INTERNATIONAL ATOMIC ENERGY AGENCY
UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS
I.C.T.P., P.O. BOX 586, 34100 TRIESTE, ITALY, CABLE: CENTRATOM TRIESTE

SMR.637/18

ADVANCED WORKSHOP ON ARITHMETIC ALGEBRAIC GEOMETRY

(31 August - 11 September 1992)

Elliptic Curves

J. Nekovar
Department of Mathematics
University of California
Berkeley, CA 94720
U.S.A.

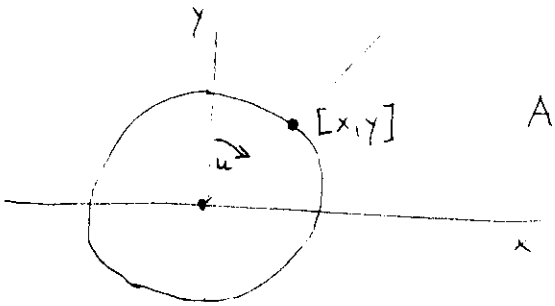
ELLIPTIC CURVES (Jan Nekovář)

(1) Trigonometric functions

Let $E : x^2+y^2 = 1$ be the "unit circle"; its real points $E(\mathbb{R}) = \{x,y \in \mathbb{R} \mid x^2+y^2=1\}$ are parametrized by the pair of functions $s(u) = \sin(u)$, $s'(u) = \cos(u)$: the formula

$$u \longmapsto [x,y] = [s(u), s'(u)]$$

furnish us with a bijection between $\mathbb{R}/2\pi\mathbb{Z}$ and $E(\mathbb{R})$. Geometrically, u is the angle between the y-axis and the line connecting $[x,y]$ and the origin:



Allowing complex coordinates, we get a bijection between complex points $E(\mathbb{C}) = \{x,y \in \mathbb{C} \mid x^2+y^2=1\}$ and $\mathbb{C}/2\pi\mathbb{Z}$.

Both $\mathbb{R}/2\pi\mathbb{Z}$ and $\mathbb{C}/2\pi\mathbb{Z}$ are abelian groups, hence we get group structures on $E(\mathbb{R})$, $E(\mathbb{C})$ (with $[0,1]$ as a neutral element). If $[x_i, y_i]$ correspond to u_i $(i=1,2,3)$ and $u_3 = u_1 + u_2$, then the classical formulas

$$s(u+v) = s(u)\,s'(v) + s(v)\,s'(u)$$
$$s'(u+v) = s'(u)\,s'(v) - s(u)\,s(v)$$

describe the group operation

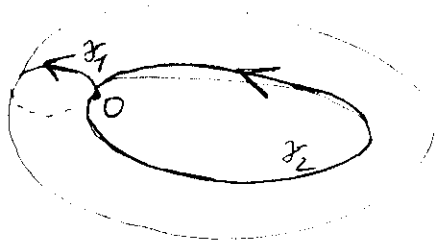
$$[x_1, y_1] \boxplus [x_2, y_2] = [x_1 y_2 + x_2 y_1 \,,\, y_1 y_2 - x_1 x_2]$$

(2) Elliptic functions

In a similar way, elliptic (= doubly periodic) functions parametrize non-singular plane cubic curves.

Fix $\omega_1, \omega_2 \in \mathbb{C}$ such that ω_1, ω_2 are linearly independent over $\mathbb{R}$. Then $\Gamma = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ is a lattice in $\mathbb{C}$:

Put $X = \mathbb{C}/\Gamma$ — this is an abelian group, but also a Riemann surface, which is obtained from $\mathbb{C}$ by identifying points that differ by some $\gamma \in \Gamma$. Geometrically, X is a torus:



γ_1, γ_2 — correspond to paths from 0 to ω_1 resp. ω_2

Def: elliptic function (with respect to Γ) is a meromorphic function on X:

$\Leftrightarrow$ a meromorphic function f on $\mathbb{C}$ such that $f(z+\gamma) = f(z)$ $(z \in \mathbb{C}, \gamma \in \Gamma)$

$\Leftrightarrow$ a holomorphic map $X \longrightarrow \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$

Recall: $f : U \longrightarrow \mathbb{C} \cup \{\infty\}$ $(U \subset \mathbb{C})$ is meromorphic, if, in a neighbourhood of each $z_0 \in U$, $f(z) = \sum_{n \geq m} a_n (z - z_0)^n$.

The order of f at z_0 is defined as

$$\mathrm{ord}_{z_0}(f) = \min \{ n \mid a_n \neq 0 \}$$

Proposition 1: Let $f \neq 0$ be an elliptic function w.r.t. Γ. Then

(1) $\sum_{x \in X} \mathrm{ord}_x(f) = 0 \quad \in \mathbb{Z}$

(2) $\sum_{x \in X} \underbrace{\mathrm{ord}_x(f) \cdot x}_{\in \mathbb{Z}} = 0 \quad \in X$

Proof. Let $\Delta = \{ \lambda_1 \omega_1 + \lambda_2 \omega_2 \mid 0 \leq \lambda_1, \lambda_2 \leq 1 \}$ be a "fundamental parallelogram" of Γ. Replacing, possibly, ω_1, ω_2 by another basis of Γ, we can assume that f has no poles or zeroes on the boundary $\partial\Delta$ of Δ.

(1) The left hand side is equal to

$$\frac{1}{2\pi i} \int_{\partial\Delta} \frac{df}{f} = 0 \quad \text{by periodicity}$$

(2) Similarly, the LHS is equal to (mod Γ)

$$\frac{1}{2\pi i} \int_{\partial\Delta} z \frac{df}{f} = m\omega_1 + n\omega_2 \in \Gamma \quad \text{(for some } m, n \in \mathbb{Z}\text{)}$$

■

(3) Divisors, divisor classes

Our next aim is to characterize possible configurations of zeroes and poles of elliptic functions. We show that the conditions (1), (2) in the above Proposition 1 are not only necessary, but also sufficient.

