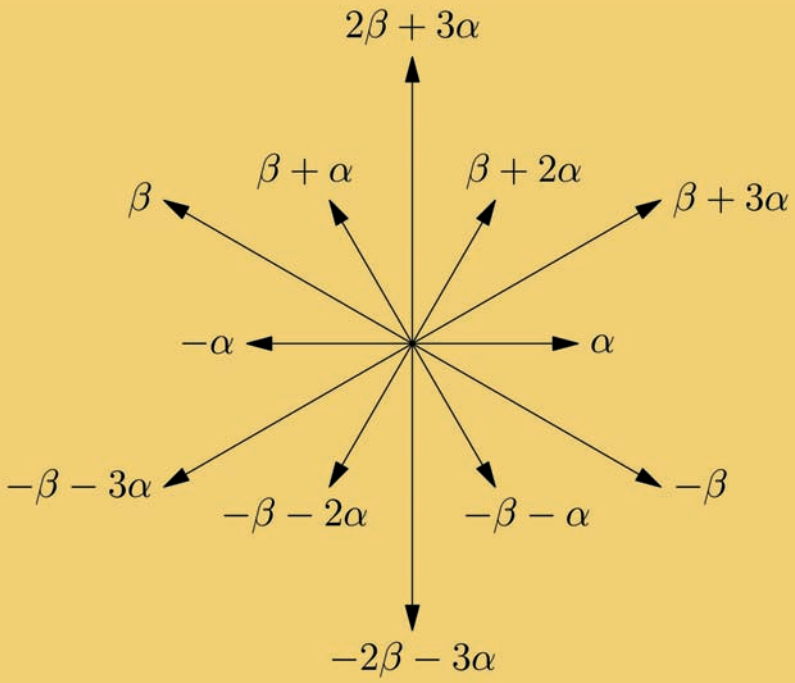
Ina Kersten

Lineare Algebraische Gruppen

LaTeX-Bearbeitung Ole Riedlin



G_2

$$n(\beta, \alpha) := 2\,\frac{\langle \beta, \alpha \rangle}{\langle \alpha, \alpha \rangle} = -3$$

Universitätsdrucke Göttingen

Ina Kersten

Lineare algebraische Gruppen

erschienen in der Reihe der Universitätsdrucke
im Universitätsverlag Göttingen 2007

Ina Kersten

Lineare algebraische Gruppen

LaTeX-Bearbeitung
von Ole Riedlin

Universitätsverlag Göttingen
2007

Bibliographische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über <http://dnb.ddb.de> abrufbar

Anschrift der Autorin

Prof. Dr. Ina Kersten
Bunsenstraße 3–5
37073 Göttingen

http://www.uni-math.gwdg.de/kersten/
kersten@uni-math.gwdg.de

Satz und Layout: Ina Kersten und Ole Riedlin
Umschlaggestaltung: Margo Bargheer

© 2007 Universitätsverlag Göttingen
http://univerlag.uni-goettingen.de
ISBN: 978-3-940344-05-2

Vorwort

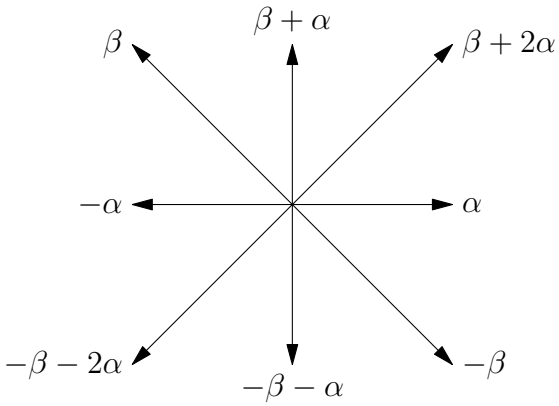
Dieser Universitätsdruck enthält mit einigen Ergänzungen den Stoff der Vorlesung *Lineare Algebraische Gruppen*, die ich im Sommersemester 2001 an der Universität Göttingen gehalten habe. Die Vorlesung schloss sich an die Algebra-Vorlesung an. Entsprechend setzt dieser Universitätsdruck die ebenfalls als Universitätsdruck erschienene Reihe *Analytische Geometrie und Lineare Algebra* (AGLA) und *Algebra* fort und dient im WS 2007/08 als Begleittext zur Vorlesung über lineare algebraische Gruppen. Soweit Ergebnisse aus den Universitätsdrucken AGLA I, II und Algebra benutzt werden, werden sie in der Form von „vgl. AGLA 11.4“ oder „vgl. Algebra 16.1“ zitiert.

Herzlich danke ich Nils Achtergarde und Kristin Stroth für das Korrekturlesen. Ein ganz besonderer Dank geht an Kristin Stroth für viele Anmerkungen und Verbesserungsvorschläge.

September 2007 *Ina Kersten*

Ein Beispiel

Wurzelsystem vom Rang 2:



B_2

$n(\beta, \alpha) := 2\,\frac{\langle \beta, \alpha \rangle}{\langle \alpha, \alpha \rangle} = -2$

Schreibweisen und Bezeichnungen

Abkürzende Schreibweisen

$A := B$	A ist definitionsgemäß gleich B
$\exists$	es gibt
$\forall$	für alle
$\Longrightarrow$	folgt
$\Longleftrightarrow$	genau dann, wenn
$\setminus$	ohne
$\square$	Ende des Beweises
$\lvert M\rvert$	Anzahl der Elemente der Menge M
$m \in M$	m ist Element der Menge M
$M \subset N$	M ist Teilmenge von N (schließt $M = N$ mit ein)
$a \leqslant b$	a ist kleiner oder gleich b
$a < b$	a ist kleiner als b

Standardbezeichnungen

$\mathbb{N} := \{1, 2, 3, \dots\}$ Menge der natürlichen Zahlen
$\mathbb{N}_0 := \{0, 1, 2, 3, \dots\}$
$\mathbb{Z} := \{0, \pm 1, \pm 2, \pm, \dots\}$ Ring der ganzen Zahlen
$\mathbb{Q}$ Körper der rationalen Zahlen
$\mathbb{R}$ Körper der reellen Zahlen
$\mathbb{C}$ Körper der komplexen Zahlen
$\mathbb{F}_q$ Körper mit q Elementen
$\emptyset$ Leere Menge (besitzt kein Element)

Bezeichnungen

$\mathrm{M}_{n\times n}(K)$ Ring der $n \times n$-Matrizen über K,
E_n Einheitsmatrix in $\mathrm{M}_{n\times n}(K)$,
$\mathrm{GL}_n(K)$ Gruppe der invertierbaren $n \times n$-Matrizen mit Einträgen in K,
$\mathrm{GL}(Z)$ Gruppe der Automorphismen eines Vektorraums Z,
$\mathrm{id}\colon M \to M\,,\ m \mapsto m\,,$ Identität,
${}^t x$ zu x transponierte Matrix,
$\overline{K}$ algebraischer Abschluss von K,
$K[X_1, \dots, X_n]$ Polynomring in n Unbestimmten,
$K[V] := K[X_1, \dots, X_n]/\mathfrak{I}(V)$ affiner Koordinatenring einer Varietät V,
$\mathfrak{I}(V) := \{f \in K[X_1, \dots, X_n] \mid f(x) = 0 \ \ \forall\, x \in V\}$ Verschwindungsideal,
$\mathfrak{V}(I) := \{x \in \overline{K}^{\,n} \mid f(x) = 0 \ \ \forall\, f \in I\}$, wobei I Ideal im Polynomring,
$\mathrm{Rad}(I) := \{r \in R \mid r^m \in I \text{ für ein } m\}$ Radikal eines Ideals I im Ring R,
$\mathfrak{I}_V(W) := \{\varphi \in K[V] \mid \varphi(w) = 0\ \forall\, w \in W\}$ für $W \subset V$,
$\mathfrak{V}_V(I) := \{v \in V \mid \varphi(v) = 0\ \forall\, \varphi \in I\}\,,$ wobei I Ideal in $K[V]$,
$\mathbb{E}$ euklidischer Vektorraum mit Skalarprodukt $E \times E \to \mathbb{R}$, $(\alpha, \beta) \mapsto \langle \alpha, \beta \rangle$.

Inhaltsverzeichnis

0 Worum geht es?

Wir gehen von einem Körper K aus. Bekanntlich bildet die Menge der invertierbaren $n \times n$-Matrizen

$$\mathrm{GL}_n(K) := \{x = (x_{ij})_{1 \leqslant i,j \leqslant n} \in \mathrm{M}_{n\times n}(K) \mid \det(x) \neq 0\}$$

eine Gruppe bezüglich Matrizenmultiplikation für jedes $n \in \mathbb{N}$.
Lineare Gruppen sind Untergruppen einer „allgemeinen linearen Gruppe“ $\mathrm{GL}_n(K)$.
Lineare algebraische Gruppen sind Untergruppen einer Gruppe $\mathrm{GL}_n(K)$, die durch endlich viele polynomiale Gleichungen $f(X_{ij}) = 0$ in n^2 Unbestimmten X_{ij} definiert sind (die n^2 Unbestimmten stehen für die n^2 Matrixeinträge).

0.1 Beispiele für lineare algebraische Gruppen

1) Es ist

$$\begin{aligned}\mathrm{SL}_2(K) &:= \{x \in \mathrm{GL}_2(K) \mid \det(x) = 1\} \\ &= \left\{ \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \in \mathrm{GL}_2(K) \;\middle|\; x_{11}x_{22} - x_{12}x_{21} - 1 = 0 \right\}\end{aligned}$$

definiert durch die polynomiale Gleichung $X_{11}X_{22} - X_{12}X_{21} - 1 = 0$.

2) Allgemein ist die *spezielle lineare Gruppe*

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

durch die polynomiale Gleichung $\det(X_{ij}) - 1 = 0$ in den n^2 Unbestimmten X_{ij} definiert. Dass die Determinante als Polynom im Ring $K[(X_{ij})_{1 \leqslant i,j \leqslant n}]$ aufgefasst werden kann, folgt aus der *Leibniz-Formel* für die Determinante (vgl. Aufgabe 1). Für $x = (x_{ij}) \in \mathrm{M}_{n\times n}(K)$ gilt

$$\boxed{\det(x) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma)\, x_{1\sigma(1)} \cdot \ldots \cdot x_{n\sigma(n)}}.$$

3) Die Gruppe der *oberen Dreiecksmatrizen*

$$\Delta_n(K) := \left\{ \begin{pmatrix} * & \cdots & * \\ & \ddots & \vdots \\ 0 & & * \end{pmatrix} \in \mathrm{GL}_n(K) \right\}$$

ist durch die $\frac{n(n-1)}{2}$ polynomialen Gleichungen $X_{ij} = 0$ für $i > j$ definiert.

4) Die Gruppe der *Diagonalmatrizen*

$$\mathrm{D}_n(K) := \left\{ \begin{pmatrix} * & & 0 \\ & \ddots & \\ 0 & & * \end{pmatrix} \in \mathrm{GL}_n(K) \right\}$$

ist durch die n^2-n polynomialen Gleichungen $X_{ij} = 0$ für $i \neq j$ definiert.

5) Die Gruppe der *unipotenten Matrizen*

$$\mathrm{U}_n(K) := \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in \mathrm{GL}_n(K) \right\}$$

ist durch die polynomialen Gleichungen $X_{ij} = 0$ für $i > j$ und $X_{ii}-1 = 0$ definiert.

6) Die *orthogonale Gruppe*

$$\mathrm{O}_3(\mathbb{R}) := \left\{ x \in \mathrm{GL}_3(\mathbb{R}) \;\middle|\; {}^t\!xx = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} =: E_3 \right\}$$

ist durch die 9 polynomialen Gleichungen

$$\boxed{X_{1i}X_{1j} + X_{2i}X_{2j} + X_{3i}X_{3j} - \delta_{ij} = 0}$$

mit $i, j \in \{1, 2, 3\}$ definiert, wobei $\delta_{ij} = \begin{cases} 1 & \text{für } i = j \\ 0 & \text{für } i \neq j \end{cases}$ das *Kronecker-Symbol* bezeichnet. Analog ist für $n > 1$ die orthogonale Gruppe $\mathrm{O}_n(\mathbb{R})$ durch n^2 polynomiale Gleichungen definiert.

Bemerkung
Es ist $\mathrm{O}_3(\mathbb{R}) = \operatorname{Stab} E_3$ der Stabilisator von E_3 unter der Operation

$$\mathrm{M}_{3\times 3}(\mathbb{R}) \times \mathrm{GL}_3(\mathbb{R}) \to \mathrm{M}_{3\times 3}(\mathbb{R}),\ (A, T) \mapsto {}^t\!TAT\,.$$

7) Die *symplektische Gruppe* ($\operatorname{char}(K) \neq 2$)

$$\mathrm{Sp}_{2m}(K) = \left\{ x \in \mathrm{GL}_{2m}(K) \;\middle|\; {}^t\!x \left(\begin{array}{c|c} 0 & E_m \\ \hline -E_m & 0 \end{array} \right) x = \left(\begin{array}{c|c} 0 & E_m \\ \hline -E_m & 0 \end{array} \right) \right\}$$

ist durch $(2m)^2$ polynomiale Gleichungen definiert.

8) Die *multiplikative Gruppe* $K^* := \{x \in K \mid x \neq 0\}$ ist isomorph zur linearen algebraischen Gruppe

$$\mathbb{G}_{\mathrm{m}}(K) := \left\{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \in \mathrm{GL}_2(K) \right\}$$

definiert durch die Gleichungen $X_{12} = 0$, $X_{21} = 0$ und $X_{11}X_{22} - 1 = 0$ (der Buchstabe ‚m' bei $\mathbb{G}_{\mathrm{m}}$ steht für multiplikativ).

9) Die Gruppe $\mathrm{GL}_n(K)$ ist isomorph zur linearen algebraischen Gruppe

$$\left\{ x \in \mathrm{GL}_{n+1}(K) \;\middle|\; x = \left(\begin{array}{ccc|c} & & & 0 \\ & y & & \vdots \\ & & & 0 \\ \hline 0 & \dots & 0 & \det(y)^{-1} \end{array}\right) \text{ mit } y \in \mathrm{GL}_n(K) \right\}$$

definiert durch die Gleichungen $X_{i,n+1} = X_{n+1,j} = 0$ für $1 \leqslant i, j \leqslant n$ und $\det\left((X_{ij})_{1 \leqslant i,j \leqslant n}\right) \cdot X_{n+1,n+1} - 1 = 0$.

0.2 Beispiele für affine algebraische Gruppen

Eine *affine algebraische Gruppe* G ist eine Teilmenge von K^n, die durch polynomiale Gleichungen definiert ist und die mit einer algebraisch definierten Gruppenstruktur

$$G \times G \to G,\ (x, y) \mapsto x \circ y\,,$$
$$G \to G,\ x \mapsto x^{-1}\,,$$

versehen ist (genaue Definition in Kapitel 3).

- Matrizenmultiplikation ist algebraisch definiert. Jede lineare algebraische Gruppe ist also eine affine algebraische Gruppe.

Wir werden in der Vorlesung zeigen, dass umgekehrt jede affine algebraische Gruppe eine lineare algebraische Gruppe ist.

Beispiele 1. Die *additive Gruppe* $\mathbb{G}_{\mathrm{a}}(K) := \{x \in K\}$ ist durch das Nullpolynom definiert und hat die Gruppenstruktur

$$(x, x') \mapsto x + x' \quad \text{und} \quad x \mapsto -x\,.$$

Es ist $\mathbb{G}_{\mathrm{a}}(K) \simeq K^+ \simeq \mathrm{U}_2(K)$ (wie in 0.1.5 definiert).

2. Die *Kreisgruppe* $S^1(\mathbb{R}) = \{(a,b) \in \mathbb{R}^2 \mid a^2+b^2=1\}$ ist eine affine algebraische Gruppe mit der Verknüpfung
$$(a,b)(a',b') = (aa'-bb', ab'+a'b)\,,$$
dem Einselement $(1,0)$ und dem Inversen $(a,b)^{-1} = (a,-b)$ für alle $(a,b) \in S^1(\mathbb{R})$. Es ist $S^1(\mathbb{R})$ isomorph zur linearen algebraischen Gruppe
$$\mathrm{SO}_2(\mathbb{R}) := \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) \right\},$$
definiert durch die Gleichungen: $X_{11} - X_{22} = 0$ und $X_{12} + X_{21} = 0$. Diese Gruppe beschreibt die Drehungen der Ebene um 0, vgl. auch AGLA 10.8.

Frage
Was passiert, wenn man Koeffizienten aus $\mathbb{C}$ zulässt?
Es ist (analog zu oben)
$$\mathrm{SO}_2(\mathbb{C}) := \left\{ \begin{pmatrix} z_1 & -z_2 \\ z_2 & z_1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C}) \right\}.$$
Setze $T := \left(\begin{smallmatrix} 1 & -i \\ 1 & i \end{smallmatrix}\right)$. Dann ist T invertierbar mit $T^{-1} = \frac{1}{2i}\left(\begin{smallmatrix} i & i \\ -1 & 1 \end{smallmatrix}\right)$, und man hat einen Isomorphismus $\mathrm{SO}_2(\mathbb{C}) \xrightarrow{\sim} \mathbb{G}_{\mathrm{m}}(\mathbb{C}) \simeq \mathbb{C}^*$ mit
$$\begin{pmatrix} z_1 & -z_2 \\ z_2 & z_1 \end{pmatrix} \mapsto T \begin{pmatrix} z_1 & -z_2 \\ z_2 & z_1 \end{pmatrix} T^{-1}$$
$$= \begin{pmatrix} z_1 - iz_2 & 0 \\ 0 & z_1 + iz_2 \end{pmatrix} = \begin{pmatrix} z_1 - iz_2 & 0 \\ 0 & (z_1 - iz_2)^{-1} \end{pmatrix}.$$
Allgemein nennt man eine affine algebraische Gruppe G über K einen *n-dimensionalen Torus*, wenn es eine Körpererweiterung L von K gibt mit
$$G \times L \simeq \underbrace{L^* \times \cdots \times L^*}_{n \text{ Faktoren}}.$$

0.3 Bemerkung zur Klassifikation

Chevalley hat in den Jahren 1955–58 die „halbeinfachen“ algebraischen Gruppen über einem algebraisch abgeschlossenen Körper mittels „Dynkin-Diagrammen“ klassifiziert. Er hat auch gesehen, dass diese Gruppen über $\mathbb{Z}$ und damit über jedem Körper definiert sind.
In dieser Vorlesung werden wir einige Grundlagen der Theorie der linearen algebraischen Gruppen kennenlernen und damit Klassifikationssätze formulieren.

0.4 Übungsaufgaben 1–2

Aufgabe 1
Sei K ein Körper. Man zeige für jede Matrix $x = (x_{ij}) \in \mathrm{M}_{n\times n}(K)$ die LEIBNIZ-Formel

$$\det(x) = \sum_{\sigma\in S_n} \operatorname{sign}(\sigma)\; x_{1\sigma(1)} \cdot \ldots \cdot x_{n\sigma(n)}\,.$$

Dabei ist $S_n = \{\sigma\colon \{1,\ldots,n\} \to \{1,\ldots,n\} \mid \sigma \text{ bijektiv}\}$ die *symmetrische Gruppe* der Ordnung $n!$ mit der Hintereinanderausführung von Abbildungen als Verknüpfung.

Aufgabe 2
Sei $\varphi\colon R \to S$ ein Homomorphismus kommutativer Ringe. Für ein Ideal I in R sei I^e das von $\varphi(I)$ in S erzeugte Ideal, also

$$I^e = \varphi(I)\,S = \{\sum_i^{\text{endl.}} \varphi(r_i)\,s_i \mid r_i \in I\,,\; s_i \in S\,\}\,.$$

Für ein Ideal J in S sei J^c das durch $J^c = \varphi^{-1}(J)$ definierte Ideal in R. Man zeige:

(a) $I \subset I^{ec}$ und $J \supset J^{ce}$.

(b) $I^e = I^{ece}$ und $J^c = J^{cec}$.

(c) Das *Radikal* $\mathrm{Rad}(I) := \{r \in R \mid \exists\, m \in \mathbb{N} \text{ mit } r^m \in I\}$ ist ein Ideal in R.

(d) Ist $\mathfrak{p}$ ein Primideal in R, so ist $\mathrm{Rad}(\mathfrak{p}^n) = \mathfrak{p}$ für alle $n \in \mathbb{N}$.

(Der Buchstabe e bei I^e steht für „extended“, und der Buchstabe c bei J^c steht für „contracted“. Wenn S eine Ringerweiterung von R ist, dann ist $J^c = J \cap R$.)

1 Hilbertscher Nullstellensatz

Sei R ein kommutativer Ring (Beispiel $R = \mathbb{Z}$).

1.1 Kommutative Algebren

Definition
Eine *kommutative R-Algebra* ist ein kommutativer Ring A zusammen mit einem Ringhomomorphismus $\iota_A \colon R \to A$. Es ist dann A ein R-Modul mit der Skalarmultiplikation $ra := \iota_A(r)\, a$ für alle $r \in R$, $a \in A$.

Beispiele 1. Ist R ein Unterring eines kommutativen Ringes S, so ist S eine R-Algebra, wobei ι_S die Inklusion ist. Man nennt S eine *Ringerweiterung von R*.

2. Der Polynomring $R[X_1, \ldots, X_n]$ ist eine R-Algebra, sogar Ringerweiterung von R (vgl. Algebra 20.3).

Definition
Ein *Homomorphismus* $\varphi \colon A \to B$ von kommutativen R-Algebren ist ein Ringhomomorphismus, für den zusätzlich gilt:

$$\varphi(ra) = r\varphi(a) \quad \forall\, r \in R,\ a \in A\,.$$

Man nennt φ dann auch einen *R-Algebrahomomorphismus*.

1.2 Endlich erzeugte Algebren

(1) Eine kommutative R-Algebra A heißt *endlich erzeugt* (als R-Algebra), wenn es ein $n \in \mathbb{N}$ und einen surjektiven R-Algebrahomomorphismus

$$\varphi \colon R[X_1, \ldots, X_n] \twoheadrightarrow A$$

gibt. Die Elemente $x_1 := \varphi(X_1), \ldots, x_n := \varphi(X_n)$ heißen dann *Erzeugende von A* (als R-Algebra). Man schreibt dann $A = R[x_1, \ldots, x_n]$.

(2) Sind $y_1, \ldots, y_n$ beliebige Elemente einer kommutativen R-Algebra A, so gibt es stets einen R-Algebrahomomorphismus

$$\varphi \colon R[X_1, \ldots, X_n] \to A$$

mit $\varphi(X_i) = y_i$ für $i = 1, \ldots, n$, den sogenannten *Einsetzhomomorphismus* (dieser ist eindeutig bestimmt, wie aus Algebra 20.6 folgt). Es ist dann

$$\operatorname{bild}(\varphi) =: R[y_1, \ldots, y_n]$$

die *von $y_1, \ldots, y_n$ erzeugte Unteralgebra von A*.

Bemerkung
Es gilt

$$\boxed{A \text{ endlich erzeugt als } R\text{-Modul}} \Longrightarrow \boxed{A \text{ endlich erzeugt als } R\text{-Algebra}}.$$

Die Umkehrung gilt i. Allg. nicht, wie schon der Polynomring $K[X]$ über einem Körper K zeigt. Es ist $\{X^i \mid i \in \mathbb{N}_0\}$ eine Basis von $K[X]$ als K-Vektorraum, aber das eine Element X erzeugt $K[X]$ als K-Algebra.

Ist L eine Körpererweiterung eines Körpers K, so unterscheiden wir sogar zwischen drei Endlichkeitsbegriffen!

(a) L ist endlich-dimensional als K-Vektorraum ($\underset{\text{AGLA}}{\Longleftrightarrow}$ L ist endlich erzeugt als K-Vektorraum),

(b) L ist endlich erzeugt als Ringerweiterung von K,

(c) L ist endlich erzeugt als Körpererweiterung von K.

Es gilt $(a) \Longrightarrow (b) \Longrightarrow (c)$, die umgekehrten Richtungen gelten i. Allg. jedoch nicht.

Beispiel
Sei K ein Körper. Der Quotientenkörper $L := K(X_1, \ldots, X_n)$ des Polynomrings $A := K[X_1, \ldots, X_n]$ in n Unbestimmten ist endlich erzeugt als Körpererweiterung von K, aber nicht endlich erzeugt als Ringerweiterung von K (vgl. auch Lemma 1.10 unten).

Beweis. Angenommen, L besitzt endlich viele Ringerzeugende

$$h_1 = \frac{f_1}{g_1}, \ldots, h_m = \frac{f_m}{g_m} \text{ mit } f_i, g_i \in A\,,\ g_i \neq 0 \text{ für } i = 1, \ldots, m\,.$$

Dann gibt es zu jedem $h \in L$ Polynome $f, g \in A$ mit $g \neq 0$ so, dass $h = \frac{f}{g}$ gilt und in der Primfaktorzerlegung von g nur Primelemente auftreten, die eines der g_i teilen (denn A ist faktoriell, vgl. Algebra 8.9 und 9.4).
Da A unendlich viele Primelemente besitzt, gibt es ein Primelement $p \in A$ mit $p \nmid g_i$ für alle $i = 1, \ldots, m$. Dann ist aber $h = \frac{1}{p}$ nicht so darstellbar wie oben beschrieben. Widerspruch. □

1.3 Ganze Ringerweiterungen

Die Übertragung des Begriffs „algebraische Körpererweiterung“ in die kommutative Ringtheorie führt zum Begriff „ganze Ringerweiterung“.

Definition
Sei S eine kommutative Ringerweiterung von R. Ein Element $s \in S$ heißt *ganz über* R, wenn s Nullstelle eines normierten Polynoms $f \in R[X]$ ist, d. h. wenn es ein Polynom

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

mit $a_0, \ldots, a_{n-1} \in R$ und $f(s) = 0$ gibt. Der Ring S heißt *ganz über* R, wenn jedes Element $s \in S$ ganz über R ist.

Beispiel
$\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ ist ganz über $\mathbb{Z}$, denn

$$f = X^2 - 2aX + a^2 + b^2$$

erfüllt $f(a + bi) = 0$ für alle $a, b \in \mathbb{Z}$.

Frage
Ist $\mathbb{Q}$ eine ganze Ringerweiterung von $\mathbb{Z}$?

Darüber gibt der folgende Satz Aufschluss:

Satz
Sei S eine ganze Ringerweiterung von R. Wenn S ein Körper ist, dann ist R ein Körper.

Beweis. Sei $r \in R \setminus \{0\}$. Da S ein Körper ist, existiert das Inverse r^{-1} in S. Zu zeigen: $r^{-1} \in R$. Da S ganz über R ist, erfüllt r^{-1} eine Gleichung

$$r^{-n} + a_{n-1}r^{-n+1} + \cdots + a_0 = 0 \quad | \cdot r^{n-1}$$

mit $a_0, \ldots, a_{n-1} \in R$. Es folgt

$$r^{-1} + a_{n-1} + a_{n-2}r + \cdots + a_o r^{n-1} = 0$$

und also $r^{-1} = -a_0 r^{n-1} - \cdots - a_{n-1} \in R$. □

1.4 Endliche Ringerweiterungen sind ganz

Satz
Sei S eine kommutative Ringerweiterung von R. Wenn S als R-Modul endlich erzeugt ist, so ist S ganz über R.

Beweis. Sei $s \in S$, und sei $\{s_1, \ldots, s_n\}$ ein Erzeugendensystem von S als R-Modul. Dann ist $ss_i = a_{i1}s_1 + \cdots + a_{in}s_n$ für gewisse $a_{i1}, \ldots, a_{in} \in R$ und $i = 1, \ldots, n$, und für die Matrix $A = (a_{ij})_{1 \leqslant i,j \leqslant n}$ gilt

$A \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} ss_1 \\ \vdots \\ ss_n \end{pmatrix}$ bezüglich Matrizenmultiplikation. Sei $\vec{s} := \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}$ und $B := A - sE_n$ mit der Einheitsmatrix $E_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$. Dann folgt $\boxed{B\vec{s} = \vec{0}}$.
Zeige nun, dass $\det B = 0$ gilt, d. h. dass s Nullstelle des charakteristischen Polynoms $\det(A - XE_n)$ und somit ganz ist.
Sei $\widetilde{B} = (\widetilde{b}_{ik}) \in \mathrm{M}_{n\times n}(R)$ mit $\widetilde{b}_{ik} := (-1)^{k+i} \det(B_{ki})$, wobei B_{ki} aus B durch Streichen der k-ten Zeile und i-ten Spalte entsteht. Sei $B = (b_{kj})$. Dann ist nach Definition der Matrizenmultiplikation $\widetilde{B}B = (c_{ij})$ mit

$$\begin{aligned} c_{ij} &= \sum_{k=1}^{n} \widetilde{b}_{ik} b_{kj} = \sum_{k=1}^{n} (-1)^{k+i} \det(B_{ki})\, b_{kj} \quad \text{(nach Definition von } \widetilde{B}) \\ &= \det B' \quad \text{(Entwicklung nach der } j\text{-ten Spalte, gilt auch über } R) \end{aligned}$$

wobei B' aus B entsteht, indem die i-te Spalte durch die j-te Spalte ersetzt wird, also

$$c_{ij} = \begin{cases} \det B & \text{für } i = j \\ 0 & \text{für } i \neq j, \text{ da dann in } B' \text{ zwei Spalten gleich sind.} \end{cases}$$

Es folgt $\widetilde{B}B = \det(B)E_n$. Da $B\vec{s} = \vec{0}$ gilt, erhalten wir $\vec{0} = \widetilde{B}B\vec{s} = \det(B)E_n\vec{s}$ und also $\det(B)s_i = 0$ für alle $i = 1, \ldots, n$. Da $\{s_1, \ldots, s_n\}$ ein Erzeugendensystem von S als R-Modul ist, gibt es $\lambda_1, \ldots, \lambda_n \in R$ mit

$$1 = \lambda_1 s_1 + \cdots + \lambda_n s_n\,,$$

und es folgt $\det(B) \cdot 1 = 0$. □

1.5 Charakterisierung endlicher Ringerweiterungen

Sind $K \subset L$ Körper und ist $x \in L$, dann gelten nach Algebra 11.12:

$$\boxed{x \text{ algebraisch über } K} \iff \boxed{\dim_K K(x) < \infty}$$

und nach Algebra 12.1:

$$\boxed{\dim_K L < \infty} \iff \boxed{L = K(x_1, \ldots, x_n) \text{ mit algebraischen } x_1, \ldots, x_n}.$$

Wir beweisen nun die ringtheoretische Version dieser beiden Äquivalenzen.

Definition
Sei S eine kommutative Ringerweiterung von R. Dann heißt S *endlich über* R, wenn S als R-Modul endlich erzeugt ist.

Satz
(a) *Für $s \in S$ gilt:* $\boxed{s \text{ ganz über } R} \iff \boxed{R[s] \text{ endlich über } R}$.

(b) *Es sind äquivalent:*

(i) *S ist endlich über R.*

(ii) *S wird als R-Algebra von endlich vielen ganzen Elementen erzeugt.*

Beweis. (a) „$\Longrightarrow$“ Da s ganz über R ist, gibt es ein normiertes Polynom $f \in R[X]$ mit $f(s) = 0$. Nach Algebra 8.1 ist jedes Polynom $g \in R[X]$ darstellbar als $g = hf + r$ mit $\operatorname{grad}(r) < \operatorname{grad}(f)$ (oder $r = 0$). Es folgt $g(s) = h(s)f(s) + r(s) = r(s)$, da $f(s) = 0$ ist. Also bilden $1, s, \ldots, s^{n-1}$ ein Erzeugendensystem von $R[s]$ als R-Modul, wobei $n = \operatorname{grad}(f)$ gilt.

„$\Longleftarrow$“ Wende Satz 1.4 mit $S = R[s]$ an.

(b) „(i)$\Longrightarrow$(ii)“ Wenn S endlich über R ist, so besitzt S als R-Modul ein endliches Erzeugendensystem, dessen Elemente nach Satz 1.4 ganz über R sind. Da jedes Modulerzeugendensystem auch ein Algebraerzeugendensystem ist, folgt (ii).

„(ii)$\Longrightarrow$(i)“ Sei S als R-Algebra von n ganzen Elementen $s_1, \ldots, s_n$ erzeugt. Führe Induktion nach n durch:
Für $n = 1$ folgt die Behauptung aus (a).
Nach Induktionsvoraussetzung ist $R' := R[s_1, \ldots, s_{n-1}]$ endlich über R, und nach (a) ist $S = R'[s_n]$ endlich über R', also auch über R.

□

1.6 Die Eigenschaft „ganz“ ist transitiv

Satz
Seien $R \subset S \subset T$ kommutative Ringerweiterungen. Wenn S über R und T über S ganz sind, so ist T über R ganz.

Beweis. Sei $t \in T$ ganz über S. Dann gibt es $s_0, \ldots, s_{n-1} \in S$ so, dass $t^n + s_{n-1}t^{n-1} + \cdots + s_0 = 0$ gilt. Nach Voraussetzung sind $s_0, \ldots, s_{n-1}$ ganz über R, also ist $R' := R[s_0, \ldots, s_{n-1}]$ endlich über R nach 1.5 (b). Da t ganz über R' ist, folgt mit 1.5 (a), dass $R'[t]$ endlich über R' ist. Es folgt, dass $R'[t]$ endlich über R ist, und daher ist t ganz über R nach 1.4. □

1.7 Homogene Bestandteile eines Polynoms

Sei R ein kommutativer Ring, und sei $f \in R[X_1, \ldots, X_n]$ ein Polynom in n Unbestimmten $X_1, \ldots, X_n$, also

$$f = \sum_{(m_1,\ldots,m_n)\in\mathbb{N}_0^n} a_{m_1\ldots m_n} X_1^{m_1} \cdot \ldots \cdot X_n^{m_n}$$

mit Koeffizienten $a_{m_1\ldots m_n} \in R$, die bis auf endlich viele gleich 0 sind.

Definition
Ist $f \neq 0$, so heißt f *homogen vom Grad* j, falls $m_1 + \cdots + m_n = j$ für alle $(m_1, \ldots, m_n) \in \mathbb{N}_0^n$ mit $a_{m_1\ldots m_n} \neq 0$ gilt.

Beispiel
$X_1^2 - X_1X_2 + 5X_2^2$ ist homogen vom Grad 2 in $\mathbb{Z}[X_1, X_2]$.

Bemerkung
Das Nullpolynom ist homogen von jedem Grad $j \in \mathbb{N}_0$. Ist $f \neq 0$ und nicht homogen, so fasst man die Summanden mit $m_1 + \cdots + m_n = j$ zu einem Polynom f_j zusammen und nennt f_j den *homogenen Bestandteil von* f *vom Grad* j. Es gibt dann ein $d \in \mathbb{N}_0$ mit $f_d \neq 0$ so, dass $f = f_0 + f_1 + \cdots + f_d$ gilt. Es ist also $f_j = 0$ oder $f_j = \sum_{m_1+\cdots+m_n=j} a_{m_1\ldots m_n} X_1^{m_1} \cdot \ldots \cdot X_n^{m_n}$.

Ist $f \neq 0$, so heißt $\max\{j \in \mathbb{N}_0 \mid f_j \neq 0\}$ der *Totalgrad von* f.

1.8 Algebraische Unabhängigkeit

Definition
Sei S eine kommutative Ringerweiterung eines kommutativen Ringes R. Dann heißen $x_1, \ldots, x_n \in S$ *algebraisch unabhängig* oder *transzendent* über R, wenn der Einsetzhomomorphismus

$$R[X_1, \ldots, X_n] \to S,\ f \mapsto f(x_1, \ldots, x_n),$$

injektiv ist. In diesem Fall kann man den Unterring $R[x_1, \ldots, x_n]$ von S als Polynomring auffassen. Sind $x_1, \ldots, x_n \in S$ nicht algebraisch unabhängig, so heißen sie *algebraisch abhängig* über R.

1.9 Noethersches Normalisierungslemma

Lemma (Emmy Noether)
Sei K ein Körper, und sei A eine kommutative, endlich erzeugte K-Algebra. Dann ist A entweder ganz über K oder es gibt algebraisch unabhängige Elemente $Y_1, \ldots, Y_m \in A$ über K so, dass A ganz über $K[Y_1, \ldots, Y_m]$ ist.

Beweis. Der Beweis wird für den Fall geführt, dass K unendlich viele Elemente hat (der Fall $|K| < \infty$ ist komplizierter zu beweisen und wird hier nicht benötigt).
Da A endlich erzeugt ist, gibt es $x_1, \ldots, x_n \in A$ so, dass $A = K[x_1, \ldots, x_n]$ gilt. Sind $x_1, \ldots, x_n$ algebraisch unabhängig, so folgt die Behauptung, da A ganz über A ist.
Sei nun $A = K[x_1, \ldots, x_n]$, wobei $x_1, \ldots, x_n$ algebraisch abhängig (und $\neq 0$) sind. Dann gibt es ein Polynom $f \in K[X_1, \ldots, X_n]$ mit

$$(*) \qquad f(x_1, \ldots, x_n) = 0 \quad \text{und} \quad f \neq 0\,.$$

Induktion nach n:
$n = 1$: Da f normiert werden kann, ist x_1 ganz über dem Körper K nach Definition 1.3, und daher ist auch $A = K[x_1]$ ganz über K nach 1.5, 1.4.
$n \geqslant 2$: Zerlege f in seine homogenen Bestandteile $f = f_0 + \cdots + f_d$ mit $f_d \neq 0$ wie in 1.7. Dann ist $f_d(X_1, \ldots, X_{n-1}, 1) \in K[X_1, \ldots, X_{n-1}]$. Da K unendlich ist, gibt es also nach Aufgabe 4 Elemente $\lambda_1, \ldots, \lambda_{n-1} \in K$ mit $f_d(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$. Setze $\boxed{y_i := x_i - \lambda_i x_n}$ für $i = 1, \ldots, n-1$. Dann folgt durch Ausmultiplizieren:

$$\begin{aligned} 0 &\underset{(*)}{=} f(y_1 + \lambda_1 x_n, \ldots, y_{n-1} + \lambda_{n-1} x_n, x_n) \\ &= \underbrace{f_d(\lambda_1, \ldots, \lambda_{n-1}, 1)}_{\neq 0 \text{ in } K} x_n^d + g_1 x_n^{d-1} + \cdots + g_d \end{aligned}$$

mit $g_i \in K[y_1, \ldots, y_{n-1}]$ für $i = 1, \ldots, d$. Also ist x_n und damit A ganz über $K[y_1, \ldots, y_{n-1}]$ nach 1.5 und 1.4. Nach Induktionsvoraussetzung ist $K[y_1, \ldots, y_{n-1}]$ ganz über K, oder es gibt über K algebraisch unabhängige Elemente $Y_1, \ldots, Y_m$ so, dass $K[y_1, \ldots, y_{n-1}]$ ganz über $K[Y_1, \ldots, Y_m]$ ist. Aus der Transitivität der Ganzheit 1.6 folgt nun die Behauptung. □

1.10 Schwacher Nullstellensatz

Lemma
Sei K ein Körper, und sei L eine Körpererweiterung von K, die als Ringerweiterung von K endlich erzeugt sei. Dann ist L algebraisch (sogar endlich) über K.

Beweis. Wäre L nicht ganz über K, so wäre L nach 1.9 ganz über einem Polynomring $R := K[Y_1, \ldots, Y_m]$, und R wäre nach Satz 1.3 ein Körper. Das ist ein Widerspruch, da $Y_1, \ldots, Y_m$ in R nicht invertierbar sind (nach Algebra 6.13). □

Satz (Schwacher Nullstellensatz)
Im Polynomring $K[X_1, \ldots, X_n]$ sind die Ideale der Form

$$(X_1 - a_1, \ldots, X_n - a_n) \quad \textit{mit} \quad a_1, \ldots, a_n \in K$$

maximale Ideale. Ist K ein algebraisch abgeschlossener Körper, so gibt es keine weiteren maximalen Ideale in $K[X_1, \ldots, X_n]$.

Beweis. Sei $\varphi\colon K[X_1, \ldots, X_n] \to K,\ f \mapsto f(a_1, \ldots, a_n)$, der Einsetzhomomorphismus. Dann ist φ surjektiv, da $\varphi(a) = a$ für jedes $a \in K$ gilt. Wir berechnen den Kern von φ. Jedes $f \in K[X_1, \ldots, X_n]$ hat die Gestalt $f = \sum a_{m_1 \ldots m_n} X_1^{m_1} \cdot \ldots \cdot X_n^{m_n}$. Hierin setzen wir $X_i = Y_i + a_i$ für $i = 1, \ldots, n$ ein und erhalten f in der Form

$$f = f(a_1, \ldots, a_n) + \sum_{i=1}^{n} g_i \cdot Y_i = f(a_1, \ldots, a_n) + \sum_{i=1}^{n} g_i \cdot (X_i - a_i)$$

mit $g_i \in K[X_1, \ldots, X_n]$. Es ist also f genau dann in $\ker \varphi$, wenn f in dem von $X_1 - a_1, \ldots, X_n - a_n$ erzeugten Ideal liegt. Nach dem Homomorphiesatz für Ringe folgt, dass $K[X_1, \ldots, X_n]/(X_1 - a_1, \ldots, X_n - a_n) \simeq K$ gilt (vgl. Algebra 7.7). Das Ideal $(X_1 - a_1, \ldots, X_n - a_n)$ ist also maximal nach Algebra 7.4.
Sei nun K algebraisch abgeschlossen, und sei $\mathfrak{m}$ ein beliebiges maximales Ideal in $K[X_1, \ldots, X_n]$. Dann ist $L := K[X_1, \ldots, X_n]/\mathfrak{m}$ ein Körper (nach Algebra 7.4), und L ist endlich erzeugt als Ringerweiterung von K nach Definition 1.2. Da K algebraisch abgeschlossen ist, folgt nach dem Lemma $L = K$ und also $K \hookrightarrow K[X_1, \ldots, X_n]/\mathfrak{m} = K$. Es gibt daher $a_1, \ldots, a_n \in K$ mit $a_i + \mathfrak{m} = X_i + \mathfrak{m}$, d. h. mit $X_i - a_i \in \mathfrak{m}$ für $i = 1, \ldots, n$ (vgl. Algebra 7.2). Da $I := (X_1 - a_1, \ldots, X_n - a_n)$ maximales Ideal ist, folgt $I = \mathfrak{m}$. □

Korollar
Ist K algebraisch abgeschlossen, so gibt es eine Bijektion zwischen den Punkten von K^n und den maximalen Idealen in $K[X_1, \ldots, X_n]$, nämlich

$$\begin{aligned} K^n &\longrightarrow \{\textit{maximale Ideale in } K[X_1, \ldots, X_n]\}, \\ (a_1, \ldots, a_n) &\longmapsto (X_1 - a_1, \ldots, X_n - a_n). \end{aligned}$$

Geometrie Algebra

Hier liegt der Ursprung der algebraischen Geometrie.

1.11 Lösbarkeit von Systemen polynomialer Gleichungen

Definition
Sei K ein Körper, und sei $\overline{K}$ ein algebraischer Abschluss von K (gemäß Algebra 20.2). Für eine nichtleere Teilmenge $I \subset K[X_1, \ldots, X_n]$ setzen wir

$$\boxed{\mathfrak{V}(I) := \{x \in \overline{K}^n \mid f(x) = 0 \quad \forall\, f \in I\}}$$

und nennen $\mathfrak{V}(I)$ eine *algebraische Menge in* $\overline{K}^n$ oder die *Nullstellenmenge von* I *in* $\overline{K}$.

Satz
Ist $I \neq (1)$ *ein Ideal in* $K[X_1, \ldots, X_n]$ *, so ist* $\mathfrak{V}(I) \neq \emptyset$ *.*

Beweis. Es ist I in einem maximalen Ideal $\mathfrak{m}$ von $K[X_1, \ldots, X_n]$ enthalten (vgl. Algebra 7.6), und $L := K[X_1, \ldots, X_n]/\mathfrak{m}$ ist dann ein Körper, der als Ringerweiterung von K endlich erzeugt ist. Nach Lemma 1.10 ist L also algebraisch über K und kann daher in $\overline{K}$ eingebettet werden (vgl. Algebra 20.5). Setze $x_i = X_i + \mathfrak{m}$ in L und $x = (x_1, \ldots, x_n)$. Dann ist $x \in \mathfrak{V}(\mathfrak{m}) \subset \mathfrak{V}(I)$. □

Korollar
Das System $f_1 = 0, \ldots, f_m = 0$ *mit* $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ *hat genau dann keine Lösung in* $\overline{K}^n$*, wenn es Polynome* $p_1, \ldots, p_m \in K[X_1, \ldots, X_n]$ *gibt so, dass* $1 = p_1 f_1 + \cdots + p_m f_m$ *gilt.*

Beweis. Sei $R = K[X_1, \ldots, X_n]$, und sei I das von $f_1, \ldots, f_m$ erzeugte Ideal in R , also $I = \{q_1 f_1 + \cdots + q_m f_m \mid q_1, \ldots, q_m \in R\}$. Dann gilt $\mathfrak{V}(I) = \{x \in \overline{K}^n \mid f_1(x) = 0, \ldots, f_m(x) = 0\}$, wie leicht zu sehen ist. Gilt $\mathfrak{V}(I) = \emptyset$, so ist $1 \in I$ nach dem Satz. Ist umgekehrt $1 \in I$, so ist $I = K[X_1, \ldots, X_n]$ und ersichtlich $\mathfrak{V}(I) = \emptyset$. □

1.12 Radikalideale

Sei I ein Ideal in einem kommutativen Ring R , und sei

$$\mathrm{Rad}(I) := \sqrt{I} := \{r \in R \mid r^m \in I \text{ für ein } m \in \mathbb{N}\}\,.$$

das *Radikal von* I. Ersichtlich gilt $I \subset \mathrm{Rad}(I)$, und $\mathrm{Rad}(I)$ ist ein Ideal in R nach Aufgabe 2 c.

Definition
- Ein Ideal I heißt *Radikalideal*, falls $I = \mathrm{Rad}(I)$ gilt.
- Ein Element $r \in R$ heißt *nilpotent*, falls $r^m = 0$.

