Maximal integral forms of the algebraic group G_2 defined by finite subgroups

Arjeh M. Cohen, Fac. Wisk. en Inf.,
TU Eindhoven
Postbox 513,
5600 MB Eindhoven,
The Netherlands

Gabriele Nebe, Wilhelm Plesken
RWTH,
Lehrstuhl B für Mathematik,
Templergraben 64,
52062 Aachen,
Germany

Abstract

We coin the notation maximal integral form of an algebraic group generalizing Gross' notion of a model. We extend the mass formula given by Gross to our context. For the finite Lie primitive subgroups of G_2 there are unique maximal integral forms defined by them.

1 Introduction

There are various concepts to express that a given finite subgroup F of a simple algebraic group G is big. For instance sometimes one can require F to be maximal finite in $G(k)$ for some number field k, or F to be irreducible, when one thinks of $G(k)$ as a subgroup of $GL_n(k)$. There are also such concepts which make use of a more arithmetic situation, like Thompson's concept of utter irreducibility (cf. [Tho 76]) or its generalization to global irreducibility ([Gro 90]). These concepts take the finite group F as a primary object.

Another approach is suggested by Gross' concepts of $\mathbb{Z}$-models (cf. [Gro 96]), which take the algebraic group G and certain of its integral forms $\underline{G}$ as the primary objects to obtain finite groups as $\underline{G}(\mathbb{Z})$, which one might hope are big, at least sometimes. In the present paper we work from both ends. On the one hand we extend Gross' notion of $\mathbb{Z}$-models to maximal integral forms (cf. Definition 3.4).

The modification is twofold: The field of definition of the algebraic group is allowed to be an algebraic number field and the condition at the finite primes is that one obtains a maximal compact subgroup of the algebraic group over the local field rather than a hyperspecial subgroup.

On the other hand we start with a finite subgroup F of $G(\mathbb{C})$. T. Springer suggested to call F *irreducible* if its centralizer in G is contained in the center of G. It turns out (cf. Section 2) that in this case there exists a unique minimal number field k and a unique k-form $\hat{G}$ of G, such that F is conjugate to a subgroup of $\hat{G}(k)$. One might then ask what the maximal integral forms $\underline{\hat{G}}_i$ of G are such that F lies in $\underline{\hat{G}}_i(o_k)$ where o_k is the ring of integers of k.

In Section 5 the maximal integral forms determined by the four Lie primitive maximal finite subgroups F of $G_2(\mathbb{C})$ (cf. [CNP 96]) are shown to be unique. The result makes heavy use of the determination (in Section 4) of lattices in the 7-dimensional $G_2(k)$-module invariant under a parahoric subgroup of $G_2(k)$, where k is a finite extension of $\mathbb{Q}_p$.

The concept of being a maximal integral form $\underline{G}$ of G is shared by all integral forms in the genus of $\underline{G}$. A measure for the chance of finding other "big" finite subgroups by looking at the other integral forms in the genus of $\underline{G}$ can be obtained from the mass of the genus. In Section 3 we generalize Gross' mass formula for $\mathbb{Z}$-forms in the genus of a given $\mathbb{Z}$-model to given maximal integral forms.

Again in the example of G_2 some of the genera described above are completely enumerated. The class number is 1 in two cases, 8 in one, and big in the final case (cf. Section 5).

We thank T. Springer for his inspiring remarks on our earlier paper [CNP 96].

2 Minimal defining field

In this paragraph we elaborate and extend some results communicated to us by T. Springer as a reaction to [CNP 96].

Let G be a semisimple, connected, complex linear algebraic group (which can be viewed as a complex connected Lie group with semisimple Lie algebra). It is well known that G can be defined over $\mathbb{Q}$ via the choice of a Chevalley basis in a faithful representation, and we shall think of G that way. Denote the algebraic closure of $\mathbb{Q}$ by $\overline{\mathbb{Q}}$.

Remark 2.1. *Let F be a finite subgroup of $G = G(\mathbb{C})$. Then F is conjugate in G to a subgroup of $G(\overline{\mathbb{Q}})$.*

PROOF. By [Slo 97, Theorem 1] (which is based on earlier results by Weil) there are only finitely many homomorphisms of F into $G(K)$ up to conjugacy in $G(K)$ for any algebraically closed field K of characteristic 0. Moreover, each conjugacy class is a Zariski open subset of the subvariety

$$R(F, G(K)) := \{\varphi : F \to G(K) \mid \varphi(f_1)\varphi(f_2) = \varphi(f_1 f_2) \text{ for all } f_1, f_2 \in F\}$$

of the affine variety $G(K)^F$. Clearly $R(F, G(\mathbb{C}))$ is already defined over $\mathbb{Q}$. Hence $R(F, G(\overline{\mathbb{Q}}))$ has as many connected components as $R(F, G(\mathbb{C}))$ which implies the statement. QED

From now on we work with $G = G(\overline{\mathbb{Q}})$ and denote the Galois group of $\overline{\mathbb{Q}}$ over $\mathbb{Q}$ by Γ. For subfields k of $\overline{\mathbb{Q}}$ denote by $\Gamma(k)$ the Galois group of $\overline{\mathbb{Q}}$ over k.

Note that Γ acts (continuously) on $G(\overline{\mathbb{Q}})$; the action can be realized via a faithful linear representation of G defined over $\mathbb{Q}$. Choosing a basis for the underlying vector space of the representation, we can view G as a group of matrices. Now $\gamma \in \Gamma$ acts entrywise on the representing matrices and hence on G; we shall write x^γ to denote the image of $x \in G$ under γ. Recall that $\mathrm{Aut}\,(G)$, the group of algebraic automorphisms of G (cf. [Hum 75], [Hoc 71]), is also an algebraic group defined over $\mathbb{Q}$, which we identify again with the group of $\overline{\mathbb{Q}}$-rational points. The connected component of $\mathrm{Aut}\,(G)$ is the group of inner automorphisms $\mathrm{Int}\,(G)$ isomorphic to $G/Z(G)$ as an abstract group, where $Z(G)$ is the center of G. The Γ-action on G induces an action on $\mathrm{Int}\,(G)$, namely the inner automorphism induced by $h \in G$ is mapped on the one induced by h^γ. This action can obviously be extended to an action of Γ on $\mathrm{Aut}\,(G)$ by viewing both $\mathrm{Aut}\,(G)$ and Γ as bijections on G.

Let k be a finite extension field of $\mathbb{Q}$ contained in $\overline{\mathbb{Q}}$. The Γ-action $G \times \Gamma \to G$; $(g, \gamma) \mapsto g^\gamma$ may be restricted to $\Gamma(k) \leq \Gamma$ and twisted by a continuous 1-cocycle $\alpha : \Gamma(k) \to \mathrm{Aut}\,(G)$, resp. $\alpha : \Gamma(k) \to \mathrm{Int}\,(G)$. The resulting twisted $\Gamma(k)$-action $G \times \Gamma(k) \to G; (g, \gamma) \mapsto (g^\gamma)\alpha(\gamma)$ yields an algebraic group G_α defined over k. This group G_α is called an *outer* resp. *inner k-form of G*.

Proposition 2.2. *Let F be a finite subgroup of $G = G(\overline{\mathbb{Q}})$ where G is as above.*

1) *Assume that the centralizer $C_G(F) := \{g \in G \mid gf = fg \text{ for all } f \in F\}$ is equal to the center $Z(G)$ of G. Then there is a unique minimal number field $k = k_{int}$ with the property that there exists an inner k-form G_α of G such that F is a subgroup of $G_\alpha(k)$. Moreover G_α is unique.*

2) *Assume that $C_{\mathrm{Aut}\,(G)}(F) := \{\beta \in \mathrm{Aut}\,(G) \mid f\beta = f \text{ for all } f \in F\}$ consists only of id_G. Then there is a unique minimal number field $k = k_{aut}$ with the property that there exists an outer k-form G_α of G such that F is a subgroup of $G_\alpha(k)$. Moreover G_α is unique.*

Proof. Let $H = \mathrm{Aut}\,(G)$ or $\mathrm{Int}\,(G)$. In both cases, we have $C_H(F) = 1$. Since the number of H-orbits on representations of F in G is finite (cf. [Slo 97]),

$$\Delta = \{\gamma \in \Gamma \mid \text{ there exists an } \alpha_\gamma \in H \text{ with } f^\gamma = f\alpha_\gamma \text{ for all } f \in F\} \qquad (1)$$

is a closed subgroup of Γ. To show that Δ is open in Γ, i.e., of finite index, note that $F \leq G(k')$ for some finite extension $k' \subset \overline{\mathbb{Q}}$ of $\mathbb{Q}$, since F is finite. Hence $\Gamma(k') \leq \Delta$ and therefore $[\Gamma : \Delta] < \infty$.

Let k be the fixed field of Δ, so that $\Delta = \Gamma(k)$. According to the definition of Δ, for each $\gamma \in \Delta$ there exists $\alpha_\gamma \in H$ such that, for all $f \in F$, we have

$f^\gamma = f\alpha_\gamma$. As $C_H(F) = 1$, the element α_γ is uniquely determined. The resulting map $\alpha : \Gamma(k) \to H$ is clearly a continuous 1-cocycle and therefore defines the k-form G_α of G with $F \leq G_\alpha(k)$. If k' is another algebraic number field such that F lies in a k'-form of G, then the corresponding 1-cocycle α' satisfies, for each $\gamma \in \Gamma(k')$ and $f \in F$, the identity $f^\gamma = f\alpha'_\gamma$ so that $\gamma \in \Delta$, whence $\Gamma(k') \subseteq \Delta$, proving $k \subseteq k'$. Finally, if $k = k'$, then $\Gamma(k') = \Delta$, and, as $C_H(F) = 1$, the cocycles α and α' coincide, proving uniqueness of the k-form. The assertions now follow with $k = k_{int}$ if $H = \mathrm{Int}\,(G)$ and $k = k_{aut}$ if $H = \mathrm{Aut}\,(G)$. QED

Definition 2.3. We shall call k_{int} the *minimal defining field* and k_{aut} the *minimal outer defining field* for F. The corresponding k_{int}-form G_α will be called the *enveloping (inner) form* of G for F and similarly, the corresponding k_{aut}-form G_α will be called the *enveloping outer form* of G for F.

We note that both cases of Proposition 2.2 hold also for $G = GL_n$ in the same formulation and with the same proof. The fact that $\mathrm{Aut}\,(GL_n)$ is algebraic can be found in [Hoc 71].

Example 2.4.

1. In the inner case for $G = GL_n$ or $G = SL_n$, the condition on the centralizer of F boils down to (absolute) irreducibility. The minimal defining field k_{int} is the character field $\mathbb{Q}[\chi]$ of the natural character χ of F obtained from the embedding of F in G. In the case of $G = GL_n$, the group of k_{int}-rational points of the enveloping inner form is the unit group $(e_\chi \mathbb{Q}[\chi]F)^*$ of the component $e_\chi \mathbb{Q}[\chi]F$ of the group ring $\mathbb{Q}[\chi]F$ whose primitive central idempotent e_χ corresponds to χ. If $G = SL_n$ one has to take the subgroup of elements of norm 1 in $(e_\chi \mathbb{Q}[\chi]F)^*$.

