DEFINABLE GROUPS AND COMPACT p-ADIC LIE GROUPS

ALF ONSHUUS AND ANAND PILLAY

ABSTRACT. We formulate a version of the o-minimal group conjectures from [11], which is appropriate for groups G definable in a (saturated) p-adically closed field K, We discuss the conjectures in two cases, when G is defined over $\mathbb{Q}_p$ and when G is of the form $E(K)$ for E an elliptic curve over K.

1. Introduction

In [11] questions were raised concerning recovering a compact Lie group from a definable group G in saturated o-minimal structures, by quotienting by a type-definable subgroup of G of bounded index. Related work was done in [1], [2] and [9]. As Gregory Cherlin suggested to us, it is rather natural to consider p-adic analogues of the questions. This is what we discuss in the present paper. The right level of model-theoretic generality is probably that of so-called P-minimal expansions of p-adically closed fields. However we restrict ourselves here to p-adically closed fields. In fact for notational convenience, we look at groups definable in a saturated elementary extension $(K, +, \cdot)$ of the p-adic field $\mathbb{Q}_p$. So one could view this as the study of uniformly definable families of groups in $\mathbb{Q}_p$.

Before stating the conjectures and results of this paper, we give some definitions, state some elementary facts, and recall some facts about p-adic analytic groups. We refer to [5] for background on compact groups and profinite groups, and to [4] for background on p-adic analytic groups.

To begin with let $\bar{M}$ be a saturated model (of cardinality $\kappa > |T|$ say where κ is inaccessible) of an arbitrary complete theory T in a language L, and let G be a group definable in $\bar{M}$. Let $\mathcal{F}_G$ denote the family of definable subgroups of G of finite index.

Definition 1.1. *(i) Suppose that the family $\mathcal{F}_G$ of definable subgroups of G of finite index has cardinality $< \kappa$. Then we define G^0 to be $\cap\mathcal{F}$, and we also say that "G^0 exists".*

(ii) Suppose that there is a smallest type-definable subgroup of G of bounded index. Them we call this group G^{00} and we say G^{00} exists.

Lemma 1.2. *(i) If G^0, G^{00} respectively, exists, then it is a normal subgroup of G which is definable, respectively type-definable, over the same set of parameters G is. If G^{00} exists then so does G^0 and G^{00} is a subgroup of G^0.*
(ii) G^0 exists if and only if for each L-formula $\phi(x,y)$ and $n < \omega$ there are only finitely many subgroups of G of index n defined by $\phi(x,b)$ for some b. In this case $\mathcal{F}$ has cardinality $\leq |T|$. The group G/G^0 then has cardinality $\leq 2^{|T|}$.
(iii) Likewise, if G^{00} exists then G/G^{00} has cardinality at most $2^{|T|}$.

Recall the *logic topology* on quotients of type-definable sets by type-definable equivalence relations of bounded index: If X is a type-definable set and E a type-definable equivalence relation on X with boundedly many classes, then we call $Z \subseteq X/E$ closed if $\pi^{-1}(Z) \subseteq X$ is type-definable, this is a topology on X/E, and under this topology X/E is a compact (Hausdorff) space.

Remark 1.3. *(i) If G^0 exists, then G/G^0 with the logic topology is a compact totally disconnected (namely profinite) topological group.*
(ii) If G^{00} exists then G/G^{00} with the logic topology is a compact topological group and G/G^0 is its maximal profinite quotient.

Supposing that G^0 exists we shall, for obvious reasons, call G/G^0 the *definable profinite completion* of G.

Lemma 1.4. *Suppose that T does not have the independence property. Then for any definable group G in $\bar{M}$, G^0 exists.*

Proof. Let $\phi(x,y) \in L$ and $n < \omega$. Suppose for a contradiction that there are infinitely many distinct subgroups of G of index n defined by $\phi(x,b)$ for some b. So there is an indiscernible sequence $(b_i : i < \omega)$ such that each $\phi(x,b_i)$ defines a subgroup of G of index n, and the $\phi(x,b_i)$ are pairwise inequivalent. For J a finite subset of ω let H_J be defined by $\wedge_{i\in J}\phi(x,b_i)$. Let m denote the subset $\{0,..,m-1\}$ of ω. By our assumption that T does not have the independence property and [14] there is $k < \omega$ such that for each $m \geq k$, $H_m = H_J$ for some $J \subseteq m$ of cardinality k. Note that H_k is a proper subgroup of H_{k+1}. But the latter equals H_J for some $J \subset (k+1)$ of cardinality k and by indiscernibility H_k and H_J have the same (finite) index in G, a contradiction.

Question Assume T does not have the independence property and G is a group definable in $\bar{M}$. Does G^{00} exist?

