The Big Book of Small Modules

Barbara Baumeister
Ulrich Meierfrankenfeld
Gernot Stroth

July 13, 2010

Notes for the authors

U: strong steinberg tensor product theorem

U: the weights of a module are really weights on Φ^*

U: Need to think about the notations (α, β) and $<\alpha, \beta>$. For example $<\alpha, \beta>$ currently also denotes the root system generated by α and β.

U: I added the GLS reference. According the Parker/Rowler, it contains a proof (Theorem 2.8.2) that the irreducible modules of the untwisted groups stay irreducible for the twisted group.

Contents

Chapter 1

Introduction

In this book we classify modules for finite groups fullfiling certain properties which forces the module to be "small" in some sense or annother. The main motivation for the book is provide the information about modules necessary in the local classification of finite groups of local characterisic p [LGCP].

Chapter 2

Some Group Theory

Lemma 2.0.1 [**three subgroup lemma**] *Let* A, B, C *be subroups of* G *with* $[A, B, C] + [B, C, A] = 1$. *Then* $[C, A, B] + 1$.

Proof:

Lemma 2.0.2 [**nilpotent groups**] *Let* M *be a nilpotent group and* A *a proper subgroup of* M. *Then* A *is a proper subgroup of* $\mathbb{N}_M(A)$ *and* $\langle A^M \rangle$ *is a proper subgroup of* M.

Chapter 3

Some elementary representation theory

Lemma 3.0.3 *Let G be a finite group and V an irreducible $\mathbb{K}G$-module. If $\operatorname{char}\mathbb{K} = p$, p a prime and $\Omega^p(G)$ acts homogenously on V, $\Omega^p(G)$ acts irreducible on V.*

Proof: **Comment: ref? any extra assumptions on $\mathbb{K}$?**

Chapter 4

Quadratic pairs in odd characteristic

The proof of the Glauberman-Thompson Theorem presented in

4.1 sec:glauberman thompson

is essentially due to Paul Flavell.

4.2 a,b and ab-quadratic

[**sec:ab quadtratic**]

Lemma 4.2.1 [**ab quadratic**] *Let G a group, R a ring, V a faithful RG-module and $a, b \in G$ such that a, b and ab are quadratic in V and $G = \langle a, b \rangle$. Then*

(a) [**z**] *If G is abelian, then G is quadratic on $2V$.*

(b) [**a**] *G is nilpotent of class at most two.*

(c) [**y**] $[V, G'] \leq 2[V, G, G]$.

(d) [**b**] $[V, G', G] = [V, G, G'] = 0$.

(e) [**c**] *$\langle h \rangle G'$ is quadratic for all $h \in G$.*

(f) [**d**] *$\alpha\beta = -\beta\alpha$ and $\gamma = 2\alpha\beta$, where $\alpha = a - 1, \beta = b - 1$ and $\gamma = [a, b] - 1$.*

(g) [**e**] *Put $C_\delta = \{v \in V \mid v\delta = 0\}$. Then $C_{2\beta} \leq V\alpha + C_{2\beta} \leq C_\gamma \leq V$ and $V\gamma \cong V\alpha + C_{2\beta}/C_{2\beta} \cong V/C_\gamma$ as R-modules.*

(h) [**f**] *Suppose that R is field, then $\dim_R[V, [a, b]] \leq \frac{1}{2}\min\{\dim_R[V, a], \dim_R[V, b]\}$.*

Proof: Let $\delta = ab-1$. Then $\delta = (\alpha+1)(\beta+1)-1 = \alpha\beta+\alpha+\beta$. Since $\alpha^2 = \beta^2 = \delta^2 = 0$ we conclude that

1° [**1**] $\alpha\beta\alpha\beta + \alpha\beta\alpha + \alpha\beta + \beta\alpha\beta + \beta\alpha = 0$

Suppose that G is abelian, then $\alpha\beta = \beta\alpha$ and so (1°) implies $2\alpha\beta = 0$. Thus (a) holds.

Multiplying (1°) with β from the right we have

2° [**2**] $\alpha\beta\alpha\beta + \beta\alpha\beta = 0$

Multiplying (2°) with α from the left we get

3° [**3**] $\alpha\beta\alpha\beta = 0.$

Substituting (3°) into (2°) we have

4° [**4**] $\beta\alpha\beta = 0$

Multiplying (1°) with α from the right and using (3°) we have

5° [**5**] $\alpha\beta\alpha = 0$

¿From (1°), (3°),(4°) and (5°) we get

6° [**6**] $\alpha\beta + \beta\alpha = 0$

Let $g = [a, b]$. Then $g-1 = (1-\alpha)(1-\beta)(1+\alpha)(1+\beta)-1 = \alpha\beta-\alpha\beta-\beta\alpha+\alpha\beta = 2\alpha\beta$ Thus (f) holds. (b),(c) and (d) are immediate consequences of (f). By (b) every element $h \in G$ can be written as $h = a^k b^l g^m$ with $\kappa, l, m \in \mathbb{Z}$. Thus

$$h - 1 = (1 + k\alpha)(1 + l\beta)(1 + 2m\alpha\beta) - 1 = k\alpha + l\beta + (kl + 2m)\alpha\beta$$

and so

$$(h-1)^2 = kl(\alpha\beta + \beta\alpha) = 0$$

Thus all elements in G are quadratic. Hence (e) follows from (d).
(g) follows from $\gamma = 2\alpha\beta$.
Suppose R is a field. Then by (g),

$$\dim V\beta = \dim V/C_\beta \geq \dim V/C_{2\beta} \geq \dim V\alpha + C_{2\beta}/C_{2\beta} + \dim V/C_\gamma = 2\dim V_\gamma$$

By symmetry in a and b we conclude that (g) holds. □

4.3 The Glauberman-Thompson Theorem

Let $\mathbb{F}$ be a field with $\operatorname{char}\mathbb{F} \neq 2$, G a group and V a faithfully and finitary $\mathbb{F}G$-module. ote here that we allow infinite fields and fields in characteristic 0. For $a \in G$ let $C_a = C_V(a)$, $V_a = V(a-1)$ and $d_a = \dim V_a$. Let $\mathcal{Q}$ be the set on non trivial quadratic elements in G, that is $\mathcal{Q} = \{1 \neq a \in G \mid V_a \leq C_a\}$. Put $d = \min_{a \in Q} d_a$ and $\mathcal{QR} = \{a \in Q \mid d_a = d\}$. The elements of $\mathcal{QR}$ are called roots. Fix two roots a and b and let $H = \langle a, b\rangle$. Put $\alpha = a - 1$, $b = \beta - 1$, $g = [a, b]$ and $\gamma = g - 1$. Then $V_a = V\alpha$ and $C_\alpha = \ker\alpha$. Suppose that H is niloptent, i.e that H acts unipotenly on V. In this section we prove the Glauberman-Thompson theorem which says that among other things H has class at most 2.

Lemma 4.3.1 [**class two**] *Suppose that H has class two. Then*

(a) [**a**] *g is a root.*

(b) [**b**] $V_a \cap V_b = 0$.

(c) [**c**] *$V_g = V\alpha\beta \oplus V\beta\alpha$ and $V\alpha\beta = V\beta \cap C_b = V\beta \cap V\gamma$.*

(d) [**d**] $V = C_a + C_b$.

(e) [**e**] *V is a direct sum of indecomposable $\mathbb{F}H$-submodules.*

(f) [**f**] *Let W be non-trivial indecomposable direct summand of the $\mathbb{F}H$-module V. Then there exists a basis for V such that the matrices for α and β are (in some order)*

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

(g) [**g**] *Let $1 \neq d \in H$. Then d is quadratic on V iff q is a root and iff $d \in \langle a^H\rangle \cup \langle b^H\rangle$. Moreover, both $\langle a^H\rangle$ and $\langle b^H\rangle$ act quadratically on V.*

Proof: Let $A = \langle a, a^b\rangle = \langle a, g\rangle$. Since H has class two, A is abelian and A is normal in H. Moreover, $a^{b^2} = ag^2 = a^{2b}a^{-1}$. Hence 4.2.1(b) implies that $\langle a^{2b}, a^{-1}\rangle$ is quadratic. Since $\operatorname{char}\mathbb{F} \neq 2$ and a is quadratic, we have $a^2 \neq 1$. Hence the minimality of $d_a = d$ implies $V_{a^2} = V_a$ and we conclude that A is quadratic. Then a centralizes V_g and by symmetry b centalizes V_g. Therefore

1° [**0**] $\quad Vg \leq C_V(H)$.

Note that

$$V\alpha + V\gamma = [V, A] = V\alpha + V\alpha^b = V\alpha + V\alpha\beta$$

In particular, $C_b \cap [V, A] = (V\alpha \cap C_b) + V\alpha\beta$ and so

$$V\gamma \leq (V\alpha \cap C_\beta) + V\alpha\beta$$

By definition of d, $\dim V\gamma \geq d$. On the otherhand $\dim(V\alpha \cap C_b) + \dim V\alpha\beta = \dim V\alpha = d$ and we conclude that

2° [**1**] $\quad V\gamma = (V\alpha \cap C_\beta) \oplus V\alpha\beta$ *and g is a root.*

In particular, $V\alpha\beta \leq V\gamma \leq C_V(H)$. By symmetry $V\beta\alpha \leq V\gamma \leq C_V(H)$. In particular, $V\alpha\beta + V\beta\alpha$ is an $\mathbb{F}H$-submodule in V and H acts quadtratically on $V/(V\alpha\beta + V\beta\alpha)$. Thus $V\gamma \leq V\alpha\beta + V\beta\alpha$. Since $V\beta\alpha \leq V\alpha \cap V\gamma \leq V\alpha \cap C_b$ we conclude from (2°) that

3° [**2**] $\quad V\gamma = V\beta\alpha \oplus V\alpha\beta \leq C_V(H)$ *and* $V\alpha \cap C_\beta = V\beta\alpha = V\alpha \cap V\gamma$

In particular, $V\alpha \cap V\beta = (V\alpha \cap C_b) \cap (V\beta \cap C_a) = V\beta\alpha \cap V\alpha\beta = 0$ and (a), (b) and (c) are proved. (d) follows from (b) applied to the dual module of V.

Let U_a be an $\mathbb{F}$-complement to $V\alpha + C_V(H)$ in C_a. Then $U_a \cap C_b \leq U_a \cap C_V(H) = 0$ and so $\dim U_a = \dim U_a\beta$. Let $u \in U_a$ with $u\beta\alpha = 0$. Then $u\beta \in V\beta \cap C_\alpha = V\alpha\beta$ and so $u\beta = v\alpha\beta$ for some $v \in V$. Hence $u - v\alpha \in C_b$ and $u \in (C_b + V\alpha) \cap C_\alpha = (C_\alpha \cap C_\beta) + V\alpha = V\alpha + C_V(H)$. Thus $u = 0$ and $U_a\beta \cap C_a = 0$. Also $U_a\beta \cap U_a\beta\alpha \leq U_a\beta \cap C_a = 0$. Furthermore, $U_a\beta + U_a\beta\alpha \cap C_a \leq (V\beta \cap C_\alpha) + V\alpha \leq C_V(H) + V\alpha$ and so $U_a \cap U_a b + U_a\alpha\beta = 0$. Put $W_a = U_a + U_a\beta + U_a\beta\alpha$. Then $W_a = U_a \oplus U_a\beta \oplus U_a\beta\alpha$ and $\dim U_a = \dim U_a\beta = \dim U_\alpha\beta$. Thus if $u_i, 1 \leq i \leq m$, is a basis for U_α, then $u_i, u_i\beta, u_i\beta\alpha, 1 \leq i \leq m$ is a basis for W_a. Since a centralizes U_a and $U_a\beta\alpha$ and b centralizes $U_a\beta$ and $U_a\beta\alpha$ we see that $\mathbb{F}\langle u_i, u_i\beta, u_i\beta\alpha$ is a 3-dimensional $\mathbb{F}H$-submodule on which α and β as in (f).

Similarly define U_b and W_b. Suppose that $W_a \cap W_b \neq 0$. Then also $W_\alpha \cap W_\beta \cap C_V(H) \neq 0$. But $W_a \cap C_V(H) = U_a\beta\alpha$ and $W_\beta \cap C_V(H) = U_b\alpha\beta$ and we obtain a contradiction to (b). Thus $W_a \cap W_b = 0$.

Put $\overline{V} = V/W_a + W_b + C_V(H)$. Since $V = C_a + C_b = U_a + U_b + V\alpha + V\beta + C_V(H) = W_a + W_b + C_V(H)$ we have $\overline{V} = [\overline{V}, H]$. Since H is nilpotent on $\overline{V}$, this implies $\overline{V} = 0$. Thus

$$V = W_a + W_b + C_V(H) = W_a \oplus W_b \oplus C$$

for some $C \leq C_V(H)$. Hence (e) holds and (f) follows from the above and the Krull-Schmidt Theorem. (g) follows easily from (f). □

Lemma 4.3.2 [**va cap vb**] *Suppose that $V\alpha \cap V\beta \neq 0$. Then H is abelian.*

Proof: Note that $V\alpha \cap V\beta \leq C_V(H)$ and so $V\alpha \cap V\beta \leq V\delta$ for all $\delta \in \alpha^H \cap \beta^H$. Hence by induction on the maximum of the subnormal lengths of a and b in H, both $\langle a^H \rangle$ and $\langle b^H \rangle$ are abelian. Thus H has class at most two and the lemma follows from 4.3.1(b).

Lemma 4.3.3 [**A abelian**] *H has class at most two.*

Proof: Since H is unipotent on V, there exists $v \in V$ with $[v, H, H] = 0$ and $[v, H] \neq 0$. Interchanging a and b if necessary we may assume that $v\alpha \neq 0$. Then $v\alpha \in V\alpha \cap C_V(H) \leq V\delta$ for all $\delta \in \alpha^H$. Thus by 4.3.2, $A := \langle a^H \rangle$ is abelian. By induction on the subnormal maximum of the subnormal lengths of a and b to H we may assume that $B := \langle b, b^a \rangle$ has class at most two. If B is abelian that $g \in Z(B) \cap A \leq Z(H)$ and we are done. So suppose that B has class two. Note that $H = AB$. Since A is abelian, $A \cap B$ is normal in A. Since A is normal in H, $A \cap B$ is normal in B and so $A \cap B \trianglelefteq H$. Since $g \in A \cap B$, $H/A \cap B$ is abelian. Hence $[A, B] \leq A \cap B$ and B is normal in H. By 4.3.1(g), B has exactly two maximal quadratic subgroups, namely $\langle b^B \rangle$ and $\langle b^{aB} \rangle$. Thus a^2 normalizes $\langle b^B \rangle$ and $b^{a^2} \in \langle b^B \rangle$. Since $[b, a, a] \in [A, A] = 1$ we conclude $b^{2a} = (b[b, a])^2 \in bb[b, a]^2 B' = bb^{a^2} B' \subseteq < b^B \rangle$. Thus $[B, b^{2a}, B] = 0$. By minimality of d, $[V, b^{2a}] = [V, b^a]$ and so $[V, b^a, B] = 0$. Since $B = B^{a^{-1}}$ we also have $[V, b, B] = 0$, $[V, B, B] = 0$ and B is abelian, a contradiction. $\square$

4.4 The $SL_2(q)$-Lemma

Let G be a finite group, $\mathbb{F}$ a field with positive characteristic $p \neq 2$, V a faithful, finite dimensional $\mathbb{F}G$-module and a, b quadratic elemennts. Put $H = \langle a, b \rangle$. In this section we show (with some exceptions for $p = 3$), that if a and b are roots than either H is p-group or $H \cong SL_2(q)$ for some power q of p. Put $\delta = \alpha\beta + \beta\alpha$.

Lemma 4.4.1 [**d commutes**] *$\delta h = h\delta$ for all $h \in H$.*

Proof: $\alpha\delta = \alpha\beta\alpha = \delta\alpha$.

Lemma 4.4.2 [**d as scalar**] *Suppose that d acts as the scalar ξ on V.*

(a) [**a**] *If $\xi = 0$, then H is nilpotent of class at most two and all elements in H act quadratically on V.*

(b) [**b**] *Suppose $\xi \neq 0$.*

  (a) [**a**] *V is the direct sum of isomorphic 2-dimensional simple $\mathbb{F}H$ submodules.*

  (b) [**b**] *For each simple $\mathbb{F}H$-submodule in V there exists a basis such that the matrices of α and β are*

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 \\ \xi & 0 \end{pmatrix}$$

  (c) [**c**] *$H \cong SL_2(\mathbb{F}_p[\xi])$ or $p = 3$, $|\xi| = 4$ and $H \cong SL_2(5)$.*

Proof: Suppose first that $\xi = 0$. Then $\alpha\beta = -\beta\alpha$ and so ab acts quadratic on V. Thus (a) follows from 4.2.1.

So suppose that $\xi \neq 0$. Then $V = \xi V = V\delta = V\alpha + V\beta = C_a + C_b$ and $C_a \cap C_b \leq C_V(H) \leq \ker\delta = 0$. Thus $V\alpha = C_a, V\beta = C_b$ and $V = C_b \oplus C_a$. In particular the $C_b \to C_a, v \to v\alpha$ is an isomorphism. Let $v \in C_\beta$. Then $v\alpha\beta = v(\delta - \beta\alpha) = \xi v$. Let $v_i, 1 \leq i \leq m$ be a basis for C_b. Then $v_i, v_i\alpha$ is a basis for V and we see (b:a) and (b:b) holds. (b:c) now follows from Dickson's Theorem (see [**?**]) □

For $\xi \in \mathbb{F}$ let V_ξ be the generalized ξ-eigenspace for δ on V. Note that by 4.4.1V_ξ is an H-submodule.

Lemma 4.4.3 [**v xi**] *Let $\xi \in \mathbb{F}^\sharp$ and suppose that $V = V_\xi$. Then $H/O_p(H) \cong SL_2(\mathbb{F}_p[\xi])$ respectively $SL_2(5)$ if $p = 3$ and $|\xi| = 4$.*

Proof: Note that $\epsilon := \delta - \xi$ act nilpotenly on V and δ acts as the scalar ξ in each $V\epsilon^n/V\epsilon^{n+1}$. Thus the lemma follows from 4.4.2.

Lemma 4.4.4 [**n central**] *Let $N/O_p(H) = Z(H/O_p(H)$ and put $Z = O^p(N)$. Then Z acts as a scalar± 1 on each V_ξ. Inparticular, $Z \leq Z(H)$, Z is an elementary abelian 2-group and $N = O_p(H) \times Z$.*

Proof: Note that N acts as a scalar on each composition factor of H on V. In particular, $N/O_p(H)$ is a p'-group and so $N = O_p(H)Z$. Let h be a p' element in N and $\xi \in \mathbb{F}$. If $\xi = 0$, then $O^p(H)$ and so also h centralize V_ξ. So suppose that $\xi \neq 0$. Since $[h, H]$ centralizes all the composition factors for H on V_ξ we conclude from 4.4.3 that h either centalizes all the composition factors or h inversts all the composition factors of H on V_ξ. Since h is a p' we conclude that h acts as ± 1 on V_ξ. To prove the remaing assertions we may assume that $\mathbb{F}$ is algebraicly closed. Then V is the direct sum of its eigenspaces and so $h^2 = 1$ and $[h, H] = 1$. □

Lemma 4.4.5 [**op central**] *Suppose that a is a root. Then $[O_p(H), O^p(H)] = 1$.*

Let W be a non-trivial simple submodule for H in V. The $W\alpha \neq 0$. Moreover, N normalizes $W\alpha$, $A := \langle a^N \rangle$ is a p-group and $[W\alpha \leq V\alpha^n$ for all $n \in N$. Thus by 4.3.2, A is abelian. Thus A act on N. Let X be a composition factor for H on $O_p(H)$. Then by 4.4.4, N acts trivially on X. On the otherhand by 4.4.3 H/N is a subdirect product of $L_2(q)$ for odd $q's$ and so H/N is p-stable. Thus a and so also $O^p(H)$ centralizes X. □

With ring we mean a ring with one. Let $M_n(R)$ be the ring of $n \times n$ matrices over the ring R.

Lemma 4.4.6 [**ideals**] *Let R and S be a rings, $\phi : R \to S$ an onto ringhomomorphism and $I = \ker\phi$. Then*

(a) [**a**] $\phi_1 : M_m(R) \to M_m(S), (a_{ij}) \mapsto (\phi(a_{ij})$ *is an onto ring homomorphism with* $\ker\phi_1 = M_n(I)$.

(b) [**b**] *$\phi_2 : GL_m(R) \to GL_m(S)$, $(a_{ij}) \mapsto (\phi(a_{ij})$ is an group homomorphism with $\ker \phi_1 = 1 + M_n(I)$.*

(c) [**c**] *Let $a, b \in GL_m(R)$. Then the following are equivalent: $ab^{-1} \in 1 + M_n(R)$, $a - b \in M_n(R)$ and $\phi_2(a) = \phi_2(b)$.*

Proof: Obvious. □

Lemma 4.4.7 [**direct sum of rings**] *Let R_1 and R_2 be commuative rings. Then $GL_n(R_1 \oplus R_2) \cong GL_n(R_1) \times GL_n(R_2)$ and $SL_n(R_1 \oplus R_2) \cong SL_n(R_1) \times SL_n(R_2)$.*

Proof: Obvious. □

Lemma 4.4.8 [**trace 0**] *Let k, l, m be postive integers, R a commutative ring with one, $\mathbb{F}$ a subfield of R and $\mu \in R$ with $R = \mathbb{F}[\mu]$ and $\mu^k = 0$ for some $k \in \mathbb{N}$. Let $M_m^\circ(R)$ be the ring of trace 0, $m \times m$ matrices over $\mathbb{F}$. Put*

$$I_l := \{1 + \mu^l b \mid b \in M_m^\circ(R)\}$$

Nonsense, thsi is not even a subgroup. Just use determined to describe the correct subgroup.

(a) [**a**] *I_l is a normal subgroup of $GL_m(R)$*

(b) [**b**] *$[1 + \mu^r a, 1 + \mu^s b] \in 1 + \mu^{r+s}(ba - ab)I_{r+s+1}$ for all $a, b \in M_m^\circ(R)$ and $r, s \in \mathbb{N}$.*

(c) [**c**] *$[I_r, I_s] = I_{r+s}$. In particular, $I_2 = I_1'$ and I_1 is nilpotent of class $k - 1$.*

(d) [**d**] *For all $1 \leq l \leq k$, I_l/I_{l+1} is isomorphic to $M_m \circ (\mathbb{F})$ as a module for $GL_m(\mathbb{F})$.*

(e) [**e**] *Let $a \in GL_m(\mathbb{F})$ and $i \in I_1$. Then $a^i \in (a + \mu d)I_2$ for some uniquely determined $d \in M_m(\mathbb{F})$. Moreover, d has trace 0 and μ^2 divides the trace of $a^i - a$.*

Proof:
Let $a, b \in M_m^\circ(R)$ and $d \in GL_m(R)$.
(a) $(1 + \mu^l a)(1 + \mu l b) = 1 + \mu(a + b + \mu^l ab)$ and so I_l is a subgroup of $GL_m(R)$. Also $(1 + \mu^l a)^d = 1 + \mu^l a^d$ and so I_l is a normal subgroup of $GL_m(R)$.
(b)
Let $x = 1 + \mu^r a$, $y = 1 + \mu^s b$ and $z = 1 + \mu^{r+s}(ba - ab)$. Then modulo I_{r+s+1}

$$xyc \equiv (1+\mu^r a+\mu^s b+\mu^{r+s}ab)(1+\mu^{r+s}ba-\mu^{r+s}ab) \equiv (1+\mu^r a+\mu^s b+\mu^{r+s}ab)+\mu^{r+s}ba-\mu^{r+s}ab \equiv 1+\mu^r a+\mu^s b+\mu^{r+}$$

Thus $[x, y] = x^{-1}y^{-1}xy \equiv c$ modulo I_{r+s+1} and (b) holds.
(c) follows fro (b) and some straightforward calculations.
(d) The map $\mathcal{M}_m \circ (\mathbb{F}) \to I_l/I_{l+1}, a \to (1 + \mu^l a)I_{l+1}$ is $GL_m(\mathbb{F})$-isomorphism.

(e) We may assume without loss that $\mu^2 = 0$. The $I_2 = 0$. We first show the uniqueness of d. So suppose that $a + \mu d = a + \mu e)$ with $d, e \in M_m(\mathbb{F})$. Then $\mu(d - e) = 0$ and since $d - e \in M_m(\mathbb{F})$, $d - e = 0$ and $d = e$.

For the existence of d, note that $i = 1 + \mu b$ with $b \in M_m(\mathbb{F})$ and so $i^{-1} = 1 - \mu b$. Thus

$$a^i \in (1 - \mu b)a(1 + \mu b) = a + \mu(ab - ba)$$

So $d = ab - ba$ works. Also ab and ba have the same trace and so $ab - ba$ has trace 0.□

Let R be a commutative ring and $O \neq \xi \in R$. Let S_ξ be the subgroup of $SL_2(R)$ generated by

$$a := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad b_\xi : \begin{pmatrix} 1 & 0 \\ \xi & 1 \end{pmatrix}$$

Lemma 4.4.9 [**sxi irreducible**] *Let $\mathbb{F}$ be a locally finite field with $0 \neq p := \operatorname{char} F \neq 2$ and $0 \neq \xi \in \mathbb{F}$. Then S_ξ acts irreducible on $M_2^\circ(\mathbb{F}_p[\xi])$*

Proof: Let $b = b_\xi$, $S = S_\xi$ and $\mathbb{K} = \mathbb{F}_p[\xi]$. Then $S \leq SL_2(\mathbb{K})$. Put $V = M_2^\circ(\mathbb{K})$ and let $0 \neq U$ an $\mathbb{F}_pS$ submodule in V. We need to show that $U = V$. Note that V is an $\mathbb{K}S$-module. Put $x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $y := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $z := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Direct martix calculations show that

1° [**1**] $\quad [x, a] = 0, [y, a] = 2x$ *and* $[z, a] = y - x$.

2° [**2**] $\quad [x, b] = \xi y - \xi^2 z,\ [y, b] = -2\xi z$ *and* $[z, b] = 0$

In particular,

3° [**3**] $\quad [x, a, a] = [y, a, a] = 0$ *and* $[z, a, a] = 2x$.

and

4° [**4**] $\quad [z, a, a] = [y, a, a] = 0$ *and* $[x, a, a] = -2\xi^2 z$.

Thus $C_V(a) = \mathbb{K}x$. Put $E := \{a \in K \mid lx \in U\}$ and $D := \{d \in \mathbb{K} \mid dx \in U + \mathbb{K}y + \mathbb{K}z$. Then E and D are $\mathbb{F}_p$ subspace of $\mathbb{K}$ and $E \leq D$. Since $C_U(a) \neq 0$, $E \neq \{0\}$. Let $d \in D$. Then $[dx, b, b] \in U$ and so from (4°), $-2\xi^2 z \in U$ and so by (4°) $[-2\xi^2 z, a, a] = -4\xi^2 x \in U$. Thus $\xi^2 E \leq \xi^2 D \leq E$. Since multiplication by ξ^2 is invertible we conclude that

5° [**5**] $\quad E = D = \xi^2 D$.

Let $e \in E$. Then $[ex, b, a] = e[\xi y - \xi^2 z, a] = e((2\xi + \xi^2)x - \xi^2 y) \in U$. Thus $(2\xi + \xi^2)e \in D = E$. Since by (5°), $\xi^2 e \in E$ we get $e\xi \in E$. Thus E is invaraint under multiplication by ξ. Since $\mathbb{K} = \mathbb{F}_p[\xi]]$, ξ acts irreducible on $\mathbb{K}$ by left multipication. Hence $E = \mathbb{K}$. It now follows from (2°) and (4°) that $V = \mathbb{K}x + \mathbb{K}y + \mathbb{K}z \leq Ex + [Ex, b] + [Ex, b, b] \leq U$ and so $V = U$. This completes the proof of the lemma.

□

Lemma 4.4.10 [**a+y a root**] *Let $\mathbb{F}$ be a field, f a polynomial over $\mathbb{F}$, n be a non-negative integer and a a root of f in some extension field $\mathbb{K}$ of $\mathbb{F}$.*

(a) [**a**] *a has multiplicity at least n as a root of f if and only if $a + y$ is a root of f in $\mathbb{K}[y]/(y^n)$.*

(b) [**b**] *The map $\phi : \mathbb{F}[x]/(f^n) \to \mathbb{K}[y]/(y^n)$, $g + (f^n) \to f(a + y) + (y^n)$ is a well-defined ringhomomorphsim.*

(c) [**c**] *Suppose that $\mathbb{K} = \mathbb{F}(a)(\cong \mathbb{F}[x]/(f))$ and that f is irreducible and seperable. Then ϕ is an isomorphism.*

Proof: (a) The proof is by induction on n. Write $f = g \cdot (x - a) + b$ with $g \in \mathbb{K}[x]$ and $b = f(a) \in \mathbb{K}$. Then $f(a + y) = g(a + y)y + b$. Hence $f(a + y) \in (y^n)$ if and only if $b = 0$ and $g(a + y) \in (y^{n-1})$. By induction this is true if and only if a is a root of f and a is has multiplicity at least $n - 1$ as a root of g. Thus (a) holds.

(b) Consider the ringhomorphism $\psi : \mathbb{F}[x] \to \mathbb{K}[y]/(y^n), g \to g(a + y)$. Since a has multiplicity at least n as a root of f^n we get from (a) that $\psi(f^n) = 0$. Thus $(f^n) \leq \ker \psi$ and (b) holds.

