FAITHFUL REPRESENTATIONS OF CHEVALLEY GROUPS OVER QUOTIENT RINGS OF NON-ARCHIMEDEAN LOCAL FIELDS

MOHAMMAD BARDESTANI, CAMELIA KARIMIANPOUR, KEIVAN MALLAHI-KARAI, AND HADI SALMASIAN

Abstract. Let F be a non-Archimedean local field with the ring of integers $\mathcal{O}$ and the prime ideal $\mathfrak{p}$ and let $G = \mathbf{G}_{ad}(\mathcal{O}/\mathfrak{p}^n)$ be the adjoint Chevalley group. Let $m_{\mathfrak{f}}(G)$ denote the smallest possible dimension of a faithful representation of G. Using the Stone-von Neumann theorem, we determine a lower bound for $m_{\mathfrak{f}}(G)$ which is asymptotically the same as the results of Landazuri, Seitz and Zalesskii for split Chevalley groups over $\mathbb{F}_q$. Our result yields a conceptual explanation of the exponents that appear in the aforementioned results

1. Introduction

For a finite group G, let $\mathrm{Rep}_{\mathfrak{f}}(G)$ denote the set of all finite dimensional faithful representations of G over complex vector spaces, and set

$$m_{\mathfrak{f}}(G) := \min\{d_\rho \,:\, \rho \in \mathrm{Rep}_{\mathfrak{f}}(G)\},$$

where d_ρ denotes the dimension (also called the degree) of ρ. Lower bounds on $m_{\mathfrak{f}}(G)$ can be found in group theory literature as old as the work of Frobenius [9]. Indeed, by constructing the character table of $\mathrm{PSL}_2(\mathbb{F}_p)$, Frobenius showed that

$$m_{\mathfrak{f}}\left(\mathrm{PSL}_2(\mathbb{F}_p)\right) \geq \frac{p-1}{2} \text{ for every prime } p \geq 5.$$

Apart from its intrinsic interest, the Frobenius bound has applications in many questions in number theory and additive combinatorics. To name a few, Sarnak and Xue [22] were the first to use this bound to obtain a lower bound for the smallest non-trivial eigenvalue of the Laplace-Beltrami operator on the hyperbolic space. This idea was subsequently used by Bourgain and Gamburd [4] to answer the 1-2-3 question of Lubotzky on the uniform expansion bounds for the Cayley graphs of $\mathrm{SL}_2\left(\mathbb{F}_p\right)$.

The Frobenius bound has been generalized by Landazuri, Seitz and Zalesskii [14, 23] to other families of finite simple groups of Lie type. These bounds play an essential role in the theory of expander graphs and approximate groups [5, 16]. Some of the finite simple groups of Lie type are canonically obtained by reduction mod $\mathfrak{p}$ of the group $\mathbf{G}(\mathcal{O})$ of $\mathcal{O}$-points of a Chevalley group, where $\mathcal{O}$ is the ring of integers of a local field. However, despite interesting applications (see below), little work has been done to extend the aforementioned bounds to reduction mod $\mathfrak{p}^n$ of $\mathbf{G}(\mathcal{O})$. Bourgain and Gamburd [3] considered this problem for $\mathrm{SL}_2\left(\mathbb{Z}/p^n\mathbb{Z}\right)$ in order to show that, for any sufficiently large prime p and any symmetric set S generating a Zariski-dense subgroup of $\mathrm{SL}_2(\mathbb{Z})$, the family of Cayley graphs $\left\{\mathrm{Cay}\left(\mathrm{SL}_2\left(\mathbb{Z}/p^n\mathbb{Z}\right), \pi_{p^n}(S)\right)\right\}_{n\geq 1}$ is an expander family (here π_{p^n} is the reduction map modulo p^n). Indeed, they proved

$$m_{\mathfrak{f}}\left(\mathrm{SL}_2\left(\mathbb{Z}/p^n\mathbb{Z}\right)\right) \geq \frac{p^{n-2}(p^2-1)}{2} \quad \text{for } n \geq 2.$$

Motivated by the works of Bourgain and Gamburd mentioned above, the first and third authors of this paper studied $m_{\mathfrak{f}}\left(\mathrm{SL}_k\left(\mathbb{Z}/p^n\mathbb{Z}\right)\right)$ and $m_{\mathfrak{f}}\left(\mathrm{Sp}_{2k}\left(\mathbb{Z}/p^n\mathbb{Z}\right)\right)$ [1]. The same problem for $m_{\mathfrak{f}}\left(\mathrm{SL}_k\left(\mathbb{Z}/p^n\mathbb{Z}\right)\right)$ has been considered by de Saxcé [8].

Let F be a non-Archimedean local field with the ring of integers $\mathcal{O}$ and the prime ideal $\mathfrak{p}$. The order of residue field $\mathcal{O}/\mathfrak{p}$ is denoted by $q = p^l$ where p is a prime number. Our aim in this paper is to obtain a bound for the minimal dimension of all faithful complex representations of adjoint Chevalley groups over

1991 *Mathematics Subject Classification.* Primary 20C33; Secondary 20G35.

Key words and phrases. Chevalley groups; faithful representation; Heisenberg subgroups; Local fields; Stone-von Neumann theorem.

the ring $\mathcal{O}/\mathfrak{p}^n$ where n is a positive integer. Indeed for the Chevalley group $\mathbf{G}_{ad}(\mathcal{O}/\mathfrak{p}^n)$ associated to a simple Lie algebra $\mathfrak{g}$ we will obtain the following bound

$$m_{\mathrm{f}}(\mathbf{G}_{ad}(\mathcal{O}/\mathfrak{p}^n)) \geq Cq^{\frac{n(r+1)}{2}}, \tag{1}$$

where r is the dimension of the nilpotent radical of the Heisenberg parabolic subalgebra of $\mathfrak{g}$, and $C > 0$ is an absolute constant (independent of q and r).

We remark that all adjoint Chevalley groups over $\mathcal{O}/\mathfrak{p}$ (except for a few cases) are simple groups, and so all of their non-trivial representations are faithful. Therefore, our Theorem 1 below for $n = 1$ yields lower bounds for non-trivial representations of $\mathbf{G}_{ad}(\mathbb{F}_q)$, which, are asymptotically the same as the results of [14, 23] for split Chevalley groups over $\mathbb{F}_q$. By being asymptotically the same we mean that the exponents that appear in (1) are the same as those in the work Landazuri, Seitz and Zalesskii. For a corrigendum to [14] the cases $\mathsf{F}_4(q)$, q odd, and ${}^2\mathsf{E}_6(q)$, we refer the reader to [23].

Let us briefly sketch the idea of this paper. For a given simple Lie algebra $\mathfrak{g}$, following Gross and Wallach's idea [10], we consider its Heisenberg parabolic subalgebra whose nilpotent radical is a two step nilpotent subalgeba. This nilpotent subalgebra gives rise to a two step nilpotent subgroup of the adjoint Chevalley group associated to $\mathfrak{g}$ (this is the general $(2n+1)$-dimensional Heisenberg group for some n). The irreducible representations of a Heisenberg group are classified by their central characters via the Stone-von Neumann theorem. Given a faithful representation ρ of $\mathbf{G}_{ad}(\mathcal{O}/\mathfrak{p}^n)$, we consider its restriction to the aforementioned Heisenberg subgroup and we find the polarizing subgroup of the generic character of the center. Our bound then is obtained by orbit counting of the action of a certain subgroup on an irreducible component of the representation ρ. Our main theorem is the following:

Theorem 1. *Let F be a non-Archimedean local field with the ring of integers $\mathcal{O}$, prime ideal $\mathfrak{p}$, and residue field $\mathcal{O}/\mathfrak{p} \cong \mathbb{F}_q$, where $q = p^l$ for a prime number p. Let $\mathfrak{g}$ be a finite dimensional complex simple Lie algebra with root system Φ. Let*

$$\mathbf{G}_{ad}\left(\mathcal{O}/\mathfrak{p}^n\right) := \mathbf{G}_{ad}\left(\mathcal{O}/\mathfrak{p}^n, \Phi\right),$$

be the adjoint Chevalley group associated to $\mathfrak{g}$. Then $m_{\mathrm{f}}\left(\mathbf{G}_{ad}\left(\mathcal{O}/\mathfrak{p}^n\right)\right) \geq h_{\mathrm{f}}(\Phi, q, n)$, where $h_{\mathrm{f}}(\Phi, q, n)$ is given in the following table

