A CHARACTERIZATION OF GROUPS OF PARAHORIC TYPE

FRANÇOIS COURTÈS

ABSTRACT. Let $F$ be a local henselian nonarchimedean field of residual field $k$, and let $G$ be the group of $F$-points of a connected reductive group defined over $F$. It is well-known that the quotient of any parahoric subgroup of $G$ by its first congruence subgroup is isomorphic to the group of $k$-points of a reductive group defined over $k$, and conversely; In this paper, we generalize this result by studying a class of linear algebraic groups named groups of parahoric type; we prove that, under certain conditions, any such group is $k$-isomorphic to the quotient of a parahoric subgroup of some reductive group over $F$ by its $h$-th congruence subgroup for a suitable $h$.

1. Introduction

Let $k$ be a perfect field, and let $F$ be a henselian local field of discrete valuation with residual field $k$. Let $G$ be the group of $F$-points of a connected reductive group defined over $F$, and let $K$ be a parahoric subgroup of $G$. It is well-known that the quotient of $K$ by its first congruence subgroup $K^1$ is the group $\mathbb{G}$ of $k$-points of a connected reductive group over $k$; conversely, any such group is isomorphic to the quotient of a parahoric subgroup of a suitable reductive $F$-group by its first congruence subgroup. This is a very useful tool in the theory of representations of $G$: if $(\pi, V)$ is a smooth representation of $G$ such that the subspace $V^{K^1}$ of elements of $V$ fixed by $K^1$ is nontrivial, the restriction of $\pi$ to $K$ factors into a representation of $\mathbb{G}$ on $V^{K^1}$, and the theory of representations of $\mathbb{G}$, which is usually easier, in particular when $k$ is finite (see for example [3]), gives us lots of important informations about our representation $\pi$. This possibility has been, for example, widely used by the author in [5] to study invariant distributions in the level 1 case.

But of course smooth representations of $G$ don’t always have nontrivial $K^1$-fixed vectors. A natural question which arises then is: what do the quotients of $K$ by bounded open subgroups smaller than $K^1$, and in particular by its $h$-th congruence subgroup when $h > 1$, look like, and in particular, is it possible to generalize the definition of reductive group to groups of that kind ? Unfortunately, finding a definition which is as simple and elegant as the definition of a reductive group while encompassing all of our quotients and only them seems to be really hard; that explains our choice of giving a definition of groups of parahoric type (first introduced in [7]) largely inspired by the definition of Bruhat-Tits valued
root data (see [2, I.6]): that kind of definition doesn’t really qualify as simple and elegant, but is useful enough for our purposes.

It is easy to check that all our quotients of parahorics match our definition (since it was tailor-made for that). But what about the converse? In other words, given a group of parahoric type $\mathcal{G}$ of given depth $h$ defined over a perfect field $k$, we want to find a henselian local field of discrete valuation $F$ with residual field $k$, a reductive group $\mathcal{G}$ defined over $F$ and a parahoric group $\mathcal{K}$ of $\mathcal{G}$ also defined over $F$ such that $\mathcal{G}$ is $k$-isomorphic to $\mathcal{K}/K^h$.

In this paper we restrict ourselves to the case when $\mathcal{G}$ is quasi-split over $k$. It turns out that at least in this case, as soon as we have a suitable field $F$, it is possible to find suitable $\mathcal{G}$ and $\mathcal{K}$ as well. More precisely, for every element $\alpha$ of the absolute root system of $\mathcal{G}$, we can put a ring structure on the root subgroup $U_\alpha$, and that ring $R_\alpha$ is the quotient of the ring of integers of some henselian local field $F_\alpha$ by its ideal of elements of valuation at least either $h$ or $h - 1$, depending whether $\alpha$ lies inside the reductive part of $\mathcal{G}$ or not. Our main result (theorem [6.1]) states that as soon as all the $R_\alpha$, with $\alpha$ lying inside (resp. outside) the reductive part of $\mathcal{G}$ are isomorphic to each other, then $\mathcal{G}$ is isomorphic to a quotient of parahoric subgroup. Unfortunately, not every group of parahoric type satisfies that condition; but it works at least for large classes of groups, as we will see at the end of the paper. We conjecture that our result extends to non-quasisplit groups of parahoric type satisfying the required condition.

The paper is organized as follows. In section 2, we recall the definition of a group of parahoric type and prove a few results which will be needed in the sequel. We also observe that the quotients of parahoric subgroups of reductive groups defined over a local field by their $h$-th congruence subgroup actually match our definition.

In section 3, we introduce the notion of a truncated valuation ring. We also attach a ring $R_\alpha$ to every root subgroup of a group of parahoric type, and prove that in most cases, either the rings attached to two different roots or suitable quotients of them are isomorphic.

In section 4, we prove our main result in the particular case of groups with a root system of rank 1.

In section 5, we make a detailed study of the commutator relations, in order to prove that the structural constants involved in them are similar to the Chevalley constants of reductive groups (see [4]). An additional difficulty compared to the case of reductive groups is that we want our constants to lie in (quotients of) a truncated valuation ring $R$ of residual field $k$, and $\text{Lie}(\mathcal{G})$ not being a $R$-module, we are forced to work in $\mathcal{G}$ directly, which makes things a bit messier.

In section 6, we prove our main result in the general case.

In section 7, we give a few examples of cases in which the conditions of the theorem are fulfilled, as well as an explicit example of case in which it is not.
2. Definition and first properties

Let $\mathbb{G}$ be a connected algebraic group defined over any perfect field $k$, and let $h$ be a positive integer. The group $\mathbb{G}$ is said to be of parahoric type of depth $h$ if it satisfies the following conditions:

- its Cartan subgroups are abelian, and their dimension is $hr$, where $r$ is the rank of $\mathbb{G}$;
- let $\mathbb{T}$ be a maximal torus of $\mathbb{G}$; the set of roots of $\mathbb{G}$ with respect to $\mathbb{T}$ is a reduced root system $\Phi$, and if $\Phi^\vee$ is the corresponding set of coroots in $X_*(\mathbb{T})$, the quadruplet $(X^*(\mathbb{T}), \Phi, X_*(\mathbb{T}), \Phi^\vee)$ is a root datum;
- let $R_u(\mathbb{G})$ be the unipotent radical of $\mathbb{G}$, and let $\Psi$ be the root system of the reductive group $\mathbb{G}/R_u(\mathbb{G})$ with respect to $\mathbb{T}$ (viewed as a maximal torus of the quotient); $\Psi$ is a root subsystem of $\Phi$, and for every $\alpha \in \Phi$, the root subgroup $U_\alpha$ of $\mathbb{G}$ with respect to $\alpha$ is of dimension $h$ (resp. $h-1$) if $\alpha \in \Psi$ (resp. if $\alpha \notin \Psi$);
- there exists a concave function $f_0$ from $\Phi$ to $\mathbb{Z}$ and, for every $\alpha \in \Phi$ and every integer $i \geq f_0(\alpha)$, a subgroup $U_{\alpha,i}$ of $U_\alpha$ satisfying the following conditions:
  - $U_{\alpha,f_0(\alpha)} = U_\alpha$;
  - for every $i$, $U_{\alpha,i+1} \subset U_{\alpha,i}$, and if $U_{\alpha,i}$ is nontrivial, $\dim(U_{\alpha,i+1}) = \dim(U_{\alpha,i}) - 1$;
  - the commutator relations: for every $\alpha, \beta, i, j$ such that $\alpha + \beta \in \Phi$, we have $[\text{Lie}(U_{\alpha,i}), \text{Lie}(U_{\beta,j})] = \text{Lie}(U_{\alpha+\beta,i+j})$;
  - for every $\alpha, i$ such that $i \geq f_0(\alpha) + f_0(-\alpha)$, the dimension of the subalgebra $L_{\alpha,i} = [\text{Lie}(U_{\alpha}), \text{Lie}(U_{\alpha,-i-f_0(\alpha)})]$ of $\text{Lie}(\mathbb{H})$ is $\text{Sup}(h-i, 0)$, and for every $j \geq f_0(\alpha)$, we have $[L_{\alpha,i}, \text{Lie}(U_{\alpha,j})] = \text{Lie}(U_{\alpha,i+j})$.

Note that the above definition is slightly different from the definition used in [7]; we’ve added the requirement that $(X^*(\mathbb{T}), \Phi, X_*(\mathbb{T}), \Phi^\vee)$ has to be a root datum.

Remember that a ($\mathbb{Z}$-valued) concave function $f_0$ on $\Phi$ is a function from $\Phi$ to $\mathbb{Z}$ satisfying the following properties:

- for every $\alpha \in \Phi$, $f_0(\alpha) + f_0(-\alpha) \geq 0$;
- for every $\alpha, \beta \in \Phi$ such that $\alpha + \beta \in \Phi$, $f_0(\alpha + \beta) \leq f_0(\alpha) + f_0(\beta)$.

Since all maximal tori of $\mathbb{G}$ are conjugated, these properties don’t depend on the choice of $\mathbb{T}$.

For every $\alpha \in \Phi$ and every $u \in U_\alpha$, we’ll call valuation of $u$ in $U_\alpha$ and denote by $v(u)$ the largest integer $v$ such that $u \in U_{\alpha,v}$. By convention the valuation of the identity element is infinite.

We can check in a similar way as in [7] that we have:
Proposition 2.1. Let $G$ be a connected reductive algebraic group defined over a henselian local field $F$ and split over the unramified closure $F_{nr}$ of $F$, and let $G_{nr}$ be the group of $F_{nr}$-points of $G$. Assume the residual characteristic $p$ of $F$ and the root system $\Phi$ of $G$ satisfy one of the following conditions:

- $p > 3$;
- $p = 3$ and $\Phi$ has no irreducible component of type $G_2$;
- $p = 2$ and all irreducible components of $\Phi$ are of type $A_n$ for some $n$.

Let $K$ be a parahoric group of $G_{nr}$; assume $K$ is stable by the action of $\text{Aut}(F_{nr}/F)$ over $G_{nr}$. For any integer $h > 0$, let $K_h$ be the $h$-th congruence subgroup of $K$. Then $G = K/K_h$ is an algebraic group of parahoric type of depth $h$ defined over the residual field $k$ of $F$.

The following facts also have already been observed in [7].

Proposition 2.2. The group $R_u(G)$ is generated by $R_u(H)$, which is of dimension $(h − 1)r$, and subgroups of dimension $h − 1$ of the $U_\alpha$, $\alpha \in \Phi$. In particular, when $h = 1$, $G$ is simply a reductive group.

Proposition 2.3. For every $\alpha \in \Phi$, we have $f_0(\alpha) + f_0(-\alpha) = 0$ (resp. $f_0(\alpha) + f_0(-\alpha) = 1$) if $\alpha \in \Psi$ (resp. $\alpha \not\in \Psi$). Moreover, $f_0$ is entirely determined by its values on the elements of a given set of simple roots of $\Phi$, and those values can be chosen arbitrarily.

We can easily check in a similar way as in proposition 8.2.3 of [9] that for every $\alpha, \beta \in \Phi$ such that $\alpha + \beta \in \Phi$, the set of commutators $[U_\alpha, U_\beta]$ is contained in the product of the $U_{\alpha + \beta + j}$, with $i$ and $j$ being positive integers. We can then rewrite the last two conditions as follows:

- the commutator relations: for every $\alpha, \beta, i, j$ such that $\alpha + \beta \in \Phi$, the projection of $[U_{\alpha,i}, U_{\beta,j}]$ on $U_{\alpha + \beta + i + j}$ is surjective,
- for every $\alpha, i$ such that $i \geq f_0(\alpha) + f_0(-\alpha)$, the dimension of the subgroup $H_{\alpha,i}$ of $H$ which is the projection on $H$ of $[U_{\alpha}, U_{-\alpha,i-f_0(\alpha)}]$ is $\text{Sup}(h-i,0)$, and for every $j \geq f_0(\alpha)$, we have $[H_{\alpha,i}, U_{\alpha,j}] = U_{\alpha,i+j}$.

Proposition 2.4. For every $\alpha \in \Phi$, $U_\alpha$ is an abelian group.

The group $T$ acts on the subspace $[\text{Lie}(U_\alpha), \text{Lie}(U_\alpha)]$ of $\text{Lie}(G)$ via the weight $2\alpha$. But since $\Phi$ is reduced, it cannot contain $2\alpha$, hence that subspace must be trivial. □

Proposition 2.5. For every $\alpha \in \Phi$ and every integer $i$, the action of $H$ by conjugation on the set of elements of $U_\alpha$ of valuation $i$ is transitive.

We can of course assume that $i$ is such that $U_\alpha$ actually contains elements of valuation $i$. Let $u_1, u_2$ be two such elements; we want to prove that there exists $h \in H$ such that $hu_1h^{-1} = u_2$. Since $T$ acts transitively by conjugation on
the non-identity elements of the one-dimensional quotient group $\mathbb{U}_{\alpha,i}/\mathbb{U}_{\alpha,i+1}$, by conjugating $u_1$ by an element of $\mathbb{T}$, we can assume that $u_1 \in \mathbb{U}_{\alpha,i+1}$.  

Consider the application $(h, u) \mapsto [h, u]$ from $\mathbb{H}_{\alpha,1} \times \mathbb{U}_{\alpha,i}$ to $\mathbb{U}_{\alpha,i+1}$. Since the image of $\mathbb{H}_{\alpha,2} \times \mathbb{U}_{\alpha,i}$ is contained in $\mathbb{U}_{\alpha,i+2}$, this application induces an application from $\mathbb{H}_{\alpha,1}/\mathbb{H}_{\alpha,2} \times \mathbb{U}_{\alpha,i}/\mathbb{U}_{\alpha,i+1}$ to $\mathbb{U}_{\alpha,i+2}$, which we will also denote by $(h, u) \mapsto [h, u]$. Moreover, we have:

$$[hh', u] = hh'u h'^{-1} h^{-1} u^{-1} = h[h', u][h, u]u[h, u],$$

and since $[h, h'][u] \in \mathbb{U}_{\alpha,i+2}$ and $\mathbb{U}_{\alpha,i}$ is abelian, in the quotient group we obtain $[hh', u] = [h, u][h', u]$. Similarly, we have:

$$[h, uu'] = [h, u]u[h, u']u^{-1} = [h, u][h, u'].$$

Finally, we have for every $t \in \mathbb{T}$, since $t$ and $h$ commute:

$$[h, Ad(t)u] = Ad(t)[h, u].$$

Consider now the application $(h, u) \mapsto [h, u]$ as an algebraic map from $\mathbb{G}^2$ to $\mathbb{G}$. Since both $u$ and $[h, u]$ belong to $\mathbb{U}_{\alpha}$, $Ad(t)$ is just the multiplication by $\alpha(t)$ in $\mathbb{G}$. In both cases, hence the application $(h, u) \mapsto [h, u]$ is $k$-linear in $u$ and $\mathbb{Z}$-linear in $h$; it must then be of the form $(h, u) \mapsto ch^a u$, where $a = 1$ when char$(k) = 0$ and $a$ is a power of $p$ when char$(k) = p$. On the other hand, by definition of a group of parahoric type, there exist $h_0, u_0$ such that $[h_0, u_0] \neq 0$; we then have $c \neq 0$. Since $k$ is perfect, it implies that the map $h \mapsto [h, u]$ is surjective for every nonzero $u$; in particular there exists $h \in \mathbb{H}_{\alpha}$ such that $[h, u_1] \in u_2 H_{\alpha,i+2}$, hence $hu_1h^{-1} \in u_2 u_{\alpha,i+2}$. 

We can iterate the reasoning, replacing $\mathbb{H}_{\alpha}$ by $\mathbb{H}_{\alpha,2}, \mathbb{H}_{\alpha,3}, \ldots$ until we obtain that $u_1$ is conjugated to an element of $\mathbb{U}_{\alpha,i+j} u_2$ with $i + j \geq h - f_0(-\alpha)$. Since the group $\mathbb{U}_{\alpha,i+j}$ is then trivial, the proposition is proved. □

For every $\alpha \in \Phi$, if $\alpha$ is the corresponding element in $\Phi^\vee$ and $\mathbb{T}_{\alpha}$ is the image of $\alpha^\vee$ in $\mathbb{T}$, let $\mathbb{H}_{\alpha}$ be the subgroup of $\mathbb{H}$ generated by $\mathbb{T}_{\alpha}$ and $\mathbb{H}_{\alpha,1}$. From the demonstration of the above proposition we deduce easily that the action of $\mathbb{H}_{\alpha} = \mathbb{H}_{\alpha,-\alpha}$ on $\mathbb{U}_{\alpha}$ (resp. $\mathbb{U}_{-\alpha}$) is transitive.

3. Truncated valuation rings

3.1. Generalities. Let $R$ be a ring, and let $h$ be a positive integer. A truncated valuation (of depth $h$) on $R$ is an application $v$ from $R$ to the set $V = \{0, 1, \ldots, h - 1, +\infty\}$ satisfying the following conditions:

- for every $x \in R$, $v(x) = +\infty$ iff $x = 0$;
- for every $x, y \in R$, $v(xy) = v(x) + v(y)$ if $v(x) + v(y) \in V$, and $+\infty$ otherwise;
- for every $x, y \in R$, $v(x + y) \geq \text{Inf}(v(x), v(y))$.

Note that the first two conditions imply $xy = 0$ as soon as $v(x) + v(y) \geq h$. In particular, if $h \geq 2$, $R$ is not an integral domain.
Proposition 3.1. The invertible elements of $R$ are all of valuation 0, and the subsets $R_i = \{ x \in R | v(x) \geq i \}$, $i \in \{0, \ldots, h\}$ are ideals of $R$.

Conversely, assume $R_1$ is the only prime ideal of $R$. Then $x \in R$ is invertible if and only if $v(x) = 0$, and the $R_i$ are the only ideals of $R$.

This is clear from the definitions. □

The quotient $R/R_1$ will be called the residual ring (resp. the residual field when $R$ is local) of $R$.

Since the product of two elements of $R$ of valuation 0 is also of valuation 0, $R/R_1$ is an integral domain, hence its characteristic $p$ is either 0 or a prime number. Let $e$ be the valuation of $p$ in $R$; $e$ will be called the absolute ramification index of $R$.

An uniformizer of $R$ is an element of $R$ of valuation 1. We have the following result:

Proposition 3.2. Let $\varpi$ be an uniformizer of $R$, and let $S$ be a system pf representatives of $R/R_1$ in $R$. Then any element $x \in R$ has an unique decomposition of the form:

$$x = \sum_{i=0}^{h-1} s_i \varpi^i$$

where the $s_i$ are elements of $S$.

The proof is similar to the corresponding proof for valued rings (see [3], II, proposition 5]). □

Proposition 3.3. Let $R$ be a valued ring and let the $R_i$, $i \in \mathbb{N}$, be defined as in proposition 3.1. For every $i \geq 1$, the valuation on $R$ canonically induces a truncated valuation on $R/R_i$.

This is obvious from the definitions. □

Conversely, we have the following result:

Proposition 3.4. Let $R$ be a local ring with a truncated valuation of depth $h$ and with perfect residual field $k$. There exists a henselian local field $F$ such that $R$ is isomorphic to the quotient $\mathcal{O}/p^h$, where $\mathcal{O}$ is the ring of integers of $F$ and $p$ is the maximal ideal of $\mathcal{O}$.

First assume that $R$ is of infinite absolute ramification index; the rings $R$ and $k$ then have the same characteristic, and we deduce from [3], II.4, prop. 6 and 8] that there exists a subring $R_0$ of $R$ isomorphic to $k$ and such that the restriction to $R_0$ of the canonical projection $R \to k$ is an isomorphism; $R$ is then a finite-dimensional $k$-algebra. Let $\varpi$ be any uniformizer of $R$, and consider the morphism $k[[X]] \to R$ sending $k$ to $R_0$ and $X$ to $\varpi$; it is obviously surjective and its kernel is the ideal $X^h k[[X]]$. Hence we can take $F = k((X))$ in this case.
Now assume that $R$ is of finite absolute ramification index. By [8, II.5, theorem 3], there exists a unique local field $F_0$ which is complete (hence henselian), absolutely unramified, and whose residual field is $k$. Let $\mathcal{O}_0$ be its ring of integers; by [8, II.5, proposition 10], there exists a ring morphism $\varphi$ from $\mathcal{O}_0$ to $R$ such that, \[ \pi \circ \varphi = \pi'. \] Let $R'$ be the image of $\varphi$ in $R$; $R'$ is then an absolutely unramified local ring with a truncated valuation, and $R$ is of the form $R'[\varpi]$, where $\varpi$ is any uniformizer of $R$.

