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. 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 $\iota : G \to G$ 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 1.2. *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 operationse, ι, s is a group.*

Proof. This follows immediately from the definition. □

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 $e := (0, 0, \ldots, 0) \in \mathbb{A}^n(K)$,

$$s\colon \mathbb{A}^n \times \mathbb{A}^n \to \mathbb{A}^n \tag{1.1}$$
$$((a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n)) \mapsto (a_1 + b_1, a_2 + b_2, \ldots, a_n + a_n) \text{ and} \tag{1.2}$$
$$\iota\colon \mathbb{A}^n \to \mathbb{A}^n \tag{1.3}$$
$$(a_1, a_2, \ldots, a_n), \mapsto (-a_1, -a_2, \ldots, -a_n). \tag{1.4}$$

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 1.4. 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 $\phi : G_1 \to G_2$ 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 1.5. *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 1.6. 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: $\mathrm{Hom}(\mathbb{A}^1_K, \mathbb{A}^1_K) \cong K[x]$).

1.2. **Elliptic curves.**

1.3. **Some group theory.**

Definition 1.7. 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 1.8. 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 $\rho : G \times S \to S$ 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 1.9. *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 1.10. *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 lemma 1.9. □

Definition 1.11. 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 1.12. *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 1.13. *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*

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

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 $\mathrm{stab}_G(s_2)s_1 = \mathrm{stab}_G(s_2')s_1'$. □

1.4. **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 group action of $\mathrm{GL}_2(\mathbb{R})$ on $\mathbb{C} \setminus \mathbb{R}$ as follows:

$$\begin{aligned} \rho : \mathrm{GL}_2(\mathbb{R}) \times \mathbb{C} \setminus \mathbb{R} &\to \mathbb{C} \setminus \mathbb{R} \\ \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \tau \right) &\mapsto \frac{a\tau + b}{c\tau + d}. \end{aligned}$$

3. A hint towards Shimura varieties

3.1. **The circle group.**

Definition 3.1. The *circle group* is the group variety $\mathbb{S} \subseteq \mathbb{A}^3_{\mathbb{R}}$ 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 3.2. Show that the circle group satisfies the axioms of a group variety.

Exercise 3.3. Let ϕ be defined by

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

Show that ϕ is a group homomorphism.

References