2. In the outer case for $G = GL_n$ or $G = SL_n$, the condition on the centralizer of F boils down to absolute irreducibility with a non-real valued natural character χ. The minimal outer defining field k_{aut} is the maximal real subfield of $\mathbb{Q}[\chi]$ and the enveloping outer form is the unitary resp. special unitary group of $((e_\chi + e_{\overline{\chi}})k_{aut}F, \circ)$ with the involution $\circ$ induced by the natural involution $\sum a_f f \mapsto \sum a_f f^{-1}$ of $k_{aut}F$.
   For the proof one needs the fact that the k-forms of GL_n are in bijection with the central simple k-algebras of dimension n^2, cf. [Ser 94, p. 133].

3. In the case $G = G_2$ one has $\mathrm{Int}\,(G) = \mathrm{Aut}\,(G)$ and Proposition 2.2 explains the observation that the four maximal finite subgroups of $G_2(\mathbb{C})$ considered in [CNP 96] have a unique minimal defining field.

3 Integral forms and the mass formula

Let k be a number field and o_k its ring of integers. Let G be a reductive linear algebraic group defined over k. Consider G as a subgroup of GL_m. In this chapter a more schematic view of algebraic groups is appropriate since we need to look at integral and adelic structures.

An *integral form* $\underline{G}$ of G can be obtained from an o_k-lattice Λ in k^m, i.e., a finitely generated o_k-module with $k \otimes_{o_k} \Lambda = k^m$. Then $\underline{G}(o_l)$ is the stabilizer of the o_l-lattice $o_l \otimes_{o_k} \Lambda$ in $G(l)$ for any finite extension l of k with o_l the integral closure of o_k in l. Similarly for any completion $k_\wp$ of k at a finite prime $\wp$ the group $\underline{G}(o_\wp)$ is the stabilizer of the $o_\wp$-lattice $\Lambda_\wp := o_\wp \otimes_{o_k} \Lambda$ in $G(k_\wp)$ where $o_\wp$ is the valuation ring of $\wp$.

Since finite groups always fix lattices one has the following result.

Remark 3.1. *Let F be a finite subgroup of $G(k)$. Then there exists an integral form $\underline{G}$ of G such that F lies in $\underline{G}(o_k)$.*

Obviously, $G(k)$ acts on the set of all integral forms of G by conjugation. Integral forms in the same orbit are called *isomorphic*. In general an isomorphism class of integral forms cannot be defined by local data. But on the other hand a lattice Λ is uniquely determined by all its completions $\Lambda_\wp$, where $\wp$ runs over the set $\mathcal{P} = \mathcal{P}_k$ of all finite primes of k. This gives rise to an action of the adele group $G(A)$ on the set of integral forms of G, as follows. First of all $A = \{(x_\wp)_{\wp \in \mathcal{P} \cup \mathcal{V}} \in \prod_{\wp \in \mathcal{P} \cup \mathcal{V}} k_\wp \mid x_\wp \in o_\wp \text{ for almost all } \wp \in \mathcal{P}\}$ is the full adele ring of k and $\mathcal{V}$ denotes the set of infinite places of k (which will be relevant only later on). Now $G(A)$ acts on the set of integral forms of G as follows. Let $\beta = (\beta_\wp)_{\wp \in \mathcal{P} \cup \mathcal{V}} \in G(A)$. The lattice $\Lambda\beta \leq k^m$ is defined via $o_\wp \otimes_{o_k} (\Lambda\beta) = (o_\wp \otimes_{o_k} \Lambda)\beta_\wp$ for all $\wp \in \mathcal{P}$. If $\underline{G}$ is defined as the stabilizer of Λ, then $\underline{G}\beta$ is the one of $\Lambda\beta$. Hence $\underline{G}\beta =: \underline{H}$ satisfies $\underline{H}(o_\wp) := \beta_\wp^{-1}\underline{G}(o_\wp)\beta_\wp$ for all finite primes $\wp \in \mathcal{P}$.

Definition 3.2. Two integral forms $\underline{G}$ and $\underline{H}$ of G lie in the same *genus*, if there is a $\beta \in G(A)$ with $\underline{G}\beta = \underline{H}$. If such a β can be found within the subgroup $G(k)$ of $G(A)$ then $\underline{G}$ and $\underline{H}$ are said to be *isomorphic*.

For semisimple groups G, the number of isomorphism classes in a genus is known to be finite ([BoH 62]).

An invariant of a genus of integral forms of G is the conjugacy class of $\underline{G}(o_\wp)$ in $G(k_\wp)$. This opens the possibility to apply the Bruhat-Tits theory of affine buildings to describe genera. The family of these invariants describes the genus.

Proposition 3.3. *Let $\underline{G}$ be an integral form of the algebraic group G as above. For all $\wp \in \mathcal{P}$ the group $\underline{G}(o_\wp)$ is a subgroup of finite index in a maximal compact subgroup of $G(k_\wp)$. The group $\underline{G}(o_\wp)$ is a hyperspecial maximal compact subgroup for all but finitely many primes $\wp \in \mathcal{P}$.*

PROOF. Let $\Lambda \subset k^m$ be a lattice that defines $\underline{G}$. The group $\underline{G}(o_\wp)$ is clearly compact and hence contained in a maximal compact subgroup H of $G(k_\wp)$. The group H is a compact subgroup of $GL_m(k_\wp)$, hence it preserves a lattice $M_\wp \subset k_\wp^m$. Multiplying $\Lambda_\wp$ by a certain power of $\wp$, we assume that $\Lambda_\wp \subseteq M_\wp$ and choose $\alpha \in \mathbb{N}$ such that $\wp^\alpha M_\wp \subseteq \Lambda_\wp$. Since there are only finitely many $o_\wp$-lattices between $M_\wp$ and $\wp^\alpha M_\wp$, the length of the orbit of $\Lambda_\wp$ under H is finite. As $\underline{G}(o_\wp)$ is the stabilizer of $\Lambda_\wp$ this settles the first assertion. The second one is 3.9.1. of [Tit 79]. It follows because

two group schemes over o_k with generic fibre G are isomorphic almost everywhere.
QED

Extending Gross' definition to arbitrary number fields, we call an integral form $\underline{G}$ a *model*, if $\underline{G}(o_\wp)$ is a hyperspecial maximal compact subgroup of $G(k_\wp)$ for all finite primes $\wp \in \mathcal{P}$.

Beside the models, the most interesting integral forms $\underline{G}$ are the ones where $\underline{G}(o_\wp)$ is a maximal compact subgroup of $G(k_\wp)$ for all $\wp \in \mathcal{P}$.

Definition 3.4. Let G be a semisimple algebraic group defined over k. An integral form $\underline{G}$ of G is called *maximal*, if $\underline{G}(o_\wp)$ is a maximal compact subgroup of $G(k_\wp)$ for all $\wp \in \mathcal{P}$.

Remarks. Let F be a finite subgroup of $G(k)$. As in Remark 3.1 one sees that there is always a maximal integral form $\underline{G}$ such that $F \leq \underline{G}(o_k)$. But even if F and G satisfy the assumptions of Proposition 2.2 and $G(k)$ is the unique enveloping k-form of F such a maximal integral form $\underline{G}$ with $F \leq \underline{G}(o_k)$ need not be unique as the following examples for the special orthogonal group resp. the spin group show:
Let $L = BW_{32}$ be the Barnes-Wall lattice in dimension 32 (cf. [Wal 62]). Then L is an even unimodular lattice with automorphism group $F \cong 2_+^{1+10}.O_{10}^+(2)$. The group F embeds into a unique $\mathbb{Q}$-form $G(\mathbb{Q})$ of the special orthogonal group of degree 32 since the natural representation of F is absolutely irreducible. F fixes a sublattice L' of index 2^{16} in L, that is a rescaling of a unimodular lattice. The two lattices L and L' define two models $\underline{G}$ and $\underline{G}'$ for G with $\underline{G}(\mathbb{Z}) = \underline{G}'(\mathbb{Z}) = F$. Though the two models $\underline{G}$ and $\underline{G}'$ are isomorphic they are not equal, because the group $\underline{G}(\mathbb{Z}_2)$ does not fix the 2-adic completion of L'.
Let F be the maximal finite subgroup $\pm D_{78}.C_{12}$ of $GL_{24}(\mathbb{Q})$ (cf. [Neb 96]). Then the natural representation of F is absolutely irreducible and therefore F embeds into a unique $\mathbb{Q}$-form of the (special) orthogonal group of degree 24. Let L be the F-invariant lattice of determinant $3^{12}13^2$. For each $a \in \mathbb{N}$ the group F fixes a unique sublattice of L of index 13^{2a}, namely $L(1-x)^a$ where x generates the 13-Sylow subgroup of F. They yield 6 different maximal integral forms $\underline{G}_a$ $(0 \leq a \leq 5)$ of the special orthogonal group with $F = \underline{G}_a(\mathbb{Z})$.
There are other examples where the integral form of the orthogonal group determined by a maximal finite subgroup of $GL_n(\mathbb{Q})$ (e.g., $n = 12$, $F \cong (3_+^{1+2} : SL_2(3) \times SL_2(3)).2)$ is not unique.

Integral forms can be viewed as a bridge between algebraic groups over fields of characteristic zero and groups over fields of finite characteristic. Reducing scalars modulo $\wp o_\wp$ one obtains from the algebraic group $\underline{G}$ an algebraic group $\underline{G}^\wp$ defined over $o_k/\wp$ such that $\underline{G}(o_\wp)$ maps onto $\underline{G}^\wp(o_\wp/\wp o_\wp)$ (cf. [Tit 79, 3.4]).

Definition 3.5. Let $\underline{G}$ be a maximal integral form of the algebraic group G as above. Let $\underline{G}^{\wp,red}$ be a Levi subgroup of the connected component $(\underline{G}^\wp)^0$ containing a maximal split torus (cf. [Tit 79, 3.5]). The *type* of $\underline{G}$ is the function $t_{\underline{G}} : \mathcal{P} \to \{\text{Dynkin diagrams}\}$ assigning to each $\wp \in \mathcal{P}$ the Dynkin diagram of $\underline{G}^{\wp,red}$ as defined in [Tit 79, 3.5.1].

We now derive a mass formula for integral forms in a given genus. The strategy is the same as the one applied by Gross to models over $\mathbb{Z}$ and can be found in [Wei 61], [Kne 67], [Cas 78]. Let G be a semisimple algebraic group defined over k. We assume that k is a totally real number field and $G(k_v)$ is compact for all $v \in \mathcal{V}$.