(c) Hence $\mathbb{F}[x]$ is a PID, $\ker \psi = (h)$ for some $h \in \mathbb{F}[x]$. Since $\psi(f^n) = 0$, h divides f^n. Since f is irreducible we can choose $h = f^m$ for some $m \leq n$. From (a) we have that a has multiplicity at least n as a root of $h = f^m$. As f is seperable(that is f has no double roots) we concclude that $m \leq n$ and so $m = n$. Hence $\ker \psi = (f^n)$ and so ϕ is one to one. Let $d = \deg f$. Then both $\mathbb{F}[x]/(f^n)$ and $\mathbb{K}[y]/(y^n)$ have dimension nd over $\mathbb{F}$ and so ϕ is an isomorphism. □

Lemma 4.4.11 [**Sf**] *Let p be a prime and f a non-constant polynomial over $\mathbb{F}_p$ with $f(0) \neq 0$. Let $\xi_f = x + (f) \in R_f$, $R_f = \mathbb{F}_p[x]/(f)$ and $S_f = S_{\xi_f}$*

(a) [**a**] *Suppose that f is irreducible. Then R_f is a field and exactly one of the follwing holds.*

1. [**a**] *$S_\xi = SL_2(R_\xi)$ and either $p \neq 3$, or $\xi^2 = -1$.*
2. [**b**] *$S_\xi \cong SL_2(5)$, $p = 3$ and $\xi^2 = -1$.*

(b) [**b**] *Suppose that $f = g^n$ for an irreducible polynomial g. Then*

(a) [**a**] $R_f \cong R_g[y]/(y^n)$.

(b) [**b**] *According to (b:a), view R_g has a subfield of R_f. Then*

$$S_f = (1 + M_2^\circ(R_f)S_g.$$

(c) [**c**] *Suppose that $f = \prod_{i=1}^m g_i$, where $g_i = f_i^{n_i}$ and the f_i are pairwise distinct irreducible polynomials in $F_p[x]$. Then*

(a) [**a**] $R_f \cong \oplus_{i=1}^m R_{g_i} \cong \oplus_{i=1}^m R_{f_i}[y]/(y^{n_i})$.

(b) [**b**] $SL_2(R_f) \cong \bigtimes_{i=1}^m SL_2(R_{g_i}) \cong \bigtimes_{i=1}^m SL_2(R_{f_i}[y]/(y^{n_i}))$.

(c) [**c**] $S_f \cong \bigtimes_{i=1}^n S_{g_i}$.

Proof: (a) is Dickson's Theorem ([**?**]).

(b:a) follows from 4.4.10(c).

(b:b) Let $\mathbb{F} = R_g$ and $R = \mathbb{F}[y]/(y^n)$. Then $\xi := \xi_g = x + (f)$ is root of f in $\mathbb{F}$. Also put $\mu = y + (y^n)$. Then $\mu^n = 0$ and $R = \mathbb{F}[\mu]$. By (b:a), $SL_2(R_f)$ and $SL_2(R)$ are isomorphic. Moreover, (see 4.4.10(b)) we can choose this isomorphism such that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 0 \\ \xi_f & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ \xi + \mu & 1 \end{pmatrix}$$

So we need to compute the subgroup $S := S_{\xi+\mu}$ of $SL_2(R)$. Let $I = (1 + M_2^\circ(R)$, $H = IS_\xi$ and $\rho = \xi + \mu$. By 4.6.6, S_g normalizes I and so H is a subgroup of $SL_2(R)$. $b_{\xi+\mu} = b_\mu b_\xi$ and $b_\mu \in I$ we see that both a and $b_{\xi+\mu}$ are in H. Hence $S \leq H$ and $H = SI$. Note that we can choose $\epsilon \in \pm 1$ such that $ab_{\epsilon\xi}$ is a p' element. Suppose that $S \cap I \leq \Phi(I)$. Then $S/S \cap I' \cong S_\xi$ and so $ab\epsilon\rho I'$ is a p' element. Thus there exists $i \in I$ with $ab_{\epsilon\rho} = (ab_{\epsilon\xi})^i$ modulo I'. We will now apply 4.6.6(d). Note that with the notations from 4.6.6, $I_1 = I$ and by 4.6.6(c), $I_2 = I\prime$. We conclude that μ^2 divides the trace of $ab_{\epsilon\rho} - ab_{\epsilon\xi} = a(b_{\epsilon\mu} - 1)$. But the latter has trace $\epsilon\mu$, a contradiction.

Thus $S \cap I \not\leq I'$. By 4.6.6(d) and 4.4.9 we have that S acts irreducible on $I/I\prime$. Thus $I = (S \cap I)I'$. Since I is nilpotent this implies $I \leq S$ and so $H = SI = S$. Thus (b:b) is proved.

The first part of (c:a) follows from the Chinese Remainder Theorem. The second part follows from (b:a).

(c:b) follows from (c:a) and 4.4.7.

(c:c) Put $S = S_f$, $S_i = S_{g_i}$ and $b_i = b_{g_i}$. We use the isomorphism in (c:b) to identify $SL_2(R_f)$ with $\bigtimes_{i=1}^m SL_2(R_{g_i})$. Then $S \leq \bigtimes_{i=1}^m S_i$. Let $A = S_1$ and $B = \bigtimes_{i=2}^m S_i$. Then $AB = SB$ and by induction on m, $AB = SA$. Hence $A \cap S \trianglelefteq A$, $B \cap S \trianglelefteq B$ and $A/A \cap S \cong$

$S/(A \cap S)(B \cap S) \cong B/B \cap S$. If $A \leq S$ we also get that $B \leq S$ and we are done. So we may assume that $S_i \not\leq S$ for all i.

Suppose first that $n_i = 1$ for all $1 \leq i \leq m$.

If A is not perfect then by (a), $R_{g_i} \cong \mathbb{F}_3$. So $p = 3$ and $g_i = x \pm 1$. Moreover,$B\infty \leq S^\infty$ and $S_i \not\leq S$ implies that $m = 2$ and wthout loss $g_1 = x + 1$ and $g_2 = x - 1$. Since $ab_1 \in S_1\prime$ but $ab_2 \notin S_2\prime$, we get that $S/(AB') = AB$. Thus S contains a Sylow p-subgroup of AB. Hence $A = (A \cap S)A'$ and as $A \cap S$ is normal in A, $A \leq S$, contrary to our assumnptions.

So we may assume that A is perfect and by symmetry that all the S_i's are perfect. Hence by (a) each of the S_i are quasisimple. In particular, $A \cap S_i \leq Z(A)$ and $A/A \cap S$ is quasimple. Suppose that $B \cap S \not\leq Z(B)$. Then B contains a component or B and thus $S_i \leq S$ for some i, contray to our assumptions.

Thus $B \cap S \leq Z(B)$. Since $B/B \cap S \cong A/A \cap S$ is quasisimple we conclude that $m = 2$. Moreover, the exists an isomorphism $\phi : S_1/Z(S_1) \to S_2/Z(S_2)$ which sends $a_1 Z(S_1)$ to $a_2 Z(S_2)$ and $b_1 Z(S_1)$ to $b_2 Z(S_2)$. Note that for $p = 3$ at most one of the S_i are isomorphic to $SL_2(5)$ (since $g_i = x^2 * 1$ if this holds. We conclude that $S_i = SL_2(R_i)$ and that ϕ is induced from a ismorphism of field $\sigma : R_1 \to R_2$. But then $g_1 = g_2$, a contradiction.

This completes the analysis of the case $n_i = 1$ for all $1 \leq i \leq m$. Let $T = O_p(AB) = O_p(A)O_p(B)$. Put $h = \prod_{i=1}^m f_i$. Since $AB/T = S_h$ we conclude from the preceeding case that $AB = ST$. Then $AT = (S \cap AT)T$ and so $O^p(A) \leq S$. By 4.6.6(d) and 4.4.9, $O_p(A) = [O_p(A), A] = [O_p(A), O^p(A)] \leq O^p(A)$ and so $O_p(A) \leq S$. By symmetry $O_p(S_i) \leq S$ for all i and so $T \leq S$ and $AB = ST = S$. $\square$

4.5 A second proof for the $SL_2(q)$-lemma

.

Lemma 4.5.1 [**ab semisimple**] *Let $\mathbb{F}$ a field, V a finite dimensional vector space over $\mathbb{F}$, and $a, b \in GL_{\mathbb{F}}(V)$. Suppose that a, b are quadratic and put $H = \langle a, b \rangle$.*

(a) [**a**] *Let $\lambda \, \mathrm{GL}_{\mathbb{F}}(V)$ with $[\lambda, H] = 1$. Let R be a commutative of $\mathrm{End}_{\mathbb{F}H}(V)$ containing $\mathbb{F}$, λ and λ^{-1}. Suppose that v be an eigenvector with eigenvalue λ for ab on V, that is $v^a b = \lambda v$. Put $W := Rv + Rv^a$ and $w = v^a$, then*

  (a) [**a**] *$v^a = w$ and $w^a = -v + 2w$.*

  (b) [**b**] *$v^b = 2v - \lambda^{-1} w$ and $w^b = \lambda v$*

  (c) [**c**] *$v^{ab} = \lambda v$ and $w^{ab} = 2(\lambda - 1) + \lambda^{-1} w$*

  (d) [**d**] *W is H-invariant.*

  (e) [**e**] *Suppose that $\lambda + \lambda^{-1}$ is invertible in R. Put $t := w - 2(\lambda + \lambda^{-1})^{-1}(\lambda - 1)v$. Then $t^{ab} = \lambda{-}1t$ and $W = Rv \oplus Rt$.*

(b) [**b**] *Suppose that ab is semisimple.*

(a) [**a**] *$V = C_V(ab) \oplus [V, ab]$ and both $[V, ab]$ and $C_V(ab)$ are H invariant.*

(b) [**b**] *If $\mathbb{F}$ is algebraicly closed then $[V, ab]$ is the direct sun of simple 2-dimensional $\mathbb{F}H$-submodules.*

(c) [**c**] *Suppose that $-ab$ is quadratic and $p = \operatorname{char} \mathbb{F} \neq 2$.*

(a) [**a**] *If $p \neq 0$, then $H \cong SL_2(p)$.*

(b) [**b**] *V is the direct sum of isomorphic simple 2-dimensional $\mathbb{F}H$-module.*

(c) [**c**] *There exists basis $v_i, w_i, 1 \leq i \leq m$ for V such that $\mathbb{F}v_i \oplus \mathbb{F}w_i$ is H invariant and the matrix for a and b with respect to v_i, w_i is*

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$$

Proof: (a) Since a is quadratic, $v^a - v = (v^a - v)^a$ and so $w - v = w^a - w$ and $w^a = -v + 2w$. Thus (a:a) holds.

Note that $\lambda v = v^{ab} = w^b$. Hence $v^{b^{-1}} = \lambda^{-1} w$. Since b is quadratic, $[v, b] = -[v, b^{-1}] = v - v^{b^{-1}} = v - \lambda^{-1} w$ amd so $v^b = 2v - \lambda^{-1} w$. Thus (a:b) holds. (a:d) follows immediately form (a:a) and (a:b).

Moreover, $v^{ab} = \lambda v$ and $w^{ab} = (v^{a^2})^b = (-v + 2w)^b = (-2v + \lambda^{-1} w) + 2\lambda v = 2(\lambda - 1)v + \lambda^{-1} w$ and so also (a:c) holds.

That $t^{ab} = \lambda^{-1} t$ follows by direct calulation from (**??**). The definition of t implies $Rv + Rt = Rv + Rw = W$. Let $u \in Rv \cap Rt$. Then $\lambda u = u^{ab} = \lambda - 1u$ and so $(\lambda - \lambda^{-1})u = 0$. Since by assumption $(\lambda - \lambda^{-1})$ is invertible we have $u = 0$ and $Rv \cap Rt = 0$. Thus (a:e) holds.

(b) We may assume that $\mathbb{F}$ is algebraicly closed. Since ab is semsimple, V is the direct sum of the eigenspaces for ab on V. Let $\lambda \in \mathbb{F}$, V_λ the corresponding eigenspaces and $v \in V_\lambda$. Since ab is semisimple, (a:c) implies that $w \in \mathbb{F}v + V_{\lambda^{-1}}$. Thus $V_\lambda + V_{\lambda^{-1}}$ is H invariant. Thus (b:a) holds.

Suppose now that $\lambda \neq 1$ and $v \neq 0$. If $w \in \mathbb{F}v$, then the qudratic action of a and b imply that H centralizes v, a contradiction to $v^{ab} = \lambda v \neq v$. Thus $\mathbb{F}v + \mathbb{F}w$ is 2-dimensional and we conclude that (b:b) holds.

(c) Suppose that $-ab$ is quadratic. Then $(ab + 1)^2 = 0$ and -1 is the only eigenvalue for ab on V. Let v be a nonzero eigenvector with eigenvalue -1 for ab on V. Then as we saw in the previous paragraph, $\mathbb{F}v + \mathbb{F}w$ is 2-dimensional. Moreover, by (a:c), $\mathbb{F}v$ is the unique 1-dimesional ab-invariant subspace of $\mathbb{F}v + \mathbb{F}w$ and we conclude that $U := \langle \ker ab + 1^H \rangle$ is the direct sum of simple 2-dimesional $\mathbb{F}H$-submodule. Thus $\dim V \geq \dim U = 2 \dim \ker ab + 1$ and since $ab + 1 = 0$ we conclude that $V = U$. Thus (c:b) holds.

Finally we compute from (a) that the matrices of a and b with respect to the basis $v + w, v - w$ of $\mathbb{F}v + \mathbb{F}w$ is are as given in (c:c). Thus (c:c) and so also (c:a) holds. □

4.6 R-compostion rings

Definition 4.6.1 [**def:composition ring**] *Let R be a commutative ring with* 1. *An R-*composition ring is pair $(A, \bar{\cdot})$ such that

(a) [**a**] A is a ring with $R \leq Z(A)$ (and $1_R = 1_A$).

(b) [**b**] $\bar{\cdot}$ is an R-linear anti-automorphism of A.

(c) [**c**] $\mathrm{N}(a) := a\overline{a} \in R$ for all $a \in A$.

(d) [**d**] $\mathrm{tr}(a) := a + \overline{a} \in R$ for all $a \in A$.

Lemma 4.6.2 [**norm quadratic**] *Let $(A, \cdot)$ be an R-composition ring and define $f(a, b) = a\overline{b} + b\overline{a} = \mathrm{tr}(a\overline{b})$.*

(a) [**a**] $\mathrm{N} : A \to R$ *is a multiplicative homomorphism.*

(b) [**b**] N *is a quadratic form on A over R with f as associate R-bilinear symmetric form.*

Proof: (a) $\mathrm{N}(ab) = ab\overline{ab} = ab\overline{b}a = a(b\overline{b})\alpha = (b\overline{b})(a\overline{a}) = \mathrm{N}\, a\, \mathrm{N}\, b$.

(b) Note that $f(\cdot, \cdot)$ is a R-bilinear symmetric form. Also $\mathrm{N}(a + b) = (a + b)(\overline{a + b}) = a\overline{a} + a\overline{b} + b\overline{a} + b\overline{b} = \mathrm{N}\, a + f(a, b) + \mathrm{N}\, b$. $\square$

Lemma 4.6.3 [**groups from nilpotent rings**] *Let A be a ring and N a nilpotent subring of A. Let $G = 1 + N$. Then G is a nipotent subgroup of A^*. Let $k, l \in \mathbb{Z}^+$ and define $G_k = 1 + N^k$. Then $[G_k, G_l] \leq G_{k+l}$ and for all $n \in N_k, m \in N_l$*

$$[1 + n, 1 + m] \equiv 1 + \lceil n, n \rceil \mod G_{k+l+1},$$

where $\lceil n, m \rceil = nm - mn$.

Proof: Let $n \in N$. Since N is nilpotent, $n^k = 0$ for some $k \in \mathbb{N}$. Thus $\sum_{i=0}^{\infty}(-n)^i$ is well defined and is an inverse for $1 + n$ in $1 + N$. Also $(1 + n)(1 + m) = 1 + (n + m + nm)$ and so $1 + N$ is closed under multiplication. Thus G is a group under multiplication. Now let $n \in N_k$ and $m \in N_l$. Put $x = 1 + n$, $y = 1 + m$ and $x = \lceil x, y \rceil = \lceil n, m \rceil$. Then

$$[x, y] = x^{-1}y^{-1}xy = x^{-1}y^{-1}(yx + z) = 1 + x^{-1}y^{-1}z$$

Since $x^{-1}y^{-1} \in G$, $x^{-1}y^{-1} = 1 + r$ for some $a \in N$. Now $z \in N^{k+l}$, $az \in N^{k+l+1}$ and $[x, y] = 1 + z + az \in 1 + z + N^{k+l+1}$. Hence $(1 + z)^{-1}[x, y] \in 1 + N^{k+l+1} = G_{k+l+1}$. $\square$

Lemma 4.6.4 [**rnf(n)**] *Let R be a commutative ring and N a nilpotent ideal in R. Let $f \in R[x]$ sich that $f(0)$ is invertible. Then the map $N \to N : n \to nf(n)$ is a bijection.*

Proof: Let k be minimal with $N^k = 0$ and put $A = N^{k-1}$. If $k = 0$, $N = 0$ and the lemma holds. Suppose $k > 0$ and let $m \in N$. By induction on k, there exists a unique $n + A \in N/A$ with $a := m - nf(n) \in A$. Let $b \in A$. Since A is an ideal in R, $f(n+b) = f(n) + d$ for some $d \in A$. Also $f(n) = f(0) + e$ with $e \in N$. From $NA = 0$ we conclude

$(n+b)f(n+b) = (n+b))(f(n)+d) = (n+b)f(n) = nf(n) + bf(n) = nf(n) + bf(0) = m - a + f(0)b$. Thus $n + f(0)^{-1}a$ is the unique solution of $m = nf(n)$ in N. □

Lemma 4.6.5 [**nilpotent and composition**] *Let $(A, \bar{\cdot})$ be an R-composition ring and N be nilpotent subring of A with $\overline{N} = N$. Supppose that 2 is invertible in A. For $S \subseteq A$ let $S_\circ = S \cap \ker \mathrm{tr}$. Let $H = 1 + N$ and $H^* = \{h \in H \mid \mathrm{N}(h) = 1\}$.*

(a) [**a**] *For each $a \in A$ there exist unique $r_a \in R$ and $t_a \in A^\circ$ with $a = r_a + t_a$.*

(b) [**b**] *For any subring B of A with $B = \overline{B}$, $B = (B \cap R) \oplus B_\circ$.*

(c) [**z**] *Let $a, b \in A_\circ$. Then $t_{ab} = \frac{1}{2}\lceil a, b \rceil$.*

(d) [**c**] *For each $n \in N_\circ$ there exists a unique $s_n \in R \cap N$ with $1 + s_n + n \in H^*$. Moreover, $s_n \in R \cap N^2$.*

(e) [**d**] *The map $\phi : N_\circ \to H^*$, $n \to 1 + s_n + n$ is a bijection with inverse $h \to t_h$.*

(a) $r_a = \frac{1}{2}\,\mathrm{tr}\, a = \frac{1}{2}(a + \overline{a})$ and $t_a = a - r_a = \frac{1}{2}(a - \overline{a})$.

(b) Let $b \in B$. Since $B = \overline{B}$, $\mathrm{tr}\, b \in B$. Thus also r_b and $t_b \in B$. Therefore $B = (B \cap R) + B^\circ$. If $b \in R \cap B^\circ$, then $2b = \mathrm{tr}\, b = 0$ and so $b = 0$ since 2 is invertible.

(c) Since $a, b \in A_\circ$ we have $\overline{a} = -a$ and $\overline{b} = -b$. Thus

$$t_{ab} = \frac{1}{2}ab - \overline{ab} = \frac{1}{2}(ab - \overline{b}\overline{a}) = \frac{1}{2}(ab - ba).$$

(d) Let $s \in R \cap N$ and $n \in N^\circ$. Then $\mathrm{N}(1 + s + n) = (1+s)^2 + (1+s)\,\mathrm{tr}\, n + \mathrm{N}\, s = (1+s)^2 + \mathrm{N}\, s$. Thus $1 + s + n \in H^*$ if and only if

$$\mathrm{N}(s) = -2s(s - \frac{1}{2})$$

So by 4.6.4, there exists a unqique such s. Since $\mathrm{N}(s) \in N^2$, we can alreay such an s in $R \cap N^2$.

(e) Let $n \in N^\circ$. Since $1 + s_n \in R$, $t_{1+s_n+n} = n$. Let $h \in H^*$. Then $h = 1 + m$ for some $m \in N$. Also $h = 1 + (r_m + t_m) = (1 + r_m) + t_m$. Thus implies $t_h = t_m \in N$ and $\phi(t_m) = h$.
□

Lemma 4.6.6 [**trace 0**] *Let $(A, \bar{\cdot})$ be an R-composition ring and N be nilpotent subring of A which is generated by $N_\circ$ as a ring. Suppose also 2 is invertible in A. Then $N = \overline{N}$ and for all $k \in \mathbb{Z}^+$:*

(a) [**a**] $N^k = (R \cap N^k) \oplus N_\circ^{\lceil k \rceil}$ *and*

(b) [**b**] $\phi(N_\circ^{\lceil k \rceil}) = (1 + N^k) \cap H = H^{[k]}$

(c) [**c**] $\phi_k : N_\circ^{\lceil k \rceil}/N_\circ^{\lceil k+1 \rceil} \to H^{[k]}/H^{[k+1]},\ n + N_\circ^{\lceil k+1 \rceil} \to \phi(n)H^{[k+1]}$ *is a well defined isomorphism.*

Proof: Since $\overline{a} = -a$ for all $a \in N_\circ$ we have $N = \overline{N}$ and we can apply 4.6.5.

(a) For $k = 1$ this follows from 4.6.5(b). Suppose **??** holds for k, we will show that it also holds for $k + 1$. Let $a \in N_\circ$ and $b \in N_\circ^{\lceil k \rceil}$. Thus by 4.6.5(a) and d

$$ab = r_{ab} + t_{ab} = r_{ab} + \lceil a, b \rceil \in D := (R \cap N^{k+1}) + N_\circ^{\lceil k+1 \rceil}$$

So the set of all $m \in A$ with $mN_\circ^{\lceil k \rceil} \leq D$ is a subring containing N° and so $NN_\circ^{\lceil k \rceil} \leq D$. Similarly $N_\circ^{\lceil k \rceil}N \leq D$

This implies

$$\begin{aligned} N^{k+1} &= ((R \cap N) + N_\circ)((R \cap N^k) + N_\circ^{\lceil k \rceil}) \\ &= (R \cap N)(R \cap N^k) + NN_\circ^{\lceil k \rceil} + N_\circ^{\lceil k \rceil}N \\ &\leq D \end{aligned}$$

As $D \leq N^{k+1}$ we get $N^{k+1} = D$ By 4.6.5(b) the sum defining D is a direct sum and (a) holds.

(b) Let $n \in N_\circ^{\lceil k \rceil} \leq N^k$ and put $H_k = (1 + N^k) \cap H$. Then $t_n \in N^k$, $s_n \in N^{2k}$ and $\phi(n) \in H_k$. Conversely, $m \in N^k$ with $1 + m \in H$. By (b) $t_{1+m} = t_m \in N_\circ^{\lceil k \rceil}$. Since $\phi(t_m)1 + m$ we have $\phi(N_\circ^{\lceil k \rceil}) = H_k$.

We will show by induction on k that $H^{[k]}H_{k+1} = H_k$. For $k = 1$, this is obvious. So suppose its true for n. By 4.6.3, $H^{[k+1]} \leq [H, H_k] \leq H_{k+1}$. Let $h \in H_k$ and choose $n \in N_\circ^{\lceil k+1 \rceil}$ with $h = \phi(n)$. Then there exists finitely many $n_i \in N^\circ$ and $m_i \in N_\circ^{\lceil k \rceil}$ with $n = \sum_i \lceil n_i, m_i \rceil$. By the inductions assumption $\phi(m_i) \in h_i H_{k+1}$ for some $h_i \in H^{[k]}$. Put $d = \prod_i [\phi(n_i), h_i]$. Then $d \in H^{[k=1]}$. By 4.6.3,

$$[\phi(n_i), h_i] \equiv 1 + \lceil \phi(n_i) - 1, h_i \rceil mod H^{k+2}$$

and so also

$$[\phi(n_i), h_i] \equiv 1 + \lceil \phi(n_i) - 1, h_i - 1 \rceil \mod N^{k+2}$$

sicne $h_i - 1 - m_i \in R$ and $\phi(n_i) - 1 - n_i \in R$. We get

$$[\phi(n_i), h_i] \equiv 1 + \lceil n_i, m_i \rceil \mod N^{k+2}$$

and so

$$d \equiv 1 + \sum_i [\lceil n_i, m_i] \equiv 1 + n \mod N^{k+2}$$

By 4.6.5(d), $s_n \in N_{k+1}^2 \in N_{k+2}$.

$$h = \phi(n) = 1 + s_n + n \equiv 1 + n \equiv d \mod N^{k+2}$$

Hence also

$$h \equiv d \mod H^{[k+2]}.$$

This completes the proof that $H^{[k]}H_{k+1} = H_k$. In particular if $H^{[k+1]} = H_{k+1}$ then also $H^{[k]} = H_k$.. Let $t \in \mathbb{N}$ with $N^t = 0$. Then $H^{[t]} \leq H_t = 1$. Thus $H^{[k]} = H_k$ for all k and (b) holds.

(c) Let $n, m \in N_\circ^{\lceil k \rceil}$. Then $\phi(n) \equiv 1 + n \mod N^{k+1}$. So $\phi(n) \equiv \phi(m) \mod H_{k+1}$ if and only if $n \equiv m \mod N^{k+1}$. By (a), $N^{k+1} \cap N_\circ^{\lceil k \rceil} = N_\circ^{\lceil k+1 \rceil}$. So $\phi(n)H_{k+1} = \phi(m)H_{k+1}$ if and only if $n + N_\circ^{\lceil k+1 \rceil} = m + N_\circ^{\lceil k+1 \rceil}$. Thus ϕ_k is well defined and one to one.

Also $\phi(n)\phi(m) \equiv 1 + n + m \equiv \phi(n+m) \mod N^{k+1}$ and so $\phi_k(n)\phi_k(m) = \phi_k(n+m)$. Thus ϕ_k is a homomorphism and (c) is proved. □

4.7 The ring $M_R(\delta)$

Let R be a commutative ring and $\delta \in R$. Define $M = M_R(\delta)$ to be the ring with $R \leq Z(M)$ and generated by R, α and β subject to the relation $\alpha^2 = 0, \beta^2 = 0$ and $\delta = \alpha\beta + \beta\alpha$.

Lemma 4.7.1 [**aba**] *Let $n \in N$. Then*

(a) [**a**] $\alpha\beta\alpha = \delta\alpha$.

(b) [**b**] $\beta\alpha\beta = \delta\beta$

(c) [**c**] $(\alpha\beta)^2 = \delta\alpha\beta$.

(d) [**d**] *M is a free R-module with basis $1, \alpha, \beta, \alpha\beta$.*

Proof: Since $\alpha\beta = \delta - \beta\alpha$ and $\alpha\alpha = 0$, (a) holds. By symmetry (b) holds and (c) follows from (a). From (a)-(b) we conclude that M is spanned by $1, \alpha, \beta$ and $\alpha\beta$ as an R-module and it is easy to see that (d) holds. □

Since $\delta = (-\beta)(-\alpha) + (-\alpha)(b)$, the opposite ring of M is isomorphic to R and their exists an unique R-linear anti-automorphism $\bar{\cdot} : M \to M, m \to \overline{m}$ with $\overline{\alpha} = -\alpha$ and $\overline{\beta} = -\beta$. Note that $\bar{\cdot}$ has order two. For $m, x, y \in N$ define $\operatorname{tr} m = m + \overline{m}$, $\operatorname{N} m = m\overline{m}$ and $f(x, y) = x\overline{y} + y\overline{x}$.

Lemma 4.7.2 [**direct sums and m**]

(a) [**a**] *Suppose that* $R = \bigtimes_{i\in I} R_i$ *and* $\delta = (\delta_i)_{i\in I} \in R$. *Then* $M_R(\delta) \cong \bigtimes_{i\in I} M_{R_i}(\delta_i)$.

(b) [**b**] *Let* I *be an ideal in* R. *Then* MI *is an ideal in* M, $MI = I \oplus I\alpha + I\beta + I\alpha\beta$, *and* $M_(R/I)(\delta + I) \cong M/MI$.

Proof: (a): Put $M^* = \bigtimes_{i\in i} M_{R_i}(\delta_i)$, $\alpha^* = (\alpha_i)_{i\in I}$ and $\beta^* = (\beta_i)_{i\in I}$. Then $R \leq Z(M^*)$ and $\alpha^*\beta^* + \beta^*\alpha^* = \delta$. Hence there exists an unique R-linear ring homomorphism $\phi : M_R(\delta) \to M^*$ with $\phi(\alpha) = \alpha^*$ and $\phi(\beta) = \beta^*$.

Lemma 4.7.3 [**trace and norm**]

(a) [**a**] $\overline{1} + 1$, $\overline{\alpha} = a$, $\overline{\beta} = -\beta$ *and* $\overline{\alpha\beta} = \beta\alpha = \delta - \alpha\beta$.

(b) [**b**] $\operatorname{tr} 1 = 1, \operatorname{tr}\alpha = \operatorname{tr}\beta = 0$ *and* $\operatorname{tr}(\alpha\beta) = \delta$.

(c) [**c**] $\mathrm{N}\,1 = 1$, $\mathrm{N}\,\alpha = \mathrm{N}\,b = \mathrm{N}(\alpha\beta) = 0$.

(d) [**d**] $\operatorname{tr} : M \to R$ *is* R *linear.*

(e) [**e**] $f : M \to M \to R$ *is a symmetric and* R*-bilinear.*

(f) [**f**] $\mathrm{N} : M \to R$ *is a quadratic form with* f *as its associate symmetric form, that is* $\mathrm{N}(x + y) = \mathrm{N}(x) + f(x, y) + \mathrm{N}(y)$ *for all* $x, y \in M$.

(g) [**g**] $\mathrm{N} : M \to R$ *is a multiplicative homomorphisms.*

Proof: (a),(b) and (c) are readily verified. Clearly tr is a Rlinear map from M to M. Since M is spanned by $1, \alpha, \beta$ and $\alpha\beta$ we conclude from (b) that $\operatorname{tr}(M) \leq R$ and so (d) holds.

Clealry f is symmetic and R-bilinear. Since $f(x, y) = \operatorname{tr}(x\overline{y})$, we conclude from (d) that f takes values in R and so (d) holds.

$\mathrm{N}(x+y) = (x+y)(\overline{x + y}) = (x+y)(\overline{x}+\overline{y}) = x\overline{x}+x\overline{y}+y\overline{x}+\overline{y}\overline{y} = \mathrm{N}(x)+f(x, y)+\mathrm{N}(y)$. Also for $r \in R$, $\mathrm{N}(rx) = r^2\,\mathrm{N}(x)$. So (c) and (d) imply that $\mathrm{N}(M) \subseteq R$ and (e) is proved.

