Lineare Algebraische Gruppen
– Arbeitsversion –

Prof. Dr. Ina Kersten
geTEXt von Ole Riedlin

20. März 2002

Inhaltsverzeichnis

0 Worum geht es?

Wir gehen von einem Körper K aus.
Lineare Gruppen sind Untergruppen einer „allgemeinen linearen Gruppe“

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

Verknüpfung: Matrizenmultiplikation

mit $n \in \mathbb{N}$.
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 $K[(X_{ij})_{1\leq i,j\leq n}]$ aufgefasst werden kann, folgt aus der *Leibniz-Formel* für die Determinante. Für $x = (x_{ij}) \in \mathrm{M}_{n\times n}(K)$ gilt

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

(vgl. Aufgabe 1).

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 $X_{ij} = \delta_{ij}$ mit dem Kronecker-Symbol $\delta_{ij} = \begin{cases} 1 & \text{für } i = j \\ 0 & \text{für } i \neq j \end{cases}$ definiert.

6) Die *orthogonale Gruppe*

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

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.

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

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

Analog ist für $n > 1$ die orthogonale Gruppe $\mathrm{O}_n(\mathbb{R})$ durch n^2 polynomiale Gleichungen definiert.

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

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

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

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

$$\begin{aligned} G \times G &\longrightarrow G,\ (x,y) \longmapsto x \circ y, \\ G &\longrightarrow G,\ x \longmapsto x^{-1}, \end{aligned}$$

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.

Beispiele1) Die additive Gruppe $\mathbb{G}_{\mathrm{a}}(K) = \{x \in K\}$ ist durch das Nullpolynom definiert und hat die Gruppenstruktur

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

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.
Verknüpfung: $(a,b)(a',b') = (aa' - bb', ab' + a'b)$
Inverses: $(a,b)^{-1} = (a,-b)$
Einselement: $(1,0)$
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. AGLA 11.8.
Jede Matrix $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$ hat die Form $\left(\begin{smallmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{smallmatrix}\right)$ mit $\varphi \in \mathbb{R}$ und $0 \leq \varphi \leq 2\pi$. Man erhält Isomorphien

$$S^1(\mathbb{R}) \simeq \underbrace{\mathrm{SO}_2(\mathbb{R})}_{\text{spez. orth. Gruppe}} \simeq \mathbb{R}^+/2\pi\mathbb{Z} \simeq \mathbb{R}^+/\mathbb{Z} \simeq \underset{\text{Torus}}{\bigcirc}$$

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

$$\begin{aligned} \mathrm{SO}_2(\mathbb{C}) \xrightarrow{\sim} \mathbb{G}_{\mathrm{m}}(\mathbb{C}) \simeq \mathbb{C}^*, \quad \begin{pmatrix} z_1 & -z_2 \\ z_2 & z_1 \end{pmatrix} &\longmapsto T \begin{pmatrix} z_1 & -z_2 \\ z_2 & z_1 \end{pmatrix} T^{-1} \\ &= \begin{pmatrix} z_1 - iz_2 & 0 \\ 0 & z_1 + iz_2 \end{pmatrix} = \begin{pmatrix} z_1 - iz_2 & 0 \\ 0 & (z_1 - iz_2)^{-1} \end{pmatrix} . \end{aligned}$$

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

Sei L ein algebraisch abgeschlossener Körper (d.h. jedes nicht konstante Polynom aus $L[X]$ hat eine Nullstelle in L, vgl. AGLA 21.1). Chevalley hat in den Jahren 1955–58 die „halbeinfachen" algebraischen Gruppen 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 die Struktur linearer algebraischer Gruppen untersuchen und den Klassifikationssatz formulieren.

0.4 Aufgaben

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

Aufgabe 2
Für ein Ideal I in R sei I^e das von $\varphi(I)$ in S erzeugte Ideal, also

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

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

$$\iota_A \colon R \longrightarrow A\,.$$

Es ist dann A ein R-Modul mit der Skalarmultiplikation $ra := \iota_A(r)\,a$ $\forall\, r \in R\,,\ a \in A\,.$

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 21.3).

Definition
Ein Homomorphismus $\varphi\colon A \longrightarrow B$ 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

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

mit $\varphi(X_i) = y_i$ für $i = 1, \dots, n$, den sogenannten *Einsetzhomomorphismus* (dieser ist eindeutig bestimmt, wie aus Algebra 21.6 folgt). Es ist dann

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

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

Bemerkung1) 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.a. 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.

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

(a) L ist endlich dimensional als K-Vektorraum ($\underset{AGLA}{\Longleftrightarrow}$ 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.a. jedoch nicht.

Beispiel

Sei K ein Körper. Der Quotientenkörper $L := K(X_1, \dots, X_n)$ des Polynomrings $A := K[X_1, \dots, X_n]$ 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 $h_1 = \frac{f_1}{g_1}, \dots, h_m = \frac{f_m}{g_m}$ mit $f_i, g_i \in A$, $g_i \neq 0$ für $i = 1, \dots, m$.
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 8.10 und 9.4).
Da A unendlich viele Primelemente besitzt, gibt es ein Primelement $p \in A$ mit $p \nmid g_i \ \forall\, i = 1, \dots, m$. Dann ist aber $h = \frac{1}{p}$ nicht so darstellbar wie oben beschrieben. Widerspruch. $\square$

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 $f(a + bi) = 0 \; \forall \, a, b \in \mathbb{Z}$.

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

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

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

$$ss_j = a_{j1}s_1 + \cdots + a_{jn}s_n \quad \text{für gewisse} \quad a_{j1}, \ldots, a_{jn} \in R \text{ und } j = 1, \ldots, n\,,$$

und für die Matrix $A = (a_{ij})_{1 \le i,j \le n}$ gilt

$$A \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} ss_1 \\ \vdots \\ ss_n \end{pmatrix} \text{ bezüglich Matrizenmultiplikation.}$$

Es folgt

$$(*) \qquad \boxed{(A - sE_n) \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}}$$

mit der Einheitsmatrix $E_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$.

Zeige nun, dass s Nullstelle des charakteristischen Polynoms $\det(A - XE_n)$ ist. Sei $\boxed{B := A - sE_n}$, und sei $\widetilde{B} = (\widetilde{b}_{ik}) \in \mathrm{M}_{n \times n}(R)$ mit $\widetilde{b}_{ik} := (-1)^{i+k} \det(B_{ki})$, wobei B_{ki} aus B durch Streichen der k-ten Zeile und i-ten Spalte entsteht, vgl. AGLA 6.10.

Es ist $\widetilde{B}B = (c_{ij})$ mit $c_{ij} = \sum\limits_{k=1}^{n} \widetilde{b}_{ik} b_{kj} = \begin{cases} \det(B) & \text{für } i = j \\ \det(C) & \text{für } i \neq j\,, \end{cases}$

wobei C aus B entsteht, wenn man in B die i-te Spalte durch die j-te Spalte ersetzt (vgl. Laplacescher Entwicklungssatz AGLA 6.5). In C sind zwei Spalten gleich, also $\det(C) = 0$, und es folgt $\widetilde{B}B = \det(B) \cdot E_n$. Nach $(*)$ gilt

$$B \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \quad \text{und also} \quad \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \widetilde{B}B \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \det(B)E_n \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}.$$

Es folgt $\det(B)s_i = 0 \; \forall\, i = 1, \ldots, n$.
Da es nach Voraussetzung $\lambda_1, \ldots, \lambda_n \in R$ mit $1 = \lambda_1 s_1 + \cdots + \lambda_n s_n$ gibt, folgt $\det(B) \cdot 1 = 0$. □

1.5 Charakterisierung endlicher Ringerweiterungen

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

Korollar *(a) Für $s \in S$ gilt:*

$$\boxed{s \textit{ ganz über } R} \quad \Longleftrightarrow \quad \boxed{R[s] \textit{ endlich über } R}$$

(b) Es sind äquivalent:

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

Bemerkung
Seien $K \subset L$ Körper. Dann ist (a) die ringtheoretische Version von Algebra 11.12:

$$\boxed{x \text{ algebraisch über } K} \quad \Longleftrightarrow \quad \boxed{[K(x):K] < \infty}$$

und (b) die von Algebra 12.3:

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

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 $\mathrm{grad}(r) < \mathrm{grad}(f)$ (oder $r = 0$).
Es folgt $g(s) = h(s)\underbrace{f(s)}_{=0} + r(s) = r(s)$.
Also bilden $1, s, \ldots, s^{n-1}$ ein Erzeugendensystem von $R[s]$ als R-Modul ($n = \mathrm{grad}(f)$).

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

(b) „(i)$\Longrightarrow$(ii)"

$$\begin{tikzcd}
S \text{ endlich über } R \arrow[rr, Rightarrow, "1.4"'] \arrow[dr, Rightarrow] & & S \text{ ganz über } R \\
& \text{Behauptung} \arrow[ur, Rightarrow] &
\end{tikzcd}$$

„(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.

$\square$

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 eine Gleichung

$$\boxed{t^n + s_{n-1}t^{n-1} + \cdots + s_0 = 0 \quad \text{mit} \quad s_0, \ldots, s_{n-1} \in S}.$$

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. Nach 1.5(a) und (b) ist t dann ganz über R. □

1.7 Homogene Bestandteile eines Polynoms

Definition
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

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

mit Koeffizienten $a_{m_1\ldots m_n} \in R$, die bis auf endlich viele Null sind (und $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$).
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
$X^2 - X_1X_2 + 5X_2^2$ 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 $f_d \neq 0$, und es ist

$$\boxed{f = f_0 + f_1 + \cdots + f_d},$$

wobei f_j homogen vom Grad j ist (Es gilt 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

$$R[X_1, \ldots, X_n] \longrightarrow S,\ f \longmapsto f(x_1, \ldots, x_n)\,,$$

injektiv ist. In diesem Fall kann man den Unterring $R[x_1, \ldots, x_n]$ von S als Polynomring auffassen.

1.9 Noethersches Normalisierungslemma

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

Beweis. Der Beweis wird geführt für den Fall, 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 $x_1, \ldots, x_n \in A$ mit $A = K[x_1, \ldots, x_n]$ (vgl. 1.2.1).
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.
$n \geq 2$: Zerlege f in seine homogenen Bestandteile $f = f_0 + \cdots + f_d$ mit $f_d \neq 0$ wie in 1.7. Da K unendlich ist, gibt es $\lambda_1, \ldots, \lambda_{n-1} \in K$ 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 $g_i \in K[y_1, \dots, y_{n-1}]$ für $i = 1, \dots, d$.
Also ist x_n und damit A ganz über $K[y_1, \dots, y_{n-1}]$. Nach Induktionsvoraussetzung ist $K[y_1, \dots, y_{n-1}]$ ganz über K, oder es gibt über K algebraisch unabhängige Elemente $Y_1, \dots, Y_m$ so, daß $K[y_1, \dots, y_{n-1}]$ ganz über $K[Y_1, \dots, Y_m]$ 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 $R := K[Y_1, \dots, Y_m]$, und R wäre nach Satz 1.3 ein Körper. Widerspruch, da $Y_1, \dots, Y_m$ in R nicht invertierbar sind (nach Algebra 6.13). □

Satz
Sei K ein algebraisch abgeschlossener Körper. Dann sind die maximalen Ideale im Polynomring $K[X_1, \dots, X_n]$ genau die Ideale $(X_1 - a_1, \dots, X_n - a_n)$ mit $a_1, \dots, a_n \in K$.

Beweis. Die Ideale $(X_1 - a_1, \dots, X_n - a_n)$ sind maximal nach Aufgabe 5.
Sei nun $\mathfrak{m}$ ein beliebiges maximales Ideal in $K[X_1, \dots, X_n]$. Dann ist
$L := K[X_1, \dots, X_n]/\mathfrak{m}$ 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 $K \hookrightarrow K[X_1, \dots, X_n]/\mathfrak{m} = K$. Es gibt daher $a_1, \dots, a_n \in K$ mit $a_i + \mathfrak{m} = X_i + \mathfrak{m}$, d.h. mit $X_i - a_i \in \mathfrak{m} \; \forall \, i = 1, \dots, n$ (vgl. Algebra 7.2).
Da $I = (X_1 - a_1, \dots, X_n - a_n)$ 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 $K[X_1, \dots, X_n]$, nämlich

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

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 21.2, 21.4). Für eine nichtleere Teilmenge $I \subset K[X_1, \dots, X_n]$ 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* $K[X_1, \dots, X_n]$ *, so ist* $\mathfrak{V}(I) \neq \emptyset$ *.*

Beweis. Nach Algebra 7.6 ist I in einem maximalen Ideal $\mathfrak{m}$ von $K[X_1, \dots, X_n]$ enthalten. Es ist dann $L := K[X_1, \dots, X_n]/\mathfrak{m}$ 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 21.5). Setze $x_i = X_i + \mathfrak{m}$ für $i = 1, \dots, n$ in L . Dann ist $(x_1, \dots, x_n) \in V(\mathfrak{m}) \subset \mathfrak{V}(I)$. □

Korollar
Seien $f_1, \dots, f_m \in K[X_1, \dots, X_n]$ *. Dann hat das System*

$$f_1 = 0\,, \dots,\, f_m = 0$$

genau dann keine Lösung in $\overline{K}$ *, wenn*

$$1 = p_1 f_1 + \cdots + p_m f_m \quad \textit{mit} \quad p_1, \dots, p_m \in K[X_1, \dots, X_n]$$

gilt.

Beweis. Sei $I = (f_1, \dots, f_m)$ das von $f_1, \dots, f_m$ erzeugte Ideal in $K[X_1, \dots, X_n]$, also

$$\boxed{I = \{q_1 f_1 + \cdots + q_m f_m \mid q_1, \dots, q_m \in K[X_1, \dots, X_n]\}}\,.$$

Dann ist $\mathfrak{V}(I) = \{x \in \overline{K}^n \mid f_1(x) = 0, \dots, f_m(x) = 0\}$, 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 $I = K[X_1, \dots, X_n]$ 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.

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

Bemerkung
Ein *reduzierter Ring* ist ein kommutativer Ring, in dem 0 das einzige nilpotente Element ist. Dabei heißt ein Element r *nilpotent*, wenn $r^m = 0$ für ein $m \in \mathbb{N}$ ist. Es gilt

$$\boxed{I \text{ Radikalideal in } R} \quad \Longleftrightarrow \quad \boxed{R/I \text{ ist reduziert}}\,.$$

Beweis. Sei $r \in R$.

„$\Longrightarrow$“ Ist $r + I$ nilpotent in R/I
$\Longrightarrow r^m \in I$ für ein $m \in \mathbb{N}$
$\Longrightarrow r \in \mathrm{Rad}(I) \underset{\text{Vor.}}{=} I$
$\Longrightarrow r + I = I = 0_{R/I}$.