Φ		$h_{\mathrm{f}}(\Phi, q, n)$
A_1	$p \geq 3$	$\frac{1}{2}\left(q^n - q^{n-1}\right)$
A_m	$m \geq 2,\ p \geq 3$	$\left(q^n - q^{n-1}\right) q^{(m-1)n}$
B_m	$m \geq 3,\ p \geq 3$	$\left(q^n - q^{n-1}\right) q^{(2m-3)n}$
C_m	$m \geq 2,\ p \geq 3$	$\frac{1}{2}\left(q^n - q^{n-1}\right) q^{(m-1)n}$
D_m	$m \geq 4,\ p \geq 3$	$\left(q^n - q^{n-1}\right) q^{(2m-4)n}$
G_2	$p \geq 5$	$\left(q^n - q^{n-1}\right) q^{2n}$
F_4	$p \geq 3$	$\left(q^n - q^{n-1}\right) q^{7n}$
E_6	$p \geq 3$	$\left(q^n - q^{n-1}\right) q^{10n}$
E_7	$p \geq 3$	$\left(q^n - q^{n-1}\right) q^{16n}$
E_8	$p \geq 3$	$\left(q^n - q^{n-1}\right) q^{28n}$

Unfortunately our proof of this theorem fails when $\mathrm{char}(\mathcal{O}/\mathfrak{p}) = 2$. We refer the reader to Remark 4, for further details.

Remark 1. Ree [20] (see also [7, Theorem 11.3.2]) proved that the groups $\mathbf{G}_{ad}(\mathbb{F}_q)$ are indeed what one would expect to obtain, namely, $\mathrm{PSL}_m(\mathbb{F}_q)$ if $\mathfrak{g}$ is of type A_{m-1}; $\mathrm{PSp}_{2m}(\mathbb{F}_q)$ if $\mathfrak{g}$ is of type C_m; $\mathrm{P}\Omega_{2m}(\mathbb{F}_q)$ if $\mathfrak{g}$ is of type D_m and $\mathrm{P}\Omega_{2m+1}(\mathbb{F}_q)$ if $\mathfrak{g}$ is of type B_m and $q \geq 3$. Moreover Chevalley proved that the group $\mathbf{G}_{ad}(\mathbb{F}_q)$ is simple except for $\mathsf{A}_1(2)$, $\mathsf{A}_1(3)$, $\mathsf{B}_2(2)$ and $\mathsf{G}_2(2)$ (see [7, Theorem 11.1.2]).

Remark 2. The above theorem is also valid for *simply connected* Chevalley groups with a similar proof. The sharpness of Landazuri–Seitz bounds (corresponding to the case $n = 1$) has been the source of several

investigations [11, 15, 27]. It would be interesting to consider sharpness of our bounds. For type A_ℓ, the permutation representation of $\mathrm{PSL}_{\ell+1}(\mathcal{O}/\mathfrak{p}^n)$ on the projection space $\mathbb{P}^\ell_{\mathcal{O}/\mathfrak{p}^n}$ is faithful of dimension $O(q^{\ell n})$, which is consistent with our lower bound. However, we do not know about sharpness of our bounds in general for other groups.

Remark 3. Let us point out that the idea of restriction to nilpotent subgroups was also used in [14]. Nevertheless, the arguments in [14] are long and case by case. One of our main goals in writing this paper is to give a uniform argument based on the idea of Heisenberg parabolic subalgebras to obtain lower bounds which, in the special case of $\mathcal{O}/\mathfrak{p}$, are asymptotically the same as those given in [14]. (See the discussion after (1) for a precise meaning.) Such bounds are enough for the existing applications. Another important technical detail that has been worked out in our paper is to verify that many facts about Chevalley groups over fields remain valid for Chevalley groups over rings of our interest (see Section 4).

2. Notations and preliminaries

In this section we set some notation which will be used throughout this paper. We also recall some basic facts about local fields that can be found in [19, 24].

If X is any set, f any function on X, and $Y \subseteq X$ any subset, then $f|_Y$ is the restriction of f to Y. $|X|$ is the cardinality of a finite set X. We will use the shorthand $\mathbf{e}(x) := \exp(2\pi i x)$. For a given group G, its identity element is denoted by $\mathbf{1}$. Moreover $\mathrm{char}(F)$ is the characteristic of a given field.

By the well-known classification of local fields, any non-Archimedean local field is isomorphic to a finite extension of $\mathbb{Q}_p$ (p is a prime number) or is isomorphic to the field of formal Laurent series $\mathbb{F}_q((T))$ over a finite field with $q = p^l$ elements. For a non-Archimedean local field F with the discrete valuation ν, we will denote its ring of integers and its unique prime ideal by $\mathcal{O}$ and $\mathfrak{p}$, respectively. We will also fix a uniformizer $\varpi \in \mathfrak{p}$. For any integer $m \in \mathbb{Z}$, we write

$$\mathfrak{p}^m := \{x \in F : \nu(x) \geq m\}.$$

Then $\mathfrak{p}^m/\mathfrak{p}^{m+n} \cong \mathcal{O}/\mathfrak{p}^n$ as additive groups, for every $m, n \in \mathbb{Z}$ with $n > 0$. Let n be a positive integer. Our goal in this section is to describe all additive characters of the finite local rings $\mathcal{O}/\mathfrak{p}^n$ using the ring structure.

From now on, if $\mathrm{char}(F) = 0$ we set $E = \mathbb{Q}_p$ and if $\mathrm{char}(F) = p > 0$ we set $E = F$. Now we define

$$\mathrm{Tr} := \mathrm{Tr}_{F/E} : F \to E,$$

the trace map of F over E. The *Dedekind's complementary module*, (or *inverse different*) is defined by

$$\mathcal{O}^* := \{x \in F : \nu(\mathrm{Tr}(sx)) \geq 0 \text{ for all } s \in \mathcal{O}\}.$$

One can show that $\mathcal{O}^*$ is a fractional ideal of F and hence for some $\ell \geq 0$ we have $\mathcal{O}^* = \varpi_F^{-\ell}\mathcal{O} = \mathfrak{p}^{-\ell}$. Throughout this paper ℓ designates this exponent. Note that $\ell = 0$ when $\mathrm{char}(F) > 0$.

We will now construct additive characters $\psi : E \to \mathbb{C}^*$, where E is as above. Let us first consider the zero characteristic case. For every $x \in \mathbb{Q}_p$, let n_x be the smallest non-negative integer such that $p^{n_x}x \in \mathbb{Z}_p$. Let $r_x \in \mathbb{Z}$ be such that $r_x \equiv p^{n_x}x \pmod{p^{n_x}}$. It is easy to see that the following map (known as the Tate character)

$$\psi : \mathbb{Q}_p \to \mathbb{C}^*, \qquad x \mapsto \mathbf{e}(r_x/p^{n_x}), \tag{2}$$

is a non-trivial additive character of $\mathbb{Q}_p$ with the kernel $\mathbb{Z}_p$.

Similarly for $\mathbb{F}_q((T))$, we have $\mathcal{O} = \mathbb{F}_q[[T]]$ and $\varpi = T$. We now set

$$\psi : \mathbb{F}_q((T)) \to \mathbb{C}^*, \qquad \sum_{i \geq N} a_i T^i \to \mathbf{e}\left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a_{-1})/p\right). \tag{3}$$

Notice that the trace map from $\mathbb{F}_q$ to $\mathbb{F}_p$ is surjective. Hence, $\psi|_{\mathcal{O}} = 1$ but $\psi|_{\mathfrak{p}^{-1}} \neq 1$ (sometimes we say that the conductor of ψ is $\mathcal{O} = \mathbb{F}_q[[T]]$).