We now recall some facts about p-adic analytic groups ([4]). We assume familiarity with the topology on the p-adic field $\mathbb{Q}_p$, and the notion of a a (p-adic) analytic function. A p-adic analytic group (or p-adic Lie group) G is a p-adic analytic manifold with a group operation which is p-adic analytic. As such G is also a topological group. Any p-adic Lie group has an open subgroup which is compact. Moreover any compact p-adic Lie group G has an open subgroup H (of finite index) such that H, as a topological group, is pro-p, namely H has a collection of open normal subgroups $\{H_i : i \in I\}$ such that $\cap_{i\in I} H_i = \{1\}$ and each H/H_i has order a power of p.

However not every pro-p group is (the underlying topological group of) a compact p-adic Lie group. Necessary and sufficient conditions for a topological group G to be a compact p-adic Lie group are: (a) G is profinite and finitely generated and (b) G has a open pro-p subgroup H such that $H/\overline{H}^p$ is commutative. (Here $\overline{H}^p$ denotes the closure of the subgroup of H generated by pth powers.)

As our general conjectures are related to finding an "intrinsic" standard part map, it is worth saying a few words about the standard part map from nonstandard analysis. Let X be an arbitrary compact Hausdorff space. Let V be the universe of sets. Let ${}^*V$ be an elementary extension, and ${}^*X$ the nonstandard extension of X in ${}^*V$. For any $x \in {}^*X$ there is a unique $y \in X$ such that $x \in {}^*U$ for every open subset of X containing y. We write $y = st(x)$, and call $st{:}{}^*X \to X$ the standard part map. If G is a compact group, ${}^*G$ has a group structure and $st{:}{}^*G \to G$ is a (surjective) homomorphism, whose kernel is the group of "infinitesimals" of ${}^*G$.

The general point of the conjectures from [11] and in the present paper is that for suitable groups G definable in suitable saturated structures $\bar{M}$, the map $G \to G/G^{00}$ identifies with the standard part map ${}^*(G/G^{00}) \to G/G^{00}$ where G/G^{00} is equipped with the logic topology.

Finally we discuss (the model theory of) p-adically closed fields and groups definable therein. Possible references are [15] and [3]. We view $\mathbb{Q}_p$ as a structure in the language of rings L_r. The valuation ring $\mathbb{Z}_p$ is definable in $\mathbb{Q}_p$. Hence the the value group $(\mathbb{Z}, +, <)$, residue field $(\mathbb{F}_p, +, .)$, as well as the valuation $v : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ and residue map from $\mathbb{Z}_p$ to $\mathbb{F}_p$ are interpretable. By a p-adically closed field we mean a model of $Th(\mathbb{Q}_p)$ If K is such we let R denote the valuation ring, and Γ the value group. The residue field is of course still $\mathbb{F}_p$. A p-adically closed field is then precisely a Henselian valued field, whose residue field is $\mathbb{F}_p$ and whose value group is a model of Pressburger arithmetic, namely $Th(\mathbb{Z},+,<)$. Macintyre's quantifier-elimination theorem states that $Th(\mathbb{Q}_p)$ (in the ring language) eliminates quantifiers after adjoining predicates P_n for the nth powers of the multiplicative group for all n. $\mathbb{Q}_p$ is a locally compact topological field, with basis given by the sets $v(x-a) \geq n$ for $a \in \mathbb{Q}_p$ and $n \in \mathbb{Z}$, the value group. $\mathbb{Z}_p$ is compact. Note the topology is "uniformly first order definable" that is one can quantify over open neighborhoods. All of this remains true for K an arbitrary p-adically closed field, except the topology is longer locally compact. Any definable subset of K^n has a well-defined dimension: the algebraic-geometric dimension of its Zariski closure. Equivalently, as model-theoretic algebraic closure coincides with field-theoretic algebraic closure, algebraic closure gives a pregeometry on K and dimension can be calculated from this is the usual way. Definable subsets of K^n will also be called semialgebraic sets.

From now on K denotes a p-adically closed field, R its valuation ring and Γ its value group. In analogy with the o-minimal context we have the notion of an *n-dimensional definable manifold over K* (or a semialgebraic manifold over K). Such an object is a topological space X with a covering by finitely many open subsets $U_1,..,U_m$, and homeomorphisms of U_i with some definable open $V_i \subset K^n$ for $i=1,..,m$, such that the transition maps are definable (and of course continuous). If the transition maps are C^k we call X a definable C^k manifold over K (of dimension n). A definable manifold over K is clearly then something interpretable in K.

