Hyperdefinable groups and modularity

Davide Penazzi

Submitted in accordance with the requirements for the degree of

Doctor of Philosophy

The University of Leeds

Department of Pure Mathematics

January 2011

The candidate confirms that the work submitted is his own and that appropriate credit has been given where reference has been made to the work of others.

This copy has been supplied on the understanding that it is copyright material and that no quotation from the thesis may be published without proper acknowledgement.

©2011 The University of Leeds and Davide Penazzi.

Acknowledgements

I would firstly like to thank my supervisor Prof. Anand Pillay, for his kind guidance, his patience and for his generosity in sharing his knowledge. I thank Sarah for having learnt a little of my English and taught me lots of proper English. I am grateful to the logic group in Leeds and to the postgraduates of Level 11, for making me enjoy my time here, in particular Gareth, Lotte and Alex for many chats, mathematical and non, and Sung Ho for making me cook Korean food for him. I would also like to thank Prof. Zambella, that introduced me to Model Thoery, and the examiners Prof. Macpherson and Dr. Tressl, for their useful suggestions. Finally, thanks go to my family and friends who, from far away, supported me.

Abstract

In this thesis is presented a study of groups of the form G/G^{00}, where G is a 1-dimensional, definably compact, definably connected, definable group in a saturated real closed field M, with respect to a notion called 1-basedness.

In particular G will be one of the following:

(1) $([-1,1), + \ mod \ 2)$
(2) $\left(\left[\frac{1}{b}, b\right), \cdot \ mod \ b^2\right)$
(3) $(SO_2(M), *)$ and truncations
(4) $(E(M)^0, \oplus)$ and truncations, where E is an elliptic curve over M,

where a truncation of a linearly or circularly ordered group $(G, *)$ is a group whose underlying set is an interval $[a, b)$ containing the identity of G, and whose operation is $* \ mod \ (b * a^{-1})$.

Such groups G/G^{00} are only hyperdefinable, i.e., quotients of a definable group by a type-definable equivalence relation, in M, and therefore we consider a suitable expansion M' in which G/G^{00} becomes definable.

We obtain that M' is interdefinable with a real closed valued field M_w, and that 1-basedness of G/G^{00} is related to the internality of G/G^{00} to either the residue field or the value group of M_w.

In the case when G is the semialgebraic connected component of the M-points of an elliptic curve E, there is a relation between the internality of G/G^{00} to the residue field or the value group of M_w and the notion of algebraic geometric reduction. Among our results is the following:

If $G = E(M)^0$, the expansion of M by a predicate for G^{00} is interdefinable with a real closed valued field M_w and G/G^{00} is internal to the value group of M_w if and only if E has split multiplicative reduction; G/G^{00} is internal to the residue field of M_w if and only if E has good reduction or nonsplit multiplicative reduction.

Contents

CHAPTER 1

Introduction

1. Assumptions and notation

We assume that the reader is familiar with the basic notions of model theory: saturation, quantifier elimination, the M^{eq} construction.

We also assume a basic knowledge of o-minimality and the theory of valued fields, though we shall recall the main notions throughout the thesis.

We denote a structure by $M = (M, L_M)$, where L_M is the language of the structure M. When we consider the expansion of a structure by a predicate P we often omit part of the language, for example if we expand M by P, we denote the new structure $M' = (M, P, \dots)$, where the dots stand for the language of the original structure.

We denote a single element with a latin letter, e.g. x, whilst a tuple is denoted by an overlined latin letter, e.g., $\overline{x}$.

Unless otherwise stated any definable set is intended definable with parameters.

When there is an ordered set we may use a slightly incorrect notation, by writing, for example, given A a set, b an element and $\alpha = (C, D)$ a cut, $A < b$ to mean $a < b$ for all $a \in A$; $\alpha < b$, to mean $b \in D$; or $\alpha + 1$ to mean the cut (C', D'), where $x \in C' \iff x - 1 \in C$ and $x \in D' \iff x - 1 \in D$.

We say that a structure M is saturated if it is $|M|$-saturated. The existence of such M relies on set theoretical hypotheses that we shall not discuss here.

As is common practice in model theory we shall often identify a formula with the set it defines. Where it is needed more care, we denote the set defined by a formula φ in a structure M by φ^M.

2. Motivation and preliminaries

The main motivations behind the project developed in this thesis are Pillay's conjecture and the extension of geometrical stability theory outside the stable context.

Pillay's conjecture is actually now a theorem, a result of work of several people, to name a few: Pillay, Hrushovski, Peterzil, Otero and Berarducci. In [**28**] it is proved in a special case. The complete proof is in [**11**]. The article [**25**] gives a detailed account of the proof, gathering only the needed theorems from a number of papers. I shall describe this theorem better in the next subsection, but the rough idea is that a definable group G in a saturated real closed field, quotiented by the subgroup of its "infinitesimals", G^{00}, is a real Lie group.

The motivating example is $G = ([-1,1), +\ mod\ 2)$ in a saturated real closed field M. Here, G^{00} is the usual set of infinitesimals and therefore G/G^{00} is $[-1,1)^{\mathbb{R}}$.

This gives rise to a functor $\mathbb{L} : G \to G/G^{00}$ between the categories of definable (definably compact, definably connected) groups and of (compact, connected) Lie groups. How topological and algebraic topological properties are preserved under this functor is now a very active area of study in model theory.

It makes then sense to study on its own the group G/G^{00}, which, as we shall see, is a hyperdefinable set (a quotient of a type-definable set by a type-definable equivalence relation, although in this thesis G will be definable), from a model theoretical and stability theoretical point of view.

The other motivation lies in the context of the trichotomy theorems for certain well behaved definable sets.

Recall that a strongly minimal set is an infinite definable set in a saturated model whose definable subsets are either finite or cofinite, and that, moreover, it eliminates $\exists^{\infty}$. For such sets algebraic closure is a pregeometry, and therefore it defines a notion of dimension.

In the early 80s Zil'ber [**36**] conjectured that given a strongly minimal set X exactly one of the following is true:

- X is trivial: for each set $A \subset X$, $acl(A) = \cup_{a \in A} acl(a)$.
- X is (nontrivial) locally modular: X interprets a strongly minimal infinite group G all of whose definable sets are essentially cosets.
- X interprets a strongly minimal algebraically closed field.

The idea is that strongly minimal sets can be classified up to structural complexity: a strongly minimal set "resembles" either a pure set, or a vector space or a field.

This conjecture turned out to be false in this form; Hrushovski in fact disproved it [**9**] constructing an example of a non-locally modular strongly minimal theory that does not interpret an infinite group.

The conjecture though is true in a smaller class of structures, the Zariski Geometries, as proved by Hrushovski and Zilber in [**10**].

In more recent years part of the machinery developed for stable theories has been extended to wider classes of structures, such as the simple and NIP theories.

A special class of theories introduced by van den Dries, Pillay and Steinhorn in the 80s, and that have been deeply studied by themselves, along with others, is the class of o-minimal theories. There are many analogies between these theories and the strongly minimal ones, in particular algebraic closure is a pregeometry, and they have elimination of $\exists^{\infty}$. Both then are geometric structures and admit a notion of dimension.

It was then natural to ask if it was possible to obtain a trichotomy theorem also for these structures. A positive answer to this question has been given by Peterzil and Starchenko in [**23**]. Their theorem roughly says that if M is o-minimal and sufficiently saturated, and $a \in M$, then either

(1) a is trivial, or

(2) a has a convex neighbourhood on which M induces the structure of an ordered vector space, or
(3) a is contained in an open interval on which M induces the structure of an expansion of a real closed field.

The first two points (triviality and local modularity) can be expressed in terms of dimension of interpretable curves. We recall that a definable (or interpretable) family of curves $\{C_{\overline{u}}, \overline{u} \in U\}$, where U is interpretable, is normal if for $\overline{u} \neq \overline{v}$, $C_{\overline{u}}$ and $C_{\overline{v}}$ intersect in at most finitely many points; the family of curves is of dimension n if $dim(U) = n$. Triviality has a technical definition, and we will not discuss it here, since it plays no role in this thesis.

For an o-minimal structure M, Peterzil and Starchenko proved that if $a \in M$ is non-trivial, then a has a convex neighbourhood on which M induces the structure of an ordered vector space if and only if there is an open interval I containing a such that every interpretable normal family of definable curves in I^n is of dimension at most 1. Moreover a is contained in an open interval on which M induces the structure of an expansion of a real closed field if and only if given any interval I containing a, there is an interpretable normal family of curves of dimension > 1.

So, for o-minimal structures, the behaviour (2) can be seen as a property of certain families of curves; when for all elements a of the structure we have (2), we say that the structure is locally modular. Moreover, the property that every interpretable normal family of definable curves in I^n is of dimension at most 1 is equivalent to a property called 1-basedness, defined in [**29**] (or CF-property, in [**18**]), which will be described in Chapter 2. 1-basedness is the notion that seems more convenient rather than modularity because it is easier to check in computations and therefore it is the one that will be used throughout the thesis.

We recall the basic examples of structures that fit into the classification in the article of Peterzil and Starchenko:

(1) Trivial: e.g. $(\mathbb{Q}, <)$.
(2) Locally modular/ 1-based: e.g. $(\mathbb{R}, +, 0, <)$.
(3) Non-1-based: e.g. $(\mathbb{R}, +, \cdot, 0, 1, <)$.

A natural question that can then be asked is the following: given a saturated real closed field, is it possible to find a modular/1-based or a trivial hyperdefinable set?

We firstly would like to point out that the question above is ill-posed: a hyperdefinable set is not definable in the real closed field, and we need to modify the notions of 1-basedness and triviality to adapt them to this context.

A possible example comes from the behaviour of certain groups of the form G/G^{00}. In particular, if we consider the group G of points of an elliptic curve and we quotient it by G^{00}, we always obtain a Lie group. On the other hand there is an algebraic notion of reduction over the reals, which in certain cases does not behave well, in the sense that the reduced curve is no longer an elliptic curve (in this case we say that the elliptic curve has bad reduction). Such "strange" hyperdefinable groups seemed a good candidate for a 1-based hyperdefinable set.

In this thesis we try to answer a refined version of the question above and study the hyperdefinable groups of the form G/G^{00} in an expansion of a real closed field where they become definable; we then define what we mean by 1-basedness in this context, together with a suitable construction that allows us to consider the theory of G/G^{00} with all the induced structure from this expansion of a real closed field.

We consider a set of examples of 1-dimensional, definably compact, definably connected, definable groups G in a saturated real closed field M:

List A:

(1) $([-1, 1), + \ mod\ 2)$, additive truncation.
(2) $\left(\left[\frac{1}{b}, b\right), \cdot \ mod\ b^2\right)$, multiplicative truncation.
(3) $(SO_2(M), *)$ and truncations.

(4) $(E(M)^0, \oplus)$ and truncations, where E is an elliptic curve over M.

For 1-dimensional, definably compact, definably connected definable groups there is a classification over the reals, due to Madden and Stanton [**20**], see Theorem 1.11 in the next subsection. We conjecture a similar classification for such groups defined over real closed fields obtaining List A.

We shall analyse case by case the groups G/G^{00} and find that indeed there are hyperdefinable groups that are 1-based, even non elliptic curves, and the behaviour of elliptic curves turns out to be not exactly as expected: there is a relation between reduction and 1-basedness, but some curves which have bad reduction are non-1-based; see the theorem in the abstract.

This analysis of groups of the form G/G^{00} is, moreover, strongly linked with the theory of real closed valued fields; in particular, G/G^{00} is 1-based in a sufficiently enriched structure if G/G^{00} is internal to the value group of a real closed valued field interpretable in it. On the other hand, G/G^{00} is non-1-based if and only if it is internal to the residue field in the enriched structure.

A complete formulation of the main theorem, highlighting all the links described, which considers all the cases of List A can be found at the end of Chapter 4.

3. Groups definable in o-minimal structures

We explain here what 1-dimensional, definably connected, definably compact, definable groups in a saturated real closed field are. Then we state Pillay's conjecture, and the Madden and Stanton classification for 1-dimensional Nash groups over the reals.

We conclude this section with a lemma motivating our expectation of a classification similar to that of Madden and Stanton for 1-dimensional, definably connected, definably compact, definable groups in a saturated real closed field.

For the rest of this subsection M will be a totally ordered, o-minimal and saturated expanson of a real closed field, but many of the following results are true in a more general setting. Here we will not recall the notion of o-minimality, but its definition, generalized to the context of definable sets, can be found in Chapter 2.

A definable group $(G, *)$ in M is a group with definable underlying set $G \subset M^n$, and whose operations $* : G \times G \to G$ and $^{-1} : G \to G$ have definable graphs.

For a definable group we define the following subgroups:

Definition 1.1. Given a set $A \subset G$ of parameters, we define G^0_A as the smallest A-definable subgroup of finite index, if any. If for each $A, B \subset G$ we have $G^0_A = G^0_B$, then G^0 is $\emptyset$-definable and we say that G^0 exists.

Given a set $A \subset G$ of parameters, we define G^{00}_A as the smallest subgroup of bounded index type-definable with parameters from A. If for each $A, B \subset G$ we have $G^{00}_A = G^{00}_B$, then G^{00} is $\emptyset$-definable and we say that G^{00} exists.

When the structure in which G is defined is o-minimal, both G^0 and G^{00} exist, and G^0 is a finite index definable subgroup.

We shall consider groups definable in saturated models, but no such group can be compact with the usual o-minimal topology. The analogy of compactness for infinite groups in saturated o-minimal structures is the following, introduced by Peterzil and Steinhorn in [**24**]:

Definition 1.2. G is *definably compact* if, given an interval $I = [a, b)$ in M and a definable, continuous function $f : I \to G$, then $\lim_{a \to b} f(x)$ exists in G.

If M is an o-minimal expansion of a real closed field then a definably compact group is definably isomorphic to a closed and bounded definable group G such that the t-topology of G coincides with the topology inherited from the ambient space M^n.

Also a notion corresponding to connectedness can be defined:

DEFINITION 1.3. G is *definably connected* if there are no proper definable subgroups of finite index.

From [**26**] definable connectedness is equivalent to G not being the disjoint union of two non-empty definable t-open subsets, where the t-topology is the topology induced on a definable manifold explained below.

The o-minimal theories carry a notion of dimension, on which more details can be found in [**35**].

DEFINITION 1.4. Given a definable set X,

$$dim(X) = max\{i_1 + \cdots + i_m | \ X \ contains \ an \ (i_1, \cdots, i_m) - cell\}.$$

Here an $(i_1, \cdots, i_m) - cell$ is defined inductively by:

(1) A $(0) - cell$ is a point $x \in M$, a $(1) - cell$ is an interval $(a, b) \in M$.
(2) Suppose $(i_1, \ldots, i_m)-cells$ are already defined; then an $(i_1, \ldots, i_m, 0)-cell$ is the graph of a definable continuous function $f : Y \to M$, where Y is an $(i_1, \ldots, i_m)$-cell; further an $(i_1, \ldots, i_m, 1) - cell$ is a set $(f, g)_Y$ (i.e., the set of points $(\overline{x}, y)$, $\overline{x} \in Y$, $f(\overline{x}) < y < g(\overline{x})$), where f, g are definable continuous functions $f, g : Y \to M$, $f < g$ and Y is a $(i_1, \ldots, i_m) - cell.$

We say that a definable group G is n-dimensional if its underlying set is n-dimensional.

3.1. The definable manifold structure. In [**26**] Pillay proved that a group definable in an o-minimal structure can be equipped with the structure of a *definable manifold* where the group operation and the inverse become continuous. Here we present a brief survey and recall Pillay's conjecture, stated in [**28**] and completely proved in [**11**].

DEFINITION 1.5. Given a set X equipped with a topology τ, a *definable atlas* is a **finite** collection of open subsets $\{(U_1, \psi_1), (U_2, \psi_2), \ldots, (U_n, \psi_n)\}$ such that for each U_j there is a bijective homeomorphism $\psi_j : U_j \to V_j$, where V_j is a definable open subset of M^{n_j}, and whenever $U_j \cap U_k \neq \emptyset$ then the map $\psi_j \circ \psi_k^{-1}$ is a definable bijective homeomorphism $\psi_k(U_j \cap U_k) \to \psi_j(U_j \cap U_k)$.

Two definable atlases are *compatible* if their union is a definable atlas. For fixed X, compatibility of definable atlases is an equivalence relation.

We call $n = sup\{n_j | j < n\}$ the *dimension* of the atlas.

A *definable manifold* of dimension n is a definable set X with an equivalence class of definable atlases of dimension n.

A definable manifold has an induced topology, called the *t-topology*: $Y \subset X$ is open if and only if each $\psi_i(Y \cap U_i)$ is open in M^n.

The main result in [**26**] is the following:

FACT 1.6. *When M is an o-minimal structure, a group G definable in M can be given the structure of a definable manifold over M in which multiplication and inverse are continuous operations with respect to the t-topology.*

OBSERVATION 1.7. This result is obtained by finding a large $\emptyset$-definable subset V of G for which the above holds, where "large" means that $dim(G \setminus V) < dim(G)$. By Lemma 2.4 of [**26**], finitely many translates of V cover G, and we can therefore "patch" them to obtain the manifold structure on all G.

REMARK 1.8. G is isomorphic to a definable affine group with continuous operations in M^n, i.e., a group in which the topology is induced by the topology of M.

This is obtained applying the o-minimal version of Robson's embedding theorem, Thm. 1.8 pag. 159 of [VdD] to the observation above.

We state now the final formulation of Pillay's conjecture, as it appears in [**28**], where it is proved for 1-dimensional G, and for abelian G; the conjecture has been proved in full generality in [**11**].

THEOREM 1.9. *[Pillay's conjecture] Given G a definably connected definable group in M, then*

1. *G has a smallest type-definable subgroup of bounded index G^{00}.*
2. *G/G^{00} is a compact connected real 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.*

Here by Lie group dimension we mean the real manifold dimension of the underlying Lie group, i.e. n, where G is locally homeomorphic to a Euclidean n-space.

An important point is that the logic topology is a topology on bounded hyperdefinable sets, whose closed sets are subsets of the hyperdefinable set whose preimage is type-definable. For an accurate definition see Definition 2.1. Pillay's conjecture implies that the logic topology on G/G^{00} as a hyperdefinable group agrees with the o-minimal topology of G/G^{00} as definable group in a suitable expansion of the original structure. We defer a detailed explanation of this sentence to Chapter 2.

3.2. Nash manifolds. Recall that a *semialgebraic subset* of M^n is a finite union of sets of the form $\{x \in M^n : f_1(x) = 0, \ldots, f_k(x) = 0; g_1(x) > 0, \ldots, g_r(x) > 0\}$, where $f_1, \ldots, f_n, g_1, \ldots, g_r$ are polynomial functions defined over M.

A *semialgebraic function* is a function whose graph is a semialgebaic set.

A *Nash function* is a function from an open semialgebraic subset U of M^n to M, which is at once semialgebraic and C^∞.

Given a semialgebraic subset N of M^n, a *Nash chart* is a Nash function that is a homeomorphism $\psi : U \to S$, where $U \subset N$ and $S \subset M^n$ are open. Two Nash charts ψ_i, ψ_j, with domain U_i, U_j respectively, are *Nash compatible* if

$\psi_i(U_i \cap U_j)$ is semialgebraic and

$$\psi_j \circ \psi_i^{-1} : \psi_i(U_i \cap U_j) \to \psi_j(U_i \cap U_j)$$

is a Nash diffeomorphism. The maps $\psi_j \circ \psi_i^{-1} : S_i \to S_j$ are called *transition maps.*

A locally Nash atlas on N is a set of Nash compatible charts whose domains cover N. We then call N equipped with such atlas a *locally Nash manifold.* If the above atlas has finitely many charts we call N a *Nash Manifold.*

Given a Nash manifold N with atlas $\{\psi_i\}_{i<k}$, its dimension is

$$dim(N) = sup_{i<k}\{n|\psi_i(U_i) \text{ is open in } M^n\}.$$

A group is a *Nash Group* if its underlying set is a Nash manifold, and its multiplication and inverse are Nash functions.

Observation 1.10. Given a definable group G in a real closed field, we know that a definable function f over a semialgebraic set S is semialgebraic, by Tarski's theorem of quantifier elimination. Moreover, a real closed field admits smooth (or C^∞)) cell decomposition, by [**15**], therefore there is a large subset S' of S over which f is smooth, i.e., the partial derivatives of any order are defined. We can then choose the large set V in Observation 1.7 (and indeed in the proof of Proposition 2.5 of [**26**]) to be a large smooth subset of S', so that multiplication and inversion are smooth (and of course semialgebraic) functions on G. This implies that G can be definably equipped with the structure of a Nash group.

3.3. Madden Stanton theorem. We sketch the proof of the Madden and Stanton classification as proved in [**20**]:

Theorem 1.11 (List B:). *Every connected* 1*-dimensional real Nash group is isomorphic as a Nash group (equivalently, definably isomorphic as a definable group) to one of the following:*

(1) $(\mathbb{R}, +)$

(2) $(\mathbb{R}^{>0}, \cdot)$

(3) $([-1, 1), + \ mod\ 2)$

(4) $\left(\left[\frac{1}{b}, b\right), \cdot \ mod\ b^2\right)$

(5) $(SO_2(\mathbb{R}), *)$ *and truncations*

(6) $(E(\mathbb{R})^0, \oplus)$ *and truncations,*

where $E(\mathbb{R})^0$ *is the semialgebraic connected component of the group of* $\mathbb{R}$*-points of an elliptic curve* E.

A *truncation* of a group with a linear order (maybe obtained from a circular one by fixing a point) $(\hat{G}, *, <)$ is a group G whose underlying set is an interval $[a, b)$ containing the identity of $\hat{G}$ and whose operation is $a \cdot b = a * b\ mod\ (b * a^{-1})$. If $\hat{G}$ is a Nash group then also G is a Nash group, but it is not necessarily definably isomorphic to $\hat{G}$.

It is a well known fact that the only simply connected (with trivial fundamental group) real Lie Group is $(\mathbb{R}, +)$.

This is unique up to isomorphism in the category of Lie groups. For example $(\mathbb{R}, \cdot)$ is isomorphic to $(\mathbb{R}, +)$ via the function *exp*. But clearly the function *exp* is not semialgebraic, so in the category of Nash groups $(\mathbb{R}, +)$ and $(\mathbb{R}, \cdot)$ are different objects. The classification of Madden and Stanton produces a classification of one-dimensional, connected, Nash groups up to isomorphism in this category.

We can limit our attention to to a classification of the maps sending $(\mathbb{R}, +)$ onto Nash groups.

In [**20**] the approach is somewhat local: it is proved that the translates of a given single Nash chart on any neighbourhood of the identity of G satisfying certain algebraicity conditions produce a locally Nash atlas on the group.

More precisely: suppose that there is a map $\varphi : U \to S$, where $U \subset G$ is a neighbourhood of the identity and $S \subset \mathbb{R}$ is semialgebraic such that φ is analytic, the image by φ of the graph of the multiplication of elements of U is semialgebraic, and such that for each $g \in G$ there is a neighbourhood $U_g \subseteq U$ such that conjugation by g restricted to U_g: $(h, g^{-1}hg)$ has semialgebraic image by ψ. Then ψ and its translates determine a locally Nash group atlas on G.

Observe that if G is abelian or connected, the conjugation hypothesis can be dropped.

In our case, with $(\mathbb{R}, +)$, we observe that if a function φ is as above, after complexification it satisfies the *algebraic addition theorem*: given a domain $D \subset \mathbb{C}$ there is a nonzero polynomial $G(X, Y, Z)$ with complex coefficients (in fact in this case they will be real), such that $G(\varphi(x), \varphi(y), \varphi(x + y)) = 0$ whenever $x, y, x + y \in D$.

