

# COMPOSITIO MATHEMATICA

RICHARD PINK

**Classification of pro- $p$  subgroups of  $SL_2$  over a  $p$ -adic ring, where  $p$  is an odd prime**

*Compositio Mathematica*, tome 88, n° 3 (1993), p. 251-264

[http://www.numdam.org/item?id=CM\\_1993\\_\\_88\\_3\\_251\\_0](http://www.numdam.org/item?id=CM_1993__88_3_251_0)

© Foundation Compositio Mathematica, 1993, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (<http://www.compositio.nl>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

## Classification of pro- $p$ subgroups of $SL_2$ over a $p$ -adic ring, where $p$ is an odd prime

RICHARD PINK

*Max Planck Institut für Mathematik, Gottfried Claren Str. 26, 5300 Bonn 3, Germany*

Received 15 March 1991; accepted in revised form 26 August 1992

Let  $A$  be a semi-local ring and  $I$  the intersection of its maximal ideals. We assume that  $A$  is complete and compact with respect to the  $I$ -adic topology, and that  $A/I$  is annihilated by an odd rational prime  $p$ . The main example we have in mind is a flat algebra of finite degree over  $\mathbf{Z}_p$  or over  $\mathbf{Z}_p[[X]]$ .

The aim of this article is to give a convenient description for all pro- $p$  subgroups  $\Gamma \subset SL_2(A)$ . Here “convenient” means that the congruence conditions defining  $\Gamma$  should have a simple standard form. Let us call a pro- $p$ -subgroup *basic* if it can be written as

$$\{x \in SL_2(A) \mid x - \text{Id} \in M\}$$

for some closed subgroup  $M$  of the additive group of  $2 \times 2$ -matrices with entries in  $A$ . (Caution: beginning with an  $M$ , this defines a pro- $p$  group only under certain additional conditions, cf. section 2.) Although there exist other subgroups, the basic ones are pervasive enough. Hereafter, when we speak of the descending central or the derived series of a pro-finite group, we always mean the *closed* subgroups that are topologically generated by the respective commutators. Let  $\Gamma'$  denote the (by our convention, closed) commutator subgroup of  $\Gamma$ . The following result is typical.

**COROLLARY (3.5)** *The descending central and derived series of  $\Gamma$ , beginning with  $\Gamma'$ , consist of basic subgroups.*

For the classification, then, let  $H_1$  denote the unique smallest basic subgroup containing  $\Gamma$ . It turns out that  $\Gamma' = H_1$ , hence giving  $\Gamma$  is equivalent to giving  $H_1$  and a certain subgroup of the abelian factor group  $H_1/H_1'$ . For the full statement see theorem 3.4.

More information about the method is given in the introduction to each section. Here let us only mention that it might have been nice to use the Campbell-Hausdorff formula (see Lazard [3] 3.2.2) to express everything in terms of the Lie algebra right from the beginning. Unfortunately this formula is applicable only for “small” congruence subgroups.

Since  $p$  is odd and the order of the center of  $\mathrm{SL}_2(A)$  is a power of 2 our results immediately extend to pro- $p$  subgroups of  $\mathrm{GL}_2(A)$  or of  $\mathrm{PGL}_2(A)$ . Moreover, it should now be easy to extend the classification to arbitrary closed subgroups  $\Gamma$ . Namely, consider the maximal normal pro- $p$  subgroup  $\Gamma_+$  of  $\Gamma$ ; it has finite index. Our results give an explicit description for  $\Gamma_+$ , and it should be standard to analyze the possible extensions. When  $\Gamma$  contains sufficiently many elements of order prime to  $p$  the analysis is easier, because these elements induce symmetries which can be used to decompose  $\Gamma_+$ . (For a similar situation compare Borevich and Vavilov [1], [5].) In [4] Papier considered the case of a pro- $p$  subgroup normalized by the matrix

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

under certain additional assumptions. There the extra symmetry was too weak to provide substantial simplifications. Papier's treatment of this case was the main inspiration – and the model – for the present article.

The results in this article cannot be extended directly to the case  $p = 2$  or to larger linear groups, say  $\mathrm{GL}_n$ . For instance, corollary (3.5) becomes false for  $p = 2$ ; the quaternion group yields a counterexample. It would be interesting to test the following hypothesis. Let  $A$  be as above, but for arbitrary  $p$ .

**HYPOTHESIS  $H(n, p)$ .** *There exists an integer  $m(n, p)$ , depending only on  $n$  and  $p$ , such that the descending-central series of any pro- $p$  subgroup  $\Gamma \subset \mathrm{GL}_n(A)$ , beginning with the  $m(n, p)$ th step, consists of basic subgroups.*

Our result affirms  $H(2, p)$  for all odd  $p$ , with the best possible bound  $m(2, p) = 2$ .

