Linear algebraic groups

by
T.A. Springer
Birkhäuser, Boston 1981

Problem:
Die Operation eines Gruppenelements $g \in G$ durch Linkstranslationen auf den Funktionen $f: G \to k$ wird unten mit λ_g bezeichnet. Dabei ist es manchmal sinnvoll

$$(\lambda_g f)(x) = f(gx)$$

zu setzen und manchmal

$$(\lambda_g f)(x) = f(g^{-1}x)$$

(damit man wieder eine Linksoperation erhält).
Vorschlag:
Vielleicht sollte man für die erste Art der Defintion das Symbol L_g verwenden, d.h. die naive Art der Operation werde mit L_g bezeichnet und die 'theoretische' mit λ_g ?

Notation

$\alpha_G: \mathrm{Der}(k[G], k[G]) \to T_e G$ evaluation of the vector fields on the linear algebraic group G at $e \in G$, 3.3.5

a_n nilpotent part of the linear endomorphism a, convention behind 2.4.5

a_s semi-simple part of the linear endomorphism a, convention behind 2.4.5, semi-simple part of the element a of an algebraic group, 2.4.8.

a_u unipotent part of the linear endomorphism a, convention behind 2.4.5 unipotent part of the element a of an algebraic group, 2.4.8.

$\mathbf{B}(G)$ Varietät der Borel-Untergruppen der zusammenhängenden linearen algebraischen Gruppe G, vgl. 7.3.10

$\mathbf{B}_T(G)$ Varietät der Borel-Untergruppen der zusammenhängenden linearen algebraischen Gruppe G, die den maximalen Torus T enthalten,vgl. 8.1.6

$D(B)$ Menge der einfachen Wurzeln bezüglich der Borel-Untergruppe B, vgl. 10.1.10

$\mathrm{End}(V)$ the algebra of endomorphisms of the finite dimensional k-vector space V, 2.4.1

$\mathrm{GL}(V)$ the group of invertible endomorphisms of the k-vector space V, 2.4.1

$\mathfrak{gl}_n$ Lie algebra of n×n-matrices over k, 3.3.9(3)

$\mathfrak{gl}(V)$ Lie algebra of endomorphisms of the vector space V, 3.3.13

G_α die zur Wurzel α gehörige Gruppe vom halbeinfachen Rang 1, vgl. 9.1.8

G_σ set of fixed points of the automorphism $\sigma: G \to G$, 4.4.1

L_g left translation on a linear algebraic group G by the group element g∈G, 2.3.4 first and second part

M_n k-algebra of all nxn -matrices

$M(x)$ fiber of the module M at the point x, 3.2.15

$m(s,t)$ Ordnung des Produkts der Spiegelungen s und t in der Weyl-Gruppe, vgl. 10.2.3

$N_G(H)$ Noramlisator der abgeschlossenen Untergruppe H in der linearen algebratischen Gruppe G, 2.5.11

λ_g left translation on the coordinate ring of a linear algebraic group G by the group element g∈G, 2.3.4 second part

$\mathbb{P}(V)$ projectivation of the k-vector space V, proof of 5.1.4

R_g right translation on a linear algebraic group G by the group element g∈G, 2.3.4 second part

$R^+(B)$ Menge der positiven Wurzeln zur Borel-Untergruppe B, vgl. 9.3.1

ρ_g right translation on the coordinate ring of a linear algebraic group G by the group element g∈G, 2.3.4 second part

$S(B)$ Menge der Spiegelungen zu den einfachen Wurzeln bezüglich der Borel-Untergruppe B, vgl. 10.1.10

σ action on the coordinate ring of a G-space, 2.3.3

$Z_G(D)$ centralizer of the diagonalizable group D in the lineare algebraic group G, 4.4.6

$\mathfrak{Z}_{Lie(G)}(D)$ centralizer of the diagonalizable group D in the Lie group of the linear algebraic group G, 4.4.6

1. Some algebraic geometry

1.9. Some results on morphisms

xxx Eine Anwendung von Zariskis Hauptsatz

Sei f: X → Y ein bijektiver Morphismus algebraischer Varietäten mit folgenden Eigenschaften.

1. X und Y sind irreduzibel.
2. Y ist normal.
3. f ist separabel.

Dann ist f ein Isomorphismus.

Beweis. Nach Zariskis Hauptsatz (vgl Milne, Etale Cohomology) zerfällt f in eine Zusammensetzung

$$f: X \xrightarrow{f'} X' \xrightarrow{f''} Y$$

aus einer offenen Einbettung f' und einen endlichen Morphismus f''. Wir können dabei X' durch die Abschließung des Bildes von f' ersetzen, also annehmen,

4. X' ist irrreduzibel
5. Im(f') liegt dicht in X'.

Wegen der Bijektivität von f gilt nach dem Satz von der Dimension der Faser,

6. dim X = dim Y = dim X'.

Wegen 5 hat die abgeschlossene Menge

$$S := X' - Im(f')$$

eine kleinere Dimension als X'. Dasselbe gilt für das Bild von S in Y. Insbesondere ist

$$f''(S)$$

eine echte abgeschlossen Teilmenge von Y. Außerhalb von f''(S) sind bestehen alle Fasern von f'' aus genau einem Punkt (wegen der Bijektivität von f). Deshalb ist der Separabilitätsgrad von f'' gleich 1. Wegen 3 folgt

$$1 = \deg f'' = [k(X'): k(Y)].$$

Mit anderen Worten, f'' ist birational,

6. $k(X') = k(Y)$.

Als endlicher Morphismus ist f'' affin. Die affinen Koordinatenringe von X' sind daher gerade die Normalisierungen in $k(X') = k(Y)$ der affinen Koordinatenringe von Y. Weil Y normal ist (vgl. 2), muß f'' ein Isomorphismus sein. Wir können also annehmen

$$X' = Y, f'' = Id.$$

Die offene Einbettung f' ist dann aber surjektiv, d.h. f = f' ist ein Isomorphismus.

QED.

Bemerkung

Die Bedingung, daß Y normal ist, kann man nicht weglassen: Man nehme für Y die semikubische Parabel und für f: X → Y die Aufblasung in der Spitze.

1.9.3 Extending ring homomorphism into algebraically closed fields I

Lemma

Let B be an integral domain and A a subring such that B=A[b] for some $b \in B$.

Write

$$B=A[T]/I$$

where I is the ideal of all $f(T) \in A[T]$ with f(b)=0. Denote by $J(I) \subseteq A$ the set of the leading coefficients of the polynomials of I. It is easy to see that J(I) is an ideal. Let $\phi: A \to F$ be a homomorphism into an algebraically closed field F such that $\phi J(I) \neq 0$. Then ϕ can be extented to a homomorphism $B \to F$.

Proof. Let

$$f=f_0 + f_1 T^1 + ... + f_m T^m \in I$$

be a polynomial of minimal degree in I satisfying

$$\phi(f_m) \neq 0.$$

Extend $\phi: A \to F$ to a homomorphism $\phi': A[T] \to F[T]$ mapping the variable T into itself.

Assume that the ideal $\phi'(I) \subseteq \phi'(A[T])$ doesn't contain non-zero constants, hence generates a proper ideal in F[T]. If $z \in F$ is a zero of this ideal,

$$\phi'(I) \cdot F[T] \subseteq (T-z)F[T],$$

then the composition

$$A[T] \xrightarrow{\phi'} F[T] \to F,$$

where the second homomorphism maps T into z, has a kernel containing I, hence factors

$$B=A[T]/I \to F,$$

giving this way the required extension of ϕ to B.

Now assume that $\phi'(I)$ contains a nonzero constant. We will prove that this case is impossible. The assumption means that there is a polynomial

$$g=g_0 + g_1 T + ... + g_n T^n \in I \text{ with } \phi(g_0) \neq 0, \phi(g_i) = 0 \text{ for } i>0.$$

The division algorithm shows that there are polynomials $q,r \in A[T]$ and an integer $d>0$ such that

$$f_m^d g = qf+r \text{ and } \deg r < m.$$

Then $\phi(f_m^d)\phi(g_0) = \phi(q)\cdot\phi(f)+\phi(r)$. Since ϕf has degree $m>0$, this is possible only in case $\phi(q)=0$, so that $\phi(r)$ is also a non-zero constant. Replacing g by r we may assume that

$$n = \deg g < m.$$

If $m=1$, $g \in I$ is a non-zero element of A, contradicting the assumption $A \subseteq B$. So assume $m>1$ and that the assertion of the lemma is true for smaller values of m.

For every polynomial $h=h_0+h_1T+\ldots+h_sT^s$ with $h_s \neq 0$ define $\tilde{h}$ to be

$$\tilde{h} = h_s+h_{s-1}T+\ldots+h_0T = h(\frac{1}{T})\cdot T^{\deg(h)}.$$

Claim: the set $\tilde{I}$ of polynomials $T^a\tilde{h}$ with $h \in I$ and $a \geq 0$ form an ideal of A[T].

Let $h:=h'\cdot T^{a'}+h''\cdot T^{a''}$. Then

$$\begin{aligned}\tilde{h} &= (h'(\frac{1}{T})\cdot T^{-a'}+h''(\frac{1}{T})\cdot T^{-a''})\cdot T^{\deg(h)}\\ &= \tilde{h'}\cdot T^{\deg(h)-\deg(h')-a'}+\tilde{h''}\cdot T^{\deg(h)-\deg(h'')-a''}\end{aligned}$$

showing that the sum of two elements in $\tilde{I}$ is again in $\tilde{I}$.

Now let $h:=h'\cdot h''\cdot T^a$. Then

$$\begin{aligned}\tilde{h} &= (h'(\frac{1}{T})\cdot h''(\frac{1}{T})\cdot T^{-a})\cdot T^{\deg(h)}\\ &= \tilde{h'}\cdot\tilde{h''},\end{aligned}$$

hence the product of an element of $\tilde{I}$ with an arbitrary polynomial is again in $\tilde{I}$. This proves the claim.

Using the claim, we are going to ...

1.9.4 Extending ring homomorphism into algebraically closed fields II

Lemma

Let B be an integral domain and A a subring such that B is of finite type over A. Given any non-zero $b \in B$ there exists some non-zero $a \in A$ such that every homomorphism $\phi: A \to F$ with $\phi(a)\neq 0$ where F is an algebraically closed field can be extented to a homomorphism $\phi: B \to F$ with $\phi(b)\neq 0$.

Proof. Write $B=A[b_1,\ldots,b_r]$. By induction we may assume $r=1$, i.e., $B=A[b_1]=A[T]/I$ for some prime ideal I.

Assume first that I is non-zero. Let $f \in I$ be non-zero of minimal degree and let a' be the leading coefficient of f. The division algorithm applied to $g \in A[T]$ shows,

$$g \in I \Leftrightarrow (a')^d g \text{ for some } d \in \mathbb{N}.$$

Since I is prime and a similar criterion holds in the polynomial ring Q(A)[T], f is irreducible over Q(A).

Now let $g \in I$ represent the given element b. Since $b\neq 0$, $h \notin I$. Since f is irreducible over Q(A), f and h are coprime over Q(A), i.e., there are $u,v \in A[T]$ and $a'' \in A-\{0\}$ with

$$(*) \qquad uh+vf = a''.$$

Claim: $a := a'\cdot a''$ satisfied the the conditions of the lemma.

For, if $\phi(a)\neq 0$, the leading coefficient of $f \in I$ is mapped to something non-zero, hence ϕ can be extented to B by the previous lemma. Passing to the residue classes modulo I, identity (*) gives $u(b_1)b = a''$, hence $\phi(u(b_1))\phi(b) = \phi(a'')\neq 0$, hence $\phi(b)\neq 0$. This settles the case that I is non-zero. The case $I=0$ is easy.

1.9.5. The image of a morphism

Theorem

Let $\phi:X \to Y$ be a morphism of varieties. Then ϕX contains a non-empty open piece of $\overline{\overline{\phi X}}$.

Proof. Using suitable coverings of X and Y by affine open sets one sees that it suffices to consider the case that X and Y are affine. If $X_1, \ldots, X_r$ are the components of X, then $\overline{\overline{\phi X}} = \overline{\overline{\phi X_1}} \cup \ldots \cup \overline{\overline{\phi X_r}}$ and one sees that one can assume X to be irreducible. We may then also replace Y by $\overline{\overline{\phi X}}$. Thus we are reduced to the case that X and Y are affine and irreducible and that $\overline{\overline{\phi X}} = Y$. Given an integral domain $B(:=\mathcal{O}(X))$ and a subring $A(:=\mathcal{O}(Y))$ of B such that B is of finite type over A, it will be sufficient to show that there is some $a \in A$ such that each $p \in D(a)$ is the restriction of some $P \in \operatorname{Spec} B$. For the latter is will be enough to show that the natural homomorphism

$$A \to A/p \subseteq \text{algebraic closure of } Q(A/p)$$

can be extented to a homomorphism on B. But this is the claim of 1.9.4 with b=1.

2. Linear algebraic groups, first properties

Notation:
k is an algebraically closed field.

2.1. Algebraic groups

2.1.1 Definitions(algebraic group, linear algebraic group, homomorphism, direct product

An algebraic group over k is a variety G, which is also a group, such that the maps defining the group structure,

$$\pi:G\times G \to G,\ (x,y)\mapsto xy$$
$$\iota:G \to G,\ x\mapsto x^{-1}$$

are morphisms of varieties. If the underlying variety is affine, then G is called to be a linear algebraic group. These are the ones we shall concerned with (it is common to use the term 'linear' instead of 'affine' in this context).
Let G and G' be algebraic groups. A morphism of varieties $\phi:G \to G'$ is a homomorphism of algebraic groups if it is also a group homomorphism. It is an isomorphism of algebraic groups if it is an isomorphism of varieties and of groups. Automorphisms are defined similarly.

Let G be a linear algebraic group, and put A:=k[G]. Then the group structure of G is defined by algebra homomorphisms

$$\pi^*:A \to A\otimes_k A$$
$$\iota^*:A \to A,$$

and the identity element e gives rise to a homomorphism $A \to k$. These have to satisfy a number of conditions, reflecting the group axioms (see the next exercise).

The underlying set of the product variety $G\times G'$ can be considered to be the set-theoretical product and can be equipped with the usual direct product group structure. This makes $G\times G'$ into an algebraic group, the direct product of the algebraic groups G and G'.
2.1.2 Exercises

(1) Let A,π^*,ι^* and e as above. Denote by $\gamma:G \to G$ the constant morphism $g \mapsto e$. The corresponting algebra homomorphism $\gamma^*:A \to A$ is given by $\gamma^*f=f(e)$. Show that the group axioms for G are expressed by the commutativity of the following diagrams:

$$\begin{array}{ccc} A\otimes A\otimes A & \xleftarrow{\pi^*\otimes id} & A\otimes A \\ {\scriptstyle id\otimes\pi^*}\uparrow & & \uparrow{\scriptstyle \pi^*} \\ A\otimes A & \xleftarrow{\pi^*} & A \end{array} \qquad \begin{array}{ccc} A & \xleftarrow{\iota^*\otimes id} & A\otimes A \\ {\scriptstyle id\otimes\iota^*}\uparrow & \nwarrow id & \uparrow{\scriptstyle \pi^*} \\ A\otimes A & \xleftarrow{\pi^*} & A \end{array}$$

$$\begin{array}{ccc} A & \xleftarrow{\gamma^*\otimes id} & A\otimes A \\ {\scriptstyle id\otimes\gamma^*}\uparrow & \nwarrow id & \uparrow{\scriptstyle \pi^*} \\ A\otimes A & \xleftarrow{\pi^*} & A \end{array}$$

(2) Check that $G\times G'$, as defined above, is indeed an algebraic group.

(3) Let G be an algebraic group and H a closed subset of G which is also a subgroup. Let $\phi:H \to G$ be the inclusion map. There is a structure of algebraic group on H such that ϕ is a homomorphism of algebraic groups.

(4) Define a notion of pre-algebraic group, starting with a prevariety G, instead of a variety. Show that a pre-algebraic group is an algebraic group.

2.1.3 Examples

(1) The additive group

$G=\mathbb{A}^1$, with addition as group operation. This defines a linear algebraic group, with $A=k[T]$. It is called the additive group and denoted $\mathbf{G}_a$. The algebra homomorphisms induced by the group operations are as follows:

$$\pi^*:A \to A\otimes A,\ T \mapsto T\otimes 1+1\otimes T$$
$$\iota^*:A \to A,\ T \mapsto -T$$
$$e:A \to k,\ T \mapsto 0$$

(2) The multiplicative group

$G=\mathbb{A}^1-\{0\}$, with multiplication as group operation, is an algebraic group called the multiplicative group and denoted $\mathbf{G}_m$. Its coordinate ring is $A=k[T,T^{-1}]$ and the group operations induce algebra homomophisms

$$\pi^*:A \to A\otimes A,\ T \mapsto T\otimes T$$
$$\iota^*:A \to A,\ T \mapsto T^{-1}$$
$$e:A \to k,\ T \mapsto 1.$$

If n is any non-zero integer, then $\phi:\mathbf{G}_m \to \mathbf{G}_m$, $x \mapsto x^n$ defines a homomorphism of algebraic groups. If k has characteristic $p>0$, and n is a power of p, then ϕ is an isomorphism of abstract groups but not of algebraic groups (since $\phi^*:A \to A$ is not surjective, see 1.4.8(3)).

(3) The general linear group

Consider the space $\mathbf{M}_n$ of all $n\times n$- matrices to be k^{n^2}. If $x \in \mathbf{M}_n$, let det(x) its determinant. The general linear group $\mathbf{GL}_n$ is the principal open set $\{x \in \mathbf{M}_n \mid \det(x)\neq 0\}$, with matrix multiplication as group operation. Is coordinate ring is

$$A:=k[\mathbf{GL}_n] = k[T_{ij}, D^{-1} \mid i,j=1,...,n]$$

where $D:=\det(T_{ij})$. The group operations induce algebra homomorphisms

$$\pi^*:A \to A\otimes A,\ T_{ij} \mapsto \sum_{h=1}^{n} T_{ih} \otimes T_{hj}$$

$$\iota^*:A \to A,\ T_{ij} \mapsto (T^{-1})_{ij}$$

$$e:A \to k,\ T_{ij} \mapsto \delta_{ij},$$

where T denotes the matrix with T_{ij} at position (i,j).

$\mathbf{GL}_n$ is an irreducible variety of dimension n^2 since so is $\mathbf{M}_n$.

(4) Closed subgroups of the general linear group

Any subgroup of $\mathbf{GL}_n$ which is closed in the Zariski topology, is a linear algebraic group. Here are a number of examples.

(a) finite subgroups.

(b) $\mathbb{D}_n$:=the group of nonsingular diagonal matrices.

(c) $\mathbb{T}_n$:=the group of upper triangular matrices. By definition,

$$\mathbb{T}_n := \{x=(x_{ij}) \in \mathbf{GL}_n \mid x_{ij}=0 \text{ if } i>j\}.$$

(d) $\mathbb{U}_n$:=the group of unipotent upper triangular matrices. By definition,

$$\mathbb{U}_n := \{x=(x_{ij}) \in \mathbb{T}_n \mid x_{ii}=1 \text{ for every } i\}.$$

(e) $\mathbf{SL}_n$:=the special linear group,

$$\mathbf{SL}_n := \{x \in \mathbf{GL}_n \mid \det(x)=1\}.$$

(f) $\mathbf{O}_n$:=the orthogonal group,

$$\mathbf{O}_n := \{x \in \mathbf{GL}_n \mid x\cdot x^T=1\},$$

where x^T denotes the transpose of x.

(g) $\mathbf{SO}_n$:=the special orthogonal group, $\mathbf{SO}_n := \mathbf{SL}_n \cap \mathbf{O}_n$.

(h) $\mathbf{Sp}_{2n}$:=the symplectic group,

$$\mathbf{Sp}_{2n} := \{x \in \mathbf{GL}_n \mid x^T \cdot \begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix} \cdot x = \begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix}\}.$$

(5) Non-linear algebraic groups

As examples of non-linear algebraic groups (not needed in the sequel) we mention the elliptic curves. These are closed subsets of the projective plane $\mathbb{P}^n$. Assuming for convenience that $\mathrm{char}(k)\neq 2,3$ such a group G can be defined as the set

$$G:=\{(x_0,x_1,x_2) \in \mathbb{P}^2 \mid x_0 x_2^2 = x_1^3 + ax_1 x_0^2 + bx_0^3\},$$

where $a,b \in k$ are such that the polynomial T^3+aT+b has no multiple roots.

The neutral element e is $(0,0,1)$. The group operation of G is abelian, and is written additively. It is such that if three distinct points of G are collinear (i.e., if their homogeneous coordinates satisfy a nontrivial linear equation $c_0 x_0 + c_1 x_1 + c_2 x_2 = 0$), then their sum is e. This defines the addition, and it is easy to check that if

$$x=(x_0,x_1,x_2) \in G, \text{ then } -x = (x_0,x_1,-x_2).$$

The addition may, in fact, be given explicitely by formulas, which are, however, not very enlightening. A proof of the associativity of the group operation starting from these formulas would be quite glumsy.
There are better, more geometric ways, to deal with the group structure on such a curve, We refer to [21, p. 321].

2.1.4 Exercises

(1) Let V be a finite dimensional vector space over k. Define a linear algebraic group GL(V) whose underlying abstract group is the group of all invertible linear maps V → V, and which is isomorphic to $\mathbf{GL}_n$ (n=dim V) .

(2) Chech that all subgroups of $\mathbf{GL}_n$ of 2.1.3(4) are indeed closed.

(3) Write A:=k[$\mathbf{SL}_2$] = k[T_1 ,T_2 ,T_3 ,T_4]/(T_1 T_4 -T_2 T_3 -1)=k[t_1 ,t_2 ,t_3 ,t_4] (t_i denoting the residue class of T_i). Let $\pi:\mathbf{SL}_2 \times \mathbf{SL}_2 \to \mathbf{SL}_2$ and $\iota:\mathbf{SL}_2 \to \mathbf{SL}_2$ define the group structure of $\mathbf{SL}_2$, and let B be the subalgebra of A generated by the products t_i t_j (i,j=1,...,4) .

(a) Show that $\pi^*(B) \subseteq B \otimes_k B$ and deduce that there is an algebraic group $\mathbf{PSL}_2$ with coordinate ring B, together with a homomorphism of algebraic groups $\mathbf{SL}_2 \to \mathbf{PSL}_2$ having kernel {+1,-1}. It is not an isomorphism algebraic groups.

(b) Assume char(k)≠2. Then B is the algebra of functions $f \in A$ such that f(-x)=f(x) for all $x \in \mathbf{SL}_2$.

(c) Assume char(k)=2. Then the homomorphism $\mathbf{SL}_2 \to \mathbf{PSL}_2$ of (a) is an isomorphism of abstract groups.

(4) Show that the group $\mathbb{U}_n$ of 2.1.3(4d) is solvable (it is even nilpotent).

2.2. Elementary properties of algebraic groups

2.2.0. The translation isomorphisms

Let G be an algebraic group. If $g \in G$, the maps

$$G \to G,\ x \mapsto gx, \text{ and } G \to G,\ x \mapsto xg$$

are isomorphisms of the variety G. We shall often use this.

2.2.1. The connected component of the identity element

Proposition.

(i) There is a unique irreducible component G^0 of G containing the identity element e; it is a closed normal subgroup of finite index.

(ii) G^0 is the connected component of e, for the Zariski topology.

(iii) Any closed subgroup H of G of finite index contains G^0 .

Proof. (i). Let X and Y be irreducible components of G containing e. Let

$$\pi:G\times G \to G \text{ and } \iota:G \to G$$

be the morphisms defining the group operations of G. Then

$$XY := \pi(X\times Y)$$

is irreducible, and the same is true for its closure $\overline{XY}$. By assumption, e is contained in X and Y, hence $X \subseteq \overline{XY}$ and $Y \subseteq \overline{XY}$, hence $X = \overline{XY} = Y$, the latter being a consequenc of the fact that there is no inclusion relation between irreducible components.

In the special case X=Y we see that $X=\overline{XX}$, hence X=XX, hence X is closed und multiplication. Note that X^{-1} is an irreducible component containing e (since $\iota:G \to G$ is an isomorphism) so

that the above implies $X=X^{-1}$. We have proved that X is a closed subgroup of G. For every $x \in G$, xXx^{-1} is an irreducible component containing e (since conjugation with x is an isomorphism), hence coincides with X. It follows that X is a closed normal subgroup. Every coset xX of X is an irreducible component of G (since multiplication by x is an isomorphism), hence the number of such cosets must be finite. This completes the proof of (i).

(ii). Write $X:=G^0$. The complement of X in G is a union of finitely many cosets of X (see the last assertion of (i)), hence a union of finitely irreducible components. Therefore, G-X is a closed set and X is open (and closed) in G. Moreover, as an irreducible set, X must be connected. Thus X is a maximal conneced subset of G containing e. This proves (ii).

(iii). Let $H \subseteq G$ be a closed subgroup with finite index. Then G-H is the union of finitely many cosets xH. Each such coset being closed, the complement G-H must be closed. Therefore, H is simultaneously open and closed in G. Since e is in H, the connected component of e must be in completely in H, $G^0 \subseteq H$, as claimed.

Remarks and conventions.

(i) It follows from the above Proposition 2.2.1 that for an algebraic group the notions of connectedness and irreducibility coincide. It is usual to speak of a connected algebraic group, and not of an irreducible one. We follow this convention.

(ii) In the sequel, we always denote by G^0 the identity component of an algebraic group G. Dimensions being defined as in 1.8.1, if follows from the above Proposition 2.2.1 that

$$\dim G = \dim G^0$$

2.2.2. Exercises

(1) The groups $\mathbf{G}_a$, $\mathbf{G}_m$, $\mathbf{D}_n$, $\mathbf{U}_n$, $\mathbf{GL}_n$, $\mathbf{SL}_n$ of 2.1.3 are all connected. If char(k)≠2, the group $\mathbf{O}_n$ is not connected (then $\mathbf{SO}_n$ and $\mathbf{Sp}_{2n}$ are also connected, but this requires a bit more work, see 6.14).

(2) The variety V(TU) in $\mathbb{A}^2$ defined by the equation TU=0 is connected, but reducible (hence it cannot be the underlying variety of an algebraic group).

(3) Let G be a connected algebraic group and N a finite normal subgroup of G. Then N lies in the center of G (Hint: let $n \in N$ and consider the morphism $g \mapsto gng^{-1}$ of G into N).

2.2.3. Dense open subsets

Lemma

Let U and V be dense open subsets of G. Then $U \cdot V = G$.

Proof. Let $x \in G$. Then xV^{-1} and U are both open and dense in G, hence they have a non-empty intersection. This means that $x \in UV$.

Remark

Note that if G is connected, every non-empty open subset is dense. In that case we need only require U and V to be open and non-empty.

2.2.4. The closure of a subgroup

Proposition

Let H be a subgroup of G.

(i) Its closure $\bar{G}$ is a subgroup of G.

(ii) If H contains a non-empty open subset of $\bar{H}$, then $\bar{H} = H$.

Proof. (i). Let $x \in H$. Then $H = xH \subseteq x\bar{H}$. Since $x\bar{H}$ is closed, $\bar{H} \subseteq x\bar{H}$, hence $x^{-1}\bar{H} \subseteq \bar{H}$. Since x is arbitrary, $H \cdot \bar{H} \subseteq \bar{H}$.

Now let $x \in \bar{H}$. Then, as we have just seen, $Hx \subseteq \bar{H}$, hence

$$\bar{H}\, x = \bar{\bar{H}x} \subseteq \bar{H}$$

the identity on the right comming from the fact that multiplication by x is an isomorphism. Again, since x is arbitrary, $\bar{H} \cdot \bar{H} \subseteq \bar{H}$. We have proved, $\bar{H}$ is multiplicatively closed. Moreover, since $x \mapsto x^{-1}$ is an isomorphism,

$$(\bar{H})^{-1} = \bar{H^{-1}} = \bar{H}.$$

We conclude that $\bar{H}$ is a group.

(ii). Let $U \subseteq H$ be a non-empty and open in the closure $\bar{H}$. Then H, being a union of translates of U, is also open in $\bar{H}$. But then by 2.2.3, $\bar{H} = H \cdot H = H$.

2.2.5. The image and the kernel of a homomorphism

Proposition

Let $\phi: G \to G'$ be a homomorphism of algebraic groups.

(i) Ker ϕ is a closed subgroup of G.

(ii) ϕG is a closed subgroup of G'.

(iii) $\phi(G^0) = \phi(G)^0$.

Proof. **(i)**. Since ϕ is continuous, Ker $\phi = \phi^{-1}(e)$ is closed in G.

(ii). By 1.9.5 we know that ϕG contains a non-empty open piece of its closure $\bar{\phi G}$, hence ϕG is closed by 2.2.4(ii).

(iii). ϕG is an algebraic group (by (ii)) containing $\phi(G^0)$ as a connected normal subgroup of finite index (by 2.2.1). $\phi(G^0)$ is closed in ϕG by (ii), hence $\phi(G)^0 \subseteq \phi(G^0)$ by 2.2.1(iii). Since $\phi(G^0)$ is connected and $\phi(G)^0$ is the connected component of e, $\phi(G^0) = \phi(G)^0$.

2.3. G-spaces

2.3.1 G-spaces, morphisms of G-spaces, isotrophy groups, regular representations

A G-variety, or G-space, is a variety X, on which G acts as a permutation group, the action being given by a morphism of varieties.

More precisely, there is a morphism of varieties

$$\alpha: G \times X \to X, (g,x) \mapsto g \cdot x,$$

such that $g \cdot (g' \cdot x) = (gh) \cdot x$ and $e \cdot x = x$. The variety X is called homogeneous space for G if it is a G-space on which G acts transitively. If, moreover, the action is simply transitive, X is called a principal homogeneous space.

Let X and Y be G-spaces. A morphism $\phi: X \to Y$ is a G-morphism, or is said to be equivariant, if

$$\phi(g\cdot x)=g\cdot\phi(x) \text{ for } g \in G \text{ and } x \in X.$$

Note that, if Y is a homogeneous space, ϕ is automatically surjective.

Let X be a G-space. If $x \in X$ its orbit is the set

$$G\cdot x := \{g\cdot x \mid g \in G\}.$$

Note that the group G acts transitively on $G\cdot x$. We will see below that orbits are homogeneous spaces (see 4.3.1(i) and 4.3.5(2)).

The isotropy group of $x \in X$ in G is the subgroup

$$G_x := \{g \in G \mid g\cdot x=x\}.$$

Note that G_x is closed since it is the inverse image of x under the morphism $G \to X$, $g \mapsto g\cdot x$.

Let V be a finite dimensional vector space over k. A homomorphism of algebraic groups

$$\phi: G \to GL(V)$$

is called a rational representation of G in V. In this case, V can be considered as a G-space, defining the action by

$$G\times V \to V, (g,v) \mapsto \phi(g)(v).$$

From Exercise 2.3.2(3) below we see that $\mathbb{P}(V)$ can be considered as a $\mathbf{GL}(V)$-space.

G-space structures on G itself

(i) Action by inner automorphisms. Define the action as

$$G\times G \to G, (g,x) \mapsto gxg^{-1}.$$

Note that G cannot be a homogeneous space under this action (except for G={e}).

(ii) Action by left translations. Define the action by

$$G\times G \to G, (g,x) \mapsto gx.$$

Under this action, G is a principal homogeneous space.

(iii) Action by right translations. Define the action as

$$G\times G \to G, (g,x) \mapsto xg^{-1}.$$

Again, G is a principal homogeneous space.

2.3.2 Exercises

(1) Let G be a closed subgroup of $\mathbf{GL}_n$ $(n\geq 1)$. Then $\mathbb{A}^n$ can be made into a G-space, which is not homogeneous.

(2) The action of $G=\mathbf{GL}_2$ on $\mathbb{A}^2$ defines an action of G on $\mathbb{P}^1$ which makes $\mathbb{P}^1$ into a homogeneous space. Describe the isotropy group of a point. The induced action of G on $\mathbb{P}^1\times\mathbb{P}^1$ is not homogeneous, in fact G has 2 orbits in $\mathbb{P}^1\times\mathbb{P}^1$.[1]

---

[1] The diagonal subset $\Delta\subseteq\mathbb{P}^1\times\mathbb{P}^1$ is mapped into itself under the action of G and the same is true for the complement of Δ. Both Δ and its complement are orbit under G: in affine terms this translates into the follow two assertions:

1. For any two non-zero vektors of k^2 there is an element of $\mathbf{GL}_2$ mapping these two vectors into each other.

2. For any two bases of k^2 there is an element of $\mathbf{GL}_2$ mapping these bases into each other.

(3) Generalize the results of (2) to $\mathbf{GL}_n$ and $\mathbb{P}^{n-1}$.

Convention

From now on we assume that G is a linear algebraic group.

2.3.3 Action on the coordinate ring of a G-space

Let X be an affine G-space, and let $\alpha: G\times X \to X$ define its action on X. Then

$$k[G\times X] = k[G]\otimes_k k[X]$$

and α defines an algebra homomorphism

$$\alpha^*: k[X] \to k[G]\otimes_k k[X].$$

Consider the representation

$$\sigma: G \to GL(k[X]),\ g \mapsto (f \mapsto f\circ L_{g^{-1}})$$

of G in the (on the possibly infinite dimensional) vektor space k[X]. Here

$$L_g : G \to G,\ x \mapsto gx,$$

denotes left translation by $g \in G$. From the result that follows we see that the representation σ is locally finite, i.e., that k[X] is a union of finite dimensional subspaces which are $\sigma(G)$-stable.

2.3.4 Local finiteness of the action on the coordinate ring of a G-space

Proposition

Let X be an affine G-space, let $\alpha: G\times X \to X$ define its action on X, and let F be a finite dimensional subspace of k[X].

(i) There is a finite dimensional subspace E of F in k[X] which contains F and is stable under every $\sigma(g)$ with $g \in G$.

(ii) F is stable under every $\sigma(g)$, $g\in G$, if and only if

$$\alpha^*F \subseteq k[G]\otimes_k F.$$

Proof. (i). We may assume that F is 1-dimensional,

$$F = kf$$

for some $f\in k[X]$. Write

$$\alpha^* f = \sum_{i=1}^{n} u_i \otimes f_i \quad (u_i \in k[G],\ f_i \in k[X]).$$

Then

$$\sigma(g)f(x) = f(g^{-1}x) = f(\alpha(g^{-1},x)) = (\alpha^* f)(g^{-1},x) = \sum_{i=1}^{n} u_i(g^{-1})\cdot f_i(x),$$

and we see that every $\sigma(g)f$ is in the subspace

$$E' := \sum_{i=1}^{n} k\cdot f_i$$

of k[X] spanned by the functions f_i. In particular, the subspace

$$E := \sum_{g\in G} k\cdot\sigma(g)f$$

of E' spanned by all functions $\sigma(g)f$ with $g \in G$ is finite dimensional, hence satisfies the requirements of (i).

(ii). Let $f_1, \ldots, f_n$ be a k-linear basis of F. Then if

$$\alpha^*F \subseteq k[G]\otimes_k F,$$

there are functions $u_{ij} \in k[G]$ with

$$\alpha^* f_i = \sum_{j=1}^{n} u_{ij} \otimes f_j$$

for every j. Therefore,

$$(\sigma(g)f_i)(x) = f_i(g^{-1}x) = \sum_{j=1}^{n} u_{ij}\,(g^{-1})f_j(x).$$

This holds for every $x \in X$, i.e.,

$$(\sigma(g)f_i) = f_i(g^{-1}x) = \sum_{j=1}^{n} u_{ij}\,(g^{-1})f_j,$$

and $\sigma(g)f_i$ is in F for every g. This shows that F is stable under the action σ.

Conversely assume that F is stable under σ. As above, let $f_1, \ldots, f_n$ be a k-linear basis of F. Extent it to a k-linear basis $\{f_i\} \cup \{g_j\}$ of k[X]. Then

$$\{1 \otimes f_i\} \cup \{1 \otimes g_j\}$$

is free generating system of $k[G] \otimes_k k[X]$ over k[G].

Let $f \in F$ and write

$$\alpha^* f = \sum_i u_i \otimes f_i + \sum_j v_j \otimes g_j \text{ with } u_i, v_j \in k[G].$$

Then

$$\sigma(g)f = \sum_j u_i\,(g^{-1})f_i + \sum_j v_j(g^{-1})g_j.$$

Since $\{f_i\} \cup \{g_j\}$ is a basis and $\sigma(g)f$ is in F by assumption, $v_j(g^{-1}) = 0$ for every $g \in G$. Hence the functions v_j are identically zero and $\alpha^* f$ is in $k[G] \otimes_k F$ for every $f \in F$. This completes the proof of (ii).

QED.

The action of G on its coordinate ring by left or right translations

Let

$$L: G \times G \to G,\ (g,x) \mapsto L_g(x) := gx,$$

and

$$R: G \times G \to G,\ (g,x) \mapsto R_g(x) := xg^{-1},$$

denote the action of G on itself by left and right translations, respectively. For $f \in k[G]$ define

$$\lambda_g(f) := f \circ L_g \quad \text{and} \quad \rho_g(f) := f \circ R_g.$$

Then $\lambda_{gg'} = \lambda_g \circ \lambda_{g'}$ and $\rho_{gg'} = \rho_g \circ \rho_{g'}$, i.e.,

$$\lambda: G \times k[G] \to k[G],\ (g,f) \mapsto \lambda_g(f) := f \circ L_g,$$

and

$$\rho: G \times k[G] \to k[G],\ (g,f) \mapsto \rho_g(f) := f \circ R_g,$$

are representations of G on the vector space k[G]. These representations are faithfull[2]:

---

[2] i.e., $\lambda: G \to GL(k[G])$ and $\rho: G \to GL(k[G])$ are injective.

if $\lambda_g = id$, then $f \circ L_g = f$ hence $f(g^{-1}) = f(e)$ for every $f \in k[G]$, hence $g^{-1} = e$, i.e., $g = e$. A similar arguments works for ρ.

Note that if $\iota x := x^{-1}$, then

$$\rho(g) = i^* \lambda(g) (i^*)^{-1}.$$

2.3.5 Linear algebraic groups as subgroups of GL_n

Theorem

Let G be a linear algebraic group. Then there is an isomorphism of G onto a closed subgroup of some $\mathbf{GL}_n$.

Proof. Take some finite-dimensional subspace of k[G] generating k[G] as a k-algebra. By the previous result we may assume that this subspace is stable under the action of G on k[G] via left translations λ_g. Let $f_1, ..., f_n \in k[G]$ be a basis of this subspace. Then

$$k[G] = k[f_1, ..., f_n]$$

and

$$f(gx) = (\lambda_g f_i)(x) = \sum_{j=1}^{n} m_{ij}(g) f_j(x)$$

for certain regular functions $m_{ij} \in k[G]$. Then

$$\phi: G \to \mathbf{GL}_n, \; g \mapsto (m_{ij}(g)),$$

is a group homomorphism which is obviously a morphism of linear algebraic groups.[3]

ϕ is injecitive: if $\phi(g) = id$, i.e., $\lambda_g f_i = f_i$ for every i, then $f_i(g) = f_i(e)$ for every i. Since the polynomials f_i generate k[G], $f(g) = f(e)$ for every $f \in k[G]$. In particular, g and e have the same affine coordinates, hence $g = e$.

ϕ is a closed embedding: the algebra homomorphism induced by ϕ on the coordinate rings is given by

$$\phi^*: k[T_{ij}, D^{-1}] \to k[G], \; T_{ij} \mapsto m_{ij}.$$

Since

$$f_i(g) = (\lambda_g f_i)(e) = \sum_{j=1}^{n} m_{ij}(g) f_j(e)$$

for every g, i.e.,

$$f_i = \sum_{j=1}^{n} m_{ij} f_j(e)$$

---

[3] A coordinate free version of ϕ is just the restriction to the finite dimensional subspace

$$kf_1 + ... + kf_n \subseteq k[G]$$

of the infinite dimensional representation

$$\lambda: G \to GL(k[G]), \; g \mapsto \lambda_g,$$

of G by left translations on the coordinate ring of G.

In other words, the polynomials f_i are in the image of ϕ^*. Since these polynomials generate $k[G]$, we see that ϕ^* is surjective. But this means that ϕ is a closed embedding.
QED.

2.3.6 Invariance of the ideal defining a subgroup

Lemma

Let G be a linear algebraic group, let $H \subseteq G$ be a closed subgroup. Then

$$H = \{x \in G \mid \lambda_x I_G(H) = I_G(H)\}$$
$$= \{x \in G \mid \rho_x I_G(H) = I_G(H)\}$$

Here λ_x denotes left translation with x, ρ_x right translation with x, and $I_G(H)$is the ideal of H in $k[G]$.

Proof. It is sufficient to prove the identity for left translations.[4] Note that the set on the right does not change if one replaces the defining identities

$$\lambda_x I_G(H) = I_G(H)$$

by corresponding inclusions

$$\lambda_x I_G(H) \subseteq I_G(H).$$

For $x,y \in H$ and $f \in I_G(H)$,

$$(\lambda_x f)(y) = f(x^{-1} y) = 0,$$

hence $\lambda_x f \in I_G(H)$ for every $x \in H$ and every $f \in I_G(H)$. Conversely, if $\lambda_x f \in I_G(H)$ for every function $f \in I_G(H)$, then

$$f(x^{-1}) = (\lambda_x f)(e) = 0,$$

hence $x^{-1} \in H$, hence $x \in H$.
QED.

2.3.7 Exercise

Let G be a linear algebraic group and X an affine G-variety. Show that there is an isomorphism $\psi: X \to \mathbb{A}^n$ of X onto a closed subvariety of some $\mathbb{A}^n$, and a rational representation $\phi: G \to \mathbf{GL}_n$ such that $\psi(g \cdot x) = \phi(g)\psi(x)$ for $g \in G, x \in X$ (Hint: adapt the proof of 2.3.5).

Solution. As in the proof of 2.3.5 take a finitely generated linear subspace $V \subseteq k[X]$ generating $k[X]$ as an algebra over k and invariant under the action of G via left translations. Let $\dim V = n$ and write

$$V = kf_1 + \ldots + kf_n$$

$$f_i(gx) = \sum_{j=1}^{n} m_{ij}(g)\, f_j(x).$$

Then

$$f_i(ghx) = \sum_{j=1}^{n} m_{ij}(g)\, f_j(hx) = \sum_{j,k=1}^{n} m_{ij}(g) m_{jk}(h) f_k(x)$$

---

[4] The identity for right translation is obtained by replacing G with the group equipped with the dual multiplication $a \circ b := b \cdot a$.

$$= \sum_{k=1}^{n} m_{ik}(gh)\ f_k(x)$$

Comparing coefficients we see that

$$\phi: G \to \mathbf{GL}_n\ ,\ g \mapsto (m_{ij}(g)),$$

is a homomorphism of linear algebraic groups. Moreover, consider

$$\psi: X \to \mathbb{A}^n\ ,\ x \mapsto (f_1(x)\ ,\ldots,f_n(x)\ ).$$

Since the functions f_i generate $k[X]$, this is a closed embedding. By construction, the following diagram is commutative:

$$\begin{array}{ccc} k[G]\otimes k[X] & \xleftarrow{\mu^*} & k[X] \\ \phi^*\otimes\psi^* \uparrow & & \uparrow\ \psi^* \\ k[\mathbf{GL}_n] & \xleftarrow{\nu^*} & k[\mathbb{A}^n] \end{array}$$

for

$$\mu^*\circ\psi^*(T_i) = \mu^*(f_i\ ) = \sum_{j=1}^{n} m_{ij}\otimes f_j$$

and

$$(\phi^*\otimes\psi^*)\circ\nu^*(T_i) = (\phi^*\otimes\psi^*)(\sum_{j=1}^{n} T_{ij}\otimes T_j) = \sum_{j=1}^{n} m_{ij}\otimes f_j$$

Hence we have a commutative diagram

$$\begin{array}{ccc} G\times X & \xrightarrow{\mu} & X \\ \phi\times\psi\ \downarrow & & \downarrow\ \psi \\ \mathbf{GL}_n\times\mathbb{A}^n & \xrightarrow{\nu} & \mathbb{A}^n \end{array}$$

as required. Here μ denotes the action of G on X and ν the natural action of $\mathbf{GL}_n$ on $\mathbb{A}^n$.

2.4 Jordan decomposition

2.4.1 Semi-simple, nilpotent, and unipotent Automorphisms

Let V be a finite dimensional vector space over k. An endomorphism $a: V \to V$ is <u>semi-simple</u> if there is a basis of V consisting of eigen vectors of a. We say that a is <u>nilpotent</u> if $a^N = 0$ for some N and that a is <u>unipotent</u> if a-1 is nilpotent.

Note that if the characteristics p of k is positive, a is unipotent if and only if $a^{p^s} = 1$ for some $s>0$.

We denote by

End(V)	the algebra of endomorphisms of V
GL(V)	the group of invertible endomorphisms of V

If dim V = n we may view End(V) as the algebra M_n of all nxn -matrices and GL(V) as GL_n.

2.4.2 Simultaneous diagonalization

Lemma

Let $S \subseteq M_n$ be a set of commuting matrices.

(i) There is some $x \in GL_n$ such that xSx^{-1} consists of upper triangular matrices.

(ii) If all elements of S are semi-simple, there exists some $x \in GL_n$ such that xSx^{-1} consists of diagonal matrices.

Proof. Let $s:V \to V$ be an Endomorphism and let $W \subseteq V$ be the eigenspace of s belonging to the eigenvalue λ,

$$W := \{x \in V | sx=\lambda x\}.$$

Then W is stable under every endomorphism $s':V \to V$ commuting with s. For, $x \in W$ implies

$$s(s'x)=s's(x)=s'(\lambda x)=\lambda s'(x),$$

i.e., $s'(x) \in W$.

(i). The claim means, there is a flag

$$0=W_0 \subseteq W_1 \subseteq ... \subseteq W_{n-1} \subseteq W_n =V$$

of S-stable linear subspaces $W_i \subseteq V$ with $\dim W_i = i$. We may assume that S is a linear subspace of M_n. Given any non-zero $s \in S$, let $W \subseteq V$ denote any nonzero eigenspace of s. In case all $s \in S$ are scalar multiplications, the claim of the lemma is trivial. Otherwise there is some s, such that W is a proper subspace, which is S-stable because of the assumption about S. The claim follows now by induction on n = dim V.

(ii) is proved similarly, using decompositions of V in a direct sum of eigenspaces of the elements $s \in S$ instead of flags of invariant subspaces.

QED.

2.4.3 Operations with semi-simple, nilpotent, unipotent Endomorphisms

Lemma

Let V be a finite dimensional vector space over k.

(i) The product of two commuting semi-simple (nilpotent, unipotent) endomorphisms of V is semi-simple (nilpotent, unipotent, respectively).

(ii) If $a:V \to V$ and $b:W \to W$ are semi-simple (nilpotent, unipotent), then the same is true for

$$a \oplus b \in End(V \oplus W),\ a \otimes b \in End(V \otimes W),\ a \otimes 1 + 1 \otimes b \in End(V \otimes W).$$

Proof. (i) Use 2.4.2 to repreent the endomorphismus by a upper triangular matrices.

(ii) In the case of the direct sum, use bases of V and W such that a und b have upper triangular matrices.

In the case of the tensor product, note that

$$a \otimes b = a \otimes Id \circ Id \otimes b$$

and the two maps on the right commute, so that the claim follows from (i). As for the claim about

$$a \otimes 1 + 1 \otimes b \in End(V \otimes W)$$

use bases of V and W such that a and b have upper triangular matrices und note that, for a certain basis von $V \otimes W$, the matrix of $a \otimes 1$ is a direct sum of copies of the matrix of a.

QED.

2.4.4 Additive Jordan decomposition

Proposition

Let V be a finite dimensional vector space over k. Let $a \in \mathrm{End}(V)$.

(i) There are unique $a_s, a_n \in \mathrm{End}(V)$ such that

(a) a_s is semi-simple, a_n is nilpotent,

(b) $a_s a_n = a_n a_s$ and

(c) $a = a_s + a_n$

(additive Jordan decomposition).

(ii) There are polynomials $P, Q \in k[T]$ without constant term such that

$$a_s = P(A) \text{ and } a_n = Q(a)$$

for every $a \in \mathrm{End}(V)$ (V fixed).

(iii) If $b \in \mathrm{End}(V)$ commutes with a, then it also commutes with a_s and a_n.

(iv) If $W \subseteq V$ is an a-stable subspace of V, then W is also stable under a_s and a_n, and

$$a|_W = a_s|_W + a_n|_W$$

is the additive Jordan decomposition of the induced endomorphism $a|_W$.

(v) Let $W \subseteq V$ be an a-stable subspace and deonote by $\bar{a}$, $\bar{a}_s$ and $\bar{a}_n$ the linear maps induced by, respectively, a, a_s and a_n on V/W. Then

$$\bar{a} = \bar{a}_s + \bar{a}_n$$

is the Jordan-decomposition of $\bar{a}$.

Proof. Let

$$\det(T \cdot \mathrm{Id} - a) = \prod_i (T - a_i)^{n_i}$$

be the characteristic polynomial of a, the a_i being the distinct eigenvalues of s. Write

$$V_i := \{x \in V \mid (a - a_i)^{n_i} x = 0\}$$

for the maximal subspaces of V, where a reduces to a matrix with one single eigenvalue. Note that V is the direct sum of the subspaces V_i. Since the polynomials $T - a_i$ are relatively prime, the Chinese remainder theorem implies that there is some $P \in k[T]$ with[5]

$$P(T) \equiv a_i \mod (T - a_i)^{n_i}, \qquad P(T) \equiv 0 \mod T.$$

Define a_s to be $a_s := P(a)$. Then all spaces V_i are stable under a_s and

$$a_s|_{V_i} =^{6} a_i \cdot \mathrm{Id}.$$

---

[5] In case all eigenvalues are none-zero, T is another polynomial relatively prime to each of the polnomials $(T - a_i)^{n_i}$. In case some eigenvalue is zero, the corresponding condition follows automatically from the last condition $P(T) \int 0 \mod T$.

[6] The endomorphism $a_s|_{V_i}$ differs from $P(a)|_{V_i}$ by a multiple of $(a - a_i)^{n_i}|_{V_i} = 0$.

It follows that a_s is semi-simple and $a-a_s$ is nilpotent (since a_s is diagonal on V_i with the same unique eigenvalue a_i like a).[7] The statements of the Proposition are now immediate, except for the uniqueness in (i). To prove the latter, let

$$a = b_s + b_n$$

be a second decomposition with b_s semi-simple and b_n nilpotent, both commuting with a. Then from (iii) we see that b_s and b_n commute with a_s and a_n, hence

$$a_s - b_s = b_n - a_n$$

is both semi-simple and nilpotent (by the previous Lemma). It follows $0 = a_s - b_s = b_n - a_n$.

QED.

2.4.5 Multiplicative Jordan decomposition

Corollary

Let $a \in GL(V)$. There are unique $a_s, a_u \in GL(V)$ such that the following conditions are satisfied.

(i) a_s is semi-simple

(ii) a_u is unipotent

(iii) $a = a_s \cdot a_u = a_u \cdot a_s$.
(multiplicative Jordan decomposition).

(iv) Multiplicative Jordan decompostion commutes with the formation of a-stable linear subspaces and their factors, i.e. we have properties similar to those of 2.4.3 (iv) with a_n replaced by a_u.

Proof. Let $a=a_s+a_n$ be the additive Jordan decomposition of a. Since a is invertible, it has no eigenvalue 0, and from the proof of 2.4.4 we see that a_s is invertible.[8] Therefore,

$$a = a_s(1+a_s^{-1}a_n)$$

and $a_u := 1+a_s^{-1}\cdot a_n$ is as required.[9]

Convention

---

[7] On V_i the Jordan decomposition of a consists of Jordan blocks with the only eigenvalue a_i.

[8] According to the mentioned proof, a_s is just multiplication by the i-th eigenvalue a_i on the i-th main spaces V_i of a.

[9] i.e., such that $a_u - Id = a_s^{-1}\cdot a_n$ is nilpotent. Moreover the found decomposition ist such that a_u and a_s commute with every endomorphism which commutes with a. In particular, if there is a second composition

$$a = b_s \cdot b_u$$

as claimed, then b_s and b_u commute with a and hence with a_s and a_u. Therefore the endomorphism

$$b_s^{-1}a_s = b_u a_u^{-1}$$

is both semisimple and unipotent. Hence it is equal to Id and the multiplicative Jordan decomposition is unique.

We always write $a = a_s + a_n = a_s \cdot a_u$ for the additive and multiplicative Jordan decomposition of $a \in End(V)$, respectively $a \in GL(V)$. We call a_s, a_n, a_u the semi-simple, nilpotent, unipotent part of a, respectively.

2.4.6 Jordan decomposition of direct sums and tensor products

Corollary

Let $a=a_s\ a_u \in GL(V)$ and $b=b_s\ b_u \in GL(W)$. Then

$$a \oplus b = (a_s \oplus b_s)(a_u \oplus b_u) \in GL(V \oplus W)$$
$$a \otimes b = (a_s \otimes b_s)(a_u \otimes b_u) \in GL(V \otimes W)$$

is the Jordan-decomposition of $a \oplus b$ and $a \otimes b$, respectively.

Proof. Follows from Lemma 2.4.3 (ii).[10]

QED.

2.4.7 Jordan decomposition of locally finite actions on infinite dimensional vector spaces

Additive Case

Let V be a not necessarily finite dimensional vector space over k. Denote again by

$$End(V) \text{ and } GL(V)$$

the algebra of endomorphisms of V and the group of invertible endomorphisms, respectively. We say that $a \in End(V)$ is locally finite if V is a union of finite dimensional a-stable subspaces. We say that a is semi-simple (locally nilpotent) if its restriction to any finite dimensional a-stable subspace is semi-simple (nilpotent). If a is semi-simple, it is also semi-simple in the sense of 2.4.1. The analogous statement for "nilpotent" is not true. For a locally finite $a \in End(V)$ we again have an additive Jordan decomposition

$$a = a_s + a_n$$

satisfying 2.4.4(i) with locally finite a_s and a_n and “nilpotent” replaced by “locally nilpotent”.

Proof. To define $a_s\ x$ and $a_n\ x$ for $x \in V$, take a finite dimensional a-stable subspace $W \subseteq V$ containing x and define

$$a_s\ x := (a|_W)_s\ x$$
$$a_n\ x := (a|_W)_n\ x$$

It follows from 2.4.4 that this is independent of the choise of W and that a_s and a_n are as required.

QED.

Multiplicative Case

Similarly for $a \in GL(V)$ locally finite, we have a multiplicative Jordan decomposition

$$a = a_s \cdot a_u .$$

The properties 2.4.4(iv) and 2.4.5 continue to hold, and the same is true for 2.4.4(iii), if b is locally finite.

Special case: the action of a linear algebraic group on its coordinate ring

Now let G be a linear algebraic group, and let A:=k[G]. If $x \in G$, then the right translation $\rho(x)$ is a locally finite element of GL(A) (by 2.3.4), hence we have a Jordan decomposition

---

[10] i.e. from the fact that direct sums tensor products of commuting semi-simple endomorphisms are semi-simple and the same is true with unipotent instead of semi-simple.

$$\rho(x) = \rho(x)_s \ \rho(x)_u \ .$$

2.4.8 Jordan decomposition inside a linear algebraic group

Theorem.
Let G be a linear algebraic group over the field k and let

$$\rho: G \to \mathrm{Aut}(k[G])$$

the (infinite) representation of G by right translations (2.3.3 and 2.3.4 second part).

(i) (Jordan decomposition in G) For every $x \in G$, there are uniquely determined elements $x_s, x_u \in G$ such that

$$\rho(x)_s = \rho(x_s)$$
$$\rho(x)_u = \rho(x_u)$$
$$x = x_s \cdot x_u = x_u \cdot x_s .$$

(ii) If $\phi: G \to G'$ is a homomorphism of algebraic groups then

$$\phi(x)_s = \phi(x_s)$$
$$\phi(x)_u = \phi(x_u)$$

(iii) If $G=GL_n$, then x_s and x_u are the semi-simple and unipotent parts of x as defined in 2.4.5.

The element x_s and x_u of (i) is called the semi-simple part and the unipotent part of x, respectively.

Proof. (i). Let A := k[G] and let

$$q: A \otimes A \to A, \ a \otimes a' \mapsto aa'$$

be the surjective homomorphism induced by multiplication in A.

For every $x \in G$, the right translation associated with x,

$$\rho(x): A \to A, \ f(y) \ a \ f(yx),$$

is an algebra automorphism of A. Therefore,

$$q \circ (\rho(x) \otimes \rho(x)) = \rho(x) \circ q .$$

As a first step in the proof, we show that the same is true with $\rho(x)$ replaced by its semi-simple part $\rho(x)_s$, i.e.,

(*) $$q \circ (\rho(x)_s \otimes \rho(x)_s) = \rho(x)_s \circ q .$$

This can be done using 2.4.4 and 2.4.6.[11] Identity (*) means that

---

[11] In more details the argument is as follows. Use Exercise 2.37 to get embeddings

$$G \subseteq GL_n \text{ and } G \subseteq \mathbb{A}^n$$

such that the operation of G onto itself by right translations is the restriction to G of the natural action

$$GL_n \times \mathbb{A}^n \to \mathbb{A}^n$$

of the general linear group on affine space. Let I be the ideal of G in GL_n,

$$I = I(G).$$

An element $g \in GL_n$ is in G iff I is stable under right translation by g,

$$g \in G \Leftrightarrow \rho(g)I \subseteq I$$

(see 2.3.6).

Given $x \in G \subseteq GL_n$, let

$$\rho(x)_s : A \to A$$

is an automorphism of k-algebras. Hence the map

$$A \to k, f \mapsto (\rho(x)_s f)(e)$$

(which is the composition of $\rho(x)_s$ with evaluation at e) is a homomorphism of k-algebras defining a point $x_s \in G$ such that

$$f(x_s) = (\rho(x)_s f)(e) \qquad (**)$$

for every $f \in A$.

Since $\rho(x)$ commutes with all left multiplications $\lambda(y)$ (which are locally finite), we have by 2.4.4(iii),

$$\begin{aligned}(\rho(x)_s f)(y) &= (\lambda(y^{-1})\rho(x)_s f)(e) = (\rho(x)_s \lambda(y^{-1})f)(e)\\ &= (\lambda(y^{-1})f)(x_s) \qquad \text{(by (**))}\\ &= f(yx_s)\\ &= (\rho(x_s)f)(y)\end{aligned}$$

$$x = s \cdot u$$

be the Jordan decomposition of the matrix x. Then

$$\rho(x) = \rho(s)\,\rho(u), \qquad (2)$$

and it will be sufficient to show that this is the Jordan decomposition of $\rho(x)$. For, in this case $\rho(s)$ and $\rho(u)$ are locally polynomials of $\rho(x)$ and the inclusion

$$\rho(x)I \subseteq I$$

implies that one has inclusions $\rho(s)I \subseteq I$ and $\rho(u)I \subseteq I$, i.e.,

$$s, u \in G.$$

In particular, right translation $\rho(s)$ is well-defined on A and is equal to the semi-simple part of $\rho(x)$,

$$\rho(x)_s = \rho(s): A \to A .$$

As a consequence, $\rho(x)_s$ is an algebra automorphism.

So let us prove that (2) is the Jordan decomposition on

$$k[GL_n] = k[T_{ij}, \det(T)],\ T := (T_{ij}).$$

Obviously $\rho(s)\,\rho(u) = \rho(su) = \rho(us) = \rho(u)\,\rho(s)$. So it will be sufficient to show that $\rho(s)$ is semi-simple and $\rho(u)$ is locally unipotent. Using a linear base change we may assume that x is upper triangular, i.e. s is diagonal and u is upper triangular with 1's on the main diagonal. Then

$$\rho(s)\det(T) = \det(Ts) = \det(s)\det(T) \text{ and } \rho(u)\det(T) = \det(Tu) = \det(T),$$

and it is sufficent that $\rho(s)$ and $\rho(u)$ are semi-simple resp. unipotent on the polynomial algebra $k[T_{ij}]$. Now the polynomial algebra is the symmetric algebra over its linear part and it is sufficient to show that $\rho(s)$ and $\rho(u)$ are semi-simple resp. unipotent on each homogeneous part of this algebra. This is obvious for the linear part $L \subseteq k[T_{ij}]$. To prove it for the degree d part,

$$\wedge^d L ,$$

note that this is a factor of the d-th tensor power $L^{\otimes d}$. By 2.4.4 it is sufficient to show that the actions of $\rho(s)$ and $\rho(u)$ on the tensor power induced by the actions on L is semi-simple resp. unipotent. But the latter follows from 2.4.6.

for every y, i.e., $\rho(x)_s = \rho(x_s)$.

Similarly[12] one defines x_u such that $\rho(x)_u = \rho(x_u)$. Then

$$\rho(x_s x_u) = \rho(x_s)\rho(x_u) = \rho(x)_s\rho(x)_u = \rho(x)_u\rho(x)_s = \rho(x_u)\rho(x_s).$$

Since $\rho: G \to GL(A)$ is faithfull[13], it follows that $x_s x_u = x_u x_s$. We have now established (i).

(ii). A homomorphism of algebraic groups $\phi: G \to G'$ can be factored $G \to Im(\phi) \to G'$. Since $Im(\phi)$ is a closed subgroup in G' by 2.2.5(ii), it suffices to prove (ii) in two special cases.

(a). G is a closed subgroup of G' and

$$\phi\ G \to G'$$

is the canonical injection. Then $k[G] = k[G']/I$, and by 2.3.6,

$$G = \{x \in G' \mid \rho(x)I = I\}.$$

The assertion of (ii) is now a consequence of the fact that Jordan decomposition commutes with the formation of factor spaces w.r.t. stable linear subspaces (see 2.4.4(iv)).[14]

(b). ϕ is surjective. In this case, $\phi^*: k[G'] \to k[G]$ is injektive and k[G'] can be considered as a subspace of k[G] (see 1.9.1(i)), which is invariant under all $\rho(x)$ with $x \in G$. Again the assertion follows from the fact that Jordan decompostion commutes with the passage to invariant subspaces (see 2.4.4(iv)).

(iii). If $G=GL_n$, then $A=k[T_{ij},D^{-1}]$ (see 2.1.3(3)). Put

$$e_i := T_{1i}.$$

Then, if $x=(x_{ij}) \in G$, $(\rho(x)e_i)(y)=e_i(yx) = \sum_{j=1}^{n} y_{1j}x_{ji} = \sum_{j=1}^{n} e_j(y)x_{ji}$, hence

$$\rho(x)e_i = \sum_{j=1}^{n} x_{ji}e_j.$$

---

[12] Replace in the above arguments everywhere the subscript 's' by the subscript 'u'.

[13] We have proved in 2.3.5 that a restriction of ρ to a certain invariant subspace of k[G] gives an embedding of G into some GL_n.

[14] More explicitely, for $x \in G$ in the subgroup of G' there is a commutative diagramm

$$\begin{array}{ccc} k[G'] & \xrightarrow{\gamma} & k[G] \\ \rho(x)_s \downarrow & & \downarrow \rho(x_s) \\ k[G'] & \xrightarrow{\gamma} & k[G] \end{array}$$

where the vertical arrows denote the canonical surjection. If x_s and x'_s denote the semi-simple part of x in G and G' respectively (as defined via (**)), then for $f' \in k[G']$,

$$\begin{aligned} f(x_s) &= \gamma(f')(x_s) && (\gamma \text{ is restriction to G and } x_s \text{ is in G}) \\ &= (\rho(x)_s\gamma(f'))(e) && (\text{by } (**)) \\ &= \gamma(\rho(x)_s f')(e) && (\text{the diagramm is commutative}) \\ &= \rho(x)_s f')(e) && (\gamma \text{ is restriction to } G \subseteq G') \\ &= f'(x'_s) && (\text{by } (**)) \end{aligned}$$

Since this is true for every function f' on G', $x_s = x'_s$. The same argument works for the unipotnent parts.

Thus, the subspace $V := ke_1 + \ldots + ke_n$ of A is $\rho(G)$-stable and the restriction of $\rho(x)$ to V is represented by the matrix of $\rho(x)$ with respect to the basis $\{e_i\}$. By the very definition of x_s we have,

$$\rho(x_s)|_V =^{15} \rho(x)_s|_V =^{16} (\rho(x)|_V)_s ,$$

where the operators in the middle and on the right are the semi-simple parts in the sense of 2.4.7 and 2.4.5. In other words, the matrix $\rho(x_s)|_V$ of x_s is the "usual" semi-simple part of the matrix $\rho(x)|_V$ of x. Similarly one obtains

$$\rho(x_u)|_V = \rho(x)_u|_V = (\rho(x)|_V)_u .$$

QED.

2.4.9 Criterion for semi-simple and unipotent elements

Corollary

Let $x \in G$. Then the following are equivalent.

(i) x is semi-simple (resp., unipotent).

(ii) There is an isomorphism $\phi: G \to GL_n$ onto a closed subgroup of some GL_n such that $\phi(x)$ is semi-simple (resp. unipotent).

Proof. (i)⇒(ii) follows from 2.3.5 and 2.4.8(ii).

(ii)⇒(i). By 2.4.8(iii), the semi-simple (unipotent) part of a semi-simple (unipotent) matrix in Gl_n is the matrix itself. Hence the claim follows 2.4.8(ii) and the fact that ϕ is injective.

QED.

2.4.10 Exercises

We use the notations of 2.4.8.

(1) Show that $\lambda(x)_s = \lambda(x_s)$ and $\lambda(x)_u = \lambda(x_u)$.[17]

(2) The set G_u of unipotent elements of G is a closed subset.

(3) Show by an example that the set G_s of semi-simple elements of G is not necessarily open or closed.

Solutions

(1). Let G' be the linear algebraic group obtained from G by inverting the order of multiplication. Then, considering G as a closed subgroup of GL_n, G' can be considered as a closed subgroup of $(GL_n)' \cong GL_n$, $x \mapsto x^T$.

The semi-simple part of a regular $n \times n$ matrix x considered as an element of GL_n is identical with its semi-simple part, when considered as an element of $(GL_n)'$. Hence the formations of the semi-simple parts in G and G' coincide, and the same is true for the unipotent parts.

Therefore, if ρ' denotes right translation with respect to G',

$$\lambda(x)_s = \rho'(x)_s = \rho'(x_s) = \lambda(x_s)$$
$$\lambda(x)_u = \rho'(x)_u = \rho'(x_u) = \lambda(x_u)$$

---

[15] This is the definition of x_s restricted to V.

[16] This is due to the fact that the semi-simple part of a locally finite action coinsides (by construction) on all invariant finite-dimensional subspaces with the usual definition.

[17] It is sufficient to prove that these identities hold on finite dimensional G-invariant subspaces of the coordinate ring of G. But then they follow from the fact that homomorphisms of linear algebraic groups respect the Jordan decomposition.

(2). We may assume that G is a closed subgroup of GL_n . Then

$$G_u = \{x \in G \mid \text{all eigenvalues of } x \text{ are } =1\}$$

$$= \{x \in G \mid \det(T\cdot Id - x) = (T-1)^n = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} T^i \}$$

$$= \{x \in G \mid s_i(x) = (-1)^{n-i}\binom{n}{i} \text{ for } i=1,\ldots,n \}$$

where s_i denotes the i-th coefficient of the characteristic polynomial of the matrix of x.

(3). Consider the closed subgroup of GL_2 ,

$$G= \{x \in GL_n \mid T_{21}(x) =0\} = \{x= \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a,b,c \in k,\ a\neq 0,\ b\neq 0\}.$$

The open subset of all x with $a\neq c$ consists entirely of semi-simple matrices. Its closure is equal to G, since G is irreducible. The matrix

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

is not semi-simple but in G. This shows that G_s cannot be closed in G. Assume that G_s is open in G. Then $F\cap G_s$ is open in

$$F := \{x= \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in k\}.$$

Since $F\cap G_s$ contains the identity matrix, it isn't empty. Hence all but a finite number of elements in F must be semi-simple, which is wrong.

Definition (unipotent group)

The linear algebraic group G is called unipotent if all its elements are unipotent.

Warning (semi-simple group)

A semi-simple linear algebraic group is not one all whose elements are semi-simple, see the definition in 6.14.

2.4.11 Unipotent groups as subgroups of $\mathbb{U}_n$

The next result, which is in fact one from linear algebra, together with 2.3.5 and 2.4.9, shows that an unipotent G is isomorphic to a closed subgroup of some $\mathbb{U}_n$ of unipotent upper triangular matrices.

Theorem

Let G be a subgroup of GL_n consisting of unipotent matrices. Then there is some $x \in GL_n$ such that $xGx^{-1} \subseteq \mathbb{U}_n$.

Proof. Let $V=k^n$, so G is a subgroup of $GL(V)=\mathbf{GL}_n$. Using induction on n, it suffices to prove that there is some $v \in V$, $v\neq 0$ such that $gv=v$ for every $g \in G$.[18] If G stabilizes a nontrivial proper subspace of V, the existence of v follows by induction. So we are reduced to the case that G acts irreducibly on V.

Let $A\subseteq \mathbf{M}_n$ be the subspace

---

[18] Then there is a complete flag of invariant subspaces in V, i.e., there is a basis in V such that all elements of G are represented w.r.t. this basis by upper triangular matrices. Since all elements of G are unipotent, the matrices are even in $\mathbb{U}_n$.

$$A := \sum_{g \in G} kg$$

spanned by all $g \in G$. This is a subalgebra of $\mathbf{M}_n$, which acts irreducibly on V. By Burnside's theorem (see e.g. [26, Ch. XVII, § 3) it follows that $A = M_n$. If $g,h \in G$,

$$\mathrm{Tr}((1-g)h) = \mathrm{Tr}(h) - \mathrm{Tr}(gh) = 0,$$

where the last identity comes from the fact that the elements of G are unipotent matrices.[19] Therefore,

$$\mathrm{Tr}((1-g)a) = 0$$

for every $a \in A = \mathbf{M}_n$ and every $g \in G$. But then we must have $g=1$. It follows $G=\{1\}$, $\dim V = 1$, and the existence of v is trivial.
QED.

Remark
In the rest of this chapter we shall deal with various kinds of abelian groups. First we prove a structure theorem for abelian groups

2.4.12 Commutative groups as direct products of G_s and G_u

Theorem
Let G be a commutative linear algebraic group.
(i) The sets G_s and G_u of semi-simple and unipotent elements are closed subgroups.
(ii) The product map $\pi: G_s \times G_u \to G$ is an isomorphism of algebraic groups.

Proof. We may assume G to be a closed subgroup of $\mathbf{GL}_n$. Since the product of commuting semi-simple (resp. unipotent) Endomorphisms is again semi-simple (resp. unipotent) by 2.4.3(i), we see that G_s and G_u are subgroups of G in the commutative case. Moreover, G_u is closed by Exercise 2.4.10(2).[20] It follows from 2.4.2(ii) that there is a direct sum decomposition of $V := k^n$ into G-stable subspaces[21], say

$$V = \oplus_i V_i ,$$

and there are homomorphisms $\phi_i : G_s \to k^*$ such that

$$g \cdot v = \phi_i(g)\, v \text{ for } g \in G_s \text{ and } v \in V_i .$$

Trigonalizing the restrictions of G to V_i (2.4.2(i)) we may assume that $G \subseteq \mathbf{T}_n$. But then $G_s = G \cap \mathbf{D}_n$ (notations of 2.1.3) . In particula, G_s is closed, whence (i).
The uniqueness of the Jordan decomposition in G implies that π is an isomorphism of abstract groups. It is clearly a morphism of algebraic varieties. To establish (ii), it suffices

---

[19] i.e. for each such matrix there is a base change (depending upon the matrix) such that the matrix becomes upper triangular and henc an element of $\mathbf{U}_n$. In particular, the trace of such a matrix is equal to the dimension of the linear space it is acting on.
[20] It can be conjugated into the upper triangular matrices. There it is defined by the equations $T_{ii} = 1$.
[21] Take the direct sum decomposition with exists for G_s according to 2.4.2. Since G is commutative, the direct summands can is G-stable (also by 2.4.2).

to show that π^{-1} is also a morphism. But the map $x \mapsto x_s$ is a morphism, being "projection into diagonal matrices". Hence $\pi: x \mapsto (x_s, xx_s^{-1})$ is also a morphism.

QED.

2.4.13 The semi-simple and unipotent parts of connected commutative groups

Corollary

Let G be a connected commutative linear algebraic group. Then so are G_s and G_u.

Proof. Immediate from the proof of 2.4.12.[22]

QED.

2.5 Diagonalizable groups and tori

2.5.1 Characters, 1-parameter subgroups, diagonalizable groups and tori

Let G be a linear algebraic group. A homomorphism of algebraic groups $\chi: G \to \mathbf{G}_m$ is called a rational character of G. The set of characters is denoted

$$X^*(G) := \mathrm{Hom}_{\mathrm{alg.groups}}(G, \mathbf{G}_m) .$$

It has a natural structure of an abelian group. Its group operation is usually written additively. We may consider $X^*(G)$ as a subset

$$X^*(G) \subseteq k[G].$$

We denote by $X_*(G)$ the set

$$X_*(G) := \mathrm{Hom}_{\mathrm{alg.groups}}(\mathbf{G}_m, G) .$$

An element of $X_*(G)$ is called multiplicative 1-parameter subgroup of G. If G is commutative, $X_*(G)$ has also the structure of an additive (i.e. abelian) group: we define

$$(\lambda+\mu)(t) := \lambda(t)\mu(t),\ (-\lambda)(t) := \lambda(t)^{-1} \quad \text{for } t \in \mathbf{G}_m \text{ and } \lambda, m \in X_*(G)$$

A linear algebraic group G which is isomorphic to a closed subgroup of some group of diagonal matrices $\mathbf{D}_n$ is called diagonalizable. It is called an algebraic torus (or simply a torus) if it is isomorphic to some $\mathbf{D}_n$.

2.5.2 Characterization of diagonalizable groups

Theorem

Let G be a linear algebraic group. Then the following conditions are equivalent.

(a) G is diagonalizable.

(b) $X^*(G)$ is a finitely generated abelian group generating k[G] as a k-vector space.

(c) Every rational representation of G is a direct sum of 1-dimensional ones.

Proof. (a) $\Rightarrow$ (b). Let $\chi_i : \mathbf{D}_n \to k$ be the projection onto the i-th diagonal entry such that $d \in D_n$ can be written as $d=\mathrm{diag}(\chi_1(d), \ldots, \chi_n(d))$. Then χ_i is a rational character of $\mathbf{D}_n$, and we have

$$k[\mathbf{D}_n] = k[\chi_1, \ldots, \chi_n, \chi_1^{-1}, \ldots, \chi_n^{-1}].$$

We see that the elements of $X^*(\mathbf{D}_n)$ generates $k[\mathbf{D}_n]$.

---

[22] According to this proof, G_s and G_u are images of G under regular maps.

Now let G be diagonalizable, i.e., a closed subgroup of $\mathbf{D}_n$ with n appropriate. Then k[G] is a factor ring of k[$\mathbf{D}_n$], hence generated over k by the the restrictions to G of the characters χ_i and χ_i^{-1} . This shows that X*(G) generates k[G] as a k-vector space. Moreover, the restrictions

$$\phi_i := \chi_i \mid_G \qquad (i=1,\ldots,n)$$

generate X*(G). For, every $\phi \in X^*(G)$ is an elment of k[G], hence a linear combination of power products of $\phi_1, \ldots, \phi_n$. Since different characters are linearly independent, ϕ must be equal to one of these power products. This shows that X*(G) is generated by the elements ϕ_i hence is finitely generated.

(b) $\Rightarrow$ (c). By assumption, the characters $\chi \in X^*(G)$ generate the coordinate ring k[G], hence form a basis of k[G] over k (since different characters are linearly independent). Let $\phi: G \to \mathbf{GL}_n$ be a rational representation of G. Write $V := k^n$. Expressing the matrix elments of $\phi(g)$ as linear combinations of elements of X*(G) we see that we can write $\phi(g)$ as a finite sum

$$\phi(g) =^{23} \sum_{\chi \in X^*(G)} \chi(g) A_\chi ,$$

with uniquely[24] determined coefficients $A_\chi \in \mathbf{M}_n$. From $\phi(gh)=\phi(g)\cdot\phi(h)$ we infer

$$\sum_{\chi \in X^*(G)} \chi(g)\chi(h)A_\chi = \sum_{\chi,\chi' \in X^*(G)} \chi(g)\chi'(h)A_\chi A_{\chi'} .$$

Since different characters on G×G are linearly independent, this implies

(1) $$A_\chi A_{\chi'} = \delta_{\chi,\chi'} \cdot A_\chi .$$

Moreover, the defining identity $\phi(g) = \sum \chi(g)A_\chi$ yields for g=e,

(2) $$1 = \sum_{\chi \in X^*(G)} A_\chi .$$

Define

$$V_\chi := A_\chi V.$$

Then by the last identity, every $v \in V$ is a sum of $v_\chi \in V_\chi$. From the former identity (1) we see that v_χ is uniquely[25] determined by v, i.e., V is a direct sum of the subspaces V_χ . Moreover, for $v \in V_\chi$, i.e., $v = A_\chi v$,

$$\phi(g)v = \chi(g)v.$$

This completes the proof of the implication (b) $\Rightarrow$ (c).

(c) $\Rightarrow$ (a). Embed G into some **GL**(V) and write V as a direct sum of G-modules which are 1-dimensional as k-vector spaces. This is possible by condition (c).

---

[23] $\phi(g)$ is a linear combination of elementary matrices where the coefficients are regular functions in g, i.e., k-lineare combinations of characters.

[24] since sets of pairwise characters are linearly indepentend.

[25] Let $v = \Sigma v_\chi = \Sigma w_\chi$ be two decompositions. In view of (1),

$$A_{\chi'}v_\chi = \delta_{\chi,\chi'}\cdot v_{\chi'} \text{ and } A_{\chi'}w_\chi = \delta_{\chi,\chi'}\cdot w_{\chi'}.$$

Applying $A_{\chi'}$ to the two decompositins und using (1) we obtain

$$v_{\chi'} = A_{\chi'}v_{\chi'} = A_{\chi'}v = A_{\chi'} w_{\chi'} = w_{\chi'} .$$

2.5.3 Subgroups of diagonalizable groups and kernels of characters

Corollary

Let H be a closed subgroup of the diagonalizable group G. Then H is diagonalizable, and is the intersection of the kernels of finitely many rational characters of G

Proof. The first assertion is clear from the definition of a diagonalizable group. As for the second, consider the ideals

$$I := \{f \in k[G] \mid f(H)=0\} \qquad \text{(the ideal of H in k[G])}$$

$$J := (\chi - 1 \mid \chi \in X^*(G) \mid \chi(H)=1).$$

It will be sufficient to show that I=J. For, if $\chi_1 - 1,...,\chi_r - 1$ generate the ideal J, equality of I and J implies

$$H = \{g \in G \mid f(g)=0 \text{ for } f \in J\} = \{\chi_i(g) = 1 \mid i=1,...,r\} = \bigcap_{i=1}^{r} \mathrm{Ker}(\chi_i).$$

Obviously, $J \subseteq I$. Let $f \in I$. Since $X^*(G)$ generates k[G],

$$f = c_1\chi_1 + ... + c_s\chi_s$$

with $c_i \in k$, $\chi_i \in X^*(G)$. Restriction to H yields a linear combination of characters on H which is identically zero. Since sets of pairwise different characters are linearly independent, there are i and j with $\chi_i = \chi_j$ on H. Write

$$\chi_j = \chi_i + (\chi_j - \chi_i) = \chi_i + \chi_i(\chi - 1).$$

with $\chi := (\chi_i)^{-1}\chi_j$. Then χ is a character restricting to the trivial one on H, i.e., the term $\chi_i(\chi-1)$ is in J. Reducing f modulo J, the function f can be written as a linear combination of s-1 characters. Induction on s shows that $f \in J$ as required.

QED.

2.5.4 k[G] as the group algebra of the character group

Corollary

Let G be diagonalizable. Then $X^*(G)$ is a finitely generated abelian group, without p-torsion, if the characteristics p = char(k) of k is positive. Moreover, the algebra k[G] is isomorphic to the group algebra of $X^*(G)$.

Proof. By 2.5.2(b), $X^*(G)$ is a finitely generated abelian group. Assume that $X^*(G)$ has p-torsion. Then there is a non-trivial character $\chi \in X^*(G)$ with $p\cdot\chi = 0$, i.e., $\chi(g^p)=1$ for every $g \in G$. Since k is algebraically closed, every element of $G \subseteq \mathbf{D}_n$ can be written as a p-th power, hence χ is trivial, contrary to the choise of χ. This shows, $X^*(G)$ cannot have p-torsion.

Again by 2.5.2(b), k[G] is generated by the elements of $X^*(G)$. Since finite sets of pairwise different characters are linearly independent, the characters form a free generating system of k[G], i.e., the coordinate ring can be identified with the group algebra of $X^*(G)$.

2.5.5. Exercises

(1) Determine the rational characters of $\mathbf{G}_m$.

(2) Let G be a linear algebraic group. G acts on the 1-parameter subgroups $X_*(G)$ by conjugation,

$$(g\cdot\lambda)(t) = g\chi(t)g^{-1} \quad \text{for } g \in G,\ \chi \in X_*(G),\ t \in \mathbf{G}_m.$$

If $g \in G$, $\lambda \in X_*(G)$, define

$$\theta_{g,\lambda} : \mathbf{G}_m \to G,\ t \mapsto \lambda(t)g\lambda(t)^{-1}.$$

This is a morphism of algebraic varieties. Considering $\mathbf{G}_m$ as an open subset of the affine line, let

$$P(\lambda) := \{g \in G \mid \theta_{g,\lambda} \text{ extends to a morphism } \mathbb{A}^1 \to G\}.$$

(a) $P(\lambda)$ is a subgroup of G, containing the centralizer $H \subseteq G$ of $\lambda(\mathbf{G}_m)$. Moreover, we have

$$P(g\cdot\lambda) = gP(\lambda)g^{-1}.$$

(b) $P(\lambda) \cap P(-\lambda) = H$ (Hint: use 1.6.12(2), last part).

(c) Let $G := \mathbf{GL}_n$, acting on $V := k^n$. For any $\lambda \in X_*(G)$ there exists a family of subspaces $V_1 \subseteq V_2 \subseteq \ldots \subseteq V_s \subseteq V$ (a flag) such that

$$P(\lambda) = \{g \in G \mid g\cdot V_i = V_i \quad \text{for } i=1,2,\ldots,s\}.$$

(Hint: using 2.5.2(c), reduce to the case that $\lambda(t) = \mathrm{diag}(t^{a_1}, \ldots, t^{a_s})$, where $a_1 \geq a_2 \geq \ldots \geq a_s$).

(d) Show that $P(\lambda)$ is a closed subgroup of G, for any G and $\lambda \in X_*(G)$.

Solutions

(1)

Determine the rational characters of $G := \mathbf{G}_m$.

$k[G] = k[T,T^{-1}]$ is generated as a k-vector space by the powers T^n, $n \in \mathbb{Z}$, of the indeterminates. Each such power (considered as a function on G) is in fact a character $\chi_n : G \to \mathbf{G}_m$, $g \mapsto g^n$, of G. An arbitrary character χ of G, considered as an element of the coordinated ring, is a linear combination of the characters χ_n (since these generate the coordinate ring). Since every set of pairwise different characters is linearly independent, χ must be equal to one of these. We have proved,

$$X^*(\mathbf{G}_m) = \{\chi_n \mid n \in \mathbb{Z}\}$$

---

(2)

Let G be a linear algebraic group. G acts on the 1-parameter subgroups $X_*(G)$ by conjugation,

$$(g\cdot\lambda)(t) = g\chi(t)g^{-1} \quad \text{for } g \in G,\ \chi \in X_*(G),\ t \in \mathbf{G}_m.$$

If $g \in G$, $\lambda \in X_*(G)$, define

$$\theta_{g,\lambda} : \mathbf{G}_m \to G,\ t \mapsto \lambda(t)g\lambda(t)^{-1}.$$

This is a morphism of algebraic varieties. Considering $\mathbf{G}_m$ as an open subset of the affine line, let

$$P(\lambda) := \{g \in G \mid \theta_{g,\lambda} \text{ extends to a morphism } \mathbb{A}^1 \to G\}.$$

(a)

$P(\lambda)$ is a subgroup of G, containing the centralizer $H \subseteq G$ of $\lambda(\mathbf{G}_m)$. We have $P(g\cdot\lambda) = gP(\lambda)g^{-1}$.

Let $g_1, g_2 \in G$ be two elements such that

$$\theta_{g_i,\lambda} : \mathbf{G}_m \to G,\ t \mapsto \lambda(t) g_i\ \lambda(t)^{-1}$$

extends to a morphism $\mathbb{A}^1$. By definition,

$$\theta_{g_1 g_2^{-1},\lambda}(t) = \lambda(t) g_1\ g_2^{-1}\ \lambda(t)^{-1} = \lambda(t) g_1\ \lambda(t)^{-1}\ \lambda(t) g_2^{-1}\ \lambda(t)^{-1}$$

$$= \theta_{g_1,\lambda}(t) \cdot (\theta_{g_2,\lambda}(t))^{-1},$$

hence

$$\theta_{g_1 g_2^{-1},\lambda} = \mu \circ (\mathrm{id} \times \iota) \circ (\theta_{g_1,\lambda} \times \theta_{g_2,\lambda}) \circ \Delta$$

where $\mu: G \times G \to G$ is multiplication, $\iota: G \to G$ is inversion, and $\Delta: \mathbf{G}_m \to \mathbf{G}_m \times \mathbf{G}_m$ is the diagonal. Since the diagonal $\Delta: \mathbf{G}_m \to \mathbf{G}_m \times \mathbf{G}_m$ is the restriction of the diagonal $\mathbb{A}^1 \to \mathbb{A}^1 \times \mathbb{A}^1$, the above decomposition can be extended to a morphism on $\mathbb{A}^1 \to G$ (since $\theta_{g_1,\lambda}$ and $\theta_{g_2,\lambda}$ can by assumption). This shows $g_1 g_2^{-1} \in P(\lambda)$, i.e., $P(\lambda)$ is a subgroup of G.

The formula

$$P(g \cdot \lambda) = g P(\lambda) g^{-1}$$

holds since

$$\theta_{x, g\cdot\lambda}(t) = (g\cdot\lambda)(t)\, x\, (g\cdot\lambda)(t)^{-1}$$

$$= (g \cdot \lambda(t) \cdot g^{-1}) x ((g \cdot \lambda(t) \cdot g^{-1})^{-1}$$

$$= g \cdot \lambda(t) \cdot g^{-1} \cdot x \cdot g \cdot \lambda(t)^{-1} \cdot g^{-1}$$

$$= g \cdot \theta_{g^{-1} x g, \lambda}(t) \cdot g^{-1},$$

i.e., $x \in P(g\cdot\lambda) \Leftrightarrow g^{-1} x g \in P(\lambda) \Leftrightarrow x \in g P(\lambda) g^{-1}$.

Finally, if $g \in G$ is in the centralizer $H \subseteq G$ of $\lambda(\mathbf{G}_m)$,

$$\theta_{g,\lambda}(t) = \lambda(t) g \lambda(t)^{-1} = g \cdot \lambda(t) \lambda(t)^{-1} = g$$

is a constant function and hence can extended to $\mathbb{A}^1$. Therefore $H \subseteq P(\lambda)$.

(b)

$P(\lambda) \cap P(-\lambda) = H$ (Hint: use 1.6.12(2), last part).

Let $g \in P(\lambda) \cap P(-\lambda)$. Then

$$\theta_{g,\lambda} : \mathbf{G}_m \to G,\ t \mapsto \lambda(t) g \lambda(t)^{-1}$$

$$\theta_{g,-\lambda} : \mathbf{G}_m \to G,\ t \mapsto \lambda(t)^{-1} g \lambda(t) = \theta_{g,\lambda}(t^{-1})$$

both can be extented to $\mathbb{A}^1$. In other words, the coordinate functions

$$\theta_{ij}(T) \in k[\mathbf{G}_m] = k[T, T^{-1}]$$

of the morphism

$$\theta_{g,\lambda} : \mathbf{G}_m \to G \subseteq \mathbf{GL}_n$$

are even polynomials, $\theta_{ij}(T) \in k[T]$, and the same is true if T is replaced by T^{-1}. But then each $\theta_{ij}(T)$ must be a constant, and

$$\lambda(t) g \lambda(t)^{-1} = \theta_{g,\lambda}(t) = \theta_{g,\lambda}(1) = g.$$

In other words, g is in the centralizer H of $\lambda(\mathbf{G}_m)$.

(c)

Let $G := \mathbf{GL}_n$, acting on $V := k^n$. For any $\lambda \in X_*(G)$ there exists a family of subspaces $V_1 \subseteq V_2 \subseteq \ldots \subseteq V_s \subseteq V$ (a flag) such that

$$P(\lambda) = \{g \in G \mid g \cdot V_i = V_i \quad \text{for } i=1,2,\ldots,s\}.$$

(Hint: using 2.5.2(c), reduce to the case that $\lambda(t) = \mathrm{diag}(t^{a_1}, \ldots, t^{a_s})$, where $a_1 \geq a_2 \geq \ldots \geq a_s$).

The 1-parameter subgroup $\lambda : \mathbf{G}_m \to G$ can be used to lift the natural action of G on V to an action of $\mathbf{G}_m$ on V. Let

$$V = W_1 \oplus \ldots \oplus W_n$$

be a decomposition of V into 1-dimensional $\mathbf{G}_m$-stable subspaces (such a decomposition exists, since $\mathbf{G}_m$ is diagonalizable (2.5.2(c))). Then

$$\lambda(t) w = t^{\nu_i} w \text{ for } w \in W_i .$$

We may assume that $\nu_1 = \ldots = \nu_{n_1} < \nu_{n_1+1} = \ldots = \nu_{n_1+n_2} < \ldots < \nu_{n_1+\ldots+n_s} = \ldots = \nu_n$.

Let $\{e_i\}_{i=1,\ldots,n}$ be a basis of V such that e_i generates W_i. For $g \in G$ write $g=(g_{ij})$ for the matrix of the linear transformation g in terms of this basis. Then the matrix of $\theta_{g,\lambda}(t)$ in terms of the basis $\{e_i\}_{i=1,\ldots,n}$ is equal to

$$\theta_{g,\lambda}(t) = \lambda(t) g \lambda(t)^{-1} = (g'_{ij}(t))$$

$$\text{with } g'_{ij}(t) := g_{ij} \cdot t^{\nu_i - \nu_j}.$$

Therefore, $\theta_{g,\lambda}$ can be extended to $\mathbb{A}^1$ if and only if $g_{ij} = 0$ for every pair (i,j) such that $\nu_j > \nu_i$. The latter condition means that (g_{ij}) has matrices of type $n_1 \times n_1, n_2 \times n_2, \ldots, n_s \times n_s$ in the main diagonale, has zeros beneth theses matrices, and has arbitrary elements above them. This can be expressed also using flags. Write

$$V_i := W_1 + \ldots + W_{n_1+\ldots+n_i} .$$

Then $P(\lambda) = \{g \in G \mid gV_i \subseteq V_i\} = \{g \in G \mid gV_i = V_i\}$.

(d)

Show that $P(\lambda)$ is a closed subgroup of G, for any G and $\lambda \in X_*(G)$.

See the description of of $P(\lambda)$ in terms of the basis $\{e_i\}$ in (c).

2.5.6. The group algebra of an abelian group Γ and its coalgebra operations

$k[\Gamma]$:= k-algebra with k-vector space basis Γ and the multiplication induced by the group multiplication. Note that

$$k[\Gamma_1 \oplus \Gamma_2] \cong k[\Gamma_1] \otimes k[\Gamma_2].$$

Equip $k[\Gamma]$ with morphisms as follows ($\gamma \in \Gamma$):

$\pi^*: k[\Gamma] \to k[\Gamma] \otimes_k k[\Gamma]$, $\gamma \mapsto \gamma \otimes \gamma$ (comultiplication)

$\iota^*: k[\Gamma] \to k[\Gamma]$, $\gamma \mapsto \gamma^{-1}$ (inversion)

$e: k[\Gamma] \to k$, $\gamma \mapsto 1$ (counit)

2.5.7. The linear algebraic group defined by a finitely generated abelian group

Proposition

Let Γ be a finitely generated abelian group without p-torsion where p:=char(k).

(i) $k[\Gamma]$ is an affine k-algebra.

(ii) There is a diagonalizable group $G(\Gamma)$ with $k[G(\Gamma)] = k[\Gamma]$ such that multiplication, inversion, and unit induce π^*, ι^*, and e as above on the coordinate ring.

(iii) $X^*(G(\Gamma)) = \Gamma$.

(iv) If G is diagonalizable, $G(X^*(G)) \cong G$.

The isomorphisms of (iii) and (iv) are functorial in the appropriate category.

Proof. (i). All we have to show is that $k[\Gamma]$ is reduced. Writing Γ as a direct sum of cyclic groups, we may assume that Γ is cyclic. In case $\Gamma=\mathbb{Z}$, $k[\Gamma] = k[T, T^{-1}]$ is obviously an integral domain. If Γ is finite, $\Gamma=\mathbb{Z}/(d)$, the characteristics p=char(k) doesn't divide d (by assumption) and $k[\Gamma] = k[T]/(T^d-1)$ is reduced, for, T^d-1 has no multiple roots.

(ii). As above we may assume that Γ is cyclic. In case $\Gamma=\mathbb{Z}$, $k[\Gamma] = k[T, T^{-1}] = k[\mathbf{G}_m]$, hence $G(\Gamma) = \mathbf{G}_m$. Suppose that $\Gamma=\mathbb{Z}/(d)$, d not a multiple of p. Then $k[\Gamma] = k[T]/(T^d-1)$ is the coordinate ring of the finite group $G(\Gamma) = \mathbb{Z}/(d)$ (of d-th roots of unity).

(iii), Again we may assume that Γ is cyclic. By direct calculation,

$$X^*(G(\mathbb{Z})) = X^*(\mathbf{G}_m) = \mathbb{Z}$$

$$X^*(G(\mathbb{Z}/(d))) =^{26} X^*(\mathbb{Z}/(d)) = \mathbb{Z}/(d).$$

(iv). For G diagonalizable k[G] is isomorphic to the group algebra of Γ:=X*(G) by Corollary 2.5.4, hence by (ii), $k[G(\Gamma)] = k[\Gamma] = k[G]$. But this implies $G(\Gamma) = G$ as claimed.

2.5.8. Characterization of affine tori

Proposition

Let G be a diagonalizable group.

(i) G is a direct product of a torus and a finite abelian group.

(ii) G is a torus if and only if G is connected.

(iii) G is a torus if and only if X*(G) is a free abelian group.

---

[26] As we have just seen, $G(\mathbb{Z}/(d)))$ consists of the d-th roots of unity. A character on this group is determined by its value of any primitive root of unity. This value must be a d-th root of unity and every d-th root of unity occurs as a value. So $G(\mathbb{Z}/(d)))$ is just the group of d-th roots of unity. The same arguments applies to give the equality sign on the right.

Proof. Write $X^*(G)$ as a direct sum of a free abelian group Γ_1 and a finite one, Γ_2. Then, by the previous result, $G \cong G(\Gamma_1)\times G(\Gamma_2)$. Since $k[\Gamma_2]$ is finite dimensional, $G(\Gamma_2)$ must be finite. In particular, if G is connected then $G(\Gamma_2)=1$, i.e., $\Gamma_2 = 0$.

Moreover, $X^*(\mathbf{D}_n) = \mathbb{Z}^n$ and $G(\mathbb{Z}^n) = \mathbf{D}_n$ as one can easily see by direct calculation. This concludes the proof of the proposition.

2.5.9. Exercises

(1) Make diagonalizable groups and abelian groups without p-torsion into categories and show that these two categories are anti-equivalent (p:= char(k)).

(2) Let G be diagonalizable. If H is a closed subgroup of G and Y is a subgroup of $X^*(G)$, define

$H^0 := \{\chi \in X^*(G) \mid \chi(H) = 1\}$

$Y^0 := \{x \in G \mid \chi(x)=1 \text{ for every } \chi \in Y\}$

Then $H^{00} = H$ and $Y^{00} = Y$ if $X^*(G)/Y$ has no p-torsion.

Remark. We conclude this section with some special results about diagonalizable groups and tori (partly in the form of exercises).

2.5.10. Rigity of diagonalizable groups

Proposition

Let G and G' be diagonalizable groups, V a connected affine variety, and

$$\phi: V\times G \to G'$$

a morphism of affine varieties such that for every $v \in V$ the map

$$G \to G',\ x \mapsto \phi(v,x),$$

defines a homomorphism of algebraic groups. Then $\phi(v,x)$ is independent upon v.

Bemerkung

Diese Aussage heißt auch Starrheitssatz für diagonalisierbare Gruppen.

Proof. If $\chi' \in X^*(G')$, the regular function $\chi'\circ\phi(v,g)$ on $V\times G$ can be written in the form

$$\chi'\circ\phi(v,g) = \sum_{\chi\in X^*(G)} f_{\chi,\chi'}(v)\ \chi(g)$$

with $f_{\chi,\chi'} \in k[V]$ (since k[G] is generated as a k vector space by the characters of G, hence so is $k[V\times G] = k[V]\otimes k[G]$ as a module over k[V]). Since $x \mapsto \phi(v,x)$ defines a group homomorphism for every fixed v,

$$\chi'\circ\phi(v,g_1\ g_2) = \chi'\circ\phi(v,g_1)\chi'\circ\phi(v,g_2)$$

$$= \sum_{\chi_1,\chi_2\in X^*(G)} f_{\chi,_1\chi'}(v)\ f_{\chi,_2\chi'}(v)\ \chi_1(g_1)\ \chi_2(g_2)$$

Comparing this with

$$\chi'\phi(v,g_1\ g_2) = \sum_{\chi_1\in X^*(G)} f_{\chi,_1\chi'}(v)\ \chi_1(g_1)\ \chi_1(g_2)$$

and using the fact that the charactes of G form a vector space base of k[G] over k (so that the products $1\otimes\chi_1\ \otimes\chi_2$ with $\chi_1, \chi_2 \in X^*(G)$ form a free basis of $k[V]\otimes k[G]\otimes k[G]$ over k[V]), we see that

$$f_{\chi,1\chi'}(v)\ f_{\chi,2\chi'}(v) = \begin{cases} f_{\chi,1\chi'}(v) & \text{if } \chi_1=\chi_2 \\ 0 & \text{otherwise} \end{cases}.$$

In particular, $f_{\chi\chi'}(v)$ is an idempotent element of k[V], hence takes only the values 0 and 1. For ε = 0,1 put

$$V_\varepsilon := \{v \in V \mid f_{\chi\chi'}(v) = \varepsilon\}$$

(χ and χ' fixed). Then V_0 and V_1 are disjoint closed subsets of V, and V is their union. Since V is connected, it must be equal to one of them, i.e., each $f_{\chi\chi'}(v)$ must be independent upon v. But then $\chi'\circ\phi(v,g)$ is independent upon v for every character χ' of G'. Since the characters of G' generate the coordinate ring k[G], the coordinates of $\phi(v,g)$, hence $\phi(v,g)$ itself is independent upon v.

QED.

2.5.11. Normalizer and Centralizer of a diagonalizable subgroup

Definition (normalizer, centralizer)

Let G be a linear algebraic group and $H\subseteq G$ be a closed subgroup. Then

$$Z_G(H) := \{g \in G \mid ghg^{-1} = h \text{ for every } h \in H\}$$

is called the centralizer of H in G and

$$N_G(H) := \{g \in G \mid gHg^{-1} = H \text{ for every } h \in H\}$$

is called the normalizer of H in G.

Both are closed subgroups of G. For,

$$N_G(H) = \{g\in G \mid f(ghg^{-1}) = 0 \text{ for every } f\in k[G] \text{ vanishing on H and every } h\in H\}$$

is defined by a set of polynomial functions, and the same is true for

$$Z_G(H) := \{g \in G \mid f(ghg^{-1})-f(h)=0 \text{ for every } h\in H \text{ and } f\in k[G]\}$$

Corollary

Let H be a diagonalizable subgroup of G. Then

$$N_G(H)^0 = Z_G(H)^0$$

and $N_G(H)/Z_G(H)$ is finite.

Proof. Define $V:= N_G(H)^0$ and consider the map

$$\phi: V\times H \to H,\ (v,h) \mapsto vhv^{-1}.$$

By the previous result, $\phi(v,h)$ is independent upon v, i.e., $vhv^{-1} = ehe^{-1} = h$, hence $v \in Z_G(H)$. This proves $N_G(H)^0 \subseteq Z_G(H)$. Since $N_G(H)^0$ is connected, $N_G(H)^0 \subseteq Z_G(H)^0$. The converse inclusion is trivial. The finiteness assertion follows from the first part of the corollary, i.e., from the fact that $Z_G(H)$ contains $N_G(H)^0$, and the fact that $N_G(H)/N_G(H)^0$ is finite.

2.5.12. Exercises about tori

Let T be a torus. We write $X^*:=X^*(T)$ and $X_* := X_*(T)$.

(1) Let $T=\mathbf{D}_n$. Then X^* consists of the functions

$$\mathbf{D}_n \to \mathbf{G}_m,\ \mathrm{diag}(x_1,\ldots,x_n) \mapsto x_1^{a_1}\ldots x_n^{a_n},$$

with $(a_1,\ldots,a_n) \in \mathbb{Z}^n$ and X_* consists of the maps

$$\mathbf{G}_m \to \mathbf{D}_n,\ x \mapsto \mathrm{diag}(x^{b_1},\ldots,x^{b_n})$$

with $(b_1,\ldots,b_n) \in \mathbb{Z}^n$.

(2) If $\chi \in X^*, \lambda \in X_*$ define $(\chi,\lambda) \in \mathbb{Z}$ by the condition

$$x^{(\chi,\lambda)} = \chi(\lambda(x)).$$

Then (χ,λ) defines a perfect pairing $X^* \times X_* \to \mathbb{Z}$, i.e., every homomorphism $X^* \to \mathbb{Z}$ is of the form $\chi \mapsto (\chi,\lambda)$ with $\lambda \in X_*$, and similarly for homomorphisms $X_* \to \mathbb{Z}$.

(3) Let V be an affine T-space, and let A:=k[V]. Denote by $B:=A^T$ the subalgebra of T-invariant functions of V,

$$B := A^T := \{f \in A \mid f(t\cdot v) = f(v) \text{ for } t \in T,\ v \in V\}.$$

(a) B is an affine subalgebra of A.

(b) If W is an affine variety with $k[W] \cong B$ then the injection $B \to A$ defines a morphism of affine varieties $\phi: V \to W$ such that $\phi(t\cdot v)=\phi(v)$ for $t \in T$, $v \in V$. Show that the following holds: if W' is an affine variety and $\phi': V \to W'$ a morphism with $\phi'(t\cdot v)=\phi'(v)$ for $t \in T$, $v \in V$, then there is a unique morphism $\psi: W \to W'$ such that

$$\begin{array}{ccc} V & \xrightarrow{\phi'} & W' \\ \downarrow\phi & \nearrow_{\psi} & \\ W & & \end{array} \quad \text{,i.e., } \phi' = \phi \circ \psi$$

(Hint: use the decomposition

$$A = \bigoplus_{\chi \in X^*} A_\chi \quad \text{where } A_\chi := \{f \in A \mid f(t\cdot v)=\chi(t)f(v) \text{ for } t \in T,\ v \in V\}.$$

(4) An equivariant affine embedding of a torus T is an affine T-space V containing T as an open subvariety such that the action $T \times V \to V$ extends the product map $T \times T \to T$.

(a) There is a finitely generated sub-semigroup S of X^*, which generates X^*, such that $k[V]$ is isomorphic to the semigroup algebra $k[S]$ of S (Hint: view $k[V]$ as a $\rho(T)$-stable subspace of $k[T]$ and use that $k[T]$ is the group algebra $k[X^*]$).

(b) Conversely, for every S with the properties of (a) there is an equivariant affine embedding V such that $k[V] = k[S]$. It is unique up to isomorphism of T-spaces.

For details on equivariant embeddings we refer to G. Kempf et al., Toroidal embeddings, Lecture Notes in Math. 339, Springer, Berlin 1973, Chapter I.

2.6. One dimensional groups

2.6.1 Preview

In this section we are going to prove that a 1-dimensional connected linear algebraic group is isomorphic to $\mathbf{G}_a$ or $\mathbf{G}_m$. This is a non-trivial result.

A geometric argument to prove it, but which requires more knowledge of algebraic geometry then we presuppose here, runs as follows. Imbed the affine variety G as an open subvariety in some irreducible smooth projective curve C. So

$$G = C - F,$$

where F is finite and non-empty. The variety G has an infinite group of automorphisms via left translations by its elements. Extending them to automorphisms of C such that F is stable one sees that C has an infinite group of automorphisms fixing a point. Then C is isomorphic to the line $\mathbb{P}^1$ (a proof of this using the Jacobian of C is given in [3, p. 250-252], see also [21, p. 305-306].

Thus G is an open subset of $\mathbb{P}^1$ and it follows by elementary arguments that G is as described. The important point here is that the automorphim group of the variety $\mathbb{P}^1$ is $\mathbf{PSL}_2$ (see [3, p.252-258] for details) .

We follow here an elementary approach. The difficult case is that of a unipotent group in characteristic p>0.

Convention

We denote in this section by G a 1-dimensional connected linear algebraic group over k. We put p := char(k) (p may be zero).

2.6.2 Commutativity, the non-unipotent case

Lemma

(i) G is commutative

(ii) If G is not unipotent, then G is isomorphic to $\mathbf{G}_m$.

(iii) If G is unipotent and p>0, then for every $g \in G$ we have $g^p = e$.

Proof. (i). Fix some $g \in G$ and consider the morphism

$$\phi: G \to G, x \mapsto xgx^{-1} .$$

Since G is supposed to be connected, the image of ϕ is either a single point, $\phi G = \{g\}$, or one-dimensional, $\overline{\phi G} = G$ (see 1.8.2). In the latter case, the difference

$$G - \phi G$$

is finite (by 1.9.5). Consider G as a closed subgroup of $\mathbf{GL}_n$ (2.3.5) . If $G - \phi G$ is finite, then there are only finitely many possibilities for the characteristic polynomial $\det(T \cdot e - g)$ of $g \in G$.[27] The connectedness of G then implies that the characteristic polynomial must be constant, hence equal to $\det(T \cdot e - e) = (T-1)^n$. Thus G is unipotent, and by 2.4.11 it is contained in $\mathbf{U}_n$ and hence by Exercise 2.1.4(4) it is solvable.

On the other hand, since $g^{-1} \cdot \phi G$ lies in the commutator subgroup G' of G, the finiteness of $G - \phi G$ implies that $G - G'$ is finite, hence $\overline{G'} = G$, and 2.2.4(ii) shows that G'=G. But this contradicts the solvability of G. We

---

[27] One possibility for every $x \in G - \phi G$ and one for ϕG, the latter being the conjugation class of g.

arrive at a contradiction proving that $\phi G = \{g\}$. Since $g \in G$ was arbitrary, it follows that G is commutative. We have proved (i).

(ii). By 2.4.12 and 2.4.13, we now have that G is the direct product of the two connected subgroups G_s and G_u. Since dim G = 1, one must be trivial (use 1.8.3). If $G = G_s$ it is diagonalizable (2.4.2(ii)) and by 2.5.8(ii) it is a torus, which must be $\mathbf{G}_m$. This establishes (ii). (iii) Since in the situation of (iii), the map

$$G \to G, g \mapsto g^p ,$$

is a homomorphism of G into itself. By 2.2.5(ii), using that dim G =1, the image is either {e} or G. Since G can be considered as a subgroup of $\mathbf{U}_n$ by 2.4.11 (see also 2.4.1) if follows that all elements of G have p-power order:

$$(1-g)^{n} = 0 \text{ , hence } 0 = (1-g)^{p^r} = 1 - g^{p^r} \text{ for some r.}$$

Thus the second alternative is impossible. This proves (iii).

Remark

To deal with the remaining case when G unipotent, we need a number of auxiliary results.

2.6.3 p-Polynomials

Definition(p-Polynomial)

A polynomial $P \in k[T_1,...,T_m]$ is a p-polynomial if one of the following conditions is satisfied.

(i) p>0 and P is a linear combination of terms $T_i^{p^h}$ (i = 1,...,m and h $\geq$ 0).

(ii) P is homogeneous of degree 1.

Lemma(characterization of p-polynomials)

$P \in k[T_1,...,T_m]$ is a p-polynomial if and only if

(1) $P(T_1+U_1,...,T_m+U_m)=P(T_1,...,T_m)+P(U_1,...,U_m)$

where T_i and U_j denote Indeterminates.

Proof. It suffices to prove that a polynomial P satisfying (1) is a p-polynomial. Let D_i denote the partial derivative in $k[T_1,...,T_m]$ with respect to T_i. Then (1) implies that

$$D_i P(T) = \frac{P(T+\lambda e_i)-P(T)}{\lambda} \Big|_{\lambda=0} = \frac{P(\lambda e_i)}{\lambda} \Big|_{\lambda=0} = a_i \in k$$

is a constant.Write

$$Q(T_1,...,T_m) = P(T_1,...,T_m) - \sum_{i=1}^{n} a_i T_i .$$

Then $D_iQ = 0$ for i=1,...,m. If the characteristics is zero, this implies that Q is a constant (treat the case m=1 and use induction on m).

$$Q(T_1,...,T_m) = Q(0,...,0) = P(0,...,0).$$

Since P satisfies condition (1), P(0) = P(0)+P(0) hence P(0) = 0, we see that Q is zero, hence

$$P(T_1,...,T_m) = \sum_{i=1}^{n} a_i T_i .$$

This proves the claim in case the characteristics is zero. In case p>0 the identities $D_iQ = 0$ imply that there is a polynomial

$$Q_1 \in k[T_1,...,T_m]$$

with

$$Q(T_1,...,T_m) = Q_1(T_1^p,...,T_m^p) .$$

Since Q has property (1), the same is true for Q_1 (use the fact that $T_1^p,...,T_m^p$ are algebraically independent over k) . Since deg Q_1 < deg Q the induction hypothesis implies that Q_1 is a p-polynomial. But then so are Q and P.

2.6.4 Additive functions and p-dependence

Definition (additive function)

Let H be a connected linear algebraic group. An additive function α on H is an element of k[H] such that

$$\alpha(h\cdot h')=\alpha(h)+\alpha(h')$$

for arbitrary $h,h' \in H$. Note that if $\alpha_1,...,\alpha_m$ are additive functions and $P \in k[T_1,...,T_m]$ is a p-polynomial, then $P(\alpha_1,...,\alpha_m)$ is also an additive function.

Definition (p-dependence)

Let H be a linear algebraic group. The additive functions $\alpha_1,...,\alpha_m$ on H are called algebraically dependent (p-dependent) if there is a nonzero polynomial (resp. a p-polynomial) $P \in k[T_1,...,T_m]$ such that

$$P(\alpha_1(h),...,\alpha_m(h)) = 0$$

for every $h \in H$. It is clear how to define the corresponding notions of independence. If p=0 then p-dependence is the same as linear dependence.

Lemma

Let H be a linear algebraic group.

(i) If the additive functions $\alpha_1,...,\alpha_m$ on H are algebraically dependent they are p-dependent, so the notions of algebraic dependence and p-dependence of additive functions coincide.

(ii) If the additive functions $\alpha_1,...,\alpha_m$ are p-dependent there exist additive functions $\beta_1,...,\beta_n$ and p-polynomials $P_i \in k[T_1,...,T_m]$ such that the following conditions are satisfied.

(a) $n < m$.

(b) $\beta_1,...,\beta_n$ are p-independent.

(c) $\alpha_i = P_i(\beta_1,...,\beta_n)$ for every i.

Proof. (i). Let $\alpha_1,...,\alpha_m$ be algebraically dependent and take a nonzero polynomial $P \in k[T_1,...,T_m]$ of minimal degree such that

$$P(\alpha_1(h),...,\alpha_m(h)) = 0 \text{ for } h \in H.$$

Then $P(T_1+\alpha_1(h),...,T_m+\alpha_m(h))-P(T_1,...,T_m)$ is a polynomial of degree smaller than that of P, giving an algebraic dependence between $\alpha_1,...,\alpha_m$. Hence it is zero. Let $Q(U_1,...,U_m)$ denote the coefficient of some monomial $T_1^{a_1}\cdot...\cdot T_m^{a_m}$ in

$$P(T_1+U_1,...,T_m+U_m) - P(T_1,...,T_m) - P(U_1,...,U_m).$$

Then deg Q < deg P and $Q(\alpha_1(h),...,\alpha_m(h)) = 0$ $(h \in H)$. It follows that Q = 0. This establishes (i).

(ii). Assume first m = 1. Then $P(\alpha_1)=0$ for some p-polynomial $P \in k[T]$. It follows that $\alpha_1(H)$ is finite, hence $\alpha_1=0$ since H is connected. Now let m > 1, and assume that $\alpha_1,...,\alpha_m$ are p-dependent. If p=0 they are linearly dependent, and (ii) is well-known. So suppose

p>0. We may assume, replacing α_1 by a suitable linear combination of $\alpha_1,\ldots,\alpha_m$, that some dependence relation has the form[28]

(2) $$\alpha_1+c_1\alpha_1^p+\ldots+c_s\alpha_1^{p^s}+l_1(\alpha_2,\ldots,\alpha_m)^p+\ldots+ l_t(\alpha_2,\ldots,\alpha_m)^{p^t}= 0$$

where $l_i\in k[T_2,\ldots,T_m]$ are homogeneous, linear, and not all 0.[29] In other words we may assume that the linear term equals α_1 . Define

$$\tilde{\alpha}_1 := -c_1^{1/p}\alpha_1 -\ldots-c_s^{1/p}\alpha_1^{p^{s-1}} - l_1(\alpha_2,\ldots,\alpha_m) -\ldots- l_t(\alpha_2,\ldots,\alpha_m)^{p^{t-1}}.$$

This is an additive function satifying

(2') $$\alpha_1 - (\tilde{\alpha}_1)^p = 0$$

From the very definition of $\tilde{\alpha}_1$ we find a p-dependence relation for $\tilde{\alpha}_1$, $\alpha_2,\ldots,\alpha_m$ of lower degree then (2).[30] Induction on this degree then establishes (ii).

QED.

2.6.5 Polynomial cocycles

Definition

Next we establish a result about "polynomial cocycles" in $k[T_1,T_2]$. Recall that p = char(k). If p>0, put

$$c(T_1,T_2) := \frac{(T_1+T_2)^p-T_1^p-T_2^p}{p} = \sum_{i=1}^{p-1}\frac{(p-1)\cdot\ldots\cdot(p-t+1)}{i!}\,T_1^{p-i}T_2^i$$
$$\in(\mathbb{Z}/p\mathbb{Z})[T_1,T_2].$$

Lemma

Let $f \in k[T_1,T_2]$ satisfy

(3) $f(T_1+T_2,T_3) + f(T_1,T_2) = f(T_1,T_2+T_3) + f(T_2,T_3)$

(4) $f(T_1,T_2) = f(T_2,T_1)$

Then the following assertions are true.

(i) If p=0 there is some $g \in k[T]$ such that

---

[28] We may assume the relation has at least one term of degree 1, for, otherwise it would be a p-th power and we could replace it by its p-th root.

[29] Otherwise, α_1 would be p-dependent and by the induction start would be zero and could be omitted.

[30] Replace in (2) α_1 by $(\tilde{\alpha}_1)^p$ and take the p-th root.

$$f(T_1,T_2) = g(T_1+T_2) - g(T_1) - g(T_2).$$

(ii) If $p>0$ there are $g \in k[T]$, $a \in k$, $h \geq 0$ such that

$$f(T_1,T_2) = g(T_1+T_2) - g(T_1) - g(T_2) + a\cdot c(T_1,T_2)^{p^h} .$$

(iii) If moreover

$$(5) \qquad \sum_{i=0}^{p-1} f(T,iT) = 0$$

then $a = 0$.