Since $\mathrm{N}(y) \in R \leq Z(M)$ we compute $\mathrm{N}(xy) = (xy)(\overline{xy}) = xy\overline{y}x = x\,\mathrm{N}(y)\overline{x} = (x\overline{x})\,\mathrm{N}(y) = \mathrm{N}(x)\,\mathrm{N}(y)$. So also (g) is proved. □

Define $GL_R(\delta)$ the set of invertible elements in M. Let $SL_R(\delta) = \{m \in M \mid \mathrm{N}(m) = 1\}$. Note that both $GL_R(\delta)$ form groups under multiplication. Let R^* be set of invertibel elements in R.

Lemma 4.7.4 [**glrd**]

(a) [**a**] *Let* $m \in M$. *Then* $m \in GL_R(\delta)$ *if and only if* $\mathrm{N}(m) \in R^*$.

(b) [**b**] *Let* $m \in GL_R(\delta)$. *Then* $m^{-1} = \mathrm{N}\,m^1\overline{m}$.

(c) [**c**] *$SL_R(\delta)$ is a normal subgroup of $GL_R(\delta)$ and $SL_R(\delta) = \{m \in GL_R(\delta) \mid \overline{m} = m^{-1}\}$.*

Proof: Let m be in M. If m is invertible than $\mathrm{N}(m)\,\mathrm{N}(m^{-1}) = \mathrm{N}(mm^{-1}) = \mathrm{N}(1) = 1$ and so $\mathrm{N}(m)$ is inverible. Suppose now that $\mathrm{N}(m)$ is invertible, then $\mathrm{N}(m^{-1}\overline{m})m = \mathrm{N}(m^{-1})\,\mathrm{N}(m) = 1$. Thus m is invertible and (a) and (b) hold. Since $SL_R(\delta)$ is the kernel of the group homorphism $\mathrm{N} : GL_R(\delta) \to R^*$, the first statement in (c) holds. The second is obvious. □

Lemma 4.7.5 [**1+a in sl**]

(a) [**a**] *Let $m \in M$. Then $\mathrm{N}(m) = 1 + \mathrm{tr}(m) + \mathrm{N}(m)$. In particular, $1 + a \in SL_R(\delta)$ if and only if $\mathrm{tr}(m) = -\mathrm{N}(m)$.*

(b) [**b**] *Let $x \in M$ with $\mathrm{tr}(\alpha) = \mathrm{N}(a) = 0$. Then $x^2 = 0$ and $1 + Rx$ is a subgroups of $SL_R(\delta)$ isomorphic to $(R/\operatorname{Ann}_R(x), +)$. In particular, $1+Ra$ and $1+Rb$ are subgroups of $SL_R(\delta)$ isomorphic to R.*

Proof: $\mathrm{N}(1 + x) = \mathrm{N}(1) + \mathrm{tr}(y) + \mathrm{N}(y)$ and so (a) holds.

(b): Since $\mathrm{tr}(x) = 0$ we have $\overline{x} = -x$ and so $\mathrm{N}(x) = -x^2$. Thus $x^2 = 0$. Let $r, s \in R$. Then also $\mathrm{N}(rx) = 0 = \mathrm{tr}(rx)$ and so by (a), $1 + rx \in SL_R(\delta)$. Since $x^2 = 0$, the map $(R, +) \to 1 + Rx, r \mapsto 1 + rx$ is an onto groups homomorphism and so (b) holds. □

Put $R_\delta = \{r \in R \mid r\delta = 0\}$. For $m \in M$ let ϕ_m be the ring homomorphism from M to $\mathrm{End}_R(mM)$ resulting from the right M module mM.

Lemma 4.7.6 [**sld=sl2**]

(a) [**a**] *αM is a free R-module with basis $\alpha, \alpha\beta$.*

(b) [**b**] *The matrices of $\phi_(\alpha)$, $\phi_a(\beta)$, $\phi_a(\alpha\beta)$ and $\phi_\alpha(\beta\alpha)$ with respect to the basis α $\alpha\beta$ are*

$$\begin{pmatrix} 0 & 0 \\ \delta & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & \delta \end{pmatrix} \text{ and } \begin{pmatrix} \delta & 0 \\ 0 & 0 \end{pmatrix}$$

(c) [**c**] *The image of M in $\mathrm{End}_R(aM) = M_2(R)$ consists of all the matrices $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$, with $r - s \in R\delta$ and $t \in R\delta$.*

(d) [**d**] $\ker \phi_a = R_\delta a + R_\delta \beta\alpha$.

(e) [**e**] *$M/\alpha M + \beta M \cong R/Rd$ and $\alpha M \cap \beta M = R_\delta \alpha\beta$.*

(f) [**f**] *If δ is invertible, then ϕ_α is an isomorphism and $M = aM \oplus bM$.*

Proof: (a) follows easily from 4.7.1(d). (b) is readily verified. Let $m = r_1 + r_\alpha\alpha + r_\beta\beta + r_{\alpha\beta}\alpha\beta \in M$. Then by (b), $\phi_\alpha(M)$ has the matrix

$$\begin{pmatrix} r_1 & r_\alpha\delta \\ (,\beta) & r_1 + (,\alpha\beta)\delta \end{pmatrix}$$

Thus (c) holds. Moreover, $\phi(m) = 0$ if and only if $r_1 = r_\beta = r_\alpha\delta = r_{\alpha\beta}\delta = 0$ and so (d) is proved.

¿From (a) and symmetry $bM = R\beta + R\beta\alpha$. Since $\beta\alpha = \delta - \alpha\beta$ we get that $aM + bM = Rd + R\alpha + R\beta + R\alpha\beta$. Thus $M/aM + bM \cong R/Rd$. Also if $m \in aM \cap bM$, then $m = r\alpha\beta = s\beta\alpha = s\delta + s\alpha\beta$ for some $r, <\in, R>$. Thus $r = s$ and $s\delta = 0$ and (e) is proved.

(f) is an easy consequence of the previous statements. □

Let M° be the ideal in M generated by α and β.

Lemma 4.7.7 [**mcirc**] *$M\circ = \mathbb{R}\delta + R\alpha + R\beta + R\alpha\beta$, $M/M^\circ \cong R/R\delta$ and M° is nilpotent if an only if δ is nilpotent.*

Proof: This is easily verified. It might be also interesting to observe that the definition of M implies that $M/M\circ$ is the quotient ring of R definition by setting $\delta = 0$. □

Lemma 4.7.8 [**ideals**] *Let I be an ideal in $M_R(\delta)$ with $I \cap R = 0$.*

(a) [**a**] *Let $m = r_1 + r_\alpha\alpha + r_\beta\beta + r_{\alpha\beta}\alpha\beta \in I$. Then $\delta^2 r_1 = 0, \delta^2 r_\alpha = 0$, $\delta^2 r_\beta = 0$ and $\delta^3 r_{\alpha\beta} = 0$. In particular, $\delta^3 I = 0$.*

(b) [**b**] *Suppose that $R = \mathbb{F}[\delta]$ for some field $\mathbb{F} \leq R$. Suppose also that there exists $n \in \mathbb{N}$ with $\delta^{n+1} = 0$ and that n is minimal with this property.*

Proof:

1° [**1**] *If $r \in R$ with $r\alpha \in I$ or $r\beta \in I$ then $\delta r = 0$.*

¿From $r\alpha \in I$ we get $r\alpha\beta \in I$ and $r\beta\alpha = 0$. Hence also $r\delta = r(\alpha\beta + \beta\alpha) \in I$. From $R \cap I = 0$ we conclude that $r\delta = 0$.

Let $m = r_1 + r_\alpha\alpha + r_\beta\beta + r_{\alpha\beta}\alpha\beta \in I$.

2° [**2**] *$\delta^2 r_\alpha = 0 = \delta^2 r_\beta$.*

$\alpha m\alpha = r_\beta\alpha\beta\alpha = \delta r_\beta\beta$. So by (1°), $\delta^2 r_\beta = 0$. Also $\beta m\beta = \delta r_\alpha\alpha$ and by (1°) $\delta^2 r_\alpha = 0$.

3° [**3**] *$\delta^2 r_1 = 0$*

$\alpha m = r_1\alpha + r_\beta\alpha\beta \in I$ so (3°) follows from (2°) applied to αm in place of m.

4° [**4**] $\delta^3 r_{\alpha\beta} = 0$

$m\alpha = r_1\alpha + (,b)\beta\alpha + r_{\alpha\beta}\delta\alpha = r_\beta\delta + (r_1 + \delta r_{\alpha\beta})\alpha - r_\beta\alpha\beta$. So by (2°) applied to $m\alpha$ and using (3°) we have $0 = \delta^2(r_1 + \delta r_{\alpha\beta}) = \delta^3 r_{\alpha\beta}$. $\square$

What to do next: assume $R = \mathbb{F}[\delta]$, zentral series of for M° (maybe only if δ nilpotent). ideals in M, subgroup H generated by $1+\alpha, 1+\beta$. Prove some lemma if H is nilpotent. For example usually there exists $1 \neq h \in Z(H)$ with $[V, h, H] = 0$.

Chapter 5

Root Systems

5.1 Root Systems

Definition 5.1.1 [**def:root system**] *A root system is a set* Φ *together with a vectorspace* V_Φ *over* $\mathbb{Q}$ *and a non-degenerate, positive definite, symmetric form* $(\ ,\ )$ *on* V_Φ *such that*

(a) [**RS1**] Φ *is a finite set of non zero vectors in* V_Φ *and* Φ *spans* V_Φ.

(b) [**RS2**] *For all* $\alpha, \beta \in \Phi$, $<\alpha, \beta> := 2\frac{(\alpha,\beta)}{(\beta,\beta)} \in \mathbb{Z}$.

(c) [**RS3**] *For all* $\alpha, \beta \in \Phi$, $\omega_\alpha(\beta) \in \Phi$, *where*

$$\omega_\alpha : V_\Phi \to V_\Phi, v \to v - <v, \alpha>\alpha$$

is the reflection associated to α.

(d) [**RS4**] *If* $\alpha, \beta \in \Phi$ *are linearly dependent over* $\mathbb{Q}$ *then* $\alpha = \pm\beta$.

Let Φ be a root system. The elements of Φ are called *roots*. Put $W := \langle \omega_\alpha \mid \alpha \in \Phi \rangle \leq \mathrm{O}(V_{\mathbb{Q}}, (\ ,\ ))$. Note that (RS3) just says that Φ is invariant under W. Since Φ is finite and spans $V_{\mathbb{Q}}$, W is finite.

Lemma 5.1.2 [**dual root system**] *Let* Φ *be a root system. For* $\alpha \in \Phi$ *define* $\alpha^* := \frac{2}{(\alpha,\alpha)}\alpha$. *Let* $\Phi^* = \{\alpha^* \mid \alpha \in \Phi\}$ *Then for all* $\alpha, \beta \in \Phi$.

(a) [**a**] $<\alpha, \beta> = (\alpha, \beta^*)$.

(b) [**b**] $<\alpha, \beta> = <\beta^*, \alpha^*>$.

(c) [**c**] $\omega_\alpha = \omega_{\alpha^*}$

(d) [**d**] $\omega_{\alpha^*}(\beta^*) = (\omega_\alpha(\beta))^*$

(e) [**e**] Φ^* *(together with* V_Φ *and* $(\ ,\ )$*) is a root system.*

Proof: (a)-(d) are readily verified and (e) follows from (c) and (d). □

Definition 5.1.3 [**basis**] *Let Φ be a root system. A* basis *for Φ is a linearly independent subset Π of Φ such that $\Phi = \Phi^+ \mathbin{\dot\cup} \Phi^-$ where $\Phi^+ = \Phi \cap \mathbb{Q}^+\Pi$ and $\Phi^- = \Phi \cap \mathbb{Q}^-\Pi = -\Phi^+$.*

Lemma 5.1.4 [**alpha string**] *Let Φ be a root system and $\alpha, \beta \in Phi$ with $\alpha \neq \pm\beta$. Then*

(a) [**a**] *There exists non-negative integers p_-, p_+ such that for $i \in \mathbb{Z}$, $\beta + i\alpha \in \Phi$ if and only if $-p \leq i \leq q$.*

(b) [**b**] *Put $\epsilon = \mathrm{sgn}(\alpha, \beta)$, then one of the following holds.*

1. [**a**] *$p_{-\epsilon} = |{<}\beta, \alpha{>}|$ and $p_\epsilon = 0$.*
2. [**b**] *$p_{-\epsilon} = |{<}\beta, \alpha{>}| + 1$ and $p_\epsilon = 1$.*

(c) [**c**] *(b) holds iff α and β are not long and $\mathbb{Z}\{\alpha, \beta\} \cap \Phi$ is a root system of type B_2 or G_2.*

Proof: See [?] □

Lemma 5.1.5 [**linear combinations of roots**] *Let Φ be a root system, $A \subseteq \Phi$ and for $a \in A$ let $n_a \in \mathbb{Q}$. Put $\phi = \sum_{a \in A} n_a a$ and suppose that $\phi \in \Phi$. Then there exists $b \in A$ with $n_b(\phi, b) > 0$. Moreover, for any such b either $\phi = \pm b$ or $\phi - \mathrm{sgn}(n_a)a \in \Phi$.*

Proof: Note that $0 < (\phi\phi) = \sum_{a \in A} n_a(\phi, a)$. Hence there exists $b \in A$ with $n_b(\phi, b) > 0$.

Given any such b with $\phi \neq \pm b$. Then $\epsilon := \mathrm{sgn}(\phi, b) = \mathrm{sgn}\, n_n$. Also $|{<}\phi, a{>}| \geq 1$ and 5.1.4 implies that $\phi - \epsilon a \in \Phi$. □

Lemma 5.1.6 [**existence of simple roots**] *Let Φ be a root system.*

(a) [**a**] *Φ has basis.*

(b) [**b**] *Any two basis are conjugate under W.*

(c) [**c**] *If Π is any basis, than $\Phi^+ = \Phi \cap \mathbb{N}^+\Pi$.*

Definition 5.1.7 [**def: long**] *A root α in a root system Φ is called long (short) if $(\alpha, \alpha) \geq (\beta, \beta)$ $((\alpha, \alpha) \leq (\beta, \beta))$ for all $\beta \in \Phi$.*

Note here that if all roots in Φ have the same length, then all roots are long and short.

Lemma 5.1.8 [**dual basis**] *Let Φ be a root system with basis Π. Then $\Pi^* := \{\alpha^* \mid \alpha \in \Pi\}$ is a basis for Φ^*.*

Proof: Since for all $\alpha \in \Phi$, α and α^* only differ by a positive rational factor, $\mathbb{Q}^+\Pi = \mathbb{Q}^+\Pi^*$ and $\alpha \in Q^+\Pi$ if and only if $\alpha^* \in \mathbb{Q}^+\Pi^*$. Hence the lemma follows from the definition of a basis. $\square$

$$\Lambda := \{\lambda \in V_\Phi \mid (\lambda, \alpha^*) \in \mathbb{Z}, \forall \alpha^* \in \Phi^*\}.$$

The elements in Λ are the integral weights.

The elements in
$$\{\lambda \in V_\Phi \mid (\lambda, \alpha^*) > 0, \forall \alpha^* \in \Phi^*\}$$
are called dominant weights.

Note that by (RS2) $\Phi \subseteq \lambda$. Let $(\lambda_\alpha \mid \alpha \in \Pi)$ be the basis of $V_\mathbb{Q}$ dual to Π^* so $(\lambda_\alpha, \beta^*) = \begin{cases} 1 & \text{if } \alpha = \beta \\ 0 & \text{if } \alpha \neq \beta \end{cases}$. Then $(\lambda_\alpha \mid \alpha \in \Pi)$ is a $\mathbb{Z}$ basis for Λ.

For $\alpha, \beta \in \Phi$ let $r, s \in \mathbb{N}$ be maximal such that

$$\beta - r\alpha, \beta - (r-1)\alpha, \ldots, \beta - \alpha, \beta, \beta + \alpha, \ldots \beta + s\alpha)$$

all are roots. We call this sequence of roots the α-string through β. r will be denoted by $r_{\alpha\beta}$ and s by $s_{\alpha\beta}$.

5.2 Root Subsystems

Definition 5.2.1 [**def:root subsystem**] *Let Φ be a root system and $\Psi \subseteq \Phi$.*

(a) [**a**] *Ψ is a* root subsystem *of Φ if $(\Psi, \mathbb{Q}\Psi)$ is a root system.*

(b) [**b**] *Let R be a subring of Q. Then Ψ is called R-closed if $\Psi = \Phi \cap R\Psi$.*

Lemma 5.2.2 [**root subsystems**] *Let Φ be a root system and $\Psi \subseteq \Phi$. Then*

(a) [**a**] *Ψ is a root subsystem iff Φ is invariant under $W(\Psi) := \langle \omega_\psi \mid \psi \in \Psi \rangle$.*

(b) [**b**] *Ψ is $\mathbb{Z}$-closed iff $-\Psi \subseteq \Psi$ and $\alpha + \beta \in \Psi$ for all $\alpha, \beta \in \Psi$ with $\alpha + \beta \in \Phi$.*

(c) [**c**] *If Ψ is $\mathbb{Z}$-closed, then Ψ is a root subsystem. If Ψ is $\mathbb{Q}$-closed then Ψ is $\mathbb{Z}$ closed.*

(d) [**d**] *Ψ is a root subsystem if and only if Ψ^* is a root subsystem of Φ^*. Ψ is $\mathbb{Q}$-closed if and only if Ψ^* is $\mathbb{Q}$ closed.*

(e) [**e**] *If Ψ is a root subsystem and all roots in Ψ are long, then Ψ is $\mathbb{Z}$-closed.*

Proof: (a): Note that $(\Psi, \mathbb{Q}\Psi)$ fulfills (RS1),(RS2) and (RS4). Hence Ψ is a root subsystem iff $\omega_a(b) \in \Psi$ for all $\alpha, \beta \in \Psi$. This is the case iff Ψ is invariant $W(\Psi)$.

(b) One direction is obvious. Suppose now that $-\alpha \in \Psi$ for all $\alpha \in \Psi$, and $\alpha + \beta \in \Psi$ for all $\alpha, \beta \in \Psi$ with $\alpha + \beta \in \Phi$. Let $\phi = \sum_{\psi \in \Psi} n_\psi \psi \in \mathbb{Z}\Psi \cap \Phi$, where $n_\psi \in \mathbb{Z}$. We show by induction on $\sum |n_\psi|$ that $\phi \in \Psi$. By 5.1.5 we can choose $\psi \in \Psi$ with $n_\psi(\phi, \psi) > 0$. If $\phi = \pm\psi$, then $\phi \in \Psi$. So suppose $\phi \neq \pm\psi$. Then by 5.1.5 $\alpha := \phi - \operatorname{sgn} n_\psi \psi \in \Phi$. By induction $\alpha \in \Psi$ and so also $\phi = \alpha + \operatorname{sgn} n_\psi \psi \in \Phi$.

(c), (d) and (e) are readily verified. □

Given a connected root system Φ with two different root lengths. Then the short roots form a root subsystem which is not $\mathbb{Z}$-closed. And the long roots form a subsystem which is $\mathbb{Z}$-closed but not $\mathbb{Q}$-closed.

¿From the affine diagram of E_8 we see that E_8 has a root subsystem D_8. Since D_8 and E_8 both have rank 8, the $\mathbb{Q}$ closure of D_8 is E_8. On the otherhand D_8 is $\mathbb{Z}$-closed and contains the $\mathbb{Q}$-closure of any two of its elements.

The $\mathbb{Z}$ closure of $\Phi_{\text{long}} \times \Phi_{\text{short}}$ in $\Phi \times \Phi$ is $\Phi_{\text{long}} \times \Phi$. The $\mathbb{Q}$ closure is $\Phi \times \Phi$.

Let n, m be integers with $n \geq 2$ and $m \geq 1$. Then B_{n+m} has a subsystem $B_n \times B_m$. The long roots in B_n form a subsystem D_n and the short roots in B_m a subsystem A_1^m. Then $\mathbb{Z}$-closure of $D_n \times A_1^m$ is $D_n \times B_m$, while the $\mathbb{Q}$-closure is B_{n_m}.

Now let Ψ be a connected root subsystem of Φ. We claim that either Ψ is $\mathbb{Z}$ closed or that the $\mathbb{Z}$ closure of Ψ is $\mathbb{Q}$-closed. So suppose that Ψ is not $\mathbb{Z}$ closed. Then Ψ contains roots which are not long in Φ. Without loss Φ is the $\mathbb{Q}$-closure of Ψ. Then Φ is connected. Since Ψ is connected $\mathbb{Q}\Psi_{\text{short}} = \mathbb{Q}\Psi = \mathbb{Q}\Phi$. Thus Ψ_{short} has the same rank as Φ_{short}. Since Φ_{short} is of type A_n, D_n or A_1^m we conclude that $\Phi_{\text{short}} = \Phi_{\text{short}}$.

Thus $\Phi \subseteq \mathbb{Z}\Phi_{\text{short}} \leq \mathbb{Z}\Psi$ and Φ is the $\mathbb{Z}$ closure of Ψ.

Lemma 5.2.3 [**closure in rank 2**] *Let Φ be a root system and $\alpha, \beta \in \Phi$ with $(\alpha, \beta) \neq 0$. Then*

(a) [**a**] $\alpha \in \mathbb{Q}\langle \beta, \omega_\beta(\alpha) \rangle$.

(b) [**b**] *If α is not shorter than β then $\alpha \in \mathbb{Z}\langle \beta, \omega_\beta(\alpha) \rangle$.*

(c) [**c**] *If α and β have the same length, the $\alpha \in \langle \beta, \omega_\beta(\alpha) \rangle$.*

Proof: Readily verified, for example by inspection of the rank 2 root system $\mathbb{Q}\langle \alpha, \beta \rangle$ □

Lemma 5.2.4 [**z closure of phishort**] *Let Φ be a connected root system. Then Φ is the $\mathbb{Z}$ closure of Φ_{short}.*

Proof: Let α be a long root and choose a short root β with $(\alpha, \beta) \neq 0$. Then by 5.2.3(b), α is in the $\mathbb{Z}$ closure of β and $\omega_\alpha(\beta)$. □

Lemma 5.2.5 [**covering root systems**] *Let Φ be a root system.*

(a) [**a**] *Let Ψ be a root subsystem of Φ, $\alpha \in \Psi$ and $\beta \in \Phi \setminus \Psi$. Then $\omega_\alpha(\beta) \notin \Psi$.*

(b) [**b**] *Suppose that $\Phi \subseteq X \cup Y$ where X and Y are proper root subsytems of Φ. If X is $\mathbb{Q}$ closed or both X and Y are $\mathbb{Z}$-closed, then Φ is disconnected.*

(c) [**c**] *Suppose that Φ is connected and $\alpha, \beta \in \Phi$. Then there exists $\gamma \in \Phi$ such that γ is neither perpendicular to α nor to β. In particular α and β are contained in a connected subroot system of rank at most 3.*

Proof: (a) If $\omega_\alpha(\beta) \in \Psi$, then $\beta = \omega_\alpha(\omega_\alpha(\beta)) \in \Psi$ a contradiction.

(b) Choose X and Y as in (b) with $|X \cap Y|$ minimal. Let $A = \Phi \setminus Y$, $B = \Phi \setminus X$ and $C = \Phi \cap X \cap Y$. Let $a \in A$ and $b \in B$. Suppose for contradiction that $(a, b) \neq 0$. Then by (a), $\omega_b(a) \notin Y$ and so $\omega_b(a) \in X$. If X is $\mathbb{Q}$ closed, then by 5.2.3(a), $b \in \mathbb{Q}\langle a, \omega_b(a)\rangle \cap \Phi \subseteq X$, a contradiction. Thus X is not $\mathbb{Q}$ closed and so by assumption, X and Y are $\mathbb{Z}$-closed. Hence we may assume that b is not shorter than a. Thus by 5.2.3(b) $b \in \mathbb{Z}\langle a, \omega_b(a)\rangle \cap \Phi \subseteq X$, again a contradiction.

Thus $A \perp B$. Let $\tilde{X} = B^\perp \cap X$ and $\tilde{Y} = A^\perp \cap Y$. Then $\tilde{X}$ and $\tilde{Y}$ are subsystems. Moreover, either $\tilde{X}$ is $\mathbb{Q}$-closed or both $\tilde{X}$ and $\tilde{Y}$ are $\mathbb{Z}$-closed. Also $A \subseteq X$ and $B \subseteq Y$.

We claim that $\Phi = \tilde{X} \cup \tilde{Y}$, that is that $C \subseteq \tilde{X} \cup \tilde{Y}$. Let $c \in C$ and suppose that $c \notin \tilde{X}$. Then $(c, a) \neq 0$ for some $a \in A$. Since $c \in Y$ and a is not, (a) implies $\omega_c(a) = a - < a, c > c \in A$. Thus $\omega_c(a)$ and a both perpendicular to B. Hence $c \perp B$ and $c \in \tilde{Y}$.

Thus $C = \tilde{X} \cup \tilde{Y}$. The minimal choice of $X \cap Y$ implies $X \cap Y = \tilde{X} \cap \tilde{Y}$. Hence $C \subseteq \tilde{X} \cap \tilde{Y} \leq A^\perp \cap B^\perp$. Since also $A \perp B$, $A \cup B \cup C$ is a decompostion of Φ into pairwise orthorgonal subsets. Thus Φ is disconnected and (b) is proved.

(c) By (a) there exists $\gamma \in \Phi \setminus (\alpha^\perp \cup \beta^\perp)$. Also $\Phi \cap \mathbb{Q}\langle \alpha, \beta, \gamma\rangle$ is connected root system of rank at most 3. Thus (c) holds. □

Lemma 5.2.6 [**generation by non perpendicular roots**] *Let Φ be a connected root system, and α a short root.*

(a) [**a**] *Then $\mathbb{Q}\Phi = \mathbb{Q}\Phi_{long} = \mathbb{Q}\Phi_{Short}$.*

(b) [**b**] *Let Ψ be the root subsystem generated by α and the long roots, then $\Psi = \Phi$.* **Comment:false for** F_4

(c) [**c**] *Let Ψ be the root subsystem generated by α and the long roots which are not perpendicular to α. If Φ is not of type $C_n, n \geq 3$ or F_4, then $\Psi = \Phi$.* **Comment:maybe false for** F_4 **– indeed, it is false: if** $\alpha = e_1$**, then we obtain a subsystem of type** B_4

Proof:

(a) Let $\{i,j\} = \{long, short\}$. Since Φ is connected there exists $\alpha\Phi_i$ and $\beta \in \Phi_j$ with $<\alpha,\beta> \neq 0$. If $b \notin \mathbb{Q}\Phi_i$ then 5.2.5(a) implies $\omega_\beta(\alpha) \notin \mathbb{Q}\Phi_i$ a contradiction. Thus $\beta \in \mathbb{Q}\Phi_i$ and the transitivity of W_Φ on Φ_j implies $\mathbb{Q}\Phi_j \subseteq \mathbb{Q}\Phi_i$.

For (b) and (c) note that if Φ has rank two, then every subsystem containing a long and a short system equals Φ (**Comment:false for G_2, it contains a** $A_1(long) \times A_1(short)$ Also $\mathbb{Q}\Phi_{long} = \mathbb{Q}\Phi$ and so Ψ contains a long root. So we may assume that Φ has rank at least two. Let Σ be the subsystem generated by the long root.

(b) Without loss α is the highest short root. Let β be any short root. By (a) there exists a long root δ with $<\delta,\beta> < 0$. Then $\omega_\delta(\beta)$ has larger height than β **Comment:this is false if β is negative** and so by induction $\omega_\delta(\beta) \in \Psi$. Hence also $\beta \in \Psi$.

(c) We may assume that Φ is not of type C_n or F_4. Thus Σ is connected. By definition of Ψ, $\Sigma = (\Sigma \cap \Psi) \cup (\Sigma \cap \alpha^\perp)$. Since $\Sigma \cap \alpha^\perp$ is closed in Σ, 5.2.5(b) implies that $\Sigma \subseteq \Psi$. So (c) follows from (b). $\Box$

Lemma 5.2.7 [**height induction**] *Let Φ be a root system with simple roots Π and $\alpha \in \Phi^+ \setminus \Pi$. Then there exists $\beta \in \Pi$ and $\gamma,\delta \in \Phi^+$ with $\alpha = \omega_\beta(\gamma) = \beta + \delta$ and $(\beta,\gamma) < 0$.* **Comment:maybe combine with 5.1.5**

Proof: Since α is a positive linear combination of Π and since $(\alpha,\alpha) > 0$ there exists $\beta \in \Pi$ with $(\alpha,\beta) > 0$. Put $\gamma = \omega_\beta(\alpha)$ and $\delta = \alpha - \beta$. Then $(\beta,\gamma) = (\omega_\beta(\beta), \omega_\beta(\gamma)) = (-\beta,\alpha) < 0$. Since $\gamma = \alpha - <\alpha,\beta>\beta$ and α is not a multiple of β, γ is positive. Also δ is on the β-string from γ to α. So δ is a root and δ is positive. $\Box$

Lemma 5.2.8 [**perp of weight**] *Let Φ be a root system with simple roots Π and λ a dominant integral weight for Π. Then $\Pi \cap \lambda^\perp$ is a system of simple roots for $\Phi \cap \lambda^\perp$.*

Proof: Let Ψ be the root subsytem generated by $\Pi \cap \lambda^\perp$. It suffices to show that $\Psi = \Phi \cap \lambda^\perp$. Let $\alpha \in \Phi^+$ with $\lambda(\alpha) = 0$ (that is $\alpha \in \lambda^\perp$). We show by induction on $\mathrm{ht}\,\alpha$ that $\alpha \in \Psi$. If α has height 1, then $\alpha \in \Pi$ and so $\alpha \in \Psi$. If α ahs height larger than 1 then $\alpha \notin \Pi$ By 5.2.7, there exists $\beta,\gamma \in \Phi^+$ with $\alpha = \omega_\beta(\gamma)$ and $m := <\gamma,\beta> > 0$. Then $\alpha = m\beta + \gamma$. Since λ is dominant, both $\lambda(\beta)$ and $\lambda(\gamma)$ are non-negative. Thus $\lambda(\beta) = 0 = \lambda(\gamma)$. By induction, both β and γ are in Ψ and so also $\alpha \in \Psi$. $\Box$

5.3 Quadratic weights

Definition 5.3.1 [**def: quadratic weight**] *An integral weight λ on the root system Φ is called quadratic provided that $1 \leq (\alpha,\lambda) \leq 1$ for all short roots $\alpha \in \Phi_{\mathrm{short}}$.*

Theorem 5.3.2 [**quadratic weights**] *Let Φ be a connected root system and λ a non-zero dominant integral weight on Φ. Let $t \in \{\mathrm{long}, \mathrm{short}\}$ and α_t the heighest t-root in Φ. Then the following are equivalent.*

(a) [**d**] $(\alpha_t, \lambda) \leq 1$.