Beispiel
Jedes Primideal ist ein Radikalideal (vgl. Aufgabe 2 d).

Bemerkung
Es ist I genau dann ein Radikalideal in R, wenn R/I reduziert ist (d. h. kein nilpotentes Element außer 0 enthält).

Beweis. Sei I ein Radikalideal in R, und sei $r \in R$. Ist $r + I$ nilpotent in R/I, so gilt $r^m \in I$ für ein $m \in \mathbb{N}$ und also $r \in \mathrm{Rad}(I) \underset{\text{Vor.}}{=} I$. Hieraus folgt $r + I = I = 0_{R/I}$. Ist umgekehrt $r \in \mathrm{Rad}(I)$ und R/I reduziert, dann folgt $r^m \in I$ für ein $m \in \mathbb{N}$ und also $r \in I$. □

1.13 Verschwindungsideal

Definition
Seien K ein Körper und $\overline{K}$ ein algebraischer Abschluss von K. Zu jeder Teilmenge $V \subset \overline{K}^n$ gehört das Ideal

$$\mathfrak{I}(V) := \{f \in K[X_1, \ldots, X_n] \mid f(x) = 0 \ \ \forall\, x \in V\},$$

genannt das *Verschwindungsideal* oder *Ideal von* V.

Lemma
$\mathfrak{I}(V)$ ist ein Radikalideal.

Beweis. Sei $f \in \mathrm{Rad}(\mathfrak{I}(V))$. Dann existiert ein $m \in \mathbb{N}$ mit $f^m \in \mathfrak{I}(V)$, also mit $f^m(x) = 0$ für alle $x \in V$. Da der Einsetzhomomorphismus $\varphi_x \colon K[X_1, \ldots, X_n] \to \overline{K},\ g \mapsto g(x)$, multiplikativ ist, folgt

$$0 = f^m(x) = \varphi_x(f^m) = \varphi_x(f)^m = f(x)^m \ \ \forall\, x \in V.$$

Da $\overline{K}$ ein Körper ist, folgt $f(x) = 0\ \forall\, x \in V$ und daher $f \in \mathfrak{I}(V)$. □

1.14 $\mathfrak{I}(\mathfrak{V}(I)) = \mathrm{Rad}(I)$

Seien K ein Körper, $\overline{K}$ ein algebraischer Abschluss von K und I ein Ideal in $K[X_1, \ldots, X_n]$ sowie $V \subset \overline{K}^n$. Wie gehabt seien

$$\mathfrak{V}(I) := \{x \in \overline{K}^n \mid f(x) = 0 \ \ \forall\, f \in I\}$$
$$\mathfrak{I}(V) := \{f \in K[X_1, \ldots, X_n] \mid f(x) = 0 \ \ \forall\, x \in V\}.$$

Nullstellensatz (David Hilbert)
$\mathfrak{I}(\mathfrak{V}(I)) = \mathrm{Rad}(I)$.

Beweis. Wir zeigen zunächst $\mathrm{Rad}(I) \subset \mathfrak{I}(\mathfrak{V}(I))$. Sei $g \in \mathrm{Rad}(I)$. Dann ist $g^m \in I$ für ein $m \in \mathbb{N}$ und also $0 = g^m(x) = g(x)^m$ für alle $x \in \mathfrak{V}(I)$. Da $g(x)$ im Körper $\overline{K}$ liegt, folgt $g \in \mathfrak{I}(\mathfrak{V}(I))$.
Wir zeigen nun umgekehrt: $\mathfrak{I}(\mathfrak{V}(I)) \subset \mathrm{Rad}(I)$.
Sei $R = K[X_1, \ldots, X_n]$. Nach dem Hilbertschen Basissatz (Algebra 6.14) ist I endlich erzeugt, d. h. es gibt ein $\ell \in \mathbb{N}$ und Polynome $f_1, \ldots, f_\ell \in R$ mit $I = (f_1, \ldots, f_\ell) := \{\sum_{i=1}^{\ell} p_i f_i \mid p_i \in R\}$. Sei $g \in \mathfrak{I}(\mathfrak{V}(I))$ und $g \neq 0$. Dann folgt

$$(*) \qquad \boxed{g(x) = 0 \ \ \forall\, x \in \overline{K}^{\,n} \ \text{ mit } f_1(x) = 0, \ldots, f_\ell(x) = 0}$$

nach Definition von $\mathfrak{I}(\mathfrak{V}(I))$. Zu zeigen: $\exists\, m \in \mathbb{N}$ mit $g^m \in I$. Betrachte in $R[X]$ die $\ell+1$ Polynome $f_1, \ldots, f_\ell, 1-gX$. Diese können keine gemeinsame Nullstelle in $\overline{K}^{\,n+1}$ haben, da jede gemeinsame Nullstelle von $f_1, \ldots, f_\ell$ nach $(*)$ auch Nullstelle von g ist und daher keine von $1 - gX$ sein kann. Nach Korollar 1.11 gilt also $1 = p_1 f_1 + \cdots + p_\ell f_\ell + p_{\ell+1}(1 - gX)$ mit $p_1, \ldots, p_{\ell+1} \in R[X]$. Setze $\frac{1}{g}$ für die Unbestimmte X ein. Dann folgt

$$1 = \widetilde{p_1} f_1 + \cdots + \widetilde{p_\ell} f_\ell$$

mit $\widetilde{p_1}, \ldots, \widetilde{p_\ell} \in R[\frac{1}{g}]$. Multipliziere diese Gleichung mit g^m, wobei m so groß gewählt wird, dass alle Nenner in den Potenzen von g verschwinden. Es folgt $g^m = p_1^* f_1 + \cdots + p_\ell^* f_\ell$ mit $p_i^* \in R$ und also $g^m \in I$. („Trick des Rabinowitsch“) □

1.15 Folgerung

Seien K ein Körper und $\overline{K}$ ein algebraischer Abschluss von K. Eine Teilmenge $V \subset \overline{K}^{\,n}$ heißt *algebraisch*, falls es ein Ideal I in $K[X_1, \ldots, X_n]$ mit $V = \mathfrak{V}(I) := \{x \in \overline{K}^{\,n} \mid f(x) = 0 \ \ \forall\, f \in I\}$ gibt.

Theorem
Es gibt eine inklusionsumkehrende Bijektion

$$\begin{array}{ccc} \{V \subset \overline{K}^{\,n} \mid V \textit{ algebraisch}\} & \xrightarrow{\sim} & \{I \subset K[X_1, \ldots, X_n] \mid I \textit{ Radikalideal}\} \\ V & \longmapsto & \mathfrak{I}(V) \\ \text{Objekte der Geometrie} & & \text{Objekte der Algebra} \end{array}$$

Beweis. Sei I ein Ideal in $K[X_1, \ldots, X_n]$. Dann gilt $\mathfrak{V}(\mathfrak{I}(\mathfrak{V}(I))) = \mathfrak{V}(I)$ (vgl. Aufgabe 7). Hieraus folgt die Injektivität. Die Surjektivität ergibt sich direkt aus Hilberts Nullstellensatz 1.14. Dass $\mathfrak{I}(V)$ ein Radikalideal ist, wurde in 1.13 gezeigt. □

Eine kommutative K-Algebra heißt *affin*, wenn sie endlich erzeugt (als K-Algebra) ist und keine nilpotenten Elemente außer 0 besitzt.

Korollar
Sei A eine affine K-Algebra. Dann gibt es ein $n \in \mathbb{N}$ und eine algebraische Menge $V \subset \overline{K}^n$ so, dass $A \simeq K[X_1, \ldots, X_n]/\mathfrak{I}(V)$ gilt.

Beweis. Da A endlich erzeugt ist, gibt es ein $n \in \mathbb{N}$ und einen surjektiven K-Algebrahomomorphismus $\varphi\colon K[X_1, \ldots, X_n] \twoheadrightarrow A$ nach Definition 1.2. Der Homomorphiesatz ergibt $A \simeq K[X_1, \ldots, X_n]/\operatorname{kern}\varphi$. Da A reduziert ist, ist $\operatorname{kern}\varphi$ ein Radikalideal nach Bemerkung 1.12. Nach dem Theorem gibt es eine algebraische Menge $V \subset \overline{K}^n$ mit $\mathfrak{I}(V) = \operatorname{kern}\varphi$. □

1.16 Übungsaufgaben 3–7

Aufgabe 3
Sei S ein Integritätsring. Man zeige:
Wenn S eine ganze Ringerweiterung eines Körpers ist, so ist S ein Körper.

Aufgabe 4
Sei K ein Körper mit unendlich vielen Elementen und $f \in K[X_1, \ldots, X_m]$ ein Polynom mit $f \neq 0$.
Man zeige, dass es unendlich viele Punkte $(a_1, \ldots, a_m)$ in K^m gibt mit $f(a_1, \ldots, a_m) \neq 0$.

Hinweis zu Aufgabe 4:
Man überlege sich, dass f in der Form $f = g_0 + g_1 X_m + \cdots + g_r X_m^r$ mit $g_i \in K[X_1, \ldots, X_{m-1}]$ und $g_r \neq 0$ geschrieben werden kann, falls $m \geqslant 2$ ist und X_m in f wirklich vorkommt, und führe Induktion nach m durch.

Aufgabe 5
Sei S eine kommutative Ringerweiterung eines kommutativen Ringes R. Man zeige, dass die Menge $\overline{R} := \{s \in S \mid s \text{ ist ganz über } R\}$ ein Unterring von S ist.

Aufgabe 6
Sei R ein Integritätsring und sei R^* die Gruppe der Einheiten in R. Man zeige, dass $(R[X_1, \ldots, X_n])^* = R^*$ gilt.

Aufgabe 7
Sei $\overline{K}$ ein algebraischer Abschluss von K. Man zeige:

(a) $\mathfrak{I}(\emptyset) = K[X_1, \ldots, X_n]$ und $\mathfrak{I}(\overline{K}^n) = (0)$.

(b) Ist $V \subset \overline{K}^n$ algebraisch, so gilt $\mathfrak{V}(\mathfrak{I}(V)) = V$.

(c) Sind $V_1, V_2 \subset \overline{K}^n$ algebraisch, so gilt $\mathfrak{I}(V_1 \cup V_2) = \mathfrak{I}(V_1) \cap \mathfrak{I}(V_2)$.

2 Affine algebraische Varietäten

Sei K ein Körper, und sei $\overline{K}$ ein algebraischer Abschluss von K.

2.1 Algebraische Mengen

Für eine nichtleere Teilmenge $M \subset K[X_1, \ldots, X_n]$ sei

$$\boxed{\mathfrak{V}(M) := \{x \in \overline{K}^n \mid f(x) = 0 \ \ \forall\, f \in M\}}.$$

Ist I das von M erzeugte Ideal in $K[X_1, \ldots, X_n]$, so gilt $\mathfrak{V}(M) = \mathfrak{V}(I)$.

Definition
Eine Teilmenge $V \subset \overline{K}^n$ heißt *algebraisch* oder (K)-*abgeschlossen*, falls es endlich viele Polynome $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ so gibt, dass

$$\boxed{V = \{x \in \overline{K}^n \mid f_i(x) = 0 \ \ \forall\, i = 1, \ldots, m\}}$$

gilt. Der Buchstabe V steht für Varietät.

Da jedes Ideal in $K[X_1, \ldots, X_n]$ endlich erzeugt ist (nach dem Hilbertschen Basissatz, Algebra 6.14), stimmt diese Definition mit der in 1.15 gegebenen Definition einer algebraischen Menge überein.

2.2 Zariski-Topologie

Satz
Die algebraischen Mengen in $\overline{K}^n$ erfüllen die Axiome für die abgeschlossenen Mengen einer Topologie auf $\overline{K}^n$.
Die Topologie ist kompakt, aber nicht hausdorffsch.

Beweis. (a) Die Mengen $\emptyset = \mathfrak{V}(\{1\})$ und $\overline{K}^n = \mathfrak{V}(\{0\})$ sind algebraisch.

(b) Endliche Vereinigungen algebraischer Mengen sind algebraisch, denn für $V_1 = \mathfrak{V}(\{f_1, \ldots, f_m\})$ und $V_2 = \mathfrak{V}(\{g_1, \ldots, g_\ell\})$ ist

$$V_1 \cup V_2 = \mathfrak{V}(\{f_i g_j \mid i = 1, \ldots, m\,,\ j = 1, \ldots, \ell\})\,.$$

(c) Beliebige Durchschnitte algebraischer Mengen sind algebraisch, denn für jedes System $(I_j)_{j \in J}$ von Idealen in $K[X_1, \ldots, X_n]$ gilt

$$\bigcap_{j \in J} \mathfrak{V}(I_j) = \mathfrak{V}\left(\bigcup_{j \in J} I_j\right) \underset{2.1}{=} \mathfrak{V}\left(\sum_{j \in J} I_j\right)\,.$$

(d) Die Topologie ist kompakt. Zu zeigen: In jeder Familie abgeschlossener Mengen, deren Durchschnitt leer ist, gibt es endlich viele Mengen, deren Durchschnitt leer ist.
Es gelte $\emptyset = \bigcap_{j\in J} \mathfrak{V}(I_j) \overset{(c)}{=} \mathfrak{V}\left(\sum_{j\in J} I_j\right)$. Dann folgt

$$(1) \underset{\text{Aufg. 7}}{=} \mathfrak{I}(\emptyset) = \mathfrak{I}\left(\mathfrak{V}\left(\sum_{j\in J} I_j\right)\right) \underset{1.14}{=} \operatorname{Rad}\left(\sum_{j\in J} I_j\right)$$

und also $1 \in \sum_{j\in J} I_j$. Es gibt daher endlich viele Ideale $I_1, \ldots, I_\ell$ unter den Idealen $\{I_j \mid j \in J\}$ mit $1 \in \sum_{j=1}^{\ell} I_j$ und also mit $(1) = \sum_{j=1}^{\ell} I_j$. Hieraus folgt $\emptyset \underset{(a)}{=} \mathfrak{V}((1)) = \mathfrak{V}\left(\sum_{j=1}^{\ell} I_j\right) \underset{(c)}{=} \bigcap_{j=1}^{\ell} \mathfrak{V}(I_j)$.

(e) Eine (K)-*offene* Menge in $\overline{K}^n$ ist das Komplement einer (K)-abgeschlossenen Menge in $\overline{K}^n$. Das *hausdorffsche Trennungsaxiom*:

„Je zwei verschiedene Punkte besitzen disjunkte Umgebungen"

gilt nicht, da $\overline{K}^n$ „irreduzibel" ist. Letzteres besagt, dass je zwei nichtleere (K)-offene Mengen einen nichtleeren Durchschnitt besitzen (vgl. 2.3, 2.4 unten). □

Definition
Die durch den Satz definierte Topologie auf $\overline{K}^n$ heißt *Zariski-K-Topologie* von $\overline{K}^n$. Im Fall $K = \overline{K}$ spricht man von der *Zariski-Topologie*.

Punkte und endliche Mengen in $\overline{K}^n$ sind in der Zariski-Topologie stets abgeschlossen.

2.3 Irreduzible algebraische Mengen

Definition
Eine algebraische Menge $V \neq \emptyset$ in $\overline{K}^n$ ist *irreduzibel*, falls es keine Darstellung $V = V_1 \cup V_2$ mit abgeschlossenen Mengen $V_1 \neq V$ und $V_2 \neq V$ gibt.

Satz
Eine algebraische Menge $V \neq \emptyset$ in $\overline{K}^n$ ist genau dann irreduzibel, wenn $\mathfrak{I}(V)$ ein Primideal in $K[X_1, \ldots, X_n]$ ist. Insbesondere ist $\overline{K}^n$ irreduzibel.

Beweis. Sei V irreduzibel und $f_1, f_2 \in K[X_1, \ldots, X_n]$ mit $f_1 \cdot f_2 \in \mathfrak{I}(V)$. Dann folgt $f_1(x) \cdot f_2(x) = 0$ für jedes $x \in V$ und also

$$V = (V \cap \mathfrak{V}(f_1)) \cup (V \cap \mathfrak{V}(f_2)).$$

Da V irreduzibel ist, folgt $V \subset \mathfrak{V}(f_1)$ oder $V \subset \mathfrak{V}(f_2)$ und also $f_1 \in \mathfrak{I}(V)$ oder $f_2 \in \mathfrak{I}(V)$. Damit ist gezeigt, dass $\mathfrak{I}(V)$ ein Primideal ist.

Sei umgekehrt $\mathfrak{I}(V)$ ein Primideal. Angenommen, es gibt algebraische Mengen $V_1, V_2 \subset \overline{K}^n$ mit $V_1 \subsetneq V$ und $V_2 \subsetneq V$ sowie $V = V_1 \cup V_2$. Dann gibt es Polynome $f_1 \in \mathfrak{I}(V_1) \setminus \mathfrak{I}(V)$ und $f_2 \in \mathfrak{I}(V_2) \setminus \mathfrak{I}(V)$. Es folgt $f_1 \cdot f_2 \in \mathfrak{I}(V_1) \cap \mathfrak{I}(V_2) \underset{\text{Aufg. 7}}{=} \mathfrak{I}(V_1 \cup V_2) = \mathfrak{I}(V)$. Da $\mathfrak{I}(V)$ Primideal ist, folgt der Widerspruch $f_1 \in \mathfrak{I}(V)$ oder $f_2 \in \mathfrak{I}(V)$. Da $\mathfrak{I}(\overline{K}^n) = (0)$ Primideal in $K[X_1, \ldots, X_n]$ ist, folgt die letzte Behauptung. □

Beispiel
$V := \{i, -i\} = \mathfrak{V}(X^2 + 1) \subset \mathbb{C}$ ist bezüglich der Zariski-$\mathbb{R}$-Topologie von $\mathbb{C}$ irreduzibel, da $X^2 + 1$ ein Primideal in $\mathbb{R}[X]$ ist, aber V ist bezüglich der Zariski-Topologie nicht irreduzibel, da $V = \mathfrak{V}(X - i) \cup \mathfrak{V}(X + i)$ gilt.

2.4 Irreduzible topologische Räume

Ein topologischer Raum $T \neq \emptyset$ heißt *irreduzibel*, wenn T nicht als Vereinigung zweier abgeschlossener echter Teilmengen darstellbar ist.
• Durch Negation und Komplementbildung erhält man:
T ist genau dann irreduzibel, wenn je zwei offene, nichtleere Teilmengen einen nichtleeren Durchschnitt haben.
• Eine Teilmenge $S \neq \emptyset$ in T heißt *irreduzibel*, wenn S als topologischer Raum bezüglich der induzierten Topologie irreduzibel ist.
• Für $S \subset T$ sei $\overline{S}$ der *Abschluss von S in T*, d. h. der Durchschnitt aller abgeschlossenen Teilmengen von T, die S enthalten. Es ist S genau dann abgeschlossen in T, wenn $S = \overline{S}$ gilt.
• $S \subset T$ heißt *dicht in T*, wenn $\overline{S} = T$ gilt.

Satz
Seien $T \neq \emptyset$ und $T' \neq \emptyset$ topologische Räume. Dann gelten:

(a) *Für jede nichtleere Teilmenge $S \subset T$ gilt:*
S *irreduzibel* $\iff$ $\overline{S}$ *irreduzibel*.

(b) T *irreduzibel* $\iff$ *Jede nichtleere offene Menge $U \subset T$ ist dicht in T.*

(c) $f\colon T \to T'$ *stetig und T irreduzibel* $\implies$ $f(T)$ *irreduzibel.*

Beweis. **(a)** „$\Longrightarrow$“:
Sei S irreduzibel, und sei $\overline{S} = A_1 \cup A_2$ mit abgeschlossenen Mengen $A_1, A_2 \subset \overline{S}$. Dann ist $S = (A_1 \cap S) \cup (A_2 \cap S)$ die Vereinigung zweier in S abgeschlossener Mengen, und also gilt $S = A_1 \cap S$ oder $S = A_2 \cap S$, da S irreduzibel ist. Es folgt $S \subset A_1$ oder $S \subset A_2$ und daher $\overline{S} \subset A_1$ oder $\overline{S} \subset A_2$ nach Definition von $\overline{S}$. Also ist $\overline{S}$ irreduzibel.

(a) „$\Longleftarrow$“:
Sei $\overline{S}$ irreduzibel, und sei $S = (B_1 \cap S) \cup (B_2 \cap S)$, wobei $B_1, B_2 \subset T$ abgeschlossen in T seien. Nach Definition von $\overline{S}$ ist dann $\overline{S} \subset B_1 \cup B_2$ und also $\overline{S} = (B_1 \cap \overline{S}) \cup (B_2 \cap \overline{S})$. Da $\overline{S}$ irreduzibel ist, folgt $\overline{S} = B_1 \cap \overline{S}$ oder $\overline{S} = B_2 \cap \overline{S}$. Hieraus folgt $S = B_1 \cap S$ oder $S = B_2 \cap S$. Also ist S irreduzibel.
(b) „$\Longrightarrow$“:
Es sind $U \cap (T \setminus \overline{U}) = \emptyset$ und $T \setminus \overline{U}$ offen. Da T irreduzibel ist, folgt $T \setminus \overline{U} = \emptyset$ und also $\overline{U} = T$.
(b) „$\Longleftarrow$“:
Seien U_1, U_2 offen in T und nichtleer. Dann gilt nach Voraussetzung $\overline{U_1} = T = \overline{U_2}$. Angenommen: $U_1 \cap U_2 = \emptyset$. Dann folgt $U_1 \subset T \setminus U_2$ und also der Widerspruch $\overline{U_2} = \overline{U_1} \subset T \setminus U_2$.
(c):
Seien U_1, U_2 offen in T' mit $U_1 \cap f(T) \neq \emptyset$ und $U_2 \cap f(T) \neq \emptyset$. Zu zeigen: $U_1 \cap U_2 \cap f(T) \neq \emptyset$. Da f stetig ist, sind $f^{-1}(U_1)$ und $f^{-1}(U_2)$ offen in T (und nichtleer). Da T irreduzibel ist, folgt $U := f^{-1}(U_1) \cap f^{-1}(U_2) \neq \emptyset$ und also $\emptyset \neq f(U) \subset U_1 \cap U_2 \cap f(T)$. □

2.5 Zerlegung in irreduzible Komponenten

Sei $T \neq \emptyset$ ein topologischer Raum.

Definition (1)
Eine *irreduzible Komponente von T* ist eine (bezüglich Inklusion) maximale irreduzible Teilmenge.

Definition (2)
T heißt *noethersch*, wenn jede absteigende Kette $A_1 \supset A_2 \supset \cdots$ von abgeschlossenen Mengen in T stationär wird. **Äquivalent**: T ist *noethersch*, wenn jede nichtleere Menge von abgeschlossenen Mengen in T ein minimales Element besitzt (vgl. Aufgabe 13).

Satz
Es gelten:

(a) *Jede irreduzible Menge $S \subset T$ ist in einer irreduziblen Komponente von T enthalten.*
(b) *T ist die Vereinigung seiner irreduziblen Komponenten.*
(c) *Ist T noethersch, so besitzt T endlich viele irreduzible Komponenten $V_1, \ldots, V_m$. Diese sind abgeschlossen, und es ist $T = V_1 \cup \cdots \cup V_m$.*

Beweis. **(a)** mit dem Lemma von Zorn (vgl. Algebra 7.5):
Sei $M := \{T' \subset T \mid T' \text{ irreduzibel und } S \subset T'\}$. Dann ist M bezüglich Inklusion halbgeordnet, und es ist $M \neq \emptyset$, weil $S \in M$.

Sei N eine geordnete Teilmenge vom M. Dann ist $V := \bigcup_{T' \in N} T' \in M$, denn: Seien U_1, U_2 offen in T und $U_i \cap V \neq \emptyset$ für $i = 1, 2$. Dann existieren $T_1, T_2 \in N$ mit $U_1 \cap T_1 \neq \emptyset$ und $U_2 \cap T_2 \neq \emptyset$. Da N geordnet ist, können wir $T_1 \subset T_2$ annehmen. Es folgt $\emptyset \underset{T_2 \text{ irr.}}{\neq} U_1 \cap U_2 \cap T_2 \subset U_1 \cap U_2 \cap V$.
Damit ist gezeigt, dass V irreduzibel ist. Da $S \subset V$ gilt, folgt $V \in M$, und V ist obere Schranke für N. Nach dem Lemma von Zorn gibt es ein maximales Element in M.
(b):
Für jedes $t \in T$ ist $\{t\}$ eine irreduzible Menge. Daher folgt (b) aus (a).
(c):
Angenommen: T ist nicht als endliche Vereinigung irreduzibler, in T abgeschlossener Mengen darstellbar. Da T noethersch ist, gibt es dann eine nichtleere minimale abgeschlossene Menge A in T, die sich nicht als endliche Vereinigung irreduzibler abgeschlossener Mengen in T darstellen läßt. Es ist A reduzibel, also $A = A_1 \cup A_2$, wobei A_1, A_2 abgeschlossene echte Teilmengen von A sind. Da A minimal ist, sind A_1 und A_2 endliche Vereinigungen irreduzibler abgeschlossener Teilmengen im Widerspruch dazu, dass $A = A_1 \cup A_2$ dies nicht ist. Es folgt $T = V_1 \cup \cdots \cup V_m$, wobei $V_1, \ldots, V_m$ irreduzibel und abgeschlossen sind. Sei V eine irreduzible Komponente von T. Dann ist $V = \bigcup_{i=1}^{m} (V \cap V_i)$ und also $V = V \cap V_i$ für ein i nach Definition der Irreduzibilität. Es folgt $V \subset V_i$ und daher $V = V_i$, da V maximal. □

Korollar
Ist V eine algebraische Menge in $\overline{K}^n$, so besitzt V nur endlich viele irreduzible Komponenten $V_1, \ldots, V_m$, und es ist $V = V_1 \cup \cdots \cup V_m$.

Beweis. Es ist V ein topologischer Raum bezüglich der induzierten Zariski-K-Topologie von $\overline{K}^n$.
Sei $A_1 \supset A_2 \supset \cdots$ eine Kette von (K-)abgeschlossenen Mengen in V. Die aufsteigende Kette

$$\mathfrak{I}(A_1) \subset \mathfrak{I}(A_2) \subset \cdots$$

ist stationär, da $K[X_1, \ldots, X_n]$ nach dem Hilbertschen Basissatz (Algebra 6.14) noethersch ist. Also ist

$$A_1 = \mathfrak{V}(\mathfrak{I}(A_1)) \supset A_2 = \mathfrak{V}(\mathfrak{I}(A_2)) \supset \cdots$$

stationär. Es folgt, dass V noethersch ist. Satz (c) ergibt die Behauptung. □

2.6 Affiner Koordinatenring $K[V]$

Sei $\overline{K}$ ein algebraischer Abschluss von K. Dann gibt es Bijektionen

- $\{\text{Punkte in } \overline{K}^n\} \underset{1.10}{\overset{\sim}{\longleftrightarrow}} \{\text{maximale Ideale in } \overline{K}[X_1, \ldots, X_n]\}$
- $\{K\text{-abgeschl. Mengen in } \overline{K}^n\} \underset{1.15}{\overset{\sim}{\longleftrightarrow}} \{\text{Radikalideale in } K[X_1, \ldots, X_n]\}$
- $\{\text{irred. } K\text{-abgeschl. Mengen in } \overline{K}^n\} \underset{1.15}{\overset{2.3}{\longleftrightarrow}} \{\text{Primideale in } K[X_1, \ldots, X_n]\}$

Analoge Resultate werden erzielt, wenn man links (statt von $\overline{K}^n$) von einer beliebigen algebraischen Menge $V \subset \overline{K}^n$ ausgeht und rechts (statt von $K[X_1, \ldots, X_n]$) von der K-Algebra $K[X_1, \ldots, X_n]/\mathfrak{I}(V)$ (vgl. Aufgabe 18).

Definition
Für eine algebraische Menge $V \subset \overline{K}^n$ heißt die K-Algebra

$$\boxed{K[V] := K[X_1, \ldots, X_n]/\mathfrak{I}(V)}$$

der *affine Koordinatenring von V* oder die *affine Algebra von V*.

Beispiele
- Ist $V = \overline{K}^n$, so ist $K[V] = K[X_1, \ldots, X_n]/(0) = K[X_1, \ldots, X_n]$.
- Ist $\mathfrak{V} = \emptyset$, so ist $K[V] = K[X_1, \ldots, X_n]/(1) = (0)$ (Nullring).

2.7 Eigenschaften des affinen Koordinatenrings

1) $K[V]$ ist reduziert (d. h. enthält keine nilpotenten Elemente außer 0) und endlich erzeugt als K-Algebra, also eine *affine K-Algebra*, vgl. 1.13, 1.12 und 1.2.

2) $K[V]$ ist noethersch (als homomorphes Bild eines noetherschen Ringes).

3) Die Elemente von $K[V]$ lassen sich als Funktionen $V \to \overline{K}$ auffassen: Ist $\varphi \in K[V]$, so ist $\varphi = f + \mathfrak{I}(V)$ mit einem $f \in K[X_1, \ldots, X_n]$. Für $v \in V$ setze $\varphi(v) := f(v)$. Man erhält so eine wohldefinierte Inklusion

$$K[V] \hookrightarrow \mathrm{Abb}(V, \overline{K}),$$

denn für $f, g \in K[X_1, \ldots, X_n]$ gilt:

$$\begin{aligned} f + \mathfrak{I}(V) = g + \mathfrak{I}(V) &\underset{\text{Algebra 7.2}}{\Longleftrightarrow} f - g \in \mathfrak{I}(V) \\ &\underset{\text{Def 1.13}}{\Longleftrightarrow} (f-g)(v) = 0 \ \ \forall\, v \in V \\ &\Longleftrightarrow f(v) = g(v) \ \ \forall\, v \in V. \end{aligned}$$

Es folgt

$$K[V] = \{\varphi\colon V \to \overline{K} \mid \exists\, f \in K[X_1, \ldots, X_n] \text{ mit } \varphi(v) = f(v)\ \forall\, v \in V\}.$$

Es ist $K[V]$ die K-Algebra der „polynomialen Funktionen“ $V \to \overline{K}$. Wir schreiben $K[V] = \mathrm{Mor}(V, \overline{K})$.

Beispiele
Zu jedem $x_i := X_i + \mathfrak{I}(V)$ gehört die i-te Koordinatenfunktion $x_i\colon V \to \overline{K},\ (a_1, \ldots, a_n) \mapsto a_i,$ für $i = 1, \ldots, n$.

4) Mit der Interpretation aus 3) ist das *Verschwindungsideal* einer Teilmenge $W \subset V$ definiert als

$$\mathfrak{I}_V(W) := \{\varphi \in K[V] \mid \varphi(w) = 0\ \forall\, w \in W\}.$$

Es gilt $\mathfrak{I}_V(W) = \mathfrak{I}(W)/\mathfrak{I}(V)$, und die Zuordnung $\varphi \mapsto \varphi|_W$ induziert einen Isomorphismus

$$K[V]/\mathfrak{I}_V(W) \xrightarrow{\sim} K[W],$$

denn nach dem zweiten Noetherschen Isomorphiesatz (Algebra 1.6) gilt:

$$\underbrace{K[X_1, \ldots, X_n]/\mathfrak{I}(W)}_{K[W]} \simeq (\underbrace{K[X_1, \ldots, X_n]/\mathfrak{I}(V)}_{K[V]})/(\underbrace{\mathfrak{I}(W)/\mathfrak{I}(V)}_{\mathfrak{I}_V(W)}).$$

5) Sei umgekehrt I ein beliebiges Ideal in $K[V] = K[X_1, \ldots, X_n]/\mathfrak{I}(V)$. Dann ist die *Nullstellenmenge von I* definiert als

$$\mathfrak{V}_V(I) := \{v \in V \mid \varphi(v) = 0\ \forall\, \varphi \in I\}.$$

Es ist $\mathfrak{V}_V(I)$ eine K-abgeschlossene Menge in V, denn I ist endlich erzeugt nach 2), also $I = (\varphi_1, \ldots, \varphi_m)$ mit $\varphi_i = f_i + \mathfrak{I}(V)$ und $f_i \in K[X_1, \ldots, X_n]$ für $i = 1, \ldots, m$, und es folgt $\mathfrak{V}_V(I) = \mathfrak{V}(f_1, \ldots, f_m) \cap V$.

2.8 Morphismen von algebraischen Mengen

Seien $V \subset \overline{K}^n$ und $W \subset \overline{K}^m$ algebraische Mengen.

Definition
Eine Abbildung $\alpha\colon V \to W$ heißt *polynomial* oder *Morphismus*, wenn es Polynome $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ gibt mit

$$\alpha(v) = (f_1(v), \ldots, f_m(v))\ \ \forall\, v \in V.$$

Ein Morphismus $\alpha\colon V \to W$ heißt *Isomorphismus*, wenn es einen Morphismus $\beta\colon W \to V$ gibt mit $\alpha \circ \beta = \mathrm{id}_W$ und $\beta \circ \alpha = \mathrm{id}_V$.

Beispiel
Sei $V = \{(a,b) \in \overline{K}^2 \mid b = a^2\} = \mathfrak{V}(X_1^2 - X_2)$ und $W = \overline{K} = \mathfrak{V}(0 \cdot K[X])$. Die Projektion von V auf die x_1-Achse ($= W$) ist dann ein Isomorphismus $\pi\colon V \to W,\ (a,a^2) \mapsto a$, mit Umkehrabbildung $\pi^{-1}\colon W \to V,\ a \mapsto (a,a^2)$. Es sind π und π^{-1} polynomial, denn es ist $\pi(a,a^2) = a = f(a)$ mit $f = X_1 \in K[X_1,X_2]$ und $\pi^{-1}(a) = (a,a^2) = (f_1(a), f_2(a))$ mit $f_1 = X$ und $f_2 = X^2$ in $K[X]$.

2.9 Eine Äquivalenz von Kategorien

Seien $V \subset \overline{K}^n$ und $W \subset \overline{K}^m$ algebraische Mengen. Dann induziert jeder Morphismus $\alpha\colon V \to W$ einen K-Algebrahomomorphismus

$$\begin{array}{ccc} K[W] & \longrightarrow & K[V] \\ \| & & \| \\ \alpha^*\colon \operatorname{Mor}(W,\overline{K}) & \longrightarrow & \operatorname{Mor}(V,\overline{K}) \\ \varphi & \longmapsto & \varphi \circ \alpha \end{array}$$

und für Morphismen $V \xrightarrow{\alpha} V' \xrightarrow{\beta} V''$ gilt $(\beta \circ \alpha)^* = \alpha^* \circ \beta^*$. Ferner ergibt sich $(\mathrm{id}_V)^* = \mathrm{id}_{K[V]}$.

In Kategoriensprache: Es gibt einen kontravarianten Funktor

$$\mathcal{F}\colon \left\{\begin{array}{c}\text{Kategorie der algebraischen}\\ \text{Mengen in } \overline{K}^n\\ \text{und Morphismen}\end{array}\right\} \longrightarrow \left\{\begin{array}{c}\text{Kategorie der affinen}\\ K\text{-Algebren und } K\text{-Algebra-}\\ \text{homomorphismen}\end{array}\right\}$$

Objekte: $V \mapsto K[V]$, Morphismen: $\alpha \mapsto \alpha^*$

Sei $\operatorname{Mor}(V,W)$ die Menge der Morphismen $V \to W$,
und sei $\operatorname{Hom}_{\mathrm{Alg}}(K[W],K[V])$ die Menge der K-Algebrahomomorphismen $K[W] \to K[V]$.

Satz
Der Funktor $\mathcal{F}$ ist volltreu*, d. h. die Abbildung*

$$\mathcal{F}_{V,W}\colon \operatorname{Mor}(V,W) \to \operatorname{Hom}_{\mathrm{Alg}}(K[W],K[V]),\ \alpha \mapsto \alpha^*,$$

ist bijektiv. Insbesondere gilt

$$\underbrace{\boxed{V \textit{ isomorph } W}}_{\text{als algebraische Mengen}} \iff \underbrace{\boxed{K[V] \textit{ isomorph } K[W]}}_{\text{als } K\text{-Algebren}}.$$

Beweis. **Injektivität von $\mathcal{F}_{V,W}$:**
Für $\alpha, \beta \in \mathrm{Mor}(V,W)$ sei $\alpha^* = \beta^*$. Zu zeigen: $\alpha = \beta$. Nach Definition 2.8 eines Morphismus gibt es $f_1, \ldots, f_m$ und $g_1, \ldots, g_m \in K[X_1, \ldots, X_n]$ mit $\alpha(v) = (f_1(v), \ldots, f_m(v))$ und $\beta(v) = (g_1(v), \ldots, g_m(v))$ für alle $v \in V$. Für alle $\varphi \in K[W] = K[Y_1, \ldots, Y_m]/\mathfrak{I}(W) = \mathrm{Mor}(W, \overline{K})$ gilt

$$\varphi \circ \alpha \underset{\text{Def von } *}{=} \alpha^*(\varphi) = \beta^*(\varphi) \underset{\text{Def von } *}{=} \varphi \circ \beta\,.$$

Es folgt $y_i \circ \alpha = y_i \circ \beta$ für alle $i = 1, \ldots, m$, wobei $y_i = Y_i + \mathfrak{I}(W)$ die i-te Koordinatenabbildung ist (vgl. 2.7.3) und also

$$f_i(v) \underset{\text{Def von } y_i}{=} (y_i \circ \alpha)(v) = (y_i \circ \beta)(v) \underset{\text{Def von } y_i}{=} g_i(v)$$

für alle $i = 1, \ldots, m$ und alle $v \in V$. Es folgt $\alpha(v) = \beta(v)$ für alle $v \in V$.

Surjektivität von $\mathcal{F}_{V,W}$:
Sei $\gamma\colon K[W] \to K[V]$ ein K-Algebrahomomorphismus. Wähle $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ so, dass $\gamma(y_i) = f_i + \mathfrak{I}(V)$ für alle $i = 1, \ldots, m$ gilt.
Der Morphismus $\alpha\colon V \to \overline{K}^m,\ v \mapsto (f_1(v), \ldots, f_m(v))$ induziert den K-Algebrahomomorphismus $\alpha^*\colon K[Y_1, \ldots, Y_m] \to K[V],\ g \mapsto g \circ \alpha$, wobei

$$\begin{aligned} g \circ \alpha &\underset{\text{Def von } \alpha}{=} g \circ (f_1, \ldots, f_m) = g \circ (\gamma(y_1), \ldots, \gamma(y_m)) \\ &= \gamma(g + \mathfrak{I}(W)) \quad \text{siehe folgende Bemerkung} \\ &= \gamma\left(0_{K[W]}\right) \quad \text{falls } g \in \mathfrak{I}(W) \\ &= 0_{K[V]}\,. \end{aligned}$$

Da $W = \mathfrak{V}(\mathfrak{I}(W))$ gilt, folgt $\alpha(v) \in W$ für alle $v \in V$. Weiter folgt, dass α^* auch auf $K[W] = K[Y_1, \ldots, Y_m]/\mathfrak{I}(W)$ wohldefiniert ist und $\alpha^* = \gamma$ gilt.

Bemerkung
Es ist $g = \sum_{(r_1,\ldots,r_m)\in\mathbb{N}_0^m}^{\text{endl}} a_{r_1\ldots r_m} Y_1^{r_1} \cdot \ldots \cdot Y_m^{r_m}$, woraus folgt:
$g + \mathfrak{I}(W) = \sum a_{r_1} \ldots a_{r_m}\ y_1^{r_1} \cdot \ldots \cdot y_m^{r_m}$ und also
$\gamma(g + \mathfrak{I}(W)) = \sum a_{r_1} \ldots a_{r_m} \gamma(y_1)^{r_1} \ldots \gamma(y_m)^{r_m} = g \circ (\gamma(y_1), \ldots, \gamma(y_m))$.

Die letzte Behauptung des Satzes folgt leicht:

„$\Longrightarrow$“ gilt, weil $\mathcal{F}$ ein Funktor mit $(\alpha \circ \beta)^* = \beta^* \circ \alpha^*$ und $(\mathrm{id}_V)^* = \mathrm{id}_{K[V]}$ ist.

„$\Longleftarrow$“ gilt, weil $\mathcal{F}_{V,W}$ bijektiv ist. □

Folgerung
Der Funktor $\mathcal{F}$ ist eine Äquivalenz von Kategorien, denn $\mathcal{F}$ ist volltreu, und jede affine K-Algebra ist von der Form $K[X_1, \ldots, X_n]/\mathfrak{I}(V)$ mit einer geeigneten algebraischen Menge $V \subset \overline{K}^n$ (vgl. Korollar 1.15).

2.10 Zum Tensorprodukt

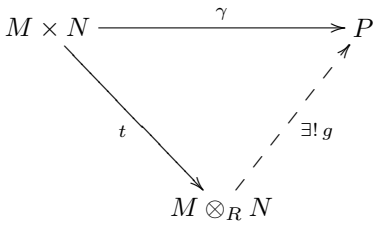
Gegeben seien ein kommutativer Ring R und R-Moduln M, N. Das *Tensorprodukt* $M \otimes_R N$ wurde in Algebra 10.7 eingeführt. Es besteht aus endlichen Summen der Form $z = \sum m_i \otimes n_i$ mit $m_i \in M, n_i \in N$. Da R kommutativ ist, ist $M \otimes_R N$ ein R-Modul, und es gelten die Regeln

$$\begin{aligned}(m + m') \otimes n &= m \otimes n + m' \otimes n \\ m \otimes (n + n') &= m \otimes n + m \otimes n' \\ rm \otimes n &= m \otimes rn \quad \forall\, m, m' \in M, n, n' \in N, r \in R\,.\end{aligned}$$

Universelle Eigenschaft
Zu jeder R-bilinearen Abbildung $\gamma\colon M \times N \to P$ in einen R-Modul P gibt es eine eindeutig bestimmte R-lineare Abbildung $g\colon M \otimes_R N \to P$ mit

$$\boxed{g(m \otimes n) = \gamma(m, n) \;\; \forall\, m \in M,\; n \in N}\,.$$

Folgendes Diagramm, bei dem $t(m, n) = m \otimes n$ gilt, ist also kommutativ:



Dabei ist γ eine *R-bilineare Abbildung*, falls die Abbildungen

$$\begin{aligned}\gamma_n\colon M \to P,\; m \mapsto \gamma(m, n) \quad &\text{für jedes } n \in N \\ \text{und } \gamma_m\colon N \to P,\; n \mapsto \gamma(m, n) \quad &\text{für jedes } m \in M\end{aligned}$$

jeweils R-linear sind.

Beispiele (i) Sei A eine kommutative R-Algebra. Dann ist die Multiplikation $A \times A \to A$, $(a, a') \mapsto aa'$, ersichtlich R-bilinear, und es gibt eine eindeutig bestimmte R-lineare Abbildung

$$\boxed{m_A\colon A \otimes_R A \to A, \quad \text{mit} \quad m_A(a \otimes a') = aa' \;\; \forall\, a, a' \in A}$$

genannt *Multiplikationsabbildung* oder *Multiplikation*.

(ii) Die beiden Abbildungen $M \times N \to N \otimes_R M,\ (m,n) \mapsto n \otimes m$, und $N \times M \to M \otimes_R N,\ (n,m) \mapsto m \otimes n$, sind R-bilinear. Es gibt also eine kanonische R-Modulisomorphie

$$M \otimes_R N \xrightarrow{\sim} N \otimes_R M,\ m \otimes n \mapsto n \otimes m\,.$$

(iii) *Tensorprodukt von R-linearen Abbildungen*
Gegeben seien R-lineare Abbildungen $u\colon M \to M'$ und $v\colon N \to N'$. Zu der R-bilinearen Abbildung

$$M \times N \to M' \otimes_R N',\ (m,n) \mapsto u(m) \otimes v(n)$$

gibt es genau eine R-lineare Abbildung $w\colon M \otimes_R N \to M' \otimes_R N'$ mit

$$w(m \otimes n) = u(m) \otimes v(n)\ \ \forall\, m \in M,\, n \in N\,.$$

Die Abbildung w heißt *Tensorprodukt von u und v*.

(iv) *Tensorprodukt von kommutativen Algebren*
Seien A, B kommutative R-Algebren. Dann ist das Tensorprodukt $A \otimes_R B$ eine kommutative R-Algebra mit Einselement $1 \otimes 1$, und es gilt

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb' \quad \forall\, a, a' \in A,\, b, b' \in B\,,$$

denn nach (ii) gibt es eine R-Modulisomorphie

$$h\colon\ (A \otimes_R B) \otimes_R (A \otimes_R B) \to (A \otimes_R A) \otimes_R (B \otimes_R B)$$

mit $h\,((a \otimes b) \otimes (a' \otimes b')) = (a \otimes a') \otimes (b \otimes b')\ \forall\, a, a' \in A,\, b, b' \in B$, und $A \otimes_R B$ ist eine R-Algebra bezüglich des Produktes

$$x \cdot y = (m_A \otimes m_B)(h(x \otimes y)) \text{ für } x, y \in A \otimes_R B\,,$$

wobei $m_A \otimes m_B$ durch (i) und (iii) gegeben ist.

(v) Für kommutative R-Algebren A, B ist $A \otimes_R B$ sowohl eine A-Algebra als auch eine B-Algebra, denn

$$A \to A \otimes_R B,\ a \mapsto a \otimes 1$$
$$B \to A \otimes_R B,\ b \mapsto 1 \otimes b$$

sind Ringhomomorphismen (vgl. Definition 1.1 einer kommutativen Algebra).

(vi) Ist I ein Ideal in R, so wird durch $(r,m) \mapsto rm + IM$, eine bilineare Abbildung $R/I \times M \to M/IM$, $(r+I, m) \mapsto rm + IM$, induziert und daher eine (R/I)-lineare Abbildung

$$R/I \otimes_R M \xrightarrow{\sim} M/IM\,.$$

Diese ist bijektiv; die Umkehrabbildung wird durch $m \mapsto (1+I) \otimes m$ induziert.

(vii) Seien S eine kommutative Ringerweiterung von R und I ein Ideal in $R[X_1, \ldots, X_n]$, und sei $J = I \cdot S[X_1, \ldots, X_n]$. Dann wird durch $(R[X_1, \ldots, X_n]/I) \times S \to S[X_1, \ldots, X_n]/J$, $(f+I, s) \mapsto sf + J$, ein Isomorphismus $(R[X_1, \ldots, X_n]/I) \otimes_R S \xrightarrow{\sim} S[X_1, \ldots, X_n]/J$ von S-Algebren induziert. (Durch $X_i \mapsto (X_i + I) \otimes 1$ wird die Umkehrabbildung erhalten.)

