Contents

1 Elliptic Curves, the Finiteness Theorem of SHAFAREVIČ

1.1 Elliptic Curves over $\mathbb{C}$

Instead of the introduction we remember to an arithmetic-geometric part of the theory of elliptic curves. Let $\wedge$ be a *lattice in* $\mathbb{C}$, that means a discrete additive subgroup of ($\mathbb{Z}$)-rank 2. Two lattices $\wedge$ and $\wedge'$ in $\mathbb{C}$ are said to be *equivalent,* if there is a complex number $\alpha \neq 0$ such that $\wedge' = \alpha\wedge$. Each of our lattices is equivalent to a lattice $\wedge_\tau = \mathbb{Z} + \mathbb{Z}\tau$ with

$$\tau \in \mathbb{H} = \{z \in \mathbb{C}; \operatorname{Im} z > 0\} \ .$$

$\mathbb{H}$ is called the *POINCARÉ upper half plane.* The quotient spaces

$$E_\wedge = \mathbb{C}/\wedge \ , \quad E_\tau = \mathbb{C}/\wedge_\tau$$

are one-dimensional complex tori, that means complete RIEMANN surfaces with abelian group structures. For equivalent lattices $\wedge, \wedge'$ we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \wedge & \longrightarrow & \mathbb{C} & \longrightarrow & E & \longrightarrow & 0 \\ & & \downarrow\wr & & \downarrow\| & & \downarrow\wr & & \\ 0 & \longrightarrow & \wedge' & \longrightarrow & \mathbb{C} & \longrightarrow & E' & \longrightarrow & 0 \end{array}$$

with obvious notations. The tori E, E' are isomorphic. So each $E = E_\wedge$ is isomorphic to a complex torus E_τ for a suitable $\tau \in \mathbb{H}$.

Each torus E has a smooth complex projective algebraic structure. More precisely, it can be analytically embedded into the complex projective plane $\mathbb{P}^2(\mathbb{C})$. A torus together with such an embedding is called an *elliptic curve over* $\mathbb{C}$*).* For the embeddings we need elliptic functions on $\mathbb{C}$. A meromorphic function on $\mathbb{C}$ is called *elliptic,* if it is $\wedge$-periodic for a suitable $\mathbb{C}$-lattice $\wedge$.

A central role among the elliptic functions play the *WEIERSTRASS* $\wp$*-functions.* For a fixed lattice $\wedge$ it is defined as

$$\begin{aligned} \wp_\wedge &: \mathbb{C} \longrightarrow \mathbb{P}^1(\mathbb{C}) \ , \\ \wp_\wedge(z) = 1/z^2 &+ \sum_{\omega\in\wedge^*} \left(1/(z-\omega)^2 - 1/\omega^2\right) \ , \end{aligned}$$

where $\wedge^* = \wedge\backslash 0$. The field of meromorphic function of $E_\wedge$ is generated by $\wp_\wedge$ and $\wp'_\wedge$. Both functions are related by a simple algebraic equation producing a differential equation for $\wp_\wedge$:

$$\wp'_\wedge(z)^2 = 4\wp_\wedge(z)^3 - g_2(\wedge)\wp_\wedge(z) - g_3(\wedge) \ ,$$

where

$$g_2(\wedge) = 60 \sum_{\omega\in\wedge^*} 1/\omega^4 \ , \quad g_3(\wedge) = 140 \sum_{\omega\in\wedge^*} 1/\omega^b \ .$$

On this way we get a projective embedding

$$\begin{aligned} h : \mathbb{C}/\wedge \quad &\hookrightarrow \quad \mathbb{P}^2(\mathbb{C}) \\ z \bmod \wedge \quad &\longmapsto \quad (1 : \wp(z) : \wp'(z)) \quad (z \notin \wedge) \end{aligned}$$

Using projective coordinates $(w : x : y)$ the image curve $= E(\wedge)$ is defined by the following equation:

$$E : WY^2 = 4X^3 - g_2(\wedge)W^2X - g_3(\wedge)W^3 \tag{1.1}$$

Conversely, if E is a smooth projective curve of degree 3, then there is a projectively equivalent curve E' of equation type

$$E' : WY^2 = 4X^3 - g_2W^2X - g_3W^3 \ . \tag{1.2}$$

The equation in (1.2) or the corresponding cubic form is called a *WEIERSTRASS normal form* of E. Moreover, there is a $\mathbb{C}$-lattice $\wedge$ such that $g_2 = g_2(\wedge)$, $g_3 = g_3(\wedge)$. So we get in any case a *uniformization* $\mathbb{C} \to \mathbb{C}/\wedge \xrightarrow{\sim} E$.