„$\Longleftarrow$“ Ist $r \in \mathrm{Rad}(I) \Longrightarrow r^m \in I$ für ein $m \in \mathbb{N}$
$\Longrightarrow r \in I$, da R/I reduziert.

□

1.13 Das 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

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

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

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

Beweis. Sei $f \in \operatorname{Rad}(\mathfrak{I}(V))$. Dann existiert ein $m \in \mathbb{N}$ mit $f^m \in \mathfrak{I}(V)$, also mit $f^m(x) = 0 \;\forall\, x \in V$.
Da der Einsetzhomomorphismus $\varphi_x\colon K[X_1,\dots,X_n] \longrightarrow \overline{K}\,, g \longmapsto g(x)$, 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 $\mathfrak{I}(\mathfrak{V}(I)) = \operatorname{Rad}(I)$

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

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

Nullstellensatz
$\mathfrak{I}(\mathfrak{V}(I)) = \operatorname{Rad}(I)$.

Beweis. Es ist $\operatorname{Rad}(I) \subset \mathfrak{I}(\mathfrak{V}(I))$, denn:
$g \in \operatorname{Rad}(I) \Longrightarrow g^m \in I$ für ein $m \in \mathbb{N}$
$\Longrightarrow 0 = g^m(x) = g(x)^m \;\forall\, x \in \mathfrak{V}(I)$
$\Longrightarrow g(x) = 0 \;\forall\, x \in \mathfrak{V}(I)$, da $g(x)$ im Körper $\overline{K}$ liegt,
$\Longrightarrow g \in \mathfrak{I}(\mathfrak{V}(I))$.
Zu zeigen: $\boxed{\mathfrak{I}(\mathfrak{V}(I)) \subset \operatorname{Rad}(I)}$.
Nach dem Hilbertschen Basissatz (Algebra 6.14) ist I endlich erzeugt, d.h. es gibt ein $\ell \in \mathbb{N}$ und $f_1,\dots,f_\ell \in K[X_1,\dots,X_n]$ mit
$I = (f_1,\dots,f_\ell) := \{\sum_{i=1}^{\ell} p_i f_i \mid p_i \in K[X_1,\dots,X_n]\}$.
Sei $g \in \mathfrak{I}(\mathfrak{V}(I))$ und $g \neq 0$. Dann folgt

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

nach Definition von $\mathfrak{I}(\mathfrak{V}(I))$.
Zu zeigen: $\exists\, m \in \mathbb{N}$ mit $g^m \in I$.
Betrachte in $K[X_1,\dots,X_n][X]$ die $\ell+1$ Polynome $f_1,\dots,f_\ell, 1-gX$.
Diese können keine gemeinsame Nullstelle in $\overline{K}^{n+1}$ haben, da jede gemeinsame Nullstelle von $f_1,\dots,f_\ell$ 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 $p_1,\dots,p_{\ell+1} \in K[X_1,\dots,X_n][X]$.
Setze $\frac{1}{g}$ für die Unbestimmte X ein. Dann folgt

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

mit $\widetilde{p_1}, \ldots, \widetilde{p_\ell} \in K[X_1, \ldots, X_n][\frac{1}{g}]$. Mutipliziere diese Gleichung mit g^m, wobei m so groß gewählt wird, dass alle Nenner in den Potenzen von g verschwinden. Es folgt

$$g^m = p_1^* f_1 + \cdots + p_\ell^* f_\ell \quad \text{mit} \quad p_i^* \in K[X_1, \ldots, X_n]$$

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

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

Objekte der Geometrie Objekte der Algebra

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 8). 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). □

Hier liegt der Ausgangspunkt der algebraischen Geometrie.

1.16 Aufgaben

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 sei $f \in K[X_1, \ldots, X_n]$ ein nicht konstantes Polynom. Man zeige, dass es unendlich viele Punkte $(a_1, \ldots, a_n)$ in K^n gibt mit $f(a_1, \ldots, a_n) \neq 0$.

Aufgabe 5
Seien $a_1, \ldots, a_n$ beliebige Elemente eines Körpers K. Man zeige, dass das von den Elementen $X_1 - a_1, \ldots, X_n - a_n$ im Polynomring $K[X_1, \ldots, X_n]$ erzeugte Ideal I ein maximales Ideal ist.

Hinweis
Unter Berücksichtigung des Homomorphiesatzes für Ringe genügt es zu zeigen, dass $\mathrm{kern}(\varphi) = I$ *gilt für den Einsetzhomomorphismus*
$\varphi\colon K[X_1, \ldots, X_n] \longrightarrow K,\ f \longmapsto f(a_1, \ldots, a_n)$.

Aufgabe 6
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 7
Sei R ein Integritätsring, und sei R^* die Gruppe der Einheiten in R. Man zeige, dass $R^* = (R[X_1, \ldots, X_n]\,)^*$ gilt.

Aufgabe 8
Man zeige:

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

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

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

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

Aufgabe 9
Seien K ein algebraisch abgeschlossener Körper und A eine affine K-Algebra. Man zeige, dass $A \simeq K[X_1, \ldots, X_n]/\mathfrak{I}(V)$ mit einer Teilmenge $V \subset K^n$ gilt.

2 Affine algebraische Varietäten

Seien K ein Körper und $\overline{K}$ ein algebraischer Abschluss von K.

2.1 Algebraische Mengen

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.

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

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

Dann gelten:

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

ii) Es ist $\mathfrak{V}(I)$ eine algebraische Menge in $\overline{K}^n$ für jedes Ideal I in $K[X_1, \ldots, X_n]$, denn nach dem Hilbertschen Basissatz (Algebra 6.14) ist jedes Ideal in $K[X_1, \ldots, X_n]$ endlich erzeugt.

2.2 Die 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.
Sei $\bigcap_{j\in J}\mathfrak{V}(I_j)=\emptyset \underset{(c)}{\Longrightarrow} \mathfrak{V}\left(\sum_{j\in J} I_j\right)=\emptyset$
$\Longrightarrow \operatorname{Rad}\left(\sum_{j\in J} I_j\right) \underset{1.14}{=} \mathfrak{I}(\mathfrak{V}(\sum_{j\in J} I_j))=\mathfrak{I}(\emptyset) \underset{Aufgabe\ 8}{=} (1)$
$\Longrightarrow 1 \in \sum_{j\in J} I_j \Longrightarrow$ es gibt endlich viele Ideale $I_1,\dots,I_\ell$ unter den Idealen $\{I_j \mid j\in J\}$ mit $1\in\sum_{j=1}^{\ell} I_j$
$\Longrightarrow (1)=\sum_{j=1}^{\ell} I_j \Longrightarrow \emptyset \underset{(a)}{=} \mathfrak{V}((1))=\mathfrak{V}\left(\sum_{j=1}^{\ell} I_j\right)=\bigcap_{j=1}^{\ell}\mathfrak{V}(I_j)\,.$

(e) Eine (K)–*offene* Menge in $\overline{K}^n$ ist das Komplement einer in $\overline{K}^n$ (K)–abgeschlossenen Menge. 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).

□

Bemerkung 1. Die durch den Satz definierte Topologie auf $\overline{K}^n$ heißt *Zariski-K-Topologie* von $\overline{K}^n$.

2. Im Fall $K=\overline{K}$ spricht man von der Zariski-Topologie. Punkte und endliche Mengen in $\overline{K}^n$ sind dann 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

$$\boxed{V\ \textit{irreduzibel in}\ \overline{K}^n} \quad\Longleftrightarrow\quad \boxed{\mathfrak{I}(V)\ \textit{Primideal in}\ K[X_1,\dots,X_n]}\,.$$

Insbesondere ist $\overline{K}^n$ irreduzibel.

Beweis. „$\Longrightarrow$“ Seien $f_1,f_2\in K[X_1,\dots,X_n]$ mit $f_1\cdot f_2\in\mathfrak{I}(V)$
$\Longrightarrow f_1(x)\cdot f_2(x)=0$ für jedes $x\in V$
$\Longrightarrow V=(V\cap\mathfrak{V}(f_1))\cup(V\cap\mathfrak{V}(f_2))$

$\Longrightarrow V = V \cap \mathfrak{V}(f_1)$ oder $V = V \cap \mathfrak{V}(f_2)$, da V irreduzibel
$\Longrightarrow V \subset \mathfrak{V}(f_1)$ oder $V \subset \mathfrak{V}(f_2)$
$\underset{1.15}{\Longrightarrow} f_1 \in \mathfrak{I}(V)$ oder $f_2 \in \mathfrak{I}(V)$.

„$\Longleftarrow$" Angenommen, es gibt algebraische Mengen $V_1, V_2 \subset \overline{K}^n$ mit

$$\boxed{V_1 \subsetneqq V \text{ und } V_2 \subsetneqq V} \quad \text{und} \quad \boxed{V = V_1 \cup V_2}.$$

Dann gibt es $f_1 \in \mathfrak{I}(V_1) \setminus \mathfrak{I}(V)$ und $f_2 \in \mathfrak{I}(V_2) \setminus \mathfrak{I}(V)$.
$\Longrightarrow f_1 f_2 \in \mathfrak{I}(V_1) \cap \mathfrak{I}(V_2) \underset{\text{Aufgabe 8}}{=} \mathfrak{I}(V_1 \cup V_2) = \mathfrak{I}(V)$.
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. $\square$

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 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
  $$\overline{S} := \bigcap_{A \supset S \text{ abgeschlossen in } T} A$$
  der *Abschluss von S in T*. Es gilt:
  $$\boxed{S \text{ abgeschlossen in } T} \quad \Longleftrightarrow \quad \boxed{S = \overline{S}}.$$

- $S \subset T$ heißt *dicht in T*, wenn $\overline{S} = T$ gilt.

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

(a) Für jede nichtleere Teilmenge $S \subset T$ gilt:

$$\boxed{S \text{ irreduzibel}} \iff \boxed{\overline{S} \text{ irreduzibel}}.$$

(b) $\boxed{T \text{ irreduzibel}} \iff \boxed{\text{Jede nichtleere offene Menge } U \subset T \text{ ist dicht in } T}$

(c) $\boxed{f : T \longrightarrow T' \text{ stetig und } T \text{ irreduzibel}} \implies \boxed{f(T) \text{ irreduzibel}}$

Beweis. (a) „$\Longrightarrow$“
Sei $\overline{S} = A_1 \cup A_2$ mit abgeschlossenen Mengen $A_1, A_2 \subset \overline{S}$
$\Longrightarrow S = \underbrace{(A_1 \cap S)}_{\text{abgeschlossen in } S} \cup \underbrace{(A_2 \cap S)}_{\text{abgeschlossen in } S}$
$\underset{S \text{ irr.}}{\Longrightarrow} S = A_1 \cap S$ oder $S = A_2 \cap S$
$\Longrightarrow S \subset A_1$ oder $S \subset A_2 \underset{\text{Def. von } \overline{S}}{\Longrightarrow} \overline{S} \subset A_1$ oder $\overline{S} \subset A_2$
$\Longrightarrow \overline{S}$ irreduzibel.

„$\Longleftarrow$“ Sei $S = (B_1 \cap S) \cup (B_2 \cap S)$, wobei $B_1, B_2 \subset T$ abgeschlossen in T seien $\Longrightarrow \overline{S} \subset B_1 \cup B_2$
$\Longrightarrow \overline{S} = (B_1 \cap \overline{S}) \cup (B_2 \cap \overline{S})$
$\underset{\overline{S} \text{ irr.}}{\Longrightarrow} \overline{S} = B_1 \cap \overline{S}$ oder $\overline{S} = B_2 \cap \overline{S}$
$\Longrightarrow S = B_1 \cap S$ oder $S = B_2 \cap S$
$\Longrightarrow S$ irreduzibel.

(b) „$\Longrightarrow$“ Es ist $U \cap (T \setminus \overline{U}) = \emptyset$ und $T \setminus \overline{U}$ offen
$\underset{T \text{ irr.}}{\Longrightarrow} T \setminus \overline{U} = \emptyset \Longrightarrow T = \overline{U}$.

„$\Longleftarrow$“ Seien $U_1, U_2 \neq \emptyset$ offen in T.
Dann gilt nach Voraussetzung $\overline{U_1} = T = \overline{U_2}$.
Angenommen: $U_1 \cap U_2 = \emptyset$
$\Longrightarrow U_1 \subset X \setminus U_2 \Longrightarrow \overline{U_2} = \overline{U_1} \subset X \setminus U_2$. Widerspruch.

(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 $\neq \emptyset$)
$\underset{T \text{ irr.}}{\Longrightarrow} U := f^{-1}(U_1) \cap f^{-1}(U_2) \neq \emptyset$
$\Longrightarrow \emptyset \neq f(U) \subset U_1 \cap U_2 \cap f(T)$.

$\square$

2.5 Zerlegung in irreduzible Komponenten

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

Definition1) Eine *irreduzible Komponente von* T ist eine (bezüglich Inklusion) maximale irreduzible Teilmenge.

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 15).

Satz*(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 $V := \bigcup\limits_{T' \in N} T' \in M$, 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

$V_1 \cup \cdots \cup V_m$ 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 ($\Longrightarrow A_i = V_i \cap V$ mit K-abgeschlossenen Mengen V_i in $\overline{K}^n \Longrightarrow$ A_i ist K-abgeschlossen in $\overline{K}^n$, da V algebraisch, d.h. K-abgeschlossen in $\overline{K}^n$). 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 Der affine Koordinatenring

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

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

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 17, 18).

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

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

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

Beispiele • $V = \overline{K}^n \Longrightarrow K[V] = K[X_1, \dots, X_n]/(0) = K[X_1, \dots, X_n]$.

• $V = \emptyset \Longrightarrow K[V] = K[X_1, \dots, X_n]/(1) = 0$ (Nullring).

2.7 Eigenschaften des affinen Koordinatenrings

1) $K[V]$ ist reduziert und endlich erzeugt als K-Algebra, also eine *affine K-Algebra* (vgl. 1.12, 1.13 und Definition 1.2).

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

3) Die Elemente von $K[V]$ lassen sich als Funktionen $V \longrightarrow \overline{K}$ auffassen: Ist $\varphi \in K[V]$, so ist $\varphi = f + \mathfrak{I}(V)$ mit einem $f \in K[X_1, \dots, X_n]$. 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 $f, g \in K[X_1, \dots, X_n]$ 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

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

Es ist $K[V]$ die K-Algebra der „polynomialen Funktionen“ $V \longrightarrow \overline{K}$.