Let $\underline{G}_j := \underline{G}\beta_j$ $(j = 1, \dots, h)$ be a system of representatives of isomorphism classes of integral forms in the genus of $\underline{G} = \underline{G}_1$ and $S_j \leq G(A)$ be the stabilizer of $\underline{G}_j$. Then $G(A)$ is a disjoint union $G(A) = \cup_j S_1 \beta_j G(k)$. By definition of the action of $G(A)$ we have

$$S_j = \beta_j^{-1} S_1 \beta_j = \prod_{v \in \mathcal{V}} G(k_v) \times \prod_{\wp \in \mathcal{P}} \underline{G}_j(o_\wp).$$

The Tamagawa number of G is defined as

$$\tau(G) := \int_{G(A)/G(k)} \omega$$

(if this integral converges) where ω is a gauge form on the algebraic variety G (cf. [Wei 61]). The Tamagawa measure ω is a product measure $\omega = \mu_k^{-n} \prod_{\wp \in \mathcal{P} \cup \mathcal{V}} \omega_\wp$, where the product is taken over all places of k, the number n is the dimension of G (as an algebraic variety), and μ_k is the square root of the discriminant of k over $\mathbb{Q}$.

For the finite places $\wp$ of k let $\lambda_\wp := \int_{\underline{G}(o_\wp)} \omega_\wp = \int_{\underline{G}_j(o_\wp)} \omega_\wp$ for $j = 1, \dots, h$. For the infinite places v define $\lambda_v := \int_{G(k_v)} \omega_v$ which is finite since $G(k_v)$ is assumed to be compact.

The group $G(k)$ embeds in $G(A)$ as a discrete subgroup. Since ω is left invariant and additive, we have $\tau(G) = \sum_{j=1}^h \int_{X_j} \omega$ where $X_j = S_j G(k)/G(k) \cong S_j/\underline{G}_j(o_k)$, as $G(k) \cap S_j = \underline{G}_j(o_k)$. Therefore,

$$\int_{X_j} \omega = \mu_k^{-n} |\underline{G}_j(o_k)|^{-1} \prod_{\wp \in \mathcal{P} \cup \mathcal{V}} \lambda_\wp.$$

This proves the following lemma, which is implicit in many derivations of mass formulas, representing the step which can be proved in the above generality.

Lemma 3.6. *With the notation introduced above, the following equality holds.*

$$\sum_{j=1}^h |\underline{G}_j(o_k)|^{-1} = \tau(G) \mu_k^n \prod_{\wp \in \mathcal{P} \cup \mathcal{V}} \lambda_\wp^{-1}.$$

Now assume that $G(k_\wp)$ is split for all $\wp \in \mathcal{P}$. For all $\wp \in \mathcal{P}$ for which $\underline{G}(o_\wp)$ is not a hyperspecial maximal compact subgroup of $G(k_\wp)$ let $H_\wp$ be a hyperspecial maximal compact subgroup of $G(k_\wp)$. Then $a_\wp := [H_\wp : (\underline{G}(o_\wp) \cap H_\wp)] < \infty$ and $b_\wp := [\underline{G}(o_\wp) : (\underline{G}(o_\wp) \cap H_\wp)] < \infty$. Define $c_\wp = a_\wp b_\wp^{-1}$ and let c be the product of all these $c_\wp$.

Theorem 3.7. *Let G be a simply connected quasisimple algebraic group defined over a totally real number field k. Assume that $G(k_\wp)$ is split for all finite primes $\wp \in \mathcal{P}$, and $G(k_v)$ compact for all infinite places $v \in \mathcal{V}$. Then the following mass formula holds.*

$$\sum_{j=1}^h |\underline{G}_j(o_k)|^{-1} = c \prod_{i=1}^r \frac{1}{2^N} \zeta_k(1 - d_i)$$

Here $\underline{G}_1, \ldots, \underline{G}_h$ represent the isomorphism classes of integral forms in the genus of $\underline{G}$, c is defined above, $N = [k : \mathbb{Q}]$, and $d_1, \ldots, d_r$ are the degrees of the basic polynomial invariants of the Weyl group of G over $\overline{\mathbb{Q}}$, usually referred to as the degrees *of G.*

PROOF. This is a slight generalization of [Gro 96, Prop. 2.2 2)], which treats the case of $k = \mathbb{Q}$ and $c = 1$. If $\underline{G}(o_\wp)$ is hyperspecial, then $\lambda_p = |\underline{G}^\wp(o_\wp/\wp o_\wp)| q_\wp^{-n}$ where $q_\wp = |o_\wp/\wp o_\wp|$ is the order of the residue class field and $n = \dim(G) = \sum_{i=1}^r (2d_i - 1)$ is the dimension of G (cf. [Wei 61, p. 20]). By [Car 72, Theorem 9.4.10] $|\underline{G}^\wp(o_\wp/\wp o_\wp)| = q_\wp^a \prod_{i=1}^r (q_\wp^{d_i} - 1)$ where $a = \sum_{i=1}^r (d_i - 1)$. (Note that one has to omit the factor $\frac{1}{d}$ since G is simply connected.) This shows that $\prod_{\wp \in \mathcal{P}} \lambda_\wp = c^{-1} \prod_{i=1}^r \zeta_k(d_i)^{-1}$ where ζ_k is the zeta-function of k (cf. [Gro 96]). If $N := [k : \mathbb{Q}]$ is the degree of k and d is an even natural number, one has the following transformation formula for the zeta function of k:

$$\frac{1}{2^N} \zeta_k(1-d) = \mu_k^{2d-1} \zeta_k(d) \left(\frac{(d-1)!}{(2\pi i)^d} \right)^N \quad \text{(cf. [Lan 70, p. 254]).}$$

Since G is simply connected and quasisimple, $\tau(G) = 1$ and since $G(k_v)$ is compact for $v \in \mathcal{V}$, the d_i $(1 \leq i \leq r)$ are even (cf. [Gro 96, Prop. 2.2 1)]). Moreover, for the real places v, one has $\lambda_v = \prod_{i=1}^r \frac{(2\pi i)^{d_i}}{(d_i - 1)!}$ (cf. [Gro 96]). Hence the theorem follows from Lemma 3.6. QED

In the most relevant cases, e.g., for maximal integral forms, the local factors of c can be computed from the local Dynkin diagram.

Lemma 3.8. *Let G, k be as in the theorem, and let $\wp$ be a finite place of k. If $\underline{G}$ is a maximal integral form of G, and $e_1, \ldots, e_r$ are the degrees of the semisimple algebraic group of type $t_{\underline{G}}(\wp)$, then, with $q_\wp = |o_\wp/\wp o_\wp|$ as before,*

$$c_\wp = \frac{\prod_{1 \leq i \leq r} (q_\wp^{d_i} - 1)}{\prod_{1 \leq j \leq r} (q_\wp^{e_j} - 1)}.$$

PROOF. As in the paragraph preceding Theorem 3.7, let $H_\wp$ denote a hyperspecial maximal compact subgroup of $G(k_\wp)$. Since the quotient $c_\wp$ does not depend on the choices $H_\wp$ and $\underline{G}(o_\wp)$ within their $G(k_\wp)$ conjugacy classes, we may take them to contain the same parahoric subgroup B. Then $c_\wp$ is the quotient of $|H_\wp : B|$ by $|\underline{G}(o_\wp) : B|$, which is the number of chambers in the affine building of G containing $H_\wp$ divided by the number of chambers containing $\underline{G}(o_\wp)$. The residues of the vertices $H_\wp$ and $\underline{G}(o_\wp)$ of that building are the buildings with types the Dynkin diagrams of G and $t_{\underline{G}}(\wp)$ over $o_\wp/\wp o_\wp$ of order $q_\wp$, respectively (cf. [Tit 79, 3.5]). Hence the two indices satisfy

$$|H_\wp : B| = \prod_{1 \leq i \leq r} \frac{q_\wp^{d_i} - 1}{q_\wp - 1} \text{ and } |\underline{G}(o_\wp) : B| = \prod_{1 \leq j \leq r} \frac{q_\wp^{e_j} - 1}{q_\wp - 1},$$

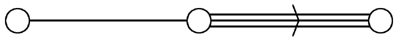
respectively. The quotient gives the asserted value for $c_\wp$. QED

4 The local picture for G_2

4.1 The maximal local compact subgroups of G_2

Let k be a finite extension of $\mathbb{Q}_p$ with valuation ring o_k and maximal ideal $\wp = \pi o_k$, and let V_0 be the simple seven-dimensional $G_2(k)$-module. Then the $G_2(k)$-module $V_0 \oplus k$ supports a unique $G_2(k)$-invariant (non-associative) Cayley algebra structure.

In this section the invariant lattices in V_0 of all parahoric subgroups of $G_2(k)$ are classified. At the same time the maximal multiplicatively closed invariant lattices in the Cayley algebra are determined. The latter turn out to be unique (this is a consequence of Theorem 4.7 below). The results of this section allow for any compact subgroup U of $G_2(k)$ to determine the parahoric supergroups of U from the U-invariant lattices in V_0. In the next section this will be used for the finite Lie-primitive groups U studied in [CNP 96]. Since the nature of the results and proofs is rather technical we state the relevant result for Section 5 first, before going into details. Note first that the Cayley multiplication $(V_0 \oplus k) \times (V_0 \oplus k) \to (V_0 \oplus k)$ induces a $G_2(k)$-invariant symmetric bilinear form $\Phi : V_0 \times V_0 \to k$. Fix an Iwahori subgroup B of $G_2(k)$. The extended Dynkin diagram of G_2 is

 .

For $i = 1, 2, 3$, omitting the i-th vertex yields the Dynkin diagram for the maximal compact subgroup P_i containing B, namely G_2, $A_1 \times A_1$, and A_2, respectively.

Theorem 4.1. *(i) Assume that* char$(o_k/\wp) \neq 2$. *Then there are eight lattices* L_1, L_1', L_2, ..., L_7 *in* V_0 *such that each* B*-invariant lattice in* V_0 *is a scalar multiple of one of them, and such that their inclusion scheme is as given in Figure 1, while* L_1 *and* L_1' *are selfdual with respect to* Φ. *Moreover, up to scalar multiples, the only* P_1*-invariant lattice among them is* L_1, *the* P_2*-invariant lattices are* L_3 *and* L_6, *and the* P_3*-invariant ones are* L_1', L_4, *and* L_5.
(ii) Assume that char$(o_k/\wp) = 2$ *and* k *is unramified over* $\mathbb{Q}_2$, *i.e.,* $\wp = 2o_k$. *Then there are lattices* L_i, L_i' $(i = 1, \ldots, 7)$, L_2'' , L_5'', L_6'', *whose inclusions are given in Figure 2 such that, up to scalar multiples, the lattices invariant under one of* P_1, P_2, P_3 *are among these 17 lattices. Moreover, the dual lattice of* L_6 *with respect to* Φ *is* $2L_5$; *up to multiples the* P_1*-invariant lattices among them are* L_5 *and* L_6, *the* P_2*-invariant lattices are* L_1, L_3', L_4, L_7 *and in case* $k = \mathbb{Q}_2$ *the two additional lattices* L_2' *and* L_2''; *the* P_3*-invariant lattices are the multiples of* L_1', L_2, L_3, L_5', *and* L_6'.