We want to introduce and to explain now the *moduli space of elliptic curves.*

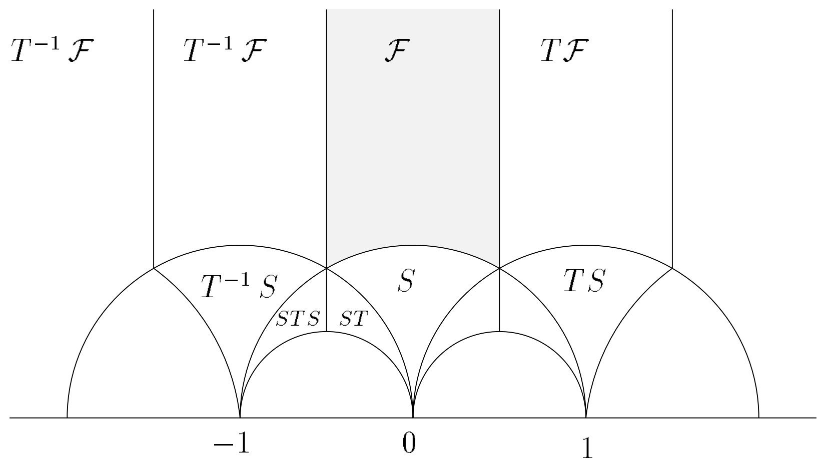
POINCARÉ's upper half plane $\mathbb{H}$ is the simplest non-euclidean model of a homogeneous (symmetric) space. On $\mathbb{H}$ acts transitively the real special linear group $\mathbb{S}l(2,\mathbb{R})$ via fractional linear transformations

$$\tau \mapsto (a\tau + b)/(c\tau + d) \ , \quad \tau \in \mathbb{H} \ , \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{S}l(2,\mathbb{R}) \ .$$

The quotient space $\mathbb{S}l(2,\mathbb{Z})\backslash\mathbb{H}$ has a natural complex structure. It is isomorphic to the affine complex line $\mathbf{A}^1(\mathbb{C}) = \mathbb{C}$. Its natural (smooth) compactification is the projective complex line $\mathbb{P}^1(\mathbb{C})$.

This can be made visible by decomposing $\mathbb{H}$ into infinitely many $\mathbb{S}l(2,\mathbb{Z})$-fundamental domains as it has been first done by GAUSS. The elements $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ generate the unimodular group $\mathbb{S}l(2,\mathbb{Z})$. There is a nice central fundamental domain $\mathcal{F}$ as drawn in the figure (1.3). By identification of equivalent boundary points one gets $\mathbf{A}^1(\mathbb{C})$ and the compactification by addition of the external boundary point not lying in $\mathbb{H}$. Shifting $\mathcal{F}$ by means of products of S, T, S^{-1}, T^{-1} one obtains a covering of $\mathbb{H}$ consisting of $\mathbb{S}l_2(2,\mathbb{Z})$-fundamental domains.

(1.3)



The geometric imagination can be made precise by means of *modular functions.* These are $\mathbb{S}l(2,\mathbb{Z})$-invariant meromorphic functions on $\mathbb{H}$ allowing a meromorphic extension on $\mathbb{S}l(2,\mathbb{Z})\backslash\mathbb{H}$ to the compactification $\mathbb{P}^1(\mathbb{C})$. For $i = 2, 3$ we set $g_i(\tau) = g_i(\wedge_\tau)$. Looking at the discriminant of the polynomial $p_3(X)$ in the WEIERSTRASS equation $Y^2 = p_3(X) = 4X^3 - g_2X - g_3$ of E_τ we define

$$\Delta(\tau) = 27g_3^2(\tau) - g_2^3(\tau) \ .$$

Then $g_2^3(\tau)/\Delta(\tau)$ is a modular function. The *elliptic modular function* is defined as $j(\tau) = 12^3 g_2^3(\tau)/\Delta(\tau)$. Especially it is invariant under $S : \tau \mapsto \tau + 1$. It can be written as Fourier series:

$$j(\tau) = q^{-1} + 744q^0 + \sum_{n=1}^{\infty} a_n q^n \ , \quad q = e^{2\pi i \tau} \ , \quad a_n \in \mathbb{Z} \ .$$

The elliptic modular function $j : \mathbb{H} \to \mathbb{C}$ goes down to an analytic isomorphism $\mathbb{S}l(2,\mathbb{Z})\backslash\mathbb{H} \to \mathbb{C}$.