This is the hypothesis for the Weierstrass theorem: we are given $\varphi(u)$ holomorphic in a connected open set containing the origin and satisfying the algebraic addition theorem. Let Φ be the complete analytic function determined by $\varphi(u)$. Then one of the following holds:

(1) Φ is algebraic over $\mathbb{C}(z)$.
(2) Φ is algebraic over $\mathbb{C}(exp(\alpha z))$, for some $\alpha \in \mathbb{C}$.
(3) Φ is algebraic over $\mathbb{C}(\wp(z))$ for some Weierstrass $\wp$-function.

The Weierstrass theorem is applied to $(\mathbb{R}, +)$. It is possible since, given a locally Nash structure on $(\mathbb{R}, +)$, $+$ is a locally Nash map. Moreover, if we have a Nash chart $\varphi : U \to \mathbb{R}$, where U is a neighbourhood of the identity, we can find an open V which still contains the identity, such that $\varphi(V) \subset \mathbb{R}$ is semialgebraic, and $V + V \subset U$. Then also the graph of $(\varphi(x), \varphi(y)) \mapsto \varphi(x+y)$, contained in $\varphi(U) \times \varphi(U) \times \varphi(U)$, is semialgebraic. So the required conditions are satisfied.

After some consideration on these maps, and the fact that we are working on the reals and not on the complex numbers we find that the 1-dimensional locally Nash groups are: $(\mathbb{R}, +)$, $(\mathbb{R}, \cdot)$, $([0, 1), + \ mod\ 1)$, $([1, 2), \times\ mod\ 2)$, $(SO_2(\mathbb{R}), *)$, $(E_\wp, \oplus)$, where $E_\wp$ is the elliptic curve satisfied by the Weierstrass $\wp$ function. Observe that, apart from the first two, these groups are Nash.

Actually Madden and Stanton classify such groups further, defining an equivalence relation between two Nash groups obtained from $(\mathbb{R}, +)$, with charts φ, ψ if the graph (φ, ψ) is semialgbraic. However, for our purposes this is not needed.

It is worth observing that then $(\mathbb{R}, +)$ is the universal cover of all groups from List B, via the identity map, the exponential map, the trigonometric functions Sin and Cos, or the Weierstrass $\wp$ functions.

In this thesis it is conjectured that a similar result is true for definable, definably connected, definably compact 1-dimensional groups over a real closed field, namely:

CONJECTURE 1.12. *[List A] A definable, definably connected, definably compact,* 1*-dimensional group over a real closed field* M *is, up to definable isomorphism of definable groups, one of the following:*

(1) $([-1, 1), + \ mod \ 2)$
(2) $\left(\left[\frac{1}{b}, b\right), \cdot \ mod \ b^2\right)$
(3) $(SO_2(M), *)$ *and truncations*
(4) $(E(M)^0, \oplus)$ *and truncations.*

In this thesis we proceed with an analysis of the groups in List A. If Conjecture 1.12 is true, then ours will be a complete analysis of 1-dimensional, definably compact, definably connected, definable groups in a saturated real closed field.

Conjecture 1.12 is interesting in its own right, and could be a topic for future research.

One possible approach is to generalize the proof of Madden and Stanton to the real closed fields, but this involves obtaining results such as the Weierstrass theorem in a nonstandard context.

A different approach to prove Conjecture 1.12 is to prove a "uniformly definable version" of Theorem 1.11, i.e. to prove that if the 1-dimensional connected

Nash groups vary in a definable family then the definable homomorphism with groups from List B can also be found within a definable family.

The equivalence of this latter version of Theorem 1.11 and Conjecture 1.12 follows easily from a compactness argument. It is therefore requires only a strengthening of the proof in the real case in place of the generalization of analytic results used in the proof of Theorem 1.11 to nonstandard fields.

4. Valued fields

Fundamental to this thesis are valued fields. These will be used both as a tool in calculations and to determine structural properties of groups of the form G/G^{00}. We shall therefore recall the definition of a real closed valued field and state its main properties.

Given a field K and an ordered abelian group Γ, a *valuation* is a surjective map $w : K \to \Gamma \cup \{\infty\}$ satisfying the following axioms: for all $x, y \in K$

(1) $w(x) = \infty \iff x = 0$
(2) $w(xy) = w(x) + w(y)$
(3) $w(x - y) \geq min\{w(x), w(y)\}$

We easily obtain the following consequences:

- $w(1) = 0$
- $w(x) = w(-x)$
- $w(x^{-1}) = -w(x)$
- if $w(x) \neq w(y)$ then $w(x + y) = min\{w(x), w(y)\}$
- If K is an ordered field with convex valuation and $sign(x) = sign(y)$, then $w(x + y) = min\{w(x), w(y)\}$

We call the structure $K_w = (K, L_K, \Gamma, L_\Gamma, w, \infty)$, where L_K is the signature in the language of ordered rings, L_Γ the signature of ordered abelian groups, a *valued field* with signature L_w.

We call Γ the *value group*.

We define the *valuation ring* of v: $R_w = \{x \in K | w(a) \geq 0\}$; this is a local ring, and its unique maximal ideal is $I_w : \{x \in K | w(a) > 0\}$, called the *valuation ideal.* Observe that with this definition we can define the value group via $\Gamma = K/(R_w \setminus I_w)$; we denote it by Γ_w to emphasize the valuation.

The *residue field* is $k_w = R_w/I_w$.

From now on we suppose the field K is real closed, and the valuation ring R_w is convex; K_w is then called a *real closed valued field.*

Remark: in a real closed valued field K_w, Γ_w is divisible. To see this let $\gamma \in \Gamma_w$, then there exists $x \in K$ positive, with $w(x) = \gamma$, but by real closedness there exists y such that $y^n = x$, so $nw(y) = x$.

Cherlin and Dickmann (see [**5**]) proved quantifier elimination for real closed valued fields in the language above:

THEOREM 1.13. *The theory of a real closed valued field K_w in the language L_{K_w} is complete and admits quantifier elimination.*

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

REMARK 1.14. 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 $w(u) = \gamma$, is well defined in the quotients, thus $B_{\geq\gamma}(0)/B_{>\gamma}(0) \to B_{\geq 0_{\Gamma_w}}(0)/B_{>0_{\Gamma_w}}(0) = k_w$ is a field isomorphism.

4.1. Standard valuation and standard part map. The most commonly used valuation on a real closed valued field K extending the reals is the *standard valuation.* The standard valuation ring is Fin: the convex hull of $\mathbb{Q}$ in K; the maximal ideal is the infinitesimal neighbourhood of 0:

$\mu = \bigcap_{i\in\omega} \left\{x \in K | -\frac{1}{n} < x < \frac{1}{n}\right\}$; we denote the standard valuation by v, and the standard real closed valued field by K_v. The value group is then $\Gamma_v = K/(Fin \setminus \mu)$ and the residue field is $k_v = Fin/\mu$.

The *standard part map* $st : Fin \to \mathbb{R}$ is then defined by $st(x) = y$ where y is the only element of $\mathbb{R}$ such that $v(x - y) > 0$.

We can identify $\mathbb{R}$ with k_v and the residue map $Fin \to k_v$ with the standard part map.

Clearly $\mu = ker(st)$ and $st(Fin) = \mathbb{R}$.

CHAPTER 2

Fundamental notions

In this chapter we shall recall some general facts about the logic topology on a bounded hyperdefinable set, as developed in [**28**], and generalize them to a wider class of sets, namely the bounded ind-hyperdefinable sets. We give some details of proofs of known results when the old proofs are sketchy. In Section 2 we define the Shelah expansion of a structure and the version of o-minimality localized to definable sets and related notions. In Section 3 we introduce the localized version of 1-basedness for o-minimal stably embedded sets and prove some results for value groups and residue fields of a real closed valued field. In this Chapter we restrict our attention to countable theories, and we shall always denote by M a saturated model.

1. The Logic Topology

The results below for the hyperdefinable sets are from [**28**]. We generalize them to ind-hyperdefinable sets, inspired by Chapter 6 of [**11**]. The generalization to ind-hyperdefinable sets is used mainly in Chapter 5 but, for reasons of readability, it is presented here.

Given a theory T and a saturated model M, a *type-definable set* (over A, $|A| < |M|$) is a set that is the realization in M of a collection of $< |M|$ formulas (with parameters from A).

Analogously, given a saturated model M and a type definable set $X \subseteq M^n$, we say that an equivalence relation $E \subset X \times X$ is *type-definable* if its graph is a type-definable subset of $X \times X$. In this case the quotient X/E is called a *hyperdefinable set* in M. If, moreover, E is a bounded equivalence relation, i.e., $|X/E| < |M|$, we say that X/E is a *bounded hyperdefinable set.*

A basic fact is that a hyperdefinable set X/E in a saturated model M is bounded if and only if there is a submodel $M_0 \prec M$ such that both X and E are defined (type-defined) over M_0 and such that whenever $M_0 \prec M_1$ for some model M_1, we have $\left|(X/E)^{M_0}\right| = \left|(X/E)^{M_1}\right|$.

Therefore for a bounded equivalence relation we have that, given $M' \succ M$, X' the realization in M' of the formula defining X, and E' the equivalence relation defined by the same type as E, the canonical injection $i : X/E \to X'/E'$ given by $i(a/E) = a/E'$ is a bijection.

We denote by $\pi : X \to X/E$ the canonical projection.

DEFINITION 2.1. Let X/E be a bounded hyperdefinable set of a structure M. We call a subset Y of X/E *closed* if $\pi^{-1}(Y)$ is type-definable in M.

These sets induce a topology on X/E called the *logic topology*.

We recall now the main lemma concerning the logic topology, with the proof, since we refer to it when proving Theorem 2.6. The first part is due to Pillay in [**28**], the moreover part is obtained as an easy consequence of results in [**3**].

LEMMA 2.2. *The bounded hyperdefinable set X/E equipped with the logic topology is a compact Hausdorff space. If, moreover, E is defined by a countable number of formulae, X/E is separable.*

PROOF. Compactness: We have to prove that for every family $\mathcal{F}$ of closed sets with the finite intersection property (FIP) we have $\bigcap \mathcal{F} \neq \emptyset$.

Since the number of classes is bounded we can give an enumeration $z_\alpha, \alpha < \lambda$ of the elements of $\mathcal{F}$; let $Z_\alpha = \pi^{-1}(z_\alpha)$, and let Φ_α be the type defining Z_α. The FIP says that $\bigcup_{\alpha<\gamma} \Phi_\alpha$ is finitely satisfiable, but by saturation it is satisfiable. Let $x \in \bigcap Z_\alpha$; thus we easily see that $\pi(x)$ is the witness we are looking for. In fact, suppose that there exists $y \in X$ such that $E(x, y)$ but $y \notin \bigcap Z_\alpha$, so, for some j, $y \notin Z_j$; this contradicts $E(x, y)$ by the way in which the Z_α are defined.

Hausdorff: Consider $\overline{y}, \overline{z} \in X/E$, $\overline{y} \neq \overline{z}$. We want to find two open disjoint neighborhoods, i.e., two sets such that the inverse projections of their complements are type-definable in X.

Let y, z be representatives of $\overline{y}, \overline{z}$ respectively. Since $\overline{y} \neq \overline{z}$, we have $\neg E(y, z)$, thus, by compactness, there is a formula φ such that $\varphi(y)$ and $\neg\varphi(z)$, and also $\overline{y} \subset \varphi(x)$ and $\overline{z} \subset \neg\varphi(x)$. Consider then $Y = \varphi(x)$ and $Z = \neg\varphi(x)$. These sets are definable in X, disjoint, they partition X, and $\pi^{-1}(y) \subseteq Y$, $\pi^{-1}(z) \subseteq Z$. The projection of this set does not respect the equivalence relation, so there could be a class with elements both in Y and in Z (and in fact there is such a class by compactness of X/E), so we have to refine these sets somewhat. Consider now $\overline{Z} = \{x \in X | \exists t \in Z, E(x, t)\}$: the closure of Z via E. Analogously, consider $\overline{Y}$.

Now $\pi(\overline{Y})$ and $\pi(\overline{Z})$ are closed in X/E, since $\overline{Y}$ and $\overline{Z}$ are type-definable by compactness, with $\overline{y} \in \pi(\overline{Y})$ and $\overline{z} \in \pi(\overline{Z})$. Those two sets are overlapping and cover X/E, so on taking the complements we get two open sets $\pi(\overline{Y})^c$ and $\pi(\overline{Z})^c$, with $\overline{y} \in \pi(\overline{Z})^c$ and $\overline{z} \in \pi(\overline{Y})^c$.

Separability: We shall prove that X/E is second countable (i.e., has a countable basis), this will imply that it is separable (i.e., it contains a countable dense subset).

Remark 1.6 from [**3**] states: If $M_0 \models T$, X definable over M_0, E type-definable over M_0, then the space X/E has a basis of cardinality of at most $|M_0| + |L|$, where L is the language of M.

Since E is defined by countably many formulae, only countably many parameters (a_i) appear in its definition. We then consider $X \subseteq M$ definable in M with (finitely many) parameters (b_j). Let M_0 be the model of T which contains $(a_i), (b_j)$; by the Lowenheim-Skolem theorem it can be chosen to be of countable cardinality. We apply now Remark 1.6 of [**3**] to get a countable basis. Hence X/E is second countable, and therefore separable. □

We now present some results obtained by considering an *ind*-definable set $\tilde{X}$. These are inspired by Remark 7.6 of [**11**], where it is asked which one is the right definition for an ind-hyperdefinable set. But firstly we must clarify what we mean by a "type-definable equivalence relation" in this context.

DEFINITION 2.3. Let $M \vDash T$, let $X_0 \subset X_1 \subset X_2 \subset \dots$ be a chain of definable subsets of M and let $\tilde{X} = \bigcup_{i\in\omega} X_i$. If a set $\tilde{X}$ can be defined in this way, we call it an *ind-definable* set. We say that $E \subseteq \tilde{X} \times \tilde{X}$ is a *type-definable equivalence relation* on $\tilde{X}$ if it is an equivalence relation, for each $n \in \omega$, $E \restriction (X_n \times X_n)$ is type-definable, and for each $i \in \omega$ there exists $j \in \omega$ such that all the classes whose intersection with X_i is nonempty are contained in X_j. In this case $\tilde{X}/E$ is called an *ind-hyperdefinable set.* Analogous to the bounded hyperdefinable sets, we call $\tilde{X}/E$ a *bounded ind-hyperdefinable set* if $E \restriction (X_n \times X_n)$ has a bounded number of classes for each n.

REMARK 2.4. Definition 2.3 is the one required for Remark 7.6 in [**11**].

Again we denote by $\pi : \tilde{X} \to \tilde{X}/E$ the canonical projection.

The logic topology on a bounded ind-hyperdefinable set $\tilde{X}/E$ is defined by: $Y \subseteq \tilde{X}/E$ is closed if $\pi^{-1}(Y) \cup X_n$ is type-definable for all $n \in \omega$.

It is clearly a topology: in fact, for each $i \in \omega$, $\pi^{-1}(\emptyset) \restriction X_i$ is defined by $x \neq x$; and $\pi^{-1}(\tilde{X}/E) \restriction X_i$ is defined by the formula defining X_i. Given two closed sets Y, Z, their preimages are type-defined in each X_i by $(\varphi^i_\alpha)_{\alpha<\lambda}$ and $(\psi^i_\beta)_{\beta<\mu}$, so $\pi^{-1}(Z \cup Y) \restriction X_i$ is defined by $\bigwedge(\varphi^i_\alpha \cup \psi^i_\lambda)$. Given a family of closed sets $\mathcal{F}$, each $C \in \mathcal{F}$ has preimage restricted to i defined by a type, and by boundedness we have $< |M|$ closed sets in $\mathcal{F}$, so $\pi^{-1}(\mathcal{F}) \restriction X_i$ is defined by a type, and hence $\mathcal{F}$ is closed.

Observe moreover that $\tilde{X}/E$ is the topological union of the $X_n/E \restriction (X_n \times X_n)$.

In [**11**] it is observed the following Fact:

FACT 2.5. *A subset of $\tilde{X}/E$ is compact if and only if its preimage is type-definable and contained in X_i for some i.*

THEOREM 2.6. *A bounded ind-hyperdefinable set $\tilde{X}/E$ with the logic topology is a locally compact Hausdorff space.*

PROOF. Take a point $c \in \tilde{X}/E$, the aim is to find a compact neighbourhood of it, i.e., by Fact 2.5 a neighbourhood of c whose preimage is type-definable and contained in X_i for some i.

First, note that $\pi^{-1}(c)$ is contained in X_i for some i.

Then consider the set O of the classes completely contained in X_i, i.e., the set such that:

$$\pi^{-1}(O) = \left\{ x \in \tilde{X} | \neg \exists t (\neg X_i(t)) \wedge E(x,t) \right\}.$$

O is an open set in the logic topology being the complement of a closed set (or we can easily see that its preimage is ind-definable using saturation).

Analogously, we can find a closed set C of all classes meeting X_i, i.e., a set such that:

$$\pi^{-1}(C) = \{x \in \tilde{X} | (\exists t X_i(t) \wedge E(x,t))\}.$$

C is closed by saturation of the structure. Moreover, C is contained in X_j for some $j \geq i$, by the definition of an ind-hyperdefinable set, and is therefore compact.

This C contains O, and so is the required compact neighbourhood of c.

The proof that $\tilde{X}/E$ is Hausdorff is entirely analogous to the proof in Theorem 2.2.

□

2. o-minimality of definable sets

We want to view the hyperdefinable sets as o-minimal sets, therefore we need to firstly define a suitable expansion of a model in which we can interpret them, and then define o-minimality of a set. We introduce here the Shelah expansion by all externally definable sets, proving some results in full generality. These results will then hold also in the reducts used in computations.

Here we recall a theorem due to Baisalov and Poizat, which was then generalized by Shelah to a wider class of theories.

Let N be any structure. A subset $X \subseteq N^n$ is *externally definable* if, there is $N' \succ N$ and parameters $c \in N'$ and a formula $\varphi(x, y) \in L_N$ such that $\varphi(x, c)^{N'} \cap N$ defines X.

Equivalently, X is externally definable in N if there is a structure $N' \models Th(N)$, $N' \succ N$, and a definable set X' in N' such that $X = X' \cap N$.

We construct from N a new theory $Th(N^{\mathrm{Sh}})$ in the following way: for each externally definable set, defined by an $L_{N'}$-formula φ say, we add a relation symbol R_φ to the language. We call the new language L^{Sh}; the model will be denoted by N^{Sh} and this gives rise to a new theory $Th(N^{\mathrm{Sh}})$. This new theory is called *Shelah's expansion* of the structure N.

Baisalov and Poizat proved in [**1**] the following theorem:

THEOREM 2.7. *If N is an o-minimal structure, $Th(N^{\mathrm{Sh}})$ admits quantifier elimination.*

We recall that a structure N in a language with a total linear order, in which every definable set in one variable is a finite union of convex sets is a *weakly o-minimal* structure. If every model of $Th(N)$ is weakly o-minimal we say that N has *weakly o-minimal theory* (it is *uniformly weakly o-minimal*).

We remind the reader that weakly o-minimal theories have NIP.

Theorem 2.7 has been generalized by Baizhanov in [**2**] to the class of weakly o-minimal theories, and it has been generalised further by Shelah in [**32**] to the NIP theories:

THEOREM 2.8. *If N is a model of a theory with NIP, then $Th(N^{Sh})$ admits quantifier elimination and has NIP.*

From [**16**] we get the important fact:

FACT 2.9. *Any o-minimal model N is uniformly o-minimal.*

This is equivalent to saying that any superstructure $N' \succ N$ is o-minimal.

Note that this fact does not hold in general for weakly o-minimal theories.

An immediate consequence of Theorem (2.8) 2.7 is the following:

REMARK 2.10. If N is (uniformly weakly) o-minimal then N^{Sh} is uniformly weakly o-minimal.

We now define o-minimality of a set.

DEFINITION 2.11. Let N be any structure with language L_N, and X a definable linearly ordered set in N.

- X is *o-minimal*, if given any formula $\varphi(x) \in L_N$, it defines on X a finite union of intervals and points.
- X is *uniformly o-minimal* if, given any formula $\varphi(x, \overline{y}) \in L_N$, we can find a number $n_\varphi \in \omega$ such that for each choice of parameters $\overline{b} \in N$, $\varphi(x, \overline{b})$ defines on X no more than n_φ intervals and points.
- X is *weakly o-minimal* if, given any formula $\varphi(x) \in L_N$, it defines on X a finite union of convex sets.
- X is *uniformly weakly o-minimal* if, given any formula $\varphi(x, \overline{y}) \in L_N$, we can find a number $n_\varphi \in \omega$ such that for each choice of parameters $\overline{b} \in N$, $\varphi(x, \overline{b})$ defines on X no more than n_φ convex sets.

We now consider again the Shelah expansion and prove directly a special case of Theorem 8.6 [**12**]:

THEOREM 2.12. *Given an o-minimal theory T, a saturated model M, a definable, definably densely linearly ordered,* 1*-dimensional, o-minimal set $X \subset M^n$ and a type-definable, externally definable, convex (with each class convex with respect to the order of X) equivalence relation E with a bounded number of* *classes, then the hyperdefinable set X/E, definable in $(M^{\mathrm{Sh}})^{eq}$, is uniformly o-minimal in $(M^{Sh})^{eq}$.*

(Note: the convexity assumption is not necessary, but it simplifies the definition of the induced order on X/E.)

Proof. Since E is convex, the order on X/E can be trivially defined by $[x]_\sim \leq' [y]_\sim$ if $x \leq y$. We shall drop the $'$ in the future. (If it is not convex, it is nevertheless possible to define the order using o-minimality of the structure; see Proposition 8.6 of [**12**].)

We work in M^{Sh}, and we consider a formula $\varphi(x, \overline{y}, \overline{c})$ in $\mathcal{L}$ with $\overline{c} \in M' \succ M$. Since M^{Sh} is uniformly weakly o-minimal, for each choice of $\overline{b} \in M$, the set Y defined by $\varphi(x, \overline{b}, \overline{c})$, is a union of $\leq \alpha_\varphi$ convex sets. Without loss of generality we can suppose $Y \subset X$, in fact Y will determine $\leq \alpha_\varphi$ cuts also in X. Let $\psi(x, \overline{b}, \overline{c})$ be the formula in $(M^{\mathrm{Sh}})^{eq}$ that defines the quotient $Y/E \subseteq X/E$; it will define $\leq \alpha_\varphi$ convex subsets of X/E. Since $\overline{b}$ was arbitrarily chosen, we get that X/E is uniformly weakly o-minimal.

To prove now that X/E is uniformly o-minimal it is sufficient to prove that it is complete (all the convex sets will then have a supremum and an infimum, and therefore they will be intervals).

Now we forget about Shelah's expansion and we regard E as a bounded type-definable equivalence relation in a model M. Consider a Dedekind cut (A, B) of X/E. For each $a \in A$ we can define the set $A_a = \{x \in X/E | a \leq x\}$; the preimage of this set is type-definable in M and therefore it is a closed set. Analogously for each $b \in B$ we define $B_b = \{x \in X/E | b \geq x\}$, which has type-definable preimage, and is therefore closed. Consider now the family of closed sets $\{B_b, A_a\}_{a,b}$; it has the finite intersection property by density of the order, so, since X/E with the logic topology is compact by Lemma 2.2, there is an element in the intersection. Thus X/E is complete, and hence weakly o-minimal.

