Algebraic number theory: elliptic curves

These are notes of lecture course on elliptic curves in the Independent University of Moscow in Spring 2016 based on books [13], [9], [4], [7]. If you have any questions or comments, please write to daryaschedrina@gmail.com

Aknowledgements. I am very grateful to IUM for hospitality and help, and to Michael Rosenblum for numerous helpful comments.

1 Lecture 1: basic definitions

1.1 Brief history

The first appearance of elliptic curves is in "Arithmetica" by Diophantus: To divide a given number into two numbers such that their product is a cube minus its side. We call the sum of them a given number a and then we have to find x and y, s. t. $y(a-y) = x^3 - x$. This is a curve of degree 3 and a line intersects it in three points counted with multiplicities, so if we construct one rational point we can obtain some other by building tangent lines or lines through two points. Later this method will grow up to an "Additional law" on a curve. In these lectures we will come to more explicit

Definition 1.1. *An elliptic curve is a smooth, projective algebraic curve of genus one with a specified point O.*

Sometimes more general definition is used: any algebraic curve of genus one. Or another definition we will work with: it is a curve defined by an equation of the form $y^2 = P(x)$, where P is a polynomial of degree 3. Developing of theory of elliptic curves depends on a field k, where we look at E defined over k, for example one may work with rational numbers, real numbers, complex numbers, fields of finite characteristic in particular of char 2 or 3.

In this course we will discuss geometry of elliptic curves, theory over finite fields and over complex numbers and also connection to modular forms and class field theory.

Elliptic curves were used in the proof of Fermats Last Theorem by Andrew Wiles. They also find applications in elliptic curve cryptography and integer factorization.

1.2 Affine algebraic varieties

We begin with theory of *algebraic curves* — by definition projective varieties of dimension one. Most of definitions are taken from book by J. Silverman [13]

Notation: K is a perfect field (not necessarily algebraically closed)

V/K means that V is defined over K.

Reminders: affine n-space over K is $\mathbb{A}^n(K) = \{P = (x_1, ..., x_n) : x_i \in K\}$. Let $K[X] = K[X_1, ..., X_n]$ and $I \subset K[X]$ is an ideal. For I we define $V_I = \{P \in \mathbb{A}^n(K) \,|\, f(P) = 0 \, for \, all \, f \in I\}$ and call it an affine algebraic set. For an algebraic set V we have $I(V) = \{f \in K[X] : f(P) = 0 \, for \, all \, P \in V\}$ the ideal of V. A related problem is Hilbert Nullstellensatz:

Proposition 1.2. *Here we need K — algebraically closed. For any ideal J in $K[X]$ we have $I(V_J) = \mathrm{rad}(J)$.*

Exercise 1.3. *Play with definitions (here K is not necessarily algebraically closed):*

1. $V_{I(W)} \supset W$,
2. $I(V_I) \supset I$,
3. $W_1 \subset W_2 \Rightarrow I(W_1) \supset I(W_2)$,
4. $I_1 \subset I_2 \Rightarrow V_{I_1} \supset V_{I_2}$,
5. $I(V_{I(W)}) = I(W)$,
6. $V_{I(V_I)} = V_I$.

For any ideals $I_1, I_2 \subset K[X]$ and any subsets $V_1, V_2 \subset \mathbb{A}^n$

1. $V_{I_1+I_2} = V_{I_1} \cap V_{I_2}$;
2. $V_{I_1 \cap I_2} = V_{I_1} \cup V_{I_2}$;
3. $I(V_1 \cup V_2) = I(V_1) \cap I(V_2)$;
4. $I(V_1 \cap V_2) = \mathrm{rad}(I(V_1) + I(V_2))$.

Example 1.4. *An algebraic set $V : X^n + Y^n = 1$ defined over $\mathbb{Q}$. Famous problem is to prove that for $n \geq 3$ we have $V(\mathbb{Q}) = \{(1, 0), (0, 1)\}$ if n is odd and $V(\mathbb{Q}) = \{(\pm 1, 0), (0, \pm 1)\}$ if n is even.*

Now suppose that V is an irreducible (means that V can't be written as the union of nonempty algebraic varieties) affine variety, defined by an ideal I in $K[x_1, ..., x_n]$ we define its *coordinate ring* $K[V] = K[X]/I(V)$.

For $\overline{K}$ is algebraical closure of K we define the dimension of V as the transcendence degree of $\overline{K}(V)$ over $\overline{K}$ and denote it as $\dim(V)$.

Exercise 1.5. *Prove that* $\dim(\mathbb{A}^n) = n$.

Definition 1.6. *For a point $P \in V$ and a set of generators $\{f_i\}_{1\leq i\leq m}$ of $I(V)$ in $\overline{K}[X]$ we say that V is nonsingular at P if the $m \times n$ matrix*

$$\Big(\frac{\partial f_i}{\partial X_j}(P)\Big)_{1\leq i\leq m, 1\leq j\leq n}$$

has rank $n - \dim V$. We call V smooth, if it is nonsingular at every point.

Note that for another set of generators $\{g_i\}_{1\leq i\leq m}$ of $I(V)$ in $\overline{K}[X]$ the rank of

$$\Big(\frac{\partial g_i}{\partial X_j}(P)\Big)_{1\leq i\leq m, 1\leq j\leq n}$$

will be the same (we just multiply by a $m \times m$-matrix of full rank).

Now we look at another approach to smoothness. For every point $P \in V$ over an algebraically closed K we define an ideal $m_P = \{f \in K[V] : f(P) = 0\}$. We have an isomorphism $K[V]/m_P \to K$, defined by $f \mapsto f(P)$, so m_P is a maximal ideal. We know that m_P/m_P^2 is a finite-dimensional K-vector space. We will also use

Exercise 1.7. *Prove that a point $P \in V$ is nonsingular iff* $\dim_{m_P/m_P^2} = \dim V$ *[4].*

Now we define $K[V]_P$ the local ring of V at P, or a localization of $K[V]$ at $m_P = \{F \in K(V) : F = f/g$, where $f, g \in K[V]$ and $g(P) \neq 0\})$,

Denote by M_P the maximal ideal of $\overline{K}[V]_P$.

1.3 Projective algebraic varieties

Definition 1.8. *Projective n-space over a field K is the set of $(n+1)$-tuples $(x_0, ..., x_n) \in \mathbb{A}^{n+1}$, such that at least one of $x_i \neq 0$ modulo an equivalence* *relation defined as follows* $(x_0, ..., x_n) \sim (y_0, ..., y_n)$ *if there exists* $\lambda \neq 0 \in K$ *s. t.* $x_i = \lambda y_i$ *for any* i. *An equivalence class containing* $(x_0, ..., x_n)$ *is denoted* $[x_0, ..., x_n]$ *or* $(x_0 : ... : x_n)$.

We call a polynomial $f \in K[X]$ *homogeneous of degree* d if $f(\lambda x_0, ..., \lambda x_n) = \lambda^d f(x_0, ..., x_n)$ for any $\lambda \in K^*$.

An ideal $I \subset K[X]$ is homogeneous if it is generated by homogeneous polynomials.

Definition 1.9. *A projective algebraic set is any set of the form* $V_I = \{P \in \mathbb{P}^n : f(P) = 0\}$ *for all* $f \in I$, *where* I *is a homogeneous ideal.*

For a projective algebraic set V we define its ideal $I(V)$ as generated by homogeneous polynomials $\{f \in K[X]; f(P) = 0\}$ for all $P \in V$.

For the case when K is not algebraically closed we first define V over closure $\overline{K}$ and then say that V is defined over K if ideal $I(V)$ can be generated by homogeneous polynomials in $K[X]$. The set of K-rational points of V is $V(K) = V \cap \mathbb{P}^n(K)$.

An obvious example of projective algebraic set is a hyperplane in $\mathbb{P}^n$ defined by an equation $a_0X_0 + ... + a_nX_n = 0$, where not all of a_i are zero.

Exercise 1.10. *Solve exercise 1.3 for projective varieties.*

Example 1.11. *Let* $K = \mathbb{Q}$ *a field of rational numbers. Then a point of* $\mathbb{P}^n(\mathbb{Q})$ *is of the form* $(x_0 : ... : x_n)$, *where* $x_i \in \mathbb{Q}$. *We can find such* $\lambda \in \mathbb{Q}$ *that multiplying by* λ *we kill denominators and common factors of* x_i*'s. It means that we can find a representation of* $(x_0 : ... : x_n)$ *where all* $x_i \in \mathbb{Z}$ *and* $\mathrm{gsd}(x_0, ..., x_n) = 1$.

So to describe V_I *for homogeneous ideal* I *generated by* f_i, $1 \leq i \leq m$ *we need to find all solutions of the system* $f_i(X) = 0, 1 \leq i \leq m$ *in relatively prime integers.*

Exercise 1.12. *Describe projective algebraic sets* $V_1 : x^2 + y^2 = 3z^2$ *and* $V_2 : x^2 + y^2 = 5z^2$ *over* $\mathbb{Q}$, *(difficult*)* $V_3 : 3x^3 + 4y^3 + 5z^3 = 0$ *(Selmer's counterexample to Hasse principle).*

Now we want to define projective closure for affine variety.

Definition 1.13. *A projective algebraic set is called a projective variety if if it's ideal* $I(V)$ *is prime in* $\overline{K}[X]$.

We denote by $\phi_i : \mathbb{A}^n \to \mathbb{P}^n$ a corresponding inclusion defined by

$$(y_1, ..., y_n) \mapsto (y_1 : ... : y_{i-1} : 1 : y_{i+1} : ... : y_n).$$

We denote by H_i the hyperplane in $\mathbb{P}^n$ defined as

$$H_i = \{P = (x_0 : ... : x_n) \in \mathbb{P}^n \,|\, x_i = 0\},$$

and $U_i = \mathbb{P}^n \setminus H_i$ is the complement of H_i.

We define a bijection $\phi_i^{-1} : U_i \to \mathbb{A}^n$ as a map

$$(x_0 : ... : x_n) \mapsto \Big(\frac{x_0}{x_i}, ..., \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, ..., \frac{x_n}{x_i}\Big).$$

We can divide by x_i here because of definition of U_i.

Exercise 1.14. *For a projective algebraic set V with ideal $I(V)$ prove that $V \cap \mathbb{A}^n$ defined as $\phi_i^{-1}(V \cap U_i)$ for fixed i, is an affine algebraic set with ideal $I(V \cap \mathbb{A}^n) = \{f(y_1 : ... : y_{i-1} : 1 : y_{i+1} : ... : y_n) \,|\, f(x_0 : ... : x_n) \in I(V)\}$.*

Sets U_i for $1 \le i \le n$ cover whole $\mathbb{P}^n$, so projective variety V is covered by affine varieties $V \cap U_i$ for $1 \le i \le n$.

Conversely we define $f^*(x_0 : ... : x_n) = x_i^d f(\frac{x_0}{x_i}, ..., \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, ..., \frac{x_n}{x_i})$, where $d = \deg f$.

Definition 1.15. *Now let V be an affine algebraic set with ideal $I(V)$. Then the projective closure of V denoted by $\overline{V}$ is a projective algebraic set with homogeneous ideal $I(\overline{V})$ generated by $\{f^*(X) \,|\, f \in I(V)\}$.*

Proposition 1.16. *1 For an affine variety V its corresponding projective variety $\overline{V}$ satisfies $V = \overline{V} \cap \mathbb{A}^n$.*

2 For a projective variety V its corresponding affine variety $V \cap \mathbb{A}^n = \emptyset$ or $V = \overline{V \cap \mathbb{A}^n}$.

3 If an affine variety V is defined over K, then projective also, and reverse.

Now we use this definition of projectivization to define some properties of V in terms of $V \cap \mathbb{A}^n$.

Definition 1.17. *For a projective variety V/K we look at $\mathbb{A}^n \subset \mathbb{P}^n$ s. t. $V \cap \mathbb{A}^n$ is nonempty. Then we define the dimension of V as the dimension of $V \cap \mathbb{A}^n$. The function field $K(V)$ of V is the function field of $V \cap \mathbb{A}^n$.*

If for chosen $P \in V$ our $\mathbb{A}^n$ contains P, then we say that V is nonsingular at P if $V \cap \mathbb{A}^n$ is nonsingular at P.

The local ring $K[V]_P$ is the local ring of $V \cap \mathbb{A}^n$ at P. A function $f \in K(V)$ is regular at P if $f \in K[V]_P$.

Now we want to describe the function field of $V(\overline{K})$, where V is a projective variety. It is defined as the field of rational functions $F(X) = \frac{f(X)}{g(X)}$ such that f and g are homogeneous of the same degree, g is not contained in $I(V)$, we identify functions $\frac{f_1}{g_1}$ and $\frac{f_2}{g_2}$ if $f_1g_2 - f_2g_1 \in I(V)$.

We are going to talk about maps between projective varieties. For two projective varieties V_1 and $V_2 \in \mathbb{P}^n$ a rational map $\phi : V_1 \to V_2$, defined by $\phi = (f_1 : ... : f_n)$ where for all $f_i \in \overline{K}(V_1)$ defined in P we have that $\phi(P) = (f_1(P) : ... : f_n(P)) \in V_2$.

The difficulty is that a rational map is not necessarily defined at every point of V_1. We call a rational map $\phi = (f_1 : ... : f_n) : V_1 \to V_2$ is defined at $P \in V_1$ if here is a function $g \in \overline{K}(V_1)$ such that any gf_i is regular at P and there exists i s.t. $(gf_i)(P) \neq 0$. then we define $\phi(P) = ((gf_1)(P) : ... : (gf_n)(P))$.

Now we look at the case when $V_1 \subset \mathbb{P}^m$ and $V_2 \subset \mathbb{P}^n$ are projective varieties. If necessary we multiply a rational map $\phi = (f_1 : ... : f_n)$ by a homogeneous polynomial that kills denominators of the f_i.

Definition 1.18. 1. *A rational map $\phi = (f_1 : ... : f_n) : V_1 \to V_2$, where not all of f_i are in $I(V_1)$, f_i are homogeneous of the same degree. And for every $g \in I(V_2)$ we have $g(f_1 : ... : f_n) \in I(V_1)$.*

2. *A rational map $\phi = (f_1 : ... : f_n) : V_1 \to V_2$ is regular at P, if there exist homogeneous polynomials $\psi_0, ...\psi_n \in \overline{K}[X]$ such that*

1. *$\psi_0, ...\psi_n$ have the same degree;*
2. *$f_i\psi_j = f_j\psi_i (\mod I(V_1))$ for all $0 \leq i, j \leq n$;*
3. *$\psi_i(P) \neq 0$ for some i.*

Then we define $\phi(P) = (\psi_1(P) : ... : \psi_n(P))$.

We call two varieties V_1 and V_2 isomorphic, if there are morphisms $\phi : V_1 \to V_2$ and $\psi : V_2 \to V_1$ such that their compositions $\psi \circ \phi$ and $\phi \circ \psi$ are identities on V_1 and V_2.

Example 1.19. *We look at varieties $V : y^2z = x^3 = x^2z$ and $\mathbb{P}^1$ with coordinates $(s : t)$ and rational maps $\psi : \mathbb{P}^1 \to V$ and $\phi : V \to \mathbb{P}^1$, defined as $\psi(s : t) = ((s^2 - t^2)t : (s^2 - t^2)s : t^3)$ and $\phi(x : y : z) = (y : x)$. In this example ψ is a morphism, but φ is not defined at $(0 : 0 : 1)$, where V has singularity.*

1.4 Exercises

Exercise 1.20. *For following affine varieties find their singular points, projectivizations and singular points on them:*

1. $y^2 = x^3$;
2. $y^2 = x^4 + y^4$;

Exercise 1.21. *Let $V \subset \mathbb{P}^n$ be a variety, given by a single homogeneous polynomial $f \in K[X]$. Prove that $P \in V$ is a singular point iff $\frac{\partial f}{\partial x_0}(P) = ... = \frac{\partial f}{\partial x_n}(P) = 0$.*

Exercise 1.22. *For projective varieties V_1, V_2, which are defined over a field K we call $G_K = \mathrm{Gal}(\overline{K}/K)$ the absolute Galois group and define its action on a rational map $\phi : V_1 \to V_2$ by*

$$\phi^\sigma(P) = (f_0^\sigma(P) : ... : f_n^\sigma(P)),$$

then we have $\phi(P)^\sigma = \phi^\sigma(P^\sigma)$ for all $\sigma \in G_K$ and $P \in V_1$.

We say that ϕ is defined over K if there exists $\lambda \in \overline{K}^*$ such that $\lambda f_0, ..., \lambda f_n \in K(V_1)$.

1. *Let V be an affine variety over a field K. Show that $K[V] = \{f \in \overline{K}[V] \,|\, f^\sigma = f\}$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$.*
2. *For projective space $\mathbb{P}^n(K) = \{P \in \mathbb{P}^n(\overline{K}) \,|\, P^\sigma = P\}$ for all $\sigma \in G_K = \mathrm{Gal}(\overline{K}/K)$;*
3. *Let $\phi : V_1 \to V_2$ be a rational map of projective varieties. Prove that ϕ is defined over K iff $\phi^\sigma = \phi$ for all $\sigma \in G_K$.*

Exercise 1.23. *Let $K = \mathbb{F}_q$ be a finite field and $V \subset \mathbb{P}^n$ is a projective variety. Prove that $\phi : (x_0 : ... : x_n) \mapsto (x_0^q : ... : x_n^q)$ is a bijection of sets V. But is it an isomorphism of algebraic varieties? Show that $V(\mathbb{F}_q) = \{P \in V \mid \phi(P) = P\}$.*

2 Lecture 2: curves, divisors, differentials

In this lecture we will use theory of algebraic varieties developed in the first lecture for the case of algebraic curve — a variety of dimension 1. First we remind useful facts from lecture 1.

C/K is smooth irreducible projective curve defined over a field K.

$K(C)$ is the function field of C over K; $I(C)$ — the ideal in $K[X]$ of polynomials equal to 0 at all points of C.

For a point $P \in C$ we define the local ring of C at P by $K[C]_P$ and its maximal ideal M_P.

Proposition 2.1. *The local ring $K[C]_P$ is DVR (discrete valuation ring).*

Proof. The only thing left to prove, that it is a principal ideal domain, since there is a unique maximal ideal M_P. It is enough to prove that M_P is principal which is equivalent to $\dim_K M_P/M_P^2 = 1 = \dim C$. Note that a statement like this can only be true for curves. □

Definition 2.2. *For a point $P \in C$ we define the normalized valuation* $\mathrm{ord}_P : K[C]_P \to \{0, 1, 2, ...\} \cup \{\infty\}$ *by* $\mathrm{ord}_P(f) = \sup\{d \in \mathbb{Z} : f \in M_P^d\}$. *Then we extend* ord_P *to $K(C)$ by* $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$. *We will call a function $t \in K(C)$ a uniformizer at P if the order of t at P is* $\mathrm{ord}_P(t) = 1$.

For a function $f \in K(C)$ we say that f is defined at P if $\mathrm{ord}_P(f) \geq 0$, if $\mathrm{ord}_P(f) > 0$ we say that f has a zero at P and if $\mathrm{ord}_P < 0$ then it has a pole.

Proposition 2.3. *Let C be a curve and $f \neq 0 \in K(C)$. Then there are only finitely many zeroes and poles of f on C.*

The proof of statement about finiteness of number of poles follows from an algebraic geometry exercise. To prove it for zeroes we may look at $1/f$.

Proposition 2.4. *Let P be a smooth point on a curve C and t be the corresponding uniformizer. Then $K(C)$ is finite separable extension of $K(t)$.*

Proof. We give a sketch of proof. The field $K(C)$ is finitely generated over K and has transcendence degree 1, since t not in K we have that $K(C)$ is finite algebraic extension of $K(t)$.

Next for $x \in K(C)$ we have to prove that it is separable over $K(t)$. Assume that it's not. We may look only at characteristic p fields, since all extensions in characteristic zero are separable. We choose a minimal polynomial $\psi(x)$ of x over $K(t)$ as a polynomial of two variables x and t, then conclude to the case when it is a polynomial of x^p and t. If $\psi(x,t)$ contains a term $q_{i,j}t^i x^j$ where $j \not\equiv 0(\mod p)$, then $\frac{\partial q(t,x)}{\partial x} \neq 0$, so x is separable over $K(t)$, so we may assume that $\psi(x,t) = \psi(x^p,t)$.

Then regroup coefficients of $\psi(t,x^p)$ with powers of $t \mod p$ using perfectness of field K like $\psi(t,x^p) = \sum_{k=0}^{p-1}(\sum_{i,j} a_{i,j,k}t^{ip}x^{jp})t^k = \sum_{k=0}^{p-1}\phi_k(t,x)^p t^k$.

We have $\psi(t,x) = 0$, but counting of orders of each summand give us $\text{ord}_P(\phi_k(t,x)^p t^k) = p\text{ord}_P(\phi(t,x)) + k\text{ord}_P(t) \equiv k(\mod p)$. So all $\phi_k(t,x) = 0$, but then since one of them includes x and have less degree than ψ we get a contradiction. □

2.1 Maps between curves

We will use the statement that a rational map $\phi : C \to V$ from a curve to projective variety is regular at smooth points.