Consider now the elliptic curve family $\mathcal{E}$ over $\mathbb{H}$ defined by

$$\mathcal{E} = \{(w : x : y), \tau) \in \mathbb{P}^2(\mathbb{C}) \times \mathbb{H} \, ; \quad wy^2 = 4x^3 - g_2(\tau)w^2x - g_3(\tau)w^3\}.$$

It has a natural projection onto $\mathbb{H}$. The fibres are the elliptic curves E_τ. The upper half plane $\mathbb{H}$ appears as parameter space for (up to isomorphy) all elliptic curves. This analytic family of curves is denoted by $\mathcal{E}/\mathbb{H}$. The fibres $E_\tau, E_{\tau'}$, are isomorphic iff $\tau' \in \mathbb{S}l(2,\mathbb{Z})\tau$. Therefore we get a bijection

$$\mathbb{C} = \mathbb{S}l(2,\mathbb{Z})\backslash\mathbb{H} \Longleftrightarrow \quad \{\text{isomorphy classes of elliptic curves}\}\ .$$

In this (rough) sense we say that $\mathbb{P}^1$ is the (compactified) *moduli space of elliptic curves.* Altogether we have a commutative diagram (1.4) for each $\tau \in \mathbb{H}$.

$$\begin{array}{ccccc}
E_\tau & \hookrightarrow & \mathcal{E} & \hookrightarrow & \mathbb{P}^2(\mathbb{C}) \times \mathbb{H} \\
\downarrow & & \downarrow & \swarrow & \text{projection} \\
\{\tau\} & \hookrightarrow & \mathbb{H} & & \\
 & & \downarrow \mathbb{S}l(2,\mathbb{Z}) & & \\
 & & \mathbb{S}l(2,\mathbb{Z}) \setminus \mathbb{H} \cong \mathbb{C} \subset \mathbb{P}^1(\mathbb{C}) & &
\end{array}$$

1.2 Elliptic Curves Over Arbitrary Fields

We use the following notations:

K	a field, L a field extension of K,
$\bar{K}$	the algebraic closure of K,
$\mathbb{P}^2_K$	the projective plane over K,
$\mathbb{P}^2(L)$	the points of this plane with coordinates in L,
f	a homogeneous polynomial in $K[W,X,Y]$,
$\mathbb{P}\mathbb{G}l(3,K)$	the projective linear group $\mathbb{G}l(3,K)/K^*$,
$C : f = 0$	the plane projective curve defined by f,
$C(L)$	the points of C with coordinates in L (L-points).

The group $\mathbb{P}\mathbb{G}l(3,L)$ acts on $\mathbb{P}^2(L)$ and $\mathbb{G}l(3,L)$ on $L[W,X,Y]$ in obvious manner. For $G \in \mathbb{G}l(3,L)$ we define the inverse image curve of C by $G^*C : G^*f = 0$, where G^*f denotes the inverse image of f. We have

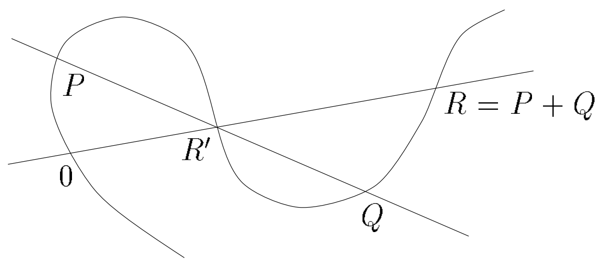
$$G^*C(L) = \{P \in \mathbb{P}^2(L); G^*f(P) = f(G(P)) = 0\}\ .$$

Two curves C, C' are called *L-linearly equivalent,* if there is a linear transformation $G \in \mathbb{G}l(3,L)$ such that $C' = G^*C$.

A point $P \in C(L)$ is called *singular* iff the derived polynomials $\partial f/\partial W$, $\partial f/\partial X$, $\partial f/\partial Y$ vanish at P. The curve C is *non-singular* iff each point $P \in C(\bar{K})$ is non-singular.

Definition 1.1 An *elliptic curve* E/K is a non-singular curve of degree 3 in $\mathbb{P}^2_K$ together with a point $0 \in E(K)$.

We are able to define a commutative group structure on E/K. For this purpose consider the L-points of E. Denote by PQ the line through two points $P, Q \in E(L)$. If $P = Q$, then it is defined as tangent line of E through P. By BEZOUT's, theorem there is a unique third intersection point $R' \in \mathbb{P}^2(L)$ of $E(\bar{L})$ and $PQ(\bar{L})$ beside of P, Q. It is easy to see that it belongs to $E(L)$. We apply the same procedure to OR' instead of PQ in order to receive a third intersection point R. Now define $P + Q = R$. Then one gets a commutative group law on $E(L)$, L an arbitrary field extension of K (see [41]). The auxiliary point R' is nothing else than $-(P+Q)$ and O is the neutral element of our addition with figure (1.4).