Let $\varpi$ be such an uniformizer, and let $P$ be a polynomial of degree $e$ in $F_0[X]$ such that (with a slight abuse of notation) $P(\varpi) = 0$; $P$ is then an Eisenstein polynomial, hence irreducible. Let $F$ be a splitting field for $P$ over $F_0$, and let $\mathcal{O}$ be its ring of integers; the morphism $\varphi$ then extends to a surjective morphism from $\mathcal{O}$ to $R$, and its kernel must then be $p^h$, where $p$ is the maximal ideal of $\mathcal{O}$, which proves the proposition. □

Note that the field $F$ is not unique. In the infinite absolute ramification case, we can take as $F$ any henselian local field of absolute ramification index $\geq h$ and of residual field $k$. Even in the case of finite ramification index, and even if we restrict ourselves to complete fields, there may be several possibilities for $F$ (for exemple, with $R = \mathbb{Z}_2[\sqrt{2}]/2\sqrt{2}\mathbb{Z}_2[\sqrt{2}]$, we can of course take $F = \mathbb{Q}_2[\sqrt{2}]$, but $F = \mathbb{Q}_2[\sqrt{3}]$ works as well.)

**Corollary 3.5.** The truncated valuation ring $R$ is a henselian ring.

This is an immediate consequence of the henselianity of $F$. (Note that it can also be proved directly; the proof is similar to the proof of Hensel’s lemma for complete local fields.) □

### 3.2. The group $U$ as a truncated valuation ring.

Let $G$ (resp. $T$, $H$) be the group of $k$-points of $G$ (resp. $T$, $H$), let $\Phi$ (resp. $\Psi$) be the relative root system of $G$ (resp. $G/R_u(G)$), and for every $\alpha \in \Phi$, let $U_\alpha$ be the corresponding root subgroup of $G$. From now on until part 5 included, we will make the following assumptions:

- $G$ is split over $k$ (hence $\Phi = \Phi$, $\Psi = \Psi$ and for every $\alpha$, $U_\alpha$ is the group of $k$-points of $U_\alpha$);
- $p \neq 2$, and if $\Phi$ has any irreducible component of type $G_2$, $p$ is not 3 either;
- the application $x \mapsto x^2$ is surjective on $k$ (which means, since $p \neq 2$, that every element of $k$ has two opposite square roots).

**Lemma 3.6.** Let $R$ be a truncated valuation ring of residual field $k$. Then every element of $R$ of valuation 0 has two opposite square roots in $R$.

Since $p \neq 2$, this is simply a particular case of Hensel’s lemma. □

Let $\alpha$ be an element of $\Phi$; set $U = U_\alpha$. In this section, we’ll treat the group $U$ as an additive group on which $H$ acts by adjunction, and write its composition
law as $+$. For the rest of the section we will assume $f_0(\alpha) = 0$ to simplify the notations. (In the general case, an element of $U$ will have two distinct valuations: its valuation as an element of $U_{\alpha}$, and its valuation as an element of the ring $R_{\alpha}$ defined below, which differ by $f_0(\alpha)$. We thus will have to be careful about which valuation we’re talking about.)

Let’s fix arbitrarily an element $u_1$ of $U$ of valuation 0; for every $u \in U$ of valuation 0, there exists an element $h_u$ of $H$, unique up to the centralizer of $U$ in $H$, such that $Ad(h_u)u_1 = u$. In particular, $Ad(h_u)$ is entirely determined by $u$. We’ll define the following multiplication on $U$: let $u, u' \in U$. If $v(u) = 0$, we’ll set:

$$u \cdot u' = Ad(h_u)u'.$$

If now $v(u) > 0$, then $v(u + u_1) = 0$, and we’ll set:

$$u \cdot u' = (u + u_1).u' - u'.

Of course the multiplication depends on the choice of $u_1$.

**Proposition 3.7.** The multiplication defined above makes the group $(U, +)$ into a commutative local ring $R = R_{\alpha}$, and the valuation $v$ is a truncated valuation on that ring.

First we’ll check that the multiplication is commutative. We’ll begin with the following lemma:

**Lemma 3.8.** Let $u, u'$ be two elements of valuation 0 of $U$. We have $Ad(h_{u.w}) = Ad(h_u)Ad(h_{w'})$.

We have $u \cdot u' = Ad(h_{u,w})(u_1)$; on the other hand, we also have $u \cdot u' = Ad(h_u)(u') = Ad(h_uh_{w'})(u_1)$. The lemma then comes from the unicity of $Ad(h_{u,w'})$. $\square$

**Corollary 3.9.** We have $Ad(h_{u,w}) = Ad(h_{w',u})$. $\square$

This is an immediate consequence of the previous lemma and the commutativity of $H$. $\square$

We immediately deduce from that corollary that $u \cdot u' = u'.u$ when $u$ and $u'$ are both of valuation 0. Now assume $v(u) = 0$ and $v(u') > 0$; we have:

$$u \cdot u' = Ad(h_u)(u') = Ad(h_u)(u' + u_1) - Ad(h_u)(u_1) = u.(u' + u_1) - u = (u' + u_1).u - u = u'.u.$$

Finally assume $u$ and $u'$ are both of positive valuation; we have:

$$u \cdot u' = (u + u_1).u' - u' = u'.(u + u_1) - u' = (u' + u_1)(u + u_1) - u - u_1 - u',$$

and by a similar reasoning:

$$u'.u = (u + u_1)(u' + u_1) - u' - u_1 - u.$$

Since $u + u_1$ and $u' + u_1$ commute, $u$ and $u'$ also commute. Hence the multiplication is commutative.

We deduce from this the following lemma:
Lemma 3.10. Let \( u, u' \) be two elements of \( \mathbb{U} \) with \( v(u') > 0 \). We have:

\[
u . u' = u . (u' + u_1) - u.
\]

We'll now check that \( u_1 \) is the identity element for the multiplication. Since \( \text{Ad}(h_{u_1})(u_1) = u_1 \), by unicity \( \text{Ad}(h_{u_1}) \) must be the identity, hence \( u . u = u \) for every \( u \in \mathbb{U} \); we also obtain \( u . u_1 = u \) by commutativity.

We'll now check the distributivity. Since we already know that the multiplication is commutative we only have to check its left distributivity; let then be \( u, u', u'' \) three elements of \( \mathbb{U} \), we'll prove that \( u . (u' + u'') = u . u' + u . u'' \).

When \( v(u) = 0 \), it simply comes from the distributivity of \( \text{Ad}(h_u) \). Assume then \( v(u) > 0 \); we have, using the fact that \( v(u + u_1) = 0 \):

\[
u . (u' + u'') = (u + u_1) . (u' + u'') - u' - u'' = (u + u_1) . u' - (u + u_1) . u'' + u . u'
\]

which proves the assertion.

We'll now check the associativity. Let \( u, u', u'' \) be three elements of \( \mathbb{U} \); we'll prove that \( (u . u') . u'' = u . (u'. u'') \). First assume \( v(u) = v(u') = 0 \); we have \( (u . u') . u'' = \text{Ad}(h_{u . u'})(u'') \) and \( u . (u'. u'') = \text{Ad}(h_u)(\text{Ad}(h_{u'})(u'')) \), and the first lemma then implies the result. Next assume \( v(u) > 0 \) and \( v(u') = 0 \); we have:

\[
(u . u') . u'' = ((u + u_1) . u' - u') . u'' = (u + u_1) . u' . u'' - u' . u''
\]

\[
= (u + u_1) . (u' . u'') - u' . u'' = u . (u'. u'')
\]

Finally assume \( v(u') > 0 \); we then have \( v(u . u') > 0 \), and, using the second lemma:

\[
(u . u') . u'' = (u . (u' + u_1) - u) . u'' = (u . (u' + u_1)) . u'' - u . u''
\]

\[
= u . ((u' + u_1) . u'') - u . u'' = u . ((u' + u_1) . u'' - u'') = u . (u'. u'')
\]

We thus have proved that \( (\mathbb{U}, +, \cdot) \) is a commutative ring. Moreover, we deduce immediately from the definition of the multiplication that for every \( i \geq 0 \), the subgroup \( \mathbb{U}_i \) of the \( u \in \mathbb{U} \) such that \( v(u) \geq i \) is an ideal of that ring. To prove that \( \mathbb{U} \) is local, we only have to check that every element of \( \mathbb{U} \) of valuation \( 0 \) is invertible. Let \( u \) be such an element, and set \( u' = \text{Ad}(h_u^{-1})(u_1) \); we then have \( u'. u = u_1 \), hence \( u \) is invertible.

We finally have to check that \( v \) is a truncated valuation on the ring \( \mathbb{U} \). Since \( v \) is already a valuation on the group \( \mathbb{U} \), we only have to check that for every \( u, u' \in \mathbb{U} \) such that \( u . u' \neq 0 \), we have \( v(u . u') = v(u) + v(u') \).

For every \( h \in \mathbb{H} \), let \( v_\alpha(h) \) be the unique integer \( a \) such that \([h, \mathbb{U}] = \mathbb{U}_a,a;\). Obviously, \( v_\alpha(h) \) depends only on the class of \( h \) modulo the centralizer of \( \mathbb{U} \) in \( \mathbb{H} \), hence \( v_\alpha(h_{u_1}) \) depends only on \( u \in \mathbb{U} \). We have the following lemma:

Lemma 3.11. For every \( u \in \mathbb{U} \) such that \( v(u) > 0 \) and every choice of \( h_{u+u_1} \), we have \( v_\alpha(h_{u+u_1}) = v(u) \).

We have \([h_{u+u_1}, u_1] = u + u_1 - u_1 = u \), which proves the assertion since \( v(u_1) = 0 \). \( \square \)
Let’s go back to the proof of the proposition. If \( v(u) = 0 \) the equality \( v(u.u') = v(u) + v(u') \) comes immediately from the definition of the multiplication; assume \( v(u) > 0 \). We then have \( u.u' = (u + u_1).u' - u' = [h_{u+u_1}, u'] \), hence when \( u.u' \neq 0 \), \( v(u.u') = v_0(h_{u+u_1}) + v(u') = v(u) + v(u') \), as required. \( \square \)

We will now check that up to isomorphism, this ring doesn’t depend on the choice of \( u_1 \).

**Proposition 3.12.** Let \( u'_1 \) be another element of \( \mathbb{U} \) of valuation 0, and let \( R' \) be the ring constructed over the group \( \mathbb{U} \) the same way as \( R = (\mathbb{U}, +, .) \), but taking \( u'_1 \) instead of \( u_1 \) as unit element. Then the map \( \phi = \text{Ad}(h_{u'_1}) \) is a ring isomorphism between \( R \) and \( R' \).

We already know that \( \phi \) is a group automorphism of \( \mathbb{U} \); moreover, by definition of \( h_{u'_1}, \phi(u_1) = u'_1 \). We thus only have to check that for every \( u, u' \in \mathbb{U}, \phi(u.u') = u * u' \), where \(*\) designates the multiplication of \( R' \).

Assume first \( v(u) = 0 \); we have:

\[
\phi(u.u') = \text{Ad}(h_{u'_1})(\text{Ad}(h_u)u') = \text{Ad}(h_{u'_1}h_u h_{u'_1}^{-1})(\phi(u'))
\]

\[
= \text{Ad}(h_{u'_1}h_u h_{u'_1}^{-1})(u'_1) \ast \phi(u') = \text{Ad}(h_{u'_1})(u) \ast \phi(u') = \phi(u) \ast \phi(u'),
\]

Assume now \( v(u) > 0 \); we have:

\[
\phi(u.u') = \phi((u + u_1).u' - u') = (\phi(u) + u'_1) \ast \phi(u') - \phi(u') = \phi(u) \ast \phi(u'),
\]

which proves the result. \( \square \)

Now we’ll establish some relations between the rings associated to the various elements of \( \Phi \). Let \( u_\omega \) be an uniformizer of \( R_\alpha \); we’ll write \( R'_\alpha = R_\alpha / u_\omega^{h_0^{-1}}R_\alpha \). If \( \alpha \notin \Psi \), we have of course \( R'_\alpha = R_\alpha \).

**Proposition 3.13.** Let \( \alpha, \beta, \gamma \) be three elements of \( \Phi \) such that \( \alpha = \beta + \gamma \). Then all three rings \( R'_\alpha, R'_\beta \) and \( R'_\gamma \) are isomorphic to each other.

By symmetry it is enough to prove that \( R'_\alpha \) and \( R'_\beta \) are isomorphic. Assume first \( f_0(\alpha) = f_0(\beta) + f_0(\gamma) \). According to the commutator relations, for every \( h \in Z_{\Xi}(\mathbb{U}_\gamma) \), every \( u \in \mathbb{U}_\beta \) and every \( u' \in \mathbb{U}_\gamma \), we then have:

\[
[\text{Ad}(h)u, u'] \in \text{Ad}(h)([u, u']) \prod_{\alpha'} \mathbb{U}_{\alpha'},
\]

where the \( \alpha' \) are the roots of the form \( i\beta + j\gamma \), with \( i, j \geq 1 \) and \( \alpha' \neq \alpha \). Moreover, since \( f_0(\alpha) = f'_0(\beta) + f_0(\gamma) \), it is possible to chose \( u_{\alpha,1}, u_{\beta,1} \) and \( u_{\gamma,1} \) in such a way that the projection of \( [u_{\alpha,1}, u_{\beta,1}] \) on \( \mathbb{U}_\gamma \) is \( u_{\gamma,1} \).

Let \( \phi \) be the application from \( \mathbb{U}_\beta \) to \( \mathbb{U}_\alpha \) defined the following way: for every \( u \in \mathbb{U}_\beta, \phi(u) \) is the canonical projection on \( \mathbb{U}_\alpha \) of \( [u, u_{\gamma,1}] \). Since \( \beta \) and \( \gamma \) are linearly independant, the intersection \( \mathbb{H}_\alpha \cap \mathbb{H}_\beta \) is trivial, hence the product \( Z_{\Xi}(\mathbb{U}_\beta)Z_{\Xi}(\mathbb{U}_\gamma) \) is the whole group \( \mathbb{H} \); we deduce from this that the action of \( Z_{\Xi}(\mathbb{U}_\gamma) \) on the set of elements of valuation \( i \) of \( \mathbb{U}_\beta \) is transitive for every \( i \). It is now obvious that \( \phi \) factors into a group isomorphism between \( R'_\beta \) and \( R'_\alpha \).
and by the assumptions we have made, \( \phi(u_{\beta_1}) = u_{\alpha_1} \). To prove that \( \phi \) is a ring isomorphism, it only remains to check that \( \phi \) preserves the product of two elements.

Let then \( u, u' \) be in \( U_\beta \). Assume first \( v(u) = 0 \), and let \( h_u \) be the element of \( H_\xi \) such that \( u = Ad(h_u)u_{\beta_1} \); from the above relation we deduce that we also have \( \phi(u) = Ad(h_u)\phi(u_{\alpha_1}) \), hence:

\[
\phi(u_u') = \phi(Ad(h_u)u') = Ad(h_u)\phi(u') = \phi(u).\phi(u').
\]

If now \( v(u) > 0 \), we have:

\[
\phi(u_u') = \phi ((u + u_1).u' - u) = (\phi(u) + \phi(u_1)).\phi(u') - \phi(u') = \phi(u).\phi(u').
\]

Hence \( \phi \) is a ring isomorphism between \( R_\beta' \) and \( R_\alpha' \) and the assertion of the proposition is proved.

Assume now \( f_0(\alpha) < f_0(\beta) + f_0(\gamma) \). We will check that we then have \( f_0(\beta) = f_0(\alpha) + f_0(-\gamma) \); the proposition will then follow from the previous case. Assume \( f_0(\beta) < f_0(\alpha) + f_0(\gamma) \); we then have:

\[
f_0(\alpha) \leq f_0(\beta) + f_0(\gamma) - 1 \leq f_0(\alpha) + f_0(-\gamma) + f_0(\gamma) + 2,
\]

which contradicts the fact that \( f_0(\gamma) + f_0(-\gamma) = -1 \). \( \square \)

**Corollary 3.14.** Assume \( \Phi \) is connected and not of type \( A_1 \). Then all rings \( R'_\alpha \), \( \alpha \in \Phi \), are isomorphic to each other.

Let \( \Delta \) be any extended set of simple roots of \( \Phi \) (i.e. the union of set of simple roots with the singleton containing the inverse of the largest root of \( \Phi \) w.r.t that set); since every element \( \alpha \) of \( \Phi \) can be written as a sum of elements of \( \Delta \), assuming \( \alpha \) itself doesn’t belong to \( \Delta \), there exists \( \delta \in \Delta \) such that \( \alpha - \delta \) is a root. Applying the above proposition we obtain that \( R'_\gamma \) and \( R'_\delta \) are isomorphic. It is then enough to show that all \( R'_\delta \), \( \delta \in \Delta \), are isomorphic to each other.

Since \( \Phi \) is connected and not of type \( A_1 \), its extended Dynkin diagram is connected and for every \( \delta, \delta' \in \Delta \) such that there is an edge between them, \( \delta + \delta' \) is a root, hence \( R'_\delta \) and \( R'_\delta \) are isomorphic by the above proposition. Hence all \( R'_\delta \) are isomorphic and the corollary is proved. \( \square \)

We also have the following result:

**Proposition 3.15.** Let \( w \) be an element of the Weyl group of \( \Psi \) and let \( n \) be a representative of \( w \) in \( N_\zeta(\mathbb{T}) \). Then \( Ad(n) \) acts on \( H \), and induces an isomorphism between \( R_\alpha \) and \( R_{wa} \) (resp. between \( R'_\alpha \) and \( R'_{wa} \)).

We already know that \( Ad(n) \) is a group isomorphism between \( U_\alpha \) and \( U_{wa} \). The fact that it induces ring isomorphisms between \( R_\alpha \) and \( R_{wa} \) and between \( R'_\alpha \) and \( R'_{wa} \) is proved the same way as in proposition 3.13. \( \square \)

**Corollary 3.16.** Assume \( \Phi \) is of type \( A_1 \) and \( \Psi = \Phi \). Let \( \pm \alpha \) be the elements of \( \Phi \); then \( R_\alpha \) and \( R_{-\alpha} \) (resp. \( R'_\alpha \) and \( R'_{-\alpha} \)) are isomorphic.
This is immediate from the above proposition, with \( w \) being the only nontrivial element of \( W \). \( \square \)

Note that at this point, we still don’t know whether \( R'_\alpha \) and \( R'_{-\alpha} \) are isomorphic when \( \Phi \) is of type \( A_1 \) and \( \Psi = \emptyset \). This assertion will be proved in the next section.

Now consider the rings \( R_\alpha \) when they are different from \( R'_\alpha \), i.e. when \( \alpha \in \Psi \). We can prove, always the same way, the following proposition:

**Proposition 3.17.** Let \( \alpha, \beta \) two elements of \( \Psi \). Assume \( \alpha \) and \( \beta \) belong to the same irreducible component of \( \Psi \); then \( R_\alpha \) and \( R_\beta \) are isomorphic. In particular, when \( \Psi \) is irreducible, all the \( R_\alpha, \alpha \in \Psi \), are isomorphic to each other.

Unfortunately this is not true anymore when \( \Psi \) is reducible. We’ll give an explicit counterexample at the end of the paper.

### 4. The rank 1 case

Now we’ll investigate what happens in the case when \( \Phi \) is of rank 1. We will consider two different cases separately: the case when \( \Psi = \Phi \) (which implies \( G \) is not solvable) and the case when \( \Psi = \emptyset \) (which implies \( G \) is solvable). In the first case, we already know that \( R_\alpha \) and \( R_{-\alpha} \) are isomorphic, in the second case we still have to prove it.

#### 4.1. The non-solvable case.

First consider the case when \( G \) is not solvable. Let \( \pm \alpha \) be the elements of \( \Phi = \Psi \); we can assume \( f_0(\alpha) = f_0(-\alpha) = 0 \).