□

Observation 2.13. Note that the theorem above holds also if T is uniformly weakly o-minimal.

Observation 2.14. The theorem above holds also when X/E is considered in a reduct of M^{Sh} over which it is definable, in particular over $(M, P, \dots)^{eq}$, the structure obtained by adding a predicate P for an externally definable set to M.

Observation 2.15. In the cases we study it is easy to prove directly that each group G considered is *o*-minimal. But by the results in Razenj [**30**] if we work with a definably connected group (as we do in the following chapters of the thesis), then our group G, seen as a definable manifold and maybe after taking off a point, can be equipped with definable orientation $\leq$ that is piecewise o-minimal, and the group itself "resembles" either the real line or the circle group S^1. By inspecting the overlapping charts we obtain that G is o-minimal with respect to $\leq$.

We can easily generalize Theorem 2.12 to ind-hyperdefinable sets. Firstly notice that the definitions of induced order and those related to o-minimality can be extended to ind-hyperdefinable sets in the obvious way (in particular we say that an ind-definable set $\tilde{X}$ is 1-dimensional if each X_i is 1-dimensional).

Theorem 2.16. *Given an o-minimal theory T, a saturated model M, an ind-definable, externally definable, 1-dimensional, o-minimal convex set $\tilde{X} = \bigcup_i X_i$, densely linearly ordered, such that the restriction of the ordering onto X_i is definable; and a type-definable, externally definable, convex equivalence relation E on $\tilde{X}$ with a bounded number of classes, then the ind-hyperdefinable set $\tilde{X}/E$, definable in $(M^{\mathrm{Sh}})^{eq}$, is uniformly o-minimal in $(M^{\mathrm{Sh}})^{eq}$.*

Proof. The proof of uniform weak o-minimality of $\tilde{X}/E$ goes through exactly as in the previous theorem.

We now need to prove completeness: consider a Dedekind cut (A, B) of $\tilde{X}/E$. Denote $\tilde{X}/E \restriction X_i$ by X_i/E. Then there exists $X_i \subset \tilde{X}$ such that $A \cap X_i/E \neq \emptyset$

and $B \cap X_i/E \neq \emptyset$. As in the previous theorem we define $A_a = \{x \in X_i/E : a \leq x\}$, $B_b = \{x \in X_i/E : b \geq x\}$, for $a \in A$ and $b \in B$. Again the family of closed sets $\{A_a, B_b\}_{a,b}$ has the finite intersection property. Theorem 2.6 states that $\tilde{X}/E$ is locally compact, so X_i/E is compact, by Fact 2.5, and we can find an element in the intersection of $\{A_a, B_b\}_{a,b}$. This gives us completeness of $\tilde{X}/E$ and completes the proof. □

Observation 2.17. Also this theorem holds in reducts of M^{Sh} over which $\tilde{X}/E$ is definable.

We are now able to consider o-minimality issues for hyperdefinable sets and ind-hyperdefinable sets by working in a suitably enriched structure.

3. One-basedness

In the last few years it has been noticed that properties typical of stable theories can be observed also in unstable theories. In this context Peterzil and Loveys introduced a notion called CF-linearity in [**22**]. Such theories present a "trichotomy-like" behaviour, as studied by Peterzil and Starchenko in [**23**]; in [**29**] Pillay introduced an equivalent of CF-linearity, called 1-basedness for o-minimal theories, since it would provide an o-minimal version of 1-basedness for stable theories. We shall recall that definition and localize it to stably embedded definable sets, in order to obtain a structural complexity classification of the groups we are studying.

Let M be o-minimal. Given $f(x, \overline{y})$ a $\emptyset$-definable partial function, 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 $f(-, \overline{c})$ nor $f(-, \overline{c}')$ 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 $\overline{c}/\sim_a$.

Definition 2.18. Given an o-minimal theory T, we say that T is 1-*based* if in any saturated model $M \models T$, 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 $\overline{c}/\sim_a \in dcl(a, f(a,\overline{c}))$ as an imaginary element, i.e. in the appropriate sort of M^{eq}.

DEFINITION 2.19. Given a theory T and $\varphi(x) \in L^{eq}$, φ is *stably embedded* in T if for any saturated model $N \models T$ and $X = \varphi(N)$, any subset of X^n definable (with parameters) in N is definable with parameters from X.

If $X = \varphi(N)$ for some saturated model N, we say that X is a stably embedded set if $\varphi(x)$ is.

We localize 1-basedness to stably embedded sets. Let X be stably embedded in N, then we define the structure $\mathcal{X} = (X, R_i)$, where R_i is a relation symbol for any $\emptyset$-definable (in N) subset of X^n. Observe that this is sufficient to capture in $\mathcal{X}$ all the structure induced on X by N. To see this observe that if we consider a superstructure $N' \succ N$, and denote by X' the subset of N defined by the formula defining X and by $\mathcal{X}'$ the structure obtained by adding a relational symbol to X' for any $\emptyset$-definable (in N') subset of $(X')^n$, then $\mathcal{X}' \succ \mathcal{X}$.

DEFINITION 2.20. We say that a uniformly o-minimal stably embedded set X in a saturated structure N is 1-*based* in T if the theory $T_X = Th(\mathcal{X})$ is 1-based.

Let $\varphi(x)$ be an L^{eq}-formula, M any model of T, and suppose $X = \varphi(M)$ is a uniformly o-minimal set in M. Then X is stably embedded by Theorem 2 of [**8**].

An easy example of non-1-based sets are intervals: let M be an o-minimal expansion of a saturated real closed field. Then:

REMARK 2.21. Any interval $I \subseteq M$, is in definable bijection with $[-1, 1)$.

We obtain then easily a lemma:

LEMMA 2.22. *An interval I in M is non-*1*-based (as a definable set).*

PROOF. By Remark 2.21 I is stably embedded in M, and so it makes sense to talk about its 1-basedness.

Let f be the definable bijection of I with the interval $[0,1)$, and let $a<b<c$ be independent elements in $[0,1)$ such that $a\cdot b+c=d$ is still an element of $[0,1)$, and thus $dim(a,b,c,d)=3$ (we mean here the dimension determined by the definable closure dcl).

Observe that in this case the imaginary element $(b,c)/\sim_a$ is simply the tuple (b,c).

Define partial maps on I as follows: given $x,y\in I$, let $x\tilde{+}y=f^{-1}\left(f(x)+f(y)\right)$ and $x\tilde{\cdot}y=f^{-1}\left(f(x)\cdot f(y)\right)$. So the partial function $g_{bc}(x)=x\tilde{\cdot}f^{-1}(b)\tilde{+}f^{-1}(c)$ witnesses non-1-basedness of I, since if I were 1-based we would have $(b,c)\in dcl(a,d)$, and so $dim(a,b,c,d)=2$, but this is clearly not possible since $dim(a,b,c,d)=3$. This proves then that I has to be non-1-based. □

3.1. Internality and useful lemmas. We define the notion of internality, introduced in [**27**].

DEFINITION 2.23. Given a definable set X in a saturated structure N 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.

The obvious example of a set Y internal to X is when Y is a definable subset of X.

In [**7**] (Chapter 7.5, pages 77-78) internality is used in the context of stability in algebraically closed valued fields, mainly to correlate stability of definable sets with their internality to the residue field sort.

In this thesis we shall consider bijections between groups G/G^{00} and 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 fundamental lemma for our results is:

LEMMA 2.24. *Given a saturated structure N expanding a field, uniformly o-minimal 1-dimensional definable sets X, Y, and a definable bijection $f : X \to Y$, then X is (non-) 1-based if and only if Y is (non-) 1-based.*

PROOF. By Theorem A of Ramakhrishnan in [**14**], whose solution in the 1-dimensional case was already known to Steinhorn, we have that there is a definable, piecewise order preserving, embedding g_1 of X into N, and a definable, piecewise order preserving, embedding g_2 of Y into N. Since any two intervals of N are in definable bijection, and such a bijection is piecewise either order preserving or order reversing, we have that $f : X \to Y$ is piecewise order preserving or order reversing. Let us then consider a function h witnessing non-1-basedness in an interval I of X. Without loss of generality we can suppose f to be order preserving in I (if f is order reversing the case is analogous), then clearly $f \cdot h$ witnesses non-1-basedness in Y. This proves the lemma. □

3.2. One-basedness in real closed valued fields. A classical example of a structure that has both a 1-based and a non-1-based uniformly o-minimal set is a real closed valued field. We prove here that given a saturated real closed valued field M_w, with language L_w, the value group Γ_w is 1-based and the residue field k_w is non-1-based. In the rest of the thesis these two sets will be the "basic" sets that we shall use to check (non-) 1-basedness for groups of the form G/G^{00}, using Lemma 2.22 and Lemma 2.24.

The following is a theorem of Mellor (Lemma 3.13 of [**21**]). We recall a strengthening of stable embeddedness, and the proof of the Lemma.

DEFINITION 2.25. Given a structure N in language L, and a definable set X; let L' a sublanguage of L and N' be an L'-structure whose base set is X, then N' is *fully embedded* if

- X is a stably embedded set in N, and
- for every $\emptyset$-definable set $C \subseteq N$ in the language L, the set $C \cap N'$ is $\emptyset$-definable in the language L' (if this condition is satisfied we say that N' is *canonically embedded* in N).

The meaning of this definition is that for a set X fully embedded as an L'-structure, the structure induced on X by the ambient structure N as a stably embedded set (i.e, $\mathcal{X}$) is precisely the L'-structure we considered.

LEMMA 2.26. *Given a real closed valued field M_w, its value group Γ_w, as a divisible ordered abelian group (with constants), and its residue field k_w, as a real closed field, are fully embedded.*

PROOF. By Theorem 1.13, M_w admits quantifier elimination in the language L_w, thus any definable set in the value group sort can be defined by a boolean combination of formulae of the form

$$t\big(\gamma_1, \dots, \gamma_n, v(p(\overline{a}))\big) \geq t'\big(\gamma'_1, \dots, \gamma'_m, v(p'(\overline{a}'))\big),$$

where t, t' are terms in the language of the value group sort, $\gamma_i, \gamma_j \in \Gamma$, and $p(\overline{a}), p'(\overline{a}')$ are polynomials in variables $\overline{a} = (a_1, \dots, a_r), \overline{a}' = (a'_1, \dots, a'_s) \in M$. By using the properties of valuation, and factorizing as much as we can, $v(p(\overline{a}))$ can be written as $\sum_i \alpha_i v(h(a_i))$, similarly $v(p'(\overline{a}'))$ becomes $\sum_i \alpha'_i v(h(a'_i))$, with $\alpha_i, \alpha'_i \in \mathbb{Z}$ and h a polynomial of degree 1 or 2; clearly $v(h(a_i)), v(h(a'_i))$ are elements of Γ and the sum is in L_w. Therefore any formula defining a set in Γ is equivalent to a formula with parameters only from Γ in the language of a divisible ordered abelian group, and therefore is fully embedded as a divisible ordered abelian group.

The proof of full embeddedness of k_w as a real closed field is similar. □

COROLLARY 2.27. *The value group Γ_w of a real closed valued field M_w is 1-based in M_w.*

The residue field k_w of a real closed valued field M_w is non-1-based in M_w.

PROOF. Full embeddedness of Γ_w, proved in Lemma 2.26, implies that $T_{\Gamma_w} = Th(\mathbb{Q}, +, <, 0)$. Since it is well known that the theory of a divisible ordered abelian group is 1-based, we obtain the corollary.

We recall the proof of 1-basedness for the theory of divisible ordered abelian groups. Let D be a saturated model of $Th(\mathbb{Q}, +, <, 0,)$. By quantifier elimination a definable function $f(x, \overline{y})$ on D is piecewise of the form $f(x, \overline{y}) = \sum_i q_i y_i + qx$, there $q_i, q \in \mathbb{Q}$. Thus, given a tuple $\overline{c} = (c_i)$, in a neighbourhood U_a of a, $f(x, \overline{c}) = qx + \sum q_i c_i$. Suppose that $f(x, \overline{c'}) \sum_i q_i y'_i + qx = f(x, \overline{c})$ in u, this happens if and only if $\sum_i q_i y'_i = \sum_i q_i y_i$; we call $d = \sum_i q_i y_i$. Thus the germ is $\overline{c}/ \sim_a = d$ and we can define it using $a, f(a, \overline{c})$ by $d = f(a, \overline{c}) - a$. This proves that $\overline{c}/ \sim_a \in dcl(a, f(a, \overline{c}))$, and thus that $Th(\mathbb{Q}, +, <, 0,)$ is 1-based.

For the proof that k_w is non-1-based in M_w, we recall that by Lemma 2.26, the theory of the residue field is the theory of real closed fields, therefore k_w is non-1-based in M_w, following the same proof as that of theorem 2.22.

□

4. Summary

In this section we recalled the logic topology and the main results concerning it, gathering them from various sources. We then introduced the localized notions of (uniformly) (weakly) o-minimality of a set, and defined 1-basedness of a stably embedded set. All of this material has then been generalized to ind-hyperdefinable sets. The latter will become fundamental in Chapter 5 of the thesis. Moreover, we presented the fundamental examples of a 1-based and a non-1-based set, and lemmas to transfer such properties between definable sets of a structure via definable bijections.

CHAPTER 3

Easy cases

In this chapter we study one-basedness for G/G^{00}, where G is one of the first three cases of List A, i.e., G is either an additive truncation, a multiplicative truncation, or it is $SO_2(M)$ or one of its truncations. The case when G is determined by an elliptic curve is treated in the next chapter and requires some notions from elliptic curve theory.

We firstly give a general outline of the procedure, then the single cases will be dealt with in following subsections.

For the rest of this chapter we denote by M a saturated real closed field. A group $(G, *)$, which is 1-dimensional, definably connected, definably compact, definable in M can be definably circularly ordered by Proposition 2 of [**30**]. By fixing a point (for example the identity) we can suppose G is linearly ordered and o-minimal with respect to this ordering.

Without harm o-minimality could be defined for a circular ordering, and the results of this thesis can be obtaining just considering the groups of List A as circularly ordered groups. This approach, though, is just a rather tedious elaboration of the notions defined and is therefore not carried on in this thesis.

Pillay showed in Proposition 3.5 of [**28**] that the logic topology on G/G^{00} (as a hyperdefinable set in M) coincides the standard topology of G/G^{00} as a Lie group. Moreover this latter topology is exactly the o-minimal topology on G/G^{00} (as a uniformly o-minimal set in $M' = (M, G^{00}, \dots)^{eq}$).

Again in Proposition 3.5 of [**28**], Pillay proved the following Lemma:

LEMMA 3.1. *Given a definably connected, definably compact, definable group G in an o-minimal structure, then G^{00} is the neighbourhood of the identity bounded by the torsion points*

In this sense it can be viewed as the set of "infinitesimals" of G. We can consider the equivalence relation determined by G^{00}: $x \sim y$ if and only if $x * y^{-1} \in G^{00}$. This is externally definable, being determined by the cuts of G^{00}; type-definable, using the torsion points; and convex with respect to the ordering of G. Thus G/G^{00} is a bounded hyperdefinable set in M and it satisfies the hypothesis of Theorem 2.12.

We then consider the structure $M' = (M, G^{00}, \overline{a}, \dots)^{eq}$ obtained by adding a predicate for G^{00} and parameters $\overline{a}$ defining G, if needed. Then G/G^{00} is a $\emptyset$-definable linearly ordered set in M'. By Theorem 2.12 (to be precise, by the observation that the theorem holds in reducts of M^{Sh}), G/G^{00} is uniformly o-minimal in M'.

We can therefore extract the theory of G/G^{00}; it makes sense to apply Definition 2.20 to the group G/G^{00} in M', and talk about G/G^{00} being 1-based or non-1-based in M'. In Chapter 5 we shall prove that in fact if G/G^{00} is 1-based it will be 1-based also in the expansion by all externally definable sets M^{Sh}.

We shall prove directly 1-basedness or non-1-basedness for the simplest cases; for the harder ones, we need to use Lemma 2.24.

1. Additive and multiplicative truncations

These cases are the fundamental examples to which we shall refer throughout the thesis.

1.1. The additive truncation. Consider now the case in which G is a truncation $([-1, 1), + \ mod\ 2)$ of the additive group of M.

We firstly need to compute G^{00}. We recall that the torsion points are of the form $T_n = \{x | [n]x = 0\}$ for some $n \in \mathbb{N}$, where $[n]x$ indicates the formal product by a natural number defined by:

$$[n]x = x \ (+ \ mod\ 2) \ x \ (+ \ mod\ 2) \ \dots \ (+ \ mod\ 2) \ x, \quad n \ times \ ;$$

or, using the usual product of M, we have $T_n = \{x | n \cdot x \in \mathbb{Z}\}$ for some $n \in \mathbb{N}$.

Since G^{00} is the subgroup of G bounded by the torsion points, it is type defined by $\bigcap_{n\in\omega}\{x| -1 < n \cdot x < 1\}$; this clearly is the set of the infinitesimal elements around 0 (with the standard valuation), therefore $G/G^{00} = [-1,1)/\mu = [-1,1)^{\mathbb{R}}$. Clearly the operation $(+ \ mod\ 2)$ is well defined in the quotient, so $(G/G^{00}, + \ mod\ 2) = \big([-1,1)^{\mathbb{R}}, + \ mod\ 2\big)$.

We add now a predicate for G^{00} to M, obtaining $M' = (M, G^{00}, \dots)^{eq}$. We discuss 1-basedness of G/G^{00} in M'. We shall do it in two ways: firstly by witnessing non-1-basedness with a function, then by showing that G/G^{00} lives in a non-1-based sort.

Let $\mathcal{G}'$ be of the form $G'/(G')^{00}$ where $(G')^{00}$ is the interpretation of the predicate for G^{00} in a sufficiently saturated extension M'' of M'.

Clearly we identify $\mathcal{G}'$ with $G'/(G')^{00}$, and therefore define in $\mathcal{G}'$ the operations $+, \cdot$ as follows: given $g, h \in \mathcal{G}'$, let $\hat{g}, \hat{h}$ be the identification of g, h in $G'/(G')^{00}$, then let $\hat{g}\hat{+}\hat{h}$ be $\pi^{-1}(\pi(\hat{g}) +_{M''} \pi(\hat{h}))$ and $\hat{g}\hat{\cdot}\hat{h}$ be $\pi^{-1}(\pi(\hat{g}) \cdot_{M''} \pi(\hat{h}))$ for a suitable projection on a coordinate of M''. Then let $g+h$ and $g \cdot h$ be the identification in $\mathcal{G}'$ of $\hat{g}\hat{+}\hat{h}$ and $\hat{g}\hat{\cdot}\hat{h}$.

By saturation of $\mathcal{G}'$ we can find algebraically independent elements $a, b, c \in \mathcal{G}'$. Let $d = a \cdot b + c$; clearly $dim(a, b, c, d) = 3$ (where dim refers to the *dcl*-dimension).

Let us now define a function $f_{b,c}(x) = x \cdot b + c$; the germ of this function at a is exactly $(b, c)/\sim_a = (b, c)$: in fact $f_{b,c} = f_{b',c'}$ at a neighbourhood of a if and only if $(b, c) = (b', c')$. If G/G^{00} were 1-based we would have then $(b, c)/\sim_a = (b, c) \in acl\,(a, f_{b,c}(a)) = acl(a, d)$, so $dim(a, b, c, d) = 2$, which contradicts that which we have previously observed.

This proves non-1-basedness of G/G^{00}.

We have therefore proved:

THEOREM 3.2. *If G is a truncation of an additive group of M, then G/G^{00} is non-1-based in M'.*

There is also an indirect way to prove a strengthening of Theorem 3.2. We noticed that $G^{00} = \mu = I_v$, therefore M' is interdefinable with the standard real closed valued field M_v^{eq}.

LEMMA 3.3. *Given an additive truncation G in M, the structures M' and M_v^{eq} are interdefinable.*

PROOF. In M', $G^{00} = I_v$, the standard valuation ideal; we can then define R_v by $\{x \in M | x^{-1} \notin I_v\}$. The value group Γ_v is then as usual $\Gamma_v = M/(R_v \setminus I_v)$ and the residue field $k_v = R_v/I_v$.

On the other hand in M_v^{eq}, I_v is definable and it is equal to G^{00}.

Therefore M' and M_v^{eq} are interdefinable. □

This means that $G/G^{00} = [-1,1)^{\mathbb{R}}$ is a $\emptyset$-definable subset of k_v, therefore G/G^{00} is non-1-based in $M_v^{eq} = M'$ by Lemma 2.22 or Corollary 2.27.

We obtain therefore an improvement of Theorem 3.2:

THEOREM 3.4. *If G is a truncation of an additive group of M, then G/G^{00} is non-1-based in M', and it is a definable subset of k_v in M_v^{eq}.*

Note: It will be common notation throughout the thesis to call M' the expansion of M by a predicate for G^{00} and, if necessary, a finite number of constants. Moreover we shall improperly denote M_w^{eq} by M_w, where M_w is a saturated real closed valued field, since the additional imaginaries of M_w play no role in this project. When M' is interdefinable with a real closed valued field M_w we shall use M' and M_w interchangeably.

OBSERVATION 3.5. If we consider any additive truncation $A = ([-a,a), + \ mod\ 2a)$, then there is a definable isomorphism of A with $([-1,1), + \ mod\ 2)$; thus A/A^{00} is non-1-based, and internal to k_v.

1.2. The multiplicative truncations. The second case is when G is a multiplicative truncation, i.e., $G = \big([b^{-1}, b), \cdot \ mod \ b^2\big)$, with $b > 1$.

Again the first step is to compute G^{00}. Since G^{00} is the neighbourhood of the identity bounded by the torsion points, $G^{00} = \bigcap_{n\in\omega}\{x|b^{-1/n} < x < b^{1/n}\}$, truncation of $(M^{>0}, \cdot)$.

The operation $\cdot \ mod \ b^2$ on G^{00} coincides with the multiplication on M and is closed, so G^{00} is also a multiplicative subgroup of M.

The following valuation theoretical observation is fundamental (see [**34**] Definition 3.4 and Proposition 3.5):

OBSERVATION 3.6. Given a convex multiplicative subgroup S of M,

- If $2 \in S$, then S is the set of positive units of the convex valuation ring R_w defined as $\{a||a| < g$ for some $g \in S\}$
- If $2 \notin S$ and S is closed under taking square roots (of positive elements), then $S-1$ is the underlying set of a (convex) additive subgroup of M (note that also the converse holds: for every additive convex subgroup S of M such that $1 \notin S$, $1 + S$ is the set of a multiplicative group of M). Moreover, $S - 1$ is the maximal ideal I_w of a valuation ring R_w.

We shall apply this observation to G^{00} in place of S and show how the behaviour of G/G^{00} depends entirely on whether the parameter b defining G is finite or infinite.

1.2.1. *Small multiplicative truncations.* Let $G = ([b^{-1}, b), \cdot \ mod \ b^2)$, with b a finite element (i.e., $v(b) \geq 0$, where v, we recall, is the standard valuation). Then $2 \notin G^{00}$, so $G^{00} - 1$ is the maximal ideal I_w for some valuation w. Analogously to the additive case, we can either prove non-1-basedness of G/G^{00} in a direct way: we define the operation $\oplus : G \times G \to G$: $a \oplus b = a + b - 1$, that is well defined in the quotient G/G^{00}, and witness non-1-basedness with the function $f : (x \cdot y) \oplus z$.

Or we can simply observe that, given $x, y \in G$, $x/G^{00} = y/G^{00}$ in G^{00} if and only if $x - y \in I_w$, and thus G/G^{00} embeds as a set in k_w.