Lemma 1. *Let F be a local field with the ring of integers $\mathcal{O}$ and prime ideal $\mathfrak{p}$. All additive characters of the ring $\mathcal{O}/\mathfrak{p}^n$ are given by*

$$\psi_{\bar{b}} : \mathcal{O}/\mathfrak{p}^n \to \mathbb{C}^*, \qquad x + \mathfrak{p}^n \mapsto \psi(\mathrm{Tr}(bx)),$$

where $\bar{b} = b + \mathfrak{p}^{-\ell} \in \mathfrak{p}^{-(n+\ell)}/\mathfrak{p}^{-\ell}$.

Proof. First assume that $\mathrm{char}(F) = 0$, that is, F is a p-adic field. Let $\bar{b}_1 = b_1 + \mathfrak{p}^{-\ell}$ and $\bar{b}_2 = b_2 + \mathfrak{p}^{-\ell}$ be distinct elements and assume that $\psi_{\bar{b}_1} = \psi_{\bar{b}_2}$. Then for all $x \in \mathcal{O}$ we have $\psi(\mathrm{Tr}((b_1 - b_2)x)) = 1$, which implies that $\mathrm{Tr}((b_1 - b_2)x) \in \mathbb{Z}_p$. Thus $b_1 - b_2 \in \mathfrak{p}^{-\ell}$, which is a contradiction. This construction provides exactly $|\mathfrak{p}^{-(n+\ell)}/\mathfrak{p}^{-\ell}|$ distinct additive characters. Since $|\mathcal{O}/\mathfrak{p}^n| = |\mathfrak{p}^{-(n+\ell)}/\mathfrak{p}^{-\ell}|$, we are done.

Next assume that $\mathrm{char}(F) > 0$. It is clear that the map $\psi_{\bar{b}}$ is well defined. Now suppose for some $b \in \mathfrak{p}^{-n}$ we have $\psi(bx) = 1$ for all $x \in \mathcal{O}$. Hence the fractional ideal $b\mathcal{O}$ is a subset of $\ker(\psi)$. Therefore $b \in \mathcal{O}$ since the conductor of ψ is $\mathcal{O}$. This construction provides exactly $|\mathfrak{p}^{-n}/\mathcal{O}|$ distinct additive characters. Since $|\mathcal{O}/\mathfrak{p}^n| = |\mathfrak{p}^{-n}/\mathcal{O}|$, we are done. □

3. The Stone-von Neumann theorem

In this section, we state a version of Stone-von Neumann theorem that suits our purposes in this paper. The Stone-von Neumann theorem holds in a broader setting [12, 17, 18]. However, we only present it in the finite group case, which is needed in this paper.

Let U be a finite two step nilpotent group, and let $Z(U)$ denote its center. If A is any subgroup of U containing $Z(U)$, we will denote $\bar{A} := A/Z(U)$. Let $\chi : Z(U) \to \mathbb{C}^*$ be a one-dimensional representation of $Z(U)$. We define a pairing

$$U/Z(U) \times U/Z(U) \to \mathbb{C}^* \ , \ \langle xZ(U), yZ(U)\rangle_\chi := \chi\left([x,y]\right).$$

We call χ a *generic character of* $Z(U)$ if the above pairing is non-degenerate, in the sense that for every $x \in U$, if $\langle xZ(U), yZ(U)\rangle_\chi = 1$ for every $y \in U$, then $x \in Z(U)$. Assuming χ is generic character of $Z(U)$, we say that a subgroup $Z(U) \leq A \leq U$ is *isotropic* if $\bar{A} \subseteq \bar{A}^\perp$, where

$$\bar{A}^\perp := \left\{ xZ(U) \ : \ \langle xZ(U), yZ(U)\rangle_\chi = 1 \text{ for all } y \in A \right\}.$$

We say that A is *polarizing* if $\bar{A} = \bar{A}^\perp$. For the next theorem we refer the reader to [6, §4.1].

Theorem 2 (Stone-von Neumann theorem)**.** *Let U be a finite two step nilpotent group, and let χ be a generic character of $Z(U)$. Then there exists a unique isomorphism class of irreducible representations of U with central character χ. Such a representation may be constructed as follows: Let A be any polarizing subgroup of U, and let $\tilde{\chi}$ be any extension of χ to A. Then the representation $\mathrm{Ind}_A^U(\tilde{\chi})$ is of this class.*

4. The Heisenberg parabolic subalgebra

This section is devoted to a rapid review of some basic facts in the theory of simple Lie algebras. We closely follow Gross and Wallach's paper [10], Sections 1 and 2 (see also [21, §3]). Let $\mathfrak{g}$ be a complex finite dimensional simple Lie algebra. Fix a Cartan subalgebra $\mathfrak{h}$ of $\mathfrak{g}$. Let $\Phi \subseteq \mathfrak{h}^*$ be the root system of $\mathfrak{g}$ with respect to $\mathfrak{h}$. Then, we have the Cartan decomposition

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{g}_\alpha, \tag{4}$$

where $\mathfrak{g}_\alpha = \{x \in \mathfrak{g} : [H, x] = \alpha(H)x, \forall H \in \mathfrak{h}\}$. Let $E = \mathrm{Span}_{\mathbb{R}}\{\alpha \,|\, \alpha \in \Phi\}$. Note that E is equipped with a symmetric positive definite inner product $(\ ,\ )$ obtained from the Killing form of $\mathfrak{g}$ via the isomorphism between $\mathfrak{h}$ and $\mathfrak{h}^*$. For $\alpha, \beta \in \Phi$, set $\langle \alpha, \beta\rangle = 2(\alpha, \beta)/(\beta, \beta)$. Let $\beta \neq \pm\alpha$ be two independent roots. Assume that $\|\beta\| \geq \|\alpha\|$. Then the values of $\langle \alpha, \beta\rangle$ and $\langle \beta, \alpha\rangle$ are given by Table 1 (see [13, Table 1, §9.4]).

$\langle\alpha,\beta\rangle$	$\langle\beta,\alpha\rangle$	$(\|\beta\|/\|\alpha\|)^2$
0	0	undetermined
1	1	1
−1	−1	1
1	2	2
−1	−2	2
1	3	3
−1	−3	3

Table 1: Root structure

Let Δ be a base of Φ. Let $\Phi^+ \subseteq \Phi$ the set of positive roots with respect to Δ, and let $\tilde{\beta}$ be the highest root. It is known that $\tilde{\beta}$ is a long root and $m_\alpha \geq n_\alpha$, where $\tilde{\beta} = \sum_{\alpha\in\Delta} m_\alpha\alpha$ and $\gamma = \sum_{\alpha\in\Delta} n_\alpha\alpha$ is any $\gamma \in \Phi$. Given the above notation, we define the *Heisenberg parabolic subalgebra* $\mathfrak{q} = \mathfrak{l} \oplus \mathfrak{u}$. The Levi subalgebra and the nilpotent radical of $\mathfrak{q}$ are:

$$\mathfrak{l} = \mathfrak{h} \oplus \bigoplus_{\substack{\alpha\in\Phi \\ \langle\alpha,\tilde{\beta}\rangle=0}} \mathfrak{g}_\alpha, \qquad \text{and} \qquad \mathfrak{u} = \bigoplus_{\substack{\alpha\in\Phi \\ \langle\alpha,\tilde{\beta}\rangle>0}} \mathfrak{g}_\alpha.$$

Lemma 2. *The inequality $\langle\alpha,\tilde{\beta}\rangle > 0$ implies that $\alpha \in \Phi^+$, and either $\alpha = \tilde{\beta}$ or $\langle\alpha,\tilde{\beta}\rangle = 1$. Moreover, if $\langle\alpha,\tilde{\beta}\rangle = 1$, then $\tilde{\beta} - \alpha \in \Phi^+$ and $\langle\tilde{\beta} - \alpha, \tilde{\beta}\rangle = 1$.*

Proof. If $\langle\alpha,\tilde{\beta}\rangle > 0$ then $\tilde{\beta} - \alpha \in \Phi$ (see [13, Lemma of §9.4]). This implication, along with the fact that $\tilde{\beta}$ is the highest root, implies $\alpha \in \Phi^+$.

