One dimensional groups definable in the p-adic numbers and groups definable in Presburger arithmetic

Juan Pablo Acosta

For the first main result I set up some notation

$U_\alpha = \{x \in Q_p^\times \mid v(x-1) \geq \alpha\}$.

Given $a \in Q_p^\times$ such that $v(a) > \mathbb{Z}$, set

$O(a) = \{x \in Q_p^\times \mid$ there exists $n \in \mathbb{Z}_{>0}, |v(x)| \leq nv(a)\}$

$o(a) = \{x \in Q_p^\times \mid$ for all $n \in \mathbb{Z}_{>0}, n|v(x)| < v(a)\}$.

If $d \in \mathbb{Q}_p^\times \setminus (\mathbb{Q}_p^\times)^2$ with $v(d) \geq 0$ set

$$F(d) = \{\begin{bmatrix} x & dy \\ y & x \end{bmatrix} \mid x^2 - dy^2 = 1\}, \text{ and}$$

$$F_\alpha(d) = \{\begin{bmatrix} x & dy \\ y & x \end{bmatrix} \mid x^2 - dy^2, v(x-1) \geq \alpha, v(y) \geq \alpha\}$$

Given an elliptic curve E with minimal Weierstrass equation $f(x, y)$

Set $E_{1,\alpha}$ to be $\{(x, y) \in E \mid v(x) < 0, v(xy^{-1}) \geq \alpha\}$ together with the point at infinity.

$U_\alpha, F_\alpha(d)$ and $E_{1,\alpha}$ form fundamental systems of neighborhoods around the unit which are a filtration by subgroups.

The main result is the following

Theorem

If G is a one dimensional group definable in the p-adic numbers then there exists $K \leq H \leq G$ such that H is definable and of finite index in G, H is abelian, K is a finite subgroup and H/K is definably isomorphic to one of the following groups

1. $(Z_p, +)$
2. $(Q_p, +)$
3. $(Q_p^{\times}, \cdot)$
4. U_α
5. $O(a)^n/\langle a^n \rangle$
6. $F_\alpha(d)$
7. $E_{1,\alpha}$
8. $O_E(a)^n/\langle a^n \rangle$, E *a nonstandard Tate elliptic curve*

The result relies on the following

Theorem

(S. Montenegro, A. Onshuus, P. Simon)
Let G be a group definable in a NTP_2 theory which extends the theory of fields and which is algebraically bounded. If G is definably amenable then G has a type-definable subgroup of bounded index T and there is an algebraic group H and a type-definable group morphism $T \to H(K)$ with finite kernel.

Maybe the most restrictive hypothesis is definable amenability which in this case holds from

Theorem

(A. Pillay, N. Yao)
If G is a one dimensional group definable in Q_p then G is abelian-by-finite.

Connected one dimensional algebraic groups are classified in a result from algebraic geometry.
Over a field of characteristic 0 they are the additive group, the multiplicative group, the twisted multiplicative group, and the elliptic curves.
So we look at each of these cases and calculate their type-definable subgroups.

The additive case

The type-definable subgroups of $(Q_p, +)$ are bounded intersections of balls around the origin. The proof goes as follows:
A definable subgroup G has, as a definable set, a cell decomposition $G = X_1 \cup \cdots \cup X_n$.
The cells are translates of annuli around the origin intersected with cosets of $(Q_p^\times)^n$.
But as G is a group then also $G = \langle X_1 \rangle + \cdots + \langle X_n \rangle$.
It becomes a matter of calculating the group generated by a cell.
If we have a type-definable injective group map $T \to H$ where T is an intersection of balls, this extends by compactness to a definable group injection $(Z_p, +) \cong B \to H$.

The multiplicative case

The proof of the determination of the type-definable subgroups of $Q_p^\times$ follows the same idea as the additive case.
The multiplicative group has a feature the additive group does not have, the type-definable subgroup $o(a)$ is not a bounded intersection of definable subgroups.
We have that $O(a)/o(a) \cong \mathbb{R}$ (valuation followed by standard part).
Now use the observation that $\mathbb{R}$ has a local-to-global extension property: For every local group morphism from a local subgroup of $\mathbb{R}$, its germ extends in a unique way to a global group morphism.
In the same way given $o(a) \to G$ we get a group morphism $O(a) \to G$. And then its kernel generated by one element.