(b) [**e**] $\lambda = \lambda_\beta$ *for some root* $\beta \in \Pi$ *with* $n^t_\beta = 1$*, where* n^t_γ *for* $\gamma \in \Pi$ *is defined by* $\alpha_t = \sum_{\gamma\in\Pi} n^t_\gamma \gamma$.

(c) [**d+**] $\lambda = \lambda_\beta$ *for some root* $\beta \in \Pi$ *such that* β *is long if* $t = \mathrm{long}$ *and such that* Φ_t *is contained in the root subsystem generated by* $\Phi \cap \lambda^\perp$ *and* α

(d) [**g**] *One of the following holds:* **Comment:labeling of roots needs to be introduced Comment:needs to be updated, inparticular**

1. [**1**] $\Phi = A_n$ *and* $\lambda = \lambda_i$ *for some* $1 \leq i \leq n$.
2. [**2**] $\Phi = B_n$ *and* $\lambda = \lambda_1$ *or* λ_n.
3. [**3**] $\Phi = C_n$ *and* $\lambda = \lambda_i$ *for some* $1 \leq i \leq n$.
4. [**4**] $\Phi = D_n$ *and* $\lambda = \lambda_1, \lambda_{n-1}$ *or* λ_n.
5. [**5**] $\Phi = E_6$ *and* $\lambda = \lambda_1$ *or* λ_6.
6. [**6**] $\Phi = E_7$ *and* $\lambda = \lambda_1$.
7. [**7**] $\Phi = E_8$*: No such module.*
8. [**8**] $\Phi = G_2$ *and* $\lambda = \lambda_1$.
9. [**9**] $\Phi = F_4$ *and* $\lambda = \lambda_1$

(e) [**f**] λ *is the (unique) minimal (with respect to* $\prec$*) dominant weight in* $\lambda^{W(\Phi)} + \Phi_t^*$. **Comment:needs some work, maybe make extra lemma**

Proof: Put $\alpha = \alpha_t$.

(a)$\Longleftrightarrow$ (b): Let $\lambda = \sum_{\beta\in\Pi} m_\beta \lambda_\beta$. Then each m_β is a non-negative integer and each n^t_γ is a positive integer. Also $(\alpha, \lambda) = \sum_{\beta\in\Pi} m_\beta n^t_\beta$ and so (a) and (b) are equivalent.

(b)$\Longrightarrow$ (c): Let Ψ be the root subsystem generated by $\Phi \cap \lambda^\perp$ and α.

Let $\delta \in \Phi^+_t$. We need to show that $\delta \in \Psi$. Since (b) implies (a), $(\alpha, \lambda) = 1$ and so $(\delta, \lambda) = 0$ or $(\delta, \lambda) = 1$.

Suppose that $(\delta, \lambda) = 0$, then $\delta \in \Phi \cap \lambda^\perp$ and so $\delta \in \Psi$.

Suppose next that $(\delta, \lambda) = 1$ and that δ is not perpendicular to α. Since $(\alpha, \delta) \geq 0$ and α_t and δ have the same length we conclude that $<\alpha, \delta> = 1$ and so $\omega_\alpha(\delta) = \delta - \alpha$. Also $(\delta, \lambda) = (\alpha, \lambda)$ and hence $\delta - \alpha \in \Phi \cap \lambda^\perp \subseteq \Psi$. Thus $\delta = \omega_\alpha(\delta - \alpha) \in \psi$.

Suppose finally that $(\delta, \lambda) = 1$ and δ is perpendicular to α. By 5.2.5(c), there exists $\gamma \in \Phi$ such that γ is neither perpendicular to α nor to δ. If $\gamma \in \Phi_t$ then by the previous paragraph both γ and $\omega_\gamma(\delta)$ are in Ψ, so also $\delta \in \Psi$. So suppose that $\gamma \notin \Phi_t$. Since the diagram of (α, γ, δ) is not sperical, we see that α, γ, δ are not linear independent. Let Δ be the root sytem generated by α, γ and δ. Then Δ has rank two, is connected and has a pair of perpendicular roots of the same length. Δ is of type B_2. Put $r = |<\gamma, \alpha>|$ and

$\mu = \alpha - r\delta$. In δ we see that $\mu \in \Phi$, and $\delta = \omega_\mu(\alpha)$. Since $(\delta, \lambda) = (\mu, \lambda)$ we have $\mu \in \Phi \cap \lambda^\perp$. Hence $\delta = \omega_\mu(\alpha) \in \Psi$.

It remains to show that β is long if t is not short. So suppose that Φ has two distinct roots length, $t =$ long and β is a short. The there exists $\delta \in Phi^+_{\text{long}}$ with $(\delta, \beta) < 0$. Put then $-{<}\alpha, \beta{>} \geq 2$ and so $(\omega_\beta(\delta), \lambda) = (\delta, \lambda) - {<}\alpha, \beta{>} \geq 2$, a contradiction.

(c)$\Longrightarrow$ (a): Let $\delta \in \Phi_t^+$ with $(\delta, \lambda) \neq 0$. By (c), $\delta = \gamma + n\alpha$ for some $n \in \mathbb{Z}$ and $\gamma \in \lambda^\perp$. Since $(\delta, \lambda) \geq 0$, $n > 0$. Since α is the highest t- root, the β-coefficent of δ is not larger than the β coefficent of α. Thus $n \leq 1$ and so $n = 1$. Hence $(\delta, \lambda) = (\alpha, \delta)$. It remains to show that there exists $\delta \in \Phi^t$ with $(\delta, \lambda) = 1$. If $\beta \in \Phi_t$ we can choose $\delta = \beta$. So we may assume that $\beta \notin \Phi_t$. The assumptions of (c) imply that $t =$ short. Thus β is long. Let Ψ be the $\mathbb{Q}$ closure of $\Phi_{\text{short}} \cap \lambda^\perp$. Then $\Pi_{\text{short}} \in \Psi$ and all roots in $\lambda^\perp \setminus \Psi$ are perpendicular to Ψ. Since Φ is connected we conclude that β is not perpendicular to Ψ. Thus there exists a $\gamma \in \Phi_{\text{short}} \cap \lambda^perp$ with $(\gamma, \beta) < 0$. Put $\delta = \omega_\beta(\gamma)$. Since β is long, $\delta = \gamma + \beta$. Thus $(\delta, \lambda) = 1$ and we are done.

(b)$\Longleftrightarrow$ (d): Follows from a glance at the highest t- root of Φ (**??**).

(a) $\Longrightarrow$ (e): Suppose that μ is a dominant weight with $\mu \prec \lambda$ and $\mu \in \lambda + \mathbb{Z}\Phi_t^*$. Put $\delta = \lambda - \mu$. Then $\delta \in \mathbb{N}\Phi^* \cap \mathbb{Z}\Phi_t^*$. In particular $(\alpha, \delta) \geq 0$. Since $(\alpha, \lambda) = 1$ we conclude that $(\alpha, \mu) = 1$ and $(\alpha, \delta) = 0$. Hence for all $\phi \in \Phi_t^+$ we have $(\phi, \mu) \in \{0, 1\}$. It follows that $|(\phi, \delta)| \leq 1$. Therefore there exists $w \in W(\Phi)$ such that $\rho := \delta^\phi$ is an dominant integral weight with $(\alpha, \rho) = 1$. Also $\rho \in \mathbb{Z}\Phi_t^*$. Using (d) we can express the restriction of ρ to $\mathbb{Z}\Phi_t$ as rational linear combination of a basis for Φ_t^*. Since not all the coefficents are integers we obtain a contradiction. **Comment:make an explicit list of the quadratic weights as linear combination of Π^*. Or find a better proof**

(e)$\Longrightarrow$ (a): Let λ be a dominant weight such that λ is minimal under the dominant weights in $\lambda + \mathbb{Z}\Phi_t^*$. We will show that $(\alpha, \lambda) \leq 1$ and that λ is unique in $\lambda + \mathbb{Z}\Phi_t^*$.

Consider first the case where all roots in Φ have the same length.

Suppose that $(\alpha, \lambda) \geq 2$ and choose $\delta \in \Phi_t = \Phi$ of minimal height with respect to $(\delta, \lambda) \geq 2$. By minimality of λ, $\lambda - \delta^*$ is not dominant and so there exists $\beta \in \Pi$ such that $(\beta, \lambda - \delta^*) < 0$. Thus $(\beta, \lambda) < (\beta, \delta^*)$. Since β and δ^* have equal length we conclude that $(\beta, \delta^*) + 1$ and $(\beta, \lambda) = 0$. Thus $\delta - \beta$ is a root and $(\delta - \beta, \lambda) = (\delta, \lambda) \geq 2$, contradicting the minimal height of δ.

Hence $(\alpha, \lambda) \leq 1$.

Suppose next that $\mu \in \lambda + \mathbb{Z}\Phi^*$ is also minimal with respect to being dominant. Then also $(\alpha, \mu) \leq 1$. Put $\delta = \lambda - \mu$. Then $-1 \leq (\phi, \delta) \leq 1$ for all $\phi \in \Phi^=$ and so ϕ is a quadratic weight. Since $\delta \in \mathbb{Z}\Phi^*$ we conclude from the " (a) $\Longrightarrow$ (e):" step that $\delta = 0$. Thus $\lambda = \mu$ and the one root length case is completed.

Now consider the case where Φ has roots of two different lengths. Let $\{r, t\} = \{\text{long}, \text{short}\}$. Put $\Sigma = \bigcup \Pi_t^{W(\Pi_r)}$. Then Σ is a basis for Φ_t. and Σ is invariant under $W(\Pi_r))$. Note that $W(\Phi_t))$ acts trivial on $\Lambda(\Phi)/\mathbb{Z}\Phi_t^*$ and $W(\Phi) = W(\Phi_t)W(\Pi_r))$. So $\lambda^{W(\Phi)} + \mathbb{Z}\Phi_t^* = \lambda^{W(\Pi_r)} + \mathbb{Z}\Phi_t^*$. For $\mu \in \Lambda(\Phi)$ let $\overline{\mu}$ the restriction of μ to $\mathbb{Z}\Phi_\tau$. Then $\bar{l}$ is a minimal dominant integral weight in $\bar{l} + \mathbb{Z}\overline{\Phi_t^*}$. Thus by the one root length case $(\alpha, \lambda) = 1$. Let μ be any minimal dominant weight in $\lambda^{W(\Phi)} + \mathbb{Z}\Phi_t^*$ and pick $w \in W(\Pi_r)$ with $\mu \in \lambda^w + \mathbb{Z}\Phi_t^*$. Since Σ is invariant under w, $\overline{l}^w$ and $\overline{\mu}$ are minimal dominant weights in $\overline{\mu} + \mathbb{Z}\overline{\Phi}_t^*$. Thus by the one root length case, $\overline{\mu} = \overline{l}^w$. Thus $\mu - \lambda^w \in \Phi_t^\perp$ and so $\mu = \lambda^w$. Since every $W(\Phi)$ orbit on $\Lambda(\Phi)$ contains a unique dominant weight we conclude that $\mu = \lambda$. □

5.4 Subdiagrams

Definition 5.4.1 [**def:diagram**] *Let $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ be a tuple of roots. Then the diagram of $\underline{\alpha}$ is the matrix $(<\alpha_i, \alpha_j>)$. If Φ is a connected root system and $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ is basis for Φ in the standard order, then the diagram of $\underline{\alpha}$ is called an Φ-diagram.*

Note that the Φ-diagram is just the Cartan matrix of Φ.

Lemma 5.4.2 [**conjugation to pi**] *Let Φ be a root system with simple roots Π and λ a dominant integral weight for Φ. Let $\phi \in \Phi$ with $\lambda(\phi) = 1$. Let $\omega \in W_{\Phi\cap\lambda^\perp}$ with $\operatorname{ht}\phi^\omega$ minimal. Then there exist $\beta_1, \beta_2, \ldots, \beta_k \in \Pi$ such that*

(a) [**a**] $\phi^\omega = \beta_1 + \beta_2 + \ldots + \beta_k$.

(b) [**b**] *If $k > 1$ then $(\beta_1, \beta_2, \ldots, \beta_k)$ has B_k or G_2 diagram.*

(c) [**c**] $\lambda(\beta_1) = 1$ *and* $\lambda(\beta_i) = 0$ *for* $2 \le i \le k$.

Proof: Put $\Psi = \Phi \cap \lambda^\perp$ and $\alpha := \phi^\omega$. If $\alpha \in \Pi$, then the lemma holds with $k = 1$ and $\beta_1 = \alpha$. So suppose that $\alpha \notin \Phi$. Let β and γ be as in 5.2.7 and put $m = (\alpha, \beta^*)$. Then $\alpha = m\beta + \gamma$. Suppose that $\lambda(\beta) = 0$. Then $\omega_\beta \in W_\Psi$ and $\gamma = \omega_\beta(\alpha)$ has smaller height than α, a contradiction to the choice of α. Thus $\lambda(\beta) \neq 0$. Since λ is dominant integral and $\lambda(\alpha) = 1$ we conclude that $m = 1$, $\lambda(\beta) = 1$ and $\lambda(\gamma) = 0$. Since $m = 1$, $(\alpha, \alpha) \le (\beta, \beta)$ and $\alpha = \beta + \gamma$.

Suppose that $(\alpha, \alpha) = (\beta, \beta)$. Then $\omega_\gamma(\alpha) = \beta$ and β has smaller height than α, contradiction the choice of α.

Suppose that $2(\alpha, \alpha) = (\beta, \beta)$. Since $\beta \in \Pi \setminus \Psi$, β^* is a dominant integral weight on Ψ. Moreover by 5.2.8, $\Pi \cap \Psi$ is basis for Ψ. Also $(\gamma, \beta^*) = m = 1$. Let $w \in W_{\Psi\cap\beta^\perp}$. Then $w \in W_\Psi$ and $\alpha^w = \beta + \gamma^w$. Thus the choice of α implies that $\operatorname{ht}(\gamma) \le \operatorname{ht}(\gamma^w)$. So by induction on Π there exists $b_2, \ldots, b_k \in \Pi \cap \Psi$ such that

- [**e**] $\gamma = \beta_2 + \ldots + \beta_k$.
- [**f**] $(\beta_2, \beta_2, \ldots, \beta_k)$ has B_{k-1} or G_2 diagram.
- [**g**] $(\beta_2, \beta) = 1$ and $(\beta_i, \beta) = 0$ for $3 \le i \le k$

Since no connected component of Φhas roots of three different lengths, $(\beta_2, \ldots, \beta_k)$ cannot have G_2-diagram. Put $\beta_1 = \beta$. Then clearly (a) and (c) holds. If $k \leq 3$, then both β_1 and β_2 are long and so $(\beta_1, \ldots, \beta_k)$ has B_k-diagram. If $k = 2$, then $\beta_2 = \gamma$ is short and (β_1, β_2) has B_2-diagram. Thus in any case (b) holds.

Suppose finally that $3(\alpha, \alpha) = (\beta, \beta)$. Then Φ is of type G_2 and $\Pi = \{\beta, \gamma\}$. Thus the lemma holds with $\beta_1 = \beta$ and $\beta_2 = \gamma$. □

Lemma 5.4.3 [**an strings**] *Let Φ be a connected root system and $(\alpha_0, \alpha_1, \ldots, \alpha_k)$ an ordered tuple of roots in Φ with diagram X_{k+1} where $\mathrm{X} \in \{\mathrm{A}, \mathrm{B}, \mathrm{G}\}$. Suppose that α_0 is long. Then there exists an integer $m \geq k$, roots $\beta_0, \beta_1, \ldots, \beta_m$ in Φ and $w \in W(\Phi)$ such that*

(a) [**z**] $\alpha_i^w = \beta_i$ *for all* $0 \leq i < k$ *and* $a_k^w = \beta_k + \ldots + \beta_m$.

(b) [**a**] $\beta_0 = -\alpha_{\mathrm{long}}$.

(c) [**b**] $\beta_i \in \Pi$ *for all* $1 \leq i \leq m$.

(d) [**e**] *One of the following holds;*

1. [**a**] $\mathrm{X} = \mathrm{A}$, $k = m$, $a_k^w = b_k$ *and* $(\beta_0, \beta_1, \ldots, \beta_k)$ *has diagram* A_{k+1}.
2. [**b**] $X \neq A$ *and* $(\beta_0, \beta_1, \ldots, \beta_m)$ *has diagram* X_{m+1}.

(e) [**c**] *Put* $\Psi_i = (\Phi \cap \alpha_0^\perp \cap \ldots \cap \alpha_i^\perp)^w$. *Then for all* $0 \leq i \leq k$, $\Psi_i \cap \Pi$ *is a system of simple roots for* Ψ_i.

Proof: By induction on k. Suppose first that $k = 0$. Since $\mathbb{A}_o$ is long and Φ is connected $\alpha_0^w = -\alpha_{\mathrm{long}}$ for some $w \in W$. Put $m = 0$ and $\beta_0 = -\alpha_{\mathrm{long}}$. Then clearly (b) to (d) holds. Note also that α_{long}^* induces a dominant integral weight on Π and so (e) follows from 5.2.8.

Suppose now that $k \leq 1$ and that the statement has been proved for $k - 1$. Since $(\alpha_0, \ldots, a_{k-1})$ has A_k diagram we conclude that exists $v \in W_\Phi$ and $\beta_0, \ldots, \beta_{k-1}$ in Φ such that $\alpha_i^v = \beta_i$ for all $0 \leq i < k$, $\beta_0 = -\alpha_{\mathrm{long}}$ and (e) holds for all $i < k$. Put $\Psi = \Psi_{k-2}$ if $k \geq 2$ and $\Psi = \Phi$ if $k = 1$. Also put $\alpha = a_k^v$ and $\beta = \beta_{k-1}$. Note that $\beta \notin \Psi$ and $\phi \in \Psi$. Also since (e) holds for $k - 2$, $\Pi \cap \Psi$ is a system of simple roots for Ψ. Thus $-\beta^*$ induces a dominant integral weight λ on Ψ. Note also that $\lambda(\alpha) = (\phi, -\beta^*) = -(\alpha_{k-1}, \alpha_k) = 1$.

Thus by 5.4.2 there exists $\omega \in W_{\Psi \cap \lambda^\perp}$ and $\beta_k, \ldots, \beta_m \in \Psi$ such that

1° [**1**]

(a) [**1:a**] $\alpha^\omega = \beta_k + \ldots + \beta_m$.

(b) [**1:b**] $(\beta_k, \ldots, \beta_m)$ *has* B_{m-k} *or* G_{m-k} *diagram.*

(c) [**1:c**] $\lambda(\beta_k) = 1$ *and* $\lambda(\beta_i)$ *for* $k \leq i \leq m$.

Note that ω fixes $\beta_0, \beta_1, \ldots b_{k-1}$. Put $w = v\omega$. Then (a) to (c) holds. Also since (e) holds for $i = k-1$, $\Psi_{k-1} \cap \Pi$ is a system of simple roots for Ψ_{k-1}.

Suppose that $k = m$. Then $b_\kappa = a_k^w$ and so (d) holds. Also $-\beta_k^*$ induces a dominant integral weight on $\Psi_{k-1} \cap \Pi$. Also $\Psi_k = \Psi_{k-1} \cap b_k^\perp$ we conclude from 5.2.8 that (e) holds.

Suppose next that $k \neq m$. Then α is not long and so $X \neq A$. Let Y be the diagram type of $(\beta_k, \ldots, \beta_m)$. From $(1°)$(a) we conclude that Y = B or Y = G. Thus $(1°)$(c) implies that (d) holds. Put $\delta = \alpha_k^w = \alpha^\omega$. Then $\Psi_k = \Psi_{k-1} \cap \delta^\perp$. From $(1°)$(a) we conclude that $-\delta^*$ is a dominant integral weight on $\Psi_{k-1} \cap \Pi \setminus \{\beta_k, \ldots, \beta_m\}$.

Suppose Y = B. Then δ is perpendicular to $b_{k+1}, \ldots, b_m$. Now $b_\kappa \notin \Psi_k$ and thus $-\delta^*$ is a dominant integral weight on Ψ_k. Thus (e) follows from 5.2.8.

Suppose Y = G. Then X = G, $\Psi = \Phi$, $k = 1$ and α_0, α_1 generate Φ. Hence $\Psi_k = \emptyset$ and again (e) holds. $\square$

Chapter 6

Same Characteristic Representations

This chapter is devoted to $\mathbb{K}G(\mathbb{F})$ modules, where $\mathbb{K}$ and $\mathbb{F}$ are fields in the same characteristic and $G(\mathbb{F})$ is a group of Lie type over a field $\mathbb{K}$.

6.1 Lie Algebras

Let Φ be a root system. We continue to use the notation introduced in 5.

Definition 6.1.1 [**chevalley basis**] *Let $\mathbb{K}$ be a field and $\mathfrak{g}$ a Lie-algebra over $\mathbb{K}$. A* Chevalley basis *for $\mathfrak{g}$ is a basis*

$$(\mathfrak{G}_\alpha, \alpha \in \Phi; \mathfrak{H}_\gamma, \gamma \in \Pi^*)$$

such that for all $\alpha, \beta \in \Phi$, $\gamma, \delta \in \Pi^*$:

(a) [**CB1**] $[\mathfrak{H}_\gamma, \mathfrak{H}_\delta] = 0$.

(b) [**CB2**] $[\mathfrak{H}_\gamma, \mathfrak{G}_\alpha] = (\alpha, \gamma)\mathfrak{G}_\alpha$

(c) [**CB3**] $[\mathfrak{G}_\alpha, \mathfrak{G}_{-\alpha}] = \mathfrak{H}_{\alpha^*}$
where $\mathfrak{H}_\rho$ for $\rho = \sum_{\gamma\in\Pi^*} m_\gamma \gamma \in \Phi^*$ is define by $\mathfrak{H}_\rho := \sum_{\gamma\in\Pi^*} m_\gamma \mathfrak{H}_\gamma$.

(d) [**CB4**] $[\mathfrak{G}_\alpha, \mathfrak{G}_\beta] = \pm(r_{\alpha\beta} + 1)\mathfrak{G}_{\alpha+\beta}$ *if* $\alpha + \beta \in \Phi$.

(e) [**CB5**] $[\mathfrak{G}_\alpha, \mathfrak{G}_\beta] = 0$ *if* $0 \neq \alpha + \beta \notin \Phi$.

Lemma 6.1.2 [**nilpotent action for lie algebras**] *Let $\mathfrak{g}$ be a Lie algebra over $\mathbb{K}$ and V be a finite dimensional $\mathfrak{g}$-module.*

(a) [**a**] *Then there exists unique maximal ideal $\mathfrak{u}_v(\mathfrak{g})$ which acts nilpotently on V.*

(b) [**b**] *Let $\mathfrak{d}$ be an ideal in $\mathfrak{g}$, X a $\mathfrak{d}$-submodule of V and $\mathfrak{G} \in \mathfrak{g}$.*

(a) [**a**] *Define* $T : X \to V/X, x \to \mathfrak{G}x + X$. *Then* T *is a* $\mathfrak{d}$*-equivariant. In particular* $\mathfrak{G}X + X$ *is a* $\mathfrak{d}$*-submodule of* V.

(b) [**b**] *If* V *is irreducible for* $\mathfrak{g}$ *then all composition factors for* $\mathfrak{d}$ *on* V *are isomorphic.*

(c) [**c**] *If* X *is irreducible for* $\mathfrak{d}$ *and* $\mathfrak{G}X \not\leq X$ *then* $\mathfrak{G}X \cap X = 0$ *and* $\mathrm{Ann}_X(\mathfrak{G}) = 0$.

Proof: (a) $\mathfrak{u}_V(\mathfrak{g})$ is just the intersection of the annhilators of the composition factors of $\mathfrak{g}$ on V.

(b) Let $\mathfrak{D} \in \mathfrak{d}$ and $x \in X$. Then $[\mathfrak{G}, \mathfrak{D}]x \in \mathfrak{d}x \leq X$ and so

$$T(\mathfrak{D}x) = \mathfrak{G}\mathfrak{D}x + X = (\mathfrak{D}\mathfrak{G} + [\mathfrak{G}, \mathfrak{D}])x + X = \mathfrak{D}(\mathfrak{G}x + X) = \mathfrak{D}(T(x))$$

So (b:a) holds.

For (b:b) let Y be a $\mathfrak{d}$-submodule maximal such that all composition factors for $\mathfrak{d}$ on Y are isomorphic. By (b:a) applied to Y, all composition factors of $\mathfrak{d}$ on $\mathfrak{G}Y + Y/Y$ are isomorphic to a composition factor of Y. Hence by maximality of Y, $\mathfrak{G}Y \leq Y$. Since $\mathfrak{G} \in \mathfrak{g}$ was arbitray and $\mathfrak{g}$ acts irreducibly, $V = Y$.

For (b:c) note that the irreducibilty of X and (b:a) imply $\ker T = 0$. □

We remark that under the assumption of part (b:b) of the preceeding lemma, V does not need be completely reducible for $\mathfrak{d}$. For example let $\mathfrak{g} = \mathfrak{sl}_2(\mathbb{K})$ with $\mathrm{char}\,\mathbb{K} = 2$ and V the natural 2-dimensional module. Then $\mathfrak{d} := \mathbb{K}\langle \mathfrak{G}_\alpha, \mathfrak{H}_\alpha \rangle$ is an ideal in $\mathfrak{sl}_2(\mathbb{K})$ and has a unique proper submodule (namely $\mathfrak{G}_\alpha V$). This example also shows that an ideal does not need to act faithfully on its proper submodules.

Lemma 6.1.3 [**X+bX**] *Let* $\mathfrak{g}$ *be a Lie algebra,* $\mathfrak{a}$ *and* $\mathfrak{b}$ *subspaces of* $\mathfrak{g}$ *with* $\mathfrak{g} = \mathfrak{a} + \mathfrak{b}$. *Let* X *be an* $\mathfrak{a}$ *invariant subspace of* V.

(a) [**a**] *For all* $n \in \mathbb{N}$, $\sum_{i=0}^{n} \mathfrak{b}^i X$ *is* $\mathfrak{a}$*-invariant.*

(b) [**b**] $\sum_{i=0}^{\infty} \mathfrak{b}^i X$ *is* $\mathfrak{g}$*-invariant.*

(c) [**c**] *If* $X \neq 0$ *and* V *is irreducible as* $\mathfrak{g}$*-module, then* $V = \sum_{i=0}^{\infty} \mathfrak{b}^i X$.

Proof: (a) By induction on i it suffices to show that $X + \mathfrak{b}X$ is $\mathfrak{a}$ invariant. Note that $\mathfrak{g}X = (\mathfrak{a} + \mathfrak{b})X \leq X + \mathfrak{b}X$. Let $\mathfrak{A} \in \mathfrak{a}$ and $\mathfrak{B} \in \mathfrak{b}$. Then

$$(\mathfrak{A}\mathfrak{B})X = (\mathfrak{B}\mathfrak{A} + [\mathfrak{A}, \mathfrak{B}])X \leq \mathfrak{B}(\mathfrak{A}X) + \mathfrak{g}X \leq X + \mathfrak{b}X.$$

So (a) holds.

(b) By (a)

$$\sum_{i=0}^{\infty} \mathfrak{b}^i X = \bigcup_{n=1}^{\infty} (\sum_{i=0}^{n} \mathfrak{b}^i X)$$

is $\mathfrak{a}$ invariant. Clearly it is also $\mathfrak{b}$ invariant and so (b) follows from $\mathfrak{g} = \mathfrak{a} + \mathfrak{b}$.

(c) Follows from (b). □

Proposition 6.1.4 [**smith's lemma**] *Let $\mathfrak{g}$ be a Lie algebra, $\mathfrak{l}, \mathfrak{q}_+$ and $\mathfrak{q}_-$ sub algebras and V an irreducible $\mathfrak{g}$ module. Suppose that*

(a) [**i**] $\mathfrak{g} = \mathfrak{q}_+ + \mathfrak{l} + \mathfrak{q}_-$

(b) [**ii**] $[\mathfrak{l}, \mathfrak{q}_+] \leq \mathfrak{q}_+$ *and* $[\mathfrak{l}, \mathfrak{q}_-] \leq \mathfrak{q}_-$.

(c) [**iii**] $\mathfrak{q}_+$ *and* $\mathfrak{q}_-$ *both act nilpotently on* V.

Then

(a) [**a**] $\mathfrak{l}$ *acts irreducible on* $\mathrm{Ann}_V(q_+)$.

(b) [**b**] $V = \mathrm{Ann}_V(\mathfrak{q}_+) \oplus \mathrm{Ann}^*_V(\mathfrak{q}_-)$, *where* $\mathrm{Ann}^*_V(\mathfrak{q}_-)$ *is smallest* q_- *submodule of* V *containing* $\mathfrak{q}_-V$.

(c) [**c**] $V = \sum_{i=0}^{\infty} \mathfrak{q}_-^i \mathrm{Ann}_V(\mathfrak{q}_+)$.