The motivation for this article came from the study of  $l$ -adic representations of Galois groups. Here the closed subgroup  $\Gamma \subset \mathrm{GL}_2(A)$  arises as the image of the Galois group in a representation of rank 2 over  $A$ . Such a representation is typically associated to one or several classical holomorphic cusp forms on the upper half plane. For certain purposes it is important to have a good hold on the structure of  $\Gamma$ : for congruences of modular forms see, e.g., Papier [4]; for another application see joint work with Harder [2].

## 1. Universal formulas, and conventions

We begin with a collection of useful formulas that have a meaning for any ring of coefficients in which 2 is invertible. The (associative) algebra of  $2 \times 2$ -matrices is

denoted by  $\mathfrak{gl}_2$ , it is a Lie algebra via

$$[x, y] := xy - yx.$$

The subspace of all matrices of trace 0 is the simple Lie algebra  $\mathfrak{sl}_2$ . Letting  $\text{Id}$  denote the identity matrix, the canonical projection is given by

$$\Theta: \mathfrak{gl}_2 \rightarrow \mathfrak{sl}_2, x \mapsto x - \frac{\text{tr}(x)}{2} \cdot \text{Id}.$$

The (algebraic) group of all matrices  $x \in \mathfrak{gl}_2$  with determinant 1 is denoted by  $SL_2$ .

The following formulas are basic and easy to check. Let  $x, y \in \mathfrak{gl}_2$ .

$$[x, y] = [\Theta(x), y] = [x, \Theta(y)]. \tag{1.1}$$

$$[x, y] = \Theta(xy) - \Theta(yx). \tag{1.2}$$

$$2 \cdot \Theta(xy) = [\Theta(x), \Theta(y)] + \text{tr}(x) \cdot \Theta(y) + \text{tr}(y) \cdot \Theta(x). \tag{1.3}$$

$$2 \cdot \text{tr}(xy) = 2 \cdot \text{tr}(\Theta(x) \cdot \Theta(y)) + \text{tr}(x) \cdot \text{tr}(y). \tag{1.4}$$

$$\text{tr}(xy) = \text{tr}(yx). \tag{1.5}$$

$$\text{tr}(x)^2 = 4 \cdot \det(x) + 2 \cdot \text{tr}(\Theta(x)^2). \tag{1.6}$$

$$x, y \in \mathfrak{sl}_2 \Rightarrow \text{tr}(xy) \cdot \text{Id} = xy + yx. \tag{1.7}$$

$$x \in SL_2 \Rightarrow \Theta(x^{-1}) = -\Theta(x), \text{tr}(x^{-1}) = \text{tr}(x). \tag{1.8}$$

$$x \in SL_2 \Rightarrow \text{tr}(x) \cdot \Theta(y) = \Theta(xy) + \Theta(x^{-1}y). \tag{1.9}$$

The remaining two formulas hold for all  $x, y, u, v \in \mathfrak{sl}_2$ . Their straightforward, though tedious, proof is left to the reader.

$$4 \cdot \text{tr}(xy) \cdot [u, v] = [y, [x, [u, v]]] + [x, [y, [u, v]]] \\ + [[x, v], [y, u]] + [[y, v], [x, u]]. \tag{1.10}$$

$$4 \cdot \text{tr}([u, v] \cdot x) \cdot y = [y, [x, [u, v]]] - [x, [y, [u, v]]] \\ + [[x, v], [y, u]] + [[y, v], [x, u]]. \tag{1.11}$$

For the remainder of this article we fix a commutative ring with identity  $A$  satisfying the following conditions. Let  $I$  denote the intersection of all maximal ideals of  $A$ . We endow  $A$  with the  $I$ -adic topology, that is, the ideals  $I^n$  form a fundamental system of open neighborhoods of zero. We assume that  $A$  is compact with respect to this topology. This implies in particular that  $A$  is  $I$ -

adically separated and complete and is isomorphic to the inverse limit  $\varprojlim A/I^n$ . Moreover  $A/I$  is finite and without nilpotent elements, and  $A$  a semi-local ring. We assume that  $A/I$  is annihilated by an *odd* rational prime  $p$ .

Although we shall not use this, let us describe the possibilities for  $A$  a little more concretely. As a complete semi-local ring  $A$  must be a finite direct sum of complete local rings. It is easy to see that each direct summand is isomorphic to a quotient of a power series ring in finitely many variables  $\mathcal{O}[[X_1, \dots, X_n]]$ , where  $\mathcal{O}$  is the ring of integers in a finite unramified extension of  $\mathbf{Q}_p$ . The main example we have in mind is a flat algebra of finite degree over  $\mathbf{Z}_p$  or  $\mathbf{Z}_p[[X]]$ . Nevertheless in this article we allow  $A$  to have nilpotent elements; in particular any finite algebra that is annihilated by a power of  $p$  is an example.

