

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. Group varieties	1
1.3. Elliptic curves	2
1.4. Some group theory	2
1.5. Adeles	4
2. Modular curves $\mathbb{C} \setminus \mathbb{R}$ and the upper half plane	4
2.1. Möbius transformations	4
3. A hint towards Shimura varieties	5
3.1. The circle group	5
References	5

1. BACKGROUND

1.1. Notations.

- If K is a field and V_1, V_2 are vector spaces over K then $\text{Iso}_{K\text{-vec}}(V_1, V_2)$ 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.

1.2. Group varieties.

Definition 1.1. 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 $\iota : G \rightarrow G$ defined over K called the inverse map,
- a morphism $s : G \times G \rightarrow G$ 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 1.2. *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 operation s, ι is a group.*

Proof. This follows immediately from the definition. \square

Example 1.3. 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 $e := (0, 0, \dots, 0) \in \mathbb{A}^n(K)$,

$$s: \mathbb{A}^n \times \mathbb{A}^n \rightarrow \mathbb{A}^n \quad (1.1)$$

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

$$\iota: \mathbb{A}^n \rightarrow \mathbb{A}^n \quad (1.3)$$

$$(a_1, a_2, \dots, a_n) \mapsto (-a_1, -a_2, \dots, -a_n). \quad (1.4)$$

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 side has is just coordinate wise addition in K .

Definition 1.4. 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 $\phi: G_1 \rightarrow G_2$ 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 $\text{Hom}_{\text{grp-var}}(G_1, G_2)$.

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 1.5. *Let $\phi: G_1 \rightarrow G_2$ 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 $G_1(L) \rightarrow G_2(L)$.*

Proof. This follows immediately from the definition. \square

Exercise 1.6. Let K be a field of characteristic 0. Show that $\text{Hom}_{\text{grp-var}}(\mathbb{A}_K^1, \mathbb{A}_K^1)$ consists of the linear polynomials $ax \in K[x]$ (hint: $\text{Hom}(\mathbb{A}_K^1, \mathbb{A}_K^1) \cong K[x]$).

1.3. Elliptic curves.

1.4. Some group theory.

Definition 1.7. Let G be a group and let $s: G \times G \rightarrow G$ 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

$$m^{op}: G \times G \rightarrow G$$

$$g, h \mapsto m(h, g)$$

Definition 1.8. 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 $\rho: G \times S \rightarrow S$ 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 $\rho : S \times G \rightarrow S$ 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 1.9. *Let G be a group and S be a set and let $\rho : G \times S \rightarrow S$ be an arbitrary map. Then the following are equivalent:*

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

$$f_\rho : G \rightarrow \text{Hom}(S, S)$$

$$g \mapsto (s \mapsto \rho(g, s))$$

is contained in $\text{Aut}(S) \subset \text{Hom}(S, S)$ and the induced map $f_\rho : G \rightarrow \text{Aut}(S)$ 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 $f_\rho(g) \in \text{Aut}(S)$. The rest of the proof is a relatively straightforward rewriting of the definitions of group action and group homomorphisms. \square

The above lemma looks slightly different for right group actions.

Lemma 1.10. *Let G be a group and S be a set and let $\rho : S \times G \rightarrow S$ be an arbitrary map. Then the following are equivalent:*

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

$$f_\rho : G^{op} \rightarrow \text{Hom}(S, S)$$

$$g \mapsto (s \mapsto \rho(s, g))$$

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

Proof. Similar to that of lemma 1.9. \square

Definition 1.11. Let $\rho G \times S \rightarrow S$ be a left action of the group G on the set S and let $s \in S$. Then the stabilizer of s in G is defined as

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

Lemma 1.12. *Let $\rho : G \times S \rightarrow S$ be a left action of the group G on the set S and let $s \in S$, then $\text{stab}_G(s)$ is a subgroup of G .*

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

Lemma 1.13. *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*

$$\phi : \coprod_{s_2 \in C} \text{stab}_G(s_2) \backslash S_1 \rightarrow G \backslash (S_1 \times S_2)$$

$$\text{stab}_G(s_2) s_1 \mapsto G(s_1, s_2)$$

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 $\text{stab}_G(s_2)s_1$. Now suppose $gs_1 \in \text{stab}_G(s_2)s_1$ with $g \in \text{stab}_G(s_2)$ is another element in the same orbit then

