www.theoryofgroups.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 2 No. 1 (2013), pp. 145-155.

www.ui.ac.ir

OMISSIBLE EXTENSIONS OF $SL_2(k)$ WHERE k IS A FIELD OF POSITIVE CHARACTERISTIC

M. R. DIXON, M. J. EVANS* AND H. SMITH

Communicated by Patrizia Longobardi

Abstract. A normal subgroup N of a group G is said to be an *omissible* subgroup of G if it has the following property: whenever $X \leq G$ is such that $G = XN$, then $G = X$. In this note we construct various groups G, each of which has an omissible subgroup $N \neq 1$ such that $G/N \cong SL_2(k)$ where k is a field of positive characteristic.

1. Introduction

In [4] we investigated groups in which every proper subgroup is soluble-by-finite rank and we proved the following theorem.

Theorem 1.1. *Let G be a locally (soluble-by-finite) group with all proper subgroups soluble-by-finite rank. Then either*

(i) *G is locally soluble, or*
(ii) *G is soluble-by-finite rank and almost locally soluble, or*
(iii) *G is soluble-by-$PSL_2(k)$, or*
(iv) *G is soluble-by-$Sz(k)$,*

where k is an infinite locally finite field with no infinite proper subfields.

In part (iv) above, $Sz(k)$ denotes the Suzuki group defined over k and so k must have characteristic 2. In contrast there are no restrictions on the characteristic of the field k in part (iii). (The notation and terminology employed in this introduction are discussed in detail below.)

In this note we construct non-obvious groups G of type (iii).

MSC(2010): Primary: 20H25; Secondary: 20F50.

Keywords: Omissible subgroup, special linear group, Frattini extension, locally (soluble-by-finite) group.

Received: 19 December 2012, Accepted: 14 March 2013.

*Corresponding author.

Theorem 1.2. *Let k be an infinite locally finite field of characteristic p with no infinite proper subfields and let $l \geq 1$ be an integer. Then there exists a countable locally finite group G with all proper subgroups soluble-by-finite rank such that:*

(i) *G has a normal subgroup H of finite exponent that is soluble of derived length l, and*
(ii) *$G/H \cong PSL_2(k)$.*

We will deduce Theorem 1.2 from the following theorem which is our main technical result and is of independent interest.

Theorem 1.3. *Let p be a prime and let (R, pR, k) be a discrete valuation ring of characteristic 0 such that $|k| \geq 5$. Suppose that k is perfect if $p = 2$. Let $X \leq SL_2(R)$ be such that $SL_2(R) = \langle X, SL_2(R, pR)\rangle$. Then $SL_2(R) = \langle X, SL_2(R, p^n R)\rangle$ for each integer $n \geq 1$.*

On our way to deducing Theorem 1.2 from Theorem 1.3 we prove the following.

Theorem 1.4. *Let k be a field of characteristic $p > 0$ such that $|k| \geq 5$ and suppose that k is perfect if $p = 2$. Let $l \geq 1$ be an integer. There exists a group G with a nilpotent normal p-subgroup N of finite exponent and derived length l such that*

(i) *$G/N \cong SL_2(k)$, and*
(ii) *N is an omissible subgroup of G.*

Moreover, if k is infinite then $|G| = |k|$.

Here and throughout we say that a normal subgroup N of a group G is an *omissible* subgroup of G, (or that N is omissible if G is clear from the context), if it has the following property: whenever $X \leq G$ is such that $G = XN$, then $G = X$. If N is an omissible subgroup of G we say that G is an omissible extension of N.

The literature concerning SL_2 over a commutative ring R is vast and difficult to navigate; to the best of our knowledge there is no comprehensive survey of this material and we cannot give one here. However, we wish to draw the reader's attention to two works. J.-P. Serre [8, IV-23] considered the groups $SL_2(\hat{\mathbb{Z}}_p)$, where $\hat{\mathbb{Z}}_p$ denotes the ring of p-adic integers and $p \geq 5$. He proved what is essentially our Theorem 1.3 for $R = \hat{\mathbb{Z}}_p$, although his result is couched in the terminology of topological groups. Indeed, for $p \geq 5$ our proof of Theorem 1.3 can be substantially simplified by imitating his work. S. D. Kozlov [5] considered omissible extensions of $SL_n(K)$ for finite fields K and all integers $n \geq 2$.

2. Omissible subgroups

In this section we record some elementary facts about omissible subgroups.

It is well known that if G is a *finitely generated* group and $\Phi(G)$ denotes the Frattini subgroup of G then $\Phi(G)$ is an omissible subgroup of G. However, even if G is countable, it need not be the case that $\Phi(G)$ is an omissible subgroup of G, (consider a countable group G that has no maximal subgroups). Nevertheless, omissible subgroups of a group G share many properties with the Frattini subgroups of finitely generated groups:

Lemma 2.1. (i) *Let N be a normal subgroup of a group G and suppose that $N \leq X$ where X is an omissible subgroup of G. Then N is an omissible subgroup of G and X/N is an omissible subgroup of G/N.*

(ii) *Let N_1 and N_2 be normal subgroups of a group G such that $N_1 \leq N_2$. Suppose that N_1 is an omissible subgroup of G and N_2/N_1 is an omissible subgroup of G/N_1. Then N_2 is an omissible subgroup of G.*

(iii) *Let G be a group and let G' and $Z(G)$ denote the derived subgroup of G and the centre of G respectively. Then $G' \cap Z(G)$ is an omissible subgroup of G.*

(iv) *Let G be a nilpotent group. Then G' is an omissible subgroup of G.*

Proof. Part (i) is obvious. For part (ii), let $X \leq G$ be such that $G = \langle X, N_2 \rangle$. Then $G/N_1 = \langle X, N_2 \rangle / N_1 = \langle XN_1/N_1, N_2/N_1 \rangle$ and, since N_2/N_1 is omissible in G/N_1, we deduce that $XN_1 = G$ which implies that $X = G$ since N_1 is omissible in G. This proves (ii).