Proposition 2.5. *Let C_1 be a smooth irreducible projective curve over a field K, C_2 is an irreducible curve over K and $f : C_1 \to C_2$ is a morphism defined everywhere. Then $f(C_1)$ is either a point on C_2, or $f(C_1) = C_2$ in this case $K(C_1)$ is a finite extension of the field $K(C_2)$.*

Proof. The image of C_1 under f is closed subset in C_2 as an image of closed set (this is a difficult for this moment statement which we should believe). Also the image $f(C_1)$ is irreducible, so either $f(C_1)$ is a point or $f(C_1)$ is all C_2. In the second case we use the fact that it defines an inclusion of function fields $K(Y) \subset K(X)$ (here for a morphism $\phi : C_1 \to C_2$ we have a morphism $\phi^* : K(C_2) \to K(C_1)$ is the composition $\phi^* f = f \circ \phi$). Both these fields are finitely generated and have transcendence degree 1 over K, so $K(C_1)$ is a finite extension of the field $K(C_2)$. □

Proposition 2.6. *Let C_1 and C_2 be curves defined over a field K.*

1. *Let $\iota : K(C_2) \to K(C_1)$ be an injection of fields fixing K. Then there exists unique nonconstant $\phi : C_1 \to C_2$ s.t. $\phi^* = \iota$.*

2. *Let $k \subset K(C_1)$ be a subfield of finite index containing K. Then there exists a smooth curve C'/K, unique up to K-isomorphism and a nonconstant map $\phi : C_1 \to C'$ s.t. $\phi^* K(C') = k$.*

For the first statement we take $\phi = (1 : \iota(g_1) : ... : \iota(g_n))$ where $g_i \in K(C_2)$ is the function on C_2 corresponding to x_i/x_0.

The second statement follows from equivalence of categories
{Objects: *smooth projective curves*,
maps: *dominant morphisms*;}
{Objects: *function fields of transcendence degree* 1 *over K*,
maps: *K-homomorphisms*}.

Now we define a degree of rational map:

Definition 2.7. *Let $\phi : C_1 \to C_2$ be a map of curves defined over K. The degree of any constant map is zero, if ϕ is not constant then we call it finite morphism and its degree* $\deg \phi = [K(C_1) : \phi^* K(C_2))]$*. We call a map separable, or purely inseparable if $K(C_1) : \phi^* K(C_2))$ has corresponding property. Separable degree is denoted* $\deg_s \phi$ *and inseparable* $\deg_i \phi$.

Here we have for an extension of fields K/L a tower $K \supset F \supset L$, where F/L is separable and K/F is purely inseparable, then a separable degree is $[F : L]$ and inseparable is $[K : F]$ for extensions corresponding to a morphism we get in such a way its separable and inseparable degree.

Now we want to define a map $\phi_* : K(C_1) \mapsto K(C_2)$ by $\phi_* = (\phi^*)^{-1} \circ \mathrm{N}_{K(C_1):\phi^* K(C_2))}$ (here the norm map is the product of all conjugant elements $\mathrm{N}_{L/K}(a) = \prod_{g \in \mathrm{Gal}(L/K)} g(a)$).

Proposition 2.8. *Let $\phi : C_1 \to C_2$ be a map of smooth curves s.t.* $\deg \phi = 1$*. Then ϕ is an isomorphism.*

Proof. First we note that ϕ^* is an isomorphism of function fields. Next we look at $(\phi^*)^{-1} : K(C_1) \to K(C_2)$, by 2.6 there exists a unique morphism $\psi : C_2 \to C_1$, s.t. $\psi^* = (\phi^*)^{-1}$. Then the $(\phi \circ \psi)^* = \psi^* \circ \phi^*$ is the identity on $K(C_1)$ and $(\psi \circ \phi)^* = \phi^* \circ \psi^*$ is the identity on $K(C_2)$ then $\phi \circ \psi$ is identity on C_2 and $\psi \circ \phi$ is identity on C_1. □

Fact 2.9. *We have the equivalence of following categories: $\{$ Objects: smooth curves defined over K, maps defined over $K\}$ and*

$\{$Objects: finitely generated extensions k/K of transcendence degree 1 s.t. $k \cap \overline{K} = K$, maps: field injections fixing $K\}$.

Now we define a ramification index of a map.

Definition 2.10. *Let $\phi : C_1 \to C_2$ be a nonconstant map of smooth curves and let $P \in C_1$. The ramification index of ϕ at P is $e_\phi(P) = \operatorname{ord}_P(\phi^* t_{\phi(P)})$, where $t_{\phi(P)} \in K(C_2)$ is a uniformizer at $\phi(P)$. We call ϕ unramified at P if $e_\phi(P) = 1$.*

Proposition 2.11. *Let $\phi : C_1 \to C_2$ be a nonconstant map of smooth curves.*

1. *For every $Q \in C_2$, $\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi$;*
2. *For all but finitely many $Q \in C_2$ a number of elements in $\phi^{-1}(Q) = \deg_s(\phi)$;*
3. *Let $\psi : C_2 \to C_3$ be another nonconstant map of smooth curves. Then for all $P \in C_1$*
$$e_{\psi\circ\phi}(P) = e_\phi(P) e_\psi(\phi P).$$

Proof. 1. Let $V = \operatorname{Spec} B$ be an open affine neighborhood of Q in C_2, A is an integral closure of B in $K(C_1)$. Then $U = \operatorname{Spec} A$ is an open subset of $\phi^{-1}V$ in C_1. Denote m_Q the maximal ideal of Q in B and localize A and B with respect to multiplicative system $B - m_Q$. We get an extension of rings $\mathcal{O}_Q \hookrightarrow A'$. Here we use another notation $\mathcal{O}_Q$ is just a local ring at a point $K[C]_Q$.

Here A' is torsion-free and has rank $r = [K(C_1) : \phi^* K(C_2)] = \deg \phi$. Denote t_Q a local parameter in the point Q, then $A'/t_Q A'$ is a K-vector space of dimension r.

On the other hand points P_i s.t. $\phi(P_i) = Q$ are in one-to-one correspondence with maximal ideals m_i of A', so by $A'_{m_i} = \mathcal{O}_{P_i}$ and $t_Q A' = \cap_i (t_Q A'_{m_i} \cap A')$ and chineese remainder theorem we get

$$\deg \phi = r = \dim_K A'/t_Q A' = \sum_i \dim_K A'/(t_Q A'_{m_i} \cap A') = \sum \operatorname{ord}_{P_i}(\phi^* t_Q).$$

2. Roughly speaking an inseparable degree of a morphism does not influence a number of pre-images of a given point. Intuitively the statement is natural: inseparable degree is a "degree of a monom" which have a zero, this gives us multiplicity but not more points. Distinct points could be obtained from polynom without multiple roots like for separable extensions. Explicitly statement follows from the part of proof of (1) about one-to-one correspondence of points and ideals and local statements.

3. For uniformizers t_Q and $t_{\psi Q}$ the functions $t_Q^{e_\psi(\phi P)}$ and $\psi^* t_{\psi Q}$ have the same order in Q. Now take ϕ^* of them and orders at P.

□

Corollary 2.12. *From second statement a map $\phi : C_1 \to C_2$ is unramified iff number of points in $\phi^{-1}(Q) = \deg \phi$.*

2.2 char K = p

Here we discuss the Frobenius map. Let $q = p^r$.

We define for a polynomial $f \in K[X]$ its $f^{(q)}$ as the polynomial obtained from f by raising each coefficient to qth power.

Next we define for a curve C corresponding $C^{(q)}$ as a curve associated to a homogeneous ideal $I(C^{(q)})$:=genereted by $\{f^{(q)} : f \in I(C)\}$.

The *Frobenius morphism* $\mathrm{F} : C \to C^{(q)}$, $\mathrm{F}(x_0 : ... : x_n) = (x_0^q : ... : x_n^q)$.

Exercise 2.13. *Show that* F *is well defined. You need to prove that its image is contained in $C^{(q)}$.*

Proposition 2.14. *Let K be a perfect field,* char$K = p$*, $q = p^r$, C — a curve over K, and $\mathrm{F} : C \to C^{(q)}$ the qth power Frobenius morphism.*

1. $\mathrm{F}^* K(C^{(q)}) = K(C)^{(q)} = \{f^q : f \in K(C)\}$.

2. F *is purely inseparable;*

3. $\deg \mathrm{F} = q$.

Proof. 1. by definition $\mathrm{F}^* K(C^{(q)})$ is the subfield of $K(C)$ given by $\mathrm{F}^* \left(\frac{f}{g}\right) = \frac{f(x_0^q,...,x_n^q)}{g(x_0^q,...,x_n^q)}$. Now use perfectness of K.

2. follows from 1 by definition.

3. assume that there is a smooth point $P \in C(K)$ (or take an extension). Let t be a uniformizer in P, then $K(C)$ is separable over $K(t)$. We look at extensions $K(C)^q(t)/K(t)$ and $K(C)^q(t)/K(C)^q$. then we get $K(C) = K(C)^q(t)$, so $\deg \mathrm{F} = [K(C)^q(t) : K(C)^q]$. To prove that $[K(C)^q(t) : K(C)^q] = q$ is an exercise.

□

Corollary 2.15. *Any map $\psi : C_1 \to C_2$ of smooth curves over a field of characteristic p factors as $C_1 \xrightarrow{\mathrm{F}} C_1^{(q)} \xrightarrow{\lambda} C_2$, here $q = \deg_i(\psi)$ and λ is separable map.*

Proof. First look at a separable closure K' of $\psi^* K(C_2)$ in $K(C_1)$. Then $K(C_1)/K'$ is purely inseparable of degree q, so $K(C_1)^q \subset K'$. We have $K(C_1)^q = \mathrm{F}^*(K(C_1^{(q)}))$ and $[K(C_1) : \mathrm{F}^*(K(C_1^{(q)}))] = q$. Then conclude that $K' = \mathrm{F}^*(K(C_1^{(q)}))$, so we have $K(C_1)/\mathrm{F}^* K(C_1^{(q)})/\psi^* K(C_2)$ which corresponds to $C_1 \xrightarrow{\mathrm{F}} C_1^{(q)} \xrightarrow{\lambda} C_2$. □

2.3 Divisors

Definition 2.16. *A divisor D on a curve C is a formal sum $D = \sum_{P \in C} n_p(P)$, for $n_P \in \mathbb{Z}$ and P are closed points, for all but finitely many $P \in C$ we have $n_P = 0$.*

The degree of a divisor is $\deg D = \sum_{P \in C} n_P$.

All divisors on curve form a free abelian group, generated by divisors (P) which we denote by $\mathrm{Div}(C)$, it has a subgroup $\mathrm{Div}^0(C)$ of divisors with zero degree.

Definition 2.17. *Let C be a smooth curve and $f \in \overline{K}(C)$. We define a divisor of f by $\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P)$.*

So we can define a homomorphism of abelian groups $\mathrm{div} : K(C)^* \to \mathrm{Div}(C)$

We call a divisor $D \in \mathrm{Div}(C)$ *principal* if it is of the form $D = \mathrm{div}(f)$, and we have an equivalence relation $\sim$ defined by $D_1 \sim D_2$ if $D_1 - D_2$ is principal. We call a *Picard group* a divisor class group $\mathrm{Pic} = \mathrm{Div}(C)/\sim$.

For a nonconstant map $f : C_1 \to C_2$ of smooth curves we define corresponding maps of divisor groups $f^* : \mathrm{Div}(C_2) \to \mathrm{Div}(C_1)$ and $f_* : \mathrm{Div}(C_1) \to$

$\mathrm{Div}(C_2)$ corresponding as following:

$$(Q) \mapsto \sum_{P \in f^{-1}(Q)} e_f(P)(P) \qquad (P) \mapsto (fP).$$

Here for a divisor D such that $\mathrm{div}(f)$ and D have disjoint supports (support of something is where it is nonzero) we have a definition: $f(D) = \prod_{P \in C} f(P)^{n_P}$.

Proposition 2.18. *Let $f : C_1 \to C_2$ be a nonconstant map of smooth curves. Then*

1. *for all $D \in \mathrm{Div}(C_2)$ we have $\deg(f^*D) = (\deg f)(\deg D)$;*
2. *for all $g \in \overline{K}(C_2)^*$ we have $f^*(\mathrm{div} g) = \mathrm{div}(f^*g)$;*
3. *for all $D \in \mathrm{Div}(C_1)$ we have $\deg(f_*D) = \deg D$;*
4. *for all $g \in \overline{K}(C_1)^*$ we have $f_*(\mathrm{div} g) = \mathrm{div}(f_*g)$;*
5. *$f_* \circ f^*$ acts on $\mathrm{Div}(C_2)$ as multiplication by $\deg f$;*
6. *for a nonconstant map $g : C_2 \to C_3$ we have $(g \circ f)^* = f^* \circ g^*$ and $(g \circ f)_* = g_* \circ f_*$.*

Proof. Statements 1., 5., 6 follow from 2.11. Second statement reduces to prove that $\mathrm{ord}_P(f^*g) = e_f(P)\mathrm{ord}_{fP}(g)$, which is left as an exercise. Fourth reduces to $\mathrm{ord}_Q(f_*g) = \sum_{P \in \phi^{-1}(Q)} e_f(P)\mathrm{ord}_P(g)$. □

Proposition 2.19. *For a smooth curve C and $f \in K(C)^*$*
$\mathrm{div}(f) = 0$ *iff* $f \in K^*$*;*
$\deg(\mathrm{div}(f)) = 0$.

Proof. First follows from the statement that if $\mathrm{div}(f) = 0$, than f has no poles, so the corresponding map $f : C \to \mathbb{P}^1$ is not surjective, so it is constant.

Here we use the rational morphism defined as following: for a function $f \in K(C)$ we have $f : C \to \mathbb{P}^n$ defined as $P \mapsto (f(P) : 1)$.

Second statement: if $f \in K$ it's obvious, so we may assume $f \notin K$, then an inclusion of fields $K(f) \hookrightarrow K(C)$ induce a finite morphism $\phi : C \to \mathbb{P}^1$, then $(f) = \phi^*((\{0\}) - (\{\infty\}))$ and since degree of divisor $(\{0\}) - (\{\infty\})$ on $\mathbb{P}^1$ is zero we conclude that $\deg \mathrm{div}(f) = 0$. □

Example 2.20. *On $\mathbb{P}^1$ every divisor of degree 0 is principal. Let $D = \sum n_P(x_P : y_P) \in \mathbb{P}^1$, we look at function $\prod_{P \in \mathbb{P}^1}(y_P X - x_P Y)^{n_P}$.*

2.4 Differentials

Definition 2.21. *Let V be a variety. We define the space Ω_V of differential forms on V as the $\overline{K}(V)$-vector space, generated by symbols $\mathrm{d}f$ for $f \in \overline{K}(V)$ with relations:*

(i) $\mathrm{d}(f+g) = \mathrm{d}f + \mathrm{d}g$ *for all* $f, g \in \overline{K}(V)$*;*

(ii) $\mathrm{d}(fg) = g\mathrm{d}f + f\mathrm{d}g$ *for all* $f, g \in \overline{K}(V)$*;*

(iii) $\mathrm{d}a = 0$ *for all* $a \in \overline{K}$*.*

Proposition 2.22. *Let C be a curve. Then Ω_C is a 1-dimensional $\overline{K}(C)$-vector space. For an element $f \in \overline{K}$ we have $\mathrm{d}f$ is a basis for Ω_C iff $\overline{K}(C)/\overline{K}(f)$ is a finite separable extension.*

Let $\phi : C_1 \to C_2$ be a nonconstant map of curves. We define corresponding map on differentials $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ by $\phi^*(\sum f_i \mathrm{d}g_i) = \sum(\phi^* f_i)\mathrm{d}(\phi^* g_i)$.

Corollary 2.23. *From previous proposition we deduce that a nonconstant map of curves $\phi : C_1 \to C_2$ is separable iff corresponding $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ is injective.*

Proof. We choose $f \in \overline{K}(C_2)$ s.t. $\Omega_{C_2} = \overline{K}(C_2)\mathrm{d}y$, from proposition $\overline{K}(C_2)/\overline{K}(f)$ is separable extension, so $\phi^*\overline{K}(C_2)$ is separable over $\phi^*\overline{K}(f) = \overline{K}(\phi^* f)$. Then ϕ^* is injective $\Leftrightarrow \mathrm{d}(\phi^* f) \neq 0 \Leftrightarrow \mathrm{d}(\phi^* f)$ is a basis for $\Omega_{C_1} \Leftrightarrow \overline{K}(C_1)/\overline{K}(\phi^* f)$ is separable $\Leftrightarrow \overline{K}(C_1)/\phi^*\overline{K}(C_2)$ is separable, the last from the tower of separable extensions. □

Proposition 2.24. *Let C be a curve, $P \in C$ a point and $t_P \in \overline{K}(C)$ a uniformizer at P.*

1. *For any $\omega \in \Omega_C$ there exists a unique $f \in \overline{K}(C)$, depending on ω, t_P s.t. $\omega = f\mathrm{d}t_P$.*

2. *If $f \in \overline{K}(C)$ is regular at P, then $\frac{\mathrm{d}f}{\mathrm{d}t_C}$ is also regular at P.*

3. *Let $\omega \neq 0 \in \Omega_C$, then $\mathrm{ord}_P(\omega/\mathrm{d}t) =: \mathrm{ord}_P(\omega)$ does not depend on the choice of uniformizer.*

4. *Let $\mathrm{char}K = p$, $f, g \in \overline{K}(C)$ s.t. $g(P) = 0$. Then $\mathrm{ord}_P(f\mathrm{d}g) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g) - 1$, if $p = 0$ or $p \nmid \mathrm{ord}_P(g)$, and $\mathrm{ord}_P(f\mathrm{d}g) \geqslant \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$, if $p > 0$ and $p \mid \mathrm{ord}_P(g)$.*

5. *Let $\omega \neq 0 \in \Omega_C$, then* $\mathrm{ord}_P(\omega) = 0$ *for all but finitely many* P.

Here, after a lot of time, lecture 2 ends. I would ask you to read the end of this lecture and solve exercises for it.

Proof.

3. For another uniformizer t' we know from 2. that $\frac{\mathrm{d}t'}{\mathrm{d}t}$ and $\frac{\mathrm{d}t}{\mathrm{d}t'}$ are regular at P. We have $\omega = g\mathrm{d}t' = g(\frac{\mathrm{d}t'}{\mathrm{d}t})\mathrm{d}t$, so $\mathrm{ord}_P(\frac{\mathrm{d}t'}{\mathrm{d}t}) = 0$.

4. computation for $g = ut_P^n$ with $\mathrm{ord}_P(u) = 0$.

5. We take $f \in \overline{K}(C)$ s.t. $\overline{K}(C)/\overline{K}(x)$ is separable and represent $\omega = g\mathrm{d}f$. We know that a map $f : C \to \mathbb{P}^1$ ramifies at only finitely many points of C. We look at all other and pay attention to $P \in C$ s.t. $g(P) \neq 0$, $g(P) \neq \infty$, $f(P) \neq \infty$ and $f : C \to \mathbb{P}^1$ is unramified at P. Then $f - f(P)$ is a uniformizer at P, so $\mathrm{ord}_P(\omega) = \mathrm{ord}_P(g\mathrm{d}(f - f(P))) = 0$. □

Now we define a divisor for a differential form ω by $\mathrm{div}(\omega) = \sum_{P\in C} \mathrm{ord}_P(\omega)(P) \in \mathrm{Div}(C)$, we call $\omega \in \Omega_C$ regular if $\mathrm{ord}_P(\omega) \geqslant 0$ for all $P \in C$, and nonvanishing if $\mathrm{ord}_P(\omega) \leqslant 0$.

Since Ω_C is a 1-dimensional $\overline{K}$-vector space we have for nonzero differentials $\omega_1, \omega_2 \in \Omega_C$ the existence of a function $f \in \overline{K}(C)^*$ s.t. $\omega_1 = f\omega_2$, so $\mathrm{div}(\omega_1) = \mathrm{div}(f) + \mathrm{div}(\omega_2)$.

Definition 2.25. *The canonical divisor of C is an element of canonical divisor class — the image in* $\mathrm{Pic}(C)$ *of* $\mathrm{div}(\omega)$ *for any nonzero* $\omega \in \Omega_C$.

For example there are no holomorphic differentials on $\mathbb{P}^1$. We take a coordinate function t on $\mathbb{P}^1$, and see that for all $a \in \overline{K}$ the function $(t - a)$ is a uniformizer at a, so $\mathrm{ord}_a(\mathrm{d}t) = \mathrm{ord}_a(\mathrm{d}(t - a)) = 0$. This works everywhere except ∞, here we have a unifomizer $1/t$, so $\mathrm{ord}_\infty(\mathrm{d}t) = \mathrm{ord}_\infty(-t^2\mathrm{d}(1/t)) = -2$. For every nonzero $\omega \in \Omega_{\mathbb{P}^1}$ we have $\deg \mathrm{div}(\omega) = \deg \mathrm{div}(\mathrm{d}t) = -2$, so ω is not holomorphic.

Another useful for us example is about a curve C given by an equation $y^2 = (x - e_1)(x - e_2)(x - e_3)$, then $\mathrm{div}(\mathrm{d}x) = (P_1) + (P_2) + (P_3) - 3(P_\infty)$. We know that $\mathrm{d}x = \mathrm{d}(x - e_i) = x^2\mathrm{d}(1/x)$, so $\mathrm{div}(\frac{\mathrm{d}x}{y}) = 0$.

2.5 Exercises

Exercise 2.26. *Let R be a Noetherian local ring that is not a field, m — its maximal ideal, and $k = R/m$ its residue field. Show that following conditions are equivalent:*

1. *R is discrete valuation ring;*
2. *m is principal;*
3. $\dim_{m/m^2} = 1$.