(1.4)

From projective (homogeneous) equations $f = 0$ we change over to affine (inhomogeneous) equations $F = 0$, $F(X, Y) = f(1, X, Y)$. It defines an affine curve in $\mathbf{A}^2_K$ and an affine geometric curve in $\mathbf{A}^2(L)$ as algebraic set of points. Adding some points at infinity $(W = 0)$ we get back $C(L)$, especially $C(\bar{L})$, hence $C : f = 0$, $f(W, X, Y) = F(X/W, Y/W)W^{\deg F}$. In our elliptic cases we keep the distinction between affine and projective equations/curves only in mind.

Two elliptic curves E/K, E'/K are *K-(linearly) isomorphic,* iff there exists an element $\alpha \in \mathbb{G}l(3, K)$ such that $E = \alpha^* E'$ and $\alpha(O) = O'$, O' the zero point of E'.

Each elliptic curve E/K is K-isomorphic to an elliptic curve of type

$$E'/K : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{1.5}$$

with $0' = (0:0:1)$, the point at infinity of E'.

If char $K \neq 2, 3$, then the above statement remains to be true, if we set $a_i = 0$ for $i = 1, 2, 3$, that means we substitute (1.5) by

$$E'/K : Y^2 = 4X^3 - g_2X - g_3 \ . \tag{1.6}$$

The equations or curves in (1.5) or (1.6) are called *WEIERSTRASS normal forms* (of E). Up to isomorphy it suffices to investigate elliptic curves given in WEIERSTRASS normal form. So we assume now that:

(i) char $K) \neq 2, 3$;

(ii) $E/K : Y^2 = 4X^3 - g_2X - g_3$

(iii) $O = (0 : 0 : 1)$;

the same for E'/K.

As in the classical (complex) case we look for invariants and their meaning. We set

$$\Delta(E/K) = 27g_3^2 - g_2^3 \ , \quad j(E/K) = 12^3 g_2^3 / \Delta(E/K) \ . \tag{1.7}$$

Given a plane projective curve $C/K : f = 0$. We also write C_L, C_L/L or simply C/L for the curve in $\mathbb{P}_L^2$ defined by $f = 0$. With obvious notations and the assumptions (i), (ii), (iii) above the following basic facts are well-known:

Proposition 1.2

(i) E/K is non-singular, hence an elliptic curve, iff $\Delta(E/K) \neq 0$.

(ii) Let E'/L be another elliptic curve, $\bar{L} = \bar{K}$. Then $E/\bar{K}$ and $E'/\bar{K}$ are $\bar{K}$-isomorphic if an only if $j(E/K) = j(E'/L)$ in $\overline{K}$.

(iii) The elliptic curves E/K and E'/K are $\bar{K}$-isomorphic iff there exists an element $u \in \sqrt{K^\times} = \{v \in \bar{K}; v^2 \in K^\times\}$ such that $g_2' = u^4 g_2$, $g_3' = u^6 g_3$.

(iv) The elliptic curves E/K and E'/K are K-isomorphic iff there exists $u \in K^\times$ such that $g_2' = u^4 g$, $g_3' = u^6 g_3$.

1.2.1 Reduction of Elliptic Curves

Let $R \subseteq K$ be an integral domain (with 1), such that $K = \text{Quot } R$, the quotient field of R. We write E/R instead of E/K, if the coefficients of the defining equation belong to R, and we say that *E is defined over R*. An *R-model* of the elliptic curve E'/K is an elliptic curve E/R such that E/K is K-isomorphic to E'/K. It is easy to see that each elliptic curve E'/K has at least one R-model. In fact, there are a lot of them.

Now, let $(R, \mathcal{M})$ be a local ring, $\mathcal{M}$ the maximal ideal of R and $k = R/\mathcal{M}$ the residue field. We write $\bar{g}$ for the residue class of $g \in R$ modulo $\mathcal{M}$. For an elliptic curve $E/R : Y^2 = X^3 - g_2X - g_3$ we define the *reduction* E_k of E/R by

$$E_k/k : Y^2 = X^3 - \bar{g}_2X - \bar{g}_3 \ .$$

We say that E/R has *good reduction,* if E_k is smooth, that means that E_k is an elliptic curve over k. There is a nice simple criterion:

Lemma 1.3 (local criterion for good reduction) *The elliptic curve E/R has good reduction if and only if its discriminant $\Delta(E/R)$ is a unit in the local ring R.*