2.11 Tensorprodukt von affinen Algebren

Satz
Seien A, B endlich erzeugte kommutative Algebren über einem algebraisch abgeschlossenen Körper K. Dann gelten:

(i) *Sind A und B reduziert, so ist $A \otimes_K B$ reduziert.*

(ii) *Sind A und B Integritätsringe, so ist $A \otimes_K B$ ein Integritätsring.*

Beweis. Nach Korollar 1.15 gibt es eine algebraische Menge $V \subset K^n$ und eine algebraische Menge $W \subset K^m$ so, dass $A = K[V]$ und $B = K[W]$ gilt. Nach 2.12 i) unten ist $V \times W$ eine algebraische Menge, und nach 2.12 ii) unten gilt $K[V \times W] \simeq K[V] \otimes_K K[W]$. Da der affine Koordinatenring $K[V \times W]$ reduziert ist (vgl. 2.7 1), folgt nun (i).

(ii): Seien $f = \sum_{i=1}^{m} a_i \otimes b_i$ und $g = \sum_{j=1}^{n} c_j \otimes d_j$ Elemente in $A \otimes_K B$, und es gelte $fg = 0$. Zu zeigen ist, dass $f = 0$ oder $g = 0$ gilt. Wir können annehmen, dass $\{b_1, \ldots, b_m\}$ und $\{d_1, \ldots, d_n\}$ jeweils linear unabhängig sind, vgl. Algebra 10.11 (1). Sei $\mathfrak{M}$ ein maximales Ideal in A. Dann gilt $A/\mathfrak{M} = K$, wie aus Lemma 1.10 folgt, da K algebraisch abgeschlossen ist. Sei $\bar{a} := a + \mathfrak{M}$ für $a \in A$. Dann ist $\big(\sum \bar{a}_i \otimes b_i\big)\big(\sum \bar{c}_j \otimes d_j\big) = 0$ in $A/\mathfrak{M} \otimes_K B = K \otimes_K B \simeq B$. Da B ein Integritätsring ist, folgt $\sum \bar{a}_i \otimes b_i = 0$ oder $\sum \bar{c}_j \otimes d_j = 0$. Also sind alle a_i in $\mathfrak{M}$ oder alle c_j in $\mathfrak{M}$. Es ist $\mathfrak{M}_v := \mathfrak{I}_V(\{v\})$ für jedes $v \in V$ ein maximales Ideal in $A = K[V]$, da $\mathfrak{I}_V(\{v\}) = \ker(K[V] \to K,\ \varphi \mapsto \varphi(v))$ gilt. Für jedes $v \in V$ folgt nun

$$v \underset{\text{Aufg 17}}{\in} \mathfrak{V}_V(\mathfrak{M}_v) \subset \mathfrak{V}_V(a_1, \ldots, a_m) \cup \mathfrak{V}_V(c_1, \ldots, c_n)\,.$$

Da V nach Voraussetzung und 2.3 irreduzibel ist, folgt $V = \mathfrak{V}_V(a_1, \ldots, a_m)$ oder $V = \mathfrak{V}_V(c_1, \ldots, c_n)$. Da $\mathfrak{V}_V(0) = V$ gilt, erhalten wir im ersten Fall

$$\begin{aligned} \mathrm{Rad}(0) &\overset{\text{Aufg 18}}{=} \mathfrak{I}_V(\mathfrak{V}_V(0)) = \mathfrak{I}_V(V) = \mathfrak{I}_V(\mathfrak{V}_V(a_1, \ldots, a_m)) \\ &\overset{\text{Aufg 18}}{=} \mathrm{Rad}(a_1, \ldots, a_m)\,. \end{aligned}$$

Hieraus folgt $a_i \in \mathrm{Rad}(0)$ und also $a_i = 0$ für alle i, da A ein Integritätsring ist. Analog folgt $c_j = 0$ für alle j im zweiten Fall. □

Bemerkung
Mit den im Beweis von (ii) benutzen Methoden erhält man einen alternativen Beweis von (i).
Der obige Satz ist i. Allg. falsch, wenn K nicht algebraisch abgeschlossen ist, z. B. ist $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ kein Integritätsring, vgl. Aufgabe 22.

2.12 Produkt algebraischer Mengen

Satz
Seien $V \subset K^n$ und $W \subset K^m$ algebraische Mengen, wobei K algebraisch abgeschlossen sei.

i) *Die Menge $V \times W$ ist algebraisch.*

ii) *Es gibt eine Isomorphie $K[V \times W] \xrightarrow{\sim} K[V] \otimes_K K[W]$.*

iii) *Wenn V und W irreduzibel sind, so ist $V \times W$ irreduzibel.*

Beweis. i) Es ist $V = \mathfrak{V}(f_1, \ldots, f_k)$ mit $f_1, \ldots, f_k \in K[X_1, \ldots, X_n]$ und $W = \mathfrak{V}(g_1, \ldots, g_\ell)$ mit $g_1, \ldots, g_\ell \in K[Y_1, \ldots, Y_m]$ nach 2.1. Dann ist

$$V \times W = \mathfrak{V}(f_1, \ldots, f_k, g_1, \ldots, g_\ell) \subset K^{n+m}\,,$$

wobei $f_1, \ldots, f_k, g_1, \ldots, g_\ell$ als Polynome in $K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ aufgefasst werden.

ii) Die Abbildung

$$\gamma\colon K[V] \times K[W] \to K[V \times W]\,,\ (g, h) \mapsto \begin{cases} V \times W \to K \\ (v, w) \mapsto g(v) \cdot h(w) \end{cases}$$

ist K-bilinear und induziert also nach 2.10 einen K-Algebrahomomorphismus $\Gamma\colon K[V] \otimes_K K[W] \to K[V \times W]$.

Surjektivität von Γ: Jedes Polynom aus $K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ ist als endliche Summe von Produkten gh mit $g \in K[X_1, \ldots, X_n]$ und $h \in K[Y_1, \ldots, Y_m]$ darstellbar. Dies gilt dann auch für die polynomialen Funktionen, vgl. 2.7.3.

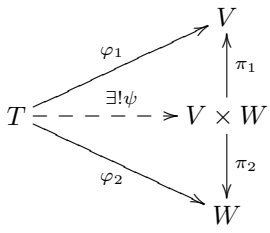
Injektivität von Γ: Schreibe $f \in K[V] \otimes_K K[W]$ als $f = \sum_{i=1}^{k} g_i \otimes h_i$ mit minimalem k. Sei $\Gamma(f) = 0$.
Angenommen: $f \neq 0$. Dann gibt es ein $w \in W$ und ein $j \in \{1, \ldots, k\}$ mit $h_j(w) \neq 0$. Da $\sum_{i=1}^{k} g_i(v)h_i(w) = 0$ für alle $v \in V$ gilt, folgt $\sum_{i=1}^{k} h_i(w)g_i = 0$, und also sind $g_1, \ldots, g_k$ linear abhängig über K, und es ist g_j eine Linearkombination der übrigen g_i. Es folgt $k = 1$, da man sonst einen Widerspruch zur Minimalität von k hätte. Folglich gilt $f = g_1 \otimes h_1$ mit $g_1(v) = 0$ für alle $v \in V$ und also $f = 0$ im Widerspruch zur Annahme.

iii) Nach 2.11 ist $K[V \times W] \overset{\text{(ii)}}{\simeq} K[V] \otimes_K K[W]$ ein Integritätsring und also $\mathfrak{I}(V \times W)$ ein Primideal in $K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$. Mit 2.3 folgt, dass $V \times W$ irreduzibel ist. □

Bemerkung

1. Die algebraische Menge $V \times W$ trägt die durch die Zariski-Toplologie von K^{n+m} induzierte Topologie. Diese stimmt *nicht* mit der Produkttopologie überein.

2. Das *Produkt* $V \times W$ zusammen mit den *Projektionen* $\pi_1 \colon V \times W \to V$, $(v, w) \mapsto v$ und $\pi_2 \colon V \times W \to W$, $(v, w) \mapsto w$, ist ein Produkt im Sinne der Kategorientheorie und daher bis auf Isomorphie eindeutig. Es gilt: Für jede algebraische Menge T und Morphismen $\varphi_1 \colon T \to V$ und $\varphi_2 \colon T \to W$ gibt es genau einen Morphismus $\psi \colon T \to V \times W$ mit $\pi_i \circ \psi = \varphi_i$ für $i = 1, 2$.



Das Problem der Existenz und gegebenenfalls Konstruktion von *Quotienten* ist i. Allg. schwierig.

2.13 Lokalisierungen

Sei R ein kommutativer Ring. In Algebra 6.10 haben wir jeder multiplikativ abgeschlossenen Menge $S \subset R \setminus \{0\}$ einen Quotientenring zugeordnet:

$$S^{-1}R = \left\{ \frac{r}{s} \mid r \in R, s \in S \right\} .$$

Satz
Seien $\mathfrak{p}$ ein Primideal in R und $S = R \setminus \mathfrak{p}$. Dann ist

$$R_{\mathfrak{p}} := S^{-1}R = \left\{ \frac{r}{s} \mid r, s \in R, s \notin \mathfrak{p} \right\}$$

ein Ring mit genau einem maximalen Ideal $\mathfrak{m} = \left\{ \frac{r}{s} \in R_{\mathfrak{p}} \mid r \in \mathfrak{p} \right\}$.

Beweis. Es ist $\mathfrak{m}$ ein Ideal, da $\frac{r}{s} + \frac{r'}{s'} = \frac{rs'+sr'}{ss'} \in \mathfrak{m}$ und $\lambda \cdot \frac{r}{s} \in \mathfrak{m}$ für alle $r, r' \in \mathfrak{p}$, $s, s' \in S$, $\lambda \in R_{\mathfrak{p}}$. Sei I ein Ideal in $R_{\mathfrak{p}}$ mit $I \supsetneq \mathfrak{m}$. Dann enthält I ein Element $\frac{r}{s}$ mit $r \notin \mathfrak{p}$, also mit $r \in S$. Es ist dann $\frac{r}{s}$ invertierbar in $R_{\mathfrak{p}}$, und es folgt $I = R_{\mathfrak{p}}$. Also ist $\mathfrak{m}$ ein maximales Ideal in $R_{\mathfrak{p}}$, und zwar das einzige, weil alle Nichteinheiten aus $R_{\mathfrak{p}}$ in $\mathfrak{m}$ liegen. □

Definition 1. Ein *lokaler Ring* ist ein kommutativer Ring mit genau einem maximalen Ideal.

2. Der Ring $R_{\mathfrak{p}}$ heißt *Lokalisierung von R nach $\mathfrak{p}$*.

3. Ist $f \in R$ kein Nullteiler in R und $S = \{f^m \mid m \in \mathbb{N}_0\}$, so wird die Bezeichnung R_f anstelle von $S^{-1}R$ benutzt. (Auch dieser Ring wird manchmal Lokalisierung genannt.)

2.14 Reguläre Funktionen

In diesem Abschnitt sei K algebraisch abgeschlossen (also $K = \overline{K}$).

Definition
Sei $V \subset K^n$ eine irreduzible algebraische Menge. Dann ist die affine Algebra $K[V]$ ein Integritätsring nach Satz 2.3. Sei

$$K(V) := \left\{ \frac{g}{h} \mid g, h \in K[V], h \neq 0 \right\}$$

der Quotientenkörper von $K[V]$ (vgl. Algebra 6.11). Der Körper $K(V)$ heißt *Funktionenkörper von V* oder *Körper der rationalen Funktionen über K*.

Beispiel
$V = \{(x_1, x_2) \in K^2 \mid x_1 = 0\} = \mathfrak{V}(X_1)$. Dann ist

$$K[V] = K[X_1, X_2]/(X_1) = K[X_2],$$

und $f = \frac{1}{X_2} \in K(V)$ ist in $(0,0)$ nicht definiert (und also nicht „regulär“). Der Punkt $(0,0)$ ist ein „Pol“ von f.
Dabei heißt allgemein ein Punkt $x \in V$ *Pol einer Funktion* $f \in K(V)$, falls für alle $g, h \in K[V]$, für die $f = \frac{g}{h}$ gilt, $h(x) = 0$ ist.

Wie in 2.7.3 beschrieben, fassen wir die Elemente von $K[V]$ als Funktionen $V \to K$ auf. Zu jedem $v \in V$ gehört ein lokaler Ring

$$\mathcal{O}_v := \left\{ \frac{g}{h} \mid g, h \in K[V],\ h(v) \neq 0 \right\}.$$

Es ist $\mathcal{O}_v$ gerade die Lokalisierung $K[V]_{\mathfrak{m}_v}$ nach dem maximalen Ideal

$$\mathfrak{m}_v := \{g \in K[V] \mid g(v) = 0\} = \operatorname{kern}(K[V] \to K,\ g \mapsto g(v)).$$

Die Elemente von $\mathcal{O}_v$ können wir nun i. Allg. nicht mehr als Funktionen $V \to K$ interpretieren. Daher ordnen wir jeder nichtleeren, offenen Menge $U \subset V$ den folgenden Ring zu

$$\boxed{\mathcal{O}_V(U) := \bigcap_{x \in U} \mathcal{O}_x}.$$

Dann lassen sich die Elemente aus $\mathcal{O}_V(U)$ als Funktionen $U \to K$ auffassen, denn ist $\psi \in \mathcal{O}_V(U)$, so gibt es zu jedem $x \in U$ Elemente $g, h \in K[V]$ mit $\psi = \frac{g}{h}$ und $h(x) \neq 0$. Wir setzen $\psi(x) := \frac{g(x)}{h(x)}$ und erhalten eine wohldefinierte Funktion $\psi\colon U \to K$: Ist $\frac{g}{h} = \frac{g'}{h'}$, wobei $h(x) \neq 0$ und $h'(x) \neq 0$, so ist $g(x)h'(x) - g'(x)h(x) = 0$ und also $\frac{g(x)}{h(x)} = \frac{g'(x)}{h'(x)}$. (Hier ist eingegangen, dass V irreduzibel und also $K[V]$ ein Integritätsring ist.)

Satz
Sei $A = K[V]$, *und für* $f \in A$ *sei* $D(f) := V_f := \{v \in V \mid f(v) \neq 0\}$. *Dann ist* $\mathcal{O}_V(V_f) = A_f$. *Insbesondere gilt* $\mathcal{O}_V(V) = K[V]$.

Beweis. Es ist $A_f \subset \mathcal{O}_V(V_f)$, denn für $\frac{g}{f^m}$ mit $g \in A$ gilt $\frac{g}{f^m} \in \mathcal{O}_v$ für alle $v \in V_f$ (nach Definition von V_f und $\mathcal{O}_v$). Also ist $\frac{g}{f^m} \in \bigcap_{v \in V_f} \mathcal{O}_v = \mathcal{O}_V(V_f)$.

Zu zeigen: $\mathcal{O}_V(V_f) \subset A_f$. Sei $\psi \in \mathcal{O}_V(V_f)$. Dann ist $\psi \in \mathcal{O}_v$ für alle $v \in V_f$. Nach Definition von $\mathcal{O}_v$ folgt $\psi = \frac{g_v}{h_v}$ mit $g_v, h_v \in A$ und $h_v(v) \neq 0$ für alle $v \in V_f$. Dies ergibt $h_v \in I := \{h' \in A \mid h'\psi \in A\}$ und $v \notin \mathfrak{V}_V(I)$ für alle

$v \in V_f$. Es folgt $\mathfrak{V}_V(I) \subset V \setminus V_f = \mathfrak{V}_V(f)$, und daher gilt $f \in \mathrm{Rad}(I)$ nach dem Hilbertschen Nullstellensatz (vgl. 1.14 und Aufgabe 18). Es gibt also ein $m \in \mathbb{N}$ mit $f^m \in I$. Nach Definition von I folgt $f^m\psi =: g \in A$ und also $\psi \in A_f$ nach Definition von A_f. Für $f\colon V \to K,\ v \mapsto 1$, ist $V_f = V$ und $A_f = A$. Daher folgt die zweite Behauptung. □

Bemerkung
Sei nun $V \subset K^n$ eine beliebige algebraische Menge. Dann orden wir jeder nichtleeren offenen Menge $U \subset V$ wie im irreduziblen Fall eine K-Algebra $\mathcal{O}_V(U)$ zu, und zwar die *Algebra der regulären Funktionen auf* U, wobei folgende Definition gilt.

Definition
Eine Funktion $f\colon U \to K$ heißt *regulär in* $x \in U$, wenn es $g, h \in K[V]$ und eine offene Umgebung $U' \subset U \cap V_h$ von x gibt so, dass $f(y) = \frac{g(y)}{h(y)}$ für alle $y \in U'$ gilt. Man nennt f *regulär*, falls f in jedem Punkt $x \in U$ regulär ist.

2.15 Geringte Räume

Sei V wie in Bemerkung 2.14 gegeben. Für nichtleere, offene Mengen $U' \subset U$ von V gilt dann

$$\mathcal{O}_V(U) \hookrightarrow \mathcal{O}_V(U')\,.$$

Die Zuordnung $\mathcal{O}_V\colon U \to \mathcal{O}_V(U)$ aus Bemerkung 2.14 definiert eine *Garbe von Funktionen*.
Dabei ist allgemein ist auf einem topologischen Raum T eine *Garbe* $\mathcal{O}$ *von Funktionen* gegeben, wenn es zu jeder nichtleeren, offenen Menge U in T eine K-Algebra $\mathcal{O}(U)$ von Funktionen $U \to K$ gibt und Folgendes gilt:

1) Ist $U' \neq \emptyset$ eine offene Teilmenge einer offenen Menge U, so definiert $f \mapsto f|_{U'}$ einen K-Algebrahomomorphismus $\mathcal{O}(U) \to \mathcal{O}(U')$.

2) Sei $U \neq \emptyset$ offen in T und $U = \bigcup_{j\in J} U_j$ eine offene Überdeckung von U, wobei J eine Indexmenge sei. Wenn für jedes $i \in J$ ein $f_i \in \mathcal{O}(U_i)$ gegeben ist, und wenn $f_i|_{U_i\cap U_j} = f_j|_{U_i\cap U_j}$ für alle $i, j \in J$ gilt, so gibt es ein $f \in \mathcal{O}(U)$ mit $f|_{U_i} = f_i$ für alle $i \in J$.

Das Paar $(T, \mathcal{O})$ nennt man dann einen *geringten Raum*.

2.16 Morphismen von geringten Räumen

Seien $(T, \mathcal{O})$ und $(T', \mathcal{O}')$ geringte Räume wie in 2.15 definiert, und sei $\alpha\colon T' \to T$ eine stetige Abbildung. Ist U eine offene Menge in T, so induziert α eine Abbildung $\alpha^*_U\colon \mathcal{O}(U) \to \mathrm{Abb}(\alpha^{-1}(U), K),\ f \mapsto f \circ \alpha|_{\alpha^{-1}(U)}$.

Definition
Man nennt α einen *Morphismus von geringten Räumen*, wenn $\alpha_U^*(\mathcal{O}(U)) \subset \mathcal{O}(\alpha^{-1}(U))$ für jede offene Menge U in T ist.
Ein Morphismus $\alpha\colon T' \to T$ heißt *Isomorphismus*, wenn es einen Morphismus $\beta\colon T \to T'$ mit $\alpha \circ \beta = \mathrm{id}$ und $\beta \circ \alpha = \mathrm{id}$ gibt.

2.17 Algebraische Varietäten

Wir kennen zwei Möglichkeiten der Definition der additiven Gruppe:
$\mathbb{G}_{\mathrm{a}}(K) = K \subset K^1$ mit Addition und $\mathbb{G}_{\mathrm{a}}(K) = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(K) \right\} \subset K^4$ mit Matrizenmultiplikation. Was ist nun die Definition von $\mathbb{G}_{\mathrm{a}}(K)$? Dies klärt der Varietätenbegriff.

Sei K ein algebraisch abgeschlossener Körper.

1) **Irreduzible affine algebraische Varietäten**
Eine *irreduzible affine algebraische Varietät* (oder kurz *irreduzible affine Varietät*) über K ist ein geringter Raum der Form $(V, \mathcal{O}_V)$ mit einer irreduziblen algebraischen Menge $V \subset K^n$ für passendes $n \in \mathbb{N}$ und einer Garbe $\mathcal{O}_V$, definiert durch $\mathcal{O}_V(U) = \bigcap_{x \in U} \mathcal{O}_x$ wie in 2.14.

2) **Der affine Raum**
Für jedes $n \in \mathbb{N}$ ist $(K^n, \mathcal{O}_{K^n}) =: \mathbb{A}^n$ ein Beispiel zu 1).

3) **Affine algebraische Varietäten**
Eine *affine algebraische Varietät* (oder kurz *affine Varietät*) über K ist ein geringter Raum der Form $(V, \mathcal{O}_V)$ mit einer algebraischen Menge $V \subset K^n$ und passendem $n \in \mathbb{N}$, wobei $\mathcal{O}_V(U)$ für eine offene Menge $U \subset V$ wie folgt gegeben ist: Es ist $V = V_1 \cup \cdots \cup V_m$ mit irreduziblen Komponenten $V_1, \ldots, V_m$ nach Korollar 2.5 und also $U = U_1 \cup \cdots \cup U_m$, wobei $U_i = U \cap V_i$ offen in V_i ist für alle $i = 1, \ldots, m$. Setze

$$\mathcal{O}_V(U) := \{ f\colon U \to K \mid f|_{U_i} \in \mathcal{O}_{V_i}(U_i) \ \forall\, i = 1, \ldots, m \}.$$

Es ist dann $\mathcal{O}_V(V) = K[V]$ wie im irreduziblen Fall, vgl. Satz 2.14. Die *Zariski-Topologie* von V ist die durch die Zariski-Topologie von K^n induzierte Topologie.

4) **Prävarietäten**
Eine *Prävarietät* (über K) ist ein geringter Raum $(V, \mathcal{O})$, wobei V noethersch ist und jeder Punkt $v \in V$ eine offene Umgebung U so besitzt, dass der geringte Raum $(U, \mathcal{O}|_U)$ isomorph zu einer affinen algebraischen Varietät ist. Jede solche Menge U heißt *offene affine* Teilmenge von V.

Ein *Morphismus von Prävarietäten* ist ein Morphismus von geringten Räumen wie in 2.16 definiert. Auch für Prävarietäten V, W existiert ein Produkt $V \times W$, das bis auf Isomorphie eindeutig ist, vgl. [5], 2.4.

5) **Projektive Varietäten**
Beispiele für nicht affine Prävarietäten sind *projektive Varietäten*, das sind abgeschlossene Untervarietäten eines projektives Raumes $\mathbb{P}^n(K)$. Eine *projektive algebraische Menge* in $\mathbb{P}^n(K)$ ist eine Menge der Form

$$\mathfrak{V}^*(I) := \{(x_0 : \cdots : x_n) \in \mathbb{P}^n(K) \mid f(x_0, \ldots, x_n) = 0 \ \forall\, f \in I\}\,,$$

wobei I ein homogenes Ideal in $K[X_0, \ldots, X_n]$ ist, d. h. ein Ideal, das von homogenen Polynomen erzeugt wird (vgl. 1.7).
Dies sind dann die abgeschlossenen Mengen in der Zariski-Topologie von $\mathbb{P}^n(K)$. Es gibt einen projektiven Hilbertschen Nullstellensatz, und mit Hilfe von regulären Funktionen kann man eine Garbe $\mathcal{O}_{\mathbb{P}^n}$ definieren.

6) **Algebraische Varietäten**
Eine Prävarietät heißt *algebraische Varietät* oder *Varietät* (über K), wenn das folgende Hausdorff-Axiom erfüllt ist:
Die Diagonale $\Delta_V = \{(v, v) \mid v \in V\}$ ist abgeschlossen in $V \times V$. Hierbei trägt $V \times V$ die Zariski-Topologie und nicht die Produkttopologie, vgl. Aufgabe 11.
Beispiel: Ist V eine affine Varietät, so ist dieses Hausdorff-Axiom erfüllt (Δ_V ist abgeschlossen in $V \times V$.)

7) **Zum Begriff eines Schemas**
Es gibt einen allgemeineren Garbenbegriff als den der Funktionengarben aus 2.15. Ist R ein kommutativer Ring, so definiert man auf der Menge $\mathrm{Spec}(R)$ der Primideale von R eine gewisse ringwertige Garbe $\mathcal{O}_{\mathrm{Spec}(R)}$. Das Paar $(\mathrm{Spec}(R), \mathcal{O}_{\mathrm{Spec}(R)})$ nennt man dann ein *affines Schema*. Ein *Schema* ist ein „geringter Raum“ (topologischer Raum mit einer Garbe $\mathcal{O}$ von Ringen), in dem es zu jedem Punkt eine offene Umgebung U so gibt, dass $(U, \mathcal{O}|_U)$ isomorph zu einem affinen Schema ist, vgl. z. B. [9] Kap. V.
Man kann dann von einem Schema über einem beliebigen Grundkörper ausgehen statt von einer Prävarietät über einem algebraisch abgeschlossenen Körper wie in 4).

2.18 Bild eines Morphismus

Sei K ein algebraisch abgeschlossener Körper. Wir schreiben meist V statt $(V, \mathcal{O}_V)$ für eine Varietät V über K. Ein Morphismus von Varietäten ist als Morphismus von Prävarietäten zu verstehen.

Satz 1
Sei $\alpha\colon V \to W$ ein Morphismus von affinen algebraischen Varietäten V, W, und sei $\alpha^*\colon K[W] \to K[V]$, $\varphi \mapsto \varphi \circ \alpha$, der zugehörige Algebrahomomorphismus. Dann ist $\alpha(V)$ genau dann dicht in W, wenn α^* injektiv ist.

Beweis. Sei $\overline{\alpha(V)}$ der Abschluss von $\alpha(V)$ in W. Dann ist

$$\begin{aligned}\operatorname{kern}\alpha^* &= \{\varphi \in K[\overline{\alpha(V)}] \mid \varphi(\alpha(v)) = 0 \,\forall\, v \in V\} \underset{2.7}{=} \mathfrak{I}_W(\alpha(V)) \\ &= \mathfrak{I}_W(\,\overline{\alpha(V)}\,)\,.\end{aligned}$$

Also gilt $\operatorname{kern}\alpha^* = \{0\}$ genau dann, wenn $W = \overline{\alpha(V)}$ ist. □

Sei V eine irreduzible affine algebraische Menge in K^n. Dann ist die affine Algebra $A = K[V]$ ein Integritätsring und wird von n Elementen $y_1, \ldots, y_n$ als Algebra erzeugt. Für jedes $f \in A \setminus \{0\}$ ist dann A_f die von $y_1, \ldots, y_n$ und f^{-1} im Quotientenkörper $K(V)$ von A erzeugte K-Algebra, vgl. 2.13. Nach Korollar 1.15 gehört zu A_f eine algebraische Menge in K^{n+1}. Für diese können wir die in V offene Menge $V_f := \{v \in V \mid f(v) \neq 0\}$ nehmen, und es gilt dann $A_f = K[V_f]$, vgl. Satz 2.14.

Das folgende Fundamentallemma wird im nächsten Kapitel gebraucht, um zu zeigen, dass auch das Bild einer linearen algebraischen Gruppe unter einem Homomorphismus eine lineare algebraische Gruppe ist.

Fundamentallemma
Sei $\alpha\colon V \to W$ ein Morphismus von affinen algebraischen Varietäten V, W. Dann enthält $\alpha(V)$ eine nichtleere Menge, die offen in $\overline{\alpha(V)}$ ist.

Beweis. Seien V_ℓ, $\ell \in L$ die Irreduzibilitätskomponenten von V. Dann ist $\overline{\alpha(V)} = \bigcup_{\ell\in L} \overline{\alpha(V_\ell)}$ mit irreduziblen Mengen $\overline{\alpha(V_\ell)}$, vgl. Satz 2.4. Falls die Aussagen des Lemmas für alle $\alpha_\ell := \alpha|_{V_\ell}$ gelten, so auch für α. Also kann man ohne Einschränkung kann man annehmen, dass V irreduzibel ist. Ohne Einschränkung kann man $W = \overline{\alpha(V)}$ setzen, sodass $\alpha(V)$ dicht in W ist. Dann ist auch W irreduzibel nach Satz 2.4, und es ist $\alpha^*\colon K[W] \to K[V]$ injektiv nach Satz 1 oben. Man kann also $S := K[W]$ als Unterring von $R := K[V]$ auffassen. Es sind R und S Integritätsbereiche, die als K-Algebren endlich erzeugt sind. Ihre Quotientenkörper seien $E \subset F$.
Sei R' die Lokalisierung von R bezüglich der multiplikativen Menge $S \setminus \{0\}$ der Nichtnullteiler in S. Wegen $E \subset R'$ kann R' als E-Algebra aufgefasst werden. Nach dem Noetherschen Normalisierungslemma 1.9 gibt es über E algebraisch unabhängige Elemente $T_1, \ldots, T_n$ in R' so, dass R' ganz über $E[T_1, \ldots, T_n]$ ist. Die Elemente $T_1, \ldots, T_n$ können offenbar sogar in R gewählt werden, da alle auftretenden Nenner invertierbar in E sind.

Es ist R als Ring endlich erzeugt über S, und jeder Erzeuger erfüllt eine normierte polynomiale Gleichung über $E[T_1, \ldots, T_n]$. Sei $f \in R$ ein gemeinsames Vielfaches der Nenner aller Koeffizienten in diesen Gleichungen. Dann ist R_f ganz über $S_f[T_1, \ldots, T_n]$, wobei die T_i weiterhin algebraisch unabhängig über S_f sind, vgl. Definition 2.13. Wegen $R_f = K[V_f]$ und $S_f = K[W_f]$ kann $S_f[T_1, \ldots, T_n] \cong S_f \otimes_K K[T_1, \ldots, T_n]$ als affine Algebra $K[V_f \times \mathbb{A}^n]$ von $V_f \times \mathbb{A}^n$ aufgefasst werden, vgl. 2.12.

Nun kann die Einschränkung $\alpha|_{V_f} \colon V_f \to W_f$ als $V_f \xrightarrow{\beta} W_f \times \mathbb{A}^n \xrightarrow{\pi_1} W_f$ geschrieben werden. Der Morphismus β erfüllt die Voraussetzungen von Satz 2 unten und ist demgemäß surjektiv. Schließlich ist $U = W_f$ die gesuchte offene Teilmenge von $\alpha(V)$, denn $\alpha^{-1}(U) = V_f$, und sowohl π_1 als auch β sind surjektiv, d. h. $U \subseteq \alpha(V)$. □

Satz 2
Sei $\beta \colon V \to W$ ein Morphismus von affinen Varietäten V, W so, dass $\beta^* \colon K[W] \to K[V]$ injektiv ist und $K[V]$, betrachtet als Ringerweiterung von $K[W]$, ganz über $K[W]$ ist. Dann ist β surjektiv.

Beweis. Die Punkte $w = (a_1, \ldots, a_n)$ von W entsprechen bijektiv den maximalen Idealen $\mathfrak{m}_w = (x_1 - a_1, \ldots, x_n - a_n)$ von $K[W]$, wobei

$$x_i \colon W \to K\,,\ (a_1, \ldots, a_n) \mapsto a_i\,,$$

die i-te Koordinatenfunktion bedeutet, vgl. Satz 1.10, 2.7.3 und Aufgabe 16. Die algebraische Menge $\beta^{-1}(w)$ wird durch die Gleichungen

$$\beta^*(x_1) - a_1 = 0\,, \ldots\,, \beta^*(x_n) - a_n = 0$$

definiert, und es ist $\beta^{-1}(w) = \emptyset$ genau dann, wenn $\mathfrak{m}_w K[V] = K[V]$ gilt. Letzteres ist aber nach dem Hilfssatz unten nicht möglich, da $K[V]$ nach Voraussetzung ganz und damit nach Satz 1.5 endlich über $K[W]$ ist. Deshalb gilt $\beta^{-1}(w) \neq \emptyset$ für alle $w \in W$. □

Hilfssatz
Sei B eine kommutative endliche Ringerweiterung eines kommutativen Ringes A, und sei I ein echtes Ideal in A. Dann gilt $B \neq IB$.

Beweis. Angenommen, es gilt $B = IB$. Wir zeigen durch Induktion nach der Anzahl n eines Erzeugendensystem $\{x_1, \ldots, x_n\}$ von B als A-Modul, dass es ein Element $a \in A$ so gibt, dass $a - 1 \in I$ und $aB = \{0\}$ gilt. Letzteres impliziert $a = 0$, weil $1 \in B$ gilt, und damit folgt $1 \in I$ im Widerspruch dazu, dass I ein echtes Ideal ist.
Sei $n = 1$ und also $B = Ax_1$. Da $B = IB$ gilt und I ein Ideal in A ist,

folgt $Ax_1 = IA\,x_1 = Ix_1$. Es gibt also ein $y \in I$ so, dass $x_1 = yx_1$ gilt. Für $a = 1 - y$ folgt dann $a - 1 \in I$ und $ax_1 = 0$, also $aB = \{0\}$.
Sei $n > 1$. Der A-Modul $B' = B/Ax_n$ wird von $n-1$ Elementen erzeugt, und es gilt $B' = IB'$. Nach Induktionsvoraussetzung gibt es ein $a \in A$ so, dass $a - 1 \in I$ und $aB' = \{0\}$ gilt. Letzteres impliziert $aB \subset Ax_n$. Da $B = IB$ gilt, folgt außerdem $aB = IaB \subset IAx_n = Ix_n$. Es ist also $ax_n = yx_n$ mit einem $y \in I$. Hieraus folgt, da $aB \subset Ax_n$ gilt, dass $(a - y)aB = \{0\}$ ist. Ferner gilt $(a-y)a \equiv 1 \mod I$, denn es ist $a = 1 + x$ mit einem $x \in I$. □

Bemerkung
Sei $\alpha\colon V \to W$ ein Morphismus von Varietäten. Dann heißt α *dominant*, wenn das Bild $\alpha(V)$ dicht in W ist. Sind V und W affine Varietäten, so heißt α *endlich*, wenn der affine Koordinatenring $K[V]$ ganz über dem Unterring $\alpha^*(K[W])$ ist. Mit diesen Begriffen lautet Satz 1:
Ein Morphismus $\alpha\colon V \to W$ von affinen Varietäten ist genau dann dominant, wenn $\alpha^*\colon K[W] \to K[V]$ injektiv ist.
Und Satz 2 lautet:
Dominante endliche Morphismen von affinen Varietäten sind surjektiv.

2.19 F-Strukturen

Sei F ein Teilkörper eines Körpers K, und sei $V \subset \overline{K}^n$ eine algebraische Menge (gemäß 2.1).

Definition 1. V heißt *F-abgeschlossen*, falls $V = \mathfrak{V}(I)$ mit einem Ideal I in $F[X_1, \ldots, X_n]$ gilt.

2. V heißt *F-definiert* (oder *definiert über F*), falls das Verschwindungsideal $\mathfrak{I}(V) = \{f \in K[X_1, \ldots, X_n] \mid f(x) = 0 \ \forall\, x \in V\}$ ein Erzeugendensystem in $F[X_1, \ldots, X_n]$ besitzt.

Da $V = \mathfrak{V}(\mathfrak{I}(V))$ gilt, folgt

$$\boxed{V \text{ ist } F\text{-definiert}} \quad \Longrightarrow \quad \boxed{V \text{ ist } F\text{-abgeschlossen}}.$$

Warnung
Die Umkehrung gilt im Allgemeinen nicht (da $\mathfrak{I}(\mathfrak{V}(I)) = \mathrm{Rad}(I)$).

Beispiel
Sei p eine Primzahl, und sei $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ der Primkörper mit p Elementen. Ferner sei $F := \mathbb{F}_p(Y)$ der rationale Funktionenkörper in einer Unbestimmten Y über $\mathbb{F}_p$. Es ist dann $K := F(\sqrt[p]{Y}) \simeq F[X]/(X^p - Y)$. Für das Ideal $I := (X^p - Y)$ in $F[X]$ gilt $\mathfrak{V}(I) = \left\{\sqrt[p]{Y}\right\}$.

Also ist $V := \mathfrak{V}(I)$ eine F-abgeschlossene Menge. Aber es ist

$$\mathfrak{I}(V) = \mathfrak{I}(\mathfrak{V}(I)) = \left\{ f \in K[X] \mid f\left(\sqrt[p]{Y}\right) = 0 \right\} = \left(X - \sqrt[p]{Y}\right) \cdot K[X]\,,$$

und also ist V nicht F-definiert. (Es ist $\left(X - \sqrt[p]{Y}\right)^p = X^p - Y \in I$).

Bemerkung

1) Ist F vollkommen, so kann man zeigen:
V ist F-abgeschlossen $\Longleftrightarrow$ V ist F-definiert.

2) Sei V über F definiert. Dann gibt es ein Ideal I in $F[X_1, \ldots, X_n]$ so, dass $\mathfrak{I}(V) = I \cdot K[X_1, \ldots, X_n]$ gilt. Setzt man $F[V] := F[X_1, \ldots, X_n]/I$, so hat man eine K-Algebraisomorphie $K \otimes_F F[V] \simeq K[V]$ nach 2.10 (vii). Diese Beobachtung führt zur folgenden Definition.

3) **Definition:** Eine *F-Struktur auf V* ist eine F-Unteralgebra $F[V]$ der zu V gehörigen affinen Algebra $K[V]$ mit den Eigenschaften:

   (a) $F[V]$ ist endlich erzeugt als F-Algebra.

   (b) Der von der Multiplikation $K \times F[V] \to K[V]$, $(\lambda, a) \mapsto \lambda a$, induzierte F-Algebrahomomorphismus $K \otimes_F F[V] \to K[V]$ ist ein Isomorphismus.

   Im Allgemeinen besitzt V verschiedene F-Strukturen.

4) Die Menge der *F-rationalen Punkte* einer F-Struktur $F[V]$ ist die Menge $V(F) := \mathrm{Hom}_{\mathrm{Alg}}(F[V], F)$ der F-Algebrahomomorphismen $F[V] \to F$. Diese Definition ist durch Aufgabe 15 motiviert, in der $F = K = \overline{K}$ ist.

Wegen der geschilderten Schwierigkeiten werden wir hier bis auf wenige Ausnahmen nur algebraische Gruppen über einem algebraisch abgeschlossenen Körper studieren.

2.20 Übungsaufgaben 8–22

Aufgabe 8
Sei K ein algebraisch abgeschlossener Körper. Man ermittle, welche der folgenden Teilmengen von K^n algebraisch sind:

(a) K^n und die leere Menge $\emptyset$,
(b) die Mengen $\{x\}$ mit $x \in K^n$,
(c) alle endlichen Teilmengen,
(d) $\{\, (z^2, z^3) \in \mathbb{C}^2 \mid z \in \mathbb{C} \,\}$.

Aufgabe 9
Für einen kommutativen Ring R sei $\mathrm{Spec}(R)$ die Menge der Primideale von R. Man zeige, dass $\mathrm{Spec}(R)$ eine Topologie trägt, deren abgeschlossenen Mengen gerade die sogenannten Zariski-*abgeschlossenen* Mengen

$$\mathcal{Z}(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \supset I\}$$

sind, wobei I alle Ideale von R durchläuft.

Aufgabe 10
Seien K ein algebraisch abgeschlossener Körper, $R = K[X_1, \ldots, X_n]$ und $\mathrm{Max}(R)$ die Menge der maximalen Ideale von R. Man zeige, dass die Abbildung

$$\psi\colon K^n \to \mathrm{Max}(R)\,,\ (a_1, \ldots, a_n) \mapsto (X_1 - a_1, \ldots, X_n - a_n),$$

ein Homöomorphismus ist, wenn K^n die Zariski-Topologie trägt und die Topologie von $\mathrm{Max}(R)$ durch die in Aufgabe 9 beschriebene Topologie von $\mathrm{Spec}(R)$ induziert wird.

Aufgabe 11
Sei K ein algebraisch abgeschlossener Körper. Man zeige, dass die *Diagonale* $\Delta := \{(a, b) \in K^2 \mid a = b\}$ bezüglich der Zariski-Topologie abgeschlossen in K^2 ist und dass Δ bezüglich der Produkttopologie nicht abgeschlossen in $K^1 \times K^1$ ist (wobei K^1 jeweils die Zariski-Topologie trage).

Ein topologischer Raum heißt *zusammenhängend*, wenn er nicht als disjunkte Vereinigung zweier abgeschlossener echter Teilmengen geschrieben werden kann.

Aufgabe 12
Sei K ein algebraisch abgeschlossener Körper. Man zeige, dass

$$V := \{(a, b) \in K^2 \mid ab = 0\}$$

eine abgeschlossene Menge in K^2 ist, die zusammenhängend, aber nicht irreduzibel ist.

Aufgabe 13
Sei T ein topologischer Raum, $T \neq \emptyset$. Dann heißt T noethersch, wenn jede Kette $A_1 \supset A_2 \supset \ldots$ von abgeschlossenen Mengen in T stationär wird, d. h. wenn es ein $n \in \mathbb{N}$ gibt mit $A_{n+k} = A_n$ für alle $k \in \mathbb{N}$.
Man zeige, dass T genau dann noethersch ist, wenn jede nichtleere Menge M von abgeschlossenen Mengen in T ein minimales Element besitzt (d. h. eine abgeschlossene Menge A enthält mit der Eigenschaft: $B \in M$ und $B \subset A \Longrightarrow B = A$).

Aufgabe 14
Seien R ein kommutativer Ring, I ein Ideal in R und $\pi\colon R \to R/I$ der kanonische Homomorphismus. Man zeige, dass die Abbildung

$$\{\text{Ideale } \mathfrak{a} \text{ in } R/I\} \to \{\text{Ideale } J \text{ in } R\,,\ \text{die } I \text{ enthalten}\}\,,\ \mathfrak{a} \mapsto \pi^{-1}(\mathfrak{a})$$

eine inklusionserhaltende Bijektion mit Umkehrabbildung $J \mapsto \pi(J) = J/I$ ist.

Aufgabe 15
Seien K ein algebraisch abgeschlossener Körper, V eine algebraische Menge in K^n und $K[V] = K[X_1, \ldots, X_n]/\mathfrak{I}(V)$ die affine Algebra von V. Man zeige, dass es Bijektionen

$$V \to \operatorname{Max}(K[V]) \quad \text{und} \quad \operatorname{Max}(K[V]) \to \operatorname{Hom}_{\mathrm{Alg}}(K[V], K)$$

gibt, wobei $\operatorname{Hom}_{\mathrm{Alg}}(K[V], K)$ die Menge der K-Algebrahomomorphismen von $K[V]$ nach K bezeichnet.

Aufgabe 16
Sei K ein Körper und A eine affine K-Algebra, die von n Elementen $x_1, \ldots, x_n$ erzeugt werde. Man zeige, dass es eine algebraische Menge V in $\overline{K}^n$ und einen K-Algebraisomorphismus $K[V] \xrightarrow{\sim} A$ gibt, bei dem die i-te Koordinatenfunktion auf V mit x_i für $i = 1, \ldots, n$ identifiziert wird.

Hinweis zu Aufgabe 16
Man modifiziere den Beweis von Korollar 1.15 entsprechend.

Aufgabe 17
Sei K ein algebraisch abgeschlossener Körper. Sei $V \subset K^n$ eine algebraische Menge. Man zeige, dass $\mathfrak{V}_V(\mathfrak{I}_V(U)) = \overline{U}$ für jede Teilmenge U von V gilt. Hierbei bezeichnet $\overline{U}$ den Abschluss von U in V bezüglich Zariski-Topologie.

Aufgabe 18
Seien K ein Körper, $\overline{K}$ ein algebraischer Abschluss von K und V eine K-abgeschlossene Teilmenge von $\overline{K}^n$. Man zeige:

(a) Für jedes Ideal I in $K[V]$ gilt $\operatorname{Rad}(I) = \mathfrak{I}_V(\mathfrak{V}_V(I))$.

(b) Durch $W \mapsto \mathfrak{I}_V(W)$ wird die Menge der K-abgeschlossenen Teilmengen W von V bijektiv auf die Menge der Radikalideale von $K[V]$ abgebildet.

(c) Bei der Zuordnung $W \mapsto \mathfrak{I}_V(W)$ entsprechen die irreduziblen Teilmengen von V eineindeutig den Primidealen in $K[V]$.

(d) Bei der Zuordnung $W \mapsto \mathfrak{I}_V(W)$ entsprechen die irreduziblen Komponenten von V eineindeutig den minimalen Primidealen in $K[V]$. Deren Anzahl ist somit endlich.

Aufgabe 19
Sei K ein Körper, und sei $n \in \mathbb{N}$. Man zeige, dass die Abbildung

$$K[X_1, \ldots, X_n] \longrightarrow \mathrm{Abb}(K^n, K)\,,\ f \longmapsto \varphi_f$$

mit $\varphi_f : K^n \to K,\ (a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n)$, genau dann injektiv ist, wenn K ein Körper mit unendlich vielen Elementen ist.

Aufgabe 20
Sei $V = \{(z_1, z_2) \in \mathbb{C}^2 \mid z_1^2 + z_2^2 = 1\}$. In $\mathbb{C}[V] = \mathbb{C}[X_1, X_2]/\mathfrak{I}(V)$ seien $a = X_1 + \mathfrak{I}(V)$ und $b = X_2 + \mathfrak{I}(V)$. Man zeige, dass die $\mathbb{R}$-Unteralgebren $\mathbb{R}[a, b]$ und $\mathbb{R}[ia, ib]$ von $\mathbb{C}[V]$ verschiedene $\mathbb{R}$-Strukturen auf V definieren.

Aufgabe 21
Sei K algebraisch abgeschlossen, und sei $K(V)$ der Funktionenkörper einer irreduziblen algebraischen Menge $V \subset K^n$. Man zeige, dass die Menge der Pole einer Funktion $f \in K(V)$ eine algebraische Menge in V ist.

Aufgabe 22
Man zeige, dass $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ kein Integritätsring ist.