To prove (iii), suppose that $X \leq G$ is such that $\langle X, G' \cap Z(G) \rangle = G$ and that $g_1, g_2 \in G$. Now there exist $z_1, z_2 \in G' \cap Z(G)$ such that $g_1 z_1, g_2 z_2 \in X$. Therefore $[g_1, g_2] = [g_1 z_1, g_2 z_2] \in X$ and it follows that $G' \leq X$. The result follows at once.

Finally, we suppose that G is nilpotent of class $c \geq 1$ and show that G' is an omissible subgroup of G. If $c = 1$ there is nothing to prove. If $c = 2$, then $G' = G' \cap Z(G)$, and the result follows from (iii). We now argue by induction on c supposing G has class $r + 1 \geq 3$ and the desired result holds when $c \leq r$. Now $\gamma_{r+1}(G)$ is the last non-trivial term of the lower central series of G so $\gamma_{r+1}(G) \leq Z(G)$ and it follows from (ii) that $\gamma_{r+1}(G)$ is an omissible subgroup of G. Moreover, since $G/\gamma_{r+1}(G)$ has class $r \geq 2$, our inductive hypothesis implies that $(G/\gamma_{r+1}(G))' = G'/\gamma_{r+1}(G)$ is an omissible subgroup of $G/\gamma_{r+1}(G)$. The result now follows from (ii). □

3. Fields of prime characteristic and Discrete valuation rings (DVRs)

We write $\mathbb{F}_{p^n}$ or $GF(p^n)$ for the field that contains exactly p^n elements. By a *locally finite* field we mean a field k such that every finite set of elements of k generates a finite subfield of k. Clearly locally finite fields have prime characteristic. Moreover, each locally finite field k of characteristic p is *countable* since it is a subfield of the algebraic closure of $\mathbb{F}_p$, which is itself countable. Infinite locally finite fields k of characteristic p that have no proper infinite subfields exist for all primes p. Each can be viewed as a union of finite fields in the following way:

$$k = \bigcup_{n=1}^{\infty} GF(p^{q^n})$$

where q is a prime, (see, for instance, [1, Cor. 2.6]).

Let k be a field of characteristic $p > 0$. If p is odd then for each $x \in k$ we have that

$$x = 1 + (x/2)^2 - (1 - x/2)^2 = 1 + (x/2)^2 + \sum_{i=1}^{p-1} (1 - x/2)^2$$

and so x is a sum of squares in k. On the other hand, if $p = 2$ then an element $x \in k$ is a sum of squares in k if and only if x is itself a square in k. Consequently, in case $p = 2$, each element of k is a sum of squares in k if and only if k is perfect. (Recall that a field k of characteristic $p > 0$ is said to be *perfect* if the Frobenius endomorphism $k \to k$ given by $x \to x^p$ for all $x \in k$ is onto.) It is easy to see that locally finite fields are perfect.

A commutative ring A is said to be a *local* ring if it has a unique maximal ideal $\mathfrak{m}$. If this is the case, we call the field $A/\mathfrak{m} = k$ the *residue* field of A and record all of this information by saying that $(A, \mathfrak{m}, k)$ is a local ring. A *discrete valuation ring* (DVR) is a principal ideal domain that has a unique non-zero prime ideal. Clearly DVRs are local rings. (We refer the reader to [6] and [9, Chapter 1] for information about DVRs.)

Let R be a DVR. Then, up to multiplication by invertible elements, R has only one irreducible element, π say, and it follows easily that the non-zero ideals of R are of the form $\pi^n R$. Hence R is Noetherian, and using this fact it is not difficult to show that $\cap_{i=1}^{\infty} \pi^i R = 0$, (see, for instance, [9, p. 7]). Note that the element π is not nilpotent since R is a domain.

The following beautiful result is well known.

Theorem 3.1. [6, Theorem 29.1] *Let $(A, \pi A, K)$ be a DVR and let k be an extension field of K. Then there exists a DVR $(B, \pi B, k)$ containing A.*

Let p be a prime and let $\mathbb{Z}_{p\mathbb{Z}} = \{ \frac{a}{b} \in \mathbb{Q} | \, p \not| b \}$, the ring obtained by localizing $\mathbb{Z}$ at its prime ideal $p\mathbb{Z}$. It is easy to see that $\mathbb{Z}_{p\mathbb{Z}}$ is a DVR of characteristic 0 that has $p\mathbb{Z}_{p\mathbb{Z}}$ as its unique maximal ideal. (Thus, in the terminology of [6], $\mathbb{Z}_{p\mathbb{Z}}$ is a p-ring.) Note that $\mathbb{Z}_{p\mathbb{Z}}/p\mathbb{Z}_{p\mathbb{Z}} \cong \mathbb{F}_p$.

