ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

Abstract. These are notes of lectures for students given by M. Vlasenko at the Institute of Mathematics of NAS of Ukraine

1. Elliptic curve is an algebraic group

Elliptic curve is an abelian variety of dimension 1, or, what is the same, an irreducible smooth projective algebraic curve of genus 1 furnished with a point O, the origin for the group law. If we consider it over the field K of characteristics $\neq 2, 3$ it can be given by homogenous equation in 2-dimensional projective space P^2

$$y^2z = x^3 - axz^2 + bz^3 \tag{1}$$

with some $a, b \in K$. Below we consider elliptic curves over $\mathbb{C}$ or its subfields, so the characteristics is 0.

The affine piece of an elliptic curve. All 3 roots of a cubic polynomial $x^3 - ax + b$ are different iff

$$\Delta = 4a^3 - 27b^2 \neq 0.$$

Elliptic curve E is an algebraic variety defined by equation $\{y^2 = x^3 - ax + b\}$ with $4a^3 - 27b^2 \neq 0$. Let $a, b \in K$ and L is any field containing K. We can consider the set of solutions

$$E(L) = \{(x, y) \in L^2 | y^2 = x^3 - ax + b\}.$$

These are L-points of an elliptic curve E. **scise.** Draw $E(\mathbb{R})$ (suppose $a, b \in \mathbb{R}$).

Elliptic curve as a projective curve. Let $4a^3 - 27b^2 \neq 0$. Elliptic curve E is a smooth projective curve defined by the homogenous polynomial 1 .

Now $E(L) = \{[x : y : z] \in P^2(L) | y^2z = x^3 - axz^2 + bz^3\}$. We see that E is embedded into 2-dimensional projective space P^2 in this definition, and (over any field L) all but one points of $E(L)$ lie in the affine piece of $P^2(L)$ defined by $\{z \neq 0\}$. Indeed,

$$E(L) \cap \{z = 0\} = [0 : 1 : 0]$$

since $z = 0$ implies $x = 0$. Note that the point $O = [0 : 1 : 0]$ exists over any field. In previous subsection we considered the curve without this point in fact.

Below we often write E, P^2 instead of $E(\mathbb{C})$ and $P^2(\mathbb{C})$.

The group law. Exercise. Check that any line $Ax + By + Cz = 0$ in $P^2(\mathbb{C})$ intersects $E(\mathbb{C})$ at 3 points counting multiplicities.

It is known that the following rule describes an abelian group law $E \times E \to E$ with neutral element $O = [0 : 1 : 0]$. For each three points P, Q, R of intersection of any line with E we put $P + Q + R = 0$. In particular, $-[x : y : z] = [x : -y : z]$. The map $E \times E \to E$ is algebraic. Indeed,

let us show it in affine coordinates. Take $(x_i, y_i) \in E$, $i = 1, 2$. Then $(x, -y) = (x_1, y_1)+(x_2, y_2)$ should satisfy the equation $y = \frac{y_2-y_1}{x_2-x_1}(x-x_1)+y_1$ and the equation of E. So, for x we get the qubic equation

$$F(x) = x^3 - ax + b - \left(\frac{y_2 - y_1}{x_2 - x_1}(x - x_1) + y_1\right)^2 = 0,$$

and we know this is satisfied by x_1 and x_2. Then

$$-\frac{F(x)}{(x - x_1)(x - x_2)}\Big|_{x=0}$$

is the third solution, and it is now given by the rational function

$$x = \frac{\left(y_1 - \frac{y_2-y_1}{x_2-x_1}x_1\right)^2 - b}{x_1x_2}.$$

Definition 1. *An algebraic group G is an algebraic variety which is also a group, such that the inverse map $G \to G$ and the multiplication map $G \times G \to G$ are algebraic.*

We see that elliptic curve is an algebraic group. It is a smooth projective curve with an abelian group law.

2. Riemann surfaces and Riemann-Roch theorem

See e.g. [1].

3. Jacobian of an elliptic curve

Let us consider 3 types of groups.