Now let R be a DEDEKIND domain with quotient field $K = \text{Quot } R$, $\mathcal{P} \in \text{Spec } R$ a prime ideal and $R_{\mathcal{P}}$ the corresponding (local) quotient ring. We say that the elliptic curve E'/K has *good reduction at $\mathcal{P}$,* if there is an $R_{\mathcal{P}}$-model $E/R_{\mathcal{P}}$ of E' with good reduction. Otherwise we say that E'/K has *bad reduction at P.* In any case E'/K has good reduction at almost all points of Spec R. If T is a subset of Spec R, then we say that E'/K has *good reduction on T,* if E'/K has good reduction at all points of T. In obvious manner one explains the meaning of: bad *reduction outside T, bad reduction on $S \subset$ Spec R, good reduction outside S.*

In our applications we will work with the ring $R = \mathcal{O}$ of integers of a number field K. Fixing these notations we notice

1.2.2 Two Finiteness Theorems of Number Theory

Denote by $I = I(\mathcal{O})$ the semigroup of integral ideals of $\mathcal{O}$, the group of fractional ideals of K by $I^* = I^*(\mathcal{O}) = I^*(K)$ and by $H^* = H^*(K)$ its subgroup of principal ideals. The group $Cl(K) = I^*/H^*$ is called the *class group of K.*

Theorem 1.4 (Finiteness of class group) *The class group $Cl(K)$ has finite order.*

The order $h(K) = \sharp Cl(K)$ is called the *class number of K.*

For a subset $S \subseteq \text{Spec } \mathcal{O}$ the *ring of S-integers* of K is defined by

$$\mathcal{O}_S = \{a/b;\ a, b \in \mathcal{O},\ b \notin \mathcal{P} \text{ for all } \mathcal{P} \in T = \text{Spec } \mathcal{O} \backslash S\}$$

Take care of the difference between the local ring

$$\mathcal{O}_{\mathcal{P}} = \{a/b;\ a, b \in \mathcal{O},\ b \notin \mathcal{P}\}$$

and the global ring $\mathcal{O}_{\{\mathcal{P}\}}$.

Corollary 1.5 *For each finite $S' \subset$ Spec $\mathcal{O}$ there exists a finite $S \subset$ Spec $\mathcal{O}$ containing S' such that $\mathcal{O}_S$ is a principal domain.*

Proof: The semigroup homomorphism

$$I(\mathcal{O}) \longrightarrow I(\mathcal{O}_S)\ ,\ \ \mathcal{A} \longmapsto \mathcal{A}_S = \mathcal{O}_S \mathcal{A}$$

extends to the exact sequence of group homomorphisms

$$1 \longrightarrow \langle S \rangle \longrightarrow I^*(\mathcal{O}) \longrightarrow I^*(\mathcal{O}_S)\ , \tag{1.8}$$

where $\langle S \rangle$ denotes the group generated by S.

Now let $\{\mathcal{A}_1, \ldots, \mathcal{A}_h\}$ be a system of representatives of the class group $cl(\mathcal{O})$ and

$$S = S' \cup \{\text{prime divisors of } \mathcal{A}_1 \cdot \ldots \cdot \mathcal{A}_h\}\ .$$

For each ideal $\mathcal{A}$ of K we find $a \in K$ and $i \in \{1, \ldots, h\}$ such that $\mathcal{A}_S = (a\mathcal{A}_i)_S = a\mathcal{O}_S$ because of $\mathcal{A}_i \in \langle S \rangle$ and (1.8). ■

Theorem 1.6 (DIRICHLET's Unit Theorem) *For finite $S \subset$ Spec $\mathcal{O}$ the group of units $\mathcal{O}_S^*$ of $\mathcal{O}_S$ is finitely generated.* ■

Corollary 1.7 *For each natural number n the factor group $\mathcal{O}_S^*/\mathcal{O}_S^{*n}$ is finite.*

1.2.3 SHAFAREVIČ's Finiteness Theorem

Lemma 1.8 (global criterion for good reduction) *Let S be a finite subset of Spec $\mathcal{O}_S$ such that $\mathcal{O}_S$ is a principal domain. The elliptic curve E'/K has good reduction outside of S iff it has an $\mathcal{O}_S$-model $E/\mathcal{O}_S$ such that $\Delta(E/\mathcal{O}_S) \in \mathcal{O}_S^*$.*

Proof: The discriminant condition is sufficient by the local criterion 1.3.

