MODULAR CURVES

MAARTEN DERICKX

Abstract. These are lecture notes for a course on modular curves given in Zagreb. The language of schemes is avoided in order to keep the notes accessible to an audience that is familiar with varieties but not with schemes.

Contents

1. Background

1.1. Notations.

- If K is a field and V_1, V_2 are vector spaces over K then $\mathrm{Iso}_{K\text{-}\mathbf{vec}}(V_1, V_2)$ denotes the set of isomorphisms between V_1 and V_2 as K vector spaces.
- If R is a ring and $n > 0$ an integer then $M_n(R)$ denotes the set of n by n matrices.
- If $A \in M_n(R)$ is a matrix then A^t denotes its transpose.
- If $\mathcal{C}$ is a category then $\mathcal{C}^{op}$ denotes the oposite category. I.e. the category that has the same objects, but where the direction of all morphisms are reversed.

1.2. **Varieties.**

say something about varieties over non algebraically closed fields as in section 1 of Silverman

1.2.1. *Families of varieties.*

Definition 1.1 (Family of varieties.)**.** Let S by a variety over a field K. A *family of varieties over* S is a pair (X, f) where

i) X is a variety over K,
ii) $f : X \to S$ is a regular map,
iii) for every $s \in S(\overline{K})$ the fiber $f^{-1}(s) \subseteq X$ is a variety over K.

Notation 1.2. Let (X, f) be a family of varieties over S and $s \in S(\overline{K})$, then $X_s := f^{-1}(s)$ is used as shorthand notation for the fiber above s.

Note that $f^{-1}(s)$ is always an algebraic subset of $X(\overline{K})$. So Definition 1.1(iii) is equivalent to the fiber $f^{-1}(s)$ being irreducible.

Definition 1.3 (Morphism of families)**.** Let S by a variety over a field K and $(X_1, f_1), (X_2, f_2)$ be two families of varieties over S. A morphism of families from (X_1, f_1) to (X_2, f_2) is a regular map $h : X_1 \to X_2$ defined over K such that $f_1 = f_2 \circ h$.

$$\begin{array}{ccc} X_1 & \xrightarrow{\quad h \quad} & X_2 \\ & {\scriptstyle f_1}\searrow \quad \swarrow{\scriptstyle f_2} & \\ & S & \end{array}$$

Let $s \in S(\overline{K})$ and let $h_s : X_{1,s} \to X_{2,s}$ denote the restriction of h to the fibers above s. It follows from Definition 1.3 that h_s is a regular map between varieties over $\overline{K}$. Note that if s lies in some field $L \subset \overline{K}$ and $K \subset L$ then h_s is actually defined over L.

Notation 1.4. Let $(T, f_1), (X, f_2)$ be two families of varieties over S, then $X(T)$ is shorthand notation for the set of morphisms as in Definition 1.3. Similarly $X(S)$ is shorthand notation where $(T, f_1) = (S, \mathrm{Id}_S)$.

The notation $X(S)$ also agrees by definition with the set of sections of $f_2 : X \to S$ since the commutative diagram in Definition 1.3 reduces to the relation $\mathrm{Id}_S = f_2 \circ h$ when $(T, f_1) = (S, \mathrm{Id}_S)$.

1.3. **Fiber products.**

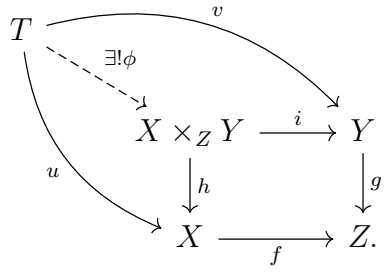
Definition 1.5. Let $f : X \to Z$ and $g : Y \to Z$ be regular maps between varieties over a field K. The *fiber product of* X *and* Y *over* Z, if it exists, is a variety $X \times_Z Y$ together with commutative diagram of the form

$$\begin{array}{ccc} X \times_Z Y & \xrightarrow{\quad i \quad} & Y \\ \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle g} \\ X & \xrightarrow[\quad f \quad]{} & Z \end{array}$$

that satisfied the following universal property. If T is another variety sitting in a commutative diagram

$$\begin{array}{ccc} T & \xrightarrow{u} & Y \\ \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle g} \\ X & \xrightarrow[f]{} & Z, \end{array}$$

then there is a unique $\phi : T \to X \times_Z Y$ making the following diagram commute:



If a fiber product $X \times_Z Y$ exists as in the definition, then it is unique up to a unique isomorphim as is always the case with objects defined using universal properties.

Definition 1.6. A cartesian square is a diagram of the form

$$\begin{array}{ccc} T & \xrightarrow{u} & Y \\ \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle g} \\ X & \xrightarrow[f]{} & Z, \end{array}$$

such that the map ϕ from Definition 1.5 is an isomorphsim.

Remark 1.7. Instead of using the language of universal properties, one could also define the fiber product in terms of a varieties representing a functor. I.e. $X \times_Z Y$, if it exists, is the variety representing the contravariant functor

$$\begin{aligned} F_{f,g} : \mathrm{Var}_K^{op} &\to \mathrm{Sets} \\ T &\mapsto \{u, v \in \mathrm{Hom}_{\mathrm{Var}}(T, X) \times \mathrm{Hom}_{\mathrm{Var}}(T, Y) \mid f \circ u = g \circ v\} \end{aligned}$$

Remark 1.8. If the fiber product $X \times_Z Y$ exists then $f \circ h = g \circ i$. So the fiber product $X \times_Z Y$ comes equiped with a canonical map $f \circ h = g \circ i$ to Z.

