CONSTRUCTING CHEVALLEY GROUPS

1. Generators and relations

In this section we shall describe a simple Lie algebra $\mathfrak{g}$ corresponding to an irreducible simply laced root system Φ. Fix Φ^+, a choice of positive roots, and

$$\Delta = \{\alpha_1, ..., \alpha_l\}$$

the set of simple roots. Let $\langle \alpha, \beta \rangle$ be the Killing form on the set of roots Φ, normalized so that $\langle \alpha, \alpha \rangle = 2$ for every root. The form allows us to identify roots with co-roots. Let P be the integer valued bilinear form on the root lattice defined by

$$P(\alpha_i, \alpha_j) = \begin{cases} 0 & \text{if } i < j \\ \frac{1}{2}\langle \alpha_i, \alpha_j \rangle & \text{if } i = j \\ \langle \alpha_i, \alpha_j \rangle & \text{if } i > j. \end{cases}$$

Let $c(\alpha, \beta) = (-1)^{P(\alpha,\beta)}$. Note that $c(\alpha, \beta)c(\beta, \alpha) = (-1)^{\langle \alpha,\beta \rangle}$. Let $\mathfrak{h}$ be the root lattice. Write h_α for α. Let $\mathfrak{g}$ be $\mathbb{Z}$ module spanned by $\mathfrak{h}$ and e_α, $\alpha \in \Phi$. We define a bracket as follows:

$$\begin{cases} [e_\alpha, -e_{-\alpha}] = h_\alpha \\ [h_\alpha, e_\beta] = \langle \alpha, \beta \rangle e_\beta \\ [e_\alpha, e_\beta] = \begin{cases} c(\alpha, \beta)e_{\alpha+\beta} & \text{if } \alpha + \beta \text{ is a root} \\ 0 & \text{otherwise.} \end{cases} \end{cases}$$

For example, in the case of SL_2, and in terms of the standard 2 dimensional representation, these generators are

$$e_\alpha = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, h_\alpha = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ and } e_{-\alpha} = \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix}.$$

Proposition 1.1. *$\mathfrak{g}$ is a Lie algebra.*

Proof. This is a case by case verification. We will prove the Jacobi identity in the following case, which has been omitted in Kac's book:

$$[e_\alpha, [e_\beta, e_\gamma]] + [e_\beta, [e_\gamma, e_\alpha]] + [e_\gamma, [e_\alpha, e_\beta]] = 0$$

when $\langle \alpha, \beta \rangle = \langle \beta, \gamma \rangle = -1$ and $\langle \alpha, \gamma \rangle = 0$. In this case the second term is trivial, and the Jacobi identity is equivalent to

$$c(\alpha, \beta + \gamma)c(\beta, \gamma) + c(\gamma, \alpha + \beta)c(\alpha, \beta) = 0.$$

Since $c(\alpha, \gamma) = c(\gamma, \alpha)$ and $c(\beta, \gamma) = -c(\gamma, \beta)$, the identity holds. $\square$

2. Simplicity of $\mathfrak{g}$

We can extend the form $\langle \cdot, \cdot \rangle$ from $\mathfrak{h}$ to $\mathfrak{g}$ by

$$\langle e_\alpha, -e_{-\beta} \rangle = \delta_{\alpha,\beta}.$$

Proposition 2.1. *Let k be a field. The Lie algebra $\mathfrak{g}$ is simple.*

Proof. Let $\mathfrak{i}$ be an ideal. Since $[\mathfrak{h}, \mathfrak{i}] \subseteq \mathfrak{i}$ it follows that the action of $\mathfrak{h}$ on $\mathfrak{i}$ can be diagonalized. Thus, there exists a root α such that $\mathfrak{g}_\alpha \subseteq \mathfrak{i}$.

Lemma 2.2. *If $\mathfrak{i}$ is an ideal and $\mathfrak{g}_\alpha \subseteq \mathfrak{i}$, then $\mathfrak{g}_{w(\alpha)} \subseteq \mathfrak{i}$ for every element w in the Weyl group.*

Proof. Obviously, it suffices to check this for $w = w_\beta$. If $w_\beta(\alpha) = \alpha$ there is nothing to prove. If $w_\beta(\alpha) = \alpha + \beta$ then

$$[e_\alpha, e_\beta] = \pm e_{\alpha+\beta}$$

If $s_\beta(\alpha) = -\alpha$ then

$$[e_{-\alpha}, [e_{-\alpha}, e_\alpha]] = 2e_{-\alpha}.$$

This part of the proof fails if the characteristic is 2. However, if the root system is not A_1, then there exists a root β such that $\alpha + \beta = \gamma$ is a root. Then

$$[e_{-\gamma}, [e_{-\alpha}, [e_\beta, e_\alpha]]] = \pm e_{-\alpha}$$

□

Since W acts transitively on Φ, it follows that $\mathfrak{g}_\alpha \subseteq \mathfrak{i}$ for every root. □

3. Representations of $\mathfrak{sl}(2)$

In this section we shall describe (without proofs for now) all irreducible representations of the Lie algebra $\mathfrak{sl}(2)$ over an algebraically closed field k of characteristic 0. It turns out that every irreducible representation can be realized on the space of homogeneous polynomials in two variables x and y. The action is given by

$$\begin{cases} e = y\frac{\partial}{\partial x} \\ f = x\frac{\partial}{\partial y}. \end{cases}$$

let V_n be the space of homogeneous of degree n. Its basis is given by $v_n = x^n$, $v_{n-2} = x^{n-1}y$, $\ldots$, $v_{-n} = y^n$. In terms of this basis the action takes form

$$\begin{cases} ev_i = ?v_{i-2} \\ fv_i = ?v_{i+2} \\ hv_i = v_i. \end{cases}$$

Moreover, every representation of $\mathfrak{sl}_2$ can be decomposed as a sum of irreducible representations. In particular, the element h can be diagonalized on every representation.