Def A *divisor* on X is a *formal* sum (finite)

$$\sum n_i (P_i) \quad , \; n_i \in \mathbb{Z} \; , \; P_i \in X \; .$$

Divisors form a group $\mathrm{Div}(X)$ under formal addition (i.e. $\mathrm{Div}(X)$ is a free abelian group on X).

For a divisor $D = \sum n_i (P_i)$, define

$$\deg(D) := \sum n_i \in \mathbb{Z}$$

$$\boxplus D := \boxplus n_i P_i \in X \quad (\text{sum in } X = \mathbb{C}/\Gamma)$$

Let $\mathrm{Div}^0(X) = \{ D \in \mathrm{Div}(X) \mid \deg(D) = 0 \}$

be the group of divisors of degree 0.

For an elliptic function $f \neq 0$ on X, put

$$\mathrm{div}(f) = \sum_{x \in X} \mathrm{ord}_x(f) \cdot (x) \quad \in \mathrm{Div}(X)$$

As $\mathrm{div}(f \cdot g) = \mathrm{div}(f) + \mathrm{div}(g)$,

$P(X) = \{ \mathrm{div}(f) \}$ is a subgroup ("principal divisors") of $\mathrm{Div}(X)$

$\boxplus : \mathrm{Div}^0(X) \longrightarrow X$ is a homomorphism

Prop 1: (1) $P(X) \subseteq \mathrm{Div}^0(X)$ (= above Prop. 1)

(2) $P(X) \subseteq \ker(\boxplus)$

Thm 1: $P(X) = \ker(\boxplus)$

Cor: $\mathrm{Pic}^0(X) := \dfrac{\mathrm{Div}^0(X)}{P(X)} \xrightarrow{\boxplus} X$

$(P) - (O) \longmapsto P$

In other words, $\boxplus$ induces an isomorphism between divisor classes of degree 0 and X.

Proof of Thm 1: Let $D \in \ker(\boxplus)$ i.e. $\deg(D) = 0$, $\boxplus D = O$. We shall construct f with $\mathrm{div}(f) = D$.

Basic tool: Weierstrass' σ-function:

(i) • $\sigma : \mathbb{C} \longrightarrow \mathbb{C}$ holomorphic

(ii) • all its zeroes are simple zeroes at $\gamma \in \Gamma$

(iii) • $\dfrac{\sigma(z+\gamma)}{\sigma(z)} = \exp(\ell(\gamma) z + m(\gamma))$ $\left(\begin{matrix}\forall \gamma \in \Gamma \\ \forall z \in \mathbb{C}\end{matrix}\right)$

$(\ell(\gamma), m(\gamma) \in \mathbb{C})$

Representing D by $\sum n_i (z_i)$, $z_i \in \mathbb{C}$ with $\sum n_i z_i = O \in \mathbb{C}$, $\sum n_i = O \in \mathbb{Z}$, we see that (by (iii))

$$f(z) := \prod \sigma(z - z_i)^{n_i}$$ satisfies $f(z+\gamma) = f(z)$,

hence is a meromorphic function on X.

By (ii) $\mathrm{div}(f) = D$. ∎

Writing $\mathcal{M}(X)^*$ for the multiplicative group of non-zero meromorphic functions on X, we get an exact sequence

$$0 \longrightarrow \mathbb{C}^* \longrightarrow \mathcal{M}(X)^* \xrightarrow{\text{div}} \mathrm{Div}^0(X) \xrightarrow{\boxplus} X \longrightarrow 0$$

Compare with an analogous sequence

$$0 \longrightarrow \mathcal{O}_F^* \longrightarrow \mathbb{A}_F^* \longrightarrow \underbrace{\mathcal{Y}_F}_{\text{ideals}} \longrightarrow \mathcal{Cl}_F \longrightarrow 0$$

for a number field F.

(4) Formulas

$$\sigma(z) = z \prod_{\substack{\gamma \in \Gamma \\ \gamma \neq 0}} \left(1 - \frac{z}{\gamma}\right) \exp\left(\frac{z}{\gamma} + \frac{1}{2}\left(\frac{z}{\gamma}\right)^2\right)$$

$$\wp(z) := -\frac{d^2}{dz^2} \log \sigma(z) = \frac{1}{z^2} + \sum_{\substack{\gamma \in \Gamma \\ 0 \neq \gamma}} \left[\frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2}\right]$$

is elliptic w.r.t. Γ, its derivative

$$\wp'(z) = -2 \sum_{\gamma \in \Gamma} \frac{1}{(z-\gamma)^3}$$

is elliptic, too.

The only pole of $\wp$ (resp. $\wp'$) is a double (resp. triple) pole at 0.

Thm 2. $\wp'^2 = 4\wp^3 - g_2\wp - g_3$, where

$$g_2 = 60 \sum_{\substack{\gamma\in\Gamma \\ \gamma\neq 0}} \gamma^{-4} \quad , \quad g_3 = 140 \sum_{\substack{\gamma\in\Gamma \\ \gamma\neq 0}} \gamma^{-6} .$$

Proof. The difference $\wp'^2 - (4\wp^3 - g_2\wp)$ is an elliptic function with only possible pole at 0. Calculation of its Laurent expansion around $z=0$ shows that it has in fact no pole, hence must be constant – its value is computed easily.