Definition 1.9. Let $f : X \to Z$ and $g : Y \to Z$ be regular maps between varieties over a field K. Define $X \times'_Z Y \subset X \times Y$ to be the closed subset

$$X \times'_Z Y := \{x, y \subset X \times Y \mid f(x) = g(y)\}.$$

While $X \times'_Z Y$ will always be a union of closed sub-varieties of $X \times Y$ over $\overline{K}$, it will not always be a variety. This is because varieties are geometrically irreducible by definition.

Exercise 1.10. Let K be a field of characteristic > 2. Let $X = Y = Z = \mathbb{A}^1_K$ and let $f : X \to Z$ and $g := Y \to Z$ both be the map $\mathbb{A}^1_K \to \mathbb{A}^1_K$ given by $x \to x^2$. Show that $X \times'_Z Y$ is not irreducible.

Exercise 1.11. Let K be a field of characteristic > 2 and $t \in K^*$ not a square. Let $X = Y = Z = \mathbb{A}^1_K$ and let $f : X \to Z$ be given by $x \to x^2$ and $g := Y \to Z$ be given $x \to tx^2$. Show that $X \times'_Z Y$ is irreducible but not geometrically irreducible.

Lemma 1.12. *If $X \times'_Z Y$ from definition 1.9 is geometrically irreducible then $X \times'_Z Y$ and furthermore $X \times'_Z Y$ together with the two projection maps to X and Y satisfies the universal property of the fiber product.*

Proof. add proof

□

Exercise 1.13. Let S be a variety over a field K and $(X_1, f_1), (X_2, f_2)$ be two families of varieties over S such that the fiber product $X_1 \times_S X_2$ exists. Show that

(1) $X_1 \times_S X_2 \to S$ is a family of varieties over S, where $X_1 \times_S X_2 \to S$ is the map from Remark 1.8,
(2) for all $s \in S(\overline{K})$ one has $(X_1 \times_S X_2)_s$ is isomorphic to $X_{1,s} \times X_{2,s}$, i.e. the fiber above s of the fiber product is just the product of the the fibers.

1.4. **Group varieties.**

Definition 1.14. Let K be a field, a *group variety* over K is a variety G over K together with

- a point $e \in G(K)$ called the identity element,
- a morphism $\iota : G \to G$ defined over K called the inverse map,
- a morphism $s : G \times G \to G$ defined over K, called the addition map

such that the usual group axioms hold for e, ι, s for all elements in $G(\overline{K})$. To be precise for all $a, b, c \in G(\overline{K})$ one has

- $s(a, e) = a = s(e, a)$ (e is an identity element),
- $s(s(a, b), c)) = s(a, s(b, c))$ (s is associative),
- $s(\iota(a), a) = e = s(a, \iota(a))$ (ι is an inverse).

If furthermore s is symmetric, i.e. $s(a, b) = s(b, a)$, then G is called an *abelian* group variety.

Lemma 1.15. *Let G be a group variety over a field K and $L \subset \overline{K}$ be a subfield containing K. Then $G(L)$ with the operationse, ι, s is a group.*

Proof. This follows immediately from the definition. □

Example 1.16. Let K be a field and n an integer. Then $\mathbb{A}^n$ can be given the structure of a group variety over K by defining $e := (0, 0, \ldots, 0) \in \mathbb{A}^n(K)$,

$$s \colon \mathbb{A}^n \times \mathbb{A}^n \to \mathbb{A}^n \tag{1.1}$$

$$((a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n)) \mapsto (a_1 + b_1, a_2 + b_2, \ldots, a_n + a_n) \text{ and} \tag{1.2}$$

$$\iota \colon \mathbb{A}^n \to \mathbb{A}^n \tag{1.3}$$

$$(a_1, a_2, \ldots, a_n), \mapsto (-a_1, -a_2, \ldots, -a_n). \tag{1.4}$$

Notice that the usual bijection $\mathbb{A}^n(K) \cong K^n$ is actually a group isomorphism where the left hand side has the group law coming from the group variety structure and the right hand right hand side has is just coordinate wise addition in K.

Definition 1.17. Let $(G_1, e_1, \iota_1, s_1), (G_2, e_2, \iota_2, s_2)$ be group varieties over a field K. Then a *group variety homomorphism over K* is morphism $\phi : G_1 \to G_2$ of varieties defined over K such that

- $\phi(e_1) = e_2$
- for all $a, b \in G_1(\overline{K})$ the relation $\phi(s_1(a, b)) = s_2(\phi(a), \phi(b))$ holds.

The set of all group variety homomorphisms over K is denoted by $\mathrm{Hom}_{\mathbf{grp\text{-}var}}(G_1, G_2)$.

Notice the absence of a compatibility condition for the inverse map, the reason for this omission is that inverse of an element is unique. And hence the compatibility $\phi(\iota(a)) = \iota(\phi(a))$ follows from the group variety and group variety homomorphism axioms.

Lemma 1.18. *Let $\phi : G_1 \to G_2$ be a group variety homomorphism over a field K and $L \subset \overline{K}$ be a subfield containing K. Then ϕ induces a group homomorphism $G_1(L) \to G_2(L)$.*

Proof. This follows immediately from the definition. □

Exercise 1.19. Let K be a field of characteristic 0. Show that $\mathrm{Hom}_{\mathbf{grp\text{-}var}}(\mathbb{A}^1_K, \mathbb{A}^1_K)$ consists of the linear polynomials $ax \in K[x]$ (hint: $\mathrm{Hom}(\mathbb{A}^1_K, \mathbb{A}^1_K) \cong K[x]$).

