sim} (1 + \mathfrak{m}^i, \times)$.

2.4 The torsion subgroup of $E_1(K)$ via formal groups

In this section we assume that the discrete valuation ring R is complete. Let E, $\mathcal{E}$ and $\widetilde{E}$ be as in 2.2, i.e. E is an elliptic curve over $K = \mathrm{Frac}(R)$, $\mathcal{E}$ is a minimal Weierstrass model of E over R and $\widetilde{E}$ its reduction modulo π.

(2.4.1) Substituting to the universal power series (2.3.1.2) and (2.3.2.1-2) the values of the coefficients $a_i \in R$ of $\mathcal{E}$, we obtain power series $x(z), y(z) \in R[[z]]$ and a formal group over R, which will still be denoted by $\widehat{\mathcal{E}}$.

(2.4.2) Proposition-Definition. *For $i \geq 1$, put*

$$E_i(K) = \{O\} \cup \{(x,y) \in E(K) \,|\, \mathrm{ord}_\pi(x) \leq -2i,\ \mathrm{ord}_\pi(y) \leq -3i\}$$

(for $i = 1$ this definition agrees with that from 2.2.11). The map $z \mapsto (x(z), y(z))$ defines a bijection $\pi^i R \xrightarrow{\sim} E_i(K)$, hence an isomorphism of abelian groups $\widehat{\mathcal{E}}(\pi^i R) \xrightarrow{\sim} E_i(K)$ (in particular, $E_i(K)$ is a subgroup of $E_0(K)$).

Proof. See [Si 1], VII.2.2 in the case $i = 1$; the same argument applies for all $i \geq 1$.

(2.4.3) Lemma. *Let $\mathscr{F}$ be a formal group over R in the sense of 2.3.3 (e.g. $\widehat{\mathbf{G}}_m$ or $\widehat{\mathcal{E}}$). Then:*
(i) *For each $i \geq 1$, there are canonical isomorphisms of abelian groups $\mathscr{F}(\pi^i R)/\mathscr{F}(\pi^{i+1}R) \xrightarrow{\sim} \pi^i R/\pi^{i+1}R \xrightarrow{\sim} (k,+)$.*
(ii) *If $n \in \mathbf{Z}$ and $char(k) \nmid n$, then the power series $[n]_{\mathscr{F}}(T) \in R[[T]]$ is invertible, in the sense that there exists (a unique) power series $g(T) \in R[[T]]$ such that $[n]_{\mathscr{F}}(g(T)) = T$. The power series $g(T)$ also satisfies $g([n]_{\mathscr{F}}(T)) = T$.*

Proof. (i) For $x, y \in \pi^j R$ $(j \geq 1)$, $F(x,y) \equiv x + y \pmod{\pi^{j+1}R}$ (where F is the formal group law of $\mathscr{F}$).
(ii) The assumption on n implies that $n \in R^*$ is invertible in R. As the power series $[n]_{\mathscr{F}}(T)$ begins with $nT + \cdots$, one constructs the coefficients of $g(T) = n^{-1}T + \cdots$ by induction (see [Si 1], IV.2.4).

(2.4.4) Corollary. *If $n \in \mathbf{Z}$ and $char(k) \nmid n$, then $\mathscr{F}(\pi R)_n = 0$. In particular, $E_1(K)_n = \widehat{\mathcal{E}}(\pi R)_n = 0$, i.e. there is no n-torsion in the kernel of the reduction map.*

(2.4.5) Lemma. *If $char(k) = p > 0$, then there exist power series $f(T), g(T) \in R[[T]]$ such that*

$$[p]_{\widehat{\mathcal{E}}}(T) = pf(T) + g(T^p) = pT + \cdots. \tag{2.4.5.1}$$

Proof. Denote the power series $[p]_{\widehat{\mathcal{E}}}(T) \in R[[T]]$ by $P(T)$. The translation invariance of the differential $\omega = \omega(z) = h(z)dz$ implies that

$$ph(T)dT = p\omega = [p]^*_{\widehat{\mathcal{E}}}\omega = h(P(T))P'(T)dT,$$

hence

$$h(P(T))P'(T) \in pR[[T]].$$

As $h(T) = 1 + h_1 T + \cdots$ (cf. (2.3.1.2)) and $P(T) = pT + \cdots$, we obtain $P'(T) \in pR[[T]]$; lemma follows.

(2.4.6) A toy model: For $\mathscr{F} = \widehat{\mathbf{G}}_m$, the torsion subgroup $\mathscr{F}(\pi R)_{tors}$ is just the group of roots of unity contained in $1 + \pi R$. If $char(k) = p > 0 = char(K)$, then each element $x \in \mathscr{F}(\pi R)_{tors} - \{0\}$ has order $m = p^n$ $(n \geq 1)$, i.e. $\zeta := 1 + x$ is a primitive p^n-th root of unity. It follows from

$$(\forall j \not\equiv 0 \pmod p) \quad (1-\zeta^j)/(1-\zeta) \in R^*, \qquad \prod_{\substack{0<j<p^n \\ p\nmid j}} (1-\zeta^j) = p$$

that the absolute ramification index of R is equal to

$$e := \mathrm{ord}_\pi(p) = p^{n-1}(p-1)\,\mathrm{ord}_\pi(x) \implies p^{n-1}(p-1) \leq e.$$

(2.4.7) Definition. *For $Q \in \widehat{\mathcal{E}}(\pi R)$, put $\mathrm{ord}_\pi(Q) = \max\{i \geq 1 \,|\, Q \in \widehat{\mathcal{E}}(\pi^i R)\}$ (i.e. $\mathrm{ord}_\pi(x,y) = i \iff i = -\mathrm{ord}_\pi(x)/2 = -\mathrm{ord}_\pi(y)/3$, by 2.4.2).*

(2.4.8) Theorem. *Assume that $char(k) = p > 0$, $char(K) = 0$; denote by $e = \mathrm{ord}_\pi(p)$ the absolute ramification index of R. Let $Q \in \widehat{\mathcal{E}}(\pi R)_{tors}$ be a torsion element of exact order $m > 1$. Then $m = p^n$ with*

$$p^{n-1}(p-1) \leq e, \qquad \mathrm{ord}_\pi(Q) \leq \frac{e}{p^{n-1}(p-1)}.$$

Proof. Let $Q \in \widehat{\mathcal{E}}(\pi R)$. The formula (2.4.5.1) implies that

$$\mathrm{ord}_\pi([p]_{\widehat{\mathcal{E}}}(Q)) \begin{cases} \geq \min(e + \mathrm{ord}_\pi(Q), p \cdot \mathrm{ord}_\pi(Q)) & \\ = e + \mathrm{ord}_\pi(Q), & \text{if } (p-1)\mathrm{ord}_\pi(Q) > e. \end{cases} \tag{2.4.8.1}$$

Assume that Q is torsion, of exact order $m > 1$. As there is no prime-to-p torsion in $\widehat{\mathcal{E}}(\pi R)$ (by 2.4.4), we have $m = p^n$, $n \geq 1$. Assume first that $n = 1$. If $(p-1)\mathrm{ord}_\pi(Q) > e$, then (2.4.8.1) implies that $\mathrm{ord}_\pi([p]_{\widehat{\mathcal{E}}}(Q)) = e + \mathrm{ord}_\pi(Q) < \infty$, hence $[p]_{\widehat{\mathcal{E}}}(Q) \neq 0$, which is a contradiction. Thus $1 \leq \mathrm{ord}_\pi(Q) \leq e/(p-1)$, as claimed. If $n > 1$, then the same argument applied to $[p^{n-1}]_{\widehat{\mathcal{E}}}Q$ shows that $\mathrm{ord}_\pi([p^{n-1}]_{\widehat{\mathcal{E}}}Q) \leq e/(p-1)$, hence $\mathrm{ord}_\pi([p^i]_{\widehat{\mathcal{E}}}Q) \leq e/(p-1)$ for all $i = 0, \ldots, n-1$. Applying (2.4.8.1) to all $[p^i]_{\widehat{\mathcal{E}}}Q$ $(i = 0, \ldots, n-1)$ yields $\mathrm{ord}_\pi([p^{i+1}]_{\widehat{\mathcal{E}}}Q) \geq p \cdot \mathrm{ord}_\pi([p^i]_{\widehat{\mathcal{E}}}Q)$. The statement of the Theorem then follows by induction.

(2.4.9) Corollary. *If $e < p-1$, then $\widehat{\mathcal{E}}(\pi R)_{tors} = 0$, hence the restriction of the reduction map to the torsion subgroup*

$$E_0(K)_{tors} \hookrightarrow E_0(K) \xrightarrow{\mathrm{red}} \widetilde{E}^{\mathrm{sm}}(k)$$

is **injective**.

