

LIE ALGEBRAS AND COHOMOLOGY OF CONGRUENCE SUBGROUPS FOR $SL_n(R)$

JONATHAN LOPEZ

ABSTRACT. Let R be a commutative ring that is free of rank k as an abelian group, p a prime, and $SL_n(R)$ the special linear group. We show that the Lie algebra associated to the filtration of $SL_n(R)$ by p -congruence subgroups is isomorphic to the tensor product $\mathfrak{sl}_n(R \otimes_{\mathbb{Z}} \mathbb{Z}/p) \otimes_{\mathbb{F}_p} t\mathbb{F}_p[t]$, the Lie algebra of polynomials with zero constant term and coefficients $n \times n$ traceless matrices with entries polynomials in k variables over \mathbb{F}_p .

We use the Lie algebra structure along with the Lyndon-Hochschild-Serre spectral sequence to compute the d^2 homology differential for certain central extensions involving quotients of p -congruence subgroups. We also use the underlying group structure to obtain several homological results. For example, we compute the first homology group of the level p -congruence subgroup for $n \geq 3$. We show that the cohomology groups of the level p^r -congruence subgroup are not finitely generated for $n = 2$ and $R = \mathbb{Z}[t]$. Finally, we show that for $n = 2$ and $R = \mathbb{Z}[i]$ (the Gaussian integers) the second cohomology group of the level p^r -congruence subgroup has dimension at least two as an \mathbb{F}_p -vector space.

1. INTRODUCTION

The method of constructing a Lie algebra from a filtered group is classical (see [17], for example), and congruence subgroups have been widely studied for many years by mathematicians such as Bass, Milnor, and Serre (in [1]), among others. Linear groups over commutative rings admit natural filtrations by p -congruence subgroups, i.e., subgroups consisting of matrices that reduce to the identity modulo powers of p . As a result, we are able to construct an associated Lie algebra, and the structure of this Lie algebra encodes homological information, as well as information concerning the structure of certain central extensions involving quotients of congruence subgroups. It should be noted that filtrations of this type, i.e., filtrations of linear groups by p -congruence subgroups, appear in linearity problems of groups (see [4] and [16]).

We start with a commutative ring R that is free of rank k as a \mathbb{Z} -module (unless otherwise stated, we allow k to be infinite). Let $G_n(R)$ denote an $n \times n$ matrix group with coefficients in R . In this paper, we assume $G_n(R) = SL_n(R)$ unless otherwise stated. Examples involving other linear groups appear in [15]. For a prime p , there is a filtration

$$(1.1) \quad \cdots \subseteq \Gamma(G_n(R), p^r) \subseteq \cdots \subseteq \Gamma(G_n(R), p^2) \subseteq \Gamma(G_n(R), p)$$

2010 *Mathematics Subject Classification.* 20J06, 17B45, 20H05.

Key words and phrases. Congruence Subgroup, Filtration, Lie Algebra, Group Cohomology.

for $r \geq 1$, where

$$(1.2) \quad \Gamma(G_n(R), p^r) = \ker(G_n(R) \longrightarrow G_n(R \otimes_{\mathbb{Z}} \mathbb{Z}/p^r)).$$

Classically, there is a Lie algebra

$$(1.3) \quad \mathrm{gr}_*(\Gamma(G_n(R), p)) = \bigoplus_{r \geq 1} \Gamma(G_n(R), p^r) / \Gamma(G_n(R), p^{r+1})$$

associated to filtration (1.1) in which the Lie bracket

$$(1.4) \quad [-, -] : \mathrm{gr}_*(\Gamma(G_n(R), p)) \otimes_{\mathbb{F}_p} \mathrm{gr}_*(\Gamma(G_n(R), p)) \longrightarrow \mathrm{gr}_*(\Gamma(G_n(R), p))$$

is induced by the restriction of the group commutator map in $G_n(R)$. Our main results include an explicit description of the Lie algebra structure of $\mathrm{gr}_*(\Gamma(G_n(R), p))$ for the case $G_n(R) = SL_n(R)$, as well as the following theorem.

Theorem 1 (2.4). *Let $\mathfrak{g} = \mathfrak{sl}_n(R \otimes_{\mathbb{Z}} \mathbb{Z}/p)$, and let \mathfrak{L} be the kernel of the evaluation map $\mathfrak{g} \otimes_{\mathbb{F}_p} \mathbb{F}_p[t] \xrightarrow{t=0} \mathfrak{g}$. Then*

$$(1.5) \quad \mathfrak{L} \cong \mathrm{gr}_*(\Gamma(G_n(R), p))$$

as Lie algebras.

We also explore the group structure of the filtration quotients for the filtration of $\Gamma(G_n(R), p)$ given in (1.1). The group structure is used to compute the structure of the Lie algebra $\mathrm{gr}_*(\Gamma(G_n(R), p))$, and it is also used in the proof of Theorem 1. Our main results concerning the filtration quotients are as follows, where $V = \{v_i\}_{i \in I}$ is a \mathbb{Z} -basis for R (recall that R is a free \mathbb{Z} -module of rank k).

Theorem 2 (3.2 and 3.7). *For $n \geq 2$ and $r \geq 1$,*

$$(1.6) \quad \Gamma(G_n(R), p^r) / \Gamma(G_n(R), p^{r+1}) \cong \bigoplus_{n^2-1} \mathbb{F}_p[V].$$

Moreover,

$$(1.7) \quad \Gamma(G_n(R), p^r) / \Gamma(G_n(R), p^{r+1}) \cong \mathfrak{sl}_n(\mathbb{F}_p[V])$$

as abelian groups.

The next corollary is a direct application of this theorem and a result of Bass-Milnor-Serre [1].

Corollary 3 (3.3). *For $n \geq 3$,*

$$(1.8) \quad H_1(\Gamma(G_n(R), p); \mathbb{Z}) \cong \mathfrak{sl}_n(\mathbb{F}_p[V]).$$

Finally, we use the structure of $\mathrm{gr}_*(\Gamma(G_n(R), p))$ to obtain some homological information concerning p -congruence subgroups for $SL_n(R)$. The Lie algebra structure can be used to explicitly compute the d^2 homology differential in the Lyndon-Hochschild-Serre spectral sequence for certain central extensions involving quotients of p -congruence subgroups. More specifically, suppose one has a central extension

$$(1.9) \quad 1 \longrightarrow \Gamma_{r+s-1} / \Gamma_{r+s} \longrightarrow \Gamma_r / \Gamma_{r+s} \longrightarrow \Gamma_r / \Gamma_{r+s-1} \longrightarrow 1,$$

where we have used the convention $\Gamma_r = \Gamma(G_n(R), p^r)$. Furthermore, suppose that defining a map

$$(1.10) \quad \theta : F[x, y] \longrightarrow \Gamma_r / \Gamma_{r+s}$$

induces a map of extensions as in Figure 1, where $F[x, y]$ is the free group on

$$\begin{array}{ccccccc}
1 & \longrightarrow & K & \longrightarrow & F[x, y] & \longrightarrow & \mathbb{Z} \oplus \mathbb{Z} & \longrightarrow & 1 \\
& & \downarrow \theta & & \downarrow \theta & & \downarrow \theta & & \\
1 & \longrightarrow & \Gamma_{r+s-1}/\Gamma_{r+s} & \longrightarrow & \Gamma_r/\Gamma_{r+s} & \longrightarrow & \Gamma_r/\Gamma_{r+s-1} & \longrightarrow & 1
\end{array}$$

FIGURE 1. Map of Extensions Induced by (1.10)

two generators. In many cases, the Lie algebra structure can be used to explicitly compute d^2 for extension (1.9), thus informing on $H_1(\Gamma_r/\Gamma_{r+s})$. The main result concerning this is presented in the next theorem.

Theorem 4 (7.2). *Let χ be the generator of $H_2(\mathbb{Z} \oplus \mathbb{Z}) \cong \mathbb{Z}$. Given the map of extensions θ described above,*

$$(1.11) \quad d^2(\theta_*(\chi)) = [\theta_*(x), \theta_*(y)].$$

We are also able to obtain some cohomological information by examining certain subgroups of $\Gamma(G_n(R), p^r)$. For the case $n = 2$ and $R = \mathbb{Z}[t]$, we are able to produce a subgroup $\bigoplus_{i \geq 0} \mathbb{Z} \subseteq \Gamma(G_2(R), p^r)$, from which we are able to prove the following result.

Theorem 5 (5.1). *Suppose $n = 2$ and $R = \mathbb{Z}[t]$. For all $j, r \geq 1$ and for all primes p ,*

$$(1.12) \quad H^j(\Gamma(G_2(\mathbb{Z}[t]), p^r); \mathbb{F}_p)$$

is infinitely generated.

For the case $n = 2$ and $R = \mathbb{Z}[i]$, we construct a map

$$(1.13) \quad (\mathbb{Z} \oplus \mathbb{Z}) * (\mathbb{Z} \oplus \mathbb{Z}) \longrightarrow \Gamma(G_2(R), p^r)$$

that can be used to show that $H^2(\Gamma(G_2(R), p^r); \mathbb{F}_p)$ has dimension at least 2 as an \mathbb{F}_p -vector space. In particular, this confirms that the level p^r -congruence subgroup for $SL_2(\mathbb{Z}[i])$ is not free for any $r \geq 1$.

Theorem 6 (6.1). *Suppose $n = 2$ and $R = \mathbb{Z}[i]$. For all $r \geq 1$ and for all primes p ,*

$$(1.14) \quad H^2(\Gamma(G_2(\mathbb{Z}[i]), p^r); \mathbb{F}_p) \supseteq \mathbb{F}_p \oplus \mathbb{F}_p.$$

Acknowledgments. The author would like to thank Fred Cohen for suggesting many of the problems discussed in this paper and for countless conversations concerning these topics over the past several years. The author would also like to thank Stratos Prassidis for helpful suggestions concerning the layout of this paper, as well as several insightful discussions concerning its content.

2. PRELIMINARIES, BASIC NOTATION

We now collect the notation that will be used throughout this paper: R is a commutative ring that is free of rank k as an abelian group; $V = \{v_i\}_{i \in I}$ is a \mathbb{Z} -basis for R ; $G_n(R)$ is an $n \times n$ matrix group with coefficients in R ; p is a prime; and $\Gamma(G_n(R), p^r)$ is the kernel of the mod- p^r reduction map

$$(2.1) \quad G_n(R) \longrightarrow G_n(R \otimes_{\mathbb{Z}} \mathbb{Z}/p^r).$$

The following is a classical result (see, for example, [7]):

Theorem 2.1. *There is a Lie algebra $\mathrm{gr}_*(\Gamma(G_n(R), p))$ associated to the filtration*

$$(2.2) \quad \cdots \subseteq \Gamma(G_n(R), p^r) \subseteq \cdots \subseteq \Gamma(G_n(R), p^2) \subseteq \Gamma(G_n(R), p)$$

in which the Lie bracket is induced by the restriction of the commutator map in $G_n(R)$,

$$(2.3) \quad [-, -] : \Gamma(G_n(R), p^r) \times \Gamma(G_n(R), p^s) \longrightarrow \Gamma(G_n(R), p^{r+s}).$$

As one of the main results of this paper will be describing the construction and structure of this Lie algebra for $SL_n(R)$, it may be worthwhile to first consider an elementary case ($n = 2$, $R = \mathbb{Z}$) in order to explicitly see the full calculation of the Lie algebra structure.