Note that for any $\alpha \in \Phi^+$, $|\langle\alpha,\tilde{\beta}\rangle| \leq |\langle\tilde{\beta},\alpha\rangle|$. Assume $\alpha \neq \tilde{\beta}$. Then by applying Table 1 and a simple calculation we deduce that $\langle\alpha,\tilde{\beta}\rangle\langle\tilde{\beta},\alpha\rangle \in \{1,2,3\}$. Hence, $\langle\alpha,\tilde{\beta}\rangle > 0$ implies $\langle\alpha,\tilde{\beta}\rangle = 1$. The last claim in the statement follows from linearity of $\langle\ ,\ \rangle$ in the first component. □

Let $\Sigma^+ := \{\alpha \in \Phi^+ : \langle\alpha,\tilde{\beta}\rangle = 1\}$. Lemma 2 allows us to define a fixed-point free involution of Σ^+ defined by $\alpha \mapsto \tilde{\beta} - \alpha$. We pick one element from each equivalence class. Therefore, we have the following disjoint decomposition:

$$\Sigma^+ = \{\alpha_i : 1 \leq i \leq d\} \cup \{\tilde{\beta} - \alpha_i : 1 \leq i \leq d\}. \tag{5}$$

Hence, $|\Sigma^+| = 2d$, where the value of the integer d is explicitly calculated in Proposition 1.3 of [10]. In particular, Table 2 is given in [10]:

$\mathfrak{g}$		d
A_m	$m \geq 1$	$m-1$
B_m	$m \geq 2$	$2m-3$
C_m	$m \geq 2$	$m-1$
D_m	$m \geq 3$	$2m-4$
G_2		2
F_4		7
E_6		10
E_7		16
E_8		28

Table 2: Values of d

Lemma 3. *The subalgebra $\mathfrak{u}$ is a two-step nilpotent Lie algebra with center $\mathfrak{g}_{\tilde{\beta}}$.*

Proof. It follows from Lemma 2 that $[\mathfrak{u},\mathfrak{u}] \subseteq \mathfrak{g}_{\tilde{\beta}} \subseteq \mathrm{Z}(\mathfrak{u})$, which implies $\mathfrak{u}$ is a two-step nilpotent Lie algebra. For $\gamma_1, \gamma_2 \in \Sigma^+$, notice that $[\mathfrak{g}_{\gamma_1}, \mathfrak{g}_{\gamma_2}] = 0$ unless $\gamma_2 = \tilde{\beta} - \gamma_1$, and in this case we have $[\mathfrak{g}_{\gamma_1}, \mathfrak{g}_{\tilde{\beta}-\gamma_1}] = \mathfrak{g}_{\tilde{\beta}}$. Using these equalities, one can see that $\mathfrak{g}_{\tilde{\beta}} = \mathrm{Z}(\mathfrak{u})$. □

Notice that $\mathfrak{u} = \mathfrak{g}_{\tilde{\beta}} \oplus \bigoplus_{\alpha\in\Sigma^+} \mathfrak{g}_\alpha$ is of dimension $2d+1$. Let us choose a $(d+1)$-dimensional maximal abelian subalgebra $\mathfrak{a}$ of $\mathfrak{u}$, defined to be

$$\mathfrak{a} = \mathfrak{g}_{\tilde{\beta}} \oplus \bigoplus_{i=1}^{d} \mathfrak{g}_{\alpha_i}. \tag{6}$$

The maximality can be seen with the help of Lemma 2, specifically the fact that $\mathfrak{g}_{\tilde{\beta}} = [\mathfrak{g}_{\tilde{\beta}-\alpha_i}, \mathfrak{g}_{\alpha_i}]$. In Section 5, we show that this subalgebra produces a polarizing subgroup of a Heisenberg subgroup.

Lemma 4. *Let $\alpha \in \Phi$ be an arbitrary root. There exists a simple root $\gamma \in \Delta$ such that $\langle \alpha, \gamma\rangle = \pm 1$ or ± 2.*

Proof. The statement is clear if $\alpha \in \pm\Delta$ (since we can set $\gamma = \pm\alpha$) and so we can assume that $\alpha \in \Phi \setminus \pm\Delta$. In this case there exists a root $\gamma \in \Delta$ such that $\langle \alpha, \gamma\rangle \neq 0$. For root systems other than G_2, the lemma follows from Table 1. For G_2, the lemma can be verified by a direct examination of the roots. □

Set

$$F(\Phi) := \min\left\{ \langle \tilde{\beta}, \alpha\rangle > 0 : \alpha \in \Phi \right\}. \tag{7}$$

Obviously $F(\Phi) \leq 2$. For the root systems $\mathsf{A}_m, \mathsf{D}_m, \mathsf{E}_6, \mathsf{E}_7$ and E_8 have only one root length and so a similar argument as above shows that $F(\Phi) = 1$ unless $\Phi = \mathsf{A}_1$ which in this case we have $F(\mathsf{A}_1) = 2$. For $\mathsf{B}_m, \mathsf{F}_4$, and G_2, we observe that these root systems have non-perpendicular long roots and so for these root systems we also have $F(\Phi) = 1$.

We show that $F(\mathsf{C}_m) = 2$. If $\langle \tilde{\beta}, \alpha\rangle = 1$ then α is a long root, but in C_m all non-proportional distinct long roots are perpendicular. Hence $F(\mathsf{C}_m) = 2$. Therefore we have

$$F(\Phi) = \begin{cases} 1, & \Phi \neq \mathsf{A}_1;\ \mathsf{C}_m,\ m \geq 2 \\ 2, & \Phi = \mathsf{A}_1;\ \mathsf{C}_m,\ m \geq 2. \end{cases} \tag{8}$$

5. Heisenberg subgroups of adjoint Chevalley groups

In this section we review the construction of *elementary adjoint Chevalley groups* and we define Heisenberg subgroups of Chevalley groups which are obtained by exponentiating the nilpotent radical of the Heisenberg parabolic subalgebra $\mathfrak{q}$ defined in the previous section. Moreover, we verify that the construction of Chevalley groups over fields given in [7, 26] can be extended to elementary Chevalley groups defined over $\mathcal{O}/\mathfrak{p}^n$. One way to approach this is to use the language of group schemes [2]. However, in this paper we consider the explicit construction of Chevalley groups using Chevalley bases. The theory of elementary Chevalley groups over rings has also been presented in detail in [28].

As before F is a non-Archimedean local field with the ring of integers $\mathcal{O}$, the prime ideal $\mathfrak{p}$ and the residue field $\mathbb{F}_q$, $q = p^l$. Here we assume that $p \geq 3$ and we set $R = \mathcal{O}/\mathfrak{p}^n$, $n \geq 1$. We will use the standard notation, which can be found in [7, 25, 26]. Let

$$\{H_\alpha :\ \alpha \in \Delta\} \cup \{e_\alpha :\ \alpha \in \Phi\},$$

be a *Chevalley basis*, with respect to our choice of base Δ. Let $\mathfrak{g}_\mathbb{Z} \subseteq \mathfrak{g}$ be the free $\mathbb{Z}$-module generated by the Chevalley basis. One can show that $\mathfrak{g}_\mathbb{Z}$ is indeed a Lie algebra over $\mathbb{Z}$. For any $\alpha \in \Phi$ and $\xi \in \mathbb{C}$, $\mathrm{ad}_{\xi e_\alpha} = \xi\,\mathrm{ad}_{e_\alpha}$ is a nilpotent derivation of $\mathfrak{g}$. Hence, the exponential map

$$x_\alpha(\xi) := \exp(\xi\,\mathrm{ad}_{e_\alpha}),$$

is a Lie algebra automorphism of $\mathfrak{g}$. Moreover, the entries of the matrix of $x_\alpha(\xi)$, with respect to the Chevalley basis, are of the form $a\xi^i$, where $a \in \mathbb{Z}$ and i is a non-negative integer. Let us denote this matrix by $A_\alpha(\xi)$. Consider the R-Lie algebra $\mathfrak{g}_R := \mathfrak{g}_\mathbb{Z} \otimes_\mathbb{Z} R$ with the Chevalley basis

$$\{H_\alpha = H_\alpha \otimes 1 :\ \alpha \in \Delta\} \cup \{\ e_\alpha = e_\alpha \otimes 1 :\ \alpha \in \Phi\}.$$