We omit the details of the proofs.

1.2.2. *Big multiplicative truncations.* In this case b is an infinite element (i.e., $v(b) < 0$). Clearly $2 \in G^{00}$, so G^{00} is the set of positive units of a valuation w, say.

It is easy to show that $M' = (M, G^{00}, b, \dots)^{eq}$ is interdefinable with the real closed valued field M_w, the proof is as in Lemma 3.3.

Moreover, since $G/G^{00} = G/(R_w \setminus I_w) \subset M^{\neq 0}/(R_w \setminus I_w) = \Gamma_w$, we have that $(G/G^{00}, \cdot \ mod\ b^2)$ is a truncation of $(\Gamma, +)$ in M_w.

We proved in Corollary 2.27, Chapter 2, that Γ_w is 1-based in M_w.

We can then consider Γ_w as a model of T_{Γ_w}, and G/G^{00} will be a group definable in this structure. By stable embeddedness of Γ_w in M_w, all definable sets of G/G^{00} in M_w are definable with parameters from Γ_w. We can therefore use 1-basedness of T_{Γ_w} to obtain 1-basedness of G/G^{00} in $M' = M_w$. Consider a saturated model $\mathcal{G}'$ of $T_{G/G^{00}}$; there is a saturated model Γ' of T_{Γ_w} for which $\mathcal{G}'$ is a truncation. If $\mathcal{G}'$ were non-1-based, then Γ' would not be 1-based, contradicting what we have just observed.

We have therefore proved:

THEOREM 3.7. *The group G/G^{00}, where $G = ([b^{-1}, b), \cdot\ mod\ b^2)$, is 1-based in M' if and only if $v(b) < 0$ and if and only if it is a definable subset of Γ_w in M_w. If $v(b) \geq 0$, then G/G^{00} is non-1-based in M' and is a definable subset of k_w in M_w.*

2. $SO_2(M)$ and truncations

The last family of groups we consider in this chapter are $(SO_2(M), *)$ and its truncations. We can consider them as subsets of M^2 by Remark 1.8.

We denote the definable circular anticlockwise ordering on $SO_2(M)$ by $\prec$, the inverse of a point P by $-P$, the formal product $P * P * \cdots * P$, n times, by $[n]P$, and the projections of P onto the x- and y-axis by x_P and y_P respectively. We can suppose the ordering to be linear by fixing $O = (1, 0)$, the identity of $SO_2(M)$ and supposing $(-1, 0)$ to be the smallest element. Observe that this ordering is not translation invariant.

A truncation of $SO_2(M)$ is a group $\big([-S, S), *\ mod\ [2]S\big)$, where $[-S, S)$ is an interval with respect to the ordering $\prec$. Let then $G = (SO_2(M), *)$, or $G = \big([-S, S), *\ mod\ [2]S\big)$.

The case when $G = SO_2(M)$ is straightforward, clearly $G^{00} = \{P \in G | x_P > 0 \wedge v(y_P) > 0\}$, so we can define the standard valuation in $M' = (M, G^{00}, \dots)^{eq}$, and G/G^{00} can be identified with $SO_2(k_v) = SO_2(\mathbb{R})$. Thus, in $M' = M_v$, G/G^{00} is a definable subset in the standard residue field and is therefore non-1-based.

If G is a truncation, it is sufficient to consider G when it is a truncation with $x_S \in \big[\frac{1}{2}, 1\big)$; in fact if such truncation is non-1-based then any other truncation G' with $G^{00} = G'^{00}$ is non-1-based. Given a truncation $G = \big([-S, S), *\ mod\ [2]S\big)$ of $SO_2(M)$, either $x_S \in \big[\frac{3}{4}, 1\big)$ or $G^{00} = \{P \in G | x_P > 0 \wedge v(y_P) > 0\}$, in fact, in the second case, by inspecting the torsion points we obtain that G^{00} coincide with $SO_2(M)^{00} = \{P \in G | x_P > 0 \wedge v(y_P) > 0\}$.

We need now to compute G^{00}. The following lemma gives us a definition of G^{00} in terms of the standard valuation:

Lemma 3.8. *A group* $G = \big([-S, S), *\ mod\ [2]S\big)$, $x_S \in \big[\frac{3}{4}, 1\big)$ *has*

$$G^{00} = \{P \in G | v(y_P) > v(y_S)\}.$$

Proof. The lemma follows immediately from the following claim: and the fact that G^{00} is bounded by its torsion points:

CLAIM: either $v(y_{[2^n]P}) = v(y_P)$ for any $n \in \omega$, or $v(y_P) = 0$.

This follows from the fact that if P is a torsion point, the points $[2^n]P$, for $n \in \omega$, are a subset of the torsion points that are cofinal in $G \setminus G^{00}$. Thus if the claim is true, the sequence $y_{[2^n]P}$, $n \in \omega$, is cofinal in $M \setminus \{y : v(y) > v(y_S)\}$, and so it defines G^{00} as $\{P \in G | v(y_P) > v(y_S)\}$.

We now prove the claim by induction. We fix P such that $v(y_P) > 0$; observe that $x_{[2]P} = x_P^2 - y_P^2$ and $y_{[2]P} = 2x_P y_P$. If $v(y_P) > 0$, then $v(x_P) = 0$, so $v(y_{[2]P}) = v(2x_P y_P) = v(y_P)$. Suppose now $v(y_{[2^n]P}) = v(y_P)$, then $v(y_{[2^{n+1}]P}) = v(2x_{[2^n]P} y_{[2^n]P}) = v(y_{[2^n]P}) = v(y_P)$.

This proves the claim and therefore that $G^{00} = \{P \in G | v(y_P) > v(y_S)\}$. □

We work now in $M' = (M, G^{00}, x_s, y_s, \dots)^{eq}$.

To prove non-1-basedness we use Lemma 2.24: we construct a definable (in M') bijection of G/G^{00} with a non-1-based group, namely the quotient of an additive truncation A by its own A^{00}.

Lemma 3.9. *Given $G = ([-S, S), * \ mod \ [2]S)$, $x_S \in \left[\frac{3}{4}, 1\right)$, the group G/G^{00} is in definable bijection in M' with A/A^{00}, where $A = \left(\left[-\frac{y_S}{x_S}, \frac{y_S}{x_S}\right), + \ mod \ 2\frac{y_S}{x_S}\right)$ is an additive truncation.*

Proof. We define the function $l : G \to M$ which sends a point $P \in G$ to the second coordinate of the intersection of the line through P and the origin with the line $x = 1$. Namely $l(P) = \frac{y_P}{x_P}$. We then define $A = \Big([-l(S), l(S)), + \ mod \ 2 \ l(S)\Big)$. Observe that $v(l(S)) = v(y_S)$, and therefore $A^{00} = \big\{x | v(x) > v(l(S))\big\} = l(G^{00})$ by Lemma 3.8. It is then sufficient to prove that $l : G/G^{00} \to A/A^{00}$ is well defined and injective passing to the quotient; by construction l will then be a bijection. So it suffices to show that, given $\tilde{P}, \tilde{Q} \in G \setminus G^{00}$, and $P, Q \in G$ representatives of the respective equivalence classes, $v(l(P * -Q)) > v(l(S))$ if and only if $v(l(P) - l(Q)) > v(l(S))$. By assumption $v(y_P) = v(y_Q) = v(y_S)$, and since we impose $x_S \in \left[\frac{3}{4}, 1\right)$, we have $v(x_P x_Q - y_P y_Q) = 0$, so $v(l(P)) = v(l(Q)) = v(l(S))$, and then $v\big(l(P * -Q)\big) = v\left(\frac{x_Q y_P - x_P y_Q}{x_P x_Q - y_P y_Q}\right) = v\left(x_Q y_P - x_P y_Q\right) = v\left(x_P x_Q \left(\frac{y_P}{x_P} - \frac{y_Q}{x_Q}\right)\right) = v\left(\frac{y_P}{x_P} - \frac{y_Q}{x_Q}\right) = v(l(P) - l(Q))$. This proves the statement. □

Observe that the proof above shows that l is a group isomorphism $l : G/G^{00} \to A/A^{00}$.

By Lemma 2.24, Theorem 3.4 and Observation 3.5 we get the theorem:

THEOREM 3.10. *Given $G = SO_2(M)$ or G a truncation of $SO_2(M)$, G/G^{00} is non-1-based in M' and it is internal to k_v in M_v.*

3. Local completeness of nonstandard value groups

We analysed 1-basedness for G/G^{00} where G is one of the first three cases in List A; i.e. G is either an additive truncation, a multiplicative truncation, $SO_2(M)$ or one of its truncations.

We found that there is only one case in which G/G^{00} is 1-based: when G is a "big" multiplicative truncation, a truncation of the multiplicative groups by an infinite element, and that in this case we can see G/G^{00} as a definable subset of the value group Γ_w of a nonstandard real closed valued field.

We know that G/G^{00} is a compact Lie group, and this suggests that the value group of a nonstandard real closed valued field is somehow "small", at least in a neighbourhood of the identity:

THEOREM 3.11. *The value group Γ_w of a nonstandard real closed valued field M_w, where M is saturated, determined by the G^{00} of a big multiplicative truncation G, has a complete (in the usual metric) neighbourhood of the identity.*

PROOF. We have shown in the proof of 3.7 that $G^{00} = R_w \setminus I_w$.

Since G/G^{00} is a definable set in Γ_w, it is sufficient to prove that it has a metric for which it is complete. This obviously implies the theorem.

Since G/G^{00} is o-minimal we can use the standard o-minimal distance as a metric. With the o-minimal topology G/G^{00} is compact by Pillay's conjecture 1.9; and it is a well known fact that a compact metric space is complete. $\square$

In the next chapter the M-points of certain elliptic curves will provide more examples of groups in which we obtain 1-basedness of the quotient.

CHAPTER 4

Elliptic Curves

The only groups remaining to be considered from List A are the semialgebraic connected component of the group of M-points of an elliptic curve and its truncations.

In Section 1 we introduce some theory of elliptic curves, adapting some known notions, in particular the notion of minimal form for the Weierstrass equation and the notion of algebraic geometric reduction, to the context of real closed fields. This allows us to limit our attention to groups defined by equations in a simple form, depending only on one parameter. We shall split such curves into two categories: r-curves and c-curves. The former will be analysed in Section 2, and the latter in Section 3. In Section 4 we shall consider the truncations of the groups mentioned above, completing a study of all the possible cases.

1. Elliptic curves

The book of Silverman [**33**] gives an introduction to the theory of elliptic curves; here the notions needed for this project are recalled.

An *elliptic curve* over a field F is a nonsingular projective curve satisfying the following equation:

$$ZY^2 + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2 + a_4XZ^2 + a_6Z^3;$$

the identity is $O = [0 : 1 : 0]$.

When we consider the affine equation (i.e., we put $Z = 1$), we obtain:

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

where $a_1, a_2, a_3, a_4, a_6 \in F$. The identity becomes the point at infinity.

If the characteristic of F is other than 2, we can rewrite E as

$$E:\ y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \tag{1}$$

where $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$.

Define $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$.

A curve in the form 1 is an elliptic curve (i.e., is nonsingular) if and only if $\Delta \neq 0$, where $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$ is the discriminant of the curve.

Equations of this form are called *Weierstrass equations*.

Given a field F we denote by $E(F)$ the F-points of E, i.e., the realization of the formula defining E in F^2 plus a point at infinity: the identity O.

Given a point $P \in F$ we denote by x_P, y_P the projections of P onto the x and y-axis respectively.

The curve $E(F)$ can be endowed with a group structure; we denote the operation by $\oplus$ and the inverse of a point P by $\ominus P$. On an elliptic curve any line intersects the curve in precisely three points (considering also O as a point). Given points P, Q, the line through P and Q (or the tangent line if $P = Q$) intersects E at the point R. The vertical line through R will again intersect E at one point, which we call R'. $P \oplus Q$ is then defined to be this R'.

It is then immediate that if $P = (x_P, y_P)$ then $\ominus P = (x_P, -y_P)$.

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

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

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:

$$x_{[2]P} = \frac{x_P^4 - b_4 x_P^2 - 2b_6 x_P - b_8}{4x_P^3 + b_2 x_P^2 + 2b_4 x_P + b_6}.$$

1.1. Minimal form. In order to analyse elliptic curves, we need to perform some simplifications. Since all the properties we are going to deal with are invariant under definable isomorphisms, we will consider, for each curve E, a curve E' definably isomorphic to E, expressed in a generalized version of the minimal Weierstrass equation.

Firstly we recall that two elliptic curves E and E' over F are isomorphic over F and preserve the form $E: \ y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$ if it is possible to obtain E' from E by the following change of variables:

$$\begin{cases} x = & u^2x' + r, \\ y = & u^3y' + u^2sx' + t, \end{cases} \tag{2}$$

where $u, r, s, t \in F$, $u \neq 0$. Such a transformation is a combination of a translation and a homothety, and it is clearly definable.

When applying the transformation (2) the new curve will have determinant $\Delta' = u^{-12}\Delta$.

Observe that given a valuation ring R_w with valuation w, we can always write the curve with coefficients from R_w (recall that $x \in R_w \iff w(x) \geq 0$):

LEMMA 4.1. *Given a curve $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, we can always suppose that the coefficients a_i are in R_w.*

PROOF. If this is not the case, there exists a coefficient a_i such that $w(a_i) < 0$. 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 $w(u) \geq max_i(\frac{-1}{i}w(a_i))$, so that for each a_iu^i we shall have $w(a_iu^i) = w(a_i) + iw(u) \geq 0$.

Hence we obtain a curve with all coefficient in R_w. □

We recall that if we work in a local field the valuation is discrete, so the minimal Weierstrass equation can be defined in a unique way as the equation whose coefficients are all in the valuation ring and $w(\Delta) \geq 0$ is minimized.

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 $w(\Delta) \geq 0$ is minimized subject to the condition $a_1, a_2, a_3, a_4, a_6 \in R$.

In our case since we are in a real closed field, equipped with a valuation ring, the definition above gives us a family of curves, and we need to adapt the definition as follows:

By a *root* of E we mean a solution of the equation with $y = 0$.

DEFINITION 4.2. An elliptic curve E defined over a real closed field M 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 of E is in $(0, 0)$ and $w(a_i) = 0$ for some i.

An analogue of Proposition 1.3 of [**33**] can now be proved in this context:

PROPOSITION 4.3. (1) *Every elliptic curve E defined over a real closed field M has a minimal Weierstrass equation of the form $y^2 = x(x^2 + ax + b)$.*
(2) *This minimal Weierstrass equation is unique up to a change of coordinates*

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

where $r = -a \pm \sqrt{a^2 - 4b}$ and $w(u) = 0$ (if possible, i.e., if $a^2 \geq 4b$).

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 translate a root of E at $(0, 0)$. We can then suppose our curve is in the form $y^2 = x(x^2 + ax + b)$, with $a, b \in Fin$. For curves in this form the determinant is $\Delta = 16a^2b^2(a - b)^2$. 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

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

gives us a curve $E' : y^2 = x(x^2 + a'x + b')$, 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 E' 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 $w\left(\frac{a+\sqrt{a^2-4b}}{2u^2}\right) + w\left(\frac{a-\sqrt{a^2-4b}}{2u^2}\right) = w(a^2 - a^2 + 4b) - w(u^4) = w(b)$. By the proof of (1), either $v(a)$ or $v(b)$ is 0. Now if we have $w(b) = 0$, then $w\left(\frac{a+\sqrt{a^2-4b}}{2u^2}\right)$ and $w\left(\frac{a-\sqrt{a^2-4b}}{2u^2}\right)$ are both 0, since they are both non-negative. Thus the valuation of the determinant Δ' of E' is $w(\Delta) = 2w\left(\frac{a+\sqrt{a^2-4b}}{2u^2}\right) + 2w\left(\frac{a-\sqrt{a^2-4b}}{2u^2}\right) + 2w\left(\frac{a+\sqrt{a^2-4b}}{2u^2} - \frac{a-\sqrt{a^2-4b}}{2u^2}\right) = w(a^2 - 4b)$, that is equal to the determinant of E, and so the new equation is still a minimal Weierstrass equation.

Otherwise, $w(b) > 0$, and $w(a)$ has to be 0 by minimality of the starting Weierstrass equation $y^2 = x(x^2 + ax + b)$. Therefore either $w\left(\frac{a+\sqrt{a^2-4b}}{2u^2}\right)$ or $w\left(\frac{a-\sqrt{a^2-4b}}{2u^2}\right)$ has to be 0. We consider the first case, the second is identical, so $w(\Delta') = 2w\left(\frac{a-\sqrt{a^2-4b}}{2u^2}\right) = w(a^2 - 4b)$ and the new equation is still minimal.

□

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

1.2. 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 [**33**].

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 M, and equip M with the standard valuation. As we noticed in Lemma 4.1 we can suppose E to be defined by coefficients in Fin, and by Property 4.3 we can moreover suppose E to be in minimal form.

When we project the M-points $E(M)$ 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 $y^2 + st(a_1)xy + st(a_3)y = x^3 + st(a_2)x^2 + st(a_4)x + st(a_6)$. Here $st : Fin \to k_v$ is the standard part map defined in Chapter 1, Section 4.

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

This gives us a reduction map

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

defined as follows: given a point $P = (x, y) \in E(M)$ 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 $\lambda \in M$, 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

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

This operation, however, is not harmless: $\tilde{E}$ may not longer be an elliptic curve, and it could have singularities. The set of nonsingular points of $\tilde{E}$ forms a group defined over $\mathbb{R}$, denoted by $\tilde{E}_{ns}$ (see Proposition 2.5 pag. 61 and Exercise 3.5 pag 104 of [**33**]).

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

$$E_0(M) = \{P \in E(M) : \tilde{P} \in \tilde{E}_{ns}(\mathbb{R})\}, \tag{4}$$

i.e., the set of all points of $E(M)$ whose reduction is nonsingular (as in the usual sense, has both partial derivatives vanishing at a point), and

$$E_1(M) = \{P \in E(M) : \tilde{P} = \tilde{O}\} \ (= \{P \in E(M) | v(x_P) < 0\}), \tag{5}$$

i.e., the set of all points whose reduction is the identity of $\tilde{E}(\mathbb{R})$, or, equivalently, the set of all points whose reduction is infinite.

Such notions are well defined by Proposition 4.3.

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

A useful proposition is the following:

PROPOSITION 4.4. *There is a group isomorphism* $E_0(M)/E_1(M) \cong \tilde{E}_{ns}(\mathbb{R})$.

PROOF. The proof is in Proposition 2.1 of [**33**], observing that a real closed valued field satisfes Hensel's lemma. □

Taking the algebraic closure of M: $M[i]$ we can factorize our equation into $y^2 = (x - e_1)(x - e_2)(x - e_3)$ (applying $y \mapsto \frac{y}{2}$ to the Weierstrass equation (1)), where the e_i's are the roots of the curve in $M[i]$. By the properties of real closed fields we have only two possibilities:

(1) $e_1, e_2, e_3 \in M$, and so the curve has 3 roots and two connected components.

(2) $e_1 \in M$, $e_2, e_3 \in M[i]$ and $e_2 = \overline{e_3}$. I.e., the curve has an unique semialgebraic component and only one root $(e_1, 0)$.

We call the curves of the first kind ($y^2 = (x-e_1)(x-e_2)(x-e_3)$, $e_1, e_2, e_3 \in M$) *elliptic r-curves*, and the curves of the second kind ($y^2 = (x-e_1)(x-e_2)(x-\overline{e_2})$, $e_1 \in M, e_2, \overline{e}_2 \in M[i]$) *elliptic c-curves*. We shall analyse these two cases separately in the next two sections.

For the rest of the chapter, M will denote a saturated real closed field.

2. Elliptic r-curves

The methodology will be similar for both r-curves and c-curves: firstly we determine the minimal Weierstrass equation for E. The group G is $E(M)^0$, the semialgebraic connected component of the M-points of the elliptic curve E containing the identity; we compute G^{00} in terms of the standard valuation, characterizing also the unique valuation definable from G^{00}. Then we use Lemma 2.24 to prove 1-basedness or non-1-basedness of G/G^{00}, either by constructing a definable bijection from G/G^{00} onto a group already studied in Chapter 3, or by using internality to the residue field of the real closed valued field obtained by adding a predicate for G^{00}.

If E is an elliptic r-curve, its equation is $y^2 = (x - e_1)(x - e_2)(x - e_3)$ with $e_i \in M$, $i = 1, 2, 3$. 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 at $(0, 0)$: $y^2 = x(x-e_2')(x-e_3')$, 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 $v(e''_2) = 0, v(e''_3) \geq 0$, 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 $\epsilon \neq \epsilon' \in M$ such that they define curves in the same isomorphism class).

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 $\mathrm{Fin}\setminus\mu$, thus the determinant has valuation $v(\Delta) = v(16 \cdot 1^2 \cdot \epsilon^2 \cdot (\epsilon+1)^2) = 2v(\epsilon) + 2v(\epsilon+1)$. 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 (3) in Proposition 4.3 with $v(u) \neq 0$ would send -1 to either μ or to $M \setminus \mathrm{Fin}$, 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: given $P, Q \in E(M)^0$, $P \neq Q$:

$$x_{P\oplus Q} = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - (1-\epsilon) - x_Q - x_P, \tag{6}$$

$$x_{[2]P} = \frac{(x_P^2 + \epsilon)^2}{4x_P(x_P+1)(x_P-\epsilon)}. \tag{7}$$

We can also explicitly define an ordering $\lhd$ on $E(M)^0$:

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

Observe that this definition is compatible with $\oplus$: we remark that $\ominus P$ is the other intersection point of the vertical line passing through P and the elliptic curve, and so $P \rhd O \Rightarrow \ominus P \lhd O$.

Moreover we have the following fact, that will be fundamental in the computations below:

FACT 4.5. *Given* T_4 *and* $\ominus T_4$ *the 4-torsion points with projection on the y-axis positive and negative respectively, if* $O \lhd P \unlhd Q \lhd T_4$ *then* $O \lhd P \unlhd Q \lhd P \oplus Q$.

PROOF. We consider the geometric definition of the operation $\oplus$, if $O \lhd P \unlhd Q \lhd T_4$, the line between P and Q (or the tangent line to P if $P = Q$) intersects $E(M)$ in a point R such that $y_R < 0$ and $x_R < x_Q, x_P$ (it is sufficient to observe that the slope of such line has to be negative). Therefore $P \oplus Q = R'$ ($[2]P = R$) and the intersection of the vertical line through R and $E(M)$ has $y_{R'} > 0$ and $x_{R'} < x_Q, x_P$. Thus $Q \lhd P \oplus Q$ ($P \lhd [2]P$). □

Immediate consequences are the following:

- $O \lhd P \lhd Q \lhd T_4$, then $x_{P\oplus Q} < x_Q$ and $v\left(x_{P\oplus Q}\right) \geq max\left\{v\left(x_P\right), \left(x_Q\right)\right\}$.
- $O \lhd P \lhd T_4$, then $x_{[2]P} < x_P$ and $v\left(x_{[2]P}\right) \geq v\left(x_P\right)$.
- $O \rhd P \rhd Q \rhd \ominus T_4$, then $x_{P\oplus Q} < x_Q$ and $v\left(x_{P\oplus Q}\right) \geq max\left\{v\left(x_P\right), \left(x_Q\right)\right\}$.
- $O \rhd P \rhd \ominus T_4$, then $x_{[2]P} < x_P$ and $v\left(x_{[2]P}\right) \geq v\left(x_P\right)$.