Theorem 2.2. *Suppose $n = 2$ and $R = \mathbb{Z}$, so that $G_n(R) = SL_2(\mathbb{Z})$. For $r \geq 1$, consider the following matrices:*

$$(2.4) \quad A_{12,r} = \begin{pmatrix} 1 & p^r \\ 0 & 1 \end{pmatrix} \quad A_{21,r} = \begin{pmatrix} 1 & 0 \\ p^r & 1 \end{pmatrix} \quad A_{11,r} = \begin{pmatrix} 1+p^r & 0 \\ 0 & 1-p^r \end{pmatrix}.$$

The Lie algebra $\mathrm{gr}_(\Gamma(SL_2(\mathbb{Z}), p))$ is generated (as a restricted Lie algebra over \mathbb{F}_p) by the three matrices $A_{12,1}$, $A_{21,1}$, and $A_{11,1}$. Furthermore, the following relations are satisfied for all $r, s \geq 1$ and for all primes p :*

- (1) $[A_{11,r}, A_{12,s}] = A_{12,r+s}^2$
- (2) $[A_{11,r}, A_{21,s}] = A_{21,r+s}^{-2}$
- (3) $[A_{12,r}, A_{21,s}] = A_{11,r+s}$
- (4) $A_{ij,r}^p = A_{ij,r+1}$ for $(i, j) \in \{(1, 2), (2, 1), (1, 1)\}$.

One feature of the Lie algebra $\mathrm{gr}_*(\Gamma(G_n(R), p))$ is the fact that it is finitely generated as a restricted Lie algebra whenever $k < \infty$. This is suggested by Theorem 2.2 for the case $n = 2$ and $k = 1$, and is, in fact, true for all $n \geq 2$ and $k < \infty$.

We now provide a description of the Lie algebra \mathfrak{L} introduced in Theorem 1. Recall that $\mathfrak{sl}_n(\mathbb{F}_p[V])$ is the Lie algebra of $n \times n$ traceless matrices over $\mathbb{F}_p[V]$, where the Lie bracket is defined by

$$(2.5) \quad [A, B] = AB - BA$$

for $A, B \in \mathfrak{sl}_n(\mathbb{F}_p[V])$. Let $\mathbb{F}_p[t]$ be the polynomial ring in one indeterminate over \mathbb{F}_p , and let I denote the kernel of the evaluation map

$$(2.6) \quad \mathbb{F}_p[t] \xrightarrow{t=0} \mathbb{F}_p.$$

Notice that I is the \mathbb{F}_p -linear span of $\{t^i \mid i > 0\}$.

Writing $\mathfrak{g} = \mathfrak{sl}_n(\mathbb{F}_p[V])$, consider the Lie algebra $\mathfrak{g} \otimes_{\mathbb{F}_p} \mathbb{F}_p[t]$, where the Lie bracket is defined by

$$(2.7) \quad [A \otimes t^i, B \otimes t^j] = [A, B] \otimes t^{i+j} = (AB - BA) \otimes t^{i+j}$$

for $A, B \in \mathfrak{g}$ and $i, j \geq 0$. The evaluation map (2.6) induces a morphism of Lie algebras

$$(2.8) \quad \mathfrak{g} \otimes_{\mathbb{F}_p} \mathbb{F}_p[t] \xrightarrow{t=0} \mathfrak{g}$$

whose kernel is exactly $\mathfrak{L} = \mathfrak{g} \otimes_{\mathbb{F}_p} I$. It is easy to verify that \mathfrak{L} is a Lie algebra with Lie bracket as defined in 2.7. These facts are collected in the next lemma.

Lemma 2.3. *The split short exact sequence of abelian groups*

$$(2.9) \quad 0 \longrightarrow I \longrightarrow \mathbb{F}_p[t] \xrightarrow{t=0} \mathbb{F}_p \longrightarrow 0$$

gives rise to a split short exact sequence of Lie algebras

$$(2.10) \quad 0 \longrightarrow \mathfrak{L} \longrightarrow \mathfrak{g} \otimes_{\mathbb{F}_p} \mathbb{F}_p[t] \xrightarrow{t=0} \mathfrak{g} \longrightarrow 0.$$

Proof. The splitting $\mathbb{F}_p \longrightarrow \mathbb{F}_p[t]$ in the first short exact sequence is given by the inclusion map $x \mapsto x$.

Since the tensor product is over the field \mathbb{F}_p , the fact that (2.10) is exact is immediate. The map $\mathfrak{g} \longrightarrow \mathfrak{g} \otimes_{\mathbb{F}_p} \mathbb{F}_p[t]$ defined by $x \mapsto x \otimes t^0$ gives the splitting. In fact, since $[x, y] \mapsto [x, y] \otimes t^0 = [x \otimes t^0, y \otimes t^0]$, the sequence is split as Lie algebras. \square

Theorem 2.4. *Let $\mathfrak{g} = \mathfrak{sl}_n(\mathbb{F}_p[V])$, and let \mathfrak{L} be the kernel of the evaluation map*

$$(2.11) \quad \mathfrak{g} \otimes_{\mathbb{F}_p} \mathbb{F}_p[t] \xrightarrow{t=0} \mathfrak{g}$$

as discussed above. Then

$$(2.12) \quad \mathfrak{L} \cong \text{gr}_*(\Gamma(G_n(R), p))$$

as Lie algebras.

An immediate application of Theorem 2.4 is the computation of the Lie algebra homology of $\text{gr}_*(\Gamma(G_n(R), p))$. Let $\langle t^i \rangle$ denote the \mathbb{F}_p -span of t^i .

Corollary 2.5. *Let $\mathfrak{g} = \mathfrak{sl}_n(\mathbb{F}_p[V])$ as above. Then*

$$(2.13) \quad H_1(\text{gr}_*(\Gamma(G_n(R), p))) = (\mathfrak{g} \otimes_{\mathbb{F}_p} \langle t \rangle) \oplus \left(\bigoplus_{i \geq 2} H_1(\mathfrak{g}) \otimes_{\mathbb{F}_p} \langle t^i \rangle \right).$$

The proof of Theorem 2.4 is included in Section 10. We first record some basic results concerning the group structure of the filtration quotients for the filtration of $\Gamma(G_n(R), p)$ defined in (1.1) and (2.2).

3. THE STRUCTURE OF THE FILTRATION QUOTIENTS FOR $\Gamma(G_n(R), p)$

The following theorem is due to Lee and Szczarba [14].

Theorem 3.1. *Let $G_n(R) = SL_n(\mathbb{Z})$, and suppose $n \geq 3$. There is an epimorphism*

$$(3.1) \quad \varphi_1 : \Gamma(SL_n(\mathbb{Z}), p) \longrightarrow \mathfrak{sl}_n(\mathbb{F}_p)$$

whose kernel is the commutator subgroup. Thus, $H_1(\Gamma(SL_n(\mathbb{Z}), p); \mathbb{Z}) \cong \mathfrak{sl}_n(\mathbb{F}_p)$.

Generalizing to the level p^r -congruence subgroup and to coefficient rings other than \mathbb{Z} , we obtain the following result.

Theorem 3.2. *Suppose $n \geq 2$ and $r \geq 1$. For $G_n(R) = SL_n(R)$, there is an epimorphism*

$$(3.2) \quad \varphi_r : \Gamma(G_n(R), p^r) \longrightarrow \mathfrak{sl}_n(\mathbb{F}_p[V])$$

whose kernel is $\Gamma(G_n(R), p^{r+1})$. Thus,

$$(3.3) \quad \Gamma(G_n(R), p^r) / \Gamma(G_n(R), p^{r+1}) \cong \mathfrak{sl}_n(\mathbb{F}_p[V]).$$

The proof of this theorem will be included in Section 8. An immediate application of Theorem 3.2 is the following corollary, which uses a result of Bass-Milnor-Serre [1].

Corollary 3.3. For $n \geq 3$ and $G_n(R) = SL_n(R)$,

$$(3.4) \quad \Gamma(G_n(R), p^2) = [\Gamma(G_n(R), p), \Gamma(G_n(R), p)].$$

In particular,

$$(3.5) \quad H_1(\Gamma(G_n(R), p); \mathbb{Z}) \cong \mathfrak{sl}_n(\mathbb{F}_p[V]).$$

Proof. That $\Gamma(G_n(R), p^2) \supseteq [\Gamma(G_n(R), p), \Gamma(G_n(R), p)]$ follows from the fact that filtration (2.2) is Lie-like, as will be proved in Lemma 4.3.

Let e_{ij} denote the $n \times n$ matrix with a 1 in the (i, j) position and zeros elsewhere. Let $E(G_n(R), p^r)$ be the normal subgroup of $\Gamma(G_n(R), p^r)$ generated by matrices of the form $1 + \alpha e_{ij}$, where $i \neq j$, 1 denotes the identity matrix, $\alpha \in R$, and $\alpha \equiv 0 \pmod{p^r}$. By the work of Bass-Milnor-Serre [1], we have $\Gamma(G_n(R), p^r) = E(G_n(R), p^r)$ and

$$(3.6) \quad E(G_n(R), p^{r+s}) \subseteq [E(G_n(R), p^r), E(G_n(R), p^s)]$$

for $n \geq 3$. Thus,

$$(3.7) \quad \Gamma(G_n(R), p^2) \subseteq [E(G_n(R), p), E(G_n(R), p)] \subseteq [\Gamma(G_n(R), p), \Gamma(G_n(R), p)].$$

It follows that $\Gamma(G_n(R), p^2) = [\Gamma(G_n(R), p), \Gamma(G_n(R), p)]$ for $n \geq 3$. Using this along with Theorem 3.2 (for $r = 1$), $H_1(\Gamma(G_n(R), p); \mathbb{Z}) \cong \mathfrak{sl}_n(\mathbb{F}_p[V])$ for $n \geq 3$. \square

Next, we provide an alternate description of the filtration quotients that we use to describe the structure of the Lie algebra $\text{gr}_*(\Gamma(G_n(R), p))$. We make use of the following fact, whose proof we include here for completeness.

Lemma 3.4. Let p be a prime and suppose $A = (a_{ij}) \in \text{Mat}_n(R)$. For $r \geq 1$,

$$(3.8) \quad \det(1 + p^r A) \equiv (1 + p^r \text{tr}(A)) \pmod{p^{r+1}},$$

where $\text{tr}(A)$ denotes the trace of A . In particular, if $\det(1 + p^r A) \equiv 1 \pmod{p^{r+1}}$, it must be the case that

$$(3.9) \quad \text{tr}(A) \equiv 0 \pmod{p}.$$

In other words, $a_{nn} \equiv -(a_{11} + \cdots + a_{n-1, n-1}) \pmod{p}$.