3. Elliptic curves over number fields

Throughout this section, K will denote a number field, $\mathcal{O}_K$ its ring of integers, M_K (resp. M_K^f) the set of all primes (resp. of all finite primes) of K. For each $v \in M_K^f$ we denote by $\mathcal{O}_v$ the localization of $\mathcal{O}_K$ at v and by $\widehat{\mathcal{O}}_v$ (resp. $K_v = \mathrm{Frac}(\widehat{\mathcal{O}}_v)$) the v-adic completion of $\mathcal{O}_K$ (resp. of K). The (finite) residue field of $\mathcal{O}_v$ will be denoted by $k(v)$ and the valuation associated to v by ord_v. The basic example is that of $K = \mathbf{Q}$, when $\mathcal{O}_K = \mathbf{Z}$, $v = p$ is a usual prime, $\mathcal{O}_v$ consists of all rational numbers with denominators prime to p, $k(v) = \mathbf{F}_p$, $\widehat{\mathcal{O}}_v = \mathbf{Z}_p$ and $K_v = \mathbf{Q}_p$.

3.1 Minimal Weierstrass models

(3.1.1) Let E be an elliptic curve over K. For each $v \in M_K^f$ there is a minimal Weierstrass model of E over $\mathcal{O}_v$, with minimal discriminant $\Delta_{v,\min} \in \mathcal{O}_v - \{0\}$. Is it possible to find a *global* Weierstrass model $\mathcal{E}$ of E in the (affine) form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_i \in \mathcal{O}_K) \tag{3.1.1.1}$$

that would satisfy the minimality condition

$$\mathrm{ord}_v(\Delta(\mathcal{E})) = \mathrm{ord}_v(\Delta_{v,\min}) \tag{3.1.1.2}$$

for all $v \in M_K^f$? Let us investigate this question. Choosing any Weierstrass model $\mathcal{E}$ of E of the form (3.1.1.1), we have

$$(\forall v \in M_K^f) \qquad \mathrm{ord}_v(\Delta(\mathcal{E})) \equiv \mathrm{ord}_v(\Delta_{v,\min}) \pmod{12}, \tag{3.1.1.3}$$

as any change of variables (2.1.2.2) multiplies Δ by u^{-12}. Defining the **global minimal discriminant ideal of** E by

$$\Delta_{min} = \prod_{v \in M_K^f} \mathfrak{p}_v^{\mathrm{ord}_v(\Delta_{v,min})}$$

(where $\mathfrak{p}_v \subset \mathcal{O}_K$ is the prime ideal corresponding to v), we can rewrite (3.1.1.3) as

$$\Delta_{min} = \frac{\Delta(\mathcal{E})}{I^{12}},$$

where $I \subset \mathcal{O}_K$ is a non-zero *ideal*.

(3.1.2) If I is not principal, then we cannot achieve (3.1.1.2) by any change of variables (2.1.2.2), hence there is no minimal Weierstrass model of the form (3.1.1.1). However, one can construct a slightly more general minimal Weierstrass model as follows. Let S be the (finite) set of primes $v \in M_K^f$ such that our chosen $\mathcal{E}$ is not minimal at v, i.e.

$$S = \{v \in M_K^f \,|\, \mathrm{ord}_v(\Delta(\mathcal{E})) > \mathrm{ord}_v(\Delta_{v,min})\} \subset \{v \in M_K^f \,|\, \mathrm{ord}_v(\Delta(\mathcal{E})) \geq 12\}.$$

Denote by $\mathcal{O}_{K,S} = \mathcal{O}_K[1/S]$ the ring of S-integers in K. One can then glue together $\mathcal{E} \otimes \mathcal{O}_{K,S}$ with local minimal Weierstrass models of E over each $\mathcal{O}_v$ ($v \in S$) along the common "general fibre" E. What one obtains is a minimal Weierstrass model $\mathcal{E}$ of E which is not contained in $\mathbf{P}^2_{\mathcal{O}_K}$, but in a slightly more general version of $\mathbf{P}^2$. The point is that the usual construction of $\mathbf{P}^2 = \mathbf{P}(V)$ parametrizing lines (or hyperplanes) in a three-dimensional "vector space" V works well over a field or a local ring, but not over a more general base, when one has to consider "families of vector spaces", i.e. vector bundles. In concrete terms, $\mathcal{E} \subset \mathbf{P}(V)$ will be contained in the "projective space" over $\mathcal{O}_K$ associated to a suitable projective $\mathcal{O}_K$-module V, which will not be free.

(3.1.3) If $I = (u)$ is principal, then for each $v \in S$ there is a change of variables

$$x = u_v^2 x_v + r_v, \qquad y = u_v^3 y_v + u_v^2 s_v x_v + t_v$$

producing a minimal Weierstrass model over $\mathcal{O}_v$, where $r_v, s_v, t_v, u_v \in \mathcal{O}_v$ are v-integral (by 2.1.5(iv)) and $\mathrm{ord}_v(u_v) = \mathrm{ord}_v(u)$. Choosing a triple $(r, s, t) \in \mathcal{O}_K^3$ that is v-adically close to $(r_v, s_v, t_v) \in \mathcal{O}_v^3$ for each $v \in S$, the transformation

$$x = u^2 x' + r \qquad y = u^3 y' + u^2 s x' + t$$

will produce the desired global minimal Weierstrass model of E over $\mathcal{O}_K$ in the form (3.1.1.1) (see [Si 1], VIII.8.2 for more details).

(3.1.4) In particular, if $\mathcal{O}_K$ is a principal ideal domain (e.g. if $K = \mathbf{Q}$), every elliptic curve over K admits a global minimal Weierstrass model in the form (3.1.1.1).

(3.1.5) Definition. *Let E be an elliptic curve over K and $v \in M_K^f$. We define* **the reduction $\widetilde{E}_v$ of E modulo v** *to be the reduction modulo v of any minimal Weierstrass model $\mathcal{E}_v$ of E over $\mathcal{O}_v$. We say that E has* **good reduction at** *v if $\widetilde{E}_v$ is an elliptic curve over $k(v)$ ($\iff \mathrm{ord}_v(\Delta(\mathcal{E}_v)) = 0 \iff \mathrm{ord}_v(\Delta_{min}) = 0$).*

3.2 The torsion subgroup of $E(K)$

(3.2.1). *Let E be an elliptic curve over K and $v \in M_K^f$ a prime such that E has good reduction at v and $\mathrm{ord}_v(p) < p-1$ (where $p = char(k(v))$). Then the restriction of the reduction map $\mathrm{red}_v : E(K_v) \longrightarrow \widetilde{E}_v(k(v))$ to the torsion subgroup of $E(K)$*

$$E(K)_{tors} \hookrightarrow E(K_v)_{tors} \hookrightarrow E(K_v) \xrightarrow{\mathrm{red}_v} \widetilde{E}_v(k(v))$$

is injective.

Proof. By 2.4.9, already the restriction of red_v to $E(K_v)_{tors}$ is injective (note that $E_0(K_v) = E(K_v)$, as we are assuming that E has good reduction at v).

(3.2.2) Corollary. *The torsion subgroup $E(K)_{tors}$ is finite and effectively computable.*

(3.2.3) Proposition. *Let $D \in \mathbf{Z}$ be a cube-free integer $D \geq 1$, and E the elliptic curve over $K = \mathbf{Q}$ given by $E : X^3 + Y^3 = DZ^3$. Then*

$$E(\mathbf{Q})_{tors} = \begin{cases} \mathbf{Z}/3\mathbf{Z}, & D = 1 \\ \mathbf{Z}/2\mathbf{Z}, & D = 2 \\ 0, & D > 2. \end{cases}$$

Proof. E has good reduction at each prime $p \nmid 3D$. Put

$$P_D = \{p \text{ prime} \,|\, p \equiv 5 \pmod 6, p \nmid D\}.$$

For each $p \in P_D$, the map $x \mapsto x^3$ is a bijection $\mathbf{F}_p \xrightarrow{\sim} \mathbf{F}_p$, hence the number of points in $\widetilde{E}_p(\mathbf{F}_p)$ is the same as in $C_D(\mathbf{F}_p)$, where $C_D : X + Y = DZ$. As $C_D \xrightarrow{\sim} \mathbf{P}^1$ (over $\mathbf{F}_p$), we have $\#\widetilde{E}_p(\mathbf{F}_p) = \#\mathbf{P}^1(\mathbf{F}_p) = p + 1$. It follows from 3.2.1 that

$$\#E(\mathbf{Q})_{tors} \,|\, \gcd\{p + 1 \,|\, p \in P_D\} = 6$$

(where the last equality is a consequence of Dirichlet's theorem on primes in arithmetic progressions). It remains to investigate the torsion points of order 2 and 3. As

$$E(\mathbf{C})_2 - \{O\} = \{(1 : 1 : \rho^j (2/D)^{1/3})\} \qquad (\rho = e^{2\pi i/3},\ O = (1 : -1 : 0)),$$

it follows that

$$E(\mathbf{Q})_2 = \begin{cases} \mathbf{Z}/2\mathbf{Z}, & D = 2 \\ 0, & D \neq 2. \end{cases}$$

Similarly,

$$E(\mathbf{C})_3 = \{(X : Y : Z) \in E(\mathbf{C}) \,|\, XYZ = 0\},$$

hence

$$E(\mathbf{Q})_3 = \begin{cases} \mathbf{Z}/3\mathbf{Z}, & D = 1 \\ 0, & D \neq 1. \end{cases}$$

Proposition follows.