(I) Elliptic curve $E(\mathbb{C}) = \{(x, y) \in \mathbb{C}^2 y^2 = x^3 - ax + b\} \cup \{\infty\}$ with the group law described above.

(II) The quotient $\mathbb{C}/\{\mathbb{Z}w_1 + \mathbb{Z}w_2\}$ where $w_1, w_2 \in \mathbb{C}$ with $\frac{w_1}{w_2} \in \mathbb{C} - \mathbb{R}$. Since the lattice $\{\mathbb{Z}w_1+\mathbb{Z}w_2\}$ is a subgroup of $\mathbb{C}$ w.r.t. addition the quotient is an abelian group.

(III) Riemann surface X of genus 1 with fixed point $O \in X$. Let us introduce the group law with neutral element O on X. Since we fixed a point O there is a canonical way to construct for any two points $P_1, P_2 \in X$ the third point P_3. For simplicity we assume that P_1, P_2 and O are all different. We take the divizor $D = (P_1) + (P_2)$, then the space of meromorphic functions on X with poles of order not greater than D

$$L(D) = \{f \mid div(F) + D \geq 0\}$$

has dimension 2 due to the Riemann-Roch theorem. So there is some non-constant function $f \in L(D)$. Consider $g = f - f(O)$. Since $\sum_{x\in X} Res_x g = 0$ then g has simple poles at P_i with opposite residues. Since g has no other poles, we see that g has exactly 2 zeros (counting multiplicities). So there is a well defined point $P_3 \in X$ s.t. $\mathrm{div}(g) = (O) + (P_3) - (P_1) - (P_2)$. We put $(P_3) = (P_1) + (P_2)$.

Remark. We say they all are groups, but it is not obvious that the binary operation in (I) and (III) is a group law in fact. This will follow from the theorem below, where we identify them with objects of type (II) by means of analytic isomorphisms preserving our binary operation.

Theorem 1. *For any group of any type as above there is an analytically isomorphic group of any one of other types.*

We prove it below with a serie of lemmas and exercises.

Lemma 1. $E(\mathbb{C})$ *is a torus.*

Proof. Let us check $E(\mathbb{C})$ is a smooth variety of dimension 1 over $\mathbb{C}$. Indeed, on the affine piece $\{z \neq 0\}$ the rank of $\left(\frac{\partial \Phi}{\partial x}, \frac{\partial \Phi}{\partial y}\right)$ is 1 since $x^3 - ax + b$ has no double roots. Analogously near the point $[0:1:0]$ we consider the affine piece $\{y \neq 0\}$, where for $\Phi(x,z) = x^3 - ax + b - z$ the rank of $\left(\frac{\partial \Phi}{\partial x}, \frac{\partial \Phi}{\partial z}\right)$ is 1 at $(0,0)$.

$P^2(\mathbb{C})$ is compact, so $E(\mathbb{C})$ is a compact Riemann surface. It remains to calculate its genus g. The map from $E(\mathbb{C})$ to $P^1(\mathbb{C})$ defined by $[x:y:z] \mapsto [y:z]$ is well-defined because $y = z = 0$ on E implies $x = 0$. So, it is a covering of a Riemann sphere of degree 3 (i.e. all but finite number of points have 3 preimages). To find exceptional points we look at the equation

$$X^3 - (az^2)X + (bz^3 - y^2 z) = 0.$$

If $a = 0$ all exceptional points are defined by $bz^3 - y^2 z = 0$ and each such point has 1 preimage. There are 3 such points: $[1:0]$ and $[\pm\sqrt{b}:1]$. We join them by 3 edges and calculate Euler characteristics of the preimage as $3 * 1 - 3 * 3 + 2 * 3 = 0 = 2 - 2g$, so $g = 1$. If $a \neq 0$ then the point $[1:0]$ still has 1 preimage, and 4 more points have 2 preimages each. Latter points are defined by $\left(\frac{y}{z}\right)^2 = b \pm \sqrt{\frac{27}{4}a^3}$. We join them by 5 edges, so Euler characteristics is $(1 * 1 + 4 * 2) - 5 * 3 + 2 * 3 = 0$ and $g = 1$ again. □