We’ll start by proving the following result:

**Proposition 4.1.** Assume \( k \) is any infinite field. Let \( \mathbb{H}, \mathbb{H}' \) be the groups of \( k \)-points of two algebraic groups defined over \( k \). Assume there exists a dense Zariski-open subset \( \Omega \) (resp. \( \Omega' \)) of \( \mathbb{H} \) (resp. \( \mathbb{H}' \)), a dense Zariski-open subset \( \Omega'' \) of \( \mathbb{H} \times \mathbb{H} \) such that the map \( (h, l) \mapsto hl \) from \( \Omega'' \) to \( \mathbb{H} \) is surjective, and an isomorphism of algebraic varieties \( \phi : \Omega \to \Omega' \) such that for every \( h, l \in \Omega \) such that \( (h, l) \in \Omega'' \) and \( hl \in \Omega \), \( \phi(hl) = \phi(h)\phi(l) \). Then \( \phi \) can be extended into an isomorphism of algebraic groups between \( \mathbb{H} \) and \( \mathbb{H}' \).

Since \( \Omega \) is Zariski-open and dense, \( V = \mathbb{H} - \Omega \) is a closed subset of \( \mathbb{H} \) of strictly smaller dimension. Hence for every \( h \in V \), \( V \cup h^{-1}V \) is strictly contained in \( \mathbb{H} \), which proves that there exist \( h_1, h_2 \in \Omega \) such that \( h = h_1h_2 \). Set \( \phi(h) = \phi(h_1)\phi(h_2) \); we first have to prove that the definition is consistent.

First assume \( h = 1 \). Let \( h_1 \) be an element of \( \Omega \) such that \( h_1^{-1} \) is also in \( \Omega \), and let \( l \) be any element of \( \Omega \) such that \( h_1l \in \Omega, (h_1, l) \in \Omega'' \) and \( (h_1l, h_1^{-1}) \in \Omega'' \); by density such an \( h_1 \) always exists, and we have:

\[
\phi(l) = \phi(h_1^{-1}h_1l) = \phi(h_1^{-1})\phi(h_1l) = \phi(h_1^{-1}\phi(h_1)\phi(l),
\]

hence:

\[
\phi(h_1^{-1})\phi(h_1) = 1.
\]
Hence $\phi(1) = 1,$ and $\phi(h^{-1}) = \phi(h_1)^{-1}.$ Note that these assertions are trivially true when $1$ belongs to $\Omega.

Now look at the general case. Let $h_1, h_2, h_3, h_4 \in \Omega$ be such that $h = h_1h_2 = h_3h_4.$ Assume $h_2^{-1}, h_3^{-1}$ and $h_1h_3^{-1} = h_4h_2^{-1}$ belong to $\Omega$ and $(h_1, h_3^{-1})$ and $(h_4, h_2^{-1})$ belong to $\Omega'$; we then have:

$$\phi(h_1)\phi(h_3)^{-1} = \phi(h_4)\phi(h_2)^{-1},$$

hence $\phi(h_1)\phi(h_2) = \phi(h_3)\phi(h_4).$ If this is not the case, by the same density argument as above we can always find $h_5, h_6 \in \Omega$ such that both quadruplets $(h_1, h_2, h_5, h_6)$ and $(h_3, h_4, h_5, h_6)$ satisfy the above properties, hence the desired result.

Now let $h, l$ be any two elements of $\mathbb{H};$ we will check that $\phi(hl) = \phi(h)\phi(l).$ If $h, l \in \Omega$ and $(h, l) \in \Omega'$ this is simply the definition of $\phi.$ Assume now either $h \in V$ or $(h, l) \notin \Omega,$ and $l \in \Omega,$ and write $h = h_1h_2,$ with $h_1, h_2 \in \Omega$ be such that $h_2l \in \Omega,$ $(h_1, h_2) \in \Omega'$ and $(h_2, l) \in \Omega'$; we then have:

$$\phi(hl) = \phi(h_1)\phi(h_2l) = \phi(h_1)\phi(h_2)\phi(l) = \phi(h)\phi(l).$$

The case $h \in \Omega$ and $l \in F$ is symmetrical, and the case $h, l \in F$ is treated similarly, using that last case.

We now have to prove that $\phi$ is an isomorphism. Let $h$ be an element of its kernel; for every $l \in \Omega$ such that $hl \in \Omega,$ we then have $\phi(h) = \phi(hl);$ since $\phi$ is a bijection on $\Omega,$ we must then have $h = 1.$ Let now $h'$ be an element of $\mathbb{H}$ which doesn't belong to the image of $\phi;$ then $h'\Omega'$ is a nonempty Zariski-open subset disjoint from $\Omega'$, which is impossible. Hence $\phi$ is an isomorphism.

Finally we have to check that $\phi$ is an isomorphism of algebraic varieties. For every $h \in \mathbb{H},$ the application $l \mapsto \phi(h)\phi(h^{-1}l)$ from $h\Omega$ to $\phi(h)\Omega'$ is an isomorphism of algebraic varieties which coincides with $\phi$ on $\Omega \cap h\Omega.$ Moreover, since $\Omega$ is Zariski-open and dense, it is easy to check that $\mathbb{H}$ is the union of a finite number of subsets of the form $h\Omega;$ by gluing the corresponding applications we obtain that $\phi$ is algebraic on the whole group and the proposition is proved. $\square$

Now we'll prove the main result of the paper in the case $\Phi$ of rank 1 and $G$, not solvable. Actually we'll prove the corresponding result for the group $G$ of $k$-points of $G$; since, with the hypotheses we have made, $k$ is infinite, $G$ is Zariski-desne in $G$, hence the result for $G$ implies the result for $G$ as well (and conversely).

**Proposition 4.2.** Assume $\Phi$ is of rank 1 and $G$ is not solvable. There exists a nonarchimedean henselian local field $F$ of residual field $k$ and an algebraic group $G$ of type $A_1$ defined and split over $F$ such that $G$ is isomorphic to the quotient $G_0$ of a maximal parahoric subgroup of the group $G$ of $F$-points of $G$ by its $h$-th congruence subgroup.

Let $\mathbb{B}$ be the pseudo-Borel subgroup of $G$ generated by $\mathbb{H}$ and $U_a,$ and let $w$ be the nontrivial element of the Weyl group of $G$ w.r.t $T$; the Bruhat decomposition
of \( G \) can be written the following way:

\[
G = BU_{-\alpha, 1} \sqcup BwB.
\]

We deduce from this that the subset \( BwB \) is Zariski-open and dense in \( G \); according to the previous proposition we then only have to find a bijection \( \phi \) between \( BwB \) and the corresponding subset of \( G_0 \) such that for every \( g, g' \in BwB \) such that \( gg' \in BwB \), \( \phi(gg') = \phi(g)\phi(g') \).

Since \( w \) normalizes \( T \), it also normalizes \( H \), and we can then assume that it belongs to the group \( N_G(H)/H \). We have the following lemma:

**Lemma 4.3.** Let \( n \) be any representant of \( w \) in \( N_G(H) \); there exist \( u \in U_\alpha \) and \( u' \in U_{-\alpha} \) such that \( n = uu'u = u'u'u' \); moreover, we have \( u' = n^{-1}un = nun^{-1} \).

Let \( u' \) be any element of \( U_{-\alpha} \) of valuation \( 0 \). Since it doesn’t belong to \( B U_{-\alpha, 1} \), it must belong to \( BwB = BwU_\alpha \). Moreover, since \( B = U_\alpha H \), there exists a representative \( n_0 \) of \( w \) such that \( u' \) belongs to \( U_\alpha n_0 U_\alpha \). Write \( n_0 = u_1 u' u_2 \), \( u_1, u_2 \in U_\alpha \); to prove the assertion of the lemma for \( n_0 \), we only have to check that \( u_1 = u_2 \).

**Lemma 4.4.** For every \( n \in w \), there exists \( h \in H \) such that \( n = hn_0 h^{-1} \).

Let \( x_0 \) (resp. \( x \)) be the element of \( R_{-\alpha} \) such that \( Ad(n_0)u_{\alpha, 1} = u_{-\alpha, x_0} \) (resp. \( u_{-\alpha, x} \)); \( x_0 \) and \( x \) are both of valuation \( 0 \). Let \( y \) be a square root of \( x_0^{-1}x \) in \( R_{-\alpha} \), and set \( h = h_\gamma \) (as an element of \( H_{-\alpha} \)); we have:

\[
Ad(hn_0 h^{-1})u_{\alpha, 1} = Ad(hn_0)(u_{\alpha, y^{-1}}) = Ad(h)u_{-\alpha, x_0 y} = u_{-\alpha, x_0 y^2} = u_{-\alpha, x}.
\]

Hence we have \( n = zn_0 h^{-1} \), where \( z = h_{\pm 1} \). If \( z \) is trivial we are done; if \( z = h_{-1} \), replacing \( y \) by \( -y \) yields the desired result.

We deduce from this lemma that for such a \( h \), we have \( n = (hu_1 h^{-1})(hu'h^{-1})(hu_2 h^{-1}) \). This is true in particular for \( n = n_0^{-1} \), for which \( h \) is such that \( Ad(h) \) is the isomorphism \( x \mapsto x^{-1} \) on both \( U_\alpha \) and \( U_{-\alpha} \). We thus obtain:

\[
n_0 = (n_0^{-1})^{-1} = (u_1^{-1}u'^{-1}u_2^{-1})^{-1} = u_2 u' u_1,
\]

hence \( u' = u_2 n_0 u_1 \). On the other hand, since \( U_\alpha \) and \( n_0 U_\alpha n_0^{-1} = U_{-\alpha} \) have a trivial intersection, any element of \( U_\alpha n_0 U_\alpha \) can be written in an unique way in the form \( u n_0 v \); hence \( u_1 = u_2 \). For every \( n \in w \), we then have:

\[
n = (hu_1 h^{-1})(hu'h^{-1})(hu_1 h^{-1}),
\]

with \( h \) defined as above, which completes the proof of the first equality of the lemma.

To prove the next two, we observe that we have:

\[
u'^{-1} u'^{-1} n = u;
\]

which can be rewritten as:

\[
u'^{-1} n (n^{-1} u'^{-1} n) = u,
\]
hence:

\[ n = u'u(n^{-1}un) \]

By the same reasoning as above (with \( \alpha \) and \(-\alpha \) switched), we must then have \( n^{-1}un = u' \), hence \( n = u'uu' \). The equality \( u' = nun^{-1} \) is obtained in a similar way. \( \square \)

Now we’ll prove the proposition. By proposition \ref{prop:characterization} we know that there exists a nonarchimedean henselian local field \( F \) such that the quotient of its ring of integers \( \mathcal{O} \) by \( \mathfrak{p}^h \), where \( \mathfrak{p} \) is the maximal ideal of \( \mathcal{O} \), is isomorphic to \( R_\alpha \) and \( R_{-\alpha} \). Let \( \mathcal{G} \) be an algebraic group defined and split over \( F \) whose root datum is \((X^*(\mathbb{T}), \Phi, X_-(\mathbb{T}), \Phi^\vee)\); such a group exists by theorem 10.1.1 of [\ref{Dove}]. Let \( G \) be the group of \( F \)-points of \( \mathcal{G} \), let \( K \) be any maximal parahoric subgroup of \( G \) and set \( G_0 = K/K_0 \); \( G_0 \) is then the group of \( k \)-points of an algebraic group of parahoric type defined and split over \( k \) which has the same root datum as \( \mathcal{G} \); moreover, since \( K \) is necessarily special, \( G_0 \) is not solvable. Let \( \mathbb{B}_0 \) be any pseudo-Borel subgroup of \( G_0 \); consider a pseudo-Levi decomposition \( \mathbb{B}_0 = \mathbb{H}_0 \mathbb{U}_0 \) of \( \mathbb{B}_0 \) and let \( \phi \) be a group isomorphism between \( \mathbb{U}_0 \) and \( \mathbb{U}_0 \) coming from a ring isomorphism between \( R_\alpha \) and \( \mathcal{O}/\mathfrak{p}^h \); \( \phi \) can be extended to an isomorphism from \( \mathbb{B} \) to \( \mathbb{B}_0 \) by setting, for \( h \in \mathbb{H}_0 \), \( \phi(h) = h_0 \) where \( h_0 \) is the unique element of the group \( \mathbb{H}_{\alpha,0} \) corresponding to \( \mathbb{H}_0 \) in \( G_0 \) such that \( Ad(h_0)\phi(u) = \phi(Ad(h)u) \) for every \( u \in \mathbb{U} \), and choosing arbitrarily an isomorphism between \( \mathbb{Z} \) and the center \( \mathbb{Z}_0 \) of \( G_0 \). Let \( w_0 \) be the nontrivial element of the Weyl group of \( \mathbb{B}_0 \) relatively to the maximal torus \( T_0 \) of \( \mathbb{H}_0 \); we can extend \( \phi \) to a bijection between \( \mathbb{B}w\mathbb{B} \) and \( \mathbb{B}_0w_0\mathbb{B}_0 \) by choosing an arbitrary element \( n_0 \) (resp. \( n \)) of \( w_0 \) (resp \( w \)) and setting for every element \( g = unb \) of \( \mathbb{U}w\mathbb{B} = \mathbb{B}w\mathbb{B} \) such that \( gg' \in \mathbb{B}w\mathbb{B} \), \( \phi(unb) = \phi(u)n_0\phi(b) \).

It remains to check that \( \phi(gg') = \phi(g)\phi(g') \) for every \( g, g' \in \mathbb{B}w\mathbb{B} \). We see immediately from the definitions that we can assume \( g \in w\mathbb{B} \) and \( g' \in \mathbb{U}w \); moreover, writing \( g = nhu \) and \( g' = uu'n^{-1} \), with \( n \in w_0 \), \( h \in \mathbb{H} \) and \( u, u' \in \mathbb{U}_\alpha \), the condition \( gg' \in \mathbb{B}w\mathbb{B} \) is equivalent to \( v(uu') = 0 \). Moreover, we have \( \phi(g) = \phi(nhn^{-1})\phi(n)\phi(u) \), \( \phi(g') = \phi(u')\phi(n^{-1}) \) and \( \phi(uu') = \phi(u)\phi(u') \), which shows that we can assume \( h = u' = 1 \).

Since we can always replace \( n \) by another element of \( w \), we can assume \( n \) is of the form \( n = uu' - u = u'uu' \), with \( u \in \mathbb{U}_\alpha \). We then have, by definition of \( \phi \):

\[ \phi(u^-) = \phi(u)^{-1}\phi(n)\phi(u)^{-1}, \]

hence:

\[ \phi(n) = \phi(u)\phi(u^-)\phi(u) = \phi(u^-)\phi(u)\phi(u^-), \]

hence:

\[ \phi(nu)\phi(n^{-1}) = \phi(n)\phi(u)\phi(n^{-1}) \]
\[ = \phi(u^-)\phi(u)\phi(u^-)\phi(n)\phi(n^{-1}) \]
\[ = \phi(u^-)\phi(n)\phi(n)^{-1} = \phi(u^-) = \phi(nun^{-1}). \]

which proves the proposition. \( \square \)
Now we’ll prove a relation between some elements of $G$ which will be useful in the sequel. Assume first $G$ is generated by $U_\alpha$ and $U_{-\alpha}$. Then $G$ is semisimple, hence isomorphic to either $SL_2$ or $PGL_2$, hence can be written as (a quotient of) a group of $2 \times 2$ matrices, and it is then also the case for $G_0$. We can then assume that $H_0$ is the Cartan subgroup of diagonal elements of $G_0$, and that $U_0$ (resp. the image of $U_{-\alpha}$ in $G_0$) is the subgroup of upper (resp. lower) triangular elements of $G$ with both diagonal terms being 1. (Note that we can’t just say “unipotent upper (lower) triangular elements because an upper (lower) triangular element of $G$ may be unipotent while having diagonal terms different from 1.)

For every $u \in U_\alpha$ (resp. $U_{-\alpha}$), if $x$ is the corresponding element in $R_\alpha$ (resp. $R_{-\alpha}$), we’ll write $u = u_{\alpha,x}$ (resp. $u = u_{-\alpha,x}$). If $h$ is the inverse image of $\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$ (resp. $\begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix}$) in $H_\alpha$ we’ll write $h = h_{\alpha^\vee,x}$ (resp. $h = h_{-\alpha^\vee,x}$). Note that for every $x \in R_\alpha^*$, we have $h_{-\alpha^\vee,x} = h_{\alpha^\vee,x}^{-1}$.

In the general case, since $H_\alpha$ is contained in the subgroup $G_\alpha$ of $G$ generated by $U_\alpha$ and $U_{-\alpha}$, which is itself a group of parahoric type, we’ll define $h_{\alpha^\vee,x}$ as an element of $G_\alpha$ the same way as above.

**Proposition 4.5.** For suitable choices of the unit elements in $U_\alpha$ and $U_{-\alpha}$, we have, for every $\lambda \in R_\alpha$, $\lambda \neq -1$:

$$u_{-\alpha,\lambda} u_{\alpha,1} = u_{\alpha,\frac{1}{\lambda}} h_{\alpha^\vee,\frac{1}{\lambda}} u_{-\alpha,1} \cdot$$

We see by an easy matrix computation that the result is true in $G_0$. By the isomorphism obtained in the previous proposition, it is true in $G$ as well. \(\Box\)

**4.2. The solvable case.** Now we’ll examine the case when $G$ is solvable. We’ll define the elements $u_{\alpha,x}$ of $U_\alpha$ the same way as in the previous subsection; same for the $u_{-\alpha,x}$. Moreover, we can easily find an isomorphism between $H_\alpha$ and the subgroup of diagonal elements of (a quotient of) a group of $2 \times 2$ matrices, which allow us to define the elements $h_{\alpha^\vee,x}$ as above as well. We can choose the isomorphism in such a way that $Ad(h_{\alpha^\vee,x})(u_{\alpha,y}) = u_{\alpha,x^2y}$ for every $x, y$; we then have $Ad(h_{\alpha^\vee,x})(u_{-\alpha,y}) = u_{-\alpha,\frac{x}{y^2}}$ for every $x, y$.

**Proposition 4.6.** Assume $G$ is solvable of semisimple rank 1. Then if $\pm \alpha$ are the elements of $\Phi$, $R_\alpha$ and $R_{-\alpha}$ are isomorphic, and there exists a henselian nonarchimedean local field $F$ of residual field $k$ and an algebraic group $G$ of type $A_1$ defined and split over $F$ such that $G$ is isomorphic to the quotient of an Iwahori subgroup of the group $G$ of $F$-points of $\mathbb{G}$ by its $h$-th congruence subgroup.

Let $\pm \alpha$ be the elements of $\Phi$: we have an Iwahori decomposition:

$$G = U_\alpha H \cup U_{-\alpha}.$$ 

We deduce from that decomposition that there exists functions $a, b, c$ from $R_{-\alpha}$ to respectively $R_\alpha$, $H_\alpha$, $R_{-\alpha}$ such that we have, for every $\lambda \in R_{-\alpha}$:

$$u_{-\alpha,\lambda} u_{\alpha,1} = u_{\alpha,a(\lambda)} h_{\alpha^\vee,b(\lambda)} u_{-\alpha,c(\lambda)}. $$
Similarly, there exist functions $a', b', c'$ from $R_{\alpha}$ to respectively $R_{-\alpha}, H_{\alpha}, R_{\alpha}$ such that for every $\lambda' \in R_{\alpha}$: we have:

$$u_{\alpha,\lambda'}u_{-\alpha,1} = u_{-\alpha,a'(-\lambda)}h_{\alpha\vee, b'(-\lambda')}u_{\alpha,c'(-\lambda')}.$$

These six functions are morphisms of $k$-varieties.

Let $\phi$ be the isomorphism between $R_{\alpha}^*$ and $R_{-\alpha}^*$ such that for every $h \in H$, $\phi(Ad(h)u_{\alpha,1}) = Ad(h)^{-1}u_{-\alpha,1}$. Choose (arbitrarily for the moment) an uniformizer $\varpi$ of $R_{-\alpha}$ and an uniformizer $\varpi'$ of $R_{\alpha}$; $\phi$ extends to a semigroup isomorphism between $R_{\alpha}$ and $R_{-\alpha}$ (viewed as multiplicative semigroups) by setting $\phi(\varpi') = \varpi$.