By a definable (or semialgebraic) group over K we mean a group whose universe is a definable subset of some K^n and whose group operation is definable. The methods of [13] together with the structure of definable functions show that any definable group G can be equipped (uniquely) with the structure of a definable manifold over K such that the group operation is continuous (in fact C^∞). Any definable group will be always considered with the topology coming from this definable group manifold topology.

In the special case that $K=\mathbb{Q}_p$, then G is definably equipped with the structure of a p-adic Lie group. We will call the latter a *semialgebraic p-adic Lie group.* Note:

Remark 1.5. *Any open compact subgroup of semialgebraic p-adic Lie group is semialgebraic.*

The following was asked in [12]
Problem. Is any open (not necessarily compact) subgroup of a semialgebraic p-adic Lie group semialgebraic?

This problem was answered in [8] for $SL_2(\mathbb{Q}_p)$, and it was pointed out that results of Prasad yield it for arbitrary semisimple groups in place of SL_2. The understanding of imaginaries in the p-adics ([6]) probably makes the problem currently accessible.

Following [10] in the o-minimal case, for X a definable manifold over K, we say that X is definably compact, if for any definable continuous function $f : R \setminus \{0\} \to X$, $lim_{x\to 0}f(x)$ exists in X. We leave it to the reader to check (i) if $K = \mathbb{Q}_p$ definable compactness agrees with compactness, and (ii) for X a definable subset of K^n with the induced topology, X is definably compact if and only if X is closed and bounded.

Let us note by Lemma 1.4 that for G definable in K, G^0 exists.

In general the "interesting" examples of definable groups in a p-adically closed field K will be groups of the form $G = H(K)$ where H is an algebraic group defined over K. Among definably compact groups are $A(K)$ for A any abelian variety over K, and $GL_n(R)$.

We can now state some p-adic versions of the questions from [11]

Naive conjecture.
Let G be a definably compact group definable in a saturated p-adically closed field K. Then
(i) G^{00} exists and equals G^0.
(ii) G/G^0 (with the logic topology, namely as a profinite group) is a compact p-adic Lie group of dimension equal to $dim(G)$.

In section 2 we observe that the naive conjecture holds in the case that G is defined *over* $\mathbb{Q}_p$. We will also give a theory of "generic" sets in this case. However in section 3 we will see by considering suitable elliptic curves that both (i) and (ii) fail in general. So we make the following modified) conjecture, which now concerns all definable groups not just definably compact ones.

Refined conjecture.
Let G be a group definable in a saturated p-adically closed field. Then G has an open definable subgroup H such that
(i) H^{00} exists and equals H^0,
(ii) H/H^0 is a compact p-adic Lie group of dimension equal to $dim(H) = dim(G)$.

In section 3 we observe that (ii) of the refined conjecture holds for G of the form $E(K)$ where E is an elliptic curve defined over K. It would be even better to include in the refined conjecture an intrinsic characterization of H. Note that the refined conjecture *will* be true for G defined over $\mathbb{Q}_p$.

Thanks to Tom Scanlon for some helpful comments.

2. The tautological case

We work in the saturated p-adically closed field K, an elementary extension of $\mathbb{Q}_p$ and follow earlier notation (Γ for the value group etc.).

We will call elements of K that have valuation larger than all elements of $\mathbb{Z}$ infinitesimals and and those that have valuation smaller than all elements in $\mathbb{Z}$ transfinite.

If $a \in K$ is not transfinite (there is some $m \in \mathbb{N}$ such that $v(a) \geq n$) by completeness of $\mathbb{Q}_p$ there is some $\dot{a} \in \mathbb{Q}_p$ such that $a - \dot{a}$ is infinitesimal. We will call $\dot{a}$ the *standard part* of a. Given a polynomial $p(x)$ with none of its coefficients transfinite $\dot{p}(x) \in \mathbb{Q}_p$ be the polynomial we get by changing all the coefficients of p for their standard part.

Lemma 2.1. *Given any polynomial $p(x)$ with n variables and any $\mathbb{Q}_p$-definable n-ball U, there is a $\mathbb{Q}_p$-definable n-ball $U_0 \subset U$ where $v(p(x))$ is constant. If none of the coefficients of $p(x)$ is transfinite, then we can choose U_0 such that $v(p(x)) = k \in \mathbb{Z}$ for all x in U_0.*

Proof. Let a_I be the coefficient of $p(x)$ with smallest valuation. Let $p(x) = a_I q(x)$ where all the coefficients of $q(x)$ have positive valuation and one of them is equal to 1. So $\dot{q}(x)$ exists and is different from 0. Let a be any tuple in $\mathbb{Q}_p$ which is not a root of $\dot{q}$ and let $v(\dot{q}(a)) = m$.