(3.2.4) Exercise. *Let $E : y^2 = x^3 - Dx$, where $D \in \mathbf{Z} - \{0\}$ is an integer not divisible by the fourth power of any prime. Show that*

$$E(\mathbf{Q})_{tors} = \begin{cases} \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}, & D = n^2, n \in \mathbf{Z} \\ \mathbf{Z}/4\mathbf{Z}, & D = -4 \\ \mathbf{Z}/2\mathbf{Z}, & \textit{otherwise.} \end{cases}$$

(3.2.5) Proposition. *Let E be an elliptic curve over a number field K and $\mathcal{E}$ any Weierstrass model of E over $\mathcal{O}_K$ (as in (3.1.1.1)). If $P = (x, y) \in \mathcal{E}(K)_{tors}$ is a torsion point of exact order $m > 1$, then*
(i) *If $m \neq p^n$ is not a prime power, then $x, y \in \mathcal{O}_K$.*
(ii) *If $m = p^n$ is a prime power, then*

$$(\forall v \in M_K^f) \qquad \mathrm{ord}_v(x) \geq -2r_v, \quad \mathrm{ord}_v(y) \geq -3r_v,$$

where $r_v \geq 0$ is the largest integer satisfying $p^{n-1}(p-1)r_v \leq \mathrm{ord}_v(p)$ ($p = char(k(v))$).

Proof. Fix v and work with $\mathcal{E}_v := \mathcal{E} \otimes_{\mathcal{O}_K} \widehat{\mathcal{O}}_v$ over $\widehat{\mathcal{O}}_v$. If $x, y \in \mathcal{O}_K$, then there is nothing to prove. If not, then we can assume that $\mathcal{E}_v$ is minimal (if we pass to a minimal Weierstrass model via the transformation (2.1.2.2), the values of $\mathrm{ord}_v(x), \mathrm{ord}_v(y)$ decrease, by 2.1.5(iv)). If $\mathrm{ord}_v(x) < 0$ or $\mathrm{ord}_v(y) < 0$, then $(x, y) \in E_1(K_v) = \widehat{\mathcal{E}}_v(\pi_v \widehat{\mathcal{O}}_v)$, and we can apply the local result 2.4.8.

(3.2.6) Theorem (Lutz, Nagell). *Let E be an elliptic curve over $\mathbf{Q}$ in the Weierstrass form*

$$y^2 = x^3 + Ax + B, \qquad (A, B \in \mathbf{Z}).$$

Assume that $P = (x, y) \in E(\mathbf{Q})_{tors} - \{O\}$. Then
(i) $x, y \in \mathbf{Z}$.
(ii) *Either $y = 0$ (i.e. $[2]P = O$), or $y^2 | 4A^3 + 27B^2$.*

Proof. (i) Let $m > 1$ be the exact order of P. If $m = 2$, then $y = 0$, which implies that $x \in \mathbf{Z}$ (as $A, B \in \mathbf{Z}$). If $m > 2$, then the integers r_p in 3.2.5 are equal to $r_p = 0$ for all primes p, hence $x, y \in \mathbf{Z}$.
(ii) We can assume $y \neq 0$. Then $[2]P = (x_2, y_2) \in E(\mathbf{Q})_{tors} - \{O\}$, hence $x_2 \in \mathbf{Z}$. Explicit formulas for x_2 then give

$$4A^3 + 27B^2 = y^2(4(3x^2 + 4A)x_2 - (3x^3 - 5Ax - 27B)).$$

(3.2.7) Exercise. *Describe explicitly $E(\mathbf{Q})_{tors}$ (i.e. give the coordinates of all $\mathbf{Q}$-rational torsion points) for the following elliptic curves $E = E_j$:*

$$E_1 : y^2 = x^3 + 1, \qquad E_2 : y^2 = x^3 + 4x, \qquad E_3 : y^2 = x^3 - 4x, \qquad E_4 : y^2 - y = x^3 - x^2.$$

(3.2.8) The following general results on $E(K)_{tors}$ are much more difficult.

(3.2.9) Theorem (Mazur, 1977). *Let E be an elliptic curve over $\mathbf{Q}$. Then*

$$E(\mathbf{Q})_{tors} \xrightarrow{\sim} \begin{cases} \mathbf{Z}/m\mathbf{Z}, & 1 \leq m \leq 10 \text{ or } m = 12 \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2m\mathbf{Z}, & 1 \leq m \leq 4. \end{cases}$$

(3.2.10) Theorem. *For each $d \geq 1$ there is a constant $C(d)$ such that, for every number field K of degree $[K : \mathbf{Q}] = d$ and every elliptic curve E over K, $\#E(K)_{tors} \leq C(d)$.*

(3.2.11) This result was proved in the early 1990's for $d = 2, \ldots, 8$ by Kamieny-Mazur; their method was extended by Abramovich to $d = 9, \ldots, 14$. The general result is due to Merel (1994); subsequent work by Oesterlé and Parent yielded explicit upper bounds for $C(d)$.

3.3 The descent method

(3.3.1) The Congruent Number Problem. A **congruent number** is an integer $D \geq 1$ which occurs as the area of a right triangle with rational sides, i.e. such that there exist $a, b, c \in \mathbf{Q}^*_{>0}$ satisfying $a^2 + b^2 = c^2$ and $D = ab/2$. The parametrization (0.4.1.0.0) of the Pythagorean triples gives

$$(\exists t \in \mathbf{Q},\, t > 1) \qquad \frac{a}{c} = \frac{t^2 - 1}{t^2 + 1}, \qquad \frac{b}{c} = \frac{2t}{t^2 + 1} \quad \Longrightarrow \quad (\exists t \in \mathbf{Q},\, t > 1) \qquad D\left(\frac{t^2 + 1}{c}\right)^2 = t^3 - t. \tag{3.3.1.1}$$

This implies (possibly after replacing t by $-1/t$ - exercise!) that D is a congruent number if and only if the elliptic curve $E_D : Ds^2 = t^3 - t$ has a rational point $(t, s) \in E_D(\mathbf{Q})$ with $s \neq 0$. Note that the change of variables $D^2 s = s'$, $Dt = t'$ transforms E_D into the curve $s'^2 = t'^3 - D^2 t'$. The same argument as in the proof of 3.2.3 then shows (with a little help from 1.2.3(2a)) that

$$\{O\} \cup \{(0, 0), (\pm 1, 0)\} = E_D(\mathbf{Q})_2 = E_D(\mathbf{Q})_{tors},$$

hence

$$D \text{ is a congruent number} \quad \Longleftrightarrow \quad E_D(\mathbf{Q}) \neq E_D(\mathbf{Q})_{tors}.$$

(3.3.2) Theorem (Fermat). *$D = 1$ is not a congruent number.*

Proof. Assume that $0 < a, b, c \in \mathbf{Q}$ satisfy $a^2 + b^2 = c^2$, $ab/2 = 1$. As in (3.3.1.1), these values give rise to a rational point $(t, s) \in E_1(\mathbf{Q}) - \{O\}$, with $t, s > 0$. Writing $t = u/v$, where $u > v \geq 1 \in \mathbf{Z}$ are relatively prime integers, we have $w := sv^2 \in \mathbf{Z}$, hence

$$w^2 = uv(u + v)(u - v). \tag{3.3.2.1}$$

Replacing (u, v, w) by $((u + v)/2, (u - v)/2, w/2)$ if both u, v are odd, we can assume that $u \not\equiv v \pmod 2$, which implies that the four numbers $u, v, u + v, u - v$ are pairwise relatively prime. The equation (3.3.2.1) then implies that

$$u = L^2, \qquad v = M^2, \qquad u + v = X^2, \qquad u - v = Y^2,$$

for positive integers L, M, X, Y. It follows from

$$\left(\frac{X+Y}{2}\right)^2 + \left(\frac{X-Y}{2}\right)^2 = \frac{X^2+Y^2}{2} = u = L^2, \qquad \frac{1}{2}\left(\frac{X+Y}{2}\right)\left(\frac{X-Y}{2}\right) = \frac{X^2-Y^2}{8} = \frac{v}{4} = \left(\frac{M}{2}\right)^2$$

that

$$a_1 = \frac{X+Y}{M}, \qquad b_1 = \frac{X-Y}{M}, \qquad c_1 = \frac{2L}{M}$$

is another triple of rational numbers satisfying $a_1^2 + b_1^2 = c_1^2$, $a_1 b_1/2 = 1$. Applying the parametrization (3.3.1.1) once again, we obtain another rational point $(t_1, s_1) = (u_1/v_1, w_1/v_1^2) \in E_1(\mathbf{Q})$, hence another solution of (3.3.2.1) in positive integers u_1, v_1, w_1. More precisely, we have

$$\frac{X+Y}{2L} = \frac{a_1}{c_1} = \frac{t_1^2 - 1}{t_1^2 + 1}, \qquad \frac{X-Y}{2L} = \frac{b_1}{c_1} = \frac{2t_1}{t_1^2+1}$$

for $t_1 = u_1/v_1 \in \mathbf{Q}$, where $u_1 > v_1 \geq 1 \in \mathbf{Z}$ are relatively prime integers. It follows that

$$t = \frac{u}{v} = \left(\frac{L}{M}\right)^2 = \frac{2L^2}{X^2 - Y^2} = \frac{(t_1^2+1)^2}{4t_1^3 - 4t_1} = \frac{(u_1^2+v_1^2)^2}{4u_1v_1(u_1^2 - v_1^2)}. \tag{3.3.2.2}$$

As $\gcd(u_1 v_1, u_1^2 + v_1^2) = 1$, we have $v \geq u_1 v_1 > v_1^2 \geq v_1$. Continuing this process we obtain an infinite decreasing sequence of positive integers $v > v_1 > v_2 > \cdots$ ("the infinite descent"), which is impossible.