3 Lineare algebraische Gruppen

Sei K ein algebraisch abgeschlossener Körper. Alle Varietäten seien Varietäten über K.

3.1 Definition

1. Eine *algebraische Gruppe* ist eine algebraische Varietät G, die so mit einer Gruppenstruktur

$$\mu\colon G \times G \to G,\ (x, y) \mapsto xy$$

versehen ist, dass μ und

$$i\colon G \to G,\ x \mapsto x^{-1}$$

Morphismen von Varietäten sind. Ist die Varietät affin, so heißt G eine *affine algebraische Gruppe* oder eine *lineare algebraische Gruppe*. (Es ist hierbei $G \times G$ mit der Zariski-Topologie versehen, und nicht mit der Produkttopologie.)

2. Ein *Homomorphismus $G \to G'$ von algebraischen Gruppen* G, G' ist ein Morphismus von Varietäten, der gleichzeitig ein Gruppenhomomorphismus ist (entsprechend ist ein Isomorphismus definiert).

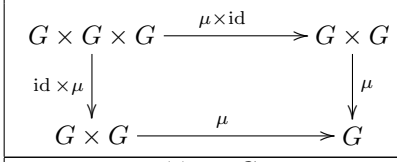
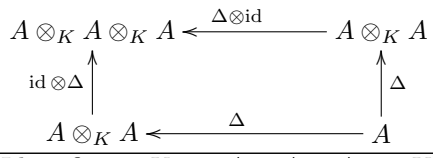
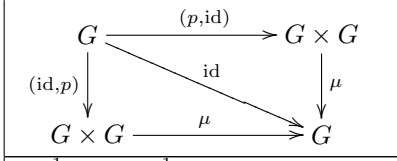
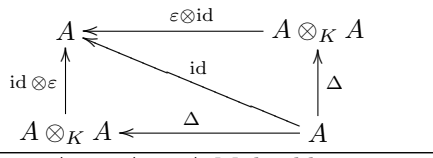
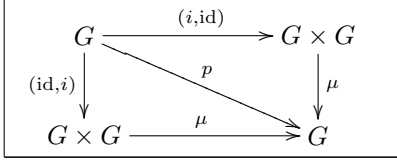
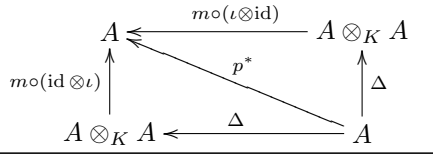
3. Eine Untergruppe H einer linearen algebraischen Gruppe G heißt *abgeschlossene Untergruppe*, falls H abgeschlossen bezüglich der Zariski-Topologie auf G ist.

Für die *additive Gruppe* $\mathbb{G}_{\mathrm{a}}(K)$ ist z. B. $\mu(x, y) = x+y$ und also $i(x) = -x$.

Bemerkung
Ist H eine abgeschlossene Untergruppe einer linearen algebraischen Gruppe G, so ist die Inklusion $H \hookrightarrow G$ ein Homomorphismus von algebraischen Gruppen.

3.2 Affine Algebra $K[G]$

Sei G eine lineare algebraische Gruppe, und sei $A := K[G] = \mathrm{Mor}(G, K)$ die affine Algebra gemäß 2.6 und 2.7.3. Die affine Algebra können wir jeder algebraischen Menge in K^n gemäß 2.9 zuordnen, und es erhebt sich die Frage, ob oder wie sich die Gruppenstruktur von G in der Algebra A widerspiegelt. Tatsächlich entspricht der Gruppenstruktur von G eine sogenannte „Koalgebrastruktur“ von A, wie aus der folgenden Tabelle mit kommutativen Diagrammen zu ersehen ist.

Morphismen von Gruppen	**Algebrahomomorphismen**
Multiplikation $\mu\colon G \times G \to G$	*Komultiplikation* $\Delta = \mu^*\colon A \to A \otimes_K A \underset{2.12}{\simeq} K[G \times G]$
Eins $e\colon \{e\} \to G$	*Koeins* (*Augmentation*) $\varepsilon = e^*\colon A \to K\,,\ f \mapsto f(e)$
Inverses $i\colon G \to G\,,\ x \mapsto x^{-1}$	*Koinverses* (auch *Antipode* genannt) $\iota = i^*\colon A \to A\,,\ f \mapsto (x \mapsto f(x^{-1}))$
Konstanter Morphismus $p\colon G \to G\,,\ x \mapsto e$	$p^*\colon A \to A\,,\ f \mapsto (x \mapsto f(e))$
Assoziativität von G 	*Koassoziativität* von A 
$ex = xe = x\ \forall x \in G$ 	Identifiziere $K \otimes_K A = A = A \otimes_K K$ 
$x^{-1}x = xx^{-1} = e\ \forall x \in G$ 	$m : A \otimes_K A \to A$ Multiplikation $\Rightarrow$ 

Man nennt eine mit obiger Kostruktur versehene Algebra eine *Hopf-Algebra*.

3.3 F-Gruppen

Definition
Die Bezeichnungen seien wie in 3.2. Sei F ein Teilkörper von K. Dann heißt G eine *F-Gruppe*, wenn G mit einer F-Struktur gemäß 2.19.3 versehen ist und also $A \simeq K \otimes_F A_0$ mit einer endlich erzeugten F-Algebra A_0 gilt, und wenn es F-Algebrahomomorphismen

$$\Delta_0\colon A_0 \to A_0 \otimes_F A_0\,, \quad \varepsilon_0\colon A_0 \to F\,, \quad \iota_0\colon A_0 \to A_0$$

so gibt, dass $\Delta = \mathrm{id} \otimes \Delta_0$ und $\varepsilon = \mathrm{id} \otimes \varepsilon_0$ und $\iota = \mathrm{id} \otimes \iota_0$ gelten.

3.4 Beispiele

1) *Die additive Gruppe* $G = \mathbb{G}_{\mathrm{a}}(K)$. Dann ist $K[G] = K[X]$ der Polynomring in einer Unbestimmten X. Es ist $\Delta(X) = X \otimes 1 + 1 \otimes X$ sowie $\iota(X) = -X$ und $\varepsilon(X) = 0$.
Für $\mu\colon G \times G \to G$, $(x, y) \mapsto x + y$, ist $\mu^* = \Delta\colon K[G] \to K[G \times G] \underset{2.12}{=} K[G] \otimes_K K[G]$ gegeben durch $\mu^*(X)(x, y) = (X \circ \mu)(x, y) = X(x + y) = x + y$, und es ist $(X \otimes 1 + 1 \otimes X)(x, y) \underset{2.12}{=} X(x) \cdot 1 + 1 \cdot X(y) = x + y$ nach 2.12 ii), wo $K[G] \otimes_K K[G] \xrightarrow{\sim} K[G \times G]$ gezeigt ist..

2) *Die multiplikative Gruppe* $G = \mathbb{G}_{\mathrm{m}}(K)$. Dann ist $K[G] = K[X, X^{-1}]$ und $\Delta(X) = X \otimes X$, $\varepsilon(X) = 1$, $\iota(X) = X^{-1}$.

3) *Die allgemeine lineare Gruppe* $\mathrm{GL}_n(K) = \{x \in \mathrm{M}_{n\times n}(K) \mid \det(x) \neq 0\}$ ist eine offene Menge in $\mathrm{M}_{n\times n}(K) \simeq K^{n^2}$. Die Gruppenstruktur ist durch Matrizenmultiplikation gegeben. Ferner ist $\mathrm{GL}_n(K)$ irreduzibel, denn K^{n^2} ist irreduzibel nach 2.3, und also ist $\mathrm{GL}_n(K)$ dicht in K^{n^2} nach 2.4 (b), was nach 2.4 (a) die Irreduzibilität von $\mathrm{GL}_n(K)$ impliziert. Es ist $\mathrm{GL}_n(K)$ eine lineare algebraische Gruppe nach Definition 3.1 und 2.17.1 sowie 0.1.9, und es ist

$$K[\mathrm{GL}_n(K)] = K[X_{ij}, d^{-1}]_{1\leqslant i,j\leqslant n}$$

mit $d = \det(X_{ij})$. Ferner gilt:

$$\begin{aligned} \Delta(X_{ij}) &= \sum_{k=1}^{n} X_{ik} \otimes X_{kj} \\ \text{sowie} \quad \varepsilon(X_{ij}) &= \delta_{ij} \\ \text{und} \quad \iota(X_{ij}) &= (-1)^{i+j} d^{-1} \det(X_{rs})_{r\neq j,\ s\neq i}\,. \end{aligned}$$

3.5 Zusammenhangskomponente der Eins

Satz
Sei G eine lineare algebraische Gruppe. Dann gelten:

(1) *Es gibt genau eine irreduzible Komponente G^0 von G, die das neutrale Element $e \in G$ enthält.*
(2) *G^0 ist abgeschlossener Normalteiler von endlichem Index in G, und die Nebenklassen gG^0 sind gerade die Irreduzibilitätskomponenten von G.*
(3) *$G = G^0 \iff G$ irreduzibel $\iff G$ zusammenhängend.*
(4) *Jede abgeschlossenen Untergruppe von endlichem Index in G enthält G^0.*

Beweis. (1) Nach Korollar 2.5 hat G nur endlich viele irreduzible Komponenten. Seien $G_1, \ldots, G_m$ die irreduziblen Komponenten, die e enthalten. Zu zeigen: $m = 1$. Es ist $G_1 \cdot \ldots \cdot G_m$ als Bild der Multiplikation $G_1 \times \cdots \times G_m \overset{\text{stetig}}{\longrightarrow} G_1 \cdot \ldots \cdot G_m$ irreduzibel. Also gibt es ein $i \in \{1, \ldots, m\}$ mit $G_1 \cdot \ldots \cdot G_m \subset G_i$, da jede irreduzible Menge in einer irreduziblen Komponente enthalten ist nach 2.5(a) und $e \in G_1 \cdot \ldots \cdot G_m$ ist. Es folgt $G_j \subset G_i$ für alle $j = 1, \ldots, m$, da $G_j \subset G_1 \cdot \ldots \cdot G_m$ gilt. Hieraus folgt $G_j = G_i$ für alle $j = 1, \ldots, m$, da G_j als irreduzible Komponente maximal nach Definition 2.5.1 ist. Es ist also $m = 1$.

(2) Als irreduzible Komponente ist G^0 abgeschlossen in G.

(i) G^0 ist eine Untergruppe von G, denn:
Als Bild der Multiplikation $G^0 \times G^0 \to G^0 G^0$ ist $G^0 G^0$ irreduzibel. Da $G^0 \subset G^0 G^0$ gilt und G^0 maximal ist, folgt $G^0 = G^0 G^0$. Da $i\colon G \to G^{-1},\ x \mapsto x^{-1}$, ein Homöomorphismus ist, ist $(G^0)^{-1}$ eine irreduzible Komponente von G, die e enthält, und also gilt $G^0 = (G^0)^{-1}$ nach (1).

(ii) G^0 ist Normalteiler in G, denn:
Für jedes $x \in G$ ist xG^0x^{-1} eine irreduzible Komponente von G, die e enthält, und also gilt $xG^0x^{-1} = G^0$ für alle $x \in G$ nach (1).

(iii) Jede Nebenklasse xG^0 mit $x \in G$ ist homöomorph zu G^0 und also eine irreduzible Komponente von G. Da G nur endlich viele davon besitzt, folgt (2) mit Hilfe von Korollar 2.5.

(3) Nach Definition ist G genau dann zusammenhängend, wenn G nicht als disjunkte Vereinigung zweier abgeschlossener echter Teilmengen geschrieben werden kann. Aus „G irreduzibel“ folgt also stets „G zusammenhängend“. Aus (2) folgt auch die umgekehrte Richtung, denn danach ist die Zerlegung von G in irreduzible Komponenten disjunkt.

(4) Sei H eine abgeschlossene Untergruppe von endlichem Index in G. Dann ist auch H^0 eine abgeschlossene Untergruppe von endlichem Index in G^0. Es gibt also ein $k \in \mathbb{N}$ so, dass $G^0 = H^0 \cup g_1 H^0 \cup \cdots \cup g_k H^0$ mit $g_1, \ldots, g_k \in G^0$ gilt. Es ist dann $G^0 \setminus H^0$ eine endliche Vereinigung abgeschlossener Mengen und daher selbst abgeschlossen. Es folgt $H^0 = G^0$, weil es andernfalls eine Zerlegung $G^0 = H^0 \cup G^0 \setminus H^0$ in echte abgeschlossene Teilmengen von G^0 geben würde im Widerspruch zur Irreduzibilität von G^0. Aus $H^0 = G^0$ folgt nun $G^0 \subset H$.

□

Bemerkung (a) Ist F ein Teilkörper von K und G eine F-Gruppe, so ist G^0 eine F-Gruppe. (Hier ohne Beweis)

(b) Wegen (3) nennt man eine irreduzible algebraische Gruppe auch *zusammenhängend* und reserviert den Begriff „irreduzibel“ für die Darstellungstheorie von Gruppen.

Beispiel
Sei $G_{\mathbb{R}} = \{x \in \mathrm{M}_{n\times n}(\mathbb{R}) \mid {}^t\!xx = e\}$ die *orthogonale Gruppe über* $\mathbb{R}$. Dann ist $1 = \det(e) = \det({}^t\!xx) = \det(x)^2$ und daher $\det(x) = \pm 1$. Also ist $G^0_{\mathbb{R}} = \mathrm{SO}_n(\mathbb{R}) := \{x \in G_{\mathbb{R}} \mid \det(x) = 1\}$, und es ist $G_{\mathbb{R}} = G^0_{\mathbb{R}} \cup G^-_{\mathbb{R}}$ mit $G^-_{\mathbb{R}} = \{x \in G_{\mathbb{R}} \mid \det(x) = -1\}$ die Zerlegung von $G_{\mathbb{R}}$ in irreduzible Komponenten. Es ist $G^-_{\mathbb{R}}$ eine Nebenklasse von $G^0_{\mathbb{R}}$ in $G_{\mathbb{R}}$, denn es gilt $G^-_{\mathbb{R}} = aG^0_{\mathbb{R}}$ mit $a = -e$, falls n ungerade ist, und mit $a = -e^{n+1}$, falls n gerade ist.

3.6 Produkt gewisser Teilmengen

Satz
Seien U, V Teilmengen einer algebraischen Gruppe G. Ist U offen und nicht-leer und ist V dicht in G, so ist $UV = G$.

Beweis. Sei $g \in G$. Zu zeigen: $U \cap gV^{-1} \neq \emptyset$ (denn dann gibt es $u \in U$ und $v \in V$ mit $u = gv^{-1}$, und es folgt $g = uv \in UV$).
Es ist $\psi\colon G \to G$, $x \mapsto gx^{-1}$, ein Homöomorphismus, und also folgt

$$G = \psi(G) \underset{V \text{ dicht}}{=} \psi(\overline{V}) \underset{\psi \text{ Homöo.}}{=} \overline{\psi(V)} = \overline{gV^{-1}}\,.$$

Angenommen: $U \cap gV^{-1} = \emptyset$. Dann folgt $gV^{-1} \subset G \setminus U$, und $G \setminus U$ ist abgeschlossen, da U offen ist. Dies ergibt $\overline{gV^{-1}} \subset G \setminus U$ nach Definition des Abschlusses, und also gilt $U \underset{\text{Vor.}}{\subset} G = \overline{gV^{-1}} \subset G \setminus U$. Dies ist ein Widerspruch, da $U \neq \emptyset$. □

Bemerkung
Ist G irreduzibel, so ist $G = UV$, falls U, V offen und nicht-leer sind, vgl. 2.4 (b).

3.7 Abschluss einer Untergruppe

Satz
Sei H eine Untergruppe einer algebraischen Gruppe G.

(i) *Der Abschluss $\overline{H}$ ist eine Untergruppe von G.*

(ii) *Enthält H eine nichtleere Menge, die offen in $\overline{H}$ ist, so ist H abgeschlossen.*

Beweis. (i) Da $G \xrightarrow{\sim} G$, $x \mapsto x^{-1}$, ein Homöomorphismus ist, folgt $\overline{H}^{-1} = \overline{H^{-1}} \underset{H \text{ Gruppe}}{=} \overline{H}$.
Da $G \to G$, $x \mapsto gx$, ein Homöomorphismus für jedes $g \in G$ ist, folgt $h\overline{H} = \overline{hH} \underset{H \text{ Gruppe}}{=} \overline{H}$ für jedes $h \in H$ und also $H\overline{H} = \overline{H}$.
Ist $y \in \overline{H}$, so folgt $Hy \subset H\overline{H} = \overline{H}$ und also $\overline{H}y = \overline{Hy} \subset \overline{H}$. Daher gilt $\overline{H}\,\overline{H} = \overline{H}$.

(ii) Ist $U \subset H$ offen in $\overline{H}$ und $U \neq \emptyset$, so folgt $H \supset UH \underset{3.6}{=} \overline{H}$. □

3.8 Kern und Bild eines Homomorphismus

Satz
Sei $\alpha\colon G \to G'$ ein Homomorphismus von linearen algebraischen Gruppen. Dann gelten:

(i) $\operatorname{kern}(\alpha)$ *ist eine abgeschlossene Untergruppe von* G.

(ii) $\operatorname{bild}(\alpha)$ *ist eine abgeschlossene Untergruppe von* G'.

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

Beweis. (i) Es ist $\operatorname{kern}(\alpha) = \alpha^{-1}(\{e\})$ und α stetig.

(ii) Nach dem Fundamentallemma 2.18 enthält $\alpha(G)$ eine nicht-leere Teilmenge, die offen in $\overline{\alpha(G)}$ ist. Nach 3.7 (ii) folgt daher, dass $\alpha(G)$ abgeschlossen ist.

(iii) Nach (ii) ist $\alpha(G^0)$ abgeschlossen, und nach 2.4 (c) irreduzibel. Da $e \in \alpha(G^0)$, folgt $\alpha(G^0) \subset (\alpha(G))^0$ nach 3.5 (1). Da $(G : G^0) < \infty$ nach 3.5 (2) gilt, ist auch $(\alpha(G) : \alpha(G^0)) < \infty$, und mit Hilfe von 3.5 (4) folgt $\alpha(G^0) \supset (\alpha(G))^0$. □

3.9 Operationen von G

Sei G eine lineare algebraische Gruppe, die vermöge

$$\alpha\colon G \times V \to V\,,\ (x, v) \mapsto xv\,,$$

auf einer affinen Varietät V operiere. Es gelte also

$$x(yv) = (xy)v \quad \text{und} \quad ev = v \quad \forall\, x, y \in G,\ v \in V\,.$$

Ist α ein Morphismus von Varietäten, so induziert α einen K-Algebrahomomorphismus

$$\begin{array}{ccc} K[V] & \xrightarrow{\alpha^*} & K[G\times V] \\ \| & & \| \\ \mathrm{Mor}(V,K) & \longrightarrow & \mathrm{Mor}(G\times V,K) \end{array} \qquad \underset{2\overline{1}2}{\simeq} \quad K[G]\otimes_K K[V]$$

$$f \longmapsto f\circ\alpha \longmapsto \sum_{i=1}^{n} f_i\otimes h_i\,,$$

wobei Folgendes gilt

$$(1) \qquad (f\circ\alpha)(x,v) = f(xv) = \sum_{i=1}^{n} f_i(x)h_i(v) \quad \forall\, x\in G,\ v\in V\,.$$

Der Homöomorphismus $V\to V,\ v\mapsto g^{-1}v$, induziert einen K-Algebrahomomorphismus

$$\lambda_g\colon K[V]\to K[V]\,,\ f\mapsto \begin{cases} V\to K \\ v\ \mapsto f(g^{-1}v)\,, \end{cases}$$

genannt *Linkstranslation mit g*, und es gilt

$$\lambda_{gh} = \lambda_g\cdot\lambda_h \quad \forall\, g,h\in G\,.$$

Satz
Sei Z ein endlich-dimensionaler Untervektorraum von $K[V]$. Dann gelten:

(i) *Es gibt einen endlich-dimensionalen Untervektorraum W von $K[V]$, der Z enthält und der stabil unter allen Linkstranslationen λ_g ist, d. h. es gilt $\lambda_g(W)\subset W$ für alle $g\in G$.*

(ii) *$\lambda_g(Z)\subset Z$ für alle $g\in G \iff \alpha^*(Z)\subset K[G]\otimes_K Z$.*

Beweis. (i) Sei zunächst Z erzeugt von einem Element $f\in K[V]$. Dann gilt: $(\lambda_g(f))(v) \underset{\text{Def. }\lambda_g}{=} f(g^{-1}v) \underset{(1)}{=} \sum_{i=1}^n f_i(g^{-1})h_i(v)\ \forall\, v\in V,\ g\in G$.
Es folgt $\lambda_g(f) = \sum_{i=1}^n f_i(g^{-1})h_i$, und also liegt $\lambda_g(f)$ in dem von $h_1,\dots,h_n$ erzeugten Untervektorraum W' von $K[V]$ für jedes $g\in G$. Der Untervektorraum W von W', der von allen $\lambda_g(f)$, $g\in G$ erzeugt wird, erfüllt $\lambda_g(W)\subset W$ und enthält $Z = Kf$.
Ist Z endlich-dimensional und $\{z_1,\dots,z_k\}$ eine Basis von Z, so bildet man die Summe der Räume, die man in der oben beschriebenen Weise zu jedem z_i für $i=1,\dots,k$ erhält, und (i) folgt.

(ii) „$\Longleftarrow$“ : Ist $\alpha^*(Z) \subset K[G] \otimes_K Z$, so zeigen der obige Beweis und (1), dass jedes h_i aus Z gewählt werden kann.

„$\Longrightarrow$“ : Sei $\lambda_g(Z) \subset Z$ für alle $g \in G$. Wähle eine Basis $\mathcal{B} = \{z_1, \ldots, z_k\}$ von Z und ergänze diese zu einer Basis $\mathcal{B} \cup \{h_j \mid j \in J\}$ von $K[V]$. Für $f \in Z$ gilt dann

$$\alpha^*(f) = \sum_{i=1}^{k} u_i \otimes z_i + \sum_{j}^{\text{endlich}} v_j \otimes h_j \in K[G] \otimes_K K[V]$$

mit eindeutig bestimmten $u_i, v_j \in K[G]$ (vgl. Algebra 10.11). Nach (1) und Voraussetzung gilt dann

$$\lambda_g(f) = \sum_{i=1}^{k} u_i(g^{-1}) z_i + \sum_{j}^{\text{endlich}} v_j(g^{-1}) h_j \underset{\text{Vor.}}{\in} Z$$

für alle $g \in G$. Es folgt $v_j(g^{-1}) = 0$ für alle $g \in G$, und daher $v_j = 0$. Dies ergibt $\alpha^*(f) = \sum_{i=1}^{k} u_i \otimes z_i \in K[G] \otimes_K Z$ für jedes $f \in Z$. $\square$

3.10 Linearisierung affiner Gruppen

Wir wenden nun Satz 3.9 mit $V = G$ an. Für jedes $g \in G$ gibt es die *Linkstranslation*

$$\lambda_g \colon K[G] \to K[G],\ f \mapsto \begin{cases} G \to K, \\ y \mapsto f(g^{-1}y) \end{cases}$$

und die *Rechtstranslation*

$$\rho_g \colon K[G] \to K[G],\ f \mapsto \begin{cases} G \to K, \\ y \mapsto f(yg)\,. \end{cases}$$

Hierdurch erhält man injektive Gruppenhomomorphismen

$$\lambda \colon G \to \mathrm{GL}(K[G]),\ g \mapsto \lambda_g$$
$$\rho \colon G \to \mathrm{GL}(K[G]),\ g \mapsto \rho_g\,,$$

wobei $K[G]$ als K-Vektorraum aufgefasst wird und $\mathrm{GL}(K[G])$ die Gruppe der K-linearen bijektiven Abbildungen $K[G] \to K[G]$ bezüglich der Hintereinanderausführung von Abbildungen bezeichnet. Es gilt $\rho_g = \iota \circ \lambda_g \circ \iota^{-1}$, wobei $\iota \colon K[G] \to K[G]$ für alle $g \in G$ wie in 3.2 definiert ist, und Satz 3.9 ist auch für Rechtstranslationen anwendbar.

Satz
Sei G eine lineare algebraische Gruppe. Dann gibt es ein $n \in \mathbb{N}$ und eine abgeschlossene Untergruppe H von $\mathrm{GL}_n(K)$ so, dass $G \simeq H$ ist.

Beweis. Wähle ein K-linear unabhängiges Erzeugendensystem $\{h_1, \ldots, h_k\}$ von $K[G]$ als K-Algebra. Nach 3.9 (i) gibt es einen ρ-stabilen Untervektorraum W von $K[G]$ mit $\mathcal{B} := \{h_1, \ldots, h_k, h_{k+1}, \ldots, h_n\}$ als Basis. Nach 3.9 (1) und Satz 3.9 (i) gibt es Elemente $a_{ij} \in K[G]$ mit $1 \leqslant i, j \leqslant n$ und

$$\rho_g(h_j) = \sum_{i=1}^{n} a_{ij}(g) h_j \quad \text{für jedes } g \in G\,.$$

Es ist also $(a_{ij}(g))_{1 \leqslant i,j \leqslant n}$ die Matrix von $\rho_g|_W$ bezüglich der Basis $\mathcal{B}$, und $\psi\colon G \to \mathrm{GL}_n(K)$, $g \mapsto a_{ij}(g)$, ist ein Gruppenhomomorphismus. Wir zeigen nun, dass ψ injektiv ist. Sei $\psi(g) = e$. Dann ist $\rho_g(h_j) = h_j$ für alle j, und also gilt $\rho_g(f) = f$ für alle $f \in K[G]$, da $h_1, \ldots, h_n$ die Algebra $K[G]$ erzeugen und ρ_g ein Algebrahomomorphismus ist. Es folgt $\rho_g = \mathrm{id}$ und also $g = e$. Ferner ist ψ ein Morphismus von affinen Varietäten. Der zugehörige Algebrahomorphismus

$$\psi^*\colon K[\mathrm{GL}_n(K)] \underset{3.4}{=} K[X_{ij}, d^{-1}] \to K[G]$$

ist gegeben durch $\psi^*(X_{ij}) = a_{ij}$ und $\psi^*(d^{-1}) = \det(a_{ij})^{-1}$. Die Gruppe $\psi(G)$ ist abgeschlossen in $\mathrm{GL}_n(K)$ nach 3.8 (ii). Noch zu zeigen ist, dass $\psi\colon G \to \psi(G)$ ein Isomorphismus von Varietäten ist. Es ist

$$h_j(g) = h_j(eg) = (\rho_g(h_j))(e) = \sum_{i=1}^{n} a_{ij}(g) h_j(e)$$

und also $h_j = \sum_{i=1}^{n} h_j(e) a_{ij}$. Hieraus folgt, dass ψ^* surjektiv ist (und also folgt nach Aufgabe 24 (b) erneut, dass $\psi(G)$ abgeschlossen in $\mathrm{GL}_n(K)$ ist). Ferner gilt

$$K[\psi(G)] \simeq K[\mathrm{GL}_n(K)]/\ker(\psi^*) \simeq K[G]\,,$$

und also vermittelt ψ einen Isomorphismus $G \simeq \psi(G)$ nach Satz 2.9. □

Bemerkung
Ist F ein Teilkörper von K, so lässt sich 3.9 leicht auch für F-Strukturen beweisen, und der Beweis von 3.10 geht auch durch. Man wähle das Erzeugendensystem $f_1, \ldots, f_k$ als Erzeugendensystem der F-Strukturen.

3.11 Übungsaufgaben 23–30

Aufgabe 23
Sei K ein Körper, und sei $\overline{K}$ ein algebraischer Abschluss von K. Sei $V \subset \overline{K}^n$ eine algebraische Menge, und sei $D(f) := \{v \in V \mid f(v) \neq 0\}$ für $f \in K[V]$. Man zeige:

(a) Die Menge $D(f)$ ist offen in V.

(b) Jede nicht-leere, offene Menge in V ist eine Vereinigung von Mengen der Form $D(f)$.

(c) Man zeige, dass die Eigenschaften (a) und (b) auch für die in Aufgabe 9 definierte Topologie auf der Menge $\mathrm{Spec}(R)$ der Primideale eines kommutativen Ringes R gelten, wenn $D(f) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid f \notin \mathfrak{p}\}$ für $f \in R$ ist.

Aufgabe 24
Sei K ein algebraisch abgeschlossener Körper. Sei $\alpha : V \longrightarrow W$ ein Morphismus von algebraischen Mengen $V \subset K^n$ und $W \subset K^m$.
Ferner sei $\alpha^* : K[W] \to K[V], \varphi \mapsto \varphi \circ \alpha$, der zugehörige K-Algebrahomomorphismus. Man zeige:

(a) α ist stetig bezüglich der Zariski-Topologie.

(b) Wenn α^* surjektiv ist, ist $\alpha(V)$ abgeschlossen in W.

Aufgabe 25
Seien R ein kommutativer Ring, $\mathfrak{N}$ der Durchschnitt aller Primideale und $\mathfrak{R}$ der Durchschnitt aller maximalen Ideale in R. Man zeige:

(a) Es ist $\mathfrak{N}$ die Menge der nilpotenten Elemente in R.

(b) $r \in \mathfrak{R} \iff 1 - ar$ ist eine Einheit in R für jedes $a \in R$.

(Man nennt $\mathfrak{N}$ das *Nilradikal* und $\mathfrak{R}$ das *Jacobson- Radikal* von R.)

Aufgabe 26
Sei K ein algebraisch abgeschlossenen Körper, und sei G eine lineare algebraische Gruppe über K mit affiner Algebra $A = K[G]$. Dann induzieren die Multiplikation $G \times G \to G$, die Einsabbildung $\{e\} \to G$ und die Inversenabbildung $G \to G$, $x \mapsto x^{-1}$, jeweils einen K-Algebrahomomorphismus

$\Delta_A : A \longrightarrow A \otimes_K A$ (*Komultiplikation*)
$\varepsilon_A : A \longrightarrow K,\ f \longmapsto f(e)$ (*Koeins*)
$\iota_A : A \longrightarrow A,\ f \longmapsto (x \mapsto f(x^{-1}))$ (*Koinverses*).

Den Gruppengesetzen von G entsprechen gewisse Kobedingungen für A. Man überprüfe den in 3.2 angegebenen Übersetzungsschlüssel von Gruppengesetzen zu Koalgebragesetzen.

(Man nennt A dann eine *Hopf-Algebra.*)

Aufgabe 27

Sei G eine lineare algebraische Gruppe über einem algebraisch abgeschlossenen Körper K, und sei $A = K[G]$. Man zeige, dass die Menge $\mathrm{Hom}_{\mathrm{Alg}}(A, K)$ der *rationalen Punkte* von G eine Gruppe ist, und gebe die Gruppenstruktur explizit an.

Aufgabe 28

Seien G, H lineare algebraische Gruppen mit affinen Algebren $A = K[G]$ und $B = K[H]$, und sei $\alpha : G \longrightarrow H$ ein Morphismus von Varietäten.

(a) Man zeige, dass $\alpha : G \longrightarrow H$ genau dann ein Gruppenhomomorphismus ist, wenn $\alpha^* : B \longrightarrow A$, $f \longmapsto f \circ \alpha$, ein Koalgebrahomomorphismus ist (das heißt, wenn $\Delta_A \circ \alpha^* = (\alpha^* \otimes \alpha^*) \circ \Delta_B$ und $\varepsilon_A \circ \alpha^* = \varepsilon_B$ gilt).

(b) Sei G kommutativ. Man ermittle eine entsprechende Bedingung dafür, dass A *kokommutativ* ist.

Aufgabe 29

Man zeige, dass die multiplikative Gruppe $\mathbb{G}_{\mathrm{m}}(K)$ nicht isomorph zur additiven Gruppe $\mathbb{G}_{\mathrm{a}}(K)$ ist.

Aufgabe 30

Man gebe ein Beispiel für einen Morphismus $\alpha : V \longrightarrow W$ von algebraischen Mengen V, W derart an, dass das Bild $\alpha(V)$ nicht abgeschlossen in W ist.

4 Jordanzerlegungen

4.1 Simultane Diagonalisierbarkeit

Sei K ein Körper, und sei W ein K-Vektorraum mit $\dim_K W =: n < \infty$.

Definition
Eine Teilmenge $S \subset \mathrm{End}_K(W)$ heißt *diagonalisierbar*, wenn es eine Basis $\mathcal{B}$ von W gibt derart, dass $\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\sigma)$ für alle $\sigma \in S$ eine Diagonalmatrix ist.

Satz
Wenn $\sigma \circ \tau = \tau \circ \sigma$ für alle $\sigma, \tau \in S$ gilt, und wenn jedes $\sigma \in S$ diagonalisierbar ist, dann ist S diagonalisierbar.

Beweis. Durch Induktion nach n:
Ist $n = 1$, so erfüllt jede Basis von W die Behauptung. ✓
Sei $n > 1$. Ist jedes $\sigma \in S$ ein skalares Vielfaches der Identität, so ist $\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\sigma)$ eine Diagonalmatrix für jedes $\sigma \in S$ und jede Basis $\mathcal{B}$ von W. ✓
Es gebe nun ein $\sigma \in S$, das kein skalares Vielfaches der Identität ist. Für jedes $\lambda \in K$ ist $W_\lambda := \{w \in W \mid \sigma(w) = \lambda w\} = \ker(\sigma - \lambda\,\mathrm{id})$ stabil unter allen $\tau \in S$, denn für $w \in W_\lambda$ und alle $\tau \in S$ gilt

$$\sigma(\tau(w)) \underset{\text{Vor.}}{=} \tau(\sigma(w)) \underset{\text{Def. von } W_\lambda}{=} \tau(\lambda w) \underset{\tau \text{ lin.}}{=} \lambda\tau(w)$$

und also $\tau(w) \in W_\lambda$. Da σ diagonalisierbar ist, gilt $W = W_{\lambda_1} \oplus \cdots \oplus W_{\lambda_k}$, wobei $\lambda_1, \ldots, \lambda_k$ die verschiedenen Eigenwerte von σ sind (vgl. AGLA 8.8). Nach Wahl von σ ist $k > 1$ und also $\dim_K W_{\lambda_i} < n$ für alle $i = 1, \ldots, k$. Die Induktionsvoraussetzung angewandt auf jedes W_{λ_i} ergibt dann die Behauptung. □

4.2 Additive Jordanzerlegung

Sei K ein Körper, und sei W ein endlich-dimensionaler K-Vektorraum.

Satz (Additive Jordanzerlegung)
Sei $\sigma \in \mathrm{End}_K(W)$ ein Endomorphismus, dessen Eigenwerte alle in K liegen. Dann gibt es eindeutig bestimmte Endomorphismen $\sigma_s, \sigma_n \in \mathrm{End}_K(W)$ so, dass $\sigma = \sigma_\mathrm{s} + \sigma_\mathrm{n}$ ist, σ_s diagonalisierbar und σ_n nilpotent ist und $\sigma_\mathrm{s} \circ \sigma_\mathrm{n} = \sigma_\mathrm{n} \circ \sigma_\mathrm{s}$ gilt.

Beweis. Nach Voraussetzung zerfällt das charakteristische Polynom χ_σ von σ in Linearfaktoren, also $\chi_\sigma = \pm \prod_{i=1}^{k} (X - \lambda_i)^{n_i}$, wobei $\lambda_1, \ldots, \lambda_k$ paarweise verschieden seien und $n_1, \ldots, n_k \in \mathbb{N}$. Sei $W_i := \ker((\sigma - \lambda_i\,\mathrm{id})^{n_i})$ der *verallgemeinerte Eigenraum zum Eigenwert* λ_i für $i = 1, \ldots, k$.

Es gilt $W = W_1 \oplus \cdots \oplus W_k$ und $\dim_K W_i = n_i$ sowie $\sigma(W_i) \subset W_i$ für alle $i = 1, \ldots, k$, vgl. AGLA 14.4. Nach dem Chinesischen Restsatz (vgl. Algebra 7.8) gibt es ein Polynom $P \in K[X]$ mit

$$(*) \qquad P \equiv \lambda_i \bmod (X - \lambda_i)^{n_i} \quad \forall\, i = 1, \ldots, k\,,$$

und, falls 0 kein Eigenwert ist, zusätzlich mit $P \equiv 0 \bmod (X)$. Wir setzen $\sigma_{\mathrm{s}} = P(\sigma)$. Dann folgt

$$(**) \qquad \sigma_{\mathrm{s}}(w) = \lambda_i\, w \quad \forall\, w \in W_i \text{ und } \forall\, i = 1, \ldots, k\,,$$

denn nach $(*)$ gibt es $f_i \in K[X]$ mit $P - \lambda_i = f_i \cdot (X - \lambda_i)^{n_i}$ und also mit $\sigma_{\mathrm{s}} - \lambda_i \,\mathrm{id} = f_i(\sigma)(\sigma - \lambda_i \,\mathrm{id})^{n_i}$, da $\sigma_{\mathrm{s}} = P(\sigma)$ gilt. Es folgt $\sigma_{\mathrm{s}}(w) - \lambda_i w = 0$ für alle $w \in W_i$ nach Definition von W_i. Also ist $\sigma_{\mathrm{s}}|_{W_i}$ diagonalisierbar für alle $i = 1, \ldots, k$ und daher auch σ_{s}, da $W = W_1 \oplus \cdots \oplus W_k$. Ferner folgt, dass $\sigma_{\mathrm{n}} := \sigma - \sigma_{\mathrm{s}}$ nilpotent ist, denn für jedes $w \in W_i$ gilt

$$0 = (\sigma - \lambda_i \,\mathrm{id})^{n_i}(w) \underset{(**)}{=} (\sigma - \sigma_{\mathrm{s}})^{n_i}(w) = \sigma_{\mathrm{n}}^{n_i}(w)\,,$$

und es ist $\sigma_{\mathrm{n}}(W_i) \subset W_i$. Da $P(\sigma) = \sigma_{\mathrm{s}}$ mit σ vertauschbar ist, folgt $\sigma_{\mathrm{n}} \circ \sigma_{\mathrm{s}} = (\sigma - \sigma_{\mathrm{s}}) \circ \sigma_{\mathrm{s}} = \sigma \circ \sigma_{\mathrm{s}} - \sigma_{\mathrm{s}}^2 = \sigma_{\mathrm{s}} \circ \sigma - \sigma_{\mathrm{s}}^2 = \sigma_{\mathrm{s}} \circ (\sigma - \sigma_{\mathrm{s}}) = \sigma_{\mathrm{s}} \circ \sigma_{\mathrm{n}}$.
Eindeutigkeit:
Sei $\sigma_{\mathrm{n}} + \sigma_{\mathrm{s}} = \sigma = \sigma'_{\mathrm{s}} + \sigma'_{\mathrm{n}}$. Da σ'_{s} mit σ'_{n} kommutiert, kommutieren σ'_{s} und σ'_{n} mit σ und also mit $\sigma_{\mathrm{s}} = P(\sigma)$. Es folgt, dass auch σ_{n} und σ'_{n} kommutieren. Also gilt $\sigma_{\mathrm{s}} - \sigma'_{\mathrm{s}} = \sigma'_{\mathrm{n}} - \sigma_{\mathrm{n}}$, wobei $\sigma_{\mathrm{s}} - \sigma'_{\mathrm{s}}$ diagonalisierbar und $\sigma'_{\mathrm{n}} - \sigma_{\mathrm{n}}$ nilpotent ist, wie aus 4.1 folgt, vgl. Aufgabe 34. Die Eigenwerte eines nilpotenten Endomorphismus sind alle 0 (vgl. Aufgabe 32). Es folgt $\sigma_{\mathrm{s}} - \sigma'_{\mathrm{s}} = 0$, da $\sigma_{\mathrm{s}} - \sigma'_{\mathrm{s}}$ diagonalisierbar ist. Also ist auch $\sigma'_{\mathrm{n}} - \sigma_{\mathrm{n}} = 0$. □

Korollar
Die Voraussetzungen seien wie im Satz, und es sei $\sigma = \sigma_{\mathrm{s}} + \sigma_{\mathrm{n}}$ die additive Jordanzerlung von σ. Dann gelten:

(i) *Es gibt Polynome $P, Q \in K[X]$ ohne konstanten Term derart, dass $P(\sigma) = \sigma_{\mathrm{s}}$ und $Q(\sigma) = \sigma_{\mathrm{n}}$ gilt. Insbesondere kommutieren σ_{s} und σ_{n} mit jedem Endomorphismus von W, der mit σ kommutiert.*

(ii) *Ist $Z \subset W$ ein σ-stabiler Untervektorraum von W, so ist Z auch σ_{s}- und σ_{n}-stabil, und $\sigma|_Z = \sigma_{\mathrm{s}}|_Z + \sigma_{\mathrm{n}}|_Z$ ist die additive Jordanzerlegung von Z.*

Beweis. (i) folgt direkt aus dem Satz nach Definition $P(\sigma) = \sigma_{\mathrm{s}}$ und $Q(\sigma) = \sigma_{\mathrm{n}}$.
Aus (i) folgt, dass Z von σ_{s} und σ_{n} stabilisiert wird. Das charakteristische Polynom von $\sigma|_Z$ teilt das charakteristische Polynom von σ, vgl. AGLA 14.2 und (ii) folgt analog wie im Satz mit dem Polynom P. □

4.3 Multiplikative Jordanzerlegung

Seien K ein Körper und W ein endlich-dimensionaler K-Vektorraum. Es bezeichne $\mathrm{Aut}_K(W)$ die Gruppe der Vektorraumisomorphismen $W \to W$. Aus der additiven Jordanzerlegung lässt sich leicht die entsprechend multiplikative Aussage herleiten.

Satz (Multiplikative Jordanzerlegung)
Sei $\sigma \in \mathrm{Aut}_K(W)$ ein Automorphismus, dessen Eigenwerte alle in K liegen. Dann besitzt σ eine eindeutige Zerlegung $\sigma = \sigma_\mathrm{s} \circ \sigma_\mathrm{u}$, wobei $\sigma_\mathrm{s} \in \mathrm{Aut}_K(W)$ diagonalisierbar und $\sigma_\mathrm{u} \in \mathrm{Aut}_K(W)$ unipotent *(d. h. $\sigma_\mathrm{u} - \mathrm{id}$ nilpotent) ist und $\sigma_\mathrm{s} \circ \sigma_\mathrm{u} = \sigma_\mathrm{u} \circ \sigma_\mathrm{s}$ gilt. Ferner gilt: Ist Z ein σ-stabiler Untervektorraum von W, so ist Z auch σ_s- und σ_u-stabil, und $\sigma|_Z = \sigma_\mathrm{s}|_Z \circ \sigma_\mathrm{u}|_Z$ ist die multiplikative Jordanzerlegung von $\sigma|_Z$.*

Beweis. Seien $\lambda_1, \ldots, \lambda_m$ die Eigenwerte von σ (wobei mehrfache Eigenwerte entsprechend mehrfach aufgeführt werden), und sei $P := \det(\sigma - X\,\mathrm{id})$. Nach Voraussetzung ist $P = (\lambda_1 - X) \cdot \ldots \cdot (\lambda_m - X)$ und also $P(0) = \det(\sigma) = \lambda_1 \cdot \ldots \cdot \lambda_m$. Da σ invertierbar ist, ist $\det(\sigma) \neq 0$, und es folgt $\det(\sigma_\mathrm{s}) \neq 0$, also $\sigma_\mathrm{s} \in \mathrm{Aut}_K(W)$. Nach Satz 4.2 ist $\sigma = \sigma_\mathrm{s} \circ \sigma_\mathrm{u}$ mit $\sigma_\mathrm{u} = \mathrm{id} + \sigma_\mathrm{s}^{-1}\sigma_\mathrm{n}$, und σ_u ist unipotent. Die letzte Behauptung folgt aus Korollar 4.2. □

4.4 Jordanzerlegung von Matrizen

Seien K ein Körper, $\overline{K}$ ein algebraischer Abschluss von K und W ein endlich-dimensionaler K-Vektorraum.

Definition
Eine Matrix $x \in \mathrm{M}_{n\times n}(K)$ heißt *halbeinfach*, wenn x über $\overline{K}$ diagonalisierbar ist, d. h. wenn es ein $s \in \mathrm{GL}_n(\overline{K})$ so gibt, dass sxs^{-1} eine Diagonalmatrix in $\mathrm{M}_{n\times n}(\overline{K})$ ist. Analog heißt ein Endomorphismus $\sigma\colon W \to W$ *halbeinfach*, wenn $\sigma \otimes \mathrm{id}\colon W \otimes_K \overline{K} \to W \otimes_K \overline{K}$ diagonalisierbar ist. (Im Fall $K = \overline{K}$ stimmen die Begriffe „halbeinfach“ und „diagonalisierbar“ überein.) Sei E_n die Einheitsmatrix in $\mathrm{M}_{n\times n}(K)$.
Eine Matrix $x \in \mathrm{M}_{n\times n}(K)$ heißt *unipotent*, wenn $x - E_n$ nilpotent ist.

Beispiel
$x = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ ist unipotent, denn $x - E_2 = \left(\begin{smallmatrix} 0 & a \\ 0 & 0 \end{smallmatrix}\right)$ und $(x - E_2)^2 = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$.

Die matrizentheoretische Version von 4.2 und 4.3 lautet:

Satz
Sei K algebraisch abgeschlossen. Dann besitzt jede Matrix $x \in \mathrm{M}_{n\times n}(K)$ eine Jordanzerlegung $x = x_\mathrm{s} + x_\mathrm{n}$ und jede Matrix $g \in \mathrm{GL}_n(K)$ eine Jordanzerlegung $g = g_\mathrm{s}g_\mathrm{u} = g_\mathrm{u}g_\mathrm{s}$, wobei $g_\mathrm{s}, x_\mathrm{s}$ halbeinfach, x_n nilpotent und g_u unipotent sind und $x_\mathrm{s} \circ x_\mathrm{n} = x_\mathrm{n} \circ x_\mathrm{s}$ gilt. Die Zerlegungen sind eindeutig.