Proof. The proof is by induction on n . For $n = 2$, suppose

$$(3.10) \quad 1 + p^r A = \begin{pmatrix} 1 + p^r a_{11} & p^r a_{12} \\ p^r a_{21} & 1 + p^r a_{22} \end{pmatrix},$$

where $a_{ij} \in R$. Then

$$\begin{aligned} \det(1 + p^r A) &= 1 + p^r(a_{11} + a_{22}) + p^{2r}(a_{11}a_{22} - a_{12}a_{21}) \\ &\equiv (1 + p^r(a_{11} + a_{22})) \pmod{p^{r+1}}. \end{aligned}$$

If $\det(1 + p^r A) \equiv 1 \pmod{p^{r+1}}$, it must be the case that $\text{tr}(A) \equiv 0 \pmod{p}$. This proves the claim for the case $n = 2$.

Suppose $n - 1$ and smaller cases have been proved. Let \hat{A}_{ij} be the $(n - 1) \times (n - 1)$ matrix obtained by removing the i^{th} row and j^{th} column from $1 + p^r A = 1 + p^r(a_{ij})$.

By induction, we can write

$$\begin{aligned} \det(1 + p^r A) &= (1 + p^r a_{11}) \det(\hat{A}_{11}) + p^r \sum_{j=2}^n (-1)^{j+1} a_{1j} \det(\hat{A}_{1j}) \\ &\equiv [(1 + p^r a_{11})(1 + p^r (a_{22} + \cdots + a_{nn})) \\ &\quad + p^r \sum_{j=2}^n (-1)^{j+1} a_{1j} \det(\hat{A}_{1j})] \pmod{p^{r+1}}. \end{aligned}$$

Notice that each of \hat{A}_{1j} for $2 \leq j \leq n$ is an $(n-1) \times (n-1)$ matrix whose first column is

$$(3.11) \quad \begin{pmatrix} p^r a_{21} \\ p^r a_{31} \\ \vdots \\ p^r a_{n1} \end{pmatrix}.$$

If we use the cofactor expansion on this column to compute the determinant of \hat{A}_{1j} , it is clear that $\det(\hat{A}_{1j}) \equiv 0 \pmod{p^r}$ for $2 \leq j \leq n$, say $\det(\hat{A}_{1j}) = p^r \alpha_{1j}$. Using this above, we see that

$$\begin{aligned} \det(1 + p^r A) &\equiv [(1 + p^r a_{11})(1 + p^r (a_{22} + \cdots + a_{nn})) \\ &\quad + p^{2r} \sum_{j=2}^n (-1)^{j+1} a_{1j} \alpha_{1j}] \pmod{p^{r+1}} \\ &\equiv [(1 + p^r a_{11})(1 + p^r (a_{22} + \cdots + a_{nn}))] \pmod{p^{r+1}} \\ &\equiv [1 + p^r \operatorname{tr}(A) + p^{2r} a_{11}(a_{22} + \cdots + a_{nn})] \pmod{p^{r+1}} \\ &\equiv [1 + p^r \operatorname{tr}(A)] \pmod{p^{r+1}}. \end{aligned}$$

If $\det(1 + p^r A) \equiv 1 \pmod{p^{r+1}}$, it must be the case that $\operatorname{tr}(A) \equiv 0 \pmod{p}$. This completes the proof of the lemma. \square

Theorem 3.5. *Let V be a \mathbb{Z} -basis for R . Suppose $|V| < \infty$ or $s = 1$. For $r \geq s \geq 1$ and p a prime,*

$$(3.12) \quad \Gamma(G_n(R), p^r) / \Gamma(G_n(R), p^{r+s}) \cong \bigoplus_{n^2-1} \mathbb{Z}/p^s \mathbb{Z}[V].$$

The proof is by induction on s . For the sake of continuity, we prove the case $s = 1$ in the next lemma, and complete the induction in Section 9. We first state a corollary that follows directly from Theorem 3.5.

Corollary 3.6. *For all primes p ,*

$$(3.13) \quad \varprojlim_s \Gamma(G_n(R), p^s) / \Gamma(G_n(R), p^{2s}) = \bigoplus_{n^2-1} \hat{\mathbb{Z}}_p[V],$$

where $\hat{\mathbb{Z}}_p$ denotes the p -adic integers.

Proof. Follows immediately from Theorem 3.5 and the fact that inverse limits commute with direct sums. \square

Lemma 3.7. *For $r \geq 1$ and p a prime,*

$$(3.14) \quad \Gamma(G_n(R), p^r) / \Gamma(G_n(R), p^{r+1}) \cong \bigoplus_{n^2-1} \mathbb{F}_p[V],$$

where V is a \mathbb{Z} -basis for R .

Proof. Consider the commutative diagram in Figure 2, where ϕ_r , ϕ_{r+1} , and θ_r are

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & \Gamma(G_n(R), p^{r+1}) & \xrightarrow{Id} & \Gamma(G_n(R), p^{r+1}) & \longrightarrow & \{1\} \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & \Gamma(G_n(R), p^r) & \longrightarrow & SL_n(R) & \xrightarrow{\phi_r} & SL_n(R \otimes_{\mathbb{Z}} \mathbb{Z}/p^r) \longrightarrow 1 \\
 & & \downarrow & & \downarrow \phi_{r+1} & & \downarrow Id \\
 1 & \longrightarrow & \ker \theta_r & \longrightarrow & SL_n(R \otimes_{\mathbb{Z}} \mathbb{Z}/p^{r+1}) & \xrightarrow{\theta_r} & SL_n(R \otimes_{\mathbb{Z}} \mathbb{Z}/p^r) \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 1 & & 1 & & 1
 \end{array}$$

FIGURE 2

the natural reduction maps and $\phi_r = \theta_r \circ \phi_{r+1}$. In [18], it is shown that reduction maps such as ϕ_r , ϕ_{r+1} , and θ_r are surjections. Given this, it is immediate that the three rows and two right columns are exact. A standard diagram chase can be used to show that the first column is also exact. This gives

$$(3.15) \quad \ker \theta_r \cong \Gamma(G_n(R), p^r) / \Gamma(G_n(R), p^{r+1}).$$

The reader should note that this isomorphism allows us to consider

$$(3.16) \quad \Gamma(G_n(R), p^r) / \Gamma(G_n(R), p^{r+1}) \subseteq SL_n(R \otimes_{\mathbb{Z}} \mathbb{Z}/p^{r+1}).$$

This will prove to be a useful fact at many points throughout this paper.

A priori, an element of $\ker \theta_r$ is a matrix of the form $1 + p^r A$ where $A = (a_{ij}) \in \text{Mat}_n(R)$ and $\det(1 + p^r A) \equiv 1 \pmod{p^{r+1}}$. Since $1 + p^r A \in SL_n(R \otimes_{\mathbb{Z}} \mathbb{Z}/p^{r+1})$, we can assume $A \in \text{Mat}_n(R \otimes_{\mathbb{Z}} \mathbb{Z}/p)$.

Define a map $\Phi : \bigoplus_{n^2-1} \mathbb{F}_p[V] \longrightarrow \ker \theta_r$ by

$$(3.17) \quad (a_{11}, \dots, a_{1n}, a_{21}, \dots, a_{2n}, \dots, a_{n1}, \dots, a_{n,n-1}) \mapsto 1 + p^r (a_{ij}),$$

where $a_{nn} = -(a_{11} + a_{22} + \dots + a_{n-1,n-1})$. By Lemma 3.4, we see immediately that Φ is surjective. By inspection, the kernel is trivial, so that Φ is a bijection.

To check that Φ is a homomorphism, notice that

$$\begin{aligned}
 (1 + p^r A)(1 + p^r B) &= 1 + p^r(A + B) + p^{2r} AB \\
 &\equiv 1 + p^r(A + B) \pmod{p^{r+1}}.
 \end{aligned}$$

Thus, Φ is the required isomorphism. This completes the proof. \square

This lemma has several immediate consequences. Recall that $V = \{v_i\}_{i \in I}$ is a \mathbb{Z} -basis for R . For $r \geq 1$, $1 \leq i, j \leq n$, and $i + j < 2n$, define a family of matrices by

$$(3.18) \quad A_{ij,k,r} = \begin{cases} 1 + p^r v_k e_{ij} & \text{if } i \neq j \\ 1 + p^r v_k (e_{ii} - e_{nn}) & \text{if } i = j, \end{cases}$$

where 1 denotes the $n \times n$ identity matrix, and the matrices $\{e_{ij}\}$ are as defined in the proof of Corollary 3.3.

Corollary 3.8. *For $r \geq 1$, $\Gamma(G_n(R), p^r)/\Gamma(G_n(R), p^{r+1})$ is generated by the family of matrices $\{A_{ij,k,r}\}$ defined in 3.18.*

Remark. It is clear that $\det(A_{ij,k,r}) = 1$ for $i \neq j$. When $i = j$, notice that

$$(3.19) \quad \det(A_{ii,k,r}) = (1 + p^r v_k)(1 - p^r v_k) = 1 - p^{2r} v_k^2 \equiv 1 \pmod{p^{r+1}}.$$

Since $\Gamma(G_n(R), p^r)/\Gamma(G_n(R), p^{r+1}) \subseteq SL_n(R \otimes_{\mathbb{Z}} \mathbb{Z}/p^{r+1})$, this suffices.

4. THE LIE ALGEBRA ASSOCIATED TO $SL_n(R)$

We begin with some preliminary definitions concerning the existence of the associated Lie algebra, and then describe its structure completely. The following definition is stated as in [4].

Definition 4.1. *A filtration $\{F_n(G)\}_{n \geq 0}$ of the group G is said to be Lie-like if, for all $m, n \geq 0$, the commutator map*

$$(4.1) \quad [-, -] : G \times G \longrightarrow G$$

given by $[g, h] \mapsto g^{-1}h^{-1}gh$ restricts to a map

$$(4.2) \quad [-, -] : F_m(G) \times F_n(G) \longrightarrow F_{m+n}(G).$$

The next theorem is classical and can be found in [17], for example. The theorem gives a general procedure for constructing a Lie algebra from a filtered group whenever the filtration is Lie-like.

Theorem 4.2. *Given a Lie-like filtration for the group G , there is an associated Lie algebra*

$$(4.3) \quad \text{gr}_*(G) = \bigoplus_{n \geq 1} F_n(G)/F_{n+1}(G).$$

The Lie bracket is obtained by linearly extending the maps

$$(4.4) \quad [-, -] : F_m(G)/F_{m+1}(G) \times F_n(G)/F_{n+1}(G) \longrightarrow F_{m+n}(G)/F_{m+n+1}(G)$$

that are induced by the restriction of the commutator map.

Remark. Note that these Lie algebras are not, in general, graded Lie algebras. In other words, it is not necessarily true that $[x, y] = (-1)^{|x||y|}[y, x]$, and the graded Jacobi identity need not be satisfied.

Next, we verify that the filtration of $\Gamma(G_n(R), p)$ given by (2.2) is Lie-like.