Exercise. Let $Ax + By + Cz = 0$ be any projective line in $P^2(\mathbb{C})$. Let $P_i = [x_i : y_i : z_i]$ for $i = 1, 2, 3$ be points of intersection with $E(\mathbb{C})$. (Suppose they all are different and different from $O = [0:1:0]$.) Construct the rational function g on $P^2(\mathbb{C})$ (a quotient of two homogenous polynomials of the same degree) with poles at P_1 and P_2 on $E(\mathbb{C})$ of order 1, and zeros at " $-P_3'' = [x_3 : -y_3 : z_3]$ and $O = [0:1:0]$.

This Exercise together with Lemma show (I)⇒(III).

The map (III)⇒(II) is the classical Abel-Jacoby map from Riemann surface to its Jacobian, which is an isomorphism if genus is 1, i.e. in our case. Due to the Riemann-Roch theorem the space of holomorhic differentials of X has dimension 1 over $\mathbb{C}$, so we pick any holomorphic differential ω. Consider for $x \in X$

$$x \in X \mapsto \int_O^x \omega.$$

The value is defined up to the integrals of ω arround the loops in X, and integrals along homotopic loops are equal. So, there is an image of $H_1(X) \cong \mathbb{Z}^2$ in $\mathbb{C}$, which is a lattice $\mathbb{Z}w_1 + \mathbb{Z}w_2$ since $H_1(X) \cong \mathbb{Z}^2$. w_1 and w_2 are integrals of ω along any two loops generating $H_1(X)$. And the map above is from X to $\mathbb{C}/\{\mathbb{Z}w_1 + \mathbb{Z}w_2\}$. Since it is an isomorphism (we don't prove this fact here) we have $\frac{w_1}{w_2} \in \mathbb{C} - \mathbb{R}$. Let us explain why it transforms one "group" law into another one. This map can be extended to divizors by

linearity:

$$D = \sum_i n_i(x_i) \mapsto \sum_i n_i \int_O^x \omega \in \mathbb{C}/\{\mathbb{Z}w_1 + \mathbb{Z}w_2\}. \tag{2}$$

Proposition 2. *The map (2) transforms principal divizors to 0.*

Proof. Let us take two differentials of third kind ω_1, ω_2 on X. Let us fix any generators γ_1, γ_2 of $H_1(X)$ on X so that they don't go through residues and poles of ω_i. We cut X along this loops, so we get a rectangle. For each differential we join poles to zeros inside of our rectangle obtaining an oriented graph which we denote by $arr(\omega_i)$. **Exercise.** Prove the formula

$$\int_{\gamma_1} \omega_1 \int_{\gamma_2} \omega_2 - \int_{\gamma_2} \omega_1 \int_{\gamma_1} \omega_2 = \pm 2\pi i \left(\int_{arr(\omega_2)} \omega_1 - \int_{arr(\omega_1)} \omega_2 \right).$$

Let g be any meromorphic function. Then $\omega_1 = \frac{dg}{g}$ is a differential of third kind and we take $\omega_2 = \omega$ to be our holomorphic differential. Then $\int_{\gamma_i} \frac{dg}{g} \in 2\pi i\mathbb{Z}$ and the above formula implies that $\int_{arr(\omega_1)} \omega \in \mathbb{Z}w_1 + \mathbb{Z}w_2$. Note that $arr(\omega_1)$ differs from the join of pathes from O to $\mathrm{div}(g)$ by a number of loops, what implies our statement. □

For the implication (II)⇒(I) we consider the Weierstrass function

$$\rho(z) = \frac{1}{z^2} + \lim_{M,N\to\infty} \sum_{m=-M}^{M} \sum_{n=-N}^{N} \frac{1}{(z + mw_1 + nw_2)^2}.$$

