One-basedness and reductions of elliptic curves over real closed fields

Davide Penazzi

November 1, 2010

Abstract

We proceed with an analysis of 1-basedness for bounded hyperdefinable groups of the form G/G^{00} where $G = E(K)^0$ is the semialgebraic connected component of the K-points of an elliptic curve over a saturated real closed field K, or G a truncation of $E(K)^0$; we follow the method developed in [1]. We then relate the map $G \to G/G^{00}$ with the algebraic geometric notion of reduction, and we characterize 1-basedness of G/G^{00} in terms of algebraic geometric reduction and the notion of *internality* to the value group or to the residue field of a real closed valued field.

1 Introduction

In this section we shall recall Pillay's conjecture and the main results obtained in [1].

In section 2 we introduce elliptic curves and some tools useful for the calculations: the notion of minimal form for an elliptic curve, the definition of algebraic reduction and a simplification of the Weierstrass equation that allows us to describe the groups studied using only one parameter.

In section 3 we proceed in the study of 1-basedness when $G = E(K)^0$ where E is an elliptic curve with three "real" roots.

In section 4 we extend the results obtained to truncations of the groups studied in section 3.

This research has its roots in the positive solution of Pillay's conjecture [5]:

Theorem 1.1 (Pillay's conjecture)**.** *Given G a definably connected definable group in a saturated o-minimal structure M, then*

1. *G has a smallest type definable subgroup of bounded index G^{00}.*
2. *G/G^{00} is a compact connected Lie group, when equipped with the logic topology.*
3. *If, moreover, G is definably compact, then the dimension of G/G^{00} (as a Lie group) is equal to the o-minimal dimension of G.*
4. *If G is commutative then G^{00} is divisible and torsion free.*

This theorem gives us a functor from the category of definable, definably connected, definably compact groups to the category of compact Lie groups: $\mathbb{L} : G \to G/G^{00}$. It has become a mainstream topic in model theory to study which (topological, algebraic geometric...) properties are conserved by $\mathbb{L}$.

Another reason for my research is the extension of stability geometric notions, such as modularity and 1-basedness, to a broader context: to NIP theories and to definable sets.

For the rest of the paper K denotes a saturated model of the real closed fields.

We suppose that the reader is familiar with o-minimality, in particular with the notion of dimension of a definable set in an o-minimal theory; the book of Van den Dries [12] provides all the necessary theory.

The aim here is to give a dichotomy classification, on the lines of [2], of the groups G/G^{00} where G is a 1-dimensional definable, definably connected, definably compact group in K. We say that a definable group G is definably connected if there are no proper definable subgroups of finite index, and that it is definably compact if any function from an open interval of the base structure to G has limit in G.

Observe that G^{00} is only type definable in K, so G/G^{00} is a hyperdefinable group. We need to expand the structure we work on, in order to be able to "extract" the theory $T_{G/G^{00}}$ of G/G^{00}, and to define 1-basedness for G/G^{00} in terms of 1-basedness for $T_{G/G^{00}}$. This construction is presented in [1], where K is expanded by a predicate for G^{00}.

We recall the main definitions and facts:

Given an *o*-minimal theory T, and a model M, $f(x, \overline{y})$ a $\emptyset$-definable function in M, and $a \in M$, we define an equivalence relation $\sim_a$ on tuples of the same length as $\overline{y}$ by $\overline{c} \sim_a \overline{c}'$ if neither of $f(-, \overline{c})$, $f(-, \overline{c}')$ is defined in an open neighbourhood of a or if there is an open neighbourhood U of a such that $f(-, \overline{c}) = f(-, \overline{c}')$ in U. We call the equivalence class of $\overline{c}$ the *germ of* $f(-, \overline{c})$ *at* a, and denote it by $\overline{c}/\sim_a$.

We say that T is 1-based if in any saturated model $M \vDash T$, for any $a \in M$, for all definable functions $f(x, \overline{y}) : M \times M^n \to M$, and for any $\overline{c} \in M^n$ such that $a \notin dcl(\overline{c})$, we have $\overline{c}/\sim_a \in dcl(a, f(a, \overline{c}))$. This definition was introduced by Pillay in [7] and is equivalent to the notion of CF-linearity of [8].

The basic example of a 1-based *o*-minimal theory is the theory of an ordered vector space over a field, an example of non-1-based theory is the theory of real closed fields.

Let K' be a model of the theory $Th(K, G^{00}, \dots)$; we consider the structure $\mathcal{G}$ whose universe is G/G^{00} and there is a predicate for each $\emptyset$-definable (in K') subset of G/G^{00}. Then $\mathcal{G}$ is uniformly-*o*-minimal, by theorem 2.6 of [1], and, by theorem 2 of [10], G/G^{00} is stably embedded in K', i.e., every subset of $(G/G^{00})^n$ definable with parameters from K' is definable with parameters from G/G^{00}, it makes therefore sense to talk about the theory of $\mathcal{G}$.

We say then that G/G^{00} is 1-based in M' if the theory $T_{G/G^{00}} = Th(\mathcal{G})$ is 1-based.

Observe that the construction above can be generalised in the obvious way to define 1-basedness for any definable, uniformly-o-minimal set in a structure

M.

We define the notion of internality, introduced in [9].

Definition 1.2. *Given a definable set X in a saturated structure M we say that a definable set Y is internal to X if $Y \subseteq dcl(X \cup A)$ where A is a finite set of parameters.*

In [6] internality is used the context of algebraically closed valued fields, mainly to correlate stability of definable sets with their internality to the residue field. In our context we shall consider internality to the sorts Γ_w (value group) or k_w (residue field) of a real closed valued field, in order to transfer 1-basedness (or non-1-basedness, respectively) from Γ_w or k_w to our groups G/G^{00} in a suitable ambient structure.

A simple but useful remark is the following:

Remark 1.3. *Given saturated model M, a definable uniformly-o-minimal set Y internal to a 1-based set X is 1-based.*

Proof. Internality implies that there is a definable (with parameters) surjection g from X^n to Y. Then it is a definable bijection from a definable subset Z of X^n into Y. Suppose Y is non-1-based. This is witnessed by a function $f(y, \overline{y}) : Y \times Y^n \to Y$. The function $h : Z \times Z^n \to Z$ defined as $h(x, \overline{x}) = g^{-1}(f(g(x), g(\overline{x})))$ witnesses non-1-basedness of Z and therefore non-1-basedness of X, contradicting our hypotesis. □

An immediate consequence is the corollary:

Corollary 1.4. *Given a model M, uniformly-o-minimal definable sets X, Y in M, and a definable bijection $f : X \to Y$, then X is (non-) 1-based if and only if Y is (non-) 1-based.*

We shall maintain the notation of [1].

We assume basic knowledge of valuation theory. We denote a real closed valued field by $K_w = (K, \Gamma_w, w : K \to \Gamma_w \cup \infty)$, where K is a saturated real closed field with its signature, Γ_w a divisible abelian ordered group, called the value group, with its signature, and w a surjective map called valuation.

We denote the valuation ring by R_w, its unique maximal ideal (the valuation ideal) by I_w, $k_w = R_w/I_w$ the residue field; we recall moreover that $\Gamma_w = K/(R_w \setminus I_w)$.

When the valuation ring is Fin: the convex hull of $\mathbb{Q}$ in K, we call the valuation the *standard valuation* and denote it by v; the corresponding real closed valued field is M_v. The valuation ideal is μ, the infinitesimal neighbourhood of 0. The standard residue field, k_v, is $\mathbb{R}$, and the projection Fin $\to K_v$ is called *standard part map.*

We recall the notation for the open balls $B_{>\gamma}(a) = \{x \in K | w(x - a) > \gamma\}$ and closed balls $B_{\geq\gamma}(a) = \{x \in M | w(x - a) \geq \gamma\}$, where $\gamma \in \Gamma_w$ and $a \in K$. A simple remark is:

Remark 1.5. *There is a definable field isomorphism $B_{\geq\gamma}(0)/B_{>\gamma}(0) \cong k_w$ for any $\gamma \in \Gamma_w$*

Clearly the map $f : B_{\geq\gamma}(0) \to B_{\geq 0_{\Gamma_w}}(0)$, sending $x \mapsto \frac{x}{u}$, where $u \in K$ such that $v(u) = \gamma$, is well defined in the quotients $B_{\geq\gamma}(0)/B_{>\gamma}(0) \to B_{\geq 0_{\Gamma_w}}(0)/B_{>0_{\Gamma_w}}(0) = k_v$ and is a field isomorphism.

Remark 1.6. *In [11], Mellor proved that both Γ_w and k_w are stably embedded in M_w. This implies that $Th(\Gamma_w) = Th(\mathbb{Q}, +, 0, <, \lambda_q)_{q\in\mathbb{Q}}$, and therefore Γ_w is 1-based in M_w. Analogously $Th(k_w) = Th(\mathbb{R}, +, \cdot, 0, 1, <)$, and therefore k_v is non-1-based in M_w.*

Given a point $P \in M^2$ we shall denote by x_P and y_P the projections of P on the x-axis and the y-axis respectively.