4. Irreducible representations of $\mathfrak{g}$

Let (π, V) be an irreducible representation. For every root α we have a copy of $\mathfrak{sl}_2$ spanned by $e_{-\alpha}, h_\alpha$ and e_α. By representation theory of $\mathfrak{sl}_2$, we know that h_α can be diagonalized. Since elements in $\mathfrak{h}$ commute, we can diagonalize all h_α simultaneously, which means that we can write

$$V = \oplus V_\lambda$$

where the sum is taken over all functionals λ of $\mathfrak{h}$ and $V_\lambda = \{v \in V \mid hv = \lambda(h)v\}$. By representation theory of $\mathfrak{sl}_2$ the eigenvalues of h_α must be integers. It follows that λ with $V_\lambda \neq 0$ must sit in the *weight* lattice

$$\Lambda_w = \{\lambda \in \mathfrak{h}^\times \mid \lambda(h_\alpha) \in \mathbb{Z}\}.$$

The weight lattice Λ_w clearly contains the root lattice Λ_r. In fact the index is given by

Φ	A_n	D_{2n}	D_{2n+1}	E_6	E_7	E_8
Λ_w/Λ_r	C_{n+1}	$C_2 \times C_2$	C_4	C_3	C_2	C_1

5. Maximal parabolic subalgebras

Every positive root can be written as a sum $\alpha = \sum_{i=0}^{l} m_i(\alpha)\alpha_i$ for some non-negative integers $m_i(\alpha)$. To every simple root α_i we can attach a subalegebra $\mathfrak{p} = \mathfrak{m} \oplus \mathfrak{n}$ such that

$$\begin{cases} \mathfrak{m} = \mathfrak{h} \oplus (\oplus_{m_i(\alpha)=0}\ \mathfrak{g}_\alpha) \\ \mathfrak{n} = \oplus_{m_i(\alpha)>0}\ \mathfrak{g}_\alpha. \end{cases}$$

Note that $\mathfrak{m}$ contains a semi-simple Lie algebra corresponding to the Dynkin diagram of $\Delta \setminus \{\alpha_i\}$, which we shall denote by $\mathfrak{g}_1$. Let β be the highest root, and $b = n_i(\alpha)$. For every j between 1 and b, define

$$\mathfrak{n}_j = \oplus_{m_i(\alpha)=j}\ \mathfrak{g}_\alpha.$$

The adjoint action of $\mathfrak{g}_1$ preserves every $\mathfrak{n}_j$. These representations are called inner-modules. Here is the list of dimensions of $\mathfrak{n}_1$ for various choices of $\mathfrak{g}$:

Φ	A_{n+1}	D_{n+1}	E_6	E_7	E_8	E_8
Φ_1	A_n	D_n	D_5	E_6	E_7	D_7
$dim(\mathfrak{n}_1)$	$n+1$	$2n$	16	27	56	64

Explanation: in the first two cases, the inner module is the so-called standard representations of $\mathfrak{sl}(n+1)$ and $\mathfrak{so}(2n)$. In other cases we spin-modules of D_5 and D_7 and two smallest non-trivial representations of E_6 and E_7 (notice that 27 is the dimension of the exceptional Jordan algebra).

6. Kostant's results

7. Chevalley groups

Let $\mathfrak{g}$ be a simple Lie algebra over $\mathbb{C}$. A representation of $\mathfrak{g}$ on a vector space V is a linear map

$$\pi : \mathfrak{g} \to End(V)$$

such that $\pi([x,y]) = [\pi(x), \pi(y)]$. The classification of finite-dimensional representations of $\mathfrak{g}$ is not an easy matter. The only canonical representation of $\mathfrak{g}$ is the adjoint representation

$$ad : \mathfrak{g} \to End(\mathfrak{g}).$$

given a representation V, we can consider e_α an element of the associative algebra $End(V)$. Define

$$\exp(te_\alpha) = \sum_{n=0}^{\infty} \frac{t^n e_\alpha^n}{n!}$$

where t is considered a formal variable.

Every irreducible representation V admits a lattice $V_{\mathbb{Z}}$ (a generalization of the Chevalley basis) invariant under $\mathfrak{g}_{\mathbb{Z}}$, and such that $\exp(te_\alpha)$ is a polynomial of finite degree with coefficients in $V_{\mathbb{Z}}$. Again, we shall not prove this fact, except for the adjoint representation and, therefore, for all inner modules:

Example: (Adjoint representation) Then $\exp(te_\alpha)$ is a polynomial of degree two with coefficients in $End(\mathfrak{g}_{\mathbb{Z}})$. To this end, notice that $[e_\alpha, [e_\alpha, e_\beta]] = 0$ unless $\beta = -\alpha$ in which case $[e_\alpha, [e_\alpha, e_{-\alpha}]] = 2e_\alpha$. It follows that $e_\alpha^3 = 0$, and $e_\alpha^2/2$ is integral. The claim follows.

Now, if k is a field, define $\mathfrak{g}_k = \mathfrak{g}_{\mathbb{Z}} \otimes k$ and $V_k = V_{\mathbb{Z}} \otimes k$. For every t in k, define $e_\alpha(t) = \exp(te_\alpha)$. Then $e_\alpha(t)$ is an element of $End(V_k)$. Note that

$$\begin{cases} e_\alpha(t)^{-1} = e_\alpha(-t) \\ e_\alpha(t)e_\alpha(u) = e_\alpha(tu) \end{cases}.$$

In particular, $e_\alpha(t)$ form a subgroup $E_\alpha \subseteq Aut(V_k)$ isomorphic to k.

Definition: The Chevalley group G is a subgroup of $Aut(V_k)$ generated by the one parameter subgroups E_α for all α in Φ. If V_k is the adjoint representation, then the group is denoted G_{ad}, and called the adjoint group.

Example: If $\mathfrak{g} = \mathfrak{sl}(n)$ and $V_{\mathbb{Z}} = \mathbb{Z}^n$, the standard representation, then $G(k) = SL_n(k)$.

8. Relations

Proposition 8.1. *Let $V_{\mathbb{Z}}$. Then the following holds in the ring $End(V_{\mathbb{Z}})[t]$*

$$\exp(te_\alpha)x\exp(-te_\alpha) = \exp(t \cdot ade_\alpha)(x).$$

Proof. Since we need to verify an equality of two polynomials, it suffices to check that the n-th derivatives of both sides coincide at $t = 0$, for every n. For example, the first derivatives, of the left and right hand sides, are $e_\alpha x - xe_\alpha$ and $ade_\alpha(x)$, respectively, at $t = 0$. For general n the derivative of the right hand side is $(ade_\alpha)^n(x)$, whereas of the left hand sides it is the same expression written in terms of associative algebra multiplication. We leave details to the reader. □

We record here some special cases of the above proposition. First of all, if α and β are two roots such that $\alpha + \beta \neq 0$, then If $\alpha + \beta \neq 0$, then the following hold in $End(V_k)$.

$$\begin{cases} e_\alpha(t)e_\beta e_\alpha(-t) = e_\beta + c(\alpha,\beta)te_{\alpha+\beta} \text{ if } \alpha+\beta \in \Phi \\ e_\alpha(t)e_\beta e_\alpha(-t) = e_\beta \text{ if } \alpha+\beta \notin \Phi \end{cases}$$

Finally, if $\beta+\alpha=0$, then

$$e_\alpha(t)e_{-\alpha}e_\alpha(-t)=e_{-\alpha}-th_\alpha+t^2e_\alpha.$$

Now notice that the corollary implies that $e_\alpha(t)\mapsto\exp(t\cdot ade_\alpha)$ gives a homomorphism from G to G_{ad}.

