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.**

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:

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

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