Lemma 4.3. *Suppose that $X \in \Gamma(G_n(R), p^r)$ and $Y \in \Gamma(G_n(R), p^s)$ for some $r, s \geq 1$. Then $[X, Y] \in \Gamma(G_n(R), p^{r+s})$, where $[X, Y] = X^{-1}Y^{-1}XY$ is the group commutator.*

Proof. We can write $X = 1 + p^r A$ and $Y = 1 + p^s B$ for some matrices $A, B \in \text{Mat}_n(R)$. Then

$$\begin{aligned} [1 + p^r A, 1 + p^s B] &= (1 + p^r A)^{-1}(1 + p^s B)^{-1}(1 + p^r A)(1 + p^s B) \\ &= \sum_{i=0}^{\infty} (-p^r A)^i \sum_{j=0}^{\infty} (-p^s B)^j (1 + p^r A)(1 + p^s B) \\ &= 1 + p^{r+s}(AB - BA) + p^{r+s+1}C, \end{aligned}$$

where $C \in \text{Mat}_n(R)$ is some combination of A and B . Thus,

$$(4.5) \quad [X, Y] \in \Gamma(G_n(R), p^{r+s}),$$

as desired. \square

By Theorem 4.2, there is an associated Lie algebra

$$(4.6) \quad \text{gr}_*(\Gamma(G_n(R), p)) = \bigoplus_{r \geq 1} \Gamma(G_n(R), p^r) / \Gamma(G_n(R), p^{r+1}),$$

in which the Lie bracket is induced by the restriction of the commutator map. In the next corollary, we use the notation $\Gamma_r = \Gamma(G_n(R), p^r)$.

Corollary 4.4. *The commutator map*

$$(4.7) \quad [-, -] : \Gamma(G_n(R), p^r) \times \Gamma(G_n(R), p^s) \longrightarrow \Gamma(G_n(R), p^{r+s})$$

extends to a well-defined map on the filtration quotients

$$(4.8) \quad [-, -] : \Gamma_r / \Gamma_{r+1} \times \Gamma_s / \Gamma_{s+1} \longrightarrow \Gamma_{r+s} / \Gamma_{r+s+1}.$$

The Lie bracket

$$(4.9) \quad [-, -] : \text{gr}_*(\Gamma(G_n(R), p)) \otimes_{\mathbb{F}_p} \text{gr}_*(\Gamma(G_n(R), p)) \longrightarrow \text{gr}_*(\Gamma(G_n(R), p))$$

is obtained by extending the maps in (4.8) linearly.

Proof. This follows immediately from the proof of Lemma 4.3 and [17]. \square

The next result will be used to describe $\text{gr}_*(\Gamma(G_n(R), p))$ as a restricted Lie algebra. Recall that $\Gamma(G_n(R), p^r) / \Gamma(G_n(R), p^{r+1})$ for $r \geq 1$ is generated by the family of matrices $\{A_{ij,k,r}\}$ defined in Corollary 3.8.

Proposition 4.5. *The Frobenius map*

$$(4.10) \quad \Gamma(G_n(R), p^r) \longrightarrow \Gamma(G_n(R), p^{r+1})$$

defined by $A_{ij,k,r} \mapsto (A_{ij,k,r})^p$ induces a map

$$(4.11) \quad \psi_r^p : \Gamma(G_n(R), p^r) / \Gamma(G_n(R), p^{r+1}) \longrightarrow \Gamma(G_n(R), p^{r+1}) / \Gamma(G_n(R), p^{r+2}).$$

This map is an isomorphism, except in the case $p = 2, r = 1$. Furthermore, $\psi_r^p(A_{ij,k,r}) = A_{ij,k,r+1}$.

Proof. Assume that $p \neq 2$ or $r > 1$.

A typical element of $\Gamma(G_n(R), p^r) / \Gamma(G_n(R), p^{r+1})$ is of the form $1 + p^r A$ where $A \in \text{Mat}_n(R)$. In the proof of Lemma 3.7, it was noted that

$$(4.12) \quad \Gamma(G_n(R), p^r) / \Gamma(G_n(R), p^{r+1}) \subseteq SL_n(R \otimes_{\mathbb{Z}} \mathbb{Z}/p^{r+1}),$$

so we can assume that $A \in \text{Mat}_n(R \otimes_{\mathbb{Z}} \mathbb{Z}/p)$. To see that the image of ψ_r^p lies in $\Gamma(G_n(R), p^{r+1})/\Gamma(G_n(R), p^{r+2})$, notice that

$$\begin{aligned} \psi_r^p(1 + p^r A) &= (1 + p^r A)^p \\ &= \sum_{i=0}^p \binom{p}{i} (p^r A)^i \\ &\equiv (1 + p^{r+1} A) \pmod{p^{r+2}}. \end{aligned}$$

To check that ψ_r^p is a homomorphism, consider two elements $1 + p^r A, 1 + p^r B \in \Gamma(G_n(R), p^r)/\Gamma(G_n(R), p^{r+1})$. Then

$$\begin{aligned} \psi_r^p((1 + p^r A)(1 + p^r B)) &= \psi_r^p(1 + p^r(A + B)) \\ &= (1 + p^r(A + B))^p \\ &\equiv (1 + p^{r+1}(A + B)) \pmod{p^{r+2}} \\ &\equiv (1 + p^{r+1}A)(1 + p^{r+1}B) \pmod{p^{r+2}} \\ &= \psi_r^p(1 + p^r A)\psi_r^p(1 + p^r B). \end{aligned}$$

Thus, ψ_r^p is a homomorphism.

To see that ψ_r^p is surjective, we show that it maps onto the generators of $\Gamma(G_n(R), p^{r+1})/\Gamma(G_n(R), p^{r+2})$. For $i \neq j$,

$$\begin{aligned} (A_{ij,k,r})^p &= (1 + p^r v_k e_{ij})^p \\ &= \sum_{l=0}^p \binom{p}{l} (p^r v_k e_{ij})^l \\ &\equiv (1 + p^{r+1} v_k e_{ij}) \pmod{p^{r+2}} \\ &= A_{ij,k,r+1}. \end{aligned}$$

For $i = j$, a similar computation gives the following:

$$\begin{aligned} (A_{ii,k,r})^p &= (1 + p^r v_k (e_{ii} - e_{nn}))^p \\ &= \sum_{l=0}^p \binom{p}{l} (p^r v_k (e_{ii} - e_{nn}))^l \\ &\equiv (1 + p^{r+1} v_k (e_{ii} - e_{nn})) \pmod{p^{r+2}} \\ &= A_{ii,k,r+1}. \end{aligned}$$

Thus, $\psi_r^p(A_{ij,k,r}) = A_{ij,k,r+1}$, which gives that ψ_r^p is surjective.

Finally, suppose that $\psi_r^p(1 + p^r A) = 1$. Then it must be the case that

$$(4.13) \quad p^{r+1} A \equiv 0 \pmod{p^{r+2}}.$$

Since $A \in \text{Mat}_n(R \otimes_{\mathbb{Z}} \mathbb{Z}/p)$, we conclude that $A \equiv 0 \pmod{p}$. Hence,

$$(4.14) \quad (1 + p^r A) \equiv 1 \pmod{p^{r+1}},$$

so that ψ_r^p is injective. This completes the proof of the proposition. \square

We are now ready to give the structure of the Lie algebra $\text{gr}_*(\Gamma(G_n(R), p))$, and we do so in the next theorem. In our computations, we make use of the following well-known result.

Lemma 4.6. *For the matrices $\{e_{ij}\}$ defined in the proof of Corollary 3.3, we have the following:*

$$(4.15) \quad [e_{ij}, e_{kl}] = e_{ij}e_{kl} - e_{kl}e_{ij} = \begin{cases} -e_{kj} & \text{if } i = l \text{ and } j \neq k, \\ e_{il} & \text{if } i \neq l \text{ and } j = k, \\ e_{il} - e_{kj} & \text{if } i = l \text{ and } j = k, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. It is clear that the first term, $e_{ij}e_{kl}$, is non-zero only when $j = k$, and the second term, $e_{kl}e_{ij}$, is non-zero precisely when $i = l$. In these cases, $e_{ij}e_{kl} = e_{il}$ and $e_{kl}e_{ij} = e_{kj}$. The result follows. \square

In the next theorem, we use the notation $A_{ij,q_1q_2,r} = 1 + p^r v_{q_1} v_{q_2} e_{ij}$. Here, $v_{q_1}, v_{q_2} \in V$.

Theorem 4.7. *Suppose $r \geq 1$ and p is a prime. For the Lie algebra*

$$(4.16) \quad \text{gr}_*(\Gamma(G_n(R), p)) = \bigoplus_{r \geq 1} \Gamma(G_n(R), p^r) / \Gamma(G_n(R), p^{r+1}),$$

the following properties are satisfied:

- (1) $\Gamma(G_n(R), p^r) / \Gamma(G_n(R), p^{r+1}) \cong \bigoplus_{n^2-1} \mathbb{F}_p[V]$.
- (2) $\Gamma(G_n(R), p^r) / \Gamma(G_n(R), p^{r+1}) \cong \mathfrak{sl}_n(\mathbb{F}_p[V])$.
- (3) $\psi_r^p(A_{ij,k,r}) = A_{ij,k,r+1}$, where the matrices $\{A_{ij,k,r}\}$ are as defined in Corollary 3.8.
- (4) $\text{gr}_*(\Gamma(G_n(R), p))$ is generated as a restricted Lie algebra by the matrices $\{A_{ij,k,1}\}$.
- (5) The Lie bracket is defined on the generators $\{A_{ij,k,r}\}$ as follows:

$$[A_{ij,q_1,r}, A_{kl,q_2,s}] = \begin{cases} A_{kj,q_1q_2,r+s}^{-1} & \text{if } i = l, j \neq k, i \neq j, k \neq l \\ A_{ii,q_1q_2,r+s}^{-1} A_{jj,q_1q_2,r+s}^{-1} & \text{if } i = l, j = k, i \neq j, k \neq l \\ A_{il,q_1q_2,r+s} & \text{if } i \neq l, j = k, i \neq j, k \neq l \\ A_{in,q_1q_2,r+s}^{-2} & \text{if } i = k = l, i \neq j, j = n \\ A_{ij,q_1q_2,r+s}^{-1} & \text{if } i = k = l, i \neq j, j \neq n, i \neq n \\ A_{nj,q_1q_2,r+s}^2 & \text{if } j = k = l, i \neq j, i = n \\ A_{ij,q_1q_2,r+s} & \text{if } j = k = l, i \neq j, i \neq n, j \neq n \\ A_{in,q_1q_2,r+s}^{-1} & \text{if } k = l, i \neq k, j \neq k, i \neq j, j = n \\ A_{nj,q_1q_2,r+s} & \text{if } k = l, i \neq k, j \neq k, i \neq j, i = n \\ A_{in,q_1q_2,r+s}^{-2} & \text{if } i = j = l, k \neq l, k = n \\ A_{ki,q_1q_2,r+s}^{-1} & \text{if } i = j = l, k \neq l, k \neq n, l \neq n \\ A_{in,q_1q_2,r+s}^2 & \text{if } i = j = k, k \neq l, l = n \\ A_{il,q_1q_2,r+s} & \text{if } i = j = k, k \neq l, k \neq n, l \neq n \\ A_{nl,q_1q_2,r+s}^{-1} & \text{if } i = j, k \neq l, i \neq l, i \neq k, k = n \\ A_{kn,q_1q_2,r+s} & \text{if } i = j, k \neq l, i \neq l, i \neq k, l = n \\ 1 & \text{otherwise.} \end{cases}$$