Proof: Since $\mathfrak{q}_+$ acts nilpotently on V, $\mathrm{Ann}_V(\mathfrak{q}_+) \neq 0$. By (ii) $\mathrm{Ann}_V(\mathfrak{q}_+)$ is an $\mathfrak{l}$ submodule. Let X be a non-zero $\mathfrak{l}$-submodule of $\mathrm{Ann}_V(\mathfrak{q}_+)$ and $Y = \sum_{i=1}^{\infty} \mathfrak{q}_-^i X$. Then X is an $\mathfrak{q}_+ + \mathfrak{l}$ submodule of $\mathrm{Ann}_V(\mathfrak{q}_+)$ and $Y \leq \mathrm{Ann}^*_V(\mathfrak{q}_-)$. By 6.1.3,

(*) $\quad V = X + Y$

Suppose that $\tilde{X} := \mathrm{Ann}_V(\mathfrak{q}_+) \cap \mathrm{Ann}^*_V(\mathfrak{q}_-) \neq 0$. Since $\tilde{X}$ is $\mathfrak{l}$ invariant, (*) applied to X yields $V = \tilde{X} + \mathrm{Ann}^*_V(\mathfrak{q}_-) \leq \mathrm{Ann}^*_V(\mathfrak{q}_-)$. Since $\mathfrak{q}_-$ acts nilpotently this implies $\mathrm{Ann}^*_V(\mathfrak{q}_-)) = 0$, a contradiction to $\tilde{X} \neq 0$.

Thus $\tilde{X} = 0$. Hence also $\mathrm{Ann}_V(\mathfrak{q}_+) \cap Y = 0$ and so using (*)

$$\mathrm{Ann}_V(\mathfrak{q}_+) = X + (\mathrm{Ann}_V(\mathfrak{q}^+) \cap Y) = X$$

Since X was an arbitray $\mathfrak{l}$ submodule of $\mathrm{Ann}_V(\mathfrak{q}_+)$ the lemma is proved. $\square$

Lemma 6.1.5 [**q- quadratic**] *Let $\mathfrak{g}$ be a Lie algebra, $\mathfrak{l}, \mathfrak{q}_+$ and $\mathfrak{q}_-$ subalgebras and V an irreducible $\mathfrak{g}$-module. Suppose that*

(a) [**i**] $\mathfrak{g} = \mathfrak{q}_+ + \mathfrak{l} + \mathfrak{q}_+$

(b) [**ii**] $[\mathfrak{l}, \mathfrak{q}_+] \leq \mathfrak{q}_+$ *and* $[\mathfrak{l}, \mathfrak{q}_-] \leq \mathfrak{q}_-$.

(c) [**iii**] $\mathfrak{q}_-^2 V = 0$ *and* $\mathfrak{q}_- V \neq 0$.

(d) [**iv**] $\mathfrak{q}^+$ *acts nilpotently on* V.

Then

(a) [**a**] $V = \mathrm{Ann}_V(\mathfrak{q}_+) \oplus \mathrm{Ann}_V(\mathfrak{q}_-)$.

(b) [**b**] $\mathfrak{l}$ *acts irreducibly on both* $\mathrm{Ann}_V(\mathfrak{q}_+)$ *and* $\mathrm{Ann}_V(\mathfrak{q}_-)$.

(c) [**c**] $\mathfrak{q}_+^2 V = 0$ *and* $\mathfrak{q}_+ V \neq 0$.

(d) [**d**] $\mathrm{Ann}_V(\mathfrak{q}_+) = \mathfrak{q}_+ V$ *and* $\mathrm{Ann}_V(\mathfrak{q}_-) = \mathfrak{q}_- V$.

Proof: Note that $\mathfrak{q}_- V \leq \mathrm{Ann}_V(\mathfrak{q}^-)$. By 6.1.4(a) (applied with the roles of $+$ and $-$ interchanged, $\mathrm{Ann}_V(\mathfrak{q}_-)$ is an irreducible $\mathfrak{l}$ module. Thus

$$\mathfrak{q}_- V = \mathrm{Ann}_V(\mathfrak{q}_-) = \mathrm{Ann}^*_V(\mathfrak{q}_-)$$

Thus by 6.1.4(b) implies that (a) holds. In particular $\mathfrak{q}_+ + \mathfrak{l}$ acts irreducibly on $V/\mathrm{Ann}_V(\mathfrak{q}_+))$. Hence $\mathfrak{q}_+$ annhilates $V/\mathrm{Ann}(\mathfrak{q}_+)$ and the remaiing parts of the lemma are readily verified. □

Comment:The preceeding lemma could be also used to in some later places to avoid the use of the graph automorphism for A_n

Definition 6.1.6 [**root faithful**] *Let V be a $\mathfrak{g}_\Phi(K)$-module. We say that $\mathfrak{g}_\Phi(K)$ acts* root faithful *on V if $\mathfrak{G}_\alpha V \neq 0$ for all $\alpha \in \Phi$.*

Lemma 6.1.7 [**ideal**] *Let $\lambda \neq 0$ be a p-restricted dominant weight and Φ a connected root system with basis Π, $\mathfrak{g}_\Phi(\mathbb{K})$ the Lie algebra of type Φ over $\mathbb{K}$ and V a $\mathfrak{g}_\Phi(\mathbb{K})$-module of highest weight λ. Let $\alpha \in \Phi$ and suppose that $\mathfrak{G}_\alpha V = 0$. Then the following holds.*

(a) [**a**] *Φ has two different root lengths and α is short.*

(b) [**b**] $(\lambda, \beta^*) = 0$, *for all short roots* $\beta \in \Pi$.

(c) [**c**] $\mathrm{char}\,\mathbb{K} = p_\Phi$.

6.2 Groups of Lie Type and Irreducible Rational Representations

Let Φ be a connected root system, $\mathbb{K}$ a field, $\mathbb{E}$ the algebraic closure of $\mathbb{K}$ and $G_\Phi(K)$ the corresponding universal group of Lie type. Then $G_\Phi(K)$ is generated by elements $\chi_\alpha(t), \alpha \in \Phi, t \in \mathbb{K}$ fulfilling the Steinberg Relations: For $t \in \mathbb{K}^\#$ define $\omega_\alpha(t) = \chi_\alpha(t)\chi_\alpha(t^{-1})\chi_\alpha(t)$ and $h_\alpha(t) := \omega_\alpha(t)\omega_\alpha(1)^{-1}$.

(a) [**St1**] $\chi_\alpha(t)\chi_\alpha(s) = \chi_\alpha(t+s)$

(b) [**St2**] $h_\alpha(u)h_\alpha(v) = h_\alpha(uv)$

(c) [**St3**] If $\alpha^* = \sum_{i=1}^n n_i\beta_i^*$ for some $n_i \in \mathbb{Z}, \beta_i \in \Phi$ then $h_\alpha(u) = \prod_{i=1}^n h_{\beta_i}(u^{n_i})$.

(d) [**St4**] $h_\alpha(u)\chi_\beta(t)h_\alpha(u)^{-1} = \chi_\alpha(u^{(\beta,\alpha^*)}t)$

(e) [**ST5**] $\omega_\alpha(1)\chi_\beta(t)\omega_\alpha(1)^{-1} = \chi_{\omega_\alpha(\beta)}(\epsilon_{\alpha\beta}t)$ for some $\epsilon_{\alpha\beta} = \pm 1$.

(f) [**ST6**] If $\alpha+\beta$ is not a root, and $\alpha \neq -\beta$ then $[\chi_\alpha(t), \chi_\beta(s)] = 1$.

(g) [**ST7**] If $\alpha+\beta$ is a root then

$$[\chi_\alpha(t), \chi_\beta(s)] = \chi_{\alpha+\beta}(N_{\alpha\beta}ts) \prod_{i,j>1} \chi_{i\alpha+j\beta}(C_{\alpha\beta ij}t^i s^j)$$

Let $H_\alpha = \{h_\alpha(u) \mid u \in \mathbb{K}^\#\}$, $X_\alpha = \{\chi_\alpha(t) \mid t \in \mathbb{K}^\#\}$, $U = \prod_{\alpha\in\Phi^+} X_\alpha$, $H = \prod_{\alpha\in\mathcal{P}} H_\alpha$ and $B = HU$.

Let V be a finite dimensional rational $\mathbb{E}G_\Phi(\mathbb{E})$ module. For $g \in G_\Phi(\mathbb{E})$ denote by g^V the image of $g \in \mathrm{End}_{\mathbb{E}}(V)$. Slighty abusing notation we will often just write g for g^V. Since V is rational and finite dimensional we have

$$\chi_\alpha(t) = \sum_{i=0}^{d_\alpha} t^i \mathfrak{G}_{\alpha,i}$$

for some $d_\alpha \in \mathbb{N}$ and some $\mathfrak{G}_{\alpha,i} \in \mathrm{End}_{\mathbb{E}}(V)$. Note that $\mathfrak{G}_{\alpha,0} = \chi_\alpha(0) = 1$.

(We remark that, if V is obtained from a module in characteristic zero via an admissible lattice and taking tensor products, then $\mathfrak{G}_{\alpha,i} = (\frac{1}{i!}\mathfrak{G}_\alpha^i) \otimes 1$.)

Comment:It might be interesting to figure out what (ST1) means for the $\mathfrak{G}_{\alpha,i}$

Since $\mathbb{E}$ is infinite (and so $|E| > d_\alpha$) it is easy to see that the subalgebra of $\mathrm{End}_{\mathbb{E}}(V)$ generated by X_α contains all of the $\mathfrak{G}_{\alpha,i}$. Let $\mathfrak{G}_\alpha^V = \mathfrak{G}_{\alpha,1}$ and $\mathfrak{g}^V$ the Lie subalgebra of $\mathfrak{gl}(V)$ generated by the G_α^V. Let A^V be the subalgebra of $\mathrm{End}_{\mathbb{E}}(V)$ generated by all the $\mathfrak{G}_{\alpha,i}$ (As usual we will ommit the superscript V). Then every $G_\Phi(\mathbb{E})$ submodule of V is also an $\mathfrak{g}$ submodule and $\mathfrak{G}_\Phi(E)$ and A have the same submodules. **Comment: Maybe One should define $\mathfrak{H}_\alpha^V$ and verify the remaining relation for the Lie algebra**)).

¿From (ST6)

$$[\mathfrak{G}_\alpha, \mathfrak{G}_\beta] = 0$$

if $\alpha+\beta$ is not a root and from (ST7)

$$[\mathfrak{G}_\alpha, \mathfrak{G}_\beta] = N_{\alpha\beta}\mathfrak{G}_{\alpha+\beta}$$

if $\alpha+\beta$ is a root. By (ST4)

$$h_\alpha(u)\mathfrak{G}_{\beta,i}h_\alpha(u)^{-1} = u^{i(\alpha^*,\beta)}\mathfrak{G}_\beta$$

Let $\mu \in \Lambda$ and $v \in V$. We say that v is a weight vector for μ if

$$h_\alpha(u)v = u^{(\alpha^*,\mu)}v$$

for all $u \in \mathbb{K}^\#$ and $\alpha \in \Phi$. Since $\mathbb{E}$ is infinite and every polynomial as at most finitely many roots, two weights with a common non zero weight vector are equal. Let V_μ be the set of all weight vectors for μ.

Lemma 6.2.1 [Gb Vmu] *Let $\beta \in \Phi$, $i \in \mathbb{N}$ and $\mu \in \Lambda(\Phi^*)$ and $v \in V_\mu$*

(a) [**a**] $\mathfrak{G}_{\beta,i} V_\mu \leq V_{\mu+i\beta}$.

(b) [**b**] $\mathfrak{H}_\beta v = (\beta, \mu) v$.

Proof: (a): Let $\alpha \in \Phi$ and $u \in \mathbb{K}^\sharp$. Then

$$h_\alpha(u)\mathfrak{G}_{\beta,i} v = u^{i(\alpha^*,\beta)}\mathfrak{G}_{\beta,i} h_\alpha(u) v = u^{i(\alpha^*,\beta)}\mathfrak{G}_{\beta,i} u^{(\alpha^*,\mu)} v = u^{(\alpha^*,\mu+i\beta)}\mathfrak{G}_{\beta,i} v$$

(b) ???????? □

Since the different weight spaces are linear independent (that is the sum of the weight spaces is a direct sum) for a weight vector v that X_α fixes v if and only if $\mathfrak{G}_{\alpha,i} v = 0$ for all $1 \leq i \leq \infty$.

A weight vector is called a highest weight vector if $uv = v$ for all $u \in U$. In the view of the preceeding this means $\mathfrak{G}_{\alpha,i} v = 0$ for all $\alpha \in \Phi^+$. If V is irreducible there exists a non-zero weight vector. Indeed, since U acts unipotenly **Comment:why?** $C_V(U) \neq 0$. Since H is abelian and $\mathbb{E}$ is algebraicly closed, there exists a one dimensional $\mathbb{E}H$ submodule $\mathbb{K}v$ in $C_V(U)$. Since V is rational it is easy to see that v is a weight vector for some weight $\lambda \in \Lambda$. Now $V = Av$ and so $(**)$ implies that V is the direct sum of its weight spaces.

A way to obtain the group $G_\Phi(\mathbb{K})$ is to start with a faithful representation

$$\pi : \mathfrak{g}_\Phi(\mathbb{C}) \to gl(V)$$

of the Lie algebra $\mathfrak{g}_\Phi(C)$ and to identify the complex vector space V with $\mathbb{C}^n$ via the admissable $\mathbb{Z}$-lattice Λ (in fact, Λ consists of all the weights of all the rational representations of $\mathfrak{g}_\Phi(\mathbb{C})$). Then

$$G_\Phi(\mathbb{K}) = \langle x_a(t) \mid t \in \mathbb{K} \rangle.$$

We obtain the quotients of $G_\Phi(\mathbb{K})$ by following the same procedure but replacing Λ by any admissable $\mathbb{Z}$-lattice. Then $G_\Phi(\mathbb{K})$ is the group of rational points of the algebraic group $G = G_\Phi(\mathbb{E})$. There is a well know method to relate a Lie-algebra $L(G)$ to an algebraic group G:
see for instance Humphreys. According to Borel [Bo, 3.3] the Lie algebras $L(G_\Phi(\mathbb{E}))$ and $\mathfrak{g}_\Phi \otimes_\mathbb{Z} \mathbb{E} = \mathfrak{g}_\Phi(\mathbb{E})$ are isomorphic as well as the Lie algebras $L(G_\Phi(\mathbb{K})) = L(G_\Phi)(\mathbb{K})$ and $\mathfrak{g}_\Phi \otimes_\mathbb{Z} \mathbb{K} = g_\Phi(\mathbb{K})$.

Let $\pi : G_\Phi(\mathbb{K}) \to GL(W)$ be an irreducible and faithful $\mathbb{F}_p$-representation for $G_\Phi(\mathbb{K})$, where $p = char\mathbb{K}$. Then π induces an irreducible, faithful and rational representation $\pi : G_\Phi(\mathbb{E}) \to GL(V)$ for $G = G_\Phi(\mathbb{E})$ on $V = W \otimes_{End_{\mathbb{F}_p G}(V)} \mathbb{E}$ (rational means that all the weights λ of π are in the lattice Λ) and the differential $d\pi$ defines a representation

$$d\pi : L(G) \to gl(V)$$

of the to G related Lie algebra $\mathfrak{g} \cong L(g)$.

Definition 6.2.2 [**L**]*et λ be the highest weight of π. We say that π is p-restricted, if $\lambda = \sum c_i\lambda_i$ with $0 \leq c_i < p$.*

According to [Bo, 6.4] the following holds.

Theorem 6.2.3 (Curtis, Borel) *If π is a p-restricted irreducible representation of G, then $d\pi$ is an irreducible representation of $\mathfrak{g}$.*

If V is an irreducible $\mathbb{F}_p$-module for ${}^2G_\Phi(\mathbb{K})$, then V is an irreducible $\mathbb{F}_p$-module for $G_\Phi(\mathbb{K})$, as well, and therefore the following fact holds.

Theorem 6.2.4 [**trans**] *If $V(\lambda)$ is a p-restricted irreducible $\mathbb{F}_p{}^\sigma G_\Phi(\mathbb{K})$-module, then $V(\lambda)\otimes_{End_{\mathbb{F}_pG}(V)}$ $\mathbb{E}$ is an irreducible module for $\mathfrak{g}_\Phi(\mathbb{E})$.*

Later we will need some more information about the elements of a unipotent subgroup U^1 of ${}^2F_4(K)$. Here we follow the description given in the book of Carter [Ca, 13.6].

Lemma 6.2.5 [**system F4**] *Let Φ be a root system of type F_4 and $\Pi = \{\alpha, \beta, \gamma, \delta\}$ a fundamental system of Φ where α, β are long and γ, δ short and where α and δ are perdendicular. Let τ be a mapping of $V_\Phi(\mathbb{K})$ into $V_\Phi(\mathbb{K})$ defined by*

$$\tau(r) = f(r)\sigma(r), \text{ where}$$

r is a root and $\sigma(r)$ the permutation of Φ induced by the graph automorphism and

$$f(r) = \sqrt{\frac{1}{2}} \text{ if } r \text{ is short and } f(r) = \sqrt{2} \text{ if } r \text{ is long.}$$

Then τ is an isometrie of $V_\Phi(\mathbb{K})$. Let W be the related Weyl group (the group generated by the reflections on the hyperplanes perpendicular to the roots) and let $W^1 = C_W(\tau)$. Then

$$W^1 = \langle w_\alpha w_\delta, (w_\beta w_\gamma)^2\rangle \cong D_{16},$$

where for r a root, w_r is the reflection on the hyperplane perpendicular to r. The orbits of W^1 on Φ^+ partition Φ^+. These orbits are

$$S_1 = \{\alpha, \delta\},$$

$$S_2 = \{\alpha + 2\beta + 2\gamma, \beta + 2\gamma + \delta\},$$
$$S_3 = \{\alpha + 2\beta + 2\gamma + 2\delta, \alpha + \beta + 2\gamma + \delta\},$$
$$S_4 = \{a + 2\beta + 4\gamma + 2\delta, \alpha + 2\beta + 2\gamma + \delta\},$$
$$S_5 = \{\beta, \gamma, \beta + \gamma, \beta + 2\gamma\},$$
$$S_6 = \{\alpha + \beta, \gamma + \delta, \alpha + \beta + 2\gamma + 2\delta, \alpha + \beta + \gamma + \delta\},$$

$$S_7 = \{\alpha+\beta+2\gamma, \beta+\gamma+\delta, \alpha+2\beta+3\gamma+\delta, \alpha+3\beta+4\gamma+2\delta\},$$
$$S_8 = \{\beta+\gamma+2\delta, \alpha+\beta+\gamma, \alpha+2\beta+3\gamma+2\delta, 2\alpha+3\beta+4\gamma+2\delta\}.$$

Let $S = \{S_i \mid 1 \leq i \leq 8\}$. Notice that these orbits are either of type $A_1 \times A_1$ or B_2. If $S_i = \{r, s\}$ is of type $A_1 \times A_2$ with r long and s short, then define

$$x_{S_i}(t) = x_s(t^\theta)x_r(t),$$

where $t \in \mathbb{K}$ and θ a field automorphism of $\mathbb{K}$. In this case set

$$X_{S_i} = \langle x_{S_i}(t) \mid t \in \mathbb{K}\rangle.$$

If S_i is of type B_2 and $\{r, s\}$ is a fundamental system with r long and s short, then define

$$x(t,u) = x_r(t^\theta)x_s(t)x_{r+s}(t^{\theta+1}+u^\theta)x_{2s+r}(u^{2\theta}),$$

where $t, u \in \mathbb{K}$ and θ a field automorphism of $\mathbb{K}$. In this case set

$$X_{S_i} = \langle x(t,u) \mid t, u \in \mathbb{K}\rangle.$$

Then

$$U^1 = \prod_{T\in S} X^1_S.$$

6.3 Translation form the group to the Lie algebra

Comment:This is taking from Tim's file, needs to be adapted

Lemma 6.3.1 [**splitting field**] *Let $K \subseteq k$ be a subfield of k and λ a dominant weight with $\lambda(\alpha) < |K|$, for all $\alpha \in \Sigma$. Then $A(\lambda)$ is irreducible as a $kG(K)$-module.*

Proof: □

Let λ be a dominant p-restricted integral weight and $V = V(\lambda)$ an irreducible $GF(p)G_\Phi(K)$-module with highest weight λ. Then by 6.2.4 $V \otimes E$ is an irreducible module for $\mathfrak{g}_\Phi(E)$ with E the algebraic closure of K.

Order Π in some way and then order the set of weights lexicographically. **Comment: mention positive, by carter we can choose the order to be compatible with the height function**

Definition 6.3.2 [**u+**]

(a) [**a**] $U^+_\alpha = \langle X_\beta \mid \beta \geq \alpha\rangle$

(b) [**b**] $U^-_\alpha = \langle X_\beta \mid \beta > \alpha\rangle$. *Note that $U^+_\alpha = X_\alpha U^-_\alpha$.*

(c) [**c**] *V_μ a weight space (as usual)*

(d) [**d**] $V_\mu^+ = \bigoplus_{\gamma\geq\mu} V_\gamma$

(e) [**e**] $V_\mu^- = \bigoplus_{\gamma>\mu} V_\gamma$

Let P be a subgroup of a unipotent group U of $G_\Phi(K)$ and let

$$\Phi_P = \{\alpha \in \Sigma^+ \mid P \cap U_\alpha^+ \not\leq U_\alpha^-\}.$$

For $\alpha \in \Phi_P$, pick $g_\alpha \in (P \cap U_\alpha^+) \setminus U_\alpha^-$. Then $g_\alpha = x_\alpha(t)u_\alpha$ for some $u_\alpha \in U_\alpha^-$ and $t \neq 0$.

Lemma 6.3.3 [**special order**] *Let P be a subgroup of a unipotent group U of ${}^2G_2(q)$, ${}^B{}_2(q)$ or ${}^2F_4(q)$. Then there is an ordering of Π such that Φ_P consists only of short roots.*

Proof: Assume first that Φ is of type B_2. Then the elements of a unipotent subgroup U^1 of ${}^2\mathrm{B}_2(\mathbb{K})$ are

$$x(y,u) = x_\alpha(t^\theta)x_\beta(t)x_{\alpha+\beta}(t^{\theta+1}+u)x_{2\alpha+\beta}(u^{2\theta}),$$

where $\Pi = \{\alpha,\beta\}$ with α short and β long and $u,t \in \mathbb{K}$ and θ a field automorphism, see for instance [Ca, 13.6.1]. Choose the ordering on Φ such that $\alpha < \beta$. Then Φ_P is a subset of $\{\alpha, \alpha+\beta\}$, which is a set of short roots, the assertion.

Now assume that Φ is of type G_2. The elements of a unipotent subgroup U^1 of ${}^2\mathrm{G}_2(\mathbb{K})$ have the form

$$x(t,u,v) = x_\alpha(t^\theta)x_\beta(t)x_{\alpha+\beta}(t^{\theta+1}+u^\theta)x_{2\alpha+\beta}(t^{2\theta+1}+v^\theta)x_{3\alpha+\beta}(u)x_{3\alpha+2\beta}(v),$$

where $\Pi = \{\alpha,\beta\}$ with α short and β long, $t,u,v \in \mathbb{K}$ and θ an automorphism of $\mathbb{K}$, see for instance [Ca, 13.6.1]. We choose again the ordering on Φ such that $\alpha < \beta$. Then Φ_P is a subset of $\{\alpha, \alpha+\beta, 2\alpha+\beta\}$, which is again a set of short roots, the assertion.

Finally assume that Φ is of type F_4. The elements of a unipotent subgroup U^1 of ${}^2\mathrm{F}_4(\mathbb{K})$ are described in 6.2.5. We are going to use the same notation as in 6.2.5. We order Φ such that $\beta > \gamma > \alpha > \delta$. Then Φ_P is again a subset of a set of short roots. $\square$

$$\mathfrak{g} = \sum_{\alpha\in\Phi_P} \mathbb{E}\mathfrak{G}_\alpha + \sum_{\alpha\in\Phi_P} \mathbb{E}\mathfrak{H}_\alpha.$$

Lemma 6.3.4 [**L1**]

1. *$\mathfrak{g}$ is a subalgebra of $\mathfrak{g}_\Phi(\mathbb{E})$.*

2. *If P has nilpotent class m, then $\mathfrak{g}$ has nilpotent class at most m.*

3. *If $[P[P[\underbrace{\ldots}_{n-times}[P[P,A]]\ldots]]] = 0$, then $D^nA = 0$.*

4. $\dim(\mathrm{Ann}_A(D)) \geq \dim(C_A(P))$.

5. *Suppose that there are* $\alpha, \beta \in \Phi_D$ *and* $k \in \mathbb{K}$ *such that* $\alpha < \beta$ *and* $(g_\alpha - 1) \equiv k(g_\beta - 1)$. *Then* $\mathfrak{G}_\alpha \equiv 0$.

Proof: Notice that $[g_\alpha, g_\beta]U^-_{\alpha+\beta} = [x_\alpha(t_\alpha), x_\beta(t_\beta)]U^-_{\alpha+\beta} = x_{\alpha+\beta}(N_{\alpha\beta}t_\alpha t_\beta]U^-_{\alpha+\beta}$, where $[X_\alpha, X_\beta] = N_{\alpha+\beta}X_{\alpha+\beta}$ in $\mathfrak{g}_\Phi(E)$. If $N_{\alpha+\beta} \neq 0$, then $[g_\alpha g_\beta] \in U^+_{\alpha+\beta} \setminus U^-_{\alpha+\beta}$. Hence, $\alpha + \beta \in \Phi_P$, so D is a subalgebra of $\mathfrak{g}_\Phi(E)$, proving (1).

Now $[g_{\alpha_1}, g_{\alpha_2}, \ldots, g_{\alpha_n}]U^-_{\alpha_1+\alpha_2+\cdots+\alpha_n} = x_{\alpha_1+\alpha_2+\cdots+\alpha_n}(rt_{\alpha_1}t_{\alpha_2}\ldots t_{\alpha_n})U^-_{\alpha_1+\alpha_2+\cdots+\alpha_n}$. So if $[g_{\alpha_1}, g_{\alpha_2}, \ldots, g_{\alpha_n}] = 1$, then $r = 0$ and so $[X_{r_1}, X_{r_2}, \ldots, X_{r_n}] = rX_{r_1+r_2+\cdots+r_n} = 0$.

Now let $a \in A^+_\mu$ with $a = a_\mu + a^-_\mu$ where $a_\mu \in A_\mu$ and $a_\mu \in A^-_\mu$.
Then

$$[x_\alpha(t_\alpha), a] = \sum_{n=1}^{\infty} frac1n!t^n_\alpha X^n_\alpha)a \in t_\alpha X_\alpha a_\mu + A^-_{\mu+\alpha}$$

So $[g_\alpha, a] \in t_\alpha X_\alpha a_\mu + A^-_{\mu+\alpha}$, and in particular,

$$[g_{\alpha_1}[g_{\alpha_2}[\ldots[g_{\alpha_n}, a]\ldots]] \in t_{\alpha_1}t_{\alpha_2}\ldots t_{\alpha_n}X_{\alpha_1}X_{\alpha_2}\ldots X_{\alpha_n}a_\mu + A^-_{\mu+\alpha_1+\alpha_2+\cdots+\alpha_n}.$$

So, if $[P[P[\ldots[P, A]\ldots]] = 0$, then $X_{\alpha_1}X_{\alpha_2}\ldots X_{\alpha_n}a_\mu \in A^-_{\mu+\alpha_1+\alpha_2+\cdots+\alpha_n} \cap A_{\mu+\alpha_1+\alpha_2+\cdots+\alpha_n} = 0$.

Hence $X_{\alpha_1}X_{\alpha_2}\ldots X_{\alpha_n}A = 0$. That is, $D^nA = 0$, proving (2).

Choose $E_\mu \leq A_\mu$ so that $C_{A^+_\mu}(P) + A^-_\mu \geq E_\mu + A^-_\mu$ $(E_\mu = A_\mu \cap (C_{A^+_\mu}(P) + A^-_\mu))$. Let $E = \bigoplus_\mu E_\mu$. Then $\dim_k(E) = \dim_k(C_A(P))$.

Now, if $a \in C_{A^+_\mu}(P)$, then $a = a_\mu + a^-_\mu$, so $[g_\alpha, a] \in t_\alpha X_\alpha a_\mu + A^-_{\mu+\alpha}$ implies that $x_\alpha a_\mu = 0$.

Hence, $X_\alpha E = 0$ and so $DE = 0$, proving (3).

It remains to show (5). Let $a \in A_\mu$. By what was proved before
$(g_\alpha - 1)a = [g_\alpha, a] \in t_\alpha\mathfrak{G}_\alpha a_\mu + A^+_{\mu+\alpha}$ and $(g_\beta - 1)a[= g_\beta, a] \in t_\beta\mathfrak{G}_\beta a_\mu + A^+_{\mu+\beta} \in A^+_{\mu+\alpha}$

Since $(g_\alpha - 1) \equiv k(g_\beta - 1)$ we conclude that $t_\alpha\mathfrak{G}_\alpha a_\mu = 0$ and so $\mathfrak{G}_\alpha a_\mu = 0$ and $\mathfrak{G}_\alpha \equiv 0$, hence (5).

□

Chapter 7

Quadratic Modules

7.1 Quadratic modules for $\mathfrak{g}$

For a root system Φ let $p_\Phi := \frac{(\alpha,\alpha)}{(\beta,\beta)}$ where α is a long and β is a short root in Φ. Note that if Φ is connected then $p_\Phi \in \{1,2,3\}$. If $\mathfrak{g} = \mathfrak{g}_\Phi(\mathbb{K})$ and $p_\Phi = \operatorname{char}\mathbb{K}$, then $\mathfrak{g}_{\text{short}}$ (the subalgebra of $\mathfrak{g}$ generated by $\{\mathfrak{G}_\alpha \mid, \alpha \in \Phi_{\text{short}}\}$) is an ideal in $\mathfrak{g}$. Note that this happens for $p = 2$ and Φ of type B_n, C_n and F_4 and for $p = 3$ and Φ of type G_2. These cases will require special attention throughout this section.