It is periodic w.r.t. the lattice, so giving a meromorphic functions on the quotient torus. Let us suppose for simplicity that $w_1 = \tau$, $w_2 = 1$. Then the Laurent expression of ρ at $z = 0$ starts with

$$\rho(z) = \frac{1}{z}^2 + 3G_4(\tau)z^2 + 5G_6(\tau)z^4 + \dots$$

where $G_{2k}(\tau) = \sum_{m,n} \frac{1}{(mz+n)^{2k}}$ are Eisenstein series (see [2]). Then one can easily check that

$$(\rho'(z))^2 - 4\rho(z)^3 + g_4\rho(z) + g_6 = o(z),\ z \to 0$$

with $g_4 = 60G_4(\tau)$ and $g_6 = 140G_6(\tau)$. Since there is no holomorphicfunctions on torus except constants the above expression iz 0 everywhere. So, functions $x = \rho(z)$ and $y = \rho'(z)$ are coordinates on elliptic curve. To prove that this map transforms group law into group law one needs to construct a periodic analytic function whith zeros exactly at z_1, z_2 and poles exactly at 0 and $z_1 + z_2$. (**Exercise.**)

Now our theorem is proved.

4. The endomorphism ring of an elliptic curve. Complex multiplication.

Let E_1, E_2 be elliptic curves. $Hom(E_1, E_2)$ is the set of algebraic maps from E_1 to E_2 which intertwin group laws. Then $Hom(E_1, E_2)$ is an abelian group (we can add such maps pointwise). $End(E) = Hom(E, E)$is a ring

with composition as multiplication. Note that always $\mathbb{Z} \subset End(E)$ where for $n > 0$

$$n : x \mapsto x + x + \cdots + x$$

(n times), -1 means inverse and 0 maps everything to 0.

By $Hom_{an}(\cdot,\cdot)$ and $End_{an}(\cdot)$ we denote corresponding hom's in category of analytic spaces.

We denote $E_\tau = \mathbb{C}/\{\mathbb{Z}\tau+\mathbb{Z}\}$ for τ in upper halfplane. Due to Theorem (1) for every elliptic curve there is an analytic isomorphism to one of E_τ. We now see how easy one can describe Hom of two elliptic curves in analytic category.

Proposition 3.

$$Hom_{an}(E_\tau, E_{\tau'}) \cong \{\alpha \in \mathbb{C} \mid \alpha(\mathbb{Z}\tau + \mathbb{Z}) \subset \mathbb{Z}\tau' + \mathbb{Z}\}$$

Proof. Any analytic map $f : E_\tau \to E_{\tau'}$ can be lifted to the analytic map of universal coverings $\bar{f} : \mathbb{C} \to \mathbb{C}$ with $\bar{f}(0) = 0$. Then for $\lambda \in \mathbb{Z}\tau + \mathbb{Z}$ we have $g(z) = \bar{f}(z + \lambda) - \bar{f}(z)$ is an analytic function with values in discrete set $\mathbb{Z}\tau' + \mathbb{Z}$, hence it is constant. Thus f is a linear map $f(z) = \alpha$. Obviously every such a map with α as in the statement intertwins group laws. □

Evidently $Hom(E_1, E_2) \subset Hom_{an}(E_1, E_2)$, since every algebraic map is analytic. But in case of projective varieties we can state the converse! This is due to the Theorem of Chow which allows to pass between analytic and algebraic categories:

Theorem 2. *(Chow) An analytic subset of a projective space which is closed in the strong topology is algebraic.*

By strong topology we mean usual topology on $P^n(\mathbb{C})$ restricted from $\mathbb{C}^{n+1}$. This theorem implies that $Hom(E_1, E_2) = Hom_{an}(E_1, E_2)$. So,

$$End(E) = \{\alpha \in \mathbb{C} \mid \alpha(\mathbb{Z}\tau + \mathbb{Z}) \subset \mathbb{Z}\tau + \mathbb{Z}\}.$$

This means that every algebraic map $E \to E$ preserves group law (see the proof of the Proposition above).

Exercise. Show that E_τ and $E_{\tau'}$ are isomorphic as complex manifolds if and only if $\tau = g\tau'$ for some $g \in SL_2(\mathbb{Z})$, or equivalently $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ are isomorphic if and only if lattices Λ and Λ' are homotetic. Show that under isomorphism of E_τ and $E_{g\tau}$ the numbers in $End(E_\tau)$ go to the same numbers in $End(E_{g\tau})$.