(3.3.3) Why does this argument work? The point is that the formula (3.3.2.2), namely

$$t = \frac{(t_1^2+1)^2}{4t_1^3 - 4t_1},$$

is exactly the expression in the duplication formula on E_1 (cf. (I.7.5.8.2) in the analytic context); thus we have, for a suitable choice of the sign,

$$[2](t_1, \pm s_1) = (t, s).$$

In other words, the original point $P = (t, s)$ is equal to $[2]P_1$ for some $P_1 \in E(\mathbf{Q})$; repeating this procedure, we obtain $P = [2]P_1 = [4]P_2 = [8]P_3 = \cdots$, which will contradict the fact that multiplication by 2 "increases the size" of (non-torsion) points in $E(\mathbf{Q})$.

The fact that we were able to "divide" $P = (t, s)$ by 2 had something to do with the fact the factors in (3.3.2.1) were relatively prime to each other, hence each of them – not just their product – was a square.

These two observations, i.e. (I) the possibility of dividing rational points by 2, and (II) the fact that multiplication by 2 increases the "size" of rational points [in fact, 2 can be replaced by any integer $n > 1$] are at the basis of the proof of the following fundamental result.

(3.3.4) Theorem ("Mordell-Weil Theorem"). *Let E be an elliptic curve over a number field K. Then $E(K)$ is finitely generated, i.e. $E(K) \xrightarrow{\sim} E(K)_{tors} \times \mathbf{Z}^r$, with $E(K)_{tors}$ finite and $0 \le r < \infty$. [As we have seen in 3.2, the torsion subgroup $E(K)_{tors}$ can be determined quite easily. Effective determination of the "rank" $r = r(E/K)$ is a major open problem.]*

(3.3.5) Proposition. *$D = 2$ is not a congruent number.*

Proof. As in the proof of 3.3.2, we have to show that the diophantine equation

$$2w^2 = uv(u+v)(u-v) \tag{3.3.5.1}$$

has no integral solution $u, v, w \in \mathbf{Z}$ with $u, v, w > 0$ and $\gcd(u, v) = 1$. There are three possible cases:

$$(a)\ 2 \nmid uv; \qquad (b)\ 2|u,\ 2 \nmid v; \qquad (c)\ 2 \nmid u,\ 2|v.$$

As in 3.3.2, the case (a) gives rise to another solution $((u+v)/2, (u-v)/2, w/2)$, which satisfies (b) or (c).

In the case (b), the four numbers $u, v, u+v, u-v$ are pairwise relatively prime and u is even, hence

$$u = 2L^2, \qquad v = M^2, \qquad u+v = X^2, \qquad u-v = Y^2,$$

for positive integers L, M, X, Y. As $2 \nmid XY$, we have

$$u + v \equiv u - v \equiv 1 \pmod 4,$$

which contradicts the fact that $2 \nmid v$.

In the case (c), we obtain

$$u = L^2, \qquad v = 2M^2, \qquad u+v = X^2, \qquad u-v = Y^2,$$

for positive integers L, M, X, Y. The formulas

$$\left(\frac{X+Y}{2}\right)^2 + \left(\frac{X-Y}{2}\right)^2 = u = L^2, \qquad \frac{1}{2}\left(\frac{X+Y}{2}\right)\left(\frac{X-Y}{2}\right) = \frac{v}{4} = 2\left(\frac{M}{2}\right)^2$$

then yields another right triangle with rational sides

$$a_1 = (X+Y)/M, \qquad b_1 = (X-Y)/M, \qquad c_1 = 2L/M$$

and area $a_1 b_1/2 = 2$, which gives rise to a new integral solution (u_1, v_1, w_1) of (3.3.5.1) satisfying $w_1 < w$, leading to a contradiction.

(3.3.6) Analysis of the 2-descent. Let us investigate the division of points by 2 in more detail. Assume that L is a field of characteristic $char(L) \neq 2$ and E an elliptic curve over L such that $E(\overline{L})_2 = E(L)_2$ (i.e. all 2-torsion points are defined over L). This means that E can be given by a Weierstrass equation

$$E : y^2 = g(x) = (x - e_1)(x - e_2)(x - e_3),$$

where $g(x)$ has three distinct roots $e_1, e_2, e_3 \in L$ *contained in* L. Assume that $(x, y) \in E(L) - E(L)_2$. Following the same method as in the proof of 3.3.2, we shall write each of the factors $x - e_j = d_j z_j^2 \in L^*$ as a product of its "square-free part" d_j and a square of $z_j \in L^*$. If the square-free parts d_j are fixed (of course, $d_1 d_2 d_3 = (y/z_1 z_2 z_3)^2 \in L^{*2}$ has to be a square in L), elimination of the variable x gives equations

$$\begin{aligned} d_1 z_1^2 - d_2 z_2^2 &= e_2 - e_1 \\ d_2 z_2^2 - d_3 z_3^2 &= e_3 - e_2 \\ d_3 z_3^2 - d_1 z_1^2 &= e_1 - e_3 \end{aligned} \tag{3.3.6.1}$$

for the values $z_j \in L^*$. In other words, a point $(x, y) \in E(L) - \{O\}$ satisfying $y \neq 0$ defines L-rational points $(\pm z_1, \pm z_2, \pm z_3)$ on the curve (3.3.6.1), for suitable $d_j \in L^*$ satisfying $d_1 d_2 d_3 \in L^{*2}$. Conversely,

any L-rational point (z_1, z_2, z_3) on (3.3.6.1) gives rise to L-rational points $(e_1 + d_1 z_1^2, \pm(d_1 d_2 d_3)^{1/2} z_1 z_2 z_3) \in E(L) - \{O\}$.

More precisely, one needs to work also with points at infinity; passing to the homogeneous coordinates $(Z_0 : Z_1 : Z_2 : Z_3)$ in $\mathbf{P}^3$, consider for each triple $d = (d_1, d_2, d_3) \in (L^*)^{\oplus 3}$ the projectivization C_d of (3.3.6.1), given by

$$\begin{aligned} d_1 Z_1^2 - d_2 Z_2^2 &= (e_2 - e_1) Z_0^2 \\ d_2 Z_2^2 - d_3 Z_3^2 &= (e_3 - e_2) Z_0^2 \\ d_3 Z_3^2 - d_1 Z_1^2 &= (e_1 - e_3) Z_0^2 \end{aligned} \tag{3.3.6.2}$$

(where $z_j = Z_j/Z_0$, $j = 1, 2, 3$). Note that if we replace each d_j by $d'_j = d_j c_j^2$ (for $c_j \in L^*$), then the curve $C_{d'}$ will be isomorphic to C_d (over L); one has to replace Z_j by $c_j Z'_j$ $(j = 1, 2, 3)$.

Put

$$G(L) = \operatorname{Ker}\left(\text{product} : (L^*/L^{*2})^{\oplus 3} \longrightarrow L^*/L^{*2}\right);$$

this is a natural space of parameters for the triples $d = (d_1, d_2, d_3)$. We have just seen that the curve C_d depends (up to isomorphism defined over L) only on the image of d in $G(L)$.

If L is a number field, then, as we shall see in 3.3.10 below, congruence considerations severely restrict the possible values of d for which the curve C_d admits an L-rational point.

(3.3.7) Proposition. *Let $E : y^2 = (x - e_1)(x - e_2)(x - e_3) = g(x)$ be an elliptic curve over a field L, with $e_1, e_2, e_3 \in L$. For each $i = 1, 2, 3$, define a map $f_i : E(L) \longrightarrow L^*$ by*

$$f_i(O) = 1, \qquad f_i((x, y)) = x - e_i \quad (\text{if } x \neq e_i), \qquad f_i((e_i, 0)) = (e_j - e_i)(e_k - e_i) \qquad (\text{if } \{i, j, k\} = \{1, 2, 3\}).$$

Then: (i) *The map $f = (f_1, f_2, f_3) \pmod{(L^{*2})^{\oplus 3}} : E(L) \longrightarrow G(L)$ is a homomorphism of abelian groups.*
(ii) *The kernel of f is equal to $\operatorname{Ker}(f) = 2E(L) = [2]E(L)$.*
(iii) *The image of f consists of those $d = (d_1, d_2, d_3) \in G(L)$ for which $C_d(L) \neq \emptyset$, i.e. for which the curve C_d has an L-rational point.*

Proof. (i) The equation of the curve implies that the image of the map f is indeed contained in $G(L)$. By definition, $f_i(\boxminus P) = f_i(P) = f_i(P)^{-1} \pmod{L^{*2}}$; thus it is enough to check that

$$P \boxplus Q \boxplus R = O \quad \stackrel{?}{\Longrightarrow} \quad f_i(P) f_i(Q) f_i(R) \in L^{*2}$$

in the case when $\{P, Q, R\} \subset E(L)$ (possibly with multiplicities) is the intersection of E with a non-vertical line $y = \ell(x) = ax + b$.