By continuity of $\dot{q}$ in $\mathbb{Q}_p$ there is some open n-ball $U_0 \subset U$ centered around a such that $v(\dot{q}(y)) = m$ for all $y \in U_0(\mathbb{Q}_p)$ and by elementary embeddedness $v(\dot{q}(y)) = m$ for all $y \in U_0$. We may assume that U_0 has no elements with transfinite coordinates: U_0 is a product of balls centered around $a = \langle a_1, \ldots, a_n \rangle \in \mathbb{Q}_p$; we can even assume that $v(y_i) = v(a_i)$ for all $y\langle y_1, \ldots, y_n \rangle \in U_0$.

Claim. $v(q(y)) = m$ for all $y \in U_0$.
Proof of claim. Suppose not so $v(q(b)) \neq v(\dot{q}(b)) = m$ for some $b \in U_0$ and $v((q - \dot{q})(b)) \leq m$. All the coefficients in $q - \dot{q}$ are infinitesimal and none of the b_i's are transfinite (by assumption on U_0) so the valuation of each of the monomials in $(q - \dot{q})(b)$ is bigger than all integers. The claim follows.

By the claim, $v(p(y)) = v(a_I) + v(q(y)) = v(a_I) + m$ for all $y \in U_0$, which completes the proof of the lemma.

Proposition 2.2. *Let $X \subseteq K^n$ be open, definable and defined over $\mathbb{Q}_p$. Let $X = Y_1 \cup Y_2$, where the Y_i are definable in K. Then one of the Y_i contains an open $\mathbb{Q}_p$-definable subset.*

Proof. By quantifier elimination, (see [7]) any definable set in a p-adically closed field is a Boolean combination of sets of the following form:

(1) Graphs of polynomials.
(2) $h^{-1}(R) \cap \{x | g_2(x) \neq 0\}$ where $h(x) = \frac{g_1(x)}{g_2(x)}$ and g_1, g_2 are polynomials.
(3) $h^{-1}(P_m)$ where $h(x) = \frac{g_1(x)}{g_2(x)}$, $m \in \mathbb{Z}$ and g_1, g_2 are polynomials.

We may assume that X is a $\mathbb{Q}_p$-definable n-ball $X = B_1 \times \cdots \times B_n$ and by quantifier elimination it is enough to show the proposition when Y_1 is a definable set satisfying one of the above descriptions.

Case 1: Let

$$Y_1 = \{(\bar{x}, y) \mid p(\bar{x}) = y\}.$$

Let $B = B_1 \times \cdots \times B_{n-1}$ and $X = B \times B_n$. By Lemma 2.1 there is some $B_0 \subset B$ such that $v(p(\bar{x})) = \gamma$ for all $\bar{x}$ in B_0 and some $\gamma \in \Gamma$. Let $m\mathbb{Z}$ such that $m \neq \gamma$ and let m and a be such that the ball $B_{=m}(a)$ of radius m around a is contained in B_n. Then $B_0 \times B_{=m}(a)$ is a subset of X containing no point in Y_1, so it is contained in Y_2.

Case 2:

Let Y_1 be a set of type 2 in B,

$$\begin{aligned} Y_1 := & \quad \{x \mid v(g_1(x)) - v(g_2(x)) \geq 0\}, \\ = & \quad \{x \mid v(g_1(x)) \geq v(g_2(x))\}. \end{aligned}$$

Using Lemma 2.1 twice, we can find some $\mathbb{Q}_p$ definable n-ball $U_0 \subset X$ where both $v(g_1)$ and $v(g_2)$ are constant with values γ_1 and γ_2 respectively. If $\gamma_1 \geq \gamma_2$ then U_0 is contained in Y_1. Otherwise, $U_0 \cap Y_1 = \emptyset$ and $U_0 \subset Y_2$.

Case 3: Since there are finitely many residues in the multiplicative group modulo powers of n, it is enough to prove the case where

$$Y_1 := \{x \mid p(x) \in P_m\}$$

for any polynomial $p(x)$.

Also, we can always find powers of m of any valuation as small as we want. In particular if a_I is the coefficient of $p(x)$ of smallest valuation, we can find some $b \in P_m(F)$ such that

$$0 \leq v(a_I) - v(b) \leq m;$$

by taking $p'(x) = \frac{1}{b}p(x)$ we may assume that all the coefficients in $p(x)$ have positive valuation and that at least one of them is non infinitesimal.

Let $U_0 \subset X$ be such that $v(x) = k \in \mathbb{Z}$ for any $x \in U_0$ and by Hensel-Rychlik $Y_1 \cap U_0$ are finite unions of $\mathbb{Q}_p$-definable balls of radius $2v(m) + 2k$.

As usual a definable subset X of a definable group G (in some structure) is said to be left generic if finitely many left translates of X cover G.