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

4) Mit der Interpretation aus 3) ist das *Verschwindungsideal* einer K-abgeschlossenen Menge $W \subset V$ definiert als

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

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

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

denn nach dem zweiten Noetherschen Isomorphiesatz (Algebra 1.7) 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 $\alpha\colon V \longrightarrow W$ heißt *polynomial* oder *Morphismus*, wenn es Polynome $f_1,\ldots,f_m \in K[X_1,\ldots,X_n]$ gibt mit

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

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

Beispiel

$V = \{(a,b) \in \overline{K}^2 \mid b = a^2\} = \mathfrak{V}(X_1^2 - X_2)$ und $W = \overline{K} = \mathfrak{V}(0 \cdot K[X])$.
Die Projektion von V auf die x_1-Achse $(= W)$ ist ein Isomorphismus
$\pi\colon V \longrightarrow W,\ (a,a^2) \longmapsto a$, mit Umkehrabbildung $\pi^{-1}\colon W \longrightarrow V$,
$a \longmapsto (a,a^2)$. 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 $\alpha\colon V \longrightarrow W$ einen K-Algebrahomomorphismus

$$\begin{tikzcd} K[W] \arrow[r] \arrow[d, equal] & K[V] \arrow[d, equal] \\ \alpha^*\colon \operatorname{Mor}(W,\overline{K}\,) \arrow[r] & \operatorname{Mor}(V,\overline{K}\,) \end{tikzcd}$$

$$\varphi \longmapsto \varphi \circ \alpha$$

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

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

Objekte: $V \mapsto\!\rightsquigarrow K[V]$
Morphismen: $\alpha \mapsto\!\rightsquigarrow \alpha^*$
Sei $\operatorname{Mor}(V,W)$ die Menge der Morphismen $V \longrightarrow W$ und $\operatorname{Hom}_{\mathrm{Alg}}(K[W],K[V])$ die Menge der K-Algebrahomomorphismen $K[W] \longrightarrow K[V]$.

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

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

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 $\alpha,\beta \in \operatorname{Mor}(V,W)$ sei $\alpha^* = \beta^*$.
Zu zeigen: $\alpha = \beta$.
Nach Definition 2.8 eines Morphismus gibt es $f_1,\dots,f_m$ und $g_1,\dots,g_m \in K[X_1,\dots,X_n]$ mit $\alpha(v) = (f_1(v),\dots,f_m(v))$ und $\beta(v) = (g_1(v),\dots,g_m(v))\ \forall\, v \in V$.

Ist $\alpha^* = \beta^* \underset{\text{Def von } *}{\Longrightarrow} \varphi\circ\alpha = \varphi\circ\beta \quad \forall\, \varphi \in K[W] = K[Y_1,\dots,Y_m]/\mathfrak{I}(W) =$ $\mathrm{Mor}(W, \overline{K}\,)$
$\Longrightarrow y_i \circ \alpha = y_i \circ \beta \;\forall\, i = 1,\dots,m$, wobei $y_i = Y_i + \mathfrak{I}(W)$ die i-te Koordinatenabbildung ist (vgl. 2.7.3).
$\Longrightarrow f_i(v) \underset{\text{Def von } y_i}{=} (y_i \circ \alpha)(v) = (y_i \circ \beta)(v) \underset{\text{Def von } y_i}{=} g_i(v)$
$\forall\, i = 1,\dots,m,\ \forall\, v \in V$.
$\Longrightarrow \alpha(v) = \beta(v) \;\forall\, v \in V$.

Surjektivität von $\mathcal{F}_{V,W}$: Sei $\gamma\colon K[W] \longrightarrow K[V]$ ein K-Algebrahomomorphismus. Wähle $f_1,\dots,f_m \in K[X_1,\dots,X_n]$ so, daß $\gamma(y_i) = f_i + \mathfrak{I}(V)$ für alle $i = 1,\dots,m$ gilt. Der Morphismus

$$\alpha\colon V \longrightarrow \overline{K}^{\,m},\ v \longmapsto (f_1(v),\dots,f_m(v))$$

induziert den K-Algebrahomomorphismus

$$\alpha^*\colon K[Y_1,\dots,Y_m] \longrightarrow K[V],\ g \longmapsto g\circ\alpha\,,$$

wobei

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

Da $W = \mathfrak{V}(\mathfrak{I}(W))$ gilt, folgt $\alpha(v) \in W \;\forall\, v \in V$. Weiter folgt, daß α^* auch auf $K[W] = K[X_1,\dots,X_n]/\mathfrak{I}(W)$ wohldefiniert ist und $\alpha^* = \gamma$ gilt.

Bemerkung

Es ist $g = \sum\limits_{(r_1,\dots,r_m)\in\mathbb{N}_0^m}^{\text{endl}} a_{r_1\dots r_m} Y_1^{r_1}\cdot\ldots\cdot Y_m^{r_m}$
$\Longrightarrow g + \mathfrak{I}(W) = \sum a_{r_1}\dots a_{r_m}\, y_1^{r_1}\cdot\ldots\cdot y_m^{r_m}$
$\Longrightarrow \gamma(g{+}\mathfrak{I}(W)) = \sum a_{r_1}\dots a_{r_m}\gamma(y_1)^{r_1}\dots\gamma(y_m)^{r_m} = g\circ(\gamma(y_1),\dots,\gamma(y_m))$

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.

$\square$

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

Beweis. Sei A eine affine K-Algebra, d.h. eine endlich erzeugte und reduzierte K-Algebra. Da A endlich erzeugt ist, gibt es ein $n \in \mathbb{N}$ und einen surjektiven K-Algebrahomomorphismus $\varphi\colon K[X_1, \dots, X_n] \twoheadrightarrow A$ nach Definition 1.2. Da $A \simeq K[X_1, \dots, X_n]/\operatorname{kern}\varphi$ reduziert ist, ist $\operatorname{kern}\varphi$ ein Radikalideal nach Bemerkung 1.12. Nach 1.15 gibt es also eine algebraische Menge $V \subset \overline{K}^n$ mit $\mathfrak{I}(V) = \operatorname{kern}\varphi$. □

2.10 Zum Tensorprodukt

Gegeben seien ein kommutativer Ring R und R-Moduln M, N. Das *Tensorprodukt* $M \otimes_R N$ (bestehend aus Elementen der Form $z = \sum_{\text{endl.}} m_i \otimes n_i$ mit $m_i \in M, n_i \in N$) wurde in Algebra 10.7 eingeführt. 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 $\gamma\colon M \times N \longrightarrow P$ in einen R-Modul P gibt es eine eindeutig bestimmte R-lineare Abbildung $g\colon M \otimes_R N \longrightarrow P$ mit

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

Als Diagramm

$$\begin{tikzcd} M \times N \arrow[rr, "\gamma"] \arrow[dr, "t"'] & & P \\ & M \otimes_R N \arrow[ur, dashed, "\exists!\, g"'] & \end{tikzcd}$$

wobei $t(m, n) = m \otimes n$.

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

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

jeweils R-linear sind.

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

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

genannt *Multiplikationsabbildung* oder *Multiplikation*.

(ii) Die Abbildungen $M \times N \longrightarrow N \otimes_R M,\ (m, n) \longmapsto n \otimes m$, und $N \times M \longrightarrow M \otimes_R N,\ (n, m) \longmapsto m \otimes n$, sind R-bilinear. Es gibt also eine kanonische Ringisomorphie

$$\boxed{M \otimes_R N \longrightarrow N \otimes_R M,\ m \otimes n \longmapsto n \otimes m}\,.$$

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

$$M \times N \longrightarrow M' \otimes_R N',\ (m, n) \longmapsto u(m) \otimes v(n)$$

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

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

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

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

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

$$\begin{aligned} A &\longrightarrow A \otimes_R B,\ a \longmapsto a \otimes 1 \\ B &\longrightarrow A \otimes_R B,\ b \longmapsto 1 \otimes b \end{aligned}$$

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

(vi) Seien S eine kommutative Ringerweiterung von R und I ein Ideal in $R[X_1, \ldots, X_n]$ sowie $J = I \cdot S[X_1, \ldots, X_n]$. Dann ist

$$S \times (R[X_1, \ldots, X_n]/I) \longrightarrow S[X_1, \ldots, X_n]/J,\ (s, f + I) \longmapsto sf + J\,,$$

wohldefiniert und induziert einen S-Algebrahomomorphismus

$$\boxed{S \otimes_R (R[X_1, \ldots, X_n]/I) \longrightarrow S[X_1, \ldots, X_n]/J}\,.$$

Die Umkehrabbildung wird von dem durch $X_i \longmapsto 1 \otimes (X_i + I)$ definierten S-Algebrahomomorphismus

$$S[X_1, \ldots, X_n] \longrightarrow S \otimes_R (R[X_1, \ldots, X_n]/I)$$

induziert.

2.11 F-Strukturen

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

Definition1) 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.

Es gilt:

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

denn es ist $V = \mathfrak{V}(\mathfrak{I}(V))$.

Warnung

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

Beispiel
$I := (X^p - Y) \Longrightarrow I \subset F[X] \Longrightarrow V := \mathfrak{V}(I) = \left\{\sqrt[p]{Y}\right\}$ ist F-abgeschlossen nach Definition. Aber es ist

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

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

Bemerkung1) 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

$$\boxed{K \otimes_F F[V] \simeq K[V]}$$

nach 2.10 (vi).
Diese Beobachtung führt zur

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 $K \times F[V] \longrightarrow K[V]$, $(\lambda, a) \longmapsto \lambda a$, induzierte F-Algebrahomomorphismus

$$K \otimes_F F[V] \longrightarrow K[V]$$

ist ein Isomorphismus.

Im allgemeinen besitzt V verschiedene F-Strukturen.

4) Die Menge der *F-rationalen Punkte* einer F-Struktur $F[V]$ ist als die Menge

$$V(F) := \mathrm{Hom}_{\mathrm{Alg}}(F[V], F)$$

der F-Algebrahomomorphismen $F[V] \longrightarrow F$ definiert. Diese Definition ist durch Aufgabe 17 motiviert, in der $F = K = \overline{K}$ gilt.

2.12 Lokalisierungen

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

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

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

zugeordnet.

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 lokaler Ring mit maximalem 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

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + sr'}{ss'} \in \mathfrak{m} \quad \text{und} \quad \lambda \cdot \frac{r}{s} \in \mathfrak{m} \quad \forall\, r, r' \in \mathfrak{p},\ s, s' \in S,\ \lambda \in R_{\mathfrak{p}} .$$

Sei I ein Ideal in $R_{\mathfrak{p}}$ mit $I \not\supseteq \mathfrak{m}$. 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. □

Definition1) Der Ring $R_{\mathfrak{p}}$ heißt *Lokalisierung von R nach $\mathfrak{p}$*.

2) 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.)

2.13 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 $V \longrightarrow K$ auf. Zu jedem $v \in V$ gehört ein lokaler Ring

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

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

$$\mathfrak{m}_v := \{g \in K[V] \mid g(v) = 0\} = \mathrm{kern}(K[V] \longrightarrow K,\ g \longmapsto g(v))\,.$$

Jeder nichtleeren, offenen Menge $U \subset V$ ordnen wir den folgenden Ring zu

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

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 $\frac{g}{f^m} \in \mathcal{O}_v\ \forall\, v \in V_f$ (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 $\psi \in \mathcal{O}_V(V_f) \Longrightarrow \psi \in \mathcal{O}_v\ \forall\, v \in V_f$
$\underset{\text{Def von } \mathcal{O}_v}{\Longrightarrow}\ \psi = \frac{g_v}{h_v}$ mit $g_v, h_v \in A$ und $h_v(v) \neq 0\ \forall\, v \in V_f$

$\Longrightarrow h_v \in I := \{h' \in A \mid h'\psi \in A\}$ und $v \notin \mathfrak{V}_V(I)\ \forall\, v \in V_f$
$\Longrightarrow \mathfrak{V}_V(I) \subset V \setminus V_f = \mathfrak{V}_V(f)$
$\Longrightarrow f \in \mathrm{Rad}(I)$ nach dem Hilbertschen Nullstellensatz (vgl. 1.14 und Aufgabe 18)
$\Longrightarrow \exists\, m \in \mathbb{N}$ mit $f^m \in I \underset{\text{Def von } I}{\Longrightarrow} f^m\psi =: g \in A$
$\Longrightarrow \psi \in A_f$ nach Definition von A_f.
Für $f\colon V \longrightarrow K,\ v \longmapsto 1$ ist $V_f = V$ und $A_f = A$. Daher folgt die zweite Behauptung. □

Bemerkung
Die Elemente aus $\mathcal{O}_V(U)$ lassen sich als Funktionen $U \longrightarrow K$ auffassen, denn ist $\psi \in \mathcal{O}_V(U)$ und $x \in U$, so ist $\psi \in \mathcal{O}_x$ und also $\psi = \frac{g}{h}$ mit $g, h \in K[V]$ und $h(x) \neq 0$. Es ist ψ dann in x definiert, und man setzt

$$\psi(x) = \frac{g(x)}{h(x)}\,.$$

Dies ist wohldefiniert:
Ist $\frac{g}{h} = \frac{g'}{h'}$, wobei $h'(x) \neq 0$, so ist $g(x)h'(x) = g'(x)h(x)$ und also $\frac{g(x)}{h(x)} = \frac{g'(x)}{h'(x)}$.

Definition
Eine Funktion $f\colon U \longrightarrow K$ 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 $f(y) = \frac{g(y)}{h(y)}\ \forall\, y \in U'$ gilt.
Man nennt f *regulär*, wenn f in jedem Punkt $x \in U$ regulär ist. Die K-Algebra $\mathcal{O}_V(U)$ wird Algebra der regulären Funktionen auf U genannt.

2.14 Geringte Räume

Sei K ein algebraisch abgeschlossener Körper, und sei V eine algebraische Menge in K^n. Für nichtleere, offene Mengen $U' \subset U$ von V gilt
$\mathcal{O}_V(U) \hookrightarrow \mathcal{O}_V(U')$. Die Zuordnung $\mathcal{O}_V\colon U \longrightarrow \mathcal{O}_V(U)$ definiert eine *Garbe von Funktionen* mit *Halmen* $\mathcal{O}_v$ für $v \in V$.
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 $U \longrightarrow K$ gibt und folgendes gilt:

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

2) Sei $U \neq \emptyset$ offen in T und $U = \bigcup\limits_{j\in J} U_j$ 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 $f|_{U_i} = f_i\ \forall\, i \in J$.

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

2.15 Morphismen von geringten Räumen

Definition

Seien $(T, \mathcal{O})$ und $(T', \mathcal{O}')$ geringte Räume wie in 2.14 definiert, und sei $\alpha\colon T' \longrightarrow T$ eine stetige Abbildung. Ist U eine offene Menge in T, so induziert α eine Abbildung

$$\alpha_U^*\colon \mathcal{O}(U) \longrightarrow \mathrm{Abb}(\alpha^{-1}(U), K),\ f \longmapsto f \circ \alpha|_{\alpha^{-1}(U)}\,.$$

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 $\alpha\colon T' \longrightarrow T$ heißt *Isomorphismus*, wenn es einen Morphismus $\beta\colon T \longrightarrow T'$ mit $\alpha \circ \beta = \mathrm{id}$ und $\beta \circ \alpha = \mathrm{id}$ gibt.