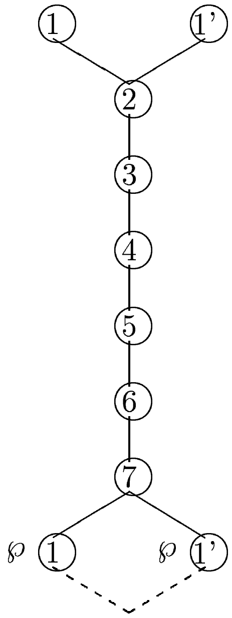


Figure 1

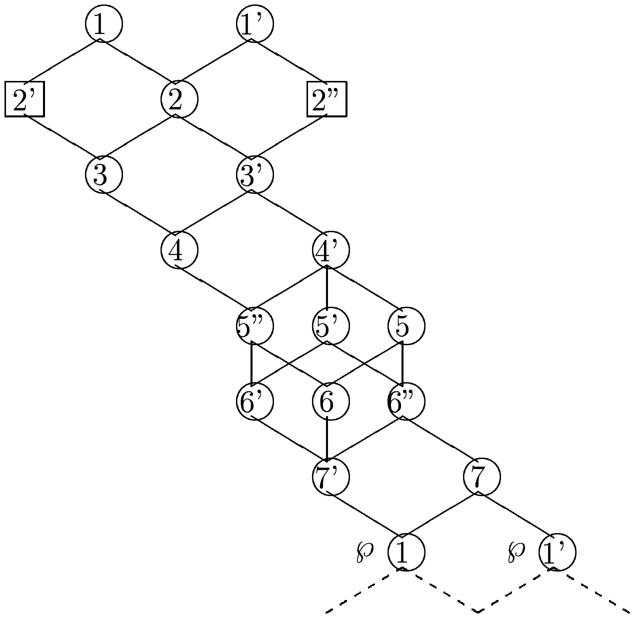


Figure 2

We note that for proper unramified extensions k of $\mathbb{Q}_2$ Figure 2 with L_2' and L_2'' omitted displays all B-invariant lattices (class number 15), whereas for $k = \mathbb{Q}_2$ this class number is 31. In the proof below the general case will be treated which is much more involved.

4.2 Preliminaries of the proof

With respect to the standard basis $(e_1, \ldots, e_7)$ of k^7 the Lie algebra $\mathfrak{g} = g_2(k)$ of type G_2 is realized as a subalgebra of the Lie algebra $so_7(k) := \{g \in k^{7\times 7} \mid gF + Fg^\top = 0\}$ with

$$F := \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

We shall write out a basis for $\mathfrak{g}$. The Cartan subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ is generated by $h_1 = \mathrm{diag}(0, 1, -1, 0, 1, -1, 0)$ and $h_2 = \mathrm{diag}(-1, -1, 0, 0, 0, 1, 1)$. The fundamental roots α and β take values 2 and -1 on h_1 and -1 and 0 on h_2, respectively. One can choose $g_\alpha := -e_{23} + e_{56}$ and $g_\beta := e_{12} - e_{34} + 2e_{45} - e_{67}$ as root vectors of $\mathfrak{h}$ for α, β. Here $e_{ij} = (\delta_{ik}\delta_{jl})_{kl}$ $(1 \le i, j \le 7)$ are the standard matrix units. Let Δ^+ be the set of positive roots corresponding to α, β. For each $\gamma \in \Delta_+$ one finds the root vector g_γ by taking successive Lie products of g_α and g_β in $\mathfrak{g}$ as follows

$$g_{\alpha+\beta} = [g_\beta, g_\alpha], \quad g_{\alpha+2\beta} = \tfrac{1}{2}[g_\beta, g_{\alpha+\beta}], \quad g_{\alpha+3\beta} = \tfrac{1}{3}[g_\beta, g_{\alpha+2\beta}], \quad g_{2\alpha+3\beta} = [g_\alpha, g_{\alpha+3\beta}].$$

Choosing $g_{-2\alpha-3\beta} = e_{61} - e_{72}$ one builds up the other root vectors as

$$g_{-\alpha-3\beta} = [g_\alpha, g_{-2\alpha-3\beta}], \quad g_{-\alpha-2\beta} = [g_\beta, g_{-\alpha-3\beta}],$$
$$g_{-\alpha-\beta} = \tfrac{1}{2}[g_\beta, g_{-\alpha-2\beta}], \quad g_{-\beta} = [g_{-\alpha-\beta}, g_\alpha], \quad g_{-\alpha} = \tfrac{1}{3}[g_\beta, g_{-\alpha-\beta}].$$

Thus the basis for $\mathfrak{g}$ is $(h_1, h_2, g_\gamma, g_{-\gamma} \mid \gamma \in \Delta^+)$.

We now describe the Iwahori subgroup B of $G_2(k)$. For $t \in k^*$ and a root γ write

$$w_\gamma(t) = \exp(tg_\gamma)\exp(-t^{-1}g_{-\gamma})\exp(tg_\gamma)$$

and $h_\gamma(t) = w_\gamma(t)w_\gamma(1)$ (cf. [Ste 68]). Then

$$B := \langle h_\gamma(t), \exp(ag_\gamma), \exp(\pi a g_{-\gamma}) \mid a \in o_k, t \in o_k^*, \gamma \in \Delta^+\rangle.$$

To describe the invariant lattices of B and of the other six proper parahoric subgroups of $G_2(k)$, we use the language of graduated orders and exponent matrices as developed in [Ple 83].

Let O be an o_k-order in $k^{d\times d}$. We take O to be *graduated*, i.e., O contains a system of orthogonal primitive idempotents of $k^{d\times d}$. Then one may assume without loss of generality that $e_{ii} \in O$ $(1 \leq i \leq d)$, and that $O \subseteq o_k^{d\times d}$. Then there are $n_1, \ldots, n_t \in \mathbb{N}$ and $M = (m_{ij})_{1\leq i,j\leq t} \in \mathbb{Z}^{t\times t}$ with $d = n_1 + \ldots + n_t$ such that $O = \mathcal{O}(n_1, \ldots, n_t; M)$, where the right hand side denotes the subset of $o_k^{d\times d}$, consisting of all block matrices with $t \times t$ blocks, such that the i,jth block is $\pi^{m_{ij}} o_k^{n_i\times n_j}$. M is called the *exponent matrix* of O.

The O-invariant lattices in k^d can immediately be read off from $n_1, \ldots, n_t$ and M, namely they are of the form $L(n_1, \ldots, n_t; m) := \{(a_1, \ldots, a_t) \mid a_i \in \pi^{m_i} o_k^{1\times n_i}\}$ where $m = (m_1, \ldots, m_t)$ satisfies $m_i + m_{ij} \geq m_j$ $(1 \leq i, j \leq t)$ (cf. [Ple 83, Remark II.4] for details). For instance, the exponent matrix E_1 given in the next proposition yields the lattices of Figure 2 (with L_2' and L_2'' omitted), where $L_6 = L(1,1,1,1,1,1,1;(0,0,0,0,0,0,0))$. The exponent rows of the lattices with exactly one maximal sublattice correspond to the rows of the exponent matrix E_1.

The investigation is subdivided according to the order of the residue class field $f_\wp := o_k/\wp$. If $|f_\wp| > 3$ then one obtains a full set of orthogonal primitive idempotents in $k^{7\times 7}$ in $o_k B$ as o_k-linear combination of the torus elements $h_\gamma(t)$, $t \in o_k^*$, $\gamma \in \Delta^+$. If $|f_\wp| \leq 3$ then $o_k B$ is only a suborder of a graduated order; the case $|f_\wp| = 2$ is the hardest one.

4.3 The case $|o_k/\wp| > 2$

Let $v : k \to \mathbb{Z} \cup \{\infty\}$ denote the discrete valuation of k and put $w = v(2)$.

Proposition 4.2.

1) If $|f_\wp| > 3$ then the enveloping order $o_kB \leq o_k^{7\times 7}$ is a graduated order $o_kB = \mathcal{O}(1,1,1,1,1,1,1;E_w) =: \mathcal{O}(E_w)$ with exponent matrix

$$E_w := \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1+w & 1+w & 1+w & 0 & w & w & w \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 2 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

2) Let $|f_\wp| = 3$ and let $\mathcal{O}(E_0)$ be the graduated order with exponent matrix E_0 as in 1). Then

$$o_kB = \{A = (a_{ij}) \in \mathcal{O}(E_0) \mid a_{11} \equiv a_{77}, a_{22} \equiv a_{66}, a_{33} \equiv a_{55} \pmod{\wp}\}.$$

PROOF. 1) Since $|f_\wp| > 3$, the idempotents e_{ii} $(1 \leq i \leq 7)$ lie in o_kB. Hence o_kB is a graduated order.

Looking at the valuations of the entries of the generating matrices of B one sees that o_kB is contained in $\mathcal{O}(E_w)$ and contains the vector space with exponent matrix $\tilde{E_w}$ where $(\tilde{E_w})_{ij} = (E_w)_{ij}$ if $(i,j) \neq (5,3),(6,2)$ and $(\tilde{E_w})_{5,3} = (\tilde{E_w})_{6,2} = 2$. Hence the order o_kB contains the multiplicative closure of this vector space, which is $\mathcal{O}(E_w)$.
2) Follows from an inspection of the generating matrices and from the fact that o_kB contains the idempotents $e_{11}+e_{77}$, $e_{22}+e_{66}$, $e_{33}+e_{55}$, and e_{44}. QED

With the preliminary remark in 4.2 we now find the B-invariant lattices as asserted in 4.1 (see Figure 1 for $w = 0$ and Figure 2 for $w > 0$). To determine the lattices of the other parahoric subgroups the description of the Weyl group in [Ste 68, Lemma 19] is used. According to this lemma, preimages of the reflections in the corresponding Weyl group may be chosen as $\sigma_1 := w_{-2\alpha-3\beta}(\pi) = (e_1, \frac{1}{\pi}e_6, -\pi e_1, -e_6)(e_2, -\frac{1}{\pi}e_7, -\pi e_2, e_7)$, $\sigma_2 := w_\alpha(1)(e_2,-e_3,-e_2,e_3)(e_5,e_6,-e_5,-e_6)$, $\sigma_3 := w_\beta(1) = (e_1,e_2,-e_1,-e_2)(e_3,-e_5)(e_4,-e_4)(e_6,-e_7,-e_6,e_7)$. For $\{h,i,j\} = \{1,2,3\}$, the parahoric subgroups containing B are $P_i = \langle B, \sigma_j, \sigma_h\rangle$ and $P_{ij} := P_i \cap P_j = \langle B, \sigma_h\rangle$.

Note that σ_1 does not act on the o_k-lattice $\langle e_1,\ldots,e_7\rangle_{o_k}$.