Given a linearly ordered group $G = (G, *, <)$ a *truncation* of G by an element a is the group $\left(\left[a^{-1}, a\right), *_{\mod a^2}\right)$, where the operation $*_{\mod a^2}$ is defined as follows:

$$b *_{\mod a^2} c = \begin{cases} b * c & if\ a^{-1} < b * c < a \\ b * c * a^{-1} & if\ b * c > a \\ b * c * a & if\ b * c < a^{-1} \end{cases} .$$

In [1] the following theorem is proved:

Theorem 1.7. *Given a definable, definably compact, definably connected, one dimensional (in the o-minimal sense) group G in a saturated real closed field M, if G is an additive truncation, a small multiplicative truncation (a truncation of the multiplicative group by an element of nonnegative valuation) or a truncation of $SO_2(M)$, G/G^{00} is non-1-based in the expansion of M by a predicate for G^{00}.*

If G is a big multiplicative truncation, i.e. $G = \left(\left[b^{-1}, b\right), *\ mod\ b^2\right)$, with $v(b) < 0$, the group G/G^{00} is 1-based in the expansion of M by a predicate for G^{00}.

In this paper we shall often refer to the result above.

We shall observe that when we consider G to be the semialgebraic connected component of the K-points of an elliptic curve over K: $E(K)^0$, or G is a truncation of $E(K)^0$; its unique minimal, bounded index, type-definable subgroup G^{00} determines a cut on K. Adding a predicate for G^{00} to K, the cut becomes definable and it determines a valuation w on K. We denote the enriched structure $(K, G^{00}, \dots)$ by K'. Given the group G as above, we determine (definably in K') canonically a value group Γ_w and a residue field k_w, therefore K' will be interdefinable with a real closed valued field K_w.

We shall moreover determine a notion of minimal form of an elliptic curve, for curves in minimal form we define three kinds of reductions of their K-points.

Theorem 1.8. *Given an the group $G = E(K)^0$, or G a truncation of $E(K)^0$, where E is an elliptic curve with three "real" roots, over a saturated real closed field K, the structure K' obtained by adding a predicate for G^{00} to K is interdefinable with a real closed valued field K_w.*

There are two possible behaviours, either one of the following conditions hold:

1. *The group G/G^{00} is 1-based.*
2. *The group G/G^{00} is internal to Γ_w in K'.*

3. - *Either $G = E(K)^0$ and E has split multiplicative reduction, or*
   - *G is the truncation of $E(K)^0$ by a point P with infinitesimal projection on the x-axis, where E is an elliptic curve with split multiplicative reduction.*

Or one of the following condition holds:

1. *The group G/G^{00} is non-1-based.*
2. *The group G/G^{00} is internal to k_w in K'.*
3. - *Either $G = E(K)^0$ and E has good or nonsplit multiplicative reduction, or*
   - *G is the truncation of $E(K)^0$ by a point P with projection on the x-axis non infinitesimal, where E is an elliptic curve with split multiplicative reduction.*

2 Elliptic curves in minimal form

An elliptic curve over a field F is a one-dimensional projective curve defined by an equation of the form

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, \ldots, a_6 \in F$, plus a point at infinity, denoted by O.

When we work in the projective space we define it by $ZY^2 + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2 + a_4XZ^2 + a_6Z^3$, and the point at infinity is $O = [0:1:0]$.

Such a curve can be endowed with a group structure, whose identity is O; we denote the operation by $\oplus$ and the inverse of a point P by $\ominus P$.

Any line will intersect an elliptic curve at precisely three points (recall that also O is a point in this context). Given points P, Q, the line through P and Q (or the tangent line if $P = Q$) intersects E at the point R. The line between R and O will again intersect E at one point, which we call R'. We then define $P \oplus Q$ to be R'.

The explicit addition formula, given $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$, $P \neq Q$ is:

$$x_{P\oplus Q} = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 + a_1\frac{y_Q - y_P}{x_Q - x_P} - a_2 - x_P - x_Q.$$

Observe that $E(K)$ is a topological group, but since the usual topology of K it is totally disconnected (by saturation), we consider its semialgebraic connected component $E(K)^0$.

To work with elliptic curves we need some simplifications. Since all properties we are going to deal with are invariant under definable isomorphisms, we can limit our study to curves expressed in a "minimal" form.

Firstly we recall that two elliptic curves E and E' are isomorphic if you can obtain E' from E by the following change of variables:

$$\left\{\begin{array}{ll} x = & u^2x' + r \\ y = & u^3y' + u^2sx' + t, \end{array}\right. \tag{1}$$

where $u, r, s, t \in K$, $u \neq 0$. These transformations are clearly definable in the structure K.

Given a valuation ring R_w with valuation w, we can always express the curve with an equation with coefficients from R_w (recall that $x \in R_w \iff w(x) \geq 0$):

Lemma 2.1. *Given a curve $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, defined over K, and a valuation w, we can always suppose that the coefficients a_i are in R_w.*

Proof. If it is not the case, we can replace (x, y) by $(u^{-2}x, u^{-3}y)$. So each a_i in the equation becomes a_iu^i. Therefore it is sufficient to take u such that $w(u) \geq max_i(-w(a_i))$, so, for each a_iu^i, we shall have $w(a_iu^i) = w(a_i) + iw(u) \geq 0$. □

It is a well known fact that in K, we can rewrite E as

$$y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}, \tag{2}$$

(it is sufficient to complete the square, i.e., use the function $y \mapsto \frac{1}{2}(y - a_1x - a_3)$, and then change again variable $y \mapsto 2y$).

A curve in this form is an elliptic curve (i.e., is nonsingular) if and only if the discriminant of the curve $\Delta \neq 0$, in this case $\Delta = -b_2^2 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$.

When applying the transformation $(\circ)$ the new curve will have discriminant $\Delta' = u^{-12}\Delta$.

We can define a formal multiplication by integers: Given $m \in \mathbb{Z}$, we define

$$[m]P = \begin{cases} P \oplus P \oplus \cdots \oplus P \ (m \text{ times}) & if\ m > 0 \\ O & if\ m = 0 \\ [-m] \ominus P & if\ m < 0 \end{cases}$$

The doubling formula is:

$$x_{[2]P} = \frac{x_P^4 - b_4x_P^2 - 2b_6x_P - b_8}{4x_P^3 + b_2x_P^2 + 2b_4x_P + b_6}$$

The definably connected component $G = E(K)^0$ is therefore a definable group in K, clearly definably connected. Since $E(K)$ is nonsingular and has a point at infinity it is definably compact.

Moreover G can be naturally endowed with a linear ordering (by fixing a point, e.g. O), denoted $\lhd$. It is defined by:

$$P \lhd Q \ \ if \begin{cases} y_P < 0 & and\ y_Q > 0 \\ x_P > x_Q & and\ y_P, y_Q > 0 \\ x_Q < x_P & and\ y_P, y_Q < 0 \\ P \oplus P = O & \\ y_P < 0 & and\ Q = O \\ y_Q > 0 & and\ P = O \end{cases}$$

For a more extensive introduction to the theory of the elliptic curves the reader is invited to refer to [3].

2.1 Minimal form of an elliptic curve

In a local field there is a discrete valuation w, and we can in an unique way (up to certain transformations, see proposition 2.3 below) define a minimal form for an elliptic curve (this is the usual definition, we shall use a slightly different one given later):

Given an elliptic curve E defined over a local field, with valuation ring R and valuation w, an equation for E is in *minimal form* if $w(\Delta)$ is minimised subject to the condition $a_1, a_2, a_3, a_4, a_6 \in R$.

When we are in a real closed field, equipped with a valuation ring, the definition above gives us a family of curves, we adapt the definition as follows:

Definition 2.2. *An elliptic curve E defined over a real closed field K equipped with a valuation ring R_w and a valuation w is in* minimal form *if $w(\Delta)$ is minimised subject to the conditions: $a_1, a_2, a_3, a_4, a_6 \in R$, one root is in $(0,0)$ and $w(a_i) = 0$ for some i.*

An analogy of proposition 1.3 of [3] can now be proved in this context:

Proposition 2.3. *1. Every curve E defined over K has a minimal Weierstrass equation*

2. This minimal Weierstrass equation is unique up to a change of coordinates

$$\begin{cases} x = & u^2x' + r, \\ y = & u^3y', \end{cases}$$

where $r = -a \pm \sqrt{a^2 - 4b}$ and $v(u) = 0$.

Proof. 1) The equation of an elliptic curve over a real closed field can always be factorized as $y^2 = (x - e_1)(x^2 + ax + b)$, with $a, b \in M$. A translation guarantees that we can fix a root at $(0,0)$. We can then suppose our curve is in the form $y^2 = x(x^2 + ax + b)$, with $a, b \in Fin$. If neither a nor b have valuation 0, then $w(\Delta) = w(16a^2b^3 - 64b^3) = 2w(b) + w(a - 16b) > 0$. A transformation

$$\begin{cases} x = u^2x', \\ y = u^3y', \end{cases}$$

gives us a curve $E' = x(x^2 + a'x + b')$, for which $a' = a/u^2$ and $b' = b/u^4$. We can therefore find u with positive valuation such that either a' or b' have valuation 0. Such u will then be the unique element which produces an elliptic curve satisfying the conditions on the minimal form.