Beweis. Da $K = \overline{K}$ ist, liegen alle Eigenwerte der Standardabbildung

$$\sigma\colon K^n \to K^n, \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto x \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \quad \text{bzw.} \quad \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto g \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

in K. Auf σ können wir 4.2 bzw. 4.3 anwenden, und dann folgt die Behauptung auch für die zugehörigen Matrizen, vgl. AGLA 5.4, 5.6 und 5.11. □

Bemerkung
Sei G eine Untergruppe von $\mathrm{GL}_n(K)$. Dann besitzt jedes $g \in G$ nach dem Satz eine Jordanzerlegung $g = g_\mathrm{s} g_\mathrm{u}$ mit $g_\mathrm{s}, g_\mathrm{u} \in \mathrm{GL}_n(K)$.

Problem
Liegen g_s und g_u wieder in G?
Im Allgemeinen: nein. Das ist aber der Fall, wenn G abgeschlossen und also eine lineare algebraische Gruppe ist, vgl. 4.6 unten.

4.5 Jordanzerlegung der Rechtstranslation in $K[G]$

Seien K algebraisch abgeschlossen, G eine lineare algebraische Gruppe und $K[G] = \mathrm{Mor}(G, K)$ die affine Algebra zu G. Der Isomorphismus

$$G \to G\,,\ x \mapsto xg\,,$$

induziert nach 2.9 für jedes $g \in G$ einen K-Algebraautomorphismus

$$\rho_g\colon K[G] \to K[G]\,,\ f \mapsto \begin{cases} G \to K, \\ x \mapsto f(xg)\,, \end{cases}$$

genannt *Rechtstranslation* mit g.

Satz
Für jedes $g \in G$ besitzt die Rechtstranslation $\rho_g\colon K[G] \to K[G]$ eine Jordanzerlegung $\rho_g = (\rho_g)_\mathrm{s} \circ (\rho_g)_\mathrm{u} = (\rho_g)_\mathrm{u} \circ (\rho_g)_\mathrm{s}$ so, dass $(\rho_g)_\mathrm{s}|_W$ halbeinfach und $(\rho_g)_\mathrm{u}|_W$ unipotent für jeden endlich-dimensionalen ρ_g-stabilen Untervektorraum W von $K[G]$ ist. Die Zerlegung ist eindeutig.

Beweis. Induktiv konstruieren wir eine Kette von endlich-dimensionalen Untervektorräumen

$$W_1 \subset W_2 \subset \cdots \subset W_n \subset \cdots$$

von $K[G]$, wobei $\rho_g(W_n) \subset W_n$ für alle $g \in G$ und $K[G] = \bigcup_{n\in\mathbb{N}} W_n$ gilt. Da $K[G]$ als K-Algebra endlich erzeugt ist, besitzt $K[G]$ eine abzählbare

Basis $\{w_i \mid i \in \mathbb{N}\}$ als K-Vektorraum. Der von w_1 erzeugte Untervektorraum von $K[G]$ liegt nach Satz 3.9 (angewandt auf Rechts- statt auf Linkstranslationen) in einem endlich-dimensionalen Untervektorraum W_1 von $K[G]$, der stabil unter allen Rechtstranslationen ρ_g ist, d. h. es gilt $\rho_g(W_1) \subset W_1$ für alle $g \in G$.
Analog liegt beim Induktionsschluss von n nach $n+1$ der von W_n und w_{n+1} erzeugte Untervektorraum von $K[G]$ in einem endlich-dimensionalen Untervektorraum W_{n+1} von $K[G]$, der stabil unter allen ρ_g mit $g \in G$ ist. Jedes $f \in K[G]$ ist eine endliche Linearkombination von endlich vielen w_i. Hieraus folgt $f \in W_n$ für ein $n \in \mathbb{N}$. Also ist $K[G] = \bigcup_{n\in\mathbb{N}} W_n$. Nach 4.3 besitzt $(\rho_g)|_{W_n}$ eine Jordanzerlegung $\rho_g|_{W_n} = (\rho_g|_{W_n})_{\mathrm{s}} \circ (\rho_g|_{W_n})_{\mathrm{u}}$ für jedes $n \in \mathbb{N}$ und jedes $g \in G$, die nach 4.3 kompatibel mit der Jordanzerlegung von $\rho_g|_{W_{n-1}}$ ist.
Sei nun $g \in G$ vorgegeben, und sei W ein ρ_g-stabiler Untervektorraum von $K[G]$ mit einer endlichen Basis $\mathcal{B}$. Dann ist jedes $f \in \mathcal{B}$ in einem W_n enthalten und also ist $\mathcal{B} \subset W_m$ für ein $m \in \mathbb{N}$. Es folgt $W \subset W_m$ und mit 4.3 die Behauptung. □

4.6 Jordanzerlegung in G

Sei K ein algebraisch abgeschlossener Körper, und sei G eine lineare algebraische Gruppe über K. Für jedes $g \in G$ sei $\rho_g = (\rho_g)_{\mathrm{s}} \circ (\rho_g)_{\mathrm{u}}$ die Jordanzerlegung der Rechtstranslation $\rho_g \colon K[G] \to K[G]$ wie in 4.5 beschrieben.

Satz (i) *Zu jedem $g \in G$ gibt es eindeutig bestimmte Elemente g_{s} und $g_{\mathrm{u}} \in G$ mit den Eigenschaften $(\rho_g)_{\mathrm{s}} = \rho_{g_{\mathrm{s}}}$ und $(\rho_g)_{\mathrm{u}} = \rho_{g_{\mathrm{u}}}$ sowie $g = g_{\mathrm{s}}g_{\mathrm{u}} = g_{\mathrm{u}}g_{\mathrm{s}}$.*

(ii) *Ist $\alpha \colon G \to G'$ ein Homomorphismus von algebraischen Gruppen, so ist $\alpha(g_{\mathrm{s}}) = \alpha(g)_{\mathrm{s}}$ und $\alpha(g_{\mathrm{u}}) = \alpha(g)_{\mathrm{u}}$ für jedes $g \in G$.*

(iii) *Ist $G = \mathrm{GL}_n(K)$, so ist g_{s} der halbeinfache und g_{u} der unipotente Anteil von $g \in G$ wie in Satz 4.4.*

Beweis. (i) Sei $\mu \colon K[G] \otimes_K K[G] \to K[G]$ die Multiplikation in $K[G]$. Da ρ_g ein K-Algebrahomomorphismus ist, gilt $\mu \circ (\rho_g \otimes \rho_g) = \rho_g \circ \mu$, und also ist das folgende Diagramm kommutativ.

$$\begin{array}{ccc} K[G] \otimes_K K[G] & \xrightarrow{\mu} & K[G] \\ {\scriptstyle \rho_g \otimes \rho_g}\downarrow & & \downarrow{\scriptstyle \rho_g} \\ K[G] \otimes_K K[G] & \xrightarrow{\mu} & K[G] \end{array}$$

Wie man mit Hilfe von 4.3, 4.2 nachprüft, erhält man hieraus ein kommutatives Diagramm

$$\begin{array}{ccc} K[G] \otimes_K K[G] & \xrightarrow{\mu} & K[G] \\ \downarrow{\scriptstyle (\rho_g)_s \otimes (\rho_g)_s} & & \downarrow{\scriptstyle (\rho_g)_s} \\ K[G] \otimes_K K[G] & \xrightarrow{\mu} & K[G]\,. \end{array}$$

Es ist also $(\rho_g)_s \colon K[G] \to K[G]\,,\ f \mapsto (\rho_g)_s(f)$ ein K-Algebrahomomorphismus, was einen K-Algebrahomomorphismus

$$\varphi \colon K[G] \to K\,,\ f \mapsto ((\rho_g)_s(f))(e)\,,$$

ergibt. Es gibt also einen Punkt $g_s \in G$ so, dass $f(g_s) = \varphi(f)$ für alle $f \in K[G]$ gilt, vgl. Aufgabe 15. Es ist also

$$\boxed{f(g_s) = ((\rho_g)_s(f))(e) \quad \forall\, f \in K[G]}\,.$$

Da ρ_g ein Automorphismus ist, der mit allen Linkstranslationen

$$\lambda_x \colon K[G] \to K[G]\,,\ f \mapsto \begin{cases} G \to K, \\ y \mapsto f(x^{-1}y)\,, \end{cases}$$

kommutiert, folgt aus 4.2 (i), dass $(\rho_g)_s$ mit λ_x kommutiert für jedes $x \in G$. Für alle $f \in K[G]$ und $x \in G$ folgt nun

$$\begin{aligned} ((\rho_g)_s(f))(x) &= ((\lambda_{x^{-1}} \circ (\rho_g)_s)(f))(e) \quad \text{nach Definition von } \lambda_{x^{-1}} \\ &= (((\rho_g)_s \circ \lambda_{x^{-1}})(f))(e) \quad \text{nach 4.2 (i)} \\ &= (\lambda_{x^{-1}}(f))(g_s) \quad \text{nach Definition von } g_s \\ &= f(xg_s) \quad \text{nach Definition von } \lambda_{x^{-1}} \\ &= (\rho_{g_s}(f))(x)\,. \end{aligned}$$

Es ist also $(\rho_g)_s = \rho_{g_s}$. Analog zeigt man die Existenz von $\rho_{g_u} \in G$ mit $(\rho_g)_u = \rho_{g_u}$. Da $\rho \colon G \to \mathrm{GL}(K[G])$ ein injektiver Gruppenhomomorphismus ist (vgl. 3.10), folgt nun (i) mit Hilfe der Jordanzerlegung von ρ_g aus 4.5.

(ii) $\alpha \colon G \to G'$ spaltet in zwei Morphismen $G \twoheadrightarrow \alpha(G) \hookrightarrow G'$. Da $\alpha(G)$ nach Satz 3.8 (ii) abgeschlossen in G' ist, genügt es, die zwei Fälle „α surjektiv“ und „α injektiv“ abzuhandeln.
Ist α surjektiv, so ist $\alpha^* \colon K[G'] \to K[G]$ injektiv (folgt aus 2.9) und

$K[G']$ kann als Untervektorraum von $K[G]$, der stabil unter allen ρ_g mit $g \in G$ ist, aufgefasst werden. Es gilt $\rho_g|_{K[G']} = \rho_{\alpha(g)}$, und mit 4.3 folgt die Behauptung.
Ist α injektiv, so kann G als abgeschlossene Untergruppe von G' aufgefasst werden. Sei $I := \mathfrak{I}_{G'}(G) = \{f \in K[G'] \mid f(x) = 0 \,\forall\, x \in G\}$ das Verschwindungsideal von G (vgl. 2.7.4). Dann ist $K[G] = K[G']/I$. Ferner gilt

$$G = \{x \in G' \mid \rho_x(I) \subset I\},$$

denn: Sei $x \in G$. Dann ist $(\rho_x(f))(y) = f(yx) = 0$ für alle $y \in G$ und $f \in I$ und also $\rho_x(f) \in I$ für alle $f \in I$. Sei umgekehrt $\rho_x(f) \subset I$ für ein $x \in G'$. Dann gilt $(\rho_x(f))(e) = 0$ für alle $f \in I$ und also $f(x) = 0$ für alle $f \in I$. Es folgt $x \in \mathfrak{V}_{G'}(\mathfrak{I}_{G'}(G)) \underset{\text{Aufg17}}{=} G$.
Sei nun $g \in G$ und $g = g_\mathrm{s} g_\mathrm{u}$ mit $g_\mathrm{s}, g_\mathrm{u} \in G'$ die Jordanzerlegung von g in G'. Dann wird I durch $\rho_{g_\mathrm{s}} = (\rho_g)_\mathrm{s}$ und $\rho_{g_\mathrm{u}} = (\rho_g)_\mathrm{u}$ stabilisiert, und daher sind $g_\mathrm{s}, g_\mathrm{u}$ in G.

(iii) Sei $G = \mathrm{GL}_n(K)$. Identifiziere jedes $x \in G$ mit der Standardabbildung $K^n \to K^n$, $v \mapsto xv$. Für $g \in G$ zeigen wir, dass es eine injektive K-lineare Abbildung $\widetilde{\varphi}\colon K^n \to K[G]$ gibt so, dass

$$\boxed{g_\mathrm{s} = \widetilde{\varphi}^{-1} \circ (\rho_g)_\mathrm{s} \circ \widetilde{\varphi}}$$

gilt. Da $(\rho_g)_\mathrm{s}|_{\mathrm{bild}(\widetilde{\varphi})}$ nach 4.5 halbeinfach ist, ist auch g_s halbeinfach. Sei $\varphi \neq 0$ in $\mathrm{Hom}_K(K^n, K)$. Dann ist

$$\widetilde{\varphi}\colon K^n \to K[G],\ v \mapsto \begin{cases} G \to K, \\ x \mapsto \varphi(xv), \end{cases}$$

injektiv, und es gilt $(\widetilde{\varphi}(g_\mathrm{s} v))(x) = \varphi(x g_\mathrm{s} v)$ sowie $(\rho_{g_\mathrm{s}}(\widetilde{\varphi}(v)))(x) = (\widetilde{\varphi}(v))(x g_\mathrm{s}) = \varphi(x g_\mathrm{s} v)$ für jedes $x \in G$. Es folgt

$$\widetilde{\varphi} \circ g_\mathrm{s} = \rho_{g_\mathrm{s}} \circ \widetilde{\varphi} = (\rho_g)_\mathrm{s} \circ \widetilde{\varphi}.$$

Analog ist $g_\mathrm{u} = \widetilde{\varphi}^{-1} \circ (\rho_g)_\mathrm{u} \circ \widetilde{\varphi}$ und also g_u unipotent. Aus den Eindeutigkeitsaussagen in (i) und 4.4 folgt nun (iii). □

4.7 Unipotente Gruppen

Sei K ein Körper. Eine Untergruppe U von $\mathrm{GL}_n(K)$ heißt *unipotent*, falls jedes Element aus U unipotent, d. h. von der Form $E_n + a$ mit einer nilpotenten Matrix $a \in \mathrm{M}_{n\times n}(K)$ ist. Hierbei ist $E_n := 1_{\mathrm{M}_{n\times n}(K)}$ die $n \times n$-Einheitsmatrix.

Beispiel

$$\mathrm{U}_n(K) := \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right\} \subset \mathrm{GL}_n(K)$$

ist eine unipotente Gruppe.

Beweis. Betrachte in $\mathrm{M}_{n\times n}(K)$ die Unteralgebra aller oberen Dreiecksmatrizen und darin das Ideal

$$\mathcal{N} := \left\{ \begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix} \in \mathrm{M}_{n\times n}(K) \right\} .$$

Dann ist $\mathcal{N}^n = (0)$ und also $\mathrm{U}_n(K) = E_n + \mathcal{N}$. □

Sei nun K algebraisch abgeschlossen, und sei G eine lineare algebraische Gruppe über K. Dann hat jedes $g \in G$ nach 4.6 eine Jordanzerlegung $g = g_\mathrm{s} g_\mathrm{u}$ mit einem *halbeinfachen Element* $g_\mathrm{s} \in G$ und einem *unipotenten Element* $g_\mathrm{u} \in G$. Die Menge

$$\boxed{G_\mathrm{u} := \{g \in G \mid g = g_\mathrm{u}\}}$$

ist abgeschlossen in G. Dies folgt aus 3.10 und 4.6 (ii), weil für eine unipotente Matrix $x \in \mathrm{GL}_n(K)$ stets $(x - E_n)^n = 0$ gilt.

Definition
Eine Untergruppe U einer linearen algebraischen Gruppe heißt *unipotent*, wenn jedes Element aus U unipotent ist.

Warnung
Halbeinfache algebraische Gruppen sind **nicht** analog definiert.

Bemerkung
Falls K algebraisch abgeschlossen ist, kann man zeigen, dass jede unipotente Untergruppe von $\mathrm{GL}_n(K)$ konjugiert zu einer Untergruppe von $\mathrm{U}_n(K)$ ist.

4.8 Übungsaufgaben 31–34

Seien K ein Körper, $\overline{K}$ ein algebraischer Abschluss von K und W ein K-Vektorraum der Dimension $n < \infty$.
Für einen Endomorphismus $\sigma : W \to W$ sei $p_\sigma := \det(\sigma - X \cdot \mathrm{id})$ das *charakteristische Polynom* von σ.

Aufgabe 31
Sei $\sigma \in \mathrm{End}_K(W)$. Jedes Polynom $f = a_m X^m + \cdots + a_1 X + a_0 \in K[X]$ definiert einen Endomorphismus $f(\sigma) = a_m \sigma^m + \cdots + a_1 \sigma + a_0 \,\mathrm{id} \in \mathrm{End}_K(W)$. Man zeige:

Ist $\lambda \in \overline{K}$ ein Eigenwert von σ, so ist $f(\lambda) \in \overline{K}$ ein Eigenwert von $f(\sigma)$ für jedes Polynom $f \in K[X]$.

Aufgabe 32
Man zeige, dass die folgenden Bedingungen für $\sigma \in \mathrm{End}_K(W)$ äquivalent sind:

(i) σ ist nilpotent.

(ii) $\sigma^m = 0$ für ein $m \in \mathbb{N}$ mit $m \leqslant n$.

(iii) Alle Eigenwerte von σ in $\overline{K}$ sind 0.

(iv) $p_\sigma = \pm X^n$.

Aufgabe 33
Man zeige, dass ein Endomorphismus $\sigma \in \mathrm{End}_K(W)$ genau dann unipotent ist, wenn alle Eigenwerte von σ in $\overline{K}$ gleich 1 sind.

Aufgabe 34
Für $\sigma, \tau \in \mathrm{End}_K(W)$ gelte $\sigma \circ \tau = \tau \circ \sigma$. Man zeige:

(a) σ, τ nilpotent $\Longrightarrow$ $\sigma + \tau$ nilpotent,

(b) σ, τ diagonalisierbar $\Longrightarrow$ $\sigma + \tau$ diagonalisierbar,

(c) σ, τ halbeinfach $\Longrightarrow$ $\sigma + \tau$ halbeinfach.

5 Kommutative algebraische Gruppen

Sei K ein algebraisch abgeschlossener Körper.

5.1 Strukturtheorem

Sei G eine kommutative lineare algebraische Gruppe. Dann gelten:

(i) *Die Mengen $G_{\mathrm{s}} := \{g \in G \mid g = g_{\mathrm{s}}\}$ und $G_{\mathrm{u}} := \{g \in G \mid g = g_{\mathrm{u}}\}$ sind abgeschlossene Untergruppen von G.*

(ii) *Die Produktabbildung $\mu\colon G_{\mathrm{s}} \times G_{\mathrm{u}} \to G$ ist ein Isomorphismus von algebraischen Gruppen.*

(iii) *Ist G zusammenhängend, so sind G_{s} und G_{u} zusammenhängend.*

Beweis. Nach Satz 3.10 und Satz 4.6 können wir annehmen, dass G eine abgeschlossene Untergruppe von $\mathrm{GL}_n(K)$ mit einem $n \in \mathbb{N}$ ist.

(1) G_{s} ist eine Untergruppe von G, denn seien $x, y \in G_{\mathrm{s}}$, dann gibt es nach 4.4 und 4.1 ein $g \in G$ so, dass gxg^{-1} und gyg^{-1} Diagonalmatrizen sind. Dann ist auch $gxyg^{-1} = gyg^{-1}gxg^{-1}$ eine Diagonalmatrix. Es ist $gx^{-1}g^{-1} = (gxg^{-1})^{-1}$ eine Diagonalmatrix und also $x^{-1} \in G_{\mathrm{s}}$. Ferner gilt $E_n \in G_{\mathrm{s}}$ für die Einheitsmatrix E_n aus $\mathrm{GL}_n(K)$.

(2) G_{u} ist eine Untergruppe von G, denn seien $x, y \in G_{\mathrm{u}}$. Dann gilt $x = E_n + a$ und $y = E_n + b$ mit nilpotenten Matrizen $a, b \in \mathrm{M}_{n\times n}(K)$ und also $xy = E_n + b + a + ab$. Es ist ab nilpotent, da $xy = yx$ und also $ab = ba$ gilt. Daher ist $b + a + ab$ nilpotent, und es folgt $xy \in G_{\mathrm{u}}$. Es ist $x^{-1} = E_n - a + a^2 - a^3 + \cdots$ und also $x^{-1} \in G_{\mathrm{u}}$. Ferner gilt $E_n \in G_{\mathrm{u}}$.

(3) G_{u} ist abgeschlossen in G nach 4.7.

(4) Sei $\mathrm{D}_n(K)$ die Gruppe der Diagonalmatrizen und $\Delta_n(K)$ die Gruppe der oberen Dreiecksmatrizen in $\mathrm{GL}_n(K)$. Diese Gruppen sind abgeschlossen in $\mathrm{GL}_n(K)$ nach 0.1. Da G kommutativ und K algebraisch abgeschlossen ist, kann G nach Aufgabe 35 simultan trigonalisiert werden. Es gibt also ein $z \in \mathrm{GL}_n(K)$ so, dass G vermöge

$$G \hookrightarrow \Delta_n(K),\ g \mapsto zgz^{-1},$$

in $\Delta_n(K)$ eingebettet werden kann. Die Jordanzerlegung wird dabei nach 4.6 (ii) respektiert. Sei also ohne Einschränkung $G \subset \Delta_n(K)$ (dies wird in (5) gebraucht).

Nach 4.1 kann G_s simultan diagonalisiert werden. Es gibt also ein $x \in \mathrm{GL}_n(K)$ so, dass G_s vermöge $G_\mathrm{s} \hookrightarrow \mathrm{D}_n(K)\,,\ g_\mathrm{s} \mapsto x g_\mathrm{s} x^{-1}$, in $\mathrm{D}_n(K)$ eingebettet werden kann. Für jedes $g \in G$ gilt dann

$$g \underset{4.6}{=} \underbrace{x g_\mathrm{s} x^{-1}}_{\in \mathrm{D}_n(K)} \cdot \underbrace{g_\mathrm{u}}_{\in \Delta_n(K)} \in \Delta_n(K)\,.$$

Sei also ohne Einschränkung $G \subset \Delta_n(K)$ und $G_\mathrm{s} = G \cap \mathrm{D}_n(K)$. Letzteres impliziert, dass G_s abgeschlossen in G ist. Mit (3) folgt nun offensichtlich, dass μ ein Morphismus von algebraischen Gruppen ist.

(5) $\mu^{-1}\colon G \to G_\mathrm{s} \times G_\mathrm{u}\,,\ g \mapsto (g_\mathrm{s}, g_\mathrm{u})$, ist ein Morphismus, denn die Eigenwerte von $g =: (a_{ij}) \in G \subset \Delta_n(K)$ sind nach (4) die Nullstellen des charakteristischen Polynoms

$$\det \begin{pmatrix} a_{11} - X & a_{12} & \dots & a_{1n} \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{n-1,n} \\ 0 & \dots & 0 & a_{nn} - X \end{pmatrix} = \prod_{i=1}^{n} (a_{ii} - X)\,,$$

bilden also gerade den Diagonalanteil von g. Da g_s dieselben Eigenwerte wie g hat (vgl. Beweis von 4.2) und $g_\mathrm{s} \in \mathrm{D}_n(K)$ nach (4) ist, folgt aus 4.2, dass g_s der Diagonalanteil von g ist. Daher ist die Projektion $\pi_\mathrm{s}\colon G \to G_\mathrm{s}\,,\ g \mapsto g_\mathrm{s}$, ein Morphismus und ebenso die Projektion $\pi_\mathrm{u}\colon G \to G_\mathrm{u}\,,\ g \mapsto g_\mathrm{s}^{-1} g = g_\mathrm{u}$.

(6) Ist G zusammenhängend (d. h. irreduzibel nach 3.5), so sind G_s als Bild von π_s und G_u als Bild von π_u irreduzibel nach 2.4 (c), da π_s und π_u nach (5) stetig sind. □

5.2 Dimension einer irreduziblen affinen Varietät

Sei V eine affine algebraische Varietät über K. Dann gilt:

$$\boxed{V \text{ irreduzibel}} \quad \underset{2.3}{\Longleftrightarrow} \quad \boxed{K[V] \text{ Integritätsring}}\,.$$

Ist V irreduzibel, so ist die *Dimension* von V der Transzendenzgrad des Quotientenkörpers $K(V)$. Wir schreiben $\dim V$ dafür.
Ist $K[V] = K[x_1, \dots, x_n]$, so ist $\dim V$ die maximale Anzahl algebraisch unabhängiger Elemente unter den x_i (vgl. 1.2, 1.8 und 2.6).

Beispiele (1) Die multiplikative Gruppe $G = \mathbb{G}_{\mathrm{m}}(K)$ ist eindimensional, denn es ist $K[G] = K[X, X^{-1}]$, und G ist diagonalisierbar nach 0.1.8.

(2) Auch die additive Gruppe $G = \mathbb{G}_{\mathrm{a}}(K)$ ist eindimensional, denn es ist $K[G] = K[X]$, und G ist unipotent nach 0.2.1.

Lemma
Seien V_1, V_2 affine irreduzible algebraische Varietäten. Dann gelten:

(a) $\dim(V_1 \times V_2) = \dim V_1 + \dim V_2$.

(b) *Ist V_1 eine abgeschlossene echte Untervarietät von V_2, so gilt* $\dim V_1 < \dim V_2$.

Beweis. (a) Sind $\{x_1, \ldots, x_m\}$ und $\{y_1, \ldots, y_n\}$ maximale Mengen von algebraisch unabhängigen Elementen in $K[V_1]$ bzw. $K[V_2]$, so ist

$$\{x_1 \otimes 1, \ldots, x_m \otimes 1, 1 \otimes y_1, \ldots, 1 \otimes y_n\}$$

eine solche Menge in $K[V_1] \otimes_K K[V_2] \underset{2.12}{=} K[V_1 \times V_2]$.

(b) Es ist $K[V_1] = K[V_2]/\mathfrak{p}$ mit einem Primideal $\mathfrak{p} \neq 0$ (vgl. 2.7.4 und 2.9). Sei $\dim V_1 = d$, und seien $\overline{x_1} = x_1 \bmod \mathfrak{p}, \ldots, \overline{x_d} = x_d \bmod \mathfrak{p}$ algebraisch unabhängig in $K[V_1]$. Dann sind $x_1, \ldots, x_d$ algebraisch unabhängig in $K[V_2]$. Es folgt $d \leqslant \dim V_2$.
Angenommen $d = \dim V_2$. Sei $a \in \mathfrak{p}$ und $a \neq 0$. Da $\dim V_2 = d$ ist, gibt es ein Polynom $f \in K[X_0, \ldots, X_d]$ mit $f \neq 0$ und $f(a, x_1, \ldots, x_d) = 0$. Da $a \neq 0$ ist, darf angenommen werden, dass f nicht von X_0 geteilt wird. Dann gilt:

$$g(X_1, \ldots, X_d) := f(0, X_1, \ldots, X_d) \neq 0,$$

aber $g(\overline{x_1}, \ldots, \overline{x_d}) = f(0, \overline{x_1}, \ldots, \overline{x_d}) \underset{a \in \mathfrak{p}}{=} 0$ im Widerspruch dazu, dass $\overline{x_1}, \ldots, \overline{x_d}$ algebraisch unabhängig sind. □

Bemerkung
Mit Hilfe des Lemmas und der Tatsache, dass die Kommutatorgruppe $[G, G]$ einer zusammenhängenden linearen algebraischen Gruppe G zusammenhängend ist, zeigt man Folgendes:
Jede eindimensionale zusammenhängende lineare algebraische Gruppe ist kommutativ, und es gilt entweder $G = G_{\mathrm{s}}$ oder $G = G_{\mathrm{u}}$. Mit Hilfe der Theorie der „diagonalisierbaren Gruppen“ und der „Vektorgruppen“ zeigt man dann weiter, dass sogar entweder $G \simeq \mathbb{G}_{\mathrm{m}}(K)$ oder $G = \mathbb{G}_{\mathrm{a}}(K)$ gilt.

5.3 Charaktere

Sei K algebraisch abgeschlossen, und sei G eine lineare algebraische Gruppe über K. Ein *Charakter von G* ist ein Morphismus von algebraischen Gruppen $\chi\colon G \to \mathbb{G}_{\mathrm{m}}(K)$. Das Produkt zweier Charaktere χ, ψ ist definiert durch

$$(\chi\psi)(x) = \chi(x)\psi(x) \text{ für alle } x \in G\,.$$

Die Charaktere von G bilden eine abelsche Gruppe $X^*(G)$, genannt *Charaktergruppe von G*.
Es ist $X^*(G) \subset K[G] \overset{2.7}{=} \mathrm{Mor}(G, K)$. Ist F ein Teilkörper von K, und ist G über F definiert, so bilden die über F definierten Charaktere von G eine Untergruppe von $X^*(G)$.

Lemma
Sei G irgendeine Gruppe, und sei L ein Körper, so bilden die Homomorphismen $G \to L^*$ eine linear unabhängige Teilmenge der Menge aller Funktionen $G \to L$.

Beweis. Algebra 18.4. □

Beispiel
Sei $G = \mathrm{D}_n(K)$ die Gruppe der Diagonalmatrizen in $\mathrm{GL}_n(K)$ (wie in 0.1.4). Dann ist G kommutativ, und man hat für jedes $i = 1, \ldots, n$ einen Charakter

$$\chi_i\colon G \to K^*,\ \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \mapsto a_i\,.$$

Es ist $K[G] = K[\chi_1, \ldots, \chi_n, \chi_1^{-1}, \ldots, \chi_n^{-1}]$ mit

$$\chi_i^{-1}\colon G \to K^*,\ \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \mapsto a_i^{-1}\,.$$

Nach dem Lemma sind die Monome $\chi_1^{m_1} \cdot \ldots \cdot \chi_n^{m_n}$ linear unabhängig in $K[G]$ für alle Tupel $(m_1, \ldots, m_n) \in \mathbb{Z}^n$ und bilden daher eine Basis von $K[G]$ als K-Vektorraum. Da insbesondere jeder Charakter ein solches Monom ist, folgt

$$\boxed{X^*(G) \simeq \mathbb{Z}^n}\,.$$

5.4 Diagonalisierbare Gruppen

Sei K algebraisch abgeschlossen, und sei G eine lineare algebraische Gruppe über K. Dann heißt G *diagonalisierbar*, wenn G isomorph zu einer abgeschlossenen Untergruppe von $\mathrm{D}_n(K)$ für ein $n \in \mathbb{N}$ ist. Eine diagonalisierbare Gruppe ist offensichtlich kommutativ und besteht aus halbeinfachen Elementen.

Satz
Äquivalent sind:

(a) *G ist diagonalisierbar.*

(b) *Die Charaktergruppe $X^*(G)$ ist eine endlich erzeugte abelsche Gruppe, und die Elemente von $X^*(G)$ bilden eine Basis von $K[G]$ als K-Vektorraum.*

(c) *Ist $\alpha\colon G \to \mathrm{GL}_n(K)$ ein Morphismus, so ist $\alpha(G)$ konjugiert zu einer abgeschlossenen Untergruppe von $\mathrm{D}_n(K)$.*

Beweis. (a) $\Longrightarrow$ (b): Identifiziere G mit dem Bild von G in $\mathrm{D}_n(K) =: \mathbb{D}_n$. Die Inklusion $\iota\colon G \hookrightarrow \mathbb{D}_n$ induziert dann nach 2.7.4 einen surjektiven K-Algebrahomomorphismus $\iota^*\colon K[\mathbb{D}_n] \to K[G]$, $f \mapsto f|_G$. Dann wird $K[G]$ nach Beispiel 5.3 erzeugt von den Restriktionen von Charakteren von $\mathbb{D}_n$. Mit Lemma 5.3 folgt, dass $X^*(G)$ eine Basis von $K[G]$ ist. Also ist der von ι induzierte Homomorphismus $X^*(\mathbb{D}_n) \to X^*(G)$, $\chi \mapsto \chi|_G$, surjektiv. Da $X^*(\mathbb{D}_n) \simeq \mathbb{Z}^n$ nach Beispiel 5.3 gilt, folgt, dass $X^*(G)$ endlich erzeugt und abelsch ist.

(b) $\Longrightarrow$ (c): $K[G]$ wird von endlich vielen Charakteren $\chi_1, \ldots, \chi_d$ als K-Algebra erzeugt. Definiere

$$\varphi\colon G \to \underbrace{\mathbb{G}_\mathrm{m} \times \cdots \times \mathbb{G}_\mathrm{m}}_{d \text{ Kopien}} \ (\simeq \mathbb{D}_d)$$

durch $\varphi(x) = (\chi_1(x), \ldots, \chi_d(x))$ für $x \in G$. Dann ist φ ein Morphismus von algebraischen Gruppen mit trivialem Kern, da $\chi_1, \ldots, \chi_d$ Algebraerzeugende von $K[G]$ sind. Also ist G kommutativ und besteht aus halbeinfachen Elementen. Gleiches gilt für $\alpha(G) \subset \mathrm{GL}_n(K)$ nach 4.6 (ii). Nach 4.1 (simultane Diagonalisierbarkeit) gibt es ein $x \in \mathrm{GL}_n(K)$ so, dass $x\,\alpha(G)x^{-1} \subset \mathbb{D}_n$. Da $\alpha(G)$ nach 3.8 abgeschlossen in $\mathrm{GL}_n(K)$ ist, folgt (c).

(c) $\Longrightarrow$ (a): Nach Satz 3.10 gibt es eine Einbettung $G \hookrightarrow \mathrm{GL}_n(K)$ mit einem $n \in \mathbb{N}$. Wende hierauf (c) an, dann folgt (a). □

Korollar
Sei G diagonalisierbar. Dann gelten:

(i) *Jede abgeschlossene Untergruppe H von G ist diagonalisierbar.*

(ii) *Ist $\alpha\colon G \to G'$ ein Morphismus von algebraischen Gruppen, so ist $\alpha(G)$ diagonalisierbar.*

Beweis. (i) Der von der Inklusion $\iota\colon H \hookrightarrow G$ induzierte K-Algebrahomomorphismus $\iota^*\colon K[G] \to K[H]\,,\ f \mapsto f|_H$, ist surjektiv nach 2.7.4. Da $K[G]$ nach (a) $\Longrightarrow$ (b) von $X^*(G)$ erzeugt wird, wird $K[H]$ von den Restriktionen von Charakteren erzeugt, und diese sind linear unabhängig nach Lemma 5.3. Ferner folgt, dass mit $X^*(G)$ auch $X^*(H)$ endlich erzeugt und abelsch ist. Nach (b) $\Longrightarrow$ (a) folgt nun, dass H diagonalisierbar ist.

(ii) Nach Satz 3.10 lässt sich G' in $\mathrm{GL}_n(K)$ für ein $n \in \mathbb{N}$ einbetten. Nach (a) $\Longrightarrow$ (c) ist dann $\alpha(G)$ konjugiert zu einer abgeschlossenen Untergruppe von $\mathrm{D}_n(K)$ und also $\alpha(G)$ diagonalisierbar. □

5.5 Charaktere zusammenhängender Gruppen

Satz
Sei K algebraisch abgeschlossen, und sei G eine zusammenhängende lineare algebraische Gruppe. Dann ist die Charaktergruppe $X^*(G)$ torsionsfrei, d. h. $X^*(G)$ besitzt keine Elemente endlicher Ordnung außer 1.

Beweis. Sei $\chi\colon G \to \mathbb{G}_{\mathrm{m}}(K) =: \mathbb{G}_{\mathrm{m}}$ ein Charakter. Dann ist $\chi(G)$ zusammenhängend nach 2.4 (c). Die einzigen zusammenhängenden Untergruppen von $\mathbb{G}_{\mathrm{m}}$ sind $\{1\}$ und $\mathbb{G}_{\mathrm{m}}$. Es folgt $\chi^n \neq 1$ für alle $n > 1$. □

5.6 Tori

Definition
Sei K algebraisch abgeschlossen. Eine lineare algebraische Gruppe G heißt *algebraischer Torus* oder kurz *Torus*, falls $G \simeq \mathrm{D}_n(K)$ für ein $n \in \mathbb{N}$ gilt. Hierbei bezeichnet $\mathrm{D}_n(K)$ wie bisher die Untergruppe der Diagonalmatrizen in $\mathrm{GL}_n(K)$.

Satz
Für eine lineare algebraische Gruppe T sind äquivalent:

(a) *T ist ein n-dimensionaler Torus.*

(b) *T ist zusammenhängend und diagonalisierbar, und es gilt* $\dim T = n$.

(c) *T ist diagonalisierbar, und es ist $X^*(T) \simeq \mathbb{Z}^n$.*

Beweis. (a) $\Longrightarrow$ (b): Da $\mathrm{D}_n(K) \simeq \mathrm{GL}_1(K) \times \cdots \times \mathrm{GL}_1(K)$ mit n Kopien gilt und $\mathrm{GL}_1(K)$ nach 3.4.3 irreduzibel ist, ist auch $\mathrm{D}_n(K)$ irreduzibel nach 2.12 iii). Ferner folgt $\dim_K \mathrm{D}_n(K) = n$ nach Beispiel 5.3.

(b) $\Longrightarrow$ (c): Da T diagonalisierbar ist, ist $X^*(T)$ eine endlich erzeugte abelsche Gruppe, die eine Basis von $K[G]$ als K-Vektorraum bildet, vgl. Satz 5.4. Nach 5.5 ist $X^*(T)$ torsionsfrei, und nach dem Hauptsatz für endlich erzeugte abelsche Gruppen (Algebra 10.12) folgt $X^*(T) \simeq \mathbb{Z}^n$ mit $n = \mathrm{rang}(X^*(T)) = \dim T$.

(c) $\Longrightarrow$ (a): Sei $\chi_1, \ldots, \chi_n$ eine $\mathbb{Z}$-Basis von $X^*(T)$. Dann ist

$$K[T] \simeq K[\chi_1, \ldots, \chi_n, \chi_1^{-1}, \ldots, \chi_n^{-1}]$$

nach 5.4 und also $\dim T = n$. Da T diagonalisierbar ist, ist T isomorph zu einer abgeschlossenen Untergruppe von $\mathrm{D}_n(K)$. Es folgt $T \simeq \mathrm{D}_n(K)$ nach 5.2 (b), da $\dim T = \dim \mathrm{D}_n(K)$. □

5.7 Strukturtheorem für diagonalisierbare Gruppen

Seien K algebraisch abgeschlossen, G eine lineare algebraische Gruppe und G^0 die Zusammenhangskomponente von $e \in G$ wie in 3.5.

Satz
Ist G diagonalisierbar, so ist $G = H \times G^0$ mit einer endlichen Gruppe H, und G^0 ist ein Torus. Falls $\mathrm{char}(K) = p > 0$ ist, so gilt $p \nmid |H|$.

Beweis. Man kann annehmen, dass G eine abgeschlossene Untergruppe von $\mathrm{D}_m(K) =: \mathbb{D}_m$ mit einem $m \in \mathbb{N}$ ist, vgl. 5.4 und 3.10. Nach Korollar 5.4 (i) ist G^0 ein Torus. Die Inklusion $G^0 \hookrightarrow \mathbb{D}_m$ induziert wie im Beweis von Satz 5.4 einen surjektiven Gruppenhomomorphismus

$$\mathbb{Z}^m \underset{5.3}{\simeq} X^*(\mathbb{D}_m) \overset{\varphi}{\twoheadrightarrow} X^*(G^0) \underset{5.6}{\simeq} \mathbb{Z}^n$$

mit $n := \dim G^0$. Es folgt $X^*(\mathbb{D}_m) \simeq \ker\varphi \oplus X^*(G^0)$, weil $X^*(G^0)$ ein freier $\mathbb{Z}$-Modul ist. Also besitzt $X^*(\mathbb{D}_m)$ eine $\mathbb{Z}$-Basis $\chi_1, \ldots, \chi_m$ so, dass $\chi_i(x) = 1$ für alle $x \in G^0$ und für alle $i = 1, \ldots, m-n$ ist. Man hat also einen Isomorphismus

$$\mathbb{D}_m \xrightarrow{\sim} \mathbb{D}_m\,,\ x \mapsto \begin{pmatrix} \chi_1(x) & & 0 \\ & \ddots & \\ 0 & & \chi_m(x) \end{pmatrix},$$

bei dem für jedes $x \in G^0$ die ersten $m-n$ Diagonaleinträge gleich 1 sind.

Es folgt

$$\mathbb{D}_m = \mathbb{D}_{m-n} \times G^0 \quad \text{und}$$
$$G = H \times G^0 \quad \text{mit} \quad H = G \cap \mathbb{D}_{m-n}\,.$$

Nach 3.5 (2) ist $H \simeq G/G^0$ eine endliche Gruppe. Ferner ist die Multiplikation $H \times G^0 \to G$ ein Isomorphismus von algebraischen Gruppen. Da H endlich ist, besteht H aus Einheitswurzeln aus K.
Ist $\mathrm{char}(K) = p > 0$, so besitzt K aber keine p-te Einheitswurzel $\neq 1$ nach Algebra 17.1. □

5.8 Torsion in diagonalisierbaren Gruppen

Korollar
Sei K algebraisch abgeschlossen, und sei G diagonalisierbar. Dann ist die Torsionsuntergruppe G_{tors} von G dicht in G.

Beweis. Nach 5.7 ist

$$G \simeq H \times \underbrace{\mathbb{G}_{\mathrm{m}} \times \cdots \times \mathbb{G}_{\mathrm{m}}}_{\dim G^0 \text{ Kopien}}$$

mit einer endlichen Gruppe H und $\mathbb{G}_{\mathrm{m}} = K^*$. Es genügt also, die Behauptung für $G = \mathbb{G}_{\mathrm{m}}$ zu zeigen. In diesem Fall besteht G_{tors} aus allen Einheitswurzeln von K^*, also ist $|G_{\mathrm{tors}}| = \infty$, da K algebraisch abgeschlossen ist. Da $\dim G = 1$ ist, folgt $\overline{G_{\mathrm{tors}}} = \mathbb{G}_{\mathrm{m}}$ aus Lemma 5.2 (b). □

5.9 Rigidität diagonalisierbarer Gruppen

„Rigid“ heißt „starr“ und bedeutet „wenig Automorphismen“.

Sei K algebraisch abgeschlossen. Seien H, H' algebraische Gruppen mit den Eigenschaften

(1) H' enthält für jedes $m \in \mathbb{N}$ nur endlich viele Elemente der Ordnung m.

(2) H_{tors} ist dicht in H.

Diese sind erfüllt, wenn H und H' diagonalisierbar sind (nach Algebra 17.1 und 5.8) Sei V eine irreduzible Varietät, und sei $\alpha\colon V \times H \to H'$ ein Morphismus von Varietäten so, dass zusätzlich gilt:

(3) Für jedes $v \in V$ ist $\alpha_v\colon H \to H'$, $h \mapsto \alpha(v,h)$, ein Gruppenhomomorphismus.

Satz
Dann ist die Abbildung $V \to \mathrm{Mor}(H, H')\,,\ v \mapsto \alpha_v\,,$ *konstant.*

Beweis. Für $h \in H$ ist die Abbildung $\beta_h \colon V \to H'\,,\ v \mapsto \alpha(v,h)\,,$ ein Morphismus von Varietäten, da α ein solcher ist. Ist $\mathrm{ord}(h) < \infty\,,$ so ist $\beta_h(V)$ eine endliche Menge nach (1) und (3). Da mit V nach 2.4 (c) auch $\beta_h(V)$ irreduzibel ist, ist $\beta_h(V) = \{h'\}$ mit einem $h' \in H'$. Für $v, w \in V$ schickt

$$\gamma \colon H \to H',\ h \mapsto \underbrace{\alpha_v(h)}_{=\beta_h(v)}\underbrace{\alpha_w(h)^{-1}}_{=\beta_h(w)^{-1}},$$

jedes $h \in H$ mit $\mathrm{ord}(h) < \infty$ nach $e' = 1_{H'}$. Da mit $\{e'\}$ auch $\gamma^{-1}(e')$ abgeschlossen ist, folgt aus (2), dass $\gamma(h) = e'$ für alle $h \in H$ gilt. Es folgt $\alpha_v = \alpha_w$ für alle $v, w \in V$. □

5.10 Normalisator und Zentralisator

Sei G eine beliebige algebraische Gruppe. Dann operiert G per Konjugation

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

auf sich selbst, und α ist ein Morphismus. Für $x \in G$ sei

$$\boxed{\mathrm{Stab}(x) := \{g \in G \mid gxg^{-1} = x\}}$$

der *Stabilisator von* x, und für eine Untergruppe H von G seien

$$\boxed{\mathcal{Z}_G(H) := \bigcap_{h \in H} \mathrm{Stab}(h) = \{g \in G \mid ghg^{-1} = h\ \ \forall\, h \in H\}}$$

der *Zentralisator von* H *in* G und

$$\boxed{\mathcal{N}_G(H) := \{g \in G \mid gHg^{-1} = H\}}$$

der *Normalisator von* H *in* G.

Lemma
Ist H *eine abgeschlossene Untergruppe einer algebraischen Gruppe* G*, so sind* $\mathcal{N}_G(H)$ *und* $\mathrm{Stab}(h)$ *für alle* $h \in H$ *sowie* $\mathcal{Z}_G(H)$ *abgeschlossene Untergruppen von* G*. Ferner ist* $\mathcal{Z}_G(H)$ *Normalteiler von* $\mathcal{N}_G(H)$*.*

Beweis. Für jedes $h \in H$ ist $\alpha_h \colon G \to G\,,\ g \mapsto ghg^{-1}$, ein Morphismus, da α ein solcher ist. Da H und $\{h\}$ abgeschlossen in G sind, sind also auch $\alpha_h^{-1}(H) = \{g \in G \mid ghg^{-1} \in H\}$ und $\alpha_h^{-1}(\{h\}) = \mathrm{Stab}(h)$ abgeschlossen in G. Es folgt, dass $\mathcal{N}_G(H) = \bigcap\limits_{h\in H} \alpha_h^{-1}(H)$ und $\mathcal{Z}_G(H) = \bigcap\limits_{h\in H} \mathrm{Stab}(h)$ abgeschlossen in G sind.
Es sind $\mathrm{Stab}(h)$ und $\mathcal{N}_G(H)$ Untergruppen von G nach Algebra 2.2 und Algebra 2.10. Es ist dann auch $\mathcal{Z}_G(H)$ als Durchschnitt von Untergruppen wieder eine Untergruppe.
Für jedes $g \in \mathcal{N}_G(H)$ und jedes $z \in \mathcal{Z}_G(H)$ ist $gzg^{-1} \in \mathcal{Z}_G(H)$, denn für alle $h \in H$ gilt:

$$\begin{aligned}(gzg^{-1})h(gzg^{-1})^{-1} &= gz \underbrace{(g^{-1}hg)}_{\in H,\ \text{da } g\in\mathcal{N}_G(H)} z^{-1}g^{-1}\\ &= g(g^{-1}hg)g^{-1}, \quad \text{da } z \in \mathcal{Z}_G(H)\\ &= h\,.\end{aligned}$$

Es folgt, dass $\mathcal{Z}_G(H)$ Normalteiler in $\mathcal{N}_G(H)$ ist. □

Satz
Sei G eine lineare algebraische Gruppe über einem algebraisch abgeschlossenen Körper, und sei H eine diagonalisierbare Untergruppe von G. Dann gilt $\mathcal{N}_G(H)^0 = \mathcal{Z}_G(H)^0$, und die Faktorgruppe $\mathcal{N}_G(H)/\mathcal{Z}_G(H)$ ist endlich.