Let k be a field of characteristic p. On viewing k as an extension field of $\mathbb{F}_p$ and setting $K = \mathbb{F}_p$, $\pi = p$ and $A = \mathbb{Z}_{p\mathbb{Z}}$ in Theorem 3.1 we deduce the following corollary.

Corollary 3.2. *Let k be a field of characteristic $p > 0$. Then there exists a DVR (R, pR, k) of characteristic 0.*

4. SL_2 over DVRs

Let J be a proper ideal of a commutative ring R and let $\eta : R \to R/J$ be the natural map. Evidently η induces a group homomorphism $\eta^* : SL_2(R) \to SL_2(R/J)$. We write $SL_2(R, J)$ for the kernel of this map and note that $SL_2(R, J)$ consists of all 2×2 matrices of determinant 1 that are of the form $I_2 + B$ where the entries of the 2×2 matrix B lie in J.

Lemma 4.1. *Let $(R, \mathfrak{m}, K)$ be a local ring and let J be a proper ideal of R. Then*

(i) *the natural map $\eta^* : SL_2(R) \to SL_2(R/J)$ is onto and so $SL_2(R)/SL_2(R, J) \cong SL_2(R/J)$,*

(ii) $SL_2(R) = \left\langle \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} | \, b \in R \right\rangle$, *and*

(iii) *$SL_2(R)$ is a perfect group if $|K| \geq 4$.*

Proof. Let $A = \left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right)$ be an arbitrary element of $SL_2(R/J)$ and let b_i be a preimage of a_i under the natural map $\eta : R \to R/J$. Let $B = \left(\begin{smallmatrix} b_1 & b_2 \\ b_3 & b_4 \end{smallmatrix}\right)$ and note that $det(B) = \delta$ is congruent to 1 modulo J.

Since $J \subseteq \mathfrak{m}$ it follows that δ is a unit of R and it is easy to see that $\left(\begin{smallmatrix} b_1\delta^{-1} & b_2\delta^{-1} \\ b_3 & b_4 \end{smallmatrix}\right)$ is an element of $SL_2(R)$ that maps to A under η^*. Part (i) now follows easily.

Part (ii) can be proved by the usual 'row reduction' argument that establishes the result in the special case that R is a field, (see, for instance, [7, 3.2.10]).

Suppose now that $|K| \geq 4$ so that there exists $0 \neq \bar{a} \in K$ such that $\bar{a}^2 - 1 \neq 0$. Let $a \in R$ be a preimage of $\bar{a}$ under the natural map $R \to R/\mathfrak{m} = K$ and note that a and $1 - a^2$ are invertible elements of R. Part (iii) now follows from (ii) on observing that for each $b \in R$ we have that $\left[\left(\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & b(1-a^2)^{-1} \\ 0 & 1 \end{smallmatrix}\right)\right] = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ and $\left[\left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ b(1-a^2)^{-1} & 1 \end{smallmatrix}\right)\right] = \left(\begin{smallmatrix} 1 & 0 \\ b & 1 \end{smallmatrix}\right)$.

□

Let $(R, \pi R, K)$ be a DVR of characteristic 0 and let $B = \left(\begin{smallmatrix} 1+\pi a & \pi b \\ \pi c & 1+\pi d \end{smallmatrix}\right)$ be an element of $SL_2(R, \pi R)$. Since $det(B) = 1$ we have that $1 + \pi a + \pi d \equiv 1$ modulo $\pi^2 R$ and it follows easily that $a + d \equiv 0$ modulo πR. This observation will be used throughout the sequel.

Let p be a prime. In the proof of the following lemma we will need to know a little about the divisors of the binomial coefficients $\binom{p^m}{i}$ where $1 \leq i \leq p^m$. To be more precise we first recall that the p-adic valuation $\nu_p : \mathbb{Q} \setminus \{0\} \to \mathbb{Z}$ is defined in the following way: for each $x \in \mathbb{Q} \setminus \{0\}$, let $\nu_p(x)$ be the unique integer such that $x = p^{\nu_p(x)}(a/b)$ where $a, b \in \mathbb{Z} \setminus \{0\}$ and a, b are not divisible by p. The (well-known) fact that we require is that $\nu_p(\binom{p^m}{i}) = m - \nu_p(i)$ for $1 \leq i \leq p^m$. This is quite easy to prove by induction on i after noticing that $\binom{p^m}{i+1} = \binom{p^m}{i}((p^m - i)/(i + 1))$ so that $\nu_p(\binom{p^m}{i+1}) = \nu_p(\binom{p^m}{i}) + \nu_p(((p - i)/(i + 1)))$ for $1 \leq i \leq p^m - 1$. As a consequence of this fact we have that p^{m+1} divides $\binom{p^m}{i}p^i$ for $1 \leq i \leq p^m$.

Lemma 4.2. *Let p be a prime and let (R, pR, K) be a DVR of characteristic 0. Then*

(i) *$SL_2(R, pR)/SL_2(R, p^2R)$ is an elementary abelian p-group,*
(ii) *for each $n \geq 2$, $SL_2(R, pR)/SL_2(R, p^nR)$ is a nilpotent p-group of finite exponent,*
(iii) *$\cap_{n=1}^{\infty} SL_2(R, p^nR) = 1$, and*
(iv) *$SL_2(R, pR)$ is insoluble.*

Proof. Let $B = \left(\begin{smallmatrix} 1+pa & pb \\ pc & 1+pd \end{smallmatrix}\right) \in SL_2(R, pR)$ and let m be a positive integer. Since p^{m+1} divides $\binom{p^m}{i}p^i$ for $i = 1, \ldots, p^m$ the binomial theorem implies that $B^{p^m} = \left\{I_2 + p\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right\}^{p^m} \in SL_2(R, p^{m+1}R)$ and so $SL_2(R, pR)/SL_2(R, p^nR)$ has exponent dividing p^{n-1} for each $n \geq 2$. In particular, it follows that $SL_2(R, pR)/SL_2(R, p^2R)$ has exponent p.