Corollary 8.2. *Let α and β be two roots such that $\alpha+\beta\neq 0$. If $\alpha+\beta$ is not a root, then $e_\alpha(t)$ and $e_\beta(u)$ commute. Otherwise, the group commutator is*

$$(e_\alpha(t),e_\beta(u))=e_{\alpha+\beta}(c(\alpha,\beta)tu).$$

Proof. The first case is clear, since e_α and e_β commute. To check second case, we shall use the previous proposition with $x=ue_\beta$. Then

$$e_\alpha(t)ue_\beta e_\alpha(-t)=ue_\beta+ctue_{\alpha+\beta}$$

The corollary follows by exponentiating both sides, and using $exp(ue_\beta+ctue_{\alpha+\beta})=e_\beta(u)e_{\alpha+\beta}(ctu)$. □

Corollary 8.3. *Let U be the group generated by all E_α with α positive. Let U_i be the subgroup of U generated by all E_α with α such that $ht(\alpha)\geq i$. Then*

- *U_i is a normal subgroup of U.*
- *$(U,U_i)\subseteq U_{i+1}$.*
- *U is nilpotent.*

We shall now derive some more precise results on the structure of U. Order positive roots so that $ht(\alpha)<ht(\beta)$ implies that $\alpha<\beta$. Now notice that any element u in U can be written as a product of $e_\alpha(t)$ in the just defined order. We claim that each such expression is unique. Since U maps onto U_{ad}, it suffices to check this claim for the adjoint group.

Proposition 8.4. *Let $\beta_1,\dots,\beta_m$ be all roots of height i. Then $\phi(t_1,\dots,t_m)=\prod_{k=1}^m e_{\beta_k}(t_k)$ defines an isomprhism between k^m and U_i/U_{i+1}.*

Proof. Since every element u_i in U_i can be written as a product $u_i=(\prod_{k=1}^m e_{\beta_k}(t_k))u_{i+1}$ for some u_{i+1} in U_{i+1}, the map ϕ is surjective. To prove injectivity, we proceed as follows. Let $\mathfrak{u}=\oplus_{\alpha\in\Phi}k\cdot e_\alpha$. We shall consider the adjoint action of U on $\mathfrak{g}$ modulo $\mathfrak{u}$. More precisely, let $y=\sum_{k=1}^m e_{-\beta_k}$. If α is a root such that $ht(\alpha)\geq i+1$, then $ht(\alpha-\beta_k)\geq 1$ and $Ade_\alpha(t)y-y\in\mathfrak{u}$. It follows that U_{i+1} acts trivially on y modulo $\mathfrak{u}$. Thus, to prove injectivity, it suffices to show that the map ϕ induces a one-to-one map from k^m to the U_i-orbit of y. To that end, note that $\beta_m-\beta_k$ cannot be a root since $ht(\beta_m-\beta_m)=0$. It follows that

$$\exp(t_m\cdot ade_{\beta_m})(y)\equiv y-t_mh_{\beta_m}\pmod{\mathfrak{u}}.$$

Furthermore, using $h_{\beta_1}=[e_{\beta_1},-e_{-\beta_1}]$, one can easily check that $\exp(t_2\cdot ade_{\beta_2})(h_{\beta_1})\equiv h_{\beta_1}$ (mod $\mathfrak{u}$). By induction on m, it follows that

$$\prod_{k=1}^m\exp(t_k\cdot ade_{\beta_k})(y)\equiv y-\sum_{k=1}^m t_kh_{\beta_k}\pmod{\mathfrak{u}}.$$

Since h_{β_k} are linearly independent, the map ϕ is one-to-one and $U_i/U_{i+1}\cong k^m$, as claimed. □

Example: Let $\mathfrak{g} = \mathfrak{sl}_3$, and pick positive roots in the standard fashion so that $\mathfrak{u}$ is the set of strictly upper-triangular matrices. If $i = 1$, then

$$y = \begin{pmatrix} 0 & 0 & 0 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix} \text{ and } u_1 = \begin{pmatrix} 1 & t_1 & * \\ 0 & 1 & t_2 \\ 0 & 0 & 1 \end{pmatrix}.$$

One easily checks that

$$u_1 y u_1^{-1} = \begin{pmatrix} -t_1 & * & * \\ -1 & t_1 - t_2 & * \\ 0 & -1 & t_2 \end{pmatrix} \equiv y - t_1 h_{\beta_1} - t_2 h_{\beta_2} \pmod{\mathfrak{u}}$$

where β_1 and β_2 are the two simple roots.

Corollary 8.5. *If k is a finite field of order q then $|U|$, the order of the group U, is equal to $q^{|\Phi^+|}$.*

9. Group H

Having defined the group U, our next task will be to define two more groups which, together with U will allow us to establish several structural results for G. For every root α define $w_\alpha(t) = e_\alpha(t)e_{-\alpha}(1/t)e_\alpha(t)$. (Note that $w_\alpha(t)^{-1} = w_\alpha(-t)$.) Define also $h_\alpha(t) = w_\alpha(t)w_\alpha(-1)$.

Example: $G = SL_2(k)$

$$w_\alpha(t) = \begin{pmatrix} 0 & -t \\ t^{-1} & 0 \end{pmatrix} \quad h_\alpha = \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}.$$

Proposition 9.1. *The following relations hold in $End(V)$: (here $\gamma = w_\alpha(\beta)$ and $c = c(\alpha, \beta)$)*

- $w_\alpha(t)e_\beta w_\alpha(t)^{-1} = ct^{\langle\alpha,\gamma\rangle}e_\gamma$
- $h_\alpha(t)e_\beta h(t)^{-1} = t^{\langle\alpha,\beta\rangle}e_\beta$.
- $w_\alpha(t)h_\beta w_\alpha(t)^{-1} = h_\gamma$
- $h_\alpha(t)h_\beta h_\alpha(t)^{-1} = h_\beta$.