Exercise 2.27. *A generalization of an exercise from previous lecture. Let C be a curve in $\mathbb{P}^2$ given by an equation $x^2 + y^2 = pz^2$.*

1. *Prove that C is isomorphic to $\mathbb{P}^1$ over $\mathbb{Q}$ iff $p \equiv 1(\mod 4)$;*
2. *Prove that if $p \equiv 3(\mod 4)$ than all these curves are not isomorphic to each other and to $\mathbb{P}^1$.*

Exercise 2.28. *Prove statement (3.) from 2.11*

Exercise 2.29. *Try to prove proposition 2.18. If there are any questions about this proposition you can ask me.*

Exercise 2.30. *Let C be a smooth curve over a field K and $P \in C(K)$. Prove that $K(C)$ contains a uniformizer at P (that there exists a uniformizer at P, defined over K).*

Exercise 2.31. *Let C be smooth irreducible curve over field of characteristic $p > 0$ and $t \in K(C)$. Prove that for almost all points $P \in C$ a function $t - t(P)$ is a uniformizer at P and $t \notin K(C)^p$.*

Exercise 2.32. *Related to note after definition 2.17. Let ϕ be nonconstant map of smooth curves. Prove that following two equalities are true if well defined:*

1. *$f(\phi^* D) = (\phi_* f)(D)$ for all $f \in \overline{K}(C_1)^*$ and $D \in \mathrm{Div}(C_2)$;*
2. *$f(\phi_* D) = (\phi^* f)(D)$ for all $f \in \overline{K}(C_2)^*$ and $D \in \mathrm{Div}(C_1)$;*

3 Lecture 3: The Riemann-Roch theorem

One can define a partial order on $Div(C)$ by $D_1 \geq D_2$ if $D_1 - D_2 \geq 0$. Here we say that a divisor D is effective or $D = \sum n_P(P) \geq 0$ if all $n_P \geq 0$.

To a divisor D we associate a finite-dimensional vector space $\mathcal{L}(D) = \{f \in \overline{K}(C)^* : \operatorname{div}(f) + D \geq 0\} \cup \{0\} = \{f \in K(C) \,|\, \forall P \in C \quad \nu_P(f) + n_P \geq 0\}$. By $l(D)$ we denote the dimension of $\mathcal{L}(D)$ over $\overline{K}$.

Exercise 3.1. *Show that $\mathcal{L}(D) = 0$ if $D < 0$. For principal divisor* $\operatorname{div}(f)$ *construct an isomorphism $\mathcal{L}(D) \xrightarrow{\sim} \mathcal{L}(D + (f))$.*

Proposition 3.2. *The set $\mathcal{L}(D)$ is a finite-dimensional $\overline{K}$-vector space.*

Proof. Assume that $D \geq 0$, otherwise $\mathcal{L}(D) = 0$. The proof is by induction on number of points in divisor's support: assume that $D = P + E$, where $E \geq 0$ and P is a point on C.

There are two cases: first if $D = \sum n_{P_i} P_i + P$ and $D = \sum n_{P_i} P_i$, second more difficult is when $E = n_P P + ...$, $D = (n_P + 1)P + ...$ In both cases we have an inclusion $\mathcal{L}(E) \hookrightarrow \mathcal{L}(D)$.

In first case we define a morphism $\phi : \mathcal{L}(D) \to \overline{K}$ by $f \mapsto (ft_P)(P)$, where t_P is a uniformizer at P. In the second case for $f \in \overline{K}(C)$ we define a morphism $\phi_P : \mathcal{L}(D) \to \overline{K}$ by $f \mapsto (ft_P^{n_P+1})(P)$. Then we have an exact sequence of vector spaces: $0 \to \mathcal{L}(E) \to \mathcal{L}(D) \to \overline{K}$. So when we add a point to a divisor, dimension of corresponding vector space grows not more than 1. □

Example 3.3. *Let $K_C = $* $\operatorname{div}(\omega)$ *be a canonical divisor on C, then for any function $f \in \mathcal{L}(K_C)$ we have* $\operatorname{div}(f) \geq -\operatorname{div}(\omega)$*, so* $\operatorname{div}(f\omega) \geq 0$*, therefore $f\omega$ is holomorphic. The converse is also true: if the differential $f\omega$ is holomorphic, then $f \in \mathcal{L}(K_C)$. Every differential on C is of the form $f\omega$ for some f, so we have an isomorphism of $\overline{K}$-vector spaces: $\mathcal{L}(K_C)$ and the space of holomorphic $\{\omega \in \Omega_C\}$. Denote the dimension of these spaces as $l(K_C)$.*

Now we are going to prove the fundamental result from theory of projective curves — The Riemann-Roch theorem:

Theorem 3.4. *Let C be a smooth projective curve and K_C be a canonical divisor on C. Then there exists an integer $g \geq 0$, such that for every divisor*

$D \in \mathrm{Div}(C)$ *we have*

$$l(D) - l(K_C - D) = \deg(D) - g + 1.$$

To prove this theorem we need to discuss some new constructions. we will just rewrite Weil's proof in [6] Remind the notation for a point $P \in C$ we have its local ring $K[C]_P$ and maximal ideal M_P. By proposition 2.1 we know that $K[C]_P$ is a discrete valuation ring, therefore we can introduce a discrete valuation on its field of fractions. We define here a residue field $K(P) = K[C]_P/M_P$, which is isomorphic to K in the case of algebraically closed field.

Definition 3.5. *A discrete valuation on a field F is a function $\nu : F \to \mathbb{Z} \cup \{\infty\}$ with following properties for any $x, y \in F$:*

1. $\nu(x \cdot y) = \nu(x) + \nu(y)$;
2. $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$;
3. $\nu(x) = \infty \Leftrightarrow x = 0$.

Take a DV on the ring $K[C]_P$ from definition 2.2, which can be extended to the field $\mathrm{Frac}(K[C]_P)$. We will work with completion of this field with respect to a valuation defined by a point $P \in C$. One may look at the local ring $K[C]_P$ as $\{f \in K(C) \,|\, \mathrm{ord}_P(f) \geq 0\}$, then the completion of $K[C]_P$ is $\widehat{K[C]_P} = \varprojlim_n K[C]_P/M_P^n$. We set $K_P = \mathrm{Frac}(\widehat{K[C]_P})$.

We can describe the completion of the field as following: let t be a generator of maximal ideal $K[C]_P$ and $x \in K[C]_P$, then there exist a constant $a_0 \in K$, for which we have: $x \equiv a_0 \mod M_P$. Then the function $x - a_0 \in M_P$ and we have $x - a_0 = tx_0$ then do the same operation to x_0, get $x_0 - a_1 = tx_1$ and we obtain an expansion of x into power series: $x = a_0 + a_1 t + a_2 t^2 + ...$ which depends only on P.

Lets look at fraction field K' of $K[C]_P$, by extension of discrete valuation to K' we can embed K' into a field of power series $K((t))$, we denote the correspondent to P field of power series as K_P. And represent any element of $\xi \in K_P$ as $\xi = \sum_{i=-m}^{\infty} a_i t^i$. Where $m = \mathrm{ord}_P(\xi)$.

One of the main construction is adelic ring (it is a topological ring, so we may think about it as a topological vector space).

Let A' be the cartesian product $\prod_{P\in C} K_P$, where each element can be viewed as an infinite vector $\xi = (..., \xi_P, ...)$. Then we restrict this product under conditions: we want to work with a subring

$$\mathbb{A}_C = {\prod_{P\in C}}' K_P = \left\{(\xi_P) \in \prod_{P\in C} K_P \mid \text{for almost all } P \in C : \xi_P \in \widehat{K[C]_P}\right\}$$

called a ring of adeles. And we have a diagonal embeddings $K(C) \hookrightarrow \mathbb{A}_C$ namely $x \mapsto (x, ...x, ...)$ and the constant field $K \hookrightarrow \mathbb{A}_C$.

For a divisor D we define the subset

$$\mathbb{A}(D) = \{\xi \in \mathbb{A}_C, \mid \text{such that} \, \mathrm{ord}_P \xi_P + \mathrm{ord}_P(D) \geq 0\},$$

and see that $\mathbb{A}(D)$ is a K-subspace of $\mathbb{A}_C$.

Note that the set of all parallelotopes $\mathbb{A}(D)$ define topology on $\mathbb{A}_C$ as a fundamental system of neighborhoods. Also there is a good exercise on definitions to understand that $\mathbb{A}(D) \cap K(C) = \mathcal{L}(D)$.

Our main aim is to describe the space $\mathbb{A}_C/(K(C) + \mathbb{A}(D))$ as a parallelotope for some divisor depending on D, find its dimension over K and deduce the main theorem.

We want to define differential adeles: First we need to define differentials for $\widehat{K[C]_P}$ as Kahler differentials $\Omega_{\widehat{K[C]_P}/K}$ and for a field K_P as $\Omega_{K_P/K}$.

Here $\Omega_{A/B}$ are Kahler differentials for ring A containing B, they are defined in the same way as the space of differentials for an algebraic variety — modulo relations over B.

Then we have the same statement as proposition 1 for our definition of of differentials:

Proposition 3.6. *The space $\Omega_{K_P/K}$ is one-dimensional space over K_P and a basis is $\mathrm{d}t$, where t is generator of the maximal ideal in $K[C]_P$.*

As a consequence from the proposition one can represent any element of $\Omega_{K_P/K}$ as $\sum_{i=-m}^{\infty} a_i t^i \mathrm{d}t$. Then we can define a residue map

$$\mathrm{res}_P : \Omega'_{\widehat{K_P}/K} \to K(P), \quad \sum_{i=-m}^{\infty} a_i t^i \mathrm{d}t \mapsto a_{-1}.$$

Next step is definition of differential adeles:

$$\Omega_{\mathbb{A}_C} = {\prod_{P\in C}}' \Omega_{K_P} = \left\{(\omega_P) \in \prod_{P\in C} \Omega_{K_P} \mid \text{for almost all } P \in C : \omega_P \in \Omega_{\widehat{K[C]_P}/K}\right\}.$$

And analogically to the case of usual adeles we define the space of differential adeles for divisor D.

$$\Omega_{\mathbb{A}_C}(D) = \{(\omega_P) \in \Omega_{\mathbb{A}_C}, | \text{ such that}\, \mathrm{ord}_P\omega_P + \mathrm{ord}_P(D) \geq 0\},$$

Then for any divisor of differential form $(\omega) = \sum_{P\in C}\mathrm{ord}_P(\omega)P$ we define a map $\mathbb{A}_C \overset{\sim}{\to} \Omega_{\mathbb{A}_C}$ by multiplication on ω pointwise, which sends $K(C)$ to $\Omega_{K(C)}$. What we need from this map is that it defines an isomorphism $\mathcal{L}(D+(\omega)) \overset{\sim}{\to} \Omega_{K(C)} \cap \Omega_{\mathbb{A}_C}(D)$.

Definition 3.7. *A pairing $\mathbb{A}_C \times \Omega_{\mathbb{A}_C} \to K$ defined by $\langle (f_P), (\omega_P)\rangle = \sum_{P\in C}\mathrm{Tr}_{K(P)/K}\mathrm{res}_P(f_p\omega_P)$ is correctly defined and non-degenerate. Here we work with algebraically closed field, so we assume that $K(P) = K$ and the formula is $\langle (f_P), (\omega_P)\rangle = \sum_{P\in C}\mathrm{res}_P(f_p\omega_P)$.*

If we take a non-degenerate pairing $V \times W \to k$ then any element $w \in W$ defines a homomorphism from V to k by $v \mapsto v \times w$. Here we say that pairing $\varphi : V \times W \to k$ is non-degenerate if for any element $v \in V$ a morphism $\varphi_v : W \to k$ vanishes for all $w \in W$, then $v = 0$ and analogical statement is true for elements of W.

The fact about pairing that it is correctly defined follows from adelic condition, which means that for almost all $P \in C$ we have $\mathrm{res}_P(f_P\omega_P) = 0$. The statement about non-degenerateness follows from properties of residue map. We discuss here only the case of non-degenerateness for $\mathbb{A}_C$, the case for Ω_{A_C} is similar. Take any element $(f_P) \in \mathbb{A}_C$ and look at map $\langle (f_P), *\rangle :$ $\Omega_{A_C} \to k$ defined by $(\omega_P) \mapsto \sum_{P\in C}\mathrm{res}_P(f_P\omega_P)$. If we have that $(\omega_P) \mapsto 0$ for any $(\omega_P) \in \Omega_{A_C}$ than $(f_P) = 0$. If it's not so, than take P, such that $f_P = ut_P^n$, where u is a unit in $K[C]_P$ and correspondent adele in Ω_{A_C} such that $(\omega_P) = (0, ..., t_P^{-n-1}\mathrm{d}t_P, 0...)$ than $\langle (f_P), (\omega_P)\rangle \neq 0$.

Lemma 3.8. *The pairing $K_P \times \Omega_{K_P} \to K$ obtained as*

$$\langle f_P, \omega_P\rangle = \mathrm{Tr}_{K(P)/K}\mathrm{res}_P(f_P\omega_P)$$

defines an isomorphism $\Omega_{K_P} \simeq Hom_K(K_P, K)$.

For a maximal ideal $(M_P^n)^\perp = (M_P^{-n})\Omega_{K_P}$.

This lemma is the local statement which holds for any local field $K = k((t))$ (complete DV field, whose residue field is finite k).

Corollary 3.9. *From lemma follows two global statements:*

Here for a pairing $V \times W \to k$ we denote by $V^{\perp}$ a subspace of W of the elements $\{w\,\text{such that for any}\,v \in V\,\text{we have}\,v \times w \mapsto 0.\}$

1. $\mathbb{A}_C(D)^{\perp} = \Omega_{\mathbb{A}_C}(-D)$;

2. $K(C)^{\perp} = \Omega_{K(C)}$.

Proof.

1. If for a divisor D an element $(\omega_P) \in \mathbb{A}_C(D)^{\perp}$, then (and inverse implication is true) for any P we have $\omega_P \in (M_P^{n_P})^{\perp}$ and by the second statement of lemma we get what need.

2. exercise: first prove the inclusion $\Omega_{K(C)} \subseteq K(C)^{\perp}$, then inverse inclusion.

□

From developed theory there are two important consequences:

Theorem 3.10. *For a divisor D on a curve C and a canonical divisor $K_C = (\omega)$, $\omega \in \Omega_{K(C)}$ if the dimension of space $\mathbb{A}_C/(K(C) + \mathbb{A}_C(D))$ is finite, then we have an isomorphism of vector spaces over K*

$$\mathrm{Hom}_K(\mathbb{A}_C/(K(C) + \mathbb{A}_C(D)), K) \simeq \mathcal{L}(K_C - D).$$

Proof. First we observe that by recent result (about a map of multiplication by (ω)) we have that $\mathcal{L}(K_C - D) \simeq \Omega_K(C) \cap \Omega_{\mathbb{A}_C}(-D)$. Then we have by previous corollary that $\Omega_K(C) \cap \Omega_{\mathbb{A}_C}(-D) = K(C)^{\perp} \cap \mathbb{A}_C(D)^{\perp}$. So the thing left to prove is $\mathrm{Hom}_K(\mathbb{A}_C/(K(C) + \mathbb{A}_C(D)), K) \simeq K(C)^{\perp} \cap \mathbb{A}_C(D)^{\perp}$.

We should note that by this property any element from $K(C)^{\perp} \cap \mathbb{A}_C(D)^{\perp}$ defines a morphism from $\mathbb{A}_C$ to K, which is zero on elements from $(K(C) + \mathbb{A}_C(D))$. So we got an inclusion $K(C)^{\perp} \cap \mathbb{A}_C(D)^{\perp} \subseteq \mathrm{Hom}_K(\mathbb{A}_C/(K(C) + \mathbb{A}_C(D)), K)$, by non-degenerateness of pairing we have that this inclusion is an isomorphism. □

Now we are going to Riemann-Roch theorem.

Proof. of the theorem 3.4 So we have the following data: $\mathcal{L}(D) = \mathbb{A}_C(D) \cap K(C)$; $\dim_K \mathcal{L}(D) = l(D)$;

$\mathcal{L}(K_C - D) = \mathrm{Hom}_K(\mathbb{A}_C/(K(C) + \mathbb{A}_C(D)), K)$; $\dim_K \mathcal{L}(K_C - D) = l(K_C - D)$;

First we understand that RR is true for the case $D = 0$. Then add a point P to a divisor D and look at two sides of equality: $l(D) - l(K_C - D) = \deg(D) + 1 - g$. Righthand side, we denote it by $\delta(D)$ grows by 1, we should prove the same for left, $l(D) - l(K_C - D) = \chi(D)$. Here we use adelic description of $\mathcal{L}(D)$.

Therefore we have to prove that for divisors $D = E + P$, E only one of the following is true:

- $\mathcal{L}(D) = \mathcal{L}(E) \oplus K$;
- $\mathrm{Hom}_K(\mathbb{A}_C/(K(C)+\mathbb{A}_C(D)), K) \oplus K = \mathrm{Hom}_K(\mathbb{A}_C/(K(C)+\mathbb{A}_C(E)), K)$ and $\mathcal{L}(D) = \mathcal{L}(E)$;

Since we assume that $\mathbb{A}_C/(K(C) + \mathbb{A}_C(D))$ is a finite-dimensional vector space, than we may look only at the space $K(C) + \mathbb{A}_C(D)$, then second statement becomes: $K(C) + \mathbb{A}_C(D) = (K(C) + \mathbb{A}_C(E)) \oplus K$.

Assume that we have $l(D) = l(E) + 1$, then lets prove that $K(C) + \mathbb{A}_C(D) = K(C) + \mathbb{A}_C(E)$. There exists a function $f \in K(C)$, such that $\mathcal{L}(D) = \mathcal{L}(E) + \langle f \rangle$ as spaces over K. Assume that $K(C) + \mathbb{A}_C(D)$ is bigger and take an element $g + (h_Q) \in K(C) + \mathbb{A}_C(D)$, such that $g + (h_Q) \notin K(C) + \mathbb{A}_C(E)$, then there exists $\alpha \in K$, such that $(h_Q - \alpha f) \in \mathbb{A}_C(E)$. Since $(h_Q) \in \mathbb{A}_C(D) \setminus \mathbb{A}_C(E)$, so for all $Q \neq P$ it satisfy conditions defined by divisor E, the only exception is for h_P in point P. So we just take a function f from assumption, which also have big enough pole at P and suitable α to get an adele $(h_Q - \alpha f) \in \mathbb{A}_C(E)$, then an element $g + (h_Q) = g + \alpha f + (h_Q - \alpha f) \in K(C) + \mathbb{A}_C(E)$.

Second part: now assume that $\mathcal{L}(D) = \mathcal{L}(E)$, then we need to prove that $K(C) + \mathbb{A}_C(D) = (K(C) + \mathbb{A}_C(E)) \oplus K\langle(f_Q)\rangle$ as K-vector spaces. Let $D = (n_P + 1)P + ...$ and $E = n_P P + ...$, then take any element $g + (h_Q) \in K(C) + \mathbb{A}_C(E)$ and for $g + (h'_Q) \in (K(C) + \mathbb{A}_C(D)) \setminus (K(C) + \mathbb{A}_C(E))$ we take for all $Q \neq P$ the same h_Q, but for P take $h'_P = h_P + t_P^{-n_P - 1}$, where t_P is the uniformizer at P. Then, since $\mathcal{L}(D) = \mathcal{L}(E)$ we don't have any function f to represent $g + (h'_Q)$ as an element of $K(C) + \mathbb{A}_C(E)$.

□

To finish proofs of this section we need only finiteness of dimension of the space $\mathbb{A}_C/(K(C) + \mathbb{A}_C(D))$ for any divisor D. The reader can find this statement in [1] chapters 13.2 and 14.2 with another proof of the Riemann-Roch theorem.

In the previous lecture we noted some useful results which follow from Riemann-Roch theorem.

Corollary 3.11. *1. $\deg K_C = 2g-2$; here use $D = K_C$;*

2. If $\deg D > 2g-2$ then $l(D) = \deg D - g + 1$. Here from 1. $\deg(K_C - D) < 0$.

Now we discuss some examples

Example 3.12. *Let $C = \mathbb{P}^1$. We have no holomorphic differentials on $\mathbb{P}^1$, so $l(K_C) = 0$. Previous corollary says that $\mathbb{P}^1$ has genus 0, so from RR $l(D) - l(-2(\infty) - D) = \deg D + 1$.*

Note that we can work with $C = \mathbb{P}^1$ without Riemann-Roch theorem. Let $D = n\infty$, then $\mathcal{L}(D)$ is just the set of all polynomials of degree less than n, so $l(D) = n+1$.

Example 3.13. *Let C be a curve $y^2 = (x-e_1)(x-e_2)(x-e_3)$, we have seen that $\operatorname{div}(dx/y) = 0$, so $K_C = 0$, then $g(C) = l(K_C) = l(0) = 1$. From RR we have $l(D) = \deg D$.*

We finish with a statement about relationship for general curves and nonconstant map.

Theorem 3.14. *Let $\phi : C_1 \to C_2$ be a nonconstant separable map of smooth curves of genus g_1, g_2 respectively. Then*

$$2g_1 - 2 \geq (\deg \phi)(2g_2 - 2) + \sum_{P \in C_1} (e_\phi(P) - 1).$$

The equality holds either for $\operatorname{char} K = 0$, or for $\operatorname{char} K = p$ and $p \nmid e_\phi(P)$ for all $P \in C_1$.

Proof. For a nonzero differential $\omega \in \Omega_C$ and $P \in C_1$ let $Q = \phi(P)$. Since ϕ is separable we have $\phi^*\omega \neq 0$. We need to relate the valuation of $\operatorname{ord}_P(\phi^*\omega)$ and $\operatorname{ord}_Q(\omega)$. Write $\omega = f dt$ with $t \in \overline{K}(C_2)$ a uniformizer at Q, denote $e = e_\phi(P)$. We have $\phi^* t = us^e$, where s is a uniformizer at P and u s.t. $u(P) \neq 0, \infty$.