Suppose that $A = \left(\begin{smallmatrix} 1+p^ma' & p^mb' \\ p^mc' & 1+p^md' \end{smallmatrix}\right) \in SL_2(R, p^mR)$. A routine calculation shows that $[A, B]$ is congruent modulo $SL_2(R, p^{m+1}R)$ to the scalar matrix

$$(1 + pa + p^ma' + pd + p^2ad + p^md' - p^2bc)I_2.$$

If $m = 1$ the argument in the paragraph immediately preceding this lemma shows that $a + d \equiv a' + d' \equiv 0$ modulo pR and we deduce that $[A, B] \equiv I_2$ modulo $SL_2(R, p^2R)$ and so $SL_2(R, pR)/SL_2(R, p^2R)$ is abelian and therefore elementary abelian, by the above, and (i) is proved.

If $m > 1$ we still have that

$$[SL_2(R, p^m R), SL_2(R, pR), SL_2(R, pR)] \leq SL_2(R, p^{m+1}R),$$

and it follows that the normal series

$$SL_2(R, pR) \geq SL_2(R, p^2R) \geq SL_2(R, p^3R) \geq \dots$$

can be refined to a descending central series of $SL_2(R, pR)$ by inserting at most one new term between each pair of successive terms. It follows that $SL_2(R, pR)/SL_2(R, p^n R)$ is a nilpotent p-group of finite exponent for each $n \geq 2$.

Recall from Section 3 that $\cap_{i=1}^{\infty} p^i R = 0$ and so $\cap_{i=1}^{\infty} SL_2(R, p^i R) = 1$.

Since R has characteristic 0, we may identify $\mathbb{Z}$ with the subring of R generated by 1. Consequently, we may view $SL_2(\mathbb{Z})$ as a subgroup of $SL_2(R)$ and $SL_2(\mathbb{Z}, p\mathbb{Z})$ as a subgroup of $SL_2(R, pR)$. It is well known that the subgroup of $SL_2(\mathbb{Z}, p\mathbb{Z})$ generated by $\left(\begin{smallmatrix} 1 & p \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ p & 0 \end{smallmatrix}\right)$ is a free group of rank 2, (see, for instance, [2, p. 26]), and it follows that $SL_2(R, pR)$ is insoluble.

□

Lemma 4.3. *Let p be a prime and let (R, pR, K) be a DVR where $|K| \geq 5$. Suppose that $X \leq SL_2(R)$ is such that $SL_2(R) = \langle X, SL_2(R, pR)\rangle$.*

(i) *If p is odd then X contains an element that is congruent modulo $SL_2(R, p^2R)$ to an element of the form $\left(\begin{smallmatrix} 1 & p\alpha \\ 0 & 1 \end{smallmatrix}\right)$ where $\alpha \notin pR$.*

(ii) *If $p = 2$ then X contains an element that is congruent modulo $SL_2(R, 4R)$ to an element of the form $\begin{pmatrix} \lambda & 2\beta \\ 0 & \lambda \end{pmatrix}$, where $\beta \notin 2R$.*

Proof. Let $\alpha \in R \setminus pR$. It follows from Lemma 4.1(i) that X contains an element of the form $M = \left(\begin{smallmatrix} 1+pa & \alpha+pb \\ pc & 1+pd \end{smallmatrix}\right)$ where $a, b, c, d \in R$.

We view M as a sum of matrices in the following way,

$$M = I_2 + \left\{ \begin{pmatrix} 0 & \alpha \\ 0 & 0 \end{pmatrix} + p \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right\},$$

and use the binomial theorem along with the fact that $\left(\begin{smallmatrix} 0 & \alpha \\ 0 & 0 \end{smallmatrix}\right)^2 = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ to verify that

$$M^p \equiv \begin{cases} \begin{pmatrix} 1 & p\alpha \\ 0 & 1 \end{pmatrix}, & \text{modulo } SL_2(R, p^2R), \text{ if } p > 3; \\ \begin{pmatrix} 1 & 3\alpha(1+c\alpha) \\ 0 & 1 \end{pmatrix}, & \text{modulo } SL_2(R, 9R), \text{ if } p = 3; \\ \begin{pmatrix} 1+2\alpha c & 2\alpha(1+d+a) \\ 0 & 1+2\alpha c \end{pmatrix}, & \text{modulo } SL_2(R, 4R), \text{ if } p = 2. \end{cases}$$

The result follows if $p > 3$.