Proof. Having calculated the action of $e_\alpha(t)$ on e_β (and thus on $h_\beta = [e_\beta, -e_{-\beta}]$), it is not too difficult to check the first statement. We leave details to the reader. The other three follow from the first. □

Corollary 9.2. *The action of $h_\alpha(t)$ is diagonal with respect to Chevalley's basis. Moreover, $h_\alpha(t) = h_{-\alpha}(t^{-1})$, $h_\alpha(s)h_\alpha(t) = h_\alpha$ and $h_\alpha(t)^{-1} = h_\alpha(t^{-1})$. If $\Phi \neq A_1$, then for every root α, elements $h_\alpha(t)$ form a group H_α isomorphic to $k^\times$.*

Proof. All but the last statement are evident. The last follows from the fact that there exists a root β such that $\langle\alpha, \beta\rangle = 1$. Then $h_\alpha(t)e_\beta h(\alpha)(t)^{-1} = te_\beta$, so $h_\alpha(t) \neq 1$ unless $t = 1$. □

Proposition 9.3. *Let H be the group generated by H_α for all roots α. Then H is commutative, it normalizes U and $H \cap U = \{1\}$.*

Proof. The first two statements are clear. Finally, elements in U are unipotent (all eigenvalues are 1), while elements of H are semi-simple. thus $H \cap U$ is trivial as claimed. □

Proposition 9.4. *(Case G_{ad}.) The group H is generated by H_{α_i}, where $\alpha_1, \ldots, \alpha_n$ are (all) simple roots. If we abbreviate $h_i(t) = h_{\alpha_i}(t)$, then $h_1(t_1) \cdot \ldots \cdot h_n(t_n) = 1$ if and only if*

$$\prod_{i=1}^{n} (t_i^{\langle \alpha_i, \beta \rangle}) = 1$$

for every root β. (Therefore for every β in the root lattice!)

The proposition implies that $H = (H_1 \times \ldots \times H_n)/Z$ where Z is the subgroup of $h_1(t_1) \cdot \ldots \cdot h_n(t_n)$ satisfying the above relation for every β in the root lattice. It is not too difficult to determine Z, as we will see in the following example.

Example: $\Phi = A_2$. Let α_1 and α_2 be two simple roots. If we take $\beta = 2\alpha_1 + \alpha_2$ or $\alpha_1 + 2\alpha_2$ then we get $t_1^3 = 1$ and $t_2^3 = 1$, respectively. Finally, if we take $\beta = \alpha_1 + \alpha_2$, then the equation becomes $t_1 t_2 = 1$. Therefore $Z = \mu_3$.

Exercise: Show that Z is given by the following table:

Φ	A_n	D_{2n}	D_{2n+1}	E_6	E_7	E_8
Z	μ_{n+1}	$\mu_2 \times \mu_2$	μ_4	μ_3	μ_2	1

10. Miniscule representations

The group SL_n, as well as some other, classical, groups is familiar to most mathematicians in large part due to the fact that it admits the standard n-dimensional representation.On the other hand, despite the fact that the rank of E_8 is just 8, the 248 dimensional adjoint representation is the smallest representation of this group. Thus, to "write down" E_8, one needs 248×248 matrices at best. In this section we shall describe so-called miniscule representation, some of which are considered the "standard" representations of the Lie algebra $\mathfrak{g}$.

Recall that every positive root can be written as a sum $\alpha = \sum_{i=0}^{l} m_i(\alpha)\alpha_i$ for some non-negative integers $m_i(\alpha)$. Let β be the highest root.

Proposition 10.1. *Let V be an irreducible representation of $\mathfrak{g}$ with the highest weight λ. The following are equivalent:*

(i) *W acts transitively on all weights of V_λ.*
(ii) *$e_\alpha^2 = 0$ for every α.*
(iii) *λ is fundamental for α_i such that $m_i(\beta) = 1$*

Proof. (i) implies (ii). We need to show that $\langle \alpha, \mu \rangle = -1, 0$ or 1. By replacing α by $-\alpha$ if necessary, we can assume that the dot product is non-negative. If it is positive, then $\mu - \alpha$ is a weight. However, if W acts transitively on all weights, then they all have the same lengths. But

$$\langle \mu - \alpha, \mu - \alpha \rangle = \langle \mu, \mu \rangle - 2\langle \alpha, \mu \rangle + 2,$$

which is equal to $\langle \mu, \mu \rangle$ if and only if $\langle \alpha, \mu \rangle = 1$.

(ii) implies (iii). Write $\lambda = n_1\lambda_1 + \ldots + n_r\lambda_r$ where λ_i are the fundamental weights and n_i some non-negative integers. Then

$$\langle \beta, \lambda \rangle = m_1(\beta)n_1 + \ldots + m_r(\beta)n_r.$$

Since $e_\beta^2 = 0$ we must have $\langle \beta, \lambda \rangle \leq 1$. This is possible only if λ is a fundamental weight for a simple root α_i such that $m_i(\beta) = 1$.

(iii) implies (i). Albeit stupid, this can be made a straightforward check, as the possible fundamental weights λ_i are easily tabulated. □

We now list all possible miniscule representations. Here Δ is the set of simple roots and Δ_1 is the subset of Δ obtained by deleting a simple root α_i such that $m_i(\beta) = 1$.

Δ	A_n	D_n	D_n	E_6	E_7
Δ_1	$A_{n-k} \times A_{k-1}$	D_{n-1}	A_{n-1}	D_5	E_6
$dim(V)$	(n/k)	$2n$	2^{n-1}	27	56

Explanation: In the case A_n, the miniscule representation V is the k-th exterior power of the standard representations of $\mathfrak{sl}(n+1)$. In the case D_n, we have first the standard $2n$-dimensional representation of $\mathfrak{so}(2n)$ and then one of the two spin representations. Finally, the algebra of type E_6 acts on a 27 dimensional exceptional Jordan algebra.

The structure of H for (some) miniscule representations is given by

Δ	A_n	D_n	D_{2m}	D_{2m+1}	E_6	E_7
Z	1	μ_2	μ_2	1	1	1

11. Bruhat-Tits decomposition

Let N be the group generated by $w_\alpha(t)$ for all α and $t \in k^\times$.

Proposition 11.1. *The group H is a normal subgroup of N, and $w_\alpha(t) \mapsto w_\alpha$ induces an isomorphism of N/H and the Weyl group W.*

Proof. Conjugation of $\mathfrak{h}$ by elements of N induces a homomorphism from N to W. Since H is in the kernel of the homomorphism, we have a natural homomorphism $\phi : N/H \to W$, such that $\varphi(w_\alpha(t)) = w_\alpha$. Clearly, this map is surjective. To show that ϕ is injective, it suffices to show that there exists a map $\varphi' : W \to N/H$ such that $\varphi' \circ \varphi$ is identity map on N/H. To that end, we shall describe N/H in terms of generators and relations. Since $w_\alpha(t) = h_\alpha(t) w_\alpha(1)$, the projection of $w_\alpha(t)$ in N/H does not depend on t and it will be denoted by $\hat{w}_\alpha$. Clearly, N/H is generated by $\hat{w}_\alpha$. Since $w_\alpha(-1)w_\alpha(-1) = h_\alpha(-1)$, it follows that

$$\hat{w}_\alpha^2 = 1.$$

Furthermore, using $w_\beta = e_\beta(1)e_{-\beta}(1)e_\beta(1)$ and Proposition ?, it is easy to check that

$$\hat{w}_\alpha \hat{w}_\beta \hat{w}_\alpha^{-1} = \hat{w}_\gamma.$$

where $\gamma = s_\alpha(\beta)$. On the other hand, as an abstract group, W is generated by w_α modulo relations $w_\alpha^2 = 1$ and $w_\alpha w_\beta w_\alpha^{-1} = w_\gamma$ where $\gamma = w_\alpha(\beta)$. It follows that $\varphi'(w_\alpha) = \hat{w}_\alpha$ is a well defined map which satisfies the required properties. □

As a consequence, BwB makes a perfect sense as a subset of G, for every $w \in W$.

