INTEGRAL EMBEDDINGS OF CUBIC NORM STRUCTURES

WEE TECK GAN AND BENEDICT H. GROSS

To Nathan Jacobson, in memorium

1. Introduction

This paper is a direct sequel to our earlier work [GG]. We begin by recalling the results obtained there briefly. Let R be Coxeter's order in the $\mathbb{Q}$-algebra of Cayley's octonions [GG, Pg. 265]. This is a non-associative ring with involution $x \mapsto \bar{x}$, and the quadratic form $\mathbb{N} : R \to \mathbb{Z}$ defined by $\mathbb{N}(x) = x \cdot \bar{x}$ satisfies $\mathbb{N}(x \cdot y) = \mathbb{N}(x) \cdot \mathbb{N}(y)$. The triple $(R, \mathbb{N}, \cdot)$ is a composition algebra over $\mathbb{Z}$.

Let J_2 be the free abelian group of 2×2 Hermitian symmetric matrices with entries in R. The determinant gives a quadratic form $\det : J_2 \to \mathbb{Z}$, and the identity matrix I satisfies $\det(I) = 1$. The triple $(J_2, \det, I)$ is a pointed quadratic space over $\mathbb{Z}$, and gives a Jordan algebra over $\mathbb{Z}[\frac{1}{2}]$ (or if one prefers, a quadratic Jordan algebra over $\mathbb{Z}$).

Let J_3 be the free abelian group of 3×3 Hermitian symmetric matrcies with entries in R. The determinant (miraculously) gives a cubic form $\det : J_3 \to \mathbb{Z}$. The identity matrix I, as well as the matrix

$$E = \begin{pmatrix} 2 & \alpha & \bar{\alpha} \\ \bar{\alpha} & 2 & \alpha \\ \alpha & \bar{\alpha} & 2 \end{pmatrix}$$

with

$$\alpha = \frac{1}{2}(-1 + e_1 + e_2 + ... + e_7) \in R$$

both satisfy $\det(I) = \det(E) = 1$. The triples $J_I = (J_3, \det, I)$ and $J_E = (J_3, \det, E)$ are pointed cubic spaces over $\mathbb{Z}$. Using the polarizations I and E (in the sense of [EG]), we may define symmetric bilinear forms T_I and T_E on J_3, as well as quadratic maps $M \mapsto M^{\#}$ from J_3 to J_3. The 5-tuples $(J_3, \det, I, \#_I, T_I)$ and $(J_3, \det, E, \#_E, T_E)$ define cubic norm structures over $\mathbb{Z}$, which give rise to Jordan algebras over $\mathbb{Z}[\frac{1}{2}]$ (or if one prefers, quadratic Jordan algebras over $\mathbb{Z}$).

Now let A be the ring of integral elements in an étale quadratic or cubic algebra k over $\mathbb{Q}$. When A is quadratic, $(A, \mathbb{N}, \cdot)$ is a composition algebra, and $(A, \mathbb{N}, 1)$ is a pointed quadratic space. When A is cubic, $(A, \mathbb{N}, 1)$ is a pointed cubic space, which gives rise to the cubic norm structure $(A, \mathbb{N}, 1, \#, \mathrm{Tr})$, where $a \cdot a^{\#} = \mathbb{N}(a)$.

1991 *Mathematics Subject Classification.* 11F30, 17C40, 20G25.

In our previous paper [GG], we counted the number of embeddings

$$\begin{array}{ll} A \to R & \text{of composition algebras, when } A \otimes \mathbb{R} = \mathbb{C}; \\ A \to J_2 & \text{of pointed quadratic spaces, when } A \otimes \mathbb{R} = \mathbb{R}^2; \\ \left.\begin{array}{l} A \to J_I \\ A \to J_E \end{array}\right\} & \text{of pointed cubic spaces, when } A \otimes \mathbb{R} = \mathbb{R}^3. \end{array}$$

This number is expressed in terms of the zeta function $\zeta_A(s)$ of A at $s = -2$ and $s = -3$. To be more precise, in the cubic case, what we computed is the weighted sum

$$N_A = 91 \cdot N(A, J_I) + 600 \cdot N(A, J_E).$$

of the numbers $N(A, J_I)$ and $N(A, J_E)$ of embeddings of A into J_I and J_E. This reflects the fact that J_I and J_E, though inequivalent over $\mathbb{Z}$, are isomorphic over $\mathbb{Z}_p$ for all primes p. Moreover, it was shown in [GG, Lemma 2] that an embedding of the above pointed cubic spaces over $\mathbb{Z}$ is always an embedding of the corresponding cubic norm structures. Hence, what we counted in the cubic case are embeddings of cubic norm structures.

The results of [GG] were obtained by applying the adelic framework of Kneser, Tamagawa and Weil (as described, for example, in Serre's résumé des cours [Se]), which reduces the counting of global embeddings to a problem of local embeddings (over $\mathbb{Z}_p$) and a comparison of two natural global measures. The local results were contained in [GG, Proposition 2], the statement of which we now recall. Let $\underline{G}$ be the automorphism group of R, J_2, J_I or J_E over $\mathbb{Z}$. Then $\underline{G}$ is a group over $\mathbb{Z}$ in the sense of [G], and is of type G_2, B_4 and F_4 respectively. Let $\underline{H}$ be the stabilizer of a global embedding. Then [GG, Proposition 2] states that for each prime p,

(i) $\underline{G}(\mathbb{Z}_p)$ acts transitively on the set of embeddings over $\mathbb{Z}_p$, and

(ii) $\underline{H}(\mathbb{Z}_p)$ is a special maximal parahoric subgroup of $\underline{H}(\mathbb{Q}_p)$.

The proof given in [GG] for this crucial local result is based on the assertion that, among the smooth integral models $\underline{H}$ of H over $\mathbb{Q}_p$, the orders $\#\underline{H}(\mathbb{Z}/p^n\mathbb{Z})$ are largest when $\underline{H}(\mathbb{Z}_p)$ is a special maximal compact subgroup [GG, Pg. 277]. This is only true if we restrict attention to the class of smooth group schemes over $\mathbb{Z}_p$ associated to the parahoric subgroups of $H(\mathbb{Q}_p)$. However, since it is not a priori clear that the stabilizer $\underline{H}$ of an integral embedding belongs to this class, the proof of Proposition 2 given in [GG] is incomplete as it stands.

The present paper provides a complete proof of the above local result and thus serves as an erratum to [GG]. When k is quadratic, this is achieved using the results of Bruhat and Tits [BT2], who gave a description of the parahoric subgroups of classical groups as the stabilizers of certain lattices in the standard representation. When k is cubic, which is the main case of interest in [GG], the relevant group $\underline{H}$ is a trialitarian form of $Spin_8$, which is not treated in [BT2]. In this case, we need to extend the results of [BT2] to trialitarian groups, and the proof that $\underline{H}(\mathbb{Z}_p)$ is a special maximal compact subgroup occupies Sections 8-13. We refer the reader to Section 4 for a precise statement of the results.

Acknowledgments

The results obtained here rely heavily on the poineering work of Nathan Jacobson on composition algebras, Jordan algebras and exceptional algebraic groups. This paper is dedicated to his memory.

We are also grateful to Jiu-Kang Yu for his generous help in performing some crucial computer calculations, and for clarifying various points in Bruhat-Tits theory.

2. **Cubic Norm Structures**

In this section, we establish some notations, and recall the basic objects of interest in greater detail. Since the situation is entirely local, our notations will be somewhat different from those of the introduction. The results established in this paper hold over any non-archimedean local field of characteristic $\neq 2$ with the same proof, but we will restrict ourselves to working over $\mathbb{Q}_p$ for simplicity.

Let R be a maximal order in the (split) octonion algebra over $\mathbb{Q}_p$. It is unique up to conjugacy by the automorphism group of $R \otimes \mathbb{Q}_p$ [BS], and can be obtained, for example, from Coxeter's order over $\mathbb{Z}$ [GG, Pg. 265] by base extension to $\mathbb{Z}_p$. Since the octonion algebra here is split, an alternative description, more convenient for computation, is obtained by taking R as the $\mathbb{Z}_p$-lattice of integral matrices in the space of Zorn's vector matrices over $\mathbb{Q}_p$ [KMRT, Pg. 507, Ex. 5]. We call this **Zorn's model** for R. In any case, R is a non-associative ring with unit, equipped with an anti-involution $x \mapsto \bar{x}$, such that $x \cdot \bar{x} \in \mathbb{Z}_p$. The quadratic form $\mathbb{N}(x) = x \cdot \bar{x}$ satisfies

$$\mathbb{N}(x \cdot y) = \mathbb{N}(x) \cdot \mathbb{N}(y),$$

so that the triple $(R, \mathbb{N}, \cdot)$ is a **composition algebra** over $\mathbb{Z}_p$. The trace $\mathrm{Tr}(x) = x + \bar{x}$ is a linear form on the free $\mathbb{Z}_p$-module R, and the symmetric bilinear form associated to $\mathbb{N}$ is given by

$$T(x, y) = \mathrm{Tr}(x \cdot \bar{y}).$$

The symmetric bilinear module (R, T) is nondegenerate or unimodular over $\mathbb{Z}_p$.

Denote by J_2 the additive group of 2×2 Hermitian symmetric matrices with entries in R. Then J_2 is a free $\mathbb{Z}_p$-module of rank 10. An element of J_2 has the form

$$m = \begin{pmatrix} a & x \\ \bar{x} & b \end{pmatrix},$$

with $a, b \in \mathbb{Z}_p$ and $x \in R$. Further, J_2 is equipped with a nondenegerate quadratic form

$$\det : J_2 \to \mathbb{Z}_p$$

$$\det(m) = ab - \mathbb{N}(x),$$

with associated nondegenerate symmetric bilinear form T. Let I be the identity matrix. Then the triple $(J_2, \det, I)$ is a **pointed quadratic space** over $\mathbb{Z}_p$. By abuse of language, we shall simply say that J_2 is a pointed quadratic space, suppressing the mention of det and I. Note that J_2 gives rise to a quadratic Jordan algebra [JM], so it makes sense to speak of the elements m^α for any positive integer α.

Denote by J_3 the additive group of 3×3 Hermitian symmetric matrices with entries in R, so that J_3 is a free $\mathbb{Z}_p$-module of rank 27. An element of J_3 has the form:

$$m = \begin{pmatrix} a & z & \bar{y} \\ \bar{z} & b & x \\ y & \bar{x} & c \end{pmatrix},$$

with $a, b, c \in \mathbb{Z}_p$, and $x, y, z \in R$. There is a natural cubic form on J_3, given by:

$$\det : J_3 \to \mathbb{Z}_p$$

$$\det(m) = abc + \mathrm{Tr}(xyz) - a \cdot \mathbb{N}(x) - b \cdot \mathbb{N}(y) - c \cdot \mathbb{N}(z),$$

and a natural nondegenerate symmetric bilinear form T, given by:

$$T(m_1, m_2) = a_1 a_2 + b_1 b_2 + c_1 c_2 + \mathrm{Tr}(x_1 \cdot \bar{x}_2) + \mathrm{Tr}(y_1 \cdot \bar{y}_2) + \mathrm{Tr}(z_1 \cdot \bar{z}_2).$$

There is also a quadratic map $\#$ on J_3 given by:

$$m^{\#} = \begin{pmatrix} bc - \mathbb{N}(x) & \overline{x \cdot y} - cz & z \cdot x - b\bar{y} \\ x \cdot y - c\bar{z} & ca - \mathbb{N}(y) & \overline{y \cdot z} - ax \\ \overline{z \cdot x} - by & y \cdot z - a\bar{x} & ab - \mathbb{N}(z) \end{pmatrix}.$$

For $m, n \in J_3$, we set:

$$m \times n = (m + n)^{\#} - m^{\#} - n^{\#}.$$

Let I be the identity matrix. Then the 5-tuple $(J_3, \det, I, \#, T)$ is a **cubic norm structure** over $\mathbb{Z}_p$. By a cubic norm structure over a ring A, we mean a 5-tuple $(J, N, 1, \#, T)$ consisting of

- a free A-module J,
- a cubic form $N : J \to A$,
- an element $1 \in J$,
- a quadratic map $\# : J \to J$, and
- a symmetric bilinear form $T : J \times J \to A$,

which satisfies

(i) $N(1) = 1$ and $1^{\#} = 1$,

(ii) $x^{\#\#} = N(x) \cdot x$,

(iii) $T(m, 1) \cdot 1 = 1 \times m + m$ for any $m \in J$,

(iv) over the ring $A[\lambda]$, we have the identity

$$N(m + \lambda n) = N(n)\lambda^3 + T(m, n^{\#})\lambda^2 + T(m^{\#}, n)\lambda + N(m).$$

There are other possible definitions of a cubic norm structure; here we follow the definition used in [KMRT]. We refer the reader to [KMRT, §38] for other properties of cubic norm structures. As before, we shall simply say that J_3 is a cubic norm structure, suppressing the other ingredients. Again, J_3 gives rise to a quadratic Jordan algebra over $\mathbb{Z}_p$.

Remarks:

(i) We do not require the symmetric bilinear form T to be nondegenerate in the definition of a cubic norm structure, though this is the case for the cubic norm structure J_3 defined above.