(5) Cubic curves

Put $a = -\frac{g_2}{4}$, $b = -\frac{g_3}{4}$. The affine curve $y^2 = x^3 + ax + b$ is completed by a point $[0:1:0]$ at infinity to a projective curve

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3 \qquad \left(x = \frac{X}{Z} , y = \frac{Y}{Z}\right)$$

We define a map

$$\varphi : \mathbb{C}/\Gamma \longrightarrow E(\mathbb{C}) \quad \text{(complex points of } E\text{)}$$

by

$$z \longmapsto [\wp(z) : \tfrac{1}{2}\wp'(z) : 1] \qquad z \neq 0$$

$$0 \longmapsto [0:1:0] .$$

Proposition 2: (1) φ is a bijection

(2) φ induces an isomorphism

$$\mathcal{M}(X) \simeq \mathbb{C}(x,y) \quad (= \mathbb{C}(E))$$

Proof: (1) Both $\mathbb{C}/\Gamma$ and $E(\mathbb{C})$ are Riemann surfaces; φ is holomorphic $\Rightarrow$ φ is open. As $\mathbb{C}/\Gamma$ is compact and $E(\mathbb{C})$ is connected, $\varphi(\mathbb{C}/\Gamma) = E(\mathbb{C})$.

If $\varphi(z_1) = \varphi(z_2) \Rightarrow z_1 = \pm z_2$ & $\wp'(z_1) = \wp'(z_2) \Rightarrow$

$\Rightarrow z_1 = z_2 \in \mathbb{C}/\Gamma$.

(2) Excercise

Via φ, $E(\mathbb{C})$ inherits the group structure (commutative) of $\mathbb{C}/\Gamma$.

Using the group isomorphism

$$\begin{array}{ccc} Pic^0(X) & \xrightarrow{\boxplus} & X \\ \downarrow & & \downarrow \\ \text{class of } (P)-(O) & \longmapsto & P \end{array}$$

and (2) of Proposition 2, we see that

$$P_1 \boxplus P_2 = P_3 \qquad (P_i \in E(\mathbb{C}))$$

$$\Updownarrow$$

$\exists$ function $f \in \mathbb{C}(x,y)$ such that

$$(P_1)-(O) + (P_2)-(O) = (P_3)-(O) + \operatorname{div}(f)$$

Let $\ell: aX + bY + cZ = 0$

($ax + by + c = 0$ in affine coordinates)

be any line. It intersects E at

three points P_1, P_2, P_3 (not necessarily distinct — $P_1 = P_2$ if ℓ is tangent to E at P_1; $P_1 = P_2 = P_3$ if ℓ is a triple tangent at P_1, i.e. if P_1 is an inflection point and ℓ an inflection tangent). Then

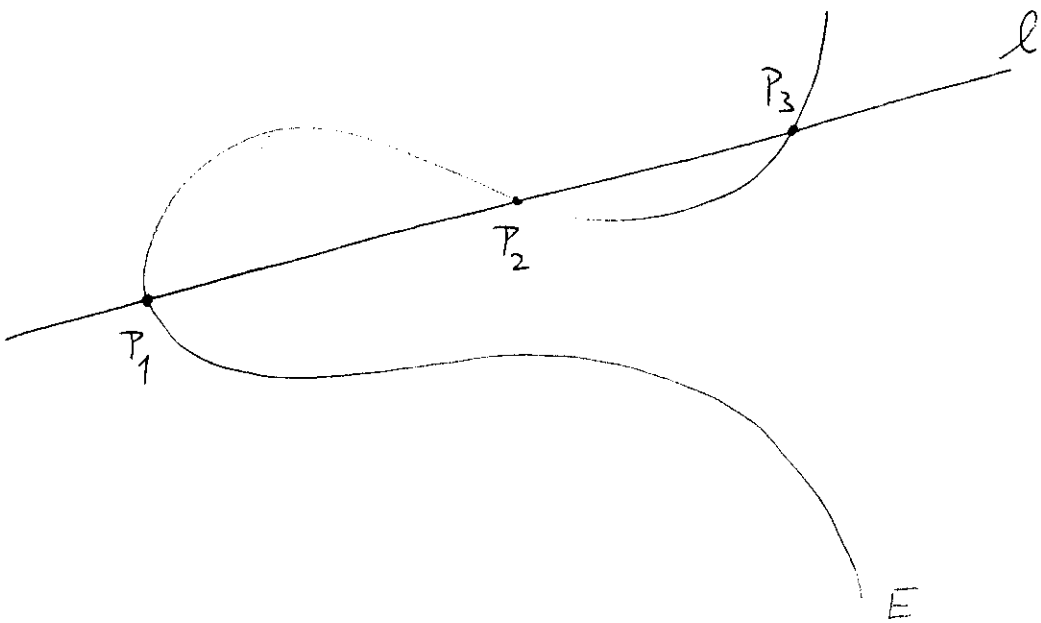
$$f = \frac{\alpha X + \beta Y + \gamma Z}{Z} = \alpha x + \beta y + \gamma \in \mathbb{C}(x, y)$$

has divisor

$$\operatorname{div}(f) = (P_1) + (P_2) + (P_3) - 3(O),$$

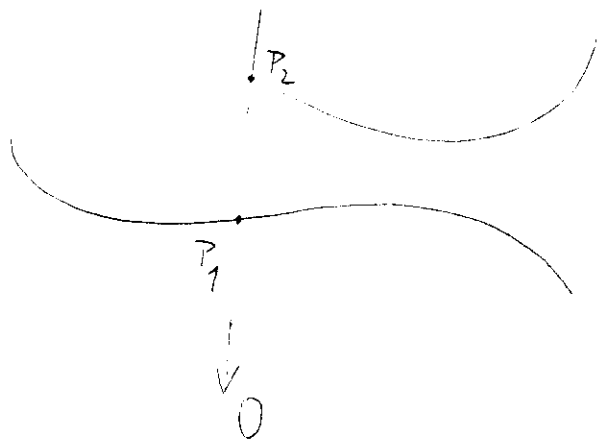
which means that

$$\underline{P_1 \boxplus P_2 \boxplus P_3 = O} \quad (= [0:1:0])$$



i.e. $P_3 = \boxminus(P_1 \boxplus P_2)$

Any "vertical line" $x = \text{const.}$ intersects E at points P_1, P_2, O, hence $P_2 = \boxminus P_1$:



This gives a geometric construction of $P_1 \boxplus P_2$: draw the unique line l between P_1, P_2 (= tangent to E at P_1 if $P_1 = P_2$), take the third intersection with E and change the sign of the y-coordinate.