The twisted multiplicative group I

Given a degree two extension $Q_p(\sqrt{d})/Q_p$ we have a norm map $N : Q_p(\sqrt{d})^\times \to Q_p^\times$. Given explicitly $N(a + b\sqrt{d}) = a^2 - db^2$.
The Q_p-points of the twisted multiplicative groups are the subgroups of $Q_p(\sqrt{d})^\times$ of norm 1.
$F(d)$ acts by multiplication Q_p-linearly on $Q_p(\sqrt{d})$ so we get a group injection $F \to \mathrm{GL}_2(Q_p)$ once we fix a basis, say $\{1, \sqrt{d}\}$.
This is were the matrix group seen before comes in

$$F(d) = \{\begin{bmatrix} x & dy \\ y & x \end{bmatrix} \mid x^2 - dy^2 = 1\}.$$

The twisted multiplicative group II

The twisted multiplicative group is definable over $\mathbb{Q}_p$ and its $\mathbb{Q}_p$-points form a compact p-adic Lie group.
The exponential function is an isomorphism of an open, finite index subgroup onto $(Z_p, +)$.
This is a function definable in the analytic expansion of the valued field language, which is also well behaved. In particular analytic definable subsets of one-dimensional algebraically definable sets are algebraically definable. (p-minimality).
So up to finite index type-definable subgroups of $F(d)$ are bounded intersections of $F_\alpha(d)$

Elliptic curves I

The K-points of an elliptic curve are of the form $\{(x, y) \mid y^2 = x^3 + ax + b\}$ together with a point at infinity. This is a projective algebraic curve. It is also an algebraic group.

Elliptic curves II

In Q_p, the elliptic group E either has a finite index subgroup where the p-adic exponentiation gives an isomorphism with $(Z_p, +)$ or it is a Tate curve.
A Tate curve has a uniformization map $O(a)/\langle a \rangle \cong E$ definable in the analytic language.
Using translations we can obtain a definable copy of $O(a)$, O_E. As in the observation that an Abelian topological, local lie group is a Lie group.
More precisely O_E is an $\vee$-definable group with an analytically definable group isomorphism $O_E \cong O(a)$, such that the composition $O_E \to O(a) \to E$ is definable.

Lattices

The second main theorem concerns groups definable in Presburger arithmetic. Presburger arithmetic is the theory of $(Z, +, <)$. We need some terminology

- For $a = (a_1, \ldots, a_r) \in Z^r$, $O(a) = O(a_1) \times \cdots \times O(a_r)$ and $o(a) = o(a_1) \times \cdots \times o(a_r)$.
- A lattice $\Lambda \subset \mathbb{R}^r$ is a subgroup or $(\mathbb{R}^r, +)$ which is discrete in the subspace topology.
- Equivalently it is generated as a group by linearly independent elements.
- The lattice is full if the linear span is the whole $\mathbb{R}^r$.
- In other words it it is generated by a basis.
- A local lattice $\Lambda \subset O(a)$ is a subgroup such that $\Lambda \cap o(a) = 0$ and $st(\Lambda)$ is a full lattice.
- In other words $\Lambda = \sum_i \mathbb{Z} b_i$ for $\{st(b_i)\}_i$ a basis.

Bounded Groups

A set $X \subset Z^r$ is bounded if $X \subset [-a, a]^r$ for a $a \in Z$.
This is a definable invariant.
If $\Lambda \subset O(a)$ is a local lattice then $O(a)/\Lambda$ is a bounded definable group.

Theorem

(A. Onshuus, M. Vicaria)
If G is a group definable in $(Z, +, <)$, then G is abelian-by-finite

Theorem

(A. Onshuus, M. Vicaria)
If A is a bounded definable group in $(Z, +, <)$, then A has a finite index group isomorphic as a definable group to $O(a)/\Lambda$.

Theorem

If A is an abelian group definable in $(Z, +, <)$ then there exists a subgroup $B \subset A$ isomorphic as a definable group to Z^r such that A/B is bounded.

Proof, associativity

We start with the particular case $A = (Z, \oplus)$, such that $\oplus$ is afin.

$$a \oplus b = na + mb + d$$

Then from associativity we get So $n^2 = n$ and $m^2 = m$.
$\oplus$ is injective on each factor so $n, m \neq 0$ and so $n = m = 1$.
Where does d come from?
$Z \to Z$ the function $x \mapsto x + d$ is a bijection. The sum $\oplus$ is the one that makes $(Z, \oplus) \to (Z, +)$ a group isomorphism.