2) In the change of coordinates above, the choice of r preserves one root at $(0,0)$. Observe that the new curve is $y^2 = x\left(x - \frac{a+\sqrt{a^2-4b}}{2u^2}\right)\left(x - \frac{a-\sqrt{a^2-4b}}{2u^2}\right)$, and that $v\left(\frac{a+\sqrt{a^2-4b}}{2u^2}\right) + v\left(\frac{a-\sqrt{a^2-4b}}{2u^2}\right) = v(a^2 - a^2 + 4b) - v(u^2) = v(b)$. Now if we have $v(b) = 0$, then $v\left(\frac{a+\sqrt{a^2-4b}}{2u^2}\right)$ and $v\left(\frac{a-\sqrt{a^2-4b}}{2u^2}\right)$ are both 0, since they are both positive, and so the new equation is still a minimal Weierstrass equation.

Otherwise, $v(b) > 0$, and $v(a)$ has to be 0 by minimality of the Weierstrass equation, and therefore either $v\left(\frac{a+\sqrt{a^2-4b}}{2u^2}\right)$ or $v\left(\frac{a-\sqrt{a^2-4b}}{2u^2}\right)$ has to be 0, and so the new equation is still minimal.

□

By working with a curve in minimal form we guarantee that we can define certain properties in an unique way for the all the curves in the isomorphism class (in particular it determines a unique reduction over a residue field, discussed in the following chapters).

2.2 Algebraic geometric reductions

An important tool in the arithmetic study of elliptic curves defined over local fields is the notion of reduction over a residue field. This topic is developed in Chapter VII of [3].

We present here a description of this tool, adapted to the context of real closed fields.

We suppose E is defined over a saturated real closed field K, and equip K with the standard valuation. As we noticed in lemma 2.1 we can suppose E to be defined by coefficients in Fin, and by property 2.3 we can moreover suppose E to be in minimal form.

When we project the K-points $E(K)$ of the elliptic curve onto the standard residue field we obtain a curve $\tilde{E}(\mathbb{R})$ which is easier to study. The definition of this operation is delicate and requires some care.

We define the reduction $\tilde{E}$ of a curve $E : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ in minimal form as the curve over k_v defined by $y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6$.

Observe that the eqution over k_v is well defined since we supposed the coefficients to be in Fin (and $\text{Fin}/\mu = k_v = \mathbb{R}$).

This gives us a reduction map

$$\begin{aligned} E(K) &\to \tilde{E}(\mathbb{R}), \\ P &\mapsto \tilde{P}, \end{aligned}$$

defined as follows: given a point $P = (x, y) \in E(K)$ we rewrite it in homogeneous coordinates: $P = [x; y; 1]$. This clearly can always be rewritten with coefficients in Fin: $P = [x'; y'; z']$ (it is sufficient to multiply the factors by a sufficiently small $\lambda \in K$, if x and y are infinite). We can now project the coordinates onto the residue field, and P reduces to $\tilde{P} = [st(x'); st(y'); st(z')]$. We multiply back by λ^{-1} to obtain $\tilde{P} = [\lambda^{-1}(st(x'))\,; \lambda^{-1}(st(y'))\,; \lambda^{-1}(st(z'))]$. In affine coordinates it is then simply

$$\begin{cases} \tilde{P} = (st(x), st(y)) & if\ x, y \in \text{Fin} \\ \tilde{P} = O & if\ x, y \notin \text{Fin}\,. \end{cases}$$

This operation, however, is not harmless: $\tilde{E}(\mathbb{R})$ may not longer be an elliptic curve, and it could have singularities. The set of nonsingular points of $\tilde{E}(\mathbb{R})$ forms a group, denoted by $\tilde{E}_{ns}(\mathbb{R})$.

We define two subsets of $E(K)$ depending on how the curve reduces:

$$E_0(K) = \{P \in E(K) : \tilde{P} \in \tilde{E}_{ns}(\mathbb{R})\}, \tag{3}$$

i.e., the set of all points of E whose reduction is nonsingular, and

$$E_1(K) = \{P \in E(K) : \tilde{P} = \tilde{O}\}\ (= \{P \in E(K) | v(x_P) < 0\}), \tag{4}$$

i.e., the set of all points whose reduction is the identity.

Such notions are well defined by Property 2.3.

By $E_0(K)^0$ and $E_1(K)^0$ we shall denote $\{P \in E(K)^0 | \tilde{P} \in \tilde{E}_{ns}(\mathbb{R})\}$ and $\{P \in E(K)^0 | \tilde{P} = \tilde{O}\}$ respectively.

A useful proposition is the following:

Proposition 2.4. *There is a group isomorphism* $E_1(K)/E_0(K) \cong \tilde{E}_{ns}(\mathbb{R})$.

Proof. The proof is in proposition 2.1 of [3], observing that a real closed valued field satisfes Hensel's lemma. □

2.3 Three "real" roots elliptic curves

We have two cases, either we can factorise the right hand side of equation 2 into three roots in K^2, or in only a root and a quadratic term. In this article we consider the first case.

We use the terms "real" and "complex" in this context in an improper way: by "real" we mean in the real closed field K, and by "complex" we mean in its algebraic closure $K[i]$.

Our equation becomes $y^2 = (x - e_1)(x - e_2)(x - e_3)$ with $e_i \in K$, $i = 1, 2, 3$. We want to write this curve in a minimal form with respect to the standard valuation and fix two roots.

We apply the transformation

$$\begin{cases} x & \mapsto x + e_1, \\ y & \mapsto y. \end{cases}$$

and get an isomorphic curve with a root on $(0, 0)$: $y^2 = x(x - e_2')(x - e_3')$, where $e_2' = e_2 - e_1$ and $e_3' = e_3 - e_1$.

We can suppose that $v(e_2') \leq v(e_3')$; by divisibility of the value group we can take u such that $v(u^2) = -v(e_2)$. Applying the transformation

$$\begin{cases} x & \mapsto u^{-2}x, \\ y & \mapsto u^{-3}y. \end{cases}$$

we get an isomorphic curve $y^2 = x(x - e_2'')(x - e_3'')$ where $e_2'' = u^2 e_2$, and $e_3'' = u^2 e_3$. Therefore $v(e_2''), v(e_3'') > 0$, i.e. all the roots are in Fin.

This is a necessary condition for a minimal equation.

We have now 2 possibilities: either $e_2'' > 0$ or $e_2'' < 0$.

1. If $e_2'' > 0$ then $(e_2'')^{\frac{1}{2}}$ is in M, and we can therefore apply the transformation

$$\begin{cases} x & \mapsto e_2'' x \\ y & \mapsto (e_2'')^{\frac{3}{2}} y. \end{cases}$$

   This produces the isomorphic curve $y^2 = x(x - 1)\left(x - \frac{e_3''}{e_2''}\right)$; observe that since $v(e_2'') \leq v(e_3'')$, we have that $\frac{e_3''}{e_2''} \in \text{Fin}$.

We can transform such a curve into a curve of the form $y^2 = x(x+1)(x-\epsilon)$, via

$$\begin{cases} x & \mapsto x+1 \\ y & \mapsto y. \end{cases}$$

2. If $e_2'' < 0$ then $(-e_2'')^{\frac{1}{2}}$ is in M, and we can therefore apply the transformation

$$\begin{cases} x & \mapsto -e_2'' x \\ y & \mapsto (-e_2'')^{\frac{3}{2}} y. \end{cases}$$

This produces the isomorphic curve $y^2 = x(x+1)\left(x + \frac{e_3''}{e_2''}\right)$, where again $-\frac{e_3''}{e_2''} \in \text{Fin}$. Renaming $-\frac{e_3''}{e_2''} = \epsilon$ we get $y^2 = x(x+1)(x-\epsilon)$.

We have therefore obtained a form for the equations of the elliptic curves with three "real" roots in which each curve (and its isomorphism class) is determined by a single parameter (note that there can be $\epsilon \neq \epsilon' \in K$ such that they define curves in the same isomorphism class though they can be different.)

We need to check that it is a minimal form with respect to the standard valuation.

One of the roots is at $(0,0)$, and one is in $\text{Fin} \setminus \mu$, thus the determinant has valuation $v(\Delta) = 2v(\epsilon) + 2v(\epsilon+1)$. Clearly either $v(\epsilon)$ or $v(\epsilon+1)$ is equal to 0. If both are equal to 0 we are done, if not, any transformation of the form $(\circ)$ with $v(u) \neq 0$ would send -1 to either μ or to $K \setminus \text{Fin}$, contradicting minimality. Therefore this is a minimal form.