Formulas: if $P_i = [x_i, y_i]$ $(i = 1, 2, 3)$

$$P_3 = P_1 \boxplus P_2,$$

the line through P_1, P_2 is $y = \alpha x + \beta$,

$$\alpha = \frac{y_2 - y_1}{x_2 - x_1} \quad ; \quad \beta = \frac{y_1 x_2 - x_1 y_2}{x_2 - x_1}$$

Intersections $l \cap E \iff (\alpha x + \beta)^2 = x^3 + Ax + B$,

i.e. $x^3 - \alpha^2 x^2 + (A - 2\alpha\beta)x + B - \beta^2 = (x - x_1)(x - x_2)(x - x_3)$

Coefficient of x^2: $\alpha^2 = x_1 + x_2 + x_3 \implies$

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \quad , \quad y_3 = -(\alpha x_3 + \beta)$$

Geometric description also makes clear that

(i) $2P = O \iff P = O$ or $P = [e_i, 0]$, e_i a root of $x^3 + Ax + B$

(ii) $3P = O \iff P$ is a point of inflection of E

More generally, if C is a curve of degree m, not containing E, then $E \cap C = \{P_1, \dots, P_{3m}\}$ (possibly with multiplicities) and $P_1 \boxplus \cdots \boxplus P_{3m} = O$.

---

(6) Diophantine properties

Let $K \subset \mathbb{C}$ be a subfield containing A, B. It follows from the formulas describing $\boxplus$ that the set of K-rational points $E(K)$ of E is a subgroup of $E(\mathbb{C})$.

Question: Describe the structure of $E(K)$ if K is a number field (e.g. $K = \mathbb{Q}$).

Mordell-Weil theorem: For a number field K, $E(K)$ is finitely generated, i.e.

$$E(K) \simeq (\text{finite}) \times \mathbb{Z}^r$$

This will be proved in the second lecture.

Excercise: Write down a curve $E: y^2 = x^3 + Ax + B$ ($A, B \in \mathbb{Q}$) with a point $P = [x, y] \in E(\mathbb{Q})$ with rational coefficients. Compute coordinates of multiples nP for $n = 2, \ldots, 10$.

The number of digits of numerators and denominators of the coordinates of nP grows as $c \cdot n^2$ (for $c \geq 0$, $c = 0$ iff $mP = O$ for some $m > 0$). This follows from basic properties of heights, to be proved in the second lecture.

Def: For a $\mathbb{Q}$-rational point P in a projective plane $\mathbb{P}^2$ we define its height as $h(P) = \log \max(|x_0|, |x_1|, |x_2|)$, where $P = [x_0 : x_1 : x_2]$ with $x_i \in \mathbb{Z}$, $\gcd(x_0, x_1, x_2) = 1$.

If $A, B \in \mathbb{Q}$, any $\mathbb{Q}$-rational point on $E: y^2 = x^3 + Ax + B$, viewed as a point in $\mathbb{P}^2$, has a height $h(P) \in \mathbb{R}_{\geq 0}$.

The basic property of $h: E(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 0}$ is the "parallelogram law"

Thm 3 There is a constant $c = c(A, B)$ such that for all $P, Q \in E(\mathbb{Q})$

$$\left| h(P+Q) + h(P-Q) - 2h(P) - 2h(Q) \right| \leq c$$

Cor The function $\hat{h}(P) := \lim_{n \to \infty} n^{-2} h(nP)$ on $E(\mathbb{Q})$ satisfies

(i) $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$

(ii) $|h - \hat{h}|$ is bounded on $E(\mathbb{Q})$.

$\hat{h} : E(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 0}$ is called <u>canonical height</u> and is characterized by (i), (ii).

---

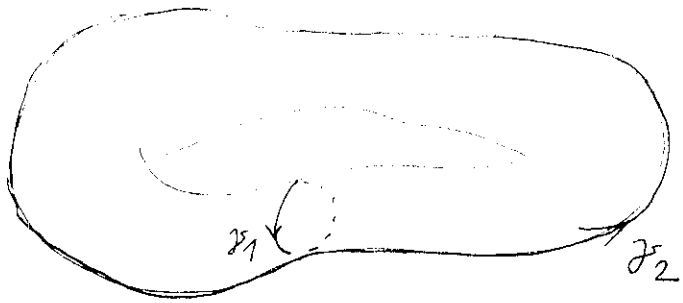
(7) Abelian integrals

Under φ, the differential $\omega = \frac{dx}{2y}$ (on E) corresponds to dz on $X = \mathbb{C}/\Gamma$. The inverse of the map $\varphi : \mathbb{C}/\Gamma \longrightarrow E(\mathbb{C})$, which should express $z \in X$ in terms of $[x, y] \in E(\mathbb{C})$, is given by integrating ω, as

$z = \int dz$: $\varphi^{-1} : E(\mathbb{C}) \longrightarrow \mathbb{C}/\Gamma$ "P" associates to $P \in E(\mathbb{C})$ the value of $\int_0^P \omega$ (mod Γ), where

$\int_0^P \omega$ denotes integral of ω along any path on $E(\mathbb{C})$ between 0 and P.