Proof. The first four parts of the theorem follow immediately from Lemma 3.7, Theorem 3.2, Proposition 4.5, and Corollary 3.8, respectively. By Lemma 4.3, we

have the following:

$$[A_{ij,q_1,r}, A_{kl,q_2,s}] = \begin{cases} 1 + p^{r+s} v_{q_1} v_{q_2} [e_{ij}, e_{kl}] & \text{if } i \neq j, k \neq l \\ 1 + p^{r+s} v_{q_1} v_{q_2} ([e_{ij}, e_{kk}] + [e_{nn}, e_{ij}]) & \text{if } i \neq j, k = l \\ 1 + p^{r+s} v_{q_1} v_{q_2} ([e_{ii}, e_{kl}] + [e_{kl}, e_{nn}]) & \text{if } i = j, k \neq l \\ 1 + p^{r+s} v_{q_1} v_{q_2} ([e_{ii}, e_{kk}] + [e_{nn}, e_{ii}] + [e_{kk}, e_{nn}]) & \text{if } i = j, k = l. \end{cases}$$

Using Lemma 4.6, the reader can verify the relations listed in the statement of the theorem. \square

5. COHOMOLOGY OF CONGRUENCE SUBGROUPS FOR $SL_2(\mathbb{Z}[t])$

Suppose $n = 2$ and $R = \mathbb{Z}[t]$, so that $G_n(R) = G_2(\mathbb{Z}[t]) = SL_2(\mathbb{Z}[t])$, where $\mathbb{Z}[t]$ is a polynomial ring in one indeterminate. For fixed $r \geq 1$ and $i \geq 0$, consider the matrix

$$(5.1) \quad A_{12,i,r} = \begin{pmatrix} 1 & p^r t^i \\ 0 & 1 \end{pmatrix} \in \Gamma(G_2(\mathbb{Z}[t]), p^r).$$

The collection $\{A_{12,i,r}\}_{i \geq 0}$ is a family of pairwise commutative matrices, each of infinite order in $\Gamma(G_2(\mathbb{Z}[t]), p^r)$. This collection generates a copy of $\bigoplus_{i \geq 0} \mathbb{Z} \subseteq \Gamma(G_2(\mathbb{Z}[t]), p^r)$. Thus, we have the diagram

$$\begin{array}{ccccc} \bigoplus_{i \geq 0} \mathbb{Z} & \xrightarrow{i} & \Gamma(G_2(\mathbb{Z}[t]), p^r) & \xrightarrow{\pi} & \Gamma(G_2(\mathbb{Z}[t]), p^r) / \Gamma(G_2(\mathbb{Z}[t]), p^{r+1}) \\ & & & & \downarrow \Phi_2^{-1} \\ & & & & \mathbb{F}_p[t] \\ & & & \searrow f & \\ & & & & \end{array}$$

FIGURE 3

where i is the inclusion map, π is the natural quotient map, Φ_2^{-1} is the projection onto the second coordinate under the isomorphism Φ_2^{-1} defined in the proof of Lemma 3.7, and f is the composite. Notice that $f(A_{12,i,r}) = t^i$ under this mapping. We now consider the cases $p = 2$ and $p > 2$ separately.

$p = 2$: Recall that

$$(5.2) \quad H^*(\mathbb{F}_2[t]; \mathbb{F}_2) \cong H^*(\bigoplus_{i \geq 0} \mathbb{F}_2; \mathbb{F}_2) \cong \mathbb{F}_2[x_0, x_1, \dots],$$

a polynomial ring in an infinite number of indeterminates of degree one, where each x_i is dual to the image of $A_{12,i,r}$ in $\Gamma(G_2(\mathbb{Z}[t]), 2^r) / \Gamma(G_2(\mathbb{Z}[t]), 2^{r+1})$. Also,

$$(5.3) \quad H^*(\bigoplus_{i \geq 0} \mathbb{Z}; \mathbb{F}_2) \cong \Lambda^*(y_0, y_1, \dots; \mathbb{F}_2),$$

an exterior algebra in an infinite number of indeterminates of degree one over \mathbb{F}_2 , where each y_i is dual to $A_{12,i,r}$ in $\Gamma(G_2(\mathbb{Z}[t]), 2^r)$.

As illustrated in Figure 4, there are induced maps in cohomology for which $f^*(x_i) = y_i$ for $j = 1$. This implies that f^* is an epimorphism for $j \geq 1$, forcing i^* to be an epimorphism for $j \geq 1$ as well. In this case, $H^j(\bigoplus_{i \geq 0} \mathbb{Z}; \mathbb{F}_2)$ is a quotient of $H^j(\Gamma(G_2(\mathbb{Z}[t]), 2^r); \mathbb{F}_2)$. Since $H^j(\bigoplus_{i \geq 0} \mathbb{Z}; \mathbb{F}_2)$ is not finitely generated for $j \geq 1$, neither is $H^j(\Gamma(G_2(\mathbb{Z}[t]), 2^r); \mathbb{F}_2)$.

$$\begin{array}{ccccc}
H^j(\mathbb{F}_2[t]; \mathbb{F}_2) & \xrightarrow{(\Phi_2^{-1} \circ \pi)^*} & H^j(\Gamma(G_2(\mathbb{Z}[t]), 2^r); \mathbb{F}_2) & \xrightarrow{i^*} & H^j(\bigoplus_{i \geq 0} \mathbb{Z}; \mathbb{F}_2) \\
& & & & \parallel \\
& & & & H^j(\bigoplus_{i \geq 0} \mathbb{Z}; \mathbb{F}_2) \\
& \searrow f^* & & &
\end{array}$$

FIGURE 4

$p > 2$: Recall that

$$(5.4) \quad H^*(\mathbb{F}_p[t]; \mathbb{F}_p) \cong H^*(\bigoplus_{i \geq 0} \mathbb{F}_p; \mathbb{F}_p) \cong \Lambda^*(x_0, x_1, \dots; \mathbb{F}_p) \otimes \mathbb{F}_p[\beta x_0, \beta x_1, \dots],$$

the tensor product of an exterior algebra with a polynomial ring. Here, each x_i has degree one, and $\beta : H^1(\mathbb{F}_p; \mathbb{F}_p) \longrightarrow H^2(\mathbb{F}_p; \mathbb{F}_p)$ is the Bockstein homomorphism. As above, each x_i is dual to the image of $A_{12,i,r}$ in $\Gamma(G_2(\mathbb{Z}[t]), p^r)/\Gamma(G_2(\mathbb{Z}[t]), p^{r+1})$. Also,

$$(5.5) \quad H^*(\bigoplus_{i \geq 0} \mathbb{Z}; \mathbb{F}_p) \cong \Lambda^*(y_0, y_1, \dots; \mathbb{F}_p),$$

an exterior algebra in an infinite number of indeterminates of degree one over \mathbb{F}_p , where each y_i is dual to $A_{12,i,r}$ in $\Gamma(G_2(\mathbb{Z}[t]), p^r)$.

There are induced maps in cohomology

$$\begin{array}{ccccc}
H^j(\mathbb{F}_p[t]; \mathbb{F}_p) & \xrightarrow{(\Phi_2^{-1} \circ \pi)^*} & H^j(\Gamma(G_2(\mathbb{Z}[t]), p^r); \mathbb{F}_p) & \xrightarrow{i^*} & H^j(\bigoplus_{i \geq 0} \mathbb{Z}; \mathbb{F}_p) \\
& & & & \parallel \\
& & & & H^j(\bigoplus_{i \geq 0} \mathbb{Z}; \mathbb{F}_p) \\
& \searrow f^* & & &
\end{array}$$

FIGURE 5

for which $f^*(x_i) = y_i$ for $j = 1$. This implies that f^* is an epimorphism for $j \geq 1$, forcing i^* to be an epimorphism for $j \geq 1$ as well. In this case, $H^j(\bigoplus_{i \geq 0} \mathbb{Z}; \mathbb{F}_p)$ is a quotient of $H^j(\Gamma(G_2(\mathbb{Z}[t]), p^r); \mathbb{F}_p)$. Since $H^j(\bigoplus_{i \geq 0} \mathbb{Z}; \mathbb{F}_p)$ is not finitely generated for $j \geq 1$, neither is $H^j(\Gamma(G_2(\mathbb{Z}[t]), p^r); \mathbb{F}_p)$. Thus, we have proved the following theorem.

Theorem 5.1. *Suppose $n = 2$ and $R = \mathbb{Z}[t]$. For all $j, r \geq 1$ and for all primes p ,*

$$(5.6) \quad H^j(\Gamma(G_2(\mathbb{Z}[t]), p^r); \mathbb{F}_p)$$

is infinitely generated.

6. COHOMOLOGY OF CONGRUENCE SUBGROUPS FOR $SL_2(\mathbb{Z}[i])$

Suppose $n = 2$ and $R = \mathbb{Z}[i]$, so that $G_n(R) = G_2(\mathbb{Z}[i]) = SL_2(\mathbb{Z}[i])$, where $\mathbb{Z}[i]$ is the Gaussian integers. Let e_{ij} denote the 2×2 matrix with a 1 in the (i, j) position and zeros elsewhere. For fixed $r \geq 1$, $\epsilon \in \{0, 1\}$, and $i \neq j$, consider the matrices $A_{ij,\epsilon,r} = 1 + p^r i^\epsilon e_{ij} \in \Gamma(G_2(\mathbb{Z}[i]), p^r)$. Each of these four matrices has infinite order in $\Gamma(G_2(\mathbb{Z}[i]), p^r)$. Notice that $A_{12,0,r}$ and $A_{12,1,r}$ commute, so they generate a copy of $\mathbb{Z} \oplus \mathbb{Z} \subseteq \Gamma(G_2(\mathbb{Z}[i]), p^r)$. The same is true for the matrices $A_{21,0,r}$ and $A_{21,1,r}$. Thus, we have embeddings $i_1 : \mathbb{Z} \oplus \mathbb{Z} \longrightarrow \Gamma(G_2(\mathbb{Z}[i]), p^r)$ and $i_2 : \mathbb{Z} \oplus \mathbb{Z} \longrightarrow \Gamma(G_2(\mathbb{Z}[i]), p^r)$. These embeddings give the following diagram:

$$\begin{array}{ccc}
(\mathbb{Z} \oplus \mathbb{Z}) * (\mathbb{Z} \oplus \mathbb{Z}) & \xrightarrow{i_1 * i_2} & \Gamma(G_2(\mathbb{Z}[i]), p^r) \xrightarrow{\pi} \Gamma(G_2(\mathbb{Z}[i]), p^r) / \Gamma(G_2(\mathbb{Z}[i]), p^{r+1}) \\
& \searrow f & \downarrow \Phi^{-1} \\
& & \oplus_6 \mathbb{F}_p
\end{array}$$

FIGURE 6

Here, π is the natural quotient map, Φ is the isomorphism defined in the proof of Lemma 3.7, and f is the composite. We now consider the cases $p = 2$ and $p > 2$ separately.