Now write $\phi^*\omega = (\phi^* f)d(\phi^* t) = (\phi^* f)d(us^e) = (\phi^*)(eus^{e-1}+(du/ds)s^e)ds$. We know that $\operatorname{ord}_P(du/ds) \geq 0$, so $\operatorname{ord}_P(\phi^*\omega) \geq \operatorname{ord}(\phi^* f)+e-1$, with equality iff $e \neq 0$.

Then $\operatorname{ord}_P(\phi^* f) = e_\phi(P)\operatorname{ord}_Q(f) = e_\phi(P)\operatorname{ord}_Q(\omega)$. Add over all $P \in C_1$ and get

$$\deg \operatorname{div}(\phi^*\omega) \geq \sum_{P\in C_1} (e_\phi(P)\operatorname{ord}_{\phi(P)}(\omega) + e_\phi(P) - 1) =$$

$$= \sum_{Q\in C_2} \sum_{P\in\phi^{-1}(Q)} e_\phi(P)\operatorname{ord}_Q(\omega) + \sum_{P\in C_1} (e_\phi(P) - 1) =$$

$$(\deg\phi)(\deg \operatorname{div}\omega) + \sum_{P\in C_1} (e_\phi(P) - 1).$$

Here $(\deg \operatorname{div}\omega) = 2g_2 - 2$. □

Remark 3.15. *There exists a more general formulation of Hurwitz theorem: for the definition of ramification divisor, equality of its degree to* $\sum_{P\in C_1}(e_\phi(P)-1)$ *and Hurwitz equality the reader is advised to study second paragraph in chapter IV of [4].*

4 Lecture 4: Weierstrass equations

4.1 Definition

From here we denote the curve by E. Our main object of study are elliptic curves — nonsingular curves of genus one with specified point O. We will see later that any such curve can be given by an equation as the set of points $P = (x, y) \in \mathbb{P}^2$ satisfying Weierstrass equation with the point $O = (0 : 1 : 0)$ at infinity.

Definition 4.1. *An elliptic curve is a pair (E, O), where E is nonsingular curve of genus 1 and $O \in E$. We denote it by E. For a subfield $L \subset K$ we say that E is defined over L if also $O \in E(L)$.*

We begin with the statement that every elliptic curve can be written as a plane cubic, which is smooth and conversely every plane cubic is an elliptic curve.

Proposition 4.2. *Let E be an elliptic curve defined over K.*

1. *There exist functions $x, y \in K(E)$ such that the map $\phi : E \to \mathbb{P}^2$ defined by $\phi = (x : y : 1)$ gives an isomorphism of E with the projective closure of a curve C, given by equation*

   $$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

   with coefficients $a_i \in K$ and such that $\phi(O) = (0 : 1 : 0)$. The functions x, y are called Weierstrass coordinates for E.

2. *We can get another Weierstrass equation for E by change of variables: $X = u^2X' + r$, $Y = u^3Y' + su^2X' + t$, where $u \in K^*$, and $r, s, t \in K$.*

3. *Every cubic curve given by a Weierstrass equation as above is an elliptic curve with base point $O = (0 : 1 : 0)$.*

Proof. 1. We look at vector spaces $\mathcal{L}(n(O))$ for various ns. In our case we use the Riemann-Roch theorem for $g = 1$, then $l(n(O)) = dim\mathcal{L}(n(O)) = n$ for all $n \geq 1$. So we choose functions $x, y \in K(E)$ such that $\{1, x\}$ is the basis for $\mathcal{L}(2(O))$ where x has pole of exact order 2 at O, and $\{1, x, y\}$ is the basis for $\mathcal{L}(3(O))$ where y has pole of order 3 at O. The statement about orders of poles follows from the fact that on a curve of genus 1 by Riemann-Roch theorem we have that $\mathcal{L}((O)) = K = \mathcal{L}(0)$. So function x can not have a pole of order 1 at O.

But $\mathcal{L}(6(O))$ has dimension 6, while it contains seven functions $1, x, y, x^2, xy, y^2, x^3$, so there is a linear equation

$$a_1 + a_2x + a_3y + a_4x^2 + a_5xy + a_6y^2 + a_7x^3 = 0.$$

Where $a_i \in K$ and $a_6a_7 \neq 0$, otherwise every term of equation would have a pole of different order. We replace x, y by $-a_6a_7x, a_6a_7^2y$ respectively and then divide by $a_6^3a_7^4$ to get an equation of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, called Weierstrass equation. So we get a map $\phi : E \to \mathbb{P}^2$, $\phi = (x : y : 1)$, whose image C lies in the locus described by Weierstrass equation. Since its image is not one point, it is surjective, and y has higher-order pole at O, than x, so $\phi(O) = (0 : 1 : 0)$.

What is left to prove is that $\phi : E \to C \subset \mathbb{P}^2$ has degree 1 and that C is smooth. We prove the first using equivalent statement $K(E) = K(x, y)$. Look at maps $(x : 1) : E \to \mathbb{P}^1$ and $(y : 1) : E \to \mathbb{P}^1$, we know that

x has a pole of degree 2 at O and no other poles, and y has a pole of degree 3 at O and no other, so maps $(x:1):E\to\mathbb{P}^1$ and $(y:1):E\to\mathbb{P}^1$ have degrees 2 and 3 respectively, then $[K(E):K(x)]=2$ and $[K(E):K(y)]=3$, therefore $K(E):K(x,y)$ divides 2 and 3 so it's 1.

To prove that C is smooth we need a

Lemma 4.3. *If a curve given by Weierstrass equation is singular, then there exists a rational map $\phi:E\to\mathbb{P}^1$ of degree one, it means that E is birationally equivalent to $\mathbb{P}^1$ (there exists a rational map from E to $\mathbb{P}^1$, such that inverse is also rational).*

Proof. If necessary we do linear change of variables and assume that the singular point is $(0,0)$. Using partial derivatives we see that Weierstrass equation is of the form $y^2+a_1xy=x^3+a_2x^2$. Then the map $E\to\mathbb{P}^1$, defined by $(x,y)\mapsto(x:y)$ has degree one, since it has inverse $\mathbb{P}^1\to E$, given by $(1:t)\mapsto(t^2+a_1t-a_2,t^3+a_1t^2-a_2t)$. □

Now assume that our C is singular. Then by lemma there is a rational map $\psi:c\to\mathbb{P}^1$ of degree one. Then the composition $\psi\circ\phi:E\to\mathbb{P}^1$ is a map of degree one between smooth curves, so it defines an isomorphism between function fields $K(E)$ and $(\psi\circ\phi)^*K(\mathbb{P}^1)$, so it is an isomorphism of curves. But the genus of E is 1. We got a contradiction, so C is smooth and isomorphic to E.

2. Let $\{x,y\}$ and $\{x',y'\}$ be two sets of Weierstrass coordinates on E. Then x,x' have poles of order 2 at O, and y,y' have poles of order 3 at O. Then $\{1,x\}$ and $\{1,x'\}$ are bases for $\mathcal{L}(2(O))$, and $\{1,x,y\}$ and $\{1,x',y'\}$ are bases for $\mathcal{L}(3(O))$, so there exist $u_1,u_2\in K^*$ and $r,s,t\in K$ such that $x=u_1x'+r$ and $y=u_2y'+sx'+t$. Substitute this to Weierstrass equations and get $u_1^3=u_2^2$, we set $u=u_2/u_1$ and $s=s_2/u^2$ to get desired formula.

3. To prove this statement we need a

   Lemma 4.4. *Let C be a smooth curve given by Weierstrass equation, then the invariant differential (we will discuss this name on the next lecture)*
   $$\omega=\frac{\mathrm{d}x}{2y+a_1x+a_3}=\frac{\mathrm{d}y}{3x^2+2a_2x+a_4-a_1y}$$
   is holomorphic and non-vanishing, i.e. $\operatorname{div}(\omega)=0$.

Proof is left as an exercise from A. Zykin's list. (Hint: first observe a case of general $P = (x_0, y_0)$ and write $\omega = \frac{\mathrm{d}(x-x_0)}{F_y(x,y)} = -\frac{\mathrm{d}(y-y_0)}{F_x(x,y)}$, and conclude that ω has no poles on C, then count order of ω at P and get that it also has no zeroes. After that look at case of $P = O$).

We have now that $\omega = \frac{\mathrm{d}x}{2y+a_1x+a_3} \in \Omega_C$ has no zeroes and poles, so $\mathrm{div}(\omega) = 0$. By Riemann-Roch theorem we have $2g(C) - 2 = \deg \mathrm{div}(\omega) = 0$, so C has genus 1.

□

Remark 4.5. *While proving first assertion of previous proposition we got that for elliptic curve E following is true: $K(E) = K(x,y)$ and $[K(E) : K(x)] = 2$.*

Now we understand why studying of theory of Weierstrass equation is necessary for discussing elliptic curves. As we have seen every elliptic curve can be represented by a cubic equation with the base point on the line at ∞. Then an elliptic curve has an equation of the Weierstrass form. In A. Zykin's list of problems there proposed ways to simplify this equation depending on characteristic of the base field and you are strongly encouraged to solve that problems.

4.2 Nice Weierstrass equation

We will assume form this point (if other is not stated) that characteristic of our base field is not 2 or 3. Then one can write an equation of the curve in the form:

$$E : y^2 = x^3 + ax + b$$

Now we want to describe elliptic curves using this equation.

Proposition 4.6.

1. *The curve $E(a,b) : y^2 = x^3 + ax + b$ for $a, b \in K$ is nonsingular and defines an elliptic curve over K iff $4a^3 + 27b^2 \neq 0$;*
2. *Every elliptic curve over K is isomorphic to one of the form $E(a,b)$;*
3. *Two elliptic curves $E(a,b)$ and $E(a',b')$ are isomorphic iff there exists a $c \in K^\times$ such that $a' = c^4a$, $b' = c^6b$, then we have an isomorphism $(x : y : z) \mapsto (c^2x' : c^3y' : z)$.*

For a curve given by such equation we define its j-invariant by

$$j(E(a,b)) = \frac{1728(4a^3)}{4a^3+27b^2},$$

its discriminant

$$\Delta(E) = -16(4a^3+27b^2),$$

note that discriminant of a curve is related to a discriminant of polynomial $f(x) = x^3+ax+b$, explicitly we have $\Delta_f = -(4a^3+27b^2)$. and the invariant differential

$$\omega = \frac{\mathrm{d}x}{2y} = \frac{\mathrm{d}y}{3x^2+a}.$$

4. *For $j_0 \in K$ there exists an elliptic curve E defined over K with $j(E) = j_0$.*

Proof. 1. If there is a singular point P, then we have for it: $2y(P) = 0$, $3x(P)^2+a = 0$, $y(P)^2 = x(P)^3+ax(P)+b$. Since char$K \neq 2$, we have $y(P) = 0$ and $x(P)$ is a double root of $x^3+ax+b = 0$. So nonsingularity of E is equivalent to nonvanishing of discriminant $\Delta(E)$.

2. this follows from todays big proposition; Here we can assume by 1. that curve is nonsingular at $(0:1:0)$.

3. this statement is equal to the following: two elliptic curves are isomorphic iff they have equal j-invariants. We prove a statement in the proposition, but will use later equivalent.

   If two elliptic curves are isomorphic, then we can compute their j-invariants by formula $\frac{(4a)^3}{4a^3+27b^2}$ and observe, that they are the same. From previous proposition we know the form of all linear change of variables, but isomorphisms, preserving reduced Weierstrass equation are only of the form $(x,y) = (u^2x', u^3y')$, which stated to an equation gives us that $a' = u^4a$ and $b' = u^6b$. Inverse assume, that necessary c exists, then we have that $a^3b'^2 = a'^3b^2$. In this case we check 3 cases:

Case 1. $a = 0$, then $j = 0$ and $b \neq 0$, since $\delta \neq 0$, so $a' = 0$ and we take $c = (b/b')^{1/6}$;

Case 2. $b = 0$, then $j = 1728$, similar to previous, take $c = (a/a')^{1/4}$;

Case 3. $ab \neq 0$, then $j \neq 0, 1728$ and $a'b' = 0$ by previous cases. We take $c = (a/a')^{1/4} = (b/b')^{1/6}$; we have that it is the same, because $a^3b'^2 = a'^3b^2$;

4. Assume that $j_0 \neq 0, 1728$ and look at a curve

$$E : y^2 + xy = x^3 - \frac{36x}{j_0 - 1728} - \frac{1}{j_0 - 1728};$$

Calculate $\Delta(E) = \frac{j_0^3}{(j_0-1728)^3}$ and $j(E) = j_0$, so we constructed a curve for cases $j_0 \neq 0, 1728$.

For $j_0 = 0$ we take $E : y^2 = x^3 - 1/4$, and for $j_0 = 1728$ take $E : y^2 = x^3 + x$.

□

Now we discussed necessary theory of Weierstrass equations and we continue by studying the Group law on elliptic curve.

For exercises the reader is strongly recommended to solve problems from the list `http://www.mccme.ru/ium/postscript/f11/zykin-Problems_2.pdf` .

5 Lecture 5: The Group Law

In this lecture we will often use the Riemann-Roch theorem 3.4 in case $g(C) = 1$ which looks like $l(D) - l(K_C - D) = \deg(D)$, moreover for every divisor D of degree $\deg D \geq 0$ we know that $l(K_C - D) = 0$, so $l(D) = \deg D$.

The first corollary is

Lemma 5.1. *Let C be a curve of genus 1 and $P, Q \in C$. Then $(P) \sim (Q)$ iff $P = Q$.*

Proof. If $(P) \sim (Q)$ we chose $f \in \overline{K}(C)$ such that $\operatorname{div}(f) = (P) - (Q)$, then $f \in \mathcal{L}((Q))$ and by RR theorem $\dim \mathcal{L}((Q)) = 1$, since $\mathcal{L}((Q))$ contains $\overline{K}$ we get $f \in \overline{K}$ and $P = Q$. □

Some time ago we formulated already the composition law, but let me remind it.

We will assume that out main object of study — an elliptic curve E is given by a Weierstrass equation of the form $E : y^2z = x^3 + axz^2 + bz^3$, $P = (x, y) \in E$, and $O = (0 : 1 : 0)$. Let L be a line in $\mathbb{P}^2$, then since the equation of E has a degree 3, the line L intersects E at 3 points.

Fact 5.2. *Let $P, Q \in E$ and L — the line through P and Q (or tangent if they coincide). Let R be the third point of intersection of L and E. Then we take a line L' through R and O, which intersects E at one more point, which we will call $P \oplus Q$.*

Proposition 5.3. *We have the following properties for the composition law:*

1. *If a line L intersects E at points P, Q, R, then $(P \oplus Q) \oplus R = O$.*
2. *$P \oplus Q = Q \oplus P$ for all $P, Q \in E$;*
3. *$P \oplus O = P$ for any $P \in E$;*
4. *For any $P \in E$ there exists a point $\ominus P$ such that $P \oplus (\ominus P) = O$;*
5. *For $P, Q, R \in E$ we have associativity: $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.*

So we can say that the composition law makes E into an abelian group with identity element O.

From here we will denote the addition by just $+$, not $\oplus$

Proof.

1. By construction $O + O = O$ and using a line through $(P + Q)$ and R we get that $(P + Q) + R + O = O$, so $(P + Q) + R = O$.
2. Follows from the symmetry of construction with respect to P and Q;
3. A line through P and O intersects a curve E for the third time in point Q, such that $P + Q = O$ by 1. and that $P + Q + O = O$, so we get what needed.
4. For usual P we take a point Q from previous, for the point O one should take O.
5. This assertion has more difficult proof, which actually works for all others, since it is just an isomorphism (as abelian groups) between an elliptic curve E and its Picard group. We will discuss here the proof using RR, but there is one using coordinates, which is left for you. The proof includes 3 steps:

a. For every divisor $D \in \mathrm{Div}^0(E)$ of degree 0, there exists a point $P \in E$, such that $D \sim (P) - (O)$. We define $\sigma : \mathrm{Div}^0(E) \to E$ the map which sends D to P, and observe that it is surjective.

b. σ acts on equivalence classes of divisors and induces a bijection of sets $\sigma : \mathrm{Pic}^0(E) \overset{\sim}{\to} E$, i.e. for divisors $D_1, D_2 \in \mathrm{Div}^0(E)$ we have $\sigma(D_1) = \sigma(D_2)$ iff $D_1 \sim D_2$.

c. The inverse to σ is the map $\kappa : E \overset{\sim}{\to} \mathrm{Pic}^0(E)$ defined by $P \mapsto$ class of $(P) - (O)$. And the geometric group law defined above is the same as the algebraic group law, induced from κ.

First we prove a.: We look at $\mathcal{L}(D+(O))$ and by RR we have $\dim \mathcal{L}(D+(O)) = 1$, then take a nonzero element $f \in \mathcal{L}(D+(O))$, which is a basis of this space over $\overline{K}$, so we get $\mathrm{div}(f)+D+(O) \geq 0$ and $\deg \mathrm{div}(f) = 0$, therefore there exists a point P, such that $\mathrm{div}(f) = (P) - (O) + D$. If there are two such points P, P', then $(P) \sim D + (O) \sim (P')$, so by previous lemma $P = P'$. For surjectivity we take for $P \in E$ its preimage — divisor $(P) - (O)$.

Next we should prove b.: We take two divisors $D_1, D_2 \in \mathrm{Div}^0(E)$ and set $P_i = \sigma(D_i)$. By definition of σ we have $(P_1) - (P_2) \sim D_1 - D_2$, so if $P_1 = P_2$, then $D_1 \sim D_2$, inverse way: if $D_1 \sim D_2$, then $(P_1) \sim (P_2)$, and by lemma $P_1 = P_2$.

To prove c. we only need to show that for two points $P, Q \in E$ the image of their sum is sum of their images: $\kappa(P + Q) = \kappa(P) + \kappa(Q)$, where the second addition if of divisor classes in $\mathrm{Pic}^0(E)$. Then we will just use the group structure on $\mathrm{Pic}^0(E)$ to deduce this structure on E.

We take two functions $f(x, y, z) = ax + by + cz = 0$ is a line in $\mathbb{P}^2$ through points P and Q, which intersects E also in point R, and a function $f'(x, y, z) = a'x + b'y + c'z = 0$ the line through R and O. We know that line $z = 0$ intersects E at O with multiplicity 3, so

$$\mathrm{div}\left(\frac{f}{z}\right) = (P) + (Q) + (R) - 3(O), \quad \mathrm{div}\left(\frac{f'}{z}\right) = (P + Q) + (R) - 2(O);$$

Then $\mathrm{div}\left(\frac{f'}{f}\right) = (P + Q) - (P) - (Q) + (O) \sim 0$, so $\kappa(P + Q) - \kappa(P) - \kappa(Q) = 0$.

□

Corollary 5.4. *For an elliptic curve E, a divisor $D = \sum n_P(P) \in \operatorname{Div}(E)$ is principal if and only if $\sum_{P\in E} n_p = 0$ and $\sum_{P\in E}[n_P](P) = O$.*

This is clear because $D \sim 0 \Leftrightarrow \sigma(D) = O \Leftrightarrow \sum_{P\in E}[n_P]\sigma((P)-(O)) = O$.

Note that for any field $L \subset \overline{K}$ if the curve E is defined over L, then one can get the group structure on the set $E(L)$ by the structure on $E(\overline{K})$. It comes out, because when we take two points P, Q from $E(L)$ then the line through these points is also with coefficients from L, so third intersection point has coordinates in L.

Further, for a point $P \in E$ and integer n we will denote by $[n]P = P + ... + P$ a sum by group operation of n points P, also $[0]P = O$. In the list of problems from previous lecture you can find explicit formulas for addition of points on elliptic curve, the notation there λ, ν are coefficients of the equation of the line $y = \lambda x + \nu$ through points P_1, P_2.

Exercise 5.5. *We say that a function $f \in \overline{K}(E)$ is even if $f(P) = f(-P)$ for all $P \in E$. Prove that f is even iff $f \in \overline{K}(x)$.*

Hint: one side is obvious. To prove another write $f(x, y) = g(x) + h(x)y$ and use the coordinate description of $-P$ to deduce $h(x) = 0$.

5.1 Singular curves

Now we talk about the case when the Weierstrass equation gives us a singular curve. That happens only when its discriminant $\Delta(E) = 0$ and the most famous examples are curves with equations $y^2 = x^3$ — cusp curve with one singular point and one tangent line at that point, and $y^2 = x^3 + x^2$ — node curve with one singular point and two different tangent lines at that point. In the list of problems are stated conditions for curve to have a cusp or a node.

So in this section we assume that $\Delta(E) = 0$. We denote by E_{ns} the set of nonsingular points of E. we already have a result about singular curves — they are birational to $\mathbb{P}^1$.

Proposition 5.6. *Let E be a curve given by a Weierstrass equation with $\Delta(E) = 0$, then the composition law makes E_{ns} an abelian group and we want to describe it using the field $\overline{K}$.*

1. *Assume that E has a node at point P_0 and let $y = a_1x + b_1$ and $y = a_2x + b_2$ be distinct tangent lines to E at P_0. Then the map $E_{ns} \to \overline{K}^*$ defined by $(x, y) \mapsto \frac{y-a_1x-b_1}{y-a_2x-b_2}$ is an isomorphism of abelian groups.*

2. *If E has a cusp at P_0, let $y = ax + b$ be a tangent line to E at P_0, then the map $E_{ns} \to \overline{K}^+$ defined by $(x, y) \mapsto \frac{x - x(P_0)}{y - ax - b}$ is an isomorphism of abelian groups.*

Proof. First we understand that E_{ns} is closed under composition law: it means that if a line L intersects E at two points, then is does not contain a singular, which is clear because P_0 should has multiplicity at least two in the intersection $E \cap L$.