(ii) As mentioned in the introduction, it is possible to suppress T and $\#$ in the datum defining J_3. Indeed, the pointed cubic space $(J_3, \det, I)$ is admissible in the sense of Jacobson [J5]. To an admissible pointed cubic space, Jacobson associates naturally a cubic norm structure (whose symmetric bilinear form T is nondegenerate). An automorphism of an admissible pointed cubic space is also an automorphism of the corresponding cubic norm structures. However, we do not know whether an arbitrary morphism of admissible pointed cubic spaces, which is not an isomorphism, necessarily gives rise to a morphism of the corresponding cubic norm structures.

There is another model of the cubic norm structure J_3 which is due to Tits [KMRT, §39, Pg. 525]. This model is more useful for computation, and we describe it briefly. Let $M_3(\mathbb{Z}_p)$ be the $\mathbb{Z}_p$-algebra of 3×3 matrices with entries in $\mathbb{Z}_p$, with trace map Tr and determinant map det. Write ab for the matrix multiplication of $a, b \in M_3(\mathbb{Z}_p)$, and $a^\#$ for the adjoint matrix of a. Consider the direct sum $M_3(\mathbb{Z}_p)^+ \oplus M_3(\mathbb{Z}_p) \oplus M_3(\mathbb{Z}_p)$ of 3 copies of $M_3(\mathbb{Z}_p)$, where $M_3(\mathbb{Z}_p)^+$ denotes the first copy. Set

$$\begin{cases} e = (I, 0, 0) \\ N(a, b, c) = \det(a) + \det(b) + \det(c) - \mathrm{Tr}(abc) \\ T((a_1, b_1, c_1), (a_2, b_2, c_2)) = \mathrm{Tr}(a_1 a_2) + \mathrm{Tr}(b_1 c_2) + \mathrm{Tr}(c_1 b_2) \\ (a, b, c)^\# = (a^\# - bc, c^\# - ab, b^\# - ca). \end{cases} \tag{2.1}$$

Then $(M_3(\mathbb{Z}_p)^3, N, e, \#, T)$ is a cubic norm structure which is easily seen to be isomorphic to J_3 (using Zorn's model for R). We shall call this the **Tits model** for J_3. It is clear from (2.1) that the Tits model can be defined over $\mathbb{Z}$.

Let Λ denote R, J_2 or J_3. Further, let $F = \Lambda \otimes \mathbb{Q}_p$ and $\kappa = \Lambda \otimes \mathbb{Z}/p\mathbb{Z}$. By Jacobson, for every element m of F or κ, one can speak of its characteristic polynomial (sometimes called generic minimal polynomial), and its minimal polynomial. For example, if $\Lambda = J_3$, then the characteristic polynomial of m is the cubic polynomial

$$\det(\lambda I - m) = \lambda^3 - T(m, I)\lambda^2 + T(m^\#, I)\lambda + \det(m).$$

The identity component of the algebraic group of automorphisms of F will be denoted by G, and is the split group of type G_2, SO_9 and F_4 respectively. The stabilizer in G of the lattice Λ is a smooth integral group scheme $\underline{G}$ over $\mathbb{Z}_p$, which is the Chevalley model of G (see [G] for $\Lambda = R$ or J_3; the case $\Lambda = J_2$ can be checked easily). In particular, $\underline{G}(\mathbb{Z}_p)$ is a hyperspecial maximal compact subgroup of $G(\mathbb{Q}_p)$.

Finally, let k be an étale quadratic or cubic algebra over $\mathbb{Q}_p$, with maximal order A, trace map Tr_k and norm map $\mathbb{N}_k$. In the case where k is quadratic, the triple $(A, \mathbb{N}_k, \cdot)$ is a composition algebra over $\mathbb{Z}_p$, and the triple $(A, \mathbb{N}_k, 1)$ is a pointed quadratic space over $\mathbb{Z}_p$. Suppose now that k is cubic. Then every $x \in A$ has a charactristic polynomial $\lambda^3 -$

$\mathrm{Tr}_k(x)\lambda^2 + S_k(x)\lambda - \mathbb{N}_k(x)$, for some $S_k(x) \in \mathbb{Z}_p$. Set:

$$\begin{cases} T_k(x,y) = \mathrm{Tr}_k(xy), \\ x^\# = x^2 - \mathrm{Tr}_k(x)x + S_k(x). \end{cases}$$

Then $(A, \mathbb{N}_k, 1, \#, T_k)$ is a cubic norm structure over $\mathbb{Z}_p$.

3. Integral Embeddings and the Affine Scheme $\underline{X}$

Henceforth, we fix the étale $\mathbb{Q}_p$-algebra k, and consider morphisms:

$$\begin{cases} j : A \longrightarrow R \text{ of composition algebras;} \\ j : A \longrightarrow J_2 \text{ of pointed quadratic spaces;} \\ j : A \longrightarrow J_3 \text{ of cubic norm structures.} \end{cases}$$

We call such a j an **integral embedding**.

Lemma 3.1. *Integral embeddings exist.*

Proof. This was checked in [GG, Pg. 276], but is even more obvious if one uses Zorn's model for R, and the Tits model for J_3 introduced in the previous section. □

Our goal in this section is to define an affine scheme $\underline{X}$ over $\mathbb{Z}_p$ such that $\underline{X}(\mathbb{Z}_p)$ is precisely the set of integral embeddings. If k is a quadratic étale algebra or a cubic field, A is singly generated over $\mathbb{Z}_p$, say $A = \mathbb{Z}_p[\alpha]$. To give a morphism $j : A \to \Lambda$, it is necessary and sufficient to specify the image $m \in \Lambda$ of α. The element m must have the same characteristic polynomial as α, and it is not difficult to check that conversely, any such element m of Λ gives rise to a morphism j with $j(\alpha) = m$. Hence, let $\underline{X}$ be the closed subscheme of the affine space Λ consisting of elements with the same characteristic polynomial as α. For example, when $\Lambda = J_3$, for any $\mathbb{Z}_p$-algebra B, $\underline{X}(B)$ consists of those elements m of $J_3 \otimes B$ satisfying:

$$\begin{cases} T(m, I) = \mathrm{Tr}_k(\alpha), \\ T(m^\#, I) = \mathrm{Tr}_k(\alpha^\#), \\ \det(m) = \mathbb{N}_k(\alpha). \end{cases} \tag{3.2}$$

We stress that the affine scheme $\underline{X}$ may a priori depend on the choice of α, but for our purposes, this is not important.

Now suppose that $k = \mathbb{Q}_p \times k'$, for some quadratic étale algebra k', with ring of integers $A_{k'} = \mathbb{Z}_p[\alpha]$. To give a morphism $j : A \to J_3$, it is necessary and sufficient to specify $m = j(1,0)$ and $n = j(0,\alpha)$. The elements m and n must satisfy

$$\begin{cases} T(m, I) = 1, \\ m^\# = 0, \\ T(m, n) = 0, \\ T(n, I)m = (I - m) \times n \\ T(n, I) = \mathrm{Tr}_{k'}(\alpha) \\ \det(m + n) = \mathbb{N}_{k'}(\alpha), \end{cases} \tag{3.3}$$

since these are satisfied by $(1,0)$ and $(0,\alpha)$ in A. Conversely, it is not difficult to see that any pair (m,n) satisfying the above gives a morphism $A \to J_3$. In the language of Jordan algebras, the first two equations of (3.3) say that m is a primitive idempotent; as an example, take

$$m = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

For this m, the next two equations of (3.3) simply say that the element n lies in the sublattice J consisting of elements of the form

$$n = \begin{pmatrix} 0 & 0 & 0 \\ 0 & b & x \\ 0 & \bar{x} & c \end{pmatrix}.$$

Indeed, the two equations give a characterization of such elements in J_3 [Sp, Proposition 10.3(ii)]. Note that J has a natural structure of a pointed quadratic space over $\mathbb{Z}_p$, with quadratic form

$$n \mapsto \det(m+n),$$

and distinguished point $I - m$. This pointed quadratic space is in fact isomorphic to J_2; this is clear for the example above, and we shall see in Proposition 5.3 that any primitive idempotent in J_3 is conjugate to the above m by an element of $\underline{G}(\mathbb{Z}_p)$. Now the last two equations of (3.3) say that n determines an embedding $A_{k'} \to J$ of pointed quadratic spaces.

Hence, when $k = \mathbb{Q}_p \times k'$, we define $\underline{X}$ to be the closed subscheme of $J_3 \times J_3$ such that for any $\mathbb{Z}_p$-algebra B, $\underline{X}(B)$ consists of those pairs $(m,n) \in (J_3 \otimes B)^2$ satisfying the equations in (3.3). We note that here, A is still singly generated over $\mathbb{Z}_p$, unless $p = 2$ and $A = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. However, it is more convenient to define $\underline{X}$ as we have done, so as to apply the results of [BT2] later.

In all cases, for any $\mathbb{Z}_p$-algebra B, $\underline{X}(B)$ is the set of morphisms $j : A \otimes B \to \Lambda \otimes B$. If B is flat over $\mathbb{Z}_p$, then these morphisms are injective, but this need not be the case if $B = A \otimes \mathbb{Z}/p\mathbb{Z}$. For example, if k is a ramified cubic field, then $\underline{X}(\mathbb{Z}/p\mathbb{Z})$ is the set of all elements $x \in \kappa$ which satisfy $x^3 = 0$, and the subset of embeddings corresponds precisely to the subset of those x for which $x^2 \neq 0$. We have:

Lemma 3.4. *The image of the reduction map*

$$\underline{X}(\mathbb{Z}_p) \to \underline{X}(\mathbb{Z}/p\mathbb{Z})$$

is precisely the subset of embeddings.

Proof. We give the proof in the case when k is a cubic field; the other cases are similar. To show that the image of the reduction map is contained in the subset of embeddings, we need to show that

$$pJ_3 \cap A = pA,$$

when A is considered a sublattice of J_3 by the integral embedding under consideration. It is clear that $pA \subset pJ_3 \cap A$. On the other hand, suppose that $a = p \cdot m \in A \cap pJ_3$. Then $m \in k \cap J_3$. Since the maximal order A is characterized as the set of elements of k integral over $\mathbb{Z}_p$, we have $k \cap J_3 = A$, and the desired inclusion follows.

Conversely, suppose that $A = \mathbb{Z}_p[\alpha]$, where α has characteristic polynomial P. Suppose that $m_1 \in J_3$ has the property that $m_1 \bmod p$ has minimal polynomial P (thus giving rise to an embedding modulo p). We show that, for positive integers i, one can successively find $m_i \in J_3$ such that

$$\begin{cases} P(m_i) = 0 \bmod p^i; \\ m_{i+1} = m_i \bmod p^i. \end{cases}$$

The inverse limit of the m_i's then defines an element m of $\underline{X}(\mathbb{Z}_p)$ such that $m = m_1 \bmod p$. Suppose we have found m_i, and let $m_{i+1} = m_i + p^i n_i$ for some $n_i \in J_3$ to be determined. From the defining equations (3.2) for $\underline{X}$, we see that, for $P(m_{i+1})$ to be divisible by p^{i+1}, n_i must satisfy equations of the form

$$\begin{cases} T(n_i, I) = a_i \pmod p; \\ T(n_i, m_1) = b_i \pmod p; \\ T(n_i, m_1^2) = c_i \pmod p, \end{cases} \tag{3.5}$$

for some $a_i, b_i, c_i \in \mathbb{Z}_p$. Since $m_1 \pmod p$ gives rise to an embedding, the 3 linear forms

$$\begin{cases} n \mapsto T(n, I) \\ n \mapsto T(n, m_1) \\ n \mapsto T(n, m_1^2) \end{cases}$$

on $J_3 \otimes \mathbb{Z}/p\mathbb{Z}$ are linearly independent, and hence we can always solve for n_i in (3.5). This proves the lemma. □

As a consequence, the reduction map is not always surjective, and $\underline{X}$ is in general not smooth. In fact, the smooth locus of $\underline{X} \times \mathbb{Z}/p\mathbb{Z}$ is precisely the open subvariety of embeddings.

4. **The Main Theorem**

In this section, we shall state the main theorem of the paper. We have defined the affine scheme $\underline{X}$ in the previous section. In all cases, it is clear from the definition that $\underline{G}$ acts naturally on $\underline{X}$. Let X be the generic fiber of $\underline{X}$. By results of Jacobson [J1, J2], X is a homogeneous space for G, and by results of Jacobson [J1] and Soda [So], the stabilizer H of an element of $X(\mathbb{Q}_p)$ is a quasi-simple linear algebraic group which is quasi-split and of type given by the following table.