$p = 2$: Recall that

$$(6.1) \quad H^*(\oplus_6 \mathbb{F}_2; \mathbb{F}_2) \cong \mathbb{F}_2[x_1, x_2, y_1, y_2, z_1, z_2],$$

a polynomial ring in six indeterminates of degree one, where x_1 is dual to the image of $A_{12,0,r}$, x_2 is dual to the image of $A_{12,1,r}$, y_1 is dual to the image of $A_{21,0,r}$, and y_2 is dual to the image of $A_{21,1,r}$ in $\Gamma(G_2(\mathbb{Z}[i]), 2^r) / \Gamma(G_2(\mathbb{Z}[i]), 2^{r+1})$. Also,

$$(6.2) \quad H^*((\mathbb{Z} \oplus \mathbb{Z}) * (\mathbb{Z} \oplus \mathbb{Z}); \mathbb{F}_2) \cong \Lambda^*(u_1, u_2; \mathbb{F}_2) \oplus \Lambda^*(w_1, w_2; \mathbb{F}_2),$$

where u_1 is dual to $A_{12,0,r}$, u_2 is dual to $A_{12,1,r}$, w_1 is dual to $A_{21,0,r}$, and w_2 is dual to $A_{21,1,r}$ in $\Gamma(G_2(\mathbb{Z}[i]), 2^r)$. All of $u_1, u_2, w_1,$ and w_2 have degree one. In particular, notice that

$$(6.3) \quad H^2((\mathbb{Z} \oplus \mathbb{Z}) * (\mathbb{Z} \oplus \mathbb{Z}); \mathbb{F}_2) \cong \mathbb{F}_2 \oplus \mathbb{F}_2,$$

generated by the classes $u_1 u_2$ and $w_1 w_2$.

There are induced maps in cohomology

$$\begin{array}{ccc}
H^j(\oplus_6 \mathbb{F}_2; \mathbb{F}_2) & \xrightarrow{(\Phi^{-1} \circ \pi)^*} & H^j(\Gamma(G_2(\mathbb{Z}[i]), 2^r); \mathbb{F}_2) \xrightarrow{(i_1 * i_2)^*} & H^j((\mathbb{Z} \oplus \mathbb{Z}) * (\mathbb{Z} \oplus \mathbb{Z}); \mathbb{F}_2) \\
& \searrow f^* & & \parallel \\
& & & H^j((\mathbb{Z} \oplus \mathbb{Z}) * (\mathbb{Z} \oplus \mathbb{Z}); \mathbb{F}_2)
\end{array}$$

FIGURE 7

for which $f^*(x_i) = u_i$ and $f^*(y_i) = w_i$ for $j = 1$. Thus, we see that f^* is an epimorphism for $j = 2$, forcing $(i_1 * i_2)^*$ to be an epimorphism for $j = 2$ as well. As a result, $H^2((\mathbb{Z} \oplus \mathbb{Z}) * (\mathbb{Z} \oplus \mathbb{Z}); \mathbb{F}_2)$ is a quotient of $H^2(\Gamma(G_2(\mathbb{Z}[i]), 2^r); \mathbb{F}_2)$, so that $\mathbb{F}_2 \oplus \mathbb{F}_2 \subseteq H^2(\Gamma(G_2(\mathbb{Z}[i]), 2^r); \mathbb{F}_2)$.

$p > 2$: Recall that

$$(6.4) \quad H^*(\oplus_6 \mathbb{F}_p; \mathbb{F}_p) \cong \Lambda^*(x_1, x_2, y_1, y_2, z_1, z_2; \mathbb{F}_p) \otimes \mathbb{F}_p[\beta x_1, \beta x_2, \beta y_1, \beta y_2, \beta z_1, \beta z_2],$$

the tensor product of an exterior algebra with a polynomial ring. Here, each $x_i, y_i,$ and z_i is of degree one and $\beta : H^1(\mathbb{F}_p; \mathbb{F}_p) \longrightarrow H^2(\mathbb{F}_p; \mathbb{F}_p)$ is the Bockstein homomorphism. Similar to above, x_1 is dual to the image of $A_{12,0,r}$, x_2 is dual to

the image of $A_{12,1,r}$, y_1 is dual to the image of $A_{21,0,r}$, and y_2 is dual to the image of $A_{21,1,r}$ in $\Gamma(G_2(\mathbb{Z}[i]), p^r)/\Gamma(G_2(\mathbb{Z}[i]), p^{r+1})$. Also,

$$(6.5) \quad H^*((\mathbb{Z} \oplus \mathbb{Z}) * (\mathbb{Z} \oplus \mathbb{Z}); \mathbb{F}_p) \cong \Lambda^*(u_1, u_2; \mathbb{F}_p) \oplus \Lambda^*(w_1, w_2; \mathbb{F}_p),$$

where u_1 is dual to $A_{12,0,r}$, u_2 is dual to $A_{12,1,r}$, w_1 is dual to $A_{21,0,r}$, and w_2 is dual to $A_{21,1,r}$ in $\Gamma(G_2(\mathbb{Z}[i]), p^r)$. All of u_1, u_2, w_1 , and w_2 have degree one. In particular, notice that

$$(6.6) \quad H^2((\mathbb{Z} \oplus \mathbb{Z}) * (\mathbb{Z} \oplus \mathbb{Z}); \mathbb{F}_p) \cong \mathbb{F}_p \oplus \mathbb{F}_p,$$

generated by the classes $u_1 u_2$ and $w_1 w_2$.

As illustrated in Figure 8, there are induced maps in cohomology for which

$$\begin{array}{ccc} H^j(\oplus_6 \mathbb{F}_p; \mathbb{F}_p) & \xrightarrow{(\Phi^{-1} \circ \pi)^*} & H^j(\Gamma(G_2(\mathbb{Z}[i]), p^r); \mathbb{F}_p) & \xrightarrow{(i_1 * i_2)^*} & H^j((\mathbb{Z} \oplus \mathbb{Z}) * (\mathbb{Z} \oplus \mathbb{Z}); \mathbb{F}_p) \\ & \searrow f^* & & & \parallel \\ & & & & H^j((\mathbb{Z} \oplus \mathbb{Z}) * (\mathbb{Z} \oplus \mathbb{Z}); \mathbb{F}_p) \end{array}$$

FIGURE 8

$f^*(x_i) = u_i$ and $f^*(y_i) = w_i$ for $j = 1$. Thus, we see that f^* is an epimorphism for $j = 2$, forcing $(i_1 * i_2)^*$ to be an epimorphism for $j = 2$ as well. As a result, $H^2((\mathbb{Z} \oplus \mathbb{Z}) * (\mathbb{Z} \oplus \mathbb{Z}); \mathbb{F}_p)$ is a quotient of $H^2(\Gamma(G_2(\mathbb{Z}[i]), p^r); \mathbb{F}_p)$, so that $\mathbb{F}_p \oplus \mathbb{F}_p \subseteq H^2(\Gamma(G_2(\mathbb{Z}[i]), p^r); \mathbb{F}_p)$. We have now proved the following theorem.

Theorem 6.1. *Suppose $n = 2$ and $R = \mathbb{Z}[i]$. For all $r \geq 1$ and for all primes p ,*

$$(6.7) \quad H^2(\Gamma(G_2(\mathbb{Z}[i]), p^r); \mathbb{F}_p) \supseteq \mathbb{F}_p \oplus \mathbb{F}_p.$$

7. COMPUTING d^2 FOR CENTRAL EXTENSIONS OF CONGRUENCE SUBGROUPS

In this section, we use the convention $\Gamma_r = \Gamma(G_n(R), p^r)$. Let $F[x, y]$ be the free group on two letters, and let K denote the kernel of the abelianization map $F[x, y] \longrightarrow \mathbb{Z} \oplus \mathbb{Z}$.

Suppose $r, s, l \geq 1$. Specifying elements $\theta(x), \theta(y) \in \Gamma_r/\Gamma_{r+s}$ defines a unique homomorphism

$$(7.1) \quad \theta : F[x, y] \longrightarrow \Gamma_r/\Gamma_{r+s}.$$

We are interested in situations in which two conditions are satisfied:

$$(7.2) \quad 1 \longrightarrow \Gamma_{r+s-l}/\Gamma_{r+s} \longrightarrow \Gamma_r/\Gamma_{r+s} \longrightarrow \Gamma_r/\Gamma_{r+s-l} \longrightarrow 1$$

is central; and defining a map θ as above induces a morphism of extensions

$$\begin{array}{ccccccc} 1 & \longrightarrow & K & \longrightarrow & F[x, y] & \longrightarrow & \mathbb{Z} \oplus \mathbb{Z} \longrightarrow 1 \\ & & \downarrow \theta & & \downarrow \theta & & \downarrow \theta \\ 1 & \longrightarrow & \Gamma_{r+s-l}/\Gamma_{r+s} & \longrightarrow & \Gamma_r/\Gamma_{r+s} & \longrightarrow & \Gamma_r/\Gamma_{r+s-l} \longrightarrow 1. \end{array}$$

FIGURE 9

It is straightforward to determine when the former condition is satisfied.

Lemma 7.1. *For $r, s, l \geq 1$, extension (7.2) is central if and only if $r \geq l$.*

Proof. In the proof of Theorem 3.5 (which is included in Section 9), we show that $\Gamma(G_n(R), p^r)/\Gamma(G_n(R), p^{r+s})$ is generated by the images of the matrices $\{A_{ij,k,r}\}$ and that $\Gamma(G_n(R), p^{r+s-l})/\Gamma(G_n(R), p^{r+s})$ is generated by the images of the matrices $\{A_{ij,k,r+s-l}\}$. A straightforward calculation will verify that the following relation is satisfied, where $[g, h] = g^{-1}h^{-1}gh$ denotes the group commutator:

$$(7.3) \quad [A_{i_1 j_1, k_1, r+s-l}, A_{i_2 j_2, k_2, r}] = 1 + p^{2r+s-l} v_{k_1} v_{k_2} (e_{i_1 j_1} e_{i_2 j_2} - e_{i_2 j_2} e_{i_1 j_1}).$$

From this, we see that the commutator is trivial in Γ_r/Γ_{r+s} if and only if $2r+s-l \geq r+s$. \square

If $l = 1$ and $r \geq s-1$, one can check that extension (7.2) also satisfies the second condition mentioned above. Namely, defining a map $\theta : F[x, y] \longrightarrow \Gamma_r/\Gamma_{r+s}$ induces a morphism of extensions

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \longrightarrow & F[x, y] & \longrightarrow & \mathbb{Z} \oplus \mathbb{Z} & \longrightarrow & 1 \\ & & \downarrow \theta & & \downarrow \theta & & \downarrow \theta & & \\ 1 & \longrightarrow & \Gamma_{r+s-1}/\Gamma_{r+s} & \longrightarrow & \Gamma_r/\Gamma_{r+s} & \longrightarrow & \Gamma_r/\Gamma_{r+s-1} & \longrightarrow & 1. \end{array}$$

FIGURE 10

Let χ denote the generator of $H_2(\mathbb{Z} \oplus \mathbb{Z}; \mathbb{Z}) \cong \mathbb{Z}$. Working out the local coefficient system in the Lyndon-Hochschild-Serre spectral sequence for the extension

$$(7.4) \quad 1 \longrightarrow K \longrightarrow F[x, y] \longrightarrow \mathbb{Z} \oplus \mathbb{Z} \longrightarrow 1,$$

one can check that $H_0(\mathbb{Z} \oplus \mathbb{Z}; H_1(K)) \cong \mathbb{Z}$. Furthermore, this group is generated by the class of the element $[x, y] \in K$. Since it is known that $H_2(F[x, y]; \mathbb{Z}) = 0$, it must be the case that the differential $d_{2,0}^2$ is an isomorphism. In other words, $d_{2,0}^2(\chi) = [x, y]$.