Two different paths differ by a cycle homologous to $m\gamma_1 + n\gamma_2$ $(m, n \in \mathbb{Z})$, where γ_1, γ_2 are basic cycles on $E(\mathbb{C})$:



The value of the integral then changes by $\int_{m\gamma_1 + n\gamma_2} \omega = m\omega_1 + n\omega_2 \in \Gamma$.

The formulas for the group operation on $E(\mathbb{C})$ can, therefore, be interpreted as addition formulas for $\int \omega$:

$$\int_0^{P_1} \omega + \int_0^{P_2} \omega = \int_0^{P_1 \boxplus P_2} \omega \pmod{\Gamma}$$

Similarly, on the circle, we integrate $\frac{dx}{y}$ on $x^2 + y^2 = 1$.

(8) Abstract finiteness theorem

The rest of the notes is devoted to the proof of the Mordell – Weil theorem, namely that the group of K-rational points of an elliptic curve over K (for a number field K) is finitely generated.

First we prove an abstract finiteness statement:

Suppose that A is an abelian group and $\hat{h} : A \longrightarrow \mathbb{R}_{\geq 0}$ a function, satisfying

(A) A/mA is finite for some integer $m \geq 2$

(B) $\hat{h}$ is quadratic, i.e. satisfies $(\forall x, y, z \in A)$

$$\hat{h}(x+y+z) - \hat{h}(x+y) - \hat{h}(x+z) - \hat{h}(y+z) + \hat{h}(x) + \hat{h}(y) + \hat{h}(z) = 0$$

(C) the set $\{x \in A \mid \hat{h}(x) \leq c\}$ is finite for any $c > 0$

Observe: These assumptions imply that

- $\hat{h}(nx) = n^2 \hat{h}(x)$ $\quad (n \in \mathbb{Z},\ x \in A)$
- $\langle x, y \rangle := \frac{1}{2}(\hat{h}(x+y) - \hat{h}(x) - \hat{h}(y))$ is a *bilinear* form $\langle\ ,\ \rangle : A \times A \longrightarrow \mathbb{R}$
- $\langle x, x \rangle = \hat{h}(x) \geq 0$ $\quad (x \in A)$
- $\hat{h}(x) = 0 \iff x$ is torsion, i.e. $nx = 0$ for some integer $n \geq 1$.

Thm 4 Under the assumptions (A) – (C), the abelian group A is finitely generated,

$$A \simeq A_{tors} \oplus \mathbb{Z}^r$$

Proof: Fix a set $S \subseteq A$ of representatives of A modulo mA; by (A), S is finite.

For every $P \in A$, there is a sequence of elements $P_0 = P, P_1, P_2, \ldots \in A$, such that

$$P_j = m P_{j+1} + Q_j \quad \text{for some } Q_j \in S.$$

Then

$$m^2 \hat{h}(P_{j+1}) = \langle mP_{j+1}, mP_{j+1} \rangle = \hat{h}(P_j) + \hat{h}(Q_j) - 2\langle P_j, Q_j \rangle \leq$$

$$\leq \hat{h}(P_j) + c_1 + c_2 \hat{h}(P_j)^{1/2} \qquad \text{(Cauchy-Schwarz)}$$

$$\leq (1+\varepsilon)\hat{h}(P_j) + c_3$$

(where $\varepsilon > 0$ is arbitrary, c_1, c_2 depending on A, S and c_3 depending on A, S, ε)

Taking $\varepsilon < m^2 - 1$, we get $(\forall j > 0)$

$$\hat{h}(P_j) \leq \left(\frac{1+\varepsilon}{m^2}\right)^j \hat{h}(P) + \frac{c_3}{m^2 - (1+\varepsilon)}$$

Fix any $c_4 > \frac{c_3}{m^2-(1+\varepsilon)}$. Then $\hat{h}(P_j) \leq c_4$ for all sufficiently large j, independently of the point $P \in A$ we started with.

Therefore A is generated by the set

$$S \cup \{x \in A \mid \hat{h}(x) \leq c_4\},$$ which is finite. ∎

We now have to prove that $A = E(K)$ satisfies axioms (A) – (C). For simplicity, we shall assume that $K = \mathbb{Q}$ in the sequel, but ~~although~~ this restriction is made only for convenience

(9) Weak Mordell-Weil theorem

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over $\mathbb{Q}$. Replacing $[x, y]$ by $[\alpha^2 x, \alpha^3 y]$, we can assume that $A, B \in \mathbb{Z}$. Let e_1, e_2, e_3 be roots of $x^3 + Ax + B = P(x)$.
The discriminant $\Delta = \prod_{i<j} (e_i - e_j)^2 = -4A^3 - 27B^2$
of P is always non-zero (otherwise E would be singular and $E(\mathbb{C})$ could not be homeomorphic to a torus $\mathbb{C}/\Gamma$).
We make a further assumption

(*) all roots e_1, e_2, e_3 are rational (hence integral)

The aim of this section is to prove

Thm 5 Under the assumption (*), $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

Put $$G = \{ (d_1, d_2, d_3) \mid d_i \in \mathbb{Q}^*/\mathbb{Q}^{*2},\ d_1 d_2 d_3 = 1 \in \mathbb{Q}^*/\mathbb{Q}^{*2} \} \subset (\mathbb{Q}^*/\mathbb{Q}^{*2})^{\oplus 3}$$

We define a map $f : E(\mathbb{Q}) \longrightarrow G$ by the following formulas:

$$\begin{array}{ccc} E(\mathbb{Q}) & \longrightarrow & G \\ \downarrow & & \downarrow \\ [x, y] & \longmapsto & (x-e_1,\ x-e_2,\ x-e_3) \qquad y \neq 0, \infty \\ 0 & \longmapsto & (1, 1, 1) \\ [e_1, 0] & \longmapsto & \left(\frac{1}{(e_1-e_2)(e_1-e_3)},\ e_1-e_2,\ e_1-e_3\right) \\ [e_2, 0] & \longmapsto & \left(e_2-e_1,\ \frac{1}{(e_2-e_1)(e_2-e_3)},\ e_2-e_3\right) \\ [e_3, 0] & \longmapsto & \left(e_3-e_1,\ e_3-e_2,\ \frac{1}{(e_3-e_1)(e_3-e_2)}\right) \end{array}$$

Prop 3 (1) $f : E(\mathbb{K}) \longrightarrow G$ is a homomorphism

(2) $\mathrm{Ker}(f) = 2E(\mathbb{K})$

If (1) Let $P_i = [x_i, y_i] \in E(\mathbb{K})$ satisfy $P_1 \boxplus P_2 \boxplus P_3 = 0$.