Proposition 11.2. *(Bruhat's Lemma) Let $w \in W$, and α a simple root. Then*

$$BwBw_\alpha B = \begin{cases} Bww_\alpha B \text{ if } w(\alpha) \in \Phi^+ \\ BwB \cup Bww_\alpha B \text{ if } w(\alpha) \in \Phi^- \end{cases}$$

Proof. The proof of this proposition is surprisingly simple. First of all, since $w_\alpha E_\beta w_\alpha^{-1} \subseteq U$, for every positive root β different from α. It follows that

$$BwBw_\alpha B = BwE_\alpha w_\alpha B = \cup_{t\in k} Bwe_\alpha(t)w_\alpha B.$$

If $w(\alpha)$ is positive, then $we_\alpha(t)w^{-1} \in B$, and the first case follows. Otherwise, if $w(\alpha)$ is negative then we have two cases. If $t = 0$, then the coset is contained in $Bww_\alpha B$. If $t \neq 0$, then

$$Bwe_\alpha(t)w_\alpha B = Bwe_{-\alpha}(1/t)e_\alpha(t)e_{-\alpha}(1/t)w_\alpha B = Bww_{-\alpha}(1/t)w_\alpha B = BwB.$$

□

Theorem 11.3. *(Bruhat-Tits decomposition)*

(i) $G = \cup_{w\in W} BwB$.
(ii) $BwB = Bw'B$ *implies that* $w = w'$.

Proof. (i) Let $X = \cup_{w\in W} BwB$. Then $X^{-1} = X$, and $X \cdot X \subseteq X$, by the Bruhat's lemma. It follows that X is a subgroup. Since X contains generators of G, we must have $X = G$ as claimed.

(ii) Is proved by induction on $N(w)$. If $N(w) = 0$, then $w = 1$, and we have to check $w' = 1$, as well. Clearly, it suffices to show that w' is not in B if $w' \neq 1$. To that end, let n be the number of positive roots, and consider $\wedge^n \mathfrak{g}$. Let L be the line in $\wedge^n \mathfrak{g}$ spanned by $e_\alpha \wedge \ldots$ where the product is taken over all e_α with α positive. Since $w'(\Phi^+) \neq \Phi^+$, we must have $w'(L) \neq L$. On the other hand $B \cdot L = L$. This completes the proof if $N(w) = 0$. Otherwise, pick a simple root α such that $w(\alpha) < 0$. then $N(ww_\alpha) = N(w) - 1$, as α is not in $\Phi^+(ww_\alpha)$. Since $ww_\alpha \in Bw'Bw_\alpha B \subseteq Bw'w_\alpha B \cup Bw'B = Bw'w_\alpha B \cup BwB$. It follows that $Bww_\alpha B = Bw'w_\alpha B$ or BwB. Using the induction assumption, we must have $ww_\alpha = w'w_\alpha$ or $ww_\alpha = w$. Since the second inequality is impossible, we must have $w = w'$ as desired. □

Let $\bar{U}$ be the subgroup of G generated by $e_\alpha(t)$ for all α negative. Then $\bar{U} \cap B = \{1\}$. Further, for every w define

$$\begin{cases} U_w = \prod_{\alpha\in\Phi^+(w)} E_\alpha \\ U^w = \prod_{\alpha\in\Phi\setminus\Phi^+(w)} E_\alpha \end{cases}$$

Since $\Phi^+(w)$ and $\Phi \setminus \Phi^+(w)$ are closed under the addition, our main relation (?) implies that both U_w and U^w are subgroups of U, and clearly, $U = U^w U_w$ as a product of sets. Moreover, $wU^w w^{-1} \subseteq U$. Thus

$$BwU = BwU_w.$$

W claim that every element in BwU can be written uniquely as a product bwu with u in U_w. Indeed, if $bwu = b'wu'$ then $(b')^{-1}b = wu'uw^{-1}$. Since $wU_w w^{-1} \subseteq \bar{U}$, the claim follows.

Corollary 11.4. *Let k be a finite field with q elements. Let n be the number of the positive roots, and r the rank of $\mathfrak{g}$. Then*

$$|G_{ad}| \cdot |Z| = q^n(q-1)^r(\sum_{w\in W} q^{\ell(w)}).$$

12. Parabolic subgroup

We derive here some consequences of Bruhat's Lemma. If I is a subset of Δ let W_I be the subgroup of W generated by simple reflections corresponding to simple roots in I. Put

$$P_I = \cup_{w \in W_I} BwB$$

Bruhat's Lemma implies that the set P_I is closed under multiplication. Since, clearly, it is closed under inverse, P_I is a subgroup, called parabolic subgroup. More importantly, we have the following converse.

Proposition 12.1. *If P is a subgroup of G containing B then $P = P_I$ for some $I \subseteq \Delta$.*

Proof. Clearly, P must be a union of BwB for a collection of w. If we write $w = w_1 \dots w_k$ be a shortest expression for w in terms of simple reflections. To prove the claim, we must show that all $w_1, \dots, w_k$ are in P.

Lemma 12.2. *We above notation: $BwBw^{-1}B \supseteq Bw_1B$.*

Proof. By induction on $\ell(w) = k$. If $\ell(w) = 1$ then this is a special case of Bruhat's lemma. Otherwise, write $w = w'w_k$. Since $BwB = Bw'Bw_kB$,

$$G \supseteq BwBw^{-1}B = Bw'Bw_kBw_k^{-1}B(w')^{-1}B \supseteq Bw'B(w')^{-1}B,$$

and the lemma follows by induction. □

The lemma implies that w_1 is in P. The same argument implies that w_2 is in P and so on. The proposition is proved. □

Corollary 12.3. *The normalizer of B in G is B.*

13. Simplicity of G_{ad}

Theorem 13.1. *G_{ad} is simple group.*

Proof.