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

REMARK 4.6. We obtain three kinds of curves:

(1) Good reduction curves: if $v(\epsilon) = 0$ and $v(\epsilon + 1) = 0$, this implies that the standard part of the root $(\epsilon, 0)$ (i.e., $(st(\epsilon), 0)$) does not coincide with any of the other roots, and therefore the reduced curve is nonsingular.
(2) Non-split multiplicative reduction curves: if $v(\epsilon + 1) > 0$ (and so $v(\epsilon) = 0$), 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 (i.e. a singularity of multiplicity 2 and complex slopes).
(3) Split multiplicative reduction curves: if $v(\epsilon) > 0$ (and so $v(\epsilon+1) = 0$) and $\epsilon > 0$, 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 (i.e. a singularity of multiplicity 2 and real slopes).

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

We proved that any elliptic r-curve is isomorphic to a curve of the form $y^2 = x(x+1)(x-\epsilon)$ with $\epsilon \in \text{Fin}$.

Our first step is to determine the cut on M produced by G^{00} (or, better, by its projection onto the first coordinate). In order to compute it we need to consider a sequence of torsion points. We recall that a torsion point is a point T such that $[n]T = O$ for some $n \in \omega$.

Definition 4.7. We call *bounding sequence of torsion points* the sequence $(T_n)_{2<n<\omega}$ of torsion points so defined: T_n is the smallest positive n-torsion point in the order $\lhd$, i.e., $[n]T_n = O$ and there is no other point T such that $O \lhd T \lhd T_n$ and T is an n-torsion point.

The reason of defining such sequence is that, since by Lemma 3.1:

$$G^{00} = \bigcap_{n\in\omega} \{P | \forall T \left[(T \rhd O \wedge [n]T = O) \rightarrow \ominus T \lhd P \lhd T \right] \}, \tag{8}$$

we can determine G^{00} using the torsion point is the bounding sequence:

$$G^{00} = \cap_{2<n<\omega} \{T | \ominus T_n \lhd T \lhd T_n \}. \tag{9}$$

Moreover the sequence above has the following properties (easy to verify, using Fact 4.5):

(1) For $i < j < \omega$, $x_{T_i} < x_{T_j}$.
(2) For $i < j < \omega$, $y_{T_i} < y_{T_j}$.
(3) For $i < j < \omega$, $T_i \rhd T_j$.

In the computations we shall often use a subsequence of the bounding sequence: $(T_{2^n})_{n\in\omega}$, on which it is possible to use the duplication formula (7).

We know that the root of G is either $(0,0)$ or $(\epsilon, 0)$, if $\epsilon < 0$ or $\epsilon > 0$ respectively, by the study of minimal forms for r-curves.

It is convenient to compute separately the projection of the 4-torsion points T_4; the 4-torsion points have a valuation that is meaningful to determine G^{00}. We shall then compute inductively an approximation of $x_{T_{2^n}}$ for $n \in \omega$.

Lemma 4.8. *The 4-torsion points of G are $(\sqrt{-\epsilon}, \pm\sqrt{1-\epsilon+2\sqrt{-\epsilon}})$ if $\epsilon < 0$, and $(\epsilon+\sqrt{\epsilon}\sqrt{\epsilon+1}, \sqrt{\epsilon\sqrt{\epsilon+1}(\sqrt{\epsilon}(2+\epsilon)+\sqrt{\epsilon+1}(2\epsilon+1))}$ if $\epsilon > 0$.*

Proof. We split the proof in the two cases: $\epsilon < 0$ and $\epsilon > 0$.

- If $\epsilon < 0$ (so $T_2 = (0,0)$), 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

$$x^2 + (1-\epsilon-\alpha^2)x - \epsilon = 0. \tag{10}$$

  The α must then satisfy $(1-\epsilon-\alpha^2)^2+4\epsilon = 0$, so $\alpha^2 = 1-\epsilon\pm2\sqrt{-\epsilon}$; we take the positive root to obtain the tangent to G (otherwise, taking the negative root, we obtain the tangent to the semialgebraic component $E(M) \setminus G$).

  Substituting into the solution of (10) we get $x = \frac{1-\epsilon+2\sqrt{-\epsilon}+\epsilon-1}{2} = \sqrt{-\epsilon} = x_{T_4}$. Thus $T_4 = (\sqrt{-\epsilon}, +\sqrt{1-\epsilon+2\sqrt{-\epsilon}})$ and $\ominus T_4 = (\sqrt{-\epsilon}, -\sqrt{1-\epsilon+2\sqrt{-\epsilon}})$.
- If $\epsilon > 0$ (so $T = (\epsilon, 0)$), 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 $x_{T_4} = \epsilon+\sqrt{\epsilon}\sqrt{\epsilon+1}$.

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

□

Before proving the main lemma we do the following observation:

OBSERVATION 4.9. If E has $v(\epsilon) > 0$, there is an elliptic curve $E' : y^2 = x(x+1)(x-\epsilon')$ isomorphic to E with $v(\epsilon') > 0$ and $\epsilon' > 0$.

In fact if $\epsilon < 0$ we can apply to $E : y^2 = x(x-1)(x+\epsilon)$ the homothety:

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

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 4.3.

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

We recall now and we shall often use without further mention the following fact: if $v(a) \neq v(b)$ or $\mathrm{sign}(a) = \mathrm{sign}(b)$, then $v(a+b) = \min\{v(a), v(b)\}$.

LEMMA 4.10. *Let E be a curve in the form $y^2 = x(x+1)(x-\epsilon)$, $G = E(M)^0$. 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.

We consider a bounding sequence of torsion points T_n, thus $x_{T_n} > x_{T_i}$ for $i < n$, $v\left(x_{T_{n+1}}\right) \leq v\left(x_{T_n}\right)$ and $y_{T_n} \geq 0$ for all $n \in \omega$.

We have two cases:

(1) $v(\epsilon) = 0$, i.e., ϵ is not infinitesimally 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, by 9.

The first part is easy, by inspecting the bounding sequence of torsion points of Definition 4.7, the second is equivalent to the statement that for each $s \in \mathrm{Fin}$ we can find a torsion point whose projection onto the x-axis is greater than s; it suffices to prove that for some

$n \in \mathbb{N}$ the point P such that $x_P = s$ has $x_{[n]P} \leq x_{T_4}$. In fact this implies that for some n, $x_P \leq x_{T_{2^{n-2}}}$, by Fact 4.5, i.e. $P \rhd T_{2^{n-2}}$, thus $P \notin G^{00}$ by 9.

We have two sub-cases:

- $\epsilon > 0$, so $x_{T_4} = \epsilon + \sqrt{\epsilon}\sqrt{\epsilon+1} > 2\epsilon$ by Lemma 4.8. 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 define a sequence of points p_i using the formula above, setting $p_0 = x_P$ and defining $p_i = \frac{p_0}{2^i} + \frac{\sum_{j=0}^{i-1} 2^i}{2^{i+4}\epsilon} = \frac{p_0}{2^i} + \frac{2^i-1}{(2-1)2^{i+4}\epsilon} = \frac{p_0}{2^i} - \frac{1}{2^{i+4}\epsilon} + \frac{1}{16\epsilon}$. Observe then that for each i, $p_i \geq x_{[2^i]P}$. 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 $x_{T_4} = \sqrt{-\epsilon}$ by Lemma 4.8. 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 Observation 4.9, $\epsilon > 0$, 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 n-torsion points (n even) from a bounding sequence can be then written as:

$$x_{T_{n/2}} = \frac{1}{4}\frac{x_{T_n}^4 + 2\epsilon x_{T_n}^2 + \epsilon^2}{x_{T_n}^3 + (1-\epsilon)x_{T_n}^2 - \epsilon x_{T_n}}. \tag{11}$$

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 2^n be the smallest such that $v(x_{T_{2^n}}) \leq 0$. Then $v\left(x_{T_{2^{n-1}}}\right) = 2v(x^2_{T_{2^n}}) - v(x_{T_{2^n}}) - v(x_{T_{2^n}} + 1) - v(x_{T_{2^n}}) = 4v(x_{T_{2^n}}) - 3v(x_{T_{2^n}}) = v(x_{T_{2^n}}) \leq 0$, contradicting our assumption that $T_{2^{n-1}} \lhd T_{2^n}$ and $y_{T_{2^n}}, y_{T_{2^{n-1}}} > 0$.
- 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 $\frac{1}{2}v(\epsilon) = v(x_{T_4}) = 2v(x^2_{T_8} + \epsilon) - v(x_{T_8}) - v(x_{T_8} + 1) - v(x_{T_8} - \epsilon) \geq 2v(\epsilon) - \frac{1}{2}v(\epsilon) - \frac{1}{2}v(\epsilon) = v(\epsilon)$, 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 above we get $v(x_{T_{2^{n-1}}}) = 2v(x^2_{T_{2^n}}) - v(x_{T_{2^n}}) - v(x_{T_{2^n}}) = 2v(x_{T_{2^n}})$, i.e., $v(x_{T_{2^n}}) = \frac{1}{2}v(x_{T_{2^{n-1}}})$.

By Lemma 4.8, $v(x_{T_4}) = \frac{1}{2}v(\epsilon)$. Applying this and $v(x_{T_n}) = \frac{1}{2}v(x_{T_n})$ in 9 we obtain $G^{00} = \bigcap_{n \in \omega} \left\{P \in G | v\left(x_P\right) < \frac{1}{n}v(\epsilon)\right\}$.

□

We recall that a *valuational cut* in a structure $(N, +, 0, <, \dots)$ expanding an ordered group is a cut α such that there is $\epsilon \in N$, $\epsilon > 0$, for which $\alpha + \epsilon = \alpha$. By Theorem 6.3 of [**19**], if N is a weakly o-minimal expansion of an ordered field with a definable valuational cut, then N has a nontrivial definable convex valuation.

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 a unique valuation w, not necessarily the standard one, associated to G^{00}, definable in $M' = (M, G^{00}, \dots)^{eq}$.

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

We have three possible kinds of reduction; see Remark 4.6.

2.2. 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 $\tilde{E}(\mathbb{R}) : y^2 = x(x+1)(x - st(\epsilon))$.

Clearly then $E(M) = E_0(M)$, and, by Lemma 4.10,

$$E_1(M) = \{P \in E(M) | v(x_P) < 0\} = G^{00}.$$

This, together with Proposition 4.4, implies that

$$G/G^{00} = E(M)^0/E(M)^{00} = E_0(M)^0/E_1(M)^0 \cong \tilde{E}^0(\mathbb{R}). \qquad (12)$$

We add now to M a predicate for G^{00} as in Chapter 3: let $M' = (M, G^{00}, \dots)^{eq}$. We can define in it the sets Fin and μ:

$$\mathrm{Fin} = \left\{x \in M | \forall y \in M \Big((x,y) \notin G^{00} \wedge (-x,y) \notin G^{00} \Big) \right\}, \qquad (13)$$

$$\mu = \left\{x \in M | x^{-1} \notin \mathrm{Fin} \right\}. \qquad (14)$$

Clearly in the standard real closed valued field $M_v = (M, \mathrm{Fin}, \mu, v, \dots)^{eq}$ the set G^{00} is definable, so M' is interdefinable with M_v; since the standard part map is definable in M', then also the isomorphism $G/G^{00} \cong \tilde{E}(\mathbb{R})^0$ is definable.

Moreover G/G^{00} is definably isomorphic to a definable set in k_v and it is clearly internal to k_v in M'. By Remark 2.26 k_v is non-1-based in $M_v = M'$ and by Lemma 2.24 also G/G^{00} is non-1-based in M'.

2.3. The non-split multiplicative reduction case. In this case we have a curve $E : y^2 = x(x+1)(x-\epsilon)$, with $v(\epsilon+1) > 0$ and $v(\epsilon) = 0$, 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 $G^{00} = \{P \in G | v(x_P) < 0\} = E_1(M)^0 = E_1(M)$ and $G = E_0(M)^0 = E_0(M)$.

We can use the same argument as in the good reduction case to prove non-1-basedness of G/G^{00}. By Proposition 4.4 and Lemma 4.10 we have that $G/G^{00} = E_0(M)^0/E_1(M)^0 \cong \tilde{E}(\mathbb{R})^0$ as abelian groups.

Again the structure $M' = (M, G^{00})$ defines Fin and μ and so we find that M' is interdefinable with the standard real closed valued field M_v, the isomorphism $G/G^{00} \cong \tilde{E}(\mathbb{R})^0$ is definable, and that G/G^{00} is internal to $k_v = \mathbb{R}$. Thus, by Lemma 2.24, G/G^{00} inherits non-1-basedness from k_v.

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

LEMMA 4.11. *Given an elliptic curve E in minimal form, and such that $E(M)$ has good or nonsplit multiplicative reduction, the group G/G^{00}, where $G = E(M)^0$, is non-1-based in $M' = (M, G^{00}, \dots)$ and is internal to k_v, the residue field of the standard real closed valued field, interdefinable with M'.*

We highlight now what is the actual Lie group structure of G/G^{00}. By Proposition 4.4, 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 [**33**]: 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 it 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, so that 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 [**33**]. 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 the full set of M-points of an elliptic curve with non-split multiplicative reduction $E(M)$ and the functor $\mathbb{L} : E(M) \to E(M)/E(M)^{00}$. With the algebraic geometric reduction we obtain a connected component isomorphic to $SO_2(\mathbb{R})$ and an isolated point $(-1, 0)$ (see [**33**] exercise 3.5, page 104 for details), whereas the image under the functor $\mathbb{L}$ is instead a nonsingular curve with the two connected components in bijection (via the map $x \mapsto \frac{x-\epsilon}{x+1}$), and therefore both isomorphic to $SO_2(\mathbb{R})$.

2.4. 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 $\left([\epsilon, \frac{1}{\epsilon}), \cdot\ mod\ \epsilon^2\right)$ (the truncation of the multiplicative group by ϵ). Theorem 3.7 states that the group H/H^{00} is 1-based in $M_{H^{00}} = (M, H^{00}, \dots)^{eq}$.

To obtain 1-basedness for G/G^{00} in $M' = (M, G^{00}, \dots)$ from the known case of the "big" multiplicative truncation, it will suffice, by Lemma 2.24, to show that $M_{H^{00}}$ is interdefinable with M', 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 P is a representative. Analogously with x we denote an element of H and with $x_\sim$ we denote an element 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 4.12. *The map f_* sends G^{00} to H^{00}.*

PROOF. We recall Lemma 4.10:
$G^{00} = \bigcap_{n\in\omega} \{P|\ \forall T \rhd O, [n]T = O \Rightarrow \ominus T \lhd P \lhd T\} =$
$\bigcap_{n\in\omega} \left\{P|\ v(x_P) < \frac{1}{n}v(\epsilon)\right\}$. And it is 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 characterize $(T_2)_\sim$ via the valuation of the projection of its points on the x-axis.

LEMMA 4.13. *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 $v(x_{P\ominus T_2}) < \frac{1}{n}v(\epsilon)$, for all n.

Then, using Formula (6),
$v(x_{P\ominus T_2}) = v\left(\frac{y_P^2}{(x_P-\epsilon)^2} - 1 + \epsilon - x_P - \epsilon\right) = v\left(\frac{x_P(x_P+1)(x_P-\epsilon)}{(x_P-\epsilon)^2} - 1 - x_P\right) =$
$v\left(\frac{x_P^2+x_P-x_P+\epsilon-x_P^2+x_P\epsilon}{x_P-\epsilon}\right) = v(\epsilon) + v(1 + x_P) - v(x_P - \epsilon)$.

Since $v(1 + x_P) = 0$ and since $P \in (T_2)_\sim$ implies that $v(x_{P\ominus T_2}) < \frac{1}{n}v(\epsilon)$, we have that $v(\epsilon) - v(x_P - \epsilon) < \frac{1}{n}v(\epsilon)$, for all n. Therefore $-v\left(\frac{x_P}{\epsilon} - 1\right) < \frac{1}{n}v(\epsilon)$, from which we get the Lemma. □

It is now easy to prove the following lemma:

LEMMA 4.14. *The function f is well defined for $(T_2)_\sim$, i.e., if $P \in (T_2)_\sim$, then $f_*(P) \cdot f_*(T_2)^{-1} \in H^{00}$.*

PROOF. Observe that $f_*(T_2) = \frac{1}{\epsilon}$, and that if $y_P > 0$, then $f_*(P) = \frac{1}{x_P}$. So $f_*(P)f_*(T_2)^{-1} = \frac{\epsilon}{x_P}$, thus $f_*(P)f_*(T_2)^{-1}$ 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 $0 \geq v(\frac{x_P}{\epsilon}) > \frac{1}{n}v\left(\frac{1}{\epsilon}\right)$ 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 $v\left(\frac{x_P}{\epsilon}\right) < \frac{1}{k}v\left(\frac{1}{\epsilon}\right)$ for some $k \in \omega$, $v\left(\frac{x_P}{\epsilon}\right) < 0$, then $v\left(\frac{x_P}{\epsilon} - 1\right) = v\left(\frac{x_P}{\epsilon}\right) < \frac{1}{k}v\left(\frac{1}{\epsilon}\right)$, contradicting $P \in (T_2)_\sim$. Thus $f_*(P) \cdot f_*(T_2)^{-1} \in H^{00}$.

□

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

THEOREM 4.15. *The map $f : *$ induces a well defined function $f : G/G^{00} \to H/H^{00}$.*

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

$$v(x_P) < \frac{1}{n_P}v(\epsilon) \textit{ and } v(x_Q) < \frac{1}{n_Q}v(\epsilon) \textit{ for some } n_P, n_Q \in \mathbb{N}. \qquad (15)$$

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 $v(x_Q) > v(\epsilon)$, contradicting Equation (15).

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

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 $(y_P + y_Q)^2 = y_P^2 \left(1 + \frac{y_Q}{y_P}\right)^2 = y_P^2 \left(1 + \sqrt{\frac{x_Q}{x_P}} \sqrt{\frac{x_Q+1}{x_P+1}} \sqrt{\frac{x_Q-\epsilon}{x_P-\epsilon}}\right)^2$, 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 $(*) < \frac{1}{n} v(\epsilon)$, for all n, 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 $(*) = v(x_P^2) - v(x_P) = v(x_P)$, or $(*) = v(x_Q) - v(x_P) = v(h)$; if the former happens $(*) < \frac{1}{n}v(\epsilon)$ for all n, which contradicts (15), if the latter $v(h) = (*) < \frac{1}{n}v(\epsilon)$ 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 of Theorem 4.15.

□

Easy to check now is

COROLLARY 4.16. *The map f is a bijection.*

PROOF. Surjectivity: trivial by construction.

Injectivity: Suppose $f(P_\sim) = f(Q_\sim)$. By 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. $\square$

A natural and seemingly easy, but involving hard computations is the following question:

QUESTION 4.17. *Is f a group isomorphism $G/G^{00} \to H/H^{00}$?*

In Section 3 it was highlighted how the structure $(M, H^{00}, \dots)$ is interdefinable with a nonstandard real closed field M_w, whose valuation is w and how H/H^{00} is a definable subset of Γ_w in M_w. Hence the bijection f together with Lemma 2.24 implies the following theorem:

THEOREM 4.18. *Given an elliptic r-curve E with split multiplicative reduction, let $G = E(M)^0$, then the group G/G^{00} is 1-based in the structure $M' = (M, G^{00}, \dots)^{eq}$.*

3. Elliptic c-curves

This is the case where the curve is defined by $E : y^2 = (x-e_1)(x-e_2)(x-\overline{e_2})$, $e_1 \in M$, $e_2 \in M[i]$. If either e_1 or $|e_2|$ are not in Fin, then we can find

$u > 0$ ($\in M$) such that $v(u^2) = -min\{v(e_1), v(e_2)\}$, and apply

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

With this transformation we can suppose both e_1 and $|e_2|$ are in Fin.

Applying then the transformation

$$\begin{cases} x' = x + e_1, \\ y' = y. \end{cases}$$

we get $y^2 = x(x - e)(x - \overline{e})$ where $e = e_1 + Re(e_2) + i[Im(e_2)] \in M[i]$.

Observe that since $v(|e|) = v\left(\sqrt{Re(e)^2 + Im(e)^2}\right) =$

(since squares are positive, and so we get the equality in the valuation)

$= \frac{1}{2}min\{2v(Re(e)), 2v(Im(e))\} = min\{v(Re(e)), v(Im(e))\}$,

and, since $v(|e|) \geq 0$, we get both $Re(e), Im(e) \in Fin$.

To obtain a minimal equation we calculate the determinant Δ: for $y^2 = x(x^2 - 2Re(e)x + |e|^2)$, $\Delta = 64|e|^4(Re(e)^2 - |e|^2) = -64|e|^4 Im(e)^2$, so its valuation is $v(\Delta) = 4v(|e|) + 2v(Im(e))$. It is minimized when $v(Im(e)) = 0$, so $Im(e) \in Fin \setminus \mu$. For simplicity of calculation we can canonically put $Im(e) = 1$.

The transformation to obtain such $Im(e)$ is

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

where u is such that $u^2 = \frac{1}{|e|}$ (we can find such u, since $|e| > 0$).

The resulting equation can be written either as $E : y^2 = x(x-e)(x-\overline{e})$, where $e \in M[i]$ and $|e| = 1$, or as $E : y^2 = x(x^2 - 2rx + 1)$, where $r \in M$ is $Re(e)$. With the latter equation Δ is simply $1 - r^2$.

We have then proved:

LEMMA 4.19. *Any elliptic c-curve is isomorphic to a curve of the form* $E : y^2 = x(x^2 - 2rx + 1)$*, with* $-1 < r < 1$*. Moreover such a curve is in minimal Weierstrass form.*

For such curves the sum and doubling formulae assume the following form:

$$x_{P\oplus Q} = \frac{(y_Q + y_P)^2}{(x_Q - x_P)^2} + 2r - x_P - x_Q, \tag{16}$$

$$x_{[2]P} = \frac{(x_P^2 - 1)^2}{4x_P(x_P^2 - 2rx_P + 1)}. \tag{17}$$

The definition of the ordering is the same as in the r-curve case.

We consider its M-points, so let $G = E(M)$. (Observe that in this case $E(M) = E(M)^0$).

The torsion point T_2 is $(0,0)$ and we can easily compute $T_4 = (1, \sqrt{2(1-r)})$ and $\ominus T_4 = (1, -\sqrt{2(1-r)})$: to obtain these values this we solve

$$\begin{cases} y = \alpha x, \\ y = x^3 - 2rx^2 + x, \end{cases}$$

with $\Delta = 0$, so we get $\alpha^2 x = x^2 - 2rx + 1$. Imposing $\Delta = 0$ we get $\alpha^2 = \pm 2(1-r)$, from which we get $x = \pm 1$. We can exclude $x = -1$ since on substitution we would get $y = \sqrt{-2(1+r)}$, which leads to a "complex" y (in fact $1 + r = \sqrt{r^2 + Im(e)} + r \geq 0$, so $-2 - 2r < 0$, and its square root is "complex").

We have then only two kinds of reduction for curves of such form:

(1) either the curve E has good reduction, if $v(1-r) = 0$, or
(2) it has split multiplicative reduction, if $v(1-r) > 0$.

3.1. Computing G^{00}. As in the previous section we compute G^{00} in terms of the standard valuation.

LEMMA 4.20. *Let E be a curve in the form $y^2 = x^3 - 2rx^2 + x$ and $G = E(M)$. Then* $G^{00} = \bigcap_{n\in\omega}\{P \in G | v(x_P - 1) < \frac{1}{n}v(r-1) \wedge x_P > 1\} = \bigcap_{n\in\omega}\{P \in G | v(y_P) < \frac{1}{n}v(r-1) \wedge x_P > 1\}$.