Now let G be a definably compact group definable in K, and defined with parameters from $\mathbb{Q}_p$. So in particular $G(\mathbb{Q}_p)$ is a compact p-adic Lie group.

Corollary 2.3. *Let $X \subseteq G$ be K-definable. Then*
(i) X is left generic if and only if X contains a translate of a definable subgroup of finite index if and only if X is right generic.
(ii) If $X = X_1 \cup X_2$ with X_i definable, and X is generic then one of the X_i is generic.
(iii) Any generic definable subset of G has a point in $G(\mathbb{Q}_p)$

Proof. (i) Suppose finitely many left translates of X cover G. By Proposition 2.2, one of them, say $a \cdot X$ contains an open $\mathbb{Q}_p$-definable subset U of G. So $U(\mathbb{Q}_p)$ is open in $G(\mathbb{Q}_p)$ and so as the latter is profinite, contains a translate $b \cdot H$ of an open subgroup H of $G(\mathbb{Q}_p)$ of finite index. H is definable in $\mathbb{Q}_p$, so let $H(K)$ be its interpretation in K. Then X contains $a^{-1} \cdot b \cdot H(K)$. It follows that X is also right generic.
(ii) By (i) let U be an open (in G) $\mathbb{Q}_p$-definable subset of X. Then $U = (U \cap X_1) \cup (U \cap X_2)$. By Proposition 2.2, one of $U \cap X_1$, $U \cap X_2$ contains an open $\mathbb{Q}_p$-definable subset of G and hence a translate of an open subgroup of finite index. Hence one of X_1, X_2 is generic.
(iii) follows from (i), as every coset of a finite index definable subgroup of G is defined over $\mathbb{Q}_p$ (by 1.4).

Corollary 2.4. *(The naive conjecture holds.) G^{00} exists and equals G^0. So G/G^{00} is $G(\mathbb{Q}_p)$.*

Proof. Let H be any type-definable subgroup of G of bounded index. Let $(X_i : i \in I)$ be a (small) family of definable subsets of G such that $H = \cap_{i \in I} X_i$. As H has bounded index in G it follows that each X_i is generic. As H is a group, we may choose the X_i such that also $H = \cap_{i \in I} X_i \cdot X_i^{-1}$. By Corollary 2.3 (i) each $X_i \cdot X_i^{-1}$ contains a definable subgroup H_i of finite index in G. Thus $G^0 \subseteq \cap_{i \in I} H_i \subseteq H$.

We have shown that G^0 is the smallest type-definable subgroup of G of bounded index. But G^0 is clearly the group of infinitesimals of G, hence is the kernel of the standard part map from G onto $G(\mathbb{Q}_p)$.

Corollary 2.5. *Let G be a any group definable in K, and defined over $\mathbb{Q}_p$. Then the refined conjecture holds.*

Proof. $G(\mathbb{Q}_p)$ is a semialgebraic p-adic Lie group. It has an open compact subgroup which will be semialgebraic and thus of the form $H(\mathbb{Q}_p)$ for a $\mathbb{Q}_p$- definable subgroup H of G. Corollary 2.4 then applies to H.

3. Elliptic curves over p-adically closed fields

We start by recalling from [16] some facts concerning elliptic curves, their isomorphisms, and their points over p-adic fields. We may at some point assume $p \neq 2$ for simplicity.

K will for now be an arbitrary perfect field. An elliptic curve E over K is a smooth projective curve over K equipped with a distinguished K-rational point 0 say. E then has a unique structure of an algebraic group over K with identity 0. We will say that E is in *Weierstrass form* (over K) if it is given by a smooth cubic in $\mathbb{P}^2$ with affine equation
(*) $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$,
where $a_i \in K$. The identity element of the elliptic curve is the point at infinity, namely the point in $\mathbb{P}^2$ with homogeneous coordinates $[0, 1, 0]$. Moreover any such smooth cubic over K gives an elliptic curve over K,

Fact 3.1. *(*[16]*, III.3.1)*
(i) Any elliptic curve over K is isomorphic over K to an elliptic curve in Weierstrass form.
(ii) If E, E' are elliptic curves over K in Weierstrass form, and E is isomorphic over K to E' then such an isomorphism can be given by some change of variables $x = u^2x' + r$, $y = u^3y' + su^2x' + t$, with $u, r, s, t \in K$ and $u \neq 0$. Conversely any such isomorphism preserves Weierstrass form.

Given an elliptic curve E over K, we will in general say that (*) is a Weierstrass equation for E over K if the $a_i \in K$ and E is isomorphic over K to the curve given by (*).