Assume $v(\lambda) = 0$. Let $\mu$ be a square root of $-\lambda$ in $R_{-\alpha}$; by conjugating the previous expression by $h_{\alpha\vee, \mu}$, we obtain:

$$u_{-\alpha,-1}u_{\alpha,\phi^{-1}(-\lambda)} = u_{\alpha,\phi^{-1}(-\lambda)\lambda a(\lambda)}h_{\alpha\vee, b(\lambda)}u_{-\alpha,-c(\lambda)};$$

from which we deduce that for every $\lambda$ such that $v(\lambda) = 0$, we have:

$$\lambda a'\phi^{-1}(\lambda) = c(\lambda),$$
$$b'(\phi^{-1}(\lambda)) = b(\lambda)^{-1};$$
$$c'(\phi^{-1}(\lambda)) = \lambda a(\lambda).$$

When $v(\lambda) > 0$ may the left-hand sides of these three equalities depend on the choice of $\phi$; we'll find a suitable $\phi$ later in the proof of the proposition. we can already remark that all three of them are trivially true when $\lambda = 0$.

Now we'll prove a few unicity lemmas:

**Lemma 4.7.** Let $\lambda, \lambda'$ be two elements of $R_{-\alpha}$. Assume that $a(\lambda) = a(\lambda')$. Then $\lambda$ and $\lambda'$ differ only by an element of $p_{-\alpha}^{h-2}$.

We have:

$$u_{\alpha,-1}u_{-\alpha,\lambda'-\lambda}u_{\alpha,1} = u_{-\alpha,-c(\lambda)}h_{\alpha\vee, b(\lambda)-1}\lambda b(\lambda')u_{\alpha,c(\lambda')}.$$

The right-hand side is an element of $B^- = HU_{-\alpha}$, and we deduce from the definition of a group of parahoric type that the left-hand side belongs to $B^-$ only if $\lambda - \lambda' \in p_{-\alpha}^{h-2}$, which proves the lemma. □

**Lemma 4.8.** Let $\lambda, \lambda'$ be two elements of $R_{-\alpha}$. Assume that $c(\lambda) = c(\lambda')$. Then $\lambda = \lambda'$.

We have:

$$u_{-\alpha,\lambda'-\lambda} = u_{\alpha,a(\lambda)h_{\alpha\vee, b(\lambda)}\lambda^{-1}u_{\alpha,-a(\lambda')}}$$

The left-hand side belongs to $U_{-\alpha}$ and the right-hand side to $B = HU_{\alpha}$; since the intersection of these two groups is trivial, the assertion follows. □

**Lemma 4.9.** Let $\lambda, \lambda'$ be two elements of $R_{-\alpha}$. Assume that $b(\lambda) = b(\lambda')$. Then $\lambda = \lambda'$.
We have:
\[
[u_{\alpha,-1}, u_{-\alpha,\lambda}] = u_{\alpha,a(\lambda)-1} h_{\alpha^\vee,b(\lambda)} u_{-\alpha,c(\lambda)-\lambda}
\]
and a similar expression with \(\lambda'\) instead of \(\lambda\). The result then follows immediately from the following lemma:

**Lemma 4.10.** The application \(\psi\) which associates to every \(u \in U_{-\alpha}\) the projection on \(H\) of \([u_{\alpha,-1}, u]\) is a bijective morphism of \(k\)-varieties between \(U_{-\alpha}\) and \(H_{\alpha^\vee,1}\).

From the definition of a group of parahoric type, we know that every element of \(H_{\alpha^\vee,h-1}\) is the projection on \(H\) of \([u, u']\) for some \(u \in U_{-\alpha,h-2}\) and some \(u' \in U_{\alpha}\), which we can assume to be of valuation 0. By conjugating the commutator by an appropriate element of \(H\) we can even assume \(u' = u_{\alpha,-1}\). The restriction of \(\psi\) to \(U_{-\alpha,h-2}\) is then a surjective morphism of \(k\)-varieties.

On the other hand, \(H_{\alpha^\vee,h-1}\) lies in the center of \(G\), and a simple computation shows that the restriction of \(\psi\) to \(U_{-\alpha,h-2}\) is a morphism of algebraic groups between \(U_{-\alpha,h-2}\) and \(H_{\alpha^\vee,h-1}\). Since both groups are isomorphic to \(G^m\) and the above morphism is surjective, it must be bijective.

For every \(i < h\), by replacing \(G\) by its quotient by its \(i\)-th congruence subgroup, we see in a similar way that the restriction of \(\psi\) to \(U_{-\alpha,i-2}\) factors into a bijective morphism of \(k\)-varieties between \(U_{-\alpha,i-2}/U_{-\alpha,i-1}\) and \(H_{\alpha^\vee,i-1}/H_{\alpha^\vee,i}\). By combining all these morphisms we see that \(\psi\) is a bijective morphism as well. □

These unicity results imply in particular that for every uniformizer \(\varpi'\) of \(R_{\alpha}\), there exists a unique uniformizer \(\varpi\) of \(R_{-\alpha}\) such that \(b(\varpi) = b'(\varpi')^{-1}\). From now on we will assume that the uniformizers \(\varpi\) and \(\varpi'\) we have chosen in the definition of \(\phi\) satisfy that condition.

Now we’ll prove that \(R_{\alpha}\) and \(R_{-\alpha}\) are isomorphic. Since we already know that \(\phi\) is a semigroup isomorphism between \((R_{\alpha}, *)\) and \((R_{-\alpha}, *)\), it remains to prove that \(\phi\) is a group isomorphism between \((R_{\alpha}, +)\) and \((R_{-\alpha}, +)\).

Let \(\lambda, \mu\) be two elements of \(R_{-\alpha}\). We have:
\[
u(\lambda) = 0\)
and let \(\nu\) be a square root of \(a(\lambda)\) in \(R_{\alpha}\); we have:
\[
u(\lambda) = h_{\alpha^\vee,\nu} \phi(\alpha(\lambda)) u_{\alpha,1} h_{\alpha^\vee,\nu}^{-1}
\]
\[
u(\lambda) = u_{\alpha,1} \phi(\alpha(\lambda)) u_{\alpha,1} h_{\alpha^\vee,\nu}^{-1}
\]
from which we deduce the following expressions:
\[
a(\lambda + \mu) = a(\lambda) a(\lambda) \phi(\alpha(\lambda)) \mu;
\]
\[
b(\lambda + \mu) = b(\lambda) b(\phi(\alpha(\lambda)) \mu);
\]
\[
c(\lambda + \mu) = c(\lambda) + \phi(b(\lambda)^2 b(\phi(\alpha(\lambda)) \mu))
\]
We will check that these expressions remain true when $v(\lambda) \neq 0$. Let $\lambda_1, \lambda_2$ be any two elements of $R_{-\alpha}$ such that $v(\lambda_1) = v(\lambda_2) = 0$ and $\lambda_1 + \lambda_2 = \lambda$; we have:

$$
\begin{align*}
 b(\lambda + \mu) &= b(\lambda_1 + (\lambda_2 + \mu)) \\
 &= b(\lambda_1)b(\phi(a(\lambda_1)))(\lambda_2 + \mu)) \\
 &= b(\lambda_1)b(\phi(a(\lambda_1))\lambda_2)b(\phi(a(\phi(a(\lambda_1))\lambda_2))\phi(a(\lambda_1))\mu) \\
 &= b(\lambda_1 + \lambda_2)b(\phi(a(\lambda_1 + \lambda_2))\mu) \\
 &= b(\lambda)b(\phi(a(\lambda))\mu).
\end{align*}
$$

The proof for $a$ is obtained by simply replacing $b$ with $a$ in the above expressions. The proof for $c$ is also very similar and is left to the reader.

Similarly, we have, for every $\lambda', \mu' \in R_{\alpha}$:

$$
\begin{align*}
 a'(\lambda' + \mu') &= a'(\lambda')a'(\phi^{-1}(a'(\lambda'))\mu'); \\
 b'(\lambda' + \mu') &= b'(\lambda')b'(\phi^{-1}(a'(\lambda'))\mu'); \\
 c'(\lambda' + \mu') &= c'(\lambda') + \frac{b'(\lambda')^2}{\phi^{-1}(a'(\lambda'))}c'(\phi^{-1}(a'(\lambda'))\mu').
\end{align*}
$$

For every $\lambda \in R_{-\alpha}$, we can set $\mu = -\lambda$ to obtain:

$$
1 = b(0) = b(\lambda)b(-\phi(a(\lambda))\lambda).
$$

On the other hand, since $-1$ is the only square root of 1 different from 1 in $R_{-\alpha}$ we must have $\phi(-1) = -1$, hence $\phi^{-1}(-\lambda) = -\phi^{-1}(\lambda)$ and:

$$
1 = b'(0) = b'(\phi(\lambda))b'(-\phi^{-1}(a'(\phi^{-1}(\lambda))\lambda)).
$$

Assume $v(\lambda) = 0$; since we know that $b'(\phi^{-1}(\lambda)) = b(\lambda)^{-1}$, we obtain:

$$
b(-\phi(a(\lambda))\lambda) = b'(-\phi^{-1}(a'(\phi^{-1}(\lambda))\lambda))^{-1}.
$$

On the other hand, we have:

$$
b(-\phi(a(\lambda))\lambda) = b'(-a(\lambda)\phi^{-1}(\lambda))^{-1}.
$$

By unicity (lemma 4.9), we obtain:

$$
a'(\phi^{-1}(\lambda)) = -\phi(a(\lambda)).
$$

Now let $\mu$ be an element of $R_{-\alpha}$ such that either $v(\mu) = 0$ or $\phi(a(\lambda))\mu = v$. We have:

$$
\begin{align*}
 b(\lambda + \mu) &= b(\lambda)b(\phi(a(\lambda))\mu) \\
 &= b'(\phi^{-1}(\lambda))^{-1}b'(a(\lambda)\phi^{-1}(\mu))^{-1} \\
 &= b'(\phi^{-1}(\lambda))^{-1}b'(\phi^{-1}(a'(\phi^{-1}(\lambda))\mu))^{-1} \\
 &= b'(\phi^{-1}(\lambda) + \phi^{-1}(\mu))^{-1}.
\end{align*}
$$

Assume now that either $v(\lambda + \mu) = 0$ or $\lambda + \mu = v$, we also have:

$$
b(\lambda + \mu) = b'(\phi^{-1}(\lambda + \mu))^{-1}.
$$

hence by unicity (lemma 4.9 again):

$$
\phi^{-1}(\lambda + \mu) = \phi^{-1}(\lambda) + \phi^{-1}(\mu).
$$
Using the facts that $\phi(-1) = -1$ and that $\phi$ is a multiplicative semigroup isomorphism, we see that the above equality is true as soon as two of $\lambda, \mu, \lambda + \mu$ have the same valuation $v$ and that the third one has valuation either $v$ or $v + 1$. We will now prove by induction that it remains true when the third one has any valuation $v' \geq v$; since by the properties of valuations this is always true, it will be enough to prove that $\phi$ is a ring isomorphism.

We can assume that $\mu$ is the element with the greater valuation. Assume then $v' - v \geq 2$ and let $\nu$ be an element of $R_\alpha$ such that $v < v(\nu) < v'$. We have, applying the induction hypothesis at each step:

$$
\phi^{-1}(\lambda + \mu) + \phi^{-1}(\nu) = \phi^{-1}(\lambda + \mu + \nu)
$$

$$
= \phi^{-1}(\lambda) + \phi^{-1}(\mu + \nu) = \phi^{-1}(\lambda) + \phi^{-1}(\mu) + \phi^{-1}(\nu),
$$

which proves the desired identity.

In the sequel we will drop $\phi$ and identify $R_\alpha$ with $R_{-\alpha}$ to simplify the notations. Note though that we still don’t know whether $\phi$ is algebraic on $R_\alpha$.

For every $\lambda \in R_{-\alpha}$ such that $v(\lambda) = 0$, we have:

$$
c(\lambda) = \lambda a'(\lambda) = \lambda a(\lambda).
$$

This is obviously also true when $\lambda = 0$.

Let $\lambda, \mu, \lambda + \mu$ be three elements of $R_{\alpha}$ which are either zero or of valuation 0; we have:

$$(\lambda + \mu)a(\lambda + \mu) = \lambda a(\lambda) + \frac{b(\lambda)^2}{a(\lambda)} a(\lambda) \mu a(\lambda) \mu,$$

hence, since $a(\lambda + \mu) = a(\lambda)a(a(\lambda)\mu)$:

$$(\lambda + \mu - \frac{b(\lambda)^2}{a(\lambda)} \mu)a(\lambda + \mu) = \lambda a(\lambda).$$

When $\lambda + \mu = 0$ and $\lambda, \mu \neq 0$, we get:

$$
\frac{b(\lambda)^2}{a(\lambda)} \lambda = \lambda a(\lambda),
$$

hence $b(\lambda)^2 = a(\lambda)^2$. Since both $a$ and $b$ have their image contained in $1+p_\alpha$, we must have $a(\lambda) = b(\lambda)$. We thus obtain:

$$a(\lambda + \mu) = \frac{\lambda a(\lambda)}{\lambda + (1 - a(\lambda))\mu}.$$

Now we can assume $\varpi$ to be the unique uniformizer of $R_{-\alpha}$ such that $b(1) = \frac{1}{1+\varpi}$. We then also have $a(1) = \frac{1}{1+\varpi}$, and for every $\lambda$ such that $v(\lambda)$ and $v(\lambda - 1)$ are both zero, we have:

$$a(\lambda) = a(1 + (\lambda - 1)) = \frac{\frac{1+\varpi}{\lambda} + \frac{1-\lambda}{1+\varpi}}.$$
A CHARACTERIZATION OF GROUPS OF PARAHORIC TYPE

\[ \frac{1}{(1 + \varpi)\lambda + 1 - \lambda} = \frac{1}{1 + \varpi\lambda}. \]

Since the set of such \( \lambda \) is a Zariski-dense open subset of \( R_{-\alpha} \) and \( a \) and \( \lambda \mapsto \frac{1}{1 + \varpi\lambda} \) are both maps of \( k \)-varieties, the equality holds for every \( \lambda \in R_{-\alpha} \). We obtain similarly that for every \( \lambda \in R_{-\alpha} \), we have:

\[ b(\lambda) = \frac{1}{1 + \varpi\lambda}, \quad c(\lambda) = \frac{\lambda}{1 + \varpi\lambda}. \]

Let now \( F \) and \( G \) defined as in the previous section. Assume first \( G \) is semisimple; then it is isomorphic to either \( SL_2 \) or \( PSL_2 \). Let \( G \) be the group of \( F \)-points of \( G \), and let \( I \) be the Iwahori group of the elements of \( G(\mathcal{O}_F) \) which are upper triangular mod \( p_F \), and set \( \mathcal{G}_0 = K/K^h \). Consider now the map:

\[ u_{\alpha,\lambda} h_{\alpha^\vee,\mu} u_{-\alpha,\nu} \mapsto \left( \begin{array}{cc} 1 & \lambda \\ 1 & 1 \end{array} \right) \left( \begin{array}{cc} \mu & 0 \\ 0 & \mu^{-1} \end{array} \right) \left( \begin{array}{cc} 1 & \varpi\lambda \\ 1 & 1 \end{array} \right) \]

from \( \mathcal{G} \) to \( \mathcal{G}_0 \); with the help of easy matrix computations we see that it is an isomorphism. The general case follows easily. □

5. A More Detailed Study of the Commutator Relations

Now we return to the case when \( \Phi \) is of any rank. In [4], Chevalley has computed some structural constants for reductive groups, which arise when we study in detail the commutator relations. Our goal in this section is to find similar constants for groups of parahoric type; we will prove that these constants are in fact similar to the Chevalley constants.

In this section, we will assume that all the \( R_\alpha, \alpha \in \Psi \), are isomorphic to each other. This allows us to introduce a nonarchimedean henselian local field \( F \) such that any \( R_\alpha \) is isomorphic to the quotient \( \mathcal{O}_F/p_F^i \); \( i \) being either \( h \) or \( h-1 \) depending whether \( \alpha \) lies in \( \Psi \) or not. We will also set \( R = \mathcal{O}_F/p_F^h \); for every \( \alpha \in \Phi \), \( \mathbb{H}_\alpha \) is then isomorphic to the unit ring \( \mathbb{R}^* \) of \( \mathbb{R} \).

5.1. Generalities. Let \( \varpi_F \) be an uniformizer of \( F \). For every \( \alpha \in \Phi \), let’s define the element \( u_{\alpha,x}, x \in \varpi^{f_0(\alpha)} \mathcal{O}_F/\varpi^{h-f_0(-\alpha)} \mathcal{O}_F \) the following way: choose \( u_{\alpha,\varpi^{f_0(\alpha)}} \) arbitrarily (for the moment), and for every \( x \in R_\alpha \), set \( u_{\alpha,\varpi^{f_0(\alpha)}x} \) as the element of \( \mathbb{U}_\alpha \) corresponding to \( x \).

Note that this definition is not consistent with the one we have previously used in the case of groups of rank one, but it has the advantage of greatly simplifying the notations when dealing with the Chevalley constants. When \( \alpha \in \Psi \), with a suitable choice of \( u_{\alpha,\varpi^{f_0(\alpha)}} \), we can always manage to make the proposition [4.5] still work. When \( \alpha \not\in \Psi \), it is not hard to see that the expressions we have found for the functions \( a, b, c \) also yield the result of proposition [4.5] for a suitable choice of \( u_{\alpha,\varpi^{f_0(\alpha)}} \).

First we’ll check the existence of our constants:
Proposition 5.1. Let $\alpha, \beta$ be two elements of $\Phi$ such that $\alpha + \beta \in \Phi$. There exist elements $c_{\alpha,\beta,i,j}$ of $R$, with $i,j$ being positive integers such that $i\alpha + j\beta \in \Phi$, such that we have, for every $x, y \in R$:

$$[u_{\alpha,\lambda}, u_{\beta,\mu}] = \prod_{i,j} u_{i\alpha+j\beta, c_{\alpha,\beta,i,j}, \lambda', \mu'}.$$

Let’s define the $c_{\alpha,\beta,i,j}$ as the ones satisfying the above equality for $\lambda = \mu = 1$; we’ll prove that the above equality holds for any $\lambda$ (still with $\mu = 1$). First assume $v(\lambda) = 0$. Since $\alpha + \beta$ is a root and $\Phi$ is reduced, $\alpha$ and $\beta$ are linearly independent; there exists then an element $h$ of $\mathbb{H}$ commuting with $U_\beta$ and such that $Ad(h)u_{\alpha,1} = u_{\alpha,h}$. We then have:

$$[u_{\alpha,\lambda}, u_{\beta,1}] = Ad(h)[u_{\alpha,1}, u_{\beta,1}] = \prod_{i,j} Ad(h)u_{i\alpha+j\beta, c_{\alpha,\beta,i,j}}.$$

By the same reasoning as in the proof of proposition 3.13 and an obvious induction we see that $Ad(h)u_{i\alpha+j\beta, c_{\alpha,\beta,i,j}} = u_{i\alpha+j\beta, c_{\alpha,\beta,i,j}}$ for any $j$ such that $\alpha + j\beta$ is a root. Moreover, assuming $2\alpha + \beta$ is a root and applying the previous equality to $(\alpha, \alpha + \beta)$, we see that $Ad(h)u_{2\alpha+\beta, c_{\alpha,\beta,2,1}}$ is the projection on $U_{2\alpha+\beta}$ of:

$$[Ad(h)u_{\alpha, c_{\alpha,\beta,2,1}}^{-1}, Ad(h)u_{\alpha+\beta,1}] = [u_{\alpha, c_{\alpha,\beta,2,1}}^{-1} c_{\alpha+\beta,1,1}, u_{\alpha+\beta,1}],$$

hence $Ad(h)u_{2\alpha+\beta, c_{\alpha,\beta,2,1}} = u_{2\alpha+\beta, c_{\alpha,\beta,2,1}}$. The case of the remaining pairs $(i,j)$ follow from an easy induction. By Zariski-density, the relations remain true when $v(\lambda) > 0$. Finally, the case of any $\mu$ with $\lambda$ arbitrarily fixed is treated symmetrically. □

To simplify the notation, when $i = j = 1$, we’ll write $c_{\alpha,\beta}$ instead of $c_{\alpha,\beta,1,1}$. Similarly, when $j = 1$ and there’s no ambiguity, we can drop it (i.e. write $c_{\alpha,\beta,i}$ instead of $c_{\alpha,\beta,i,1}$); we can do the same when $i = 1$.

Note that although the $c_{\alpha,\beta,i,j}$ are elements of $R_{\alpha+\beta}$, they are in general only defined up to some ideal of $R_{\alpha+\beta}$. More precisely, set $d = h - f_0(-i\alpha - j\beta) - if_0(\alpha) - jf_0(\beta)$; the constant $c_{\alpha,\beta,i,j}$ is an element of the quotient of $R_{\alpha}$ by its ideal of elements of valuation $\geq d$. (If $d \leq 0$, that simply means that the term in $U_{i\alpha+j\beta}$ in the decomposition of $[u_{\alpha,\lambda}, u_{\beta,\mu}]$ is trivial.)