2.16 Tensorprodukt von affinen Algebren

Satz

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

(i) A, B reduziert $\Longrightarrow A \otimes_K B$ reduziert.

(ii) A, B Integritätsringe $\Longrightarrow A \otimes_K B$ Integritätsring.

Beweis. (i) Sei $\sum\limits_{i=1}^{m} a_i \otimes b_i$ nilpotent in $A \otimes_K B$. Nach Algebra 10.11(1) können wir annehmen, daß $\{b_1, \ldots, b_m\}$ linear unabhängig über K sind. Für jeden K-Algebrahomomorphismus $h\colon A \longrightarrow K$ erhält man vermöge $h \otimes \mathrm{id}$ einen K-Algebrahomorphismus

$$A \otimes_K B \longrightarrow B \quad (\text{mit } a \otimes b \longmapsto h(a)b)$$

(vgl. 2.10 und Algebra 10.9).
Es ist also $\sum\limits_{i=1}^{m} h(a_i)b_i$ nilpotent in B und daher $h(a_i) = 0\ \forall\, i = 1, \ldots, m$, da B reduziert ist und $b_1, \ldots, b_m$ linear unabhängig sind.
Es ist $A \overset{\text{Folgerung}}{\underset{2.9}{=}} K[V] \overset{K=\overline{K}}{\underset{2.7}{=}} \mathrm{Mor}(V, K)$ mit einer algebraischen Menge V ($\neq \emptyset$ für $A \neq (0)$, vgl. Beispiel 2.6) und also $\varphi_v(a_i) = 0\ \forall\, v \in V$, wobei

$$\varphi_v\colon A \longrightarrow K\,,\ a \longmapsto a(v)\,,$$

und $i \in \{1, \ldots, m\}$. Es folgt

$$V = \mathfrak{V}_V(a_i) = \{v \in V \mid \varphi_v(a_i) = a_i(v) = 0\}.$$

Da $\mathfrak{V}_V(0) = V$ gilt, erhalten wir

$$\operatorname{Rad}(0) \underset{\text{Aufg18}}{=} \mathfrak{I}_V(\mathfrak{V}_V(0)) = \mathfrak{I}_V(V) = \mathfrak{I}_V(\mathfrak{V}_V(a_i)) \underset{\text{Aufgabe 18}}{=} \operatorname{Rad}(a_i)$$

und daher $a_i \in \operatorname{Rad}(a_i) = \operatorname{Rad}(0) \underset{\text{Def. 1.12}}{=}$ Menge der nilpotenten Elemente. Es folgt $a_i = 0 \ \forall\, i = 1, \ldots, m$, da A reduziert ist, und damit $\sum\limits_{i=1}^{m} a_i \otimes b_i = 0$. Es folgt (i).

(ii) Seien $f = \sum\limits_{i=1}^{m} a_i \otimes b_i$ und $g = \sum\limits_{j=1}^{n} c_j \otimes d_j$ Elemente in $A \otimes_K B$, wobei $\{b_1, \ldots, b_m\}$ und $\{d_1, \ldots, d_n\}$ jeweils linear unabhängig seien.
Ist $fg = 0$, so ist

$$\left(\sum_{i=1}^{m} h(a_i) b_i\right) \cdot \left(\sum_{j=1}^{n} h(c_j) d_j\right) = 0$$

für jedes $h \in \operatorname{Hom}_{\mathrm{Alg}}(A, K)$. Da B Integritätsring ist, folgt $\sum_i h(a_i) \cdot b_i = 0$ oder $\sum_j h(c_j) \cdot d_j = 0$, und analog wie in (i) folgt $f = 0$ oder $g = 0$, da A Integritätsring ist.

$\square$

Bemerkung
Der Satz ist i.a. falsch, wenn K nicht algebraisch abgeschlossen ist, z.B. ist $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ kein Integritätsring, vgl. Aufgabe 23.

2.17 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) $K[V \times W] \xrightarrow{\sim} K[V] \otimes_K K[W]$.

(iii) V, W irreduzibel $\Longrightarrow V \times W$ irreduzibel.

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

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

wobei $f_1, \dots, f_k, g_1, \dots, g_\ell$ als Polynome in $K[X_1, \dots, X_n, Y_1, \dots, Y_m]$ aufgefaßt werden, und $V \times W$ trägt die durch die Zariski-Topologie auf K^{n+m} induzierte Topologie (diese stimmt *nicht* mit der Produkttopologie überein).

(ii) Die Abbildung

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

ist K-bilinear, induziert also nach 2.10 einen K-Algebrahomomorphismus

$$\Gamma\colon K[V] \otimes_K K[W] \longrightarrow K[V \times W]$$

Surjektivität von Γ: Jedes Polynom aus $K[X_1, \dots, X_n, Y_1, \dots, Y_m]$ ist als endliche Summe gh mit $g \in K[X_1, \dots, X_n]$ und $h \in K[Y_1, \dots, Y_m]$ 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 $j \in \{1, \dots, k\}$ mit $h_j(w) \neq 0$. Da $\sum_{i=1}^{k} g_i(v) h_i(w) = 0 \ \forall\, v \in V$ gilt, folgt $\sum_{i=1}^{k} h_i(w) g_i = 0$, und also sind $g_1, \dots, g_k$ 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 $g_1(v) = 0 \ \forall\, v \in V$ und also $f = 0$ im Widerspruch zur Annahme.

(iii) Nach 2.16 ist $K[V \times W] \underset{\text{(ii)}}{\simeq} K[V] \otimes_K K[W]$ ein Integritätsring und also $\mathfrak{I}(V \times W)$ ein Primideal in $K[X_1, \dots, X_n, Y_1, \dots, Y_m]$. Mit 2.3 folgt, daß $V \times W$ irreduzibel ist.

□

Bemerkung1) Ist $V \times W$ irreduzibel, so ist der lokale Ring $\mathcal{O}_{(v,w)}$ gerade die Lokalisierung von $\mathcal{O}_V \otimes_K \mathcal{O}_W$ nach dem maximalen Ideal $\mathfrak{m}_v \otimes \mathcal{O}_w + \mathcal{O}_v \otimes \mathfrak{m}_w$ (Beweis siehe Humphreys 2.4).

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

$$\begin{tikzcd} & V \\ T \arrow[ur, "\varphi_1"] \arrow[dr, "\varphi_2"'] \arrow[r, dashed, "\exists!\psi"] & V \times W \arrow[u, "\pi_1"'] \arrow[d, "\pi_2"] \\ & W \end{tikzcd}$$

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

2.18 Varietäten

Beispiel (Die additive Gruppe) (i) $\mathbb{G}_\mathrm{a}(K) = K \subset K^1$ mit Addition

(ii) $\mathbb{G}_\mathrm{a}(K) = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(K) \right\} \subset K^4$ mit Matrizenmultiplikation

Was ist nun die Definition von $\mathbb{G}_\mathrm{a}(K)$? Dies klärt der Varietätenbegriff.

Sei K ein algebraisch abgeschlossener Körper.

1) Eine *irreduzible affine algebraische 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 $\mathcal{O}_V(U) = \bigcap\limits_{x \in U} \mathcal{O}_x$ wie in 2.13.

2) **Beispiel:** Die irreduzible Varietät $(K^n, \mathcal{O}_{K^n}) =: \mathbb{A}^n$ ist der *affine Raum.*

3) Eine *affine algebraische 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

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

Es ist dann $\mathcal{O}_V(U) = K[V]$ wie im irreduziblen Fall.

4) Eine *Prävarietät* (über K) ist ein geringter Raum $(V, \mathcal{O})$ mit den Eigenschaften

   (a) V ist kompakt.

   (b) Jeder Punkt $v \in V$ besitzt eine offene Umgebung U, so daß der geringte Raum $(U, \mathcal{O}|_U)$ isomorph zu einer affinen algebraischen Varietät ist.

   Jede solche offene Menge U heißt *offene affine* Teilmenge von V. Ein *Morphismus von Prävarietäten* ist ein Morphismus von geringten Räumen wie in 2.15 definiert.

5) Beispiele für nicht affine Prävarietäten sind die *projektiven 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 Menge 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) Auch für Prävarietäten V, W existiert ein Produkt $V \times W$, das bis auf Isomorphie eindeutig ist. Eine Prävarietät heißt *Varietät* oder *algebraische 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 13.
   Beispiel: Ist V eine affine Varietät, so ist dieses Hausdorff-Axiom erfüllt (Δ_V ist abgeschlossen in $V \times V$).

7) Es gibt einen allgemeineren Garbenbegriff als den der Funktionengarben aus 2.14. Ein *affines Schema* ist ein „lokal geringter Raum“ (topologischer Raum mit einer Ringgarbe $\mathcal{O}$), der isomorph zum Spektrum $\mathrm{Spec}(R)$ eines kommutativen Ringes R ist, das mit einer Garbe $\mathcal{O}_{\mathrm{Spec}(R)}$ versehen ist. Ein Schema ist analog wie in 4(b) definiert.
   Man kann dann von einem beliebigen Schema ausgehen statt von einem algebraisch abgeschlossenen Körper wie in 4.

2.19 Aufgaben

Aufgabe 10
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 11
Für einen kommutativen Ring R sei $\operatorname{Spec}(R)$ die Menge der Primideale von R. Man zeige, dass $\operatorname{Spec}(R)$ eine Topologie trägt, deren abgeschlossenen Mengen gerade die sogenannten ZARISKI-*abgeschlossenen* Mengen $\mathcal{Z}(I) := \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \supset I\}$ sind, wobei I alle Ideale von R durchläuft.

Aufgabe 12
Seien K ein algebraisch abgeschlossener Körper, $R = K[X_1, \ldots, X_n]$ und $\operatorname{Max}(R)$ die Menge der maximalen Ideale von R. Man zeige, dass die Abbildung

$$\psi\colon K^n \longrightarrow \operatorname{Max}(R)\,,\ (a_1, \ldots, a_n) \longmapsto (X_1 - a_1, \ldots, X_n - a_n),$$

ein Homöomorphismus ist, wenn K^n die ZARISKI-Topologie trägt und die Topologie von $\operatorname{Max}(R)$ durch die in Aufgabe 11 beschriebene Topologie von $\operatorname{Spec}(R)$ induziert wird.

Aufgabe 13
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 14
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 15
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 nicht leere 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 16
Seien R ein kommutativer Ring, I ein Ideal in R und $\pi\colon R \longrightarrow R/I$ der kanonische Homomorphismus. Man zeige, dass die Abbildung

$$\{\text{Ideale } \mathfrak{a} \text{ in } R/I\} \longrightarrow \{\text{Ideale } J \text{ in } R,\ \text{die } I \text{ enthalten}\},\ \mathfrak{a} \longmapsto \pi^{-1}\mathfrak{a}$$

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

Aufgabe 17
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

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

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

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

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

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

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

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

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

$$\mu\colon G \times G \longrightarrow G\,,\ (x, y) \longmapsto xy\,,$$

   versehen ist, daß μ und

$$i\colon G \longrightarrow G\,,\ x \longmapsto x^{-1}\,,$$

   Morphismen von Varietäten sind. Ist die Varietät affin, so heißt G eine *affine algebraische Gruppe* oder eine *lineare algebraische Gruppe*.

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

3. Eine abgeschlossene Untergruppe H einer linearen algebraischen Gruppe ist eine Untergruppe von G, die abgeschlossen bezüglich Zariski-Topologie auf G ist. Die Inklusion $H \hookrightarrow G$ ist dann ein Homomorphismus von algebraischen Gruppen.

Bemerkung
$G \times G$ ist wie in 2 mit Zariski-Topologie versehen (und nicht mit Produkttopologie).

3.2 Die 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.
Der Gruppenstruktur von G entspricht eine „Koalgebrastruktur“ von A gemäß 2.9.

Morphismen von Gruppen	Algebrahomomorphismen
Multiplikation	*Komultiplikation*
$\mu\colon G \times G \longrightarrow G$	$\Delta = \mu^*\colon A \longrightarrow A \otimes_K A \underset{2.17}{\simeq} K[G \times G]$
Eins	*Koeins (Augmentation)*

Morphismen von Gruppen	Algebrahomomorphismen
$e\colon \{e\} \longrightarrow G$	$\varepsilon = e^*\colon A \longrightarrow K\,,\ f \longmapsto f(e)$
Inverses	*Koinverses* (auch *Antipode* genannt)
$i\colon G \longrightarrow G\,,\ x \longmapsto x^{-1}$	$\iota = i^*\colon A \longrightarrow A\,,\ f \longmapsto (x \longmapsto f(x^{-1}))$
Konstanter Morphismus	
$p\colon G \longrightarrow G\,,\ x \longmapsto e$	$p^*\colon A \longrightarrow A\,,\ f \longmapsto (x \longmapsto f(e))$
Assoziativität von G	*Koassoziativität*

$$\begin{tikzcd} G \times G \times G \arrow[r, "\mu\times\mathrm{id}"] \arrow[d, "\mathrm{id}\times\mu"'] & G \times G \arrow[d, "\mu"] \\ G \times G \arrow[r, "\mu"] & G \end{tikzcd} \qquad \begin{tikzcd} A \otimes_K A \otimes_K A & A \otimes_K A \arrow[l, "\Delta\otimes\mathrm{id}"'] \\ A \otimes_K A \arrow[u, "\mathrm{id}\otimes\Delta"] & A \arrow[l, "\Delta"] \arrow[u, "\Delta"'] \end{tikzcd}$$

$ex = xe = x\ \forall\, x \in G$ Identifiziere $K \otimes_K A = A = A \otimes_K K$

$$\begin{tikzcd} G \arrow[r, "(p{,}\mathrm{id})"] \arrow[d, "(\mathrm{id}{,}p)"'] \arrow[dr, "\mathrm{id}"] & G \times G \arrow[d, "\mu"] \\ G \times G \arrow[r, "\mu"] & G \end{tikzcd} \qquad \begin{tikzcd} A & A \otimes_K A \arrow[l, "\varepsilon\otimes\mathrm{id}"'] \\ A \otimes_K A \arrow[u, "\mathrm{id}\otimes\varepsilon"] & A \arrow[l, "\Delta"] \arrow[u, "\Delta"'] \arrow[ul, "\mathrm{id}"'] \end{tikzcd}$$

$x^{-1}x = xx^{-1} = e$

$$\begin{tikzcd} G \arrow[r, "(i{,}\mathrm{id})"] \arrow[d, "(\mathrm{id}{,}i)"'] \arrow[dr, "p"] & G \times G \arrow[d, "\mu"] \\ G \times G \arrow[r, "\mu"] & G \end{tikzcd} \qquad \begin{tikzcd} A & A \otimes_K A \arrow[l, "m\circ(\iota\otimes\mathrm{id})"'] \\ A \otimes_K A \arrow[u, "m\circ(\mathrm{id}\otimes\iota)"] & A \arrow[l, "\Delta"] \arrow[u, "\Delta"'] \arrow[ul, "p^*"'] \end{tikzcd}$$

Man nennt A 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 2.11.3 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

$$\Delta_0\colon A_0 \longrightarrow A_0 \otimes_F A_0 \qquad \varepsilon_0\colon A_0 \longrightarrow F \qquad \iota_0\colon A_0 \longrightarrow A_0$$

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

3.4 Beispiele

1) *Die additive Gruppe* $G = \mathbb{G}_a(K)$. Dann ist $K[G] = K[X]$ der Polynomring in einer Unbestimmten X.