We can rewrite the sum and the doubling formulae for curves in this form in a simpler way:

$$\pi_1(P \oplus Q) = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - (1-\epsilon) - x_Q - x_P, \tag{5}$$

$$\pi_1([2]P) = \frac{(x_P^2 + \epsilon)^2}{4x_P(x_P+1)(x_P-\epsilon)} \tag{6}$$

For such curves we can compute the possible reductions over the reals:

Remark 2.5. *We obtain three kinds of curves:*

1. *Good reduction curves: if $v(\epsilon) = 0$ and $v(\epsilon+1) = 0$, this imples that the standard part of the root $(\epsilon, 0)$ does not coincide with any of the other roots, and therefore the reduced curve is nonsingular.*

2. *Non-split multiplicative reduction curves: if $v(\epsilon+1) > 0$, this implies that the root $(\epsilon, 0)$ is sent by the standard part map to the root $(-1, 0)$, and therefore the reduced curve has a complex node.*

3. *Split multiplicative reduction curves: if $v(\epsilon) > 0$, this implies that the root $(\epsilon, 0)$ is sent by the standard part map to the root $(0, 0)$, and therefore the reduced curve has a real node.*

3 Case study

We can now check for which curves E the groups G/G^{00}, where $G = E(K)^0$, are 1-based in the structure $K' = (K, G^{00}, \dots)^{eq}$.

In section 2 we proved that any elliptic curve with three real roots is isomorphic to a curve of the form $y^2 = x(x+1)(x-\epsilon)$ with $\epsilon \in \mathrm{Fin}$.

Our first step is to determine the cut on K produced by G^{00} (or, better, by its projection on the first coordinate). In order to compute it we consider the torsion points, i.e., the points $T_n \in G$ such that $[n]T_n = O$ for $n \in \omega$. We such call T_n an n-torsion point.

We can then type-define G^{00} as follows:

$$E^{00} = \bigcap_{n\in\omega} \{P | \forall T\, [(T \rhd O \wedge [n]T = O) \to \ominus T \lhd P \lhd T]\}. \tag{7}$$

We already know that T_2 is either $(0,0)$ or $(\epsilon, 0)$, if $\epsilon < 0$ or $\epsilon \geq 0$ respectively.

It is convenient to compute aside the projection of the 4-torsion points T_4, we shall then compute inductively an approximation of $x_{T_{2^n}}$ for $n \in \omega$.

- If $\epsilon < 0$ ($T_2 = (0,0)$), the tangent to the curve passing from T_2 is $y = \alpha x$, with α such that the following system has a double solution:

$$\begin{cases} y &= \alpha x \\ y^2 &= x(x+1)(x-\epsilon). \end{cases}$$

  On solving it we obtain

$$x^2 + (1 - \epsilon - \alpha^2)x - \epsilon = 0. \tag{8}$$

  The α must then satisfy $(1-\epsilon-\alpha^2)^2 - 4\epsilon = 0$, so $\alpha^2 = 1 - \epsilon \pm 2\sqrt{-\epsilon}$; we take the positive root to obtain the tangent to G (otherwise, taking the negative root, we obtain the tangent to the semialgebraic component $E(K) \setminus G$).

  Substituting into the solution of (8) we get $x = \frac{1-\epsilon+2\sqrt{-\epsilon}+\epsilon-1}{2} = \sqrt{-\epsilon} = x_{T_4}$.
  (I.e., $T_4 = (\sqrt{-\epsilon}, +\sqrt{1-\epsilon+2\sqrt{-\epsilon}})$, and $\ominus T_4 = (\sqrt{-\epsilon}, -\sqrt{1-\epsilon+2\sqrt{-\epsilon}})$).

- If $\epsilon > 0$ ($T = (\epsilon, 0)$), the system to be solved to obtain the 4-torsion points is

$$\begin{cases} y &= \alpha x - \alpha\epsilon \\ y^2 &= x(x+1)(x-\epsilon). \end{cases}$$

  This leads to the solutions $\alpha^2 = \epsilon \pm \sqrt{\epsilon^2 - \epsilon}$ and so $x = \epsilon + \sqrt{\epsilon}\sqrt{\epsilon+1} = x_{T_4}$.

  (Observe that we cannot have $\epsilon = 0$ since E is an elliptic curve, therefore it is nonsingular)

Before proving the main lemma we observe that if $v(\epsilon) > 0$ we can suppose $\epsilon > 0$. In fact if $\epsilon < 0$ we can apply to $E : y^2 = x(x-1)(x+\epsilon)$ the homotety:

$$\begin{cases} x &= \frac{1}{1+\epsilon} x' \\ y &= y'. \end{cases}$$

Since $v(\epsilon) > 0$ we have $v(\frac{1}{1+\epsilon}) = 0$, and therefore such a transformation does not harm the minimality of the equation by Proposition 2.3.

We can now compute G^{00} in terms of ϵ.

A fact that we shall often use without mention is that if $v(a) \neq v(b)$ or $\text{sign}(a) = \text{sign}(b)$, $v(a+b) = \min\{v(a), v(b)\}$.

Lemma 3.1. *Let E be a curve in the form $y^2 = x(x+1)(x-\epsilon)$, $G = E(K)^0$. Then $G^{00} = \bigcap_{n\in\omega} \left\{P \in G | v\left(x_P\right) < \frac{1}{n} v(\epsilon)\right\}$.*

Proof. The idea is to compute the valuation of the projection of the torsion points using the doubling formula: an induction will show the behaviour of the valuation of the 2^n-torsion points.

Without harm we shall always consider torsion points T_n that have projection on the x-axis greater than the projection of the torsion points T_i where $i < n$; this is due to the definition of G^{00}: (7), and the symmetry of the elliptic curve. Thus we shall suppose that $v\left(x_{T_{n+1}}\right) \leq v\left(x_{T_n}\right)$. Moreover, due to the symmetry of G with respect to the x-axis, we shall consider only torsion points with positive projection on the second cordinate, i.e., $v\left(y_{T_n}\right) \geq 0$ for all $n \in \omega$.

We have two cases:

1. $v(\epsilon) = 0$, i.e. ϵ is not infintesimally close to 0.

   To get the desired $G^{00} = \{P \in G | v(x_P) < 0\}$ we need to prove that the torsion points have projection, and are cofinal, in Fin.

   The first part is trivial, the second is equivalent to the statement that that for each $s \in \text{Fin}$ we can find a torsion point whose projection on the x-axis is greater than s; it sufficies to prove that for some $n \in \mathbb{N}$ the point P such that $x_P = s$ has $x_{[n]P} \leq x_{T_4}$.

   We have two sub-cases:

   - $\epsilon > 0$, so $x_{T_4} = \epsilon + \sqrt{\epsilon}\sqrt{\epsilon+1} > 2\epsilon$. We prove that if $P = (x_P, y_P)$ has $x_P > x_{T_4}$ then $x_{[2^n]P} \leq x_{T_4}$, for some $n \in \mathbb{N}$.

     Recall the duplication formula: $x_{[2]P} = \frac{(x_P^2+\epsilon)^2}{4x_P(x_P+1)(x_P-\epsilon)}$. Since we suppose P is smaller (with respect to the order $\lhd$ of $E^0(M)$) than T_4, then $x_P > 2\epsilon$, so $x_{[2]P} < \frac{(x_P^2+\frac{x_P}{2})^2}{4x_P(x_P+1)(x_P-\frac{x_P}{2})} = \frac{(x_P+\frac{1}{2})^2}{2(x_P+1)} = \frac{x_P(x_P+1)+\frac{1}{4}}{2(x_P+1)} = \frac{x_P}{2} + \frac{1}{8(x_P+1)} < \frac{x_P}{2} + \frac{1}{8x_P} < \frac{x_P}{2} + \frac{1}{16\epsilon}$.
     We can therefore define a sequence of points p_i such that for each i, $p_i \geq x_{[2^i]P}$ using the formula above. It is easy to observe that, setting $p_0 = x_P$, we have $p_i = \frac{p_0}{2^i} + \frac{\sum_{j=0}^{i-1} 2^i}{2^{i+4}\epsilon} = \frac{p_0}{2^i} + \frac{2^i-1}{(2-1)2^{i+4}\epsilon} = \frac{p_0}{2^i} - \frac{1}{2^{i+4}\epsilon} + \frac{1}{16\epsilon}$. But since $\lim_{i\to\omega} p_i = \frac{1}{16\epsilon}$, we must have that for some $n \in \omega$, $x_{[2^n]P} \leq p_n \leq x_{T_4}$.
   - $\epsilon < 0$, so $x_{T_4} = \sqrt{-\epsilon}$. As above we take $P = (x_P, x_Q)$ and suppose $x_P > \sqrt{-\epsilon}$. Using the duplication formula we get $x_{[2]P} = \frac{(x_P^2+\epsilon)^2}{4x_P(x_P+1)(x_P-\epsilon)} < \frac{x_P^4}{4x_P^3} = \frac{x_P}{4}$. We can therefore find an $n \in \omega$ such that $x_{[2^n]P} \leq x_{T_4}$ as in the previous case.