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

To show it is surjective, let $G(s_1, s_2) \in G \setminus (S_1 \times S_2)$ be an arbitrary. Since C is a set of representatives of $G \setminus S_2$ we can find a $s'_2 \in C$ and $g \in G$ such that $s_2 = gs'_2$. Now surjectivity follows since

$$G(s_1, s_2) = G(s_1, gs'_2) = Gg(g^{-1}s_1, s'_2) = \phi(\text{stab}_G(s'_2)g^{-1}s_1).$$

For injectivity let $s_1, s'_1 \in S$ and $s_2, s'_2 \in C$. If $\text{stab}_G(s_2)s_1$ and $\text{stab}_G(s'_2)s'_1$ map to the same element in $G \setminus (S_1 \times S_2)$ then s_2 and s'_2 must be in the same G orbit. However since C consists of representatives of $G \setminus S_2$ 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 $g \in \text{stab}_G(s_2)$ showing that $\text{stab}_G(s_2)s_1 = \text{stab}_G(s'_2)s'_1$. \square

1.5. Adeles.

2. MODULAR CURVES $\mathbb{C} \setminus \mathbb{R}$ AND THE UPPER HALF PLANE

2.1. Möbius transformations.

Definition 2.1 (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 $\text{GL}_2(\mathbb{R})$ on $\mathbb{C} \setminus \mathbb{R}$ as follows:

$$\rho : \text{GL}_2(\mathbb{R}) \times \mathbb{C} \setminus \mathbb{R} \rightarrow \mathbb{C} \setminus \mathbb{R} \quad (2.1)$$

$$\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \tau \right) \mapsto \frac{a\tau + b}{c\tau + d}. \quad (2.2)$$

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

$$\rho : \text{GL}_2(\mathbb{R}) \times \text{Iso}_{\mathbb{R}\text{-vec}}(\mathbb{R}^2, \mathbb{C}) \rightarrow \text{Iso}_{\mathbb{R}\text{-vec}}(\mathbb{R}^2, \mathbb{C}) \quad (2.3)$$

$$(\gamma, f) \mapsto f \circ \gamma^t. \quad (2.4)$$

The transpose is there to make it a left action. Indeed, if $\gamma_1, \gamma_2 \in \text{GL}_2(\mathbb{R})$ and $f \in \text{Iso}_{\mathbb{R}\text{-vec}}(\mathbb{R}^2, \mathbb{C})$ 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 2.2. *The map*

$$T : \text{Iso}_{\mathbb{R}\text{-vec}}(\mathbb{R}^2, \mathbb{C}) \rightarrow \mathbb{C} \setminus \mathbb{R} \quad (2.5)$$

$$f \mapsto \frac{f(1, 0)}{f(0, 1)} \quad (2.6)$$

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

Proof. First for the compatibility of the $\mathrm{GL}_2(\mathbb{R})$ action. Let $\gamma := \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{R})$ 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 $\mathrm{Iso}_{\mathbb{R}\text{-}\mathbf{vec}}(\mathbb{R}^2, \mathbb{C})/\mathbb{C}^* \rightarrow \mathbb{C} \setminus \mathbb{R}$. First note that if $\lambda \in \mathbb{C}^*$ then $T(\lambda f) = T(f)$ so that T factors through a map $T' : \mathrm{Iso}_{\mathbb{R}\text{-}\mathbf{vec}}(\mathbb{R}^2, \mathbb{C})/\mathbb{C}^* \rightarrow \mathbb{C} \setminus \mathbb{R}$. One can show that T' is bijective by proving that

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

is an inverse of T' . □

3. A HINT TOWARDS SHIMURA VARIETIES

3.1. The circle group.

Definition 3.1. The *circle group* is the group variety $\mathbb{S} \subseteq \mathbb{A}_{\mathbb{R}}^3$ 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

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

Exercise 3.2. Show that the circle group satisfies the axioms of a group variety.

Exercise 3.3. Let ϕ be defined by

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

Show that ϕ is a group homomorphism.

REFERENCES