G	H
G_2	SU_3^k
SO_9	SO_8^k
F_4	$Spin_8^k$

By Lemma 3.1, $\underline{X}(\mathbb{Z}_p)$ is non-empty. Now fix an arbitrary $j_0 \in \underline{X}(\mathbb{Z}_p)$, and consider the morphism:

$$\begin{aligned} f : \underline{G} &\longrightarrow \underline{X} \\ g &\mapsto g \cdot j_0. \end{aligned}$$

Let Lie($\underline{G}$) be the Lie algebra of $\underline{G}$, and let $T(\underline{X})$ be the tangent space of $\underline{X}$ at the element $j_0 \in \underline{X}(\mathbb{Z}_p)$. The morphism f induces a map of tangent spaces

$$df : \mathrm{Lie}(\underline{G}) \longrightarrow T(\underline{X}).$$

Let $\underline{H}$ be the fiber of f over j_0. It is an integral model for H, with $\underline{H}(\mathbb{Z}_p)$ equal to the stabilizer of j_0 in $\underline{G}(\mathbb{Z}_p)$.

Having introduced such a large number of notations, the main result of this paper can be neatly stated as:

Theorem 4.1. *(i) The morphism f is smooth. In particular, $\underline{H}$ is a smooth affine group scheme over $\mathbb{Z}_p$.*

(ii) $\underline{G}(\mathbb{Z}_p)$ acts transitively on $\underline{X}(\mathbb{Z}_p)$.

(iii) $\underline{H}(\mathbb{Z}_p)$ is a special maximal parahoric subgroup of $H(\mathbb{Q}_p)$.

The proof of this theorem occupies the rest of the paper.

5. **Smoothness and Conjugacy**

The goal of this section is to prove Theorem 4.1(i) and (ii). We first make a series of reductions through the following lemmas.

Lemma 5.1. *To show the smoothness of $f : \underline{G} \to \underline{X}$, it is necessary and sufficient to show the smoothness of $f \times \mathbb{Q}_p$ and $f \times \mathbb{Z}/p\mathbb{Z}$.*

Proof. This is [EGA4, Prop. 17.8.2]. See also [GY, Lemma 5.5.1]. □

Lemma 5.2. *Let l denote $\mathbb{Q}_p$ or $\mathbb{Z}/p\mathbb{Z}$. To show that $f \times l$ is smooth, it suffices to show that the induced map on tangent spaces*

$$df \otimes l : Lie(\underline{G}) \otimes l \longrightarrow T(\underline{X}) \otimes l$$

is surjective.

Proof. By [EGA4, Cor. 17.7.3], it suffices to show the smoothness of $f \times \bar{l}$, where $\bar{l}$ is the algebraic closure of l. Then it suffices to show that $f \times \bar{l}$ is smooth at every closed point of $\underline{G} \times \bar{l}$. Using translation, it is enough to show that $f \times \bar{l}$ is smooth at the identity element. By [EGA4, Thm. 17.11.1], this would follow if the induced map of tangent spaces

$$d(f \times \bar{l}) = df \otimes \bar{l} : \mathrm{Lie}(\underline{G}) \otimes \bar{l} \longrightarrow T(\underline{X}) \otimes \bar{l}$$

is surjective. For this, it is clearly enough to check the surjectivity of $df \otimes l$. □

Hence, to prove Theorem 4.1(i), it suffices to consider the map $df \otimes l$ for $l = \mathbb{Q}_p$ and $\mathbb{Z}/p\mathbb{Z}$. In each case, we shall be able to compute the dimension of $T(\underline{X}) \otimes l$; thus we are reduced to showing that the kernel of $df \otimes l$ has the appropriate dimension. If $\mathrm{char}(l) \neq 2$, many of the results we need concerning $\mathrm{Ker}(df \otimes l)$ are due to Jacobson. To deal with the characteristic 2 case, we shall sometimes resort to the use of computer, though in the case $\Lambda = R$ or J_2, everything can be checked by hand. We refer the reader to the Appendix in Section 14 for the description of the computer calculations we use below, and simply note that in all these computations, Zorn's model for R and the Tits model for J_3 are used in place of the usual models.

We now begin the proof of Theorem 4.1(i). First, consider the case when k is a quadratic algebra or a cubic field. Then $\underline{X} \times l$ is a closed subscheme of $\Lambda \otimes l$, so that $T(\underline{X}) \otimes l$ can be regarded as a vector subspace of $\Lambda \otimes l$. For example, if k is a cubic field, and $m_0 = j_0(\alpha)$, then $T(\underline{X}) \otimes l$ is the subspace of elements $m \in J_3 \otimes l$ which satisfy

$$\begin{cases} T(m, I) = 0, \\ T(m, m_0) = 0, \\ T(m, m_0^{\#}) = 0. \end{cases}$$

Hence, $T(\underline{X}) \otimes l$ is precisely the subspace of $J_3 \otimes l$ which is orthogonal to the image of $j_0 \otimes l$. This is also true in the quadratic case. By Lemma 3.4,

$$j_0 \otimes l : A \otimes l \longrightarrow J_3 \otimes l$$

is injective. It is thus easy to compute the dimension of $T(\underline{X}) \otimes l$.

Consider the case $\Lambda = R$. Then $T(\underline{X}) \otimes l$ has dimension 6, so we need to show that $\mathrm{Ker}(df \otimes l)$ has dimension 8. If $\mathrm{char}(l) \neq 2$, and $A \otimes l$ is étale (for example, if $l = \mathbb{Q}_p$), Jacobson showed that $\mathrm{Ker}(df \otimes l)$ is isomorphic to $\mathfrak{sl}_3$ over the algebraic closure of l [J3, Proposition 3, Pg. 12]. This can also be checked in the case of characteristic 2. If $A \otimes l$ is non-étale, then one can check that $\mathrm{Ker}(df \otimes l)$ is the derived algebra of a maximal parabolic subalgebra of $\mathrm{Lie}(\underline{G}) \otimes l = \mathfrak{g}_2$. In all cases, we see that $\mathrm{Ker}(df \otimes l)$ has dimension 8.

The case when $\Lambda = J_2$ can also be checked easily. Here, the tangent space $T(\underline{X}) \otimes l$ has dimension 8; so we need to show that $\mathrm{Ker}(df \otimes l)$ has dimension 28. We omit the details and simply describe the answers. If $A \otimes l$ is étale, then $\mathrm{Ker}(df \otimes l)$ is isomorphic to $\mathfrak{so}_8$ over the algebraic closure of l. If $A \otimes l$ is non-étale, then $\mathrm{Ker}(df \otimes l)$ is the derived algebra of a maximal parabolic subalgebra, with Levi subalgebra $\mathfrak{so}_7$. In all cases, we find that $\mathrm{Ker}(df \otimes l)$ has dimension 28.

Now suppose $\Lambda = J_3$ and k is a cubic field. The tangent space $T(\underline{X}) \otimes l$ has dimension 24; so we need to show that $\mathrm{Ker}(df \otimes l)$ has dimension 28. If $\mathrm{char}(l) \neq 2$, and $A \otimes l$ is étale, Jacobson showed that $\mathrm{Ker}(df \otimes l)$ is isomorphic to $\mathfrak{spin}_8$ over the algebraic closure of l [J3, §5, Theorem 6], and hence has dimension 28. The case of characteristic 2 can be checked by computer. If $A \otimes l$ is non-étale, i.e. k is a ramified extension of $\mathbb{Q}_p$, then nothing seems to be known about $\mathrm{Ker}(df \otimes l)$ even when $\mathrm{char}(l) \neq 2$. Here, we check by computer that $\mathrm{Ker}(df \otimes l)$ has dimension 28, and in the Appendix (c.f. Example 3), we describe in detail how the computation is done here. Hence in all cases, we find that $\mathrm{Ker}(df \otimes l)$ has the required dimension.

Finally, we come to the case when $k = \mathbb{Q}_p \times k'$, with k' quadratic. We first prove the following Proposition.

Proposition 5.3. *Let $\underline{Y}$ be the closed subscheme of J_3 consisting of primitive idempotents, i.e. elements m satisfying:*

$$\begin{cases} T(m, I) = 1, \\ m^{\#} = 0. \end{cases}$$

Let $m_0 \in \underline{Y}(\mathbb{Z}_p)$ and consider the morphism

$$\begin{aligned}\varphi :&\underline{G} \to \underline{Y}\\ &g \mapsto g \cdot m_0.\end{aligned}$$

Then

(i) φ is smooth.

(ii) $\underline{G}(\mathbb{Z}_p)$ acts transitively on $\underline{Y}(\mathbb{Z}_p)$.

(iii) Let $\underline{H}_1 = \varphi^{-1}(m_0)$. Then its generic fiber H_1 is the group $Spin_9$ and $\underline{H}_1(\mathbb{Z}_p)$ is a hyperspecial maximal compact subgroup of $\underline{H}_1(\mathbb{Q}_p)$, i.e. $\underline{H}_1$ is the Chevalley group scheme of $Spin_9$.

(iv) Let J be the sublattice of J_3 consisting of elements n satisfying

$$\begin{cases} T(m_0, n) = 0, \\ T(n, I)m_0 = (I - m_0) \times n. \end{cases}$$

Then J has a natural structure of a pointed quadratic space, which is isomorphic to J_2 and stable under $\underline{H}_1$. The restriction of $\underline{H}_1$ to J defines the natural isogeny $\pi : \underline{H}_1 \to Aut(J) = \underline{SO}_9$.

Proof. Without loss of generality, we set:

$$m_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in J_3.$$

Then, as we have seen in Section 2, J is the sublattice consisting of elements of the form:

$$n = \begin{pmatrix} 0 & 0 & 0 \\ 0 & b & x \\ 0 & \bar{x} & c \end{pmatrix}.$$

All assertions of (iv) have been noted before, except for the last.

Let $T(\underline{Y})$ be the tangent space of $\underline{Y}$ at m_0. By Lemmas 5.1 and 5.2, to show that φ smooth, it suffices to show that the induced map on tangent spaces

$$d\varphi \otimes l : \mathrm{Lie}(\underline{G}) \otimes l \longrightarrow T(\underline{Y}) \otimes l \tag{5.4}$$

is surjective, for $l = \mathbb{Q}_p$ and $\mathbb{Z}/p\mathbb{Z}$. Now the tangent space $T(\underline{Y}) \otimes l$ is the subspace of those elements $m \in J_3 \otimes l$ satisfying:

$$\begin{cases} T(m, I) = 0, \\ m_0 \times m = 0, \end{cases} \tag{5.5}$$

which is precisely the subspace of elements of the form:

$$m = \begin{pmatrix} 0 & z & \bar{y} \\ \bar{z} & 0 & 0 \\ y & 0 & 0 \end{pmatrix}. \tag{5.6}$$

In particular, $T(\underline{Y}) \otimes l$ has dimension 16. Hence, to prove (i), we need to show that the dimension of the kernel of $d\varphi \otimes l$ is 36. If the characteristic of l is not 2, then it is a result of Jacobson [J2, Chap. IX, Theorem 16, Pg. 407] that the kernel of $d\varphi \otimes l$ is the Lie algebra $\mathfrak{spin}_9$, which has dimension 36. If $\mathrm{char}(l) = 2$, we verify the required result on the dimension using the computer, as explained in Example 1 in the Appendix (actually the computer verification works over $\mathbb{Z}$, and so it checks the result in all characteristics). This proves (i), i.e. that φ is smooth.

By (i), $\underline{H}_1$ is smooth and each of its fibers has dimension 36. By restricting the action of $\underline{H}_1$ to J above, we obtain a morphism

$$\eta : \underline{H}_1 \to \mathrm{Aut}(J). \tag{5.7}$$

One can check that the kernel of η is the finite group scheme μ_2. Indeed, let J' be the sublattice of elements of J_3 satisfying (5.5); this is precisely the sublattice of elements of the form in (5.6). Then $\underline{H}_1$ preserves J', and any element $g \in \mathrm{Ker}(\eta)(B)$, where B is any $\mathbb{Z}_p$-algebra, is completely determined by its action on $J' \otimes B$. One can then check that the action of $g \in \mathrm{Ker}(\eta)(B)$ on $J' \otimes B$ is scalar multiplication by some $\lambda \in B$ satisfying $\lambda^2 = 1$, thus identifying $\mathrm{Ker}(\eta)$ with μ_2. In fact, this can also be verified using the computer, as we explain in Example 2 of Section 14.

Let $\underline{H}_1^0$ be the connected component of $\underline{H}_1$. Then the morphism

$$\eta \times l : \underline{H}_1^0 \times l \to \mathrm{Aut}(J) \times l \cong SO_9$$

is an isogeny, since it has finite kernel and both sides are connected with the same dimension. In fact, if $\mathrm{char}(l) \neq 2$, it was shown by Jacobson [J2, Chap. IX, Theorem 4, Pg. 376] that $\underline{H}_1 \times l$ is the group $Spin_9$. In any case, the above shows that the special fiber of the smooth group scheme $\underline{H}_1^0$ is reductive. By results of Bruhat and Tits [BT1], this implies that $\underline{H}_1$ is connected, and $\underline{H}_1(\mathbb{Z}_p)$ is a hyperspecial maximal compact subgroup of $H_1(\mathbb{Q}_p)$. Hence we have shown (iii), as well as the last assertion of (iv).