Since we have assumed that  $p$  is odd, it is easy to extract square roots. Namely, by the  $I$ -adic completeness of  $A$  the binomial series defines a well-defined continuous map

$$I \rightarrow A, \quad \alpha \mapsto \sqrt{1 + \alpha} := \sum_{n=0}^{\infty} \binom{1/2}{n} \cdot \alpha^n.$$

Moreover, it is easy to check that this formula yields the unique solution of the equation  $\beta^2 = 1 + \alpha$  with  $\beta \equiv 1 \pmod I$ .

We shall use the following convention: when  $L, L' \subset \mathfrak{gl}_{2,A}$  and  $C \subset A$  are closed additive subgroups, then  $L \cdot L', [L, L'], \text{tr}(L), C^n$  etc. denote the closed additive subgroups generated by the described set.

Since  $A$  is compact, any closed subgroup of  $\text{SL}_2(A)$ —with respect to the obvious topology—is a pro-finite group. Any closed subgroup consisting of elements that are congruent to the identity modulo  $I$  is a pro- $p$  group. When we speak of the descending central or the derived series of a pro-finite group, we shall always mean the *closed* subgroups that are topologically generated by the respective commutators.

## 2. The structure of subgroups of a certain type

In this section we study certain pro- $p$  subgroups of  $\text{SL}_2(A)$ . By explicit calculations of commutators we express the descending central series for these subgroups in terms of Lie algebra data. In section 3 we shall prove *a posteriori* that the special assumptions made here are in fact always satisfied.

Throughout the section we fix a closed additive subgroup  $L \subset \mathfrak{sl}_{2,A}$  and define  $C := \text{tr}(L \cdot L) \subset A$ . We assume the following axioms:

$$\bigcap_n L^n = \{0\}. \tag{2.1.1}$$

$$[L, L] \subset L. \tag{2.1.2}$$

$$C \cdot L \subset L. \tag{2.1.3}$$

These axioms imply:

**PROPOSITION (2.2)**

$$\bigcap_n C^n = \{0\}. \text{ In particular } C \subset I. \tag{2.2.1}$$

$$C \cdot C \subset C. \tag{2.2.2}$$

*Proof.* For the first assertion observe that 1.7 implies  $C \cdot \text{Id} \subset L^2$ , so the assertion follows from 2.1.1. The second assertion is a consequence of 2.1.3 and the definition of  $C$ , namely by

$$C \cdot C = C \cdot \text{tr}(L \cdot L) = \text{tr}(C \cdot L \cdot L) \subset \text{tr}(L \cdot L) = C. \quad \square$$

The axiom 2.1.2 says that  $L$  is a Lie subalgebra of  $\mathfrak{sl}_{2,A}$ . We now define a descending sequence of closed additive subgroups inductively by

$$L_1 := L, \quad L_{n+1} := [L, L_n] \text{ for all } n \geq 1.$$

These are also Lie subalgebras; in fact we have more:

**PROPOSITION (2.3)**

$$\bigcap_n L_n = \{0\}. \tag{2.3.1}$$

$$L_{n+1} \subset L_n \text{ for all } n \geq 1. \tag{2.3.2}$$

$$[L_n, L_m] \subset L_{n+m} \text{ for all } n, m \geq 1. \tag{2.3.3}$$

$$C \cdot L_n \subset L_{n+2} \text{ for all } n \geq 2. \tag{2.3.4}$$

*Proof.* The first assertion follows from 2.1.1 since  $L_n \subset L^n$  for all  $n$ . The second follows from induction over  $n$ :

$$L_{n+2} = [L, L_{n+1}] \subset [L, L_n] = L_{n+1},$$

the case  $n = 1$  being just the assertion of 2.1.2. The third assertion holds by definition for  $n = 1$ . Proceeding by induction over  $n$ , consider elements  $x \in L$ ,  $y \in L_n$ , and  $z \in L_m$ . The Jacobi identity and the induction hypothesis show

$$\begin{aligned} [[x, y], z] &= [x, [y, z]] - [y, [x, z]] \\ &\in [L, [L_n, L_m]] + [L_n, [L, L_m]] \subset L_{n+m+1}, \end{aligned}$$

as desired. Finally apply formula 1.10 to elements of  $L$ . Using 2.3.3 the last assertion follows in the case  $n = 2$ . For general  $n$  we again use induction:

$$C \cdot L_{n+1} = C \cdot [L, L_n] = [L, C \cdot L_n] \subset [L, L_{n+2}] = L_{n+3}. \quad \square$$