Lemma 13.2. *A normal subgroup K of G_{ad} cannot be contained in B.*

Proof. Let w_0 be in W such that $w_0(\Phi^+) = \Phi^-$. Then $w_0Bw_0^{-1} = \bar{B} = H\bar{U}$. Thus, since K is normal, it has to be contained in $B \cap \bar{B} = H$. Let h be an element in $K \subseteq H$. If $h \neq 1$ then there exists a root α such that $h(e_\alpha) = te_\alpha$ with $t \neq 1$. Then $e_\alpha(u)he_\alpha(-u) = e_\alpha(u(1-t))h$ which is not in H. Thus there are no normal subgroups contained in H, and therefore in B. □

Lemma 13.3. *If K is a non-trivial normal subgroup of G then $G = KB$.*

Proof. We already know that K cannot be contained in B, so $KB = P_I$ for some non-empty subset I of Δ. Let α be in I and β in $\Delta \setminus I$ such that $\langle \alpha, \beta \rangle = -1$. Then $w_\alpha b = k$ for some $k \in K$ and $b \in B$. Thus, on one hand, $w_\beta k w_\beta^{-1}$ is in K and, on the other hand,

$$w_\beta k w_\beta^{-1} = w_\beta w_\alpha b w_\beta^{-1} \in Bw_\beta Bw_\alpha Bw_\beta B = Bw_\beta w_\alpha w_\beta B.$$

It follows that $K \cap Bw_\beta w_\alpha w_\beta B \neq \{\}$. A contradiction. □

We can now finish the proof easily. Since $G = KB$, the second isomorphism theorem implies that $G/K \cong B/(B \cap K)$. But G is perfect, and B is solvable. Thus $G/K = \{1\}$. □

14. Outer Automorphisms of $\mathfrak{g}$ and non-simply laced groups

15. Algebraic groups

Now assume that G is simply connected. This means that $H = H_1 \times \ldots \times H_r$. Then G is an affine algebraic group. We shall now describe the ring A of regular functions on G. Using the Bruhat decomposition $G = \bar{U}WB$ - see the discussion preceding Corollary 7.4 - every double coset $X_w = \bar{U}wB$ can be identified with

$$X_w = k^{n-\ell(w)} \times (k^\times)^r \times k^n.$$

In particular, $X = \bar{U}B$ is naturally an affine variety with the ring of regular functions

$$k[x_\alpha, t_i, t_i^{-1}, y_\alpha].$$

where x_α and y_α are the coordinates of $U = k^n$ and $\bar{U} = k^n$, respectively. Thus, to determine A, it suffice to check which regular functions on X to all X_w. In fact, it suffices to restrict to X_w of co-dimension one. These are X_{w_α} where α is a simple root. To do so, consider the open set $w_\alpha \cdot X$. Then

$$w_\alpha X \setminus X = X_{w_\alpha}$$

so to see whether a regular function on X extends to X_{w_α} we need to restrict it to the open set $w_\alpha \cdot X \cap X$, and then see whether it extends to $w_\alpha \cdot X$.

Homework: Let's do this for SL_2. Then X consists of matrices $g = e_{-\alpha}(y)h_\alpha(t)e_\alpha(x)$, that is,

$$g = \begin{pmatrix} 1 & 0 \\ -y & 1 \end{pmatrix} \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

On the other hand, elements of $w_\alpha X$ are of the form $g' = w_\alpha e_{-\alpha}(y')h_\alpha(t')e_\alpha(x')$. Of course,

$$w_\alpha = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

You need to find a transformation $m(x', t', y') = (x, t, y)$ (birational map) such that $g' = g$. Then you can easily determine the ring A. Indeed, a function f in $k[x, t, t^{-1}, y]$ extends to a regular function on SL_2 if and only if $f \circ m$ is in $k[x', t', (t')^{-1}, y']$.

16. Steinberg group

In this section we shall describe the simply-connected G in terms of generators and relations. Let G' be the abstract group generated by $e_\alpha(t)$ modulo relations

$$e'_\alpha(t)e'_\alpha(u) = e'_\alpha(t+u) \tag{A}$$

and

$$(e'_\alpha(t), e'_\beta(u)) = e'_{\alpha+\beta}(c(\alpha,\beta)tu) \tag{B}$$

Clearly, we have a canonical map $\pi : G' \to G$. Moroever, the elements $e'_\alpha(t)$ form a one-parameter subgroup in G' which we shall also denoted by E'_α. Let U' be the subgroup of G' generated by E'_α for all positive roots α. Using the relation (B), any element in U' can be written as a product of elements in E'_α in any fixed ordering of positive roots. It follows that π gives an isomorphism between U' and U. Next, define elements $w'_\alpha(t)$ and $h'_\alpha(t)$ as before.

Proposition 16.1. *The following relations hold in G'. Notice that they are the same as the relations in G. Put $\gamma = w'_\alpha(\beta)$ and $c = c(\alpha, \beta)$.*

- $w'_\alpha(t)e'_\beta(u)w'_\alpha(t)^{-1} = e'_\gamma(ct^{\langle\alpha,\gamma\rangle}u)$
- $h'_\alpha(t)e'_\beta(u)h'_\alpha(t)^{-1} = e'_\beta(t^{\langle\alpha,\beta\rangle}u)$.

Proof. If α and β are perpendicular, then there is nothing to prove. So assume that $w_\alpha(\beta) = \alpha+\beta$, and let $\Sigma = \{\beta, \alpha+\beta\}$. Let U'_Σ be the group generated by E'_β and $E'_{\alpha+\beta}$. Let G'_α be the subgroup of G' generated by E'_α and $E'_{-\alpha}$. Notice that the proposed relations are in U'_Σ since it is normalized by G'_α. But U'_Σ is isomorphic to U_Σ, so we are done. The case $w_\alpha(\beta) = \beta - \alpha$ is, of course, proved the same. It remains to check the case $\beta = \pm\alpha$. To do so, we can find two roots β and γ such that $\alpha = \beta + \gamma$ and the use the previous cases to check the statement. □

Corollary 16.2. *Put $\gamma = w_\alpha(\beta)$ and $c = c(\alpha, \beta)$.*

- $w'_\alpha(t)w'_\beta(u)w'_\alpha(t)^{-1} = w'_\gamma(ct^{\langle\alpha,\gamma\rangle}u)$
- $w'_\alpha(t)h'_\beta(u)w'_\alpha(t)^{-1} = h'_\gamma(ct^{\langle\alpha,\gamma\rangle}u)h'_\gamma(ct^{\langle\alpha,\gamma\rangle})^{-1}$
- $h'_\alpha(t)w'_\beta(u)h'_\alpha(t)^{-1} = w'_\beta(t^{\langle\alpha,\beta\rangle}u)$
- $h'_\alpha(t)h'_\beta(u)h'_\alpha(t)^{-1} = h'_\beta(t^{\langle\alpha,\beta\rangle}u)h'_\beta(t^{\langle\alpha,\beta\rangle})^{-1}$

Proof. The first two are straightforward. We shall check the last using $h'_\alpha(t) = w'_\alpha(t)w'_\alpha(-1)$. Put $\epsilon = (-1)^{\langle\alpha,\beta\rangle}$ $c' = (\alpha, \gamma)$. Notice that $\epsilon cc' = 1$. Using (ii) twice,

$$= w'_\alpha(t)h'_\gamma(\epsilon cu)h'_\gamma(\epsilon c)^{-1}w'_\alpha(t)^{-1} = h'_\beta(t^{\langle\alpha\beta\rangle}u)h'_\beta(c't^{\langle\alpha,\beta\rangle})^{-1}[h'_\beta(t^{\langle\alpha,\beta\rangle})h'_\beta(c't^{\langle\alpha,\beta\rangle})]^{-1}$$

which reduces to $h'_\beta(t^{\langle\alpha\beta\rangle}u)h'_\beta(t^{\langle\alpha,\beta\rangle})$, as desired. Since □

Let H' be the subgroup of G' generated by and $h'_\alpha(t)$, and put $B' = H'U'$. The above relations imply that $N'/H' \cong N/H$, and that the Bruhat decomposition holds for G'. It follows that $\pi^{-1}(B) = B'$. In particular, the kernel Z' of the projection π is contained in B'. Since π is one-to-one on U' the kernel of π must be contained in H'.