2. If $v(\epsilon) > 0$, then by our observation $\epsilon > 0$, and so $T_2 = (\epsilon, 0)$. We denote by p_n the projection on the x axis of the n-torsion point. The calculation of the 4-torsion points leads to $x_{T_4} = \epsilon + \sqrt{\epsilon}\sqrt{\epsilon+1}$. So $v(x_{T_4}) = v(\sqrt{\epsilon}) - v(\sqrt{\epsilon} + \sqrt{\epsilon+1}) = v(\sqrt{\epsilon}) = \frac{1}{2}v(\epsilon)$.

   The doubling formula for torsion points can be then written as:

$$x_{T_{n/2}} = \frac{1}{4}\frac{x_{T_n}^4 + 2\epsilon x_{T_n}^2 + \epsilon^2}{x_{T_n}^3 + (1-\epsilon)x_{T_n}^2 - \epsilon x_{T_n}}. \tag{9}$$

   Passing to the valuation we get $v\left(x_{T_{n/2}}\right) = 2v\left(x_{T_n}^2 + \epsilon\right) - v(x_{T_n}) - v(x_{T_n} + 1) - v(x_{T_n} - \epsilon)$.

   A couple of considerations:

   - All torsion points have valuation of the first coordinate strictly positive. In fact, by induction let n be the smallest such that $v(x_{T_n}) \leq 0$. Then $v\left(x_{T_{n/2}}\right) = 2v(x_{T_n}^2) - v(x_{T_n}) - v(x_{T_n}+1) - v(x_{T_n}) = 4v(x_{T_n}) - 3v(x_{T_n}) = v(x_{T_n}) > 0$, contradicting our assumption that $T_{n/2} \lhd T_n$ and $y_{T_n}, y_{T_{n/2}} > 0$.
   - We need to make sure that the valuation of x_{T_8} is strictly less than $v(x_{T_4})$. Again by contradiction suppose $v(x_{T_8}) = v(x_{T_4}) = \frac{1}{2}v(\epsilon)$. Then $\frac{1}{2}v(\epsilon) = v(x_{T_4}) = 2v(x_{T_8}^2 + \epsilon) - v(x_{T_8}) - v(x_{T_8}+1) - v(x_{T_8} - \epsilon) \geq 2v(\epsilon) - \frac{1}{2}v(\epsilon) - \frac{1}{2}v(\epsilon) = v(\epsilon)$, which contradicts $v(\epsilon) > 0$. In conclusion we have for $n \geq 8$: $\frac{1}{2}v(\epsilon) > v(x_{T_n}) > v(x_{T_{2n}}) > 0$ (It is in fact trivial to prove this for $n > 8$).

   By the considerations we get $v(x_{T_n}) = 2v(x_{T_{2n}}^2) - v(x_{T_{2n}}) - v(x_{T_{2n}}) = 2v(x_{T_{2n}})$, i.e., $v(x_{T_{2n}}) = \frac{1}{2}v(x_{T_n})$.
   This implies $G^{00} = \bigcap_{n\in\omega}\left\{P \in G | v\left(x_P\right) < \frac{1}{n}v(\epsilon)\right\}$.

□

It is easy and left to the reader to check that the projection on the x-axis of G^{00} is a valuational cut, and that therefore there is an unique valuation associated to G^{00}.

We now check which curves produce 1-based G/G^{00}, relating them to the behaviour of $E(K)$ when reduced over the standard residue field.

We have three possible kind of reductions, see Remark 2.5.

3.1 The good reduction case

This is the case of a curve $E : y^2 = x(x+1)(x-\epsilon)$ with $v(\epsilon) = 0$, and $v(\epsilon + 1) = 0$. Here the algebraic geometric reduction leads to the elliptic curve curve $\tilde{E}(\mathbb{R}) : y^2 = x(x+1)(x - st(\epsilon))$.

Clearly then $E(K) = E_0(K)$, and, by lemma 3.1, $E_1(K) = \{P \in E(K) | v(x_P) < 0\} = G^{00}$.

This, together with proposition 2.4, implies that

$$G/G^{00} = E(K)^0/E(K)^{00} = E_0(K)^0/E_1(K)^0 = \tilde{E}^0(\mathbb{R}). \tag{10}$$

We add now to K a predicate for G^{00} as in [1]: let $K' = (K, G^{00}, \dots)$. We can define in it the sets Fin and μ:

$$\text{Fin} = \left\{ x \in K | \exists y \in K \Big((x,y) \in G^{00} \vee (-x,y) \in G^{00} \Big) \right\}, \tag{11}$$

$$\mu = \left\{ x \in K | x^{-1} \in \text{Fin} \right\}. \tag{12}$$

Clearly in the standard real closed valued field $K_v = (K, \text{Fin}, \mu, v, \dots)$ the set G^{00} is definable, so K' is interdefinable with K_v.

Moreover G/G^{00} is a definable set of k_v and it is clearly internal to k_v in K'. By remark 1.6 k_v is non-1-based in $K_v = K'$ and by lemma 1.3 also G/G^{00} is non-1-based in K'.

3.2 The non-split multiplicative reduction case

In this case we have a curve $E : y^2 = x(x+1)(x-\epsilon)$, with $v(\epsilon+1) > 0$, i.e., the roots $(\epsilon, 0)$ and $(-1, 0)$ are infinitely close.

The algebraic geometric reduction here leads to a singular curve with a "complex node": the semialgebraic component without the identity is sent by the standard reduction map to the point $(-1, 0)$.

We can easily compute the sets $G^{00} = \{P \in G | v(x_P) < 0\} = E_1(K)^0 = E_1(K)$ and $G = E_0(K)^0 = E_0(K)$.

We can use the same argument of the good reduction case to prove non-1-basedness of G/G^{00}. By proposition 2.4 and our considerations we have that $G/G^{00} = E_0(K)^0/E_1(K)^0 \cong (=)\tilde{E}^0(\mathbb{R})$ as abelian groups.

Again the structure $K' = (K, E^{00})$ defines Fin and μ and so we again get that K' is interdefinable with the standard real closed valued field K_v, and that G/G^{00} is internal to $k_v = \mathbb{R}$. Thus, by lemma 1.3, G/G^{00} inherits non-1-basedness from k_v.

In the previous and this subsection we proved the following lemma:

Lemma 3.2. *Given an elliptic curve E in minimal form, and such that $E(K)$ has good or nonsplit multiplicative reduction, the group G/G^{00}, where $G = E(K)^0$, is non-1-based in $K' = (K, G^{00}, \dots)$ and is internal to k_v, the residue field of the real closed valued field interdefinable with K'.*

We highlight now what is the actual Lie group structure of G/G^{00}, by proposition 2.4, it is sufficient to consider the connected component of $y^2 = x(x+1)^2$, i.e., of $\tilde{E}(\mathbb{R})$. We will follow the procedure shown in Exercise 3.5, page 104 of [3]: first we find an isomorphism of $E(\mathbb{C})$ into $(\mathbb{C}, \cdot)$, then show that $E(\mathbb{R}) \cong \{t \in \mathbb{C} : |t| = 1\}$, therefore $E(\mathbb{R}) \cong SO_2(\mathbb{R})$.

The node is clearly $N = (-1, 0)$, and to find the tangent is sufficient to solve the system

$$\begin{cases} y & = \alpha x + \alpha \\ y^2 & = x^3 + 2x^2 + x \end{cases}$$

In a way in which α leads to a multiple root, therefore we have $(\alpha^2 - x)(x+1)^2 = 0$, and so $\alpha = \pm i$. The isomorphism $f : (E(\mathbb{C}), \oplus) \cong (\mathbb{C}, \cdot)$ is $(x, y) \mapsto \frac{y-ix-i}{y+ix+i}$, by Proposition 2.5, page 61 of [3]. We now have just to show that if $x, y \in \mathbb{R}$ then $|f(x, y)| = 1$. In fact $\frac{y-ix-i}{y+ix+i} = \frac{1}{y^2+(x+1)^2}|(y - i(x+1))^2| = \frac{1}{y^2+(x+1)^2}\sqrt{(y^2 - (x+1)^2)^2 + 4y^2(x+1)^2} = \frac{y^2+(x+1)^2}{y^2+(x+1)^2} = 1$.

We notice here a difference between the algebraic geometric reduction of $E(K)$ and the functor $\mathbb{L} : E(K) \to E(K)/E(K)^{00}$: with the former we obtain a connected component isomorphic to $SO_2(\mathbb{R})$ and an isolated point $(-1, 0)$ (see [3] exercise 3.5, page 104 for details), whereas the image under the functor $\mathbb{L}$ is instead still a nonsingular curve; with the two connected components in bijection and therefore both isomorphic to $SO_2(\mathbb{R})$.

3.3 The split multiplicative reduction case

This is the case of a curve $E : y^2 = x(x+1)(x-\epsilon)$, where $v(\epsilon) > 0$ and $\epsilon > 0$.

The algebraic geometric reduction leads here to a curve with a singularity, more precisely a "real" node, in $(0, 0)$.