It remains to prove (ii). If $m \in \underline{Y}(\mathbb{Z}_p)$, then $\underline{Y}_m := \varphi^{-1}(m)$ is smooth over $\mathbb{Z}_p$ by (i). Hence the natural map $\underline{Y}_m(\mathbb{Z}_p) \to \underline{Y}_m(\mathbb{Z}/p\mathbb{Z})$ is surjective, and to prove (ii), it suffices to show that $\underline{Y}_m(\mathbb{Z}/p\mathbb{Z})$ is non-empty, or equivalently, that $\underline{G}(\mathbb{Z}/p\mathbb{Z})$ acts transitively on $\underline{Y}(\mathbb{Z}/p\mathbb{Z})$. By the above, we certainly have

$$\#\underline{Y}_m(\mathbb{Z}/p\mathbb{Z}) \geq \#\underline{G}(\mathbb{Z}/p\mathbb{Z})/\#\underline{H}_1(\mathbb{Z}/p\mathbb{Z}),$$

with equality if and only if $\underline{G}(\mathbb{Z}/p\mathbb{Z})$ acts transitively. But it was shown in [J4, Pg. 91-92] that

$$\#\underline{Y}_m(\mathbb{Z}/p\mathbb{Z}) = \#\underline{G}(\mathbb{Z}/p\mathbb{Z})/\#\underline{H}_1(\mathbb{Z}/p\mathbb{Z}),$$

and hence (ii) is proved. □

We can now prove the smoothness of f when $k = \mathbb{Q}_p \times k'$. Recall that in this case, $\underline{X}$ is a closed subscheme of $J_3 \times J_3$. Let π_1 and π_2 be the projection maps onto the first and second factor respectively. Then π_1 restricts to a map

$$\pi_1 : \underline{X} \to \underline{Y},$$

where $\underline{Y}$ is as defined in Proposition 5.3, and we have

$$\varphi = \pi_1 \circ f, \tag{5.8}$$

for the appropriate choice of m_0. With $\underline{H}_1 = \varphi^{-1}(m_0)$, we can consider the restriction of $\pi_2 \circ f$ to $\underline{H}_1$. This gives a morphism

$$\pi_2 \circ f : \underline{H}_1 \longrightarrow J \subset J_3, \tag{5.9}$$

which by Proposition 5.3(iv) factors as

$$\underline{H}_1 \xrightarrow{\pi} \mathrm{Aut}(J) \xrightarrow{f'} \underline{X}' \hookrightarrow J \tag{5.10}$$

where $\underline{X}'$ is the affine subscheme of J parametrizing the embeddings $A_{k'} \to J$ of pointed quadratic spaces. Note that we have already shown that the morphism $f' : \underline{\mathrm{Aut}}(J) \to \underline{X}'$ is smooth.

Now we need to show that $\mathrm{Ker}(df \otimes l)$ has dimension 28. By (5.8), we have

$$\mathrm{Ker}(df \otimes l) \hookrightarrow \mathrm{Ker}(d\varphi \otimes l) = \mathrm{Lie}(\underline{H}_1) \otimes l.$$

Indeed, from (5.10), it is precisely the kernel of $(df' \otimes l) \circ (d\pi \otimes l)$. If the characteristic of l is not 2, then $d\pi \otimes l$ is an isomorphism and $\mathrm{Ker}(df' \otimes l)$ has dimension 28, and so we are done. There is a slight subtlety when $\mathrm{char}(l) = 2$: $d\pi \otimes l$ has a 1-dimensional kernel, since μ_2 is not smooth over l. Nevertheless, it is easy to see that $\mathrm{Ker}(df' \otimes l)$ is not contained in the image of $d\pi \otimes l$, so that the kernel of $(df' \otimes l) \circ (d\pi \otimes l)$ does have dimension 28, as required.

We have now proven Theorem 4.1(i) in all cases. Theorem 4.1(ii) now follows from the following lemma, as in the proof of Proposition 5.3(ii):

Lemma 5.11. *$\underline{G}(\mathbb{Z}/p\mathbb{Z})$ acts transitively on the image of $\underline{X}(\mathbb{Z}_p)$ in $\underline{X}(\mathbb{Z}/p\mathbb{Z})$.*

Proof. It suffices to check that any two elements in $\underline{X}(\mathbb{Z}/p\mathbb{Z})$, whose corresponding morphisms are embeddings, are conjugate under $\underline{G}(\mathbb{Z}/p\mathbb{Z})$.

If $\Lambda = R$, the required result can be found in [KMRT, Corollary 33.21] for $A \otimes \mathbb{Z}/p\mathbb{Z}$ étale, and in [A, Theorem 2] for $A \otimes \mathbb{Z}/p\mathbb{Z}$ non-étale. For $\Lambda = J_2$, the required result is essentially a consequence of Witt's theorem [B, Pg. 71, Theorem 1], and we omit the details.

Now consider $\Lambda = J_3$. If $k = \mathbb{Q}_p \times k'$, then we have seen in the proof of Proposition 5.3 that $\underline{G}(\mathbb{Z}/p\mathbb{Z})$ acts transitively on the primitive idempotents of κ, and the stabilizer is the group $Spin_9(\mathbb{Z}/p\mathbb{Z})$. This reduces us to the case $\Lambda = J_2$, and the result follows from the fact that $Spin_9(\mathbb{Z}/p\mathbb{Z})$ acts transitively on $\underline{G}(\mathbb{Z}/p\mathbb{Z})/\underline{H}(\mathbb{Z}/p\mathbb{Z})$.

Finally, we consider the case when k is a cubic field. If $p \neq 2$, then the transitivity is a result of Jacobson [J2, Chap. IX, Theorem 10, Pg. 389]. If $p = 2$, let N be the order of the image of $\underline{X}(\mathbb{Z}_p)$ in $\underline{X}(\mathbb{Z}/p\mathbb{Z})$. Then certainly,

$$N \geq \#\underline{G}(\mathbb{Z}/p\mathbb{Z})/\#\underline{H}(\mathbb{Z}/p\mathbb{Z}).$$

Now a brute-force enumeration using the computer shows that in fact we have equality above. □

This concludes the proof of Theorem 4.1(i) and (ii).

6. The lattice $L = A^\perp$

It remains to prove Theorem 4.1(iii), i.e. that $\underline{H}(\mathbb{Z}_p)$ is a special maximal parahoric subgroup. In this section, we outline the strategy of the proof.

Fix an integral embedding $j_0 \in \underline{X}(\mathbb{Z}_p)$, which induces an embedding of k into $F = \Lambda \otimes \mathbb{Q}_p$. We identify k with its image in F, and let $k^\perp$ denote the orthogonal complement of k with respect to the symmetric bilinear form T. Then $k^\perp$ is a rational representation of H. As we noted in the proof of Lemma (3.4), it is clear that $\Lambda \cap k = A$. Let A^* denote the dual lattice of A in k. Then A^* is equal to the inverse of the different ideal $\mathfrak{D}$ of A. Set

$$L = \Lambda \cap k^\perp.$$

and let L^* be the dual lattice of L in $k^\perp$. We have:

Lemma 6.1. *The lattice L^* (respectively A^*) is the projection of Λ onto $k^\perp$ (respectively k), and there is a natural isomorphism*

$$\theta : A^*/A \cong L^*/L$$

of abelian groups. This isomorphism is induced by the map which, to $x \in A^*$, assign the unique $y(\ mod\ L)$ satisfying $x + y \in \Lambda$. The natural bilinear forms

$$T : A^*/A \times A^*/A \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

$$L^*/L \times L^*/L \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

satisfy

$$T(\theta x, \theta x') = -T(x, x') \quad (mod\ \mathbb{Z}_p).$$

Proof. Since

$$A + L \subset \Lambda \subset A^* + L^*,$$

projection onto the first and second factor defines injections

$$\Lambda/A + L \hookrightarrow \begin{cases} A^*/A, \\ L^*/L. \end{cases}$$

Hence,

$$N = \#(\Lambda/A + L) \leq \begin{cases} \#(A^*/A), \\ \#(L^*/L). \end{cases}$$

On the other hand, since Λ is unimodular with respect to T, we must have

$$\#(A^*/A) \cdot \#(L^*/L) = N^2,$$

so that the above two injections are isomorphisms. This proves the first assertion of the lemma, as well as the existence of θ. Finally, since $x + \theta x \in \Lambda$ for $x \in A^*$, we have

$$T(x, x') + T(\theta x, \theta x') = T(x + \theta x, x' + \theta x') \in \mathbb{Z}_p,$$

which proves the last assertion. □

Let K_L denote the the stabilizer of L in $H(\mathbb{Q}_p)$. Clearly, $\underline{H}(\mathbb{Z}_p) \hookrightarrow K_L$. Indeed we have:

Lemma 6.2.

$$\underline{H}(\mathbb{Z}_p) = \{g \in K_L : (g-1)L^* \subset L\}.$$

Proof. If $y \in L^*$, then there exists $x \in A^*$ such that $x + y \in \Lambda$, by Lemma 6.1. Since $\underline{H}(\mathbb{Z}_p)$ is the subgroup of $H(\mathbb{Q}_p)$ which stabilizes Λ, for $g \in \underline{H}(\mathbb{Z}_p)$, $(g-1)(y) = (g-1)(x+y)$ lies in $\Lambda \cap k^\perp = L$, as required. Conversely, any $z \in \Lambda$ can be expressed as $x + y$ with $x \in A^*$ and $y \in L^*$. Hence, if $g \in K_L$ satisfies $(g-1)L^* \subset L$, then $g(z) = z + (g(y) - y) \in \Lambda$, so that g stabilizes Λ. □

With this lemma, our strategy to prove Theorem 4.1(iii) will be to show that K_L is a special maximal compact subgroup of $H(\mathbb{Q}_p)$, and then to identify those elements $g \in K_L$ which satisfy $(g-1)L^* \subset L$. In particular, it suffices to work with the lattice L in the representation $k^\perp$ of $H(\mathbb{Q}_p)$. It will turn out that in fact $\underline{H}(\mathbb{Z}_p) = K_L$ in all cases, except when $\Lambda = J_2$ and k is a ramified quadratic extension of $\mathbb{Q}_p$.

7. The Group Scheme $\underline{H}$: Quadratic Case

In this section, we carry out the strategy laid out in the previous section, and prove Theorem 4.1(iii) when k is not a cubic field.

We first consider the case $\Lambda = R$, so that $H = SU_3^k$. The 6-dimensional $\mathbb{Q}_p$-vector space $k^\perp$ has the structure of an k-vector space. Indeed, if $\alpha \in k$ and $x \in k^\perp$, then one shows easily that $\alpha \cdot x \in k^\perp$ [J1]. Further, L is an A-submodule. There is a natural hermitian form on the k-vector space $k^\perp$ defined as follows. If $x, y \in k^\perp$, then write:

$$x \cdot y = -h(x,y) + x \times y,$$

with $h(x,y) \in k$ and $x \times y \in k^\perp$. Then h is a hermitian form on $k^\perp$ (see [J1] and [KMRT, Pg. 507, Ex. 6]), and Jacobson showed in [J1] that the action of H on $k^\perp$ identifies H with $SU(k^\perp, h)$, the special unitary group of the hermitian space $(k^\perp, h)$. Moreover, if $x, y \in L$, then $h(x,y) \in A^*$, and $h(x,x) = \mathbb{N}(x) \in \mathbb{Z}_p$. Further, if we let

$$\tilde{L} = \{x \in k^\perp : h(x, L) \subset A^*\},$$

then one sees easily that $\tilde{L} = L^*$. We claim that the A-module L is a maximal lattice in the hermitian space $(k^\perp, h)$, maximal with respect to the property that $h(x,x) \in \mathbb{Z}_p$ for all $x \in L$. Indeed, L must be contained in some maximal lattice M, and M satisfies $\#\tilde{M}/M = \#A^*/A$ (see[GHY, Sections 3 and 5]); hence the claim follows in view of Lemma 6.1.

By results of Bruhat and Tits [BT2], the stabilizer K_L of the maximal lattice L is a special maximal compact subgroup of $H(\mathbb{Q}_p)$ (see also [GHY, Section 3]). Further, by [GHY, Lemma 5.6], any $g \in K_L$ satisfies

$$(g-1)\tilde{L} \subset L.$$

Hence, in view of Lemma 6.2, $\underline{H}(\mathbb{Z}_p) = K_L$ and we have proven Theorem 4.1(iii) in the case $\Lambda = R$.

The case $\Lambda = J_2$ can be similarly treated, and we shall only give a brief sketch. Here $(k^\perp, \det)$ is a nondegenerate quadratic space, and via its action on $k^\perp$, H is identified with the special orthogonal group of this quadratic space. One checks as above, using Lemma 6.1, that L is a maximal lattice in $k^\perp$. Again, by [BT2], K_L is a special maximal compact subgroup (see also [GHY, Section 6]). Let $\underline{H}_1$ be the smooth group scheme underlying the special maximal compact subgroup K_L by Bruhat-Tits theory, and let $\underline{H}_1^0$ be its connected

component. Note that $\underline{H}_1$ is connected unless k is a ramified quadratic extension, in which case $\underline{H}_1^0$ is of index two in $\underline{H}_1$. Now by [GHY, Proposition 6.15], $g \in K_L$ satisfies $(g-1)L^* \subset L$ if and only if $g \in \underline{H}_1^0(\mathbb{Z}_p)$. Hence $\underline{H}(\mathbb{Z}_p) = \underline{H}_1^0(\mathbb{Z}_p)$ is a maximal parahoric subgroup.