Suppose that $p = 3$ and note that, in this case, the result follows from the above calculation unless $1 + c\alpha \in 3R$, i.e. unless $c \equiv -\alpha^{-1}$ modulo $3R$. Consequently we may assume that *every* matrix in X of the form $\left(\begin{smallmatrix} 1+3a & \alpha+3b \\ 3c & 1+3d \end{smallmatrix}\right)$ where $\alpha \notin 3R$ is congruent to $\left(\begin{smallmatrix} 1+3a & \alpha+3b \\ -3\alpha^{-1} & 1+3d \end{smallmatrix}\right)$ modulo $SL_2(R, 9R)$. Since $|K| \geq 5$ there exists $\beta \in R$ such that $\beta \not\equiv -1, 0, 1$ modulo $3R$. Now X contains matrices A and B that are congruent to $\left(\begin{smallmatrix} 1+3a & 1+3b \\ -3 & 1+3d \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1+3a' & \beta+3b' \\ -3\beta^{-1} & 1+3d' \end{smallmatrix}\right)$ modulo $SL_2(R, 9R)$, respectively. However, AB is congruent modulo $SL_2(R, 9R)$ to a matrix of the form $\left(\begin{smallmatrix} 1+3a'' & 1+\beta+3b'' \\ -3(1+\beta^{-1}) & 1+3d'' \end{smallmatrix}\right)$. It follows that $1 + \beta^{-1} \equiv (1 + \beta)^{-1}$ modulo $3R$, which implies, (after multiplying by $1 + \beta$), that $1 + \beta + \beta^2 \equiv 0$ modulo $3R$. Hence $(\beta - 1)^2 \equiv 0$ modulo $3R$ and we deduce that $\beta \equiv 1$ modulo $3R$, a contradiction.

Finally, suppose that $p = 2$. Again the desired result follows from the above calculation of M^2 unless $1 + a + d \in 2R$, i.e. unless $a + d \equiv 1$ modulo $2R$. Moreover, since $M \in X \leq SL_2(R)$ the determinant of M is 1 and so $1 + 2a + 2d - 2c\alpha \equiv 1$ modulo $4R$ and it follows that $a + d + c\alpha \in 2R$ and so $c \equiv (a+d)\alpha^{-1}$ modulo $2R$. Consequently, the result follows from the above calculation unless $c \equiv \alpha^{-1}$ modulo $2R$. Thus we may assume that *every* matrix in X of the form $\left(\begin{smallmatrix} 1+2a & \alpha+2b \\ 2c & 1+2d \end{smallmatrix}\right)$ where $\alpha \notin 2R$ is congruent to $\left(\begin{smallmatrix} 1+2a & \alpha+2b \\ 2\alpha^{-1} & 1+2d \end{smallmatrix}\right)$ modulo $SL_2(R, 4R)$. It is now easy to derive a contradiction using an argument similar to that used for the case $p = 3$ after noticing that there exists $\beta \in R$ such that $\beta \not\equiv 0, 1$ modulo $2R$ and $\beta^2 + \beta + 1 \not\equiv 0$ modulo $2R$. □

5. **Some simple modules**

Let (R, pR, K) be a DVR of characteristic 0. Recall from Lemma 4.2 that $N = SL_2(R, pR)/SL_2(R, p^2R)$ is an elementary abelian p-group. Since N is clearly a normal subgroup of $SL_2(R)/SL_2(R, p^2R)$ it follows that N can be viewed as an $\mathbb{F}_p(SL_2(K))$-module in a natural way: The action of $SL_2(K)$ on N is given by $(A.SL_2(R, p^2R))^M = A^{M^*}SL_2(R, p^2R)$ for all (cosets) $A.SL_2(R, p^2R) \in N$ and all $M \in SL_2(K)$ where M^* denotes a preimage of M under the natural map $SL_2(R) \to SL(K)$. (This latter map is onto by Lemma 4.1.) In this section we investigate the module-theoretic structure of N. The unpleasant notation we have just used can, to an extent, be avoided by introducing the Lie algebra $\mathfrak{sl}_2(K)$, (although we will only need to consider its additive structure). Accordingly, we proceed to introduce $\mathfrak{sl}_2(K)$.

Let $\mathfrak{sl}_2(K)$ denote the collection of 2×2 matrices with entries in K that have trace zero. Thus $\mathfrak{sl}_2(K) = \{\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & -\alpha \end{smallmatrix}\right) | \alpha, \beta, \gamma \in K\}$. We view $\mathfrak{sl}_2(K)$ as an abelian group under matrix addition and note that $\mathfrak{sl}_2(K)$ is closed under conjugation by elements of $SL_2(K)$ since $tr(A^{-1}BA) = tr(B)$ for all $A \in SL_2(K)$ and $B \in \mathfrak{sl}_2(K)$. Thus the elementary abelian p-group $\mathfrak{sl}_2(K)$ can be viewed as an $\mathbb{F}_p(SL_2(K))$-module.

As we have seen, if $\left(\begin{smallmatrix} 1+pa & pb \\ pc & 1+pd \end{smallmatrix}\right) \in SL_2(R, pR)$ then $a + d \equiv 0$ modulo pR. With this information in hand the proof of the next lemma is straightforward. (For each $x \in R$ we let $\bar{x}$ denote the image of x in K under the natural map $R \to K$.)

Lemma 5.1. *Let (R, pR, K) be a DVR of characteristic 0. Then the function $\theta : SL_2(R, pR)/SL_2(R, p^2R) \to \mathfrak{sl}_2(K)$ given by*

$$\theta : \begin{pmatrix} 1+pa & pb \\ pc & 1+pd \end{pmatrix}.SL_2(R, p^2R) \to \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}$$

is an isomorphism of $\mathbb{F}_p(SL_2(K))$-modules.