For every $t \in R$, we obtain a new matrix $\bar{A}_\alpha(t)$ from $A_\alpha(\xi)$, by replacing the entries $a\xi^i$ by $\bar{a}t^i$, where $\bar{a}$ is a reduced modulo $\mathfrak{p}^n$. The linear transformation $\bar{x}_\alpha(t)$ associated with the matrix $\bar{A}_\alpha(t)$ is a Lie algebra automorphism of $\mathfrak{g}_R$. The subgroup of the automorphism group of $\mathfrak{g}_R$, generated by transformations $\bar{x}_\alpha(t)$ for each $\alpha \in \Phi$ and $t \in R$, is called the *elementary adjoint Chevalley group*. We denote it by

$\mathbf{G}_{ad}(R) := \mathbf{G}_{ad}(R, \Phi)$. Let $\alpha \in \Phi$ be an arbitrary root. The *one-parameter subgroup* X_α of $\mathbf{G}_{ad}(R)$ is defined by

$$X_\alpha = \langle \bar{x}_\alpha(t) : t \in R \rangle .$$

Lemma 5. *The subgroup X_α is isomorphic to the additive group of R.*

Proof. The map $t \to \bar{x}_\alpha(t)$ gives the desired group isomorphism. Note that the injectivity can be seen through the action of $\bar{x}_\alpha(t)$ on the Chevalley basis for the Lie algebra $\mathfrak{g}_R$. More precisely, we have (see [7], §4.4) $\bar{x}_\alpha(t)H_\gamma = H_\gamma - \langle \alpha, \gamma \rangle t e_\alpha$. By Lemma 4, if $\bar{x}_\alpha(t) = \mathbf{1}$, then $t = 0$ since $p \geq 3$. □

Let us define the *Heisenberg subgroup* U of $\mathbf{G}_{ad}(R)$

$$U = \left\langle \bar{x}_\alpha(t) : \langle \alpha, \tilde{\beta} \rangle \geq 1, \, t \in R \right\rangle . \tag{9}$$

Here the right hand side of (9) is the subgroup of $\mathbf{G}_{ad}(R)$ generated by the given elements $\bar{x}_\alpha(t)$. This subgroup is analogous to the nilpotent radical of the Heisenberg parabolic subalgebra. This analogy will be apparent in Proposition 1. From now on, we fix a total ordering $\prec$ of Φ which is compatible with the height function ht, i.e. $\alpha \prec \beta$ implies $\mathrm{ht}(\alpha) \leq \mathrm{ht}(\beta)$. We recall a theorem due to Chevalley (the proof over R is similar to [7, Theorem 5.2.2]) that expresses the commutator of two generators of $\mathbf{G}_{ad}(R)$ as a product of generators. Let $\alpha, \beta \in \Phi$ such that $\alpha \neq \pm\beta$, and let t_1, t_2 be elements of R. Let us define the commutator $[\bar{x}_\alpha(t_2), \bar{x}_\beta(t_1)] := \bar{x}_\alpha(t_2)^{-1}\bar{x}_\beta(t_1)^{-1}\bar{x}_\alpha(t_2)\bar{x}_\beta(t_1)$. The Chevalley commutator formula states that

$$[\bar{x}_\alpha(t_2), \bar{x}_\beta(t_1)] = \prod_{i,j>0} \bar{x}_{i\beta+j\alpha}\left(C_{i,j,\beta,\alpha}(-t_1)^i t_2^j\right), \tag{10}$$

where the product is taken over all pairs of positive integers i, j for which $i\beta + j\alpha$ is a root, and the terms of the product are in increasing order of $i + j$. The constants $C_{i,j,\beta,\alpha}$ are in the set $\{\pm 1, \pm 2, \pm 3\}$.

Next, we point out that every element of U can be expressed uniquely in the form

$$\prod_{\langle \alpha, \tilde{\beta} \rangle \geq 1} \bar{x}_\alpha(t_\alpha), \tag{11}$$

where the product is taken over positive roots α, increasing in the chosen total ordering. Indeed, given an element of U in the form of a product of $\bar{x}_\alpha(t)$'s, the desired order can be achieved by performing a rearrangement as follows: if there is a pair of consecutive terms $\bar{x}_\alpha(t_\alpha)\bar{x}_\beta(t_\beta)$ with $\beta \prec \alpha$, we swap them by use of (10):

$$\bar{x}_\alpha(t_\alpha)\bar{x}_\beta(t_\beta) = \bar{x}_\beta(t_\beta)\bar{x}_\alpha(t_\alpha) \prod_{i,j>0} \bar{x}_{i\beta+j\alpha}\left(C_{i,j,\beta,\alpha}(-t_\beta)^i t_\alpha^j\right). \tag{12}$$

In this fashion, $\bar{x}_\beta(t_\beta)\bar{x}_\alpha(t_\alpha)$ is in the increasing order, and all the extra terms introduced by use of the commutator formula are in the desired order because the total ordering $\prec$ is compatible with the height function. This rearrangement terminates after finitely many iterations. The uniqueness of such an expression of elements in U is proved by an argument similar to the proof of [7, Theorem 5.3.3(ii)]. The following lemma can be proved easily.

Lemma 6. *Let Φ be a root system different from G_2. Then for any α_i, chosen from the decomposition (5) and $t \in R$, we have*

$$\bar{x}_{\alpha_i}(1)\bar{x}_{\tilde{\beta}-\alpha_i}(t) = \bar{x}_{\tilde{\beta}-\alpha_i}(t)\bar{x}_{\alpha_i}(1)\bar{x}_{\tilde{\beta}}(Ct),$$

where $C \in \{\pm 1, \pm 2\}$.

Proof. From (12) we have

$$\bar{x}_{\alpha_i}(1)\bar{x}_{\tilde{\beta}-\alpha_i}(t) = \bar{x}_{\tilde{\beta}-\alpha_i}(t)\bar{x}_{\alpha_i}(1)\bar{x}_{\tilde{\beta}}(-C_{1,1,\tilde{\beta}-\alpha_i,\alpha_i}t).$$

But (see [7], Theorem 5.2.2) $C_{1,1,\tilde{\beta}-\alpha_i,\alpha_i} = \pm(r+1)$, where

$$(\tilde{\beta} - \alpha_i) - r\alpha_i, \cdots, (\tilde{\beta} - \alpha_i), \cdots, (\tilde{\beta} - \alpha_i) + s\alpha_i,$$

is the α_i-chain through $(\tilde{\beta}-\alpha_i)$. Since $\tilde{\beta}$ is the highest root, $(\tilde{\beta}-\alpha_i)+s\alpha_i$ is not a root for $s>1$, and therefore $s=1$. Also, it is known that $\langle\tilde{\beta}-\alpha_i,\alpha_i\rangle=r-s$. It follows that

$$r+1=\langle\tilde{\beta},\alpha_i\rangle.$$

Notice that $\langle\tilde{\beta},\alpha_i\rangle\in\{1,2\}$, since otherwise $\|\tilde{\beta}\|/\|\alpha_i\|=3$, which is impossible when the root system is different from G_2. □

Lemma 7. *Let G be a finitely generated group generated by g_i, $1\leq i\leq n$. Let $A\trianglelefteq G$ and assume that $[g_i,g_j]\in A$ for any $1\leq i,j\leq n$. Then $[G,G]\subseteq A$.*

Proposition 1. *Let $p\geq 3$ if G is not of type G_2 and $p\geq 5$ otherwise. Then the group U is two step nilpotent and $[U,U]=X_{\tilde{\beta}}$.*