Es ist $\Delta(X) = X \otimes 1 + 1 \otimes X$.
$\iota(X) = -X$ und $\varepsilon(X) = 0$.
(Für $\mu\colon G \times G \longrightarrow G$, $(x,y) \longmapsto x+y$, ist $\mu^* = \Delta\colon K[G] \longrightarrow K[G \times G] \underset{2.17}{=} K[G] \otimes_K K[G]$ gegeben durch $\mu^*(X)(x,y) = (X \circ \mu)(x,y) = X(x+y) = x+y$, und es ist $(X \otimes 1 + 1 \otimes X)(x,y) \underset{2.17}{=} X(x) \cdot 1 + 1 \cdot X(y) = x+y$ nach 2.17(ii), Definition von $K[G] \otimes_F K[G] \xrightarrow{\sim} K[G \times G]$)

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* $GL_n(K) = \{x \in \mathrm{M}_{n\times n}(K) \mid \det(x) \neq 0\}$ ist eine offene Menge in $\mathrm{M}_{n\times n}(K) \simeq K^{n^2}$. Die Gruppenstruktur ist durch Matrizenmultiplikation gegeben, und $\mathrm{GL}_n(K)$ ist irreduzibel nach 2.4(b), (a), da K^{n^2} nach 2.3 irreduzibel ist.
Es ist $\mathrm{GL}_n(K)$ eine lineare algebraische Gruppe nach Definition 3.1 und 2.18.1 sowie 0.1.9, und es ist

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

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 Die Zusammenhangskomponente der Eins

Sei G eine lineare algebraische Gruppe.

Satz *(1) Es gibt genau eine irreduzible Komponente G^0 von G, die $e \in G$ 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 $G_1 \times \cdots \times G_m \xrightarrow{\text{stetig}} G_1 \cdot \ldots \cdot G_m$ 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 $G_j \subset G_i \; \forall\, j = 1, \ldots, m$, da $G_j \subset G_1 \cdot \ldots \cdot G_m$ und daher $G_j = G_i \; \forall\, j = 1, \ldots, m$, da G_j als irreduzible Komponente maximal ist nach Definition 2.5.1. Es ist also $m = 1$.

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

(i) G^0 ist eine Untergruppe von G:
Als Bild der Multiplikation $G^0 \times G^0 \longrightarrow G^0 G^0$ 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 $i \colon G \longrightarrow G^{-1}$, $x \longmapsto x^{-1}$, 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 $xG^0x^{-1} = G^0 \; \forall\, x \in G$ 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, ist nun (2) bewiesen.

(3) Nach Definition ist G genau dann zusammenhängend, wenn G nicht als disjunkte Vereinigung zweier abgeschlossener echter Teilmengen geschrieben werden kann, und es gilt: G irreduzibel $\Longrightarrow$ G zusammenhängend. Aus (2) folgt auch die umgekehrte Richtung, denn danach ist die Zerlegung von G in irreduzible Komponenten disjunkt (vgl. AGLA 10.1).

(4) Sei H eine abgeschlossene Untergruppe mit $(G : H) < \infty \Longrightarrow H^0$ ist abgeschlossene Untergruppe von G^0 mit $(G^0 : H^0) < \infty$
$\Longrightarrow G^0 = H^0 \cup \underbrace{g_1 H}_{\text{abgeschl.}} \cup \cdots \cup g_k H^0$ mit $k \in \mathbb{N}_0$ und $g_1, \ldots, g_k \in G^0$.
$\Longrightarrow G^0 \setminus H^0$ ist abgeschlossen (als endliche Vereinigung abgeschlossener Mengen)
$\Longrightarrow H^0 = G^0$, da $G^0 = \underbrace{H^0}_{\text{abg.}} \cup \underbrace{G^0 \setminus H^0}_{\text{abg.}}$ und G^0 irreduzibel und $H^0 \neq \emptyset$
$\Longrightarrow G^0 \subset H$.

$\square$

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 $G^0_{\mathbb{R}} = \mathrm{SO}_n(\mathbb{R}) := \{x \in G_{\mathbb{R}} \mid \det(x) = 1\}$, und $G_{\mathbb{R}}$ zerfällt in zwei irreduzible Komponenten

$$G_{\mathbb{R}} = G^0_{\mathbb{R}} \cup -eG^0_{\mathbb{R}}\,, \quad \text{wobei } e = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = E_n\,.$$

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

$$\boxed{UV = G}\,.$$

Beweis. Sei $g \in G$. Zu zeigen: $\boxed{U \cap gV^{-1} \neq \emptyset}$ (denn dann gibt es $u \in U$ und $v \in V$ mit $u = gv^{-1}$, und es folgt $g = uv \in UV$).
Es ist $\psi\colon G \longrightarrow G\,,\ x \longmapsto gx^{-1}$, 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: $U \cap gV^{-1} = \emptyset$.
$\Longrightarrow gV^{-1} \subset G \setminus U$ und $G \setminus U$ ist abgeschlossen, da U offen ist
$\Longrightarrow \overline{gV^{-1}} \subset G \setminus U$ nach Definition des Abschlusses
$\Longrightarrow U \underset{\text{Vor.}}{\subset} G = \overline{gV^{-1}} \subset G \setminus U$
Dies ist ein Widerspruch, da $U \neq \emptyset$. □

Bemerkung
Ist G irreduzibel, so ist $G = UV$, falls U, V offen und nicht leer sind.

3.7 Der 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 $G \xrightarrow{\sim} G\,,\; x \longmapsto x^{-1}$, ein Homöomorphismus ist, folgt $\overline{H}^{\,-1} = \overline{H^{-1}} \underset{H \text{ Gruppe}}{=} \overline{H}\,.$
Da $G \longrightarrow G\,,\; x \longmapsto gx\,$, 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 $y \in \overline{H} \Longrightarrow Hy \subset H\overline{H} = \overline{H} \Longrightarrow \overline{H}y = \overline{Hy} \subset \overline{H}\,.$
Also 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

Benutze folgendes

Fundamentallemma
Sei $\alpha\colon V \longrightarrow W$ ein Morphismus von Varietäten. Dann enthält $\alpha(V)$ eine nicht leere Menge, die offen in $\overline{\alpha(V)}$ ist.

Der Beweis wird nachgetragen.

Satz
Sei $\alpha\colon G \longrightarrow G'$ 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 Fundementallemma 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 $(\alpha(G) : \alpha(G^0)) < \infty$, und es folgt $\alpha(G^0) \supset (\alpha(G))^0$ nach 3.5(4).

□

3.9 Operationen von G

Sei G eine lineare algebraische Gruppe, die vermöge

$$\alpha\colon G \times V \longrightarrow V\,,\ (x,v) \longmapsto xv\,,$$

auf einer affinen Varietät V operiere. Es gilt dann

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

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

$$\begin{array}{ccccc}
K[V] & \xrightarrow{\alpha^*} & K[G \times V] & \underset{2.17}{\simeq} & K[G] \otimes_K K[V] \\
\| & & \| & & \\
\mathrm{Mor}(V,K) & \longrightarrow & \mathrm{Mor}(G \times V, K) & &
\end{array}$$

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

wobei

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

gilt. Der Homöomorphismus $V \longrightarrow V,\ v \longmapsto g^{-1}V$, induziert einen K-Algebrahomomorphismus

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

genannt *Linkstranslation mit* G, und es gilt

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

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. $\lambda_g(W) \subset W \quad \forall\, g \in G$.

(ii) $\lambda_g(Z) \subset Z \Longleftrightarrow \alpha^*(Z) \subset K[G] \otimes_K Z$.

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 $h_1, \ldots, h_n$ 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 $\{z_1, \ldots, z_k\}$ eine Basis von Z, so bildet man die Summe der Räume, die man in der oben beschriebenen Weise zu jedem $z_i, i = 1, \ldots, k$ erhält, und (i) folgt.

(ii) "$\Longrightarrow$": 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.
"$\Longleftarrow$": Sei $\lambda_g(Z) \subset Z \;\forall\, g \in G$. 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

$$\lambda_g(f) = \sum_{i=1}^{k} u_i(g^{-1})z_i + \sum_{j}^{\text{endlich}} v_j(g^{-1})h_j \in Z \;\forall\, g \in G\,,$$

also $v_j(g^{-1}) = 0 \;\forall\, g \in G$, d.h. $v_j = 0$. Es folgt $\alpha^*(f) = \sum_{i=1}^{k} u_i \otimes z_i \in K[G] \otimes_k Z$ für jedes $f \in Z$.

□

3.10 Linearisierung affiner Gruppen

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

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

und die *Rechtstranslation*

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

Hierdurch erhält man injektive Gruppenhomomorphismen

$$\lambda\colon G \longrightarrow \mathrm{GL}(K[G]),\ g \longmapsto \lambda_g$$
$$\rho\colon G \longrightarrow \mathrm{GL}(K[G]),\ g \longmapsto \rho_g\,.$$

Es ist $\rho_g = \iota \circ \lambda_g \circ \iota^{-1}$, wobei $\iota\colon K[G] \longrightarrow K[G]$ 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 $\{h_1, \dots, h_k\}$ von $K[G]$ als K-Algebra. Nach 3.9(i) gibt es einen ρ-stabilen Untervektorraum W von $K[G]$ mit $\{h_1, \dots, h_k, h_{k+1}, \dots, h_n\}$ als Basis. Nach 3.9(1) und 3.9(i) gibt es Elemente $a_{ij} \in K[G]$ mit $1 \le i, j \le n$ mit

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

Es ist also $(a_{ij}(g))_{1\le i,j\le n}$ die Matrix von $\rho_g|_W$ bezüglich der Basis $\{h_1, \dots, h_n\}$.
Es ist $\psi\colon G \longrightarrow \mathrm{GL}_n(K),\ g \longmapsto a_{ij}(g)$, ein Morphismus von algebraischen Gruppen. Es ist ψ injektiv:
Sei $\psi(g) = e \Longrightarrow \rho_g(h_j) = h_j\ \forall\, j$
$\Longrightarrow \rho_g(f) = f\ \forall\, f \in K[G]$, da $h_1, \dots, h_n$ die Algebra $K[G]$ erzeugen und ρ_g ein Algebrahomomorphismus ist
$\Longrightarrow \rho_g = \mathrm{id} \Longrightarrow g = e\,.$
Die Gruppe $\psi(G)$ ist abgeschlossen in $\mathrm{GL}_n(K)$ nach 3.8(i). Noch zu zeigen ist, daß ψ ein Morphismus von Varietäten ist. Es ist

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

gegeben durch $\psi^*(X_{ij}) = a_{ij}$ und $\psi^*(d^{-1}) = \det(a_{ij})^{-1}$. 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 $h_j = \sum_{i=1}^{n} h_j(g) a_{ij}$. Hieraus folgt, daß ψ^* surjektiv ist (und also $\psi(G)$ abgeschlossen in $\mathrm{GL}_n(K)$ nach Aufgabe 26(b)).
Es ist $K[\psi(G)] \simeq K[\mathrm{GL}_n(K)]/\ker(\psi^*) \simeq K[G]$ und also vermittelt ψ einen Isomorphismus $G \simeq \psi(G)$ nach 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 $f_1, \dots, f_k$ als Erzeugendensystem der F-Strukturen.

4 Jordanzerlegung

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

$$W_\lambda := \{w \in W \mid \sigma(w) = \lambda w\} = \mathrm{kern}(\sigma - \lambda\,\mathrm{id})$$

stabil unter allen $\tau \in S$, denn es gilt:
$w \in W_\lambda \Longrightarrow \sigma(\tau(w)) \underset{\text{Vor.}}{=} \tau(\sigma(w)) \underset{\text{Def. von } W_\lambda}{=} \tau(\lambda w) \underset{\tau \text{ lin.}}{=} \lambda\tau(w) \; \forall \tau \in S$
$\Longrightarrow \tau(w) \in W_\lambda \; \forall \tau \in S$.
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 9.12).
Nach Wahl von σ ist $k > 1$ und also $\dim_K W_{\lambda_i} < n \; \forall\, i = 1, \ldots, k$. Die Induktionsvoraussetzung angewandt auf jedes λ_i ergibt dann die Behauptung. □

4.2 Additive Jordanzerlegung

Satz

Seien K ein Körper, W ein endlich-dimensionaler K-Vektorraum und $\sigma \in \mathrm{End}_K(W)$ ein Endomorphismus, dessen Eigenwerte in K liegen. Dann gelten:

(i) Es gibt eindeutig bestimmte Elemente $\sigma_s, \sigma_n \in \mathrm{End}_K(W)$ mit den Eigenschaften

- *(a) σ_s ist diagonalisierbar, und σ_n ist nilpotent*
- *(b) $\sigma = \sigma_s + \sigma_n$*
- *(c) $\sigma_s \circ \sigma_n = \sigma_n \circ \sigma_s$.*

(ii) *Es gibt Polynome $P, Q \in K[X]$ ohne konstanten Term mit $P(\sigma) = \sigma_s$ und $Q(\sigma) = \sigma_n$. Insbesondere kommutieren σ_s und σ_n mit jedem Endomorphismus von W, der mit σ kommutiert.*

(iii) *Ist $Z \subset W$ ein σ-stabiler Untervektorraum von W, so ist Z auch σ_s- und σ_n-stabil, und $\sigma|_Z = \sigma_s|_Z + \sigma_n|_Z$ ist die additive Jordanzerlegung von Z.*

Beweis. (i) Nach Voraussetzung zerfällt das charakteristische Polynom P von σ in Linearfaktoren, also $P = \pm\prod_{i=1}^{k}(X - \lambda_i)^{n_i}$, wobei $\lambda_1, \dots, \lambda_k$ paarweise verschieden seien und $n_1, \dots, n_k \in \mathbb{N}$.
Sei $W_i := \operatorname{kern}((\sigma - \lambda_i \operatorname{id})^{n_i})$ der *verallgemeinerte Eigenraum zum Eigenwert* λ_i für $k = 1, \dots, k$. Nach AGLA 13.3 gilt $W = W_1 \oplus \cdots \oplus W_k$ und $\dim_K W_i = n_i$ sowie $\sigma(W_i) \subset W_i \ \forall\, i = 1, \dots, k$.
Nach dem Chinesischen Restsatz Algebra 8.12 gibt es ein Polynom $P \in K[X]$ mit