Assume conversely that for each $\mathcal{P} \in T = \text{Spec } \mathcal{O} \backslash S$ there is a model

$$E_{\mathcal{P}}/\mathcal{O}_{\mathcal{P}} : Y^2 = 4X^3 - g_{2\mathcal{P}}X - g_{3\mathcal{P}}$$

of E'/K with $\Delta_{\mathcal{P}} = \Delta(E_{\mathcal{P}}/\mathcal{O}_{\mathcal{P}}) \in \mathcal{O}_{\mathcal{P}}^*$. With obvious notations we have

$$g_2' = u_{\mathcal{P}}^4 \cdot g_{2\mathcal{P}} \ , \ \ g_3' = u_{\mathcal{P}}^6 \cdot g_{3\mathcal{P}}, \Delta' = u_{\mathcal{P}}^{12}\Delta_{\mathcal{P}} \tag{1.9}$$

for suitable $u_{\mathcal{P}} \in K$, $\mathcal{P} \in T$. Without loss of generality we can assume that we start with a model $E'/\mathcal{O}_K$, hence $g_i' \in \mathcal{O}_K$. Let $\{\mathcal{P}_1, \ldots, \mathcal{P}_r\}$ be the set of prime divisors of $\Delta' \in \mathcal{O}_K$. Then

$$u_{\mathcal{P}} \in \mathcal{O}_{\mathcal{P}}^* \quad \text{for} \quad \mathcal{P} \in T \backslash \{\mathcal{P}_1, \ldots m\mathcal{P}_r\}$$

by the last identities of (1.9) and our assumptions. So $(\mathcal{O}_{\mathcal{P}} u_{\mathcal{P}})_{\mathcal{P} \in T}$ belongs to the restricted product group (with components 1 almost everywhere)

$$\prod_{\mathcal{P} \in T}{}' \, I^*(\mathcal{O}_{\mathcal{P}}) \xrightarrow{\sim} I^*(\mathcal{O}_S) \ .$$

Since $\mathcal{O}_S$ is principal we can represent our tuple by $\mathcal{O}_S u$, $u \in K$; so

$$u_{\mathcal{P}} = \varepsilon_{\mathcal{P}} u \ , \ \ \varepsilon_{\mathcal{P}} \in \mathcal{O}_{\mathcal{P}}^* \quad \text{for all} \quad \mathcal{P} \in T \ . \tag{1.10}$$

Now we define the elliptic curve

$$E/\mathcal{O}_S : Y^2 = X^3 - g_2 X - g_3$$

setting

$$g_2 = g_2'/u^4 \ , \ \ g_3 = g_3'/u^6 \tag{1.11}$$

The coefficients of the equation of E differ from those of $E_{\mathcal{P}}$ only by local units because of (1.11), (1.9) and (1.10). This is also true for $\Delta = \Delta(E/\mathcal{O}_S)$ and Δ' for the same reasons. Therefore $\Delta \in \mathcal{O}_{\mathcal{P}}^*$ for all $\mathcal{P} \in T$, hence $\Delta \in \mathcal{O}_S^*$. ■

Theorem 1.9 (SHAFAREVIČ) *Let K be a number field, $\mathcal{O} = \mathcal{O}_K$ its ring of integers and S a finite set of prime ideals of $\mathcal{O}$. Then, up to K-isomorphy, there are only finitely many elliptic curves E/K with good reduction outside of S.*

Proof: Without loss of generality we can assume that all prime divisors of 2 and 3 belong to S. So we can work locally along $T = \mathrm{Spec}\mathcal{O} \setminus S$ and also globally with WEIERSTRASS normal forms in the narrow sense of (1.6). The class of all elliptic curves E/K with good reduction outside of S is denoted by $\mathcal{E}(K,S)$. The domain can be assumed to be principal by Corollary 1.5. Each member of $\mathcal{E}(K,S)$ has models $E/\mathcal{O}_S$ with $\Delta(E/\mathcal{O}_S) \in \mathcal{O}_S^*$ by Lemma 1.8. Together with Proposition 1.2 (iv) we see that the map

$$\delta : \mathcal{E}(K,S) \longrightarrow \mathcal{O}_S^*/\mathcal{O}_S^{*12}\ ,\ \ E/\mathcal{O}_S \longmapsto \Delta(E/\mathcal{O}_S)\mathrm{mod}^{\times}\mathcal{O}_S^{*12}$$

is well-defined. The image is finite by Corollary 1.7. So it suffices to prove that for a given S-unit D there exist only finitely many elliptic curves

$$E/\mathcal{O}_S : Y^2 = X^3 - g_2X - g_3$$

with $\Delta(E/\mathcal{O}_S) = D$. This follows immediately from the definition of the discriminant and the next lemma. ■

Lemma 1.10 *With the above notations the diophantine equation*

$$U^3 - 27V^2 = D$$

has only finitely many solutions u, v in $\mathcal{O}_S$. ■

1.2.4 Basic References

For an introduction to the classical theory of elliptic and modular functions we refer to [46]. All we need in I.1 can be found in the first chapters there. The omitted proofs of some basic results on elliptic curves over finite fields are contained in [41]. K-isomorphy of curves needs in general the finer scheme language. It will be necessarily used later. Our style of writing is a good preparation. The basic introduction is HARTSHORNE's book [27]. Proofs of the two basic finiteness theorems 1.4 and 1.6 can be found in [16].