Proof. (ii). We may assume f to be homogeneous of degree d. Let D_i denote the partial derivative with respect to $T_i (i=1,2)$. From (3) we get

$$(6) \quad (D_1 f)(T_1+T_2,T_3) + (D_1 f)(T_1,T_2) = (D_1 f)(T_1,T_2+T_3)$$

$$(7) \quad (D_1 D_2 f)(T_1+T_2,T_3) =^{31} (D_1 D_2 f)(T_1,T_2+T_3)$$

From (7) we conclude that the homogeneous polynomial $D_1 D_2 f$ is a multiple of $(T_1+T_2)^{d-2}$,

$$(D_1 D_2 f)(T_1,T_2) =^{32} b\cdot(T_1+T_2)^{d-2}$$

Case 1: $d \not\equiv 1 \pmod p$. The last identity implies

$$(*) \qquad (D_1 f)(T_1,T_2) =^{33} b\cdot((T_1+T_2)^{d-1} - T_1^{d-1}) + h(T_1, T_2^p).$$

for some homogeneous $h \in k[T_1,T_2]$ The first term on the right hand side of (*) satisfies identy (6). Hence substitution of (*) into (6) gives

$$h(T_1+T_2, T_3^p) + h(T_1, T_2^p) = h(T_1, T_2^p+T_3^p).$$

Setting $T_1=0$ and substituting $T_i \mapsto T_{i-1}$ we find:

---

[31] Differentiating (6) with respect to T_3 we get

$$(D_1 D_2 f)(T_1+T_2,T_3) = (D_1 D_2 f)(T_1,T_2+T_3).$$

[32] Substitute in (7) $T_3 =0$. Then the left hand side is a homogeneous polynomial of degree d-2 in T_1+T_2 , hence is equal to $b\cdot(T_1+T_2)^{d-2}$ for some $b \in k$

[33] Application of D_2 to this identity gives the above expression for $(D_1 D_2 f)(T_1,T_2)$. Moreover the polynomials in the kernel of D_2 are precisely those of type

$$h(T_1, T_2^p).$$

(8) $$h(T_1, T_2^p) = h(0, T_1^p+T_2^p)-h(0, T_1^p).$$

Hence the degree d-1 of $h(T_1,T_2^p)$ is a multiple of p.[34] Since by assumption $d \not\equiv 1 \pmod p$, h must be identically zero, i.e.,

(9) $$(D_1 f)(T_1,T_2) = b\cdot((T_1+T_2)^{d-1} - T_1^{d-1}).$$

Case 2: $d \equiv 1 \pmod p$. We are going to prove that identity (9) holds also in this case. The expression $b\cdot(T_1+T_2)^{d-2}$ cannot be written as an derivative with respect to T_2 of any non-zero homogeneous polynomial of degree d-1 except in case b=0. Therefore

$$(D_1 D_2 f)(T_1,T_2)=0,$$

hence $(D_1 f)(T_1,T_2) = h(T_1, T_2^p)$. From (8) we see that we have an identity (9) also in the present case.

"Integrating" identity (9), we will prove now the assertion of (ii). Again we have to distinguish several cases.

Case 1: $d \not\equiv 0 \pmod p$. From (9) we obtain

$$f(T_1,T_2) =^{35} a\cdot((T_1+T_2)^d - T_1^d - T_2^d) + h_1(T_1^p,T_2)$$

with $a \in k$ and $h_1 \in k[T_1,T_2]$.

The symmetry condition (4) implies that $h_1(T_1^p,T_2)$ must be a polynomial in T_1^p and T_2^p. Since the degree d of f is assumed to be not a multiple of p, this implies $h_1=0$. We have proved that f is of the required form in this case.

Case 2: $d \equiv 0 \pmod p$, $d>p$. The binomial coefficient

$$\binom{d-1}{p-1} = \frac{(d-1)\cdot(d-2)\cdot\ldots\cdot(d-(p-1))}{(p-1)(p-2)\cdot\ldots\cdot2\cdot1}$$

---

[34] The polynomial on the right has this property.

[35] Applying D_1 to this expression we obtain (9), hence the identity follows from the fact that the kernel of D_1 consists precisely of the polynomials of type

$$h_1(T_1^p,T_2).$$

is not a multiple of p, hence, if b is none-zero, there is a nonzero term $T_1^{p-1}T_2^{d-p}$ on the right hand side of (9). Such a term cannot be obtained by differentiation with respect to T_1. Thus b = 0, hence

$$D_1 f=0 \text{ (and } D_2 \text{ f=0 by symmetry)}$$

and f must be the p-th power of a polynomial satisfying also the conditions (3) and (4) of the Lemma. Hence we can use induction on d. We have yet to treat the induction start:

Case 3: d=p. As in case 1 we see that f can be written as

$$f(T_1,T_2) = a\cdot((T_1+T_2)^p - T_1^p - T_2^p) + h_2(T_1^p, T_2^p)$$

where h_2 is now linear. By direct calculation one sees that the conditions (3) and (4) imply that f is a multiple of $c(T_1,T_2)$ in this case. This finishes the proof of (ii).

(iii). For $f(T_1,T_2) = g(T_1+T_2) - g(T_1) - g(T_2)$ with g homogeneous the condition of (iii) is trivially satisfied:

$$\sum_{i=0}^{p} f(T,iT) = \sum_{i=0}^{p} (g((i+1)T)-g(T)-g(iT))$$

$$= p\cdot g(T)+ \sum_{i=0}^{p} g((i+1)T)-g(iT)$$

$$= p\cdot g(T) + g(p\cdot T) - g(0\cdot T)$$

On the other hand, for $f(T_1,T_2) = a\cdot c(T_1,T_2)$ (which is formally the previous case with $g(T)= a\cdot T^p /p$)the condition reads

$$0 = a\cdot(p\cdot T^p + (pT)^p)/p = a\cdot T^p ,$$

which is satisfied if and only if a=0.

(i). This is a simplified version of (ii) and left to the reader.

QED.

Corollary

Let $f \in k[S_1,...,S_n,T_1,...,T_n]$ satisfy

(3) $f(S+T,U) + f(S,T) = f(S,T+U) + f(T,U)$

(4) $f(S,T) = f(T,S)$.

If char k = p > 0, assume moreover

(5) $$\sum_{i=0}^{p-1} f(T,iT) = 0$$

Then there is some $g \in k[S_1,\ldots,S_n]$ such that

$$f(S,T) = g(S+T) - g(S) - g(T).$$

Proof. We may assume that f ist homogeneous of degree d. We proceed by induction on n. The case n = 1 follows from the previous lemma.

Consider f a

So let n > 1. Write

$$S' := (S_2,\ldots,S_n) \text{ and } T' := (T_2,\ldots,T_n)$$

consider f as a polynomial in S_1 and T_1 with coefficients in k[S',T']. Then the coefficients of f also satify the conditions of the corollary.[36]

and consider f as a polynomial in S' and T' (with coefficients from and algebraically closed extension k' of $k(S_1,T_1)$). By induction hypothesis, there is some $g' \in k'[S',T']$ such that

$$f = g'(S'+T') - g'(S') - g'(T').$$

QED.

2.6.6 Classification of connected 1-dimensional linear algebraic groups

Theorem

Let G be a connected 1-dimensional linear algebraic group. Then G is isomorphic to either $\mathbf{G}_a$ or $\mathbf{G}_m$.

Proof. By 2.6.2 we may assume that G is unipotent. We have to prove $G \cong \mathbf{G}_a$, which means (check this) that there is a nonzero additive function $\alpha \in k[G]$ such that $k[G] = k[\alpha]$.

We assume that G is a closed subgroup of some $\mathbf{U}_n$ of unipotent upper triangular matrices (see 2.4.11). Let $f_{ij} \in k[G]$ be the (i,j)-matrix entry function ($1 \le i < j \le n$). We use induction on n. For n=1 there is nothing to prove (for, $G=\mathbf{U}_1 \cong \mathbf{G}_a$ in this case). So assume n>1 and that the assertion has been proved for closed subgroups of $\mathbf{U}_{n-1}$.

---

[36] In (3) replace T by $T' = (0, T_2,\ldots,T_n)$.

There are two homomorphisms of algebraic groups

$$\phi_1, \phi_2 : U_n \to U_{n-1},$$

the first one being obtained by erasing the first row and column of a matrix, the second one by erasing the last row and column. For example,

$$\phi_1 : U_n \to U_{n-1}, \begin{pmatrix} a & \mathbf{b} \\ \mathbf{0} & \mathbf{D} \end{pmatrix} \mapsto \mathbf{D}.$$

Note that

$$\phi_1\left(\begin{pmatrix} a & \mathbf{b} \\ \mathbf{0} & \mathbf{D} \end{pmatrix} \cdot \begin{pmatrix} a' & \mathbf{b}' \\ \mathbf{0}' & \mathbf{D}' \end{pmatrix}\right) = \phi_1\left(\begin{pmatrix} aa' & a\mathbf{b}'+\mathbf{b}\mathbf{D}' \\ \mathbf{0} & \mathbf{D}\mathbf{D}' \end{pmatrix}\right) = \mathbf{D}\cdot\mathbf{D}'.$$

By induction, there are additive functions $\alpha_1, \alpha_2 \in k[G]$ such that

$$k[\phi_i G] = k[\alpha_i] \text{ for } i=1,2.$$

This means that the f_{ij} with $i>1$ lie in $k[\alpha_1]$ and those with $j<n$ in $k[G]$. Since dim $G = 1$, we have that α_1 and α_2 are algebraically dependent. By 2.6.4 there is an additive $\beta \in k[G]$ such that $\alpha_1, \alpha_2 \in k[\beta]$. Hence all f_{ij} with $(i,j) \neq (1,n)$ are in $k[\beta]$.

From the multiplication rule for matrices we see that there is a unique $f \in k[T_1, T_2]$ such that

$$f_{1n}(xy) - f_{1n}(x) - f_{1n}(y) = f(\beta(x), \beta(y)) \text{ for } x,y \in G,$$

and it follows that f satisfies (3) and (4) of 2.6.5.

[By definition,

$$f(\beta X, \beta Y) = \sum_{i=2}^{n-1} f_{1i}(X) f_{in}(Y)$$

Therefore, since the functions f_{ij} are linear,

$$f(\beta X+\beta Y,\beta Z)+f(\beta X,\beta Y)-f(\beta X,\beta Y+\beta Z)-f(\beta Y,\beta Z)$$

$$= \sum_{i=2}^{n-1} (f_{1i}(X+Y)f_{in}(Z)+f_{1i}(X)f_{in}(Y)-f_{1i}(X)f_{in}(Y+Z)-f_{1i}(Y)f_{in}(Z)) = 0$$

Since the group G is commutative, $f(\beta X, \beta Y)=f(\beta Y, \beta X)$.]

If $p>0$, (5) also holds

$$\sum_{j=0}^{p-1} f(\beta X, j\beta Y) = \sum_{j=0}^{p-1} \sum_{i=2}^{n-1} f_{1i}(X)\ f_{in}(jX) = (\sum_{j=0}^{p-1} j)\ (\sum_{i=2}^{n-1} f_{1i}(X)\ f_{in}(X))$$

$$= \frac{p(p-1)}{2} \cdot (\sum_{i=2}^{n-1} f_{1i}(X)\ f_{in}(X))$$

$$= 0$$

By 2.6.5 (ii) there exists some $g \in k[T]$ with

$$f(T_1, T_2) = g(T_1 + T_2) - g(T_1) - g(T_2)$$

Then

$$\gamma(x) := f_{1n}(x) - g(\beta(x)) \in k[G]$$

is again additive:

$$\gamma(xy) = \sum_{i=1}^{n} f_{1i}(X)\ f_{in}(Y) - g(\beta(x)+\beta(y))$$

$$= f(\beta(x),\beta(y)) + f_{1n}(x) + f_{1n}(y) - g(\beta(x)+\beta(y))$$

$$= g(\beta(x)+\beta(y)) - g(\beta(x)) - g(\beta(y)) + f_{1n}(x) + f_{1n}(y) - g(\beta(x)+\beta(y))$$

$$= -g(\beta(x)) - g(\beta(y)) + f_{1n}(x) + f_{1n}(y)$$

$$= \gamma(x) + \gamma(y).$$

Since β and γ are algebraically dependent, they are expressible in an additive functions α. (by 2.6.4). By construction, every f_{ij} is in $k[\alpha]$, hence $k[G] \subseteq k[\alpha]$. Conversely, α is an additive function on G, so that $\alpha \in k[G]$ hence $k[G] = k[\alpha]$. This proves the theorem.

QED.

2.6.7 Exercises

(1) Let G be a linear algebraic group which is connected, unipotent and commutative. If p>0 assume moreover that

$$G^p = \{e\}.$$

Show that G is isomorphic to a "vector group" $(\mathbf{G_a})^n$ (Hint: proceed as in the proof of 2.6.6).

(2) (p>0) Let c be as in 2.6.6. Define the structure of a linear algebraic groups on $\mathbb{A}^2$ such that

$$(x,y)\cdot(x',y') = (x+x',y+y'+c(x,x')).$$

This group is connected, unipotent, commutative, of dimension 2. Show that it is not isomorphic to $(\mathbf{G_a})^2$.

Remarks about Exercise (1)

We have to show that there are algebraically independent additive functions

$$\alpha_i\ ,\ i = 1,\ldots, m$$

such that

$$k[G] = k[\alpha_1,\ldots,\alpha_m]$$

By assumption G is unipotent, so we may assume

$$G \subseteq U_n.$$

Denote by

$$f_{ij}: G \subseteq U_n \to k \quad (1\le 1<j\le n)$$

the projection onto the entry in position (i,j).

We use induction on n. The case n = 1 is trivial. So assume n > 1 and that the assertion has been proved for closed connected commutative subgroups of U_{n-1}.

Consider the two homomorphisms of algebraic groups

$$\phi_1: U_n \to U_{n-1}, \begin{pmatrix} 1 & a \\ 0 & A \end{pmatrix} \mapsto A,$$

and

$$\phi_2: U_n \to U_{n-1}, \begin{pmatrix} A & b \\ 0 & 1 \end{pmatrix} \mapsto A,$$

which erase the first (respectively the last) row and colum. By induction, there are two families of algebraically independent additive functions $\alpha^i_1,\ldots,\alpha^i_{r_i}$ (i=1,2) such that

$$k[\phi_i\cdot G] = k[\alpha^i_1,\ldots,\alpha^i_{r_i}].$$

Since ϕ_1 and ϕ_2 are surjective, these rings can be considered as subrings of k[G]. Then

$$f_{ij}\in k[\phi_1 G] \text{ for } i>1$$
$$f_{ij}\in k[\phi_2 G] \text{ for } j<n.$$

By 2.6.4 there are additive and linearly independent $\beta_1, \ldots, \beta_s \in k[G]$ such that

$$\alpha^i_j \in k[\beta_1, \ldots, \beta_s] \text{ for every i and j,}$$

hence

$$f_{ij} \in k[\beta_1, \ldots, \beta_s] \text{ for every i and j such that } (i,j)\neq(1,n).$$

From the multiplication rule for matrices we see that there a unique $f\in k[S_1,\ldots,S_s,T_1,\ldots,T_s]$ such that[37]

---

[37] for, the sum in the middle is in $k[\beta_1, \ldots, \beta_s]$.

$$f_{1n}(xy) - f_{1n}(x) - f_{1n}(y) = \sum_{i=2}^{n-1} f_{1i}(x)f_{in}(y) = f(\beta(x),\beta(y)).$$

From the definition of f we see that f satisfies (3) and (4) of Lemma 2.6.5 if the variables T_1 and T_2 there are replaced by the sets of variables $S_1,...,S_s$ and $T_1,...,T_s$, respectively (this follows from the associative and the commutative laws in G). If char k = p > 0, (5) also holds (by 2.6.2(iii)). Therefore by (2.6.5(i) + (iii)), if f is considered as a polynomial only in S_i and T_i then

$$f = g(S_i+T_i) - g(S_i) - g(T_i).$$

for some polynomial g whose coefficients are polynomials in the variables

$$S_1,...,S_{i-1},S_{i+1},...,S_s \text{ and } T_1,...,T_{i-1},T_{i+1},...,T_s$$

Let $g \in k[T_1,...,T_s]$ as in 2.6.5. Then

$$\gamma(x) = f_{1n}(x) - g(\beta(x))$$

is again an additive function. By 2.6.4 $\beta_1, \dots, \beta_s$ and γ are expressible by linearly independ additive functions $\gamma_1, \dots, \gamma_t$, and we have $k[G] = k[\gamma_1, \dots, \gamma_t]$.

.

QED.

Notes

Chapter 2 contains material on algebraic groups which can be handled with the limited amount of algebraic geometry developed in the first chapter. The material of the first three sections is fairly standard.

The Jordan decomposition in linear algebraic groups has been introduced as soon as possible, in 2.4. In our proof of the basic theorem (2.4.8) we do not follow the usual method, in which the group G is first imbedded into some GL_n. We use, as much as possible, the formal properties of the Jordan decomposition of linear maps of a vector space.

When the Jordan decomposition is available it is not difficult to establish the basic results about commutative linear algebraic groups and diagonalizable ones. This is done in 2.4 and 2.5.

The proof of the rigidity theorem 2.5.10 shows that the affine varitey V in the statement of that theorem may be replaced by any connected affine scheme over k. One thus gets a stronger result. It implies that a diagonalizable group has no "infinitesimal automorphisms".

The classification of 1-dimensional linear algebraic groups is always a tricky point in the theory. The reader may consult [11, 7, no.4], [3, p. 257-259], [23, no. 20]. If one does not want to invoke results from curve theory (see 2.6.1), one has trouble in handling 1-dimensional unipotent groups of characterisc p>0 (the geometric explanation seems to be that the affine line $\mathbb{A}^1$ is not simply connected in characteristic p>0). We have given an elementary treatment of these groups, in which we need the results on polynomial cocycles contained in 2.6.5 (such results are due to M. Lazard [27, lemme 3]. We also need some results on p-polynomials. Another elementary treatment, which also requires properties of p-polynomials, can be found in [23, no. 20].

3. Derivations, differentials, Lie algebras

3.1. Derivations and tangent spaces

3.1.1 Derivation of a module over a commutative ring, an exact sequence

Let R be a commutative ring, A a commutative R-algebra and M a left A-module. An R-derivation of A in M is an R-linear map $D:A \to M$ such that

$$D(ab) = a\cdot D(b)+b\cdot D(a).$$

One sees immediately that $D(1)=0$, hence

$$D(r\cdot 1) = 0 \text{ for } r \in R.$$

These derivations form an A-module denoted

$$\mathrm{Der}_R(A,M),$$

the module structure being defined by

$$(D+D')a := Da+D'a$$
$$(b\cdot D)a := b(Da)$$

The elements of $\mathrm{Der}_R(A,A)$ are called the (R-linear) derivations of A.

Let $\phi:A \to B$ is a homomorphism of R-algebras, and N a B-module, then there is an exact sequence

(1) $$0 \to \mathrm{Der}_A(B,N) \to \mathrm{Der}_R(B,N) \to \mathrm{Der}_R(A,N)$$

3.1.2 Tangent space, heuristic introduction

Let X be a closed subvariety of $\mathbf{A}^n$. We identify its algebra of regular functions k[X] with $k[T_1,...,T_n]/I$, where I is the ideal of polynomial functions vanishing on X. Assume that I is generated by $f_1,...,f_s$.

Let $x \in X$ be some point and L a line in $\mathbf{A}^n$ through x. Its points can be written as x+tv, where v is a direction vector, and t runs through k. The points of the intersection $L \cap X$ are found by solving the set of equations (for t)

(2) $$f_i(x+tv) = 0 \quad (i=1,...,s).$$

One solution is t=0.

Let D_i denote partial derivation in k[T] with repect to T_i. Then

$$f_i(x+tv) = t\cdot \sum_{j=1}^{n} v_j(D_j f_i)(x) + t^2\cdot(...) + ...,$$

and we see that t=0 will be a multiple root of the set of equations (2) if and only if

$$\sum_{j=1}^{n} v_j(D_j f_i)(x) = 0 \text{ for } i=1,...,s.$$

If this is so, we call L a tangent line anf v a tangent vector (of X in x).

Write $D' = \sum_{j=1}^{n} v_j D_j$. This is a derivation of the ring k[T]. The last set of equations then says that $(D'f_i)(x)=0$ for i=1,...,s. Denoting by M_x the maximal ideal in $k[T_1,...,T_n]$ of all functions vanishing in x, it follows that $D'I \subseteq M_x$. The linear map

$$k[T] \to k,\ f \mapsto (D'f)(x),$$

factors through k[T] /I and gives a linear map $D:k[X] \to k=k[X]/M_x$.

Viewing k as a k[X]-module k_x via the homomorphism $f \mapsto f(x)$, we see that D is in fact a k-derivation $k[X] \to k_x$.

Conversely, every element of $\mathrm{Der}_k(k[X], k_x)$ can be obtained in this manner from a derivation D' of $k[T_1,...,T_n]$ with $D'I \subseteq M_x$ (check this).We conclude that there is a bijection of the set of tangent vectors v of X at x and $\mathrm{Der}_k(k[X], k_x)$.

3.1.3 Tangent spaces

Definition for affine varieties

Let X be an affine variety and $x \in X$ a point. Then the tangent space of X at x is defined to be the vector space

$$T_x(X) := \mathrm{Der}_k(k[X], k_x)$$

where k_x is the residue class field of k[X] at x.

Differential of a morphism at a given point

Let $\phi: X \to Y$ be a morphism of affine varieties. Then the induced algebra homomorphisms of coordinate rings and residue class fields,

$$\phi^*: k[Y] \to k[X], f \mapsto f \circ \phi$$
$$\phi_x: k_y \to k_x$$

(for $x \in X$ and $y = f(x)$) define a k-linear map

$$\mathrm{Der}_k(k[X], k_x) \to \mathrm{Der}_k(k[Y], k_y), D \mapsto \phi_x^{-1} \circ D \circ \phi^*$$

which is called to be the differential of ϕ at x and is denoted

$$(d\phi)_x : T_x X \to T_y Y$$

Functoriality

By the very definition this construction is functorial, i.e.,

$$d(\phi \circ \psi)_x = d(\phi)_{\phi x} \circ d(\psi)_x$$
$$d(id)_x = id$$

In particular, the differential of an isomorphism is an isomorphism.

3.1.4 The tangent space of an open neighbourhood

Let X and Y be affine varieties and let $\phi: X \to Y$ an isomorphism onto an affine open subvariety. Then $d\phi_x : T_x X \to T_y Y$ is an isomorphism.

Proof. We may assume that X is an open subset of Y. Take some regular function $f \in k[Y]$ on Y such that

$$D(f) \subseteq X \subseteq Y.$$

Since f is also a regular function on X and D(f) coinsides with the principal open set on X of the restriction $f|_X$, we are reduced to the case X=D(f). In this case,

$$k[X] = k[Y][T]/(1-f \cdot T).$$

Surjectivity. Given a derivation $D: K[Y] \to k_x$, there is always a derivation $D': k[Y][T] \to k_x$ extending D and sending T to any given element of the base field. Since $x \in X = D(f)$, i.e., $f(x) \neq 0$, D' can be chosen such that $D'(T) := -(Df)/f(x)^2$. But then D' annihilates the ideal $(1-f \cdot T)$ and induces a derivation $k[X] \to k_x$. This proves that $d\phi_x$ is surjective. Note

that the residue class t of T is a regular function on X with value $f(x)^{-1}$ at x.

Injectivity. Follows from the fact that the extension of derivations to quotient rings is unique.

QED.

3.1.5 The case of an abstract variety, simple points, smoothness

Remark

The preceding result expresses the local character of the definition of tangent space in a point x of an affine variety X.

Tangent space at a point of an arbitrary variety

Let X be an arbitrary variety (see 1.6) and $x \in X$ any point. The tangent space of X at x is defined to be

$$T_x X := \varinjlim_{x \in U \subseteq X} T_x U$$

where the limit is taken over all open affine neighborhoods U of x (hence is canonically isomorphic to $T_x U$ for every such neighborhood).

The Differential at a point

Given a morphism $\phi: X \to Y$ of varieties, the differential of ϕ at x is defined to be

$$d\phi_x := \varinjlim_{x \in U, f(U) \subseteq V} d(\phi|_U : U \to V)$$

where the limit is taken over all pairs (U,V) of affine open subsets of X and Y, respectively, satisfying $x \in U$ and $\phi(U) \subseteq V$.

Functoriality

$$d(\phi \circ \psi)_x = d(\phi)_{\phi x} \circ d(\psi)_x$$

$$d(id)_x = id$$

This follows from the corresponding formulas for the affine situation.

Simple points

Let X be a variety. The point $x \in X$ is called a simple point of X, if

$$\dim T_x X = \dim X.$$

In this case X is also called to be smooth or non-singular at x. A variety is called to be smooth or non-singular, if all its points are simple points.

3.1.6 The tangent space as the dual of m/m^2

Let X be an affine variety and $x \in X$ any point. Then the k-linear map

$$T_x X = Der_k(k[X], k_x) \to Hom_k(M_x/M_x^2, k_x),\ D \mapsto (f \bmod M_x^2 \mapsto D(f))$$

is well-defined and an isomorphism. Here M_x denotes the ideal of regular functions on X vanishing at x.

Proof. Since k_x is annihilated by M_x the product rule for the derivation D implies that $D(M_x^2) = 0$. This shows that the above linear map is well-defined.

Injectivity. Assume that the derivations $D \in T_x X$ is mapped to the trivial homorphism. Then $D(f) = 0$ for every $f \in M_x$. For $f \in k[X]$ arbitrary let $c := f(x) \in k$. Then $f-c \in M_x$, hence

$$D(f) = D(f-c)-D(c) = 0+0 = 0,$$

i.e., D=0.

Surjectivity. Since $k \subseteq k[X]$ is a natural direct sum decomposition,

$$k[X]/M_x^2 = k \oplus M_x/M_x^2.$$

Hence any given linear map $L: M_x/M_x^2 \to k_x$ can be extended to a linear map on $k[X]/M_x^2$ by sending the unity to zero. Direct calculation shows that this is in fact a derivation:

$$L((c\cdot 1+m)\cdot(c'\cdot 1+m')) = L(cc'\cdot 1 + cm'+c'm) = cL(m')+c'L(m)$$
$$=(c\cdot 1+m)L((c'\cdot 1+m')) + (c'\cdot 1+m')L((c\cdot 1+m))$$

Composition of L with the natural homomorphism $k[X] \to k[X]/M_x^2$ gives a derivation mapping to the given linear map. This proves surjectivity. **QED**

3.1.7 Exercises

(1) Using 3.1.6, describe $T_x X$ in the following cases:

(a) X is a point, (b) $X = \mathbb{A}^n$,

(c) $X = V(xy) \subseteq \mathbb{A}^2$, x=(0,0)

(d) $X = V(x^2-y^3) \subseteq \mathbb{A}^2$, x=(0,0)

(2) Let X be an affine variety, $O_{X,x}$ the local ring of X at x (see 1.4.4(1)), and m_x the maximal ideal of $O_{X,x}$. Prove that $T_x X$ is isomorphic to the dual of the vector space m_x/m_x^2.

(3) Let X and Y be varieties and let $x \in X$, $y \in Y$ be points. Prove that

$$T_{(x,y)} X \times Y \cong T_x \oplus T_y Y.$$

(4) If X is a closed subvariety of Y, and $\phi: X \to Y$ the injection, then $(d\phi)_x: T_x X \to T_y Y$ is injective.

3.2. Differentials, separability

3.2.1 Kähler differentials

Let R be a commutative ring and A a commutative R-algebra. Denote by

$$q: A \otimes_R A \to A,\ a \otimes a' \mapsto a \cdot a'$$

the product homomorphism and by

$$I := \mathrm{Ker}(q)$$

its kernel. Then

$$\Omega_{A/R} := I/I^2$$

is called the module of (Kähler-) <u>differentials</u> of A over R. Note that this is a module over $A \otimes_R A/I = A$. The R-linear map

$$d = d_{A/R}: A \to \Omega_{A/R},\ a \mapsto da = (a \otimes 1 - 1 \otimes a \bmod I^2)$$

is called the <u>universal derivation</u> of A over R.

3.2.2 The universality property of Kähler differentials

Let R be a commutative ring and A a commutative R-algebra.

(i) For every A-module M, the map

$$\circ d: \mathrm{Hom}_A(\Omega_{A/R}, M) \to \mathrm{Der}_R(A,M),\ \phi \mapsto \phi \circ d$$

is an isomorphism of A-modules.

(ii) The pair $(\Omega_{A/R}, d)$ of an A-module, together with an R-derivation d of A to $\Omega_{A/R}$, is determined up to an isomorphism of A-modules by the property (i).

Proof. straightforward

3.2.3 Functoriality

Let R be a commutative ring and $\phi: A \to B$ an R-algebra homomorphism. Then there is a unique homomorphism of A-modules

$$\phi^0: \Omega_{A/R} \to \Omega_{B/R}$$

such that the following diagram is commutative:

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \downarrow d & & \downarrow d \\ \Omega_{A/R} & \xrightarrow{\phi^0} & \Omega_{B/R} \end{array}$$

Moreover, given any B-module N, there is a commutivative diagram

$$\begin{array}{ccc} \mathrm{Der}_R(B,N) & \xrightarrow{\circ d} & \mathrm{Hom}_B(\Omega_{B/R}, N) \\ \circ\phi \downarrow & & \downarrow \phi^0 \\ \mathrm{Der}_R(A,N) & \xrightarrow{\circ d} & \mathrm{Hom}_A(\Omega_{A/R}, N) \end{array}$$

where the horizontal homomorphisms are the isomorphisms of 3.2.2

Proof. straightforward.

3.2.4 Generators and relations for the module of Kähler differentials

Let R be a commutative ring and A a finitely generated R-algebra,

$$A = R[T_1,...,T_n]/(f_1,...,f_m).$$

Then the module of Kähler differentials

$$\Omega_{A/R} = A\cdot dt_1 + ... + A\cdot dt_m$$

is generated by the differentials of the generators $t_i = T_i \bmod (f_1,...,f_m)$. The module of relations between these differentials, i.e., the kernel of the A-linear map

$$\bigoplus_{i=1}^{n} A dT_i \to \Omega_{A/R},\ dT_i \mapsto dt_i,$$

is generated by the elements

$$df_j := \sum_{i=1}^{n} \frac{\partial f_j}{\partial T_i}(t)\cdot dT_i$$

3.2.5 Exercises

(1) If $A = R[T_1,...,T_n]$ then $\Omega_{A/R}$ is a free A-module with basis $(dT_i)_{i=1,...,n}$.

(2) In the situation of 3.2.4, with m=n=1, give a condition on $f=f_1$ under which $\Omega_{A/R}=0$. Discuss the particular case that R is a field.

(3) Let A be an R-algebra which is an integral domain, let F be the quotient field of A. Then $\Omega_{F/A} \cong \Omega_{A/R}\otimes_A F$.

(4) Let F be a field and $E:=F(x_1,...,x_n)$ be an extension field of finite type. Then $\Omega_{E/F}$ is a finite dimensional vector space over E spanned by the dx_i.

(5) Let $A = k[T_1,T_2]/(T_1^2-T_2^3)$. Show that $\Omega_{A/k}$ is not a free A-module.

(6) Let A and B R-algebras. There is an isomophism of $A\otimes_R B$-modules (all tensor products over R):

$$\Omega_{A\otimes B} \to (\Omega_{A/R}\otimes B)\oplus(A\otimes\Omega_{B/R})$$

identifying the universal differential of $A\otimes B$ with

$$(d_{A/R}\otimes id_B)\oplus(id_A\otimes d_{B/R})$$

3.2.6 Field extensions

1. The first basic exact sequence

Let F be a field, and E, E' be two extension of F of finite type with $E\subseteq E'$. Then there is an exact sequence

$$\Omega_{E'/F}\otimes_{E'},E \xrightarrow{\alpha} \Omega_{E/F} \to \Omega_{E/E'} \to 0$$

called the first basic exact sequence. Here $\alpha(d_{E'/F}a\otimes 1) = d_{E/F}a$.

Proof. By (3.1(1)) we have an exact sequence

$$0\to Der_{E'}(E,E)\to Der_F(E,E)\to Der_F(E',E)$$

Using the representation of the Der-modules as Hom-modules (3.2.2(i)) we obtain an exact sequence

$$0\to Hom_{E'}(\Omega_{E/E'}, , E)\to Hom_E(\Omega_{E/F} , E)\to Hom_{E'}(\Omega_{E/F} , E)$$

The map

$$\Omega_{E'/F}\to\Omega_{E'/F}\otimes_{E'},E, \quad u\ a \quad u\otimes 1$$

defines an isomorphism of vector spaces over E

$$Hom_{E'}(\Omega_{E'/F}\otimes_{E'},E , E) \cong Hom_{E'}(\Omega_{E'/F} , E).$$

Hence dualizing the above exact sequence, we get the result. Note that all involved vector spaces are finite dimensional.

QED.

2. Separability

The field extension E of F is called to be separable over F if for each $x\in E$ there is a polynomial $f\in F[T]$ without multiple roots such that $f(x)=0$ [26, Ch. VII,34]. We may assume f to be irreducible and in that case its derivative f' is nonzero. If char(F)=0, then every algebraic extension of F is separable.

3.2.7 The first basic exact sequence in the separable case

If E is a separably algebraic extension over E' then the isomophism α of 3.2.6 is injective.

Proof. The claim essentially means, derivations can be uniquely extented to separably algebraic extensions, which is easily checked (Take a simple algebraic extension).

QED.

3.2.8 Characterization of separability in terms of derivations (simple extensions)

Let E = F(x) be a simple field extension. Then:

(i) $\dim_E \Omega_{E/F} \leq 1$.

(ii) $\Omega_{E/F} = 0$ if and only if x is separably algebraic over F.

Proof. If x is transcendental over F, this is a consequence of Exercise 3.2.5 (1). If x is algebraic over F, we have

$$E \cong F[T]/(f),$$

where f is the minimum polynomial of x over F. The assertion then follows from 3.2.4 , using that $f'(x) \neq 0$ if and only if x is separably algebraic.

QED.

3.2.9 Characterization of separability in terms of derivations (general case)

1. Definitions

Let E be a field extension of finite type over F. Then

$$\mathrm{trdeg}_F E$$

denotes the transcendence degree of E over F. If $E=F(x_1,...,x_r)$, the trancendence degree t is the maximum number of x_i which are algebraically independent over F. In case t=r, E is purely transcendental over F. E is called to be separably generated over F if it is a separable algebraic extension of a purely trancendental extension. In case the characteristics p:=char(F) is zero, E is always separably generated over F.

The field F is called perfect if either the characteristics p=char(F) is zero or the Frobenius morphism

$$F \to F,\ x \mapsto x^p,$$

is surjective.

2. Theorem

Let E be a finitely generated field extension over F. Then:

(i) $\dim_E \Omega_{E/F} \geq \mathrm{trdeg}_F E$.

(ii) Equality holds in (i) iff E is separably generated over F.

(iii) If F is perfect then E is separably generated over F.

Proof. Standard stuff in commutative algebra.

3.2.10 Criterion for separably generated field extensions

Let F be a perfect field und E, E' two extension fields of finite type over F such that

$$F \subseteq E' \subseteq E.$$

Then the following conditions are equivatlent.

(i) E is separably generated over E'.

(ii) The natural E-linear map $\alpha: \Omega_{E'/F} \otimes_{E'} E \to \Omega_{E/F}$ is injective.

(iii) The natural E-linear map $\mathrm{Der}_F(E,E) \to \mathrm{Der}_F(E',E)$ is surjective.

Proof. (ii) ⇔ (iii). This follows from the universality property of Kähler differentials (see 3.2.2), i.e.

$$\mathrm{Der}_F(E', M) = \mathrm{Hom}_{E'}(\Omega_{E'/F}, M)$$

for E'-Moduls M and similarly with E instead of E. Note that

$$\mathrm{Hom}_E(\Omega_{E'/F} \otimes_{E'} E, E) = \mathrm{Hom}_{E'}(\Omega_{E'/F}, E) = \mathrm{Der}_F(E',E).$$

(i) ⇔ (ii). By 3.2.9(iii) and (ii) one has

$$\dim_{E'} \Omega_{E'/F} = \mathrm{tr.deg}_F E'$$

$$\dim_E \Omega_{E/F} = \mathrm{tr.deg}_F E$$

hence from the exact sequence of 3.2.6

$$\dim \Omega_{E/E'} \geq \mathrm{tr.deg}_{E'} E$$

where equality holds if and only if α is injective. Thus the claim follows from assertion (ii) of the theorem of 3.2.9.

QED.

3.2.11 Exercise

(1) Let E' ⊆ E be finitely generated over the perfect field F. Prove that if E is separably algebraic over E', then the Morphisms α in 3.2.10 is an isomorpisms.

(2) Let F be a perfect field, E a field extension of F of finite type. Define

$$p := \mathrm{char}\ (F).$$

If $a \in E$ is such that $d_{E/F} a = 0$, then $a \in F$ in case p = 0 and a is a p-th power of an element of E if p>0. (Hint : use 3.2.9(iii) and 3.1(i)).

3.2.12 The Module $\mathfrak{M}(A)$ associated with a matrix

Let R be an integral domain with fraction field F,

$$F := Q(R).$$

For none-zero elements $f \in R$ we write

$$R_f := R[T]/(1-fT) = R[f^{-1}] \subseteq F,$$

and for every R-Module M let

$$M_f := M \otimes_R R_f .$$

Let $A \in M_{m,n}(R)$ be an m×n-Matrix with entries in R and

$$f_{A^T}: R^m \to R^n, x \mapsto A^T x,$$

the linear map defined by the transpose of A. The cokernel of this map is denoted

$$\mathcal{M}(A) := \mathrm{Coker}(f_{A^T})$$

Further, let $GL_n(R)$ be the group of invertible n×n-matrices with entries in R.

3.2.13 A normalization lemma

Let R be an integral domain and $A \in M_{m,n}(R)$ an m×n-matrix with entries from R. Then:

(i) $\mathcal{M}(BA) = \mathcal{M}(A)$ for every $B \in GL_m(R)$.

(ii) $\mathcal{M}(AC) \cong \mathcal{M}(A)$ for every $C \in GL_n(R)$.

(iii) There are $f \in R-\{0\}$, $B \in GL_m(R_f)$, $C \in GL_n(R_f)$ such that

$$A = B \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} C$$

where I_r is the r×r-identy matrix.

Proof. Idea: solve the problem over the quotient field and note that there are only finitely many elements occuring as denominators

…

QED.

3.2.14 Lemma: the freeness locus of $\mathcal{M}(A)$

Let R be an integral domain and $A \in M_{m,n}(R)$ an m×n-matrix with entries from R. Then there is an element $f \in R-\{0\}$ such that $\mathcal{M}(A)_f$ is a free R_f-module. Moreover, one may choose f such that the residue classes of certain standard unit vectors e_i of R^n form a basis of $\mathcal{M}(A)$.

Proof.

…

QED.

3.2.15 Specialization to the geometric case

Let X be an irreducibel affine variety over k. We are going to apply the preceding results for

$$R := k[X]$$
$$F := k(X).$$

Recall that the field k is algebraically closed, hence perfect. If $x \in X$, let

$$M_x := \{f \in k[X] \mid f(x) = 0\}$$

be the maximal ideal defined by the point x. If M a a k[X]-module, put

$$M(x) := M/M_x M.$$

This is a vector space over k (sind $k[X]/M_x \cong k$) called the fiber of M at x.

Let A be as in 3.2.12 be an m×n-matrix with entries in R := k[X]. Since the entries of A are functions on X, the matrix A(x) with entries in k is defined. It is immediate that

$$\mathfrak{M}_{k[X]}(A)(x) = \mathfrak{M}_k(A(x)).$$

3.2.16 Lemma: the freeness locus of $\mathfrak{M}(A)$

Let X be an irreducible affine variety,

$$R := k[X]$$

and $A \in M_{m,n}(R)$ an m×n-matrix with entries from R. Denote by r the rank of the matrix A considered over the quotient field of R.

(i) The set of $x \in X$ such that

$$\dim \mathfrak{M}_{k[X]}(A)(x) = n\text{-}r$$

is open and none-empty.

(ii) If $x \in X$ and $\dim \mathfrak{M}_{k[X]}(A)(x) = n\text{-}r$ there is some $f \in k[X]$ with $f(x) \neq 0$ such that $\mathfrak{M}_{k[X]}(A)_f$ is a free $k[X]_f$-module of n-r.

Proof.

QED.

Geometric terminology

Let Y be an affine variety. We put

$$\Omega_X := \Omega_{k[X]/k}.$$

If $x \in X$, the tangent space

$$T_x X = \mathrm{Der}_k(k[X], k_x)$$

(see 3.1.3) is, by 3.2.2(i) isomorphic to

$$T_x X \cong \mathrm{Hom}_{k[X]}(\Omega_X, k_x).$$

Since for any k[X]-module M we have

$$\mathrm{Hom}_{k[X]}(M, k_x) = \mathrm{Hom}_k(M(x), k),\ M(x) := M/M_x M,$$

it follows

$$T_x X \cong \mathrm{Hom}_k(\Omega_X(x), k).$$

The dual vector space of the tangent space $T_x X$ is called the cotangent space (of X at x) and is denoted $(T_x X)^*$. It can be identified with the vector space $\Omega_X(x)$.

3.2.17 Theorem: the smooth locus and freeness of differentials

Let X be an irreducible variety of dimension e.

(i) If x is a simple point of X, there is an affine open neighborhood U of x on X such that Ω_U is a free k[U]-module with a basis

$$(df_1,\ldots,df_e)$$

for suitable $f_i \in k[U]$.

(ii) The simple points of X form a none-empty open subset of X.

Proof. Requires the previously skippen preparations.

...

QED.

3.2.18 Exercises

(1) The elements of a system of local coordinates are algebraically independent over k.

(2) Let X be an irreducible affine variety. If $\Omega_X := \Omega_{k[X]/k}$ is a free k[X]-module, then X is smooth.

3.2.19 Definitions: dominant and separable morphisms

Let $\phi: X \to Y$ be a morphism of irreducible varieties. This morphisms is called dominant, if $\phi(X)$ is dense in Y. If this is the case, then there is by 1.9.1(ii) an injection

$$\phi^*: k(Y) \to k(X)$$

of the fields of rational functions on y and X, respectively. So we can view k(X) as a field extension of k(Y). If this field extension is separably generated, then the morphism ϕ is called separable.

Remarks in the affine situation

(i) Let $\phi: X \to Y$ be a dominant morphism of irreducible varieties. Assume moreover that X and Y are affine and denote by ϕ^* the canonical injection

$$\phi^*: k[Y] \to k[X].$$

According to 3.2.3 there is a homomorphism of k[Y]-modules

$$(\phi^*)^0: \Omega_Y \to \Omega_X.$$

For $x \in X$ let k_x be the k[X]-module k, with the module structure define via evaluation at x (see 3.1.2). Viewed as an k[Y]-module via ϕ^* this is $k_{\phi x}$ (check this).

(ii) We are going to study the linear map

$$(d\phi)_x : T_x X \to T_{\phi x} Y$$

of 3.1.3. Using the preceding remark and the diagramm of 3.2.3, we see that we can view this map also as the homomorphism

$$\mathrm{Hom}_{k[X]}(\Omega_X, k_x) \to \mathrm{Hom}_{k[Y]}(\Omega_Y, k_{\phi x})$$

induced by $(\phi^*)^0$. It can also be viewed as a linear map

$$\mathrm{Hom}_k(\Omega_X(x), k) \to \mathrm{Hom}_k(\Omega_Y(\phi x), k).$$

3.2.20 Theorem (separability and surjectivity of the differential)

Let X and Y be irreducible varieties and $\phi: X \to Y$ a morphism.

(i) Assume that $x \in X$ and $y := \phi(x) \in Y$ are simple points of X and Y, respectively, such that

$$(d\phi)_x : T_x X \to T_y Y$$

is surjective. Then ϕ is dominant and separable.

(ii) Assume that ϕ is dominant and separable. Then there is a none-empty open subset $U \subseteq X$ such that for $x \in U$, the point $y := \phi(x)$ is simple on Y and that

$$(d\phi)_x : T_x X \to T_y Y$$

is surjective.

Proof. Requires the above skipped preparations.

QED.

3.2.21 Theorem (smoothness of G-spaces and separability of morphisms of G-spaces)

Let G be a connected algebraic group.

(i) Let X be a homogeneous space for G.Then X is irreducible and smooth. In particular, G is smooth.

(ii) Let $\phi: X \to Y$ be a G-morphism of homogeneous spaces. The ϕ is separable if and only if the tangent map $(d\phi)_x : T_x X \to T_{f(x)} Y$ is surjective for some $x \in X$. If so, then $(d\phi)_x$ is surjective for every point $x \in X$.

(iii) Let $\phi: G \to G'$ be a surjective homomorphism of algebraic groups. Then ϕ is separable if and only if $(d\phi)_e$ is surjective.

Proof. (i). Fix some point $x \in X$ and consider the morphism

$$G \to X, g \mapsto gx.$$

Since X is a homogeneous space, this morphism is surjective. Hence X is irrreducible.
For every $g \in G$ the morphism

$$X \to X, x \mapsto gx,$$

is an isomorphism of X. Hence if x is a simple point of X, the same is true for gx. Since G act transitively on X, every point of X is a simple point of X, i.e., X is smooth (cf. 3.2.17).
(ii). Follows from 3.2.20.
(iii). The is a consequence of (ii), viewing G and G' as homogeneours spaces for G.
QED.

3.3. The Lie algebra of a linear algebraic group

3.3.1 Terminology

Let G be a linear algebraic group. We will use the following notation.

$L_g : G \to G,\ x \mapsto gx,$	the left translation on G defined by $g \in G$
$R_g : G \to G, x \mapsto xg,$	the right translation on G defined by $g \in G$
$A := k[G]$	the affine coordinate ring of the group G
$\lambda_g : A \to A, f \mapsto f \circ L_g,$	the left translation on A defined by $g \in G$
$\rho_g : A \to A, f \mapsto f \circ R_g,$	the right translation on A defined by $g \in G$
$q: A \otimes_k A \to A, a \otimes a' \mapsto a \cdot a',$	the multiplication map
$\lambda_g : \Omega_{G/k} \to \Omega_{G/k}, a \cdot da' \mapsto \lambda_g a \cdot d(\lambda_g a')$,	the left translation on $\Omega_{G/k}$ defined by $g \in G$
$\rho_g : \Omega_{G/k} \to \Omega_{G/k}, a \cdot da' \mapsto \rho_g a \cdot d(\rho_g a')$,	the right translation on $\Omega_{G/k}$ defined by $g \in G$
$Int_g : G \to G, x \mapsto gxg^{-1},$	the interior Automorphism of G defined by $g \in G$
$Ad_g : T_e X \to T_e X, X \mapsto X \circ Int_g$	the linear map on the tangent space induced by the action of g on G as an interior automorphism.
$(Ad_g)^* : (T_e G)^* \to (T_e G)^*, l \mapsto l \circ Ad_g$,	the linear map on the tangent space induced by the action of g on G as an interior automorphism.

Remarks

1. The Group G acts by translations from the left on itself, but from the rigth on A and $\Omega_{G/k}$. Moreover, the differential

$$d: A \to \Omega_{G/k}, a \mapsto da,$$

is an equivariant map with respect to these actions:

$$\lambda_g(da) = (\lambda_g 1) \cdot d(\lambda_g a) = d(\lambda_g a)$$

$$\rho_g(da) = (\rho_g 1)\cdot d(\rho_g a) = d(\rho_g a)$$

2. By 3.1.6 the restriction of derivations $X: A \to k_e$ to the maximal ideal M_e of function vanishing at x induces an isomorphism of vector spaces

$$T_eG \to \mathrm{Hom}_k(M_e/M_e^2, k_e),\ X \mapsto \left\{(a \bmod M_e^2) \mapsto X(a)\right\}$$

i.e., the following pairing

$$T_eG \times M_e/M_e^2 \to k_e,\ (X, a \bmod M_e^2) \to X(a)$$

is exact. In particular, the (k-linear) evaluation map

$$M_e/M_e^2 \to (T_eG)^*,\ a \bmod M_e^2 \mapsto (X \mapsto X(a))$$

is bijective. Identifying the latter two vector spaces and letting $\delta a := (a - a(e)) \bmod M_e^2$ we obtain

$$(\delta a)(X) := X \text{ evaluated at } a - a(e) = X(a)$$

(since k-derivations are identically zero on k).

3.3.2 Trivializing the cotangent bundle

Let G be a linear algebraic group over k. Then the map

$$\phi: \Omega_{G/k} \to k[G] \otimes_k (T_eG)^*,\ da \mapsto \delta(R_y a)$$

is an isomorphism of k[G]-modules, where the module structur of $\Omega_{G/k}$ is given by

$$(a, a'\cdot da'') \mapsto (aa')\cdot da''$$

Moreover,

(i) The action of $g \in G$ on the differentials via left translation corresponds under this isomorhism to the action on the first factor:

$$\phi \circ \lambda_g \circ \phi^{-1} = \lambda_g \otimes id$$

(ii) The action of $g \in G$ on the differential via right translation corresponds up to innter automorphism to the action on the first factor:

$$\phi \circ \rho_g \circ \phi^{-1} = \rho_g \otimes (Ad_g^{-1})$$

(iii) The universal differential d on G corresponds under this isomorphism to the derivation given by the following formula:

$$(\phi \circ d)(f) = \sum_{i=1}^{r} f_i \otimes \delta g_i$$

if f is a function on G such that $f \circ \mu = \sum_{i=1}^{r} f_i \otimes g_i$. Here $\mu: G \times G \to G$ denotes the multiplication map.

Remarks

- The above formula for ψ means that, for a given function $a \in k[G]$, one has to take the right translate $(R_y a)(x)$ for every $y \in G$ and consider it as a function of y. Hence

$$\delta(R_y a)$$

can be considered as an element of $(T_eG)^*$ depending upon $x \in G$, hence as an element of $k[G] \otimes_k (T_eG)^*$.

- The module structure of $\Omega_{G/k}$ comes from the module structure of $k[G] \otimes k[G]$ given by

$$k[G] \otimes_k k[G] \to k[G], (a, a' \otimes a'') \mapsto aa' \otimes a''.$$

which is obviously well-defined.

Proof. Consider the isomorphism of algebraic varieties

$$G \times G \to G \times G, (x,y) \mapsto (x, xy)$$

which can be written as a composition

$$G \times G \xrightarrow{\Delta \times id} G \times G \times G \xrightarrow{id \times \mu} G \times G, (x,y) \mapsto (x,x,y) \mapsto (x,xy)$$

It induces an isomorphism of the algebra $A \otimes_k A = k[G \times G]$,

(1) $$\psi = (\Delta \otimes id)^* \circ (id \otimes \mu)^* : A \otimes A \to A \otimes A,\ a(x,y) \mapsto a(x,xy) = a \circ (id \times \mu) \circ (\Delta \times id)$$

such that the following diagrams are commutative:

(2)
$$\begin{array}{ccc} A \otimes A & \xrightarrow{\lambda_g \otimes \lambda_g} & A \otimes A \\ \psi \downarrow & & \downarrow \psi \\ A \otimes A & \xrightarrow{\lambda_g \otimes id} & A \otimes A \end{array} \qquad \begin{array}{ccc} A \otimes A & \xrightarrow{\rho_g \otimes \rho_g} & A \otimes A \\ \psi \downarrow & & \downarrow \psi \\ A \otimes A & \xrightarrow{\rho_g \otimes Int_g^{-1}} & A \otimes A \end{array}$$

Note that,

$$\psi((\lambda_g \otimes \lambda_g)(a)) = \psi(a \circ (L_g \otimes L_g)) = a \circ (L_g \otimes L_g) \circ (id \times \mu) \circ (\Delta \times id)$$

$$(\lambda_g \otimes id)(\psi(a)) = (\lambda_g \otimes id)(a \circ (id \times \mu) \circ (\Delta \times id)) = a \circ (id \times \mu) \circ (\Delta \times id) \circ L_g \times id$$

Hence, to prove the first diagram (1) is commutative, it is sufficient to show, the following two maps are equal.

$$(L_g \times L_g) \circ (id \times \mu) \circ (\Delta \times id) : (x,y) \mapsto (x,x,y) \mapsto (x,xy) \mapsto (gx, gxy)$$

$$(id \times \mu) \circ (\Delta \times id) \circ (L_g \times id) : (x,y) \mapsto (gx,y) \mapsto (gx,gx,y) \mapsto (gx,gxy)$$

and similarly, the second diagram (2) is commutative, since the following two maps are equal.

$$(R_g \times R_g) \circ (id \times \mu) \circ (\Delta \times id) : (x,y) \mapsto (x,xy) \mapsto (xg, xyg)$$

$$(id \times \mu) \circ (\Delta \times id) \circ (R_g \times Int_g^{-1}) : (x,y) \mapsto (xg, g^{-1}yg) \mapsto (x, xyg)$$

From the very definition of ψ we see that ψ maps $I = Ker(q: A \otimes A \to A)$ onto the ideal of functions vanishing on $G \times \{e\}$:

$$a \in I \Leftrightarrow a(x,x) = 0 \text{ for } x \in G \Leftrightarrow (\phi a)(x,e) = 0 \text{ for } x \in G$$

In other words, $\psi I = k[G] \otimes_k M_e$. Therefore, $\Omega_{G/k} = I/I^2$ is isomorphically mapped to $k[G] \otimes M_e/M_e^2$. This gives the claimed isomorphism

$$\phi : \Omega_{G/k} \to k[G] \otimes_k (T_eG)^*$$

Note that

$$\phi(da) =^{38} - \phi(cl(a(y) - a(x))) = a(xy) - a(x) \bmod k[G]\otimes M_e^2$$
$$= - (R_y a)(x) - (R_e a)(x) \bmod k[G]\otimes M_e^2$$
$$= - \delta(R_y a)(x)$$

In particular, if a=f and $R_y f = f(?y) = \sum_{i=1}^{r} f_i(?)g_i(y)$,

hence

$$\delta(R_? f) = \sum_{i=1}^{r} f_i\otimes(g_i - g_i(e) \bmod M_e^2)$$

This gives the claim of assertion (iii):

$$(\phi\circ d)(f) = \phi(df) = - \delta(R_? f) = - \sum_{i=1}^{r} f_i\otimes(g_i - g_i(e) \bmod M_e^2)$$

The two commutative squares above give the assertions of (i) and (ii). **QED**.

3.3.3 The Lie algebra structure on Der(A,A)

Let A be an algebra over k. Then the space of derivations

$$\mathbf{D} := Der_k(A,A)$$

is a Lie algebra with the Lie bracket

$$[D,D'] := D\circ D' - D'\circ D$$

If the characteristics p = char(k) > 0 is positive, Leibniz' formula shows that

$$D^p(ab) = \sum_{p=0}^{p} \binom{p}{i} D^i a\cdot D^{p-i} b = a\cdot D^p b + b\cdot D^p a$$

for a,b∈ A. Hence D^p is again a derivation. This means, in this case **D** is a restricted Lie algebra in the following sense.

Definition: Restricted Lie algebra

Let k be a field of positive characteristics p := char(k) > 0. Then a Lie algebra **D** over k is called <u>restricted</u> or <u>p-Lie algebra</u> if it is equipped with a mapping

$$\mathbf{D} \to \mathbf{D}, D \mapsto D^{[p]}$$

called p-operation such that

(a) $(\xi D)^{[p]} = \xi^p D^{[p]}$ ($\xi\in k$, $D\in\mathbf{D}$)

(b) $(ad\ D)^p = ad(D^{[p]})$

---

[38] The sign on the right is, to some extent, a question of convention. Here we use the convention

da = residue class of $(a\otimes 1 - 1\otimes a)$.

We could equally have choosen the other sign in the definition of da.

(c) $(D+D')^{[p]} = D^{[p]} + D'^{[p]} + \sum_{i=1}^{p-1} i^{-1} s_i(D,D')$

where $s_i(D,D')$ is the coefficient of ξ^i in $\mathrm{ad}(\xi D+D')^{p-1}(D)$ "Jacobson's formula"). Here we write

$$(\mathrm{ad}\ D)D' := [D, D'].$$

Definition: The Lie algebra L(G) of an algebraic group

Let A = k[G] be the coordinate ring of an algebraic group G. Then G acts by left an right translations on the Lie algebra of vector fields on G,

$$\mathbf{D} = \mathrm{Der}_k(A, A).$$

The actions are given by

$$L_g: G\times D \to D,\ (g,X) \mapsto \lambda_g \circ X \circ \lambda_g^{-1}$$

$$R_g: G\times D \to D,\ (g,X) \mapsto \rho_g \circ X \circ \rho_g^{-1}$$

The Lie algebra of G is defined to be the subalgebra of **D** of all vector fields invariant under all left translations:

$$L(G) := \{X\in \mathrm{Der}_k(A,A) \mid X\circ\lambda_g = \lambda_g \circ X\}$$

Since left and right translations commute, L(G) is stable under right translations, i.e., G acts on L(G) via right translations. Moreover, it is easy to see that L(G) is also stable under the p-operations on $\mathbf{D} = \mathrm{Der}_k(A,A)$.

3.3.4 Trivializing the tangent bundle

There is an isomorphism of k[G]-modules

$$\psi: \mathbf{D} = \mathrm{Der}_k(k[G],k[G]) \to k[G]\otimes_k T_eG$$

where the module structure on the right is defined by

$$a\cdot(f\otimes X) = (af)\otimes X.$$

Moreover,

(i) $\psi\circ\lambda_g\circ\psi^{-1} = \lambda_g\otimes id$

(ii) $\psi\circ\rho_g\circ\psi^{-1} = \rho_g\otimes \mathrm{Ad}_g$

(iii) $\psi^{-1}(a\otimes X)(f) = -\sum_{i=1}^{r} (af_i)\cdot X(g_i)$ if $f\in k[G]$ is such that $f\circ\mu = \sum_{i=1}^{r} f_i\otimes g_i$.

Proof. Dualizing 3.3.2 we obtain a linear isomorphism over A := k[G],

(1) $\mathrm{Hom}_A(A\otimes_k (T_eG)^*, A) \to \mathrm{Hom}_A(\Omega_{G/k}, A),\ h \mapsto (df \mapsto -h(\delta(R_y f)))$

If $f\circ\mu = \sum_{i=1}^{r} f_i \otimes g_i$ then by 3.3.2(iii),

$$\delta(R_y f) = \sum_{i=1}^{r} f_i \otimes \delta g_i$$

hence for A-linear maps h,

$$h(\delta(R_y f)) = \sum_{i=1}^{r} f_i \; h(1\otimes\delta g_i)$$

The left hand side Hom module is isomorphic to

$$k[G]\otimes_k T_eG \cong \mathrm{Hom}_A(A\otimes_k (T_eG)^*, A),\ a\otimes X \mapsto (a'\otimes 1 \mapsto aa'a1(X)),$$

hence the isomorphism writes

$$k[G]\otimes_k T_eG \to \mathrm{Der}_k(A,A),\ a\otimes X \mapsto (f \mapsto af - \sum_{i=1}^{r} f_i \; h(1\otimes\delta g_i))$$

where h is the map $a'\otimes 1 \mapsto aa'a1(X)$, i.e.,

$$h(1\otimes\delta g_i) = a(\delta g_i)(X) =^{39} aX(g_i)$$

Thus the isomorphism is given as follows:

$$k[G]\otimes_k T_eG \to \mathrm{Der}_k(A,A),\ a\otimes X \mapsto (f \mapsto af - \sum_{i=1}^{r} af_i \; X(g_i))$$

This gives the claimed isomorphism and assertion (iii). Assertions (i) and (ii) are dualizations of the corresponding formulas of 3.3.2. **QED**.

3.3.5 The Lie algebra structure and the tangent space at e

Let α_G be the linear map

$$\alpha_G : D = \mathrm{Der}_k(k[G], k[G]) \to T_eG,\ X \mapsto (f \mapsto aX(f)(e))$$

Then:

---

[39] The differential δg_i applied to the fector field X is just $X(g_i)$.

(i) α_G defines an isomorphism of vector spaces $\beta_G: L(G) \to T_eG$ such that the right translation ρ_g on the Lie algebra corresponds to Ad_g^{-1} on the tangent space.[40]

(ii) $Ad^{-1}: G \to Aut(T_eG)$ is a rational representation, called the adjoint representation of G on the tangent space.

Proof. Consider the commutative diagram

$$\begin{array}{ccccc} T_eG & \xleftarrow{\alpha_G} & Der_k(A,A) & \xrightarrow{\psi} & A\otimes T_eG \\ \| & & \cup & & \cup \\ T_eG & \leftarrow & L(G) & \to & k\otimes T_eG \end{array}$$

By the formulas (i) and (ii) of 3.3.4 the left invariant vector fields of L(G) are mapped under ψ to the elements of[41] $k\otimes T_eG$, i.e., the lower horizontal map on the right is an isomorphism. Moreover, on $k\otimes T_eG$ the map $\alpha_G \circ \psi^{-1}$ acts as follows (by 3.3.4(iii)):

$$(1) \quad (\alpha_G \circ \psi^{-1})(1\otimes X)(f) = -\sum_{i=1}^{r} (f_i X(g_i))(e)$$

$$= -\sum_{i=1}^{r} f_i(e) X(g_i)$$

$$= -X(\sum_{i=1}^{r} f_i(e) g_i)$$

$$= -X(f).$$

This shows, both lower horizontal maps are isomorphisms. According to 3.3.4(ii),

$$\psi \circ \rho_g \circ \psi^{-1} = \rho_g \otimes Ad_g ,$$

e.g. right translation with g on L(G) corresponds to $Id\otimes Ad_g$ on $k\otimes T_eG$, hence to Ad_g on T_eG. This proves assertion (i).

As for (ii) we have to show that

---

[40] Note that, $Ad_g : T_eX \to T_eX, X \mapsto X\circ Int_g$ defines a right operation of G on the tangent space. To get a left operation, we have to compose it with the inversion map $G \to G$.

[41] According to 3.3.4 (i), $\psi \circ \lambda_g \circ \psi^{-1} = \lambda_g \otimes id$, invariance under left translations on $Der_k(A,A)$ correspond to invariance under $\lambda_g \otimes id$ for the elements of $A\otimes T_eG$.

$$G \times T_eX \to T_eX, (g, X) \mapsto X \circ Int_g^{-1},$$

is a regular map.
As we have seen in 2.3.4, the operation of G on itself by conjugation induces a rational representations on the finite dimensional invariant subspaces of k[G]. This implies that this operation induces a rational representation on[42] $M_e/M_e^2 = (T_eX)^*$. Passing to the induces representation on the dual we see that the representation of G on the tangent space is a rational representation.
QED.

3.3.6 Functoriality: the case of closed immersions

Let $G' \subseteq G$ be a closed subgroup of G with ideal $I \subseteq k[G]$. Then

$$D_{G,G'} := \{X \in Der_k(k[G], k[G]) \mid X(I) \subseteq I\}$$

is a sub-Lie-algebra of $Der_k(k[G],k[G])$, and there is an obvious homomorphism of Lie-algebras

$\lambda: D_{G,G'} \to D_{G'} := Der_k(k[G'], k[G']), X \mapsto (f \bmod I \mapsto X(f) \bmod I)$

such that the following diagram is commutative:

$$\begin{array}{ccc} D_{G,G'} & \xrightarrow{\lambda} & D_{G'} \\ \alpha_G \downarrow & & \downarrow \alpha_{G'} \\ T_eG & \supset & T_eG' \end{array},$$

Moreover,

$$T_eG' =^{43} \{X \in T_eG \mid X(I) = 0\}$$

3.3.7 Lemma

λ induces an isomorphism $D_{G,G'} \cap L(G) \to L(G')$.

Proof. By 3.3.5 the restriction of α_G (resp. $\alpha_{G'}$) to the Lie algebra L(G) (resp. L(G')) is injective (resp. an isomorphism). Hence λ is

---

[42] Consider a finite dimensional linear invariant subspace of M_e containing a finite set of generators of the ideal M_e.

[43] Note that for $f \in I$, $X(f) = df(X)$. Hence the identity says, that T_eG' is the linear subspace of T_eG defined by the linear equations

$$df = 0 \text{ with } f \in I.$$

given by the differentials of the equations of G', But this is true for arbitrary affine subvarietes G' of arbitrary affine varieties G.

injective on the intersection $D_{G,G'} \cap L(G)$ (since the above diagram is commutative.

To prove surjectivity, we have to show that for $X \in T_e G'$ the invariant vector field $\psi^{-1}(1 \otimes X)$ (which maps to -X under λ)[44] is in $D_{G,G'}$.

Let $f \in I$. We have to show $\psi^{-1}(1 \otimes X)(f) \in I$. Write

$$f = \sum_{i=1}^{r} f_i \otimes g_i$$

Since $f(xy) = 0$ for $x,y \in G'$ and since the ideal defining $G' \times G'$ is $I \otimes A + A \otimes I$ we may assume that $f_i \in I$ or $g_i \in I$ for every i. From the formula of 3.3.4 we see

$$\psi^{-1}(1 \otimes X)(f) = \sum_{i=1}^{r} f_i X(g_i)$$

Since each term on right vanishes on G', this is a function of I as required.

QED.

Convention

In that what follows, we identify the Lie algebra L(G) and the tangent space $T_e G$ via ψ. We thus obtain a Lie algebra structure on the latter space.

We shall also denote the Lie algebra of a linear algebraic group G, H, ... by $\mathfrak{g}$, $\mathfrak{H}$, ...

If $\Phi: G \to G'$ is a homomorphism of algebraic groupsm we write $d\Phi$ for the induced tangent map

$$(d\Phi)_e : \mathfrak{g} \to \mathfrak{g}'.$$

We call $d\Phi$ the differential of Φ.

3.3.8 Functoriality: general case

Let $\phi: G \to G'$ be a homomorphism of linear algebraic groups. Then $d\phi : \mathfrak{g} \to \mathfrak{g}'$ is a homomorphism of Lie algebras which is compatible with the p-operations if $p := \mathrm{char}(k) > 0$.

Proof. Consider the factorization

$$G \xrightarrow{\rho} G \times G' \xrightarrow{\sigma} G'$$

where

$$\rho(x) := (x, \phi(x)) \text{ for } x \in G$$

---

[44] By the calculation (1) in the proof of 3.3.5.

and σ is the projection onto the second factor. From this we see that it is sufficient to prove the claim in the following three special cases.

1. ϕ is an isomorphism.
2. ϕ is a projection (like σ).
3. ϕ is a closed subgroup.

Case 3 follows from 3.3.6 and 3.3.6 (since λ is essentially the inverse of the natural inclusion $T_eG \to T_eG'$ of the tangent spaces induced by ϕ).

The first two cases are easy and left to the reader.

QED.

3.3.9 Examples

(1) The additive group

Let $G = G_a$, so $k[G] = k[T]$. The k-derivations

$$X: k[G] \to k[G]$$

are such that for $\alpha \in k[T]$,

$$X\alpha =^{45} \frac{d\alpha}{dT} X(T) \text{ with } X(T) \in k[T]$$

hence

$$X = f \cdot \frac{d}{dT} \text{ with } f \in k[T].$$

Hence, derivations commuting with all translations $T \mapsto T+a$, $a \in k$, can be written[46]

$$X = \lambda \cdot \frac{d}{dT} \text{ with } \lambda \in k.$$

If $p = \text{char}(k) > 0$, the p-fold derivative with respect to T is zero, i.e. $D^p = 0$. Therefore,

$$\mathfrak{g} = T_eG_a = k \cdot \frac{d}{dT}$$

is the 1-dimensional (restricted) Lie-algebra with

$$[X,X] = 0 \text{ for } X \in \mathfrak{g}$$

and (in case $p>0$)

$$X^p = 0 \text{ for } X \in \mathfrak{g}.$$

(2) The multiplicative group

Let $G = G_m$, so $k[G] = k[T,T^{-1}]$. The k-derivations

---

[45] For polynomials, the chain rule is a consequence of the product rule. It is sufficient to check this for power products of the indeterminates.

[46] $X\alpha(T+a) = (X\alpha)(T+a) \Leftrightarrow f(T) \frac{d\alpha(T+a)}{dT} = F(T+a) \frac{d\alpha(T+a)}{dT}$ for all $\alpha \Leftrightarrow f(T) = f(T+\alpha)$

$$X: k[G] \to k[G]$$

are such that for $\alpha \in k[T]$,

$$X\alpha =^{47} \frac{d\alpha}{dT} X(T) \text{ with } X(T) \in k[T,T^{-1}]$$

hence

$$D = f \cdot \frac{d}{dT} \text{ with } f \in k[T,T^{-1}].$$

Hence, derivations commuting with all translations $T \mapsto aT$, $a \in k^*$, can be written[48]

$$X = \lambda \cdot T \frac{d}{dT} \text{ with } \lambda \in k^*.$$

Thus,

$$\mathfrak{g} = T_e G_m = k \cdot X, \; X := T \cdot \frac{d}{dT}$$

is the 1-dimensional (restricted) Lie algebra with

$$[X,X] = 0$$

and (in case $p>0$)

$$X^p =^{49} X.$$

(3) The general linear group

Let $G = GL_n$. Then

$$k[G] = k[T_{ij}, \det^{-1}(T) \mid i,j = 1,...,n].$$

Denote by

$$\mathfrak{gl}_n$$

the Lie-algebra of all $n \times n$-matrices over k with product

$$[X,Y] := XY - YX$$

(and the p-product in case $p>0$ just the usual p-th power). For

$$x = (x_{ij}) \in \mathfrak{gl}_n$$

let $D_x: k[G] \to k[G]$ be the k-derivation with

$$D_x T_{ij} = - \sum_{\alpha=1}^{n} T_{i\alpha} \cdot x_{\alpha j} = - (TX)_{ij}.$$

---

[47] For polynomials, the chain rule is a consequence of the product rule. It is sufficient to check this for power products of the indeterminates.

[48] $X(\alpha(aT)) = (X\alpha)(aT) \Leftrightarrow af(T) \frac{d\alpha(T)}{dT}(aT) = F(aT) \frac{d\alpha(T)}{dT}(aT)$ for all $\alpha \Leftrightarrow af(T) = f(aT)$

[49] Note that $X(T) = T$ hence $X^p(T) = T = X(T)$, i.e., X^p and X are derivations with the same value on T, hence by the product rule on the powers T^n, $n \in \mathbb{Z}$. Hence they have the same values on a generating system of the k-vector space $k[G] = k[T,T^{-1}]$

For $y = (y_{ij}) \in \mathfrak{gl}_n$ we have

$$D_x(\lambda_y(T_{ij})) = D_x((yT)_{ij}) = D_x\Big(\sum_{\beta=1}^{n} y_{i\beta} T_{\beta j}\Big)$$

$$= -\sum_{\beta=1}^{n} y_{i\beta} D_x(T_{\beta j})$$

$$= -\sum_{\beta=1}^{n} y_{i\beta} \sum_{\alpha=1}^{n} T_{\beta\alpha} \cdot x_{\alpha j}$$

$$= -(yTx)_{ij}$$

$$= -\lambda_y((Tx)_{ij})$$

$$= \lambda_y(D_x T_{ij}).$$

In other words, the derivations $D_x \circ \lambda_y$ and $\lambda_y \circ D_x$ conincide on the variables T_{ij}, henc on k[G] (by the product rule). We have proved

$$D_x \in L(G) \text{ for every } X.$$

The map

$$\mathfrak{gl}_n \to L(G),\ x \mapsto D_x,$$

is k-linear and injective. Since

$$\dim \mathfrak{g} = \dim G = n^2 = \dim \mathfrak{gl}_n.$$

the map must be bijective. Moreover, it is an isomorphism of Lie algebras, for

$$D_{[x,y]}(T_{ij}) = -(T[x,y])_{ij} = -(Txy - Tyx)_{ij} = -(Txy)_{ij} + (Tyx)_{ij}$$

$$= -D_y((Tx)_{ij}) + D_x((Ty)_{ij})$$

$$= -D_y(D_x T_{ij}) + D_x(D_y T_{ij})$$

$$= [D_x, D_y].$$

So the Lie algebra of G may be identified with

$$L(G) = \mathfrak{gl}_n.$$

Moreover, since

$$\mathrm{Int}_g : GL_n \to GL_n,\ x \mapsto gxg^{-1},$$

is linear with respect to x, its differential (=linearization at e) is

$$\mathrm{Ad}(x) : L(G) \to L(G),\ x \mapsto gxg^{-1}.$$

Also, the isomorphism $L(GL_n) \cong \mathfrak{gl}_n$ is compatible with the passage to subgroups (check this) so that, for any closed subgroup $G \subset GL_n$, the Lie algebra $\mathfrak{g}$ may be considered as a subalgebra of $\mathfrak{gl}_n$.

3.3.10 Exercises

(1) The Lie algebra of SL_n is the subalgebra $\mathfrak{sl}_n$ of $\mathfrak{gl}_n$ consisting of all matrices with trace 0 (Hint: use 3.3.7).

(2) Determine the Lie algebras of the groups $\mathbf{D}_n$, $\mathbf{T}_n$ and $\mathbf{U}_n$ of 2.1.3.

(3) Let $\phi: SL_2 \to PSL_2$ be the homomorphism of 2.1.4. Show that $d\phi$ is surjective if $p \neq 2$.

(4) If $p := \mathrm{char}(k) \neq 2$, then $L(SO_n)$ is isomorphic to the Lie group of all skew-symmetric $n \times n$-matrices.

(5) $L(G) = L(G^0)$.

(6) Show that $\mathrm{Ad}(x)$ is an automorphism of the Lie algebra $L(G)$ for every $x \in G$. If $G = GL_n$, then $\mathrm{Ad}(x)X = xXx^{-1}$ for $x \in GL_n$ and $X \in \mathfrak{gl}_n$.

Remark

Next we give some differential formulas to be used in the sequel.

3.3.11 The Lie algebra of a direct product

Let G be a linear algebraic group,

$$\pi: G \times G \to G, (x,y) \mapsto xy,$$

the product map and

$$i: G \to G, x \mapsto x^{-1},$$

the inversion (see 2.1.1). We have

$$L(G \times G) = L(G) \oplus L(G)$$

(since this is true for the tangent spaces at the neutral element, see 3.1.7(3)). The differentials of these maps can be described as follows.

$$(d\pi)_e: L(G) \times L(G) \to L(G), (X,Y) \mapsto X+Y.$$

$$(di)_e: L(G) \to L(G), X \mapsto -X.$$

Proof. The product map π defines a k-linear map

$$\tilde{\pi} := (\pi^*)^0 : \Omega_G \to \Omega_{G \times G}, f dg \mapsto \pi^*(f) d\pi^*(g),$$

(see 3.2.3) and

$$\Omega_{G \times G} = \Omega_G \otimes k[G] \oplus k[G] \otimes \Omega_G.$$

Let $f \in k[G]$ and $\pi^* f = \sum_{i=1}^{r} f_i \otimes g_i$. Then, since $(?^*)^0$ commutes with the exterior differential[50],

$$(1) \qquad \tilde{\pi}(df) = d(\pi^* f) = \sum_{i=1}^{r} (df_i \otimes g_i + f_i \otimes dg_i).$$

Since $\sum_{i=1}^{r} f_i(e) g_i = \sum_{i=1}^{r} f_i g_i(e) = f$, hence

$$\sum_{i=1}^{r} f_i(e) dg_i = \sum_{i=1}^{r} g_i(e) d f_i = df$$

we have[51]

$$\tilde{\pi}(df) - df \otimes 1 - 1 \otimes df \in M_{(e,e)} \Omega_{G \times G} .$$

Therefore, the linear map

$$\tilde{\pi}(e): \Omega_G(e) \to \Omega_{G \times G}(e,e) = \Omega_G(e) \oplus \Omega_G(e)$$

induced by $\tilde{\pi}$ is given by

$$(2) \qquad df \mapsto df \otimes 1 + 1 \otimes df \mapsto (df, df).$$

The dual of this map is

$$(d\pi)_e : T_e G \times T_e G \to T_e G$$

and from (2) we see that

$$(d\pi)_e(X,Y) = (X,Y) \circ \tilde{\pi}(e)$$

hence this vector field has on the differential $df \in \Omega_G(e) = (T_e G)^*$ the value

$$\begin{aligned} (d\pi)_e(X,Y)(df) &= (X,Y) \circ \tilde{\pi}(e)(df) \\ &= (X,Y)(df,df) \qquad \text{(see (2))} \\ &= X(df) + Y(df) \\ &= (X+Y)(df) \end{aligned}$$

Thus $(d\pi)_e$ is the map $(X,Y) \mapsto X+Y$, as claimed.

As for the second formula, note that

$$\pi \circ (id, i): G \to G, \; x \mapsto (x, x^{-1}) \mapsto e$$

is the trivial map. Therefore

$$0 = d\pi_{(e,e)} \circ (Id, di_e)$$

---

[50] The map $\tilde{\pi}$ was defined by a commutative square.

[51] Write $f_i = f_i(e)$ + something which vanishes at e and similarly for g_i and substitue these expressions in formula (1).

i.e., for $X \in T_e G$ we have

$$0 = d\pi_{(e,e)} \circ (Id, di_e)(X) = d\pi_{(e,e)}(X, di_e X) = X + di_e X.$$

QED.

3.3.12 The differential of the commutator map

Let G be a linear algebraic group.

(i) Let $\sigma: G \to G$ be a morphism of algebraic varieties and let

$$\phi: G \to G, x \mapsto \sigma(x)x^{-1},$$

Then $(d\phi)_e = (d\sigma)_e - id$.

(ii) For $x \in G$ let

$$\phi_x: G \to G, y \mapsto xyx^{-1}y^{-1},$$

be the commutator map for x. Then

$$(d\phi_x)_e = Ad(x) - id.$$

Proof. (i). Write the morphism ϕ as the following composition

$$G \xrightarrow{\Delta} G \times G \xrightarrow{\sigma \times i} G \times G \xrightarrow{\pi} G, x \mapsto (x,x) \mapsto (\sigma x, x^{-1}) \mapsto \sigma(x)x^{-1}$$

Therefore,

$$\begin{aligned}(d\phi)_e(X) &= d\pi((d\sigma \times di)(d\Delta(X))) \\ &= d\pi((d\sigma \times di)(X,X)) \\ &= d\pi((d\sigma(X), di(X)) \\ &= d\pi\,(d\sigma(X), -X) \\ &= d\sigma(X) - X.\end{aligned}$$

This proves (i).

(ii). From assertion (i) we see that

$$(d\phi_x)_e = dInt_x - id = Ad(x) - id.$$

QED.

3.3.13 The differential of direct sum and tensor product representations

Let V be a finite dimensional vector space. We write

$$\mathfrak{gl}(V)$$

for the Lie algebra of all endomorphisms of V. So

$$\mathfrak{gl}(V) \cong \mathfrak{gl}_n$$

if dim V = n. If

$$\phi: G \to GL(V)$$

is a rational representation (see 2.3.1) then its differential $d\phi$ is a homomorphism of Lie algebras

$$d\phi: \mathfrak{g} \to \mathfrak{gl}(V),$$

i.e., a representation of the Lie algebra $\mathfrak{g}$ on the vector space V.

Lemma

Let G' and G" be two linear algebraic groups and let

$$\phi': G' \to GL(V') \text{ and } \phi'': G'' \to GL(V'')$$

be rational representations. Denote by

$$\phi'\oplus\phi'': G'\times G'' \to GL(V'\oplus V'')$$

and

$$\phi'\otimes\phi'': G'\times G'' \to GL(V'\otimes V'')$$

the direct sum and tensor product representations of ϕ' and ϕ'', resp. We identify

$$L(G'\times G'') = L(G)\oplus L(G'').$$

Then

(i) $d(\phi'\oplus\phi'') = d\phi' \oplus d\phi''$,

(ii) $d(\phi'\otimes\phi'')(X',X'')(v'\otimes v'') = d\phi'(X')(v')\otimes v'' + v'\otimes d\phi''(X'')(v'')$.

Proof. (ii). It suffices to prove (ii) for $X'' = 0$. In that case we have that $d(\phi'\otimes\phi'')(X',0)(v'\otimes v'')$ is the differential of the morphism

$$G' \to V'\otimes V'', \; x \mapsto \phi'(x)v'\otimes v'',$$

evaluated at X'.[52] But the differential (=linearization) of the latter map, evaluated at X',is just

$$d\phi'(X')(v')\otimes v''.$$

(i). The proof is similar and left to the reader.

QED.

3.3.14 Exercises

(1) Let $\phi: G \to GL_n$ be a rational representation. Write

$$\phi(x) = (f_{ij}(x))$$

for $x\in G$ with $f_{ij}\in k[G]$. Then

$$d\phi(X) = (X(f_{ij}))$$

for $X\in T_eG$.

(2) Let $V\subset k[G]$ be a finite dimensional subspace of k[G] which is stable under all left translations λ_g, $x\in G$ (resp. under all ρ_g). Let

$$\phi: G \to GL(V)$$

the rational representation defined by λ (resp. ρ). Then

$$(d\phi(X))f =^{53} Xf,$$

---

[52] Since evaluation at $v'\otimes v''$ is a linear map, hence is equal to its differental, hence commutes with the formation of the differential.

[53] The differential of ϕ is a map

where $X \in L(G)$ is viewed as an element of

$$L(G) \subset \mathrm{Der}(k[G],k[G]).$$

(3) The differential of the adjoint representation is given by

$$(dAd)(X)Y = [X,Y]$$

for $X,Y \in \mathfrak{g}$.

(Hint: first deal with the case $G = GL_n$ and then use an embedding $G \subseteq GL_n$).

(4) Let $\phi: G \to GL(V)$ be a rational representation. Let $\wedge^h V$ be an exterior power of V (see [26, Ch. XVI,§6]), and let

$$\wedge^h\phi: G \to GL(\wedge^h V)$$

be the representation with

$$(\wedge^h\phi)(x)(v_1 \wedge v_2 \wedge \ldots \wedge v_h) = \phi(x)v_1 \wedge \phi(x)v_2 \wedge \ldots \wedge \phi(x)v_h$$

for $x \in G$ and $v_i \in V$. Then $\wedge^h\phi$ is a rational representation and its differential is given by

$$(d\wedge^h\phi)(X)(v_1 \wedge v_2 \wedge \ldots \wedge v_h) = \sum_{i=1}^{h} v_1 \wedge \ldots \wedge (d\phi)(X)v_i \wedge \ldots \wedge v_h$$

for $X \in \mathfrak{g}$ and $v_i \in V$.(Hint: deduce this from from the analog statements about the tensor product 3.3.13(ii)).

Remark

As an application of the differential calculus on lineare algebraic groups developed so far we shall prove now Lang's theorem about the Frobenius of algebraic groups over finite fields. We start with a few definitions concerning fields of definition.

3.3.15 Lang's theorem about algebraic groups over finite fields: preparation

Let X be an affine variety over k and let $k_0 \subseteq k$ be a subfield. A <u>k_0-structure</u> on X is a k_0-subalgebra $A_0 \subseteq A := k[G]$ of finite type over k_0 such that

---

$$d\phi: L(G) \to gl(V),$$

hence $d\phi(X)$ is an Element of gl(V) and $(d\phi(X))f$ is in V for every $f \in V$. The formula claims, in particular, that V is stable under differentiation with elements

$$X \in L(G) \subseteq \mathrm{Der}(k[G],k[G]).$$

$$A = A_0 \otimes_{k_0} k.$$

If such a structure is given we say that X is a $\underline{k_0\text{-variety}}$, or is $\underline{\text{defined}}$ over k_0, or that k_0 is a $\underline{\text{field of definition}}$ of X.

A closed subvariety $X \subseteq \mathbb{A}^n$ is defined over k_0 if and only if the ideal

$$I(X) \subseteq k[T_1,...,T_n]$$

(see 1.1.1) is generated by polynomials which are contained in

$$k_0[T_1,...,T_n]$$

(check this). This is $\underline{\text{not}}$ equivalent to the weaker property that there are $f_1,...,f_s \in k_0[T_1,...,T_n]$ such that X is the set of common zeros of the f_i $(1 \le i \le s)$ (counter example: char $k = p > 0$, k_0 a none-perfect field, $n = s = 1$, $f_1 = T^p - a$, where $a \in k_0$ but the p-th root of a is not in k_0). However, this equivalence holds if k_0 is perfect. For a discussion of these questions see e.g. [3, AG, §12]. We do not need to go into details.

If X and Y are affine k_0-varieties, defined by k_0-algebras A_0 and B_0, a morphism

$$\phi: X \to Y$$

is a $\underline{k_0\text{-morphism}}$ or is $\underline{\text{defined}}$ over k_0, If there is a homomorphism of k_0-algebras

$$\phi_0^*: B_0 \to A_0,$$

such that the homomorphism $\phi^*: k[Y] \to k[X]$ defining ϕ is $\phi_0^* \otimes \mathrm{id}$. It is now clear how to define a k_0-structure on a linear algebraic group G. In that case we say that G is a k_0-group or is defined over k_0.

Now let $k_0 := \mathbb{F}_q$ be the finite field with q elements, and let k be an algebraic closure of $\mathbb{F}_q$. If X is an affine variety defined over k_0, and A, A_0 are as before, the homomorphism

$$A_0 \to A_0, f \mapsto f^q,$$

defines a morphism

$$F: X \to X$$

which is defined over $\mathbb{F}_q$. This is the Frobenius morphism.

If $\phi: X \to \mathbb{A}^n$ is an $\mathbb{F}_q$-embedding of X into affine n-space, so that we can view X as a subset of k^n, we have

$$F(x_1,...,x_n) = (x_1^q,...,x_n^q)$$

if $(x_1,...,x_n) \in X$. It is clear from the definition of F that the tangent map $(dF)_x$ is trivial for every $x \in X$.

3.3.16 Lang's theorem

Let G be a connected linear algebraic group which is defined over $\mathbb{F}_q$ and let F be the corresponding Frobenius morphism. Then

$$\phi: G \to G,\ x \mapsto (Fx)x^{-1},$$

is a surjective morphism.

Proof. Step 1. $F: G \to G$ is a homomorphism of algebraic groups.
By assumption, G is defined over $\mathbb{F}_q$. In particular, the multiplication

$$\pi: G \times G \to G,\ (x,y) \mapsto (f_1(x,y),\ ...,\ f_n(x,y))$$

is defined, with respect to some embeding $G \subseteq \mathbb{A}^n$, by polynomial functions f_i with coefficients in $\mathbb{F}_q$. Therefore, $f_i(Fx,Fy) = f_i(x,y)^q$, hence

$$F(x \cdot y) = F(x)F(y),$$

i.e., F is a homomorphism of algebraic groups.
Step 2. $\phi(G)$ contains a none-empty open subset $U \subseteq G$.
By 3.3.12(i)

$$(d\phi)_e = (dF)_e - id = -id,$$

i.e.,

$$(d\phi)_e: T_eG \to T_eG$$

is bijektive. Since

$$\phi(x) = (Fx)x^{-1} = (Fa)\cdot (F(a^{-1}x)(a^{-1}x)^{-1}a^{-1}$$
$$= (Fa)\cdot\phi(a^{-1}x)a^{-1},$$

the differential

$$(d\phi)_a: T_aG \to T_aG$$

is bijective for arbitrary $a \in G$. Now let

$$X := \overline{\phi G}$$

be the Zariski closure of the image of ϕ. This is an irreducible closed subset of G. The none-singular points of X form a none-empty open

subset of X (see 3.2.17(ii)). In particular, there is a singular point in X of the form

$$\phi(a) \in X,\ a \in G.$$

Therefore, if we consider ϕ as a morphism $\phi: G \to X$,

$$\dim X = \dim T_a X \geq \dim \mathrm{Im}(d\phi)_a \geq \dim T_a G \geq \dim G,$$

hence

$$X = G.$$

By 1.9.5, the Image of ϕ contains a none-empty open subset of G,

$$\emptyset \neq U \subseteq \phi(G),\ U \subseteq G \text{ open.}$$

Step 3. For every $a \in G$ there is a none-empty open subset V of G,

consisting of Elements of the form $(Fy)ay^{-1}$.

Write

$$\sigma_a(x) := F(x)a = \rho_a(F(x))$$

$$\phi_a(x) := \sigma_a(x)x^{-1}.$$

Then by 3.3.12(i),

$$(d\phi_a)_e = (d\sigma_a)_e - \mathrm{id} = (\rho_a)\circ(dF)_e - \mathrm{id} = \mathrm{id}.$$

Inparticular $(d\phi_a)_e$ is bijective. Moreover,

$$\phi_a(x) = (Fx)ax^{-1} = (Fb)\cdot (F(b^{-1}x)a(b^{-1}x)^{-1}b^{-1}$$

$$= (Fb)\cdot\phi_a(b^{-1}x)b^{-1},$$

Therefore, $(d\phi_a)_b$ is bijecitive for every $b \in G$. The claim now follows by the same arguments as in step 2.

Step 4. The proof.

Given any $a \in G$ choose the none-empty open subsets $U,V \subseteq G$ as in Step 2 and 3. As G is connected, these sets have a none-empty intersection, i.e., there are points $x,y \in G$ such that

$$(Fx)x^{-1} = (Fy)ay^{-1}.$$

But then

$$a = (Fy)^{-1}(Fx)x^{-1}y = F(y^{-1}x)(y^{-1}x)^{-1} = \phi(y^{-1}x),$$

i.e., ϕ is surjective.

QED.

Remark

Let G as in the theorem. Then the fixed point set of F,

$$G^F := \{ x \in G \mid Fx = x \}$$

is a finite group. All “finite Chevalley groups” are of this type. Lang’s theorem is the basic tool in the study of these groups. We give an instance of an application in the next exercises below.

3.3.17 Exercises

(1) Let G and G^F be as before. Let $x \in G^F$. Then the centralizer $Z_G(x)$ of x is a closed subgroup of G (see 2.5), which is F-stable. Assume that $Z_G(x)$ is connected. If $y \in G^F$ is conjugate to x in G, then is is alread conjugate to x in the finite group G^F (for more details see [6, part E, Ch. I]).

(2) Let G be a connected linear algebraic group and $\sigma; G \to G$ an endomorphism of algebraic groups such that $d\sigma: \mathfrak{g} \to \mathfrak{g}$ is a nilpotent linear map. Then $G \to G$, $x \mapsto (\sigma x)x^{-1}$, is surjective.

3.4. Jordan decomposition in L(G)

Let G be a linear algebraic group, with Lie algebra $\mathfrak{g}$. We view the elements of $\mathfrak{g}$ as derivations of k[G]. There is a Jordan decomposition of elements of $\mathfrak{g}$, quite similar to the one in G (2.4.8), which will be briefly discussed.

3.4.1 Existence of the Jordan decomposition

Let F be a finite dimensional subspace of k[G]. There is a finite dimensional subspace E of k[G] which contains F and is stable under all derivations $X \in Lie(G)$. In other words, the action of Lie(G) on k[G] is locally finite. In particular, there is an additive Jordan decomposition $X = X_s + X_n$ for left invariant vector fields X on G.

Proof. We may assume that F is generated by one single element $f \in k[G]$. Write

$$f(xy) = \sum_{i=1}^{n} f_i(x)g_i(y).$$

Then

$$\lambda_x \circ f = \sum_{i=1}^{n} f_i(x)g_i,$$

hence for $D \in Lie(G)$,

$$D(\lambda_x \circ f) = \sum_{i=1}^{n} f_i(x)D(g_i),$$

Since D is supposed to be invariant under left translation,

$$\lambda_x \circ D(f) = \sum_{i=1}^{n} f_i(x)D(g_i),$$

Evaluating at y=e we get

$$D(f)(x) = \sum_{i=1}^{n} f_i(x)D(g_i)(e),$$

This last identity shows that D(f) is contained in the k-vector space generated by $f_1,..,f_n$, i.e., the vector space generated by the functions D(f) where D runs over the invariant vector fields, is finite dimensional.
QED.

3.4.2 Properties of the Jordan decomposition

Let $X \in Lie(G)$ and let $X = X_s+X_n$ be the Jordan decomposition of X. Then
(i) $X_s, X_n \in Lie(G)$ and $[X_s,X_n] = 0$.
(ii) If $\phi:G\to G'$ is a homomorphism of linear algebraic groups then $d\phi$ commutes with the Jordan decomposition in Lie(G): $((d\phi)X)_s = (d\phi)X_s$ and $((d\phi)X)_n = (d\phi)X_n$
(iii) If $G=\mathbf{GL}_n$ then X_s and X_n are the semi-simple and nilpotent parts of the matrix $X\in\mathbf{gl}_n$.

3.4.3 Exercises

(1) Prove 3.4.2 (Hint: the proof is similar to the proof for the multiplicative Jordan decomposition in G (see 2.4.8)).
(2) If G is a torus, then all $X\in L(G)$ are semi-simple.
(3) If G is unipotent, then all $X\in L(G)$ are nilpotent.

3.4.4 Note about the methods used in this book

4. Further study of morphisms, applications

4.1. General properties of morphisms of varieties

4.1.1 The situation, notation

Let X and Y be two irreducible varieties and

$$\phi: X \to Y$$

a dominant morphism (see 3.2.19). We may view the quotient field k(X) (see 1.8.1) as an extension of the field k(Y). The transcendence degree of the extension is

$$\mathrm{trdeg}_{k(X)}k(X) = \dim X - \dim Y.$$

We shall give in 4.16 (ii) a geometric interpretation of this integer.

If F is any field and E a finite algebraic extension, the elements of E which are separable over F form a subfield

$$E_s := \{ x \in E \mid x \text{ separable over } F\}$$

Its degree is called the separable degree of E over F and denoted

$$[E:F]_s := [E_s:F].$$

For any $x \in E$ there is a power x^{p^e} which is in E_s, where $p := \text{char}(F)$ (see 26, Ch.VII, §4).

If X and Y are as before and dim X = dim Y, then k(X) is a finite algebraic extension of k(Y). In 4.1.6(iii) a geometric interpretation is given of $[k(X):k(Y)]_s$.

If k(X) = k(Y) then ϕ is said to be birational.

4.1.2 Criterion for birational morphisms

Let $\phi: X \to Y$ be a dominant morphism of irreducible varieties. The the following are equivalent.

(i) ϕ is birational.

(ii) There is a none-empty open subset $U \subseteq X$ such that $\phi(U) \subseteq Y$ is open and such that ϕ induces an isomorphism $U \to V$.

Proof.

QED.

4.1.3 Lemma: the purely transcentental case

Let $\phi: X \to Y$ be a dominant morphism of affine irreducible varieties such that

$$k[X] = k[Y][a],$$

where a is trancendental over k(Y). Then

(i) ϕ is an open morphism.

(ii) If $Y' \subseteq Y$ is an irreducible closed subvariety, then $\phi^{-1}(Y') \subseteq X$ is an irreducible close subvariety of dimension

$$\dim \phi^{-1}(Y') = \dim Y' + 1.$$

Proof.

QED.

4.1.4 Lemma: the separable algebraic case

Let $\phi: X \to Y$ be a dominant morphism of affine irreducible varieties such that

$$k[X] = k[Y][a],$$

where a is separably algebraic over k(Y). Then there is a none-empty open subset
$U \subseteq X$
with the following properties.
(i) The restriction of ϕ to U is an open morphism $U \to Y$.
(ii) If $Y' \subseteq Y$ is an irreducible closed subset and $X' \subseteq X$ an irreducible component of $\phi^{-1}(Y')$ such that $X' \cap U \neq \emptyset$, then dim X' = dim Y'.
(iii) For $x \in U$,

$$\#\phi^{-1}(\phi(x)) = [k(X):k(Y)].$$

Proof.

QED.

4.1.4 Lemma: the purely inseparable case

Let $\phi: X \to Y$ be a dominant morphism of affine irreducible varieties such that

$$k[X] = k[Y][a],$$

where $a^p \in k(Y)$. Then there is a none-empty open subset $U \subseteq X$ with the following properties.
(i) ϕ induces an open morphism $U \to Y$ which is a homeomorphism onto its image.
(ii) If $Y' \subseteq Y$ is an irreducible closed subset, then there is at most one irreducible component X' of $\phi^{-1}(Y')$ such that $X' \cap U \neq \emptyset$. If X' exists, then dim X' = dim Y'.

Proof.

QED.

4.1.6 Theorem

Let $\phi: X \to Y$ be a dominant morphism of irreducible varieties of relative dimension

$$r := \dim X - \dim Y.$$

Then there is a none-empty open subset $U \subseteq X$ with the following properties.
(i) ϕ induces an open morphism $U \to Y$.
(ii) If $Y' \subseteq Y$ is an irreducible closed subvariety and X' an irreducible component of $\phi^{-1}(Y')$ such that $X' \cap U \neq \emptyset$, then

$$\dim X' = \dim Y' + r.$$

In particular, if $y \in Y$, any irreducible component of $\phi^{-1}(y)$ which intersects U has dimension r.

(iii) If k(X) is algebraic over k(Y) then for all $x \in U$ the number of points in the fiber $\phi^{-1}(\phi(x))$ equals $[k(X):k(Y)]_s$,

Proof.
QED.

4.1.7 Corollary

In the situation of 4.1.6 we may replace assetion (i) by the stronger property

(i)' For any variety Z, the restriction of ϕ to U defines an open morphism $U \times Z \to Y \times Z$.

Proof.
QED.

4.1.8 Exercises

(1) Show, using 4.1.6(iii), that an isomorphism $\phi: \mathbb{A}^1 \to \mathbb{A}^1$ is of the form $\phi(t) = at+b$ $(a,b \in k,\ a \neq 0)$. Deduce that an isomorphism ψ of the projective line $\mathbb{P}^1$ (see 1.7.1) is of the form

$$\psi(x,y) = (ax+by, cx+dy) \text{ with } \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0.$$

(2) Let $X := \{(x,y) \in \mathbb{A}^2 \mid x^3 = y^2\}$. This is an irreducible closed subset of dimension 1. Define $\phi: X \to \mathbb{A}^1$ by $\phi(x,y) := y/x$ if (x,y) is not the origin and $\phi(0,0) = 0$. Show that ψ is a morphism of varieties which is birational and bijective, but is not an isomorphism of varieties.

(3) Consider the morphism $\phi: \mathbb{A}^2 \to \mathbb{A}^2$, (x,y) a (x,xy). Show that ϕ is birational, and that it is not an open morphism. Determine the components of its fibers.

(4) Consider the morphism $\phi: \mathbb{A}^3 \to \mathbb{A}^3$, (x,y,z) a (x,xy,z). Let

$$X := \{(x,y,z) \in \mathbb{A}^3 \mid y^2 = x+1\}.$$

Show that X and $Y = \phi Y$ are irreducible closed subvarieties of $\mathbb{A}^3$ of dimension 2. Let

$$Y' := \{(x,y,z) \in \mathbb{A}^3 \mid y = xz,\ z^2 = x+1\}.$$

Show that Y' is irreducible, close, of dimension 1 and that if char $k \neq 2$, $\phi^{-1}Y' \cap X$ has a component of dimension 0.

4.2. Finite morphisms

4.2.1 Definition

Let B be a ring and $A \subseteq B$ a subring. We say that B is <u>finite</u> over A if B is an A-module of finite type. We say that $b \in B$ is <u>integral</u> over A if it satisfies an equation

$$b^n + a_1 b^{n-1} + ... + a_n = 0 \ , \ a_i \in A \ .$$

If every $b \in B$ is integral over A then B is said to be integral over A.

4.2.2 Lemma: finiteness and integralness

Let B be an A-algebra of finite type. Then B is integral over A if and only if B is finite over A.

Proof.

QED.

Remarks

(i) The lemma implies that the elements $b \in B$ which are integral over A form a subring called the integral closure of A in in B.

(ii) If the ring C in integral over B and B is integral over A, then C is integral over A.

(iii) A dominant morphism $\phi: X \to Y$ of affine irreducible varieties is called finite if k[X] is finite over k[Y].

4.2.3 Proposition: surjectivity and closedness of finite morphisms

Any finite morphism is surjective and closed.

Proof.

QED.

4.2.4 Proposition: finiteness and quasi-finiteness

Let $\phi: X \to Y$ be a dominant morphism of irreducible affine varieties and

$$x \in X$$

any point such that its fiber

$$\phi^{-1}(\phi(x)) \text{ is finite.}$$

Then there is an affine open neighborhood $V \subseteq Y$ of $\phi(x)$ such that

$$\phi^{-1}(V) \subseteq X$$

is an affine open neighborhood of x and such that the morphism

$$\phi^{-1}(V) \to V$$

induced by ϕ is finite.

Proof.

QED.

4.2.5 Corollary: preservation of dimension

Let $\phi: X \to Y$ be a dominant morphism of irreducible affine varieties such that for at least one point $x \in X$ the fiber

$$\phi^{-1}(\phi(x)) \text{ is finite.}$$

Then dim X = dim Y.

Proof.

QED.

4.2.6 Exercises

(1) Let $\phi : X \to Y$ be a finite morphism. Then, for any variety Z, the induced morphism

$$\phi \times id: X \times Z \to Y \times Z$$

is closed.

(2) Let $\phi: X \to Y$ be a surjective morphism of irreducible affine varieties. Assume that $\phi^{-1}(\phi(x))$ is finite for all $x \in X$. Then ϕ is finite (Hint: Take $f \in k[X]$ and put $I := \{g \in k[Y] \mid gf \text{ is integral over } k[Y]\}$, show that $I=k[Y]$).

(3) An integral domain A is said to be <u>normal</u> if every element of its quotient field which is integral over A, lies already in A. An irreducible affine variety X is <u>normal</u>, if k[X] is normal.
Let $\phi: X \to Y$ be a morphism of irreducible affine varieties which is bijective and birational. Assume Y to be normal. Show that ϕ is an isomorphism (This is a version of "Zariski's main theorem". Hint: use Exercise (2)).

4.3. Applications to algebraic groups

4.3.1 Lemma: closed and locally closed orbits

Let G be a connected algebraic group acting on the G-space X.

(i) An orbit of G in X is open in its closure. Each orbit and its Zariski closure are irreducible varieties.

(ii) There exist closed orbits. All orbits of minimal dimension are closed.

Proof. <u>(i)</u>. Let $x \in X$ and write $\mathcal{O} := G \cdot x$ for its orbit. Consider the morphism

$$G \to X, g \mapsto gx.$$

The closure of its image contains a none-empty open subset U which is completely in its image

$$U \subseteq \mathcal{O},$$

(see 1.9.5). Since G acts transitively on $\mathcal{O}$, the open sets gU cover $\mathcal{O}$. This proves (i) the first claim of (i). Moreover, we see that $\mathcal{O}$ is an open subvariety of $\overline{\mathcal{O}}$. Since G is irreducible, the same is true for $\mathcal{O}$ and $\overline{\mathcal{O}}$. This proves (i).

<u>(ii)</u>. Take $\mathcal{O}$ such that dim $\mathcal{O}$ is minimal. If $\mathcal{O}$ were not closed, the difference

$$\overline{\mathcal{O}} - \mathcal{O}$$

would contain an orbit of dimension less than dim $\overline{\mathcal{O}}$ = dim $\mathcal{O}$, which contraticts the choise of $\mathcal{O}$.

QED.

4.3.2 Lemma: G-obits and G^0-orbits

Let G be an algebraic group and X a homogeneous space for G. Then:

(i) Each irreducible component of X is a homogeneous space for G^0.

(ii) The components of X are open and closed, and X is their disjoint union.

Proof. Let $X' \subseteq X$ be an orbit of G^0. Since G acts transitively on X and G^0 has finite index in G (by 2.2.1(i)),

$$G = g_1G^0 \cup \ldots \cup g_rG^0,$$

$$X = GX' = g_1G^0X' \cup \ldots \cup g_rG^0X' = g_1X' \cup \ldots \cup g_rX',$$

i.e., X is the disjoint union of finitely many translates gX', $g \in G$, Each of them is a G^0-orbit.[54] From 4.3.1(ii) follows that one of them is closed, hence all of them are closed. This proves the claim.
QED.

4.3.3 Theorem: Dimension of the fibres for morphisms of homogeneous spaces

Let G be an algebraic group and $\phi: X \to Y$ and equivariant morphism of homogeneous spaces for G. Define

$$r := \dim X - \dim Y.$$

Then

(i) For any variety Z, the induced morphism $\phi \times id: X \times Z \to Y \times Z$ is open.

(ii) If Y' is an irreducible closed subvariety of Y and X' an irreducible component of $\phi^{-1}Y'$, then $\dim X' = \dim Y' + r$. In particular, for every point $y \in Y$, the irreducible components of $\phi^{-1}y$ all have dimension r.

(iii) Equivalent conditions:

(a) ϕ is an isomorphism.

(b) ϕ is bijective and the map induced on the tangent spaces, $(d\phi)_x: T_xX \to T_{\phi x}Y$ is bijective for some $x \in X$.

Proof. Using the previous lemma (4.3.2) the proof of the theorem is easily reduced to the case that G is connected and X,Y are irreducible. Then ϕ is surjective, hence dominant, and we can apply the theorem on the dimension of the fibers (4.1.6 and 4.1.7). Let $U \subseteq X$ be an open subset with the properties as in this theorem. Since the morphism is equivariant, all translates $g \cdot U$ also enjoy these properties, hence does

---

[54] For, G^0 is an invariant subgroup, $g_iG^0 = G^0g_i$ for every i.

the union of all these translates. Since the union equals X, assertions (i) and (ii) follow.

As for assertion (iii), assume that ϕ is bijective. Then the field extension $k(X)/k(Y)$ is purely inseparable (4.1.6)(iii). If $(d\phi)_x$ is bijective too, we see that this extension also is separable. Hence $k(X)=k(Y)$ and ϕ is birational, hence induces an isomorphism on certain open subsets of X and Y (4.1.2). Since ϕ is equivariant, this implies that it is an isomorphism. This proves (b)$\Rightarrow$ (a). The converse implication is trivial.

QED.

4.3.4 Corollary: Criterion for isomorphisms of linear algebraic groups

Let $\phi: G \to G'$ be a surjective homomorphism of algebraic groups. Then

(i) $\dim G = \dim G' + \dim \mathrm{Ker}(\phi)$.

(ii) Equivalent assertions:

(a) ϕ is an isomophism.

(b) ϕ is an isomophism of abstract groups and the induced Lie algebra homomorphism $d\phi: L(G) \to L(G')$ is an isomorphism.

Proof. Consider G and G' as homogeneous spaces for G: the first one via left translations (2.3.1) and second one via ϕ and left translations on G'. Then ϕ is an equivariant morphism and the assertions follow from 4.3.3.

QED.

4.3.5 Exercises

(1) The connectedness assumption of in 4.3.1 can be ommitted (except for the irreducibility assertions).

(2) In the situation of 4.3.1, an orbit is a homogeneous space (this fact was already stated in 2.3.1).

(3) Let G be a unipotent linear algebraic group and X an affine G-space. Denote by O a G-orbit in X and let $\bar{O}$ be its closure. Assume that $\bar{O} \neq O$. Then the difference

$$O' := \bar{O} - O$$

is closed (by 4.3.1 and (1)). Let I and I' be the ideals in k[X] of functions vanishing on $\bar{O}$ and $\bar{O} - O$ respectively. Then $I \subseteq I'$, $I \neq I'$, and $I' \neq k[X]$. Deduce from the fact that unipotent groups can be embedded into some $\mathbf{U}_n$ (see, 2.4.11) that there exists some $f \in I' - I$ such that $f(g \cdot x) = f(x)$ for $g \in G$ and $x \in X$, and show that this leads to

a contradiction. Hence all orbits of G in X are closed ("theorem of Konstant-Rosenlicht").[55]

(4) Give an example of a bijective homomorphism of algebraic groups $G \to G'$ which is not an isomorphism of algebraic groups.[56]

(5) If char k = 0, a homorphism of algebraic groups $\phi: G \to G'$ is an isomophisms of algebraic groups if and only if it is an isomorphism of abstract groups. Similarly for homogeneous spaces.

(6) (a) Let $\sigma: G \to G'$ be a homorphism of algebraic groups. Then

$$\dim \mathrm{Ker}(\sigma) + \dim \mathrm{Im}(\sigma) = \dim G.$$

(b) Assume moreover that G is connected, $G' \cong G$, and σ is surjective. Then $\mathrm{Ker}(\sigma)$ is a finite subgroup of the center of G (Hint for the proof of the last statement: let $g \in \mathrm{Ker}(\sigma)$ and consider the morphism $G \to \mathrm{Ker}(\sigma)$, $x \mapsto xgx^{-1}g^{-1}$).

4.4. Semi-simple automorphisms

4.4.1 Notation, the Lie algebra of the fixed point group of an automorphism of algebraic groups

Let G be a connected linear algebraic group and

$$\sigma: G \to G$$

an automorphism of G in the sense of algebraic groups. We write

$$G_\sigma := \{ x \in G \mid \sigma x = x \}$$

for the set of fixed points of σ.This is a closed subgroup.[57] Also,

$$\phi: G \to G, \; x \mapsto (\sigma x)x^{-1},$$

is a morphism of varieties. The induced map on the tangent spaces,

$$d\sigma : L(G) \to L(G),$$

is an automorphism of the Lie algebra $\mathfrak{g} := L(G)$. We write

(1) $$\mathfrak{g}_\sigma := \{X \in \mathfrak{g} \mid (d\sigma)X = X \} =^{58} \mathrm{Ker}(d\phi)_e.$$

Since $\phi G_\sigma = \{e\}$, we have $(d\phi)_e \mathrm{Lie}(G_\sigma) = \{0\}$ hence

(2) $$\mathrm{Lie}(G_\sigma) \subseteq \mathfrak{g}_\sigma = \mathrm{Ker}(d\phi)_e .$$

---

[55] The operation of G on I'/I is locally finite: for any $f \in I'/I$ the k-linear subspace $V \subseteq I'$ generated by all gf, $g \in G$, is finite dimensional. The operation of G on V is by unipotent matrices, hence there is an invariant subspace where G operates trivially. Take a representative in I' of a generator of this subspace and repeate the above argument.

[56] Take an algebraic group defined over some $\mathbb{F}_q$ and its Frobenius morphism.

[57] For, it the fiber over e of $G \to G$, $x \mapsto (sx)x^{-1}$.

[58] By 3.3.12(i) $(d\phi)_e = (d\sigma)_e$ - Id.

Equality need not hold (see Exercise 4.4.9(1) below). From Lemma 4.4.2 will follow that equality holds if char(k) = 0.

In general this question is related to the dominant morphism

$$\psi: G \to \overline{\phi G}, x \mapsto \phi x,$$

considered as an equivariant morphism of G-spaces, where G acts onto itself by left translations and on $\overline{\phi G}$ as follows.

$$G \times \overline{\phi G} \to \overline{\phi G}, (g,x) \mapsto (\sigma g)xg^{-1}.$$

Note that ϕG is an orbit of G under the action just defined. By 4.3.1(i) ϕG is open in its closure $\overline{\phi G}$, i.e. it is a variety with a transitive action of G, i.e. a homogeneous space. By 3.2.21 (i) ϕG is smooth. In particular, $e \in \overline{\phi G}$ is a non-singular point.

Moreover[59],

$$\dim \overline{\phi G} = \dim G - \dim G_\sigma.$$

4.4.2 Lemma: Criterion for equality in $L(G_\sigma) \subseteq L(G)_\sigma$

Let G be a connected linear algebraic group and

$$\sigma: G \to G$$

an automorphism of G in the sense of algebraic groups. Then the following are equivalent.

(i) $\mathrm{Lie}(G_\sigma) = \mathfrak{g}_\sigma$

(ii) $\psi: G \to \overline{\phi G}, x \mapsto (\sigma x)x^{-1}$, is separable.

Proof. Using the notations of 4.4.1 we get

$$\begin{aligned}
\dim \mathrm{Im}(d\psi)_e &= \dim L(G) - \dim \mathrm{Ker}(d\phi)_e && \text{(homomorphism theorem)}\\
&= \dim L(G) - \dim \mathfrak{g}_\sigma && \text{(by 4.4.1(1))}\\
&\geq \dim L(G) - \dim L(G_\sigma) && \text{(by 4.4.1(2))}\\
&= \dim G - \dim G_\sigma\\
&= \dim \phi G && \text{(by 4.3.3(ii))}^{60}\\
&= \dim \overline{\phi G} && (\phi G \subseteq \overline{\phi G} \text{ is open})
\end{aligned}$$

---

[59] By the formula for the dimension of a fiber for an equivariant morphism of homogeneous space (4.3.3(ii)),

$$\dim G_\sigma = \dim G - \dim \phi G = \dim G - \dim \overline{\phi G}.$$

[60] Theorem about the dimension of the fiber of equivariant maps of homogeneous spaces.

If condition (i) is satisfied, then equality holds everywhere in the above estimation. In particular, $(d\psi)_e$: $L(G) \to L(\overline{\phi}\overline{G})$ is surjective. By 3.2.21(ii) this implies that ψ is separable.

Conversely, if condition (ii) is satisfied, the outer members of the above estimation are equal (by 3.2.21(ii))[61]. The equality holds everywhere in the estimation. In particular, condtion (i) is satisfied. **QED**.

Definition: semi-simple automorphisms

Let G be a connected linear algebraic group and

$$\sigma: G \to G$$

an automorphism of G in the sense of algebraic groups. Then σ is called semi-simple if the action of σ on k[G] is semi-simple in the sense of 2.4.7.[62]

4.4.3 Lemma: Criterion for semi-simplicity of an automorphism

Let G be a connected linear algebraic group and

$$\sigma: G \to G$$

an automorphism of G in the sense of algebraic groups. Then the following are equivalent.

(i) σ is semi-simple.

(ii) There is an isomorphism $\tau: G \to GL_n$ onto a closed subgroup of some GL_n and a semi-simple element $s \in GL_n$ such that

$$\tau(\sigma x) = s\tau(x)s^{-1} \text{ for all } x \in G.$$

In other words, semi-simple automorphisms are essentially the same as conjugation with semi-simple elements.

Proof. Choose a finite dimensional k-linear subspace $V \subseteq k[G]$ containing a set of generators of the k-algebra k[G]. By 2.3.4(i) we may assume that V is invariant under left transformations with respect to element of G. Then

$$\tau: G \to GL(V), g \mapsto \lambda_g,$$

is a closed embedding of linear algebraic groups (see proof of 2.3.5). Since the operation of σ^* on k[G] is locally finite,

$$V \subseteq W$$

for some finite dimensional σ^*-stable k-linear subspace $W \subseteq k[G]$. In particular

---

[61] For morphisms of homogeneous spaces separability is equivalent to the surjectivity of one (of all) differential(s).

[62] i.e., σ induces a locally finite action on the coordinate ring such that the unipotent part of this action is trivial.

(1) $$\sum_{n=0}^{\infty} \sigma^{*n}(V)$$

is a finite-dimensional k-linear subspace of k[G]. For x,y∈G von f∈V one has

$$\begin{aligned}\lambda_x(\sigma^{*n}(f))(y) &= \sigma^{*n}(f))(xy)\\ &= f(\sigma^n(xy))\\ &= f(\sigma^n(x)\sigma^n(y))\\ &= (\lambda_{\sigma^n(x)}f)(\sigma^n(y))\\ &= \sigma^{*n}(\lambda_{\sigma^n(x)}f)(y)\end{aligned}$$

hence

$$\lambda_x(\sigma^{*n}(f)) = \sigma^{*n}(\lambda_{\sigma^n(x)}f)$$

for f∈V and x∈G. Since V is invariant under left translation, $\lambda_{\sigma^n(x)}$ f∈V, i.e., the right hand side of the above expression is in (1). We have prove, (1) is stable under both, left translations and the operation of σ*. Therefore, we may assume that the vector space V defining the closed embedding τ is σ*-stable.

Let s∈GL(V) be the restriction of σ* to V,

$$s := (\sigma^*|_V)^{-1}.$$

Since the action $\sigma^*|_V$ is semi-simple, the same is true for the inverse action s. Moreover, for x,y∈G, f∈V, we have

$$\begin{aligned}(\tau(\sigma(x))(f))(y) &= (\lambda_{\sigma(x)}f)(y)\\ &= f(\sigma(x)y)\\ &= f(\sigma(x\cdot\sigma^{-1}(y))\\ &= (\sigma^*f)(x\cdot\sigma^{-1}(y))\\ &= \lambda_x(\sigma^*f)(\sigma^{-1}(y))\\ &= (\sigma^{-1})^*(\lambda_x(\sigma^*f))(y)\end{aligned}$$

hence

$$\tau(\sigma(x))(f) = (\sigma^{-1})^*(\lambda_x(\sigma^*f)) = (\sigma^{-1})^*((\tau(x))(\sigma^*f))$$

hence

$$\tau(\sigma(x)) = (\sigma^{-1})^* \circ \tau(x) \circ \sigma^* = s\tau(x)s^{-1}.$$

Therefore, τ and s are as claimed in (ii).