To describe the order o_kP_{23} the basis $(e_1, \frac{1}{\pi}e_6, e_2, \frac{1}{\pi}e_7, e_3, e_4, e_5)$ is used, for o_kP_3 we use $(e_1, \frac{1}{\pi}e_5, \frac{1}{\pi}e_6, e_2, e_3, \frac{1}{\pi}e_7, e_4)$, and for P_2 the basis $(e_1, e_2, \frac{1}{\pi}e_6, \frac{1}{\pi}e_7, e_3, e_5, e_4)$. Then one finds the following

Corollary 4.3.

$$o_kP_{13} = \mathcal{O}(1,2,1,2,1, \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1+w & 1+w & 0 & w & w \\ 1 & 1 & 1 & 0 & 0 \\ 2 & 1 & 1 & 1 & 0 \end{pmatrix}) =: O_1(o_k) \text{ if } |f_\wp| > 3$$

$$o_kP_{13} = \{A = (a_{ij})_{1\leq i,j\leq 7} \in O_1(o_k) \mid a_{11} \equiv a_{77} \pmod{\wp}\} \text{ if } |f_\wp| = 3.$$

$$o_kP_{12} = \mathcal{O}(2,2,1,2,\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1+w & w & 0 & w \\ 1 & 1 & 1 & 0 \end{pmatrix}).$$

$$o_kP_{23} \cong \mathcal{O}(2,2,1,1,1,\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1+w & 1+w & 1+w & 0 & w \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}) =: O_3(o_k), \text{ if } |f_\wp| > 3$$

$$o_kP_{23} \cong \{A = (a_{ij})_{1\leq i,j\leq 7} \in O_3(o_k) \mid a_{55} \equiv a_{77} \pmod{\wp}\} \text{ if } |f_\wp| = 3.$$

$$o_kP_1 = \mathcal{O}(6,1,\begin{pmatrix} 0 & 0 \\ w & 0 \end{pmatrix}).$$

$$o_kP_3 \cong \mathcal{O}(3,3,1,\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1+w & 1+w & 0 \end{pmatrix}).$$

$$o_kP_2 \cong \mathcal{O}(4,2,1,\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1+w & w & 0 \end{pmatrix}).$$

PROOF. Follows immediately by grouping together the different 1-dimensional constituents of o_kB according to the orbits of the respective subgroups of the Weyl group. QED

4.4 The case $|o_k/\wp| = 2$

Proposition 4.4. *Let $|f_\wp| = 2$ and $\mathcal{O}(E_w)$ be the graduated order with exponent matrix E_w as in Proposition 4.2. Let O be the suborder $O := \{A = (a_{ij}) \in \mathcal{O}(E_w) \mid a_{ii} \equiv a_{jj} \pmod{\wp}$ for all $1 \leq i,j \leq 7, a_{61} \equiv a_{72} \pmod{\wp^2}, a_{12} \equiv a_{34} \equiv a_{35} \equiv \frac{1}{2}a_{45} \equiv a_{67} \pmod{\wp}, a_{13} \equiv \frac{1}{2}a_{46} \pmod{\wp}, a_{14} \equiv \frac{1}{2}a_{47} \pmod{\wp}, a_{23} \equiv a_{56} \pmod{\wp}, a_{24} \equiv a_{57} \pmod{\wp}, a_{25} + a_{24} + a_{13} \equiv a_{36} \pmod{\wp}\}$. Then $o_kB = O$.*

PROOF. It can easily be checked that O is indeed a suborder of $\mathcal{O}(E_w)$. Since the generators of the o_k-order o_kB lie in O, it follows that $o_kB \subseteq O$.

The order O is generated as an o_k-module by $\pi\mathcal{O}(E_w)$ and the matrices I_7, e_{15}, e_{16}, e_{17}, e_{26}, e_{27}, e_{37}, πe_{ij}, where $4 \neq i > j$, $(i,j) \neq (7,1), (6,1)$ or $(7,2)$, $2\pi e_{41}$, $2\pi e_{42}$, $2\pi e_{43}$, $k_{61} := \pi e_{61} + \pi e_{72}$, $\pi^2 e_{71}$, $k_{12} := e_{12} - e_{34} - e_{35} + 2e_{45} - e_{67}$, $k_{13} := -e_{13} - e_{36} + 2e_{46}$, $k_{14} := -e_{14} + 2e_{47}$, $k_{23} := -e_{23} + e_{56}$, $k_{24} := e_{24} + e_{36} - e_{57}$, and $k_{25} := e_{25} - e_{36}$.

Let

$a_0 := \exp(g_\alpha)$, $p_0 := \exp(\pi g_{-\alpha})$, $a_1 := \exp(g_\beta)$, $p_1 := \exp(\pi g_{-\beta})$,
$a_2 := \exp(g_{\alpha+\beta})$, $p_2 := \exp(\pi g_{-\alpha-\beta})$, $a_3 := \exp(g_{\alpha+2\beta})$, $p_3 := \exp(\pi g_{-\alpha-2\beta})$,
$a_4 := \exp(g_{\alpha+3\beta})$, $p_4 := \exp(\pi g_{-\alpha-3\beta})$, $a_5 := \exp(g_{2\alpha+3\beta})$, $p_5 := \exp(\pi g_{-2\alpha-3\beta})$.

Then the p_i and a_i lie in B. We claim that these matrices together with I_7 generate the o_k-order O. This can be seen by use of the following equalities:

$$e_{17} = -I_7 + a_5 + a_1 - a_1 a_5, \qquad e_{27} = I_7 - a_0 - a_4 + a_0 a_4,$$
$$e_{16} = I_7 - a_0 - a_4 + a_4 a_0, \qquad e_{26} = I_7 - a_0 - a_3 + a_0 a_3,$$
$$\pi e_{51} = (I_7 - a_0)(I_7 - p_5), \text{ and } \qquad \pi e_{73} = I_7 - p_4 + e_{51}.$$

Thus $o_k B$ contains the left hand sides from which one constructs the πe_{ii}, $1 \leq i \leq 7$ as follows:

$$\pi e_{11} = e_{16}(p_5 - I_7), \quad \pi e_{22} = e_{27}(I_7 - p_5), \quad \pi e_{33} = (I_7 - a_4)\pi e_{73},$$
$$\pi e_{55} = \pi e_{51}(a_4 - I_7), \quad \pi e_{66} = (p_5 - I_7)e_{16}, \quad \pi e_{77} = (-p_5 + I_7)e_{27},$$
$$\pi e_{44} = \pi I_7 - e_{11} - e_{22} - e_{33} - e_{55} - e_{66} - e_{77}.$$

Multiplying the $a_i - I_7$ and $p_i - I_7$ $(0 \leq i \leq 5)$ from the left and from the right with the elements πe_{jj} one finds that $\pi \mathcal{O}(E_w) \subseteq o_k B$. Using this one sees that the elements $e_{15} = a_1 a_3 - a_1 - a_3 + I_7 + 2e_{37}$ and $e_{37} = -a_4 + I_7 + e_{15}$ also belong to $o_k B$.

Now one easily computes the remaining generators:

$$k_{23} = a_0 - I_7, \qquad k_{12} = a_1 - I_7,$$
$$k_{14} = I_7 + a_1 a_2 - a_1 - a_2 + e_{16} + e_{37} + 2e_{36},$$
$$k_{25} = a_3 - I_7 - k_{14} + e_{17}, \qquad k_{24} = a_0 a_1 - k_{25} - a_0 - a_1 + I_7,$$
$$k_{61} = p_5 - I_7, \qquad k_{13} = I_7 + a_1 a_0 - a_1 - a_0,$$
$$\pi e_{21} = e_{26}(p_5 - I_7), \qquad \pi e_{52} = \pi e_{51}(a_1 - I_7),$$
$$2\pi e_{41} = (a_2 - I_7)(p_5 - I_7) + \pi e_{21} + \pi e_{52},$$
$$\pi e_{31} = k_{13}(I_7 - p_5) + 2\pi e_{41},$$
$$\pi e_{32} = e_{37}(I_7 - p_5), \qquad 2\pi e_{42} = k_{14}(I_7 - p_5),$$
$$\pi e_{53} = (a_0 - I_7)(p_3 - 1), \qquad \pi e_{54} = \pi e_{51}(I_7 - a_3) - (\pi e_{55}(a_2 - I_7)),$$
$$\pi e_{76} = (-p_5 + I_7)e_{26}, \qquad 2\pi e_{43} = I_7 - p_1 - \pi^2 e_{53} + \pi e_{54} - \pi e_{76} + \pi e_{21},$$
$$\pi e_{62} = (p_5 - I_7)k_{12}, \qquad \pi e_{63} = (I_7 - a_1)\pi e_{73},$$
$$\pi e_{64} = (I_7 - p_5)k_{14}, \qquad \pi e_{65} = (p_5 - I_7)e_{15},$$
$$\pi e_{74} = (p_5 - I_7)(a_2 - I_7) + \pi e_{63} - \pi e_{76},$$
$$\pi e_{75} = (I_7 - p_5)(a_3 - I_7) - \pi e_{64} - (\pi e_{66}(I_7 - a_1)),$$
$$\text{and } \pi e_{71} = I_7 - p_3 + 2\pi e_{41} - \pi e_{52} + \pi e_{63} - \pi e_{74}.$$

Hence $O \subseteq o_k B$. QED

Corollary 4.5. *If* $|f_\wp| = 2$ *then*

$$o_k P_{13} = \{A = (a_{ij})_{1 \leq i,j \leq 7} \in O_1(o_k) \mid a_{11} \equiv a_{44} \equiv a_{77},\ a_{22} \equiv a_{55},\ a_{23} \equiv a_{56},\ a_{32} \equiv a_{65},$$
$$a_{33} \equiv a_{66},\ a_{12} \equiv \frac{1}{2}a_{45},\ a_{13} \equiv \frac{1}{2}a_{46},\ a_{14} \equiv \frac{1}{2}a_{47},\ a_{24} \equiv a_{57},\ a_{34} \equiv a_{67} \pmod{\wp}\}$$

$$o_k P_{12} \cong \{A = (a_{ij})_{1 \leq i,j \leq 7} \in O(2,2,1,2, \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ w+1 & w+1 & 0 & w \\ 1 & 1 & 1 & 0 \end{pmatrix}) \mid$$

$$a_{11} \equiv a_{33} \equiv a_{66},\ a_{12} \equiv a_{34} \equiv a_{67},\ a_{21} \equiv a_{43} \equiv a_{76},\ a_{22} \equiv a_{44} \equiv a_{77} \pmod{\wp}\}$$