Our proof of SHAFAREVIČ's Finiteness Theorem for elliptic curves is a detailed version of SERRE's proof in [69]. The theorem was announced by SHAFAREVIČ on the

International Congress in Stockholm 1962, together with a far-reaching conjecture on algebraic curves over number fields (SHAFAREVIČ-conjecture) proved by FALTINGS in 1983 together with the MORDELL-conjecture as consequence. The diophantine equation in Lemma 1.10 can be solved effectively by methods of BAKER [4], see also SERRE's lectures [71]. Altogether one has an effective way for finding up to isomorphy all elliptic curves over a fixed number field with prescribed places of bad reduction. An algorithm has been established by TATE [88].

Recently ESTRADA-SARLABOUS, see Appendix I, found a way to transfer the methods and the effective result to PICARD curves

$$C : Y^3 = X^4 + G_2X^2 + G_3X + G_4$$

of genus 3. These curves play a central role in all the following chapters.

2 PICARD Curves

2.1 The Moduli Space of PICARD Curves

Definition 2.1 Let C' be a compact algebraic curve over $\mathbb{C}$. It is called a *PICARD curve*, if it is isomorphic to a plane projective curve $C/\mathbb{C}$ of the following equation type:

$$C' \xrightarrow{\sim} C : WY^3 = \sum_{i=0}^{4} G_i W^i X^{4-i} \ , \quad G_0 \neq 0 \ .$$

In affine coordinates the plane PICARD curve C is described by

$$C : Y^3 = G_0 X^4 + G_1 X^3 + G_2 X^2 + G_3 X + G_4 \ .$$

One has to add the point $\infty = (0 : 0 : 1)$ in order to obtain the projective model from the affine one. By means of projective TSCHIRNHAUS transformation one can reduce the equations to the following *normal forms*

$$\begin{aligned} WY^3 &= X^4 + G_2 W^2 X^2 + G_3 W^3 X + G_4 W^4 \quad \text{(projective)}, \\ Y^3 &= X^4 + G_2 X^2 + G_3 X + G_4 = p_4(X) \quad \text{(affine)}. \end{aligned} \tag{2.1}$$

The singular locus of

$$C : F(W, X, Y) = WY^3 - X^4 - G_2 W^2 X^2 - G_3 W^3 X - G_4 W = 0$$

can be determined by solving the system of homogeneous equations

$$F = \partial F/\partial W = \partial F/\partial X = \partial F/\partial Y = 0 \ . \tag{2.2}$$

The point ∞ is a smooth one because $\partial F/\partial W(0, 0, 1) = 1$. So all singular points of C lie in the affine part. It is easy to see that only the intersection points with the line $L_0 : Y = 0$ are possible singularities. These are the points

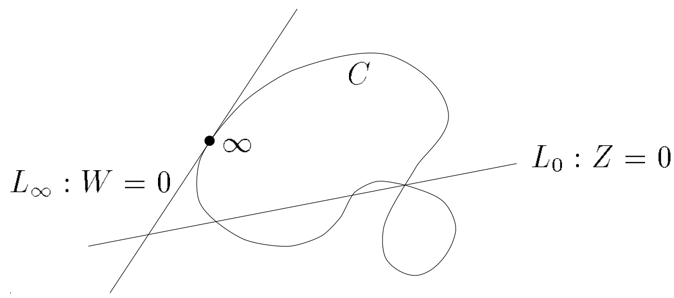
$$R_i = (1 : a_i : 0) \ , \quad i = 1, \ldots, 4 \ , \tag{2.3}$$

where $a_1, \ldots, a_4$ are the zeros of $p_4(X)$. As in the case of elliptic curves we have a *discriminant* criterion: $\Delta(C) \neq 0$. The discriminant of C is defined as $\Delta(C) = \prod_{i \neq j} (a_j - a_i)$. In terms of the coefficients of F it is described by

$$\Delta(C) = 16G_2^4 \cdot G_4 - 128G_2^2 \cdot G_4^2 - 4G_2^3 \cdot G_3^2 + 144G_2G_3^2G_4 - 27G_3^4 + 256G_4^3$$

The picture (2.4) gives an imagination of (the real part of) a PICARD curve in normal form with exactly one (real) singularity.