Conversely, if τ and s are as in (ii), then conjugation by s is a semi-simple operation on k[GL(V)].[63] The induced operation on the factor space k[G] of k[GL(V)] is semi-simple, since Jordan decomposition is compatible with passage to factor spaces.
QED.

4.4.4 Theorem: properties of semi-simple automorphisms
Let G be a connected linear algebraic group and

$$\sigma: G \to G$$

a semi-simple automorphism of G. Define

$$\phi(x) := (\sigma x)x^{-1}.$$

Then:
(i) The subset $\phi G \subseteq G$ is closed and the induced morphism $\psi: G \to \phi G$ is separable.
(ii) $Lie(G_\sigma) = Lie(G)_\sigma$.

Proof. By 4.4.3 we may assume that G is a closed subgroup of GL_n and that there is a semi-simple $s \in GL_n$ such that

$$\sigma x = sxs^{-1} \text{ for every } x \in G.$$

Step 1. Separability of ψ.
Step 1.1. The case $G = GL_n$
If $G = GL_n$ write s as a diagonal matrix

$$s = diag(a_1,\ldots,a_1,a_2,\ldots,a_2,\ldots,a_r,\ldots,a_r)$$

with pairwise different eigenvalues a_i . Then

$$G_\sigma$$

consists of the n×n-matrices commuting with s, i.e.,

$$G_\sigma = GL_{n_1} \times GL_{n_2} \times \ldots \times GL_{n_r}$$

where n_i denotes the multiplicity of a_i. For the Lie-algebra we get

$$L(G_\sigma) = gl_{n_1} \oplus gl_{n_2} \oplus \ldots \oplus gl_{n_r}$$

The operation of σ on L(G) is by conjugation with s. Therefore $L(G)_\sigma$ consists of the n×n-matrices commuting with s, i.e.,

$$L(G)_\sigma = L(G_\sigma).$$

By 4.4.2, ψ is separable.

---

[63] In a suitable Koordinate system, conjugation with s multiplies the i-th row with the i-th eigenvalue and divides the j-th column by the j-th eigenvalue.

Step 1.2. The case G arbitrary.
Extend σ to an automorphism of GL_n acting via conjugation with s,

$$\sigma: GL_n \to GL_n, x \mapsto sxs^{-1}$$

Also, extend ϕ to a morphism

$$\phi: GL_n \to GL_n, x \mapsto sxs^{-1}x^{-1}.$$

Let $X \in T_e\overline{\phi G}$. Since $T_e\overline{\phi G} \subseteq T_e\overline{\phi G L_n}$ and we have already dealt with the case of GL_n, it follows that there is some $Y \in L(GL_n)$ with

$$(d\phi)_e Y = X.$$

By 3.3.12 (i) the left hand side of this identity is $(d\sigma - 1)Y$, i.e.

$$X = (d\sigma - 1)Y.$$

Since, by assumption, σ is semi-simple, the same is true for $d\sigma$, i.e.,

$$d\sigma: gl_n \to gl_n$$

is a semi-simple automorphism stabilizing the subspace $L(G) \subseteq gl_n$.[64] We may write gl_n as a direct sum of $d\sigma$ -stable subspaces,

$$gl_n = L(G) \oplus \xi'.$$[65]

Since X is in the first direct summand and $d\phi = d\sigma - Id$ respects the direct sum decomposition, we may assume,

$$Y \in L(G).$$[66]

We have proved, $(d\phi)_e: L(G) \to T_e\overline{\phi G}$ is surjective. Hence ψ is separable (see 3.2.21(ii)). But then assertion (ii) is true (see 4.4.2).
Step 2. ϕG is closed in G.

Let m(T) denote the minimum polynomial of s^{-1} over k,

$$m(T) =^{67} \prod_{i=1}^{r} (T - a_i^{-1}).$$

---

[64] Both, σ and $d\sigma$ are conjugation by the semi-simple matrix s.
[65] Extend an eigenbasis of L(G) to an eigenbasis of gl_n.
[66] Replace the second component by zero.
[67] In the original one considers the minimum polynomial of s instead. Note that, on the i-th eigenspace, s is multiplication by the i-th eigenvalue a_i^{-1}, hence the difference $s^{-1} - a_i^{-1} \cdot Id$ is zero on this eigenspace. But then m(s) = 0 everywhere. On the other hand, s^{-1} is multiplication by a_i^{-1} in the i-th eigenspace of s, i.e.

Consider the set

$$X \subseteq GL_n$$

of elements $x \in GL_n$ satisfying the following three conditions.

(a) x normalizes G,i.e., $xGx^{-1} \subseteq G$.
(b) $m(x) = 0$
(c) the charactistic polynomial of $Ad(x)|_{L(G)}$ equals that of $d\sigma$.

Then X is a closed subset[68] of GL_n containing s^{-1}. Since m(T) has no multiple roots, all elements of X are semi-simple.[69]

If $x \in X$, let

$$G_x := G_{\sigma_x} := \{ y \in G \mid xyx^{-1} = y \} =^{70} \{ y \in G \mid yxy^{-1} = x \}$$
$$L(G)_x := \{ X \in L(G) \mid Ad(x)\, X = X \}$$

Apply (ii), which we have already proved, with $\sigma = \sigma_x$: y a xyx^{-1}. It follows that

$$\dim G_x = \dim L(G)_x$$

The dimension on the right is just the multiplicity of the eigenvalue 1 of $Ad(x)|_{L(G)}$, which is $\dim L(G)_\sigma$ by condition (c)[71], i.e.,

---

$$0 = m(s^{-1})|_{V_i} = m(s^{-1}|_{V_i}) = m(a_i^{-1}),$$

i.e., m(T) is a multiple of $T\text{-}a_i^{-1}$.

[68] Condition (a) means, x is in the normalizer of G in GL_n, which is a closed subgroup by 2.5.11. As for (c), the coefficients of the characteristic polynomial of $Ad(x) = x \cdot ? \cdot x^{-1}$ are polynomials in the entries of x.

inverse image of G under $GL_n \to GL_n$, y a zyz^{-1}

[69] If x is not semi-simple, there is some main space V, which is not an eigenspace. On this main space x has one single eigenvalue λ, but $x\text{-}\lambda \cdot Id$ is not zero on V (but nilpotent). In particular, the minimum polynomial of x on V is a power of $T - \lambda$ of degree > 1. It vanishes at λ together with its first derivative. Hence the minimum polynomial of x has a multiple root. Since m(T) has no multiple roots, m(x) cannot be zero (even on V).

[70] Both sets consist of all $y \in G$ commuting with x.

[71] Both $Ad(x)|_{L(G)}$ and $d\sigma$ are semi-simple. The is no difference between geometric and algebraic multiplicities of eigenvalues. Equality of the characteristic polynomials implies equality of the mutliplicities (whether geometric or algebraic).

(1) $\dim G_x = \dim L(G)_\sigma$ for every $x \in X$.

Now G operates on X by inner automorphisms[72],

$$G \times X \to X, (g,x) \mapsto gxg^{-1}.$$

Consider the morphism

$$G \to G, g \mapsto gxg^{-1}, x \in X \text{ fixed.}$$

This morphism is G-equivariant if the action on the left is left translation and on right is conjugation. Replacing the image by the orbit O(x) of x we obtain an equivariant morphism of homogeneous spaces. The theorem on the fiber dimension (see 4.3.1(ii)) gives for the fiber over x (as for all fibers),

$$\dim G_x = \dim G - \dim O(x)$$

i.e.

$$\begin{aligned} \dim O(x) &= \dim G - \dim G_x \\ &= \dim G - \dim L(G)_\sigma \qquad \text{(cf. (1))} \end{aligned}$$

is independent upon x, All orbits have the same dimension, hence all orbits are closed. In particular

$$O(s^{-1}) = \{gs^{-1}g^{-1} \mid g \in G\}$$

is closed in X, hence in G. But then

$$\phi G = \{ sgs^{-1}g^{-1} \mid g \in G \} = sO(s^{-1})$$

is closed in G, i.e. assertion (ii) is true.

QED.

4.4.5 Corollary: an application to conjugacy classes and centralizers

Let G be a connected linear algebraic group and let $s \in G$ be semi-simple. Then:

(i) The conjugacy class $C := \{xsx^{-1} \mid x \in G\}$ of s in G is closed. The morphism

$$G \to C, x \mapsto xsx^{-1},$$

is separable.

(ii) Let $Z := \{x \in G \mid xsx^{-1} = s\}$ be the centralizer of s in G. Then

$$L(G) = (\mathrm{Ad}(s)-\mathrm{Id})L(G) \oplus \mathrm{Lie}(Z).$$

Proof. Consider the automorphism of algebraic groups

---

[72] Condition (a) is preserved under conjugation since G normalizes itself.

Condition (b) is preserved since x and gxg^{-1} have the same minimum polynomial, $m(gxg^{-1}) = g \cdot m(x) \cdot g^{-1} = 0$.

Condition (c) is preserved sind Ad(x) and $\mathrm{Ad}(gxg^{-1}) = \mathrm{Ad}(g) \circ \mathrm{Ad}(x) \circ \mathrm{Ad}(g)^{-1}$ have the same characteristic polynomial on L(G).

$$\sigma: G \to G, x \mapsto sxs^{-1}.$$

By 4.4.3 it is semi-simple. Let ϕ as in 4.4.4, i.e. $\phi x = (\sigma x)x^{-1} = sxs^{-1}x^{-1}$, then

$$C = s\cdot\phi(G) \text{ and } Z := G_\sigma.$$

Assertion (i) is, in the special case considered here, assertion (i) of 4.4.4. Consider the decomposition

$$L(G) = \mathrm{Ker}(d\sigma)\oplus\mathrm{Im}(d\sigma)$$

of L(G) into the eigenspace of $d\sigma$ for the eigenvalue 0 and the sum of all other eigenvalues.[73] By 3.3.12

$$\mathrm{Im}(d\sigma) = (\mathrm{Ad}(s)-\mathrm{Id})L(G)$$

and

$$\begin{aligned}\mathrm{Ker}(d\sigma) &= L(G)_\sigma && \text{(by definition, see 4.4.1(1))}\\ &= L(G_\sigma) && \text{(by 4.4.4(ii))}\\ &= L(Z) && \text{(see above).}\end{aligned}$$

This proves the claim of assertion (ii).
QED.

Remark

Conjugacy classes of arbitrary elements need not be closed. See, for example, Exercise 4.4.9(6).

4.4.6 Notation: Zentralizers of a diagonalizable group

Let D be a diagonalizable linear algebraic group, which acts as a group of automorphisms on the connected group G. This means that G is a D-space in the sense of 2.3.1 and that for all $d\in D$ the morphism

$$G \to G, g \mapsto d\cdot g.$$

is a group automorphism of G. From 2.5.2 we infer that these are semi-simple automorphisms[74]. Let

$$Z_G(D) := \{g\in G \mid d\cdot g = g \text{ for all } d\in D\}$$

The group D also acts as a group of automorphisms on the Lie algebra $\mathfrak{g}=L(G)$. Let

$$\mathfrak{z}_{\mathrm{Lie}(G)}(D) := \{X\in\mathrm{Lie}(G) \mid d\cdot X = X \text{ for all } d\in D\}.$$

4.4.7 Corollary: the Lie algebra of the centralizer

Let D be a diagonalizable linear algebraic group, which acts as a group of automorphisms on the connected linear algebraic group G. Then

---

[73] Since $d\sigma$ is semi-simple we may consider $d\sigma$ as multiplication by a diagonal matrix.

[74] D consists of semi-simple elements. The action of D on the finite-dimensional invariant subspaces of k[G] is by semi-simple matrices (see the basic property of diagonalizable groups, theorem .2.5.2.).

$$\text{Lie } Z_G(D) = \mathfrak{Z}_{\text{Lie}(G)}(D).$$

Proof. Note that if

$$Z_G(D) = G,$$

then G acts trivially on G and hence on L(G). The assertion is trivial in this case.[75]

Now we proceed by induction on dim G. If dim G = 0, G = {e} and the claim is trivial in view of the above note. Now assume dim G is arbitrary. In view of the above note we may additionally assume,

$$Z_G(D) \neq G.$$

Choose $d \in D$ such that the dimension of the fixed point group

$$G_d := \{g \in G \mid d \cdot g = g\}$$

is minimal. Note that this is a closed subgroup of G (by 4.4.1) of dimension less than dim G. Since D is commutative, D stabilizes G_d, and since the action is by automorphisms, D even stabilizes the identity component

$$H := G_d^0 .$$

Obviously,

$$Z_G(D) = Z_{G_d}(D).$$

Therefore

(1) $$Z_G(D)^0 = Z_{G_d}(D)^0 =^{[76]} Z_H(D)^0.$$

---

[75] For both sides of the identity to be proved we obtain L(G).

[76] $Z_{G_d}(D)$ is a closed subgroup of G_d (for, it is the intersection of closed subgroups of type G_d). Therefore

$$Z_{G_d}(D)^0 \subseteq G_d^0 = H.$$

All elements of the left hand side set are fixed points with respect to D, hence

$$Z_{G_d}(D)^0 \subseteq Z_H(D)$$

hence

$$Z_{G_d}(D)^0 \subseteq Z_H(D)^0.$$

On the other hand, the inclusion $H \subseteq G_d$ implies $Z_H(D) \subseteq Z_{G_d}(D)$ hence

$$Z_H(D)^0 \subseteq Z_{G_d}(D)^0.$$

But then,

$$\begin{aligned} L(Z_G(D)) &= L(Z_H(D)) && \text{(by (1)).}\\ &= \mathfrak{z}_{L(H)}(D) && \text{(by induction hypothesis)}\\ &= \mathfrak{z}_{L(G)}(D)\cap L(H) && \text{(by definition of } \mathfrak{z}_G(D))\\ &= \mathfrak{z}_{L(G)}(D)\cap L(G_d) && \text{(by definition of H)}\\ &= \mathfrak{z}_{L(G)}(D)\cap L(G)_d && \text{(by theorem 4.4.4(ii))}^{77}\\ &= \mathfrak{z}_{L(G)} && \text{(since } d\in D). \end{aligned}$$

QED.

Remark

The corollary applies, in particular, if D is a diagonalizable subgroup of G which acts by inner automorphisms. In this case, $Z_G(D)$ is the usual centralizer of D in G, which justifies, to some extend the above notation.

4.4.8 Proposition: the semi-simple elements of connected nilpotent groups

Let G be a connected nilpotent linear algebraic group. Then the set G_s of semi-simple elements is a central subgroup of G.

Proof. If $x,y\in G$ write

$$(x, y) := xyx^{-1}y^{-1}$$

for the commutator. Recall that G is nilpotent if there is some $n>0$ such that all iterated commutators

$$(x_1,(x_2,\ldots,(x_n , x_{n+1})\ldots))$$

are equal to e.

Now let $s\in G$ be semi-simple. We have to show that s is in the center of G. Write

$$\sigma(x) := sxs^{-1} \text{ and } \phi(x) := s(x)x^{-1} = (s, x).$$

If n is as above, then

$$\phi^n(G) = \{e\}.$$

Hence the linear map

$$d\phi = d\sigma - Id : L(G) \to L(G)$$

(see 3.3.12(i) for this formula) is nilpotent. On the other hand, $d\sigma$ is, if one fixes an embedding into some general linear group, also conjugation with s, hence a semi-simple linear map. Therefore, $d\phi$ is both semi-simple and nilpotent, i.e., $d\phi = 0$. But then

---

[77] d defines a semi-simple automorphism of G, see 4.4.6.

$$L(G_\sigma) = L(G)_\sigma = \{ X \in L(G) \mid (d\phi)X = X \} = L(G).$$

The closed subvariety G_σ of the irreducible variety G has dimension dim G, i.e., $G_\sigma = G$, i.e, $\sigma = Id$, i.e., s is in the center of G.

QED.

Remark

A more precise result will be given later (6.8). It should be observed that the connectedness assumption in 4.4.8 is essential (see Exercise 4.4.9(5)).

4.4.9 Exercises

(1) Let char k = 2, $G = SL_2$ and $\sigma: G \to G$ the inner automorphism defined by the matrix

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

Show that $L(G_\sigma) \neq L(G)_\sigma$.

(2) Let $G = GL_n$ and let σ be an inner automorphism of G. Show that $L(G_\sigma) = L(G)_\sigma$.

(3) Let G be a closed subgroup of GL_n. The Lie algebra $\mathfrak{g}$:= L(G) is a subalgebra of gl_n. Assume that there is a complementary subspace $\mathfrak{g}'$ of $\mathfrak{g}$ in gl_n which is stable under Ad G,

$$gl_n = \mathfrak{g} \oplus \mathfrak{g}'.$$

(a) If σ is an inner automorphism of G then $L(G_\sigma) = L(G)_\sigma$. (Hint: imitate the argument in the second part of the proof of theorem 4.4.4).

(b) Let $x \in G$ and C be the conjugacy class of x in GL_n. Show that $C \cap G$ consists of finitely many conjugacy classes of G. (Hint: let X be a component of $C \cap G$ and let D be conjugacy class of some $x \in X$ in G. Deduce from (a) that $T_x X = T_x D$ and X = D).

(4) (a) Show that the number of unipotent conjugacy classes in GL_n is finite (use the theory of Jordan normal forms, see [26, Ch. XV, §3]).

(b) Let char k ≠ 2 and $G := SO_n$ embedded into GL_n in the usual manner. Then G satisfies the condition of the previous exercise. Deduce from (a) and exercise 3(b) that the number of unipotent conjugacy classes in G is finite.

Remark: This conclusion can be drawn, by the same argument, in more general circumstances. See for example, R. Steinberg : Conjugacy classes in algebraic groups, Lecture Notes in Math 366, Springer 1974, p. 106. One gets involved here in the structure theory of reductive linear algebraic groups, discussed in our later chapters.

(5) Let G be the dihedral Group[78] of order 8. Then G is nilpotent and has an irreducible complex representation of degree 2. This shows that 4.4.8 cannot be extended to non-connected groups (similar properties hold for all non-abelian p-groups).

(6) (a) Show that the conjugacy class of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in GL_2 is not closed.

(b) More generally, one can show as folllows that the conjugacy class of an unipotent element $x \neq 1$ in GL_n is not closed. Let $x = 1+X$, where X is a nonzero nilpotent $n \times n$-matrix. Using the theory of Jordan normal forms, define a multiplicative 1-parameter subgroup λ of GL_n (2.5.1) such that $\lambda(t)X\lambda(t)^{-1} = t^2X$ $(t \in k^*)$. Deduce from this that 1 lies in the closure of the conjugacy class of x.

Notes

(about the methods used in this chapter)

5. Quotients

5.1 Chevalley's theorem

5.1.1 Lemma: Subgroups and their Lie algebras as stabilizers

Let G be a linear algebraic group and $H \subseteq G$ a closed subgroup. Then there is a finite dimensional k-linear subspace

$$V \subseteq k[G],$$

which is invariant under right translations, and a k-linear subspace

$$W \subseteq V$$

satisfying

(1) $$H = \{x \in G \mid \rho_x W = W\}$$

---

[78] the symmetry group of a regular polygon in the plain having n vertices is denoted D_{2n}. It consists of the n rotations and of the reflexions with respect to the lines connecting the center of the polygon with one of the vertices. It can be considered as the extension of $\mathbb{Z}_2 = \langle b \rangle$ by $\mathbb{Z}_n = \langle a \rangle$ using the relation $ab = ba^{-1}$. With other word its the semi-direct product of these groups, where a operates on $\mathbb{Z}_n$ via inversion map $g \mapsto g^{-1}$.

and

(2) $$L(H) = \{ X \in L(G) \mid X(W) \subseteq W \}.$$

Proof. Let

$$I = I(H) = (f_1,\ldots,f_r) \subseteq k[G]$$

be the ideal of the subgroup H and

$$V \subseteq k[G]$$

a finite dimensional k-linear subspace containing the set of generators f_i of the ideal I. We may assume that V is stable under right translation ρ_g , $g \in G$ (see 2.3.4). Restriction to V of right translation defines a rational representation (see 2.3.5)

$$\phi: G \to GL(V),\ g \mapsto \rho_g|_V .$$

Let

$$W := V \cap I.$$

Since I is invariant under right translations with elements of H (see 2.3.6), we have

$$\rho_x W = W \text{ for } x \in H.$$

Conversely, if $x \in G$ is such that this identity holds, then

$$\rho_x f_i \in W \subseteq I$$

for every generator f_i , hence $\rho_x I \subseteq I$. From 2.3.6 we see that $x \in H$. This proves (1).

Proof of the inclusion "$\subseteq$" of (2).

As we have seen above, the subspace $W \subseteq V$ is invariant under $\phi(H)$, i.e. ϕ maps H to the closed subgroup subgroup $GL_W(V) \subseteq GL(V)$ of linear transformations preserving W. There is a commutative square

$$\begin{array}{ccc} H & \xrightarrow{\psi} & GL_W(V) \\ \downarrow & & \downarrow \\ G & \xrightarrow{\phi} & GL(V) \end{array}$$

where the vertical maps are the natural inclusions and ψ is the restriction of ϕ. Passing to the tangent spaces at e we obtain a commuative square

$$\begin{array}{ccc} L(H) & \xrightarrow{d\psi} & gl_W(V) \\ \downarrow & & \downarrow \\ L(G) & \xrightarrow{d\phi} & gl(V) \end{array}$$

where the upper right Lie algebra consists of the linear maps preserving W. This means

$$(d\phi)(X) \in gl_W(V) \text{ for } X \in L(H),$$

i.e.,

$$(d\phi)(X)W \subseteq W \text{ for } X \in L(H).$$

This gives the inclusion to be proved (since, $(d\phi)(X)f = X(f)$ for $f \in W$, see Exercise 3.3.4).

Proof of the inclusion "$\supseteq$" of (2).

We have to use Lemma 3.3.7 which says that the restriction map[79]

$$\lambda: D_{G,H} \to D_H \quad X \mapsto X|_H$$

where

$$D_H = Der_k(k[H], k[H])$$

$$D_{G,H} = \{X \in Der_k(k[G],k[G]) \mid X(I) \subseteq I\}$$

induces an isomorphism

$$D_{G,H} \cap L(G) \to L(H).$$

Let $X \in L(G)$ such that $X(W) \subseteq W$. We have to prove

$$X \in L(H).$$

By assumption

$$X(f_i) \in W \subseteq I$$

for every i, hence

$$X(I) \subseteq I.$$

Therefore X is in $D_{G,H} \cap L(G)$ and its restriction Y to H is in L(H), i.e., there is a tangent vector $Y \in L(H)$, which, considered as a tangent vector to G, is Y. This proves the converse inclusion.

QED.

5.1.2 Lemma: Invarianz and passage to exterior powers

Let V be a finite dimensional k-vectorspace,

$$W \subseteq V$$

a k-linare subspace of dimension

$$d := \dim W$$

and

$$\phi: GL(V) \times V \to V, \quad (x, v) \mapsto x(v)$$

the canonical rational representation. Denote by

$$\phi_d: G \times \wedge^d V \to \wedge^d$$

---

[79] The notation $X|_H$ is rather incorrect. The symbol denotes here the derivation induced on the factor ring k[H] of k[G].

the rational representation induced by ϕ on the d-th exterior power and let

$$L := \wedge^d W \ (\subseteq \wedge^d V).$$

Then:

(i) For $x \in GL(V)$ one has $x \cdot W = W \Leftrightarrow (\phi_d(x)L = L$.

(ii) For $X \in gl(V)$ one has $XW \subseteq W \Leftrightarrow d\phi_d(X)L \subseteq L$.

Proof. The implications "" are trivial. It will be sufficient to prove the converse implications "$\Leftarrow$".

Proof of (i). Fix some $x \in GL(V)$. Let

$$v_1,\ldots,v_n \in V$$

be a basis of V such that

$$v_1,\ldots,v_d \in W$$

is a basis of W. The elements

$$v_{i_1} \wedge \ldots \wedge v_{i_d} \text{ with } i_1 < \ldots < i_{i_d}$$

form a basis of $\wedge^d V$ and

$$v_1 \wedge \ldots \wedge v_d \in L$$

is one of L. For the given $x \in GL(V)$ one can choose the above basis of V such that, moreover,

$$v_{1+l},\ldots,v_{d+l} \in x(W)$$

is a basis of x(W). We have to prove $l = 0$ if L ist stable under $\phi_d(x)$. Write

$$e := v_1 \wedge \ldots \wedge v_d$$

$$f := v_{1+l} \wedge \ldots \wedge v_{d+l}$$

Then $\phi_d(x)e = \lambda f$ for some $\lambda \in k$. If $l > 0$, then e and f are linearly independent and $\phi_d(x)$ does not stabilize L.

Proof of (ii). Fix some $X \in gl(V)$. Then (cf. 3.3.14(4))

$$d\,\phi_d(X)e = \sum_{i=1}^{d} v_1 \wedge \ldots \wedge v_{i-1} \wedge Xv_i \wedge v_{i+1} \wedge \ldots \wedge v_d .$$

Writing $Xv_i = \sum_{j=1}^{n} a_{ij} v_j$ we have

$$d\,\phi_d(X)e = \sum_{i=1}^{d} \sum_{j=1}^{n} a_{ij} v_1 \wedge \ldots \wedge v_{i-1} \wedge v_j \wedge v_{i+1} \wedge \ldots \wedge v_d .$$

In case $a_{ij} \neq 0$ for some $i \leq d$ and $d < j$, then L cannot be stable under

$$d\,\phi_d(X).$$

Hence $a_{ij} = 0$ for $i \leq d$ and $d < j$. But then W is stable under X.

QED.

5.1.3 Theorem: Subgroups and their Lie algebras as stabilizers of lines

Let G be linear algebraic group and $H \subseteq G$ a closed subgroup. Then there is a rational representation

$$\phi: G \to GL(V)$$

and a 1-dimensional k-linear subspace $L \subseteq V$ such that

$$H = \{x \in G \mid (\phi x)L = L\}$$

and

$$L(H) = \{X \in L(G) \mid d\phi(X)L \subseteq L\}.$$

Proof. This is a consequence of the previous two results 5.1.1 and 5.1.2.

QED.

5.1.4 Corollary (Theorem of Chevalley)

Let G be a linear algebraic group and $H \subseteq G$ a closed subgroup. Then there is a quasi-projective[80] homogeneous G-space X and a point $x \in X$ such that the following conditions are satisfied.

(i) H is the isotropy group of x in G, $H = G_x = \{ g \in G \mid g \cdot x = x \}$.

(ii) The morphism $\psi: G \to X$, $g \mapsto g \cdot x$, induces a separable morphism

$$\psi^0: G^0 \to \phi G^0.$$

(iii) The fibers of ψ^0 are the cosets gH ($g \in G$).

Proof. Let V and L and be as in the previous theorem 5.1.3. Denote by

$$\mathbb{P}(V)$$

the projective space of 1-dimensional k-linear subspaces of V (called projectivation of V). Let

$$x \in \mathbb{P}(V)$$

be the point defined by $L \subseteq V$. Denote by π the canonical morphism

$$\pi: V - \{0\} \to \mathbb{P}(V)$$

mapping each none-zero vector to the 1-space generated by it. The group G acts on $\mathbb{P}(V)$ such that

$$g \cdot \pi(v) = \pi(g \cdot v) \text{ for } v \in V, g \in G,$$

and $\mathbb{P}(V)$ is a G-space with this action. Denote by X the orbit of x under this action. Then X is open in its closure (see 4.3.1(i)), hence is a quasi-projective variety. Assertions (i) and (iii) follow now from the previous result 5.1.3 and the fact that the orbital map

---

[80] i.e. an open subvariety of a projective variety.

$$\psi: G \to X, g \mapsto gx,$$

is equivariant as a map of G-spaces.

For the proof of (ii) it is sufficient to show that (see 3.2.21(ii)) the differential

$$d\psi = (d\phi)_e : L(G) = T_e G \to T_e X,$$

is surjective. Since

$$\begin{aligned} \dim T_e X &= \dim X && \text{(homogeneous spaces are non-singular)} \\ &= \dim G - \dim \phi^{-1}(x) && \text{(see 4.3.3(ii))}^{81} \\ &= \dim G - \dim H && \text{(see 5.1.3 above)} \\ &= \dim L(G) - \dim L(H) \end{aligned}$$

it is sufficient to show

$$\mathrm{Ker}(d\psi) = L(H).$$

Since ψ is constant on $H \subseteq G$, i.e., the composition

$$H \to G \xrightarrow{\psi} X$$

factors over the one-point space, the restriction of $d\psi$ to $L(H)$ is zero, i.e.

$$L(H) \subseteq \mathrm{Ker}(d\psi).$$

Conversely, assume $X \in \mathrm{Ker}(d\psi)$. The morphism ψ is the composition

$$G \to V - \{0\} \xrightarrow{\pi} \mathbb{P}(V), \; g \mapsto g \cdot e \mapsto \phi(g)L,$$

where $e \in L \subseteq V$ denotes a none-zero vector and the first map comes from the action ϕ of G on V. Therefore[82],

$$(d\phi)(X)(e) \in \mathrm{Ker}\,(d\pi)_e = \pi^{-1}(\pi(e)) \cup \{0\} =^{83} L .$$

Since $(d\phi)(X)$ is linear and e generates L, this implies

$$(d\phi)(X)L \subseteq L .$$

From the second identity of 5.1.3 we see that $X \in L(H)$.

---

[81] All fibers of morphisms of homogeneous space have the same dimension.

[82] We use the fact that evaluation at e commutes with the differential.

[83] We may assume $V = k^{n+1}$ and $e = (1,0,...,0)$. Choosing appropriate affine coordinates on $\mathbb{P}(V)$ the map π looks locally like

$$k^{n+1} = V - \{0\} \to \mathbb{P}(V), \; (x_0,...,x_n) \mapsto [x_0,...,x_n] \mapsto (x_1/x_0,...,x_n/x_0),$$

and the differential at e is

$$k^{n+1} \to k^n,$$

$$(dx_0,...,dx_n) \mapsto (dx_1/x_0 - (x_1/x_0^2)dx_0,...,dx_n/x_0 - (x_n/x_0^2)dx_0)|_e$$
$$= (dx_1,...,dx_n).$$

We see that the kernel can be identified with the subspace generated by e.

QED.

5.2 Construction of quotients

5. 2.1 Quotients of lineare algebraic groups modulo closed subgroups

Let G be a linear algebraic group and H⊆G a closed subgroup. A quotient of G modulo H is a pair (G/H, a) of a homogeneous space G/H for G together with a point a∈G/H whose isotropy group is H, such that the following universal property holds:

´(*) For any pair (Y,b) of a homogeneous G-space Y and a point b∈Y, whose isotropy group contains H, there is a unique G-morphism

$$\phi: G/H \to Y \text{ with } \phi a = b.$$

Remark

The main result of this section is the following existence theorem.

5.2.2 Theorem: existence and uniqueness of quotiens

Let G be a linear algebraic group and H ⊆ G a closed subgroup. Then a quotient (G/H, a) exists and is unique up a G-isomorphism.

More precisely, if X and x are as in 5.1.4, then (X,x) is a quotient.

Proof. The uniqueness part of the claim is trivial. To prove the existence statement we proceed as follows.

First we define G/H as a ringed space. Using 5.1.4 it will be shown that this ringed space is an algebraic variety.

Step 1. G/H as a set.

As usual let

$$G/H := \{ gH \mid g \in G \}$$

the set of left cosets modulo H. Denote by

$$\pi: G \to G/H,\ g \mapsto gH,$$

the canonical map.

Step 2. G/H as topological space. Define a subset

$$U \subseteq G/H$$

to be open, if $\pi^{-1}(U)$ is open in G. This defines a topology in G such that π is a continuous and open map (cf. 4.1.6(i)).

Step 3. The structure sheaf of G/H. We define a sheaf $\mathcal{O}$ of k-valued functions on G/H as follows (see 1.4.2). Let U ⊆ G/H be open. Then

$$\mathcal{O}(U)$$

is the ring of functions f:U→k such that $f\circ\pi:\pi^{-1}(U) \to k$ is regular on

$$\pi^{-1}(U) \subseteq G.$$

Step 4. G/H as a G-space.

G acts transitively on G/H by left translations (set theoretically). These left translations are isomorphisms of the ringes space (G/H, $\mathcal{O}$). More precisely, if g∈G, then

$$G/H \to G/H,\ xH \mapsto gxH,$$

is an isomorphism of ringed spaces.[84]

If (Y, b) is as in 5.2.1 (*) then the map

$$\phi: G/H \to Y,\ xH \mapsto xb,$$

is well-defined[85]. It is the only G-equivariant map such that

$$\phi a = b$$

where a := eH. Moreover, the composition of ϕ with the canonical map is just the orbital map

$$G \to Y,\ g \mapsto gb.$$

Since the latter is a morphism of varieties, ϕ is continuous and lift along ϕ map regular functions to regular function, i.e., ϕ is a morphism of ringed spaces.

To finish the proof of the theorem, it is sufficient to show that the ringed space G/H is isomorphic to a homogeneous space in the sense of 2.3.1. To do so, we use 5.1.4. Let X, x and $\psi: G \to X, g \mapsto gx$, as in 5.1.4. By the properties of the ringed space G/H there is a G-equivariant morphism of ringed spaces

$$\phi: G/H \to X \text{ with } \phi a = x.$$

It is sufficient to show that this is an isomorphism of ringed spaces.

Consider the commutative diagram

$$\begin{array}{ccc} G & & \\ \downarrow & \searrow^{\psi} & \\ G/H & \xrightarrow{\phi} & X \end{array}$$

where the vertical map at the left is the natural map.

---

[84] This map is bijective and open: for U⊆G/H open, the preimage $\pi^{-1}U$ is open in G, hence so is $\pi^{-1}gU = g\pi^{-1}U$.
Since g runs through a group, the map is also continuous, hence a homeomorphism.
Moreover, section f of $\mathcal{O}$, i.e. functions f such that $f\circ\pi$ is regular are mapped to functions $\lambda_g f$ such that $(\lambda_g f)\circ\pi = \lambda_g(f\circ\pi)$ = regular, i.e. to section of $\mathcal{O}$. The map induced a morphism of ringed spaces.

[85] If xH = yH then $y^{-1}x \in H$, hence $y^{-1}xb = b$, hence xb = yb.

By property 5.1.4(i), H is the isotropy group of x in G. Therefore the map f is bijective. As a morphism of ringed spaces it is continuous.
For $U \subseteq G/H$ open, the set

$$\phi U = \psi(\phi^{-1}(U))$$

is open (since morphisms of homogeneous spaces are open, see 4.3.3(i)). Hence ϕ is open, ϕ^{-1} is continuous, i.e. ϕ is a homeomorphism of topological spaces.

To prove that ϕ is an isomorphism of ringed spaces, it is sufficient to show the following.

For $U \subseteq X$ the homomorphism of k-algebras

$$(1) \qquad \mathcal{O}_X(U) \to \mathcal{O}(\phi^{-1}(U)),\ f \mapsto f\circ\phi,$$

defined by ϕ is bijective. Since the orbital map ψ is surjective, the same is true for ϕ (by the above diagram), hence (1) is injective. We have yet to prove surjectivity. From the definition of $\mathcal{O}$ we see that this means the following: if

$$f\colon V := \psi^{-1}(U) \to k$$

is any regular function, which is constant on the fibers of ϕ,

$$f(gh) = f(g) \text{ for } g\in V \text{ and } h\in H,$$

then there is a regular function

$$F\colon U \to k$$

such that

$$F\circ\psi = f.$$

Since f is constant on the fibers of ϕ, it comes from a function on the set $\phi^{-1}(U)$, and therefore, since ϕ is bijective, from a function on U. In other words, F exists (and is unique) if we omit the regularity condition. Thus, all we have to prove is that F is regular. This is a local condition and we may consider the irreducible components of the variety X separately (which are G^0-orbits by 4.3.2). The reduces the the prove to the case that G is connected.
Let

$$\Gamma \subseteq V\times\mathbb{A}^1$$

be the graph of $f\colon V \to k$, i.e.,

$$\Gamma := \{(g,f(g)) \mid g\in V\}.$$

Moreover, let

$$\Gamma' := (\psi\times Id)\Gamma \subseteq U\times\mathbb{A}^1.$$

Then

$$U\times\mathbb{A}^1 - \Gamma' =^{86} (\psi\times Id)(V\times\mathbb{A}^1 - \Gamma).$$

Since the graph Γ of the function f is closed[87] in $V\times\mathbb{A}^1$, the difference

$$V\times\mathbb{A}^1 - \Gamma$$

is open. By 4.3.3(i) the equivariant map $\psi\times Id$ is open, i.e.,

$$U\times\mathbb{A}^1 - \Gamma'$$

is open, hence Γ' is closed in $U\times\mathbb{A}^1$. Consider the projection

$$\lambda: \Gamma' \to U$$

onto the first factor. Since ψ induces a surjection $V \to U$ and f is constant on the fibers, the map λ bijective (and is trivially a morphism of varieties). Composition with $\psi\times Id$ gives a morphism

$$V \cong \Gamma \to U,$$

which is, up to isomorphism equal to ψ, hence separable by 5.1.4(ii). Therefore, λ is separable. Since λ is bijective, its degree is 1, i.e., it is birational (see 4.1.6(iii)). Hence the is an open subset

$$U' \subseteq U$$

such that λ induces an isomorphism $\lambda^{-1}U' \to U'$ (see 4.1.2). But then the same is true with U' replaced by $gU'\cap U$ for any $g\in G$, Since G acts transitively on itself by left translations we see that

$$\lambda: \Gamma' \to U$$

is an isomorphism. The composition of λ^{-1} with the projection to the second factor is hence a regular function

$$F: U \to k$$

such that the graph is Γ'. But then, $f = \psi\circ F$.
QED.

5.2.3 Corollary: quasi-projecitivity of the quotient and separability of the canonical map

Let G be a linear algebraic group and $H\subseteq G$ a closed subgroup. Then:

(i) G/H is a quasi-projective variety of dimension

$$\dim G/H = \dim G - \dim H.$$

(ii) If G is connected, the canonical morphism $G \to G/H$ is separable.

Proof. The assertions follow from the contruction of G/H in 5.2.2 and the assertions of 5.1.4, except for the dimension formula. The latter follows from 4.3.3.

---

[86] Since f is constant on the cosets gH, $(g, c) \in\Gamma$ implies $gH\times\{c\} \subseteq\Gamma$. Therefore, all fibers of the map $\psi\times Id$ are either completely inside Γ or completely outside.

[87] The graph of any morphism $X\to Y$ of varieties is closed in $X\times Y$ (see 1.6.10(i)).

QED.

5.2.4 Exercises

Let G be a linear algbraic group and $H \subseteq G$ a closed subgroup.

(1) The follwing properties are equivalent.
   (a) H meets all components of G.
   (b) $G = G^0H$.

(2) An open subvariety of an affine algebraic variety is called quasi-affine variety (see 1.6.12(4) for a quasi-affine variety which is not affine). If all homomorphisms of algebraic groups $H \to \mathbf{G}_m$ are trivial, then G/H is quasi-affine.[88]

(3) Let $G := SL_2$ and $H \subseteq G$ the subgroup of upper triangular matrices. Then $G/H \cong \mathbb{P}^1$.[89]

(4) Let H_i be a closed subgroup of a linear algebraic group G_i for i =1,2. Prove that there is an isomorphism of $G_1 \times G_2$-spaces

$$G_1/H_1 \times G_2/H_2 \cong G_1 \times G_2/H_1 \times H_2.$$

(5) Let H and K be connected closed subgroups of the linear algebraic group G. Then:
   (a) HK is an irreducible quasi-affine subvariety of G, whose dimension equals dim H + dim K - dim $H \cap K$ (Hint: let $H \times K$ act on G by $(x,y)g := xgy^{-1}$ and consider the orbit of e).
   (b) Let π: $G \to G/K$ the canonical map g a gK (the points of G/K being identified with the cosets gK). By (a) we have
   $$\dim \pi H = \dim H - \dim H \cap K.$$
   Show that the restriction of π to H is a separable morphism onto its image if and only if
   $$\dim L(H) \cap L(K) = \dim H \cap K.$$
   (c) Let $G := SL_2$, H the subgroup of diagonal matrices and K a distinct conjugate of H. Show that, if char k = 2, we have
   $$\dim L(H) \cap L(K) \neq \dim H \cap K.$$

(6) Let char $k \neq 2$. $G := SO_n$, $n \geq 3$ (see Exercise 2.1.3(4)) acting on

---

[88] As we have seen, there is a rational representation $G \to GL(V)$ such that H is the stabilizer of a 1-dimensional subspace $L \subseteq V$. By assumption H act trivially on L, i.e. H is even the stabilizer of a point $x \in V$. But then, G/H may be identified with the Orbit of x in V, which is something quasi-affine.

[89] The natural action of SL_2 on $\mathbb{P}^1$ is transitive where the stabilizer of a fixed point $x \in \mathbb{P}^1$ can be identified with H.

$$V := k^n$$

in the standard manner. Let

$$X := \{ (x_1,...,x_n) \in V \mid x_1^2 + ... + x_n^2 = 1\}$$

and e := (0,...,0, 1). Then G acts on X. The isotropy group of e∈X is SO_{n-1} , viewed as subgroup of SO_n, Show that SO_n/SO_{n-1} is isomorphic to the affine G-variety X (Hint: use Witt's theorem[90], see [26, Ch. XIV, §5]).

5.2.5 Proposition: quotients modulo normal subgroups are linear algebraic groups

Let G be a linear algebraic group and N⊆G a closed normal subgroup. Then:

(i) G/N is an affine variety.

(ii) Provided with the usual group structure, G/N becomes a linear algebraic group.

Proof. Consider the following action of G×G on G/N.

$$G\times G\times G/N \to G/N,\ (g',g'',xN) \mapsto g'xg''^{-1}N.$$

This action is correctly defined, since N is a normal subgroup, and G/N becomes a homogeneous G×G-space. The isotropy group of H contains H×H. By the universality property of quotient spaces 5.2.1 there is a morphism of G×G-spaces

$$G/H\times G/H = G\times G/H\times H \to G/H$$

preserving the base points, i.e.,

$$(g'H, g''H) \mapsto g'g''^{-1}H,$$

defines a morphism. From this we see that G/H is an algebraic group variety. It remains to be proved assertion (i).

For this, choose V, L and

$$\phi: G \to GL(V),$$

i.e. ϕ is a rational representation such that N is the stabilizer of L in G and L(N) is the stabilizer of L in L(G). For any rational character

$$\chi:N \to G_m$$

of H we write

$$V_\chi := \{v\in V \mid \phi(h)v = \chi(h)v \text{ for } h\in N\}.$$

---

[90] Each isometry of subspaces of V may be extended to an isometry of V. In other words SO_n acts transitively on the k-linear (n-1)-planes of V.

From the linear independence of characters it follows that the subspace $V' \subseteq V$ spanned by the spaces V_χ is a direct sum of these spaces,

$$V' := \oplus_{\chi \in X^*(N)} V_\chi \subseteq V.$$

Since N is normal in G, each $g \in G$ permutes the spaces V_χ :

$$\phi(h)(\phi(g)v) = \phi(hg)v = \phi(gh')v = \phi(g)\chi(h')v = \chi'(h)\phi(g)v$$

with $h' = g^{-1}hg \in N$ and $\chi' : H \to G_m$ the character such that

$$\chi'(h) := \chi(g^{-1}hg).$$

Therefore, V' is $\phi(G)$-stable. Since $L \subseteq V$ is contained in one of the spaces V_χ it is contained in V' and the stabilizers of L in G and L(G) do not change if the representation ϕ is restricted to V'. Hence we may assume,

$$V' = V.$$

Denote by

$$W \subseteq \mathrm{End}(V)$$

the subspace of linear endomorphisms stabilizing each direct summand V_χ and consider the rational map[91]

$$\psi : G \to GL(W),\ x \mapsto (w \mapsto \phi(x)w\phi(x)^{-1}).$$

It is obviously a homomorphism of algebraic groups.

Claim. $\mathrm{Ker}(\psi) = N$.

If $h \in N$, $\phi(h)$ is multiplication by $\chi(h)$ on V_χ and $\phi(h)^{-1}$ is multiplication by $\chi(h)^{-1}$, hence

$$\psi(h)w = \chi(x)w\chi(x)^{-1}w = w,$$

$\psi(h) = \mathrm{Id}$.

Conversely, if $h \in \mathrm{Ker}(\psi)$, then $\phi(h)w\phi(h)^{-1} = w$, i.e., commutes $\phi(h)$ with every $w \in W$. But then $\phi(h)$ is scalar multiplication on each V_χ. In particular $\phi(h)$ stabilizes L. But then $h \in N$.

This proves the claim. In particular, ψ induces an injective morphism of algebraic varieties

$$\lambda : G/H \to GL(W),\ xH \mapsto (w \mapsto \phi(x)w\phi(x)^{-1}).$$

---

[91] Since $\phi(x)$ and $\phi(x)^{-1} = \phi(x^{-1})$ are in W, the same is true for $\phi(x)w\phi(x)^{-1}$. Hence ψ is welldefined. It is obviously a morphism of varieties: choosing a basis of V, $\phi(x)$ and $\phi(x)^{-1}$ can be identified with matrices whose entries are regular functions of x.

The explicit formula shows, this is in fact a homomorphism of algebriac groups. In particular, the image of λ is a closed subgroup of GL(W) (see 2.2.5(ii)). Since GL(W) is affine, this image is affine. Hence it will be sufficent to show, that

$$\lambda: G/H \to \mathrm{Im}(\lambda)$$

is an isomorphism. By construction, this map is bijective. Hence it is sufficient to show that the tangent map

$$(d\lambda)_e: T_e(G/H) \to T_e(\mathrm{Im}\ \lambda)$$

is bijective (see 4.3.3(iii)). Since λ is a morphism of homogeneous spaces, Im λ is none-singular, i.e.,

$$\dim T_e(\mathrm{Im}\ \lambda) = \dim \mathrm{Im}\ \lambda \le \dim G/H = \dim T_e(G/H).$$

Thus, it will be sufficient to show that

$$(d\lambda)_e \text{ is injective.}$$

Consider the composition with the differential of the natural map $\rho: G \to G/H$, i.e. with

$$(d\rho)_e: L(G) \to L(G/H).$$

Note that

$$\mathrm{Ker}(d\rho)_e =^{92} L(H).$$

Hence it is sufficient to prove the following.

(*) If $X \in L(G)$ and $(d\psi)_e X = 0$ then $X \in L(H)$.

To prove this, write ψ as the following decomposition[93].

$$\psi : G \xrightarrow{\Delta} G\times G \xrightarrow{id\times\iota} G\times G \xrightarrow{\phi\times\phi} W\times W \xrightarrow{R\times L} GL(W)\times GL(W) \xrightarrow{\mu} GL(W),$$

$$x \mapsto (x,x) \mapsto (x,x^{-1}) \mapsto (\phi(x), \phi(x)^{-1}) \mapsto R_{\phi(x)}\times L_{\phi(x)^{-1}} \mapsto R_{\phi(x)}\circ L_{\phi(x)^{-1}}$$

Passing to the differentials at e we obtain

$$d\psi: LG \xrightarrow{\Delta} LG\times LG \xrightarrow{id\times(-1)} LG\times LG \xrightarrow{d\phi\times d\phi} LW\times LW \xrightarrow{R\times L} gl(W)\times gl(W) \xrightarrow{+} gl(W),$$

$$X \mapsto (X,X) \mapsto (X,-X) \mapsto (d\phi(X),-d\phi(X)) \mapsto R_{d\phi(X)}\times L_{-d\phi(X)} \mapsto R_{d\phi(X)}+L_{-d\phi(X)}$$

Note that R and L are linear, hence equal to their differentials, and the differential of the multiplication map is summation. In other words,

$$(d\psi)(X)w = w\cdot d\phi(X) - d\phi(X)\cdot w \text{ for } w\in W \text{ and } X\in L(G).$$

Therefore, if X is as in (*),

$$0 = (d\psi)(X)w = w\cdot d\phi(X) - d\phi(X)\cdot w \text{ for every } w\in W.$$

---

[92] Since ρ is constant on H, $d\rho|_{L(H)} = 0$, i.e. $L(H)\subseteq \mathrm{Ker}(d\rho)$. On the other hand, $\dim \mathrm{Ker}(d\rho) \le \dim L(G/H) - \dim L(G) = \dim H = \dim L(H)$.

[93] Here ι denotes inversion, L left translation and R right translation.

Hence $d\phi(X)$ commutes with every $w \in W$, i.e., $d\phi(X)$ is scalar multiplication on every V_χ and, therefore, stabilizes L,

$$d\phi(X)L \subseteq L.$$

But then $X \in L(H)$ as required (see 5.1.3).

QED.

5.2.6 Exercises

Let G be a linear algebraic group and $H \subseteq G$ a closed subgroup.

(1) Let N be a closed normal subgroup in H. Then

$$G/H \cong (G/N)/(H/N).$$

(2) Let $A := \{f \in k[G] \mid f(gh) = f(g) \text{ for } g \in G, h \in H\}$.

(a) If G/H is affine then $k[G/H] = A$.

(b) For G/H to be affine it is necessary and sufficient that A is a k-algebra of finite type which separates the cosets of H.

The latter requirement means that if xH and yH are distinct cosets then there is some $f \in A$ such that $f(xH) = 1$ and $f(yH) = 0$. (Hint: If A is a k-algebra of finite type let X be an affine algebraic variety with $k[X] = A$. Show that left translations induce a structure of homogeneous space on X, which satisfies the requirements of 5.2.1).

(c) Let H be a torus. Then G/H is affine. (Hint: If xH and yH are distinct cosets, let I and J be the ideals in k[G] which they define. Then $I+J = k[G]$. Deduce from 2.5.2(c) that $I \cap A + J \cap A = A$ and verify the condition of (b)).

(3) Let T be a torus and $T' \subseteq T$ any subtorus (i.e. a closed subgroup which is a torus. Then:

(a) T/T' is a torus.

(b) The short exact sequence

$$\{e\} \to T' \to T \to T/T' \to \{e\}$$

induces a short exact sequence

$$0 \to X(T/T') \to X(T) \to X(T') \to 0$$

of the character groups.

Solutions

(3)

Since T is commutative, T' is normal in T, hence T/T' is a linear algebraic group. Every rational representation

$$T/T' \to \mathrm{Aut}(V)$$

of T/T' can be considered as a rational representation of T, hence decomposes into 1-dimensional representations (by 2.5.2). Hence

T/T' is diagonalizable. As an image of a connected variety T/T' is also connected, hence a torus. This proves (a).
Consider the sequence

$$0 \to X(T/T') \to X(T) \to X(T') \to 0$$

By funtoriality, we see that it is a complex (the composition of two sucessive maps is trivial). Since $T \to T/T'$ is surjective, the sequence is exact at X(T/T'). A character

$$\chi: T \to G_m$$

with trivial restriction to T' factors over T/T' by the universality property of T/T'. Therefore, the sequence is exact at X(T). We have yet to prove surjectivity of

$$X(T) \xrightarrow{\alpha} X(T').$$

Since X(T') is a free abelian group of finite rank, the same is true for the subgroup

$$\mathrm{Im}(\alpha) \subseteq X(T').$$

Hence there is a torus S such that

$$X(S) = \mathrm{Im}\,(\alpha) \subseteq X(T').$$

The inclusion of the character groups induces an inclusion of the coordinate rings

$$k[S] \subseteq k[T']$$

(which are freely generated by the characters) and hence a dominant morphism

$$f: T' \to S.$$

It will be sufficient to show that this is an isomorphism of algebraic groups.

This morphism is a homomorphism of algebraic groups. To see this, let $s,t \in T'$ and $\chi \in X(S)$. Then

$$\begin{aligned}
\chi(f(st)) &= f^*(\chi)(st) \\
&= \chi(st) \quad \text{(since f induces the inclusion } \mathrm{Im}(\alpha) \subseteq X(T')) \\
&= \chi(s)\chi(t) \\
&= \chi(f(s))\chi(f(t)) \quad \text{(as above)} \\
&= \chi(f(s)f(t))
\end{aligned}$$

Since the characters S generate the coodinate ring of S, this implies

$$f(st) = f(s)f(t),$$

i.e., f a homomorphism of algebraic groups as claimed. But then, Im(f) is closed in S and

$$f: T' \to S \text{ is surjective.}$$

Moreover, the surjection

$$X(T) \xrightarrow{\alpha} \mathrm{Im}(\alpha) = X(S)\ (\subset X(T')).$$

induces a surjection $k[T] \to k[S]$ of the coordinate rings and hence an injection

$$S \to T$$

such that the diagram of canonical maps

$$\begin{array}{ccc} T' & \subseteq & T \\ \downarrow & \nearrow & \\ S & & \end{array}$$

is commutative. But then, $T' \to S$ must be injective and $S \to T$ is the inverse of $T' \to S$, i.e. $T' \to S$ is an isomorphism.

QED.

Notes

6. Solvalble groups

This chapter deals with the structure theory of connected solvable linear algebraic groups, which is basic for the general theory.

6.1 Closed subgroups generated by irreducible subvarieties

G	algebraic group
$(f_i : X_i \to G)_{i \in I}$	a family of morphisms of algebraic varieties
Y_i	$= f_i(X_i)$
H	smallest closed subgroup of G containing all Y_i

Assume that, X_i is irreducible and $e \in Y_i$ for every $i \in I$. Then

(i) H is connected.

(ii) There are finite sequences $\{a(i) \mid i=1,...,n\}$ and $\{\varepsilon(i) \mid i=1,...,n\}$ such that $a(i) \in I$, $\varepsilon(i) \in \{+1,-1\}$ and

$$H = Y_{a(1)}^{\varepsilon(1)} \cdot Y_{a(2)}^{\varepsilon(2)} \cdot \ldots \cdot Y_{a(n)}^{\varepsilon(n)}.$$

Proof. We may assume the sets Y_i^{-1} occure among the sets Y_i and hence $\varepsilon(i) = 1$ for every i. Write

$$Y_a := Y_{a(1)} \cdot Y_{a(2)} \cdot \ldots \cdot Y_{a(n)} \quad \text{for } a = (a(1),a(2),...,a(n)) \in I^n.$$

Properties of Y_a and its closure $\bar{Y}_a$ in G:

Y_a is irreducible, for, it is the image of the irreducible variety

$$X_{a(1)} \times \ldots \times X_{a(n)}.$$

$\bar{Y}_a$ is irreducible, for, a decomposition of $\bar{Y}_a$ into closed subvarieties gives one for Y_a.

$Y_a \cdot Y_b = Y_{(a,b)}$ (by the very definition).

$\bar{Y}_a \cdot \bar{Y}_b \subseteq \bar{Y}_{(a,b)}$ (since multiplication is a morphism)

Choose some a such that dim Y_a is maximal. Then one has

$$\bar{Y}_a \subseteq \bar{Y}_a \cdot \bar{Y}_b \subseteq \bar{Y}_{(a,b)}$$

hence $\bar{Y}_a = \bar{Y}_{(a,b)}$ for every b, hence $\bar{Y}_b \subseteq \bar{Y}_a$ for every b. In particular:

$$\bar{Y}_a \cdot \bar{Y}_a \subseteq \bar{Y}_a .$$

This shows that $\bar{Y}_a$ is a closed subgroup of G. Since Y_a contains a non-empty open subset of its closure $\bar{Y}_a$ (this is true for the image of every morphism $f:X \to Y$ of algebraic varieties by Th. 1.9.5), we get $\bar{Y}_a = Y_a \cdot Y_a$ (by Lemma 2.2.3, $G=U \cdot V$ for dense open subsets U,V of an algebraic group G). This proves the claim.
QED.

6.2 Abstract groups generated by closed connected subgroups

G algebraic group
$(H_i)_{i \in I}$ family of closed connected subgroups

If G is generated as an abstract group by the groups H_i, then G is connected. Moreover, there is a finite sequence a(1),...,a(n) in I such that

$$G = H_{a(1)} \cdot \ldots \cdot H_{a(n)}$$

Proof. Immediate consequence of 6.1.
QED.

6.3 Commutator subgroups

Let G be a algebraic group. Given subgroups $H,K \subseteq G$ we define the commutator subgroup of H and K to be

(H,K) := subgroup generated by the the commutators $(x,y) := xyx^{-1}y^{-1}$, $x \in H, y \in K$

Note that if H and K are normal, then so ist (H,K) (since automorphisms map commutators into commutators). In particular (G,G) is a normal subgroup and G/(G,G) is abelian.

The higher commutator groups of G are inductively defined by

$$D^0G := G$$
$$D^{n+1}G := (D^nG, D^nG)$$

The group G is called solvable if $D^nG = \{e\}$ for some n.
Moreover, we define a sequence of normal subgroups by

$$C^0G := G$$
$$C^{n+1}G := (G, C^nG)$$

The group G is called nilpotent if $C^nG = \{e\}$ for some n, which means that all iterated commutators
$(x_1,(\ldots,(x_n,x_{n+1})\ldots)$ are equal to e.
The center Z(G) of G is defined to be

$$Z(G) := \{x \in G \mid (x,g) = e \text{ for every } g \in G\}$$

6.4 Commutator group of closed connected subgroups

G algebraic group
H,K closed subgroups
Suppose one of these subgroups is connected.
Then (H,K) is closed and connected.
Proof. Assume, for example, that H is connected. Consider the family of morphism

$$f_k: H \to G,\ h \mapsto khk^{-1},\ (k \in K)$$

Then 6.1 tells us that (H,K) is the smallest closed subgroup generated by the images of these morphisms. Moreover (H,K) is connected by **QED**.

6.5. The higher commutators and the center of a connected group

Let G be a connected algebraic group. Then

(i) The groups D^nG and C^nG are closed connected subgroups of G.
(ii) Z(G) is a closed subgroup.
(iii) If G is nilpotent and non-trivial, then $Z(G)^0$ is non-trivial.
Proof. (i) follows from 6.4.
(ii). Consider the family of morphisms

$$f_g: G \to G,\ x \mapsto (x,g),\ (g \in G).$$

Then Z(G) is by definition the intersection of the fibers $f_g^{-1}(e)$, hence it is closed.

(iii). Assume that G is nilpotent and non-trivial. Then there is some n such that $C^nG \neq \{e\}$ and $C^{n+1}G = \{e\}$. Then C^nG is connected, non-trivial and contained in the center.
QED

6.6 Exercises

(1) Connectedness of SO_n. Assume char $k \neq 2$. Let $V := k^n$ and define a symmetric bilinear form

$$(,): V \times V \to k$$

by

$$((x_1,\ldots,x_n), (y_1,\ldots,y_n)) := \sum_{i=1}^{n} x_i y_i .$$

Then O_n (see 2.1.3(4)) is the group of linear transformations $g \in GL_n$ such that $(gx, gy) = (x,y)$ for all $x,y \in V$.

If $x \in V$ satisfies $(x,x) = 1$ put

$$s_x y := y - (x,x)x.$$

This is a reflection, contained in O_n and one knows the reflections s_x generate O_n (see [25, p. 353]). Put

$$X := \{(x,y) \in V \times V \mid (x,x) = (y,y) = 1 \}.$$

This is an irreducible affine variety and

$$f: X \to SO_n, (x,y) \mapsto s_x s_y,$$

is a morphism of varieties.

(a) Deduce from 6.1 that SO_n is connected.

(b) Show that the condition $e \in Y_i$ of 6.1 cannot be omitted.

(2) Connectedness of Sp_{2n}. Let $V = k^{2n}$ and define an alternating bilinear form

$$(,): V \times V \to k$$

by

$$((x_1,\ldots,x_{2n}), (y_1,\ldots,y_{2n})) := \sum_{i=1}^{n} (x_i y_{n+i} - x_{n+i} y_i).$$

The group of linear transformations $g \in GL_{2n}$ such that $(gx,gy) = (x,y)$ for all $x,y \in V$ is the symplectic group Sp_{2n} (see 2.1.3(4)). One knows that Sp_{2n} is generated by the symplectic transvections $t_{x,a}: V \to V, y \mapsto y - a(x,y)x$,

($x \in V$, $a \in k$, see [25, p. 373]). Deduce from 6.1 that Sp_{2n} is connected.

(3) The dimension of the the normalizer. Let G be a connected nilpotent linear algebraic group and $H \subseteq G$ a proper connected closed subgroup. Show that

$$\dim H < \dim N_G H,$$

where $N_G H$ denotes the normaliser. In particular, if $\dim H = \dim G - 1$, then H is a normal subgroup (Hint: use 6.5 (ii)).

(4) Nilpotentness of U_n. The group $\mathbf{U}_n$ of unipotent upper triangular matrices is connected and nilpotent.

Lösungen

Zu (3)

First note that the subgroup $N_G H$ of G is closed, for

$$N_G H = \{g \in G \mid ghg^{-1} \in H \text{ for every } h \in H\} = \bigcap_{h \in H} f_h^{-1}(H)$$

where f_h denotes the morphism $f_h : G \to G$, $g \mapsto ghg^{-1}$.

Since G is nilpotent, there is some n such that $\mathbf{C}^n G \not\subseteq H$ and $\mathbf{C}^{n+1} G \subseteq H$. Then $\mathbf{C}^n G$ is a connected closed subgroup[94] (6.5(i)) of $N_G H$ not completely contained in H. Since $\mathbf{C}^n G$ is connected, it is even in the identity component $(N_G H)^0$, and the latter must be strictly greater than H. But then, $\dim H < \dim (N_G H)^0 \leq \dim N_G H$.

Zu (4)

To see that $\mathbf{U}_n$ is connected, let $N := \frac{n \cdot (n-1)}{2}$ and equip the set of matrices

$$X = \{A = (a_{ij}) \in \mathbf{M}_{n,n} \mid a_{ij} = 0 \text{ for } i \geq j\}$$

---

[94] Let $x \in \mathbf{C}^n G$. We have to show, $x \in N_G H$, i.e.

$$xHx^{-1} \subseteq H.$$

Let $h \in H$. Then $h^{-1}xhx^{-1} \in [H, \mathbf{C}^n G] \subseteq \mathbf{C}^{n+1} G \subseteq H$, i.e. there is some $h' \in H$ such that

$$h^{-1}xhx^{-1} = h'$$

hence $xhx^{-1} = hh' \in H$.

with the structure of an algebraic variety by identifying it with $\mathbf{A}^N$. Then

$$X \to \mathbf{U}_n, A \mapsto E+A$$

is a morphism of algebraic varieties which is obviously an isomorphism. Since $\mathbf{A}^N$ is irreducible, this shows that $\mathbf{U}_n$ is connected. We have yet to show that $\mathbf{U}_n$ is nilpotent.

Given an n×n matrix A define

d(A) = i if the i-th diagonal above the main diagonal is the first one containing a non-zero element. By convention d(E) = 0 and d(0) = n.

Then

$$\mathbf{U}_n^i := \{E+N \in \mathbf{U}_n \mid d(N) \geq i\}$$

is a subgroup of $\mathbf{U}_n$ for every i (since (E+N)(E+N') = E+N+N'+NN'). To prove that $\mathbf{U}_n$ is nilpotent, it is sufficient to show that

$$(\mathbf{U}_n, \mathbf{U}_n^i) \subseteq \mathbf{U}_n^{i+1}.$$

Let $E-N \in \mathbf{U}_n$ and $E-N' \in \mathbf{U}_n^i$ and write

$$(E-N)^{-1} = E+N+N^2+... = E+L \qquad (d(L) > 0)$$

$$(E-N')^{-1} = E+N'+N'^2+... = E+L' \qquad (d(L') \geq i)$$

Then one has modulo additive terms X with d(X)>i:

$$\begin{aligned}(E-N,E-N') &= (E-N)(E-N')(E-N)^{-1}(E-N')^{-1} \\ &\equiv (E-N-N')(E+L+L') \\ &\equiv E+L+L' - N - NL - N' \\ &\equiv E+L - N - NL \qquad \text{since } d(L'-N') > i \\ &\equiv E \qquad \text{since } L = N + NL\end{aligned}$$

This proves $(E-N,E-N') \in \mathbf{U}_n^{i+1}$, i.e., $\mathbf{U}_n$ is nilpotent.

6.7 Strukture of connected solvable groups (Lie-Kolchin)

Let $G \subseteq \mathbf{GL}_n$ be a connected solvable closed subgroup of $\mathbf{GL}_n$. Then some conjugate of G lies in the upper triangular matrices,

$$xGx^{-1} \subseteq \mathbf{T}_n .$$

Proof. Let $V := k^n$. Then G operates on V. It is sufficient to show that V contains a complete flag of invariant linear subspaces. For this it

suffices to show that there is a non-zero $v \in V$ which is a common eigenvector of all $g \in G$. We prove this by induction on the dimension

$$\dim G$$

starting with $G = \{e\}$.

The commutator subgroup $D^1G = (G,G)$ is a connected solvable closed subgroup (by 6.5(i)). Since it is a proper subgroup, it has smaller dimension. By induction we know there is a common eigenvector of the elements of (G,G). Write

$$V_\chi := \{v \in V \mid g \cdot v = \chi(g)v \text{ for } g \in (G,G)\}$$

for every rational character χ of (G,G). Then G permutes the distinct non-zero subspaces V_χ : for $g \in G$ and $h \in (G,G)$ one has

$$hgV_\chi = gh(h^{-1},g^{-1})V_\chi = g\chi(h(h^{-1},g^{-1}))V_\chi = \chi(g^{-1}hg)gV_\chi$$

hence $gV_\chi = gV_{\chi'}$, with $\chi'(x) = \chi(g^{-1}xg)$. The sum of the linear subspaces V_χ must be direct (since characters are linearly independent), hence there are only finitely many such subspaces. Let $\dim V_\chi = r$ and consider the action

$$G \times \mathbf{Grass}_r \to \mathbf{Grass}_r \quad (g,W) \mapsto gW.$$

The orbit of V_χ under this action consists of spaces $V_{\chi'}$, where χ' runs throught a set of characters of (G,G), hence is finite. Since G is connected, the orbit consists of one single element. This means the spaces V_χ are stable under G, $G \cdot V_\chi \subseteq V_\chi$. To find a comon eigenvector in V, we may assume

$$V = V_\chi$$

for some χ (replacing G by its image in $GL(V_\chi)$). Consider the action.

$$G \times V \to V, \quad (g,v) \mapsto gv.$$

The subgroup (G,G) acts on V by scalar multiplication. Commutators $(x,y) = xyx^{-1}y^{-1}$ always act via matrices with determinant 1. Hence (G,G) acts via scalar matrices with determinant 1. Thus (G,G) acts by finitely many matrices. Since (G,G) is connected, it must act trivially. Therefore (G,G) is trivial and G is commutative. But in the commutative case theorem 6.7 was already proved (see 2.4.2(i))[95] so that a common eigenvector exists in this case.

---

[95] G is conjugate to a set of diagonal matrices in this case.

QED.

6.8 Decompositon of connected nilpotent groups

Let G be a connected nilpotent linear algebraic group.

(i) The sets G_s, G_u of semi-simple and unipotent elements are closed connected subgroups, and G_s is a central torus of G.

(ii) The product map $\pi: G_s \times G_u \to G$ is an isomorphism of algebraic groups.

Proof. The fact that G_s is contained in the center was already proved (4.4.8)[96]. In particular, G_s is commutative. We may assume that $G \subseteq \mathbf{GL}_n$ is a closed subgroup. By (2.4.2)(ii)[97] there is a direct sum decomposition of $V := k^n$ such that G_s acts by scalar multiplication on each summand. As in the previous proof we see that G commutes these direct summands, hence (being connected) leaves them invariant[98]. By the previous theorem 6.7 we can triagonalize the action of G on each summand, i.e., we may assume

$$G \subseteq \mathbf{T}_n \,,\; G_s =^{99} G \cap \mathbf{D}_n \,.$$

In particular, G_s is closed in G. As one easily sees now, $G_u =^{100} G \cap \mathbf{U}_n$, hence G_u is closed.

---

[96] For connected nilpotent linear algebraic groups G_s is contained in the center.

[97] Any set of commuting semi-simple matrices in conjugate to a set of diagonal mtrices.

[98] One can see this here more directly: If $W \subseteq V$ is the eigenspace of the "haracter" $\chi: G_s \to k^*$ such that $hw = \chi(h)w$ for $h \in G_s$ and $w \in W$, then for every $g \in G$ one has

$$\begin{aligned} h(gw) &= (hg)w = (gh)w \quad (G_s \text{ is in the center of G}) \\ &= g(\chi(h)w) \\ &= \chi(h)gw \end{aligned}$$

Therefore $gW = W$ for every $g \in G$.

[99] An upper triangular matrix is semi-simple if and only if it is diagonal (otherwise it would have two different Jordan decompositions).

[100] An upper triangular matrix A is unipotent if and only if it is in U_n: if A is unipotent, then at least some conjugate SAS^{-1} is in U_n, i.e. $SAS^{-1} = Id + N$ with some upper triangular matrix N with zeros on the main diagonal. Then

$$A = Id + S^{-1}NS$$

and $S^{-1}NS$ is upper triangular and nilpotent (since A is unipotent). But then

$$S^{-1}NS$$

The map of (ii) is obviously a morphism. It is bijective by the uniqueness of the Jordan decomposition. We have yet to show that its inverse is a morphism too.
The map

$$G \to G_s,\ x \mapsto x_s,$$

is a morphism (being projection onto the diagonal matrices). Hence

$$x \mapsto (x_s, x x_s^{-1})$$

is also a morphism.
QED.

6.9 The unipotent part of a solvable connected group

Let G be a connected solvable linear algebraic group. Then:
(i) (G,G) is closed, unipotent, and connected.
(ii) The unipotent elments of G form a subgroup G_u which is closed nilpotent connected, and normal. The quotient G/G_u is a torus.

Proof. (i). By 6.7 we may assume that $G \subseteq \mathbf{T}_n$ is contained in the upper triangular matrices. Then (G,G) consists of upper triangular matrices such that all entries on the main diagonal are 1[101], i.e., (G,G) is unipotent. The fact that (G,G) is closed and connected was proved in (6.5)(i)[102].
(ii). Denoting by $\mathbf{U}_n$ the group of unipotent upper triangular matrices, one has

$$G_u = G \cap \mathbf{U}_n,$$

hence G_u is closed and normal.[103] Moreover, it is nilpotent, since $\mathbf{U}_n$ is nilpotent by exercise 6.6(4). Inclusion defines an injective homomorphism of algebraic groups

$$G/G_u \to \mathbf{T}_n/\mathbf{U}_n.$$

The group on the right is a torus, hence G/G_u is commutative with all elements being semi-simple. Consider G/G_u as a closed subgroup of

---

cannot have a non-zero element on the main diagonal, i.e., A is in U_n.

[101] The only eigenvalue, a commutator matrix A can have is 1. So Jordan decomposition A = Id + N with N upper triangular with zeros on the main diagonal, i.e. $A \in U_n$. Therefore, any group generated by matrices of this type must be contained in U_n.

[102] For G connected, D^nG and C^nG are closed connected subgroups.
[103] The conjugate of an unipotent element is unipotent.

some GL_N. By Lemma 2.4.2(ii)[104] we may assume that it is even contained in D_N. So G/G_u is a connected diagonalizable group, and hence a torus by (2.5.8).

We have yet to show that G_u is connected. The identity component G_u^0 is a closed normal subgroup of G. Replacing G by the quotient group G/G_u^0 we may assume that G_u is finite.

Since G_u is normal, G acts by conjugation on G_u. Since G is connected, the orbits under this action are connected. Since G_u is finite, this means all orbits consist of single elements. In other words,

$$G_u \subseteq Z(G)$$

is contained in the center. Since $(G,G) \subseteq G_u$, as we have seen above, this implies that G is nilpotent. But than G_u is connected by (6.8)(ii).

QED.

The assertion that follows is a lemma needed in the proof the structure theorem 6.11 for connected solvable groups.

6.10 Lemma: connected solvable groups contain some G_a in the center of their unipotent part

Let G be a linear algebraic group which is connected and solvable but not a torus. Then there is a closed normal subgroup $N \subseteq G$ such that

(i) $N \subseteq Z(G_u)$

(ii) $N \cong \mathbf{G}_a$ (the additive group)

Proof. By (6.9) the unipotent elements form a closed nilpotent connected normal subgroup G_u of G. Moreover, G_u is non-trivial, for otherwise G would be a torus by (6.9)(ii). By (6.5)(iii) G_u has a center with non-tivial identity component. Hence there exists a non-trivial connected closed normal subgroup H of G contained in

$$H \subseteq Z(G_u).$$

Note that, since G_u is normal in G, the same is true $Z(G_u)$, and hence for $Z(G_u)^0$. If char(k) = p > 0, we may additionally assume[105] that

---

[104] Sets of semi-simple commuting matrices are, up to conjugation, sets of diagonal matrices.

$$H^p = \{e\}.$$

By exercise (2.6.7)(1)[106], H is isomorphic to a vector group $(\mathbf{G}_a)^n$. If n = 1 we are done. Otherwise, let $V \subseteq k[H]$ be the subspace of additive functions ($f(hh')=f(h)+f(h')$, see 2.6). The torus $T = G/G_u$ operates on H via conjugation, hence it operates on k[H], stabilizing V. Since the action of T on k[H] is locally finite and since each rational represention of a torus decomposes into 1-dimensional ones (2.5.2)(iii), there is some $\alpha \in V$ such that $k\alpha \subseteq V$ is stable under the action of T. But then the identity component of $\mathrm{Ker}(\alpha) = \{h \in H \mid \alpha(h) = 0\}$ has dimension n-1 and is a subgroup which has the same properties as H. **QED**.

The notion of maximal Torus

The next theorem gives the most important facts about the internal structure of a connected solvable linear algebraic group G. A <u>maximal torus</u> of G is a subtorus of G which has the same dimension as the torus $S = G/G_u$. It will follow (see (6.12)(i)) that a maximal torus is also a maximal torus in the set-theoretical sense.

6. 11 The structure of connected solvable groups

Let G be a connected solvable linear algebraic group. Then

(i) Every semi-simple element $s \in G$ is contained in a maximal torus (in particular, a maximal torus exists).

(ii) The centraliser $Z_G(s)$ of every semi-simple element $s \in G$ is connected.

(iii) Any two maximal tori of G are conjugate.

(iv) If T is any maximal torus, the product map $\varphi: T \times G_u \to G$ is an isomorphism of varieties (not of groups).

Proof. (iv). Let the direct product $T \times G_u$ operate on G by

$$T \times G_u \times G \to G,\ (t,g,x) \mapsto txg^{-1}.$$

---

[105] By the theorem of Lie-Kolchin (6.7) we may assume that G consists of upper triangular matrices. Hence the elements of $H \subseteq G_u$ can be written A = E+N with N nilpotent. Hence for n large enough, $H^{p^n} = \{e\}$. Replacing H by H^{p^n} with n appropriate, we get a non-trivial group satisfying the above condition.

[106] Let G be a linear algebraic group which is connected, unipotent and commutative. If p>0 assume moreover that

$$G^p = \{e\}.$$

Show that G is isomorphic to a "vector group" $(\mathbf{G}_a)^n$.

The orbit of e is the $T \cdot G_u$, which is a subgroup (since G_u is normal by (6.9)(ii)). The isotropy group of e in $T \times G_u$ is trivial (for, $T \cap G_u = \{e\}$). Therefore, dim $\overline{T \cdot G_u}$ = dim T + dim G_u = dim G. Since every orbit is open in its closure (by (4.3.1)(i)) and $T \cdot G_u$ is a subgroup of G,

$$G = T \cdot G_u$$

by 2.2.4(ii), i.e., the product mophism

$$\varphi: T \times G_u \to G$$

is surjective. The tangent map induced by φ is

$$\mathrm{Lie}(T) \oplus \mathrm{Lie}(G_u) \to \mathrm{Lie}(G), (X,Y) \mapsto X+Y,$$

(see 3.3.11). Now the tangent vectors to T are semi-simple and the tangent vektors to G_u are nilpotent (see exercise (3.4.3)(1) and (2)), hence $\mathrm{Lie}(T) \cap \mathrm{Lie}(G_u) = 0$, i.e., the tangent map is injective, hence bijective. In other words, φ is an equivariant homomorphism of homogeneous spaces inducing isomorphisms on the tangent spaces. By (4.3.3)(iii), φ is an isomorphism. This proves (iv).

Next we prove the other assertions in case dim $G_u = 1$.

The case dim G_u = 1.

Since G_u is connected by (6.9)(iii), $G_u \cong \mathbf{G}_a$ (see 2.6.6). Fix some isomorphism

$$\phi: \mathbf{G}_a \to G_u$$

and let

$$\pi: G \to S := G/G_u$$

be the canonical homomorphism.
Since G_u is normal in G, G operates on G_u by conjugation

$$G \times G_u \to G_u , (g,x) \mapsto gxg^{-1}.$$

Since $G_u \cong \mathbf{G}_a$ is commutative, conjugation with elements from G_u induces the identity map on G_u, hence conjugation defines an operation of G/G_u on G_u

$$S \times G_u \to G_u , (gG_u,x) \mapsto gxg^{-1}, S := G/G_u.$$

Vía ϕ this gives an operation on the affine line $\mathbf{G}_a$ by group homomorphisms. Now the only group homomorphism on $\mathbf{G}_a$ are multiplication by constants (An automorphism $\mathbf{G}_a \to \mathbf{G}_a$ is given by a linear additive polynomial). In other words, there is a rational character $\alpha: G/G_u \to \mathbf{G}_m$ such that

(1) $$g\phi(x)g^{-1} = \phi(\alpha(\pi g)\cdot x),\ g\in G,\ x\in \mathbf{G}_a .$$

If $\alpha=1$ is constant, G acts trivially on G_u . But then G is commutative[107]. So all assertions follow from (2.4.12)[108] with $T = G_s$ being the only maximal torus of G (note that every torus consits of semi-simple elements and hence is contained in G_s).

So assume $\alpha\neq 1$. Let $s\in G$ be any semi-simple element and write

$$Z := \mathbf{Z}_G(s).$$

Then there is a direct sum decomposition

(2) $$\mathrm{Lie}(G) = (\mathrm{Ad}(s)-1)\mathrm{Lie}(G)\oplus \mathrm{Lie}(Z)$$

by (4.4.5)(ii). Since $S = G/G_u$ is commutative, $\pi(x) = \pi(gxg^{-1})$, hence

$$d\pi = d\pi\circ d\mathrm{Int}_s = d\pi\circ \mathrm{Ad}(s)$$

hence $d\pi\circ(\mathrm{Ad}(s)-1) = 0$, hence

(3) $$(\mathrm{Ad}(s)-1)\mathrm{Lie}(G) \subseteq \mathrm{Ker}(d\pi) = \mathrm{Lie}(G_u).$$

As for the identity on the right, note that the canonical homomorphism $\pi: G \to S := G/G_u$ is separable by (5.2.3)(ii) with

---

[107] By assumption, every $g\in G$ commutes with every $u\in G_u$. In particular, any two elements of G_u commutes and any semi-simple element $s\in G_s$ commutes with any element $u\in G_u$. In view of the Jordan decomposition, it is sufficient to show any two semi-simple elements s' and s" commute. Since G/G_u is commutative (by 6.9), one has at any case,

$$s's" = s"s'u \text{ for some } u\in G_u.$$

But then,

$$s' = s"s'us"^{-1} = s"s's"^{-1}u$$

and uniqueness of Jordan decomposition implies $s' = s"s's"^{-1}$ and $e = u$. Hence s' and s" commute.

[108] In the commutative case G decomposes into a direct product of closed subgroups $G = G_s \times G_u$.

fibers isomorphic to G_u, hence the differential $d\pi$ has kernel $\mathrm{Lie}(G_u)$. From these inclusions we see

$$\dim\ (\mathrm{Ad}(s)-1)\mathrm{Lie}(G) \leq 1$$

$$\dim\ Z^0 = \dim\ \mathrm{Lie}(Z) \geq \dim\ G - 1.$$

To prove that s is contained in some maximal torus we distinguish to cases.

1. Case: $\alpha(\pi s)\neq 1$. Note that there are semi-simple elements satisfying this condition: just take the semi-simple part of any $g\in G$ with $\alpha(\pi g)\neq 1$ (on the unipotent part of g, α is trivial). Then by (1),

(4) $$Z\cap G_u =^{109} \{e\}.$$

Therefore $Z^0\neq G$ and $\mathrm{Lie}(Z^0)\neq\mathrm{Lie}(G)$. Thus Z^0 is an (n-1)-dimensional closed connected solvable subgroup of G with trivial unipotent part. By (4), Z^0 maps injectively (hence bijectively) to the torus G/G_u, hence is a maximal torus. By assertion (iv) we have

$$G = Z^0 G_u\ .$$

If $g=xy$ ($x\in Z^0, y\in G_u$) commutes with s,[110] then y commutes with s, hence $y = e$,[111] hence $g=x\in Z^0$. Therefore,

$$Z = Z^0.$$

We have proved, the centralizer of a semi-simple element $s\in G$ with $\alpha(\pi s)\neq 1$ is a maximal torus, which proves assertions (i) and (ii) is this case.

2. Case: $\alpha(\pi s)=1$. From identity (1) we see that conjugation with s is a trivial operation on G_u hence $G_u\subseteq Z$ hence $\mathrm{Lie}(G_u)\subseteq\mathrm{Lie}(Z)$. From (3) we see that the direct sum decompositin of Lie(G) degenerates to

$$\mathrm{Lie}(G) = \mathrm{Lie}(Z).^{112}$$

---

[109] Assume there is some $u\in Z\cap G_u$ different from e. Then

$$u = \phi(x) \text{ with } x\in G_a - \{0\} = \mathbb{A}^1 - \{0\}.$$

Then

$$\begin{aligned}\phi(x) &= s\phi(x)s^{-1} \quad (\text{since } \phi(x) = u \in Z)\\ &= \phi(\alpha(s)x) \quad (\text{by } (1)).\end{aligned}$$

Since x is none-zero and ϕ is an isomorphism, $\alpha(s) = 1$ contradicting the choise of s.

[110] for $y\in G_u$ commutes with everything.

[111] by (4).

[112] One direct summand of the decomposition (2) is contained in the other.

Hence dim Z = dim G, hence Z = G, and s lies in the center of G. In particular, s lies in some maximal torus (e.g., in the centralizer of some element s' with $\alpha(\pi s') \neq 1$).

We have yet to prove assertion (iii) (in the case that dim $G_u = 1$). If T is any maximal torus, the projection π onto G/G_u induces a bijection

$$T \to G/G_u.^{113}$$

In particular, there is some $t \in T$ such that $\alpha(\pi t) \neq 1$. As we have seen above, this implies that $Z_G(t)$ is a maximal torus (containing T since T is commutative). Thus

$$T = Z_G(t).$$

Let T' be another maximal torus and choose $t' \in T'$ such that

$$T' = Z_G(t').$$

We may assume that t and t' map to the same element[114] of G/G_u, i.e., $t' = t \cdot \phi(x)$ for some $x \in \mathbf{G}_a$.

For arbitrary $y \in \mathbf{G}_a$ we have,

$$\begin{aligned} t\cdot\phi(x+(\alpha(\pi t'))^{-1}-1)y) &= t\cdot\phi(x+(\alpha(\pi t'))^{-1}y - y) \\ &= t\cdot\phi(x)\cdot\phi((\alpha(\pi t'))^{-1}y)\cdot\phi(y)^{-1} && (\phi \text{ is a group isomorphism}) \\ &= t\cdot\phi(x)\cdot t'^{-1}\cdot\phi(y)\cdot t'\cdot\phi(y)^{-1} && (\text{by formula (1)}) \\ &= t'\cdot t'^{-1}\cdot\phi(y)\cdot t'\cdot\phi(y)^{-1} && (\text{since } t' = t\cdot\phi(x)) \\ &= \phi(y)\cdot t'\cdot\phi(y)^{-1} \end{aligned}$$

Since $\alpha(\pi t') = \alpha(\pi t) \neq 1$, we may choose $y \in \mathbf{G}_a$ such that

$$x+(\alpha(\pi t'))^{-1}-1)y = 0,$$

i.e. such that

$$t = \phi(y)\cdot t'\cdot\phi(y)^{-1}.$$

But then, the centralizers of t and t' are conjugate,

$$T = \phi(y)\cdot T'\cdot\phi(y)^{-1}$$

as claimed.

General case.

---

[113] The map is surjective for dimensional reasons (and by the definition of maximal torus). It is injective by uniqueness of Jordan decomposition.

[114] The only condition on t and t' is that their images in G/G_u are not in the kernel of $\alpha: G/G_u \to G_m$.

Proof of (i). Assume dim $G_u > 1$. Let N be as in 6.10.[115] Write

$$\bar{G} := G/N.$$

Then $\bar{G}/\bar{G}_u \cong$[116] G/G_u. Let $s \in G$ be any semi-simple element and let $\bar{s}$ its image in $\bar{G}$. By induction on dim G we may assume that $\bar{s}$ is in a maximal torus $\bar{T}$ of $\bar{G}$. The inverse image of $\bar{T}$ in G is a connected[117] closed subgroup H of G. Since $\bar{T}$ consists of semi-simple elements, $H_u \subseteq N$, hence dim $H_u \leq 1$. By induction we know that s lies in a maximal torus T' of H, which is also a maximal torus of G, for,

$$\dim T' = \dim H/H_u \geq \dim H - 1 = \dim \bar{T} = \bar{G}/\bar{G}_u \cong G/G_u .$$

This proves (i).

Proof of (iii). Given two maximal tori $S,T \subseteq G$, let $\bar{S}$ and $\bar{T}$ their image in $\bar{G}$. Since S und T map bijectively to $\bar{S}$ and $\bar{T}$, respectively, the latter are maximal tori of $\bar{G}$, hence are conjugate by induction. Conjugating S

---

[115] i.e., N is a closed normal subgroup of G contained in $Z(G_u)$ and isomorphic to the additive group G_a.

[116] Consider the commutative diagram

$$\begin{array}{ccc} G & \xrightarrow{\beta} & \bar{G} \\ \downarrow & & \downarrow \\ G/G_u & \to & \bar{G}/\bar{G}_u \end{array}$$

where the verical homomorphisms and the upper horizontal one are surjective. Let $g \in G$ be such that $\beta(g)$ is unipotent. It will be sufficient to show that g is unipotent. Write

$$g = us$$

with u unipotent and s semi-simple. It will be sufficient to show that s = e. By assumption

$$\beta(g) = \beta(u)\beta(s)$$

is unipotent, hence $\beta(s) = e$, hence $s \in \mathrm{Ker}(\beta) = N \subseteq Z(G_u) \subseteq G_u$. Hence s is both, unipotent and semi-simple, i.e., s = e.

[117] Assume H isn't connected. Then at least one component of H maps surjectively to $\bar{T}$ (since the latter is irreducible). But then the fibers of the map $H \to \bar{T}$ cannot be irreducible, a contractiction.

with an appropriate element of G we may therefore assume that S and T have the same image in $\bar{G}$. For every $s \in S$ there are elements $t \in T$ and $n \in N$ such that $s = t \cdot h$. Uniqueness of Jordan decompositon implies $h = e$, hence $s = t$. This shows $S \subseteq T$, hence $S = T$.

Proof of (ii). Let $s \in G$ be semi-simple. Denote by $\bar{s}$ the image of s in $\bar{G}$ .Denote

$$G_1 := \{g \in G \mid sgs^{-1}g^{-1} \in N\}.$$

This is the inverse image of the centralizer of $\bar{s}$,

$$G_1 := \rho^{-1}(Z_{\bar{G}}(\bar{s})),\ \rho: G \to \bar{G} = G/N \text{ the natural map.}$$

Since $Z_{\bar{G}}(\bar{s})$ is connected by induction, G_1 is a closed connected subgroup of G such that

$$\mathbf{Z}_G(s) \subseteq G_1 \text{ and } G_1/N \cong \mathbf{Z}_{\bar{G}}(\bar{s}).$$

If G_1 is different from G, $\mathbf{Z}_G(s)$ is connected by induction hypothesis. So assume

$$G_1 = G.$$

Write $Z := \mathbf{Z}_G(s)$. As above we have a direct sum decomposition

$$\mathrm{Lie}(G) = (\mathrm{Ad}(s)-1)\mathrm{Lie}(G) \oplus \mathrm{Lie}(Z).$$

Let $\rho: G \to G/N$ denote the canonical map. From $G_1 = G$ we deduce that $G/N = \mathbf{Z}_{\bar{G}}(\bar{s})$, hence $\rho(x) = \rho(sxs^{-1})$ for every $x \in G$. Therefore

$$d\rho = d\rho \circ d\mathrm{Int}_s = d\rho \circ \mathrm{Ad}(s)$$

hence $d\rho \circ (\mathrm{Ad}(s)-1) = 0$, hence

$$(\mathrm{Ad}(s)-1)\mathrm{Lie}(G) \subseteq \mathrm{Ker}(d\rho) = \mathrm{Lie}(N). \tag{5}$$

If $(\mathrm{Ad}(s)-1)\mathrm{Lie}(G) = 0$, one has $\mathrm{Lie}(G) = \mathrm{Lie}(Z)$, hence $\dim Z^0 = \dim G$, hence $Z^0 = G$, hence $Z = G$ is connected.
Thus assume

$$(\mathrm{Ad}(s)-1)\mathrm{Lie}(G) = \mathrm{Lie}(N).$$

Then $\dim Z = \dim G - 1$ and

$$Z^0 \cap N = \{e\}$$

(consider the action of G/N on N and use a relation like (1))[118]. Hence the product map

$$Z^0 \times N \to G$$

is bijective, which implies (as above) $Z = Z^0$, i.e., Z is connected. This completes the proof of the theorem.
QED.

6.12 Non-maximal tori of connected solvable groups

Let G be a connected solvable linear algebraic group and $H \subseteq G$ a subgroup all of whose elements are semi-simple. Then

(i) H lies in a maximal torus of G. In particular, any subtorus of G lies in a maximal torus.

(ii) The centralizer $\mathbf{Z}_G H$ is connected and coincides with the normalizer $\mathbf{N}_G H$.

Proof. If $s \in G$ is semi-simple and contained in the center Z(G) of G, it lies in all maximal tori of G (by 6.11(i) and (iii)). Therefore (i) is true in case $H \subseteq Z(G)$. The second assertion (ii) is trivially true in this case.

If H is not contained in Z(G), choose any $s \in H - Z(G)$. Then the centralizer

$$Z_G(s) \subset G$$

is a proper connected (see 6.11(ii)) subgroup of G.

---

[118] First note that conjugation by s is none-trivial map on N, for otherwise one would have

$$N \subseteq Z_G(s) = Z$$

hence

$$L(N) \subseteq L(Z).$$

Thus by (5) the decomposition (2) degenerates to

$$L(G) = L(Z)$$

and (Ad(s)-1)Lie(G) = 0 contrary to our assumption that (Ad(s)-1)Lie(G) = L(N). So, indeed, the action of s on $N \cong G_a$ by conjugation is none-trivial. Denoting by

$$\phi: G_a \to N$$

an Isomorphism, on has

$$s\phi(x)s^{-1} = \phi(\alpha(s)x) \text{ for every } x \in N$$

with $\alpha: G/N \to G_m$ some character and $\alpha(s) \in k$ different from 1. If there were some

$$u \in Z^0 \cap N$$

different from e, then

$$u = \phi(x),\ x \in G_a - \{0\},$$

and

$$\phi(x) = s\,\phi(x)s^{-1} \quad (\text{since } \phi(x) = u \in Z^0)$$
$$= \phi(\alpha(s)x)$$

hence $x = \alpha(s)x$, hence $\alpha(s) = 1$ contrary to the choise of $\alpha(s)$.

Since H maps injectively under

$$G \to G/G_u ,$$

the groups H is commutative. So $H \subseteq \mathbf{Z}_G(s)$. The claim of (i) follows by induction on dim G. The same argument[119] shows that $\mathbf{Z}_G H$ is connected.

Finally let $x \in \mathbf{N}_G H$. Then for all $h \in H$ we have

$$xhx^{-1}h^{-1} \in H \cap (G,G) \subseteq H \cap G_u = \{e\}$$

(use 6.9(i)), i.e., $x \in \mathbf{Z}_G H$, hence $\mathbf{Z}_G H = \mathbf{N}_G H$.

QED.

6.13 Regular functions on homogeneous of connected solvable groups

Let G be a connected solvable linear algebraic group and $H \subseteq G$ a proper closed subgroup of G. Then there exists a non-constant regular function on the variety G/H.

Proof. We use induction on dim G + dim G/H. This integer is at least 2.

1. Step: the case dim G + dim G/H = 2.

Then

$$\dim G = \dim G/H = 1.$$

Inparticular, G is isomorphic to $\mathbf{G}_m$ or $\mathbf{G}_a$ hence abelian. So H is a normal subgroup and G/H is affine by (5.2.5)(i). The claim is triavially true in this case.

2. Step: the case $G_u = \{e\}$.

Then G is abelian by (6.9)(ii), G/H is affine for the same reason, and the claim is trivially true again.

3. Step: the case $G_u \neq \{e\}$.

Let $N \subseteq Z(G_u)$ be a closed connected normal subgroup of G isomorphic to G_a as in 6.10. Then HN is a closed subgroup. If it is different from G, then by induction hypothesis there is a non-constant regular function on G/HN. Using the canonical map $G/H \to G/HN$ we get a non-constant regular function on G/H. Hence assume that

---

[119] In case $H \subseteq Z(G)$, the centralizer $Z_G(H) = G$ is trivially connected. If H is not contained in Z(G), take some $s \in H - Z(G)$. Then

$$H \subseteq Z_G(s) = \text{proper closed connected subgroup of G,}$$

and the claim follows by induction on dim G.

$$HN = G.$$

Then $(H^0)_u$ is a normal subgroup of G (for, it is invariant under both H and N, hence under G). Moreover,

$$(*) \qquad G/H = (G/(H^0)_u)/H/(H^0)_u.$$

If $(H^0)_u$ is non-trivial, the claim follows by induction again. So assume

$$(H^0)_u = \{e\}.$$

Then $T:=H^0$ is a torus, hence is contained in a maximal torus of G (by 6.12). Now

$$\dim T = \dim H \geq \dim HN - 1 = \dim G - 1$$

(note that dim N = 1), and T maps injectively into G/G_u. Therefore

$$\dim G_u = 1$$

and $N = G_u$ hence

$$G/H = HN/H = N/N\cap H = G_u/H_u.$$

This reduces the proof to the first step (since dim G_u = 1).

QED.

6.14 Reductive groups

Let G be an arbitrary linear algebraic group. Consider the family of all

closed, connected, solvable, normal

subgroups. The group generated by all these groups is a group of the same kind[120]. Hence there is a maximal closed, connected, solvable, normal subgroup. It is denoted

$$\mathbf{R}G$$

and called the radical of G. Similarly, there is a maximal closed, connected, unipotent, normal subgroup[121] of G denoted

$$\mathbf{R}_u G$$

and called unipotent radical of G. These two are related[122] by

---

[120] Let A,B be closed connected solvable normal subgroups. Then AB is a normal subgroup hence is closed and connected by 6.1. Moreover there is a short exact sequence

$$1 \to A \to AB \to AB/A \to 1$$

with the outer groups being solvable, hence the group in the middle is solvable, too.

[121] Any two closed connected unipotent normal subgroups A,B are contained in G_u hence so is AB.

[122] $\mathbf{R}_u G$ can be considered as a subgroup of some $\mathbf{U}_n$ (by 2.4.11), hence is nilpotent by Exercise (6.6)(4) hence resolvable. Therefore $\mathbf{R}_u G \subseteq \mathbf{R}G$.

$$(\mathbf{R}G)_u = \mathbf{R}_u G.$$

The group is called <u>semi-simple</u> if $\mathbf{R}G = \{e\}$ and <u>reductive</u> if $\mathbf{R}_u G = \{e\}$.

6.15 The radical of a connected reductive group

Let G be a connected, reductive linear algebraic group. Then $\mathbf{R}G$ is a torus. It coincides with the identity component of the center $\mathbf{Z}G$,

$$\mathbf{R}G = (\mathbf{Z}G)^0$$

Moreover

$$\mathbf{R}G \cap (G,G)$$

is finite.

Proof. Since $(\mathbf{R}G)_u = \mathbf{R}_u G = \{e\}$, we have that $T := \mathbf{R}G$ is a torus by (6.9)(ii). Normalizer and centralizer of the diagonlizable subgroup T have the same identity component by (2.5.11)[123],

$$G = (\mathbf{N}_G T)^0 = (\mathbf{Z}_G T)^0,$$

i.e., T lies in the center of G, i.e.,

$$T \subseteq (\mathbf{Z}G)^0.$$

Since $(\mathbf{R}G)_u = \{e\}$, $(\mathbf{Z}G)^0_u = \{e\}$. As a commutative group consisting of semi-simple elements $(\mathbf{Z}G)^0$ is diagonalizable by (2.4.2)(ii). Being connected it is even a torus by (2.5.8). Since it is closed, connected, solvable and normal, it is contained in $T := \mathbf{R}G$. We have proved

$$T = (\mathbf{Z}G)^0.$$

To prove the last statement, assume G to be a closed subgroup of $\mathbf{GL}(V)$. Decompose V into a direct sum $\oplus V_\chi$ such that $t \in T$ acts as scalar multiplication by $\chi(t)$ on V_χ, the χ's being pairwise distinct rational characters of T. Then $G \subseteq Z_{\mathbf{GL}(V)}(T)$ permutes hence stabilizes all V_χ and (G,G) is contained in $\prod_\chi \mathbf{SL}(V_\chi)$, i.e., the elements of

$$\mathbf{R}G \cap (G,G) = T \cap (G,G)$$

are direct sums of scalar matrices with determinant 1. Hence this set is finite.

Consequently $\mathbf{R}_u G \subseteq (\mathbf{R}G)_u$. By 6.9 the group $(\mathbf{R}G)_u$ is closed connected unipotent and normal. Since $\mathbf{R}_u G$ is maximal with respect to these properties, $\mathbf{R}_u G = (\mathbf{R}G)_u$.

[123] For every diagonalizable subgroup $H \subseteq G$ of a linear algebraic group, $N_G(H)$ and $Z_G(H)$ have the same identity component.

QED.

6.16 Exercises

(1) Give an example of a finite solvable subgroup of $\mathbf{GL}_2(\mathbb{C})$ which is not conjugate to a group of triangular matrices (this shows that the connectedness assumption in Kolchin's theorem (6.7) is essential).

In the exercises that follow, G is a connected solvable linear algebraic group.

(2) Let H be a closed connected nilpotent subgroup of G which is equal to its normalizer. Show that H is the centralizer of a maximal torus of G. (Hint: By 6.8 we have $H = H_s \times H_u$. Show that $H = Z(H_s)$ and use 6.12(i) to prove that H_s is a maximal Thurs).

(3) There is a sequence $G = G_n \supseteq G_{n-1} \supseteq \ldots \supseteq G_1 \supseteq G_0 = \{e\}$ of closed connected normal subgroups of G sucht that all quotient groups G_i/G_{i-1} are either isomorphic to $\mathbf{G}_a$ or $\mathbf{G}_m$.

(4) Let H be a closed subgroup of G such that dim G/H = 1. Then G/H is either isomorphic to $\mathbf{G}_a$ or to $\mathbf{G}_m$ (as a variety). (Hint: use 6.10).

Solutions

(1) Let $H \subseteq GL_2(\mathbb{R}) \subseteq \mathbf{GL}_2(\mathbb{C})$ the symmetry group of the regular hexagon consisting of 6 rotations and 6 reflections. The rotations form a commutative normal subgroup and the corresponding factor group has order 2, hence is commutative. Therefore, H is solvable.

Assume that H would be conjugate to a subgroup $H' := gHg^{-1}$ of upper triangular matrices. Then H' contains 6 elements of order 2 (the 6 reflections). Each is of the form

$$A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix},\ A^2 = \mathrm{Id},\ \det A = -1$$

i.e., with

$$a^2 = d^2 = 1,\ ab+bd = 0,\ ad = -1.$$

The only solutions of this system are

$a = 1,\ d = -1,\ b$ arbitrary

$a = -1,\ d = 1,\ b$ arbitrary

The second group of solutions differs only by sign from the first. Now

$$\begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+b' \\ 0 & 1 \end{pmatrix},$$

i.e., all these elements commute with each other. But this is not the case with the 6 reflections of H.

(2) By assumption

(+) $$H = N_G(H) = N_G(H_s \times H_u) \quad \text{(see 6.8)}$$
$$= N_G(H_s) \cap N_G(H_u)$$

Taking unipotent parts on both sides we see,

(*) $$H_u = G_u \cap N_{G_u}(H_u) = N_{G_u}(H_u)$$

Note that, since H_s is a central torus (by 6.8), $G_u \subseteq N_G(H_s)$. Since G_u is nilpotent, there is some i such that

$$C^i(G_u) \subseteq H_s \text{ and } C^{i-1}(G_u) \not\subseteq H_s$$

(exept in case $H_u = G_u$). But then for $g \in C^{i-1}(G_u)$ and $h \in H_s$,

$$ghg^{-1}h^{-1} \in C^i(G_u) \subseteq H_s$$

hence $ghg^{-1} \in H_s$, i.e., each element $g \in C^{i-1}(G_u)$ is in $N_{G_u}(H_s)$. But then $N_{G_u}(H_u)$ is strictly larger than H_u in contradiction with (*). This proves

$$H_u = G_u .$$

Since G_u is normal in G, $N_G(H_u) = N_G(G_u) = G$ and identity (+) reads

$$H = N_G(H_s) = Z_G(H_s)$$

For the second equality sign see 6.12(ii). The proof is complete if we can show that H_s is a maximal torus. By 6.12(i) H_s is contained in a maximal torus of G, say

$$H_s \subseteq T.$$

Since T is commutative,

$$H = Z_G(H_s) \supseteq T.$$

Since T consists of semi-simple elements, $T \subseteq H_s$. Therefore,

$$H_s = T.$$

(3) Since G is solvable there is at least such a sequence with the factors being abelian (by 6.5). This reduces the proof the case that G is abelian. But then G is the direct Product of a torus and

a connected unipotent group (by 2.4.12). But then the claim follows from previously proved results. Note, in particular that by 6.5 a connected nilpotent none-trivial G has a none-trivial $Z(G)^0$.

(4) By 6.10 there is a closed normal subgroup $N \subseteq G$ such that

$$N \subseteq Z(G_u) \text{ and } N \cong G_a.$$

Consider the restriction

$$\phi: N \to G/H$$

of the natural map. The image of ϕ is 1-dimensional or 0-dimensional. In the second case Im ϕ is finite, hence equal to {e} (since N is connected), i.e., $N \subseteq H$ and

$$G/H = (G/N)/(H/N)$$

and the claim follows by induction on dim H. So assume we are in the first case. Then ϕ is surjective and G/H is a homogeneous space such that the stabilizer of H is finite,

$$N_H = N \cap H = \text{finite}.$$

Since N is commutative, $N \cap H$ is normal in N and

$$N/N \cap H \cong G/H$$

is affine the coordinate ring being

$$k[G/H] = k[N]^{N \cap H} = k[T]^{N \cap H}$$

where $N \cap H$ can be considered as a finite Group of automorphisms of the polynomial ring k[T], i.e., $N \cap H$ operates on k[T] via translation,

$$T \mapsto T + g, \; g \in N \cap H \subseteq N = k.$$

It will be sufficient to show that $k[T]^{N \cap H}$ is isomorphic to k[T]. Since $N \cap H$ is finite, each $g \in N \cap H$ has finite order, i.e. either char k = 0 and $N \cap H$ is trivial or g is a fraction of the characteristics. So it is sufficient to show that the invariants of k[T] under the translations of type

$$T \mapsto T + p/n$$

form a ring isomorph to k[T]. But this ring is just

$$k[f] \text{ with } f = \prod_{i=0}^{n-1} (T - i \diamond p/n).$$

Notes

The first results of this chapter give standard elementary material. 6.3 is also true if H and K are closed subgroups (not nessarily connected), such that H normalizes K (see [3], p. 108).
The proof of the main result 6.11 is somewhat different from the usual one, which is due to Borel ([2], §12, see also [3], p. 244). We have exploited here the auxiliary result 6.10.
6.13 is rather a weak result. As a matter of fact, in that case the quotient G/H is an affine variety (see [5], 9.13).

Notes

7. Complete varieties. Borel subgroups, parabolic subgroups and their properties

7.1 Vollständige Varietäten

An algebraic variety X is said complete if the following holds: for any variety Y, the projection morphism $X\times Y\to Y$ is closed, i.e., maps closed sets onto closed sets. The example in 1.91 shows that the affine line $\mathbb{A}^1$ is not complete. One should view the notion of completeness as an analogue, in the category of algebraic varieties, of the notion of compactness in the category of locally compact topological spaces (see exercise 7.1.5(1)).

7.1.1 Properties of complete varieties

Let X be a complete variety.
(i) A closed subvariety of x is complete.
(ii) If Y is a complete variety, then so is $X\times Y$.
(iii) If $\phi: X\to Y$ is a morphism of varieties, then ϕX is closed and complete.
(iv) If X is a subvariety of a the variety Y then X is closed in Y.
(v) If X is irreducible then any regular function on X is constant.
(vi) If X is affine, then X is finite.

Proof. (i) and (ii) follow immediately from the definition of completeness.
(iii). Let

$$\Gamma := \{(x,\phi(x)) \mid x\in X\}$$

be the graph of ϕ. Note that Γ is the inverse image of the diagonal $\Delta\subseteq Y\times Y$ under the morphism

$$X\times Y \to Y\times Y,\ (x,y) \mapsto (\phi x,y),$$

i.e., Γ is closed in $X\times Y$. Since ϕX is the projection of Γ onto Y, and X is complete, this projection is closed. To prove that ϕX is complete, let Z be any variety. We have to prove that the projection $\phi X\times Z\to Z$ is a

closed map. Since Γ maps surjectively onto ϕX, it will be sufficient to show that the projection

$$\Gamma \times Z \to Z$$

is closed. But this follows from the fact that Γ is isomorphic to X, hence is complete.

(iv). This is a special case of (iii) with $\phi: X \to Y$ being the natural injection.

(v). Let f be a regular function on X and consider it as a morphism

$$f: X \to \mathbb{A}^1 \subseteq \mathbb{P}^1$$

If f in non-constant, than fX is a non-empty dense subset of $\mathbb{P}^1$. Since X is complete fX must be closed in $\mathbb{P}^1$, hence $fX = \mathbb{P}^1$, which is impossible. Thus f must be constant.

(iv). Let $X \subseteq \mathbb{A}^n$ be affine. By (v) the coordinate functions on X must be constant on each irreducible component of X, hence X consists of a finite number of points.

QED.

7.1.2 Completeness of projective varieties

A projective variety is complete.

Proof(Shafarevich). It suffices to prove that projective n-space $\mathbb{P}^n$ is complete. So we have to prove the projection morphism

$$\pi: \mathbb{P}^n \times Y \to Y$$

is closed for all varieties Y. Since Y has an open cover by affine subvarieties, we may assume that Y is affine. Since Y is contained in some $\mathbb{A}^m$ we may assume that $Y = \mathbb{A}^m$. Therefore all be have to prove ist that the projection morphism

$$\pi: \mathbb{P}^n \times \mathbb{A}^m \to \mathbb{A}^m$$

is closed.

A closed subset in $\mathbb{P}^n \times \mathbb{A}^m$ is given by a set of polynomial equations

$$(*) \qquad g_i(x,y) = 0 \quad (i=1,\ldots,r,\ x \in \mathbb{P}^n,\ y \in \mathbb{A}^m),$$

which are homogeneous with respect to $x = (x_0,\ldots,x_n)$. We have to show the set of points $y \in \mathbb{A}^m$ such that (*) has a solution x is closed. Denote by $(x)^i$ the set of power products of degree i of $x_0,\ldots,x_n$. By Hilbert's Nullstellensatz, (*) has a solution if and only if the ideal

$$\langle g_i(x,y) \mid i=1,\ldots,r \rangle$$

generated by the polynomials $g_i(x,y)$ doesn't contain any $(x)^i$ as a subset. Write

$$T_i := \{y \in \mathbb{A}^m \mid (x)^i \text{ is not contained in } \langle g_i(x,y) \mid i=1,...,r\rangle\}.$$

We have to show the intersection $\cap T_i$ is closed in $\mathbb{A}^m$. Obviously

$$T_i \supseteq T_{i+1} .$$

Hence it will be sufficient to showt that T_i is closed for every sufficiently large i. Fix some i greater than the degree of any g_i (with respect to x). To prove that T_i is closed replace g_j by the set of all products of g_j with all elements from $(x)^{i-\deg g_j}$ (this doesn't change the degree i part of the ideal generated by the g_j's). Thus we may assume that each g_j has degree i. Now consider the polynomials g_j as vectors in the space of homogeneous polynomials of degree i with coordinates depending in a polynomial way upon $y \in \mathbb{A}^m$.

Then the condition

$$(x)^i \subseteq \langle g_i(x,y) \mid i=1,...,r\rangle$$

means that the set $\{g_i(x,y)\}$ contains a basis of this vector space, a condition that can be expressed by saying that certain determinants are non-zero. In particular this is an open condition on y, i.e., $\mathbb{A}^m - T_i$ is open. But then T_i is closed.

QED.

7.1.3 Complete algebraic groups are commutative

Let G be a connected algebraic group which is complete. Then X is commutative.

Complete algebraic groups are called abelian varieties. An example are the elliptic curves. For the theory of abelian varieties we refer to Mumford [29].

To prove the claim we need

7.1.4 A rigitity result

Let X,Y,Z be irreducible varieties with X complete. Let

$$\varphi: X \times Y \to Z$$

be a morphism and write $\varphi_y(x) := \varphi(x,y)$. Assume that there is some $a \in Y$ such that φ_a is constant. Then φ_y is constant for every $y \in Y$.

Proof of 7.1.3. Let with $X := Y := Z := G$ and $\varphi(x,y) := xyx^{-1}$. Then $\varphi(x,e)$ is constant as a function of x. By 7.1.4 $\varphi(x,y)$ is constant as a function of x for every y. In particular

$$\varphi(x,y) = \varphi(e,y) = y$$

for every x and every y. But then G is commutative.
QED.

Proof of 7.1.4. Let Γ be the graph of φ,

$$\Gamma := \{(x,y,\varphi(x,y)) \mid x \in X, y \in Y\}.$$

In particular, Γ is closed in $X \times Y \times Z$. Since X is complete, the subset

$$A := \{(y,\varphi(x,y)) \mid x \in X, y \in Y\}$$

of $Y \times Z$ is closed. As the image of an irreducible set is also irreducible. Consider the projection

$$\pi: A \to Y.$$

By assumption, $\pi^{-1}(a)$ consists of one single point. Hence dim A = dim Y. For $x \in X$ the subset

$$A_x := \{(y,\varphi(x,y)) \mid y \in Y\}$$

of A is closed (since it is the graph of a morphism $Y \to Z$) and is isomorphic to Y. Hence it is irreducible and its dimension is equal to dim Y = dim A. Therefore

$$A_x = A$$

for every x. But the $\varphi_y(x) := \varphi(x,y)$ is constant for every $y \in Y$.

QED.

7.1.5 Exercises

(1) Let X be a locally compact Hausdorff space. Show that X is compact if and only if for any locally compact space Y the projection map $X \times Y \to Y$ is closed.
Hint: in the proof of the if part use a one point compactification of a non-compact X.

(2) (a) Let G be a connected algebraic group and H a closed connected, complete subgroup. Then H lies in the center of G.
(b) Let G be a connected algebraic group. There exists a maximal closed, connected complete subgroup of G. It lies in the center of G.

Solutions

(1) Let $\bar{X} := X \cup \{\infty\}$ be such that the open neighbourhoods of ∞ are the complements of compact subsets of X. Suppose

$$X \times Y \to Y \text{ is closed}$$

for every locally compact Y. Inparticular, $X \times \bar{X} \to \bar{X}$ is closed.Since X is Hausdorff, the diagonal Δ is closed in $X \times \bar{X}$. Projecting to the second factor, we see that X is closed in $\bar{X}$, hence $\{\infty\}$ is a neighbourhood of ∞, hence the closed subset

$$X = \bar{X} - \{\infty\}$$

of $\bar{X}$ is compact.
Conversely, assume that X is compact. Let Y be locally compact, $F \subseteq X \times Y$ be a closed subset and F' be its image under the projection $X \times Y \to Y$. Assume that there F' isn't closed, i.e., Y-F' isn't open. Then there is a point $y \in Y$ such that every neighbourhood U of y has points in common with F'. We can choose U such that the closure $\bar{U}$ of U is compact. Replacing Y by $\bar{U}$ we may assume that Y is compact. But then $X \times Y$ is compact, F is compact, hence so is F'. But than F' is closed.

(2) (a). Consider the morphism $\varphi: H \times G \to G$, $(h,g) \mapsto hgh^{-1}$. Then $\varphi(h,e)$ is constant as a function of h. But then by 7.1.3 $\varphi(h,g)$ is a constant function of h for every $g \in G$. In particular,

$$hgh^{-1} = \varphi(h,g) = \varphi(e,g) = g$$

for arbitrary $h \in H$, $g \in G$, i.e., H is in the center of G, as claimed.
(b). Let $X, Y \subseteq G$ be two closed, connected, complete subgroups. By (a) both X and Y are in the center of G, hence are normal subgroups. But then XY is a subgroup which is connected by 6.1 and complete 7.1.1. This shows there is a maximal one in the set of all closed, connected, complete subgroups of G.

7.2 Parabolische Untergruppen und Borel-Untergruppen einer linearen algebraischen Gruppe

Convention

G denotes a linear algebraic group.

7.2.1 Completeness of homogeneous spaces

Let G be a linear algebraic group and X, Y be homogeneous spaces. Assume there is a bijective G-morphism $\varphi: X \to Y$.

Then X is complete if and only if Y is so.

Proof. From 4.3.3 we know that the induced map

$$X\times Z\to Y\times Z$$

is open for every variety Y, hence is a homeomorphism of topological spaces. From this fact the claim is obvious.

QED.

Parabolic subgroups

Let G be a linear algebraic group. A closed subgroup $P\subseteq G$ is called a parabolic subgroup if the quotient variety G/P is complete.

Remark. $P\subseteq G$ is parabolic if and only if $P\cap G^0$ is parabolic in G^0.

Proof. "$\Rightarrow$" is trivial, and the converse implication follows from the fact the the components of an algebraic group are isomorphic as varieties.

QED.

7.2.2 Existence of parabolic subgroups

Let G be a connected linear algebraic group. Then the following are equivalent.

(i) There is a proper parabolic subgroup of G.

(ii) G is non-solvable.

Proof. (ii)$\Rightarrow$(i). We may assume that G is closed in some $\mathbf{GL}(V)$. Then G operates on the projective space $\mathbb{P}(V)$ and by 4.3.1(ii) there is a closed orbit X for this action. By 7.1.2 this orbit X is a complete homogeneous space for G. Let $x\in X$ be any point and let

$$P := G_x := \{g\in G \mid gx = x\}$$

be the isotropy subgroup of x in G. Then

$$G/P \to X,\ gP \mapsto gx,$$

is a bijective G-morphism of homogeneous spaces. Inparticular, G/P is complete (by 7.2.1) and P is a parabolic subgroup of G.

It is a proper one if dim X>0. If dim X = 0, then X = {x}. Let $v\in V$ any point on the line x and let

$$V_1 := V/kv.$$

Then G operates on V_1 and we can find a closed orbit in $\mathbb{P}(V_1)$. Continuing this way one either finds a complete homogeneous space of positive dimension (hence a proper parabolic subgroup) or G is isomorphic to a subgroup of a group of triangular matrices, hence is solvable. This proves the implication

G has no proper parabolic subgroup $\Rightarrow$ G is solvable.