1.5. **Some group theory.**

Definition 1.20. Let G be a group and let $s : G \times G \to G$ be associated group law on G. Then G^{op} is defined to be the group whose underlying set and identity element are the same as that of G but whose group law is given by

$$\begin{aligned} m^{op} : G \times G &\to G \\ g, h &\mapsto m(h, g) \end{aligned}$$

Definition 1.21. Let G be a group with identity element e and S be a set. Then a *left group action* of G on S is a map $\rho : G \times S \to S$ such that for all $g, h \in G$ and $s \in S$:

- $\rho(e, s) = s$
- $\rho(g, \rho(h, s)) = \rho(gh, s)$

Similarly a *right group action* of G on S is a map $\rho : S \times G \to S$ such that for all $g, h \in G$ and $s \in S$:

- $\rho(s, e) = s$
- $\rho(\rho(s, h), g) = \rho(s, hg)$

Lemma 1.22. *Let G be a group and S be a set and let $\rho : G \times S \to S$ be an arbitrary map. Then the following are equivalent:*

- *ρ is a left action of G on S*
- *The image of the map*

$$\begin{aligned} f_\rho : G &\to \mathrm{Hom}(S, S) \\ g &\mapsto (s \mapsto \rho(g, s)) \end{aligned}$$

  is contained in $\mathrm{Aut}(S) \subset \mathrm{Hom}(S, S)$ and the induced map $f_\rho : G \to \mathrm{Aut}(S)$ is a group homomorphism.

Proof. Note that if ρ is a group action then $f_\rho(g^{-1})$ is the inverse of $f_\rho(g)$, which shows that $f_\rho(g) \in \mathrm{Aut}(S)$. The rest of the proof is a relatively straightforward rewriting of the definitions of group action and group homomorphisms. □

The above lemma looks slightly different for right group actions.

Lemma 1.23. *Let G be a group and S be a set and let $\rho : S \times G \to S$ be an arbitrary map. Then the following are equivalent:*

- *ρ is a right action of G on S*
- *The image of the map*

$$f_\rho : G^{op} \to \mathrm{Hom}(S,S)$$
$$g \mapsto (s \mapsto \rho(s,g))$$

is contained in $\mathrm{Aut}(S) \subset \mathrm{Hom}(S,S)$ *and the induced map* $f_\rho : G^{op} \to \mathrm{Aut}(S)$ *is a group homomorphism.*

Proof. Similar to that of lemma 1.22. □

Definition 1.24. Let $\rho : G \times S \to S$ be a left action of the group G on the set S and let $s \in S$. Then the stabalizer of s in G is defined as

$$\mathrm{stab}_G(s) := \{g \in G \mid \rho(g,s) = s\}$$

Lemma 1.25. *Let $\rho : G \times S \to S$ be a left action of the group G on the set S and let $s \in S$, then $stab_G(s)$ is a subgroup of G.*

Proof. If $\rho(g,s) = s$ and $\rho(h,s) = s$ then $\rho(gh,s) = \rho(g,\rho(h,s)) = s$. □

Lemma 1.26. *Let G be a group, and let S_1 and S_2 be sets with a left G action. Let $C \subset S_2$ be a set of representatives of $G\backslash S_2$. Then the map*

$$\phi : \coprod_{s_2 \in C} stab_G(s_2)\backslash S_1 \to G\backslash(S_1 \times S_2)$$
$$stab_G(s_2)s_1 \mapsto G(s_1,s_2)$$

is well defined and bijective.

Proof. For well it being well defined we need to show that it doesn't depend on the representative s_1 that was chosen for the orbit $\mathrm{stab}_G(s_2)s_1$. Now suppose $gs_1 \in \mathrm{stab}_G(s_2)s_1$ with $g \in \mathrm{stab}_G(s_2)$ is another element in the same orbit then

$$\phi(\mathrm{stab}_G(s_2)gs_1) = G(gs_1,s_2) = Gg(s_1,g^{-1}s_2) = G(s_1,s_2) = \phi(\mathrm{stab}_G(s_2)s_1).$$

To show it is surjective, let $G(s_1,s_2) \in G\backslash(S_1 \times S_2)$ be an arbitrary. Since C is a set of representatives of $G\backslash S_2$ we can find a $s_2' \in C$ and $g \in G$ such that $s_2 = gs_2'$. Now surjetivity follows since

$$G(s_1,s_2) = G(s_1,gs_2') = Gg(g^{-1}s_1,s_2') = \phi(\mathrm{stab}_G(s_2')g^{-1}s_1).$$

For injectivity let $s_1, s_1' \in S$ and $s_2, s_2' \in C$. If $\mathrm{stab}_G(s_2)s_1$ and $\mathrm{stab}_G(s_2')s_1'$ map to the same element in $G\backslash(S_1 \times S_2)$ then s_2 and s_2' must by in the same G orbit. However since C consists of representatives of $G\backslash S_2$ this forces $s_2 = s_2'$. Since we have $s_2 = s_2'$ the equality $G(s_1,s_2) = G(s_1',s_2')$ is equivalent to $s_1' = gs_1$ for some $g \in \mathrm{stab}_G(s_2)$ showing that $\mathrm{stab}_G(s_2)s_1 = \mathrm{stab}_G(s_2')s_1'$. □

1.6. **Adeles.**

2. Elliptic curves

2.1. **Elliptic curves of arbitrary fields.** The following is the abstract definition of elliptic curve

Definition 2.1. Let K be a field. An *elliptic curve* over K is a pair $(E,0)$ where E is a smooth proper and geometrically irreducible curve of genus 1 defined over K and $0 \in E(K)$ is a point. A *morphism* of elliptic curves $\phi : (E_1,0) \to (E_2,0)$ is a morphism of varieties $\phi : E_1 \to E_2$ such that $\phi(0) = 0$.