(with respect to the basis $(e_1, e_2, e_3 + e_4, e_5 - e_4, 2e_3 + e_4 + 2e_5, e_6, e_7)$*),*

$$o_k P_{23} \cong \{A = (a_{ij})_{1 \le i,j \le 7} \in O_3(o_k) \mid a_{11} \equiv a_{33},\ a_{12} \equiv a_{34},\ a_{21} \equiv a_{43},\ a_{22} \equiv a_{44},$$

$$a_{55} \equiv a_{66} \equiv a_{77},\ a_{56} \equiv a_{57} \equiv \frac{1}{2} a_{67} \pmod{\wp}\}$$

(with respect to the basis $(e_1, \frac{1}{\pi}e_6, e_2, \frac{1}{\pi}e_7, e_3, e_4, e_5)$*).*

$$o_k P_1 \cong \mathcal{O}(6, 1, \begin{pmatrix} 0 & 0 \\ w & 0 \end{pmatrix})$$

(with respect to the basis $(e_1, e_2, e_3, e_5, e_6, e_7, e_4)$*),*

$$o_k P_3 \cong \mathcal{O}(3, 3, 1, \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ w+1 & w+1 & 0 \end{pmatrix})$$

(with respect to the basis $(e_1, \frac{1}{\pi}e_5, \frac{1}{\pi}e_6, e_2, e_3, \frac{1}{\pi}e_7, e_4)$*),*

$$o_k P_2 \cong \mathcal{O}(4, 2, 1, \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ w+1 & w+1 & 0 \end{pmatrix})$$

(with respect to the basis $(e_1, e_2, \frac{1}{\pi}e_6, \frac{1}{\pi}e_7, e_3 + e_4, e_5 - e_4, 2e_3 + e_4 + 2e_5)$*).*

PROOF. One has to keep track of the remaining congruences after joining the additional generator. For instance orthogonal primitive idempotents in $o_k P_{12}$ are $X := 2e_{54} + 4e_{55} + 2e_{44} - k_{12}\sigma_3 - \sigma_3 k_{12} - I_7 + \sigma_3(2e_{53})\sigma_3 + 2e_{53}$ and $I_7 - X$ (the notation is as in the proof of the Proposition 4.4). QED

From Corollary 4.5 and 4.3 one now finds that the P_i-invariant lattices are as described in Theorem 4.1.

4.5 The Cayley multiplication

In this section we determine the P_i-invariant lattices among those of Theorem 4.1 that are multiplicatively closed.

Lemma 4.6. *Let* $(e_1, \dots, e_7)$ *be the standard basis of* $V_0 \cong k^7$ *as in the previous sections and 1 be the unit element in the Cayley algebra* $V = V_0 \oplus k$*. Then the* B*-invariant Cayley multiplication is determined by the following table:*

1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	0	0	0	e_1	e_2	$-e_3$	$\frac{1}{2} - \frac{1}{2}e_4$
e_2	0	0	e_1	$-e_2$	0	$\frac{1}{2} + \frac{1}{2}e_4$	$-e_5$
e_3	0	$-e_1$	0	$-e_3$	$\frac{1}{2} + \frac{1}{2}e_4$	0	e_6
e_4	$-e_1$	e_2	e_3	1	$-e_5$	$-e_6$	e_7
e_5	$-e_2$	0	$\frac{1}{2} - \frac{1}{2}e_4$	e_5	0	e_7	0
e_6	e_3	$\frac{1}{2} - \frac{1}{2}e_4$	0	e_6	$-e_7$	0	0
e_7	$\frac{1}{2} + \frac{1}{2}e_4$	e_5	$-e_6$	$-e_7$	0	0	0

Theorem 4.7. *Let* $V = V_0 \oplus k$ *be as in Lemma 4.6.*

a) *Let* $T_1 := \langle e_1, e_2, e_3, e_5, e_6, e_7 \rangle_{o_k}$ *and* $T_2 := \langle e_4 \rangle_{o_k}$. *A set of representatives of isomorphism classes of* $o_k P_1$*-lattices in* V_0 *is given by* $\wp^a T_1 + T_2$, *where* $0 \leq a \leq w = v(2)$. *The multiplicatively closed* $o_k P_1$*-lattices in* V *are the ones contained in* $T_1 + T_2 + o_k(\frac{1}{2}e_4 + \frac{1}{2})$.

b) *Let* $T_1 := \langle e_1, \frac{1}{\pi}e_5, \frac{1}{\pi}e_6 \rangle_{o_k}$, $T_2 := \langle e_2, e_3, \frac{1}{\pi}e_7 \rangle_{o_k}$, *and* $T_3 := \langle e_4 \rangle_{o_k}$. *A set of representatives of isomorphism classes of* $o_k P_3$*-lattices in* V_0 *is given by* $\{\wp^a T_1 + \wp^a T_2 + T_3 \mid 0 \leq a \leq w+1\} \cup \{\wp^{a+1} T_1 + \wp^a T_2 + T_3 \mid 0 \leq a \leq w\}$. *The multiplicatively closed* $o_k P_3$*-lattices in* V *are the ones contained in* $\wp T_1 + \wp T_2 + T_3 + o_k(\frac{1}{2}e_4 + \frac{1}{2})$.

c) *Let* $T_1 := \langle e_1, e_2, \frac{1}{\pi}e_6, \frac{1}{\pi}e_7 \rangle_{o_k}$, $T_2 := \langle e_3, e_5 \rangle_{o_k}$, *and* $T_3 := \langle e_4 \rangle_{o_k}$. *A set of representatives of isomorphism classes of* $o_k P_2$*-lattices in* V_0 *is given by* $\{\wp^a T_1 + \wp^a T_2 + T_3 \mid 0 \leq a \leq w\} \cup \{\wp^{a+1} T_1 + \wp^a T_2 + T_3 \mid 0 \leq a \leq w\}$. *If* $|f_\wp| = 2$ *then there are two additional isomorphism classes of* $o_k P_2$*-lattices represented by* $\wp T_1 + T_2 + \wp T_3$ *and* $\wp^{w+1} T_1 + \wp^{w+1} T_2 + T_3$. *The multiplicatively closed* $o_k P_2$*-lattices in* V *are the ones contained in* $\wp T_1 + T_2 + T_3 + o_k(\frac{1}{2}e_4 + \frac{1}{2})$.

PROOF. The description of the invariant lattices follows immediately from the description of the graduated orders $o_k P_i$ in Corollaries 4.3 and 4.5. So we only show the statements about the multiplicatively closed lattices:
a) By the multiplication table, one has $T_1 \cdot T_1 = T_1 + o_k(\frac{1}{2}e_4 + \frac{1}{2})$, $T_1 \cdot T_2 = T_2 \cdot T_1 = T_1$, and $T_2 \cdot T_2 = o_k$. Suppose that L is a multiplicatively closed $o_k P_1$-lattice in V. Then $L \cap V_0$ is an $o_k P_1$-lattice in V_0 and hence of the form $\wp^a T_1 + \wp^b T_2$, where $0 \leq (a-b) \leq w$. Because $(L \cdot L) \cap V_0 = L \cap V_0$, one finds $2a \geq a$, $2a \geq b$, and $a + b \geq a$. Especially $a, b \geq 0$ and $L \cap V_0$ is contained in $T_1 + T_2$. Since $T_2/2T_2$ is the largest trivial $o_k P_1$-constituent module of a lattice in V_0, the multiplicative closure $T_1 + T_2 + o_k(\frac{1}{2}e_4 + \frac{1}{2})$ of $T_1 + T_2$ is the maximal P_1-invariant multiplicatively closed lattice.
b) Let L be a multiplicatively closed $o_k P_3$-lattice in $V_0 + k$. Then $L \cap V_0 = \wp^a T_1 + \wp^b T_2 + \wp^c T_3$. Since $T_1 \cdot T_1 = \wp^{-1} T_2$, $T_1 \cdot T_2 = T_2 \cdot T_1 = \wp^{-1} o_k(\frac{1}{2}e_4 + \frac{1}{2}) + \wp^{-1} T_3$, $T_1 \cdot T_3 = T_3 \cdot T_1 = T_1$, $T_2 \cdot T_2 = T_1$, $T_2 \cdot T_3 = T_3 \cdot T_2 = T_2$, and $T_3 \cdot T_3 = o_k$, one finds, as in a), that the integral numbers a, b, c satisfy the following conditions: $2a \geq b+1$, $a + b \geq c + 1$, $c \geq 0$, and $2b \geq a$. This implies that $L \cap V_0$ is contained in $\wp T_1 + \wp T_2 + T_3$. Left multiplication with $\frac{1}{2}e_4 - \frac{1}{2}$ induces the identity on T_1. Hence L can not contain the vector $\pi^{-1}(\frac{1}{2}e_4 - \frac{1}{2})$. The conclusion is that the lattice $\wp T_1 + \wp T_2 + T_3 + o_k(\frac{1}{2}e_4 + \frac{1}{2})$ is the unique maximal multiplicatively closed P_3-invariant lattice in V.
c) As in a) and b), a multiplicatively closed $o_k P_2$-lattice L in V is found which satisfies $L \cap V_0 \subseteq \wp T_1 + T_2 + T_3$. As in b), one finds that $\wp T_1 + T_2 + T_3 + o_k(\frac{1}{2}e_4 + \frac{1}{2})$ is the unique maximal multiplicatively closed P_2-invariant lattice in V. QED

Corollary 4.8. *For* $i = 1, 2, 3$ *let* L_i *be the intersection with* V_0 *of the maximal multiplicatively closed* $o_k P_i$ *lattice* M_i *in* $V = V_0 \oplus k$. *Then the discriminant of* L_i *with respect to the bilinear form* Φ *of Lemma 4.6 is* 2^{-6}, $2^{-6}\pi^4$, $2^{-6}\pi^6$ *and the* *discriminant of M_i with respect to the Cayley norm is 2^{-8}, $2^{-8}\pi^4$, $2^{-8}\pi^6$, in the respective cases.*

5 Arithmetic of the four maximal finite Lie primitive subgroups of $G_2(\mathbb{C})$

In this final section, we establish the connection with the paper [CNP 96]. There the maximal multiplicatively closed F-invariant lattices in the Cayley algebra were determined for F one of the maximal finite Lie primitive subgroups of $G_2(\mathbb{C})$. That is, F is isomorphic to one of $2^3.GL_3(2)$, $G_2(2)$, $PSL_2(8)$ and $PSL_2(13)$ (cf. [CoW 83]). Denote by C the complex Cayley algebra and by k the character field of the F-character belonging to the action of F on $C_o := \{x \in C \mid tr(x) = 0\}$. According to [CNP 96] F acts on a unique k-form C_k of C. In the light of Section 2, k can be identified as the unique minimal defining field $k_{int} = k_{aut}$ for F as subgroup of $G_2(\mathbb{C}) = \mathrm{Aut}\,(C)$ and $\mathrm{Aut}\,(C_k)$ as the unique the enveloping k-form of G_2 for F.

It is also shown in [CNP 96] that there is a unique o_k-lattice that is F-invariant and multiplicatively closed and maximal with these properties where o_k is the ring of integers of k. This result should be compared with the following theorem, which is an immediate consequence of the results of the previous section (notably Theorem 4.1 and Corollary 4.8) and the description of the F-invariant lattices in [CNP 96].