If G is solvable, then there is a non-constant function of G/P by 6.13 of every proper closed subgroup P⊆G. But then P cannot be parabolic. **QED**.

7.2.3 Projectivity of factors modulo parabolic subgroups Let G be linear algebraic group and P ⊆ G a parabolic subgroup. Then G/P is a projective variety.

Proof. By 5.2.3 G/P is quasi-projective, i.e., an open subvariety of a projective variety. Since G/P is complete, it must be closed in this projective variety, hence itself projective.
QED.

7.2.4 Transitivity of the property to be parabolic Let P and Q be closed subgroups of G with P⊆Q. If P ⊆ Q and Q ⊆ G are parabolic then so is P ⊆ G.

Proof. We have to show that for any variety X, the projection G/P×X→X is closed. Since the natural morphism G→G/P is an equivariant morphism of homogeneous spaces, the induced map G×X→G/P×X is open by 4.3.3(i). Hence closed subsets of G/P×X are in 1-1 correspondence to closed subsets A⊆G×X satisfying

$$(g,x)\in A \Rightarrow gP\times\{x\} \subseteq A.$$

We have to show, closed sets of this type map onto closed subsets of X.[124]

Consider the morphism

$$\alpha\colon Q\times G\times X\to G\times X,\ (q,g,x)\ a\ (gq,x).$$

If A is as above, then

$$\alpha^{-1}A = \{(q,g,x) \mid (gq,x)\in A\},$$

which is closed in Q×G×X.[125] The completeness of Q/P implies that the projection of $\alpha^{-1}A$ onto G×X is closed in G×X, i.e., the set

$$\bigcup_{(g,x)\in A} gQ\times\{x\}$$

is closed in G×X.[126] The completeness of G/Q implies that the projection onto X of the last set is closed in X. But this is just the image of A in X.
QED.

---

[124] Roughly speaking, projectivity of G/P means that the projections

$$G\times X \to X$$

map closed P-invariant sets into closed sets. This will be applied now for differnt G and P.

[125] And it is P-invariant in the sense of previous footnote with respect to the first factor.

[126] And it is Q-invariant with respect to the first factor G.

7.2.5 Borel's fixed point theorem

Let G be a connected solvable linear algebraic group and X a complete G-space. Then there is a point $x \in X$ which is fixed by all elements of G.

Proof.By (4.3.1)(ii) there is a closed orbit Y for the action of G on X. Let $y \in Y$ and

$$P := G_y$$

be the isotropy group of x in G. Then there is a bijection $G/P \to Y$ of homogeneous spaces, i.e. P is a parabolic subgroup. Since G is solvable, P = G by 7.2.2, whence the orbit Y consists of a single point. This proves the claim.

QED.

Borel subgroups

Let G be a linear algebraic group. A Borel subgroup of G is a connected, solvable, closed subgroup which is maximal with respect to these properties. A maximal torus of G is a closed subtorus of G of maximal dimension. This last notion occured already in 6.11 in the case that G is connected and solvable.

7.2.6 First Properies of Borel subgroups

Let G be a linear algebraic group.

(i) A closed subgroup of G is parabolic if and only if it contains a Borel subgroup.

(ii) If B is a Borel subgroup of G then G/B is complete.

(iii) All Borel subgroups of G are conjugate.

(iv) All maximal tori of G are conjugate.

Proof. We may assume that G is connected.

(i). Let B be a Borel subgroup of G and P any parabolic subgroup. Then the connected solvable group B acts on the projective variety G/P (by left translations). By Borel's fixed point theorem there is some $x \in G$ such that BxP = xP. In particular,

$$x^{-1}Bx \subseteq P.$$

Since $x^{-1}Bx$ is a Borel subgroup of G, this proves the only if part of (i), i.e., every parabolic subgroup contains a Borel subgroup.

To prove the if part, it will be sufficient to prove (ii). For if G/B is complete and $B \subseteq P$, then the image of G/P of G/B under the natural morphism $G/B \to G/P$ is complete, too (by 7.1.1(iii)).

(ii). We use induction on dim G/B. The case dim G/B = 0 (i.e. G solvable) is trivial. So assume that G is non-solvable. Then there is a proper parabolic subgroup $P \subseteq G$ (by 7.2.2). Replacing P by a conjugate, we may assume $P \supseteq B$. Then B is a Borel subgroup of P. By induction on dim G/B

we may assume that B is parabolic in P. But then B is parabolic in G by by transitivity (see 7.2.4). This proves (ii).
(iii). Let B and B' be two Borel subgroups. Then B and B' are parabolic by (ii). The argument in the proof of (i) shows that B is conjugate to a subgroup of B'. In particular dim B≤dim B', hence dim B = dim B' by symmetry. But the B and B' are conjugate.
(iv). Let T and T' be two maximal tori. Then T is contained in a Borel subgroup B (by the definition of Borel subgroup). By (iii) we may assume that T' is also contained in B. But maximal tori of connected solvable groups are conjugate by (6.11(iii)).
QED.

7.2.7 Homomorphic images of parabolic subgroups and maximal tori

Let $\phi: G \to G'$ be a surjective homomorphism of linear algebraic groups. Let $H \subseteq G$ be a Borel subgroup (parabolic subgroup, a maximal torus, respectively) of G. Then ϕH is a subgroup of G' of the same type.

Proof. If H is a
subgroup of G, then ϕH is closed (by 2.2.5(ii)), connected and solvable. Moreover, the induced morphism $G/H \to G'/\phi H$ is surjective. But then $G'/\phi H$ is complete (by 7.2.6(ii) and 7.1.1(iii)), hence ϕH contains a Borel subgroup (by 7.2.6(i)). By the definition of Borel subgroup, ϕH itself must be Borel.

If H is parabolic, then G/H is complete. From the surjection $G/H \to G'/\phi H$ one sees that $G'/\phi H$ is complete, too. Hence ϕH is parabolic in G'.
Now let H be a maximal torus. Take a Borel subgroup B containing T. Then there is a decomposition

$$B = H \cdot B_u$$

by 6.11(iv). Applying ϕ one obtains

$$\phi B = \phi H \cdot \phi B_u.$$

Since ϕB is a Borel subgroup and ϕB_u is unipotent, the isomorphisms of 6.11(v) implies that ϕH must be a maximal torus of ϕB. Since any two maximal tori are conjugate an are contained in a Borel subgroup, ϕH is a maximal torus of G'.

QED.

7.2.8 The center of a Borel subgroup

Let G be a connected linear algebraic group and $B \subseteq G$ a Borel subgroup. Then $\mathbf{Z}(G)^0 \subseteq \mathbf{Z}(B) \subseteq \mathbf{Z}(G)$.

Proof. $\mathbf{Z}(G)^0$ is connected, solvable and (trivially) closed, hence contained in some Borel subgroup B. By the conjugacy result

(7.2.6(iii)) for Borel subgroups, $\mathbf{Z}(G)^0$ is contained in every Borel subgroup. This proves the first inclusion.
Now let $g \in \mathbf{Z}(B)$. Consider the morphism

$$\phi: G \to G, x \mapsto gxg^{-1}x^{-1}.$$

By the choise of g, $\phi(xB) = \phi(x)$, hence induces a morphism $G/B \to G$. Since G/B is complete, this latter morphism must be constant (by 7.1.1(v)). But then ϕ is contant, i.e., $g \in \mathbf{Z}(G)$.
QED.

7.2.9 Nilpotent Borel subgroups

Let G be an algebraic group and $B \subseteq G$ a Borel subgroup. Then if B is nilpotent, $G^0 = B$.

Proof. We may assume that G is connected. The claim will be proved by induction on dim G. If $B = \{e\}$, then $G = G/B$ is complete, hence $G = \{e\}$ by (7.1.1(v)). So assume $B \neq \{e\}$. Since B is assumed to be nilpotent, dim $Z(B) > 0$ by 6.5(ii), hence dim $Z(G) > 0$ by 7.2.8.
Since $\mathbf{Z}(G)^0 \subseteq B$, it will be sufficient the prove the claim for $G/\mathbf{Z}(G)^0$. But then the result follows by induction.
QED.

7.2.10 Cartan subgroups

Let G be an algebraic group. A Cartan subgroup of G is a subgroup of type

$$C := Z_G(T)^0,$$

where $T \subseteq G$ is a maximal torus of G (a Cartan subgroup is the connected centralizer of a maximal torus). Since maximal tori of G are conjugate, the same is true of Cartan subgroups.

Corollary

Each Cartan subgroup C of G is nilpotent and equal to its connected normalizer $N_G(C)^0$.

Proof. T is a maximal torus of C and lies in the center of C.

Let B be a Borel subgroup of C. Then B contains a conjugate of T (by 7.2.6(iv)), hence T itself, since T is in the center of C. Moreover, the multiplication map $T \times B_u \to B$ is bijective by 6.11 and defines a direct product decomposition, since T is in the center of C. Note that, by 6.9(ii), B_u is a nilpotent connected closed normal subgroup of B. Note

that since the product decomposition $B=T\cdot B_u$ is direct, every normal subgroup of B_u is normal in B. Therefore, B is nilpotent.
We have proved, every Borel subgroup of C is nilpotent. But then C is itself nilpotent (by 7.2.9).

By 2.5.11,

$$C = Z_G(T)^0 = N_G(T)^0$$

Let $g\in N_G(C)^0$. Then the inner automorphism defined by g defines an automorphism $C\to C$, $x \mapsto gxg^{-1}$ that maps T onto a maximal torus. Since any two tori are conjugate and T is in the center of C, T is mapped onto itself. Therefore $g\in N_G(T)$. We have proved,

$$N_G(C)^0 \subseteq N_G(T), \text{ hence } N_G(C)^0 \subseteq N_G(T)^0.$$

From the identities above we see, $N_G(C)^0\subseteq C$. The converse inclusion is trivial.
QED.

7.2.11 Exercises

G is assumed to be a connected linear algebraic group.

(1) Aufgabe

Let H be a closed subgroup of G containing a maximal torus T. Then

$$N_G H\subseteq H^0\cdot N_G T.$$

(2) Aufgabe

Let B be a Borel subgroup of G. Then $(N_G B)^0 = B$.

(3) Aufgabe

If all elements of G are semi-simple then G is a torus.

(4) Aufgabe

Let $G = \mathbf{GL}_n$.

(a) The group $\mathbf{T}_n$ of upper triangular matrices in $\mathbf{GL}_n$ is a Borel subgroup.

(b) Let G act on $V = k^n$. A flag in V is a sequence of distinct subspaces V_i $(1\le i\le s)$ of V such that $V_1\subseteq V_2\subseteq\ldots\subseteq V_s$. Then G also acts on the set of flags. The flag is complete if $s = n-1$ and $\dim V_i = i$ for every i. The Borel subgroups of G are the subgroups whose elements fix a given complete flag. (**Hint** for the proof of (a): Let

G act on $\mathbb{P}^{n-1}$. Use that the isotropy group of a point of $\mathbb{P}^{n-1}$ is a parabolic subgroup, and show by induction on n that $\mathbf{GL}_n/\mathbf{T}_n$ is complete).

(5) Aufgabe

Assume char(k) $\neq 2$. Let $G=\mathbf{SO}_n$, viewed as a subgroup of $\mathbf{GL}_n$ fixing the symmetric bilinear form <?,?> of 6.6(1). A subspace W of $V = k^n$ is isotropic if the restriction of this form to W is zero. The Borel subgroups of G are the subgroups whose elements fix a given isotropy flag, i.e., a maximal flag consisting of isotropic subspaces. (Hint: proceed as in the preceding exercise; one has to use Witt's theorem, see [26, Ch. XIV, §5]).

(6) Aufgabe

Establish a similar result for the symplectic group $\mathbf{Sp}_{2n}$ (see 6.16(2)).

(7) Aufgabe

Assume that G is defined over $\mathbb{F}_q$ and let F be the corresponding Frobenius morphism (see 3.3.15). There exists a maximal torus T of G and a Borel subgroup $B \supseteq T$ such that FT = T , FB = B. If (T',B') is another such pair, there exists $x \in G$ with Fx = x such that $T' = xTx^{-1}$, $B' = xBx^{-1}$. (Hint: Use Lang's theorem 3.3.16 and 7.2.6(iii),(iv)).

(8) Aufgabe

Let B be a Borel subgroup of G and σ an automorphism of G (in the sense of algebraic groups) fixing all elements of B. Then σ=id.

(9) Aufgabe

Let P and Q be parabolic subgroups of G, with $P \subseteq Q$. Assume that X is a closed subset of G such that XP = X. Then XQ is closed (Hint: use the completeness of G/P).

Solutions

Zu (1)

Let $g \in N_G H$. Then gTg^{-1} is a maximal torus of H^0. Since any two tori of H^0 are conjugate in H^0, there exists some $x \in H^0$ such that $gTg^{-1} = xTx^{-1}$. But then $x^{-1}g$ normalizes T, i.e. $g \in xN_G T$. This proves the claim.

Zu (2)

Take some maximal torus T of G contained in B. Then, by exercise (1), $N_G B \subseteq B \cdot N_G T$, hence

(*) $$(N_G B)^0 \subseteq B \cdot N_G T.$$

Since the Cartan subgroup $C := (N_G T)^0$ is connected and nilpotent, some conjugate of C is contained in B, i.e.,

$$x(N_G T)^0 x^{-1} \subseteq B \text{ for some } x \in G.$$

But then, $B \supseteq x(N_G T)^0 x^{-1} = N_G(xTx^{-1})^0 \supseteq xTx^{-1}$. Since (*) is true for every maximal torus of G contained in B, we may replace T with xTx^{-1} and hence assume that

$$(N_G T)^0 \subseteq B.$$

But then $B \cdot (N_G T)^0 = B$ and $B \cdot N_G T$ is the disjoint union of a finite number of certain cosets of B. Since $(N_G B)^0$ is connected, it is contained in precisedly one of those cosets. Since it has e in common with B, it must be contained in B,

$$(N_G B)^0 \subseteq B.$$

The converse inclusion is trivial.

Zu (3)

Take some Borel subgroup $B \subseteq G$ and a maximal torus T of G contained in B. Since B is connected and solvable, one has a direct sum decomposition $B = T \cdot B_u$ by (6.11). Since the elements of G are semi-simple, B = T. In particular, B is nilpotent. But then B = G by (7.2.9), i.e., G = B = T is a torus.

Zu (4)

(a) Since $\mathbf{T}_n$ is conected and solvable[127], it will be sufficient to show that $\mathbf{T}_n$ is parabolic. Let $e_1,\ldots,e_n$ be the standard basis of V $= k^n$ and define $V_i = k \cdot e_1 + \ldots + k \cdot e_i$. Then

$$\mathbf{T}_n = \{g \in G \mid gV_i = V_i \text{ for } i=1,\ldots, n-1\}.$$

Define G_j to be the subgroup

$$G_j = \{g \in G \mid gV_i = V_i \text{ for } i=1,\ldots, j\}.$$

---

[127] Der Kommutator zweier Matrizen aus $\mathbf{T}_n$ hat Einsen auf der Hauptdiagonalen. Deshalb gilt $(\mathbf{T}_n, \mathbf{T}_n) \subseteq \mathbf{U}_n$. Es reicht also zu zeigen, $\mathbf{U}_n$ ist auflösbar. Dem ist aber so nach Aufgabe 2.1.4 (4). $\mathbf{U}_n$ ist sogar nilpotent (nach Aufgabe 7.2.11(4)).

Then $\mathbf{T}_n = G_{n-1}$, and it will be sufficient to show that each G_j is parabolic. Let G act on the projective space $\mathbb{P}(V)$ in the usual way. Then G_1 is the isotropy subgroup of V_1 considered as a point of $\mathbb{P}(V)$ hence is parabolic in G. Moreover, there is an action of G_1 on the projective space $\mathbb{P}(V/V_1)$ and G_2 is the isotropy subgroup of V_2/V_1 considered as a point of $\mathbb{P}(V/V_1)$. Assume we have already proved that G_j is parabolic. Consider the action of G_j on $\mathbb{P}(V/V_j)$. Then, with respect to this action, G_{j+1} is the isotropy subgroup of V_{j+1}/V_j considered as a point of $\mathbb{P}(V/V_j)$, hence is parabolic.

(b) Follows easily from the fact that any two Borel subgroups are conjugate.

(4) 1. Step. If $W \subseteq V$ is any isotropic subspace, then $\dim W \leq k := [\frac{n}{2}]$.

Since the scalar product is non-degenerate,

$$\dim W + \dim W^{\perp} = \dim V = n.$$

Moreover, since W is isotropic, $W \subseteq W^{\perp}$. Therefore, this identity implies

$$2 \cdot \dim W \leq n.$$

2. Step. Construction of a maximal isotropic subspace W of V.

Fix any orthonormal base $e_1,\ldots,e_n$ of V. Define another base by

$$f_j := \frac{1}{\sqrt{2}} (e_{2j-1} + \sqrt{-1} \cdot e_{2j})$$

$$\bar{f}_j := \frac{1}{\sqrt{2}} (e_{2j-1} - \sqrt{-1} \cdot e_{2j})$$

for $j=1,\ldots,k:=[\frac{n}{2}]$. Then

$$W := \langle f_1,\ldots,f_k \rangle$$

$$\bar{W} := \langle \bar{f}_1,\ldots,\bar{f}_k \rangle$$

are isotropic subspaces of V. By the first step they are even maximal isotropic subspaces.

3. Step. Let $0 \subset W_1 \subset W_2 \subset \ldots \subset W_k$ be an isotropy flag. Then

$$0 \subset W_1 \subset W_2 \subset \ldots \subset W_k \subseteq W_k^{\perp} \subset W_{k-1}^{\perp} \subset \ldots \subset W_1^{\perp} \subset V$$

is a complete flag (if equality holds in the middle, skip W_k).

By Witts theorem, $G=\mathbf{SO}_n$ acts transitively on the set of isotropy flags. Hence it is sufficient to show the claim for one such flag. Let W be the maximal isotropic subspace of the previous step, and let $0 \subset W_1 \subset W_2 \subset \ldots \subset W_k = W$ be any complete flag of W. Then

$$W_k^{\perp} = \begin{cases} W_k & \text{if } n \text{ is even} \\ W_k + \langle e_n \rangle & \text{if } n \text{ is odd} \end{cases}$$

Moreover, since the scalar product is non-degenerate, $\dim W_j^{\perp} =$ n-dim W_j = n-j. This proves the claim of the third step.

4. Step. Let $0 \subset W_1 \subset W_2 \subset \ldots \subset W_k$ be an isotropy flag. Then

$$B := \{g \in \mathbf{SO}_n \mid gW_j = W_j, \text{ for } j=1,\ldots,k\}$$

is a Borel subgroup of $G:=\mathbf{SO}_n$.

Since G consits of isometries, the condition $gW_j=W_j$ implies that g also fixes the orthogonal complement of W_j. Hence B consits of the Elements of G fixing a certain complete Flag of V. This means, there is a Borel subgroup $B' \subseteq \mathbf{GL}_n$ such that

$$B = B' \cap G.$$

In particular, B is resolvable. Since $G:=\mathbf{SO}_n$ acts transitively on $\mathbb{P}(V)$, the same argument as in (4) shows that B is parabolic. Thus all we have to show is that B is connected. Fixing a basis of V associated with the complete flag of Step 3, B consists of the upper triangular matrices of $\mathbf{SO}_n$,

$$B = \mathbf{SO}_n \cap \mathbf{T}_n .$$

To see that this group is connected note that an orthogonal upper triangular matrix is automatically diagonal. Therefore, in an appropriate affine Space, B is defined by the equations

$$x_1 \cdot x_2 \cdot \ldots \cdot x_n = 1.$$

$$x_i \cdot x_{k+i} = 1 \quad (i=1,\ldots,k)$$

$$x_n^2 = 1 \text{ (in case that n is odd).}$$

These identities imply that $x_1,...,x_n$ represent units in k[B] and allow to eliminate the last k indeterminates.

If n is even, k[B] is a polynomial algebra over

$k[x_1,...,x_n]/(x_i \cdot x_{k+i}-1 \mid i=1,...,k)$

$= k[x_1,...,x_n]_{x_1 x_2 \cdot ... \cdot x_k}/(x_i \cdot x_{k+i}-1 \mid i=1,...,k)$

$= k[x_1,...,x_k]_{x_1 x_2 \cdot ... \cdot x_k}$

If n is odd, a similar calculation shows that k[B] is a polynomial algebra over this ring, too.

At any case, k[B] has no zero divisors, i.e., B is connected.

Zu (5)

7.3 Weitere Eigenschaften von Borel-Untergruppen

Situation

Let G be a connected linear algebraic group

7.3.1 Lemma: die Konjugierten einer abgeschlossenen Untergruppe

Let H be a closed subgroup of the connected linear algebraic group G. Put

$$X = \bigcup_{x \in G} xHx^{-1}.$$

(i) X contains an open subset of its closure $\bar{X}$. If G/H is complete then X is closed.

(ii) If some element of G lies in (at least one but) only finitely many conjugates of H then $\bar{X} = G$.

Proof. We may assume H to be connected. Then

$$Y = \{(x,y) \in G \times G \mid x^{-1}yx \in H\}$$

is an irreducible closed subset of G×G. Moreover, if $(x,y) \in Y$, then $(xH,y) \subseteq Y$ (check these properties). The canonical morphism $G \to G/H$ is G-equivariant, hence induces an open map

$$G \times G \to G/H \times G$$

(by 4.3.3(i)). It follows that the image

$$Y_1 = \{(xH,y) \mid x^{-1}yx \in H\}$$

of Y in G/H×G is closed in G/H×G and is irreducible. Let

$$\pi: G/H \times G \to G$$

be the projection onto the second factor. Since $X = \pi Y_1$, the assertions (i) follow from 1.9.5 and the definition of completeness. The fibers of the projection morphism $Y_1 \to G/H$ all have dimension dim H. Therefore,

$$\dim Y_1 = \dim G/H + \dim H = \dim G$$

by 4.1.6(ii). Now let $x \in G$ have the property of (ii). Then $Y_1 \cap \pi^{-1}x$ is finite. Hence $\pi|Y_1$ has finite fibers over a dense open set by 4.2.5. In particular,

$$\dim \bar{X} = \dim Y_1 = \dim G.$$

But then $\bar{X} = G$.
QED.

7.3.2 Lemma: Zentralisator eines Torus als Zentralisator eines Elements

Let S be a torus in the connected linear algebraic group G. Then there is some $s \in S$ with

$$Z_G(S) = Z_G(s).$$

Proof. We may assume $G = \mathbf{GL}(V)$. The rational representations of S decompose into 1-dimensional ones (2.5.2c). Therefore,

$$V = \bigoplus_{\chi \in A} V_\chi ,$$

where

A is a finite set of characters of S

and

$$V_\chi := \{v \in V \mid s \cdot v = \chi(s)v \text{ for every } s \in S\}.$$

Elements $g \in G$ commuting with all $s \in S$, leave the subspaces V_χ invariant: for $v \in V_\chi$ and $gs = sg$ for every $s \in S$ one has

$$s \cdot gv = g \cdot sv = g \cdot (\chi(s)v) = \chi(s) \cdot gv,$$

i.e., $gv \in V_\chi$. Therefore,

$$Z_G(S) = \{g \in G \mid gV_\chi = V_\chi \text{ for every } \chi\}.$$

Choose $s \in S$ such that $\chi(s) \neq \chi'(s)$ for any two different $\chi, \chi' \in A$. This is possible since the regular function $\chi - \chi'$ is not identically zero on S (hence defines a proper closed subset) and since S is not the union of finitely many proper closed subsets (for it is connected). The element

s acts on different spaces V_χ by multiplication with different scalars. Hence theses spaces are the eigenspaces of s on V. But then the above argument shows that

$$Z_G(s) = \{g \in G \mid gV_\chi = V_\chi \text{ for every } \chi\}$$

hence $Z_G(s) = Z_G(S)$.

QED.

7.3.3 Überdeckungen aus Borel-Untergruppen, aus maximalen Tori und aus Cartan-Untergruppen

Let G be a connected linear algebraic group.

(i) Every element of G lies in a Borel subgroup.

(ii) Every semi-simple element of G lies in a maximal torus.

(iii) The union of the Cartan subgroups of G contains a dense open subset of G.

Proof. (iii).Let T be a maximal torus of G and $C := Z_G(T)^0$ the associated Cartan subgroup. Since any two Cartan subgroups are conjugate, the claim of (iii) follows from 7.3.1 provided we can show the existence of an element t which is contained in at least one and at most finitely many conjugacy classes of C.

Take some $t \in T$ such that

$$C = Z_G(t)^0,$$

which is possible by the preceding result 7.3.2. Then

$$t \in xCx^{-1} \text{ for some } x \in G$$

if and only if t lies in the unique maximal torus T of xCx^{-1} (see 6.11(i)). But then

$x^{-1}tx \in T$ hence

$$C = Z_G(T)^0 \subseteq Z_G(x^{-1}tx)^0 = x^{-1}Z_G(t)^0x = x^{-1}Cx$$

(taking the centralizer is an inclusion reversing operation). This implies $C = x^{-1}Cx$. We have proved, C is the only conjugate containing t. This proves (iii).

(i). Choose some Borel subgroup $B \subseteq G$ containing C,

$$C \subseteq B$$

(such B exists since C is nilpotent). Then

$$\bigcup_{x \in G} xCx^{-1} \subseteq \bigcup_{x \in G} xBx^{-1}$$

In particular, the set on the right is dense in G. Moreover, since G/B is complete, it is equal to G by 7.3.1.

(ii). Follows from (i) and 6.11(i).
QED.

7.3.4 Das Zentrum der Borel-Untergruppen

Let G be connected and let B⊆G be a Borel subgroup. Then Z(B) = Z(G).

Proof. By (7.2.8)

$$Z(B) \subseteq Z(G).$$

Conversely let x∈Z(G). Then x lies in a Borel subgroup by 7.3.3(i). Since any two Borel subgroups are conjugate, x lies in the center of every Borel subgroup, hence in Z(B).
QED.

7.3.5 Zusammenhang der Torus-Zentralisatoren, deren Borel-Untergruppen

Let G be connected and let S⊆G be a torus in G.

(i) The centralizer $Z_G(S)$ is connected.

(ii) Given a Borel subgroup B of G containing S, then

$$B \cap Z_G(S)$$

is a Borel subgroup of $Z_G(S)$. Moreover, all Borel subgroups of the centralizer $Z_G(S)$ are obtained in this way.

Proof. (i). Let $x \in Z_G(S)$. It is sufficient to show, x is in the connected centralizer of S. Let B be a Borel subgroup of G containing x (which exists by (7.3.3)). Moreover, let

$$X := \{gB \mid xgB \subseteq gB, g \in G\}$$

be the fixed point set of x in G/B. Then B∈X, and X is a closed subvariety of the projective variety G/B, hence is complete by (7.1.1(i)). By Borel's fixed point theorem 7.2.5, the action of the connected solvable group S on X has a fixed point, i.e., SgB = gB and xgB = gB for some g∈G. This means, both S and x are contained in one and the same Borel subgroup gBg^{-1} of G. By 6.12(ii) the centralizer of S in this Borel subgroup is connected, i.e., $x \in Z_G(S)^0$ as claimed.

(ii). Let B as in assertion (ii). Then $B \cap Z_G(S)$ is the centralizer of S in B and hence is connected by (6.12)(ii). Moreover it is solvable. To prove the first part of (ii) it is sufficient to show that $Z_G(S)/B \cap Z_G(S)$ is complete (by (7.2.6)(i)). Consider the injective morphism of homogeneous spaces

$$Z_G(S)/B \cap Z_G(S) \to G/B.$$

By 7.2.1 it will be sufficient to show that its image $Z_G(S)\cdot B/B$ is complete. Since the of the morphism $G\to G/B$ is open, it will be sufficient to show that

$$Y := Z_G(S)\cdot B$$

is closed in G. Note that Y is irreducible (as an image of $Z_G(S)\times B$ under a morphism). Moreover, for every $s\in S$, the set Y is mapped to B under

$$G \to G,\ g \mapsto g^{-1}sg.$$

For, if $y = z\cdot b \in Y$, then $y^{-1}Sy = b^{-1}Sb \subseteq B$ (for, $S\subseteq B$).

Since B is closed, the same is true for the closure $\bar{Y}$ of Y. The morphism

$$\bar{Y}\times S \to B/B_u\ ,\ (y,s) \mapsto y^{-1}syB_u\ ,$$

satisfies the hypothesies of the rigidity theorem (2.5.10):

$\bar{Y}$ is a connected affine variety as we have seen above
S and B/B_u are diagonlizable groups by assumption and by (6.9), respectively.
The morphism gives a homomorphism $S\to B/B_u$ for every fixed $y\in\bar{Y}$.

From 2.5.10 it follows that the latter map is independent upon y, i.e.,

(*) $$y^{-1}sy\in sB_u$$

for every $y\in\bar{Y}$ and every $s\in S$, i.e.,

$$y^{-1}Sy \subseteq SB_u \text{ for every } y\in\bar{Y}.$$

With these preparations we are now able to prove that Y is closed.

aLet $y\in\bar{Y}$. We have to show that y is in Y.

Note that SB_u is an algebraic group (it is contained in B and isomorphic to $S\times B_u$ by (6.11)(iv) as a variety and a group since B_u is normal in B). Moreover,

$$y^{-1}Sy$$

is a torus with dimension $\geq \dim SB_u/B_u$, hence a maximal torus of SB_u. Since any two tori in SB_u are conjugate by (6.11)(iii), there is some $x \in SB_u$ with

$$y^{-1}Sy = x^{-1}Sx.$$

We may assume[128]

$$x \in B_u.$$

Consider the element

$$y' = yx^{-1}.$$

This element satisfies

$$(**) \qquad (y')^{-1}Sy' = S$$

and it is also an element of $\bar{Y}$,

$$y' \in \bar{Y}.$$[129]

Therefore, relation (*) holds for y' (as for all elements from $\bar{Y}$): for every $s \in S$ there is some $b \in B_u$ such that

$$y'^{-1}sy' = sb.$$

On the other hand, $y'^{-1}sy' \in S$ (in view of (**)), i.e.

$$b \in S \cap B_u = \{e\},$$

i.e., $y'^{-1}sy' = s$. Since this is true for every $s \in S$,

$$yx^{-1} = y' \in Z_G(S)$$

hence $y \in Z_G(S) \cdot B = Y$. We have proved, $\bar{Y} \subseteq Y$, i.e., Y is closed. This completes the proof of the first part of (ii).

The remaining part follows from the fact that any two Borel subgroups of $Z_G(S)$ are conjugate.

QED.

7.3.6 Cartan-Untergruppen, ihre Beziehung zu den Borel-Untergruppen

Let G be connected and let $T \subseteq G$ be a maximal torus in G. Then

---

[128] Write $x = sb$ with $s \in S$ and $b \in B_u$. Then $x^{-1}Sx = b^{-1}Sb$.

[129] For every $b \in B_u$ the morphism

$G \to G, g \mapsto gb,$

maps Y into $Y \subseteq \bar{Y}$, hence $\bar{Y}$ into $\bar{Y}$.

(i) $C = Z_G T$ is a Cartan subgroup of G

(ii) If B is a Borel subgroup containing T then $C \subseteq B$.

Proof. (i). By 7.3.5, C is connected, hence equal to the connected centralizer of the maximal torus T, hence a Cartan subgroup of G.
(ii) By 7.3.5, $B \cap C$ is a Borel subgroup of C. By (7.2.10), C is nilpotent, hence resolvable, hence equal to its only Borel subgroup, $B \cap C = C$. But then $C \subseteq B$.

QED.

7.3.7 Der Normalisator einer Borel-Untergruppe

Let G be a connected linear algebraic group and $B \subseteq G$ a Borel subgroup. Then $N_G B = B$.

Proof. Let $N := N_G B$. We prove $N = B$ by induction on dim G.

Let T denote a maximal torus of B. If $x \in N$, then xTx^{-1} is a maximal torus of B, hence there is some $b \in B$ with $xTx^{-1} = bTb^{-1}$, i.e., $b^{-1}x$ normalizes T. To prove that x is in B we may assume that x normalizes T. Consider the homomorphism

$$\phi: T \to T,\ t \mapsto xtx^{-1}t^{-1}.$$

There are two cases.

1. case: ϕ is not surjective. Then $S := (\mathrm{Ker}\ \phi)^0$ is a non-trivial subtorus of T (by (2.5.3) it is diagonalizable, and it is a tous by (2.5.8)(ii)). Obviously, $x \in Z_G S$ (for, Ker ϕ consists of all elements of T commuting with x, so that x centralizes Ker ϕ hence S). Now x normalizes B by assumption, hence it normalizes the Borel subgroup $Z_G S \cap B$ of $Z_G S$. In case that $Z_G S \neq G$ induction hypothesis implies $x \in Z_G S \cap B$ hence $x \in B$. In case $Z_G S = G$, S is contained in the center and replacing G by G/S we can again use the induction hypothesis.

2. case: ϕ is surjective. By Chevalley's theorem (5.1.3) there is a rational representation

$$\rho: G \to GL(V)$$

such that the closed subgroup N of G is the stabilizer of a line $k \cdot v \subseteq V$,

$$(*) \qquad N = \{g \in G \mid \rho(g)v \in k \cdot v\}.$$

If $g \in B_u$ we have $\rho(g)v = v$ (homomorphisms $B_u \to G_m$ must be trivial since G_m has no unipotent elements)

If $t \in T$, write $t = x t_1 x^{-1} t_1^{-1}$ (we assume that ϕ is surjective). One sees that, again, $\rho(t)v = v$ (use (*), i.e., v is an eigen vector of x and t_1).

Thus $\rho(B)v = v$ and there is a morphism $G/B \to V$, $gB \mapsto \rho(g)v$. Since G/B is complete and V is affine, this morphism must be constant, i.e., $\rho(g)v = v$ for all g, i.e., $G = N$. But then by Exercise (7.2.11)(2) $B = N^0 = N$. This completes the proof of the theorem.

QED.

7.3.8 Der Normalisater einer parabolischen Untergruppe, Zusammenhang

Let G be connected and let $P \subseteq G$ be a parabolic subgroup. Then

$$N_G P = P.$$

Moreover, P is connected.

Proof. Let $B \subseteq P^0$ be a Borel subgroup. If $x \in N_G P$, then xBx^{-1} is also a Borel subgroup of P^0, hence there is some $y \in P^0$ with $xBx^{-1} = yBy^{-1}$ (by 7.2.6(iii)). Then $y^{-1}x$ normalizes B, hence is in B by (7.3.7). In particular $y^{-1}x \in P^0$ hence $x \in P^0$. This proves the claim.

QED.

7.3.9 Konjugierte parabolische Untergruppen, die eine Borel-Untergruppe enthalten

Let G be connected and let $P,Q \subseteq G$ be parabolic subgroups containing a Borel subgroup B.

Then, if P and Q are conjugate in G, $P = Q$.

Proof. Let $Q = xPx^{-1}$. Then B and xBx^{-1} are both Borel subgroups of Q, hence $xBx^{-1} = yBy^{-1}$ for some $y \in Q$. Then $y^{-1}x$ normalizes B, hence lies in B, hence in Q, hence $x \in Q$. But then $P = Q$ as claimed.

QED.

7.3.10 Die Varietät der Borel-Untergruppen

Sei G eine zusammenhängende lineare algebraische Gruppen und bezeichne

$$\mathbf{B} = \mathbf{B}(G)$$

die Menge der Borel-Untergruppen von G. Fixieren wir ein $B \in \mathbf{B}$ und betrachten wir die Abbildung

$$G/B \to \mathbf{B},\ gB \mapsto gBg^{-1}.$$

Die Abbildung ist wohldefiniert (da B eine Gruppe ist). Sie ist surjektiv, da je zwei Borel-Untergruppen konjugiert sind (nach

7.2.6(iii)), und sie ist injektiv wegen $N_G B = B$ (nach 7.3.7). Mit Hilfe dieser Abbildung können wir auf **B** die Struktur einer projektiven Varietät definieren. Da je zwei Borel-Untergruppen konjugiert sind, $B' = gBg^{-1}$, und die Konjugation mit g einen Isomorphismus $G/B \to G/B'$ definiert, ist diese Struktur von **B** sogar unabhängig von der speziellen Wahl von B. Wir haben auf diese Weise die Varietät der Borel-Untergruppen von G definiert. Diese ist ein homogener Raum bezüglich G.

Allgemeiner können wir für jede parabolische Untergruppe $P \supseteq B$ von G auf der Menge

$$\mathbf{P} = \mathbf{P}(P)$$

der zu P konjugierten Untergruppen die Struktur einer projektiven Varietät definieren. Es besteht dann eine Surjektion

$$(G/B \cong)\ \mathbf{B} \to \mathbf{P}\ (\cong G/P)\ ,$$

welche ein Morphismus von homogenen Räumen über G ist.

7.3.11 Aufgaben

Im folgenden sei G eine zusammenhängende lineare algebraische Gruppe.

(1) Ein Element $x \in G$ heißt <u>regulär</u>, wenn die Vielfachheit des Eigenwertes 1 von Ad(x) minimal ist.

(1a) Die regulären Elemente von G bilden eine nicht-leere offene Untermenge von G.

(1b) Ein Element x ist genau dann regulär, wenn der halbeinfache Teil von x regulär ist.

(1c) Ein halbeinfaches Element x ist genau dann regulär, wenn der Zentralisator von x minimale Dimension hat (man benutze 4.4.4(ii)).

(1d) Ein halbeinfaches Element x ist genau dann regulär, wenn $Z_G(x)^0$ eine Cartan-Untergruppe von G ist. (Hinweis: man verwende 7.3.2 und 7.3.3(ii)).

(2a) Eine abgeschlossene nilpotente Untergruppe $C \subseteq G$ mit $C = (N_G C)^0$ ist eine Cartan-Untergruppe (Hinweis: man benutze 6.16(2)).

(2b) Sei C eine maximale nilpotente Untergruppe von G mit der Eigenschaft , daß jede Untergruppe mit endlichen Index in C einen endlichen Index in ihrem Normalisator hat. Dann ist C eine Cartan-Untergruppe. (Dies ist eine gruppentheoretische Charakterisierung der Cartan-Untergruppen. Hinweis für einen Beweis: man zeige, die Abschließung einer nilpotenten

Untergruppe of G ist nilpotent. Man schlußfolgere, C ist abgeschlossen, und weiter, C genügt den Bedingungen von (a))

Lösungen

(1a) Sei G in den affinen Raum eingebettet. Dann ist die Konjugation mit g,

$$G \to G,\ x \mapsto gxg^{-1} =: f(x,g),$$

eine in x und g reguläre Funktion. Ihr Differential in x=e,

$$\mathrm{Ad}(g): T_eG \to T_eG$$

ist durch eine Matrix gegeben, die in regulärer Weise von g abhängt. Dasselbe gilt von der Matrix $\mathrm{Ad}(g)-\lambda\cdot\mathrm{Id}$, also auch vom charakteristischen Polynom $p(\lambda)$. Die Bedingung, daß $p(\lambda)$ die n-fache Nullstelle 1 haben soll, bedeutet, $p(\lambda)$ ist an der Stelle 1 zusammen mit seinen ersten n-1 Ableitungen Null. Dies ist eine abgeschlossene Bedingung, d.h. die Forderung, daß die Anzahl der Eigenwerte von g nicht minimal sein soll ist abgeschlossen.

(1b) Sei $x=s\cdot u$ die Jordan-Zerlegung. Sei G in GL_n, und zwar derart, daß x, s und u obere Dreiecksgestalt bekommen (das ist möglich, da s und u kommutieren). Dann hat u lauter Einsen auf der Hauptdialgonalen, d.h. x und s haben den Eigenwert 1 mit derselben Vielfachheit.

(1c) Sei $g\in G$ halbeinfach. Nach 4.4.4 ist der Morphismus

$$G \to G,\ x \mapsto gxg^{-1}x^{-1},$$

separabel. Die Faser über e hat deshalb dieselbe Dimension wie der Kern des Differentials $\mathrm{Ad}(g)-1: T_eG \to T_eG$. Letztere Dimension ist aber die Vielfachheit des Eigenwertes 1. Die regulären halbeinfache Elemente g sind also diejenigen mit

$$\dim \{x\in G \mid gxg^{-1}x^{-1} = e\} = \min.$$

Links steht aber die Dimension des Zentralisators von g.

(1d) Sei g halbeinfach. Wir wählen einen maximalen Torus T mit $g\in T$ (das ist möglich nach 7.3.3(ii)). Dann gilt

$$Z_G(T)^0 \subseteq Z_G(g)^0.$$

Nach 7.3.2 gibt es weiter ein $g'\in T$ mit

$$Z_G(g')^0 = Z_G(T)^0 \subseteq Z_G(g)^0.$$

Nach (1c) ist g genau dann regulär, wenn überall das Gleichheitszeichen gilt, d.h. wenn $Z_G(g)^0$ eine Cartan-Untergruppe ist.

(2a) Nach Annahme ist C abgeschlossen nilpotent und zusammenhängend. Nach Ex. 6.16(2) genügt es zu zeigen, $C=N_G C$, d.h. es genügt zu zeigen, $N_G C$ ist zusammenhängend.

7.3.12 Notes

8. Linear action of a torus on a projective variety

8.1 Fixpunkte

8.1.1 Bezeichnungen und Vereinbarungen (1-dimensionaler Fall)

Sei ρ: $\mathbf{G}_m \to GL(V)$ eine rationale Darstellung. Diese definiert eine Operation der multiplikativen Gruppe $\mathbf{G}_m$ auf der Projektivierung $\mathbb{P}(V)$ von V,

$$\mathbf{G}_m \times \mathbb{P}(V) \to \mathbb{P}(V),\ (g,x) \mapsto g\cdot x.$$

Sei

$$X \subseteq \mathbb{P}(V)$$

eine abgeschlossene Teilvarietät, die unter der Operation von $\mathbf{G}_m$ stabil ist. Wir identifizieren im folgenden $\mathbf{G}_m$ als die Teilmenge

$$\mathbf{G}_m = \mathbb{P}^1 - \{0,\infty\}$$

der projektiven Geraden.

8.1.2 Fixpunkte und assymptotische Limites von $\mathbf{G}_m$-Orbits

(i) For jeden Punkt $x \in X$ kann die Orbitalabbildung $\mathbf{G}_m \to X$, $g \mapsto g\cdot x$, auf die ganze projektive Gerade fortgesetzt werden. Bezeichnungsweise:

$$\mathbb{P}^1 \to X,\ g \mapsto g\cdot x.$$

(ii) Für jedes $x \in X$ sind die Punkte $0\cdot x$ und $\infty\cdot x$ Fixpunkte von $\mathbf{G}_m$ auf X. Weiter gilt $0\cdot x = \infty\cdot x$ genau dann, wenn $x \in X$ ein Fixpunkt ist.

Beweis. Wir wählen eine Basis $\{e_i\}_{i=1,\dots,n}$ von V, auf der $\mathbf{G}_m$ durch Multiplikation mit Charakteren operiert,

$\rho(g)e_i = g^{m_i} e_i$

mit $m_i \in \mathbb{Z}$ wobei gelte

$$m_1 \geq m_2 \geq \dots \geq m_n.$$

Sei $v \in V$. Wir schreiben v in der Gestalt

$$v = \sum_{i=a}^{b} v_i e_i \text{ mit } v_a \neq 0,\ v_b \neq 0.$$

Ist $x = [v]$ der zugehörige Punkt im projektiven Raum $\mathbb{P}(V)$, so gilt

$$g \cdot x = [\sum_{i=a}^{b} g^{m_i} v_i e_i] = f(g) = h(g^{-1})$$

mit

$$f(g) := [\sum_{i=a}^{b} g^{m_i - m_b} v_i e_i]$$

$$h(g) := [\sum_{i=a}^{b} g^{m_a - m_i} v_i e_i]$$

Durch f ung h sind Abbildungen $\mathbb{A}^1 \to \mathbb{P}(V)$ definiert mit $f(g) = h(g^{-1})$ für $g \neq 0$. Sei können verheftet werden zu einer Abbildung

$$\phi: \mathbb{P}^1 \to \mathbb{P}(V) \text{ mit } \phi(0) = [\sum_{m_i = m_b} v_i e_i] \text{ und } \phi(\infty) = [\sum_{m_i = m_a} v_i e_i].$$

Dies ist der in (i) beschriebene Morphismus. Nach Konstruktion sind $0 \cdot x = \phi(0)$ und $\infty \cdot x = \phi(\infty)$ Fixpunkte. Die Bedingung $0 \cdot x = \infty \cdot x$ bedeutet, daß alle m_i mit $v_i \neq 0$ gleich sind. Das ist aber gleichbedeutend damit, daß x ein Fixpunkt ist.

QED.

8.1.3 Bezeichnungen (algemeine Dimension)

Wir werden unten ein ähnliches Ergebnis wie in 8.1.2 für beliegige Tori beweisen, indem wir den allgemeinen Fall auf den 1-dimensionalen zurückführen.

Sei T ein Torus und

$$\rho: T \to GL(V)$$

eine rationale Darstellung. Diese Darstellung definiert eine Operation

$$T \times \mathbb{P}(V) \to \mathbb{P}(V),\ (t,x) \mapsto t \cdot x.$$

Sei

$$Y \subseteq \mathbb{P}(V)$$

eine T-stabile Teilvarietät von $\mathbb{P}(V)$. Bezeichnungen:

X := X*(T) Gruppe der Charaktere von T, d.h. der Homomorphismen $T \to \mathbf{G}_m$.

$X^V := X_*(T)$ Gruppe der 1-parametrigen Untergruppen von T, d.h. der Homomorphismen $\mathbf{G}_m \to T$.

Wir wissen nach den Ergebnissen des 2. Kapitels (2.5.1), X und x^V sind freie abelsche Gruppen endlichen Rangs. Zwischen ihnen besteht eine Paarung

$$(,): X \times X^V \to \mathbb{Z}, (\chi, \lambda) \mapsto <\chi, \lambda>$$

mit $\chi(\lambda(g)) = g^{<\chi, \lambda>}$.

8.1.4 Einschränkung auf 1-dimensionale Untergruppen bei Erhaltung der Fixpunkt-Menge

Seien T ein Torus, $\rho: G \to GL(V)$ eine rationale Darstellung und

$$Y \subseteq \mathbb{P}(V)$$

eine T-stabile Teilvarietät bezüglich der induzierten Operation auf dem projektiven Raum. Dann gibt es endlich viele Charaktere

$$\chi_1, \ldots, \chi_r \in X$$

derart daß für alle $\lambda \in X^V$ mit

$$<\chi_i, \lambda > \neq 0 \text{ für } i = 1,\ldots,r$$

die Fixpunkte in Y der eingeschränkten Operation

$$\rho \circ \lambda: \mathbf{G}_m \to T \to GL(V)$$

dieselben sind wie die von $\rho: T \to GL(V)$.

Beweis. Für $\chi \in X$ sei

$$V_\chi := \{v \in V \mid \rho(t)v = \chi(t)v \text{ für alle } t \in T\}$$

der Eigenraum zum Charakter χ. Dann ist V die direkte Summe zu endlich vielen solchen (von Null verschiedenen) Eigenräumen. Die Fixpunkte von T auf $\mathbb{P}(V)$ sind gerade die Punkte [v] welche in einem solchen Eigenraum liegen.Der eindimensionale Torus $\mathbf{G}_m$, der über $\rho \circ \lambda$ auf $\mathbb{P}(V)$ operiert hat genau dann dieselben Fixpunkte wie T, wenn alle Einschränkungen verschiedener Charaktere die in der Zerlegung von V auftreten, verschieden bleiben, d.h. die

$$\chi(\lambda(g)) = g^{<\chi, \lambda>}$$

müssen paarweise verschieden sein, d.h. $<\chi, \lambda> \neq <\chi', \lambda>$ falls χ und χ' verschiedene Charaktere nichtrivialen Eigenräumen sind. Mit anderen Worten, die notwendigen und hinreichenden Bedingungen sind

$$<\chi - \chi', \lambda> \neq 0.$$

QED.

8.1.5 Operation auf irreduziblen Varietäten

Seien T ein Torus, $\rho: G \to GL(V)$ eine rationale Darstellung und

$$Y \subseteq \mathbb{P}(V)$$

eine T-stabile Teilvarietät bezüglich der induzierten Operation auf dem projektiven Raum. Die Varietät Y sei irreduzibel und in keinem echten linearen Unterraum $\mathbb{P}(W) \subseteq \mathbb{P}(V)$ enthalten. Dann gilt

(i) Ist dim Y ≥ 1, so hat T wenigstens 2 Fixpunkte auf Y.

(ii) Ist dim Y ≥ 2, so hat T wenigstens 3 Fixpunkte auf Y.

Beweis. (i). Nach 8.1.4 können wir annehmen, $T = \mathbf{G}_m$. Wenn alle Punkte von Y Fixpunkte sind, ist die Aussage trivial. Sei also $y \in Y$, welcher kein Fixpunkt ist. Dann sind $0 \cdot y$ und $\infty \cdot y$ nach 8.1.2 zwei verschiedene Fixpunkte.

(ii). Wir wählen die Bezeichnungen wie im Beweis von 8.1.2. Sei W der von $e_2,\ldots,e_n$ erzeugte Unterraum von V. Da $\mathbb{P}(V)$-$\mathbb{P}(W)$ isomorph zum affinen Raum $\mathbb{A}^{n-1}$ ist, kann Y nicht ganz in $\mathbb{P}(V)$-$\mathbb{P}(W)$ liegen. Also

$$Y \cap \mathbb{P}(W)$$

eine nicht-leere projektive Varietät einer Dimension ≥1, welche stabil unter der betrachteten Operation ist (nach Wahl der e_i). Nach dem ersten Teil gibt es in diesem Durchschnitt mindestens 2 Fixpunkte. Um noch einen dritten Fixpunkt zu finden, wählen wir ein

$$x \in Y\text{-}\mathbb{P}(W).$$

Dann ist $\infty \cdot x$ ein Fixpunkt. Dieser liegt nach Wahl der Vektoren e_i nicht in $\mathbb{P}(W)$, ist also von den bereits gefundenen Fixpunkten verschieden.

QED.

8.1.6 Die Weyl-Gruppe

Seien G eine zusammnenhängende lineare algebraische Gruppe und T ein maximaler Torus von G. Die Weyl-Gruppe von G bezüglich T ist definiert als die endliche Gruppe

$$W := N_G T / Z_G T$$

(vgl. 2.5.11). Weiter bezeichne **B** die Varietät der Borel-Untergruppen von G (7.3.10) und $\mathbf{B}_T$ die Menge der Fixpunkte von T auf **B**, d.h. die Menge der Borel-Untergruppen, die den Torus T enthalten.[130]

Bemerkungen

---

[130] Für Borel-Untergruppen B mit $T \subseteq B$ gilt trivialerweise $tBt^{-1} = B$ für alle $t \in T$. Ist umgekehrt B eine Borel-Untergruppe mit $tBt^{-1} = B$ für alle $t \in T$, so gilt $t \in N_G(B) = B$ (vgl. 7.3.7) für alle $t \in T$, d.h. $T \subseteq B$.

(i) Die Elemente von $N_G T$ operieren durch Konjugation auf T. Die induzierten Abbildungen sind Automorphismen der algebraischen Gruppe T. Deshalb kann man W(T) als eine Untergruppe der Automorphismengruppe von T auffassen,

$$W(T) \subseteq \mathrm{Aut}(T).$$

(ii) Offensichtlich operiert $N_G T$ auf $\mathbf{B}_T$. Auf Grund des nachfolgenden Ergebnisses induziert diese Operation eine Operation der Weyl-Gruppe auf $\mathbf{B}_T$.

8.1.7 Die Operation Weyl-Gruppe auf $\mathbf{B}_T$

Seien G eine zusammnenhängende lineare algebraische Gruppe und T ein maximaler Torus von G.

(i) Der Zentralisator $Z_G T$ operiert trivial auf $\mathbf{B}_T$.

(ii) Die Operation von $N_G T$ auf $\mathbf{B}_T$ definiert eine einfach transitive Operation der Weyl-Gruppe auf $\mathbf{B}_T$.

Beweis. Zu (i). Sei $B \in \mathbf{B}_T$ und $g \in Z_G T$. Das erste bedeutet $T \subseteq B$. Nach 7.3.6(ii) gilt dann $g \in Z_G T \subseteq B$, also $gBg^{-1} = B$, d.h. g operiert auf $B \in \mathbf{B}_T$ trivial.

Zu (ii). Seien $B, B' \in \mathbf{B}_T$ zwei Borel-Untergruppen, d.h. sei $B \supseteq T$ und $B' \supseteq T$. Nach 7.2.6(iii) gibt es ein $x \in G$ mit

$$B' = xBx^{-1} \ (\supseteq T).$$

Also ist $x^{-1}Tx \subseteq B$. Nach 6.11(iii) existiert ein $b \in B$ mit $x^{-1}Tx = b^{-1}Tb$, d.h. mit

$$n := xb^{-1} \in N_G T.$$

Wegen $b \in B$ gilt

$$nBn^{-1} = xBx^{-1} = B'.$$

Wir haben gezeigt, W operiert transitiv auf $\mathbf{B}_T$. Sei jetzt $n \in N_G T$ ein Element mit $nBn^{-1} = B$. Nach 7.3.7 gilt dann $n \in N_G B = B$, also

$$\begin{aligned} n \in N_G T \cap B &= N_B T && \text{(tivial)} \\ &= Z_B T && \text{(nach 6.12(ii))}. \end{aligned}$$

Das Element n repräsentiert das neutrale Element der Weyl-Gruppe. Die Operation von W ist also einfach transitiv.

QED.

8.1.8 Fixpunkte parabolischer Untergruppen, kleine Weyl-Gruppen und Erzeuger von G

Seien G eine zusammenhängende lineare algebraische Gruppe und $T \subseteq G$ ein maximaler Torus.

(i) Ist $P \subseteq G$ eine echte parabolische Untergruppe, so hat T auf G/P mindestens 2 Fixpunkte und im Fall dim G/P>1 sogar mindestens 3.

(ii) $W(T) = \{e\} \Leftrightarrow$ G ist auflösbar.

(iii) Im Fall $\#W(T) = 2$ gilt dim $\mathbf{B} = 1$.

(iv) G wird von den Borel-Untergruppen B, welche T enthalten, erzeugt.

Beweis. Zu (i). Nach dem Satz von Chevalley 5.1.3 gibt es eine rationale Darstellung

$r: G \to GL(V)$

und eine Gerade $L \subseteq V$ durch den Ursprung derart, daß G/P gerade das G-Orbit von L in $\mathbb{P}(V)$ ist. Aussage (i) ergibt sich damit aus 8.1.5.

Zu (ii). Die Implikation "$\Leftarrow$" gilt nach 6.12(ii). Sei jetzt umgekehrt W trivial. Angenommen G ist nicht auflösbar. Dann gibt es eine echte Borel-Untergruppe B in G,

$B \subseteq G, B \neq G$.

Nach (i) hat T mindestens zwei Fixpunkte auf G/B, d.h. es $\#\mathbf{B}_T \geq 2$. Da W transitiv auf $\mathbf{B}_T$ operiert (nach 8.1.7), kann W dann nicht trivial sein.

Zu (iii). Weil W einfach transitiv auf $\mathbf{B}_T$ operiert, gilt $\#\mathbf{B}_T = 2$. Nach (i) folgt dim G/B $\leq$1. Der Fall dim G/B<1 ist aber nicht möglich, weil dann G auflösbar wäre, also nach (ii) #W=1 gelten würde. Also gilt dim G/B = 1. Das ist aber die Aussage von (iii).

Zu (iv). Wir führen den Beweis durch Induktion nach dim G. Im Fall dim G = 0, d.h. G= {e} ist nichts zu beweisen. Sei Q die Untergruppe, welche von den Borel-Untergruppen $B \in \mathbf{B}_T$ erzeugt wird. Nach 6.1(ii) und (i) ist Q zusammenhängend und abgeschlossen. Da Q eine Borel-Untergruppe enthält, ist Q parabolisch (7.2.6(i)). Angenommen, es ist $Q \neq G$. Nach (i) hat T auf G/Q mindestens 2 Fixpunkte. Identifiziert man G/Q mit der Varietät der zu Q konjugierten parabolischen Untergruppen (7.3.10), so sind die Fixpunte von T gerade die zu Q konjugierten parabolischen Untergruppen Q' mit

$$tQ't^{-1} = Q' \text{ für alle } t \in T.$$

Wegen $N_G Q' = Q'$ (vgl. 7.3.8) ist letztere Bedingung äquivalent zu

$$T \subseteq Q'.$$

Mit anderen Worten es gibt ein $Q' = gQg^{-1}$, $g \in G$, mit $T \subseteq Q' \neq Q$. Mit Q ist auch Q' eine echte Untergruppe. Nach Induktionsvoraussetzung bzgl. dim G gilt also

$$\begin{aligned} Q' &= \langle B \mid B \text{ Borel-Untergruppe von } Q' \text{ mit } T \subseteq B \rangle \\ &\subseteq \langle B \mid B \text{ Borel-Untergruppe von } G \text{ mit } T \subseteq B \rangle \\ &= Q. \end{aligned}$$

Man beachte die Enthaltenseinsrelation kommt von der Tatsache, daß jede Borel-Untergruppe von Q' in einer von G enthalten ist. Da Q' und Q konjugiert sind, folgt aus der Inklusion, daß Q = Q' gilt. Das widerspricht aber der Wahl von Q und Q'. Also gilt Q=G.
QED.

8.2 Gruppen vom Rang 1

8.2.1 Rang und halbeinfacher Rang

Seien G eine lineare algebraische Gruppe und T ein maximaler Torus von G. Dann ist der Rang von G definiert als die Zahl

$$\text{rk } G := \dim T.$$

Der halbeinfache Rang von G ist definiert als

$$\text{ss-rk } G := \text{rk } G/R(G).$$

Dabei bezeiche R(G) wie bisher das Radikal von G (vgl. 6.14).

8.2.2 Die Situation in diesem Abschnitt

In diesem Abschnitt sei G eine lineare zusammenhängende algebraische Gruppe deren Rang gleich 1 ist,

$$\text{rk } G = 1,$$

und welche nicht auflösbar ist.
Weiter sei B eine Borel-Untergruppe von G und $T \subseteq B$ ein maximaler Torus von G. Mit W bezeichnen wir die zu T gehörige Weyl-Gruppe,

(1) $$W := N_G T/Z_G T.$$

Weil G den Rang 1 hat, gilt $T \cong \mathbf{G}_m$ und W kann mit einer Untergruppe der Automorphismengruppe von $\mathbf{G}_m$ identifiziert werden:

(2) $$W \subseteq \text{Aut}(\mathbf{G}_m) = \text{Einheitengruppe von } \mathbb{Z} = \{\pm 1\}.$$

Da G nicht auflösbar sein soll, gilt nach 8.1.8(ii) sogar

(3) $$W = \text{Aut}(\mathbf{G}_m) = \{\pm 1\}.$$

Repräsentiere $n \in N_G T$ das vom neutralen Element verschiedene Element von W, d.h. die Konjugation mit n ist gerade der Übergang zum Inversen,

(4) $$ntn^{-1} = t^{-1} \text{ für alle } t \in T.$$

Da W die Ordnung 2 hat, gilt weiter

(5) $$n^2 \in Z_G T.$$

Schließlich sei $U := B_u$ der unipotente Teil von B.Nach 6.11 läßt sich G/U mit einem maximalen Torus von G identifizieren, d.h. es gilt dim G/U = 1.

8.2.3 Lemma 2.2: Das Radikal

Sei G eine zusammenhängende nicht-auflösbare Gruppe vom Rang 1. Dann gilt mit den Bezeichnungen von 8.2.2.

(i) G ist disjunkte Vereinigung der Doppelrestklassen B und $U \cdot n \cdot B$.

(ii) $RG = (U \cap nUn^{-1})^0$ (das Radikal von G).

(iii) $\dim U/U \cap nUn^{-1} = 1$.

Beweis. Sei $\xi \in \mathbf{B}$ der dem Punkt $B \in G/B$ entsprechende Punkt. Wegen $T \subset B$ gilt

$$\xi \in \mathbf{B}.$$

Da $W=\{e,\bar{n}\}$ nach 8.1.7(ii) auf $\mathbf{B}_T$ transitiv operiert, gilt

$$\mathbf{B}_T = \{\xi, n \cdot \xi\}.$$

Zeigen wir zunächst, es gilt

(*) $\xi \notin U n\xi \supset \{n\xi\}$ (echte Inklusion)

Angenommen, es gilt $\xi \in Un\xi$. Dann gilt $\xi = un\xi$ für ein $u \in U$, d.h.

$$B = unBn^{-1}u^{-1}$$

Wegen $u \in U \subseteq B$ folgt $B = nBn^{-1}$, d.h. $\xi = n \cdot \xi$, was im Widerspruch steht zur Transitivität der Operation von W auf $\mathbf{B}_T$. Dies beweist die linke Hälfte von (*). Angenommen, es gilt $Un\xi = \{n\xi\}$, d.h.,

$$unBn^{-1}u^{-1} = nBn^{-1} \text{ für alle } u \in U.$$

Dann ist $U \subseteq N_G(nBn^{-1}) = nBn^{-1}$ (vgl. 7.3.7). Wegen $n \in N_G T$ gilt außerdem $T \subseteq nBn^{-1}$, also nach 6.11 auch

$$B = U \cdot T \subseteq nBn^{-1}.$$

Dann ist aber $B = nBn^{-1}$, d.h. $\xi = n \cdot \xi$. Dieser Widerspruch beweist (*). Als stetiges Bild von B ist $Un\xi$ zusammenhängend (6.11) und $\neq \{n\xi\}$, also mindestens eindimensional,

$$\dim Un\xi \geq 1.$$

Nun liegt $Un\xi$ ganz im 1-dimensionalen Raum $\mathbf{B} \cong G/B$, d.h. $Un\xi$ enthält eine dichte offene Teilmenge. Da offene Mengen im 1-dimensionalen Fall Komplemente von endlichen Mengen sind, ist $Un\xi$ offene dichte Teilmenge von $\mathbf{B}$,

$$Un\xi = \mathbf{B} - S \text{ mit } S \text{ endlich.}$$

Zeigen wir, die Menge $Un\xi$ ist stabil unter T, d.h.

$$TUn\xi = Un\xi.$$

Die Inklusion "$\supseteq$" ist trivial. Zum Beweis von "$\subseteq$" betrachten wir Elemente $u \in U$ und $t \in T$. Es gilt

$$tun\xi = tut^{-1}tn\xi \in Un\xi$$

(denn tut^{-1} ist unipotent, also in B und $n\xi$ ist fest bei T). Damit ist gezeigt, daß T die Menge $Un\xi$ stabilisiert. Dann ist aber auch das Komplement S stabil unter T. Da S endlich ist und T zusammenhängend, sind die Elemente von S Fixpunkte unter T, d.h.

$$S \subseteq \{\xi, n\cdot\xi\}.$$

Wegen (*) gilt $\{\xi\} \subseteq S \subseteq \{\xi\}$, d.h. $S = \{\xi\}$. Es gilt also

$$Un\xi = \mathbf{B} - \{\xi\}.$$

Das ist aber die Aussage von (i): der Zerlegung von $\mathbf{B}$ in $\{\xi\}$ und $Un\xi$ entspricht gerade die Zerlegung von G in diejenigen Elemente g, welche ξ in die eine oder die andere Teilmenge von $\mathbf{B}$ abbilden. Genauer:

$$\begin{aligned} G &= \{g \in G \mid g\xi = \xi\} \vee \{g \in G \mid g\xi \in Un\xi\} \\ &= \{g \in G \mid gBg^{-1} = B\} \vee \{g \in G \mid gBg^{-1} = unGn^{-1}u^{-1} \text{ für ein } u \in U\} \\ &= N_G(B) \vee \{g \in G \mid (un)^{-1}g \in N_G(B) = B\} \\ &= B \vee \{g \in G \mid g \in unB \text{ für ein } u \in U\} \\ &= B \vee UnB \end{aligned}$$

Zu (iii). Die Menge $Un\xi = \mathbf{B} - \{\xi\}$ ist ein homogener Raum von U. Der Stabilisator von $n\xi$ ist gerade

$$U \cap nUn^{-1}$$

($un\xi = n\xi \Leftrightarrow n^{-1}un\xi = \xi \Leftrightarrow n^{-1}un \in N_G(B) = B \Leftrightarrow u \in nUn^{-1}$). Also gilt

$$U/U \cap nUn^{-1} \cong Un\xi = \text{offen und dicht in } G/B.$$

Insbesondere ist $\dim U/U \cap nUn^{-1} = 1$.

Zu (ii). Es gilt nach (iii)

$$\dim U/(U \cap nUn^{-1})^0 = \dim U/(U \cap nUn^{-1}) = 1.$$

Nach Übungsaufgabe 6.6(3) gilt für jede echte abgeschlossene zusammenhängende Untergruppe $H \subseteq G$ einer zusammenhängenden nilpotenten Gruppe G stets $\dim H < \dim N_G H$.[131] Im Fall $\dim G/H = 1$ ist

---

[131] Wegen der Nilpotenz gibt es eine zusammenhangende Untergruppe

$$H' \subseteq G \text{ mit } H' \supsetneq H \text{ und } (H', G) \subseteq H.$$

d.h. für $a \in H'$ und $g \in G$ gilt $aga^{-1}g^{-1} \in H$. Speziel ist für jedes $g := h \in H$ auch

$$aga^{-1} \in H,$$

d.h. H' liegt im Normalisator $N_G H$.

also H automatisch normal. Angewandt auf unsere Situation erhalten wir daraus, daß

$$(U \cap nUn^{-1})^0 \text{ normal in } U$$

ist. Diese Untergruppe wird auch normalisiert durch n (denn $\{B, nBn^{-1}\}$ ist das Orbit von B bei $W=\{e,\bar{n}\}$) und durch T (denn $\{B, nBn^{-1}\}$ sind die Fixpunkte von T). Also wird sie auch normalisiert von

$$B = U \cdot T \text{ und } nBn^{-1}.$$

Nun wird G nach 8.1.8 erzeugt von B und nBn^{-1}, d.h. $(U \cap nUn^{-1})^0$ ist normal in G. Damit gilt $(U \cap nUn^{-1})^0 \subseteq RG$. Trivialerweise gilt $RG \subseteq (B \cap nBn^{-1})^0$, zusammen also

$$(U \cap nUn^{-1})^0 \subseteq RG \subseteq (B \cap nBn^{-1})^0.$$

Die Gruppen in dieser Kette können sich in der Dimesion um höchstens 1 unterscheiden (wegen dim T =1)[132]. Also muß bei einer der beiden Inklusionen das Gleichheitszeichen gelten. Zum Beweis von (ii) genügt es also zu zeigen, $RG \neq (B \cap nBn^{-1})^0$. Dazu wiederum genügt es zu zeigen, T liegt nicht in RG. Wäre $T \subseteq RG$, so würden alle Konjugiert von T auch in RG liegen, also auch in $B \cap nBn^{-1}$, also auch in B. Dann würden aber auch alle Konjugierten von B den Torus T enthalten, d.h. es wäre

$$\mathbf{B}_T = \mathbf{B}.$$

Das ist aber nicht möglich, denn die Menge links ist endlich, und die rechts 1-dimensional.
QED.

8.2.4 Lemma 8.2.3: Die Zerlegung der Lie-Algebra

Sei G eine zusammenhängende halbeinfache nicht-auflösbare Gruppe vom Rang 1. Dann gilt mit den Bezeichnungen von 8.2.2:

(i) $Z_G T = T$ und $U \cap nUn^{-1} = \{e\}$.

(ii) Es gibt einen von Null verschiedenen rationalen Charakter $a: T \to G_m$ mit

$$\text{Lie}(G) = \text{Lie}(T) \oplus \text{Lie}(G)_\alpha \oplus \text{Lie}(G)_{-\alpha}.$$

---

[132] Es gilt

$$\begin{aligned}\dim (B \cap nBn^{-1})^0/(U \cap nUn^{-1})^0 &= \dim B \cap nBn^{-1}/U \cap nUn^{-1} \\ &= \dim UT \cap nUn^{-1}T/\ U \cap nUn^{-1} \quad (T \text{ ist max. Torus in B und } nBn^{-1}) \\ &= \dim (U \cap nUn^{-1})T/\ U \cap nUn^{-1} \leq \dim T = 1\end{aligned}$$

Dabei sei $\mathrm{Lie}(G)_\beta := \{X \in \mathrm{Lie}(G) \mid \mathrm{Ad}(t)X = \beta(t)X \text{ für alle } t \in T\}$. Die direkten Summanden der Zerlegung sind 1-dimensional und es gilt

$$\mathrm{Lie}(G)_\alpha = \mathrm{Lie}(U) \text{ und } \mathrm{Lie}(G)_{-\alpha} = \mathrm{Lie}(nUn^{-1}).$$

(iii) Die Abbildung $U \times B \to UnB = G\text{-}B$, $(u,b) \mapsto unb$, ist ein Isomorphismus von Varietäten.

Beweis. Zu (i). Da G halbeinfach ist, gilt $RG = \{e\}$. Nach 8.2.3(ii) ist deshalb

$$(U \cap nUn^{-1})^0 = RG = \{e\}.$$

Der Durchschnitt $U \cap nUn^{-1}$ ist deshalb endlich. Nach 8.2.3 ist $\dim U/(U \cap nUn^{-1}) = 1$, also gilt

$$\dim U = 1.$$

Die Produktabbildung $U \times T \to B$ ist nach 6.11 ein Isomorphismus. Wegen $\dim T = 1$ folgt

$$\dim B = 2.$$

Betrachten wir die Inklusionen

$$T \subseteq Z_G T \subseteq B.$$

Die linke Inklusion ist trivial. Die rechte folgt aus 7.3.6.[133] Die rechte Inklusion ist sogar echt, denn andernfalls wäre $B = Z_G T$ nilpotent (7.2.10), also nach 7.2.9 $G = B$, d.h. G wäre auflösbar im Widerspruch zu unseren Annahmen. Da sich T und B in der Dimension nur um 1 unterscheiden und $Z_G T$ zusammenhängend ist (7.3.5) folgt aus der Echtheit der rechten Inklusion, daß links das Gleichheitzeichen gelten muß:

$$T = Z_G T.$$

Damit ist der erste Teil von (i) bewiesen. Zum Beweis des verbleibenden Teils beachten wir, daß $\{B, nBn^{-1}\}$ nach 8.1.7 und 8.2.2 gerade die Menge der Fixpunkte von T auf der Varietät **B** der Borel-Untergruppen ist. Insbesondere operiert T (durch Konsjugation) auf B und auf nBn^{-1} also auch auf den Normalteilern U und nUn^{-1} von B bzw. nBn^{-1}, also auch auf

$$U \cap nUn^{-1}.$$

---

[133] Ist B eine Borel-Untergruppe mit $T \subset B$, so liegt auch die Cartan-Untergruppe $C = Z_G T$ ganz in B.

Letzterer Durchschnitt ist endlich (wie wir am Anfang des Beweises gesehen haben). Da T zusammenhängend ist, muß die Operation von T auf dieser Menge trivial sein, d.h. es gilt

$$U \cap nUn^{-1} \subseteq Z_G T = T.$$

Der Durchschnitt links besteht also aus unipotenten Elementen, die gleichzeitig halbeinfach sind. Also muß gelten $U \cap nUn^{-1} = \{e\}$.

Zu (ii). Wie wir in (i) gesehen haben, hat die unipotente Gruppe U die Dimension 1. Nach 2.6.6 gilt deshalb

$$U \cong G_a .$$

Wir fixieren einen Isomorphismus

$$x: G_a \to U.$$

Die Konjugation von Elementen aus T induziert eine Operation von T auf G_a. Da die Automorphismen von $G_a = \mathbb{A}^1$ durch lineare homogene Polynome des Grades 1 gegeben sind[134], ist dies eine Operation mit Hilfe eines Charakters, d.h. es gibt einen Charakter

$$\alpha: T \to G_m$$

mit

(1) $$x(\alpha(t)\xi) = t \cdot x(\xi) \cdot t^{-1} \text{ für alle } t \in T \text{ und alle } \xi \in G_a.$$

Die Operation von T auf U ist nicht-trivial (sonst wäre $U \subseteq Z_G T = T$, also $U=\{e\}$ im Widerspruch zu dim U =1), d.h. es gilt

$$\alpha \neq 0,$$

d.h. α ist nicht der triviale Charakter ξ a 1. Der Isomorphismus x induziert einen Isomorphismus der Lie-Algebren

$$dx: \mathrm{Lie}(G_a) \to \mathrm{Lie}(U).$$

Wegen (1) wirkt die Einschränkung der adjungierte Darstellung von G auf T auf der Teilalgebra L(U) = Im(dx) gerade durch Multiplikation mit dem Charakter α,[135]

$$\mathrm{Ad}(t)X = \alpha(t)X \text{ für } t \in T \text{ und } X \in \mathrm{Lie}(U) \ (\subseteq \mathrm{Lie}(G)).$$

Mit anderen Worten, es gilt

(2) $$\mathrm{Lie}(U) \subseteq \mathrm{Lie}(G)_\alpha .$$

Konjugation mit n bildet B auf nBn^{-1} ab. Also ist

$$\mathrm{Lie}(nBn^{-1}) = \mathrm{Ad}(n)\mathrm{Lie}(B)$$

---

[134] Linear, weil es sich um Isomorphismen handeln soll, homogen, weil es Automorphismen der algebraischen Gruppe sein sollen.

[135] Multiplikation mit $\alpha(t)$ ist eine lineare Abbildung, also gleich dem eigenen Differential.

und für $X \in Lie(B)$ und $t \in T$ gilt

$$\begin{aligned} Ad(t)Ad(n)X &= Ad(tn)X \\ &= Ad(nt^{-1})X \quad \text{(nach 8.2.2 (4) gilt } ntn^{-1} = t^{-1}\text{)} \\ &= Ad(n)Ad(t)^{-1}X \\ &= Ad(n)\alpha(t)^{-1}X \\ &= \alpha(t)^{-1}Ad(n)X. \end{aligned}$$

Wir haben gezeigt, es gilt

(3) $$Lie(nUn^{-1}) = Ad(n)Lie(B) \subseteq Lie(G)_{-\alpha}.$$

Schließtlich gilt, da T kommutativ ist,

(4) $$Lie(T) \subseteq Lie(G)_0$$

Damit haben wir Eigenräume von Lie(G) zu drei verschiedenen Charakteren gefunden,

(5) $$Lie(G)_\alpha \oplus Lie(T) \oplus Lie(G)_{-\alpha} \subseteq Lie(G).$$

Nach (2), (3) und (4) ist jeder dieser Eigenräume mindestens 1-dimensional. Zum Beweis von (ii) genügt es deshalb zu zeigen, daß G höchstens 3-dimensional ist (so daß in (2), (3), (4) und (5) das Gleichheitszeichen gilt).

Nach 8.2.3(i) gilt

$$G = B \cup UnB.$$

Wegen dim U = 1 und dim B = 2 folgt daraus aber gerade dim $G \leq 3$.

Zu (iii). Nach 8.2.3(i) ist die Abbildung

$$U \times B \to UnB = G\text{-}B,\ (u,b) \mapsto unb,$$

wohldefiniert. Durch Zusammensetzen mit den Isomorphismen

$$n^{-1}Un \times B \to U \times B,\ (v,b) \mapsto (nvn^{-1},b),$$

und

$$G \to G,\ g \mapsto n^{-1}g,$$

erhalten wir einen Morphismus

$$\varphi\colon nUn^{-1} \times B \to G\text{-}n^{-1}B,\ (v,b) \mapsto vb.$$

Es reicht zu zeigen, letzterer ist ein Isomorphismus. Sei $V := nUn^{-1}$. Wir führen auf Quelle und Ziel von φ folgende Operationen von $V \times B$ ein, bezüglich welcher φ offensichtliche äquivariant ist.

Operation von $V \times B$ auf sich:

$$(V \times B) \times (V \times B) \to V \times B,\ ((v',b'),(v,b)) \mapsto (v'v, bb'^{-1})$$

Operation von $V \times B$ auf G:

$$(V \times B) \times G \to G,\ ((v',b'), g) \mapsto v'gb'^{-1}$$

Operation von V×B auf G-nB: Es reicht zu zeigen, die letzte Operation überführt nB in sich. Wir haben zu zeigen, für b∈B, v'∈V, b'∈B gilt

$$v'nbb'^{-1}\in nB.$$

Wir schreiben $v'\in V = nUn^{-1}$ in der Gestalt $v' = nu'n^{-1}$ mit u'∈U. Dann gilt

$$v'nbb'^{-1} = nu'n^{-1}nbb'^{-1} = nu'bb'^{-1}\in nB.$$

Surjektivität von φ: Es gilt

$$Im(\varphi) = VB = nUn^{-1}B =^{136} n^{-1}UnB = G\text{-}n^{-1}B \quad \text{(vgl. 8.2.3(i))}.$$

Die Operation von V×B auf sich selbst ist offensichtlich transitiv, d.h. V×B ist ein homogener Raum. Dann ist aber auch $Im(\varphi) = G\text{-}n^{-1}B$ ein homogener Raum. Zum Beweis der Isomorphie von φ fehlen damit noch die folgenden Aussagen (vgl. 4.3.3(iii)).

1. φ ist bijektiv.
2. $T_e\varphi$ ist bijektiv.

Zu 1: Die Surjektivität von φ haben wir bereits gezeigt. Beweisen wir die Injektivität. Sei (v,b)∈V×B und φ(v, b) = e, d.h. vb = e. Dann gilt

$$v = b^{-1} \in B,$$

und weil $v \in V = n^{-1}Un$ unipotent ist, sogar

$$v = b^{-1} \in B_u = U.$$

Damit ist nach (i) auch

$$v \in V\cap U = n^{-1}Un\cap U = \{e\}$$

also v = e und $b = v^{-1} = e$.

Zu 2: Es gilt nach (ii)

$$Lie(V) = Lie(n^{-1}Un) = Lie(G)_{-\alpha}$$

$$Lie(B) = Lie(UT) = Lie(G)_{\alpha}\oplus Lie(T)$$

also

$$Lie(G) = Lie(G)_{-\alpha}\oplus Lie(T)\oplus Lie(G)_{\alpha} = Lie(V\times B).$$

Die durch φ:V×B→(G-nB), (v,b)avb, auf den Lie-Algebren induzierte Abbildung

$$d\varphi:Lie(V)\times Lie(B) \rightarrow Lie(G)$$

---

[136] Das Orbit von B bezüglich W(T) = {e,$\bar{n}$} ist gerade die Fixpunktmenge

$$\mathbf{B}_T = \{B, nBn^{-1}\}.$$

Nun ist $\bar{n} = \bar{n}^{-1}$, d.h. $nBn^{-1} = n^{-1}Bn$.

ist gerade die Addition. Identifiziert man Lie(V×B) mit der zugehörigen Teilalgebra von Lie(G), so wird diese Addition zur identischen Abbildung. Also ist dφ bijektiv.

QED.

8.2.5 Theorem 8.2.4: Klassifikation der halbeinfachen Gruppen vom Rang 1

Sei G eine zusammenhängende halbeinfache Gruppe vom Rang 1. Dann gilt $G \cong SL(2,k)$ oder $G \cong PSL(2,k)$.

Beweis. G ist nicht auflösbar, denn dann würde aus der Halbeinfachheit folgen G = {e} folgen, was mit dem Rang 1 nicht vereinbar ist. Wir fixieren folgende Daten.

T	ein maximaler Torus.
B	eine Boreluntergruppe mit $T \subseteq B$.
U	$:= B_u$ der unitpotente Teil von B
$y: G_m \to T$	einen Isomorphismus (existiert, weil G den Rang 1 hat)
$x: G_a \to U$	einen Isomorphismus (existiert nach 8.2.3(iii) und 8.2.4(i))
W	$:= N_G T / Z_G T$ die Weilgruppe zu T (hat die Ordnung 2 nach 8.2.2)
n	$\in N_G T - Z_G T$, Repräsentant eines Erzeugers von $W = \{e, \bar{n}\}$, vgl. 8.2.2

Der Torus T operiert durch einen Charakter auf U:

$$(1) \qquad y(\eta)x(\xi)y(\eta^{-1}) = x(\eta^a \cdot \xi) \text{ für } \eta \in k^*, \xi \in k$$

Die Operation von T auf B ist nicht-trivial, denn sonst wäre $U \subseteq Z_G T = T$, also U={e} im Widerspruch zu dim U =1). Also gilt $a \neq 0$. Wir können annehmen, es gilt

$$a > 0$$

(andernfalls könnten wir den Isomorphismus y abändern). Weiter ist nach 8.2.2(4):

$$(2) \qquad n \cdot y(\eta) \cdot n^{-1} = y(\eta^{-1}) \text{ für } \eta \in k^*$$

und, da die Weilgruppe die Ordnung 2 hat,

$$n^2 \in Z_G(T) = T.$$

Wir wählen ein $\varepsilon \in k^*$ derart, daß gilt

$$(3) \qquad n^2 = y(\varepsilon)$$

Damit gilt nach (2) und (3)

$$y(\varepsilon) = n y(\varepsilon) n^{-1} \text{ (nach (3))}$$

$= y(\varepsilon^{-1})$ (nach (2))

also

$y(\varepsilon) = y(\varepsilon^{-1})$

also

$$\boxed{(4) \qquad \varepsilon^2 = 1}$$

Die Isomophismen von 611(iv) und 8.2.4(iii) liefern einen Isomorphismus

(5) $G_a \times G_m \times G_a \to U \times B \to G\text{-}B,$

$(\xi,\eta,\zeta) \quad a \quad (x(\xi),y(\eta)x(\zeta)) \quad a \quad x(\xi)ny(\eta)x(\zeta).$

Bemerkungen zur Beweisidee

(i) Seien G eine (abstrakte) Gruppe, $N \subseteq G$ ein Normalteiler und $H \subseteq G$ eine Untergruppe derart, daß die Multiplikation

$$N \times H \to G, (n,h) \; a \; nh$$

bijektiv ist. Die Gruppenstruktur von G ist dann vollständig bestimmt, wenn wir die Gruppenstrukturen von N und H kennen und die Operation von H auf N durch Konjugation. G ist dann halbdirektes Produkt von N und H. Mit anderen Worten, um das Produkt von zwei Elementen nh und n'h' zu kennen,

$$(nh)(n'h') = (n(hn'h^{-1}))(hh'),$$

müssen wir die Multiplikation in jedem der Faktoren kennen und die Operation von H auf N durch Konjugation.

(ii) Die hier vorliegende Situation ist mit der eben geschilderten vergleichbar. Der Isormorphismus (5) definiert G im wesentlichen als Varietät (genauer eine offene dichte Teilmenge von G).

Zur Konstruktion eines Isomorphismus von G mit einer anderen Gruppe, werden wir diesen zunächst auf G-B definieren und dann zeigen, er läßt sich auf ganz G fortsetzen.

Dann haben wir zu zeigen, daß bei beiden Gruppen die Produktbildung in derselben Weise erfolgt. Zu diesem Zweck haben wir zu beschreiben, wie sich zwei Produkte der

(1) $$x(\xi)ny(\eta)x(\zeta)$$

multiplizieren (auf ganz G ergibt sich dann die Produktbildung durch Grenzübergang). Zur Beschreibung des Produkts zweier Elemente der Gestalt (1) benötigen wir folgende Daten:

1. Die Beschreibung der Produktbildung von je zwei $x(\xi)$ und $y(\eta)$.
2. Die Beschreibung der Operation der $y(\eta)$ auf den $x(\xi)$ durch Konjugation (d.h. der Art wie die $x(\xi)$ mit den $y(\eta)$ kommutieren, vgl. (1)).

3. Die Beschreibung der Operation von n auf den $y(\eta)$ durch Konjugation (vgl. (2)).
4. Die Beschreibung der Operation von n auf den $x(\xi)$ durch Konjugation.

   Mit Ausnahme von 4. haben wir bereits alle diese Daten (abgesehen von der konkreten Bestimmung der Zahlen a und ε). Der nachfolgende Beweis wird im wesentlichen in der Suche nach der konkreten Beschreibung der Konjugation von n auf den $x(\xi)$ bestehen.

Wir betrachten jetzt die algebraische Varietät G_m als offene Teilvarietät von G_a und betrachten ein Element

$$\xi \in G_a - \{0\} = G_m .$$

Nach 8.2.4(i) ist $U \cap nUn^{-1} = \{e\}$. Deshalb gilt $nx(\xi)n^{-1} \notin U$. Da das Element $nx(\xi)n^{-1}$ unipotent ist, folgt damit sogar

(6) $$nx(\xi)n^{-1} \notin B.$$

Mit anderen Worten es gilt $nx(\xi)n^{-1} \in G\text{-}B$. Wegen des Isomorphismus (5) gibt es reguläre Funktionen f,g,h auf $G_m (\subseteq G_a)$

$$f: G_m \to G_a,\ g: G_m \to G_m,\ h: G_m \to G_a$$

mit

(7) $$nx(\xi)n^{-1} = x(f(\xi))ny(g(\xi))x(h(\xi)) \text{ für } \xi \neq 0.$$

Die Funktionen f,g,h sind durch diese Bedingung eindeutig bestimmt.

Bemerkung
Wie auf Grund der obigen Bemerkungen zu erwarten ist, wird die Gruppenstruktur von G durch die Formeln (1), (2), (3) und (7) eindeutig bestimmt[137], d.h. sie ist festgelegt durch die Konstanten $a \in N$ und $\varepsilon = \pm 1$ und die Funktionen f, g und h.

Um die Funktionen f, g und h genauer zu bestimmen, konjugieren wir jetzt beide Seiten von (7) mit $y(\eta)$. Wir erhalten:

<u>LHS von $y(\eta)(7)y(\eta)^{-1}$</u>:

$$y(\eta)nx(\xi)n^{-1}y(\eta)^{-1} = y(\eta)nx(\xi)n^{-1}y(\eta^{-1})$$

---

[137] Zusammen mit der Forderung der Stetigkeit dieser Operationen.

$= ny(\eta^{-1})x(\xi)y(\eta)n^{-1}$ (nach (2))

$= n \cdot x(\eta^{-a} \cdot \xi) \cdot n^{-1}$ (nach (1))

$= x(f(\eta^{-a} \cdot \xi))ny(g(\eta^{-a} \cdot \xi))x(h(\eta^{-a} \cdot \xi))$ (nach (7)).

RHS von $y(\eta)(7)y(\eta)^{-1}$:

$y(\eta)x(f(\xi))ny(g(\xi))x(h(\xi))y(\eta)^{-1}$

$= x(\eta^a \cdot f(\xi))y(\eta)ny(g(\xi))y(\eta)^{-1}\ x(\eta^a \cdot h(\xi))$ (nach (1))

$= x(\eta^a \cdot f(\xi)) \cdot n \cdot y(\eta^{-1})y(g(\xi))y(\eta)^{-1}\ x(\eta^a \cdot h(\xi))$ (nach (2))

$= x(\eta^a \cdot f(\xi)) \cdot n \cdot y(\eta^{-2} \cdot g(\xi)) \cdot x(\eta^a \cdot h(\xi))$

Vergleich der beiden Seiten liefert, da f,g,h durch (7) eindeutig bestimmt sind,

(8a) $f(\eta^{-a} \cdot \xi) = \eta^a \cdot f(\xi)$

(8b) $g(\eta^{-a} \cdot \xi) = \eta^{-2} \cdot g(\xi)$

(8c) $h(\eta^{-a} \cdot \xi) = \eta^a \cdot h(\xi)$

für alle $\xi, \eta \in k^*$. Nun sind f,g,h reguläre Funktionen auf G_m, d.h. Elemente von

$$k[G_m] = k[\xi, \xi^{-1}].$$

Die Relationen (8) implizieren, daß es sich um homogene Elemente handelt:

(9a) $f(\xi) = \alpha \cdot \xi^{-1}$

(9b) $h(\xi) = \beta \cdot \xi^{-1}$

Aus (8b) erhalten wir, indem wir $\xi=1$ setzen $\eta^{-2} \cdot g(1) = g(\eta^{-a})$, also

(9c) $g(\eta^{-a}) = \eta^{-2} \cdot g(1)$, a= 1 oder 2, g homogen.[138]

Um weitere Relationen für f,g,h zu erhalten, ersetzen wir beide Seiten von (7) durch ihr Inverses. Wir erhalten

LHS von $(7)^{-1}$:

$nx(-\xi)n^{-1} = x(f(-\xi))ny(g(-\xi))x(h(-\xi))$

RHS von $(7)^{-1}$:

$x(h(\xi))^{-1}y(g(\xi))^{-1}n^{-1}x(f(\xi))^{-1}$

$= x(-h(\xi))y(g(\xi)^{-1})n^{-1}x(-f(\xi))$

---

[138] Weil $g(\xi)$ das Vielfache einer ganzzahligen Potenz von ξ ist, gilt a|2. Wegen $a > 0$ nach Konstruktion (siehe die Bemerkungen nach Formel (1), folgt $a = 1$ oder $a = 2$.

$= x(-h(\xi))n^{-1}y(g(\xi))x(-f(\xi))$ (nach (2))
$= x(-h(\xi))ny(\varepsilon g(\xi))x(-f(\xi))$ (nach (4) und (3))

Vergleich der beiden Seiten liefert

$f(-\xi) = -h(\xi)$
$g(-\xi) = \varepsilon g(\xi)$
$h(-\xi) = -f(\xi)$

Zusammen mit (9) ergibt sich daraus:

(10) $\alpha = \beta$ und $g(-\xi) = \varepsilon g(\xi)$

Wir unterscheiden jetzt vorübergehend die beiden Fäll a=1 und a=2.

1. Fall a=1. Aus (9c) folgt $g(\eta^{-1}) = \eta^{-2}\cdot g(1)$ also

(11') $g(\eta) = \gamma\cdot\eta^2$ für ein $\gamma\in k^*$

Aus (10) erhalten wir $\gamma\cdot\eta^2 = \varepsilon\cdot\gamma\cdot\eta^2$ also

(12') $\varepsilon = 1$.

2. Fall a=2. Aus (9c) folgt $g(\eta^{-2}) = \eta^{-2}\cdot g(1)$ also

(11") $g(\eta) = \gamma\cdot\eta$ für ein $\gamma\in k^*$

Aus (10) erhalten wir $\gamma\cdot(-\eta) = \varepsilon\cdot\gamma\cdot\eta$ also

(12") $\varepsilon = -1$.

Wir behandeln jetzt wieder die beiden Fälle a=1 und a=2 gemeinsam. Wir zeigen als nächstes:

Durch Ersetzen von n durch $n\cdot y(\lambda)$ mit geeigneten $\lambda\in k^*$ kann man erreichen, daß

(13) $\alpha = \beta = -1$

gilt.

Die Konjugation von $x(\xi)$ mit einem Element der Gestalt $y(\lambda)$ entspricht nach (1) der Multiplikation von ξ mit λ^a. Setzt man

$$n\cdot y(\lambda) = n'$$

d.h. $n = n'\, y(\lambda^{-1})$ Formel (7) ein, so erhält man damit also

$$n'x(\lambda^{-a}\xi)n'^{-1} = x(f(\xi))n'y(\lambda^{-1}g(\xi))x(h(\xi)) \text{ für } \xi\neq 0.$$

d.h.

$$n'x(\xi)n'^{-1} = x(f(\lambda^a\xi))n'y(\lambda^{-1}g(\lambda^a\xi))x(h(\lambda^a\xi)) \text{ für } \xi\neq 0.$$

Durch geeignete Wahl von λ können wir erreichen, daß die Koeffizienten der neue homogenen Funktionen (des Grades -1)

$$f'(\xi) = f(\lambda^a\xi) \text{ und } h'(\xi) = h(\lambda^a\xi)$$

den Koeffizienten -1 haben, d.h. wir können annehmen, es gilt (13). Relation (7) nimmt damit die folgende Gestalt an.

(14) $nx(\xi)n^{-1} = x(-\xi^{-1})ny(g(\xi))x(-\xi^{-1})$ für $\xi\neq 0$.

Dabei ist

$$(15)\qquad g(\xi) = \begin{cases} \gamma\xi^2 \text{ falls } a = 1 \\ \gamma\xi \text{ falls } a = 2 \end{cases} \quad \text{mit einem } \gamma \in k^*$$

und (vgl. 12') und (12")

$$(16)\qquad \varepsilon = \begin{cases} 1 \text{ falls } a = 1 \\ -1 \text{ falls } a = 2 \end{cases}$$

Es fehlt uns noch eine genauere Bestimmung des Koeffizienten γ. Dazu nehmen wir jetzt an, ξ ist ungleich 0 und -1 und wenden Formel (14) für ξ und $\xi+1$ und 1 an. Genauer, wir setzen die entsprechenden rechten Seiten von (14) in die Relation

$$nx(\xi+1)n^{-1} = nx(\xi)n^{-1} \cdot nx(1)n^{-1}$$

ein und erhalten

$$x(-(\xi+1)^{-1})ny(g(\xi+1))x(-(\xi+1)^{-1})$$
$$= x(-\xi^{-1})ny(g(\xi))x(-\xi^{-1}) \cdot x(-1)ny(g(1))x(-1)$$

also

$$x(-(\xi+1)^{-1} + \xi^{-1})ny(g(\xi+1))x(-(\xi+1)^{-1}+1)$$
$$= ny(g(\xi))x(-\xi^{-1}) \cdot x(-1)ny(g(1))$$
$$= ny(g(\xi))x(-\xi^{-1}-1)ny(g(1))$$
$$= nx(-g(\xi)^a(\xi^{-1}+1))y(g(\xi))ny(g(1))$$
$$= nx(-g(\xi)^a(\xi^{-1}+1))ny(g(\xi)^{-1})y(g(1)) \quad \text{(nach (2))}$$
$$= nx(-g(\xi)^a(\xi^{-1}+1))ny(g(\xi)^{-1}g(1))$$

also

$$x(-(\xi+1)^{-1} + \xi^{-1})ny(g(\xi+1))x(-(\xi+1)^{-1}+1)y(g(\xi)^{-1}g(1))^{-1}$$
$$= nx(-g(\xi)^a(\xi^{-1}+1))n$$

also

$$nx(-g(\xi)^a(\xi^{-1}+1))n$$
$$= x(-(\xi+1)^{-1} + \xi^{-1})ny(g(\xi+1))x(-(\xi+1)^{-1}+1)y(g(\xi)/g(1))$$
$$= x(-(\xi+1)^{-1}+\xi^{-1})ny(g(\xi+1))y(\frac{g(\xi)}{g(1)})x((\frac{g(\xi)}{g(1)})^{-a}(1-(\xi+1)^{-1}))$$
$$= x(-(\xi+1)^{-1}+\xi^{-1})ny(g(\xi+1)\frac{g(\xi)}{g(1)})x((\frac{g(\xi)}{g(1)})^{-a}(1-(\xi+1)^{-1}))$$
$$= x(-(\xi+1)^{-1}+\xi^{-1})ny(g(\xi+1)\frac{g(\xi)}{g(1)})x((\frac{g(\xi)}{g(1)})^{-a}(\xi/(1+\xi)))$$

also

$$nx(-g(\xi)^a(\xi^{-1}+1))n^{-1}$$

$$= x(-(\xi+1)^{-1}+\xi^{-1})ny(g(\xi+1)\frac{g(\xi)}{g(1)})x((\frac{g(\xi)}{g(1)})^{-a}(\xi/(1+\xi)))n^{-2}$$

$$= x(-(\xi+1)^{-1}+\xi^{-1})ny(g(\xi+1)\frac{g(\xi)}{g(1)})x((\frac{g(\xi)}{g(1)})^{-a}(\xi/(1+\xi)))y(\varepsilon^{-2})$$

$$= x(-(\xi+1)^{-1}+\xi^{-1})ny(g(\xi+1)\frac{g(\xi)}{g(1)})\ y(\varepsilon^{-2})x((\frac{g(\xi)}{\varepsilon^2 g(1)})^{-a}(\xi/(1+\xi)))$$

$$= x(-(\xi+1)^{-1}+\xi^{-1})ny(g(\xi+1)\frac{g(\xi)}{\varepsilon^2 g(1)})x((\frac{g(\xi)}{\varepsilon^2 g(1)})^{-a}(\xi/(1+\xi)))$$

Vergleich liefert

$$-(-g(\xi)^a(\xi^{-1}+1))^{-1} = -(\xi+1)^{-1}+\xi^{-1}$$

d,h.

$$-(\xi+1)^{-1}+\xi^{-1} \quad = g(\xi)^{-a}(\xi^{-1}+1)^{-1}$$

Wir multiplizieren mit $\xi(\xi+1)$ und erhalten

$$-\xi+(\xi+1) \quad = g(\xi)^{-a}\frac{\xi(\xi+1)}{\xi^{-1}+1} = g(\xi)^{-a}.\xi^2$$

d.h.

(17) $\qquad g(\xi)^a \quad = \xi^2$

Für den weiteren Beweis unterscheiden wir die Fälle a = 1 und a = 2.

1. Fall: a = 2. Wir haben $g(\xi) = \gamma\xi$ und $\varepsilon = -1$. Nach (17) ist

$$\gamma^2 = 1.$$

Wenn wir in Formel (14) das Element n durch $ny(\gamma)$ ersetzen, so nimmt diese die folgende Gestalt an.

$$ny(\gamma)x(\xi)\ y(\gamma)n^{-1} = x(-\xi^{-1})ny(\gamma g(\xi))x(-\xi^{-1}) \text{ für } \xi\neq 0.$$

Die linke Seite ist nach Formel (1) gleich

$$nx(\gamma^2\xi)n^{-1} = nx(\xi)n^{-1}$$

Mit anderen Worten, wir können durch diese Substitution erreichen, daß $\gamma = 1$ gilt. O.B.d.A. sei also $g(\xi) = \xi$, Formel (14) bekommt dann die Gestalt

(18) $\qquad nx(\xi)n^{-1} = x(-\xi^{-1})ny(\xi)x(-\xi^{-1})$ für $\xi\neq 0$, $n = y(-1)$.

Betrachten wir die Abbildung

$$\phi: G \to SL_2$$

mit

$$\phi|_B : x(\xi)y(\eta) \mapsto \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{pmatrix}$$

und

$$\phi|_{G\text{-}B}: x(\xi)ny(\eta)x(\zeta) \mapsto \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{pmatrix}\begin{pmatrix} 1 & \zeta \\ 0 & 1 \end{pmatrix}$$

Formel (18)ist dann das exakte Gegenstück zur folgenden in SL_2 geltenden Formel.

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -\xi^{-1} \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}\begin{pmatrix} 1 & -\xi^{-1} \\ 0 & 1 \end{pmatrix}$$

Die Multiplikation der abstrakten Gruppe G ist durch (18) und die anderen oben angegebenen Multiplikationsregeln vollständig bestimmt. Die analoge Aussage gilt für SL_2. Deshalb definiert ϕ einen Isomorphismus abstrakter Gruppen. Dieser ist eine Isomorphismus algebraischer Varietäten auf G - B.
Da ϕ ein Isormophismus abstrakter Gruppen ist, ist ϕ auch auf jeder Verschiebung von G-B eine Isomorphismus algebraischer Varietäten.[139] Da dieser Verschiebungen G überdecken ist ϕ auf ganz G ein Isormophismus algebraischer Varietäten.

2. Fall a = 1. In diesem Fall gilt $g(\xi) = \xi$ und $\varepsilon = 1$.
Formel (14) bekommt damit die Gestalt

(19) $$nx(\xi)n^{-1} = x(-\xi^{-1})ny(g(\xi))x(-\xi^{-1}) \text{ für } \xi \neq 0.$$

und es ist $n^2 = y(1) = e$. Wir schreiben den Koordinatenring von SL_2 in der Gestalt

$$k[SL_2] = k[T_1,T_2,T_3T_4]/(T_1T_4-T_2T_3-1) = k[t_1,t_2,t_3t_4].$$

Der Koordinatenring von PSL_2 ist nach Aufgabe 2.1.4(3) die Teilalgebra

$$k[PSL_2] \subseteq k[SL_2]$$

die von den Produkten t_it_j mit $1 \leq i,j \leq 4$ erzeugt wird, oder, anders ausgedrückt, die Invariantenalgebra bezüglich der Substitution

$$X \mapsto -X,$$

d.h. nach Definition ist

---

[139] Man kann ϕ auf jeder Verschiebung schreiben als Zusammensetzung einer Verschiebung in G, der Einschränkung von ϕ auf G-B und einer Verschiebung in SL_2.

$$PSL_2 = SL_2/\{\pm Id\} =^{140} SL_2/Z(SL_2)$$

Eine andere Beschreibung der PSL_2 ist die folgende. Die Adjungierte Darstellung von SL_2 definiert einen Homomorphismus algebraischer Gruppen

$$\rho: SL_2 \to Aut(sl_2),\ g \mapsto (X \mapsto gXg^{-1}).$$

Dabei sei sl_2 die Lie-Algebra von SL_2 der 2×2-Matrizen mit der Spur 0. Der Kern dieser Abbildung ist gerade das Zentrum von SL_2, d.h. das Bild ist PSL_2. Das Bild von

$$g = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$$

bei ρ hat bezüglich der Basis

$$e_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ e_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ e_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

die Matrix

$$\rho(g) = \begin{pmatrix} x_1x_4+x_2x_3 & -x_1x_3 & x_2x_4 \\ -2x_1x_2 & x_1^2 & -x_2^2 \\ 2x_3x_4 & -x_3^2 & x_4^2 \end{pmatrix}$$

Wir definieren eine Abbildung

$$\phi: G \to PSL_2$$

mit

$$\phi|_B : x(\xi)y(\eta) \mapsto \rho\left(\begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{pmatrix}\right)$$

und

$$\phi|_{G-B}: x(\xi)ny(\eta)x(\zeta) \mapsto \rho\left(\begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{pmatrix}\begin{pmatrix} 1 & \zeta \\ 0 & 1 \end{pmatrix}\right).$$

Wie im vorangehenden Fall zeigt man, daß ϕ ein Isomorphismus algebraischer Gruppen ist. Die Einzelheiten seien dem Leser überlassen.

QED.

---

[140] Liegt $A \in SL_2$ im Zentrum von SL_2, so auch im Zentrum von GL_2 (da jede umkehrbare Matrix Vielfaches einer Matrix von SL_2 ist), d.h. es gilt $A = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ mit $\lambda^2 = 1$, d.h. $\lambda = \pm 1$.

8.2.6 Aufgaben 8.2.5

(1) Sei G wie in 8.2.5. Man zeige, G hat keinen echten abgeschlossenen Normalteiler einer Dimension > 0. Insbesondere gilt $G = (G,G)$ (Kommutator-Untergruppe) und PSL_2 ist einfach (als algebraische Gruppe).

(2) Sei ρ eine nicht-triviale rationale Darstellung von SL_2. Dann ist

$$\operatorname{Im} \rho$$

isomorph zu SL_2 oder PSL_2.

(3) Man zeige, jede 2-dimensionale zusammenhängende lineare algebraische Gruppe ist auflösbar.

Zu (1).

Angenommen G hat einen echten abgeschlossenen Normalteiler $N \subset G$ positiver Dimension. Wir können annehmen, N ist zusammenhängen,

$$N = N^0.$$

Es reicht zu zeigen, daß in dieser Situation N auflösbar sein muß, denn das steht im Widerspruch dazu, daß das Radikal (d.h. der größte auflösbare Normalteiler) der halbeinfachen Gruppe G trivial ist.
Nacht 8.2.5 gilt

$$\dim G = 3$$

also $\dim N \leq 2$, d.h.

$$\dim N = 1 \text{ oder } \dim N = 2.$$

Im ersten Fall ist $N = G_a$ oder $N = G_m$, d.h. N ist auflösbar. Im zweiten Fall ist N auflösbar nach Aufgabe (3).

Zu G = (G,G).

Mit G ist (G,G) zusammenhängend. Wäre (G,G) null-dimensional, so wäre $(G,G) = \{e\}$, d.h. G kommutativ, was nach 8.2.5 nicht der Fall ist. Also ist $\dim (G, G) > 0$. Nach dem eben bewiesenen Ergebnis ist dann aber $(G,G) = G$.

Zur Einfachheit der PSL_2.

Es reicht zu zeigen, der einzige echte Normalteiler von

$$G = SL_2$$

ist $\{\pm Id\}$. Sei N ein echter Normalteiler der SL_2. Wie gerade bewiesen ist dann N endlich,

$$\# N < \infty.$$

Beweisidee: man zeige, G/N genügt den Bedingungen von 8.2.5 ist somit gleich SL_2 oder PSL_2.

Behauptung 1: $\operatorname{rk} G/N = 1$.

Da natürliche Bild eines Torus von G in G/N ist ein Torus. Deshalb gilt

$$\text{rk } G/N \geq 1.$$

Angenommen,

$$\text{rk } G/N > 1.$$

Dann gibt es einen maximalen Torus

$$T' \subset G/N \text{ mit } \dim T' \geq 2.$$

Sei $B' \subseteq G/N$ eine Borel-Untergruppe mit $T' \subseteq B'$. Dann kann nicht

$$T' = B'$$

gelten, denn dann wäre B' auflösbar, also $T' = B' = G/N$, d.h.G/N wäre kommutativ, d.h. $(G,G) \subseteq N$ = endlich, was nicht der Fall ist. Also gilt

$$T' \neq B'$$

also $\dim B' > \dim T' \geq 2$, also $B' = G/N$, d.h. G/N ist auflösbar. Es reicht also zu zeigen:

Behauptung 2: G/N ist nicht auflösbar.

Angenommen G/N ist auflösbar. Sei T' ein maximaler Torus von G/N. Wie oben sieht man,

$$T' \neq G/N$$

(denn sonst wäre G/N kommutativ, also $(G,G) \subseteq N$). Dann ist aber der unipotente Anteil

$$U' = (G/N)_u$$

ein (zusammenhängender) Normalteiler G/N der Dimension

$$\dim U' = \dim G/N - \dim T' = \dim G - \dim T' < \dim G$$

Das vollständige Urbild in G ist ein Normalteiler positiver Dimension von G, also nach (1) gleich G. Das ist aber wegen $\dim U' < \dim G$ nicht möglich. Wir haben gezeigt, G/N ist nicht auflösbar.

Behauptung 3. G/N ist halbeinfach

Andernfalls ware R(G/N) ein nicht-trivialer zusammenhängender Normalteiler positiver Dimension. Das vollständige Urbild in G müßte (wie oben gezeigt) gleich G sein, d.h.

$$\dim R(G/N) = \dim G = \dim G/N,$$

d.h. $G/N = R(G/B)$ wäre auflösbar, im Widerspruch zu Behauptung 2.

Zusammenfassung.

Wir haben gezeigt, G/N genügt den Bedingungen von 8.2.5, d.h. es gibt einen Isomorphismus

$$G/N \to SL_2 \text{ bzw. } G/B \to PSL_2$$

Zur Konstruktion können wir das Bild einer Borel-Untergruppe $B \subseteq G$ und das Bild eines maximalen Torus $T \subseteq B$ und das Bild eines Repräsentanten $n \in Z_G(T)$ des nicht-trivialen Erzeugers der Weyl-Gruppe von G nehmen. Durch Vergleich mit den entsprechenden Isomorphismen für G sehen wir, daß

$$N \subseteq \{\pm Id\}$$

gelten muß.

Zu (2).

Folgt aus den Argumenten mit denen die Einfachheit von PSL_2 bewiesen wurde.

Zu (3).

Angenommen G ist nicht auflösbar.

Wegen dim G = 2 hat G einen Rang ≤ 2. Im Fall rk G = 2 ist G ein Torus, also auflösbar. Im Fall rk G = 1 gilt nach 8.2.3 für jede Borel-Untergruppe

$$B = U \times T,\ U = B_u,\ T \text{ ein maximaler Torus},$$

daß dim U ≥ 1 ist, also dim B ≥ 2, also G = B, d.h. G ist auflösbar.
Bleibt noch der Fall rk G = 0 zu betrachten. Dann gilt für jeden maximalen Torus T,

$$T = \{e\}$$

und für jede Boreluntergruppe B,

$$B = B_u,$$

d.h. B ist nilpotent. Dann ist aber G = B (nach 7.2.9), d.h. G ist auflösbar.

8.2.7 Folgerungen (p. 181)

Wir leiten jetzt einige Folgerungen aus dem Klassifikationssatz 8.2.5 ab, die wir im nächsten Kapitel benötigen. Wir betrachten die folgende Situation.

G sei zusammenhängende reduktive Gruppe vom halbeinfachen Rang 1, d.h.

$$rk(G/RG)=1.$$

Das Radikal von G ist dann ein Torus[141] C. Es gilt

(i) $C := RG = Z(G)^0$ ist ein Torus.
(ii) G/C ist halbeinfach vom Rang 1.
(iii) $(G,G) \cap C$ ist endlich.
(iv) G/C = (G/C, G/C).
(v) (G,G) ist zusammenhängend und halbeinfach von Rang 1.
(vi) $(G,G) = SL_2$ oder $= PSL_2$.
(vii) Seien

[141] Nach Definition ist RG ein auflösbarer Normalteiler. Der unipotente Teil von RG ist damit ebensfalls ein Normalteiler, liegt also im unipotenten Radikal und ist damit, da G reduduktiv sein soll, trivial. Nach 6.11 ist dann aber RG ein Torus.

$$T_1 \subseteq G_1 := (G,G)$$

ein maximaler Torus der Kommutator-Untergruppe und

$$T \subseteq G$$

ein maximaler Torus von G mit

$$T_1 \subseteq T,$$

Dann gibt es einen nicht-trivialen Charakter

$$\alpha: T \to G_m.$$

mit

$$L(G) = L(G)_\alpha \oplus L(T) \oplus L(G)_{-\alpha}$$

und

$$\alpha(C) = 1.$$

Dabei sind die Eigenräume zu α und $-\alpha$ eindimensional,

$$\dim L(G)_\alpha = \dim L(G)_{-\alpha} = 1.$$

Beweis. Zu (i). Das erste Gleichheitszeichen gilt nach Definition. Das zweite ergibt sich wie folgt. Es gilt

$$Z_G(C)^0 = N_G(C)^0 = G$$

Das erste Gleichheitszeichen ergibt sich aus 2.5.11, das zweite Gleichheitszeichen gilt, weil C = RG ein Normalteiler ist. Sämtliche Elemente von G zentralisieren also C, d.h. $C \subseteq Z(G)^0$. Da $Z(G)^0$ ein auflösbarer Normalteiler von G ist, gilt aber auch $Z(G)^0 \subseteq RG = C$. Also gilt überall das Gleichheitszeichen.

Zu (ii). Hätte G/C einen echten auflösbaren Normalteiler, so wäre dessen Urbild in G ein auflösbarer Normalteiler, der echt größer ist als C = RG, im Widerspruch zur Definition des Radikals RG. Die Rangaussage ist einfach eine der Voraussetzungen.

Zu (iii). siehe 6.15.

Zu (iv). siehe Aufgabe 8.2.5 (1).

Zu (v). (G,G) ist zusammenhängend nach (6.3). Der Morphismus (G,G)ÆG/C hat nach (3) endliche Fasern und ist surjektiv nach (iv). Da G/C halbeinfach ist, muß damit auch (G,G) halbeinfach sein.[142] Weiter gilt auf Grund des endlichen Kerns dieses Homomorphismus und nach (2),

$$\text{rk } (G,G) \leq \text{rk } G/C = 1.$$

Es gilt auch die umgekehrte Inklusion:

Im Fall rk (G,G) = 0 wären die Borel-Untergruppen B von (G,G) unipotent, also nach 7.2.9 wäre B = (G,G), d.h. (G,G) wäre auflösbar.

---

[142] Andernfalls hätte (G,G) einen zusammenhängenden auflösbaren Normalteiler positiver Dimension. Dessen Bild in G/C wäre ebenfalls ein solcher (weil der Kern endlich ist). Das ist aber nicht möglich, weil G/C halbeinfach ist nach (2).

Dann wäre aber auch G auflösbar, also auch G/C. Das steht aber im Widerspruch zu (2)(vgl. den Klassifikationssatz 8.2.5)
Zu (vi). Folgt aus (v) und dem Klassifikationssatz 8.2.5.
Zu (vii). Sei $B_1 \subseteq G_1 := (G,G)$ eine Borel-Untergruppe, die T_1 enthält und

$$x: G_a \to (B_1)_u =: U_1$$

ein Isomorphismus.

Nach 8.2.4 gibt es einen nicht-trivialen rationalen Charakter

$$\alpha: T_1 \to G_m$$

von T_1 mit

$$(1) \qquad L(G_1) = L(G_1)_\alpha \oplus L(T_1) \oplus L(G_1)_{-\alpha} .$$

wobei alle drei Eigenräume 1-dimensional sind. Die Multiplikation mit $\alpha(t)$, $t \in T_1$, entspricht beim Isomorphismus x gerade der Konjugation mit t. Der Charakter α läßt sich fortsetzen zu einem (nicht-trivialen) Charakter[143]

$$\alpha; T \to G_m.$$

Die natürliche Inklusion

$$G_1 \subseteq G$$

induziert Inklusionen von Lie-Algebren

$$L(G_1) = L(G_1)_\alpha \oplus L(T_1) \oplus L(G_1)_{-\alpha} \subseteq L(G)_\alpha \oplus L(T) \oplus L(G)_{-\alpha} \subseteq L(G).$$

Zum Beweis der Behauptung reicht es zu zeigen,

$$\dim L(G_1)_\alpha \oplus L(T) \oplus L(G_1)_{-\alpha} \geq \dim L(G),$$

d.h.

$$\dim G/T \leq 2.$$

Da T ein maximaler Torus von G und $C = R(G)$ ein Torus ist, folgt $C \subseteq T$. Wegen (iv) besteht eine Surjektion

---

[143] U_1 bildet sich injektiv nach G/C ab. Bei der Surjection
$(G,G) \to G/C$
wird der maximale Torus T mit $T_1 \subseteq T$ in einen Torus, der das Bild von T_1 enthält abgebildet. Da G/C den Rang 1 hat, ist dieser Torus gleich dem Bild von T_1, d.h.

$$T = C \cdot T_1.$$

Die Konjugation mit Elementen aus T induziert deshalb auf $U_1 \subseteq G/C$ eine Operation, die die Konjugation mit Elementen aus T_1 fortsetzt. Man beachte, die Elemente von C operieren dabei trivial auf U_1.

$$G_1 = (G,G) \to G/C \to G/T$$

und wegen $T_1 \subseteq T$ liegt T_1 im Kern dieser Surjektion, d.h. es besteht eine Surjektion

$$G_1/T_1 \to G/T.$$

Deshalb gilt wegen (1)

$$\dim G/T \leq \dim G_1/T_1 = \dim L(G_1)_\alpha \oplus L(G_1)_{-\alpha} = 2.$$

QED.

Bemerkung

Sei

$$y: G_m \to T_1$$

ein Isomorphismus algebraischer Gruppen und sei α der Charakter von 8.2.7. Wir betrachten y als 1-Parameter-Untergruppe von T, sodaß wir das Skalarprodukt von y mit α bilden können. Dann gilt

$$<\alpha, y> = \pm 1 \text{ oder } \pm 2.$$

je nachdem ob G/R(G) isomorph ist zu PSL_2 oder SL_2.

Beweis. Sei

$$x: G_m \to T_1$$

der zur Definition des Charakters α verwendete Isomorphismus. Dann entspricht die Multiplikation mit $\alpha(t)$ gerade der Konjugation mit t. Für $t = y(\eta) \in T_1$ ist damit

$$x(\alpha(y(\eta))\xi) = x(\alpha(t)\xi) = tx(\xi)t^{-1} = y(\eta)x(\xi)y(\eta)^{-1} = x(\eta^a\xi)$$

(vgl. die Formel (1) im Beweis von 8.2.5). Dabei gilt

$$a = \pm 1 \text{ oder } \pm 2$$

je nachdem ob G/R(G) isomorph ist zu PSL_2 oder SL_2. Da x ein Isomorphismus ist, folgt

$$\alpha(y(\eta)) = \eta^a,$$

d.h.

$$<\alpha, y> = \pm 1 \text{ oder } \pm 2.$$

QED.