We denote by H the group $\left([\epsilon, \frac{1}{\epsilon}), * \; mod \; \epsilon^2\right)$ (the truncation of the multiplicative group by ϵ). Theorem 4.10 of [1] states that the group H/H^{00} is 1-based in $K_{H^{00}} = (K, H^{00}, \dots)$.

By Corollary 1.4 to obtain 1-basedness for G/G^{00} in $K' = (K, G^{00}, \dots)$ from the known case of the "big" multiplicative truncation, it will suffice to show that $K_{H^{00}}$ is interdefinable with K', and to find a definable bijection $f : G/G^{00} \to H/H^{00}$.

We denote by P a point in G and by $P_\sim$ the class in G/G^{00} of which it is a representative. Analogously we denote $x \in H$ and $x_\sim \in H/H^{00}$.

We firstly define a map $f_* : G \to H$ as follows:

$$f_*(P) = \begin{cases} 1 & if \; x_P \geq 1, \\ \left(\frac{1}{x_P}\right) & if \; y_P \geq 0 \wedge x_P < 1, \\ x_P & if \; y_P < 0 \wedge x_P < 1. \end{cases}$$

We prove that f_* induces a well defined map $f : G/G^{00} \to H/H^{00}$ on the quotients, i.e., that given $P_\sim$ the image $f(P_\sim)$ does not change if we change the representative P.

It is convenient to study aside the cases of G^{00} and of $(T_2)_\sim$.

Lemma 3.3. *The map f sends G^{00} to H^{00}.*

Proof. We recall lemma 3.1: $G^{00} = \bigcap_{n\in\omega} \{P| \; \forall T \rhd O, [n]T = A \Rightarrow \ominus T \lhd P \lhd T\} = \bigcap_{n\in\omega} \left\{P| \; v(x_P) < \frac{1}{n}v(\epsilon)\right\}$. And it easy to see that $H^{00} = \bigcap_{n\in\omega} \left\{x| \; \epsilon < x^n < \frac{1}{\epsilon}\right\} = \bigcap_{n\in\omega} \left\{x| \; |v(x)| < \frac{1}{n}v(\epsilon)\right\}$. Thus $f_*(G^{00}) = H^{00}$, and then also $f(G^{00}) = H^{00}$. □

We characterise $(T_2)_\sim$ via the valuation of the projection of its points on the x-axis.

Lemma 3.4. *We have* $(T_2)_\sim = \bigcap_{n\in\omega} \left\{P \in G | v\left(\frac{x_P}{\epsilon} - 1\right) > \frac{1}{n} v\left(\frac{1}{\epsilon}\right)\right\}$.

Proof. By definition $P \in (T_2)_\sim$ if and only if $P \ominus T_2 \in G^{00}$ if and only if $v(P \ominus T_2) < \frac{1}{n} v(\epsilon)$, for all n.

Then $v(x_{P\ominus T_2}) = v\left(\frac{y_P^2}{(x_P-\epsilon)^2} - 1 + \epsilon - x - \epsilon\right) = v\left(\frac{x_P(x_P+1)(x_P-\epsilon)}{(x_P-\epsilon)^2} - 1 - x_P\right) = v\left(\frac{x_P^2+x_P-x_P+\epsilon-x_P^2+x_P\epsilon}{x_P-\epsilon}\right) = v(\epsilon) + v(1+x_P) - v(x_P-\epsilon)$.

Clearly $v(1+x_P) = 0$ and since $P \in (T_2)_\sim$: $v(\epsilon) - v(x-\epsilon) < \frac{1}{n} v(\epsilon)$, for all n. Therefore $-v\left(\frac{x_P}{\epsilon} - 1\right) < \frac{1}{n} v(\epsilon)$, from which we get the conclusion. □

It is now easy to prove the lemma:

Lemma 3.5. *The function f is well defined for $(T_2)_\sim$, i.e., if $P \in (T_2)_\sim$, then $f(P) \cdot f(T_2)^{-1} = H^{00}$.*

Proof. Observe that $f_*(T_2) = \frac{1}{\epsilon}$, and that if $y_P > 0$, then $f_*(P) = \frac{1}{x_P}$. So $f_*(P) f_*(T_2)^{-1} = \frac{\epsilon}{x_P}$. $f_*(P) f_*(T_2)^{-1}$ is in H^{00} if and only if $\frac{1}{n} v(\epsilon) > v(\frac{\epsilon}{x_P}) \geq 0$ for all n; i.e., if $0 \geq v(\frac{x_P}{e}) > \frac{1}{n} v\left(\frac{1}{\epsilon}\right)$ for all n.

On the other hand if $y_P < 0$, then $f_*(P) = x_P$, so $f_*(P) f_*(T_2)^{-1} \in H^{00}$ if and only if $0 \geq v\left(\frac{x_P}{\epsilon}\right) > \frac{1}{n} v\left(\frac{1}{\epsilon}\right)$.

So what we need to prove is that if $P \in (T_2)_\sim$, i.e., $v\left(\frac{x_P}{\epsilon} - 1\right) > \frac{1}{n} v\left(\frac{1}{\epsilon}\right)$ for all n, then $v(\frac{x_P}{\epsilon}) > \frac{1}{n} v(\frac{1}{\epsilon})$ for all n.

This is obvious: suppose not, then $v\left(\frac{x_P}{\epsilon}\right) < 0$, so $v\left(\frac{x_P}{\epsilon} - 1\right) = v\left(\frac{x_P}{\epsilon}\right) < \frac{1}{k} v\left(\frac{1}{\epsilon}\right)$, for some $k \in \omega$, contradicting $P \in (T_2)_\sim$.

□

We want to prove for all the other cases that the map f is well defined.

Theorem 3.6. *The map f is a well defined function $G/G^{00} \to H/H^{00}$.*

Proof. Let $P, Q \in P_\sim$, then $P \ominus Q \in G^{00}$, i.e., $v(x_{P\ominus Q}) < \frac{1}{n} v(\epsilon)$, for all n. Our aim is to prove that $f_*(P) \sim f_*(Q)$: i.e., $f_*(P) f_*(Q)^{-1} \in H^{00}$. Notice that we already proved this for the class of T_2 and for G^{00}, we shall then suppose $P, Q \notin (T_2)_\sim$, and $P, Q \notin G^{00}$, so we have, by convexity of the equivalence relation, $\text{sign}(y_P) = \text{sign}(y_Q)$, $v(x_P) > 0$ and $v(x_Q) > 0$. Moreover

$$(\diamond) \quad v(x_P) < \frac{1}{n_P} v(\epsilon) \text{ and } v(x_Q) < \frac{1}{n_Q} v(\epsilon) \text{ for some } n_P, n_Q \in \mathbb{N}.$$

We make now some observations regarding the choice of $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$.

Due to the symmetry of E with respect to the x-axis there is no harm in supposing $x_Q < x_P$, and $y_P, y_Q > 0$, the other case is analogous. Let us call $f_*(P) f_*(Q)^{-1} = \frac{x_Q}{x_P} = h$.

$$\textit{Observation } 1: \ 0 \leq v(h) < v(\epsilon).$$

Proof: Since we supposed $x_Q < x_P$ we get $0 \leq v(h)$, for the other inequality suppose $v(h) = v(x_Q) - v(x_P) \geq v(\epsilon)$, but $v(x_P) > 0$, so $v(x_Q) \geq v(\epsilon)$, contradicting $(\diamond)$.

We proceed now with the proof that if $v(x_{P\ominus Q}) < \frac{1}{n} v(\epsilon)$ $\forall n$ then $v(\frac{x_Q}{x_P}) = h < \frac{1}{n} v(\epsilon)$ $\forall n$.

Obviously if $v(h) = 0$ we are already done, so let $v(h) > 0$.

Recall that $x_{P\ominus Q} = \frac{(y_P+y_Q)^2}{(x_P-x_Q)^2} - 1 - x_P - x_Q + \epsilon$.

The y_i's are hard to deal with directly, but observe that $(y_P + y_Q)^2 = y_P^2\left(1 + \frac{y_Q}{y_P}\right)^2 = y_P^2\left(1 + \sqrt{\frac{x_Q}{x_P}}\sqrt{\frac{x_Q+1}{x_P+1}}\sqrt{\frac{x_Q-\epsilon}{x_P-\epsilon}}\right)^2$, and, since $x_Q < x_P$, we get $\frac{x_Q+1}{x_P+1} < 1$ and $\frac{x_Q-\epsilon}{x_P-\epsilon} < h$. Thus $(y_P + y_Q)^2 < y_P^2(1 + h)^2 = x_P(x_P + 1)(x_P - \epsilon)(1 + h)^2$.

