MODULAR CURVES

MAARTEN DERICKX

Abstract. These are lecture notes for a course on modular curves given in Zagreb. The language of schemes is avoided as much as possible in order to keep the notes accessible.

Contents

1. Background 1
1.1. Notations 1
1.2. Fiber products 2
1.3. Group varieties 3
1.4. Elliptic curves 4
1.5. Some group theory 4
1.6. Adeles 5
2. Elliptic curves 5
2.1. Elliptic curves of arbitrary fields 5
2.2. Elliptic curves over C 6
2.3. Families of elliptic curves 7
3. Modular curves $\mathbb{C} \setminus \mathbb{R}$ and the upper half plane 7
3.1. Möbius transformations 7
4. A hint towards Shimura varieties 8
4.1. The circle group 8
Todo list 8
References 9

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 it's transpose.

1.2. **Fiber products.**

Definition 1.1. 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

$$\begin{tikzcd} X \times_Z Y \arrow[r, "i"] \arrow[d, "h"] & Y \arrow[d, "g"] \\ X \arrow[r, "f"'] & Z \end{tikzcd}$$

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

$$\begin{tikzcd} T \arrow[r, "u"] \arrow[d, "v"] & Y \arrow[d, "g"] \\ X \arrow[r, "f"'] & Z, \end{tikzcd}$$

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

$$\begin{tikzcd} T \arrow[drr, bend left, "v"] \arrow[ddr, bend right, "u"'] \arrow[dr, dashed, "\exists!\phi"] & & \\ & X \times_Z Y \arrow[r, "i"] \arrow[d, "h"] & Y \arrow[d, "g"] \\ & X \arrow[r, "f"'] & Z. \end{tikzcd}$$

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.

Remark 1.2. 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

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

Definition 1.3. 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 1.4. 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 1.5. 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 1.6. *If $X \times'_Z Y$ from definition 1.3 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

□

1.3. Group varieties.

Definition 1.7. 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 1.8. *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 1.9. 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 1.10. 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 $\mathrm{Hom}_{\textbf{grp-var}}(G_1, G_2)$.

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 1.11. *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 1.12. Let K be a field of characteristic 0. Show that $\mathrm{Hom}_{\textbf{grp-var}}(\mathbb{A}^1_K, \mathbb{A}^1_K)$ consists of the linear polynomials $ax \in K[x]$ (hint: $\mathrm{Hom}(\mathbb{A}^1_K, \mathbb{A}^1_K) \cong K[x]$).

1.4. **Elliptic curves.**

1.5. **Some group theory.**

Definition 1.13. 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 1.14. 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 1.15. *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 1.16. *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*
$$\begin{aligned} f_\rho : G^{op} \to& \mathrm{Hom}(S, S) \\ g \mapsto& (s \mapsto \rho(s, g)) \end{aligned}$$

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 **??**. □

Definition 1.17. 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 1.18. *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 1.19. *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*

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

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 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 $\phi(0) = 0$.

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 $a_1, a_2, a_3, a_4, a_6 \in K$ then define $E_{a_1,a_2,a_3,a_4,a_6} \subset \mathbb{P}^2$ 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 $(x : y : z) = (0 : 1 : 0)$.

Proposition 2.3. *If E_{a_1,a_2,a_3,a_4,a_6} is smooth then $(E_{a_1,a_2,a_3,a_4,a_6}, 0)$ is an elliptic curve.*

Proof. add reference

□

Proposition 2.4. *Let $(E, 0)$ be an elliptic curve over K then there are $a_1, a_2, a_3, a_4, a_6 \in K$ such that*

$$(E, 0) \cong (E_{a_1,a_2,a_3,a_4,a_6}, 0)$$

Proof. add reference

□

say something about isomorphisms between weierstrass models

2.1.2. *Group law.*

2.1.3. *Level structure.*

Definition 2.5. Let E be an elliptic curve over a field K and let N be an integer that is invertible in K. Then a *full level N structure on E* is a group isomorphism $\phi : (\mathbb{Z}/N\mathbb{Z})^2 \to E[N](K)$.

Definition 2.6. 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. **Elliptic curves over C.**

Theorem 2.7. *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

□

Proposition 2.8. *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

□

2.3. **Families of elliptic curves.**

Definition 2.9. 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

- E is a variety over K,
- $f : E \to S$ is a smooth and proper map,
- 0 is a section of f; i.e. a regular map $0 : S \to E$ such that $f \circ 0 = \mathrm{Id}_S$,
- 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 $s \in S(\overline{K})$. Note that since f is smooth and proper the fiber E_s will be smooth and proper over $\overline{K}$. It is also reduced and of genus 1 by definition and 0_s will be a point on E_s. In particular for every $s \in S(\overline{K})$ the pair $(E_s, 0_s)$ is an elliptic curve over $\overline{K}$. This explains where the term "family of elliptic curves" comes from.

Definition 2.10. Let $(E_1, f_1, 0)$ and $(E_2, f_2, 0)$ be elliptic curve curves over S then a *morphisms 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:

$$\begin{tikzcd} E \arrow[rr, "h"] \arrow[dr, "f"'] & & E \arrow[dl, "g"] \\ & S & \end{tikzcd} \qquad \begin{tikzcd} E \arrow[rr, "h"] & & E \\ & S \arrow[ul, "0"] \arrow[ur, "0"'] & \end{tikzcd} .$$

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

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

is an inverse of T'. □

4. A hint towards Shimura varieties

4.1. The circle group.

Definition 4.1. 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 4.2. Show that the circle group satisfies the axioms of a group variety.

Exercise 4.3. 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.

Todo list

add proof 3
add reference 6
add reference 6
say something about isomorphisms between weierstrass models 6
add reference 6
add reference 6

References