8.2.8 Bezeichnung: Die orthogonale Transformation s

G sei zusammenhängende reduktive Gruppe vom halbeinfachen Rang 1, d.h.

$$rk(G/RG)=1.$$

Wir verwenden die Bezeichnungen von 8.2.7. Weiter sei

$$n \in N_{(G,G)}(T_1) - T_1$$

ein Repräsentant des nicht-trivialen Elements der Weyl-Gruppe von (G,G) und

$$s: T \to T,\ t \mapsto ntn^{-1}$$

die Konjugation mit n. Dann operiert s auf $X := X(T)$ und $X^v = X^v(T)$ durch

$$(s\cdot x)(t) := x(s^{-1}(t)) \quad \text{für } x\in X$$
$$(s\cdot x^v)(\xi) := s(x^v(\xi)) \quad \text{für } x^v\in X^v.$$

Nach Konstruktion gilt $(s\cdot x)\circ(s\cdot x^v) = x\circ x^v$, d.h.

$$< s\cdot x , s\cdot x^v> = < x, x^v> \text{ für } x\in X \text{ und } x^v\in X^v,$$

d.h. s ist für die natürliche Paarung auf $X\times X^v$ eine "orthogonale" Transformation.

8.2.9 Lemma:Eigenschaften von s,die Homomorphismen x_α

G sei zusammenhängende reduktive Gruppe vom halbeinfachen Rang 1. Dann gilt mit den Bezeichnungen von 8.2.8 bzw. 8.2.7:

(i) Es gibt genau ein $\alpha^v\in X^v$ mit

$$s\cdot x = x - <x,\alpha^v>\alpha \text{ für } x\in X.$$

Außerdem ist $<\alpha, \alpha^v> = 2$ und $s^2 = 1$.

(ii) n^2 ist unabhängig von der speziellen Wahl von n und es gilt

$$x(n^2) = (-1)^{<x,\alpha^v>}$$

für jedees $x\in X$.

(iii) Es gibt einen Homomorphismus algebraischer Gruppen

$$x_\alpha: G_a \to G$$

mit

$$tx_\alpha(\xi)t^{-1} = x_\alpha(\alpha(t)\xi) \quad \text{für } t\in T \text{ und } \xi\in k$$

und

$$\mathrm{Im}(dx_\alpha) = L(G)_\alpha.$$

Hat $x'_\alpha: G_a \to G$ ebenfalls die angegebenen Eigenschaften, so gibt es ein eindeutig bestimmtes $c\in k^*$ mit $x'_\alpha(\xi) = x_\alpha(c\xi)$.

(iv) T und $\mathrm{Im}(x_\alpha)$ erzeugen eine Borel-Untergruppe B von G mit der Lie-Algebra

$$L(B) = L(T)\oplus L(G)_\alpha .$$

Beweis. Zu (i). Eindeutigkeit von α^v. Sei

$$y: G_m \to T_1$$

ein Isomorphismus algebraischer Gruppen. Nach Definition ist die Abbildung s auf T_1 (die Konjugation mit n, d.h.) der Übergang zum inversen Element, d.h. für

$$t = y(\xi) \in T_1$$

ist $(s\cdot x)(t) = x(s^{-1}t) = x(t^{-1})$, d.h.

$$\begin{aligned}(s\cdot x)(y(\xi)) &= x(y(\xi)^{-1}) = x(y(\xi))x(y(\xi)^{-2}) \\ &= x(y(\xi))\cdot\xi^{-2<x,y>}.\end{aligned}$$

Die letzte Identität besteht dabei nach Definition der Paarung $< , >$. Den Ausdruck links können wir, wenn α^v wie in (i) ist, auch wie folgt schreiben.

$$\begin{aligned}(s\cdot x)(y(\xi)) &= (x - <x,\alpha^v>\alpha)(y(\xi)) \\ &= x(y(\xi))/\alpha(y(\xi))^{<x,\alpha^v>} \\ &= x(y(\xi))\cdot(\xi^{<\alpha,y>})^{-<x,\alpha^v>} \\ &= x(y(\xi))\cdot\xi^{-<\alpha,y><x,\alpha^v>}\end{aligned}$$

Vergleich der beiden Ergebnisse liefert

$$<\alpha, y><x, \alpha^v> = 2<x, y>.$$

Im Fall $(G,G) \cong SL_2$ ist $<\alpha, y> = \pm 2$ also[144]

$$\alpha^v = \pm y.$$

Im Fall $(G,G) \cong PSL_2$ ist $<\alpha, y> = \pm 1$ also

$$\alpha^v = \pm 2y.$$

In beiden Fällen zeigen diese Formeln, daß α^v eindeutig bestimmt ist.[145]

Existenz von α^v. Wir benutzen die eben bewiesenen Formeln für α^v als Definition,

(1) $$\alpha^v = \varepsilon y \text{ falls } <\alpha,y> = (2/\varepsilon).$$

Dann ist

(2) $$<\alpha, \alpha^v> = <\alpha, \varepsilon y> = \varepsilon<\alpha,y> = 2.$$

---

[144] Die Paarung $<x, y>$ ist nicht degeneriert.

[145] Welches der beiden Vorzeichen in diesen Formeln gilt ist durch das Vorzeichen des Skalarprodukts $<\alpha, y>$ eindeutig festgelegt.

Für jedes $t \in T_1$ gibt es ein η mit $t = y(\eta)$. Also gilt

$$\begin{aligned}
(x-<x,\alpha^v>\alpha)(t) &= x(t)\alpha(t)^{-<x,\alpha^v>} \\
&= x(t)\alpha(y(\eta))^{-\varepsilon<x,y>} && \text{(wegen } t = y(\eta) \text{ und (1))} \\
&= x(t)\eta^{-<\alpha,y>\varepsilon<x,y>} && \text{(Definition von } <\alpha,y>) \\
&= x(t)\eta^{-2<x,y>} && \text{(wegen (1))} \\
&= x(t)x(y(\eta))^{-2} \\
&= x(t)x(t)^{-2} && \text{(wegen } t = y(\eta)) \\
&= x(t^{-1}) \\
&= x(n^{-1}tn) && \text{(wegen } t\in T_1) \\
&= (sx)(t)
\end{aligned}$$

Die zu beweisende Identität gilt also zumindest für $t\in T_1$.

Betrachten wir jetzt den Fall, daß t im Torus C liegt,

$$t\in C = R(G) \subseteq T.$$

Es gilt

$$\alpha(C) = 1$$

(vgl. 8.2.7(vii)). Also ist für $t\in C$:

$$\begin{aligned}
(x-<x,\alpha^v>\alpha)(t) &= x(t)\alpha(t)^{-<x,\alpha^v>} \\
&= x(t)\cdot 1^{-<x,\alpha^v>} \\
&= x(t) \\
&= x(n^{-1}tn) \text{ (wegen } C = Z(G)^0, \text{vgl. 8.2.7(i))} \\
&= x(s^{-1}(t)) \text{ (Definition von } s) \\
&= (sx)(t).
\end{aligned}$$

Die zu beweisende Identität gilt damit auch für $t\in C$, insgesamt also auf

$$C\cdot T_1 = T.$$

Nach (2) gilt

$$<\alpha, \alpha^v> = 2. \tag{3}$$

Wir haben noch zu zeigen $s^2 = 1$. Wegen

$$s\cdot x = x - <x,\alpha^v>\alpha$$

gilt

$$
\begin{aligned}
s^2x &= s(x - \langle x,\alpha^v\rangle\alpha) \\
&= x - \langle x,\alpha^v\rangle\alpha - (\langle x - \langle x,\alpha^v\rangle\alpha\,,\,\alpha^v\rangle\alpha) \\
&= x - \langle x,\alpha^v\rangle\alpha - \langle x,\alpha^v\rangle\alpha + \langle x,\alpha^v\rangle\langle\alpha\,,\,\alpha^v\rangle\alpha \\
&= x - \langle x,\alpha^v\rangle\alpha - \langle x,\alpha^v\rangle\alpha + \langle x,\alpha^v\rangle 2\alpha \qquad \text{(wegen (3))} \\
&= x.
\end{aligned}
$$

Zu (ii). Sei $n' \in N_{(G,G)}(T_1) - T_1$ ein weiteres Element wie n. Dann gilt

$$n' = nt \text{ für ein } t \in T_1,$$

also

$$
\begin{aligned}
(n')^2 &= ntnt \\
&= n^2 n^{-1} tnt \\
&= n^2 t^{-1} t \qquad \text{(wegen } ntn^{-1} = t^{-1}\text{)} \\
&= n^2,
\end{aligned}
$$

d.h. n^2 ist unabhängig von der speziellen Wahl von n.

Wir haben noch die Formel für $x(n^2)$,

$$x(n^2) = (-1)^{\langle x,\alpha^v\rangle} \text{ für } x \in X, \tag{4}$$

zu beweisen. Sei

$$X_1 := \{x \in X \mid \langle x, y\rangle = 0\}$$

Wegen $\mathrm{Im}(y: G_m \to T_1) = T_1$ ist X_1 gerade der Kern der Einschränkungsabbildung

$$X = X(T) \to X(T_1),\ \chi \mapsto \chi|_{T_1}.$$

Diese Einschränkungsabbildung ist surjektiv (vgl. Aufgabe 5.2.6 (3)), d.h.

$$X/X_1 = X(T_1)$$

ist canonisch isomorph zur Charaktergruppe von T_1.

Sei zunächst $x \in X_1$. Dann ist $x|_{T_1}$ der triviale Charakter und wegen $n^2 \in T_1$ ist die linke Seite von (4) gleich

$$\text{LHS (4)} = x(n^2) = 1.$$

Weil α^v ein ganzzahliges Vielfaches von $y: G_m \to T_1$ ist gilt weiter

$$\langle x, \alpha^v\rangle = 0$$

also

$$\text{RHS (4)} = (-1)^{\langle x,\alpha^v\rangle} = (-1)^0 = 1.$$

Damit gilt (4) für $x \in X_1$. Wir haben außerdem gezeigt, beide Seiten von (4) ändern sich nicht, wenn man x um ein Element aus X_1 abändert, d.h. beide Seiten hängen nur von der Einschränkung von x auf T_1 ab. Zum Beweis von (4) können wir also T durch T_1 und G durch (G,G) ersetzen, d.h. wir können annehmen,

$$G = SL_2$$

$$T = \{\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \mid \xi \in k^*\}$$

$$U = \{\begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix} \mid \eta \in k\}$$

$$n = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$x: G_a \to U, \eta \mapsto \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}$$

$$y: T \to G_m, \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \mapsto \xi,$$

Wir haben die Relaton (4) in dieser Situation zu überprüfen (und die analoge Relation für $G = PSL_2$).

Bestimmen wir zunächst den Charakter $\alpha: T \to G_m$. Die Multiplikation mit $\alpha(t)$, $t \in T$, entspricht bei x gerade der Konjugation mit t, d.h. es gilt

$$\begin{aligned} x(\alpha(\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix})\eta) &= \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} x(\eta) \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}^{-1} \\ &= \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}\begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \xi^{-1} & 0 \\ 0 & \xi \end{pmatrix} \\ &= \begin{pmatrix} \xi & \xi\eta \\ 0 & \xi^{-1} \end{pmatrix}\begin{pmatrix} \xi^{-1} & 0 \\ 0 & \xi \end{pmatrix} \\ &= \begin{pmatrix} 1 & \xi^2\eta \\ 0 & 1 \end{pmatrix} \\ &= x(\xi^2\eta) \end{aligned}$$

d.h. α ist die Abbildung

$$\alpha: T \to G_m, \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \mapsto \xi^2.$$

Als nächstes müssen wir

$$\alpha^v: G_m \to T, \xi \mapsto \begin{pmatrix} f(\xi) & 0 \\ 0 & f(\xi)^{-1} \end{pmatrix}$$

bestimmen aus der Relation

$$sx = x - \langle x, \alpha^v \rangle \alpha \text{ für } x \in X.$$

Sei $x: T \to G_m$ der Charakter mit $x(\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}) = \xi^l$, d.h. mit

$$2x = l\alpha.$$

Dann ist sx der Charakter mit

$$(sx)(t) = x(s^{-1}ts) = x(n^{-1}tn) = x(t^{-1}) = x(t)^{-1}$$

d.h.

$$sx = -x = x - 2x = x - l\alpha.$$

Es folgt

$$l = \langle x, \alpha^v \rangle$$

d.h.

$$\xi^l = x(\alpha^v(\xi)) = f(\xi)^l$$

Dies gilt für alle Charaktere $x \in X$, d.h. für alle ganzen Zahlen l. Damit ist $f(\xi) = \xi$, d.h. α^v ist die 1-Parameter-Untergruppe

$$\alpha^v: G_m \to T, \xi \mapsto \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}.$$

Insbesondere ist mit den obigen Bezeichnungen

$$\langle x, \alpha^v \rangle = l$$

Damit gilt

$$x(n^2) = x(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}) = x(\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}) = (-1)^l = (-1)^{\langle x,\alpha^v \rangle},$$

d.h. es gilt (4).

Die analogen Rechnungen modulo $\{\pm Id\}$ liefern die Gültigkeit von (4) in der PSL_2. Genauer, wir haben die folgende Situation zu untersuchen (alle 2×2-Matrizen sind modulo $\{\pm Id\}$ zu nehmen).

$$G = PSL_2 = SL_2/\{\pm Id\}$$

$$T = \{\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \mid \xi \in k^*\}$$

$$U = \{\begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix} \mid \eta \in k\}$$

$$n = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$x: G_a \to U, \eta \mapsto \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}$$

$$y: T \to G_m, \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \mapsto \xi^2,$$

$$\alpha: T \to G_m, \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \mapsto \xi^2.$$

Wie oben müssen wir

$$\alpha^v: G_m \to T, \xi \mapsto \begin{pmatrix} f(\xi) & 0 \\ 0 & f(\xi)^{-1} \end{pmatrix}$$

bestimmen aus der Relation

$$sx = x - \langle x, \alpha^v \rangle \alpha \text{ für } x \in X.$$

Sei $x: T \to G_m$ der Charakter mit $x\left(\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}\right) = \xi^{2l}$, d.h. mit

$$x = l\alpha.$$

Dann ist sx der Charakter mit

$$(sx)(t) = x(s^{-1}t) = x(n^{-1}tn) = x(t^{-1}) = x(t)^{-1}$$

d.h.

$$sx = -x = x - 2x = x - 2l\alpha.$$

Es folgt

$$2l = \langle x, \alpha^v \rangle$$

d.h.

$$\xi^{2l} = x(\alpha^v(\xi)) = f(\xi)^{2l}$$

Dies gilt für alle Charaktere $x \in X$, d.h. für alle ganzen Zahlen l. Damit ist $f(\xi) = \pm\xi$, d.h. α^v ist die 1-Parameter-Untergruppe

$$\alpha^v: G_m \to T, \xi \mapsto \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}.$$

Insbesondere ist mit den obigen Bezeichnungen

$$\langle x, \alpha^v \rangle = 2l$$

Damit gilt

$$x(n^2) = x\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = x\left(\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right) = (-1)^{2l} = (-1)^{\langle x, \alpha^v \rangle},$$

d.h. es gilt (4).

Zu (iii). Wir nehmen zunächst an, $x_\alpha: G_a \to G$ ist ein Homomorphismus algebraischer Gruppen wie in (iii). Für $t \in T$ und $\xi \in k$ gilt dann

$$tx_\alpha(\xi)t^{-1}x_\alpha(\xi)^{-1} = x_\alpha(\alpha(t)\xi - \xi) = x_\alpha((\alpha(t)-1)\xi).$$

Insbesondere gilt somit

$$\text{Im } x_\alpha \subseteq (G,G).$$

Es reicht deshalb, die Existenz- und Eindeutigkeitsaussage für $G = SL_2$ bzw. $G = PSL_2$ zu beweisen.

Der Fall $G = SL_2$: Wie oben können wir annehmen

$$G = SL_2$$

$$T = \{\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \mid \xi \in k^*\}$$

$$U = \{\begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix} \mid \eta \in k\}$$

$$n = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$x: G_a \to U, \eta \mapsto \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}$$

$$y: T \to G_m, \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \mapsto \xi,$$

$$\alpha: T \to G_m, \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \mapsto \xi^2.$$

Wir können

$$x_\alpha = x$$

setzen, denn es gilt

$$\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} x(\eta) \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \xi^{-1} & 0 \\ 0 & \xi \end{pmatrix} = \begin{pmatrix} 1 & \xi^2\eta \\ 0 & 1 \end{pmatrix} = x(\xi^2\eta) = x(\alpha(\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix})\eta)$$

und

$$\text{Im}(dx) = \{dx(\eta) \mid \eta \in k\} = \{\begin{pmatrix} 0 & \eta \\ 0 & 0 \end{pmatrix} \mid \eta \in k\}$$

Für die Vektoren dieses Vektorraums bewirkt Konjugation mit $\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}$ gerade die Multiplikation von η mit ξ^2, d.h. dieser Raum liegt im

Eigenraum von α. Letzterer ist aber 1-dimensional, d.h. Im(dx) ist der Eigenraum zu α.

Wir haben noch die Eindeutigkeitsaussage zu beweisen. Sei

$$x_\alpha : G_a \to G,\ \eta \mapsto \begin{pmatrix} f(\eta) & g(\eta) \\ u(\eta) & v(\eta) \end{pmatrix},$$

irgendein homomorphismus algebraischer Gruppen mit

$$\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} x_\alpha(\eta) \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}^{-1} = x_\alpha(\alpha(\xi)\eta)$$

Dann gilt

$$\begin{pmatrix} f(\eta) & \xi^2 g(\eta) \\ \xi^{-2} u(\eta) & v(\eta) \end{pmatrix} = \begin{pmatrix} f(\xi^2\eta) & g(\xi^2\eta) \\ u(\xi^2\eta) & v(\xi^2\eta) \end{pmatrix}$$

also

$$\begin{aligned} f(\xi^2\eta) &= f(\eta) \\ g(\xi^2\eta) &= \xi^2 g(\eta) \\ u(\xi^2\eta) &= \xi^{-2} u(\eta) \\ v(\xi^2\eta) &= v(\eta). \end{aligned}$$

Damit sind f und v konstant, g homogen vom Grad 1 und u homogen vom Grad -1:

$$f = a,\ g(\eta) = b\eta,\ u(\eta) = c\eta^{-1},\ v = d$$

also

$$x_\alpha(\eta) = \begin{pmatrix} a & b\eta \\ c\eta^{-1} & d \end{pmatrix}$$

Nun ist x_α auf ganz G_a regulär, d.h. es ist $c = 0$. Weiter ist x_α ein Gruppenhomomorphismus, also $x_\alpha(0) = \mathrm{Id}$, d.h. $a = d = 1$. Damit ist

$$x_\alpha(\eta) = \begin{pmatrix} 1 & b\eta \\ 0 & 1 \end{pmatrix} = x(b\eta),$$

d.h. x_α ist von der behaupteten Gestalt.

Der Fall $G = PSL_2$: unterscheidet sich nur unwesentlich vom Fall $G = SL_2$.

Zu (iv). Es reicht, die Behauptung für $G = SL_2$ bzw. für $G = PSL_2$ zu überprüfen. Für diese Fälle ist die Behauptung aber trivial.
QED.

8.2.10 Eine Eigenschaft der SL_2

Seien gegeben

$$G := SL_2$$

und die Borel-Untergruppe

$$B := \{\begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix} \mid x \in k^*,\ y \in k\}$$

Die Kommutator-Untergruppe von B ist dann gerade die unipotente Gruppe[146]

$$(B,B) = B_u = \{\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \mid y \in k\}.$$

Die rationalen Charaktere auf B haben die Gestalt[147]

$$B \to G_m\ ,\ \begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix} \mapsto x^m\ .$$

Lemma

Sei $f \in k[G]$ eine von Null verschiedene reguläre Funktion auf $G = SL_2$ mit der Eigenschaft, daß es einen rationalen Charakter $\chi: B \to G_m$ von B gibt mit

$$f(gb) = f(g)\chi(b) \text{ für } g \in G \text{ und } b \in B\ .$$

---

[146] Der Kommutator von zwei Matrizen der Gestalt $\begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix}$ hat Einsen auf der Hauptdiagonale, liegt also in B_u. Da B nicht kommutativ ist, ist (B,B) nicht-trivial (und zusammenhängend), also mindestens 1-dimensional. Dann muß aber

$$(B,B) = B_u$$

gelten.

[147] Die Abbildungen dieser Gestalt sind Charaktere auf B. Sei $\chi: B \to G_m$ jetzt ein beliebiger Charakter. Die Einschränkung von χ auf den maximalen Torus

$$T \subseteq B$$

ist von der oben angegebenen Gestalt (da die Charaktere dieser Gestalt den Koordinatenring von T erzeugen). Also gibt es einen Charakter $\beta: B \to G_m$ der oben angegebenen Gestalt derart, daß

$$\chi - \beta: B \to G_m$$

auf T den trivialen Charakter induziert. Mit anderen Worten, die Differenz faktorisiert sich über $B/T \cong G_a$. Die induzierte Abbildung $G_a \to G_m$ muß trivial sein (da unipotente Elemente in unipotente Elemente abgebildet werden). Dann gilt aber $\chi - \beta = 0$, d.h. $\chi = \beta$.

Die Einschränkungen auf den Torus sind von dieser Gestalt.

Dann ist $\chi\begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix} = x^m$ mit $m \geq 0$. Falls f nicht konstant ist, so gilt sogar $m > 0$.

Beweis. Es gilt in SL_1 für $z \neq 0$:

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

Es gibt also ein Polynom $g \in k[T]$ und ein $m \in \mathbb{Z}$ mit

$$f\left(\begin{pmatrix} x & y \\ z & t \end{pmatrix}\right) = f\left(\begin{pmatrix} 1 & z^{-1}x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right)\chi\left(\begin{pmatrix} z & t \\ 0 & z^{-1} \end{pmatrix}\right)$$

$$= z^m g(z^{-1}x).$$

Insbesondere gilt

$$f\left(\begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix}\right) = z^m g(z^{-1})$$

für $z \neq 0$. Da f auf ganz G regulär ist, muß diese Funktion auch für $z = 0$ definiert sein. Das ist nur möglich, wenn $m \geq 0$ ist. Man beachte, falls f nicht konstant ist, so muß $m > 0$ sein.[148]

QED.

8.2.11 Aufgaben

(1) Man leite aus 8.2.10 ein ähnliches Ergebnis für $G = PSL_2$ ab.

(2) (a) Man zeige in der Situation von 8.2.10 daß die Funktionen f mit vorgegebenen $m \geq 0$ einen Unterraum V_m von k[G] bilden der Dimension m+1, welcher stabil gegenüber Linkstranslationen ist.
(b) Sei ρ_m die rationale Darstellung von G auf V_m durch Linkstranslationen. Man zeige, es gibt eine Basis $e_0,\ldots,e_m$ von V_m mit

$$\rho_m\left(\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}\right)e_i = x^{m-2i}e_i \qquad \text{für } x \in k^*$$

$$\rho_m\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\right)e_i = \sum_{j=0}^{i} (-1)^{i-j}\binom{i}{j}x^{i-j}e_j \qquad \text{für } x \in k.$$

(c) Sei p = char k. Ist p = 0 oder $p > m$, so ist ρ_m irreduzibel.

(3) Seien (ρ, V) eine rationale Darstellung von $G = SL_2$ und (ρ^*, V^*) die duale Darstellung, d.h. V^* ist das Dual des Vektorraums V und

$$(\rho^*(g)u)(v) =^{149} u(\rho(g)v)$$

---

[148] Im Fall m = 0 ist $f\left(\begin{pmatrix} x & y \\ z & t \end{pmatrix}\right) = g(z^{-1}x)$ mit nicht-konstantem g, d.h. $f\left(\begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix}\right) = g(z^{-1})$ mit nicht-konstantem g. Dann ist aber f nicht auf ganz G regulär.

für $v \in V$, $u \in V^*$ und $g \in G$.

(a) Man leite aus 6.7[150] ab, daß es ein $v \in V - \{0\}$ gibt und ein $m \in \mathbb{Z}$ mit

$$\rho\left(\begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix}\right)v = x^m v.$$

Sei $\phi: V^* \to k[G]$ die lineare Abbildung mit

$$(\phi u)(g) = u(\rho(g)v).$$

Man zeige, es gilt $m \geq 0$.

(b) Ist ρ irreduzibel, so ist ϕ injektiv.

(c) Jede irreduzible Darstellung von G ist äquivalent zu einer Faktordarstellung und ebenfalls zu einer Teildarstellung eines ρ_m.

(d) Ist char k = 0, so ist jede irreduzible rationale Darstellung von G äquivalent zu einem ρ_m.

(4) Die Bezeichnungen seien wie in den vorangehenden Aufgaben.

(a) Der Raum V_m^* hat eine Basis $e_0^*,\ldots,e_m^*$ mit[151]

$$\rho_m^*\left(\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}\right)e_i^* = x^{-m+2i}e_i \qquad \text{für } x \in k^*$$

$$\rho_m^*\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\right)e_0^* = \sum_{j=0}^{m} (-1)^i x^i e_i^* \qquad \text{für } x \in k.$$

Ist $\tilde{e}_0^*,\ldots,\tilde{e}_m^*$ eine weitere Basis, für welche diese Identitäten gelten, so gibt es ein $a \in k^*$ mit $\tilde{e}_i^* = e_i^*$ für alle i.

(b) Sei (ρ, V) eine rationale Darstellung von $G = SL_2$ mit folgenden Eigenschaften.

1. Es gibt ein $v \in V - \{0\}$ mit $\rho\left(\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}\right) = x^m v$.

2. $m \neq 0$.

---

[149] Im Original steht auf der rechten Seite $u(\rho(g)^{-1}v)$.

[150] besser aus dem Fixpunktsatz von Borel (7.2.5).

[151] Die Formeln sollten lauten

$$\rho_m^*\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}e_i^* = x^{-m+2i}e_i^*$$

$$\rho_m^*\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}e_m^* = \sum_{j=0}^{m} x^{m-j}e_j$$

3. dim V = m+1
4. Die Vektoren der Gestalt $(\rho(g)-1)v$ mit $g \in G$ erzeugen V.

Dann ist ρ äquivalent zu ρ^*_m.

Lösungen

Zu (1).

Im Beweis des Lemmas ersetze man jede 2×2-Matrix durch deren Bild bei der natürlichen Abbildung

$$SL_2 \to Aut(sl_2),\ g \mapsto (v \mapsto gvg^{-1}).$$

Zu (2)(a).

Je zwei Funktionen f zum selben m untersheiden sich nur im Polynom g mit

$$f\left(\begin{pmatrix} x & y \\ z & t \end{pmatrix}\right) = z^m g(z^{-1}x), \tag{1}$$

sodaß insbesondere

$$f\left(\begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix}\right) = z^m g(z^{-1})$$

gilt. Aus der letzten Identität ergibt sich die Bedingung

$$\deg g \le m,$$

wenn f auf ganz G definiert sein soll. Deshalb hat der von diesen Funktionen erzeugte Vektorraum eine Dimension $\le m+1$,

$$\dim V_m \le m+1.$$

Zum Beweis der Behauptung genügt es deshalb zu zeigen, die Funktionen der Gestalt (1) mit $\deg g \le m$ genügen den Bedingungen des Lemmas 8.2.10, d.h. sie sind auf ganz G definiert und es gilt

$$f(gb) = f(g)\chi(b)$$

für $b = \begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix}$ und $\chi\begin{pmatrix} x & y \\ 0 & x^{-1} \end{pmatrix} = x^m$. Die Regularität von f auf ganz G ist trivial. Überprüfen wir die angegebene Relation. Seien dabei

$$g = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \text{ und } b = \begin{pmatrix} u & v \\ 0 & u^{-1} \end{pmatrix}$$

d.h.

$$gb = \begin{pmatrix} xu & xv+yu^{-1} \\ zu & zv+tu^{-1} \end{pmatrix}$$

Es gilt

$$f(gb) = (zu)^m g((zu)^{-1}xu) = z^m g(z^{-1}x)u^m = f(g)\chi(b).$$

Wir haben noch zu zeigen, der Raum der regulären Funktionen $f \in k[G]$ mit

$$f(gb) = f(g)\chi(b)$$

mit fest vorgegebenen Charakter $\chi \in X(B)$ ist invariant gegenüber Linkstranslationen. Sei

$$f' := \lambda_g, f .$$

Dann gilt für $g \in G$ und $b \in B$:

$$f'(gb) = f(g'^{-1}gb)\ f(g'^{-1}g)\chi(b) = f'(g)\chi(b),$$

d.h. f' liegt wieder in diesem Raum.

Zu (2)(b).

Sei $e_i \in V_m$ die Funktion f zu $g(T) = T^i$, d.h.

$$e_i\begin{pmatrix} x & y \\ z & t \end{pmatrix} := z^m (x/z)^i = z^{m-i}x^i \qquad (i = 0,...,m).$$

Für $t = \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}$ ist dann

$$(\lambda_t e_i)\begin{pmatrix} x & y \\ z & t \end{pmatrix} = e_i(\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}\begin{pmatrix} x & y \\ z & t \end{pmatrix}) = e_i\begin{pmatrix} \xi^{-1}x & \xi^{-1}y \\ \xi z & \xi t \end{pmatrix} = (\xi z)^{m-i}(\xi^{-1}x)^i = \xi^{m-2i}\ z^{m-i}x^i$$

$$= \xi^{m-2i} e_i\begin{pmatrix} x & y \\ z & t \end{pmatrix}$$

d.h.

$$\lambda_t e_i \quad = \xi^{m-2i} e_i \text{ für } t = \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}.$$

Für $u = \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}$ ist weiter

$$(\lambda_u e_i)\begin{pmatrix} x & y \\ z & t \end{pmatrix} = e_i(\begin{pmatrix} 1 & -\eta \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x & y \\ z & t \end{pmatrix}) = e_i\begin{pmatrix} x-\eta z & y-\eta t \\ z & t \end{pmatrix} = z^{m-i}(x-\eta z)^i$$

$$= \sum_{j=0}^{i} \binom{i}{j} x^j (-\eta)^{i-j} z^{i-j}\ z^{m-i}$$

$$= \sum_{j=0}^{i} (-1)^{i-j}\binom{i}{j} x^j \eta^{i-j} z^{m-j}$$

$$= \sum_{j=0}^{i} (-1)^{i-j}\binom{i}{j}\ \eta^{i-j} e_j\begin{pmatrix} x & y \\ z & t \end{pmatrix},$$

d.h.

$$\lambda_u e_i \quad = \sum_{j=0}^{i} (-1)^{i-j}\binom{i}{j}\ \eta^{i-j} e_j \qquad \text{für } u = \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}.$$

Für spätere Verwendung beschreiben wir noch die Wirkung von einigen weiteren Matrizen:

Für $n = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ ist

$$\lambda_n e_i \begin{pmatrix} x & y \\ z & t \end{pmatrix} = e_i(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} x & y \\ z & t \end{pmatrix}) = e_i \begin{pmatrix} z & t \\ -x & -t \end{pmatrix} = (-x)^{m-i} z^i = (-1)^{m-i}\, e_{m-i} \begin{pmatrix} x & y \\ z & t \end{pmatrix}$$

d.h.

(2) $\lambda_n e_i = (-1)^{m-i}\, e_{m-i}$

Für $n' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ ist

$$\lambda_{n'} e_i \begin{pmatrix} x & y \\ z & t \end{pmatrix} = e_i(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x & y \\ z & t \end{pmatrix}) = e_i \begin{pmatrix} -z & -t \\ x & t \end{pmatrix} = x^{m-i}(-z)^i = (-1)^i\, e_{m-i} \begin{pmatrix} x & y \\ z & t \end{pmatrix}$$

d.h.

(3) $\lambda_{n'} e_i = (-1)^i\, e_{m-i}$

Zu (2)(c).

Sei $W \subseteq V_m$ ein nicht-trivialer Unterraum minimaler Dimension, der gegenüber Linkstranslationen invariant ist. Die Darstellung von G auf W induziert eine Darstellung von $T = \{\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \mid \xi \in k^*\}$. Diese Zerfällt in 1-dimensionale invariante Unterräume. Nach (b) werden die T-invarianten Unterräume von V gerade von den e_i erzeugt (und diese gehören zu paarweise verschiedenen Charakteren. Deshalb liegt mindestens ein e_i in W,

(4) $$f_i = (-1)^i e_i \in W \text{ für ein } i.$$

und gewisse der f_j bilden eine Basis von W. Weiter:

(*) Liegt ein Linearkombination von f_j in W, so liegt jedes f_j, das mit einem von Null verschiedenen Koeffizienten vorkommt, ebenfalls in W.

Nach der Rechnung im letzten Teil des Beweises von (b) gilt weiter,

(**) $f_i \in W \Rightarrow f_{m-i} \in W$.

Nach (b) gilt

$$\rho_m \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} f_i = \sum_{j=0}^{i} \binom{i}{j} x^{i-j} f_j \in W$$

für jedes $x \in k$. Nach (*) gilt damit

$$f_0 \in W$$

und nach (**) auch

$$f_m \in W.$$

Wir können also annehmen i = m,

$$\rho_m\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}f_m = \sum_{j=0}^{m}\binom{m}{j}x^{m-j}f_j \in W$$

Wegen m < p im Fall der Charakteristik p sind aber alle $\binom{m}{j} \neq 0$, d.h. es liegen alle f_j in W, d.h. W = V.

QED.

Zu (3)(a).

Seien T der maximale Torus

$$T := \{\begin{pmatrix}x & 0\\ 0 & x^{-1}\end{pmatrix} \mid x\in k^*\}$$

und B die Borel-Untergruppe

$$B := \{\begin{pmatrix}x & y\\ 0 & x^{-1}\end{pmatrix} \mid x\in k^*,\ y\in k\}$$

von $G := SL_2$. Die Operation von G auf V induziert eine Operation von G auf der Projektivierung $\mathbb{P}(V)$ und damit eine von B auf $\mathbb{P}(V)$. Nach dem Fixpunktsatz von Borel (7.2.5) besitzt B auf $\mathbb{P}(V)$ mindestens einen Fixpunkt, d.h. es gibt ein $v\in V - \{0\}$ derart, daß

$$vK \subseteq V$$

ein B-stabiler Unterraum ist. Insbesondere gibt es einen Charakter

$$\chi: B \to G_m$$

mit

$$\rho\begin{pmatrix}x & y\\ 0 & x^{-1}\end{pmatrix}v = \chi\begin{pmatrix}x & y\\ 0 & x^{-1}\end{pmatrix}v \text{ für alle } \begin{pmatrix}x & y\\ 0 & x^{-1}\end{pmatrix}\in B.$$

Nach 8.2.10 haben die Charaktere von B aber die Gestalt

$$\chi: B \to G_m,\ \begin{pmatrix}x & y\\ 0 & x^{-1}\end{pmatrix} \mapsto x^m,$$

d.h. es gibt ein $m\in\mathbb{Z}$ mit

$$\rho\begin{pmatrix}x & y\\ 0 & x^{-1}\end{pmatrix}v = x^m v \text{ für alle } \begin{pmatrix}x & y\\ 0 & x^{-1}\end{pmatrix}\in B.$$

Damit ist der erste Teil von Aufgabe (3)(a) bewiesen.

Betrachten wir die Abbilung

$$\phi: V^* \to k[G],\ l \mapsto (x \mapsto l(\rho(x)v)).$$

Diese Abbildung ist nach Konstruktion nicht identisch Null. Für $g \in G$ und $b \in B$ gilt

$$\begin{aligned}\phi(l)(gb) &= l(\rho(gb)^{-1}v) = l(\rho(g)\rho(b)v) = l(\rho(g)\chi(b)v) \\ &= l(\rho(g)v)\chi(b) \quad \text{(weil l eine lineare Funktion auf V ist)} \\ &= \phi(l)(g)\chi(b).\end{aligned}$$

Damit ist $\phi(l)$ für jedes $l \in V^*$ eine Funktion wie im Lemma von 8.2.10. Insbesondere ist also $m \geq 0$.

Bemerkung

Die Abbildung ϕ ist äquivariant, wenn man V^* mit der zu ρ dualen Operation ρ^* versieht und $k[G]$ mit der Operation durch Linkstranslationen:

$$\begin{aligned}((\lambda_g(\phi(l))(x) &= \phi(l)(g^{-1}x) = l(\rho(g^{-1}x)v)) = l(\rho(g^{-1})\rho(x)v)) \\ &= (\lambda_{\rho(g)}(l))(\rho(x)v) \\ &= \phi(\lambda_{\rho(g)}(l))(x) \\ &= \phi(\rho^*(g)l)(x)\end{aligned}$$

Mit anderen Worten, es gilt

$$\lambda_g(\phi(l)) = \phi(\rho^*(g)l) \text{ für alle } l \in V^*,$$

d.h.

$$\lambda_g \circ \phi = \phi \circ \rho^*(g)$$

Zu (3)(b).

Angenommen, ϕ ist nicht injektiv. Dann gibt es ein l mit

$$0 \neq l \in \mathrm{Ker}(\phi) \subseteq V^*$$

und es gilt

$$0 = \phi(l)(g) = l(\rho(g)v))$$

für alle $g \in G$. Also ist der von den $\rho(g)v$ erzeugte Unterraum von V ein (nicht-trivialer) echter Unterraum. Er ist nach Definition G-invariant. Dann ist die Darstellung

$$\rho: G \to \mathrm{Aut}(V)$$

aber reduzibel.

Zu (3)(c).

Sei

$$\rho: G \to \mathrm{Aut}(V)$$

eine irreduzible rationale Darstellung. Dann ist auch die auf dem dualen Raum induzierte (duale) Darstellung

$$G \to \mathrm{Aut}(V^*)$$

eine irreduzible rationale Darstellung, und das doppelte Dual von ρ ist ρ selbst. Es reicht also zu zeigen, das Dual von ρ ist von der behaupteten Gestalt.

Weil ρ irreduzibel ist, kann man mit Hilfe der Abbildung

$$\phi: V^* \to k[G]$$

von (b) den Raum V^* als k-linearen Unterraum von k[G] auffassen. Für $l \in V^* \subseteq k[G]$, $g \in G$ und $b \in B$ gilt dann

$$\begin{aligned} l(gb) &=^{152} l(\rho(gb)v)) \\ &= l(\rho(g)\rho(b)v)) = l(\rho(g)\chi(b)v)) \\ &= l(\rho(g)v))\chi(b) \\ &=^{153} l(g)\chi(b) \end{aligned}$$

Mit anderen Worten, es gilt

$$V^* \subseteq V_m ,$$

wenn V_m den Raum von Aufgabe (2) bezeichnet und m der den Charakter χ definierende Exponent ist. Mit anderen Worten, V^* ist eine Teildarstellung von V_m und V ist eine Faktordarstellung von V_m^*.

Zum Beweis der Behauptung reicht es zu zeigen, die Darstellung ρ_m^* von G auf V_m^* ist äquivalent zu der Darstellung ρ_m von G auf V_m.

Auf Grund der Formeln von (2)(b) operiert das Element $\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \in T \subseteq G$ auf dem Basiselement $e_i \in V_m$ durch Multiplikation mit x^{m-2i}. Deshalb operiert $\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$ auf der dualen Basis (durch die transponierte Matrix also) ebenfalls durch Multiplikation mit x^{m-2i},

$$(5) \qquad \rho_m^*\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} e_i^* = x^{m-2i}\, e_i^* .$$

Damit folgt die Behauptung aus Aufgabe (4)(b), denn es ist

$$\rho_m^*\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} e_0^* = x^m\, e_0^*$$

und die Vektoren der Gestalt

$$(\rho_m^*\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} - 1)e_0^* = (x^{m-2i} - 1)e_0^* \text{ mit } x \in k^*$$

$$(\rho_m^*\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} - 1)e_0^* + e_0^* = \sum_{i=0}^{m} x^{m-i} e_i^* \text{ mit } x \in k$$

---

[152] wegen der Identifikation des Raums V^* mit dessen Bild in k[G].
[153] wegen der Identifikation des Raums V^* mit dessen Bild in k[G].

erzeugen den gesamten Raum V_m^*: für m+1 paarweise verschiedene Werte

$$x_0,\ldots,x_m \in k$$

ist

$$\det\,(x_j^{m-i}) \neq 0$$

(es ist bis aufs Vorzeichen gerade die Vandermondesche Determinante).

Bemerkung

Ohne Verwendung der Aussage von Aufgabe (4) haben wir gezeigt: ist

$$\rho\colon G = SL_2 \to \mathrm{Aut}(V)$$

eine irreduzible Darstellung mit der Eigenschaft, daß die Matrizen

$$\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix},\ x \in k^*,$$

auf einem Vektor von V - {0} durch Multiplikation mit x^m operieren, so ist ρ eine Teildarstellung von V_m und eine Faktordarstellung von V_m^*.

Zu (3)(d).

Folgt aus (3)(c) und der Tatsache, daß die Darstellungen ρ_m (nach (2)(c) irreduzibel sind.

Zu (4)(a).

Diese Relationen von Aufgabe (2)(b) beschreiben die Matrizen der linearen Endomorphismen $\rho_m\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$ und $\rho_m\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ bezüglich der Basis $\{e_i\}$ von V. Die Matrizen bezüglich der dualen Basis sind gerade die zugehörigen transponierten Matrizen, d.h.

$$\rho_m^*\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} e_i^* = x^{m-2i} e_i^*$$

$$\rho_m^*\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} e_i^* = \sum_{j=i}^{m} (-1)^{j-i} \binom{j}{i} x^{j-i} e_j^*$$

Speziell für i = 0 erhalten wir

$$\rho_m^*\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} e_0^* = \sum_{j=0}^{m} (-1)^j x^j e_j^*$$

Mit $f_j^* := e_{m-j}^*$ erhalten wir

$$\rho_m^*\begin{pmatrix} x & 0 \\ 0 & x^{-1}\end{pmatrix} f_i^* = x^{m-2(m-i)} f_i^* = x^{-m+2i} f_i^*$$

$$\rho_m^*\begin{pmatrix} 1 & x \\ 0 & 1\end{pmatrix} f_m^* = \sum_{j=0}^{m} (-1)^j x^j f_{m-j}^* = \sum_{j=0}^{m} (-1)^{m-j} x^{m-j} f_j$$

Mit $g_j^* = (-1)^j f_j^*$ folgt

$$\rho_m^*\begin{pmatrix} x & 0 \\ 0 & x^{-1}\end{pmatrix} g_i^* = x^{-m+2i} g_i^*$$

(6) $$\rho_m^*\begin{pmatrix} 1 & x \\ 0 & 1\end{pmatrix} g_m^* = \sum_{j=0}^{m} x^{m-j} g_j^*$$

Damit ist die Existenzaussage von Aufgabe (4)(a) bewiesen. Die ersten Relationen sagen aus, die g_i^* sind Eigenvektoren bezüglich der Operation des maximalen Torus $T = \{\begin{pmatrix} x & 0 \\ 0 & x^{-1}\end{pmatrix} \mid x \in k^*\}$ zu paarweise verschiedenen Charakteren. Jede andere Basis $\{h_i^*\}$ mit den angegebenen Eigenschaften muß ebenfalls aus solchen Eigenvektoren bestehen, d.h.

$$h_i^* = c_i \cdot g_i^* \text{ mit } c_i \in k^*.$$

Wir haben noch zu zeigen, die Koeffizienten c_i sind alle gleich. Zum Beweis multiplizieren wir (6) mit c_m und ziehen das Ergebnis von der entsprechenden Identität für die h_i^* ab. Wir erhalten:

$$0 = \sum_{j=0}^{m} x^{m-j} (c_m - c_j) g_j^* \text{ für alle } x \in k^*.$$

Da die g_j^* linear unabhängig sind, folgt $x^{m-j}(c_m - c_j) = 0$ für alle j und alle $x \in k^*$, also $c_j = c_m$ für alle j.

<u>Zu (4)(b).</u>

Wir betrachten die in Aufgabe (3) konstruierte Abbildung

$$\phi: V^* \to k[G],\ \mathrm{la}(\mathrm{gal}(\rho(g)v)).$$

Wie wir gesehen haben, ist diese Abbildung äquivariant, und ihr Bild liegt in V_m,

$$\phi(V^*) \subseteq V_m .$$

Zeigen wir, unter den gegebenen Voraussetzungen ist ϕ injektiv: sei $l \in V^*$ derart, daß gilt

$$\phi(l) = 0.$$

Wir haben zu zeigen, daß dann $l = 0$ ist. Es gilt für jedes $g \in G$

$$0 = \phi(l)(g) = l(\rho(g)v).$$

Insbesondere für $g = e$ erhalten wir $l(v) = 0$, also

$$0 = l((\rho(g)-1)v) = 0 \text{ für alle } g \in G.$$

Da nach Voraussetzung die Vektoren der Gestalt $(\rho(g)-1)v$ den Raum V erzeugen, folgt $l = 0$. Wir haben gezeigt, ϕ ist injektiv. Wir können V^* mit dem Bild bei ϕ identifizieren und erhalten

$$V^* \subseteq V_m .$$

Da beide Räume die Dimension m+1 besitzen, folgt $V^* = V_m$. Wir haben gezeigt, es besteht eine Isomorphie von G-Räumen

$$V \cong V_m^* .$$

Da speziell der Raum V_m den an V gestellten Bedingungen genügt (mit $v = e_0$), gilt insbesondere $V_m \cong V_m^*$. Zusammen erhalten wir

$$V \cong V_m .$$

QED.

Notes

Der Beweis des Klassifikationssatzes 8.2.5 für halbeinfache Gruppen des Rangs 1 ist vom üblichen Beweis verschieden. Wir benutzen das Lemma von Bruhat (8.2.3(i)). Das Argument für den Beweis von 8.2.5 stammt von Zassenhaus (vgl. [19, p. 393]). Es ist sehr angenehm, Satz 8.2.5 zu einem frühen Zeitpunkt zur Verfügung zu haben. So bekommt man zum Beispiel die Spiegelungen von 8.2.9.

9. Roots, the Weyl group

9.1 Wurzeln

9.1.1 Die Situation

G eine zusammenhängende lineare algebraische Gruppe.
T ein maximaler Torus von G.
X := $X^*(T)$ die Gruppe der Charaktere $T \to G_m$ von T.

X^v := $X_*(T)$ die Gruppe der 1-parametrigen Untergruppen $G_m \to T$ von T.

Zur Erinnerung: X und X^V sind Gitter, d.h. freie abelschen Gruppen endlichen Rangs, und die Komposition der Elemente dieser Gruppen definiert eine Paarung

$$X \times X^V \to \mathbb{Z}, (\chi, \lambda) \mapsto \langle \chi, \lambda \rangle,$$

mit

$$\xi^{\langle \chi, \lambda \rangle} = \chi(\lambda(\xi)) \text{ für alle } \xi \in k.$$

Im folgenden werden wir uns mit den Teiltori $S \subseteq T$ der Kodimension 1 befassen.

9.1.2 Gewiche einer Torus-Operation auf einem Vektorraum.

Sei S ein Torus, welcher linear auf dem Vektorraum V operiere. Die Gewichte von S auf V sind dann definiert als diejenigen Charaktere $\chi \in X^*(X)$, für welche die Gewichtsräume

$$V_\chi := \{v \in V \mid s \cdot v = \chi(s)v\}$$

nicht-trivial sind. Ein Vektor $v \in V_\chi - \{0\}$ heißt Gewichtsvektor von S mit dem Gewicht χ. Wir wissen, V ist die direkte Summe der Gewichtsräume, wobei χ die Gewichte von S auf V durchläuft (vgl. im Original 2.5.2(c)).

9.1.3 Erzeugung von G durch die Zentralisatoren der Tori der Kodimension 1

Sei G eine zusammenhängende lineare algebraische Gruppe. Dann wird G wird erzeugt von den Zentralisatoren $Z_G(S)$ wobei $S \subseteq T$ die Teiltori der Kodimension 1 des fixierten maximalen Torus T durchläuft.

Beweis. Die Untergruppen $Z_G(S)$ sind nach 7.3.5(i) zusammenhängend. Seien

$$\chi_1, \dots, \chi_r$$

die unterschiedlichen von Null verschiedenen Gewichte von T auf der Lie-Algebra L(G). Dann zerfällt L(G) in eine direkte Summe

$$(1) \qquad L(G) = L(G)_{\chi_1} \oplus \dots \oplus L(G)_{\chi_r} \oplus L(G)_0 ,$$

wobei $L(G)_0$ gerade die Fixpunktmenge von Ad(T) ist. Sei

$$S_i := \mathrm{Ker}(\chi_i : T \to G_m)^0.$$

Die S_i sind Teiltori[154] von T der Kodimension 1. Nach 4.4.7[155] enthält die Lie-Algebra $L(Z_G S_i)$ sowohl $L(G)_0$ als auch $L(G)_{\chi_i}$,

---

[154] Als Untergruppe einer diagonalisierbaren Gruppe sind sie diagonalisierbar. Nach Konstruktion sind sie zusammenhängend.

(2) $L(G)_0 , L(G)_{\chi_i} \subseteq L(Z_G S_i)$.[156]

Sei G_1 die von den $Z_G(S_i)$ erzeugte Untergruppe von G. Nach 6.1 ist G_1 abgeschlossen und zusammenhängend. Die Lie-Algebra von G_1 enthält wegen (2) die Unterräume $L(G)_0$ und $L(G)_{\chi_i}$ für alle i, also wegen (1) die gesamte Lie-Algebra von G. Deshalb gilt $G_1 = G$, d.h. es gilt die Behauptung.
QED.

9.1.4 Reguläre und singuläre Tori

Sei G eine zusammenhängende lineare algebraische Gruppe mit dem maximalen Torus T. Ein Teiltorus $S \subseteq T$ der Kodimension 1 heißt regulär, wenn sein Zentralisator $Z_G(S)$ auflösbar ist und ansonsten singulär.

9.1.5 Das zu einem singulären Torus gehörige Gewichtspaar

Sei wieder G eine zusammenhängende lineare algebraische Gruppe mit dem maximalen Torus T und $S \subseteq T$ ein singulärer Teiltorus (der Kodimension 1). Dann gibt es ein Gewicht α von T auf[157] Lie(G) mit

---

[155] Let D be a diagonalizable linear algebraic group, which acts as a group of automorphisms on the connected group G. This means that G is a D-space in the sense of 2.3.1 and that for all $d \in D$ the morphism

$$G \to G, g \mapsto d \cdot g.$$

is a group automorphism of G. From 2.5.2 we infer that these are semi-simple automorphisms[155]. Let

$$Z_G(D) := \{g \in G \mid d \cdot g = g \text{ for all } d \in D\}$$

The group D also acts as a group of automorphisms on the Lie algebra $\mathfrak{g} = L(G)$. Let

$$\mathfrak{z}_{Lie(G)}(D) := \{X \in Lie(G) \mid d \cdot X = X \text{ for all } d \in D\}.$$

Then assertion 4.4.7 says,

$$Lie\, Z_G(D) = \mathfrak{z}_{Lie(G)}(D).$$

[156] $L(Z_G S_i)$ besteht nach 4.4.7 aus den Vektorfeldern $X \in L(G)$, die bei Konjugation mit Elementen aus S_i fest bleiben. Das gilt aber auch für die Vektorfelder aus $L(G)_0$ (Konjugation induziert die Multiplikation mit dem trivialen Charakter) und die aus $L(G)_{\chi_i}$ (Konjugation induziert die Multiplikation mit χ_i und χ_i ist trivial auf S_i).

[157] Bezüglich der adjungierten Darstellung von G auf Lie(G).

(i) $S = (\mathrm{Ker}\ \alpha)^0$.

(ii) $L(\mathbf{Z}_G(S)/\mathbf{R}_u\mathbf{Z}_G(S)) \cong L(T) \oplus kX_\alpha \oplus kX_{-\alpha}$.[158]

Dabei sind X_α und $X_{-\alpha}$ Gewichtsvektoren zu den Gewichten α bzw. $-\alpha$.

Das Gewicht α ist bis auf das Vorzeichen eindeutig bestimmt.

Der Zentralisator Z_G (S) hat den halbeinfachen Rang 1.

Beweis. 1. Schritt: Wir beweisen zunächst das

Lemma

Seien G eine zusammenhängende lineare algebraische Gruppe und $N \subseteq G$ ein zusammenhängender auflösbarer Normalteiler. Dann gilt:

1. Die natürliche Abbildung $G \to G/N$ bildet maximale Tori in maximale Tori ab.
2. Ist G vom halbeinfachen Rang 1, so gilt dasselbe für G/N.

Beweis des Lemmas. Zu 1. Die natürliche Abbildung $\rho : G \to G/N$ hat zusammenhängende Fasern. Sei $T' \subseteq G/N$ ein maximaler Torus, der das Bild des maximalen Torus $T \subseteq G$ enthält. Dann ist $\rho^{-1}(T')$ zusammenhängend und man hat eine exakte Sequenz

$$0 \to N \to \rho^{-1}(T') \to T' \to 0.$$

Insbesondere ist $\rho^{-1}(T')$ auflösbar, d.h.

$$\rho^{-1}(T') = T \cdot \rho^{-1}(T')_u \quad \text{(halbdirektes Produkt)}.$$

Der zweite Faktor liegt vollständig im Kern von ρ, (weil T' aus halbeinfachen Elementen besteht), d.h. ρ induziert eine Surjektion

$$T \to T'.$$

Zu 2. Das Bild von R(G) in G/N ist ein zusammenhängender auflösbarer Normalteiler, d.h. es gilt

$$\rho R(G) \subseteq R(G/N).$$

Die obige Surjektion $T \to T'$ induziert also eine Surjektion

$$T \bmod R(G) \to T' \bmod R(G/N),$$

d.h. es gilt

$$\mathrm{rk}(T' \bmod R(G/N)) \leq \mathrm{rk}(T \bmod R(G)) = 1,$$

d.h. G/N hat einen halbeinfachen Rang ≤ 1. Wäre der halbeinfache Rang von G/N gleich Null, so wäre jede Borel-Untergruppe von G/N unipotent, also gleich nilpotent, also gleich G/N, d.h. G/N wäre auflösubar. Wegen der exakten Sequenz

---

[158] Im Original steht auf der rechten Seite $L(\mathbf{Z}_G(T)) \oplus kX_\alpha \oplus kX_{-\alpha}$ (das ist ein Druckfehler, vgl. auch Humphreys, Chap. IX.24,3)

$$0 \to N \to G \to G/N \to 0$$

wäre dann aber auch G auflösbar, d.h.

$$G = R(G)$$

und rk G/R(G) = 0. Das steht im Widerspruch zu der Annahme, daß der halbeinfache Rang von G gleich 1 sein soll.

QED für das Lemma.

2. Schritt. $Z := \mathbf{Z}_G(S)$ hat den halbeinfachen Rang 1.

Wegen

$$S \subseteq T = \text{kommutativ}$$

gilt

$$T \subseteq \mathbf{Z}_G(S),$$

d.h. T ist ein maximaler Torus von $\mathbf{Z}_G(S)$. Nach Definition liegt S im Zentrum von $\mathbf{Z}_G(S)$, d.h. $S \subseteq R(Z)$. Damit hat

$$T \bmod R(Z) \longleftarrow\!\!\!

Es gilt also (ii). Die Eindeutigkeit von α bis aufs Vorzeichen ergibt sich aus der Tatsache, daß jeder Eigenraume den zugehörigen Charakter eindeutig festlegt. Wegen

$$Z = Z_G(S)$$

induziert die Konjugation mit Elementen aus S auf Z und damit auch auf $L(Z/R_u(Z))$ die identische Abbildung. Insbesondere gilt damit

$$\alpha(s)X_\alpha = X_\alpha \text{ für jedes } s \in S,$$

also $S \subseteq \mathrm{Ker}(\alpha)$ ($\subseteq T$). Nach Wahl von S hat aber S in T die Kodimension 1 (und α ist ein nicht-trivialer Charakter), d.h. es gilt

$$\dim S = \dim \mathrm{Ker}(\alpha),$$

also $S = \mathrm{Ker}(\alpha)^0$. Damit ist auch Aussage (i) bewiesen.
QED.

9.1.6 Die Wurzeln von G und die Operation der Weyl-Gruppe auf den Wurzeln

Die Charaktere χ von T, die in der in 9.1.5 beschriebenen Weise zu den singulären Teiltori S der Kodimension 1 gehören[160], heißen Wurzeln von G bezüglich des maximalen Torus T. Bezeichne

$$R(G,T)$$

die Menge aller Wurzeln von G bezüglich T. Bezeichne

$$W(G,T) := N_G(T)/Z_G(T)$$

die Weyl-Gruppe von G bezüglich T. Die Weyl-Gruppe operiert auf den Charakteren $\chi \in X^*(T)$ und den 1-parametrigen Untergruppen $\lambda \in X_*(T)$ nach den folgenden Vorschriften.

$$(\bar{w}\cdot\chi)(t) := \chi(w^{-1}\cdot t\cdot w) \text{ für } w \in N_G(T),\ t \in T$$

$$(\bar{w}\cdot\lambda)(\xi) = w\cdot\lambda(\xi)\cdot w^{-1} \text{ für } w \in N_G(T),\ \xi \in G_m.$$

Das in 9.1.1 definierte Skalarprodukt ist invariant bei diesen Operationen,

$$\langle \bar{w}\cdot\chi, \bar{w}\cdot\lambda\rangle = \langle\chi,\lambda\rangle \quad \text{für } \bar{w} \in W(G,T).$$

Die Operation der Weyl-Gruppe auf den Charakteren induziert eine Operation auf den Wurzeln.

---

[160] d.h. $\chi: T \to G_m$ ist ein nicht-trivialer Charakter und die Konjugation mit Elementen aus T induziert auf

$$L(Z_G(S)/R_u Z_G(S))$$

eine Operation von T, bei welcher χ einen nicht-trivialen Eigenraum besitzt.

Beweis. Durch Konjugation mit einem Element $w \in N_G(T)$ wird ein gegebener singulärer Teiltorus S von T in einen singulären Teiltorus S' überführt. Durch Anwenden dieser Konjugation in der Situation von 9.1.5 erhält man die analogen Aussagen mit S' anstelle von S und $\bar{w} \cdot \alpha$ anstelle von α. Insbesondere ist $\bar{w} \cdot \alpha$ wieder eine Wurzel.
QED.

9.1.7 Die Endlichkeit der Menge der Wurzeln

Die Menge der Wurzeln R(G,T) von G bezüglich T ist endlich.

Beweis. Da der Faktorisierungshomomorphismus

$$\mathbf{Z}_G S \to \mathbf{Z}_G S / R_u \mathbf{Z}_G S$$

separabel ist, d.h.

$$\text{Lie } \mathbf{Z}_G S \to \text{Lie } \mathbf{Z}_G S / R_u \mathbf{Z}_G S$$

ist surjektiv, ist jede Wurzel auch ein Gewicht der Operation von T auf Lie $\mathbf{Z}_G S$, also eines der endlich vielen Gewichte der adjungierten Operation von T auf Lie(G).
QED.

9.1.8 Die zu einer Wurzel gehörige Gruppe vom halbeinfachen Rang 1 und die zugehörige Spiegelung

Sei $\alpha \in R(G,T)$ eine Wurzel von G und

$$G_\alpha := Z_G(\text{Ker } \alpha)^0$$

die zugehörige Gruppe vom halbeinfachen Rang 1 (d.h. nach Faktorisieren nach dem unipotenten Radikal erhält man eine reduktive Gruppe vom Rang 1, vgl. 9.1.5). Nach Definition des Wurzelbegriffs (und des Begriffs des singulären Teiltorus) ist G_α nicht auflösbar. Insbesondere gilt

$$\mathbf{N}_{G_\alpha}(T) \neq \mathbf{Z}_{G_\alpha}(T),$$

d.h. die Weyl-Gruppe $W(G_\alpha,T)$ ist nicht-trivial (nach 8.1.8(ii)). Nach 8.2.2(3) hat sie die Ordnung 2. Wir wählen ein Element

$$n_\alpha \in \mathbf{N}_{G_\alpha}(T) - \mathbf{Z}_{G_\alpha}(T)$$

und bezeichnen mit

$$s_\alpha \in W(G,T)$$

das durch n_α repräsentierte Element. Man beachte, die natürliche Inklusion

$$G_\alpha \to G$$

induziert Inklusionen

$$Z_{G_\alpha}(T) \to Z_G(T) \text{ und } N_{G_\alpha}(T) \to N(T)$$

und damit eine natürliche Abbildung

$$W(T, G_\alpha) \to W(G,T).$$

Diese ist eine injektiver[161] Gruppenhomomorphismus.

9.1.9 Die zu einer Wurzel gehörige Kowurzel, die Spiegelungseigenschaft von s_α

Sei $\alpha \in R(G,T)$ eine Wurzel von G bezüglich T. Dann gilt

(i) Es gibt genau eine 1-parametrige Untergruppe $\alpha^V: \mathbf{G}_m \to T$ mit folgenden Eigenschaften

a) $<\alpha, \alpha^V> = 2$.

b) $s_\alpha \cdot \chi = \chi - <\chi, \alpha^V>\alpha$ für alle $\chi \in X^*(T)$.

c) $s_\alpha \cdot \lambda = \lambda - <\alpha, \lambda>\alpha^V$ für alle $\lambda \in X_*(T)$.

(ii) $s_{-\alpha} = s_\alpha$ und $s_\alpha^2 = 1$.

(iii)[162] a) $w \cdot s_\alpha \cdot w^{-1} = s_{w\cdot\alpha}$ für alle $w \in W(G,T)$.

b) $w \cdot \alpha^V =^{163} (w\cdot\alpha)^V$ für alle $w \in W(G,T)$.

Die 1-parametrigen Untergruppen der Gestalt α^V heißen Kowurzeln von G bezüglich T. Die Menge der Kowurzeln wird mit

$$R^V(G,T)$$

bezeichnet.

Beweis. Zu (i) und (ii). Nach Definition von G_α ist $G_\alpha/R_u G_\alpha$ reduktiv vom halbeinfachen Rang 1. Dann gibt es nach 8.2.9(i) genau eine 1-Parameter-Untergruppe

$$\alpha^V: G_m \to G_\alpha/R_u G_\alpha$$

mit der Eigenschaft, daß (i)b) gilt mit einem maximalen Torus

$$T' \subseteq G_\alpha/R_u G_\alpha$$

---

[161] Wegen $N_{G_\alpha}(T) \cap Z_G(T) = Z_{G_\alpha}(T)$.

[162] W(G,T) operiert durch Konjugation auf T und dadurch auf den Wurzeln und Kowurzeln.

[163] d.h. das Bild der Kowurzel zu α bei w ist gerade die Kowurzel zu $w\cdot\alpha$.

anstelle von T. Es gelten dann (nach 8.2.9(i)) auch (i)a) und die die zweite Identität von (ii).

Insbesondere können wir für T' das Bild von $T \subseteq G_\alpha$ in $G_\alpha/R_u G_\alpha$ nehmen (vgl. das Lemma von 9.1.5). Da $R_u G_\alpha$ unipotent ist, ist die natürliche Projektion $T \to T'$ ein Isomorphismus, d.h. wir können T' in natürlicher Weise mit T identifizieren. Wir bekommen so die entsprechenden Aussagen für T.

Wir haben noch (i)c) und die erste Identität von (ii) zu beweisen.
Zu (i)c). Nach Konstruktion ist s_α eine "orthogonale" Transformation, d.h.

$$<s_\alpha x, s_\alpha \lambda> = <x, \lambda> \text{ für } x \in X \text{ und } \lambda \in X^v.$$

Da s_α selbst-invers ist, impliziert dies,

$$<s_\alpha x, \lambda> = <x, s_\alpha \lambda> \text{ für } x \in X \text{ und } \lambda \in X^v.$$

d.h. s_α ist auch adjungiert. Insbesondere gibt es genau eine Abbildung s' mit

(1) $$<s_\alpha x, \lambda> = <x, s'\lambda> \text{ für } x \in X \text{ und } x^v \in X^v,$$

nämlich $s' = s_\alpha$. Es reicht also zu zeigen, die letzte Identität besteht auch mit

$$s' \cdot \lambda = \lambda - <\alpha, \lambda>\alpha^v.$$

Es gilt

$$\begin{aligned} \text{LHS}(1) &= <x, \lambda - <\alpha, \lambda>\alpha^v> = <x, \lambda> - <\alpha, \lambda><x, \alpha^v> \\ &= <x - <x, \alpha^v>\alpha, \lambda> \\ &= < s_\alpha x, \lambda> \\ &= \text{RHS (1)}. \end{aligned}$$

Zur ersten Identität von (ii). Nach Definition ist $s_\alpha \in W(G,T)$ das durch ein beliebiges Element

$$n_\alpha \in \mathbf{N}_{G_\alpha}(T) - \mathbf{Z}_{G_\alpha}(T),\ G_\alpha := \mathrm{Ker}(\alpha)^0$$

repräsentierte Element der Weyl-Gruppe W(G,T). Ersetzt man α durch $-\alpha$, so ändert sich $\mathrm{Ker}(\alpha)$ nicht, d.h. auch alle anderen Daten bleiben unverändert. Insbesondere ändert sich auch s_α nicht.

Zu (iii). Sie $n \in N_G(T)$ ein Repräsentant von $w \in W(G,T)$. Dann gilt

$$G_{w\cdot\alpha} = \mathrm{Ker}(w\alpha)^0 = n\cdot\mathrm{Ker}(\alpha)^0 n^{-1} = n\cdot G_\alpha n^{-1}.$$

Als Repräsentanten des nicht-trivialen Elements von $W(G_{w\cdot\alpha},T)$ können wir

$$n_{w\cdot\alpha} = n\cdot n_\alpha n^{-1}$$

wählen und erhalten damit

$$s_{w\cdot\alpha} = n\cdot s_\alpha \cdot n^{-1} = w\cdot s_\alpha \cdot w^{-1}$$

Zur zweiten Identität von (iii): Sei $\chi \in X(T)$. Wir verpflanzen χ nacheinander entlang der Konjugation mit $s_{w\cdot\alpha} = n\cdot s_\alpha \cdot n^{-1}$ und erhalten (nach (i)b)

$$\begin{aligned} s_{w\cdot\alpha}\chi &= s_n(s_\alpha(s_n{}^{-1}(\chi)) = s_n(s_n{}^{-1}(\chi) - \langle s_n{}^{-1}(\chi),\alpha^\vee\rangle\alpha) \\ &= \chi - \langle s_n{}^{-1}(\chi),\alpha^\vee\rangle s_n(\alpha) \\ &= \chi - \langle \chi, s_n\alpha^\vee\rangle s_n(\alpha) \quad (s_n \text{ is orthogonal}) \\ &= \chi - \langle \chi , w\,\alpha^\vee\rangle\, w\alpha. \end{aligned}$$

Andererseits gilt nach (i)b) auch

$$s_{w\cdot\alpha}\chi = \chi - \langle\chi, (w\alpha)^\vee\rangle w\alpha .$$

Vergleich liefert

$$\langle\chi , w\,\alpha^\vee\rangle = \langle\chi, (w\alpha)^\vee\rangle$$

für alle $\chi \in X(T)$, also

$$w\,\alpha^\vee = (w\alpha)^\vee$$

wie behauptet.
QED.

9.1.10 Bezüglich der Weyl-Gruppe invariante Metriken

Seien G wie bisher eine zusammenhängende lineare algebraische Gruppe mit dem maximalen Torus T und der Charaktergruppe X = X(T). Wir bezeichnen mit R die Menge der Wurzeln von G und mit

$$R^\vee := \{\, \alpha^\vee \mid \alpha \in R \,\}$$

die Menge der Wurzeln. Weiter sei

$$X_{\mathbb{R}} := X \otimes_{\mathbb{Z}} \mathbb{R}$$

Die Operation der Weyl-Gruppe

$$W = W(G,T)$$

auf T (durch Konjugation) induziert eine Operation von W auf $X_{\mathbb{R}}$.
Weil W endlich ist, gibt es eine positiv definite symmetrische Bilinearform

$$(,): X_{\mathbb{R}} \times X_{\mathbb{R}} \to X_{\mathbb{R}}$$

welche invariant gegenüber der Operation von W ist. Bezüglich jeder solchen Form (,) sind die Abbildungen

$$s_\alpha : X_{\mathbb{R}} \to X_{\mathbb{R}} \ , x \mapsto x - \langle x, \alpha^v \rangle \alpha,$$

($\alpha \in R$)euklidische Spiegelungen. Es gilt

$$\langle x, \alpha^v \rangle = 2(\alpha, \alpha)^{-1}(x, \alpha)$$

für $x \in X_{\mathbb{R}}$, $\alpha \in R$. Benutz man die Form (,) um $X_{\mathbb{R}}$ mit seinem Dual zu identifizieren (und damit R^v mit einer Teilmenge von $X_{\mathbb{R}}$) so gilt

$$\alpha^v = 2(\alpha,\alpha)^{-1}\alpha$$

und

$$R^v = \{\alpha^v = 2(\alpha,\alpha)^{-1}\alpha \mid \alpha \in R\}$$

Beweis. Zur Existenz von (,). Sei

$$f: X_{\mathbb{R}} \times X_{\mathbb{R}} \to X_{\mathbb{R}}$$

irgendeine positiv definite symmetrische Bilinearform. Dann ist auch

$$(x,y) := \sum_{w \in W} f(wx, wy)$$

positiv definit und symmetrisch. Außerdem ist (,) nach Konstruktion W-invariant.

Die Relation $\langle x, \alpha^v \rangle = 2(\alpha, \alpha)^{-1}(x, \alpha)$.

Es gilt $s_\alpha(x) = x - \langle x, \alpha^v \rangle \alpha$ also

(1) $s_\alpha(x) = x$ für $\langle x, \alpha^v \rangle = 0$ (nach Definiton)

(2) $s_\alpha(\alpha) = -\alpha$. (nach Bem.(i) von 9.1.10)

Die erste Identität bedeutet, s_α bildet eine die Hyperebene

$$H_\alpha := \{x \in X_{\mathbb{R}} \mid \langle x, \alpha^v \rangle = 0\}$$

von $X_{\mathbb{R}}$ punktweise in sich ab (dies ist eine Hyperebene, da $\langle , \rangle$ nicht entartet ist). Aus der zweiten Identität folgt für $x \in H_\alpha$

$$(x, \alpha) = (s_\alpha(x), s_\alpha(\alpha)) = (x, -\alpha) \quad \text{(wegen (,) W-invariant)}$$

also

$$2(x, \alpha) = 0,$$

d.h.

(3) $\alpha \perp H_\alpha$

Für beliebiges $x \in X$ können wir

$$x = h + c\alpha \text{ mit } h \in H_\alpha \text{ und } c \in \mathbb{R}$$

schreiben. Dann gilt

$$\begin{aligned} \langle x, \alpha^v \rangle &= \langle h, \alpha^v \rangle + \langle c\cdot\alpha, \alpha^v \rangle \\ &= \langle c\cdot\alpha, \alpha^v \rangle \qquad \text{(wegen } h \in H_\alpha\text{)} \\ &= c\cdot\langle \alpha, \alpha^v \rangle = 2c \quad \text{(nach 9.1.9(i))} \end{aligned}$$

und

$$\begin{aligned} (x, \alpha) &= (h, \alpha) + (c\alpha, \alpha) \\ &= (c\alpha, \alpha) \qquad \text{(wegen (3) und } h \in H_\alpha\text{)} \\ &= (\alpha, \alpha)c \end{aligned}$$

Zusammen ist damit

(4) $\langle x, \alpha^v \rangle = 2(\alpha, \alpha)^{-1} (x, \alpha)$ für beliebige $x \in X$,

d.h. es besteht die behauptete Relation zwischen $\langle\ ,\ \rangle$ und $(\ ,\ )$.

Die Spiegelungseigenschaft von $s_\alpha : X_{\mathbb{R}} \to X_{\mathbb{R}}$.

Wir setzen (4) in die Formel für s_α ein und erhalten

$$s_\alpha(x) = x - 2(\alpha, \alpha)^{-1} (x, \alpha)\alpha ,$$

d.h. s_α ist gerade die Spiegelung an der zu α orthogonalen Hyperebene.

Die Beschreibung der Menge R^v:

Die duale Wurzel α^v ist durch die Bedingung

$$s_\alpha(x) = x - \langle x, \alpha^v \rangle \alpha \text{ für alle } x \in X$$

eindeutig festgelegt. Vergleichen wir dies mit

$$\begin{aligned} s_\alpha(x) &= x - 2\cdot(\alpha, \alpha)^{-1}(x, \alpha)\alpha \\ &= x - (x\ ,\ 2\cdot(\alpha, \alpha)^{-1}\alpha)\alpha \end{aligned}$$

so hat α^v als Funktion auf $X_{\mathbb{R}}$ die Gestalt

$$\alpha^v(x) = (x\ ,\ 2\cdot(\alpha, \alpha)^{-1}\alpha)$$

Benutzen wir das Skalarprodukt (,) um die linearen Funktionen auf $X_{\mathbb{R}}$ mit den Elementen von $X_{\mathbb{R}}$ zu identifizieren, so bedeutet letztere Identität gerade

$$\alpha^v = 2\cdot(\alpha,\alpha)^{-1}\alpha .$$

QED.

Bemerkung

Die obigen Betrachtungen gelten unverändert auch für den Körper $\mathbb{Q}$ der rationalen Zahlen anstelle von $\mathbb{R}$.

9.1.11 Wurzel-Data

Ein Wurzel-Datum ist ein Tupel (X,R,X^v,R^v) bestehend aus

1. zwei freien abelschen Gruppen X und X^v endlichen Rangs, die mit einer nicht-entarteten Paarung
$$X\times X^v \to \mathbb{Z},\ (x,x^v) \mapsto \langle x,x^v\rangle,$$
versehen sind,
2. zwei endlichen Teilmengen $R\subseteq X$ und $R^v\subseteq X^v$, zu denen eine Bijektion
$$R \to R^v,\ \alpha \mapsto \alpha^v,$$
gehört.

Für jedes $\alpha\in R$ setzen wir

$$s_\alpha x := x - \langle x,\alpha^v\rangle\alpha \text{ für jedes } x\in X$$

$$s_\alpha x^v := x^v - \langle \alpha, x^v\rangle\alpha^v \text{ für jedes } x^v\in X^v.$$

Die folgenden Axiome sollen erfüllt sein.

(RD1) $\langle\alpha,\alpha^v\rangle = 2$ für jedes $\alpha\in R$.

(RD2) $s_\alpha(R)\subseteq R$ und $s_\alpha(R^v)\subseteq R^v$ für jedes $\alpha\in R$.

Bemerkungen.

(i) Aus (RD1) folgt $s_\alpha^2 = \mathrm{Id}$, $s_\alpha(\alpha) = -\alpha$ und $s_\alpha(\alpha^v) = -\alpha^v$.

(ii) Sei (X,R,X^v,R^v) ein Wurzel-Datum mit $R\neq\emptyset$. Bezeichne Q die von R erzeugte Untergruppe von X und sei $V := Q\otimes_{\mathbb{Z}}\mathbb{R}$. Dann ist R ein Wurzelsystem im Sinne von N. Bourbaki: Algèbre de Lie, Hermann, Paris 1971-75, Ch. VI, no. 1, d.h. es gelten folgende Axiome.

(RS1) R ist endlich und erzeugt V, $0\notin R$.

(RS2) Für jedes $\alpha \in R$ gibt es ein $\alpha^V \in V^V$ aus dem Dual V^V von V mit $<\alpha, \alpha^V> = 2$ und die zu α gehörige Spiegelung s_α stabilisiert R.

(RS3) Für $\alpha \in R$ gilt $\alpha^V(R) \subseteq \mathbb{Z}$.

Der Rang des Wurzelsystems R ist definiert als die Dimension von V.

(iii) Seien R := R(G,T) die Menge der Wurzeln der algebraischen Gruppe G bezüglich des maximalen Torus T,

$$X := X^*(T),\ X^V := X_*(T)$$

und $R^V := R^V(G,T)$ die in 9.1.9 eingeführte Menge der Kowurzeln. Dann ist (X,R, X^V,R^V) ein Wurzel-Datum. Dieses Wurzel-Datum wird mit

$$\Psi = \Psi(G,T)$$

bezeichnet.

Beweis . Zu (i). Es gilt

$$\begin{aligned} s_\alpha^2 x &= s_\alpha(x - <x, \alpha^V>\alpha) \\ &= x - <x, \alpha^V>\alpha - < x - <x, \alpha^V>\alpha, \alpha^V>\alpha \\ &= x - <x, \alpha^V>\alpha - <x , \alpha^V>\alpha + <x, \alpha^V>< \alpha\ \alpha^V>\alpha \\ &= x - <x, \alpha^V>\alpha - <x , \alpha^V>\alpha + <x, \alpha^V>2\alpha \qquad \text{(wegen RD1)} \\ &= x \end{aligned}$$

Die Rechnung für die Elemente aus X^V ist analog. Weiter gilt

$$\begin{aligned} s_\alpha(\alpha) &= \alpha - <\alpha, \alpha^V>\alpha \quad \text{nach Definition von } s_\alpha \\ &= -\alpha. \end{aligned}$$

Die Rechnung für die duale Wurzel ist analog.

Zu (ii). (RS1). Die Endlichkeit von R gilt nach Voraussetzung und die Tatsache, daß R den Raum V erzeugt, nach Konstruktion. Die zweite Bedinung ist erfüllt wegen $<\alpha, \alpha^V> = 2$ für jede Wurzel.

(RS2). Folgt direkt aus (RD1) und (RD2). Die Paarung

$$< , >: X \times X^V \to \mathbb{Z}$$

erlaubt es, das Erzeugnis V^V von R^V mit dem Dual von V zu identifizieren.

(RS3). Kommt von der Tatsache, daß < , > über $\mathbb{Z}$ definiert ist.

Zu(iii). Die Endlichkeit von R und R^V folgt aus 9.1.7. Die Inklusion

$$s_\alpha(R) \subseteq R$$

aus 9.1.6. Schließlich folgt

$$s_\alpha(R^V) \subseteq R^V$$

aus der zweiten Identität von 9.1.9 (iii)(b). Wir haben noch die Bijektivität von

$$R \to R^V, \alpha \mapsto \alpha^V,$$

zu beweisen. Die Surjektivität ergibt sich aus der Definition von R^V. Seien α und β zwei Wurzeln mit

$$\alpha^V = \beta^V.$$

Wir haben zu zeigen, es gilt $\alpha = \beta$. Nach 9.1.10 können wir eine Metrik $(,)$ auf $X = X \otimes_{\mathbb{Z}} \mathbb{R}$ einführen, mit

$$\langle x, \alpha^V \rangle = 2(\alpha, \alpha)^{-1} (x, \alpha)$$

und

$$\alpha^V = 2(\alpha,\alpha)^{-1}\alpha$$

für jedes $x \in X$ und jede Wurzel α. Aus der letzten Identität ergibt sich insbesondere, daß α und β proportional sind und daß die Formeln

$$s_\alpha(x) = x - \langle x, \alpha^V \rangle \alpha$$

$$s_\beta(x) = x - \langle x, \beta^V \rangle \beta$$

Spiegelungen an derselben Hyperebene beschreiben. Insbesondere gilt

$$s_\alpha(x) = s_\beta(x) \text{ für jedes } x \in X,$$

d.h.

$$x - \langle x, \alpha^V \rangle \alpha = x - \langle x, \beta^V \rangle \beta = x - \langle x, \alpha^V \rangle \beta$$

d.h.

$$\langle x, \alpha^V \rangle (\alpha - \beta) = 0$$

für jedes $x \in X$. Speziell für $x = \alpha$ folgt

$$2(\alpha - \beta) = 0$$

d.h. $\alpha = \beta$.

QED.

9.1.12 Reduziertheit des Wurzel-Datums $\Psi(G,T)$

Sei $(X,R, X^V,R^V) = \Psi(G,T)$ das Wurzel-Datum der algebraischen Gruppe G bezüglich des maximalen Torus T. Es gelte

$$\alpha \in R \text{ und } r\alpha \in R \text{ für ein } r \in \mathbb{Q}.$$

Dann ist $r = \pm 1$. Ein Wurzel-Datum mit dieser zusätzlichen Eigenschaft heißt reduziert.

Beweis. Nach Definition gilt

$$G_\alpha := (\mathrm{Ker}\ \alpha)^0 = (\mathrm{Ker}\ r\alpha)^0.$$

Nach Definition des Wurzelbegriffs gehören zu $\pm r\alpha$ auf

$$L(G_\alpha/R_u G_\alpha)$$

nicht-triviale Eigenräume bezüglich der adjungierten Operation von T. Und diese Eigenräume sind Eigenräumen zu nicht-trivialen Charakteren. Nach 9.1.5 ist $r\alpha$ dadurch bis auf das Vorzeichen eindeutig bestimmt, also gleich $\pm\alpha$.

QED.

9.1.13 Erzeugbarkeit der Weyl-Gruppe durch die Spiegelungen s_α

Seien G eine zusammenhängende lineare algebraische Gruppe und T ein maximaler Torus von G. Dann wird die Weyl-Gruppe

$$W(G,T)$$

durch die Spiegelunge s_α mit $\alpha \in R(G,T)$ erzeugt.

Beweis. Wir führen den Beweis durch Induktion nach dim G. Der Fall dim G = 0 ist trivial. Falls W = W(G,T) trivial ist, ist nichts zu beweisen. Sei also

(1) $$W \neq \{e\}.$$

Falls R(G,T) leer ist, d.h. es gibt keine Wurzeln, so sind alle Teiltori

$$S \subseteq T$$

der Kodimensions 1 regulär, d.h. $Z_G(S)$ ist auflösbar. Nach 9.1.3 wird G von den Zentralisatoren $Z_G(S)$ erzeugt (welche zusammenhängend sind nach 7.3.5). Nach 6.1 wird also G von endlich vielen auflösbaren Untergruppen erzeugt und ist damit selbst auflösbar. Nach 8.1.8 ist dann aber W trivial. Für den weiteren Beweis können wir also annehmen,

$$R(G,T) \neq \varnothing.$$

Sei

$$e \neq w \in W$$

und sei

$$n \in N_G(T)$$

ein Repräsentant von w. Wir betrachten den Morphismus

$$\phi: T \to T,\ t \mapsto ntn^{-1}t^{-1}\ .$$

Weil T abelsch ist, ist dies ein Homomorphismus algebraischer Gruppen.[164] Wir unterscheiden jetzt die beiden Fälle, daß ϕ surjektiv ist bzw. es nicht ist.

1. Fall: ϕ ist nicht surjektiv.

Dann ist

$$S := \mathrm{Ker}(\phi)^0$$

ein echter Teiltorus von T. Jedes Element s aus diesem Kern kommutiert mit n, d.h. Konjugation mit n induziert die identische Abbildung auf S.

Fall 1.1: S liegt im Zentrum von G.

Wir setzen

$G' := G/S$

$T' := T/S$

Dann ist T' ein maximaler Torus von G' (vgl. 1. Schritt im Beweis von 9.1.5). Bezeichne

$$\rho: G \to G'$$

die natürliche Abbildung. Für jeden Torus U mit

$$S \subseteq U \subseteq T$$

setzen wir U':= U/S. Es gilt dann

(2) $$\rho^{-1}(N_{G'}(U')) = N_G(U)$$

und

(3) $$\rho^{-1}(Z_{G'}(U')) = Z_G(U)$$

Die Identität (2) ist einfach und in Inklusion '$\supseteq$' von (3) ebenfalls. Beweisen wir die Inklusion '$\subseteq$' von (3). Dazu betrachten wir den Morphismus affiner algebraischer Varietäten

$$\Phi: V \times U \to U,\ (z, u) \mapsto zuz^{-1}u^{-1},\ \text{mit } V := \rho^{-1}(Z_{G'}(U')).$$

Φ ist korrekt definiert, denn für $z \in V$ und $u \in U$ liegt

$$\rho(zuz^{-1}) = \rho(z)\rho(u)\rho(z^{-1})$$

in U', d.h. zuz^{-1} liegt in $\rho^{-1}(U') = U$. Dann liegt aber auch $zuz^{-1}u^{-1}$ in U. $\Phi(z, ?): U \to U$ ist ein Homomorphismus algebraischer Gruppen für jedes $z \in V$:

Zu mindest trifft dies zu für

$$U \to U,\ u \mapsto zuz^{-1},\ \text{und } U \to U,\ u) \mapsto u^{-1},$$

denn U ist kommutativ. Dann ist dies aber auch der Fall für das Produkt dieser beiden Homomorphismen (weil U kommutativ ist).

Nach dem Starrheitssatz 2.5.10 ist damit aber

---

[164] ϕ ist das Produkt der beiden Homomorphismen $t \mapsto ntn^{-1}$ und $t \mapsto t^{-1}$.

$$\Phi(z, u) \text{ unabhängig von } z \in V,$$

d.h. es gilt

$$zuz^{-1}u^{-1} = \Phi(z, u) = \Phi(e, u) = e,$$

d.h.

$$zuz^{-1} = u \text{ für } z \in V \text{ und } u \in U.$$

Mit anderen Worten, es gilt $V \subseteq Z_G(U)$, d.h. es besteht in (3) auch die Inklusion '$\subseteq$'.

Aus (2) und (3) ergibt sich insbesondere

$$W(G',T') = \rho^{-1}(N_G,(T'))/\rho^{-1}(Z_G,(T')) = N_G(T)/Z_G(T) = W(G,T).$$

Nach Induktionsvoraussetzung ist jedes Element von W(G',T') ein Produkt von Elementen der Gestalt s_α, mit $\alpha' \in R(G',T')$. Es reicht also zu zeigen, jedes s_α, kommt von einer Wurzel aus R(G,T). Die Wurzel α' von G' ist insbesondere ein Charakter von T',

$$\alpha': T' \to G_m .$$

Sei α die Zusammensetzung von α' mit der natürlichen Abbildung,

$$\alpha: T \xrightarrow{\rho|T} T' \xrightarrow{\alpha'} G_m .$$

Es reicht zu zeigen, α ist eine Wurzel von G mit $s_\alpha = s_{\alpha'}$. Seien

$$U' := \mathrm{Ker}(\alpha')^0 \text{ bzw. } U := \mathrm{Ker}(\alpha)^0$$

die zu α' bzw. α gehörigen singulären Tori. Dann besteht eine exakte Sequenz

$$0 \to S \to U \xrightarrow{\rho|U} U'$$

und es gilt

$$\dim U = \dim U' + \dim S,$$

d.h. das Bild von U in U' hat dieselbe Dimension wie U', d.h. man hat sogar eine exakte Sequenz

$$0 \to S \to U \xrightarrow{\rho|U} U' \to 0$$

und es gilt

$$U = \rho^{-1}(U').$$

Damit hat man auch eine exakte Sequenz

$$0 \to S \to Z_G(U) \xrightarrow{\rho'} Z_G,(U') \to 0 \text{ mit } \rho' = \rho|_{Z_G(U)}$$

(die Surjektivität der Abbildung rechts ergibt sich aus (3)). Weil U' ein singulärer Torus ist, ist

$$Z' := Z_G,(U')$$

nicht auflösbar. Wegen der Exaktheit der letzten Sequenz ist dann aber auch

$$Z := Z_G\ (U)$$

nicht auflösbar, d.h. U ist ein singulärer Torus. Insbesondere haben wir Zerlegungen (vgl. 8.2.7(vii)):

$L(Z'/R_uZ') = L(T')\oplus kX_\alpha,\oplus kX_{-\alpha}$,

$L(Z/R_uZ) = L(T)\oplus kX_\beta\oplus kX_{-\beta}$ für ein $\beta\in R(G,T)$

und die Surjektion ρ' induziert eine Surjektion

$L(Z/R_uZ) \to L(Z'/R_uZ')$

Diese Surjektion ist äquivariant bezüglich der durch die Konjugation mit Elementen von G induzierten Operationen. Die Multiplikation mit den Charakteren β bzw. $-\beta$ auf den Teilräumen kX_β bzw. $kX_{-\beta}$ geht bei dieser Surjektion über in die Multiplikation mit eben diesen Charakteren, d.h. β und $-\beta$ faktorisieren sich über die natürliche Abbildung

$$T \to T'$$

wobei die zugehörigen Charaktere von T' gerade α' bzw. $-\alpha'$ sein müssen. Es folgt

$$\beta = \pm\alpha.$$

Insbesondere ist α eine Wurzel von G und für die Konjugation (auf T bzw. T') mit den zugehörigen Elementen der Weyl-Gruppe gilt

$$s_\alpha = s_\beta = s_\alpha, .$$

Fall 1.2: S liegt nicht im Zentrum von G.
Es gilt dann

$$(T \subseteq)\ Z_G(S) \neq G.$$

Da n mit den Elementen von S kommutiert, gilt

$$n \in Z_G(S).$$

Die singulären Teiltori[165] von T bezüglich $Z_G(S)$ sind auch singuläre Teiltori bezüglich G. Deshalb gilt

$$R(Z_G(S), T) \subseteq R(G, T).$$

Trivialerweise gilt[166]

---

[165] d.h. diejenigen Teiltori der Kodimension 1, deren Zentralisator nicht auflösbar ist.

[166] Ein Element aus $N_{Z_G(S)}(T) \subseteq N_G(T)$, welches in $Z_G(T)$ liegt, liegt auch in

$$(w\in)\ W(Z_G(S), T) \subseteq W(G, T).$$

Wir wenden die Induktionsvoraussetzung auf $Z_G(S)$ an und erhalten, daß w ein Produkt von Spielgelungen ist.

2. Fall: ϕ ist surjektiv.
Die Induzierte Abbildung auf den Charakteren ist dann injektiv, d.h.

$$X \to X,\ x \mapsto (w^{-1} - Id)x\ ,$$

ist injektiv. Dann ist aber auch die induzierte $\mathbb{R}$-lineare Abbildung

$$X_{\mathbb{R}} \to X_{\mathbb{R}}$$

injektiv, also bijektiv. Sei $\alpha\in R(G,T)$ eine Wurzel.Dann gibt es einen Charakter $\chi_\alpha\in X$ mit

$$(w^{-1} - Id)\chi_\alpha = \alpha.$$

Da α als Wurzel nicht trivial ist, ist auch χ_α nicht trivial. Ist $(\ ,\ )$ wie bisher das W-invariante euklidische Skalarprodukt, so folgt

$$(\chi_\alpha, \chi_\alpha) = (w^{-1}\chi_\alpha, w^{-1}\chi_\alpha) = (\chi_\alpha+\alpha\ , \chi_\alpha+\alpha\ )$$
$$= (\chi_\alpha, \chi_\alpha) + 2(\chi_\alpha,\alpha\ ) + (\alpha\ ,\alpha\ ),$$

also

$$2(\chi_\alpha,\alpha\ ) + (\alpha\ ,\alpha\ ) = 0,$$

also

$$<\chi_\alpha, \alpha^v> = 2(\alpha\ ,\alpha\ )^{-1}\ (\chi_\alpha,\alpha\ ) = -1.$$

Damit ist

$$s_\alpha(\chi_\alpha) = \chi_\alpha - <\chi_\alpha, \alpha^v>\alpha = \chi_\alpha +\alpha\ = w^{-1}\chi_\alpha\ ,$$

d.h.

$$ws_\alpha(\chi_\alpha) = \chi_\alpha,$$

d.h. χ_α bleibt fest bei

$$w' := ws_\alpha \in W.$$

Sei $n'\in N_G(T)$ ein Repräsentant für w' und

$$\phi': T \to T,\ t \mapsto n'tn'^{-1}t^{-1}\ .$$

$$Z_{Z_G(S)}(T).$$

die zu ϕ analoge Abbildung. Wie oben betrachten wir die durch ϕ' auf den Charakteren induzierte Abbildung

$$X \to X,\ x \mapsto (w'^{-1} - Id)x\ ,$$

Wegen $w'(\chi_\alpha) = \chi_\alpha$ ist diese nicht injektiv, d.h. w' genügt nicht wie w den Bedingungen des 2. Falls. Damit ist w' wie im ersten Fall und damit ein Produkt von zu Wurzeln gehörigen Spiegelungen. Wegen

$$w' = ws_\alpha$$

d.h. $w = w's_\alpha$ gilt dann aber dasselbe für w.

QED.

9.1.13 Aufgaben

(1) Seien $\Phi := (X,R,X^v,R^v)$ ein Wurzel-Datum und p der Gruppenhomomorphismus

$$p: X \to X^v\ ,\ x \mapsto \sum_{\alpha\in R} <x,\ \alpha^v>\ \alpha^v.$$

(a) Man leite aus der Identität

$$<\alpha, \beta^v>^2\alpha^v = <\alpha, \beta^v>\beta^v + <\alpha, s_\alpha(\beta^v)>s_\alpha(\beta^v)$$

ab, daß gilt

$$p(\alpha) = \frac{1}{2} <\alpha, p(\alpha)>\alpha^v$$

für jedes $\alpha\in R$. Man zeige weiter

$$X_0 := Ker(p) = \{x\in X \mid <x, \alpha^v> = 0 \text{ für alle } \alpha\in R\}.$$

(b) Man zeige, es gilt

$$Q\cap X_0 = \{0\} \text{ und } [X: Q+X_0] < \infty.$$

Dabei bezeichne wie bisher Q die von den Wurzeln erzeugte Untergruppe von X,

$$Q = <R>.$$

(c) Die Weyl-Gruppe $W(\Phi)$ ist definiert als die Gruppe der Endomorphismen von X, die von den s_α erzeugt wird. Man zeige, $W(\Phi)$ ist eine endliche Gruppe.

In den beiden nachfolgenden Aufgaben seien G und T wie in 9.1.1 und

$$W = W(G,T),$$

d.h. G sei eine zusammenhängende lineare algebraische Gruppe und T sei ein maximaler Torus von G.

(2) Ist $w \in W$ ein Element welches $x \in X_{\mathbb{R}}$ fest läßt, so ist w ein Produkt von Spiegelungen, welche x ebenfalls festlassen.

(3) Hat G den halbeinfachen Rang r, so ist jedes Element $w \in W$ Produkt von höchstens r Spiegelungen s_α.

Lösungen

Zu (1)(a).

Zur ersten Identität:

Nach 9.1.9 gilt

$$s_\alpha \cdot \lambda = \lambda - <\alpha, \lambda>\alpha^v \text{ für } \lambda \in X^v$$

also

$$<\alpha, s_\alpha(\beta^v)> s_\alpha(\beta^v) = (<\alpha, \beta^v - <\alpha, \beta^v>\alpha^v>)(\beta^v - <\alpha, \beta^v>\alpha^v)$$

$$= <\alpha, \beta^v> \beta^v - <\alpha, \beta^v>^2\alpha^v$$

$$- < \alpha, \alpha^v><\alpha, \beta^v> \beta^v+< \alpha, \alpha^v><\alpha, \beta^v>< \alpha, \beta^v>\alpha^v$$

$$= -<\alpha, \beta^v> \beta^v + <\alpha, \beta^v>^2\alpha^v \quad \text{(wegen } < \alpha, \alpha^v> = 2 \text{ nach 9.1.9).}$$

Dies ist die gesuchte erste Identität.

Zur Formel für $p(\alpha)$.

Es gilt nach Definition von p und der gerade bewiesenen Formel

$$p(\alpha) = \sum_{\beta \in R} <\alpha, \beta^v> \beta^v$$

$$= \sum_{\beta \in R} (<\alpha, \beta^v>^2\alpha^v - <\alpha, s_\alpha(\beta^v)>s_\alpha(\beta^v))$$

Da s_α Kowurzeln in Kowurzeln abbildet und selbstinvers ist, folgt

$$p(\alpha) = \sum_{\beta \in R} <\alpha, \beta^v>^2\alpha^v - \sum_{\beta \in R} <\alpha, \beta^v> \beta^v) = \sum_{\beta \in R} <\alpha, \beta^v>^2\alpha^v - p(\alpha)$$

also

$$p(\alpha) = \frac{1}{2} (\sum_{\beta \in R} <\alpha, \beta^v><\alpha, \beta^v>) \alpha^v$$

$$= \frac{1}{2} (\sum_{\beta \in R} <\alpha, <\alpha, \beta^v>\beta^v>)\alpha^v$$

$$= \frac{1}{2} < \alpha, (\sum_{\beta \in R} <\alpha, \beta^v> \beta^v) > \alpha^v$$

$$= \frac{1}{2} < \alpha, p(\alpha) > \alpha^v$$

Zur Beschreibung des Kerns von p.
Wir setzen

$$X_0 := \{x \in X \mid <x, \alpha^v> = 0 \text{ für alle } \alpha \in R\}$$

und haben zu zeigen $X_0 = \mathrm{Ker}(p)$. Für $x \in X_0$ gilt nach Definition von p,

$$p(x) = \sum_{\alpha \in R} <x, \alpha^v> \alpha^v = 0,$$

d.h. es ist

$$X_0 \subseteq \mathrm{Ker}(p).$$

Sei jetzt $\chi \in \mathrm{Ker}(p)$. Wir haben zu zeigen,

$$<\chi, \alpha^v> = 0 \text{ für jedes } \alpha \in R.$$

Beim Beweis können wir p durch die $\mathbb{Q}$-lineare Abbildung

$$p: X_{\mathbb{Q}} \to X^v_{\mathbb{Q}}, \; x \mapsto \sum_{\alpha \in R} <x, \alpha^v> \alpha^v,$$

mit derselben Abbildungsvorschrift ersetzen. Wir führen eine W-invariante positiv-definite und W-invariante symmetrische Bilinearform

$$(,): X_{\mathbb{Q}} \times X_{\mathbb{Q}} \to \mathbb{Q}$$

ein und benutzen diese um $X^v_{\mathbb{Q}}$ mit $X_{\mathbb{Q}}$ zu identifizieren. Nach 9.1.12 (und der anschließenden Bemerkung) wird dann

$$<x, \alpha^v> = 2(\alpha, \alpha)^{-1}(x, \alpha)$$

$$\alpha^v = 2(\alpha, \alpha)^{-1}\alpha \text{ für jedes } \alpha \in R.$$

Insbesondere bekommt dann die Abbildung p die Gestalt

$$p: X_{\mathbb{Q}} \to X^v_{\mathbb{Q}}, \; x \mapsto \sum_{\alpha \in R} 4(\alpha, \alpha)^{-2}(x, \alpha)\alpha.$$

Weiter sei wie bisher

$$Q_{\mathbb{Q}} := \sum_{\alpha \in R} \mathbb{Q}\,\alpha$$

der von den Wurzel erzeugte Unterraum von $X_{\mathbb{Q}}$. Dann gilt

$$X_{\mathbb{Q}} = Q_{\mathbb{Q}} \oplus Q_{\mathbb{Q}}^{\perp}$$

wobei das orthogonale Komplement bezüglich (,) zu nehmen ist. Für $x \in Q_{\mathbb{Q}}^{\perp}$ gilt $(x, \alpha) = 0$, also $\langle x, \alpha^{v} \rangle = 0$, also $x \in (X_0)_{\mathbb{Q}}$, d.h. es ist

$$Q_{\mathbb{Q}}^{\perp} \subseteq (X_0)_{\mathbb{Q}} \subseteq \mathrm{Ker}(p).$$

Es reicht zu zeigen, es gilt überall das Gleichheitszeichen. Dazu reicht es zu zeigen,

$$(\dim X_{\mathbb{Q}} - \dim Q_{\mathbb{Q}}) = \dim Q_{\mathbb{Q}}^{\perp} = \dim \mathrm{Ker}(p) \; (= \dim X_{\mathbb{Q}} - \dim \mathrm{Im}(p)),$$

d.h.

$$\dim Q_{\mathbb{Q}} = \mathrm{Im}\,(p).$$

Nach Definition gilt $\mathrm{Im}(p) \subseteq Q_{\mathbb{Q}}$. Es reicht zu zeigen, $\mathrm{Im}(p) = Q_{\mathbb{Q}}$. Der Raum $Q_{\mathbb{Q}}$ wird von den $\alpha \in R$ erzeugt. Es reicht also zu zeigen,

$$\alpha \in \mathrm{Im}(p) \text{ für jedes } \alpha \in R.$$

Wie wir oben gesehen haben, ist das Bild von α ein Vielfaches von α,

$$p(\alpha) = \frac{1}{2} \langle \alpha, p(\alpha) \rangle \alpha^{v} = \frac{1}{2} \langle \alpha, p(\alpha) \rangle \, 2(\alpha,\alpha)^{-1} \alpha.$$

Es reicht also, zu zeigen,

$$p(\alpha) \neq 0 \text{ für jedes } \alpha \in R.$$

d.h. es reicht zu zeigen,

$$(1) \qquad p(\alpha) = \sum_{\beta \in R} 4(\beta, \beta)^{-2} (\alpha,\beta)\beta \neq 0 \text{ für jedes } \alpha \in R.$$

Sei jetzt $\alpha \in R$ fest vorgegeben. Wir lassen in (1) alle Summanden weg, für welche β orthogonal zu α ist und betrachten einen der übrig gebliebenen Summanden (zum Beispiel den mit $\beta = \alpha$). Es gilt

$$(\alpha,\beta) \neq 0.$$

Wir betrachten die Hyperebene der zu α orthogonalen Vektoren und wählen einen zu β proportionalen Einheitsvektor[167]

---

[167] Wir betrachten vorübergehend $X_{\mathbb{Q}}$ als Unterraum von $X_{\mathbb{R}}$ und führen die weiteren Rechnungen in dem größeren Raum durch.

$$v_\beta = r\cdot\beta$$

der auf derselben Seite der Hyperebene liegt wie α. Dann gilt

$$(v_\beta , v_\beta) = 1 \text{ und } (\alpha, v_\beta) > 0$$

also

$$4(\beta,\beta)^{-2}(\alpha,\beta)\beta = 4(v_\beta, v_\beta)^{-2}(\alpha, v_\beta)\, v_\beta = 4\,(\alpha, v_\beta)\, v_\beta.$$

Damit ist

$$p(\alpha) = \sum_{\beta\in R} 4\,(\alpha, v_\beta)\, v_\beta$$

eine konvexe Linearkombination von Vektoren, die alle auf derselben Seite der zu α orthogonalen Hyperebene liegen. Da mindestens ein von Null verschiedener Summand vorkommt (der mit $\beta = \alpha$), ist diese Summe ungleich Null.

Zu (1)(b).

Zum Beweis der ersten Identität reicht es zu zeigen, daß sogar

$$Q_{\mathbb{Q}}\cap(X_0)_{\mathbb{Q}} = \{0\}.$$

gilt. Das folgt aber aus dem Beweis von (1)(a), denn dort haben wir gezeigt, es gilt

$$(X_0)_{\mathbb{Q}} = Q_{\mathbb{Q}}^{\perp}$$

bezüglich einer W-invarianten positiv definiten Bilinearform (,) auf dem Vektorraum $X_{\mathbb{Q}}$.

Zur zweiten Identität. Es gilt

$$X_{\mathbb{Q}} = Q_{\mathbb{Q}}\oplus Q_{\mathbb{Q}}^{\perp} = Q_{\mathbb{Q}}\oplus(X_0)_{\mathbb{Q}}$$

Es gibt also Elemente[168]

$$x_1,\ldots,x_r \in Q$$

und

$$x_{r+1},\ldots,x_s \in X_0$$

die zusammen eine Basis des Vektorraums $X_{\mathbb{Q}}$ bilden. Jedes Element von X ist deshalb eine $\mathbb{Q}$-Linearkombination der x_i. Mit anderen Worten, jedes Element von

$$X/(Q+X_0)$$

wird von einer natürlichen Zahl annulliert (dem Hauptnenner in der Darstellung eines Repräsentanten als Linearkombination der x_i). Die

---

[168] Q ist nach Definition die von den Wurzeln $\alpha\in R$ erzeugte Untergruppe von X.

Faktorgruppe $X/(Q+X_0)$ ist somit eine endlich erzeugte abelsche Gruppe ohne freie Bestandteile, d.h. sie ist endlich.

Zu (1)(c).

Jeder Automorphismus $X \to X$ induziert einen Automorphismus auf den zugehörigen $\mathbb{Q}$-Vektorräumen, d.h. wir haben einen Gruppenhomomorphismus

$$\mathrm{Aut}(X) \to \mathrm{Aut}_{\mathbb{Q}}(X_{\mathbb{Q}}) = \mathrm{Aut}_{\mathbb{Q}}(Q_{\mathbb{Q}} \oplus Q_{\mathbb{Q}}^{\perp})$$

Da X eine freie abelsche Gruppe ist, können wir X als Teilmenge von $X_{\mathbb{Q}}$ auffassen, d.h. dieser Homomorphismus ist injektiv,

$$\mathrm{Aut}(X) \subseteq \mathrm{Aut}_{\mathbb{Q}}(Q_{\mathbb{Q}} \oplus Q_{\mathbb{Q}}^{\perp}),\ \sigma \mapsto \sigma_{\mathbb{Q}}$$

Die Spiegelungen s_α bilden das Erzeugendensystem R von $Q_{\mathbb{Q}}$ in sich ab,

$$s_\alpha(Q_{\mathbb{Q}}) \subseteq Q_{\mathbb{Q}}$$

und lassen außerdem jedes Element von $Q_{\mathbb{Q}}^{\perp} = (X_0)_{\mathbb{Q}}$ fest[169],

$$s_\alpha \mid Q_{\mathbb{Q}}^{\perp} = \mathrm{Id}.$$

Deshalb ist der Gruppenhomomorphismus

$$W(\Phi) \to \mathrm{Aut}_{\mathbb{Q}}(Q_{\mathbb{Q}}),\ \sigma \mapsto (\sigma_{\mathbb{Q}})|_{Q_{\mathbb{Q}}}$$

injektiv, d.h. wir können $\mathrm{Aut}(X)$ als Untergruppe von $\mathrm{Aut}_{\mathbb{Q}}(Q_{\mathbb{Q}})$ auffassen,

$$W(\Phi) \subseteq \mathrm{Aut}_{\mathbb{Q}}(Q_{\mathbb{Q}}),\ \sigma \mapsto (\sigma_{\mathbb{Q}})|_{Q_{\mathbb{Q}}}.$$

Außerdem bilden die Elemente von $W(\Phi)$ das Erzeugendensystem R von $Q_{\mathbb{Q}}$ in sich ab und sind durch ihre Wirkung auf R bereits eindeutig festgelegt. Damit ist sogar die Abbildung

$$W(\Phi) \to \mathrm{Aut}(R),\ \sigma \mapsto (\sigma_{\mathbb{Q}})|_R.$$

Die Automorphismengruppe der endlichen Menge R ist aber endlich. Also ist auch $W(\Phi)$ endlich.

Zu (2).

Wir wiederholen den Beweis von 9.1.12. Alle Argumente lassen sich für die hier behandelte Frage verwenden. Die Behandlung des zweiten

---

[169] Für $x \in Q_{\mathbb{Q}}^{\perp}$ gilt $s_\alpha(x) = x - \langle x, \alpha^v \rangle \alpha = x - 2(\alpha,\alpha)^{-1}(x,\alpha)\alpha = x$, denn $(x,\alpha) = 0$ für $x \in Q_{\mathbb{Q}}^{\perp}$.

Falls vereinfacht sich: da es nach Voraussetzung ein $x \in X$ gibt mit $w(x) = x$ ist die durch

$$\phi: T \to T,\ t \mapsto ntn^{-1}t^{-1} .$$

auf den Charakteren induzierte Abbildung

$$X \to X,\ x \mapsto (w^{-1} - Id)x ,$$

niemals injektiv, d.h. ϕ ist nicht surjektiv, d.h. der zweite Fall tritt nicht auf.

Zu (3).

Man wiederhole die Argumente des Beweises von 9.1.12. Nur im zweiten Fall vergrößert sich die Anzahl der Faktoren der Zerlegung von w in Spiegelungen s_α (und zwar um 1). Dieser zweite Fall wird aber auf den ersten zurückgeführt, und bei letzterem verkleinert sich der halbeinfache Rang: auch im Fall, daß S nicht im Zentrum von G liegt und man von G zu $Z_G(S)$ übergehen muß. Dann S liegt im Zentrum von $Z_G(S)$ und man kann weiter von $Z_G(S)$ zu $Z_G(S)/S$ übergehen. QED

9.2 Die gegenseitige Lage der Wurzeln zueinander

In diesem Abschnitt leiten wir Aussagen zur gegenseitigen Lage der Wurzeln zueinander her, wie wir sie später benötigen.

9.2.1 Die Situation

$$\Phi := (X, R, X^v, R^v)$$

sei ein Wurzel-Datum. Die Gruppe

$$W = W(\Phi),$$

die von den Spiegelungen s_α mit $\alpha \in R$ erzeugt wird, ist endlich (siehe Aufgabe 9.1.13 (1)(c). Bezeichne

$$(,): X_{\mathbb{R}} \times X_{\mathbb{R}} \to \mathbb{R}$$

eine positiv definite Bilinearform auf $X_{\mathbb{R}}$, welche W-invariant ist.

9.2.2 Lemma: Eine Schranke für $|<\alpha, \beta^v>|$

Seien $\alpha, \beta \in R$ zwei linear unabhängige Wurzeln. Dann gilt:

(i) $0 \le <\alpha, \beta^v><\beta, \alpha^v> \le 3$

$|<\alpha, \beta^v>| \in \{0, 1, 2, 3\}$

Ist $|<\alpha, \beta^v>| > 1$ so gilt $|<\beta, \alpha^v>| = 1$.

(ii) $<\alpha, \beta^v> = 0 \Leftrightarrow <\beta, \alpha^v> = 0$.

Beweis. Zu (i). Es gilt

$$s_\alpha s_\beta(\alpha) = s_\alpha(\alpha - <\alpha, \beta^V>\beta)$$
$$= (\alpha - <\alpha, \beta^V>\beta) - <\alpha - <\alpha, \beta^V>\beta, \alpha^V>\alpha$$
$$= (1 - <\alpha, \alpha^V> + <\alpha, \beta^V><\beta, \alpha^V>)\alpha - <\alpha, \beta^V>\beta$$
$$= (<\alpha, \beta^V><\beta, \alpha^V> - 1)\alpha - <\alpha, \beta^V>\beta$$

und

$$s_\alpha s_\beta(\beta) = s_\alpha(\beta - <\beta, \beta^V>\beta)$$
$$= s_\alpha(-\beta)$$
$$= -\beta + <\beta, \alpha^V>\alpha$$

Die Abbildung $s_\alpha s_\beta$ stabilisiert den von α und β aufgespannten Unterraum und hat bezüglich der Basis α, β auf diesem Unterraum die Matrix

$$M_{\alpha\beta} := \begin{pmatrix} <\alpha, \beta^V><\beta, \alpha^V> - 1 & <\beta, \alpha^V> \\ - <\alpha, \beta^V> & -1 \end{pmatrix}$$

Nun hat $s_\alpha s_\beta$ als Element der Weylgruppe endliche Ordnung, d.h. die Eigenwerte von $M_{\alpha\beta}$ sind Einheitswurzeln (welche komplex konjugiert sind, da $M_{\alpha\beta}$ eine reelle Matrix ist)[170]. Deshalb ist der Absolutbetrag der Spur von $M_{\alpha\beta}$ höchstens 2,

$$|<\alpha, \beta^V><\beta, \alpha^V> - 2| \leq 2 .$$

Die Wurzeln α und β sind durch die zugehörigen Spiegelungen bis auf das Vorzeichen eindeutig bestimmt.[171] Deshalb gilt $s_\alpha \neq s_\beta$, d.h. $s_\alpha s_\beta$ ist nicht die identische Abbildung. Die Eigenwerte von $M_{\alpha\beta}$ können nicht beide gleich 1 sein. Deshalb gilt sogar

$$-2 \leq <\alpha, \beta^V><\beta, \alpha^V> - 2 < 2,$$

d.h.

$$0 \leq <\alpha, \beta^V><\beta, \alpha^V> \leq 3.$$

Damit gilt (i) mit eventueller Ausnahme der zweiten Aussage. Zum Beweis letzterer genügt es zu zeigen, daß (ii) gilt.

Zu (ii). Es gilt

---

[170] $M_{\alpha\beta}$ beschreibt eine zusammensetzung von zwei Spiegelungen, d.h. eine ebene Drehung, hat also keine reellen Eigenwerte.

[171] Durch s_α sind die Werte der Skalarprodukte $<\alpha, x^V>$ festgelegt, d.h. α steht fest.

$$<\alpha, \beta^V> = 0 \Leftrightarrow M_{\alpha\beta} \text{ ist obere Dreiecksmatrix}$$

$$< \beta, \alpha^V> = 0 \Leftrightarrow M_{\alpha\beta} \text{ ist untere Dreiecksmatrix}$$

Die Behauptung folgt deshalb aus der Tatsache, daß $M_{\alpha\beta}$ endliche Ordnung hat: eine Dreiecksmatrix über $\mathbb{Q}$ (mit Einheitswurzeln auf der Hauptdiagonalen hat genau dann endliche Ordnung, wenn es sich um eine Diagonalmatrix handelt)[172].

QED.

9.2.3 Systeme positiver Wurzeln

Eine Teilmenge $R^+ \subseteq R$ heißt System von positiven Wurzeln in R, wenn sie die folgenden Eigenschaften besitzt.

(a) Keine positive Linearkombination

$$\sum_i n_i\alpha_i \text{ mit } n_i > 0 \text{ und } \alpha_i \in R^+,$$

von Elementen aus R^+ ist gleich Null.

(b) $R = (R^+)\cup(-R^+)$.

Bemerkungen

(i) Solche Systeme existieren: man wähle ein $x\in X_{\mathbb{R}}$ mit

$$(x, \alpha) \neq 0 \text{ für jedes } \alpha\in R$$

und setze

$$R^+ := \{\alpha\in R \mid (x, \alpha)> 0\}.$$

(ii) Wir werden später sehen (≈ 10.1.6) daß man in der in (i) beschriebenen Weise jedes System positiver Wurzeln finden kann.

(iii) Wir nehmen in folgenden an, daß wir ein System positiver Wurzeln fixiert haben und schreiben

$$\alpha > 0 \Leftrightarrow \alpha\in R^+$$

$$\alpha < 0 \Leftrightarrow -\alpha\in R^+$$

(iv) Ist eine Wurzel α positive Linearkombination positiver Wurzeln,

$$\alpha = \sum_i n_i\alpha_i \text{ mit } n_i > 0,$$

so ist sie selbst auch positiv.[173]

---

[172] $M^2_{\alpha\beta}$ hat die Gestalt $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ bzw. $\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}$. Eine solche Matrix (über $\mathbb{Q}$) hat genau dann endliche Ordnung, wenn $x = 0$ (bzw. $y = 0$) ist.

[173] Anderfalls wäre $-\alpha$ positiv und $(-\alpha) + \sum_i n_i\alpha_i$ gleich Null.

9.2.4 Lemma: Überführung von Wurzel-Paaren in positive Wurzeln durch die Weylgruppe

Seien $\alpha, \beta \in R$ linear unabhängige Wurzeln. Dann gibt es ein Element der Weylgruppe $w \in W$ mit

$$w\alpha > 0 \text{ und } w\beta > 0.$$

Beweis.

Wir setzen

$$a := \langle \alpha, \beta^V \rangle \langle \beta, \alpha^V \rangle.$$

Nach Lemma 9.2.2 gilt dann

$$a \in \{0, 1, 2, 3\}.$$

1. Fall $a = 0$.

Nach 9.2.2 ist dann

$$\langle \alpha, \beta^V \rangle = \langle \beta, \alpha^V \rangle = 0,$$

also

$$s_\alpha(\alpha) = -\alpha \ , \ s_\alpha(\beta) = \beta$$

$$s_\beta(\alpha) = \alpha \ , \ s_\beta(\beta) = -\beta$$

d.h. s_α ändert das Vorzeichen von α und läßt das von β unverändert und be s_β ist es umgekehrt. Dann gilt aber die Behauptung.

2. Fall $a \neq 0$.

Sind beide Wurzeln positiv, so können wir $w = e$ wählen. Sei also o.B.d.A.

$$\alpha < 0.$$

Dann gilt

$$s_\alpha(\alpha) = -\alpha > 0$$

und

$$s_\alpha(\beta) = \beta - \langle \alpha, \beta^V \rangle \alpha.$$

Ist $s_\alpha(\beta) > 0$, so gibt es nichts weiter zu beweisen. Wir können also annehmen, $s_\alpha(\beta) < 0$.