By a slight abuse of notation, for such constants we will write $c = c'$ instead of "if $d$ (resp. $d'$) is the integer associated to $c$ (resp. $c'$) as above, $c$ and $c'$ are identical up to an element of valuation at least $\inf (d, d')$ of $R$. We will make a similar abuse with expressions of the form $cc' = x$, with $x$ being an element of $R$. Note that this kind of "equality" is not transitive; we thus have to be particularly careful when manipulating it.

We’ll first prove a few preliminary results:

Proposition 5.2. For every $\alpha, \beta \in \Phi$ such that $\alpha + \beta \in \Phi$, we have $c_{\beta,\alpha} = -c_{\alpha,\beta}$.

Let $U'$ be the product of the $U_{i\alpha+j\beta}$, with $i, j > 0$ and $i + j > 2$; it is obvious from the commutator relations that $U_{\alpha+\beta}$ normalises $U'$. Moreover, we have
\[ [u_{\alpha,1}, u_{\beta,1}] \in u_{\alpha+\beta,c_{\alpha,\beta}} U' \text{ and } [u_{\beta,1}, u_{\alpha,1}] \in u_{\alpha+\beta,c_{\beta,\alpha}} U'; \text{ since these two commutators are inverse of each other, we must have } u_{\alpha+\beta,c_{\alpha,\beta}} = u_{\alpha+\beta,c_{\beta,\alpha}}^{-1}, \text{ hence the result.} \]

\[ \square \]

**Lemma 5.3.** Let \( n \) be a positive integer. The relation on the subsets of \( \{1, \ldots, n\} \) defined by \( I \leq J \) if either \( I = J \) or the smallest element of their symmetrical difference belongs to \( I \) is a total order.

It is obvious that the relation is reflexive, antisymmetrical, and that for every \( I, J \) we have either \( I \leq J \) or \( J \leq I \); we only have to check transitivity. Let \( I \leq J \leq K \) be three subsets of \( \{1, \ldots, n\} \); since the result is trivial when two of them are identical, we may assume \( I < J < K \). Let \( x \) (resp. \( y \)) be the smallest element of the symmetrical difference between \( I \) and \( J \) (resp. \( J \) and \( K \)). Then \( x \) belongs to \( J \) and \( x \) doesn’t, hence \( x \neq y \). Moreover, we have:

- if \( x < y \), then \( x \) doesn’t belong to the symmetrical difference between \( J \) and \( K \), hence \( x \notin K \);
- if \( x > y \), then \( y \) doesn’t belong to the symmetrical difference between \( I \) and \( J \), hence \( y \in I \);

In both cases, \( \inf(x, y) \) belongs to \( I \) and not to \( K \). On the other hand, for every \( z \in \inf(x, y) \), \( z \) belongs either to all three subsets or to none of them. Hence \( I < K \) and the lemma is proved. \( \square \)

We’ll use this lemma to prove the following result:

**Proposition 5.4.** Let \( a_1, \ldots, a_n, b \) be elements of a group \( G \) such that all the \( a_i \) commute. We have:

\[ [a_1, [a_2, \ldots, [a_n, b] \ldots]] = \prod_{I \subseteq \{1, \ldots, n\}} \prod_{i \in I} [a_i, b]^{n-\#(I)} \]

where the product is taken with the following order on the subsets of \( \{1, \ldots, n\} \): for every \( I \neq J, I \) precedes \( J \) if the smallest element of their symmetrical difference belongs to \( I \).

We’ll prove the result by induction on \( n \), the case \( n = 1 \) being trivial. Assume first \( n = 2 \); we have:

\[ [a_1, [a_2, b]] = a_1 a_2 b a_2^{-1} b^{-1} a_1^{-1} b a_2 b^{-1} a_2^{-1} = (a_1 a_2 b a_2^{-1} a_1^{-1} b)(b a_1 b^{-1} a_1^{-1})(b a_2 b^{-1} a_2^{-1}) = [a_1 a_2, b][a_1, b]^{-1}[a_2, b]^{-1}. \]

Checking that the terms are in the correct order is immediate. Note that \( [1, b] = 1 \).

Now assume \( n > 2 \). Applying the case \( n = 2 \) to \( a_1, a_2 \) and \( [a_3, \ldots, [a_n, b] \ldots] \), we obtain:

\[ [a_1, [a_2, \ldots, [a_n, b] \ldots]] = [a_1 a_2, [a_3, \ldots, a_n, b] \ldots][a_1, [a_3, \ldots, [a_n, b] \ldots]]^{-1}[a_2, [a_3, \ldots, [a_n, b] \ldots]]^{-1}; \]
Applying the induction hypothesis to each of the three terms of the right-hand side, and remarking that in the first two, the terms coming from \([a_3, \ldots, [a_n, b] \ldots]\) cancel out, we obtain the result of the lemma up to the order of the terms; checking that they actually are in the desired order is straightforward. □

**Proposition 5.5.** Let \(\alpha, \beta, \gamma\) be three elements of \(\Phi\) such that \(\alpha + \beta, \alpha + \gamma\) and \(\alpha + \beta + \gamma\) are roots but \(\beta + \gamma\) is neither a root nor 0. We have:

\[c_{\alpha, \beta}c_{\gamma, \alpha+\beta} = c_{\gamma, \alpha}c_{\alpha+\gamma, \beta}.\]

We’ll first prove the following lemma:

**Lemma 5.6.** Let \(h, h', h''\) be three elements of a group \(H\), such that \(h'\) and \(h''\) commute; we have:

\[[[h, h'], h''] = h[[h^{-1}, h'], h'']^{-1}h^{-1}.\]

By rewriting the right-hand side as \(h[[h', [h^{-1}, h'']]h^{-1}\) and developing both sides we immediately obtain the result. □

Now we’ll prove the proposition. Assume that the only triplet \((i, j, k)\) of positive integers such that \(i\alpha + j\beta + k\gamma = \alpha + \beta + \gamma\) is \((1, 1, 1)\). By applying the above lemma to \(u_{\alpha, 1}, u_{\beta, 1}, u_{\gamma, 1}\) and considering only the terms in \(u_{\alpha+j\beta+k\gamma}\) in both sides, we obtain the assertion of the proposition.

Assume now there exists a triplet \((i, j, k)\) different from \((1, 1, 1)\) such that \(i\alpha + j\beta + k\gamma = \alpha + \beta + \gamma\). We then have \((i-1)\alpha + (j-1)\beta + (k-1)\gamma = 0\). Since \(\alpha\) and \(\beta\) (resp. \(\alpha\) and \(\gamma\)) are not proportional, we have \(k \neq 1\) (resp. \(j \neq 1\)). If \(i = 1\), then \(\beta\) must be equal to \(-\gamma\), which leads to a contradiction. If \(i > 1\), then \((1-i)\alpha\) is a linear combination with positive integer coefficients of \(\beta\) and \(\gamma\), which implies (using [II, proposition 19] and the fact that \(\Phi\) is reduced) that \(\beta + \gamma\) must be a root, hence another contradiction. □

The next three subsections will be devoted to establishing relations between our structural constants by examining what happens in subsystems of rank 2 of \(\Phi\). Let \(\alpha, \beta\) be two linearly independent elements of \(\Phi\) such that \(\alpha + \beta\) is a root and \(\alpha - \beta\) is not. We can always assume that \(f_0\) is such that \(f_0(\alpha) = f_0(\beta) = 0\). We will also assume that when \(\alpha\) and \(\beta\) are of different length, \(\alpha\) is the shortest one.

**5.2. The \(A_2\) case.** Assume first that \(\alpha\) and \(\beta\) generate a subsystem of type \(A_2\) of \(\Phi\). Then the roots it contains are \(\pm \alpha, \pm \beta\) and \(\pm (\alpha + \beta)\), which are all of the same length.

**Proposition 5.7.** We have:

\[c_{\alpha, \beta}c_{\alpha+\beta, -\beta} = 1.\]

Moreover, for every \(\lambda \in R^*\) and every \(\mu \in R_\alpha\), we have \(Ad(h_{\beta^\vee, \lambda})(u_{\alpha^\vee, \mu}) = u_{\alpha^\vee, \frac{\lambda}{\mu}}\).

For any \(\lambda \neq 1\) such that \(u_{-\beta, \lambda}\) exists, we have:

\[[[u_{\alpha, 1}, u_{\beta, 1}], u_{-\beta, \lambda}] = [u_{\alpha+\beta, c_{\alpha, \beta}}, u_{-\beta, \lambda}] = u_{\alpha, c_{\alpha, \beta}c_{\alpha+\beta, -\beta} \lambda},\]
Proposition 5.8. We have:

\[ [u_{\alpha,1}, u_{\beta,1}] u_{-\beta,\lambda} = u_{-\beta,\lambda} u_{\alpha,c_{\alpha,\beta} c_{\alpha+\beta,-\beta} \lambda} u_{\alpha+\beta, c_{\alpha,\beta}}. \]

On the other hand, we have:

\[
\begin{align*}
[u_{\alpha,1}, u_{\beta,1}] u_{-\beta,\lambda} &= u_{\alpha,1} u_{\beta,1} u_{\alpha,-1} u_{\beta,1} u_{-\beta,\lambda} \\
&= u_{\alpha,1} u_{\beta,1} u_{\alpha,-1} u_{-\beta,1} u_{-\beta,\lambda} \frac{h_{\beta^\vee,1}^{-1} u_{\beta,1}}{u_{-\beta,1}^{-1}} \\
&= u_{\alpha,1} u_{\beta,1} u_{-\beta,1} u_{-\beta,\lambda} \frac{h_{\beta^\vee,1}^{-1} u_{\beta,1}}{u_{-\beta,1}^{-1}} \\
&= u_{\alpha,1} u_{-\beta,\lambda} h_{-\beta,1}^{-1} u_{\beta,1} \frac{h_{\beta^\vee,1}^{-1} u_{\beta,1}}{c_{\beta,\alpha} \lambda} \\
&= u_{-\lambda,\alpha} u_{\alpha,1} u_{\beta,1} \frac{h_{\beta^\vee,1}^{-1} u_{\beta,1}}{u_{-\beta,1}^{-1}} \\
&= u_{-\lambda,\alpha} u_{\alpha,1} u_{\beta,1} \frac{h_{\beta^\vee,1}^{-1} u_{\beta,1}}{u_{-\beta,1}^{-1}} \\
&= \text{where } u_{\alpha,\mu} = Ad(h_{\beta^\vee,1}) u_{\alpha,-1}. \] 

From the previous equality we see that we must have \( \mu = \lambda - 1, \) hence:

\[ [u_{\alpha,1}, u_{\beta,1}] u_{-\beta,\lambda} = u_{\alpha,\lambda} u_{-\beta,\lambda} [u_{\alpha,1} u_{\beta,1}^{1-x}] \]

Since we have:

\[ [u_{\alpha,1} u_{\beta,1}^{1-x}] = u_{\alpha+\beta, c_{\alpha,\beta}} = [u_{\alpha,1}, u_{\beta,1}], \]

we obtain that \( u_{\alpha,c_{\alpha,\beta} c_{\alpha+\beta,-\beta} \lambda} = u_{\alpha,\lambda} \) for every \( \lambda \neq 1, \) hence the first assertion.

Now let’s prove the second one. We see from above that for every \( \lambda \in R, \) we have \( Ad(h_{\beta^\vee,\lambda}) u_{\alpha,-1} = u_{\alpha,-\frac{1}{\lambda}} \) as soon as \( h_{\beta^\vee,\lambda} \) belongs to \( \mathbb{H}_{\beta,1}. \) By definition of a root subgroup this is also true when \( h_{\beta^\vee,\lambda} \in T_{\beta}, \) hence it is true for any \( \lambda. \) Since we know that for any element \( h \) of \( \mathbb{H}, \) \( Ad(h) \) acts on \( R_{\alpha} \) as the multiplication by some element of \( R_{\alpha}, \) the end of the proof is straightforward. \( \Box \)

Now we come to the point where we actually have to be careful about the rings in which the constants live. The following proposition, for example, can be easily deduced from the previous ones when at least one of \( \alpha, \beta, \alpha + \beta \) belongs to \( \Psi, \) but when none of those three roots lies in \( \Psi \) and \( f_{0}(\alpha + \beta) < f_{0}(\alpha) + f_{0}(\beta), \) \( c_{\alpha,\beta}, \) \( c_{\beta,-\alpha-\beta} \) and \( c_{-\alpha-\beta,\alpha} \) are defined up to an element of valuation \( h-1 \) of \( R, \) but the previous proposition only yields the relations below up to an element of valuation \( h-2 \) of \( R. \) We thus need to prove them directly.

Proposition 5.8. We have:

\[ c_{\alpha,\beta} = c_{\beta,-\alpha-\beta} = c_{-\alpha-\beta,\alpha}. \]

For every \( \lambda \neq 1 \) such that \( u_{\alpha,-\beta,\lambda} \) exists, we have:

\[ [u_{\alpha,1}, u_{\beta,1}] u_{-\alpha,-\beta,\lambda} = u_{\alpha+\beta, c_{\alpha,\beta} \lambda} u_{-\alpha,-\beta,\lambda} \]

On the other hand, we have:

\[ [u_{\alpha,1}, u_{\beta,1}] u_{(-\alpha,-\beta,\lambda)} = u_{\alpha,1} u_{\beta,1} u_{\alpha,-1} u_{\beta,1} u_{-\alpha,-\beta,\lambda} \]

\[ = u_{-\alpha,-\beta,\lambda} u_{-\alpha,-\beta,\lambda} u_{\alpha,1} u_{\beta,1} u_{-\alpha,-\beta,\lambda} u_{\alpha,-1} u_{-\alpha,-\beta,\lambda} u_{\alpha,-1} \\
= u_{-\alpha,-\beta,\lambda} u_{-\alpha,-\beta,\lambda} u_{\alpha,1} u_{\beta,1} u_{-\alpha,-\beta,\lambda} u_{\alpha,-1} u_{\alpha,-\beta,\lambda} u_{\alpha,-1} \\
= u_{-\alpha,-\beta,\lambda} u_{-\alpha,-\beta,\lambda} u_{\alpha,1} u_{\beta,1} u_{-\alpha,-\beta,\lambda} u_{\alpha,-1} u_{\alpha,-\beta,\lambda} u_{\alpha,-1} \\
**Corollary 5.9.** We have:

\[ c_{\alpha,\beta}c_{-\alpha,-\beta} = -1. \]

By the previous two propositions we have \( c_{\alpha,\beta}c_{\alpha+\beta,-\beta} = 1 \) and \( c_{\alpha+\beta,-\beta} = c_{-\alpha,-\beta} \), hence the result. \( \square \)

5.3. **The \( B_2 \) case.** Assume now \( \alpha \) and \( \beta \) generate a subsystem of \( \Phi \) of type \( B_2 \). The elements of \( \Phi \) are then \( \pm \alpha \) (short), \( \pm \beta \) (long), \( \pm (\alpha + \beta) \) (short) and \( \pm (2\alpha + \beta) \) (long). Moreover we have \( \alpha^\vee + \beta^\vee = (2\alpha + \beta)^\vee \) and \( 2\alpha^\vee + \beta^\vee = (\alpha + \beta)^\vee \).

**Proposition 5.10.** We have:

\[ c_{\beta,\alpha,2} = -c_{\alpha,\beta,2}. \]

This is immediate from the equality \([u_{\beta,1}, u_{\alpha,1}] = [u_{\alpha,1}, u_{\beta,1}]^{-1}\) and the fact that \( U_{\alpha+\beta} \) and \( U_{2\alpha+\beta} \) commute. \( \square \)

**Proposition 5.11.** We have:

\[ c_{\alpha,\beta,2} = \frac{1}{2} c_{\alpha,\beta} c_{\alpha+\beta}. \]

According to proposition 5.4 we have:

\[ [u_{\alpha,1}, [u_{\alpha,1}, u_{\beta,1}]] = [u_{\alpha,2}, u_{\beta,1}] [u_{\alpha,1}, u_{\beta,1}]^{-2}. \]

By evaluating both sides, we obtain:

\[ u_{2\alpha+\beta, c_\alpha, c_{\alpha+\beta}} = u_{\alpha+\beta, 2c_\alpha, c_{\alpha+\beta}} u_{2\alpha+\beta, 4c_\alpha, c_{\alpha+\beta}} u_{\alpha+\beta, c_\alpha, c_{\alpha+\beta}} u_{2\alpha+\beta, c_\alpha, c_{\alpha+\beta}}^{-2}, \]

hence, considering the terms in \( U_{2\alpha+\beta} \):

\[ c_{\alpha,\beta} c_{\alpha+\beta} = 2c_{\alpha,\beta,2}, \]

which proves the proposition. \( \square \)
Proposition 5.12. We have:
\[ c_{\alpha, \beta}c_{\alpha + \beta, -\beta} = 1. \]
Moreover, for every \( \lambda \in R^* \) and every \( \mu \in R_\alpha \), we have \( \text{Ad}(h_{\beta^\vee, \lambda})u_{\alpha, \mu} = u_{\alpha, \lambda \mu} \).

For every possible \( \lambda \), we have:
\[ [[u_{\alpha, 1}, u_{\beta, 1}], u_{-\beta, \lambda}] = [u_{\alpha + \beta, c_{\alpha, \beta}}u_{2\alpha + \beta, c_{\alpha, \beta}, 2}, u_{-\beta, \lambda}]. \]
Using proposition 5.4, we see that the right-hand side is equal to:
\[ [u_{\alpha + \beta, c_{\alpha, \beta}}, [u_{2\alpha + \beta, c_{\alpha, \beta}, 2}, u_{-\beta, \lambda}]] = [u_{\alpha + \beta, c_{\alpha, \beta}}, u_{\alpha + \beta, c_{\alpha, \beta}, 2}, u_{-\beta, \lambda}]. \]
Since \((2\alpha + \beta) - \beta = 2\alpha\) is not a root, only the last commutator is nontrivial, and we thus obtain:
\[ [[u_{\alpha, 1}, u_{\beta, 1}], u_{-\beta, \lambda}] = u_{\alpha, c_{\alpha, \beta}c_{\alpha + \beta, -\beta}, \lambda}. \]
The rest of the proof is similar to the proof of proposition 5.7. \( \square \)

Proposition 5.13. We have:
\[ c_{\beta, \alpha}c_{\alpha + \beta, -\alpha} = 2. \]
Moreover, for every \( \lambda \in R^* \) and every \( \mu \in R_\beta \), we have \( \text{Ad}(h_{\alpha^\vee, \lambda})u_{\beta, \mu} = u_{\beta, \lambda^2 \mu} \).

For every possible \( \lambda \), we have:
\[ [[u_{\beta, 1}, u_{\alpha, 1}], u_{-\alpha, \lambda}] = [u_{\alpha + \beta, c_{\beta, \alpha}}u_{2\alpha + \beta, c_{\beta, \alpha}, 2}, u_{-\alpha, \lambda}]. \]
Using proposition 5.4, we see that the right-hand side is equal to:
\[ [u_{\alpha + \beta, c_{\beta, \alpha}}, [u_{2\alpha + \beta, c_{\beta, \alpha}, 2}, u_{-\alpha, \lambda}] = [u_{\alpha + \beta, c_{\beta, \alpha}}, u_{\alpha + \beta, c_{\beta, \alpha}, 2}, u_{-\alpha, \lambda}]. \]

It’s easy to see that the first commutator is trivial. We thus have:
\[ [[u_{\beta, 1}, u_{\alpha, 1}], u_{-\alpha, \lambda}] = u_{\alpha + \beta, c_{\beta, \alpha}, 2c_{\beta, \alpha}, -\alpha, \lambda}u_{\beta, c_{\beta, \alpha}, 2c_{\beta, \alpha}, -\alpha, 2\lambda^2 + c_{\beta, \alpha}c_{\alpha + \beta, -\alpha, \lambda}}. \]

On the other hand, we have:
\[ u_{\beta, 1}u_{\alpha, 1}u_{\beta, -1}u_{\alpha, -1}u_{-\alpha, \lambda} = u_{\beta, 1}u_{\alpha, 1}u_{\beta, -1}u_{-\alpha, \lambda}h_{\alpha^\vee, 1 - \lambda}u_{\alpha, 1 - \lambda}. \]

As in proposition 5.7 we see easily that we must have \( \text{Ad}(h_{\alpha^\vee, 1 - \lambda})u_{\beta, 1} = u_{\beta, -(1 - \lambda)^2} \).