Note that, up to conjugacy by the adjoint group, the special maximal parahoric subgroup is uniquely determined, except in the case when $\Lambda = R$ and k is a ramified quadratic extension, where there are two possibilities. These two possibilities can be distinguished by their maximal reductive quotient, which is either SL_2 or SO_3. The results of [BT2] showed that the special maximal parahoric subgroup arising here is the one whose maximal reductive quotient is SL_2.

Finally, consider the case when $k = \mathbb{Q}_p \times k'$, with k' quadratic. Here, the required result follows immediately from Proposition 5.3 and the result for $\Lambda = J_2$ shown above; we leave the details to the reader. We have thus proven Theorem 4.1 in all cases, except when k is a cubic field.

8. **Springer Decomposition and Twisted Composition**

In the previous section, we have used crucially the results of Bruhat and Tits [BT2], who described the building and the parahoric subgroups of $H(\mathbb{Q}_p)$ in terms of the standard representation when H is a classical group. Unfortunately, when k is a cubic field, the group H is a trialitarian form of $Spin_8$, which is not covered in [BT2]. Hence, we need to extend the results to [BT2] to such groups, and this is the objective of Sections 8 to 13. Fortunately, all we need is to be able to detect the special maximal compact subgroup, and not an arbitrary parahoric subgroup; so it suffices to partially carry out the program of [BT2] for such groups (though it will be interesting to carry out the full program).

In this section, we let k be an arbitrary étale cubic algebra (not necessarily a field), and fix an integral embedding $j_0 : A \to J_3$, which induces an embedding $j : k \to F = J_3 \otimes \mathbb{Q}_p$. Our goal in this section is to describe some very rich algebraic structures on $k^\perp$, the orthogonal complement of k in J_3. It will turn out that H is the automorphism group of these structures. We refer the reader to [KMRT, §36 and §38A] for more information on the topics discussed below.

The orthogonal direct sum $F = k \oplus k^\perp$ is known as the **Springer decomposition** of F. The 24-dimensional vector space $k^\perp$ has the additional structure of a k-module, defined as follows. For $\lambda \in k$ and $x \in k^\perp$, the scalar multiplication is given by

$$\lambda \cdot x := -\lambda \times x.$$

Further, for $x \in k^\perp$, if we write:

$$x^\# = -\mathrm{Q}(x) + \text{ß}(x)$$

for $\mathrm{Q}(x) \in k$ and $\text{ß}(x) \in k^\perp$, then Q is a quadratic form on the k-module $k^\perp$, and ß is a quadratic map of the $\mathbb{Q}_p$-vector space $k^\perp$. These satisfy

$$\begin{cases} \text{ß}(\lambda \cdot x) = \lambda^\# \cdot \text{ß}(x), \\ \mathrm{Q}(\text{ß}(x)) = \mathrm{Q}(x)^\#. \end{cases}$$

Let

$$\begin{cases} \mathrm{Q}(x,y) = \mathrm{Q}(x+y) - \mathrm{Q}(x) - \mathrm{Q}(y), \\ ß(x,y) = ß(x+y) - ß(x) - ß(y). \end{cases}$$

Then we have

$$\mathrm{Q}(x, ß(x)) = \det(x) \cdot I.$$

The 4-tuple $(k^\perp, k, \mathrm{Q}, ß)$ forms what is known as a **twisted composition** [KMRT, §36, Pg. 489].

As an example, suppose that $k = \mathbb{Q}_p \times \mathbb{Q}_p \times \mathbb{Q}_p$, embedded into $J_3 \otimes \mathbb{Q}_p$ along the diagonal. Then $k^\perp$ consists of elements of the form

$$x = \begin{pmatrix} 0 & x_3 & \overline{x_2} \\ \overline{x_3} & 0 & x_1 \\ x_2 & \overline{x_1} & 0 \end{pmatrix}$$

with $x_i \in R \otimes \mathbb{Q}_p$. The action of $a = (a_1, a_2, a_3) \in k$ on x is given by:

$$a \cdot x = \begin{pmatrix} 0 & a_3 \cdot x_3 & a_2 \cdot \overline{x_2} \\ a_3 \cdot \overline{x_3} & 0 & a_1 \cdot x_1 \\ a_2 \cdot x_2 & a_1 \cdot \overline{x_1} & 0 \end{pmatrix}.$$

The quadratic form Q is given by

$$\mathrm{Q}(x) = (\mathbb{N}(x_1), \mathbb{N}(x_2), \mathbb{N}(x_3)),$$

and the quadratic map ß is given by:

$$ß(x) = \begin{pmatrix} 0 & \overline{x_1} \cdot \overline{x_2} & x_1 \cdot x_3 \\ x_2 \cdot x_1 & 0 & \overline{x_2} \cdot \overline{x_3} \\ \overline{x_3} \cdot \overline{x_1} & x_3 \cdot x_2 & 0 \end{pmatrix}.$$

The action of H on $k^\perp$ embeds H into the automorphism group of the twisted composition $(k^\perp, k, \mathrm{Q}, ß)$. Soda showed in [So] that H is a form of $Spin_8$. On the other hand, it was shown in [KMRT, Proposition 36.5] that the automorphism group of the twisted composition is also a form of $Spin_8$. Hence the action of H on $k^\perp$ identifies H with the automorphism group of $(k^\perp, k, \mathrm{Q}, ß)$.

9. **More on** $A^\perp$

We continue with the notations of the previous section. Let L be the lattice $A^\perp = J_3 \cap k^\perp$. Then L becomes an A-submodule of $k^\perp$, and on restricting Q and ß to L, we obtain

$$\begin{cases} \mathrm{Q} : L \to A^*, \\ ß : L \to L^*. \end{cases}$$

Let

$$\tilde{L} = \{x \in k^\perp : \mathrm{Q}(x, L) \subset A^*\} \tag{9.1}$$

be the dual lattice of L relative to Q, then because

$$T = \mathrm{Tr}_k \circ \mathrm{Q},$$

(here, Q is the symmetric bilinear form) we find that $\tilde{L} = L^*$.

Assume now that k is a field, and let π be a uniformizer of A. We shall determine the structure of the A-module L^*/L when $p \neq 3$. Note that by Lemma 6.1, we have an isomorphism of abelian groups

$$\theta : A^*/A \cong L^*/L.$$

Hence, if k is unramified over $\mathbb{Q}_p$, $L^* = L$. For the rest of this section, assume that $p \neq 3$ and k is ramified. Then

$$A^*/A = A/\mathfrak{D} = \pi^{-2}A/A$$

as A-modules, so that $\#L^*/L = p^2$. Now we have:

Lemma 9.2. *If $p \neq 2$, then $L^*/L \cong A/\pi^2$ as A-modules. If $p = 2$, then $L^*/L \cong A/\pi \times A/\pi$ as A-modules.*

Proof. If $p \neq 2$, we need to show that πL^* is not contained in L. Suppose on the contrary that $\pi L^* \subset L$. Then we deduce that $\mathrm{Q}(\pi L^*, L^*) \subset A^*$, so that $\mathrm{Q}(L^*, L^*) \subset \pi^{-3}A$. However, consider the element

$$x = \pi^{-2} + y \in J_3,$$

where $y = \theta(\pi^{-2}) \in L^*$. Then from the fact that $x^{\#} \in J_3$, we deduce that $Q(y) \in k$ has valuation -4. This contradiction proves the lemma when $p \neq 2$. We leave the case of $p = 2$ to the reader. □

If $p \neq 2$, the above lemma implies that L^*/L has a unique proper A-submodule. Hence, there is a unique $\mathbb{Z}_p$-lattice $L \subset M \subset L^*$ stable under A. Indeed, we have

$$M = \pi L^* + L.$$

From this, it is easy to see that

$$T : M \times M \longrightarrow \mathbb{Z}_p,$$

and (M, T) is unimodular. Equivalently, $\mathrm{Q}(M) \subset A^*$.

Recall that T induces a symmetric bilinear form

$$T : L^*/L \times L^*/L \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

This actually takes values in $p^{-1}\mathbb{Z}_p/\mathbb{Z}_p$, and $(L^*/L, T)$ is a split rank 2 quadratic space over $\mathbb{Z}/p\mathbb{Z}$. As such, it has 2 isotropic lines. When $p \neq 2$, the above lemma shows that there is a distinguished isotropic line: the unique proper A-submodule M/L of L^*/L. The same is true of the quadratic space $(A^*/A, T)$, which is isomorphic to $(L^*/L, -T)$ under the map θ in Lemma 6.1.

It is natural to ask if θ is an isomorphism of A-modules when $p \neq 2$. One can show that it is not so in general. However, we have:

Lemma 9.3. *The map θ identifies $\pi^{-1}A/A$ with M/L.*

Proof. The proof here is similar to that of the previous lemma. Suppose on the contrary that θ identifies M/L with the other isotropic line in A^*/A. This isotropic line is generated by an element x of valuation -2, so that $x + y \in J_3$ for some $y \in M$. From the fact that $(x + y)^{\#} \in J_3$, we deduce that $\mathrm{Q}(y) \in k$ has valuation -4. However, we have seen that $\mathrm{Q}(y) \in A^*$ for all $y \in M$. This contradiction proves the lemma. □

Let K_M be the stabilizer of M in $H(\mathbb{Q}_p)$. When $p \neq 2, 3$, Lemma 9.2 implies that $K_L \hookrightarrow K_M$. Hence, $\underline{H}(\mathbb{Z}_p) \subset K_L$ acts on the lattices L, M and L^*. As a representation of $K_L = K_{L^*}$, $L/\pi L$ has a 1-dimensional submodule $\pi M/\pi L$, and $L^*/\pi L^*$ has a 7-dimensional submodule $M/\pi L^*$. On the other hand, as a representation of K_M,

$$M/\pi M = L/\pi M \oplus \pi L^*/\pi M.$$

In the proof of Theorem 4.1(iii), we shall show that $\underline{H}(\mathbb{Z}_p) = K_L = K_M$ is s special maximal compact subgroup of $H(\mathbb{Q}_p)$. The facts discussed in this section will not be used in the actual proof. However, they provide us with a better understanding of the special fiber of $\underline{H}$ and help to clarify the proof; when suitably globalized, they provide an interesting way of constructing certain Neimeier lattices, as discussed briefly in [GG, §7 and §8].

10. **Cyclic Compositions**

Henceforth, we assume that k is a cubic field, with ring of integers $A = \mathbb{Z}_p[\alpha]$. In this section, we further assume that k is **Galois** over $\mathbb{Q}_p$, and fix a generator σ of the Galois group $\mathrm{Gal}(k/\mathbb{Q}_p)$. We remark that, although we work over $\mathbb{Q}_p$, the results below are valid over any finite extension of $\mathbb{Q}_p$.

We have introduced the twisted composition $(k^\perp, k, \mathrm{Q}, ß)$ in Section 8. By [KMRT, Lemma 36.1], the 4-tuple

$$(k^\perp, k, q, \beta) = (k^\perp, k, \lambda_{\sigma,\alpha}^{\#}\mathrm{Q}, \lambda_{\sigma,\alpha} \cdot ß)$$

where

$$\lambda_{\sigma,\alpha} := \sigma^2(\alpha) - \sigma(\alpha) \neq 0$$

is again a twisted composition, and for various reasons, it is more convenient to work with this renormalized twisted composition. As before, let

$$\begin{cases} q(x,y) = q(x+y) - q(x) - q(y), \\ \beta(x,y) = \beta(x+y) - \beta(x) - \beta(y). \end{cases}$$

Let $SO(q)$ be the special orthogonal group of $(k^\perp, q)$ (a linear algebraic group over k). Then H is precisely the subgroup of $\mathrm{Res}_{k/\mathbb{Q}_p} SO(q)$ which respects the map β. We remind the reader that we are trying to show that K_L is a special maximal compact subgroup of $H(\mathbb{Q}_p)$. For this, it is necessary for us to be able to decide if an element of $SO(q)(k)$ is in $H(\mathbb{Q}_p)$. However, it is rather difficult to work with the map β, and hence to check whether an element of $\mathrm{Res}_{k/\mathbb{Q}_p} SO(q)$ is in H or not.

Fortunately, there is a refinement of the quadratic map β due to Springer [KMRT, Prop. 36.12, Pg. 496]. More precisely, there is a $\mathbb{Q}_p$-bilinear map

$$k^\perp \times k^\perp \to k^\perp$$

$$(x, y) \mapsto x * y$$

which is σ-linear in x and σ^2-linear in y, and such that

$$\beta(x, y) = x * y + y * x,$$

The composition $*$ satisfies various compatibility conditions with the quadratic form q [KMRT, §36b, Pg. 495], and the 4-tuple $(k^\perp, k, q, *)$ is called a **cyclic composition** relative to σ. Explicitly, $x * y$ can be computed by:

$$\begin{aligned} x * y &= \lambda_\sigma^{-1} \cdot (\beta(\alpha \cdot x, y) - \sigma^2(\alpha) \cdot \beta(x, y)) \\ &= \sigma^2(\alpha) \cdot ß(x, y) - ß(\alpha \cdot x, y). \end{aligned} \tag{10.1}$$

If $\{e_1, ..., e_8\}$ is a basis of the k-vector space $k^\perp$, then the cyclic composition structure is completely determined by the products $e_i * e_j$. Our goal in the remainder of this section is to find a nice basis of $k^\perp$, with a particularly simple multiplication table.