Note that if $p = 2$, then $\mathfrak{Z}(K) = \{\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha \end{smallmatrix}\right) | \alpha \in K\}$ is a subset of $\mathfrak{sl}_2(K)$. Clearly $\mathfrak{Z}(K)$ is an $\mathbb{F}_2(SL_2(K))$-submodule of $\mathfrak{sl}_2(K)$ on which $SL_2(K)$ acts trivially.

Lemma 5.2. *Let k be a field of characteristic $p > 0$ such that $|k| \geq 4$ and suppose that k is perfect if $p = 2$.*

(i) *If $p \neq 2$ the $\mathbb{F}_p(SL_2(k))$-module $\mathfrak{sl}_2(k)$ is simple.*

(ii) *If $p = 2$ the $\mathbb{F}_2(SL_2(k))$-module $\mathfrak{sl}_2(k)$ is generated by any element of $\mathfrak{sl}_2(k)$ that is not contained in $\mathfrak{Z}(k) = \{\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha \end{smallmatrix}\right) | \alpha \in k\}$.*

Proof. Recall from Section 3 that each element of k is a sum of squares in k. Throughout this proof we let $D(y) = \left(\begin{smallmatrix} y^{-1} & 0 \\ 0 & y \end{smallmatrix}\right)$ whenever $0 \neq y \in k$. Evidently each such $D(y)$ is an element of $SL_2(k)$.

Let $B = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & -\alpha \end{smallmatrix}\right)$ be a non-zero element of $\mathfrak{sl}_2(k)$ and suppose that $B \notin \mathfrak{Z}(k)$ if $p = 2$. Let M denote the $\mathbb{F}_p(SL_2(k))$-submodule of $\mathfrak{sl}_2(k)$ generated by B. Our goal is to show that $M = \mathfrak{sl}_2(k)$.

Our first step is to prove that M contains an element of the form $\left(\begin{smallmatrix} 0 & x \\ 0 & 0 \end{smallmatrix}\right)$ where $x \neq 0$. If $\alpha = \gamma = 0$ there is nothing to prove, so suppose that α and γ are not both zero. Let $U = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, an element of $SL_2(k)$. Now M contains $C := B^U - B = \left(\begin{smallmatrix} -\gamma & 2\alpha - \gamma \\ 0 & \gamma \end{smallmatrix}\right)$ and $C^U - C = \left(\begin{smallmatrix} 0 & -2\gamma \\ 0 & 0 \end{smallmatrix}\right)$ and we are done if $p \neq 2$. On the other hand, if $p = 2$ then $C = \left(\begin{smallmatrix} \gamma & \gamma \\ 0 & \gamma \end{smallmatrix}\right)$ and it follows that M contains a matrix $V = \left(\begin{smallmatrix} \alpha & \beta \\ 0 & \alpha \end{smallmatrix}\right)$ in which $\beta \neq 0$. Since $|k| \geq 4$ there exists $0 \neq \zeta \in k$ such that $\zeta^2 \neq 1$. Now $V^{D(\zeta^{-1})} - V = \left(\begin{smallmatrix} 0 & (\zeta^{-2}-1)\beta \\ 0 & 0 \end{smallmatrix}\right)$ and the claim is proved.

We next show that M contains $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$. As we have seen, M contains a matrix of the form $\left(\begin{smallmatrix} 0 & x \\ 0 & 0 \end{smallmatrix}\right)$ where $x \neq 0$. Let us write x^{-1} as the sum of squares $x^{-1} = \sum_{i=1}^{l} y_i^2$ where each y_i is a non-zero element of k. It is easy to verify that

$$\sum_{i=1}^{l} \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}^{D(y_i)} = \sum_{i=1}^{l} \begin{pmatrix} 0 & xy_i^2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

as required.

To complete the proof of the lemma it now suffices to show that $\mathfrak{sl}_2(k)$ is generated by $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ as an $\mathbb{F}_p(SL_2(k))$-module. To this end, let L denote the submodule of $\mathfrak{sl}_2(k)$ generated by $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$. Our claim is that $L = \mathfrak{sl}_2(k)$. Since an arbitrary element of $\mathfrak{sl}_2(k)$ is of the form $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & -\alpha \end{smallmatrix}\right) = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & -\alpha \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 & \beta \\ 0 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 & 0 \\ \gamma & 0 \end{smallmatrix}\right)$ it is enough to show that L contains $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & -\alpha \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & \alpha \\ 0 & 0 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 0 & 0 \\ \alpha & 0 \end{smallmatrix}\right)$ for all $\alpha \in k$. Clearly we may assume that $\alpha \neq 0$.

Let $W = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $Y = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. Now $\left(\begin{smallmatrix} 0 & \alpha \\ 0 & 0 \end{smallmatrix}\right)^W = -\left(\begin{smallmatrix} 0 & 0 \\ \alpha & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & \alpha \\ 0 & 0 \end{smallmatrix}\right)^Y = \left(\begin{smallmatrix} \alpha & \alpha \\ -\alpha & -\alpha \end{smallmatrix}\right) = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & -\alpha \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 & \alpha \\ 0 & 0 \end{smallmatrix}\right) - \left(\begin{smallmatrix} 0 & 0 \\ \alpha & 0 \end{smallmatrix}\right)$ and so the lemma will be proved once we show that $\left(\begin{smallmatrix} 0 & \alpha \\ 0 & 0 \end{smallmatrix}\right) \in L$ for all $0 \neq \alpha \in k$. Accordingly, let $0 \neq \alpha \in k$ and write $\alpha = \sum_{i=1}^{l} y_i^2$ where each y_i is a non-zero element of k. Now $\sum_{i=1}^{l} \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)^{D(y_i)} = \left(\begin{smallmatrix} 0 & \alpha \\ 0 & 0 \end{smallmatrix}\right)$, and the proof is complete. □