PROOF. The proof is similar to the computation of G^{00} in the r-curve case: Lemma 4.10. We recall that, by Lemma 3.1,

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

By using the bounding sequence of torsion points defined in Definition 4.7, we obtain again that

$$G^{00} = \cap_{2<n<\omega}\{T| \ominus T_n \lhd T \lhd T_n\}. \tag{18}$$

Recall that the 4-torsion points are $T_4 = (1, +\sqrt{2(1-r)})$ and $\ominus T_4 = (1, -\sqrt{2(1-r)})$.

We find now a general formula for the valuation of the 2^n-torsion points.

By Equation (17) $v(x_{T_{2^{n-1}}}) = 2v(x^2_{T_{2^n}} - 1) - v(x_{T_{2^n}}) - v(x^2_{T_{2^n}} - 2rx_{T_{2^n}} + 1)$. We work by induction for $n > 2$, considering, for symmetry reasons, only the torsion points with $x_{T_n} > 1$, $y_{T_n} > 0$, and $T_n \rhd T_{n+1}$; therefore we can suppose $v(x_{T_{2^{n-1}}}) = 0$ and $v(x_{T_{2^n}}) \leq 0$.

If $v(x_{T_{2^n}}) < 0$ then $v(x_{T_{2^{n-1}}}) = 4v(x_{T_{2^n}}) - v(x_{T_{2^n}}) - 2v(x_{T_{2^n}}) = v(x_{T_{2^n}}) < 0$ contradicting the inductive hypotesis.

So $v(x_{T_{2^n}}) = 0$.

We distinguish 2 cases: either $v(r-1) = 0$ or $v(r-1) > 0$.

(1) If $v(r-1) = 0$, i.e., $v(y_{T_4}) = 0$ and $E(M)$ has good reduction. We want to prove that supposing $v(x_{T_{2^{n-1}}} - 1) = 0$, we get $v(x_{T_{2^n}} - 1) = 0$. Then, observing that $v(x^2_{T_{2^n}} - 1) = v(x_{T_{2^n}} - 1) + v(x_{T_{2^n}} + 1) = v(x_{T_{2^n}} - 1)$, we get $0 = v(x_{T_{2^{n-1}}}) = 2v(x^2_{T_{2^n}} - 1) - v(x^2_{T_{2^n}} - 2rx_{T_{2^n}} + 1) = 2v(x_{T_{2^n}} - 1) - v\left((x_{T_{2^n}} - 1)^2 + 2(1-r)x_{T_{2^n}}\right)$.

Since $(x_{T_{2^n}} - 1)^2 > 0$, $2(1-r)x_{T_{2^n}} > 0$ and $v(1-r) = 0$, $v\left((x_{T_{2^n}} - 1)^2 + 2(1-r)x_{T_{2^n}}\right) = min\{v((x_{T_{2^n}} - 1)^2), v(2(1-r)x_{T_{2^n}})\} = 0$. Thus $0 = 2v(x_{T_{2^n}} - 1) + 0$, and so $v(x_{T_{2^n}} - 1) = 0$, as demanded.

We have to prove now that the torsion points of a bounding sequence have projection and are cofinal in $Fin^{>0}$.

As in the proof of Lemma 4.10, we prove that if $x_P > x_{T_4}$ then there is $n \in \omega$ such that $x_{[2^n]P} \leq x_{T_4}$. By Formula (17), and since $r < 1 < x_P$, $x_{[2]P} = \frac{(x_P^2-1)^2}{4x_P(x_P^2-2rx+1)} < \frac{2x_P(x_P+1)(x_P-1)^2}{4x_P(x_P^2-2x+1)} = \frac{(x_P+1)(x_P-1)^2}{2(x_P-1)^2} = \frac{x_P}{2} + \frac{1}{2}$. This clearly implies that by iterating the duplication formula finitely many times we obtain that $x_{[2^n]P} \leq x_{T_4}$, for some n.

(2) If $v(r-1) > 0$, we proceed in computing the 8-torsion points. Since $x_{T_4} = 1$, $1 = x_{T_4} = \frac{(x_{T_8}^2-1)^2}{4x_{T_8}(x_{T_8}^2-2rx_{T_8}+1)}$, i.e., $x_{T_8}^4 - 4x_{T_8}^3 + 2(4r-1)x_{T_8}^2 - 4x_{T_8} + 1 = 0$. Let $x_{T_8} = 1 + s$; substituting this in the equation we obtain $s^4 = 8(1-r)(1+s)^2$. Since we supposed $v(1+s) = 0$ and $v(1-r) > 0$ we have $v(x_{T_8} - 1) = v(s) = \frac{1}{4}v(1-r) > 0$.

We compute now $v(x_{T_{2^n}})$. Let $1 + t = x_{T_{2^{n-1}}}$ and $1 + s = x_{T_{2^n}}$. Equation (17) becomes now $1 + t = \frac{((1+s)^2-1)^2}{4(1+s)((1+s)^2-2r(1+s)+1)}$, thus $s^4 = 4t\left((1+s)^3 - 2r(1+s)^3 + (1+s)\right) - 8(1+s)^2(1-r)$.

Before proceeding in the computation, we recall that by inductive hypothesis $v(s) \leq v(t) \leq \frac{1}{4}v(1-r)$.

Consider firstly $((1+s)^3 - 2r(1+s)^3 + (1+s)) =$
$= (2(1+s)^2(1-r) + s^2(1+s))$; we have $v(1+s) = 0$ and $v(s^2) = 2v(s) < v(1-r)$.

Therefore $v\left(4t\left(2(1+s)^2(1-r) + s^2(1+s)\right)\right) = v(t) + 2v(s)$.

On the other hand $v(8(1+s)^2(1-r)) = v(1-r)$, and, since $v(t) + 2v(s) < v(1-r)$, we get $v(s^4) = 4v(s) = v(t) + 2v(s)$, from which $v(s) = \frac{1}{2}v(t)$, i.e., $v(x_{T_{2^n}} - 1) = \frac{1}{2}v(x_{T_{2^{n-1}}} - 1)$. An induction argument similar to the one in Lemma 4.10 proves that $G^{00} = \bigcap_{n\in\omega}\{P \in G | v(x_P - 1) < \frac{1}{n}v(r-1) \wedge x_P > 1\}$.

To prove that $G^{00} = \bigcap_{n\in\omega}\{P \in G | v(y_P) < v(r-1) \wedge x_P > 1\}$ we observe that $v(y_P) = \frac{1}{2}[v(x_P) + v(x_P^2 - 2rx_P + 1)] = \frac{1}{2}v\left((x_P-1)^2 + 2x_P(1-r)\right)$. Since $v(x_P - 1) < \frac{1}{n}v(r-1)$, we easily get that $v(y_P) = v(x_P - 1)$.

□

3.2. The good reduction case. If $E(M)$ has good reduction, $v(1-r) = 0$. Thus the algebraic geometric reduction leads to an elliptic curve $\tilde{E}(\mathbb{R})$ defined by $y^2 = x(x^2 - 2st(r)x + 1)$.

Thus $E(M) = E_0(M)$, and by Lemma 4.20, $E_1(M) = \{P \in E(M) | v(x_P) < 0\} = \{P \in E(M) | v(x_P - 1) < 0\} = G^{00}$.

Again this and Proposition 4.4 imply that

$$G/G^{00} = E(M)^0/E(M)^{00} = E_0(M)^0/E_1(M)^0 \cong \tilde{E}^0(\mathbb{R}). \tag{19}$$

As in the good reduction case for the elliptic r-curves, M' is interdefinable with the standard real closed valued field M_v; G/G^{00} is internal to k_v, and, by Lemma 2.24, G/G^{00} is non-1-based in M'.

3.3. The split multiplicative reduction case. Suppose $E(M)$ has split multiplicative reduction, i.e., $v(1-r) > 0$.

We want to construct a definable bijection of G/G^{00} with a group we know is 1-based. We can just consider a restriction of G to a subset of M^2: the box B determined on M^2 by the convex sets $\mu + 1$ on the x-axis and μ on the y-axis, this allows to exclude most points that aer either in G^{00} or in the class of the 2-torsion point. We shall prove that there is a representative in this box for each element of G/G^{00}; this is an easy consequence of the computation of the classes G^{00} and $(T_2)_\sim$.

We then compute $(T_2)_\sim$.

LEMMA 4.21. $(T_2)_\sim = \bigcup_{n\in\omega} \{P \in G | v(1 - x_P) < \frac{1}{n} v(1-r) \wedge x_P < 1\}$.

PROOF. A point P is in $(T_2)_\sim$ if and only if $v\left(x_{P\ominus T_2} - 1\right) < \frac{1}{n} v(1-r)$ for all $n \in \omega$. By Equation (16) $v\left(x_{P\ominus T_2} - 1\right) = v\left(\frac{y_P^2}{x_P^2} + 2r - x_P - 1\right) = v\left(\frac{x_P(x_P^2 - 2rx_P + 1)}{x_P^2} + 2r - x_P - 1\right) = v(x_P - 1) - v(x_P)$.

If $v(x_P) > 0$, then $v(x_P - 1) = 0$, and $v\left(x_{P\ominus T_2} - 1\right) = v(x_P - 1) - v(x_P) = -v(x_P) < 0 < \frac{1}{n} v(1-r)$, for all n. Thus $P \in (T_2)_\sim$.

If $v(x_P) = 0$, then $v\left(x_{P \ominus T_2} - 1\right) = v(1 - x_P)$, therefore $P \in (T_2)_\sim$ if and only if $v\left(x_P - 1\right) < \frac{1}{n} v(1 - r)$ for all $n \in \omega$. $\square$

Since G^{00} determines a convex equivalence relation, and from the computation of G^{00} and $(T_2)_\sim$, it is clear that $G \setminus \{G^{00} \cup (T_2)_\sim\} \subset B$ and there is both a representative of G^{00} and one of $(T_2)_\sim$ in B.

We shall need also a characterization of the classes of the 4-torsion points. We compute them now.

LEMMA 4.22. *The 4-torsion points of G/G^{00} are*
$(T_4)_\sim = \bigcap_{n \in \omega} \{P \in G | v(1 - x_P) > \frac{1}{2} v(1 - r) - \frac{1}{n} v(1 - r) \wedge y_P > 0\}$ *and* $(\ominus T_4)_\sim = \bigcap_{n \in \omega} \{P \in G | v(1 - x_P) > \frac{1}{2} v(1 - r) - \frac{1}{n} v(1 - r) \wedge y_P < 0\}$.

PROOF. It is clearly sufficient to compute one of them, $(T_4)_\sim$ say.

A point P is in $(T_4)_\sim$ if $[2]P \in (T_2)_\sim$, i.e., if $v(x_{[2]P} - 1) < \frac{1}{n} v(1 - r)$, for all $n \in \omega$. Working in B we recall that $v(x_P) = 0$.

But $v(x_{[2]P} - 1) = v\left(\frac{(x_P^2 - 1)^2}{4x_P(x_P^2 - 2rx_P + 1)} - 1\right) = v((x_P^2 - 1)^2 - 4x_P(x_P^2 - 2rx_P + 1)) - v((x_P - 1)^2 + 2x_P(1 - r)) = v((x_P - 1)^4 - 8x_P(1 - r)) - v((x_P - 1)^2 + 2x_P(1 - r))$.

Now we could compute this splitting into various cases: $4v(x_P - 1) < v(r - 1)$; $4v(x_P - 1) = v(r - 1)$; $4v(x_P - 1) > v(r - 1)$ and $2v(x_P - 1) < v(r - 1)$; $4v(x_P - 1) > v(r - 1)$ and $2v(x_P - 1) = v(r - 1)$; and $4v(x_P - 1) > v(r - 1)$ and $2v(x_P - 1) > v(r - 1)$. But since the equivalence relation determined by G^{00} is convex, it is sufficient to consider the unique case among those above in which there are both points in $(T_4)_\sim$ and points not in $(T_4)_\sim$.

This is the case $4v(x_P - 1) > v(r - 1)$ and $2v(x_P - 1) < v(r - 1)$; in fact then $v(x_{[2]P}) = v(1 - r) - 2v(1 - x_P)$, and this is in $(T_4)_\sim$ if and only if $v(1-r) - 2v(1-x_P) < \frac{1}{n} v(1-r)$ for all n, i.e. $v(1-x_P) > \frac{1}{2} v(1-r) - \frac{1}{n} v(1-r)$ for all n. This determines the points that are either in class $(T_4)_\sim$ or $(\ominus T_4)_\sim$. $\square$

OBSERVATION 4.23. From now on, when we consider a point $P \notin (T_4)_\sim, (\ominus T_4)_\sim$, we can suppose the following: $v(x_P - 1) < \frac{1}{2}v(1-r)$, and in particular we have $v(x_P^2 - 2rx_P + 1) = 2v(x_P - 1)$.

We define a group H as follows: consider the interval $\left[\sqrt{2(1-r)}, \frac{1}{\sqrt{2(1-r)}}\right)$ and plug two copies of it in M^2, one on the x-axis, and one on the line $y = 1$. The group H is definable in M, since its universe is the set

$$\left\{(x,y)|x \in \left[\sqrt{2(1-r)}, \frac{1}{\sqrt{2(1-r)}}\right), y \in \{0,1\}\right\};$$

the operation is the obvious modular operation having the unit $(1,0)$, the 2-torsion point at $(1,1)$ and seeing this as living in a Möbius band (i.e., we glue together the points $\left(\frac{1}{\sqrt{2(1-r)}}, 1\right)$ and $(\sqrt{2(1-r)}, 0)$, and glue together $\left(\frac{1}{\sqrt{2(1-r)}}, 0\right)$ and $(\sqrt{2(1-r)}, 1)$).

It is immediate to see that H is definably isomorphic to the group

$$H' = \left(\left[2(1-r), \frac{1}{2(1-r)}\right), \cdot \ mod\ 2(1-r)^{-2}\right).$$

(The definable isomorphism $\varphi : H \to H'$ is $\varphi(h,0) = h$, $\varphi(h,1) = \frac{2(1-r)}{h}$ if $h \geq 1$, and $\varphi(h,1) = \frac{1}{2(1-r)h}$ if $h < 1$).

We define a function $f_* : G \restriction B \to H$ and prove that it is well defined and induces a bijection on the quotient $G/G^{00} \to H/H^{00}$ (in the structure (M, G^{00}), after showing it is interdefinable with (M, H^{00})). We denote such map by $f : G/G^{00} \to H/H^{00}$.

$$f_*(P) = \begin{cases} \left(\frac{1}{y_P}, 0\right) & if\ x_P \geq 1 \wedge 0 < y_P < 1, \\ (y_P, 1) & if\ x_P < 1 \wedge 0 < y_P < 1, \\ \left(-\frac{1}{y_P}, 1\right) & if\ x_P < 1 \wedge -1 < y_P \leq 0, \\ (-y_P, 0) & if\ x_P \geq 1 \wedge -1 < y_P \leq 0. \end{cases} \tag{20}$$

We need to study the torsion points of H. In order to compute H^{00}, observe that the 4-torsion points h_4 and h_4^{-1} are $\left(\sqrt{2(1-r)}, 0\right)$ and $\left(\sqrt{2(1-r)}, 1\right)$

respectively, therefore, as seen in Chapter 3, Section 1.2,

$$\begin{aligned} H^{00} = &\ \bigcap_{n\in\omega}\left\{(t,0)|\sqrt{2(1-r)}<t^n<\tfrac{1}{\sqrt{2(1-r)}}\right\}= \\ = &\ \bigcap_{n\in\omega}\left\{(t,0)|-\tfrac{1}{n}v(1-r)<v(t)<\tfrac{1}{n}v(1-r)\right\}. \end{aligned} \tag{21}$$

We compute also the class $(h_2)_\sim$ of the 2-torsion point, and the classes $(h_4^+)_\sim$ and $(h_4^-)_\sim$ of the 4-torsion points.

LEMMA 4.24. *The class* $(h_2)_\sim$ *is*

$$\{(h,1)\in H|(h,0)\in H^{00}\}=\left\{(h,1)\in H|-\frac{1}{n}v(1-r)<v(h)<\frac{1}{n}v(1-r)\right\}.$$

PROOF. To compute, recall that $H\cong H'$, where H' is defined above. Clearly $(H')^{00}=\varphi(H^{00})$, so $(h_2')_\sim=\{\varphi(h)|h^2\in H^{00}\}$. We now compute $(h_2')_\sim$. Let $t\in H'$ such that $t^2\in(H')^{00}$, then it is obvious that either $t>\frac{1}{\sqrt{2(1-r)}}$ or $t<\sqrt{2(1-r)}$. By symmetry we just need to compute the case $t>\frac{1}{\sqrt{2(1-r)}}$, this means $t=\frac{1}{2(1-r)h}$ for some $(h,1)\in H$, with $h<1$. So the condition $t\in(h_2')_\sim$ is equivalent to $t\cdot t\cdot(2(1-r))^2\in(H')^{00}$ (actually it is in the part of $(H')^{00}$ that is less than 1, i.e., $v(t\cdot t\cdot(2(1-r))^2)>-\frac{1}{n}v(1-r)$, for every n); thus $v\left(\frac{(2(1-r))^2)}{h\cdot h\cdot(2(1-r))^2)}\right)>-\frac{1}{n}v(1-r)$, for every n. This clearly means that $v(h)<\frac{1}{n}v(1-r)$ for every n. Analogously $t<\sqrt{2(1-r)}$ implies $v(h)>-\frac{1}{n}v(1-r)$, for every n. Thus $t\in(h_2')_\sim$ if (and only if) its preimage $f^{-1}(t)=(h,1)$ is projected by the map $\iota(s,1)\mapsto(s,0)$ into H^{00}. This proves the statement. □

LEMMA 4.25. $(h_4^+)_\sim=\bigcap_{n\in\omega}\big\{P\in H|\big(P=(x,0)\wedge v(x)<-\frac{1}{2}v(1-r)+\frac{1}{n}v(1-r)\big)\vee\big(P=(x,1)\wedge v(x)>\frac{1}{2}v(1-r)-\frac{1}{n}v(1-r)\big)\big\}$, *and* $(h_4^-)_\sim=\bigcap_{n\in\omega}\big\{P\in H|\big(P=(x,1)\wedge v(x)<-\frac{1}{2}v(1-r)+\frac{1}{n}v(1-r)\big)\vee\big(P=(x,0)\wedge v(x)>\frac{1}{2}v(1-r)-\frac{1}{n}v(1-r)\big)\big\}$.

PROOF. We compute $(h_4^+)_\sim$; it is defined by $(h_4^+)_\sim=\{(x,i)\in H|(x,i)\cdot(x,i)\in(h_2)_\sim\}$, i.e., it is such that $(x,i)\cdot(x,i)=(h,1)$ and $-\frac{1}{n}v(1-r)<v(h)<\frac{1}{n}v(1-r)$. For symmetry reasons we need only to compute the points in $H \restriction (y=0)$ such that $-\frac{1}{n}v(1-r) < v(x \cdot_{mod\ (2(1-r))^{-1}} x) < \frac{1}{n}v(1-r)$, from these it is immediate to deduce $(h_4^+)_\sim$.

If $x > 1$, and therefore $v(x) \leq 0$, $x \cdot_{mod\ (2(1-r))^{-1}} x = x \cdot x \cdot 2(1-r)$, thus by our assumption $v(x) < -\frac{1}{2}v(1-r) + \frac{1}{n}v(1-r)$ for all $n \in \omega$.

Analogously if $x < 1$, and therefore $v(x) \geq 0$, $x \cdot_{mod\ (2(1-r))^{-1}} x = x.x.(2(1-r))^{-1}$, so $v(x) > \frac{1}{2}v(1-r) - \frac{1}{n}v(1-r)$ for all $n \in \omega$.

Putting them together and back on the Möbius strip, $(h_4^+)_\sim = \bigcap_{n\in\omega} \{P \in H | \big(P = (x,0) \wedge v(x) < -\frac{1}{2}v(1-r) + \frac{1}{n}v(1-r)\big) \vee \big(P = (x,1) \wedge v(x) > \frac{1}{2}v(1-r) - \frac{1}{n}v(1-r)\big)\}$. □

We shall now prove that the map f_* is well-defined in the quotient. We firstly check it for G^{00} and the classes of the 2-torsion and 4-torsion points.

Lemma 4.26. *(1) $f_*(G^{00}) = H^{00}$,*
(2) $f_*((T_2)_\sim) = (h_2)_\sim$,
(3) $f_*(T_4)_\sim = (h_4^+)_\sim$, and
(4) $f_*(\ominus T_4)_\sim = (h_4^-)_\sim$.

Proof. (1) In fact, for any P such that $x_P > 1$ we have that the second coordinate of the image is 0. We have two cases:

- If $P \in G^{00}$ and $y_P > 0$, then $f_*(P) = \left(\frac{1}{y_P}, 0\right)$, with $0 \leq v(y_P) < \frac{1}{n}v(r-1)$ for each n (the bound $0 \leq v(y_P)$ is because we work in the restriction of G to B), so $0 \geq \frac{1}{y_P} > -\frac{1}{n}v(r-1)$, so $f_*(P) \in H^{00}$.
- If $P \in G^{00}$ and $y_P < 0$, $f_*(P) = (-y_P, 0)$, with $0 \leq v(y_P) < \frac{1}{n}v(r-1)$, so also $0 \leq v(-y_P) < \frac{1}{n}v(r-1)$, proving that $f_*(P) \in H^{00}$.

It is clear then that $f_*(G^{00}) = H^{00}$.

(2) By (20), given $P \in (T_2)_\sim$ (i.e., $(1-x_P) < \frac{1}{n}v(1-r)$) we have either $f_*(P) = (y_P, 1)$ if $y_P \geq 0$, or $f_*(P) = (-\frac{1}{y_P}, 1)$ if $y_P < 0$. In the former case $v(y_P) = \frac{1}{2}(v(x_P) + v((x_P-1)^2 - 2x_P(1-r))) = \frac{1}{2}(v((x_P-1)^2)) = v(x_P - 1) < \frac{1}{n}v(1-r)$ by our assumption that $P \in (T_2)_\sim$, but then

also $f_*(P) \in (h_2)_\sim$. The latter case is analogous. It is immediate to check that this map is surjective.

(3) Recalling that $v(y_P) = v((x_P-1)^2 + 2x_P(1-r))$, we have two possibilities when $P \in (T_4)_\sim$: either $2v(x_P-1) < v(1-r)$, then $v(y_P) = v(x_P-1) > \frac{1}{2}v(1-r) - \frac{1}{n}v(1-r)$, $f_*(P) = (y_P, 1)$ and $v(y_P) > \frac{1}{2}v(1-r) - \frac{1}{n}v(1-r)$; or $f_*(P) = \frac{1}{y_P}$, and therefore $v\left(\frac{1}{y_P}\right) < -\frac{1}{2}v(1-r) + \frac{1}{n}v(1-r)$, so the image $f_*(P)$ is $(h_4^+)_\sim$.

(4) Analogous to (3) above.

□

We complete now the proof that the map f is a well defined map $f: G/G^{00} \to H/H^{00}$.

THEOREM 4.27. *The map $f: G/G^{00} \to H/H^{00}$ is well defined.*

PROOF. We want to prove that given $P, Q \in G$, $P \sim Q$ if and only if $f_*(P) \sim f_*(Q)$.