Beweis. H ist abgeschlossen in G. Wende 5.9 mit $V = \mathcal{N}_G(H)^0$ und

$$\alpha \colon V \times H \to H\,,\ (x,h) \mapsto xhx^{-1},$$

an. Dann ist $V \to \mathrm{Mor}(H,H)\,,\ x \mapsto \alpha_x\,,$ mit $\alpha_x(h) = xhx^{-1}$ für $h \in H\,,$ konstant. Also gilt $\alpha_x = \alpha_e$ für alle $x \in V$. Es folgt $x \in \mathcal{Z}_G(H)^0$ für alle $x \in V$. Umgekehrt gilt $\mathcal{Z}_G(H)^0 \subset \mathcal{N}_G(H)^0$, und also ist $\mathcal{Z}_G(H)^0 = \mathcal{N}_G(H)^0$. Hieraus und aus dem zweiten Noetherschen Isomorphiesatz (Algebra 1.6) folgt nun

$$\mathcal{N}_G(H)/\mathcal{Z}_G(H) \simeq (\mathcal{N}_G(H)/\mathcal{N}_G(H)^0)/(\mathcal{Z}_G(H)/\mathcal{Z}_G(H)^0)\,.$$

Dabei sind $\mathcal{N}_G(H)^0$ und $\mathcal{Z}_G(H)^0$ jeweils von endlichem Index nach 3.5, woraus die zweite Behauptung folgt. □

Beispiel
Sei $M \subset \mathrm{GL}_n(K)$ die Gruppe der monomialen Matrizen, das sind die $n \times n$-Matrizen, die in jeder Zeile und jeder Spalte genau einen Eintrag $\neq 0$ haben. Dann ist:

1) $M^0 = \mathrm{D}_n(K) =: \mathbb{D}_n$,

2) $M/M^0 \simeq S_n$ die symmetrische Gruppe, also $|M/M^0| = n!$,

3) $\mathcal{N}_{\mathrm{GL}_n(K)}(\mathbb{D}_n) = M$,

4) $\mathcal{Z}_{\mathrm{GL}_n(K)}(\mathbb{D}_n) = \mathbb{D}_n$,

und nach 3) und 4) gilt $\mathcal{N}_{\mathrm{GL}_n(K)}(\mathbb{D}_n)/\mathcal{Z}_{\mathrm{GL}_n(K)}(\mathbb{D}_n) \simeq S_n$
(vgl. auch [12], S. 73).

5.11 Bemerkung über auflösbare Gruppen

Sei G eine Gruppe mit neutralem Element e, und sei H eine Untergruppe von G. Dann heißt die Menge

$$[a, b] := ab\,a^{-1}b^{-1} \quad \text{mit} \quad a \in G\,,\, b \in H$$

der *Kommutator* von $a \in G$ und $b \in H$. Die von allen solchen Kommutatoren erzeugte Untergruppe von G wird als $[G, H]$ geschrieben. In G betrachte man die jeweils induktiv definierten Untergruppen

$$\mathcal{C}^0(G) = G\,,\ \ldots\,,\ \mathcal{C}^{i+1}(G) = [G, \mathcal{C}^i(G)] \ \text{ und}$$

$$\mathcal{D}^0(G) = G\,,\ \ldots\,,\ \mathcal{D}^{i+1}(G) = [\mathcal{D}^i(G), \mathcal{D}^i(G)]\,.$$

Die Gruppe G ist *nilpotent*, wenn es ein $m \in \mathbb{N}_0$ so gibt, dass $\mathcal{C}^m(G) = \{e\}$ gilt, und G ist *auflösbar*, wenn es ein $k \in \mathbb{N}_0$ so gibt, dass $\mathcal{D}^k(G) = \{e\}$ gilt. Für auflösbare (also nicht notwendig kommutative) Gruppen gilt folgender

Struktursatz
Sei G eine zusammenhängende auflösbare lineare algebraische Gruppe über einem algebraisch abgeschlossenen Körper. Dann gelten:

(i) *Die Gruppen $\mathcal{D}^i(G)$ und $\mathcal{C}^i(G)$ sind abgeschlossene, zusammenhängende Untergruppen und Normalteiler in G.*

(ii) *G_{u} ist abgeschlossener Normalteiler in G, der die Kommutatorgruppe $[G, G]$ enthält, und G_{u} ist zusammenhängend.*

(iii) *G/G_{u} ist ein Torus.*

(iv) *G ist nilpotent $\Longleftrightarrow$ G_{s} ist eine Untergruppe von G.*
In diesem Fall ist G_{s} abgeschlossen, und es ist $G = G_{\mathrm{s}} \times G_{\mathrm{u}}$.

(v) *Die maximalen Tori in G sind konjugiert unter $\bigcap\limits_{i \in \mathbb{N}_0} \mathcal{C}^i(G)$.*

(vi) *Ist T ein maximaler Torus in G, so ist $G = T \ltimes G_{\mathrm{u}}$ (d. h. G_{u} ist Normalteiler in G sowie $G = TG_{\mathrm{u}}$ und $T \cap G_{\mathrm{u}} = \{e\}$).*

Dabei ist ein Torus ein *maximaler Torus* in G, wenn er in G enthalten ist und wenn er in keinem anderen Untertorus von G echt enthalten ist. Ein Beweis des Struktursatzes steht z. B. in [5] 17.2 bis 17.4 und 19.

5.12 Übungsaufgaben 35–44

Aufgabe 35
Simultane Trigonalisierbarkeit:
Sei K ein algebraisch abgeschlossener Körper, und sei $S \subset \mathrm{M}_{n\times n}(K)$ eine Menge von paarweise vertauschbaren Matrizen. Man zeige, dass es eine Matrix $x \in \mathrm{GL}_n(K)$ derart gibt, dass xSx^{-1} aus oberen Dreiecksmatrizen besteht.

Aufgabe 36
Man zeige, dass jede nilpotente Gruppe auflösbar ist. (Vgl. 5.11 für die Definition von „nilpotent“ und „auflösbar“.)

Aufgabe 37
Sei K ein Körper, und sei $\mathrm{U}_n(K)$ die Gruppe der oberen Dreiecksmatrizen in $\mathrm{M}_{n\times n}(K)$, deren Diagonalelemente 1 sind. In der K-Algebra aller oberen $n \times n$-Dreiecksmatrizen sei $\mathcal{N}$ das zweiseitige Ideal der Matrizen, deren Diagonalelemente 0 sind. Sei E_n die Einheitsmatrix in $\mathrm{M}_{n\times n}(K)$.

Man zeige, dass $E_n + \mathcal{N}^i$ für $i \in \mathbb{N}$ ein Normalteiler in $\mathrm{U}_n(K)$ ist, und verifiziere die Kommutatorformel $[E_n + \mathcal{N}^i\,,\, E_n + \mathcal{N}^j\,] \subset E_n + \mathcal{N}^{i+j}$ für $i, j \in \mathbb{N}$. Man folgere hieraus, dass $\mathrm{U}_n(K)$ unipotent ist.

Aufgabe 38
Sei K ein Körper. Man zeige, dass die Gruppe $\Delta_n(K)$ der oberen Dreiecksmatrizen in $\mathrm{GL}_n(K)$ auflösbar ist.

Die folgenden sechs Aufgaben sind Extraaufgaben, die im Kurs 2001 als Vorbereitung zur Klausur dienten.

Aufgabe 39
Man ermittle, welche der folgenden Mengen algebraisch sind:

(a) $\{(z^3, z^2, z) \mid z \in \mathbb{C}\} \subset \mathbb{C}^3$

(b) $\mathbb{Q}(i) \subset \mathbb{C}$

Aufgabe 40
Sei R ein kommutativer Ring, und seien $\mathcal{I}, \mathcal{J}$ Ideale in R. Man beweise: $\mathrm{Rad}(\mathcal{I} + \mathcal{J}) = \mathrm{Rad}(\mathrm{Rad}(\mathcal{I}) + \mathrm{Rad}(\mathcal{J}))$.

Aufgabe 41
Man ermittle, welche der folgenden Ideale in $\mathbb{C}[X, Y]$ Verschwindungsideale von Teilmengen des $\mathbb{C}^2$ sind:

(a) $\mathcal{I}_1 = (X^2 + Y^2 - 2XY)$

(b) $\mathcal{I}_2 = (X^2 - Y^2 - 1)$

Aufgabe 42
Sei R ein kommutativer Ring. Man beweise: Zu $\mathfrak{p}_1$, $\mathfrak{p}_2 \in \operatorname{Spec}(R)$ mit $\mathfrak{p}_1 \neq \mathfrak{p}_2$ gibt es eine offene Menge $U \subset \operatorname{Spec}(R)$, die genau einen der beiden Punkte $\mathfrak{p}_1$ oder $\mathfrak{p}_2$ enthält.

Aufgabe 43
Sei K ein Körper. Man bestimme $\sigma, \tau \in \operatorname{End}(K^2)$ so, dass σ und τ nilpotent sind, aber $\sigma + \tau$ nicht nilpotent ist.

Aufgabe 44
Sei K ein algebraisch abgeschlossener Körper der Charakteristik 0. Für $x \in K \setminus \{0\}$ sei $H_x \subset \mathbb{G}_{\mathrm{a}}(K)$ die von x erzeugte Untergruppe. Man zeige, dass H_x keine lineare algebraische Gruppe ist, und bestimme den Abschluss $\overline{H_x}$ von H_x in $\mathbb{G}_{\mathrm{a}}(K)$.

6 Die Liealgebra einer linearen algebraischen Gruppe

6.1 Liealgebren

Sei K ein Körper.

1) Ein K-Vektorraum L zusammen mit einer bilinearen Abbildung

$$L \times L \to L\,,\ (x,y) \mapsto [xy]$$

heißt *Liealgebra*, wenn $[xx] = 0$ für alle $x \in L$ gilt und die „Jacobi-Identität“

$$[x[yz]] + [y[zx]] + [z[xy]] = 0$$

(als Ersatz für das Assoziativgesetz) für alle $x, y, z \in L$ erfüllt ist. (Man nennt $[xy]$ die *Lie-Klammer* von $x, y \in L$.)

2) Eine Liealgebra L heißt *kommutativ*, falls $[xy] = 0$ für alle $x, y \in L$ gilt.

3) Eine K-lineare Abbildung $\varphi\colon L \to L'$ mit Liealgebren L, L' heißt *Homomorphismus*, falls $\varphi([xy]) = [\varphi(x), \varphi(y)]$ für alle $x, y \in L$ gilt.

4) Ein Untervektorraum L' einer Liealgebra L heißt *Lieunteralgebra*, falls $[xy] \in L'$ für alle $x, y \in L'$ gilt.

Bemerkung
Ist L eine Lieunteralgebra, so gilt $[xy] = -[yx]$ für alle $x, y \in L$, denn

$$\begin{aligned} 0 &\underset{1)}{=} [x+y, x+y] \underset{\text{bil.}}{=} [x+y, x] + [x+y, y] \\ &\underset{\text{bil.}}{=} \underbrace{[xx]}_{=0} + [yx] + [xy] + \underbrace{[yy]}_{=0} \\ &\underset{1)}{=} [yx] + [xy]\,. \end{aligned}$$

6.2 Beispiele

1. Sei B eine K-Algebra. Setze $[xy] := xy - yx$ für $x, y \in B$. Dann ist B eine Liealgebra über K.

2. Ist $B = \mathrm{End}_K(W)$ mit einem K-Vektorraum W und ist die Lie-Klammer wie in 1. definiert, so heißt B die *Liealgebra der Endomorphismen von W* und wird als $\mathfrak{gl}(W)$ geschrieben. Ist $W = K^n$, so schreibt man $\mathfrak{gl}_n(K)$ und identifiziert $\mathfrak{gl}(W)$ mit $\mathrm{M}_{n\times n}(K)$ (bezüglich Standardbasis).

3. Sei $n = 2$. Dann ist

$$\mathfrak{sl}_2(K) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_{2\times 2}(K) \mid a + d = 0 \right\}$$

eine Lieunteralgebra von $\mathfrak{gl}_2(K)$. Eine K-Basis von $\mathfrak{sl}_2(K)$ ist

$$\left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\},$$

da

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = b \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + a \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + c \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

falls $a + d = 0$.

4. Lieunteralgebren von $\mathfrak{gl}_n(K)$ sind z. B.

$$\mathfrak{sl}_n(K) = \{x \in \mathfrak{gl}_n(K) \mid \mathrm{Spur}(x) = 0\} \quad \text{und}$$
$$\mathfrak{o}_n(K) = \{x \in \mathfrak{gl}_n(K) \mid {}^t x = -x\}.$$

5. E. Witt, 1935: Sei $\mathrm{char}(K) = p > 2$, und sei L ein p-dimensionaler K-Vektorraum. Ist $\{e_0, \ldots, e_{p-1}\}$ eine Basis von L über K, so wird durch

$$[e_i e_j] := (j - i) e_{(i+j) \bmod p}$$

eine Liealgebrastruktur auf L definiert.

6.3 Derivationen

Definition
Seien R ein kommutativer Ring, A eine kommutative R-Algebra (d. h. es gibt einen Ringhomomorphismus $R \to A$) und M ein A-Modul. Eine R-lineare Abbildung $D\colon A \to M$ heißt *R-Derivation*, falls gilt:

$$\boxed{D(ab) = aD(b) + bD(a) \quad \forall\, a, b \in A}.$$

Für eine R-Derivation $D\colon A \to M$ gilt:

$$\boxed{D(r) = 0 \quad \forall\, r \in R},$$

denn $D(1) = D(1 \cdot 1) = 1D(1) + 1D(1) = D(1) + D(1)$, also $D(1) = 0$ und daher $D(r) = D(r \cdot 1) = rD(1) = 0$ wegen der R-Linearität von D. Sei

$$\boxed{\mathrm{Der}_R(A, M) := \{R\text{-Derivationen } A \to M\}}.$$

Dann ist $\mathrm{Der}_R(A,M)$ ein R-Modul. Für $A = M$ und $D_1, D_2 \in \mathrm{Der}_R(A,A)$ gilt dann $D_1 \circ D_2 - D_2 \circ D_1 \in \mathrm{Der}_R(A,A)$. Insbesondere ist $\mathrm{Der}_K(A,A)$ eine Lieunteralgebra von $\mathfrak{gl}(A)$, falls $R = K$ ein Körper ist.

Beispiel
Ist $\mathrm{char}(K) = p > 0$ und $D \in \mathrm{Der}_K(A,A)$, so gilt

$$D^p(ab) = \sum_{i=0}^{p} \binom{p}{i} D^i(a) D^{p-i}(b) = aD^p(b) + bD^p(a)\,,$$

und also ist D^p eine K-Derivation.

6.4 Differentialmoduln

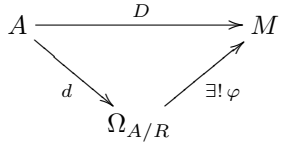
Seien R ein kommutativer Ring und A eine kommutative R-Algebra. Es sei $\mu\colon A \otimes_R A \to A$ die Multiplikation und $J := J_A := \ker \mu$. Da μ surjektiv ist, folgt aus dem Homomorphiesatz für Ringe (vgl. Algebra 7.7), dass μ einen Isomorphismus $(A \otimes_R A)/J \xrightarrow{\sim} A$ induziert. Es ist J/J^2 ein $(A \otimes_R A)$-Modul, der offensichtlich von J annuliert wird. Also kann J/J^2 auch als A-Modul vermöge $A \simeq (A \otimes_R A)/J$ betrachtet werden.

Definition
Der A-Modul $\Omega_{A/R} := J/J^2$ heißt *Differentialmodul von A über R*, und die Abbildung $d := d_{A/R}\colon A \to \Omega_{A/R}\,,\ a \mapsto a \otimes 1 - 1 \otimes a \bmod J^2$, wird *universelle R-Derivation* genannt.

Lemma
Es ist d tatsächlich eine Derivation, und die Elemente $d(a)$ mit $a \in A$ erzeugen den A-Modul $\Omega_{A/R}$.

Beweis. Es ist $d(ab) = (a \otimes 1)d(b) + (1 \otimes b)d(a)$ und also d eine Derivation. Für $x = \sum_i a_i \otimes b_i \in J$ gilt $\sum_i a_i b_i = 0$ und also $x = \sum_i a_i(1 \otimes b_i - b_i \otimes 1) = -\sum_i a_i(b_i \otimes 1 - 1 \otimes b_i)$. □

Universelle Eigenschaft des Paares $(\Omega_{A/R}, d)$
Ist M ein A-Modul und $D\colon A \to M$ eine R-Derivation, so gibt es genau eine A-lineare Abbildung $\varphi\colon \Omega_{A/R} \to M$ so, dass $D = \varphi \circ d$ gilt. Folgendes Diagramm ist also kommutativ:



Beweis. Durch die Vorschrift $\psi(a \otimes b) = bD(a)$ erhält man ein R-lineare Abbildung $\psi\colon A \otimes_R A \to M$, und für alle $x, y \in J = \ker \mu$ gilt

$$\psi(xy) = \underbrace{\mu(x)}_{=0}\psi(y) + \underbrace{\mu(y)}_{=0}\psi(x) = 0\,.$$

Also induziert ψ eine R-lineare Abbildung $\varphi\colon \Omega_{A/R} \to M$. Da $D(1) = 0$ gilt, ist $\psi(a \otimes 1 - 1 \otimes a) = D(a)$ für alle $a \in A$. Mit Hilfe des Lemmas folgt hieraus, dass $\varphi \circ d = D$ gilt und dass φ sogar A-linear ist. Gilt nun für $\xi\colon \Omega_{A/R} \to M$ ebenfalls $\xi \circ d = D$, so folgt $\xi(d(a)) = D(a) = \varphi(d(a))$ für alle $a \in A$ und daher nach dem Lemma $\xi = \varphi$. □

Satz
Für jeden A-Modul M ist die Abbildung

$$\Phi\colon \operatorname{Hom}_A(\Omega_{A/R}, M) \to \operatorname{Der}_R(A, M)\,,\ \varphi \mapsto \varphi \circ d\,,$$

ein Isomorphismus von A-Moduln.

Beweis. Dies folgt direkt aus der universellen Eigenschaft. □

Bemerkung
Sei $E = K(x)$ eine einfache Körpererweiterung eines Körpers K. Dann gilt $\dim_E(\Omega_{E/K}) \leqslant 1$, und es ist E genau dann separabel (algebraisch) über K, wenn $\Omega_{E/K} = (0)$ gilt, vgl. z. B. [11] 4.2.8.

6.5 Linksinvariante Derivationen von $K[G]$

Seien K algebraisch abgeschlossen, G eine lineare algebraische Gruppe und $A = K[G] = \operatorname{Mor}(G, K)$ die affine Algebra von G sowie

$$\lambda_g\colon A \to A\,,\ f \mapsto \begin{cases} G \to K\,, \\ x \mapsto f(g^{-1}x) \end{cases}$$

die *Linkstranslation mit $g \in G$*. Die Liealgebra $\operatorname{Lie}(G)$ ist definiert als

$$\boxed{\operatorname{Lie}(G) := \{D \in \operatorname{Der}_K(A, A) \mid \lambda_g \circ D = D \circ \lambda_g\ \forall\, g \in G\}}\,.$$

Es ist $\operatorname{Lie}(G)$ eine Lieunteralgebra von $\operatorname{Der}_K(A, A)$, genannt *Liealgebra der linksinvarianten K-Derivationen* von A. Sie hat folgende Eigenschaften:

(a) $\operatorname{Lie} G = \operatorname{Lie} G^0$, wobei G^0 wie in 3.5 gegeben ist.

(b) $\dim_K \operatorname{Lie} G = \dim G^0$, insbesondere $\dim_K \operatorname{Lie} G < \infty$.

(c) Ist $\alpha\colon G \to G'$ ein Morphismus von algebraischen Gruppen, so induziert α einen Liealgebrahomomorphismus $\overline{\alpha}\colon \operatorname{Lie} G \to \operatorname{Lie} G'$.

Um diese Eigenschaften zu beweisen, betrachtet man den *Tangentialraum* $T_e(G)$ von G in e und zeigt, dass $\operatorname{Lie} G$ als K-Vektorraum isomorph zu $T_e(G)$ ist.

6.6 Tangentialräume

Sei K algebraisch abgeschlossen, und sei V eine affine algebraische Varietät über K. Für $v \in V$ sei K_v der Körper K, betrachtet als $K[V]$-Modul vermöge $K[V] \to K$, $f \mapsto f(v)$. Der *Tangentialraum* T_vV *in* V ist der K-Vektorraum

$$\boxed{T_vV := \operatorname{Der}_K(K[V], K_v)}.$$

Bemerkung
Ist $\alpha\colon V \to V'$ ein Morphismus von Varietäten, so induziert

$$\alpha^*\colon K[V'] \to K[V]\,,\ f \mapsto f \circ \alpha\,,$$

eine K-lineare Abbildung

$$\boxed{d\alpha_v\colon T_vV \to T_{\alpha(v)}V'\,,\ D \mapsto D \circ \alpha^*}\,,$$

genannt *Differential von* α *in* v oder *Tangentialabbildung von* α *in* v. Für $V \xrightarrow{\alpha} V' \xrightarrow{\beta} V''$ gilt die *Kettenregel* $d(\beta\circ\alpha)_v = d\beta_{\alpha(v)} \circ d\alpha_v$. Ferner gilt: Ist $\alpha\colon V \to V'$ ein Isomorphismus von Varietäten, so ist $d\alpha_v$ ein Isomorphismus für alle $v \in V$ (vgl. Satz 2.9).
Sei $\mathfrak{m}_v := \{f \in K[V] \mid f(v) = 0\} = \operatorname{kern}(K[V] \to K,\ f \mapsto f(v))$. Für $D \in T_vV$ gilt dann (nach Definition von K_v):

$$D(fg) = \underbrace{f(v)}_{=0} D(g) + \underbrace{g(v)}_{=0} D(f) = 0 \ \ \forall\, f, g \in \mathfrak{m}_v\,.$$

Also induziert jedes $D \in T_vV$ eine K-lineare Abbildung $\ell(D)\colon \mathfrak{m}_v/\mathfrak{m}_v^2 \to K$.

Satz
Die Abbildung

$$\ell\colon T_vV \longrightarrow \operatorname{Hom}_K(\mathfrak{m}_v/\mathfrak{m}_v^2, K)\,,\ D \longmapsto \ell(D)\,,$$

ist ein Isomorphismus von K*-Vektorräumen mit Umkehrabbildung*

$$\operatorname{Hom}_K(\mathfrak{m}_v/\mathfrak{m}_v^2, K) \longrightarrow T_vV\,,$$
$$\psi \longmapsto \left[D_\psi\colon K[V] \to K_v\,,\ f \mapsto \psi(f - f(v) + \mathfrak{m}_v^2)\right].$$

Beweis. Da $f(v) = 0$ für alle $f \in \mathfrak{m}_v$ gilt, ist $\ell(D_\psi) = \psi$ für alle $\psi \in \mathrm{Hom}_K(\mathfrak{m}_v/\mathfrak{m}_v^2, K)$ und $D_{\ell(D)} = D$ für alle $D \in T_vV$. Noch zu zeigen ist, dass D_ψ eine K-Derivation ist. Es ist

$$\begin{aligned} D_\psi(fg) &\underset{\text{Def.}}{=} \psi(fg - f(v)g(v) + \mathfrak{m}_v^2) \text{ und} \\ fD_\psi(g) + gD_\psi(f) &= f(v)\psi(g - g(v) + \mathfrak{m}_v^2) + g(v)\psi(f - f(v) + \mathfrak{m}_v^2) \\ &\underset{\psi \text{ lin.}}{=} \psi\big(f(v)g - f(v)g(v) + g(v)f - g(v)f(v) + \mathfrak{m}_v^2\big)\,. \end{aligned}$$

Es ist $h := fg - f(v)g - g(v)f + g(v)f(v) = \underbrace{(f - f(v))}_{\in \mathfrak{m}_v} \cdot \underbrace{(g - g(v))}_{\in \mathfrak{m}_v} \in \mathfrak{m}_v^2$.

Daher folgt durch Addition von h in der großen Klammer, dass

$$fD_\psi(g) + gD_\psi(f) = \psi(fg - f(v)g(v) + \mathfrak{m}_v^2) = D_\psi(fg)$$

für alle $f, g \in K[V]$ gilt. □

6.7 Alternative Beschreibung

Seien K algebraisch abgeschlossen, V eine affine, algebraische Varietät und $V_f = \{v \in V \mid f(v) \neq 0\}$ für $f \in K[V]$. Ist $v \in V$, so bilden die offenen Mengen in V, die v enthalten, ein direktes System bezüglich Inklusion, und man kann den direkten Limes der in 2.14 definierten Ringe $\mathcal{O}_V(U)$ bilden. Ist V irreduzibel, so gilt (vgl. auch [9] V, § 1):

$$\varinjlim_{\substack{U \text{ offen} \\ U \ni v}} \mathcal{O}_V(U) \underset{\text{Aufg23}}{=} \varinjlim_{V_f \ni v} \mathcal{O}_V(V_f) \underset{2.14}{=} \varinjlim_{f(v) \neq 0} K[V]_f = \bigcup_{f(v) \neq 0} K[V]_f \underset{2.14}{=} \mathcal{O}_v\,,$$

denn da $K[V]$ ein Integritätsring ist (vgl. 2.3), geht der Limes im Funktionenkörper $K(V)$ in die Vereinigung über. Man definiert nun, auch wenn V nicht irreduzibel ist, den *Halm* $\mathcal{O}_v$ durch $\mathcal{O}_v := \varinjlim_{\substack{U \text{ offen} \\ U \ni v}} \mathcal{O}_V(U)$. Es ist $\mathcal{O}_v$ ein lokaler Ring mit maximalem Ideal M_v, und es gilt $\mathcal{O}_v/M_v \simeq K$.

Bemerkung 1. Für $v \in V$ ist $T_vV \simeq \mathrm{Der}_K(\mathcal{O}_v, K)$.
(Dies folgt aus der Quotientenregel, vgl. [11] 4.1.5.)

2. Ist V irreduzibel, so gilt $\dim_K(T_vV) \geqslant \dim V$ für alle $v \in V$.

3. Ein Punkt $v \in V$ heißt *einfach*, falls $\dim_K(T_vV) = \dim V$. Die Menge der einfachen Punkte von V liegt dicht in V (vgl. [11] 4.3.3).

Zum Beweis von 2. Sei $\mathfrak{m}_v = \{f \in K[V] \mid f(v) = 0\}$. Dann ist

$$\mathfrak{m}_v/\mathfrak{m}_v^2 \simeq M_v/M_v^2\,,$$

und es folgt $\dim_K(T_vV) \underset{6.6}{=} \dim_K(M_v/M_v^2) \geqslant \dim \mathcal{O}_v = \dim V$. Die letzten beiden Beziehungen zeigt man in der kommutativen Algebra. Mit $\dim \mathcal{O}_v$ ist die *Krulldimension von* $\mathcal{O}_v$ gemeint (das ist die größte Länge von Primidealketten $0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n = M_v$). □

6.8 Tangentialraum von G in e

Bemerkung
Seien K algebraisch abgeschlossen, G eine lineare algebraische Gruppe über K und T_eG der Tangentialraum von G in e. Dann gelten:

(i) $T_eG = T_eG^0$.

(ii) G ist glatt, d. h. jeder Punkt von G ist einfach.

(iii) $\dim_K(T_eG) = \dim G^0$.

Zum Beweis. Nach 3.5 (2) ist $G \setminus G^0$ die endliche Vereinigung von abgeschlossenen Mengen und daher abgeschlossen. Also ist G^0 offen und enthält e nach 3.5 (1). Aus der Definition des Halmes und 6.7.1 folgt nun (i).
Nach 6.7.3 gibt es einfache Punkte in G. Da $G \to G$, $x \mapsto gx$, für jedes $g \in G$ ein Isomorphismus von Varietäten ist, folgt (ii).
Nach (ii) ist e einfach. □

Sei $A = K[G] \overset{2.7}{=} \mathrm{Mor}(G, K)$. Jede K-Derivation $D\colon A \to A$, $f \mapsto Df$, definiert eine K-Derivation $D_e\colon A \to K_e$, $f \mapsto (Df)(e)$.

Satz
Die K-lineare Abbildung $\mathrm{Der}_K(A, A) \to T_eG$, $D \mapsto D_e$, *induziert einen Isomorphismus* $\psi\colon \mathrm{Lie}\, G \to T_eG$ *von K-Vektorräumen.*

Beweis. **Injektivität:** Sei $D \in \mathrm{Lie}\, G$ mit $D_e = 0$. Für alle $f \in A$ und für alle $g \in G$ folgt dann

$$\begin{aligned}
0 = D_e(\lambda_g(f)) &= D(\lambda_g(f))(e) && \text{nach Definition von } D_e\\
&= ((D \circ \lambda_g)(f))(e)\\
&= ((\lambda_g \circ D)(f))(e) && \text{nach Definition von } \mathrm{Lie}\, G \text{ in 6.5}\\
&= (Df)(g^{-1}e) && \text{nach Definition von } \lambda_g\\
&= (Df)(g^{-1})
\end{aligned}$$

und also $Df = 0$ für alle $f \in A$, d. h. $D = 0$.

Surjektivität: Sei $\delta \in T_eG$. Dann ist die *Konvolution*

$$*\delta\colon A \to A,\ f \mapsto f * \delta\colon \begin{cases} G \to K, \\ x \mapsto \delta(\lambda_{x^{-1}}(f)), \end{cases}$$

eine K-Derivation, denn $*\delta$ ist K-linear, und für $x \in G$, $f, g \in A$ ist

$$\begin{aligned}(fg * \delta)(x) &= \delta(\lambda_{x^{-1}}(fg)) = \delta(\lambda_{x^{-1}}(f)\lambda_{x^{-1}}(g)) \\ &= f(x) \cdot \delta(\lambda_{x^{-1}}(g)) + g(x) \cdot \delta(\lambda_{x^{-1}}(f)), \quad \text{da } \delta \in \mathrm{Der}_K(A, K_e) \\ &= (f(g * \delta) + g(f * \delta))(x).\end{aligned}$$

Ferner ist $*\delta$ linksinvariant, denn für $x, g \in G$ und $f \in A$ ist

$$\begin{aligned}((\lambda_g \circ *\delta)(f))(x) &= (\lambda_g(f * \delta))(x) \\ &= (f * \delta)(g^{-1}x) && \text{nach Definition von } \lambda_g \\ &= \delta(\lambda_{x^{-1}g}(f)) && \text{Definition von } f * \delta \\ &= \delta(\lambda_{x^{-1}}(\lambda_g(f)) \\ &= (\lambda_g(f) * \delta)(x) && \text{Definition von } *\delta \\ &= ((*\delta \circ \lambda_g)(f))(x)\end{aligned}$$

Es ist
$(\psi(*\delta))(f) \underset{\text{Def. von } \psi}{=} (*\delta)_e(f) = (f * \delta)(e) = \delta(f)$. Also $\psi(*\delta) = \delta$. □

Liealgebra $\mathfrak{g}$
Sei $\mathfrak{g} := T_eG$ als K-Vektorraum. Wir versehen $\mathfrak{g}$ durch Strukturtransport von $\mathrm{Lie}(G)$ vermöge $\psi\colon \mathrm{Lie}(G) \xrightarrow{\sim} T_eG$ mit einer Liealgebrastruktur und erhalten die *Liealgebra* $\mathfrak{g}$ zu G. Damit erhalten wir dann auch die in 6.5 (c) angekündigte „funktorielle Eigenschaft“ (vgl. [5] 9.2):

Ist $\alpha\colon G \to G'$ ein Morphismus von algebraischen Gruppen, so ist das Differential $d\alpha_e\colon \mathfrak{g} \to \mathfrak{g}'$, $\delta \mapsto \delta \circ \alpha^*$, ein Liealgebrahomomorphismus.

Es ist noch nachzurechnen, dass $d\alpha_e$ die Lie-Klammer respektiert.

6.9 Adjungierte Darstellung

Sei G wie in 6.8 gegeben, und sei $\iota_g\colon G \to G$, $x \to gxg^{-1}$, der durch $g \in G$ definierte innere Automorphismus von G. Dann erhält man einen Liealgebraautomorphismus

$$\mathrm{Ad}\, g := (d_{\iota_g})_e\colon T_eG \to T_eG,\ \delta \mapsto \delta \circ \iota_g^*.$$

Dies wiederum ergibt einen Morphismus $\mathrm{Ad}\colon G \to \mathrm{GL}(\mathfrak{g})$, $g \mapsto \mathrm{Ad}\, g$, von algebraischen Gruppen, genannt *adjungierte Darstellung* von G, vgl. z. B. [5] 9.1.

6.10 Beispiele

1) Sei $G = \mathbb{G}_{\mathrm{a}}(K)$, also $K[G] = K[X]$. Die Derivationen, die mit den Translationen $X \mapsto X + a$, $a \in K$, kommutieren, sind die Vielfachen von $D = \frac{d}{dX}$. Es ist $\mathfrak{g} = KD$ eindimensional mit $[D, D] = 0$ (und $D^p = 0$, wenn $\mathrm{char}(K) = p > 0$).

2) $G = \mathbb{G}_{\mathrm{m}}(K)$. Die Derivationen, die mit den Translationen $X \mapsto aX$ vertauschbar sind, sind die Vielfachen von $X\frac{d}{dX}$. Ist $\mathrm{char}(K) = p > 0$, so ist $D^p = D$. Es ist $[D, D] = 0$.

6.11 Klausuraufgaben 2001

Aufgabe 45
Man ermittle, welche der folgenden Mengen algebraisch sind:

(a) $\{(z^2, 0, z) \mid z \in \mathbb{C}\} \subset \mathbb{C}^3$,

(b) $\mathbb{Z} \subset \mathbb{C}$.

Aufgabe 46
Sei R ein kommutativer Ring, und sei $\mathcal{I}$ ein Ideal in R. Man beweise:

$\mathrm{Rad}(\mathcal{I}) = R \quad \Longleftrightarrow \quad \mathcal{I} = R$.

Aufgabe 47
Man ermittle, welche der folgenden Ideale in $\mathbb{C}[X, Y]$ Verschwindungsideale von Teilmengen des $\mathbb{C}^2$ sind:

(a) $\mathcal{I}_1 = (X^2)$,

(b) $\mathcal{I}_2 = (X^2 + Y^2 + 1)$.

Aufgabe 48
Sei K ein algebraisch abgeschlossener Körper, und sei K^n mit der Zariski-Topologie versehen. Man zeige, dass es zu je zwei verschiedenen Punkten $x, y \in K^n$ eine offene Menge $U \subset K^n$ gibt, die genau einen der beiden Punkte enthält.

Aufgabe 49
Sei K ein Körper. Man bestimme $\sigma, \tau \in \mathrm{End}_K(K^2)$ so, dass σ und τ diagonalisierbar sind, aber $\sigma + \tau$ nicht diagonalisierbar ist.

Aufgabe 50
Man bestimme bis auf Isomorphie alle nulldimensionalen, zusammenhängenden, linearen algebraischen Gruppen über einem algebraisch abgeschlossenen Körper K.

7 Wurzelsysteme und Dynkin-Diagramme

Sei $\mathbb{E}$ ein euklidischer Vektorraum, das ist ein endlich-dimensionaler $\mathbb{R}$-Vektorraum, versehen mit einer positiv definiten, symmetrischen Bilinearform

$$s\colon \mathbb{E}\times\mathbb{E}\longrightarrow\mathbb{R}\,,\ (\alpha,\beta)\longmapsto\langle\alpha,\beta\rangle\,.$$

7.1 Spiegelungen

Für $\alpha\in\mathbb{E}\setminus\{\vec{0}\}$ definieren wir

$$\sigma_\alpha\colon \mathbb{E}\longrightarrow\mathbb{E}\,,\ \beta\longmapsto\beta-2\,\frac{\langle\beta,\alpha\rangle}{\langle\alpha,\alpha\rangle}\,\alpha\,.$$

Dann ist σ_α die *Spiegelung* an der zu $\mathbb{R}\alpha$ senkrechten Hyperebene $H_\alpha := (\mathbb{R}\alpha)^\perp$, denn es gilt $\sigma_\alpha(\alpha)=-\alpha$ und $\sigma_\alpha(h)=h$ für alle $h\in H_\alpha$.

Behauptung
Es gilt $\sigma_\alpha\circ\sigma_\alpha=\mathrm{id}$, und σ_α ist eine Isometrie.

Beweis. Setze $\sigma:=\sigma_\alpha$. Aus der Bilinearität von s folgt die Linearität von σ, denn es ist $\sigma(r\beta)=r\beta-2\,\frac{\langle r\beta,\alpha\rangle}{\langle\alpha,\alpha\rangle}\,\alpha=r\sigma(\beta)$ für alle $r\in\mathbb{R}$ und $\beta\in\mathbb{E}$ und $\sigma(\beta+\beta')=\beta+\beta'-2\,\frac{\langle\beta+\beta',\alpha\rangle}{\langle\alpha,\alpha\rangle}\,\alpha=\beta+\beta'-2\,\frac{\langle\beta,\alpha\rangle}{\langle\alpha,\alpha\rangle}\,\alpha-2\,\frac{\langle\beta',\alpha\rangle}{\langle\alpha,\alpha\rangle}\,\alpha=\sigma(\beta)+\sigma(\beta')$ für alle $\beta,\beta'\in\mathbb{E}$. Hieraus folgt $\sigma\circ\sigma=\mathrm{id}$, denn es gilt

$$\begin{aligned}
\sigma(\sigma(\beta)) &= \sigma\big(\beta-2\,\frac{\langle\beta,\alpha\rangle}{\langle\alpha,\alpha\rangle}\,\alpha\big)\\
&= \sigma(\beta)-2\,\frac{\langle\beta,\alpha\rangle}{\langle\alpha,\alpha\rangle}\,\sigma(\alpha) \qquad \text{da } \sigma \text{ linear}\\
&= \beta-2\,\frac{\langle\beta,\alpha\rangle}{\langle\alpha,\alpha\rangle}\,\alpha+2\,\frac{\langle\beta,\alpha\rangle}{\langle\alpha,\alpha\rangle}\,\alpha \qquad \text{da } \sigma(\alpha)=-\alpha\\
&= \beta \ \text{ für alle } \beta\in\mathbb{E}.
\end{aligned}$$

Also ist σ bijektiv, und σ erhält das Skalarprodukt, denn es gilt

$$\begin{aligned}
\langle\sigma(\beta),\sigma(\beta')\rangle &= \langle\beta-2\,\frac{\langle\beta,\alpha\rangle}{\langle\alpha,\alpha\rangle}\,\alpha\,,\beta'-2\,\frac{\langle\beta',\alpha\rangle}{\langle\alpha,\alpha\rangle}\,\alpha\,\rangle\\
&= \langle\beta,\beta'\rangle-2\,\frac{\langle\beta',\alpha\rangle}{\langle\alpha,\alpha\rangle}\,\langle\beta,\alpha\rangle-2\,\frac{\langle\beta,\alpha\rangle}{\langle\alpha,\alpha\rangle}\,\langle\alpha,\beta'\rangle\\
&\qquad+4\,\frac{\langle\beta,\alpha\rangle\langle\beta',\alpha\rangle}{\langle\alpha,\alpha\rangle^2}\langle\alpha,\alpha\rangle\\
&= \langle\beta,\beta'\rangle \ \text{ für alle } \beta,\beta'\in\mathbb{E},\ \text{da } s \text{ symmetrisch ist.}
\end{aligned}$$

□

7.2 Wurzelsysteme

Eine Teilmenge $R \subset \mathbb{E}$ heißt *Wurzelsystem*, falls gelten:

(1) R ist ein endliches Erzeugendensystem von $\mathbb{E}$ und enthält nicht $\vec{0}$.

(2) Für jedes $\alpha \in R$ gilt $\sigma_\alpha(R) = R$. Insbesondere ist $-\alpha = \sigma_\alpha(\alpha) \in R$.

(3) Für $\alpha, \beta \in R$ ist

$$n(\beta, \alpha) := 2\,\frac{\langle \beta, \alpha \rangle}{\langle \alpha, \alpha \rangle} \in \mathbb{Z}\,.$$

Bemerkung
Ist R ein Wurzelsystem und gilt $\lambda\alpha \in R$ für ein $\alpha \in R$ und ein $\lambda \in \mathbb{R}$, so folgt $\lambda \in \{\pm 1, \pm\frac{1}{2}, \pm 2\}$.

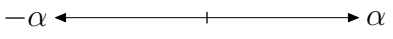
Beweis. Ist $\lambda\alpha \in R$, so folgt $-\lambda\alpha = \sigma_\alpha(\lambda\alpha) = \lambda\alpha - n\alpha$ mit $n \in \mathbb{Z}$ (nach Definition von σ_α und nach (3)). Es folgt $(2\lambda - n)\alpha = 0$ und also $\lambda = \frac{n}{2}$, da $\alpha \neq 0$ nach (1). Ist $|\lambda| < 1$, so ist $\lambda = \pm\frac{1}{2}$, da $n \in \mathbb{Z}$ und $\lambda \neq 0$ nach Voraussetzung und (1) gilt. Ist $|\lambda| > 1$, so gilt $R \ni \alpha = \frac{1}{\lambda}(\lambda\alpha)$ mit $\lambda\alpha \in R$ und $|\frac{1}{\lambda}| < 1$. Wie oben folgt nun $\frac{1}{\lambda} = \pm\frac{1}{2}$. □

Definition

- Ein Wurzelsystem R heißt *reduziert*, wenn gilt:
  Für jedes $\alpha \in R$ sind α und $-\alpha$ die einzigen Vielfachen von α in R.
- Der *Rang eines Wurzelsystems* $R \subset \mathbb{E}$ ist definiert als $\operatorname{rang} R := \dim_{\mathbb{R}} \mathbb{E}$.
- Zwei Wurzelsysteme $R \subset \mathbb{E}$ und $R' \subset \mathbb{E}'$ heißen *isomorph*, wenn es einen Vektorraumisomorphismus $f\colon \mathbb{E} \longrightarrow \mathbb{E}'$ gibt mit $f(R) = R'$ und $n(\alpha, \beta) = n(f(\alpha), f(\beta))$ für alle $\alpha, \beta \in R$.

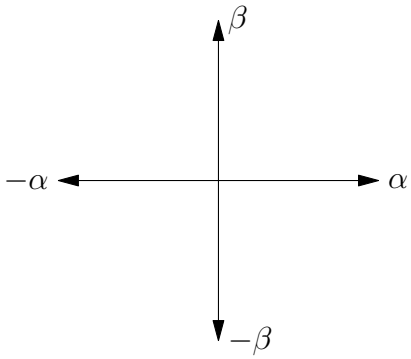
Beispiele
Reduzierte Wurzelsysteme vom Rang 1 und 2 lassen sich einfach grafisch darstellen:

Reduzierte Wurzelsysteme vom Rang 1
Jedes reduzierte Wurzelsystem vom Rang 1 ist von der Form

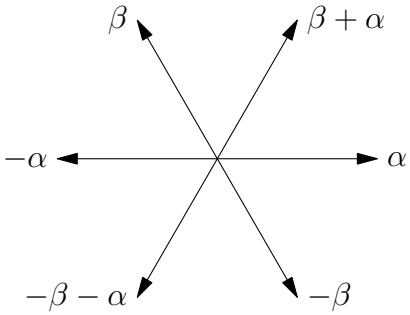


A_1

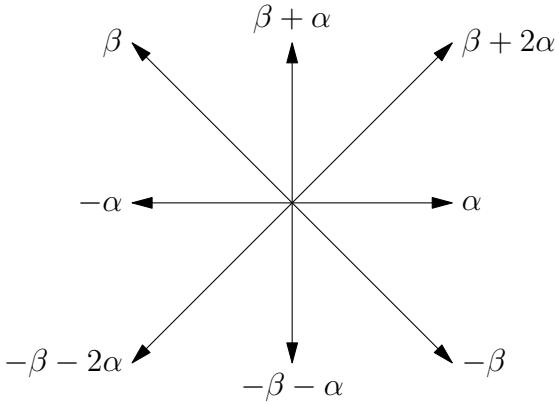
Reduzierte Wurzelsysteme vom Rang 2
Wie aus 7.5 unten folgt, ist jedes reduzierte Wurzelsystem vom Rang 2 zu einem der folgenden vier Wurzelsysteme isomorph.



$A_1 \times A_1$

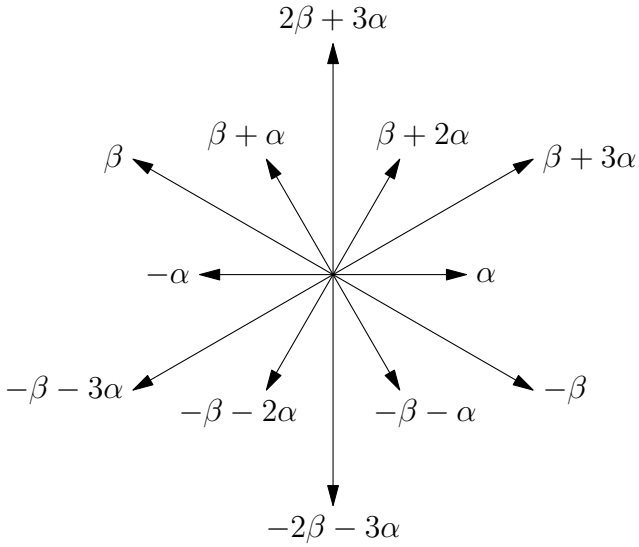


A_2



B_2

Bei A_2 ist $\|\beta\| = \|\alpha\|$. Bei B_2 ist $\|\beta\| = \sqrt{2}\,\|\alpha\|$.