Now we start transporting the given data to the group  $\mathrm{SL}_2(A)$ . For all  $n \geq 1$  define

$$H_n := \{x \in \mathrm{SL}_2(A) \mid \Theta(x) \in L_n, \mathrm{tr}(x) - 2 \in C\}.$$

These sets constitute a descending sequence of closed subgroups:

**PROPOSITION (2.4)**

$$\bigcap_n H_n = \{\mathrm{Id}\}. \quad (2.4.1)$$

For all  $n \geq 1$ :

$$H_{n+1} \subset H_n. \quad (2.4.2)$$

$$\text{The map } H_n \rightarrow L_n, x \mapsto \Theta(x) \text{ is a homeomorphism.} \quad (2.4.3)$$

$$H_n \text{ is a pro-} p \text{ subgroup of } \mathrm{SL}_2(A). \quad (2.4.4)$$

$$H_n \text{ is normalized by } H_1. \quad (2.4.5)$$

*Proof.* The first assertion follows from 2.3.1 and the third; the second assertion is a direct consequence of 2.3.2. For the third assertion consider the continuous map

$$L_n \rightarrow \mathrm{SL}_2(A), \quad u \mapsto u + \sqrt{1 + \mathrm{tr}(u^2)/2} \cdot \mathrm{Id}.$$

By the definition of  $C$  and by 2.2.1 we have  $\mathrm{tr}(u^2) \in C \subset I$ , so the square root is well-defined in the sense explained at the end of section 1. The relation 2.2.2 implies that the image of this map is contained in  $H_n$ . It is easy to check that this is the desired inverse map.

For the fourth assertion consider  $x, y \in H_n$ . Relation 1.8 immediately shows that  $x^{-1} \in H_n$ . As for the product, we have by 1.3

$$\begin{aligned} 2 \cdot \Theta(xy) &= [\Theta(x), \Theta(y)] + \mathrm{tr}(x) \cdot \Theta(y) + \mathrm{tr}(y) \cdot \Theta(x) \\ &\in [L_n, L_n] + L_n + C \cdot L_n \end{aligned}$$

which by 2.3 is contained in  $L_n$ . For the trace, 1.4 implies

$$\begin{aligned}
 & 2 \cdot (\text{tr}(xy) - 2) \\
 &= 2 \cdot \text{tr}(\Theta(x) \cdot \Theta(y)) + \text{tr}(x) \cdot \text{tr}(y) - 4 \\
 &= 2 \cdot \text{tr}(\Theta(x) \cdot \Theta(y)) + 2 \cdot (\text{tr}(x) - 2) + 2 \cdot (\text{tr}(y) - 2) \\
 &\quad + (\text{tr}(x) - 2) \cdot (\text{tr}(y) - 2) \\
 &\in \text{tr}(L \cdot L) + C + C^2
 \end{aligned}$$

which by 2.2.2 is contained in  $C$ . This shows that  $H_n$  is a subgroup of  $SL_2(A)$ . To prove the fourth assertion it remains to show that it is pro- $p$ . For this we may calculate modulo  $I$  which by 2.2.1 contains  $C$ . Thus without loss of generality we may assume that  $I = C = \{0\}$ . Then  $H_n$  is a finite group of the same cardinality as the finite  $\mathbb{F}_p$ -vector space  $L_n$ . This is a power of  $p$ , as desired.

For the last assertion we must prove that  $\Theta(xyx^{-1}) \in L_n$  for all  $x \in H_1$  and  $y \in H_n$ . We calculate

$$\begin{aligned}
 2 \cdot \Theta(xyx^{-1}) &= 2 \cdot \Theta(y + (xy - yx) \cdot x^{-1}) \\
 &= 2 \cdot \Theta(y) + 2 \cdot \Theta([x, y] \cdot x^{-1}) \\
 &\stackrel{1.3}{=} 2 \cdot \Theta(y) + [\Theta([x, y]), \Theta(x^{-1})] + \text{tr}(x^{-1}) \cdot \Theta([x, y]) \\
 &\stackrel{1.1}{=} 2 \cdot \Theta(y) + [[\Theta(x), \Theta(y)], \Theta(x^{-1})] + \text{tr}(x^{-1}) \cdot [\Theta(x), \Theta(y)] \\
 &\in L_n + [[L, L_n], L] + (2 + C) \cdot [L, L_n].
 \end{aligned}$$

By 2.3 this lies in  $L_n$ , as desired. □

Next we want to describe the group structure of  $H_n/H_{n+1}$ . Given  $x \in H_n$  or  $L_n$  we denote its residue class in  $H_n/H_{n+1}$ , respectively in  $L_n/L_{n+1}$ , by  $\bar{x}$ . For  $n \geq 2$  it is easy to determine the group structure of  $H_n/H_{n+1}$ . It is convenient to calculate commutators at the same time:

**PROPOSITION (2.5)**

(2.5.1) For all  $n \geq 2$  the map

$$H_n/H_{n+1} \rightarrow L_n/L_{n+1}, \quad \bar{x} \mapsto \overline{\Theta(x)}$$

is a well-defined bicontinuous group isomorphism. In particular,  $H_n/H_{n+1}$  is abelian.