Assume first that $(e_i, 0) \neq P, Q, R$. Then

$$g(x) - \ell(x)^2 = (x - e_1)(x - e_2)(x - e_3) - \ell(x)^2 = (x - x(P))(x - x(Q))(x - x(R));$$

substituting $x = e_i$, we obtain $f_i(P) f_i(Q) f_i(R) = \ell(e_i)^2 \in L^{*2}$.

If $R = (e_i, 0)$, then $\ell(x) = c(x - e_i)$ with $c \in L$, hence

$$\frac{f_i(P) f_i(Q)}{f_i((e_j, 0)) f_i((e_k, 0))} = \frac{(x - x(P))(x - x(Q))}{(x - e_j)(x - e_k)}\bigg|_{x = e_i} = \frac{g(x) - \ell(x)^2}{g(x)}\bigg|_{x = e_i} = 1 - \frac{c^2(x - e_i)}{(x - e_j)(x - e_k)}\bigg|_{x = e_i} = 1,$$

proving (i). As regards (ii), we know from I.7.5.9 (or from II.1.2.1) that

$$f_i(2[P]) = h_i(P)^2 \tag{3.3.7.1}$$

for some rational function on E (possibly defined over an extension of L). However, an explicit calculation shows that (3.3.7.1) holds for

$$h_i(x,y) = \frac{x^2 - 2e_i x - (e_i^2 + e_j e_k)}{2y} = \frac{(x-e_i)(x-e_j) + (e_j - e_i)(x-e_k)}{2y} = \frac{1}{2}\left(\frac{y}{x-e_k} + (e_j - e_i)\frac{x-e_k}{y}\right)$$

(where $\{i,j,k\} = \{1,2,3\}$). As h_i is defined over L, it follows automatically from (i) and (3.3.7.1) that

$$[2]E(L) \subset \mathrm{Ker}(f).$$

In order to prove the converse, assume that $Q = (A,B) \in \mathrm{Ker}(f) \subset E(L)$. If $B \neq 0$, then $A - e_j = h_j^2$ and $B = h_1 h_2 h_3$ for some $h_j \in L^*$ $(j = 1,2,3)$. We would like to find $P = (x,y) \in E(L)$ satisfying $h_j(P) = h_j$ $(j = 1,2,3)$. Put

$$\begin{aligned} C &= h_1h_2 + h_1h_3 + h_2h_3 \\ x &= A + C = (h_i + h_j)(h_i + h_k) + e_i \in L \\ y &= (h_1 + h_2)(h_1 + h_3)(h_2 + h_3) \in L. \end{aligned}$$

Then $y^2 = (x-e_1)(x-e_2)(x-e_3)$, hence $P := (x,y) \in E(L)$, and

$$h_i + h_j = \frac{y}{x - e_k}, \qquad h_i - h_j = \frac{h_i^2 - h_j^2}{h_i + h_j} = (e_j - e_i)\frac{x-e_k}{y},$$

showing that $h_j = h_j(P)$ for all $j = 1,2,3$, hence $(A,B) = (A, h_1h_2h_3) = [2](x, \pm y)$ for a suitable choice of the sign. This proves (ii) (at least if $B \neq 0$; we leave the case $Q = (e_i, 0)$ to the reader). Finally, (iii) follows from the definitions (observing that C_d has an L-rational point with $Z_0 = 0$ (i.e. "at infinity") if and only if $d = (1,1,1) \in G(L)$ is the neutral element of $G(L)$).

(3.3.8) Why f_i? The rational functions $f_i \in R(E)^*$ are characterized (up to a scalar) by their divisors

$$\mathrm{div}(f_i) = 2((e_i,0)) - 2(O), \qquad [2](e_i,0) = O.$$

This gives a hint how to generalize 3.3.7: if $n > 1$ is prime to the characteristic of L and $E(L)_n = E(\overline{L})_n$, choose a basis T_1, T_2 of $E(L)_n = (\mathbf{Z}/n\mathbf{Z}) \cdot T_1 + (\mathbf{Z}/n\mathbf{Z}) \cdot T_2$. For each $i = 1,2$ there exist rational functions $f_i, h_i \in R(E)^*$ (unique up to scalar multiples) satisfying

$$\mathrm{div}(f_i) = n(T_i) - n(O), \qquad f_i([n]P) = h_i(P)^n.$$

Defining suitably the values of f_i at T_i and O, one obtains a map

$$f = (f_1, f_2) : E(L) \longrightarrow (L^*/L^{*n})^{\oplus 2},$$

which turns out to be a homomorphism with kernel $\mathrm{Ker}(f) = [n]E(L)$. We leave the details as an exercise to the reader (who will have to rediscover the Weil pairing in the process)!

(3.3.9) Theorem ("Weak Mordell-Weil theorem"). *Let $E : y^2 = (x-e_1)(x-e_2)(x-e_3)$ be an elliptic curve over a number field K, with $e_1, e_2, e_3 \in K$. Then $E(K)/2E(K)$ is finite.*

Proof. We are going to apply 3.3.6 for $L = K$ and all the completions $L = K_v$ of K $(v \in M_K)$. For each v the inclusion $K \subset K_v$ induces a commutative diagram

$$\begin{array}{ccc} f : E(K)/2E(K) & \xrightarrow{\sim} & \{d \in G(K) \mid C_d(K) \neq \emptyset\} \\ \downarrow & & \downarrow loc_v \\ f_v : E(K_v)/2E(K_v) & \xrightarrow{\sim} & \{d_v \in G(K_v) \mid C_{d_v}(K_v) \neq \emptyset\}. \end{array}$$

We define the **Selmer group** for the 2-descent on E (over K) by

$$S(E/K,2) = \{d \in G(K) \mid (\forall v \in M_K) \quad loc_v(d) \in \mathrm{Im}(f_v)\} = \{d \in G(K) \mid (\forall v \in M_K) \quad C_d(K_v) \neq \emptyset\}.$$

What does this mean? The isomorphism f is not particularly useful, as we do not know how to decide, in general, whether or not a given curve C_d admits a K-rational point. Replacing $E(K)/2E(K)$ by the Selmer group simply means that, instead of testing solvability of the equations (3.3.6.2) in $Z_j \in \mathcal{O}_K$, we test solvability of the corresponding congruences modulo all ideals of $\mathcal{O}_K$.

By definition, $E(K)/2E(K) \subseteq S(E/K,2)$, so it is enough to prove the finiteness of $S(E/K,2)$. Put

$$S = \{v \in M_K^f \,|\, (\forall i < j) \quad \mathrm{ord}_v(e_i - e_j) \neq 0\},$$
$$K(S,2) = \{c \in K^*/K^{*2} \,|\, (\forall v \in M_K^f - S) \quad \mathrm{ord}_v(c) \equiv 0 \pmod 2\}.$$

(3.3.10) Lemma. *If $d = (d_1, d_2, d_3) \in S(E/K,2)$, then $d_j \in K(S,2)$ $(j = 1,2,3)$.*

Proof. Let $v \in M_K^f - S$; assume that there exists $P \in C_d(K_v)$. If $P \in \{Z_0 = 0\}$ lies at infinity, then $d_j \in K_v^{*2}$ for all $j = 1,2,3$, hence $\mathrm{ord}_v(d_j) \equiv 0 \pmod 2$. So we can assume that $P = (z_1, z_2, z_3) \in C_d(K_v)$ is not at infinity, with its affine coordinates z_j satisfying 3.3.6.1. By assumption, $\mathrm{ord}_v(e_i - e_j) = 0$ for all $i < j$. Put $n_j = \mathrm{ord}_v(d_j z_j^2) \equiv \mathrm{ord}_v(d_j) \pmod 2$; then $n_1 + n_2 + n_3 \equiv 0 \pmod 2$, and we must show that all n_i are even. If $n_i < 0$ for some i, then $n_1 = n_2 = n_3$, hence $n_i \equiv 0 \pmod 2$ for all i. If $n_i > 0$ for some i, then $n_j = n_k = 0$ for the remaining two, hence $n_i \equiv 0 \pmod 2$. Lemma is proved.

(3.3.11) Corollary. *The map $(d_1, d_2, d_3) \mapsto (d_1, d_2)$ induces an injective homomorphism $S(E/K,2) \hookrightarrow K(S,2) \oplus K(S,2)$.*

End of Proof of Theorem 3.3.9. In view of 3.3.11, it is enough to show:

(3.3.12) Lemma. *For every finite subset $S \subset M_K^f$, $K(S,2)$ is finite.*

Proof. Denote by $\mathcal{O}_{K,S} = \mathcal{O}_K[1/S]$ the ring of S-integers in K and by $Cl(\mathcal{O}_{K,S})$ its group of classes of ideals. Then the homomorphism

$$K(S,2) \longrightarrow Cl(\mathcal{O}_{K,S}), \qquad c \pmod{K^{*2}} \mapsto \sum_{v \notin S} \left(\tfrac{1}{2}\mathrm{ord}_v(c)\right) \cdot v$$

sits in an exact sequence

$$0 \longrightarrow \mathcal{O}_{K,S}^*/\mathcal{O}_{K,S}^{*2} \longrightarrow K(S,2) \longrightarrow Cl(\mathcal{O}_{K,S})_2.$$

Dirichlet's unit theorem implies that $\mathcal{O}_{K,S}^*$ is a finitely generated abelian group, hence $\mathcal{O}_{K,S}^*/\mathcal{O}_{K,S}^{*2}$ is finite. The group $Cl(\mathcal{O}_{K,S})$ is finite, being a quotient of $Cl(\mathcal{O}_K)$. Lemma follows.