Wir ersetzen α und β durch $s_\alpha(\beta)$ und $-\alpha$, und können annehmen, es gilt

(1) $\alpha < 0, \quad \beta > 0, \quad s_\alpha(\beta) < 0.$[174]

Nach 9.2.3 Bemerkung (iv) muß dann

$$<\alpha, \beta^V> < 0$$

sein.[175]

Es gilt

$$s_\alpha s_\beta(\alpha) = s_\alpha(\alpha - <\alpha, \beta^V>\beta)$$
$$= \alpha - <\alpha, \beta^V>\beta - < \alpha - <\alpha, \beta^V>\beta, \alpha^V>\alpha$$
$$= (a -1)\alpha - < \alpha, \beta^V>\beta$$
$$s_\alpha s_\beta(\beta) = s_\alpha(-\beta)$$
$$= -\beta + <\beta, \alpha^V>\alpha$$

Der zweite Ausdruck ist positiv (nämlich gleich - $s_\alpha(\beta)$.

Fall 2.1: a = 1.
In diesem Fall ist auch der ersten Ausdruck positiv:

$$s_\alpha s_\beta(\alpha) = - < \alpha, \beta^V>\beta$$

(als positives Vielfaches einer positiven Wurzel), d.h. wir können

$$w = s_\alpha s_\beta$$

setzen.
Fall 2.2: a ≠ 1 (d.h. a = 2 oder a = 3).
Wir betrachten die Matrix

$$M_{\alpha\beta} := \begin{pmatrix} <\alpha, \beta^V>< \beta, \alpha^V> - 1 & <\beta, \alpha^V> \\ - <\alpha, \beta^V> & -1 \end{pmatrix}$$

der Einschränkung von

Dann gilt $s_\alpha s_\beta$ auf den von α und β erzeugten reellen Vektorraum (vgl. den Beweis von 9.2.2). Für diese Matrix gibt es in unserer Situation nur die folgenden Möglichkeiten.

$$\begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix} \quad (a=2=(-2)(-1)=(-1)(-2))$$

---

[174] Wenn die dritte Bedingung nicht erfüllt ist, sind wir, wie wir gerade gesehen haben, fertig mit dem Beweis.

[175] Andernfalls wäre $s_\alpha(\beta) = \beta + <\alpha, \beta^V>(-\alpha)$ positive Linearkombination positiver Wurzeln, also positiv.

$\begin{pmatrix} 2 & -3 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 2 & -1 \\ 3 & -1 \end{pmatrix}$ (a=3=(-1)(-3)=(-3)(-1))

Es gilt

$\begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ = -Id und analog für $\begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}$

und

$\begin{pmatrix} 2 & -3 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 2 & -3 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 2 & -3 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -3 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 2 & -3 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ = -Id und analog für $\begin{pmatrix} 2 & -1 \\ 3 & -1 \end{pmatrix}$

Zusammen erhalten wir

$$(s_\alpha s_\beta)^a = -1.$$

Anwenden von $(s_\alpha s_\beta)^a$ überführt die Wurzeln α und β in deren Negatives. Wir können bei Bedarf α und β ersetzen durch $-\beta$ und $-\alpha$. Die Bedingungen von (1) bleiben dabei erhalten. Insbesondere können wir annehmen

$$<\alpha, \beta^v> = -1 \text{ und } <\beta, \alpha^v> = -a.$$

Fall 2.2.1: a = 2.

Es gilt

$s_\alpha(\alpha) = -\alpha$, $s_\beta(\alpha) = \alpha+\beta$, $s_\alpha s_\beta(\alpha) = \alpha+\beta$

$s_\alpha(\beta) = 2\alpha+\beta$, $s_\beta(\beta) = -\beta$, $s_\alpha s_\beta(\beta) = -2\alpha-\beta$

Im Fall $2\alpha+\beta > 0$ setzen wir $w = s_\alpha$.

Im Fall $\alpha+\beta < 0$ setzen wir $w = -s_\beta$.[176]

Im Fall $2\alpha+\beta < 0$ und $\alpha+\beta > 0$ setzen wir $w = s_\alpha s_\beta$.

Fall 2.2.2: a = 3.

Es gilt:

$s_\alpha\alpha = -\alpha$, $s_\beta\alpha = \alpha+\beta$, $s_\alpha s_\beta\alpha = 2\alpha+\beta$, $s_\beta s_\alpha(\alpha) = -\alpha-\beta$, $s_\alpha s_\beta s_\alpha\alpha = -2\alpha-\beta$

$s_\alpha\beta = 3\alpha+\beta$, $s_\beta\beta = -\beta$, $s_\alpha s_\beta\beta = -3\alpha-\beta$, $s_\beta s_\alpha(\beta) = 3\alpha+2\beta$, $s_\alpha s_\beta s_\alpha\beta = 3\alpha+2\beta$

Im Fall $3\alpha+\beta > 0$ setzen wir $w = s_\alpha$.

Im Fall $\alpha+\beta < 0$ setzen wir $w = -s_\beta$.

Im Fall $3\alpha+\beta < 0$ und $2\alpha+\beta > 0$ setzen wir $w = s_\alpha s_\beta$.

Im Fall $\alpha+\beta > 0$ und $3\alpha+2\beta < 0$ setzen wir $w = -s_\beta s_\alpha$.

Im Fall $2\alpha+\beta < 0$, $3\alpha+2\beta > 0$ setzen wir $w = s_\alpha s_\beta s_\alpha$.

---

[176] Übergang zum Negativen ist, wie wir gesehen haben eine Operation eines Elements der Weyl-Gruppe.

QED.

9.2.5 Aufgaben

Seien $\alpha, \beta \in R$ linear unabhängige Wurzeln und sei wie oben

$$a := <\alpha, \beta^V><\beta, \alpha^V>.$$

Wir nehmen an, es gilt

$$a > 0$$

$$<\alpha, \beta^V> = -1, \text{ d.h. } <\beta, \alpha^V> = -a.$$

Dann ist die nachfolgend definierte Teilmenge S von R stabil bei s_α und s_β .

Falls a = 0 ist: $S := \{ \pm\alpha, \pm\beta\}$

Falls a = 1 ist: $S := \{ \pm\alpha, \pm\beta, \pm(\alpha+\beta)\}$

Falls a = 2 ist: $S := \{ \pm\alpha, \pm\beta, \pm(\alpha+\beta), \pm(2\alpha+\beta)\}$

Falls a = 3 ist: $S := \{ \pm\alpha, \pm\beta, \pm(\alpha+\beta), \pm(2\alpha+\beta), \pm(3\alpha+\beta), \pm(3\alpha+2\beta)\}$

9.3 Borel-Gruppen, Systeme positiver Wurzeln, das unipotente Radikal

Bisher sind Wurzeln in Paaren $(\alpha, -\alpha)$ aufgetreten. Wir benutzen jetzt die Borel-Untergruppen, um in einem gegebenen Paar, die eine Wurzel als ‘positiv’ auszuzeichnen.

9.3.1 Begriff der positiven Wurzel

Seien G eine zusammenhängende lineare algebraische Gruppe,

$$T \subseteq G$$

ein maximaler Torus und

$$S \subseteq T$$

ein singulärer Teiltorus (der insbesondere die Kodimension 1 besitzt). Dann gibt es für jede Borel-Untergruppe B, die den Torus T enthält, eine Wurzel

$$\alpha \in R(G,T)$$

mit

$$L(B \cap Z_G S/R_u Z_G S) = L(T) \oplus kX_\alpha,$$

wobei X_α einen Gewichtsvektor zur Wurzel α bezeichne. Eine Wurzel mit dieser Eigenschaft heißt <u>positiv</u> bezüglich B. Bezeichne

$$R^+(B)$$

die Menge der bezüglich B positiven Wurzeln (d.h. die Menge der verschiedenen α zu den unterschiedlichen singulären Teiltori S von T.

Beweis der Existenz positiver Wurzeln.

Nach 7.3.5(ii) ist

$$B \cap Z_G(S)$$

eine Borel-Untergruppe von $Z := Z_G(S)$. Nach 9.1.5 gibt es ein Gewicht α von T auf [177] Lie(G) mit

(1) $S = (\mathrm{Ker}\ \alpha)^0$.

(2) $L(Z/\mathbf{R}_u Z) \cong L(T) \oplus kX_\alpha \oplus kX_{-\alpha}$.

Dabei sind X_α und $X_{-\alpha}$ Gewichtsvektoren zu den Gewichten α bzw. $-\alpha$, und $Z/\mathbf{R}_u Z$ ist reduktiv vom halbeinfachen Rang 1. Insbesondere ist α eine Wurzel von G,

$$\alpha \in R(G,T).$$

und nach 8.2.9 (iii) und (iv) gibt es einen Homomorphismus algebraischer Gruppen

$$x_\alpha : G_a \to Z/\mathbf{R}_u Z$$

derart, daß T und $\mathrm{Im}(x_\alpha)$ eine Borel-Untergruppe B' von $Z/\mathbf{R}_u Z$ erzeugen mit der Lie-Algebra

$$L(B') = L(T) \oplus L(Z/\mathbf{R}_u Z)_\alpha = L(T) \oplus kX_\alpha.$$

Das natürliche Bild von $Z \cap B$ in $Z/\mathbf{R}_u Z$ ist eine Borel-Untergruppe. Wir können annehmen, das Vorzeichen von α wurde so gewählt daß

$$B' = Z \cap B \bmod \mathbf{R}_u Z$$

gilt.[178] Dann ist α im oben beschriebenen Sinne eine bezüglich B positive Wurzel.

QED.

9.3.2 Proposition: $R^+(B)$ als System positiver Wurzeln

Seien G eine zusammenhängende lineaere algebraische Gruppe, $T \subseteq G$ ein maximaler Torus und $B \subseteq G$ eine Borel-Untergruppe, die den Torus T enthält. Dann ist

$$R^+(B)$$

ein System positiver Wurzeln im Sinne von 9.2.3.

Beweis. Sei α eine Wurzel. Wir setzen

$$G_\alpha := Z_G(\mathrm{Ker}(\alpha)^0).$$

---

[177] Bezüglich der adjungierten Darstellung von G auf Lie(G).

[178] Die Weyl-Gruppe von $Z/\mathbf{R}_u Z$ besteht aus zwei Elementen. Es gibt also nur zwei Borel-Untergruppen von $Z/\mathbf{R}_u Z$, die das Bild des Torus T enthalten. Eine gehört zum Character α, die andere zum Charakter $-\alpha$. Das nicht-triviale Element der Weyl-Gruppe vertauscht die beiden Borel-Untergruppen.

Dann ist $B \cap G_\alpha$ eine Borel-Untergruppe von G_α[179] , welche den Torus T enthält, d.h. $L(B \cap G_\alpha)$ wird von L(T) und einem von zwei Gewichtsvektoren X_α bzw. $X_{-\alpha}$ erzeugt. Mit anderen Wort α oder $-\alpha$ liegt in $R^+(B)$. Wir haben gezeigt, für die Menge der Wurzeln R gilt

$$(1) \qquad R = R^+(B) \cup - R^+(B),$$

Axiom (b) von 9.2.3 ist somit erfüllt.
Zum Nachweis der Gültigkeit von Axiom (a) wählen wir auf dem reellen Vektorraum

$$X_{\mathbb{R}}$$

eine positiv definite W(G,T)-invariante Bilinearform

$$(,): X_{\mathbb{R}} \times X_{\mathbb{R}} \to \mathbb{R}$$

(vgl. 9.1.10) und konstruieren einen Charakter x derart ,daß die Elemente von $R^+(B)$ sämtlich auf derselben Seite der Hyperebene $x^\perp$ liegen. Daraus ergibt sich dann die Gültigkeit von Axiom (b) (nach Bemerkung (i) von 9.2.3).

Man beachte, wegen (1) liegen dann die übrigen Wurzeln auf der anderen Seite.

Zur Konstruktion von x wählen wir eine rationale Darstellung

$$\rho: G \to GL(V)$$

und einen Vektor $v \in V-\{0\}$ mit

$$B = \{g \in G \mid \rho(g)v \in kv \}$$

(vgl. 5.1.3). Dann gibt es einen Charakter

$$\chi \in X(B)$$

mit

$$\rho(b)v = \chi(b)v \text{ für jedes } b \in B .$$

Wir fixieren eine Basis

$$e_1,..,e_n \in V \text{ mit } e_1 = v$$

und schreiben

---

[179] $S = \mathrm{Ker}(\alpha)^0$ ist der zu α gehörige singuläre Torus, $G_\alpha/R_u G_\alpha$ die zugehörige reduktive Gruppe vom Rang 1 (vgl. 9.1.5 und 9.1.8). $B \cap G_\alpha$ ist Borel-Untergruppe von G_α nach 7.3.5(ii).Insbesondere besteht die Weyl-Gruppe von $G_\alpha/R_u G_\alpha$ aus genau zwei Elementen (vgl. 8.2.2) und besitzt damit genau zwei Borel-Untergruppen, die das natürliche Bild des Torus T enthalten (nach 8.1.7(ii)).

$$\rho(g)e_i = \sum_{j=1}^{n} a_{ij}(g)e_j$$

Weiter sei

$$F(g) := a_{11}(g).$$

Dann gilt

$$F \in k[G],\ F(e) = 1$$

Weiter ist

$$\begin{aligned} a_{11}(gb)e_1 + \ldots + a_{1n}(gb)e_n &= \rho(gb)e_1 \\ &= \rho(g)\rho(b)e_1 \\ &= \rho(g)\chi(b)e_1 \\ &= a_{11}(g)\ \chi(b)e_1 + \ldots + a_{1n}(g)\ \chi(b)e_n \end{aligned}$$

Durch Vergleich der Koeffizienten von $e_1 = v$ folgt

$$F(gb) = F(g)\chi(b) \text{ für } g \in G \text{ und } b \in B.$$

Wir können annehmen

$$B \neq G$$

denn andernfalls ist G auflösbar, d.h. die Weylgruppe ist trivial und die Menge der Wurzeln ist leer. Es gilt dann

$$\chi \neq 0$$

ist verschieden vom trivialen Charakter, denn andernfalls wäre

$$B = \{x \in G \mid \rho(x)v = v\}$$

d.h.

$$G/B \cong \text{Orbit von } v \text{ bei } \rho \subseteq V.$$

Die vollständige zusammenhängende Varietät G/B wäre Teilvarietät von V, was nicht möglich ist (außer im Fall G/B = { ein Punkt }). Damit ist also χ ein nicht-trivialer Charakter.

Es reicht zu zeigen,

$$(\chi, \alpha) > 0 \text{ für jedes } \alpha \in R.$$

Sei also $\alpha \in R$. Wie oben sei

$$G_\alpha := Z_G(\mathrm{Ker}(\alpha)^0).$$

Dann ist $B_\alpha := G_\alpha \cap B$ eine Borel-Untergruppe von G_α und dieselbe Argumentation wie oben zeigt,

(2) $$\chi|_{B_\alpha} \neq 0.$$[180]

Auf dem unipotenten Radikal von G_α ist der Charakter $\chi: B \to G_m$ trivial,

$$\chi(R_u G\cdot_\alpha) = 1.$$[181]

Also gilt

$$F(gb) = F(g)\chi(b) = F(g) \text{ für } g \in G_\alpha \text{ und } b \in R_u G\cdot_\alpha .$$

Also definiert F eine reguläre Funktion auf der Gruppe $G\cdot_\alpha / R_u G\cdot_\alpha$ und damit auch auf deren Kommutator-Untergruppe

$$H \subseteq G\cdot_\alpha / R_u G\cdot_\alpha ,$$

welche isomorph ist zu SL_2 oder PSL_2 (nach 8.2.5). Es gilt

$$L(G\cdot_\alpha / R_u G\cdot_\alpha) = L(T) \oplus kX_\alpha \oplus kX_{-\alpha}$$

und die Lie-Algebra der halbeinfachen Gruppe H enthält die beiden Gewichtsvektoren (vgl. 8.2.7):

$$X_\alpha, X_{-\alpha} \in L(H),$$

d.h. α ist eine Wurzel von H. Sei $\alpha^v \in X_*(H) \subseteq X_*(T)$ die zu α gehörige Kowurzel. Dann gilt nach Definition von F,

$$F(h\alpha^v(\xi)) = F(h)\chi(\alpha^v(\xi)) = \xi^{<\chi, \alpha^v>} F(h) \text{ für } h \in H \text{ und } \xi \in k^*.$$

Dasselbe Argument wie für (2) zeigt, χ ist nicht konstant auf $B \cap H$, d.h. ist F nicht konstant auf H. Nach 8.2.10 und Aufgabe 8.2.11(1) ist dann aber

$$<x, \alpha^v> > 0.$$

QED.

Bemerkung

Unser nächstes Ziel ist eine neue Beschreibung des unipotenten Radikals der zusammenhängenden linearen algebraischen Gruppe G. Dazu führen wir zunächst eine Bezeichnung ein.

---

[180] Die vollständige zusammenhängende Varietät $G\cdot_\alpha / B\cdot_\alpha$ (positiver Dimension) kann nicht Teilvarietät des affinen Raums V sein.

[181] $R_u G\cdot_\alpha$ ist ein zusammenhängender unipotenter (also auflösbarer) Normalteiler von $G\cdot_\alpha$, liegt also in jeder Borel-Untergruppe von $G\cdot_\alpha$, also insbesondere in $G\cdot_\alpha \cap B$. Also gilt $R_u G\cdot_\alpha \subseteq B$. Die obige Aussage ist also sinnvoll. Sie ist wahr, weil $R_u G\cdot_\alpha$ aus unipotenten und G_m aus halbeinfachen Elementen besteht.

9.3.3 Bezeichnung: H_α für $\alpha \in R(G,T)$

Bezeichne

$$V := (\cap_{B \in \mathbf{B}_T} B_u)^0$$

die Einskomponente des Durchschnitts aller Borel-Untergruppen, die den maximalen Torus T von G enthalten. Für jede Wurzel $\alpha \in R(G,T)$ setzen wir

$$H_\alpha := (\cap_{B \in \mathbf{B}_T,\ \alpha \in R^+(B)} B_u)^0$$

Bemerkungen

(i) Nach Konstruktion ist H_α zusammenhängend und besteht aus unipotenten Elementen.

(ii) Insbesondere ist H_α also nilpotent.

9.3.4 Lemma: V ist Normalteiler in H_α

Sei $\alpha \in R(G,T)$ eine Wurzel. Dann gilt $V \subseteq H_\alpha$ und V ist ein abgeschlossener Normalteiler in H_α.

Beweis. Die Inklusion

$$V \subseteq H_\alpha$$

ist trivial.

Nach Definition[182] von $\mathbf{B}_T$ bildet die Konjugation mit Elementen aus T jede Borel-Untergruppe von $\mathbf{B}_T$ in sich ab. Insbesondere wird dabei auch H_α in sich abgebildet. Mit anderen Worten, T operiert auf V und H_α durch Konjugation. Bezüglich dieser Operation zerfallen L(V) und $L(H_\alpha)$ in direkte Summen von Gewichts-Unterräumen. Es gilt

$$L(H_\alpha) = L(V) \oplus kX_{\beta_1} \oplus kX_{\beta_2} \oplus \ldots \oplus kX_{\beta_s}$$

mit gewissen Gewichtsvektoren $\beta_1, \ldots, \beta_s : T \to G_m$.

Behauptung:

Die Gewichtsvektoren β_i sind sogar Wurzeln von G mit der folgenden Eigenschaft:

---

[182] $\mathbf{B}_T$ die Fixpunktmenge der Operation von T auf den Borel-Unterguppen (durch Konjugation).

(1) $\beta \in R^+(B)$ für jedes $B \in \mathbf{B}_T$ mit $\alpha \in R^+(B)$.

Zeigen wir zunächst, die Aussage des Satzes folgt aus dieser Behauptung. Dazu fixieren wir eine Borel-Untergruppe B_0 von $\mathbf{B}_T$. Für jedes $w \in W$ mit

$$w\alpha \in R^+(B_0)$$

gilt dann $\alpha \in R^+(w^{-1}B_0)$.[183] Nach (1) gilt also $\beta \in R^+(w^{-1}B_0)$, und damit

$$w\beta \in R^+(B_0).$$

Wir haben gezeigt, es gibt ein System positiver Wurzeln (nämlich das System $R^+(B_0)$) mit

(2) $w\beta > 0$ für jedes $w \in W$ mit $w\alpha > 0$.

Wären die Wurzeln α und $-\beta$ linear unabhängig, dann gäbe es nach 9.2.4 ein $w \in W$ mit $w\alpha > 0$ und $w(-\beta) > 0$ im Widerspruch zu (2). Die Wurzeln α und β sind also proportional. Da das Wurzel-Datum von G nach 9.1.12 reduziert ist, folgt

$$\beta = \pm\alpha .$$

Wegen (2) ist damit sogar $\beta = \alpha$. Die Anzahl der β in der obigen Zerlegung der Lie-Algebra $L(H_\alpha)$ ist also $s = 1$. Insbesondere gilt

$$\dim H_\alpha/V \leq 1.$$

Nach Aufgabe 6.6 (3)[184] ist dann aber V ein Normalteiler in H_α.

---

[183] α ist eine Abbildung $\alpha: T \to G_m$ und $w\alpha$ ist die Zusammensetzung

$$\begin{array}{ccccc} w\alpha: & T & \xrightarrow{w^{-1}} & T & \xrightarrow{\alpha} G_m \\ & \cap & & \cap & \\ & B_0 & \xrightarrow{w^{-1}} & w^{-1}B_0 & \end{array}$$

Identifiziert man mit Hilfe des Isomorphismus w^{-1} die Borel-Untergruppe B_0 mit der der Borel-Untergruppe $w^{-1}B_0$ so wird bei dieser Identifikation das Gewicht $w\alpha$ von B_0 identifiziert mit dem Gewicht α von $w^{-1}B_0$.

[184] (3) Let G be a connected nilpotent linear algebraic group and $H \subseteq G$ a proper connected closed subgroup. Show that

Wir haben noch die obige Behauptung zu beweisen, d.h. wir haben zu zeigen, $L(H_\alpha)$ wird modulo L(V) von Wurzeln erzeugt, die positiv sind bezüglich jeder Borel-Untergruppe B mit $\alpha \in R^+(B)$.

Sei B eine Borel-Untergruppe mit $\alpha \in R^+(B)$. Dann gilt $H_\alpha \subseteq B$, also

$$L(H_\alpha) \subseteq L(B).$$

Es reicht also zu zeigen, für jede Borel-Untergruppe B von G, wird

$$L(B)$$

modulo L(V) von B-positiven Wurzeln erzeugt. Wegen $T \subseteq B$ operiert T durch Konjugation auf B, d.h. es gilt

(3) $$L(B) = L(B)_{\chi_1} \oplus \ldots \oplus L(B)_{\chi_r} \oplus L(B)_0$$

mit gewissen von 0 verschiedenen Gewichten

$$\chi_i : T \to G_m$$

Betrachten wir die zugehörigen Teiltori der Kodimension 1,

$$S_i := \mathrm{Ker}(\chi_i)^0.$$

Nach 4.4.7 gilt

$$L(Z_G(S_i)) = \{X \in L(G) \mid sX = X \text{ für alle } s \in S_i\}$$
$$\supseteq L(G)_{\chi_i}$$

(da S_i im Kern von χ_i liegt, operieren die $s \in S_i$ trivial auf $L(G)_{\chi_i}$). Wir sehen also,

(4) χ_i ist Gewicht von T auf $L(Z_G(S_i))$ (i=1,...,r).[185]

Für jede Borel-Untergruppe $B' \in \mathbf{B}_T$ ist $B' \cap Z_G(S_i)$ eine Borel-Untergruppe von $Z_G(S_i)$, d.h. es gilt

$$R_u Z_G(S_i) \subseteq B' \cap Z_G(S_i) \subseteq B',$$

Da dies für alle $B' \in \mathbf{B}_T$ gilt, folgt

$$\dim H < \dim N_G H,$$

where $N_G H$ denotes the normaliser. In particular, if dim H = dim G - 1, then H is a normal subgroup (Hint: use 6.5 (ii)).

[185] d.h. χ_i hat dort einen nicht-trivialen Eigenraum.

$$R_u\, Z_G(S_i) \subseteq (\cap_{B' \in \mathbf{B}_T} B'_u)^0 = V.$$

Die Gewichtsvektoren der Zerlegung (3), welche nicht in L(V) liegen, gehören somit sogar zu den Gewichten von[186]

$$L(Z_G(S_i)/ R_u\, Z_G(S_i)) = L(T) \oplus kX_{\chi_i} \oplus kX_{-\chi_i}$$

d.h. die zugehörigen Gewichte sind Wurzeln von G. Man beachte, dies ist die Lie-Algebra einer Gruppe mit genau zwei Borel-Untergruppen, die T enthalten, und die Gewichtsvektoren X_{χ_i} und $X_{-\chi_i}$ sind tangential zu jeweils genau einer dieser Borel-Untergruppen. Eine dieser Borel-Untergruppen ist

$$B \cap Z_G(S_i)/ R_u\, Z_G(S_i).$$

Wegen $L(H_\alpha) \subseteq L(B)$ gilt damit

(5) $$L(H_\alpha) = L(H_\alpha)_{\chi_{i_1}} \oplus \ldots \oplus L(H_\alpha)_{\chi_{i_s}} \oplus L(V)$$

mit

$$L(H_\alpha)_{\chi_{i_\nu}} \subseteq L(B \cap Z_G(S_{i_\nu})/ R_u\, Z_G(S_{i_\nu}))$$

mit anderen Worten, die Gewichte χ_{i_ν} in der Zerlegung von (5) sind B-positive Wurzeln.

QED.

9.3.5 Theorem: Beschreibung des unipotenten Radikals

Seien G eine zusammenhängende lineare algebraische Gruppe mit dem maximalen Torus T. Dann ist die 1-Komponente

---

[186] Die Gewichtsvektoren zu χ_i , welche nicht in L(V) liegen, also auch nicht in $L(R_{uG}(S_i))$, d.h. sie sind nicht tangential zu $R_u Z_G(S_i)$. werden beim Differential der natürlichen Abbildung

$$Z_G(S_i) \to Z_G(S_i)/R_u Z_G(S_i)$$

nicht in die Null abgebildet.

Man beachte, falls es einen solchen Gewichtsvektor gibt, so ist $Z_G(S_i)$ nicht auflösbar, d.h. S_i ein singulärer Torus: wäre nämlich $Z_G(S_i)$ auflösbar, so wäre sogar $Z_G(S_i) \subseteq V$ (nach dem obigen Argument), d.h. es wäre

$$L(G)_{\chi_i} \subseteq L(Z_G(S_i)) \subseteq L(G),$$

d.h. die Gewichtsvektoren zu χ_i liegen dorch sämtlich in L(G).

$$V = (\cap_{B \in \mathbf{B}_T} B_u)^0$$

des Durchschnitts der unipotenten Radikale der Borel-Untergruppen B, welche T enthalten, gleich dem unipotenten Radikal von G,

$$V = R_u G .$$

Beweis. Für jede Borel-Untergruppe $B \in \mathbf{B}_T$ gilt

$$R_u G \subseteq B$$

also ist

$$R_u G \subseteq \cap_{B \in \mathbf{B}_T} B_u$$

also

$$R_u G \subseteq V.$$

Zum Beweis der umgekehrten Inklusion reicht es zu zeigen, V ist ein Normalteiler von G.[187] Da G von den Borel-Untergruppen $B \in \mathbf{B}_T$ erzeugt wird (nach 8.1.8(iv)), reicht es zu zeigen, jede Borel-Untergruppe $B \supseteq T$ normalisiert V. Nun wird die Borel-Untergruppe B erzeugt von den Zentralisatoren

(1) $$Z_B(S) = B \cap Z_G(S),$$

wobei S die Teiltori der Kodimension 1 von T durchläuft (nach 9.1.3). Es reicht also zu zeigen, jede der Untergruppen (1) normalisiert V.

1. Fall: S ist ein regulärer Torus.

Dann ist $Z_G(S)$ auflösbar. Nach 7.3.5 ist für jede Borel-Untergruppe B', welche S enthält, $B' \cap Z_G(S)$ eine Borel-Untergruppe von $Z_G(S)$. Es folgt

$$Z_G(S) = B' \cap Z_G(S) \subseteq B'$$

d.h.

$$Z_G(S)_u \subseteq \cap_{B' \in \mathbf{B}_T} B'_u .$$

Da $Z_G(S)$ nach 7.3.5(i) zusammenhängend ist, folgt

$$Z_G(S)_u \subseteq V.$$

Nun ist $Z_G(S)$ auflösbar, also nach 6.11

$$Z_G(S) = T \cdot Z_G(S)_u \subseteq T \cdot V.$$

---

[187] Denn $R_u G$ ist der "größte" unipotente zusammenhängende Normalteiler von G.

Nun wird V von sich selbst und von T normalisiert, also auch vom Zentralisator $Z_G(S)$.

2. Fall: S ist ein singulärer Torus.
Dann gibt es eine Wurzel $\alpha \in R(G,T)$ mit

$$S = (\mathrm{Ker}\ \alpha)^0$$

und mit den Bezeichnungen von 9.1.8 ist

$$Z_G(S) = G_\alpha .$$

Außerdem ist

$$B_\alpha := B \cap G_\alpha$$

eine Borel-Untergruppe von G_α und für jede Borel-Untergruppe B' von G mit $\alpha \in R^+(B')$ gilt[188]

$$B_\alpha \subseteq B'.$$

Dann gilt aber

$$(B_\alpha)_u \subseteq \cap_{B' \in \mathbf{B}_T, \alpha \in R^+(B')} {B'}_u ,$$

also

$$(B_\alpha)_u \subseteq H_\alpha$$

also

$$B_\alpha = T \cdot (B_\alpha)_u \subseteq T \cdot H_\alpha .$$

Weil nun V von T und von H_α normalisiert wird (vgl. 9.3.4), gilt dasselbe von $B_\alpha = B \cap G_\alpha = B \cap Z_G(S)$.

---

[188] Die Weyl-Gruppe von G_α hat nach 9.1.8 die Ordnung 2, d.h. G_α besitzt genau zwei Borel-Untergruppen (nach 8.1.7(ii). Nach 9.3.1 ist α positiv bezüglich einer Borel-Untergruppe B',

$$\alpha \in R^+(B'),$$

wenn gilt

$$L(B' \cap G_\alpha / R_u G_\alpha) = L(T) \oplus kX_\alpha$$

mit einem Gewichtsvektor X_α zur Wurzel α. Da G_α nur zwei Borel-Untergruppen besitzt, wobei die Lie-Algebra der einen gleich $L(T) \oplus kX_\alpha$ und die der anderen gleich $L(T) \oplus kX_{-\alpha}$ ist, ist durch diese Bedingung der Durchschnitt $B' \cap G_\alpha$ eindeutig bestimmt, d.h. wenn α sowohl B-positiv als auch B'-positiv ist, muß gelten

$$B_\alpha = B \cap G_\alpha = B' \cap G_\alpha ,$$

d.h. es besteht die behauptete Inklusion.

Wir haben gezeigt, für jede Borel-Untergruppe B von G mit $T \subseteq B$ normalisiert der Durchschnitt $B \cap Z_G(S)$ die Untergruppe V, d.h. die Borel-Untergruppen von $Z_G(S)$ normalisieren V (vgl. 7.3.5(ii)). Nun wird die Gruppe $Z_G(S)$ von ihren Borel-Untergruppen erzeugt (vgl. 7.3.3 (i)), d.h. $Z_G(S)$ normalisiert V.

QED.

9.3.6 Folgerung: der Zentralisator eines Torus im reduktiven Fall

Seien G eine zusammenhängende reduktive lineare Gruppe und T ein maximaler Torus von G. Dann gilt:

(i) Für jeden Teiltorus S von T ist $Z_G(S)$ zusammenhängend und reduktiv.

(ii) $Z_G(T) = T$, d.h. die Cartan-Untergruppen von G sind gerade die maximalen Tori von G.

(iii) Das Zentrum von G liegt ganz in T, $Z(G) \subseteq T$.

Beweis. Zu (i).Das unipotente Radikal von $Z_G(S)$ liegt in jeder Borel-Untergruppe, und damit sogar in deren unipotenten Anteil. Nachnach 7.3.5(ii) gilt damit

$$R_u Z_G(S) \subseteq \cap_{B \in \mathbf{B}_T} (Z_G(S) \cap B)_u \subseteq \cap_{B \in \mathbf{B}_T} B_u$$

also nach 9.3.5

$$R_u Z_G(S) \subseteq (\cap_{B \in \mathbf{B}_T} B_u)^0 = R_u G = \{e\},$$

d.h. $Z_G(S)$ ist reduktiv. Nach 7.3.5(i) ist $Z_G(S)$ zusammenhängend.

Zu (ii). Nach 7.2.10 ist die Cartan-Untergruppe

$$C := Z_G(T)^0 \ (= Z_G(T) \text{ nach (i)})$$

nilpotent, also auflösbar. Nach 6.11 zerfällt sie in ein halbdirektes Produkt aus dem maximalen Torus T und dem unipotenten Teil C_u. Nun ist C_u ein maximaler zusammenhängender unipotenter Normalteiler von C, also gleich dem unipotenten Radikal von C. Da C nach (i) reduktiv ist, folgt $C_u = \{e\}$. Also ist

$$T = C = Z_G(T).$$

Zu (iii). Sei $g \in Z(G)$ im Zentrum von G. Dann kommutiert g auch mit jedem Element von T. Nach (ii) gilt damit

$$g \in Z_G(T) = T.$$

QED.

Vereinbarung

Von jetzt an sei G eine zusammenhängende reduktive lineare algebraische Gruppe mit dem maximalen Torus T und dem Wurzelsystem R = R(G,T).

9.3.7 Proposition: die Untergruppen X_α

Sei G eine zusammenhängende reduktive lineare algebraische Gruppe mit dem maximalen Torus T und dem Wurzelsystem

$$R = R(G,T).$$

Dann gilt

(i) Für jede Wurzel $\alpha \in R$ gibt es einen Isomorphismus[189]

$$x_\alpha : G_a \to X_\alpha$$

von G_α mit einer eindeutig bestimmten Untergruppe X_α von G mit

$$t x_\alpha(\xi) t^{-1} = x_\alpha(\alpha(t)\xi) \text{ für } t \in T \text{ und } \xi \in k.$$

Es gilt

$$L(X_\alpha) = \mathrm{Im}(dx_\alpha) = L(G)_\alpha.$$

(ii) T und die X_α erzeugen zusammen die Gruppe G.

(iii) L(T) und die $L(X_\alpha)$ erzeugen (als Vektorräume) zusammen die Lie-Algebra L(G)

Beweis. Zu (i). Für reduktive Gruppen vom halbeinfachen Rang 1 haben wir diese Aussage bereits bewiesen (vgl. 8.2.9(iii)).

Betrachten wir die Untergruppe (vgl. 9.1.8)

$$G_\alpha = Z_G((\mathrm{Ker}\ \alpha)^0)$$

Nach 9.3.6(i) ist G_α reduktiv und nach 9.1.5 hat G_α den halbeinfachen Rang 1. Die Existenzaussage von (i) folgt damit aus 8.2.9(iii). Ist x_α ein Isomorphismus mit der angegebenen Eigenschaft, so gilt

$$t x_\alpha(\xi) t^{-1} = x_\alpha(\xi) \text{ für } t \in \mathrm{Ker}(\alpha)^0,$$

d.h. $x_\alpha(\xi) \in Z_G(\mathrm{Ker}(\alpha)^0) = G_\alpha$. Das Bild von x_α liegt also in G_α. Die Eindeutigkeitsaussage folgt damit ebenfalls aus 8.2.9.

Zu (ii) und (iii). Nach 9.1.3 wird G von den Zentralisatoren

---

[189] Der Beweis zeigt sogar (unter Verwendung der vollen Aussage von 8.2.9), daß x_α bis auf einen Isomorphismus von G_a (Multiplikation mit einem $c \in k^*$) eindeutig bestimmt ist.

$$Z_G(S)$$

erzeugt, wenn S die Teiltori von G der Kodimension 1 durchläuft. Ist S ein regulärer Torus, d.h. ist $Z_G(S)$ auflösbar, so gilt nach 6.11

$$Z_G(S) = T \cdot R_u Z_G(S).$$

Nach 9.3.6(i) ist $Z_G(S)$ reduktiv, d.h. das unipotente Radikal ist trivial,

$$Z_G(S) = T.$$

Damit wir G erzeugt von T und den Zentralisatoren

$$Z_G(S) \text{ mit } S \text{ singulär},$$

d.h. G wird erzeugt von T und den Gruppen G_α mit $\alpha \in R$. Da die G_α reduktiv von halbeinfachen Rang 1 sind, d.h.

$$L(G_\alpha) = L(T) \oplus kX_\alpha \oplus kX_{-\alpha}$$

mit Gewichtsvektoren X_α und $X_{-\alpha}$ zu α bzw. $-\alpha$ (vgl. 8.2.7(vii)), wird damit L(G) von L(T) und den Gewichtsvektoren X_α, $X_{-\alpha}$ mit $\alpha \in R$ erzeugt.[190] Erst recht wird damit L(G) erzeugt von L(T) und den Gewichtsräumen

$$L(G)_\alpha \text{ mit } \alpha \in R.$$

Sei G_1 die von T und den X_α erzeugte Untergruppe. Dann gilt

$$L(T) \subseteq L(G_1) \text{ und } L(G)_\alpha \subseteq L(G_1)$$

(denn nach (i) gilt $L(X_\alpha) = L(G)_\alpha$). Damit ist aber

---

[190] Wird G von endlich vielen zusammenhängenden Untergruppen $G_1, \ldots, G_r$ erzeugt, so können wir nach 6.1 annehmen, es die Gruppen-Multiplikation induziert eine Surjektion

$$(*) \qquad G_1 \times \ldots \times G_r \to G$$

(wenn wir in der Folge der G_i Wiederholungen zulassen). Dieser Morphismus ist separabel: zum Beweis können wir die zu (*) gehörige Körpererweiterung vergrößern und jede der Untergruppen G_i durch G ersetzen. Dann ist aber das Differential von (*) in e trivialerweise surjektiv, d.h. (*) ist nach Theorem 3.2.20 separabel.
Da (*) separabel ist, ist die induzierte Abbildung der Lie-Algebren

$$L(G_1) \oplus \ldots \oplus L(G_r) \to L(G),$$

surjektiv (vgl. Theorem 3.2.20), d.h. es gilt

$$L(G) = \sum_{i=1}^{r} L(G_i).$$

$$L(T)+ \sum_{\alpha\in R} L(G)_\alpha \subseteq L(G_1) \subseteq L(G) \subseteq L(T)+ \sum_{\alpha\in R} L(G)_\alpha.$$

Also gilt überall das Gleichheitszeichen,

$$L(G_1) = L(G) = L(T)+ \sum_{\alpha\in R} L(G)_\alpha,$$

und insbesondere ist

$$G_1 = G.$$

QED.

9.3.8 Folgerung: Die Gewichtsräume von T auf L(G) im reduktiven Fall

Sei G eine zusammenhängende reduktive lineare algebraische Gruppe mit dem maximalen Torus T und dem Wurzelsystem

$$R = R(G,T).$$

Dann gilt

(i) Die Wurzeln von G bezüglich T sind gerade die von Null verschiedenen Gewichte von T auf L(G),

$$L(G) = L(G)_0 \oplus (\oplus_{\alpha\in R} L(G)_\alpha)$$

mit $L(G)_0 = L(T)$.

(ii) Für jedes $\alpha\in R$ gilt $\dim L(G)_\alpha = 1$.

Beweis. Nach 9.3.7 wird G von T und den X_α erzeugt und es gilt

$$L(G) = L(T)+ \sum_{\alpha\in R} L(X_\alpha).$$

Wegen

$$L(T) \subseteq L(G)_0 \text{ und } L(X_\alpha) = L(G)_\alpha$$

(nach 9.3.7) folgt

$$L(G) = L(T)+ \sum_{\alpha\in R} L(X_\alpha) \subseteq L(G)_0 \oplus (\oplus_{\alpha\in R} L(G)_\alpha) \subseteq L(G).$$

Damit gilt überall das Gleichheitszeichen und die Summe links ist direkt,

$$L(G) = L(T)\oplus(\oplus_{\alpha\in R} L(X_\alpha)),\ L(X_\alpha) = L(G)_\alpha$$

Insbesondere gilt

$$\dim L(G)_\alpha = \dim L(X_\alpha) = \dim X_\alpha = 1.$$

QED.

9.3.9 Folgerung: Kriterium für positive Wurzeln, die Dimensionen von G und B

Sei G eine zusammenhängende reduktive lineare algebraische Gruppe mit dem maximalen Torus T und dem Wurzelsystem

$$R = R(G,T).$$

Weiter seien $B \supseteq T$ eine Borel-Untergruppe von G und $\alpha \in R$ eine Wurzel. Dann gilt:

(i) Die folgenden Aussagen sind äquivalent.

(a) $\alpha \in R^+(B)$.

(b) $X_\alpha \subseteq B$.

(c) $L(G)_\alpha \subseteq L(B)$.

(ii) $\dim B = \dim T + \frac{1}{2} \# R$.

(iii) $\dim G = \dim T + \# R$.

Beweis. (i). (a) $\Rightarrow$ (b). Auf Grund der Definition von $R^+(B)$ in 9.3.1 der Konstruktion der X_α in 9.3.7 ist

(1) $$L(B \cap Z_G S/R_u Z_G S) = L(T) \oplus L(X_\alpha)^{191} \text{ mit } S := \mathrm{Ker}(\alpha)^0.$$

Da X_α aus unipotenten Elementen besteht, liegt das Bild von X_α in einer der beiden Borel-Untergruppen von

$$Z_G S/R_u Z_G S.$$

Die Lie-Algebra der einen Borel-Untergruppe ist (1), die der anderen ist

(2) $$L(T) \oplus L(X_{-\alpha}).$$

Da $L(X_\alpha)$ nicht in (2) liegt, kann das Bild von X_α nicht in der zugehörigen Borel-Untergruppe liegen, d.h, es gilt

$$X_\alpha \subseteq B \cap Z_G S.$$

Damit gilt (b).

(i). (b) $\Rightarrow$ (c). Trivial, denn nach 9.3.7 ist $L(X_\alpha) = L(G)_\alpha$.

(i). (c) $\Rightarrow$ (a). Angenommen (a) ist falsch. Dann gilt $-\alpha \in R^+(B)$, also auf Grund der bereits bewiesenen Implikation (a) $\Rightarrow$ (b) auch

$$X_{-\alpha} \subseteq B.$$

---

[191] Man beachte, $L(X_\alpha) = L(G)_\alpha$ ist 1-dimensional und liegt im Eigenraum von α auf der Lie-Algebra rechts (nach 9.3.7).

Insgesamt liegen also beide Gruppen X_α und $X_{-\alpha}$ ganz in B. Nach 9.3.7 liegen beide Gruppen auch ganz in

$$G_\alpha := Z_G S \ , \ S := \mathrm{Ker}(\alpha)^0,$$

und sogar in (G_α, G_α) (vgl. 8.2.7) und haben damit nicht-triviale Bilder in

$$(3) \qquad G_\alpha/R_u\, G_\alpha = Z_G S/R_u Z_G S.$$

Diese Bilder liegen beide ganz in der Borel-Untergruppe

$$(4) \qquad B \cap Z_G S/R_u Z_G S.$$

Die Lie-Algebren $L(X_\alpha) = L(G)_\alpha$ und $L(X_{-\alpha}) = L(G)_{-\alpha}$ sind damit beide tangential zu (4). Dasselbe gilt trivialerweise für L(T). Damit haben also (3) und (4) dieselbe Lie-Algebra, d.h. die Gruppe (3) stimmt mit einer ihrer Borel-Untergruppen überein und ist damit auflösbar. Das steht im Widerspruch dazu, daß α eine Wurzel, d.h. S ein singulärer Torus sein soll.

(ii). Nach 9.3.8 gilt

$$L(G) = L(G)_0 \oplus (\oplus_{\alpha \in R} L(G)_\alpha)$$

also

$$\dim G = \dim L(G) = \dim L(G)_0 + \sum_{\alpha \in R} \dim L(G)_\alpha.$$

Die Räume $L(G)_\alpha$ haben nach 9.3.7 die Dimension 1.[192] Also gilt

$$\dim G = \dim L(G)_0 + \#R.$$

Weiter ist,

$$L(G_0) =^{193} L(Z_G(T)) =^{194} L(T),$$

also

$$\dim G = \dim T + \#R.$$

Damit ist di e erste Identität von (ii) bewiesen. Zum Beweis der zweiten beachten wir, daß L(B) in Eigenräume bezüglich der Operation von T zerfällt, d.h. L(B) ist die direkte Summe von L(T) und derjenigen Räume $L(G)_\alpha$ welche in L(B) liegen. Nach (i) folgt

$$L(B) = L(T) \oplus (\oplus_{\alpha \in R^+(B)} L(G)_\alpha),$$

also

---

[192] Wegen $\dim X_\alpha = \dim G_a = 1$.

[193] by 4.4.7

[194] by 9.3.6(ii), $Z_G(T) = T$.

$$\dim B = \dim T + \#R^+(B) = \dim T + \frac{1}{2}\#R.$$

QED.

9.3.10 Aufgaben

Seien G eine zusammenhängende reduktive lineare algebraische Gruppe und T ein maximaler Torus von G.

(1) Ist X eine 1-dimensionale zusammenhängende unipotente Untergruppe von G, welche normalisiert wird durch T, so gibt es ein $\alpha \in R = R(G,T)$ mit $X = X_\alpha$ (wie in 9.3.7).

(2) (a) Sei $t \in T$. Dann wird der zusammenhängende Zentralisator

$$Z_G(t)^0$$

erzeugt von T und den Untergruppen X_α mit $\alpha(t) = 1$. (Hinweis: man benutze 4.4.4(ii)).

(b) Der Zentralisator eines halbeinfachen Elements von G ist reduktiv.

(3) Das Wurzelsystem A_{n-1}. Seien $G = GL_n$ und $T = D_n$ (vgl. 2.1.3).

(a) Wir setzen

$$a_{ij}\begin{pmatrix} x_1 & 0 & \dots & 0 \\ 0 & x_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & x_n \end{pmatrix} := x_i x_j^{-1} \text{ für } 1 \le i,j \le n,\ i \ne j.$$

Man zeige, die a_{ij} sind Wurzeln, d.h. $a_{ij} \in R(G,T)$.

(b) $L(G) = gl_n$ ist die direkte Summe aus L(T) und den $L(G)_{a_{ij}}$ mit $i \ne j$. Man zeige, G ist reduktiv.

(c) Das Wurzel-Datum $\Phi(G,T)$ is isomorph zu (X,R,X^v,R^v) mit

$$X = X^v = \mathbb{Z}^n$$

(wobei die Paarung gerade das Standard-Skalarprodukt sei) und

$$R = R^v = \{ e_i - e_j \mid i \ne j \}.$$

Die e_i seien die Standard-Einheitsvektoren.

(d) Seien $G' := SL_n$ und $T' := T \cap G'$. Dann ist G' eine zusammenhängende halbeinfache Gruppe und T' ein maximaler Torus von G. Das Wurzel-Datum $\Phi(G',T')$ ist isomorph zu (X',X'^v,R',R'^v) mit

$$X' = X/\mathbb{Z}\cdot(e_1+\dots+e_n)$$

$X'^{v} = \{ (x_1,...,x_n) \in X^v \mid x_1+...+x_n = 0\}$

$R' = \pi R$,

$R'^{v} = R^v$.

Dabei sei $\pi: X \to X'$ die natürliche Abbildung.

(e) Sei $Z \subseteq GL_n$ die Untergruppe der skalaren Vielfachen der Einheitsmatrix (d.h. das Zentrum von GL_n). Wir setzen

$$G'' := G/Z,\ T'' := T/Z.$$

Dann ist G" eine zusammenhängende halbeinfache Gruppe mit dem maximalen Torus T" und das Wurzel-Datum $\Phi(G'',T'')$ ist isomorph zum Wurzel-Datum $\Phi(G',T')$ von (d).

(4) Das Wurzelsystem B_n. Sei char $k \neq 2$. Wir setzen

$$V := k^{2n+1}$$

und bezeichnen mit $(,)$ die symmetrische Bilinearform

$$(,): V\times V \to k, \left(\begin{pmatrix}\xi_0\\ ...\\ \xi_{2n}\end{pmatrix},\begin{pmatrix}\eta_0\\ ...\\ \eta_{2n}\end{pmatrix}\right) \mapsto \xi_0\eta_0 + \sum_{i=1}^{n} (\xi_i\eta_{n+i} + \xi_{n+i}\eta_i).$$

Weiter bezeichne G die Einskomponente der Gruppe

$$\{ t \in GL(V) \mid (tv,tw) = (v,w) \text{ für } v,w \in V\}$$

der Elemente aus GL(V), die diese Bilinearform invariant lassen.

(a) Man zeige, G ist isomorph zu SO_{2n+1} und die Gruppe T der Transformationen

$$\begin{pmatrix}\xi_0\\ ...\\ \xi_{2n}\end{pmatrix} \mapsto \begin{pmatrix}\xi_0\\ x_1\xi_1\\ ...\\ x_n\xi_n\\ x_1^{-1}\xi_{n+1}\\ ...\\ x_n^{-1}\xi_{2n}\end{pmatrix} \text{ mit } x_i \in k^* \text{ für alle } i$$

ist ein maximaler Torus von G. Die Abbildungen

$$\begin{pmatrix}x_1\\ ...\\ x_n\end{pmatrix} \mapsto x_i^{\varepsilon} \quad \text{und} \quad \begin{pmatrix}x_1\\ ...\\ x_n\end{pmatrix} \mapsto x_i^{2} x_j^{n} \text{ mit } i \neq j,\ n = \pm 1,\ \varepsilon = \pm 1$$

definieren Wurzeln von R(G,T).

(b) Die Lie-Algebra L(G) ist die Menge der $t \in End(V)$ mit

$$(tv, w) + (v, tw) = 0 \text{ für alle } v,w \in V$$

(Hinweis: man verwende 4.4.4(ii)). L(G) ist die direkte Summe aus L(T) und den $L(G)_\alpha$ mit α wie in (a). Man zeige, G ist halbeinfach.

(c) Das Wurzel-Datum $\Phi(G,T)$ ist isomorph zu $(X,R,X^\vee,R^\vee)$ mit

$$X = X^\vee = \mathbb{Z}^n$$
$$R = \{ \pm\varepsilon_i , \pm\varepsilon_i \pm\varepsilon_j \mid i \neq j \}$$
$$R^\vee = \{ \pm 2\varepsilon_i , \pm\varepsilon_i \pm\varepsilon_j \mid i \neq j \}$$

(5) Das Wurzelsystem D_n. Sei char $k \neq 2$. Wir setzen

$$V := k^{2n}.$$

Bezeichne $(,)$ die symmetrische Bilinearform

$$(,): V\times V \to k, \left(\begin{pmatrix} \xi_1 \\ \dots \\ \xi_{2n} \end{pmatrix}, \begin{pmatrix} \eta_1 \\ \dots \\ \eta_{2n} \end{pmatrix}\right) \mapsto \sum_{i=1}^{n} (\xi_i\eta_{n+i} + \xi_{n+i}\eta_i).$$

Wie in der vorigen Aufgabe bezeichne G die Einskomponente der Gruppe

$$\{ t \in GL(V) \mid (tv,tw) = (v,w) \text{ für } v,w \in V \}$$

der Elemente aus GL(V), die diese Bilinearform invariant lassen und T die Untergruppe der Transformationen

$$\begin{pmatrix} \xi_1 \\ \dots \\ \xi_{2n} \end{pmatrix} \mapsto \begin{pmatrix} x_1\xi_1 \\ \dots \\ x_n\xi_n \\ x_1^{-1}\xi_{n+1} \\ \dots \\ x_n^{-1}\xi_{2n} \end{pmatrix} \text{ mit } x_i \in k^* \text{ für alle } i.$$

Man zeige, G ist halbeinfach (und isomorph zu SO_{2n} und T ist ein maximaler Torus von G. Das Wurzeldatum $\Psi(G,T)$ ist isomorph zu

$$(X,R,X^\vee,R^\vee)$$

mit

$$X = X^\vee = \mathbb{Z}, R = R^\vee = \{\pm\varepsilon_i \pm\varepsilon_j \mid i \neq j\}.$$

(6) Das Wurzelsystem C_n. Sei

$$V = k^{2n}$$

und (,) die alternierende Bilinearform

$$(,) : V\times V \to k, \left(\begin{pmatrix}\xi_1\\ \dots \\ \xi_{2n}\end{pmatrix},\begin{pmatrix}\eta_1\\ \dots \\ \eta_{2n}\end{pmatrix}\right) \mapsto \sum_{i=1}^{n}(\xi_i\eta_{n+i} - \xi_{n+i}\eta_i).$$

Sei G die symplektische Gruppe Sp_{2n} , d.h. die (nach 6.6.(2) zusammenhängende) Gruppe

$$G = \{ t\in GL(V) \mid (tv,tw) = (v,w) \text{ für } v,w\in V\}.$$

Weiter sei T wie in (5) die Untergruppe der Transformationen

$$\begin{pmatrix}\xi_1\\ \dots \\ \xi_{2n}\end{pmatrix} \mapsto \begin{pmatrix} x_1\xi_1 \\ \dots \\ x_n\xi_n \\ x_1^{-1}\xi_{n+1} \\ \dots \\ x_n^{-1}\xi_{2n}\end{pmatrix} \text{ mit } x_i\in k^* \text{ für alle } i.$$

Man zeige, T ist ein maximaler Torus von G und G ist halbeinfach. Das zugehörige Wurzeldatum $\Psi(G,T)$ ist isomorph zu

$$(X,R,X^\vee,R^\vee)$$

mit

$$X = X^\vee = \mathbb{Z},$$
$$R = \{\pm 2\varepsilon_i , \pm\varepsilon_i\pm\varepsilon_j \mid i\neq j\}.$$
$$R^\vee = \{\pm\varepsilon_i , \pm\varepsilon_i\pm\varepsilon_j \mid i\neq j\}.$$

Lösungen

Zu (1)

Nach dem Struktursatz 2.2.6 für 1-dimensionale lineare algebraische Gruppen gibt es einen Isomorphismus linearer algebraischer Gruppen

$$x: G_a \to X .$$

Nach Voraussetzung ist die Abbildung

$$X \to X, g \mapsto tgt^{-1},$$

für jedes $t\in T$ ein wohldefinierter Automorphismus linearer algebraischer Gruppen. Mit Hilfe von x induziert dieser einen Automorphismus

(1) $$G_a \to G_a ,$$

der seinerseits einen Automorphismus von $k[G_a] = k[T]$ induziert. Letzterer ist (wie jeder Morphismus von Varietäten) durch ein Polynom definiert (das Bild von T). Da es sich um einen Automorphismus handelt, ist dieses Polynom linear. Da der Automorphismus von einem Gruppenhomomorphismus kommt, ist das Polynom additiv, d.h. es ist ein lineares homogenes Polynom in T. Der Automorphismus (1) hat damit die Gestalt

$$G_a \to G_a\ ,\ \xi \mapsto \alpha(t)\xi,$$

mit $\alpha(t) \in k^*$. Damit gilt

(2) $$tx(\xi)t^{-1} = x(\alpha(t)\xi) \quad \text{für } t\in T,\ \xi\in G.$$

Insbesondere ist $\alpha(t) = x^{-1}(tx(\xi)t^{-1})/\xi$ von ξ unabhängig und als Funktion von t eine reguläre Funktion. Weiter gilt
$\alpha(tt') = \alpha(t)\alpha(t')$ für $t,t'\in T$,
d.h.

$$\alpha: T \to G_m$$

ist ein Charakter. Seien

$$S := \mathrm{Ker}(\alpha)^0$$
$$Z := Z_G(S).$$

Nach 9.3.6 (i) ist Z zusammenhängend und reduktiv. Wäre α trivial, so wäre S = T und nach 9.3.6 T = Z. Wegen (2) wäre damit
$\mathrm{Im}(x) \subseteq Z_G(T) = Z_G(S) = Z = T$,
d.h. jedes $x(\xi)$, $\xi\in G_a$, wäre sowohl unipotent als auch halbeinfach, d.h. $x(\xi) = e$. Das steht im Widerspruch dazu, daß x ein Isomorphismus sein sollte. Also ist

$$\alpha: T \to G_m \text{ nicht trivial.}$$

Insbesondere ist S ein Torus der Kodimension 1 in T. Nach (2) gilt

$$X = \mathrm{Im}(x) \subseteq Z_G(S) = Z,$$

denn $\alpha(t) = 1$ für $t\in S$. Wir haben nocht zu zeigen, α ist eine Wurzel, d.h. Z ist nicht auflösbar. Angenommen, Z ist auflösbar. Für jede Borel-Untergruppe $B\in \mathbf{B}_T$ ist dann $S \subseteq T \subseteq B$, d.h. $B\cap Z$ ist eine Borel-Untergruppe von Z (vgl. 7.3.5(ii)), d.h.

$$Z = B\cap Z \subseteq B.$$

Nach (2) gilt aber $X = \mathrm{Im}(x) \subseteq Z$, d.h. es ist $X \subseteq B$ für jedes $B\in \mathbf{B}_T$. Wegen $X \cong G_a$ gilt damit sogar

$$X \subseteq B_u \text{ für jedes } B\in \mathbf{B}_T\ ,$$

also

$$X \subseteq \cap_{B \in \mathbf{B}_T} B_u$$

also nach (9.3.5) sogar $X \subseteq R_u G$. Das unipotente Radikal von G ist aber trivial, da G nach Voraussetzung reduktiv sein soll. Also ist X trivial. Das steht aber im Widerspruch zur Voraussetzung dim X = 1. Also ist Z nicht auflösbar, d.h. S ein singulärer Torus, d.h. α eine Wurzel von G.

Nach (9.3.8) ist L(G) die direkte Summe von L(T) und den $L(G)_\alpha$ mit $\alpha \in R = R(G,T)$ und nach 9.3.7 gilt $L(G)_\alpha = L(X_\alpha)$. Insbesondere sind die letzteren Räume 1-dimensional. Die Teil-Lie-Algebra

(1) $$L(Z) \subseteq L(G),\ Z := Z_G(t))$$

zerfällt in eine direkte Summe von T-invarianten Unterräumen (weil T diagonalisierbar ist) und enthält L(T) (wegen $T \subseteq Z$). Jeder invariante direkte Summand der Dimension 1 der Lie-Algebra L(Z() ist auch ein solcher von L(G). Deshalb ist L(Z) eine direkte Summe aus L(T) und denjenigen $L(X_\alpha)$, die ganz in L(Z():

$$L(Z) = L(T) \oplus (\oplus_{\alpha \in R, L(X_\alpha) \subseteq L(Z)} L(X_\alpha)).$$

Nun gilt nach (4.4.4(ii))

$$L(Z) = L(G_{\sigma_t}) = L(G)_{\sigma_t} = \{X \in L(G) \mid Ad(t)X = X\}$$

Die Bedingung $L(X_\alpha) \subseteq L(Z)$ ist daher äquivalent zu

$$Ad(t)X = X \text{ für alle } X \in L(X_\alpha),$$

d.h. zu

$$\alpha(t)X = X \text{ für alle } X \in L(X_\alpha),$$

d.h. zu $\alpha(t) = 1$. Die obige direkte Zerlegung von L(Z) bekommt damit die Gestalt

(2) $$L(Z) = L(T) \oplus (\oplus_{\alpha \in R, \alpha(t)=1} L(X_\alpha)).$$

Sei jetzt Z' die von T und den X_α mit $\alpha(t) = 1$ erzeugte Untergruppe von G. Nach 6.1 ist Z' abgeschlossen und zusammenhängend. Wegen

(3) $$T \subseteq Z \text{ und } X_\alpha \subseteq Z \text{ für } \alpha(t) = 1$$

gilt $Z' \subseteq Z$ also $Z' \subseteq Z^0$. Es reicht also, zu zeigen, dim $Z' \geq$ dim Z^0. Dazu wiederum reicht es, zu zeigen

$$L(Z') \supseteq L(Z).$$

Wegen (2) reicht es zu zeigen

$$L(Z') \supseteq L(T) \text{ und } L(Z') \supseteq L(X_\alpha) \text{ für } \alpha(t) = 1.$$

Letzteres ergibt sich aber aus den Inklusionen (3).

Zu (2)(b).

Sei $t \in G$ ein halbeinfaches Element. Wir zeigen, der zusammenhängende Zentralisator

$$Z := Z_G(t)^0$$

ist der Zentralisator eines Torus S. Nach (9.3.6)(i) ist damit Z reduktiv.

Nach (7.3.3)(ii) gibt es einen maximalen Torus $T \subseteq G$ mit $t \in T$. Wir setzen

$$R(t) := \{ \alpha \in R(G,T) \mid \alpha(t) = 1\}$$

Nach Aufgabe (2)(a) hängt Z nur von R(t) (und nicht von t) ab, d.h. für alle $t' \in T$ mit $R(t') = R(t)$ ist der zusammenhängende Zentralisator von t' gleich Z, d.h. es gilt

$$Z_G(t')^0 = Z \text{ falls } \alpha(t') = 1 \text{ für alle } \alpha \in R(t) \text{ und } \alpha(t') \neq 1 \text{ für alle } \alpha \in R - R(t)$$

Sei

$$D(t) := \cap_{\alpha \in R(t)} \mathrm{Ker}(\alpha)$$

Dann kann man die letzte Aussage in der folgenden Gestalt aufschreiben:

(4) $Z_G(t')^0 = Z$ für jedes $t' \in D(t)$ mit $\alpha(t') \neq 1$ für alle $\alpha \in R - R(t)$.

Nach Konstruktion ist D(t) eine abgeschlossene Untergruppe des maximalen Torus T, also insbesondere diagonalisierbar. Sei

$$\alpha \in R - R(t)$$

Dann ist

(5) $$\mathrm{Ker}(\alpha) \cap D(t)$$

eine abgeschlossene Untergruppe von D(t). Insbesondere haben alle Komponenten von dieser Untergruppe dieselbe Dimension, d.h. (5) ist entweder gleich D(t) oder eine Hyperfläche von D(t). Der erste Fall kann nicht eintreten, weil t in D(t) liegt aber nicht in $\mathrm{Ker}(\alpha)$. Insbesondere hat (5) eine kleinere Dimension als D(t) und es gilt

$$S := D(t)^0 \not\subseteq \mathrm{Ker}(\alpha) \text{ für } \alpha \in R - R(t).$$

Weil S irreduzibel ist, folgt

$$S \not\subseteq \cup_{\alpha \in R-R(t)} \mathrm{Ker}(\alpha),$$

d.h.

$$U(t) := S - \cup_{\alpha \in R-R(t)} \mathrm{Ker}(\alpha)$$

ist eine nicht-leere offene Teilmenge von S und wegen (4) gilt

(6) $Z_G(t')^0 = Z$ für jedes $t' \in U(t)$.

Falls man t' aus der größeren Menge $S \subseteq D(t)$ wählt so gilt nach Definition von D(t) wenigstens $\alpha(t') = 1$ für alle $\alpha \in R(t)$, d.h.

$$R(t) \subseteq R(t'),$$

d.h. die Menge der zu t' gehörigen X_α ist eventuell größer als die Menge der X_α die zu t gehören. Nach Aufgabe (2)(a) ist damit

$$Z \subseteq Z_G(t').$$

Wir haben gezeigt,

(7) $Z_G(t')^0 \supseteq Z$ für jedes $t' \in S$.

Nach (6) und (7) gilt mit damit

(8) $$Z = \cap_{t' \in S} Z_G(t')^0 \subseteq \cap_{t' \in S} Z_G(t') = Z_G(S),$$

Nun ist S eine zusammenhängende diagonalisierbare Gruppe, also ein Torus. Nach (9.3.6)(i) ist $Z_G(S)$ zusammenhängend und reduktiv. Insbesondere gilt

$$Z_G(S) \subseteq Z_G(t')^0 \text{ für jedes } t' \in S.$$

Wählt man ein t' aus der offenen dichten Teilmenge U(t) von S, so sieht man auf Grund von (6), daß sogar $Z_G(S) \subseteq Z$ gilt. Zusammen mit (8) ergibt sich

$$Z = Z_G(S).$$

Insbesondere ist Z reduktiv.

QED.

Zu (3).

1 Schritt. $T = D_n$ ist ein maximaler Torus von G.

Nach Aufgabe 7.2.11 (4) bilden die oberen Dreiecksmatrizen in G eine Borel-Untergruppe

$$B = \mathbf{T}_n.$$

Der unitpotente Anteil der Gruppe ist gerade

$$B_u = \mathbf{U}_n$$

die Gruppe der oberen Dreiecksmatrizen mit Einsen auf der Hauptdiagonalen und B/B_u hat die Dimension eines maximalen Torus von B (also von G). Wegen

$$\dim B/B_u = n$$

ist damit die Gruppe der Diagonalmatrizen

$$D_n \subseteq G$$

ein maximaler Torus von G.

2 Schritt. Die a_{ij} sind Wurzeln von G.

Offensichtlich sind die $a_{ij}: D_n \to G_m$ Charaktere. Zum Beweis der Wurzeleigenschaft können wir annehmen i = 1 und j = 2 (andernfalls permutiere man die Basis von k^n). Wir schreiben $a = a_{12}$. Es gilt

$$S := \mathrm{Ker}(a) = \{ \begin{pmatrix} x_1 & 0 & \dots & 0 \\ 0 & x_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & x_n \end{pmatrix} \mid x_1 = x_2 \} = \mathrm{Ker}(a)^0$$

Berechnen wir den Zentralisator des Torus S in G. Für $s = \begin{pmatrix} x_1 & 0 & \dots & 0 \\ 0 & x_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & x_n \end{pmatrix} \in S$

und $g = (g_{ij})$ ist der Eintrag in der Position von (i,j) der Matrix tgt^{-1} gleich $x_i g_{ij} x_j^{-1}$. Deshalb gilt

$$g \in Z_G(S) \Leftrightarrow x_i g_{ij} x_j^{-1} = g_{ij} \text{ für alle i und j und alle } x_1 \text{ mit } x_1 = x_2.$$

$$\Leftrightarrow g_{ij}(x_i x_j^{-1} - 1) = 0 \text{ für alle i und j und alle } x_1 \text{ mit } x_1 = x_2.$$

Für $(i,j) \neq (1,2), (2,1)$ ist das nur möglich falls i = j gilt oder $g_{ij} = 0$. Daraus ergibt sich

$$(*) \qquad Z_G(S) = \{ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \mid A \in GL_2 , B \in D_{n-2} \} \cong GL_2 \times D_{n-2}$$

Wegen

$$SL_2 \subseteq GL_2$$

ist GL_2 und damit auch $Z_G(S)$ nicht auflösbar[195], d.h. $S = \mathrm{Ker}(a)^0$ ist ein singulärer Torus. Dann ist aber a eine Wurzel von G.

3. Schritt: die Zerlegung der Lie-Algebra von G.

Da die a_{ij} Wurzeln sind, sind die Gewichtsräume

$$L(G)_{a_{ij}}$$

mindestens 1-dimensional. Gewichtsvektoren ´zu verschiedenen Gewichten sind stets linear unabhängig, d.h. die Summe

---

[195] Jede Untergruppe einer auflösbaren Gruppe ist auflösbar.

$$L(D_n) + \sum_{i \neq j} L(G)_{a_{ij}}$$

ist direkt und damit von der Dimension

$$\dim D_n + \sum_{i \neq j} \dim L(G)_{a_{ij}} \geq^{196} n + n(n-1) = n.$$

Damit gilt $\dim L(G)_{a_{ij}} = 1$ für $i \neq j$ und

$$L(G) = L(D_n) \oplus (\oplus_{i \neq j} L(G)_{a_{ij}}).$$

4. Schritt. G ist reduktiv.
Das Radikal R(G) liegt in einer, also in jeder Borel-Untergruppe von G. Insbesondere gilt

$$R(G) \subseteq \mathbf{T}_n \quad \text{(obere Dreiecksmatrizen)}.$$

Das Unipotente Radikal besteht also aus lauter oberen Dreicksmatrizen mit Einsen auf der Hauptdiagonale:

$$R_u(G) \subseteq \mathbf{U}_n.$$

Aus Symmetriegründen gilt dann aber auch

$$R_u(G) \subseteq U'$$

wenn U' die unteren Dreiecksmatrizen mit Einsen auf der Hauptdiagonale bezeichnet. Wege $\mathbf{U}_n \cap U' = \{e\}$ folgt $R_u(G) = \{e\}$, d.h. G ist reduktiv.

5. Schritt. Das Wurzeldatum (X,R,X^v,R^v) von G.
Bezeichne

$$\chi_i : D_n \to G_m$$

die Projektion auf den i-ten Eintrag der Hauptdiagonalen. Dann ist X die von den χ_i erzeugte freie abelsche Gruppe, d.h. die $\mathbb{Z}$-lineare Abbildung

$$\mathbb{Z}^n \to X,\ e_i \mapsto \chi_i\ ,$$

ist ein Gruppen-Isomorphismus. Die Menge der Wurzeln a_{ij} wird dabei in die oben angegebene Menge R abgebildet. Sei weiter

$$\chi_i^v : G_m \to D_n$$

die Abbildung, welche $t \in k^*$ abbildet in die Diagonalmatrix, deren i-ter Eintrag auf der Hauptdiagonalen gleich t ist und die sonst mit der

---

[196] In der Summe links gibt es für jede Position außerhalb der Hauptdiagonalen einen Summanden ≥ 1.

Einheitmatrix übereinstimmt. Dann ist X^v die von den χ_i^v erzeugte freie abelsche Gruppe[197], d.h. die $\mathbb{Z}$-lineare Abbildung

$$\mathbb{Z}^n \to X^v, e_i \mapsto \chi^v{}_i ,$$

ist ein Gruppen-Isomorphismus. Die Paarung

$$X \times X^v \to \mathbb{Z}, (\chi, \chi^v) \mapsto <\chi, \chi^v>,$$

entspricht bei den obigen Isomorphismen gerade dem Standard-Skalarprodukt

$$(,) : \mathbb{Z}^n \times \mathbb{Z}^n \to \mathbb{Z}, \left(\begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \dots \\ y_n \end{pmatrix} \right) \mapsto \sum_{i=1}^{n} x_i y_i ,$$

(wegen $< \chi_i, \chi_j^v > = \delta_{ij}$)[198].

Wir haben noch zu zeigen, die Menge R^v der Kowurzeln ist gerade die oben angegebene Menge. Dazu reicht es zu zeigen, die Kowurzel zur Differenz $\chi_i - \chi_j$ ist gerade $\chi_i^v - \chi_j^v$, d.h. die Spiegelung an der zu $\chi_i - \chi_j$ orthogonalen Hyperebene ist gerade

$$s(x) = x - <x, \chi_i^v - \chi_j^v>(\chi_i - \chi_j).$$

Wir benutzen die obigen Isomorphismen um X und X^v mit $\mathbb{Z}^n$ zu identifizieren. Die Abbildung s bekommt dann die Gestalt

$$s(x) = x - (x, e_i - e_j) (e_i - e_j)$$

---

[197] Sei $f: G_m \to D_n$ ein Homomorphismus algebraischer Gruppen. Bezeichne

$$p_i : D_n \to G_m$$

die Projektion auf den i-ten Eintrag der Hauptdiagonalen. Dann ist

$$p_i \circ f : G_m \to G_m$$

ein Charakter, d.h. $p_i \circ f (\xi) = \xi^{\nu_i}$. Desghalb hat f die Gestalt

$$f(\xi) = \begin{pmatrix} \xi^{\nu_1} & 0 & \dots & 0 \\ 0 & \xi^{\nu_2} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \xi^{\nu_n} \end{pmatrix}$$

und für beliebige $\nu_1, \dots, \nu_n \in \mathbb{Z}$ ist auf diese Weise eine 1-parametrige Untergruppe von D_n definiert.

[198] Es gilt $\chi_i(\chi_j^v(\xi)) = \begin{cases} \xi \text{ falls } i=j \\ 1 \quad \text{sonst} \end{cases}$

Sei n_{ij} ein Vektor der Länge 1 in Richtung $e_i - e_j$, d.h.

$$n_{ij} = \frac{\varepsilon}{\sqrt{2}} (e_i - e_j)$$

mit $\varepsilon = \pm 1$. Dann gilt

$$s(x) = x - 2\,(x, n_{ij})n_{ij},$$

d.h. s ist tatsächlich die erwähnte Spiegelung.

6. Schritt. Beschreibung von SL_n (Aussage von (3)(d)

6.1: SL_n ist zusammenhängend.

Jedes $x \in SL_n$ ist konjugiert zu einer oberen Dreieksmatrix[199]:

$$gxg^{-1} \in \mathbf{T}_n \text{ für eine } g \in G.$$

Weil k algebraisch abeschlossen ist kann man g in der Gestalt $g = \lambda \cdot g'$ schreiben mit $\lambda \in k^*$ und $g' \in SL_n$. Damit ist

$$g'xg'^{-1} = gxg^{-1} \in \mathbf{T}_n\,,\ g' \in SL_n.$$

Mit anderen Worten die Untergruppen der Gestalt

$$gB'g^{-1} \text{ mit } B' := \mathbf{T}_n \cap SL_n \text{ und } g \in SL_n$$

überdecken SL_n und erzeugen also SL_n. Nach (6.1) reicht es zu zeigen, B' ist zusammenhängend. Offensichtlich ist $\mathbf{T}_n$ zusammenhängend (als zariski-offene Menge des $k^{n(n+1)/2}$). B' ist in $\mathbf{T}_n$ definiert durch die Gleichung

$$1 = \det \begin{pmatrix} x_1 & 0 & \dots & 0 \\ 0 & x_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & x_n \end{pmatrix} = x_1 x_2 \cdot \ldots \cdot x_n$$

Wir haben zu zeigen, der Koordinatenring von B',

$$k[B'] = k[\mathbf{T}_n]/(f)$$
$$= k[T_1,\ldots,T_n, \text{ weitere Unbestimmte}]_g/(f)$$

mit $g = T_1 T_2 \cdot \ldots \cdot T_n$ und $f = g - 1$, ist nullteilerfrei.

Dazu reicht es zu zeigen,

$$k[T_1,\ldots,T_n,\ldots]/(f) \cong k[T_1,\ldots,T_{n-1}]_h \text{ mit } h = T_1 T_2 \cdot \ldots \cdot T_{n-1},$$

---

[199] Weil k algebraisch abgeschlossen ist, gibt es in k^n eine vollständige Fahne von linearen Unterräumen, die invariant sind bezüglich Multiplikation mit x.

denn dann ist k[B'] ein iterierter Quotientenring eines nullteilerfreien Rings (nämlich von $k[T_1,...,T_n, ...]$). Allgemeiner reicht es zu zeigen, für kommutative Ringe R mit 1 und Elemente $r \in R$ gilt

$$R[T]/(Tr - 1) \cong R_r .$$

Das ist aber der Fall, weil die linke Seite die Universatitätseigenschaft der rechten hat.[200]

6.2 : $B' := \mathbf{T}_n \cap SL_n$ ist Borel-Untergruppe von SL_n

Wie in 6.1 gezeigt ist B' zusammenhängend. Die Untergruppe ist auflösbar, weil $\mathbf{T}_n$ es ist. Wir haben noch zu zeigen, B' ist maximal bezüglich dieser Eigenschaften. Dazu reicht es zu zeigen, B' enthält eine Borel-Untergruppe. Um letzteres zu zeigen, reicht es wenn wir zeigen, B' ist parabolisch (vgl. 7.2.6(i)). Nun ist $\mathbf{T}_n$ der Stabilisator der Standard-Fahne

$$V_0 \subset V_1 \subset ... \subset V_n = k^n \ , \ V_i = \text{erzeugt von } e_1, ... , e_i$$

in G. Deshalb ist B' der Stabilisator dieser Fahne in SL_n. Genau wie G operiert SL_n transitiv auf den vollständigen Fahnen (weil jedes Element von G ein k*-Vielfaches eines Elements von SL_n ist). Deshalb gilt

$$SL_n/B' \cong \{ \text{ vollständige Fahnen von } k^n \} \cong G/\mathbf{T}_n .$$

Der Faktor ist also eine projektive Varietät, d.h. B' ist parabolisch.

6.3 : $T' := D_n \cap SL_n$ ist maximaler Torus von SL_n.

Es reicht zu zeigen, T' ist maximaler Torus der Borel-Untergruppe B'. Das ist aber der Fall, denn die natürliche Abbildung induziert eine Bijektion $T' \to B'/B'_u$.[201]

6.4: Jeder Normalteiler von SL_n ist auch Normalteiler von $G = GL_n$.

---

[200] Sei $h:R \to S$ ein ein Homomorphismus, der r in eine Einheit abbildet. Dann läßt sich h auf den Polynomring fortsetzen:

$$R[T] \to S \ , \ T \mapsto h(r)^{-1} .$$

Die Fortsetzung bildet Tr - 1 in die Null ab, induziert also einen Homomorphismus

$$R[T]/(Tr-1) \to S .$$

Ist umgekehrt $h': R[T]/(Tr-1) \to S$ eine Fortsetzung von h, so gilt

$$0 = h'(cl(T)r - 1) = h'(cl(T))\, h(r) - 1,$$

d.h. $h'(cl(T)) = h(r)^{-1}$, d.h. die Fortsetzung von h ist eindeutig bestimmt.

[201] Der halbeinfache Faktor der Jordan-Zerlegung in B' liefert zu jedem Element von B'/B'_u ein Urbild. Die Abbildung ist injektiv, weil nur unipotente Elemente im Kern liegen.

Jedes Element $g \in G$ hat die Gestalt $g = \lambda \cdot g'$ mit $g' \in SL_n$. Die Konjugation mit g ist also gleich der Konjugation mit g'.

6.5.: SL_n ist halbeinfach.

$R(SL_n)$ ist nach 6.4 ein zusammenhängender auflösbarer Normalteiler in G. Deshalb gilt

$$R(SL_n) \subseteq R(G)$$

also $R_u(SL_n) \subseteq R_u(G) = \{e\}$ (da G reduktiv ist). Deshalb ist

$$S := R(SL_n)$$

ein Torus. Er liegt in einem maximalen Torus und als Normalteiler damit in jedem maximalen Torus. Insbesondere gilt

$$S \subseteq T' \subseteq D_n.$$

Nun ist S ein Normalteiler in SL_n, also nach 6.4 auch einer in G. Für $s \in S$ ist also insbesondere gsg^{-1} eine Diagonalmatrix für jedes $g \in G$. Das ist aber nur möglich, wenn s ein Vielfaches der Einheitsmatrix ist.[202] Damit gilt

$$S \subseteq \{\lambda \cdot Id \mid \lambda \in k^*\}.$$

Wegen $S \subseteq SL_n$ folgt sogar

$$S \subseteq \{\lambda \cdot Id \mid \lambda \in k^* \text{ und } \lambda^n = 1\}.$$

Rechts steht eine endliche Menge und S ist zusammenhängend. Deshalb gilt

---

[202] Der Übergang von s zu gsg^{-1} entspricht dem Wechsel zu einer anderen Basis des k^n. Dabei ist gsg^{-1} genau dann von Diagonalgestalt, wenn die neue Basis eine Eigenbasis ist. Fall s unterschiedliche Eigenwerte besitzt, gibt es aber stets eine Basis, die keine Eigenbasis ist.

Explizit:

Ist s keine Skalarmatrix, d.h. hat s mehr als einen Eigenwert, so gibt es Indizes i und j mit

$$se_i = c_i e_i \text{ und } se_j = c_j e_j \text{ und } c_i \neq c_j.$$

Sei g die Matrix mit

$$ge_\nu = e_\nu \text{ für } \nu \neq i \text{ und } ge_i = e_i + e_j$$

Für die inverse Matrix gilt dann

$$g^{-1}e_\nu = e_\nu \text{ für } \nu \neq i \text{ und } g^{-1}e_i = e_i - e_j$$

Damit ist

$$(gsg^{-1})e_i = gs(e_i - e_j) = g(c_i e_i - c_j e_j) = c_i e_i + c_i e_j - c_j e_j = c_i e_i + (c_i - c_j)e_j,$$

d.h. e_i ist kein Eigenwert von gsg^{-1}, d.h. gsg^{-1} ist keine Diagonalmatrix.

$$R(SL_n) = S = \{e\},$$

d.h. SL_n ist halbeinfach.

6.6.: Vergleich der Charaktergruppen X und X' von G und G'.
Wir betrachten die exakte Sequenz von Tori

$$1 \to T' \to T \to T/T' \to 1.$$

Sie induziert eine exakte Sequenz der Charaktergruppen

$$0 \to X(T/T') \to X \to X' \to 0$$

(vgl. Aufgabe ...). Die Charaktere von T/T' kann man mit den Charakteren $\chi \in X$ von T identifizieren,

$$\chi\begin{pmatrix} x_1 & \dots & \dots \\ \dots & \dots & \dots \\ 0 & \dots & x_n \end{pmatrix} = x_1^{\nu_1} \cdot \dots \cdot x_n^{\nu_n},$$

die auf T' trivial sind, d.h. für $x_n = 1/(x_1 \cdot \dots \cdot x_{n-1})$ ist der obige Ausdruck Null, d.h.

$$x_1^{\nu_1 - \nu_n} \cdot \dots \cdot x_{n-1}^{\nu_{n-1} - \nu_n} = 1 \text{ für beliebige } x_1, \dots, x_{n-1} \in k^*.$$

Das ist nur möglich, falls alle Exponenten gleich sind,

$$\nu_1 = \dots = \nu_n .$$

Identifiziert man jeden Charakter mit dem Tupel der zugehörigen Exponenten, $X = \mathbb{Z}^n$, so bekommt die obige exakte Sequenz die Gestalt

$$0 \to \mathbb{Z} \cdot (e_1 + \dots + e_n) \to \mathbb{Z}^n \to X' \to 0,$$

d.h. X' hat die behauptete Gestalt,

$$X' = \mathbb{Z}^n / \mathbb{Z} \cdot (e_1 + \dots + e_n).$$

Bezeichne π: X → X' die natürliche Abbildung.

6.7.: Die Einschränkungen $a'_{ij} := a_{ij}|_{T'}: T' \to G_m = \pi(a_{ij})$ der Wurzeln von G auf T' sind Wurzeln von G' = SL_n , es gibt keine weiteren.

O.B.d.A. sei i = 1 und j= 2. Nach dem zweiten Schritt gilt

$$S' := (\operatorname{Ker} a'_{12})^0 = T' \cap S = \left\{ \begin{pmatrix} x_1 & 0 & \dots & 0 \\ 0 & x_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & x_n \end{pmatrix} \mid x_1 = x_2 \,,\, x_1 x_2 \cdot \dots \cdot x_n = 1 \right\}.$$

Man beachte, die Menge rechts ist zusammenhängend (auf Grund desselben Arguments wie für die Irreduzibilität von $\mathbf{T}_n$ in 6.1). Weiter ist

$$Z_{G'}(S') = \{g' \in G' \mid g't' = t'g' \text{ für } t' \in S\} = G' \cap Z_G(S)$$

(weil jedes Element von G skalares Vielfaches eines Elements von G' ist und analog für S und S'). Nach dem zweiten Schritt ist damit

$$Z_{G'}(S') = SL_n \cap (GL_2 \times D_{n-2}) \supseteq SL_2 \times \{e\},$$

d.h. $Z_{G'}(S')$ ist nicht auflösbar und S' damit ein singulärer Torus. Dann ist aber a'_{12} eine Wurzel von G'. Analog sind die a'_{ij} Wurzeln von G'. Wir haben noch zu zeigen, es gibt keine weiteren.

Weil G' halbeinfach, also reduktiv ist, kennen wir nach 9.3.8 die Zerlegung der Lie-Algebra von G',

$$L(G') = L(T') \oplus (\oplus_{i \neq j} L(G_{a_{ij}})) \oplus ???,$$

wobei die weiteren direkten Summanden eventuellen weiteren Wurzeln entsprechen. Nun ist aber

$$\dim L(G') = \dim SL_n = n^2 - 1.$$

$$\dim L(T') = n - 1$$

und die Anzahl der a_{ij} ist gerade $n^2 - n$. Aus Dimensionsgründen kann es also keine weiteren direkten Summanden geben. Die Menge der Wurzeln von G' ist damit gleich der Menge der a_{ij}, d.h.

$$R' = \pi(R).$$

6.8.: die 1-Parameter-Untergruppen von T'.
T' hat in T die definierende Gleichung

$$x_1 \cdot \ldots \cdot x_n = 1.$$

Eine 1-Parameter-Untergruppe $h: G_m \to T$,

$$h(\xi) = \begin{pmatrix} \xi^{\nu_1} & 0 & \ldots & 0 \\ 0 & \xi^{\nu_2} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \xi^{\nu_n} \end{pmatrix}$$

ist genau dann eine solche von T', wenn das Produkt der Einträge auf der Hauptdiagonalen für alle ξ gleich 1 ist, d.h. wenn die Summe der Exponenten 0 ist:

$$X'^{\nu} = \{(x_1, \ldots, x_n) \in X^{\nu} \mid x_1 + \ldots + x_n = 0\}$$

6.9.: Die Kowurzeln von G'.

Die oben konstruierten Kowurzeln von GL_n haben die Gestalt

$$a_{ij}^{v}(\xi) = \mathrm{diag}(1,...,\xi,...,\xi^{-1},...,1)$$

wobei die von 1 verschiedenen Koordinaten gerade die i-te bzw. j-te Koordinate sind. Insbesondere liegen die Werte der Kowurzeln sogar in T', d.h. es sind Elemente von X'^{v}. Schließlich liefern die definierenden Identitäten für die Kowurzeln von G durch Einschränken der Charaktere auf T' gerade die definierenden Identitäten für die Kowurzeln von G'.

7. Schritt. Die Aussage von (3)(e).

Man verwende Argumente, die in gewisser Weise dual zu den Argumenten des 6. Schritts sind.

Zu (4).

9.4 Halbeinfache Gruppen

Wir beenden dieses Kapitel mit einigen Eigenschaften der halbeinfachen Gruppen.

Vereinbarung

Wie bisher sei G eine zusammenhängende reduktive lineare algebraische Gruppe mit dem maximalen Torus T und dem Wurzelsystem R = R(G,T).

9.4.1 Theorem: Die zusammenhängenden abgeschlossenen Normalteiler einer halbeinfachen Gruppe

Sei G eine halbeinfache zusammenhängende lineare algebraische Gruppe. Dann gilt:

(i) Die Untergruppen X_α mit $\alpha \in R$ (vgl. 9.3.7) erzeugen G.

(ii) G = (G,G).

(iii) Sei $N' \subseteq G$ ein zusammenhängender abgeschlossener Normalteiler. Dann ist N' halbeinfach. Es gibt einen zusammenhängenden abgeschlossenen Normalteiler N" mit

$$(N', N'') = \{e\} \text{ und } N' \cap N'' \text{ endlich, } G = N'N''.$$

(iv) Die Anzahl der minimalen nicht-trivialen zusammenhängenden abgeschlossenen Normalteiler von G ist endlich. Sind

$$N_1,...,N_r$$

diese Normalteiler, so gilt

$$(N_i, N_j) = \{e\}, \; N_i \cap \Big(\prod_{i \neq j} G_j\Big) \text{ endlich, } G = N_1 \cdot ... \cdot N_r .$$

Die N_i besitzen keine abgeschlossenen Normalteiler positiver Dimension.

Beweis. 1. Schritt: die Halbeinfachheit der Gruppe N' von (iii).

Das Radikal R(N') von N' ist zusammenhängend, auflösbar, abgeschlossen in G und ist ein Normalteiler in G. Also liegt R(N') im Radikal von G und ist damit trivial. Also ist N' auflösbar.

2. Schritt. Beweis von (i).

Sei G' die von den X_α erzeugte Untergruppe von G,

$$G' := \text{Erzeugnis der } X_\alpha.$$

Wir haben zu zeigen, G' = G. Nach 6.1 ist

G' abgeschlossen und zusammenhängend.

Die X_α erzeugen zusammen mit T die Gruppe G (nach (9.3.7)(ii)). Es reicht also zu zeigen,

$$T \subseteq G'.$$

Die X_α normalisieren[203] G'. Also ist

(1) G' Normalteiler in G.

Der Durchschnitt

$$(\cap_{\alpha\in R}\ \mathrm{Ker}(\alpha))^0$$

ist ein Torus von G und liegt im Zentrum[204] von G. Damit liegt der Durchschnitt im Radikal von G, ist also trivial,

$$(\cap_{\alpha\in R}\ \mathrm{Ker}(\alpha))^0 = \{e\}.$$

Das bedeutet insbesondere, die $\alpha\in R$ erzeugen ein Gitter in X mit endlichem Index[205]

---

[203] X_α normalisiert G' wegen $X_\alpha \subseteq G'$. T normalisiert G', weil T jedes X_α normalisiert (nach Definition der X_α).

[204] Die Konjugation mit einem Element aus diesem Durchschnitt ist trivial auf jedem X_α (nach Definition der X_α) und ist trivial auf dem maximalen Torus T (weil T kommutativ ist), also trivial auf dem Erzeugnis dieser Gruppen, d.h. auf G.

[205] Wir betrachten die α als Elemente des Koordinatenrings $k[T] = k[T_1,\ldots,T_n]_{T_1\cdot\ldots\cdot T_n}$ (n = Rang von G) von $T \cong D_n$. Die Nullstellen-Menge

(*) $$V(\alpha - 1 \mid \alpha\in R) = \cap\ \mathrm{Ker}(\alpha)$$

ist endlich. Es gibt daher Wurzeln $\alpha_1,\ldots,\alpha_n \in R$ derart, daß

$$\alpha_1 - 1,\ldots,\alpha_n - 1$$

ein reguläres Parametersystem von T im Punkt $e\in T$ bilden (sind $\alpha_1,\ldots,\alpha_i$ bereits gewählt, so gibt es wegen der Endlichkeit von (*) ein α_{i+1} derart, daß $\alpha_{i+1} - 1$ auf der Komponente von $V(\alpha_1-1,\ldots,\alpha_i-1)$ durch e nicht identisch Null ist. Man beachte, eine algebraische Gruppe hat nur eine Komponente durch e). Die algebraische Gruppe

$$[X : <\alpha \mid \alpha \in R>] < \infty.$$

Außerdem wird T von den Bildern der Kowurzeln erzeugt,

$$T =^{206} <\alpha^V(G_m) \mid \alpha \in R>.$$

Es reicht also zu zeigen,

$$\alpha^V(G_m) \subseteq G' \text{ für } \alpha \in R.$$

(wegen 9.3.7(ii)). Dazu wiederum reicht es zu zeigen,

$$\alpha^V(G_m) \subseteq <X_\alpha , X_{-\alpha}>$$

Nach Definition gilt

$$\alpha^V(G_m) \subseteq T \subseteq G_\alpha := Z(Ker(\alpha)^0).$$

Nach 9.3.5(i) ist G_α reduktiv und zusammenhängend und hat nach (9.1.5) den halbeinfachen Rang 1. Nach 8.2.7(iv) ist (G_α, G_α) halbeinfach vom Rang 1, d.h. (G_α, G_α) ist isomorph zu SL_2 oder PSL_2 und insbesondere gilt

---

$$V(\alpha_1 - 1,...,\alpha_n - 1)$$

hat eine 1-Komponente der Dimension 0, ist also selbst 0-dimensional. Nun sind die α_i Potenzprodukte der T_j. Die Dimensionsaussage impliziert deshalb, daß je zwei der α_i teilerfremd sind. Durch geeignete Wahl der Indizierung der α_i können wir also erreichen,

$$\alpha_i = T_i^{\nu_i} \text{ mit } \nu_i \in \mathbb{Z}.$$

Die von den α erzeugte Untergruppe von X hat somit endlichen Index.

[206] Die von der rechten Seite erzeugte Untergruppe T' ist zusammenhängend (nach (6.1)) und diagonalisierbar (weil $\subseteq$ T), also ein Torus. Wäre es ein echter Teiltorus, so gäbe es einen nicht-trivialen Charakter

$$\chi: T \to G_m \text{ mit } T' \subseteq Ker(\chi)$$

(man verpflanze einen nicht-trivialen Charakter von T/T' entlang der natürlichen Abbildung $T \to T/T'$).

Nach Konstruktion gilt für jede Kowurzel α^V, $Im(\alpha^V) \subseteq Ker(\chi)$, d.h. $\chi \circ \alpha^V$ ist identisch 1, d.h.

$$<\chi, \alpha^V> = 0.$$

Mit anderen Worten, die α^V liegen in der durch χ definierten Hyperebene von X^V. Nun läßt sich die Wurzel α interpretieren als Vektor, der orthogonal ist zu der durch α^V definierten Hyperebene von X (wegen $<\alpha, \alpha^V> = 2$). Wenn also die α^V in einer Hyperelbene von X^V liegen, so liegen die α in einer Hyperebene von X. Das steht aber im Widerspruch zur Endlichkeit des Index der von den α erzeugten Untergruppe von X.

$$\dim (G_\alpha, G_\alpha) = 3.$$

Die Kowurzel α^V ist definiert durch die Bedingung

$$s_\alpha(x) = x - \langle x, \alpha^V \rangle \alpha \text{ für } x \in X(T)$$

wobei s_α die Konjugation mit dem nicht-trivialen Element der Weyl-Gruppe von G_α bezeichnet. Sei T_1 ein maximaler Torus von (G_α, G_α), welcher ganz in T liegt. Dann ist α^V auch die Kowurzel der Einschränkung $\alpha|_{T_1}$ von α auf T_1.[207] Insbesondere gilt

$$\alpha^V(G_m) \subseteq T_1 \subseteq (G_\alpha, G_\alpha).$$

Die Untergruppen X_α und $X_{-\alpha}$ erzeugen in der Gruppe (G_α, G_α) einen zusammenhängenden (vgl. 6.1) Normalteiler[208] einer Dimension ≥ 2 (weil der Tangentialraum mindestens 2-dimensional ist), also die ganze Gruppe (da die Gruppe außer den trivialen Normalteilern nur noch endliche Normalteiler besitzt). Es folgt

$$\alpha^V(G_m) \subseteq T_1 \subseteq (G_\alpha, G_\alpha) = \langle X_\alpha , X_{-\alpha} \rangle.$$

3. Schritt. Beweis von (ii).
Für $\alpha \in R$ und $t \in T$ gilt

$$(2) \qquad t x_\alpha(\xi) t^{-1} x_\alpha(-\xi) = x_\alpha((\alpha(t)-1)\xi).$$

Diese Formel zeigt, es gilt

$$X_\alpha \subseteq (G,G).$$

Da nach dem zweiten Schritt die X_α die Gruppe G erzeugen, folgt

$$G = (G,G),$$

d.h. es gilt (ii).
4. Schritt. Beweis von (iii).
Sei $N' \subseteq G$ zusammenhängender abgeschlossener Normalteiler. Wir haben im ersten Schritt bereits gezeigt, daß N' dann halbeinfach ist. Wir charakterisieren als nächstes die Wurzeln $\alpha \in R$, für welche X_α in N' liegt. Sei

$$T' \subseteq N'$$

---

[207] Beim Existenzbeweis für α^V in 8.2.9 wurde α^V zunächst für $\alpha|_{T_1}$ konstruiert und dann gezeigt, es ist auch die Kowurzel von α.
[208] Nach (*) mit (G_α, G_α) anstelle von G.

ein maximaler Torus von G' mit T' $\subseteq$ T. Dann gilt

(3) $\quad X_\alpha \subseteq N' \Leftrightarrow \alpha|_T, \neq 0.$

Beweis von '$\Rightarrow$':

Angenommen $\alpha|_T, = 0$. Nach (2) sind dann die Kommutatoren der Elemente von X_α mit denen von T' trivial, d.h. die Elemente von T' kommutieren mit denen von X_α. Da nach Voraussetzung $X_\alpha \subseteq N'$ gilt, folgt

$$X_\alpha \subseteq Z_{N'}(T').$$

Nach dem ersten Schritt ist aber N' halbeinfach, also reduktiv. Also ist in N' der Zentralisator des maximalen Torus T' gleich T' (nach 9.3.6(ii)), $\quad X_\alpha \subseteq Z_{N'}(T') = T'.$

Das ist aber unmöglich: X_α besteht aus unipotenten Elementen und T' aus halbeinfachen.

Beweis von "$\Leftarrow$".

Wir betrachten (2) mit $t \in T'$ ($\subseteq$ N'). Das Produkt der letzten drei Elemente der linken Seite liegt in N' (weil N' ein Normalteiler ist). Also liegt die linke Seite in N', also gilt

$$x_\alpha((\alpha(t)-1)\xi) \in N' \text{ für alle } t \in T' \text{ und alle } \xi \in k.$$

Da α nach Voraussetzung nicht identisch 1 ist auf T', folgt

$$X_\alpha = \mathrm{Im}(x_\alpha) \subseteq N'.$$

Damit ist (3) bewiesen. Zeigen wir, es gilt sogar

(4) $\quad X_\alpha \subseteq N' \Leftrightarrow \alpha|_T, \neq 0 \Leftrightarrow \alpha|_T,$ ist Wurzel von N'.

Es ist nur noch die letzte Implikation zu beweisen. Die Richtung "$\Leftarrow$" ist trivial (der triviale Charater auf T' kann keine Wurzel sein). Die Richtung "$\Rightarrow$" wird wie folgt bewiesen: ist $\alpha|_T, \neq 0$, so ist nach (3) auch

$$X_\alpha \subseteq N',$$

d.h. X_α ist eine 1-dimensionale zusammenhängende unipotente Untergruppe von N'. Nach Aufgabe 9.3.10(1) gibt es eine Wurzel $\beta \in R(N',T')$ mit

$$X_\alpha = X_\beta$$

Nach Definition von X_α bzw. X_β operiert T' auf dieser Gruppe durch Multiplikation mit den Charakter α bzw. β. Deshalb gilt $\alpha|_T, = \beta$.

Insbesondere ist $\alpha' := \alpha|_T$, eine Wurzel von N'. Damit ist (4) bewiesen.

Wir setzen jetzt

$$R' := \{ \alpha \in R \mid \alpha|_T, \text{ ist Wurzel von } N' \}$$

$$R'' := R - R'.$$

Ist $R' = \emptyset$, so gilt nach (4) und dem zweiten Schritt

$$T' \subseteq (\cap_{\alpha \in R} \operatorname{Ker}(\alpha))^0 = \{e\}.$$

Nach (9.3.9)(iii) ist

$$\dim N' = \dim T' + \# R' = 0, \text{ d.h. } N' = \{e\},$$

d.h. wir können $N'' = G$ setzen.

Ist $R'' = \emptyset$, so gilt $N' = G$ (nach (4) und (i)) und wir können $N'' = \{e\}$ setzen. In beiden Fällen gilt also die Aussage von (iii). Sei jetzt

$$R' \neq \emptyset \text{ und } R'' \neq \emptyset.$$

Wir definieren N'' als die von den X_α mit $\alpha \in R''$ erzeugte Untergruppe,

$$N'' := < X_\alpha \mid \alpha \in R'' >.$$

Dann ist N'' abgeschlossen und zusammenhängend (nach (6.1)). Zeigen wir, es gilt

(5) $$(N', N'') = \{e\}.$$

Sei $\alpha' \in R'$ und $\alpha'' \in R''$. Wir setzen

$$x(\xi) = x_{\alpha''}(\eta) x_{\alpha'}(\xi) x_{\alpha''}(-\eta).$$

Dann gilt $x(\xi) \in N'$ (weil N' Normalteiler ist und $\operatorname{Im}(x_{\alpha''})$ nach (4) in N' liegt) und

$$t x(\xi) t^{-1} = x(\alpha'(t)\xi) \text{ für } t \in T'$$

(weil α'' nach (4) auf T' trivial ist). Nach Aufgabe (9.3.10)(1) gibt es eine Wurzel $\alpha \in R(N', T') \subseteq R(G,T)$ mit

$$x(\xi) = x_\alpha(f(\eta)\xi)$$

mit einem Homomorphismus algebraischer Gruppen[209]

$$f: G_a \to G_m .$$

Da G_a aus unipotenten und G_m aus halbeinfachen Elementen besteht, folgt $f(\eta) = 1$ für alle η, d.h. $x(\xi)$ hängt nicht von η ab. Es folgt

$$x_{\alpha''}(\eta) x_{\alpha'}(\xi) x_{\alpha''}(-\eta) = x_{\alpha'}(\xi),$$

---

[209] Zunächst ist f auf Grund der Übungsaufgabe nur irgendeine Abbildung. Wegen $f(\eta) = x_\alpha^{-1}(x_{\alpha''}(\eta) x_{\alpha'}(\xi) x_{\alpha''}(-\eta))/\xi$ ist f ein Morphismus algebraischer Varietäten und ein Gruppenhomomorphismus, also ein Homormophismus algebraischer Gruppen handeln.

d.h. die Elemente von X_α, kommutieren mit denen von $X_{\alpha"}$. Nun erzeugen die X_α, (wegen (i)) den Normalteiler N' und die $X_{\alpha"}$ erzeugen N" (nach Definition von N"). Also gilt (5). Außerdem erzeugen die X_α, und $X_{\alpha"}$ zusammen die gesamte Gruppe G (nach (i)) und normalisieren N". Deshalb ist N" Normalteiler in G und es gilt

(6) $$N'N" = G.$$

Schließlich ist $(N'\cap N")^0$ ein abgeschlossener zusammenhängender Normalteiler von G und jedes $\alpha\in R$ ist trivial auf einem passend gewählten maximalen Torus, d.h. die Menge der Wurzeln ist leer (vgl. (4)), d.h. die Menge der X_α, die diesen Normalteiler (nach (i)) erzeugen ist leer. Es folgt $(N'\cap N")^0 = \{e\}$, d.h.

(7) $N'\cap N"$ ist endlich.

Mit (5), (6) und (7) ist Aussage (iii) des Satzes bewiesen.

5. Schritt. Beweis von (iv).

Die Endlichkeitsaussage folgt aus (i) und der Tatsache, daß die Menge der Teilmengen von

$$\{ X_\alpha \mid \alpha\in R\}$$

endlich ist. Die übrigen Aussage ergeben sich durch wiederholtes anwenden von (iii) (und der Tatsache, daß der Durchschnitt von zwei minimalen N trivial sein muß.

QED.

9.4.2 Definitionen: Wurzel- und Gewichtsgitter, fundamentale Gruppe eines Wurzeldatums

Sei G eine zusammenhängende halbeinfache Gruppe mit dem Wurzeldatum (X,R,X^V,R^V). Dann heißt die von den Wurzeln $\alpha\in R = R(G,T)$ erzeugte Untergruppe von X Wurzelgitter von R und wird mit

$$Q := Q(R,T) := \{ \sum_i n_i\alpha_i \mid n_i \in\mathbb{Z}, \alpha_i\in R \}$$

bezeichnet. Sei

$$V := Q\otimes_{\mathbb{Z}}\mathbb{R}$$

wie in 9.1.11 Bemerkung (ii). Dann heißt

$$P := P(G,T) := \{v\in V \mid <v, \alpha^V> \in \mathbb{Z} \text{ für } \alpha^V\in R^V\}$$

Gewichtsgitter von R. Nach Definition gilt

$$Q \subseteq X \subseteq P.$$

Die halbeinfache Gruppe G heißt adjungiert im Fall X = Q und einfach zusammenhängend im Fall X = P. Die Gruppe

$$P/Q$$

heißt fundamentale Gruppe von R.

Bemerkungen

(i) Q hat auf Grund des Beweises von 9.4.1 (vgl. 2. Schritt) endlichen Index in X,

$$[X: Q] < \infty.$$

(ii) Die natürliche Einbettung

$$Q \subseteq X$$

einen Isomorphismus $V = Q \otimes_{\mathbb{Z}} \mathbb{R} \xrightarrow{\cong} X \otimes_{\mathbb{Z}} \mathbb{R}$ und die Paarung

$$X \times X^V \to \mathbb{Z}, (x, x^V) \mapsto \langle x, x^V \rangle$$

induziert eine Paarung

$$V \times V^V \to \mathbb{R}, (x, x^V) \mapsto \langle x, x^V \rangle \text{ mit } V^V := X^V \otimes_{\mathbb{Z}} \mathbb{R},$$

welche X^V mit dem zu X dualen Gitter identifiziert, d.h.

$$V^V \to \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R}), x^V \mapsto \langle ?, x^V \rangle,$$

ist bijektiv und das Bild von X^V ist gerade $\mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z})$.

(iii) Durch Einführung eines symmetrischen Skalarproduktes auf V (das invariant gegenüber der Operation der Weyl-Gruppe ist) kann man V^V mit V identifizieren (vgl. 9.1.10). Dabei wird gerade

$$\alpha^V = 2(\alpha,\alpha)^{-1}\alpha.$$

Insbesondere gibt es eine Basis von V über $\mathbb{R}$, die aus Kowurzeln besteht (da dasselbe nach (i) für die Wurzeln gilt). Das bedeutet aber, die von den Kowurzeln erzeugte Untergruppe

$$Q^V := \langle \alpha^V \mid \alpha \in R \rangle$$

hat endlichen Index in X^V,

$$[X^V: Q^V] < \infty.$$

(iv) Als Untergruppe der freien abelschen Gruppe X^V ist Q^V eine freie abelsche Gruppe (nach dem Elementarteilersatz). Seien

$$e_1^V, \ldots, e_n^V \in Q^V \subseteq V^V = \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})$$

eine ($\mathbb{Z}$-linear unabhängige) Basis von Q^V und $e_1, \ldots, e_n \in V$ die duale Basis, d.h.

$$\langle e_i, e_j^V \rangle = \delta_{ij}.$$

Dann gilt $e_i \in P$ für jedes i und jedes $x = m_1 e_1 + \ldots + m_n e_n \in P$ hat ganzzahlige Koordinanten

$$m_j = \langle x, e_j^v \rangle \in \mathbb{Z}$$

bezüglich der e_i. Mit anderen Worten, P ist der von den e_i erzeugte $\mathbb{Z}$-Modul in V, d.h. P ist ein Gitter.

(v) Da, wie wir gerade gesehen haben Q und P Gitter sind und die Inklusionen

$$Q \subseteq X \subseteq P$$

bestehen, gibt es zu gegebenen Wurzelsystem R nur endlich viele Möglichkeiten für X.

9.4.3 Aufgaben

(1) (a) Man definiere den Begriff der direkten Summe zweier Wurzelsysteme.
(b) Ein Wurzelsystem heißt reduzibel, wenn es eine nicht-triviale direkte Summe ist und ansonsten irreduzibel. Man zeige, das Wurzelsystem R einer halbeinfachen zusammenhängenden linearen algebraischen Gruppe G ist genau dann reduzibel, wenn G einen echten zusammenhängenden abgeschlossenen Normalteiler besitzt. Man zeige, die Wurzelsystem der Gruppen N_i von 9.4.1 (iv) sind irreduzibel.

(2) Sei (X,R,X^v,R^v) das Wurzelsystem einer reduktiven Gruppe G und sei

$$X_0 := \{ x \in X \mid \langle x, R^v \rangle = 0 \}.$$

Bezeichne wie bisher Q die von den Wurzeln in X erzeugte Untergruppe.
(a) (G,G) ist genau dann adjungiert, wenn $X = Q \oplus X_0$.
(b) (G,G) ist genau dann einfach zusammenhängend, wenn gilt

$$P \subseteq X + (X_0 \otimes \mathbb{Q}).$$

(3) Man bestimme Wurzelgitter, Gewichtsgitter und fundamentale Gruppe für jedes der Wurzelsysteme A_{n-1}, B_n, C_n, D_n der Aufgaben von 9.3.10.

Lösungen

Zu (3). Das Wurzelsystem A_{n-1}

Nach 9.3.10 (3)(d) ist das Wurzeldatum $A_{n-1} = (X',X'^v,R', R'^v)$ der Gruppe $G' = SL_n$ gegeben durch

$$X' = X/\mathbb{Z}\cdot e,\ e := e_1+\ldots+e_n$$

$$X'^{\vee} = \{ (x_1,...,x_n) \in X^{\vee} \mid x_1+...+x_n = 0 \}$$

$$R' = \pi R,$$

$$R'^{\vee} = R^{\vee}.$$

mit $X = X^{\vee} = \mathbb{Z}^n$ und $R = R^{\vee} = \{ e_i - e_j \mid i \neq j \}$.

Bestimmung des Wurzelgitters.

Wir können X' mit der Untergruppe des reellen Vektorraums

$$V' = \mathbb{R}^n/\mathbb{R}\cdot e = e^{\perp} = \mathbb{R}(e_1-e_2)+...+\mathbb{R}(e_1-e_n)$$

identifizieren, welche von den Restklassen πe_i erzeugt wird. Die Identifikation mit dem orthogonalen Komplement von e geschieht mit Hilfe der natürlichen Abbildung. Dem Erzeuger πe_i von X' entspricht bei dieser Identifikation der Vektor $e_i - \frac{1}{n} e$. Die Charaktergruppe entspricht dabei gerade der von diesen Vektoren erzeugten abelschen Gruppe,

$$X' = < e_1 - \frac{1}{n} e , ... , e_n - \frac{1}{n} e >$$

(diese bilden keine freie Basis).

Für das Wurzelgitter erhalten wir

$$Q' = < e_1-e_2 ,... ,e_1-e_n >,$$

d.h. es ist die freie abelsche Gruppe, die von den angegebenen Differenzen erzeugt wird.

Bestimmung des Wurzelgitters.

Das Gewichtsgitter besteht aus allen

$$v = r_2(e_1-e_2)+...+r_n(e_1-e_n) \in V'$$

mit

$$(v, e_i - e_j) \in \mathbb{Z} \text{ für alle i und alle j.}$$

Für $i = 1 < j = \beta$ erhalten wir

$$\sum_{\alpha=2}^{n} r_\alpha + r_\beta \in \mathbb{Z} \text{ für } \beta = 2,...,n.$$

Für $1 < i = \alpha < \beta = j$ erhalten wir

$$r_\alpha - r_\beta \in \mathbb{Z},$$

$$r_\alpha = r_2 + g_\alpha \text{ mit } g_\alpha \in \mathbb{Z}.$$

Einsetzen liefert

$$v = g_2(e_1-e_2)+...+g_n(e_1-e_n) + r_2 (ne_1 - e).$$

Damit gilt

$$v \in P' \Leftrightarrow r_2 n \langle e_1 - \frac{1}{n}e, e_i - e_j \rangle \in \mathbb{Z} \text{ für alle i und j. .}$$

Das Skalarprodukt rechts ist Null falls i und j beide > 1 sind. Für 1=i<j hat das Skalarprodukt den Wert $1 - \frac{1}{n} + \frac{1}{n} = 1$. Damit gilt

$$v \in P' \Leftrightarrow r_2 \in \frac{1}{n}\mathbb{Z},$$

d.h.

$$P' = Q' + (e_1 - \frac{1}{n}e)\mathbb{Z} \subseteq X'.$$

Die umgekehrt Inklusion gilt stets, d.h. es ist

$$P' = X'.$$

Die Gruppe SL_2 ist insbesondere adjungiert.

Bestimmung der fundamentalen Gruppe.
Die $\mathbb{Z}$-lineare Abbildung

$$\mathbb{Z}^{n-1} \to X', (x_1,...,x_n) \text{ a Restklasse von } (x_1,...,x_n,0),$$

ist ein Gruppen-Isomorphismus[210]. Das Wurzelsystem R' bei diesem Ismorphismus entspricht der Teilmenge

$$\{ e_i - e_j \mid i \neq j \} \subseteq \mathbb{Z}^{n-1} \text{ mit } e_n := - e_1 - e_2 - ... - e_{n-1}.$$

Das Wurzelgitter wird von den Vektoren $e_1 - e_j$ mit j = 2,...,n erzeugt,

$$Q := \langle e_1 - e_2 , ... , e_1 - e_{n-1} , 2e_1 + e_2 + ... + e_{n-1} \rangle$$
$$= \langle e_1 - e_2 , ... , e_1 - e_{n-1}, ne_1 \rangle$$

es hat den Rang n-1 und den Index n in $X' = \mathbb{Z}^{n-1}$, d.h.

$$P'/Q' = X'/Q' \cong \mathbb{Z}/n\mathbb{Z}.$$

9.4.4 Notes

10. Further properties of reductive groups

In diesem Kapitel ist

$$G$$

eine zusammenhängende reduktive lineare algebraische Gruppe,

$$T \subseteq G$$

---

[210] Die Abbildung ist injektiv: wenn $(x_1,...,x_n,0)$ die Nullrestklasse repräsentiert, d.h. eine Vielfaches von e ist, so muß der Koeffizient von e Null sein (weil die letzte Koordinaten Null ist).
Die Abbildung ist surjektiv: die Restklasse von e_n hat $(-1,...,-1) = -e_1 - ... - e_{n-1}$ als Urbild.

ein maximaler Torus von G und

$$B \supseteq T$$

eine Borel-Untergruppe von G. Wir bezeichnen mit

$$R := R(G,T)$$

das Wurzelsystem von G bezüglich T und schreiben

$$R^+ := R^+(B).$$

Der Begriff der positiven Wurzel soll ist stets auf das System R^+ beziehen (vgl. 9.2.3). Die Weyl-Gruppe bezeichnen wir wie bisher mit

$$W := W(G,T) = N_G(T)/Z_G(T) = N_G(T)/T$$

(vgl. 9.3.6(ii)). Für $\alpha \in R$ seien x_α und X_α wie in 9.3.7.

10.1 Borel-Gruppen und Systeme positiver Wurzel

Wir beginnen mit der Untersuchung von Eigenschaften der 1-parametrischen Untergruppen $x_\alpha: G_a \to X_\alpha$, $\alpha \in R$.

10.1.1 Proposition: Erzeuger für Borel-Untergruppen
Seien G eine zusammenhängende reduktive lineare algebraische Gruppe mit der Borel-Untergruppe B und den n positiven Wurzeln $\alpha_1, \ldots, \alpha_n$, d.h.

$$R^+ = \{\alpha_1, \ldots, \alpha_n\}.$$

Dann ist der Morphismus

$$\Phi; G_a^n \to B_u, (\xi_1,\ldots,\xi_n) \mapsto (x_{\alpha_1}(\xi_1), \ldots, x_{\alpha_n}(\xi_n)),$$

ein Isomorphismus algebraischer Varietäten. Insbesondere wird B_u erzeugt von den Untergruppen X_α mit $\alpha > 0$.

Zum **Beweis** benötigen wir die folgende allgemeinere Aussage.

10.1.2 Lemma: Erzeuger für auflösbare Gruppen
Seien H eine zusammenhängende auflösbare lineare algebraische Gruppe, $S \subseteq H$ ein maximaler Torus und

$$U := H_u .$$

Weiter existiere eine endliche Familie

$$x_i: G_a \to X_i , i = 1,\ldots,m,$$

von Isomorphismen mit abgeschlossenen Untergruppen $X_i \subseteq H$, sodaß die folgenden Bedingungen erfüllt sind.
(a) Es gibt paarweise verschiedene Charaktere β_i (i=1,..,m) von S mit

$$sx_i(\xi)s^{-1} = x_i(\beta_i(s)\xi) \text{ für } s\in S \text{ und } \xi\in k.$$

(b) L(U) ist die direkte Summe der Gewichtsräume $L(U)_{\beta_i}$ (i=1,...,m) und diese Gewichtsräume sind sämtlich 1-dimensional.

Dann ist der Morphismus

$$\psi: G_a^m \to U, (\xi_1,...,\xi_m) \mapsto x_{\beta_1}(\xi_1)\cdot \ldots \cdot x_{\beta_m}(\xi_m),$$

ein Isomorphismus algebraischer Varietäten.

Beweis von 10.1.2 durch Induktion nach m.

Der Fall m = 1. Es existiert genau eine Isomorphismus

$$x: G_a \to X \subseteq H$$

mit einer abgeschlossenen Untergruppe. Weil G_a aus unipotenten Elementen besteht, gilt sogar

$$x: G_a \to X \subseteq U$$

Nach (b) induziert x einen Isomorphismus

$$L(G_a) \to L(U).$$

Insbesondere ist dim U = 1 = dim X, d.h. es gilt X = U und Φ = x ist der behauptete Isomorphismus.