Theorem 5.1. *Let F be one of the (four) maximal finite Lie primitive subgroups of $G_2(\mathbb{C})$, $k = k_{int} = k_{aut}$ its minimal defining field, and $\widehat{G}_2$ its enveloping k-form. Then there is a unique maximal integral form $\underline{\widehat{G}}$ of $\widehat{G}_2$ with $F = \underline{\widehat{G}}(o_k)$, where o_k is the ring of algebraic integers of k.*

In this case, the genus of a maximal integral form is determined by its type. The type $t\underline{\widehat{G}}$ of the integral form $\underline{\widehat{G}}$ of the theorem satisfies $t_{\underline{\widehat{G}}}(\wp) = G_2$ for all finite primes $\wp$ of k that do not divide 2. Since 2 is inert in both fields $k \neq \mathbb{Q}$ the following table gives complete information about the genus of $\underline{\widehat{G}}$ and the minimal defining fields k.

Table 5.2.

F	$2^3.GL_3(2)$	$G_2(2)$	$PSL_2(8)$	$PSL_2(13)$
k	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}[\zeta_9 + \zeta_9^{-1}]$	$\mathbb{Q}[\sqrt{13}]$
$t_{\underline{\widehat{G}}}(2)$	A_2	G_2	$A_1 + A_1$	G_2

An interesting point of course is what the other maximal integral forms in the genus of $\underline{\widehat{G}}$ are. This can be studied using the mass formula developed in Section 3.

Theorem 5.3. *Let F be one of the four groups of the theorem above and $\underline{\widehat{G}}$ be the corresponding unique maximal integral form. Then the genus of $\underline{\widehat{G}}$ consists of one isomorphism class in the cases $F = 2^3.GL_3(2)$ or $G_2(2)$ (where $k = \mathbb{Q}$), of 8 classes if $F = PSL_2(13)$ and of more than 13472 classes if $F = PSL_2(8)$.*

In order to apply the mass formula for maximal integral forms as given in Theorem 3.7, one has to calculate the local factors of the constant c given there.

Let $\underline{G}$ be a maximal integral form of a k-form of G_2 and let P be the set of finite places of k. Put $M_1 := \{\wp \in P \mid t_{\underline{G}}(\wp) = A_2\}$ and $M_2 := \{\wp \in P \mid t_{\underline{G}}(\wp) = A_1 + A_1\}$. Then, by Lemma 4.8,

$$c = \prod_{\wp \in M_1} (q_\wp^3 + 1) \prod_{\wp \in M_2} (q_\wp^4 + q_\wp^2 + 1), \tag{2}$$

where $q_\wp$ is as usual the order of the residue class field of $o_\wp$.

The enveloping k-forms $\widehat{G}_2$ of G_2 for the four groups F in Theorem 5.1 are such that the groups $\widehat{G}_2(k_v)$ are compact for all real completions k_v of k. This property determines $\widehat{G}_2$ uniquely. In the following $\widehat{G}_2$ always denotes such a compact form of G_2.

Proposition 5.4. *If $k = \mathbb{Q}$ then up to isomorphism there is a unique maximal integral form $\underline{G}$ of $\widehat{G}_2$ for which $t_{\underline{G}}(p) = G_2$ for all primes $p > 2$ and $t_{\underline{G}}(2) = G_2$, A_2, resp. $A_1 + A_1$.*

Proof. If $t_{\underline{G}}(2) = G_2$ it is already shown by Gross ([Gro 96]) that the class of the $\mathbb{Z}$-model $\widehat{\underline{G}}$ with $\widehat{\underline{G}}(\mathbb{Z}) = G_2$ is unique in its genus.

If $t_{\underline{G}}(2) = A_2$, computation of the right hand side of the mass formula of Theorem 3.7 with $d_1 = 2$, $d_2 = 6$ and $c = 2^3 + 1$ (cf. (2)) gives

$$\sum_{j=1}^{h} |\underline{G}_j(\mathbb{Z})|^{-1} = \frac{9}{2^6 \cdot 3^3 \cdot 7} = \frac{1}{2^6 \cdot 3 \cdot 7},$$

hence the integral form defined by $2^3.GL_3(2)$ is unique in its genus.

If $t_{\underline{G}}(2) = A_1 + A_1$ one gets

$$\sum_{j=1}^{h} |\underline{G}_j(\mathbb{Z})|^{-1} = \frac{21}{2^6 \cdot 3^3 \cdot 7} = \frac{1}{2^6 \cdot 3^2}.$$

Here $h = 1$ again because there is a subgroup $F := \underline{G}_1(\mathbb{Z})$ of order $2^6 \cdot 3^2$. In fact, F is isomorphic to a subgroup of index 2 in the Weyl group of type F_4. The Cayley order defining $\underline{G}_1$ contains 48 units of norm 1. They form a loop which has a subloop of index 2 isomorphic to the tetrahedral group $SL_2(3)$. QED

Proposition 5.5. *Let $k = \mathbb{Q}[\sqrt{13}]$ and $\underline{G}$ be a model for $\widehat{G}_2$. Then the genus of $\underline{G}$ contains the following 8 classes.*

j	$F = \underline{G}_j(o_k)$	$\|F\|$	*units*	$\|Aut\,(N_C)\|$
1	$G_2(2)$	$2^6 \cdot 3^3 \cdot 7$	E_8	$2^{10} \cdot 3^4 \cdot 5 \cdot 7$
2	$PSL_2(13)$	$2^2 \cdot 3 \cdot 7 \cdot 13$	A_1	$2^3 \cdot 3 \cdot 7 \cdot 13$
3	$SL_2(3) \circ SL_2(3)$	$2^5 \cdot 3^2$	$F_4 + F_4$	$2^9 \cdot 3^3$
4	$S_3 \times S_3$	$2^2 \cdot 3^2$	$A_2 + A_2 + A_2 + A_2$	$2^5 \cdot 3^3$
5	$S_3 \times C_2$	$2^2 \cdot 3$	$A_1 + A_1 + A_1 + A_1$	$2^5 \cdot 3$
6	$(C_3 \times C_3) : 2$	$2 \cdot 3^2$	$A_2 + A_2$	$2^3 \cdot 3^3$
7	$GL_2(3)$	$2^4 \cdot 3$	A_2	$2^7 \cdot 3^2$
8	$(Q_8 \circ C_3).2$	$2^4 \cdot 3$	A_2	$2^5 \cdot 3^2$

The second column contains the automorphism group of the Cayley order, the third its order. The notation to describe the groups is quite standard. Cyclic groups of order n are denoted by C_n or simply by n, The symbol $\times$ denotes a direct product and $\circ$ a central product, : stands for split extensions and . for extensions that are most often non split.

The units of Cayley norm $1 \in k$ form a root system, which is displayed in the fourth column. The last column contains the order of the orthogonal group of the lattice of trace 0 elements in the Cayley order with respect to the Cayley norm form N_C.

PROOF. One calculates the mass of the genus to be

$$\frac{109 \cdot 307}{2^6 \cdot 3^3 \cdot 7 \cdot 13}$$

and easily checks the completeness of the list above. QED

Remark 5.6. To determine the integral forms in the genus, we calculate in the group $\widehat{G}_2(k_\wp)$ where $\wp$ is a prime ideal of $\mathbb{Q}[\sqrt{13}]$ dividing 17. We choose a torus T in $\widehat{G}_2(k_\wp)$ and apply Weyl group elements σ to the integral form $\underline{\widehat{G}}_2$ such that $(\underline{\widehat{G}}_2\sigma)(o_\wp)$ runs through the maximal parahoric subgroups of $\widehat{G}_2(k_\wp)$ that correspond to hyperspecial points in the apartment of the building of $\widehat{G}_2(k_\wp)$. If T is chosen general enough (with respect to $\underline{\widehat{G}}_2(o_k)$) one finds representatives of all the isomorphism classes of integral forms in the genus of $\underline{\widehat{G}}_2$ in this way.

PROOF OF 5.3. For $F = G_2(2)$, $2^3.GL_3(2)$, or $PSL_2(13)$ the theorem follows from Propositions 5.4 and 5.5. For $k = \mathbb{Q}[\zeta_9 + \zeta_9^{-1}]$ the genus of the maximal integral form of $\widehat{G}_2$ for $PSL_2(8)$ contains more than 13472 classes because its mass is $4161\frac{43 \cdot 1171}{2^6 \cdot 3^5} > 13472$, so that there are at least this many class representatives $\underline{G}_j(\mathbb{Z}[\zeta_9 + \zeta_9^{-1}])$. QED

We now give some more examples of genera of maximal integral forms.

Example 5.7. Any integral form $\underline{G}$ of $\widehat{G}_2$ gives us an integral form $\underline{H}$ of the orthogonal group $O_7(N_C)$ by taking the lattice of the trace 0 elements in the Cayley order with respect to the norm form N_C.

If the $t_{\underline{G}}(\wp)$ is G_2, A_2, $A_1 + A_1$ then $t_{\underline{H}}(\wp)$ is B_3, A_3, $A_1 + A_1 + A_1$, and the mass of $\underline{H}$ has to be multiplied by 1, q^3+1, $(q^2+1)(q^4+q^2+1)$, respectively, where $q = |O_\wp/\wp O_\wp|$.

For $k = \mathbb{Q}$ the genera of the integral forms of $O_7(N_C)$ derived from the three integral forms of $\widehat{G}_2$ described in Proposition 5.4 each contain only one class. For $k = \mathbb{Q}[\sqrt{13}]$, the genus of the model of $O_7(N_C)$ defined by $PSL_2(13)$ consists of $h = 12$ classes, only eight of which come from models of $\widehat{G}_2$ as listed in the table above. The other four models are:

j	$F = \underline{H}_j(o_k)$	$\lvert F \rvert$	root system
9	$C_2 \times C_2 \times A_4 \times S_3$	$2^5 \cdot 3^2$	$A_1 + A_1 + A_1 + A_2$
10	$\pm PSU_4(2) : 2$	$2^8 \cdot 3^4 \cdot 5$	E_6
11	$\pm S_5 \times C_2 \times C_2$	$2^6 \cdot 3 \cdot 5$	$A_4 + A_1 + A_1$
12	$\pm S_6 \times S_3$	$2^6 \cdot 3^3 \cdot 5$	$A_5 + A_2$

Example 5.8. If $k = \mathbb{Q}$ then there are up to isomorphism 1, respectively 2, maximal integral forms $\underline{G}$ of $\widehat{G}_2$ with $t_{\underline{G}}(p) = G_2$ for all primes $p \neq 3$ and $t_{\underline{G}}(3) = A_2$, respectively $A_1 \perp A_1$, as listed in the following table.