Then make a change of variables such that our singular point is $(0, 0)$. Then E is given by a Weierstrass equation of the form $y^2 = x^3 + ax^2$ and if $a = 0$, then E has a cusp, otherwise a singularity is a node.

For the case of cuspidal curve we take a map $E_{ns} \to \overline{K}^+$ defined by $(x, y) \mapsto x/y$, we can do that because $y = 0$ only at $(0, 0)$, which is singular. In this case the inverse map is defined by $t \mapsto (t^{-2}, t^{-3})$. □

This is all that we need now from theory of singular elliptic curves. And now we are going to prove the fundamental result in the theory of elliptic curves is that the addition map $E \times E \to E$ is a morphism. We state this as a theorem.

Theorem 5.7. *Let E be an elliptic curve. Then the group law and negation define morphisms:*

$$+ : E \times E \to E,\ (P, Q) \mapsto P + Q \quad - : E \to E,\ P \mapsto -P$$

Proof. The negation map is a morphism by definition, since it is obviously rational and regular.

For a point $Q \in E$ we define the translation map $\tau_Q : E \to E$ by $\tau_Q(P) = P + Q$. This is a rational map and so a morphism, moreover it has an inverse — the translation for $-Q$, so is an isomorphism.

To prove that the the addition map $+ : E \times E \to E$ is a morphism we have to prove regularity at pairs of points: (P, P); $(P, -P)$; (P, O); (O, P), since for all other cases we have that coefficients $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ and $\nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$ of a line $y = \lambda x + \nu$ through points (x_1, y_1) and (x_2, y_2) are well-defined.

For one of those cases we take a composition of maps

$$E \times E \xrightarrow{\tau_1 \times \tau_2} E \times E \xrightarrow{+} E \xrightarrow{\tau_1^{-1}} E \xrightarrow{\tau_2^{-1}} E$$

Where τ_1 is the translation map for a point Q_1 and τ_2 is the translation map for a point Q_2.

and look what happens to a pair of points (P_1, P_2), indeed they go to $(P_1, P_2) \overset{\tau_1 \times \tau_2}{\to} (P_1 + Q_1, P_2 + Q_2) \times P_1 + Q_1 + P_2 + Q_2 \overset{+}{\to} P_1 + P_2 + Q_2 \overset{\tau_1^{-1}}{\to} P_1 + P_2$. So this composition is just an addition of points. Since we know that τ_Q is an isomorphism, then the composition above is regular everywhere except set $(P - Q_1, P - Q_2)$; $(P - Q_1, -P - Q_2)$; $(P - Q_1, -Q_2)$; $(-Q_1, P - Q_2)$, but Q_i are arbitrary points, so we can take another pair of points Q_3, Q_4 for new description of additional morphism and it will be regular in points mentioned above. □

5.2 Isogenies: definition

We want to work with appropriate morphisms between elliptic curves: such that they take a special point of one curve to special point of another.

Definition 5.8. *Let E_1, O_1, E_2, O_2 be two elliptic curves. An isogeny is a morphism of curves $\phi : E_1 \to E_2$ such that $\phi(O_1) = O_2$. We call two curves E_1, E_2 isogenuous if there is an isogeny $\phi : E_1 \to E_2$ such that $\phi(E_1) \neq O$ (in this case we have $\phi(E_1) = E_2$).*

Next we should define the degree of isogeny. For the case of zero isogeny we set $\deg[O] = 0$, otherwise the isogeny is a finite map of curves, so we have an injection of function fields $\phi^* : \overline{K}(E_2) \to \overline{K}(E_1)$ and the degree of ϕ is is the degree of extension $[\overline{K}(E_1) : \phi^* \overline{K}(E_2)]$. Definitions of separable and inseparable degree are corresponding.

Definition of degree implies that for composition $E_1 \overset{\phi}{\to} E_2 \overset{\psi}{\to} E_3$ the degree $\deg(\psi \circ \phi) = \deg(\psi) \deg \phi$.

By the group law elliptic curves are abelian groups. One can define a structure of a group on the set of isogenies between two curves. Explicitly: denote $\mathrm{Hom}(E_1, E_2)$ the set of isogenies $E_1 \to E_2$, then for two isogenies $\psi, \phi : E_1 \to E_2$ define a morphism $(\phi + \psi)(P) = \phi(P) + \psi(P)$, which is also an isogeny, so we get a structure of a group on $\mathrm{Hom}(E_1, E_2)$.

Now we turn to case when $E_1 = E_2$, i. e. $\mathrm{End}(E) = \mathrm{Hom}(E, E)$, here we can look at composition of isogenies $(\psi\phi)(P) = \phi(\psi(P))$ and get a structure of a ring on $\mathrm{End}(E)$, we denote the subgroup of invertible elements $\mathrm{Aut}(E)$.

Example 5.9. *The transition map from previous section τ_Q is of course not an isogeny (unless $Q = O$, but it's not interesting). We have an example of isogeny: multiplication by n map where $n \in \mathbb{Z}$, defined as $[n] : E \to E$, $[n](P) = P + ... + P$, in the case $n < 0$ we set $[n](P) = [-n](-P)$.*

5.3 Exercises

Exercise 5.10. *Let C over algebraically closed field K is an algebraic curve of genus 1. Take any point $O \in C$ and j-invariant for curve $j(C, O)$.*

1. *For curve (C', O') and isomorphism $\phi : C \to C'$ such that $\phi(O) = O'$ prove that $j(C, O) = j(C', O')$;*

2. *For two points $O, O' \in C$ prove that there exists an isomorphism $C \to C$, which sends O to O'. Deduce that $j(C, O) = j(C, O')$.*

Exercise 5.11. *How to get $[m]P$.*

Here we will discuss the case of a curve $E : y^2 = x^3 + Ax + B$. But one can write formulas in similar way for case of general Weierstrass equation. We define polynomials $\psi_m \in \mathbb{Z}[A, B, x, y]$ by first few:

$$\psi_1 = 1, \quad \psi_2 = 2y, \quad \psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,$$

$$\psi_4 = \psi_2(2x^6 + 10Ax^4 + 40Bx^3 - 10A^2x^2 - 8ABx - 2A^3 - 16B^2),$$

and then by induction with following formulas:

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \textit{ if } m \geq 2;$$

$$\psi_2\psi_{2m} = \psi_{m-1}^2\psi_m\psi_{m+2} - \psi_{m-2}\psi_m\psi_{m+1}^2, \textit{ if } m \geq 3.$$

Then we define polynomials ϕ_m, ω_m in the following way:

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}, \quad 4y\omega_m = \psi_{m-1}^2\psi_{m+2} + \psi_{m-2}\psi_{m+1}^2.$$

1. *Prove that if m is odd (even) polynomials ψ_m, ϕ_m, $y^{-1}\omega_m$ (corresponding $(2y)^{-1}\psi_m\phi_m\,\omega_m$) are elements of the ring $\mathbb{Z}[A, B, x, 4x^3{+}4Ax{+}4B]$;*

2. *Prove that ψ_m, ϕ_m as polynomials of x start with x^{m^2} and $m^2x^{m^2-1}$;*

3. *Prove that if $\Delta(E) \neq 0$, then $\phi_m(x), \psi_m(x)$ are coprime;*

4. *Prove that if $\Delta(E) \neq 0$, then for any point $P = (x_0, y_0)$ one can compute $[m]P = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3}\right)$;*

5. *Prove that divisor of $\operatorname{div}(\psi_m) = \sum_{T \in E[m]}(T) - m^2(O)$, so ψ_m has a zero in m-torsion points;*

6. *Prove that degree of the map $[m] : E \to E$ has degree m^2.*

Exercise 5.12. *Let E be an elliptic curve with homogeneous Weierstrass equation $F(x_0 : x_1 : x_2) = x_1^2 x_2 - x_0^3 - Ax_0 x_2^2 - Bx_2^3 = 0$, let $P \in E$. Prove that following conditions are equal:*

- $[3]P = O$;
- *The tangent line to E in P intersects E only at P;*
- *Determinant of $\left(\frac{\partial F}{\partial x_i x_j}(P)\right)$ equals to 0.*

Exercise 5.13. *Let C be a smooth curve of genus g (from RR)and $n \geq 2g+1$ an integer. We choose a basis $f_0, ...f_n$ in $\mathcal{L}(n(P_0))$ and define a map $\phi = (f_0 : ... : f_n) : C \to \mathbb{P}^{n-g}$. Prove that the image of this map is a curve C' in $\mathbb{P}^{n-g}$, that $\deg \phi = 1$, and (harder) that C' is smooth and ϕ is an isomorphism.*

6 Lecture 6: Isogenies

We continue to study isogenies of elliptic curves (they are morphisms, sending point O_1 to O_2).

Proposition 6.1. 1. *The multiplication map $[n]$ is nonconstant if $n \neq 0$;*

2. *For two elliptic curves E_1, E_2 the group of isogenies $\mathrm{Hom}(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module;*

3. *For an elliptic curve E its endomorphism ring $\mathrm{End}(E)$ is an integral domain of characteristic zero.*

Proof. 1. To prove the first assertion we will use that $[mn] = [m] \circ [n]$, so we have to prove that $[2] \neq [0]$ and $[p] \neq [0]$ for odd primes p. The idea is to show that $[2]$ is a nonconstant map, however there always exists a point P of order 2, which means that for n odd we have $[n]P = P \neq O$.

This is not difficult to find out that there always exist a point of order 2 (except the case of char$K = 2$), but there are only finitely many such points since their x coordinates are roots of polynomial, here one should use an exercise from list of problems which gives the formula of x coordinate for doubling point. In the case of char $= 2$ one should look for points of order 3.

In the case of characteristic 2 of the base field one should look at multiplication by [3] map and points of order 3.

2. This is the corollary of previous. Assume we have $\phi \in \mathrm{Hom}(E_1, E_2)$ and $n \in \mathbb{Z}$, such that $[n] \circ \phi = [0]$, then taking degrees $(\deg[n])(\deg \phi) = 0$, so either $[n] = [0]$, or $\phi = [0]$.

3. From previous characteristic of $\mathrm{End}(E)$ is 0, assume there exist two isogenies ϕ, ψ such that $\phi \circ \psi = [0]$, then $(\deg \phi) \circ (\deg \psi) = 0$, so either $\phi = [0]$, or $\psi = [0]$.

□

We look at E as an abelian group and for an integer $m \geq 1$ define its m-torsion subgroup by $E[m] = \{P \in E : [m]P = O\}$, and its torsion subgroup $E_{tors} = \bigcup_{m=1}^{\infty} E[m]$.

Example 6.2. *Curves with complex multiplication.*

Assume $\mathrm{char}K = 0$, *then usually* $\mathrm{End}(E) \simeq \mathbb{Z}$, *but sometimes happens an exception when* $\mathrm{End}(E)$ *is larger than* $\mathbb{Z}$, *then we say that a curve E has complex multiplication. Here we give an example of such curve.*

Let $i \in \overline{K}$ be a primitive fourth root of unity, $i^2 = -1$. Look at elliptic curve $E : y^2 = x^3 - x$. Then in $\mathrm{End}(E)$ *there is a map $[i] : (x, y) \mapsto (-x, iy)$, for which $[i] \circ [i] = [-1]$, so there is a ring homomorphism $\mathbb{Z}[i] \to$* $\mathrm{End}(E)$, *defined as $m + ni \mapsto [m] + [n] \circ [i]$.*

Example 6.3. *The Frobenius endomorphism. Here we assume that* $\mathrm{char}K = p > 0$.

Remember there was a curve $E^{(q)}$, obtained by raising to q-th power all coefficient of equation for E?

The Frobenius morphism $\phi_q : E \to E^{(q)}$ is defined by $(x, y) \mapsto (x^q, y^q)$. We know that $E^{(q)}$ is given by Weierstrass equation, and we want it to be a nonsingular elliptic curve.

Writing j-invariant and discriminant in terms of Weierstrass coefficients we get $\Delta(E^{(q)}) = \Delta(E)^q$ and $j(E^{(q)}) = j(E)^q$, so equation for $E^{(q)}$ is nonsingular. For $K = \mathrm{F}_q$ the q-th power of Frobenius is an identity and so ϕ_q is an endomorphism of $E = E^{(q)}$. The set of points fixed by ϕ_q is the finite group $E(\mathrm{F}_q)$.

Remark 6.4. *A view of arbitrary morphism between elliptic curves. Consider a morphism $\phi : E_1 \to E_2$ of elliptic curves, then the composition*

$\psi = \tau_{-\phi(O_1)} \circ \phi$ is an isogeny, since $\psi(O_1) = (O_2)$, so any morphism between elliptic curves can be written as a composition of an isogeny and translation.

We defined an isogeny as a map, sending O_1 to O_2, but don't we want it to preserve a group law? Next theorem shows that this property follows from definition.

Theorem 6.5. *Let $\phi : E_1 \to E_2$ be an isogeny, then $\phi(P+Q) = \phi(P)+\phi(Q)$.*

Proof. We assume that ϕ is nonconstant (as in any case when we prove something about isogenies), so ϕ is finite map and induces a homomorphism $\phi_* : \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2)$ defined by $\phi_*(class \sum n_i(P_i)) = class \sum n_i(\phi P_i)$. So we get a commutative diagram:

$$\begin{tikzcd}
E_1 \arrow[r, "\kappa_1"] \arrow[d, "\phi"'] & \mathrm{Pic}^0(E_1) \arrow[d, "\phi_*"'] \\
E_2 \arrow[r, "\kappa_2"] & \mathrm{Pic}^0(E_2)
\end{tikzcd}$$

Using the fact that κ_i are isomorphisms we get that ϕ is group homomorphism. □

Corollary 6.6. *The kernel $\phi^{-1}(O)$ of a nonzero isogeny $\phi : E_1 \to E_2$ is a finite subgroup of E_1 of order not more than* $\deg \phi$.

The following statements give us some properties of isogeny, its separable and inseparable degree and left without proof.

Proposition 6.7. *Let $\phi : E_1 \to E_2$ be a nonzero isogeny.*

1. *For every $P \in E_1$ and $Q \in E_2$ we have $\#\phi^{-1}(Q) = \deg_s \phi$ and $e_\phi(P) = \deg_i \phi$;*

2. *The map $\ker \phi \to Aut(\overline{K}(E_1)/\phi^*\overline{K}(E_2))$, defined by $T \mapsto \tau_T^*$ is an isomorphism.*

3. *If ϕ is separable, then ϕ is unramified, $\# \ker \phi = \deg \phi$, and $\overline{K}(E_1)$ is a Galois extension of $\phi^*\overline{K}(E_2)$.*

Reminder: ramification index of a morphism between curves $e_\phi(P) = \mathrm{ord}_P(\phi^* t_{\phi(P)})$, morphism is called unramified if $e_{\phi(P)} = 1$ for all P, τ_T^* is the automorphism of $\overline{K}(E_1)$ induced by τ_T.

Proposition 6.8. *Let E be an elliptic curve and G a finite subgroup of E. Then there exist unique elliptic curve E/G and separable isogeny $\phi : E \to E/G$, such that* $\ker\phi = G$.

Sketch of the proof: Look at fixed subfield $\overline{K}(E)^G$ of $\overline{K}(E)$, one see that $\overline{K}(E)/\overline{K}(E)^G$ is Galois extension and $\overline{K}(E)^G$ has transcendence degree one over $\overline{K}$, so there is a unique curve C and a morphism $\phi : E \to C$ such that $\phi^*\overline{K}(C) = \overline{K}(E)^G$, then show that ϕ is unramified and by Hurwitz genus formula compute $g(C) = 1$.

6.1 The dual isogeny

For a nonconstant isogeny $\phi : E_1 \to E_2$ there is an induced map $\phi^* : \mathrm{Pic}^0(E_2) \to \mathrm{Pic}^0(E_1)$, but we have also two isomorphisms $\kappa_i : E_i \to \mathrm{Pic}^0(E_i)$, sending a point P to the class $(P) - (O)$. So one obtains a morphism

$$E_2 \xrightarrow{\kappa_2} \mathrm{Pic}^0(E_2) \xrightarrow{\phi^*} \mathrm{Pic}^0(E_1) \xrightarrow{\kappa_1^{-1}} E_1.$$

The composition $\kappa_1^{-1} \circ \phi^* \circ \kappa_2$ is a rational map sending O_2 to O_1, so is an isogeny. We call it the dual isogeny for ϕ and denote $\widehat{\phi}$.

Theorem 6.9. *Let $\phi : E_1 \to E_2$ be a nonconstant isogeny of degree m. Then there exists a unique isogeny $\widehat{\phi} : E_2 \to E_1$ such that $\widehat{\phi} \circ \phi = [m]$. One can define $\widehat{\phi}$ as composition*

$$E_2 \overset{Q\mapsto(Q)-(O)}{\longrightarrow} \mathrm{Div}^0(E_2) \xrightarrow{\phi^*} \mathrm{Div}^0(E_1) \overset{\sum n_P(P)\mapsto\sum[n_P]P}{\longrightarrow} E_1.$$

Proof. Uniqueness is obvious, since for another such morphism $\widehat{\phi}'$ we have that $(\widehat{\phi} - \widehat{\phi}') \circ \phi = [0]$. To prove existence we look at the image of $Q = \phi(P) \in E_2$ by composition defined in statement of theorem:

$$Q \mapsto (Q)-(O) \mapsto \sum_{P\in\phi^{-1}Q} e_\phi(P)P - \sum_{R\in\ker\phi} e_\phi(R)R \mapsto [\deg_i\phi](\sum_{P\in\phi^{-1}Q} P - \sum_{R\in\ker\phi} R)$$

$$= [\deg_i\phi] \circ [\#\phi^{-1}(Q)]P = [\deg\phi]P$$

Here first arrow is by definition of ϕ^*, second and equalities are from first and third part of proposition 6.7. Note that we didn't use anywhere characteristic of the base field. □

Let us state some properties of this isogeny:

Proposition 6.10. *Let $\phi : E_1 \to E_2$ be an isogeny of degree m.*

1. *Let $m = \deg\phi$, then $\widehat{\phi} \circ \phi = [m]$ on E_1 and $\phi \circ \widehat{\phi} = [m]$ on E_2;*
2. *Let $\psi : E_2 \to E_3$ be isogeny, then $\widehat{\psi \circ \phi} = \widehat{\phi} \circ \widehat{\psi}$;*
3. *Let $\psi : E_1 \to E_2$ be another isogeny, then $\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}$;*
4. *For an integer $m \in \mathbb{Z}$ defined isogeny $\widehat{[m]} = [m]$ and $\deg[m] = m^2$;*
5. *$\deg\widehat{\phi} = \deg\phi$;*
6. *$\widehat{\widehat{\phi}} = \phi$.*

Proof. 1. We prove that $\phi \circ \widehat{\phi} = [m]$: write $(\phi \circ \widehat{\phi}) \circ \phi = \phi \circ [m] = [m] \circ \phi$;

2. Let $\deg\psi = n$, then $(\widehat{\phi} \circ \widehat{\psi}) \circ (\psi \circ \phi) = \widehat{\phi} \circ [n] \circ \phi = [n] \circ \widehat{\phi} \circ \phi = [nm]$, from uniqueness property we get that $\widehat{\phi} \circ \widehat{\psi} = \widehat{\psi \circ \phi}$;
3. We will prove it later, using the Weil pairing;
4. This is obvious for $m = 0, 1$, apply 3. for maps $\phi = [m]$, $\psi = [1]$, then $\widehat{[m+1]} = \widehat{[m]} + \widehat{[1]}$, so by induction $\widehat{[m]} = [m]$. Let $d = \deg[m]$ and look at multiplication by d. Then by definition of dual isogeny $[d] = \widehat{[m]} \circ [m] = [m^2]$, so $d = m^2$;
5. By 4.,1. we have $m^2 = \deg[m] = \deg(\phi \circ \widehat{\phi}) = (\deg\phi)(\deg\widehat{\phi}) = m(\deg\widehat{\phi})$, so $m = \deg\widehat{\phi}$;
6. By 1,2,4 $\widehat{\phi} \circ \phi = [m] = \widehat{[m]} = \widehat{\widehat{\phi} \circ \phi} = \widehat{\phi} \circ \widehat{\widehat{\phi}}$, so $\phi = \widehat{\widehat{\phi}}$.

□

6.2 The Tate module

To work further with Tate module we need a view of m-torsion group of E. Here we look only at points of $E(\overline{K})$. Explicitly:

Proposition 6.11. *If $m \neq 0$ in field K, then $E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.*

If $\mathrm{char}K = p$, then one of the following is true:

1. $E[p^n] = O$ *for all* $n \in \mathbb{N}$*;*

2. $E[p^n] = \mathbb{Z}/p^n\mathbb{Z}$ *for all* $n \in \mathbb{N}$.