(3.3.13) Note that the proof of 3.3.9 gives an explicit upper bound for the number of generators of $E(K)/2E(K)$ (see [Si 1], X.1 for an example of explicit calculations). In fact, one can effectively compute the Selmer group $S(E/K,2)$ (not only in theory, but also in practice).

(3.3.14) Exercise. *Let E be an elliptic curve over a field L, L'/L a finite Galois extension and $n > 1$. Then the group* $\mathrm{Ker}(E(L)/nE(L) \longrightarrow E(L')/nE(L'))$ *is finite.*

(3.3.15) Corollary. *Let E be an elliptic curve over a number field K. Then $E(K)/2E(K)$ is finite.*

(3.3.16) Exercise ([Ca 1], [Se]). *Let L be a field of characteristic $char(L) \neq 3$ containing a primitive cubic root of unity ρ (i.e. $\rho^3 = 1 \neq \rho$). For $A \in L^*$, consider the elliptic curve $E_A : X^3 + Y^3 = AZ^3$ (with $O = (1 : -1 : 0)$).*
(i) *Show that the map*

$$(x,y) \mapsto \left(\frac{x+y}{\rho - \rho^2}, \frac{\rho x + \rho^2 y}{\rho - \rho^2}, \frac{\rho^2 x + \rho y}{\rho - \rho^2}\right)$$

(where $x = X/Z, y = Y/Z$) induces an injective homomorphism of groups

$$f : E_A(L)/(\rho - \rho^2)E_A(L) \hookrightarrow (L^*/L^{*3})^{\oplus 3}.$$

(ii) *The image of f consists of those triples (a,b,c) with $abc = A \in L^*/L^{*3}$ for which the projective curve $aX^3 + bY^3 + cZ^3 = 0$ has a L-rational point.*
(iii) *If $L = K$ is a number field, give an upper bound for $\mathrm{Im}(f)$ in the spirit of 3.3.11.*
(iv) *Show that $E_1(\mathbf{Q}(\sqrt{-3})) = \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$.*

(3.3.17) Exercise. *Let L be a field of characteristic $char(L) \neq 2$ and*

$$E : y^2 = x^3 + ax^2 + bx + c, \qquad E_D : Dy^2 = x^3 + ax^2 + bx + c$$

elliptic curves (with $a, b, c, D \in L$). If $D \notin L^{*2}$ is not a square in L, show that there is a natural exact sequence

$$0 \longrightarrow E(L) \longrightarrow E(L(\sqrt{D})) \longrightarrow E_D(L) \longrightarrow S \longrightarrow 0,$$

where $2 \cdot S = 0$.

(3.3.18) Exercise. *Let L be a field of characteristic $char(L) \neq 3$ containing a primitive cubic root of unity. For $A, D \in L^*$, consider the elliptic curves*

$$E : X^3 + Y^3 = AZ^3, \qquad E_D : X^3 + Y^3 = ADZ^3, \qquad E_{D^2} : X^3 + Y^3 = AD^2Z^3.$$

If $D \notin L^{*3}$ is not a cube in L, relate the groups $E(L), E_D(L), E_{D^2}(L)$ and $E(L(\sqrt[3]{D}))$.

(3.3.19) Exercise. *If $D \equiv 3 \pmod 8$ is a prime number, show that D is not a conguent number and that, in the notation of 3.3.1, $S(E_D/\mathbf{Q}, 2) = E_D(\mathbf{Q})_{tors}/2E_D(\mathbf{Q})_{tors} \xrightarrow{\sim} (\mathbf{Z}/2\mathbf{Z})^2$.*

(3.3.20) Higher descent. Let E be an elliptic curve over a number field K and $n > 1$ an integer. It is possible to define an auxilliary family of smooth projective curves C_α over K that generalizes the family C_d from (3.3.6.2). The parameter α is contained in a certain abelian group generalizing $G(K)$ from 3.3.6 and there is a natural isomorphism

$$E(K)/nE(K) \xrightarrow{\sim} \{\alpha \,|\, C_\alpha(K) \neq \emptyset\}.$$

The Selmer group for the n-descent is defined in the same way as for $n = 2$:

$$S(E/K, n) \xrightarrow{\sim} \{\alpha \,|\, (\forall v \in M_K) \quad C_\alpha(K_v) \neq \emptyset\}.$$

$S(E/K, n)$ is finite abelian group of exponent n; its number of generators can be bounded above in terms of the unit group and the ideal class group of the field generated over K by the coordinates of all points from $E(\overline{K})_n$ (in analogy to 3.3.10-12). The Selmer group $S(E/K, n)$ is effectively computable, at least in theory, and for small values of n even in practice.

In order to determine the rank r of $E(K)$, one would need to know more about the difference between the Selmer group and $E(K)/nE(K)$. The quotient group $S(E/K, n)/(E(K)/nE(K))$ is equal to $Ш(E/K)_n$, the group of elements of order n in the so-called Tate-Šafarevič group of E. Unfortunately, this group is very difficult to control, although $Ш(E/K)$ is conjectured to be always finite.

3.4 Heights

Roughly speaking, the height measures the size of a rational point on an elliptic curve by counting the number of digits necessary to write down the coordinates of the point (or perhaps just its x-coordinate).

If one makes a numerical experiments and calculates the coordinates of the multiples $[n]P$ of a (non-torsion) rational point P, a parabolic shape appears: the number of digits necessary to write $[n]P$ grows quadratically with n. This quadratic behaviour is the second ingredient used in the proof of the Mordell-Weil Theorem.

(3.4.1) Heights on a projective space (over Q). Consider the n-dimensional projective space $\mathbf{P}^n_{\mathbf{Q}}$ over $\mathbf{Q}$ with a fixed homogeneous coordinate system. Given a rational point $x \in \mathbf{P}^n(\mathbf{Q})$, we can write $x = (x_0 : \cdots : x_n)$, with $x_j \in \mathbf{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$. This determines the values of the homogeneous

coordinates x_j up to a common factor in $\{\pm 1\}$. One defines the **height** of x (in fact, two heights: the "logarithmic height" h will be more useful) by

$$H(x) = \max(|x_0|, \dots, |x_n|) \geq 1$$
$$h(x) = \log(H(x)) \geq 0.$$

In particular, a rational number $x = a/b$ (for $a, b \in \mathbf{Z}$, $\gcd(a,b) = 1$) is naturally a point of $\mathbf{P}^1(\mathbf{Q})$; its height will then be equal to

$$h\left(\frac{a}{b}\right) = \log(\max(|a|, |b|)).$$

(3.4.2) Heights on a projective space (over $\overline{\mathbf{Q}}$). If one works over a number field, one needs to use the *normalized valuations* on K, which are defined as follows (for $v \in M_K$):

$$\|x\|_v = \begin{cases} (Nv)^{-\mathrm{ord}_v(x)}, & v \in M_K^f \\ |x|^{[K_v:\mathbf{R}]}, & v|\infty, \end{cases}$$

where $Nv = \#k(v)$. The normalized valuations satisfy the product formula

$$(\forall x \in K^*) \qquad \prod_{v \in M_K} \|x\|_v = 1.$$

For $x \in \mathbf{P}^n(K)$, we choose any homogeneous coordinates $x = (x_0 : \cdots : x_n)$ of x ($x_j \in K$) and put

$$H_K(x) = \prod_{v \in M_K} \max(\|x_0\|_v, \dots, \|x_n\|_v) \geq 1,$$

which is a finite product, independent of the choice of the homogeneous coordinates (thanks to the product formula). The quantities

$$H(x) = H_K(x)^{1/[K:\mathbf{Q}]}, \qquad h(x) = \log(H(x)) \geq 0$$

are then independent on the number field K; they define a function

$$h : \mathbf{P}^n(\overline{\mathbf{Q}}) \longrightarrow \mathbf{R}_{\geq 0},$$

which depends only on the fixed coordinate system in $\mathbf{P}^n$ (and which coincides on $\mathbf{P}^n(\mathbf{Q})$ with the height defined in 3.4.1).

(3.4.3) Proposition-Definition. (i) *Two real valued functions $f, f' : S \longrightarrow \mathbf{R}$ on a set S are* **equivalent** *(notation: $f \sim f'$) if the function $|f(x) - f'(x)|$ is bounded on S.*
(ii) *If $h' : \mathbf{P}^n(\overline{\mathbf{Q}}) \longrightarrow \mathbf{R}_{\geq 0}$ is the height defined by another system of homogeneous coordinates, then $h' \sim h$.*

Proof (Sketch). The change of coordinates is given by a matrix $g \in GL_{n+1}(K)$; for every $v \in M_K^f$,

$$\max_i(\|\sum_j g_{ij} x_j\|_v) \leq (\max_{i,j} \|g_{ij}\|_v) \max_j \|x_j\|_v = C_v(g) \max_j \|x_j\|_v,$$

where $C_v(g) = 1$ for all but finitely many v; similar bounds exist for $v|\infty$ (see [Si 1], VIII.5.8 for more details).