So $\frac{1}{n}v(\epsilon) > v(x_{P\ominus Q}) \geq (*)$, for all n, where

$$(*) = v\left(\frac{(x_P + 1)(x_P - \epsilon)(1 + h)^2}{x_P(1 - h)^2} - 1 - x_P(1 + h) + \epsilon\right).$$

We shall use $(*)$ to compute $v(h)$.

$$\textit{Observation } 2: \ v\left(\frac{(x_P + 1)(x_P - \epsilon)(1 + h)^2}{x_P(1 - h)^2}\right) = 0.$$

In fact $v\left(\frac{(x_P+1)(x_P-\epsilon)(1+h)^2}{x_P(1-h)^2}\right) = v(x_P + 1) + v(x_P - \epsilon) + 2v(1 + h) - v(x_P) - 2v(1 - h)$. Since $0 < v(x_P) < v(\epsilon)$ and $v(h) > 0$, $v(1 + h) = v(1 - h) = 0$; so $v\left(\frac{(x_P+1)(x_P-\epsilon)(1+h)^2}{x_P(1-h)^2}\right) = 0 + v(x_P) - v(x_P) - 0 = 0$.

This implies that there are two summands with same valuation in $(*)$ (the other one is 1, so to compute $(*)$ we need to expand the whole expression).

Moreover $(*) \geq \min\left\{v\left(\frac{(x_P+1)(x_P-\epsilon)(1+h)^2}{x_P(1-h)^2} - 1 - x_P(1 + h)\right), v(\epsilon)\right\}$.. Since we supposed $(*) < \sup_n\left\{\frac{1}{n}v(\epsilon)\right\}$, clearly $\frac{(x_P+1)(x_P-\epsilon)(1+h)^2}{x_P(1-h)^2} - 1 - x_P(1 + h)$ has to have smaller valuation than $v(\epsilon)$, and we can exclude ϵ from the computation of $(*)$:

$$(*) = v\left(\frac{(x_P + 1)(x_P - \epsilon)(1 + h)^2}{x_P(1 - h)^2} - 1 - x_P(1 + h)\right).$$

This implies $(*) \geq \min\left\{v\left(\frac{(x_P+1)(x_P-\epsilon)(1+h)^2}{x_P(1-h)^2} - 1\right), v(x_P(1 + h))\right\}$. We already observed that $v(x_P(1 + h)) = v(x_P)$. Moreover if the two valuations are different the inequality becomes an equality (this will be the first case in the following two cases). We distinguish two cases:

- $v\left(\frac{(x_P+1)(x_P-\epsilon)(1+h)^2}{x_P(1-h)^2} - 1\right) \neq v(x_P)$.

  Then $(*) = v(x_P^2(1 + h)^2 + 4hx_P - \epsilon(1 + h)^2(1 + x_P)) - v(x_P)$. Clearly $v(\epsilon(1 + h)^2(1 + x_P)) = v(\epsilon)$ is greater than $v(x_P^2(1 + h)^2) = 2v(x_P)$ and $v(4hx_P) = v(x_Q)$.

  Observe that since both $x_P^2(1 + h)^2$ and $4hx_P$ are positive, $v(x_P^2(1 + h)^2 + 4hx_P) = \min\{v(x_P^2(1 + h)^2), v(4hx_P)\}$. So either $(*) = v(x_P^2) - v(x_P) = v(x_P)$, but since $(*) < \frac{1}{n}v(\epsilon)$ for all n, which contradicts $(\diamond)$, or $(*) = v(x_Q) - v(x_P) = v(h)$, in this case $v(h) = (*) < \frac{1}{n}v(\epsilon)$ for all n by the hypothesis, and this concludes the proof of the case.

- $v\left(\frac{(x_P+1)(x_P-\epsilon)(1+h)^2}{x_P(1-h)^2} - 1\right) = v(x_P)$.

Then

$$(*) = v\left(\frac{(x_P+1)(x_P-\epsilon)(1+h)^2}{x_P(1-h)^2} - 1 - x_P(1+h)\right) =$$
$$= v\left(hx_P^2(1+h)(2-h) + 4x_Ph - \epsilon(1+x_P)(1+h)^2\right) - v(x_P).$$

Since $v(hx_P^2(1+h)(2-h)) = v(x_Px_Q)$, $v(4x_Ph) = v(x_Q)$ and $v(\epsilon(1+x_P)(1+h)^2) = v(\epsilon)$, we get $(*) = v(h)$, so $v(h) < \frac{1}{n}v(\epsilon)$ and we have finished the proof.

□

Easy to check now is

Corollary 3.7. *The map f is a bijection.*

Proof. Surjectivity: trivial by construction.

Injectivity: Suppose $f(P_\sim) = f(Q_\sim)$. Choosing the representatives P, Q such that $\text{sign}(y_P) = \text{sign}(y_Q)$ in case P or Q are in $T_2)_\sim$, we have $\left|v\left(\frac{x_Q}{x_P}\right)\right| = v(h) < \frac{1}{n}v(\epsilon)$, for all n.

Now we need to prove that also $|v(x_{P\ominus Q})| < \frac{1}{n}v(\epsilon)$ for all n. We can suppose $x_P > x_Q$, so $0 \leq v(x_{P\ominus Q})$, and, by the choice of the representatives, $(y_P + y_Q)^2 < y_P^2$. So $0 \leq v(x_{P\ominus Q}) \leq (\circ)$, where

$$(\circ) = v\left(\frac{(x_P+1)(x_P-\epsilon)}{x_P(x_P-h)^2} - 1 - x_P(1+h) - \epsilon\right).$$

Thus $0 \leq v(x_{P\ominus Q}) \leq (\circ) = v(-\epsilon(x_P+1) + h(2x_P - hx_P + hx_P^2 - h^2x_P^2) + \epsilon(x_P(1-x_P)^2)) - v(x_P) = v(hx_P) - v(x_P) = v(h) < \frac{1}{n}v(\epsilon)$, for all n. Thus $P \sim Q$, so $P_\sim = Q_\sim$ and f is injective. □

In [1] it is highlighted how the structure $(K, H^{00}, \dots)$ is interdefinable with a nonstandard real closed field K_w, whose valuation is w and that H/H^{00} is a definable subset of Γ_w in K_w. Having found a definable bijection between G/G^{00} and H/H^{00} we get then that G/G^{00} is internal to Γ_w, and Corollary 1.4 implies the following theorem:

Theorem 3.8. *Given an elliptic curve E with split multiplicative reduction, the group G/G^{00} is 1-based in the structure $K' = (K, G^{00}, \dots)$.*

This and the results in chapter 3.1 and 3.2 prove part of theorem 1.8. In the next chapter is proved the remaining part, with the analysis of the truncations.

4 Truncations of elliptic curves

Given an elliptic curve E defined over a saturated real closed field K, we call a group G of the form $([\ominus P, P) \oplus \mod [2]P)$, where $P \in E(K)^0$ and the interval is considered according to the order $\lhd$ of $E(K)$, a *truncation* of $E(K)$.

We shall denote by $Q^*, \lhd^*, \oplus^*, [n]^*$ the points, order, operation and formal multiplication on $E(K)$ respectively and by $Q, \lhd, \oplus, [n]$ those in G.

Our aim is to extend the classification above to truncations of elliptic curves. We shall consider separately the case of E when $E(K)$ has good reduction

and nonsplit multiplicative reduction, and when $E(K)$ has split multiplicative reduction.

We shall prove the following theorem:

Theorem 4.1. *The truncation $G = ([\ominus P, P), \oplus \mod [2]P)$ of the K-points of an elliptic curve E is 1-based if and only if G/G^{00} is internal to the value group determined by G^{00}, and if and only if $E(K)$ has split multiplicative reduction and $v(x_P) > 0$.*

Proof. We shall consider all the possible cases, and therefore get all the implications in the theorem by exhaustion.

Firstly we prove that for the good reduction and nonsplit multiplicative reduction case non-1-basedness is preserved in truncations.

We split into two subcases:

Subcase 1: if the point P defining the truncation is in $E(K)^0 \setminus E(K)^{00}$; and Subcase 2: if it is in $E(K)^{00}$.

1. $G = ([\ominus P, P), \oplus \mod [2]P)$ and $P \notin E(K)^{00}$. Then this implies that $T_n^* \lhd^* P \lhd^* T_{n+1}^*$ (or $T_n^* \rhd^* P \rhd^* T_{n+1}^*$) for some n. We consider the first inequality, the second one is identical. Let T_k be a torsion point of G, then it is easy to see that $x_{T_{kn}^*} < x_{T_k} < x_{T_{k(n+1)}^*}$. So for each torsion point T of G, there are two torsion points of E whose projections on the x-axis bound the projection of T, therefore $G^{00} = E(K)^{00}$. Moreover G/G^{00} is a definable truncation of $E(K)^0/E(K)^{00} = \tilde{E}(\mathbb{R})^0$ in the expansion of K by a predicate for G^{00}, and so it is non-1-based by Corollary 3.7.

2. $G = ([\ominus P, P), \oplus \mod [2]P)$ and $P \in E(K)^{00}$. Clearly then $G^{00} \neq E(K)^{00}$, we show then that G^{00} is still definable in the expansion K' of K by $E(K)^{00}$ and that moreover it is definable in a sort of $(K')^{eq}$ interdefinable with $k_v \cong \mathbb{R}$ in $(K')^{eq}$, this clearly implies non-1-basedness.