Note that often when talking about elliptic curves, the element $0 \in E(K)$ is understood to be implicitly part of the data. And one writes E instead of $(E, 0)$.

2.1.1. *Weierstrass models.* The above definition is quite abstract. However, sometimes it is easier to work with explicit equations for elliptic curves. The goal of this subsection is to show that every elliptic curve over a field can be given by a Weierstrass model.

Definition 2.2 (Weierstrass model)**.** Let $a := (a_1, a_2, a_3, a_4, a_6) \in K^5$ then define $E_a \subset \mathbb{P}^2$ to be the curve given by

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

The point 0 on E is defined the point where $(x : y : z) = (0 : 1 : 0)$.

Note there is no a_5 in the above definition. This is on purpose and will become clear later. Before we continue we need to define a quantity called the discriminant.

Definition 2.3 (Discriminant)**.** The b-invariants $b_2, b_4, b_6, b_8 \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ and the discriminant $\Delta \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ are defined as follows:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{aligned}$$

If R is a ring and $a := (a_1', a_2', a_3', a_4', a_6') \in R^5$ then Δ_a will be shorthand notation for $\Delta(a_1', a_2', a_3', a_4', a_6')$.

The first hint of why the 5-th coefficient is labeled a_6 and not a_5 is already visible in this definition. Namely if we see $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ as a weighted polynomial ring where a_i has weight i, then the b_i are homogeneous of weight i and Δ is homogeneous of weight 12.

Proposition 2.4 (A smooth Weierstrass model is an elliptic curve)**.** *Let K be a field and $a := (a_1, a_2, a_3, a_4, a_6) \in K^5$ then the following are equivalent:*

- *The pair $(E_a, 0)$ is an elliptic curve.*
- *The curve E_a is smooth.*
- $\Delta_a \neq 0$.

Proof. add reference to silverman

□

Theorem 2.5 (Existence of Weierstrass model)**.** *Let $(E, 0)$ be an elliptic curve over K then there is an $a := (a_1, a_2, a_3, a_4, a_6) \in K^5$ such that*

$$\Delta_a \neq 0 \text{ and } (E, 0) \cong (E_a, 0).$$

Proof. add reference to silverman

□

Proposition 2.6 (Isomorphisms between Weierstrass models)**.** *Let K be a field, $a := (a_1, a_2, a_3, a_4, a_6)$ and $a' := (a'_1, a'_2, a'_3, a'_4, a'_6)$ elements of K^5 such that $\Delta_a \neq 0$ and $\Delta_{a'} \neq 0$. If $f : E_a \to E_{a'}$ is an isomorphism of elliptic curves. Then there are $u \in K^*$ and $r, s, t \in K$ such that $f = f_{u,r,s,t}$ where $f_{u,r,s,t}$ is given by*

$$\begin{aligned} f_{u,r,s,t} : \quad E_a &\to E_{a'} \\ (x : y : z) &\mapsto (u^2x + rz : u^3y + u^2sx + tz : z) \end{aligned} \tag{2.1}$$

Proof. add reference to silverman and say that we use an inverse convention □

Note that there is also the following converse to the above proposition.

Proposition 2.7 (Change of Weierstrass model)**.** *Let K be a field, $a := (a_1, a_2, a_3, a_4, a_6) \in K^5$, $u \in K^*$ and $r, s, t \in K$. Define*

$$\begin{aligned} a'_1 &:= ua_1 - 2s \\ a'_2 &:= u^2a_2 + usa_1 - s^2 - 3r \\ a'_3 &:= u^3a_3 - a'_1r - 2t \\ a'_4 &:= u^4a_4 - 2a'_2r + u^3sa_3 + uta_1 - 3r^2 - 2st \\ a'_6 &:= u^6a_6 - a'_4r - a'_2r^2 + \left(u^3t\right)a_3 - r^3 - t^2 \\ a' &:= (a'_1, a'_2, a'_3, a'_4, a'_6). \end{aligned} \tag{2.2}$$

Then $f_{u,r,s,t}$ from eq. (2.1) defines an isomorphism between E_a and $E_{a'}$.

Proof. add reference to silverman and say that we use an inverse convention □

2.1.2. *Group law.*

2.1.3. *Division Polynomials.*

cite A. Enge. Elliptic curves and their applications to cryptography — an introduction. Kluwer, 199 and Jinbi Jin `https://arxiv.org/pdf/1303.4327`

Let $\mathcal{W} := y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6) \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x, y]$ be the inhomogenous version of the equation defining the Weierstrass Model from Definition 2.2 obtained by setting $z = 1$.

Definition 2.8. The *division polynomials* $\Psi_n \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x, y]/\mathcal{W}$ are the polynomials satisfying the recurrence relation:

$$\Psi_{m+2}\Psi_{m-2} = \Psi_2^2\Psi_{m+1}\Psi_{m-1} - \Psi_m^2\Psi_3$$

and the initial conditions

$$\begin{aligned} \Psi_0 &:= 0 \\ \Psi_1 &:= 1 \\ \Psi_2 &:= 2y + a_1x + a_3 \\ \Psi_3 &:= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8 \\ \Psi_4 &:= \Psi_2(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2), \end{aligned}$$

where the b_i are as in Definition 2.3.

