One dimensional groups definable in the p-adic numbers

Juan Pablo Acosta

For the 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

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

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

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

$F(d) = \{\begin{bmatrix} x & dy \\ y & x \end{bmatrix} \mid x^2 - dy^2 = 1\}$, 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 is a group definable in a NIP theory which extends the theory of fields such the field K 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.

The additive case I

A connected one dimensional algebraic group over a field of characteristic 0 is the additive group, the multiplicative group, a twisted multiplicative group or an elliptic curve.
In the case of the additive group $(Q_p, +)$ the type-definable subgroups are either Q_p or bounded intersection of balls around the origin. So we may finish by compactness. These are the cases Z_p and Q_p.

The additive case II

The proof of the determination of the type-definable subgroups of Q_p in the previous frame is in outline as follows. Such a group T is a bounded intersection of definable sets S_i. Each of the sets S_i has a cell decomposition which is a finite union of annuli intersected with $(Q_p^\times)^n$ cosets. An important part of the group generated by S_i is already in $S_i - S_i$, as we can fill the hole of the annuli in two steps. As this number two does not depend on the definable set S_i one can obtain the result required.

The multiplicative case I

In the multiplicative case the type-definable groups $G \subset Q_p^\times$ fall in two cases.
If $v(G) = 0$, G is a direct product of a group generated by a root of unity and a bounded intersection of U_α. In this case we conclude like in the additive case. This is the case U_α.
If $v(G) \neq 0$, then it is $Q_p^\times$ or is a bounded intersection of $o(a_i)$ intersected with groups $G_n = (Q_p^\times)^n G$ between $(Q_p^\times)^n$ and $Q_p^\times$.
This is the case $O(a)^n/\langle a^n \rangle$.

The multiplicative case II

The proof of the determination of the type-definable subgroups of $Q_p^\times$ with non-trivial valuation follows the same outline, with different details, as the additive proof case.
The trivial valuation case follows from the isomorphism via the natural exponential function, which is definable in the analytic language, $Z_p \to U_1$ which takes the filtration D_α into $U_{\alpha+1}$. As the analytic language has a cell decomposition we conclude from the additive case.
The final isomorphism with $O(a)^n/\langle a^n \rangle$ is as follows, $O(a)/o(a) \cong O_Z(v(a))/o_Z(v(a)) \cong \mathbb{R}$, the first given by the valuation and the second similar to the real case. A morphism $o(a) \to G$ generates by compactness a morphism of local groups $U \to G/T$ $U \subset \mathbb{R}$. The germ of this morphism extends in a unique way to a morphism of groups $\mathbb{R} \to G/T$. The kernel is a discrete subgroup. This gives the isomorphism.

The twisted multiplicative case

The twisted multiplicative group is the group of elements of norm 1 in a extension of degree two $Q_p(\sqrt{d})$ of the field Q_p. This group acts linearly on $Q_p(\sqrt{d})$ by multiplication, so it embeds as $F(d) \subset \mathrm{GL}_2(Q_p)$.
Over the standard model $\mathbb{Q}_p$ this is a one-dimensional compact p-adic Lie group, so there is an exponential map $\mathbb{Z}_p \to F(d)(\mathbb{Q}_p)$ which is an isomorphism onto a finite index open subgroup, and sends the filtration $\{D_\alpha\}$ into the filtration $\{F_{\alpha+1}(d)\}$. This morphism is definable in the analytic language, so we conclude that any type-definable subgroup of $F(d)$ is a bounded intersection of groups of the form $F_\alpha(d)$. Also we may conclude as in the additive case by compactness.

The elliptic curve case I

The elliptic curve case divides into some cases called additive, split multiplicative, non-split multiplicative and good case, depending of the isomorphism type of E mod p. In the additive, the non-split multiplicative, the good case, and in the split multiplicative case with discriminant in $\mathbb{Z}$, there is a finite index subgroup which is isomorphic via an exponential map definable in Q_p^{an} to Z_p, and which sends the filtration D_α into $E_{1,\alpha+2}$.
In the nonstandard split multiplicative case $O(a)/\langle a\rangle \cong E$ via the Tate uniformization map $O(a) \to E$ which is definable in Q_p^{an}.
Also U_α is sent into $E_{1,\alpha}$. Finally one constructs a $\vee$-definable (in Q_p) group O_E with a Q_p^{an} isomorphism $O \to O_E$, such that under this isomorphism the Tate uniformization map becomes Q_p-definable and $O_E^n/\langle a^n\rangle$ is Q_p-definable, so we finish as in the multiplicative case.

The elliptic curve case II

The construction of O_E in the previous frame is in outline as follows.
The uniformization map $O \to E$ sends o to a type-definable group. This is not immediate but follows from the proofs in the Tate uniformization treatment in Silverman's book. From a set of O which contains o and is in bijection with a definable set of E via the uniformization map, we obtain a definable structure on a copy of O by translation.