(3.4.4) Proposition. *For every $C, D > 0$, the set*

$$\{x \in \mathbf{P}^n(\overline{\mathbf{Q}}) \,|\, h(x) \leq C,\ [k(x) : \mathbf{Q}] \leq D\}$$

is finite (where $k(x)$ denotes the field of definition of x).

Proof. It is enough to consider the points x of a fixed degree $[k(x) : \mathbf{Q}] = d$. If $d = 1$, then the statement follows from the definition of the height given in 3.4.1. The general case can be reduced to the case $d = 1$ as follows: consider the map

$$f : \{x \in \mathbf{P}^n(\overline{\mathbf{Q}}) \mid [k(x) : \mathbf{Q}] = d\} \longrightarrow \{y \in \mathbf{P}^N(\mathbf{Q})\}$$

defined by sending $x = (x_0 : \cdots : x_n)$ to the coefficients $y = (y_0 : \cdots : y_N)$ of the norm form

$$N_{k(x)/\mathbf{Q}}(x_0T_0 + \cdots + x_nT_n) = \sum_\alpha y_\alpha T^\alpha$$

(where α is a multi-index). The map f has finite fibres (more precisely, $\#f^{-1}(y) \leq d$ for each y) and

$$h(f(x)) \leq dh(x) + c(n, d),$$

where $c(n, d)$ is a constant depending only on n, d (see [Si 1], VIII.5.11).

(3.4.5) Heights on elliptic curves. Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over a number field K. Then the x-coordinate defines a morphism $x : E \longrightarrow \mathbf{P}^1_K$ of degree 2. We fix a coordinate system on $\mathbf{P}^1$ and define

$$\begin{aligned} h_x : E(\overline{K}) &\longrightarrow \mathbf{R}_{\geq 0} \\ P &\mapsto h(x(P)). \end{aligned}$$

This function is even, i.e. satisfies $h_x(\boxminus P) = h_x(P)$.

(3.4.6) Theorem (Quadraticity of the height). *The function h_x is* **almost quadratic** *in the sense that the function*

$$\begin{gathered} \mathrm{Cube}(h_x) : (E \times E \times E)(\overline{K}) \longrightarrow \mathbf{R} \\ (P, Q, R) \mapsto h_x(P \boxplus Q \boxplus R) - h_x(P \boxplus Q) - h_x(P \boxplus R) - h_x(Q \boxplus R) + h_x(P) + h_x(Q) + h_x(R) \end{gathered}$$

is bounded, i.e. $\mathrm{Cube}(h_x) \sim 0$.

(3.4.7) In the lectures, Theorem 3.4.6 was related to the "Theorem of the cube". An elementary proof can be found in [Si 1], VIII.6.2 (+ 9.3).

(3.4.8) Corollary. (i) *(Tate) For each point $P \in E(\overline{K})$, the limit*

$$\widehat{h}(P) = \frac{1}{2} \lim_{N \longrightarrow \infty} \frac{h_x([m^N]P)}{m^{2N}} \geq 0$$

exists and does not depend on the choice of $m \geq 2$ ($\widehat{h}$ is the **canonical height** *= the* **Néron-Tate height***).*
(ii) $\widehat{h} \sim \frac{1}{2}h_x, \quad \widehat{h}(\boxminus P) = \widehat{h}(P)$.
(iii) $\mathrm{Cube}(\widehat{h}) = 0$, *i.e. $\widehat{h}$ is quadratic.*
(iv) $\langle P, Q\rangle := \frac{1}{2}(\widehat{h}(P \boxplus Q) - \widehat{h}(P) - \widehat{h}(Q))$ *is a bilinear symmetric form*

$$\langle\ ,\ \rangle : E(\overline{K}) \times E(\overline{K}) \longrightarrow \mathbf{R}$$

satisfying $\langle P, P\rangle \geq 0$ for all $P \in E(\overline{K})$.
(v) *A point $P \in E(\overline{K})$ satisfies $\langle P, P\rangle = 0$ if and only if $P \in E(\overline{K})_{tors}$.*

Proof . This is an easy consequence of 3.4.6; see [Si 1], VIII.9.1-3 for more details.

(3.4.9) Corollary (Weak properties of the height). (i) *For every $P_0 \in E(K)$ there is a constant $C_1 = C_1(E, K, P_0)$ such that*

$$(\forall P \in E(K)) \quad h_x(P \boxplus P_0) \leq 2h_x(P) + C_1.$$

(ii) *There is a constant $C_2 = C_2(E, K)$ such that*

$$(\forall P \in E(K)) \quad h_x([2]P) \geq 4h_x(P) - C_2.$$

(iii) *For every $C > 0$, the set $\{P \in E(K) \,|\, h_x(P) < C\}$ is finite.*

(3.4.10) What really matters in 3.4.9 is the fact that $4 > 2$ (and the finiteness result 3.4.4, which implies (iii)). For $K = \mathbf{Q}$, the properties (i), (ii) can be established by an explicit calculation, without any elaborate machinery ([Si 1], VIII.4.2).

(3.4.11) Proof of the Mordell-Weil Theorem. Let K be a number field and $E : y^2 = x^3 + Ax + B$ an elliptic curve over K. We want to prove that $E(K)$ is finitely generated. Extending K, we can assume that the roots of the cubic polynomial $x^3 + Ax + B$ are all contained in K; Theorem 3.3.9 then implies that $E(K)/2E(K)$ is finite (in fact, it was not necessary to extend K; cf. 3.3.14-15). This finiteness result, combined with 3.4.9(i)–(iii), is all one needs to prove that $E(K)$ is finitely generated:

Fix representatives $Q_1, \ldots, Q_m \in E(K)$ of all classes in $E(K)/2E(K)$. For every $P \in E(K)$ there exists a sequence $P_j \in E(K)$ of K-rational points obtained by "division by 2 with remainder":

$$P = P_0 = [2]P_1 \boxplus Q_{i_1}, \qquad P_1 = [2]P_2 \boxplus Q_{i_2}, \qquad P_2 = [2]P_3 \boxplus Q_{i_3} \qquad \text{etc.}$$

It follows that, for each $j \geq 1$,

$$h_x(P_j) \leq \frac{h_x([2]P_j) + C_2}{4} = \frac{(P_{j-1} \boxminus Q_{i_j}) + C_2}{4} \leq \frac{2h_x(P_{j-1}) + C_1 + C_2}{4} = \frac{1}{2}\, h_x(P_{j-1}) + \frac{C_1 + C_2}{4},$$

where $C_1 = \max C_1(Q_i)$. By induction, we obtain

$$h_x(P_j) \leq \frac{1}{2^j}\, h_x(P) + \left(1 + \frac{1}{2} + \cdots + \frac{1}{2^{j-1}}\right) \frac{C_1 + C_2}{4} < \frac{1}{2^j}\, h_x(P) + \frac{C_1 + C_2}{2}.$$

This implies that, for each $P \in E(K)$, there exists j such that

$$h_x(P_j) \leq 1 + \frac{C_1 + C_2}{2},$$

which proves that $E(K)$ is generated by the finite set

$$\{Q_1, \ldots, Q_m\} \cup \{R \in E(K) \,|\, h_x(R) \leq 1 + (C_1 + C_2)/2\}.$$

Theorem 3.3.4 is proved.

3.5 The Conjecture of the Birch and Swinnerton-Dyer

None of the existing proofs of the Mordell-Weil theorem are effective; they yield an upper bound on the rank $r = r(E/K)$ of the group $E(K) \xrightarrow{\sim} E(K)_{tors} \times \mathbf{Z}^r$, but not the true value of r nor a bound on the heights of a set of generators of $E(K)$.