Der Fall m > 1. Wir wählen einen Normalteiler

$$N \subseteq U,$$

welcher im Zentrum von U liegt und isomorph ist zu G_a. Ein solcher Normalteiler existiert nach (6.10). Nach (b) ist dann L(N) einer der Gewichtsräume von L(U), sagen wir $L(U)_{\beta_j}$. Die Konjugation mit Elementen des maximalen Torus $S \subseteq H$ auf N entspricht dann beim Isomorphismus

$$N \cong G_a$$

gerade der Multiplikation mit dem Charakter β_j. Insbesondere operiert $Ker(\beta_j)$ trivial auf N,

$$N \subseteq Z_H(Ker(\beta_j)^0) \ (\supseteq \text{Im } x_j).$$

Wir gehen zu den unipotenten Teilen über und erhalten

(1) $$N \subseteq U\cap Z_H(Ker(\beta_j)^0) = Z_U(Ker(\beta_j)^0) \ (\supseteq \text{Im } x_j),$$

Nach 4.4.7 ist

$$L(Z_U(Ker(\beta_j)^0)) = \{ X\in L(U) \mid Ad(s)X = X \text{ für } s\in Ker(\beta_j)^0\} \subseteq L(U)_{\beta_j}.$$

Der Vektorraum rechts ist 1-dimensional nach Voraussetzung. Also gilt sogar das Gleichheitszeichen, d.h. die Gruppe in der Mitte von (1) ist 1-dimensional und auch in (1) gilt überall das Gleichheitszeichen. Insbesondere ist

(2) $$N = \mathrm{Im}\,(x_j)$$

Wir wollen jetzt die Induktionsvoraussetzung auf die Gruppe H/N anwenden. Dazu müssen wir zeigen, die Voraussetzungen des Satzes sind auch für H/N erfüllt. Das ist der Fall, ausgenommen eventuell die Aussage, daß die Zusammensetzungen der Isomorphismen

$$G_a \xrightarrow{x_i} X_i$$

mit der natürlichen Abbildung $H \to H/N$ wieder Isomorphismen sind. Um letzteres zu beweisen, müssen wir zeigen, $X_i \cap N = \{e\}$ für $i \neq j$. Es reicht zu zeigen, je zwei X_i haben nur das Element e gemeinsam. Das folgt aus der Tatsache daß die X_i bezüglich der Operation von S durch Konjugation in die zwei Orbits

$$\{e\} \text{ und } X_i - \{e\}$$

zerfällt. Hätten zwei X_i einen Punkt $x \neq e$ gemeinsam, so hätten sie das gesamte Orbit von x gemeinsam, d.h. die beiden X_i wären gleich. Damit können wir die Induktionvoraussetzung auf H/N anwenden und erhalten, daßdie Abbildung

$$\psi' : G_a^{m-1} \to U/N,\ (\xi_1,\ldots,\hat{\xi}_j,\ldots,\xi_m) \mapsto x_{\beta_1}(\xi_1)\cdot \ldots \cdot \hat{x}_{\beta_j}(\xi_j) \cdot \ldots \cdot x_{\beta_m}(\xi_m),$$

ein Isomorphismus ist. Betrachen wir jetzt die Abbildung

$$\psi : G_a^{m} \to U,\ (\xi_1,\ldots,\xi_m) \mapsto x_{\beta_1}(\xi_1)\cdot \ldots \cdot x_{\beta_m}(\xi_m),$$

<u>Surjektivität von</u> ψ. Die Zusammensetzung mit der natürlichen Abbildung $U \to U/N$ ist surjektiv, weil das Bild der Zusammensetzung das Bild von ψ' enthält. Damit gilt

$$U \subseteq \mathrm{Im}(\psi)\cdot N = \mathrm{Im}(\psi).$$

Das Gleichheitszeichen rechts gilt wegen $N \subseteq \mathrm{Im}(\psi)$.

<u>Injektivität von</u> ψ. Aus $\psi(\xi_1,\ldots,\xi_m) = \psi(\xi'_1,\ldots,\xi'_m)$ folgt

$$\psi(\xi_1,\ldots,\xi_m) \equiv \psi(\xi'_1,\ldots,\xi'_m) \bmod N,$$

also

$$\psi'(\xi_1,\ldots,\hat{\xi}_j,\ldots,\xi_m) = \psi'(\xi'_1,\ldots,\hat{\xi}'_j,\ldots,\xi'_m),$$

also wegen der Injektivität von ψ' sogar

$$\xi_i = \xi'_i \text{ für alle } i \neq j.$$

Aus

$$x_{\beta_1}(\xi_1)\cdot \ldots \cdot x_{\beta_m}(\xi_m) = \psi(\xi_1,\ldots,\xi_m) = \psi(\xi_1,\ldots,\xi'_j,\ldots,\xi_m)$$
$$= x_{\beta_1}(\xi_1)\cdot \ldots \cdot x_{\beta_j}(\xi'_j)\cdot \ldots \cdot x_{\beta_m}(\xi_m)$$

erhalten wir durch Kürzen der äußeren Faktoren

$$x_{\beta_j}(\xi_j) = x_{\beta_j}(\xi'_j)$$

also auch $\xi_j = \xi'_j$.

Damit ist die Bijektivität von ψ bewiesen.

Insbesondere ist

$$\psi: G_a^m \to U$$

ein dominanter Morphismus irreduzibler Varietäten, dessen Fasern sämtlich aus genau einem Punkt bestehen, d.h. es gilt (vgl. 4.1.6)

$$\dim G_a^m = \dim U,$$

d.h. $k[G_a^m]$ ist algebraisch über $k[U]$ und der Separabilitätsgrad ist 1,

$$[k(G_a^m): k(U)]_s = 1.$$

Nach (3.2.20)(i) ist ψ separabel, denn wegen (b) ist das Differential $d\psi_{(0,\ldots,0)}$ bijektiv, also surjektiv. Damit gilt $[k(G_a^m): k(U)] = 1$, d.h. ψ ist ein birationaler Morphismus, d.h. auf einer offenen Mengen induziert ψ einen Isomorphismus.

Nach dem Hauptsatz von Zariki[211] zerfällt ψ in eine Zusammensetzung

$$G_a^m \xrightarrow{f'} U' \xrightarrow{g} U$$

aus einer offenen Einbettung f' und einem endlichen Morphismus g. Wir können annehmen U' ist zusammenhängend. Dann ist f' birational, also auch g. Nun ist U glatt (also ganz abgeschlossen). Der endliche Morphismus muß deshalb ein Isomorphismus sein. Wir erhalten,

---

[211] vgl. J.S. Milne: Etale Cohomology, Theorem 1.8 (Chap 1, §1): Seien X ein quasi-kompaktes Schema und f: Y → X ein separierter quasi-endlicher Morphismus. Dann zerfällt f: $Y \xrightarrow{f'} Y' \xrightarrow{g} X$ in eine offene Einbettung und einen endlichen Morphismus.

$$\psi = f' : G_a^m \to U$$

ist eine offene Einbettung (d.h. ein Isomorphismus von G_a^m mit einer offenen Teilmenge von U). Da ψ surjektiv ist, ist damit ψ sogar ein Isomorphismus.
QED.
Beweis von 10.1.1. Wir haben zu zeigen, unter den Voraussetzungen von 10.1.1 sind die Bedingungen von 10.1.2 erfüllt (mit B anstelle von H).
Offensichtlich ist B zusammenhängend und auflösbar. Als Isomorphismen

$$x_i : G_a \to X_i \ (\subseteq B)$$

verwenden wir die $x_\alpha : G_a \to X_\alpha$ mit $\alpha \in R^+$. Nach Definition der x_α (in 9.3.7) ist dann Bedingung (a) von 10.1.2 erfüllt.

Nach 9.3.8 gilt

$$L(G) = L(G)_0 \oplus (\oplus_{\alpha \in R} L(G)_\alpha)$$

mit $L(G)_0 = L(T)$ und $L(G)_\alpha = L(X_\alpha)$. Nach 9.3.9(i) gilt

$$\alpha \in R^+(B) \Leftrightarrow X_\alpha \subseteq B \ (\Leftrightarrow X_\alpha \subseteq B_u),$$

also

(1) $$\oplus_{\alpha \in R^+} L(X_\alpha) \subseteq L(B_u)$$

Außerdem ist

$$\begin{aligned} \dim B_u &= \dim B - \dim T \\ &= (\dim T + \frac{1}{2} \# R) - \dim T \quad \text{(nach 9.3.9(ii))} \\ &= \#R^+ \end{aligned}$$

In (1) gilt deshalb das Gleichheitszeichen. Wegen $L(X_\alpha) = L(G)_\alpha$ ist damit aber gerade die Forderung (b) von 10.1.2. erfüllt.
QED.

10.1.3 Lemma: die Konstanten $c_{n,\alpha}$

Seien G eine zusammenhängende reduktive lineare algebraische Gruppe mit dem maximalen Torus $T \subseteq G$ und $n \in N_G(T)$ ein Element. Wir setzen

$$w := nT \in W :=^{212} W(G,T).$$

Dann gibt es Konstanten $c_{n,\alpha} \in k^*$ mit

$$nx_\alpha(\xi)n^{-1} = x_{w\cdot\alpha}(c_{n,\alpha}\xi) \text{ für alle } \xi \in k.$$

Beweis. Nach 9.3.7 (i) sind die Untergruppen $X_\alpha = \text{im } x_\alpha$ durch die folgende Bedingung definiert.

(1) $tx_\alpha(\xi)t^{-1} = x_\alpha(\alpha(t)\xi)$ für $t \in T$ und $\xi \in k$

und nach 9.1.6 ist die Operation der Weyl-Gruppe auf dem Charakter α wie folgt definiert.

$$(w\cdot\alpha)(t) := \alpha(n^{-1}\cdot t\cdot n) \text{ für } t \in T.$$

Damit gilt für $\xi \in k$ und $t \in T$:

$$\begin{aligned} ntn^{-1}\, x_{w\alpha}(\xi)nt^{-1}n^{-1} &= (ntn^{-1})x_{w\alpha}(\xi)(ntn^{-1})^{-1} \\ &= x_{w\alpha}((w\alpha)(ntn^{-1})\xi) \\ &= x_{w\alpha}(\alpha(t)\xi) \end{aligned}$$

also

$$tn^{-1}\, x_{w\alpha}(\xi)nt^{-1} = n^{-1}x_{w\alpha}(\alpha(t)\xi)n$$

Vergleich mit (1) zeigt, die Abbildung

$$G_a \to n^{-1}X_{w\alpha}n,\ \xi \mapsto n^{-1}\, x_{w\alpha}(\xi)n,$$

genügt der definierenden Bedingung für X_α. Sie unterscheidet sich also nur um einen Isomorphismus von x_α,

$$n^{-1}\, x_{w\alpha}(\varphi(\xi))n = x_\alpha(\xi)$$

mit einem Automorphismus $\varphi: G_a \to G_a$. Ein solcher Automorphismus besteht aber gerade in der Multiplikation[213] mit einem $c \in k$, d.h.

$$x_{w\alpha}(c\xi) = nx_\alpha(\xi)n^{-1}$$

Das ist aber gerade die Behauptung.

QED.

10.1.4 Proposition: die Kommutatoren der x_α

---

[212] Nach 9.3.6(ii) gilt $Z_G(T) = T$ (wenn G reduktiv ist).

[213] Wegen $k[G_a] = k[T]$ ist der Automorphismus durch ein Polynom f(T) gegeben. Weil es sich um einen umkehrbaren Morphismus handelt, ist das Polynom linear. Weil es sich um einen Gruppenhomomorphismus handelt, ist es additiv.

Sei G eine zusammenhängende reduktive lineare algebraische Gruppe. Dann gibt es Konstanten $c_{\alpha,\beta,i,j} \in k$ mit der Eigenschaft, daß für je zwei Wurzeln $\alpha,\beta \in R$ mit $\alpha \neq \pm\beta$ gilt

$$(x_\alpha(\xi), x_\beta(\eta)) = \prod_{i\alpha+j\beta \in R, i,j>0} x_{i\alpha+j\beta}(c_{\alpha,\beta,i,j}\xi^i\eta^j)$$

Das Produkt rechts ist über alle Linearkombinationen[214] von α und β zu erstrecken, die wieder in R liegen, wobei eine beliebige Reihenfolge der Faktoren vorgegeben werden kann.

Beweis. Nach 9.2.4 können wir auf α und β ein Element der Weyl-Gruppe anwenden und so erreichen, daß gilt

$$\alpha > 0 \text{ und } \beta > 0.$$

Nach Lemma 10.1.3 reicht es, die Behauptung für den Spezialfall, daß beide Wurzeln positiv sind, zu beweisen. Nach 9.3.9 gilt dann

$$X_\alpha, X_\beta \subseteq B.$$

Nach 10.1.1 wird B_u von den X_γ mit $\gamma \in R^+$ erzeugt, d.h.

$$(x_\alpha(\xi), x_\beta(\eta)) = \prod_{\gamma \in R^+} x_\gamma(P_\gamma(\xi,\eta))$$

mit eindeutig bestimmten Elementen $P_\gamma(\xi,\eta) \in k$. Wegen der Isomorphie-Aussage von 10.1.1 sind die P_γ reguläre Funktionen in ξ und η, d.h. es sind Polynome $P_\gamma \in k[T',T'']$. Die Reihenfolge der Faktoren im obigen Produkt kann dabei vorgegeben werden. Wir konjugieren die obige Identität mit $t \in T$, vergleichen einander entsprechende Argumente rechts und erhalten:

$$P_\gamma(\alpha(t)\xi,\beta(t)\eta) = \gamma(t)\, P_\gamma(\xi,\eta) \text{ für alle } \xi,\eta \in k \text{ und alle } t \in T.$$

Wir schreiben P_γ in der Gestalt $P_\gamma(T',T'') = \sum_{i,j\geq 0} c_{ij}\, T'^i T''^j$. Die Identität nimmt dann die folgende Gestalt an.

$$\gamma(t) \sum_{i,j\geq 0} c_{ij}\, \xi^i\eta^j = \sum_{i,j\geq 0} c_{ij}\, \alpha(t)^i\beta(t)^j\, \xi^i\eta^j.$$

Auf Grund der linearen Unabhängigkeit der Charaktere können auf der linken Seite nur solche Charaktere γ auftreten, die auch auf der rechten Seite zu finden sind, d.h. nur Charaktere der Gestalt $i\alpha+j\beta$. Wegen $\alpha \neq \pm\beta$ sind die Wurzeln α und β in X linear unabhängig (vgl.

---

[214] mit positiven ganzen Koeffizienten

9.1.12). Eine Wurzel der Gestalt $i\alpha+j\beta$ tritt deshalb rechts höchstens einmal auf. Zum Abschluß des Beweises reicht es zu zeigen, daß für alle Wurzeln der Gestalt

$$\gamma = i\alpha+j\beta$$

die rechts wirklich auftreten, die Koeffizienten i und j beide von Null verschieden sein müssen, d.h.

$$i > 0 \text{ und } j > 0.$$

Angenommen, wir hätten eine Formel der behaupteten Art,

$$(1) \qquad (x_\alpha(\xi),\, x_\beta(\eta)) = \prod_{i\alpha+j\beta\in R,\, i,j\geq 0} x_{i\alpha+j\beta}(c_{\alpha,\beta,i,j}\xi^i\eta^j)$$

wobei rechts tatsächlich ein Glied mit $j = 0$ auftritt. Es kann nur ein solches Glied geben, denn der zugehörige Koeffizient i muß gleich 1 sein (nach 9.1.12). Die Formel hat somit die Gestalt

$$(x_\alpha(\xi),\, x_\beta(\eta)) = x_\alpha(c\xi) \prod_{i\alpha+j\beta\in R,\, i\geq 0,\, j>0} x_{i\alpha+j\beta}(c_{\alpha,\beta,i,j}\xi^i\eta^j)$$

mit $c\neq 0$. Doch dann würde eine ähnliche Formel für alle iterierten Kommutatoren gelten[215]:

---

[215] Seien $\alpha_1,\ldots,\alpha_r$ alle positiven Wurzeln der Gestalt $i\alpha+j\beta$ mit $i\geq 0$ und $j\geq 0$ (bzw. $i>0$ und $j>0$). Wir setzen

$$H := (\text{bzw. } H' :=) \prod_{i=1}^{r} X_{\alpha_i}$$

Es reicht zu zeigen:

1. H (bzw. H') ist eine Untergruppe in $U := B_u$
2. H' ist ein Normalteiler in H.

Denn dann kann man die obige Identität in der folgenden Gestalt schreiben:

$$(x_\alpha(\xi),\, x_\beta(\eta)) \equiv x_\alpha(c\xi) \bmod H'$$

(als Identität in H). Für die iterierten Normalteiler hat man dann eine analoge Identität.

Zu 1. Nach 10.1.1 wird $U = B_u$ von den X_γ mit $\gamma\in R^+$ erzeugt, d.h. es gilt

$$\prod_{i=1}^{r} x_{\alpha_i}(\xi_i)\cdot\prod_{i=1}^{r} x_{\alpha_i}(\eta_i) = \prod_{\gamma\in R^+} x_\gamma(P_\gamma(\xi,\eta))$$

mit eindeutig bestimmten Polynomen

$$P_\gamma(\xi,\eta) = \sum_{\mu,\nu\geq 0} c_{\mu\nu}\xi^\mu\eta^\nu$$

mit Koeffizienten aus k (Multi-Index-Schreibweise) Wir konjugieren das obige Produkt mit $t\in T$ und erhalten

$$\gamma(t) \sum_{\mu,\nu\geq 0} c_{\mu\nu}\xi^\mu\eta^\nu = \sum_{\mu,\nu\geq 0} c_{\mu\nu}\,\alpha(t)^{\mu+\nu}\,\xi^\mu\eta^\nu$$

$$((x_\alpha(\xi), x_\beta(\eta))..., x_\beta(\eta)) = x_\alpha(d\xi) \prod_{i\alpha+j\beta\in R, i\geq 0, j>0} x_{i\alpha+j\beta}(d_{\alpha,\beta,i,j}\xi^i\eta^j)$$

mit $d \neq 0$. Insbesondere ist der Ausdruck rechts stets ungleich e. Das widerspricht jedoch der Tatsache, daß der unipotente Teil B_u der Borel-Untergruppe B nilpotent ist.
QED.

10.1.5 Theorem: Transitivität der Operation von W auf den positiven Wurzelsystemen

Seien G eine zusammenhängende reduktive lineare algebraische Gruppe mit dem maximalen Torus T, der Borel-Untergruppe $B \in \mathbf{B}_T$, dem Wurzelsystem R = R(G,T) und der Weyl-Grupep W = W(G,T). Weiter sei $\tilde{R}^+$ irgendein System positiver Wurzeln in R. Dann gilt:

Wegen der lineare Unabhängigkeit der Charaktere können links nur Charaktere auftreten, die auch rechts auftreten, d.h. nur solche γ mit $\gamma(t) = \alpha(t)^{\mu+\nu}$ treten wirklich auf. Diese sind aber Wurzeln der Gestalt α_i. Damit nimmt die obige Formel die folgende Gestalt an:

$$\prod_{i=1}^{r} x_{\alpha_i}(\xi_i)\cdot\prod_{i=1}^{r} x_{\alpha_i}(\eta_i) = \prod_{i=1}^{r} x_{\alpha_i}(P_{\alpha_i}(\xi,\eta))$$

Da die rechte Seite in H (bzw. H') liegt, ist somit H (bzw. H') eine Untergruppe von U.

Zu 1. Nach 10.1.1 wird $U = B_u$ von den X_γ mit $\gamma\in R^+$ erzeugt, d.h. es gilt

$$x_{\alpha_j}(\eta)\cdot\prod_{i=1}^{r} x_{\alpha_i}(\xi_i)\cdot x_{\alpha_j}(-\eta) = \prod_{\gamma\in R^+} x_\gamma(P_\gamma(\xi,\eta))$$

mit eindeutig bestimmten Polynomen

$$P_\gamma(\xi,\eta) = \sum_{\mu,\nu\geq 0} c_{\mu\nu}\xi^\mu\eta^\nu$$

mit Koeffizienten aus k (Multi-Index-Schreibweise bezüglich ξ) Wir konjugieren das obige Produkt mit $t\in T$ und erhalten

$$\gamma(t)\sum_{\mu,\nu\geq 0} c_{\mu\nu}\xi^\mu\eta^\nu = \sum_{\mu,\nu\geq 0} c_{\mu\nu}\,\alpha(t)^{\mu+\nu}\,\xi^\mu\eta^\nu$$

Wegen der linearen Unabhängigkeit der Charaktere können links nur Charaktere auftreten, die auch rechts auftreten, d.h. nur solche γ mit $\gamma(t) = \alpha(t)^{\mu+\nu}$ treten wirklich auf. Diese sind aber Wurzeln der Gestalt α_i. Damit nimmt die obige Formel die folgende Gestalt an:

$$x_{\alpha_j}(\eta)\cdot\prod_{i=1}^{r} x_{\alpha_i}(\xi_i)\cdot x_{\alpha_j}(-\eta) = \prod_{i=1}^{r} x_{\alpha_i}(P_{\alpha_i}(\xi,\eta))$$

Falls links das Produkt in der Mitte in H' liegt, so gilt dies auch für das Produkt rechts, d.h. es gilt
Da die rechte Seite in H (bzw. H') liegt, ist somit.

$$x_{i\alpha+j\beta}(\eta)\cdot H'\cdot x_{i\alpha+j\beta}(-\eta) \subseteq H'$$

für alle positiven Wurzeln $i\alpha+j\beta$ mit $i,j\geq 0$. Da die zugehörigen $x_{i\alpha+j\beta}(\xi)$ die Gruppe H erzeugen, ist damit H' Normalteiler in H.

(i) T und die X_α mit $\alpha \in \tilde{R}^+$ erzeugen eine Borel-Untergruppe $\tilde{B}$ von G mit $R^+(\tilde{B}) = \tilde{R}^+$.

(ii) Es gibt genau ein $w \in W = W(G,T)$ mit $\tilde{R}^+ = w \cdot R^+(B)$.

Beweis. Zu (i). Wir setzen

$$\tilde{R}_n^+ := \{\alpha \in \tilde{R}^+ \mid \begin{matrix}\alpha \text{ kann als Summe von n oder mehr} \\ \text{Elementen aus } \tilde{R}^+ \text{ geschrieben werden}\end{matrix}\}$$

Für große n ist $\tilde{R}_n^+$ leer[216], für n = 1 gilt $\tilde{R}_n^+ = \tilde{R}^+$. Weiter sei

$$U_n := \langle X_\alpha \mid \alpha \in \tilde{R}_n^+ \rangle$$

die von den X_α mit $\alpha \in \tilde{R}_n^+$ erzeugte Untergruppe von G. Es reicht die folgende Aussage zu beweisen.

Behauptung:

(1) U_n ist eine abgeschlossene zusammenhängende unipotente Untergruppe von G der Dimension

$$\dim U_n = \# \tilde{R}_n^+,$$

---

[216] Sei $\tilde{R}^+ = \{\alpha_1, \ldots, \alpha_r\}$. Nach Definition gilt $\tilde{R}_n^+ \supseteq \tilde{R}_{n+1}^+$. Angenommen, keines der $\tilde{R}_n^+$ ist leer. Dann ist auch

$$\cap_{n=1}^{\infty} \tilde{R}_n^+$$

nicht leer (denn sonst gäbe es für jedes α ein $\tilde{R}_n^+$, in welchem α nicht liegt). Es gibt also ein α welches in allen $\tilde{R}_n^+$ liegt. Sei

$$\alpha = n_1\alpha_1 + \ldots + n_r\alpha_r \text{ mit } n_i \geq 0 \text{ und } \sum_{i=1}^{r} n_i = n.$$

Wir teilen durch n. Da dann die Koeffizienten rechts im Intervall [0,1] liegen, können wir durch Übergang zu einer Teilfolge Konvergenz erreichen. Durch Grenzübergang erhalten wir, daß eine Linearkombination der α_i mit Koeffizienten ≥ 0 gleich Null ist. Die Linearkombination ist nicht-trivial (da die Summe der Koeffizienten gleich 1 ist). Durch Weglassen gewisser Sumanden erreichen wir, daß alle Koeffizienten > 0 sind. Da die α_i über $\mathbb{Z}$ definiert sind, wird der Raum der Relationen zwischen den α_i von Vektoren aus $\mathbb{Q}^r$ erzeugt. Eine Linearkombination der Relationen hat lauter positive Koordinaten. Also gibt es auch eine Relation der α_i mit positiven rationalen Koordinaten und damit eine mit positiven ganzen Koordinaten. Das widerspricht aber der Positivität der α_i.

die von T normalisiert.

Für n = 1 ergibt sich dann nämlich dim $U_1 = \# \tilde{R}^+ = \frac{1}{2} \#R$. Die von U_1 und T erzeugte Untergruppe hat wegen der Normalisierungseigenschat der U_n die Gestalt

$$\tilde{B} = T \cdot U_1 .$$

Sie ist auflösbar und zusammenhängend und die Multiplikationsabbildung

$$T \times U_1 \to \tilde{B}$$

ist ein bijektiver [217]Morphismus. Damit ist aber

$$\dim \tilde{B} = \dim T + \frac{1}{2} \#R.$$

Nach 9.3.9(ii) ist dies die Dimension einer Borel-Untergruppe, d.h. die von T und den X_α mit $\alpha \in \tilde{R}^+$ erzeugte Untergruppe $\tilde{B}$ ist eine Borel-Untergruppe. Außerdem gilt nach (9.3.9)(i)

$$\alpha \in R^+(\tilde{B}) \Leftrightarrow X_\alpha \subseteq \tilde{B} \; (\Leftarrow \alpha \in \tilde{R}^+)$$

d.h. $\tilde{R}^+ \subseteq R^+(\tilde{B})$, also $\tilde{R}^+ = R^+(\tilde{B})$. Damit ist der Beweis von (i) auf den Beweis der obigen Behauptung zurückgeführt.

Wir beweisen (1) durch absteigende Induktion nach n. Für große n ist $\tilde{R}_n^+$ leer, $U_n = \{e\}$ und die Behauptung trivial. Sei jetzt

$$1 \leq n_0$$

und (1) für alle $n > n_0$ bereits bewiesen. Die Gruppe U_{n_0} wird von T normalisiert, da dies für die erzeugenden Gruppen X_α gilt (nach Definition der X_α).

Es reicht also, die Unipotenz und die Dimensionsaussage zu beweisen. Dazu benutzen wir die Formel von 10.1.4: für je zwei Wurzeln $\alpha, \beta \in R$ gilt

---

[217] Surjektiv ist sie nach Definition von $\tilde{B}$, injektiv, weil aus $t \cdot b = t' \cdot b'$ folgt $t'^{-1} t = b' \cdot b^{-1}$ und e das einzige Element ist, welches gleichzeitig halbeinfach und unipotent ist.

(2) $$(x_\alpha(\xi),\, x_\beta(\eta)) = \prod_{i\alpha+j\beta\in R,\, i,j>0} x_{i\alpha+j\beta}(c_{\alpha,\beta,i,j}\,\xi^i\eta^j)$$

Im Fall $\alpha\in\tilde{R}^+_{n_0}$ und $\beta\in\tilde{R}^+_{n_0+1}$ liegen die Wurzel $i\alpha+j\beta$ wegen

$$i\cdot n_0 + j(n_0+1) \geq 2n_0+1 \geq n_0+1$$

in $\tilde{R}^+_{n_0+1}$ und das Produkt rechts ist ein Element von U_{n_0+1}:

$$x_\alpha(\xi)x_\beta(\eta)\, x_\alpha(\xi)^{-1} \in U_{n_0+1}\; x_\beta(\eta) \subseteq U_{n_0+1}$$

für beliebige $\alpha\in\tilde{R}^+_{n_0}$ und $\beta\in\tilde{R}^+_{n_0+1}$. Da die $x_\alpha(\xi)$ mit $\alpha\in\tilde{R}^+_{n_0}$ die Gruppe U_{n_0} und die $x_\beta(\eta)$ mit $\beta\in\tilde{R}^+_{n_0+1}$ die Gruppe U_{n_0+1} erzeugen, ist

(3) $$U_{n_0+1} \text{ Normalteiler in } U_{n_0}$$

Betrachten wir jetzt (2) für den Fall zweier verschiedener (also linear unabhängiger) Wurzeln $\alpha,\beta \in\tilde{R}^+_{n_0}$. Die Wurzeln der Gestalt $i\alpha+j\beta$ auf der rechten Seite liegen dann wegen

$$i\cdot n_0 + jn_0 \geq 2n_0 \geq n_0 + 1$$

ebenfalls mindestens in $\tilde{R}^+_{n_0+1}$, d.h. der Kommutator

$$x_\alpha(\xi)x_\beta(\eta)\, x_\alpha(\xi)^{-1}x_\beta(\eta)^{-1}$$

liegt in U_{n_0+1}. Mit anderen Worten, die Elemente von X_α und X_β kommutieren modulo U_{n_0+1} und die Faktorgruppe U_{n_0} / U_{n_0+1} besitzt ein Erzeugendensystem aus paarweise kommutierenden Elementen. Insbesondere ist

(4) $$U_{n_0} / U_{n_0+1} \text{ kommutativ}$$

und die Abbildung

(5) $$\times_{\alpha\in\tilde{R}^+_{n_o}-\tilde{R}^+_{n_0+1}} X_\alpha \to U_{n_0} / U_{n_0+1}\,,\ (a_\alpha) \mapsto \prod_\alpha a_\alpha \bmod U_{n_0+1},$$

ist ein surjektiver Homomorphismus algebraischer Gruppen. Aus der Surjektivität der letzten Abbildung folgt

$$\dim U_{n_0} \leq \dim U_{n_0+1} + \#(\tilde{R}^+_{n_0} - \tilde{R}^+_{n_0+1})$$

also nach Induktionsvoraussetzung

$$\dim U_{n_0} \leq \#\tilde{R}^+_{n_0} \tag{6}$$

Aus (4) und der Unipotenz von U_{n_0+1} folgt, daß U_{n_0} auflösbar ist,

$$U_{n_0} = S\cdot(U_{n_0})_u$$

mit einem maximalen Torus $S \subseteq U_{n_0}$. Die natürliche Abbildung induziert eine Abbildung

$$S \to U_{n_0} / U_{n_0+1}.$$

Diese ist injektiv, weil U_{n_0+1} nach Induktionsvoraussetzung unipotent ist. Das Bild dieser Abbildung ist trivial, weil S aus halbeinfachen Elementen besteht und das Bild wegen[218] (5) und (4) aus unipotenten Elementen. Damit ist S trivial, d.h.

$$U_{n_0} \text{ ist unipotent.}$$

Wir haben nocht zu zeigen, in (6) gilt das Gleichheitszeichen. Nach Konstruktion gilt

$$L(X_\alpha) \subseteq L(U_{n_0}) \text{ für } \alpha\in\tilde{R}^+_{n_0}.$$

Die Summe der $L(X_\alpha)$ mit $\alpha\in\tilde{R}^+_{n_0}$ ($\subseteq \tilde{R}^+$) ist aber direkt, da diese in Gewichtsräumen zu unterschiedlichen Gewichten liegen: $L(X_\alpha)\subseteq L(G)_\alpha$ (vgl. 9.3.8). Also gilt in (6) auch "≥".

Zu (ii). Folgt aus (i) und der Transitivität der Operation der Weyl-Gruppe auf den Borel-Untergruppen von $\mathbf{B}_T$ (vgl. 8.1,7(ii)): durch ein Element $w\in W$ können wir B ind $\tilde{B}$ überführen, und damit $R^+ = R^+(B)$ in $\tilde{R}^+ = R^+(\tilde{B})$.

QED.

---

[218] Produkte kommutierender unipotenter Matrizen sind unipotent, da man sie simultan in die oberen Dreiecksmatrizen konjugieren kann (nach Lemma 2.4.2).

10.1.6 Folgerung

Seien G eine zusammenhängende reduktive lineare algebraische Gruppe mit dem maximalen Torus T, der Borel-Untergruppe $B \in \mathbf{B}_T$, dem Wurzelsystem R = R(G,T) und der Weyl-Grupep W = W(G,T).

Wie in 9.1.10 fixieren wir eine positiv definite symmetrische Bilinearform

$$(,) X_{\mathbb{R}} \times X_{\mathbb{R}} \to \mathbb{R}$$

welche W-invariant ist.

Weiter sei $\tilde{R}^+$ irgendein System positiver Wurzeln in R. Dann gibt es ein $x \in X_{\mathbb{R}}$ mit

$$\tilde{R}^+ = \{\alpha \in R \mid (x, \alpha) > 0\}.$$

Wir können für x einen beliebigen Vektor aus $X_{\mathbb{R}}$ mit $(x, \alpha) > 0$ für jedes $\alpha \in \tilde{R}^+$ wählen.

Beweis. Die Aussage ist richtig für das positive Wurzelsystem

$$R^+ = R^+(B)$$

(vgl. Beweis von 9.3.2). Der erste Teil der Behauptung ergibt sich damit aus der Transitivität der Operation der Weyl-Gruppe auf den positiven Wurzelsystemen (vgl. 9.1.5(ii)). Der zweite Teil der Behauptung folgt wegen

$$R = \tilde{R}^+ \cup -\tilde{R}^+$$

(nach Definition des Begriffs System positiver Wurzeln).

QED.

10.1.7 Benachbarte Borel-Untergruppen

Seien G eine zusammenhängende reduktive lineare algebraische Gruppe mit dem maximalen Torus T. Zwei der Borel-Untergruppen B' und B" von G, die den Torus T enthalten,

$$B', B'' \in \mathbf{B}_T,$$

heißen <u>benachbart</u> (<u>adjacent</u>), wenn gilt

$$\dim B' \cap B'' = \dim B' - 1 = \dim B'' - 1.$$

Bemerkung

Sind $\alpha_1, \ldots, \alpha_{r-1}$ die Wurzeln von G mit $X_\alpha \subseteq B' \cap B''$, so gilt

$$R^+(B') = \{\alpha, \alpha_1, \ldots, \alpha_{r-1}\}$$

$$R^+(B'') = \{-\alpha, \alpha_1, \ldots, \alpha_{r-1}\}$$

Dabei ist α die eindeutig bestimmte Wurzel von G, welche nicht positiv bezüglich beider Borel-Untergruppen ist.

10.1.8 Verbindung von Borel-Untergruppen durch Ketten benachbarter

Seien G eine zusammenhängende reduktive lineare algebraische Gruppe mit dem maximalen Torus T und B' und B" Borel-Untergruppen von G, die den Torus T enthalten,

$$B', B'' \in \mathbf{B}_T ,$$

Dann gibt es eine Kette von Borel-Untergruppen

$$B_0 , \dots , B_h \in \mathbf{B}_T$$

mit folgenden Eigenschaften.

1. $B' = B_0$.
2. B_i und B_{i+1} sind benachbart für $i = 0,\dots,h-1$.
3. $B_h = B''$.

Beweis. Wir können annehmen,

$$B' \neq B''.$$

Wie in 9.1.10 fixieren wir eine positiv definite symmetrische Bilinearform

$$(,) X_{\mathbb{R}} \times X_{\mathbb{R}} \to \mathbb{R}$$

welche W-invariant ist. Nach 10.1.6 gibt es Vektoren $x', x'' \in X_{\mathbb{R}}$ mit

$$R'^{+} := R^{+}(B') = \{\alpha \in R \mid (\chi , x') > 0 \}$$

$$R''^{+} := R^{+}(B'') = \{\alpha \in R \mid (\chi , x'' > 0 \}$$

Dabei bilden die x', x" mit diesen Eigenschaften eine offene Teilmenge des reellen Vektorraums $X_{\mathbb{R}}$. Indem wir x' und x" geeignet abändern, erreichen wir, daß gilt[219]

$$(\alpha, x')^{-1}(\beta, x') \neq (\alpha, x'')^{-1}(\beta, x'') \text{ für je zwei } \alpha, \beta \in R \text{ mit } \alpha \neq \pm\beta.$$

Betrachten wir jetzt die Strecke, welche x' und x" verbindet:

$$x(t) := (1-t)x' + tx'', \quad 0 \leq t \leq 1.$$

Das Skalarprodukt $\langle x(t), \alpha \rangle$ kann als Funktion von t nicht für alle α ein konstantes Vorzeichen haben, denn dann wäre $R'^{+} = R''^{+}$, also B'=B". Falls das Skalarprodukt für ein α das Vorzeichen wechselt, so gibt es ein t mit

(1) $$0 = (x(t), \alpha) = (1-t)\langle x', \alpha \rangle + t\langle x'', \alpha \rangle$$

d.h. $\langle x', \alpha \rangle$ entgegengesetztes Vorzeichen,

---

[219] Die Menge $V(\alpha,\beta) := \{ (x', x'') \in X_{\mathbb{R}} \times X_{\mathbb{R}} \mid (\alpha,x')(\alpha,x'') = (\beta,x')(\beta,x'')\}$ ist eine Hyperfläche von $X_{\mathbb{R}} \times X_{\mathbb{R}}$. Man muß also (x',x") lediglich aus dem Komplement von endlich vielen Hyperflächen wählen.

$$\langle x', \alpha\rangle - \langle x'', \alpha\rangle \neq 0$$

und

$$t = t_\alpha = (\langle x', \alpha\rangle - \langle x'', \alpha\rangle)^{-1}\langle x', \alpha\rangle$$

Wegen (1) gilt $t_\alpha \neq t_\beta$ für $\alpha \neq \pm\beta$, d.h. die Vorzeichenwechsel der Funktionen $(x(t), \alpha)$ finden an verschiedenen Stellen statt (für nicht-proportionale α). Es gibt also Zahlen t_i (aus der Menge der t_α) mit

$$0 = t_0 < t_1 < \ldots < t_h = 1$$

mit

1. Alle Funktionen $(x(t), \alpha)$ haben konstantes Vorzeichen auf jedem der Intervalle $I_i = (t_i , t_{i+1})$.
2. Die Vorzeichen der Funktionen $(x(t),\alpha)$ auf I_i und auf I_{i+1} unterscheidet sich für genau ein $\alpha \in R'^{+}$.

Wir setzen

$$R_i^+ := \{\alpha \in R \mid (x(t), \alpha) > 0 \text{ auf } I_i\}$$

und sei

$$B_i \in \mathbf{B}_T$$

die Borel-Untergruppe mit

$$R^+(B_i) = R_i^+$$

(vgl. 10.1.5). Dann entsteht R_{i+1}^+ aus R_i^+ indem man genau eine Wurzel durch ihr Negatives ersetzt, d.h. B_{i+1} entsteht aus B_i , indem man eine der erzeugenden Untergruppen X_α durch $X_{-\alpha}$ ersetzt. Dann wir aber B_i modulo $B_i \cap B_{i+1}$ von nur einem X_α erzeugt, d.h.

$$\dim B_i/B_i \cap B_{i+1} \leq 1,$$

Die umgekehrte Ungleichung ist trivial, weil B_i verschieden sind B_{i+1} und B_i zusammenhängend ist. Also sind B_{i+1} und B_i benachbart.

QED.

10.1.9 Lemma

Seien G eine reduktive lineare algebraische Gruppe, $T \subseteq G$ ein maximaler Torus und

$$B', B'' \in \mathbf{B}_T$$

zwei benachbarte Borel-Untergruppen. Dann gibt es genau eine Wurzel $\alpha \in R^+(B')$ mit

$$B'' = s_\alpha B'.$$

Dabei bezeichen $s_\alpha \in W(G,T)$ wie bisher die zu α gehörige Spiegelung.

Bemerkungen

(i) Die Wurzel α ist die eindeutig bestimmte Wurzel mit

$$\alpha \in R^+(B') \text{ und } -\alpha \in R^+(B'')$$

(ii) Die von B' und B" erzeugte parabolische Untergruppe P ist vom halbeinfachen Rang 1, hat α und $-\alpha$ als einzige Wurzeln und für

$$\overline{P} = P/R_u G$$

gilt

$$G_\alpha(\overline{P}) = \overline{P},$$

Beweis. Es gilt

$$(B' \cap B'')^0 = T \cdot (B'_u \cap B''_u)^0$$

und

(1) $(B'_u \cap B''_u)^0$ hat die Kodimension 1 in B'_u und B''_u

und ist deshalb ein Normalteiler in diesen beiden Gruppen (nach Aufgabe 6.6(3)[220]). Sei

$$P = \langle B', B'' \rangle$$

die von B' und B" erzeugte parabolische Untergruppe. Weil $(B'_u \cap B''_u)^0$ ein Normalteiler in B'_u und B''_u ist, gilt dasselbe auch für P:

(2) $(B'_u \cap B''_u)^0$ ist Normalteiler in P.[221]

Beweis-Idee: Wir zeigen P ist eine der Gruppen G_α mit einer Wurzel α, und es gilt $B'' = s_\alpha B'$.

Nach Konstruktion von P liegen B' und B" ganz in P, sind also Borel-Untergruppen von P. Betrachten wir die Borel-Untergruppen[222]

---

[220] Let G be a connected nilpotent linear algebraic group and $H \subseteq G$ a proper connected closed subgroup. Show that

$$\dim H < \dim N_G H,$$

where $N_G H$ denotes the normaliser. In particular, if dim H = dim G - 1, then H is a normal subgroup (Hint: use 6.5 (ii)).

[221] P wird erzeugt von B'_u, B''_u und T. Wie gerade gezeigt, ist $(B' \cap B'')^0$ invariant gegenüber Konjugation mit Elementen aus B'_u und B''_u. Konjugation mit Elementen aus T läßt aber B' und B" ($\in \mathbf{B}_T$) invariant, also auch $(B' \cap B'')^0$.

$$\overline{B}' := B'/R_u(P),\ \overline{B}'' := B''/R_u(P)$$

der reduktiven Gruppe

$$\overline{P} := P/R_u(P).$$

Nach 9.3.9(ii) gilt

$$\dim \overline{B}' = \dim T + \frac{1}{2}\ \#\, R(\overline{P},T)$$

Andererseits besteht wegen (2) die Inklusion $(B'_u \cap B''_u)^0 \subseteq R_u(P)$, d.h. es gilt

$$\dim \overline{B}' \leq \dim B'/(B'_u \cap B''_u)^0 \leq \dim T + \dim B'_u/(B'_u \cap B''_u)^0 \leq \dim T + 1$$

Die letzte Abschätzung besteht wegen (1). Zusammen erhalten wir

$$\#\, R(\overline{P},T) \leq 2.$$

Da $\overline{P}$ mindestens zwei verschiedene Borel-Untergruppe besitzt, nämlich $\overline{B}'$ und $\overline{B}''$, ist $\overline{P}$ nicht auflösbar. Nach 8.1.8 ist deshalb

$$W(\overline{P}, T) \neq \{e\}.$$

Nach 9.1.13 wird $W(\overline{P}, T)$ von den Spielgelungen $s_{\overline{\alpha}}$ mit $\overline{\alpha} \in R(\overline{P}, T)$ erzeugt. Also gilt $R(\overline{P}, T) \neq \emptyset$, d.h. $R(\overline{P}, T)$ enthält mindestens zwei Elemente $\overline{\alpha}$ und $-\overline{\alpha}$. Insgesamt sehen wir, daß $R(\overline{P}, T)$ aus genau zwei Elementen besteht,

(3) $$R(\overline{P}, T) = \{\overline{\alpha}, -\overline{\alpha}\}$$

Wie oben bemerkt wird $W(\overline{P}, T)$ von der Spiegelung $s_{\overline{\alpha}} = s_{\overline{-\alpha}}$ erzeugt, d.h.

$$W(\overline{P}, T) = \{\ 1, s_{\overline{\alpha}}\}$$

Nach 8.1.7(ii) operiert $W(\overline{P}, T)$ einfach transitiv auf den Borel-Untergruppen von $\mathbf{B}_T(\overline{P})$, d.h. es gilt

$$\#\, \mathbf{B}_T(\overline{P}) = 2.$$

Nun liegt $R_u(P)$ in einer, also in jeder Borel-Untergruppe von P. Deshalb gilt

$$\#\, \mathbf{B}_T(P) = \#\, \mathbf{B}_T(\overline{P}) = 2,$$

d.h.

$$\mathbf{B}_T(P) = \{B', B''\}.$$

---

[222] $R_u(P)$ liegt als auflösbarer Normalteiler in einer, also in jeder Borel-Untergruppe von P.

Wegen der einfachen Transitivität der Operation von W(P,T) auf $\mathbf{B}_T(P)$ (vgl. 8.1.7(ii)) folgt

$$\# W(P,T) = 2,$$

und da W(P,T) von Spiegelungen s_α mit $\alpha \in R(P,T)$ erzeugt wird (vgl. 9.1.13),

$$W(P,T) = \{ 1, s_\alpha \} \text{ mit } \alpha \in R(P,T) \ (\subseteq^{223} R(G,T)).$$

Nach 8.1.7(ii) operiert die Weyl-Gruppe von P einfach transitiv auf den Borel-Untergruppen von P, d.h.

$$B'' = wB'$$

mit einem eindeutig bestimmten w. Wege $B' \neq B''$ mußt w das nicht-triviale Element sein,

$$B'' = s_\alpha B'.$$

Wir haben noch die Aussagen der Bemerkung zu beweisen.

Zu (i). Wie wir gerade gesehen haben, vertauscht s_α die Borel-Untergruppen B' und B". Da s_α außerdem auch α und $-\alpha$ vertauscht, kann α nicht positiv bezüglich beider Borel-Untergruppen sein. Damit gilt die erste Aussage (eventuell mit $-\alpha$ anstelle von α).

Zu (ii). Nach Definition ist $\overline{P} = P/R_u P$ reduktiv, d.h. es gilt

$$\dim \overline{P} = \dim T + \# R(\overline{P},T) = \dim T + 2.$$

und für die beiden Borel-Untergruppen von $\overline{P}$ erhält man die Dimension

$$\dim \overline{B}' = \dim \overline{B}'' = \dim T + \frac{1}{2} \# R(\overline{P},T) = \dim T + 1.$$

Insbesondere sind deren unipotente Teile 1-dimensional, d.h.

$$\overline{B}'_u = X_\alpha \text{ und } \overline{B}''_u = X_{-\alpha}$$

(α und $-\alpha$ sind die einzigen Wurzeln von $\overline{P}$). Nach Definiton von X_α und $X_{-\alpha}$ operiert

$$S := \mathrm{Ker}(\alpha)^0$$

trivial auf $\overline{B}'_u$ und $\overline{B}''_u$, d.h. es gilt

$$G_\alpha(\overline{P}) = Z_{\overline{P}}(T) \supseteq \overline{B}'_u, \overline{B}''_u$$

und damit

$$G_\alpha(\overline{P}) = Z_{\overline{P}}(T) \supseteq \overline{B}', \overline{B}''$$

---

[223] Die Wurzeln α und $-\alpha$ besitzen auf L(P) nicht-triviale Eigenräume, also auch auf L(G). Sie sind also Gewichte von G. Da G reduktiv ist, sind sie auch Wurzeln von G (vgl. 9.3.8).

nun wird aber $\overline{P}$ (nach Definition von P) von $\overline{B}'$, $\overline{B}''$ erzeugt, d.h. es gilt

$$G_\alpha(\overline{P}) = \overline{P}.$$

Insbesondere ist $\overline{P}$ vom halbeinfachen Rang 1.
QED.

10.1.10 Die Basis eines Systems positiver Wurzeln, einfache Wurzeln

Sei G eine reduktive zusammenhängende lineare algebraische Gruppe, $T \subseteq T$ ein maximaler Torus und $B \in \mathbf{B}_T$ eine Borel-Untergruppe, die den Torus T enthält. Dann heißt die Menge

$$D(B) := \{ \alpha \in R^+(B) \mid s_\alpha B \text{ und } B \text{ sind benachbart } \}$$

die Basis von $R^+(B)$. Die Elemente von D(B) heißen einfache Wurzeln von $R^+(B)$. Wir setzen weiter

$$S(B) := \{ s_\alpha \mid \alpha \in D(B) \}$$

Bemerkung
Für $w \in W(G,T)$ gilt

$$D(wB) = wD(B) \text{ und } S(wB) = wS(B)w^{-1}.$$

Beweis. Mit

$$s_\alpha B \text{ und } B \text{ benachbart}$$

gilt auch

$$ws_\alpha B = s_{w\cdot\alpha} wB \text{ und } wB \text{ benachbart}$$

(denn nach 9.1.9(iii) a) ist $ws_\alpha w^{-1} = s_{w\cdot\alpha}$. Entsprechend ist

$$\begin{aligned} S(wB) &= \{ s_\alpha \mid \alpha \in D(wB) \} \\ &= \{ s_\alpha \mid s_\alpha wB \text{ und } wB \text{ benachbart } \} \\ &= \{ s_\alpha \mid w^{-1}s_\alpha wB \text{ und } B \text{ benachbart } \} \\ &= \{ ws_\alpha w^{-1} \mid s_\alpha B \text{ und } B \text{ benachbart } \} \\ &= \{ ws_\alpha w^{-1} \mid s_\alpha \in S(B) \} \\ &= wS(B)w^{-1}. \end{aligned}$$

QED.

10.1.11 Lemma: Operation von s_α im Fall einfacher Wurzeln α

Sei G eine reduktive zusammenhängende lineare algebraische Gruppe, $T \subseteq T$ ein maximaler Torus und $B \in \mathbf{B}_T$ eine Borel-Untergruppe, die den Torus T enthält. Dann gilt:

(i) Ist $\alpha \in D(B)$, so permultiert s_α die Elemente von $R^+(B) - \{\alpha\}$.

(ii) Sind $\alpha, \beta \in D(B)$ verschieden, so gilt $(\alpha, \beta) \leq 0$.

Beweis. Zu (i). Es gilt

$$s_\alpha R^+(B) = R^+(s_\alpha B).$$

Da B und $s_\alpha B$ benachbart sind, entsteht $s_\alpha R^+(B)$ aus $R^+(B)$ indem man eine Wurzel durch ihr Negatives ersetzt. Wegen $s_\alpha(\alpha) = -\alpha$ ist dies gerade die Wurzel α. Das Komplement von $\{\alpha\}$ in $R^+(B)$ bleibt also beim Anwenden von s_α unverändert.

Zu (ii). Seien $(\ , \ )$ eine positiv definite W-invariante Bilinearform (wie in 9.1.10) und $x \in X_{\mathbb{R}}$ ein Vektor mit

$$R^+(B) = \{\alpha \in R(G,T) \mid (x, \alpha) > 0\}$$

(vgl. 10.1.6). Nach 9.1.10 gilt dann

(*) $$\langle y, \alpha^v \rangle = 2(\alpha, \alpha)^{-1}(y, \alpha)$$

für alle Wurzeln α und alle $y \in X_{\mathbb{R}}$.

Sei x wie im Beweis von ..., dann gilt

$$\begin{aligned}
(x, \langle \alpha, \beta^v \rangle s_\alpha\beta + s_\beta\alpha) &= \langle \alpha, \beta^v \rangle (x, s_\alpha\beta) + (x, s_\beta\alpha) \\
&= \langle \alpha, \beta^v \rangle (x, \beta - \langle \beta, \alpha^v \rangle \alpha) + (x, \alpha - \langle \alpha, \beta^v \rangle \beta) \\
&= \langle \alpha, \beta^v \rangle (x, \beta) - \langle \alpha, \beta^v \rangle \langle \beta, \alpha^v \rangle (x, \alpha) + (x, \alpha) \\
&\qquad - \langle \alpha, \beta^v \rangle (x, \beta) \\
&= - \langle \alpha, \beta^v \rangle \langle \beta, \alpha^v \rangle (x, \alpha) + (x, \alpha) \\
&= (1 - \langle \alpha, \beta^v \rangle \langle \beta, \alpha^v \rangle (x, \alpha).
\end{aligned}$$

Angenommen $(\alpha, \beta) > 0$. Dann ist der ursprüngliche Ausdruck > 0, denn $s_\alpha\beta$ und $s_\beta\alpha$ liegen nach (i) beide in $R^+(B)$. Man beachte, wegen (*) ist dann auch $(\alpha, \beta^v) > 0$.

Andererseits gilt nach Lemma 9.2.2

(i) $0 \leq \langle \alpha, \beta^v \rangle \langle \beta, \alpha^v \rangle \leq 3$

(ii) $\langle \alpha, \beta^v \rangle = 0 \Leftrightarrow \langle \beta, \alpha^v \rangle = 0$,

d.h. auch $<\alpha, \beta^v>$ ist > 0, d.h. der Ausdruck (**) ist ≤ 0. Dieser Widerspruch zeigt, es gilt die Ungleichung $(\alpha, \beta) \leq 0$.
QED.

10.1.12 Theorem: die Haupteigenschaften der einfachen Wurzeln

Sei G eine reduktive zusammenhängende lineare algebraische Gruppe, $T \subseteq T$ ein maximaler Torus und $B \in \mathbf{B}_T$ eine Borel-Untergruppe, die den Torus T enthält. Dann gilt:

(i) S(B) erzeugt die Weylgruppe W := W(G,T).

(ii) $R(G,T) = W \cdot D(U)$.

(iii) (a) Die einfachen Wurzeln sind linear unabhängig.

(b) Jedes Element von $R^+(B)$ ist eine ganzzahlige Linearkombination

$$\sum_{\alpha \in D(B)} n_\alpha \cdot \alpha \text{ mit } n_\alpha \geq 0.$$

Die beiden Eigenschaften (a) und (b) charakterisieren die Menge der einfachen Wurzeln.

Beweis. 1.Schritt: Beweis von (i). Sei $w \in W$. Nach 10.1.8 gibt es eine Kette benachbarter Borel-Untergruppen

$$B_0, \ldots, B_h \in \mathbf{B}_T \text{ mit } B_0 = B \text{ und } B_h = wB.$$

Wir haben zu zeigen, w ist das Produkt von Elementen aus S(D). Wir führen den Beweis durch Induktion nach h.

Im Fall h = 1 sind wB und B benachbart, d.h. es gibt nach Lemma 10.1.9 eine einfache Wurzel $\alpha \in D(B)$ mit

$$wB = s_\alpha B.$$

Weil W einfach transitiv auf $\mathbf{B}_T$ operiert (nach 8.1.7(ii)), folgt

$$w = s_\alpha.$$

Sei jetzt $h > 1$. Weil W einfach transitiv auf $\mathbf{B}_T$ operiert, können wir B_{h-1} in der Gestalt

$$B_{h-1} = w'B \text{ mit } w' \in W$$

schreiben. Nach Induktionsvoraussetzung ist w' Produkt von Elementen aus S(D),

(1) $w' \in <S(D)>$:= die von S(D) erzeugte Untergruppe.

Da

$$w'B = B_{h-1} \text{ und } wB = B_h$$

benachbart sind, gilt dasselbe auch für

$$B \text{ und } w'^{-1}wB.$$

Nach 10.1.9 gilt deshalb

$$w'^{-1}w \in S(D),$$

also $w \in w' \cdot S(D)$. Wegen (1) gilt damit die Behauptung.

2. Schritt: Beweis der linearen Unabhängigkeit der einfachen Wurzeln. Angenommen, es gibt eine nicht-triviale Relation

$$\sum_{\alpha \in D(B)} n_\alpha \cdot \alpha = 0.$$

Wir können annehmen, wenigstens ein n_α ist positiv, d.h.

$$D_1 := \{ \alpha \in D(B) \mid n_\alpha > 0 \} \neq \emptyset.$$

Wir schreiben die Relation in der Gestalt

$$(2) \quad t := \sum_{\alpha \in D_1} n_\alpha \cdot \alpha = \sum_{\beta \in D(B)-D_1} m_\alpha \cdot \alpha \text{ mit } n_\alpha > 0 \text{ und } m_\alpha \geq 0.$$

Dann gilt

$$(t, t) = \sum_{\alpha \in D_1} \sum_{\beta \in D(B)-D_1} n_\alpha \cdot m_\beta \langle \alpha, \beta \rangle \leq 0$$

(nach 10.1.11 (ii)). Deshalb gilt $t = 0$. Ist nun $x \in X_{\mathbb{R}}$ ein Vektor, welcher $R^+(B)$ definiert, d.h.

$$R^+(B) = \{\alpha \in R \mid (\alpha, x) > 0 \},$$

so gilt wegen (2) auch

$$(t, x) > 0$$

im Widerspruch zu $t = 0$. Dieser Widerspruch beweist die lineare Unabhängigkeit der einfachen Wurzeln.

3. Schritt. Für jedes $\alpha \in R^+(B)$ gibt es ein $\beta \in D(B)$ mit $\langle \alpha, \beta^v \rangle > 0$.
Sei $\alpha \in R$ eine Wurzel mit

$$\langle \alpha, \beta^v \rangle \leq 0 \text{ für alle } \beta \in D(B).$$

Es reicht zu zeigen, $\alpha \in -R^+(B)$. Wir zerlegen $X_{\mathbb{R}}$ in eine orthogonale direkte Summe bezüglich des W-invarianten Skalarprodukts (,),

$$X_{\mathbb{R}} := X' \oplus X'^{\perp} \text{ mit } X' := \sum_{\beta \in D(B)} \mathbb{R}\beta ,$$

und schreiben

$$\alpha = x' + x'^{\perp} \text{ mit } x' \in X'^{\perp} \text{ und } x' \in X'^{\perp}.$$

Betrachten wir $\alpha' \in D(B)$ die zugehörige Spiegelung

$$s_{\alpha'}(\chi) = \chi - <\chi, \alpha'^{\vee}> \alpha'$$

Sie überführt X' in sich (da die Erzeugenden $\beta \in D(B)$ in Elemente von X' abgebildet werden) und läßt die Elemente aus $X'^{\perp}$ fest[224]. Nach der bereits bewiesenen Aussage (i) erzeugen die $s_{\alpha'}$, mit $\alpha' \in D(B)$ die gesamte Weyl-Gruppe, d.h. es gilt

$$w(X') \subseteq X' \text{ und } w|_{X^{\perp}} = Id \text{ für alle } w \in W.$$

Wir wenden dies speziell für $w = s_{\alpha'}$ auf die obige orthogonale Zerlegung von α an und erhalten

Speziell für $w = s_{\alpha'}$ erhalten wir durch Anwenden auf die direkte Zerleung von α,

$$x'^{\perp} = 0.^{225}$$

Wir können also α in der Gestalt

$$\alpha = \sum_{\beta \in D(B)} \xi_{\beta} \beta \text{ mit } \xi_{\beta} \in \mathbb{R}$$

schreiben. Sei

$$u := \alpha - \sum_{\xi_{\beta} < 0} \xi_{\beta} \beta.$$

Dann gilt

$$(u, u) = (\alpha - \sum_{\xi_{\beta} < 0} \xi_{\beta} \beta, \sum_{\xi_{\beta} \geq 0} \xi_{\beta} \beta)$$

$$= (\alpha, \sum_{\xi_{\beta} \geq 0} \xi_{\beta} \beta) - (\sum_{\xi_{\beta} < 0} \xi_{\beta} \beta, \sum_{\xi_{\beta} \geq 0} \xi_{\beta} \beta)$$

$$\leq 0$$

---

[224] denn mit $(\chi, \alpha'^{\vee}) = 0$ gilt auch $<\chi, \alpha'^{\vee}> = 0$, denn nach. 9.1.10 gilt für alle Wurzeln α und alle χ, $<\chi, \alpha^{\vee}> = 2(\alpha, \alpha)^{-1}(\chi, \alpha)$.

[225] Wir wenden $s_{\alpha'}$ auf die Zerlegung $\alpha = x' + x'^{\perp}$ an und erhalten

$$-\alpha = s_{\alpha'}(x') + x'^{\perp}.$$

Vergleich mit $-\alpha = -x' + (-x'^{\perp})$ liefert $x'^{\perp} = -x'^{\perp}$, also $x'^{\perp} = 0$.

(denn nach Wahl von α ist der erste Summand ≤ 0 und nach Lemma 10.1.11(ii) gilt dasselbe für den Zweiten Summanden). Damit gilt aber $u = 0$, d.h.

$$\alpha = \sum_{\xi_\beta < 0} \xi_\beta \beta .$$

Mit anderen Worten, α ist eine negative Linearkombination der Elemente von D(B) ($\subseteq R^+(B)$), d.h. die Wurzel α liegt in $-R^+(B)$.

4. Schritt. Beweis von (ii) und der zweiten Aussage von (iii).

Wir wählen $x \in X_{\mathbb{R}}$ derart, daß gilt

$$R^+(B) = \{ \alpha \in R(G,T) \mid (x , \alpha) > 0 \}$$

(vgl. 10.1.6). Es reicht zu zeigen, für jedes

$$\alpha \in R^+(B) - D(B)$$

gilt:[226]

1. $\alpha \in W \cdot D(B)$.
2. α ist eine positive ganzzahlige Linearkombination von Elementen aus D(B).

Die Menge der Werte

$$\{ (x, \alpha) \mid \alpha \in R^+(B) \}$$

ist endlich. Wir können deshalb den Beweis durch "Induktion" nach (x, α) führen, d.h. wir können beim Beweis von 1. und 2. annehmen, daß für alle $\alpha' \in R^+(B)$ mit

$$(x, \alpha') < (x , \alpha)$$

die Aussagen 1. und 2. gelten.[227] Nach dem dritten Schritt gibt es ein $\beta \in D(B)$ mit

(3) $$<\alpha, \beta^v> > 0.$$

Es gilt $s_\beta(\alpha) = \alpha - <\alpha, \beta^v>\beta$, d.h.

(4) $$\alpha = s_\beta(\alpha) + <\alpha, \beta^v>\beta$$

---

[226] Für $\alpha \in D(B)$ sind die beiden Aussagen trivialerweise erfüllt. Man beachte weiter, daß mit 1 sogar $R(G,T) \subseteq W \cdot D(B)$ gilt. Mit $R^+(B) \subseteq W \cdot D(B)$ liegt nämlich jede Wurzel α in $W \cdot D(B)$, denn wegen

$$\alpha \in R^+(B) \text{ oder } -\alpha \in R^+(B)$$

ist dann $\alpha \in W \cdot D(B)$ oder $-\alpha \in W \cdot D(B)$. Durch Anwenden von

$$s_\alpha = s_{-\alpha} \in W$$

ergibt sich, daß auch das Negative der Wurzel, die bereits in $W \cdot D(B)$ liegt, ebenfalls ein Element von $W \cdot D(B)$ sein muß.

[227] Ist (x, α) minimal in der angegebenen Menge, so ist die Menge dieser α' leer.

und

(5) $$(x, \alpha) = (x, s_\beta(\alpha)) + <\alpha, \beta^v>(x, \beta)$$

Wegen $\beta \in D(B)$ und $\alpha \in R^+(D)$ gilt $\alpha \neq \beta$ also nach 10.1.11(i) auch

$$s_\beta(\alpha) \in R^+(B).$$

Es reicht zu zeigen, die Aussagen 1 und 2 gelten mit $s_\beta(\alpha)$ anstelle von α, denn trivialerweise liegt dann auch

$$\alpha = s_\beta\, s_\beta(\alpha) \text{ in } W \cdot D(B)$$

und wegen (3) und (4) ist dann auch α ein positive Linearkombination von Elementen aus D(B). Die Aussagen 1 und 2 gelten trivialerweise für $s_\beta(\alpha)$, falls $s_\beta(\alpha)$ in D(B) liegt. Wir können also annehmen,

$$s_\beta(\alpha) \in R^+(B) - D(B).$$

Wegen (3) und (5) ist

$$(x, s_\beta(\alpha)) < (x, \alpha),$$

d.h. $s_\beta(\alpha)$ genügt den Bedinungen der Induktionsvoraussetzung, d.h. 1 und 2 gelten für $s_\beta(\alpha)$.

Damit sind alle Aussagen des Satzes bewiesen, außer der folgenden:
5. Schritt: durch die Bedingungen (a) und (b) von (iii) sind die einfachen Wurzeln eindeutig festgelegt.
Aus (a) und (b) ergibt sich, daß eine Wurzel genau dann einfach ist, wenn sie positiv ist und nicht als Summe zweier positiver Wurzeln geschrieben werden kann:

Die Bedingung ist notwendig.
Ist α einfache Wurzel, so ist α (trivialerweise) positiv. Außerdem kann α sich Summe positiver Wurzeln sein, weil es sonst zwei verschiedene Darstellungen von α als Linearkombination einer Wurzeln gäbe.

Die Bedingung ist hinreichend.
Sei α positive Wurzel, die nicht als Summe positiver Wurzeln geschrieben werden kann. Dann ist α wenigstens eine positive ganzzahlige Linearkombination einfacher Wurzeln. Von den Koeffizienten müssen dann aber alle bis auf einem Null sein, und der eine von Null verschiedene Koeffizient muß 1 sein.
QED.

10.1.13 Folgerung

Seien G eine reduktive zusammenhängende lineare algebraische Gruppe, T ein maximaler Torus von G und $B \in \mathbf{B}_T$ eine Borel-Untergruppe von G. Dann wir G von T und den Untergruppen

$$X_{\pm\alpha} \text{ mit } \alpha \in D(B)$$

erzeugt.

Beweis. Sei G' die von T und den $X_{\pm\alpha}$ mit $\alpha \in D(B)$ erzeugte Untegruppe von G,

(1) $$G' := < T, X_{\pm\alpha} \mid \alpha \in D(B) >.$$

Es reicht zu zeigen,

(2) $$X_\alpha \subseteq G' \text{ für alle } \alpha \in R(G,T),$$

denn dann liegen alle Borel-Untergruppen von G in G' (nach 10.1.1)[228], d.h. es ist $G \subseteq G'$[229]. Zum Beweis von (2) reicht es zu zeigen,

(3) $$X_\beta \subseteq G' \text{ und } \alpha \in D(B) \Rightarrow X_{s_\alpha(\beta)} \subseteq G',$$

denn die s_α mit $\alpha \in D(B)$ erzeugen die Weylgruppe W:= W(G,T) (nach 10.1.12(i)). d.h. mit (3) gilt auch

$$X_\beta \subseteq G' \text{ und } w \in W \Rightarrow X_{w\cdot\beta} \subseteq G'.$$

Da nun alle X_α mit $\alpha \in D(B)$ in G' liegen (wegen (1)) und

$$W \cdot D(B) = R(G,T)$$

gilt (nach 10.1.12(ii)), so gilt mit (3) auch (2). Zum Beweis von (3) reicht es zu zeigen,

(4) Jede Wurzel $\alpha \in D(B)$ ist auch eine Wurzel von G'

denn dann gibt es ein $n \in N_{G'}(T) \subseteq G'$, welches die Spiegelung s_α zu $\alpha \in D(B)$ repräsentiert und nach Lemma 10.1.3 gilt für β wie in (3)

$$X_{s_\alpha(\beta)} = nX_\beta n^{-1} \subseteq G'.$$

Beweisen wir (4). Sei $\alpha: T \to G_m$ ein Wurzel aus D(B). Wir haben zu zeigen,

$$S := \mathrm{Ker}(\alpha)^0$$

ist eine singulärer Torus von G'. Zumindest gilt

$$S \subseteq T \subseteq G'.$$

---

[228] Zusammen mit T erzeugen die X_α zu den positiven Wurzeln die Borel-Untergruppe.

[229] Nach 7.3.3(i) Überdecken die Borel-Untergruppen von G die Gruppe G.

Nach Definition von $X_{\pm\alpha}$ und wegen (1) gilt

$$X_{\pm\alpha}, T \subseteq Z_G,(S).$$

Wegen $S \subseteq T \subseteq B$ ist $B \cap Z_G,(S)$ ein Borel-Untergruppe von $Z_G,(S)$ (vgl. 7.3.5(ii)). Wäre $Z_G,(S)$ auflösbar, so wäre

$$B \cap Z_G,(S) = Z_G,(S)$$

d.h.

$$X_{\pm\alpha} \subseteq Z_G,(S) \subseteq B.$$

Insbesondere wären die Wurzeln α und $-\alpha$ beide positiv bezüglich B (nach 9.3.9(i)), was nicht möglich ist (nach Definition des Begriffs "System positiver Wurzeln", vgl. 9.2.3). Also ist $Z_G,(S)$ nicht auflösbar, d.h. S ist ein singulärer Torus von G', d.h. α ist eine Wurzel von G'.

QED.

10.1.14 Aufgaben

Seien G eine reduktive zusammenhängende lineare algebraische Gruppe, $T \subseteq G$ ein maximaler Torus, $B \in \mathbf{B}_T$,

$$R := R(G,T),\ W := W(G,T),\ D = D(B).$$

(1) Sei R eines der Wurzelsysteme A_{n-1}, B_n, C_n, D_n wie in 9.3.10.

Dann gilt:

(a) Die Basis von $R^+(B)$ hat die folgende Gestalt.

Fall $R = A_{n-1}$: $D = \{e_1-e_2, e_2 - e_3, \dots, e_{n-1}-e_n\}$

Fall $R = B_n$: $D = \{e_1-e_2, e_2 - e_3, \dots, e_{n-1}-e_n, e_n\}$

Fall $R = C_n$: $D = \{e_1-e_2, e_2 - e_3, \dots, e_{n-1}-e_n, 2e_n\}$

Fall $R = D_n$: $D = \{e_1-e_2, e_2 - e_3, \dots, e_{n-1}-e_n, e_{n-1}+ e_n\}$.

(b) R ist irreduzibel.

(c) Die Weyl-Gruppe hat die folgende Gestalt.

Fall $R = A_{n-1}$: $W = S_n$, S_n operiert durch Permutieren der Basis $e_1, \dots, e_n$.

Fall $R = B_n$ oder C_n:

W ist die Gruppe der linearen Transformationen

(*) $\mathbb{R}^n \to \mathbb{R}^n$. $e_i \mapsto \eta_i e_{\sigma(i)}$ mit $\sigma \in S_n$ und $\eta_i = \pm 1$.

Fall $R = D_n$: W ist die Gruppe der lineare Transfomationen (*) mit

$$\prod_i \eta_1 = 1.$$

(2) R ist genau dann irreduzibel (vgl. Aufgabe 9.4.3 (1)), wenn sich D in der Gestalt

$$D = D' \cup D''$$

schreiben läßt mit $(\alpha, \beta) = 0$ für $\alpha \in D'$ und $\beta \in D''$.

(3) Sei P das Gewichtsgitter (vgl. 9.4.2). Man zeige, P hat eine Basis

$$\{\omega_\alpha\}_{\alpha \in D}$$

mit $(\omega_\alpha, \beta^v) = \delta_{\alpha\beta}$ (Kronecker-Symbol). We gilt

$$s_\alpha(\omega_\beta) = \omega_\beta - \delta_{\alpha\beta}\alpha$$

(die ω_α's heißen <u>fundamentale Gewichte</u>).

10.2 Das Lemma von Bruhat

10.2.1 Voraussetzungen und Bezeichnungen, Länge eines Elements der Weyl-Gruppe

Wie bisher sei G eine reduktive zusammenhängende lineare algebraische Gruppe, $T \subseteq G$ ein maximaler Torus und $B \in \mathbf{B}_T$ eine Borel-Untergruppe von G. Weiter sei

$R := R(G,T)$
$W := W(G,T)$
$R^+ := R^+(B)$
$D := D(B)$
$S := S(B)$

Für $w \in W$ schreiben wir

$$R(w) := \{\alpha \in R^+ \mid w\alpha \in -R^+\}$$

für die Menge der positiven Wurzeln, die durch w in negative Wurzeln abgebildet werden.

Insbesondere gilt

$$R(s_\alpha) = \{\alpha\} \text{ falls } \alpha \in D$$

nach 10.1.11(i). Deshalb gilt

(1) Für $\alpha \in D$, $w\alpha > 0$ gilt $R(ws_\alpha) =^{230} s_\alpha R(w) \cup \{\alpha\}$ (disj. Vereinigung).

---

[230] Es gilt

$$\beta \in s_\alpha R(w) \Rightarrow s_\alpha(\beta) \in R(w)$$
$$\Rightarrow s_\alpha(\beta) > 0 \text{ und } ws_\alpha(\beta) < 0$$

Insbesondere ist $\beta \neq \alpha$, denn $s_\alpha(\alpha) = -\alpha < 0$. Außerdem ist $\beta \neq -\alpha$, denn $ws_\alpha(-\alpha) = w\alpha > 0$. Damit gilt $s_\alpha(\beta) \neq \pm\alpha$, also:

(2) Für $\alpha \in D$, $w\alpha < 0$ gilt $R(ws_\alpha) =^{231} s_\alpha(R(w) - \{\alpha\})$.

Schreiben wir $w \in W$ in der Gestalt

$\beta \in s_\alpha R(w) \Rightarrow \beta > 0$ und $ws_\alpha(\beta) < 0$ (denn s_α permutiert $R^+ - \{\alpha\}$).

$\Rightarrow \beta \in R(ws_\alpha)$.

Wir haben gezeigt

$s_\alpha R(w) \subseteq R(ws_\alpha)$.

Wegen $w\alpha > 0$ folgt

(*) $s_\alpha R(w) \cup \{\alpha\} \subseteq R(ws_\alpha)$,

wobei die Vereinigung links eine disjunkte Vereinigung ist.
Zeigen wir, in (*) gilt das Gleichzheitszeichen. Sei also

$\beta \in R(ws_\alpha)$.

Dann gilt

$\beta > 0$ und $ws_\alpha(\beta) < 0$.

Nehmen wir jetzt an, $\beta \neq \alpha$. Da s_α die Menge $R^+ - \{\alpha\}$ permutiert, folgt

$s_\alpha(\beta) > 0$ und $ws_\alpha(\beta) < 0$

also

$s_\alpha(\beta) \in R(w)$

also $\beta \in s_\alpha R(w)$. Wir haben gezeigt, in (*) gilt das Gleichheitszeichen.

[231] Es gilt

$\beta \in s_\alpha(R(w) - \{\alpha\}) \Rightarrow s_\alpha(\beta) \in R(w) - \{\alpha\}$

$\Rightarrow s_\alpha(\beta) > 0$ und $ws_\alpha(\beta) < 0$, $s_\alpha(\beta) \neq \alpha$

Da s_α die Menge $R^+ - \{\alpha\}$ permutiert, folgt

$\beta \in s_\alpha(R(w) - \{\alpha\}) \Rightarrow \beta > 0$ und $ws_\alpha(\beta) < 0$

$\Rightarrow \beta \in R(ws_\alpha)$.

Wir haben gezeigt

(*) $s_\alpha(R(w) - \{\alpha\}) \subseteq R(ws_\alpha)$.

Zeigen wir, in (*) gilt das Gleichheitszeichen. Sei also

$\beta \in R(ws_\alpha)$.

Dann gilt

$\beta > 0$ und $ws_\alpha(\beta) < 0$.

Es ist dann $\beta \neq -\alpha$ und $\beta \neq \alpha$, denn $ws_\alpha(\alpha) = w(-\alpha) > 0$. Weil s_α die Elemente von $R^+ - \{\alpha\}$ permutiert, folgt

$s_\alpha(\beta) > 0$ und $ws_\alpha(\beta) < 0$ und $\beta \neq -\alpha$.

also $s_\alpha(\beta) \in R(w) - \{\alpha\}$, also $\beta \in s_\alpha(R(w) - \{\alpha\})$. Damit gilt in (*) das Gleichheitszeichen.

(3) $w = s_1 \cdot \ldots \cdot s_h$ mit $s_i \in S$ für alle i

(vgl. 10.1.12(i)). Ist h so klein wie möglich, so heißt (3) kürzeste Zerlegung von w und h heißt Länge von w und wird mit

$$l(w) := h$$

bezeichnet (bezüglich S, D, bzw. R^+).

Bemerkung

Es gilt $l(w) = l(w^{-1})$.

10.2.2 Lemma: Eigenschaften der Länge

Seien G eine reduktive lineare algebraische Gruppe, $T \subseteq G$ ein maximaler Torus und $B \in \mathbf{B}_T$ eine Borel-Untergruppe. Weiter sei $w \in W(G,T)$ und

$$w = s_1 \cdot \ldots \cdot s_h$$

eine kürzeste Zerlegung mit $s_i = s_{\alpha_i}$ und $\alpha_i \in D(B)$. Dann gilt

(i) $R(w) = \{\alpha_h , s_h\alpha_{h-1} , s_h s_{h-1}\alpha_{h-2} , \ldots , s_h s_{h-1} \ldots s_2\alpha_1\}$
(rechts stehen paarweise verchiedene Elemente)

(ii) $l(w) = \# R(w)$.

(iii) Sei $\alpha \in D(B)$. Dann gilt

$$l(ws_\alpha) = \begin{cases} l(w)+1 \text{ falls } w\alpha > 0 \\ l(w)-1 \text{ falls } w\alpha < 0 \end{cases} \quad \text{und} \quad l(s_\alpha w) = \begin{cases} l(w)+1 \text{ falls } w^{-1}\alpha > 0 \\ l(w)-1 \text{ falls } w^{-1}\alpha < 0 \end{cases}$$

(iv) Sei $\alpha \in D(B)$ eine einfache Wurzel mit $w\alpha < 0$. Dann gibt es eine kurzeste Zerlegung

$$w = s'_1 \cdot \ldots \cdot s'_h \text{ mit } s'_h = s_\alpha .$$

(v) Ist

$$w = s'_1 \cdot \ldots \cdot s'_h$$

eine kürzeste Zerlegung, so gibt es ein i mit $1 \le i \le h$ und

$$s_1 \cdot \ldots \cdot s_{i-1}\, s_{i+1} \cdot \ldots \cdot s_h = s'_1 \cdot \ldots \cdot s'_{h-1} .$$

Beweis. Zu (i). Im Fall h = 1 ist die Behauptung richtig (vgl. 10.2.1). Sei jetzt h > 1. Wir setzen

$$w' := s_1 \cdot \ldots \cdot s_{h-1}$$

Nach Induktionsvoraussetzung gilt

$$R(w') = \{\alpha_{h-1} , s_{h-1}\alpha_{h-2} , \ldots , s_{h-1}s_{h-2} \ldots s_2\alpha_1\}.$$

1. Fall: $w'\alpha_h > 0$.

Wir wenden Formeln (1) von 10.2.1 an und erhalten die Behauptung.

2. Fall: $w'\alpha_h < 0$. Wir zeigen, daß dieser Fall unmöglich ist. Ist er es doch, so liegt α_h in $R(w')$, d.h. es gilt

$$\alpha_h = s_{h-1}s_{h-2}\cdots s_{i+1}\alpha_i$$

für ein i. Damit ist

$$s_h = s_{\alpha_h} =^{232} (s_{h-1}s_{h-2}\cdots s_{i+1})s_i(s_{h-1}s_{h-2}\cdots s_{i+1})^{-1}$$
$$= (s_{h-1}s_{h-2}\cdots s_{i+1})s_i(s_{i+1}s_{i+2}\cdots s_{h-1}).$$

Einsetzen in die Zerlegung von w liefert

$$w = s_1\cdot\ldots\cdot s_h = s_1\cdot\ldots\cdot s_{i-1}\, s_{i+1}\cdot\ldots\cdot s_h.$$

Der letzte Ausdruck steht aber im Widerspruch zur Minimalität von h. Der zweite Fall ist somit nicht möglich.

Zu (ii). Folgt aus (i).

Zu (iii). Die erste Formel folgt aus (ii) und den Identitäten (1) und (2) von 10.2.1. Zum Beweis der zweiten Formel benutzen wir die gerade bewiesene Formel

$$l(ws_\alpha) = \begin{cases} l(w)+1 \text{ falls } w\alpha > 0 \\ l(w)-1 \text{ falls } w\alpha < 0 \end{cases}$$

und beachten, daß $l(w) = l(w^{-1})$ gilt. Genauer ist

$$l(s_\alpha w) = l(w^{-1}s_\alpha) = \begin{cases} l(w^{-1})+1 \text{ falls } w^{-1}\alpha > 0 \\ l(w^{-1})-1 \text{ falls } w^{-1}\alpha < 0 \end{cases}$$

Zu (iv). Wegen $\alpha \in D(B)$ und $w\alpha < 0$ gilt $\alpha \in R(w)$, nach (i) also

$$\alpha = s_h\cdots s_{i+1}\alpha_i$$

für ein i. Die Transformation $s_h\cdots s_{i+1}$ identifiziert daher die Spiegelung s_{α_i} mit der Spiegelung s_α, d.h.

$$s_\alpha = (s_h\cdots s_{i+1})s_i(s_{i+1}\cdots s_h).$$

Wegen $w = s_1\cdot\ldots\cdot s_h$ ist damit

$$ws_\alpha = s_1\cdot\ldots\cdot s_{i-1}s_{i+1}\cdots s_h$$

also

$$w = s_1\cdot\ldots\cdot s_{i-1}s_{i+1}\cdots s_h s_\alpha.$$

Dies ist ein kürzelste Zerlegung der behaupteten Gestalt.

---

[232] Die Transformation $s_{h-1}s_{h-2}\cdots s_{i+1}$ identifiziert α_h mit α_i also die Spiegelung and der zu α_h orthogonalen Hyperebene mit der Spiegelung an der zu α_i orthogonalen Hyperebene.

Zu (v). Sei

$$w = s'_1 \cdot \ldots \cdot s'_h$$

eine weitere kürzeste Zerlegung. Sei $\alpha \in D(B)$ derart, daß gilt

$$s'_h = s_\alpha .$$

Nach (i) liegt dann α in $R(w)$, d.h. es gilt $w\alpha < 0$. Mit anderen Worten, die Voraussetzung von (iv) ist erfüllt. Wie wir gerade beim Beweis von (iv) gesehen haben, gilt

$$s_1 \cdot \ldots \cdot s_{i-1} s_{i+1} \ldots s_h s_\alpha = w \ (= s'_1 \cdot \ldots \cdot s'_h).$$

Multiplikation von rechts mit $s_\alpha = s'_h$ liefert die Behauptung.

QED.

10.2.3 Bezeichnung: m(s,t) für s,t∈S(B)

Seien G eine lineare algebraische Gruppe, T ein maximaler Torus von G und $B \in \mathbf{B}_T$ ein Borrel-Untergruppe. Für je zwei Spiegelungen

$$s, t \in S(B)$$

einfachen Wurzeln mit

$$s \neq t$$

bezeichne m(s,t) die Ordnung von st in der Weylgruppe W(G,T),

$$m(s,t) = \# \langle st \rangle .$$

Für je zwei einfache Wurzeln $\alpha, \beta \in W(G,T)$ mit

$$\alpha \neq \beta$$

setzen wir

$$m(\alpha, \beta) := m(s_\alpha, s_\beta).$$

Bemerkungen

(i) Es gilt

$$m(s, t) = m(t, s).$$

(ii) Ein <u>multiplikatives Monoid</u> M ist eine nicht-leere Menge mit assoziativer Operation

$$M \times M \to M, (a,b) \mapsto a \cdot b.$$

10.2.4 Proposition: Funktionen auf W mit Werten in multiplikativen Monoiden

Seien G eine reduktive zusammenhängende lineare algebraische Gruppe, T ein maximaler Torus von G und $B \in \mathbf{B}_T$ ein Borel-Untergruppe. Weiter sei M ein multiplikatives Monoid mit 1 und

$$\mu: S(D) \to M$$

eine Abbildung, mit der folgenden Eigenschaft.

Für $s,t \in S(D)$, $s \neq t$ gilt

$$\mu(s)\mu(t)\mu(s)\ldots = \mu(t)\mu(s)\mu(t)\ldots$$

wobei die Produkte auf beiden Seiten aus m(s,t) Faktoren bestehen.

Dann gibt es genau eine Fortsetzung

$$\tilde{\mu} : W(G, T) \to M$$

von μ auf die Weyl-Gruppe mit

(1) $$\tilde{\mu}(w) = \mu(s_1)\cdot\ldots\cdot\mu(s_h)$$

für jedes $w \in W(G, T)$ mit der kürzesten Zerlegung

$$w = s_1\cdot\ldots\cdot s_h .$$

Beweis. Wir haben zu zeigen, die rechte Seite von (1) ist unabhängig von der speziellen Wahl der kürzesten Zerlegung. Wir führen den Beweis nach Induktion nach

$$h := l(w).$$

Für $h = 1$ ist nichts zu beweisen.
Sei $h > 1$. Seien

$$w = s_1\cdot\ldots\cdot s_h = s'_1\cdot\ldots\cdot s'_h.$$

zwei kürzeste Zerlegungen. Nach 10.2.2 (v) gibt es ein i mit

(2) $$s_1\cdot\ldots\cdot s_{i-1}\, s_{i+1}\cdot\ldots\cdot s_h = s'_1\cdot\ldots\cdot s'_{h-1}.$$

1. Fall: $i > 1$.
Nach Induktionsvoraussetzung gilt

$$\mu(s'_1)\cdot\ldots\cdot\mu(s'_{h-1}) = \mu(s_1)\cdot\ldots\cdot\mu(s_{i-1})\,\mu(s_{i+1})\cdot\ldots\cdot\mu(s_h).$$

Wir multiplizieren von rechts mit $\mu(s_h)$ und erhalten

(3) $$\mu(s'_1)\cdot\ldots\cdot\mu(s'_{h-1})\cdot\mu(s'_h) = \mu(s_1)\cdot\ldots\cdot\mu(s_{i-1})\,\mu(s_{i+1})\cdot\ldots\cdot\mu(s_h)\cdot\mu(s'_h)$$

Nun gilt aber[233]

$$s_{i+1}\cdot\ldots\cdot s_h s'_h = s_i\cdot\ldots\cdot s_h$$

und dies sind zwei kurzeste Zerlegungen einer Länge $< i$ (wegne $i > 1$). Deshalb ist die rechte Seite von (3) gleich

$$\mu(s_1)\cdot\ldots\cdot\mu(s_{i-1})\,\mu(s_i)\cdot\ldots\cdot\mu(s_h),$$

d.h. es gilt die Behauptung.
2. Fall: $i = 1$.
Nach (2) gilt

$$w = s_2\cdot\ldots\cdot s_h s'_h$$

und es ist

$$\mu(s'_1)\cdot\ldots\cdot\mu(s'_h) = \mu(s'_1)\cdot\ldots\cdot\mu(s'_{h-1})\cdot\mu(s'_h)$$
$$= \mu(s_2)\cdot\ldots\cdot\mu(s_h)\,\mu(s'_h) \qquad \text{(nach (2) und Ind. vor.).}$$

---

[233] Multiplikation von (2) mit s'_h liefert

$$s_1\cdot\ldots\cdot s_{i-1}\, s_{i+1}\cdot\ldots\cdot s_h\, s'_h = w = s_1\cdot\ldots\cdot s_h$$

Aus Symmetriegründen können wir auch annehmen, es gilt[234]

$$w = s'_2 \cdot \ldots \cdot s'_h s_h$$

und

$$\mu(s_1) \cdot \ldots \cdot \mu(s_h) = \mu(s'_2) \cdot \ldots \cdot \mu(s'_h)\, \mu(s_h).$$

Wir haben damit den Beweis auf den Fall reduziert, daß w von der Gestalt

$$w = w'_1 s's = w''_1 ss'$$

ist mit

$$l(w') = l(w'') = h - 2$$

und

$$s,s' \in S(D),\ s \neq s'.$$

Indem wir die obigen Schlüsse mit den neuen kürzesten Zerlegungen wiederholen, reduzieren wir den Beweis auf den Fall

$$(4) \qquad w = w'_i (s's)^i = w''_i (ss')^i$$

mit

$$l(w'_i) = l(w''_i) = h - 2i.$$

Wir müssen zeigen, aus den Zerlegungen (4) kann man Zerlegungen derselben Art gewinnen mit i+1 anstelle von i. Dabei können wir annehmen, die beiden kürzesten Zerlegungen von (4) genügen nicht den Annahmen des oben behandelten Falls 1, d.h. Kürzen des letzten Faktors rechts hat dieselbe Wirkung wie das Kürzen des ersten Faktors links (und analog mit links und rechts vertauscht), d.h.

$$(*) \qquad w'_i (s's)^{i-1} s' = \tilde{w}''(ss')^i \quad \text{und} \quad w''_i (ss')^{i-1} s = \tilde{w}'(s's)^i$$

mit $\tilde{s}'\tilde{w}' = w'_i$ und $\tilde{s}''\tilde{w}'' = w''_i$ (identische Ausdrücke). Wir erhalten aus (4) und (*) die kürzesten Zerlegungen

$$(**) \qquad w = \tilde{w}'(s's)^i s' = \tilde{w}''(ss')^i s$$

Dabei gilt[235]

$$\mu(w'_i)(\mu(s')\mu(s))^i = \mu(w'_i)(\mu(s')\mu(s))^{i-1}\mu(s')\mu(s) \quad \text{(identische Ausdr.)}$$

$$= \mu(\tilde{w}'')(\mu(s)\,\mu(s'))^i\,\mu(s)$$

nach Induktionsvoraussetzung (angewandt auf den ersten Ausdruck von (*)). Analog sieht man

---

[234] Andernfalls folgt die Behauptung nach Fall 1, wenn man die gestrichenen und ungestrichenen Spiegelungen ihre Rollen vertauschen läßt.

[235] $\mu(w)$ bedeute hier, daß man μ faktorweise auf w anwendet.

$$\mu(w''_i)(\mu(s)\mu(s'))^i = \mu(w'_i)(\mu(s')\mu(s))^{i-1}s'$$

Wiederholung der Argumentation mit (**) liefert (4) mit i+1 anstelle von i.

Für i groß reduziert das den Beweis auf den Fall

$$w = s'ss'... = ss's... \text{ mit } s,s' \in S,\ s \neq s',$$

d.h.

(5) $$w = w'(s's)^i = w''(ss')^i$$

wobei entweder w' = s und w" =s' gilt oder w' = w' = 1. Multiplikation von rechts mit $(s's)^i$ liefert

$$w'(s's)^{2i} = w''$$

Im Fall $w' \neq 1$ multiplizieren wir noch von links mit s und von rechts mit s's und erhalten insgesamt

$$(s's)^m = 1,$$

wobei m die Anzahl der Faktoren auf beiden Seiten von (5) ist. Für letztere Anzahl gilt also

$$m(s, s') \mid m.$$

Mit anderen Worten, der Fall (5) wird gerade durch die Voraussetzung des Satzes abgedeckt.

QED.

10.2.5 Propositon: Beschreibung der Weyl-Gruppe durch Generatoren und Relationen

Seien G eine reduktive zusammenhängende lineare algebraische Gruppe, T ein maximaler Torus von G und $B \in \mathbf{B}_T$ eine Borel-Untergruppe von G. Dann definiert die Menge

$$S(B)$$

der Spiegelungen zu den einfachen Wurzeln zusammen mit den Relationen

$$s^2 = 1 \text{ und } (st)^{m(s,t)} = 1 \text{ für } s,t \in S(B) \text{ und } s \neq t$$

eine Darstellung der Weyl-Gruppe W(G, T).

Beweis. Sei $\tilde{W}$ die Gruppe

$$\tilde{W} = \langle \tilde{s} \mid s \in S(D) \rangle,$$

die von den Symbolen $\tilde{s}$ erzeugt wird, welche den Relationen

$$\tilde{s}^2 = 1 \text{ und } (\tilde{s}\tilde{t})^{m(s,t)} = 1 \text{ für } s,t \in S(D) \text{ mit } s \neq t$$

genügen. Dann existiert ein surjektiver Homomorphismus

$$\pi\colon \tilde{W} \twoheadrightarrow W,\ \tilde{s} \mapsto s,$$

denn W wird von den Spiegelungen S(D) erzeugt (vgl. 10.1.12(i)). Nach 10.2.4 gibt es weiter eine Abbildung

$$\mu\colon W \to \tilde{W}$$

mit

$$\mu(w) = \tilde{s}_1 \cdot \ldots \cdot \tilde{s}_h$$

für jedes $w \in W$ mit der kürzesten Zerlegung

$$w = s_1 \cdot \ldots \cdot s_h .$$

Nach Konstruktion gilt

(1) $$\pi \circ \mu = \mathrm{Id}.$$

Zeigen wir, μ ist ein Gruppenhomomorphismus,

(2) $$\mu(w')\mu(w'') = \mu(w'w'') \text{ für } w', w'' \in W.$$

Wir führen den Beweis durch Induktion nach $h := l(w'')$.

Im Fall $h = 1$ ist $w'' = s_\alpha$ mit $\alpha \in D(B)$. Nach 10.2.2 (iii) gilt

$$l(w's_\alpha) = \begin{cases} l(w')+1 & \text{falls } w\alpha > 0 \\ l(w')-1 & \text{falls } w\alpha < 0 \end{cases}$$

Im ersten Fall erhält man aus einer kürzesten Zerlegung von w' eine solche von $w's_\alpha$, indem man mit s_α multipliziert, d.h. es gilt

$$\mu(w's_\alpha) = \mu(w')\mu(s_\alpha).$$

Im zweiten Fall erhält man aus einer kürzesten Zerlegung von $w's_\alpha$ eine solche von w', indem man mit s_α multipliziert, d.h. es gilt

$$\mu(w') = \mu(w's_\alpha)\mu(s_\alpha).$$

Wir multiplizieren von rechts mit $\mu(s_\alpha) = \tilde{s}_\alpha$ und erhalten

$$\mu(w')\,\mu(s_\alpha) = \mu(w's_\alpha).$$

Im Fall $h > 1$ schreiben wir w'' in der Gestalt

$$w'' = s_\alpha \tilde{w} \text{ mit } l(\tilde{w}) = h-1.$$

Dann gilt

$$\begin{aligned} \mu(w'w'') &= \mu((w' s_\alpha)\tilde{w}) = \mu(w' s_\alpha)\,\mu(\tilde{w}) && \text{(Induktionsvor.)} \\ &= \mu(w')\,\mu(s_\alpha)\,\mu(\tilde{w}) && \text{(der Fall } h = 1) \\ &= \mu(w')\,\mu(s_\alpha \tilde{w}) && \text{(Induktionsvor.)} \\ &= \mu(w')\,\mu(w''). \end{aligned}$$

Damit ist (2) bewiesen. Da nach Kostruktion von μ das Bild von μ ein Erzeugendensystem von $\tilde{W}$ enthält, ist μ surjektiv. Wegen (1) ist μ injektiv.
QED.

10.2.6 Bezeichnung: das Element $w_0 = w_0(B)$

Seien G eine reduktive zusammenhängende lineare algebraische Gruppe, T ein maximaler Torus on G und $B \in \mathbf{B}_T$ eine Borel-Untergruppe.
Sei

$$w_0 = w_0(B) \in W(G,T)$$

das Element mit

$$w_0 R^+(B) = - R^+(B).$$

Bemerkungen
(i) w_0 existiert und ist eindeutig bestimmt (vgl. 10.1.5(i)).
(ii) w_0 ist das eindeutig bestimmte Element maximaler Länge (vgl. 10.2.2 (ii)).

10.2.7 Lemma: Zerlegungen von $U := B_u$

Seien G eine reduktive zusammenhängende lineare algebraische Gruppe, T ein maximaler Torus on G und $B \in \mathbf{B}_T$ eine Borel-Untergruppe. Wir setzen

$$U := B_u$$

Dann gilt:
(i) Für jedes $\alpha \in W(G,T)$ erzeugen die Gruppen X_α mit $\alpha \in R(w)$ eine abgeschlossene Untergruppe

$$U_w := \langle X_\alpha \mid \alpha \in R(w) \rangle$$

von U, die durch T normalisiert wird. Die Multiplikation von G induziert einen Isomorphismus von Varietäten

$$u: \times_{\alpha \in R(w)} X_\alpha \to U_w$$

(ii) Der Produkt-Morphismus

$$U_w \times U_{w_0 w} \to U$$

ist ein Isomorphismus von Varietäten.

Beweis. Zu (i). Folgt aus (6.1) und 10.1.4.

Die Surjektivitiät von u beweist man durch dieselbe Art von Argument wie im Beweis von 10.1.4: seien zwei Elemente aus dem Bild von gegeben,

$$x = \prod_{\alpha\in R(w)} x_\alpha(\xi_\alpha) \text{ und } y = \prod_{\alpha\in R(w)} x_\alpha(\eta_\alpha).$$

Nach 10.1.1 kann man dann das Produkt in der folgenden Gestalt schreiben,

$$\prod_{\alpha\in R(w)} x_\alpha(\xi_\alpha) \cdot \prod_{\alpha\in R(w)} x_\alpha(\eta_\alpha) = \prod_{\gamma\in R^+(B)} x_\gamma(P_\gamma(\xi\ ,\eta))$$

mit eindeutig bestimmten Polynomen $P_\gamma \in k[\xi, \eta]$. Wir konjugieren mit einem Element $t\in T$ und erhalten durch Vergleich

$$\gamma(t)\ P_\gamma(\xi\ ,\eta) = P_\gamma(\alpha(t)\xi\ ,\alpha(t)\eta).$$

Dabei steht $\alpha(t)\xi$ für das Tupel $(\alpha(t)\xi_\alpha \mid \alpha\in R(w))$ und analog ist $\alpha(t)\eta$ zu interpretieren. Auf der linken Seite der Gleichung können nur Wurzeln stehen, die auch rechts vorkommen, d.h. nur solche γ mit

$$\gamma = (\nu+\mu)\alpha,$$

d.h. nicht-negative Linearkombination von Wurzeln aus R(w). Nun sind Wurzeln der Gestalt

$$w\gamma = (\nu+\mu)w\alpha$$

nicht-negative Linearkombinationen negativer Wurzeln, also negativ. Auf der rechten Seite kommen also nur $\gamma\in R(w)$ vor. Ein Produkt von Elementen aus dem Bild von u liegt also wieder im Bild. Damit ist das Bild von u eine Untergruppe von U_w und damit gleich U_w. Mit anderen Worten, u ist surjektiv.
Die Tatsache, daß u ein Isomorphismus ist, ergibt sich aus dem nachfolgenden Beweis von (ii).
Zu (ii). Nach Definition überführt w_0 jede positive Wurzel in eine negative und jede negative in eine positive. Deshalb liegt eine positive Wurzel genau dann in R(w), wenn sie nicht in $R(w_0w)$ liegt,

(1) $\quad R^+(B) = R(w) \cup R(w_0w)$ (disjunkte Vereinigung).

Betrachten wir die Multiplikationsabbildungen

$$u: \times_{\alpha\in R(w)} X_\alpha \to U_w$$
$$v: \times_{\alpha\in R(w_0w)} X_\alpha \to U_{w_0w}$$

Nach 10.1.1 ist die Zusammensetzung

(2) $$\times_{\alpha\in R^+(B)} \xrightarrow{u\times v} U_w \times U_{w_0 w} \to U$$

ein Isomorphismus von Varietäten.Weil u und v surjektiv sind (nach (i)) hat man für die affinen Koordinatenringe

$$k[\times_{\alpha\in R^+(B)}] \supseteq k[U_w \times U_{w_0 w}] \leftarrow k[U].$$

Da die Komposition bijektiv ist, gilt daselbe für alle Teilabbildungen. Also sind alle Abbildungen von (2) Isomorphismen.
QED.

10.2.8 Die Doppelnebenklassen c(w), w∈W

Seien G eine reduktive zusammenhängende lineare algebraische Gruppe, T ein maximaler Torus on G und B∈ $\mathbf{B}_T$ eine Borel-Untergruppe.
Für jedes w∈W(G,T) bezeichne

$$\dot{w} \in N_G(T)$$

einen Repräsentanten von w. Wir setzen

$$C(w) := B\dot{w}B = \{b'\dot{w}b'' \mid b',b''\in B\}.$$

Eine Menge dieser Gestalt heißt Bruhat-Zelle von G.
Bemerkungen

(i) C(w) ist unabhängig von der Wahl des Repräsentanten $\dot{w}$ von w.
(ii) C(w) ist eine lokal abgeschlossene Teilvarietät von G.
(iii) Je zwei Bruhat-Zellen von G sind identisch oder disjunkt.

Beweis. Zu (i). Ist $\ddot{w}$ ein zweiter Repräsentant, so gilt

$$\ddot{w} = \dot{w}z \text{ mit } z\in Z_G(T) = T$$

(vgl. 9.3.6(ii)), also

$$B\ddot{w}B \subseteq B\dot{w}TB = B\dot{w}B.$$

Aus Symmetriegründen besteht auch die umgekehrte Inklusion.

Zu (ii). C(w) ist das Orbit von $\dot{w}$ bei einer Operation von B×B auf G, und als solches lokal abgeschlossen (vgl. (4.3.1)(i)).
Zu (iii). sei C(w') ∩ C(w") nicht leer. Dann gibt es Elemente

$$b',b'', \tilde{b}', \tilde{b}''\in B$$

mit

$$b'\dot{w}'\tilde{b}' = b''\dot{w}''\tilde{b}''.$$

Damit ist aber

$$B\dot{w}'B = Bb'\dot{w}'\tilde{b}'B = Bb''\dot{w}''\tilde{b}''B = B\dot{w}''B.$$

QED.

10.2.9 Lemma: Struktur der C(w) als algebraische Varietäten

Seien G eine reduktive zusammenhängende lineare algebraische Gruppe, T ein maximaler Torus on G und $B \in \mathbf{B}_T$ eine Borel-Untergruppe.
Seien weiter $w \in W(G,T)$,

$$w = s_1 \cdot \ldots \cdot s_h$$

eine kürzeste Zerlegung,

$$s_i = s_{\alpha_i} \text{ mit } \alpha_i \in D(B)$$

und $\dot{s}_i \in N_G(T)$ ein Repräsentant von s_i.
Dann ist der Morphismus

$$\Phi : \mathbb{A}^h \times B \to C(w), (\xi_1, \ldots, \xi_h, b) \mapsto x_{\alpha_1}(\xi_1)\, \dot{s}_1 x_{\alpha_2}(\xi_2)\dot{s}_2 \cdot \ldots \cdot x_{\alpha_h}(\xi_h)\dot{s}_h \cdot b$$

ein Isomorphismus von Varietäten.

Bemerkungen

Es gilt insbesondere

$$C(w) = X_{\alpha_1} \dot{s}_1 C(w') \text{ mit } w' = s_2 \cdot \ldots \cdot s_h$$

$$C(w) = U_{w^{-1}} \dot{w} B \text{ und } U_{w^{-1}} = \Phi(\mathbb{A}^h \times \{e\})$$

Beweis. Wir führen den Beweis durch Induktion nach der Länge

$$h = l(w).$$

Im Fall $\underline{h = 0}$ ist $w = 1$, also $C(w) = B1B = B$ und die Behauptung ist trivial.
Sei jetzt $\underline{h > 0}$. Es gilt mit $U := B_u$

$$C(w) = B\dot{w}B = U\dot{w}B \qquad \text{(wegen } B = UT \text{ und } \dot{w} \in N_G(T)\text{)}$$

$$= U_{w^{-1}} U_{w_0 w^{-1}} \dot{w} B \qquad \text{(vgl. 10.2.7(ii)).}$$

$$= U_{w^{-1}}\dot{w}(\dot{w}^{-1}U_{w_0w^{-1}}\dot{w})B$$

Nach 10.1.3 ist $\dot{w}^{-1}X_\alpha\dot{w} = X_{w^{-1}\alpha}$ für alle $\alpha\in R$, also

$$\dot{w}^{-1}U_{w_0w^{-1}}\dot{w} = \dot{w}^{-1}< X_\alpha \mid \alpha\in R(w_0w^{-1})>\dot{w}$$

$$= < X_{w^{-1}\alpha} \mid \alpha\in R(w_0w^{-1})>$$

$$= < X_{w^{-1}\alpha} \mid \alpha\in R^+ - R(w^{-1})> \quad (\text{denn } w_0R^+ = -R^+)$$

$$\subseteq B$$

Aus der obigen Darstellung für C(w) ergibt sich damit

(1) $C(w) = U_{w^{-1}}\dot{w}B$

Nach 10.2.2(i) ist

$$R(w^{-1}) = \{\alpha_1, s_1\alpha_2, \ldots, s_1\ldots s_{h-1}\alpha_h\}.$$

Nach 10.2.7 ist

$$U_{w^{-1}} = \prod_{\alpha\in R(w^{-1})} X_\alpha$$

(2) $$= X_{\alpha_1}\cdot X_{s_1\alpha_2}\cdot X_{s_1s_2\alpha_3}\cdot\ldots\cdot X_{s_1\ldots s_{h-1}\alpha_h}$$

$$= X_{\alpha_1}\dot{s}_1(X_{\alpha_2}\cdot X_{s_2s_3\alpha_4}\cdot\ldots\cdot X_{s_2\ldots s_{h-1}\alpha_h})\dot{s}_1^{-1}$$

$$= X_{\alpha_1}\dot{s}_1U_{w'^{-1}}\dot{s}_1^{-1}$$

mit $w' = s_2\cdot\ldots\cdot s_h$. Nach Induktionsvoraussetzung können wir annehmen, die Behauptung des Satzes ist richtig für w'. Es gilt

$$C(w) = U_{w^{-1}}\dot{w}B = X_{\alpha_1}\dot{s}_1U_{w'^{-1}}\dot{s}_1^{-1}\dot{w}B$$

$$= X_{\alpha_1}\dot{s}_1C(w') \quad (\text{nach (1) mit } w' \text{ anstelle von } w).$$

Insbesondere gelten die die Identitäten der obigen Bemerkung und die Abbilung ϕ ist surjektiv. Aus der Beschreibung (2) von $U_{w^{-1}}$ und 10.2.7(i) ergibt sich, daß Φ einen Isomorphismus

$$\mathbb{A}^h \to U_{w^{-1}}$$

induziert. Wegen[236]

$$U_{w^{-1}} \cap \dot{w}B = \{e\}$$

ist die Multiplikationsabbildung

$$U_{w^{-1}} \times \dot{w}B \to C(w)$$

bijektiv, d.h. Φ ist bijekiv. Durch Betrachtung der induzierten Abbildung der Tangentialräume im Ursprung sieht man, daß Φ sogar ein Isomorphismus ist[237].

QED.

10.2.10 Theorem: Lemma von Bruhat

Sei G ein reduktive zusammenhängende lineare algebraische Gruppe, $T \subseteq G$ ein maximaler Torus und $B \in \mathbf{B}_T$ eine Borel-Untergruppe. Dann gilt:

(i) G die disjunkte Vereinigung der Weyl-Kammern

$$C(w) = B\dot{w}B,\ w \in W(G,T).$$

(ii) $C(w) \neq C(w')$ für $w,w' \in W(G,T)$ verschieden.

Beweis. Zu (i). Wir setzen

---

[236] Wäre $u = \dot{w}b$ im Durchschnitt, so wäre

$$u^{-1}\dot{w}b = e$$

ein Element von $U_{w^{-1}}\dot{w}B = C(w)$, d.h. $C(w) = C(1) = B$. Insbesondere wäre $\dot{w} \in B$, also $\dot{w}B\dot{w}^{-1} \subseteq B$. Da W einfach transitiv auf den Borel-Untergruppen operiert, wäre $w = 1$ im Widerspruch zu $l(w) > 0$.

[237] Wegen der Bijektivität ist Φ ein Morphismus zwischen irreduziblen Varietäten gleicher Dimension. Auf einem erzeugenden System von Teilräumen der Gestalt $L(X_\alpha)$ induziert Φ Isomorphismen, d.h. Φ induziert einen Isomorphismus der Tangentialräume in Ursprung.
Die induzierte Abbildung der Funktionenkörper liefert eine endliche Körpererweiterung. Wegen der Surjektivität des Differentials im Ursprung ist die Körpererweiterung separabel. Wegen der Bijektivität von Φ ist sie vom Grad 1, d.h. Φ ist birational. Nach Zariskis Hauptsatz zerfällt

$$\Phi\colon \mathbb{A}^h \times B \xrightarrow{f} X \xrightarrow{g} C(w)$$

in eine offene Einbettung und einen endlichen Morphismus. Da Φ rational ist und C(w) regulär (als homogener Raum), also ganz abgeschlossen, ist g ein Isomorphismus. Da Φ sujektiv ist, ist damit auch f ein Isomorphismus.

$$G' := \cup_{w \in W} C(w)$$

und

$$G'' := \{g \in G \mid gG' = G'\}.$$

Offensichtlich ist G" eine Untergruppe von G. Es reicht zu zeigen,

(1) $$G'' = G,$$

denn dann ist G' stabil bei Linksmultiplikation mit Elementen aus G, also auch G' = G. Nach 10.1.3 wird G von T und den $X_{\pm\alpha}$ mit $\alpha \in D(B)$ erzeugt.

Es reicht also zu zeigen,

(2) $$T \subseteq G'' \text{ und } X_{\pm\alpha} \subseteq G'' \text{ für jedes } \alpha \in D(B).$$

Nach Definition von C(w) gilt $B \cdot C(w) = C(w)$, also auch $BG' = G'$, also $B \subseteq G''$, also

$$T \subseteq G'' \text{ und } X_{\alpha} \subseteq G'' \text{ für alle } \alpha \in R^{+}.$$

Es reicht also, zu zeigen,

(3) $$X_{-\alpha} \in G'' \text{ für alle } \alpha \in D(B).$$

Nach 10.1.3 ist

$$\dot{s}_{\alpha} X_{\alpha} \dot{s}_{\alpha}^{-1} = X_{s_{\alpha}(\alpha)} = X_{-\alpha}.$$

Es reicht also zu zeigen,

(4) $$\dot{s}_{\alpha} G' = G' \text{ für jedes } \alpha \in D(B).$$

Es reicht zu zeigen,

(5) $$\dot{s}_{\alpha} G' \subseteq G' \text{ für jedes } \alpha \in D(B).$$

Weil nämlich $s_{\alpha} \in W$ selbstinvers ist, ist $\dot{s}_{\alpha}^{-1}$ ebenfalls ein Repräsentant von s_{α}, d.h. mit (5) gilt auch $\dot{s}_{\alpha}^{-1} G' \subseteq G'$ also $G' \subseteq \dot{s}_{\alpha} G'$, d.h. es besteht auch die zu (5) umgekehrte Inklusion.

Es reicht zu zeigen,

(6) $$\dot{s}_{\alpha} C(w) \subseteq G' \text{ für jedes } \alpha \in D(B) \text{ und jedes } w \in W.$$

<u>1. Schritt</u>. $X_{\alpha} \dot{s}_{\alpha} C(w) = C(s_{\alpha} w)$ falls $l(s_{\alpha} w) = l(w) + 1$.

(Insbesondere gilt also (6) im Fall $l(s_{\alpha} w) = l(w) + 1$).

Wir wählen eine kürzeste Zerlegung

$$w = s_1 \cdot \ldots \cdot s_h$$

und erhalten eine kürzeste Zerlegung

$$s_\alpha w = s_\alpha s_1 \cdot \ldots \cdot s_h \ .$$

Nach 10.2.9 gilt damit

$$C(s_\alpha w) = X_\alpha \dot{s}_\alpha X_{\alpha_1} \cdot \dot{s}_1 X_{\alpha_2} \cdot \dot{s}_2 \cdot \ldots \cdot X_{\alpha_h} \dot{s}_h \cdot B = X_\alpha \dot{s}_\alpha C(w),$$

Wir haben noch den folgenden Fall zu behandeln (vgl. 10.2.2(iii)).

2. Schritt. $\dot{s}_\alpha C(w) \subseteq C(s_\alpha w) \cup C(w)$ falls $l(s_\alpha w) = l(w) - 1$

(Insbesondere gilt also (6) im Fall $l(s_\alpha w) = l(w) - 1$).

Wir wählen eine kürzeste Zerlegung

$$s_\alpha w = s_1 \cdot \ldots \cdot s_h$$

und erhalten eine kürzeste Zerlegung

$$w \ (= s_\alpha s_\alpha w) = s_\alpha s_1 \cdot \ldots \cdot s_h$$

Nach 10.2.9 gilt damit

(7) $$C(w) = X_\alpha \dot{s}_\alpha X_{\alpha_1} \cdot \dot{s}_1 X_{\alpha_2} \cdot \dot{s}_2 \cdot \ldots \cdot X_{\alpha_h} \dot{s}_h \cdot B = X_\alpha \dot{s}_\alpha C(s_\alpha w)$$

also

$$\dot{s}_\alpha C(w) = \dot{s}_\alpha X_\alpha \dot{s}_\alpha C(s_\alpha w) = X_{s_\alpha(\alpha)} C(s_\alpha w).$$

Das letzte Gleichheitszeichen ergibt sich dabei aus 10.1.3. Man beachte $\dot{s}_\alpha$ unterscheidet sich von $\dot{s}_\alpha^{-1}$ nur durch einen Faktor aus dem Zentralisator $Z_G(T) = T$ (vgl. 9.3.6(ii)). Damit ist

(8) $$\dot{s}_\alpha C(w) = X_{-\alpha} C(s_\alpha w) \subseteq G_\alpha \cdot C(s_\alpha w)$$

Nun ist

$$G_\alpha := Z_G(\mathrm{Ker}\ \alpha^0)$$

eine Untergruppe vom halbeinfachen Rang 1 (vgl. 9.1.5). Nach 8.2.3 (i) ist G_α Vereinigung von zwei Doppelrestklassen[238],

$$\begin{aligned} G_\alpha &= (G_\alpha \cap B) \cup (G_\alpha \cap (B \dot{s}_\alpha B)) \\ &\subseteq (G_\alpha \cap B) \cup (G_\alpha \cap C(s_\alpha)) \end{aligned}$$

---

[238] Man beachte, $G_\alpha \cap B$ ist eine Borel-Untergruppe von G_α (nach 7.3.5(ii))

$$= (G_\alpha \cap B) \cup (G_\alpha \cap (U_{s_\alpha} \dot{s}_\alpha B))$$

Man beachte, nach Formel (1) von 10.2.9 gilt $C(w) = U_{w^{-1}} \dot{w} B$. Nach Definition ist $U_{s_\alpha} = \langle X_\beta \mid \beta \in R(s_\alpha) \rangle = X_\alpha$, also

$$X_{-\alpha} \subseteq G_\alpha \subseteq (G_\alpha \cap B) \cup (G_\alpha \cap (X_\alpha \dot{s}_\alpha B)) \subseteq B \cup X_\alpha \dot{s}_\alpha B,$$

also

$$X_{-\alpha} B \subseteq B \cup X_\alpha \dot{s}_\alpha B$$

Zusammen mit (8) erhalten wir

$$\dot{s}_\alpha C(w) = X_{-\alpha} C(s_\alpha w) \subseteq C(s_\alpha w) \cup X_\alpha \dot{s}_\alpha C(s_\alpha w)$$

und mit (7)

$$\dot{s}_\alpha C(w) = X_{-\alpha} C(s_\alpha w) \subseteq C(s_\alpha w) \cup C(w)$$

Zu (ii). Es reicht zu zeigen:

(10) Mit $w, w' \in W$, $l(w) \leq l(w')$ und $C(w) = C(w')$ gilt $w = w'$.

Wir beweisen diese Aussage durch Induktion nach $h = l(w)$.

Der Fall $h = 0$. Es gilt $w = 1$, also

$$B = C(w) = C(w') = B \dot{w} B,$$

also

$$\dot{w}' \in B \cap N_G(T) = Z_G(T)$$

(Nach 6.12(ii) ist die Weyl-Gruppe im auflöbarem Fall trivial). Mit anderen Worten, das durch $\dot{w}'$ repräsentierte Element w' von W ist das neutrale Element, $w' = 1 = w$.

Der Fall $h > 0$. Wir schreiben w in der Gestalt

$$w = s_\alpha w_1 \text{ mit } l(w_1) = l(w) - 1 = h-1.$$

Wie wir oben gesehen haben (vgl. die Argumente nach Formel (6)) gilt dann

$$C(w) \supseteq \dot{s}_\alpha C(w_1).$$

Damit gilt[239]

$$C(w_1) \subseteq \dot{s}_\alpha^{-1} C(w) = \dot{s}_\alpha C(w) = \dot{s}_\alpha C(w')$$

Im Fall $l(s_\alpha w') = l(w') + 1$ ist $\dot{s}_\alpha C(w') \subseteq C(s_\alpha w')$, also $C(w_1) = C(s_\alpha w')$, und nach Induktionsvoraussetzung folgt

$$w_1 = s_\alpha w'.$$

Multiplikation von links mit s_α liefert die Behauptung $w = w'$. Wir können also annehmen,

$$l(s_\alpha w') = l(w') - 1.$$

In dieser Situation haben wir oben gesehen (vgl. 2. Schritt)

$$\dot{s}_\alpha C(w') \subseteq C(s_\alpha w') \cup C(w'),$$

zusammen also

$$C(w_1) \subseteq C(s_\alpha w') \cup C(w').$$

Wir wenden die Induktionsvoraussetzung auf w_1 an und erhalten

$$w_1 = s_\alpha w' \text{ oder } w_1 = w'.$$

Der zweite Fall ist nicht möglich, denn es gilt $l(w_1) < l(w) \leq l(w')$. Also gilt

$$w_1 = s_\alpha w'.$$

Multiplikation von links mit s_α liefert die Behauptung $w = w'$.