(2.5.2) For all  $x \in H_1$  and  $y \in H_{n-1}$ , where  $n \geq 2$ , we have

$$\overline{\Theta(xyx^{-1}y^{-1})} = \overline{[\Theta(x), \Theta(y)]}$$

in  $L_n/L_{n+1}$ .



*Proof.* For the first assertion consider elements  $x, y \in H_n$ . The formula 1.3 implies

$$\begin{aligned} 2 \cdot (\Theta(xy) - \Theta(x) - \Theta(y)) &= [\Theta(x), \Theta(y)] + (\text{tr}(x) - 2) \cdot \Theta(y) \\ &\quad + (\text{tr}(y) - 2) \cdot \Theta(x) \\ &\in [L_n, L_n] + C \cdot L_n, \end{aligned}$$

and by 2.3 this is contained in  $L_{n+1}$ . This proves that the map  $H_n \rightarrow L_n/L_{n+1}$ ,  $x \mapsto \overline{\Theta(x)}$  is a group homomorphism. Clearly its kernel is  $H_{n+1}$ . By 2.4.3 it is surjective, hence the map in 2.5.1 is a well-defined group isomorphism. Since  $H_n/H_{n+1}$  is endowed with the quotient topology, the continuity of  $\Theta$  implies that of the map in question. The same argument, in combination with 2.4.3, shows that the inverse is continuous, and the first assertion is proved.

For the second assertion we calculate as above

$$\begin{aligned} 2 \cdot \Theta(xyx^{-1}y^{-1}) &= 2 \cdot \Theta(\text{Id} + (xy - yx)x^{-1}y^{-1}) \\ &= 2 \cdot \Theta([x, y] \cdot x^{-1}y^{-1}) \\ &\stackrel{1.3}{=} [\Theta([x, y]), \Theta(x^{-1}y^{-1})] + \text{tr}(x^{-1}y^{-1}) \cdot \Theta([x, y]) \\ &\stackrel{1.1}{=} [[\Theta(x), \Theta(y)], \Theta(x^{-1}y^{-1})] \\ &\quad + \text{tr}(x^{-1}y^{-1}) \cdot [\Theta(x), \Theta(y)]. \end{aligned}$$

Thus

$$\begin{aligned} 2 \cdot (\Theta(xyx^{-1}y^{-1}) - [\Theta(x), \Theta(y)]) & \\ &= [[\Theta(x), \Theta(y)], \Theta(x^{-1}y^{-1})] + (\text{tr}(x^{-1}y^{-1}) - 2) \cdot [\Theta(x), \Theta(y)] \\ &\in [[L, L_{n-1}], L] + C \cdot [L, L_{n-1}] \end{aligned}$$

which by 2.3 is contained in  $L_{n+1}$ , as desired.  $\square$

The group structure of  $H_1/H_2$  can also, in a way similar to 2.5.1, be characterized on  $L_1/L_2$ . The difficulty is that the latter set must be endowed with a group structure that may differ from the given additive group structure. To avoid a misunderstanding it is essential to keep in mind that  $L_1/L_2$  will continue to denote the set of all cosets  $x + L_2$  for  $x \in L_1$ , with the original additive group structure. Consider the map

$$L \times L \rightarrow L, (x, y) \mapsto x * y := \sqrt{1 + \text{tr}(x^2)/2} \cdot y + \sqrt{1 + \text{tr}(y^2)/2} \cdot x. \quad (2.6.0)$$

**PROPOSITION-DEFINITION (2.6)**

(2.6.1) *The map  $(\bar{x}, \bar{y}) \mapsto \overline{x * y}$  induces a well-defined composition law on the set*

$L_1/L_2$ , again denoted by the symbol  $*$ .  $(L_1/L_2, *)$  is an abelian pro- $p$ -group with identity  $\bar{0}$ .

(2.6.2) The map

$$H_1/H_2 \rightarrow L_1/L_2, \quad \bar{x} \mapsto \overline{\Theta(x)}$$

is a well-defined bicontinuous group isomorphism onto  $(L_1/L_2, *)$ . In particular  $H_1/H_2$  is abelian.