We thus obtain:
\[ u_{\beta, 1}u_{\alpha, 1}u_{\beta, -1}u_{\alpha, -1}u_{-\alpha, \lambda} = u_{-\alpha, \lambda}u_{\beta, 1}u_{\alpha, 1}u_{\beta, -1}u_{-\alpha, \lambda}u_{b_{\beta, -(1 - \lambda)^2}u_{\alpha, 1 - \lambda}}. \]

hence:
\[ [[u_{\beta, 1}, u_{\alpha, 1}], u_{-\alpha, \lambda}] = u_{\beta, 2\lambda - \lambda^2}u_{\alpha + \beta, c_{\beta, \alpha}c_{\alpha + \beta, -\alpha, \lambda}}. \]
The first assertion follows immediately. The second is proved the same way as in proposition 5.7. \( \square \)

For the same reason as in the \( A_2 \) case, we have to prove the following result directly:
Proposition 5.14. We have:

\[ c_{\alpha,\beta} = c_{\beta,-\alpha-\beta} = \frac{1}{2} c_{-\alpha-\beta,\alpha}. \]

First we observe that if \( f_0(-\alpha - \beta) = 0 \), then all three of \( \alpha, \beta, -\alpha - \beta \) lie in \( \Psi \) and we are in a case in which we can simply apply the previous propositions to get the result. We will thus assume \( f_0(\alpha - \beta) = 1 \), and \( R_{-\alpha-\beta} \) will thus be assimilated to the maximal ideal of \( R \). In particular, for every \( \lambda \in R_{-\alpha-\beta} \), we have \( \lambda^h = 0 \), and every rational fraction of the form \( \frac{1}{1+\lambda P(\lambda)} \) is also a polynomial in \( \lambda \), since we have for every \( \lambda \):

\[ \frac{1}{1+\lambda P(\lambda)} = 1 - \lambda P(\lambda) + \cdots + (-1)^{h-1}\lambda^{h-1}P(\lambda)^h. \]

For every \( \lambda \), we have:

\[ [u_{\alpha,1}, u_{\beta,1}]u_{-\alpha-\beta,\lambda} = u_{\alpha,1}u_{\beta,1}u_{\alpha,\lambda}u_{-\alpha-\beta,\lambda} \]

\[ = u_{-\alpha-\beta,\lambda}h_{\alpha^\vee + \beta^\vee,1+c_{\alpha,\beta}}u_{\alpha,1}c_{\alpha,\beta,2u_{\alpha,-\alpha-\beta,2\alpha+\beta}c_{\alpha,\beta,2}\lambda u_{-\alpha-\beta,2\alpha+\beta,2\alpha,\beta,2\lambda^2}. \]

On the other hand, we have:

\[ [u_{\alpha,1}, u_{\beta,1}]u_{-\alpha-\beta,\lambda} = u_{\alpha,1}u_{\beta,1}u_{\alpha,-1\beta,-1u_{\alpha-\beta,\lambda}} \]

\[ = u_{-\alpha-\beta,\lambda}u_{-\beta,c_{\alpha,\beta,-\alpha-\beta}\lambda}u_{\alpha,1}u_{\alpha,c_{\alpha,\beta,-\alpha-\beta}\lambda}u_{\beta,1}u_{-\beta,-c_{\alpha,\beta,-\alpha-\beta}\lambda}u_{\alpha,1}u_{\alpha,-c_{\alpha,\beta,-\alpha-\beta}\lambda}u_{\beta,1}u', \]

where \( u' \) is a product of terms of the form \( u_{\gamma,\lambda^2P(\lambda)}, P(\lambda) \) being a polynomial in \( \lambda \). Moreover, it is easy to check that for every \( \delta, \mu \), \( [u', u_{\delta,\mu}] \) is also a product of terms of the same form; by a similar reasoning as in proposition 5.8, we are finally left with an expression of the form:

\[ [u_{\alpha,1}, u_{\beta,1}] \in \bigcup_{-\alpha-\beta}h_{\alpha^\vee,1+c_{\alpha,\beta}}h_{\beta^\vee,1+c_{\alpha,\beta}}u''\bigcup_{\alpha+\beta}, \]

with \( u'' \) being of the same form as \( u' \). Using the linear independence of \( \alpha^\vee \) and \( \beta^\vee \) and the fact that \( (\alpha + \beta)^\vee = \alpha^\vee + 2\beta^\vee \), the result follows immediately. \( \square \)

Corollary 5.15. We have:

\[ c_{\alpha,\beta} c_{\alpha,\beta} = -1, \]

\[ c_{\alpha,\alpha+\beta} c_{\alpha,\alpha-\beta} = -4, \]

As in the \( A_2 \) case, we deduce those equalities immediately from the previous three propositions. \( \square \)
5.4. The $G_2$ case. Assume now $\alpha$ and $\beta$ generate a subsystem of $\Phi$ of type $G_2$. The elements of $\Phi$ are then $\pm\alpha$ (short), $\pm\beta$ (long), $\pm(\alpha + \beta)$ (short), $\pm 3\alpha + \beta$ (long) et $\pm 3\alpha + 2\beta$ (long).

Remember that in the $G_2$ case, we're assuming the characteristic of $k$ is neither 2 nor 3.

**Proposition 5.16.** We have:
\[ c_{\alpha,\alpha+\beta,2,1} = \frac{1}{2} c_{\alpha,\alpha+\beta} c_{\alpha,2\alpha+\beta}; \]
\[ c_{\alpha,\alpha+\beta,1,2} = \frac{1}{2} c_{\alpha,\alpha+\beta} c_{2\alpha+\beta,\alpha+\beta}. \]

According to proposition [5.3], we have:
\[ [u_{\alpha,1}, [u_{\alpha,1}, u_{\alpha+\beta,1}]] = [u_{\alpha,2}, u_{\alpha+\beta,1}] [u_{\alpha,1}, u_{\alpha+\beta,1}]^{-2}. \]
The left-hand side is equal to:
\[ [u_{\alpha,1}, u_{2\alpha+\beta, c_{\alpha,\alpha+\beta}} u_{3\alpha+\beta, c_{\alpha,\alpha+\beta,2,1}} u_{3\alpha+2\beta, c_{\alpha,\alpha+\beta,1,2}}] \]
\[ = [u_{\alpha,1}, u_{2\alpha+\beta, c_{\alpha,\alpha+\beta}}] = u_{3\alpha+\beta, c_{\alpha,\alpha+\beta}} c_{2\alpha+\beta}. \]
The right-hand side is equal to:
\[ u_{2\alpha+\beta,2 c_{\alpha,\alpha+\beta}} u_{3\alpha+\beta, 4 c_{\alpha,\alpha+\beta,2,1}} u_{3\alpha+2\beta, 2 c_{\alpha,\alpha+\beta,1,2}} (u_{2\alpha+\beta, c_{\alpha,\alpha+\beta}} u_{3\alpha+\beta, c_{\alpha,\alpha+\beta,2,1}} u_{3\alpha+2\beta, c_{\alpha,\alpha+\beta,1,2}})^{-2} \]
\[ = u_{3\alpha+\beta, 2 c_{\alpha,\alpha+\beta,2,1}}, \]
hence the first assertion. The second one is obtained symmetrically. □

**Proposition 5.17.** We have:
\[ c_{\alpha,\beta,2} = \frac{1}{2} c_{\alpha,\beta} c_{\alpha,2\alpha+\beta}; \]
\[ c_{\alpha,\beta,3} = \frac{1}{6} c_{\alpha,\beta} c_{\alpha,\alpha+\beta} c_{\alpha,2\alpha+\beta}; \]
\[ c_{\alpha,\beta,3,2} = \frac{1}{3} c_{\alpha+\beta, c_{\alpha,\alpha+\beta}} c_{\alpha+\beta,2\alpha+\beta}. \]

According to proposition [5.3], we have:
\[ u_{\alpha,1}, [u_{\alpha,1}, u_{\beta,1}] = [u_{\alpha,2}, u_{\beta,1}] [u_{\alpha,1}, u_{\beta,1}]^{-2}. \]
The left-hand side is equal to:
\[ u_{\alpha,1}, u_{\alpha+\beta, c_{\alpha,\beta}} u_{2\alpha+\beta, c_{\alpha,\beta,2}} u_{3\alpha+\beta, c_{\alpha,\alpha+\beta,3}} u_{3\alpha+2\beta, c_{\alpha,\alpha+\beta,3,2}} \]
\[ = [u_{\alpha,1}, u_{\alpha+\beta, c_{\alpha,\beta}}] u_{2\alpha+\beta, c_{\alpha,\beta,2}} \]
\[ = [u_{\alpha,1}, u_{2\alpha+\beta, c_{\alpha,\beta,2}}] \]
\[ = u_{2\alpha+\beta, c_{\alpha,\beta}} u_{3\alpha+\beta, c_{\alpha,\alpha+\beta,2,1}} + c_{\alpha,\beta} c_{\alpha,2\alpha+\beta} u_{3\alpha+2\beta, c_{\alpha,\alpha+\beta,1,2}} \]
The right-hand side is equal to:
\[ u_{\alpha+\beta,2 c_{\alpha,\beta}} u_{2\alpha+\beta, 4 c_{\alpha,\beta,2}} u_{3\alpha+\beta, 8 c_{\alpha,\beta,3}} u_{3\alpha+2\beta, 8 c_{\alpha,\beta,3,2}} \]
we have:

\[ *(u_{\alpha+\beta,c_{\alpha,\beta}}u_{2\alpha+\beta,c_{\alpha,\beta},2}u_{3\alpha+\beta,c_{\alpha,\beta},3}u_{3\alpha+2\beta,c_{\alpha,\beta},2})^{-2} \]

\[ = u_{2\alpha+\beta,2c_{\alpha,\beta}}u_{3\alpha+\beta,6c_{\alpha,\beta},3}u_{3\alpha+2\beta,6c_{\alpha,\beta},3,2}-5c_{\alpha+\beta,2a+\beta}c_{\alpha,\beta}c_{\alpha,\beta,2}, \]

from which we deduce:

\[ 2c_{\alpha,\beta,2} = c_{\alpha,\beta}c_{\alpha,\alpha}; \]

\[ 6c_{\alpha,\beta,3} = c_{\alpha,\beta}c_{\alpha,\alpha+\beta,2}1 + c_{\alpha,\beta,2}c_{\alpha,\alpha+\beta} \]

\[ = \frac{1}{2}(c_{\alpha,\beta}c_{\alpha,\alpha+\beta,2} + c_{\alpha,\beta}c_{\alpha,\alpha+\beta,2}c_{\alpha,\alpha+\beta}); \]

\[ 6c_{\alpha,\beta,3} - 5c_{\alpha+\beta,2\alpha+\beta}c_{\alpha,\beta}c_{\alpha,\beta,2} = c_{\alpha,\beta}c_{\alpha,\alpha+\beta,1,2}. \]

The proposition follows immediately. \( \square \)

**Proposition 5.18.** We have:

\[ c_{\beta,\alpha,2} = -c_{\alpha,\beta,2}; \]

\[ c_{\beta,\alpha,3} = -c_{\alpha,\beta,3}; \]

\[ c_{\beta,\alpha,2,3} = -c_{\alpha,\beta,3,2} - \frac{1}{2}c^{2}_{\alpha,\beta}c_{\alpha,\alpha+\beta,2} + c_{\alpha,\beta,2}c_{\alpha,\alpha+\beta,2}; \]

\[ = -\frac{1}{6}c^{2}_{\alpha,\beta}c_{\alpha,\alpha+\beta,2}\alpha+\beta. \]

We have:

\[ [u_{\beta,1}, u_{\alpha,1}] = u_{\alpha+\beta,c_{\beta,\alpha}}u_{2\alpha+\beta,c_{\beta,\alpha,2}}u_{3\alpha+\beta,c_{\beta,\alpha,3}}u_{3\alpha+2\beta,c_{\beta,\alpha,2},3}. \]

On the other hand, we have:

\[ [u_{\beta,1}, u_{\alpha,1}] = [u_{\alpha,1}, u_{\beta,1}]^{-1} \]

\[ = u_{3\alpha+2\beta,-c_{\alpha,\beta,2}}u_{3\alpha+\beta,-c_{\alpha,\beta,2}}u_{2\alpha+\beta,-c_{\alpha,\beta,2}}u_{\alpha+\beta,-c_{\alpha,\beta}}. \]

The first two assertions follow immediately. For the third one, we observe that we have:

\[ u_{2\alpha+\beta,-c_{\alpha,\beta,2}}u_{\alpha+\beta,-c_{\alpha,\beta}} = u_{\alpha+\beta,-c_{\alpha,\beta}}u_{2\alpha+\beta,-c_{\alpha,\beta,2}}u_{3\alpha+2\beta,-c_{\alpha,\beta,2}c_{\alpha,\beta}c_{\alpha,\beta,2}+\beta}. \]

We conclude using the previous proposition. \( \square \)

Next we observe that the long roots \( \pm \beta, \pm (3\alpha + \beta), \pm (3\alpha + 2\beta) \) form a root subsystem of type \( A_2 \) of \( \Phi \); The following result follows them immediately from the \( A_2 \) case:

**Proposition 5.19.** We have:

\[ c_{\beta,3\alpha+\beta} = c_{3\alpha+\beta,-3\alpha-2\beta} = c_{-3\alpha-2\beta,\beta}; \]

\[ c_{\beta,3\alpha+\beta}c_{3\alpha+2\beta,-3\alpha-\beta} = 1; \]

\[ c_{\beta,3\alpha+\beta}c_{-\beta,-3\alpha-\beta} = -1. \]

**Proposition 5.20.** We have:

\[ c_{\alpha,\beta}c_{\alpha+\beta,-\beta} = 1. \]

Moreover, for every \( \lambda \in R^* \) and every \( \mu \in R_\alpha \), we have \( Ad(h_{\beta,\lambda})u_{\alpha,\mu} = u_{\alpha,\lambda\mu} \).
For every possible \( \lambda \), we have:
\[
[u_{a,1}, u_{\beta,1}] u_{-\beta, \lambda} = u_{a+\beta, c_{a, \beta}} u_{2a+\beta, c_{a, \beta}, 2} u_{3a+\beta, c_{a, \beta}, 3} u_{3a+2\beta, c_{a, \beta}, 3, 2} u_{-\beta, \lambda}
\]
\[
= u_{a+\beta, c_{a, \beta}} u_{-\beta, \lambda} u_{2a+\beta, c_{a, \beta}, 2} u_{3a+\beta, c_{a, \beta}, 3} u_{3a+2\beta, c_{a, \beta}, 3, 2} u_{-\beta, \lambda} u_{a, c_{a, \beta} c_{a+\beta, -\beta} \lambda u'},
\]
where \( u' \in \mathbb{U}_{2a+\beta} \mathbb{U}_{3a+\beta} \mathbb{U}_{3a+2\beta} \). On the other hand, we have:
\[
[u_{a,1}, u_{\beta,1}] u_{-\beta, \lambda} = u_{a,1} u_{\beta,1} u_{a, -1} u_{\beta, -1} u_{-\beta, \lambda}
\]
\[
= u_{-\beta, \lambda} u_{a,1} h_{\beta,\lambda}^{\alpha} u_{a,1} u_{\beta,1} u_{a, -1} u_{\beta, -1} u_{-\beta, \lambda} u_{a, \frac{1}{\lambda^2}}.
\]
We finish the proof the same way as in proposition 5.17.  

**Proposition 5.21.** We have:
\[c_{\beta, a} c_{a+\beta, -\alpha} = 3;\]
Moreover, for every \( \lambda \in R^* \) and every \( \mu \in R_{\beta} \), we have \( \text{Ad}(h_{\alpha, \lambda}) u_{\beta, \mu} = u_{\beta, \lambda^3 u'} \).

For every possible \( \lambda \), we have:
\[
[u_{\beta,1}, u_{a,1}] u_{-\alpha, \lambda} = u_{a+\beta, -c_{a, \beta}} u_{2a+\beta, -c_{a, \beta}, 2} u_{3a+\beta, -c_{a, \beta}, 3} u_{3a+2\beta, c_{a, \beta}, 3, 2} u_{-\alpha, \lambda}
\]
\[
= u_{-\alpha, \lambda} u_{a+\beta, c_{a, \beta} c_{a+\beta, -\lambda} + c_{a, \beta} c_{a+\beta, -\alpha}^2 + c_{a, \beta} c_{\alpha+\beta, \beta} \lambda^3} \lambda^3 u',
\]
where \( u' \) is a product of elements of \( \mathbb{U}_{a+\beta} \), \( i, j > 0 \). On the other hand, we have:
\[
[u_{\beta,1}, u_{a,1}] u_{-\alpha, \lambda} = u_{\beta,1} u_{a,1} u_{-\beta,1} u_{-\alpha,1} u_{-\alpha, \lambda}
\]
\[
= u_{-\alpha, \lambda} u_{\beta,1} h_{\alpha,\lambda}^{\alpha} u_{a,1} u_{\beta,1} u_{a, -1} h_{\alpha,\lambda}^{\beta} u_{a, -1} u_{\lambda} u_{\lambda} u_{a, \frac{1}{\lambda^2}}.
\]
We finish the proof in a similar way as in proposition 5.13.  

**Proposition 5.22.** We have:
\[c_{a+\beta, a} c_{2a+\beta, -\alpha} = 4;\]
For every possible \( \lambda \), we have:
\[
[u_{a+\beta,1}, u_{a,1}] u_{-\alpha, \lambda} = u_{a+\beta, c_{a+\beta, a}} u_{3a+\beta, c_{a+\beta, a}, 2} u_{3a+2\beta, c_{a+\beta, a}, 2} u_{-\alpha, \lambda}
\]
\[
= u_{-\alpha, \lambda} u_{a+\beta, c_{a+\beta, a} c_{2a+\beta, -\lambda} + c_{a+\beta, a} c_{\alpha+\beta, \beta} \lambda^2} \lambda^2 u',
\]
where \( x \) is a polynomial in \( \lambda \) and \( u' \) is a product of elements of \( \mathbb{U}_{x} \) with \( \gamma \in \{ \beta, 2a + \beta, 3a + \beta, 3a + 2\beta \} \). On the other hand, we have:
\[
[u_{a+\beta,1}, u_{a,1}] u_{-\alpha, \lambda} = u_{a+\beta,1} u_{a,1} u_{a+\beta, -1} u_{a, -1} u_{-\alpha, \lambda}
\]
\[
= u_{-\alpha, \lambda} u_{a+\beta,1} h_{\alpha,\lambda}^{\alpha} u_{a,1} u_{a, -1} h_{\alpha,\lambda}^{\beta} u_{a, -1} u_{a, \frac{1}{\lambda^2}}.
\]
We finish the proof in a similar way as in proposition 5.13.

\[\square\]
where \( u' \) and \( u'' \) are elements of \( U_{2\alpha+\beta} U_{3\alpha+\beta} U_{3\alpha+2\beta}; \) we have used the previous proposition in the process. Applying it once again, we see that the term in \( u_{\alpha+\beta} \) that we finally obtain is \( u_{\alpha+\beta,x} \), with:

\[
x = 1 - \frac{3\lambda}{1 - \lambda} + \frac{3(1 + (\lambda - 1)^2)\lambda}{1 - \lambda}
= 1 + 3\lambda(1 - \lambda) = 4\lambda - 3\lambda^2
\]

Hence we have \( c_{\alpha+\beta,\alpha} c_{2\alpha+\beta,-\alpha} = 4 \) and the proposition is proved. \( \square \)

**Proposition 5.23.** We have:

\[
c_{\alpha,\beta} = c_{\beta,-\alpha-\beta} = \frac{1}{3} c_{-\alpha-\beta,\alpha};
\]

\[
c_{\alpha,\alpha+\beta} = c_{\alpha+\beta,-2\alpha-\beta} = c_{-2\alpha-\beta,\alpha}.
\]

The first assertion can be proved in a very similar way as the corresponding ones in the \( B_2 \) case. Details are left to the reader.