These polynomials can be viewed as elements in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x, y]$ by taking the unique representative where the degree of the occurrences of y in Ψ_{m-n} is at most 1.

Proposition 2.9. *The division polynomials satisfy the relation*

$$\Psi_{m+n}\Psi_{m-n} = \Psi_n^2\Psi_{m+1}\Psi_{m-1} - \Psi_m^2\Psi_{n+1}\Psi_{n-1}$$

Proof. cite enge/jinbi jin □

Definition 2.10. The *auxiliary division polynomials* are the polynomials $\Phi_n, \Omega_n \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x, y]/\mathcal{W}$ for integer values of n are defined by

$$\begin{aligned}\Phi_n &:= X\Psi_n^2 - \Psi_{n+1}\Psi_{n-1}\\ \Omega_0 &:= 1\\ \Omega_n &:= \frac{1}{2\Psi_n}(\Psi_{2n} - \Psi_n^2(a_1\Phi_n + a_3\Psi_n^2)) \text{ if } n \neq 0\end{aligned}$$

Proposition 2.11. *Let K be a field, $a := a_1, a_2, a_3, a_4, a_6 \in K^5$ such that $\Delta_a \neq 0$ and $P := (x : y : 1)$ be a point on the Weierstrass curve E_a. Then for all integers n the point nP has coordinates*

$$nP = (\Psi_n(a, x, y)\Phi_n(x, y) : \Omega_n(a, x, y) : \Psi_n^3(a, x, y))$$

Proof. cite enge/jinbi jin □

Corollary 2.12. *The order of P is a divisor of n if and only if $\Psi_n(a, x, y) = 0$.*

2.1.4. *Level structures.*

Definition 2.13 (Level structures)**.** Let E be an elliptic curve over a field K and let N be an integer.

i) Assume N is invertible in K then a *full level N structure on E* is a group isomorphism $\phi : (\mathbb{Z}/N\mathbb{Z})^2 \to E[N](K)$,
ii) Assume N is invertible in K a *a point of order N on E* is an injective group homomorphism $\phi : \mathbb{Z}/N\mathbb{Z} \to E[N](K)$,
iii) a *a point of order $\geq N$ on E* is an group homomorphism $\phi : \mathbb{Z} \to E[N](K)$ whose image has cardinality $\geq N$.

Remark 2.14. Since $E[N](\overline{K}) \cong (\mathbb{Z}/N\mathbb{Z})^2$, Definition 2.13(i) is equivalent to giving $P, Q \in E[N](K)$ such that they together generate $E[N](\overline{K})$. Definition 2.13(ii) is equivalent to giving a point $P \in E[N](K)$ of order N, and definition 2.13(iii) is equivalent to giving a $P \in E[N](K)$ of order $\geq N$.

Definition 2.15 (Morphism with level structure)**.** Let N be an integer that is invertible in K and let (E_1, ϕ_1), (E_2, ϕ_2) two elliptic curves with full level N structure over K. Then *a morphism of elliptic curves with full level N structure* $f : (E_1, \phi_1) \to (E_2, \phi_2)$ is morphism $f : E_1 \to E_2$ of elliptic curves such that $f \circ \phi_1 = \phi_2$.

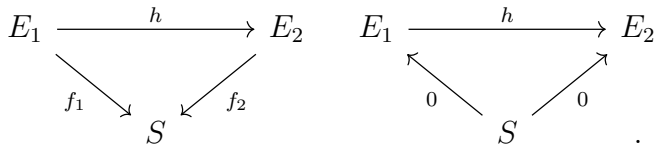
2.2. **Families of elliptic curves.**

Definition 2.16 (Family of elliptic curves)**.** Let S be a variety over a field K. An *elliptic curve over* S or *a family of elliptic curves over* S is a triple $(E, f, 0)$ where

i) E is a variety over K,
ii) $f : E \to S$ is a smooth and proper map,
iii) 0 is a section of f; i.e. a regular map $0 : S \to E$ such that $f \circ 0 = \mathrm{Id}_S$,
iv) for all $s \in S(\overline{K})$ the fiber $E_s := f^{-1}(s)$ above s is a curve over $\overline{K}$ that is irreducible and of genus 1.

Let $L \subseteq \overline{K}$ be a field extension of K and $s \in S(L)$. Note that since f is smooth and proper the fiber E_s will be smooth and proper over L. It is also geometrically reduced and of genus 1 by definition and 0_s will be a point on E_s. In particular for every $s \in S(L)$ the pair $(E_s, 0_s)$ is an elliptic curve over L according to definition 2.1. Also the pair (E, f) is a family of varieties as in Definition 1.1.

Definition 2.17 (Morphism of families of elliptic curves)**.** Let $(E_1, f_1, 0)$ and $(E_2, f_2, 0)$ be elliptic curve curves over S then a *morphism of families of elliptic curves over* S is a regular map $h : E_1 \to E_2$ such that $f_1 = f_2 \circ h$ and $0 = h \circ 0$. I.e. h should be such that the following two diagrams commute:



The first commutative diagram, i.e. the relation $f_1 = f_2 \circ h$, ensures that h is a morphsim of families of varieties (Definition 1.3). While the commutative diagram, ie. $0 = h \circ 0$ ensures that for all $s \in S(\overline{K})$ one has $h_s(0_s) = 0_s$. This means that on fibers h_s is not just a morphisms of varieties, but actually a morphism of elliptic curves as in Definition 2.1.