Definition 7.1.1 [**def:quadratic**] *A module V for $\mathfrak{g}_\Phi(\mathbb{K})$ is called* quadratic *if $(\mathfrak{H}_{\alpha^*} - 1)\mathfrak{G}_\alpha V = 0$ for all long roots $\alpha \in \Phi$.*

The definition of a quadratic module is motivated by the following lemma:

Lemma 7.1.2 [**quadratic in odd characteristic**] *Let V be a $\mathfrak{g}_\Phi(\mathbb{K})$-module and $\alpha \in \Phi$.*

(a) [**a**] *If $(\mathfrak{H}_{\alpha^*} - 1)\mathfrak{G}_\alpha V = 0$ then $\mathfrak{G}_\alpha^2 = 0$.*

(b) [**b**] *If $\operatorname{char}\mathbb{K} \neq 2$, then $\mathfrak{G}_\alpha^2 V = 0$ iff $(\mathfrak{H}_{\alpha^*} - 1)\mathfrak{G}_\alpha V = 0$.*

(c) [**c**] *Suppose that V comes from a module for $\mathcal{U}_\Phi(\mathbb{Z})$ and that $\frac{\mathfrak{G}_\alpha^2}{2} V = 0$, then $(\mathfrak{H}_{\alpha^*} - 1)\mathfrak{G}_\alpha V = 0$.*

Proof: (a) Since $(\mathfrak{H}_{\alpha^*} - 1)\mathfrak{G}_\alpha V = 0$ we have $\mathfrak{H}_{\alpha^*}\mathfrak{G}_\alpha \equiv \mathfrak{G}_\alpha$ and so

$$0 = [\mathfrak{G}_\alpha, \mathfrak{G}_\alpha] \equiv [\mathfrak{H}_{\alpha^*}\mathfrak{G}_\alpha, \mathfrak{G}_\alpha] = [\mathfrak{H}_{\alpha^*}, \mathfrak{G}_\alpha]\mathfrak{G}_\alpha = \mathfrak{G}_\alpha^2$$

(b) We compute

$[\mathfrak{G}_\alpha^2, \mathfrak{G}_{-\alpha}] = [\mathfrak{G}_\alpha, \mathfrak{G}_{-\alpha}]\mathfrak{G}_\alpha + \mathfrak{G}_\alpha[\mathfrak{G}_\alpha, \mathfrak{G}_{-\alpha}] == \mathfrak{H}_{\alpha^*}\mathfrak{G}_\alpha + \mathfrak{G}_\alpha\mathfrak{H}_{\alpha^*} = [\mathfrak{G}_\alpha, \mathfrak{H}_{\alpha^*}] + 2\mathfrak{H}_{\alpha^*}\mathfrak{G}_\alpha = -2\mathfrak{G}_\alpha + 2\mathfrak{H}_{\alpha^*}\mathfrak{G}_\alpha = 2(\mathfrak{H}_{\alpha^*} - 1)\mathfrak{G}_\alpha$. Thus

$$(*) \quad [\mathfrak{G}_\alpha^2, \mathfrak{G}_{-\alpha}] = 2(\mathfrak{H}_{\alpha^*} - 1)\mathfrak{G}_\alpha$$

So if $\mathfrak{G}_\alpha^2 \equiv 0$ and $\operatorname{char}\mathbb{K} \neq 2$ we conclude that $(\mathfrak{H}_{\alpha^*} - 1)\mathfrak{G}_\alpha \equiv 0$.

(c) Note that the (*) is also a valid equation in $\mathcal{U}_\Phi(\mathbb{Z})$. Thus in $\mathcal{U}_\Phi(\mathbb{Z})$ we have $[\frac{\mathfrak{G}_\alpha^2}{2}, \mathfrak{G}_{-\alpha}] = (\mathfrak{H}_{\alpha^*} - 1)\mathfrak{G}_\alpha$. Thus (**??**) holds. □

The irreducible quadratic modules for $\mathfrak{g}_\Phi\mathbb{K}$ are fairly easily classified (see the next theorem). The remainder of the section will be devoted to show that some weaker conditions already imply that a module is quadratic. If V is a module for $\mathfrak{g}$ and $\mathfrak{G}_1, \mathfrak{G}_2 \in \mathfrak{g}$ we write $\mathfrak{G}_1 \equiv \mathfrak{G}_2$ if $(\mathfrak{G}_1 - \mathfrak{G}_2)V = 0$, that is if the image of $\mathfrak{G}_1$ and $\mathfrak{G}_2$ in $\operatorname{End}(V)$ are equal.

Theorem 7.1.3 [**classification of quadratic modules for Lie algebras**] *Let $\mathbb{K}$ be a field, Φ a root system and $\mathfrak{g} = \mathfrak{g}_\Phi(\mathbb{K})$ the corresponding algebra. Let $V = V(\lambda)$ be the irreducible restricted $\mathfrak{g}$-module of heighest weight $\lambda \neq 0$. Let $\alpha = \alpha_{\text{long}}$ be the heighest long root of Φ. Then the following are equivalent:*

(a) [**a**] *V is quadratic.*

(b) [**b**] $(\mathfrak{H}_{\alpha^*} - 1)\mathfrak{G}_\alpha V = 0$

(c) [**c**] $\mathfrak{G}_\beta\mathfrak{G}_\alpha V = 0$ *for all* $\beta \in \Phi$ *with* $(\beta, \alpha) > 0$.

(d) [**d**] $(\lambda, \alpha^*) = 1$.

(e) [**e**] $-1 \leq (\rho, \alpha^*) \leq 1$ *for all weights* ρ *for* $\mathfrak{g}$ *on* V.

Proof: We assume without loss that $\mathbb{K}$ is algebraicly closed.

(a)$\Longrightarrow$ (b): Obvious.

(b)$\Longrightarrow$ (c): Let $\beta \in \Phi$ with $(\beta, \alpha) > 0$. If $\beta = \alpha$ then $\mathfrak{G}_\alpha^2 \equiv 0$ by 7.1.2(a). Suppose that $\beta \neq \alpha$. Then $(\alpha^*, \beta) = 1$ and so $[\mathfrak{H}_{\alpha^*}, \mathfrak{G}_\beta] = \mathfrak{G}_\beta$. Note that β is positive, so $\beta + \alpha \notin \Phi$ be the maximality of α. Thus $\mathfrak{G}_\alpha\mathfrak{G}_\beta = \mathfrak{G}_\beta\mathfrak{G}_\alpha$. Also by assumption $(\mathfrak{H}_{\alpha^*} - 1)\mathfrak{G}_\alpha \equiv 0$ and so $\mathfrak{H}_{\alpha^*}\mathfrak{G}_\alpha \equiv \mathfrak{G}_\alpha$. We compute:

$$\mathfrak{G}_\beta\mathfrak{G}_\alpha = [\mathfrak{H}_{\alpha^*}, \mathfrak{G}_\beta]\mathfrak{G}_\alpha = \mathfrak{H}_{\alpha^*}\mathfrak{G}_\beta\mathfrak{G}_\alpha - \mathfrak{G}_\beta\mathfrak{H}_{\alpha^*}\mathfrak{G}_\alpha =$$
$$= \mathfrak{H}_{\alpha^*}\mathfrak{G}_\alpha\mathfrak{G}_\beta - \mathfrak{G}_\beta\mathfrak{H}_{\alpha^*}\mathfrak{G}_\alpha \equiv \mathfrak{G}_\alpha\mathfrak{G}_\beta - \mathfrak{G}_\beta\mathfrak{G}_\alpha = 0.$$

(c)$\Longrightarrow$ (d): Let v_- be a lowest weight vector. Let $\mathfrak{u}_+ = \mathfrak{g}_{\Phi^+}(\mathbb{K})$ and let $\omega_0 \in W(\Phi)$ with $\omega_0(\Pi) = -\Pi$. Then v_- has weight $\omega_0(\lambda)$. The $\mathfrak{u}v_- = V$ (**??**). Since $[\mathfrak{u}_+, \alpha] = 0$ we conclude that $v^- \notin \operatorname{Ann}(\mathfrak{G}_\alpha)$. Hence $v := \mathfrak{G}_\alpha v_- \neq 0$ is a non zero weight vector with weight $\omega_0(\lambda) + \alpha$. Let

$$\mathfrak{q}_\alpha = \mathbb{K}\langle G_\beta \mid \beta \in \phi, (\alpha, \beta) > 0\rangle$$

and

$$\mathfrak{l}_\alpha = \mathbb{K}\langle G_\beta \mid \beta \in \phi, (\alpha, \beta) = 0\rangle + \mathfrak{h}$$

By Smith's Lemma 6.1.4 $\mathrm{Ann}(\mathfrak{q}_\alpha)$ is an irreducible module for $\mathfrak{l}_\alpha$. Since v_+ is a highest weight vector in $\mathrm{Ann}(\mathfrak{q}_\alpha)$ we conclude from **??** that all weights in $\mathrm{Ann}(\mathfrak{q}_\alpha)$ are of the form $\lambda+\mu$ for some $\mu \in \mathbb{N}(\Phi^- \cap \alpha^\perp)$.

Recall that with weight vectors we mean weight vectors for the Cartan subgroup H of $G_{\mathbb{K}}(\Phi)$. In particular two weights in Λ which share a non-zero weight vector are equal. Thus

$$\omega_0(\lambda)+\alpha = \lambda+\mu$$

for some $\mu \in \Lambda$ with $(\alpha,\mu) = 0$. Note also that ω_0 has order two, peserves $(\cdot,\cdot)$ and $\omega_0(\alpha) = -\alpha$. So we compute

$$(\omega_0(\lambda)+\alpha,\alpha^*) = (\omega_0(\lambda),\alpha^*)+(\alpha,\alpha^*) = (\lambda,\omega_0(\alpha^*))+2 = -(\lambda,\alpha^*)+2$$

On the other hand

$$(\lambda+\mu,\alpha^*) = (\lambda,\alpha^*)+(\mu,\alpha^*) = (\lambda,\alpha^*)$$

The last three displayed equations imply $2(\lambda,\alpha^*) = 2$. Since this is a statement in $\mathbb{Z}$ we conclude $(\lambda,\alpha^*) = 1$.

(d)$\Longrightarrow$ (e):

(d)$\Longrightarrow$ (a): Suppose that $(\lambda,\alpha^*) = 1$. Note that $\rho = \lambda-\phi$ for some $\phi \in \mathbb{N}\Phi^*$. Also $(\phi,\alpha^*) \geq 0$ and so $(\rho,\alpha^*) \leq (\lambda,\alpha'^*) \leq 1$. Similarly as $\rho = \omega_0(\lambda) * \psi$ for some $\psi \in \mathbb{N}\Phi^*$ we have $(\rho,\alpha^*) \geq (\omega_0(\lambda),\alpha^*) = -1$ and so (e) holds.

(e)$\Longrightarrow$ (a): It suffices to show that $(\mathfrak{H}_\alpha d-1)\mathfrak{G}_\alpha V_\mu 0$ for all weights μ on V. If $\mathfrak{G}_\alpha V_\mu = 0$ this is obvious. So suppose that $\mathfrak{G}_\alpha V_\mu \neq 0$. Thus both μ and $\mu+\alpha$ are weights on V. Thus

$$(\mu+\alpha,\alpha^*) \leq 1$$

On the other hand

$$(\mu+\alpha,\alpha^*) = (\mu,\alpha^*)+(\alpha,\alpha^*) \geq -1+2 = 2$$

and we conclude that $(\mu+\alpha,\alpha^*) = 1$. Hence 6.2.1(b) implies that $(\mathfrak{H}_{\alpha^*}-1)V_{\mu+\alpha} = 0$. Thus (a) holds. $\square$

Definition 7.1.4 [**def:quadratic tuple**] *A quadratic tuple is tuple $(\Phi,p,\lambda,\alpha,\beta)$ where Φ is a connected root system, λ is a non-zero dominant integral p-restricted weight, α and β are roots, and $V = V_{\mathbb{K}}(\lambda)$ for some field $\mathbb{K}$ with* $\mathrm{char}\,\mathbb{K} = p$ *such that*

(a) [**a**] $\mathfrak{G}_\beta\mathfrak{G}_\alpha V = 0$.

(b) [**b**] $\mathfrak{G}_\alpha V \neq 0 \neq \mathfrak{G}_\beta V$.

(c) [**c**] *If $\alpha = \beta$ then $p \neq 2$.*

In the next few lemmas we will determine all the quadratic tuples. **Comment:We should once and for all introduce weight vectors for arbitrary fields: For the algebraicly closed case define it by the action of H, in general $v \in V(\lambda)$ is called a weight vector if $1 \otimes_{\mathbb{K}} v$ is a weight vector in $\bar{K} \otimes \mathbb{K}V$. Note that for p-restricted weights, V will be the direct sum of the weight spaces.(just start with the lowest weight vector and take images under the $\mathfrak{G}_\alpha$'s**

Lemma 7.1.5 [**quadratic tuple for a=b long**] *Let $(\Phi, p, \lambda, \alpha, \beta)$ be a quadratic tuple with $\alpha = \beta$ and α long. Then V is a quadratic module.*

Proof: By assumption $p \neq 2$. So the lemma follows from 7.1.2 □

Lemma 7.1.6 [**quadratic tuples for (a,b) positive and a long**] *Let $(\Phi, p, \lambda, \alpha, \beta)$ be a quadratic tuple with α long, $\alpha \neq \beta$ and $(\alpha, \beta) > 0$. Then V is a quadratic module.*

Proof: Without loss α is the highest long root. Then β is positive. Let $\Psi = \langle \alpha, \beta \rangle$, the root subsystem generated by α and β. Then Ψ is of type A_2, B_2 or G_2. In any case $\delta = \alpha - \beta$ is a root, $\alpha = \delta + \beta$, $\alpha + \beta$ is not a root, $\mathfrak{G}_\alpha \mathfrak{G}_\beta = \mathfrak{G}_\beta \mathfrak{G}_\alpha \equiv 0$ and $r_{\beta\delta} + 1 = p_\Psi$.

Suppose first that $p \neq 2$ and $p \neq p_\Psi$.

Since $\mathfrak{G}_\beta \mathfrak{G}_\alpha \equiv 0$ taking the Lie bracket with $\mathfrak{G}_\delta$ gives $\pm p_\Psi \mathfrak{G}_\alpha^2 \equiv 0$. Thus $\mathfrak{G}_\alpha^2 = 0$ and we are done by 7.1.5.

Suppose next that $p = p_\Psi$. Then Ψ is of type B_2 or G_2, $p = p_\Phi$ and β is short. Let X be an irreducible $\mathfrak{g}_{\text{short}}$-submodule in V. If $\mathfrak{G}_\beta X = 0$ then also $\mathfrak{H}_\beta = [\mathfrak{G}_\beta, \mathfrak{G}_{-\beta}]$ annihilates X. Thus by **??**(bb), $\mathfrak{H}_\alpha$ acts nilpotently on V. But $\mathfrak{H}_\beta$ is semisimple on V and so $\mathfrak{H}_\beta V = 0$. Hence by **??** $\mathfrak{G}_\beta V = 0$, a contrdiction to the definition of a quadratic tuple.

Thus $\mathfrak{G}_\beta X \neq 0$. Since $\mathfrak{G}_\alpha \mathfrak{G}_\beta X = 0$ we conclude $\text{Ann}_X(\mathfrak{G}_\alpha) \neq 0$ and so by **??**(bc), $\mathfrak{G}_\alpha X \leq X$. By symmetry the same holds for any long root subalgebra of $\mathfrak{g}$ and so $\mathfrak{g}X \leq X$ and $V = X$. Thus $\mathfrak{g}_{\text{short}}$ acts irreducibly on V. Let $\mathfrak{q} = \mathbb{K}\langle \mathfrak{G}_\mu \mid \mu \in \Phi_{\text{short}}, (\mu, \alpha) > 0 \rangle$ and $\mathfrak{l} = \mathbb{K}\langle \mathfrak{G}_\mu \mid \mu \in \Phi_{\text{short}} \cap \alpha^\perp \rangle$. Then $\mathfrak{q} + \mathfrak{l} + \mathfrak{h}_{\text{short}}$ is a parabolic subalgebra and so by 6.1.4 $\text{Ann}_V(\mathfrak{q})$ is an irreducible $\mathfrak{l}$-module. Note that $\mathfrak{q}$ is an ideal in $\mathfrak{q}_\alpha + \mathfrak{l}_\alpha$ and so $\text{Ann}_V(\mathfrak{q})$ is an irreducible module for $\mathfrak{q}_\alpha + \mathfrak{l}_\alpha$. It follows that $\mathfrak{q}_\alpha$ annihilates $\text{Ann}_V(\mathfrak{q})$. On the other hand $W(\Phi \cap \alpha^\perp)$ acts transitively on $\{\mu \in \Phi_{\text{short}}, (\mu, \alpha) > 0\}$ and thus $\mathfrak{q}\mathfrak{G}_\alpha V = 0$ and so also $\mathfrak{q}_\alpha G_\alpha V = 0$. Thus V is quadratic by 7.1.3.

Suppose now that Ψ is of type A_2. We claim that $\mathfrak{G}_\mu \mathfrak{G}_\alpha \equiv 0$ for all $\mu \in \Phi$ with $(\mu, \alpha) > 0$. This is obvious if $\mu = \alpha$ or if (α, μ) is conjugate to (α, β) under $W(\Phi)$. If neither of this holds then Φ is of type A_n. Let V^* be $\mathfrak{g}$-module dual to V. Then $\mathfrak{G}_\alpha \mathfrak{G}_\beta V^* = 0$. Since $\mathfrak{G}_\alpha$ and $\mathfrak{G}_\beta$ commute, $\mathfrak{G}_\beta \mathfrak{G}_\alpha V^* = 0$. Now $V^* \cong V^\sigma$ where σ is the graph automorphism of $\mathfrak{g}$. Thus $\mathfrak{G}_{\sigma(\beta)} \mathfrak{G}_{\sigma(\alpha)} V = 0$. Now (α, μ) is conjugate under $W(\Phi)$ to $(\sigma(\alpha), \sigma(\beta)$ and we again conclude that $\mathfrak{G}_\mu \mathfrak{G}_\alpha \equiv 0$. Thus V is quadratic by 7.1.3.

Suppose finally that $p = 2$ and Ψ is of type G_2. Then β is short. Let $\gamma = \beta - \delta$. Then γ is a root, $r_{\delta\beta} = 3$, and $\alpha + \gamma$ is not a root.

$$0 \equiv [\mathfrak{G}_\beta \mathfrak{G}_\alpha, \mathfrak{G}_\gamma] = \pm 3 \mathfrak{G}_{\beta+\gamma} \mathfrak{G}_\alpha$$

Thus $\mathfrak{G}_{\beta+\gamma}\mathfrak{G}_\alpha \equiv 0$. Using the action of $W(\Phi \cap \alpha^\perp)$ we conclude that $\mathfrak{q}_\alpha \mathfrak{G}_\alpha \equiv 0$ and V is quadratic. □

Lemma 7.1.7 [**a long implies quadratic**] *Let $(\Phi, p, \lambda, \alpha, \beta)$ be a quadratic tuple with α long. Then V is quadratic.*

Proof: Without loss α is the highest long root. If $\beta = \alpha$ we are done by 7.1.5. So we may choose $\beta \in \Phi$ maximal with $\beta \neq a$, $\mathfrak{G}_\beta V \neq 0$ and $\mathfrak{G}_\beta \mathfrak{G}_\alpha V = 0$. If $(\beta, \alpha) > 0$ we are done by 7.1.6. So we may assume that $(\alpha, \beta) \leq 0$.

Suppose first that β is long. If Φ is of type A_1 then $\beta = -\alpha$ and so $2\mathfrak{G}_\alpha^2 = [\mathfrak{G}_\beta \mathfrak{G}_\alpha, \mathfrak{G}_\alpha, \mathfrak{G}_\alpha] = iv0$. Thus $\mathfrak{G}_\alpha^2 \equiv = 0$ and V is quadratic by 7.1.3 (Actually a moments thought even gives a contradiction).

So assume that $\Phi \neq A_1$. If Φ_{long} is connected there exists $\gamma \in \Pi(\Phi_{\text{long}})$ with $\beta + \gamma \in \Phi_{\text{long}}$. Then $N_{\beta\gamma} \neq 0$ and so $\mathfrak{G}_{\beta+\gamma}\mathfrak{G}_a = 0$. The maximal choice of β implies $\beta + \gamma = \alpha$. But then $(\alpha, \beta) > 0$.

So $\Phi_l o$ is disconnected, $\alpha \perp \beta$,Φ is of type C_n and $\gamma := \frac{1}{2}(\alpha - \beta) \in \Phi_{\text{short}}$. Then $N_{\beta\gamma} \neq 0$ and $\mathfrak{G}_{\gamma+\alpha}\mathfrak{G}_\alpha \equiv 0$. The maximal choice of γ implies $\mathfrak{G}_{\gamma+\alpha} V = 0$. In particular $p = 2$, $\mathfrak{g}_{\text{short}} V = 0$ and $[\mathfrak{H}_\beta, \mathfrak{g}]V = 0$. Thus $\mathfrak{H}_\beta$ acts as a scalar on V. Since $\alpha \perp b$, $\mathfrak{H}_\beta \mathfrak{G}_\alpha = [\mathfrak{G}_\beta \mathfrak{G}_\alpha, G_{-\beta} =\equiv 0$ and so $\mathfrak{H}_\beta V = 0$ But then $\mathfrak{g}$ acts nilpotent on V a contradiction.

Suppose next that β is not long. Note that the highest short root has positive inner product with α. So β is not the highest short root. Assume Φ_{short} is connect. Then we can choose $\gamma \in \Pi(\Phi_{\text{short}})$ with $\beta + \gamma \in \Phi_{\text{short}}$ and we get a contradiction to the maximal choice of β. Hence Φ_{short} is disconnected and Φ is of type B_n. If β is not perpendicular to α then $((b, a) < 0$, $N_{\beta\alpha} \neq 0$ and we get $G_{\alpha+\beta}\mathfrak{G}_\alpha = 0$, contradiction the maximality of β. So $\beta \perp \alpha$ and as above $\mathfrak{H}_\beta \mathfrak{G}_\alpha = 0$. Let $\gamma \in \Pi$ with $\beta + \gamma \in \Phi$. If $N_{\beta\gamma} \neq 0$, we get a contradiction to the maximality of β. Thus $p = 2$ and so $[Hb, \mathfrak{g}] = 0$ and $\mathfrak{H}_\beta$ centralizes V. But then $\mathfrak{g}_{\text{short}} V = 0$, a contradiction as β is short and $\mathfrak{G}_\beta V \neq 0$.

This settles the last case and the lemma is proved. □

Lemma 7.1.8 [**quadratic tuples with GaGb not 0**] *Let $(\Phi, p, \lambda, \alpha, \beta)$ be a quadratic tuple with $\mathfrak{G}_\alpha \mathfrak{G}_\beta V(\lambda) \neq 0$. The up to conjugacy under W $\Phi = A_n$, $\alpha = e_0 - e_n$ and either $\beta = -e_0 + e_1$ and $\lambda = \lambda_n$ or $\beta = -e_2 + e_n$ and $\lambda = \lambda_1$.*

Proof: Let V^* the dual of V. So $V^* = V(\omega_0(\lambda))$. Then $\mathfrak{G}_\alpha \mathfrak{G}_\beta V^* = 0$ and we conclude that $\lambda \neq -\omega(\lambda)$. Thus $\Phi = A_n$ or $n \geq 5, n$ is odd and $\Phi = D_n$ Also $[G_\alpha, G_b] \neq 0$ and so $(\alpha, \beta) < 0$.

But in D_n for $n > 3$, W has a unique orbits on pairs of roots (γ, δ) with $(\gamma, \delta) < 0$, namely all are conjugate to $(e_1 + e_2, -e_1 + e_3)$. Thus $(\alpha\,\beta)$ is conjugate to (β, α) contradicting the assumptions.

Thus Φ is of type A_n. By 7.1.7 V is quadratic and so by 7.1.3 $\lambda = \lambda_i$ for some $1 \leq i \leq n$.

Up to conjugation under W, we may assume $\alpha = e_0 - e_n$ and either $\beta = -e_0 + e_1$ or $\beta = -e_1 + e_n$. In view of the graph automorphismus it suffices to treat the case $\beta = -e_0 + e_1$. Let

$$\Sigma = \langle \beta, \Phi \cap \alpha^{\perp} \rangle = \{\pm(e_i - e_j) \mid 0 \leq i < j \leq n-1\}.$$

Then Σ is a closed root subsystem of type A_{n-1}. Also $\mathfrak{G}_\alpha V$ is invariant under $\mathfrak{l}_\alpha$ and $\mathfrak{G}_\beta$ and so under $\mathfrak{g}_\Sigma$. Since $\mathfrak{G}_\beta$ annihilates $\mathfrak{G}_\alpha V$ and $W(\Sigma)$ is tranisitive on Σ, g_Σ annihilates $\mathfrak{G}_\alpha V$. As $v_+ \in \mathfrak{G}_\alpha V$ we conclude that $\lambda = \lambda_n$ and the lemma is proved. □

Lemma 7.1.9 [**quadratic tuples for (a,b) not positive and a long**] *Let $(\Phi, p, \lambda, \alpha, \beta)$ be a quadratic tuple with α long, $\alpha \neq \beta$ and $(\alpha, \beta) \leq 0$. Then one of the following holds:*

(a) [**a**] $\Phi = A_n$, $\alpha = e_0 - e_n$ *and either*

  (a) [**aa**] $\lambda = \lambda_1$ *and* $\beta = e_1 - e_2$ *or* $-e_2 + e_n$ *or*

  (b) [**ab**] $\lambda = \lambda_n$ *and* $\beta = e_1 - e_2$ *or* $-e_0 + e_1$.

(b) [**b**] $\Phi = C_n$, $\lambda = \lambda_1$, $\alpha = 2e_1$ *and either* $\beta = 2e_2$ *or* $p \neq 2$, $n > 2$ *and* $\beta = e_2 - e_3$.

(c) [**c**] $\Phi = B_n, n \geq 3$, $\alpha = e_1 + e_2$ *and either*

  (a) [**ca**] $\lambda = \lambda_n$ *and* $\beta = e_1 - e_2$ *or*

  (b) [**cb**] $\lambda = \lambda_1$, $\beta = e_2 - e_3$ *or* $p \neq 2$ *and* $\beta = e_2$.

(d) [**d**] $\Phi = D_4$ $\alpha = e_1 + e_2$ *and one of the following holds:*

  (a) [**da**] $\lambda = \lambda_1$ *and* $\beta = e_3 - e_4$ *or* $e_3 + e_4$.

  (b) [**db**] $\lambda = \lambda_3$ *and* $\beta = e_1 - e_2$ *or* $e_3 + e_4$.

  (c) [**dc**] $\lambda = \lambda_4$ *and* $\beta = e_1 - e_2$ *or* $e_3 - e_4$.

(e) [**e**] $\Phi = D_n, n \geq 5, \alpha = e_1 + e_2$ *and either*

  (a) [**ea**] $\beta = e_3 - e_4$ *and* $\lambda = \lambda_1$ *or*

  (b) [**eb**] $\beta = e_1 - e_2$ *and* $\lambda = \lambda_{n-1}$ *or* λ_n.

Proof: Without loss α is the highest root. Let Ψ be the closed root subsystem generated by α and β. By 7.1.7 that V is quadratic and so by 7.1.3 $\lambda = \lambda_\mu$ for some $\delta \in \Pi$ with $n^*_{\mu^*} = 1$. Moreover, $\mathfrak{G}_\alpha V = \mathrm{Ann}(\mathfrak{q}_\alpha)$ and so $\mathfrak{G}_\beta \mathfrak{G}_\alpha V = 0$ just means that $\mathfrak{G}_\beta$ annihilates $V_\alpha := \mathrm{Ann}(\mathfrak{q}_\alpha)$.

Supose first that $(\beta,\alpha)=0$. Then $\mathfrak{G}_b \leq \mathrm{Ann}_{\mathfrak{l}_\alpha}(V_\alpha)$. If $(\mu,\alpha)\neq 0$ then all of $\mathfrak{l}_\alpha$ annihilates V_α and (a) or (b) holds. So suppose that $(\mu,\alpha)=0$. Asume that $\Phi \perp \alpha^\perp$ is connected. Then $\mathfrak{G}_\beta V_\alpha = 0$ implies that β is short and $p=p_\Phi$. On the otherhand $G_\beta V \neq 0$ implies that μ is short. But the μ is conjugate to β in $W(\Phi\cap\alpha^\perp)$ and so $\mathfrak{G}_\mu V_\alpha = 0$, a contradiction.

Thus $\Phi \perp \alpha^\perp$ is not connected and so Φ is of type B_n, $n>2$ or D_n, $n\geq 4$. It is now easu to see that one of (c), (d) or (e) holds, the assumption that $p\neq 2$ in some cases is to make sure that $\mathfrak{G}_\beta V \neq 0$.)

Suppose next that $(\beta,\alpha)<0$. If $\mathfrak{G}_\alpha\mathfrak{G}_\beta V\neq 0$, then (a) holds by 7.1.8 So we may assume that $\mathfrak{G}_\alpha\mathfrak{G}_\beta \equiv 0$. Then also $[\mathfrak{G}_\alpha,\mathfrak{G}_\beta]\equiv 0$. Since $(\beta,\alpha)<0$, $\alpha+\beta$ is a root and since α is long $N_{\alpha\beta}\neq 0$. It follows that $G_{\alpha+\beta}\equiv 0$. Thus $p=p_\Phi$ and $\alpha+\beta$ is short. Since $\mathfrak{G}_\beta \not\equiv 0$, β is long. But the sum of two long roots always long , a contradiction to $\alpha+\beta$ short. $\square$

Lemma 7.1.10 [**p=pphi and a and b short**] *Let $(\Phi,p,\lambda,\alpha,\beta)$ be a quadratic tuple and suppose that $p=p_\Phi$ and both α and β are short. Then $\Phi=C_n$, $p=2$ and $\lambda=\lambda_1$ or $\lambda_1+\lambda_n$. Moreover, $V(\lambda)$ is as a module for $\mathfrak{g}_{\mathrm{short}}$ isomorphic to a direct sum of natural modules.*

Proof: Note that Φ is B_n, C_n, G_2 or F_4 and Φ_{short} is of type A_1^n, D_n, A_2 and D_4 respectively. Moreover $W/W(\Phi_{\mathrm{short}})$ induces the full group of graph automorphisms on Φ_{short}.