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

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

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

denn: $P \equiv \lambda_i \bmod (X - \lambda_i)^{n_i}$
$\Longrightarrow \exists\, f_i \in K[X]$ mit $P - \lambda_i = f_i(X - \lambda_i)^{n_i}$
$\underset{P(\sigma)=\sigma_{\mathrm{s}}}{\Longrightarrow} \sigma_{\mathrm{s}} - \lambda_i \operatorname{id} = f_i(\sigma)(X - \lambda_i)^{n_i}$
$\Longrightarrow \sigma_{\mathrm{s}}(w) - \lambda_i w = 0 \ \forall\, w \in W_i$ nach Definition von W_i.
Also ist $\sigma_{\mathrm{s}}|_{W_i}$ diagonalisierbar für alle $i = 1, \dots, k$ und daher auch σ_{s}, da $W = W_1 \oplus \cdots \oplus W_k$. Ferner folgt, daß $\boxed{\sigma_{\mathrm{n}} := \sigma - \sigma_{\mathrm{s}}}$ nilpotent ist, denn für jedes $w \in W_i$ ist

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

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 σ_{n} und σ'_{n} kommutieren. Also gilt

$$\underbrace{\sigma_{\mathrm{s}} - \sigma'_{\mathrm{s}}}_{\text{diag.}} = \underbrace{\sigma'_{\mathrm{n}} - \sigma_{\mathrm{n}}}_{\text{nilpot.}} \quad \text{folgt aus 4.1, vgl. Aufgabe 34}.$$

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 $\sigma'_\mathrm{n} - \sigma_\mathrm{n} = 0$.✓

(ii) Wie in (i) definiert, ist $\sigma_\mathrm{s} = P(\sigma)$ und $\sigma_\mathrm{n} = Q(\sigma)$ mit $Q = X - P$. ✓

(iii) Aus (ii) folgt, daß Z von σ_s und σ_n stabilisiert wird. Das charakteristische Polynom von $\sigma|_Z$ teilt das charakteristische Polynom von σ nach AGLA 13.1 und (iii) folgt analog wie in (i) mit dem Polynom P.

□

4.3 Multiplikative Jordanzerlegung

Korollar

Seien K ein Körper, W ein endlich-dimensionaler K-Vektorraum und $\sigma \in \mathrm{Aut}_K(W)$ ein Automorphismus, dessen Eigenwerte alle in K liegen. Dann besitzt σ eine eindeutige Zerlegung

$$\boxed{\sigma = \sigma_s \circ \sigma_u},$$

wobei $\sigma_s \in \mathrm{Aut}_K(W)$ diagonalisierbar und $\sigma_u \in \mathrm{Aut}_K(W)$ unipotent *(d.h. $\sigma_u - \mathrm{id}$ nilpotent) ist und*

$$\boxed{\sigma_s \circ \sigma_u = \sigma_u \circ \sigma_s}$$

gilt. Ferner gilt: Ist Z ein σ-stabiler Untervektorraum von W, so ist Z auch σ_s- und σ_u-stabil, und $\sigma|_Z = \sigma_s|_Z \circ \sigma_u|_Z$ ist die multiplikative Jordanzerlegung von $\sigma|_Z$.

Beweis. Seien $\lambda_1, \dots, \lambda_m$ die Eigenwerte von σ, 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 4.2(b) ist $\sigma = \sigma_\mathrm{s} \circ \sigma_\mathrm{u}$ mit

$$\boxed{\sigma_\mathrm{u} = \mathrm{id} + \sigma_\mathrm{s}^{-1}\sigma_\mathrm{n}},$$

und nach 4.2(a), (c) ist σ_u unipotent. Alles weitere folgt nun leicht aus 4.2. □

4.4 Jordanzerlegung von Matrizen

Seien K ein Körper und $\overline{K}$ ein algebraischer Abschluß von K .

Definition 1) Eine Matrix $x \in \mathrm{M}_{n\times n}(K)$ heißt *halbeinfach* („semisimple"), wenn x über $\overline{K}$ diagonalisierbar ist, d.h. wenn es ein $s \in \mathrm{GL}_n(\overline{K})$ gibt, so daß sxs^{-1} eine Diagonalmatrix in $\mathrm{M}_{n\times n}(\overline{K})$ ist.
Analog heißt ein Endomorphismus $\sigma\colon W \longrightarrow W$ *halbeinfach*, wenn $\sigma \otimes \mathrm{id}\colon W \otimes_K \overline{K} \longrightarrow W \otimes_K \overline{K}$ diagonalisierbar ist. Hierbei gelte $\dim_K W < \infty$.
Im Fall $K = \overline{K}$ stimmen die Begriffe „halbeinfach" und „diagonalisierbar" überein.

2) Eine Matrix $x \in \mathrm{M}_{n\times n}(K)$ heißt *unipotent*, wenn $x - E_n$ nilpotent ist.
Beispiel
$x = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) \Longrightarrow x - E_2 = \left(\begin{smallmatrix} 0 & a \\ 0 & 0 \end{smallmatrix}\right)$ 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 $x = x_s + x_n$ und jede Matrix $g \in \mathrm{GL}_n(K)$ eine Jordanzerlegung $g = g_s g_u = g_u g_s$, wobei g_s, x_s halbeinfach, x_n nilpotent und g_u unipotent sind. Die Zerlegungen sind eindeutig.

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

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

in K. Dann besitzt σ eine eindeutige Zerlegung

$$\boxed{\sigma = \sigma_{\mathrm{s}} \circ \sigma_{\mathrm{u}}}$$

wobei $\sigma_{\mathrm{s}} \in \mathrm{Aut}_K(W)$ diagonalisierbar und $\sigma_{\mathrm{u}} \in \mathrm{Aut}_K(W)$ unipotent ist (d.h. $\sigma - \mathrm{id}$ nilpotent) und

$$\boxed{\sigma_{\mathrm{s}} \circ \sigma_{\mathrm{u}} = \sigma_{\mathrm{u}} \circ \sigma_{\mathrm{s}}}$$

gilt in K. Die Behauptung folgt nun aus 4.2 und 4.3, vgl. auch AGLA 4.4, 4.11 und 4.16. □

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.

4.5 Jordanzerlegung von $K[G]$

Seien K algebraisch abgeschlossen, G eine lineare algebraische Gruppe und $K[G] = \mathrm{Mor}(G, K)$ die affine Algebra zu G. Der Isomorphismus $G \longrightarrow G$, $x \longmapsto xg$ induziert nach 2.9 für jedes $g \in G$ einen K-Algebraautomorphismus

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

genannt *Rechtstranslation* mit g. Es ist also $(\rho_g(f))(x) = f(xg)\ \forall\, x \in G$.

Satz

Für jedes $g \in G$ besitzt die Rechtstranslation $\rho_g \colon K[G] \longrightarrow K[G]$ eine Jordanzerlegung

$$\rho_g = (\rho_g)_s \circ (\rho_g)_u = (\rho_g)_u \circ (\rho_g)_s\,,$$

so daß $(\rho_g)_s|_W$ halbeinfach und $(\rho_g)_u|_W$ 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 $n \in \mathbb{N}$ sowie $K[G] = \bigcup_{n\in\mathbb{N}} W_n$ 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 $K[G]$ für den gilt $\rho_g(W_1) \subset W_1\ \forall\, g \in G$.
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 ist mit der Jordanzerlegun von $\rho_g|_{W_{n-1}}$.
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. $\square$

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 $\rho_g \colon K[G] \longrightarrow K[G]$ wie in 4.5 beschrieben.

Satz *(i) Zu jedem $g \in G$ gibt es eindeutig bestimmte Elemente g_s und $g_u \in G$ mit den Eigenschaften $(\rho_g)_s = \rho_{g_s}$ und $(\rho_g)_u = \rho_{g_u}$ sowie $g = g_s g_u = g_u g_s$.*

(ii) Ist $\alpha \colon G \longrightarrow G'$ ein Homomorphismus von algebraischen Gruppen, so ist $\alpha(g_s) = \alpha(g)_s$ und $\alpha(g_u) = \alpha(g)_u$ 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 $\mu \colon K[G] \otimes_K K[G] \longrightarrow K[G]$ die Multiplikation in $K[G]$. Da ρ_g ein K-Algebrahomomorphismus ist, gilt

$$\mu \circ (\rho_g \otimes \rho_g) = \rho_g \circ \mu \,.$$

Wie man mit Hilfe von 4.3, 4.2 nachprüft, folgt hieraus $\mu \circ ((\rho_g)_{\mathrm{s}} \otimes (\rho_g)_{\mathrm{s}}) = (\rho_g)_{\mathrm{s}} \circ \mu$. Es ist also

$$(\rho_g)_{\mathrm{s}} \colon K[G] \longrightarrow K[G] \,,\ f \longmapsto (\rho_g)_{\mathrm{s}}(f)$$

ein K-Algebrahomomorphismus, was wiederum einen K-Algebrahomomorphismus

$$\varphi \colon K[G] \longrightarrow K \,,\ f \longmapsto ((\rho_g)_{\mathrm{s}}(f))(e) \,,$$

ergibt. Nach Aufgabe 17 gibt es einen Punkt $g_{\mathrm{s}} \in G$, so daß $f(g_{\mathrm{s}}) = \varphi(f)\ \forall\, f \in K[G]$ gilt. Es ist also

$$\boxed{f(g_{\mathrm{s}}) = ((\rho_g)_{\mathrm{s}}(f))(e)\ \forall\, f \in K[G]}\,.$$

Da ρ_g ein Automorphismus ist, der mit allen Linkstranslationen

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

kommutiert, folgt aus 4.2(ii), daß $(\rho_g)_{\mathrm{s}}$ mit λ_x kommutiert für jedes $x \in G$. Für alle $f \in K[G]$ und $x \in G$ folgt nun

$$\begin{aligned} ((\rho_g)_{\mathrm{s}}(f))(x) &= ((\lambda_{x^{-1}} \circ (\rho_g)_{\mathrm{s}})(f))(e) \quad \text{nach Definition von } \lambda_{x^{-1}} \\ &= (((\rho_g)_{\mathrm{s}} \circ \lambda_{x^{-1}})(f))(e) \quad \text{nach 4.2(ii)} \\ &= (\lambda_{x^{-1}}(f))(g_{\mathrm{s}}) \quad \text{nach Definition von } g_{\mathrm{s}} \\ &= f(xg_{\mathrm{s}}) \quad \text{nach Definition von } \lambda_{x^{-1}} \\ &= (\rho_{g_{\mathrm{s}}}(f))(x) \end{aligned}$$

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

(ii) $\alpha\colon G \longrightarrow G'$ 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 $\alpha^*\colon K[G'] \longrightarrow K[G]$ 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 $(\rho_x(f))(y) = f(yx) = 0\ \forall\, y \in G,\ f \in I$ und also $\rho_x(f) \in I\ \forall\, f \in I$.
Sei umgekehrt $\rho_x(f) \subset I$ für ein $x \in G'$. Dann gilt $(\rho_x(f))(e) = 0$ $\forall\, f \in I$ und also $f(x) = 0\ \forall\, f \in I$. Es folgt $x \in \mathfrak{V}_{G'}(\mathfrak{I}_{G'}(G)) \underset{\text{Aufg18}}{=} G$.
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 $K^n \longrightarrow K^n,\ v \longmapsto xv$. Für $g \in G$ zeigen wir

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

mit einer injektiven K-linearen Abbildung $\widetilde{\varphi}\colon K^n \longrightarrow K[G]$.
Da $(\rho_g)_\mathrm{s}|_{\mathrm{bild}(\widetilde{\varphi})}$ nach 4.5 halbeinfach ist, ist dann auch g_s halbeinfach.
Sei $\varphi \neq 0$ in $\mathrm{Hom}_K(K^n, K)$. Dann ist

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

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

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

Analog ist $g_{\mathrm{u}} = \tilde{\varphi}^{-1} \circ (\rho_g)_{\mathrm{u}} \circ \tilde{\varphi}$ 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 $E_n := \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = 1_{\mathrm{M}_{n\times n}(K)}$.

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 von G heißt *unipotent*, wenn jedes Element aus U unipotent ist.

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

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

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 $\mu\colon G_{\mathrm{s}} \times G_{\mathrm{u}} \longrightarrow G$ 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 $x, y \in G_{\mathrm{s}} \underset{4.1}{\Longrightarrow} \exists\, g \in G$, so daß gxg^{-1} und gyg^{-1} Diagonalmatrizen sind. $\Longrightarrow gxyg^{-1} = \underbrace{gyg^{-1}}_{\text{diag.}}\underbrace{gyg^{-1}}_{\text{diag.}}$ ist eine Diagonalmatrix.
Es ist $g^{-1}x^{-1}g = (gxg^{-1})^{-1}$ eine Diagonalmatrix und also $x^{-1} \in G_{\mathrm{s}}$.
Ferner $E_n \in G_{\mathrm{s}}$.

(2) G_{u} ist eine Untergruppe von G, denn:
Seien $x, y \in G_{\mathrm{u}}$
$\Longrightarrow x = E_n + a$ und $y = E_n + b$ mit nilpotenten Matrizen $a, b \in \mathrm{M}_{n\times n}(K)$
$\Longrightarrow xy = E_n + b + a + ab$.
Es ist ab nilpotent, da $xy = yx$ und also $ab = ba$.
Daher ist $b + a + ab$ nilpotent.
$\Longrightarrow xy \in G_{\mathrm{u}}$
Es ist $x^{-1} = E_n - \dfrac{a}{E_n + a} \in G_{\mathrm{u}}$ und $E_n \in G_{\mathrm{u}}$.

(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 0.1.4 und 5. 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

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

in $\Delta_n(K)$ eingebettet werden kann. Die Jordanzerlegung wird dabei nach 4.6(ii) respektiert.
Sei also o.E. $G \subset \Delta_n(K)$ (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 $G_{\mathrm{s}} \hookrightarrow \mathrm{D}_n(K)$, $g_{\mathrm{s}} \longmapsto x g_{\mathrm{s}} x^{-1}$, in $\mathrm{D}_n(K)$ eingebettet werden kann. Für jedes $g \in G$ gilt dann

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

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

(5) $\mu^{-1}\colon G \longrightarrow G_{\mathrm{s}} \times G_{\mathrm{u}}$, $g \longmapsto (g_{\mathrm{s}}, g_{\mathrm{u}})$, ist ein Morphismus, denn:
Die Eigenwerte von $g =: (a_{ij}) \in G \underset{(4)}{\subset} \Delta_n(K)$ sind 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(i)), und $g_{\mathrm{s}} \underset{(4)}{\in} \mathrm{D}_n(K)$ ist, folgt aus 4.2, daß g_{s} der Diagonalanteil von g ist. Daher ist die Projektion $\pi_{\mathrm{s}}\colon G \longrightarrow G_{\mathrm{s}}$, $g \longmapsto g_{\mathrm{s}}$, ein Morphismus und ebenso die Projektion $\pi_{\mathrm{u}}\colon G \longrightarrow G_{\mathrm{u}}$, $g \longmapsto g_{\mathrm{s}}^{-1} g = g_{\mathrm{u}}$. ✓

(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 $\pi_{\mathrm{s}}, \pi_{\mathrm{u}}$ nach (5) stetig sind.