The most important difference between G' and the Chevalley group G is that the relation $h'_\alpha(t)h'_\alpha(u) = h'_\alpha(tu)$ does not hold. For Chevalley groups this relations is checked directly on the defining representation. In general, this relation is not satisfied. Its obstruction is the Steinberg symbol which is defined by

$$(t, u) = h'_\alpha(t)h'_\alpha(u)h'_\alpha(tu)^{-1}.$$

Notice that the elements (s, t), on one had, are contained in the kernel Z' of the projection of G' on G. On the the other hand, (t, u) commute with $e'_\beta(t)$, so they lie in the center of G'. Our next goal is to show that Z' is generated by the elements (s, t), so G' is a *central extension* of G.

Proposition 16.3. *The symbol does not depend on α. In particular, we are free to drop the subscript α. The symbol (t, u) satisfies the following:*

- $(t, -t) = 1$
- $(st, u) = (s, u)(t, u)$
- $(t, u)(u, t) = 1$
- $(t, 1-t) = 1$

Proof. (i) $h_\alpha(t)h_\alpha(-t) = w_\alpha(t)w_\alpha(-1)w_\alpha(-t)w_\alpha(-1))$. Since $w_\alpha(-t) = w_\alpha(t)^{-1}$, it follows that $w_\alpha(t)w_\alpha(-1)w_\alpha(-t) = w_{-\alpha}(t^2) = w_\alpha(-t^2)$. Summarizing, $h_\alpha(t)h_\alpha(-t) = h_\alpha(-t^2)$, so $(t,-t) = 1$.

(ii) Let γ be a root such that $\langle \gamma, \alpha \rangle = 1$. Then the last relation of the previous corollary gives

$$h'_\gamma(t)h'_\alpha(u)h'_\gamma(t)^{-1} = h'_\alpha(ut)h'_\alpha(t)^{-1} = (u,t)^{-1}h'_\alpha(u)$$

We shall use this formula in two different was. First of all,

$$(s,u) = h'_\gamma(t)(s,u)h'_\gamma(t)^{-1} = [(s,t)_\alpha^{-1}h'_\beta(s)][(u,t)^{-1}h'_\alpha(u)][(su,t)^{-1}h'_\alpha(su)]^{-1},$$

which implies that $(su,t) = (s,t)(u,t)$.

(iii) The above formula can be used to calculate the commutator, $(h'_\gamma(t), h'_\alpha(u)) = (u,t)^{-1}$ and $(h'_\alpha(t), h'_\gamma(u)) = (t, u^{-1})$. Since the two commutators are inverses of each other, we get that $(t,u^{-1}) = (u,t)$, and $(t,u)(u,t) = 1$.

Next, switching the roles of α and γ, the commutator $(h_\gamma(t), h_\alpha(u)) = (u,t)^{-1}$ can be calculated in terms of the symbol corresponding to γ. A quick calculation shows that $(h_\gamma(t), h_\alpha(u)) = (u, t^{-1})'$, and the symbol does not depend on the root, as claimed.

(iv)

□

Corollary 16.4. *The following relations hold in H':*

- $h'_\alpha(t)h'_\alpha(u) = (t,u)h'_\alpha(tu)$
- $(h'_\alpha(t), h'_\beta(u)) = (t,u)^{\langle \alpha, \beta \rangle}$
- *If* $\alpha + \beta = \gamma$, *then* $h'_\alpha(t)h'_\beta(t) = h'_\gamma(t)(-c,t)$

It follows that the kernel Z' is generated by the Steinberg symbols. In particular, Z' is contained in the center of G'.

Proof. The first two have already been checked. Assume that $\alpha + \beta = \gamma$, and use the formulae?: $w'_\alpha(t)h'_\beta(t)w'_\alpha(t)^{-1} = h'_\gamma(ct^2)h'_\gamma(ct)^{-1}$ This is equivalent to $h'_\alpha(t)h'_\beta(t) = h'_\gamma(ct^2)h'_\gamma(ct)^{-1} = (ct, t^{-1})h_\gamma(t)$. This shows the third relation. Let Z'' be the subgroup of H' generated by all (u,t). The relations imply that $H'/Z'' \cong H$, so $Z' = Z''$. □

Theorem 16.5. *Let G be a simply connected Chevalley group corresponding to an irreducible simply laced root system Φ. As an abstract group, G is generated by elements $e_\alpha(t)$ satisfying the relations (A), (B) and*

$$(C) \qquad h_\alpha(t)h_\alpha(u) = h_\alpha(tu).$$

Proposition 16.6. *Let k be a finite field of odd order q. Then the Steinberg symbol is trivial. In particular, the relations (A) and (B) form a complete set of relations for G.*

Proof. We first claim that $(t,u) = 1$ when one of the variables, say u, is a square. Let v be a primitive root. Then $t = v^n$ and $u = v^{2m} = (-v)^{2m}$ for some integers n and m. Therefore $(s,t) = (v,-v)^{2nm} = 1$, which proves the claim. the number of squares in k is $(q+1)/2$. Since the squares do not form an additive subgroup, there exist two squares, a and b, such that $a + b = c$ is not a square. Put $t_1 = a/c$ and $u_1 = b/c$. Then $(t_1, u_1) = 1$ and both are non-squares. Since $t = t_1 r^2$ and $u = u_1 s^2$, we see that $(t,u) = 1$. □

17. Universal central extension

Definition: A central extension $\pi : G' \to G$ is called universal if for every central extension $\psi : G'' \to G$ there exists a unique map $\theta : G' \to G''$ such that $\psi\theta = \pi$.