$t_{\underline{G}}(3)$	j	$F = \underline{G}_j(o_k)$	$\|F\|$	units	$\|\mathrm{Aut}\,(N_C)\|$
A_2	1	$3^{1+2}.QD_{16}$	$2^4 \cdot 3^3$	A_2	$2^9 \cdot 3^4 \cdot 5$
$A_1 \perp A_1$	1	$(C_6 \times C_6).(S_3 \times C_2)$	$2^4 \cdot 3^3$	A_2^4	$2^8 \cdot 3^4$
$A_1 \perp A_1$	2	$(SL_2(3) \circ Q_8).2$	$2^6 \cdot 3$	F_4	$2^{10} \cdot 3^2$

Example 5.9 To give some more examples, we list the genera of the models of G_2 over $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\sqrt{3}]$, and $\mathbb{Q}[\sqrt{2}]$. *For real quadratic fields k, there are maximal Cayley orders of the form $\mathcal{M} \oplus \mathcal{M}j$ where $j^2 = -1$ and $\mathcal{M}$ is a maximal order in the quaternion algebra over k ramified only at the 2 infinite places. For the four real quadratic fields considered in this paper the corresponding automorphism groups $\underline{G}_j(o_k)$ are $\underline{G}_3(\mathbb{Z}[\frac{1+\sqrt{13}}{2}])$, $\underline{G}_2(\mathbb{Z}[\frac{1+\sqrt{5}}{2}])$, $\underline{G}_2(\mathbb{Z}[\sqrt{3}])$, $\underline{G}_3(\mathbb{Z}[\sqrt{3}])$, and $\underline{G}_4(\mathbb{Z}[\sqrt{2}])$, where the index j refers to the tables for the various rings o_k. The automorphism groups of these Cayley orders can be described using only properties of $\mathcal{M}$.*

Model over $o_k := \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$:

j	$F = \underline{G}_j(o_k)$	$\|F\|$	units
1	$G_2(2)$	$2^6 \cdot 3^3 \cdot 7$	E_8
2	$SL_2(5) \circ SL_2(5)$	$2^5 \cdot 3^2 \cdot 5^2$	H_4^2

Model over $o_k := \mathbb{Z}[\sqrt{3}]$:

j	$F = \underline{G}_j(o_k)$	$\|F\|$	units
1	$G_2(2)$	$2^6 \cdot 3^3 \cdot 7$	E_8
2	$(SL_2(3) \circ SL_2(3)).2$	$2^6 \cdot 3^2$	F_4^2
3	$(C_{12} \times C_{12}).(S_3 \times C_2)$	$2^6 \cdot 3^3$	A_2^8
4	$SL_2(3) \circ Q_8$	$2^5 \cdot 3$	F_4
5	$(SL_2(3) \circ Q_8).2$	$2^6 \cdot 3$	F_4^2
6	$(C_4 \times C_2).(C_2^3)$	2^6	A_1^8
7	$(C_3 \times C_3) : C_6$	$2 \cdot 3^3$	A_2^4
8	$(C_3 \times C_3) : 2$	$2 \cdot 3^2$	A_2^2
9	$(C_2 \times C_2).(C_4 \times C_2)$	2^5	A_1^4

Model over $o_k := \mathbb{Z}[\sqrt{2}]$:

j	$F = \underline{G}_j(o_k)$	$\|F\|$	units
1	$G_2(2)$	$2^6 \cdot 3^3 \cdot 7$	E_8
2	$(Q_8 \circ SL_2(3)).2$	$2^6 \cdot 3$	F_4^2
3	$(C_8 \times C_8).(C_2 \times S_3)$	$2^8 \cdot 3$	A_1^{16}
4	$\tilde{S}_4 \circ \tilde{S}_4$	$2^7 \cdot 3^2$	F_4^4

Remark. In [Bou 89, III. 2.5], Cayley algebras $\mathcal{C}$ are constructed from quaternion algebras as follows:

Let E be a positive definite quaternion algebra over k, $^-$ its canonical involution, and $\gamma \in k$. Then one defines a multiplication on $\mathcal{C} := E \oplus E$ by

$$(x,y)(x',y') := (xx' + \gamma\overline{y'}y, y\overline{x'} + y'x) \quad (x,x',y,y' \in E).$$

The unit element is $1 = (1,0)$ and $\overline{(x,y)} := (\overline{x}, -y)$ defines an involution on $\mathcal{C}$.

Hence $E = E \times \{0\}$ is a subalgebra of $\mathcal{C}$ and $\mathcal{C}$ is a non-associative "crossed product algebra" $\mathcal{C} = E \oplus Ej$ where $j := (0,1) \in \mathcal{C}$.

Proposition 5.10. *With the notation above assume that $\gamma = -1$ and let $\mathcal{M} = \overline{\mathcal{M}}$ be an order of the positive definite quaternion algebra E. Then $\mathcal{O} := \mathcal{M} \oplus \mathcal{M}j$ is a (non-associative) order in $\mathcal{C}$. If the lattice $(\mathcal{M}, \mathrm{trace}(x\overline{x}))$ is orthogonally indecomposable, then $Aut(\mathcal{O})$ is generated by the mappings $x + yj \mapsto dxd^{-1} + (bdyd^{-1})j$ where $b \in \mathcal{M}$ with $b\overline{b} = 1$ and $d \in N_{E^*}(\mathcal{M})$ normalizes the order $\mathcal{M}$.*

Proof. By [Neb 98, Cor. (4.5)] (cf. also [Vig 80]) the orthogonal group of the lattice $(\mathcal{M}, \mathrm{trace}(x\overline{x}))$ is generated by $x \mapsto \overline{x}$ and $x \mapsto abxb^{-1}$, where $a \in \mathcal{M}$ satisfies $a\overline{a} = 1$ and $b \in E^*$ normalizes $\mathcal{M}$. The lattice $\mathcal{O}$ with respect to the norm form is an orthogonal sum of two copies of $(\mathcal{M}, \mathrm{trace}(x\overline{x}))$. Since automorphisms of $\mathcal{O}$ map 1 to 1 and preserve the norm form, they induce automorphisms of the suborder $\mathcal{M}$. Hence the group $\mathrm{Aut}(\mathcal{O})$ is contained in the group $G : \langle t \rangle$, where G is generated by $\phi(a,b,d) : x + yj \mapsto axa^{-1} + (bdyd^{-1})j$ $(a, d \in N_{E^*}(\mathcal{M}), b \in \mathcal{M}$, with $b\overline{b} = 1)$ and $t : x + yj \mapsto x + \overline{y}j$. Since the automorphism group of $\mathcal{C}$ consists of matrices of determinant 1 and $\det(t) = -1$ and $\det(\phi(a,b,d)) = 1$, $\mathrm{Aut}(\mathcal{O})$ is contained in G. Now $\phi(a,b,d)((x+yj)(x'+y'j)) = axx'a^{-1} - a\overline{y'}ya^{-1} + (bdy\overline{x'}d^{-1} + bdy'xd^{-1})j$ and $\phi(a,b,d)(x+yj)\phi(a,b,d)(x'+y'j) = axx'a^{-1} - \overline{d}^{-1}\overline{y'}\overline{d}\overline{b}bdyd^{-1} + (bdyd^{-1}\overline{a}^{-1}\overline{x'}\overline{a} + bdy'd^{-1}axa^{-1})j$. If $\phi(a,b,d)$ is an automorphism, then conjugation with a coincides with conjugation with d and hence $\phi(a,b,d) = \phi(d,b,d)$. QED

Remark 5.11. If the order $\mathcal{M}$ is of the form $R+Ri$ where R is an order in a number field and $i\overline{i} = 1$, $i^2 = -1$, then the mapping $(a+bi)+(c+di)j \mapsto (a+ci)+(\overline{d}+\overline{b})j$ is an additional automorphism of $\mathcal{O} = \mathcal{M} + \mathcal{M}j$. See for example the second group of Example 5.8 and $\underline{G}_3(\mathbb{Z}[\sqrt{3}])$ of Example 5.9.

References

[BoH 62] Borel, A and Harish-Chandra, *Arithmetic subgroups of algebraic groups*, Ann. Math **75** (1962) 485-535.

[Bou 89] Bourbaki, N., *Algebra II.* 2. edition, Springer 1989.

[Car 72] R.W. Carter, *Simple groups of Lie type*, Pure and applied mathematics, vol XXVIII, J. Wiley and Sons (1972)

[Cas 78] J.W.S. Cassels, *Rational Quadratic Forms*, Academic Press (1978).

[CNP 96] A.M. Cohen, G. Nebe, W. Plesken, *Cayley Orders*, Compositio Math. **103** (1996) 63-74.

[CoW 83] A.M. Cohen, D.B. Wales, *Finite subgroups of $G_2(C)$*, Comm. Algebra, 11(1983) 441-459.

[Gro 90] B.H. Gross, *Group representations and lattices.* J. AMS **3** (1990) 929-960.

[Gro 96] B.H. Gross, *Groups over $\mathbb{Z}$*, Inventiones Math., vol 124, 263-279 (1996)

[Hoc 71] G. Hochschild, *Introduction of affine algebraic groups.* Holden-Day, San Francisco, 1971.

[Hum 75] J.E. Humphreys, *Linear algebraic groups.* GTM 21, Springer Verlag, Berlin, 1975.

[Kne 67] M. Kneser, *Semi-Simple Algebraic Groups* in J.W.S. Cassels, A. Fröhlich *Algebraic Number Theory.* Academic Press (1967).

[Lan 70] S. Lang, *Algebraic Number Theory.* Addison Wesley (1970).

[Neb 96] G. Nebe, *Finite subgroups of $GL_{24}(\mathbb{Q})$.* Experimental Math. Vol. 5, No 3 (1996), 163-195.

[Neb 98] G. Nebe, *Finite quaternionic matrix groups* (submitted).

[Ple 83] W. Plesken, *Group Rings of Finite Groups over p-adic Integers*, Lecture Notes in Math. 1026, Springer-Verlag, Berlin, 1983.

[Ser 94] J-P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Math., 5, Springer-Verlag, Berlin, 5-th edition, 1994.

[Slo 97] P. Slodowy, *Two notes on a Finiteness Problem in the Representation Theory of Finite Groups*, pp. 331–346, in "Algebraic Groups and Lie Groups", ed. G.I. Lehrer, Cambridge University Press, 1997.

[Ste 68] R. Steinberg, *Lectures on Chevalley groups*, Yale, 1968.

[Tho 76] J.G. Thompson, *Finite groups and even lattices.* J. Algebra **38** (1976) no. 2, 523-524.

[Tit 79] J. Tits, *Reductive groups over local fields*, Proc. Symp. Pure Math., vol XXIII, part 1 (AMS 1979) p. 29-69.

[Vig 80] M.-F. Vignéras, *Arithmétique des Algèbres de Quaternions.* Springer Lecture Notes 800 (1980).

[Wal 62] G.E. Wall, *On the Clifford Collineation, Transform and Similarity Groups (IV).* Nagoya Math. J. **21** (1962), 199-222.

[Wei 61] A. Weil, *Adeles and Algebraic Groups.* Birkhäuser (1982)