To a given Weierstrass equation for an elliptic curve over K is associated its discriminant Δ a certain polynomial function of the a_i.

We now specialize to the case where $K = \mathbb{Q}_p$ (in fact more generally a local field which is complete with respect to a discrete valuation). If an elliptic curve E is defined by an equation with coefficients in $\mathbb{Z}_p$ then we can apply the reduction map to these coefficients to obtain a (possibly) singular curve $\tilde{E}$ over $\mathbb{F}_p$. As we can choose homogeneous coordinates for any point $P \in E(\mathbb{Q}_p)$ we can also form a reduction map from $E(\mathbb{Q}_p)$ to $E(\mathbb{Z}_p)$ which takes P to $\tilde{P}$.

By a *minimal Weierstrass equation* for an elliptic curve over $\mathbb{Q}_p$, we mean a Weierstrass equation (*) over $\mathbb{Q}_p$ for E, such that the $a_i \in \mathbb{Z}_p$, and $v(\Delta)$ (which will be a positive integer) is minimized. The definitions of good, (split) multiplicative, and additive reduction of E can be given as a function of a minimal Weierstrass equation for E. But for now we just recall some canonical subgroups of $E(\mathbb{Q}_p)$:
Fix a minimal Weierstrass equation for an elliptic curve E over $\mathbb{Q}_p$. Let $E_0(\mathbb{Q}_p)$ be the set of points $P \in E(\mathbb{Q}_p)$ such that $\tilde{P}$ is in $\tilde{E}_{ns}(\mathbb{F}_p)$ (where $\tilde{E}_{ns}$ is the set of nonsingular points of $\tilde{E}$). Let $E_1(\mathbb{Q}_p)$ be the set of $P \in E(\mathbb{Q}_p)$ such that $\tilde{P} = \tilde{0}$ (where 0 is the identity element of E). Clearly E_1 is a subset of E_0. With this notation:

Fact 3.2. *(i) $E_0(\mathbb{Q}_p)$ and $E_1(\mathbb{Q}_p)$ are subgroups of $E(\mathbb{Q}_p)$,*
(ii) $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ is either a group of order at most 4, or a cyclic group of order $v(\Delta) = -v(j)$ (where j is the j-invariant of E).
(iii) $E_0(\mathbb{Q}_p)/E_1(\mathbb{Q}_p)$ is isomorphic (via the reduction map) to the group $\tilde{E}_{ns}(\mathbb{F}_p)$.
(iv) $E_1(\mathbb{Q}_p)$ is isomorphic (via the p-adic logarithm map) to the additive group $\mathbb{Z}_p$.

The second possibility in 3.2(ii) above corresponds to when E has "split multiplicative reduction", and the order of the cyclic group can be anything one wants. These are the so-called *Tate curves* discussed in Appendix C, section 14, of [16], and in more detail in Chapter V of [17]. More precisely for every $q \in \mathbb{Q}_p$ with $v(q) > 0$, we can consider the p-adic analytic group ${\mathbb{Q}_p}^*/ < q >$ (where $< q >$ denotes the cyclic subgroup of the multiplicative group generated by q) and find a p-adic analytic isomorphism of it with an elliptic curve E_q given by $y^2 + xy = x^3 + a_4x + a_6$ where a_4 and a_6 are given by certain power series in q. This is already a minimal Weierstrass equation for E_q. Under this isomorphism ${\mathbb{Z}_p}^*$ goes to $(E_q)_0(\mathbb{Q}_p)$, so this induces an isomorphism f_q of $E_q(\mathbb{Q}_p)/(E_q)_0(\mathbb{Q}_p)$ with $\mathbb{Z}/v(q)\mathbb{Z}$ (a quotient of the value group $\mathbb{Z}$). Although each subgroup $n\mathbb{Z}$ is definable, the subgroups are not uniformly definable as n varies. On the other hand we can also view $\mathbb{Z}/n\mathbb{Z}$ as the the interval $[0, n)$ in $\mathbb{Z}$ with addition mod n, and these groups ARE now uniformly definable as n varies. Note also that the subgroups $(E_q)_0(\mathbb{Q}_p)$ of $E_q(\mathbb{Q}_p)$ are uniformly definable as q varies. We will point out that the isomorphisms f_q are uniformly definable in the field structure on $\mathbb{Q}_p$. This easily follows from the analysis in [17].