2.2.1. *Weierstrass models.* Note that elliptic families do not always admit a global Weierstrass model. However, they do admit a Weierstrass model locally. As we will explain in this section.

However before doing this we first need to

Definition 2.18 (Weierstrass model)**.** Let S be a variety over a field K, and let $a := (a_1, a_2, a_3, a_4, a_6)$ where $a_1, a_2, a_3, a_4, a_6 \in \Gamma(S, \mathcal{O}_S)$ be regular functions such that for all $s \in S(\overline{K})$ one has $\Delta_a(s) \neq 0$ (or equivalently $\Delta_a \in \Gamma(S, \mathcal{O}_S)^*$). Then the Weierstrass-Model with invariants $a := a_1, a_2, a_3, a_4, a_6$ is defined to be the triple $(E_a, f, 0)$ over S where,

- $E_a \subset \mathbb{P}^2_K \times S$ is the curve given by

$$y^2z + a_1(s)xyz + a_3(s)yz^2 = x^3 + a_2(s)x^2z + a_4(s)xz^2 + a_6(s)z^3.$$

- The morphism $f : E_a \to S$ is projection onto the second coordinate.
- $0 : S \to E_a$ is the morphism $s \mapsto ((x : y : z), s)$.

Proposition 2.19 (A Weierstrass model over S defines family of elliptic curves)**.** *The triple* $(E_{a_1,a_2,a_3,a_4,a_6}, f, 0)$ *of definition 2.18 is a family of elliptic curves as in definition 2.16.*

Proof. add reference to Katz-Mazur? □

Proposition 2.20 (Existence of local Weierstrass model)**.** *Let $(E, f, 0)$ be a family of elliptic curve over a variety S and $s \in S$. Then there exists an affine open $U \subset S$ with $s \in U$ and regular functions $a_1, a_2, a_3, a_4, a_6 \in \Gamma(U, \mathcal{O}_U)$ such that*

$$\Delta_{a_1,a_2,a_3,a_4,a_6} \in \Gamma(S, \mathcal{O}_S)^* \text{ and } (E_U, f, 0) \cong (E_{a_1,a_2,a_3,a_4,a_6}, f, 0).$$

Proof. add reference to Katz-Mazur? □

say something about isomorphisms between weierstrass models again?

Give an example of something that doesn't have a global Weierstrass model.

2.2.2. *Group law.*

2.2.3. *Level structures.* It turns out that for defining level structures for families it is more convenient to work with the alternative way of defining level structures as in Remark 2.14.

Definition 2.21 (Level structures)**.** Let S be a variety over a field K, let E be a family of an elliptic curves over S and let N be an integer.

i) Assume N is invertible in K, a *full level N structure on E* is a pair of points $P, Q \in E[N](S)$ such that for all $s \in S(\overline{K})$ the points P_s, Q_s generate $E_s[N](\overline{K})$.
ii) Assume N is invertible in K, a *a point of order N on E* is an element $P \in E[N](S)$ such that for all $s \in S(\overline{K})$ the point P_s is of order N in $E_s(\overline{K})$.
iii) a *a point of order $\geq N$ on E* is an element $P \in E(S)$ such that for all $s \in S(\overline{K})$ the point P_s is of order $\geq N$ in $E_s(\overline{K})$.

Definition 2.22.

define morphisms of families of elliptic curves with level structure (is this actually needed)

2.2.4. *Examples.*

Example 2.23 (A family of elliptic curves with point of order ≥ 4)**.** Let K be a field. Let b, c be coordinates on $\mathbb{A}^2$. Define

$$\Delta(b, c) := (-1) \cdot b^3 \cdot (c^4 + 8bc^2 - 3c^3 + 16b^2 + 20bc + 3c^2 - b - c) \in K[b, c].$$

Let $Y_{\geq}(4) \subset \mathbb{A}^2_K$ be the open subvariety where $\Delta(b, c) \neq 0$. Define $E_{\geq}(4) \subset \mathbb{P}^2_K \times Y_{\geq}(4)$ by

$$E_{\geq}(4) : y^2z + (1 - c)xyz - byz^2 = x^3 - bx^2z$$

Let $f : E_{\geq}(4) \to Y_{\geq}(4)$ be projection onto the second coordinate. Then

$$\begin{aligned} 0 : Y_{\geq}(4) &\to E_{\geq}(4) \\ (b, c) &\mapsto ((0 : 1 : 0), (b, c)) \end{aligned}$$

is a section of f, and the triple $(E, f, 0)$ is a family of elliptic curves over $Y_{\geq}(4)$ as in Definition 2.16. Futhermore

$$\begin{aligned} P_{\geq}(4) : Y_{\geq}(4) &\to E_{\geq}(4) \\ (b, c) &\mapsto ((0:0:1), (b, c)) \end{aligned}$$

Is a point of order ≥ 4 as in Definition 2.21(iii).

2.3. **Elliptic curves over $\mathbb{C}$.**

Theorem 2.24. *Let E be an elliptic curve over $\mathbb{C}$ then there is lattice $\Lambda \subseteq \mathbb{C}$ such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ as Riemann-Surfaces.*

Proof. add reference to Silverman □

Proposition 2.25. *Let $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ then the set of morphisms of elliptic curves $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ is*

$$\mathrm{Hom}_{EC}(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2) = \{z \in \mathbb{C} \mid z\Lambda_1 \subseteq \Lambda_2\}.$$

An element $z \in \mathbb{C}$ defines an isogeny if and only if $z \neq 0$ and an isomorphism if and only if $z\Lambda_1 = \Lambda_2$.