The induced map θ_* on homology induces a map of spectral sequences associated to the two extensions in Figure 10. Using naturality and the fact that $d_{2,0}^2(\chi) = [x, y]$, we can write

$$(7.5) \quad d_{2,0}^2(\theta_*(\chi)) = \theta_*(d_{2,0}^2(\chi)) = \theta_*([x, y]) = [\theta_*(x), \theta_*(y)].$$

Thus, we have demonstrated the following formula.

Theorem 7.2. *Suppose $r, s \geq 1$, $r \geq s-1$, and a map $\theta : F[x, y] \longrightarrow \Gamma_r/\Gamma_{r+s}$ is given. Then θ induces a morphism of extensions as in Figure 10, and*

$$(7.6) \quad d_{2,0}^2(\theta_*(\chi)) = [\theta_*(x), \theta_*(y)]$$

in the LHS spectral sequence for the extension

$$(7.7) \quad 1 \longrightarrow \Gamma_{r+s-1}/\Gamma_{r+s} \longrightarrow \Gamma_r/\Gamma_{r+s} \longrightarrow \Gamma_r/\Gamma_{r+s-1} \longrightarrow 1.$$

Here, χ denotes the generator of $H_2(\mathbb{Z} \oplus \mathbb{Z}; \mathbb{Z}) \cong \mathbb{Z}$.

Notice that $[\theta_*(x), \theta_*(y)]$ can be calculated using the Lie algebra structure for $\text{gr}_*(\Gamma(G_n(R), p))$ given in Theorem 4.7. This will allow us to compute $d_{2,0}^2$ for many examples involving central extensions of congruence subgroups. This will be discussed in more detail in a sequel.

Remark. The reader should notice that the formula for the differential $d_{2,0}^2$ in Theorem 7.2 provides information that is dual, in a sense, to the extension class characterizing extension (7.7).

8. PROOF OF THEOREM 3.2

We adapt the method of the proof of Theorem 3.1 as found in [11]. Suppose that $X \in \Gamma(G_n(R), p^r)$. We can write $X = 1 + p^r A$ where 1 denotes the $n \times n$ identity matrix and $A \in \text{Mat}_n(R)$. Define the map

$$(8.1) \quad \varphi_r : \Gamma(G_n(R), p^r) \longrightarrow \mathfrak{sl}_n(\mathbb{F}_p[V])$$

by

$$(8.2) \quad \varphi_r(X) = A \pmod{p}.$$

To show that the image of φ_r lies in $\mathfrak{sl}_n(\mathbb{F}_p[V])$, we make use of the fact that $\Gamma(G_n(R), p^r) \subseteq SL_n(R)$. Thus,

$$\begin{aligned} 1 &= \det(X) \\ &= \det(1 + p^r A) \\ &\equiv (1 + p^r \text{tr}(A)) \pmod{p^{r+1}}, \end{aligned}$$

where $\text{tr}(A)$ denotes the trace of A . Thus, it must be the case that $\text{tr}(A) \equiv 0 \pmod{p}$.

One can check that φ_r is a homomorphism directly:

$$\begin{aligned} \varphi_r((1 + p^r A)(1 + p^r B)) &= \varphi_r(1 + p^r(A + B + p^r AB)) \\ &= (A + B + p^r AB) \pmod{p} \\ &\equiv (A + B) \pmod{p} \\ &= \varphi_r(1 + p^r A) + \varphi_r(1 + p^r B). \end{aligned}$$

To show that φ_r is surjective, we define a basis for $\mathfrak{sl}_n(\mathbb{F}_p[V])$ and show that φ_r surjects onto this basis. In the proof of Corollary 3.3, we defined e_{ij} to be the $n \times n$ matrix with a 1 in the (i, j) position and zeros elsewhere. A quick check will verify that a basis for $\mathfrak{sl}_n(\mathbb{F}_p[V])$ is given by $\{v_k e_{ij}\}_{i \neq j} \cup \{v_k(e_{ii} - e_{nn})\}_{i=1}^{n-1}$ for $k \in I$. Further,

$$(8.3) \quad \varphi_r(1 + p^r v_k e_{ij}) = v_k e_{ij}$$

and

$$(8.4) \quad \varphi_r(1 + p^r v_k(e_{ii} + e_{in} - e_{ni} - e_{nn})) = v_k(e_{ii} + e_{in} - e_{ni} - e_{nn}),$$

so that φ_r hits all of the basis elements in $\mathfrak{sl}_n(\mathbb{F}_p[V])$.

Finally, notice that if $X \in \Gamma(G_n(R), p^{r+1})$, we can write $X = 1 + p^{r+1} A = 1 + p^r(pA)$ for some $A \in \text{Mat}_n(R)$. So $\varphi_r(X) = 0$. Conversely, if $\varphi_r(1 + p^r A) = 0$, it must be the case that $A = pB$ for some $B \in \text{Mat}_n(R)$. Thus, $1 + p^r A = 1 + p^{r+1} B \in \Gamma(G_n(R), p^{r+1})$. So $\ker(\varphi_r) = \Gamma(G_n(R), p^{r+1})$. This completes the proof of the theorem.

9. PROOF OF THEOREM 3.5

The proof is by induction on s . The case $s = 1$ is Lemma 3.7. Suppose that $s - 1$ and smaller cases have been proved and that $|V| < \infty$. Consider the group extension

$$(9.1) \quad 1 \longrightarrow \Gamma_{r+s-1}/\Gamma_{r+s} \longrightarrow \Gamma_r/\Gamma_{r+s} \longrightarrow \Gamma_r/\Gamma_{r+s-1} \longrightarrow 1,$$

where we again use the convention $\Gamma_l = \Gamma(G_n(R), p^l)$. By Lemma 3.7,

$$(9.2) \quad \Gamma_{r+s-1}/\Gamma_{r+s} \cong \bigoplus_{n^2-1} \mathbb{Z}/p\mathbb{Z}[V],$$

so that $|\Gamma_{r+s-1}/\Gamma_{r+s}| = p^{(n^2-1)\cdot|V|}$. By induction,

$$(9.3) \quad \Gamma_r/\Gamma_{r+s-1} \cong \bigoplus_{n^2-1} \mathbb{Z}/p^{s-1}\mathbb{Z}[V],$$

so that $|\Gamma_r/\Gamma_{r+s-1}| = p^{(s-1)\cdot(n^2-1)\cdot|V|}$. It follows that $|\Gamma_r/\Gamma_{r+s}| = p^{(n^2-1)\cdot|V|} \cdot p^{(s-1)\cdot(n^2-1)\cdot|V|} = p^{s\cdot(n^2-1)\cdot|V|}$.

Any element of $\bigoplus_{n^2-1} \mathbb{Z}/p^s\mathbb{Z}[V]$ can be written as

$$(9.4) \quad (a_{11}, a_{12}, \dots, a_{1n}, a_{21}, \dots, a_{2n}, \dots, a_{n1}, \dots, a_{n,n-1}),$$

where $a_{ij} \in \mathbb{Z}/p^s\mathbb{Z}[V]$. Let $\delta_{ij} \in \bigoplus_{n^2-1} \mathbb{Z}/p^s\mathbb{Z}[V]$ be the element with a 1 in the (i, j) position and zeros elsewhere. Then $\{v_k\delta_{ij}\}$ for $1 \leq i, j \leq n$, $i + j < 2n$, and $V = \{v_k\}_{k \in I}$ is a basis for $\bigoplus_{n^2-1} \mathbb{Z}/p^s\mathbb{Z}[V]$. Consider the map

$$(9.5) \quad \Phi_{r,s} : \bigoplus_{n^2-1} \mathbb{Z}/p^s\mathbb{Z}[V] \longrightarrow \Gamma_r/\Gamma_{r+s}$$

that sends $v_k\delta_{ij} \mapsto \overline{A_{ij,k,r}}$, where $\overline{A_{ij,k,r}}$ represents the equivalence class of $A_{ij,k,r}$ in Γ_r/Γ_{r+s} , and the family $\{A_{ij,k,r}\}$ are the generators of Γ_r/Γ_{r+1} as defined in Corollary 3.8.

Claim. The group Γ_r/Γ_{r+s} is generated by the equivalence classes $\{\overline{A_{ij,k,r}}\}$ for $1 \leq i, j \leq n$, $i + j < 2n$, and $k \in I$.

Proof of Claim. We again proceed by induction on s . The case $s = 1$ is clear. Suppose that $s - 1$ and smaller cases are satisfied. By induction, Γ_r/Γ_{r+s-1} is generated by the equivalence classes of the matrices $\{A_{ij,k,r}\}$. According to Corollary 3.8, $\Gamma_{r+s-1}/\Gamma_{r+s}$ is generated by the matrices $\{A_{ij,k,r+s-1}\}$. But for each i, j , and k ,

$$(9.6) \quad A_{ij,k,r+s-1} = (\psi_{r+s-2}^p \circ \psi_{r+s-3}^p \circ \dots \circ \psi_{r+1}^p \circ \psi_r^p)(A_{ij,k,r}) = A_{ij,k,r}^{p^{s-1}}.$$

Thus, Γ_r/Γ_{r+s} is generated by the equivalence classes of the matrices $\{A_{ij,k,r}\}$, which completes the proof of the claim.

Once we have this, the reader can check that since $r \geq s \geq 2$, the generators of Γ_r/Γ_{r+s} commute, so that Γ_r/Γ_{r+s} is abelian. So $\Phi_{r,s}$ is a homomorphism of abelian groups, which is clearly surjective since Γ_r/Γ_{r+s} is generated by the equivalence classes of the matrices $\{A_{ij,k,r}\}$.

Finally, since $|\bigoplus_{n^2-1} \mathbb{Z}/p^s\mathbb{Z}[V]| = p^{s\cdot(n^2-1)\cdot|V|} = |\Gamma_r/\Gamma_{r+s}|$, it must also be the case that $\Phi_{r,s}$ is injective, making it an isomorphism. This completes the proof of Theorem 3.5.