By Lemma 4.26 it suffices now to consider the points $P \in G$ that are not in the classes $G^{00}, (T_2)_\sim, (T_4)_\sim, (\ominus T_4)_\sim$, and by symmetry of Equation (16), we can suppose that $0 < v(x_P - 1) < \frac{1}{2}v(1-r)$, $x_P > x_Q$ and $v(x_P) = v(x_Q) = 0$.

By convexity of the equivalence relation we can always suppose either $(T_2)_\sim \lhd P, Q \lhd (\ominus T_4)_\sim$, or $(\ominus T_4)_\sim \lhd P, Q \lhd G^{00}$, or $G^{00} \lhd P, Q \lhd (T_4)_\sim$, or $(T_4)_\sim \lhd P, Q \lhd (T_2)_\sim$. We shall prove in detail the theorem only when $x_P, x_Q > 1$ and $y_P, y_Q > 0$, i.e., when $G^{00} \lhd P, Q \lhd (T_4)_\sim$; the other three cases are analogous.

By (16) and (21), we need to prove that $0 < v\left(x_{P\ominus Q} - 1\right) =$
$= v\left(\frac{(y_P+y_Q)^2}{(x_Q-x_P)^2} + 2r - x_P - x_Q - 1\right) < \frac{1}{n}v(1-r)$, for all n if and only if $-\frac{1}{n}v(1-r) < v\left(\frac{y_Q}{y_P}\right) < \frac{1}{n}v(1-r)$, for all n (or, equivalently, $-\frac{1}{n}v(1-r) < v\left(\frac{x_Q-1}{x_P-1}\right) < \frac{1}{n}v(1-r)$).

We firstly prove LHS implies RHS.

Since if $v(x_P-1) = v(x_Q-1)$ we are done, we can suppose $v(x_P-1) < v(x_Q-1)$, i.e., $v(y_P) < v(y_Q)$. Observe that then $v(x_P - x_Q) = v(1-x_P) < v(1-x_Q)$.

With this consideration LHS leads to an easier supposition (substituting y_Q with y_P and $(x_P - x_Q)^2$ with $(x_Q-1)^2$: $v\left(\frac{(2y_P)^2}{(x_Q-1)^2} + 2r - x_P - x_Q - 1\right) \leq v\left(x_{P\ominus Q} - 1\right) < \frac{1}{n}v(1-r)$. We can rewrite the leftmost formula as $(\diamond) = v(4x_P(x_P^2 - 2rx_P + 1) - (x_P + 2r - x_Q - 1)(x_Q-1)^2) - 2v(x_Q - 1)$.

Since $v(4x_P(x_P^2 - 2rx_P + 1) = 2v(x_P - 1)$, $v((x_P + 2r - x_Q - 1)(x_Q - 1)^2) = 2v(x_Q - 1)$, and by our supposition, $0 > (\diamond) = 2v(x_P - 1) - 2v(x_Q - 1) = v\left(\frac{x_P - 1}{x_Q - 1}\right) > -\frac{1}{n}v(1-r)$. This proves RHS.

We now prove RHS implies LHS.

Observe that $(y_Q + y_P)^2 > y_Q^2 + y_P^2$, that $\frac{1}{(x_P - x_Q)^2} > \frac{1}{(x_P-1)^2}$, and that $2r - x_P - x_Q - 1 > -x_P - 1$ (recall that we have $0 < r < 1 < x_Q < x_P$).

Thus $v(x_{P\ominus Q} - 1) \leq v\left(\frac{y_P^2 + y_Q^2}{(1-x_P)^2} - x_P - 1\right) =$
$= v\left(\frac{y_Q^2}{(1-x_P)^2} + \frac{x_P(x_P-1)^2}{(x_P-1)^2} + \frac{2x_P(1-r)}{(x_P-1)^2} - x_P - 2(x_P - r)\right) =$
$= v\left(\frac{y_Q^2}{(1-x_P)^2} + \frac{2x_P(1-r)}{(x_P-1)^2} - 2(x_P - r)\right) = (*)$.

Now, by RHS, and the choice $x_Q < x_P$, $0 \leq v\left(\frac{y_Q^2}{(1-x_P)^2}\right) < \frac{1}{n}v(1-r)$ for all n; by the fact that $x_P \notin G^{00}$, $v(x_P - r) \geq \frac{1}{m_1}v(1-r)$ for some $m_1 \in \omega$; by the fact that $x_P \notin (T_4)_\sim = \bigcup_{n\in\omega}\{P \in G | v(1-x_P) > \frac{1}{2}v(1-r) - \frac{1}{n}v(1-r) \wedge y_P > 0\}$, $v\left(\frac{y_Q^2}{(1-x_P)^2}\right) = v(1-r) - 2v(x_P - 1) \geq \frac{1}{m_2}v(1-r)$, for some $m_2 \in \omega$. Thus $(*) = v\left(\frac{y_Q^2}{(1-x_P)^2}\right) < \frac{1}{n}v(1-r)$ for all $n \in \omega$; i.e.: $P \ominus Q \in G^{00}$, and this proves LHS.

Thus we have shown that the map $f : G/G^{00} \to H/H^{00}$ is well defined.

□

It is easy now to obtain the following corollary:

COROLLARY 4.28. *The map $f : G/G^{00} \to H/H^{00}$ is a definable bijection.*

By Theorem 3.7 and Lemma 2.24 we obtain that G/G^{00} is 1-based in M', and that it is internal to Γ_w.

We thus obtain the theorem:

Theorem 4.29. *Given an elliptic c-curve E, let $G = E(M)^0$; if E has good reduction, then G/G^{00} is non-1-based in M' and it is internal to k_w; if E has split multiplicative reduction, then G/G^{00} is 1-based in M' and internal to Γ_w.*

4. Truncations of elliptic curves

We still need to consider the possible truncations of the group of M-points of an elliptic curve seen in the two previous sections. We will again treat separately the elliptic r-curves and c-curves. Since in the latter $E(M) = E(M)^0$, to ease the notation we shall denote the original group always as $E(M)^0$, but when E has "complex" roots we should imagine it as referring to all the M-points of E.

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

We shall denote by $Q^*, \lhd^*, \oplus^*, [n]^*$ the points, order, operation and formal multiplication on $E(M)^0$ respectively and by $Q, \lhd, \oplus, [n]$ those on G.

Both for the r-curves and the c-curves, we shall consider separately the case when $E(M)^0$ has good reduction or nonsplit multiplicative reduction, and the case when $E(M)^0$ has split multiplicative reduction.

We shall prove the following theorem:

Theorem 4.30. *Given a truncation $G = ([\ominus P, P), \oplus \mod [2]P)$ of the M-points of an elliptic curve E, one of the following holds:*

Either the following equivalent conditions hold:

1. *G/G^{00} is 1-based in M'.*
2. *G/G^{00} is internal to the value group Γ_w determined by G^{00} in M'.*
3. *One of the following holds:*

- *E is an r-curve, $E(M)$ has split multiplicative reduction and $v(x_P) > 0$.*
- *E is a c-curve, $E(M)$ has split multiplicative reduction, $v(x_P - 1) > 0$ and $x_P > 1$.*

Or, G is not of either of the forms in (3), G/G^{00} is non-1-based in M', and it is internal to the residue field k_w determined by G^{00}.

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

r-curves:

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

Subcase 1: $G = ([\ominus P, P), \oplus \mod [2]P)$ and $P \notin E(M)^{00}$. 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 $E(M)^0$ whose projections on the x-axis bound the projection of T, therefore $G^{00} = E(M)^{00}$. Moreover G/G^{00} is a definable truncation of $E(M)^0/E(M)^{00} = \tilde{E}(\mathbb{R})^0$ in the expansion of M by a predicate for G^{00}, and so it is non-1-based by Corollary 4.16.

Subcase 2: $G = ([\ominus P, P), \oplus \mod [2]P)$ and $P \in E(M)^{00}$. Clearly $G^{00} \neq E(M)^{00}$. We show then that G^{00} is still definable in the expansion M' of M by $E(M)^{00}$ and that moreover it is definable in a sort of $(M')^{eq}$ interdefinable with $k_v \cong \mathbb{R}$ in $(M')^{eq}$. 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 $v(x_S) < 0$, since $G \subseteq E(M)^{00}$. 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

$$G^{00} = \{S \in G | v(x_S) < v(x_P)\}. \tag{22}$$

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 1.14), 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 Lemma 2.24.

Observe that for each $S \notin G^{00}$, $v(x_S) = v(x_P)$, by 22, so it is sufficient to show that 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: Thoughout the claim we denote $\delta = \frac{x_Q}{x_S} - 1$. Firstly we prove RHS $\Rightarrow$ LHS.

We use the standard valuation: $v(x_{S\ominus Q}) = v\left(\frac{(y_Q+y_S)^2}{(x_Q-x_S)^2} - 1 + \epsilon - x_S - x_Q\right)$. After substituting δ and a bit of manipulation we find that it is equal to:
$v\Big((x_S+1)(x_S-\epsilon)\left(\frac{y_Q}{y_S}+1\right)^2 - (1-\epsilon)x_S\delta^2 - x_S^2\delta^2 - x_S x_Q\delta^2\Big) - v(x_S) - 2v(\delta)$.
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:

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

So $v\left((x_S+1)(x_S-\epsilon)\left(\frac{y_Q}{y_S}+1\right)^2-(1-\epsilon)x_S\delta^2-x_S^2\delta^2-x_Sx_Q\delta^2\right)\geq 2v(x_S)$, therefore $v(x_{S\ominus Q})\geq 2v(x_S)-v(x_S)-2v(\delta)=v(x_S)-2v(\delta)$. 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, LHS $\Rightarrow$ RHS, suppose $v(\delta)>0$. Then $v(x_{S\ominus Q})$ is $v\left((x_S+1)(x_S-\epsilon)\left(\frac{y_Q}{y_S}+1\right)^2-(1-\epsilon)x_S\delta^2-x_S^2\delta^2-x_Sx_Q\delta^2\right)-v(x_S)-2v(\delta)$, with $v(\left((x_S+1)(x_S-\epsilon)\left(\frac{y_Q}{y_S}+1\right)^2\right)=2v(x_S)$ and, since $v(\delta)>0$, $v(1-\epsilon)x_S\delta^2), v(x_S^2\delta^2), v(x_Sx_Q\delta^2)>2v(x_S)$, thus $v(x_{S\ominus Q})=2v(x_S)-v(x_S)-2v(\delta)=v(x_S)-2v(\delta)<v(x_S)=v(x_P)$, so $S\ominus Q\in G^{00}$.

This concludes the proof of the claim, and hence of Subcase 2.

We consider now the case of $E(M)$ 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 $P\in E(M)^0\setminus E(M)^{00}$, it is analogous to Subcase 1 above: we have that $G^{00}=E(M)^{00}$. Let H be the multiplicative truncation $\left([\epsilon,\frac{1}{\epsilon}),\cdot\ mod\ \epsilon^2\right)$. The definable bijection $f: E(M)^0/E(M)^{00}\to H/H^{00}$ of Theorem 4.15 restricted to G/G^{00} is then a definable bijection $f': G/G^{00}\to H'/H'^{00}$, where

$$H'=\left(\left[f(P),\frac{1}{f(P)}\right),\cdot\ mod\ f(P)^2\right)$$

is a "big" multiplicative truncation. By Lemma 2.24, 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 4.18.

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

(3) $P\in E(M)^{00}$ 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 $H = \left(\left[x_S, \frac{1}{x_S}\right), \cdot \mod \left(\frac{1}{x_s}\right)^2\right)$ 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 4.16 gives us that f is a definable bijection. Therefore G/G^{00} inherits 1-basedness from H/H^{00} by Lemma 2.24 and again it is internal to the value group of a real closed valued field.

(4) $P \in E(M)^{00}$ and $v(x_P) = 0$. It is again immediate to observe that if $x_S \in G$ and $v(x_S) = 0$, $v\left(x_{[2]S}\right) = v(x_S)$. 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 Lemma 2.24.

c-curves:

In the good reduction case, i.e., $E : y^2 = x(x^2 - 2rx + 1)$ and $v(r-1) = 0$, and G is a truncation of $E(M)$, the proof that G/G^{00} is non-1-based and internal to k_v is an analogue of the proof for the r-curves. We quickly present it:

(1) If $P \notin E(M)^{00}$, an easy argument on the torsion points proves that $G^{00} = E(M)^{00}$ and the function f of Theorem 4.27 together with Lemma 2.24 and Theorem 3.7 witnesses non-1-basedness of G/G^{00} and its internality to Γ_w.

(2) If $P \in E(M)^{00}$, we need to compute G^{00} and again we use the torsion points. Notice that if $S \in G$, then $v(x_S) < 0$. Also $v(x_{T_{2^n-1}}) =$

$v\left(\frac{(x_{T_{2^n}}^2-1)^2}{4x_{T_{2^n}}(x_{T_{2^n}}^2-2rxT_{2^n}+1)}\right) = 4v(x_{T_{2^n}}) - 3v(x_{T_{2^n}}) = v(x_{T_{2^n}})$. From this we deduce that $G^{00} = \{S \in G | v(x_S) < v(x_P)\}$ and that therefore in $M' = M_v$, G/G^{00} is a definable subset of $B_{\geq v(x_P)}(0)/B_{>v(x_P)}(0)$. Therefore G/G^{00} is internal to k_v and non-1-based (as in the proof for the truncations of r-curves with good reduction).

We consider lastly the split multiplicative reduction case: $v(r-1) > 0$. We have again 4 subcases:

(1) If $P \in E(M) \setminus E(M)^{00}$. As before, it is 1-based and internal to Γ_w.
(2) $P \in E(M)^{00}$ and $v(x_P - 1) < 0$. Analogous to Subcase (2) of the c-curves case above, and therefore non-1-based and internal to k_v.
(3) $P \in E(M)^{00}$ and $v(x_P - 1) > 0$. The proof is identical to the analogous case for the r-curves. G/G^{00} is therefore 1-based in M', and internal to Γ_w.
(4) $P \in E(M)^{00}$ and $v(x_P - 1) = 0$. Then, if $S \in G$, $v(x_S) = v(x_S - 1) = 0$, for the torsion points we have $v(x_{T_{2^n-1}}) = v\left(\frac{(x_{T_{2^n}}^2-1)^2}{4x_{T_{2^n}}(x_{T_{2^n}}^2-2rxT_{2^n}+1)}\right) = 0$, so $G^{00} = \{S \in G | v(x_S) < 0\}$, and therefore G/G^{00} is non-1-based and internal to k_v.

With these we have considered all possible cases and concluded the proof of Theorem 4.30.

□

5. Statement of the main result

In this and the previous chapter we have analysed all the cases in List A. This, if Conjecture 1.12 holds, is a complete analysis of 1-dimensional, definably compact, definably connected, definable groups in a saturated real closed field M. We found a strong link between the geometric stability notion of 1-basedness for the group G/G^{00} in a suitably enriched ambient structure M', and the notion of internality to the value group or the residue field of a real closed valued field M_w interdefinable with M'; moreover in the elliptic curve case we obtained also a relationship with the algebraic geometrical notion of reduction.

We have therefore proved the following theorem:

THEOREM 4.31. *Given a group G from List A in a saturated real closed field M, the structure $M' = (M, G^{00}, \dots)^{eq}$ (obtained by adding a predicate for G^{00} to M) is interdefinable with a real closed valued field M_w.*

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

(1) *The group G/G^{00} is 1-based in M'.*
(2) *The group G/G^{00} is internal to Γ_w in M_w.*
(3)
- *Either $G = \left(\left[\frac{1}{b}, b\right), \cdot \bmod b^2\right)$, and b is an infinite element of M, or*
- *$G = E(M)^0$ and E is an elliptic curve with split multiplicative reduction, or*
- *G is the truncation of $E(M)^0$ by a point P such that $v(x_P) > 0$, where E is an elliptic r-curve with split multiplicative reduction, or*
- *G is the truncation of $E(M)^0$ by a point P such that $v(x_P - 1) > 0$ or $x_P < 1$, where E is an elliptic c-curve with split multiplicative reduction.*

Or the following equivalent conditions hold:

(1) *The group G/G^{00} is non-1-based in M'.*
(2) *The group G/G^{00} is internal to k_w in M_w.*
(3)
- *Either $G = ([-1, 1), + \bmod 2)$, or*
- *$G = \left(\left[\frac{1}{b}, b\right), \cdot \bmod b^2\right)$, and b is a finite (or even infinitesimal) element of M, or*
- *$G = SO_2(M)$, or*
- *G is truncation of $SO_2(M)$, or*

- *$G = E(M)^0$ and E has good or nonsplit multiplicative reduction, or*
- *G is the truncation of $E(M)^0$ by a point P such that $v(x_P) \leq 0$, where E is an elliptic r-curve with split multiplicative reduction, or*
- *G is the truncation of $E(M)$ by a point P such that $v(x_P - 1) \leq 0$ and $x_P > 1$, where E is an elliptic c-curve with split multiplicative reduction.*

CHAPTER 5

Generalizations, questions and connections

The contents of this chapter are more to give an idea of some generalizations of the results obtained so far, hence some of the proofs are not carried in complete detail and some results are only partial. In the first two sections we attempt a generalization of the main result, Theorem 4.31, in two directions: in Section 1 we consider the ind-hyperdefinable groups $\tilde{G}/\tilde{G}^{00}$, where $\tilde{G}$ is ind-defined from one of the truncations G from List A, and extend Theorem 4.31 in this way; in Section 2 we deal with a variant of Theorem 4.31 where 1-basedness of G/G^{00} is considered in the full Shelah expansion M^{Sh} of our starting saturated real closed field M. In Section 3 we show some links with work by Hrushovski in the unpublished paper "Metastable groups" [**13**].

For the rest of the chapter M denotes again a saturated real closed field.

1. Ind-hyperdefinable groups

We consider the groups $(G, *)$ from List A that are truncations of some definable 1-dimensional, definably connected, definable group $(\hat{G}, \cdot)$ in M, i.e.:

(1) $G = ([-1, 1), + \ mod\ 2)$, a truncation of $\hat{G} = (M, +)$, or
(2) $G = \left(\left[\frac{1}{b}, b\right), \cdot \ mod\ b^2\right)$, a truncation of $\hat{G} = (M^{>0}, \cdot)$, or
(3) G a truncation of $\hat{G} = (SO_2(M), *)$, or
(4) G a truncation of $\hat{G} = (E(M)^0, \oplus)$, where E is an elliptic curve.

Definition 5.1. We ind-define $\tilde{G}$ as follows: $\tilde{G} = \bigcup_{i \in \omega} G_i$ (as a set) where $G_0 = G$ and $G_{i+1} = G_i \cdot G_i$, the set of elements of the form $k \cdot h$ where $k, h \in G_i$ and the operation $\cdot$ is the operation in the untruncated group $\hat{G}$. Thus $G_{i+1} = [g^{-1} \cdot g^{-1}, g \cdot g)$, where $G_i = [g^{-1}, g)$, $g \in \hat{G}$, and the interval is considered according to the definable ordering of $\tilde{G}$ given by Proposition 2 of [**30**]. In G_{i+1} the group operation is defined as follows: $*_{i+1} = \cdot \ mod\ g^4$. Therefore $(G_i, *_i)$ is a truncation of $(\hat{G}, \cdot)$.

Observe that although the operations in G_i, and in $\tilde{G}$ are different, when we restrict them to G_i^{00} and $\tilde{G}^{00}$ we have $(G_i^{00}, \cdot) = (\tilde{G}^{00}, \cdot)$. This immediately implies the following lemma:

LEMMA 5.2. *Given a truncation G as above, then $\tilde{G}^{00} = G^{00}$.*

Observe also that $\tilde{G}$ is an ind-definable set in the sense of Definition 2.3; moreover Definition 5.1 is equivalent to Definition 7.1 of [**11**].

Our aim is to transfer 1-basedness (or non-1-basedness) from $(G, *)$ to $(\tilde{G}, \cdot)$ in a sufficiently enriched structure:

THEOREM 5.3. *A group $\tilde{G}/\tilde{G}^{00}$, where $\tilde{G}$ is ind-defined from a truncation G, defined with parameters $\overline{a}$, as in Definition 5.1, is* 1*-based in the structure $M'' = (M, \tilde{G}, \tilde{G^{00}}, \overline{a}, \dots)^{eq}$ if and only if G/G^{00} is* 1*-based in $M' = (M, G^{00}, \overline{a}, \dots)^{eq}$.*

We split into two cases: if G/G^{00} is non-1-based in M', and if G/G^{00} is 1-based in M'.

In the former case we show that M'' is interdefinable with M', in Lemma 5.4, then Theorem 5.3 will follow easily. In the latter case we shall prove 1-basedness of $\tilde{G}/G^{00}$ directly in M''.

Case 1: Let G/G^{00} be non-1-based in M'.

LEMMA 5.4. *If G/G^{00} is non-*1*-based in M', the structure $M'' = (M, \tilde{G}, \tilde{G^{00}}, \overline{a}, \dots)^{eq}$, in which $\tilde{G}/\tilde{G}^{00}$ is definable, is interdefinable with $M' = (M, G^{00}, \overline{a}, \dots)^{eq}$.*

PROOF. Since $G^{00} = \tilde{G}^{00}$ we only have to show that $\tilde{G}$ is definable in a structure with a predicate for G^{00}.

We firstly recall that if G/G^{00} is non-1-based in M', then G is one of the following:

(1) Either $G = ([-1,1), + \ mod\ 2)$: an additive truncation, or
(2) $G = \left(\left[\frac{1}{b}, b\right), \cdot \ mod\ b^2\right)$, $v(b) \geq 0$: a small multiplicative truncation, or
(3) $G = ([-S,S), * \ mod\ [2]S)$: a truncation of $SO_2(M)$, or
(4) $([\ominus P, P) \oplus \ \text{mod}\ [2]P)$, such that $P \in E(M)^0$, and either E has good or nonsplit multiplicative reduction, or E is an r-curve with split multiplicative reduction and $v(x_P) \leq 0$, or E is a c-curve with split multiplicative reduction and both $v(x_P - 1) \leq 0$ and $x_P > 1$.

We shall define $\tilde{G}$ in M' case by case:

(1) Additive truncation: if $\tilde{G}$ is constructed from an additive truncation $G = ([-1,1), + \ mod\ 2)$, then G^{00} is the set of infinitesimal elements, and $\tilde{G}$ the set of finite elements, so we can simply define $\tilde{G}$ as $\{x | x^{-1} \in G^{00}\}$. Clearly any additive truncation $A = ([-a,a), + \ mod\ 2a)$ is definably isomorphic to G above, so analogously we can define $\tilde{A}$ using A^{00}.
(2) Small multiplicative truncation: if $\tilde{G}$ is constructed from a multiplicative truncation $G = ([b^{-1}, b), \cdot \ mod\ b^2)$, with $v(b) \geq 0$, then we know that $G^{00} - 1 = A^{00}$, by Observation 3.6: the minimal bounded index type-definable subgroup of the additive truncation $A = \Big([-(b-1), b-1), + \ mod\ 2(b-1)\Big)$. We just proved that $\tilde{A}$ is definable in the structure $M' = (M, G^{00}, b, \dots)^{eq}$ using the predicate for A^{00} and this latter is definable using G^{00}. We now define $\tilde{G}$ using $\tilde{A}$: let α be the upper cut of $\tilde{A}$, it is sufficient to prove that $\alpha + 1$ is the upper cut of $\tilde{G}$. This will prove that we can define $\tilde{G}$ using G^{00}.