Proof. With the help of (10) and Lemma 2, one can see that the commutators of the generators of U are in $X_{\tilde{\beta}}$. Hence by applying Lemma 7 we conclude that the commutator subgroup of U is contained in $X_{\tilde{\beta}}$. Conversely, by Lemma 6, any element in $X_{\tilde{\beta}}$ can be obtained from commuting suitable elements of X_{α_i} and $X_{\tilde{\beta}-\alpha_i}$, for $1\leq i\leq d$. Hence, $[U,U]=X_{\tilde{\beta}}$. On the other hand, the fact that $\tilde{\beta}$ is the highest root implies that for every α satisfying $\langle\alpha,\tilde{\beta}\rangle>0$, we have $i\tilde{\beta}+j\alpha\notin\Phi$ for all $i,j>0$. Hence, by (10) we have $[X_\alpha,X_{\tilde{\beta}}]=\mathbf{1}$ which implies that $X_{\tilde{\beta}}\subseteq Z(U)$ and hence U is a two step nilpotent subgroup. □

We now recall that by a theorem of Chevalley (whose proof over R is similar to [7, Theorem 6.3.1]), for any root α there exists a surjective homomorphism

$$\phi_\alpha:\mathrm{SL}_2(R)\longrightarrow\langle X_\alpha,X_{-\alpha}\rangle, \tag{13}$$

such that

$$\phi_\alpha\begin{pmatrix}1&t\\0&1\end{pmatrix}=\bar{x}_\alpha(t),\qquad \phi_\alpha\begin{pmatrix}1&0\\t&1\end{pmatrix}=\bar{x}_{-\alpha}(t).$$

For any invertible element $\lambda\in R$, we denote

$$h_\alpha(\lambda):=\phi_\alpha\begin{pmatrix}\lambda&0\\0&\lambda^{-1}\end{pmatrix}. \tag{14}$$

Let $\alpha,\beta\in\Phi$ be any roots, then one can show that (see [7, Chapter 7])

$$h_\alpha(\lambda)\bar{x}_\beta(t)h_\alpha(\lambda)^{-1}=\bar{x}_\beta\left(\lambda^{\langle\beta,\alpha\rangle}t\right). \tag{15}$$

6. Faithful representations and generic characters

Let (ρ,V) be a faithful representation of $\mathbf{G}_{ad}(R)$ where $R=\mathcal{O}/\mathfrak{p}^n$. Let $\sigma:=\rho|_U$, be the restriction of ρ to the Heisenberg subgroup U, defined in (9), and let (σ_i,V_i), $1\leq i\leq k$, be the irreducible factors in the decomposition of the U-representation (σ,V). Then by Schur's lemma for any $z\in Z(U)$ and $v\in V_i$ we have $\sigma_i(z)v=\chi_i(z)v$, where χ_i is a one-dimensional representation of $Z(U)$. By Lemma 1 for each $1\leq i\leq k$ there exists $\bar{b}_i=b_i+\mathfrak{p}^{-\ell}\in\mathfrak{p}^{-(n+\ell)}/\mathfrak{p}^{-\ell}$ such that for any $s\in\mathcal{O}$,

$$\chi_i\left(\bar{x}_{\tilde{\beta}}(s+\mathfrak{p}^n)\right)=\psi(\mathrm{Tr}(b_is)). \tag{16}$$

With this observation we prove the following proposition. As before the characteristic of the residue field $\mathcal{O}/\mathfrak{p}$ is p.

Proposition 2. *Let $p\geq 3$ when $\Phi\neq\mathsf{G}_2$ and $p\geq 5$ when $\Phi=\mathsf{G}_2$. Let χ_i, $1\leq i\leq k$ be defined as above, and let $b_i\in\mathfrak{p}^{-(n+\ell)}$ correspond to χ_i by Lemma 1. Then $\nu(b_i)=-(n+\ell)$ for some $1\leq i\leq k$. In particular, χ_i is a generic character of $Z(U)$.*

Proof. Suppose that for each $1\leq i\leq k$ we have $\varpi^{n-1}b_i\in\mathfrak{p}^{-\ell}$. Then $\chi_i(\bar{x}_{\tilde{\beta}}(\varpi^{n-1}+\mathfrak{p}^n))=1$. This in particular implies that $\rho(\bar{x}_{\tilde{\beta}}(\varpi^{n-1}+\mathfrak{p}^n))=\mathbf{1}$ which is a contradiction since ρ is assumed to be a faithful representation. This proves the existence of $1\leq i\leq k$ such that $\nu(b_i)=-(n+\ell)$.

Next we prove that if $\nu(b_i) = -(n+\ell)$ then χ_i is a generic character of $Z(U)$. For $u \in U$ let $\chi_i([u,y]) = 1$ for all $y \in U$. By (11),

$$u = \prod_{\langle \alpha, \tilde{\beta} \rangle \geq 1} \bar{x}_\alpha(s_\alpha + \mathfrak{p}^n) \qquad s_\alpha \in \mathcal{O}, \tag{17}$$

where the product is taken over positive roots α, increasing in the chosen total ordering. We will show that the only term that contributes to (17) is the term that belongs to $X_{\tilde{\beta}}$. It follows that $u \in Z(U)$. Note that, for any $x \in U$, the map $y \mapsto [x,y]$ is a group homomorphism, since U is a two step nilpotent group.

We remark that for $\alpha, \beta \in \Sigma^+$ we have $[X_\alpha, X_\beta] = \mathbf{1}$ unless $\beta = \tilde{\beta} - \alpha$. For any $\alpha \neq \tilde{\beta}$ in (17) and arbitrary $s \in \mathcal{O}$, from the Chevalley commutator formula (10) we have

$$[u, \bar{x}_{\tilde{\beta}-\alpha}(s + \mathfrak{p}^n)] = \bar{x}_{\tilde{\beta}}(C s_\alpha s + \mathfrak{p}^n),$$

where by Lemma 6, $C \in \{\pm 1, \pm 2\}$ if Φ is different from G_2 and $C \in \{\pm 1, \pm 2, \pm 3\}$ when $\Phi = \mathsf{G}_2$. Since for any $s \in \mathcal{O}$ we have

$$1 = \chi_i\left([u, \bar{x}_{\tilde{\beta}-\alpha}(s + \mathfrak{p}^n)]\right) = \chi_i\left(\bar{x}_{\tilde{\beta}}(C s_\alpha s + \mathfrak{p}^n)\right) = \psi(\mathrm{Tr}(C b_i s_\alpha s)), \tag{18}$$

then

$$C b_i s_\alpha \in \mathfrak{p}^{-\ell}, \tag{19}$$

which implies that $\nu(s_\alpha) \geq n$ since $\nu(b_i) = -(n+\ell)$ (when $\Phi = \mathsf{G}_2$ we must assume $p \geq 5$ since C can be ± 3). Hence $s_\alpha \in \mathfrak{p}^n$. This shows that $u = \bar{x}_{\tilde{\beta}}(s_{\tilde{\beta}} + \mathfrak{p}^n)$ for some $s_{\tilde{\beta}} \in \mathcal{O}$ and so $u \in X_{\tilde{\beta}} \subseteq Z(U)$ which shows that χ_i is a generic character of $Z(U)$. □

Remark 4. When $p = 2$, the above argument fails since C can be ± 2 and then we can not deduce from (19) that $\nu(s_\alpha) \geq n$. This is crucial when one wants to apply the Stone-von Neumann theorem.

In order to apply the Stone-von Neumann theorem, we then need to find the polarizing subgroup of U. Define

$$A = \left\langle \bar{x}_{\tilde{\beta}}(t),\ \bar{x}_{\alpha_i}(t) : 1 \leq i \leq d,\ t \in R \right\rangle, \tag{20}$$

where α_i are chosen with respect to the decomposition (5). We will show that A is a polarizing subgroup of U with respect to the generic character χ_i defined above. Notice that for any α_i and α_j, $1 \leq i, j \leq d$, chosen from the first disjoint component of the decomposition (5), neither $\alpha_i + \alpha_j$ nor $\alpha_i + \tilde{\beta}$ is a root. Hence, the right hand side of (10) is always zero for elements in A, and therefore A is an abelian subgroup of U containing $X_{\tilde{\beta}}$.