Proof. add reference Silverman □

3. Modular curves $\mathbb{C} \setminus \mathbb{R}$ and the upper half plane

3.1. **Möbius transformations.**

Definition 3.1 (Möbius transformation)**.** Let $a, b, c, d \in \mathbb{R}$ with $ad - bc \neq 0$. A *Möbius transformation* is a transformation is an automorphism of $\mathbb{C} \setminus \mathbb{R}$ of the form

$$\tau \mapsto \frac{a\tau + b}{c\tau + d}.$$

The Möbius transformation induce a left group action of $\mathrm{GL}_2(\mathbb{R})$ on $\mathbb{C} \setminus \mathbb{R}$ as follows:

$$\rho : \mathrm{GL}_2(\mathbb{R}) \times \mathbb{C} \setminus \mathbb{R} \to \mathbb{C} \setminus \mathbb{R} \tag{3.1}$$

$$\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \tau \right) \mapsto \frac{a\tau + b}{c\tau + d}. \tag{3.2}$$

Similar to the Möbius transformation we can also define $\mathrm{GL}_2(\mathbb{R})$ a left action on $\mathrm{Iso}_{\mathbb{R}\text{-}\mathbf{vec}}(\mathbb{R}^2, \mathbb{C})$, the set of $\mathbb{R}$ vectors space isomorphisms between $\mathbb{R}^2$ and $\mathbb{C}$.

$$\rho : \mathrm{GL}_2(\mathbb{R}) \times \mathrm{Iso}_{\mathbb{R}\text{-}\mathbf{vec}}(\mathbb{R}^2, \mathbb{C}) \to \mathrm{Iso}_{\mathbb{R}\text{-}\mathbf{vec}}(\mathbb{R}^2, \mathbb{C}) \tag{3.3}$$

$$(\gamma, f) \mapsto f \circ \gamma^t. \tag{3.4}$$

The transpose is there to make it a left action. Indeed, if $\gamma_1, \gamma_2 \in \mathrm{GL}_2(\mathbb{R})$ and $f \in \mathrm{Iso}_{\mathbb{R}\text{-}\mathbf{vec}}(\mathbb{R}^2, \mathbb{C})$ then

$$\rho(\gamma_1, \rho(\gamma_2, f)) = f \circ \gamma_2^t \circ \gamma_1^t = f \circ (\gamma_1\gamma_2)^t = \rho(\gamma_1\gamma_2, f).$$

Without the transpose this would have been a right action.

Lemma 3.2. *The map*

$$T : \mathrm{Iso}_{\mathbb{R}\text{-}\mathbf{vec}}(\mathbb{R}^2, \mathbb{C}) \to \mathbb{C} \setminus \mathbb{R} \tag{3.5}$$

$$f \mapsto \frac{f(1,0)}{f(0,1)} \tag{3.6}$$

if compatible with the $\mathrm{GL}_2(\mathbb{R})$ *left action and induces a bijection* $\mathrm{Iso}_{\mathbb{R}\text{-}\mathbf{vec}}(\mathbb{R}^2, \mathbb{C})/\mathbb{C}^* \to \mathbb{C} \setminus \mathbb{R}$.

Proof. First for the compatibility of the $\mathrm{GL}_2(\mathbb{R})$ action. Let $\gamma := \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbb{R})$ and write τ_1 for $f(1,0)$ and τ_2 for $f(0,1)$. Then

$$\frac{(f \circ \gamma^t)(1,0)}{(f \circ \gamma^t)(0,1)} = \frac{(f \circ \gamma^t)(1,0)}{(f \circ \gamma^t)(0,1)} = \frac{f(a,b)}{f(c,d)} = \frac{a\tau_1 + b\tau_2}{c\tau_1 + d\tau_2} = \frac{a\tau_1/\tau_2 + b}{c\tau_1/\tau_2 + d} = \gamma\left(\frac{f(1,0)}{f(0,1)}\right).$$

Now for the bijection $\mathrm{Iso}_{\mathbb{R}\text{-}\mathbf{vec}}(\mathbb{R}^2, \mathbb{C})/\mathbb{C}^* \to \mathbb{C} \setminus \mathbb{R}$. First note that if $\lambda \in \mathbb{C}*$ then $T(\lambda f) = T(f)$ so that T factors through a map $T' : \mathrm{Iso}_{\mathbb{R}\text{-}\mathbf{vec}}(\mathbb{R}^2, \mathbb{C})/\mathbb{C}^* \to \mathbb{C} \setminus \mathbb{R}$. One can show that T' is bijective by proving that

$$\begin{aligned} \mathbb{C} \setminus \mathbb{R} &\to \mathrm{Iso}_{\mathbb{R}\text{-}\mathbf{vec}}(\mathbb{R}^2, \mathbb{C}) \\ \tau &\mapsto ((a,b) \mapsto a\tau + b) \end{aligned}$$

is an inverse of T'. □

3.2. **A hint towards Shimura varieties.**

3.2.1. *The circle group.*

Definition 3.3. The *circle group* is the group variety $\mathbb{S} \subseteq \mathbb{A}^3_{\mathbb{R}}$ over $\mathbb{R}$ given by the equation $(a^2 + b^2)t - 1$. The identity element is given $(a,b,t) = (1,0,1)$ and the multiplication and inverse maps are given by

$$\begin{aligned} s : \mathbb{S} \times \mathbb{S} &\to \mathbb{S} \\ (a,b,t)(a',b',t') &\mapsto (aa' - bb', ab' + ba', tt) \\ \iota : \mathbb{S} &\to \mathbb{S} \\ (a,b,t) &\mapsto (at, -bt, a^2 + b^2) \end{aligned}$$

Exercise 3.4. Show that the circle group satisfies the axioms of a group variety.