Let us recall first the isomorphism from $\mathbb{Q}_p/<q>$ to $E_q(\mathbb{Q}_p)$: So $q \in {\mathbb{Q}_p}^*$ and $v(q) > 0$. Let $X(u,q)$ and $Y(u,q)$ be the following power series:

(1) $X(u,q) = \frac{1}{u+u^{-1}-2} + \sum_{n\geq 1}(\frac{q^n u}{1-q^n u)^2} + \frac{q^n u^{-1}}{1-q^n u^{-1})^2} - 2\frac{q^n}{(1-q^n)^2})$

(2) $Y(u,q) = \frac{u^2}{(1-u)^3} + \sum_{n\geq 1}(\frac{(q^n u)^2}{(1-q^n u)^3} - \frac{q^n u^{-1}}{(1-q^n u^{-1})^3} + \frac{q^n}{(1-q^n)^2})$

Fact 3.3. *([17], V.3 and 4)*
(i) The series $X(u,q), Y(u,q)$ converge for $u \in {\mathbb{Q}_p}^* \setminus <q>$, and the map ϕ_q taking $u \in {\mathbb{Q}_p}^*$ to $(X(u,q), Y(u,q))$ and $<q>$ to the identity is a surjective homomorphism with kernel $<q>$ from ${\mathbb{Q}_p}^*$ to $E_q(\mathbb{Q}_p)$.
(ii) The image of $\mathbb{Z}_p$ under ϕ_q is precisely $(E_q)_0(\mathbb{Q}_p)$.
(iii) For each nonzero coset C of $(E_q)_0(\mathbb{Q}_p)$ in $E_q)(\mathbb{Q}_p)$ exactly one of the following occurs:
(a) $0 < v(x) = v(y) < v(q)/2$, for all $(x,y) \in C$
(b) $0 < v(x) < v(q)/2$ and $v(x) < v(y)$, for all $(x,y) \in C$.
(c) $v(x) = v(x+y) = v(q)/2$ for all $(x,y) \in C$

Lemma 3.4. *Let $u \in \mathbb{Q}_p$ with $0 < v(u) < v(q)$. Then $v(X(u,q)) \geq min(v(u), v(q) - v(u))$ with equality if $v(u) \neq v(q) - v(u)$, and $v(Y(u,q)) \geq min(2v(u), v(q) - v(u))$ with equality if $2v(u) \neq v(q) - v(u)$.*

Proof. This is immediate from the expressions above for $X(u,q)$ and $Y(u,q)$.

Corollary 3.5. *The map f_q which takes elements of $(E_q)_0(\mathbb{Q}_p)$ to 0 and elements of $E_q(\mathbb{Q}_p) \setminus (E_q)_0(\mathbb{Q}_p)$ to $v(x)$ if $v(x) < v(y)$ and to $v(q) - v(x)$ if $v(x) = v(y)$, is a surjective homomorphism from $E_q(\mathbb{Q}_p)$ to the group $([0, v(q)), +(modv(q))$, with kernel $(E_q)_0(\mathbb{Q}_p)$.*

Note that $v(q)$ is definable uniformly from the coefficients of E_q (as $v(q) = v(\Delta)$). So clearly by the Corollary we have established that the maps $f_q : E_q(\mathbb{Q}_p) \to [0, v(q)) \subset \mathbb{Z}$ are uniformly definable as E_q varies.

Consideration of "nonstandard" Tate curves will show the naive conjecture from section 1 to be false, as we now point out.

Let K now be a saturated elementary extension of the field $\mathbb{Q}_p$.

Definition 3.6. *By a nonstandard Tate curve we mean an elliptic curve over K which is a "nonprincipal ultraproduct" of Tate curves $(E_{q_i} : i < \omega)$ with $v(q_i) < v(q_j)$ for $i < j$. Namely E is defined by an equation $y^2 + xy = x^3 + b_4 x + b_6$ where $tp(b_4, b_6)$ is a limit point of $tp(a^i_4, a^i_6)$ with (a^i_4, a^i_6) the appropriate coefficients of E_{q_i}.*

Let E and $\{q_i : i < \omega\}$ be as in the definition above. Then by uniform definability of the maps f_q there is a definable homomorphism from $E(K)$ onto a group of the form $([0,a), +(moda))$ where $a \in \Gamma$ realizes the corresponding limit of $\{tp(v(q_i) : i \in \omega\}$. In particular $a \geq n$ for all $n \in \mathbb{Z}$. It is now routine to construct the correct infinitesimal subgroup of $([0,a), +(moda))$: for each $n > 0$ let $b_n \in \Gamma$ be such that nb_n is congruent to a modulo some element of $\mathbb{Z}$. Then $\{x \in \Gamma : 0 \leq x < b_n$ for all $n > 0\}$ is a type-definable subgroup of $([0,a), +(moda))$ of bounded index which is not the intersection of definable subgroups. It's preimage in $E(K)$ has the same property. Hence we have:

Proposition 3.7. *For every nonstandard Tate curve E over K, $E(K)$ has a type-definable subgroup of bounded index which is not the intersection of definable subgroups. So $E(K)^0 \neq E(K)^{00}$.*