*Proof.* In order to show the origin of the somewhat strange formula 2.6.0 we begin with the Claim:

$$\overline{\Theta(x \cdot y)} = \overline{\Theta(x) * \Theta(y)}$$

in  $L_1/L_2$  for all  $x, y \in H_1$ . Indeed, 1.3 says

$$2 \cdot \Theta(xy) = [\Theta(x), \Theta(y)] + \text{tr}(x) \cdot \Theta(y) + \text{tr}(y) \cdot \Theta(x),$$

and the first term on the right hand side lies in  $L_2$ . The explicit form of the inverse map constructed in the proof of 2.4.3 shows that

$$\text{tr}(x) = 2 \cdot \sqrt{1 + \text{tr}(\Theta(x)^2)/2},$$

and the same holds for  $y$ . Now the claim follows from the definition of  $*$ .

Next we prove that  $*$  induces a well-defined composition law on  $L_1/L_2$ . By symmetry it suffices to show that for all  $x, y \in L_1$  and  $u \in L_2$

$$((x + u) * y) - (x * y) \in L_2.$$

By definition this difference is equal to

$$\left(\sqrt{1 + \text{tr}((x + u)^2)/2} + \sqrt{1 + \text{tr}(x^2)/2}\right) \cdot y + \sqrt{1 + \text{tr}(y^2)/2} \cdot u.$$

Here the second term lies in  $(1 + C) \cdot L_2$ , whence in  $L_2$  by 2.3. It remains to show that the content of the big parentheses maps  $L_1$  to  $L_2$ . We may multiply this coefficient by the (invertible!) element

$$\sqrt{1 + \text{tr}((x + u)^2)R/2} + \sqrt{1 + \text{tr}(x^2)/2} \in 2 + C$$

which, as well as its inverse, maps  $L_2$  to itself by 2.3. Then the coefficient becomes

$$\text{tr}((x + u)^2) - \text{tr}(x^2) \stackrel{1.5}{=} \text{tr}(u \cdot (u + 2x)).$$

We must prove that this maps  $L_1$  to  $L_2$ . But 1.11 and 2.3 imply

$$\text{tr}(L_2 \cdot L_1) \cdot L_1 \subset L_4 \subset L_2,$$

which is clearly enough for our purpose.

Next we show that  $*$  makes  $L_1/L_2$  into an abelian group with identity  $\bar{0}$ . Using a little trick we can avoid a complicated calculation. Recall that by 2.4.3 the map  $H_1 \rightarrow L_1/L_2$  induced by  $\Theta$  is surjective. Since  $H_1$  is a group, this together with the above claim shows that  $(L_1/L_2, *)$  satisfies all group axioms! By 2.6.0 it is obviously abelian and the identity element is  $\bar{0}$ . Now the first assertion is proved except for the pro- $p$  part.

We already know that the map  $H_1 \rightarrow L_1/L_2$  induced by  $\Theta$  is a continuous surjective homomorphism. Clearly its kernel is  $H_2$ , so we obtain a well-defined group isomorphism from  $H_1/H_2$  to  $(L_1/L_2, *)$ . By the definition of the quotient topology this map is continuous. By 2.4.3 the inverse is also continuous, and the second assertion is proved. Finally 2.4.4 implies that  $H_1/H_2$  is pro- $p$ , hence so is  $(L_1/L_2, *)$ , and we are done.  $\square$

Now consider a closed subgroup  $\Gamma \subset H_1$  with the property

(2.7.0) The additive group  $L_1/L_2$  is topologically generated by the image of  $\Theta(\Gamma)$ .

The main result of this section is the determination of the descending central series of  $\Gamma$ , defined by  $\Gamma_1 := \Gamma$  and  $\Gamma_{n+1} = \overline{[\Gamma, \Gamma_n]}$  for every  $n \geq 1$ .

**THEOREM (2.7).** *For every  $n \geq 2$  we have  $\Gamma_n = H_n$ .*

*Proof.* The crucial point is the commutator relation 2.5.2. We begin by proving  $\Gamma_n \subset H_n$  by induction on all  $n \geq 1$ . For  $n = 1$  this was our assumption. If it holds for  $n - 1$ , the relation 2.5.2 implies  $[\Gamma_1, \Gamma_{n-1}] \subset [H_1, H_{n-1}] \subset H_n$ . But  $H_n$  is closed, hence  $\Gamma_n \subset H_n$ , finishing the induction step.