(2.4)



The line L_∞ touches C at ∞ of order (intersection number) 4.

We look now for the moduli space $\mathbf{M}$ of PICARD curves in the rough sense: to find a complex-algebraic structure on the set of isomorphy classes of these curves. More precisely, this will be done for smooth curves, and then we look for a natural compactification and interpretation:

$$\{\text{smooth PICARD curves}\}/\text{Isom.} \Longleftrightarrow \mathbf{M}^0 \subset \mathbf{M}$$

Set

$$\mathbb{C}_0^4 = \left\{(z_1, \ldots, z_4) \in \mathbb{C}^4 \; ; \; z_1 + \ldots + z_4 = 0\right\} \subset \mathbb{C}^4$$

and let $\mathcal{C}$ be the following analytic family of PICARD curves:

$$\mathcal{C} = \left\{((w : x : y), (a_1, \ldots, a_4)) \in \mathbb{P}^2(\mathbb{C}) \times \mathbb{C}_0^4 \; ; \; wy^3 = \prod_{i=1}^{4}(x - a_i w)\right\}$$

Without change of the notation $\mathcal{C}$ we omit the special singular fibre with $WY^3 = X^4$ over 0. All other PICARD curves are represented in $\mathcal{C}$ up to isomorphy. We have the following commutative diagrams

$$\begin{array}{ccccccccc} C_a & \hookrightarrow & \mathcal{C} & \hookrightarrow & \mathbb{P}^2 \times \mathbb{C}_0^4 & & & & \\ \downarrow & & \downarrow & \swarrow & \downarrow & & & & \\ \{a\} & \hookrightarrow & \mathbb{C}_0^4 \setminus 0 & \longrightarrow & \mathbb{P}\mathbb{C}_0^4 & = & \mathbb{P}\mathbb{C}^3 & = & \mathbb{P}^2 \end{array} \qquad (2.5)$$

with obvious projections and identifications.

The symmetric group S_4 acts on $\mathbb{C}_0^4$ by permutation of coordinates. This action goes down to $\mathbb{P}^2$. The compact quotient surface $\hat{\mathbf{M}} = \mathbb{P}^2/S_4$ is normal, algebraic and, by LÜROTH's theorem, rational.

We go back to $\mathbb{P}^2 = \mathbb{P}_0^3 := \mathbb{P}\mathbb{C}_0^4$ writing the elements as homogeneous quadruples $(a_1 : \ldots : a_4)$, $a_1 + \ldots + a_4 = 0$. Now we choose four points in general position. In order to be explicit we choose

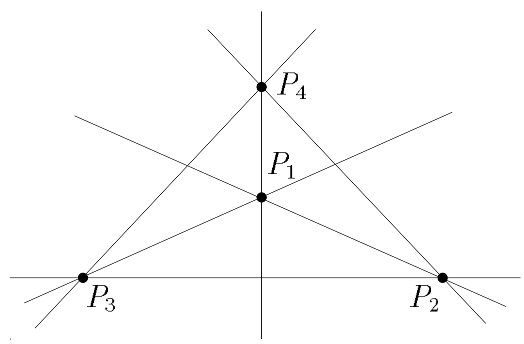
$$\begin{aligned} P_1 &= (-3:1:1:1) \quad , \quad P_2 = (1:-3:1:1) \ , \\ P_3 &= (1:1:-3:1) \quad , \quad P_4 = (1:1:1:-3) \ . \end{aligned} \tag{2.6}$$

The line through P_i, P_j is denoted by $L_{ij} = L_{ji}$. These six lines form a reduced divisor

$$\triangle = L_{12} + L_{13} + L_{14} + L_{23} + L_{24} + L_{34} \tag{2.7}$$

on $\mathbb{P}^2$ as described in picture (2.8)

(2.8)



Obviously the action of the symmetric group S_4 restricts to an action on $\mathbb{P}^2 \setminus \Delta$. We set

$$\mathbf{M}^0 := \left(\mathbb{P}^2 \setminus \triangle\right)/S_4 \subset \mathbf{M} := \mathbb{P}^2 \setminus \{P_1, \ldots, P_4\} \subset \hat{\mathbf{M}} := \mathbb{P}^2/S_4 \ .$$

Two plane PICARD curves C, C' are called *linearly isomorphic*, if there is a $G \in Gl_3(\mathbb{C})$ such that $G^*C = C'$