Exercise 3.5. Let ϕ be defined by

$$\begin{aligned} \phi : \mathbb{C}^* &\to \mathbb{S}(\mathbb{R}) \\ (a + bi) &\mapsto (a, b, (a^2 + b^2)^{-1}). \end{aligned}$$

Show that ϕ is a group homomorphism.

4. Moduli problems

4.1. **The Category** Ell_K**.**

Definition 4.1. The category Ell_K is defined to be the category where objects are families of elliptic curves $f : E \to S$. Morphisms between $f_1 : E_1 \to S_1$ and $f_2 : E_2 \to S_2$ are pairs (h, g) with $h : E_1 \to E_2$ and $g : S_1 \to S_2$ such that the square

$$\begin{array}{ccc} E_1 & \xrightarrow{h} & E_2 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} \\ S_1 & \xrightarrow[g]{} & S_2, \end{array}$$

is cartesian as in Definition 1.6.

Notation 4.2. We will often simply write E/S for an object in Ell_K, and understand that the regular map $f : E \to S$ is implicitly part of the data.

Exercise 4.3. Show that Ell_K actually is a category. For example to show that composition in this category is well defined one needs to show that if

$$\begin{array}{ccc} E_1 & \xrightarrow{h} & E_2 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} \\ S_1 & \xrightarrow[g]{} & S_2, \end{array} \quad \text{and} \quad \begin{array}{ccc} E_2 & \xrightarrow{h'} & E_3 \\ \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} \\ S_2 & \xrightarrow[g']{} & S_3, \end{array}$$

are cartesian squares, then

$$\begin{array}{ccc} E_1 & \xrightarrow{h' \circ h} & E_3 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_3} \\ S_1 & \xrightarrow[g' \circ g]{} & S_3 \end{array}$$

is cartesian as well.

4.2. **Moduli problems.**

Definition 4.4. A *moduli problem of elliptic curves* is a contravariant functor

$$\mathcal{P} : \mathrm{Ell}_K^{op} \to \mathrm{Sets}\,.$$

The level structures from Definition 2.21 can be used to define the following moduli problems:

Definition 4.5. Let K be a field and N be an integer, then moduli problems $[\Gamma(N)]$, $[\Gamma_1(N)]$ and $[\Gamma_{\geq}(N)]$ are defined as follows; where N is assumed to be invertible in K for the definition of $[\Gamma(N)]$ and $[\Gamma_1(N)]$:

$$\begin{aligned} [\Gamma(N)] &: \mathrm{Ell}_K \to \mathrm{Sets} \\ &\quad E/S \mapsto \{P, Q \in E(S) \mid P, Q \text{ define a full level structure on } E\} \\ [\Gamma_1(N)] &: \mathrm{Ell}_K \to \mathrm{Sets} \\ &\quad E/S \mapsto \{P \in E(S) \mid P \text{ a point of order } N\} \\ [\Gamma_{\geq}(N)] &: \mathrm{Ell}_K \to \mathrm{Sets} \\ &\quad E/S \mapsto \{P \in E(S) \mid P \text{ a point of order } \geq N\} \end{aligned}$$

Exercise 4.6. In Definition 4.5 the functors $[\Gamma(N)]$, $[\Gamma_1(N)]$ and $[\Gamma_{\geq}(N)]$ were only defined on sets, and not on homomorphisms. The goal of this exercise is to also describe what the functors do on morphisms.

(1) Suppose $(h,g) : E_1/S_1 \to E_2/S_2$ is a morphism in Ell_K, i.e. there is a cartesian diagram of the shape:

$$\begin{array}{ccc} E_1 & \xrightarrow{h} & E_2 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} \\ S_1 & \xrightarrow[g]{} & S_2, \end{array}$$

Let $P \in E_2(S_2)$, use the universal property of the fiber product to show that there is a unique point P' fitting in to the commutative diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{h} & E_2 \\ P' \uparrow \downarrow{\scriptstyle f_1} & & P \uparrow \downarrow{\scriptstyle f_2} \\ S_1 & \xrightarrow[g]{} & S_2, \end{array}$$

(2) For $(h,g) : E_1/S_1 \to E_2/S_2$ and $P \in E(S)$ define $(h,g)^*(P) := P'$ where P' is the point from (1). And view $(h,g)^*$ as a map $E_2(S_2) \to E_1(S_1)$. Define

$$\begin{aligned} [\Gamma(N)](h,g) : [\Gamma(N)](E_2,S_2) &\to [\Gamma(N)](E_1,S_1) \\ (P,Q) &\mapsto ((h,g)^*(P),(h,g)^*(Q)) \end{aligned}$$

Show that $[\Gamma(N)](h,g)$ is a well defined map of sets, that turns $[\Gamma(N)]$ into a functor. Similarly for $[\Gamma_1(N)]$ and $[\Gamma_{\geq}(N)]$.

Todo list

References