For the reverse inclusion we first observe that by 2.4.1 the closedness of  $\Gamma_n$  is equivalent to

$$\Gamma_n = \bigcap_{m \geq n} (\Gamma_n \cdot H_m).$$

Thus it suffices to prove

$$\Gamma_n \cdot H_m = \Gamma_n \cdot H_{m+1}$$

for all  $m \geq n \geq 2$ . By 2.5.1 this is equivalent to

$$L_m = \Theta(\Gamma_n \cap H_m) + L_{m+1}$$

for all  $m \geq n \geq 2$ . Since  $\Gamma_n$  contains  $\Gamma_{n+1}$  it suffices to prove this in the extremal

case  $n = m$ . In other words we have to show that

$$L_m = \Theta(\Gamma_m) + L_{m+1}$$

for all  $m \geq 2$ . By 2.5.1 the right hand side is in any case a closed additive subgroup of the left hand side. Thus we are done after we have proved the Claim: For all  $m \geq 1$  the additive group  $L_m/L_{m+1}$  is topologically generated by the image of  $\Theta(\Gamma_m)$ .

To facilitate notation let  $\Delta_m$  be the closed subgroup of  $L_m/L_{m+1}$  that is topologically generated by the image of  $\Theta(\Gamma_m)$ . The claim will be proved by induction on  $m$ . The case  $m = 1$  is just assumption 2.7.0. Assume that the claim has been proved for  $m - 1$ . The commutator relation 2.5.2 implies

$$\Theta([\Gamma_1, \Gamma_{m-1}]) \equiv [\Theta(\Gamma_1), \Theta(\Gamma_{m-1})] \pmod{L_{m+1}}. \tag{2.7.1}$$

By the bicontinuity of  $\Theta$  the closure of the left hand side is just  $\Theta(\Gamma_m)$ . Thus the group  $\Delta_m$  can be described in terms of the right hand side of 2.7.1. Now observe that by 2.3.3 the commutator induces a well-defined continuous bilinear pairing

$$(L_1/L_2) \times (L_{m-1}/L_m) \rightarrow L_m/L_{m+1}, (\bar{u}, \bar{v}) \mapsto \overline{[u, v]}.$$

Using the right hand side of 2.7.1,  $\Delta_m$  can be described as the closed subgroup of  $L_m/L_{m+1}$  that is topologically generated by the image of  $\Delta_1 \times \Delta_{m-1}$  under this pairing. On the other hand 2.7.0 and the inductive assumption say that  $\Delta_1 = L_1/L_2$  and  $\Delta_{m-1} = L_{m-1}/L_m$ . Moreover the definition of  $L_m$  implies that  $L_m/L_{m+1}$  is topologically generated by the image of the pairing. This shows that  $\Delta_m = L_m/L_{m+1}$ , as desired.  $\square$

**REMARK.** It is now easy to describe the derived series of  $\Gamma$  as well. Indeed, by 2.7 the commutator subgroup of  $\Gamma$  is  $H_2$ . By 2.3 the axioms 2.1.1–3 hold again when  $L$  is replaced by  $L_2$ . The “new”  $H_1$  will be the “old”  $H_2$ , and we can apply 2.7 again. By induction it follows that the derived series of  $\Gamma$  corresponds to the derived series of  $L$ , i.e. to the descending sequence of Lie subalgebras defined by  $L^{(1)} := L$  and  $L^{(n+1)} := [L^{(n)}, L^{(n)}]$ . The precise formulation is left to the reader.

### 3. Classification of all pro- $p$ subgroups

In the preceding section we started with certain Lie algebra data (see 2.1.1–3) and then studied pro- $p$  subgroups of  $SL_2(A)$  that are in a kind of special position with respect to this data (see 2.7.0). Now we go in the other direction: we extract the Lie algebra data from a given pro- $p$  subgroup of  $SL_2(A)$ . The main result is

that these processes are mutually inverse; in particular the results of section 2 apply to all pro- $p$  subgroups. This provides a classification and description of arbitrary pro- $p$  subgroups of  $SL_2(A)$  in a way that is probably as linearized as possible. As a by-product we obtain a description of the descending central series (as well as the derived series) purely in terms of Lie algebra data.

Let  $\Gamma \subset SL_2(A)$  be a pro- $p$  subgroup. By compactness it is necessarily closed. Let  $L \subset \mathfrak{sl}_{2,A}$  be the closed additive subgroup that is topologically generated by  $\Theta(\Gamma)$ . As in section 2 we put  $C := \text{tr}(L \cdot L) \subset A$ .

**PROPOSITION (3.1).** *This data satisfies the axioms 2.1.1–3.*

*Proof.* In order to prove the assertion 2.1.1 we first calculate modulo  $I$ . After conjugation by  $GL_2(A)$  we may assume that all matrices in  $\Gamma$  are of the form

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \text{ mod } I.$$

It follows that all matrices in  $L^2$  are congruent to  $0 \text{ mod } I$ . By induction it follows that all matrices in  $L^{2^n}$  are congruent to  $0 \text{ mod } I^n$ . Hence  $\bigcap_n L^n = \{0\}$ , as desired.