To this end, we need to be very explicit. For the purpose of computation, it is more convenient to work with the Tits model for $F = J_3 \otimes \mathbb{Q}_p$, obtained from the Tits model for J_3 introduced in Section 2 by base extension. Thus

$$F = M_3(\mathbb{Q}_p)^+ \oplus M_3(\mathbb{Q}_p) \oplus M_3(\mathbb{Q}_p),$$

the direct sum of three copies of the space 3×3 matrices with entries in $\mathbb{Q}_p$, and the cubic norm structure $(M_3(\mathbb{Q}_p)^3, N, e, \#, T)$ is defined by the equations in (2.1). Henceforth, we identify F with its Tits model.

To define an embedding of k into F, let k act on itself by left multiplication. This gives an injection of k into $\mathrm{End}_{\mathbb{Q}_p}(k)$, which we identify with $M_3(\mathbb{Q}_p)^+$ using the basis $\{1, \alpha, \alpha^2\}$. This gives an embedding

$$j : k \hookrightarrow F.$$

Further, we also have a group homomorphism $\mathrm{Gal}(k/\mathbb{Q}_p) \to \mathrm{Aut}_{\mathbb{Q}_p}(k)$, given by the action of $\mathrm{Gal}(k/\mathbb{Q}_p)$ on k. Writing σ for the image of σ in $M_3(\mathbb{Q}_p)^+$, we have a decomposition of vector spaces:

$$M_3(\mathbb{Q}_p)^+ = k \oplus k\sigma \oplus k\sigma^2.$$

which realizes $M_3(\mathbb{Q}_p)^+$ as a cyclic algebra, with $\sigma a \sigma^{-1} = \sigma(a)$ for $a \in k$. With these identifications, we see that

$$k^\perp = (k\sigma \oplus k\sigma^2) \oplus M_3(\mathbb{Q}_p) \oplus M_3(\mathbb{Q}_p).$$

Moreover, the k-vector space structure of $k^\perp$ is given by:

$$\lambda \cdot (a_1\sigma + a_2\sigma^2, b, c) = (\sigma^2(\lambda)a_1\sigma + \sigma(\lambda)a_2\sigma^2, \lambda b, c\lambda).$$

Let $e_{i,j}$ denote the 3×3 matrix whose (i, j)-entry is 1, and whose other entries are zero. Then a basis of the 8-dimensional k-vector space $k^\perp$ is given, for $i = 1, 2, 3$, by:

$$\begin{cases} e_i = (0, 0, e_{i,3}), \\ e_{-i} = (0, -e_{1,i}, 0) \\ e_4 = (\lambda_{\sigma,\alpha}^{-1}\sigma, 0, 0), \\ e_{-4} = (\lambda_{\sigma,\alpha}^{-1}\sigma^2, 0, 0). \end{cases}$$

From the definition of q, one checks that $\{e_i, e_{-i}, i = 1, 2, 3, 4\}$ forms a Witt basis for the quadratic space $(k^\perp, q)$, that is,

$$q(e_i, e_j) = \delta_{i,-j}.$$

In particular, the quadratic space $(k^\perp, q)$ is split.

	e_1	e_2	e_3	e_4	e_{-1}	e_{-2}	e_{-3}	e_{-4}
e_1	0	e_{-3}	$-e_{-2}$	0	$-e_{-4}$	0	0	$-e_1$
e_2	$-e_{-3}$	0	e_{-1}	0	0	$-e_{-4}$	0	$-e_2$
e_3	e_{-2}	$-e_{-1}$	0	0	0	0	$-e_{-4}$	$-e_3$
e_4	$-e_1$	$-e_2$	$-e_3$	e_{-4}	0	0	0	0
e_{-1}	$-e_4$	0	0	$-e_{-1}$	0	e_3	$-e_2$	0
e_{-2}	0	$-e_4$	0	$-e_{-2}$	$-e_3$	0	e_1	0
e_{-3}	0	0	$-e_4$	$-e_{-3}$	e_2	$-e_1$	0	0
e_{-4}	0	0	0	0	$-e_{-1}$	$-e_{-2}$	$-e_{-3}$	e_4

TABLE 1. Mulitplication Table for $e_i * e_j$

After a lengthy computation using (10.1), one can work out the multiplication table for the basis $\{e_i\}$ with respect to the composition $*$. This is given in Table 1. One observes that this multiplication table agrees with that of the standard basis elements of the split para-Cayley algebra [KMRT, §34A], as given, for example, in [Gar, §1]. In other words, the $\mathbb{Q}_p$-span of the elements e_i is the split para-Cayley algebra with respect to the composition $*$, and the cyclic composition $(k^\perp, q, *)$ is the one arising naturally from this, in the sense of [KMRT, §36.11]. Now H is precisely the algebraic subgroup of $\mathrm{Res}_{k/\mathbb{Q}_p} SO(q)$ which respects the composition $*$, and with the multiplication table above, it is not too difficult to check if an element g of $SO(q)(k)$ lies in $H(\mathbb{Q}_p)$; it suffices to check that g preserves the 64 products $e_i * e_j$.

11. **A Coherent System of Épinglage**

In this section, we describe a coherent system of épinglage for H, in the sense of [BT1, §4.1.16], using the results of the previous section. Writing H_k for $H \times k$, there is a canonical

embedding $H \hookrightarrow \mathrm{Res}_{k/\mathbb{Q}_p} H_k$, with H the subgroup fixed by the natural action of $\mathrm{Gal}(k/\mathbb{Q}_p)$. By definition, to give a coherent system of épinglage for H is the same as giving a Chevalley-Steinberg system of épinglage for $\mathrm{Res}_{k/\mathbb{Q}_p} H_k$ in the sense of [BT1, §4.1.3]. Now, by [KMRT, Proposition 36.18], we have:

Lemma 11.1. *$Res_{k/\mathbb{Q}_p} H_k$ can be realized as an algebraic subgroup of $Res_{k/\mathbb{Q}_p} SO(q)^3$ in the following way. For any $\mathbb{Q}_p$-algebra k', $Res_{k/\mathbb{Q}_p}(H_k)(k')$ is the subgroup consisting of $(g_1, g_2, g_3) \in SO(q)(k \otimes k')^3$ such that*

$$g_1(x * y) = g_2(x) * g_3(y) \quad \text{for all } x, y \in k^\perp \otimes k'.$$

The group $Gal(k/\mathbb{Q}_p) \cong \mathbb{Z}/3\mathbb{Z}$ operates on $Res_{k/\mathbb{Q}_p} H_k$ by cyclic permutation. The algebraic subgroup fixed by the action of $Gal(k/\mathbb{Q}_p)$ is H, and this realizes the canonical embedding $H \hookrightarrow Res_{k/\mathbb{Q}_p} H_k$.

Without loss of generality, we suppose that σ acts by:

$$\sigma : (g_1, g_2, g_3) \mapsto (g_3, g_1, g_2).$$

Note that the map

$$pr : (g_1, g_2, g_3) \mapsto g_1$$

realizes $\mathrm{Res}_{k/\mathbb{Q}_p} H_k$ as the simply-connected cover of $\mathrm{Res}_{k/\mathbb{Q}_p} SO(q)$.

As in [BT2, §1.14], the Witt basis $\{e_i\}$ determines a maximal torus $\mathrm{Res}_{k/\mathbb{Q}_p} T$ of the group $\mathrm{Res}_{k/\mathbb{Q}_p} SO(q)$, as well as a system of épinglage for the root subgroups relative to $\mathrm{Res}_{k/\mathbb{Q}_p} T$. More precisely, for $(a_1, a_2, a_3, a_4) \in \mathrm{Res}_{k/\mathbb{Q}_p} \mathbb{G}_m^4$, the map

$$t(a_1, a_2, a_3, a_4) : e_i \mapsto a_i \cdot e_i, \tag{11.2}$$

where $a_{-i} = a_i^{-1}$ for $i > 0$, is an element of $\mathrm{Res}_{k/\mathbb{Q}_p} T$, which identifies $\mathrm{Res}_{k/\mathbb{Q}_p} T$ with $\mathrm{Res}_{k/\mathbb{Q}_p} \mathbb{G}_m^4$. Moreover, for fixed $i, j = \pm 1, \pm 2, \pm 3, \pm 4$, there is a corresponding root subgroup $U_{i,j}$ relative to $\mathrm{Res}_{k/\mathbb{Q}_p} T$, whose k'-points are the maps

$$u_{i,j}(x) : e_r \mapsto \begin{cases} e_r, & \text{if } r \neq i, j; \\ e_i + x \circ e_{-j}, & \text{if } r = i; \\ e_j - x \circ e_{-i}, & \text{if } r = j, \end{cases} \tag{11.3}$$

for $x \in \mathrm{Res}_{k/\mathbb{Q}_p} \mathbb{G}_a(k')$, and

$$u_{i,j} : \mathrm{Res}_{k/\mathbb{Q}_p} \mathbb{G}_a \to U_{i,j}$$

is an épinglage for $U_{i,j}$. Note that $U_{i,j} = U_{j,i}$, and the two épinglages $u_{i,j}$ and $u_{j,i}$ differ up to sign. One checks easily that this system of épinglage for $\mathrm{Res}_{k/\mathbb{Q}_p} SO(q)$ is a Chevalley system, in the sense of [BT1, §3.22]. A Chevalley system of épinglage for $\mathrm{Res}_{k/\mathbb{Q}_p} SO(q)$ induces one on the simply-connected cover $\mathrm{Res}_{k/\mathbb{Q}_p} H_k$: one smply takes $pr^{-1}(\mathrm{Res}_{k/\mathbb{Q}_p} T)$ as the maximal torus Z_k for $\mathrm{Res}_{k/\mathbb{Q}_p} H_k$, and the épinglage is given by $pr^{-1} \circ u_{i,j}$, which makes sense since pr is an isomorphism on root subgroups. By abuse of notation, we shall write $U_{i,j}$ and $u_{i,j}$ instead of $pr^{-1}(U_{i,j})$ and $pr^{-1} \circ u_{i,j}$ for the corresponding root subgroup and épinglage of $\mathrm{Res}_{k/\mathbb{Q}_p} H_k$ with respect to Z_k.

Now one checks that Z_k is stabilized by the action of $\mathrm{Gal}(k/\mathbb{Q}_p)$. The subgroup of fixed points is thus a maximal torus Z for H. In fact, for any $\mathbb{Q}_p$-algebra k',

$$Z(k') = \{t(a, a/\mu, \mu/\sigma(a)\sigma^2(a), \sigma^2(a)/\sigma(a)) : a \in k \otimes k', \mu \in k'\}, \tag{11.4}$$

which identifies Z with $\mathbb{G}_m \times \mathrm{Res}_{k/\mathbb{Q}_p}\mathbb{G}_m$, and the maximal split torus $S \subset Z$ with $\mathbb{G}_m^2$. The fact that Z_k is stabilized by $\mathrm{Gal}(k/\mathbb{Q}_p)$ implies that the root subgroups $U_{i,j}$ are permuted by $\mathrm{Gal}(k/\mathbb{Q}_p)$. Using Table 1 above, another lengthy computation shows that the épinglages $(u_{i,j})$ are also permuted (up to sign) by $\mathrm{Gal}(k/\mathbb{Q}_p)$. For example, one checks that

$$(u_{-1,2}(x), u_{-1,2}(\sigma^2(x)), u_{-1,2}(\sigma(x))) \in \mathrm{Res}_{k/\mathbb{Q}_p} H_k,$$

so that

$$\sigma \circ u_{-1,2} \circ \sigma^{-1} = u_{-1,2}.$$

Similarly, one has:

$$(u_{-3,-2}(x), u_{-4,1}(\sigma^2(x)), u_{1,4}(\sigma(x))) \in \mathrm{Res}_{k/\mathbb{Q}_p} H_k,$$

so that

$$\begin{cases} \sigma \circ u_{-3,-2} \circ \sigma^{-1} = u_{1,4}, \\ \sigma \circ u_{1,4} \circ \sigma^{-1} = u_{-4,1}, \\ \sigma \circ u_{-4,1} \circ \sigma^{-1} = u_{-3,-2}. \end{cases}$$

In other words, $(u_{i,j})$ is a Chevalley-Steinberg system of épinglage. Recall that the relative root system Φ of H is of type G_2. Let a and b be (a choice of) the long and short simple roots of Φ respectively. Each element r of Φ indexes a root subgroup U_r of H relative to S. Then the following proposition is the result of the above considerations and gives a coherent system of épinglage for these root subgroups.