Proposition 3. *Let $p \geq 3$ when $\Phi \neq \mathsf{G}_2$ and $p \geq 5$ when $\Phi = \mathsf{G}_2$. Let χ_1 be a one-dimensional representation of $Z(U)$ corresponding to $b_1 \in \mathfrak{p}^{-(n+\ell)}$ via Lemma 1. Assume that $\nu(b_1) = -(n+\ell)$. Then A is a polarizing subgroup with respect to χ_1.*

Proof. We have shown that A is an abelian subgroup and so A is an isotropic subgroup of U. Assume A is not a polarizing subgroup. Each $u \in U$ has a unique presentation (17). By the length of $u \in U$ we mean the number of terms in (17). Let $u \in U \setminus A$ be an element with the shortest length such that

$$\chi_1([u,a]) = 1, \qquad \forall a \in A. \tag{21}$$

Let us denote the unique presentation of u as follows

$$u = \prod_{\langle \alpha, \tilde{\beta} \rangle \geq 1} \bar{x}_\alpha(s_\alpha + \mathfrak{p}^n) \qquad s_\alpha \in \mathcal{O}. \tag{22}$$

We claim that the leftmost term in the product in (22) cannot belong to either of $X_{\tilde{\beta}}$ and X_{α_i}, $1 \leq i \leq d$. That is because otherwise, one can eliminate this term and obtain another element in $U \setminus A$ with shorter

length that satisfies in (21). We again remark that for $\alpha, \beta \in \Sigma^+$ we have $[X_\alpha, X_\beta] = \mathbf{1}$ unless $\beta = \tilde{\beta} - \alpha$. Without loss of generality we can write

$$u = \bar{x}_{\tilde{\beta}-\alpha_1}(s_{\alpha_1} + \mathfrak{p}^n)u' \qquad s_{\alpha_1} \in \mathcal{O} \setminus \mathfrak{p}^n,$$

where α_1 is taken from the decomposition (5). Notice that none of the elements of $X_{\tilde{\beta}-\alpha_1}$ appears in the factorization of u'. Hence for an arbitrary $s \in \mathcal{O}$ we have

$$\begin{aligned}[u, \bar{x}_{\alpha_1}(s + \mathfrak{p}^n)] &= [\bar{x}_{\tilde{\beta}-\alpha_1}(s_{\alpha_1} + \mathfrak{p}^n), \bar{x}_{\alpha_1}(s + \mathfrak{p}^n)][u', \bar{x}_{\alpha_1}(s + \mathfrak{p}^n)] \\ &= [\bar{x}_{\tilde{\beta}-\alpha_1}(s_{\alpha_1} + \mathfrak{p}^n), \bar{x}_{\alpha_1}(s + \mathfrak{p}^n)] = \bar{x}_{\tilde{\beta}}(Cs_{\alpha_1}s + \mathfrak{p}^n)\end{aligned}$$

where $C \in \{\pm 1, \pm 2, \pm 3\}$. Hence from (21) we deduce that for any $s \in \mathcal{O}$

$$1 = \chi_1\left([u, \bar{x}_{\alpha_1}(s + \mathfrak{p}^n)]\right) = \psi(\mathrm{Tr}(Cb_1 s_{\alpha_1} s)). \tag{23}$$

Therefore we should have $Cb_1 s_{\alpha_1} \in \mathfrak{p}^{-\ell}$. By Lemma 6, for all root systems other than G_2, the contradiction $s_{\alpha_1} \in \mathfrak{p}^n$ is obtained when $p \geq 3$. However, for the root system G_2 the further assumption $p \geq 5$ is required in order to obtain a contradiction. □

We now compute the index of A in U.

Lemma 8. *Let d be as in Table 2. Then $[U : A] = q^{nd}$.*

Proof. Recall that $|\Sigma^+| = 2d$. From (9) and uniqueness of the product in (11) we deduce that $|U| = q^{(2d+1)n}$ and $|A| = q^{(d+1)n}$. Therefore, $[U : A] = q^{nd}$. □

7. Proof of Theorem 1

In what follows the group of units of a given ring R is denoted by $R^\times$. Let (ρ, V) be a faithful representation of $\mathbf{G}_{ad}(R)$. Let $\sigma := \rho|_U$, be the restriction of ρ to the Heisenberg subgroup U, and let (σ_i, V_i), $1 \leq i \leq k$, be the irreducible factors in the decomposition of the U-representation (σ, V) with central characters χ_i. By Proposition 2, we can assume that χ_1 is a generic character of $Z(U)$, such that the element $b_1 \in \mathfrak{p}^{-(n+\ell)}$ associated to χ_1 in Lemma 1 satisfies $\nu(b_1) = -(n + \ell)$. Then, by Proposition 3, A is a polarizing subgroup with respect to the generic character χ_1. Therefore, by Stone-von Neumann theorem and Lemma 8, we have

$$\dim(V_1) = [U : A] = q^{dn}.$$

For any $\bar{\lambda} = \lambda + \mathfrak{p}^n \in R^\times$, and any root $\alpha \in \Phi$, consider the element $h_\alpha(\bar{\lambda})$ introduced in (14). It follows from (15) that $h_\alpha(\bar{\lambda})$ normalizes any one parameter subgroup. Therefore, $h_\alpha(\bar{\lambda})$ normalizes U. Define the U-representation $\sigma^{\bar{\lambda},\alpha}$ to be the conjugation of σ by $h_\alpha(\bar{\lambda})$:

$$\sigma^{\bar{\lambda},\alpha} : U \to \mathrm{GL}(V), \qquad u \mapsto \sigma\left(h_\alpha(\bar{\lambda}) u h_\alpha(\bar{\lambda})^{-1}\right).$$

Notice that the U-intertwining operator $\rho(h_\alpha(\bar{\lambda}))$ gives a U-isomorphism between (σ, V) and $(\sigma^{\bar{\lambda},\alpha}, V)$. Therefore, $(\sigma_1^{\bar{\lambda},\alpha}, V_1)$ is also an irreducible subrepresentation of (σ, V). Hence for any $z \in X_{\tilde{\beta}} \subseteq Z(U)$ and $v \in V_1$ we have

$$\chi_1(h_\alpha(\bar{\lambda}) z h_\alpha(\bar{\lambda})^{-1})v = \sigma_1(h_\alpha(\bar{\lambda}) z h_\alpha(\bar{\lambda})^{-1})v = \sigma_1^{\bar{\lambda},\alpha}(z)v = \chi_1^{\bar{\lambda},\alpha}(z)v,$$

where $\chi_1^{\bar{\lambda},\alpha}$ is the one-dimensional representation of $Z(U)$ which is the central character of $\sigma_1^{\bar{\lambda},\alpha}$. Then for $s + \mathfrak{p}^n \in R \cong X_{\tilde{\beta}}$, from (15), we obtain

$$\chi_1^{\bar{\lambda},\alpha}\left(\bar{x}_{\tilde{\beta}}(s + \mathfrak{p}^n)\right) = \chi_1\left(\bar{x}_{\tilde{\beta}}(\lambda^{\langle\tilde{\beta},\alpha\rangle} s + \mathfrak{p}^n)\right) = \psi\left(\mathrm{Tr}\left(b_1 \lambda^{\langle\tilde{\beta},\alpha\rangle} s\right)\right).$$

Next, we count the number of mutually distinct one-dimensional representations of $\chi_1^{\bar{\lambda},\alpha}$. We consider two cases:

(1) The root system Φ is not A_1 or C_m for $m \geq 2$: Equation (8) implies that there exists a root $\alpha \in \Phi$ such that $\langle \tilde{\beta}, \alpha \rangle = 1$. Hence, for this particular root α we have

$$\chi_1^{\bar{\lambda},\alpha}(\bar{x}_{\tilde{\beta}}(s+\mathfrak{p}^n)) = \chi_1(\lambda \bar{x}_{\tilde{\beta}}(s+\mathfrak{p}^n)) = \psi\left(\mathrm{Tr}\left(b_1 \lambda s\right)\right), \qquad \forall s \in \mathcal{O}.$$

Since χ_1 is corresponding to $b_1 \in \mathfrak{p}^{-(n+\ell)}$ with $\nu(b_1) = -(n+\ell)$, we can conclude that $\chi_1^{\bar{\lambda}_1,\alpha} \neq \chi_1^{\bar{\lambda}_2,\alpha}$ when $\bar{\lambda}_1 \neq \bar{\lambda}_2 \in R^\times$, since otherwise $b_1(\lambda_1 - \lambda_2) \in \mathfrak{p}^{-\ell}$ which implies $\lambda_1 - \lambda_2 \in \mathfrak{p}^n$. Hence, there are $q^n - q^{n-1}$ distinct one-dimensional representations $\chi_1^{\bar{\lambda},\alpha}$ and therefore, there are at least $q^n - q^{n-1}$ non-isomorphic irreducible subrepresentations of V, each of dimension q^{dn}. Hence,

$$\dim(V) \geq (q^n - q^{n-1})q^{dn},$$

where d is given in Table 2.