Lemma 5.3. *Let p be a prime and let (R, pR, k) be a DVR of characteristic 0 where $|k| \geq 5$ and suppose that k is perfect if $p = 2$. Let $X \leq SL_2(R)$ be such that $SL_2(R) = \langle X, SL_2(R, pR)\rangle$. Then $SL_2(R) = \langle X, SL_2(R, p^2R)\rangle$.*

Proof. Let X be as stated and recall from Lemma 4.3 that X contains a matrix, C say, that is contained in $SL_2(R, pR)$ but is not congruent to a diagonal matrix modulo $SL_2(R, p^2R)$. Also recall, from Lemma 5.1, that $\theta : SL_2(R, pR)/SL_2(R, p^2R) \to \mathfrak{sl}_2(K)$ is an isomorphism of $\mathbb{F}_p(SL_2(K))$-modules. Evidently $\theta(C.SL_2(R, p^2R))$ is a non-diagonal element of $\mathfrak{sl}_2(K)$. It follows from Lemma 5.2 that $\theta(C)$ generates $\mathfrak{sl}_2(K)$ as an $\mathbb{F}_p(SL_2(K))$-module and so $C.SL_2(R, p^2R)$ generates $SL_2(R, pR)/SL_2(R, p^2R)$ as an $\mathbb{F}_p(SL_2(K))$-module. In other words, the normal closure of C in $SL_2(R)$ generates $SL_2(R, pR)$ modulo $SL_2(R, p^2R)$. Moreover, since $SL_2(R, pR)$ centralizes C modulo $SL_2(R, p^2R)$ and $\langle X, SL_2(R, pR)\rangle \equiv SL_2(R)$ modulo $SL_2(R, p^2R)$ it follows that the normal closure C^X is congruent to $SL_2(R, pR)$ modulo $SL_2(R, p^2R)$. The result follows at once. □

6. **The proofs of Theorems 1.2, 1.3 and 1.4**

The proof of Theorem 1.3. The proof is by induction on n. If $n = 1$ there is nothing to prove whereas if $n = 2$ the result is given by Lemma 5.3. Accordingly, suppose that $n \geq 3$ and that $SL_2(R) = \langle X, SL_2(R, p^{n-1}R)\rangle$. To complete the proof it suffices to show that for any $S \in SL_2(R, p^{n-1}R)$ there exists $Y \in X$ such that Y is congruent to S modulo $SL_2(R, p^nR)$. To this end write $S = I_2 + p^{n-1}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ where $a, b, c, d \in R$. Since $det(S) = 1$ it is easy to see that $a + d \equiv 0$ modulo pR.

Let $B_1 = \left(\begin{smallmatrix} a & a \\ -a & -a \end{smallmatrix}\right), B_2 = \left(\begin{smallmatrix} 0 & 0 \\ a+c & 0 \end{smallmatrix}\right)$ and $B_3 = \left(\begin{smallmatrix} 0 & b-a \\ 0 & 0 \end{smallmatrix}\right)$ and for $i = 1, 2, 3$ let $S_i = I_2 + p^{n-1}B_i$. Observe that $B_i^2 = 0$ and $S_i \in SL_2(R, p^{n-1}R)$ for $i = 1, 2, 3$. Furthermore, since $a + d \equiv 0$ modulo pR, it follows that $S_1S_2S_3$ is congruent to S modulo $SL_2(R, p^nR)$ and so it now suffices to show that there exists $Y_i \in X$, for $i = 1, 2, 3$, such that Y_i is congruent to S_i modulo $SL_2(R, p^nR)$.

Let $i = 1, 2$ or 3 and note that $U_i = I_2 + p^{n-2}B_i \in SL_2(R)$. By the induction hypothesis it follows that there exists $V_i \in X$ such that V_i is congruent to U_i modulo $SL_2(R, p^{n-1}R)$. We write $V_i = I_2 + p^{n-2}B_i + p^{n-1}C_i$ where, of course, C_i is a 2×2 matrix with entries in R.

Let $Y_i = V_i^p$. Clearly $Y_i \in X$. Now,

$$Y_i = I_2 + \sum_{j=1}^{p-1} \binom{p}{j} (p^{n-2}B_i + p^{n-1}C_i)^j + (p^{n-2}B_i + p^{n-1}C_i)^p =$$

$$I_2 + p^{n-1}B_i + p^nC_i + \sum_{j=2}^{p-1} \binom{p}{j} p^{j(n-2)}(B_i + pC_i)^j + p^{p(n-2)}(B_i + pC_i)^p$$

and since $n \geq 3$ we have that p^n divides $\binom{p}{j}p^{j(n-2)}$ for $j = 2, \ldots, p-1$. It follows that $Y_i \equiv S_i$ modulo $SL_2(R, p^n)$ if $p \geq 3$ or $p = 2$ and $n \geq 4$. On the other hand, if $p = 2$ and $n = 3$ we have that $Y_i = I_2 + 4B_i + 4(B_i + 2C_i)^2 \equiv I_2 + 4B_i$ modulo $SL_2(R, 8R)$ since $B_i^2 = 0$. Therefore, in all cases, Y_i is congruent to S_i modulo $SL_2(R, p^nR)$ and the proof is complete.