Proof. By 4. from previous proposition we get that $[m]$ is finite separable map, then $\#E[m] = \deg[m] = m^2$, similarly for every $d|m$ we have that $\#E[d] = d^2$. We reduced the statement to an

Exercise 6.12. *Let A be a finite abelian group of order n^r. Suppose that for every $d|n$ we have $\#A[d] = d^r$. Then $A \simeq (\mathbb{Z}/n\mathbb{Z})^r$.*

Let ϕ is p-th power Frobenius morphism. Then $\#E[p^n] = (\deg_s(\widehat{\phi \circ \phi}))^n = (\deg_s \widehat{\phi})^n$. But we know that $\deg \widehat{\phi} = \deg \phi = p$, so there are two cases: first if $\widehat{\phi}$ is inseparable, then $\deg_s \widehat{\phi} = 1$, then $\#E[p^n] = 1$ for all n; second if $\widehat{\phi}$ is separable, then $\deg_s \widehat{\phi} = p$ and $\#E[p^n] = p^n$ for all n. □

We have shown that $E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ is an isomorphism of groups. But we have some additional structure on $E[m]$, for example $G_{\overline{K}/K}$ acts on $E[m]$: $[m]P = O$, so $[m]P^\sigma = ([m]P)^\sigma = O$, so we get a representation $G_{\overline{K}/K} \to \mathrm{Aut}(E[m]) \simeq GL_2(\mathbb{Z}/m\mathbb{Z})$. What we want is to put together all these mod m representations to get a characteristic zero representation.

To do it we define the l-adic Tate module.

Definition 6.13. *Let E be an elliptic curve and $l \in \mathbb{Z}$ a prime number. The Tate module is the group $T_l(E) = \varprojlim_n E[l^n]$ the inverse limit taken with respect to the natural maps $E[l^{n+1}] \xrightarrow{[l]} E[l^n]$.*

We know that $E[l^n]$ is a $\mathbb{Z}/l^n\mathbb{Z}$-module, so the Tate module has a natural structure of $\mathbb{Z}_l$-module. Moreover as a $\mathbb{Z}_l$-module it has defined structure:

a. $T_l(E) \simeq \mathbb{Z}_l \times \mathbb{Z}_l$ if $l \neq \mathrm{char}K$;

b. $T_l(E) = \{0\}$ or $\mathbb{Z}_l$ if $l = \mathrm{char}K$.

This follows from previous proposition.

We define l-adic representation of $G_{\overline{K}/K}$ associated to E as the homomorphism $\rho_l : G_{\overline{K}/K} \to \mathrm{Aut}(T_l(E))$ induced by action of $G_{\overline{K}/K}$ on $E[l^n]$. To get a representation of $G_{\overline{K}/K}$ over a field of characteristic 0 we chose a $\mathbb{Z}_l$-basis in $T_l(E)$ and use representation $G_{\overline{K}/K} \to GL_2(\mathbb{Z}_l)$ with inclusion $\mathbb{Z}_l \subset \mathbb{Q}_l$.

Now we discuss applications of the Tate module to isogenies. Let $\phi : E_1 \to E_2$ be an isogeny of elliptic curves. Then ϕ induces maps $\phi : E_1[l^n] \to E_2[l^n]$, so it induces a map $\phi_l : T_l(E_1) \to T_l(E_2)$. So we get a map $\mathrm{Hom}_K(E_1, E_2) \to \mathrm{Hom}_K(T_l(E_1), T_l(E_2))$ defined by $\phi \mapsto \phi_l$. An important statement about this map is following

Theorem 6.14. *Let E_1, E_2 be elliptic curves and $l \neq \mathrm{char} K$ be a prime. Then the natural map $\mathrm{Hom}_K(E_1, E_2) \otimes \mathbb{Z}_l \to \mathrm{Hom}_K(T_l(E_1), T_l(E_2))$, $\phi \mapsto \phi_l$ is injective. Moreover it is an isomorphism in following cases:*

1. *K is a finite field;*
2. *K is a number field.*

We leave it without proof, because known proofs of surjectivity use techniques, not included in this course. We will not use it further.

6.3 Additional: proof of one theorem

In this section using the latest theorem of lecture 6 we will prove the following result:

Theorem 6.15. *Let E_1, E_2 be elliptic curves. Then $\mathrm{Hom}(E_1, E_2)$ is a free $\mathbb{Z}$-module of rank at most 4.*

Proof. We know already that $\mathrm{Hom}(E_1, E_2)$ is a free $\mathbb{Z}$-module, but have to prove mainly that it has finite rank, and then prove the theorem using equality $\mathrm{rk}_{\mathbb{Z}}\mathrm{Hom}(E_1, E_2) = \mathrm{rk}_{\mathbb{Z}_l}\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_l$ of ranks as $\mathbb{Z}$ and $\mathbb{Z}_l$-modules and inequality

$$\mathrm{rk}_{\mathbb{Z}_l}\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_l \leq \mathrm{rk}_{\mathbb{Z}_l}\mathrm{Hom}(T_l(E_1), T_l(E_2)) = 4.$$

Here the last equality comes from $\mathrm{Hom}(T_l(E_1), T_l(E_2)) = \mathrm{Mat}_2(\mathbb{Z}_l)$ and inequality from injection $\mathrm{Hom}_K(E_1, E_2) \otimes \mathbb{Z}_l \to \mathrm{Hom}_K(T_l(E_1), T_l(E_2))$.

To prove finiteness of rank of $\mathrm{Hom}(E_1, E_2)$ as $\mathbb{Z}$-module our main reference is [10].

We denote by $\mathrm{Hom}^0(E_1, E_2) = \mathbb{Q} \otimes \mathrm{Hom}(E_1, E_2)$ and by $\mathrm{End}^0(E) = \mathbb{Q} \otimes \mathrm{End}(E)$ then $\mathrm{End}^0(E)$ has finite dimension as $\mathbb{Q}$-vector space, because it is a ring of matrices. Also we have $\mathrm{Hom}(E_1, E_2) \subset \mathrm{Hom}^0(E_1, E_2)$, since $\mathrm{Hom}(E_1, E_2)$ is torsion-free.

For two elliptic curves E_1, E_2 over $\mathbb{C}$ the finiteness of dimension of $\mathrm{Hom}^0(E_1, E_2)$ over $\mathbb{Q}$ can be easily verified as following: look at $E_i = \mathbb{C}/L_i$ where L_i is a lattice (more precisely about this representation is written in the next lecture). Then every algebraic morphism $f : E_1 \to E_2$ lifts to a complex-analytic morphism $\widetilde{f} : \mathbb{C} \to \mathbb{C}$ which is linear, therefore we have a map $T : \mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{C}, \mathbb{C})$ a representation of $\mathrm{Hom}(E_1, E_2)$ by 2×2-integral matrices.

We want to have an l-adic analog of this construction, here $l \neq p$. A morphism $f : E_1 \to E_2$ induces a morphism $T_l(f) : T_l(E_1) \to T_l(E_2)$, providing an l-adic representation $T_l : \mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2))$. We take bases for $T_l(E_i)$ over $\mathbb{Z}_l$ to get a representation of $\mathrm{Hom}(E_1, E_2)$ by 2×2 matrices with coefficients in $\mathbb{Z}_l$.

Lemma 6.16. *Let M be a finitely generated submodule of* $\mathrm{Hom}(E_1, E_2)$*. Then $\mathbb{Q}M \cap \mathrm{Hom}(E_1, E_2) = \{\phi \in \mathrm{Hom}(E_1, E_2) | n\phi \in M\}$ for some n is also finitely generated.*

Proof. We may assume that E_1 and E_2 are isogenuous, otherwise $\mathrm{Hom}(E_1, E_2) = 0$. Then there is an injection $\mathrm{Hom}(E_1, E_2) \to \mathrm{End}(E_1)$, induced by isogeny $E_2 \to E_1$ and we will consider the case of $E_2 = E_1 = E$ for convenient notation.

Exercise 6.17. *The function $\phi \mapsto \deg \phi \in \mathbb{Z}$ on* $\mathrm{End}(E)$ *extends to homogeneous polynomial function of degree 2 on* $\mathrm{End}^0(E)$*.*

We will just use this exercise: since every $\phi \neq 0$ is an isogeny, $P(\phi) > 1$ is $\phi \in \mathrm{End}(E)$ and $\phi \neq 0$. But $\mathbb{Q}M$ is finite-dimensional space and $|P(\phi)| < 1$ is a neighborhood of 0 in this space intersecting with $\mathrm{End}(E)$ only by 0, therefore $\mathrm{End}(E) \cap \mathbb{Q}M$ is discrete in $\mathbb{Q}M$, hence finitely generated. □

From this point to prove the injectivity of

$$\mathrm{Hom}_K(E_1, E_2) \otimes \mathbb{Z}_l \to \mathrm{Hom}_K(T_l(E_1), T_l(E_2)),$$

$\phi \mapsto \phi_l$ it is enough to prove that for any finitely generated submodule $M \subset \mathrm{Hom}(E_1, E_2)$ such that $M = \mathbb{Q}M \cap \mathrm{Hom}(E_1, E_2)$, the map $\mathbb{Z}_l \otimes_{\mathbb{Z}} M \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2))$ is injective. Which is left as an exercise.

Since $\mathrm{Hom}^0(E_1, E_2)$ is finitely generated $\mathbb{Q}$-vector space it is evident by the lemma that $\mathrm{Hom}(E_1, E_2)$ is finitely generated $\mathbb{Z}$-module. □

6.4 Exercises

Exercise 6.18. *Let E be an elliptic curve and l a prime integer, not equal to* $\mathrm{char}K$ *if* $\mathrm{char}K > 0$*. Prove that the natural map* $\mathrm{Aut}(E) \to \mathrm{Aut}(E[m])$ *is injective except the case $m = 2$, when the kernel is* $[\pm 1]$*.*

Exercise 6.19. *Prove that the natural map* $\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(T_l(E_1), T_l(E_2))$ *is injective.*

Exercise 6.20. *Let E be an elliptic curve with complex multiplication over K,* $\mathrm{char}K = 0$*. Prove that for all primes l the action of $G_{\overline{K}/K}$ on the Tate module is abelian. (Hint: $f \in$* $\mathrm{End}_K(E)$ *commutes with action of $G_{\overline{K}/K}$ on $T_l(E)$).*

7 Lecture 7: Invariant differential, Weil pairing

7.1 Invariant differential

Recently we named the differential $\omega = \frac{\mathrm{d}x}{2y+a_1x+a_3}$ for elliptic curve $E : y^2 + a_1x + a_3y = x^3 + a_2x^2 + a_4x + a_6$ an invariant, now it's time to tell why.

Proposition 7.1. *Let E be an elliptic curve given by Weierstrass equation and $\omega = \frac{\mathrm{d}x}{2y+a_1x+a_3}$. Let τ_Q be a translation map, then $\tau_Q^*\omega = \omega$.*

Proof. To prove it we choose a function $a_Q \neq 0 \in \overline{K}(E)^*$ such that $\tau_Q^*\omega = a_Q\omega$, we can do it since Ω_E is one dimensional vector space over $\overline{K}(E)$. Then compute its divisor $\mathrm{div}(a_Q) = \mathrm{div}(\tau_Q^*\omega) - \mathrm{div}(\omega) = \tau_Q^*\mathrm{div}(\omega) - \mathrm{div}(\omega) = 0$, because $\mathrm{div}(\omega) = 0$.

So the function a_Q does not have any zeroes and poles, then it is a constant $a_Q \in \overline{K}^*$, now look at a rational map $f : E \to \mathbb{P}^1$, defined by $Q \mapsto (a_Q : 1)$, rational because a_Q can be viewed as a rational function of $x(Q)$ and $y(Q)$. But this map is not surjective (points $(0 : 1)$ and $(1 : 0)$), so it is constant and a_Q does not depend on Q, so equals to $a_O = 1$. □

Next theorem shows an important property of isogenies and invariant differential.

Theorem 7.2. *For two elliptic curves E, E' and invariant differential ω_E let $\phi, \psi : E' \to E$ be two isogenies. Then $(\phi + \psi)^*\omega_E = (\phi^* + \psi^*)\omega_E$.*

Proof. First one prove that if $\phi = [0]$ or $\phi + \psi = [0]$, then theorem holds. For this it's enough to check $[-1]^*\omega = -\omega$, which is calculation in coordinates for $-P$. Then we can assume that ϕ, ψ, $\phi + \psi \neq [0]$.

We want to write a formula for $\omega(P + Q) = f\omega(P) + g\omega(Q)$, where f, g are functions of variables: $x(P), y(P), x(Q), y(Q)$. If we fix a point Q, then $\mathrm{d}x(Q) = 0$ and we deduce that $f = 1$ by expressing $\omega(P + Q) = \tau_Q^*\omega(P) = \omega(P)$, similarly we can say that $g = 1$. So $\omega(P + Q) = f\omega(P) + g\omega(Q)$, then we substitute for P and Q values of ϕ and ψ in appropriate point P. Then $(\omega \circ (\phi + \psi))(P) = (\omega \circ \phi)(P) + (\omega \circ \psi)(P)$, whis implies the theorem. □

Corollary 7.3. *Let ω be an invariant differential on an elliptic curve E, let $m \in \mathbb{Z}$. Then $[m]^*\omega = m\omega$*

Proof is by induction on m: $[m + 1]^*\omega = [m]^*\omega + \omega$ by previous.

Corollary 7.4. *Let E be an elliptic curve and ω its invariant differential. We define a map $\mathrm{End}(E) \to \overline{K}$ by $\phi \mapsto a_\phi$, where a_ϕ is defined by $\phi^*\omega = a_\phi\omega$. Then*

1. *The map $\phi \mapsto a_\phi$ is a ring homomorphism;*

2. *Its kernel is the set of inseparable endomorphisms of E;*

3. *If $\mathrm{char}(K) = 0$, then $\mathrm{End}(E)$ is a commutative ring.*

Proof. First we should explain that a_ϕ from $\overline{K}(E)$ is actually in $\overline{K}$. As before we look at divisor of the function a_ϕ, say $\mathrm{div}(a_\phi) = \mathrm{div}(\phi^*\omega) - \mathrm{div}(\omega) = 0$, so a_ϕ is constant.

1. by theorem $a_{\phi+\psi}\omega = (\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega = a_\phi\omega + a_\psi\omega$. So $a_{\phi+\psi} = a_\phi + a_\psi$, then we should find $a_{\phi\circ\psi}\omega = (\phi\circ\psi)^*\omega = \psi^*(\phi^*\omega) = a_\phi\psi^*(\omega) = a_\phi a_\psi\omega$. So $a_{\phi\circ\psi} = a_\phi a\psi$.

2. Here $a_\phi = 0 \Leftrightarrow \phi^*\omega = 0 \Leftrightarrow \phi$ is inseparable.

3. In char $= 0$ everything is separable, so $\mathrm{End}(E)$ injects to $\overline{K}^*$, so $\mathrm{End}(E)$ is commutative.

□

7.2 Weil pairing

The Weil pairing has several definitions, we will use the following because of its simplicity:

For an elliptic curve E we define a pairing $e_m : E[m] \times E[m] \to \mu_m$: let $P, Q \in E[m]$ and we choose divisors $D_P \sim (P) - (O)$ and $D_Q \sim (Q) - (O)$ of degree 0 such that their supports are disjoint. Then observe functions f_P and f_Q such that $\operatorname{div}(f_P) = mD_P$ and $\operatorname{div}(f_Q) = mD_Q$, which exist because P and Q are of order m.

We define $e_m = \frac{f_P(D_Q)}{f_Q(D_P)}$ and therefore have to prove some necessary properties:

1. The definition of e_m does not depend on choice of D_P, D_Q, f_P, f_Q so e_m is well-defined.

2. e_m maps to μ_m;

3. It is bilinear: $e_m(P_1 + P_2, Q) = e_m(P_1, Q)e_m(P_2, Q)$; $e_m(P, Q_1 + Q_2) = e_m(P, Q_1)e_m(P, Q_2)$;

4. It is alternating: $e_m(P, P) = 1$; $e_m(P, Q) = e_m(Q, P)^{-1}$;

5. It is nondegenerate: if $e_m(P, Q) = 1$ for all $P \in E[m]$, then $Q = O$;

6. $e_{mm'}(P, Q) = e_m([m']P, Q)$ for all $P \in E[mm']$ and $Q \in E[m]$.

Proof. Remind first of all, how to define a function of divisor: for $D = \sum_{P \in E} n_P P$ we say $f(D) = \prod_{P \in E} f(P)^{n_P}$. More we should remember Weil reciprocity law:

$$f(\operatorname{div}(g)) = g(\operatorname{div}(f));$$

Then properties

1. and

2. follow from Weil reciprocity law: we have $f_P(\operatorname{div} f_Q) = f_P(mD_Q) = f_Q(mD_P) = f_Q(\operatorname{div} f_P)$, so $\frac{f_P(D_Q)}{f_Q(D_P)}$ takes values in μ_m and e_m does not depend on D_P, D_Q, f_P, f_Q because for any function $g \in \overline{K}(E)$ we have $g(mP - mO)$ does not depend on g since $mP = O$;

3. We prove that $e_m(P_1{+}P_2, Q) = e_m(P_1, Q)e_m(P_2, Q)$ and deduce $e_m(P, Q_1{+}Q_2) = e_m(P, Q_1)e_m(P, Q_2)$ from next statement $e_m(P, Q) = e_m(Q, P)^{-1}$, which follows immediately from definition: so we should prove that

   $$\frac{f_{P_1+P_2}(D_Q)}{f_Q(D_{P_1+P_2})} = \frac{f_{P_1}(D_Q)f_{P_2}(D_Q)}{f_Q(D_{P_1})f_Q(D_{P_2})}$$

   By criterion for Elliptic curves a divisor $\sum_{n_P} P$ is principal iff $\sum_{n_P} = 0$ and $\sum[n_P]P = O$, so for two points $P_1, P_2 \in E$ the divisor $(P_1 + P_2) - (P_1) - (P_2) - (O)$ is principal, say $\operatorname{div} h$. Then we obtain an equality $\operatorname{div}(\frac{f_{P_1+P_2}}{f_{P_1}f_{P_2}}) = \operatorname{div}(h^m)$, so $\frac{f_{P_1+P_2}}{f_{P_1}f_{P_2}} = ch^m$ for appropriate constant c.

   Now we rewrite a desired equation in following way:

   $$\frac{f_{P_1+P_2}(Q)f_{P_1}(O)f_{P_2}(O)}{f_{P_1+P_2}(O)f_{P_1}(Q)f_{P_2}(Q)} = \frac{f_Q(P_1 + P_2)f_Q(O)}{f_Q(P_1)f_Q(P_2)}$$

   The left-hand side of the equation is $(\frac{f_{P_1+P_2}}{f_{P_1}f_{P_2}})(Q)(\frac{f_{P_1}f_{P_2}}{f_{P_1+P_2}})(O) = \frac{ch^m(Q)}{ch^m(O)} = h(m(Q) - m(O)) = h(mD_Q) = h(\operatorname{div}(f_Q)) = f_Q(\operatorname{div}(h))$, the last by Weil reciprocity law. Look at right-hand side, which is by definition $f_Q(\operatorname{div}(h))$.

4. obvious from definition;

5. Assume that for all points $P, Q \in E[m]$ the following holds: $f_P(D_Q) = f_Q(D_P)$, which is equal to suggestion that the Weil pairing is degenerate. As above we have $D_{P+Q} - D_P - D_Q = \operatorname{div} h$ for some h, we will assume that $f_P(D_P) = c_P^{2m}$.

   First we take f_P of this equality and get

   $$f_P(D_{P+Q}) = f_P(D_P)f_P(D_Q)f_P(\operatorname{div} h)$$

   and by our assumption and Weil reciprocity law

   $$f_{P+Q}(D_P) = c_P^{2m} f_Q(D_P)h^m(D_P),$$

   here we used $f_P(D_Q) = f_Q(D_P)$ Now similarly take f_Q of that equality and get $f_{P+Q}(D_Q) = c_Q^{2m} f_Q(D_P)h^m(D_Q)$, after that we take f_{P+Q} of equality and obtain $c_{P+Q}^{2m} = f_{P+Q}(D_P + D_Q)h^m(D_{P+Q})$.

Then dividing second by first $f_{P+Q}(D_Q - D_P) = \frac{c_Q^{2m}}{c_P^{2m}} h^m(D_Q - D_P)$, and from here follows $f_{P+Q}(D_Q) = \frac{c_Q^{2m}}{c_P^{2m}} \frac{h^m(D_Q)}{h^m(D_P)} f_{P+Q}(D_P)$ and putting it into the $f_{P+Q}(D_P) f_{P+Q}(D_Q) = \frac{c_{P+Q}^{2m}}{h^m(D_P) h^m(D_Q)}$ we get $f_{P+Q}^2(D_P) = \frac{1}{h^{2m}(D_Q)} \frac{c_Q^{2m} c_{P+Q}^{2m}}{c_P^{2m}}$, which means since any point $R \in E[m]$ can be obtained as a sum $R = P + Q$ for given P and some Q, that $f_P = g_P^m$ for an appropriate g_P. Which is impossible unless $P = O$.

6. The proof is by induction on m', for $m' = 1$ all is ok. Assume we know $e_{m(m'-1)}(P, Q) = e_m([m'-1]P, Q)$, and now should prove $e_{mm'}(P, Q) = e_m([m']P, Q)$, by 3. we know $e_m([m'-1]P, Q) e_m(P, Q) = e_m([m']P, Q)$, so we need only to prove that

   $$e_{m(m'-1)}(P, Q) e_m(P, Q) = e_{mm'}(P, Q).$$

   Let's look at the corresponding functions: f_P, f_Q, g_P, g_Q, h_P, h_Q, for which we have $\operatorname{div}(f_P) = m(P) - m(O)$, $\operatorname{div}(h_P) = m(m'-1)(P) - m(m'-1)(O)$, $\operatorname{div}(g_P) = mm'(P) - mm'(O)$ and similarly for Q.