(2) The root system Φ is either C_m or A_1: Equation (8) implies that for no root in Φ, $\langle \tilde{\beta}, \alpha \rangle = 1$; but a root α can be chosen such that $\langle \tilde{\beta}, \alpha \rangle = 2$. Then for $s + \mathfrak{p}^n \in R \cong X_{\tilde{\beta}}$ we have

$$\chi_1^{\bar{\lambda},\alpha}(\bar{x}_{\tilde{\beta}}(s+\mathfrak{p}^n)) = \chi_1\left(\bar{x}_{\tilde{\beta}}(\lambda^2 s+\mathfrak{p}^n)\right) = \psi\left(\mathrm{Tr}\left(b_1 \lambda^2 s\right)\right).$$

Hence, we can construct $|R^\times|/2 = (q^n - q^{n-1})/2$ distinct one-dimensional representations $\chi_1^{\bar{\lambda},\alpha}$, which leads to obtaining $(q^n - q^{n-1})/2$ non-isomorphic factors in the decomposition of (σ, V), each of dimension $q^{(m-1)n}$. Hence

$$\dim(V) \geq \frac{1}{2}(q^n - q^{n-1})q^{(m-1)n}.$$

Acknowledgement

M.B. would like to thank Alexander Gamburd for his interest in this project. During the completion of this work, M.B. was supported by a postdoctoral fellowship from the University of Ottawa. He wishes to thank his supervisor Vadim Kaimanovich for useful discussions on the subject of this paper and Dmitry Jakobson and Mikael Pichot for their support and stimulating discussions during his visit at McGill University where part of this joint work was done. C.K. and H.S. thank Monica Nevins and Kirill Zaynullin for interesting discussions concerning this project. The authors are also very grateful to the referee for a very careful reading and many helpful suggestions and corrections.

References

[1] Mohammad Bardestani and Keivan Mallahi-Karai. Quasi-random profinite groups. *Glasg. Math. J.*, 57(1):181–200, 2015.

[2] Armand Borel. Properties and linear representations of Chevalley groups. In *Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, N.J., 1968/69)*, Lecture Notes in Mathematics, Vol. 131, pages 1–55. Springer, Berlin, 1970.

[3] Jean Bourgain and Alex Gamburd. Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$. I. *J. Eur. Math. Soc. (JEMS)*, 10(4):987–1011, 2008.

[4] Jean Bourgain and Alex Gamburd. Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$. *Ann. of Math. (2)*, 167(2):625–642, 2008.

[5] Emmanuel Breuillard, Ben Green, and Terence Tao. Approximate subgroups of linear groups. *Geom. Funct. Anal.*, 21(4):774–819, 2011.

[6] Daniel Bump. *Automorphic forms and representations*, volume 55 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997.

[7] Roger W. Carter. *Simple groups of Lie type*. Wiley Classics Library. John Wiley & Sons Inc., New York, 1989. Reprint of the 1972 original, A Wiley-Interscience Publication.

[8] Nicolas de Saxcé. Trou dimensionnel dans les groupes de Lie compacts semisimples via les séries de Fourier. *J. Anal. Math.*, 120:311–331, 2013.

[9] G. Frobenius. Über Gruppencharaktere. *Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin*, pages 985–1021, 1896.

[10] Benedict H. Gross and Nolan R. Wallach. On quaternionic discrete series representations, and their continuations. *J. Reine Angew. Math.*, 481:73–123, 1996.

[11] Robert M. Guralnick and Pham Huu Tiep. Low-dimensional representations of special linear groups in cross characteristics. *Proc. London Math. Soc. (3)*, 78(1):116–138, 1999.
[12] Roger E. Howe. Some recent applications of induced representations. In *Group representations, ergodic theory, and mathematical physics: a tribute to George W. Mackey*, volume 449 of *Contemp. Math.*, pages 173–191. Amer. Math. Soc., Providence, RI, 2008.
[13] James E. Humphreys. *Introduction to Lie algebras and representation theory*, volume 9 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1978. Second printing, revised.
[14] Vicente Landazuri and Gary M. Seitz. On the minimal degrees of projective representations of the finite Chevalley groups. *J. Algebra*, 32:418–443, 1974.
[15] Frank Lübeck. Small degree representations of finite Chevalley groups in defining characteristic. *LMS J. Comput. Math.*, 4:135–169 (electronic), 2001.
[16] Alexander Lubotzky. Expander graphs in pure and applied mathematics. *Bull. Amer. Math. Soc. (N.S.)*, 49(1):113–162, 2012.
[17] Peter J. McNamara. Principal series representations of metaplectic groups over local fields. In *Multiple Dirichlet series, L-functions and automorphic forms*, volume 300 of *Progr. Math.*, pages 299–327. Birkhäuser/Springer, New York, 2012.
[18] Colette Mœglin, Marie-France Vignéras, and Jean-Loup Waldspurger. *Correspondances de Howe sur un corps p-adique*, volume 1291 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1987.
[19] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.
[20] Rimhak Ree. On some simple groups defined by C. Chevalley. *Trans. Amer. Math. Soc.*, 84:392–400, 1957.
[21] Hadi Salmasian. A notion of rank for unitary representations of reductive groups based on Kirillov's orbit method. *Duke Math. J.*, 136(1):1–49, 2007.
[22] Peter Sarnak and Xiao Xi Xue. Bounds for multiplicities of automorphic representations. *Duke Math. J.*, 64(1):207–227, 1991.
[23] Gary M. Seitz and Alexander E. Zalesskii. On the minimal degrees of projective representations of the finite Chevalley groups. II. *J. Algebra*, 158(1):233–243, 1993.
[24] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.
[25] Jean-Pierre Serre. *Complex semisimple Lie algebras*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2001. Translated from the French by G. A. Jones, Reprint of the 1987 edition.
[26] Robert Steinberg. *Lectures on Chevalley groups*. Yale University, New Haven, Conn., 1968. Notes prepared by John Faulkner and Robert Wilson.
[27] Pham Huu Tiep and Alexander E. Zalesskii. Minimal characters of the finite classical groups. *Comm. Algebra*, 24(6):2093–2167, 1996.
[28] Nikolai Vavilov and Eugene Plotkin. Chevalley groups over commutative rings. I. Elementary calculations. *Acta Appl. Math.*, 45(1):73–113, 1996.

Mohammad Bardestani, Department of Mathematics and Statistics, University of Ottawa, 585 King Edward, Ottawa, ON K1N 6N5, Canada.
E-mail address: mbardest@uottawa.ca

Camelia Karimianpour, Department of Mathematics and Statistics, University of Ottawa, 585 King Edward, Ottawa, ON K1N 6N5, Canada.
E-mail address: ckari099@uottawa.ca

Keivan Mallahi-Karai, Jacobs University Bremen, Campus Ring I, 28759 Bremen, Germany.
E-mail address: k.mallahikarai@jacobs-university.de

Hadi Salmasian, Department of Mathematics and Statistics, University of Ottawa, 585 King Edward, Ottawa, ON K1N 6N5, Canada.
E-mail address: hadi.salmasian@uottawa.ca