□

The proof of Theorem 1.4. Let (R, pR, k) be a DVR of characteristic 0; the existence of such a DVR is guaranteed by Corollary 3.2.

Now Lemma 4.2 shows that for each $m \geq 1$ the normal subgroup $SL_2(R, pR)/SL_2(R, p^m R)$ of $SL_2(R)/SL_2(R, p^m R)$ is a nilpotent p-subgroup that has finite exponent. Moreover, Lemma 4.2 also shows that $\cap_{m=1}^{\infty} SL_2(R, p^m R) = 1$ and $SL_2(R, pR)$ is insoluble. It follows that for each $l \geq 1$ there exists $n \geq 1$ such that $SL_2(R, pR)/SL_2(R, p^n R)$ has derived length l. We claim that $G = SL_2(R)/SL_2(R, p^n R)$ and $N = SL_2(R, pR)/SL_2(R, p^n R)$ have the desired properties. Lemma 4.1 (i) implies that $G/N \cong SL_2(k)$ and so, in light of the remarks above, it only remains to show that N is an omissible subgroup of G and that $|G| = |k|$ if k is infinite.

To this end let $Y \leq G$ be such that $\langle Y, N\rangle = G$ and recall that Lemma 4.1 shows that the natural map $\eta^*; SL_2(R) \to SL_2(R, p^n R)$ is onto. Let $X \leq SL_2(R)$ be a preimage of Y under η^*. Then $\langle X, SL_2(R, pR)\rangle = SL_2(R)$ and so $\langle X, SL_2(R, p^n R)\rangle = SL_2(R)$ by Theorem 1.3. It follows at once that $\langle Y\rangle = G$ and so N is an omissible subgroup of G.

Finally, suppose that k is infinite. It is easy to see that $|SL_2(k)| = |k|$ and so G/N can be generated by $|k|$ elements. Since N is an omissible subgroup of G this implies that G can be generated by $|k|$ elements and therefore $|G| = |k|$. The proof is now complete. □

The proof of Theorem 1.2 . Since k is perfect, Theorem 1.4 shows that there exists a countable group G with an omissible normal subgroup N such that N is a nilpotent p-group of finite exponent and derived length l and $G/N \cong SL_2(k)$. Let H be the normal subgroup of G such that $N \leq H$ and H/N is the centre of G/N. (Thus $H = N$ if $p = 2$, whereas $|H/N| = 2$ if p is odd.) Evidently H has finite exponent and is soluble of derived length at least l. Since G/N is a perfect group, (by Lemma 4.1 (iii) for instance), Lemma 2.1 (iii) shows that H/N is an omissible subgroup of G/N and it now follows from Lemma 2.1 (ii) that H is an omissible subgroup of G. On replacing G with $G/H^{(l)}$ and H with $H/H^{(l)}$ if necessary we now have that G has an omissible normal subgroup H such that H has finite exponent and derived length l. Moreover, $G/H \cong PSL_2(k)$.

Let L be a proper subgroup of G. To complete the proof it suffices to show that L is soluble-by-finite rank. Note that $HL \neq G$ since H is omissible and so we may assume that $H \leq L$. Now H is soluble and consequently it is enough to prove that L/H is soluble-by-finite rank. We recall from [3] that each proper subgroup of $PSL_2(k)$ is finite or soluble of derived length at most 2. The result follows immediately since L/H is isomorphic to a proper subgroup of $PSL_2(k)$. □

Acknowledgments

The second author would like to thank Bucknell University for its hospitality while some of this work was being done.

References

[1] J. V. Brawley and G. E. Schnibben, *Infinite Agebraic Extensions of Finite Fields*, Contemporary Mathematics, American Math. Soc., Providence, RI., **95** 1989.

[2] P. de la Harpe, *Topics in Geometric Group Theory*, Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 2000.

[3] M. R. Dixon and M. J. Evans, Groups with the minimum condition on insoluble subgroups, *Arch. Math. (Basel)*, **72** (1999) 241–251.

[4] M. R. Dixon, M. J. Evans and H. Smith, Groups with all proper subgroups soluble-by-finite rank, *J. Algebra*, **289** (2005) 135–147.

[5] S. D. Kozlov, Frattini extensions of the projective special linear group, *Sibirsk. Math. Zh.*, **32** no. 2 (1991) 88–93. English translation in: *Siberian Math. J.*, **32** no. 2 (1991) 252–256.

[6] H. Matsumura, *Commutative Ring Theory*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, **8** 1986.

[7] D. J. S. Robinson, *A course in the theory of groups*, Graduate Texts in Mathematics, Springer Verlag, Berlin, Heidelberg, New York, **80** 1996.

[8] J-P. Serre, Abelian ℓ-adic Representations and Elliptic Curves, *W. A. Benjamin, Inc.*, New York-Amsterdam, 1968.

[9] J-P. Serre, *Local Fields*, Graduate Texts in Mathematics, Springer-Verlag, New York, Berlin, **67** 1979.

Martyn R. Dixon
Department of Mathematics, The University of Alabama, Tuscaloosa, AL. 35487-0350, U.S.A.
Email: mdixon@as.ua.edu

Martin J. Evans
Department of Mathematics, The University of Alabama, Tuscaloosa, AL. 35487-0350, U.S.A.
Email: mevans@as.ua.edu

Howard Smith
Department of Mathematics, Bucknell University, Lewisburg, PA. 17837, U.S.A.
Email: howsmith@bucknell.edu