We have to prove that $f(P_1) f(P_2) f(P_3) = 1 \in G$,

i.e. $\prod_{i=1}^{3} (x_i - e_j) \in \mathbb{K}^{\times 2}$ $(\forall j = 1, 2, 3)$

(we confine ourselves to the case when $y_i \neq 0, \infty$ $\forall i$).

Indeed, let $y = \alpha x + \beta$ be the equation of the line ℓ passing through P_1, P_2, P_3.

As $E \cap \ell = \{P_1, P_2, P_3\}$, we have equality of polynomials

$$(x - e_1)(x - e_2)(x - e_3) - (\alpha x + \beta)^2 = (x - x_1)(x - x_2)(x - x_3).$$

Substitution $x = e_j$ shows that

$$\prod_{i=1}^{3} (x_i - e_j) = (\alpha e_j + \beta)^2 \in \mathbb{K}^{\times 2}.$$

(2) For $P = [x, y]$, $2P = [x_2, y_2]$ with

$$x_2 = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4y^2},$$ thus

$$(**) \qquad x_2 - e_i = \left(\frac{x^2 - 2e_i x - (A + 2e_i^2)}{2y} \right)^2,$$

which proves that $2E(\mathbb{K}) \subseteq \mathrm{Ker}(f)$.

Similarly, if $P' = [x', y'] \in \mathrm{Ker}(f)$, one can use the formula $(**)$ (plus a judicious choice of signs) to find $P = [x, y] \in E(\mathbb{K})$ s.t. $x' = x_2$, $y' = y_2$. ∎

We can now prove Thm 5. Thank to the injection $E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow G$ induced by f, it suffices to show that $\mathrm{Im}(f)$ is finite.

Let $P = [x,y] \in E(\mathbb{Q})$, $y \neq 0, \infty$. Then $x = \frac{r}{t^2}$, $y = \frac{s}{t^3}$, $\gcd(r,t) = 1$, $s^2 = (r - t^2 e_1)(r - t^2 e_2)(r - t^2 e_3)$.

Suppose that p is a prime not dividing $\Delta = \prod_{i<j} (e_i - e_j)^2$.

Then $p \nmid \gcd(r - t^2 e_i, r - t^2 e_j)$ $(i \neq j)$.

Writing $r - t^2 e_i = d_i z_i^2$ with $d_i, z_i \in \mathbb{Z} \setminus \{0\}$ d_i square-free, we see that each such p enters into the product $d_1 d_2 d_3$ with exponent 0 or 1. As $d_1 d_2 d_3$ is a square, $p \nmid d_1 d_2 d_3$, hence d_1, d_2, d_3 are divisible only by primes dividing Δ. As $f(P) = (d_1, d_2, d_3)$, this means that $f(P)$ lies in a finitely generated subgroup of G, hence $\mathrm{Im}(f)$ is finite. This finishes the proof of Thm 5. ∎

If (*) is not satisfied, the same arguments work over the field $K = \mathbb{Q}(e_1, e_2, e_3)$, with minor adjustments due to the fact that the ideal class group of K can be non-trivial.

The reason why (**) holds, i.e. why f was defined using functions $x - e_i$, is that $\mathrm{div}(x - e_i) = 2([e_i, 0]) - 2(0)$. Replacing $x - e_i$ by f_P with $\mathrm{div}(f_P) = m(P) - m(O)$, where $mP = O$, one can prove finiteness of $E(K)/mE(K)$.

(10) Heights

We proceed to the construction of a function $\hat{h} : E(\bar{\mathbb{Q}}) \longrightarrow \mathbb{R}_{\geq 0}$ satisfying (B), (C) of Sec. 8.

Recall the naive height $h : \mathbb{P}^N(\bar{\mathbb{Q}}) \longrightarrow \mathbb{R}_{\geq 0}$ of $\bar{\mathbb{Q}}$-rational points of a projective space, defined by

$$h((a_0 : \cdots : a_n)) = \log \max(|a_0|, \cdots, |a_n|)$$

$a_i \in \mathbb{Z}$, $\gcd(a_0, \cdots, a_n) = 1$.

Clearly, for any $c > 0$, the set $\{x \in \mathbb{P}^N(\bar{\mathbb{Q}}) \mid h(x) \leq c\}$ is finite.

If $i : X_{/\bar{\mathbb{Q}}} \hookrightarrow \mathbb{P}^N_{/\bar{\mathbb{Q}}}$ is an algebraic variety embedded into projective space (everything defined over $\bar{\mathbb{Q}}$), the line bundle $\mathcal{O}(1)_{\mathbb{P}^N}$ (whose global sections are homogeneous coordinates on $\mathbb{P}^N$) restricts to a line bundle $L := i^* \mathcal{O}(1)_{\mathbb{P}^N}$ on X. Such L's are called very ample. i induces, by restriction, a height $X(\bar{\mathbb{Q}}) \longrightarrow \mathbb{R}_{\geq 0}$.