G_2

Bei G_2 ist $\|\beta\| = \sqrt{3}\,\|\alpha\|$.

7.3 Weylgruppe eines Wurzelsystems

Sei R ein Wurzelsystem in $\mathbb{E}$. Die von den Spiegelungen σ_α mit $\alpha \in R$ erzeugte Untergruppe $\mathcal{W}(R)$ von $\mathrm{GL}(\mathbb{E})$ heißt *Weylgruppe* von R. Da $\mathcal{W}(R)$ die Elemente von R permutiert, und da R endlich ist und $\mathbb{E}$ erzeugt, können wir $\mathcal{W}(R)$ als Untergruppe der symmetrischen Gruppe von R auffassen. Die Weylgruppe $\mathcal{W}(R)$ ist also eine endliche Gruppe. Aus 7.1 folgt, dass $n(\alpha,\beta) = n(\sigma(\alpha),\sigma(\beta))$ für alle $\alpha,\beta \in R$ und $\sigma \in \mathcal{W}(R)$ gilt.

Beispiele
Es ist $\mathcal{W}(A_1) \simeq \mathbb{Z}/2\mathbb{Z}$, da $\sigma(\alpha) = -\alpha$ gilt. Ferner ist $\mathcal{W}(A_1 \times A_1) \simeq D_2$, $\mathcal{W}(A_2) \simeq D_3$, $\mathcal{W}(B_2) \simeq D_4$, $\mathcal{W}(G_2) \simeq D_6$, wobei D_n die Diedergruppe mit $2n$ Elementen für $n = 2,3,4,6$ bezeichnet. Dies folgt mit Hilfe von 7.4.

Bemerkung
Sind zwei Wurzelsysteme $R \subset \mathbb{E}$ und $R' \subset \mathbb{E}'$ vermöge $f\colon \mathbb{E} \longrightarrow \mathbb{E}'$ isomorph, so ist $\mathcal{W}(R) \longrightarrow \mathcal{W}(R')$, $\sigma \longmapsto f \circ \sigma \circ f^{-1}$, ein Isomorphismus der zugehörigen Weylgruppen, denn es gilt

$$\sigma_{f(\alpha)}\,(f(\beta)) = f\,(\sigma_\alpha(\beta)) \qquad \forall\, \alpha,\beta \in R$$

und also $f^{-1} \circ \sigma_{f(\alpha)} \circ f = \sigma_\alpha$ für alle $\alpha \in R$.

7.4 Winkel zwischen zwei Wurzeln

Die Elemente eines Wurzelsystems $R \subset \mathbb{E}$ heißen *Wurzeln*. Für zwei Wurzeln $\alpha, \beta \in R$ sei wie zuvor $n(\beta,\alpha) := 2\,\frac{\langle\beta,\alpha\rangle}{\langle\alpha,\alpha\rangle} \in \mathbb{Z}$. Nach AGLA 9.7, 9.8 ist die *Länge von* α durch $\|\alpha\| = \sqrt{\langle\alpha,\alpha\rangle}$ und der *Winkel* $\varphi = \measuredangle(\alpha,\beta)$ durch $\langle\alpha,\beta\rangle = \|\alpha\|\,\|\beta\| \cdot \cos\varphi$ für $\alpha,\beta \in \mathbb{E}$ gegeben. Es folgt

$$n(\beta,\alpha) = 2\,\frac{\|\beta\|\,\|\alpha\|}{\|\alpha\|^2}\cos\varphi = 2\,\frac{\|\beta\|}{\|\alpha\|}\cos\varphi$$

und daher $\boxed{n(\beta,\alpha)n(\alpha,\beta) = 4\cos^2\varphi \in \mathbb{Z} \;\; \forall\,\alpha,\beta \in R}$.

Daher ist $n(\beta,\alpha) \in \{0, \pm1, \pm2, \pm3, \pm4\}$, da $0 \leqslant \cos^2\varphi \leqslant 1$ gilt. Die Zahlen $n(\beta,\alpha)$ und $n(\alpha,\beta)$ haben dasselbe Vorzeichen. Also können nur folgende Fälle auftreten, wobei $\|\beta\| \geqslant \|\alpha\|$ ist:

	$n(\alpha,\beta)$	$n(\beta,\alpha)$	φ	$\cos\varphi$	Länge	$\operatorname{ord}(\sigma_\alpha\sigma_\beta)$
1.	0	0	$\frac{\pi}{2} \mathrel{\widehat{=}} 90°$	0	unbestimmt	2
2.	1	1	$\frac{\pi}{3} \mathrel{\widehat{=}} 60°$	$\frac{1}{2}$	$\|\beta\| = \|\alpha\|$	3
3.	-1	-1	$\frac{2\pi}{3} \mathrel{\widehat{=}} 120°$	$-\frac{1}{2}$	$\|\beta\| = \|\alpha\|$	3
4.	1	2	$\frac{\pi}{4} \mathrel{\widehat{=}} 45°$	$\frac{\sqrt{2}}{2}$	$\|\beta\| = \sqrt{2}\|\alpha\|$	4
5.	-1	-2	$\frac{3\pi}{4} \mathrel{\widehat{=}} 135°$	$-\frac{\sqrt{2}}{2}$	$\|\beta\| = \sqrt{2}\|\alpha\|$	4
6.	1	3	$\frac{\pi}{6} \mathrel{\widehat{=}} 30°$	$\frac{\sqrt{3}}{2}$	$\|\beta\| = \sqrt{3}\|\alpha\|$	6
7.	-1	-3	$\frac{5\pi}{6} \mathrel{\widehat{=}} 150°$	$-\frac{\sqrt{3}}{2}$	$\|\beta\| = \sqrt{3}\|\alpha\|$	6

In den noch fehlenden Fällen sind α und β proportional: Ist $n(\beta,\alpha) = \pm4$, dann folgt $\beta = \pm2\alpha$. Ist $n(\beta,\alpha) = \pm2 = n(\alpha,\beta)$, dann folgt $\beta = \pm\alpha$. (Vgl. AGLA 9.7, Beweis von iv.)

Lemma
Seien $\alpha,\beta \in R$. Ist $n(\alpha,\beta) > 0$ und ist $\alpha \neq \beta$, so ist $\alpha - \beta$ eine Wurzel. Ist $n(\alpha,\beta) < 0$ und ist $\alpha \neq -\beta$, so ist $\alpha + \beta$ eine Wurzel.

Beweis. Nach 7.2 (2) gelten:

$$\begin{aligned}
&n(\alpha,\beta) = 1 \quad \Longrightarrow \quad \alpha - \beta = \sigma_\beta(\alpha) \in R,\\
&n(\beta,\alpha) = 1 \quad \Longrightarrow \quad \beta - \alpha = \sigma_\alpha(\beta) \in R \quad \Longrightarrow \quad \alpha - \beta \in R,\\
&n(\alpha,\beta) = -1 \quad \Longrightarrow \quad \alpha + \beta = \sigma_\beta(\alpha) \in R,\\
&n(\beta,\alpha) = -1 \quad \Longrightarrow \quad \beta + \alpha = \sigma_\alpha(\beta) \in R.
\end{aligned}$$

Mehr Fälle brauchen gemäß Tabelle nicht betrachtet zu werden, da der Fall $n(\beta,\alpha) = \pm2 = n(\alpha,\beta)$ zum Widerspruch zur Voraussetzung und der Fall $n(\beta,\alpha) = \pm4$ zu $n(\alpha,\beta) = \pm1$ führt. □

Um eine Übersicht über die möglichen Wurzelsysteme zu bekommen, ist der folgende Satz nützlich. Man beachte dabei, dass R nach 7.2 endlich ist.

Satz
Seien α, β zwei nicht-proportionale Wurzeln in R. Dann gelten:

a) *Die Menge $I := \{j \in \mathbb{Z} \mid \beta + j\alpha \in R\}$ ist ein Intervall $[-q, p]$ in $\mathbb{Z}$, das 0 enthält.*

b) *Die Menge $S := \{\beta + j\alpha \mid j \in I\}$ erfüllt $\sigma_\alpha(S) = S$, und es gelten*

$$\sigma_\alpha(\beta + p\alpha) = \beta - q\alpha \quad \textit{und} \quad p - q = -n(\beta, \alpha)\,.$$

c) *Für den* Ursprung $\gamma := \beta - q\alpha$ von S *gilt $-n(\gamma, \alpha) = p + q$, und es ist $S = \{\gamma + j\alpha \mid 0 \leqslant j \leqslant -n(\gamma, \alpha)\}$ mit $-n(\gamma, \alpha) = 0, 1, 2$ oder 3.*

Beweis. Es ist $0 \in I$. Sei p das größte und $-q$ das kleinste Element in I. Angenommen, es gibt eine ganze Zahl in $[-q, p]$, die nicht in I liegt. Dann gibt es Elemente $r, s \in [-q, p]$ mit $r + 1 < s$, die beide in I liegen und für die $r+1 \notin I$ und $s-1 \notin I$ gelten. Es ist also $\alpha+(\beta+r\alpha) = \beta+(r+1)\alpha \notin R$, woraus nach dem Lemma $n(\alpha, \beta + r\alpha) \geqslant 0$ folgt. Da $s - 1 \notin I$ gilt, folgt $(\beta+s\alpha)-\alpha = \beta+(s-1)\alpha \notin R$ und also nach dem Lemma $n(\beta+s\alpha, \alpha) \leqslant 0$. Da $n(\beta, \alpha) \geqslant 0$ genau dann gilt, wenn $\langle\beta, \alpha\rangle \geqslant 0$ ist, folgt $\langle\alpha, \beta + r\alpha\rangle \geqslant 0$ und $\langle\alpha, \beta + s\alpha\rangle \leqslant 0$. Dies ist ein Widerspruch, da $r < s$ und $\langle\alpha, \alpha\rangle > 0$ gilt und also $\langle\alpha, \beta + r\alpha\rangle < \langle\alpha, \beta + s\alpha\rangle$ ist. Es folgt a).
Nach 7.1 ist $\sigma_\alpha(\beta+j\alpha) = \beta-n(\beta, \alpha)\alpha-j\alpha = \beta+j'\alpha$ mit $j' = -n(\beta, \alpha)-j$. Es folgt $\sigma_\alpha(S) \subset S$ und $S \subset \sigma_\alpha(S)$, da $\sigma_\alpha^2 = \mathrm{id}$. Also ist $\sigma_\alpha(S) = S$. Die Abbildung $I \to I$, $j \mapsto j'$ ist bijektiv. Es gilt $i' < j'$ für $i > j$. Es folgt $p' = -q$ und $\sigma_\alpha(\beta + p\alpha) = \beta - q\alpha$ sowie $p - q = -n(\beta, \alpha)$, also gilt b).
Es gilt $n(\gamma, \alpha) = n(\beta - q\alpha, \alpha) = 2\,\frac{\langle\beta-q\alpha,\alpha\rangle}{\langle\alpha,\alpha\rangle} = n(\beta, \alpha) - 2q = -p + q - 2q = -p - q$. Da α und γ nicht proportional sind, ergibt die Tabelle oben, dass $|n(\gamma, \alpha)| \leqslant 3$ gilt. Die Menge S hat $p+q+1$ Elemente nach a). Es folgt c). □

Folgerung
Wir wenden nun Satz c) für $\beta = \gamma$ an und erhalten dabei genau folgende vier Möglichkeiten (vgl. auch die obige Tabelle):

1. $S = \{\beta\}$: Dann ist $n(\beta, \alpha) = 0 = n(\alpha, \beta)$ und $\measuredangle(\alpha, \beta) = \frac{\pi}{2}$.

2. $S = \{\beta, \beta + \alpha\}$: Dann ist $n(\beta, \alpha) = -1$, und es gibt drei Fälle:
1. Fall: Es ist $n(\alpha, \beta) = -1$, also $\|\beta\| = \|\alpha\|$ und $\measuredangle(\alpha, \beta) = \frac{2\pi}{3}$ sowie $\measuredangle(\alpha, \beta + \alpha) = \frac{\pi}{3} = \measuredangle(\beta + \alpha, \beta)$.
2. Fall: Es ist $n(\alpha, \beta) = -2$, also $\|\alpha\| = \sqrt{2}\,\|\beta\|$ und $\measuredangle(\alpha, \beta) = \frac{3\pi}{4}$ sowie $\measuredangle(\alpha, \beta + \alpha) = \frac{\pi}{4}$ und $\measuredangle(\beta + \alpha, \beta) = \frac{2\pi}{4}$. (Hier ist α länger als β,

und es ist $\alpha + 2\beta$ auch eine Wurzel, da $R \ni \sigma_\beta(\alpha) = \alpha + 2\beta$ gilt.)
3. Fall: Es ist $n(\alpha, \beta) = -3$, also $\|\alpha\| = \sqrt{3}\,\|\beta\|$ und $\measuredangle(\alpha, \beta) = \frac{5\pi}{6}$ sowie $\measuredangle(\alpha, \beta + \alpha) = \frac{\pi}{6}$ und $\measuredangle(\beta + \alpha, \beta) = \frac{4\pi}{6}$. (Hier ist α länger als β.)

3. $S = \{\beta, \beta + \alpha, \beta + 2\alpha\}$:
Dann ist $n(\beta, \alpha) = -2$ und also $n(\alpha, \beta) = -1$. Es folgt $\|\beta\| = \sqrt{2}\,\|\alpha\|$, $\measuredangle(\alpha, \beta) = \frac{3\pi}{4}$ und $\measuredangle(\alpha, \beta + 2\alpha) = \measuredangle(\beta + 2\alpha, \beta + \alpha) = \measuredangle(\beta + \alpha, \beta) = \frac{\pi}{4}$.

4. $S = \{\beta, \beta + \alpha, \beta + 2\alpha, \beta + 3\alpha\}$:
Dann ist $n(\beta, \alpha) = -3$ und also $n(\alpha, \beta) = -1$. Es folgt $\|\beta\| = \sqrt{3}\,\|\alpha\|$ und $\measuredangle(\alpha, \beta) = \frac{5\pi}{6}$ sowie $\measuredangle(\alpha, \beta + 3\alpha) = \frac{\pi}{6} = \measuredangle(\beta + 3\alpha, \beta + 2\alpha)$ und $\measuredangle(\beta + 2\alpha, \beta + \alpha) = \frac{2\pi}{6}$ und $\measuredangle(\beta + \alpha, \beta) = \frac{\pi}{6}$.

Die Menge S wird α-*String* durch β genannt.

7.5 Reduzierte Wurzelsysteme vom Rang 2

Sei R ein reduziertes Wurzelsystem vom Rang 2 in $\mathbb{E}$. Nach 7.2 (1) enthält R eine Basis $\{\alpha, \beta\}$ von $\mathbb{E}$. In den Fällen $A_1 \times A_1$ und B_2 sei $\mathbb{E} := \mathbb{R}^2$, und in den Fällen A_2 und G_2 sei $\mathbb{E} := \mathbb{R}\alpha + \mathbb{R}\beta \subset \mathbb{R}^3$. Wir versehen $\mathbb{R}^n$ mit dem Standardskalarprodukt, und e_1, e_2 bzw. e_1, e_2, e_3 seien die Standardbasisvektoren von $\mathbb{R}^2$ bzw. $\mathbb{R}^3$. Es gilt $n(\beta, \alpha) := 2\,\frac{\langle \beta, \alpha\rangle}{\langle \alpha, \alpha\rangle} \in \{0, -1, -2, -3\}$. Folgerung 7.4 ergibt die vier Typen vom Rang 2 aus 7.2.

1. Typ $A_1 \times A_1$:
Sei $\alpha := e_1$ und $\beta := e_2$. Dann ist $n(\beta, \alpha) = 0$ und $n(\alpha, \beta) = 0$. Es ist $R = \{\pm\alpha, \pm\beta\}$.

2. Typ A_2:
Sei $\alpha := e_1 - e_2$ und $\beta := e_2 - e_3$. Dann ist $\langle \alpha, \beta\rangle = -1$ und $\langle \alpha, \alpha\rangle = 2 = \langle \beta, \beta\rangle$ und also $n(\alpha, \beta) = n(\beta, \alpha) = -1$. Es ist $R = \{\pm\alpha, \pm\beta, \pm(\alpha + \beta)\}$.

3. Typ B_2:
Sei $\alpha := e_1$ und $\beta := e_2 - e_1$. Dann ist $\langle \alpha, \beta\rangle = -1$ und $\langle \alpha, \alpha\rangle = 1$ sowie $\langle \beta, \beta\rangle = 2$. Es folgt $n(\beta, \alpha) = -2$ und $n(\alpha, \beta) = -1$. Es ist $R = \{\pm\alpha, \pm\beta, \pm(\beta + \alpha), \pm(\beta + 2\alpha)\}$.

4. Typ G_2:
Sei $\alpha := e_1 - e_2$ und $\beta := -2e_1 + e_2 + e_3$. Dann ist $\langle \alpha, \beta\rangle = -3$, $\langle \alpha, \alpha\rangle = 2$ und $\langle \beta, \beta\rangle = 6$. Es folgt $n(\beta, \alpha) = -3$ und $n(\alpha, \beta) = -1$. Dies führt zum Typ G_2, denn es ist $2\beta + 3\alpha$ nach 7.2 (2) eine Wurzel, wie die folgende Betrachtung zeigt:
Es ist $\sigma_\beta(\alpha) = \alpha - n(\alpha, \beta)\beta = \alpha + \beta$, da $n(\alpha, \beta) = -1$ ist, und es ist $\sigma_\beta(\beta + 3\alpha) = \sigma_\beta(\beta) + 3\,\sigma_\beta(\alpha) = -\beta + 3\alpha + 3\beta = 2\beta + 3\alpha$. Es folgt $R = \{\pm\alpha, \pm\beta, \pm(\beta + \alpha), \pm(\beta + 2\alpha), \pm(\beta + 3\alpha), \pm(2\beta + 3\alpha)\}$.

Beobachtung
Sieht man sich die Wurzelsysteme genauer an, so fällt auf, dass sich stets jede Wurzel als $\mathbb{Z}$-Linearkombination von Elementen der Basis $\Delta := \{\alpha, \beta\}$ schreiben lässt, bei der entweder alle Koeffizienten $\geqslant 0$ oder alle Koeffizienten $\leqslant 0$ sind. Eine solche Basis Δ von $\mathbb{E}$ gibt es auch für Wurzelsysteme vom Rang > 2, wie wir in 7.6 zeigen werden.

7.6 Existenz von Wurzelbasen

Sei $R \subset \mathbb{E}$ ein Wurzelsystem. Eine Teilmenge $\Delta \subset R$ heißt *Wurzelbasis* von $\mathbb{E}$ oder *Basis* von R, falls gelten:

1) Δ ist eine Basis von $\mathbb{E}$ als $\mathbb{R}$-Vektorraum.

2) Jedes $\beta \in R$ lässt sich als $\mathbb{Z}$-Linearkombination $\beta = \sum_{\alpha \in \Delta} n_\alpha \, \alpha$ schreiben, wobei die n_α entweder alle nicht-negativ oder alle nicht-positiv sind.

Ist $n_\alpha \geqslant 0$ für alle $\alpha \in \Delta$, so heißt β *positiv*, andernfalls *negativ*. Die Elemente einer Wurzelbasis heißen *einfache Wurzeln*.
Um zu zeigen, dass R eine Basis besitzt, wählen wir $\gamma \in \mathbb{E}$ so, dass γ in keiner der (endlich vielen) Hyperebenen $H_\alpha := (\mathbb{R}\alpha)^\perp$ mit $\alpha \in R$ liegt, d. h. dass $\langle \gamma, \alpha \rangle \neq 0$ für alle $\alpha \in R$ gilt. Sei $R^+(\gamma) := \{\alpha \in R \mid \langle \gamma, \alpha \rangle > 0\}$. Dann ist $R = R^+(\gamma) \cup -R^+(\gamma)$ nach Wahl von γ. Sei

$$\Delta(\gamma) := \{\alpha \in R^+(\gamma) \mid \alpha \text{ ist nicht Summe zweier Elemente aus } R^+(\gamma)\}.$$

Lemma
Jede Wurzel in $R^+(\gamma)$ ist eine $\mathbb{Z}$-Linearkombination von Elementen aus $\Delta(\gamma)$ mit lauter nicht-negativen Koeffizienten. Ferner gilt $\langle \alpha, \beta \rangle \leqslant 0$ für alle $\alpha, \beta \in \Delta(\gamma)$ mit $\alpha \neq \beta$.

Beweis. Angenommen, es gibt eine Wurzel $\alpha \in R^+(\gamma)$, die dies nicht erfüllt, so sei eine solche Wurzel α mit kleinstmöglichem Wert für $\langle \gamma, \alpha \rangle$ gewählt. Dann gilt $\alpha = 1\alpha \notin \Delta(\gamma)$ und also $\alpha = \alpha_1 + \alpha_2$ mit $\alpha_1, \alpha_2 \in R^+(\gamma)$. Es folgt $\langle \gamma, \alpha \rangle = \langle \gamma, \alpha_1 \rangle + \langle \gamma, \alpha_2 \rangle$, wobei beide Summanden positiv sind. Wegen der Minimalität von $\langle \gamma, \alpha \rangle$ müssen sich also α_1 und α_2 beide als $\mathbb{Z}$-Linearkombination von Elementen aus $\Delta(\gamma)$ mit lauter nicht-negativen Koeffizienten darstellen lassen und daher auch α im Widerspruch zur Annahme.
Angenommen, es gibt $\alpha \neq \beta$ in $\Delta(\gamma)$ mit $\langle \alpha, \beta \rangle > 0$. Dann ist $\alpha - \beta$ nach Lemma 7.4 eine Wurzel. Also gilt $\alpha - \beta \in R^+(\gamma)$ oder $\beta - \alpha \in R^+(\gamma)$. Im ersten Fall ist $\alpha = \beta + (\alpha - \beta) \notin \Delta(\gamma)$, und im zweiten Fall ist $\beta = \alpha + (\beta - \alpha) \notin \Delta(\gamma)$ im Widerspruch zur Voraussetzung. □

Existenzsatz für Wurzelbasen
$\Delta(\gamma)$ *ist eine Basis von* R*.*

Beweis. Da $R = R^+(\gamma) \cup -R^+(\gamma)$ gilt, folgt 2) aus dem Lemma. Aus 2) folgt nun, dass $\Delta(\gamma)$ ein Erzeugendensystem von $\mathbb{E}$ über $\mathbb{R}$ bildet, da R nach 7.2 ein solches ist. Wie aus dem Satz unten folgt, ist $\Delta(\gamma)$ linear unabhängig, denn es ist $\langle \gamma, \alpha \rangle > 0$ für alle $\alpha \in \Delta(\gamma)$, und es gilt $\langle \alpha, \beta \rangle \leqslant 0$ für alle $\alpha, \beta \in \Delta(\gamma)$ nach dem Lemma. □

Satz
Sei $\Delta \subset \mathbb{E}$*, und sei* $\gamma \in E$*. Es gelte* $\langle \gamma, \alpha \rangle > 0$ *für alle* $\alpha \in \Delta$ *und* $\langle \alpha, \beta \rangle \leqslant 0$ *für alle* $\alpha, \beta \in \Delta$*. Dann sind die Elemente von* Δ *linear unabhängig.*

Beweis. Sei $\sum\limits_{\alpha \in \Delta} r_\alpha \, \alpha = \vec{0}$ mit $r_\alpha \in \mathbb{R}$ und $r_\alpha \neq 0$ für nur endlich viele $\alpha \in \Delta$. Dann lässt sich dies zu $\delta := \sum_{\alpha \in S} r_\alpha \, \alpha = \sum_{\beta \in T} t_\beta \, \beta$ umformen, wobei die Indexmengen S und T disjunkte endliche Teilmengen von Δ sind und $r_\alpha \geqslant 0$ sowie $t_\beta := -r_\beta \geqslant 0$ gelten. Da $\langle \alpha, \beta \rangle \leqslant 0$ ist, folgt $\langle \delta, \delta \rangle = \langle \sum_\alpha r_\alpha \, \alpha \, , \sum_\beta t_\beta \, \beta \rangle = \sum\limits_{\alpha, \beta} \underbrace{r_\alpha \, t_\beta}_{\geqslant 0} \, \underbrace{\langle \alpha, \beta \rangle}_{\leqslant 0} \leqslant 0$, also $\delta = \vec{0}$. Dies ergibt $0 = \langle \gamma, \delta \rangle = \sum_{\alpha \in S} r_\alpha \, \langle \gamma, \alpha \rangle$ und also $r_\alpha = 0$ für alle $\alpha \in S$, da $\langle \gamma, \alpha \rangle > 0$ gilt. Analog folgt $t_\beta = 0$ für alle $\beta \in T$. □

Korollar
Ist Δ *eine Basis von* R*, so ist* $\langle \alpha, \beta \rangle \leqslant 0$ *für alle* $\alpha, \beta \in \Delta$ *mit* $\alpha \neq \beta$*, und* $\alpha - \beta$ *ist keine Wurzel.*

Beweis. Ist $\langle \alpha, \beta \rangle > 0$, so ergibt Lemma 7.4, dass $\alpha - \beta$ eine Wurzel ist, was aber der Bedingung 2) für eine Wurzelbasis widerspricht. □

Bemerkung
Sei R ein reduziertes Wurzelsystem und Δ eine Basis von R. Dann gelten:

a) Es ist $\Delta = \Delta(\gamma)$ für jedes $\gamma \in \mathbb{E}$ mit der Eigenschaft $\langle \gamma, \alpha \rangle > 0$ für alle $\alpha \in \Delta$ (und es gibt ein solches γ), vgl. [4] 10.1 oder [10] V.8.

b) Ist Δ' eine weitere Basis von R, dann gilt $\sigma(\Delta') = \Delta$ mit einem $\sigma \in \mathcal{W}(R)$, d. h. die Weylgruppe $\mathcal{W}(R)$ operiert transitiv auf der Menge der Basen von R. (Und die Operation ist sogar einfach transitiv.)

c) Zu jedem $\alpha \in R$ gibt es ein $\sigma \in \mathcal{W}(R)$ so, dass $\sigma(\alpha) \in \Delta$ gilt.

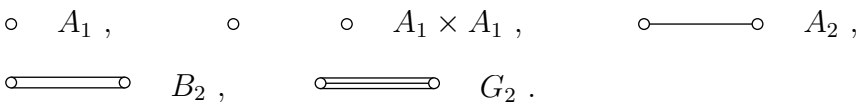
d) Die Weylgruppe $\mathcal{W}(R)$ wird von den Spiegelungen σ_α mit $\alpha \in \Delta$ erzeugt.

Für die Eigenschaften b), c) und d) vgl. [4] 10.3 oder [10] V.10.

7.7 Coxeter-Graphen

Sei R ein reduziertes Wurzelsystem und Δ eine Basis von R. Ein *Coxeter-Graph von R* ist der Graph mit den Elementen von Δ als Knoten, wobei zwei verschiedene Knoten durch $0, 1, 2$ oder 3 Kanten verbunden sind, je nachdem, ob $n(\alpha, \beta) \cdot n(\beta, \alpha) = 0, 1, 2$ oder 3 ist, vgl. 7.4.

Beispiele
Die Coxeter-Graphen zu den Beispielen von 7.2, 7.5 sind wie folgt gegeben.



Die Coxeter-Graphen zu A_1, A_2, B_2 und G_2 sind zusammenhängend, und entsprechend sind die zugehörigen Wurzelsysteme *irreduzibel*. Der Coxeter-Graph von $A_1 \times A_1$ ist unzusammenhängend, und entsprechend ist das zugehörige Wurzelsystem *reduzibel*. Dabei gilt folgende Definition.

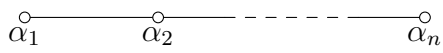
Definition
Ein Wurzelsystem R heißt *irreduzibel*, wenn sich R nicht darstellen lässt als Vereinigung $R = R_1 \cup R_2$, wobei R_1, R_2 echte Teilmengen von R sind und $\langle \alpha, \beta \rangle = 0$ für alle $\alpha \in R_1$ und alle $\beta \in R_2$ gilt. Andernfalls heißt R *reduzibel*.

Bemerkung
Ein Wurzelsystem ist genau dann irreduzibel, wenn der zugehörige Coxeter-Graph zusammenhängend ist. Da sich jedes reduzible Wurzelsystem $R \subset \mathbb{E}$ in irreduzible Bestandteile $R_i \subset \mathbb{E}_i$ zerlegen lässt, wobei $\mathbb{E}$ eine orthogonale Summe der $\mathbb{E}_i$ ist (vgl. [4] 11.3), beschränken wir uns im Folgenden auf die Betrachtung von irreduziblen Wurzelsystemen und zusammenhängenden Coxeter-Graphen.

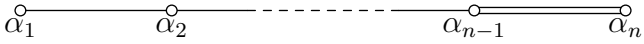
Es erhebt sich die Frage, wie sich die Beispiele oben verallgemeinern, wenn der Rang von R größer als 2 ist. Darüber gibt das folgende Theorem, dessen Beweis äußerst trickreich ist und etliche Reduktionsschritte enthält, Auskunft, vgl. [4] 11.4 oder [3] Chap. VI, § 4.1.

Theorem
Ist R ein irreduzibles, reduziertes Wurzelsystem, so ist der zu R gehörende Coxeter-Graph isomorph zu einem der folgenden Graphen.

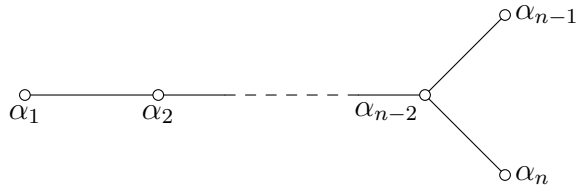
A_n , $n \geqslant 1$: Durch die Indizierung ist die Anzahl der Knoten angegeben:



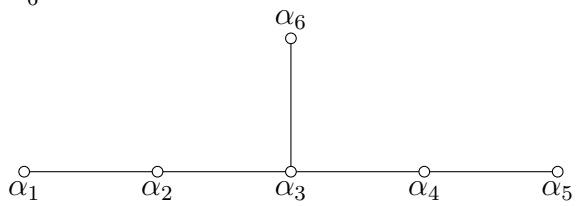
B_n , $n \geqslant 2$:



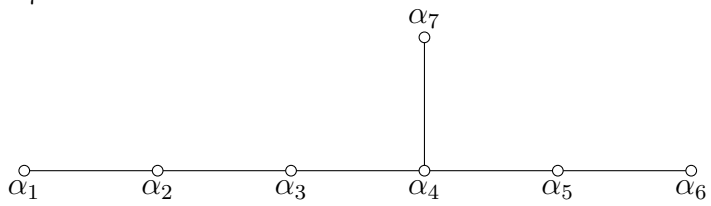
D_n , $n \geqslant 4$:



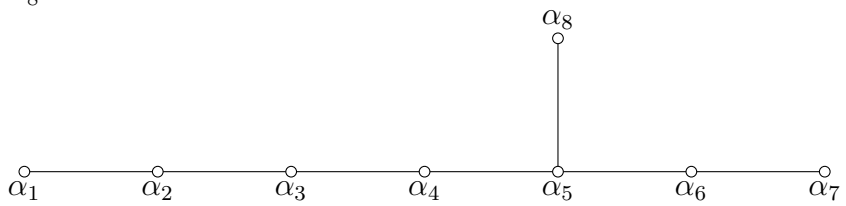
E_6 :



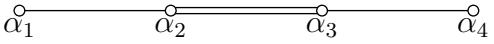
E_7 :



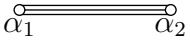
E_8 :



F_4 :



G_2 :



7.8 Cartan-Matrizen

Sei R ein reduziertes Wurzelsystem in $\mathbb{E}$, und sei $\Delta := \{\alpha_1, \ldots, \alpha_n\}$ eine (geordnete) Basis von R. Die *Cartan-Matrix* von R ist die Matrix $(n(\alpha_i, \alpha_j))$. Zum Beispiel haben die Wurzelsysteme A_2 und G_2 bezüglich der in 7.5 jeweils angegebenen Basis $\{\alpha, \beta\}$ die Cartan-Matrix

$$\begin{pmatrix} n(\alpha,\alpha) & n(\alpha,\beta) \\ n(\beta,\alpha) & n(\beta,\beta) \end{pmatrix} \overset{A_2}{=} \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}, \quad \begin{pmatrix} n(\alpha,\alpha) & n(\alpha,\beta) \\ n(\beta,\alpha) & n(\beta,\beta) \end{pmatrix} \overset{G_2}{=} \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}.$$

Die Cartan-Matrix hängt von der gewählten Ordnung der Basis ab und ist aber ansonsten unabhängig von der Wahl der Basis von R, da die Weylgruppe transitiv auf der Menge der Basen operiert. Bis auf Isomorphie ist R durch seine Cartan-Matrix eindeutig bestimmt. Genauer gilt:

Satz
Sei R' ein reduziertes Wurzelsystem mit Basis Δ' in einem euklidischen Vektorraum $\mathbb{E}'$, und sei $\phi\colon \Delta \to \Delta'$ eine Bijektion so, dass $n(\alpha,\beta) = n(\phi(\alpha),\phi(\beta))$ für alle $\alpha, \beta \in \Delta$ gilt. Dann gibt es einen eindeutig bestimmten Vektorraumisomorphismus $f\colon \mathbb{E} \to \mathbb{E}'$, der ϕ fortsetzt und für den $f(R) = R'$ gilt. Ferner ist $n(\alpha,\beta) = n(f(\alpha), f(\beta))$ für alle $\alpha, \beta \in R$.

Beweis. Da Δ und Δ' Basen sind, lässt sich ϕ eindeutig zu einem Vektorraumisomorphismus $f\colon \mathbb{E} \to \mathbb{E}'$ fortsetzen. Sind α, β in Δ, so gilt

$$\begin{aligned} (\sigma_{\phi(\alpha)} \circ f)(\beta) &= \sigma_{\phi(\alpha)}(\phi(\beta)) = \phi(\beta) - n(\phi(\beta),\phi(\alpha))\,\phi(\alpha) \\ \text{und } (f \circ \sigma_\alpha)(\beta) &= f(\beta - n(\beta,\alpha)\alpha) = \phi(\beta) - n(\beta,\alpha)\,\phi(\alpha). \end{aligned}$$

Nach Voraussetzung folgt hieraus $\sigma_{\phi(\alpha)} \circ f = f \circ \sigma_\alpha$ für alle $\alpha \in \Delta$ und daher $n(f(\alpha), f(\beta)) = n(\alpha,\beta)$ für alle $\alpha \in \Delta$ und $\beta \in R$. Sei $\mathcal{W}$ bzw. $\mathcal{W}'$ die Weylgruppe von R bzw. R'. Da $\mathcal{W}$ von den Spielgelungen σ_α mit $\alpha \in \Delta$ erzeugt wird (und analog $\mathcal{W}'$), vgl. Bemerkung 7.6, erhalten wir einen Isomorphismus $\iota\colon \mathcal{W} \to \mathcal{W}'$, $\sigma \mapsto f \circ \sigma \circ f^{-1}$, mit $\iota(\sigma_\alpha) = \sigma_{\phi(\alpha)}$ für alle $\alpha \in \Delta$. Nach Bemerkung 7.6 gibt es zu jedem $\beta \in R$ ein $\sigma \in \mathcal{W}$ und ein $\delta \in \Delta$ so, dass $\beta = \sigma(\delta)$ gilt. Es folgt $f(\beta) = (f \circ \sigma \circ f^{-1})(f(\delta)) \in R'$. Seien $\alpha, \beta \in R$, und sei $\omega \in \mathcal{W}$ und $\varepsilon \in \Delta$ so gewählt, dass $\varepsilon = \omega(\alpha)$ gilt. Dann ist $\gamma := \omega(\beta) \in R$, und es folgt

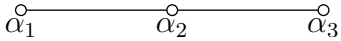
$$\begin{aligned} n(\alpha,\beta) &= n(\omega(\alpha),\omega(\beta)) = n(\varepsilon,\gamma) = n(f(\varepsilon), f(\gamma)) \quad \text{da } \varepsilon \in \Delta \\ &= n\big((f \circ \omega \circ f^{-1})(f(\alpha)), (f \circ \omega \circ f^{-1})(f(\beta))\big) \\ &= n(f(\alpha), f(\beta)) \qquad \text{da } f \circ \omega \circ f^{-1} \in \mathcal{W}' \end{aligned}$$

Damit ist der Satz mit Hilfe von Bemerkung 7.6 bewiesen. □

Typ A_3
Seien e_1, e_2, e_3, e_4 die Standardbasisvektoren in $\mathbb{R}^4$, und sei R ein Wurzelsystem vom Typ A_3. Hierzu gehört die Wurzelbasis $\Delta := \{\alpha_1, \alpha_2, \alpha_3\}$ mit $\alpha_1 := e_1 - e_2$, $\alpha_2 := e_2 - e_3$ und $\alpha_3 := e_3 - e_4$. Es ist also $\langle \alpha_1, \alpha_3 \rangle = 0$, und wir erhalten die Cartan-Matrix

$$\begin{pmatrix} n(\alpha_1,\alpha_1) & n(\alpha_1,\alpha_2) & n(\alpha_1,\alpha_3) \\ n(\alpha_2,\alpha_1) & n(\alpha_2,\alpha_2) & n(\alpha_2,\alpha_3) \\ n(\alpha_3,\alpha_1) & n(\alpha_3,\alpha_2) & n(\alpha_3,\alpha_3) \end{pmatrix} \overset{A_3}{=} \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}.$$

Aus der Matrix können wir den Coxeter-Graphen zum Typ A_3 konstruieren:



Die Wurzeln α_1 und α_3 sind durch 0 Kanten verbunden. Die Wurzeln α_1 und α_2 sowie α_2 und α_3 sind jeweils durch $(-1)\cdot(-1) = 1$ Kante verbunden. Umgekehrt kann man aus dem Coxeter-Graphen die Cartan-Matrix ablesen. Die Diagonalelemente sind stets 2, da $n(\alpha, \alpha) = 2$ für jede Wurzel α gilt. Diese Beobachtungen gelten analog für alle Typen A_n, $n \geqslant 1$.

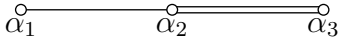
Typ B_2
Wenden wir auf das in 7.5 betrachtete Wurzelsystem vom Typ B_2 mit Basis $\{\beta := e_2 - e_1, \alpha := e_1\}$ die Spielgelung σ_β an, so erhalten wir ein isomorphes Wurzelsystem $\{\pm\alpha_1, \pm\alpha_2, \pm(\alpha_1 + \alpha_2), \pm(\alpha_1 + 2\alpha_2)\} \subset \mathbb{R}^2$ mit Basis $\{\alpha_1, \alpha_2\}$, wobei $\alpha_1 = e_1 - e_2$ und $\alpha_2 = e_2$ gilt. Dazu gehört die Cartan-Matrix

$$\begin{pmatrix} n(\alpha_1,\alpha_1) & n(\alpha_1,\alpha_2) \\ n(\alpha_2,\alpha_1) & n(\alpha_2,\alpha_2) \end{pmatrix} \overset{B_2}{=} \begin{pmatrix} 2 & -2 \\ -1 & 2 \end{pmatrix}.$$

Typ B_3
Zum Typ B_3 in $\mathbb{R}^3$ gehört die Wurzelbasis $\{\alpha_1, \alpha_2, \alpha_3\}$ mit $\alpha_1 := e_1 - e_2$, $\alpha_2 := e_2 - e_3$, $\alpha_3 = e_3$ und also die Cartan-Matrix

$$\begin{pmatrix} n(\alpha_1,\alpha_1) & n(\alpha_1,\alpha_2) & n(\alpha_1,\alpha_3) \\ n(\alpha_2,\alpha_1) & n(\alpha_2,\alpha_2) & n(\alpha_2,\alpha_3) \\ n(\alpha_3,\alpha_1) & n(\alpha_3,\alpha_2) & n(\alpha_3,\alpha_3) \end{pmatrix} \overset{B_3}{=} \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -2 \\ 0 & -1 & 2 \end{pmatrix}.$$

Es ist $\|\alpha_1\| = \sqrt{2} = \|\alpha_2\|$ und $\|\alpha_3\| = 1$, also ist α_3 die kürzere Wurzel. Aus der Cartan-Matrix ergibt sich der Coxeter-Graph

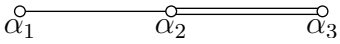


Es gibt 18 Wurzeln, nämlich $\pm e_1, \pm e_2, \pm e_3, \pm(e_1 - e_2), \pm(e_1 - e_3), \pm(e_2 - e_3)$ sowie $\pm(e_1 + e_2), \pm(e_1 + e_3), \pm(e_2 + e_3)$. Das sind genau die 18 Wurzeln $\pm\alpha_1, \pm\alpha_2, \pm\alpha_3, \pm(\alpha_1 + \alpha_2), \pm(\alpha_2 + \alpha_3), \pm(\alpha_2 + 2\alpha_3), \pm(\alpha_1 + \alpha_2 + \alpha_3)$, $\pm(\alpha_1 + \alpha_2 + 2\alpha_3), \pm(\alpha_1 + 2\alpha_2 + 2\alpha_3)$.

Typ C_3
Dieser Typ ist bisher nicht aufgetreten. Zum Typ C_3 in $\mathbb{E} := \mathbb{R}^3$ gehört die Wurzelbasis $\{\alpha_1, \alpha_2, \alpha_3\}$ mit $\alpha_1 := e_1 - e_2$, $\alpha_2 := e_2 - e_3$, $\alpha_3 = 2e_3$ und die Cartan-Matrix

$$\begin{pmatrix} n(\alpha_1,\alpha_1) & n(\alpha_1,\alpha_2) & n(\alpha_1,\alpha_3) \\ n(\alpha_2,\alpha_1) & n(\alpha_2,\alpha_2) & n(\alpha_2,\alpha_3) \\ n(\alpha_3,\alpha_1) & n(\alpha_3,\alpha_2) & n(\alpha_3,\alpha_3) \end{pmatrix} \overset{C_3}{=} \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -2 & 2 \end{pmatrix}.$$

Es ist hier $\|\alpha_1\| = \sqrt{2} = \|\alpha_2\|$ und $\|\alpha_3\| = 2$, also ist α_3 die längere Wurzel. Da $n(\alpha_2,\alpha_3) \cdot n(\alpha_3,\alpha_2) = 2$ wie im Fall B_3 gilt, ergibt sich aus der Cartan-Matrix wieder der Coxeter-Graph



Aus dem Coxeter-Graphen können wir hier nicht mehr die Cartan-Matrix zurück gewinnen. Die Cartan-Matrix gibt uns noch die zusätzliche Information, dass α_3 die lange Wurzel ist, denn es gilt

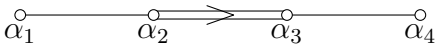
$$\frac{\|\alpha_3\|^2}{\|\alpha_2\|^2} = \frac{\langle \alpha_3, \alpha_3\rangle}{\langle \alpha_2, \alpha_2\rangle} = \frac{n(\alpha_3,\alpha_2)}{n(\alpha_2,\alpha_3)} = \frac{-2}{-1} = 2 > 1\,.$$

Es gibt die 18 Wurzeln $\pm 2e_1, \pm 2e_2, \pm 2e_3$, $\pm(e_1 - e_2), \pm(e_1 - e_3), \pm(e_2 - e_3)$ sowie $\pm(e_1 + e_2), \pm(e_1 + e_3), \pm(e_2 + e_3)$. Das sind genau die 18 Wurzeln $\pm\alpha_1, \pm\alpha_2, \pm\alpha_3, \pm(\alpha_1 + \alpha_2), \pm(\alpha_2 + \alpha_3), \pm(2\alpha_2 + \alpha_3), \pm(\alpha_1 + \alpha_2 + \alpha_3)$, $\pm(\alpha_1 + 2\alpha_2 + \alpha_3), \pm(2\alpha_1 + 2\alpha_2 + \alpha_3)$.
Die Wurzelsysteme vom Typ B_3 und C_3 sind nicht isomorph. Ist R vom Typ B_3, so ist das zu R *duale* oder *inverse* System $R^\vee := \{\alpha^\vee \mid \alpha \in R\}$ mit $\alpha^\vee := \frac{2\alpha}{\langle \alpha,\alpha\rangle}$ vom Typ C_3 und umgekehrt. Es ist $R^\vee$ ein Wurzelsystem in $\mathbb{E}$, das $n(\alpha^\vee, \beta^\vee) = n(\beta, \alpha)$ für alle $\alpha, \beta \in R$ erfüllt.

7.9 Dynkin-Diagramme

Sei $R \subset \mathbb{E}$ ein reduziertes und irreduzibles Wurzelsystem vom Rang n mit Basis Δ. Dann ist R bis auf Isomorphie durch seine Cartan-Matrix eindeutig bestimmt. Die Cartan-Matrix gibt Auskunft über die Winkel zwischen Wurzeln $\alpha, \beta \in \Delta$ und, falls $n(\alpha,\beta) \neq 0$, über deren Längenverhältnis $\frac{\langle \alpha,\alpha\rangle}{\langle \beta,\beta\rangle} = \frac{n(\alpha,\beta)}{n(\beta,\alpha)}$. Aus ihr kann man den Coxeter-Graphen konstruieren, aber umgekehrt kann man nicht unbedingt aus dem Coxeter-Graphen die Cartan-Matrix ablesen.
Das *Dynkin-Diagramm* von R entsteht aus dem Coxeter-Graphen von R durch Hinzufügen eines Pfeiles, der auf kürzere Wurzeln zeigt. Aus dem Dynkin-Diagramm kann man dann die Cartan-Matrix wieder gewinnen.