Proposition 11.5. *The root subgroups corresponding to the long positive roots of Φ can be chosen to be:*

$$\begin{cases} U_a(\mathbb{Q}_p) = \{u_{-1,2}(x) : x \in \mathbb{Q}_p\}, \\ U_{a+3b}(\mathbb{Q}_p) = \{u_{1,-3}(x) : x \in \mathbb{Q}_p\}, \\ U_{2a+3b}(\mathbb{Q}_p) = \{u_{2,-3}(x) : x \in \mathbb{Q}_p\}. \end{cases}$$

The root subgroups corresponding to short positive roots can be chosen to be:

$$\begin{cases} U_b(\mathbb{Q}_p) = \{u_{-3,-2}(x)u_{-4,1}(\sigma^2(x))u_{1,4}(\sigma(x)) : x \in k\}, \\ U_{a+b}(\mathbb{Q}_p) = \{u_{-1,-3}(x)u_{-4,2}(\sigma^2(x))u_{2,4}(\sigma(x)) : x \in k\}, \\ U_{a+2b}(\mathbb{Q}_p) = \{u_{2,1}(x)u_{4,-3}(\sigma^2(x))u_{-3,-4}(\sigma(x)) : x \in k\}. \end{cases}$$

The root subgroups corresponding to negative roots are similarly described. The collection

$$\begin{array}{ll} u_a = u_{-1,2} & u_{-a} = u_{1,-2} \\ u_{a+3b} = u_{1,-3} & u_{-a-3b} = u_{-1,3} \\ u_{2a+3b} = u_{2,-3} & u_{-2a-3b} = u_{-2,3} \\ u_b = u_{-3,-2} \cdot (u_{-4,1} \circ \sigma^2) \cdot (u_{1,4} \circ \sigma) & u_{-b} = u_{3,2} \cdot (u_{4,-1} \circ \sigma^2) \cdot (u_{-1,-4} \circ \sigma) \\ u_{a+b} = u_{-1,-3} \cdot (u_{-4,2} \circ \sigma^2) \cdot (u_{2,4} \circ \sigma) & u_{-a-b} = u_{1,3} \cdot (u_{4,-2} \circ \sigma^2) \cdot (u_{-2,-4} \circ \sigma) \\ u_{a+2b} = u_{2,1} \cdot (u_{4,-3} \circ \sigma^2) \cdot (u_{-3,-4} \circ \sigma) & u_{-a-2b} = u_{-2,-1} \cdot (u_{-4,3} \circ \sigma^2) \cdot (u_{3,4} \circ \sigma) \end{array}$$

forms a coherent system of épinglage for H relative to S. Here, if r is a long root, $u_r : \mathbb{G}_a \to H$, whereas if r is short, $u_r : Res_{k/\mathbb{Q}_p}\mathbb{G}_a \to H$.

The maximal split torus S and the long root subgroups of H can be very easily described in terms of their action on $k^\perp$. Indeed, the stabilizer in H of the embedding $M_3(\mathbb{Q}_p)^+ \hookrightarrow F$ is isomorphic to SL_3, the action of $g \in SL_3$ being given by:

$$(a, b, c) \mapsto (a, bg^{-1}, gc).$$

The maximal split torus S is then the diagonal torus in SL_3, and the long root subgroups of H are those of SL_3 relative to the diagonal torus. For $i \neq \pm 4$, the lines $k \cdot e_i$ are precisely the non-trivial weight spaces of S, and hence are canonically determined. Moreover, the lines $k \cdot e_{\pm 4}$ are precisely the two isotropic lines in the orthogonal complement of k in $M_3(\mathbb{Q}_p)^+$.

Remarks: We stress again that, though we have restricted ourselves to the base field $\mathbb{Q}_p$ in the above exposition, the results established in Sections 10 and 11, as well as their proofs, remain valid over any finite extension of $\mathbb{Q}_p$ (indeed, over any field of characteristic $\neq 2$). This remark is necessary because in Section 13, we will need to apply the above results on épinglage over a quadratic extension of $\mathbb{Q}_p$.

12. The Group Scheme $\underline{H}$: Galois Case

In this section, we prove (finally) Theorem 4.1(iii) for k a cubic field which is Galois over $\mathbb{Q}_p$. We maintain the notations of the last section.

As we have seen, $(u_{i,j})$ is a Chevalley-Steinberg system of épinglage for $\mathrm{Res}_{k/\mathbb{Q}_p} H_k$, whose associated coherent system of épinglage is given in Proposition 11.5. By [BT1, Theorem 4.2.4], the natural valuation $\tilde{\varphi}$ of root datum associated to $(u_{i,j})$ (which gives a hyperspecial point of the apartment of Z_k) descends to a valuation φ of the root datum associated to $(u_r)_{r\in\Phi}$, which is a special point on the apartment of S [BT1, §4.3.4]. Hence, the stabilizer of φ in $H(\mathbb{Q}_p)$ is a special maximal compact subgroup K of $H(\mathbb{Q}_p)$, which contains the subgroups Z_0 (the maximal compact subgroup of $Z(\mathbb{Q}_p)$), $u_r(\mathbb{Z}_p)$ for r long, and $u_r(A)$ for r short. Since H is simply-connected, these subgroups generate K. Moreover, let M be the lattice generated by the Witt basis $\{e_i\}$, and let K_M be the stabilizer of M in $H(\mathbb{Q}_p)$. Then it is easy to see, using (11.2), (11.3) and (11.4), that $K \subset K_M$, and hence $K = K_M$. In other words, K_M is a special maximal compact subgroup of $H(\mathbb{Q}_p)$. It will turn out that if $p \neq 2, 3$, then this lattice M is the one introduced in Section 9, after Lemma 9.2 (provided we start with an integral embedding j in the construction of the last 2 sections).

So far, the choice of $\alpha \in k$ in the above considerations is not important. We now choose α such that $A = \mathbb{Z}_p[\alpha]$. Then $A = k \cap J_3$, so that j is an integral embedding. Let $L = k^\perp \cap J_3$. If $\tilde{L}$ is the dual lattice of the A-lattice L relative to q, then it is easy to see that $\tilde{L} = L^*$ (and this $\tilde{L}$ is the same as the one introduced in (9.1). Now one checks that

$$L = \{v = \sum_i a_i \cdot e_i \in M : \mathrm{ord}_k(a_4 - a_{-4}) \geq \frac{1}{2} \cdot \mathrm{ord}_k(A^*)\}.$$

Note that $\mathrm{ord}_k(A^*)$ is an even integer since $k/\mathbb{Q}_p$ is Galois, and if $p \neq 3$, it is equal to 0 or 2, depending on whether k is unramified or not. Using Proposition 11.5 and (11.3), one checks that any element g of the subgroup Z_0, $u_r(\mathbb{Z}_p)$ for r long or $u_r(A)$, for r short, stabilizes L,

and satisfies $(g-1)\tilde{L} \subset L$. In particular, by Lemma 6.2, we conclude that

$$\underline{H}(\mathbb{Z}_p) = K_L = K_M = K$$

is a special maximal compact subgroup of $H(\mathbb{Q}_p)$. Observe that if k is unramified over $\mathbb{Q}_p$, $\underline{H}(\mathbb{Z}_p)$ is hyperspecial.

We have thus proven Theorem 4.1(iii) in the case when k is a cubic Galois extension of $\mathbb{Q}_p$.

13. **The Group Scheme $\underline{H}$: Non-Galois Case**

We now consider the case when $k/\mathbb{Q}_p$ is a non-Galois field extension. Let k' be the Galois closure of k in a fixed algebraic closure $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$. Then there is a quadratic extension l of $\mathbb{Q}_p$ such that k' is the compositum of k and l in $\overline{\mathbb{Q}_p}$. Let

$$\langle\tau\rangle = \mathrm{Gal}(k'/k) = \mathrm{Gal}(l/\mathbb{Q}_p),$$

and fix a generator σ of $\mathrm{Gal}(k'/l)$. By the remark at the end of Section 11, the desired results hold for $H \times l$, and the main purpose of this section is to descend those results from l to $\mathbb{Q}_p$.

Let $k = \mathbb{Q}_p[\alpha]$, so that $k' = l[\alpha]$. As in Section 10, the choice of α determines an embedding

$$j : k \hookrightarrow M_3(\mathbb{Q}_p)^+ \hookrightarrow F,$$

so that $k^\perp$ has the structure of a twisted composition $(k^\perp, k, \mathrm{Q}, ß)$. Extending scalars to l gives an embedding

$$j' : k' \hookrightarrow F' = F \otimes l,$$

and the twisted composition $(k'^\perp, k', \mathrm{Q}', ß')$. In view of the remark at the end of Section 11, all the constructions of Sections 10 and 11 can be carried out over l with respect to the Galois extension k'/l, the generator σ and the embedding j' determined by the choice of α. We shall indicate these constructions by a dash. In particular,

$$M_3(l') = M_3(\mathbb{Q}_p) \otimes l = k' \oplus k'\sigma \oplus k'\sigma^2,$$

and we have the renormalized twisted composition $(k'^\perp, k', q', \beta')$, with the Witt basis $\{e'_i, i = \pm1, \pm2, \pm3, \pm4\}$ for the quadratic space $(k'^\perp, q')$ over k'.

The elements of $M_3(l)$ or F' which are in $M_3(\mathbb{Q}_p)$ or F can be recovered as the fixed points of an action of $\mathrm{Gal}(l/\mathbb{Q}_p)$. The action of τ on $M_3(l)$ is given by:

$$a + b\sigma + c\sigma^2 \mapsto \tau(a) + \tau(c)\sigma + \tau(b)\sigma^2.$$

Hence the action of τ on $k'^\perp$ is given by:

$$\sum_i a_i \cdot e'_i \mapsto -\tau(a_4) \cdot e'_{-4} - \tau(a_{-4}) \cdot e'_4 + \sum_{i \neq \pm 4} \tau(a_i) \cdot e'_i.$$

We thus conclude that

$$M_3(\mathbb{Q}_p) = \{a + b\sigma + c\sigma^2 \in M_3(l) : a \in k \text{ and } c = \tau(b) \in k'\},$$

and

$$k^\perp = \{x = a \cdot e'_4 - \tau(a) \cdot e'_{-4} + \sum_{i \neq \pm 4} a_i \cdot e'_i : a \in k' \text{ and } a_i \in k\}.$$

The quadratic form $q' = \lambda_{\sigma,\alpha}^{\#} \mathrm{Q}'$ on $k'^{\perp}$ is defined over k, since $\lambda_{\sigma,\alpha}^{\#} \in k$, and thus descends to give a quadratic form q on $k^{\perp}$, explicitly given by:

$$q(x) = -\mathbb{N}_{l/\mathbb{Q}_p}(a) + a_1 a_{-1} + a_2 a_{-2} + a_3 a_{-3}.$$

In particular, one sees that the quadratic space $(k^{\perp}, q)$ is not split. Note however that the map $\beta' = \lambda_{\sigma,\alpha} \cdot ß'$ does not descend to a map on $k^{\perp}$, since $\lambda_{\sigma,\alpha} \notin k$, though of course the line spanned by β' is τ-stable.

Having described the action of τ on $k'^{\perp}$, we have an action of τ on $\mathrm{Res}_{k'/\mathbb{Q}_p} SO(q')$, having $\mathrm{Res}_{k/\mathbb{Q}_p} SO(q)$ as its group of fixed points, which is given by:

$$g \mapsto \tau \circ g \circ \tau.$$

This induces an action of τ on $\mathrm{Res}_{k'/\mathbb{Q}_p} H_{k'}$ (which is a subgroup of $\mathrm{Res}_{k'/\mathbb{Q}_p} SO(q')^3$ by Lemma 11.1), having $\mathrm{Res}_{k/\mathbb{Q}_p} H_k$ as its group of fixed points.

From Section 11, we have a Chevalley-Steinberg system of épinglage $(u'_{i,j})$ for $\mathrm{Res}_{k'/l} H_{k'}$. Let $u_{i,j} = \mathrm{Res}_{l/\mathbb{Q}_p} u'_{i,j}$ be the corresponding épinglage for $\mathrm{Res}_{k'/\mathbb{Q}_p} H_{k'}$. As we have seen in Section 11, the $u_{i,j}$'s are permuted by $\mathrm{Gal}(k'/l)$. To show that it is a Chevalley-Steinberg system, it remains to check that they are permuted by the action of τ described in the last paragraph. One checks this by a straightforward but lengthy computation, which we will not reproduce here. In conclusion, we obtain from $(u_{i,j})$ a coherent system of épinglage for H, and these are given by the same formulas in Proposition 11.5. The only point to note is that because $k/\mathbb{Q}_p$ is non-Galois, for $x \in k$, $\sigma(x)$ and $\sigma^2(x)$ are not in k.

Now let M be the A-lattice of $k^{\perp}$ generated by the e_i's, for $i = \pm 1, \pm 2, \pm 3$, and the elements of the form $a \cdot e_4 - \tau(a) \cdot e_{-4}$ for $a \in A_{k'}$. Then, as in Section 12, we conclude that K_M is a special maximal compact subgroup of $H(\mathbb{Q}_p)$, and is generated by the subgroups Z_0, $u_r(\mathbb{Z}_p)$ for r long and $u_r(A)$ for r short.