Thm 6 (1) Given two embeddings $i_k : X \hookrightarrow \mathbb{P}^{N_k}$ $(k = 1, 2)$ such that $L_1 = i_1^* \mathcal{O}(1)_{\mathbb{P}^{N_1}} \simeq L_2 = i_2^* \mathcal{O}(1)_{\mathbb{P}^{N_2}}$ are isomorphic, then the corresponding heights $h_1, h_2 : X(\bar{\mathbb{Q}}) \longrightarrow \mathbb{R}_{\geq 0}$ are equivalent, i.e. $|h_1 - h_2|$ is bounded.

(Notation : $h_1 \sim h_2$. the equivalence class of heights $X(\bar{\mathbb{Q}}) \longrightarrow \mathbb{R}_{\geq 0}$ depending only on the class $[L]$ of a very ample line bundle L in $\mathrm{Pic}(X)$ is denoted by h_L)

(2) L_1, L_2 very ample $\Rightarrow$ $L_1 \otimes L_2$ is and

$$h_{L_1 \otimes L_2} \sim h_{L_1} + h_{L_2}$$

(3) There exists a unique $\mathbb{Q}$-linear map

$$\begin{array}{ccc} \mathrm{Pic}(X) \otimes \mathbb{Q} & \longrightarrow & \{\text{functions } h : X(\overline{\mathbb{Q}}) \to \mathbb{R}\} \,/\, \{\text{bounded functions}\} \\ \cup & & \cup \\ [L] \otimes 1 & \longmapsto & h_L \end{array}$$

extending $L \mapsto h_L$ for very ample line bundles L in (1).

(4) For any morphism $f : X \to Y$ of varieties over $\overline{\mathbb{Q}}$ (projective) and $L \in \mathrm{Pic}(Y) \otimes \mathbb{Q}$,

$$h_{f^*(L)} \sim h_L \circ f$$

Comments • As a $\mathbb{Q}$-vector space, $\mathrm{Pic}(X) \otimes \mathbb{Q}$ is generated by classes of very ample line bundles, hence (3) follows from (1), (2)

• (4) is sufficient to check for very ample bundles (for the same reasons), which is then immediate

The main difficulty, therefore, lies in the proof of (1), (2), for which we refer to [2], [3].

Example: $X = \mathbb{P}^1_{\mathbb{Q}}$, $x = \frac{a}{b} \in X(\mathbb{Q})$, $a, b \in \mathbb{Z}$, $\gcd(a,b) = 1$.

Then $h_{\mathcal{O}(1)}(x) = \log \max(|a|, |b|)$

The n-degree embedding $i : \mathbb{P}^1 \hookrightarrow \mathbb{P}^n$ is defined by

$$(x : y) \longmapsto (x^n : x^{n-1}y : \dots : y^n)$$

and $i^* \mathcal{O}(1)_{\mathbb{P}^n} = \mathcal{O}(n)_{\mathbb{P}^1} = \mathcal{O}(1)^{\otimes n}_{\mathbb{P}^1}$.

Thus $h_{\mathcal{O}(n)}(x) = \log \max(|a^n|, |a^{n-1}b|, \dots, |b^n|) =$

$$= \log \max(|a|^n, |b|^n) = n\, h_{\mathcal{O}(1)}(x),$$

in accordance with (2).

Let $E: y^2 = x^3 + Ax + B$ be, as before, an elliptic curve defined over $\mathbb{Q}$, L the line bundle on E associated to the divisor (0). Then $L^{\otimes 3}$ is very ample for the standard embedding $i: E \hookrightarrow \mathbb{P}^2$ given by the homogeneous coordinates $(X:Y:Z)$ with $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, since on E $\operatorname{div}(Z) = 3(0)$.

Let $h_L = \frac{1}{3} h_{L^{\otimes 3}} : E(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 0}$ be the $\frac{1}{3}$ of the naive height relative to i.

Thm 7. The function

$g(P,Q,R) := h_L(P+Q+R) - h_L(P+Q) - h_L(P+R) - h_L(Q+R) + h_L(P) + h_L(Q) + h_L(R)$
$(P,Q,R \in E(\mathbb{Q}))$ has bounded absolute value $|g|$ by a constant depending only on E.

Cor: Define, for $P \in E(\mathbb{Q})$, $\hat{h}_L(P) := \lim_{n \to \infty} \frac{1}{n^2} h_L(nP)$.
Then $\hat{h}_L : E(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 0}$ satisfies the condition (B) of Sec. 8, i.e. the corresponding function $\hat{g}(P,Q,R)$ vanishes, and the difference $|h_L - \hat{h}_L|$ is bounded on $E(\mathbb{Q})$ (thus $\hat{h}_L$ also satisfies (C) of Sec. 8, as h_L does).

To deduce Cor. from Thm 7 is an exercise in linear algebra, which is left to the audience. In view of Thm 6, the statement of Thm 7 follows from the following

Thm 9 ("Theorem of the cube") Let E be an elliptic curve. For $I \subset \{1,2,3\}$, define the map $p_I : E \times E \times E \longrightarrow E$ by $p_I(x_1,x_2,x_3) = \sum_{i \in I} x_i$. Then, for any line bundle L on E, the line bundle
$M := p_{123}^*(L) \otimes p_{12}^*(L)^{-1} \otimes p_{13}^*(L)^{-1} \otimes p_{23}^*(L)^{-1} \otimes p_1^*(L) \otimes p_2^*(L) \otimes p_3^*(L)$
on $E \times E \times E$ is trivial.

"Proof". We shall indicate a proof of Thm 9 only for elliptic curves over $\mathbb{C}$. In this case we can use analytic methods — by general principales, it suffices to check that M is trivial as a holomorphic line bundle. As M depends on L additively, it suffices to consider the case when L is the (holomorphic) line bundle associated to the divisor (a), $a \in E$. Using the map φ of Sec. 5, we shall work on the torus $X = \mathbb{C}/\Gamma$, rather than E.