   One can see that $\operatorname{div}(g_P) = \operatorname{div}(f_P) + \operatorname{div}(h_P)$, so for any Q holds $g_P(D_Q) = f_P(D_Q) h_P(D_Q)$, analogous implications for Q give $g_Q(D_P) = f_Q(D_P) h_Q(D_P)$, so by definition

   $$e_{mm'}(P, Q) = \frac{g_P(D_Q)}{g_Q(D_P)} = \frac{h_P(D_Q) f_P(D_Q)}{h_Q(D_P) f_Q(D_P)} = e_{m(m'-1)}(P, Q) e_m(P, Q).$$

□

Corollary 7.5. *There exist points P, Q such that $e_m(P, Q)$ is the primitive m-th root of unity.*

The image of $e_m : E[m] \times E[m] \to \mu_m$ is a subgroup of μ_m, assume it is μ_d, then for all (P, Q) we have $e_m(P, Q)^d = e_m([d]P, Q) = 1$, which is by nondegeneracy false unless $d = m$.

Proposition 7.6. *Let $\phi : E_1 \to E_2$ be an isogeny. We take points $P \in E_1[m]$ and $Q \in E_2[m]$, then*

$$e_m(P, \hat{\phi}(Q)) = e_m(\phi(P), Q)$$

Proof. So we need to prove that

$$\frac{f_P(D_{\hat{\phi}Q})}{f_{\hat{\phi}Q}(D_P)} = \frac{f_{\phi(P)}D_Q}{f_Q(D_{\phi(P)})}$$

First, look at divisor $D_{\hat{\phi}(Q)} = (\hat{\phi}Q) - (O) = (\sum[n_P]P) - (O)$ by definition of $\hat{\phi}$, where $\sum n_P(P) = \phi^*(D_Q)$ is the image of $D_Q = (Q) - (O) = \kappa_2(Q)$ under ϕ^*, so we know that there exists a function h such that $\phi^*(D_Q) = D_{\hat{\phi}(Q)} + \mathrm{div}h$.

Now we want to find $f_{\hat{\phi}Q}$. We take $mD_{\hat{\phi}(Q)} = m\phi^*(D_Q) - m\mathrm{div}h = \phi^*(\mathrm{div}f) - \mathrm{div}(h^m)$, so by $\phi^*(\mathrm{div}f) = \mathrm{div}(f \circ \phi)$ we take $f_{\hat{\phi}Q} = \frac{f\circ\phi}{h^m}$ for an appropriate h.

Then left-hand side of desired equality transforms as following:

$$\frac{f_P(D_{\hat{\phi}Q})}{f_{\hat{\phi}Q}(D_P)} = \frac{f_P(\phi^* D_Q - \mathrm{div}h)}{f_{\hat{\phi}Q}(D_P)} = \frac{f_P(\phi^* D_Q)h^m(D_P)}{f_P(\mathrm{div}h)f_Q(\phi D_P)} = \frac{f_P(\phi^* D_Q)}{f_Q(\phi D_P)}$$

where the last equality by the Weil reciprocity law.

One can easily see that $f_Q(\phi D_P) = f_Q(D_{\phi(P)})$, so the left to prove is

$$f_P(\phi^* D_Q) = f_{\phi(P)}(D_Q),$$

but by definition of ϕ_* and since ϕ is an isogeny $\phi_*(\mathrm{div}f_P) = \phi_*(m(P) - m(O)) = m(\phi P) - m(O) = \mathrm{div}f_{\phi(P)}$ and by 2.18.4 we have $\phi_*\mathrm{div}(f_P) = \mathrm{div}(\phi_* f_P)$, so we need to prove that

$$f_P(\phi^*((Q))) = (\phi_* f_P)(Q),$$

where in left-hand side is divisor (Q) and in right-hand side Q is a point.

Then left part is $\prod_{X\in\phi^{-1}Q} f_P(X)^{e_\phi(X)}$ which is $(\phi_* f_P)(Q)$ by definition of ϕ_* on functions $\phi_* f = \phi^{*-1}(N_{K(E_1)/\phi^* K(E_2)} f)$. □

Now we want to apply this theory to get l-adic Weil pairing on the Tate module for $l \neq \mathrm{char}K$ in following way: we take all $e_{l^n} : E[l^n] \times E[l^n] \to \mu_{l^n}$ and put it into inverse limits of $E[l^{n+1}] \xrightarrow{[l]} E[l^n]$ and $\mu_{l^{n+1}} \xrightarrow{\xi\mapsto\xi^l} \mu_{l^n}$, so we have a map

$$e : T_l(E) \times T_l(E) \to T_l(\mu).$$

We need to prove that all e_{l^n}s are compatible with inverse limits. For that we have to show $e_{l^{n+1}}(P,Q)^l = e_{l^n}([l]P,[l]Q)$ for all $P, Q \in E[l^{n+1}]$. By linearity of $e_{l^{n+1}}$ we have $e_{l^{n+1}}(P,Q)^l = e_{l^{n+1}}(P,[l]Q)$, then from 6. property for points P, $[l]Q$ and values $m = l^n$, $m' = l$ follows $e_{l^{n+1}}(P,Q)^l = e_{l^n}([l]P,[l]Q)$, so e is well-defined.

It also has all properties of e_m (it is bilinear, alternating, nondegenerate) and for an isogeny $\phi : E_1 \to E_2$ and dual $\hat{\phi} : E_2 \to E_1$ we have $e(\phi P, Q) = e(P, \hat{\phi} Q)$.

7.3 Additional: Proof of statement from previous lecture

Here we will prove 3, let me remind you the statement:

Proposition 7.7. *Let $\phi : E_1 \to E_2$ be an isogeny of degree m. Let $\psi : E_1 \to E_2$ be another isogeny, then $\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}$;*

Proof. We will work with char$K \neq 2$, from the statement of proposition we have deduced already that for integer m the degree of corresponding isogeny $\deg[m] = m^2$. But now we have to prove it directly for case $m = 2^k$. First mention that for $k = 1$ the assertion is evident by explicit formula of coordinate functions for $[2]P$ depending on coordinates of P. Next from the formula for degree of composition of two isogenies $\deg(\phi \circ \psi) = \deg\phi \times \deg\psi$ deduce necessary for any k. Then since char$K \neq 2$ and $[m]$ is separable, we have $|\ker[m]| = \deg[m] = m^2$, therefore $|E[2^k]| = 4^k$ and by exercise on properties of abelian group from exam we then have $E[2^k] = \mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/2^k\mathbb{Z}$ for any k.

Now for an integer m, such that $E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ we have built the Weil pairing $e_m : E[m] \times E[m] \to \mu_m$ with all necessary properties. Then $e_m(P, \widehat{\phi + \psi}(Q)) = e_m((\phi + \psi)(P), Q) = e_m(\phi(P), Q) e_m(\psi(P), Q) = e_m(P, \widehat{\phi}(Q)) e_m(P, \widehat{\psi}(Q)) = e_m(P, \widehat{\phi}(Q) + \widehat{\psi}(Q))$ which is true for all m such that $|E[m]| = m^2$, i. e. for all $m = 2^k$ and all $P, Q \in E[m]$. From nondegeneracy of Weil pairing we deduce the desired property.

For the case of char$K = 2$ one should look at the $m = 3^k$ instead of 2^k. □

7.4 Exercises

Exercise 7.8. *Here is usual definition of the Weil pairing. For a point $P \in E[m]$ we take our function f_P with* $\operatorname{div}(f_P) = m(P) - m(O)$. *Next take a point $P' \in E[m^2]$ such that $mP' = P$, then there is a function g_P*

which divisor $\operatorname{div}(g_P) = [m]^*(P) - [m]^*(O) = \sum_{R\in E[m]}(P' + R) - (R)$*, so* $\operatorname{div}(g^m) = \operatorname{div}(f \circ [m])$.

For an m-torsion point $Q \in E[m]$ *(may be* $P = Q$*) we have* $g_P(X + Q)^m = g_P(X)^m$*, then the function* $Q \mapsto \frac{g_P(X+Q)}{g_P(X)}$ *takes only finitely many values, so* $E \to \mathbb{P}^1$ *is not surjective and therefore constant. We define* $e_m : E[m] \times E[m] \to \mu_m$ *by* $e_m(P, Q) = \frac{g_P(X+Q)}{g_P(X)}$.

The exercise consists only of proving that both definitions of Weil pairing give the same result.

8 Lecture 8: elliptic curves over $\mathbb{C}$

The main reference for this lecture is [7]. Today we will prove that elliptic curve over $\mathbb{C}$ is a Riemann surface of algebraic function and also factor $\mathbb{C}/L$ by a lattice in $\mathbb{C}$. More precisely:

Theorem 8.1. *The following categories are equivalent:*

- *Objects: Elliptic curves over* $\mathbb{C}$*, maps: isogenies;*
- *Objects: Elliptic curves over* $\mathbb{C}$*, maps: complex analytic maps taking* O *to* O*;*
- *Objects: Lattices* L *up to homothety, maps:* $\{\alpha \in \mathbb{C}, \alpha L_1 \subset L_2\}$*;*

But to describe an analytic point of view on elliptic curves over $\mathbb{C}$ we start with far away object — Riemann surface.

8.1 Elliptic curve as a Riemann surface

Definition 8.2. *The Riemann surface is Hausdorff topological space* X *with countable base and additional structure:*

1. X *is represented as a union of open subsets* U_α*, named coordinate neighborhoods;*
2. *For every coordinate neighborhood* U_α *given a homeomorphism* $\phi : U_\alpha \to V_\alpha$*, where* $V_\alpha \subset \mathbb{C}$ *is open subset;*
3. *If* U_α*,* U_β *two coordinate neighborhoods with nonempty intersection, then the map* $\phi_{\alpha\beta} : \phi_\alpha(U_\alpha \cap U_\beta) \to \phi_\beta(U_\alpha \cap U_\beta)$ *given by* $x \mapsto \phi_\beta(\phi_\alpha^{-1}(x))$ *is an isomorphism.*

Example 8.3. *Let $L \subset \mathbb{C}$ be a lattice (additive subgroup, generated by two linearly independent over $\mathbb{R}$ complex numbers ω_1, ω_2). We look at $X = \mathbb{C}/L$ with factortopology. The natural map $p : \mathbb{C} \to X$ is a covering.*

We take as coordinate neighborhoods small $U_\alpha \subset X$ such that the covering over them splits into direct product and as a local chart take any section of that covering. Coordinate change maps are translations by elements of L, so they are holomorphic, therefore X is a Riemann surface which we will call E by some reasons.

For a lattice $L = \langle \omega_1, \omega_2 \rangle$ we give a notion of an elliptic function relative to L as a function $f(z)$ on $\mathbb{C}$ that satisfies $f(z+\omega) = f(z)$ for all $z \in \mathbb{C}$ and $\omega \in L$.

One can see that a meromorphic function on E is the same thing as a meromorphic function on $\mathbb{C}$ with periods ω_1, ω_2. Such function we will call elliptic.

Definition 8.4. *Let $L \subset \mathbb{C}$ be a lattice. The Weierstrass $\wp$-function relative to L is*

$$\wp(z, L) = \frac{1}{z^2} + \sum_{\omega \neq 0 \in L} \Big(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \Big)$$

The Eisenstein series of weight $2k$ is $G_k(L) = \sum_{\omega \neq 0 \in L} \omega^{-2k}$.

Proposition 8.5. *Let L be a lattice. Then*

1. *The Eisenstein series $G_{2k}(L)$ is absolutely convergent for all $k > 1$;*

2. *The series defining the Weierstrass $\wp$-function converges absolutely and uniformly on every compact subset of $\mathbb{C}/L$. The series defines a meromorphic, even, elliptic function on $\mathbb{C}$ having a double pole with residue 0 at every point of L and no other poles.*

Proof.

The lattice L is discrete, there exist a constant c in $\mathbb{C}$, so for all $N \geq 1$ the number of points in the ring $|\{\omega \in L : N \leq |\omega| \leq N+1\}| < cN$. So

$$\sum_{\omega \in L, |\omega| \geq 1} \frac{1}{|\omega|^{2k}} \leq \sum_{N=1}^{\infty} \frac{|\{\omega \in L : N \leq |\omega| < N+1\}|}{N^{2k}} < \sum_{N=1}^{\infty} \frac{c}{N^{2k-1}} < \infty.$$

We estimate for $|\omega| > 2|z|$

$$\Big|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\Big| = \Big|\frac{z(2\omega - z)}{\omega^2(z-\omega)^2}\Big| \leq \frac{|z|(2|\omega| + |z|)}{|\omega|^2(|\omega| - |z|)^2} \leq \frac{10|z|}{|\omega|^3}.$$

Then from 1. it follows that $\wp(z)$ is absolutely convergent for all $z \in \mathbb{C} \setminus L$ and uniformly convergent on every compact subset of $\mathbb{C} \setminus L$. So $\wp(z)$ defines a holomorphic function on $\mathbb{C} \setminus L$ with double pole at any $z \in L$, moreover it is obviously even, we see $\wp(z) = \wp(-z)$.

Differentiating term by term we compute $\wp'(z) = -2\sum_{\omega \in L} \frac{1}{(z-\omega)^2}$, from here $\wp'(z)$ is an elliptic function, so $\wp'(z+\omega) = \wp'(z)$ for $\omega \in L$. After integrating we obtain $\wp(z+\omega) = \wp(z) + c(\omega)$, setting $z = -\frac{\omega}{2}$ by evenness of $\wp(z)$ we get $c(\omega) = 0$, so $\wp(z)$ is an elliptic function. □

Corollary 8.6. *The function $\wp'$ is meromorphic over $\mathbb{C}$, odd, and has periods ω_1, ω_2, poles of order 3 at every point of lattice, and doesn't have any other poles, the main Laurent series part is $-2/z^3$.*

Proposition 8.7. *Functions $\wp, \wp'$ are related as*

$$(\wp'(z))^2 = 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3).$$

Proof. Left and righthand sides are meromorphic functions on E with poles of order 6 at 0 and no other poles, and vanishing at other points of order two with multiplicity 2, having no other zeroes. So $\frac{(\wp'(z))^2}{4(\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3)}$ is holomorphic on E, so constant. Comparing coefficients we get value of this constant. □

We look at elliptic curve $E = \mathbb{C}/L$ as an abelian group, obviously isomorphic to $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$, so E has exactly four points of order 2, namely images of 0, $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$, $\frac{(\omega_1+\omega_2)}{2}$.

Proposition 8.8. *One can look at function $\wp$ as a holomorphic map from E to the Riemann sphere $\overline{\mathbb{C}} = \mathbb{C} \cup \infty$, this map has degree 2 and function $\wp'$ has degree 3. The map $\wp$ is ramified with ramification index equal to 2 in points of order 2, and it is unramified elsewhere.*

If we have $\wp(a_1) = \wp(a_2)$, where $a_i \in E$, then $a_2 = \pm a_1$ (or for complex numbers $a_2 \equiv a_1 (\mod L)$).

If $a \in \mathbb{C}$ is a number corresponding to the point of order 2, nonequal to O, then $\wp'(a) = 0$. If $\wp'(z) = 0$, then z is equivalent with respect to L to $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$, $\frac{(\omega_1+\omega_2)}{2}$.

Proposition 8.9. *Elliptic curve E is isomorphic to a Riemann surface, given by an equation*
$$y^2 = 4(z - e_1)(z - e_2)(z - e_3).$$

Proof. Here we assume numbers e_i to be different. Denote by X a compact Riemann surface, corresponding to algebraic function with above equality, by $E_0 \subset E$ subset, obtaining from E by deleting points of order 2, and by X_0 a subset of $\mathbb{C}^2$ consisting of points, for which the equality holds, but $z \notin \{e_1, e_2, e_3\}$, such that X comes from X_0 by adding points lying over e_1, e_2, e_3, ∞.

We define the holomorphic map $\phi_0 : E_0 \to X_0$ by $z \mapsto (\wp(z), \wp'(z))$. We need to show that this map is a bijection $E_0 \to X_0$, indeed if $\wp(a_1) = \wp(a_2)$ and both $a_i \in E_0$, then $a_1 = \pm a_2$ by previous proposition, but by oddness of $\wp'$ we have $\wp'(-a_1) = -\wp'(a_1)$ we throw out the case $a_1 = -a_2$ and get an injectivity.

Since $E \to \overline{\mathbb{C}}$ is surjective, for every $(z, \omega) \in X_0$ there exists $a \in E$ such that $z = \wp(a) = \wp(-a)$, therefore oddness of $\wp'$ implies that either $\wp'(a)$, or $\wp'(-a)$ equals to ω, so ϕ_0 is surjective also.

We obtained a holomorphic bijection $\phi_0 : E_0 \to X_0$, which continues to a map $\phi : E \to X$ by sending O to point over ∞ and point a of order 2 to a point over $\wp(a)$. This is evident that ϕ is continuous, therefore by Riemann theorem holomorphic and that the inverse map is also holomorphic. □

The inverse statement is also true

Proposition 8.10. *A Riemann surface given by the equation of the form*

$$y^2 = c(x - e_1)(x - e_2)(x - e_3)$$

where a constant $c \neq 0$ and all e_i are different, is an elliptic curve.

8.2 Classification of elliptic curves

We are going to study which properties of $E = \mathbb{C}/L$ depend on L. Denote by $\mathcal{L}$ the set of all lattices in $\mathbb{C}$ and for $\lambda \in \mathbb{C}^*$ by λL we denote the lattice obtained from L by multiplying all its elements.

Proposition 8.11. *Elliptic curves $E = \mathbb{C}/L$ and $E' = \mathbb{C}/L'$ are isomorphic iff $L' = \lambda L$ for some $\lambda \in \mathbb{C}^*$.*

Proof. For two homothetic lattices $L' = \lambda L$ we have an isomorphism of factorgroups $\mathbb{C}/L \to \mathbb{C}/L'$ given by multiplication by λ, so we need only to prove the part $\Rightarrow$.

Assume we have an isogeny $\phi : E \to E'$. By lifting a map ϕ to the map of universal coverings of E and E' we get a holomorphic map which sends $\tilde{\phi}(0) = 0$ and $\tilde{\phi} : \mathbb{C} \to \mathbb{C}$ such that $\tilde{\phi}(z + \omega) - \tilde{\phi}(z) \in L$ for all $z \in \mathbb{C}$ and $\omega \in L$. Since L' is discrete we get $\tilde{\phi}(z + \omega) - \tilde{\phi}(z) = \mathit{const}$ for all $\omega \in L$, so $\tilde{\phi}'(z + \omega) = \tilde{\phi}'(z)$ for all $\omega \in L$, since $\tilde{\phi}'$ is holomorphic on $\mathbb{C}$ it is a constant, so $\tilde{\phi}(z) = az + b$ for $a \neq 0, b \in \mathbb{C}$.

Since $\tilde{\phi}(0) = 0$, we have $b = 0$, and since $\tilde{\phi}$ is a lift of $\phi : \mathbb{C}/L \to \mathbb{C}/L'$ we see that $\lambda L \subset L'$ and since degree of ϕ equals to one, we get $\lambda L = L'$. □

Now let us think about lattices L with given numeration on the set $(1/2L)/L$ and maps preserving this numeration. We denote this set by $\tilde{\mathcal{L}}$. Then e_i from proposition 8.9 are functions from $\tilde{\mathcal{L}} \to \mathbb{C}$, such that for $\tilde{L} \in \tilde{\mathcal{L}}$ and $\lambda \in \mathbb{C}^*$ holds $e_i(\lambda\tilde{L}) = \lambda^{-2}e_i(\tilde{L})$.

Definition 8.12. *A function $k^2 : \tilde{\mathcal{L}} \to \mathbb{C} \setminus \{0, 1\}$ is defined by the formula $k^2(\tilde{L}) = \frac{e_2 - e_3}{e_1 - e_3}$.*

Note that from the above its clear that $k^2(\lambda\tilde{L}) = k^2(\tilde{L})$ for $\lambda \in \mathbb{C}^*$ and $\tilde{L} \in \tilde{\mathcal{L}}$.

And the map $k^2 : \tilde{\mathcal{L}} \to \mathbb{C} \setminus \{0, 1\}$ is surjective. Indeed, take for $a \in \mathbb{C} \setminus \{0, 1\}$ a lattice corresponding to an elliptic curve given by equation $y^2 = z(x - 1)(x - a)$.

Now we prove that the value of k^2 defines an elliptic curve with numeration on points of order two.

Proposition 8.13. *Elliptic curves $E = \mathbb{C}/L$ and $E' = \mathbb{C}/L'$ are isomorphic iff there are numerations on their points of order two such that corresponding values of k^2 are equal.*

Proof. Again its is necessary to prove only a part $\Leftarrow$, inverse is evident. Imagine we have two elliptic curves with numerations on theirs points of order 2 such that $k^2(\tilde{L}) = k^2(\tilde{L'})$. Then by proposition 8.9 E and E' are isomorphic to Riemann surfaces with equations $y^2 = 4(x - p_1)(x - p_2)(x - p_3)$ and $y^2 = 4(x - p'_1)(x - p'_2)(x - p'_3)$ corresponding, and there exist numbers $a \in \mathbb{C}^*$ and $b \in \mathbb{C}$ such that $p'_i = ap_i + b$. Then the map $x \mapsto ax + b$, $y \mapsto \sqrt[3]{a}y$ is an isomorphism of these Riemann surfaces. □

The final proposition of this lecture is to define a j-invariant of an elliptic curve.

Proposition 8.14. *The number*

$$j(L) = 256\frac{((k^2)^2 - k^2 + 1)^3}{(k^2)^2(k^2-1)^2}$$

Is called the j-invariant of an elliptic curve $E = \mathbb{C}/L$ and has the following properties:

1. *$j(L)$ does not depend of numeration on points of order two;*
2. *Elliptic curves $E = \mathbb{C}/L$ and $E' = \mathbb{C}/L'$ are isomorphic iff $j(L) = j(L')$;*
3. *The map $j : \mathcal{L} \to \mathbb{C}$ is surjective.*

The idea of proof 1. is to look at possible permutations of points of order two and understand that appearing changes of k^2 do not influence $j \neq 0, 1728$, in two other cases the statement should be checked by hands. Then 1. implies 2., surjectivity 3. follows from surjectivity of $k^2 : \tilde{\mathcal{L}} \to \mathbb{C} \setminus \{0,1\}$.