On the other hand, fix a prime l different from p and let q_i be such that $v(q_i) = l^i$. Let E be a nonprincipal ultraproduct of the E_{q_i}. By Corollary 3.5, each $E_{q_i}(\mathbb{Q}_p)$ has a definable quotient isomorphic to the cyclic group of order l^i. Hence for each n, $E(K)$ has a definable subgroup of index l^i. So $E(K)/E(K)^0$ could not have a subgroup of finite index which is pro-p. Namely:

Proposition 3.8. *There is a nonstandard Tate curve E over K such that $E(K)/E(K)^0$ (the definable porofinite completion of $E(K)$) is not a compact p-adic Lie group.*

The next result shows that refined conjecture from section 1 to be true for elliptic curves.

Proposition 3.9. *For any elliptic curve E over K, $E(K)$ has a definable open subgroup H such that H/H^0 is isomorphic (as a profinite group) to $\mathbb{Z}_p$.*

Proof. By Fact 3.1 we may assume that E is given in Weierstrass form. As any definable subset of $\Gamma_{\geq 0}$ has a least element, and as the transformations preserving Weierstrass form are uniformly definable, we find a "minimal Weierstrass equation"
$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
for E. Let $E_1(K)$ be the set of points P of $E(K)$ such that $\tilde{P} = \tilde{0}$. Now in $\mathbb{Q}_p$, whenever E' is an elliptic curve in minimal Weierstrass form then $E'_1(\mathbb{Q}_p)$ is isomorphic to $\mathbb{Z}_p$. It follows by transfer that $E_1(K)$ is (as an abelian group) a saturated model of $Th(\mathbb{Z}_p)$.
Claim. $E_1(K)^0 = \cap_n p^n E_1(K)$.
Proof. By $E_1(K)^0$ we mean of course in the sense of the the p-adically

closed field K, not just the abelian group $E_1(K)$. However note that $\cap_n p^n E_1(K)$ is torsion-free and divisible, hence has NO subgroups of finite index. This gives the claim.
It now follows, as $(E_1(K), +)$ is a model of $Th(\mathbb{Z}_p)$ that $E_1(K)/E_1(K)^0)$ is precisely $\mathbb{Z}_p$ and we finish.

Finally we observe that our analysis yields:

Remark 3.10. *(i) For E an elliptic curve over K, the definable profinite completion of $E(K)$ itself is a compact p-adic Lie group of dimension 1, as long as E is not a nonstandard Tate curve.*
(ii) Let E be any elliptic curve over K. Then $E(K)$ is not definably connected-by-finite. Namely $E(K)/E(K)^0$ is infinite.

References

[1] A. Berarducci and M. Otero, An additive measure in o-minimal expansions of fields, Quaterly Journal of Math., 55 (2004), 411-419.

[2] A. Berarducci, M. Otero, Y. Peterzil and A. Pillay, A descending chain condition for groups definable in o-minimal structures, to appear in Annals of Pure and Applied Logic.

[3] Raf Cluckers, Model theory of valued frields, preprint.

[4] J. D. Dixon, M.P.F. du Sautoy, A. Mann and D. Segal, *Analytic pro-p Groups*, LMS Lecture Notes Series 157, Cambridge University Press, 1991.

[5] K. H. Hofmann and S.A. Morris, *Compact Groups.*

[6] E. Hrushovski, Unpublished notes.

[7] A. Macintyre, On definable subsets of p-adic fields, Journal of Symbolic Logic, 41(3), 1976.

[8] A. Nesin and A. Pillay, Open subgroups of $GL_2(\mathbf{Q}_p)$, Proceedings of Easter meeting, DDR (1989)

[9] Y. Peterzil and A. Pillay, Generics in definably compact groups, preprint 2004.

[10] Y. Peterzil and C. Steinhorn, Definable compactness and definable subgroups of o-minimal groups, J. London Math. Soc., 59 (1999), 769-786.

[11] A. Pillay, Type-definability, o-minimality, and compact Lie groups, to appear in Journal of Math. Logic.

[12] A. Pillay, Some model theory of real and p-adic algebraic groups, Journal of Algebra, 126 (1989), 139-146.

[13] A. Pillay, On fields definable in $\mathbb{Q}_p$, Archive Math. Logic, 29 (1989), 1-7.

[14] B. Poizat,*Groupes stables*,1987.

[15] Ph. Scowcroft and L. van den Dries, On the structure of semialgebraic sets over p-adic fields, JSL, vol 53 (1988).

[16] J. H. Silverman, *The arithmetic of elliptic curves*, Springer, 1986.

[17] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer, 1994