    Consider then $g \in \tilde{G}$, and $g > 1$. To prove that $g - 1 < \alpha$, it is sufficient to show that $v\left(\frac{g-1}{b-1}\right) \geq 0$, since $\frac{1}{b-1}\alpha$ is the upper cut of Fin. But $g \in \tilde{G}$ implies that $g < b^n$ for some n, and so $\frac{g-1}{b-1} < \frac{b^n - 1}{b-1}$. Using the valuation, $v\left(\frac{g-1}{b-1}\right) \geq v\left(\frac{b^n-1}{b-1}\right) = v(b^{n-1} + b^{n-2} + \dots + 1) = 0$.

On the other hand if $a < \alpha$, $a \in \tilde{A}$, then $a < n(b-1)$ for some n, thus $a+1 < n(b-1)+1 < (b-1)^n+\cdots+n(b-1)+1 < (b-1+1)^n < b^n$, and therefore $a+1 \in \tilde{G}$.

This proves that $\tilde{G}$ is definable in $(M, G^{00}, b, \dots)^{eq}$.

(3) Truncations of $SO_2(M)$. If $\tilde{G}$ is constructed from a truncation $G = [-S, S)$ of $SO_2(M)$, then either $v(y_S) = 0$, and in this case $\tilde{G}$ is $SO_2(M)$ itself, by inspection of the torsion points, and we are done, or $v(y_S) > 0$. If this is the case, we want to construct a definable bijection (in the structure $M' = (M, \tilde{G}^{00}, x_S, y_S, \dots)^{eq}$) between $\tilde{G}/G^{00}$ and the quotient of an ind-definable group $\tilde{A}$ from an additive truncation A, by its own A^{00}.

We consider again the function $l : \tilde{G} \to M$, $l(P) = \frac{y_P}{x_P}$.

Let $A = \big([-l(S), l(S)) + \ mod\ 2 \cdot l(S)\big)$, then $A^{00} = \{x | v(x) > v(y_S)\}$, in fact $v(l(S)) = v(y_S)$. Then $\tilde{A} = \{x | v(x) \geq v(l(S))\}$.

Following the proof of Lemma 3.9 we obtain that $l(G^{00}) = A^{00}$. The same argument proves also that $l(\tilde{G}) = \tilde{A} = \{x | v(x) \geq v(y_S)\}$. Thus M' is interdefinable with $(M, A^{00}, l(S), \dots)^{eq}$, in which $\tilde{A}$ is definable. We can therefore define $\tilde{G}$ in M', by considering $\tilde{G} = l^{-1}(\tilde{A}$ and observing that l^{-1} is definable in M'.

(4) In all the cases of truncations $G = [\ominus P, P)$ of M-points of an elliptic curve, where G/G^{00} is non-1-based, by results in Chapter 5, G^{00} determines a cut on M of the form $\{x \in M | x > 0 \wedge v(x) \geq \gamma\}$, where $\gamma \in \Gamma_v$. We prove the following claim: $\{x \in M | x > 0 \wedge v(x) > \gamma\}$, definable in M', defines $\tilde{G}$.

In fact $G_{2^n} = [\ominus P_{2^n}, P_{2^n})$, and $[n]P_{2^n} = P$. But on checking the proof of Theorem 4.30 we observe that if $S \in G_{2^n} \setminus G^{00}$, $v(x_{[2]S}) = v(x_S)$, from which we obtain that for each n, $v(x_{P_{2^n}}) = v(x_P)$, from which we get the claim.

Therefore we have proved by exhaustion the lemma. $\square$

By Lemma 2.16, $\tilde{G}/G^{00}$ is uniformly o-minimal in M', so it makes sense to talk about 1-basedness of the theory of $\tilde{G}/G^{00}$ in M'.

It is clear that in these cases also $\tilde{G}/G^{00}$ is non-1-based: in fact we can witness non-1-basedness in a neighbourhood of the identity with the same function used to prove non-1-basedness of G/G^{00} in the corresponding cases of the previous section.

This proves Theorem 5.3 in the cases when G/G^{00} is non-1-based.

Case 2: Let G/G^{00} be 1-based in M'.

By Theorem 4.31, G/G^{00} is internal to Γ_w: the value group of the real closed valued field interdefinable with M'.

The only truncations G that have the behaviour described above are:

(1) $G = \left(\left[\frac{1}{b}, b\right), \cdot mod\ b^2\right)$, $v(b) < 0$: a big multiplicative truncation,
(2) $G = [\ominus P, P)$ a truncation of $E(M)^0$, M-points of an elliptic curve, with E an r-curve in minimal form with split multiplicative reduction, and $v(x_P) > 0$, or E a c-curve in minimal form with split multiplicative reduction and either $v(x_P - 1) > 0$ or $x_P < 1$.

We consider the structure $M'' = (M, G^{00}, \tilde{G}, \overline{a}, \dots)^{eq}$. Again there is a real closed valued field M_w definable in M'' with the cut determined by G^{00} on M. If G is a big multiplicative truncation, we proved in Theorem 3.7 that G/G^{00} is a definable subset of Γ_w. Moreover if G is determined by an elliptic curve, we proved in Chapter 4 that there is a definable bijection between G/G^{00} and the quotient of a big multiplicative truncation H by H^{00}. It is clear that we can extend such a bijection to the groups $G_i/G^{00} \to H_i/H^{00}$ in the ind-definition of $\tilde{G}$ and $\tilde{H}$. Thus we have a definable bijection $f : \tilde{G}/G^{00} \to \tilde{H}/H^{00}$.

As seen in Chapter 4 it is then sufficient, by Lemma 2.24, to prove that $\tilde{G}/G^{00}$ is 1-based in M'' for G a big multiplicative truncation, and thus obtain Theorem 5.3 for all $\tilde{G}/G^{00}$ when G/G^{00} is 1-based in M'.

By Theorem 2.16 the group $\tilde{G}/\tilde{G}^{00}$ is a uniformly o-minimal set in M''. It makes sense then to talk about 1-basedness of $\tilde{G}/\tilde{G}^{00}$ in M'' as in Definition 2.20.

We work in the value group Γ_w given by the valuation w, seen as living in M''.

We are within the conditions of Theorem 3.1.1 of Shaw's Thesis [**31**], thus the structure $\tilde{\Gamma}_w$, obtained from Γ_w by adding a predicate P for $w(\tilde{G}) = \tilde{G}/G^{00}$, has quantifier elimination in the language $L = (+, <, 0, c_1, c_2, \tilde{G}/G^{00})$, where c_1 is a positive element of $\tilde{G}/G^{00}$ and c_2 a positive element of $\tilde{\Gamma}_w \setminus \tilde{G}/G^{00}$.

It is then easy to prove that $\tilde{G}/G^{00}$ is fully embedded in $\tilde{\Gamma}_w$ as a divisible ordered abelian group, using quantifier elimination. The last step to prove that $\tilde{G}/G^{00}$ is 1-based in M'' is then the following claim (suggested by Pillay):

CLAIM: $\tilde{\Gamma}_w = (\Gamma_w, +, <, 0, P)$ is fully embedded in M'' as a divisible ordered abelian group.

Proof of the claim: Firstly observe that M'' is interdefinable with $(M_w, P) = ((M, +, \cdot, <, 0, 1), (\Gamma_w, +, 0, <, P), \dots)$, so it suffices to work in (M_w, P).

We work in a saturated model $(M'_w, P') = ((M', \dots), (\Gamma'_w, \dots, P), \dots)$ of $Th(M_w, P)$.

Let $\overline{c} \subset M'_w$, and X be a $\overline{c}$-definable subset of $(\Gamma'_w)^n$ in (M', P). We show that X is definable with parameters in $(\Gamma'_w, +, <, 0, P)$.

Let L_w be the language of M_w, i.e.,the language of a real closed valued field, and $\overline{d} = dcl(\overline{c}) \cap \Gamma'_w$ (note, here we work in the language without the predicate P).

Since $(\Gamma'_w, +, <, 0)$ is stably embedded in M'_w, every automorphism of $(\Gamma'_w, +, <, 0)$ fixing $\overline{d}$ extends to an automorphism of M'_w fixing $\overline{c}$.

In particular, when we work with the predicate P, any automorphism f of $(\Gamma'_w, +, <, 0, P)$ fixing $\overline{d}$, extends to an automorphism g of (M'_w, P).

It follows that given $\overline{a}, \overline{b}$ n-tuples, $tp(\overline{a}/\overline{d}) = tp(\overline{b}/\overline{d})$ in $(\Gamma'_w, +, <, 0, P)$ if and only if $tp(\overline{a}/\overline{c}) = tp(\overline{b}/\overline{c})$ in (M'_w, P).

In particular the map from complete n-types over $\overline{c}$ in $Th(M'_w, P, \overline{c})$ to complete n-types over $\overline{d}$ in $Th(\Gamma'_w, +, <, P, \overline{d})$ is a continuous (in the Stone space topology) bijection, and therefore it is a homeomorphism, and therefore sends clopens (i.e, formulae) to clopens (formulae). Therefore it is a map sending the formula defining X to a formula in $(\Gamma'_w, +, <, 0, P, \overline{d})$, and so $(\Gamma'_w, +, <, 0, P)$ is stably embedded in (M'_w, P').

When we consider $\overline{c} = \emptyset$ we obtain that $(\Gamma'_w, +, <, 0, P)$ is also canonically embedded in (M'_w, P'), and we proved the claim.

So $\tilde{G}/G^{00}$ is fully embedded in M'' as a divisible ordered abelian group, therefore it is 1-based in M''.

With this case we have proved Theorem 5.3.

2. Shelah expansion

We look now at a generalization of Theorem 4.31 in another direction: we consider 1-basedness in the full Shelah expansion of a real closed field. Observe that the expansion $M' = (M, G^{00}, \dots)^{eq}$ used in the previous chapters to turn the bounded hyperdefinable groups into definable groups (and even M'' in the previous section, to deal with certain ind-hyperdefinable groups) are all reducts of the Shelah expansion $(M^{Sh})^{eq}$. It is therefore natural to ask whether the above groups are 1-based or non-1-based in $(M^{Sh})^{eq}$.

It is clear that if G/G^{00} is non-1-based in $M' = (M, G^{00}, \dots)^{eq}$, G/G^{00} will also be non-1-based in $(M^{Sh})^{eq}$. So we need to check 1-basedness in $(M^{Sh})^{eq}$ for the groups G/G^{00} that are 1-based in M'.

The main tool to prove 1-basedness is stable embeddedness of the value group Γ, but we need here to describe what we mean by the value group in $(M^{Sh})^{eq}$. There are in fact many definable valuations in $(M^{Sh})^{eq}$, and if we consider one of these definable value groups, it has a much richer structure than a pure divisible ordered abelian group, since there are predicates for all externally definable sets.

Given a predicate P in M^{Sh} for a convex multiplicative group in M with $2 \in P$ and closed under square roots, it defines a unique valuation w. We denote by Γ_P the value group determined by w, as a sort in $(M^{Sh})^{eq}$. This will have predicates for all externally definable sets. Our aim is to prove that Γ_P is stably embedded, meaning that $Th(\Gamma_P) = Th({\Gamma_w}^{Sh})$ where Γ_w is a divisible ordered abelian group.

We recall that $M' = (M, P, \ldots)$ is interdefinable with a real closed valued field, so we call the value group, in the language $L_{M'}$, Γ_w. Observe that Γ_P and Γ_w have the same base set, they differ when considered as structures on their own.

Observe firstly that $(M^{Sh})^{eq} = ((M')^{Sh})^{eq}$. Moreover denote by $\overline{M}$ an $|M'|^+$-saturated model of $Th(M')$, then every definable set in $(M^{Sh})^{eq} = ((M')^{Sh})^{eq}$ is definable in M' with parameters from $\overline{M}$. Denote by $\overline{\Gamma}_w$ the value group of $\overline{M}$. By full embeddedness of the value groups as divisible ordered abelian groups, we have that $\overline{\Gamma}_w \succ \Gamma_w$, and that given any externally definable set X of M', $X \cap \Gamma_w$ is definable with parameters from $\overline{\Gamma}_w$. So every definable set of Γ_P is definable with parameters from an elementary extension $\overline{\Gamma}_w$ of Γ_w, and therefore $Th(\Gamma_P) = Th({\Gamma_w}^{Sh})$.

By the positive solution of the Trace Conjecture in the case of divisible ordered abelian groups, due to quantifier elimination for divisible ordered abelian groups, we have that $Th({\Gamma_w}^{Sh}) = Th({\Gamma_w}^{cuts})$, the theory of a divisible abelian ordered group expanded by all Dedekind cuts.

Consider now G a big multiplicative truncation of M. Then G/G^{00} is a definable subset of Γ_P, and, analogously to the study of big multiplicative truncations in Chapter 3, we can work in $T_{\Gamma_P} = T_{\Gamma_w^{Sh}}$.

Theorem 3.11 implies that G/G^{00}, as a set definable in Γ_P, is complete, and therefore there are no Dedekind cuts; thus, by what was shown above, there is no further structure induced on G/G^{00} in M^{Sh}. Therefore $T_{G/G^{00}}$ in Γ_P equals $T_{G/G^{00}}$ in Γ_w, and this proves that if G/G^{00} is 1-based in M', then it is 1-based in M^{Sh}.

Therefore we have proved:

THEOREM 5.5. *Given a big multiplicative truncation G in M, G/G^{00} is 1-based in $(M^{Sh})^{eq}$.*

If G is the group of M-points of an elliptic curve or a truncation of an elliptic curve, for which G/G^{00} is 1-based in $M' = (M, G^{00}, \dots)$, the definable bijection $f : G/G^{00} \to H/H^{00}$, where H is a big multiplicative truncation, seen in Chapter 4, Theorem 5.5 above and Lemma 2.24 easily imply that G/G^{00} is 1-based in M^{Sh}.

We have therefore proved the following theorem:

THEOREM 5.6. *Given a group G from List A, definable in a saturated real closed field M, G/G^{00} is 1-based in $M' = (M, G^{00}, \dots)^{eq}$ if and only if G/G^{00} is 1-based in $(M^{Sh})^{eq}$.*

3. The connection with work by Hrushovski

I shall briefly outline how my research fits into the project of Hrushovski in [**13**].

In the article [**13**] Hrushovski introduces the class of metastable theories, whose motivating example is the theory of algebraically closed valued fields.

We state what Theorem 5.9 of [**13**] roughly means:

THEOREM 5.7 (Hrushovski). *Given G a commutative definable group in an algebraically closed field K, there is a definable homomorphism $f : G \to H$, where H is a group in Γ^{eq} (the value group of K) and $ker(f)$ is a stably dominated group (i.e., a group with a definable generic type which is stably dominated).*

We are likely to prove analogous behaviour in the cases studied in this thesis in the context of real closed valued fields. We work in a saturated standard real closed valued field M, and consider elliptic curves over M: $G = E(M)^0$. The following version of the theorem above, specific to real closed valued fields, whose solution should follow from Theorem 5.7 is the following:

STATEMENT 5.8. *Given $G = E(M)^0$, then in M_v, the standard real closed valued field, either:*

(1) *there is a definable epimorphism of G onto a group H definable in Γ_v, such that in a suitably enriched structure G/G^{00} is definably isomorphic to H/H^{00}, or*
(2) *there is a definable epimorphism of G onto a group H definable in k_v; moreover it is simply the map $G \to G/G^{00} = H$.*

We would like to obtain directly the statement above from our results. This thesis shows already that for $G = E(M)^0$ and E an elliptic curve with good or nonsplit multiplicative reduction the statement is true, and we are in the second case of Statement 5.8. The only obstacle to prove that if E has split multiplicative reduction we have the behaviour described in the first case is the following open question:

QUESTION 5.9. *Does the map $f_* : G \to B$ defined in Chapter 4 for the split multiplicative reduction cases of r-curves and c-curves, and where $B = \left(\left[\frac{1}{b}, b\right), * \bmod b^2\right)$ is a multiplicative reduction, induce a group homomorphism $f'_* : G \to v(B)$ on the image of B under the standard valuation, with the usual value group operation?*

It would actually suffice to prove that f'_* defines a group structure on $v(B)$, then by a result of Eleftheriou and Starchenko (Theorem 1.4 in [**6**]), we would be able to find the epimorphism required in Statement 5.8.

Observe also that it makes no sense to talk about stable domination for such structures, since both the value group and the residue field of a real closed valued field are unstable, therefore a more suitable notion such as "o-minimal domination" needs to be developed. This could be a topic of future research.

CHAPTER 6

Summary

In Chapters 1 and 2 of this thesis we introduced and generalized some notions, and described the groups to be analysed in the following chapters. We considered G a 1-dimensional, definably compact, definably connected, definable group in a saturated real closed field M, and wrote a list (List A) inspired by a theorem of Madden and Stanton, conjecturing that it is a complete classification of such groups G. We then considered the quotient of G by its group of "infinitesimals", G^{00}, and described two topologies on it: the logic topology (viewing G/G^{00} as an hyperdefinable group in M), and the o-minimal topology (viewing G/G^{00} as a structure on its own), showing how they coincide. We then explained how can we define structural properties, such as 1-basedness, of G/G^{00} by working in a sufficiently enriched structure M'.

In Chapters 3 and 4 we proceeded with the analysis of the groups from List A up to 1-basedness. The simpler examples are contained in Chapter 3, the more involved examples of elliptic curves are in Chapter 4, after the development of some elliptic curve theory for real closed fields. We highlighted the link between the structure of G/G^{00} and the real closed valued fields by characterizing 1-basedness of G/G^{00} in terms of internality to the residue field or the value group of some real closed valued field. In Chapter 4 we also related 1-basedness with the notion of algebraic geometric reduction for elliptic curves. The main result is stated at the end of Chapter 4.

In Chapter 5 we discussed about generalizations of the results obtained, firstly considering a wider class of groups: the 1-dimensional, definably compact, definably connected, ind-definable groups G in M. Afterwards we studied the groups G/G^{00} up to 1-basedness in the full Shelah expansion of M. At the end it is described a possible link with work of Hrushovski.

We now state some open questions which could be the basis for future research after the end of my doctorate.

1. Possible future directions and questions

We conclude this thesis by stating some open questions and some ideas for possible future research.

The most important question left open in this thesis is Conjecture 1.12: the generalization to real closed fields of the theorem of Madden and Stanton 1.11.

We recall that the positive solution of Conjecture 1.12 implies that Theorem 4.31 is a complete description of G/G^{00} when G is a 1-dimensional, definably compact, definably connected, definable group in a saturated real closed field M.

A natural question from looking at the proof of 1-basedness for the split multiplicative reduction cases in Chapter 4 is the following. Is the definable bijection $f : G/G^{00} \to H/H^{00}$, where, we recall, $G = E(M)^0$ for some elliptic r-curve or c-curve E with split multiplicative reduction, and H is a "big" multiplicative truncation, a definable isomorphism of groups? A weaker conjecture, whose solution might be computationally easier is the following: does f induce an inclusion preserving bijection between the convex subgroups of G/G^{00} and H/H^{00}, where by convex we mean convex in the order defined for such groups in the thesis?

In the previous chapter we planted the seeds for a link between this thesis and the article [**13**] of Hrushovski, the solution of the question above would probably solve also Conjecture 5.8. Moreover, it would be interesting to explore the connection between my results in real closed fields (and real closed valued fields) and Hrushovski's results in algebraically closed valued fields.

It is also natural to ask what happens when G is an arbitrary abelian variety over M, or just a simple abelian variety over M. In order to obtain results in this direction it would be necessary to modify most of the notions we introduced, in fact such groups would not be o-minimal, but semi-o-minimal, as defined in [**12**]. Moreover it would be necessary to find a more general proof of Theorem 4.31, which does not involve computing G^{00} and the bijection between G/G^{00} and the value group or residue field of a real closed valued field.

Another possible generalization of the results can be obtained by considering our ambient structure M to be a polynomially bounded o-minimal expansion of a real closed field.

Bibliography

[1] Baisalov, Y.; Poizat, B., Paires De Structures O-Minimales, *The Journal Symbolic logic*, 1998, **Vol. 63, issue 2**, pp. 570-578.

[2] Baizhanov, B., Expansion of a Model of a Weakly O-Minimal Theory by a Family of Unary Predicates, *The Journal Symbolic logic*, 2001, **Vol. 66, issue 3**, pp. 1382-1414.

[3] Berarducci, A.; Otero, M.; Peterzil, Y.; Pillay, A., A descending chain condition for groups definable in o-minimal structures, *Annals of Pure and Applied Logic*, 2005, **Vol. 134**, pp. 303-313.

[4] Bochnak, J.; Coste, M.; Roy, M., Real Algebraic Geometry, *Springer*, 1998.

[5] Cherlin, G.; Dickmann, M., Real closed rings II: Model Theory, *Annals of pure and applied logic*, 1983, **Vol. 25, number 3**, pp. 213-231.

[6] Eleftheriou, P; Starchenko, S.; Groups definable in ordered vector spaces over ordered division rings, *Journal of Symbolic Logic*, 2007, **Vol. 72**, pp. 1108-1140.

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

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

[9] Hrushovski, E., A new strongly minimal set, *Annals of Pure and Applied Logic*, 1993, **Vol. 62, issue 2**, pp. 147-166.

[10] Hrushovski, E.; Zilber, B., Zariski geometries, *Journal of AMS*, 1996, **Vol. 9**, pp. 1-56.

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

[12] Hrushovski, E.; Pillay, A., NIP and invariant measures, *to appear in JEMS.*

[13] Hrushovski, E., Metastable groups, *Preprint.*

[14] Ramakrishnan, J., Definable linear orders definably embed into lexicographic orders in o-minimal structures, *Preprint.*

[15] Jones, G.; Wilkie, A., Locally polynomially bounded structures, *Bulletin of the London Mathematical Society*, 2008, **Vol. 40, issue 2**, pp. 239-248.

[16] Knight, J.; Pillay, A.; Steinhorn, C., Definable sets in ordered structures II, *Transactions of the American Mathematical Society*, 1986, **Vol. 295, number 2**, pp. 593-605.

[17] Kuhlmann, S., Ordered exponential fields, *Fields Institute Monographs*, 2000.

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

[19] Macpherson, D.; Marker, D.; Steinhorn, C., Weakly o-minimal structures and real closed fields, *Transactions of the American Mathematical Society*, 2000, **Vol. 352, no. 12**, pp. 5435-5483.

[20] Madden, J.; Stanton, C., One-dimensional Nash groups, *Pacific Journal of Mathematics*, 1992, **Vol. 154, number 2**, pp. 331-344.

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

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

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

[24] Peterzil, Y.; Steinhorn, C., Definable compacteness and definable subgroups of o-minimal groups, *J. London Math. Soc*, 1999, **Vol. 59, issue 2**, pp. 769786.

[25] Peterzil, Y., Pillay's conjecture and its solution - a survey, *proceedings of the Wroclaw Logic meeting 2007.*

[26] Pillay, A., On groups and fields definable in o-minimal structures, *Journal of pure and applied algebra*, 1988, **Vol. 53**, pp. 239-255.

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

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

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

[30] Razenj, V., One-dimensional groups over an o-minimal structure, *Annals of Pure and Applied Logic*, 1991, **Vol. 53**, pp. 269-277.

[31] Shaw, C., Weakly o-minimal structures and Skolem functions, *PhD. Thesis, University of Maryland*, 2008.

[32] Shelah, S., Dependent First Order Theories, continued, *Israel Journal of mathematics*, 2009, **Vol. 173, number 1**, pp. 1-60.

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

[34] Tressl, M., Model Completeness of o-minimal Structures expanded by Dedekind Cuts *Journal of Symbolic Logic*, 2005, **no. 1**, pp. 29-60.

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

[36] Zil'ber, B., The Structure of Models of Uncountably Categorical Theories, *Proceedings of the International Congress of Mathematics*, 1983, Warszawa.