Taking α to satisfy $A = \mathbb{Z}_p[\alpha]$, we have $k \cap J_3 = A$, so that j is an integral embedding. One checks that

$$\begin{aligned} L &= k^{\perp} \cap J_3 \\ &= \{a \cdot e_4 - \tau(a) \cdot e_{-4} + \sum_{i \neq \pm 4} a_i \cdot e_i \in M : \mathrm{ord}_{k'}(a - \tau(a)) \geq \mathrm{ord}_{k'} \lambda_{\sigma,\alpha}\}. \end{aligned}$$

If $l/\mathbb{Q}_p$ is unramified, then $A \otimes A_l = A_{k'}$, and so $\mathrm{ord}_{k'} \lambda_{\sigma,\alpha}$ is half the valuation of the different ideal of k'/l. This is not the case if $l/\mathbb{Q}_p$ is ramified (which can only happen when $p = 3$). One can also describe $\tilde{L} = L^*$ explicitly. Using these descriptions, and the formulas in (11.3) and Proposition 11.5, one checks by a direct computation that every element $g \in K_M$ stabilizes L and satisfies $(g-1)\tilde{L} \subset L$. In particular, by Lemma 6.2,

$$\underline{H}(\mathbb{Z}_p) = K_L = K_M$$

is a special maximal compact subgroup of $H(\mathbb{Q}_p)$. This completes the proof of Theorem 4.1(iii).

14. **Appendix: Machine Computations**

In this Appendix, we describe the machine computations used in various parts of the paper. These were carried out with the help of Jiu-Kang Yu.

We first describe the typical problem. Suppose that $\mathfrak{g}$ is a Lie subalgebra of $\mathrm{End}(V)$, where V is a vector space of dimension m over an arbitrary field l. For $v \in V$, let

$$\phi : \mathfrak{g} \to V$$

be the evaluation map $X \mapsto X(v)$.

Problem: Show that $\mathrm{Ker}(\phi)$ has dimension n.

This is of course a problem in linear algebra. To obtain the desired result on a computer, we first define the problem over $\mathbb{Z}$. In other words, let M be a free $\mathbb{Z}$-module, and $\mathfrak{G} \subset End(M)$ a Lie subalgebra. For $v \in M$, let $\Phi : \mathfrak{G} \to M$ be the evaluation map $X \mapsto X(v)$. Suppose that

$$\begin{cases} V = M \otimes l, \\ \mathfrak{g} = \mathfrak{G} \otimes l, \\ \phi = \Phi \otimes l. \end{cases}$$

Then, thinking of an element X of $\mathfrak{G}$ as an $m \times m$ matrix (X_{ij}) with entries in $\mathbb{Z}$, the requirement that $\Phi(X) = 0 \in J \otimes l$ is equivalent to a system of linear equations

$$F_k(X_{ij}) = 0 \in J \otimes l$$

in the entries of X. We think of F_k as an element in $\mathfrak{G}^* = \mathrm{Hom}_{\mathbb{Z}}(\mathfrak{G}, \mathbb{Z})$ and let $\mathfrak{L}^*$ be the sublattice of $\mathfrak{G}^*$ generated by $\{F_k\}$. Then to show that $\mathrm{Ker}(\phi)$ has dimension n, it certainly suffices to show that $\mathfrak{L}^*$ is a direct summand of $\mathfrak{G}^*$ of rank equal to $\dim(\mathfrak{g}) - n$. It is this last step that can be carried out by the computer.

For our applications, let $(J_3, N, e, \#, T)$ be the Tits model over $\mathbb{Z}$, defined as in Section 2. In particular, $J_3 = M_3(\mathbb{Z})^3$. Let $\{e_1, e_2, ..., e_{27}\}$ be the natural basis of of J_3. The automorphism group $\underline{G}$ of the cubic norm structure J_3 is the Chevalley group over $\mathbb{Z}$ of type F_4. Hence its Lie algebra $\mathrm{Lie}(\underline{G})$ is a direct summand of $End(J_3)$ of rank 52. More precisely, if $(\cdot, \cdot, \cdot)$ is the symmetric trilinear form associated to the cubic form N, then $\mathrm{Lie}(\underline{G})$ is the sublattice of $End(J_3)$ defined by:

$$\begin{cases} (X(e_i), e_j, e_k) + (e_i, X(e_j), e_k) + (e_i, e_j, X(e_k)) = 0, \text{ for } \textbf{distinct } i, j, k \in \{1, 2, ..., 27\}; \\ (e_i, X(e_j), e_j) + \frac{1}{2} \cdot (X(e_i), e_j, e_j) = 0, \text{ for distinct } i \text{ and } j; \\ \frac{1}{2} \cdot (X(e_i), e_i, e_i) = 0; \\ X(e) = 0, \end{cases}$$

where $e = e_1 + e_5 + e_9$ is the element $(I, 0, 0)$.

We now highlight 3 examples of computation needed in the paper.

Example 1: In the proof of Proposition 5.3, we have the map (c.f. (5.4)):

$$d\varphi \otimes l : \mathrm{Lie}(\underline{G}) \otimes l \to T(\underline{Y}) \otimes l \subset J_3 \otimes l,$$

which is the evaluation map at a primitive idmepotent m_0. We want to show that the kernel has dimension 36. To define the problem over $\mathbb{Z}$, let

$$\begin{cases} \mathfrak{G} = \mathrm{Lie}(\underline{G}), \\ M = J_3, \\ v = e_1, \end{cases}$$

where $\mathrm{Lie}(\underline{G})$ and J_3 are the $\mathbb{Z}$-models defined above. Here, $e_1 = (e_{1,1}, 0, 0) \in J_3$, where $e_{1,1}$ is the 3×3 matrice whose $(1,1)$-th entry is 1, and whose other entries are 0. Let $\Phi : \mathfrak{G} \to J_3$ be the evaluation map at e_1. The computer checks that the lattice $\mathfrak{L}^*$ is indeed a direct summand of rank 16, as required.

Example 2: In the proof of Proposition 5.3, we also need to consider the map over $\mathbb{Z}_p$ (c.f. (5.7)):

$$\eta : \underline{H}_1 \to \mathrm{Aut}(J),$$

and show that its kernel is the finite group scheme μ_2. For this, one considers the induced map $d\eta$ on the Lie algebras, and it is required to show that $d\eta \otimes l$ is an isomorphism if $\mathrm{char}(l) \neq 2$, and has a 1-dimensional kernel if $\mathrm{char}(l) = 2$.

In Example 1, the kernel $\mathfrak{H}$ of Φ provides a $\mathbb{Z}$-model for $\mathrm{Lie}(\underline{H}_1) \otimes l$. An integral model J for $J \otimes l$ can be described concretely as the sublattice of J_3 consisting of elements of the form:

$$\left(\begin{pmatrix} 0 & 0 & 0 \\ 0 & a_{22} & a_{23} \\ 0 & a_{32} & a_{33} \end{pmatrix}, \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} c_{11} & 0 & 0 \\ c_{21} & 0 & 0 \\ c_{31} & 0 & 0 \end{pmatrix} \right).$$

In other words, an integral model J for $J \otimes l$ is the lattice with basis

$$B = \{e_5, e_6, e_8, e_9, e_{10}, e_{11}, e_{12}, e_{19}, e_{22}, e_{25}\}.$$

The kernel of $d\eta \otimes l$ consists of those elements $X \in \mathfrak{H} \otimes l$ satisfying $X(e_i) = 0$, for $e_i \in B$. Hence, we define the problem over $\mathbb{Z}$ by taking:

$$\begin{cases} \mathfrak{G} = \mathfrak{H}, \\ M = J^{10}, \\ v = (e_5, e_6, e_8, ..., e_{25})), \end{cases}$$

We need to show that the evaluation map Φ is injective on reduction modulo p, for $p \neq 2$, and that Φ (mod 2) has a 1-dimensional kernel. The computer checks that the lattice $\mathfrak{L}^* \subset \mathfrak{G}^*$ has determinant 2, so that $\mathfrak{G}^*/\mathfrak{L}^* \cong \mathbb{Z}/2\mathbb{Z}$. This implies the desired result.

Example 3: We consider the situation in the proof of Theorem 4.1(i) given in Section 5. More specifically, consider the case when k is a ramified cubic extension of $\mathbb{Q}_p$. Write $A = \mathbb{Z}_p[\alpha]$, where α has minimal polynomial $x^3 + ax^2 + bx + c$, an Eisenstein polynomial. Let j_0 be the integral embedding defined by:

$$\alpha \mapsto \left(\begin{pmatrix} 0 & 0 & -c \\ 1 & 0 & -b \\ 0 & 1 & -a \end{pmatrix}, 0, 0 \right) \in J_3.$$

Now we need to consider the map:

$$df \otimes \mathbb{Z}/p\mathbb{Z} : \mathrm{Lie}(\underline{G}) \otimes \mathbb{Z}/p\mathbb{Z} \to T(\underline{X}) \otimes \mathbb{Z}/p\mathbb{Z},$$

and show that its kernel is 28-dimensional. Over the residue field $\mathbb{Z}/p\mathbb{Z}$, the morphism j_0 is given by:

$$\alpha \mapsto \alpha_0 = \left(\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, 0, 0 \right).$$

Hence, we can define the problem over $\mathbb{Z}$ by taking:

$$\begin{cases} \mathfrak{G} = \mathrm{Lie}(\underline{G}) \text{ (as defined before Example 1);} \\ M = J_3 \text{ (the Tits model over } \mathbb{Z}); \\ v = \alpha_0. \end{cases}$$

The computer verifies that the lattice $\mathfrak{L}^*$ is a direct summand of $\mathfrak{G}^*$ of rank 24, as required. Unlike the previous 2 examples, where the computation is only needed for $l = \mathbb{Z}/2\mathbb{Z}$, we need to consider all primes p in this last example.

References

[A] Aschbacher, *Chevalley Group of type G_2 as the group of a trilinear form*, Journal of Algebra 109, No. 1 (1987), Pg. 193-259.

[B] N. Bourbaki, *Algebre, Ch. 9: Formes sesquilinéares et formes quadratiques*, Paris, Hermann (1959).

[BS] F. van der Blij and T. A. Springer, *The arithmetics of octaves and the group G_2*, Indag. Math. 21, Pg. 406-418 (1959).

[BT1] F. Bruhat and J. Tits, *Groupes réductifs sur un corps local II*, Publ. Math. I.H.E.S. 60 (1984), Pg. 197-376.

[BT2] F. Bruhat and J. Tits, *Schémas en groupes et immeubles des groupes classiques sur un corps local II. Groupes unitaires*, Bulletin Soc. Math. France 115, No. 2 (1987), Pg. 141-195.

[EG] N. Elkies and B. H. Gross, *The exceptional cone and the Leech lattice*, International Math. Research Notices No. 14 (1996), Pg. 665-698.

[EGA4] A. Grothendieck (with J. Dieudonné), *EGA 4: Étude locale des schémas et des morphismes de schémas (4th partie)*, Publ. Math. IHES 32 (1967), Pg. 5-361.

[G] B. H. Gross, *Groups over $\mathbb{Z}$*, Invent. Math. 124 (1996), Pg. 263-278.

[Gar] R. Garibaldi, *Isotropic trialitarian algebraic groups*, Journal of Algebra 210, No. 2 (1998), Pg. 385-418.

[GG] B. H. Gross and W. T. Gan, *Commutative subrings of certain non-associative rings*, Math. Annalen 314 (1999), Pg. 265-283.

[GHY] W. T. Gan, J. P. Hanke and J.-K. Yu, *On an exact mass formula of Shimura*, Preprint (1999).

[GY] W. T. Gan and J.-K. Yu, *Group schemes and local densities*, to appear in Duke Math. Journal.

[J1] N. Jacobson, *Composition algebras and their automorphisms*, Rend. Palermo (1958).

[J2] N. Jacobson, *Structure and representations of Jordan algebras*, AMS Colloquium Publications, Vol. XXXIX (1968).

[J3] N. Jacobson, *Exceptional Lie algebras*, Lecture Notes in Pure and Applied Math. No. 1, Marcel Dekker, New York (1971).

[J4] N. Jacobson, *Some groups of transformations defined by Jordan algebras II: Groups of type F_4*, Journal Reine Angew. Math. 204 (1960), Pg. 74-98.

[J5] N. Jacobson, *Structure theory of Jordan algebras*, Univ. of Arkansas Lecture Notes in Math. 5 (1981).

[JM] N. Jacobson and K. McCrimmon, *Quadratic Jordan algebras of quadratic forms with base points*, Journal Indian Math. Soc. (N.S.) 35 (1971), Pg. 1-45.

[KMRT] M.-A. Knus, A. Merkejev, M. Rost and J.-P. Tignol, *The book of involutions*, A. M. S. Colloquium Publications Vol. 44 (1998).

[Se] J. P. Serre, *Résumé des cours 1982-83*, Collected Works Vol. 3, Springer (1985).
[Sp] T. A. Springer, *Jordan algebras and algebraic groups*, Erg. Math. Band 75, Springer-Verlag (1973).
[So] D. Soda, *Some groups of type D_4 defined by Jordan algebras*, Journal Reine Angew Math. 223 (1966), Pg. 150-163.

School of Mathematics, Institute for Advanced Studies, Princeton, NJ 08540, U.S.A.

Department of Mathematics, Harvard University, Cambridge, MA 02138, U.S.A.
E-mail address: wtgan@math.princeton.edu
E-mail address: gross@math.harvard.edu