   Observe that $v(x_P) < 0$. We firstly want to determine G^{00}.

   We recall that $v(\epsilon) \geq 0$, and that if $S \in G$, then $v(x_S) < 0$. Hence $v\left(x_{[2]S}\right) = v\left(\frac{(x_S^2+\epsilon)^2}{4x_S(x_S+1)(x_S-\epsilon)}\right) = 2v(x_S^2+\epsilon) - v(x_S) - v(x_S) - v(x_S) = v(x_S)$, and we find that $G^{00} = \{S \in G | v(x_S) < v(x_P)\}$.

   We prove now that $S \sim Q$ (i.e., $S \ominus Q \in G^{00}$ if and only if $v(x_S - x_Q) > v(x_P)$ and y_S, y_Q have the same sign (of course also if $S \sim P$ and $Q \sim P$), then we get that G/G^{00} is definable in the sort $B_{\geq v(x_P)}(0)/B_{>v(x_P)}(0) \cong k_v \cong \mathbb{R}$ (by remark 1.5) and therefore that G/G^{00} is internal to the residue field of a real closed valued field and so it is non-1-based by Remark 1.3.

   Observe that for each S, $v(x_S) = v(x_P)$, so it is sufficient to show the following claim holds:

   Claim: $v(x_{S\ominus Q}) < v(x_S)$ if and only if $v(x_S - x_Q) > v(x_S)$, or equivalently $v\left(\frac{x_Q}{x_S} - 1\right) > 0$.

   Proof of the claim: firstly we prove RHS $\Rightarrow$ LHS. We use valuations: $v(x_S \ominus x_Q) = v\left(\frac{(y_Q+y_S)^2}{(x_Q-x_S)^2} - 1 + \epsilon - x_S - x_Q\right)$. After denoting $\frac{x_Q}{x_S} - 1$ by δ and a bit of manipulation we find that it is equal to:

$v\left((x_S+1)(x_S-\epsilon)\left(\frac{y_Q}{y_S}+1\right)^2-(1-\epsilon)x_S\delta^2-x_S^2\delta^2-x_Sx_Q\delta^2\right)-v(x_S)-2v(\delta)$. Now some considerations: $v(x_S)=v(x_Q)$ implies $v(y_S)=v(y_Q)$, therefore $v\left(\frac{y_Q}{y_S}\right)=0$, and since $\text{sign}(y_S)=\text{sign}(y_Q)$ we get $v\left(\frac{y_Q}{y_S}+1\right)=0$; moreover $v(\delta)\geq 0$.

Also: $v(x_S+1)=v(x_S)$, $v(x_S-\epsilon)=v(x_S)$.

We consider separately the parts of the above polynomial:

- $v\left((x_S+1)(x_S-\epsilon)\left(\frac{y_Q}{y_S}+1\right)^2\right)=2v(x_S)$.
- $v\left((1-\epsilon)x_S\delta^2\right)=v(x_S)+2v(\delta)>2v(x_S)$.
- $v\left(x_S^2\delta^2+x_Sx_Q\delta^2\right)=2v(x_S)+2v(\delta)$.

Then $v\left((x_S+1)(x_S-\epsilon)\left(\frac{y_Q}{y_S}+1\right)^2-(1-\epsilon)x_S\delta^2-x_S^2\delta^2-x_Sx_Q\delta^2\right)\geq 2v(x_S)$, so $v(x_{S\ominus Q})\geq 2v(x_S)-v(x_S)-2v(\delta)=v(x_S)-2v(\delta)$. Since we assumed $v(x_{S\ominus Q})<v(x_S)$, we obtain $-v(\delta)<0$, so $v\left(\frac{x_Q}{x_S}-1\right)>0$ and we are done.

For the other direction suppose $v(\delta)>0$, $v(x_{S\ominus Q})=2v(x_S)-v(x_S)-2v(\delta)=v(x_S)-2v(\delta)<v(x_S)=v(x_P)$, so $S\ominus Q\in G^{00}$.

This concludes the proof of the claim and hence of the subcase.

We consider now the case of $E(K)$ with split multiplicative reduction, i.e., E is defined by $y^2=x(x+1)(x-\epsilon)$ where $v(\epsilon)>0$. We have four subcases:

1. If $P\in E(K)^0\setminus E(K)^{00}$, it is analogous to subcase 1 above: we have that $G^{00}=E(K)^{00}$. Let H be the multiplicative truncation $\left([\epsilon,\frac{1}{\epsilon}),*\ mod\ \epsilon^2\right)$. The definable bijection $f: E(K)^0/E(K)^{00}\to H/H^{00}$ of theorem 3.6 restricted to G/G^{00} is then a definable bijection $f': G/G^{00}\to H'/H'^{00}$, where
$$H'=\left(\left[f(P),\frac{1}{f(P)}\right),*\ mod\ f(P)^2\right)$$
is a "big" multiplicative truncation. By Corollary 1.4 G/G^{00} is then 1-based and it is clearly internal to the value group of a real closed valued field.

Therefore f' transfers 1-basedness of H'/H'^{00} to G/G^{00} as in the proof of Theorem 3.8.

2. $P\in E(K)^{00}$ and $v(x_P)<0$. This is identical to subcase 2 above, and the same calcualtion leads to non-1-basedness of G/G^{00}.

3. $P\in E(K)^{00}$ and $v(x_P)>0$. Observe that if $x_S\in G$, and $v(x_S)>0$, then also $v(x_S)<v(\epsilon)$. Then $v\left(x_{[2]S}\right)=v\left(\frac{(x_S^2+\epsilon)^2}{4x_S(x_S+1)(x_S-\epsilon)}\right)=2v(x_S^2+\epsilon)-v(x_S)-0-v(x_S)=2v(x_S)$.

As in the split multiplicative case we shall produce a definable bijection $G/G^{00}\to H/H^{00}$ with $H=\left(\left[x_S,\frac{1}{x_S}\right),*\mod\left(\frac{1}{x_s}\right)^2\right)$ a "big" multiplicative truncation.

We define the map $f_* : G \to H$ as

$$f_*(S) = \begin{cases} 1 & if\ S \in O_\sim, \\ \left(\frac{1}{x_S}\right) & if\ y_S \geq 0, \\ x_S & if\ y_S < 0, \end{cases}$$

Consider the induced map $f : G/G^{00} \to H/H^{00}$. The same calculation that led to Corollary 3.7 gives us that f is a definable bijection. Therefore G/G^{00} inherits 1-basedness from H/H^{00} by Corollary 1.4 and again it is internal to the value group of a real closed valued field.

4. $P \in E(K)^{00}$ and $v(x_P) = 0$. It is again immediate to observe that if $x_S \in G$ and $v(x_S) = 0$, $v\left(x_{[2]S}\right) = 2v(x_S)$. Therefore $G^{00} = \{S \in G | v(x_S) < 0\}$. By the same argument as Subcase 3 we obtain a definable bijection with a multiplicative truncation, though this time it is a "small" one, and therefore G/G^{00} is non-1-based and internal to the residue field of a real closed valued field again by Corollary 1.4.

□

With this last case study we have completed the proof of Theorem 4.1 and therefore of Theorem 1.8.

References

[1] Penazzi, D., One basedness and groups of the form G/G^{00} , *Submitted to Archive for Mathematical Logic*, 2010.

[2] Peterzil, Y.; Starchenko, S., A trichotomy theorem for o-minimal structures, *Proceedings of the London Mathematical Society*, 1998, *Vol. 77(3)*, pp. 481-523.

[3] Silverman, J., The Arithmetic of Elliptic Curves, *Springer Verlag*, 1986.

[4] Pillay, A., Type-Definability, Compact Lie Groups, and o-Minimality, *Journal of Mathematical Logic*, 2004, **Vol 4, issue 2** pp.147-162.

[5] Hrushovski, E.; Peterzil, Y; Pillay, A., Groups, Measures and the NIP, *Journal of the American Mathematical Society*, 2008, *Vol. 21*, pp. 563-596.

[6] Haskell, D; Hrushovski, E.; Macpherson, D., Stable Domination and Independence in Algebraically Closed Valued Fields, *Lecture notes in Logic, Cambridge Press*, 2008.

[7] Pillay, A., Canonical bases in o-minimal and related structures, *To appear in JSL.*

[8] Loveys, J., Peterzil, Y., Linear o-minimal structures, *Israel Journal of Mathematics*, 1993, **Vol 81** pp. 1-30.

[9] Pillay, A., Geometric Stability Theory, *Oxford Logic Guides*, 1996.

[10] Hasson, A.; Onshuus, A., Embedded o-minimal structures, *Bulletin of the London Mathematical Society*, 2010 **Vol. 42(1)**, pp.64-74.

[11] Mellor, T., Imaginaries in real closed valued fields, *Annals of pure and applied logic*, 2006, **Vol. 139, issues 1-3**, pp. 230-279.

[12] Van den Dries, L., Tame Topology and O-minimal Structures, *London Mathematical Society Lecture Note Series 248*, 1998.