□

5.2 Eindimensionale Gruppen

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

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

Ist V irreduzibel, so ist die *Dimension* von V der Tranzendenzgrad des Quotientenkörpers $K(V)$.

Ist $K[V] = K[x_1, \ldots, x_n]$, so ist $\dim V$ die maximale Anzahl algebraisch unabhängiger Elemente unter den x_i (vgl. 1.2, 1.8 und 2.6).

Beispiele(1) Ist $G = \mathbb{G}_{\mathrm{m}}(K)$ die multiplikative Gruppe
$\Longrightarrow K[G] = K[X, X^{-1}] \Longrightarrow \dim G = 1$, und G ist diagonalisierbar nach 0.1.8.

(2) Ist $G = \mathbb{G}_{\mathrm{a}}(K)$ die additive Gruppe
$\Longrightarrow K[G] = K[X] \Longrightarrow \dim G = 1$, 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 $K[V_1] \otimes_K K[V_2] \underset{2.17}{=} K[V_1 \times V_2]$.

(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 $K[V_2]$. Dann sind $x_1, \ldots, x_d$ algebraisch unabhängig in $K[V_1]$. Es folgt $d \leq \dim V_2$.
Angenommen $d = \dim V_2$. Sei $a \neq 0$ in $\mathfrak{p}$. 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 $x_1, \ldots, x_d$ 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 $\chi\colon G \longrightarrow \mathbb{G}_{\mathrm{m}}(K)$. Das Produkt zweier Charaktere χ, ψ ist definiert durch

$$(\chi\psi)(x) = \chi(x)\psi(x)\ \forall\, x \in G\,.$$

Die Charaktere von G bilden eine abelsche Gruppe $X^*(G)$, genannt *Charaktergruppe von* G.
Es ist $X^*(G) \subset K[G] \underset{2.7}{=} \mathrm{Mor}(G, K)$. 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 $G \longrightarrow L^*$ eine linear unabhängige Teilmenge der Menge aller Funktionen $G \longrightarrow L$.

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

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

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

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

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

Definition
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 $\alpha\colon G \longrightarrow \mathrm{GL}_n(K)$ 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 2.9 einen surjektiven K-Algebrahomomorphismus

$$\iota^*\colon K[\mathbb{D}_n] \longrightarrow K[G]\,,\ f \longmapsto f|_G\,.$$

Dann wird $K[G]$ nach Beispiel 5.3 erzeugt von den Restriktionen von Charakterern von $\mathbb{D}_n$. Mit Lemma 5.3 folgt, daß $X^*(G)$ eine Basis von $K[G]$ ist. Also ist der Homomorphismus $X^*(\mathbb{D}_n) \longrightarrow X^*(G)$ 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): Als K-Algebra wird $K[G]$ von endlich vielen Charakteren $\chi_1, \ldots, \chi_d$ erzeugt. Definiere

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

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 $\alpha\colon G \longrightarrow G'$ ein Morphismus von algebraischen Gruppen, so ist $\alpha(G)$ diagonalisierbar.

Beweis. (i) Der von der Inklusion $\iota\colon H \hookrightarrow G$ induzierte K-Algebrahomomorphismus

$$\iota^*\colon K[G] \longrightarrow K[H]\,,\ f \longmapsto f|_H\,,$$

ist surjektiv nach 2.9. 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 (a) $\Longrightarrow$ (b) ist H diagonalisierbar.

(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 $\chi\colon G \longrightarrow \mathbb{G}_m(K) =: \mathbb{G}_m$ ein Charakter. Dann ist $\chi(G)$ zusammenhängend nach 2.4(c). Die einzigen zusammenhängenden Untergruppen von $\mathbb{G}_m$ sind $\{1\}$ und $\mathbb{G}_m$. Es folgt $\chi^n \neq 1\ \forall\, n > 1$. □

5.6 Tori

Definition
Sei K algebraisch abgeschlossen. Eine lineare algebraische Gruppe G heißt *algebraischer Torus* oder kurz *Torus*, falls $G \simeq \mathrm{D}_n(K)$ gilt.

Satz
Für eine lineare algebraisch 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 $\mathrm{D}_n(K) \simeq \underbrace{\mathrm{GL}_1(K) \times \cdots \times \mathrm{GL}_1(K)}_{n \text{ Kopien}}$ gilt und $\mathrm{GL}_1(K)$ nach 3.4.3 irreduzibel ist, ist auch $\mathrm{D}_n(K)$ irreduzibel nach 2.17(iii). Ferner folgt $\dim_K \mathrm{D}_n(K) = n$ nach 5.3(a).

(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. Wie im Beweis von Satz 5.4 induziert die Inklusion $G^0 \hookrightarrow \mathbb{D}_m$ einen surjektiven Gruppenhomomorphismus

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

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

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

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

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

Nach 3.5(ii) ist $H \simeq G/G^0$ eine abelsche Gruppe. Ferner ist die Multiplikation $H \times G^0 \longrightarrow G$ ein Isomorphismus von algebraischen Gruppen. Da H endlich ist, besteht H aus Einheitswurzeln aus K.
Ist $\operatorname{char}(K) = p > 0$, so besitzt K aber keine p-te Einheitswurzel $\neq 1$ nach Algebra 17.13. □

5.8 Torsion in diagonalisierbaren Gruppen

Korollar
Sei K algebraisch abgeschlossen, und sei G diagonalisierbar wie in 5.7. Dann ist die Torsionsuntergruppe G_{tors} von G dicht in G.

Beweis. Nach 5.7 ist

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

mit einer endlichen Gruppe H und $\mathbb{G}_m = K^*$. Es genügt also, die Behauptung für $G = \mathbb{G}_m$ 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 $\overline{G_{\mathrm{tors}}} = \mathbb{G}_m$ 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 17.3.3 und 5.8)
Sei V eine irreduzible Varietät, und sei $\alpha \colon V \times H \longrightarrow H'$ ein Morphismus von Varietäten, so daß zusätzlich gilt:

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

Satz
Dann ist die Abbildung

$$V \longrightarrow \operatorname{Mor}(H,H')\,,\ v \longmapsto \alpha_v\,,$$

konstant.

Beweis. Für $h \in H$ ist die Abbildung $\beta_h \colon V \longrightarrow H'$, $v \longmapsto \alpha(v,h)$ ein Morphismus von Varietäten, da α ein solcher ist. Ist $\operatorname{ord}(h) < \infty$, 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

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

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

5.10 Normalisator und Zentralisator

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

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

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

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

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

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

der *Zentralisator von* H *in* G und

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

der *Normalisator von* H *in* G.

Lemma

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

Beweis. Für jedes $h \in H$ ist $\alpha_h \colon G \longrightarrow G$, $g \longmapsto ghg^{-1}$ 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 $\alpha_h^{-1}(\{h\}) = \operatorname{Stab}(h)$ abgeschlossen in G. Es folgt, daß $\mathcal{N}_G(H) = \bigcap\limits_{h \in H} \alpha_h^{-1}(H)$ und $\mathcal{Z}_G(H) = \bigcap\limits_{h \in H} \operatorname{Stab}(h)$ abgeschlossen in G sind.
Es sind $\operatorname{Stab}(h)$ und $\mathcal{N}_G(H)$ Untergruppen von G nach Algebra 2.3 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 $\mathcal{Z}_G(H) \triangleleft \mathcal{N}_G(H)$. □

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 $\alpha\colon V \times H \longrightarrow H$, $(x,h) \longmapsto xhx^{-1}$, an. Dann ist $V \longrightarrow \operatorname{Mor}(H,H)$, $x \longmapsto \alpha_x$, mit $\alpha_x(h) = xhx^{-1}\ \forall\, h \in H$ konstant, und also gilt $\alpha_x = \alpha_e$ für alle $x \in V$. Es folgt $x \in \mathcal{Z}_G(H)^0\ \forall\, x \in V$. 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 1.7) 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 Steinberg, S.73).

5.11 Bemerkung über auflösbare Gruppen

Für auflösbare (also nicht notwendig kommutative) Gruppen gilt der folgende
Struktursatz
Sei G eine zusammenhängende auflösbare lineare algebraische Gruppe über einem algebraisch abgeschlossenen Körper. Dann gelten:

(i) *G_u ist abgeschlossener Normalteiler in G, der die Kommutatorgruppe $[G, G]$ enthält, und G_u ist zusammenhängend.*

(ii) *G/G_u ist ein Torus.*

(iii) *G nilpotent $\Longleftrightarrow$ G_s ist eine Untergruppe von G.*
In diesem Fall ist G_s abgeschlossen, und es ist $G = G_s \times G_u$.

(iv) *Die maximalen Tori in G sind konjugiert unter $\bigcap_{i \in \mathbb{N}_0} \mathcal{C}^i(G)$, wobei $\mathcal{C}^i(G)$ wie in Aufgabe 36 definiert ist.*

(v) *Ist T ein maximaler Torus in G, so ist $G = T \ltimes G_u$ (d.h. G_u ist Normalteiler in G sowie $G = TG_u$ und $T \cap G_u = \{e\}$).*

6 Die Liealgebra einer linearen algebraischen Gruppe

Sei K ein Körper.

6.1 Liealgebren

Definition1) Ein K-Vektorraum L zusammen mit einer bilinearen Abbildung

$$L \times L \longrightarrow L\,,\ (x,y) \longmapsto \underbrace{[xy]}_{\text{„Lie-Klammern"}}$$

heißt *Liealgebra*, wenn gilt:

(i) $[xx] = 0\ \forall\, x \in L\,,$

(ii) $[x[yz]] + [y[zx]] + [z[xy]] = 0\ \forall\, x, y, z \in L$ („Jacobi-Identität", ersetzt das Assoziativgesetz).

2) Eine Liealgebra L heißt *kommutativ*, falls $[xy] = 0\ \forall\, x, y \in L$ gilt.

3) Eine K-lineare Abbildung $\varphi\colon L \longrightarrow L'$ mit Liealgebren L, L' heißt *Homomorphismus*, falls $\varphi([xy]) = [\varphi(x), \varphi(y)]\ \forall\, x, y \in L$ gilt.

4) Ein Untervektorraum L' einer Liealgebra L heißt *Lieunteralgebra*, falls $[xy] \in L\ \forall\, x, y \in L'$ gilt.

Bemerkung
Ist L eine Lieunteralgebra, so gilt

$$\boxed{[xy] = -[yx] \quad \forall\, x, y \in L},$$

denn

$$\begin{aligned} 0 \underset{(i)}{=} [x+y, x+y] &\underset{\text{bil.}}{=} [x+y, x] + [x+y, y] \\ &\underset{\text{bil.}}{=} \underbrace{[xx]}_{=0} + [yx] + [xy] + \underbrace{[yy]}_{=0} \\ &\underset{(i)}{=} [yx] + [xy]\,.\checkmark \end{aligned}$$

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 Lieklammer 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 dieses 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 $\{e_0, \dots, e_{p-1}\}$ 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 (vgl. H. Chang: Über Wittsche Lie-Ringe, Abh. Math. Sem. Universität Hamburg 1941).

6.3 Derivationen

Definition
Seien R ein kommutativer Ring, A eine kommutative R-Algebra und M ein A-Linksmodul. Eine R-lineare Abbildung $D\colon A \longrightarrow M$ heißt *R-Derivation*, falls

$$\boxed{D(ab) = aD(b) + bD(a) \qquad \forall\, a, b, \in A}$$

gilt. Für eine R-Derivation $D\colon A \longrightarrow M$ 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 $D(r) = D(r \cdot 1) \underset{R \text{ lin.}}{=} rD(1) = 0$. ✓
Es ist

$$\boxed{\mathrm{Der}_R(A, M) := \{R\text{-Derivationen } A \longrightarrow M\}}$$

ein R-Modul. Sei $A = M$. Für $D_1, D_2 \in \mathrm{Der}_R(A, A)$ gilt dann

$$D_1 \circ D_2 - D_2 \circ D_1 \in \mathrm{Der}_R(A, A)\,.$$

Insbesondere ist die Derivation $\mathrm{Der}_K(A, A)$ 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 ist

$$D^p(ab) = \sum_{i=0}^{p} \binom{p}{i} D^i(a) D^{p-i}(b) = aD^p(b) + bD^p(a)$$

und D^p eine K-Derivation.

6.4 Differentialmoduln

Seien R ein kommutativer Ring und A eine kommutative R-Algebra. Es sei $\mu\colon A \otimes_R A \longrightarrow A$ die Multiplikation und $J := J_A := \mathrm{kern}\,\mu$.

Definition
Der $A \otimes_R A$-Modul

$$\boxed{\Omega_{A/R} := J/J^2}$$

heißt *Differentialmodul von A über R*. Es ist $\Omega_{A/R}$ auch ein A-Modul, da $J \cdot \Omega_{A/R} = (0)$ ist. Die Abbildung

$$d := d_{A/R}\colon A \longrightarrow \Omega_{A/R}\,,\ a \longmapsto a \otimes 1 - 1 \otimes a \bmod J^2$$

ist eine R-Derivation, genannt *universelle R-Derivation*
(Es ist $d(ab) = (a \otimes 1)d(b) + (1 \otimes b)d(a)$).

Bemerkung
Die Elemente $d(a)$ mit $a \in A$ erzeugen den A-Modul $\Omega_{A/R}$.

Beweis. Für $x = \sum\limits_i^{\text{endl.}} a_i \otimes b_i \in J$ gilt $\sum\limits_i a_i b_i = 0$ und also
$x = \sum\limits_i a_i(1 \otimes b_i - b_i \otimes 1) = -\sum\limits_i a_i(b_i \otimes 1 - 1 \otimes b_i)$. □

Satz
Das Paar $(\Omega_{A/R}, d)$ hat die folgende universelle Eigenschaft:
Für jeden A-Modul M ist die Abbildung

$$\Phi\colon \operatorname{Hom}_A(\Omega_{A/R}, M) \longrightarrow \operatorname{Der}_R(A, M)\,,\ \varphi \longmapsto \varphi \circ d\,,$$

ein Isomorphismus von A-Moduln.