(3.5.1) Numerical experiments involving a large number of elliptic curves over $\mathbf{Q}$ lead Birch and Swinnerton-Dyer [B-SD] to conjecture that the rank $r = r(E/K)$ can be read off from the asymptotic of the product

$$\prod_{Nv \leq x} \frac{\#\widetilde{E}_v(k(v))}{Nv} \sim c(\log x)^r. \tag{3.5.1.1}$$

At least formally, the asymptotic behaviour of the L.H.S. can be reformulated in terms of the L-function of E (over K), which is defined as the infinite product over all finite primes of K

$$L(E/K, s) = \prod_v L_v(E/K, s) = \prod_v \left[(1 - \alpha_v(Nv)^{-s})(1 - \beta_v(Nv)^{-s})\right]^{-1}, \tag{3.5.1.2}$$

where

$$\beta_v = \overline{\alpha}_v, \qquad \#\widetilde{E}_v(k(v)) = (1 - \alpha_v)(1 - \beta_v)$$

if E has good reduction at v, resp.

$$\beta_v = 0, \qquad \alpha_v = \begin{cases} 0, & \text{if } E \text{ has additive reduction at } v \\ 1, & \text{if } E \text{ has split multiplicative reduction at } v \\ -1, & \text{if } E \text{ has non-split multiplicative reduction at } v. \end{cases}$$

Hasse's Theorem 1.3.2 tells us that $|\alpha_v| = |\beta_v| = (Nv)^{1/2}$ for all primes of good reduction, which implies that the infinite product (3.5.1.2) is uniformly convergent and defines a holomorphic function in the region $Re(s) > 3/2$. The L-function $L(E/K, s)$ conjecturally admits holomorphic continuation to $\mathbf{C}$ and a functional equation with respect to the change of variables $s \longleftrightarrow 2 - s$. As

$$L_v(E/K, 1)^{-1} = \frac{\#\widetilde{E}_v^{sm}(k(v))}{Nv}$$

for all v, the asymptotics (3.5.1.1) can be formally replaced by

$$L(E/K, s) \sim C(s-1)^r \qquad\qquad (s \longrightarrow 1),$$

i.e. by a conjectural equality between the *analytic rank* of E over K and the rank $r(E/K)$:

$$(BSD) \qquad\qquad r_{an}(E/K) := \mathrm{ord}_{s=1} L(E/K, s) \stackrel{?}{=} r(E/K).$$

This is a weak version of the Conjecture of Birch and Swinnerton-Dyer. The strong version also predicts the value of the constant C, which involves, among others, the order of the Tate-Šafarevič group of E. In the words of Birch and Swinnerton-Dyer, the conjecture relates the behaviour of the L-function $L(E/K, s)$ at a point at which it is not known to be defined to the order of a group not known to be finite.

(3.5.2) What is known in the direction of this conjecture? For simplicity, we confine ourselves to elliptic curves defined over $K = \mathbf{Q}$.

(1) If E has complex multiplication, then there is an explicit formula for $L(E/\mathbf{Q}, s)$ (proved by Deuring), which implies the analytic continuation and functional equation. For example, it follows from Eisenstein's result I.9.4.6 that the L-function of the curve $E - \{O\} : v^2 = u^3 - u$ (which is related to the congruent number problem for $D = 1$ treated in 3.3.2) is given by the formula from 1.4.7(3):

$$L(E_D/\mathbf{Q}, s) = \prod_{\pi} (1 - \pi|\pi|^{-2s})^{-1} = \sum_{\alpha \equiv 1 \pmod{2+2i}} \frac{\alpha}{|\alpha|^{2s}}.$$

A similar explicit formula holds for all curves $E_D : v^2 = u^3 - Du$ (cf. 1.2.3(2b)). In fact, it was these curves that served as guinea pigs for testing the conjecture (see [B-SD]). For curves E_{D^2}, which are related to the general congruent number problem, an explicit formula for $L(E_{D^2}/\mathbf{Q}, 1)$ is given in [Tu].

(2) If E has complex multiplication and $L(E/\mathbf{Q}, 1) \neq 0$, then $E(\mathbf{Q})$ is finite (Coates-Wiles [Co-Wi]).

(3) In general, any elliptic curve over $\mathbf{Q}$ is modular, thanks to the pioneering work of Wiles, Taylor-Wiles (and their followers [BCDT]); this again implies the analytic continuation and functional equation for $L(E/\mathbf{Q}, s)$.

(4) If $r_{an}(E/\mathbf{Q}) \leq 1$, then the conjecture (BSD) holds and the group Ш$(E/\mathbf{Q})$ is finite; in fact, the strong version of the conjecture (BSD) holds, up to a controlled rational factor (Kolyvagin [Ko], combined with results of Gross-Zagier [Gr-Za] and others).

(5) If E does not have additive reduction at p, then one can define a p-adic L-function $L_p(E, s)$. Kato [Ka] (see also [Col]) showed that

$$r(E/\mathbf{Q}) \leq \mathrm{ord}_{s=1} L_p(E, s).$$

(6) If E has good ordinary reduction at a prime p and if the p-primary component of Ш$(E/\mathbf{Q})$ is finite, then (see [Ne])

$$r(E/\mathbf{Q}) \equiv r_{an}(E/\mathbf{Q}) \pmod 2.$$

(THIS IS VERSION 5/2/2004)

References

[Al-Kl] A.Altman, S.Kleiman, *Introduction to Grothendieck duality theory*, Lecture Notes in Mathematics **146**, Springer, 1970.

[Be] D. Bernardi, private communication.

[B-SD] B.J. Birch, H.P.F. Swinnerton-Dyer , *Notes on Elliptic Curves. II*, J. reine und angew. Math. **218** (1965), 79–108.

[BCDT] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.

[Ca 1] J.W.S. Cassels, *Lectures on Elliptic Curves*, London Math. Society Student Texts **24**, Cambridge Univ. Press, 1991.

[Ca 2] J.W.S. Cassels, *Arithmetic on curves of genus* 1*. I. On a conjecture of Selmer*, J. Reine Angew. Math. **202** (1959), 52–99.

[Ca 3] J.W.S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291.

[Cl] C.H. Clemens, *A Scrapbook of Complex Curve Theory*, Plenum Press, 1980.

[Co-Wi] J. Coates, A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), 223–251.

[Col] P. Colmez, *La Conjecture de Birch et Swinnerton-Dyer p-adique*, Séminaire Bourbaki, Exp. 919, juin 2003.

[Ei] D. Eisenbud, *Commutative Algebra (with a view toward algebraic geometry)*, Graduate Texts in Mathematics **150**, Springer, 1995.

[Fa-Kr 1] H.M. Farkas, I. Kra, *Riemann surfaces*, Graduate Texts in Mathematics **71**, Springer, 1992.

[Fa-Kr 2] H.M. Farkas, I. Kra, *Theta constants, Riemann surfaces and the modular group*, Graduate Studies in Mathematics **37**, American Math. Society, 2001.

[Fo] O. Forster, *Lectures on Riemann surfaces*, Graduate Texts in Mathematics **81**, Springer, 1991.

[Gr-Ha] P. Griffiths, J. Harris, *Principles of algebraic geometry*, Wiley-Interscience, 1978.

[Gr-Za] B.H. Gross, D. Zagier *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225–320.

[Hu] D. Husemöller, *Elliptic Curves*, Graduate Texts in Mathematics **111**, Springer, 1987.

[Ir-Ro] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics **84**, Springer, 1982

[Ka] K. Kato, *P-adic Hodge theory and values of zeta functions of modular forms*, preprint, 2000.

[Ki] F. Kirwan, *Complex algebraic curves*, London Math. Society Student Texts **23**, Cambridge Univ. Press, 1992.

[Ko] V.A. Kolyvagin, *Euler systems*, in: The Grothendieck Festschrift, Vol. II, Progress in Math. **87** , Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.

[La] S. Lang, *Elliptic functions*, Graduate Texts in Mathematics **112**, Springer, 1987.

[Mar] A.I. Markushevich, *Introduction to the classical theory of abelian functions*, Translations of Mathematical Monographs **96**, American Math. Society, 1992.

[Mat] H. Matsumura, *Commutative ring theory*, Cambridge Univ. Press, 1986.

[McK-Mo] H. McKean, V. Moll, *Elliptic curves*, Cambridge Univ. Press, 1997.

[Mi] J. Milne, *Elliptic curves*, lecture notes, `http://www.jmilne.org/math/`.

[Mu AV] D. Mumford, *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5; Oxford Univ. Press, 1970.

[Mu TH] D. Mumford, *Tata lectures on theta. I,II,III*, Progress in Mathematics **28**, **43**, **97**, Birkhäuser, 1983, 1984, 1991.

[MK] V.K. Murty, *Introduction to abelian varieties*, CRM Monograph Series **3**, American Math. Society, 1993.

[Ne] J. Nekovář, *On the parity of ranks of Selmer groups II*, C.R.A.S. Paris Sér. I Math. **332** (2001), no. 2, 99–104.

[Re] M. Reid, *Undergraduate Algebraic Geometry*, London Math. Society Student Texts **12**, Cambridge Univ. Press, 1988.

[Ru 1] W. Rudin, *Principles of mathematical analysis*, McGraw-Hill, 1976.

[Ru 2] W. Rudin, *Real and complex analysis*, McGraw-Hill, 1987.

[Sc] N. Schappacher, *Some milestones of lemniscatomy*, in: Algebraic geometry (Ankara, 1995), Lect. Notes in Pure and Appl. Math. **193**, Dekker, New York, 1997, pp. 257–290.

[Se] E.S. Selmer, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85** (1951), 203–362.

[Si 1] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, 1986.

[Si 2] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, 1994.

[Si-Ta] J.H. Silverman, J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer, 1992.

[Tu] J.B. Tunnell, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. Math. **72** (1983), 323–334.

[Web] H. Weber, *Lehrbuch der Algebra. III*, 1908.

[Wei 1] A. Weil, *Introduction à l'étude des variétés kähleriennes*, Hermann, 1958.

[Wei 2] A. Weil, *Elliptic functions according to Eisenstein and Kronecker*, Ergebnisse der Mathematik und ihrer Grenzgebiete **88**, Springer, 1976.