QED.

10.2.11 Folgerung: das Produkt von Zellen

Sei G ein reduktive zusammenhängende lineare algebraische Gruppe, $T \subseteq G$ ein maximaler Torus, $B \in \mathbf{B}_T$ eine Borel-Untergruppe und

$$\alpha \in D(B)$$

eine einfache Wurzel. Dann gilt für jedes $w \in W(G,T)$:

1. $C(s_\alpha) \cdot C(w) = C(s_\alpha w)$ falls $l(s_\alpha w) = l(w) + 1$.
2. $C(s_\alpha) \cdot C(w) \subseteq$[240] $C(s_\alpha w) \cup C(w)$ falls $l(s_\alpha w) = l(w) - 1$.

Beweis. Im Beweis von 10.2.10 haben wir gesehen , es gilt

---

[239] $\dot{s}_\alpha^{-1}$ und $\dot{s}_\alpha$ unterscheiden sich nur um einen Faktor aus $Z_G(T) = T$.

[240] Im Original steht das Gleichheitszeichen.

(1) $X_\alpha \dot{s}_\alpha \cdot C(w) = C(s_\alpha w)$ falls $l(s_\alpha w) = l(w) + 1$

und

(2) $\dot{s}_\alpha \cdot C(w) \subseteq C(s_\alpha w) \cup C(w)$ falls $l(s_\alpha w) = l(w) - 1$.

Multiplikation von links mit B liefert die Behauptung.
QED.

10.2.12 Folgerung: Je zwei Borel-Untergruppen enthalten einen gemeinsamen maximalen Torus

Sei G eine reduktive zusammenhängende lineare algebraische Gruppe. Dann liegt im Durchschnitt von je zwei Borel-Untergruppen von G ein maximaler Torus von G.

Beweis. Seien B und B' gegebene Borel-Untergruppen. Dann gilt

$$B' = gBg^{-1} \text{ mit } g \in G.$$

Nach dem Lemma von Bruhat (10.2.10) kann man g in der Gestalt

$$g = b\dot{w}b'$$

schreiben mit $b,b' \in B$ und $w \in W(G,T)$. Dann ist

$$T' := bTb^{-1}$$

ein maximaler Torus, der sowohl in B als auch in B' liegt:

$$B' = (b\dot{w}b')B(b\dot{w}b')^{-1} = b\dot{w}B\dot{w}^{-1}b^{-1} \supseteq b\dot{w}T\dot{w}^{-1}b^{-1} = bTb^{-1}.$$

Man beachte, $\dot{w} \in N_G(T)$.

QED.

10.2.13 Folgerung: der Rand einer Zelle

Seien G eine reduktive zusammenhängende lineare algebraische Gruppe, T ein maximaler Torus von G und $B \in \mathbf{B}_T$ eine Borel-Untergruppe. Weiter sei $w_0 \in W(G,T)$ das Element maximaler Länge.

(i) Jedes C(w) mit $w \in W$ ist eine lokal abgeschlossene Teilvarietät von G. Deren Rand $\overline{C(w)} - C(w)$ ist Vereinigung von C(w') mit $l(w') < l(w)$.

(ii) $C(w_0)$ ist eine affine offene dichte Untermenge von G.

(iii) $C(w_0) \cup (\cup_{\alpha \in D(B)} C(s_\alpha w_0))$ ist eine offene Teilmenge von G. Alle Komponenten des Komplements dieser Teilmenge haben eine Dimension < dim G - 2.

Beweis. Zu (i). Die lokale Abgeschlossenheit wurde bereits bewiesen (vgl. Bemerkung (ii) von 10.2.8)). Aus dieser lokalen

Abgeschlossenheit und der Irreduzibilität von C(w) (vgl. 10.2.9) folgt, daß C(w) offen ist in seiner Abschließung[241]. Insbesondere ist

$$\partial C(w) = \overline{C(w)} - C(w).$$

Da C(w) bei der Operation von B×B auf G stabil ist, gilt dasselbe für die Abschließung $\overline{C(w)}$ und für die Differenz $\overline{C(w)} - C(w)$. Ein Element dieser Differenz hat nach dem Lemma von Bruhat (10.2.10) die Gestalt

$$b\dot{w}'b' \in \overline{C(w)} - C(w).$$

Wegen der B×B-Stabilität gilt dann aber

$$C(w') \subseteq \overline{C(w)} - C(w).$$

Die Differenz ist also Vereinigung von Bruhat-Zellen. Diese müssen eine kleinere Dimension haben als C(w), d.h. es gilt

$$l(w') = \dim C(w') - \dim B < \dim C(w) - \dim B = l(w)$$

(vgl. 10.2.9).

Zu (ii). Nach 10.2.9 ist $C(w_0)$ affin und die einzige Zelle mit derselben Dimension wie G, d.h.

$C(w_0) \supseteq$ G - endlich viele Teilvarietäten kleinerer Dimension.

Deshalb gilt

$$\overline{C}(w_0) = G.$$

Zusammen mit (i) erhalten wir

$$C(w_0) = \overline{C}(w_0) - \partial C(w_0) = G - \partial C(w_0).$$

Insbesondere ist $C(w_0)$ eine offene Teilmenge von G.

Zu (ii). Nach (ii) ist

$$G - C(w_0) = \overline{C}(w_0) - C(w_0)$$

und nach (i) ist die Differenz rechts Vereinigung von Zellen einer Dimension < dim G. Die Zellen der Gestalt $C(s_\alpha w_0)$ mit $\alpha \in D(B)$ sind gerade die Zellen der Dimension dim G - 1. Also ist das Komplement der Menge von (iii) gerade die Vereinigung aller Zellen mit einer Dimension ≤ dim G - 2. Nach (i) ist diese Menge abgeschlossen.

QED.

Bemerkungen

---

[241] C(w) ist der Durchschnitt aus einer abgeschlossenen und einer offenen Menge,

$$C(w) = F \cap U \text{ mit F abgeschlossen in G und U offen.}$$

Weil C(w) irreduzibel ist, können wir annehmen, F ist irreduzibel. Dann ist aber F∩U offen und dicht in F, d.h. F ist die Abschließung von F∩U. Mit anderen Worten, C(w) = F∩U ist offen in seiner Abschließung F.

(i) Die offene Menge $C(w_0)$ nennt man die große Zelle von G bezüglich T und B.

(ii) Das Lemma von Bruhat (10.2.10) liefert auch eine Beschreibung der geometrischen Struktur von

$$G/B,$$

der projektiven Varietät aller Borel-Untergruppen von G (vgl. 7.3.10).

(iii) Für jedes $w \in W(G,T)$ bezeichne

$$X_w$$

das Bild von C(w) bei der natürlichen Abbildung $G \to G/B$. Wir nennen die X_w Bruhat-Zellen von G/B und deren Abschließungen Schubert-Zellen.

10.2.14 Folgerung: Zell-Zerlegung von G/B

Seien G eine reduktive zusammenhängende lineare algebraische Gruppe, T ein maximaler Torus von G und $B \in \mathbf{B}_T$ eine Borel-Untergruppe.

(i) Für jedes $w \in W(G,T)$ ist X_w eine lokal abgeschlossene Teilvarietät von G/B und als solche isomorph zu $\mathbb{A}^{l(w)}$.

(ii) G/B ist die disjunkte Vereinigung der X_w mit $w \in W(G,T)$.

Beweis. Folgt aus dem Lemma von Bruhat (10.2.10) und der Gestalt der $C(w) = B\dot{w}B$.

QED.

10.2.14 Folgerung: eine Produkt-Zerlegung der Elemente von G

Seien G eine reduktive zusammenhängende lineare algebraische Gruppe, T ein maximaler Torus von G und $B \in \mathbf{B}_T$ eine Borel-Untergruppe.

Dann läßt sich jedes Element $g \in G$ auf genau eine Weise in der Gestalt

$$g = u\dot{w}b \text{ mit } w \in W,\ u \in U_{w^{-1}},\ b \in B$$

schreiben.

Beweis. Folgt aus dem Lemma von Bruhat (10.2.10) und (10.2.9).

QED.

10.2.15 Aufgaben

Gruppe, T ein maximaler Torus von G und $B \in \mathbf{B}_T$ eine Borel-Untergruppe. Wir setzen

$$W := W(G,T)$$

$R^+ := R^+(B)$
$D := D(B)$
$S := S(B)$

(1) Aufgabe

(a) Sei $w = s_1 \cdot \ldots \cdot s_h$ eine kürzeste Zerlegung von $w \in W$. Für jedes $s \in S$ mit $l(sw) < l(w)$ gibt es ein i mit

$$sw = s_1 \cdot \ldots \cdot s_{i-1} \cdot s_{i-2} \cdot \ldots \cdot s_h .$$

(b) Seien $w_0 \in W$ das Element maximaler Länge und

$$w_0 = s_1 \cdot \ldots \cdot s_N$$

eine kürzeste Zerlegung. Dann gibt es für jedes $w \in W$ mit $l(w) = h$ eine Teilfolge

$$i_1 < i_2 < \ldots < i_h$$

von { 1 , ... , N } derart, daß gilt

$$w = s_{i_1} \cdot \ldots \cdot s_{i_h} .$$

(c) Ist $w = s_1 \cdot \ldots \cdot s_h$ eine kürzeste Zerlegung von $w \in W$, so gibt es eine kürzeste Zerlegung der Gestalt

$$w_0 = s_1 \cdot \ldots \cdot s_h \cdot s_{h+1} \cdot \ldots \cdot s_N .$$

(2) Aufgabe

Sei X := G/B. Man betrachte X als die Menge der Borel-Untergruppen von G. Die Gruppe G operiert auf X×X durch

$$(g, xB, x'B) \mapsto (gxB, gx'B).$$

(a) Bezeichne $O(w) \subseteq X \times X$ das Orbit von (B,wB), für $w \in W$. Dann ist durch

$$W \to \{ \text{G-Orits in } X \times X \}, \; w \mapsto O(w),$$

eine Bijektion definiert. (Hinweis: man zeige, dies ist eine Reformulierung des Lemmas von Bruhat).

(b) Man sagt von zwei Borel-Untergruppen B',B" von G, sie sind in der Position w, wenn gilt $(B', B") \in O(w)$. Man sagt, B' und B" sind entgegengesetzt, wenn $B' \cap B"$ ein maximaler Torus ist. Man zeige, B' und B" sind genau dann entgegengesetzt, wenn sid in der Position w_0. Dabei bezeichne $w_0 \in W$ das Element maximaler Länge.

(3) Aufgabe

Sei $C(w_0)$ die große Zelle von G. Dann gilt

$$G = \cup_{w \in W} \dot{w} C(w_0)$$

(Hinweis: Man gehe über zu X = G/B. Ist $X' := \cup_{w \in W} \dot{w} X_{w_0}$ und ist $X - X' \neq \emptyset$, so würde es einen T-invarianten Punkt in X - X' geben, was zu einem Widerspruch führt).

(4) Aufgabe

Sei $w = s_1 \cdot \ldots \cdot s_h$ eine kürzeste Zerlegung von $w \in W$ mit $s_i = s_{\alpha_i}$ und $\alpha_i \in D$. Bezeichne P_i die parabolische Untergruppe

$$P_i := \langle B, X_{\alpha_i}, X_{-\alpha_i} \rangle \qquad (1 \leq i \leq h).$$

(a) Die $P_1 \cdot \ldots \cdot P_h$ ist eine irreduzible abgeschlossene Teilmenge von G, welche disjunkte Vereinigung von Bruhat-Zellen C(w') ist (Hinweis: man leite dies aus 7.2.11(9) ab durch Induktion nach h).

(b) Sei $S_w := \{s_{i_1} \cdot \ldots \cdot s_{i_m} \mid 1 \leq i_1 \leq \ldots \leq i_m \leq h\}$. Man zeige, es gilt

$$P_1 \cdot \ldots \cdot P_h = \cup_{w' \in S_w} C(w')$$

(Hinweis: man verwende $P_i = B \cup B \dot{s}_i B$).

(c) S_w hängt nicht von der spezielle Wahl der kürzesten Zerlegung von w ab. Es gilt

$$\overline{C(w)} = \cup_{w' \in S_w} C(w') \text{ und } \overline{X}_w = \cup_{w' \in S_w} X_{w'},$$

(d) Wir schreiben $w' \leq w$ für $w' \in S_w$. Dann definiert $\leq$ eine Halbordnung auf W (die Bruhat-Ordnung).

(5) Aufgabe

Seien $w, w' \in W$ Elemente der Weyl-Gruppe mit $l(w) \leq l(w')$.

(a) Gilt $w \neq w'$, so ist $\overline{X}_w \cap \dot{w}_0 \overline{X}_{w_0 w'} = \emptyset$ (Hinweis: sei Y der Durchschnitt. Ist $Y \neq \emptyset$, so enthält Y einen Punkt $\dot{w}''B$, der bei T fest bleibt. Nach 4(c) gilt dann $l(w'') \leq l(w)$, $l(w_0 w'') \leq l(w_0 w')$, wobei die Gültigkeit des Gleichheitszeichens äquivalent ist zu $w''=w$ bzw. $w'' = w'$. Man zeige, dies führt zu einem Widerspruch).

(b) $\bar{X}_w \cap \dot{w}_0 \bar{X}_{w_0 w} = \dot{w}B$ (Hinweis: man leite aus (a) ab, daß es reicht zu zeigen, es gilt $X_w \cap \dot{w}_0 X_{w_0 w} = \dot{w}B$. Man leite letzteres von 10.2.7 (iii) ab).

(6) Aufgabe

Seien wie in (2) $X := G/B$ und $O(w) \subseteq X \times X$ die Menge alle Paare der Gestalt (B, wB) $(w \in W)$.

(a) Man zeigen $\overline{O(w)} = \cup_{w' \leq w} O(w')$ (Hinweis: man verwende 4(c)).

(b) Sei

$$w = s_1 \cdot \ldots \cdot s_h$$

eine kürzeste Zerlegung. Wir definieren

$$O(s_1, \ldots, s_h) := \{ (B_0, \ldots, B_h) \in X^{h+1} \mid (B_{i-1}, B_i) \in \overline{O(s_i)} \text{ für } i = 1, \ldots, h \}$$

Man zeige, dies ist eine abgeschlossene Teilvarietät von X^{h+1}. Die Projektionsabbildung

$$O(s_1, \ldots, s_h) \to O(s_1, \ldots, s_{h-1})$$

ist ein surjektiver Morphismus, dessen Fasern sämlich isomorph sind zu $\mathbb{P}^1$.

(c) Die Abbildung

$$\pi: O(s_1, \ldots, s_h) \to X \times X \,, (B_0, \ldots, B_h) \to (B_0, B_h),$$

ist ein Morphismus mit dem Bild $\overline{O(w)}$. Die Einschränkung von π auf $\pi^{-1}(O(w))$ ist ein Isomorphismus. (Man kann zeigen, π ist eine "Auflösung" von $\overline{O(w)}$, vgl. [13, no. 3])

(7) Aufgabe

Seien $G = GL_n$ (vgl. 7.2.11(4)) und

$$(V_1, \ldots, V_{n-1}) \text{ und } (V'_1, \ldots, V'_{n-1}).$$

zwei vollständige Fahnen von $V = k^n$. Es existiere genau eine Permutation $\sigma \in S_n$ derart, daß es eine Basis $e_1, \ldots, e_n$ von V gibt mit

$$V_i = ke_1 + \ldots + ke_i$$
$$V'_i = ke_{\sigma 1} + \ldots + ke_{\sigma i}$$

für $i = 1, \ldots, n-1$. Man gebe in diesem Spezialfall einen anderen Beweis des Lemmas von Bruhat (vgl. Aufgabe (2) und 7.3.11(6)).

(8) Aufgabe

Seien $t \in T$ und $g = u\dot{w}b \in G$ wie in 10.2.14. Liegt g außerdem im Zentralisator $Z_G(T)$, so liegen u, b, $\dot{w}$ in $Z_G(t)$. Man zeigen $Z_G(t)$ wird erzeugt von $Z_G(t)^0$ und den $\dot{w}$ mit $w \in W$ und $w \cdot t = t$.

(9) Aufgabe

Sei G definiert über $\mathbb{F}_q$ und sei F der Frobenius-Morphismus (3.3.15). Wir nehmen an, es gilt

$$FB = B.$$

Dann operiert F auch auf der Menge $X = G/B$ der Borel-Untergruppen von G.

(a) Für $w \in W$ setzen wir

$$X(w) := \{B' \in X \mid B' \text{ und } FB' \text{ sind in der Position } w\}.$$

Dann ist $X(w)$ eine lokal abgeschlossene Teilmenge von X, auf welcher die Gruppe G^F der Fixpunkte des Frobenius operiert.

(b) Seien $G = GL_n$ und $B = \mathbf{T}_n$ (obere Dreiecksmatrizen). Es gilt

$$W \cong S_n$$

(vgl. 10.1.14(1)). Bezeichne w die zyklische Permutation $(1,2,\ldots,n)$. Unter Verwendung von Aufgabe (7) zeige man, $X(w)$ ist die Menge der Fahnen $(V_1,\ldots,V_{n-1})$ in $V = k^n$, für welche es ein $v \in V$ gibt mit der Eigenschaft, daß $v, Fv, \ldots, F^{i-1}v$ eine Basis von V_i ist. Man definiere eine Bijektion

$$X(w) \to Y\ (\subseteq \mathbb{A}^{n-1})$$

auf das Komplement der Vereinigung Y aller rationalen Hyperebenen des $\mathbb{A}^{n-1}$ (d.h. der Hyperebenen, die durch eine Gleichung mit Koeffizienten in $\mathbb{F}_q$ gegeben sind). Man zeige, es gibt eine Bijektion von $X(w)$ auf die Menge aller $x = [x,\ldots,x] \in \mathbb{P}^{n-1}$ mit

$$\det \begin{pmatrix} x_1 & \ldots & x_n \\ x_1^q & \ldots & x_n^q \\ \ldots & \ldots & \ldots \\ x_1^{q^{n-1}} & \ldots & x_n^{q^{n-1}} \end{pmatrix} \neq 0.$$

Zu (1) (a).

Sei $sw = s'_1 \cdot \ldots \cdot s'_{h-1}$ ein kürzeste Zerlegung. Dann ist

$$w = s \cdot s'_1 \cdot \ldots \cdot s'_{h-1}$$

eine kürzeste Zerlegung, also sind auch

$$w^{-1} = s'_{h-1} \cdot \ldots \cdot s'_1 \cdot s = s_h \cdot \ldots \cdot s_1$$

kürzeste Zerlegungen. Nach 10.2.2 (v) entspricht das Kürzen von s auf der linken Seite dem Weglassen irgendeines Faktors rechts:

$$s'_{h-1} \cdot \ldots \cdot s'_1 = s_h \cdot \ldots \cdot s_{i+1} s_{i-1} \cdot \ldots \cdot s_1$$

Wir gehen zum Inversen über und erhalten

$sw = s'_1 \cdot \ldots \cdot s'_{h-1} = s_1 \cdot \ldots \cdot s_{i-1} \cdot s_{i-2} \cdot \ldots \cdot s_h$.

Zu (1)(b).

Wir führen den Beweis durch Induktion nach $N - l(w)$. Im Fall $l(w) = N$ gilt $w = w_0$ und die Behauptung ist trivial. Sei jetzt

$$l(w) < N.$$

Es reicht zu zeigen, daß es ein $s \in S$ gibt mit

$$l(sw) = l(w) + 1,$$

denn dann gibt es nach Induktionsvorsaussetzung eine Teilfolge

$$i_1 < i_2 < \ldots < i_{h+1}$$

von $\{ 1 , .. , N\}$ mit

$$sw = s_{i_1} \cdot \ldots \cdot s_{i_{h+1}} .$$

Nach (1)(a) entspricht dann das Weglassen von s auf der linken Seite gerade dem Weglassen eines Faktor rechts, d.h. es gilt die Behauptung.

Beweisen wir also die Existenz eines $s \in S$ mit $l(sw) = l(w) + 1$. Nach 10.2.2. (iii) ist die Längenbedingung äquivalent zur Existenz eines $\alpha \in D$ mit

$$w^{-1}\alpha > 0.$$

Letztere Bedingung ist nach 10.2.2 (ii) äquivalent zu

$$\alpha \in D - R(w^{-1}).$$

Wegen

$$\# R(w^{-1}) = l(w^{-1}) = l(w) < N = \# R^+$$

gibt es zumindest eine positive Wurzel

$$\alpha \in R^+ - R(w^{-1}).$$

Wir schreiben α als nicht-negative Linearkombination einfacher Wurzeln α_i ,

$$\alpha = n_1\alpha_1 + \ldots + n_r\alpha_r \text{ mit } n_i > 0 \text{ und } \alpha_i \in D$$

(vgl. 10.1.12 (iii)). Wäre $w^{-1}(\alpha_i) < 0$ für jedes i, so wäre auch $w^{-1}(\alpha) < 0$ im Widerspruch zur Wahl von α. Also gibt es ein i mit

$$\alpha_i \in D - R(w^{-1}).$$

Zu (1)(c).

Betrachten wir die kürzeste Zerlegung

$$w^{-1} = s_h \cdot \ldots \cdot s_1$$

Beim Beweis von (1)(b) hat sich ergeben, daß es im Fall

$$l(w^{-1}) = l(w) < N$$

ein $s \in S$ mit

$$l(s\, w^{-1}) = l(w) + 1.$$

Durch wiederholtes Anwenden dieser Tatsache finden wir Elemente

$$s_{h+1}, \ldots, s_N \in S$$

derart, daß

$$s_N \cdot \ldots \cdot s_{h+1} \cdot s_h \cdot \ldots \cdot s_1$$

die maximale Länge N hat. Dann hat aber auch das inverse Element

$$s_1 \cdot \ldots \cdot s_h s_{h+1} \cdot \ldots \cdot s_N$$

diese maximale Länge. Da es genau ein Element maximaler Länge gibt, folgt

$$w_0 = s_1 \cdot \ldots \cdot s_h s_{h+1} \cdot \ldots \cdot s_N.$$

10.3 Parabolische Untergruppen

10.3.0 Voraussetzungen und Bezeichnungen

Seien G eine reduktive zusammenhängende lineare algebraische Gruppe, $T \subseteq G$ ein maximaler Torus und B eine Borel-Untergruppe von G, welche T enthält.

Das Lemma von Bruhat gestattet es uns auch, eine explizite Beschreibung der parabolischen Untegruppen von G, welche B enthalten, anzugeben.

Sei $I \subseteq D(B)$ eine Menge von einfachen Wurzeln und bezeichne

$$W_I \subseteq W(G,T)$$

die Untergruppe der Weyl-Gruppe, welche erzeugt wird von den Spiegelungen s_α mit $\alpha \in I$,

$$W_I := < s_\alpha \mid \alpha \in I >.$$

Weiter sei

$$R_I := \{ \alpha \in R \mid \alpha \in \sum_{\beta \in I} \mathbb{Q}\beta \}$$

$$R_I^+ := R_I \cap R^+(G,T)$$

$$S_I := (\cap_{\alpha \in I} \mathrm{Ker}\ \alpha)^0$$

$$L_I := Z_G(S_I)$$

Dann ist L_I ein zusammenhängende reduktive lineare Untergruppe von G (vgl. 9.3.6(i)) mit dem maximalen Torus T und der Borel-Untergruppe $B \cap L_I$ (vgl. 7.3.5 (ii)).

10.3.1 Proposition: die Wurzeln von L_I

Seien G eine reduktive zusammenhängende lineare algebraische Gruppe, $T \subseteq G$ ein maximaler Torus, B eine Borel-Untergruppe von G, welche T enthält und $I \subseteq D(B)$ eine Menge von einfachen Wurzeln. Dann gilt:

$$R(L_I, T) = R_I$$

$$W(L_I, T) = W_I$$

$$R^+(B \cap L_I) = R_I^+$$

$$D(B \cap L_I) = I$$

Beweis. 1. Schritt: die Wurzeln von L_I .

Die Wurzeln der reduktiven Gruppe L_I bezüglich T sind gerade die von Null verschiedenen Gewichte von T in $L(L_I)$ (vgl. 9.3.8(i)). Die Lie-Algebra $L(L_I)$ ist gerade die Fixpunktmenge von S_I in L(G) (vgl. 4.4.7), d.h.

$$L(L_I) =^{242} L(T) + \sum_{\alpha(S_I)=1} L(G)_\alpha \ .$$

Die Summe wird erstreckt über alle Wurzeln von G, die im Kern der Einschränkungsabbildung

---

[242] Genauer: die Lie-Algebra des Zentralisators des Torus S_I ist gleich

$$\{X \in L(G) \mid sX = X \text{ für alle } s \in S_I\}.$$

Die obige Zerlegung erhält man aus der Zerlegung von L(G) nach den Wurzelräumen.

$$X(T) \to X(S_I)\ ,\ \chi \mapsto \chi|_{S_I}$$

liegen. Dieser Kern ist gerade die Charaktergruppe von T/S_I [243] und ist eine freie abelsche Gruppe vom Rang

$$\text{rk } X(T/S_I) = \text{rk } X(T) - \text{rk } X(S_I) = \dim T - \dim S_I \leq^{244} \#I\ .$$

Weil die Elemente von $I \subseteq X(T)$ auf S_I identisch Null sind, kann man sie sogar als Element von des Kern auffassen,

$$I \subseteq X(T/S_I).$$

Nun sind die Elemente von I einfache Wurzeln von G, also linear unabhängig (vg. 10.1.12(iii)), d.h. es gilt $\text{rk } X(T/S_I) \geq \#I$. Zusammen gilt also

$$\text{rk } X(T/S_I) = \#I$$

und die linear unabhängigen Wurzeln von I erzeugen die rationale Charaktergruppe,

$$X(T/S_I)_{\mathbb{Q}} = \sum_{\alpha \in I} \mathbb{Q}\alpha\ (= \text{Ker}(X(T) \to X(S_I))_{\mathbb{Q}}$$

Die Menge der Wurzeln von L_I besteht damit gerade aus denjenigen Wurzeln von G, die rationale Linearkombinationen der Elemente von I sind,

$$R(L_I\ ,\ T) = R \cap \sum_{\alpha \in I} \mathbb{Q}\alpha = R_I\ .$$

2. Schritt: die positiven und die einfachen Wurzeln von L_I.

Da die Wurzeln von L_I Linearkombinationen der einfachen Wurzeln von G aus I sind, sind sie sogar ganzzahlige Linearkombinationen der Elemente von I (vgl. 10.1.12(iii)), wobei entweder alle Koeffizienten ≥ 0 oder alle Koeffiziente ≤ 0 sind. Insbesondere ist

$$R^+(L_I\ ,\ T) = R(L_I\ ,\ T) \cap R^+ = R_I^+.$$

---

[243] Man betrachte die kurze exakte Sequenz von Tori

$$0 \to S_I \to T \to T/S_I \to 0$$

und die zugehörige kurze exakte Sequenz der Charaktergruppen.

[244] Der Torus wird lokal in T von #I Gleichungen definiert, hat also in T eine Kodimensiion $\leq$ #I.

Es handelt sich um einfache Wurzeln von L_I, wenn sie sich nicht als echte positive Linearkombinationen positiver Wurzeln schreiben lassen, d.h.

$$D(B \cap L_I) =^{245} I.$$

3. Schritt: die Weyl-Gruppe.
Nach 10.1.12(i) ist

$$W(L_I, T) = < s_\alpha \mid \alpha \in I > = W_I$$

QED.
Bemerkung
Nach Konstruktion gilt

$$W_I \subseteq W(G,T).$$

Die Länge eines Elements $w \in W_I$ kann man also in W_I und in $W(G,T)$ berechnen. In beiden Fällen erhält man denselben Wert.
Beweis. Seien

$$w = s_1 \cdot \ldots \cdot s_h$$

eine kürzeste Zerlegung in W_I und

(1) $$\alpha_1, \ldots, \alpha_r$$

die positiven Wurzeln von R. Die Spiegelungen zu den einfachen Wurzeln sind gerade die Elemente der Länge 1, d.h. derart. daß beim Anwenden von s_α auf die Wurzeln (1) genau eine Wurzel ihr Vorzeichen wechselt (vgl. 10.1.11(i)). Wir wenden jetzt nacheinander die Spiegelungen $s_h, s_{h-1}, \ldots, s_1$ auf die Wurzeln (1) an. Bei jedem Schritt erhöht sich die Anzahl der negativen Wurzeln um höchstens 1. Wenn sie sich nicht um 1 erhöht so sinkt sie um 1 (d.h. eine negative Wurzel wird in eine positive überführt und alle anderen Wurzeln behalten ihr Vorzeichen).

Da die obige Zerlegung minimal in W_I ist, kann der zweite Fall nicht eintreten und alle Vorzeichenänderungen treten bereits bei den positiven Wurzeln von L_I auf. Die Wurzeln, welche nicht zu L_I gehören

---

[245] Es gilt "$\supseteq$" wegen $R_I^+ \supseteq I$ und weil eine Zerlegbarkeit in R_I^+ eine solche in R^+ implizieren würde. Es gilt "$\subseteq$" weil jede Wurzel von L_I Linearkombination von Elementen aus I ist, also eine Zerlegbarkeit in R^+ eine Zerlegbarkeit in R_I^+ zur Folge hat (einfache Wurzeln, die keine Wurzeln von L_I sind, können nicht vorkommen wegen der Linearen Unabhängigkeit der einfachen Wurzeln).

behalten also ihr Vorzeichen bei. Also ist h auch die Länge von w, wenn man sie in W(G,T) berechnet.
QED.

10.3.2 Theorem: die parabolischen Untergruppen von G
Seien G eine reduktive zusammenhängende lineare algebraische Gruppe, $T \subseteq G$ ein maximaler Torus, B eine Borel-Untergruppe von G, welche T enthält und $I \subseteq D(B)$ eine Menge von einfachen Wurzeln.

(i) $P_I := \cup_{w \in W_I} C(w)$ ist eine abgeschlossene Untergruppe von G, welche B enthält, mit der Weylgruppe W_I und dem Wurzelsystem R_I, d.h.

$$W(P_I. T) = W_I.$$
$$R(P_I. T) = R_I.$$

(ii) $R_u P_I = \langle X_\alpha \mid \alpha \in R^+ - R_I \rangle$

(iii) $L_I \subset P_I$ and der Produkt-Morphismus $L_I \times R_u P_I \to P_I$ ist ein Isomorphismus von Varietäten.

(iv) Für jede Parabolische Untergruppe von G, welche B enthält, gibt es genau eine Menge von einfache Wurzeln $I \subseteq S$ mit $P = P_I$.

Beweis. Zu (i). Zeigen wir, P_I ist eine Untergruppe von G. Dazu reicht es zu zeigen,

(1) $C(w)C(w') \subseteq P_I$ für beliebige $w,w' \in W_I$

Wir führen den Beweis durch Induktion nach der Länge von w (in W_I). Nach 10.2.11 gilt

1. $C(s_\alpha)\cdot C(w) = C(s_\alpha w)$ falls $l(s_\alpha w) = l(w) + 1$.
2. $C(s_\alpha)\cdot C(w) \subseteq^1 C(s_\alpha w) \cup C(w)$ falls $l(s_\alpha w) = l(w) - 1$.

Insbesondere gilt also (1) für den Fall, daß w die Länge 1 hat. Sei jetzt $w = s_\alpha w''$ mit $\alpha \in I$ und einem Element $w'' \in W_I$, dessen Länge kleiner ist als die von w. Dann gilt

$$\begin{aligned} C(w)C(w') &\subseteq C(s_\alpha)C(w'')C(w') && \text{(nach 1)} \\ &\subseteq C(s_\alpha)P_I && \text{(nach Induktion)} \\ &\subseteq P_I && \text{(Induktionsanfang)} \end{aligned}$$

Damit ist gezeigt, daß P_I eine Gruppe ist. Nach Konstruktion enthält P_I die Borel-Untergruppe B,

$$B \subseteq C(e) \subseteq P_I.$$

Wir haben noch die Abgeschlossenheit von P_I zu beweisen. Nach 2.2.4(ii) reicht es zu zeigen, P_I enthält eine nicht-leere offene Teilmenge von $\overline{P}_I$.

Da W_I die Weyl-Gruppe von L_I bezüglich T ist, gibt es in W_I ein Element w'_0 maximaler Länge. Auf Grund der Beschreibung 10.2.13 (i) des Randes einer Bruhat-Zelle liegt der Rand von P_I in einer Vereinigung von Bruhat-Zellen C(w') mit $l(w') < l(w'_0)$, d.h. das Innere von $\overline{P}_I$,

$$\text{Int } \overline{P}_I = \overline{P}_I - \partial\overline{P}_I$$

ist gerade $C(w'_0)$ und damit eine offene Teilmenge von $\overline{P}_I$, die ganz in P_I liegt.

Wir haben noch zu zeigen, R_I ist das Wurzelsystem und W_I ist die Weyl-Gruppe von P_I. Sei $\alpha \in R_I$. Dann ist α eine Wurzel von L_I (vgl. 10.3.1), also $\text{Ker}(\alpha)^0$ ein singulärer Torus in L_I. Bezeichne $C_{L_I}(w)$ für $w \in W_I$ die Zelle von w in L_I. Nach dem Lemma von Bruhat (10.2.10) gilt dann

$$L_I = \cup_{w \in W_I} C_{L_I}(w) \subseteq \cup_{w \in W_I} C(w) \subseteq P_I$$

Damit ist $\text{Ker}(\alpha)^0$ auch ein singulärer Torus in P_I[246] , d.h. α ist eine Wurzel von P_I. Wir haben gezeigt,

$$R(P_I, T) \supseteq R_I = R(L_I, T),$$

also

$$W(P_I, T) \supseteq W_I = W(L_I, T),$$

Es reicht zu zeigen, in der letzten Inklusion gilt das Gleichheitszeichen.[247] Angenommen nicht. Wir werden dann zeigen,

---

[246] Der Zentralisator in L_I liegt ganz im Zentralisator in P_I. Der letztere ist somit auch nicht auflösbar.

[247] Jede Wurzel α von $R(P_I, T)$, die nicht in R_I liegt, ließe sich nicht als Linearkombination von einfachen Wurzeln aus I schreiben. Die zugehörigen Spiegelung wäre somit kein Element aus W_I : alle einfachen Wurzeln aus I liegen in einer Hyperebene, in welcher α nicht liegt. Das orthogonale Komplement dieser Hyperebene besteht aus Punkten, die fest bleiben bei allen Elementen von $W_I = \langle s_\beta \mid \beta \in I \rangle$, aber nicht bei s_α.

in $W(P_I, T)$ gibt es ein Element von einer Länge, die größer ist als die aller Elemente von $W(L_I,T)$ und leiten daraus einen Widerspruch ab[248]. Sei

$$w \in W(P_I, T) - W(L_I,T).$$

und

$$w = s_{\alpha_1} \cdot \ldots \cdot s_{\alpha_h}$$

eine kürzeste Zerlegung in W(G,T). Falls $w(\alpha_i) < 0$ ist für ein $\alpha_i \in I$, so kann man die Zerlegung nach 10.2.2(iv) so wählen, daß das entsprechende s_{α_i} in der Zerlegung ganz rechts steht. Man kann in diesem Fall von rechts mit s_{α_i} multiplizieren und so die Länge von w verkleinern. Wir können daher annehmen,

$$w(\alpha_i) > 0 \text{ für alle } \alpha_i \in I,$$

d.h. w läßt die Vorzeichen der Wurzeln aus R_I^+ unverändert[249]. Umgekehrt läßt jedes s_α mit $\alpha \in I$ die Vorzeichen der Elemente aus

$$R^+ - R_I^+$$

unverändert (vgl. 10.1.11)[250]. Sei jetzt w'_0 ein Element maximaler Länge aus W_I. Dann verändert w'_0 nur die Vorzeichen der Elemente aus R_I^+ und w nur die Vorzeichen der Elemente aus $R^+ - R_I^+$. Insbesondere hat

$$w''_0 = ww'_0 \in W(P_I, T)$$

eine größere Länge als jedes Element aus W_I,

$$l(w''_0) > l(w'_0).$$

Es gilt

$$\dim P_I = \max \{ \dim C(w) \mid w \in W_I \} \qquad \text{(nach Definiton von } P_I\text{)}$$

---

[248] Man beachte, P_I ist nicht reduktiv. Wir können also nicht die Eigenschaften von Wurzeln reduktiver Gruppen benutzen. Insbesondere haben wir nicht den Begriff der einfachen Wurzel von P_I definiert.

[249] denn diese sind positive Linearkombinationen der Elemente aus I.

[250] Sogar die Vorzeichen der Elemente aus $R^+ - \{\alpha\}$ bleiben unverändert.

$= \max \{ l(w) + \dim B \mid w \in W_I \}$ (vgl. 10.2.9)

$= l(w'_0) + \dim B$

$<^{251} l(w''_0) + \dim B$ (nach Konstr. von w''_0)

$= \dim C(w''_0)$ (vgl. 10.2.9)

$= \dim B\dot{w}B$ (Definition von C(w))

$\leq \dim P_I$

Die letzte Ungleichung gilt wegen $B \subseteq P_I$ und $\dot{w} \in^{252} P_I$, also $B\dot{w}B \subseteq P_I$. Damit erhalten wir den gewünschten Widerspruch.

Zu (ii). Nach 9.3.5 ist

$$R_u P_I = (\cap_{B' \in \mathbf{B}_T(P_I)} B'_u)^0.$$

Man beachte, $T \subseteq B \subseteq P_I$, d.h. T ist ein maximaler Torus von P_I. Nach 8.1.7 operiert die Weyl-Gruppe einfach transitiv auf den Borel-Untergruppen, d.h.

$$R_u P_I = (\cap_{w \in W_I} \dot{w} B_u \dot{w}^{-1})^0.$$

Wir setzen

$$U := B_u .$$

und erhalten

(2) $$R_u P_I = (\cap_{w \in W_I} \dot{w} U \dot{w}^{-1})^0$$

Weiter schreiben wir

$U_I := U \cap L_I =^{253} (B \cap L_I)_u$

$U'_I := \langle X_\alpha \mid \alpha \in R^+ - R_I \rangle$

---

[251] Nach Voraussetzung gibt es eine positive Wurzel α von P_I, die keine Wurzel von L_I ist. Dann ist $\mathrm{Ker}(\alpha)^0$ ein singulärer Torus von P_I, also von G, d.h. α ist eine positive Wurzel von G.

[252] w ist ein Element der Weil-Gruppe von P_I, d.h. $\dot{w} \in N_{P_I}(T) \subseteq P_I$.

[253] Wegen $U \cap L_I \subseteq B \cap L_I$ folgt "$\subseteq$". Umgekehrt gilt $(B \cap L_I)_u \subseteq B$ also $(B \cap L_I)_u \subseteq B_u = U$, also $(B \cap L_I)_u \subseteq U \cap L_I$.

Für $\alpha \in I$ gilt $X_\alpha \subseteq L_I$, weil α eine Wurzel von L_I ist (nach 10.3.1), und es gilt $X_\alpha \subseteq B$, weil α eine positive Wurzel von G ist. Damit ist

$$X_\alpha \subseteq U \cap L_I = U_I \text{ für } \alpha \in I.$$

Nach 10.1.1 ist die Produktabbildung

$$\times_{\alpha \in R^+} X_\alpha \to U$$

ein Isomorphismus von Varietäten und analog ist die Produktabbildung

$$\times_{\alpha \in R_I^+} X_\alpha \to U_I$$

ein Isomorphismus, denn R_I^+ ist gerade die Menge der positiven Wurzeln von L_I (vgl. 10.3.2) und U_I ist der unipotente Anteil der Borel-Untergruppe $B \cap L_I$ von L_I (vgl. 10.3.1). Dieselbe Argumentation wie in 10.1.4 zeigt, daß die Multiplikationsabbildung

$$\times_{\alpha \in R^+ - R_I} X_\alpha \to U'_I$$

surjektiv[254] (also ein Isomorphismus) ist. Insbesondere gilt

(3) $$U = U_I \cdot U'_I \text{ und } U_I \cap U'_I = \{e\}$$

und die zugehörige Produktzerlegung der Elemente von U ist eindeutig.
Durch Einsetzen in (2) erhalten wir

---

[254] Jede Wurzel, die positive Linearkombination von Wurzeln aus $R^+ - R_I$ ist liegt wieder in $R^+ - R_I$. Das Produkt von zwei Elementen aus dem Bild der Produktabbildung hat die Gestalt

$$\prod_{\alpha \in R^+ - R_I} x_\alpha(\xi_\alpha) \cdot \prod_{\alpha \in R^+ - R_I} x_\alpha(\eta_\alpha) = \prod_{\gamma \in R} x_\gamma(P_\gamma(\xi, \eta))$$

mit eindeutig bestimmten Polynomen P_γ. Konjugation mit $t \in T$ liefert

$$\gamma(t)\, P_\gamma(\xi, \eta) = P_\gamma(\alpha(t)\xi, \alpha(t)\eta),$$

wobei α für ein Tupel von Wurzeln aus $R^+ - R_I$ steht. Vergleich liefert

$$\gamma = (i+j)\alpha \text{ mit Tupeln } i \geq 0 \text{ und } j \geq 0$$

und nicht beide = 0. Also kommen rechts nur Faktoren mit $\gamma \in R^+ - R_I$ vor, d.h. das Produkt von zwei Elementen aus dem Bild liegt im Bild. Das Bild ist eine Gruppe,also gleich U'_I.

(4) $$R_uP_I = (\cap_{w\in W_I} \dot{w}\, U_I \dot{w}^{-1} \cdot \dot{w} U'_I \dot{w}^{-1})^0$$

Untersuchen wir die Operation von W_I auf U'_I. Für $\alpha\in R^+ - R_I$ gilt

$$\alpha = \sum_{\beta\in D} n_\beta \beta \text{ mit } n_\beta>0 \text{ für ein } \beta\in D\text{-}I.$$

(vgl. 10.1.12(iii)). Dann gilt aber auch

$$s_\gamma(\alpha) = \sum_{\beta\in D} n_\beta\, s_\gamma(\beta) \in R^+ - R_I$$

für alle $\gamma\in I$ (vgl. 10.1.11(i)). Da die s_γ mit $\gamma\in I$ die Weyl-Gruppe W_I erzeugen (vgl. 10.3.0), sehen wir, die Menge $R^+ - R_I$ ist stabil unter der Operation von W_I. Nach Definition ist dann aber auch U'_I stabil unter dieser Operation, $\dot{w}U'_I\dot{w}^{-1} = U'_I$. Damit bekommt (4) die Gestalt

(5) $$R_uP_I = (\cap_{w\in W_I} \dot{w}\, U_I \dot{w}^{-1} \cdot U'_I)^0$$

$$=^{255} ((\cap_{w\in W_I} \dot{w}\, U_I \dot{w}^{-1}) \cdot U'_I)^0$$

$$\subseteq (\cap_{w\in W_I} \dot{w}\, U_I \dot{w}^{-1}) \cdot U'_I$$

Nun ist $(\cap_{w\in W_I} \dot{w}\, U_I \dot{w}^{-1})^0$ (nach 9.3.5) das Radikal der reduktiven Gruppe L_I also gleich {e}. Also ist $\cap_{w\in W_I} \dot{w}\, U_I \dot{w}^{-1}$ endlich. Damit liegt das Radikal R_uP_I in der Vereinigung von endlich vielen Restklassen modulo U'_I. Da das Radikal irreduzibel ist, liegt es ganz in einer von ihnen. Da das Radikal e enthält liegt es in U'_I ,

$$R_uP_I \subseteq U'_I .$$

---

[255] Mit $ab = a'b'$ mit $a\in \dot{w}\, U_I \dot{w}^{-1}$, $a'\in \dot{w}'\, U_I \dot{w}'^{-1}$ und $b,b'\in U'_I$ gilt

$$a'^{-1}a = b'b^{-1} \in \dot{w}\, U_I \dot{w}^{-1} \cap U'_I = \dot{w}\, U_I \cap U'_I \dot{w}^{-1} = \dot{w}\, \{e\} \dot{w}^{-1} = \{e\}$$

also $a = a'$ und $b = b'$.

Die umgekehrte Inklusion ergibt sich direkt aus (5), d.h. es gilt

$$R_u P_I = U'_I .$$

Zu (iii). Für $w \in W_I$ bezeichne

$$C_G(w) \text{ bzw. } C_{L_I}(w)$$

die Bruhat-Zelle von w in G bzw. in L_I. Es gilt

$$C_G(w) = C_{L_I}(w)U'_I \qquad \text{(wegen (3))}^{256}$$
$$= C_{L_I}(w)R_u(P_I)$$

für alle $w \in W_I$. Nach dem Lemma von Bruhat (10.2.10) für G und L_I folgt

$$P_I = \cup_{w \in W_I} C_G(w) = \cup_{w \in W_I} C_{L_I}(w)R_u(P_I) = L_I \cdot R_u(P_I),$$

d.h. die Produkt-Abbildung

(6) $\quad L_I \times R_u(P_I) \to P_I$

ist surjektiv. Beweisen wir als nächstes die Injektivität von (6).

Nach 7.3.5 (ii) ist $B_I = TU_I$ eine Borel-Untergruppe von L_I, d.h. die Untergruppe B_I und deren Konjugierte überdecken L_I (nach 7.3.3). Jedes Element der Faser über e von (6) liegt also bereits in einer Untergruppe der Gestalt

$$g\, B_I g^{-1} \times R_u(P_I).$$

Es reicht also, die Injektivität der Einschränkung von (6) auf dieser Untergruppen zu beweisen. Da alle Borel-Untergruppen von L_I

---

[256] Es gilt

$$C_G(w) = \dot{B}w\dot{B} = \dot{U}w\dot{B} \qquad \text{(wegen } B = UT\text{)}$$
$$= U_I U'_I \dot{w} B \quad \text{(wegen } U = U_I U'_I\text{)}$$
$$= U_I \dot{w} U'_I B \quad (W_I \text{ operiert auf } U'_I)$$
$$= U_I \dot{w} B \qquad \text{(wegen } U'_I \subseteq B\text{)}$$
$$= U_I \dot{w}\, TB_I U'_I$$
$$= C_{L_I}(w)U'_I$$

gleichberechtigt sind, können wir annehmen, g = e. Wie wir oben gesehen haben, gilt $R_u(P_I) = U'_I$, d.h. es reicht, die Injektivität der Produkt-Abbildung

$$TU_I \times U'_I \to P_I$$

zu beweisen. Aus

$$suu' = tvv'$$

mit $s,t \in T$, $u,v \in U_I$ und $u',v' \in U'_I$ folgt

$$t^{-1}s = vv'u'^{-1}u^{-1}.$$

Dieses Element ist sowohl halbeinfach als auch unipotent, also gleich e. Es folgt

$$s = t \text{ und } uu' = vv'.$$

Wegen (3) ist damit aber auch u = v und u' = v'. Damit ist die Bijektivität von (6) bewiesen. Zum Beweis der Isomorphie-Eigenschaft, reicht es zu zeigen, der Morphismus ist separabel. Dazu reicht es zu zeigen, die induzierte Abbildung der Tangentialvektorräume

$$L(L_I) \times L(R_u(P_I)) \to L(P_I)$$

im "Ursprung" ist bijektiv. Diese Abbildung wird aber gerade von der Addition von L(G) induziert. Die Bijektivität der Abbildung ergibt sich aus der folgenden Zerlegung der beteiligten Raum in Gewichtsräume bezüglich der Operation von T.

$$L(L_I) = L(T) + \sum_{\alpha \in R_I} L(X_\alpha) \qquad \text{(vgl. 10.3.0, 10.3.1, 9.3.8)}$$

$$L(R_u(P_I)) = \sum_{\alpha \in R^+ - R_I} L(X_\alpha) \quad \text{(weil } \times_{\alpha \in R_I^+} X_\alpha \to U_I \text{ surjektiv ist)}$$

$$L(P_I) = L(T) + \sum_{\alpha \in R_I} L(X_\alpha) + \sum_{\alpha \in R^+ - R_I} L(X_\alpha)$$

Zum Beweis der letzten Identität beachte man, es gilt "$\supseteq$" (weil (6) wohldefiniert ist). Außerdem ist

$$\dim L(P_I) = \dim P_I = \dim C(w'_0) \text{ (Dimension der großen Zelle)}$$
$$= \dim B + l(w'_0)$$
$$= \dim B + \#R_I^+$$

$$= \dim T + \#R^+ + \#R_I^+$$

$$= \dim L(T) + 2\#R_I^+ + (\#R^+ - \#R_I^+)$$

$$= \dim L(T) + \#R_I + \#(R^+ - R_I)$$

Also gilt sogar das Gleichheitszeichen.

Zu (iv).

1. Schritt. Die Parabolischen Untergruppen P von G mit $B \subseteq P$ und

$$\dim P = \dim B + 1$$

sind gerade die Untergruppen der Gestalt $P_{\{\alpha\}}$ mit $\alpha \in D$.

Für jede einfache Wurzel $\alpha \in D$ setzen wir

$$P_\alpha := P_{\{\alpha\}}.$$

Nach 10.3.1 hat $L_{\{\alpha\}}$ das Wurzelsystem $R_{\{\alpha\}} = \{\pm\alpha\}$, also das positive Wurzelsystem $R^+_{\{\alpha\}}$, d.h. es gilt

$$\dim P_\alpha = \dim B + \#R_I^+ = \dim B + 1.$$

Sei umgekehrt $P \supseteq B$ eine parabolische Untergruppe mit

$$\dim P = \dim B + 1.$$

Die Anzahl der Wurzeln der reduktiven Gruppe

$$\overline{P} := P/R_u P$$

ist dann gleich

$$\#R(\overline{P}) = 2(\dim P - \dim B) = 2$$

(vgl. 9.3.9(ii)) d.h.

$$R(\overline{P}) = \{\pm\alpha\}.$$

Insbesondere ist[257]

$\overline{P}$ vom halbeinfachen Rang 1.

---

[257] Es reicht zu zeigen, $S = \mathrm{Ker}(\alpha)^0$ liegt im Zentrum von $\overline{P} := P/R_u P$, denn dim T/S = 1, d.h. der halbeinfache Rang ist höchstens 1. Der Rang kann nicht 0 sein, denn jede zusammenhängende Gruppe der Dimension ≤ 2 ist auflösbar (Aufg. 8.2.6(3)), d.h. P wäre dann auflösbar im Widerspruch zu dim P > dim B.

Zeigen wir also $S = \mathrm{Ker}(\alpha)^0$ im Zentrum von P. Wir haben zu zeigen, S operiert (durch Konjugation) trivial auf P. Nach 9.3.7(ii) wird G erzeugt von T, X_α und $X_{-\alpha}$. Es reicht also zu zeigen, S operiert trivial auf diesen Untergruppen. Das ist offensichtlich für T (wegen $S \subseteq T$ und T kommutativ) und gilt nach Definition für X_α und $X_{-\alpha}$.

Da die Weyl-Gruppe von den Spiegelungen zu den Wurzeln erzeugt wird (vgl. 9.1.13), folgt

$$W(\overline{P}) = \{1, s_\alpha\},$$

d.h. die Weyl-Gruppe besteht aus 2 Elementen. Nach 8.2.3 ist

$$P =^{258} B \cup UnB$$

mit einem Repräsentanten n des nicht-trivialen Elements von

$$W_{\overline{P}}(\overline{P}) = N(T)/T.$$

Da die Weyl-Gruppe einfach transitiv auf den Borel-Untergruppen operiert (vgl. 8.1.7(ii)), besitzt $\overline{P}$ (und damit P) genau zwei Borel-Untergruppen, welche T enthalten, d.h.

$$\mathbf{B}_T(P) = \{B , B' \}.$$

Das Element $n \in N_G(T)$ genügt der Bedingung

$$B' = nBn^{-1}.$$

Die beiden Borel-Untergruppen von $\overline{P}$ (und damit die von P) sind nach 10.1.8 benachbart. Nach 10.1.8 gibt es genau eine positive Wurzel von R(P), sagen wir α, mit

$$B' = s_\alpha B.$$

d.h. n repräsentiert s_α. Damit gilt

$$P = B \cup UnB = C(e) \cup C(s_\alpha) = P_{\{\alpha\}}.$$

2. Schritt. Der allgemeine Fall.
Sei P eine abgeschlossene Untergruppe von G, welche B enthält. Nach 7.3.8 ist sie zusammenhängend. Wir setzen

$$I := \{ \alpha \in D \mid P_\alpha \subseteq P \}.$$

Nach dem ersten Schritt sind die P_α mit $\alpha \in I$ gerade die abgeschlossenen Untergruppen Q von P, welche B enthalten und für welche gilt

$$\dim Q = \dim B + 1.$$

Wenden wir die Aussage des ersten Schritts auf die reduktive Gruppe

---

[258] Die Aussage 8.2.3 gilt nur für Gruppen vom Rang 1, d.h. die Identität gilt nur modulo dem Radikal von P,

$$P/R(P) = B/R(P) \cup UR(P)/R(P) \cdot nR(P) \cdot B/R(P),$$

d.h. für jedes $p \in P$ gilt

$$p = bR(P) \text{ oder } p \in unbR(P)$$

mit $b \in B$ bzw. $u \in U$ und $b \in B$. Wegen $R(P) \subseteq B$ folgt

$$P \subseteq B \cup UnB$$

Die umgekehrte Ungleichung ist trivial wegen $B \subseteq P$.

$$\overline{P} := P/R_u P$$

und das natürliche Bild von B in $\overline{P}$ an, so sehen wir, daß die Elemente von I ein System einfacher Wurzeln für $\overline{P}$ bilden.[259] Nach dem Lemma von Bruhat (vgl. 10.1.10) gilt damit

$$\overline{P} = \cup_{w \in W_I} \overline{C}(w),$$

also

$$P = \cup_{w \in W_I} C(w) = P_I$$

QED.

10.3.3 Aufgaben

---

[259] Jedes $\alpha \in I$ ist eine Wurzel von P_α. Das natürliche Bild von P_α in $\overline{P}$ hat ebenfalls α als Wurzel (wegen der Beschreibung von $R_u P$ in (ii). Also ist der Eigenraum von α auf $L(\overline{P})$ nicht-trivial, d.h. α ist eine Wurzel von $\overline{P}$. Da $\alpha \in I$ positiv ist, gilt $X_\alpha \subseteq B$. Diese Inklusion bleibt erhalten beim Übergang zu den Restklassen modulo $R_u P$. Also besteht I aus positiven Wurzeln von $\overline{P}$,

$$I \subseteq R^+(\overline{P}).$$

Für jede Wurzel α von $\overline{P}$ ist der zugehörige Eigenraum in $L(\overline{P})$ nicht-trivial, also erst recht der zugehörige Eigenraum in L(P) und in L(G). Ist α positive Wurzel von $\overline{P}$, so liegt X_α ganz in B, ist also positive Wurzel von G, es gilt damit

$$R^+(\overline{P}) \subseteq R^+(G).$$

Da die Elemente von I sogar einfach sind als Elemente von $R^+(G)$, so sind sie erst recht einfach als Elemente von $R^+(\overline{P})$. Damit gilt

$$I \subseteq D(B/R_u P).$$

Umgekehrt definiert jede einfache Wurzel

$$\alpha \in R^+(\overline{P}) \subseteq R^+(G)$$

von $\overline{P}$ eine parabolische Untergruppe $\overline{P}_{\{\alpha\}}$ von $\overline{P}$, deren Dimension um 1 größer ist als die Dimension der Borel-Untergruppe. Das vollständige Urbild von

$$\overline{P}_{\{\alpha\}} = \overline{C}(e) \cup \overline{C}(s_\alpha)$$

in G ist gerade

$$C(e) \cup C(s_\alpha)$$

und ist eine parabolische Untergruppe von P, die B enthält und die Dimension dim B + 1 besitzt, d.h. eine Gruppe der Gestalt wie wir sie oben mit Q bezeichnet haben. Deshalb hat sie die Gestalt

$$P_\beta = C(e) \cup C(s_\beta) \text{ mit } \beta \in I.$$

Aus $C(e) \cup C(s_\alpha) = C(e) + C(s_\beta)$ folgt aber $C(s_\alpha) = C(s_\beta)$, also $s_\alpha = s_\beta$, also $\alpha = \pm\beta$. Da beide Wurzeln positiv sind, folgt $\alpha = \beta \in I$.

Bezeichne G eine reduktive zusammenhängende lineare algebraische Gruppe.

(1) Aufgabe

Sei P eine parabolische Untergruppe von G. Eine Levi-Untergruppe L von P ist eine abgeschlossene Untergruppe von P mit der Eigenschaft, daß die Produkt-Abbildung

$$L \times R_u P \to P$$

ein Isomorphismus von Varietäten ist. Man zeige, ist T ein maximaler Torus von P, so gibt es genau eine Levi-Untergruppe von P, welche den Torus T enthält.

(2) Aufgabe

Seien T ein maximaler Torus von G und H eine abgeschlossene Untergruppe von G, die den Torus T enthält. Bezeichne

$$R = R(G,T)$$

das Wurzelsystem und

$$R' := \{\alpha \in R \mid X_\alpha \subseteq H\}.$$

Man zeige, H ist genau dann parabolisch, wenn $R = R' \cup -R'$ gilt (Hinweis: die eine Implikation folgt aus 10.3.2. Zum Beweis der anderen wähle man eine Borel-Untergruppe $B' \supseteq T$ von H und eine Borel-Untergruppe B von G mit $B \cap H = B'$ und setze

$$R^+ = R^+(B).$$

Für $\alpha \in R^+$ und $X_\alpha \not\subseteq B'$ gilt dann $X_{-\alpha} \subseteq H$. Unter Verwendung der reduktiven Gruppe $H/R_u H$ führt dies zum Widerspruch $X_\alpha \subseteq H \cap B = B'$. Also ist B=B').

(3) Aufgabe

Seien P und Q zwei parabolische Untergruppen von G. Man zeige that auch $(P \cap Q)R_u(P)$ eine parabolische Untergruppe ist (Hinweis: man benutze Aufgabe (2)).

(4) Aufgabe

Sei $\lambda: G_m \to G$ eine "multiplikative 1-Parameter-Untergruppe" von G. Für $g \in G$, $t \in k^*$ setze man

$$\theta_{g,\lambda}(t) := \lambda(t) g \lambda(t)^{-1}$$

und

$$P(\lambda) := \{ g \in G \mid \theta_{g,\lambda} \text{ ist fortsetzbar zu einem Morphismus } \mathbb{A}^1 \to G \}.$$

Dann ist $P(\lambda)$ eine abgeschlossene Untergruppe von G (vgl. 2.5.5(2)). Man zeige, $P(\lambda)$ ist eine parabolische Untergruppe (Hinweis: man wählen einen maximalen Torus $T \supseteq S := \lambda(G_m)$ und verwende (2)).

(5) Aufgabe

Wir verwenden die Bezeichnungen von 10.3.2. Seien I,J $\subseteq$ D und bezeichne A eine Menge von Darstellungen in W der Doppelnebenklassen $W_I w W_J$. Dann ist G die disjunkte Vereinigung

der Doppelnebenklassen $P_I \dot{w} P_J$ mit $w \in A$.

(6) Aufgabe

Sei $G = GL_n$ und $V = k^n$ mit der natürliche Operation von G. Weiter seien

$$F = (V_1,...,V_s)$$

eine beliebige Fahne in V (vgl 7.2.11(4)) und $e_1,...,e_n$ eine Basis von V mit

$$V_h = ke_1 + ... + ke_{i_h}$$

für h = 1, ... , s. Bezeichne B die Borel-Untergruppe von G, deren Elemente die Fahne

$$ke_1 \subset ke_1 + ke_2 \subset ...$$

fest lassen und T den maximalen Torus von G, dessen Elemente alle Unterräume ke_i fest lassen.

(a) Die Untergruppe P_F von G, deren Elemente die Fahne F fest lassen, ist eine parabolische Untergruppe, welche B enthält.

(b) Sei D die Basis des Wurzelsystems R(G,T) bezüglich B (vgl. 10.1.14 (1)). Man beschreibe die Teilmenge I $\subseteq$ D mit $P_F = P_I$ (vgl. 10.3.2).

(c) Jede parabolische Untergruppe von G ist von der Gestalt P_F mit einer Fahne F.

(d) Man diskutiere die entsprechenden Aussage im Fall der speziellen orthogonalen Gruppe (char k $\neq$ 2) und der symplektischen Gruppe (7.2.11 (5) und (6)).

---------- Continue here ----------:

Notes

Das meiste Material in diesem Kapitel ist ebenfalls Standard. Wir haben bei den Aufgaben von 10.2.15 zusätzliches Material eingefügt, zum Beispiel zu den Schubert-Varietäten.

Die Varietäten X(w) von 10.2.15(9) wurden von Deligne und Lusztig [15] eingeführt und sind ziemlich wichtig für die Darstellungstheorie endlicher Chevalley-Gruppen

11. The uniqueness theorem

Wir benutzen die Bezeichnungen des vorigen Kapitels. Sei G eine reduktive zusammenhängende lineare algebraische Gruppe, T ein maximaler Torus von G und

$$\Psi := \Psi(G,T) = (X, X^v, R, R^v)$$

das zugehörige Wurzeldatum (9.1.11). Eines der Hauptergebnisse dieses Kapitels (vgl. 11.4.2) ist die Aussage, daß Ψ die Gruppe G bis auf Isomorphie bestimmt.

Um ein solches Eindeutigkeitsergebnis zu beweisen, müssen wir in allen Einzelheiten untersuchen, wie sich die Gruppe G aus dem Torus T und den 1-Parameter-Untergruppen X_α mit $\alpha \in R$ aufbaut. Im Verlauf dieser Untersuchungen benötigen wir Informationen über die Wurzelsysteme vom Rang 2. Diese werden wir als erstes diskutieren.

11.1 Die Wurzelsysteme vom Rang 2

11.1.1 Beschreibung der Wurzelsysteme vom Rang 2

Wir beginnen mit der Klassifikation der Wurzelsysteme vom Rang 2. Sei R ein solches Wurzelsystem. Wir nehmen an,

$$R \subseteq V := \mathbb{R}^2.$$

Bezeichne e_1, e_2 die Standard-Einheitsvektoren von V und sei

$(,): V \times V \to \mathbb{R}$

die symmetrische Bilinearform mit

$$(e_i, e_j) = 2\delta_{ij} \text{ für } i, j \in \{1,2\}.$$

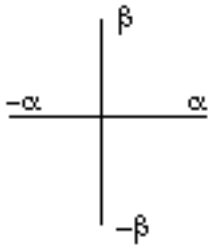
Wir beschreiben hier die reduzierten Wurzelsysteme (vgl. 9.1.12) und geben die zugehörigen Basen

$$D = \{\alpha, \beta\}$$

an. W bezeichne die Weyl-Gruppe.

11.1.1.1 Das Wurzelsystem $A_1 \times A_1$

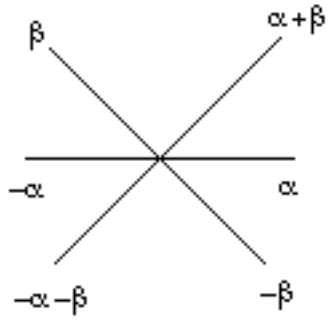
$\alpha = e_1, \beta = e_2$. $R = \{\pm\alpha, \pm\beta\}$, $W = V_4$ (Kleinscher Vierergruppe)



11.1.1.2 Das Wurzelsystem A_2

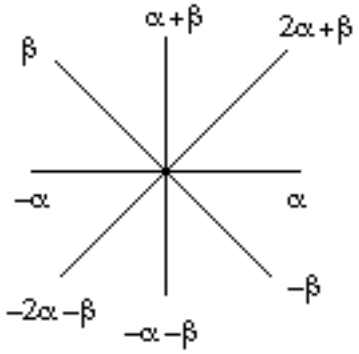
$\alpha = e_1, \beta = \frac{1}{2} e_1 + \frac{\sqrt{3}}{2} e_2$.

$R = \{\pm\alpha, \pm\beta, \pm(\alpha+\beta)\}$,
$W \cong S_3$ (symmetrische Gruppe)



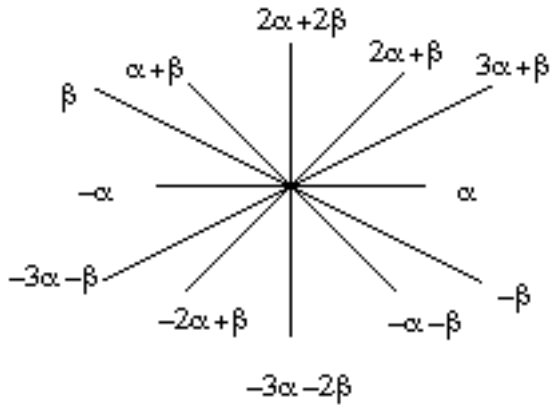
11.1.1.3 Das Wurzelsystem B_2

$\alpha = e_1$, $\beta = -e_1 + e_2$.
$R = \{\pm\alpha, \pm\beta, \pm(\alpha+\beta), \pm(2\alpha+\beta)\}$,
$W \cong D_8$ (Diedergruppe der Ordnung 8)



11.1.1.4 Das Wurzelsystem G_2

$\alpha = e_1$, $\beta = -\frac{2}{3}e_1 + \frac{\sqrt{3}}{2}e_2$.
$R = \{\pm\alpha, \pm\beta, \pm(\alpha+\beta), \pm(2\alpha+\beta), \pm(3\alpha+\beta), \pm(3\alpha+2\beta)\}$,
$W \cong D_8$ (Diedergruppe der Ordnung 8)



11.1.2 Proposition: Klassifikation

Ein reduziertes Wurzelsystem vom Rang 2 ist isomorph zu $A_1 \times A_1$, A_2, B_2 oder G_2.

Beweis.

QED.

11.2.3 Aufgabe: die nicht-reduzierten Wurzelsysteme vom Rang 2

Ein nicht-reduziertes Wurzel-System vom Rang 2 ist isomorph zu einem der folgenden

$\{\pm e_1, \pm e_2, \pm 2e_1\}$

$\{\pm e_1, \pm e_2, \pm 2e_1, \pm 2e_2\}$

$\{\pm e_1, \pm e_2, \pm e_1 \pm e_2, \pm 2e_1, \pm 2e_2\}$

11.2. 4 Voraussetzungen und Bezeichnungen

Als nächstes beweisen wir einige Tatsachen über allgemeine Wurzelsystem, die später benötigt werden und im Zusammenhang mit Wurzelsystemen des Rangs 2 stehen.

Sei R ein Wurzelsystem im reellen Vektorraum V. Bezeichne W die Weyl-Gruppe.

11.2.5 Lemma: Fortsetzung von zwei Wurzeln zu einem System positiver Wurzeln

Seien $\alpha, \beta \in R$ linear unabhängige Wurzeln. Dann gibt es ein System positiver Wurzeln R^+ derart, daß α eine einfache Wurzel ist und β eine nicht-negative Linearkombination von α und einer einfachen Wurzel.

Beweis.

QED.

11.2.6 Lemma

Seien $\alpha, \beta \in R$ linear unabhängige Wurzeln. Dann besteht die Menge

$$\{ i \in \mathbb{Z} \mid \beta + i\alpha \in R \}$$

gerade aus den ganzen Zahlen eines Intervalls

$$[-c, b]$$

mit $b - c = - \langle \alpha , \beta^v \rangle$ und $b + c \leq 3$, welches die 0 enthält.

Beweis.

QED.

11.2.7 Definition: α-String durch β

Seien $\alpha, \beta \in R$ zwei Wurzeln. Dann heißt die Menge

$$\{ i \in \mathbb{Z} \mid \beta + i\alpha \in R \}$$

von 11.2.6 α-String durch β. Die Zahl b+c von Lemma 11.2.6 heißt Länge des α-Strings durch β.

11.2.7 Bezeichnungen

Sei R^+ ein System positiver Wurzeln und D die zugehörige Basis. Die Weyl-Gruppe W wird dann von der Menge

$$S := \{ s_\alpha \mid \alpha \in D \}$$

der Spiegelungen zu den einfachen Wurzeln erzeugt. Für $\alpha, \beta \in D$ bezeichne $R_{\alpha,\beta}$ das Wurzelsystem

$$R_{\alpha,\beta} := R \cap (\mathbb{R}\alpha + \mathbb{R}\beta).$$

Dann bilden α, β eine Basis von $R_{\alpha,\beta}$. Die Weyl-Gruppe $W_{\alpha,\beta}$ von $R_{\alpha,\beta}$ wird von s_α und s_β erzeugt,

$$W_{\alpha,\beta} = \langle s_\alpha, s_\beta \rangle.$$

11.2.8 Lemma

Seien $\alpha, \beta \in D$ und $w \in W$ derart, daß gilt $w\alpha = \beta$. Dann gibt es einfache Wurzeln

$$\beta_1, \ldots, \beta_{s+1} \in D$$

und Elemente der Weyl-Gruppe

$$w_1, \ldots, w_s \in W$$

mit den folgenden Eigenschaften.

(a) $w = w_s w_{s-1} \cdot \ldots \cdot w_1$.

(b) $\beta_1 = \alpha, \beta_{s+1} = \beta$ und $w_i\beta_i = \beta_{i+1}$ für i = 1,...,s.

(c) Ist $\beta_i \neq \beta_{i+1}$, so gilt

$$w_i \in W_{\beta_i,\beta_{i+1}} ,$$

und ist $\beta_i = \beta_{i+1}$, so gilt

$$w_i \in W_{\beta_i,\beta'_{i+1}} \text{ für ein } \beta'_i \in D$$

(i = 1, ... , s).

Dieses Lemma besagt, daß eine Bewegung von α nach β, welche durch ein $w \in R$ definiert wird, durch Zusammensetzung von einfachen solchen Bewegungen innerhalb eines Wurzelsystems der Gestalt $R_{\gamma,\delta}$ mit $\gamma, \delta \in D$ entsteht.

Beweis.

QED.

11.2. Die Strukturkonstanten

Wir erinnern daran, daß man für jedes $\alpha \in R$ einen Isomorphismus algebraischer Gruppen

$$x_\alpha : G_a \to X_\alpha \ (\subseteq G)$$

wählen kann im Werten in einer T-stabilen abgeschlossenen Untergruppe, auf der T über den Charakter α operiert. Die Wahl von x_α ist nicht eindeutig. Eine erste Normalisierung ergibt sich aus dem folgenden Ergebnis.

11.2.1 Proposition: eine Normalisierung für die x_α

(i) Für jedes $a \in X_\alpha - \{e\}$ gibt es genau ein $a' \in X_{-\alpha} - \{e\}$ mit

$$aa'a \in N_G(T).$$

(ii) Die Isomorphismen x_α können so gewählt werden, daß für jedes $\alpha \in R$ das Element

$$n_\alpha := x_\alpha(1)x_{-\alpha}(-1)x_\alpha(1)$$

in $N_G(T)$ liegt und als natürliches Bild in $W = N_G(T)/T$ die Spiegelung s_α hat. Es gilt

(1) $x_\alpha(\xi')x_{-\alpha}(-\xi^{-1})x_\alpha(\xi) = \alpha^v(\xi)n_\alpha$ für alle $\xi \in k^*$.

(iii) Das Element $n_\alpha^2 = t_\alpha$ liegt in T und es gilt $t_\alpha = \alpha^v(-1)$. Außerdem ist

$$n_{-\alpha} = t_\alpha n_\alpha \text{ und } t_{-\alpha} = t_\alpha.$$

(iv) Ist $(x'_\alpha)_{\alpha \in R}$ ein zweite Familie von Isomorphismen, die der Bedingung von (ii) genügt, so gibt es $c_\alpha \in k^*$ mit

$$x'_\alpha(\xi) = x_\alpha(c_\alpha \xi) \ , \ c_{-\alpha}c_\alpha = 1$$

für alle $\alpha \in R$ und alle $\xi \in k$.

Beweis.

QED.

Bemerkung

Falls $n \in N_G(T)$ das Element $w \in W(G,T)$ repräsentiert, so gilt

$$nt_\alpha n^{-1} = t_{w\alpha}$$

für jedes $\alpha \in R$.

Das nachfolgende Ergebnis über die n_α werden wir in Kapitel 12 benötigen.

11.2.2 Bezeichnungen

Seien G eine reduktive zusammenhängende lineare algebraische Gruppe, $T \subseteq G$ ein maximaler Torus und B eine Borel-Untergruppe, die T enthält. Wir setzen

$R^+ := R^+(B)$
$D := D(B)$
$U := B_u$

Dann gilt

$$B = TU \text{ und } U = \prod_{\gamma \in R^+} X_\gamma .$$

Ist

$$u = \prod_{\gamma \in R^+} x_\gamma(\xi_\gamma)$$

und ist $\alpha \in D$ eine einfache Wurzel, so ist der Wert von ξ_α eindeutig bestimmt, d.h. unabhängig von der Wahl der Reihenfolge der Faktoren in der Produktdarstellung von u.

Denn nach 10.1.4 bildend die Produkte, in denen alle Faktoren zu nicht-einfachen Wurzeln gehören, einen Normalteiler in U und die zugehörige Faktorgruppe ist abelsch. Das ändern der Reihenfolge der Faktoren verändert also nur Faktoren zu nicht-einfachen Wurzeln.

Wir schreiben

$$\xi_\alpha(u) := \xi_\alpha$$

für einfache Wurzeln α. Wir bezeichnen mit

$$\Omega :=^{260} TUaU,\ a \in N_G(T),$$

---

[260] Es gilt

$\Omega = BaB$

die große Zelle von G. Dabei repräsentiert a das Element maximaler Länge von W(G,T). Wir schreiben weiter

$$Y := UaU.$$

Für $x = tuau' \in \Omega$ schreiben wir

$$\xi_\alpha(x) := \xi_\alpha(u) \quad \text{für } \alpha \in D(B).$$

Weiter sei

$$Y_\alpha := \{y \in Y \mid \xi_\alpha(y) \neq 0\}.$$

$$\Omega_\alpha := TY_\alpha.$$

Y_α ist eine offene Teilmenge von Y.

11.2.3 Lemma

Für jede einfache Wurzel α gibt es einen Morphismus

$$\Phi_\alpha : \Omega_\alpha \to \Omega_\alpha$$

mit

$$n_\alpha(ty) = (s_\alpha t)\alpha^\vee(-\xi_\alpha y)^{-1}\Phi_\alpha(y)$$

für alle $t \in T$ und alle $y \in Y_\alpha$. Es gilt

$$\xi_\alpha(\Phi_\alpha y) = -\xi_\alpha y \text{ und } \Phi_\alpha^2 = Id.$$

Beweis.

QED.

11.2.4 Realisierungen und Strukturkonstanten

Eine Familie $(x_\alpha)_{\alpha \in R}$ von Isomorphismen mit den Eigenschaften von 11.2.1(ii) heißt Realisierung von R in G.

Bemerkungen

(i) Nach Formel (1) von 11.2.1 sind die Kowurzeln durch eine Realisierung festgelegt.

(ii) Für lineare unabhängige Wurzeln $\alpha, \beta \in R$ (d.h. $\alpha \neq \pm\beta$) gelten Formeln

$$(2)\quad x_\alpha(\xi)x_\beta(\eta)x_\alpha(\xi)^{-1} = x_\beta(\eta) \prod_{i\alpha+j\beta \in R, i,j>0} x_{i\alpha+j\beta}(c_{\alpha,\beta,i,j}\xi^i\eta^j)$$

(vgl. 10.1.4) wobei die Produkte in einer beliebig vorgegebenen Reihenfolge zu nehmen sind. Die Elemente

$$c_{\alpha,\beta,i,j} \in k$$

$= BaTU$
$= BTaU$ wegen $a \in N_G(T)$.
$= BaU$
$= TUaU$

heißen Strukturkonstanten von G zur gegebenen Realisierung.

(iii) Ist $(c'_{\alpha,\beta,i,j})$ eine Familie von Strukturkonstanten zu einer anderen Realisierung, so gibt es Konstanten $c_\alpha \in k^*$ (nach 11.2.1(iv)) mit $c_\alpha c_{-\alpha} = 1$ und

$$c'_{\alpha,\beta,i,j} = c_\alpha^{-i} c_\beta^{-j} c_{i\alpha+j\beta} c_{\alpha,\beta,i,j} .$$

Die Familie $(c'_{\alpha,\beta,i,j})$ heißt dann äquivalent zur Familie $(c_{\alpha,\beta,i,j})$.

(iv) Wir setzen

$$c_{\alpha,\beta,0,1} = c_{\alpha,\beta,1,0} := 1.$$

Aus (2) leitet man ab, daß gilt

$$c_{\alpha,\beta,1,1} = - c_{\beta,\alpha,1,1}$$

und daß die $c_{\beta,\alpha,i,j}$ durch die $c_{\alpha,\beta,i,j}$ eindeutig bestimmt sind.

Wir müssen jetzt die Strukturkonstanten in allen Einzelheiten untersuchen. Die erste Ergebnisse dazu finden sich in der nächsten Proposition.

11.2.5 Proposition

Seien α und β linear unabhängige Wurzeln und bezeichne $(\beta - c\alpha, \ldots, \beta + b\alpha)$ den α-String durch β (vgl. 11.1.5). Dann gilt:

(i) $n_\alpha x_\beta(\xi) n_\alpha^{-1} = x_{s_\alpha\beta}(d_{\alpha,\beta}\xi)$ für alle $\xi \in k$.

Dabei ist $d_{\alpha,\beta} \in k^*$ durch die folgende Formel gegeben.

$$d_{\alpha,\beta} := \sum_{i=m(0,c-b)}^{c} (-1)^i c_{-\alpha,\beta,i,1} c_{\alpha,\beta-i\alpha,i+b-c,1}$$

Außerdem gilt

$$d_{-\alpha,\beta} = (-1)^{<\beta,\alpha^v>} d_{\alpha,\beta}$$

$$d_{\alpha,\beta} d_{-\alpha,-\beta} = (-1)^{<\beta,\alpha^v>}$$

$$d_{\alpha,\beta} d_{\alpha,-\beta} = 1$$

$$d_{\alpha,\beta} d_{\alpha,s_\alpha\beta} = (-1)^{<\beta,\alpha^v>}$$

$$d_{\alpha,\alpha} = -1$$

(ii) $n_\alpha n_\beta n_\alpha^{-1} = s_\alpha(\beta)^v(d_{\alpha,\beta}) n_{s_\alpha\beta}$

Dabei bezeichne n_α das Element von 11.2.1.

Beweis.
QED.

11.2.6 Lemma

Seien $\beta,\gamma\in R$ linear unabhängig und $i\beta+j\gamma\in R$ mit $i \geq 0$ und $j\geq 0$. Dann gilt

$$c_{s_\alpha\beta,s_\alpha\gamma,i,j} = d^{-i}_{\alpha,\beta}d^{-i}_{\alpha,\gamma}d_{\alpha,i\beta+j\gamma}c_{\beta,\gamma,i,j}$$

wobei die $d_{\alpha,\beta}$ wie in 11.2.5 sind. Für jedes $w\in W$ gilt

$$c_{\beta,\gamma,i,j}c_{-\beta,-\gamma,i,j} = c_{w\beta,w\gamma,i,j}c_{-w\beta,-w\gamma,i,j}$$

Beweis.
QED.

11.2.7 Proposition

Sei rk R = 2. Dann gilt

(i) Die Strukturkonstanten $c_{\alpha,\beta,i,j}$ mit $i\alpha+j\beta\in R$ sind ungleich Null. die anderen Strukturkonstanten $c_{\gamma,\delta,i,j}$ sind durch erstere eindeuitg festgelegt.

(ii) Es gelte stets $c_{\alpha,\beta,i,j} = 1$ für alle α,β,i,j mit $i\alpha+j\beta\in R$ und $i,j \geq 0$. Dann sind alle Strukturkonstanten von der Gestalt $n\cdot 1_k$ mit $n\in\mathbb{Z}$. Falls gilt

$$\gamma,\delta,\gamma+\delta\in R\ ,\ \gamma - c\delta\in R\ ,\ \gamma - (c+1)\delta \notin R$$

so ist $c_{\gamma,\delta,1,1} = \pm\ (c+1)$.

Beweis.
QED.

11.2.8 Proposition

Sei rk R = 2 und seien α und β einfache Wurzeln. Dann gilt

$$n_\alpha n_\beta n_\alpha \ldots = n_\beta n_\alpha n_\beta \ldots$$

wobei auf jeder Seite die Anzahl der Faktoren gleich der Ordnung $m(\alpha,\beta)$ von $s_\alpha s_\beta$ in W ist.

Beweis.
QED.

11.2.9 Beliebiger Rang: die Abbildung ϕ: $W \to N_G(T)$.

Wir nehmen jetzt an, der Rang des Wurzelsystems R ist beliebig. Wir verwenden weiter die oben eingeführten Bezeichnungen.

Sei $w \in W$ und sei $w = s_{\alpha_1} \cdot \ldots \cdot s_{\alpha_h}$ eine kürzeste Zerlegung mit einfachen Wurzeln α_i. Es folgt aus 11.2.8 und 10.2.4 daß

$$\phi(w) := n_{\alpha_1} \cdot \ldots \cdot n_{\alpha_h} \in N_G(T)$$

nur von w und nicht von der speziellen Wahl der kürzesten Zerlegung von w abhängt. Das Element

$$\phi(w)$$

ist ein Repräsentant von $w \in W$ in $N_G(T)$, und es gilt $\phi(s_\alpha) = n_\alpha$.

11.2.10 Aufgabe

(a) Sei $\phi(w)$ wie in 11.2.9. Man zeige,

$$\phi(ww') = \phi(w)\phi(w')c(w,w')$$

für alle $w,w' \in W$ mit $c(w,w') \in T$ und $c(w,w')^2 = e$. Es gilt

$$c(w,w') = 1 \text{ falls } l(ww') = l(w) + l(w').$$

(b) Sei $\bar{W}$ die von den n_α mit $\alpha \in D$ erzeugte Gruppe. Dann ist $\bar{W}$ eine Erweiterung von W durch eine elementare abelsche 2-Gruppe (Mehr Einzelheiten über $\bar{W}$ findet man in [35]).

11.2.11 Proposition

Seien $\gamma,\delta \in D$ und $w \in W$ derart, daß gilt $w\gamma = \delta$. Dann gilt

$$\phi(w)x_\gamma(\xi)\phi(w)^{-1} = x_\delta(\xi) \text{ für alle } \xi \in k.$$

Beweis.

QED.

11.3. G als abstrakte Gruppe

11.3.1 Konstruktion

Ausgangsdaten:

Seien

$$G$$

eine reduktive zusammenhängende lineare algebraische Gruppe,

$$T \subseteq G$$

ein maximaler Torus und

$$\Psi = (X, X^v, R, R^v)$$

das Wurzel-Datum von G bezüglich T.

Wir werden zeigen, G ist durch Ψ vollständig bestimmt. Als Vorbereitung diskutieren wir jetzt eine Darstellung von G als abstrakte Gruppe.

Bezeichnungen:

R^+ ein System positiver Wurzeln in R.

D Basis der einfachen Wurzeln von R^+

$R_{\alpha,\beta}$ das durch die Wurzeln $\alpha,\beta \in D$ definierte Wurzelsystem $(\mathbb{R}\alpha+\mathbb{R}\beta)\cap\mathbb{R}$. Im Fall $\alpha \neq \beta$ ist $R_{\alpha,\beta}$ vom Rang 2 und hat $\{\alpha, \beta\}$ als Basis (einfacher Wurzeln).

R_1 $:= \cup_{\alpha,\beta\in D} R_{\alpha,\beta}$

$(x_\alpha)_{\alpha\in R}$ eine Realisierung von R in G (vgl. 11.2.4)

$c_{\alpha,\beta,i,j}$ die Strukturkonstanten zur gegebenen Realisierung

Die Gruppe $\tilde{G}$:

Wir geben jetzt eine Darstellung einer Grupp $\tilde{G}$ an. Diese wird nur vom Körper k, von Ψ und den Strukturkonstanten $c_{\alpha,\beta,i,j}$ von je zwei Wurzeln $\alpha, \beta \in D$ abhängen, die beide in einem $R_{\alpha,\beta}$ liegen. Die Bestandteile der Darstellung sind die folgenden.

(a) $\tilde{T} := \mathrm{Hom}(X,k^*)$, die Gruppe der Gruppenhomomorphismen. Wir definieren einen Homomorphismus

$$\pi: \tilde{T} \to T$$

durch die Bedingung

$$x(\pi\tilde{t}) := \tilde{t}(x) \text{ für } x\in X.$$

Aus unserer Diskussion algebraische Tori in 2.5 ergibt sich, daß π wohldefiniert und ein Isomorphismus ist (man überprüfe das, indem man $T = (k^*)^n$ annehme). Die zu π gehörige Umkehrabbildunge ist gegeben durch

$$\pi^{-1}t(x) = x(t) \text{ für } t\in T \text{ und } x\in X\text{-}$$

Für jedes $x\in X$ definieren wir einen Homomorphismus

$$\tilde{x} : \tilde{T} \to k^*, \tilde{t} \mapsto \tilde{t}(x).$$

Für jedes $u\in X^v$ definieren wir einen Homomorphismus

$$\tilde{u} : k^* \to \tilde{T}, \xi \mapsto (x \mapsto \xi^{<x,u>}).$$

Die Weyl-Gruppe $W = W(G,T)$ operiert auf $\tilde{T}$ durch

$$W\times\tilde{T} \to \tilde{T}, (w, \tilde{t}) \mapsto (x \mapsto \tilde{t}(w^{-1}x)).$$

(b) Für jedes $\gamma\in R_1$ und jedes $\xi\in k$ fixieren wir einen Erzeuger

$$\tilde{x}_\gamma(\xi)$$

von $\tilde{G}$ (zusammen mit den Elementen von $\tilde{T}$). Wir unterwerfen diese Erzeuger den folgenden Relationen.

(1) $\tilde{x}_\gamma(\xi+\eta) = \tilde{x}_\gamma(\xi)\,\tilde{x}_\gamma(\eta)$

für $\xi,\eta \in k$

(2) $\tilde{x}_\gamma(\xi)\,\tilde{x}_\delta(\eta)\,\tilde{x}_\gamma(\xi)^{-1} = \tilde{x}_\delta(\eta) \prod_{i\gamma+j\delta \in R, i,j>0} \tilde{x}_{i\gamma+j\delta}(c_{\gamma,\delta,i,j}\xi^i\eta^j)$

für $\xi,\eta \in k$, falls $\gamma,\delta \in D$ linear unabhängig sind und beide in einem $R_{\alpha,\beta}$ liegen.

(3) $\tilde{t}\,\tilde{x}_\gamma(\xi)\tilde{t}^{-1} = \tilde{x}_\gamma(\tilde{\gamma}(\tilde{t})\xi)$

für $\xi \in k$, $\tilde{t} \in \tilde{T}$.

(c) Für jedes $\gamma \in R_1$ setzen wir

$$\tilde{n}_\gamma := \tilde{x}_\gamma(1)\tilde{x}_{-\gamma}(-1)\,\tilde{x}_\gamma(1).$$

Dann operiert $\tilde{n}_\gamma$ auf $\tilde{T}$ durch

$$\tilde{n}_\gamma \tilde{t}\,\tilde{n}_\gamma^{-1}(x) = \tilde{t}(s_\gamma x).$$

Wir unterwerfen die Erzeuger $\tilde{x}_\gamma(\xi)$ weiterhin den folgenden Relationen.

(4) $\tilde{n}_\gamma \tilde{x}_\gamma(\xi)\tilde{n}_\gamma^{-1} = \tilde{x}_{-\gamma}(-\xi)$ für $\xi \in k$

(5) $\tilde{n}_\gamma^2 = \tilde{t}_\gamma \in \tilde{T}$ mit $\tilde{t}_\gamma(x) := (-1)^{\langle x,\gamma^v\rangle}$ für $x \in X$.

(6) $\tilde{n}_\alpha\tilde{n}_\beta\tilde{n}_\alpha\cdot\ldots = \tilde{n}_\beta\tilde{n}_\alpha\tilde{n}_\beta\cdot\ldots$

mit $m(\alpha,\beta)$ Faktoren auf beiden Seiten, $\alpha,\beta \in D$, $\alpha \neq \beta$. Dabei sei $m(\alpha,\beta)$ die Ordnung von $s_\alpha s_\beta$ in $W(G,T)$.

(7) $\tilde{x}_\gamma(\xi)\,\tilde{x}_{-\gamma}(-\xi^{-1})\tilde{x}_\gamma(\xi) = \tilde{\gamma}^v(\xi)n_\gamma$ für $\xi \in k^*$.

Sei $\tilde{G}$ die von $\tilde{T}$ und den $\tilde{x}_\gamma(\xi)$ mit $\gamma \in R_1$ und $\xi \in k$ erzeugte Gruppe, die den obigen Relationen (1), ... , (7) genügen.
Da die entsprechenden Relationen in G gelten, kann der Homomorphismus

$$\pi : \tilde{T} \to T$$

zu einem Homomorphismus

$$\pi : \tilde{G} \to G$$

fortgesetzt werden.

11.3.2 Theorem: Bijektivität des Homomorphismus π

Der in 11.3.1 konstruierte Homorphismus

$$\pi : \tilde{G} \to G$$

ist ein Isomorphismus abstrakter Gruppen.

Bemerkung

Die angegebenen Relationen sind nicht unabhängig. Einige von ihnen kann man weglassen (vgl. 11.3.3(2)).

Beweis.

QED.

11.3.3 Aufgaben

11.3.4 Dynkin-Diagramme

Als eine erste Konsequenz des Strutursatzes 11.3.2 werden wir eine Eindeutigkeitsaussage für die Strukturkonstanten ableiten.

Vorher erinnern wir an die Definition des Dynkin-Diagramms eines Wurzelsystems R mit der Basis D. Dies ist ein Graph $\mathfrak{D}$, dessen Ecken die Elemente von D sind,

$$\text{Menge der Ecken von } \mathfrak{D} := D.$$

Je zwei verschiedene Ecken α und β werden durch

$$<\alpha, \beta^v><\beta, \alpha^v>$$

Kanten verbunden. Falls die Wurzeln unterschiedliche Länge haben, so sollen die Kanten von der längeren zu kürzeren Wurzel verlaufen.

Zwei Wurzeln sind also genau dann nicht durch eine Kante verbunden, wenn sie senkrecht aufeinander stehen bezüglich einer W-invarianten positiv definiten symmetrischen Bilinearform.

Wir erinnern an einige Eigenschaften der Dynkin-Diagramme. Die Beweise findet man in [8, Ch. VI].

(a) Das Wurzelsystem R heißt irreduzibel, wenn es nicht Vereinigung von zwei paarweise aufeinander senkrecht stehenen Teilsystemen ist. Jedes Wurzelsystem ist Vereinigung von paarweise orthogonalen irreduziblen Wurzelsystemen (vgl. Aufgaben 9.4.3).

Im folgenden sei R irreduzibel.

(b) $\mathfrak{D}$ ist zusammenhängend und ist ein Baum, d.h. $\mathfrak{D}$ enthält keine Zyklen.

(c) Tritt in $\mathfrak{D}$ eine dreifache Kante auf, so ist R vom Type G_2

(d) Tritt in $\mathfrak{D}$ eine doppelte Kante auf, so ist $\mathfrak{D}$ eine Kette (linear geordnet) und es gibt nur eine solche doppelte Kante. Die Menge

$$\{(\alpha,\alpha) \mid \alpha \in D\}$$

enthält dann nur zwei Elemente.

Die möglichen Dykin-Diagramme irreduzibler Wurzelsysteme sind in [8, Ch. VI, p. 197] aufgezählt.

Wir sagen D bzw. R ist einfach verknüpft, wenn mehrfache Kanten nicht auftreten. In der Situation von (d) spricht man von langen und kurzen Wurzeln von R.

11.3.5 Lemma:
Es gibt eine Zerlegung

$$D = D_1 \cup D_2$$

von D in zwei disjunkte Teilmengen mit der Eigenschaft, daß je zwei verschiedenen Wurzeln aus demselben D_i senkrecht aufeinander stehen.

Beweis.

QED.

11.3.6 Theorem: Vergleich von Systemen normierter Strukturkonstanten

Seien

$$G$$

eine reduktive zusammenhängende lineare algebraische Gruppe,

$$T \subseteq G$$

ein maximaler Torus und

$$\Psi = (X, X^V, R, R^V)$$

das Wurzel-Datum von G bezüglich T.
Weiter seien D eine Basis von R und $D = D_1 \cup D_2$ eine Zerlegung wie in 11.3.5. Dann gilt:

(i) Es gibt ein eindeutig bestimmtes System von Strukturkonstanten $c_{\gamma,\delta,i,j}$ (für eine geeignete Realisierung von G) mit den folgenden Eigenschaften.

(a) Haben $\alpha \in D_1$ und $\beta \in D_2$ dieselbe Länge und liegt $\alpha+\beta$ in R, so gilt $c_{\alpha,\beta,1,1} = 1$.

(b) Ist $\alpha \in D$ eine kurze Wurzel und $\beta \in D$ ein lange mit $\alpha+\beta \in R$, so gilt

$$c_{\alpha,\beta,i,j} = 1 \text{ für alle } i,j>0 \text{ mit } i\alpha+j\beta \in R.$$

(ii) Es gibt eine Realisierung $(x_\gamma)_{\gamma \in R}$ mit der Eigenschaft, daß die zugehörigen Strukturkonstanten die Bedingungen von (i) erfüllen und daß außerdem gilt

$$\phi(w)x_\gamma(\xi)\phi(w)^{-1} = x_{w\gamma}(\pm\xi)$$

für $\gamma \in R$, $w \in W$, $\xi \in k$ ($\phi : W \to N_G(T)$ sei wie in 11.2.9). In dieser Situation sind alle Strukturkonstanten von der Gestatl $n \cdot 1$ mit $n \in \mathbb{Z}$. Für

$$\gamma, \delta \in R, \gamma+\delta \in R, \gamma - c\delta \in R, \gamma - (c+1)\delta \notin R$$

ist

$$c_{\gamma,\delta,1,1} = \pm (c+1) \text{ und } c_{\gamma,\delta,1,1}c_{-\gamma,-\delta,1,1} = -(c+1)^2.$$

(iii) Ist $(x'_\gamma)_{\gamma \in R}$ eine weitere Realisierung mit den Eigenschaften von (ii), so gibt es Vorzeichen $\varepsilon_\gamma = \pm 1$ ($\gamma \in R$) mit $\varepsilon_\gamma = \varepsilon_{-\gamma}$ und

$$x'_\gamma(\xi) = x_\gamma(\varepsilon_\gamma \xi)$$

für $\gamma \in R$ und $\xi \in k$.

Beweis.

QED.

11.3.7 Folgerung: Eindeutigkeit der Strukturkonstanten

Die Strukturkonstanten $c_{\alpha,\beta,ij}$ (zu einer festen Ordnung von R) sind bis auf Äquivalenz im Sinne von 11.2.4 durch das Wurzelsystem R eindeutig festgelegt.

Beweis.

QED.

11.3.8 Eine Variante des Isomorphie-Satzes von 11.3.2

Wir beenden dieses Kapitel mit einer Variantes des Satzes 11.3.2.

Der Torus $\tilde{T}$ sei wie in 11.3.2 definiert. Für jede positive Wurzel γ und jedes $\xi \in k$ sei ein Symbol

$$\tilde{x}'_\gamma(\xi)$$

gegeben, so daß die Analoga (1)', (2)', (3)' von (1), (2) und (3) erfüllt sind. Weiter sei für jedes $\alpha \in D$ ein Symbol

$$\tilde{n}'_\alpha$$

gegeben, so daß die Analoga (5)', (6)' von (5) und (6) erfüllt sind und außerdem gelte

(7)' $\quad \tilde{x}'_\alpha(\xi)\tilde{n}'_\alpha\tilde{x}'_\alpha(\xi^{-1})\tilde{n}'_\alpha\tilde{x}'_\alpha(\xi) = \tilde{\alpha}^\vee(\xi)\tilde{n}'_\alpha$ für $\alpha \in D, \xi \in k^*$.

Sei $\tilde{G}'$ die von $\tilde{T}$, den $\tilde{x}'_\gamma(\xi)$ ($\gamma>0$, $\xi \in k$) und den $\tilde{n}'_\alpha$ ($\alpha \in D$) erzeugte Gruppe mit den Relationen (1)'-(7)' und außerdem

(8)' $\quad \tilde{n}'_\alpha \tilde{t} \tilde{n}'^{-1}_\alpha = s_\alpha(\tilde{t})$ für $\tilde{t} \in \tilde{T}, \alpha \in D$.

Dann gibt es einen offensichtlichen Gruppen-Homomorphismus

$$\pi': \tilde{G}' \to G.$$

11.3.9 Der Satz

Der in π' konstruierte Gruppen-Homomorphismus ist bijektiv.

Beweis.

QED.

11.4. The isomorphism theorem

11.4.1 Lemma: Kriterium für Morphismen

Seien G und G' algebraische Gruppen und $\psi: G \to G'$ ein Homomorphismus abstrakter Gruppen. Es existiere eine nicht-leere offene Teilmenge

$$U \subseteq G$$

derart, daß die Einschränkung von ψ auf U ein Morphismus von Varietäten ist. Dann ist ψ ein Homomorphismus algebraischer Gruppen.

Beweis.

QED.

11.4.2 Die Situation

Seien G und G' zwei zusammenhängende reduktive lineare algebraische Gruppen mit den maximalen Tori T bzw. T' und den Wurzel-Data

$$\Psi = (X, X^\vee, R, R^\vee) \text{ und } \Psi' = (X', X'^\vee, R', R'^\vee).$$

Sei weiter

$$\psi: G \to G'$$

ein surjektiver Homomorphismus algebraischer Gruppen mit endlichem Kern. Ein solcher Homomorphismus heißt Isogenie.

Bemerkungen

(i) Der Kern $\mathrm{Ker}(\psi)$ ist eine zentrale Untergruppe von G (vgl. 2.2.2(3)), liegt also in T (vgl. 9.3.6(iii)). Weiter folgt

$$\dim G = \dim G'.$$

(ii) ψ definiert einen Homomorphismus der Charaktergruppen

$$f := X(\psi): X' = X(T') \to X := X(T)$$

und einen Homomorphismus

$$f^v: X^v \to X'^v$$

der 1-Parameter-Untergruppen mit $f^v u = f \circ u$. Es gilt

$$(x', f^v u) = (fx', u) \text{ für } x' \in X', u \in X^v.$$

(iii) Sei $\alpha \in R$. Ist X_α die wie in 9.3.6 definierte Untergruppe, so ist ψX_α eine zusammenhängende 1-dimensionale Untergruppe von X', welche von T' normalisiert, aber nicht zentralisiert wird. Nach 9.3.10 (1) gibt es eine Wurzel $\alpha' \in R'$ mit

$$\psi X_\alpha = X_{\alpha'},$$

Ist umgekehrt $\alpha' \in R'$, so ist $(\psi^{-1}(X_{\alpha'},)^0$ eine zusammenhängende unipotente 1-dimensionalen Untergruppe von G, die durch T normalisiert wird, also gleich einer der Gruppen X_α. Damit gibt es eine Bijektion

$$u: R \to R' \text{ mit } \psi X_\alpha = X_{u\alpha} \text{ für jedes } \alpha \in R.$$

(iv) Sei jetzt $\psi: G \to G'$ ein Isomorphismus algebraischer Gruppen. Es ist dann klar, daß $f(u(\alpha)) = \alpha$ gilt für $\alpha \in R$. Also definiert f einen Isomrophismus

$$\Psi' \to \Psi$$

der Wurzelsysteme, d.h. einen Isomorphismus $X' \to X$, welcher R' auf R abbildet, wobei der duale Isomorphismus $X^v \to X'^v$ die Kowurzeln R^v auf die Kowurzeln R'^v abbildet. Wir schreiben

$$f = f(\psi).$$

11.4.3 Theorem (Isomorphiesatz)

Sei $f: \Psi' \to \Psi$ ein Isomorphismus. Dann gibt es einen Isomorphismus algebraischer Gruppen $\psi: G \to G'$ mit $\psi T = T'$ und $f = f(\psi)$. Ist ψ' ein zweiter solcher Isomorphismus, so gibt es ein $t \in T$ mit

$$\psi'(x) = \psi(txt^{-1})$$

für alle $x \in G$.

Beweis.

QED.

11.4.4 Wurzelsysteme mit Automorphismus, die die Zerlegung D = D'∪D" respektiert

Zur späteren Verwendung diskutieren wir eine Anwendung des Isomorphie-Satzes 11.4.3. Wir fixieren ein System

$$R^+$$

positiver Wurzeln und bezeichnen mit

$$D$$

die zugehörige Basis, mit

$$\mathfrak{D}$$

das zugehörige Dynkin-Diagramm. Sei

$$D = D' \cup D''$$

eine Zerlegung von D wie in 11.3.5. Wir machen die folgende Annahmen.

(a) G ist halbeinfach und vom adjungierten Typ (vgl. 9.4.2). Das bedeutet, X = Q (d.h. die Wurzeln erzeugen die Charaktergruppe).

(b) $\mathfrak{D}$ ist einfach verknüpft (vgl. 11.3.4), d.h. es gibt keine mehrfachen Kanten.

(c) Es gibt einen Automorphismus f von $\mathfrak{D}$ mit f(D') = D' und f(D") = D".

Da D eine Basis von Q ist (nach (a)), läßt sich f zu einen Automorphismus von Q fortsetzen, der auch mit f bezeichnet wird. Es ist klar, daß f einen Isomorphismus des Wurzeldatums

$$\Psi(G) = (Q^V, Q, R, R^V)$$

mit sich selbst definiert. Sei h die Ordnung von f (als Element der Endlichen Automorphismengruppe Ψ).

11.4.5 Folgerung: ein Automorphismus von G

In der Situation von 11.4.4 gibt es einen Automorphismus algebraischer Gruppen

$$\phi: G \to G$$

mit $f(\phi) = f$. Dieser Automorphismus ϕ hat dieselbe Ordnung h wie f.

Beweis.

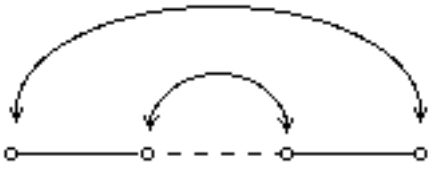
QED.

11.4.6 Die Dynkin-Diagramm der irreduziblen Wurzelsysteme

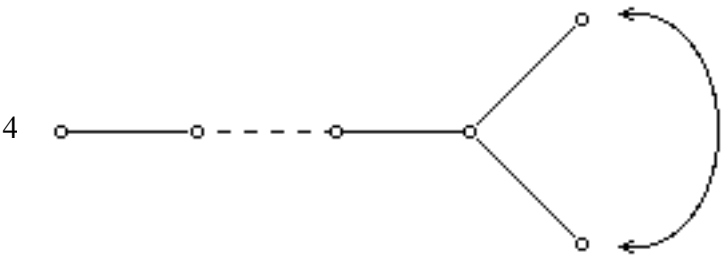
Bis jetzt haben wir die Klassifikation der Dynkin-Diagramme irreduzibler Wurzel-Systeme nicht benutzt. In dieser Stelle ist es nützlich, diese Klassifikation zu rekapitulieren (um das letzte Ergebnis zu illustrieren). Wir verweisen auf [8, Chap. VI, p. 250-275] bezüglich der Einzelheiten in Hinsicht auf die Klassifikation.

Die Dynkin-Diagramme der einfach verknüften irreduziblen Wurzel-Systeme sind die folgenden. Die Pfeile weisen auf den Automorphismus f der Ordnung 2 von 11.4.2 hin.

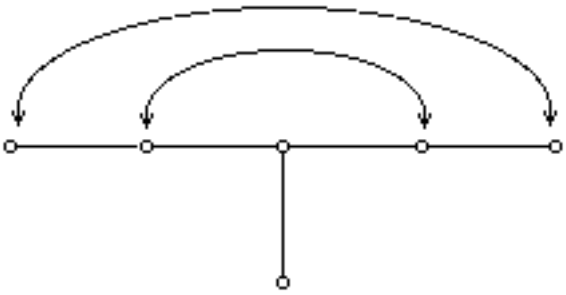
A_l mit $l \geq 1$:



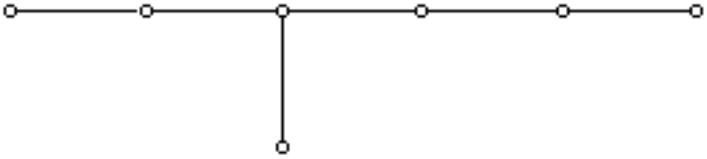
D_l mit $l \geq 4$



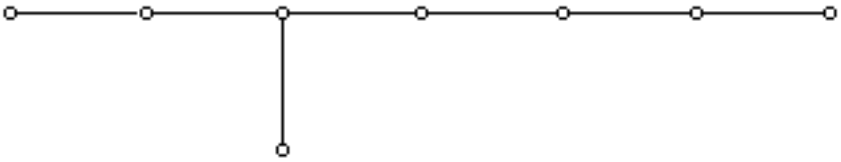
E_6:



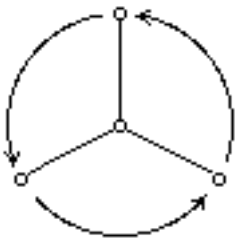
E_7:



E_8:



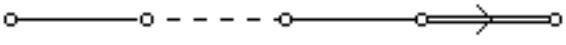
Außer den angegebenen Automorphismen gibt beim Typ D_4 einen Automorphismus der Ordnung 3 (wie man am Diagramm direkt abliest).



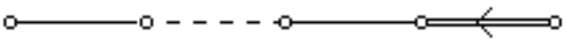
Weitere Automorphismen, die die Bedingunge (c) von 11.4.4 erfüllen, gibt es nicht. Ausgenommen A_l mit l gerade.

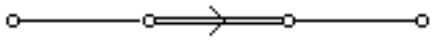
Die Dynkin-Diagramme mit mehrfachen Kanten sind die folgenden:

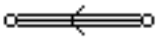
B_l mit $l \geq 2$:



C_l mit $l \geq 2$



F_4 : 

G_2 : 

Diese kann man aus den einfach verknüpften Diagrammen durch Zusammenfalten mit Hilfe eines Automorphismus f erhalten. Wir werden uns damit mit nächsten Kapitel (vgl. 12.17) beschäftigen. Dort werden wir diese Art von Verheftung benutzen, den Existenzsatz (für Wurzel-Daten zu gegebenen Wurzelsystemen) auf den einfach verknüpften Fall zurückzuführen.

11.4.7 p-Morphismen von Wurzel-Systemen

Es gibt eine Verallgemeinerung des Isomorphie-Satzes, welche Aussagen über Isogenien macht. Wir werden diese Aussagen kurz diskutieren.

Sei

$$\phi: G \to G'$$

eine Isogenie von zusammenhängenden reduktiven linearen algebraischen Gruppen.Wir benutzen die Bezeichnungen von 11.4.2 (für maximale Tori , Wurzelsysteme, ... der beteiligten Gruppen). Man beachte, die induzierte Abbildung

$$f: X' \to X$$

der Charaktergruppen ist ein injektiver Homomorphismus und das Bild fX' hat endlichen Index in X (denn der Index ist gleich der Ordnung des Kerns). Seien

$$(x_\alpha)_{\alpha\in R} \text{ und } (x'_{\alpha'})_{\alpha'\in R'}$$

Realisierungen von G bzw. G'. Dann gilt

$$\phi x_\alpha(\xi) = x'_{u\alpha}(h(\xi))$$

mit $h\in k[T]$, u geeignet und

$$h(\xi+\eta) = h(\xi) + h(\eta).$$

Falls die Charakteristik von p von k gleich Null ist, so gilt

$$h(\xi) = a\xi$$

mit einem $a\in k^*$. Ist die Charakteristik $p > 0$, so ist h ein p-Polynom (vgl. 2.6.3). Außerdem gilt

$$tx_\alpha(\xi)t^{-1} = x_\alpha(\alpha(t)\xi).$$

Wir erhalten damit

$$h(\alpha(t)\xi) = h((u\alpha)(\phi(t)\xi)) \text{ für } t\in T \text{ und } \xi\in k.$$

Es folgt im Fall $p>0$ die Existenz von p-Potenzen $q(\alpha)$ mit

$$f(u\alpha) = q(\alpha)\alpha$$

und

$$f^v(\alpha^v) = q(\alpha)(u\alpha)^v$$

(man verwende 11.2.1). Im Fall $p = 0$ definieren wir

$$q(\alpha) := 1$$

für jedes $\alpha\in R$. Die obigen Formel gelten dann auch in diesem Fall.

Definition

Wir sagen, f: X'→X , u: R →R' und die Funktion q: R → $\{p^n \mid n=1,2,3,...\}$ definieren einen p-Morphismus

$$\Psi' \to \Psi$$

falls die oben angegebenen Eigenschaften bestehen, d.h.

f: X' → X ist injektiv mit endlichem Kokern

u: R → R' ist bijektiv

$f(u\alpha) = q(\alpha)\alpha$ und $f^V(\alpha^V) = q(\alpha)(u\alpha)^V$ für alle $\alpha \in R$.

Bezeichnungen

Falls ein p-Morphismus (f,u, q) in der oben beschriebenen Art aus einer Isogenie ϕ: G→G' entsteht, so schreiben wir

$$f = f(\phi)\ ,\ u = u(\phi),\ q = q(\phi).$$

Beispiel

Ein Beispiel eines p-Morphismus im Fall p > 0 ist der Frobenius-Morphismus mit

$$\Psi' = \Psi,\ f = q\cdot Id,\ q := \text{eine p-Potenz.}$$

11.4.8 Lemma: Eigenschaften von q-Morphismen

(i) Für $\alpha,\beta \in R$ gilt $q(\beta) < u\alpha, (u\beta)^V> = q(\alpha)< \alpha, \beta^V>$

(ii) Für $\alpha,\beta \in R$ gilt $u(s_\alpha\beta) = s_{u\alpha}(u\beta)$

(iii) Für $\alpha \in R$ und $w \in W$ gilt $q(w\alpha) = q(\alpha)$

(iv) Für $\alpha,\beta \in R$, $<\alpha, \beta^V> > 0$ und $q(\alpha) < q(\beta)$ gilt p=2 oder

$$p=3 \text{ und } <\alpha, \beta^V> = p,\ <u\alpha, (u\beta)^V> = 1$$

Beweis.

QED.

11.4.9 Theorem (Isogenie-Satz)

Sei (f,u,ϕ) ein p-Morphismus $\Psi' \to \Psi$. Dann gibt es eine Isogenie

$$\phi: G \to G'$$

mit

$$\phi T = T',\ f(\phi) = f,\ u(\phi) = u,\ q(\phi) = q.$$

Ist ϕ' eine zweite solche Isogenie, so gibt es ein $t \in T$ mit

$$\phi' x = \phi(txt^{-1}) \text{ für alle } x \in G.$$

Beweis.

QED.

11.4.10 Aufgabe

Man vervollständige die Details im Beweis von von 11.4.9.

Notes

12. The existence theorem

Das letzte Kapitel ist dem Beweis des folgenden Satzes gewidmet.

12.1 Theorem (Existenzsatz)

Sei $\Psi = (X,R,X^V,R^V)$ ein Wurzeldatum. Dann gibt es eine zusammenhängende reduktive lineare algebraische Gruppe G mit einem maximalen Torus T derart, daß das Wurzeldatum $\Psi(G,T)$ isomorph ist zu Ψ.

12.2

Notes

Bibliography

For a more complete bibliography about linear algebraic groups, see [23].

[1] Azad, H., Structure constants of algebraic groups, preprint.
[2] Borel.A., Groups linéarires algébriques, Ann. Math. 64(1956)20-82.
[3] A. Borel, Linear algebraic groups, Benjamin, New York, 1969
[4] Borel, A.: Automorphic L-functions, Proc. Symp. Pure Math. 33, Part 2, Amer. Math. Soc.. 1979
[6] Borel, A., et al: Algebraic groups and related finite groups, Lecture Notes in Math 131, Springer-Verlag 1970.
[7] Bourbaki, N.: Algèbra commutative, Hermann, Paris, 1961-1965
[8] Bourbaki, N.: Algèbre de Lie, Hermann, Paris 1971-1975
[11] Chevalley, C., Classification des groupes de Lie algébriques, Séminaire Ecole Normale Supérieure, Paris 1956- 1958
[13] Demazure, M.: Désingularisation des variétés de Schubert, Ann. Ec. Norm. Sup. (4) 7 (1974) 53-88
[15] Deligne, P., Lusztig, G.: Representations of reductive groups over finite fields, Ann. Math. 103 (1976) 103-161
[21] Hartshorne,R. Algebraic geometry, Graduate Texts in Mathematics 52, Springer, New York 1977.
[23] Humphreys, J.E., Linear algebraic groups, Graduate Texts in Math. 21, Springer-Verlag 1975.
[26] Lang, S., Algebra, Addison-Wesley, 1965
[27] Lazard,M., Sur les groupes de Lie formels à un paramètre, Bull. Soc. Math. France 83(1955), 251-274.
[28] Mumford,D., Introduction to algebraic geometry, Notes Harvard University.
[29] Mumford,D., Abelian varieties, Oxford University Press, 1970
[35] Tits, J.: Normalisateurs de tores I. Groupes de Coxeter étendus, J. Alg. 4 (1966)96-116
[36] Weil,A,, Foundations of algebraic geometry, revised ed., Amer. Math. Soc., Providence 1962.

Index

—A—

action of a group by automorphisms, 97
additive group, 5
adjoint representation, 66
affine variety, 111
algebraic group, 4
algebraic torus, 26
algebraically dependent, 38

—B—

Borel subgroup, 146

—C—

Cartan subgroup, 148
center, 117
centralizer, 33
centralizer, 97
commutator map, 74
commutator subgroup, 117
complete, 139
conjugacy class, 97
connectedness, 7
cotangent space, 59

—D—

defined over a field, 77; 78
derivation, 48
diagonalizable, 26
differential, 49; 69
differentials, 52
direct product, 4
dominant, 59

—E—

elliptic curves, 6
equivariant, 9
equivariant affine embedding of a torus, 35

—F—

faithfull representation, 12
fiber, 58
field of definition, 77
finite, 85
first basic exact sequence, 54
fixed points, 90
Frobenius morphism, 78

—G—

G-morphism, 9
G-space, 9
G-variety, 9

—H—

higher commutator groups, 117
homogeneous space, 9
homomorphism of algebraic groups, 4

—I—

integral, 85
integral closure, 85
irreducibility, 7
isomorphism of algebraic groups, 4

—J—

Jordan decomposition, 16

—K—

k_0-morphism, 78
k_0-structure, 77
k_0-variety, 77

—L—

linear algebraic group, 4
locally finite, 10; 18
locally nilpotent, 18

—M—

maximal torus, 125; 146
multiplicative 1-parameter subgroup, 26
multiplicative Jordan decomposition, 18

—N—

nilpotent, 15
nilpotent, 117
nilpotent part, 18
non-singular, 51
normal, 86
normal, 86
normalizer, 33

—O—

open, 107

—P—

parabolic subgroup, 144
p-dependent, 38
perfect, 55
p-Lie algebra, 64
principal homogeneous space, 9
projectivation, 105
purely transcendental, 55

—Q—

quotient, 107

—R—

radical, 135
rational character, 25
rational representation, 9
reductive, 135
regulär, 161
restricted, 64

—S—

semi-simple, 15; 18; 24; 135
semi-simple part, 18; 19
separable, 54; 59
separable degree, 82
separably generated, 55
simple point, 51
smooth, 51
solvable, 117

—T—

tangent space, 49
torus, 26
transcendence degree, 55

—U—

unipotent, 15; 24
unipotent part, 18; 19
unipotent radical, 135
universal derivation, 52