Beweis. Φ ist A-Modulhomomorphismus, und Φ ist injektiv, da die Elemente $d(a)$ mit $a \in A$ den A-Modul $\Omega_{A/R}$ erzeugen.
Sei $D \in \operatorname{Der}_R(A, M)$. Dann erhält man durch $\psi(a \otimes b) = bD(a)$ eine R-lineare Abbildung $\psi\colon A \otimes_R A \longrightarrow M$, und es gilt

$$\psi(xy) = \underbrace{\mu(x)}_{=0}\psi(y) + \underbrace{\mu(y)}_{=0}\psi(x) = 0\ \forall\, x, y \in J\,.$$

Also induziert ψ eine R-lineare Abbildung $\varphi\colon \Omega_{A/R} \longrightarrow M$, und diese ist sogar A-linear. Es ist $\psi(a \otimes 1 - 1 \otimes a) = D(a)$. Also folgt $\varphi \circ d = D$. □

Bemerkung1) Seien K ein Körper, und $E = K(x)$ eine einfache Körpererweiterung von K. Dann gilt:

$$\dim_E(\Omega_{E/K}) \leq 1 \quad \text{und} \quad \boxed{\Omega_{E/K} = (0)} \quad\Longleftrightarrow\quad \boxed{E \text{ separabel (algebraisch über } K)}$$

2) Ist E eine algebraische Körpererweiterung von $K(X_1, \ldots, X_n)$, so gilt:

$$\dim_E \Omega_{E/K} \geq n \quad \text{und} \quad \boxed{\dim_E \Omega_{E/K} = n} \quad\Longleftrightarrow\quad \boxed{E \text{ separabel über } K(X_1, \ldots, X_n)}$$

6.5 Die Unteralgebra Lie(G)

Seien K algebraisch abgeschlossen, G eine lineare algebraische Gruppe, $A = K[G] = \operatorname{Mor}(G, K)$ die affine Algebra von G und

$$\lambda_g\colon A \longrightarrow A\,,\ f \longmapsto \begin{cases} G \longrightarrow K\,, \\ x \longmapsto f(g^{-1}x) \end{cases}$$

die *Linkstranslation mit $g \in G$.*

Definition

$$\boxed{\operatorname{Lie}(G) := \{D \in \operatorname{Der}_K(A, A) \mid \lambda_g \circ D = D \circ \lambda_g\ \forall\, g \in G\}}$$

Dann ist Lie(G) eine Lieunteralgebra von $\operatorname{Der}_K(A, A)$, genannt, *Liealgebra der linksinvarianten K-Derivationen.* Sie hat folgende Eigenschaften:

(a) $\operatorname{Lie} G = \operatorname{Lie} G^0$,

(b) $\dim_K \operatorname{Lie} G = \dim_K \operatorname{Lie} G^0$, insbesondere $\dim_K \operatorname{Lie} G < \infty$,

(c) Ist $\alpha\colon G \longrightarrow G'$ ein Morphismus von algebraischen Gruppen, so induziert α einen Liealgebrahomomorphismus $\overline{\alpha}\colon \operatorname{Lie} G \longrightarrow \operatorname{Lie} G'$. Um dies zu beweisen, zeigt man, daß $\operatorname{Lie} G$ als K-Vektorraum isomorph zum Tangentialraum $T_e(G)$ von G in e 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 $K[V] \longrightarrow K$, $f \longmapsto f(v)$. Der *Tangentialraum* T_vV *in* V ist der K-Vektorraum

$$\boxed{T_vV := \operatorname{Der}_K(K[V], K_v)}\,.$$

Bemerkung
Ist $\alpha\colon V \longrightarrow V'$ ein Morphismus von Varietäten, so induziert

$$\alpha^*\colon K[V'] \longrightarrow K[V]\,,\ f \longmapsto f \circ \alpha\,,$$

eine K-lineare Abbildung

$$\boxed{(d\alpha)_v\colon T_vV \longrightarrow T_{\alpha(v)}V'\,,\ D \longmapsto D \circ \alpha^*}\,,$$

genannt *Differential von* α *in* v oder *Tangentialabbildung von* α *in* v . Für $V \xrightarrow{\alpha} V' \xrightarrow{\beta} V''$ gilt die *Kettenregel*

$$\boxed{d(\beta \circ \alpha)_v = (d\beta)_{\alpha(v)} \circ (d\alpha)_v}\,.$$

Ferner gilt: Ist $\alpha\colon V \longrightarrow V'$ ein Isomorphismus von Varietäten, so ist $(d\alpha)_v$ ein Isomorphismus $\forall\, v \in V$ (vgl. Satz 2.9).
Sei $\mathfrak{m}_v := \{f \in K[V] \mid f(v) = 0\} = \operatorname{kern}(K[V] \longrightarrow K\,,\ f \longmapsto f(v))$. 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

$$\ell(D)\colon \mathfrak{m}_v/\mathfrak{m}_v^2 \longrightarrow K\,.$$

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 Umkehrung

$$\begin{aligned}&\operatorname{Hom}_K(\mathfrak{m}_v/\mathfrak{m}_v^2, K) \longrightarrow T_vV\,,\\ &\qquad\psi \longmapsto D_\psi\colon K[V] \longrightarrow K_v\,,\ f \longmapsto \psi(f - f(v) + \mathfrak{m}_v^2)\,.\end{aligned}$$

Beweis. Da $f(v) = 0\ \forall\, f \in \mathfrak{m}_v$ gilt, ist $f(D_\psi) = \psi$ und $D_{f(D)} = D\ \forall\, D \in T_vV$.
Noch zu zeigen ist, daß D_ψ eine K-Derivation ist. Es ist

$$\begin{aligned} D_\psi(fg) &\underset{\text{Def.}}{=} \psi(fg - f(v)g(v) - \mathfrak{m}_v^2) \text{ und}\\ fD_\psi(g) + gD_\psi(f) &= f(v)\psi(g - g(v) + \mathfrak{m}_v^2) + g(v)\psi(f - f(v) + \mathfrak{m}_v^2)\\ &\underset{\psi\text{ lin.}}{=} \psi(f(v)g - f(v)g(v) + g(v)f - g(v)f(v) + \mathfrak{m}_v^2)\,.\\ \text{Es ist } h &:= fg - f(v)g - g(v)f + g(v)f(v)\\ &= \underbrace{(f - f(v))}_{\in\mathfrak{m}_v}\cdot\underbrace{(g - g(v))}_{\in\mathfrak{m}_v}\,. \end{aligned}$$

Daher folgt durch Addition von h in der großen Klammer, daß

$$fD_\psi(g) + gD_\psi(f) = \psi(fg - f(v)g + \mathfrak{m}_v^2) = D_\psi(fg)\ \forall\, f, g \in K[V]$$

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 ein $f \in K[V]$. Ist V irreduzibel, so gilt

$$\varinjlim_{\substack{U \text{ offen}\\ U\ni v}} \mathcal{O}_V(U) \underset{\text{Aufg20}}{=} \varinjlim_{V_f\ni v} \mathcal{O}_V(V_f) \underset{2.13}{=} \varinjlim_{f(v)\neq 0} K[V]_f = \bigcup_{f(v)\neq 0} K[V]_f\,,$$

da $K[V]$ Integritätsring $= \mathcal{O}_v$ (vgl. 2.13). Man definiert daher den *Halm*

$$\mathcal{O}_v := \varinjlim_{\substack{U \text{ offen}\\ U\ni v}} \mathcal{O}_V(U)$$

auch für eine beliebige affine Varietät. Es ist $\mathcal{O}_v$ ein lokaler Ring mit maximalem Ideal M_v, und es gilt $\mathcal{O}_v/M_v \simeq K$.

Bemerkung1) Für $v \in V$ ist

$$\boxed{T_v V \simeq \mathrm{Der}_K(\mathcal{O}_v, K)}$$

(Dies folgt aus der Quotientenregel, vgl. Springer 4.15).

2) Aus 1) und der Definition des Halmes folgt $T_v V \simeq T_v U$ für jede offene Menge $U \ni v$ in V.
Sei V irreduzibel.

3) $\dim_K(T_v V) \geq \dim V \; \forall \, v \in V$.

4) Ein Punkt $v \in V$ heißt *einfach*, falls $\dim_K(T_v V) = \dim V$. Die Menge der einfachen Punkte von V liegt dicht in V (vgl. Springer 4.3.3).

Zum Beweis von 3. 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

$$\dim_K(T_v V) \underset{6.6}{=} \dim_K(M_v/M_v^2) \geq \dim \mathcal{O}_v = \dim V \,.$$

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 Der Tangentialraum von G in e

Seien K algebraisch abgeschlossen und G eine lineare algebraische Gruppe über K.

Bemerkung (i) $T_e G = T_e G^0$.

(ii) G ist glatt, d.h. jeder Punkt von G ist einfach.

(iii) $\dim G^0 = \dim_K(T_e G)$.

zum Beweis. (i) folgt aus 6.7.1, da G^0 offen in G.

(ii) Nach 6.7.4 gibt es einfache Punkte in G. Da $G \longrightarrow G$, $x \longmapsto gx$, für jedes $g \in G$ ein Isomorphismus von Varietäten ist, folgt (ii).

(iii) Nach (ii) ist e einfach.

□

Sei $A = K[G] \underset{2.7}{=} \operatorname{Mor}(G, K)$. Jede K-Derivation $D\colon A \longrightarrow A\,,\ f \longmapsto D_f\,,$ definiert eine K-Derivation $D_e\colon A \longrightarrow K_e\,,\ f \longmapsto (Df)(e)\,.$

Satz

Die K-lineare Abbildung $\operatorname{Der}_K(A, A) \longrightarrow T_eG\,,\ D \longmapsto D_e\,,$ *induziert einen Isomorphismus* $\psi\colon\ \operatorname{Lie} G \longrightarrow T_eG$ *von K-Vektorräumen.*

Beweis. **Injektivität:** Sei $D \in \operatorname{Lie} G$ mit $D_e = 0$. Für alle $f \in A$ und für alle $g \in G$ folgt dann

$$\begin{aligned}
0 = D_e(\lambda_g(f)) &= D(\lambda_g(f))(e) && \text{nach Definition von } D_e\\
&= ((D \circ \lambda_g)(f))(e)\\
&= ((\lambda_g \circ D)(f))(e) && \text{nach Definition von } \operatorname{Lie} G \text{ in 5.5}\\
&= (Df)(g^{-1}e) && \text{nach Definition von } \lambda_g\\
&= (Df)(g^{-1})
\end{aligned}$$

und also $Df = 0\ \forall\, f \in A$, d.h. $D = 0$.

Surjektivität: Sei $\delta \in T_eG$. Dann ist die *Konvolution*

$$*\delta\colon A \longrightarrow A\,,\ f \longmapsto f * \delta\colon \begin{cases} G \longrightarrow K\,,\\ x \longmapsto \delta(\lambda_{x^{-1}}(f))\,,\end{cases}$$

eine Derivation, denn für $x \in G$ und $f, g \in A$ ist

$$\begin{aligned}
(fg * \delta)(x) &= \delta(\lambda_{x^{-1}}(fg)) = \delta(\lambda_{x^{-1}}(f)\lambda_{x^{-1}}(g))\\
&= f(x)\cdot\delta(\lambda_{x^{-1}}(g)) + g(x)\cdot\delta(\lambda_{x^{-1}}(f)), \quad \text{da } \delta \in \operatorname{Der}_K(A, K_e)\\
&= (f(g * \delta) + g(f * \delta))(x)\,.
\end{aligned}$$

Ferner ist $*\delta$ linksinvariant, denn für $x, g \in G$ und $f \in A$ ist

$$\begin{aligned}
((\lambda_g \circ *\delta)(f))(x) &= (\lambda_g(f * \delta))(x)\\
&= (f * \delta)(g^{-1}x) && \text{(Definition von } \lambda_g)\\
&= \delta(\lambda_{x^{-1}g}(f)) && \text{(Definition von } f * \delta)\\
&= \delta(\lambda_{x^{-1}}(\lambda_g(f))\\
&\underset{\text{Def. von } *\delta}{=} (\lambda_g(f) * \delta)(x)\\
&= ((*\delta \circ \lambda_g)(f))(x)
\end{aligned}$$

Es ist $(\psi(*\delta))(f) \underset{\text{Def. von } \psi}{=} (*\delta)e(f) = (f * \delta)(e) = \delta(f)$. Also $\psi(*\delta) = \delta$.

$\square$

6.9 Die Liealgebra $\mathrm{L}(G)$

Sei $\mathfrak{g} := \mathrm{L}(G) := T_eG$ als K-Vektorraum, und die Liestruktur von $\mathfrak{g}$ sei durch Strukturtransport von $\mathrm{Lie}(G)$ vermöge $\psi\colon \mathrm{Lie}(G) \xrightarrow[6.8]{\sim} T_eG$ gegeben.

Bemerkung

Ist $\alpha\colon G \longrightarrow G'$ ein Morphismus von algebraischen Gruppen, so ist die Tangentialabbildung

$$(d\alpha)_e\colon \mathfrak{g} \longrightarrow \mathfrak{g}',\ \delta \longmapsto \delta \circ \alpha^*,$$

ein Liealgebrahomomorphismus (nachzurechnen ist, daß die Lieklammer respektiert wird).

6.10 Die adjungierte Darstellung

Für $g \in G$ ist $\mathrm{Ad}\, g\colon T_eG \longrightarrow T_eG$ das Differential in e des inneren Automorphismus $G \longrightarrow G$, $x \longrightarrow gxg^{-1}$. Nach 6.9 ergibt dies einen Automorphismus $\mathrm{Ad}\, g\colon \mathfrak{g} \longrightarrow \mathfrak{g}$, und man erhält einen Morphismus $\mathrm{Ad}\colon G \longrightarrow \mathrm{GL}(\mathfrak{g})$ von algebraischen Gruppen. Ist G eine abgeschlossene Untergruppe von $\mathrm{GL}_n(K)$, so ist $\mathrm{Ad}\, g$ die Konjugation mit g.

6.11 Beispiele

1) Sei $G = \mathbb{G}_{\mathrm{a}}(K)$, also $K[G] = K[X]$. Die Derivationen, die mit den Translationen $X \longmapsto X + a$ kommutieren, sind die Vielfachen von $D = \frac{d}{dT}$. Es ist $\mathfrak{g} = KD$ eindimensional mit $[D, D] = 0$ (und $D^p = 0$, wenn $\mathrm{char}(K) =: p > 0$).

2) $G = \mathbb{G}_{\mathrm{a}}(K)$. Die Derivationen, die mit den Translationen $X \longmapsto aX$ vertauschbar sind„ sind die Vielfachen von $X\frac{d}{dX}$. Ist $\mathrm{char}(K) =: p > 0$, so ist $D^p = D$. Es ist $[D, D] = 0$.

7 Index