Let μ be the restriction of λ to Φ^*_{short}. Then all composition factors for $\mathfrak{g}_{\mathrm{short}}$ on V are isomorphic to $V(\mu)$. Moreover $(\Phi_{\mathrm{short}},\mu,\alpha,\beta)$ is a quadratic tuple. This easily rules out the case $\Phi_{\mathrm{short}}=A_1^n$. Hence Φ_{short} is connected and so by 7.1.7 $V(\mu)$ is quadratic for $\mathfrak{g}_{\mathrm{short}}$. Since μ is invariant under all graph automorphism, 7.1.3 implies that $\Phi_{\mathrm{short}}=D_n$ and $\mu=$"μ_1". Then $\lambda=\lambda_1$ or $\lambda=\lambda_1+\lambda_n$. Note that $V(\lambda_1+\lambda_n)\cong V(\lambda_1)\otimes V(\lambda_n)$ and g_{short} acts trivially on $V(\lambda_n)$. So also the last statement of the lemma is proved. $\square$

It remains to look at quadratic tuples where Φ has two root lengths, α and β are short and $p\neq p_\phi$,

Lemma 7.1.11 [**a=b short**] *Let $(\Phi,p,\lambda,\alpha,\beta)$ be a quadratic tuple with $\alpha=\beta$ short and $p\neq p_\Phi\neq 1$. Then V is minuscule. That is one of the following holds*

(a) [**a**] $\Phi=B_n$ *and* $\lambda=\lambda_n$.

(b) [**b**] $\Phi=C_n$ *and* $\lambda=\lambda_1$

Proof: Without loss α is the highest short root. Since α is not the highest long, there exists $\gamma\in\Pi$ with $\alpha+\gamma\in\Phi$. Since α is the highest short root, $\alpha+\gamma$ is long, $N_{\alpha\gamma}=\pm p_\Phi$ and neither $\alpha+2\gamma$ nor $2\alpha+\gamma$ are roots Thus

$$0\equiv[\mathfrak{G}_\alpha^2,\mathfrak{G}_\gamma]=\pm 2p_\Phi\mathfrak{G}_{\alpha+\gamma}\mathfrak{G}_\alpha$$

Since $\alpha = \beta$, $p \neq 2$. By assumtion $p \neq p_\Phi$ and so $\mathfrak{G}_{\alpha+\gamma}\mathfrak{G}_\alpha \equiv 0$. Thus by 7.1.7 V is quadratic. So $\lambda = \lambda_\delta$ for some $\delta \in \Pi$ so that δ^* appears once in the highest short root of Φ^*. A glance at the highest long root of Φ^* shows that δ appears once or twice in α^*. Thus $(\lambda, \alpha^*) \in \{1, 2\}$. Note that there exists a composition factor for $\mathbb{K}\langle G\alpha, \mathfrak{H}_\alpha \mathfrak{G}_{-\alpha}\rangle$ with heighest weight the restriction of λ. Since $\mathfrak{G}_a^2$ annihilates this composition factor $(\lambda, \alpha^*) = 1$. So λ is minuscule. □

Lemma 7.1.12 [**a,b short, (a,b) not negative**] *Let $(\Phi, p, \lambda, \alpha, \beta)$ be a quadratic tuple with both α and β short, $\alpha \neq \beta$, $(\alpha, \beta) \geq 0$ and $p \neq p_\Phi \neq 1$. Then up to conjugacy under W,*

$\Phi = C_n, \lambda = \lambda_1$, $\alpha = e_1 + e_2$ and $\beta = e_2 + e_3$ or $\beta = e_3 + e_4$.

Proof: Suppose that $\alpha + \beta$ is a long root. Then $N_{\alpha\beta} = p_\Phi \neq p$. By 7.1.8 $\mathfrak{G}_\beta \mathfrak{G}_\alpha \equiv 0$ and so $N_{\alpha\beta} G_{\alpha+\beta} \equiv 0$. Thus $G_{\alpha+\beta} \equiv 0$ a contradiction.

Thus $\alpha + \beta$ is not a long root. This rules out the case $\Phi = B_n$ and $\Phi = G_2$. It also shows that $(\alpha, \beta) > 0$ for F_4. Also $p \neq p_\phi = 2$ and in view of 7.1.11 we will be done if we can show that $\mathfrak{G}_\alpha^2 \equiv 0$.

Suppose that $(\alpha, \beta) > 0$. Then $\langle \alpha, \beta\rangle$ is of type A_2. So $\gamma = \beta - \alpha$ is a short root, $\alpha + \gamma$ is not a root and $N_{\beta\gamma} = \pm 1 \neq 0$. Hence

$$0 \equiv [\mathfrak{G}_\beta \mathfrak{G}_\alpha, \mathfrak{G}_\gamma] = N_{\beta\gamma} G_\alpha^2$$

and so $\mathfrak{G}_\alpha^2 \equiv 0$.

Suppose next that $(\alpha, \beta) = 0$. Then $\Phi = C_n$, $n \geq 4$ and without loss $\alpha = e_1 + e_2$ and $\beta = e_3 + e_4$. Let $\gamma = e_2 - e_3$. Then $\beta + \gamma = e_2 + e_4$ is a root, $N_{\beta\gamma} = \pm 1 \neq 0$ and $\alpha + \gamma$ is not a root and so

$$0 \equiv [\mathfrak{G}_\beta \mathfrak{G}_\alpha, \mathfrak{G}_\gamma] = N_{\beta\gamma} \mathfrak{G}_{\beta+\gamma} \mathfrak{G}_\alpha$$

and so $\mathfrak{G}_{\beta+\gamma}\mathfrak{G}_\alpha \equiv 0$. Since $(\beta + \gamma, \alpha) > 0$, we are done by the previous case. □

Lemma 7.1.13 [**a,b short, (a,b) negative**] *Let $(\Phi, p, \lambda, \alpha, \beta)$ be a quadratic tuple with both α and β short, $\alpha \neq \beta$, $(\alpha, \beta) < 0$ and $p \neq \Phi_p \neq 1$. Then up to conjugcay under W,*

Φ is of type G_2, $\lambda = \lambda_1$, $p = 2$, $\alpha = \alpha_1 + 2\alpha_2$, $\beta = \alpha_1 + \alpha_2$

Proof: By 7.1.8 $\mathfrak{G}_\alpha \mathfrak{G}_\beta \equiv 0$ and so $[\mathfrak{G}_\alpha, \mathfrak{G}_\beta] \equiv 0$.

Suppose that $\beta = -\alpha$ then $[\mathfrak{G}_\alpha, \mathfrak{G}_\beta] = \mathfrak{H}_\alpha$. By **??** $\mathfrak{H}_\alpha \equiv 0$ implies $\mathfrak{G}_\alpha \equiv 0$, a contradicion.

Thus $\beta \neq -\alpha$ and $(\alpha, \beta) \neq 0$ implies that $\alpha + \beta$ is a root. Hence $N_{\alpha\beta} G_{\alpha\beta} \equiv= 0$ and as $p \neq p_\Phi$ we conclude $N_{\alpha\beta} = 0$. $p \neq p_\phi$ implies $N_{\alpha\beta} = \pm 2$, $p_\phi \neq 2$ and so $\Phi = G_2$ and $p = 2$. Let $\Pi = \{\alpha_1, \alpha_2\}$ with α_1 short. Define

$$\Sigma_+ = \{\alpha_1, \alpha_1 + \alpha_2, -2\alpha_1 - \alpha_2\}$$

and

$$\Sigma^- = -\Sigma^+$$

Then $\Phi_{\text{short}} = \Sigma_+ \cup \Sigma_-$ and $W(\Phi_{\text{long}})$ acts transitively on $\Phi_{\text{long}}, \Sigma_+$ and Σ_-. Let $\epsilon \in \{+,-\}$ and $\delta, \mu \in \Sigma_\epsilon$ with $\delta \neq \mu$. Then (δ, μ) is conjugate under $W(\Phi)$ to (α, β) and so $\mathfrak{G}_\delta \mathfrak{G}_\mu \equiv 0$. Since $p = 2$ also $\mathfrak{G}_\delta^2 \equiv 0$. Moreover $[G_\delta, G_\mu] = \pm 2G_{\delta+\mu} = 0$. Put

$$\mathfrak{q}_\epsilon = \mathbb{K}\langle G_\delta \mid \delta \in \Sigma^\epsilon \rangle$$

We conclude that $\mathfrak{q}_\epsilon$ is an commuative subalgebra of $\mathfrak{g}$ and that

$$q_\epsilon^2 \equiv 0$$

Also $\mathfrak{G}_{\alpha_2}$ commutes with $\mathfrak{G}_{\alpha_1+\alpha_2}$ and with $\mathfrak{G}_{-2\alpha_1-\alpha_2}$ and $[\mathfrak{G}_{\alpha_2}, \mathfrak{G}_{\alpha_1}] = \pm\mathfrak{G}_{\alpha_1+\alpha_2}$. Thus $[\mathfrak{G}_{\alpha_2}, \mathfrak{q}_+] \leq \mathfrak{q}_+$. Let $\mathfrak{l} = \mathfrak{g}_{\text{long}}$. The action of $W(\Phi_{\text{long}})$ implies $[\mathfrak{l}, \mathfrak{q}^+] \leq q_+$. Since $W(\Phi)$ interchanges Σ^+ and Σ^- we also have $[\mathfrak{l}, \mathfrak{q}^-] \leq \mathfrak{q}^-$. Thus we can apply **??** conclude that

$$V = V_+ \oplus V_-$$

where $V_\epsilon = \text{Ann}_V(q_\epsilon)$.

Since V_ϵ is H invariant, $v_+ \in V_\epsilon$ for some $\epsilon \in \{+,-\}$. Hence v_+ is annihilated by q_ϵ and $\mathfrak{u} = \mathbb{K}\langle \mathfrak{G}_\delta \mid \delta \in \Phi^+ \rangle$. It is easy to see that $\mathfrak{g}$ is (as a Lie algebra) generated by $\mathfrak{q}_-$ and $\mathfrak{u}$. Thus $v_+ =\in V_+$ and $v+$ is annihilated by $\mathfrak{q}_+$ and $\mathfrak{u}$. In particular $\mathfrak{G}_{\pm(2\alpha_1+\alpha_2)} v_+ = 0$ and so $\mathfrak{H}_{2\alpha_1+\alpha_2} v_+ = 0$. Since $(2\alpha_1 + \alpha_2)^* = 2\alpha_1^* + 3\alpha_2^*$ and $p = 2$ we have $\mathfrak{H}_{2\alpha_1+\alpha_2} = \mathfrak{H}_{\alpha_2}$. Thus $\mathfrak{H}_{\alpha_2} v_+ = 0$ and so $\lambda = \lambda_1$. $\square$

Comment:there probably exists more direct proof for the preceeding lemma, but I like the proof since it treats G_2 for $p = 2$ like an A_3

Theorem 7.1.14 [**all quadratic tuples**] *The following table lists all quadratic tuples:*

Φ	p	λ	α, β
any	*any*	*quadratic*	α *long*, $\beta \neq \alpha, (\alpha, \beta) > 0$
any	*odd*	*quadratic*	$\alpha = \beta$ *long*
classical	*any*	*natural*	α *long*, $\beta \neq \alpha, (\alpha, \beta) = 0$ *not* $\alpha = \pm e_i \pm e_j, \beta = \pm e_i \mp e_j$
A_n	*any*	λ_1 *(natural)*	$\alpha = e_i - e_j, \beta = e_j - e_k$
A_n	*any*	λ_n *(natural)*	$\alpha = e_j - e_k, \alpha = e_i - e_j$
C_n	*odd*	*natural*	$\alpha = \beta$ *short*
C_n	*any*	λ_1 *or (for p=2)*$\lambda_1 + \lambda_n$	α, β *short*, $(\alpha, \beta) \geq 0$ *not* $\alpha = \pm e_i \pm e_j, \beta = \pm e_i \mp e_j$
B_n, D_n	*any*	*spin*	$\alpha = \pm e_i \pm e_j, \beta = \pm e_i \mp e_j$
B_n	*odd*	*spin*	$\alpha = \beta$ *short*
D_4	*any*	$\lambda_m, m \in \{3, 4\}$ *(spin)*	$\alpha = \pm e_i \pm e_j, \beta = \pm e_k \pm e_l$ *number of*$- = m - 1 \mod 2$
G_2	2	λ_1	α, β*short??*, $<\alpha, \beta> = -1$

Proof: This is just a summary of the results of this section □

Next we list a lower bound d for the dimensions of $\mathfrak{G}_\alpha V$ for α the longest root of Φ and V a quadratic module for $\mathfrak{g}$ or α short, $p = 2$ and $\Phi = G_2$. In the table w_0 is the longest word in the root system Φ. In the before last column the weights of $\mathfrak{G}_\alpha V$ are written down.

Theorem 7.1.15 [**images quadratic action**]

Φ	p	λ	$w_0(\lambda)$	α	$\mathfrak{G}_\alpha V$	d
A_n	*any*	λ_i, $1 \le i \le n$	??	$e_0 - e_n$	$\lambda_i^{W_\alpha}$	$\binom{n-1}{i-1}$
B_n	*any*	λ_1	$-\lambda_1$	$e_1 + e_2$	e_1, e_2	2
		λ_n	$-\lambda_n$		$\frac{1}{2}(-e_1 - e_2 \pm e_3 \pm \dots \pm e_n)$	2^{n-2}
C_n	*any*	λ_i, $1 \le i \le n$	$-\lambda_i$	$2e_1$	$e_1 + \sum_{j=2}^{i} \pm e_j$	2^{i-1}
D_n	*any*	λ_1	$-\lambda_1$	$e_1 + e_2$	e_1, e_2	2
nodd		λ_{n-1}	$-\lambda_n$		$\prod \varepsilon_i = -1, \frac{1}{2}(e_1 + e_2\varepsilon_3 e_3 \cdots \varepsilon_n e_n)$	2^{n-3}
nev			$-\lambda_{n-1}$			
E_6	*any*	λ_1	$-\lambda_6$	λ_2	$\frac{1}{6}a + \frac{1}{2}(e_3 + e_4 + e_5 + e_6 - e_7), -e_7 - \frac{1}{3}a$, $e_k - \frac{1}{3}a, 3 \le k \le 6$, $a := e_1 + e_2 + e_8$	6
E_7	*any*	λ_1	$-\lambda_1$	$-a$	$-\frac{1}{2}a - e_k, 2 \le k \le 7$, $a := e_1 + e_8$	12
G_2	2	λ_1	$-\lambda_1$	$3a + 2b$	$a + b, 2a + b$	2
F_4	*any*	λ_1	$-\lambda_1$	$e_1 + e_4$	$e_1, e_4, \pm e_i, 2 \le i \le 3$	6

Φ	λ
A_n	$\lambda_i = \frac{1}{n+1}((n+1-i)(e_0 + \ldots + e_{i-1}) - i(e_i - \ldots - e_n), 1 \le i \le n$
B_n	$\lambda_1 = e_1$
$n \ge 2$	$\lambda_n = \frac{1}{2}(e_1 + \ldots + e_n)$
C_n	$\lambda_i = e_1 + \dots + e_i, 1 \le i \le n$
D_n	$\lambda_1 = e_1$
D_n	$\lambda_{n-1} = \frac{1}{2}(e_1 + \dots + e_{n-1} - e_n)$
E_6	$\lambda_1 = e_3 - \frac{1}{3}a, a := e_1 + e_2 + e_8$
E_7	$\lambda_1 = \frac{1}{2}a + e_2, a := e_1 + e_8$
G_2	$\lambda_1 = \lambda_a = 2a + b$
F_4	$\lambda_1 = e_4$

Theorem 7.1.16 [**quadratic subalgebras**] *Let $\mathbb{K}$ be a field of characteristic $p \ge 0$, Φ a connected root system and $\mathfrak{g} = \mathfrak{g}_\Phi(\mathbb{K})$ the corresponding algebra. Let $V = V(\lambda)$ be the irreducible restricted $\mathfrak{g}$-module of heighest weight $\lambda \ne 0$. Let $\emptyset \ne \Psi \subseteq \Sigma$ such that $\mathfrak{G}_\alpha V \ne 0$ for all $\alpha \in \Psi$. Suppose that $\mathfrak{g}_\Psi$ is quadratic on V, that is $\mathfrak{g}_\Psi^2 V = 0$. Then*

(a) [**a**] *If V is quadratic but neither natural nor spin, then one of the following holds:*

1. [**a**] *There exists a tuple $(\alpha_0, \alpha_1, \dots, \alpha_k)$ of roots with diagram Δ such that $\Psi = \{\alpha_0, \alpha_0 + \alpha_1, \dots, \alpha_0 + \dots \alpha_k\}$. Moreover, either*
   1. [**a**] *All roots in Ψ are long, and $\Delta = A_{k+1}$.*
   2. [**b**] *Ψ contains a unique short root, $p = 2$, $\Delta = \mathrm{B}_{k+1}$ or G_{k+1} and $\Phi = \mathrm{C}_n$, F_4 or G_2*
2. [**b**] *All roots in Ψ are short, $\Phi = \mathrm{G}_2$, $p = 2$, $|\Psi| = 2$ or 3 and $<\alpha, \beta> = -1$ for all $\alpha \neq \beta \in \Psi$.*

Proof: (a): Let $\beta_0, \dots, \beta_m$ be the long roots in Ψ. Then by 7.1.14 $<b_i, b_j> = 1$ for all $1 \leq i < j \leq m$. Put $\alpha_0 = \beta_0$ and $\alpha_i = \beta_i - \beta_{i-1}$ for all $1 \leq i \leq m$. Then clearly $(\alpha_0, \alpha_1, \dots, \alpha_m)$ has diagram A_{m+1}. If Ψ contains only long roots we conclude that (a:1:1) holds. Suppose next that Ψ contains a unique root β which is not long. Then by 7.1.14 $<\beta_i, \beta> = 1$ for all $1 \leq i \leq m$. Put $\alpha_{m+1} = \beta - \beta_m$. Then $<b_i, a_{m+1}> = 0$ for all $0 \leq i < m$ and $<\beta, \beta_m> = -1$. Thus $<a_{m+1}, a_i> = 0$ for all $0 \leq i < m$ and $<a_{m+1}, a_m> = -1$. Note also that a_{m+1} is short and so (a:1:2) holds.

Suppose finally that Ψ contains two distinct roots α and β which are not long. Then by 7.1.14, $p = 2$, $\Phi = G_2$ and $<\alpha, \beta> = -1$. If $|\Psi| = 2$, then (a:2) holds. So assume $\delta \in \Psi \setminus \{a, \beta\}$. Suppose that δ is long, then by 7.1.14, $<\alpha, \delta> = <\beta, \delta> = 1$ and so $<\alpha + \beta, \delta> = 2$. But $\alpha + \beta$ is a short root and we obtain a contradiction.

So δ is short. Thus by 7.1.14 we get $<\alpha, \delta> = <\beta, \delta> = -1$ and so $<\alpha + \beta, \delta> = -1$. Hence $\delta = -(\alpha + \beta)$, δ is unique, $|\Psi| = 3$ and (a:2) holds.

(**??**): □

7.2 Quadratic modules for Groups of Lie Type

Definition 7.2.1 [**A**] *quadratic system is a tuple (M, V, A, D, p) such that*

(a) [**a**] *M is a finite group.*

(b) [**b**] *p is a prime and V an irreducible faithful $GF(p)M$-module.*

(c) [**c**] *D is a p-subgroup of M with $A \leq Z(D)$ and $|D| > 2$.*

(d) [**d**] *$M = \langle A^M \rangle D$.*

(e) [**e**] *$[V, A, D] = 0$.*

The purpose of this section is to study and (under some extra assumptions) classify quadratic system.

Lemma 7.2.2 [**[V,D,A]=0**] *Let (V, M, A, D, p) be a quadratic system. Then* *(a)* [**a**] $[V, D, A] = 0$.

(b) [**b**] $M = O^p(M)D$.

Proof: (a) By the definition of a quadratic system $[V, A, D] = 0$ and $A \leq Z(D)$. Thus $[A, D, V] = 0$ and the Three Subgroup Lemma 2.0.1 implies $[D, V, A] = 0$.

(b) Since $M = \langle A^M \rangle D$, $M = \langle D^M \rangle$. So (b) follows from 2.0.2 applied to $M/O^p(M)$. □

Lemma 7.2.3 [**imprimitive quadratic systems**] *Let (M, V, A, D, p) be a quadratic system and suppose that Δ is a system of imprimitivity for M on V. Then*

(a) [**a**] *$p = 2$ and A acts non-trivially on Δ.*

(b) [**b**] *$|D/\mathbb{C}_D(W)| = 2 = |W^Q|$ for all $W \in \Delta$ with $A \not\leq \mathbb{N}_M(W)$.*

(c) [**c**] *$O^p(M)$ acts transitively on Δ.*

Proof:

Since V is faithful and $V = \sum \Delta$, there exists $W \in \Delta$ with $[W, A] \neq 0$. Suppose first that A acts trivially on Δ. Then $0 \neq [W, A] \leq C_W(D)$ and so D normalizes W. Since $M = \langle A^M \rangle D = C_G(\Delta)D$ we conclude that M normalizes W, a contradiction to the irreducibility of V.

So A acts non-trivially on Δ. Let W with $A \not\leq N_M(W)$. $[W, A, D] = 0$ implies $|W^A| = W^D| = p = 2$. Also $[W, \mathbb{N}_D(W)] \leq C_W(A)$ and so $[W, \mathbb{N}_D(W)] = 0$. Therefore $|D/C_D(W)| = 2$.

Suppose that $O^p(M)$ does not act transitively on Δ. Replacing Δ by $\{\sum W^{O^p(M)} \mid W \in \Delta\}$ we may assume that $O^p(M)$ acts trivially on Δ. Thus by 7.2.2(b) $M = C_M(\Delta)D$. Hence $\Delta = W^M = W^D$, $|\Delta| = 2$, $C_D(\Delta) = C_D(W) \leq C_M(V) = 1$ and so $|D| = 2$ a contradiction to the assumption. □

Lemma 7.2.4 [**e-linear**] *Let (M, V, A, D, p) be a quadratic system and suppose that there exists a field $\mathbb{E}$ such that V is a vector space over $\mathbb{E}$ and M acts $\mathbb{E}$-semilinear on V. Then M is $\mathbb{E}$-linear on V.*

Proof: Let $1 \neq a \in A$ and let σ be the (maybe trivial) field automorphism induced by a on $\mathbb{E}$. Let $\mathbb{E}_\sigma$ be the fixed field of σ in $\mathbb{E}$. As a is quadratic on V, $e - e^\sigma \in \mathbb{E}_\sigma$ for all $e \in \mathbb{E}$. It easy to see that this implies that $\mathbb{E} = \mathbb{E}_\sigma$ or $p = 2$ and $\mathbb{E}$ has dimension 2 over $\mathbb{E}_\sigma$ has index two in F. Moreover, $[V, a]$ is an E_σ-subspace centralized by D. So D is E_σ-linear and we may assume that $\mathbb{E}_\sigma \neq \mathbb{E}$. Since $[V, C_D(\mathbb{E})]$ is an $\mathbb{E}$-space centralized by a, $C_D(\mathbb{E}) = 1$. Thus D is isomorphic to a subgroup of $\mathrm{Aut}_{\mathbb{E}_\sigma}(\mathbb{E}) \cong C_2$, a contradiction to $|D| \geq 2$. □

Lemma 7.2.5 [**OpM irreducible in quadratic system**] *Let (M, V, A, D, p) be a quadratic system. Then $O^p(M)$ acts irreducibly on V.*

Proof: By 7.2.3 $O^p(M)$ is homogenous on V. So the lemma follows from the facts that V contains precisely $q^n - 1$ irreducible $O^p(M)$-submodules and that $M/O^p(M)$ is ap-group, see also **??**. □

Definition 7.2.6 [**dtendec**] *Let $\mathbb{K}$ be a field, H a group and V a $\mathbb{K}H$-module. Then a tensor decomposition of V for H is a tuple $(\mathbb{F}, V_i, i \in I)$ such that*

(a) [**a**] *$F \leq \mathrm{End}_K(V)$ is a field with $K \leq F$.*

(b) [**b**] *H acts F-semilinear on V.*

(c) [**c**] *Put $E = C_H(F)$ (the largest subgroup of H acting F-linear on V). Then V_i is an FE-promodule.*

(d) [**d**] *As FE-modules, V and $\bigotimes_F \{V_i \mid i \in I\}$ are isomorphic.*

Lemma 7.2.7 [**qtp**] **Comment:need to allow the case that D acts on I, giving** $O_4^+(q)$ *Let D be a group with $|D| \geq 3$. $1 \neq A \leq Z(D)$, K a field with $\mathrm{char}\, K = p$, p a prime, V a faithful KD-module with $[V, A, D] = 0$ and $(F, V_i, i \in I)$ a tensor decomposition of V for D. Then D acts F-linear and one of the following holds:*

1. [**1**] *There exists $i \in I$ so that $[V_i, A, D] = 0$ and D acts trivially on all other V_j's.*

2. [**2**] *$p = 2$, D is F-linear and there exist $i, j \in I$, $a_k \in \mathrm{End}_F(V_k)$ with $a_k^2 = 0$ (k=i,j)and a monomorphism $\lambda : D \to (F, +)$ so for $q \in D$,*

   (a) [**a**] *For $k = i, j$, q acts on V_k as $1 + \lambda(q)a_i$.*

   (b) [**b**] *D centralizes all V_s's with $s \neq i, j$.*

Proof: Note first that as A acts quadratically on V, A is an elementary abelian p-group. Also $[V, A, D] = 0$ and $[D, A] = 1$. So the three subgroup lemma implies that $[V, D, A] = 1$.

By 7.2.4 M acts $\mathbb{F}$-linear on V. Since A is a p-group, we may assume that the V_i's are actually FA-modules and not only promodules. If D acts trivially on some V_k, V is a direct sum of copies of the FD-module $\bigotimes_F \{V_i \mid i \in I - k\}$. So the latter has the same properties as V. Thus we may assume fom now on that D acts non-trivially on each V_i. If $|I| = 1$, then 1. holds

Suppose next that $|I| = 2$ and say $I = \{1, 2\}$. Note that

$$[C_{V_1}(A) \otimes V_2, A] = C_{V_1}(A) \otimes [V_2, D].$$

D acts as scalars on $[V_2, A]$ and $[V_1, A]$. Hence we may choose the promodules V_1 and V_2 so that $[V_i, A, D] = 0$ for $i = 1, 2$. For $q \in D$ let q_i be the endomorposim $q - 1$ of V_i. Then $z_i q_i = 0$. Moreover, in $\mathrm{End}_F(V_1 \otimes V)$,

$$z - 1 = (1 + z_1) \otimes (1 + z_2) - 1\otimes = z_1 \otimes 1 + 1 \otimes z_2 + z_1 \otimes z_2.$$

Thus $[V, z, q] = 0$ implies

$$z_1 \otimes q_2 = -q_1 \otimes z_2$$

If $z_1 = 0$ then as V is faithful, $z_2 \neq 0$. Thus the previuos equation implies $q_2 = 0$ for q, a contradcition to the assumption that D does not centalize V_2. Hence both z_1 and z_2 are not zero. Choosing $q = z$ we see that $p = 2$. Hence for arbitray q, $q_1 = \lambda(q)z_1$ and $q_2 = \lambda(q)z_2$ for some $\lambda(q) \in F$. Thus 2. holds in this case.

Suppose now that $|I| \geq 3$. Say $1, 2 \in I$ and but $W = \bigotimes_F \{V_i \mid i \in I \setminus \{1, 2\}$. Then $V \cong (V_1 \otimes V_2) \times W$. Then by the prviuos case D acts faithfully on $V_1 \otimes V_2$ $z - 1$ and $q - 1$ are linear dependent on $V_1 \otimes V_2$. Let $\lambda = \lambda(q)$ be as above. Then on $v_1 \otimes v_2$

$q - 1 = (1 + \lambda z_1) \otimes (1 + \lambda z_2) - 1 \otimes 1 = \lambda(z_1 \otimes 1 + 1 \otimes z_2 + \lambda z_1 \otimes z_2)$.

On the otherhand $z - 1 = z_1 \otimes 1 + 1 \times z_2 + z_1 \otimes z_2$ and we conclude that $\lambda = 0, 1$ and so $|D| = 2$, a contradiction. □

Lemma 7.2.8 [**quadratic on exterior powers**] *Let $\mathbb{F}$ be a field with $p := \operatorname{char} \mathbb{F} \geq 0$, A a group, V a faithful, finite dimensional $\mathbb{F}A$-module. Put $n = \dim_{\mathbb{F}} V$, let $2 \leq m \leq n-2$ and suppose that A acts unipotenly on V and quadratically on $\bigwedge^m V$. Then A is an elementary abelian p-group and one of the follwing holds.*

1. [**a**] $\dim[V, A] = 1$.

2. [**b**] $\dim V/C_V(A) = 1$.

3. [**c**] *$p = 2$, $m \in \{2, \dim V - 2\}$ and $A \subseteq 1 + \mathbb{F}t$ for some $t \in \operatorname{End}_{\mathbb{F}}(V)$ with $t^2 = 0$.*

4. [**d**] *$p = 2$, $V = X \oplus Y$, where X and Y are $\mathbb{F}A$-submodules of V with $\dim X = 4$ and $[Y, A] = 0$. Moreover, put $U = C_X(A)$. Then $U = [V, A]$ is 2-dimensional and A is contained in an isotropic subspace of $\operatorname{End}_{\mathbb{F}}(X/U, U)$.*

5. [**e**] *$p = 2$, $m = 2$, $\dim V = 4$ and A acts cubic but not quadratic on V.*

6. [**f**] *$p = 2 = |A|$.*

Proof: Suppose first that all elements in A are transvections. Then (1) or (2) holds. So we may assume that there exists $d \in A$ with $\dim[V, d] \geq 2$.

Suppose A does not act quadratically on V. Then there exists $D \leq A$ and an $\mathbb{F}D$ submodule X in V such that D is not quadratic on V and if we put $k = \dim U$, then either $p = 2$, $|D| = 4$ and $k = 4$ or $p \neq 2$, D is cylic and $k = 3$. Let $l = k-1$ if $m \geq k-1$ and $l = 1$ if $m < k$. Then D does not act quadratically on $\bigwedge^l X$. Suppose that $m - l \leq n - k$. Then $\bigwedge^l X \otimes \bigwedge^{m-1} V/X$ is isomorphic to an $\mathbb{F}D$ section of $\bigwedge^m V$ and we obtain a contradiction to 7.2.7. Thus $n-3-l \geq m-l-1 \geq n-k \geq n-4$. Thus $l = 1$, $n-2 = m$ and $k = 4$. Sy by choice of l, $m \leq k-2 = 2$. Hence $n = 4$. Let $D = \langle a, b \rangle$. Then $C_V(D)$ is 1-dimensional and so $C_V(D) = C_V(A)$. Moreover, $[V, D] = C_V(a) + C_V(b)$ and $C_V(a)/C_V(A)$ is 1-dimensional. Thus $[V, D, A] \leq C_V(A)$, A is cubic on V and (5) holds.