Zum Beispiel ergibt sich aus dem Dynkin-Diagramm zum Typ F_4



die Cartan-Matrix

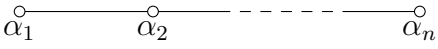
$$\begin{pmatrix} n(\alpha_1,\alpha_1) & n(\alpha_1,\alpha_2) & n(\alpha_1,\alpha_3) & n(\alpha_1,\alpha_4) \\ n(\alpha_2,\alpha_1) & n(\alpha_2,\alpha_2) & n(\alpha_2,\alpha_3) & n(\alpha_2,\alpha_4) \\ n(\alpha_3,\alpha_1) & n(\alpha_3,\alpha_2) & n(\alpha_3,\alpha_3) & n(\alpha_3,\alpha_4) \\ n(\alpha_4,\alpha_1) & n(\alpha_4,\alpha_2) & n(\alpha_4,\alpha_3) & n(\alpha_4,\alpha_4) \end{pmatrix} \overset{F_4}{=} \begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -2 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}.$$

Klassifikationssatz
Sei R ein reduziertes und irreduzibles Wurzelsystem vom Rang n mit Basis $\{\alpha_1, \ldots, \alpha_n\}$. Dann ist das Dynkin-Diagramm von R durch eines der folgenden Diagramme gegeben. Umgekehrt tritt jeder der aufgeführten Diagrammtypen als Dynkin-Diagramm eines Wurzelsystems auf.

Wir führen hier die Typen auf und geben eine Konstruktionsmethode an. Der Beweis des Klassifikationssatzes findet sich in [3], Chap. VI, [4], 11.4, 12.1, und [6], Chap. IV.

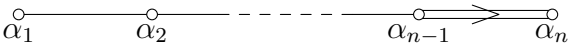
Wie zuvor ist $\mathbb{R}^n$ mit dem Standardskalarprodukt versehen, und also gilt $\langle e_i, e_j\rangle = 0$, falls $i \neq j$, und $\langle e_i, e_i\rangle = 1$ für die Standardbasisvektoren $e_1, \ldots, e_n$ von $\mathbb{R}^n$. Sei $L_n = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n$. Dann gilt $\langle \alpha, \beta\rangle \in \mathbb{Z}$ für alle $\alpha, \beta \in L_n$.

Typ A_n, $n \geqslant 1$:



Konstruktion: Sei $\mathbb{E} = (\mathbb{R}\varepsilon)^\perp$ mit $\varepsilon = e_1 + \cdots + e_{n+1}$ in $\mathbb{R}^{n+1}$, und sei $R := \{\alpha \in \mathbb{E} \cap L_{n+1} \mid \langle \alpha, \alpha\rangle = 2\}$. Dann ist $R = \{e_i - e_j \mid i \neq j\}$, und R erfüllt die Bedingungen für ein Wurzelsystem. Die n Vektoren $\alpha_i := e_i - e_{i+1}$ für $i = 1, \ldots, n$ bilden eine Basis von $\mathbb{E}$. Sie bilden eine Basis von R, da $e_i - e_j = (e_i - e_{i+1}) + \cdots + (e_{j-1} - e_j)$ für $i < j$ gilt und also auch die Wurzelbasisbedingung 2) in 7.6 erfüllt ist. Die Weylgruppe ist die Gruppe der Permutationen der Vektoren $e_1, \ldots, e_n$.

Typ B_n, $n \geqslant 2$:

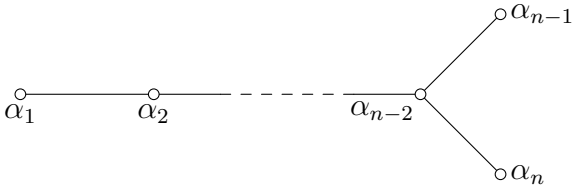


Konstruktion: Sei $E := \mathbb{R}^n$ und $R := \{\alpha \in L_n \mid \langle \alpha, \alpha\rangle = 1 \text{ oder } 2\}$. Dann besteht R aus den Vektoren e_i und $\pm(e_i - e_j)$, $\pm(e_i + e_j)$ für $i \neq j$, und die Menge $\{e_1 - e_2, e_2 - e_3, \ldots, e_{n-1} - e_n, e_n\}$ ist eine Wurzelbasis. Die Weylgruppe ist die Gruppe der Permutationen und Vorzeichenwechsel der Vektoren $e_1, \ldots, e_n$. (Es ist B_1 isomorph zu A_1, daher die Zählung für B_n ab $n = 2$.)

Typ C_n , $n \geqslant 3$ **:**

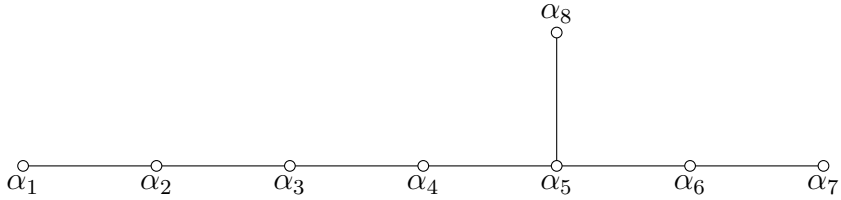
Konstruktion: Sei $E := \mathbb{R}^n$. Für $n \geqslant 2$ sei C_n das zu B_n inverse Wurzelsystem $R^\vee := \{\alpha^\vee \mid \alpha \in R\}$ mit $\alpha^\vee := \frac{2\alpha}{\langle\alpha,\alpha\rangle}$. Es gilt dann $n(\alpha^\vee, \beta^\vee) = n(\beta, \alpha)$ für alle $\alpha, \beta \in R$, und C_2 ist isomorph zu B_2. Die Vektoren $2e_i$ und $\pm(e_i - e_j)$, $\pm(e_i + e_j)$ für $i \neq j$ bilden ein Wurzelsystem in $\mathbb{E}$, und die Menge $\{e_1 - e_2, e_2 - e_3, \ldots, e_{n-1} - e_n, 2e_n\}$ ist eine Wurzelbasis. Die Weylgruppe ist isomorph zur Weylgruppe von B_n.

Typ D_n , $n \geqslant 4$ **:**



Konstruktion: Sei $\mathbb{E} := \mathbb{R}^n$ und $n \geqslant 2$. Es ist dann
$R := \{\alpha \in L_n \mid \langle\alpha,\alpha\rangle = 2\} = \{\pm(e_i - e_j), \pm(e_i + e_j) \mid i \neq j\}$ ein Wurzelsystem in $\mathbb{E}$, und die Menge $\{e_1 - e_2, e_2 - e_3, \ldots, e_{n-1} - e_n, e_{n-1} + e_n\}$ ist eine Wurzelbasis. Die Weylgruppe ist die Gruppe der Permutationen und der Vorzeichenwechsel von einer geraden Anzahl von Vorzeichen der Menge $\{e_1, \ldots, e_n\}$. (Es ist D_2 isomorph zu $A_1 \times A_1$ und D_3 isomorph zu A_3.)

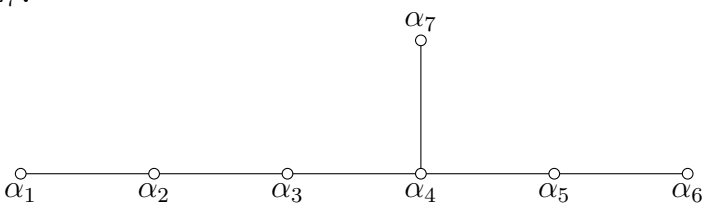
Typ E_8 **:**



Konstruktion: Sei $\mathbb{E} := \mathbb{R}^8$, und sei L_8' der $\mathbb{Z}$-Untermodul von L_8, der aus allen Elementen $x_1e_1 + \cdots + x_8e_8 \in L_8$ besteht, für die $x_1 + \cdots + x_8$ gerade ist. Ferner sei $L_8'' = L_8' + \mathbb{Z}(\frac{1}{2}(e_1 + \cdots + e_8))$. Sei R die Menge der Vektoren $\alpha \in L_8''$, für die $\langle\alpha,\alpha\rangle = 2$ gilt. Dann besteht R aus den Vektoren $\pm e_i \pm e_j$ für $1 \leqslant i < j \leqslant 8$ und $\frac{1}{2}\sum_{i=1}^8 (-1)^{m(i)} e_i$, wobei $\sum_{i=1}^8 m(i)$ gerade ist, und hat also $\binom{8}{2} \cdot 4 + 2^7 = 240$ Elemente. Eine Wurzelbasis ist durch $\alpha_1 = e_7 - e_6$, $\alpha_2 = e_6 - e_5$, $\alpha_3 = e_5 - e_4$, $\alpha_4 = e_4 - e_3$, $\alpha_5 = e_3 - e_2$, $\alpha_6 = e_2 - e_1$, $\alpha_7 = \frac{1}{2}(e_1 + e_8) - \frac{1}{2}(e_2 + e_3 + e_4 + e_5 + e_6 + e_7)$ und $\alpha_8 = e_1 + e_2$ gegeben. Die Weylgruppe hat $2^{14} \cdot 3^5 \cdot 5^2 \cdot 7$ Elemente. Die Cartan-Matrix zu der Wurzelbasis ergibt genau die zum Diagramm passende Cartan-Matrix:

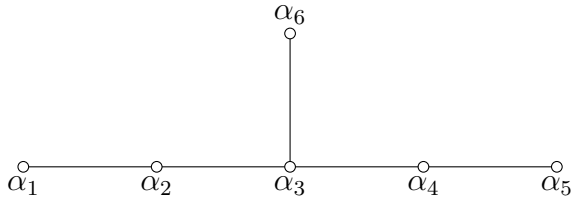
$$(n(\alpha_i,\alpha_j)) \overset{E_8}{=} \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 2 \end{pmatrix}$$

Typ E_7:



Konstruktion: Sei $\mathbb{E}$ die Hyperebene in $\mathbb{R}^8$, die von den beim Typ E_8 angegebenen Wurzeln $\alpha_2, \ldots, \alpha_8$ erzeugt wird, und sei R_8 das zu E_8 konstruierte Wurzelsystem. Dann ist $R = R_8 \cap \mathbb{E}$ ein Wurzelsystem vom Typ E_7, und eine Basis von R ist (nach Umnummerierung) gegeben durch:
$\alpha_1 = e_6 - e_5,\ \alpha_2 = e_5 - e_4,\ \alpha_3 = e_4 - e_3,\ \alpha_4 = e_3 - e_2,\ \alpha_5 = e_2 - e_1,$
$\alpha_6 = \frac{1}{2}(e_1 + e_8) - \frac{1}{2}(e_2 + e_3 + e_4 + e_5 + e_6 + e_7)$ und $\alpha_7 = e_1 + e_2$.
Hiermit ergibt sich die zu dem Diagramm passende Cartan-Matrix. Die Weylgruppe hat $2^{10} \cdot 3^4 \cdot 5 \cdot 7$ Elemente.

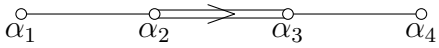
Typ E_6:



Konstruktion: Sei $\mathbb{E}$ der Vektorraum, der von den beim Typ E_8 angegebenen Wurzeln $\alpha_3, \ldots, \alpha_8$ erzeugt wird. Dann ist $R = R_8 \cap \mathbb{E}$ ein Wurzelsystem vom Typ E_6. Eine Basis von R ist (nach Umnummerierung) durch $\alpha_1 = e_5 - e_4,\ \alpha_2 = e_4 - e_3,\ \alpha_3 = e_3 - e_2,\ \alpha_4 = e_2 - e_1$ sowie $\alpha_5 = \frac{1}{2}(e_1 + e_8) - \frac{1}{2}(e_2 + e_3 + e_4 + e_5 + e_6 + e_7)$ und $\alpha_6 = e_1 + e_2$ gegeben. Die Weylgruppe hat $2^7 \cdot 3^4 \cdot 5$ Elemente. Die Cartan-Matrix zu der angegebenen Basis passt zu der Cartan-Matrix des Dynkin-Diagramms:

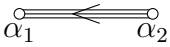
$$(n(\alpha_i,\alpha_j)) \overset{E_6}{=} \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 2 \end{pmatrix}$$

Typ F_4:



Konstruktion: Sei $\mathbb{E} := \mathbb{R}^4$ und L_4' die Untergruppe von $\mathbb{E}$, die von L_4 und $\frac{1}{2}(e_1+e_2+e_3+e_4)$ erzeugt wird. Sei $R := \{\alpha \in L_4' \mid \langle \alpha, \alpha\rangle = 1 \text{ oder } 2\}$. Dann besteht R aus den 48 Vektoren $\pm e_1, \pm e_2, \pm e_3, \pm e_4$ und $\pm e_i \pm e_j$ für $1 \leqslant i < j \leqslant 4$ und hat die Basis $\{\alpha_1 = e_2 - e_3\,,\ \alpha_2 = e_3 - e_4\,,\ \alpha_3 = e_4\,,\ \alpha_4 = \frac{1}{2}(e_1 - e_2 - e_3 - e_4)\}$. Die Weylgruppe hat $2^7 \cdot 3^2$ Elemente.

Typ G_2:



Konstruktion: Die Konstruktion ist schon explizit in 7.5 erfolgt. Hier erhalten wir das Wurzelsystem R, indem wir $\mathbb{E} = (\mathbb{R}\varepsilon)^\perp$ mit $\varepsilon = e_1+e_2+e_3$ und $R := \{\alpha \in \mathbb{E} \cap L_3 \mid \langle \alpha, \alpha\rangle = 2 \text{ oder } 6\}$ setzen. Es ist dann $R = \pm\{e_1 - e_2, e_1 - e_3, e_2 - e_3, 2e_1 - e_2 - e_3, 2e_2 - e_1 - e_3, 2e_3 - e_1 - e_2\}$, und wir können als Basis die Elemente $\alpha_1 := e_1 - e_2$ und $\alpha_2 := -2e_1 + e_2 + e_3$ wählen. Die Weylgruppe ist die Diedergruppe D_6 mit 12 Elementen.

Bemerkung

- Die Typen E_8, E_7, E_6, F_4, G_2 werden *Ausnahmetypen* genannt.
- Für das inverse Wurzelsystem $R^\vee$ gilt stets $R = R^\vee$ außer in den Fällen B_n, C_n für $n \geqslant 3$. Weitere Informationen und ausführliche Herleitungen stehen in [3] Chap. VI.

7.10 Wurzelsystem einer halbeinfachen Liealgebra

Sei $L \neq \{\vec{0}\}$ eine Liealgebra über einem Körper K. Dann wird die von L *abgeleitete Liealgebra* $[LL]$ als Vektorraum von allen Lieklammern $[xy]$ mit $x, y \in L$ erzeugt. Man definiert nun induktiv eine abgeleitete Reihe $\mathcal{D}^0(L) = L\,,\ \mathcal{D}^1(L) = [LL]\,,\ \ldots\,,\ \mathcal{D}^{i+1}(L) = [\mathcal{D}^i(L)\,\mathcal{D}^i(L)]$ und nennt L *auflösbar*, wenn es ein $n \in \mathbb{N}$ mit $\mathcal{D}^n(L) = \{\vec{0}\}$ gibt.
Ein Untervektorraum I von L heißt *Ideal* in L, wenn $[xy] \in I$ für alle $x \in L$ und $y \in I$ gilt. Die Ideale spielen in der Theorie der Liealgebren eine ähnlich wichtige Rolle wie die Normalteiler in der Gruppentheorie.

Ideale sind insbesondere Lieunteralgebren. Sind I und J auflösbare Ideale in L, so ist auch deren Summe $I+J := \{x+y \mid x \in I, y \in J\}$ ein auflösbares Ideal, und also gibt es bezüglich Inklusion ein größtes auflösbares Ideal in L. Dieses wird das *Radikal* von L genannt und als $\operatorname{Rad} L$ geschrieben.

Definition
Eine Liealgebra L heißt *halbeinfach*, falls $\operatorname{Rad} L = \{\vec{0}\}$ gilt, und L heißt *einfach*, falls L außer L und $\{\vec{0}\}$ keine Ideale enthält und $[LL] \neq \{\vec{0}\}$ gilt.

Bemerkung 1. Es ist $L/\operatorname{Rad} L$ stets halbeinfach (vgl. [4] 3.1).
2. Ist L einfach, so folgt $L = [LL]$, da $[LL]$ ein Ideal in L ist.

Für den Rest des Abschnitts sei K algebraisch abgeschlossen und L halbeinfach. Ferner gelte $\operatorname{char} K = 0$ *und* $\dim_K L < \infty$.
Es lässt sich L dann in eine direkte Summe von einfachen Liealgebren zerlegen (vgl. [4] 5.2). In der Theorie der Liealgebren werden die halbeinfachen Liealgebren durch die reduzierten Wurzelsysteme klassifiziert und die einfachen Liealgebren durch die reduzierten, irreduziblen Wurzelsysteme. Wir gehen nun der Frage nach, wie man L ein Wurzelsystem zuordnen kann.

Adjungierte Darstellung
Für $x \in L$ sei $\operatorname{ad} x \colon L \to L\,,\ y \mapsto [xy]$. Dann ist die *adjungierte Darstellung* $\operatorname{ad} \colon L \to \operatorname{Der}_K(L, L)\,,\ x \mapsto \operatorname{ad} x$, ein Isomorphismus (vgl. [4] 5.3).

Torale Lieunteralgebra
Eine Lieunteralgebra H von L heißt *toral*, falls jedes Element von H halbeinfach ist. Dabei heißt $h \in H$ *halbeinfach*, falls $\operatorname{ad} h = (\operatorname{ad} h)_{\mathrm{s}}$ in der Jordan-Zerlegung von $\operatorname{ad} h$ gemäß 4.2 gilt.

Beispiel
Sei $L = \mathfrak{sl}_n(K) = \{x \in \mathrm{M}_{n\times n}(K) \mid \operatorname{Spur} x = 0\}$. Dann ist die Menge der Diagonalmatrizen in L eine maximale torale Lieunteralgebra von L.

Definition
Man wählt nun in L eine maximale torale Lieunteralgebra H und definiert für jedes $\alpha \in \operatorname{Hom}_K(H, K) =: H^*$ den *Wurzelraum*

$$L_\alpha := \{x \in L \mid (\operatorname{ad} h)(x) = \alpha(h)x \ \ \forall\, h \in H\}$$

und das *Wurzelsystem* $\Phi := \{\alpha \in H^* \mid \alpha \neq 0 \text{ und } L_\alpha \neq \{\vec{0}\}\}$ von L bezüglich H.

Dann ist Φ endlich. Sei $\mathcal{Z}_L(H) := \{x \in L \mid [hx] = 0 \ \ \forall\, h \in H\}$ der *Zentralisator von H in L*. Dann ist $L_0 = \mathcal{Z}_L(H)$, und man hat die folgende *Wurzelraum-Zerlegung*, wobei $\coprod$ die direkte Summe bezeichnet:

$$\boxed{L = \mathcal{Z}_L(H) \oplus \coprod_{\alpha\in\Phi} L_\alpha}\,.$$

Da L halbeinfach ist, gilt $H = \mathcal{Z}_L(H)$, vgl. [4] 8.2. Weiter zeigt man:

(i) Für $\alpha, \beta \in H^*$ gilt $[L_\alpha L_\beta] \subset L_{\alpha+\beta}$, insbesondere $[L_\alpha L_{-\alpha}] \subset L_0 = H$.

(ii) Ist $\alpha \in \Phi$, so ist $-\alpha \in \Phi$.

(iii) Φ erzeugt H^* als K-Vektorraum.

(iv) Sei $\kappa\colon L \times L \to K$, $(x, y) \mapsto \operatorname{Spur}(\operatorname{ad} x \circ \operatorname{ad} y)$ die *Killing-Form*. Ihre Restriktion auf H ist nicht ausgeartet. Es gibt also zu jedem $\alpha \in H^*$ genau ein $t_\alpha \in H$ mit $\alpha(h) = \kappa(t_\alpha, h)$ für alle $h \in H$. Sei $h_\alpha := 2\,\frac{t_\alpha}{\kappa(t_\alpha, t_\alpha)}$.

(v) Zu $\alpha \in \Phi$ und $x_\alpha \neq \vec{0}$ in L_α gibt es ein eindeutig bestimmtes $y_\alpha \in L_{-\alpha}$ so, dass $h_\alpha = [x_\alpha y_\alpha]$ gilt und $x_\alpha, y_\alpha, h_\alpha$ eine dreidimensionale Lieunteralgebra von L erzeugen, die isomorph zu $\mathfrak{sl}_2(K)$ ist vermöge

$$x_\alpha \mapsto \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad y_\alpha \mapsto \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \qquad \text{und} \qquad h_\alpha \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Es ist tatsächlich $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) - \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) - \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

(vi) Für $\alpha, \beta \in \Phi$ und x_α, y_α, h_α wie in (v) sind die *Cartan-Zahlen* $\beta(h_\alpha)$ in $\mathbb{Z}$, und es gilt $\beta - \beta(h_\alpha)\,\alpha \in \Phi$.

(vii) Sei $\Delta = \{\alpha_1, \ldots, \alpha_\ell\}$ eine Basis von H^*, die aus Wurzeln besteht. Dann ist jede Wurzel $\beta \in \Phi$ darstellbar als $\beta = \sum_{i=1}^{\ell} q_i \alpha_i$ mit $q_i \in \mathbb{Q}$ für alle $i = 1, \ldots, \ell$ (da $\operatorname{char} K = 0$).

(viii) Sei $\mathbb{E}_\mathbb{Q}$ der von Φ erzeugte $\mathbb{Q}$-Untervektorraum von H^*. Dann ist $\dim_\mathbb{Q} \mathbb{E}_\mathbb{Q} = \dim_K H^*$. Die durch die Killing-Form in (iv) induzierte Form $H^* \times H^* \to K$ ergibt mit (vii) eine positiv definite, symmetrische Bilinearform $\mathbb{E}_\mathbb{Q} \times \mathbb{E}_\mathbb{Q} \to \mathbb{Q}$. Man setzt $\mathbb{E} = \mathbb{E}_\mathbb{Q} \otimes_\mathbb{Q} \mathbb{R}$ und realisiert Φ als reduziertes Wurzelsystem gemäß 7.2.

(ix) Die Korrespondenz $(L, H) \longmapsto (\Phi, \mathbb{E})$ ist bijektiv.

Die Beweise von (i) bis (ix) stehen in [4] §§ 8, 18.

7.11 Wurzelsystem einer halbeinfachen Gruppe

Seien K algebraisch abgeschlossen, $G \neq \{e\}$ eine zusammenhängende lineare algebraische Gruppe, T ein Torus in G und $\mathfrak{g}$ die Liealgebra von G wie in 6.8. Ferner sei

$$\operatorname{Ad}\colon G \longrightarrow \operatorname{Aut}(\mathfrak{g}) \subset \operatorname{GL}(\mathfrak{g})$$

die in 6.9 eingeführte adjungierte Darstellung von G.

Sei $X^*(T)$ die Charaktergruppe von T, wie in 5.3 definiert. Für jeden Charakter $\alpha \in X^*(T)$ setzen wir

$$\mathfrak{g}_\alpha := \{x \in \mathfrak{g} \mid (\operatorname{Ad} t)(x) = \alpha(t)x \ \ \forall\, t \in T\}\,.$$

Ist $\mathfrak{g}_\alpha \neq \{\vec{0}\}$, so heißt α ein *Gewicht* und $\mathfrak{g}_\alpha$ ein *Gewichtsraum* von T in $\mathfrak{g}$.

Satz
Vektoren $\neq \vec{0}$ aus verschiedenen Gewichtsräumen von T in $\mathfrak{g}$ sind stets linear unabhängig. Insbesondere gibt es nur endlich viele Gewichte von T in $\mathfrak{g}$.

Beweis. Andernfalls gibt es zu minimal gewähltem $n \geqslant 2$ paarweise verschiedene Charaktere $\alpha_1, \ldots, \alpha_n$ und Vektoren $x_i \in \mathfrak{g}_{\alpha_i}$ mit $x_i \neq \vec{0}$ für $i = 1, \ldots, n$ so, dass $x_1 + \cdots + x_n = \vec{0}$.
Da $\alpha_1 \neq \alpha_2$ ist, gibt es ein $t \in T$ mit $\alpha_1(t) \neq \alpha_2(t)$. Es folgt

$$\vec{0} = (\operatorname{Ad} t)\left(\sum_{i=1}^{n} x_i\right) \underset{\text{Def. von } \mathfrak{g}_{\alpha_i}}{=} \sum_{i=1}^{n} \alpha_i(t)x_i\,,$$

und nach Multiplikation mit $\alpha_1(t)^{-1}$ folgt $\vec{0} = x_1 + \sum_{i=2}^{n} \alpha_1(t)^{-1}\alpha_i(t)x_i$. Subtrahiert man hiervon $\sum_{i=1}^{n} x_i = \vec{0}$, so ergibt sich eine Linearkombination $\sum_{i=2}^{n} \lambda_i x_i = \vec{0}$ mit $\lambda_i \in K$ im Widerspruch zur Minimalität von n.
Da $\dim_K \mathfrak{g} < \infty$ ist, folgt auch die zweite Behauptung. □

Sei nun T ein maximaler Torus in G, und sei Φ die Menge der Gewichte $\neq 1$. Setzen wir $\mathfrak{g}^T := \{x \in \mathfrak{g} \mid (\operatorname{Ad} t)(x) = x \ \ \forall\, t \in T\}$, so gilt

$$\boxed{\mathfrak{g} = \mathfrak{g}^T \oplus \coprod_{\alpha \in \Phi} \mathfrak{g}_\alpha}\,.$$

Man identifiziert die Charaktergruppe $X^*(T)$ mit ihrem Bild in $\mathbb{E} := X^*(R) \otimes_{\mathbb{Z}} \mathbb{R}$. Nach 5.4 $(a) \Longrightarrow (b)$ ist $X^*(T)$ endlich erzeugt als $\mathbb{Z}$-Modul und also $\mathbb{E}$ endlich-dimensional als $\mathbb{R}$-Vektorraum. Es gilt $\dim_{\mathbb{R}} \mathbb{E} = \dim T$, wie aus 5.6 folgt. Man versieht dann $\mathbb{E}$ mit einer positiv definiten, symmetrischen Bilinearform, die invariant unter der Operation der Weylgruppe $\mathcal{W}(G,T)$ ist (vgl. 7.12 unten). Um zu Klassifikationsresultaten für „halbeinfache“ Gruppen G zu gelangen, benutzt man im Fall, dass $\operatorname{char} K = 0$ ist, die Wurzelraum-Zerlegung von $L = \mathfrak{g}$ aus 7.10. Im Allgemeinen benutzt man die Theorie der „Borelgruppen“ in G. Dabei ist eine *Borelgruppe* eine maximale zusammenhängende, auflösbare Untergruppe von G, und G heißt *halbeinfach*, falls das Radikal $\operatorname{Rad} G := (\bigcap_{B \text{ Borelgr.}} B)^0$ trivial ist.

Sei nun G halbeinfach, dann heißen die Gewichte $\neq 1$ *Wurzeln* von G, und die Menge $\Phi(G)$ aller dieser Wurzeln ist ein reduziertes Wurzelsystem in $\mathbb{E}$. Die Menge $\Phi(G)$ hängt bis auf Isomorphie nicht von der Wahl des maximalen Torus T ab und heißt *Wurzelsystem von* G. Die Borelgruppen in G sind konjugiert und ebenso die maximalen Tori in G, vgl. z. B. [5] 21.3.

Beispiel
Sei $G = \mathrm{SL}_{n+1}(K)$. Dann ist die Gruppe der oberen Dreiecksmatrizen

$$\mathrm{B}_{n+1}(K) := \left\{ \begin{pmatrix} * & \dots & * \\ & \ddots & \vdots \\ 0 & & * \end{pmatrix} \in G \right\}$$

eine Borelgruppe in G, und die Gruppe der Diagonalmatrizen

$$T := \left\{ \begin{pmatrix} t_1 & & 0 \\ & \ddots & \\ 0 & & t_{n+1} \end{pmatrix} =: t \in G \right\}$$

ist ein Torus der (maximalen) Dimension n in G. Sei $\mathrm{D}_{n+1}(K)$ die Gruppe der Diagonalmatrizen in $\mathrm{GL}_{n+1}(K)$. Für $i = 1, \dots, n+1$ definiert man Charaktere $e_i \colon \mathrm{D}_{n+1}(K) \to \mathbb{G}_m(K),\ t \mapsto t_i$ (wie in Beispiel 5.3) und für $i = 1, \dots, n$ Charaktere $\alpha_i \colon T \to \mathbb{G}_m(K),\ t \mapsto t_i\, t_{i+1}^{-1} =: t^{e_i - e_{i+1}}$. Man erahnt hieran schon, dass die Gruppe $\mathrm{SL}_{n+1}(K)$ eine halbeinfache Gruppe vom Typ A_n ist (vgl. 7.9).

7.12 Weylgruppe $\mathcal{W}(G,T)$

Sei T ein maximaler Torus in einer zusammenhängenden linearen algebraischen Gruppe G über einem algebraisch abgeschlossenen Körper K. Die *Weylgruppe von* G *bezüglich* T is definiert als

$$\boxed{\mathcal{W}(G,T) := \mathcal{N}_G(T)/\mathcal{Z}_G(T)}.$$

Nach Satz 5.10 ist $\mathcal{W}(G,T)$ eine endliche Gruppe. Für $g \in \mathcal{N}_G(T)$ und $\alpha \in X^*(T)$ definiert man ein Element $g.\alpha \in X^*(T)$ durch

$$(g.\alpha)(t) := \alpha(gtg^{-1}) \qquad \forall\, t \in T$$

und erhält damit durch

$$g \longmapsto \begin{cases} X^*(T) \longrightarrow X^*(T), \\ \qquad \alpha \longmapsto g.\alpha\,, \end{cases}$$

Einbettungen $\mathcal{W}(G,T) \hookrightarrow \mathrm{Aut}(X^*(T))$ und $\mathcal{W}(G,T) \hookrightarrow \mathrm{GL}(\mathbb{E})$ mit $\mathbb{E} := X^*(T) \otimes_{\mathbb{Z}} \mathbb{R}$.

Lemma
Es gibt eine positiv definite, symmetrische Bilinearform

$$b\colon \mathbb{E}\times\mathbb{E}\longrightarrow\mathbb{R}\,,\ \ (\alpha,\beta)\longmapsto b(\alpha,\beta),$$

die invariant unter der Weylgruppe $\mathcal{W}(G,T)$ ist, d. h. $b(\alpha,\beta)=b(w.\alpha,w.\beta)$ für alle $\alpha,\beta\in\mathbb{E}$, $w\in\mathcal{W}(G,T)$.

Beweis. Sei $b'\colon \mathbb{E}\times\mathbb{E}\longrightarrow\mathbb{R}$ irgendeine positiv definite, symmetrische Bilinearform. Setze $b(\alpha,\beta)=\sum_{w\in\mathcal{W}(G,T)} b'(w.\alpha,w.\beta)\,.$ □

Sei $\mathbb{E}$ mit einer solchen Bilinearform wie im Lemma versehen. Wir definieren nun wie in [11] 7.1 ein Wurzelsystem $\Phi(G,T)$. Ist α ein Gewicht $\neq 1$ von G bezüglich T wie in 7.11 definiert, so ist $S_\alpha := (\operatorname{kern}\alpha)^0$ ein Untertorus von T. Man setzt $G_\alpha := \mathcal{Z}_G(S_\alpha)$. Dann ist G_α eine abgeschlossene Untergruppe von G nach Lemma 5.10, und es gilt:

(1) G wird von den G_α erzeugt, wobei α alle Gewichte $\neq 1$ durchläuft.

(2) G ist auflösbar $\Longleftrightarrow$ G_α ist auflösbar für alle Wurzeln α.

Sei $\Phi(G,T) := \{\text{Gewichte } \alpha\neq 1 \mid G_\alpha \text{ ist nicht auflösbar}\}$. Die Elemente von $\Phi(G,T)$ heißen *Wurzeln* von G bezüglich T. Man kann zeigen, dass $\mathcal{W}(G,T)$ von den Spiegelungen

$$s_\alpha\colon \mathbb{E}\longrightarrow\mathbb{E}\,,\ \ \beta\longmapsto\beta-2\,\frac{b(\beta,\alpha)}{b(\alpha,\alpha)}\,\alpha\,,$$

mit $\alpha\in\Phi(G,T)$ erzeugt wird (vgl. [11] 7.1.9).

7.13 Übungsaufgaben 51–53

Aufgabe 51
Es sei D_n die Diedergruppe mit $2n$ Elementen für $n=2,3,4,6$. Man beweise, dass tatsächlich, wie in 7.3 behauptet, gilt: $\mathcal{W}(A_1\times A_1)\simeq D_2$, $\mathcal{W}(A_2)\simeq D_3$, $\mathcal{W}(B_2)\simeq D_4$ und $\mathcal{W}(G_2)\simeq D_6$.

Aufgabe 52
Man zeige durch Angabe eines Beispiels, dass $\alpha-\beta$ eine Wurzel in einem reduzierten Wurzelsystem sein kann, auch wenn $\langle\alpha,\beta\rangle\leqslant 0$ gilt (vgl. Lemma 7.4 und Korollar 7.6).

Aufgabe 53
Sei Δ eine Wurzelbasis von $\mathbb{E}$. Man zeige, dass es ein $\gamma\in\mathbb{E}$ so gibt, dass $\langle\gamma,\alpha\rangle>0$ für alle $\alpha\in\Delta$ gilt.

8 Formulierung von Klassifikationssätzen

In 7.7 und 7.9 haben wir bereits Klassifikationsergebnisse kennengelernt:

Klassifikation von zusammenhängenden Coxetergraphen
Jeder zusammenhängende Coxeter-Graph, der zu einem Wurzelsystem gehört, ist isomorph zu einem der Graphen $A_n, B_n, D_n, E_6, E_7, E_8, F_4, G_2$.

Klassifikation von irreduziblen, reduzierten Wurzelsystemen
Bis auf Isomorphie entsprechen die irreduziblen, reduzierten Wurzelsysteme bijektiv den Dynkin-Diagrammen A_n , $n \geqslant 1$, B_n , $n \geqslant 2$, C_n , $n \geqslant 3$, D_n , $n \geqslant 4$, E_6, E_7, E_8, F_4 *und* G_2 .

8.1 Klassifikation eindimensionaler Gruppen

Satz (vgl. Bemerkung 5.2 und [11] 3.4.9.)
Jede zusammenhängende lineare algebraische Gruppe der Dimension 1 *ist isomorph zu* $\mathbb{G}_{\mathrm{m}}(K)$ *oder zu* $\mathbb{G}_{\mathrm{a}}(K)$.

8.2 Halbeinfache und reduktive Gruppen

Sei K ein algebraisch abgeschlossener Körper, und sei G im Folgenden stets eine zusammenhängende lineare algebraische Gruppe über K .
Man nennt G *halbeinfach*, falls das Radikal $\operatorname{Rad} G := (\bigcap_{B \in \mathcal{B}} B)^0$ trivial ist, wobei $\mathcal{B}$ die Menge der Borelgruppen in G bezeichnet, vgl. [2] 11.21. Es ist dann $\operatorname{Rad} G$ ein maximaler zusammenhängender, auflösbarer Normalteiler in G . Der unipotente Teil $\operatorname{Rad}_{\mathrm{u}}(G)$ von $\operatorname{Rad} G$ wird das *unipotente Radikal* von G genannt. Es ist $\operatorname{Rad}_{\mathrm{u}}(G)$ ein maximaler zusammenhängender, unipotenter Normalteiler von G . Man nennt G *halbeinfach*, falls $\operatorname{Rad} G = \{e\}$ und $G \neq \{e\}$ gilt, und *reduktiv*, falls $\operatorname{Rad}_{\mathrm{u}}(G) = \{e\}$ gilt.

Beispiele
$\mathrm{SL}_n(K)$ und $G/\operatorname{Rad} G$ sind halbeinfach, $\mathrm{GL}_n(K)$, jeder Torus und jede halbeinfache Gruppe sind reduktiv, ebenso $G/\operatorname{Rad}_{\mathrm{u}}(G)$.

Bemerkung (vgl. [5] 21.3)
Alle maximalen Tori T in G sind konjugiert. Daher ist $\operatorname{rang} G := \dim T$ wohldefiniert.

8.3 Klassifikation halbeinfacher Gruppen vom Rang 1

Satz (vgl. [11] 7.2.4.)
Jede halbeinfache Gruppe vom Rang 1 *ist isomorph zu* $\mathrm{SL}_2(K)$ *oder zu* $\mathrm{PSL}_2(K)$, *wobei* $\mathrm{PSL}_2(K) = \mathrm{SL}_2(K)/\{\pm E_2\}$ *mit* $E_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

8.4 Klassifikation reduktiver Gruppen

Gegeben sei ein 4-Tupel $\Psi = (X, \Phi, X^\vee, \Phi^\vee)$, wobei $X, X^\vee$ endlich erzeugte freie abelsche Gruppen und $\Phi \subset X$ und $\Phi^\vee \subset X^\vee$ endliche Teilmengen sind. Es gebe eine *Dualitätspaarung* $\langle -, - \rangle \colon X \times X^\vee \longrightarrow \mathbb{Z}$ $(x, w) \longmapsto \langle x, w \rangle$, und eine Bijektion $\Phi \longrightarrow \Phi^\vee$, $\alpha \longmapsto \alpha^\vee$, sowie Automorphismen

$$s_\alpha \colon X \longrightarrow X\,,\ x \longmapsto x - \langle x, \alpha^\vee \rangle\, \alpha\,,$$
$$\text{und} \quad s_{\alpha^\vee} \colon X^\vee \longrightarrow X^\vee\,,\ w \longmapsto w - \langle \alpha, w \rangle\, \alpha^\vee\,,$$

für alle $\alpha \in \Phi$. Dann heißt Ψ ein *Wurzeldatum*, wenn $\langle \alpha, \alpha^\vee \rangle = 2$ für alle $\alpha \in \Phi$ sowie $s_\alpha(\Phi) \subset \Phi$ und $s_{\alpha^\vee}(\Phi^\vee) \subset \Phi^\vee$ gilt.
(Eine *Dualitätspaarung* ist stets bilinear und induziert einen Isomorphismus $X^\vee \xrightarrow{\sim} \mathrm{Hom}(X, \mathbb{Z})$, $w \longmapsto (\alpha \mapsto \langle \alpha, w \rangle)$.)
Es gilt dann $s_\alpha^2 = \mathrm{id}$ und $s_\alpha(\alpha) = -\alpha$. Tensorieren wir die von Φ erzeugte Untergruppe von X über $\mathbb{Z}$ mit $\mathbb{R}$, so erhalten wir einen $\mathbb{R}$-Vektorraum W, und falls $\Phi \neq \emptyset$ gilt, ist Φ ein Wurzelsystem in W d. h. in diesem Kontext (vgl. [11] 7.4.1 und [3] Chap. VI § 1):

1) Φ ist endlich, erzeugt W und enthält nicht 0.
2) Zu jedem $\alpha \in \Phi$ gibt es ein $\alpha^\vee$ im Dualraum von W so, dass $\langle \alpha, \alpha^\vee \rangle = 2$ und $s_\alpha(\Phi) = \Phi$ für alle $\alpha \in \Phi$ gilt.
3) Für jedes $\alpha \in \Phi$ ist $\alpha^\vee(\Phi) \subset \mathbb{Z}$.

Ein *Isomorphismus* $\Psi_1 \to \Psi$ von Wurzeldaten $\Psi = (X, \Phi, X^\vee, \Phi^\vee)$ und $\Psi_1 = (X_1, \Phi_1, X_1^\vee, \Phi_1^\vee)$ ist ein Isomorphismus $X \simeq X_1$ so, dass Φ auf Φ_1 und $\Phi_1^\vee$ auf $\Phi^\vee$ abgebildet wird.

Sei G nun eine zusammenhängende lineare algebraische Gruppe, und sei T ein maximaler Torus in G. Dann können wir dem Paar (G, T) ein Wurzeldatum Ψ so zuordnen: Es sei $X = X^*(T) = \mathrm{Mor}(T, \mathbb{G}_\mathrm{m})$ die Gruppe der Charaktere und $X^\vee = X_*(T) = \mathrm{Mor}(\mathbb{G}_\mathrm{m}, T)$ die Gruppe der *Kocharaktere*, wobei $\mathbb{G}_\mathrm{m} := \mathbb{G}_\mathrm{m}(K)$ sei. Es ist $X^*(T)$ eine endlich erzeugte freie abelsche Gruppe (vgl. 5.6) (c), und man erhält eine Dualitätspaarung

$$X^*(T) \times X_*(T) \longrightarrow \mathbb{Z}\,,\ (\alpha, w) \longmapsto \langle \alpha, w \rangle\,,$$

wobei $\langle \alpha, w \rangle$ durch $\alpha(w(x)) = x^{\langle \alpha, w \rangle}$ für $x \in \mathbb{G}_\mathrm{m}$ definiert ist. Es sei $\Phi = \Phi(G, T)$ die Menge Wurzeln wie in 7.12 definiert und $\Phi^\vee = \Phi(G, T)$ die Menge Kowurzeln. Es ist Φ ein reduziertes Wurzelsystem.
Seien nun G, G_1 reduktive Gruppen, und es sei (G_1, T_1) ein weiteres Paar mit Wurzeldatum Ψ_1. Ist $\varphi \colon G \to G_1$ ein Isomorphismus algebraischer Gruppen mit $\varphi(T) = T_1$, dann gibt es einen induzierten Isomorphismus $f(\varphi) \colon \Psi_1 \simeq \Psi$ von Wurzeldaten. Umgekehrt gilt folgender Isomorphiesatz.

Isomorphisatz vgl. [11] 9.6.2.
Ist $f\colon \Psi_1 \simeq \Psi$ ein Isomorphismus von Wurzeldaten, so gibt es einen Isomorphismus $\varphi\colon G \to G_1$ von algebraischen Gruppen mit $\varphi(T) = T_1$ und $f = f(\varphi)$. Ist φ' ein weiterer solcher Isomorphismus, so gibt es ein $t \in T$ so, dass $\varphi'(g) = \varphi(tgt^{-1})$ für alle $g \in G$ gilt.

Existenzsatz, vgl. [11] 10.1.1.
Zu jedem Wurzeldatum Ψ gibt es eine reduktive Gruppe G mit einem maximalen Torus T so, dass $\Psi(G,T) \simeq \Psi$ gilt.

8.5 Klassifikation halbeinfacher Gruppen

Bemerkung
Die halbeinfachen Gruppen kann man bis auf endliche Untergruppen durch die Dynkin-Diagramme klassifizieren. Eine halbeinfache Gruppe G heißt *einfach*, wenn G keinen nichttrivialen zusammenhängenden Normalteiler besitzt. Sei G eine halbeinfache Gruppe und T ein maximaler Torus in G. Man kann zeigen, dass G genau dann einfach ist, wenn das Wurzelsystem $\Phi(G)$ aus 7.11 irreduzibel ist. Man kann sich dann auf die Klassifikation einfacher Gruppen beschränken und erhält über die Wurzelsysteme eine Klassifikation mittels Dynkin-Diagrammen. Aus dem Existenzsatz folgt, dass zu jedem der Typen $A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4, G_2$ auch tatsächlich algebraische Gruppen gehören. Zum Beispiel ist die Gruppe $\mathrm{SO}_{2n+1}(K)$ vom Typ B_n und die Gruppe $\mathrm{SO}_{2n}(K)$ vom Typ D_n. Zu diesen beiden Typen gehören auch noch gewisse „Spingruppen“. Zum Typ G_2 gehört die Automorphismengruppe einer *Cayleyalgebra*, und zum Typ F_4 gehört die Automorphismengruppe einer 27-dimensionalen *Jordanalgebra*. Eine Übersicht über alle Gruppen, die zu den verschiedenen Typen gehören, ist in [13], [11] § 17 und [8] § 25 gegeben. Es wird dort auch der Fall eines beliebigen, nicht notwendig algebraisch abgeschlossenen Grundkörpers behandelt.

Literaturverzeichnis

[1] Atiyah, M. S., MacDonald I. G.: *Introduction to Commutative Algebra.* Addison-Wesley, 1969.

[2] Borel, Armand: *Linear Algebraic Groups, Second Enlarged Edition.* Springer, 1991.

[3] Bourbaki, N.: *Groupes et algèbres de Lie, Chap. 4, 5 et 6.* Hermann, 1968.

[4] Humphreys, James E.: *Introduction to Lie Algebras and Representation Theory.* Springer, 1972.

[5] Humphreys, James E.: *Linear Algebraic Groups.* Springer, 1981.

[6] Jacobson, Nathan: *Lie Algebras.* John Wiley & Sons, 1962.

[7] Kersten, Ina: *Analytische Geometrie und Lineare Algebra I und II,* sowie *Algebra.* Universitätsverlag Göttingen, 2005/06.

[8] Knus-Merkurjev-Rost-Tignol: *The Book of Involutions.* Amer. Math. Soc. Colloquium Publ. 44, 1998.

[9] Kunz, Ernst: *Einführung in die algebraische Geometrie.* vieweg studium, 1997.

[10] Serre, J-P.: *Complex Semisimples Lie Algebras.* Springer, 1987.

[11] Springer, T.: *Linear Algebraic Groups, Second Edition.* Birkhäuser, 1998.

[12] Steinberg, R.: *Conjugacy Classes in Algebraic Groups.* Springer Lecture Notes 366, 1974.

[13] Tits, Jacques: *Classification of Algebraic Semisimple Groups.* Proc. Sympos. Pure Math, vol 9, Amer. Math. Soc. pp. 33–62, 1966.

Index

Dieser Universitätsdruck wendet sich an Studierende der Mathematik ab dem vierten Semester und schließt sich an die vorangegangenen Universitätsdrucke in Linearer Algebra 1,2 und Algebra an. Es werden zunächst viele Beispiele angegeben und Grundbegriffe aus der algebraischen Geometrie bereitgestellt. Weitere Kapitel behandeln Definition und grundlegende Eigenschaften linearer algebraischer Gruppen. Danach werden Lie-Algebren, Wurzelsysteme und Dynkin-Diagramme eingeführt, um damit seit langem bekannte und berühmte Klassifikationssätze zu formulieren.

GEORG-AUGUST-UNIVERSITÄT
GÖTTINGEN

ISBN 978-3-940344-05-2

Universitätsdrucke Göttingen