The assertion 2.1.2,  $[L, L] \subset L$ , follows from the formulas 1.1 and 1.2:

$$[\Theta(x), \Theta(y)] = \Theta(xy) - \Theta(yx).$$

For the axiom 2.1.3 first observe that 1.9 implies  $\text{tr}(\Gamma) \cdot L \subset L$ . By 1.4 we have

$$C = \text{tr}(L \cdot L) \subset \text{tr}(\Gamma) + \text{tr}(\Gamma)^2,$$

hence  $C \cdot L \subset L$ , as desired.

As in section 2 we now define  $L_1 := L$  and  $L_2 := [L, L]$ , and put

$$H_n := \{x \in SL_2(A) \mid \Theta(x) \in L_n, \text{tr}(x) - 2 \in C\}$$

for  $n = 1, 2$ .

**PROPOSITION (3.2).**  *$H_1$  is a subgroup of  $SL_2(A)$ ,  $H_2$  is a normal subgroup of  $H_1$ , and  $H_1/H_2$  is abelian.*

*Proof.* Conjunction of 3.1, 2.4, and 2.6. □

The first main result of this section is:

**THEOREM (3.3).**  *$\Gamma$  is contained in  $H_1$ , and the commutator subgroup of  $\Gamma$  is  $H_2$ .*

*Proof.* We begin with the inclusion  $\Gamma \subset H_1$ . By the definition of  $H_1$  we must show that  $\text{tr}(\gamma) - 2 \in C$  for every  $\gamma \in \Gamma$ . By formula 1.6 we have

$$\text{tr}(\gamma)^2 = 4 + 2 \cdot \text{tr}(\Theta(\gamma)^2) \equiv 4 \text{ mod } C.$$

We already know that the right hand side possesses a unique square root that is congruent to  $2 \pmod I$ , and this square root is given by the binomial series. In particular it is congruent to  $2 \pmod C$ . On the other hand  $\gamma$  is – after conjugation by  $GL_2(A)$  – congruent to a matrix of the form

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod I.$$

Thus  $\text{tr}(\gamma)$  is congruent to  $2 \pmod I$ . By the above considerations it is a fortiori congruent to  $2 \pmod C$ , as desired.

Since  $\Gamma$  is compact, we now know that it is a closed subgroup of  $H_1$ . In order to be able to apply theorem 2.7 it remains to show that the hypothesis 2.7.0 holds, i.e. that the additive group  $L/[L, L]$  is topologically generated by the image of  $\Theta(\Gamma)$ . But this is clear from the definition of  $L$ . □

Since the groups  $H_1, H_2$  depend only on  $L$ , theorem 3.3 implies that  $\Gamma$  is determined completely by  $L$  and the subgroup  $\Gamma/H_2 \subset H_1/H_2$ . This allows the following classification:

**THEOREM (3.4).** *There is a canonical one-to-one correspondence between all pro- $p$  subgroups  $\Gamma \subset SL_2(A)$  and the following pairs  $(L, \Delta)$ : First,  $L$  should be a closed additive subgroup of  $sl_{2,A}$  satisfying*

$$\bigcap_n L^n = \{0\}, \tag{3.4.1}$$

$$[L, L] \subset L, \text{ and} \tag{3.4.2}$$

$$\text{tr}(L \cdot L) \cdot L \subset L. \tag{3.4.3}$$

*These three conditions imply that the formula*

$$\bar{x} * \bar{y} := \sqrt{1 + \text{tr}(x^2)/2 \cdot y} + \sqrt{1 + \text{tr}(y^2)/2 \cdot x}$$

*is a well-defined composition law on the set  $L/[L, L]$ , making it into an abelian pro- $p$  group with identity  $\bar{0}$  (see 2.6.1). Then  $\Delta$  should be a closed subgroup of  $(L/[L, L], *)$  such that*

**(3.4.4)** *The additive group  $L/[L, L]$  is topologically generated by the subset  $\Delta$ .*

*Proof.* It is now clear how the correspondence is defined. When  $\Gamma$  is given, then  $L$  is defined as at the beginning of this section, and 3.4.1–3 follow from proposition 3.1. Also,  $\Delta$  is the closed subgroup of  $(L/[L, L], *)$  which corresponds to  $\Gamma/H_2 \subset H_1/H_2$  under the isomorphism 2.6.2, and 3.4.4 holds by the definition of  $L$ .

Conversely, when  $L$  and  $\Delta$  are given, then  $\Gamma$  is defined as the unique closed subgroup of  $H_1$  containing  $H_2$  and such that  $\Gamma/H_2 \subset H_1/H_2$  corresponds to  $\Delta$  under the isomorphism 2.6.2. By 2.4.4  $H_1$  is a pro- $p$  group, hence so is  $\Gamma$ .

To show that these rules are mutually inverse let us begin with a pro- $p$