Proposition 17.1. *Universal extension is unique.*

Proof. Let G'_1 and G'_2 be two universal central extensions. Then there exist $\theta_1 : G'_1 \to G'_2$ and $\theta_2 : G'_2 \to G'_1$ such that $\theta_1\pi_2 = \pi_1$ and $\theta_2\pi_1 = \pi_2$. It follows that $\theta_2\theta_1\pi_2 = \pi_2$ and $\theta_1\theta_2\pi_1 = \pi_1$. By the uniqueness of θ's in the definition above, we must have $\theta_2\theta_1 = id_{G_1}$ and $\theta_1\theta_2 = id_{G_2}$. The proposition is proved. □

Proposition 17.2. *If $\pi : G' \to G$ is a central extension such that for every central extension $\psi : G'' \to G$ there exists a homomorphism $\theta : G' \to G''$ such that $\theta\psi = \pi$ and $(G', G') = G'$, then G' is the universal central extension.*

Proof. We need to check uniqueness of θ. Assume that there there are two maps θ_1 and θ_2 such that that $\theta_1 \circ \psi = \pi$ and $\theta_2 \circ \psi = \pi$. Then for every x in G'

$$\theta_1(x) = \theta_2(x)\chi(x)$$

for some element $\chi(x)$ in the kernel of ψ. Since the G'' is a central extension of G, it is easy to check that χ defines a homomorphism from G' into a commutative group. But G' is perfect so χ must be trivial, as desired. □

Let G be a simply connected Chevalley group, and G' the Steinberg group discussed in the previous section. We shall now prove, with some mild restrictions on k, that G' is the universal central extension of G. By Proposition ?, we have to show that G' covers any central extension $\psi : G'' \to G$ of G. To do that, it suffices to construct elements $e''_\alpha(t)$ such that $\psi(e''_\alpha(t)) = e_\alpha(t)$ and such that they satisfy properties (A) and (B). The construction is based on the following:

Remark:
Let x and y be any two elements in G. Then
1) The commutator $(\psi^{-1}(x), \psi^{-1}(y))$ is a well defined element in G''.
2) If x'' is in $\psi^{-1}(x)$, then $x''\psi^{-1}(y)(x'')^{-1} = \psi^{-1}(xyx^{-1})$.

We shall apply this remark as follows. First of all, pick an element s in $k^\times$ such that $s^2 - 1 \neq 0$ and $s^2 - s + 1 \neq 0$. These two conditions can be fulfilled if $|k| > 4$. Put $d = 1 - s^2$. Since $(h_\alpha(s), e_\alpha(u)) = e_\alpha(du)$,

$$e''_\alpha(u) = (\psi^{-1}(h_\alpha(s)), \psi^{-1}(e_\alpha(u/d)))$$

is a well defined element in G''. We can now define $h''_\alpha(t)$ as usual.

Lemma 17.3. $h''_\alpha(t)e''_\beta(u)h''_\alpha(t)^{-1} = e''_\beta(t^{\langle\alpha,\beta\rangle}u)$

Proof. Using the definition of $e''_\beta(u)$, and the second Remark,

$$h''_\alpha(t)e''_\beta(u)h''_\alpha(t)^{-1} = (\psi^{-1}(h''_\beta(s)), \psi^{-1}(e''_\beta(t^{\langle\alpha,\beta\rangle}u/d))) = e''_\beta(t^{\langle\alpha,\beta\rangle}u)$$

□

Theorem 17.4. *Let G'' be a central extension of G. Then $e''_\alpha(u)$, the elements in G'' defined above, satisfy the axioms (A) and (B). In particular, $\varphi(e'_\alpha(u)) = e''_\alpha(u)$ deines a map $\varphi : G' \to G''$ such that $\psi \circ \varphi = \pi$.*

Proof. We shall first check the relation (B) if $\alpha+\beta \neq 0$ and $\alpha+\beta$ is not a root. To that end, notice that $(e''_\alpha(t), e''_\beta(u)) = f(t,u)$ where $f(t,u)$ is an element of the kernel of ψ. Writing this relation as

$$e''_\alpha(t)e''_\beta(u)e''_\alpha(t)^{-1} = f(t,u)e''_\beta(u)$$

it is easy to check that $f(t,u)f(v,u) = f(t+v,u)$, that is, $f(t,u)$ is additive the first variable. Of course, the same argument shows that $f(t,u)$ is additive in the second variable as well. We have now three possible cases:

(i) $\langle\alpha,\beta\rangle = 0$. Then, conjugating the above equality by $h''_\alpha(s)$, gives

$$e''_\alpha(s^2t)e''_\beta(u)e''_\alpha(s^2t)^{-1} = f(t,u)e_\beta(u).$$

It follows that $f(t,u) = f(s^2t,u)$ and $f((1-s^2)t,u) = 1$ for all t and u. Since $s^2-1 \neq 0$, it follows that $f(t,u) = 1$ for all t and u.

(ii) $\langle\alpha,\beta\rangle = 1$. Pick r in $k^\times$ such that $r^3-1 \neq 0$. This can be achieved if $|k| > 4$. Then a similar argument, conjugating this time by $h''_\alpha(r^2)h''_\beta(r^{-1})$, gives $f((1-r^3)t,u) = 1$ for all t and u, so $f(t,u) = 1$ as claimed.

(iii) $\alpha = \beta$. This is the most delicate case. Let γ be root such that $\langle\alpha,\gamma\rangle = 1$. Then conjugating by $h''_\gamma(s)$ gives $f(t,u) = f(st,su)$. Then

$$f((s-s^2)t,u) = f(t,u/(s-s^2)) = f(t,u/s)f(t,u/1-s) = f(st,u)f((1-s)t,u) = f(t,u).$$

It follows that $f((1-s+s^2)t,u) = 1$ for all t and u.

Next, we will show that the relation (A) holds. Let $d = s^2-1$, as before. Let $c = e''_\alpha(t/d)e''_\alpha(u/d)e''_\alpha((t+u)/d)^{-1}$. Then, after conjugating by $h''_\alpha(s)$ and using the already proved fact that $e''_\alpha(\cdot)$ commute with each other, it follows that $c = ce''_\alpha(t)e''_\alpha(u)e''_\alpha(t+u)^{-1}$, which proves (A)

Finally, we need to prove (B) in the case when $\alpha+\beta = \gamma$ is a root. As before, define $f(t,u)$ by

$$e''_\alpha(t)e''_\beta(u)e''_\alpha(t)^{-1} = f(t,u)e''_\beta(u)e''_\gamma(ctu)$$

where $\gamma = \alpha+\beta$. Conjugating both sides by $e''_\alpha(v)$, and using that $e''_\alpha(v)$ cummutes with $e''_{\alpha+\beta}(ctu)$, shows that $f(t+v,u) = f(t,u)f(v,u)$. Moreover, conjugating by $h''_\gamma(s)$ shows that $f(t,u) = f(st,su)$, which appears in case (iii) above. The theorem is proved. $\square$