Proof, groupification

Now for a more general case $(Z_{\geq 0}, \oplus)$, $\oplus$ is cell-wise afine. We assume the cells do not have divisibility conditions.
On the triple (x, y, z) such that $c \ll x \ll y \ll z$ we may apply the associativity calculation of the previous frame to obtain
$x \oplus y = x + y$.
The subsemigroup $\{x \mid c \ll x\} \subset (Z, +)$ recovers the entire group $(Z, +)$. $(Z, +)$ is the groupification.
Similarly the function $f : Z \to A$, $f(x) = (x + y) \ominus y$ for $x \ll y$ is a group morphism.

Proof, divisibility

What happens if the sum $(Z_{\geq 0}, \oplus)$ has cells with divisibility conditions?
The divisibility type of a point $x \in Z$ is an element of $\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$ which is a compact Hausdorff space.
If $c \ll x \ll y$ then $\widehat{x \oplus y} = \hat{x} \cdot \hat{y}$ forms a binary operation $\hat{\mathbb{Z}}^2 \to \hat{\mathbb{Z}}$ which is a semigroup operation. Definability of $\oplus$ implies $\cdot$ is continous.
The Ellis-Nakamura lemma gives an idempotent p. For x such that $\hat{x} = p$ the calculation in the previous frame works.

Proof, general underlying sets

What happens for more general underlying sets?
If $X = Z^r$ then we have to replace $\hat{\mathbb{Z}}$ by a set of "types at infinity".
If X is arbitrary definable then using cell decomposition we can see that after definable bijection $Z^r_{\geq 0} \times \{0\} \subset X \subset Z^r_{\geq 0} \times [0, a)^s$.

Proof, bounded factor

I will assume $(A, \oplus)$ has underlying set $Z_{\geq 0} \times [0, a)$. Also that the cells appearing in $\oplus$ have no divisibility condition.
Then for $c \ll x \ll y$, $(x, b) \oplus (y, c) = (z, b \cdot c)$. Where $\cdot$ is a semigroup operation on $[0, a)$. Definability of $\oplus$ implies that $\cdot$ is definable.
Having an idempotent is first order expressible so $\cdot$ has an idempotent. For this idempotent the previous calculation works.

Proof, end

The general case is a combination of the divisibility case and the bounded factor case. It just requires a version of the Ellis-Nakamura Lemma that includes bounded definable semigroups and profinite topological semigroups.
The relevant technical concept for the hypothesis is that of a pro-definable sets.

A group cohomology calculation

To finish the description of the definable groups we have to calculate group extensions. To do this we use a calculation of group cohomology.

If $0 \to B \to A \to C \to 0$ is a short exact sequence of abelian groups and $s : C \to A$ is a set-theoretic section of $A \to C$, then $A \cong B \times C$ as a set and from $s(a+b) = s(a) + s(b) + g(a,b)$ we get a function $g : C^2 \to B$ which determines the group structure of A.

Calculating $s(a+b+c)$ in two ways one obtains the constraint on g, $g(a+b,c) + g(a,b) = g(a,b+c) + g(b,c)$. (the cocycle condition).

If you change the section to $s'(a) = s(a) + f(a)$, $f : C \to B$, then g' and g are cohomologous (via f).

So group extensions A up to isomorphism are (in bijection to) 2-cocycles/2-coboundaries, the second group cohomology.

Group extensions

We have a short exact sequence $0 \to Z^r \to A \to C(a,b) \to 0$.
With $C(a,b) = O(a)/\sum_i \mathbb{Z}b_i$.
On $o(a) \subset O(a)$ take the elements "infinite under a" and divisible, these form a complete invariant type p.
On the set $p^{\otimes 3}$ we may apply the cocycle condition to see the 2-cocyle is trivial.
The formal differences technique, and the local-to-global principle of $\mathbb{R}$ give a group map $O(a) \to G$. This determines the isomorphism type of G.

Groups definable in Presburger arithmetic

Theorem

If G is a group definable in $(Z, +, <)$ then G has a finite index definable group isomorphic as a definable group to

$$Z^r \oplus O(a)/\sum_i \mathbb{Z}(b_i, c_i)$$

Where $b_i \in Z^r$ and $\sum_i \mathbb{Z}c_i \subset O(a)$ is a local lattice.