For the second one, we can apply proposition 5.5 to \( \alpha,\alpha+\beta, -3\alpha - \beta \) to obtain:

\[
c_{\alpha,\alpha+\beta} c_{-3\alpha-\beta,2\alpha+\beta} = c_{-3\alpha-\beta,\alpha} c_{-2\alpha+\beta,\alpha+\beta}.
\]

The first part of the second assertion then comes from the first one applied to \( \alpha \) and \(-3\alpha - \beta \). Similarly, applying proposition 5.5 to \( \alpha+\beta, \alpha, -3\alpha - 2\beta \), we obtain:

\[
c_{\alpha+\beta,\alpha} c_{-3\alpha-2\beta,2\alpha+\beta} = c_{-3\alpha-2\beta,\alpha+\beta} c_{-2\alpha+\beta,\alpha}.
\]

The second part of the assertion then comes from the first assertion applied to \( \alpha + \beta \) and \(-3\alpha - 2\beta \). \( \square \)

**Corollary 5.24.** We have:

\[
c_{\alpha,\beta} c_{-\alpha,-\beta} = -1;
\]

\[
c_{\alpha,\alpha+\beta} c_{-\alpha,-\alpha-\beta} = -4;
\]

\[
c_{\alpha,2\alpha+\beta} c_{-\alpha,-2\alpha-\beta} = -9.
\]

Using the previous propositions, we obtain:

\[
c_{\alpha,\beta} c_{-\alpha,-\beta} = -\frac{1}{3} c_{\beta,\alpha} c_{\alpha+\beta,-\alpha} = -1.
\]

The proof of the other two assertions is similar. \( \square \)

For practical use, we will now write some of the relations of the last three sections in a more condensed form:

**Proposition 5.25.** For every \( \alpha, \beta \in \Phi \) such that \( \alpha + \beta \) is a root, there exists an integer \( p_{\alpha,\beta} \) such that \( c_{\alpha,\beta} c_{-\alpha,-\beta} = -p_{\alpha,\beta}^2 \). Moreover, we have:

\[
\frac{c_{\alpha,\beta}}{p_{\alpha,\beta}} = \frac{c_{\beta,-\alpha-\beta}}{p_{\beta,-\alpha-\beta}} = \frac{c_{-\alpha-\beta,\alpha}}{p_{-\alpha-\beta,\alpha}}.
\]
The proposition is an immediate consequence of the corollaries 5.9, 5.15 and 5.24 for the first assertion and of propositions 5.8, 5.14 and 5.23 for the second assertion. □

It can be checked that, as in [4], \( p_{\alpha,\beta} \) is the smallest integer \( c \) such that \( \beta - c\alpha \) is not a root (or rather that we can choose \( p_{\alpha,\beta} \) to be such an integer, since the \( c_{\alpha,\beta} \) don’t necessary live in rings of characteristic zero), but we won’t use this fact in the sequel. We can still assume \( p_{\alpha,\beta} \in \{1, 2, 3\} \) for every \( \alpha, \beta \), and thus depends only on the relative position of \( \alpha \) and \( \beta \) since we have assumed \( p \neq 2 \).

5.5. The unicity result. Now we’ll prove that the \( c_{\alpha,\beta} \) correspond up to normalization (and up to the fact that some of them are elements of a quotient of \( R \) and not of \( R \) itself) to the Chevalley constants for reductive groups. The fact that those constants satisfy the previous propositions either is proved in [4] or can easily be deduced from the results of that paper; the converse follows immediately from the following unicity result. Note that since the \( c_{\alpha,\beta,i,j} \), \( i + j \geq 3 \), are entirely determined by the \( c_{\alpha,\beta} \) (propositions 5.10, 5.11, 5.16, 5.17 and 5.18), we don’t have to worry about them.

**Proposition 5.26.** Let \( (c'_{\alpha,\beta})_{\alpha,\beta} \) be another family of nonzero constants such that:

- for every \( \alpha, \beta \in \Phi \) such that \( \alpha + \beta \in \Phi \), \( c'_{\alpha,\beta} \) lives in the same ring as \( c_{\alpha,\beta} \);
- the \( c'_{\alpha,\beta} \) also satisfy all the propositions and corollaries we have proved about the \( c_{\alpha,\beta} \) in the previous four subsections.

There exists then a family of nonzero constants \( (N_\alpha)_{\alpha \in \Phi} \) satisfying the following ones:

- for every \( \alpha \in \Phi \), \( N_{-\alpha} = N^{-1}_\alpha \);
- for every \( \alpha, \beta \), \( c'_{\alpha,\beta} = \frac{N_\alpha N_\beta}{N_{\alpha+\beta}} c_{\alpha,\beta} \).

Consider the system of affine roots \( \Phi' = \phi \times \mathbb{Z} \); let \( B \) be any Borel subgroup of \( G \) containing \( T \) and let \( \Phi'_B \) be the subset of the elements \((\alpha, n)\) of \( \Phi' \) such that \( n \geq f_B(\alpha) \), where \( f_B \) is the concave function associated to \( B \); since \( f_B \) is concave, \( \Phi'_B \) is a closed subset of \( \Phi' \). Consider the partial order on \( \Phi'_B \) defined by \((\alpha, n) \leq (\beta, m) \) if there exists \((\gamma, l) \in \Phi'_B \) such that \( \beta = \alpha + \gamma \) and \( m = n + l \), and let \( \Delta' \) be the set of minimal elements for that order; the set \( \Delta_0 = \{\alpha | (\alpha, n) \in \Delta' \text{forsomen} \} \) is then an extended set of simple roots of \( \Phi \).

Let \( \Delta \) be any set of simple roots of \( \Phi \) contained in \( \Delta_0 \) and let \( \Phi^+ \) be the set of positive roots of \( \Phi \) generated by \( \Delta \); we’ll assume \( \Delta \) is contained in an extended set of simple roots \( \Delta' \) satisfying the same condition as in the proof of proposition 3.13. We’ll first prove the existence of constants \( N_\alpha, \alpha \in \Phi^+ \), such that the second condition is satisfied for every \( \alpha, \beta \in \Phi^+ \); for every \( \alpha, \beta \in \Phi \) such that \( \alpha + \beta \in \Phi \) and either \( \alpha \) or \( \beta \) (say \( \alpha \)) is not in \( \Psi \), the constant \( c_{\alpha,\beta} \) then lives in \( R_\alpha \). (If both \( \alpha \) and \( \beta \) belong to \( \Psi \), \( c_{\alpha,\beta} \) always lives in \( R \) anyway). For every \( \alpha \in \Phi^+ \), let \( h_\alpha \) be the height of \( \alpha \), that is the number of elements of \( \Delta \) \( \alpha \) is the
sum of. We’ll define the $N_\alpha$ by induction on $h_\alpha$. For every $\alpha \in \Delta$, let’s choose $N_\alpha$ arbitrarily. Now assume $\alpha$ is an element of $\Delta$ of height 2; there exists then an unique pair $\beta, \gamma$ of elements of $\Delta$ such that $\beta + \gamma = \alpha$, and we can set:

$$N_\alpha = \frac{c_{\beta,\gamma}N_\beta N_\gamma}{c'_{\beta,\gamma}}.$$  

(The order in which we take $\beta$ and $\gamma$ doesn’t matter.) Now assume $\alpha$ is of height $> 2$, let $\beta \in \Phi$ and $\gamma \in \Delta$ be such that $\alpha = \beta + \gamma$; if $\alpha \in \Psi$, we also assume $\gamma \in \Psi$ whenever possible. Let’s define $N_\alpha$ as above; if $\alpha$ belongs to $\Psi$ and $\beta$ and $\gamma$ don’t, we’ll choose $N_\alpha$ arbitrarily among the elements of $R$ whose image in $R_\beta$ is the right-hand side of the above equality. (This case only occurs when $N_{\alpha,\beta}$ is the smallest root in the connected component of $\Psi$ containing the maximal root of $\Phi$ relatively to $\Delta$.)

Let now $\beta', \gamma'$ be any two elements of $\Phi^+$ such that $\alpha = \beta' + \gamma'$; we will check that $c'_{\beta',\gamma'}$ satisfies the required condition. According to [1, proposition 19], switching $\beta'$ and $\gamma'$ if necessary, we can assume $\delta = \beta' - \gamma$ is a root (or 0, but in that last case there is nothing to prove). We then have $\beta = \delta + \gamma'$ and:

$$c'_{\beta',\gamma'} c'_{\delta,\gamma} = c'_{\beta,\gamma} c_{\delta,\gamma'},$$

from which we deduce, using the induction hypothesis:

$$c'_{\beta,\gamma} \frac{N_\delta N_\gamma}{N_\beta} c_{\delta,\gamma} = \frac{N_\gamma N_\delta N_\gamma}{N_\alpha} c_{\beta,\gamma} c_{\delta,\gamma},$$

hence:

$$c'_{\beta,\gamma} c_{\delta,\gamma} = \frac{N_\beta N_\gamma}{N_\alpha} c_{\beta,\gamma} c_{\delta,\gamma}.$$

The assertion then follows from proposition 5.5.

Now consider the case of negative roots. For any $\alpha \in -\Phi^+$, set $N_\alpha = N_{-\alpha}^{-1}$. Let $\alpha, \beta$ be both negative and such that $\alpha + \beta > 0$, hence $-\alpha - \beta < 0$; we then have, using the first assertion of proposition 5.25:

$$c'_{\alpha,\beta} = \frac{-p_{\alpha,\beta}}{c'_{-\alpha,-\beta}} = \frac{p_{\alpha,\beta} N_{-\alpha-\beta}}{N_{-\alpha} N_{-\beta} c_{-\alpha,-\beta}} = \frac{N_\alpha N_\beta}{N_{\alpha+\beta} c_{\alpha,\beta}},$$

as required.

Finally consider the case when $\alpha$ is positive and $\beta$ negative. Assume $\alpha + \beta > 0$, hence $-\alpha - \beta < 0$; we have, using the second assertion of proposition 5.25:

$$c'_{\alpha,\beta} = \frac{p_{\alpha,\beta}}{p_{\beta,-\alpha-\beta}} c'_{\beta,-\alpha-\beta} = \frac{N_\beta N_{-\alpha-\beta} p_{\alpha,\beta}}{N_{-\alpha} p_{\beta,-\alpha-\beta} c_{\beta,-\alpha-\beta}} = \frac{N_\alpha N_\beta}{N_{\alpha+\beta} c_{\alpha,\beta}}.$$
as required. The case when $\alpha + \beta < 0$ being similar, the proof is now complete.

\[\square\]

6. The main theorem

Now we come to the main result of the paper. Let $k$ be any perfect field of characteristic $p \neq 2$ (eventually zero), let $h$ be a positive integer and let $G$ be a connected group of parahoric type of depth $h$ defined over $k$. Let $\Phi$ be the absolute root system of $G$ relatively to some given maximal torus $T$ and let $G$ be its group of $k$-points; we'll assume that the relative root system $\Phi$ of $G$ is connected, and not of type $G_2$ when $p = 3$.

Let $S$ be a maximal $k$-split torus of $G$; we can assume $T$ contains $S$. Remember (see [7]) that a group of parahoric type is said to be quasi-split over $k$ if it satisfies the following equivalent conditions:

- the centralizer of $S$ is a Cartan subgroup of $G$;
- let $k'$ be a Galois extension of $k$ on which $G$ splits, and let $\Gamma = Gal(k'/K)$.
  There exists a $\Gamma$-stable set of positive roots in $\Phi$;
- with $\Gamma$ defined as above, there existe a $\Gamma$-stable pseudo-Borel subgroup of $G$ containing $T$.

We'll assume $G$ is quasi-split and satisfies the following condition: let $\Psi$ be the root system of its reductive part; then all the rings $R_\alpha$, $\alpha \in \Psi$ (resp. $R'_\alpha$, $\alpha \in \Phi$), associated to the root subgroups $U_\alpha$ of $G$ are isomorphic. Note that we don’t assume $\Phi$ to be irreducible.

**Theorem 6.1.** Assume $G$ is connected and satisfies the above conditions. There exists a nonarchimeean henselian local field $F$ whose residual field is $k$ and a connected reductive group $G'$ defined and quasisplit over $k$ such that $G$ is $k$-isomorphic to the quotient of a parahoric subgroup of $G'$ defined on $F$ by its $h$-th congruence subgroup.

First assume $G$ is split over $k$ (hence $\Phi = \Phi$, $\Psi = \Psi$ and for every $\alpha \in \Phi$, $R_\alpha = R'_\alpha$) and every element of $k$ admits two opposite square roots (which is in particular the case when $k$ is algebraically closed). Assume $\Psi \neq \emptyset$ (resp. $\Psi = \emptyset$; by proposition 3.4) there exists a henselian local field $F$ such that if $O$ is the integer ring of $F$ and $p$ is the maximal ideal of $O$, for some given $\alpha \in \Psi$ (resp. $\alpha \in \Phi$), the ring $R_\alpha$ is isomorphic to $O/p^h$ (resp. $O/p^{h-1}$). We deduce from the hypotheses that for every $\alpha \in \Psi$ (resp. for every $\alpha \in \Phi$), the ring $R_\alpha$ (resp. $R'_\alpha$) is isomorphic to $O/p^h$ (resp. $O/\mathfrak{m}frac{h}{p^{h-1}}$).

Let $(X, \Phi, X', \Phi')$ be the root datum of $G$. According to [9] theorem 10.1.1, there exists a connected reductive algebraic group $G$, defined and split over $F$, whose root datum is also $(X, \Phi, X', \Phi')$. Let $T$ be a $k$-split maximal torus of $G$, for every $\alpha \in \Phi = \Phi$ let $U_\alpha$ be the root subgroup associated to $\alpha$ and let $v = (v_\alpha)$ be a valuation (in the sense of [2]) on $T$ and the $U_\alpha$; since $G$ is $k$-split we can assume that the image of the group $T$ (resp. $U_\alpha$) of $F$-points of $T$ (resp.
$U_\alpha$ for any $\alpha$) by $v_\alpha$ is $\mathbb{Z} \cup \{\infty\}$. For every $\alpha$ and every $i \in \mathbb{Z}$, let $U_{\alpha,i}$ be the subgroup of $U_\alpha$ defined the usual way; according to [6, proposition 2.6], the group $K_\alpha$ generated by the parahoric subgroup $K_T$ of $T$ and the $U_{\alpha,f_0(\alpha)}$ is then a parahoric subgroup of $G$.

Let $K_T$ be the $h$-th congruence subgroup of $K$; we'll prove now that $G$ and $K/K_T$ are $k$-isomorphic. We already know that we have $k$-isomorphisms between $H$ and $K_T/K_T^h$ and between $U_\alpha$ and $U_{\alpha,f_0(\alpha)/U_{\alpha,h-f_0(-\alpha)}}$ for every $\alpha$; moreover, we see by the unicity result (proposition 5.26) that these isomorphisms can be chosen in such a way that the constants $c_{\alpha,\beta}$ are the images of the corresponding constants for $G$ in the quotient rings in which they live; it is not hard to check that it is compatible with the fact that they are defined over $k$.

Since the condition on $k$ implies in particular that $k$ is infinite, $G$ (resp. $K/K_T$) is Zariski-dense in $G$ (resp. $K/K_T$). We thus only have to find an isomorphism between $H$ and $K/K_T$.

Assume first $G$ is solvable. We can then write $G = H \prod_{\alpha \in \Phi} U_\alpha$, with the $\alpha$ being taken in some fixed (arbitrarily chosen) order. Moreover, $K$ is then an Iwahori subgroup of $G$, and its Iwahori decomposition yields a decomposition of $G$ which is similar to the above decomposition of $G$. Using those decompositions, the above isomorphisms then yield a bijection $\phi$ from $G$ to $G$, which is also an isomorphism of $k$-varieties; it thus only remains to prove is that $\phi$ preserves the multiplication. By an obvious induction we can see that it is enough to prove that $\phi(gg') = \phi(g)\phi(g')$ when $g$ is any element of $G$ and $g'$ belongs either to $H$ or to one of the $U_\alpha$.

First we'll assume that $g' \in H$. Since we then have $U_{\alpha,g'} = g'U_\alpha$ for every $\alpha$ it is enough to prove the assertion when $g \in U_\alpha$ for some $\alpha$. But since both $H$ and $K_T/K_T^h$ act on respectively $U_\alpha$ and its image by the same character $\alpha$, we have $\phi(g^{-1}gg') = \phi(g^{-1})\phi(g)\phi(g')$. On the other hand, it is immediate from the definition of $\phi$ that $\phi(g^{-1}gg') = \phi(g^{-1})\phi(gg')$, hence the desired assertion.

Now we'll assume that $g' \in U_\alpha$ for some $\alpha = \alpha_{g'}$. For every integer $i$, let $C_i$ be the normal subgroup of $R_u(G)$ defined inductively by $C_0 = R_u(G)$ and $C_i = [R_u(G), C_{i-1}]$ for every $i \geq 1$. Since $G$ is solvable, $R_u G$ is nilpotent, i.e. the groups $C_i$ are trivial for $i$ large enough. Moreover, since $H$ normalises $R_u(G)$, it also normalises all the $C_i$; such a group is then the product of some subgroup of $H$ and of groups of the form $U_{\alpha,j}$, which means that if $g = h \prod u_\alpha$ belongs to $C_i$, then do $h$ and all of the $u_\alpha$. For every $g \in G$, we'll denote by $c_g$ the largest integer $i$ such that $g \in C_i$; by convention $c_1 = +\infty$.

Of course, $\phi(gg') = \phi(g)\phi(g')$ holds if either $g$ or $g'$ is the identity. Moreover, let $\beta = \beta_g$ be the greatest root (for the order we have used in the definition of $\phi$) such that the component of $g$ in $U_\beta$ is nontrivial; when $g \in H$, we'll set $\beta = 0$ and consider that $0 < \alpha$ for every root $\alpha$. When $\beta \leq \alpha$, the fact that $\phi(gg') = \phi(g)\phi(g')$ is immediate from the definition of $\phi$. We'll prove the general case by descending induction on $i = \text{Sup}(c_g, c_{g'})$. 


Assume then either \( c_g = i \) or \( c_g' = i \), and write \( g = g_1 u_\beta \), where \( u_\beta \) is the component of \( g \) in \( U_\beta \); we will also assume \( \beta > \alpha \). We then have:

\[
\phi(g)\phi(g') = \phi(g_1)\phi(u_\beta)\phi(g')
\]

\[
= \phi(g_1)\phi(g')\phi(u_\beta)\phi([u_\beta^{-1}, g'^{-1}]).
\]

The fact that \( \phi(u_\beta)\phi(g') = \phi(g')\phi(u_\beta)\phi([u_\beta^{-1}, g'^{-1}]) \) comes from the rank 1 solvable case when \( \beta = -\alpha \) and from the commutator relations of the previous section when \( \alpha \) and \( \beta \) are linearly independent. Now if we assume that \( \phi(g_1)\phi(g') = \phi(g_1 g') \), we obtain:

\[
\phi(g)\phi(g') = \phi(g_1)\phi(u_\beta)\phi([u_\beta^{-1}, g'^{-1}]).
\]

Since all root subgroups in which \( g_1 g' \) has a nontrivial component are \( \leq \beta \), we have \( \phi(g_1 g')\phi(u_\beta) = \phi(g_1 g'u_\beta) \). Moreover, since either \( u_\beta \) or \( g' \) is in \( C_i \), \([u_\beta^{-1}, g'^{-1}] \) belongs to \( C_{i+1} \), and we can apply the induction hypothesis to see that \( \phi(g_1 g'u_\beta)\phi([u_\beta^{-1}, g'^{-1}]) = \phi(g_1 g'u_\beta [u_\beta^{-1}, g'^{-1}]) = \phi(gg') \), as desired.

We are thus reduced to prove the assertion for \( g_1 \) and \( g' \), where \( g_1 \) belongs to \( C_i \) whenever \( g \) does, and the largest root \( \beta_1 \) such that \( g_1 \) has a component in \( U_{\beta_1} \) is strictly smaller than \( \beta \). By an obvious induction, after a finite number of steps we reach a \( \beta \) smaller than \( \alpha \), which proves the assertion. Hence the theorem holds when \( G \) is solvable.

Now we'll assume \( G \) is not solvable. Although \( G \) doesn't admit an Iwahori decomposition anymore, the subset \( H \prod_{\alpha \in \Phi} U_\alpha \), which depends on the order on \( \Phi \) that we have chosen, is a Zariski-dense open subset of \( G \).