8.3 Exercises

Exercise 8.15. *Prove that two definitions of j-invariant for elliptic curve given in these lectures, namely $j(E) = \frac{1728(4a^3)}{4a^3+27b^2}$ and $j(E) = 256\frac{((k^2)^2-k^2+1)^3}{(k^2)^2(k^2-1)^2}$ give the same answer in the case of the field $\mathbb{C}$.*

Exercise 8.16. *Find j-invariants for following lattices: 1. The square lattice: $\langle 1, i\rangle$; 2. The lattice $\langle 1, \xi = \frac{1+\sqrt{-3}}{2}\rangle$*

Exercise 8.17. *Let $E = \mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}$ be an elliptic curve, points $P_1 = a + b\tau$ and $P_2 = c + d\tau \in E[m]$ — two points of order m, namely $a, b, c, d \in \frac{1}{m}\mathbb{Z}$. We set $e_m(P_1, P_2) = \exp(2\pi i(ad - bc)) \in \mu_m$. Prove that obtained e_m, or its inverse e_m^{-1} coincides with the Weil pairing.*

9 Lecture 9: Elliptic curves over finite fields

Here we fix some notation for the whole lecture $q = p^r$, $\mathbb{F}_q$ — the field with q elements, $\mathbb{F}_{q^n}$ — its extension of degree n.

First of all we want to talk about one of the most important object associated to a curve over $\mathbb{F}_q$ — its number of rational points and Hasse theorem.

9.1 Number of rational points

We want to know number of solutions of the equation $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, where $(x, y) \in \mathbb{F}_q^2$, for which we have an evident upper bound $E(\mathbb{F}_q) \leq 2q + 1$ and the following

Theorem 9.1. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Then $|E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$.*

Proof. We know that the absolute Galois group is generated by the q^{th}-power Frobenius: $\phi : E \to E$, $(x, y) \mapsto (x^q, y^q)$, so for any point $P \in E(\overline{\mathbb{F}_q})$ we have that $P \in E(\mathbb{F}_q)$ iff $\phi(P) = P$. Therefore $E(\mathbb{F}_q) = \ker(1 - \phi)$ and so $|E(\mathbb{F}_q)| = \deg(1 - \phi)$.

For further we need

Lemma 9.2. *The degree map* $\deg \operatorname{Hom}(E_1, E_2) \to \mathbb{Z}$ *is the positive defined quadratic form.*

Lemma 9.3. *For an abelian group A and a positive defined quadratic form $d : A \to \mathbb{Z}$ we have $|d(a - b) - d(a) - d(b)| \leq 2\sqrt{d(a)d(b)}$ for all $a, b \in A$.*

Proof of this is exercise.

To prove the above theorem take instead of a, b morphisms $1, \phi$, and a quadratic form — degree of morphism. □

9.2 The Weil conjectures

We will state the Weil conjectures for a projective variety V over $\mathbb{F}_q$, but our main aim is to prove them for an elliptic curve.

Let $V/\mathbb{F}_q$ be a projective variety (a set of solutions for system of homogeneous polynomials with coefficients in $\mathbb{F}_q$). One can look at solutions of that system in $\overline{\mathbb{F}_q}$ and for any extension $\mathbb{F}_{q^n}$, namely the set of points in of $V(\overline{\mathbb{F}_q})$ with coordinates in $\mathbb{F}_{q^n}$. We are looking for a number of points in $V(\mathbb{F}_{q^n})$.

Definition 9.4. *The zeta function of $V/\mathbb{F}_q$ is the series*

$$Z(V/\mathbb{F}_{q^n}, t) = \exp(\sum_{n=1}^{\infty} |V(\mathbb{F}_{q^n})| \frac{t^n}{n}).$$

Moreover we can extract all $|V(\mathbb{F}_{q^n})|$ from $Z(V/\mathbb{F}_{q^n}, t)$ by the formula

$$|V(\mathbb{F}_{q^n})| = \frac{1}{(n-1)!} \frac{\mathrm{d}^n}{\mathrm{d}t^n} \log Z(V/\mathbb{F}_q, t)|_{t=0}.$$

Here we take usual definitions of exponent and logarithm of a series.

Exercise 9.5. *For $V = \mathbb{P}^m$ count a number of points $|\mathbb{P}^m(\mathbb{F}_{q^n})|$ for all n and write down the zeta function of V. In this case it is a rational function of t with coefficients in rational numbers.*

Note that if there are numbers $\alpha_1, ..., \alpha_r \in \mathbb{C}$ such that $|V(\mathbb{F}_{q^n})| = \pm\alpha_1^n, ..., \pm\alpha_r^n$, then the zeta function $Z(V/\mathbb{F}_q, t)$ is rational.

Now we state the Weil conjectures for an algebraic variety.

Theorem 9.6. *Let $V/\mathbb{F}_q$ be a smooth projective algebraic variety of dimension m. Then*

1. *$Z(V/\mathbb{F}_q, t) \in \mathbb{Q}(t)$ is a rational function; Namely it can be represented as*

$$Z(V/\mathbb{F}_q, t) = \frac{P_1(t)...P_{2m-1}(t)}{P_0(t)...P_{2m}(t)} = \prod_{i=0}^{2m} P_i(t)^{(-1)^{i+1}},$$

   where every $P_i(t) \in \mathbb{Z}[t]$ and $P_0(t) = 1 - t$, $P_{2m}(t) = 1 - q^m t$, and for every $0 \leq i \leq 2m$ the polynomial $P_i(t)$ factors as $P_i(t) = \prod_{j=1}^{b_i}(1 - \alpha_{ij})$ for some α_{ij};

2. *It satisfies a functional equation: there exists an integer $E(V)$ such that*

$$Z(V/\mathbb{F}_q, \frac{1}{q^m} t) = \pm q^{\frac{mE(V)}{2}} t^{E(V)} Z(V/\mathbb{F}_q, t)$$

3. *An analog of Riemann Hypothesis: the numbers α_{ij} satisfy the property $|\alpha_{ij}| = \sqrt{q}$;*

4. *If V is a good reduction modulo p of a non-singular projective variety V' defined over $\mathbb{C}$, then all b_i are the i-th Betti numbers of the space of complex numbers of V'.*

Remark 9.7. *Note that (2.) of the theorem 9.6 is equivalent to the following statement: for $t = q^{-s}$ we say $\zeta(V,s) = Z(V,t)$, then $\zeta(V, m-s) = \pm q^{\frac{mE(V)}{2} - E(V)s}\zeta(V,s)$.*

Also the analog of Riemann Hypothesis implies that all zeroes of $P_j(t)$ lie on the "critical line" of complex numbers ω with $\mathrm{Re}(\omega) = j/2$.

We will prove these conjectures for elliptic curves. For a prime number $l \neq p = \mathrm{char}(\mathbb{F}_q)$, there is a representation $\mathrm{End}(E) \to \mathrm{End}(T_l(E))$, by $\psi \mapsto \psi_l$, we choose a $\mathbb{Z}_l$-basis for $T_l(E)$ and write ψ_l as a 2×2 matrix to compute its determinant and trace $\det\psi_l$, $\mathrm{Tr}\,\psi_l \in \mathbb{Z}_l$.

Recall

Proposition 9.8. *Let $\psi \in \mathrm{End}(E)$, then $\det\psi_l = \deg\psi$, and $\mathrm{Tr}\,\psi_l = 1 + \deg\psi - \deg(1-\psi)$. This implies that for all l, $\det\psi_l$ and $\mathrm{Tr}\,\psi_l$ are in $\mathbb{Z}$, and are the equal.*

We will need it to apply for an elliptic curve over finite field and its Frobenius.

Theorem 9.9. *Let $E/\mathbb{F}_q$ be an elliptic curve and $\phi : E \to E$ as $(x,y) \mapsto (x^q, y^q)$ be a Frobenius endomorphism. We denote $a_q = Q + 1 - |E(\mathbb{F}_q)|$.*

1. *Let α_q, β_q be the roots of polynomial $x^2 - a_q x + q$, then α_q, β_q are complex conjugates with $|\alpha_q| = |\beta_q| = \sqrt{q}$ and for all n*

$$|E(\mathbb{F}_{q^n})| = q^n + 1 - \alpha_q^n - \beta_q^n.$$

2. *For the Frobenius endomorphism the following is true $\phi^2 - a_q\phi + q = 0$.*

Proof. We know already that $|E(\mathbb{F}_q)| = \deg(1-\phi)$ and now use previous proposition for $l \neq p$ to get $\det(\phi_l) = \deg(\phi) = q$, $\mathrm{Tr}(\phi_l) = 1 + \deg(\phi) - \deg(1-\phi) = 1 + q - |E(\mathbb{F}_q)| = a_q$, so the characteristic polynomial for ϕ_l is $\det(t - \phi_l) = t^2 - \mathrm{Tr}(\phi_l)t + \det(\phi_l) = t^2 - a_q t + q$.

1. Factor the characteristic polynomial of ϕ_l over $\mathbb{C}$ as $\det(t-\phi_l) = (t - \alpha_q)(t-\beta_q)$.

   For any rational $\frac{m}{n}$ we have $\det(\frac{m}{n} - \phi_l) = \frac{\det(m - n\phi_l)}{n^2} = \frac{\deg(m-n\phi)}{n^2} \geq 0$, hence for all $t \in \mathbb{R}$ we have $\det(t - \phi_l) = t^2 - a_q t + q \geq 0$, thus this polynomial has complex conjugate roots (or a double root), in both cases $|\alpha_q| = |\beta_q|$. Therefore $\alpha_q\beta_q = q$ implies $|\alpha_q| = |\beta_q| = \sqrt{q}$.

Now we look at q^n-th power Frobenius morphism and use the estimate $|E(\mathbb{F}_{q^n})| = \deg(1-\phi^n)$ to get the characteristic polynomial for ϕ_l^n, namely $\det(t-\phi_l^n) = (t-\alpha_q^n)(t-\beta_q^n)$ because the Jordan normal form of ϕ_l is upper triangular with α_q and β_q on the diagonal. Applying previous proposition $|E(\mathbb{F}_{q^n})| = \deg(1-\phi^n) = \det(1-\phi_l^n) = 1-\alpha_q^n - \beta_q^n + q^n$.

2. By Cayley-Hamilton theorem $\phi_l^2 - a_q\phi_l + q = 0$, therefore $\deg(\phi^2 - a_q\phi + q = 0) = \det(\phi_l^2 - a_q\phi_l + q) = 0$ and $\phi^2 - a_q\phi + q$ is the zero map.

□

Remark 9.10. *We name the* $a_q = q+1-|E(\mathbb{F}_q)|$ *the trace of Frobenius, since it equals to the trace of q-th power of Frobenius map* $\mathrm{Tr}(\phi_l) = 1 + \deg(\phi) - \deg(1-\phi)$*, if we think about it as of linear map of* $T_l(E)$*.*

Now we state and prove the weil conjectures for an elliptic curve

Theorem 9.11. *Let* $E/\mathbb{F}_q$ *be an elliptic curve. Then*

1. *There exists an* $a_q \in \mathbb{Z}$ *such that* $Z(E/\mathbb{F}_q, t) = \frac{1-a_qt+qt^2}{(1-t)(1-qt)}$*;*
2. $Z(E/\mathbb{F}_q, \frac{1}{qt}) = Z(E/\mathbb{F}_q, t)$*;*
3. $1-a_qt+qt^2 = (1-\alpha_qt)(1-\beta_qt)$*, where* $|\alpha_q| = |\beta_q| = \sqrt{q}$*.*

Proof. Part of the proof is an

Exercise 9.12. *Compute* $\log Z(E/\mathbb{F}_q, t)$*;*

From the result of exercise follows $Z(E/\mathbb{F}_q, t) = \frac{(1-\alpha_qt)(1-\beta_qt)}{(1-t)(1-qt)}$. This implies first part of the theorem, since $(1-\alpha_qt)(1-\beta_qt) = 1-a_qt+qt^2$;

The second part can be checked immediately from obtained equation for zeta function.

Third one follows from previous theorem and 1. □

Remark 9.13. *To get Riemann Hypothesis from theorem we take* $t = q^{-s}$ *and work with function of s. Indeed,*

$$\zeta_{E/\mathbb{F}_q}(s) = Z(E/\mathbb{F}_q, q^{-s}) = \frac{1-a_qq^{-s}+q^{1-2s}}{(1-q^{-s})(1-q^{1-s})}$$

Implies $\zeta_{E/\mathbb{F}_q}(s) = \zeta_{E/\mathbb{F}_q}(1-s)$*.*

The statement of Riemann hypothesis says: if $\zeta_{E/\mathbb{F}_q}(s) = 0$*, then* $\mathrm{Re}(s) = \frac{1}{2}$*, which is equivalent to* $|q^s| = \sqrt{q}$*.*

9.3 The endomorphism ring

Here we take the field K of characteristic p and an elliptic curve E over K. The aim of this part is to state and prove some connections between possible forms of $E[p]$ and $\mathrm{End}(E)$.

Theorem 9.14. *Let E/K be an elliptic curve, recall we denoted as $E^{(p^r)}$ its p^r-th power of Frobenius, denote also $\phi_r : E \to E^{(p^r)}$ the p^r-th power of Frobenius, and $\widehat{\phi_r} : E^{(p^r)} \to E$ its dual.*

(a) The following are equivalent:

1. $E[p^r] = 0$ *for one (all)* $r \geq 1$*;*
2. $\widehat{\phi_r}$ *is purely inseparable for one (all)* $r \geq 1$*;*
3. *The map* $[p] : E \to E$ *is purely inseparable and* $j(E) \in \mathbb{F}_q$ *for* $q = p^2$*;*
4. $\mathrm{End}(E)$ *is an order in a quaternion algebra;*

In this case we call the curve E supersingular and has Hasse invariant 0, otherwise we call it ordinary and with Hasse invariant 1.

(b) If conditions of (a) do not hold, then $E[p^r] = \mathbb{Z}/p^r\mathbb{Z}$ for all $r \geq 1$. If $j(E) \in \overline{\mathbb{F}_p}$, then $\mathrm{End}(E)$ *is an order in a quadratic imaginary field.*

Proof. (a) Conditions stated in (a) are invariant under field extension, so we may take K algebraically closed. Remind that Frobenius map is purely inseparable, so $\deg_s(\widehat{\phi_r}) = \deg_s[p^r] = (\deg_s[p])^r = (\deg_s \widehat{\phi})^r$. Next use the estimate $|E[p^r]| = \deg_s(\widehat{\phi_r}) = \deg(\widehat{\phi})^r$ to get equivalence of 1. and 2.

We will prove that 2. ⇒ 3. ⇒ 4. ⇒ 2.

2. ⇒ 3: from 2. $[p] = \widehat{\phi} \circ \phi$ is purely inseparable, thus it is left to prove that $j(E) \in \mathbb{F}_q$, where $q = p^2$. By assumption $\widehat{\phi} : E^{(p)} \to E$ is purely inseparable, so it factors as $E^{(p)} \xrightarrow{\phi'} E^{(p^2)} \xrightarrow{\psi} E$, where ϕ' is the p-th power Frobenius on $E^{(p)}$ and ψ is a morphism of degree one. It is obvious that ψ is injective and nonconstant, thus surjective, so it is an isomorphism, therefore $j(E) = j(E^{(p^2)}) = j(E)^{p^2}$.

3. ⇒ 4. Assume first that $\mathrm{End}(E)$ is not an order in quaternion algebra, then $F = \mathrm{End}(E) \otimes \mathbb{Q}$ is a number field ($\mathbb{Q}$, or its quadratic extension).

We want to know how many are there curves, isogenuous to E. Let $\psi : E \to E'$ is an isogeny, we use $\psi \circ [p] = [p] \circ \psi$ and since $[p] : E \to E$ is purely inseparable, after comparing inseparability degrees we get $[p] : E' \to E'$ is also purely inseparable. Thus $|E[p]| = \deg_s[p] = 1$, so from proven above we get $j(E') \in \mathbb{F}_q$ for $q = p^2$, so there are only finitely many (up to isomorphism) elliptic curves isogenuous to E.

Therefore we can choose a prime $l \neq p$ which is prime in $\mathrm{End}(E')$ for all E'. Now using that $E[l^i] = \mathbb{Z}/l^i\mathbb{Z} \times \mathbb{Z}/l^i\mathbb{Z}$ we choose a sequence of subgroups $G_1 \subset ... \subset E$ with $G_i \simeq Z/l^i\mathbb{Z}$, we denote by $E_i = E/G_i$ and by $\psi_i : E \to E_i$ an isogeny with kernel G_i. There are only finitely many E_i, so we can choose integers $m, n > 0$ with $E_m \overset{\alpha}{\simeq} E_{m+n}$.

One gets an endomorphism of E_m by composing obtained isomorphism with natural projection $\pi : E_m \to E_{m+n}$. The kernel of the composition is cyclic group G_{m+n}/G_m of order l^n, since l is prime in $\mathrm{End}(E_m)$ by comparing degrees we have $\pi \circ \alpha = u \circ [l^{n/2}]$ for $u \in \mathrm{Aut}(E_m)$. But the kernel of $[l^{n/2}]$ is not cyclic for $n > 0$. Hence F is not a number field, so a quaternion algebra.

It is left to prove that 4. $\Rightarrow$ 2.. Assume that $\widehat{\phi_r}$ is separable for all r, we will deduce that $\mathrm{End}(E)$ is commutative, which does not agree with 4. Part of the proof is an

Exercise 9.15. *Prove that the natural map* $\mathrm{End}(E) \to \mathrm{End}(T_p(E))$ *is injective. For* $p = \mathrm{char}K$ *the Tate module* $T_p(E)$ *is either 0 or* $\mathbb{Z}_p$.

Anyway $T_p(E)/pT_p(E) = E[p]$, and by assumption $E[p] \neq 0$, so $T_p(E) = \mathbb{Z}_p$, thus $\mathrm{End}(E) \hookrightarrow \mathrm{End}(T_p(E)) \simeq \mathbb{Z}_p$, so $\mathrm{End}(E)$ is commutative.

(b) We know that $E[p^r]$ is equal to either 0 or $\mathbb{Z}/p^r\mathbb{Z}$ for all $r > 0 \in \mathbb{Z}$, so if (a)1. is not satisfied, then $E[p^r] \simeq \mathbb{Z}/p^r\mathbb{Z}$ for all $r \geq 1$. Now suppose further $j(E) \in \overline{\mathbb{F}_p}$. Since two elliptic curves are isomorphic when their j-invariants are equal and for any number $j \in \overline{\mathbb{F}_p}$ there exist an elliptic curve E' with $j(E') = j$, we can find an elliptic curve E' defined over a field $\mathbb{F}_{p^r}$ such that $E' \simeq E$ over $\overline{\mathbb{F}_p}$, then the p^r-power Frobenius ϕ_r is an endomorphism of E'.

If $\phi_r \in \mathbb{Z} \subset \mathrm{End}(E')$, then by degrees $\phi_r = [\pm p^{r/2}]$ for some r and $|E[p^{r/2}]| = \deg_s \phi_r = 1$, which contradicts that $(a)1.$ is false. Thus $\phi_r \notin \mathbb{Z}$ and $\mathrm{End}(E')$ is strictly larger than $\mathbb{Z}$. But it is not a quaternion algebra, so it is an order in quadratic imaginary field, now remember that $\mathrm{End}(E') \simeq \mathrm{End}(E)$.

□

9.4 Exercises

Exercise 9.16. *Find the number of isomorphism classes of elliptic curves over a field* $\mathbb{F}_q$ *for* $\operatorname{char} \mathbb{F}_q \neq 2, 3$

Exercise 9.17. *Let* E, E' *be elliptic curves defined over finite field* $\mathbb{F}_q$.

1. *If* $E \sim E'$ *are isogenuous over* $\mathbb{F}_q$, *prove that* $|E(\mathbb{F}_q)| = |E'(\mathbb{F}_q)|$. *Deduce that* $Z(E/\mathbb{F}_q, t) = Z(E'/\mathbb{F}_q, t)$.
2. *Prove the converse: if* $|E(\mathbb{F}_q)| = |E'(\mathbb{F}_q)|$, *then* $E \sim E'$.

There will be no notes of lectures 10,11,12, since I used first 4 paragraphs of chapter IV of the book [9] almost without any changes to prove the Mordell-Weil theorem.

References

[1] E. Artin *Algebraic numbers and algebraic functions*, 1967.

[2] Z. Borevich, I. Shafarevich, *Number theory*, M., 1985.

[3] D. Cox, *Primes of the form $x^2 + ny^2$*, Pure and Appl. Math., Wiley, 1989.

[4] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, (1997).

[5] S. Lang, *Algebraic number theory*, 1986.

[6] S. Lang, *Introduction to algebraic and abelian functions*, 1982.

[7] S. M. Lvovsky, *Lectures on complex analysis*, MCCME, 2009.

[8] J. S. Milne, *Algebraic number theory*, 2011.

[9] J. S. Milne, *Elliptic curves*, 2006.

[10] D. Mumford, *Abelian varieties*, 1970.

[11] J. Neukirch, *Algebraic number theory.*

[12] J. Serre, *Course of arithmetic*, M. 1972.

[13] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, GTM 106, 1986.

[14] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, GTM 151, 1995.

[15] A. Weil, *Introduction to number theory*, M. 2004.