Thus we have embedding $\mathbb{Z} \subset End(E) \subset \mathbb{C}$, although τ is defined nonuniquely (up to the action of $PSL_2(\mathbb{Z})$). Any algebraic endomorphism of E can be canonically represented by a complex number.

Exercise. Show that $End(E_\tau) \neq \mathbb{Z}$ iff τ is a quadratic irrationality.

So, generically $End(E) = \mathbb{Z}$. Let us consider the case when τ is quadratic irrationality. Let $K = \mathbb{Q}(\tau)$.

Exercise. Show that if $\alpha \in End(E)$ then $\alpha \in O_K$, i.e. it satisfies monic equation with integer coefficients.

So, $End(E) \subset O_K$. It is known from algebraic number theory (see [3]) that there exist $w \in O_K$ s.t. $O_K = \mathbb{Z} + w\mathbb{Z}$. For $K = \mathbb{Q}(\sqrt{d})$ where d is a square free negative integer we put $w = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$ and $w = \sqrt{d}$ if $d \equiv 2, 3 \pmod 4$.

Exercise. Show that $End(E)$ is of finite index in O_K. (Use that $O_K = \mathbb{Z}+w\mathbb{Z}$ and $End(E) \neq \mathbb{Z}$.) Show that there exists $f \in \mathbb{Z}$ such that $End(E) = \mathbb{Z} + fO_K$.

This f is called a conductor of an elliptic curve E.

Theorem 3. *Let $R_f = \mathbb{Z} + fO_K$ for an imaginary quadratic field K and $f \in \mathbb{Z}$. There exists a finitely many nonisomorphic elliptic curves E with $End(E) = R_f$.*

Sketch of proof. See [4]. Let $Cl(R_f)$ be the group of (isomorphism classes) of projective modules of rank 1 over R_f. Then the elliptic curves with given endomorphism ring R_f correspond one to one (up to isomorphism) with $Cl(R_f)$. The last group is known from algebraic number theory to be finite. (For $f = 1$ this is the class group of the field K.) Correspondence is given by $\mathbb{C}/\Lambda \longleftrightarrow \Lambda$. □

5. Algebraicity of j-invariant

Theorem 4. *If τ in upper half-plane is quadratic then $j(\tau) \in \overline{\mathbb{Q}}$.*

Proof. E_τ is isomorphic to the elliptic curve

$$y^2 = 4x^3 - g_4(\tau)x - g_6(\tau).$$

Let $\sigma \in Aut(\mathbb{C})$ be any automorphism of $\mathbb{C}$ over $\mathbb{Q}$. For the curve $E = \{y^2z = x^3 - axz^2 + bz^3\}$ we put $E^\sigma = \{y^2z = x^3 - a^\sigma xz^2 + b^\sigma z^3\}$. Then $j(E^\sigma) = j(E)^\sigma$ since $j(E) = 1728\frac{4a^3}{4a^3-27b^2}$. Note that $End(E^\sigma) = End(E)$ since all endomorphisms of E are described by rational fuctions and we simply act on their coefficients to get endomorphisms of E^σ and vice versa. Now due to Theorem 3 there is only finitely many $\sigma \in Aut(\mathbb{C})$ s.t. $j(\tau)^\sigma \neq j(\tau)$. So $j(\tau) \in \overline{\mathbb{Q}}$. □

References

[1] J.S.Milne, Modular functions and modular forms // notes for Math 678, University of Michigan, Fall 1990 (download from http://www.jsmilne.org)

[2] A.Weil, Elliptic functions according to Eisenstein and Kronecker // Springer-Verlag, 1976

[3] U. Neukirch, Algebraic number theory // Springer-Verlag, 1999

[4] J.-P.Serre, Complex multiplication // in Algebraic Number Theory, ed. J.W.S.Cassels, A.Frohlich, Academic Press, 1967, p. 292-296

[5] D.Zagier, Aspects of complex multiplication // notes of the seminar written by J. Voight (2000) http://www.ima.umn.edu/ voight/notes/274-Zagier.pdf