Assume that, for some arbitrary choice of a set of positive roots \( \Phi^+ \) in \( \Phi \), all negative roots are smaller than any positive root for that order; we then have \( H \prod_{\alpha \in \Phi} U_\alpha = U^- B \). Let \( \phi \) be the bijection between \( U^- B \) and the corresponding subset of \( K/K^h \) defined as in the solvable case. Since both \( U^- \) and \( B \) are solvable, \( \phi \) doesn't depend on the choice of the order as long as that order satisfies the required condition. Moreover, let \( B_0 = B U_1^- \) be the unique Borel subgroup of \( G \) containing \( B \); we know from the previous case that for every \( g, g' \in B_0 \), \( \phi(gg') = \phi(g)\phi(g') \). Now assume \( g = ub \) is any element of \( U^- B \), with \( g' \) still in \( B_0 \). We then have:

\[
\phi(g)\phi(g') = \phi(u)\phi(b)\phi(g') = \phi(u)\phi(bg').
\]

Since \( bg' \in B_0 \), we can write \( bg' = u'b' \), with \( u' \in U^- \) and \( b' \in B \). Since \( U^- \) is solvable, we obtain:

\[
\phi(u)\phi(u'b') = \phi(u)\phi(u')\phi(b') = \phi(uu')\phi(b') = \phi(uu'b') = \phi(gg').
\]

By a similar reasoning, we obtain that we also have \( \phi(gg') = \phi(g)\phi(g') \) when \( g \) is an element of the only Borel subgroup \( B_0^- \) of \( G \) containing \( H \) which is opposite to \( B \), and \( g' \) is any element of \( U^- B \).

Moreover, since \( \phi \) and \( \phi' \) coincide on \( H \) and on every \( U_\alpha \), they also coincide on every solvable subgroup of \( G \) containing \( H \). We'll prove now that they coincide in fact on a Zariski-dense open subset of \( G \).
Let $\alpha$ be a simple root of $\Phi$ relatively to $\Phi^+$, and set $\Phi^+_\alpha = \Phi^+ \cup \{-\alpha\} - \{\alpha\}$; this is also a set of positive roots of $\Phi$. We will assume that the order on $\Phi$ has been chosen in such a way that $\alpha$ (resp. $-\alpha$) is the smallest positive (resp. largest negative) root for that order. For every $g \in U^-B$, if we write $g = ug_\alpha u'$, with $g_\alpha \in \mathbb{G}_\alpha$ and $u$ (resp. $u'$) belonging to the product of the root subgroups associated to negative (resp. positive) roots distinct from $\pm\alpha$, we then have $\phi(g) = \phi(u)\phi(g_\alpha)\phi(u')$.

Now consider an order on $\phi$ satisfying similar properties with $\Phi^+$ replaced by $\Phi^+_\alpha$ and $\alpha$ and $-\alpha$ switched, and let $\phi_\alpha$ be the corresponding automorphism between an open dense subset of $G$ and the corresponding subset of $K/K^h$; if $g$ belongs to the domain of definition of $\phi_\alpha$, we also have $\phi_\alpha(g) = \phi_\alpha(u)\phi_\alpha(g_\alpha)\phi_\alpha(u')$. Hence we may assume that $g \in \mathbb{G}_\alpha$; but then, by either the solvable case or proposition 4.2 depending whether $\mathbb{G}_\alpha$ is solvable or not, both $\phi$ and $\phi_\alpha$ extend to an isomorphism between $\mathbb{G}_\alpha$ and the corresponding subgroup of $K/K^h$; on the other hand, they coincide on $H$, $U_\alpha$, and $U_{-\alpha}$, which generate $\mathbb{G}_\alpha$, hence they must coincide on the whole intersection of their domains of definition.

We can iterate the process, replacing positive roots of $\Psi$ by negative roots one at a time, and after a finite number of steps we reach a situation where $\Phi^+$ has been replaced by $-\Phi^+$; by an obvious induction, we obtain that $\phi$ and $\phi'$ coincide on a Zariski-dense open subset $S$ of $G$, which is the intersection of the domains of definition of all the similar maps that we have met in the process.

Let now $g = ub$, $g' = u'b'$ be two elements of $U^-B$ such that $bu \in S$. Then $gg' \in U^-B$ and we have:

$$
\phi(gg') = \phi(ubu'b') = \phi(u)\phi(bu')\phi(b')
= \phi(u)\phi'(bu')\phi(b')
= \phi(u)\phi'(b)\phi'(u')\phi(b')
= \phi(u)\phi(b)\phi(u')\phi(b') = \phi(g)\phi(g').
$$

We finally use proposition 4.1 to see that $\phi$ extends to an isomorphism between $G$ and $K/K^h$; the assertion of the theorem is now proved.

Assume now $k$ is any perfect field (up to the conditions on its characteristic), with $\mathbb{G}$ still split over $k$. According to the previous case, there exists a nonarchimedean local field $F_0$ whose residual field is $\overline{k}$ and a connected reductive group $G_0$ defined over $F_0$ such that $\mathbb{G}$ is isomorphic to the quotient of a parahoric subgroup $K_0$ of $G_0$ by its $h$-th congruence subgroup $K_0^h$, via an isomorphism $\phi$. Moreover, if $F$ is any henselian local field associated to the rings $R_\alpha$ by proposition 3.1, we can assume that $F_0$ is the maximal unramified extension of $F$. By eventually replacing $K_0$ by one of its conjugates, we can also assume it is $Gal(F_0/F)$-stable.

If $G_0$ is defined over $F$ and $\phi$ is defined over $k$, then $\phi(\mathbb{G})$ is simply the group of $k$-points of $K_0/K_0^h$ and there is nothing to prove. On the other hand, the isomorphism $\phi$ is defined by its restrictions to $H$, $U_\alpha$, and $U_{-\alpha}$, and all these groups
as well as their images are defined over \( k \); moreover, according to [9, chapter 17], by considering the extended root datum \( (X^*(\mathcal{T}), \Phi, X_*(\mathcal{T}), \Phi^\vee, \emptyset, \text{Id}) \) we can always choose \( G_0 \) in such a way that it is defined and split over \( F \), and in that case, any of its parahoric subgroups is conjugated to a \( \text{Gal}(F_0/F) \)-stable one, hence we can always assume that \( K \) satisfies that property. We can thus always construct \( \phi \) in such a way that it is defined over \( F \), which proves the assertion.

No we'll go to the general case. We can assume that \( \mathcal{T} \) contains a maximal \( k \)-split torus \( S \) of \( G \); moreover, let \( k_0 \) be a finite Galois extension of \( k \) such that \( \mathcal{T}_\mathbb{Q} \) splits over \( k \), and let \( F_0, G_0 \) and \( K_0 \) be defined as above with \( \overline{k} \) replaced by \( k_0 \). Set \( \Gamma = \text{Gal}(k_0/k); \Gamma \) is a finite group acting on the root datum \( (X^*(\mathcal{T}), \Phi, X_*(\mathcal{T}), \Phi^\vee) \).

Let \( \alpha \) be any element of \( \Phi \) and let \( \Gamma_\alpha \) be the subgroup of the elements of \( \Gamma \) which stabilize \( \alpha \); we can always choose the unit element \( u \) in \( R_\alpha \) in such a way that it belongs to the group of \( \Gamma_\alpha \)-fixed points of \( U_\alpha \), and choose the unit element of every \( U_{\gamma(\alpha)} \) to be \( \gamma(u) \). By making similar choices in \( K_0/K_0^h \), we obtain:

\[
\phi(\prod_{\gamma \in \Gamma} \gamma(u)) = \prod_{\gamma \in \Gamma} \gamma(\phi(u)).
\]

Let \( \Phi \) be the relative root system of \( G \), that is the root system of \( G \) relatively to the group of \( k \)-points \( S \) of \( \mathcal{T} \). Since \( G \) is quasi-split, the restriction to \( S \) of every \( \alpha \in \Phi \) is nontrivial, hence in \( \Phi \). Moreover, if \( \beta \) is a nonmultiplicative element of \( \Phi \), the elements of the relative root subgroup \( U_\beta \) of \( G \) are precisely the \( \prod_{\gamma \in \Gamma} \gamma(u) \), \( u \in U_\alpha \). Hence \( \phi \) sends \( U_\beta \) to the corresponding relative root subgroup of \( K/K_1 \).

Assume now \( \beta \) is multiplicative, and let \( \alpha \) be an element of \( \Phi \) whose restriction to \( S \) is \( \beta \). Then \( \Gamma_\alpha \) is a subgroup of \( \Gamma \) of index 2, hence normal in \( \Gamma \), and if \( \gamma \) is the nontrivial element of \( \Gamma/\Gamma_\alpha \), \( \alpha + \gamma(\alpha) \) is a \( \Gamma \)-stable element of \( \Phi \) and we have:

\[
u_{\alpha,1}u_{\gamma(\alpha)},1 = u_{\alpha+\gamma(\alpha),c_{\alpha,\gamma(\alpha)}}u_{\gamma(\alpha)},1u_{\alpha,1},
\]

with \( c_{\alpha,\gamma(\alpha)} \) being an element of the quadratic extension \( k' \) of \( k \) such that \( \text{Gal}(k'/k) = \Gamma/\Gamma_\alpha \). By applying \( \gamma \) on both sides and comparing the two equalities, we obtain:

\[
c_{\alpha,\gamma(\alpha)}\gamma(c_{\alpha,\gamma(\alpha)}) = 1.
\]

Since \( c_{\gamma(\alpha),\alpha} = -c_{\alpha,\gamma(\alpha)} \), we see that it simply means that \( c_{\alpha,\gamma(\alpha)} \in k \), hence \( u_{\alpha+\gamma(\alpha),c_{\alpha,\gamma(\alpha)}} \in \mathbb{G} \). On the other hand, we have for every \( x, y \in R_\alpha \):

\[
\gamma(u_{\alpha+\gamma(\alpha),,x}u_{\alpha,y}u_{\gamma(\alpha),\gamma(y)}) = u_{\alpha+\gamma(\alpha),,\gamma(x)-c_{\alpha,\gamma(\alpha)}y\gamma(y)}u_{\alpha,y}u_{\gamma(\alpha),\gamma(y)},
\]

and the elements of \( U_\beta \) are precisely the elements of that form such that \( \gamma(x) - x = c_{\alpha,\gamma(\alpha)}y\gamma(y) \). Since this is true for the corresponding subgroup of \( K/K^h \) as well, that subgroup must be the image of \( U_\beta \) by \( \phi \). Since \( G \) is generated by \( H \) and the \( U_\beta \) and since it is not hard to find an automorphism between \( H \) and the corresponding Cartan subgroup which is defined over \( k \), we see that with such choices \( \phi \) must be defined over \( k \) as well, which completes the proof of the theorem. \( \square \)
7. Some particular cases

In this section, we give a few examples of cases in which the result of the previous section always works, as well as an explicit example of a group of parahoric type which doesn’t satisfy the required conditions.

**Proposition 7.1.** Assume \( k \) is of characteristic 0. Then all the \( R_\alpha \), \( \alpha \in \Psi \) (resp. \( \alpha \not\in \Psi \)), are \( k \)-isomorphic.

According to [8, II, theorem 2], the only complete local field with discrete valuation admitting \( k \) as its residual field is \( k((X)) \). Since any henselian local subfield of \( k((X)) \) yields the same quotient rings as \( k((X)) \), there is only one possible choice for \( R_\alpha \) when \( \alpha \in \Psi \) (resp. when \( \alpha \not\in \Psi \)), and the result follows immediately. \( \square \)

**Proposition 7.2.** Assume \( \Phi \) and \( \Psi \) are irreducible or empty. Then all the \( R_\alpha \), \( \alpha \in \Psi \) (resp. \( \alpha \not\in \Psi \)), are \( k \)-isomorphic.

Let \( k' \) be a Galois extension of \( k \) over which \( G \) splits, and set \( \Gamma = Gal(k'/k) \); the fact that \( \Phi \) (resp. \( \Psi \)) is irreducible means that the action of \( \Gamma \) on the connected components of \( \Phi \) (resp. \( \Psi \)) is transitive, and since for every \( \alpha \in \Phi \) and every \( \gamma \in \Gamma \), \( R_{\gamma(\alpha)} = \gamma(R_\alpha) \) is canonically \( k \)-isomorphic to \( R_\alpha \), we only have to check that for some fixed irreducible component \( \Phi_1 \) of \( \Phi \), all the \( R_\alpha \), with \( \alpha \) being an element of \( \Phi_1 \) contained (resp. not contained) in \( \Psi \), are \( k \)-isomorphic. When \( \Phi_1 \) is not of type \( A_1 \), the result for the roots outside \( \Psi \) is an immediate consequence of corollary 3.14, and the \( A_1 \) case has been covered in the corresponding section.

For roots inside \( \Psi \) we can use a similar reasoning. \( \square \)

For every \( \alpha \in \Phi \), let \( R_\alpha' \) be the quotient of \( R_\alpha \) by its elements of valuation at least \( h - 1 \).

**Proposition 7.3.** Assume that \( \Phi \) is connected, \( h > 2 \) and that for some \( \alpha \in \Psi \), \( R_\alpha \) is absolutely unramified. Then for every \( \beta \in \Psi \), \( R_\alpha \) and \( R_\beta \) are \( k \)-isomorphic to each other.

Since \( R_\alpha \) is absolutely unramified, its characteristic is \( p^h \) for some prime \( p \), and we have \( v(p) = 1 \) in \( R_\alpha \). For any choice of the field \( F_\alpha \) admitting \( R_\alpha \) as a quotient of its unit ring, that field must be an absolutely unramified local field whose residual field is \( k \). According to [8, II, theorem 3], there exists only one such local complete field (up to isomorphism); let \( F \) be that field.

On the other hand, since \( h > 2 \), the image of \( p \) in \( R_\beta \) is nonzero; we deduce from this, the proposition 3.13 and the proof of the previous proposition that \( p \) is also of valuation 1 in \( R_\beta \), hence \( R_\beta \) is absolutely unramified. The fields \( F_\alpha \) and \( F_\beta \) associated to respectively \( R_\alpha \) and \( R_\beta \) by proposition 3.4 must then be henselian subfields of \( F \), hence \( R_\alpha \) and \( R_\beta \) are \( k \)-isomorphic too. \( \square \)

Note that it is not true when \( h = 2 \).

We can generalize that proposition to the case of tame ramification as follows:
Proposition 7.4. Assume that $\Phi$ is connected and that for some $\alpha \in \Psi$, $R_\alpha$ is absolutely tamely ramified of ramification index $e < h - 1$. Then for every $\beta \in \Psi$ (resp. $\beta \not\in \Psi$), $R_\beta$ is $k$-isomorphic to $R_\alpha$.

Since $R_\alpha$ is absolutely ramified of ramification index $e$, its characteristic is a power of some prime number $p$ and we have $v(p) = e$ in $R_\alpha$. Hence any field $F_\alpha$ associated to $R_\alpha$ by proposition 3.4 is also absolutely ramified of index $e$. Since the ramification is tame, $F_\alpha$ is of the form $F_{nr}[\sqrt{\varpi}]$, where $F_{nr}$ is a henselian subfield of the unique absolutely unramified local field with residue field $\mathbb{k}$ and $\varpi$ is some uniformizer of $F_{nr}$; moreover, $F_{nr}[\sqrt{\varpi}]$ only depends on the class of $\varpi \mod p^2$, where $p$ is the maximal ideal of the ring of integers of $F_{nr}$.

On the other hand, since $h - 1 > e$, $R_\alpha$ is also tamely ramified of index $e$, hence $R_\beta$ is too, and there exists an uniformizer $\varpi'$ of $F_{nr}$ which is an $e$-th power of some element of $F_\beta$ and which belongs to $\varpi + p^{ce\varpi(k-1)}$; since $h - 1 > e$, $F_\alpha$ and $F_\beta$ must be henselian subfields of the same complete local field, hence $R_\alpha$ and $R_\beta$ are $k$-isomorphic. □

Note that it is not true anymore when the ramification is wild.

In these two cases assuming $\mathbb{C}$ is of semisimple rank at least 2, the fact that $\mathbb{C}$ matches the conditions of theorem 6.1 is an immediate consequence of proposition 3.14.

Now we’ll give an example of (the group of $k$-points of) a group of parahoric type with $\Psi$ reducible that doesn’t satisfy the required conditions. Consider the fields $F_1 = \mathbb{Q}_3[\sqrt{3}]$ and $F_2 = \mathbb{Q}_3[\sqrt{6}]$. Both are totally ramified extensions of $\mathbb{Q}_3$ of ramification index 2, but they are nonisomorphic. For $i = 1, 2$, let $\mathcal{O}_i$ be the ring of integers of $F_i$, and $p_i$ its maximal ideal, and let $R_i$ be the ring $\mathcal{O}_i/p_i^3$; The $R_i$ are nonisomorphic, but the quotient rings $R_i' = \mathcal{O}_i/p_i^2$ are (via the map sending $\sqrt{3} \to \sqrt{6}$); by a slight abuse of notation we’ll set $R' = R'_1 = R'_2$. Moreover, the maximal ideals $I_i$ of the $R_i$ are isomorphic as $R'$-modules (via the map sending $\sqrt{3} \to \sqrt{6}$ and 3 to 6); by a similar abuse of notation we’ll also set $I = I_1 = I_2$.

Let $\mathbb{G}$ be the set of matrices of the form: \[
\begin{pmatrix}
A & B \\
C & D
\end{pmatrix},
\] with $A \in GL_n(R_1)$, $B \in M_n(R')$, $C \in M_n(I)$ and $D \in GL_n(R_2)$. By the remarks above the usual matrix multiplication is well-defined, and it is easy to check that it defines a group law on $\mathbb{G}$. Since these maps are obviously algebraic, $\mathbb{G}$ is the group of $\mathbb{F}_3$-points of a split algebraic group $\mathbb{G}$ defined on $\mathbb{F}_3$; checking that $\mathbb{G}$ is of parahoric type, with $\Phi$ of type $A_{2n-1}$ and $\Psi$ of type $A_{n-1} \times A_{n-1}$, is also straightforward.

Let $\alpha$ (resp. $\beta$) be an element of the first (resp. second) irreducible component of $\Psi$. Then $R_\alpha$ is isomorphic to $R_1$ and $R_\beta$ is isomorphic to $R_2$. On the other hand, assume $\mathbb{G}$ is a quotient of a parahoric subgroup of a group $G(F)$ for some nonarchimedean local field $F$ of residual field $\mathbb{F}_3$; then all the $R_{\alpha}$, $\alpha \in \Psi$, must be isomorphic to $\mathcal{O}/p^3$, where $\mathcal{O}$ is the ring of integers of $F$ and $p$ its maximal ideal, hence a contradiction.
Note that in this particular case, the maximal unramified extensions of $F_1$ and $F_2$ are isomorphic; which means that if $\alpha$ and $\beta$ are two elements of $\Psi = \Psi$ not lying in the same connected component, $R_\alpha$ and $R_\beta$ are $\kappa$-isomorphic, but the isomorphism between them cannot be defined over $k$. Replacing our fields $F_1$ and $F_2$ by fields of wild absolute ramification, we can even find examples of groups of parahoric type in which the $R_\alpha$, $\alpha \in \Psi$, are not even $\overline{k}$-isomorphic.

REFERENCES

[1] N. Bourbaki. Groupes et algèbres de Lie, chapitre 6: Systèmes de racines. Hermann.
[2] F. Bruhat, J. Tits. Groupes réductifs sur un corps local. Publications Mathématiques de l’IHÉS, vol. 41 (1972), pp. 5-251 (I), et vol 60 (1984), pp. 5-184 (II).
[3] R.W. Carter. Finite groups of Lie type. John Wiley & Sons, 1985.
[4] C. Chevalley. Sur certains groupes simples. Tohoku Math. Journal, vol 7 (2), 1955, pp. 14-66.
[5] F. Courtès, Distributions invariantes sur les groupes réductifs quasi-déployés. Canadian Journal of Mathematics, volume 58 (2006), no 5, pp. 897-999.
[6] F. Courtès. On normal subgroups of parahorics, http://www.arxiv.org/pdf/math.GR/0502523
[7] F. Courtès. Steinberg representations for groups of parahoric types: the special case, to appear.
[8] J.P. Serre, Corps locaux. Hermann, 1968.
[9] T.A. Springer. Linear algebraic groups. Progress in Mathematics, Birkhäuser, vol 9, 2001 (2nd edition).

Université de Poitiers, Département de Mathématiques, UMR 7348 du CNRS, Téléport 2, Boulevard Marie et Pierre Curie, 86962 Futuroscope Chasseneuil Cedex

E-mail address: courtes@math.univ-poitiers.fr