10. PROOF OF THEOREM 2.4

Recall the map

$$(10.1) \quad \varphi_r : \Gamma(G_n(R), p^r) \longrightarrow \mathfrak{sl}_n(\mathbb{F}_p[V])$$

defined in Section 8. This induces a well-defined map on the filtration quotients

$$(10.2) \quad \overline{\varphi}_r : \Gamma(G_n(R), p^r)/\Gamma(G_n(R), p^{r+1}) \longrightarrow \mathfrak{sl}_n(\mathbb{F}_p[V]).$$

In fact, since φ_r is an epimorphism with kernel $\Gamma(G_n(R), p^{r+1})$ (as shown in Section 8), $\bar{\varphi}_r$ is an isomorphism.

Recall that I denotes the kernel of the evaluation map $\mathbb{F}_p[t] \xrightarrow{t=0} \mathbb{F}_p$. Define a map

$$(10.3) \quad \bar{\varphi}_r \otimes t^r : \Gamma(G_n(R), p^r)/\Gamma(G_n(R), p^{r+1}) \longrightarrow \mathfrak{sl}_n(\mathbb{F}_p[V]) \otimes_{\mathbb{F}_p} I$$

by

$$(10.4) \quad (\bar{\varphi}_r \otimes t^r)(X_r) = \bar{\varphi}_r(X_r) \otimes t^r$$

for $X_r \in \Gamma(G_n(R), p^r)/\Gamma(G_n(R), p^{r+1})$. We can assemble these maps for $r \geq 1$ to obtain a map

$$(10.5) \quad \varphi : \text{gr}_*(\Gamma(G_n(R), p)) \longrightarrow \mathfrak{sl}_n(\mathbb{F}_p[V]) \otimes_{\mathbb{F}_p} I$$

given by

$$(10.6) \quad \varphi(X) = \sum_{r \geq 1} (\bar{\varphi}_r \otimes t^r)(X_r).$$

Here, we have made use of the fact that

$$(10.7) \quad \text{gr}_*(\Gamma(G_n(R), p)) = \bigoplus_{r \geq 1} \Gamma(G_n(R), p^r)/\Gamma(G_n(R), p^{r+1})$$

and written $X = (X_1, X_2, \dots)$, where $X_r \in \Gamma(G_n(R), p^r)/\Gamma(G_n(R), p^{r+1})$. We claim that φ is the required Lie algebra isomorphism.

We first verify that φ is a homomorphism. Suppose $X, Y \in \text{gr}_*(\Gamma(G_n(R), p))$. Write $X = (X_1, X_2, \dots)$ and $Y = (Y_1, Y_2, \dots)$, where

$$(10.8) \quad X_r, Y_r \in \Gamma(G_n(R), p^r)/\Gamma(G_n(R), p^{r+1})$$

for $r \geq 1$. Since each $\bar{\varphi}_r$ is a homomorphism, we have the following:

$$\begin{aligned} \varphi(X + Y) &= \sum_{r \geq 1} (\bar{\varphi}_r \otimes t^r)(X_r Y_r) \\ &= \sum_{r \geq 1} (\bar{\varphi}_r(X_r Y_r) \otimes t^r) \\ &= \sum_{r \geq 1} ([\bar{\varphi}_r(X_r) + \bar{\varphi}_r(Y_r)] \otimes t^r) \\ &= \sum_{r \geq 1} ([\bar{\varphi}_r(X_r) \otimes t^r] + [\bar{\varphi}_r(Y_r) \otimes t^r]) \\ &= \sum_{r \geq 1} (\bar{\varphi}_r(X_r) \otimes t^r) + \sum_{r \geq 1} (\bar{\varphi}_r(Y_r) \otimes t^r) \\ &= \sum_{r \geq 1} (\bar{\varphi}_r \otimes t^r)(X_r) + \sum_{r \geq 1} (\bar{\varphi}_r \otimes t^r)(Y_r) \\ &= \varphi(X) + \varphi(Y). \end{aligned}$$

Thus, φ is a homomorphism.

To check that φ is surjective, we define a basis for $\mathfrak{sl}_n(\mathbb{F}_p[V]) \otimes_{\mathbb{F}_p} I$ and show that φ surjects onto this basis. In Section 8, we defined a basis for $\mathfrak{sl}_n(\mathbb{F}_p[V])$ to be $\{v_k e_{ij}\}_{i \neq j} \cup \{v_k(e_{ii} - e_{nn})\}_{i=1}^{n-1}$ for $k \in I$. The reader can check that $\{v_k e_{ij} \otimes t^r\}$

$t^r\}_{i \neq j} \cup \{v_k(e_{ii} - e_{nn}) \otimes t^r\}_{i=1}^{n-1}$ for $k \in I$ and $r \geq 1$ is a basis for $\mathfrak{sl}_n(\mathbb{F}_p[V]) \otimes_{\mathbb{F}_p} I$. It is clear that

$$(10.9) \quad \varphi(1 + p^r v_k e_{ij}) = v_k e_{ij} \otimes t^r.$$

Furthermore,

$$(10.10) \quad \varphi(1 + p^r v_k(e_{ii} + e_{in} - e_{ni} - e_{nn})) = v_k(e_{ii} + e_{in} - e_{ni} - e_{nn}) \otimes t^r,$$

so that φ hits all the basis elements in $\mathfrak{sl}_n(\mathbb{F}_p[V]) \otimes_{\mathbb{F}_p} I$.

Since $\bar{\varphi}_r$ is injective for all $r \geq 1$ (an isomorphism, in fact), it follows that φ is injective.

Finally, we need to show that φ preserves the Lie bracket. Since $[X, Y] \in \text{gr}_*(\Gamma(G_n(R), p))$, we can write

$$(10.11) \quad [X, Y] = ([X, Y]_1, [X, Y]_2, \dots),$$

where $[X, Y]_r \in \Gamma(G_n(R), p^r)/\Gamma(G_n(R), p^{r+1})$. Also, since

$$(10.12) \quad X_r, Y_r \in \Gamma(G_n(R), p^r)/\Gamma(G_n(R), p^{r+1}),$$

there exist $\hat{X}_r, \hat{Y}_r \in \text{Mat}_n(R)$ such that $X_r = 1 + p^r \hat{X}_r$ and $Y_r = 1 + p^r \hat{Y}_r$. We have the following:

$$\begin{aligned} \varphi([X, Y]) &= \sum_{r \geq 1} (\bar{\varphi}_r \otimes t^r)([X, Y]_r) \\ &= \sum_{r \geq 1} (\bar{\varphi}_r([X, Y]_r) \otimes t^r) \\ &= \sum_{r \geq 1} (\bar{\varphi}_r(\sum_{i+j=r} [X_i, Y_j]) \otimes t^r) \\ &= \sum_{r \geq 1} (\bar{\varphi}_r(\sum_{i+j=r} [1 + p^i \hat{X}_i, 1 + p^j \hat{Y}_j]) \otimes t^r) \\ &= \sum_{r \geq 1} (\sum_{i+j=r} \bar{\varphi}_r([1 + p^i \hat{X}_i, 1 + p^j \hat{Y}_j]) \otimes t^r) \\ &= \sum_{r \geq 1} (\sum_{i+j=r} ((\hat{X}_i \hat{Y}_j - \hat{Y}_j \hat{X}_i) \pmod{p}) \otimes t^r) \\ &= [\varphi(X), \varphi(Y)]. \end{aligned}$$

Thus,

$$(10.13) \quad \text{gr}_*(\Gamma(G_n(R), p)) \cong \mathfrak{sl}_n(\mathbb{F}_p[V]) \otimes_{\mathbb{F}_p} I$$

as Lie algebras. This completes the proof of the theorem.

Other Acknowledgments. The author would like to thank Paul Taylor for making his *diagram* package available, which was used to produce several of the diagrams in this paper.

REFERENCES

- [1] H. Bass, J. Milnor, J.-P. Serre, *Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$)*, Publ. IHES **33** (1969), 421–499.
- [2] S. Bigelow, *Braid groups are linear*, J. Amer. Math. Soc. **14** (2001), 471–486.
- [3] S. Bigelow, *The Burau representation is not faithful for $n = 5$* , Geom. Topol. **3** (1999), 397–404.

- [4] F. Cohen, M. Condor, J. Lopez, and S. Prassidis, *Remarks concerning Lubotzky's filtration*, Pure and Applied Mathematics Quarterly, **8** (1), pp. 79-106. [Available at arXiv:0710.3515]
- [5] D. Cooper and D.D. Long, *On the Burau representation modulo a small prime*, Geom. Topol. Monogr. **1** (1998), 127–138.
- [6] D. Cooper and D.D. Long, *A presentation for the image of Burau(4) $\otimes \mathbb{Z}_2$* , Inventiones Math. **127** (1997), 535–570.
- [7] M. du Sautoy, J.D. Dixon, et al., *Analytic pro- p groups*, Second Edition, New York: Cambridge University Press, 1999.
- [8] K. Knudson, *Congruence subgroups and twisted cohomology of $SL(n, \mathbb{F}[t])$* , J. Algebra **207** (1998), 695–721.
- [9] K. Knudson, *The homology of $SL(2, \mathbb{F}[t, t^{-1}])$* , J. Algebra **180** (1996), 87–101.
- [10] K. Knudson, *Homology and finiteness properties for $SL(2, \mathbb{Z}[t, t^{-1}])$* , Algebr. Geom. Topol., to appear.
- [11] K. Knudson, *Homology of linear groups*, Progress in mathematics Vol. 193; Basel, Boston, Berlin: Birkhäuser, 2001.
- [12] K. Knudson, *Unstable homotopy invariance and the homology of $SL(2, \mathbb{Z}[t])$* , J. Pure Appl. Algebra **148** (2000), 255–266.
- [13] D. Krammer, *Braid groups are linear*, Ann. of Math. **155** (2002), 131–156.
- [14] R. Lee and R. Szczarba, *On the homology and cohomology of congruence subgroups*, Invent. math. **33** (1976), 15-53.
- [15] J. Lopez, *Lie algebras associated to congruence subgroups*, Ph.D. Thesis, University of Rochester, 2010.
- [16] A. Lubotzky, *A group theoretic characterization of linear groups*, J. Algebra **113** (1988), 207–214.
- [17] J.P. Serre, *Lie algebras and Lie groups*, 1964 lectures given at Harvard University, Second Edition, New York: Springer-Verlag, 1992.
- [18] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, **11**, Princeton: Princeton University Press, 1971.
- [19] J. Stallings, *On torsion-free groups with infinitely many ends*, Annals of Mathematics **88** (1968), 312-334.
- [20] R. Swan, *Groups of cohomological dimension one*, Journal of Algebra **12** (1969), 585-610.

DEPARTMENT OF MATHEMATICS, NIAGARA UNIVERSITY, NIAGARA UNIVERSITY, NY 14109
E-mail address: jlopez@niagara.edu