So we may assume from now on that A acts quadratically on V.

Suppose that $p \neq 2$. Let X be 2-dimensional non-trivial $\mathbb{F}\langle d\rangle$-submodule in V. Then d acts quadratically on $X \bigotimes \bigwedge^{m-1} V/X$ and we conlude from 7.2.7 that d centralizes $\bigwedge^{m-1} V/X$ and so also V/X. Thus $[V,d] \leq C_X(d)$ and so $[V,d]$ is 1-dimensional, a contradiction to the choice of d.

Thus $p = 2$ and we may assume that $|A| \geq 4$. Let $1 \neq a, b \in A$ and put $D = \langle a, b\rangle$. Suppose that $C_V(a) \not\leq C_V(b)$. Then there exists a non-trivial 2-dimensional $\mathbb{F}D$-subspace X in V with $[X,a] = 1$. Since D acts quadratically on $X \bigotimes \bigwedge^{m-1} V/X$ we conclude from 7.2.7 that a centralizes V/X. Thus $[V,a] \leq C_X(A) = [X,b]$. Since this hold for all such X we get $[V,a] = [C_V(a), b]$, a is a transvection and $\dim[V,b] \leq 2$. In particular, $a \neq d$ and so $C_V(d) = C_V(A)$. By a dual argument, $[V,d] = [V,D]$. If $[V,d]$ is 2-dimensional it is easy to verify that (4) holds.

So assume that $\dim[V,d] \geq 3$. Hence $d \neq a$. If $C_V(a) \neq C_V(d)$ we conclude that $C_V(a) \not\leq C_V(d)$, a contradiction. Thus $C_V(a) = C_V(d)$ for all $1 \neq a \in A$.

Replacing V by V^* and m by $n-m$ if necessary we may assume that $n \geq 2m$.

Let $t = d - 1 \in \mathrm{End}_{\mathbb{F}}(V)$.

Suppose that $A \subseteq \mathbb{F}d$. Then $V = V_0 \oplus V_1 \oplus V_k$, where A centralizes V_0, $k \geq 3$ and $V_1, \dots V_k$ are pairwise isomorphic non-trivial 2-dimensional $\mathbb{F}A$-submodules. If $m \in \{2, n-2\}$, then (3) holds. So suppose for a contradiction that $3 \leq m \leq n-3$. Let $Y = V_0 + V_3 + \dots V_k$. Then $\dim Y = n - 6 \geq 2m - 6 \geq m - 3$. Thus $\bigwedge^m V$ has a section isomorphic to $V_1 \otimes V_2 \otimes V_3 \otimes \bigwedge^{m-3} Y$ and we obtain a contradiction to 7.2.7.

So we may assume that there exists $a \in A$ with $a \notin \mathbb{F}d$. Thus there exists $x \in V$ with $\mathbb{F}[x,a] \neq \mathbb{F}[x,d]$. Put $D = \langle a, d\rangle$. Since $C_V(a) = C_V(d)$ we conclude that $X := \mathbb{F}\langle x^D\rangle$ is 3-dimensional. Since $n \geq 2m$ we have $\dim V/X = n-3 \geq 2m-3 \geq m-1$. Moreover, equality holds only for $n = 2m$ and $m = 2$. But $n \geq 2\dim[V,d] \geq 6$ and so $m - 1 < \dim V/X$. Since $X \otimes \bigwedge^{m-1} V/X$ is a section of $\bigwedge^m V$ we conclude from 7.2.7 that D centralizes V/X. Thus $[V,D] \leq C_X(D)$ and $[V,D]$ is at most 2-dimensional. This contradiction completes the proof of 7.2.8. □

Definition 7.2.9 [**strong quadratic**] *Let $M \in \mathrm{Lie}_p$ and V a faithful $\mathbb{F}_p M$-module. Then V is called strongly quadratic if there exists $A \leq D \leq M$ such that*

(i) [**a**] *(M, V, A, D, p) is a quadratic system.*

(ii) [**b**] *If $p = 2$ then $|\Phi_{A^g}| \geq 2$ for some $g \in \hat{M}$ with $A^g \in U$.*

Let (M, V, A, D, p) be a quadratic system, where M is a group of Lie type. Then we may assume that D is a subgroup of the unipotent group U. As in **??** for $X = D, A$ let

$$\Phi_X = \{\alpha \in \Phi^+ \mid X \cap U_\alpha^+ \not\leq U_\alpha^-\}$$

and

$$T_X = \sum_{\alpha \in \Phi_X} \mathbb{K}\mathfrak{G}_\alpha \leq \mathfrak{g}_\Phi(\mathbb{K}).$$

Theorem 7.2.10 [**same characteristic quadratic systems**] *Let $M \in \mathrm{Lie}_p$ and V an irreducible, strongly quadratic $\mathbb{F}_pM$-module. Then M and V are as listed below.*

1. [**1**] *M is a quotient of $SL_n(\mathbb{K})$ or $SU_n(\mathbb{K})$ and $\lambda = \lambda_i$ for some $1 \leq i \leq n$.*
2. [**2**] *$M \cong \Omega_{2n+1}(\mathbb{K})$, $p \neq 2$ and $\lambda = \lambda_1$ or λ_n and $M \cong Spin_{2n+1}(\mathbb{K})$.*
3. [**3**] *$M \cong Sp_{2n}(\mathbb{K})$ and $\lambda = \lambda_i$ for some $1 \leq i \leq n$.*
4. [**4**] *$M \cong \Omega^{\pm}_{2n}(\mathbb{K})$ and $\lambda = \lambda_1, \lambda_{n-1}$ or λ_n.*
5. [**5**] *$M \cong {}^3\mathrm{D}_4(\mathbb{K})$ and $\lambda = \lambda_1$.*
6. [**6**] *$M \cong E_6(\mathbb{K})$ and $\lambda = \lambda_1$ or λ_6 or ${}^2\mathrm{E}_6(\mathbb{K})$ and $\lambda = \lambda_1$.*
7. [**7**] *$M \cong E_7(\mathbb{K})$ and $\lambda = \lambda_1$.*
8. [**8**] *$M \cong G_2(\mathbb{K})$ and $\lambda = \lambda_1$ or $p = 3$ and $\lambda = \lambda_1$ or λ_2.*
9. [**9**] *$M \cong F_4(\mathbb{K})$ and $\lambda = \lambda_1$ or $p = 2$ and $\lambda = \lambda_1$ or λ_4.*

Proof: The strategy of the proof is to translate the fact that we have a quadratic system into the fact that we have a quadratic tuple for a Lie algebra related to M and then to use the classification of quadratic tuples.

Let $\mathbb{F} = End_{\mathbb{F}_pM}(V)$ and set $W = V \otimes_{\mathbb{F}} \mathbb{E}$ where $\mathbb{E}$ is the algebraic closure of $\mathbb{F}$. Then W is an irreduzible and faithful $\mathbb{E}M$-module, therefore $W = W(\lambda)$ for some weight λ and

$$W \cong \otimes_{i=0}^{a-1} W(\mu_i)^{(p^i)},$$

where $|\mathbb{K}| = q = p^a$ and $\lambda = \sum_{i=0}^{a-1} p^i \mu_i$ with μ_i p-restricted weights for $0 \leq i \leq a-1$, see ...

By 6.2.4 the modules $W(\mu_i)^{(p^i)}$ are irreducible modules for $\mathfrak{g}_\Phi(\mathbb{E})$, for $0 \leq i \leq a-1$. We claim that we may assume that $W_1 := W(\mu_1)$ is a root faithful module for $\mathfrak{g}_\Phi(\mathbb{E})$.
Assume that W_1 is not a root faithful module for $\mathfrak{g}_\Phi(\mathbb{E})$. Then Φ is of type B_n, C_n, F_4 and $p = 2$ or Φ is of type G_2 and $p = 3$, see 6.1.7. In all these cases there exists an automorphism of M which induces a bijection from Φ onto Φ^*. The Lie algebra $\mathfrak{g}_{\Phi^*}(\mathbb{E})$ acts faithfully on W_1, see 6.1.7. Therefore we may assume that $\mathfrak{g}_\Phi(\mathbb{E})$ acts root faithfully on W_1.

Now 7.2.7 implies that either

(a) [**1**] $V \cong V(\mu_i)^{(p^i)}$ for some p-restricted weight μ_i or

(b) [**2**] $p = 2$ and $V \cong V(\mu_i)^{(p^i)} \otimes V(\mu_j)^{(p^j)}$.

Assume that (2) holds. Then, as $p = 2$, in fact $|\Phi_D| \geq 2$. Let α and β be two different elements in Φ_D such that $\alpha < \beta$ and let g_α and g_β be elements in D such that $g_\alpha \in U^+_\alpha \setminus U^-_\alpha$ and $g_\beta \in U^+_\beta \setminus U^-_\beta$. Then by 7.2.7 there exists $k_\alpha, k_\beta \in \mathbb{K}$ and $a_l \in End_{\mathbb{K}}(V_l)$ such that g_x acts on V_l as $1 + k_x a_l$ for $x \in \{\alpha, \beta\}$ and $l \in \{i, j\}$. Hence g_α acts on $V_i^{(p^i)}$ and on $V_j^{(p^j)}$ as

$$\frac{k_\alpha}{k_\beta}(g_\beta - 1).$$

Now 6.3.4(5) implies that $\mathfrak{G}_\alpha$ acts trivially on both, V_i and V_j. As we saw above we may assume that $\mathfrak{G}_\alpha$ does not act trivially on both, V_i and V_j, which is a contradiction. Hence (1) holds.

Thus W is a p-restricted $\mathbb{E}M$-module and by 6.2.4 it is a root faithful and irreducible $\mathfrak{g}_{\Phi_D}(\mathbb{E})$-module, as well, which admits by 6.3.4a quadratic tuple. If Φ_D contains a long root, then by 7.1.7 W is quadratic. Hence if Φ_D contains a long root, then by 7.1.3 we have the possibilities (1.) – (9.) of the assertion.

If M is a twisted group and of type B_2, F_4 or G_2, then by our choice of the ordering on Φ, the set Φ_D consists only of short roots, see 6.3.3.

Hence we may assume that Φ_D consists only of short roots. Then by 7.1.10, 7.1.11, 7.1.12 and 7.1.13 $p = p_\Phi$, Φ is of type $C_n, n \geq 3$ and $\lambda = \lambda_1$ or $\lambda = \lambda_1 + \lambda_n$ or $p \neq p_\Phi$, Φ is of type B_n, C_n or G_2 and $\lambda = \lambda_n, \lambda_1, \lambda_1$, respectively. If Φ is of type $C_n, \neq 3$ and $\lambda = \lambda_1 + \lambda_n$, then by **??** $V(\Lambda) \cong V(\lambda_1) \otimes V(\lambda_n)$, which is not possible as we saw above.

These cases are listed in (2.), (3.) and (8.) of the assertion. □

Theorem 7.2.11 [**same characteristic quadratic systems with outer automorphism**] *Let (M, V, D, A, p) be a quadratic system such that*

(a) [**a**] *$F^*(M)$ is a quotient of ${}^\sigma G_\Phi(\mathbb{K})$ and* $\operatorname{char} K = p$.

(b) [**b**] *$D \not\leq F^*(M)$.*

Then $p = 2$, $M = O^\epsilon_{2n}(\mathbb{K}_\sigma)$ and V is the corresponding natural module.

Proof:

Let $H = F^*(M)$. By 7.2.5 we have that H acts irreducibly on V. Let $\mathbb{F} = \operatorname{End}_H(V)$. Then by 7.2.4, M acts $\mathbb{F}$-linear on V. Let $\mathbb{E}$ be the algebraic closure of $\mathbb{F}$ and $W = V \otimes_\mathbb{F} \mathbb{E}$. Then W is a simple $\mathbb{F}H$-module.

By the Strong Steinberg Tensor Product Theorem **??** W is as an $\mathbb{E}H$-module isomorphic to $W = \bigotimes_{\sigma \in I} V(\lambda_\sigma)^\sigma$, where I is a set of Frobenius automorphisms of L and λ_σ is a non-zero p-restricted weight. Moreover, the extension $\hat{M}$ of M preserves this tensor decomposition and I is invariant under D via right multiplication.

Suppose first that D acts non-trivial on I. Then by 7.2.7 we conclude that $|I| = 2$ and $\dim V(\lambda_\sigma) = 2$ for all $\sigma \in I$. Thus $\Phi = A_1$, $N := V(\lambda_\sigma)$ is the natural module for $\hat{H}$ and $\mathbb{F} = \mathbb{K}$. Since $C_D(I)$ acts $\mathbb{E}$-linear on N we have that $C_D(I) \leq H$. So the outer automorphism group induced by D on H is generated by a field automorphism τ of order 2. Since $I = \{\sigma, \sigma\tau\}$ we conclude that $W = (N \otimes N^\tau)^\sigma$ and so $M \cong O_4^-(\mathbb{K}_\tau)$ and V is the natural $O_4^-(\mathbb{K}_\tau))$-module.

Suppose next that D acts trivially on I but $|I| \geq 2$. Then by **??** $|I| = 2$ and D acts linearly dependently on V_σ for all $\sigma \in I$. By induction on $|I|$ we conclude that $\Phi = D_n$, $p = 2$ and $V(\lambda_\sigma)$ is the natural module. It follows, if $a \in D$, then $[V(\lambda), a]$ is even dimensional if and only if $a \in H$. As $|DH/H| = 2$ and $|D| \geq 3$ we have $D \cap H \neq 1$. And we obtain a contradiction to the linear dependency of D.

Suppose finally that $|I| = 1$. It follows from **??** the outer automorphism group induced by H is a standard graph automorphism of order p. Also Φ is of type A_n, D_n or E_n.In particular, $|DH/H| = p$ and $p \in \{2, 3\}$. Moreover, the extensions of the $\mathbb{E}H$-module W to $G = G_\Phi(\mathbb{E})$ and to the Lie-algebra $\mathfrak{g}_\Phi(\mathbb{E})$ are invariant under M.

Since D is a p-group we may assume that $D \leq U\langle g\rangle$, where $U = \prod_{\alpha\in\Phi^+} X_\alpha$ is the standard maximal unipotent subgroup of G and g is the standard graph automorphism.

1° [**1**] *Suppose that W is a strong quadratic module for G. Then $\Phi = D_n, n \geq 3$ and W is natural or $\Phi = A_{2m-1}$ and $\lambda = \lambda_m$.*

Since $\lambda = \lambda^g$ this follows immediately from **??**.

2° [**2**] *If $p = 3$, then $A \leq H$.*

Note that A acts quadratically on W. As p is odd, it follows that A centralizes the abelian group $N_G(U)/U$. Since g acts non-trvial on $N_G(U)/U$ we conclude that $A \leq H$.

3° [**3**] $D \cap H \neq 1$.

This follows immediately from $|D| > 2$ and (2°).

In particular, there exists $1 \neq b \in D \cap H$ with $|b| = p$ and a $d \in D \setminus H$. If $A \leq H$ we choose $b \in A$ and if $A \not\leq H$ we choose $d \in A$. So in any case $[W, b, d] = 0$. For $1 \leq i \leq |\Pi|$, let H_i be the maximal parabolic subgroup of H corresponding to $\Pi \setminus \{\alpha_i\}$. Also let U_i be the unipotent radical of H_i. We now split the analysis into four different cases:

Case 1 [**d4**] *The case $p = 3$ does not occur.*

Suppose that $p = 3$ and so $\Phi = D_4$. Suppose that $b \notin U_2$. Then 7.2.7 applied to some chief factor for $M_2/U_2\langle d\rangle$ on W gives a contradiction. Thus $b \in U_2$. It is easy to $[U_2/Z(U_2), d]$ is at least 4 dimensional over $\mathbb{E}$. On the other hand, $C_{U_2}(b)/Z(U_2)$ has codimension at most 1 in $U_2/Z(U_2)$ and thus $[C_{U_2}(b), d] \not\leq \mathbb{E}dZ(U_2)$. Since $[W, b, [C_{U_2}(b), d]] = 0$ we conclude that W is strongly quadratic.

Case 2 [**dn**] *Suppose that $p = 2$ and $\Phi = D_n$ with $n \geq 3$. Then V is the natural module.*

Suppose that $b \in U_1$. If $[C_{H_1}(b), d] \cap U_1 \not\leq \mathbb{K}b$, then W is strongly quadratic and we are done by (1°). So we may assume that $[C_{H_1}(b), d] \cap U_1 \leq \mathbb{K}b$. In particular, $[U_1, d] \leq \mathbb{K}b$, d induces a transvection with center $\mathbb{K}b$ on the orthorgonal space U_1, b is non singular in U_1 and $[d, C_{H_1}(b)] \leq U_1$. Thus $[C_{H_1}(b), d] \leq \mathbb{K}b$. Let $B/\mathbb{K}b = Z(C_{H_1}(b)/\mathbb{K}b)$. Then either $(n, q) \neq (3, 2)$ and $|B| = 2|\mathbb{K}|$, or $(n, q) = (3, 2)$ and $B \cong D_8$. In either case all involutions in $B \setminus \mathbb{K}b$ are transvections on the natural module N for H. If $|d| = 2$ we conclude that $\langle b^{C_H(d)}\rangle$ contains a long root element c with $c \in U_1$. Then $[V, c, d] = 0$ and the preceeding argument applied with c in place of b and realizing that c is not singular in U_1 we get that W is strongly quadratic.

If d has order four, then $(n,q)=(3,2)$ and $|C_N(d)|\geq 8$. Since d is not an involution, $C_N(d)$ is not isotropic and so d centralizes non-degenerate 2-space in N. Thus d is contained in a subgroup L of M isomorphic to $O_4^{\epsilon}(2)$. Let T be a subgroup of L such that d normalizes T and T hasof order 3^2 and 5 if $\epsilon=+$ or $-$, respectively). Let W_1 be an faithful irreducible $T\langle d\rangle$-submodule of W. Then W_1 has four different T-eigenspaces which are permuted transitively by d. Therefore, $[W,b,d]\neq 0$.

Suppose next that $b\notin U_1$. By **??** we have that $[U_1,b]$ is even dimensional, while $[U_1,d]$ is odd dimensional. Thus $C_{U_1}(b)\neq C_{U_1}(d)$. Suppose first that $C_{U_1}(b)\not\leq C_{U_1}(d)$. As $[W,[C_{U_1}(b),d],b]=0$ we conclude that W is strongly quadratic, and we are done. Thus suppose $C_{U_1}(b)\leq C_{U_1}(d)$. Then there exists an element $t\in C_{U_1}(d)\setminus C_{U_1}(b)$ and we can replace b by $[t,b]$. Since $[t,b]\leq U_1$ we are done by the preceeding paragraph.

Case 3 [**an**] *Suppose that $p=2$ and $\Phi=A_n$ with $n\geq 2$. Then $\Phi=A_3=D_3$*

Put $Z=U_1\cap U_2$. Suppose that $n=2$. Then all the involutions in U are contained in $U_1\cup U_2$. Since b is an involution centralized by d and $U_1^d=U_2$ we get that $b\in Z$. Thus $[W,[U_1,b],b]=0$ and W is strongly quadratic, a contradiction.

Thus $n\neq 2$ and we may assume for contradiction that $n\geq 4$. Suppose that $b\notin U_1U_n$. Then by induction we see that every non-central chief factor for $H_1\cap H_n\langle g\rangle$ is a natural orthogonal module and $n=5$. Moreover as b has order two, $2\dim C_{U_1}(b)\geq \dim U_1=n\geq 4$ and so $C_{U_1}(b)\not\leq Z$. Thus $[C_{U_1}(b),d]\neq 1$ and W is strongly quadratic. Thus by (1°), $\lambda=\lambda_3$. But then $M_1\cap M_5$ has a 4-dimensional composition factor.

Thus $b\in U_1U_n$.

Suppose that $b\in Z$. Then $[W,[U_1,g],b]=0$ and so W is strongly quadratic. Thus by **??** $\lambda=\lambda_m$ where $n=2m-1$. But then d acts non-trivially on $C_W(U_1U_n))$ and $C_W(U_1U_n)=[W,b]$, a contradiction.

Thus $b\notin Z$ and so also $b\notin U_1$. Thus $C_{U_1}(b)$ has codimension 1 in U_1 and since $n\geq 4$, $T:=[C_{U_1}(b),d]\not\leq \mathbb{F}bZ$. Since $[W,T,b]=0$, W is strongly quadratic and again $\lambda=\lambda_m$, where $n=2m-1$. In particular, n is odd and so $n\geq 5$ and $m=n+1-m\geq 3$. Let N be the natural module for H. Then $\dim[N,b]=2$ and 7.2.8 shows that $C_N(b)\leq C_T(b)$ and $[N,T]\leq[N,b]$. It follows that TU_1/U_1 is contained in a 1-dimensional subspace of U_1U_n/U_1, a contradiction to $n\geq 4$. □

7.3 Some random results

Lemma 7.3.1 [**half quadratic**] *Let $\mathbb{F}$ be a field with* $\operatorname{char} F=p>0$ *and $p\neq$, let A be a finite abelian group, F an $\mathbb{F}A$-module $\mathcal{D}$ the set of non-trivial quadratically acting elements in A. Suppose that $|\mathcal{D}|\geq\frac{|A^{\#}|}{2}$. The one of the following holds:*

1. [**1**] *A acts quadratically on V.*

2. [**2**] $p = 3$ *and* $|A/B| = 9$ *where* $B = C_A([V, A])$.

Let E be a maximal quadratic subgroup of A. If $E = A$ then (1) holds. So suppose $A \neq E$. Let $|A/E| = p^n$. For $a \in \mathcal{D} \setminus E$ and put $E_a = \{e \in E \mid ea \in \mathcal{D}\}$. Let $e \in E_a$. Then by **??** $\langle e, a\rangle$ is quadratic and we conclude that $E_a = C_E([V, a])$. In particular, E_a is a subgroup of E_a. Note also that $E_a\langle a\rangle$ is quadratic and contains all the quadratic elements in $E\langle a\rangle$ not contained in E. In particular, by maximality of E, $E_a \neq E$. Thus $E_a a$ contains at most $\frac{1}{p}|E|$ quadratic elements.

Hence
$$|\mathcal{D}| \leq |E| - 1 + \frac{p^n - 1}{p}|E|$$

On the otherhand
$$|\mathcal{D}| \geq \frac{1}{2}|A^{\#}| = \frac{1}{2}(p^n|E| - 1)$$

Hence
$$\frac{1}{2}(p^n|E| - 1) \leq |E| - 1 + \frac{p^n - 1}{p}|E|$$
$$(p^{n+1} - 2p^n - 2 - 2p) \leq -\frac{p}{|E|} \leq 0$$
$$(p - 2)(p^n - 2) \leq 6$$

Thus $p = 3$ and $n = 1$. So $A = E\langle a\rangle$ and E_a centralizes both $[V, E]$ and $[V, a]$. Thus $E_a \leq B$. If $E_a < B$, then $A = EB$ or $A = B\langle a\rangle$ and in both cases A acts quadratically, contradicting the maximal choice of E. Thus $B = E_a$ and (2) holds. $\square$

Chapter 8

FF–modules

8.1 FF-modules for Lie algebras

Definition 8.1.1 [**FF Lie algebra**] *A module V for $\mathfrak{g}_\Phi(\mathbb{K})$ is called FF if there exists $\Psi \subseteq \Phi$ such that*

1. [**1**] $\mathfrak{G}_\alpha V \neq 0$ *for all* $\alpha \in \Psi$.

2. [**2**] $\mathfrak{G}_\beta \mathfrak{G}_\alpha V = 0$ *for all* $\alpha, \beta \in \Psi$.

3. [**3**] *dim* $\mathfrak{g}_\Psi V \leq |\Psi|$ *with* $\mathfrak{g}_\Psi = \sum_{\alpha \in \psi} \mathfrak{G}_\alpha$.

Next we classify the FF-modules for groups of Lie type.

Theorem 8.1.2 [**quadratic for Lie algebra**] *Let $\mathbb{K}$ be a field of characterstic $p > 0$, Φ a connected root system and $\mathfrak{g} = \mathfrak{g}_\Phi(\mathbb{K})$ the corresponding algebra. Let $V = V(\lambda)$ be the irreducible restricted $\mathfrak{g}$-module of highest weight $\lambda \neq 0$. If V is an FF-module for $\mathfrak{g}$, then one of the following holds.*

1. [**1**] $\Phi = A_n$, $\lambda = \lambda_1, \lambda_2, \lambda_{n-1}, \lambda_n$.

2. [**2**] $\Phi = B_n$, $\lambda = \lambda_1$; $n = 2, \lambda = \lambda_2$; $n = 3, \lambda = \lambda_3$ *or* $n = 4, \lambda = \lambda_4$ *and* $\Psi = \{e_1 + e_2, e_1 - e_2, e_1, e_1 + e_3\}$.

3. [**3**] $\Phi = C_n$, $\lambda = \lambda_1$; $n \geq 7, p = 2$ *and* $\lambda = \lambda_1 + \lambda_n$.

4. [**4**] $\Phi = D_n$, $\lambda = \lambda_1$; $n = 4, \lambda = \lambda_3, \lambda_4$; $n = 5, \lambda = \lambda_4, \lambda_5$.

5. [**5**] $\Phi = G_2$, $\lambda = \lambda_1$ *and* $p = 2$.

Proof: Suppose first that V is a quadratic module for $\mathfrak{g}$. Then according to 7.1.16 either V is natural or spin or all roots in Ψ are short, $\Phi = G_2, p = 2$, $|\Psi| = 2$ or 3, or 7.1.16(a) 1. holds.

The before last is 5 of the assertion. Assume that V is the natural module for $\mathfrak{g}$. Then we need to rule out $\Phi = E_6, E_7$ and F_4 (see 5.3.2). In these cases Ψ consists of long roots and whenever $\alpha, \beta \in Phi$ with $\alpha \neq \beta$, then $\langle \alpha, \beta \rangle = 1$. As in (the proof of) 7.1.16 we get a tuple of roots $(\alpha_0, \ldots, \alpha_k)$ with $k = |\Psi|$ with diagram A_{k+1}. Now **??** implies that $(\alpha_0, \ldots, \alpha_k)$ is conjugate under the Weyl group to a tuple $(\beta_0, \ldots, \beta_k)$ with diagram A_{k+1} such that $\beta_0 = -\alpha$, α the longest root and $\beta_i, 1 \leq i \leq k$, are elements of a chosen fundamental system of Φ. Hence if $\Phi = E_6, E_7$ or F_4, then $k \leq 5, 7, 3$. In all cases we get a contradiction to 8.1.1 3 (see 7.1.15).

Now let V be a spin module. Then the same argumentation as above yields for $\Phi = B_n$ or D_n that $n - 1 \geq 2^{n-2}$ or $n - 1 \geq 2^{n-3}$ and therefore $n \geq 3$ or $n \leq 5$, respectively, as in 2 or 4. If 7.1.16(a) 1. holds, then we again get the assertion with 5.3.2, **??** and 8.1.1. Now assume that V is not quadratic.

If $\Phi = C_n$ $p = 2$ and Ψ only consists of short roots, then $\lambda = \lambda_1 + \lambda_n$, $\mathfrak{g}_{short}$ is a Lie algebra of type D_n and V is restricted to $\mathfrak{g}_{short}$ the direct sum of two natural modules, see **??**. Then 8.1.1 implies the second statement of 3. If $\Phi = B_4$, V is the spin module and Ψ is as in 2., then 7.1.14 and 8.1.1 yields the assertion.

Now assume that V is a module which is not in the statement of the theorem. Then $\Phi = B_n, n \geq 5$ or $D_n, n \geq 6$ and V is a spin module, see 7.1.14. If $\Phi = D_n$ and $n \geq 5$, then either $\langle \alpha, \beta \rangle > 0$ for all $\alpha, \beta \in \Psi$ or $\Psi = \{\alpha, \beta)$ with $\langle \alpha, \beta \rangle = 0$ and we obtain in both cases a contradiction to 8.1.1. If $\Phi = B_n$, then Ψ contains a long root and either $\langle \alpha, \beta \rangle > 0$ for all $\alpha, \beta \in \Psi$ or for all $\alpha, \beta \in \Psi$ except for one pair of long roots. Hence we see as above that $|\Psi| \leq n$ and therefore $2^{n-2} \leq n$ and $n = 4$, a contradiction. □

Now we study FF-modules for groups of Lie type.

Definition 8.1.3 [**FF Lie group**] *Let $M \in \mathrm{Lie}_p$ and V a faithful $\mathbb{F}_p M$-module. Then V is called FF if there exists a non-trivial elementary abelian subgroup A in G such that $|V/C_V(A)| \leq |A|$.*

The group A will then be called an *offending subgroup* or an *offender*. By Thompson replacement there is an offending subgroup A with $[V, A, A] = 1$. We call such an offender *quadratic*.

Theorem 8.1.4 [**quadratic for Lie groups**] *Let $M \in \mathrm{Lie}_p$ and V an irreducible FF $\mathbb{F}_p M$-module. Then M and V are as listed below.*

Proof: The strategy of this proof is the same as for quadratic modules. Let V be an irreducible FF $\mathbb{F}_p M$-module and $E := \mathrm{End}_{\mathbb{F}_p M}(V)$. Then we consider again the Mk-module $V \otimes_E k$, where k is the algebraic closure of $\mathbb{F}_p$.

Bibliography

[Bo] A.Borel, Springer Lecture Notes 131.

[Ca] R.Carter, Simple groups of Lie type

[LGCP] The Local Structure Of Finite Groups of Local Characteristic p. (2062)

[GLS] D. Gorenstein, R. Lyons and R. Solomon, The Classification of the Finite Simple Groups, Mathematical Surveys and Monographs, 40.3. American Mathematical Society, Providence, RI, 1998.

[St] R. Steinberg, *Lectures On Chevalley Groups (1967) Yale University*

Index