Recall the Weierstrass' σ-function $\sigma: \mathbb{C} \longrightarrow \mathbb{C}$, satisfying

$$\frac{\sigma(z+\gamma)}{\sigma(z)} = \exp\left(\ell(\gamma)z + m(\gamma)\right) \qquad \forall \gamma \in \Gamma,\ \forall z \in \mathbb{C}$$

with $\ell: \Gamma \longrightarrow \mathbb{C}$ $\mathbb{Z}$-linear and

$m: \Gamma \longrightarrow \mathbb{C}$ (almost) quadratic.

The total space of the bundle L corr. to the divisor (a), $a \in \mathbb{C}/\Gamma$ is given by

$\mathbb{C} \times \mathbb{C}/\sim$, where $(z,u) \sim (z+\gamma,\ u \exp\left(\ell(\gamma)(z-a) + m(\gamma)\right))$

$(z, u \in \mathbb{C},\ \gamma \in \Gamma)$

and the projection $\mathbb{C}\times\mathbb{C}/\sim \xrightarrow{p} \mathbb{C}/\Gamma$ is simply forgetting the u-coordinate.

The formula $s: z \pmod{\Gamma} \longrightarrow (z, \sigma(z-a))$ defines a holomorphic section of p with $\mathrm{div}(s) = (a)$.

Now pass to M on $X \times X \times X$: its total space is $\mathbb{C}\times\mathbb{C}\times\mathbb{C}\times\mathbb{C}/\sim$, with

$$(z_1, z_2, z_3, u) \sim (z_1+\gamma_1,\ z_2+\gamma_2,\ z_3+\gamma_3,\ u\,\lambda(z_1, z_2, z_3, \gamma_1, \gamma_2, \gamma_3)),$$

where $\lambda(z, \gamma) = \dfrac{f(z+\gamma)}{f(z)}$, $f(z) = \dfrac{\sigma(z_1+z_2+z_3-a)\sigma(z_1-a)\sigma(z_2-a)\sigma(z_3-a)}{\sigma(z_1+z_2-a)\sigma(z_1+z_3-a)\sigma(z_2+z_3-a)}$

As both terms $\ell(y)z$, $m(y)$ are quadratic (almost) in (y,z), elementary calculation shows that $\lambda(z,x)$ is identically equal to 1, proving thus that M is a (holomorphically) trivial line bundle.

Putting all loose ends together, we obtain, finally, a proof of the Mordell - Weil theorem:

(Thm 5) $\Longrightarrow$ (A)

(B), (C) $\Longrightarrow$ Mordell - Weil (Thm 4)

$\Uparrow$ (Cor Thm 7)

(Thm 6) $\Longrightarrow$ (Thm 7)

$\Uparrow$

(Thm 8)

---

(11) Conjecture of Birch and Swinnerton-Dyer

The proof of MW does <u>not</u> give a precise structure of $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$, only an (effective) upper bound for the rank r of $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$. The torsion subgroup $E(\mathbb{Q})_{tors}$ can be computed effectively (see [4]).

The main unsolved problem is to compute r and $E(\mathbb{Q})$ effectively.

<u>L-series of E</u>: for $p \nmid \Delta$ (with possibly exception $p = 2, 3$), the curve $E: Y^2 Z = X^3 + AXZ^2 + BZ^3$ ($A, B \in \mathbb{Z}$, $\Delta = -4A^3 - 27B^2$), viewed over $\operatorname{Spec} \mathbb{Z}$, has good reduction (mod p). The number of points

(mod p) is given by the formula

$$\#E(\mathbb{Z}/p\mathbb{Z}) = p+1-\alpha_p-\overline{\alpha_p} = (1-\alpha_p)(1-\overline{\alpha_p})$$

for a suitable algebraic number α_p, such that $\alpha_p\overline{\alpha_p} = p$.

The L-series $L(E,s)$ of E is defined as

$$L(E,s) = \prod_{p\nmid\Delta} (1-\alpha_p p^{-s})^{-1}(1-\overline{\alpha_p}p^{-s})^{-1} \prod_{p\mid\Delta} (1-\varepsilon_p p^{-s})^{-1}$$

$$\varepsilon_p = 0, \pm 1$$

This product is absolutely convergent for $\mathrm{Re}(s) > \frac{3}{2}$. Conjecturally, $L(E,s)$ can be analytically continued to $\mathbb{C}$ and satisfies a functional equation relating its values at s and $2-s$. Assuming the analytic continuation around $s=1$, Birch and Swinnerton-Dyer formulated a conjecture relating the behaviour of $L(E,s)$ at $s=1$ with arithmetic of E. In its weakest form, the conjecture predicts that

$$\mathrm{ord}_{s=1} L(E,s) \overset{?}{=} r = \mathrm{rk}\,(E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}).$$

This weak conjecture has been (recently) proved for modular elliptic curves $E_{/\mathbb{Q}}$ (i.e those parametrized by modular functions on some congruence subgroup of $SL_2(\mathbb{Z})$) satisfying $\mathrm{ord}_{s=1} L(E,s)$ by Kolyvagin.

References

[1] S. Lang – Elliptic Functions, Springer, 1990

[2] S. Lang – Fundamentals of Diophantine Geometry, Springer, 1983

[3] Ju. I. Manin – Proof of the Mordell–Weil theorem, appendix to D. Mumford: Abelian Varieties, 2nd ed., Oxford,

[4] J. Silverman – Arithmetic of Elliptic Curves, GTM 105, Springer

[5] A. Weil – Elliptic Functions According to Eisenstein and Kronecker, Springer, 1976